デベロッパーガイド

AWS WAF、 AWS Firewall Manager AWS Shield Advanced、および AWS Shield ネットワークセキュリティディレクター



Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS WAF、 AWS Firewall Manager AWS Shield Advanced、および AWS Shield ネットワークセキュリティディレクター: デベロッパーガイド

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは、お客様に混乱を招く可能性がある態様、または Amazon の信用を傷つけたり、失わせたりする態様において、Amazon のものではない製品またはサービスに関連して使用してはなりません。Amazon が所有しないあらゆる商標は、各所有者の財産です。これらの各所有者は、必ずしも Amazon と提携もしくは関連し、または Amazon の支援を受けているとは限りません。

Table of Contents

..... xiii
Shield Advanced AWS WAF、 AWS Shield ネットワークセキュリティディレクター、Firewall Manager とは 1
AWS WAF 1
Shield アドバンスド 3
AWS Shield ネットワークセキュリティディレクター 4
AWS Firewall Manager 4
アカウントをセットアップする 5
にサインアップする AWS アカウント 5
ツールをダウンロード 5
AWS WAF 7
の開始方法 AWS WAF 8
セットアップ AWS WAF (新しいコンソール) 9
セットアップ AWS WAF (標準コンソール) 13
の AWS WAF 仕組み 20
で保護できるリソース AWS WAF 22
更新されたコンソールエクスペリエンスを使用する 23
新しいダッシュボードを理解する 25
保護を設定する 27
保護パック (ウェブ ACL) を作成する 29
保護パック (ウェブ ACL) を編集する 40
ルールグループの動作を管理する 46
AWS リソースとの保護の関連付けまたは関連付け解除 50
ルールとルールグループとともに保護パック (ウェブ ACL) を使用する 53
保護パック (ウェブ ACL) のデフォルトアクションの設定 61
ボディ検査に関する考慮事項 62
CAPTCHA、チャレンジ、トークンの設定 64
ウェブトラフィックメトリクスの表示 65
保護パック (ウェブ ACL) の削除 65
AWS WAF ルール 67
ルールアクションの使用 69
ルールステートメントの使用 73
文字列一致ルールステートメントを使用する 105
論理ルールステートメントの使用 131

レートベースのルールステートメントの使用 140
ルールグループステートメントの使用 161
AWS WAF ルールグループ 164
マネージドルールグループの使用 165
独自のルールグループの管理 391
AWS Marketplace ルールグループ 397
他のサービスのルールグループを識別する 401
ウェブ ACL キャパシティユニット (WCU) 402
ルールグループまたは保護パック (ウェブ ACL) の WCU を決定する 404
オーバーサイズウェブリクエストコンポーネント 404
オーバーサイズのコンポーネントのブロック 407
サポートされている正規表現 408
IP セットおよび正規表現パターンセット 408
IP セットの作成と管理 409
正規表現パターンセットの作成と管理 411
カスタマイズされたウェブリクエストとレスポンス 414
カスタムリクエストヘッダーの挿入 415
動的ラベル補間 419
カスタムレスポンスの送信 424
サポートされているレスポンスステータスコード 427
ウェブリクエストのラベル付け 429
ラベリングの仕組み 431
ラベル構文と命名要件 433
ラベルを追加するルール 436
ラベルに一致するルール 437
インテリジェントな脅威の軽減 442
緩和アクション 443
ベストプラクティス 454
インテリジェントな脅威の軽減おけるトークン 457
AWS WAF Fraud Control アカウント作成不正防止 (ACFP) 472
AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) 496
AWS WAF ボットコントロール 516
分散型サービス拒否 (DDoS) の防止 556
クライアントアプリケーション統合 568
CAPTCHA および Challenge 610
AI トラフィック収益化 623

AI トラフィック収益化の仕組み ... 623
AI トラフィック収益化の開始方法 ... 625
料金設定 ... 629
支払いネットワークと決済 ... 632
収益分析 ... 633
AI エージェントへのライセンス条項の伝達 ... 635
ウェブトラフィックのデータ保護と ログ記録 ... 636
ログ記録 ... 637
データ保護 ... 682
保護のテストと調整 ... 709
ハイレベルステップのテストとチューニング ... 711
テストの準備 ... 712
AWS WAF 保護のモニタリングと調整 ... 714
本番環境で保護の有効化 ... 732
Amazon CloudFront AWS WAF での の使用 ... 734
がさまざまなディストリビューションタイプと AWS WAF 連携する方法 ... 735
CloudFront 料金プラン AWS WAF での の使用 ... 737
AI トラフィック収益化 ... 738
ユースケース ... 739
AWS WAF サービスの使用におけるセキュリティ ... 744
データの保護 ... 745
での IAM の使用 AWS WAF ... 746
ログ記録とモニタリング ... 820
コンプライアンス検証 ... 821
耐障害性の構築 ... 822
インフラストラクチャセキュリティ ... 822
AWS WAF クォータ ... 823
AWS WAF Classic リソースの への移行 AWS WAF ... 829
に移行する理由 AWS WAF ... 830
移行に関する注意事項 ... 832
移行の仕組み ... 833
保護パック (ウェブ ACL) の移行 ... 834
AWS WAF クラシック ... 841
AWS WAF Classic のセットアップ ... 842
にサインアップする AWS アカウント ... 5
ツールをダウンロード ... 843

AWS WAF Classic の仕組み ... 844
AWS WAF クラシック料金 ... 848
AWS WAF Classic の開始方法 ... 849
ステップ 1: AWS WAF Classic をセットアップする ... 850
ステップ 2: ウェブ ACL を作成する ... 851
ステップ 3: IP 一致条件を作成する ... 852
ステップ 4: Geo 一致条件を作成する ... 852
ステップ 5: 文字列一致条件を作成する ... 853
ステップ 5A: (オプション) 正規表現条件を作成する ... 856
ステップ 6: SQL インジェクション一致条件を作成する ... 857
ステップ 7: (オプション) 追加の条件を作成する ... 859
ステップ 8: ルールを作成して条件を追加する ... 859
ステップ 9: ルールをウェブ ACL に追加する ... 861
ステップ 10: リソースをクリーンアップする ... 862
ウェブアクセスコントロールリスト (ウェブ ACL) の作成と設定 ... 865
条件の使用 ... 867
ルールの使用 ... 917
ウェブ ACL の使用 ... 930
で使用する AWS WAF Classic ルールグループの使用 AWS Firewall Manager ... 947
AWS WAF Classic ルールグループの作成 ... 948
AWS WAF Classic ルールグループへのルールの追加と削除 ... 950
AWS WAF Classic ルールを有効にする AWS Firewall Manager ための の開始方法 ... 951
ステップ 1: 前提条件を満たす ... 953
ステップ 2: ルールを作成する ... 953
ステップ 3: ルールグループを作成する ... 954
ステップ 4: AWS Firewall Manager AWS WAF Classic ポリシーを作成して適用する ... 956
チュートリアル: 階層ルールによる AWS Firewall Manager ポリシーの作成 ... 958
ステップ 1: Firewall Manager 管理者アカウントを指定する ... 959
ステップ 2: Firewall Manager 管理者アカウントを使用してルールグループを作成する ... 960
ステップ 3: Firewall Manager ポリシーを作成して共通のルールグループをアタッチする ... 960
ステップ 4: アカウント固有のルールを追加する ... 960
結論 ... 961
ウェブ ACL トラフィック情報のログ記録 ... 961
レートベースのルールごとにブロックされている IP アドレスの一覧表示 ... 969
AWS WAF Classic が Amazon CloudFront 機能と連携する方法 ... 970
CloudFront カスタムエラーページでの AWS WAF Classic の使用 ... 971

独自の HTTP サーバーで実行されているアプリケーションに CloudFront で AWS WAF Classic を使用する 971
CloudFront が応答する HTTP メソッドの選択 972
セキュリティ 973
データ保護 974
ID とアクセス管理 976
ログ記録とモニタリング 999
コンプライアンス検証 1000
耐障害性 1001
インフラストラクチャセキュリティ 1001
AWS WAF クラシッククォータ 1002
AWS Shield 1007
Shield と Shield Advanced の仕組み 1008
AWS Shield Standard の概要 1010
AWS Shield Advanced の概要 1010
Shield Advanced が保護するリソース 1012
Shield Advanced の機能とオプション 1013
にサブスクライブするかどうかの決定 AWS Shield Advanced 1016
DDoS 攻撃の例 1018
Shield がイベントを検出する方法 1019
Shield がイベントを緩和する方法 1024
DDoS 耐障害性アーキテクチャの構築 1032
ウェブアプリケーションの DDoS 耐障害性構造の例 1033
TCP および UDP アプリケーションの DDoS 耐障害性アーキテクチャの例 1035
Shield Advanced と他の の組み合わせ AWS のサービス 1038
セットアップ AWS Shield Advanced 1039
Shield Advanced をサブスクライブする 1040
リソース保護の追加と設定 1042
SRT サポートの設定 1048
DDoS ダッシュボードの作成 1050
SRT のサポート 1051
SRT へのアクセスの許可 1052
プロアクティブエンゲージメントの設定 1055
SRT への問い合わせ 1057
SRT によるカスタム緩和策の設定 1058
リソース保護 1058

保護されたリソースのリスト 1059
Amazon EC2 インスタンスおよび Network Load Balancer を保護する 1061
アプリケーションレイヤーの保護 (レイヤー 7) 1062
ヘルスチェックを使用したヘルスベースの検出 1080
リソースへの保護の追加 1090
保護の編集 1091
アラームと通知の作成 1093
リソースからの保護の削除 1094
保護グループ 1095
保護の変更の追跡 1098
DDoS イベントの可視性 1099
グローバルおよびアカウントアクティビティ 1100
イベント 1103
アカウント全体にわたるイベントの可視性 1114
攻撃フローログ 1116
フローログを Amazon S3 に発行できるようにする 1117
フローログ配信を有効にするには 1119
フローログファイル 1120
フローログレコードの構文 1120
DDoS イベントへの対応 1121
アプリケーションレイヤー攻撃についてのサポートへの問い合わせ 1122
アプリケーションレイヤー攻撃の手動による緩和 1124
攻撃後のクレジットのリクエスト 1125
Shield サービスの利用におけるセキュリティ 1127
データの保護 1128
Shield での IAM の使用 1129
ログ記録とモニタリング 1156
コンプライアンス検証 1157
耐障害性の構築 1157
インフラストラクチャセキュリティ 1157
AWS Shield Advanced クォータ 1158
AWS Shield ネットワークセキュリティディレクター (プレビュー) 1159
AWS Shield ネットワークセキュリティディレクターの料金 1159
ユースケース 1159
主要なコンセプト 1160
検出結果のリファレンス 1161

アカウントをセットアップする 1164
前提条件 1165
AWS Organizations の統合について 1165
委任管理者の選択 1166
委任管理者の IAM 要件 1166
セットアップチェックリスト 1169
AWS Shield ネットワークセキュリティディレクターの有効化 1169
AWS Shield ネットワークセキュリティディレクターの有効化とサービス管理者の委任 ... 1170
委任された管理者を持つメンバーアカウントの AWS Shield ネットワークセキュリティディレクターの有効化 1171
リソースと検出結果の調査 1172
検出結果があるアカウントを特定するには 1172
Amazon Q Developer でネットワークセキュリティを分析する 1176
質問例 1177
データ保護に関する考慮事項 1177
AWS Shield ネットワークセキュリティディレクターのクォータ 1177
AWS Shield ネットワークセキュリティディレクターのトラブルシューティング 1178
サポートされていないクロスアカウント共有リソース 1178
リソース、結果、および抑制の可用性 1179
パフォーマンスに関する考慮事項 1179
その他のリソース 1179
セキュリティ 1180
Identity and Access Management 1181
アイデンティティベースのポリシーの例 1182
サービスにリンクされたロールの使用 1186
を使用した AWS Shield Network Security Director API コールのログ記録 AWS CloudTrail 1194
CloudTrail のネットワークセキュリティディレクター情報 1195
CloudTrail によってログに記録されるネットワークセキュリティディレクター API オペレーション 1195
ネットワークセキュリティディレクターのログファイルエントリについて 1195
Amazon CloudWatch による CloudTrail ログのモニタリング 1197
ネットワークセキュリティディレクターを使用した CloudTrail のベストプラクティス 1197
AWS Firewall Manager 1198
AWS Firewall Manager 前提条件 1199
Firewall Manager を使用する AWS Organizations ための結合と設定 1199
AWS Firewall Manager デフォルトの管理者アカウントの作成 1200

Firewall Manager の使用 AWS Config の有効化 1201
AWS Marketplace でサブスクライブし、Firewall Manager サードパーティーポリシーのサードパーティー設定を構成する 1203
を使用した Network Firewall および DNS Firewall ポリシーのリソース共有の有効化 AWS RAM 1204
デフォルトでは無効になっているリージョン AWS Firewall Manager での の使用 1205
Firewall Manager 管理者を使用する 1205
Firewall Manager 管理者アカウントの作成。 1207
Firewall Manager 管理者アカウントの更新 1209
Firewall Manager 管理者アカウントを取り消す 1210
デフォルトの管理者アカウントの変更 1210
管理者アカウントに対する変更の却下 1211
AWS Firewall Manager ポリシーの設定 1212
AWS WAF ポリシーの設定 1213
AWS Shield Advanced ポリシーの設定 1216
Amazon VPC セキュリティグループポリシーの設定 1222
Amazon VPC ネットワーク ACL ポリシーの設定 1226
AWS Network Firewall ポリシーの設定 1229
DNS Firewall ポリシーの設定 1233
Palo Alto Networks Cloud NGFW ポリシーの設定 1235
Fortigate CNF ポリシーの設定 1239
AWS Firewall Manager ポリシーの使用 1243
全般設定 1245
ポリシーの作成 1245
ポリシーの削除 1284
ポリシースコープの使用 1285
AWS WAF ポリシー 1287
AWS Shield Advanced ポリシー 1301
セキュリティグループポリシー 1307
ネットワーク ACL ポリシー 1320
Network Firewall ポリシー 1329
DNS Firewall ポリシー 1341
Palo Alto Networks Cloud NGFW ポリシー 1344
Fortigate CNF ポリシー 1344
Network Firewall ポリシーと DNS Firewall ポリシーのリソース共有 1345
マネージドリストの使用 1346

マネージドリストのバージョニング 1347
マネージドリストの使用 1348
カスタムマネージドリストの作成 1348
マネージドリストの表示 1350
カスタムマネージドリストの削除 1351
リソースをグループ化する 1353
Firewall Manager でリソースセットを操作するときの考慮事項 1353
リソースセットの作成 1354
リソースセットの削除 1355
ポリシーのコンプライアンスの表示 1355
Firewall Manager と Security Hub CSPM の統合 1360
AWS WAF ポリシーの検出結果 1361
AWS Shield Advanced ポリシーの検出結果 1362
セキュリティグループ共通ポリシーの検出結果 1363
セキュリティグループコンテンツ監査ポリシーの検出結果 1364
セキュリティグループ使用状況監査ポリシーの検出結果 1364
DNS Firewall ポリシーの検出結果 1365
AWS Config 検出結果 1366
Firewall Manager サービスの利用におけるセキュリティ 1367
データ保護 1368
Identity and Access Management 1369
ログ記録とモニタリング 1400
コンプライアンス検証 1401
回復力 1401
インフラストラクチャセキュリティ 1401
AWS Firewall Manager クォータ 1402
ソフトクォータ 1402
ハードクォータ 1406
Firewall Manager での AWS WAF Classic ウェブ ACLs移行 1408
AWS WAF Classic ポリシーでのウェブ ACLs移行 1408
Shield アドバンストポリシーでのウェブ ACL の移行 1409
モニタリング 1411
モニタリングツール 1412
自動モニタリングツール 1412
手動ツール 1414
CloudWatch によるモニタリング 1414

メトリクスおよびディメンションの表示 1415
AWS WAF メトリクスとディメンション 1416
AWS Shield Advanced メトリクス 1434
AWS Firewall Manager 通知 1440
での AWS CloudTrail API コールのログ記録 1440
AWS WAF の情報 AWS CloudTrail 1441
AWS Shield Advanced CloudTrail の情報 1451
AWS Firewall Manager CloudTrail の情報 1454
AWS WAF および AWS Shield Advanced API の使用 1457
AWS SDKsの使用 1457
AWS WAF または Shield Advanced への HTTPS リクエストの実行 1457
リクエストの URI 1457
HTTP ヘッダー 1457
HTTP リクエストボディ 1459
HTTP レスポンス 1460
エラーレスポンス 1461
リクエストの認証 1461
関連情報 1464
ドキュメント履歴 1466
2018 年よりも前の更新 1528
..... mdxxxii

の新しいコンソールエクスペリエンスの紹介 AWS WAF

更新されたエクスペリエンスを使用して、 コンソールの任意の場所で AWS WAF 機能にアクセスできるようになりました。詳細については、「コンソールの使用」を参照してください。

AWS WAF AWS Shield Advanced AWS Shield ネットワークセキュリティディレクターとは何ですか AWS Firewall Manager?

AWS WAF、、AWS Shieldおよび をAWS Firewall Manager一緒に使用して、包括的なセキュリティソリューションを作成できます。 AWS WAF は、エンドユーザーがアプリケーションに送信するウェブリクエストをモニタリングし、コンテンツへのアクセスを制御するために使用できるウェブアプリケーションファイアウォールです。Shield Advanced は、ネットワークレイヤーとトランスポートレイヤー (レイヤー 3 と 4) およびアプリケーションレイヤー (レイヤー 7) で、 AWS リソースに対する分散型サービス拒否 (DDoS) 攻撃に対する保護を提供します。 AWS Firewall Manager は、新しいリソースが追加されても、アカウントとリソース間で AWS WAF や Shield Advanced などの保護を管理します。

トピック

- とは AWS WAF
- とは AWS Shield Advanced
- AWS Shield ネットワークセキュリティディレクターとは
- とは AWS Firewall Manager

とは AWS WAF

AWS WAF は、保護されたウェブアプリケーションリソースに転送される HTTP および HTTPS リクエストをモニタリングできるウェブアプリケーションファイアウォールです。以下のリソースタイプを保護できます。

- Amazon CloudFront ディストリビューション
- Amazon API Gateway REST API
- Application Load Balancer
- AWS AppSync GraphQL API
- Amazon Cognito ユーザープール
- AWS App Runner サービス
- Amazon Bedrock AgentCore Gateway

- AWS Verified Access インスタンス
- AWS Amplify

AWS WAF では、コンテンツへのアクセスを制御できます。リクエストの発生元の IP アドレスまたはクエリ文字列の値など、指定した条件に基づいて、保護されたリソースはリクエストに対し、リクエストされたコンテンツ、HTTP 403 ステータスコード (禁止)、カスタム応答のリクエストのいずれかで応答します。

最も簡単なレベルで、次のいずれかの動作 AWS WAF を選択します。

- 指定したリクエストを除くすべてのリクエストを許可する – これは、Amazon CloudFront、Amazon API Gateway、Application Load Balancer、 AWS AppSync、Amazon Cognito AWS App Runner、Amazon Bedrock AgentCore Gateway、または AWS Verified Access がパブリックウェブサイトのコンテンツを提供するが、攻撃者からのリクエストをブロックする場合に便利です。
- 指定したリクエスト以外のすべてのリクエストをブロックする - これは、制限されたウェブサイトのコンテンツを提供する場合に便利です。ユーザーは、ウェブサイトをウェブリクエストのプロパティ (ウェブサイトを参照するために使用する IP アドレスなど) によって簡単に識別できるようになります。
- 条件に一致するリクエストをカウントする - Count アクションを使用して、処理方法を変更せずにウェブトラフィックを追跡できます。これは、一般的なモニタリングのほか、新しいウェブリクエスト処理ルールをテストするためにも使用できます。ウェブリクエストの新しいプロパティに基づいてリクエストを許可またはブロックする場合は、まず、それらのプロパティに一致するリクエストをカウント AWS WAF するように を設定できます。これにより、ルールを切り替えて一致するリクエストを許可またはブロックする前に、新しい構成設定を確認できます。
- 基準に一致するリクエストに対して CAPTCHA または、チャレンジチェックを実行する – リクエストに対する CAPTCHA とサイレントチャレンジコントロールを実装して、保護されたリソースへのボットトラフィックを削減することができます。

を使用すると AWS WAF 、いくつかの利点があります。

- 指定した基準を使用した、ウェブ攻撃に対する追加の保護。基準を定義するには、次のようなウェブリクエストの特性を使用します。
  - リクエストの発生元の IP アドレス。
  - リクエスト送信元の国。
  - リクエストヘッダーの値。

- リクエストに含まれる文字列 (正規表現パターンと一致する特定の 1 つ以上の文字列)。
- リクエストの長さ。
- 悪意のある可能性がある SQL コード (SQL インジェクション) の有無。
- 悪意のある可能性があるスクリプト (クロスサイトスクリプティング) の有無。

- 指定された基準を満たすウェブリクエストを許可、ブロック、またはカウントするルール。また、ルールは、指定された基準を満たすだけでなく、1 分間または 5 分間にわたって指定された数のリクエストを超えるウェブリクエストをブロックまたはカウントすることもできます。
- 複数のウェブアプリケーションで再利用できるルール。
- AWS および AWS Marketplace 販売者からのマネージドルールグループ。
- リアルタイムのメトリクスとサンプリングされたウェブリクエスト。
- AWS WAF API を使用した自動管理。

リソースに追加する保護をよりきめ細かに制御したい場合は、 AWS WAF のみを使用することが適切な選択である場合があります。詳細については AWS WAF、「」を参照してくださいAWS WAF。

とは AWS Shield Advanced

AWS WAF ウェブアクセスコントロールリスト (ウェブ ACLs) を使用すると、分散サービス拒否 (DDoS) 攻撃の影響を最小限に抑えることができます。DDoS 攻撃に対する保護を強化するために、は AWS Shield Standard と AWS も提供します AWS Shield Advanced。 AWS Shield Standard は、すでに や他の AWS サービスに対して支払っている料金を超える追加コストなしで自動的に含まれ AWS WAF ます。

Shield Advanced は、Amazon EC2 インスタンス、Elastic Load Balancing ロードバランサー、CloudFront ディストリビューション、Route 53 ホストゾーン、および AWS Global Accelerator 標準アクセラレーターに対して拡張 DDoS 攻撃保護を提供します。Shield Advanced には追加料金が発生します。Shield Advanced のオプションと機能には、アプリケーションレイヤー DDoS 自動緩和、高度なイベント可視性、および Shield Response Team (SRT) からの専用サポートが含まれます。認知度の高いウェブサイトを所有している場合、または頻繁な DDoS 攻撃を受けやすいという場合は、Shield Advanced が提供する追加保護の購入を検討してください。詳細については、「AWS Shield Advanced 機能とオプション」および「追加の保護をサブスクライブ AWS Shield Advanced して適用するかどうかを決定する」を参照してください。

AWS Shield ネットワークセキュリティディレクターとは

AWS Shield ネットワークセキュリティディレクターは、 アカウント全体でコンピューティング、ネットワーク、およびネットワークセキュリティリソースを検出することで AWS 、環境を保護するのに役立ちます。 ネットワークセキュリティディレクターは、 AWS ベストプラクティスと脅威インテリジェンスに照らしてネットワークトポロジとセキュリティ設定を分析することで、各リソースのセキュリティ設定を評価します。セキュリティを強化するために、ネットワークセキュリティディレクターは検出結果を低い重要度から重大な重要度で評価し、Amazon Q Developer を通じて自然言語クエリを使用して調べることができる特定の修復手順を共有します。

AWS Shield ネットワークセキュリティディレクターの詳細については、「」を参照してくださいAWS Shield ネットワークセキュリティディレクター (プレビュー)。

とは AWS Firewall Manager

AWS Firewall Manager は、Amazon VPC セキュリティグループとネットワーク ACLs、 AWS Shield Advanced Amazon Route 53 Resolver DNS Firewall AWS WAFなど、さまざまな保護のために AWS Network Firewall複数のアカウントとリソースにわたる管理およびメンテナンスタスクを簡素化します。Firewall Manager を使用すると、保護を 1 回設定するだけで、アカウントとリソースに (追加する新しいアカウントとリソースにも) その保護が自動的に適用されます。

Firewall Manager の詳細については、「AWS Firewall Manager」を参照してください。

アカウントを設定してサービスを使用する

このトピックでは、アカウントの作成、使用の準備、 AWS WAF AWS Firewall Managerなどの準備手順について説明します AWS Shield Advanced。これらの暫定項目は請求されません。使用した AWS サービスに対してのみ課金されます。

トピック

- にサインアップする AWS アカウント
- ツールをダウンロード

にサインアップする AWS アカウント

の使用を開始するには AWS、 が必要です AWS アカウント。の作成の詳細については AWS アカウント、 AWS アカウント管理 リファレンスガイドの「 の開始方法 AWS アカウント」を参照してください。

ツールをダウンロード

には AWS WAF、、 AWS Shield Advanced、および のコンソール AWS マネジメントコンソール が含まれていますが AWS Firewall Manager、プログラムでサービスにアクセスする場合は、以下を参照してください。

- API ガイドには、サービスがサポートする操作が記載されており、関連する SDK および CLI のドキュメントへのリンクも確認できます。
  - AWS WAF API リファレンス
  - AWS Shield Advanced API リファレンス
  - AWS Firewall Manager API リファレンス
- raw HTTP リクエストの組み立てなどの低レベルの詳細を処理せずに API を呼び出すには、 AWS SDK を使用できます。 AWS SDKs は、 AWS サービスの機能をカプセル化する関数とデータ型を提供します。 AWS SDK をダウンロードしてインストール手順にアクセスするには、該当するページを参照してください。
  - Java
  - JavaScript
  - .NET

- Node.js
- PHP
- Python
- Ruby

AWS SDKs「Amazon Web Services のツール」を参照してください。

- AWS Command Line Interface (AWS CLI) を使用して、コマンドラインから複数の AWS サービスを制御できます。スクリプトを使用してコマンドを自動化することもできます。詳細については、「AWS Command Line Interface」を参照してください。
- AWS Tools for Windows PowerShell はこれらの AWS サービスをサポートしています。詳細については、「AWS Tools for PowerShell コマンドレットリファレンス」(Cmdlet リファレンス) を参照してください。

AWS WAF

AWS WAF は、保護されたウェブアプリケーションリソースに転送される HTTP(S) リクエストをモニタリングできるウェブアプリケーションファイアウォールです。以下のリソースタイプを保護できます。

- Amazon CloudFront ディストリビューション
- Amazon API Gateway REST API
- Application Load Balancer
- AWS AppSync GraphQL API
- Amazon Cognito ユーザープール
- AWS App Runner サービス
- Amazon Bedrock AgentCore Gateway
- AWS Verified Access インスタンス
- AWS Amplify

AWS WAF では、コンテンツへのアクセスを制御できます。リクエストの発生元の IP アドレスまたはクエリ文字列の値など、指定した条件に基づいて、保護されたリソースに関連付けられたサービスはリクエストに対し、リクエストされたコンテンツ、HTTP 403 ステータスコード (禁止)、カスタム応答のいずれかで応答します。

> **Note**
>
> AWS WAF を使用して、Amazon Elastic Container Service (Amazon ECS) コンテナでホストされているアプリケーションを保護することもできます。Amazon ECS は、クラスターで Docker コンテナを簡単に実行、停止、管理できる非常にスケーラブルで高速なコンテナ管理サービスです。このオプションを使用するには、サービス内のタスク間で HTTP(S) レイヤー 7 トラフィックをルーティングおよび保護 AWS WAF するために が有効になっている Application Load Balancer を使用するように Amazon ECS を設定します。詳細については、「Amazon Elastic Container Service デベロッパーガイド」の「Service load balancing」を参照してください。

トピック

- の使用を開始する AWS WAF
- の AWS WAF 仕組み
- での保護の設定 AWS WAF
- AWS WAF ルール
- AWS WAF ルールグループ
- のウェブ ACL キャパシティユニット (WCUs) AWS WAF
- でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF
- でサポートされている正規表現構文 AWS WAF
- の IP セットと正規表現パターンセット AWS WAF
- でカスタマイズされたウェブリクエストとレスポンス AWS WAF
- でのウェブリクエストのラベル付け AWS WAF
- でのインテリジェントな脅威の軽減 AWS WAF
- AI トラフィック収益化
- 保護 AWS WAF パック (ウェブ ACL) トラフィックのデータ保護と口グ記録
- AWS WAF 保護のテストとチューニング
- Amazon CloudFront AWS WAF での の使用
- AWS WAF サービスの使用におけるセキュリティ
- AWS WAF クォータ
- AWS WAF Classic リソースの への移行 AWS WAF

の使用を開始する AWS WAF

の使用開始 AWS WAF は、使用するコンソールエクスペリエンスによって異なります。どちらのエクスペリエンスでも同じコア AWS WAF 機能にアクセスできますが、ウェブアプリケーション保護の設定と管理方法は異なります。

AWS WAF には、 コンソールを使用するための 2 つのオプションがあります。

新しいコンソール は、標準のコンソールワークフローに必要なウェブ ACL 設定プロセスを簡素化することを目的としています。ガイド付きワークフローを使用して、保護パックを通じてウェブ ACL の作成および管理プロセスを簡素化できます。保護パックを使用すると、コンソールでのウェブ

ACL の使用と管理が容易になりますが、ウェブ ACL と機能的に違いはありません。新しいコンソールでは、保護設定プロセスの改善に加えて、セキュリティダッシュボードを通じて保護の可視性が向上し、 AWS WAF コンソール内のセキュリティ体制を簡単にモニタリングできるようになります。

標準 AWS WAF コンソールは、ウェブ ACLs を使用してウェブアプリケーションのファイアウォール保護を設定する従来のアプローチを提供します。個々のルールとルールグループをきめ細かく制御でき、既存の AWS WAF ユーザーにとって使い慣れています。このコンソールを使用すると、保護設定を詳細に制御できるため、セキュリティ設定を正確にカスタマイズできます。

> **Tip**
>
> ニーズに最適なコンソールエクスペリエンスを選択します。を初めて使用する場合 AWS WAF や、 AWS レコメンデーションに基づいて保護の設定を開始する場合は、新しいコンソールエクスペリエンスから始めることをお勧めします。ただし、標準エクスペリエンスは、コンソールのナビゲーションペインからいつでも開くことができます。

以下のセクションでは、両方のコンソールエクスペリエンスの開始方法に関するガイダンスを提供します。各アプローチを確認し、セキュリティ要件と運用上の好みに最も適したものを選択してください。

トピック

- 新しいコンソールエクスペリエンス AWS WAF の使用を開始する
- 標準コンソールエクスペリエンス AWS WAF の使用を開始する

新しいコンソールエクスペリエンス AWS WAF の使用を開始する

このセクションでは、簡素化された設定ワークフローと強化されたセキュリティ管理機能を提供する新しいコンソールエクスペリエンス AWS WAF を使用して を設定する方法について説明します。

新しいコンソールエクスペリエンスにアクセスする

新しい AWS WAF コンソールエクスペリエンスにアクセスするには:

新しい にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2-pro で AWS WAF コンソールを開きます。

- ナビゲーションペインで、新しいエクスペリエンスを試す を見つけて選択します。

> **Note**
>
> ナビゲーションペインのリンクを使用して、コンソールエクスペリエンスをいつでも切り替えることができます。

保護パック (ウェブ ACL) の使用を開始する

このチュートリアルでは、アプリケーションを保護するために保護パック (ウェブ ACL) を作成して設定する方法を示します。保護パック (ウェブ ACL) は、特定のワークロードタイプに合わせて事前設定されたセキュリティルールを提供します。

このチュートリアルの学習内容は次のとおりです。

- 保護パック (ウェブ ACL) を作成する
- アプリケーション固有の保護設定を構成する
- 保護する AWS リソースを追加する
- ルールを選択してカスタマイズする
- ログ記録とモニタリングプレーンを設定する

> **Note**
>
> AWS 通常、 は、このチュートリアルで作成したリソースに対して 1 日あたり 0.25 USD 未満を請求します。終了したら、不要な料金が発生しないようにリソースを削除することをお勧めします。

ステップ 1: をセットアップする AWS WAF

アカウントを設定してサービスを使用する の一般的なセットアップ手順をまだ実行していない場合、今すぐ実行してください。

ステップ 2: 保護パック (ウェブ ACL) を作成する

このステップでは、保護パック (ウェブ ACL) を作成し、アプリケーションタイプに合わせて基本的な設定を行います。

1. 新しい にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2-pro で AWS WAF コンソールを開きます。
2. ナビゲーションペインで、[リソースと保護パック (ウェブ ACL)] を選択します。
3. リソースと保護パック (ウェブ ACL) ページで、保護パック (ウェブ ACL) の追加 を選択します。
4. 「アプリについて教えてください」の「アプリカテゴリ」で、アプリケーションに最も該当するアプリカテゴリを 1 つ以上選択します。
5. トラフィックソース で、アプリケーションが処理するトラフィックのタイプを選択します。

   - API - API 専用アプリケーション用
   - ウェブ - ウェブ専用アプリケーション用
   - API とウェブの両方 - 両方のタイプのトラフィックを処理するアプリケーション用

ステップ 3: 保護するリソースを追加する

次に、保護パック (ウェブ ACL) で保護する AWS リソースを指定します。

1. 保護するリソース で、リソースの追加 を選択します。
2. この保護パック (ウェブ ACL) に関連付ける AWS リソースのカテゴリを選択します。

   - Amazon CloudFront ディストリビューション
   - リージョナルリソース

   リソースタイプの詳細については、「AWS リソースへの保護の関連付け」を参照してください。

ステップ 4: 初期保護を選択する

このステップでは、保護パック (ウェブ ACL) のルールを選択します。初めて使用する場合は、推奨オプションを選択することをお勧めします。

AWS WAF は、アプリに関するお問い合わせセクションで選択した内容に基づいて推奨を生成します。これらのパックは、アプリケーションタイプのセキュリティのベストプラクティスを実装します。

- 次へ を選択して、保護パック (ウェブ ACL) のセットアップを続行します。

> **Note**
>
> カスタムルールを作成したり、ビルドする オプションを使用したりする場合は、まず事前設定されたオプションの使用経験を積むことをお勧めします。カスタム保護パック (ウェブ ACL) とルールの作成については、「で保護パック (ウェブ ACL) を作成する AWS WAF」を参照してください。

ステップ 5: 保護パック (ウェブ ACL) 設定をカスタマイズする

次に、デフォルトのアクション、レート制限、ログ記録などの追加設定を行います。

1. 名前と説明 に、保護パック (ウェブ ACL) の名前を入力します。必要に応じて説明に説明を入力します。

   > **Note**
   >
   > 保護パック (ウェブ ACL) の作成後は、名前を変更することはできません。

2. 保護パック (ウェブ ACL) のカスタマイズ で、次の設定を行います。

   a. デフォルトルールアクション で、どのルールにも一致しないリクエストのデフォルトアクションを選択します。詳細については、「でカスタマイズされたウェブリクエストとレスポンス AWS WAF」を参照してください。

   b. ルール設定 で、以下の設定をカスタマイズします。

      - デフォルトのレート制限 - DDoS 攻撃から保護するための制限を設定する
      - IP アドレス - IP 許可/ブロックリストを設定する
      - 国固有のオリジン - 国ごとにアクセスを管理する

   c. ログ記録先 では、ログを保存する場所を設定します。詳細については、「AWS WAF ログ記録の送信先」を参照してください。

3. 設定を確認し、保護パック (ウェブ ACL) の追加 を選択します。

ステップ 6: リソースをクリーンアップする

これでチュートリアルは完了です。アカウントに AWS WAF 追加料金が発生しないようにするには、作成した保護パック (ウェブ ACL) を削除するか、本番環境のニーズに合わせて変更する必要があります。

保護パック (ウェブ ACL) を削除するには

1. ナビゲーションペインで、[リソースと保護パック (ウェブ ACL)] を選択します。
2. 作成した保護パック (ウェブ ACL) を選択します。
3. ごみ箱アイコンを選択し、「削除」と入力して削除を確認します。

> **Note**
>
> この保護パック (ウェブ ACL) を本番環境で使用する場合は、削除する代わりに、アプリケーションのセキュリティ要件に合わせて保護設定を確認して調整する必要があります。

標準コンソールエクスペリエンス AWS WAF の使用を開始する

AWS WAF コンソールでは、リクエストの送信元の IP アドレスやリクエストの値など、指定した条件に基づいてウェブリクエストをブロックまたは許可 AWS WAF するように を設定するプロセスについて説明します。このステップでは、保護パック (ウェブ ACL) を作成します。 AWS WAF 保護パック (ウェブ ACLs「」を参照してくださいでの保護の設定 AWS WAF。

このチュートリアルでは、 AWS WAF を使用して以下のタスクを実行する方法を示します。

- セットアップします AWS WAF。
- AWS WAF コンソールのウィザードを使用して、ウェブアクセスコントロールリスト (ウェブ ACL) を作成します。

  ウェブ ACL を作成するには

  1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
  2. AWS WAF ホームページから、ウェブ ACL の作成を選択します。
  3. [Name] (名前) で、このウェブ ACL の識別に使用する名前を入力します。

     > **Note**
     >
     > ウェブ ACL の作成後は、名前を変更することはできません。

  4. (オプション) 必要に応じて、[Description - optional] (説明 - オプション) に、ウェブ ACL の詳しい説明を入力します。

5. [CloudWatch metric name] (CloudWatch メトリクス名) で、必要に応じてデフォルト名を変更します。有効な文字については、コンソールのガイダンスに従ってください。名前には、特殊文字、空白や、「All」および「Default_Action」などの AWS WAF用に予約されたメトリクス名を使用できません。

   > **Note**
   >
   > ウェブ ACL の作成後は CloudWatch メトリクス名を変更できません。

6. [Resource type] (リソースタイプ) で、[CloudFront distributions] (CloudFront ディストリビューション) を選択します。[Region] (リージョン) が、CloudFront ディストリビューションの [Global (CloudFront)] (グローバル (CloudFront)) に自動的に入力されます。
7. (オプション) 関連 AWS リソース - オプションで、 AWS リソースの追加を選択します。ダイアログボックスで、関連付けるリソースを選択し、[Add] (追加) を選択します。 AWS WAF は [Describe web ACL and associated AWS resources] (ウェブ ACL と関連付けられた リソースの説明) ページに戻します。
8. [次へ] を選択します。

> **Note**
>
> AWS 通常、 は、このチュートリアルで作成したリソースに対して 1 日あたり 0.25 USD 未満を請求します。チュートリアルを終了したら、不要な料金が発生しないようにリソースを削除することをお勧めします。

ステップ 1: をセットアップする AWS WAF

アカウントを設定してサービスを使用する の一般的なセットアップ手順をまだ実行していない場合、今すぐ実行してください。

ステップ 2: ウェブ ACL を作成する

AWS WAF コンソールでは、リクエストの送信元の IP アドレスやリクエストの値など、指定した条件に基づいてウェブリクエストをブロックまたは許可 AWS WAF するように を設定するプロセスについて説明します。このステップでは、ウェブ ACL を作成します。 AWS WAF ウェブ ACLs「」を参照してください での保護の設定 AWS WAF。

ウェブ ACL を作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. AWS WAF ホームページから、ウェブ ACL の作成を選択します。
3. [Name] (名前) で、このウェブ ACL の識別に使用する名前を入力します。

   > **Note**
   >
   > ウェブ ACL の作成後は、名前を変更することはできません。

4. (オプション) 必要に応じて、[Description - optional] (説明 - オプション) に、ウェブ ACL の詳しい説明を入力します。
5. [CloudWatch metric name] (CloudWatch メトリクス名) で、必要に応じてデフォルト名を変更します。有効な文字については、コンソールのガイダンスに従ってください。名前には、特殊文字、空白や、「All」および「Default_Action」などの AWS WAF用に予約されたメトリクス名を使用できません。

   > **Note**
   >
   > ウェブ ACL の作成後は CloudWatch メトリクス名を変更できません。

6. [Resource type] (リソースタイプ) で、[CloudFront distributions] (CloudFront ディストリビューション) を選択します。[Region] (リージョン) が、CloudFront ディストリビューションの [Global (CloudFront)] (グローバル (CloudFront)) に自動的に入力されます。
7. (オプション) 関連 AWS リソース - オプションで、 AWS リソースの追加を選択します。ダイアログボックスで、関連付けるリソースを選択し、[Add] (追加) を選択します。 AWS WAF は [Describe web ACL and associated AWS resources] (ウェブ ACL と関連付けられた リソースの説明) ページに戻します。
8. [Next] (次へ) を選択します。

ステップ 3: 文字列一致ルールを追加する

このステップでは、文字列一致ステートメントを使用してルールを作成し、一致リクエストの処理方法を指定します。文字列一致ルールステートメントは、 AWS WAF がリクエストで検索する文字列を識別します。通常、文字列は印刷可能な ASCII 文字で構成されますが、16 進数 0x00 ～ 0xFF (10

進数 0 ～ 255) の任意の文字を指定できます。検索する文字列を指定するだけでなく、ヘッダー、クエリ文字列、リクエストボディなど、検索するウェブリクエストコンポーネントを指定します。

このステートメントタイプは、ウェブリクエストコンポーネントで動作し、次のリクエストコンポーネント設定が必要です。

- [リクエストコンポーネント] — ウェブリクエストの検査対象部分 (クエリ文字列や本文など)。

  > **Warning**
  >
  > リクエストコンポーネント本文、JSON 本文、ヘッダー、または Cookie を検査する場合は、 で検査 AWS WAF できるコンテンツの量に関する制限についてお読みくださいでのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF。

  ウェブリクエストコンポーネントの詳細については、「でのルールステートメント設定の調整 AWS WAF」を参照してください。
- オプションのテキスト変換 – 検査する前にリクエストコンポーネントで AWS WAF 実行する変換。例えば、小文字に変換したり、空白を正規化したりできます。複数の変換を指定すると、 はリストされた順序で変換 AWS WAF を処理します。詳細については、「でのテキスト変換の使用 AWS WAF」を参照してください。

AWS WAF ルールの詳細については、「」を参照してくださいAWS WAF ルール。

文字列一致ルールステートメントを作成するには

1. [Add rules and rule groups] (ルールとルールグループの追加) ページで、[Add rules] (ルールの追加)、[Add my own rules and rule groups] (独自のルールとルールグループの追加)、[Rule builder] (ルールビルダー)、[Rule visual editor] (ルールビジュアルエディタ) の順に選択します。

   > **Note**
   >
   > コンソールには、ルールビジュアルエディタとルール JSON エディタが用意されています。JSON エディタを使用すると、ウェブ ACL 間で設定を簡単にコピーできます。これは、ネストのレベルが複数あるルールセットなど、より複雑なルールセットに必要です。
   > この手順では、ルールビジュアルエディタを使用します。

2. [Name] (名前) で、このルールの識別に使用する名前を入力します。
3. [Type] (タイプ) で、[Regular rule] (通常のルール) を選択します。
4. [If a request] (リクエストの状態) で、[matches the statement] (ステートメントに一致) を選択します。

   その他のオプションは、論理ルールステートメントタイプ用です。これらを使用して、他のルールステートメントの結果を組み合わせたり、否定したりできます。
5. ステートメントで、Inspect でドロップダウンを開き、 AWS WAF 検査するウェブリクエストコンポーネントを選択します。この例では、[単一ヘッダー] を選択します。

   [単一ヘッダー] を選択した場合は、 AWS WAF で検査するヘッダーも指定します。**`User-Agent`** と入力します。この値では大文字と小文字は区別されません。
6. [Match type] (一致タイプ) で、指定した文字列が `User-Agent` ヘッダーに表示される場所を選択します。

   この例では、[Exactly matches string] (文字列に完全一致) を選択します。これは、 が各ウェブリクエストの user-agent ヘッダー AWS WAF を検査し、指定した文字列と同じ文字列がないかを示します。
7. [String to match] (照合する文字列) で、 AWS WAF で検索する文字列を指定します。[String to match] (照合する文字列) は最大 200 文字です。base64 でエンコードされた値を指定する場合、エンコード前の長さで最大 200 文字指定できます。

   この例では、MyAgent と入力します。 AWS WAF はウェブリクエストの `User-Agent`ヘッダーに値 がないか検査します`MyAgent`。
8. [Text transformation] (テキスト変換) を [None] (なし) のままにします。
9. [Action] (アクション) で、ウェブリクエストに一致したときにルールによって実行されるアクションを選択します。この例では、[Count] (カウント) を選択し、他の選択肢はそのままにしておきます。カウントアクションにより、ルールに一致するウェブリクエストのメトリクスが作成されますが、リクエストが許可またはブロックされるかどうかには影響しません。アクションの選択の詳細については、「でのルールアクションの使用 AWS WAF」および「ルールの優先度を設定する」を参照してください。
10. [Add rule] (ルールの追加) を選択します。

ステップ 4: AWS マネージドルールルールグループを追加する

AWS マネージドルールには、一連のマネージドルールグループが用意されており、その大部分は AWS WAF お客様に無料で提供されます。ルールグループの詳細については、「AWS WAF ルールグループ」を参照してください。 AWS マネージドルールルールグループをこのウェブ ACL に追加します。

AWS マネージドルールルールグループを追加するには

1. [Add rules and rule groups] (ルールとルールグループの追加) ページで、[Add rules] (ルールの追加) を選択し、[Add managed rule groups] (マネージドルールグループの追加) を選択します。
2. [マネージドルールグループを追加] ページで、[AWS マネージドルールグループ] のリストを展開します。(AWS Marketplace 販売者に提供される出品も表示されます。 サービスにサブスクライブし、 AWS マネージドルールルールグループと同じ方法で使用できます。)
3. 追加するルールグループについて、次を実行します。
   a. [Action] (アクション) 列で、[Add to web ACL] (ウェブ ACL に追加) 切り替えボタンをオンにします。
   b. [Edit] (編集) を選択し、ルールグループの [Rules] (ルール) リストで [Override all rule actions] (すべてのルールアクションをオーバーライド) ドロップダウンを開いて [Count] を選択します。これにより、ルールグループ内のすべてのルールのアクションがカウントのみに設定されます。これにより、ルールグループのルールを使用する前に、ルールグループのすべてのルールがウェブリクエストでどのように動作するかを確認できます。
   c. [Save rule] (ルールを保存) を選択します。
4. [Add managed rule groups] (マネージドルールグループを追加) ページで、[Add rules] (ルールを追加) を選択します。これにより、[Add rules and rule groups] (ルールとルールグループを追加) ページに戻ります。

ステップ 5: ウェブ ACL の設定を完了する

ルールとルールグループをウェブ ACL 設定に追加したら、ウェブ ACL 内のルールの優先順位を管理し、メトリクス、タグ付け、ログ記録などの設定を行うことで完了します。

ウェブ ACL の設定を完了するには

1. [Add rules and rule groups] (ルールとルールグループの追加) ページで、[Next] (次へ) を選択します。

2. ルールの優先度の設定 ページで、ウェブ ACL のルールとルールグループの処理順序を確認できます。 AWS WAF はリストの上部から処理します。処理順序は、ルールを上下に移動することで変更できます。これを行うには、リストで 1 つを選択し、[Move up] (上へ移動) または [Move down] (下へ移動) を選択します。ルーティングの優先度の詳細については、「ルールの優先度を設定する」をご覧ください。
3. [次へ] を選択します。
4. [Configure metrics] (メトリクスの設定) ページの [Amazon CloudWatch metrics] (Amazon CloudWatch メトリクス) で、ルールとルールグループ用の計画されたメトリクスと、ウェブリクエストのサンプリングオプションを確認できます。サンプリングされたリクエストの表示方法については、「ウェブリクエストのサンプルの表示」を参照してください。Amazon CloudWatch メトリクスの詳細については、「Amazon CloudWatch によるモニタリング」を参照してください。

   ウェブトラフィックメトリクスの概要には、 AWS WAF コンソールのウェブ ACL のページで、トラフィックの概要タブからアクセスできます。コンソールダッシュボードには、ウェブ ACL の Amazon CloudWatch メトリクスの概要がほぼリアルタイムで表示されます。詳細については、「保護パック (ウェブ ACL) のトラフィック概要ダッシュボード」を参照してください。
5. [Next] (次へ) を選択します。
6. [Review and create web ACL] (ウェブ ACL の確認と作成) ページで、設定を確認し、[Create web ACL] (ウェブ ACL の作成) を選択します。

ウィザードによって [ウェブ ACL] ページに戻ります。このページには、新しいウェブ ACL が一覧表示されます。

ステップ 6: リソースをクリーンアップする

これでチュートリアルは完了です。アカウントに AWS WAF 追加料金が発生しないようにするには、作成した AWS WAF オブジェクトをクリーンアップします。または、実際に使用するウェブリクエストに合わせて設定を変更することもできます AWS WAF。

> **Note**
>
> AWS 通常、 は、このチュートリアルで作成したリソースに対して 1 日あたり 0.25 USD 未満を請求します。終了したら、不要な料金が発生しないようにリソースを削除することをお勧めします。

が AWS WAF 課金するオブジェクトを削除するには

1. [ウェブ ACL] ページで、リストからウェブ ACL を選択し、[編集] を選択します。
2. 関連付けられた AWS リソースタブで、関連付けられたリソースごとに、リソース名の横にあるラジオボタンを選択し、関連付け解除を選択します。これにより、ウェブ ACL と AWS リソースの関連付けが解除されます。
3. 次の各画面で、[ウェブ ACL] に戻るまで [次へ] を選択します。

   [ウェブ ACL] ページで、リストからウェブ ACL を選択し、[削除] を選択します。

ルールおよびルールステートメントは、ルールグループおよびウェブ ACL 定義の外部には存在しません。ウェブ ACL を削除すると、ウェブ ACL で定義した個々のルールがすべて削除されます。ウェブ ACL からルールグループを削除する場合は、そのグループへの参照を削除するだけです。

の AWS WAF 仕組み

を使用して AWS WAF 、保護されたリソースが HTTP(S) ウェブリクエストにどのように応答するかを制御します。これを行うには、ウェブアクセスコントロールリスト (ウェブ ACL) を定義し、保護する 1 つ以上のウェブアプリケーションリソースと関連付けます。関連付けられたリソースは、ウェブ ACL による検査 AWS WAF のために受信リクエストを に転送します。

新しいコンソール は、ウェブ ACL 設定プロセスを簡素化します。セキュリティルールを完全に制御しながらセットアップを効率化する保護パックが導入されました。

保護パックはウェブ ACL の新しい場所であり、コンソールでのウェブ ACL 管理を簡素化しますが、基盤となるウェブ ACL 機能は変更されません。標準コンソールまたは API を使用する場合でも、ウェブ ACL で引き続き直接作業できます。

保護パック (ウェブ ACL) では、リクエスト内で検索するトラフィックパターンを定義し、一致するリクエストに対して実行するアクションを指定するルールを作成します。アクションの選択肢は次のとおりです。

- 処理と応答のために、リクエストを保護されたリソースに送信することを許可する。
- リクエストをブロックする。
- リクエストをカウントする。
- リクエストに対して CAPTCHA またはチャレンジチェックを実行して、人間のユーザーと標準的なブラウザの使用を確認します。

AWS WAF コンポーネント

以下は、 の主要なコンポーネントです AWS WAF。

- ウェブ ACLs – ウェブアクセスコントロールリスト (ウェブ ACL) を使用して、一連の AWS リソースを保護します。ウェブ ACL を作成し、ルールを追加してその保護戦略を定義します。ルールは、ウェブリクエストを検査する基準を定義し、条件に一致するリクエストに対して取る行動を指定します。また、ルールによってまだブロックまたは許可されていないすべてのリクエストをブロックするか、許可するかを示すウェブ ACL に対してデフォルトのアクションをセットします。ウェブ ACL の詳細については、「での保護の設定 AWS WAF」を参照してください。

  ウェブ ACL は AWS WAF リソースです。

- 保護パック (ウェブ ACL) - 新しいコンソールでは、保護パックはウェブ ACL の新しい場所になります。セットアップ時に、アプリケーションとリソースに関する情報を提供します。 はシナリオに合わせた保護パック AWS WAF を推奨し、選択した保護パック (ウェブ ACL) で定義されたルール、ルールグループ、アクションを含むウェブ ACL を作成します。保護パック (ウェブ ACL) の詳細については、「での保護の設定 AWS WAF」を参照してください。

  保護パック (ウェブ ACL) は AWS WAF リソースです。

- ルール - 各ルールには、検査基準を定義するステートメントと、ウェブリクエストがその基準を満たす場合に実行するアクションが含まれます。ウェブリクエストが条件を満たしている場合、それは一致となります。CAPTCHA パズルまたはサイレントクライアントブラウザのチャレンジを使用する一致リクエストをブロック、許可、カウント、ボットコントロールを実行するルールを設定できます。ルールの詳細については、「AWS WAF ルール」を参照してください。

  ルールは AWS WAF リソースではありません。ルールは保護パック (ウェブ ACL) またはルールグループのコンテキストでのみ定義されます。

- ルールグループ – 保護パック (ウェブ ACL) 内または再利用可能なルールグループでルールを直接定義できます。 AWS マネージドルールと AWS Marketplace 販売者は、使用するマネージドルールグループを提供します。また、独自のルールグループを定義することもできます。ルールグループの詳細については、「AWS WAF ルールグループ」を参照してください。

  ルールグループは AWS WAF リソースです。

- ウェブ ACL キャパシティユニット (WCUs) – WCUs AWS WAF を使用して、ルール、ルールグループ、保護パック (ウェブ ACLs)、またはウェブ ACLs。

  WCU は AWS WAF リソースではありません。保護パック (ウェブ ACL)、ルール、またはルールグループのコンテキストでのみ存在します。

AI トラフィック収益化 – AWS WAF コンテンツプロバイダーと API プロバイダーは、保護されたリソースへのアクセスに対して AI ボットとエージェントに課金できます。ウェブ ACL で収益化を設定することで、リクエストごとに料金を定義します。支払いは、オープン支払いプロトコルを使用してエッジで検証および決済され、資金は設定されたウォレットに直接配信されます。詳細については、「AI トラフィック収益化」を参照してください。

で保護できるリソース AWS WAF

AWS WAF 保護パック (ウェブ ACL) を使用して、グローバルまたはリージョンのリソースタイプを保護できます。保護パック (ウェブ ACL) を保護するリソースに関連付けることにより、これを実行できます。保護パック (ウェブ ACL) とそれを使用するすべての AWS WAF リソースは、関連付けられたリソースがあるリージョンに配置する必要があります。Amazon CloudFront ディストリビューションの場合、これは米国東部 (バージニア北部) に設定されます。

Amazon CloudFront ディストリビューション

AWS WAF コンソールまたは APIs を使用して、 AWS WAF 保護パック (ウェブ ACL) を CloudFront ディストリビューションに関連付けることができます。ディストリビューション自体を作成または更新するとき、保護パック (ウェブ ACL) を CloudFront ディストリビューションに関連付けることもできます。で関連付けを設定するには AWS CloudFormation、CloudFront ディストリビューション設定を使用する必要があります。Amazon CloudFront の詳細については、Amazon CloudFront デベロッパーガイド」の「 AWS WAF を使用してコンテンツへのアクセスを制御する」を参照してください。

AWS WAF は CloudFront ディストリビューションでグローバルに利用できますが、米国東部 (バージニア北部) リージョンを使用して、保護パック (ウェブ ACL) と、ルールグループ、IP セット、正規表現パターンセットなど、保護パック (ウェブ ACL) で使用されるリソースを作成する必要があります。一部のインターフェイスでは、[Global (CloudFront)] (グローバル (CloudFront)) のリージョンを選択できます。これを選択することは、米国東部 (バージニア北部) リージョンまたは us-east-1 を選択することと同じです。

地域リソース

AWS WAF が利用可能なすべてのリージョンでリージョンリソースを保護できます。「Amazon Web Services 全般のリファレンス」の「AWS WAF エンドポイントとクォータ」でリストを確認できます。

を使用して AWS WAF 、次のリージョンリソースタイプを保護できます。

- Amazon API Gateway REST API

- Application Load Balancer
- AWS AppSync GraphQL API
- Amazon Cognito ユーザープール
- AWS App Runner サービス
- Amazon Bedrock AgentCore Gateway
- AWS Verified Access インスタンス
- AWS Amplify

保護パック (ウェブ ACL) を AWS リージョン内にある Application Load Balancer にのみ関連付けることができます。例えば、保護パック (ウェブ ACL) を AWS Outposts上にある Application Load Balancer に関連付けることはできません。

Global CloudFront リージョンで Amplify アプリに関連付ける保護パック (ウェブ ACL) を作成する必要があります。にリージョン保護パック (ウェブ ACL) が既にある場合がありますが AWS アカウント、Amplify と互換性がありません。

使用する保護パック (ウェブ ACL) およびその他の AWS WAF リソースは、保護されたリソースと同じリージョンに配置する必要があります。保護されたリージョンリソースのウェブリクエストをモニタリングおよび管理する場合、 は保護されたリソースと同じリージョン内のすべてのデータ AWS WAF を保持します。

複数リソースの関連付けにおける制限

1 つの保護パック (ウェブ ACL) を 1 つ以上の AWS リソースに関連付けることができますが、以下の制限があります。

- 各 AWS リソースを関連付けることができる保護パック (ウェブ ACL) は 1 つだけです。保護パック (ウェブ ACL) と AWS リソースの関係は one-to-manyです。
- 保護パック (ウェブ ACL) を 1 つ以上の CloudFront ディストリビューションに関連付けることができます。CloudFront ディストリビューションに関連付けられている保護パック (ウェブ ACL) を他の AWS リソースタイプに関連付けることはできません。

更新されたコンソールエクスペリエンスを使用する

AWS WAF には、 コンソールを使用するための 2 つのオプションがあります。

新しいコンソール は、標準のコンソールワークフローに必要なウェブ ACL 設定プロセスを簡素化することを目的としています。ガイド付きワークフローを使用して、保護パック (ウェブ ACL) を通じてウェブ ACL の作成および管理プロセスを簡素化できます。保護パック (ウェブ ACL) を使用すると、コンソールでのウェブ ACL の使用と管理が容易になりますが、ウェブ ACL と機能的に違いはありません。新しいコンソールでは、保護設定プロセスの改善に加えて、セキュリティダッシュボードによる保護の可視性が向上し、 AWS WAF コンソール内のセキュリティ体制のモニタリングが容易になります。

標準 AWS WAF コンソールは、ウェブ ACLs を使用してウェブアプリケーションのファイアウォール保護を設定する従来のアプローチを提供します。個々のルールとルールグループをきめ細かく制御でき、既存の AWS WAF ユーザーにとって使い慣れています。このコンソールを使用すると、保護設定を詳細に制御できるため、セキュリティ設定を正確にカスタマイズできます。

> **Tip**
>
> ニーズに最適なコンソールエクスペリエンスを選択します。を初めて使用する場合、 AWS WAF または AWS レコメンデーションに基づいて保護の設定を開始する場合は、新しいコンソールエクスペリエンスから始めることをお勧めします。ただし、標準エクスペリエンスは、コンソールのナビゲーションペインからいつでも開くことができます。

新しいコンソールエクスペリエンスと標準コンソールエクスペリエンス間の機能のパリティ

新しいコンソールエクスペリエンスは、新機能を導入しながら、既存のコンソールとの完全な機能パリティを維持します。

- 既存の AWS WAF 機能はすべて引き続き使用できます。
- 統合ダッシュボードによる可視性の向上
- 設定ワークフローの簡素化
- 新しい保護パック (ウェブ ACL) テンプレート

> **Important**
>
> 新しいコンソールエクスペリエンスでは、既存のコンソールと同じ WAFv2 API を使用します。つまり、新しいコンソールで作成された保護パックは、API レベルで標準の WAFv2 ウェブ ACL として実装されます。

主な違い

コンソールエクスペリエンスの比較

機能	以前の AWS WAF コンソールエクスペリエンス	コンソールエクスペリエンスの更新
設定プロセス	マルチページワークフロー	単一ページインターフェイス
ルールの設定	個々のルールの作成	事前設定された保護パックのオプション
モニタリング	分離ダッシュボード	AI トラフィック分析を含む統一された可視性

新しいダッシュボードを理解する

新しく提供されるダッシュボードでは、次の視覚化を通じて、セキュリティ体制の統一された可視性が提供されます。

トラフィックインサイトの推奨事項 – AWS 脅威インテリジェンスは、過去 2 週間の許可されたトラフィックをモニタリングし、脆弱性を分析し、以下を提供します。

- トラフィックベースのルールの提案
- アプリケーション固有のセキュリティに関する推奨事項
- 保護最適化ガイダンス

概要 - 指定された時間範囲内のすべてのトラフィックのリクエスト数を表示します。次の条件を使用して、トラフィックデータをフィルタリングできます。

- ルール - 保護パック内の個々のルールでフィルタリングします。
- アクション - 許可、ブロック、キャプチャ、チャレンジなど、トラフィックに対して実行された特定のアクションの数を表示します。

- トラフィックタイプ - DDoS 対策やボットなどの特定のトラフィックタイプの数のみを表示します。
- 時間範囲 - 事前定義された時間範囲から選択するか、カスタム範囲を設定します。
- ローカルまたは UTC 時間 - 任意の時間形式を設定できます。

AI トラフィック分析 – AI ボットとエージェントのアクティビティを包括的に可視化します。

- ボット識別 – ボット名、組織、検証ステータス。
- 目的分析 – AI エージェントの目的と動作パターン。
- アクセスパターン – 最も頻繁にアクセスURLs とエンドポイント。
- 一時的な傾向 – 時刻別および過去の傾向 (0 ~ 14 日) 別のアクティビティパターン。
- トラフィック特性 – AI トラフィックのボリューム、分散、異常検出。

保護アクティビティ - 保護ルールとその順序がアクションの終了にどのように影響するかを視覚化します。

- ルールを通過するトラフィックフロー - ルールを通過するトラフィックフローを表示します。シーケンシャルルールビュー から 非シーケンシャルルールビュー に切り替えて、ルールの順序が結果にどのように影響するかを確認します。
- ルールアクションとその結果 - 指定した期間にルールがトラフィックに対して実行した終了アクションを表示します。

アクションの合計 - 指定された時間範囲でリクエストに対して実行されたアクションの合計数を視覚化するグラフ。現在の時間範囲と過去 3 時間の時間枠を比較するには、過去 3 時間のオーバーレイ オプションを使用します。以下でデータをフィルタリングできます。

- アクションを許可する
- アクションの合計
- キャプチャアクション
- チャレンジアクション
- ブロックブロック

すべてのルール - 保護パック内のすべてのルールのメトリクスを視覚化するグラフ。

- 現在の時間範囲と過去 3 時間の時間枠を比較するには、過去 3 時間のオーバーレイ オプションを使用します。

概要ダッシュボード - 以下を含む、セキュリティステータスの包括的でグラフィカルなビューを提供します。

- トラフィック特性 - トラフィックの概要を、オリジン、攻撃タイプ、またはリクエストを送信したクライアントのデバイスタイプ別に表示します。

- ルールの特性 - 10 個の最も一般的なルールと終了アクションによる攻撃の内訳。
- ボット - ボットアクティビティ、検出、カテゴリ、ボット関連のシグナルラベルを視覚化します。
- DDoS 対策 - 検出および軽減されたレイヤー 7 DDoS アクティビティの概要。

での保護の設定 AWS WAF

このページでは、保護パック (ウェブ ACL) とその仕組みについて説明します。

保護パック (ウェブ ACL) を使用すると、保護されたリソースが応答するすべての HTTP(S) ウェブリクエストをきめ細かく制御できます。Amazon CloudFront、Amazon API Gateway、Application Load Balancer、 AWS AppSync Amazon Cognito AWS App Runner、 AWS Amplify、Amazon CloudWatch、Amazon Bedrock AgentCore Gateway、 AWS Verified Access リソースを保護できます。

次のような基準を使用すると、リクエストを許可またはブロックできます。

- リクエストの IP アドレスの送信元
- リクエストの送信元の国
- リクエストの一部に含まれる文字列一致または正規表現 (regex) 一致
- リクエストの特定の部分のサイズ
- 悪意のある SQL コードまたはスクリプトの検出

これらの条件の任意の組み合わせをテストすることもできます。指定された条件を満たすだけでなく、1 分間にわたって指定された数のリクエストを超えるウェブリクエストを、ブロックまたはカウントできます。論理演算子を使用して条件を組み合わせることができます。リクエストに対して CAPTCHA パズルやサイレントクライアントセッションのチャレンジを実行することもできます。

一致する条件と、 AWS WAF ルールステートメントの一致に対して実行するアクションを指定します。ルールステートメントは、保護パック (ウェブ ACL) 内、および保護パック (ウェブ ACL) で使用する再利用可能なルールグループで直接定義できます。オプションの詳細なリストについては、「でのルールステートメントの使用 AWS WAF」および「でのルールアクションの使用 AWS WAF」を参照してください。

保護パック (ウェブ ACL) を作成するときに、その ACL を使用するリソースのタイプを指定します。詳細については、「で保護パック (ウェブ ACL) を作成する AWS WAF」を参照してください。保護パック (ウェブ ACL) を定義した後、その ACL をリソースに関連付けて、リソースの保護を開始でき

ます。詳細については、「AWS リソースとの保護の関連付けまたは関連付け解除」を参照してください。

> **Note**
>
> 場合によっては、リクエストを許可またはブロックするかどうかに関する関連 AWS リソースへの応答を遅らせる内部エラーが発生する AWS WAF ことがあります。そのような場合は、CloudFront がリクエストを許可するか、コンテンツを提供するのが一般的ですが、 およびリージョンレベルのサービスはリクエストを拒否し、コンテンツを提供しないのが一般的です。

> **本番稼働トラフィックのリスク**
>
> 本番稼働トラフィックの保護パック (ウェブ ACL) に変更をデプロイする前に、ステージング環境またはテスト環境でテストおよびチューニングしてトラフィックへの潜在的な影響を確認します。その後、更新したルールを有効にする前に、本番稼働用トラフィックでカウントモードでルールをテストしてチューニングします。ガイダンスについては、「AWS WAF 保護のテストとチューニング」を参照してください。

> **Note**
>
> 保護パック (ウェブ ACL) で 1,500 WCU を超える容量を使用すると、保護パック (ウェブ ACL) の基本料金を超えるコストが発生します。詳細については、「のウェブ ACL キャパシティユニット (WCUs) AWS WAF」と「AWS WAF 料金表」を参照してください。

更新中の一時的な不一致

保護パック (ウェブ ACL) または他の AWS WAF リソースを作成または変更すると、リソースが保存されているすべての領域にその変更が反映されるまでに少し時間がかかります。伝播時間は、数秒から数分までかかります。

次の内容では、変更伝播中に直面する一時的な不整合性の例を紹介します。

- 保護パック (ウェブ ACL) を作成した後、それをリソースに関連付けようとすると、保護パック (ウェブ ACL) が利用できないことを示す例外が表示される場合があります。

- ルールグループを保護パック (ウェブ ACL) に追加した後、新しいルールグループのルールは、保護パック (ウェブ ACL) が使用されるエリアで有効になり、別のエリアでは有効にならない場合があります。
- ルールのアクション設定を変更した後、古いアクションを一部のエリアで確認され、新しいアクションを別のエリアで確認される場合があります。
- ブロックルールで使用されている IP セットに IP アドレスを追加した後、新しいアドレスはあるエリアではブロックされ、別のエリアでは許可される場合があります。

トピック

- で保護パック (ウェブ ACL) を作成する AWS WAF
- での保護パック (ウェブ ACL) の編集 AWS WAF
- ルールグループの動作を管理する
- AWS リソースとの保護の関連付けまたは関連付け解除
- のルールとルールグループで保護パック (ウェブ ACLs) を使用する AWS WAF
- で保護パック (ウェブ ACL) のデフォルトアクションを設定する AWS WAF
- でのボディ検査の管理に関する考慮事項 AWS WAF
- での CAPTCHA、チャレンジ、トークンの設定 AWS WAF
- でのウェブトラフィックメトリクスの表示 AWS WAF
- 保護パック (ウェブ ACL) の削除

で保護パック (ウェブ ACL) を作成する AWS WAF

Using the new console

このセクションでは、新しい AWS コンソールを使用して保護パック (ウェブ ACLs) を作成する手順について説明します。

新しい保護パック (ウェブ ACL) を作成するには、このページの手順に従って保護パック (ウェブ ACL) 作成ウィザードを使用します。

> ⚠ 本番稼働トラフィックのリスク
>
> 本番稼働トラフィックの保護パック (ウェブ ACL) に変更をデプロイする前に、ステージング環境またはテスト環境でテストおよびチューニングしてトラフィックへの潜在的な影響を確認します。その後、更新したルールを有効にする前に、本番稼働用トラフィッ

クでカウントモードでルールをテストしてチューニングします。ガイダンスについては、「AWS WAF 保護のテストとチューニング」を参照してください。

> **Note**
>
> 保護パック (ウェブ ACL) で 1,500 WCU を超える容量を使用すると、保護パック (ウェブ ACL) の基本料金を超えるコストが発生します。詳細については、「のウェブ ACL キャパシティユニット (WCUs) AWS WAF」と「AWS WAF 料金表」を参照してください。

1. 新しい にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2-pro で AWS WAF コンソールを開きます。
2. ナビゲーションペインで、[リソースと保護パック (ウェブ ACL)] を選択します。
3. リソースと保護パック (ウェブ ACL) ページで、保護パック (ウェブ ACL) の追加 を選択します。
4. 「アプリについて教えてください」の「アプリカテゴリ」で、1 つ以上のアプリカテゴリを選択します。
5. トラフィックソース　では、アプリケーションがエンゲージするトラフィックのタイプを選択します。API、ウェブ、または API とウェブの両方 です。
6. 保護するリソース で、リソースの追加 を選択します。
7. この保護パック (ウェブ ACL) に関連付ける AWS リソースのカテゴリ (Amazon CloudFront ディストリビューションまたはリージョンリソース) を選択します。詳細については、「AWS リソースとの保護の関連付けまたは関連付け解除」を参照してください。
8. 「初期保護の選択」で、推奨、必須、または ビルドする のいずれかの保護レベルを選択します。
9. (オプション) ビルドする を選択する場合は、ルールを構築します。

    a. (オプション) 独自のルールを追加する場合は、[ルールの追加] ページで [カスタムルール] を選択し、[次へ] を選択します。

        i. ロールタイプを選択します。

        ii. [Action] (アクション) で、ウェブリクエストに一致したときにルールによって実行されるアクションを選択します。選択の詳細については、「でのルールアクションの使用 AWS WAF」と「のルールとルールグループで保護パック (ウェブ ACLs) を使用する AWS WAF」を参照してください。

[CAPTCHA] または [Challenge] アクションを使用している場合、このルールの必要に応じて [Immunity time] (イミュニティ時間) の設定を調整します。設定を指定しない場合、ルールは保護パック (ウェブ ACL) から設定を継承します。保護パック (ウェブ ACL) のイミュニティ時間設定を変更するには、保護パック (ウェブ ACL) の作成後にウェブ ACL を編集します。イミュニティ時間の詳細については、「でのタイムスタンプの有効期限とトークンイミュニティ時間の設定 AWS WAF」を参照してください。

> **Note**
>
> CAPTCHA または Challenge ルールアクションを 1 つのルールで使用、あるいはルールグループでルールアクションのオーバーライドとして使用すると、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

リクエストまたはレスポンスをカスタマイズする場合は、そのオプションを選択し、カスタマイズの詳細を入力します。詳細については、「でカスタマイズされたウェブリクエストとレスポンス AWS WAF」を参照してください。

一致するウェブリクエストにルールがラベルを追加するようにする場合は、そのオプションを選択し、ラベルの詳細を入力します。詳細については、「でのウェブリクエストのラベル付け AWS WAF」を参照してください。

iii. [Name] (名前) で、このルールの識別に使用する名前を入力します。`AWS`、`Shield`、`PreFM`、または `PostFM` で始まる名前は使用しないでください。これらの文字列は、予約されているか、他のサービスが管理するルールグループと混同される可能性があります。

iv. 必要に応じて、ルールの定義を入力します。論理 `AND` および `OR` ルールステートメントの中でルールを組み合わせることができます。ウィザードに、コンテキストに応じた各ルールのオプションが表示されます。ルールのオプションについては、「AWS WAF ルール」を参照してください。

v. [ルールを作成] を選択します。

> **Note**
>
> 保護パック (ウェブ ACL) に複数のルールを追加すると、 は保護パック (ウェブ ACL) にリストされている順序でルール AWS WAF を評価します。詳細については、「のルールとルールグループで保護パック (ウェブ ACLs) を使用する AWS WAF」を参照してください。

b. (オプション) マネージドルールグループを追加する場合は、[ルールの追加] ページで、[AWSマネージドルールグループ] または [AWS マーケットプレイスルールグループ] を選択し、[次へ] を選択します。追加するマネージドルールグループごとに次を実行します。

   i. ルールの追加ページで、マネージドルールグループまたは AWS Marketplace 販売者のリスト AWS を展開します。

   ii. ルールグループのバージョンを選択します。

   iii. 保護パック (ウェブ ACL) がルールグループを使用する方法をカスタマイズするには、[編集] を選択します。一般的なカスタマイズ設定は次のとおりです。

   - [検査] セクションにスコープダウンステートメントを追加することで、ルールグループが検査するウェブリクエストのスコープを縮小します。このオプションについては、「でのスコープダウンステートメントの使用 AWS WAF」を参照してください。
   - ルールオーバーライド の一部またはすべてのルールのルールアクションをオーバーライドします。ルールにオーバーライドアクションを定義しない場合、評価にはルールグループ内で定義されているルールアクションが使用されます。このオプションについては、「でのルールグループアクションの上書き AWS WAF」を参照してください。
   - 一部のマネージドルールグループは追加の設定が必要です。マネージドルールグループのプロバイダーのドキュメントを参照してください。 AWS マネージドルールのルールグループに固有の情報については、「」を参照してくださいAWS の マネージドルール AWS WAF。

   iv. [次へ] を選択します。

c. (オプション) 独自のルールグループを追加する場合は、[ルールの追加] ページで [カスタムルールグループ] を選択し、[次へ] を選択します。追加するルールグループごとに次を実行します。

i. [名前] で、この保護パック (ウェブ ACL) のルールグループのルールに使用する名前を入力します。AWS、Shield、PreFM、または PostFM で始まる名前は使用しないでください。これらの文字列は、予約されているか、他のサービスが管理するルールグループと混同される可能性があります。「他のサービスによって提供されるルールグループを識別する」を参照してください。

ii. リストからルールグループを選択します。

iii. (オプション) [ルール設定]で、[ルールオーバーライド] を選択します。マネージドルールグループの場合と同様に、ルールアクションを任意の有効なアクション設定に上書きできます。

iv. (オプション) [ラベルの追加] で [ラベルの追加] を選択し、ルールに一致するリクエストに追加するラベルを入力します。同じ保護パック (ウェブ ACL) で後で評価されるルールは、このルールが追加するラベルを参照できます。

v. [ルールを作成] を選択します。

10. 名前と説明 に、保護パック (ウェブ ACL) の名前を入力します。必要に応じて説明を入力します。

> **Note**
>
> 保護パック (ウェブ ACL) の作成後は、名前を変更することはできません。

11. (オプション) 保護パックのカスタマイズ (ウェブ ACL) で、デフォルトのルールアクション、設定、ログ記録の送信先を設定します。

a. (オプション) デフォルトのルールアクション で、保護パック (ウェブ ACL) のデフォルトのアクションを選択します。これは、保護パック (ウェブ ACL) のルールが明示的にアクションを実行しない場合に、リクエスト AWS WAF に対して が実行するアクションです。詳細については、「でカスタマイズされたウェブリクエストとレスポンス AWS WAF」を参照してください。

b. (オプション) ルール設定で、保護パック (ウェブ ACL) のルールの設定をカスタマイズします。

- デフォルトのレート制限 - 可用性に影響を与えたり、セキュリティを侵害したり、過剰なリソースを消費したりする可能性のあるサービス拒否 (DoS) 攻撃をブロックするようにレート制限を設定します。このルールレートは、アプリケーションの許容レートを超える IP アドレスあたりのリクエストをブロックします。詳細については、でのレートベースのルールステートメントの使用 AWS WAFを参照してください。

- IP アドレス - ブロックまたは許可する IP アドレスを入力します。この設定は、他のルールをオーバーライドします。
- 国固有のオリジン - 指定された国からのリクエストをブロックするか、すべてのトラフィックをカウントします。

c. ログ記録先 の場合は、ログ記録先タイプとログを保存する場所を設定します。詳細については、「AWS WAF ログ記録の送信先」を参照してください。

12. (オプション) AI ボットトラフィックを収益化する場合は、収益化設定を拡張し、支払いネットワーク、ウォレットアドレス、基本価格を設定します。このステップをスキップして、後で MonetizationConfig を追加できます。
13. 設定を確認し、保護パック (ウェブ ACL) の追加 を選択します。

Using the standard console

このセクションでは、 AWS コンソールを使用してウェブ ACLs を作成する手順について説明します。

新しいウェブ ACL を作成するには、このページの手順に従ってウェブ ACL 作成ウィザードを使用します。

> **本番稼働トラフィックのリスク**
>
> 本番稼働トラフィックのウェブ ACL に変更をデプロイする前に、ステージング環境またはテスト環境でテストおよびチューニングしてトラフィックへの潜在的な影響を確認します。その後、更新したルールを有効にする前に、本番稼働用トラフィックでカウントモードでルールをテストしてチューニングします。ガイダンスについては、「AWS WAF 保護のテストとチューニング」を参照してください。

> **Note**
>
> 保護パック (ウェブ ACL) で 1,500 WCU を超える容量を使用すると、保護パック (ウェブ ACL) の基本料金を超えるコストが発生します。詳細については、「のウェブ ACL キャパシティユニット (WCUs) AWS WAF」と「AWS WAF 料金表」を参照してください。

ウェブ ACL を作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインの [Web ACLs] (ウェブ ACL) を選択してから、[Create web ACL] (ウェブ ACL を作成) を選択します。
3. [Name] (名前) で、このウェブ ACL の識別に使用する名前を入力します。

   > **Note**
   >
   > ウェブ ACL の作成後は、名前を変更することはできません。

4. (オプション) 必要に応じて、[Description - optional] (説明 - オプション) に、ウェブ ACL の詳しい説明を入力します。
5. [CloudWatch metric name] (CloudWatch メトリクス名) で、必要に応じてデフォルト名を変更します。有効な文字については、コンソールのガイダンスに従ってください。名前には、「All」や「Default_Action」など AWS WAF、予約されている特殊文字、空白、またはメトリクス名を含めることはできません。

   > **Note**
   >
   > ウェブ ACL の作成後は CloudWatch メトリクス名を変更できません。

6. [リソースタイプ] で、このウェブ ACL に関連付ける AWS リソースのカテゴリ (Amazon CloudFront ディストリビューションまたはリージョンリソース) を選択します。詳細については、「AWS リソースとの保護の関連付けまたは関連付け解除」を参照してください。
7. リージョンで、リージョンリソースタイプを選択した場合は、ウェブ ACL AWS WAF を保存するリージョンを選択します。

   このオプションは、リージョン別リソースタイプの場合にのみ選択する必要があります。CloudFront ディストリビューションの場合、グローバル (CloudFront) アプリケーションであれば、リージョンは `us-east-1` (米国東部 (バージニア北部) リージョン) にハードコードされています。
8. (CloudFront、API Gateway、Amazon Cognito、App Runner、Verified Access、Amazon Bedrock AgentCore Gateway) ウェブリクエストの検査サイズ制限 - オプションで、別の本文の検査サイズ制限を指定する場合は、制限を選択します。デフォルトの 16 KB を超えるボ

ディサイズを検査すると、追加費用が発生する可能性があります。このオプションについては、「でのボディ検査の管理に関する考慮事項 AWS WAF」を参照してください。

9. (オプション) 関連 AWS リソース - オプションで、今すぐリソースを指定する場合は、リソースの追加 AWS を選択します。ダイアログボックスで、関連付けるリソースを選択し、Add. AWS WAF returns you to the Describe web ACL and associated AWS resources page を選択します。

> **Note**
>
> Application Load Balancer をウェブ ACL に関連付けることを選択すると、リソースレベルの DDoS 保護 が有効になります。詳細については、「AWS WAF 分散サービス拒否 (DDoS) の防止」を参照してください。

10. (オプション) AI ボットトラフィックを収益化する場合は、収益化設定を拡張し、支払いネットワーク、ウォレットアドレス、基本価格を設定します。このステップをスキップして、後で MonetizationConfig を追加できます。
11. [次へ] を選択します。
12. (オプション) マネージドルールグループを追加する場合は、[Add rules and rule groups] (ルールとルールグループの追加) ページで、[Add rules] (ルールの追加) を選択し、[Add managed rule groups] (マネージドルールグループの追加) を選択します。追加するマネージドルールグループごとに次を実行します。

    a. マネージドルールグループの追加ページで、マネージドルールグループまたは任意の AWS Marketplace 販売者のリスト AWS を展開します。

    b. 追加するルールグループでは、[Action] (アクション) 列で [Add to web ACL] (ウェブ ACL に追加) 切り替えボタンをオンにします。

    ウェブ ACL がルールグループを使用する方法をカスタマイズするには、[Edit] (編集) を選択します。一般的なカスタマイズ設定は次のとおりです。

    - 一部またはすべてのルールのルールアクションをオーバーライドします。ルールにオーバーライドアクションを定義しない場合、評価にはルールグループ内で定義されているルールアクションが使用されます。このオプションについては、「でのルールグループアクションの上書き AWS WAF」を参照してください。
    - スコープダウンステートメントを追加することで、ルールグループが検査するウェブリクエストのスコープを縮小します。このオプションについては、「でのスコープダウンステートメントの使用 AWS WAF」を参照してください。

- 一部のマネージドルールグループは追加の設定が必要です。マネージドルールグループのプロバイダーのドキュメントを参照してください。 AWS マネージドルールのルールグループに固有の情報については、「」を参照してくださいAWS の マネージドルール AWS WAF。

設定が完了したら、[Save rule] (ルールを保存) を選択します。

[Add rules] (ルールの追加) を選択してマネージドルールの追加を終了し、[Add rules and rule groups] (ルールとルールグループの追加) ページに戻ります。

> **Note**
>
> ウェブ ACL に複数のルールを追加すると、 はウェブ ACL にリストされている順序でルール AWS WAF を評価します。詳細については、「のルールとルールグループで保護パック (ウェブ ACLs) を使用する AWS WAF」を参照してください。

13. (オプション) 独自のルールグループを追加する場合は、[Add rules and rule groups] (ルールとルールグループの追加) ページで、[Add rules] (ルールの追加) を選択し、[Add my own rules and rule groups] (独自のルールとルールグループの追加) を選択します。追加するルールグループごとに次を実行します。

    a. [Add my own rules and rule groups] (独自のルールとルールグループの追加) ページで、[Rule group] (ルールグループ) を選択します。

    b. [Name] (名前) で、このウェブ ACL のルールグループのルールに使用する名前を入力します。`AWS`、`Shield`、`PreFM`、または `PostFM` で始まる名前は使用しないでください。これらの文字列は、予約されているか、他のサービスが管理するルールグループと混同される可能性があります。「他のサービスによって提供されるルールグループを識別する」を参照してください。

    c. リストからルールグループを選択します。

    > **Note**
    >
    > 独自のルールグループのルールアクションを上書きする場合は、まずウェブ ACL に保存し、ウェブ ACL のルールリストでウェブ ACL とルールグループ参照ステートメントを編集します。マネージドルールグループの場合と同様に、ルールアクションを任意の有効なアクション設定に上書きできます。

d. [ルールを追加] を選択してください。

14. (オプション) 独自のルールを追加する場合は、[Add rules and rule groups] (ルールとルールグループの追加) ページで、[Add rules] (ルールの追加)、[Add my own rules and rule groups] (独自のルールとルールグループの追加)、[Rule builder] (ルールビルダー)、[Rule visual editor] (ルールビジュアルエディタ) の順に選択します。

> **Note**
>
> コンソールの [Rule visual editor] (ルールビジュアルエディタ) は、1 レベルのネストをサポートします。例えば、単一の論理 AND または OR ステートメントを使用して、その中に 1 レベルの他のステートメントをネストすることはできますが、論理ステートメントの中に論理ステートメントをネストすることはできません。より複雑なルールステートメントを管理するには、[Rule JSON editor] (ルール JSON エディタ) を使用します。ルールのすべてのオプションについては、「AWS WAF ルール」を参照してください
> この手順では、[Rule visual editor] (ルールビジュアルエディタ) について説明します。

a. [Name] (名前) で、このルールの識別に使用する名前を入力します。AWS、Shield、PreFM、または PostFM で始まる名前は使用しないでください。これらの文字列は、予約されているか、他のサービスが管理するルールグループと混同される可能性があります。

b. 必要に応じて、ルールの定義を入力します。論理 AND および OR ルールステートメントの中でルールを組み合わせることができます。ウィザードに、コンテキストに応じた各ルールのオプションが表示されます。ルールのオプションについては、「AWS WAF ルール」を参照してください。

c. [Action] (アクション) で、ウェブリクエストに一致したときにルールによって実行されるアクションを選択します。選択の詳細については、「でのルールアクションの使用 AWS WAF」と「のルールとルールグループで保護パック (ウェブ ACLs) を使用する AWS WAF」を参照してください。

   [CAPTCHA] または [Challenge] アクションを使用している場合、このルールの必要に応じて [Immunity time] (イミュニティ時間) の設定を調整します。設定を指定しない場合、ルールはウェブ ACL から設定を継承します。ウェブ ACL のイミュニティ時間設定を変更するには、ウェブ ACL の作成後にウェブ ACL を編集します。イミュニティ時間

の詳細については、「でのタイムスタンプの有効期限とトークンイミュニティ時間の設定 AWS WAF」を参照してください。

> **Note**
>
> CAPTCHA または Challenge ルールアクションを 1 つのルールで使用、あるいはルールグループでルールアクションのオーバーライドとして使用すると、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

リクエストまたはレスポンスをカスタマイズする場合は、そのオプションを選択し、カスタマイズの詳細を入力します。詳細については、「でカスタマイズされたウェブリクエストとレスポンス AWS WAF」を参照してください。

一致するウェブリクエストにルールがラベルを追加するようにする場合は、そのオプションを選択し、ラベルの詳細を入力します。詳細については、「でのウェブリクエストのラベル付け AWS WAF」を参照してください。

d. [Add Rule] (ルールの追加) を選択します。

15. ウェブ ACL のデフォルトアクションに Block または Allow を選択します。これは、ウェブ ACL のルールがリクエストを明示的に許可またはブロックしない場合に、リクエストに対して が AWS WAF 実行するアクションです。詳細については、「で保護パック (ウェブ ACL) のデフォルトアクションを設定する AWS WAF」を参照してください。

    デフォルトのアクションをカスタマイズする場合は、そのオプションを選択し、カスタマイズの詳細を入力します。詳細については、「でカスタマイズされたウェブリクエストとレスポンス AWS WAF」を参照してください。

16. [Token domain list] (トークンドメインリスト) を定義して、保護されたアプリケーション間でトークンの共有を有効にできます。トークンは、 AWS WAF 不正コントロールアカウント作成不正防止 (ACFP)、 AWS WAF 不正コントロールアカウント乗っ取り防止 (ATP)、 AWS WAF ボットコントロールに AWS Managed Rules ルールグループを使用するときに実装する CAPTCHAChallengeアクションとアプリケーション統合 SDKs によって使用されます。

    パブリックサフィックスは許可されません。たとえば、`gov.au` または `co.uk` をトークンドメインとして使用することはできません。

    デフォルトでは、 は保護されたリソースのドメインに対してのみトークン AWS WAF を受け入れます。このリストにトークンドメインを追加すると、 はリスト内のすべてのドメイン

と、関連付けられたリソースのドメインのトークン AWS WAF を受け入れます。詳細については、「AWS WAF 保護パック (ウェブ ACL) トークンドメインリスト設定」を参照してください。

17. [Next] (次へ) を選択します。
18. ルールの優先度の設定ページで、ルールとルールグループを選択して、 AWS WAF 処理する順序に移動します。 は、リストの上部からルール AWS WAF を処理します。ウェブ ACL を保存すると、 AWS WAF では、リストされている順に、優先順位の数値設定がルールに割り当てられます。詳細については、「ルールの優先度を設定する」を参照してください。
19. [Next] (次へ) を選択します。
20. [Configure metrics] (メトリクスを設定) ページで、オプションを確認し、必要な更新を適用します。複数のソースからのメトリクスを組み合わせるには、それらに同じ [CloudWatch metric name] (CloudWatch メトリクス名) を指定します。
21. [Next] (次へ) を選択します。
22. [Review and create web ACL] (ウェブ ACL の確認と作成) ページで定義を確認します。エリアを変更する場合は、エリアの [Edit] (編集) を選択します。これにより、ウェブ ACL ウィザードのページに戻ります。変更を加えてから、[Review and create web ACL] (確認してウェブ ACL を作成する) ページに戻るまで、[Next] (次へ) を選択してページを進みます。
23. [Create web ACL] (ウェブ ACL の作成) を選択します。新しいウェブ ACL は、[Web ACLs] (ウェブ ACL) ページにリストされます。

での保護パック (ウェブ ACL) の編集 AWS WAF

Using the new console

このセクションでは、 AWS コンソールを使用して保護パック (ウェブ ACLs) を編集する手順について説明します。

保護パック (ウェブ ACL) のルールを追加、削除、あるいは設定を変更するには、このページの手順を使用して保護パック (ウェブ ACL) にアクセスします。保護パック (ウェブ ACL) の更新中に、 は保護パック (ウェブ ACL) に関連付けられたリソースに継続的なカバレッジ AWS WAF を提供します。

> ⚠ 本番稼働トラフィックのリスク
>
> 本番稼働トラフィックの保護パック (ウェブ ACL) に変更をデプロイする前に、ステージング環境またはテスト環境でテストおよびチューニングしてトラフィックへの潜在的な

影響を確認します。その後、更新したルールを有効にする前に、本番稼働用トラフィックでカウントモードでルールをテストしてチューニングします。ガイダンスについては、「AWS WAF 保護のテストとチューニング」を参照してください。

> **Note**
>
> 保護パック (ウェブ ACL) で 1,500 WCU を超える容量を使用すると、保護パック (ウェブ ACL) の基本料金を超えるコストが発生します。詳細については、「のウェブ ACL キャパシティユニット (WCUs) AWS WAF」と「AWS WAF 料金表」を参照してください。

保護パック (ウェブ ACL) を編集するには

1. 新しい にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2-pro で AWS WAF コンソールを開きます。
2. ナビゲーションペインで、[リソースと保護パック (ウェブ ACL)] を選択します。
3. 編集する保護パック (ウェブ ACL) を選択します。コンソールはメイン保護パック (ウェブ ACL) カードを編集可能にし、編集できる詳細を含むサイドペインも開きます。
4. 必要に応じて保護パック (ウェブ ACL) を編集します。

   以下は、編集可能な保護パック (ウェブ ACL) 設定コンポーネントの一覧です。

   このセクションでは、 AWS コンソールを使用してウェブ ACLs を編集する手順について説明します。

   ウェブ ACL のルールを追加、削除、あるいは設定を変更するには、このページの手順を使用してウェブ ACL にアクセスします。ウェブ ACL の更新中に、 はウェブ ACL に関連付けられたリソースに継続的なカバレッジ AWS WAF を提供します。

> **本番稼働トラフィックのリスク**
>
> 本番稼働トラフィックのウェブ ACL に変更をデプロイする前に、ステージング環境またはテスト環境でテストおよびチューニングしてトラフィックへの潜在的な影響を確認します。その後、更新したルールを有効にする前に、本番稼働用トラフィックでカウントモー

ドでルールをテストしてチューニングします。ガイダンスについては、「AWS WAF 保護のテストとチューニング」を参照してください。

> **Note**
>
> 保護パック (ウェブ ACL) で 1,500 WCU を超える容量を使用すると、保護パック (ウェブ ACL) の基本料金を超えるコストが発生します。詳細については、「のウェブ ACL キャパシティユニット (WCUs) AWS WAF」と「AWS WAF 料金表」を参照してください。

更新中の一時的な不一致

保護パック (ウェブ ACL) または他の AWS WAF リソースを作成または変更すると、リソースが保存されているすべての領域にその変更が反映されるまでに少し時間がかかります。伝播時間は、数秒から数分までかかります。

次の内容では、変更伝播中に直面する一時的な不整合性の例を紹介します。

- 保護パック (ウェブ ACL) を作成した後、それをリソースに関連付けようとすると、保護パック (ウェブ ACL) が利用できないことを示す例外が表示される場合があります。
- ルールグループを保護パック (ウェブ ACL) に追加した後、新しいルールグループのルールは、保護パック (ウェブ ACL) が使用されるエリアで有効になり、別のエリアでは有効にならない場合があります。
- ルールのアクション設定を変更した後、古いアクションを一部のエリアで確認され、新しいアクションを別のエリアで確認される場合があります。
- ブロックルールで使用されている IP セットに IP アドレスを追加した後、新しいアドレスはあるエリアではブロックされ、別のエリアでは許可される場合があります。

Using the standard console

このセクションでは、 AWS コンソールを使用してウェブ ACL を編集する手順について説明します。

ウェブ ACL のルールを追加、削除、あるいは設定を変更するには、このページの手順を使用してウェブ ACL にアクセスします。ウェブ ACL の更新中に、 はウェブ ACL に関連付けられたリソースに継続的なカバレッジ AWS WAF を提供します。

> **本番稼働トラフィックのリスク**
>
> 本番稼働トラフィックのウェブ ACL に変更をデプロイする前に、ステージング環境またはテスト環境でテストおよびチューニングしてトラフィックへの潜在的な影響を確認します。その後、更新したルールを有効にする前に、本番稼働用トラフィックでカウントモードでルールをテストしてチューニングします。ガイダンスについては、「AWS WAF 保護のテストとチューニング」を参照してください。

> **Note**
>
> 保護パック (ウェブ ACL) で 1,500 WCU を超える容量を使用すると、保護パック (ウェブ ACL) の基本料金を超えるコストが発生します。詳細については、「のウェブ ACL キャパシティユニット (WCUs) AWS WAF」と「AWS WAF 料金表」を参照してください。

ウェブ ACL を編集するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで [ウェブ ACL] を選択します。
3. 編集するウェブ ACL の名前を選択します。コンソールでウェブ ACL の説明が表示されます。
4. 必要に応じてウェブ ACL を編集します。関心のある設定領域のタブを選択し、ミュータブルな設定を編集します。編集する設定ごとに [保存] を選択してウェブ ACL の説明ページに戻ると、コンソールではウェブ ACL に変更が保存されます。

   ウェブ ACL 設定コンポーネントを含むタブを以下に示します。

   - [ルール] タブ
     - ウェブ ACL で定義したルール – ウェブ ACL で定義したルールは、ウェブ ACL の作成時と同様に編集および管理できます。

       > **Note**
       >
       > ウェブ ACL に手動で追加していないルールの名前は変更しないでください。他の サービスを使用してルールを管理している場合、名前を変更すると、意図し

た保護を提供する機能が削除または低下する可能性があります。 AWS Shield Advanced と AWS Firewall Manager の両方がウェブ ACL にルールを作成できます。詳細については、「他のサービスによって提供されるルールグループを識別する」を参照してください。

> **Note**
>
> ルールの名前を変更し、ルールのメトリクス名に変更を反映する場合は、メトリクス名も更新する必要があります。ルール名を変更しても、ルールのメトリクス名は自動的に更新 AWS WAF されません。ルールの JSON エディターを使用して、コンソールでルールを編集するときに、メトリック名を変更できます。API や、保護パック (ウェブ ACL) またはルールグループの定義に使用する JSON リストを使用して、両方の名前を変更することもできます。

ルールおよびルールグループの設定については、「AWS WAF ルール」と「AWS WAF ルールグループ」を参照してください。

- [使用するウェブ ACL ルールキャパシティーユニット] – ウェブ ACL の現在のキャパシティ使用量。これは表示のみです。
- [どのルールにも一致しないリクエストに対するデフォルトのウェブ ACL アクション] – この設定の詳細については、「で保護パック (ウェブ ACL) のデフォルトアクションを設定する AWS WAF」を参照してください。
- [ウェブ ACL CAPTCHA およびチャレンジ設定] – これらのイミュニティ時間によって、CAPTCHA またはチャレンジトークンの取得後の有効期間が決まります。ウェブ ACL の作成後、この設定は、このタブでしか変更できません。これらの設定については、「でのタイムスタンプの有効期限とトークンイミュニティ時間の設定 AWS WAF」を参照してください。
- トークンドメインリスト – リスト内のすべてのドメインと、関連付けられたリソースのドメインのトークン AWS WAF を受け入れます。詳細については、「AWS WAF 保護パック (ウェブ ACL) トークンドメインリスト設定」を参照してください。

- 関連付けられた AWS リソースタブ
  - [ウェブリクエスト検査サイズの制限] – CloudFront ディストリビューションを保護するウェブ ACL にのみ含まれます。ボディ検査サイズ制限は、検査 AWS WAF のために に

転送されるボディコンポーネントの量を決定します。この設定の詳細については「でのボディ検査の管理に関する考慮事項 AWS WAF」を参照してください。

- [関連付けられた AWS リソース] – ウェブ ACL が現在関連付けられ、保護しているリソースのリスト。ウェブ ACL と同じリージョン内にあるリソースを見つけて、ウェブ ACL に関連付けることができます。詳細については、「AWS リソースとの保護の関連付けまたは関連付け解除」を参照してください。

- [カスタムレスポンス本文] タブ
  - アクションが Block に設定されているウェブ ACL ルールで使用できるカスタムレスポンス本文。詳細については、「Block アクションのカスタムレスポンスの送信」を参照してください。
- [ログ記録とメトリクス] タブ
  - ログ記録 – ウェブ ACL で評価されるトラフィックのログ記録。詳細については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。
  - Security Lake 統合 – Amazon Security Lake のウェブ ACL 用に設定したデータ収集のステータス。詳細については、「Amazon Security Lake ユーザーガイド」の AWS 「サービスからのデータ収集」を参照してください。
  - サンプリングされたリクエスト – ウェブリクエストに一致するルールに関する情報。サンプリングされたリクエストの表示方法については、「ウェブリクエストのサンプルの表示」を参照してください。
  - データ保護設定 – ウェブ ACL で使用可能なすべてのデータと、 が設定されたウェブ ACL ログ記録先 AWS WAF に送信するデータに対してのみ、ウェブトラフィックデータの秘匿化とフィルタリングを設定できます。データ保護については、「保護 AWS WAF パック (ウェブ ACL) トラフィックのデータ保護と口グ記録」を参照してください。
  - CloudWatch メトリクス – ウェブ ACL 内のルールのメトリクス。Amazon CloudWatch メトリクスの詳細については、「Amazon CloudWatch によるモニタリング」を参照してください。

更新中の一時的な不一致

保護パック (ウェブ ACL) または他の AWS WAF リソースを作成または変更すると、リソースが保存されているすべての領域にその変更が反映されるまでに少し時間がかかります。伝播時間は、数秒から数分までかかります。

次の内容では、変更伝播中に直面する一時的な不整合性の例を紹介します。

- 保護パック (ウェブ ACL) を作成した後、それをリソースに関連付けようとすると、保護パック (ウェブ ACL) が利用できないことを示す例外が表示される場合があります。
- ルールグループを保護パック (ウェブ ACL) に追加した後、新しいルールグループのルールは、保護パック (ウェブ ACL) が使用されるエリアで有効になり、別のエリアでは有効にならない場合があります。
- ルールのアクション設定を変更した後、古いアクションを一部のエリアで確認され、新しいアクションを別のエリアで確認される場合があります。
- ブロックルールで使用されている IP セットに IP アドレスを追加した後、新しいアドレスはあるエリアではブロックされ、別のエリアでは許可される場合があります。

ルールグループの動作を管理する

このセクションでは、保護パック (ウェブ ACL) でルールグループを使用する方法を変更するオプションについて説明します。この情報は、すべてのルールグループタイプに適用されます。ルールグループを保護パック (ウェブ ACL) に追加すると、ルールグループ内の個々ルールのアクションを Count またはその他の有効なルールアクション設定にオーバーライドできます。ルールグループの結果として生じるアクションを Count にオーバーライドすることもできます。これは、ルールグループ内でルールがどのように評価されるかについて影響されません。

これらのオプションについては、「でのルールグループアクションの上書き AWS WAF」を参照してください。

ルールグループ内のルールアクションのオーバーライド

保護パック (ウェブ ACL) の各ルールグループにおいて、一部またはすべてのルールに含まれているルールのアクションをオーバーライドできます。

この場合の最も一般的な使用例は、ルールアクションを Count にオーバーライドし、新しいまたは更新されたルールをテストすることです。メトリクスを有効にしている場合、上書きするルールごとにメトリクスが受信されます。テストの詳細については、「AWS WAF 保護のテストとチューニング」を参照してください。

これらの変更は、マネージドルールグループを保護パック (ウェブ ACL) に追加するときに行うことができ、保護パック (ウェブ ACL) を編集するときに任意のタイプのルールグループに行うことができます。この手順は、保護パック (ウェブ ACL) にすでに追加されているルールグループを対象としています。このオプションに関する追加情報については、ルールグループのルールアクションの上書き を参照してください。

Using the new console

ルールグループのルールアクションのオーバーライド方法

1. 編集する保護パック (ウェブ ACL) を選択します。コンソールはメイン保護パック (ウェブ ACL) カードを編集可能にし、編集できる詳細を含むサイドパネルも開きます。
2. 保護パック (ウェブ ACL) カードで、[ルール] の横にある [編集] リンクを選択して、[ルールの管理] パネルを開きます。
3. ルールグループの [ルールの管理] セクションで、[マネージドルール] を選択してアクション設定を開きます。

   - ルールグループをオーバーライド – ルールグループのアクションをカウントモードに変更しますが、個々のすべてのルールアクションは変更されません。
   - すべてのルールアクションをオーバーライド – すべてのルールにルールアクションを適用し、現在の状態をオーバーライドします。
   - 単一ルールをオーバーライド – ルールアクションを個々のルールに適用します。
4. 変更が完了したら、[Save Rule] (ルールを保存) を選択します。

Using the standard console

ルールグループのルールアクションのオーバーライド方法

1. ウェブ ACL を編集します。
2. ウェブ ACL ページの [Rules] (ルール) タブで、ルールグループを選択し、[Edit] (編集) を選択します。
3. ルールグループの [Rules] (ルール) セクションで、必要に応じてアクション設定を管理します。

   - すべてのルール – ルールグループ内のすべてのルールにオーバーライドアクションを設定するには、[Override all rule actions] (すべてのルールアクションをオーバーライド) ドロップダウンを開いてオーバーライドアクションを選択します。すべてのルールのオーバーライドを削除するには、[Remove all overrides] (すべてのオーバーライドを削除) を選択します。
   - 単一ルール – 単一ルールにオーバーライドアクションを設定するには、ルールのドロップダウンを開いてオーバーライドアクションを選択します。ルールのオーバーライドを削除するには、ルールのドロップダウンを開いて [Remove override] (オーバーライドを削除) を選択します。

4. 変更が完了したら、[Save Rule] (ルールを保存) を選択します。ルールアクションおよびオーバーライドアクション設定は、ルールグループページに一覧表示されます。

次の JSON リストの例は、ルール CategoryVerifiedSearchEngine および CategoryVerifiedSocialMedia に対してルールアクションを Count にオーバーライドする保護パック (ウェブ ACL) 内のルールグループ宣言を示しています。JSON では、個々ルールごとに RuleActionOverrides エントリを指定することで、すべてのルールアクションをオーバーライドします。

```
{
    "Name": "AWS-AWSBotControl-Example",
   "Priority": 5,
   "Statement": {
    "ManagedRuleGroupStatement": {
        "VendorName": "AWS",
        "Name": "AWSManagedRulesBotControlRuleSet",
        "RuleActionOverrides": [
          {
            "ActionToUse": {
              "Count": {}
            },
            "Name": "CategoryVerifiedSearchEngine"
          },
          {
            "ActionToUse": {
              "Count": {}
            },
            "Name": "CategoryVerifiedSocialMedia"
          }
        ],
        "ExcludedRules": []
    },
   "VisibilityConfig": {
       "SampledRequestsEnabled": true,
       "CloudWatchMetricsEnabled": true,
       "MetricName": "AWS-AWSBotControl-Example"
   }
}
```

ルールグループの評価結果を Count にオーバーライド

ルールグループ内のルールの設定または評価方法を変更せずに、ルールグループ評価の結果によって発生するアクションをオーバーライドできます。このオプションは一般的に使用されません。ルールグループ内のいずれかのルールが一致した場合、このオーバーライドはルールグループの結果として生じるアクションを Count に設定します。

> **Note**
>
> これはまれなユースケースです。ほとんどのアクションオーバーライドは、ルールグループ内のルールアクションのオーバーライド で説明されているように、ルールグループ内のルールレベルで行われます。

ルールグループを追加または編集するとき、保護パック (ウェブ ACL) 内でルールグループの結果として生じるのアクションをオーバーライドできます。コンソールで、ルールグループの [Override rule group action - optional] (ルールグループアクションのオーバーライド - オプション) ペインを開いてオーバーライドを有効にします。次のリストの例に示すように、JSON セットで `OverrideAction` をルールグループステートメントに設定します。

```
{
   "Name": "AWS-AWSBotControl-Example",
   "Priority": 5,
   "Statement": {
    "ManagedRuleGroupStatement": {
     "VendorName": "AWS",
     "Name": "AWSManagedRulesBotControlRuleSet"
     }
   },
    "OverrideAction": {
       "Count": {}
    },
   "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSBotControl-Example"
   }
}
```

AWS リソースとの保護の関連付けまたは関連付け解除

を使用して AWS WAF 、保護パック (ウェブ ACLs) とリソースの間に次の関連付けを作成できます。

- リージョナル保護パック (ウェブ ACL) を以下のリージョナルリソースのいずれかに関連付けます。このオプションでは、保護パック (ウェブ ACL) はリソースと同じ地域にある必要があります。
  - Amazon API Gateway REST API
  - Application Load Balancer
  - AWS AppSync GraphQL API
  - Amazon Cognito ユーザープール
  - AWS App Runner サービス
  - Amazon Bedrock AgentCore Gateway
  - AWS Verified Access インスタンス
  - AWS Amplify
- グローバル保護パック (ウェブ ACL) を Amazon CloudFront ディストリビューションに関連付けます。グローバル保護パック (ウェブ ACL) には、米国東部 (バージニア北部) リージョンのハードコードリージョンを持ちます。

ディストリビューション自体を作成または更新するとき、保護パック (ウェブ ACL) を CloudFront ディストリビューションに関連付けることもできます。詳細については、Amazon CloudFront デベロッパーガイドAWS WAF 」の「 を使用してコンテンツへのアクセスを制御する」を参照してください。

複数の関連付けに関する制限

以下の制限に従って、1 つの保護パック (ウェブ ACL) を 1 つ以上の AWS リソースに関連付けることができます。

- 各 AWS リソースを関連付けることができる保護パック (ウェブ ACL) は 1 つだけです。保護パック (ウェブ ACL) と AWS リソースの関係は one-to-manyです。
- 保護パック (ウェブ ACL) を 1 つ以上の CloudFront ディストリビューションに関連付けることができます。CloudFront ディストリビューションに関連付けられている保護パック (ウェブ ACL) を他の AWS リソースタイプに関連付けることはできません。

追加の制限

保護パック (ウェブ ACL) の関連付けについて、次の追加制限が適用されます。

- 保護パック (ウェブ ACL) は、 AWS リージョン内の Application Load Balancer にのみ関連付けることができます。例えば、保護パック (ウェブ ACL) を AWS Outpostsにある Application Load Balancer に関連付けることはできません。
- Amazon Cognito ユーザープールを Fraud Control Account Creation AWS WAF Fraud Prevention (ACFP) マネージドルールグループ`AWSManagedRulesACFPRuleSet`または AWS WAF Fraud Control Account Takeover Prevention (ATP) マネージドルールグループ を使用する保護パック (ウェブ ACL) に関連付けることはできません`AWSManagedRulesATPRuleSet`。Account Creation Fraud Prevention については、「AWS WAF Fraud Control アカウント作成不正防止 (ACFP)」を参照してください。アカウント乗っ取り防止の情報については、「AWS WAF Fraud Control アカウント乗っ取り防止 (ATP)」を参照してください。

> ⚠ 本番稼働トラフィックのリスク
>
> 本番稼働トラフィックに保護パック (ウェブ ACL) をデプロイする前に、トラフィックへの潜在的な影響に慣れるまで、ステージング環境またはテスト環境でテストおよびチューニングします。その後、ルールを有効にする前に、本番稼働用トラフィックでカウントモードでルールをテストしてチューニングします。ガイダンスについては、「AWS WAF 保護のテストとチューニング」を参照してください。

AWS リソースへの保護の関連付け

Using the new console

1. 編集する保護パック (ウェブ ACL) を選択します。コンソールはメイン保護パック (ウェブ ACL) カードを編集可能にし、編集できる詳細を含むサイドパネルも開きます。
2. 保護パック (ウェブ ACL) カードで、[リソース] の横にある [編集] リンクを選択して、[リソースの管理] パネルを開きます。
3. ルールグループの [リソースの管理] セクションで、[リージョナルリソースの追加] または [グローバルリソースの追加] を選択します。
4. [リソース] 選択し、[追加] を選択します。

Using the standard console

ウェブ ACL を AWS リソースに関連付けるには、次の手順を実行します。

ウェブ ACL を AWS リソースに関連付けるには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで [ウェブ ACL] を選択します。
3. リソースに関連付けるウェブ ACL の名前を選択します。コンソールでウェブ ACL の説明が表示され、そこで編集できます。
4. 関連 AWS リソースタブで、 AWS リソースの追加を選択します。
5. プロンプトが表示されたら、リソースの種類を選択し、関連付けるリソースの横にあるラジオボタンを選択してから、[Add] (追加) を選択します。

AWS リソースから保護の関連付けを解除する

Using the new console

1. 編集する保護パック (ウェブ ACL) を選択します。コンソールはメイン保護パック (ウェブ ACL) カードを編集可能にし、編集できる詳細を含むサイドパネルも開きます。
2. 保護パック (ウェブ ACL) カードで、[リソース] の横にある [編集] リンクを選択して、[リソースの管理] パネルを開きます。
3. ルールグループの [リソースの管理] セクションで、関連付けを解除するリソースを選択し、[関連付けを解除] を選択します。

   > **Note**
   >
   > 一度に 1 つのリソースの関連付けを解除する必要があります。リソースを選択する際に複数選択しないでください。

4. 確認ページで「関連付け解除」と入力し、[関連付け解除] を選択します。

Using the standard console

ウェブ ACL と AWS リソースの関連付けを解除するには、次の手順を実行します。

AWS リソースからウェブ ACL の関連付けを解除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで [ウェブ ACL] を選択します。
3. リソースとの関連付けを解除するウェブ ACL の名前を選択します。コンソールでウェブ ACL の説明が表示され、そこで編集できます。
4. 関連 AWS リソースタブで、このウェブ ACL の関連付けを解除するリソースを選択します。

> **Note**
>
> 一度に 1 つのリソースの関連付けを解除する必要があります。リソースを選択する際に複数選択しないでください。

> **Note**
>
> Application Load Balancer をウェブ ACL に関連付けることを選択すると、リソースレベルの DDoS 保護 が有効になります。詳細については、「AWS WAF 分散サービス拒否 (DDoS) の防止」を参照してください。

5. [関連付け解除] を選択してください。コンソールに確認ダイアログが表示されます。 AWS リソースからウェブ ACL の関連付けを解除する選択を確認します。

のルールとルールグループで保護パック (ウェブ ACLs) を使用する AWS WAF

このセクションでは、保護パック (ウェブ ACL) とウェブ ACL がルールとルールグループと連携する方法について説明します。

保護パック (ウェブ ACL) がウェブリクエストを処理する方法は、次に応じて異なります。

- 保護パック (ウェブ ACL) およびルールグループ内のルールの優先順位の数値設定
- ルールおよび保護パック (ウェブ ACL) のアクション設定
- 追加したルールグループ内のルールに設定した上書き

ルールアクション設定のリストについては、「でのルールアクションの使用 AWS WAF」を参照してください。

ルールアクション設定とデフォルトの保護パック (ウェブ ACL) アクション設定で、リクエストと応答の処理をカスタマイズできます。詳細については、「でカスタマイズされたウェブリクエストとレスポンス AWS WAF」を参照してください。

トピック

- ルールの優先度を設定する
- がルールとルールグループのアクション AWS WAF を処理する方法
- でのルールグループアクションの上書き AWS WAF

ルールの優先度を設定する

このセクションでは、 AWS WAF が数値優先度設定を使用してルールの評価順序を設定する方法について説明します。

保護パック (ウェブ ACL) および任意のルールグループ内では、優先順位の数値設定を使用してルールの評価順序を決定します。保護パック (ウェブ ACL) 内の各ルールには、その保護パック (ウェブ ACL) 内で一意の優先順位を設定する必要があります。また、ルールグループ内の各ルールには、そのルールグループ内で一意の優先順位を設定する必要があります。

> **Note**
>
> コンソールを使用してルールグループ、保護パック (ウェブ ACLs) を管理すると、 はリスト内のルールの順序に基づいて一意の数値優先度設定 AWS WAF を割り当てます。 はリストの上部にあるルールに最小の数値優先度を割り当て、下部にあるルールに最大の数値優先度を AWS WAF 割り当てます。

は、ウェブリクエストに対してルールグループ、保護パック (ウェブ ACL) AWS WAF を評価すると、評価を終了するか、すべてのルールを使い果たす一致が見つかるまで、 の最小の数値優先度設定からルールを評価します。

例えば、保護パック (ウェブ ACL) に次のルールとルールグループがあり、次のように優先順位付けされているとします。

- Rule1 — 優先度 0

- RuleGroupA – 優先度 100
  - RuleA1 – 優先度 10,000
  - RuleA2 – 優先度 20,000
- Rule2 — 優先度 200
- RuleGroupB – 優先度 300
  - RuleB1 – 優先度 0
  - RuleB2 – 優先度 1

AWS WAF は、この保護パック (ウェブ ACL) のルールを次の順序で評価します。

- Rule1
- RuleGroupA RuleA1
- RuleGroupA RuleA2
- Rule2
- RuleGroupB RuleB1
- RuleGroupB RuleB2

がルールとルールグループのアクション AWS WAF を処理する方法

このセクションでは、 AWS WAF がルールとルールグループを使用してアクションを処理する方法について説明します。

ルールとルールグループを設定するときは、一致するウェブリクエスト AWS WAF の処理方法を選択します。

- Allow および Block は終了アクションです – Allow および Block アクションは、一致するウェブリクエストにおける保護パック (ウェブ ACL) のその他の処理をすべて停止されます。保護パック (ウェブ ACL) のルールがリクエストの一致を検出し、ルールアクションが Allowまたは の場合 Block、その一致によって保護パック (ウェブ ACL) のウェブリクエストの最終処理が決まります。AWS WAF は、一致するルールの後にある保護パック (ウェブ ACL) 内の他のルールを処理しません。これに該当するのは、保護パック (ウェブ ACL) に直接追加するルールや、追加されたルールグループに属するルールです。Block アクションでは、保護されたリソースはウェブリクエストを受信または処理しません。

- Count は非終了アクションです – Count アクションのあるルールがリクエストと一致すると、AWS WAF はリクエストをカウントし、その後に保護パック (ウェブ ACL) ルールセットに従うルールの処理を続行します。
- CAPTCHA および は、非終了アクションまたは終了アクションChallengeにすることができます – これらのアクションのいずれかを持つルールがリクエストに一致すると、 はそのトークンステータス AWS WAF をチェックします。リクエストに有効なトークンがある場合、 は一致と同様に Count一致 AWS WAF を処理し、保護パック (ウェブ ACL) ルールセットに続くルールの処理を続行します。リクエストに有効なトークンがない場合、 は評価 AWS WAF を終了し、解決する CAPTCHA パズルまたはサイレントバックグラウンドクライアントセッションチャレンジをクライアントに送信します。

ルール評価で終了アクションが発生しない場合、 は保護パック (ウェブ ACL) のデフォルトアクションをリクエスト AWS WAF に適用します。詳細については、「で保護パック (ウェブ ACL) のデフォルトアクションを設定する AWS WAF」を参照してください。

保護パック (ウェブ ACL) では、ルールグループ内のルールのアクション設定をオーバーライドしたり、ルールグループによって返されるアクションを上書きしたりできます。詳細については、「でのルールグループアクションの上書き AWS WAF」を参照してください。

アクションと優先度設定の相互作用

ウェブリクエスト AWS WAF に適用されるアクションは、保護パック (ウェブ ACL) のルールの数値優先度設定の影響を受けます。例えば、保護パック (ウェブ ACL) に Allow アクションと 50 の優先順位の数値を持つルール、ならび Count アクションと 100 の優先順位の数値を持つ別のルールがあるとします。 AWS WAF は優先順位に応じて最小のものからウェブ ACL 内のルールが評価するため、許可ルールをカウントルールより先に評価します。両方のルールに一致するウェブリクエストは、最初に許可ルールに一致します。Allow は終了アクションであるため、 AWS WAF はこの一致で評価を停止し、カウントルールに対してリクエストを評価しません。

- 許可ルールに一致しないリクエストのみをカウントルールメトリクスに含める場合は、ルールの優先度設定が便利です。
- 一方、許可ルールに一致するリクエストに対してもカウントルールのカウントメトリクスを取得する場合、カウントルールには許可ルールより小さい優先順位の数値を設定し、先に実行されるようにする必要があります。

優先順位の設定の詳細については、「ルールの優先度を設定する」を参照してください。

でのルールグループアクションの上書き AWS WAF

このセクションでは、ルールグループアクションを上書きする方法について説明します。

ルールグループを保護パック (ウェブ ACL) に追加するとき、一致するウェブリクエストに対して実行されるアクションをオーバーライドできます。保護パック (ウェブ ACL) 設定内のルールグループのアクションをオーバーライドしても、ルールグループ自体は変更されません。保護パック (ウェブ ACL) のコンテキストで がルールグループ AWS WAF を使用する方法のみを変更します。

ルールグループのルールアクションの上書き

ルールグループ内のルールのアクションは、任意の有効なルールアクションにオーバーライドきできます。これを実行すると、一致するリクエストは、設定されたルールのアクションがオーバーライド設定である場合とまったく同様に処理されます。

> **Note**
>
> ルールアクションは、終了アクションまたは非終了アクションである場合があります。終了アクションは、リクエストの保護パック (ウェブ ACL) 評価を停止し、保護されたアプリケーションへのリクエストの継続を許可またはブロックします。

ルールアクションのオプションは以下のとおりです。

- Allow – AWS WAF リクエストを保護された AWS リソースに転送して処理および応答できるようにします。これは終了アクションです。定義したルールでは、リクエストを保護されたリソースに転送する前に、カスタムヘッダーを挿入できます。
- Block – リクエストを AWS WAF ブロックします。これは終了アクションです。デフォルトでは、保護された AWS リソースは HTTP `403 (Forbidden)`ステータスコードで応答します。定義したルールでは、応答をカスタマイズできます。がリクエストを AWS WAF ブロックすると、Blockアクション設定によって、保護されたリソースがクライアントに返すレスポンスが決まります。
- Count – リクエストを AWS WAF カウントしますが、許可するかブロックするかは決定しません。これは非終了アクションです。 AWS WAF は保護パック (ウェブ ACL) の残りのルールの処理を継続します。定義したルールでは、リクエストにカスタムヘッダーを挿入し、他のルールで一致するラベルを追加できます。
- CAPTCHA および Challenge – CAPTCHA パズルとサイレントチャレンジ AWS WAF を使用して、リクエストがボットから送信されていないことを確認し、トークン AWS WAF を使用して最近成功したクライアントレスポンスを追跡します。

CAPTCHA パズルとサイレントチャレンジは、ブラウザが HTTPS エンドポイントにアクセスしている場合にのみ実行できます。トークンを取得するには、ブラウザクライアントが安全なコンテキストで実行されている必要があります。

> **Note**
>
> CAPTCHA または Challenge ルールアクションを 1 つのルールで使用、あるいはルールグループでルールアクションのオーバーライドとして使用すると、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

これらのルールアクションは、リクエスト内のトークンの状態に応じて、終了アクションまたは非終了アクションである場合があります。

- 有効で有効期限が切れていないトークンの非終了 – トークンが有効で、設定された CAPTCHA またはチャレンジイミュニティ時間に従って有効期限が切れていない場合、 は Count action のようなリクエスト AWS WAF を処理します。 AWS WAF は引き続き、保護パック (ウェブ ACL) の残りのルールに基づいてウェブリクエストを検査します。Count 設定と同様に、定義したルールでは、リクエストに挿入するカスタムヘッダーを使用してこれらのアクションを設定したり (オプション)、他のルールが照合できるラベルを追加したりできます。
- 無効または期限切れのトークンのブロックされたリクエストで終了 – トークンが無効であるか、指定されたタイムスタンプの有効期限が切れている場合、 は Block アクションと同様にウェブリクエストの検査 AWS WAF を終了し、リクエストをブロックします。 AWS WAF その後、 はカスタムレスポンスコードでクライアントに応答します。CAPTCHA には、リクエスト内容はクライアントのブラウザが処理できることが示された場合、 AWS WAF は人間のクライアントとボットを区別するように設計された JavaScript インタースティシャルで CAPTCHA パズルを送信します。Challenge アクションの場合、 は、通常のブラウザをボットによって実行されているセッションと区別するように設計されたサイレントチャレンジで JavaScript インタースティシャル AWS WAF を送信します。

詳細については、「CAPTCHA および Challengeの AWS WAF」を参照してください。

このオプションの使用方法については、「ルールグループ内のルールアクションのオーバーライド」を参照してください。

ルールアクションを Count にオーバーライド

ルールアクションオーバーライドの最も一般的な使用例は、ルールアクションの一部またはすべてを Count にオーバーライドして、ルールグループの動作を本番稼働に移行する前にテストおよびモニタリングすることです。

これを使用して誤検出を生成しているルールグループをトラブルシューティングすることもできます。誤検出は、ブロックすると想定していないトラフィックをルールグループがブロックするときに発生します。ルールグループ内で、許可したいリクエストをブロックするルールを特定した場合、そのルールに対するこのカウントアクションのオーバーライドを保持し、リクエストに対するアクションを除外できます。

テストでルールアクションのオーバーライドを使用する詳細については、「AWS WAF 保護のテストとチューニング」を参照してください。

JSON リスト: **`RuleActionOverrides`** を **`ExcludedRules`** に置き換えます

2022 年 10 月 27 日より前に保護パック (ウェブ ACL) 設定Countでルールグループのルールアクションを に設定した場合、 は保護パック (ウェブ ACL) JSON にオーバーライドを として AWS WAF 保存しましたExcludedRules。これで、ルールを Count にオーバーライドする JSON 設定が RuleActionOverrides 設定に追加されました。

JSON リストですべての ExcludedRules 設定は、アクションを Count に設定した RuleActionOverrides 設定に更新することをお勧めします。API はどちらの設定も受け付けますが、新しい RuleActionOverrides 設定のみを使用した場合、コンソール作業と API 作業の間で JSON リストの一貫性が保たれます。

> **Note**
>
> AWS WAF コンソールでは、保護パック (ウェブ ACL) のサンプルリクエストタブには、古い設定のルールのサンプルは表示されません。詳細については、「ウェブリクエストのサンプルの表示」を参照してください。

AWS WAF コンソールを使用して既存のルールグループ設定を編集すると、コンソールは JSON のすべてのRuleActionOverrides設定を ExcludedRules 設定に自動的に変換し、オーバーライドアクションは に設定されますCount。

- 現在の設定例:

```
       "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesAdminProtectionRuleSet",
          "RuleActionOverrides": [
            {
              "Name": "AdminProtection_URIPATH",
              "ActionToUse": {
                "Count": {}
              }
            }
          ]
```

- 古い設定例:

```
OLD SETTING
       "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesAdminProtectionRuleSet",
          "ExcludedRules": [
            {
              "Name": "AdminProtection_URIPATH"
            }
          ]
OLD SETTING
```

ルールグループの戻り値アクションを Count に上書き

ルールグループが返すアクションをオーバーライドして、Count に設定できます。

> **Note**
>
> これは、 がルールグループ自体 AWS WAF を評価する方法を変更しないため、ルールグループのルールをテストするには適していません。ルールグループ評価から保護パック (ウェブ ACL) に返される結果 AWS WAF の処理方法にのみ影響します。ルールグループ内のルールをテストする場合は、前述のセクションで説明したオプション ルールグループのルールアクションの上書き を使用します。

ルールグループアクションを に上書きするとCount、 はルールグループ評価を正常に AWS WAF 処理します。

ルールグループ内のルールが一致しない、あるいはすべての一致するルールに Count アクションがある場合、このオーバーライドはルールグループまたは保護パック (ウェブ ACL) の処理に影響を与えません。

ウェブリクエストに一致し、終了ルールアクションを持つルールグループの最初のルールは、 AWS WAF がルールグループの評価を停止し、終了アクションの結果を保護パック (ウェブ ACL) 評価レベルに返します。この時点で、保護パック (ウェブ ACL) 評価では、このオーバーライドが有効になります。ルールグループ評価の結果がアクションのみになるように、このオーバーライドは終了Countアクションを AWS WAF 上書きします。 AWS WAF その後、 は保護パック (ウェブ ACL) の残りのルールの処理を続行します。

このオプションの使用方法については、「ルールグループの評価結果を Count にオーバーライド」を参照してください。

で保護パック (ウェブ ACL) のデフォルトアクションを設定する AWS WAF

このセクションでは、保護パック (ウェブ ACL) のデフォルトアクションの仕組みについて説明します。

保護パック (ウェブ ACL) を作成および設定するときに、保護パック (ウェブ ACL) のデフォルトアクションを設定する必要があります。 AWS WAF は、終了アクションが適用されることなく、保護パック (ウェブ ACL) のルール評価をすべて通過したウェブリクエストすべてに、このアクションを適用します。終了アクションは、リクエストの保護パック (ウェブ ACL) 評価を停止し、保護されたアプリケーションへのリクエストの継続を許可またはブロックします。ルールアクションについては、「でのルールアクションの使用 AWS WAF」を参照してください。

保護パック (ウェブ ACL) のデフォルトアクションがウェブリクエストの最終的な処理を決定する必要があります。したがって、これは終了アクションです。

- Allow – ほとんどのユーザーに対してウェブサイトへのアクセスを許可する一方、指定した IP アドレスからのリクエストまたは悪意のある SQL コードや指定した値が含まれている可能性があるリクエストを行う攻撃者に対してアクセスを拒否する場合、デフォルトアクションとして Allow を選択します。その後、ブロックする特定のリクエストを識別してブロックするルールを、保護パック (ウェブ ACL) に追加します。このアクションを使用すると、保護されたリソースに転送する前に、カスタムヘッダーをリクエストに挿入できます。
- Block – ほとんどのユーザーに対してはウェブサイトへのアクセスを拒否する一方、指定した IP アドレスからのリクエストまたは指定した値が含まれているリクエストを行うユーザーに対してアクセスを許可する場合、デフォルトアクションとして Block を選択します。その後、許可する特定の

リクエストを識別して許可するルールを、保護パック (ウェブ ACL) に追加します。デフォルトでは、 Blockアクションでは、 AWS リソースは HTTP 403 (Forbidden)ステータスコードで応答しますが、応答をカスタマイズできます。

リクエストとレスポンスをカスタマイズする方法については、「でカスタマイズされたウェブリクエストとレスポンス AWS WAF」を参照してください。

独自のルールとルールグループの設定は、ほとんどのウェブリクエストを許可するかブロックするかに応じて、一部が異なります。例えば、ほとんどのリクエストを 許可する 場合、保護パック (ウェブ ACL) のデフォルトアクションを Allow に設定し、その後に ブロックする ウェブリクエストを識別するルールを追加します。これには次のようなリクエストが該当します。

- リクエスト数が不当に多い IP アドレスからのリクエスト
- お客様がビジネスを行っていない国、または頻繁に攻撃元になっている国からのリクエスト
- User-agent ヘッダーに不正な値が含まれているリクエスト
- 悪意のある SQL コードが含まれている可能性があるリクエスト

マネージドルールグループのルールは通常、Block アクションを使用しますが、すべての場合に限りません。例えば、Bot Control に使用される一部のルールでは、CAPTCHA および Challenge アクション設定を使用します。マネージドルールグループの詳細については、「でのマネージドルールグループの使用 AWS WAF」を参照してください。

でのボディ検査の管理に関する考慮事項 AWS WAF

本文検査サイズ制限は、 が検査 AWS WAF できるリクエスト本文の最大サイズです。ウェブリクエスト本文が制限より大きい場合、基盤となるホストサービスは、制限内のコンテンツを検査 AWS WAF のために に転送します。

- Application Load Balancer および の場合 AWS AppSync、制限は 8 KB (8,192 バイト) に固定されます。
- CloudFront、API Gateway、Amazon Cognito、App Runner、Verified Access、Amazon Bedrock AgentCore Gateway の場合、デフォルトの制限は 16 KB (16,384 バイト) であり、任意のリソースタイプの制限を 16 KB、最大 64 KB の増分で増やすことができます。設定オプションは 16 KB、32 KB、48 KB、および 64 KB です。

> **Important**
>
> AWS WAF は、gRPC トラフィックのリクエスト本文検査ルールをサポートしていません。これらのルールを CloudFront ディストリビューションまたは Application Load Balancer の保護パック (ウェブ ACL) で有効にした場合、gRPC を使用するすべてのリクエストでは、リクエスト本文の検査ルールを無視します。他のすべての AWS WAF ルールは引き続き適用されます。詳細については、Amazon CloudFront デベロッパーガイド」の「ディストリビューション AWS WAF の有効化」を参照してください。

オーバーサイズ本文の処理

ウェブトラフィックに制限を超えるサイズのボディが含まれている場合は、設定されたオーバーサイズ処理が適用されます。オーバーサイズの処理のオプションの詳細については、でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF を参照してください。

制限設定を増やすための料金に関する考慮事項

AWS WAF は、リソースタイプのデフォルト制限内にあるトラフィックを検査するためのベースレートを請求します。

CloudFront、API Gateway、Amazon Cognito、App Runner、Verified Access、Amazon Bedrock AgentCore Gateway リソースの場合、制限設定を増やすと、検査 AWS WAF できるトラフィックには、新しい制限までの本文サイズが含まれます。ボディサイズがデフォルトの 16 KB よりも大きいリクエストの検査に対してのみ、追加料金がかかります。料金の詳細については、「AWS WAF 料金」を参照してください。

ボディ検査サイズの制限の変更オプション

CloudFront、API Gateway、Amazon Cognito、App Runner、Verified Access、または Amazon Bedrock AgentCore Gateway リソースの本文検査サイズ制限を設定できます。

保護パック (ウェブ ACL) を作成または編集するときは、リソースの関連付け設定でボディ検査サイズの制限を修正できます。API については、AssociationConfig の保護パック (ウェブ ACL) の関連付け設定を参照してください。コンソールについては、保護パック (ウェブ ACL) の関連リソースを指定するページにある設定を参照してください。コンソール設定に関するガイダンスについては、「でのウェブトラフィックメトリクスの表示 AWS WAF」を参照してください。

AWS WAF Application Load Balancer での HTTP/2 トラフィックの検査コントロール

が HTTP/2 ターゲットにルーティングするときに (Application Load Balancer) で HTTP/2 リクエストボディを AWS WAF 検査する方法を設定できます。検査タイミングを調整すると、セキュリティカバレッジとアプリケーションの通信パターンのバランスをとることができます。

この設定を変更するには、HTTP/2 ターゲットのターゲットグループ属性を編集します。この設定は、Application Load Balancer ターゲットグループコンソールの WAF HTTP/2 トラフィック検査動作にあります。詳細については、「ALB ドキュメント」を参照してください。

WAF HTTP/2 トラフィック検査動作の属性は次のとおりです。

すぐに検査する (デフォルト)

AWS WAF は、使用可能なリクエストデータを使用して、各 HTTP/2 リクエストを直ちに検査します。

クライアントがリクエストの送信を完了する前にサーバーレスポンスを期待する双方向ストリーミングアプリケーションの場合は、このオプションを選択します。これにより、リアルタイムの双方向通信を必要とするアプリケーションのタイムアウトを防ぐことができます。

十分なデータの後に検査する

AWS WAF 検査は、クライアントから十分な HTTP/2 データフレームを受信した後にのみ開始され、セキュリティを強化するための完全なリクエスト検査が保証されます。

サーバーレスポンスを期待する前にクライアントがすべてのリクエストデータを送信する標準リクエストレスポンスアプリケーションの場合は、このオプションを選択します。これは、ほとんどのユースケースで推奨される設定です。

での CAPTCHA、チャレンジ、トークンの設定 AWS WAF

CAPTCHA または ルールChallengeアクションを使用するルールと、 AWS WAF マネージド保護のサイレントクライアントチャレンジを管理するアプリケーション統合 SDKs に対して、保護パック (ウェブ ACL) のオプションを設定できます。

これらの機能は、エンドユーザーに CAPTCHA パズルで挑戦させて、クライアントセッションにサイレントチャレンジを提供することにより、ボットの活動を軽減します。クライアントが応答に成功すると、 AWS WAF はクライアントがウェブリクエストで使用するトークンを提供します。このトークンは最後に成功したパズルおよびチャレンジレス応答のタイムスタンプが付いています。詳細については、「でのインテリジェントな脅威の軽減 AWS WAF」を参照してください。

保護パック (ウェブ ACL) 設定では、 がこれらのトークン AWS WAF を管理する方法を設定できます。

- CAPTCHA およびチャレンジイミュニティ時間 – CAPTCHA またはチャレンジのタイムスタンプの有効期間を指定します。保護パック (ウェブ ACL) 設定は、独自のイミュニティ時間設定が設定されていないすべてのルール、ならびにアプリケーション統合 SDK にも継承されます。詳細については、「でのタイムスタンプの有効期限とトークンイミュニティ時間の設定 AWS WAF」を参照してください。
- トークンドメイン – デフォルトでは、 は保護パック (ウェブ ACL) が関連付けられているリソースのドメインに対してのみトークン AWS WAF を受け入れます。トークンドメインリストを設定すると、 はリスト内のすべてのドメインと、関連付けられたリソースのドメインのトークン AWS WAF を受け入れます。詳細については、「AWS WAF 保護パック (ウェブ ACL) トークンドメインリスト設定」を参照してください。

でのウェブトラフィックメトリクスの表示 AWS WAF

このセクションでは、ウェブトラフィックメトリクスの概要にアクセスする方法について説明します。

使用している保護パック (ウェブ ACL) については、 AWS WAF コンソールの 保護パック (ウェブ ACL) のページのトラフィック概要タブにあるウェブトラフィックメトリクスの概要にアクセスできます。コンソールダッシュボードには、アプリケーションウェブトラフィックを評価するときに が AWS WAF 収集する Amazon CloudWatch メトリクスの概要がほぼリアルタイムで表示されます。ダッシュボードのページの詳細については、「保護パック (ウェブ ACL) のトラフィック概要ダッシュボード」を参照してください。保護パック (ウェブ ACL) のトラフィックのモニタリングに関する追加情報については、「AWS WAF 保護のモニタリングと調整」を参照してください。

保護パック (ウェブ ACL) の削除

このセクションでは、 AWS コンソールから保護パック (ウェブ ACLs) を削除する手順について説明します。

> **Important**
>
> 保護パック (ウェブ ACL) の削除は永続的であり、元に戻すことはできません。

保護パック (ウェブ ACL) を削除するには、まず保護パック (ウェブ ACL) からすべての AWS リソースの関連付けを解除します。次の手順を実行します。

Using the new console

1. 新しい にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2-pro で AWS WAF コンソールを開きます。
2. ナビゲーションペインで、[リソースと保護パック (ウェブ ACL)] を選択します。
3. 保護パック (ウェブ ACL) カードで、[リソース] の横にある [編集] リンクを選択して、[リソースの管理] パネルを開きます。
4. ルールグループの [リソースの管理] セクションで、関連付けを解除するリソースを選択し、[関連付けを解除] を選択します。

   > **Note**
   >
   > 一度に 1 つのリソースの関連付けを解除する必要があります。リソースを選択する際に複数選択しないでください。

5. 確認ページで「関連付け解除」と入力し、[関連付け解除] を選択します。保護パック (ウェブ ACL) 内の各リソースの関連付け解除を繰り返します。
6. 削除する保護パック (ウェブ ACL) を選択します。コンソールはメイン保護パック (ウェブ ACL) カードを編集可能にし、編集できる詳細を含むサイドパネルも開きます。
7. 詳細パネルで、ごみ箱アイコンを選択します。
8. 確認ページで「delete」と入力し、[削除] を選択します。

Using the standard console

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで [ウェブ ACL] を選択します。
3. 削除するウェブ ACL の名前を選択します。コンソールでウェブ ACL の説明が表示され、そこで編集できます。

> **Note**
>
> 削除するウェブ ACL が表示されない場合は、ウェブ ACL セクション内のリージョン選択が正しいことを確認してください。Amazon CloudFront ディストリビューションを保護するウェブ ACL は [グローバル (CloudFront)] にあります。

4. 関連付けられた AWS リソースタブで、関連付けられたリソースごとに、リソース名の横にあるラジオボタンを選択し、関連付け解除を選択します。これにより、 AWS リソースから保護パック (ウェブ ACL) の関連付けが解除されます。
5. ナビゲーションペインで [ウェブ ACL] を選択します。
6. 削除するウェブ ACL の横にあるラジオボタンを選択し、[Delete] (削除) を選択します。

AWS WAF ルール

このセクションでは、 AWS WAF ルールとその仕組みについて説明します。

AWS WAF ルールは、HTTP(S) ウェブリクエストを検査する方法と、検査基準に一致するリクエストに対して実行するアクションを定義します。ルールは、ルールグループまたは保護パック (ウェブ ACL) のコンテキストでのみ定義されます。

ルールは AWS WAF 、独自の には存在しません。これらは AWS リソースではなく、Amazon リソースネーム (ARNsもありません。ルールが定義されているルールグループまたは保護パック (ウェブ ACL) に含まれる名前を使用してルールにアクセスします。ルールを管理し、他の保護パック (ウェブ ACL) にコピーするには、そのルールが含まれているルールグループまたは保護パック (ウェブ ACL) の JSON ビューを使用します。また、保護パック (ウェブ ACLs) とルールグループで使用できる AWS WAF コンソールルールビルダーを使用して管理することもできます。

ルール名

各ルールには名前が必要です。AWS で始まる名前や、他のサービスによって管理されているルールグループまたはルールに使用されている名前は避けてください。「他のサービスによって提供されるルールグループを識別する」を参照してください。

> **Note**
>
> ルールの名前を変更し、ルールのメトリクス名に変更を反映する場合は、メトリクス名も更新する必要があります。ルール名を変更しても、ルールのメトリクス名は自動的に更新

AWS WAF されません。ルールの JSON エディターを使用して、コンソールでルールを編集するときに、メトリック名を変更できます。API や、保護パック (ウェブ ACL) またはルールグループの定義に使用する JSON リストを使用して、両方の名前を変更することもできます。

ルールステートメント

各ルールには、ルールがウェブリクエストを検査する方法を定義するルールステートメントも必要です。ルールステートメントには、ルールとステートメントのタイプに応じて、ネストされたステートメントを任意の深さに含めることができます。一部のルールステートメントは、条件のセットを採用します。例えば、IP セット一致ルールに最大 10,000 個の IP アドレスまたは IP アドレス範囲を指定できます。

次のような基準を検査するルールを定義できます。

- 悪意のある可能性が高いスクリプト。攻撃者は、ウェブアプリケーションの脆弱性を悪用できるスクリプトを埋め込みます。これはクロスサイトスクリプティング (XSS) と呼ばれます。
- リクエストの発生元の IP アドレスまたはアドレス範囲。
- リクエスト送信元の国または地理的場所。
- クエリ文字列など、リクエストの指定した部分の長さ。
- 悪意のある可能性が高い SQL コード。攻撃者は、ウェブリクエストに悪意のある SQL コードを埋め込むことで、データベースからデータを抽出しようとします。これは SQL インジェクションと呼ばれます。
- リクエストに表示される文字列。例えば、`User-Agent` ヘッダーに表示される値、またはクエリ文字列に表示されるテキスト文字列です。正規表現を使用してこれらの文字列を指定することもできます。
- 保護パック (ウェブ ACL) の以前のルールがリクエストに追加したラベル。

上記のリストにあるようなウェブリクエスト検査基準を持つステートメントに加えて、 は、ルール内のステートメントを組み合わせるNOTために使用される AND、OR、および の論理ステートメント AWS WAF をサポートします。

例えば、攻撃者からの最近のリクエストに基づいて、次のネストされたステートメントを組み合わせた論理 AND ステートメントを使用してルールを作成できます。

- リクエストが 192.0.2.44 から発生した。

- リクエストの User-Agent ヘッダーに BadBot 値が含まれる。
- それらのクエリ文字列には、SQL などのコードが含まれる。

この場合、上位のレベルの AND に一致するようにするには、ウェブリクエストはすべてのステートメントに一致する必要があります。

トピック

- でのルールアクションの使用 AWS WAF
- でのルールステートメントの使用 AWS WAF
- での一致ルールステートメントの使用 AWS WAF
- での論理ルールステートメントの使用 AWS WAF
- でのレートベースのルールステートメントの使用 AWS WAF
- でのルールグループルールステートメントの使用 AWS WAF

でのルールアクションの使用 AWS WAF

このセクションでは、ルールアクションの仕組みについて説明します。

ルールアクションは、ウェブリクエストがルールで定義された条件に一致する場合に、 AWS WAF ウェブリクエストの処理を指示します。オプションで、各ルールアクションにカスタム動作を追加できます。

> **Note**
>
> ルールアクションは、終了アクションまたは非終了アクションである場合があります。終了アクションは、リクエストの保護パック (ウェブ ACL) 評価を停止し、保護されたアプリケーションへのリクエストの継続を許可またはブロックします。

ルールアクションのオプションは以下のとおりです。

- Allow – AWS WAF リクエストを保護された AWS リソースに転送して処理および応答できるようにします。これは終了アクションです。定義したルールでは、リクエストを保護されたリソースに転送する前に、カスタムヘッダーを挿入できます。
- Block – リクエストを AWS WAF ブロックします。これは終了アクションです。デフォルトでは、保護された AWS リソースは HTTP 403 (Forbidden)ステータスコードで応答します。定義した

ルールでは、応答をカスタマイズできます。がリクエストを AWS WAF ブロックすると、Blockアクション設定によって、保護されたリソースがクライアントに送り返すレスポンスが決まります。

- Count – リクエストを AWS WAF カウントしますが、許可するかブロックするかは決定しません。これは非終了アクションです。 AWS WAF は保護パック (ウェブ ACL) の残りのルールの処理を継続します。定義したルールでは、リクエストにカスタムヘッダーを挿入し、他のルールで一致するラベルを追加できます。
- CAPTCHA および Challenge – CAPTCHA パズルとサイレントチャレンジ AWS WAF を使用して、リクエストがボットから送信されていないことを確認し、トークン AWS WAF を使用して最近成功したクライアントレスポンスを追跡します。

  CAPTCHA パズルとサイレントチャレンジは、ブラウザが HTTPS エンドポイントにアクセスしている場合にのみ実行できます。トークンを取得するには、ブラウザクライアントが安全なコンテキストで実行されている必要があります。

  > **Note**
  >
  > CAPTCHA または Challenge ルールアクションを 1 つのルールで使用、あるいはルールグループでルールアクションのオーバーライドとして使用すると、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

  これらのルールアクションは、リクエスト内のトークンの状態に応じて、終了アクションまたは非終了アクションである場合があります。

  - 有効で有効期限が切れていないトークンの非終了 – トークンが有効で、設定された CAPTCHA またはチャレンジイミュニティ時間に従って有効期限が切れていない場合、 は Count action と同様のリクエスト AWS WAF を処理します。 AWS WAF は引き続き、保護パック (ウェブ ACL) の残りのルールに基づいてウェブリクエストを検査します。Count 設定と同様に、定義したルールでは、リクエストに挿入するカスタムヘッダーを使用してこれらのアクションを設定したり (オプション)、他のルールが照合できるラベルを追加したりできます。
  - 無効または期限切れのトークンのブロックされたリクエストで終了 – トークンが無効であるか、指定されたタイムスタンプの有効期限が切れている場合、 はウェブリクエストの検査 AWS WAF を終了し、 Blockアクションと同様にリクエストをブロックします。 AWS WAF その後、はカスタムレスポンスコードでクライアントに応答します。CAPTCHA には、リクエスト内容はクライアントのブラウザが処理できることが示された場合、 AWS WAF は人間のクライアントとボットを区別するように設計された JavaScript インタースティシャルで CAPTCHA パズルを送信します。Challenge アクションの場合、 は、通常のブラウザをボットによって実行され

ているセッションと区別するように設計されたサイレントチャレンジで JavaScript インタースティシャル AWS WAF を送信します。

詳細については、「CAPTCHA および Challengeの AWS WAF」を参照してください。

リクエストとレスポンスをカスタマイズする方法については、「でカスタマイズされたウェブリクエストとレスポンス AWS WAF」を参照してください。

一致するリクエストへのラベルの追加については、「でのウェブリクエストのラベル付け AWS WAF」を参照してください。

保護パック (ウェブ ACL) とルール設定の相互作用の詳細については、「のルールとルールグループで保護パック (ウェブ ACLs) を使用する AWS WAF」を参照してください。

収益化アクション

Monetize アクションは、リクエスト元のクライアントに HTTP 402 Payment Required レスポンスを返します。レスポンスには、クライアントが支払いを完了し、リソースにアクセスするために使用する、機械読み取り可能な x402 支払い手順が含まれています。Monetize アクションを使用して、AI ボットとエージェントにコンテンツアクセスの料金を請求します。このアクションは、Amazon CloudFront ACLs でのみ使用でき、ウェブ ACL に MonetizationConfig が必要です。

Monetize アクションの仕組み

Monetize アクションを持つルールがリクエストと一致する場合:

1. リクエストに有効な`payment-signature`ヘッダーが含まれていない場合、 は Payment Required Challenge (HTTP 402 response with payment instructions) AWS WAF を発行します。
2. クライアントは支払い承認に署名し、 `payment-signature`ヘッダーを使用してリクエストを再送信します。
3. AWS WAF は支払い承認を検証します。
4. 検証が成功すると、リクエストはオリジンに進みます。
5. オリジンが 2xx レスポンスを返した後、支払いはサードパーティーのファシリテーションサービスを介してチェーン上で決済されます。
6. コンテンツは、決済確認とともにクライアントに提供されます。

> **Important**
>
> AI トラフィック収益化ポリシーを実装するために、動作シグナルやリスクベースのシステムなどの複数の検出手法を使用して、インバウンドトラフィックを検査および分類します。これらのメソッドは高い信頼性の分類を提供するように設計されていますが、確率的であり、すべてのボットトラフィックを正しく識別または分類できない場合があります。当社では、精度を高めるために分析方法を継続的にテストおよび更新しています。ライブ収益化を有効にする前に、テストモードを使用してポリシーが期待される結果を生成することを確認することをお勧めします。

アクションパラメータの収益化

[Parameter] (パラメータ)	[Required] (必須)	説明
`PriceMultiplier`	いいえ	ウェブ ACL の MonetizationConfig で定義された基本価格に適用される整数乗数 (1 ～ 100)。リクエストの有効な料金は、基本価格にこの値を乗じたものです。を文字列として指定します。デフォルト: "1"。

アクション動作の収益化

- 評価の終了 – ブロックと同様に、Monetize アクションは一致するリクエストのルール評価を終了します。
- CloudFront のみ – Amazon CloudFront ディストリビューションを保護するウェブ ACLs でのみサポートされます。
- メトリクス – `BlockedRequests`および とは別に、CloudWatch で`MonetizeRequests`メトリクスを出力します`AllowedRequests`。
- ログ記録 – AWS WAF ログには、トリガーされたときに収益化固有のフィールドが含まれます。

例: JSON での収益化ルール

```
{
  "Name": "MonetizeUnverifiedBots",
  "Priority": 5,
  "Statement": {
    "LabelMatchStatement": {
      "Scope": "LABEL",
      "Key": "awswaf:managed:aws:bot-control:bot:unverified"
    }
  },
  "Action": {
    "Monetize": {
      "PriceMultiplier": "2"
    }
  },
  "VisibilityConfig": {
    "CloudWatchMetricsEnabled": true,
    "MetricName": "MonetizeUnknownBotsMetric",
    "SampledRequestsEnabled": true
  }
}
```

制限事項

- Amazon CloudFront (グローバルスコープ) でのみ使用できます。
- ウェブ ACL に MonetizationConfig が必要です。
- レートベースのルールでは、アクションとして Monetize を使用することはできません。

でのルールステートメントの使用 AWS WAF

このセクションでは、ルールステートメントの仕組みについて説明します。

ルールステートメントは、ウェブリクエストを検査 AWS WAF する方法を に指示するルールの一部です。がウェブリクエストで検査基準 AWS WAF を見つけると、ウェブリクエストは ステートメントと一致すると表示されます。すべてのルールステートメントは、ステートメントのタイプに応じて、何をどのように検索するかを指定します。

のすべてのルール AWS WAF には 1 つの最上位ルールステートメントがあり、他のステートメントを含めることができます。ルールステートメントは非常にシンプルにすることができます。例えば、

ウェブリクエストを検査するための送信国のセットを提供するステートメントを作成したり、保護パック (ウェブ ACL) でルールグループを参照するだけのルールステートメントを保持したりできます。ルールステートメントはまた、非常に複雑にすることもできます。例えば、他の多くのステートメントを論理 AND、OR、および NOT ステートメントと組み合わせたステートメントを作成できます。

ほとんどのルールでは、一致するリクエストにカスタム AWS WAF ラベルを追加できます。 AWS マネージドルールルールルールグループのルールは、一致するリクエストにラベルを追加します。ルールが追加するラベルは、保護パック (ウェブ ACL) および AWS WAF ログとメトリクスの後半で評価されるルールへのリクエストに関する情報を提供します。ラベル付けの詳細については、でのウェブリクエストのラベル付け AWS WAF と ラベル一致ルールステートメント を参照してください。

ルールステートメントのネスト

AWS WAF は、多くのルールステートメントのネストをサポートしていますが、すべてではありません。例えば、ルールグループステートメントを別のステートメント内にネストすることはできません。スコープダウンステートメントや論理ステートメントなど、一部のシナリオではネストを使用する必要があります。ルールステートメントのリストとそれに続くルールの詳細では、各カテゴリとルールのネスト機能と要件について説明されています。

コンソール内のルールのビジュアルエディタでは、ルールステートメントの 1 レベルのネストしかサポートされません。例えば、論理 AND または OR ルール内に多くのタイプのステートメントをネストできますが、他の AND または OR ルールをネストすることはできません。2 レベルのネストが必要になるからです。複数のレベルのネストを実装するには、コンソールの JSON ルールエディタまたは API を使用して、JSON でルール定義を指定します。

トピック

- でのルールステートメント設定の調整 AWS WAF
- でのスコープダウンステートメントの使用 AWS WAF
- で再利用可能なエンティティを参照する AWS WAF

でのルールステートメント設定の調整 AWS WAF

このセクションでは、ウェブリクエストのコンポーネントを検査するルールステートメントで指定できる設定について説明します。使用の詳細については、「での一致ルールステートメントの使用 AWS WAF」で個別のルールステートメントを参照してください。

これらのウェブリクエストコンポーネントのサブセットは、カスタムリクエスト集約キーとしてレートベースのルールで使用することもできます。詳細については、「でのレートベースのルールの集計 AWS WAF」を参照してください。

リクエストコンポーネントの設定では、コンポーネントタイプ自体と、コンポーネントタイプに応じる追加オプションを指定します。例えば、テキストを含むコンポーネントタイプを検査する場合、検査する前にテキスト変換を適用できます。

> **Note**
>
> 特に明記されていない限り、ウェブリクエストにルールステートメントで指定されたリクエストコンポーネントがない場合、 AWS WAF はリクエストをルール条件に一致しないものとして評価します。

目次

- でコンポーネントをリクエストする AWS WAF
  - HTTP メソッド
  - 単一ヘッダー
  - すべてのヘッダー
  - ヘッダーの順序
  - cookie
  - URI フラグメント
  - URI パス
  - JA3 フィンガープリント
  - JA4 フィンガープリント
  - クエリ文字列
  - Single query parameter (単一クエリパラメータ)
  - All query parameters (すべてのクエリパラメータ)
  - [Body] (本文)
  - JSON 本文
- で転送された IP アドレスを使用する AWS WAF
- での HTTP/2 擬似ヘッダーの検査 AWS WAF
- でのテキスト変換の使用 AWS WAF

- での事前解析テキスト変換の使用 AWS WAF

でコンポーネントをリクエストする AWS WAF

このセクションでは、検査のために指定できるウェブリクエストのコンポーネントについて説明します。ウェブリクエスト内のパターンを検索する一致ルールステートメントのリクエストコンポーネントを指定します。これらのステートメントのタイプには、文字列一致、正規表現一致、サイズ制約、SQL インジェクション攻撃などのステートメントがあります。リクエストコンポーネント設定の使用方法については、「での一致ルールステートメントの使用 AWS WAF」で個々のルールステートメントを参照してください。

特に明記されていない限り、ウェブリクエストにルールステートメントで指定されたリクエストコンポーネントがない場合、 AWS WAF はリクエストをルール条件に一致しないものとして評価します。

> **Note**
>
> リクエストコンポーネントは、それを必要とするルールステートメントごとに 1 つずつ指定します。リクエストの複数のコンポーネントを検査するには、コンポーネントごとにルールステートメントを作成します。

AWS WAF コンソールと API のドキュメントには、次の場所のリクエストコンポーネント設定に関するガイダンスが記載されています。

- コンソールのルールビルダー – 通常のルールタイプの [Statement] (ステートメント) 設定で、[Request components] (コンポーネントをリクエスト) の下の [Inspect] (検査) ダイアログで検査するコンポーネントを選択します。
- API ステートメントのコンテンツ – `FieldToMatch`

このセクションの残りの部分では、ウェブリクエストの検査対象部分のオプションについて説明します。

トピック

- HTTP メソッド
- 単一ヘッダー
- すべてのヘッダー

- ヘッダーの順序
- cookie
- URI フラグメント
- URI パス
- JA3 フィンガープリント
- JA4 フィンガープリント
- クエリ文字列
- Single query parameter (単一クエリパラメータ)
- All query parameters (すべてのクエリパラメータ)
- [Body] (本文)
- JSON 本文

HTTP メソッド

リクエストの HTTP メソッドが検査されます。HTTP メソッドは、ウェブリクエストが保護対象リソースに対して実行を求めている操作のタイプ (POST または GET など) を示しています。

単一ヘッダー

リクエスト内の単一の名前付きヘッダーが検査されます。

このオプションでは、User-Agent や Referer などのヘッダー名を指定します。名前の文字列一致では大文字と小文字は区別されず、リクエストヘッダーとルールの両方から先頭と末尾のスペースをトリミングした後に実行されます。

すべてのヘッダー

すべてのリクエストヘッダー (cookie を含む) を検査します。フィルターを適用して、すべてのヘッダーのサブセットを検査できます。

このオプションでは、次の仕様を指定します。

- 一致パターン – inspection のヘッダーのサブセットを取得するために使用するフィルター。 は、ヘッダーキーでこれらのパターン AWS WAF を探します。

  一致パターン設定は、次のいずれかになります。

  - [All] (すべて) – すべてのキーに一致します。すべてのヘッダーのルール検査基準を評価します。

- [Excluded headers] (除外されるヘッダー) – ここで指定した文字列のいずれとも一致しないキーを持つヘッダーのみを検査します。キーと一致する文字列は大文字と小文字に区別されません。一致は、リクエストヘッダーと一致ルールから先頭と末尾のスペースをトリミングした後に実行されます。
- [Included headers] (含まれるヘッダー) – ここで指定した文字列のいずれかに一致するキーを持つヘッダーのみを検査します。キーと一致する文字列は大文字と小文字に区別されません。一致は、リクエストヘッダーと一致ルールから先頭と末尾のスペースをトリミングした後に実行されます。

- 一致範囲 – がルール検査基準で検査 AWS WAF するヘッダーの部分。[キー]、[値]、または [すべて] を指定して、キーと値の両方で一致するものがあるかどうかを検査することができます。

  [すべて] では、キーで一致するもの、および値で一致するものを見つける必要はありません。キー、値、またはその両方で一致するものを見つける必要があります。キーと値で一致するものを見つけるようにするには、論理 AND ステートメントを使用して、キーを検査する一致ルールと値を検査する一致ルールの 2 つを組み合わせます。
- オーバーサイズ処理 – AWS WAF が検査 AWS WAF できるよりも大きいヘッダーデータを持つリクエストを処理する方法。 は、リクエストヘッダーの最初の 8 KB (8,192 バイト) まで、および最初の 200 個のヘッダーまで検査 AWS WAF できます。コンテンツは、最初の制限に達する AWS WAF まで検査できます。検査を続行するか、検査をスキップするかを選択できます。検査をスキップする場合、リクエストがルールに一致するとマークするか一致しないとマークするかを選択できます。オーバーサイズコンテンツの処理の詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。

ヘッダーの順序

が検査のために AWS WAF 受け取るウェブリクエストに表示される順序で、リクエストのヘッダー名のリストを含む文字列を検査します。 AWS WAF は文字列を生成し、それを検査のコンポーネントと一致するフィールドとして使用します。 は、文字列内のヘッダー名をコロンで AWS WAF 区切り、スペースを追加しません。例: `host:user-agent:accept:authorization:referer`。

このオプションでは、次の仕様を指定します。

- オーバーサイズ処理 – AWS WAF が検査 AWS WAF できる数以上のヘッダーデータを持つリクエストを処理する方法。 は、リクエストヘッダーの最初の 8 KB (8,192 バイト) と最初の 200 ヘッダーを検査 AWS WAF できます。コンテンツは、最初の制限に達する AWS WAF まで検査できます。使用可能なヘッダーの検査を続行するか、検査をスキップするかを選択できます。検査をスキップする場合、リクエストがルールに一致するか一致しないかをマークします。オーバーサイズ

コンテンツの処理の詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。

cookie

すべてのリクエスト cookie を検査します。フィルターを適用して、すべての cookie のサブセットを検査できます。

このオプションでは、次の仕様を指定します。

- [Match patterns] (一致パターン) – 検査用の cookie のサブセットを取得するために使用するフィルター。 AWS WAF は、cookie キーでこれらのパターンを検索します。

  一致パターン設定は、次のいずれかになります。

  - [All] (すべて) – すべてのキーに一致します。すべての cookie のルール検査基準を評価します。
  - [Excluded cookies] (除外される cookie) – ここで指定した文字列のいずれとも一致しないキーを持つ cookie のみを検査します。キーの文字列一致は大文字と小文字が区別され、完全に一致する必要があります。
  - [Included cookies] (含まれる cookie) – ここで指定した文字列のいずれかに一致するキーを持つ cookie のみを検査します。キーの文字列一致は大文字と小文字が区別され、完全に一致する必要があります。
- 一致範囲 – がルール検査基準で検査 AWS WAF する必要がある Cookie の部分。キーと値の両方に、[Keys] (キー)、[Values] (値)、または [All] (すべて) を指定できます。

  [すべて] では、キーで一致するもの、および値で一致するものを見つける必要はありません。キー、値、またはその両方で一致するものを見つける必要があります。キーと値で一致するものを見つけるようにするには、論理 AND ステートメントを使用して、キーを検査する一致ルールと値を検査する一致ルールの 2 つを組み合わせます。
- オーバーサイズ処理 – AWS WAF が検査 AWS WAF できるよりも大きい Cookie データを持つリクエストを処理する方法。 は、リクエスト Cookie の最初の 8 KB (8,192 バイト) と最初の 200 個の Cookie を検査 AWS WAF できます。コンテンツは、最初の制限に達する AWS WAF まで検査できます。検査を続行するか、検査をスキップするかを選択できます。検査をスキップする場合、リクエストがルールに一致するとマークするか一致しないとマークするかを選択できます。オーバーサイズコンテンツの処理の詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。

URI フラグメント

> **Note**
>
> フラグメント検査は、CloudFront ディストリビューションと Application Load Balancer でのみ利用可能です。

「#」記号の後に続く URL の一部を検査し、#section2 など、リソースに関する追加情報を提供します。詳細については、「Uniform Resource Identifier (URI): 一般的な構文」を参照してください。

このオプションでテキスト変換を使用しない場合、 AWS WAF は URI フラグメントを正規化せず、リクエストでクライアントから受信したとおりに検査します。テキスト変換については、「でのテキスト変換の使用 AWS WAF」を参照してください。

ルールステートメントの要件

このルールステートメントにはフォールバック動作を指定する必要があります。フォールバック動作は、URI にフラグメントがないか、関連するサービスが Application Load Balancer または CloudFront でない場合にウェブリクエスト AWS WAF に割り当てる一致ステータスです。一致を選択した場合、 はリクエストをルールステートメントに一致するものとして AWS WAF 処理し、ルールアクションをリクエストに適用します。一致しないことを選択した場合、 はリクエストをルールステートメントと一致しないものとして AWS WAF 扱います。

URI パス

URL 内でリソースを識別する部分 (`/images/daily-ad.jpg` など) が検査されます。詳細については、「Uniform Resource Identifier (URI): 一般的な構文」を参照してください。

このオプションでテキスト変換を使用しない場合、 AWS WAF は URI を正規化せず、リクエストでクライアントから受信したとおりに検査します。テキスト変換については、「でのテキスト変換の使用 AWS WAF」を参照してください。

JA3 フィンガープリント

リクエストの JA3 フィンガープリントを検査します。

> **Note**
>
> JA3 フィンガープリント検査は、Amazon CloudFront ディストリビューションと Application Load Balancer でのみ利用可能です。

JA3 フィンガープリントは、受信リクエストの TLS Client Hello から生成される 32 文字のハッシュです。このフィンガープリントは、クライアントの TLS 設定の一意の識別子として機能します。AWS WAF は、計算に十分な TLS Client Hello 情報を持つリクエストごとに、このフィンガープリントを計算してログに記録します。この情報は、ほとんどすべてのウェブリクエストに含まれています。

クライアントの JA3 フィンガープリントを取得する方法

クライアントリクエストの JA3 フィンガープリントは、保護パック (ウェブ ACL) ログからを取得できます。 AWS WAF がフィンガープリントを計算できる場合は、それをログに含めます。フィールドのログ記録については、「保護パック (ウェブ ACL) トラフィックのログフィールド」を参照してください。

ルールステートメントの要件

JA3 フィンガープリントは、指定した文字列と完全に一致するように設定されている文字列一致ステートメント内のみで検査することができます。同じ TLS 設定を持つ将来のリクエストと一致させるために、文字列一致ステートメントの仕様のログから JA3 フィンガープリント文字列を指定します。文字列一致ルールステートメントの詳細については、「文字列一致ルールステートメント」を参照してください。

このルールステートメントにはフォールバック動作を指定する必要があります。フォールバック動作は、 が JA3 フィンガープリントを計算できない場合にウェブリクエスト AWS WAF AWS WAF に割り当てる一致ステータスです。一致を選択した場合、 AWS WAF はリクエストをルールステートメントに一致するものとして処理し、ルールアクションをリクエストに適用します。一致しないことを選択した場合、 はリクエストをルールステートメントと一致しないものとして AWS WAF 扱います。

この一致オプションを使用するには、保護パック (ウェブ ACL) トラフィックをログに記録する必要があります。詳細については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。

JA4 フィンガープリント

リクエストの JA4 フィンガープリントを検査します。

> **Note**
>
> JA4 フィンガープリント検査は、Amazon CloudFront ディストリビューションと Application Load Balancer でのみ使用できます。

JA4 フィンガープリントは、受信リクエストの TLS Client Hello から派生した 36 文字のハッシュです。このフィンガープリントは、クライアントの TLS 設定の一意の識別子として機能します。JA4 フィンガープリントは JA3 フィンガープリントの拡張機能であり、一部のブラウザでは一意のフィンガープリントが少なくなります。 AWS WAF は、計算に十分な TLS Client Hello 情報を持つリクエストごとにこのフィンガープリントを計算してログに記録します。この情報は、ほとんどすべてのウェブリクエストに含まれています。

クライアントの JA4 フィンガープリントを取得する方法

クライアントリクエストの JA4 フィンガープリントは、保護パック (ウェブ ACL) ログからを取得できます。 AWS WAF がフィンガープリントを計算できる場合は、それをログに含めます。フィールドのログ記録については、「保護パック (ウェブ ACL) トラフィックのログフィールド」を参照してください。

ルールステートメントの要件

JA4 フィンガープリントは、指定した文字列と完全に一致するように設定された文字列一致ステートメント内でのみ検査できます。同じ TLS 設定を持つ将来のリクエストと一致するように、文字列一致ステートメント仕様のログから JA4 フィンガープリント文字列を指定します。文字列一致ルールステートメントの詳細については、「文字列一致ルールステートメント」を参照してください。

このルールステートメントにはフォールバック動作を指定する必要があります。フォールバック動作は、 が JA4 フィンガープリントを計算できない場合にウェブリクエスト AWS WAF AWS WAF に割り当てる一致ステータスです。一致を選択した場合、 AWS WAF はリクエストをルールステートメントに一致するものとして処理し、ルールアクションをリクエストに適用します。一致しないことを選択した場合、 はリクエストをルールステートメントと一致しないものとして AWS WAF 扱います。

この一致オプションを使用するには、保護パック (ウェブ ACL) トラフィックを口グに記録する必要があります。詳細については、「口グ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。

クエリ文字列

URL 内で ? 文字の後に続く部分 (ある場合) が検査されます。

> **Note**
>
> クロスサイトスクリプティングの一致ステートメントについては、[Query string] (クエリ文字列) ではなく、[All query parameters] (すべてのクエリパラメータ) を選択することをお勧

めします。[All query parameters] (すべてのクエリパラメータ) を選択すると、基本コストに 10 WCU が追加されます。

Single query parameter (単一クエリパラメータ)

クエリ文字列の一部として定義した単一のクエリパラメータを検査します。 AWS WAF は、指定したパラメータの値を検査します。

このオプションでは、[Query argument] (クエリ引数) も指定します。例えば、URL が `www.xyz.com?UserName=abc&SalesRegion=seattle` である場合は、クエリ引数として `UserName` または `SalesRegion` を指定できます。引数の名前は最大 30 文字です。名前では大文字と小文字が区別されないため、`UserName` と指定すると、 AWS WAF では `UserName` のすべてのバリエーション (`username`、`UsERName` など) と一致します。

クエリ文字列に、指定したクエリ引数の複数のインスタンスが含まれている場合、 OR は口ジックを使用して一致のすべての値を AWS WAF 検査します。例えば、URL `www.xyz.com?SalesRegion=boston&SalesRegion=seattle` では、 AWS WAF は、指定された名前を `boston` および `seattle` に対して評価します。いずれかが一致する場合、検査結果は一致となります。

All query parameters (すべてのクエリパラメータ)

リクエスト内のすべてのクエリパラメータが検査されます。これは単一のクエリパラメータコンポーネントの選択に似ていますが、クエリ文字列内のすべての引数の値を AWS WAF 検査します。例えば、URL が `www.xyz.com?UserName=abc&SalesRegion=seattle` である場合は、`UserName` または `SalesRegion` の値が検査基準に一致すると、 AWS WAF は一致をトリガーします。

このオプションを選択すると、基本コストに 10 WCU が追加されます。

[Body] (本文)

プレーンテキストとして評価されて、リクエストボディが検査されます。また、JSON コンテンツタイプを使用して、本文を JSON として評価することもできます。

リクエストボディは、リクエストの一部で、リクエストヘッダーの直後に続く部分です。これには、フォームからのデータなど、ウェブリクエストに必要な追加データが含まれます。

- コンソールで、[Content type] (コンテンツタイプ) の [Plain text] (プレーンテキスト) を選択して、[Request option] (リクエストオプション) の [Body] (本文) でこれを選択します。

- API では、ルールの `FieldToMatch` の指定で、リクエストボディをプレーンテキストとして検査するように `Body` を指定します。

Application Load Balancer および の場合 AWS AppSync、 はリクエストの本文の最初の 8 KB を検査 AWS WAF できます。CloudFront、API Gateway、Amazon Cognito、App Runner、Verified Access、Amazon Bedrock AgentCore Gateway では、デフォルトで最初の 16 KB を検査 AWS WAF でき、保護パック (ウェブ ACL) 設定で制限を最大 64 KB まで増やすことができます。詳細については、「でのボディ検査の管理に関する考慮事項 AWS WAF」を参照してください。

このコンポーネントタイプには、オーバーサイズの処理を指定する必要があります。オーバーサイズ処理は、 が検査 AWS WAF できるよりも大きい本文データを持つリクエストを が AWS WAF 処理する方法を定義します。検査を続行するか、検査をスキップするかを選択できます。検査をスキップする場合、リクエストがルールに一致するとマークするか一致しないとマークするかを選択できます。オーバーサイズコンテンツの処理の詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。

本文を解析された JSON として評価することもできます。これに関する詳細については、次のセクションを参照してください。

JSON 本文

JSON として評価されて、リクエストボディが検査されます。本文をプレーンテキストとして評価することもできます。

リクエストボディは、リクエストの一部で、リクエストヘッダーの直後に続く部分です。これには、フォームからのデータなど、ウェブリクエストに必要な追加データが含まれます。

- コンソールで、[Content type] (コンテンツタイプ) の [JSON] を選択して、[Request option] (リクエストオプション) の [Body] (本文) でこれを選択します。
- API で、ルールの `FieldToMatch` の指定で `JsonBody` を指定します。

Application Load Balancer および の場合 AWS AppSync、 はリクエストの本文の最初の 8 KB を検査 AWS WAF できます。CloudFront、API Gateway、Amazon Cognito、App Runner、Verified Access、Amazon Bedrock AgentCore Gateway では、デフォルトで最初の 16 KB を検査 AWS WAF でき、保護パック (ウェブ ACL) 設定で制限を最大 64 KB まで増やすことができます。詳細については、「でのボディ検査の管理に関する考慮事項 AWS WAF」を参照してください。

このコンポーネントタイプには、オーバーサイズの処理を指定する必要があります。オーバーサイズ処理は、 が検査 AWS WAF できるよりも大きい本文データを持つリクエストを が AWS WAF 処

理する方法を定義します。検査を続行するか、検査をスキップするかを選択できます。検査をスキップする場合、リクエストがルールに一致するとマークするか一致しないとマークするかを選択できます。オーバーサイズコンテンツの処理の詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。

このオプションを選択すると、一致ステートメントの基本コスト WCU が 2 倍になります。例えば、一致ステートメントのベースコストが JSON 解析なしで 5 WCU の場合、JSON 解析を使用すると、コストが 10 WCU に倍増します。

このオプションでは、以下のセクションで説明されている通り追加の仕様を提供します。

が JSON 本文検査 AWS WAF を処理する方法

はウェブリクエスト本文を JSON として AWS WAF 検査する場合、本文を解析し、検査用に JSON 要素を抽出するステップを実行します。 は、設定の選択に従ってこれらのステップ AWS WAF を実行します。

が AWS WAF 実行するステップを以下に示します。

1. 本文の内容を解析する – は、検査用に JSON 要素を抽出するためにウェブリクエスト本文の内容を AWS WAF 解析します。 は本文のコンテンツ全体を解析するために最善を AWS WAF 尽くしますが、コンテンツのさまざまなエラー状態で解析が失敗する可能性があります。例としては、無効な文字、重複するキー、切り捨て、ルートノードがオブジェクトまたは配列ではないコンテンツなどがあります。

   オプションの本文解析フォールバック動作によって AWS WAF 、JSON 本文を完全に解析できなかった場合の動作が決まります。

   - None (デフォルトの動作) - 解析エラーが発生した時点までのみコンテンツ AWS WAF を評価します。
   - 文字列として評価 - 本文をプレーンテキストとして検査します。 は、JSON 検査用に定義したテキスト変換と検査基準を本文テキスト文字列 AWS WAF に適用します。
   - 一致 - ウェブリクエストをルールステートメントに一致するものとして扱います。 はルールアクションをリクエスト AWS WAF に適用します。
   - 一致なし - ウェブリクエストをルールステートメントと一致しないものとして処理します。

> **Note**
>
> このフォールバック動作は、JSON 文字列の解析中に でエラー AWS WAF が発生した場合にのみトリガーされます。

解析では JSON が完全に検証されません

AWS WAF 解析では入力 JSON 文字列が完全に検証されないため、無効な JSON であっても解析が成功する可能性があります。

たとえば、 はエラーなしで次の無効な JSON を AWS WAF 解析します。

- カンマ不足: `{"key1":"value1""key2":"value2"}`
- コロン不足: `{"key1":"value1","key2""value2"}`
- 余分なコロン: `{"key1"::"value1","key2""value2"}`

このように、解析は成功したものの結果が完全に有効な JSON ではない場合、評価の後続のステップの結果が異なることがあります。抽出で一部の要素が欠落したり、ルール評価で予期しない結果が出たりする可能性があります。アプリケーションで受信した JSON を検証し、必要に応じて無効な JSON を処理することをお勧めします。

2. JSON 要素を抽出 – 設定に従って検査する JSON 要素のサブセット AWS WAF を識別します。
   - オプション JSON 一致スコープは、 が検査 AWS WAF する JSON 内の要素のタイプを指定します。

     キーと値の両方に、[Keys] (キー)、[Values] (値)、または [All] (すべて) を指定できます。

     [すべて] では、キーで一致するもの、および値で一致するものを見つける必要はありません。キー、値、またはその両方で一致するものを見つける必要があります。キーと値で一致するものを見つけるようにするには、論理 AND ステートメントを使用して、キーを検査する一致ルールと値を検査する一致ルールの 2 つを組み合わせます。
   - 検査するコンテンツオプションは、 AWS WAF 検査するサブセットに設定された要素をフィルタリングする方法を指定します。

     いずれかを指定する必要があります。
     - [完全な JSON コンテンツ] – すべての要素を評価します。

- [含まれる要素のみ] – パスが提供された JSON ポインタの基準に一致する要素のみを評価します。このオプションで JSON 内のすべてのパスを表示しないでください。代わりに [完全な JSON コンテンツ] を使用してください。

  JSON ポインタ構文の詳細については、インターネットエンジニアリングタスクフォース (IETF) ドキュメントの「JavaScript オブジェクト表記 (JSON) ポインタ」を参照してください。

  例えば、コンソールで次の内容を指定できます。

  ```
  /dogs/0/name
  /dogs/1/name
  ```

  API または CLI では、次を指定できます。

  ```
  "IncludedPaths": ["/dogs/0/name", "/dogs/1/name"]
  ```

例えば、[検査するコンテンツ] 設定が [含まれる要素のみ] で、含まれている要素設定が /a/b であるとします。

たとえば、次の JSON ボディの例の場合:

```
{
  "a":{
    "c":"d",
    "b":{
      "e":{
        "f":"g"
      }
    }
  }
}
```

が各 JSON 一致スコープ設定を検査 AWS WAF する要素セットを以下に示します。含まれている要素のパスの一部であるキー b は評価されないことを注意してください。

- すべて: e、f, および g。
- キー : e および f。
- 値: g。

3. JSON 要素セットの検査 – 抽出された JSON 要素に指定したテキスト変換 AWS WAF を適用し、結果の要素セットをルールステートメントの一致基準と照合します。これは、他のウェブリクエストコンポーネントに対するものと同じ変換および評価の動作です。抽出された JSON 要素のいずれかが一致する場合、そのウェブリクエストはルールに一致します。

で転送された IP アドレスを使用する AWS WAF

このセクションは、ウェブリクエストの IP アドレスを使用するルールステートメントに適用されます。デフォルトでは、 はウェブリクエストオリジンの IP アドレス AWS WAF を使用します。ただし、ウェブリクエストが 1 つ以上のプロキシまたはロードバランサーを通過する場合、ウェブリクエストの発信元には、クライアントの発信アドレスではなく、最後のプロキシのアドレスが含まれます。この場合、通常、発信元のクライアントアドレスは別の HTTP ヘッダーに転送されます。このヘッダーは通常 `X-Forwarded-For` (XFF) ですが、別のヘッダーにすることもできます。

IP アドレスを使用するルールステートメント

IP アドレスを使用するルールステートメントは次のとおりです。

- IP セット一致 - IP セットで定義されているアドレスと一致する IP アドレスを検査します。
- 地理的一致 - IP アドレスを使用して発信元の国と地域を特定し、それを国のリストと照合します。
- ASN 一致 - IP アドレスを使用して AS 番号 (ASN) を判別し、ASN のリストに対して ASN を照合します。
- レートベースのルールステートメントの使用 - IP アドレスでリクエストを集約して、個々の IP アドレスがリクエストを過度に高いレートで送信しないようにできます。IP アドレスの集約は、単独で使用することも、他の集約キーと組み合わせて使用することもできます。

ウェブリクエストのオリジンを使用する代わりに、 `X-Forwarded-For` ヘッダーから、または別の HTTP ヘッダーから、これらのルールステートメントのいずれかに転送された IP アドレスを使用する AWS WAF ように に指示できます。仕様を指定する方法の詳細については、個別のルールステートメントタイプのガイダンスを参照してください。

> **Note**
>
> ヘッダーがない場合、 はそのヘッダーを「一致なし」として使用するステートメント AWS WAF を評価します。NOT ステートメントを「一致なし」の結果で使用すると、 は評価を

「一致 AWS WAF 」に変換します。ヘッダーが見つからない場合、フォールバック動作はトリガーされません。無効なヘッダー値のみがトリガーされます。

フォールバック動作

転送された IP アドレスを使用する場合、リクエストに指定された位置に有効な IP アドレスがない場合に AWS WAF がウェブリクエストに割り当てる一致ステータスを指定します。

- MATCH - ウェブリクエストをルールステートメントに一致するものとして扱います。 はルールアクションをリクエスト AWS WAF に適用します。
- 一致なし - ウェブリクエストをルールステートメントと一致しないものとして処理します。

AWS WAF Bot Control で使用される IP アドレス

Bot Control マネージドルールグループは、IP アドレスを使用してボットを検証します AWS WAF。Bot Control を使用し、プロキシまたはロードバランサーを介してルーティングするボットを検証した場合は、カスタムルールを使用して明示的に許可する必要があります。例えば、転送された IP アドレスを使用して検証済みボットを検出および許可するカスタム IP セット一致ルールを設定できます。ルールを使用して、さまざまな方法でボット管理をカスタマイズできます。説明と例については、「AWS WAF ボットコントロール」を参照してください。

サポートされている CDNs背後にあるクライアント IP の検出

サードパーティーの CDN AWS WAF を介して に到着したリクエストの場合、Bot Control マネージドルールグループと Anti-DDoS マネージドルールグループは、Amazon CloudFront、Cloudflare、および" の IP 範囲から発生したトラフィックを自動的に認識します。ルールグループは、これらの CDNs のいずれかからのリクエストを検出すると、アップストリーム CDN の標準クライアント IP ヘッダー (たとえば、" の `Fastly-Client-IP` ヘッダー) から発信されるクライアント IP を透過的に使用します。これらの CDNs が正しく動作するように、これらのルールグループで転送された IP アドレスを設定する必要はありません。カスタム IP セット一致、地理的一致、ASN 一致、レートベースのルールなど、IP アドレスを使用する他のルールステートメントでも、CDN の IP ではなくアップストリームクライアント IP を評価する場合は、転送された IP 設定を指定する必要があります。

転送された IP アドレスの使用に関する一般的な考慮事項

転送された IP アドレスを使用する前に、次の一般的な注意事項に留意してください。

- ヘッダーは途中でプロキシによって変更でき、プロキシはヘッダーをさまざまな方法で処理することがあります。
- 攻撃者は、 AWS WAF 検査をバイパスしようとしてヘッダーの内容を変更する可能性があります。
- ヘッダー内の IP アドレスは、形式が正しくないか、無効である可能性があります。
- 指定したヘッダーは、リクエストにまったく存在しない可能性があります。

で転送された IP アドレスを使用する際の考慮事項 AWS WAF

次のリストでは、転送された IP アドレスを で使用するための要件と注意点について説明します AWS WAF。

- 単一のルールでは、転送された IP アドレス用に 1 つのヘッダーを指定できます。ヘッダーの仕様では、大文字と小文字は区別されません。
- レートベースのルールステートメントでは、ネストされたスコープステートメントは、転送された IP 設定を継承しません。転送された IP アドレスを使用する各ステートメントの設定を指定します。
- 地理的一致、ASN 一致、レートベースのルールの場合、 は ヘッダーの最初のアドレス AWS WAF を使用します。たとえば、ヘッダーに が含まれている場合、 は `10.1.1.1, 127.0.0.0, 10.10.10.10` AWS WAF を使用します。 `10.1.1.1`
- IP セットの一致では、ヘッダーの最初のアドレス、最後のアドレス、または任意のアドレスのいずれと照合するかを指定します。指定した場合、 はヘッダー内のすべてのアドレスに一致がないか、最大 10 個のアドレス AWS WAF を検査します。ヘッダーに 10 個を超えるアドレスが含まれている場合、 は最後の 10 個 AWS WAF を検査します。
- 複数のアドレスを含むヘッダーでは、アドレスの間にカンマ区切り文字を使用する必要があります。リクエストでカンマ以外の区切り文字が使用されている場合、 AWS WAF はヘッダーの IP アドレスの形式が正しくないとみなします。
- ヘッダー内の IP アドレスが不正な形式であるか、または無効である場合、 AWS WAF は、転送された IP 設定で指定したフォールバック動作に従って、ウェブリクエストをルールに一致するか一致しないかを指定します。
- 指定したヘッダーがリクエストに存在しない場合、 AWS WAF はリクエストにルールをまったく適用しません。つまり、 AWS WAF はルールアクションを適用せず、フォールバック動作も適用しません。
- IP アドレス用に転送された IP ヘッダーを使用するルールステートメントでは、ウェブリクエストの発信元によって報告された IP アドレスは使用されません。

で転送された IP アドレスを使用するためのベストプラクティス AWS WAF

転送された IP アドレスを使用する場合は、次のベストプラクティスを使用します。

- 転送された IP 設定を有効にする前に、リクエストヘッダーの可能な状態をすべて慎重に検討してください。目的の動作を実現するには、複数のルールを使用する必要がある場合があります。
- 複数の転送された IP ヘッダーを検査したり、ウェブリクエストの発信元と転送された IP ヘッダーを検査したりするには、IP アドレスのソースごとに 1 つのルールを使用します。
- 無効なヘッダーを持つウェブリクエストをブロックするには、ブロックするようにルールアクションを設定し、転送された IP 設定のフォールバック動作を一致するように設定します。

転送された IP アドレスの JSON の例

次の地理一致ステートメントは、発信元の国が US である IP が X-Forwarded-For ヘッダーに含まれている場合にのみ一致します。

```
{
  "Name": "XFFTestGeo",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "XFFTestGeo"
  },
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ],
      "ForwardedIPConfig": {
        "HeaderName": "x-forwarded-for",
        "FallbackBehavior": "MATCH"
      }
    }
  }
}
```

次のレートベースのルールは、X-Forwarded-For ヘッダーの最初の IP に基づいてリクエストを集約します。ルールは、ネストされた地理一致ステートメントに一致するリクエストのみをカウントし、地理一致ステートメントに一致するリクエストのみをブロックします。ネストされた地理一致ステートメントは、X-Forwarded-For ヘッダーを使用して、IP アドレスが US の発信元の国を示しているかどうかも判断します。示している場合、またはヘッダーが存在していても形式が間違っている場合、地理一致ステートメントは一致を返します。

```
{
  "Name": "XFFTestRateGeo",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "XFFTestRateGeo"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": "100",
      "AggregateKeyType": "FORWARDED_IP",
      "ScopeDownStatement": {
        "GeoMatchStatement": {
          "CountryCodes": [
            "US"
          ],
          "ForwardedIPConfig": {
            "HeaderName": "x-forwarded-for",
            "FallbackBehavior": "MATCH"
          }
        }
      },
      "ForwardedIPConfig": {
        "HeaderName": "x-forwarded-for",
        "FallbackBehavior": "MATCH"
      }
    }
  }
}
```

での HTTP/2 擬似ヘッダーの検査 AWS WAF

このセクションでは、 AWS WAF を使用して HTTP/2 擬似ヘッダーを検査する方法について説明します。

HTTP/2 トラフィックをサポートする保護された AWS リソースは、検査 AWS WAF のために HTTP/2 擬似ヘッダーを に転送しませんが、 AWS WAF 検査するウェブリクエストコンポーネントに擬似ヘッダーのコンテンツを提供します。

を使用して AWS WAF 、次の表に示す擬似ヘッダーのみを検査できます。

ウェブリクエストコンポーネントにマップされた HTTP/2 疑似ヘッダーの内容

HTTP/2 擬似ヘッダー	検査するウェブリクエストコンポーネント	ドキュメント
`:method`	HTTP メソッド	HTTP メソッド
`:authority`	`Host` ヘッダー	単一ヘッダー すべてのヘッダー
`:path` URI パス	URI パス	URI パス
`:path` クエリ	クエリ文字列	クエリ文字列 Single query parameter (単一クエリパラメータ) All query parameters (すべてのクエリパラメータ)

でのテキスト変換の使用 AWS WAF

このセクションでは、リクエストを検査する前に が適用 AWS WAF する変換を提供する方法について説明します。

パターンを探したり制約を設定したりするステートメントでは、リクエストを検査する前に が適用 AWS WAF する変換を指定できます。変換では、 AWS WAFをバイパスするために攻撃者が使用する異常なフォーマットの一部を削除するために、ウェブリクエストが再フォーマットされます。

これを JSON 本文リクエストコンポーネントの選択で使用する場合、 AWS WAF は JSON から検査する要素を解析および抽出した後、変換を適用します。詳細については、「JSON 本文」を参照してください。

複数の変換が指定された場合、 AWS WAF は変換の適用順序も設定します。

WCU - テキスト変換ごとには 10 個の WCU。

AWS WAF コンソールと API のドキュメントには、以下の場所におけるこれらの設定に関するガイダンスも記載されています。

- コンソールのルールビルダー - [Text transformation] (テキスト変換)。このオプションは、リクエストコンポーネントの使用時に選択できます。
- API ステートメントのコンテンツ – `TextTransformations`

テキスト変換のオプション

各変換リストには、コンソールと API の仕様が表示され、説明が続きます。

Base64 decode – `BASE64_DECODE`

AWS WAF は Base64-encoded文字列をデコードします。

Base64 decode extension – `BASE64_DECODE_EXT`

AWS WAF は Base64-encodedされた文字列をデコードしますが、無効な文字を無視する寛容な実装を使用します。

Command line – `CMD_LINE`

このオプションは、攻撃者がオペレーティングシステムのコマンドラインコマンドを挿入し、異常なフォーマットを使用して、コマンドの一部またはすべてを偽装する状況を緩和します。

このオプションを使用して、次の変換を実行します。

- 次の文字を削除します: `\ " ' ^`
- 次の文字の前にあるスペースを削除します: `/ (`
- 次の文字をスペースに置き換えます: `, ;`
- 複数のスペースを 1 つのスペースに置き換えます。

- 大文字 A-Z を小文字 a-z に変換します。

Command line Unix – CMD_LINE_UNIX

このオプションは、攻撃者が Unix または Linux オペレーティングシステムのコマンドラインコマンドを挿入し、異常な形式を使用してコマンドの一部またはすべてを偽装する状況を軽減します。

このオプションを使用して、次の変換を実行します。

- 次の文字を削除します: \ " '
- 次の文字をスペースに置き換えます。タブ \t (ASCII 9)、改行 \n (ASCII 10)、キャリッジリターン \r (ASCII 13)、垂直タブ \v (ASCII 11)、フォームフィード \f (ASCII 12)
- 複数のスペースを 1 つのスペースに置き換えます。
- 先頭と末尾のスペースを削除する
- 大文字 A-Z を小文字 a-z に変換します。

Command line Windows – CMD_LINE_WIN

このオプションは、攻撃者が Windows オペレーティングシステムのコマンドラインまたは PowerShell コマンドを挿入し、異常な形式を使用してコマンドの一部またはすべてを偽装する状況を軽減します。

このオプションを使用して、次の変換を実行します。

- 次の文字を削除します: " ' ^ `
- キャレットライン継続シーケンス、キャレットの後に改行、\nまたはキャリッジリターンと改行を 1 つの単位\r\nとして削除する
- 次の文字をスペースに置き換えます。タブ \t (ASCII 9)、改行 \n (ASCII 10)、キャリッジリターン \r (ASCII 13)、垂直タブ \v (ASCII 11)、フォームフィード \f (ASCII 12)
- 複数のスペースを 1 つのスペースに置き換えます。
- 先頭と末尾のスペースを削除する
- 大文字 A-Z を小文字 a-z に変換します。
- 連続するバックスラッシュを 1 つのバックスラッシュに置き換えます。シングルバックスラッシュは保持されるため、 c:\windows\system32\cmd.exeや UNC パスなどの Windows パスはそのまま残ります。

Compress whitespace – COMPRESS_WHITE_SPACE

AWS WAF は、複数のスペースを 1 つのスペースに置き換え、次の文字をスペース文字 (ASCII 32) に置き換えることで、空白を圧縮します。

- フォームフィード (ASCII 12)
- タブ (ASCII 9)
- 改行 (ASCII 10)
- キャリッジリターン (ASCII 13)
- 垂直タブ (ASCII 11)
- 改行なしスペース (ASCII 160)

CSS decode – `CSS_DECODE`

AWS WAF は、CSS 2.x エスケープルール を使用してエンコードされた文字をデコードしますsyndata.html#characters。この関数は、デコード処理で最大 2 バイトを使用するため、通常はエンコードされない CSS エンコーディングを使用してエンコードされた ASCII 文字を発見するのに役立ちます。また、バックスラッシュと 16 進数以外の文字の組み合わせである回避対策にも役立ちます。たとえば、`javascript` の `ja\vascript` を設定します。

Escape sequences decode – `ESCAPE_SEQ_DECODE`

AWS WAF は、次の ANSI C エスケープシーケンスをデコードします。`\a`、`\b`、、`\f`、`\n\r`、`\t`、`\v`、、`\\\?`、`\xHH`、 (16 進数)`\"`、 `\0OOO` (8 `\'`進数) 。有効でないエンコーディングは出力に残ります。

Hex decode – `HEX_DECODE`

AWS WAF は、16 進数の文字の文字列をバイナリにデコードします。

HTML entity decode – `HTML_ENTITY_DECODE`

AWS WAF は、16 進数形式`&#xhhhh;`または 10 進数形式で表される文字を対応する文字`&#nnnn;`に置き換えます。

AWS WAF は、次の HTML エンコード文字をエンコードされていない文字に置き換えます。このリストでは小文字の HTML エンコーディングを使用しますが、処理では大文字と小文字が区別されません。例えば、`&QuOt;` と `"` は同じように扱われます。

HTML でエンコードされた文字	以下に置き換えます
`"`	`"`
`&`	`&`
`<`	`<`

HTML でエンコードされた文字	以下に置き換えます
>	>
、または	改行なしスペース、10 進数 160
\n、10 進数 10
	\t、10 進数 9
{、または {	{
|, |, または		|
} 、、または }	}
!	!
#	#
$	$
&percent; 、、または %	%
'	\
(	(
)	)
* 、、または *	*
+	+
,	,
.	.
/	/
:	:

HTML でエンコードされた文字	以下に置き換えます
;	;
=	=
?	?
˜ 、、または &Diacriti calTilde;	~
−	-
[、、または [	[
\	\\
] 、、または]	]
&hat;	^
_ 、、または &underbar;	_
` 、、または &Diacriti calGrave;	`

JS decode – JS_DECODE

AWS WAF は JavaScript エスケープシーケンスをデコードします。\uHHHH コードが FF01-FF5E の全角 ASCII コード範囲内にある場合、高位バイトを使用して下位バイトが検出され、調整されます。そうでない場合は、下位バイトのみが使用され、上位バイトはゼロになり、情報が失われる可能性があります。

JS decode extended – JS_DECODE_EXT

AWS WAF は のような JavaScript エスケープシーケンスをデコードしますがJS_DECODE、Microsoft Windows ファイルパスが変更されないように寛容な実装を使用します。 はJS_DECODE次のようにJS_DECODE_EXT異なります。

- バックスラッシュを削除し\\、後続の文字を保持\"して\/、エスケープ \'、、、 をデコードします。
- バックスラッシュと後続の文字の両方を保持\vして、1 文字のエスケープ 、\t、、\a\b\f\n\r、、 を保持します。
- バックスラッシュと後続の文字の両方を保持して、他の認識されない\Cエスケープシーケンス (\dや など\w) を保持し、 \defaultや などの Windows ファイルパス\windowsが変更されないようにします。

Lowercase – LOWERCASE

AWS WAF は、大文字 (A ~ Z) を小文字 (a ~ z) に変換します。

MD5 – MD5

AWS WAF は、入力内のデータから MD5 ハッシュを計算します。計算されたハッシュは生のバイナリ形式です。

None – NONE

AWS WAF は、テキスト変換なしで、受信したウェブリクエストを検査します。

Normalize path – NORMALIZE_PATH

AWS WAF は、入力の先頭にない複数のスラッシュ、ディレクトリの自己参照、およびディレクトリのバックリファレンスを削除することで、入力文字列を正規化します。

Normalize path Windows – NORMALIZE_PATH_WIN

AWS WAF はバックスラッシュ文字をスラッシュに変換し、NORMALIZE_PATH変換を使用して結果の文字列を処理します。

Remove comments characters – REMOVE_COMMENTS_CHAR

AWS WAF は、入力から一般的なコメント文字 /*、*/、--、# を削除します。

Remove nulls – REMOVE_NULLS

AWS WAF は入力からすべてのNULLバイトを削除します。

Remove whitespace – REMOVE_WHITESPACE

AWS WAF は、入力からすべての空白文字を削除します。

Replace comments – REPLACE_COMMENTS

AWS WAF は、C 形式のコメント (/* ... */) の各出現を 1 つのスペースに置き換えます。コメントが複数連続しているときは、圧縮しません。コメントの終端がないときもスペース (ASCII 0x20) に置き換えられます。コメントの終端 (*/) のみがあるときは変更されません。

Replace nulls – REPLACE_NULLS

AWS WAF は、入力の各バイトをスペース文字 (ASCII NULL 0x20) に置き換えます。

SHA256 – SHA256

AWS WAF は、入力内のデータから SHA-256 ハッシュを計算します。計算されたハッシュは生のバイナリ形式です。

SQL hex decode – SQL_HEX_DECODE

AWS WAF は SQL 16 進数のデータをデコードします。たとえば、 は (0x414243) を () に AWS WAF デコードしますABC。

Trim – TRIM

AWS WAF は、入力の左側と右側の両方から空白を削除します。

Trim left – TRIM_LEFT

AWS WAF は入力の左側から空白を削除します。

Trim right – TRIM_RIGHT

AWS WAF は入力の右側から空白を削除します。

Uppercase – UPPERCASE

AWS WAF は、すべての小文字 (a ~ z) を大文字 (A ~ Z) に変換します。

URL decode – URL_DECODE

AWS WAF は URL エンコードされた値をデコードします。

URL decode Unicode – URL_DECODE_UNI

URL_DECODE と同様ですが、Microsoft 固有の %u エンコーディングをサポートしています。コードが FF01-FF5E の全角 ASCII コード範囲内にある場合、高位バイトを使用して下位バイトが検出され、調整されます。それ以外の場合は、下位バイトのみが使用され、高位バイトはゼロになります。

UTF8 to Unicode – UTF8_TO_UNICODE

AWS WAF は、すべての UTF-8 文字シーケンスを Unicode に変換します。これは、入力を正規化し、非英語の言語における誤検知 (偽陽性や偽陰性) を最小限に抑えるのに役立ちます。

での事前解析テキスト変換の使用 AWS WAF

事前解析テキスト変換は、未加工のクエリ文字列を正規化してから AWS WAF 、個々のクエリ引数に解析します。これらの変換は、パーサー差分攻撃と HTTP パラメータ汚染 (HPP) に対処し、攻撃者はクエリ文字列区切り文字をエンコードまたは操作して検査ルールをバイパスします。

事前解析テキスト変換は、リクエストコンポーネントが `SingleQueryArgument`または の場合にのみ使用できます`AllQueryArguments`。 AWS WAF は、標準テキスト変換の前に事前解析テキスト変換を適用します。ルールステートメントごとに最大 10 個の事前解析テキスト変換を指定できます。事前解析テキスト変換ごとに、ルールステートメントのコストに 10 WCUs が追加されます。

API では、ルールステートメントのオプション`PreParseTextTransformations`設定を使用して事前解析テキスト変換を設定します。

> **Note**
>
> 事前解析正規化が必要ない場合は、事前解析テキスト変換を指定しないでください。デフォルトの動作は で`NONE`、未加工のクエリ文字列は変更せずにパーサーに渡されます。

次の事前解析テキスト変換を使用できます。

None – `NONE`

AWS WAF は、事前解析テキスト変換なしで、受信したウェブリクエストを検査します。

URL decode – `URL_DECODE`

AWS WAF URL は解析前に raw クエリ文字列をデコードします。%HH シーケンスをデコードします (たとえば、%26 が & になり、%3D が = になります)。これにより、以前にエンコードされた新しいクエリパラメータの境界が公開される可能性があります。

URL decode Unicode – `URL_DECODE_UNI`

と同様ですが`URL_DECODE`、Unicode でエンコードされたシーケンス (%uHHH) もデコードします。コードが `FF01-FF5E` の全角 ASCII コード範囲内にある場合、高位バイトを使用して下位バ

イトが検出され、調整されます。それ以外の場合は、下位バイトのみが使用され、高位バイトはゼロになります。

Combine duplicate query arguments by comma – `COMBINE_DUPLICATE_QUERY_ARGS_BY_COMMA`

AWS WAF は、重複するクエリパラメータキーのすべての値を最初の出現位置の単一のカンマ区切り (0x2C) 文字列にマージし、後の重複を削除します。例えば、`a=1&b=2&a=3` は `a=1,3&b=2` になります。この変換は、バックエンドが重複するクエリパラメータを配列に結合する場合に使用します。これは .NET、API Gateway、Express.js で一般的です。 AWS WAF は結合された値を 1 つのユニットとして検査します。

Replace semicolons with ampersands – `REPLACE_SEMICOLONS_WITH_AMPERSANDS`

AWS WAF は、解析前に raw クエリ文字列内のすべてのセミコロン (0x3B) をアンパサンド (0x26) に置き換えます。 AWS API Gateway REST APIs を含む一部のウェブフレームワークとサービスは、セミコロンをアンパサンドに相当するクエリパラメータ区切り文字として扱います。この変換はクエリ文字列を正規化します。 AWS WAF その後、バックエンドと同じようにセミコロンで分割されるため、一貫したパラメータ解析が可能になります。

でのスコープダウンステートメントの使用 AWS WAF

このセクションでは、スコープダウンステートメントとその仕組みについて説明します。

スコープダウンステートメントは、マネージドルールグループステートメントまたはレートベースのステートメント内に追加できるネスト可能なルールステートメントで、包含ルールが評価するリクエストのセットを絞り込むことができます。包含ルールは、スコープダウンステートメントに最初に一致するリクエストのみを評価します。

- マネージドルールグループステートメント – マネージドルールグループステートメントにスコープダウンステートメントを追加すると、 はスコープダウンステートメントと一致しないリクエストをルールグループと一致しないものとして AWS WAF 評価します。スコープダウンステートメントに一致するリクエストのみがルールグループに対して評価されます。評価されたリクエスト数に基づいて料金が発生するマネージドルールグループでは、スコープダウンステートメントはコストを抑えるのに役立ちます。

  マネージドルールグループステートメントの詳細については、「でのマネージドルールグループステートメントの使用 AWS WAF」を参照してください。
- レートベースのルールステートメント – スコープダウンステートメントのレートを含まないレートベースのルールステートメントは、評価するすべてのリクエストのレートを制限します。特定の

カテゴリのリクエストのレートのみを制御する場合は、レートベースのルールにスコープダウンステートメントを追加します。例えば、特定の地理的エリアから送信されたリクエストのレートだけを追跡および制御するには、地理的照合ステートメントでその地理的エリアを指定することで、スコープダウンステートメントとしてレートベースのルールに追加できます。

レートベースのルールステートメントの詳細については、「でのレートベースのルールステートメントの使用 AWS WAF」を参照してください。

スコープダウンステートメントでは、任意のネスト可能なルールを使用できます。利用可能なステートメントについては、「での一致ルールステートメントの使用 AWS WAF」および「での論理ルールステートメントの使用 AWS WAF」を参照してください。スコープダウンステートメントの WCU は、その中で定義するルールステートメントに必要な WCU です。スコープダウンステートメントの使用に追加コストは発生しません

スコープダウンステートメントは、通常のルールでステートメントを使用する場合と同じ方法で設定できます。例えば、検査対象のウェブリクエストコンポーネントにテキスト変換を適用したり、IP アドレスとして使用するために転送された IP アドレスを指定したりできます。これらの設定はスコープダウンステートメントにのみ適用され、包含マネージドルールグループやレートベースのルールステートメントには継承されません。

例えば、スコープダウンステートメントのクエリ文字列にテキスト変換を適用すると、スコープダウンステートメントは変換を適用後、クエリ文字列を検査します。リクエストがスコープダウンステートメントの基準に一致する場合は、 AWS WAF スコープダウンステートメントの変換を行わずに、元の状態でウェブリクエストを包含ルールに渡します。スコープダウンステートメントを含むルールは、独自のテキスト変換を適用する場合がありますが、スコープダウンステートメントから継承されるものはありません。

スコープダウンステートメントを使用して、包含ルールステートメントのリクエスト検査設定を指定することはできません。スコープダウンステートメントを、包含ルールステートメントのウェブリクエストプリプロセッサとして使用することはできません。スコープダウンステートメントの唯一の役割は、どのリクエストを包含ルールステートメントに渡して検査するかを決定することです。

で再利用可能なエンティティを参照する AWS WAF

このセクションでは、 AWS WAFでの再利用可能なエンティティの仕組みについて説明します。

一部のルールでは、再利用可能なエンティティを使用し、ユーザー AWSまたは AWS Marketplace 販売者がウェブ ACLs の外部で管理します。再利用可能なエンティティが更新されると、 AWS

WAF は更新をルールに伝達します。たとえば、保護パック (ウェブ ACL) で AWS マネージドルールルールグループを使用する場合、 がルールグループ AWS を更新すると、 はウェブ ACL に変更を AWS 伝播して動作を更新します。ルールで IP セットステートメントを使用する場合、セットを更新すると、 はそれを参照するすべてのルールに変更 AWS WAF を伝達するため、これらのルールを使用する保護パック (ウェブ ACLs) は変更に合わせてup-to-date状態を維持します。

ルールステートメントで使用できる再利用可能なエンティティを次に示します。

- IP セット - 独自の IP セットを作成および管理します。コンソールでは、ナビゲーションペインからこれらにアクセスできます。IP セットの管理については、「の IP セットと正規表現パターンセット AWS WAF」を参照してください。
- 正規表現一致セット - 独自の正規表現一致セットを作成および管理します。コンソールでは、ナビゲーションペインからこれらにアクセスできます。正規表現パターンセットの管理については、「の IP セットと正規表現パターンセット AWS WAF」を参照してください。
- AWS マネージドルールルールグループ – これらのルールグループ AWS を管理します。コンソールでは、マネージドルールグループを保護パック (ウェブ ACL) に追加する際にこれらを使用できます。これらの詳細については、「AWS マネージドルールのルールグループリスト」を参照してください。
- AWS Marketplace マネージドルールグループ – AWS Marketplace 販売者はこれらのルールグループを管理し、それらをサブスクライブして使用できます。サブスクリプションを管理するには、コンソールのナビゲーションペインで [AWS Marketplace] を選択します。 AWS Marketplace マネージドルールグループは、マネージドルールグループを保護パック (ウェブ ACL) に追加すると一覧表示されます。まだサブスクライブしていないルールグループについては、そのページ AWS Marketplace にも へのリンクがあります。 AWS Marketplace 販売者マネージドルールグループの詳細については、「」を参照してくださいAWS Marketplace ルールグループ。
- 独自のルールグループ - マネージドルールグループでは利用できない動作が必要な場合は通常、独自のルールグループを管理します。コンソールでは、ナビゲーションペインからこれらにアクセスできます。詳細については、「独自のルールグループの管理」を参照してください。

参照先のセットまたはルールグループの削除

参照されるエンティティを削除すると、 AWS WAF は、そのエンティティが保護パック (ウェブ ACL) で現在使用されているかどうかを確認します。が使用中である AWS WAF と判断した場合、警告が表示されます。 AWS WAF はほとんどの場合、エンティティが保護パック (ウェブ ACL) によって参照されているかどうかを判断できます。ただし、まれに判別できないことがあります。削除するエンティティが使用中でないことを確認する必要がある場合は、削除する前にウェブ ACL でエンティティを確認してください。

での一致ルールステートメントの使用 AWS WAF

このセクションでは、一致ステートメントとは何か、またその仕組みについて説明します。

一致ステートメントは、ウェブリクエストまたはその送信元を、指定された基準と比較します。このタイプの多くのステートメントでは、 はコンテンツのマッチングリクエストの特定のコンポーネント AWS WAF を比較します。

一致ステートメントはネスト可能です。これらのステートメントはいずれも論理ルールステートメント内にネストできる他、スコープダウンステートメントで使用できます。倫理ルールステートメントの詳細については、「での論理ルールステートメントの使用 AWS WAF」を参照してください。スコープダウンステートメントの詳細については、「でのスコープダウンステートメントの使用 AWS WAF」を参照してください。

この表では、ルールに追加できる標準の一致ステートメントについて説明し、それぞれの保護パック (ウェブ ACL) キャパシティーユニット (WCU) 使用量を計算するためのガイドラインを提供します。WCU の詳細については、「のウェブ ACL キャパシティユニット (WCUs) AWS WAF」を参照してください。

一致ステートメント	説明	WCU
地理的一致	リクエストの送信元の国を検査し、その国および地域のラベルを適用します。	1
ASN 一致	リクエストを IP アドレスおよびアドレス範囲に関連付けられた ASN と照合します。	1
IP セット一致	リクエストを一連の IP アドレスおよびアドレス範囲と照合します。	ほとんどの場合 1。転送された IP アドレスを持つヘッダーを使用するようにステートメントを設定し、Any のヘッダー内の位置を指定すると、WCU が 4 増えます。
ラベル一致ルールステートメント	同じ保護パック (ウェブ ACL) 内の他のルールによって追加	1

一致ステートメント	説明	WCU
	されたラベルのリクエストを検査します。	
正規表現一致ルールステートメント	正規表現パターンを指定されたリクエストコンポーネントと比較します。	3 (基本コストとして)。 [All query parameters] (すべてのクエリパラメータ) のリクエストコンポーネントを使用する場合、10 WCU を追加します。[JSON body] (JSON 本文) のリクエストコンポーネントを使用する場合、基本コストの WCU を倍増させます。適用する各テキスト変換について、10 WCU を追加します。
正規表現パターンセット	正規表現パターンを指定されたリクエストコンポーネントと比較します。	パターンセットあたり 25 (基本コストとして)。 [All query parameters] (すべてのクエリパラメータ) のリクエストコンポーネントを使用する場合、10 WCU を追加します。[JSON body] (JSON 本文) のリクエストコンポーネントを使用する場合、基本コストの WCU を倍増させます。適用する各テキスト変換について、10 WCU を追加します。

一致ステートメント	説明	WCU
サイズ制約	指定されたリクエストコンポーネントに対してサイズ制約をチェックします。	1 (基本コストとして)。 [All query parameters] (すべてのクエリパラメータ) のリクエストコンポーネントを使用する場合、10 WCU を追加します。[JSON body] (JSON 本文) のリクエストコンポーネントを使用する場合、基本コストの WCU を倍増させます。適用する各テキスト変換について、10 WCU を追加します。
SQLi 攻撃	指定されたリクエストコンポーネント内の悪意のある SQL コードを検査します。	20 (基本コストとして)。 [All query parameters] (すべてのクエリパラメータ) のリクエストコンポーネントを使用する場合、10 WCU を追加します。[JSON body] (JSON 本文) のリクエストコンポーネントを使用する場合、基本コストの WCU を倍増させます。適用する各テキスト変換について、10 WCU を追加します。

一致ステートメント	説明	WCU
文字列一致	指定されたリクエストコンポーネントと文字列を比較します。	基本コストは、文字列の一致のタイプによって異なり、1 ～ 10 の範囲です。 [All query parameters] (すべてのクエリパラメータ) のリクエストコンポーネントを使用する場合、10 WCU を追加します。[JSON body] (JSON 本文) のリクエストコンポーネントを使用する場合、基本コストの WCU を倍増させます。適用する各テキスト変換について、10 WCU を追加します。
XSS スクリプティング攻撃	指定されたリクエストコンポーネントでのクロスサイトスクリプティング攻撃を検査します。	40 (基本コストとして)。 [All query parameters] (すべてのクエリパラメータ) のリクエストコンポーネントを使用する場合、10 WCU を追加します。[JSON body] (JSON 本文) のリクエストコンポーネントを使用する場合、基本コストの WCU を倍増させます。適用する各テキスト変換について、10 WCU を追加します。

地理的一致ルールステートメント

このセクションでは、地理的な一致ステートメントとは何か、またその仕組みについて説明します。

地理的または地理照合ステートメントを使用して、発信元の国や地域に基づいてウェブリクエストを管理します。地理的照合ステートメントは、ウェブリクエストに発信国や発信地域を示すラベルを追

加します。これらのラベルは、ステートメントの条件がリクエストと一致するかどうかに関係なく追加されます。また、地理的照合ステートメントは、リクエストの発信国に対する一致も実行します。

地理的一致ステートメントの使用方法

地理的一致ステートメントは、次のような国や地域のマッチングに使用できます。

- 国 — 地理的一致ルールを単独で使用し、発信国のみに基づいてリクエストを管理できます。ルールステートメントは国コードに対する一致を実行します。また、発信元のラベルに一致するラベル一致ルールが適用されている地域的一致ルールに従うこともできます。

  > **Note**
  >
  > 香港からのトラフィックをフィルタリングするには、地理一致ステートメントで ISO 3166-1 alpha-2 国コード HK を使用します。

- 地域 — 地理的一致ルールに続いてラベル一致ルールを使用し、発信地域に基づいてリクエストを管理します。地理的一致ルールだけを使用して地域コードとの一致を実行することはできません。

ラベルマッチルールの使用方法については、「ラベル一致ルールステートメント」および「でのウェブリクエストのラベル付け AWS WAF」を参照してください。

地理的一致ステートメントのしくみ

geo 一致ステートメントでは、 は各ウェブリクエストを次のように AWS WAF 管理します。

1. リクエストの国とリージョンコードを決定します。IP アドレスに基づいてリクエストの国とリージョン AWS WAF を決定します。デフォルトでは、 はウェブリクエストのオリジンの IP アドレス AWS WAF を使用します。ルールステートメント設定で転送された IP 設定を有効にするX-Forwarded-Forことで、 などの代替リクエストヘッダーから IP アドレスを使用する AWS WAF ように に指示できます。

   AWS WAF は、MaxMind GeoIP データベースを使用してリクエストの場所を決定します。MaxMind は、国レベルでの非常に高精度なデータを報告しますが、精度は国や IP の種類などの要因によって異なります。MaxMind の詳細については、「MaxMind IP Geolocation」を参照してください。GeoIP データのいずれかが正しくないと思われる場合は、MaxMind Correct GeoIP2 Data で Maxmind に修正リクエストを送信できます。

   AWS WAF は、国際標準化機構 (ISO) 3166 規格の alpha-2 の国と地域のコードを使用します。コードは次の場所にあります。

- ISO ウェブサイトでは、「ISO Online Browsing Platform (OBP)」(ISO オンラインブラウジングプラットフォーム (OBP)) で国コードを検索できます。
- ウィキペディアでは、国コードは「ISO 3166-2」に一覧表示されています。

  国の地域コードは https://en.wikipedia.org/wiki/ISO_3166-2:*<ISO country code>* の URL に一覧表示されています。たとえば、米国の地域は「ISO 3166-2:US」にあり、ウクライナの地域は「ISO 3166-2:UA」にあります。

2. リクエストに追加する国ラベルおよび地域ラベルを決定します — ラベルは、地理一致ステートメントが発信元 IP 設定を使用するか、転送された IP 設定を使用するかを示します。
   - 発信元 IP

     国ラベルは awswaf:clientip:geo:country:*<ISO country code>* です。米国の例は awswaf:clientip:geo:country:US です。

     地域ラベルは awswaf:clientip:geo:region:*<ISO country code>*-*<ISO region code>* です。米国のオレゴン州の例は awswaf:clientip:geo:region:US-OR です。
   - 転送された IP

     国ラベルは awswaf:forwardedip:geo:country:*<ISO country code>* です。米国の例は awswaf:forwardedip:geo:country:US です。

     地域ラベルは awswaf:forwardedip:geo:region:*<ISO country code>*-*<ISO region code>* です。米国のオレゴン州の例は awswaf:forwardedip:geo:region:US-OR です。

   リクエストが指定した IP アドレスの国または地域コードがない場合、 AWS WAF はラベル内で値の代わりに XX を使用します。たとえば、次のラベルは国コードがないクライアント IP 用です。awswaf:clientip:geo:country:XX および次のラベルは、国が米国であるが地域コードがない転送先 IP 用です。awswaf:forwardedip:geo:region:US-XX。
3. リクエストの国コードをルール基準に参照して評価

地理一致ステートメントは、一致するものを見つけるかどうかにかかわらず、検査するすべてのリクエストに国と地域のラベルを追加します。

> **Note**
>
> AWS WAF は、ルールのウェブリクエスト評価の最後にラベルを追加します。そのため、地理的一致ステートメントのラベルに対して使用するラベル一致は、地理的一致ステートメントを含むルールとは別のルールで定義する必要があります。

地域値のみを調べる場合、Count アクションと単一の国コード一致で地域的一致ルールを記述し、その後に地域ラベルのラベル一致ルールを作成することができます。この方法でも、地域一致ルールを評価するには国コードを入力する必要があります。サイトへのトラフィック元になる可能性が非常に低い国を指定することで、ログ記録およびカウントメトリクスを減らすことができます。

CloudFront ディストリビューションおよび CloudFront 地域制限機能

CloudFront ディストリビューションでは、CloudFront の地域制限機能を使用する場合、ブロックされたリクエストは AWS WAFに転送されないことに注意してください。許可されたリクエストは に転送されます AWS WAF。地域と指定できるその他の基準に基づいてリクエストをブロックする場合は AWS WAF、 AWS WAF 地理的一致ステートメントを使用し、CloudFront の地理的制限機能を使用しないでください。

ルールステートメントの特性

ネスト可能 - このステートメントタイプはネスト可能です。

WCU - 1 つの WCU。

設定 – このステートメントは次の設定を使用します。

- 国コード – 地理一致のために比較する国コードの配列。これらは、ISO 3166 国際規格の alpha-2 の国 ISO コード (たとえば、`["US","CN"]` など) を基準とした 2 文字の国コードである必要があります。
- (オプション) 転送された IP 設定 – デフォルトでは、 はウェブリクエストオリジンの IP アドレス AWS WAF を使用して、オリジンの国を決定します。または、 `X-Forwarded-For` などの HTTP ヘッダーで転送された IP を使用するようにルールを設定できます。 は、ヘッダーの最初の IP アドレス AWS WAF を使用します。この設定では、ヘッダーに不正な形式の IP アドレスを持つウェブリクエストに適用するフォールバック動作も指定します。フォールバック動作は、リクエストの一致結果を、一致または不一致のいずれにするかを設定します。詳細については、「転送された IP アドレスの使用」を参照してください。

このルールステートメントの場所

- コンソールのルールビルダー - [Request option] (リクエストオプション) で [Originates from a country in] (次の国からの送信) を選択します。
- API – 「GeoMatchStatement」

例

地域一致ステートメントを使用して、特定の国または地域からのリクエストを管理できます。たとえば、特定の国からのリクエストをブロックしても、それらの国に属する一連の IP アドレスからのリクエストを許可するには、Block に設定されたアクションと次のネストされたステートメント (次の疑似コードで表示) を含めたルール作成できます。

- AND ステートメント
  - ブロックする国をリストした 地理一致ステートメント
  - NOT ステートメント
    - 許可する IP アドレスを指定する IP セットステートメント

または、特定の国の一部地域をブロックしても、それらの国における他の地域からのリクエストを許可するには、まずアクションセットを持った地理一致リールを Count に定義できます。その後、追加された地理一致ラベルと照合し、必要に応じてリクエストを処理するラベルマッチルールを定義します。

次の擬似コードは、このアプローチの例について説明しています。

1. 地理一致ステートメントはブロックする地域がある国をリストしますが、アクションを Count に設定された状態で実行します。これにより、マッチステータスに関係なくすべてのウェブリクエストにラベルが付けられ、対象国のカウントメトリクスも表示されます。
2. Block アクションを含む AND ステートメント
   - ブロックする国のラベルを指定するラベル一致ステートメント
   - NOT ステートメント
     - 許可する国の地域のラベルを指定するラベル一致ステートメント

次の JSON リストは、前述の擬似コードで説明した 2 つのルールの実装を示しています。これらのルールは、オレゴン州とワシントン州からのトラフィックを除く米国からのトラフィックをすべてブロックします。地理一致ステートメントは、検査するすべてのリクエストに国と地域のラベルを追加

します。ラベル一致ルールは地理一致ルールの後に実行されるため、地理一致ルールが追加したばかりの国や地域のラベルと照合できます。地理一致ステートメントは転送された IP アドレスを使用するため、ラベル一致は転送された IP ラベルも指定します。

```
{
   "Name": "geoMatchForLabels",
   "Priority": 10,
   "Statement": {
     "GeoMatchStatement": {
       "CountryCodes": [
         "US"
       ],
       "ForwardedIPConfig": {
           "HeaderName": "X-Forwarded-For",
           "FallbackBehavior": "MATCH"
       }
     }
   },
   "Action": {
     "Count": {}
   },
   "VisibilityConfig": {
     "SampledRequestsEnabled": true,
     "CloudWatchMetricsEnabled": true,
     "MetricName": "geoMatchForLabels"
   }
},
{
   "Name": "blockUSButNotOROrWA",
   "Priority": 11,
   "Statement": {
     "AndStatement": {
       "Statements": [
         {
           "LabelMatchStatement": {
             "Scope": "LABEL",
             "Key": "awswaf:forwardedip:geo:country:US"
           }
         },
         {
           "NotStatement": {
             "Statement": {
                "OrStatement": {
```

```
                "Statements": [
                  {
                     "LabelMatchStatement": {
                       "Scope": "LABEL",
                       "Key": "awswaf:forwardedip:geo:region:US-OR"
                     }
                  },
                  {
                     "LabelMatchStatement": {
                       "Scope": "LABEL",
                       "Key": "awswaf:forwardedip:geo:region:US-WA"
                     }
                  }
                ]
              }
            }
          }
        }
      ]
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "blockUSButNotOROrWA"
  }
}
```

別の例として、地理一致とレートベースのルールを組み合わせて、特定の国または地域のユーザーのリソースに優先順位を付けることができます。ユーザーを区別するために使用する地理一致またはラベル一致のステートメントごとに、異なるレートベースのステートメントを作成します。優先させる国または地域のユーザーのレート制限をより高く設定し、他のユーザーのレート制限をより低く設定します。

次の JSON リストは、米国からのトラフィック量を制限する地理一致ルールの次にレートベースのルールを示しています。このルールにより、オレゴン州からのトラフィックは、同国の他の地域からのトラフィックよりも高いレートで許可されます。

```
{
```

```
  "Name": "geoMatchForLabels",
  "Priority": 190,
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ]
    }
  },
  "Action": {
    "Count": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "geoMatchForLabels"
  }
},
{
  "Name": "rateLimitOregon",
  "Priority": 195,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 3000,
      "AggregateKeyType": "IP",
      "ScopeDownStatement": {
        "LabelMatchStatement": {
          "Scope": "LABEL",
          "Key": "awswaf:clientip:geo:region:US-OR"
        }
      }
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "rateLimitOregon"
  }
},
{
  "Name": "rateLimitUSNotOR",
```

```
  "Priority": 200,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "AggregateKeyType": "IP",
      "ScopeDownStatement": {
        "AndStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:clientip:geo:country:US"
              }
            },
            {
              "NotStatement": {
                "Statement": {
                  "LabelMatchStatement": {
                    "Scope": "LABEL",
                    "Key": "awswaf:clientip:geo:region:US-OR"
                  }
                }
              }
            }
          ]
        }
      }
    },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "rateLimitUSNotOR"
  }
}
```

IP セット一致ルールステートメント

このセクションでは、IP セット一致ステートメントとは何か、またその仕組みについて説明します。

IP セット一致ステートメントは、一連の IP アドレスおよびアドレス範囲に対してウェブリクエストの IP アドレスを検査します。これを使用して、リクエストの送信元の IP アドレスに基づいてウェブリクエストを許可またはブロックします。デフォルトでは、 AWS WAF はウェブリクエストの発信元からの IP アドレスを使用しますが、代わりに `X-Forwarded-For` などの HTTP ヘッダーを使用するようにルールを設定できます。

AWS WAF は、 を除くすべての IPv4 および IPv6 CIDR 範囲をサポートします`/0`。CIDR 表記の詳細については、Wikipedia の「Classless Inter-Domain Routing」(クラスレスドメイン間ルーティング) を参照してください。IP セットには、チェック対象として最大 10,000 個の IP アドレスまたは IP アドレス範囲を保持できます。

> **Note**
>
> 各 IP セット一致ルールは IP セットを参照します。このセットは、ルールとは無関係に作成し、維持します。複数のルールで 1 つの IP セットを使用できます。参照されるセットを更新すると、 はそれを参照するすべてのルール AWS WAF を自動的に更新します。
> IP セットの作成および管理については、「での IP セットの作成と管理 AWS WAF」を参照してください。

ルールグループまたは保護パック (ウェブ ACL) でルールを追加または更新する場合は、[IP set] (IP セット) オプションを選択し、使用する IP セットの名前を選択します。

ルールステートメントの特性

ネスト可能 - このステートメントタイプはネスト可能です。

WCU- ほとんどの場合 1 WCU。転送された IP アドレスを使用するようにステートメントを設定し、ANY の位置を指定すると、WCU の使用量が 4 増えます。

このステートメントには、次の設定を使用します。

- IP セットの指定 - 使用する IP セットをリストから選択するか、新しい IP セットを作成します。
- (オプション) 転送された IP 設定 – リクエストの発信元の代わりに使用する代替の転送された IP ヘッダー名。ヘッダーの最初のアドレス、最後のアドレス、または任意のアドレスを照合するかどうかを指定します。指定したヘッダーに不正な形式の IP アドレスを持つウェブリクエストに適用するフォールバック動作も指定します。フォールバック動作は、リクエストの一致結果を、一致または不一致のいずれにするかを設定します。詳細については、「転送された IP アドレスの使用」を参照してください。

このルールステートメントの場所

このルールステートメントの場所

- コンソールのルールビルダー - [Request option] (リクエストオプション) で [Originates from an IP address in] (次の IP アドレスからの送信) を選択します。
- コンソールの [Add my own rules and rule groups] (独自のルールとルールグループの追加) ページ - [IP set] (IP セット) オプションを選択します。
- API – 「IPSetReferenceStatement」

AS 番号 (ASN) 一致ルールステートメント

の ASN 一致ルールステートメント AWS WAF を使用すると、リクエストの IP アドレスに関連付けられた自律システム番号 (ASN) に基づいてウェブトラフィックを検査できます。ASN は、インターネットサービスプロバイダー、企業、大学、政府機関などの組織が管理する大規模なインターネットネットワークに割り当てられる一意の識別子です。ASN 一致ステートメントを使用すると、個々の IP アドレスを管理することなく、特定のネットワーク組織からのトラフィックを許可またはブロックできます。このアプローチでは、ASN は IP 範囲より変化の頻度が低くなるため、IP ベースのルールと比較して、より安定して効率的にアクセスを制御できます。

ASN マッチングは、既知の問題のあるネットワークからのトラフィックをブロックしたり、信頼できるパートナーネットワークからのアクセスのみを許可したりするなどのシナリオで特に役立ちます。ASN 一致ステートメントは、オプションの転送された IP 設定を使用してクライアント IP アドレスを柔軟に判断できるため、コンテンツ配信ネットワーク (CDN) やリバースプロキシを使用するネットワーク設定など、さまざまなネットワーク設定との互換性を確保します。

> **Note**
>
> ASN マッチングは、標準の認証と認可のコントロールを補完しますが、置き換えるものではありません。アプリケーション内のすべてのリクエストの ID を検証するために、IAM などの認証および認可メカニズムを実装することをお勧めします。

ASN 一致ステートメントの仕組み

AWS WAF は、IP アドレスに基づいてリクエストの ASN を決定します。デフォルトでは、 はウェブリクエストのオリジンの IP アドレス AWS WAF を使用します。ルールステートメント設定で転送

された IP 設定を有効にするX-Forwarded-Forことで、 などの代替リクエストヘッダーから IP アドレスを使用する AWS WAF ように を設定できます。

ASN 一致ステートメントは、リクエストの ASN をルールで指定された ASN のリストと比較します。ASN がリスト内の ASN と一致する場合、ステートメントは true と評価され、関連付けられたルールアクションが適用されます。

マッピングされていない ASN の処理

が有効な IP アドレスの ASN を決定 AWS WAF できない場合、ASN 0 が割り当てられます。これらのケースを明示的に処理するために、ルールに ASN 0 を含めることができます。

無効な IP アドレスのフォールバック動作

転送された IP アドレスを使用するように ASN 一致ステートメントを設定する場合、指定されたヘッダーに無効または欠落している IP アドレスを持つリクエストに対して、一致 または 一致なしのフォールバック動作を指定できます。

ルールステートメントの特性

ネスト可能 - このステートメントタイプはネスト可能です。

WCU - 1 つの WCU

このステートメントには、次の設定を使用します。

- ASN リスト – ASN 一致と比較する ASN 番号の配列。有効な値の範囲は 0 ~ 4294967295 です。ルールごとに最大 100 個の ASN を指定できます。
- (オプション) 転送された IP 設定 – デフォルトでは、 はウェブリクエストオリジンの IP アドレス AWS WAF を使用して ASN を決定します。または、代わりに X-Forwarded-For などの HTTP ヘッダーで転送された IP を使用するようにルールを設定することもできます。ヘッダーの最初のアドレス、最後のアドレス、または任意のアドレスを使用するかどうかを指定します。この設定では、ヘッダーに不正な形式の IP アドレスを持つウェブリクエストに適用するフォールバック動作も指定します。フォールバック動作は、リクエストの一致結果を、一致または不一致のいずれにするかを設定します。詳細については、「転送した IP アドレスの使用」を参照してください。

このルールステートメントの場所

- コンソールの ルールビルダー - [リクエストオプション] では、[次の ASN からの送信] を選択します。
- API – AsnMatchStatement

例

この例では、X-Forwarded-For ヘッダーから派生した 2 つの特定の ASN からのリクエストをブロックします。ヘッダーの IP アドレスの形式が正しくない場合、設定されたフォールバック動作は NO_MATCH です。

```
{
  "Action": {
    "Block": {}
  },
  "Name": "AsnMatchStatementRule",
  "Priority": 1,
  "Statement": {
    "AsnMatchStatement": {
      "AsnList": [64496, 64500]
    },
    "ForwardedIPConfig": {
      "FallbackBehavior": "NO_MATCH",
      "HeaderName": "X-Forwarded-For"
    }
  },
  "VisibilityConfig": {
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AsnMatchRuleMetrics",
    "SampledRequestsEnabled": true
  }
},
"VisibilityConfig": {
  "CloudWatchMetricsEnabled": true,
  "MetricName": "WebAclMetrics",
  "SampledRequestsEnabled": true
}
}
```

ラベル一致ルールステートメント

このセクションでは、ラベル一致ステートメントとは何か、またその仕組みについて説明します。

ラベル一致ステートメントは、ウェブリクエストにあるラベルを文字列指定に照らして検査します。検査用のルールで使用できるラベルは、同じ保護パック (ウェブ ACL) 評価内の他のルールによってウェブリクエストに既に追加されているラベルです。

ラベルは保護パック (ウェブ ACL) 評価の外では保持されませんが、CloudWatch のラベルメトリクスにアクセスでき、 AWS WAF コンソールで任意の保護パック (ウェブ ACL) のラベル情報の概要を確認できます。詳細については、「ラベルメトリクスとディメンション」および「AWS WAF 保護のモニタリングと調整」を参照してください。ログにはラベルも表示されます。詳細については、「保護パック (ウェブ ACL) トラフィックのログフィールド」を参照してください。

> **Note**
>
> ラベル一致ステートメントは、保護パック (ウェブ ACL) で以前に評価されたルールのラベルのみを表示できます。が保護パック (ウェブ ACL) 内のルールとルールグループ AWS WAF を評価する方法については、「」を参照してくださいルールの優先度を設定する。

ラベルの追加と一致の詳細については、「でのウェブリクエストのラベル付け AWS WAF」を参照してください。

ルールステートメントの特性

ネスト可能 - このステートメントタイプはネスト可能です。

WCU - 1 つの WCU

このステートメントには、次の設定を使用します。

- [Match scope] (一致範囲) – これを [Label] (ラベル) に設定して、ラベル名と、ならびにオプションで、先行する名前空間およびプレフィックスと照合します。これを [Namespace] (名前空間) に設定して、名前空間の指定の一部または全部、およびオプションで、先行するプレフィックスと照合します。
- [Key] (キー) – 照合する文字列。名前空間一致の範囲を指定する場合、これは、名前空間と、オプションでプレフィックスのみを指定する必要があり、末尾にコロンを付けます。ラベル一致の範囲を指定する場合、これはラベル名を含む必要があり、オプションで前述の名前空間とプレフィックスを含めることができます。

これらの設定の詳細については、「AWS WAF ラベルに一致する ルール」および「AWS WAF ラベル一致の例」を参照してください。

このルールステートメントの場所

- コンソールのルールビルダー - [Request option] (リクエストオプション) で [Has label] (ラベルあり) を選択します。

- API – 「LabelMatchStatement」

正規表現一致ルールステートメント

このセクションでは、正規表現一致ステートメントとは何か、またその仕組みについて説明します。

正規表現一致ステートメントは、リクエストコンポーネントを単一の正規表現 (正規表現) と照合 AWS WAF するように に指示します。リクエストコンポーネントが指定した正規表現と一致する場合、ウェブリクエストはステートメントと一致します。

このステートメントタイプは、数理論理を使用して一致基準を組み合わせることを希望する状況において、正規表現パターンセット一致ルールステートメント に代わる優れた方法です。例えば、リクエストコンポーネントを一部の正規表現パターンと照合し、他の正規表現パターンと照合しないようにする場合は、AND ルールステートメント と NOT ルールステートメント を使用して正規表現一致ステートメントを組み合わせることができます。

AWS WAF は、いくつかの例外`libpcre`を除いて、PCRE ライブラリで使用されるパターン構文をサポートします。ライブラリは、「PCRE - Perl Compatible Regular Expressions」で文書化されています。 AWS WAF サポートの詳細については、「」を参照してくださいでサポートされている正規表現構文 AWS WAF。

ルールステートメントの特性

ネスト可能 - このステートメントタイプはネスト可能です。

WCU- 3 WCU (基本コストとして)。[All query parameters] (すべてのクエリパラメータ) のリクエストコンポーネントを使用する場合、10 WCU を追加します。[JSON body] (JSON 本文) のリクエストコンポーネントを使用する場合、基本コストの WCU を倍増させます。適用する各テキスト変換について、10 WCU を追加します。

このステートメントタイプは、ウェブリクエストコンポーネントで動作し、次のリクエストコンポーネント設定が必要です。

- [リクエストコンポーネント] — ウェブリクエストの検査対象部分 (クエリ文字列や本文など)。

> **Warning**
>
> リクエストコンポーネントの本文、JSON 本文、ヘッダー、または Cookie を検査する場合は、 で検査 AWS WAF できるコンテンツの量に関する制限についてお読みくださいでのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF。

ウェブリクエストコンポーネントの詳細については、「でのルールステートメント設定の調整 AWS WAF」を参照してください。

- オプションのテキスト変換 – 検査する前にリクエストコンポーネントで AWS WAF 実行する変換。例えば、小文字に変換したり、空白を正規化したりできます。複数の変換を指定すると、 はリストされた順序で変換 AWS WAF を処理します。詳細については、「でのテキスト変換の使用 AWS WAF」を参照してください。

このルールステートメントの場所

- コンソールのルールビルダー – [Match type] (一致タイプ) で、Matches regular expression] (正規表現に一致) を選択します。
- API – 「RegexMatchStatement」

正規表現パターンセット一致ルールステートメント

このセクションでは、正規表現パターンセット一致ステートメントとは何か、またその仕組みについて説明します。

正規表現パターンセット一致は、ウェブリクエストの指定した部分を、正規表現パターンセット内の指定した正規表現パターンに照らして検査します。

AWS WAF は、いくつかの例外`libpcre`を除いて、PCRE ライブラリで使用されるパターン構文をサポートします。ライブラリは、「PCRE - Perl Compatible Regular Expressions」で文書化されています。 AWS WAF サポートの詳細については、「」を参照してくださいでサポートされている正規表現構文 AWS WAF。

> **Note**
>
> 各正規表現パターンセット一致ルールは、正規表現パターンセットを参照します。このパターンセットは、ルールとは無関係に作成し、維持します。複数のルールで 1 つの正規表現パターンセットを使用できます。参照されるセットを更新すると、 はそれを参照するすべてのルール AWS WAF を自動的に更新します。
> 正規表現パターンセットの作成および管理については、「での正規表現パターンセットの作成と管理 AWS WAF」を参照してください。

正規表現パターンセット一致ステートメントは、選択したリクエストコンポーネント内のセット内のパターンを検索する AWS WAF ように に指示します。リクエストコンポーネントがセット内のいずれかのパターンに一致する場合、ウェブリクエストはパターンセットルールステートメントと一致します。

論理を使用して正規表現パターンの一致を組み合わせる場合、例えば、一部の正規表現と照合し、他の正規表現とは照合しない場合は、正規表現一致ルールステートメント を使用することを検討してください。

ルールステートメントの特性

ネスト可能 - このステートメントタイプはネスト可能です。

WCU - 基本コストとして 25 WCU。[All query parameters] (すべてのクエリパラメータ) のリクエストコンポーネントを使用する場合、10 WCU を追加します。[JSON body] (JSON 本文) のリクエストコンポーネントを使用する場合、基本コストの WCU を倍増させます。適用する各テキスト変換について、10 WCU を追加します。

このステートメントタイプは、ウェブリクエストコンポーネントで動作し、次のリクエストコンポーネント設定が必要です。

- [リクエストコンポーネント] — ウェブリクエストの検査対象部分 (クエリ文字列や本文など)。

  > **Warning**
  >
  > リクエストコンポーネント本文、JSON 本文、ヘッダー、または Cookie を検査する場合は、 で検査 AWS WAF できるコンテンツ量の制限についてお読みくださいでのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF。

  ウェブリクエストコンポーネントの詳細については、「でのルールステートメント設定の調整 AWS WAF」を参照してください。
- オプションのテキスト変換 – 検査する前にリクエストコンポーネントで AWS WAF 実行する変換。例えば、小文字に変換したり、空白を正規化したりできます。複数の変換を指定すると、 はリストされた順序で変換 AWS WAF を処理します。詳細については、「でのテキスト変換の使用 AWS WAF」を参照してください。

このステートメントには、次の設定が必要です。

- 正規表現パターンセットの指定 - 使用する正規表現パターンセットをリストから選択するか、新しい IP セットを作成します。

このルールステートメントの場所

- コンソールのルールビルダー - [Match type] (一致タイプ) で [String match condition] (文字列一致条件) > [Matches pattern from regular expression set] (正規表現セットのパターンに一致) を選択します。
- API – 「RegexPatternSetReferenceStatement」

サイズ制約ルールステートメント

このセクションでは、サイズ制約ステートメントとは何か，またその仕組みについて説明します。

サイズ制約ステートメントは、ウェブリクエストコンポーネントに対して が AWS WAF 受け取るバイト数と、指定したバイト数を比較し、比較基準に従って一致させます。

比較基準は、「より大きい (>)」や「より小さい (<)」などの演算子です。例えば、100 バイトを超えるサイズのクエリ文字列を含むリクエストの一致を実行できます。

URI パスを検査する場合、パス内の / は 1 文字としてカウントされます。例えば、URI パスの `/logo.jpg` は 9 文字の長さになります。

> **Note**
>
> このステートメントはウェブリクエストコンポーネントのサイズのみを検査します。コンポーネントのコンテンツは検査されません。

ルールステートメントの特性

ネスト可能 - このステートメントタイプはネスト可能です。

WCU- 1 WCU (基本コストとして)。[All query parameters] (すべてのクエリパラメータ) のリクエストコンポーネントを使用する場合、10 WCU を追加します。[JSON body] (JSON 本文) のリクエストコンポーネントを使用する場合、基本コストの WCU を倍増させます。適用する各テキスト変換について、10 WCU を追加します。

このステートメントタイプは、ウェブリクエストコンポーネントで動作し、次のリクエストコンポーネント設定が必要です。

- [リクエストコンポーネント] — ウェブリクエストの検査対象部分 (クエリ文字列や本文など)。ウェブリクエストコンポーネントの詳細については、「でのルールステートメント設定の調整 AWS WAF」を参照してください。

  サイズ制約ステートメントは、何らかの変換が適用された後のコンポーネントのサイズのみを検査します。コンポーネントのコンテンツは検査されません。
- オプションのテキスト変換 – サイズを検査する前にリクエストコンポーネントで AWS WAF 実行する変換。例えば、空白を圧縮したり、HTML エンティティをデコードしたりすることができます。複数の変換を指定すると、 はリストされた順序で変換 AWS WAF を処理します。詳細については、「でのテキスト変換の使用 AWS WAF」を参照してください。

さらに、このステートメントには、次の設定が必要です。

- Size match condition (サイズ一致条件) - これは、提供するサイズと選択したリクエストコンポーネントを比較するために使用する数値比較演算子を示します。リストから演算子を選択します。
- Size (サイズ) - 比較で使用するサイズ設定 (バイト単位)。

このルールステートメントの場所

- コンソールのルールビルダー - [Match type] (一致タイプ) の [Size match condition] (サイズ一致条件) で、使用する条件を選択します。
- API – 「SizeConstraintStatement」

SQL インジェクション攻撃ルールステートメント

このセクションでは、SQL インジェクションルールステートメントとは何か、またその仕組みについて説明します。

SQL インジェクションルールステートメントは、悪意のある SQL コードを検査します。攻撃者は、データベースを変更したり、データベースからデータを抽出したりするために、悪意のある SQL コードをウェブリクエストに挿入します。

ルールステートメントの特性

ネスト可能 - このステートメントタイプはネスト可能です。

WCU – 基本コストは、ルールステートメントの感度レベルの設定によって異なります。Low のコストは 20 で、High のコストは 30 です。

[All query parameters] (すべてのクエリパラメータ) のリクエストコンポーネントを使用する場合、10 WCU を追加します。[JSON body] (JSON 本文) のリクエストコンポーネントを使用する場合、基本コストの WCU を倍増させます。適用する各テキスト変換について、10 WCU を追加します。

このステートメントタイプは、ウェブリクエストコンポーネントで動作し、次のリクエストコンポーネント設定が必要です。

- [リクエストコンポーネント] — ウェブリクエストの検査対象部分 (クエリ文字列や本文など)。

  > **Warning**
  >
  > リクエストコンポーネントの本文、JSON 本文、ヘッダー、または Cookie を検査する場合は、 で検査 AWS WAF できるコンテンツの量に関する制限についてお読みくださいでのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF。

  ウェブリクエストコンポーネントの詳細については、「でのルールステートメント設定の調整 AWS WAF」を参照してください。
- オプションのテキスト変換 – 検査する前にリクエストコンポーネントで AWS WAF 実行する変換。例えば、小文字に変換したり、空白を正規化したりできます。複数の変換を指定すると、 はリストされた順序で変換 AWS WAF を処理します。詳細については、「でのテキスト変換の使用 AWS WAF」を参照してください。

さらに、このステートメントには、次の設定が必要です。

- 感度レベル – この設定は、SQL インジェクション一致基準の感度を調整します。オプションは LOW と HIGH です。デフォルトの設定は LOW です。

  HIGH 設定は、より多くの SQL インジェクション攻撃を検出するため、推奨される設定です。感度が高いため、この設定では、特にウェブリクエストに通常とは異なる文字列が一般的に含まれている場合に、より多くの誤検知が生成されます。保護パック (ウェブ ACL) のテストとチューニング中に、誤検知を軽減するためにさらに多くの作業が必要になる場合があります。詳細については、「AWS WAF 保護のテストとチューニング」を参照してください。

  設定が低いほど、SQL インジェクションの検出の厳格度も緩くなり、誤検知も少なくなります。LOW は、SQL インジェクション攻撃に対する他の保護を備えているリソースや、誤検知に対する許容度が低いリソースにとって、より適切な選択肢である可能性があります。

このルールステートメントの場所

- コンソールのルールビルダー - [Match type] (一致タイプ) で [Attack match condition] (攻撃一致条件) > [Contains SQL injection attacks] (SQL インジェクション攻撃を含む) を選択します。
- API – 「SqliMatchStatement」

文字列一致ルールステートメント

このセクションでは、文字列一致ステートメントとは何か、またその仕組みについて説明します。

文字列一致ステートメントは、リクエストで AWS WAF 検索する文字列、検索するリクエスト内の場所、および方法を示します。例えば、リクエストに含まれるクエリ文字列の先頭にある特定の文字列、またはリクエストの `User-agent` ヘッダーと完全に一致する特定の文字列を検索できます。通常、文字列は印刷可能な ASCII 文字で構成されますが、16 進数 0x00 ～ 0xFF (10 進数 0 ～ 255) の任意の文字を使用できます。

ルールステートメントの特性

ネスト可能 - このステートメントタイプはネスト可能です。

WCU – 基本コストは、使用する一致のタイプによって異なります。

- 次の文字列に完全一致 - 2
- 文字列で始まる - 2
- 文字列で終わる - 2
- 文字列を含む - 10
- 単語を含む – 10

[All query parameters] (すべてのクエリパラメータ) のリクエストコンポーネントを使用する場合、10 WCU を追加します。[JSON body] (JSON 本文) のリクエストコンポーネントを使用する場合、基本コストの WCU を倍増させます。適用する各テキスト変換について、10 WCU を追加します。

このステートメントタイプは、ウェブリクエストコンポーネントで動作し、次のリクエストコンポーネント設定が必要です。

- [リクエストコンポーネント] — ウェブリクエストの検査対象部分 (クエリ文字列や本文など)。

> **Warning**
>
> リクエストコンポーネント本文、JSON 本文、ヘッダー、または Cookie を検査する場合は、 で検査 AWS WAF できるコンテンツ量の制限についてお読みくださいでのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF。

ウェブリクエストコンポーネントの詳細については、「でのルールステートメント設定の調整 AWS WAF」を参照してください。

- オプションのテキスト変換 – 検査する前にリクエストコンポーネントで AWS WAF 実行する変換。例えば、小文字に変換したり、空白を正規化したりできます。複数の変換を指定すると、 はリストされた順序で変換 AWS WAF を処理します。詳細については、「でのテキスト変換の使用 AWS WAF」を参照してください。

さらに、このステートメントには、次の設定が必要です。

- 一致する文字列 – これは、指定されたリクエストコンポーネント AWS WAF と比較する文字列です。通常、文字列は印刷可能な ASCII 文字で構成されますが、16 進数 0x00 ～ 0xFF (10 進数 0 ～ 255) の任意の文字を使用できます。
- 文字列一致条件 – AWS WAF 実行する検索タイプを示します。
  - Exactly matches string (次の文字列に完全一致) - リクエストコンポーネントの文字列と値が同一です。
  - Starts with string (次の文字列で始まる) - この文字列は、リクエストコンポーネントの先頭に出現します。
  - Ends with string (次の文字列で終わる) - この文字列は、リクエストコンポーネントの末尾に出現します。
  - Contains string (次の文字列を含む) - この文字列は、リクエストコンポーネント内の任意の場所に出現します。
  - Contains word (次の文字列を含む) - 指定した文字列がリクエストコンポーネントに出現する必要があります。

    このオプションの場合、指定する文字列には英数字またはアンダースコア (A～Z、a～z、0～9、または_) のみを使用できます。

    リクエストが一致するには、次のいずれかに当てはまる必要があります。

- 文字列が、ヘッダーの値など、リクエストコンポーネントの値と正確に一致する。
- 文字列が、リクエストコンポーネントの先頭にあり、英数字または下線 (_) 以外の文字が続く (例: `BadBot;`)。
- 文字列が、リクエストコンポーネントの末尾にあり、英数字または下線 (_) 以外の文字が先行する (例: `;BadBot`)。
- 文字列が、リクエストコンポーネントの中央にあり、英数字または下線 (_) 以外の文字が前後にある (例: `-BadBot;`)。

このルールステートメントの場所

- コンソールのルールビルダー - [Match type] (一致タイプ) で [String match condition] (文字列一致条件) を選択し、一致させる文字列を入力します。
- API – 「ByteMatchStatement」

クロスサイトスクリプティング攻撃ルールステートメント

このセクションでは、XSS (クロスサイトスクリプティング) 攻撃ステートメントとは何か、またその仕組みについて説明します。

XSS 攻撃ステートメントは、ウェブリクエストコンポーネント内の悪意のあるスクリプトを検査します。XSS 攻撃では、攻撃者は、悪意のあるクライアントサイトスクリプトを他の正当なウェブブラウザに挿入するための手段として、悪意のないウェブサイトの脆弱性を利用します。

ルールステートメントの特性

ネスト可能 - このステートメントタイプはネスト可能です。

WCU- 40 WCU (基本コストとして)。[All query parameters] (すべてのクエリパラメータ) のリクエストコンポーネントを使用する場合、10 WCU を追加します。[JSON body] (JSON 本文) のリクエストコンポーネントを使用する場合、基本コストの WCU を倍増させます。適用する各テキスト変換について、10 WCU を追加します。

このステートメントタイプは、ウェブリクエストコンポーネントで動作し、次のリクエストコンポーネント設定が必要です。

- [リクエストコンポーネント] — ウェブリクエストの検査対象部分 (クエリ文字列や本文など)。

> **Warning**
>
> リクエストコンポーネントの本文、JSON 本文、ヘッダー、または Cookie を検査する場合は、 で検査 AWS WAF できるコンテンツの量に関する制限についてお読みくださいでのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF。

ウェブリクエストコンポーネントの詳細については、「でのルールステートメント設定の調整 AWS WAF」を参照してください。

- オプションのテキスト変換 – 検査する前にリクエストコンポーネントで AWS WAF 実行する変換。例えば、小文字に変換したり、空白を正規化したりできます。複数の変換を指定すると、 はリストされた順序で変換 AWS WAF を処理します。詳細については、「でのテキスト変換の使用 AWS WAF」を参照してください。

このルールステートメントの場所

- コンソールのルールビルダー - [Match type] (一致タイプ) で [Attack match condition] (攻撃一致条件) > [Contains XSS injection attacks] (SQL インジェクション攻撃を含む) を選択します。
- API – 「XssMatchStatement」

での論理ルールステートメントの使用 AWS WAF

このセクションでは、ロジックルールステートメントとは何か、またその仕組みについて説明します。

論理ルールステートメントを使用して他のステートメントを組み合わせたり、結果を否定したりします。すべての論理ルールステートメントに、1 つ以上のネストされたステートメントが必要です。

ルールステートメントの結果を論理的に結合または否定するには、ステートメントを論理ルールステートメントの下にネストします。

論理ルールステートメントはネスト可能です。他の論理ルールステートメント内にネストして、スコープダウンステートメントで使用できます。スコープダウンステートメントの詳細については、「でのスコープダウンステートメントの使用 AWS WAF」を参照してください。

> **Note**
>
> コンソールのビジュアルエディタは、1 レベルのルールステートメントのネストをサポートしており、多くのニーズに対応しています。より多くのレベルをネストするには、コンソールでルールの JSON 表現を編集するか、API を使用します。

この表では、論理ルールステートメントについて説明し、それぞれの保護パック (ウェブ ACL) キャパシティーユニット (WCU) 使用量を計算するためのガイドラインを提供します。WCU の詳細については、「のウェブ ACL キャパシティユニット (WCUs) AWS WAF」を参照してください。

論理ステートメント	説明	WCU
AND のロジック	ネストされたステートメントを AND ロジックと組み合わせます。	ネストされたステートメントに基づく
NOT のロジック	ネストされたステートメントの結果を否定します。	ネストされたステートメントに基づく
OR のロジック	ネストされたステートメントを OR ロジックと組み合わせます。	ネストされたステートメントに基づく

AND ルールステートメント

AND ルールステートメントは、ネストされたステートメントを論理 AND 演算と組み合わせるため、AND ステートメントが一致するには、ネストされたステートメントがすべて一致する必要があります。これには、1 つ以上のネストされたステートメントが必要です。

ルールステートメントの特性

ネスト可能 - このステートメントタイプはネスト可能です。

WCU - ネストされたステートメントに応じて異なります。

このルールステートメントの場所

- コンソールのルールビルダー - [If a request] (リクエストの状態) で [matches all the statements (AND)] (すべてのステートメントに一致する場合 (AND)) を選択してから、ネストされたステートメントに入力します。
- API – AndStatement

例

次のリストは、AND および NOT 論理ルールステートメントを使用して、SQL インジェクション攻撃ステートメントの一致から誤検知を排除する方法を示しています。この例では、誤検知につながるリクエストと一致する 1 バイトの一致ステートメントを記述できるとします。

AND ステートメントは、バイト一致ステートメントと一致せず、SQL インジェクション攻撃ステートメントと一致するリクエストと一致します。

```
{
      "Name": "SQLiExcludeFalsePositives",
      "Priority": 0,
      "Statement": {
        "AndStatement": {
          "Statements": [
            {
              "NotStatement": {
                "Statement": {
                  "ByteMatchStatement": {
                    "SearchString": "string identifying a false positive",
                    "FieldToMatch": {
                      "Body": {
                        "OversizeHandling": "MATCH"
                      }
                    },
                    "TextTransformations": [
                      {
                        "Priority": 0,
                        "Type": "NONE"
                      }
                    ],
                    "PositionalConstraint": "CONTAINS"
                  }
                }
              }
```

```
            },
            {
              "SqliMatchStatement": {
                "FieldToMatch": {
                  "Body": {
                    "OversizeHandling": "MATCH"
                  }
                },
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "SQLiExcludeFalsePositives"
      }
    }
```

コンソールルールビジュアルエディタを使用して、非論理ステートメントまたは NOT ステートメントを OR または AND ステートメントの下にネストできます。NOT ステートメントのネストは、前の例に示されています。

コンソールルールビジュアルエディタを使用すると、ほとんどのネスト可能なステートメントを、前の例に示したような論理ルールステートメントの下にネストできます。ビジュアルエディタを使用して OR または AND ステートメントをネストすることはできません。このタイプのネストを設定するには、JSON でルールステートメントを指定する必要があります。例えば、次の JSON ルールリストには、AND ステートメント内にネストされた OR ステートメントが含まれています。

```
{
  "Name": "match_rule",
  "Priority": 0,
```

```
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
              }
            }
          }
        },
        {
          "OrStatement": {
            "Statements": [
              {
                "GeoMatchStatement": {
                  "CountryCodes": [
                    "JM",
                    "JP"
                  ]
                }
              },
              {
                "ByteMatchStatement": {
                  "SearchString": "JCountryString",
                  "FieldToMatch": {
                    "Body": {}
                  },
                  "TextTransformations": [
                    {
                      "Priority": 0,
                      "Type": "NONE"
                    }
                  ],
                  "PositionalConstraint": "CONTAINS"
                }
```

```
              }
            ]
          }
        }
      ]
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "match_rule"
  }
}
```

NOT ルールステートメント

NOT ルールステートメントは、単一のネストされたステートメントの結果を論理的に否定するため、NOT ステートメントが一致するには、ネストされたステートメントが一致してはならず、その逆も同様です。これには、ネストされたステートメントが 1 つ必要です。

例えば、特定の国を送信元としないリクエストをブロックする場合は、アクションをブロックに設定した NOT ステートメントを作成し、国を指定する地理的一致ステートメントをネストします。

ルールステートメントの特性

ネスト可能 - このステートメントタイプはネスト可能です。

WCU - ネストされたステートメントに応じて異なります。

このルールステートメントの場所

- コンソールのルールビルダー - [If a request] (リクエストの状態) で [doesn't match the statement (NOT)] (すべてのステートメントに一致しない場合 (NOT)) を選択してから、ネストされたステートメントに入力します。
- API – 「NotStatement」

OR ルールステートメント

OR ルールステートメントは、ネストされたステートメントを OR ロジックと組み合わせるため、OR ステートメントが一致するには、ネストされたステートメントのいずれか 1 つが一致する必要があります。これには、1 つ以上のネストされたステートメントが必要です。

例えば、特定の国から送信されたリクエストや特定のクエリ文字列を含むリクエストをブロックする場合は、OR ステートメントを作成し、その国の地理的照合ステートメントとクエリ文字列の文字列照合ステートメントをネストします。

代わりに、特定の国から送信されていないリクエストや特定のクエリ文字列を含むリクエストをブロックする場合は、前述の OR ステートメントを変更して、NOT ステートメント内の 1 レベル下に地理的照合ステートメントをネストします。コンソールでは 1 レベルのネストしかサポートされないため、このレベルのネストでは JSON 形式を使用する必要があります。

ルールステートメントの特性

ネスト可能 - このステートメントタイプはネスト可能です。

WCU - ネストされたステートメントに応じて異なります。

このルールステートメントの場所

- コンソールのルールビルダー - [If a request] (リクエストの状態) で [matches at least one of the statements (OR)] (1 つ以上のステートメントに一致する場合 (OR)) を選択してから、ネストされたステートメントに入力します。
- API – 「OrStatement」

例

次のリストは、OR を使用して他の 2 つのステートメントを結合する方法を示しています。ネストされたステートメントのいずれかが一致する場合、OR ステートメントは一致します。

```
{
  "Name": "neitherOfTwo",
  "Priority": 1,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
```

```
    "CloudWatchMetricsEnabled": true,
    "MetricName": "neitherOfTwo"
  },
  "Statement": {
    "OrStatement": {
      "Statements": [
        {
          "GeoMatchStatement": {
            "CountryCodes": [
              "CA"
            ]
          }
        },
        {
          "IPSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:111111111111:regional/ipset/test-ip-
set-22222222/33333333-4444-5555-6666-777777777777"
          }
        }
      ]
    }
  }
}
```

コンソールルールビジュアルエディタを使用すると、ネスト可能なステートメントのほとんどを論理ルールステートメントの下にネストできますが、ビジュアルエディタを使用して OR または AND ステートメントをネストすることはできません。このタイプのネストを設定するには、JSON でルールステートメントを指定する必要があります。例えば、次の JSON ルールリストには、AND ステートメント内にネストされた OR ステートメントが含まれています。

```
{
  "Name": "match_rule",
  "Priority": 0,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
          }
        },
        {
```

```
          "NotStatement": {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
              }
            }
          }
        },
        {
          "OrStatement": {
            "Statements": [
              {
                "GeoMatchStatement": {
                  "CountryCodes": [
                    "JM",
                    "JP"
                  ]
                }
              },
              {
                "ByteMatchStatement": {
                  "SearchString": "JCountryString",
                  "FieldToMatch": {
                    "Body": {}
                  },
                  "TextTransformations": [
                    {
                      "Priority": 0,
                      "Type": "NONE"
                    }
                  ],
                  "PositionalConstraint": "CONTAINS"
                }
              }
            ]
          }
        }
      ]
    }
  },
  "Action": {
    "Block": {}
  },
```

```
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "match_rule"
  }
}
```

でのレートベースのルールステートメントの使用 AWS WAF

このセクションでは、レートベースのルールステートメントとは何か、またその仕組みについて説明します。

レートベースのルールでは、受信リクエストをカウントし、レートが速すぎる場合にはリクエストを制限します。このルールは、条件に従ってリクエストを集約し、ルールの評価ウインドウ、リクエスト制限とアクション設定に基づいて集約されたグループを記入およびレート制限します。

> **Note**
>
> Bot Control AWS マネージドルールルールグループのターゲットを絞った保護レベルを使用して、ウェブリクエストをレート制限することもできます。マネージドルールグループの使用には追加料金が発生します。詳細については、「レートベースのルールとターゲットを絞った Bot Control ルールにおけるレート制限のオプション」を参照してください。

AWS WAF は、使用するレートベースのルールのインスタンスごとにウェブリクエストを個別に追跡および管理します。たとえば、2 つのウェブ ACLs で同じレートベースのルール設定を指定すると、2 つのルールステートメントはそれぞれレートベースのルールの個別のインスタンスを表し、それぞれが独自の追跡と管理を取得します AWS WAF。ルールグループ内でレートベースのルールを定義し、そのルールグループを複数の場所で使用する場合、各使用により、独自の追跡および管理を取得するレートベースのルールの個別のインスタンスが作成されます AWS WAF。

ネスト不可 - このステートメントタイプを他のステートメント内にネストすることはできません。このタイプは、保護パック (ウェブ ACL) およびルールグループに直接含めることができます。

スコープダウンステートメント – このルールタイプは、オプションのスコープダウンステートメントを使用して、レートベースのステートメントが追跡するリクエストの範囲を絞り込むことができます。スコープダウンステートメントは、他のルール設定に応じて、オプションでも必須でもかまいません。詳細については、このセクションで説明します。スコープダウンステートメントの詳細については、でのスコープダウンステートメントの使用 AWS WAF を参照してください。

WCU - 2 個の WCU (基本コストとして)。指定するカスタム集約キーごとに、30 個の WCU を追加します。ルールでスコープダウンステートメントを使用する場合は、その分の WCU を計算して追加します。

このルールステートメントの場所

- 保護パック (ウェブ ACL) のコンソールのルールビルダー – [Rule] (ルール) の [Type] (タイプ) で、[Rate-based rule] (レートベースのルール) を選択します。
- API – 「RateBasedStatement」

トピック

- でのレートベースのルールの高レベル設定 AWS WAF
- のレートベースのルールに関する注意事項 AWS WAF
- でのレートベースのルールの集計 AWS WAF
- レートベースのルール集約インスタンスとカウント
- でのリクエストへのレート制限の適用 AWS WAF
- のレートベースのルールの例 AWS WAF
- レートベースのルールによってレート制限されている IP アドレスの一覧表示

でのレートベースのルールの高レベル設定 AWS WAF

レートベースのルールステートメントでは、次の概要レベル設定を使用します。

- 評価ウィンドウ – 現在の時点から遡って、 AWS WAF がリクエスト数に含めるべき時間 (秒単位) 。たとえば、設定が 120 の場合、 がレート AWS WAF をチェックすると、現在の時刻の直前の 2 分間のリクエストがカウントされます。有効な設定は、60 (1 分) 、120 (2 分) 、300 (5 分) 、600 (10 分) で、300 (5 分) がデフォルトです。

  この設定では、レート AWS WAF をチェックする頻度ではなく、チェックするたびにレートがどの程度戻るかが決まります。 AWS WAF は、評価ウィンドウの設定とは無関係のタイミングでレートを頻繁にチェックします。
- レート制限 – 指定された評価ウィンドウに対して追跡 AWS WAF する基準に一致するリクエストの最大数。許可される最小制限設定は 10 です。この制限を超えると、 は条件に一致する追加のリクエストにルールアクション設定 AWS WAF を適用します。

AWS WAF は、設定した制限の近くにレート制限を適用しますが、 は制限の完全一致を保証しません。詳細については、「レートベースのルールの規制」を参照してください。

- リクエスト集約 – レートベースのルールがカウントおよびレート制限するウェブリクエストで使用する集約条件です。設定したレート制限は、各集約インスタンスに適用されます。詳細については、「レートベースのルールの集計」および「集約インスタンスおよびカウント」を参照してください。
- アクション – ルールによってレート制限されているリクエストに対して実行するアクションです。Allow 以外のルールアクションを使用できます。これは通常どおりルールレベルで設定されますが、レートベースのルールに固有の制限と動作があります。ルールアクションの一般情報については、「でのルールアクションの使用 AWS WAF」を参照してください。レート制限の固有情報については、このセクションの でのリクエストへのレート制限の適用 AWS WAF を参照してください。
- 検査の範囲とレート制限 – スコープダウンステートメントを追加して、レートベースのステートメントが追跡およびレート制限するリクエストの範囲を絞り込むことができます。スコープダウンステートメントを指定すると、ルールはスコープダウンステートメントに一致するリクエストのみを集約、カウント、およびリスト制限します。リクエスト集約オプションの [すべてをカウント] を選択する場合は、スコープダウンステートメントが必要です。スコープダウンステートメントの詳細については、「スコープダウンステートメントの使用」を参照してください。
- (オプション) 転送された IP 設定 – 単独で、またはカスタムキー設定の一部としてリクエスト集約で [ヘッダーの IP アドレス] を指定する場合にのみ使用されます。 AWS WAF は指定されたヘッダーの最初の IP アドレスを取得し、それを集約した値として使用します。この用途によく使用されるヘッダーは `X-Forwarded-For` ですが、任意のヘッダーを指定できます。詳細については、「転送された IP アドレスの使用」を参照してください。

のレートベースのルールに関する注意事項 AWS WAF

このセクションでは、レートベースのルールを使用するための規制を一覧表示します。

AWS WAF レート制限は、高いリクエストレートを制御し、アプリケーションの可用性を可能な限り最も効率的かつ効果的な方法で保護するように設計されています。リクエストレートを正確に制限することを意図したものではありません。

- AWS WAF は、より最近のリクエストをより重視するアルゴリズムを使用して、現在のリクエストレートを推定します。このため、 AWS WAF は設定した制限の近くにレート制限を適用しますが、 は正確な制限の一致を保証しません。

- がリクエストのレートを AWS WAF 見積もるたびに、 は設定された評価ウィンドウ中に着信したリクエストの数を AWS WAF 振り返ります。このような要因や伝播の遅延などの要因により、AWS WAF が検出してレート制限する前に、リクエストが最大数分間高すぎる可能性があります。同様に、リクエスト率が一定期間制限以下になると、 AWS WAF がその減少を検出してレート制限のアクションを停止するまで時間がかかることがあります。通常、この遅延は 30 秒未満です。
- 使用中のルールのレート制限設定を変更すると、その変更はルールのレート制限カウントをリセットします。これにより、ルールのレート制限アクティビティを最大 1 分間一時停止できます。レート制限設定は、評価ウィンドウ、レート制限、リクエスト集約設定、転送された IP 設定、検査範囲です。

でのレートベースのルールの集計 AWS WAF

このセクションでは、リクエストを集約するためのオプションについて説明します。

デフォルトでは、レートベースのルールはリクエスト IP アドレスに基づき、リクエストを集約してレート制限します。他のさまざまな集約キーやキーの組み合わせを使用するようにルールを設定できます。例えば、転送された IP アドレス、HTTP メソッド、またはクエリ引数に基づいて集約できます。IP アドレスと HTTP メソッド、または 2 つの異なる Cookie の値など、集約キーの組み合わせを指定できます。

> **Note**
>
> リクエストを評価したり、ルールによってレート制限したりするには、集約キーで指定するすべてのリクエストコンポーネントがウェブリクエストに含まれている必要があります。

レートベースのルールは、次の集約オプションを使用して設定できます。

- 送信元 IP アドレス – ウェブリクエストの発信元 IP アドレスのみを使用して集約します。

  送信元 IP アドレスには、発信元クライアントのアドレスが含まれていない場合があります。ウェブリクエストが 1 つ以上のプロキシまたはロードバランサーを経由する場合、これには最後のプロキシのアドレスが含まれます。
- ヘッダーの IP アドレス – HTTP ヘッダー内のクライアントアドレスのみを使用して集約します。これは転送された IP アドレスとも呼ばれます。

この設定では、ヘッダーに不正な形式の IP アドレスを持つウェブリクエストに適用するフォールバック動作も指定します。フォールバック動作は、リクエストの一致結果を、一致または不一致のいずれにするかを設定します。不一致の場合、レートベースのルールは、リクエストをカウントまたはレート制限しません。一致の場合、レートベースのルールは、指定されたヘッダーに不正な形式の IP アドレスを持つ他のリクエストとともに、リクエストをグループ化します。

このオプションでは、プロキシによって一貫性のないヘッダー処理が行われ、検査を回避するように変更される可能性があるため、注意が必要です。追加情報とベストプラクティスについては、「で転送された IP アドレスを使用する AWS WAF」を参照してください。

- ASN – ソース IP アドレスに関連付けられた AS 番号 (ASN) を集約キーとして使用して集約します。これは、発信元クライアントのアドレスでは可能性があります。ウェブリクエストが 1 つ以上のプロキシまたはロードバランサーを経由する場合、これには最後のプロキシのアドレスが含まれます。

  が IP アドレスから ASN を取得 AWS WAF できない場合、ASN は ASN 0 としてカウントされます。マッピングされていない ASN にレート制限を適用しない場合は、ASN 0 のリクエストを除外するスコープダウンルールを作成できます。

- ヘッダーの ASN – HTTP ヘッダー内のクライアント IP アドレスに関連付けられた ASN を使用して集約します。これは転送された IP アドレスとも呼ばれます。この設定では、無効または不正な形式の IP アドレスを持つウェブリクエストに適用するフォールバック動作も指定します。フォールバック動作は、リクエストの一致結果を、一致または不一致のいずれにするかを設定します。転送された IP 設定でフォールバック動作が一致するように設定した場合、 は無効な IP アドレスを一致する値として AWS WAF 扱います。これにより、 AWS WAF はレートベースのルールの複合キーの残りの部分の評価を継続できます。不一致の場合、レートベースのルールは、リクエストをカウントまたはレート制限しません。

  このオプションでは、プロキシによって一貫性のないヘッダー処理が行われ、検査を回避するように変更される可能性があるため、注意が必要です。追加情報とベストプラクティスについては、「で転送された IP アドレスを使用する AWS WAF」を参照してください。

- すべてをカウント – ルールのスコープダウンステートメントに一致するすべてのリクエストをカウントおよびレート制限します。このオプションには、スコープダウンステートメントが必要です。これは通常、特定のラベルが付いた全リクエストや特定の地域からの全リクエストなど、特定のリクエストセットをレート制限するために使用されます。

- カスタムキー – 1 つ以上のカスタム集約キーを使用して集約します。いずれかの IP アドレスオプションを他の集約キーと組み合わせるには、それらをカスタムキーで定義します。

カスタム集約キーは、「でコンポーネントをリクエストする AWS WAF」で説明されているウェブリクエストコンポーネントオプションのサブセットです。

キーオプションは次のとおりです。特に明記されていない限り、オプションは複数回使用できます。例えば、2 つのヘッダーや 3 つのラベル名前空間などが使用可能です。

- ラベル名前空間 – ラベル名前空間を集約キーとして使用します。指定されたラベル名前空間を持つ個別の完全修飾ラベル名はそれぞれ、集約インスタンスに影響します。カスタムキーとしてラベル名前空間を 1 つだけ使用する場合、各ラベル名は集約インスタンスを完全に定義します。

  レートベースのルールが使用するラベルは、保護パック (ウェブ ACL) であらかじめ評価されたルールによってリクエストに追加されたものに限ります。

  ラベル名前空間とラベル名の詳細については、「でのラベル構文と命名要件 AWS WAF」を参照してください。
- ヘッダー – 名前付きヘッダーを集約キーとして使用します。ヘッダー内の個別の値はそれぞれ、集約インスタンスに影響します。

  ヘッダーはオプションでテキスト変換を実行します。「でのテキスト変換の使用 AWS WAF」を参照してください。
- Cookie – 名前付き Cookie を集約キーとして使用します。Cookie 内の個別の値はそれぞれ、集約インスタンスに影響します。

  Cookie はオプションでテキスト変換を実行します。「でのテキスト変換の使用 AWS WAF」を参照してください。
- クエリ引数 – リクエスト内で 1 つのクエリ引数を集約キーとして使用します。名前付きクエリ引数の個別の値はそれぞれ、集約インスタンスに影響します。

  クエリ引数はオプションでテキスト変換を実行します。「でのテキスト変換の使用 AWS WAF」を参照してください。
- クエリ文字列 – リクエスト内のクエリ文字列全体を集約キーとして使用します。個別のクエリ文字列はそれぞれ、集約インスタンスに影響します。このキータイプは一度だけ使用できます。

  クエリ文字列はオプションでテキスト変換を実行します。「でのテキスト変換の使用 AWS WAF」を参照してください。
- URI パス — リクエスト内の URI パスを集約キーとして使用します。個別の URI パスはそれぞれ、集約インスタンスに影響します。このキータイプは一度だけ使用できます。

URI パスはオプションでテキスト変換を実行します。「でのテキスト変換の使用 AWS WAF」を参照してください。

- JA3 フィンガープリント – リクエストで JA3 フィンガープリントを集計キーとして使用します。個別の JA3 フィンガープリントはそれぞれ、集約インスタンスに影響します。このキータイプは一度だけ使用できます。
- JA4 フィンガープリント – リクエストで JA4 フィンガープリントを集計キーとして使用します。個別の JA4 フィンガープリントはそれぞれ、集約インスタンスに影響します。このキータイプは一度だけ使用できます。
- HTTP メソッド – リクエストの HTTP メソッドを集約キーとして使用します。個別の HTTP メソッドはそれぞれ、集約インスタンスに影響します。このキータイプは一度だけ使用できます。
- IP アドレス – ウェブリクエストの発信元 IP アドレスを他のキーと組み合わせて集約します。

  これには、発信元クライアントのアドレスが含まれていない可能性があります。ウェブリクエストが 1 つ以上のプロキシまたはロードバランサーを経由する場合、これには最後のプロキシのアドレスが含まれます。
- ヘッダーの IP アドレス – HTTP ヘッダー内のクライアントアドレスを他のキーと組み合わせて集約します。これは転送された IP アドレスとも呼ばれます。

  このオプションでは、プロキシによって一貫性のないヘッダー処理が行われ、検査を回避するように変更される可能性があるため、注意が必要です。追加情報とベストプラクティスについては、「で転送された IP アドレスを使用する AWS WAF」を参照してください。

レートベースのルール集約インスタンスとカウント

このセクションでは、レートベースのルールがウェブリクエストを評価する方法について説明します。

レートベースのルールが集約条件を使用してウェブリクエストを評価する場合、指定された集約キーに対してルールが検出した一意の値セットはそれぞれ、一意の 集約インスタンス を定義します。

- 複数キー - 複数のカスタムキーを定義した場合、各キーの値は集約インスタンスの定義に影響します。値の一意の組み合わせはそれぞれ、集約インスタンスを定義します。
- 単一キー - カスタムキーで単一キーを選択した場合、またはシングルトン IP アドレスの選択肢の中から単一キーを選択した場合、キーの一意の値はそれぞれ、集約インスタンスを定義します。

- すべてをカウント - キーなし - 集約オプションの [すべてをカウント] を選択した場合、ルールが評価するすべてのリクエストは、ルールの 1 つの集約インスタンスに属します。この選択には、スコープダウンステートメントが必要です。

レートベースのルールは、識別された集約インスタンスごとにウェブリクエストを個別にカウントします。

例えば、レートベースのルールが次の IP アドレスと HTTP メソッドの値を持つウェブリクエストを評価するとします。

- IP アドレス 10.1.1.1、HTTP メソッド POST
- IP アドレス 10.1.1.1、HTTP メソッド GET
- IP アドレス 127.0.0.0、HTTP メソッド POST
- IP アドレス 10.1.1.1、HTTP メソッド GET

このルールは、集約条件に従ってさまざまな集約インスタンスを作成します。

- 集約基準が IP アドレスのみの場合、個々の IP アドレスは集約インスタンスであり、 はリクエストを個別に AWS WAF カウントします。この例の集約インスタンスおよびリクエストカウントは次のようになります。
  - IP アドレス 10.1.1.1: カウント 3
  - IP アドレス 127.0.0.0: カウント 1
- 集約条件が HTTP メソッドの場合、個々の HTTP メソッドが集約インスタンスになります。この例の集約インスタンスおよびリクエストカウントは次のようになります。
  - HTTP メソッド POST: カウント 2
  - HTTP メソッド GET: カウント 2
- 集約条件が IP アドレスと HTTP メソッドの場合、各 IP アドレスと各 HTTP メソッドは、複合的な集約インスタンスに影響します。この例の集約インスタンスおよびリクエストカウントは次のようになります。
  - IP アドレス 10.1.1.1、HTTP メソッド POST: カウント 1
  - IP アドレス 10.1.1.1、HTTP メソッド GET: カウント 2
  - IP アドレス 127.0.0.0、HTTP メソッド POST: カウント 1

でのリクエストへのレート制限の適用 AWS WAF

このセクションでは、レートベースのルールでレート制限の動作の仕組みについて説明します。

レートベースのルールのリクエストをレート制限するために AWS WAF が使用する条件は、 AWS WAF がルールのリクエストを集計するために使用する条件と同じです。ルールのスコープダウンステートメントを定義すると、 はスコープダウンステートメントに一致するリクエスト AWS WAF のみを集計、カウント、レート制限します。

レートベースのルールが特定のウェブリクエストにルールアクション設定を適用する一致条件は、次のとおりです。

- ウェブリクエストは、ルールのスコープダウンステートメントと一致している (定義されている場合) 。
- ウェブリクエストは、現在リクエストカウントがルールの制限を超えている集約インスタンスに属している。

がルールアクション AWS WAF を適用する方法

レートベースのルールがリクエストにレート制限を適用すると、ルールアクションが適用されます。アクション仕様でカスタム処理やラベル付けを定義している場合、ルールはそれらを適用します。このリクエスト処理は、一致ルールが一致したウェブリクエストにアクション設定を適用する方法と同じです。レートベースのルールは、レート制限が積極的に行われているリクエストにのみラベルを適用したり、他のアクションを実行したりします。

Allow 以外のルールアクションを使用できます。ルールアクションの一般情報については、「でのルールアクションの使用 AWS WAF」を参照してください。

次のリストは、各アクションのレート制限の仕組みを示しています。

- Block – リクエストを AWS WAF ブロックし、定義したカスタムブロック動作を適用します。
- Count – リクエストを AWS WAF カウントし、定義したカスタムヘッダーまたはラベルを適用し、リクエストの保護パック (ウェブ ACL) の評価を続行します。

  このアクションはリクエストのレートを制限しません。制限を超えるリクエストのみを記入します。
- CAPTCHA または Challenge - AWS WAF はリクエストのトークンの状態に応じて、Count または Block のいずれかのようにリクエストを処理します。

このアクションは、有効なトークンを持つリクエストのレートを制限しません。これは、リクエストが指定された上限を超えていて、さらに有効なトークンが含まれていない場合、そのリクエストの数を制限します。

- リクエストに有効期限が切れていない有効なトークンがない場合、このアクションはリクエストをブロックし、CAPTCHA パズルまたはブラウザのチャレンジをクライアントに返送します。

  エンドユーザーまたはクライアントブラウザが正常に応答すると、クライアントは有効なトークンを受け取り、元のリクエストが自動的に再送信されます。集約インスタンスのレート制限がまだ有効である場合、有効期限が切れていない有効なトークンを含むこの新しいリクエストには、次の箇条書きで説明するアクションが適用されます。
- リクエストに有効期限が切れていない有効なトークンがある場合、CAPTCHA または Challenge アクションはトークンを検証し、Count アクションと同様にリクエストに対してアクションを実行しません。レートベースのルールは、終了アクションを実行せずにリクエスト評価を保護パック (ウェブ ACL) に戻し、保護パック (ウェブ ACL) はリクエストの評価を続行します。

詳細については、「CAPTCHA および Challengeの AWS WAF」を参照してください。

IP アドレスまたは転送された IP アドレスのみをレート制限する場合

転送されたIPアドレスに対してのみIPアドレスのレート制限を行うようにルールを設定すると、そのルールが現在レート制限を適用しているIPアドレスのリストを取得できます。スコープダウンステートメントを使用する場合、レート制限されるリクエストは、スコープダウンステートメントと一致する IP リスト内のリクエストだけです。IP アドレスリストの取得の詳細については、「レートベースのルールによってレート制限されている IP アドレスの一覧表示」を参照してください。

のレートベースのルールの例 AWS WAF

このセクションでは、一般的なレートベースのルールのさまざまなユースケースにおける設定例について説明します。

各例は、ユースケースの説明を提供し、カスタム設定ルールの JSON リストにそのソリューションを示します。

> **Note**
>
> これらの例に示されている JSON リストは、ルールを設定し、Rule JSON エディタを使用して編集することにより、コンソールで作成されました。

トピック

- ログインページへのリクエストをレート制限する
- 任意の IP アドレス、ユーザーエージェントペアからのログインページへのリクエストをレート制限する
- 特定のヘッダーが欠落しているリクエストをレート制限する
- 特定のラベルを使用してリクエストをレート制限する
- ラベル名前空間が指定されたラベルのリクエストをレート制限する
- 特定の ASN を使用してリクエストをレート制限する

ログインページへのリクエストをレート制限する

ウェブサイトのログインページへのリクエスト数を、サイトの他の部分へのトラフィックに影響を与えることなく制限するには、ログインページへのリクエストに一致するスコープダウンステートメントを含むレートベースのルールを作成し、リクエスト集約を [すべてをカウント] に設定します。

レートベースのルールは、単一の集約インスタンス内のログインページのすべてのリクエストをカウントし、リクエストが制限を超えたときに、スコープダウンステートメントに一致するすべてのリクエストにルールアクションを適用します。

次の JSON リストは、このルール設定の例を示しています。集約をすべてカウントするオプションは、CONSTANT 設定として JSON に記載されています。この例は、/login で始まるログインページと一致します。

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 1000,
      "EvaluationWindowSec": 300,
      "AggregateKeyType": "CONSTANT",
```

```
      "ScopeDownStatement": {
        "ByteMatchStatement": {
          "FieldToMatch": {
            "UriPath": {}
          },
          "PositionalConstraint": "STARTS_WITH",
          "SearchString": "/login",
          "TextTransformations": [
            {
              "Type": "NONE",
              "Priority": 0
            }
          ]
        }
      }
    }
  }
}
```

任意の IP アドレス、ユーザーエージェントペアからのログインページへのリクエストをレート制限する

IP アドレス、ユーザーエージェントペアが制限を超えた場合に、ウェブサイトのログインページへのリクエスト数を制限するには、リクエスト集約を [カスタムキー] に設定して集約条件を指定します。

次の JSON リストは、このルール設定の例を示しています。この例では、IP アドレス、ユーザーエージェントペアごとに 5 分間の時間枠でのお制限を 100 リクエストに設定しています。

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
```

```
      "EvaluationWindowSec": 300,
      "AggregateKeyType": "CUSTOM_KEYS",
      "CustomKeys": [
        {
          "Header": {
            "Name": "User-Agent",
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        },
        {
          "IP": {}
        }
      ],
      "ScopeDownStatement": {
        "ByteMatchStatement": {
          "FieldToMatch": {
            "UriPath": {}
          },
          "PositionalConstraint": "STARTS_WITH",
          "SearchString": "/login",
          "TextTransformations": [
            {
              "Type": "NONE",
              "Priority": 0
            }
          ]
        }
      }
    }
  }
}
```

特定のヘッダーが欠落しているリクエストをレート制限する

特定のヘッダーが欠落しているリクエスト数を制限するには、スコープダウンステートメントで [すべてをカウント] 集約オプションを使用できます。ヘッダーが存在していて値がある場合にのみ true を返すステートメントを含む、論理 NOT ステートメントを使用してスコープダウンステートメントを設定します。

次の JSON リストは、このルール設定の例を示しています。

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 1000,
      "AggregateKeyType": "CONSTANT",
      "EvaluationWindowSec": 300,
      "ScopeDownStatement": {
        "NotStatement": {
          "Statement": {
            "SizeConstraintStatement": {
              "FieldToMatch": {
                "SingleHeader": {
                  "Name": "user-agent"
                }
              },
              "ComparisonOperator": "GT",
              "Size": 0,
              "TextTransformations": [
                {
                  "Type": "NONE",
                  "Priority": 0
                }
              ]
            }
          }
        }
      }
    }
  }
}
```

特定のラベルを使用してリクエストをレート制限する

複数のカテゴリのリクエストの数を制限するには、リクエストにラベルを追加する任意のルールまたはルールグループとレート制限を組み合わせることができます。そのためには、保護パック (ウェブ ACL) を次のように設定します。

- ラベルを追加するルールまたはルールグループを追加し、レート制限するリクエストがブロックまたは許可されないように設定します。マネージドルールグループを使用する場合、この動作を実現するために一部のルールグループのルールアクションを Count にオーバーライドすることが必要になる場合があります。
- ラベル付けルールとルールグループよりも高い優先度番号設定のレートベースのルールを保護パック (ウェブ ACL) に追加します。 は、最も低いものから順にルール AWS WAF を評価するため、レートベースのルールはラベル付けルールの後に実行されます。ルールのスコープダウンステートメントのラベル一致とラベル集約を組み合わせて、ラベルのレート制限を設定します。

次の例では、Amazon IP 評価リストの AWS Managed Rules ルールグループを使用します。このルールグループのルールである `AWSManagedIPDDoSList` は、IP が DDoS 攻撃に積極的に関与していることがわかっているリクエストを検出し、ラベルを付けます。ルールのアクションは、ルールグループ定義で Count に設定されています。ルールグループの詳細については、「the section called “Amazon IP 評価リスト”」を参照してください。

次の保護パック (ウェブ ACL) JSON リストでは、IP 評価ルールグループの後にラベル一致のレートベースのルールが続いています。レートベースのルールでは、スコープダウンステートメントを使用して、ルールグループのルールでマークされたリクエストをフィルタリングします。レートベースのルールステートメントは、フィルタリングされたリクエストを IP アドレスで集約してレート制限します。

```
{
  "Name": "test-web-acl",
  "Id": ...
  "ARN": ...
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesAmazonIpReputationList",
      "Priority": 0,
```

```
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesAmazonIpReputationList"
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesAmazonIpReputationList"
      }
    },
    {
      "Name": "test-rbr",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 100,
          "EvaluationWindowSec": 300,
          "AggregateKeyType": "IP",
          "ScopeDownStatement": {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList"
            }
          }
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "test-rbr"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
```

```
    "MetricName": "test-web-acl"
  },
  "Capacity": 28,
  "ManagedByFirewallManager": false,
  "RetrofittedByFirewallManager": false,
  "LabelNamespace": "awswaf:0000000000:webacl:test-web-acl:"
}
```

ラベル名前空間が指定されたラベルのリクエストをレート制限する

> **Note**
>
> Bot Control マネージドルールグループの共通レベルルールは、さまざまなカテゴリのボットにラベルを追加しますが、ブロックするのは未検証ボットからのリクエストに限ります。これらのルールの詳細については、「Bot Control のルールリスト」を参照してください。

Bot Control マネージドルールグループを使用する場合、個々の検証済みボットからのリクエストにレート制限を追加できます。そのためには、Bot Control ルールグループの後に実行されて、リクエストをボット名のラベル別に集約するレートベースのルールを追加します。[ラベル名前空間] 集約キーを指定し、名前空間キーを `awswaf:managed:aws:bot-control:bot:name:` と設定します。指定された名前空間を持つ一意のラベルはそれぞれ、集約インスタンスを定義します。例えば、`awswaf:managed:aws:bot-control:bot:name:axios` と `awswaf:managed:aws:bot-control:bot:name:curl` というラベルは、それぞれに集約インスタンスを定義します。

次の保護パック (ウェブ ACL) JSON リストは、この設定を示しています。この例のルールでは、単一のボット集約インスタンスに対するリクエストを 2 分間で最大 1,000 件に制限しています。

```
{
  "Name": "test-web-acl",
  "Id": ...
  "ARN": ...
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesBotControlRuleSet",
      "Priority": 0,
      "Statement": {
```

```
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesBotControlRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesBotControlRuleSet": {
                "InspectionLevel": "COMMON"
              }
            }
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesBotControlRuleSet"
      }
    },
    {
      "Name": "test-rbr",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 1000,
          "EvaluationWindowSec": 120,
          "AggregateKeyType": "CUSTOM_KEYS",
          "CustomKeys": [
            {
              "LabelNamespace": {
                "Namespace": "awswaf:managed:aws:bot-control:bot:name:"
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
```

```
        "MetricName": "test-rbr"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-web-acl"
  },
  "Capacity": 82,
  "ManagedByFirewallManager": false,
  "RetrofittedByFirewallManager": false,
  "LabelNamespace": "awswaf:0000000000:webacl:test-web-acl:"
}
```

特定の ASN を使用してリクエストをレート制限する

リクエストの IP アドレスに基づいて特定の AS 番号 (ASN)からのリクエスト数を制限するには、リクエスト集約を カスタムキー に設定し、集約基準を指定します。

次の JSON は、X-Forwarded-For ヘッダーにある転送された IP アドレスから派生した ASN を集計するルールの例を示しています。IP アドレスの形式が正しくないために が ASN を取得 AWS WAF できない場合、フォールバック動作は に設定されますMATCH。

```
{
    "Name": "test-rbr",
    "Priority": 0,
    "Statement": {
        "RateBasedStatement": {
            "AggregateKeyType": "CUSTOM_KEYS",
            "CustomKeys": [
                {
                    "ASN": {}
                },
                {
                    "ForwardedIP": {}
                }
            ],
            "EvaluationWindowSec": 300,
            "ForwardedIPConfig": {
                "FallbackBehavior": "MATCH",
                "HeaderName": "X-Forwarded-For"
            },
```

```
            "Limit": 2000
        }
    },
    "VisibilityConfig": {
        "CloudWatchMetricsEnabled": true,
        "MetricName": "test-rbr",
        "SampledRequestsEnabled": true
    }
}
```

レートベースのルールによってレート制限されている IP アドレスの一覧表示

このセクションでは、CLI、API、または任意の SDK を使用して、レートベースのルールによって現在レート制限されている IP アドレスのリストにアクセスする方法を調べる方法について説明します。

レートベースのルールが IP アドレスまたは転送された IP アドレスでのみ集計される場合、ルールが現在レート制限している IP アドレスのリストを取得できます。 は、これらの IP アドレスをルールのマネージドキーリストに AWS WAF 保存します。

> **Note**
>
> このオプションは、IP アドレスのみ、またはヘッダーの IP アドレスのみを集約する場合に限り使用できます。カスタムキーのリクエスト集約を使用する場合、カスタムキーでいずれかの IP アドレス仕様を使用しても、レート制限されている IP アドレスのリストは取得できません。

レートベースのルールは、そのルールのスコープダウンステートメントと一致する、ルールのマネージドキーリストからのリクエストにルールアクションを適用します。ルールにスコープダウンステートメントがない場合は、リストに含まれている IP アドレスからのすべてのリクエストにアクションが適用されます。ルールアクションはデフォルトで Block ですが、Allow を除く有効なルールアクションであればどれでもかまいません。単一のレートベースのルールインスタンスを使用して制限をレート AWS WAF できる IP アドレスの最大数は 10,000 です。10,000 を超えるアドレスがレート制限を超えると、 はレートが最も高いアドレス AWS WAF を制限します。

CLI、API、または任意の SDK を使用して、レートベースのルールのマネージドキーリストにアクセスできます。このトピックでは、CLI および API を使用したアクセスについて説明します。現時点では、コンソールからリストにアクセスすることはできません。

AWS WAF API の場合、コマンドは GetRateBasedStatementManagedKeys です。

AWS WAF CLI の場合、コマンドは get-rate-based-statement-managed-keys です。

Amazon CloudFront ディストリビューションの保護パック (ウェブ ACL) で使用されているレートベースのルールのレート制限されている IP アドレスのリストを取得する構文を次に示します。

```
aws wafv2 get-rate-based-statement-managed-keys --scope=CLOUDFRONT --region=us-east-1
 --web-acl-name=WebACLName --web-acl-id=WebACLId --rule-name=RuleName
```

以下は、リージョンアプリケーション、Amazon API Gateway REST API、Application Load Balancer、 AWS AppSync GraphQL API、Amazon Cognito ユーザープール、 AWS App Runner サービス AWS Amplify、Amazon Bedrock AgentCore Gateway、または AWS Verified Access インスタンスの構文を示しています。

```
aws wafv2 get-rate-based-statement-managed-keys --scope=REGIONAL --region=region --web-
acl-name=WebACLName --web-acl-id=WebACLId --rule-name=RuleName
```

AWS WAF は、ウェブリクエストをモニタリングし、保護パック (ウェブ ACL)、オプションのルールグループ、レートベースのルールの一意の組み合わせごとにキーを個別に管理します。例えば、ルールグループ内でレートベースのルールを定義してから、ウェブ ACL でルールグループを使用すると、 AWS WAF はウェブリクエストをモニタリングし、その保護パック (ウェブ ACL)、ルールグループ参照ステートメント、およびレートベースのルールインスタンスのキーを管理できます。2 番目の保護パック (ウェブ ACL) で同じルールグループを使用する場合、 はウェブリクエスト AWS WAF を監視し、この 2 番目の使用状況のキーを最初とは完全に独立して管理します。

ルールグループ内で定義したレートベースのルールの場合は、ルールグループ内の保護パック (ウェブ ACL) 名とレートベースのルール名に加えて、リクエストでルールグループ参照ステートメントの名前を指定する必要があります。レートベースのルールがルールグループ内で定義され、保護パック (ウェブ ACL) でルールグループが使用されるリージョンレベルのアプリケーションの構文を次に示します。

```
aws wafv2 get-rate-based-statement-managed-keys --scope=REGIONAL --region=region --web-
acl-name=WebACLName --web-acl-id=WebACLId --rule-group-rule-name=RuleGroupRuleName --
rule-name=RuleName
```

でのルールグループルールステートメントの使用 AWS WAF

> **Note**
>
> ルールグループのルールステートメントはネストできません。

このセクションでは、保護パック (ウェブ ACL) で使用できるルールグループのルールステートメントについて説明します。ルールグループの保護パック (ウェブ ACL) キャパシティーユニット (WCU) は、ルールグループの作成時にルールグループの所有者によって設定されます。WCU の詳細については、「のウェブ ACL キャパシティユニット (WCUs) AWS WAF」を参照してください。

ルールグループステートメント	説明	WCU
マネージドルールグループステートメントを使用する	指定されたマネージドルールグループで定義されているルールを実行します。 スコープダウンステートメントを追加することで、ルールグループで評価されるリクエストの範囲を絞り込むことができます。 マネージドルールグループステートメントは、他のステートメントタイプ内にネストできません。	ルールグループと、スコープダウンステートメント用の追加の WCU によって定義されます。
ルールグループステートメントの使用	管理するルールグループで定義されているルールを実行します。 独自のルールグループのルールグループ参照ステートメントにスコープダウンステート	WCU の制限は、ルールグループを作成するときに定義します。

ルールグループステートメント	説明	WCU
	メントを追加することはできません。 ルールグループステートメントは、他のステートメントタイプ内にネストできません。	

でのマネージドルールグループステートメントの使用 AWS WAF

このセクションでは、マネージドルールグループのルールステートメントの仕組みについて説明します。

マネージドルールグループルールステートメントは、保護パック (ウェブ ACL) ルールリストに含まれる参照をマネージドルールグループに追加します。コンソールのルールステートメントにはこのオプションは表示されませんが、保護パック (ウェブ ACL) の JSON 形式を操作しているときには、追加したマネージドルールグループがこのタイプとしてウェブ ACL ルールに表示されます。

マネージドルールグループは、 AWS マネージドルールルールグループのいずれかであり、そのほとんどは AWS WAF お客様が無料で利用できます AWS Marketplace 。有料の AWS マネージドルールルールグループを保護パック (ウェブ ACL) に追加すると、自動的にサブスクライブします。 AWS Marketplace マネージドルールグループは、 を通じてサブスクライブできます AWS Marketplace。詳細については、「でのマネージドルールグループの使用 AWS WAF」を参照してください。

ルールグループを保護パック (ウェブ ACL) に追加すると、グループ内のルールのアクションを Count またはその他のルールアクションにオーバーライドできます。詳細については、「でのルールグループアクションの上書き AWS WAF」を参照してください。

がルールグループで AWS WAF 評価するリクエストの範囲を絞り込むことができます。これを行うには、ルールグループステートメント内にスコープダウンステートメントを追加します。スコープダウンステートメントの詳細については、「でのスコープダウンステートメントの使用 AWS WAF」を参照してください。これは、ルールグループがトラフィックに与える影響を管理し、ルールグループを使用するときにトラフィック量に関連するコストを抑えるのに役立ちます。 AWS WAF Bot Control マネージドルールグループでスコープダウンステートメントを使用する情報と例については、「」を参照してくださいAWS WAF ボットコントロール。

ルールステートメントの特性

ネスト不可 - このステートメントタイプを他のステートメント内にネストしたり、ルールグループに含めたりすることはできません。このタイプは保護パック (ウェブ ACL) に直接含めることができます。

(オプション) スコープダウンステートメント – このルールタイプは、オプションのスコープダウンステートメントを使用して、ルールグループが評価するリクエストの範囲を絞り込みます。詳細については、「でのスコープダウンステートメントの使用 AWS WAF」を参照してください。

WCU - 作成時にルールグループに設定します。

このルールステートメントの場所

- コンソール - 保護パック (ウェブ ACL) の作成プロセス中に、[Add rules and rule groups] (ルールとルールグループの追加) ページで [Add managed rule groups] (マネージドルールグループの追加) を選択し、使用するルールグループを見つけて選択します。
- API – 「ManagedRuleGroupStatement」

でのルールグループステートメントの使用 AWS WAF

このセクションでは、ルールグループルールステートメントの仕組みについて説明します。

ルールグループルールステートメントは、保護パック (ウェブ ACL) ルールリストへの参照を、管理されているルールグループに追加します。コンソールのルールステートメントにはこのオプションは表示されませんが、保護パック (ウェブ ACL) の JSON 形式を操作しているときには、追加した独自のルールグループがこのタイプとして保護パック (ウェブ ACL) ルールに表示されます。独自のルールグループの使用については、「独自のルールグループの管理」を参照してください。

ルールグループを保護パック (ウェブ ACL) に追加すると、グループ内のルールのアクションを Count またはその他のルールアクションにオーバーライドできます。詳細については、「でのルールグループアクションの上書き AWS WAF」を参照してください。

ルールステートメントの特性

ネスト不可 - このステートメントタイプを他のステートメント内にネストしたり、ルールグループに含めたりすることはできません。このタイプは保護パック (ウェブ ACL) に直接含めることができます。

WCU - 作成時にルールグループに設定します。

このルールステートメントの場所

- コンソール - 保護パック (ウェブ ACL) の作成プロセス中に、[Add rules and rule groups] (ルールとルールグループの追加) ページで、[Add my own rules and rule groups] (独自のルールとルールグループの追加)、[Rule group] (ルールグループ) を選択し、使用するルールグループを追加します。
- API – 「RuleGroupReferenceStatement」

AWS WAF ルールグループ

このセクションでは、ルールグループとは、また、その仕組みについて説明します。

ルールグループは、保護パック (ウェブ ACL) に追加できる再利用可能なルールのセットです。保護パック (ウェブ ACL) の詳細については、「での保護の設定 AWS WAF」を参照してください。

ルールグループは、主に次のカテゴリに分類されます。

- ユーザー独自のルールグループは、ユーザーが作成して管理します。
- マネージドルールチームが作成および管理する AWS マネージドルールグループ。
- AWS Marketplace 販売者が作成および管理するマネージドルールグループ。
- AWS Firewall Manager や Shield Advanced などの他のサービスによって所有および管理されているルールグループ。

ルールグループと保護パック (ウェブ ACL) の相違点

ルールグループと保護パック (ウェブ ACL) には、どちらもルールが含まれています。ルールは、両方の場所で同じ方法で定義されます。ルールグループは、次の点で保護パック (ウェブ ACL) と異なります。

- ルールグループには、ルールグループ参照ステートメントを含めることはできません。
- 各保護パック (ウェブ ACL) にルールグループリファレンスステートメントを追加することで、複数の保護パック (ウェブ ACL) で 1 つのルールグループを再利用できます。保護パック (ウェブ ACL) を再利用することはできません。
- ルールグループにはデフォルトのアクションがありません。保護パック (ウェブ ACL) では、含めるルールまたはルールグループごとにデフォルトのアクションを設定します。ルールグループまたは保護パック (ウェブ ACL) 内の個々のルールには、アクションが定義されています。
- ルールグループを AWS リソースに直接関連付けることはありません。ルールグループを使用してリソースを保護するには、保護パック (ウェブ ACL) でルールグループを使用します。

- システムは、保護パック (ウェブ ACL) ごとに最大容量が 5,000 の保護パック (ウェブ ACL) キャパシティユニット (WCU) を定義します。各ルールグループには、作成時に設定する必要がある WCU 設定があります。この設定を使用して、ルールグループを使用して保護パック (ウェブ ACL) に追加される追加の容量要件を計算できます。WCU の詳細については、「のウェブ ACL キャパシティユニット (WCUs) AWS WAF」を参照してください。

ルールについては、「AWS WAF ルール」を参照してください。

このセクションでは、独自のルールグループを作成および管理するためのガイダンス、使用できるマネージドルールグループの説明、マネージドルールグループの使用に関するガイダンスを提供します。

トピック

- でのマネージドルールグループの使用 AWS WAF
- 独自のルールグループの管理
- AWS Marketplace ルールグループ
- 他のサービスによって提供されるルールグループを識別する

でのマネージドルールグループの使用 AWS WAF

このセクションでは、マネージドルールグループとは何か、そしてその仕組みについて説明します。

マネージドルールグループは、 ready-to-useルールのコレクションです。 AWS AWS Marketplace マネージドルールグループの使用には、基本 AWS WAF 料金が適用されます。 AWS WAF 料金情報については、AWS WAF 「 料金表」を参照してください。

- AWS WAF Bot Control、 AWS WAF Fraud Control アカウント乗っ取り防止 (ATP)、および AWS WAF Fraud Control アカウント作成不正防止 (ACFP) の AWS Managed Rules ルールグループは、基本料金以外の追加料金で利用できます AWS WAF 。料金の詳細については、「AWS WAF の料金」を参照してください。
- 他のすべての AWS マネージドルールルールグループは、追加料金なしで AWS WAF 利用できます。
- AWS Marketplace ルールグループは、 を通じてサブスクリプションで使用できます AWS Marketplace。これらのルールグループはそれぞれ、 AWS Marketplace 販売者によって所有および管理されます。 AWS Marketplace ルールグループを使用するための料金情報については、 AWS Marketplace 販売者にお問い合わせください。

一部のマネージドルールグループは、WordPress、Joomla、PHP などの特定のタイプのウェブアプリケーションを保護するために設計されています。「OWASP Top 10」にリストされているものを含め、既知の脅威や一般的なウェブアプリケーションの脆弱性に対する幅広い保護を提供するものもあります。PCI や HIPAA などの規制の遵守が必要な場合は、マネージドルールグループを使用してウェブアプリケーションファイアウォールの要件を満たすことができます。

自動更新

絶えず変化する脅威の状況に遅れずについていくには、時間とコストがかかることがあります。マネージドルールグループを使用すると、 AWS WAFを実装して使用する際の時間を節約できます。多くの AWS および AWS Marketplace 販売者は、新しい脆弱性や脅威が発生すると、マネージドルールグループを自動的に更新し、新しいバージョンのルールグループを提供します。

場合によっては、多くのプライベート開示コミュニティへの参加により、 AWS は公開前に新しい脆弱性について通知されます。このような場合、新しい脅威が広く知られる前でも、 は AWS マネージドルールのルールグループを更新してデプロイ AWS できます。

マネージドルールグループのルールへの制限付きアクセス

各マネージドルールグループには、どのようなタイプの攻撃や脆弱性に対して保護するように設計されているかが包括的に定義されています。ルールグループプロバイダーの知的財産を保護するために、ルールグループ内の個々のルールのすべての詳細を表示することはできません。この制限は、悪意のあるユーザーが公開されたルールを特に回避する脅威を設計するのを防ぐのにも役立ちます。

トピック

- でのバージョニングされたマネージドルールグループの使用 AWS WAF
- マネージドルールグループの使用
- AWS の マネージドルール AWS WAF

でのバージョニングされたマネージドルールグループの使用 AWS WAF

このセクションでは、マネージドルールグループのバージョニングの処理方法について説明します。

多くのマネージドルールグループプロバイダーはバージョニングを利用して、ルールグループのオプションと機能を更新します。通常、マネージドルールグループの特定のバージョンは静的です。場合によっては、例えば新しいセキュリティの脅威に対応するために、プロバイダーがマネージドルールグループの静的バージョンの一部または全部を更新する必要がある場合があります。

保護パック (ウェブ ACL) でバージョニングされたマネージドルールグループを使用する場合、デフォルトバージョンを選択し、使用する静的バージョンをプロバイダーに管理させるか、特定の静的バージョンを選択できます。

必要なバージョンが見つかりませんか?

ルールグループのバージョン一覧にバージョンが表示されない場合は、そのバージョンの有効期限の失効が予定されているか、すでに期限切れになっている可能性があります。バージョンの有効期限がスケジュールされると、 ではルールグループにバージョンを選択 AWS WAF できなくなります。

AWS マネージドルールルールグループの SNS 通知

AWS マネージドルールルールグループはすべて、IP 評価ルールグループを除き、バージョニングと SNS 更新の通知を提供します。通知を提供する AWS マネージドルールルールグループは、すべて同じ SNS トピックの Amazon リソースネーム (ARN) を使用します。SNS 通知にサインアップするには、新しいバージョンとアップデートの通知を受け取る を参照してください。

トピック

- マネージドルールグループのバージョンライフサイクル
- マネージドルールグループのバージョンの有効期限
- マネージドルールグループのバージョン処理に関するベストプラクティス

マネージドルールグループのバージョンライフサイクル

プロバイダーは、マネージドルールグループの静的バージョンの次のライフサイクルステージを処理します。

- リリースとアップデート – マネージドルールグループのプロバイダーは、Amazon Simple Notification Service (Amazon SNS) トピックに対する通知を通じて、マネージドルールグループの今後のバージョンと新しい静的バージョンを知らせます。また、プロバイダーは、緊急時の必須の更新など、ルールグループに関するその他の重要な情報を伝達するためにトピックを使用する場合もあります。

  ルールグループのトピックをサブスクライブし、通知の受信方法を設定できます。詳細については、「新しいバージョンとアップデートの通知を受け取る」を参照してください。
- 有効期限のスケジュール – マネージドルールグループのプロバイダーは、古いバージョンのルールグループの有効期限をスケジュールします。失効予定のバージョンは、保護パック (ウェブ ACL) ルールに追加できません。バージョンの有効期限がスケジュールされると、 は Amazon CloudWatch のカウントダウンメトリクスを使用して有効期限 AWS WAF を追跡します。

- バージョンの有効期限 – マネージドルールグループの期限切れバージョンを使用するように保護パック (ウェブ ACL) を設定している場合、保護パック (ウェブ ACL) の評価中に、 はルールグループのデフォルトバージョン AWS WAF を使用します。さらに、 は、ルールグループを削除しない、またはそのバージョンを有効期限が切れていないものに変更しない保護パック (ウェブ ACL) の更新を AWS WAF ブロックします。

AWS Marketplace マネージドルールグループを使用する場合は、バージョンライフサイクルに関する追加情報をプロバイダーに依頼してください。

マネージドルールグループのバージョンの有効期限

このセクションでは、バージョニングされたマネージドルールグループでバージョンの有効期限がどのように機能するかについて説明します。

ルールグループの特定のバージョンを使用する場合は、有効期限切れのバージョンを使用し続けないようにしてください。バージョンの有効期限は、ルールグループの SNS 通知と Amazon CloudWatch メトリクスを通じてモニタリングできます。

保護パック (ウェブ ACL) で使用しているバージョンの有効期限が切れている場合、 は、ルールグループの有効期限が切れていないバージョンへの移行を含まない保護パック (ウェブ ACL) の更新を AWS WAF ブロックします。ルールグループを使用可能なバージョンに更新するか、保護パック (ウェブ ACL) から削除できます。

マネージドルールグループの有効期限の処理は、ルールグループプロバイダーによって異なります。AWS マネージドルールのルールグループの場合、期限切れになったバージョンはルールグループのデフォルトバージョンに自動的に変更されます。 AWS Marketplace ルールグループについては、プロバイダーに有効期限の処理方法を尋ねます。

プロバイダーは、ルールグループの新しいバージョンを作成するときに、バージョンの予測される有効期間を設定します。このバージョンは有効期限が切れるようにスケジュールされていませんが、Amazon CloudWatch メトリクス値は予測されたライフタイムに設定されており、CloudWatch でメトリクスのフラット値が表示されます。プロバイダーがメトリクスの有効期限をスケジュールすると、メトリクス値は有効期限の到来時にゼロになるまで、毎日減少します。モニタリング有効期限の詳細については、バージョンの有効期限の追跡 を参照してください。

マネージドルールグループのバージョン処理に関するベストプラクティス

バージョン管理されたマネージドルールグループを使用する場合は、このベストプラクティスのガイダンスに従ってバージョニングを行ってください。

保護パック (ウェブ ACL) でマネージドルールグループを使用する場合は、ルールグループの特定の静的バージョンを使用するか、デフォルトバージョンを使用するように選択できます。

- デフォルトバージョン – AWS WAF 常にデフォルトバージョンをプロバイダーが現在推奨している静的バージョンに設定します。推奨される静的バージョンをプロバイダーが更新すると、 AWS WAF は、保護パック (ウェブ ACL) のルールグループのデフォルトバージョンの設定を自動的に更新します。

  マネージドルールグループのデフォルトバージョンを使用する場合は、ベストプラクティスとして次の手順を実行します。

  - 通知をサブスクライブする – ルールグループへの変更に関する通知をサブスクライブし、それらを監視します。ほとんどのプロバイダーは、新しい静的バージョンとデフォルトバージョンの変更について事前通知を送信します。これにより、 が AWS デフォルトバージョンを切り替える前に、新しい静的バージョンの影響を確認できます。詳細については、「新しいバージョンとアップデートの通知を受け取る」を参照してください。
  - デフォルトを新しい静的バージョンに設定する前に、その影響を確認し、必要に応じて調整する – デフォルトを新しい静的バージョンに設定する前に、ウェブリクエストのモニタリングと管理に対する静的バージョンの影響を確認します。新しい静的バージョンには、確認する新しいルールが含まれている可能性があります。ルールグループの使用方法を変更する必要がある場合に備えて、誤検出やその他の予期しない動作を見つけます。例えば、新しい動作の処理方法を把握しながら、トラフィックをブロックしないようにするために、ルールをカウントに設定できます。詳細については、「AWS WAF 保護のテストとチューニング」を参照してください。
- 静的バージョン – 静的バージョンを使用する場合は、ルールグループの新しいバージョンを採用する準備ができたら、バージョン設定を手動で更新する必要があります。

  マネージドルールグループの静的バージョンを使用する場合は、ベストプラクティスとして次の手順を実行します。

  - バージョンを最新の状態に保つ – マネージドルールグループを可能な限り最新バージョンに近いものにします。新しいバージョンがリリースされたら、それをテストし、必要に応じて設定を調整し、適時に実装してください。テストについては、「AWS WAF 保護のテストとチューニング」を参照してください。
  - 通知をサブスクライブする – ルールグループに対する変更に関する通知をサブスクライブして、プロバイダーが新しい静的バージョンをいつリリースするかを把握します。ほとんどのプロバイダーは、バージョン変更に関する事前の通知を提供します。さらに、セキュリティホールをふさぐため、またはその他の緊急の理由で、使用している静的バージョンをプロバイダーが更新する必要がある場合があります。プロバイダーの通知をサブスクライブすると、状況について知

ることができます。詳細については、「新しいバージョンとアップデートの通知を受け取る」を参照してください。

- [Avoid version expiration] (バージョンの有効期限切れを回避する) - これ使用している間は、静的バージョンの有効期限が切れないようにします。期限切れのバージョンのプロバイダーによる処理はさまざまであり、使用可能なバージョンへのアップグレードの強制や、予期しない結果をもたらす可能性のあるその他の変更が含まれる場合があります。 AWS WAF 有効期限メトリクスを追跡し、サポートされているバージョンに正常にアップグレードするのに十分な日数を提供するアラームを設定します。詳細については、「バージョンの有効期限の追跡」を参照してください。

マネージドルールグループの使用

このセクションでは、マネージドルールグループにアクセスして管理するためのガイダンスを提供します。

マネージドルールグループを保護パック (ウェブ ACL) に追加すると、独自のルールグループと同じ設定オプションに加えて、追加設定を選択できます。

コンソールで、保護パック (ウェブ ACL) でルールを追加および編集するプロセス中に、マネージドルールグループの情報にアクセスします。API とコマンドラインインターフェイス (CLI) を通じて、マネージドルールグループの情報を直接リクエストできます。

保護パック (ウェブ ACL) でマネージドルールグループを使用する場合、次の設定を編集できます。

- [Version] (バージョン) – これは、ルールグループがバージョン管理されている場合にのみ使用できます。詳細については、「でのバージョニングされたマネージドルールグループの使用 AWS WAF」を参照してください。
- ルールアクションのオーバーライド – ルールグループ内のルールのアクションを任意のアクションにオーバーライドできます。Count に設定すると、ルールグループを使用してウェブリクエストを管理する前に、そのルールグループをテストするときに便利です。詳細については、「ルールグループのルールアクションの上書き」を参照してください。
- [Scope-down statement] (スコープダウンステートメント) – スコープダウンステートメントを追加して、ルールグループで評価したくないウェブリクエストを除外できます。詳細については、「でのスコープダウンステートメントの使用 AWS WAF」を参照してください。
- [Override rule group action] (ルールグループアクションを上書き) – ルールグループ評価の結果として生じるアクションを上書きして、Count のみに設定できます。このオプションは、一般的に使

用されません。がルールグループ内のルール AWS WAF を評価する方法は変更されません。詳細については、「ルールグループの戻り値アクションを Count に上書き」を参照してください。

保護パック (ウェブ ACL) でマネージドルールグループの設定を編集するには

- コンソール
  - (オプション) マネージドルールグループを保護パック (ウェブ ACL) に追加する場合、[Edit] (編集) を選択して、設定を表示および編集できます。
  - (オプション) マネージドルールグループを保護パック (ウェブ ACL) に追加したら、[保護パック (ウェブ ACL)] ページから、作成したばかりの保護パック (ウェブ ACL) を選択します。これにより、保護パック (ウェブ ACL) 編集ページが表示されます。
    - [Rules] (ルール) を選択します。
    - ルールグループを選択し、[Edit] (編集) を選択して、設定を表示および編集します。
- API および CLI - コンソールの外部で保護パック (ウェブ ACL) を作成および更新するときに、マネージドルールグループの設定を管理できます。

マネージドルールグループのリストの取得

保護パック (ウェブ ACL) で使用可能なマネージドルールグループのリストを取得できます。このリストには、以下が含まれます。

- すべての AWS マネージドルールルールグループ。
- サブスクライブしている AWS Marketplace ルールグループ。

> **Note**
>
> AWS Marketplace ルールグループへのサブスクライブの詳細については、「」を参照してくださいAWS Marketplace ルールグループ。

マネージドルールグループのリストを取得すると、返されるリストは、使用しているインターフェイスによって異なります。

- コンソール – コンソールでは、まだサブスクライブしていないルールグループを含む、すべてのマネージド AWS Marketplace ルールグループを表示できます。まだサブスクライブしていないものについては、インターフェイスにサブスクライブするためのリンクが用意されています。

- API および CLI - コンソールの外部では、リクエストは使用可能なルールグループのみを返します。

マネージドルールグループのリストを取得するには

- コンソール - ウェブ ACL の作成プロセス 中に、[Add rules and rule groups] (ルールとルールグループの追加) ページで [Add managed rule groups] (マネージドルールグループの追加) を選択します。最上位レベルには、プロバイダー名が一覧表示されます。各プロバイダーリストを展開して、マネージドルールグループのリストを表示します。バージョン対応ルールグループでは、このレベルで表示される情報はデフォルトバージョンの情報です。マネージドルールグループを保護パック (ウェブ ACL) に追加すると、コンソールに命名スキーム `<Vendor Name>-<Managed Rule Group Name>` に基づいて一覧表示されます。
- API –
  - `ListAvailableManagedRuleGroups`
- CLI –
  - `aws wafv2 list-available-managed-rule-groups --scope=<CLOUDFRONT|REGIONAL>`

マネージドルールグループのルールの取得

マネージドルールグループ内のルールのリストを取得できます。API コールと CLI コールは、JSON モデルまたは で参照できるルール仕様を返します AWS CloudFormation。

マネージドルールグループ内のルールの一覧を取得するには

- コンソール
  - (オプション) マネージドルールグループを保護パック (ウェブ ACL) に追加する場合、[Edit] (編集) を選択してルールを表示できます。
  - (オプション) マネージドルールグループを保護パック (ウェブ ACL) に追加したら、[保護パック (ウェブ ACL)] ページから、作成したばかりの保護パック (ウェブ ACL) を選択します。これにより、保護パック (ウェブ ACL) 編集ページが表示されます。
    - [Rules] (ルール) を選択します。
    - ルールリストを表示するルールグループを選択し、Edit を選択します。ルールグループ内のルールのリスト AWS WAF を表示します。
- API – `DescribeManagedRuleGroup`

- CLI – `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

マネージドルールグループで使用可能なバージョンの取得

マネージドルールグループの利用可能なバージョンは、まだ期限切れになる予定がないバージョンです。このリストは、ルールグループの現在のデフォルトバージョンであるバージョンを示します。

マネージドルールグループの使用可能なバージョンのリストを取得するには

- コンソール
  - (オプション) マネージドルールグループを保護パック (ウェブ ACL) に追加する場合は、[Edit] (編集) を選択して、ルールグループの情報を表示します。[Version] (バージョン) ドロップダウンを展開して、使用可能なバージョンのリストを表示します。
  - (オプション) マネージドルールグループを保護パック (ウェブ ACL) に追加したら、保護パック (ウェブ ACL) で [Edit] (編集) を選択し、ルールグループルールを選択して編集します。[Version] (バージョン) ドロップダウンを展開して、使用可能なバージョンのリストを表示します。
- API –
  - `ListAvailableManagedRuleGroupVersions`
- CLI –
  - `aws wafv2 list-available-managed-rule-group-versions --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

コンソールを通じた保護パック (ウェブ ACL) へのマネージドルールグループの追加

このセクションでは、コンソールを使用してマネージドルールグループを保護パック (ウェブ ACL) に追加する方法を説明します。このガイダンスは、すべての AWS マネージドルールルールグループと、サブスクライブしている AWS Marketplace ルールグループに適用されます。

⚠ 本番稼働トラフィックのリスク

本番稼働トラフィックの保護パック (ウェブ ACL) に変更をデプロイする前に、ステージング環境またはテスト環境でテストおよびチューニングしてトラフィックへの潜在的な影響を確認します。その後、更新したルールを有効にする前に、本番稼働用トラフィックでカウント

モードでルールをテストしてチューニングします。ガイダンスについては、「AWS WAF 保護のテストとチューニング」を参照してください。

> **Note**
>
> 保護パック (ウェブ ACL) で 1,500 WCU を超える容量を使用すると、保護パック (ウェブ ACL) の基本料金を超えるコストが発生します。詳細については、「のウェブ ACL キャパシティユニット (WCUs) AWS WAF」と「AWS WAF 料金表」を参照してください。

コンソールで保護パック (ウェブ ACL) にマネージドルールグループを追加するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで [保護パック (ウェブ ACL)] を選択します。
3. [保護パック (ウェブ ACL)] ページで、保護パック (ウェブ ACL) のリストから、ルールグループを追加する保護パック (ウェブ ACL) を選択します。これにより、単一の保護パック (ウェブ ACL) のページが表示されます。
4. 保護パック (ウェブ ACL) ページで、[ルール] タブを選択します。
5. [Rules] (ルール) ペインで、[Add rules] (ルールを追加) を選択してから、[Add managed rule groups] (マネージドルールグループを追加) を選択します。
6. [Add managed rule groups] (マネージドルールグループを追加) ページで、ルールグループのベンダーの選択を展開して、使用可能なルールグループのリストを表示します。
7. 追加するルールグループごとに、[保護パック (ウェブ ACL) に追加] を選択します。ルールグループの保護パック (ウェブ ACL) の設定を変更する場合は、[編集] を選択し、変更を加えてから、[ルールを保存] を選択します。オプションの詳細については、でのバージョニングされたマネージドルールグループの使用 AWS WAF のバージョニングに関するガイダンス、および でのマネージドルールグループステートメントの使用 AWS WAF の保護パック (ウェブ ACL) でのマネージドルールグループの使用に関するガイダンスを参照してください。
8. [Add managed rule groups] (マネージドルールグループを追加) ページの下部で、[Add rules] (ルールを追加) を選択します。
9. [Set rule priority] (ルールの優先度を設定) ページで、必要に応じてルールが実行される順序を調整し、[Save] (保存) を選択します。詳細については、「ルールの優先度を設定する」を参照してください。

保護パック (ウェブ ACL) のページで、追加したマネージドルールグループが [ルール] タブに一覧表示されます。

本番トラフィックに使用する前に、 AWS WAF 保護の変更をテストして調整します。詳細については、「AWS WAF 保護のテストとチューニング」を参照してください。

更新中の一時的な不一致

保護パック (ウェブ ACL) または他の AWS WAF リソースを作成または変更すると、リソースが保存されているすべての領域にその変更が反映されるまでに少し時間がかかります。伝播時間は、数秒から数分までかかります。

次の内容では、変更伝播中に直面する一時的な不整合性の例を紹介します。

- 保護パック (ウェブ ACL) を作成した後、それをリソースに関連付けようとすると、保護パック (ウェブ ACL) が利用できないことを示す例外が表示される場合があります。
- ルールグループを保護パック (ウェブ ACL) に追加した後、新しいルールグループのルールは、保護パック (ウェブ ACL) が使用されるエリアで有効になり、別のエリアでは有効にならない場合があります。
- ルールのアクション設定を変更した後、古いアクションを一部のエリアで確認され、新しいアクションを別のエリアで確認される場合があります。
- ブロックルールで使用されている IP セットに IP アドレスを追加した後、新しいアドレスはあるエリアではブロックされ、別のエリアでは許可される場合があります。

マネージドルールグループに対する新しいバージョンと更新の通知を受け取る

このセクションでは、新しいバージョンと更新に関する Amazon SNS 通知を受信する方法について説明します。

マネージドルールグループプロバイダーは、SNS 通知を使用して、今後の新しいバージョンや緊急のセキュリティアップデートなどのルールグループの変更を知らせます。

SNS 通知をサブスクライブするには

ルールグループの通知をサブスクライブするには、米国東部 (バージニア北部) リージョン us-east-1 のルールグループの Amazon SNS トピック ARN の Amazon SNS サブスクリプションを作成します。

サブスクライブする方法については、「Amazon Simple Notification Service デベロッパーガイド」を参照してください。

> **Note**
>
> SNS トピックのサブスクリプションを、us-east-1 リージョンでのみ作成します。

バージョニングされた AWS マネージドルールルールグループはすべて、同じ SNS トピックの Amazon リソースネーム (ARN) を使用します。 AWS マネージドルールのルールグループ通知の詳細については、「」を参照してくださいデプロイ通知。

マネージドルールグループの Amazon SNS トピック ARN を確認できる場所

AWS マネージドルールルールグループは 1 つの SNS トピック ARN を使用するため、いずれかのルールグループからトピック ARN を取得してサブスクライブし、SNS 通知を提供するすべての AWS マネージドルールルールルールグループの通知を取得できます。

- コンソール
  - (オプション) マネージドルールグループを保護パック (ウェブ ACL) に追加する場合は、[Edit] (編集) を選択して、ルールグループの Amazon SNS トピック ARN を含むルールグループの情報を表示します。
  - (オプション) マネージドルールグループを保護パック (ウェブ ACL) に追加したら、保護パック (ウェブ ACL) で [Edit] (編集) を選択し、ルールグループのルールを選択して編集し、ルールグループの Amazon SNS トピック ARN を表示します。
- API – `DescribeManagedRuleGroup`
- CLI – `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Amazon SNS 通知形式に関する一般的な情報と、受信する通知をフィルタリングする方法については、「Amazon Simple Notification Service デベロッパーガイド」の「メッセージ形式を解析する」と「Amazon SNS サブスクリプションフィルターポリシー」を参照してください。

ルールグループのバージョンの有効期限の追跡

このセクションでは、Amazon CloudWatch を介したマネージドルールグループの有効期限スケジュールをモニタリングする方法について説明します。

ルールグループの特定のバージョンを使用する場合は、有効期限切れのバージョンを使用し続けないようにしてください。

> **Tip**
>
> マネージドルールグループの Amazon SNS 通知にサインアップし、マネージドルールグループバージョンで最新の状態を維持します。ルールグループからの最新の保護により、有効期限を先取りできます。詳細については、「新しいバージョンとアップデートの通知を受け取る」を参照してください。

Amazon CloudWatch を使用してマネージドルールグループの有効期限スケジュールをモニタリングするには

1. CloudWatch で、マネージドルールグループの の有効期限メトリクスを見つけ AWS WAF ます。メトリクスには、以下のメトリック名とディメンションがあります:
   - メトリクス名: DaysToExpiry
   - メトリクスのディメンション: Region、ManagedRuleGroup、Vendor、および Version

   トラフィックを評価する保護パック (ウェブ ACL) にマネージドルールグループがある場合、そのメトリクスが取得されます。このメトリクスは、使用されていないルールグループでは使用できません。
2. 関心のあるメトリクスにアラームを設定して、新しいバージョンのルールグループに切り替えるよう通知を適時に受け取れるようにします。

Amazon CloudWatch メトリクスの使用とアラームの設定については、「Amazon CloudWatch ユーザーガイド」を参照してください。

JSON および YAML でのマネージドルールグループ設定の例

このセクションでは、マネージドルールグループの設定の例を紹介します。

API コールと CLI コールは、JSON モデルまたは で参照できるマネージドルールグループ内のすべてのルールのリストを返します AWS CloudFormation。

JSON

JSON を使用して、ルールステートメント内でマネージドルールグループを参照および変更できます。次のリストは、 AWS マネージドルールルールグループ を JSON 形式で示`AWSManagedRulesCommonRuleSet`しています。RuleActionOverrides 仕様には、アクションが Count にオーバーライドされたルールが一覧表示されています。

```
{
    "Name": "AWS-AWSManagedRulesCommonRuleSet",
    "Priority": 0,
    "Statement": {
      "ManagedRuleGroupStatement": {
        "VendorName": "AWS",
        "Name": "AWSManagedRulesCommonRuleSet",
        "RuleActionOverrides": [

          {

            "ActionToUse": {

              "Count": {}

            },

            "Name": "NoUserAgent_HEADER"

          }

        ],
        "ExcludedRules": []
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSManagedRulesCommonRuleSet"
    }
}
```

YAML

CloudFormation YAML テンプレートを使用して、ルールステートメント内のマネージドルールグループを参照および変更できます。次のリストは、 AWSManagedRulesCommonRuleSet CloudFormation テンプレート内の AWS マネージドルールルールグループ を示しています。RuleActionOverrides 仕様には、アクションが Count にオーバーライドされたルールが一覧表示されています。

```
Name: AWS-AWSManagedRulesCommonRuleSet
Priority: 0
Statement:
  ManagedRuleGroupStatement:
    VendorName: AWS
    Name: AWSManagedRulesCommonRuleSet
    RuleActionOverrides:
    - ActionToUse:
        Count: {}
      Name: NoUserAgent_HEADER
    ExcludedRules: []
OverrideAction:
  None: {}
VisibilityConfig:
  SampledRequestsEnabled: true
  CloudWatchMetricsEnabled: true
  MetricName: AWS-AWSManagedRulesCommonRuleSet
```

AWS の マネージドルール AWS WAF

このセクションでは、 の AWS マネージドルールについて説明します AWS WAF 。

AWS の マネージドルール AWS WAF は、アプリケーションの脆弱性やその他の不要なトラフィックに対する保護を提供するマネージドサービスです。最大保護パック (ウェブ ACL) 容量単位 (WCU) の制限まで、ウェブ ACL ごとに AWS マネージドルールから 1 つ以上のルールグループを選択できます。

誤検出の軽減とルールグループの変更のテスト

本番稼働でルールグループを使用する前に、AWS WAF 保護のテストとチューニング にあるガイダンスに従って、非本番稼働環境でテストします。保護パック (ウェブ ACL) にルールグループを追加する場合、新しいバージョンのルールグループをテストする場合、およびルールグループが必要に応じてウェブトラフィックを処理していないときは、テストとチューニングのガイダンスに従ってください。

セキュリティ責任の共有

AWS マネージドルールは、一般的なウェブ脅威から保護するように設計されています。ドキュメントに従って使用すると、 AWS マネージドルールルールグループはアプリケーションに別のセキュリティレイヤーを追加します。ただし、 AWS マネージドルールルールグループは、選択した AWS リ

ソースによって決定されるセキュリティ責任に代わるものではありません。責任共有モデルを参照して、 のリソースが適切に保護 AWS されていることを確認します。

> **Important**
>
> AWS マネージドルールは、一般的なウェブ脅威から保護するように設計されています。ドキュメントに従って使用すると、 AWS マネージドルールルールグループはアプリケーションに別のセキュリティレイヤーを追加します。ただし、 AWS マネージドルールルールグループは、選択した AWS リソースによって決定されるセキュリティ責任に代わるものではありません。責任共有モデルを参照して、 のリソースが適切に保護 AWS されていることを確認します。

AWS マネージドルールのルールグループリスト

このセクションでは、使用可能な AWS マネージドルールルールグループのリストを示します。

このセクションでは、 AWS マネージドルールルールグループの最新バージョンについて説明します。これらの情報は、保護パック (ウェブ ACL) にマネージドルールグループを追加するときにコンソールに表示されます。API を使用して、 を呼び出すことで、サブスクライブしている AWS Marketplace ルールグループとともにこのリストを取得できますListAvailableManagedRuleGroups。

> **Note**
>
> AWS マネージドルールのルールグループのバージョンを取得する方法については、「」を参照してくださいマネージドルールグループで使用可能なバージョンの取得。

すべての AWS マネージドルールルールグループはラベル付けをサポートし、このセクションのルールリストにはラベル仕様が含まれています。DescribeManagedRuleGroup を呼び出すことにより、API を介してマネージドルールグループのラベルを取得できます。ラベルは、応答の AvailableLabels プロパティにリストされています。ラベル付けの詳細については、「でのウェブリクエストのラベル付け AWS WAF」を参照してください。

本番トラフィックに使用する前に、 AWS WAF 保護の変更をテストして調整します。詳細については、「AWS WAF 保護のテストとチューニング」を参照してください。

AWS マネージドルールのルールグループ

- ベースラインルールグループ
  - コアルールセット (CRS) マネージドルールグループ
  - 管理者保護マネージドルールグループ
  - 既知の不正な入力マネージドルールグループ
- ユースケース固有のルールグループ
  - SQL データベースマネージドルールグループ
  - Linux オペレーティングシステムマネージドルールグループ
  - POSIX オペレーティングシステムマネージドルールグループ
  - Windows オペレーティングシステムマネージドルールグループ
  - PHP アプリケーションマネージドルールグループ
  - WordPress アプリケーションマネージドルールグループ
- IP 評価ルールグループ
  - Amazon IP 評価リストマネージドルールグループ
  - 匿名 IP リストマネージドルールグループ
- AWS WAF Fraud Control アカウント作成不正防止 (ACFP) ルールグループ
  - このルールグループの使用に関する考慮事項
  - このルールグループによって追加されるラベル
    - トークンラベル
    - ACFP ラベル
  - Account Creation Fraud Prevention ルールリスト
- AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループ
  - このルールグループの使用に関する考慮事項
  - このルールグループによって追加されるラベル
    - トークンラベル
    - ATP ラベル
  - アカウント乗っ取り防止のルールリスト
- AWS WAF Bot Control ルールグループ
  - 保護レベル
  - このルールグループの使用に関する考慮事項
  - このルールグループによって追加されるラベル

    - トークンラベル
    - Bot Control ラベル
  - Bot Control のルールリスト
- AWS WAF 分散サービス拒否 (DDoS) 防止ルールグループ
  - このルールグループの使用に関する考慮事項
  - このルールグループによって追加されるラベル
    - トークンラベル
    - DDoS 対策ラベル
  - DDoS 対策ルールのリスト

ベースラインルールグループ

ベースラインマネージドルールグループは、さまざまな一般的な脅威に対する一般的な保護を提供します。これらのルールグループを 1 つ以上選択して、リソースのベースライン保護を確立します。

コアルールセット (CRS) マネージドルールグループ

VendorName: `AWS`、名前: `AWSManagedRulesCommonRuleSet`、WCU: 700

> **Note**
>
> このドキュメントでは、このマネージドルールグループの最新の静的バージョンリリースについて説明します。バージョンの変更は、AWS マネージドルールの変更ログ の変更ログにレポートされます。他のバージョンの情報については、API コマンド DescribeManagedRuleGroup を使用してください。
> AWS マネージドルールルールのルールグループでルール用に公開する情報は、不正なアクターにルールを回避するために必要なものを与えることなく、ルールを使用するために必要なものを提供することを目的としています。
> ここに記載されている以上の情報が必要な場合は、AWS サポート センター にお問い合わせください。

コアルールセット (CRS) ルールグループには、ウェブアプリケーションに一般的に適用可能なルールが含まれています。これにより、OWASP Top 10 などの OWASP の出版物に記載されている、リスクが高く一般的に発生するいくつかの脆弱性を含む、さまざまな脆弱性の悪用に対する保護が提供されます。 AWS WAF ユースケースには、このルールグループの使用を検討してください。

このマネージドルールグループは、評価対象のウェブリクエストに保護パック (ウェブ ACL) 内のこのルールグループの後に実行されるルールでも使用できるラベルを追加します。 AWS WAF は、Amazon CloudWatch メトリクスにもラベルを記録します。ラベルとラベルメトリクスに関する一般的な情報については、「ウェブリクエストのラベル付け」および「ラベルメトリクスとディメンション」を参照してください。

ルール名	説明とラベル
`NoUserAgent_HEADER`	HTTP `User-Agent` ヘッダーが欠落しているリクエストを検査します。 ルールアクション: Block ラベル: `awswaf:managed:aws:core-rule-set:NoUserAgent_Header`
`UserAgent_BadBots_HEADER`	リクエストが不正なボットであることを示す一般的な `User-Agent` ヘッダー値を検査します。パターンの例には、nessus、nmap などがあります。ボット管理については、「AWS WAF Bot Control ルールグループ」も参照してください。 ルールアクション: Block ラベル: `awswaf:managed:aws:core-rule-set:BadBots_Header`
`SizeRestrictions_QUERYSTRING`	2,048 バイトを超える URI クエリ文字列を検査します。 ルールアクション: Block ラベル: `awswaf:managed:aws:core-rule-set:SizeRestrictions_QueryString`

ルール名	説明とラベル
SizeRestrictions_Cookie_HEADER	10,240 バイトを超える cookie ヘッダーを検査します。 ルールアクション: Block ラベル: awswaf:managed:aws:core-rule-set:SizeRestrictions_Cookie_Header
SizeRestrictions_BODY	8 KB (8,192 バイト) を超えるリクエストボディを検査します。 ルールアクション: Block ラベル: awswaf:managed:aws:core-rule-set:SizeRestrictions_Body
SizeRestrictions_URIPATH	1,024 バイトを超える URI パスを検査します。 ルールアクション: Block ラベル: awswaf:managed:aws:core-rule-set:SizeRestrictions_URIPath

ルール名	説明とラベル
`EC2MetaDataSSRF_BODY`	リクエストボディから Amazon EC2 メタデータを盗み出す試みがないかを検査します。 **Warning** このルールは、保護パック (ウェブ ACL) とリソースタイプのボディサイズ制限に達するリクエストボディのみを検査します。Application Load Balancer および の場合 AWS AppSync、制限は 8 KB に固定されます。CloudFront、API Gateway、Amazon Cognito、App Runner、Verified Access、Amazon Bedrock AgentCore Gateway の場合、デフォルトの制限は 16 KB であり、保護パック (ウェブ ACL) 設定で制限を最大 64 KB に増やすことができます。このルールは、オーバーサイズコンテンツの処理に `Continue` オプションを使用します。詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。 ルールアクション: Block ラベル: `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_Body`

ルール名	説明とラベル
EC2MetaDataSSRF_COOKIE	リクエスト cookie から Amazon EC2 メタデータを盗み出す試みがないかを検査します。 ルールアクション: Block ラベル: awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_Cookie
EC2MetaDataSSRF_URIPATH	リクエスト URI パスから Amazon EC2 メタデータを盗み出す試みがないかを検査します。 ルールアクション: Block ラベル: awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_URIPath
EC2MetaDataSSRF_QUERYARGUMENTS	リクエストクエリ引数から Amazon EC2 メタデータを盗み出す試みがないかを検査します。 ルールアクション: Block ラベル: awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_QueryArguments
GenericLFI_QUERYARGUMENTS	クエリ引数に、ローカルファイルインクルージョン (LFI) を悪用する形跡がないかを検査します。例には、../../ などの手法を使用したパストラバーサルの試行があります。 ルールアクション: Block ラベル: awswaf:managed:aws:core-rule-set:GenericLFI_QueryArguments

ルール名	説明とラベル
GenericLFI_URIPATH	URI パスに、ローカルファイルインクルージョン (LFI) を悪用する形跡がないかを検査します。例には、../../ などの手法を使用したパストラバーサルの試行があります。 ルールアクション: Block ラベル: awswaf:managed:aws:core-rule-set:GenericLFI_URIPath

ルール名	説明とラベル
`GenericLFI_BODY`	リクエストボディに、ローカルファイルインクルージョン (LFI) を悪用する形跡がないかを検査します。例には、`../../` などの手法を使用したパストラバーサルの試行があります。 **Warning** このルールは、保護パック (ウェブ ACL) とリソースタイプのボディサイズ制限に達するリクエストボディのみを検査します。Application Load Balancer および の場合 AWS AppSync、制限は 8 KB に固定されます。CloudFront 、API Gateway、Amazon Cognito、App Runner、Verified Access、Amazon Bedrock AgentCore Gateway の場合、デフォルトの制限は 16 KB であり、保護パック (ウェブ ACL) 設定で制限を最大 64 KB に増やすことができます。このルールは、オーバーサイズコンテンツの処理に `Continue` オプションを使用します。詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。 ルールアクション: Block ラベル: `awswaf:managed:aws:core-rule-set:GenericLFI_Body`

ルール名	説明とラベル
RestrictedExtensions_URIPATH	読み取りや実行が安全でないシステムファイルの拡張子が URI パスに含まれているリクエストを検査します。パターンの例には、.log や .ini などの拡張子があります。 ルールアクション: Block ラベル: awswaf:managed:aws:core-rule-set:RestrictedExtensions_URIPath
RestrictedExtensions_QUERYARGUMENTS	クエリ引数に、読み取りや実行が安全でないシステムファイル拡張子が含まれているリクエストを検査します。パターンの例には、.log や .ini などの拡張子があります。 ルールアクション: Block ラベル: awswaf:managed:aws:core-rule-set:RestrictedExtensions_QueryArguments
GenericRFI_QUERYARGUMENTS	IPv4 アドレスを含む URL を埋め込むことにより、Web アプリケーションでRFI (リモートファイルインクルード) を悪用しようとする試みに対して、すべてのクエリパラメーターの値を検査します。例としては、http://、https://、ftp://、ftps://、file などのパターンがあり、悪用の試みに IPv4 ホストヘッダーが含まれています。 ルールアクション: Block ラベル: awswaf:managed:aws:core-rule-set:GenericRFI_QueryArguments

ルール名	説明とラベル
`GenericRFI_BODY`	IPv4 アドレスを含む URL を埋め込むことにより、ウェブアプリケーションの RFI (リモートファイルインクルージョン) を悪用しようとする試行に対してリクエストボディを検査します。例としては、`http://`、`https://`、`ftp://`、`ftps://`、`file://` などのパターンがあり、悪用の試みに IPv4 ホストヘッダーが含まれています。 **Warning** このルールは、保護パック (ウェブ ACL) とリソースタイプのボディサイズ制限に達するリクエストボディのみを検査します。Application Load Balancer および の場合 AWS AppSync、制限は 8 KB に固定されます。CloudFront 、API Gateway、Amazon Cognito、App Runner、Verified Access、Amazon Bedrock AgentCore Gateway の場合、デフォルトの制限は 16 KB であり、保護パック (ウェブ ACL) 設定で制限を最大 64 KB に増やすことができます。このルールは、オーバーサイズコンテンツの処理に `Continue` オプションを使用します。詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。 ルールアクション: Block

ルール名	説明とラベル
	ラベル: awswaf:managed:aws:core-rule-set:GenericRFI_Body
GenericRFI_URIPATH	IPv4 アドレスを含む URL を埋め込むことにより、ウェブアプリケーションの RFI (リモートファイルインクルージョン) を悪用しようとする試行に対してURI パスを検査します。例としては、http://、https://、ftp://、ftps://、file などのパターンがあり、悪用の試みに IPv4 ホストヘッダーが含まれています。 ルールアクション: Block ラベル: awswaf:managed:aws:core-rule-set:GenericRFI_URIPath

ルール名	説明とラベル
`CrossSiteScripting_COOKIE`	組み込み を使用して、一般的なクロスサイトスクリプティング (XSS) パターンの Cookie ヘッダーの値を検査します AWS WAF [クロスサイトスクリプティング攻撃ルールステートメント](#)。パターンの例には、`<script>alert("hello")</script>` などのスクリプトあります。 **Note** AWS WAF ログのルール一致の詳細は、このルールグループのバージョン 2.0 では入力されません。 ルールアクション: Block ラベル: `awswaf:managed:aws:core-rule-set:CrossSiteScripting_Cookie`

ルール名	説明とラベル
`CrossSiteScripting_QUERYARGUMENTS`	組み込み を使用して、一般的なクロスサイトスクリプティング (XSS) パターンのクエリ引数の値を検査します AWS WAF [クロスサイトスクリプティング攻撃ルールステートメント]。パターンの例には、`<script>alert("hello")</script>` などのスクリプトあります。 **Note** AWS WAF ログのルール一致の詳細は、このルールグループのバージョン 2.0 では入力されません。 ルールアクション: Block ラベル: `awswaf:managed:aws:core-rule-set:CrossSiteScripting_QueryArguments`

ルール名	説明とラベル
`CrossSiteScripting_BODY`	組み込み を使用して、一般的なクロスサイトスクリプティング (XSS) パターンのリクエストボディを検査します AWS WAF [クロスサイトスクリプティング攻撃ルールステートメント](#)。パターンの例には、`<script>alert("hello")</script>` などのスクリプトあります。 **Note** AWS WAF ログのルール一致の詳細は、このルールグループのバージョン 2.0 では入力されません。 **Warning** このルールは、保護パック (ウェブ ACL) とリソースタイプのボディサイズ制限に達するリクエストボディのみを検査します。Application Load Balancer および の場合 AWS AppSync、制限は 8 KB に固定されます。CloudFront 、API Gateway、Amazon Cognito、App Runner、Verified Access、Amazon Bedrock AgentCore Gateway の場合、デフォルトの制限は 16 KB であり、保護パック (ウェブ ACL) 設定で制限を最大 64 KB に増やすことができます。このルールは、オーバーサイズコンテンツの処理に `Continue` オプションを使用します。詳細については、「[でのウェブリクエストコンポーネントの](#)

ルール名	説明とラベル
	オーバーサイズ化 AWS WAF」を参照してください。 ルールアクション: Block ラベル: `awswaf:managed:aws:core-rule-set:CrossSiteScripting_Body`
`CrossSiteScripting_URIPATH`	組み込み を使用して、一般的なクロスサイトスクリプティング (XSS) パターンの URI パスの値を検査します AWS WAF クロスサイトスクリプティング攻撃ルールステートメント。パターンの例には、`<script>alert("hello")</script>` などのスクリプトあります。 **Note** AWS WAF ログのルール一致の詳細は、このルールグループのバージョン 2.0 では入力されません。 ルールアクション: Block ラベル: `awswaf:managed:aws:core-rule-set:CrossSiteScripting_URIPath`

管理者保護マネージドルールグループ

VendorName: `AWS`、名前: `AWSManagedRulesAdminProtectionRuleSet`、WCU: 100

> **Note**
>
> このドキュメントでは、このマネージドルールグループの最新の静的バージョンリリースについて説明します。バージョンの変更は、AWS マネージドルールの変更ログ の変更ログにレポートされます。他のバージョンの情報については、API コマンド DescribeManagedRuleGroup を使用してください。
> AWS マネージドルールルールのルールグループでルール用に公開する情報は、不正なアクターにルールを回避するために必要なものを与えることなく、ルールを使用するために必要なものを提供することを目的としています。
> ここに記載されている以上の情報が必要な場合は、AWS サポート センター にお問い合わせください。

管理者保護ルールグループには、公開されている管理ページへの外部アクセスをブロックするためのルールが含まれています。これは、サードパーティーのソフトウェアを実行している場合や、悪意のあるアクターがアプリケーションへの管理アクセスを得るリスクを緩和したい場合に便利です。

このマネージドルールグループは、評価対象のウェブリクエストに保護パック (ウェブ ACL) 内のこのルールグループの後に実行されるルールでも使用できるラベルを追加します。 AWS WAF は、Amazon CloudWatch メトリクスにもラベルを記録します。ラベルとラベルメトリクスに関する一般的な情報については、「ウェブリクエストのラベル付け」および「ラベルメトリクスとディメンション」を参照してください。

ルール名	説明とラベル
`AdminProtection_URIPATH`	一般的にウェブサーバーまたはアプリケーションの管理用に確保されている URI パスの有無を検査します。パターンの例には、`sqlmanager` などがあります。 ルールアクション: Block ラベル: `awswaf:managed:aws:admin-protection:AdminProtection_URIPath`

既知の不正な入力マネージドルールグループ

VendorName: AWS、名前: AWSManagedRulesKnownBadInputsRuleSet、WCU: 200

> **Note**
>
> このドキュメントでは、このマネージドルールグループの最新の静的バージョンリリースについて説明します。バージョンの変更は、AWS マネージドルールの変更ログ の変更ログにレポートされます。他のバージョンの情報については、API コマンド DescribeManagedRuleGroup を使用してください。
> AWS マネージドルールルールのルールグループでルール用に公開する情報は、不正なアクターにルールを回避するために必要なものを与えることなく、ルールを使用するために必要なものを提供することを目的としています。
> ここに記載されている以上の情報が必要な場合は、AWS サポート センター にお問い合わせください。

既知の不正な入力ルールグループには、無効であることがわかっており脆弱性の悪用または発見に関連するリクエストパターンをブロックするルールが含まれています。これにより、悪意のあるアクターが脆弱なアプリケーションを発見するリスクを緩和できます。

このマネージドルールグループは、評価対象のウェブリクエストに保護パック (ウェブ ACL) 内のこのルールグループの後に実行されるルールでも使用できるラベルを追加します。 AWS WAF は、Amazon CloudWatch メトリクスにもラベルを記録します。ラベルとラベルメトリクスに関する一般的な情報については、「ウェブリクエストのラベル付け」および「ラベルメトリクスとディメンション」を参照してください。

ルール名	説明とラベル
JavaDeserializationRCE_HEADER	HTTP リクエストヘッダーのキーと値に、Spring Core および Cloud Function RCE の脆弱性 (CVE-2022-22963、CVE-2022-22965) などの Java デシリアライゼーション Remote Command Execution (RCE) の試行を示すパターンがないかどうかを検査します。パターンの例には、(java.lang.Runtime

ルール名	説明とラベル
	).getRuntime().exec("whoami") などがあります。 ⚠ Warning このルールは、リクエストヘッダーの最初の 8 KB または最初の 200 個のヘッダーのうち、いずれかの制限に先に達した方のみを検査し、オーバーサイズコンテンツの処理に Continue オプションを使用します。詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。 ルールアクション: Block ラベル: awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Header

ルール名	説明とラベル
`JavaDeserializationRCE_BODY`	リクエスト本文で、Spring Core および Cloud Function RCE の脆弱性 (CVE-2022-22963、CVE-2022-22965) などの Java デシリアライゼーション Remote Command Execution (RCE) の試行を示すパターンがないかどうかを検査します。パターンの例には、`(java.lang.Runtime).getRuntime().exec("whoami")` などがあります。 **Warning** このルールは、保護パック (ウェブ ACL) とリソースタイプのボディサイズ制限に達するリクエストボディのみを検査します。Application Load Balancer および の場合 AWS AppSync、制限は 8 KB に固定されます。CloudFront、API Gateway、Amazon Cognito、App Runner、Verified Access、Amazon Bedrock AgentCore Gateway の場合、デフォルトの制限は 16 KB であり、保護パック (ウェブ ACL) 設定で制限を最大 64 KB に増やすことができます。このルールは、オーバーサイズコンテンツの処理に `Continue` オプションを使用します。詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。 ルールアクション: Block

ルール名	説明とラベル
	ラベル: `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Body`
`JavaDeserializationRCE_URIPATH`	リクエスト URI で、Spring Core および Cloud Function RCE の脆弱性 (CVE-2022-22963、CVE-2022-22965) などの Java デシリアライゼーション Remote Command Execution (RCE) の試行を示すパターンがないかどうかを検査します。パターンの例には、`(java.lang.Runtime).getRuntime().exec("whoami")` などがあります。 ルールアクション: Block ラベル: `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_URIPath`
`JavaDeserializationRCE_QUERYSTRING`	リクエストクエリ文字列で、Spring Core および Cloud Function RCE の脆弱性 (CVE-2022-22963、CVE-2022-22965) などの Java デシリアライゼーション Remote Command Execution (RCE) の試行を示すパターンがないかどうかを検査します。パターンの例には、`(java.lang.Runtime).getRuntime().exec("whoami")` などがあります。 ルールアクション: Block ラベル: `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_QueryString`

ルール名	説明とラベル
Host_localhost_HEADER	リクエストのホストヘッダーに、localhost を示すパターンがないかを検査します。パターンの例には、localhost などがあります。 ルールアクション: Block ラベル: awswaf:managed:aws:known-bad-inputs:Host_Localhost_Header
PROPFIND_METHOD	リクエストの HTTP メソッドに、PROPFIND がないかを検査します。このメソッドは HEAD と同様ですが、XML オブジェクトを抽出しようとする点が異なります。 ルールアクション: Block ラベル: awswaf:managed:aws:known-bad-inputs:Propfind_Method
ExploitablePaths_URIPATH	URI パスに、悪用可能なウェブアプリケーションパスにアクセスする試みがないかを検査します。パターンの例には、web-inf などのパスがあります。 ルールアクション: Block ラベル: awswaf:managed:aws:known-bad-inputs:ExploitablePaths_URIPath

ルール名	説明とラベル
`Log4JRCE_HEADER`	リクエストヘッダーのキーと値に Log4j の脆弱性 (CVE-2021-44228、CVE-2021-45046、CVE-2021-45105) の存在の有無を検査し、Remote Code Execution (RCE) の試行から保護します。パターンの例には、`${jndi:ldap://example.com/}` などがあります。 **Warning** このルールは、リクエストヘッダーの最初の 8 KB または最初の 200 個のヘッダーのうち、いずれかの制限に先に達した方のみを検査し、オーバーサイズコンテンツの処理に `Continue` オプションを使用します。詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。 ルールアクション: Block ラベル: `awswaf:managed:aws:known-bad-inputs:Log4JRCE_Header`

ルール名	説明とラベル
`Log4JRCE_QUERYSTRING`	クエリ文字列に Log4j の脆弱性 (CVE-2021-44228、CVE-2021-45046、CVE-2021-45105) の存在の有無を検査し、Remote Code Execution (RCE) の試行から保護します。パターンの例には、`${jndi:ldap://example.com/}` などがあります。 ルールアクション: Block ラベル: `awswaf:managed:aws:known-bad-inputs:Log4JRCE_QueryString`

ルール名	説明とラベル
Log4JRCE_BODY	本文に Log4j の脆弱性 (CVE-2021-44228、CVE-2021-45046、CVE-2021-45105) の存在の有無を検査し、Remote Code Execution (RCE) の試行から保護します。パターンの例には、`${jndi:ldap://example.com/}` などがあります。 **Warning** このルールは、保護パック (ウェブ ACL) とリソースタイプのボディサイズ制限に達するリクエストボディのみを検査します。Application Load Balancer および の場合 AWS AppSync、制限は 8 KB に固定されます。CloudFront、API Gateway、Amazon Cognito、App Runner、Verified Access、Amazon Bedrock AgentCore Gateway の場合、デフォルトの制限は 16 KB であり、保護パック (ウェブ ACL) 設定で制限を最大 64 KB に増やすことができます。このルールは、オーバーサイズコンテンツの処理に `Continue` オプションを使用します。詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。 ルールアクション: Block ラベル: `awswaf:managed:aws:known-bad-inputs:Log4JRCE_Body`

ルール名	説明とラベル
`Log4JRCE_URIPATH`	URI パスに Log4j の脆弱性 (CVE-2021-44228、CVE-2021-45046、CVE-2021-45105) の存在の有無を検査し、Remote Code Execution (RCE) の試行から保護します。パターンの例には、`${jndi:ldap://example.com/}` などがあります。 ルールアクション: Block ラベル: `awswaf:managed:aws:known-bad-inputs:Log4JRCE_URIPath`

ルール名	説明とラベル
`ReactJSRCE_BODY`	CVE-2025-55182 の存在を示すパターンについて、リクエスト本文を検査します。 **Warning** このルールは、保護パック (ウェブ ACL) とリソースタイプのボディサイズ制限に達するリクエストボディのみを検査します。Application Load Balancer と AWS AppSyncの場合、その制限は 8 KB に固定されます。CloudFront、API Gateway、Amazon Cognito、App Runner、 AWS Verified Access の場合、デフォルトの制限は 16 KB であり、保護パック (ウェブ ACL) 設定で制限を最大 64 KB に増やすことができます。このルールは、オーバーサイズコンテンツの処理に `CONTINUE` オプションを使用します。詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。 ルールアクション: Block ラベル: `awswaf:managed:aws:known-bad-inputs:ReactJSRCE_Body`

ユースケース固有のルールグループ

ユースケース固有のルールグループは、さまざまな AWS WAF ユースケースに対して段階的な保護を提供します。アプリケーションに適用するルールグループを選択します。

SQL データベースマネージドルールグループ

VendorName: AWS、名前: AWSManagedRulesSQLiRuleSet、WCU: 200

> **Note**
>
> このドキュメントでは、このマネージドルールグループの最新の静的バージョンリリースについて説明します。バージョンの変更は、AWS マネージドルールの変更ログ の変更ログにレポートされます。他のバージョンの情報については、API コマンド DescribeManagedRuleGroup を使用してください。
> AWS マネージドルールルールのルールグループでルール用に公開する情報は、不正なアクターにルールを回避するために必要なものを与えることなく、ルールを使用するために必要なものを提供することを目的としています。
> ここに記載されている以上の情報が必要な場合は、AWS サポート センター にお問い合わせください。

SQL Database ルールグループには、SQL インジェクション攻撃などの SQL データベースの悪用に関連するリクエストパターンをブロックするルールが含まれています。これにより、不正なクエリのリモートインジェクションを防ぐことができます。アプリケーションが SQL データベースと連結している場合は、このルールグループを評価します。

このマネージドルールグループは、評価対象のウェブリクエストに保護パック (ウェブ ACL) 内のこのルールグループの後に実行されるルールでも使用できるラベルを追加します。 AWS WAF は、Amazon CloudWatch メトリクスにもラベルを記録します。ラベルとラベルメトリクスに関する一般的な情報については、「ウェブリクエストのラベル付け」および「ラベルメトリクスとディメンション」を参照してください。

ルール名	説明とラベル
SQLi_QUERYARGUMENTS	組み込みの を使用し AWS WAF SQL インジェクション攻撃ルールステートメント、機密レベルを に設定してLow、悪意のある SQL コードに一致するパターンがないか、すべてのクエリパラメータの値を検査します。 ルールアクション: Block

ルール名	説明とラベル
	ラベル: awswaf:managed:aws:sql-database:SQLi_QueryArguments
SQLiExtendedPatterns_QUERYARGUMENTS	すべてのクエリパラメータの値に、悪意のある SQL コードに一致するパターンがないかを検査します。このルールが検査するパターンは、ルール SQLi_QUERYARGUMENTS　の対象外です。 ルールアクション: Block ラベル: awswaf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments

ルール名	説明とラベル
SQLi_BODY	組み込みの を使用し AWS WAF SQL インジェクション攻撃ルールステートメント、機密レベルを に設定してLow、悪意のある SQL コードに一致するパターンがないかリクエストボディを検査します。 **Warning** このルールは、保護パック (ウェブ ACL) とリソースタイプのボディサイズ制限に達するリクエストボディのみを検査します。Application Load Balancer および の場合 AWS AppSync、制限は 8 KB に固定されます。CloudFront 、API Gateway、Amazon Cognito、App Runner、Verified Access、Amazon Bedrock AgentCore Gateway の場合、デフォルトの制限は 16 KB であり、保護パック (ウェブ ACL) 設定で制限を最大 64 KB に増やすことができます。このルールは、オーバーサイズコンテンツの処理に `Continue` オプションを使用します。詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。 ルールアクション: Block ラベル: `awswaf:managed:aws:sql-database:SQLi_Body`

ルール名	説明とラベル
SQLiExtendedPatterns_BODY	リクエストボディに、悪意のある SQL コードに一致するパターンがないかを検査します。このルールが検査するパターンは、ルール SQLi_BODY の対象外です。 **Warning** このルールは、保護パック (ウェブ ACL) とリソースタイプのボディサイズ制限に達するリクエストボディのみを検査します。Application Load Balancer および の場合 AWS AppSync、制限は 8 KB に固定されます。CloudFront 、API Gateway、Amazon Cognito、App Runner、Verified Access、Amazon Bedrock AgentCore Gateway の場合、デフォルトの制限は 16 KB であり、保護パック (ウェブ ACL) 設定で制限を最大 64 KB に増やすことができます。このルールは、オーバーサイズコンテンツの処理に Continue オプションを使用します。詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。 ルールアクション: Block ラベル: awswaf:managed:aws:sql-database:SQLiExtendedPatterns_Body

ルール名	説明とラベル
SQLiExtendedPatterns_HEADER	悪意のある SQL コードに一致するパターンがないかリクエストヘッダーを検査します。 ルールアクション: Block ラベル: awswaf:managed:aws:sql-database:SQLiExtendedPatterns_Header
SQLiExtendedPatterns_URIPATH	悪意のある SQL コードに一致するパターンがないかリクエストパスを検査します。このルールが検査するパターンは、ルール SQLi_URIPATH の対象外です。 ルールアクション: Block ラベル: awswaf:managed:aws:sql-database:SQLiExtendedPatterns_UriPath
SQLi_COOKIE	組み込みの を使用し AWS WAF SQL インジェクション攻撃ルールステートメント、機密レベルを に設定してLow、悪意のある SQL コードに一致するパターンがないかリクエスト Cookie ヘッダーを検査します。 ルールアクション: Block ラベル: awswaf:managed:aws:sql-database:SQLi_Cookie

ルール名	説明とラベル
SQLi_URIPATH	組み込みの を使用し AWS WAF SQL インジェクション攻撃ルールステートメント、機密レベルを に設定してLow、悪意のある SQL コードに一致するパターンがないかリクエスト Cookie ヘッダーを検査します。 ルールアクション: Block ラベル: awswaf:managed:aws:sql-database:SQLi_URIPath

Linux オペレーティングシステムマネージドルールグループ

VendorName: AWS、名前: AWSManagedRulesLinuxRuleSet、WCU: 200

> **Note**
>
> このドキュメントでは、このマネージドルールグループの最新の静的バージョンリリースについて説明します。バージョンの変更は、AWS マネージドルールの変更ログ の変更ログにレポートされます。他のバージョンの情報については、API コマンド DescribeManagedRuleGroup を使用してください。
> AWS マネージドルールルールのルールグループでルール用に公開する情報は、不正なアクターにルールを回避するために必要なものを与えることなく、ルールを使用するために必要なものを提供することを目的としています。
> ここに記載されている以上の情報が必要な場合は、AWS サポート センター にお問い合わせください。

Linux オペレーティングシステムルールグループには、Linux 固有のローカルファイルインクルージョン (LFI) 攻撃など、Linux 固有の脆弱性の悪用に関連するリクエストパターンをブロックするルールが含まれています。これにより、攻撃者がアクセスしてはならないファイルの内容を公開したり、コードを実行したりする攻撃を防ぐことができます。アプリケーションの一部が Linux で実行されている場合は、このルールグループを評価する必要があります。このルールグループは、POSIX オペレーティングシステム ルールグループと組み合わせて使用する必要があります。

このマネージドルールグループは、評価対象のウェブリクエストに保護パック (ウェブ ACL) 内のこのルールグループの後に実行されるルールでも使用できるラベルを追加します。 AWS WAF は、Amazon CloudWatch メトリクスにもラベルを記録します。ラベルとラベルメトリクスに関する一般的な情報については、「ウェブリクエストのラベル付け」および「ラベルメトリクスとディメンション」を参照してください。

ルール名	説明とラベル
LFI_URIPATH	リクエストパスに、ウェブアプリケーションのローカルファイルインクルージョン (LFI) の脆弱性を悪用する試みがないかを検査します。パターンの例には、攻撃者にオペレーティングシステムの情報を提供できる /proc/version などのファイルがあります。 ルールアクション: Block ラベル: awswaf:managed:aws:linux-os:LFI_URIPath
LFI_QUERYSTRING	クエリ文字列の値に、ウェブアプリケーションのローカルファイルインクルージョン (LFI) の脆弱性を悪用する試みがないかを検査します。パターンの例には、攻撃者にオペレーティングシステムの情報を提供できる /proc/version などのファイルがあります。 ルールアクション: Block ラベル: awswaf:managed:aws:linux-os:LFI_QueryString
LFI_HEADER	リクエストヘッダーに、ウェブアプリケーションのローカルファイルインクルージョン (LFI) の脆弱性を悪用する試みの有無を検査します。パターンの例には、攻撃者にオペレーティン

ルール名	説明とラベル
	グシステムの情報を提供できる `/proc/version` などのファイルがあります。 **Warning** このルールは、リクエストヘッダーの最初の 8 KB または最初の 200 個のヘッダーのうち、いずれかの制限に先に達した方のみを検査し、オーバーサイズコンテンツの処理に `Continue` オプションを使用します。詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。 ルールアクション: Block ラベル: `awswaf:managed:aws:linux-os:LFI_Header`

POSIX オペレーティングシステムマネージドルールグループ

VendorName: `AWS`、名前: `AWSManagedRulesUnixRuleSet`、WCU: 100

Note

このドキュメントでは、このマネージドルールグループの最新の静的バージョンリリースについて説明します。バージョンの変更は、AWS マネージドルールの変更ログ の変更ログにレポートされます。他のバージョンの情報については、API コマンド DescribeManagedRuleGroup を使用してください。
AWS マネージドルールルールのルールグループでルール用に公開する情報は、不正なアクターにルールを回避するために必要なものを与えることなく、ルールを使用するために必要なものを提供することを目的としています。

ここに記載されている以上の情報が必要な場合は、AWS サポート センター にお問い合わせください。

POSIX オペレーティングシステムルールグループには、POSIX および POSIX と同等のオペレーティングシステムに固有の脆弱性の悪用 (ローカルファイルインクルージョン (LFI) 攻撃など) に関連するリクエストパターンをブロックするルールが含まれています。これにより、攻撃者がアクセスしてはならないファイルの内容を公開したり、コードを実行したりする攻撃を防ぐことができます。アプリケーションの一部が POSIX または POSIX と同等のオペレーティングシステム (Linux、AIX、HP-UX、macOS、Solaris、FreeBSD、OpenBSD など) で実行されている場合は、このルールグループを評価する必要があります。

このマネージドルールグループは、評価対象のウェブリクエストに保護パック (ウェブ ACL) 内のこのルールグループの後に実行されるルールでも使用できるラベルを追加します。 AWS WAF は、Amazon CloudWatch メトリクスにもラベルを記録します。ラベルとラベルメトリクスに関する一般的な情報については、「ウェブリクエストのラベル付け」および「ラベルメトリクスとディメンション」を参照してください。

ルール名	説明とラベル
`UNIXShellCommandsVariables_QUERYSTRING`	Unix システム上で動作するウェブアプリケーションにおいて、コマンドインジェクション、LFI、およびパストラバーサルの脆弱性を悪用しようとする試みを検出するために、クエリ文字列の値を検査します。パターンの例には、`echo $HOME` や `echo $PATH` などがあります。 ルールアクション: Block ラベル: `awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_QueryString`
`UNIXShellCommandsVariables_BODY`	リクエストボディに、Unix システムで実行されるウェブアプリケーションのコマンドインジェクション、LFI、パストラバーサルの脆弱

ルール名	説明とラベル
	性を悪用する試みがないかを検査します。パターンの例には、`echo $HOME` や `echo $PATH` などがあります。 **Warning** このルールは、保護パック (ウェブ ACL) とリソースタイプのボディサイズ制限に達するリクエストボディのみを検査します。Application Load Balancer および の場合 AWS AppSync、制限は 8 KB に固定されます。CloudFront、API Gateway、Amazon Cognito、App Runner、Verified Access、Amazon Bedrock AgentCore Gateway の場合、デフォルトの制限は 16 KB であり、保護パック (ウェブ ACL) 設定で制限を最大 64 KB に増やすことができます。このルールは、オーバーサイズコンテンツの処理に `Continue` オプションを使用します。詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。 ルールアクション: Block ラベル: `awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_Body`

ルール名	説明とラベル
UNIXShellCommandsVariables_HEADER	すべてのリクエストヘッダーに、Unix システムで実行されるウェブアプリケーションのコマンドインジェクション、LFI、パストラバーサルの脆弱性を悪用する試みがないかを検査します。パターンの例には、echo $HOME や echo $PATH などがあります。 **Warning** このルールは、リクエストヘッダーの最初の 8 KB または最初の 200 個のヘッダーのうち、いずれかの制限に先に達した方のみを検査し、オーバーサイズコンテンツの処理に Continue オプションを使用します。詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。 ルールアクション: Block ラベル: awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_Header

Windows オペレーティングシステムマネージドルールグループ

VendorName: AWS、名前: AWSManagedRulesWindowsRuleSet、WCU: 200

Note

このドキュメントでは、このマネージドルールグループの最新の静的バージョンリリースについて説明します。バージョンの変更は、AWS マネージドルールの変更ロ

グ の変更ログにレポートされます。他のバージョンの情報については、API コマンド DescribeManagedRuleGroup を使用してください。
AWS マネージドルールルールのルールグループでルール用に公開する情報は、不正なアクターにルールを回避するために必要なものを与えることなく、ルールを使用するために必要なものを提供することを目的としています。
ここに記載されている以上の情報が必要な場合は、AWS サポート センター にお問い合わせください。

Windows オペレーティングシステムのルールグループには、PowerShell コマンドのリモート実行など、Windows 固有の脆弱性の悪用に関連するリクエストパターンをブロックするルールが含まれています。これにより、攻撃者が不正なコマンドまたは悪意のあるコードを実行できる脆弱性の悪用を防ぐことができます。アプリケーションの一部が Windows オペレーティングシステムで実行されている場合は、このルールグループを評価します。

このマネージドルールグループは、評価対象のウェブリクエストに保護パック (ウェブ ACL) 内のこのルールグループの後に実行されるルールでも使用できるラベルを追加します。 AWS WAF は、Amazon CloudWatch メトリクスにもラベルを記録します。ラベルとラベルメトリクスに関する一般的な情報については、「ウェブリクエストのラベル付け」および「ラベルメトリクスとディメンション」を参照してください。

ルール名	説明とラベル
`WindowsShellCommands_HEADER`	すべてのリクエストヘッダーを検査し、ウェブアプリケーションでの WindowsShell コマンドインジェクションの試行をブロックします。一致パターンは WindowsShell コマンドを表します。パターンの例には、`||nslookup` 、`;cmd` などがあります。 ルールアクション: Block ラベル: `awswaf:managed:aws:windows-os:WindowsShellCommands_Header`
`WindowsShellCommands_QUERYARGUMENTS`	ウェブアプリケーションでの WindowsShell コマンドインジェクションの試行についてすべて

ルール名	説明とラベル
	のクエリパラメータの値を検査します。一致パターンは WindowsShell コマンドを表します。パターンの例には、`||nslookup` 、`;cmd` などがあります。 ルールアクション: Block ラベル: `awswaf:managed:aws:windows-os:WindowsShellCommands_QueryArguments`
`WindowsShellCommands_QUERYSTRING`	クエリ文字列を検査し、ウェブアプリケーションでの WindowsShell コマンドインジェクションの試行をブロックします。一致パターンは WindowsShell コマンドを表します。パターンの例には、`||nslookup` 、`;cmd` などがあります。 ルールアクション: Block ラベル: `awswaf:managed:aws:windows-os:WindowsShellCommands_QueryString`
`WindowsShellCommands_URIPATH`	リクエストパスを検査し、ウェブアプリケーションでの WindowsShell コマンドインジェクションの試行をブロックします。一致パターンは WindowsShell コマンドを表します。パターンの例には、`||nslookup` 、`;cmd` などがあります。 ルールアクション: Block ラベル: `awswaf:managed:aws:windows-os:WindowsShellCommands_UriPath`

ルール名	説明とラベル
`WindowsShellCommands_BODY`	ウェブアプリケーションでの WindowsShell コマンドインジェクションの試行についてリクエストボディの値を検査します。一致パターンは WindowsShell コマンドを表します。パターンの例には、`||nslookup` 、`;cmd` などがあります。 **Warning** このルールは、保護パック (ウェブ ACL) とリソースタイプのボディサイズ制限に達するリクエストボディのみを検査します。Application Load Balancer および の場合 AWS AppSync、制限は 8 KB に固定されます。CloudFront 、API Gateway、Amazon Cognito、App Runner、Verified Access、Amazon Bedrock AgentCore Gateway の場合、デフォルトの制限は 16 KB であり、保護パック (ウェブ ACL) 設定で制限を最大 64 KB に増やすことができます。このルールは、オーバーサイズコンテンツの処理に `Continue` オプションを使用します。詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。 ルールアクション: Block ラベル: `awswaf:managed:aws:windows-os:WindowsShellCommands_Body`

ルール名	説明とラベル
PowerShellCommands_COOKIE	ウェブアプリケーションでの PowerShell コマンドインジェクションの試行についてリクエスト cookie を検査します。一致パターンは PowerShell コマンドを表します。例えば、Invoke-Expression 。 ルールアクション: Block ラベル: awswaf:managed:aws:windows-os:PowerShellCommands_Cookie
PowerShellCommands_QUERYARGUMENTS	ウェブアプリケーションでの PowerShell コマンドインジェクションの試行についてすべてのクエリパラメータの値を検査します。一致パターンは PowerShell コマンドを表します。例えば、Invoke-Expression 。 ルールアクション: Block ラベル: awswaf:managed:aws:windows-os:PowerShellCommands_QueryArguments

ルール名	説明とラベル
`PowerShellCommands_BODY`	ウェブアプリケーションでの PowerShell コマンドインジェクションの試行についてリクエストボディを検査します。一致パターンは PowerShell コマンドを表します。例えば、`Invoke-Expression` 。 **Warning** このルールは、保護パック (ウェブ ACL) とリソースタイプのボディサイズ制限に達するリクエストボディのみを検査します。Application Load Balancer および の場合 AWS AppSync、制限は 8 KB に固定されます。CloudFront 、API Gateway、Amazon Cognito、App Runner、Verified Access、Amazon Bedrock AgentCore Gateway の場合、デフォルトの制限は 16 KB であり、保護パック (ウェブ ACL) 設定で制限を最大 64 KB に増やすことができます。このルールは、オーバーサイズコンテンツの処理に `Continue` オプションを使用します。詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。 ルールアクション: Block ラベル: `awswaf:managed:aws:windows-os:PowerShellCommands_Body`

PHP アプリケーションマネージドルールグループ

VendorName: AWS、名前: AWSManagedRulesPHPRuleSet、WCU: 100

> **Note**
>
> このドキュメントでは、このマネージドルールグループの最新の静的バージョンリリースについて説明します。バージョンの変更は、AWS マネージドルールの変更ログ の変更ログにレポートされます。他のバージョンの情報については、API コマンド DescribeManagedRuleGroup を使用してください。
> AWS マネージドルールルールのルールグループでルール用に公開する情報は、不正なアクターにルールを回避するために必要なものを与えることなく、ルールを使用するために必要なものを提供することを目的としています。
> ここに記載されている以上の情報が必要な場合は、AWS サポート センター にお問い合わせください。

PHP アプリケーションルールグループには、安全でない PHP 関数のインジェクションなど、PHP プログラミング言語の使用に固有の脆弱性の悪用に関連するリクエストパターンをブロックするルールが含まれています。これにより、攻撃者が許可されていないコードまたはコマンドを遠隔で実行できる脆弱性の悪用を防ぐことができます。アプリケーションが連結するサーバーに PHP がインストールされている場合は、このルールグループを評価します。

このマネージドルールグループは、評価対象のウェブリクエストに保護パック (ウェブ ACL) 内のこのルールグループの後に実行されるルールでも使用できるラベルを追加します。 AWS WAF は、Amazon CloudWatch メトリクスにもラベルを記録します。ラベルとラベルメトリクスに関する一般的な情報については、「ウェブリクエストのラベル付け」および「ラベルメトリクスとディメンション」を参照してください。

ルール名	説明とラベル
PHPHighRiskMethodsVariables_HEADER	PHP スクリプトコードインジェクションの試行について、すべてのヘッダーを検査します。パターンの例には、fsockopen や $_GET スーパーグローバル変数などの関数があります。

ルール名	説明とラベル
	Warning このルールは、リクエストヘッダーの最初の 8 KB または最初の 200 個のヘッダーのうち、いずれかの制限に先に達した方のみを検査し、オーバーサイズコンテンツの処理に Continue オプションを使用します。詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。 ルールアクション: Block ラベル: awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_Header
PHPHighRiskMethodsVariables_QUERYSTRING	リクエスト URL の最初の ? 以降をすべて検査し、PHP スクリプトコードインジェクションの試行がないかを調べます。パターンの例には、fsockopen や $_GET スーパーグローバル変数などの関数があります。 ルールアクション: Block ラベル: awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_QueryString

ルール名	説明とラベル
PHPHighRiskMethodsVariables_BODY	リクエストボディの値に、PHP スクリプトコードインジェクションがないかを検査します。パターンの例には、fsockopen や $_GET スーパーグローバル変数などの関数があります。 ⚠ Warning このルールは、保護パック (ウェブ ACL) とリソースタイプのボディサイズ制限に達するリクエストボディのみを検査します。Application Load Balancer および の場合 AWS AppSync、制限は 8 KB に固定されます。CloudFront、API Gateway、Amazon Cognito、App Runner、Verified Access、Amazon Bedrock AgentCore Gateway の場合、デフォルトの制限は 16 KB であり、保護パック (ウェブ ACL) 設定で制限を最大 64 KB に増やすことができます。このルールは、オーバーサイズコンテンツの処理に Continue オプションを使用します。詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。 ルールアクション: Block ラベル: awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_Body

ルール名	説明とラベル
PHPHighRiskMethodsVariables_URIPATH	PHP スクリプトコードの挿入試行のリクエストパスを検査します。パターンの例には、fsockopen や $_GET スーパーグローバル変数などの関数があります。 ルールアクション: Block ラベル: awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_URIPath

WordPress アプリケーションマネージドルールグループ

VendorName: AWS、名前: AWSManagedRulesWordPressRuleSet、WCU: 100

> **Note**
>
> このドキュメントでは、このマネージドルールグループの最新の静的バージョンリリースについて説明します。バージョンの変更は、AWS マネージドルールの変更ログ の変更ログにレポートされます。他のバージョンの情報については、API コマンド DescribeManagedRuleGroup を使用してください。
> AWS マネージドルールルールのルールグループでルール用に公開する情報は、不正なアクターにルールを回避するために必要なものを与えることなく、ルールを使用するために必要なものを提供することを目的としています。
> ここに記載されている以上の情報が必要な場合は、AWS サポート センター にお問い合わせください。

WordPress アプリケーションルールグループには、WordPress サイト固有の脆弱性の悪用に関連するリクエストパターンをブロックするルールが含まれています。WordPress を実行している場合は、このルールグループを評価する必要があります。このルールグループは、SQL データベース および PHP アプリケーション ルールグループと組み合わせて使用する必要があります。

このマネージドルールグループは、評価対象のウェブリクエストに保護パック (ウェブ ACL) 内のこのルールグループの後に実行されるルールでも使用できるラベルを追加します。 AWS WAF

は、Amazon CloudWatch メトリクスにもラベルを記録します。ラベルとラベルメトリクスに関する一般的な情報については、「ウェブリクエストのラベル付け」および「ラベルメトリクスとディメンション」を参照してください。

ルール名	説明とラベル
`WordPressExploitableCommands_QUERYSTRING`	リクエストクエリ文字列に、脆弱なインストールまたはプラグインで悪用される可能性のある高リスクの WordPress コマンドがないかを検査します。パターンの例には、`do-reset-wordpress` などのコマンドがあります。 ルールアクション: Block ラベル: `awswaf:managed:aws:wordpress-app:WordPressExploitableCommands_QUERYSTRING`
`WordPressExploitablePaths_URIPATH`	リクエストの URI パスに、脆弱性が簡単に悪用されることがわかっている `xmlrpc.php` などの WordPress ファイルがないかを検査します。 ルールアクション: Block ラベル: `awswaf:managed:aws:wordpress-app:WordPressExploitablePaths_URIPATH`

IP 評価ルールグループ

IP 評価ルールグループはソース IP アドレスに基づいてリクエストをブロックします。

> **Note**
>
> これらのルールは、ウェブリクエストの発信元のソース IP アドレスを使用します。トラフィックが 1 つ以上のプロキシまたはロードバランサーを通過する場合、ウェブリクエスト

の発信元には、クライアントの発信アドレスではなく、最後のプロキシのアドレスが含まれます。

ボットトラフィックや悪用の試みを緩和する場合、またはコンテンツに地理的制限を適用する場合は、これらのルールグループを 1 つ以上選択します。ボット管理については、「AWS WAF Bot Control ルールグループ」も参照してください。

このカテゴリのルールグループは、バージョニングや SNS 更新通知を提供しません。

Amazon IP 評価リストマネージドルールグループ

VendorName: AWS、名前: AWSManagedRulesAmazonIpReputationList、WCU: 25

> **Note**
>
> AWS マネージドルールルールのルールグループでルール用に公開する情報は、ルールを回避するために必要なものを不正なアクターに与えることなく、ルールを使用するために必要なものを提供することを目的としています。
> ここに記載されている以上の情報が必要な場合は、AWS サポート センター にお問い合わせください。

Amazon IP 評価リストルールグループには、Amazon 内部脅威インテリジェンスに基づくルールが含まれています。これは、通常、ボットやその他の脅威に関連付けられている IP アドレスをブロックする場合に便利です。これらの IP アドレスをブロックすることで、ボットを緩和し、悪意のあるアクターが脆弱なアプリケーションを発見するリスクを緩和できます。

このマネージドルールグループは、評価対象のウェブリクエストに保護パック (ウェブ ACL) 内のこのルールグループの後に実行されるルールでも使用できるラベルを追加します。 AWS WAF は、Amazon CloudWatch メトリクスにもラベルを記録します。ラベルとラベルメトリクスに関する一般的な情報については、「ウェブリクエストのラベル付け」および「ラベルメトリクスとディメンション」を参照してください。

ルール名	説明とラベル
AWSManagedIPReputationList	悪意のあるアクティビティに積極的に関与していると特定された IP アドレスを検査しま

ルール名	説明とラベル
	す。 AWS WAF は、Amazon がサイバー犯罪から顧客を保護するために使用する脅威インテリジェンスツールである MadPot など、さまざまなソースから IP アドレスリストを収集します。MadPot の詳細については、https://www.aboutamazon.com/news/aws/amazon-madpot-stops-cybersecurity-crime を参照してください。 ルールアクション: Block ラベル: `awswaf:managed:aws:amazon-ip-list:AWSManagedIPReputationList`
`AWSManagedReconnaissanceList`	AWS リソースに対して偵察を実行している IP アドレスからの接続を検査します。 ルールアクション: Block ラベル: `awswaf:managed:aws:amazon-ip-list:AWSManagedReconnaissanceList`
`AWSManagedIPDDoSList`	DDoS アクティビティにアクティブに関与していると識別された IP アドレスを検査します。 ルールアクション: Count ラベル: `awswaf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList`

匿名 IP リストマネージドルールグループ

VendorName: `AWS`、名前: `AWSManagedRulesAnonymousIpList`、WCU: 50

> **Note**
>
> AWS マネージドルールルールのルールグループでルール用に公開する情報は、ルールを回避するために必要なものを不正なアクターに与えることなく、ルールを使用するために必要なものを提供することを目的としています。
> ここに記載されている以上の情報が必要な場合は、AWS サポート センター にお問い合わせください。

匿名 IP リストのルールグループには、ビューワー ID の難読化を許可するサービスからのリクエストをブロックするルールが含まれています。これには、VPN、プロキシ、Tor ノード、ウェブホスティングプロバイダーなどからのリクエストが含まれます。このルールグループは、アプリケーションから ID を隠そうとするビューワーを除外する場合に便利です。これらのサービスの IP アドレスをブロックすると、ボットの緩和や地理的制限の回避に役立ちます。

このマネージドルールグループは、評価対象のウェブリクエストに保護パック (ウェブ ACL) 内のこのルールグループの後に実行されるルールでも使用できるラベルを追加します。 AWS WAF は、Amazon CloudWatch メトリクスにもラベルを記録します。ラベルとラベルメトリクスに関する一般的な情報については、「ウェブリクエストのラベル付け」および「ラベルメトリクスとディメンション」を参照してください。

ルール名	説明とラベル
`AnonymousIPList`	クライアントの情報を匿名化することがわかっているソース (TOR ノード、一時プロキシ、その他のマスキングサービスなど) の IP アドレスのリストを検査します。 ルールアクション: Block ラベル: `awswaf:managed:aws:anonymous-ip-list:AnonymousIPList`
`HostingProviderIPList`	エンドユーザートラフィックのソースになる可能性が低いウェブホスティングプロバイダーとクラウドプロバイダーの IP アドレスのリストを検査します。IP リストには AWS IP アドレスは含まれません。

ルール名	説明とラベル
	ルールアクション: Block ラベル: `awswaf:managed:aws:anonymous-ip-list:HostingProviderIPList`

AWS WAF Fraud Control アカウント作成不正防止 (ACFP) ルールグループ

このセクションでは、 AWS WAF Fraud Control アカウント作成不正防止 (ACFP) マネージドルールグループの動作について説明します。

VendorName: `AWS`、名前: `AWSManagedRulesACFPRuleSet`、WCU: 50

> **Note**
>
> このドキュメントでは、このマネージドルールグループの最新の静的バージョンリリースについて説明します。バージョンの変更は、AWS マネージドルールの変更ログ の変更ログにレポートされます。他のバージョンの情報については、API コマンド DescribeManagedRuleGroup を使用してください。
> AWS マネージドルールルールのルールグループでルール用に公開する情報は、ルールを回避するために必要なものを不正なアクターに与えることなく、ルールを使用するために必要なものを提供することを目的としています。
> ここに記載されている以上の情報が必要な場合は、AWS サポート センター にお問い合わせください。

AWS WAF Fraud Control Account Creation Fraud Prevention (ACFP) マネージドルールグループは、不正なアカウント作成の試みの一部である可能性のあるリクエストにラベルを付けて管理します。ルールグループは、クライアントがアプリケーションの登録エンドポイントとアカウント作成エンドポイントに送信するアカウント作成リクエストを検査することでこれを行います。

ACFP ルールグループは、さまざまな方法でアカウント作成の試みを検査し、悪意のある可能性のあるインタラクションを可視化し、コントロールできるようにします。ルールグループは、リクエストトークンを使用して、クライアントブラウザに関する情報と、アカウント作成リクエストの作成における人間のインタラクティビティのレベルに関する情報を収集します。ルールグループは、IP アドレスとクライアントセッションごとにリクエストを集計し、物理アドレスや電話番号などの提供されたアカウント情報ごとに集計することで、一括アカウント作成の試みを検出および管理します。さら

に、ルールグループは、侵害された認証情報を使用した新しいアカウントの作成を検出してブロックします。これは、アプリケーションと新しいユーザーのセキュリティ体制の保護に役立ちます。

このルールグループの使用に関する考慮事項

このルールグループには、アプリケーションのアカウント登録パスとアカウント作成パスの仕様を含むカスタム設定が必要です。特に明記されている場合を除き、このルールグループのルールは、クライアントがこれらの 2 つのエンドポイントに送信するすべてのリクエストを検査します。このルールグループを設定および実装するには、「AWS WAF Fraud Control アカウント作成不正防止 (ACFP)」のガイダンスを参照してください。

> **Note**
>
> このマネージドルールグループを使用する場合、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

このルールグループは、 AWS WAFでのインテリジェントな脅威の軽減保護の一部です。詳細については、「でのインテリジェントな脅威の軽減 AWS WAF」を参照してください。

コストを抑え、ウェブトラフィックを希望どおりに管理していることを確実にするには、でのインテリジェントな脅威軽減のベストプラクティス AWS WAF のガイダンスに従ってこのルールグループを使用してください。

このルールグループは、Amazon Cognito ユーザープールでは使用できません。このルールグループを使用する保護パック (ウェブ ACL) をユーザープールに関連付けることはできません。また、このルールグループをユーザープールに既に関連付けられた保護パック (ウェブ ACL) に追加することはできません。

このルールグループによって追加されるラベル

このマネージドルールグループは、評価対象のウェブリクエストに保護パック (ウェブ ACL) 内のこのルールグループの後に実行されるルールでも使用できるラベルを追加します。 AWS WAF は、Amazon CloudWatch メトリクスにもラベルを記録します。ラベルとラベルメトリクスに関する一般的な情報については、「ウェブリクエストのラベル付け」および「ラベルメトリクスとディメンション」を参照してください。

トークンラベル

このルールグループは、 AWS WAF トークン管理を使用して、 AWS WAF トークンのステータスに従ってウェブリクエストを検査し、ラベル付けします。 は、クライアントセッションの追跡と検証にトークン AWS WAF を使用します。

トークンおよびトークンの管理の詳細については、「AWS WAF インテリジェントな脅威の軽減におけるトークンの使用」を参照してください。

ここで説明するラベルコンポーネントについては、「でのラベル構文と命名要件 AWS WAF」を参照してください。

クライアントセッションラベル

ラベルには、 AWS WAF トークン管理がクライアントセッションを識別するために使用する一意の識別子`awswaf:managed:token:id:`*`identifier`*が含まれています。この識別子は、クライアントが使用していたトークンを破棄した後など、新しいトークンを取得すると変わる可能性があります。

> **Note**
>
> AWS WAF は、このラベルの Amazon CloudWatch メトリクスを報告しません。

ブラウザフィンガープリントラベル

ラベルには、 AWS WAF トークン管理がさまざまなクライアントブラウザシグナルから計算する堅牢なブラウザフィンガープリント識別子`awswaf:managed:token:fingerprint:`*`fingerprint-identifier`*が含まれています。この識別子は、複数のトークン取得の試行全体で同じままです。フィンガープリント識別子は、単一のクライアントに対して一意ではありません。

> **Note**
>
> AWS WAF は、このラベルの Amazon CloudWatch メトリクスを報告しません。

トークンステータスラベル: ラベル名前空間プレフィックス

トークンステータスラベルは、トークン、チャレンジのステータス、およびそれに含まれる CAPTCHA 情報を報告します。

各トークンステータスラベルは、次のプレフィクスの 1 つで始まります。

- awswaf:managed:token:— トークンの一般的なステータスを報告したり、トークンのチャレンジ情報のステータスを報告したりするために使用されます。
- awswaf:managed:captcha:— トークンの CAPTCHA 情報のステータスを報告するために使用されます。

トークンステータスラベル: ラベル名

プレフィックスに続いて、ラベルの残りの部分には詳細なトークンステータス情報が表示されます。

- accepted - リクエストトークンが存在し、以下の内容が含まれています。
  - 有効なチャレンジまたは CAPTCHA ソリューション。
  - 有効期限が切れていないチャレンジまたは CAPTCHA タイムスタンプ。
  - 保護パック (ウェブ ACL) に有効なドメイン仕様。

  例: ラベル awswaf:managed:token:accepted には、ウェブリクエストのトークンに有効なチャレンジソリューション、有効期限が切れていないチャレンジタイムスタンプ、および有効なドメインがあることが示されています。
- rejected - リクエストトークンは存在するが、承認基準を満たしていない。

  トークン管理では、拒否されたラベルに加えて、理由を示すカスタムラベル名前空間と名前が追加されます。
  - rejected:not_solved — トークンにチャレンジまたは CAPTCHA ソリューションがない。
  - rejected:expired — 保護パック (ウェブ ACL) に設定されているトークンイミュニティ時間によると、トークンのチャレンジまたは CAPTCHA タイムスタンプの有効期限が切れている。
  - rejected:domain_mismatch — トークンのドメインが、保護パック (ウェブ ACL) のトークンドメイン設定と一致しない。
  - rejected:invalid – 指定されたトークンを読み取ることが AWS WAF できませんでした。

  例: ラベル awswaf:managed:captcha:rejected と awswaf:managed:captcha:rejected:expired とともに、トークンの CAPTCHA タイムスタンプがウェブ ACL で設定されている CAPTCHA トークンのイミュニティ時間を超えたために、リクエストには有効な CAPTCHA 解決がなかったことが示されています。
- absent — リクエストにトークンがないか、トークンマネージャーがそれを読み取れなかった。

例: ラベル `awswaf:managed:captcha:absent` には、リクエストにトークンがないことが示されています。

ACFP ラベル

このルールグループは、名前空間プレフィックス `awswaf:managed:aws:acfp:` が付いたラベルを生成し、その後にカスタム名前空間およびラベル名が付いたラベルを生成します。ルールグループは、リクエストに複数のラベルを追加する場合があります。

`DescribeManagedRuleGroup` を呼び出すことにより、API を介してルールグループのすべてのラベルを取得できます。ラベルは、応答の `AvailableLabels` プロパティにリストされています。

Account Creation Fraud Prevention ルールリスト

次のセクションには、`AWSManagedRulesACFPRuleSet` の ACFP ルールとルールグループがウェブリクエストに追加するラベルが示されています。

このルールグループ内のすべてのルールでは、最初の 2 つの `UnsupportedCognitoIDP` と `AllRequests` を除き、ウェブリクエストトークンが必要です。トークンが提供する情報の説明については、「AWS WAF トークンの特性」を参照してください。

特に明記されていない限り、このルールグループのルールは、ルールグループの設定で指定したアカウント登録ページのパスとアカウント作成ページのパスにクライアントが送信するすべてのリクエストを検査します。このルールグループの設定の詳細については、「AWS WAF Fraud Control アカウント作成不正防止 (ACFP)」を参照してください。

> **Note**
>
> このドキュメントでは、このマネージドルールグループの最新の静的バージョンリリースについて説明します。バージョンの変更は、AWS マネージドルールの変更ログ の変更ログにレポートされます。他のバージョンの情報については、API コマンド DescribeManagedRuleGroup を使用してください。
> AWS マネージドルールルールのルールグループでルール用に公開する情報は、ルールを回避するために必要なものを不正なアクターに与えることなく、ルールを使用するために必要なものを提供することを目的としています。
> ここに記載されている以上の情報が必要な場合は、AWS サポート センター にお問い合わせください。

ルール名	説明とラベル
UnsupportedCognitoIDP	Amazon Cognito ユーザープールに向かうウェブトラフィックの有無を検査します。ACFP は Amazon Cognito ユーザープールでは使用できません。このルールは、他の ACFP ルールグループのルールがユーザープールのトラフィックの評価に使用されないようにすることに役立ちます。 ルールアクション: Block ラベル: awswaf:managed:aws:acfp:unsupported:cognito_idp および awswaf:managed:aws:acfp:UnsupportedCognitoIDP
AllRequests	登録ページのパスにアクセスするリクエストにルールアクションを適用します。ルールグループを設定するときに、登録ページのパスを設定します。 デフォルトでは、このルールは Challenge をリクエストに適用します。このアクションを適用することにより、ルールは、ルールグループ内の残りのルールによってリクエストが評価される前に、クライアントがチャレンジトークンを取得するようにします。 エンドユーザーがアカウント作成リクエストを送信する前に、登録ページのパスをロードするようにします。 トークンは、クライアントアプリケーション統合 SDK、ならびに CAPTCHA および Challenge のルールアクションによってリクエストに追加されます。最も効率的にトークンを

ルール名	説明とラベル
	取得するために、アプリケーション統合 SDK を使用することを強くお勧めします。詳細については、「でのクライアントアプリケーション統合 AWS WAF」を参照してください。 ルールアクション: Challenge ラベル: なし
RiskScoreHigh	IP アドレスやその他の非常に疑わしい要素が含まれるアカウント作成リクエストを検査します。この評価は通常、複数の寄与要因に基づいており、ルールグループがリクエストに追加する risk_score ラベルで確認できます。 ルールアクション: Block ラベル: awswaf:managed:aws:acfp:risk_score:high および awswaf:managed:aws:acfp:RiskScoreHigh このルールは、medium または low のリスクスコアラベルをリクエストに適用することもできます。 AWS WAF がウェブリクエストのリスクスコアの評価に成功しない場合、ルールはラベルを追加します。 awswaf:managed:aws:acfp:risk_score:evaluation_failed さらに、このルールは、IP レピュテーションや盗難された認証情報の評価など、特定のリスクスコアの寄与要因のリスクスコアの評価ステータスと結果を含む名前空間 awswaf:managed:aws:acfp:risk_score:contributor: のラベルを追加します。

ルール名	説明とラベル
`SignalCredentialCompromised`	盗まれた認証情報データベースで、アカウント作成リクエストで送信された認証情報を検索します。 このルールにより、新しいクライアントは、好ましいセキュリティ体制でアカウントを初期化するようになります。 **Note** カスタムブロックレスポンスを追加して、エンドユーザーに問題を説明し、続行方法を伝えることができます。詳細については、「ACFP の例: 侵害された認証情報についてのカスタムレスポンス」を参照してください。 ルールアクション: Block ラベル: `awswaf:managed:aws:acfp:signal:credential_compromised` および `awswaf:managed:aws:acfp:SignalCredentialCompromised` ルールグループは次の関連ラベルを適用しますが、アカウント作成のすべてのリクエストに認証情報があるわけではないため、それに対するアクションは実行されません: `awswaf:managed:aws:acfp:signal:missing_credential` 。

ルール名	説明とラベル
`SignalClientHumanInteractivityAbsentLow`	アカウント作成リクエストのトークンで、人間によるアプリケーションとの異常なインタラクティブ性を示すデータがないかどうかを検査します。人間のインタラクティビティは、マウスの動きやキーの押下などのインタラクションを通じて検出されます。ページに HTML フォームがある場合、人間によるインタラクションにはフォームとのインタラクションが含まれます。 **Note** このルールは、アカウント作成パスに対するリクエストのみを検査し、アプリケーション統合 SDK を実装している場合にのみ評価されます。SDK を実装することで、人間のインタラクティブ性を受動的にキャプチャし、その情報をリクエストトークンに保存できます。詳細については、「AWS WAF トークンの特性」および「でのクライアントアプリケーション統合 AWS WAF」を参照してください。 ルールアクション: CAPTCHA ラベル: なし。このルールはさまざまな要因に基づいて一致を決定するため、考えられるすべての一致シナリオに適用される個別のラベルはありません。 ルールグループは、次の 1 つ以上のラベルをリクエストに適用できます。

ルール名	説明とラベル
	awswaf:managed:aws:acfp:signal:client:human_interactivity: *low|medium|high* awswaf:managed:aws:acfp:SignalClientHumanInteractivityAbsent *Low|Medium|High* awswaf:managed:aws:acfp:signal:client:human_interactivity:insufficient_data awswaf:managed:aws:acfp:signal:form_detected .
AutomatedBrowser	クライアントブラウザが自動化されている可能性を示す要素がないかを検査します。 ルールアクション: Block ラベル: awswaf:managed:aws:acfp:signal:automated_browser および awswaf:managed:aws:acfp:AutomatedBrowser
BrowserInconsistency	ブラウザ調査のデータに一貫性がないかどうかを確認するために、リクエストのトークンを検査します。詳細については、「AWS WAF トークンの特性」を参照してください。 ルールアクション: CAPTCHA ラベル: awswaf:managed:aws:acfp:signal:browser_inconsistency および awswaf:managed:aws:acfp:BrowserInconsistency

ルール名	説明とラベル
VolumetricIpHigh	個々の IP アドレスから送信された大量のアカウント作成リクエストを検査します。大量とは、10 分ウィンドウにリクエストが 20 件を超えることです。 **Note** このルールが適用するしきい値は、レイテンシーによって若干異なる場合があります。大量の場合、ルールアクションが適用される前に、いくつかのリクエストが制限を超える可能性があります。 ルールアクション: CAPTCHA ラベル: `awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:high` および `awswaf:managed:aws:acfp:VolumetricIpHigh` ルールは、中程度の量 (10 分間の時間枠あたり 15 件以上のリクエスト) および少量 (10 分間の時間枠あたり 10 件以上のリクエスト) のリクエストに対して、以下のラベル `awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:medium` および `awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:low` を適用しますが、アクションは実行しません。

ルール名	説明とラベル
VolumetricSessionHigh	個々のクライアントセッションから送信された大量のアカウントリクエストを検査します。大量とは、30 分間の時間枠にリクエストが 10 件を超えることです。 **Note** このルールが適用するしきい値は、レイテンシーによって若干異なる場合があります。ルールアクションが適用される前に、いくつかのリクエストが制限を超えることがあります。 ルールアクション: Block ラベル: `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:high` および `awswaf:managed:aws:acfp:VolumetricSessionHigh` ルールグループは、中程度の量 (30 分間の時間枠あたり 5 件以上のリクエスト) および少量 (30 分間の時間枠あたり 1 件以上のリクエスト)のリクエストに対して、以下のラベル `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:medium` および `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:low` を適用しますが、アクションは実行しません。

ルール名	説明とラベル
AttributeUsernameTraversalHigh	異なるユーザー名を使用する単一のクライアントセッションからアカウント作成リクエストが高頻度で発生していないかどうかを検査します。30 分間のリクエスト数が 10 件を超えている場合は、大量であると評価されます。 **Note** このルールが適用するしきい値は、レイテンシーによって若干異なる場合があります。ルールアクションが適用される前に、いくつかのリクエストが制限を超えることがあります。 ルールアクション: Block ラベル: `awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:high` および `awswaf:managed:aws:acfp:AttributeUsernameTraversalHigh` ルールグループは、ユーザー名トラバーサルリクエストの中程度の量 (30分間の時間枠あたり 5 件以上のリクエスト) および少量 (30 分間の時間枠あたり 1 件以上のリクエスト) に対して、以下のラベル `awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:medium` および `awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:low` を適用しますが、アクションは実行しません。

ルール名	説明とラベル
VolumetricPhoneNumberHigh	同じ電話番号を使用する大量のアカウント作成リクエストが発生していないかを検査します。30 分間のリクエスト数が 10 件を超えている場合は、大量であると評価されます。 **Note** このルールが適用するしきい値は、レイテンシーによって若干異なる場合があります。ルールアクションが適用される前に、いくつかのリクエストが制限を超えることがあります。 ルールアクション: Block ラベル: awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:high および awswaf:managed:aws:acfp:VolumetricPhoneNumberHigh ルールグループは、中程度の量 (30 分間の時間枠あたり 5 件以上のリクエスト) および少量 (30 分間の時間枠あたり 1 件以上のリクエスト)のリクエストに対して、以下のラベル awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:medium および awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:low を適用しますが、アクションは実行しません。

ルール名	説明とラベル
`VolumetricAddressHigh`	同じ物理的な住所を使用する大量のアカウント作成リクエストが発生していないかを検査します。30 分間の時間枠あたりのリクエスト数が 100 件を超えている場合は、大量であると評価されます。 **Note** このルールが適用するしきい値は、レイテンシーによって若干異なる場合があります。ルールアクションが適用される前に、いくつかのリクエストが制限を超えることがあります。 ルールアクション: Block ラベル: `awswaf:managed:aws:acfp:aggregate:volumetric:address:high` および `awswaf:managed:aws:acfp:VolumetricAddressHigh`

ルール名	説明とラベル
`VolumetricAddressLow`	同じ物理的な住所を使用する少量または中程度の量のアカウント作成リクエストが発生していないかを検査します。中程度の評価のしきい値は 30 分間の時間枠あたり 50 件以上のリクエストであり、低評価のしきい値は 30 分間の時間枠あたり 10 件以上のリクエストです。 このルールは、中程度の量または少量のいずれかの場合にアクションを適用します。 **Note** このルールが適用するしきい値は、レイテンシーによって若干異なる場合があります。ルールアクションが適用される前に、いくつかのリクエストが制限を超えることがあります。 ルールアクション: CAPTCHA ラベル: `awswaf:managed:aws:acfp:aggregate:volumetric:address:` *`low|medium`* および `awswaf:managed:aws:acfp:VolumetricAddress` *`Low|Medium`*

ルール名	説明とラベル
`VolumetricIPSuccessfulResponse`	単一の IP アドレスに対する大量の正常なアカウント作成リクエストを検査します。このルールは、保護されたリソースからのアカウント作成リクエストに対する成功レスポンスを集計します。10 分間の時間枠あたりのリクエスト数が 10 件を超えている場合は、大量であると評価されます。 このルールは、アカウントの一括作成の試みからの保護に役立ちます。リクエストのみをカウントするルール `VolumetricIpHigh` よりもしきい値が低くなります。 レスポンス本文または JSON コンポーネントを検査するようにルールグループを設定している場合、 はこれらのコンポーネントタイプの最初の 65,536 バイト (64 KB) で成功または失敗のインジケータを検査 AWS WAF できます。 このルールは、同じ IP アドレスからの最新のログイン試行に対する保護されたリソースからの成功応答と失敗応答に基づいて、IP アドレスからの新しいウェブリクエストにルールアクションとラベリングを適用します。ルールグループを設定するときに、成功数と失敗数のカウント方法を定義します。 **Note** AWS WAF は、Amazon CloudFront ディストリビューションを保護する保護パック (ウェブ ACLs) でのみこのルールを評価します。

ルール名	説明とラベル
	Note このルールが適用するしきい値は、レイテンシーによって若干異なる場合があります。ルールがその後の試みに対して一致処理を開始する前に、正常なアカウント作成の試みが、許可されているよりも多くクライアントから送信される可能性があります。 ルールアクション: Block ラベル: `awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:high` および `awswaf:managed:aws:acfp:VolumetricIPSuccessfulResponse` ルールグループは、次の関連ラベルもリクエストに適用します。関連するアクションはありません。すべてのカウントは 10 分間の時間枠のものです。5 件以上の成功したリクエストには `awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:medium` 、1 件以上の成功したリクエストには `awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:low` 、10 件以上の失敗したリクエストには `awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:high` 、5 件以上の失敗した

ルール名	説明とラベル
	リクエストには awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:medium 、1 件以上の失敗したリクエストには awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:low です。

ルール名	説明とラベル
`VolumetricSessionSuccessful Response`	単一のクライアントセッションから送信されるアカウント作成リクエストに対する、保護されたリソースからの少量の成功したレスポンスを検査します。これは、アカウントの一括作成の試みからの保護に役立ちます。30 分間の時間枠あたりのリクエスト数が 1 件を超えている場合は、少量であると評価されます。 これは、アカウントの一括作成の試みからの保護に役立ちます。このルールは、リクエストのみをカウントするルール `VolumetricSessionHigh` よりも低いしきい値を使用します。 レスポンス本文または JSON コンポーネントを検査するようにルールグループを設定している場合、 はこれらのコンポーネントタイプの最初の 65,536 バイト (64 KB) で成功または失敗のインジケータを検査 AWS WAF できます。 このルールは、同じクライアントセッションからの最新のログイン試行に対する保護されたリソースからの成功応答と失敗応答に基づいて、クライアントセッションからの新しいウェブリクエストにルールアクションとラベリングを適用します。ルールグループを設定するときに、成功数と失敗数のカウント方法を定義します。 **Note** AWS WAF は、Amazon CloudFront ディストリビューションを保護する

ルール名	説明とラベル
	保護パック (ウェブ ACLs) でのみこのルールを評価します。 **Note** このルールが適用するしきい値は、レイテンシーによって若干異なる場合があります。ルールがその後の試みに対して一致処理を開始する前に、失敗したアカウント作成の試みが、許可されているよりも多くクライアントから送信される可能性があります。 ルールアクション: Block ラベル: `awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:low` および `awswaf:managed:aws:acfp:VolumetricSessionSuccessfulResponse` ルールグループは、次の関連ラベルもリクエストに適用します。すべてのカウントは 30 分間の時間枠のものです。10 件以上の成功したリクエストには `awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:high` 、5 件以上の成功したリクエストには `awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation`

ルール名	説明とラベル
	_response:medium 、10 件以上の失敗したリクエストには awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:high 、5 件以上の失敗したリクエストには awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:medium 、1 件以上の失敗したリクエストには awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:low です。
VolumetricSessionTokenReuseIp	アカウント作成リクエストを検査して、5 つを超える異なる IP アドレス間で単一のトークンが使用されていないかどうかをチェックします。 **Note** このルールが適用するしきい値は、レイテンシーによって若干異なる場合があります。ルールアクションが適用される前に、いくつかのリクエストが制限を超えることがあります。 ルールアクション: Block ラベル: awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:token_reuse:ip および awswaf:managed:aws:acfp:VolumetricSessionTokenReuseIp

AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループ

このセクションでは、 AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) マネージドルールグループの動作について説明します。

VendorName: `AWS`、名前: `AWSManagedRulesATPRuleSet`、WCU: 50

> **Note**
>
> このドキュメントでは、このマネージドルールグループの最新の静的バージョンリリースについて説明します。バージョンの変更は、AWS マネージドルールの変更ログ の変更ログにレポートされます。他のバージョンの情報については、API コマンド DescribeManagedRuleGroup を使用してください。
> AWS マネージドルールのルールグループでルール用に公開する情報は、ルールを回避するために必要なものを不正なアクターに与えることなく、ルールを使用するために必要なものを提供することを目的としています。
> ここに記載されている以上の情報が必要な場合は、AWS サポート センター にお問い合わせください。

AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) マネージドルールグループは、悪意のあるアカウント乗っ取りの試みの一部である可能性のあるリクエストにラベルを付けて管理します。ルールグループは、クライアントでアプリケーションのログインエンドポイントに送信するログイン試行を検査することでこれを行います。

- リクエスト検査 – ATP を使用すると、異常なログイン試行や盗まれた認証情報を使用するログイン試行を可視化して制御できるため、不正行為につながる可能性のあるアカウントの乗っ取りを防ぐことができます。ATP は、盗まれた認証情報のデータベースに照らして E メールとパスワードの組み合わせをチェックします。このデータベースは、漏洩された認証情報がダークウェブ上で新しく見つかると定期的に更新されます。ATP は、IP アドレスやクライアントセッションごとにデータを集約し、不審なリクエストを大量に送信するクライアントを検出してブロックします。
- レスポンス検査 – CloudFront ディストリビューションの場合、ATP ルールグループは、受信したログインリクエストを検査するだけでなく、ログイン試行に対するアプリケーションの応答も検査して、成功率と失敗率を追跡します。この情報を使用して、ATP はログイン失敗の回数が過度に多いクライアントセッションまたは IP アドレスを一時的にブロックできます。 AWS WAF は、レスポンス検査を非同期で実行するため、ウェブトラフィックのレイテンシーが大きくなることはありません。

このルールグループの使用に関する考慮事項

このルールグループには特定の設定が必要です。このルールグループを設定および実装するには、「AWS WAF Fraud Control アカウント乗っ取り防止 (ATP)」のガイダンスを参照してください。

このルールグループは、 AWS WAFでのインテリジェントな脅威の軽減保護の一部です。詳細については、「でのインテリジェントな脅威の軽減 AWS WAF」を参照してください。

> **Note**
>
> このマネージドルールグループを使用する場合、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

コストを抑え、ウェブトラフィックを希望どおりに管理していることを確実にするには、でのインテリジェントな脅威軽減のベストプラクティス AWS WAF のガイダンスに従ってこのルールグループを使用してください。

このルールグループは、Amazon Cognito ユーザープールでは使用できません。このルールグループを使用する保護パック (ウェブ ACL) をユーザープールに関連付けることはできません。また、このルールグループをユーザープールに既に関連付けられた保護パック (ウェブ ACL) に追加することはできません。

このルールグループによって追加されるラベル

このマネージドルールグループは、評価対象のウェブリクエストに保護パック (ウェブ ACL) 内のこのルールグループの後に実行されるルールでも使用できるラベルを追加します。 AWS WAF は、Amazon CloudWatch メトリクスにもラベルを記録します。ラベルとラベルメトリクスに関する一般的な情報については、「ウェブリクエストのラベル付け」および「ラベルメトリクスとディメンション」を参照してください。

トークンラベル

このルールグループは、 AWS WAF トークン管理を使用して、 AWS WAF トークンのステータスに従ってウェブリクエストを検査し、ラベル付けします。 は、クライアントセッションの追跡と検証にトークン AWS WAF を使用します。

トークンおよびトークンの管理の詳細については、「AWS WAF インテリジェントな脅威の軽減におけるトークンの使用」を参照してください。

ここで説明するラベルコンポーネントについては、「でのラベル構文と命名要件 AWS WAF」を参照してください。

クライアントセッションラベル

ラベルには、 AWS WAF トークン管理がクライアントセッションを識別するために使用する一意の識別子`awswaf:managed:token:id:`*`identifier`*が含まれています。この識別子は、クライアントが使用していたトークンを破棄した後など、新しいトークンを取得すると変わる可能性があります。

> **Note**
>
> AWS WAF は、このラベルの Amazon CloudWatch メトリクスを報告しません。

ブラウザフィンガープリントラベル

ラベルには、 AWS WAF トークン管理がさまざまなクライアントブラウザシグナルから計算する堅牢なブラウザフィンガープリント識別子`awswaf:managed:token:fingerprint:`*`fingerprint-identifier`*が含まれています。この識別子は、複数のトークン取得の試行全体で同じままです。フィンガープリント識別子は、単一のクライアントに対して一意ではありません。

> **Note**
>
> AWS WAF は、このラベルの Amazon CloudWatch メトリクスを報告しません。

トークンステータスラベル: ラベル名前空間プレフィックス

トークンステータスラベルは、トークン、チャレンジのステータス、およびそれに含まれる CAPTCHA 情報を報告します。

各トークンステータスラベルは、次のプレフィクスの 1 つで始まります。

- `awswaf:managed:token:`— トークンの一般的なステータスを報告したり、トークンのチャレンジ情報のステータスを報告したりするために使用されます。
- `awswaf:managed:captcha:`— トークンの CAPTCHA 情報のステータスを報告するために使用されます。

トークンステータスラベル: ラベル名

プレフィックスに続いて、ラベルの残りの部分には詳細なトークンステータス情報が表示されます。

- accepted - リクエストトークンが存在し、以下の内容が含まれています。
  - 有効なチャレンジまたは CAPTCHA ソリューション。
  - 有効期限が切れていないチャレンジまたは CAPTCHA タイムスタンプ。
  - 保護パック (ウェブ ACL) に有効なドメイン仕様。

  例: ラベル awswaf:managed:token:accepted には、ウェブリクエストのトークンに有効なチャレンジソリューション、有効期限が切れていないチャレンジタイムスタンプ、および有効なドメインがあることが示されています。
- rejected - リクエストトークンは存在するが、承認基準を満たしていない。

  トークン管理では、拒否されたラベルに加えて、理由を示すカスタムラベル名前空間と名前が追加されます。
  - rejected:not_solved — トークンにチャレンジまたは CAPTCHA ソリューションがない。
  - rejected:expired — 保護パック (ウェブ ACL) に設定されているトークンイミュニティ時間によると、トークンのチャレンジまたは CAPTCHA タイムスタンプの有効期限が切れている。
  - rejected:domain_mismatch — トークンのドメインが、保護パック (ウェブ ACL) のトークンドメイン設定と一致しない。
  - rejected:invalid – 指定されたトークンを読み取ることが AWS WAF できませんでした。

  例: ラベル awswaf:managed:captcha:rejected と awswaf:managed:captcha:rejected:expired とともに、トークンの CAPTCHA タイムスタンプがウェブ ACL で設定されている CAPTCHA トークンのイミュニティ時間を超えたために、リクエストには有効な CAPTCHA 解決がなかったことが示されています。
- absent — リクエストにトークンがないか、トークンマネージャーがそれを読み取れなかった。

  例: ラベル awswaf:managed:captcha:absent には、リクエストにトークンがないことが示されています。

ATP ラベル

ATP マネージドルールグループは、名前空間プレフィックス awswaf:managed:aws:atp: が付いたラベルを生成し、その後にカスタム名前空間およびラベル名が付いたラベルを生成します。

ルールグループは、ルールリストに記載されているラベルに加えて、次のラベルのいずれかを追加する場合があります。

- awswaf:managed:aws:atp:signal:credential_compromised – リクエストで送信された認証情報が、盗まれた認証情報データベースに含まれていることを示します。
- awswaf:managed:aws:atp:aggregate:attribute:suspicious_tls_fingerprint – 保護されている Amazon CloudFront ディストリビューションでのみ利用できます。クライアントセッションが、疑わしい TLS フィンガープリントを使用した複数のリクエストを送信したことを示します。
- awswaf:managed:aws:atp:aggregate:volumetric:session:token_reuse:ip - 5 つを超える異なる IP アドレス間で単一のトークンが使用されていることを示します。このルールが適用するしきい値は、レイテンシーによって若干異なる場合があります。ラベルが適用される前に、いくつかのリクエストが制限を超えることがあります。

DescribeManagedRuleGroup を呼び出すことにより、API を介してルールグループのすべてのラベルを取得できます。ラベルは、応答の AvailableLabels プロパティにリストされています。

アカウント乗っ取り防止のルールリスト

次のセクションには、AWSManagedRulesATPRuleSet の ATP ルールとルールグループがウェブリクエストに追加するラベルが示されています。

> **Note**
>
> このドキュメントでは、このマネージドルールグループの最新の静的バージョンリリースについて説明します。バージョンの変更は、AWS マネージドルールの変更ログ の変更ログにレポートされます。他のバージョンの情報については、API コマンド DescribeManagedRuleGroup を使用してください。
> AWS マネージドルールのルールグループでルール用に公開する情報は、ルールを回避するために必要なものを不正なアクターに与えることなく、ルールを使用するために必要なものを提供することを目的としています。
> ここに記載されている以上の情報が必要な場合は、AWS サポート センター にお問い合わせください。

ルール名	説明とラベル
UnsupportedCognitoIDP	Amazon Cognito ユーザープールに向かうウェブトラフィックの有無を検査します。ATP は Amazon Cognito ユーザープールでは使用で

ルール名	説明とラベル
	きません。このルールは、他の ATP ルールグループのルールがユーザープールのトラフィックの評価に使用されないようにすることに役立ちます。 ルールアクション: Block ラベル: `awswaf:managed:aws:atp:unsupported:cognito_idp` および `awswaf:managed:aws:atp:UnsupportedCognitoIDP`

ルール名	説明とラベル
VolumetricIpHigh	個々の IP アドレスから送信された大量のリクエストを検査します。大量とは、10 分ウィンドウにリクエストが 20 件を超えることです。 **Note** このルールが適用するしきい値は、レイテンシーによって若干異なる場合があります。大量の場合、ルールアクションが適用される前に、いくつかのリクエストが制限を超える可能性があります。 ルールアクション: Block ラベル: awswaf:managed:aws:atp:aggregate:volumetric:ip:high および awswaf:managed:aws:atp:VolumetricIpHigh ルールグループは、中程度の量 (10 分間の時間枠あたり 15 件以上のリクエスト) および少量 (10 分間の時間枠あたり 10 件以上のリクエスト) のリクエストに対して、以下のラベル awswaf:managed:aws:atp:aggregate:volumetric:ip:medium および awswaf:managed:aws:atp:aggregate:volumetric:ip:low を適用しますが、アクションは実行しません。

ルール名	説明とラベル
`VolumetricSession`	個々のクライアントセッションから送信された大量のリクエストを検査します。しきい値は、30 分ウィンドウあたり 20 を超えるリクエスト数に設定します。 この検査は、ウェブリクエストにトークンがある場合にのみ適用されます。トークンは、アプリケーション統合 SDK、ならびに CAPTCHA および Challenge のルールアクションによってリクエストに追加されます。詳細については、「AWS WAF インテリジェントな脅威の軽減におけるトークンの使用」を参照してください。 **Note** このルールが適用するしきい値は、レイテンシーによって若干異なる場合があります。ルールアクションが適用される前に、いくつかのリクエストが制限を超えることがあります。 ルールアクション: Block ラベル: `awswaf:managed:aws:atp:aggregate:volumetric:session` および `awswaf:managed:aws:atp:VolumetricSession`

ルール名	説明とラベル
AttributeCompromisedCredentials	盗まれた認証情報を使用する同じクライアントセッションからの複数リクエストを検査します。 ルールアクション: Block ラベル: awswaf:managed:aws:atp:aggregate:attribute:compromised_credentials および awswaf:managed:aws:atp:AttributeCompromisedCredentials
AttributeUsernameTraversal	ユーザー名トラバーサルを使用する同じクライアントセッションからの複数リクエストを検査します。 ルールアクション: Block ラベル: awswaf:managed:aws:atp:aggregate:attribute:username_traversal および awswaf:managed:aws:atp:AttributeUsernameTraversal
AttributePasswordTraversal	パスワードトラバーサルと同じユーザー名を使用する複数のリクエストを検査します。 ルールアクション: Block ラベル: awswaf:managed:aws:atp:aggregate:attribute:password_traversal および awswaf:managed:aws:atp:AttributePasswordTraversal

ルール名	説明とラベル
`AttributeLongSession`	長期に継続するセッションを使用する同じクライアントセッションからの複数リクエストを検査します。しきい値は、30 分ごとに少なくとも 1 つのログインリクエストが存在する 6 時間を超えるトラフィックです。 この検査は、ウェブリクエストにトークンがある場合にのみ適用されます。トークンは、アプリケーション統合 SDK、ならびに CAPTCHA および Challenge のルールアクションによってリクエストに追加されます。詳細については、「AWS WAF インテリジェントな脅威の軽減におけるトークンの使用」を参照してください。 ルールアクション: Block ラベル: `awswaf:managed:aws:atp:aggregate:attribute:long_session` および `awswaf:managed:aws:atp:AttributeLongSession`

ルール名	説明とラベル
`TokenRejected`	トークン管理によって拒否された AWS WAF トークンを含むリクエストを検査します。 この検査は、ウェブリクエストにトークンがある場合にのみ適用されます。トークンは、アプリケーション統合 SDK、ならびに CAPTCHA および Challenge のルールアクションによってリクエストに追加されます。詳細については、「AWS WAF インテリジェントな脅威の軽減におけるトークンの使用」を参照してください。 ルールアクション: Block ラベル: なし。トークンが拒否されたかどうか確認するには、ラベル一致ルールを使用してラベル `awswaf:managed:token:rejected` を照合します。
`SignalMissingCredential`	認証情報を含むリクエストに、ユーザー名またはパスワードが不足しているかどうか検査します。 ルールアクション: Block ラベル: `awswaf:managed:aws:atp:signal:missing_credential` および `awswaf:managed:aws:atp:SignalMissingCredential`

ルール名	説明とラベル
`VolumetricIpFailedLoginResponseHigh`	最近のログイン試行の失敗率が過度に高い IP アドレスを検査します。大量とは、10 分間の時間枠に 1 つの IP アドレスからの失敗したログインリクエストが 10 件を超えることです。 レスポンス本文または JSON コンポーネントを検査するようにルールグループを設定している場合、 はこれらのコンポーネントタイプの最初の 65,536 バイト (64 KB) で成功または失敗のインジケータを検査 AWS WAF できます。 このルールは、同じ IP アドレスからの最新のログイン試行に対する保護されたリソースからの成功応答と失敗応答に基づいて、IP アドレスからの新しいウェブリクエストにルールアクションとラベリングを適用します。ルールグループを設定するときに、成功数と失敗数のカウント方法を定義します。 **Note** AWS WAF は、Amazon CloudFront ディストリビューションを保護する保護パック (ウェブ ACLs) でのみこのルールを評価します。 **Note** このルールが適用するしきい値は、レイテンシーによって若干異なる場合があります。ルールがその後のログイン試行に対して一致処理を開始する前

ルール名	説明とラベル
	に、許可されているよりも多い回数の失敗したログイン試行がクライアントから送信される可能性があります。 ルールアクション: Block ラベル: awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:high および awswaf:managed:aws:atp:VolumetricIpFailedLoginResponseHigh ルールグループは、次の関連ラベルもリクエストに適用します。関連するアクションはありません。すべてのカウントは 10 分間の時間枠のものです。5 件以上の失敗したリクエストには awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:medium 、1 件以上の失敗したリクエストには awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:low 、10 件以上の成功したリクエスト には awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:high 、5 件以上の成功したリクエストには awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:medium 、1 件以上の成功したリクエストには awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:low です。

ルール名	説明とラベル

ルール名	説明とラベル
`VolumetricSessionFailedLoginResponseHigh`	最近のログイン試行の失敗率が過度に高いクライアントセッションを検査します。大量とは、30 分間の時間枠にクライアントセッションからの失敗したログインリクエストが 10 件を超えることです。 レスポンス本文または JSON コンポーネントを検査するようにルールグループを設定している場合、 はこれらのコンポーネントタイプの最初の 65,536 バイト (64 KB) で成功または失敗のインジケータを検査 AWS WAF できます。 このルールは、同じクライアントセッションからの最新のログイン試行に対する保護されたリソースからの成功応答と失敗応答に基づいて、クライアントセッションからの新しいウェブリクエストにルールアクションとラベリングを適用します。ルールグループを設定するときに、成功数と失敗数のカウント方法を定義します。 **Note** AWS WAF は、Amazon CloudFront ディストリビューションを保護する保護パック (ウェブ ACLs) でのみこのルールを評価します。 **Note** このルールが適用するしきい値は、レイテンシーによって若干異なる場合があります。ルールがその後のログイ

ルール名	説明とラベル
	ン試行に対して一致処理を開始する前に、許可されているよりも多い回数の失敗したログイン試行がクライアントから送信される可能性があります。 この検査は、ウェブリクエストにトークンがある場合にのみ適用されます。トークンは、アプリケーション統合 SDK、ならびに CAPTCHA および Challenge のルールアクションによってリクエストに追加されます。詳細については、「AWS WAF インテリジェントな脅威の軽減におけるトークンの使用」を参照してください。 ルールアクション: Block ラベル: `awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:high` および `awswaf:managed:aws:atp:VolumetricSessionFailedLoginResponseHigh` ルールグループは、次の関連ラベルもリクエストに適用します。関連するアクションはありません。すべてのカウントは 30 分間の時間枠のものです。5 件以上の失敗したリクエストには `awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:medium` 、1 件以上の失敗したリクエストには `awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:low` 、10 件以上の成功したリクエスト には `awswaf:managed:aws`

ルール名	説明とラベル
	`:atp:aggregate:volumetric:session:successful_login_response:high` 、5 件以上の成功したリクエストには `awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:medium` 、1 件以上の成功したリクエストには `awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:low` です。

AWS WAF Bot Control ルールグループ

このセクションでは、Bot Control マネージドルールグループの動作について説明します。

VendorName: `AWS`、名前: `AWSManagedRulesBotControlRuleSet`、WCU: 50

> **Note**
>
> このドキュメントでは、このマネージドルールグループの最新の静的バージョンリリースについて説明します。バージョンの変更は、AWS マネージドルールの変更ログ の変更ログにレポートされます。他のバージョンの情報については、API コマンド DescribeManagedRuleGroup を使用してください。
> AWS マネージドルールルールのルールグループでルール用に公開する情報は、ルールを回避するために必要なものを不正なアクターに与えることなく、ルールを使用するために必要なものを提供することを目的としています。
> Bot Control の新しいボット分類をリクエストする必要がある場合、またはここで説明されていない追加情報が必要な場合は、AWS サポート センターにお問い合わせください。

Bot Control マネージドルールグループは、ボットからのリクエストを管理するルールを提供します。ボットは過剰なリソースを消費し、ビジネスメトリクスを歪め、ダウンタイムを引き起こし、悪意のあるアクティビティを実行する可能性があります。

保護レベル

Bot Control マネージドルールグループには、次の 2 レベルの保護から選択できます。

- 共通 – ウェブスクレイピングフレームワーク、検索エンジン、自動ブラウザなど、さまざまな自己識別ボットを検出します。このレベルの Bot Control 保護は、静的リクエストデータ分析など、従来のボット検出技術を使用して一般的なボットを識別します。ルールはこれらのボットからのトラフィックにラベルを付け、検証できないものはブロックします。
- ターゲットを絞った – 一般的な保護機能に加え、自己識別を行わない高度なボットに対するターゲットを絞った検出機能も追加されています。ターゲットを絞った保護は、レート制限と CAPTCHA およびバックグラウンドブラウザのチャレンジの組み合わせを使用してボットアクティビティを軽減します。
  - **TGT_** – ターゲットを絞った保護を提供するルールには、TGT_ で始まる名前が付いています。すべてのターゲットを絞った保護では、ブラウザ調査、フィンガープリント、行動ヒューリスティックなどの検出技術を使用して不正なボットトラフィックを識別します。
  - **TGT_ML_** – 機械学習を使用するターゲットを絞った保護のルールには、TGT_ML_ で始まる名前が付いています。これらのルールでは、ウェブサイトトラフィック統計の自動機械学習分析を使用して、分散された調整されたボットアクティビティを示す異常な動作を検出します。 は、タイムスタンプ、ブラウザの特性、以前にアクセスした URL などのウェブサイトトラフィックに関する統計 AWS WAF を分析し、Bot Control 機械学習モデルを改善します。機械学習機能はデフォルトで有効になっていますが、ルールグループ設定で無効にすることができます。機械学習が無効になっている場合、 AWS WAF はこれらのルールを評価しません。

ターゲットを絞った保護レベルと AWS WAF レートベースのルールステートメントの両方がレート制限を提供します。この 2 つのオプションの比較については、「レートベースのルールとターゲットを絞った Bot Control ルールにおけるレート制限のオプション」を参照してください。

このルールグループの使用に関する考慮事項

このルールグループは、 AWS WAFでのインテリジェントな脅威の軽減保護の一部です。詳細については、「でのインテリジェントな脅威の軽減 AWS WAF」を参照してください。

> **Note**
>
> このマネージドルールグループを使用する場合、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

コストを抑え、ウェブトラフィックを希望どおりに管理していることを確実にするには、でのインテリジェントな脅威軽減のベストプラクティス AWS WAF のガイダンスに従ってこのルールグループを使用してください。

ボットの予測を改善するために、ターゲットを絞った保護レベルの ML に基づくルールの機械学習 (ML) モデルを定期的に更新しています。ML に基づくルールには、TGT_ML_ で始まる名前があります。これらのルールによって行われたボット予測に突然、大幅な変更が見られた場合は、アカウントマネージャーを通じて当社に連絡するか、「AWS サポート センター」でケースを開いてください。

このルールグループによって追加されるラベル

このマネージドルールグループは、評価対象のウェブリクエストに保護パック (ウェブ ACL) 内のこのルールグループの後に実行されるルールでも使用できるラベルを追加します。 AWS WAF は、Amazon CloudWatch メトリクスにもラベルを記録します。ラベルとラベルメトリクスに関する一般的な情報については、「ウェブリクエストのラベル付け」および「ラベルメトリクスとディメンション」を参照してください。

トークンラベル

このルールグループは、 AWS WAF トークン管理を使用して、 AWS WAF トークンのステータスに従ってウェブリクエストを検査し、ラベル付けします。 は、クライアントセッションの追跡と検証にトークン AWS WAF を使用します。

トークンおよびトークンの管理の詳細については、「AWS WAF インテリジェントな脅威の軽減におけるトークンの使用」を参照してください。

ここで説明するラベルコンポーネントについては、「でのラベル構文と命名要件 AWS WAF」を参照してください。

クライアントセッションラベル

ラベルには、 AWS WAF トークン管理がクライアントセッションを識別するために使用する一意の識別子`awswaf:managed:token:id:`*`identifier`*が含まれています。この識別子は、クライアントが使用していたトークンを破棄した後など、新しいトークンを取得すると変わる可能性があります。

> **Note**
>
> AWS WAF は、このラベルの Amazon CloudWatch メトリクスを報告しません。

ブラウザフィンガープリントラベル

ラベルには、 AWS WAF トークン管理がさまざまなクライアントブラウザシグナルから計算する堅牢なブラウザフィンガープリント識別子`awswaf:managed:token:fingerprint:`*`fingerprint-identifier`*が含まれています。この識別子は、複数のトークン取得の試行全体で同じままです。フィンガープリント識別子は、単一のクライアントに対して一意ではありません。

> **Note**
>
> AWS WAF は、このラベルの Amazon CloudWatch メトリクスを報告しません。

トークンステータスラベル: ラベル名前空間プレフィックス

トークンステータスラベルは、トークン、チャレンジのステータス、およびそれに含まれる CAPTCHA 情報を報告します。

各トークンステータスラベルは、次のプレフィクスの 1 つで始まります。

- `awswaf:managed:token:` — トークンの一般的なステータスを報告したり、トークンのチャレンジ情報のステータスを報告したりするために使用されます。
- `awswaf:managed:captcha:` — トークンの CAPTCHA 情報のステータスを報告するために使用されます。

トークンステータスラベル: ラベル名

プレフィックスに続いて、ラベルの残りの部分には詳細なトークンステータス情報が表示されます。

- `accepted` - リクエストトークンが存在し、以下の内容が含まれています。
  - 有効なチャレンジまたは CAPTCHA ソリューション。
  - 有効期限が切れていないチャレンジまたは CAPTCHA タイムスタンプ。
  - 保護パック (ウェブ ACL) に有効なドメイン仕様。

  例: ラベル `awswaf:managed:token:accepted` には、ウェブリクエストのトークンに有効なチャレンジソリューション、有効期限が切れていないチャレンジタイムスタンプ、および有効なドメインがあることが示されています。
- `rejected` - リクエストトークンは存在するが、承認基準を満たしていない。

トークン管理では、拒否されたラベルに加えて、理由を示すカスタムラベル名前空間と名前が追加されます。

- `rejected:not_solved` — トークンにチャレンジまたは CAPTCHA ソリューションがない。
- `rejected:expired` — 保護パック (ウェブ ACL) に設定されているトークンイミュニティ時間によると、トークンのチャレンジまたは CAPTCHA タイムスタンプの有効期限が切れている。
- `rejected:domain_mismatch` — トークンのドメインが、保護パック (ウェブ ACL) のトークンドメイン設定と一致しない。
- `rejected:invalid` – 指定されたトークンを読み AWS WAF 取れませんでした。

例: ラベル `awswaf:managed:captcha:rejected` と `awswaf:managed:captcha:rejected:expired` とともに、トークンの CAPTCHA タイムスタンプがウェブ ACL で設定されている CAPTCHA トークンのイミュニティ時間を超えたために、リクエストには有効な CAPTCHA 解決がなかったことが示されています。

- `absent` — リクエストにトークンがないか、トークンマネージャーがそれを読み取れなかった。

例: ラベル `awswaf:managed:captcha:absent` には、リクエストにトークンがないことが示されています。

Bot Control ラベル

Bot Control マネージドルールグループは、名前空間プレフィックス `awswaf:managed:aws:bot-control:` の後にカスタム名前空間およびラベル名が続くラベルを生成します。ルールグループは、リクエストに複数のラベルを追加する場合があります。

各ラベルは、Bot Control ルールの検出結果を反映しています。

- `awswaf:managed:aws:bot-control:bot:` – リクエストに関連付けられたボットに関する情報。
  - `awswaf:managed:aws:bot-control:bot:name:<name>` – ボット名は (利用可能な場合)、たとえばカスタム名前空間 `bot:name:slurp`、`bot:name:googlebot`、`bot:name:pocket_parser`。
  - `awswaf:managed:aws:bot-control:bot:name:<rfc_name>` – WBA 署名の RFC 製品トークンを使用して特定のボットを識別します。これは、特定のボットの詳細なカスタムルールを作成するために使用されます。たとえば、他のクローラを許可`GoogleBot`し、レート制限します。

- awswaf:managed:aws:bot-control:bot:category:*<category>* – ボットのカテゴリ AWS WAF。 bot:category:search_engineや などで定義されますbot:category:content_fetcher。
- awswaf:managed:aws:bot-control:bot:account:*<hash>* – Amazon Bedrock エージェントコアを使用するボットのみ。このラベルには、エージェントを所有する AWS アカウントを一意に識別する不透明なハッシュが含まれています。このラベルを使用して、ログにアカウント IDs を公開することなく、特定の AWS アカウントのボットを許可、ブロック、またはレート制限するカスタムルールを作成します。
- awswaf:managed:aws:bot-control:bot:web_bot_auth:*<status>* – ウェブボット認証 (WBA) 検証がリクエストに対して実行されるときに適用されます。ステータスサフィックスは、検証結果を示します。
  - web_bot_auth:verified – パブリックキーディレクトリに対して正常に検証された署名
  - web_bot_auth:invalid – 署名はありますが、Cryptograpic の検証に失敗しました
  - web_bot_auth:expired – 期限切れの暗号キーを使用した署名
  - web_bot_auth:unknown_bot – キーディレクトリにキー ID が見つかりません

  > **Note**
  >
  > web_bot_auth:verified ラベルが存在する場合、 ルールCategory*<category_name>*と TGT_TokenAbsentルールが一致しないため、検証済みの WBA ホストを続行できます。

- awswaf:managed:aws:bot-control:bot:organization:*<organization>* – ボットのパブリッシャー (例: bot:organization:google)。
- awswaf:managed:aws:bot-control:bot:verified – 自己を識別し、Bot Control が検証できたボットを示すために使用されます。これは、一般的な望ましいボットに使用され、bot:category:search_engine のようなカテゴリラベルや bot:name:googlebot のような名前ラベルと組み合わせると便利です。

  > **Note**
  >
  > Bot Control は、ウェブリクエストの送信元の IP アドレスを使用して、ボットが検証されているかどうかを判断します。 AWS WAF 転送される IP 設定を使用して別の IP アドレスソースを検査するように設定することはできません。プロキシまたはロードバランサーを介してルーティングするボットを検証した場合、Bot Control ルールグループの前に実行するルールを追加してこの問題に対処します。転送された IP アドレスを使用

し、検証済みのボットからのリクエストを明示的に許可するように新しいルールを設定します。転送した IP アドレスの詳細については、「で転送された IP アドレスを使用する AWS WAF」を参照してください。

- awswaf:managed:aws:bot-control:bot:vendor:*<vendor_name>* – 検証済みボットのベンダーまたはオペレーターを識別します。現在、Agentcore でのみ使用できます。を使用して、個々のボット名に関係なく、特定のボットベンダーを許可またはブロックするカスタムルールを作成します。
- awswaf:managed:aws:bot-control:bot:user_triggered:verified – 検証済みのボットに類似しているが、エンドユーザーによって直接呼び出される可能性のあるボットを示すために使用されます。このカテゴリのボットは、Bot Control のルールによって未検証のボットのように扱われます。
- awswaf:managed:aws:bot-control:bot:developer_platform:verified – 検証済みのボットに類似しているが、Google Apps Script などのデベロッパープラットフォームによってスクリプト作成のために使用されるボットを示すために使用されます。このカテゴリのボットは、Bot Control のルールによって未検証のボットのように扱われます。
- awswaf:managed:aws:bot-control:bot:unverified – 自己を識別するボットを示すために使用されるため、名前を付けて分類できます。ただし、そのボットのアイデンティティを個別に検証する場合に使用する情報は公開されていません。これらの種類のボットシグネチャは改ざんされる可能性があるため、未検証として扱われます。

- awswaf:managed:aws:bot-control:targeted:*<additional-details>* — Bot Control の対象となる保護に固有のラベルに使用されます。
- awswaf:managed:aws:bot-control:signal:*<signal-details>* および awswaf:managed:aws:bot-control:targeted:signal:*<signal-details>* — 一部の状況において、リクエストに関する追加情報を提供するために使用されます。

  シグナルラベルの例は、次のとおりです。これは網羅的なリストではありません。

  - awswaf:managed:aws:bot-control:signal:cloud_service_provider:*<CSP>* – リクエストのクラウドサービスプロバイダー (CSP) を示します。CSP の例には Amazon Web Services インフラストラクチャの aws、Google Cloud Platform (GCP) インフラストラクチャの gcp、Microsoft Azure クラウドサービスの azure、Oracle Cloud サービスの oracle などがあります。
  - awswaf:managed:aws:bot-control:targeted:signal:browser_automation_extension — Selenium IDE など、自動化をサポートするブラウザー拡張機能が検出されたことを示します。

このラベルは、ユーザーがこのタイプの拡張をインストールすると、ユーザーが自発的に使用していない場合でも追加されます。このためのラベル照合ルールを実装する場合は、ルールロジックとアクション設定で誤検出が発生する可能性があることに注意してください。たとえば、オートメーションが使用されていることを確保するために、Block の代わりに CAPTCHA アクションを使用したり、このラベルマッチを他のラベルマッチと組み合わせたりすることができます。

- `awswaf:managed:aws:bot-control:signal:automated_browser` — リクエストに、クライアントブラウザが自動化されている可能性があることを示す要素が含まれていることを示します。
- `awswaf:managed:aws:bot-control:targeted:signal:automated_browser` – リクエストの AWS WAF トークンに、クライアントブラウザが自動化されている可能性があることを示すインジケータが含まれていることを示します。

`DescribeManagedRuleGroup` を呼び出すことにより、API を介してルールグループのすべてのラベルを取得できます。ラベルは、応答の `AvailableLabels` プロパティにリストされています。

Bot Control マネージドルールグループは、一般的に許可されている検証可能な一連のボットにラベルを適用します。ルールグループは、これらの検証済みボットをブロックしません。必要に応じて、Bot Control マネージドルールグループによって適用されたラベルを使用するカスタムルールを記述することで、それらのボットまたはそのサブセットをブロックできます。これと例の詳細については、「AWS WAF ボットコントロール」を参照してください。

Bot Control のルールリスト

このセクションには Bot Control ルールが表示されています。

> **Note**
>
> このドキュメントでは、このマネージドルールグループの最新の静的バージョンリリースについて説明します。バージョンの変更は、AWS マネージドルールの変更ログ の変更ログにレポートされます。他のバージョンの情報については、API コマンド DescribeManagedRuleGroup を使用してください。
> AWS マネージドルールルールのルールグループでルール用に公開する情報は、ルールを回避するために必要なものを不正なアクターに与えることなく、ルールを使用するために必要なものを提供することを目的としています。
> Bot Control の新しいボット分類をリクエストする必要がある場合、またはここで説明されていない追加情報が必要な場合は、AWS サポート センターにお問い合わせください。

ルール名	説明
CategoryAdvertising	広告目的で使用されるボットを検査します。例えば、プログラムによるウェブサイトへのアクセスを必要とするサードパーティーの広告サービスを使用する場合があります。 未検証のボットにのみ適用されるルールアクション: Block ラベル: awswaf:managed:aws:bot-control:bot:category:advertising および awswaf:managed:aws:bot-control:CategoryAdvertising 検証済みボットについては、ルールグループはこのルールに一致もしないし、アクションを実行しませんが、ボット名とカテゴリにラベル付け、また、ラベル awswaf:managed:aws:bot-control:bot:verified を追加します。
CategoryArchiver	アーカイブ目的で使用されるボットを検査します。これらのボットは、アーカイブを作成する目的でウェブをクロールし、コンテンツをキャプチャします。 未検証のボットにのみ適用されるルールアクション: Block ラベル: awswaf:managed:aws:bot-control:bot:category:archiver および awswaf:managed:aws:bot-control:CategoryArchiver 検証済みボットについては、ルールグループはこのルールに一致もしないし、アクションを実

ルール名	説明
	行しませんが、ボット名とカテゴリにラベル付け、また、ラベル awswaf:managed:aws:bot-control:bot:verified を追加します。
CategoryContentFetcher	ユーザーに代わってアプリケーションのウェブサイトにアクセスし、RSS フィードのようなコンテンツを取得したり、コンテンツを検証したりするボットを検査します。 未検証のボットにのみ適用されるルールアクション: Block ラベル: awswaf:managed:aws:bot-control:bot:category:content_fetcher および awswaf:managed:aws:bot-control:CategoryContentFetcher 検証済みボットについては、ルールグループはこのルールに一致もしないし、アクションを実行しませんが、ボット名とカテゴリにラベル付け、また、ラベル awswaf:managed:aws:bot-control:bot:verified を追加します。

ルール名	説明
`CategoryEmailClient`	アプリケーションのウェブサイトを指し示すメール内のリンクをチェックするボットを検査します。これには、E メール内のリンクを確認したり、疑わしい電子メールにフラグを立てたりする企業や E メールプロバイダーによって実行されるボットが含まれます。 未検証のボットにのみ適用されるルールアクション: Block ラベル: `awswaf:managed:aws:bot-control:bot:category:email_client` および `awswaf:managed:aws:bot-control:CategoryEmailClient` 検証済みボットについては、ルールグループはこのルールに一致もしないし、アクションを実行しませんが、ボット名とカテゴリにラベル付け、また、ラベル `awswaf:managed:aws:bot-control:bot:verified` を追加します。

ルール名	説明
CategoryHttpLibrary	さまざまなプログラミング言語の HTTP ライブラリからボットによって生成されたリクエストを検査します。これらには、許可またはモニタリングする API リクエストが含まれる場合があります。 未検証のボットにのみ適用されるルールアクション: Block ラベル: awswaf:managed:aws:bot-control:bot:category:http_library および awswaf:managed:aws:bot-control:CategoryHttpLibrary 検証済みボットについては、ルールグループはこのルールに一致もしないし、アクションを実行しませんが、ボット名とカテゴリにラベル付け、また、ラベル awswaf:managed:aws:bot-control:bot:verified を追加します。

ルール名	説明
CategoryLinkChecker	壊れたリンクをチェックするボットを検査します。 未検証のボットにのみ適用されるルールアクション: Block ラベル: awswaf:managed:aws:bot-control:bot:category:link_checker および awswaf:managed:aws:bot-control:CategoryLinkChecker 検証済みボットについては、ルールグループはこのルールに一致もしないし、アクションを実行しませんが、ボット名とカテゴリにラベル付け、また、ラベル awswaf:managed:aws:bot-control:bot:verified を追加します。
CategoryMiscellaneous	他のカテゴリに一致しないその他のボットを検査します。 未検証のボットにのみ適用されるルールアクション: Block ラベル: awswaf:managed:aws:bot-control:bot:category:miscellaneous および awswaf:managed:aws:bot-control:CategoryMiscellaneous 検証済みボットについては、ルールグループはこのルールに一致もしないし、アクションを実行しませんが、ボット名とカテゴリにラベル付け、また、ラベル awswaf:managed:aws:bot-control:bot:verified を追加します。

ルール名	説明
CategoryMonitoring	モニタリング目的で使用されるボットを検査します。例えば、パフォーマンスや稼働時間などをモニタリングするために、アプリケーションのウェブサイトに定期的に ping を送信するボットモニタリングサービスを使用することができます。 未検証のボットにのみ適用されるルールアクション: Block ラベル: awswaf:managed:aws:bot-control:bot:category:monitoring および awswaf:managed:aws:bot-control:CategoryMonitoring 検証済みボットについては、ルールグループはこのルールに一致もしないし、アクションを実行しませんが、ボット名とカテゴリにラベル付け、また、ラベル awswaf:managed:aws:bot-control:bot:verified を追加します。

ルール名	説明
CategoryPagePreview	コンテンツがメッセージングプラットフォーム、ソーシャルメディア、またはコラボレーションツールで共有されているときに、ページプレビューを生成し、プレビューをリンクするボットを検査します。 未検証のボットにのみ適用されるルールアクション: Block ラベル: awswaf:managed:aws:bot-control:bot:category:page_preview および awswaf:managed:aws:bot-control:CategoryPagePreview 検証済みボットについては、ルールグループはこのルールに一致もしないし、アクションを実行しませんが、ボット名とカテゴリにラベル付け、また、ラベル awswaf:managed:aws:bot-control:bot:verified を追加します。

ルール名	説明
CategoryScrapingFramework	ウェブサイトからのコンテンツのクロールと抽出を自動化するために使用される、ウェブスクレイピングフレームワークからのボットを検査します。 未検証のボットにのみ適用されるルールアクション: Block ラベル: awswaf:managed:aws:bot-control:bot:category:scraping_framework および awswaf:managed:aws:bot-control:CategoryScrapingFramework 検証済みボットについては、ルールグループはこのルールに一致もしないし、アクションを実行しませんが、ボット名とカテゴリにラベル付け、また、ラベル awswaf:managed:aws:bot-control:bot:verified を追加します。

ルール名	説明
CategorySearchEngine	ウェブサイトをクロールしてコンテンツをインデックス化し、その情報を検索エンジンの結果に利用できるようにする検索エンジンボットを検査します。 未検証のボットにのみ適用されるルールアクション: Block ラベル: awswaf:managed:aws:bot-control:bot:category:search_engine および awswaf:managed:aws:bot-control:CategorySearchEngine 検証済みボットについては、ルールグループはこのルールに一致もしないし、アクションを実行しませんが、ボット名とカテゴリにラベル付け、また、ラベル awswaf:managed:aws:bot-control:bot:verified を追加します。

ルール名	説明
CategorySecurity	ウェブアプリケーションの脆弱性をスキャンしたり、セキュリティ監査を実施したりするボットを検査します。例えば、ウェブアプリケーションのセキュリティをスキャン、モニタリング、または監査するサードパーティーのセキュリティベンダーを利用することができます。 未検証のボットにのみ適用されるルールアクション: Block ラベル: awswaf:managed:aws:bot-control:bot:category:security および awswaf:managed:aws:bot-control:CategorySecurity 検証済みボットについては、ルールグループはこのルールに一致もしないし、アクションを実行しませんが、ボット名とカテゴリにラベル付け、また、ラベル awswaf:managed:aws:bot-control:bot:verified を追加します。

ルール名	説明
CategorySeo	検索エンジンの最適化に使用されるボットを検査します。例えば、検索エンジンのランキングを向上させるために、サイトをクロールする検索エンジンツールを使用することができます。 未検証のボットにのみ適用されるルールアクション: Block ラベル: awswaf:managed:aws:bot-control:bot:category:seo および awswaf:managed:aws:bot-control:CategorySeo 検証済みボットについては、ルールグループはこのルールに一致もしないし、アクションを実行しませんが、ボット名とカテゴリにラベル付け、また、ラベル awswaf:managed:aws:bot-control:bot:verified を追加します。

ルール名	説明
`CategorySocialMedia`	ユーザーがコンテンツを共有するときに、コンテンツの概要を提供するためにソーシャルメディアプラットフォームで使用されるボットを検査します。 未検証のボットにのみ適用されるルールアクション: Block ラベル: `awswaf:managed:aws:bot-control:bot:category:social_media` および `awswaf:managed:aws:bot-control:CategorySocialMedia` 検証済みボットについては、ルールグループはこのルールに一致もしないし、アクションを実行しませんが、ボット名とカテゴリにラベル付け、また、ラベル `awswaf:managed:aws:bot-control:bot:verified` を追加します。

ルール名	説明
CategoryWebhooks	HTTP コールバックを介して、あるアプリケーションから別のアプリケーションに自動的に通知とデータ更新を配信するボットを検査します。 未検証のボットにのみ適用されるルールアクション: Block ラベル: awswaf:managed:aws:bot-control:bot:category:webhooks および awswaf:managed:aws:bot-control:CategoryWebhooks 検証済みボットについては、ルールグループはこのルールに一致もしないし、アクションを実行しませんが、ボット名とカテゴリにラベル付け、また、ラベル awswaf:managed:aws:bot-control:bot:verified を追加します。

ルール名	説明
`CategoryAI`	人工知能 (AI) ボットを検査します。 **Note** このルールは、ボットの検証の有無にかかわらず、すべての一致のアクションに適用します。 ルールアクション: Block ラベル: `awswaf:managed:aws:bot-control:bot:category:ai` および `awswaf:managed:aws:bot-control:CategoryAI` 検証済みボットの場合、ルールグループはこのルールに一致し、アクションを実行します。さらに、ボット名とカテゴリのラベル付け、ルールのラベル付け、ラベル `awswaf:managed:aws:bot-control:bot:verified` が追加されます。

ルール名	説明
SignalAutomatedBrowser	検証済みのボットからのリクエストを検査し、クライアントブラウザが自動化されている可能性があることを示す要素があるかどうかを確認します。自動ブラウザはテストやスクレイピングに使用できます。例えば、以下のようなタイプのブラウザを使用して、アプリケーションウェブサイトのモニタリングや検証を行うことができます。 ルールアクション: Block ラベル: awswaf:managed:aws:bot-control:signal:automated_browser および awswaf:managed:aws:bot-control:SignalAutomatedBrowser 検証済みボットの場合、ルールグループはこのルールに一致せず、シグナルラベルやルールラベルは適用されません。
SignalKnownBotDataCenter	検証済みのボットからではないリクエストを検査し、ボットが通常使用するデータセンターの要素があるかどうかを確認します。 ルールアクション: Block ラベル: awswaf:managed:aws:bot-control:signal:known_bot_data_center および awswaf:managed:aws:bot-control:SignalKnownBotDataCenter 検証済みボットの場合、ルールグループはこのルールに一致せず、シグナルラベルやルールラベルは適用されません。

ルール名	説明
SignalNonBrowserUserAgent	検証済みのボットからではないリクエストを検査し、ウェブブラウザからではないと考えられるユーザーエージェント文字列を検査します。このカテゴリには API リクエストが含まれる場合があります。 ルールアクション: Block ラベル: awswaf:managed:aws:bot-control:signal:non_browser_user_agent および awswaf:managed:aws:bot-control:SignalNonBrowserUserAgent 検証済みボットの場合、ルールグループはこのルールに一致せず、シグナルラベルやルールラベルは適用されません。

ルール名	説明
TGT_VolumetricIpTokenAbsent	検証済みのボットからではないリクエストを検査し、過去 5 分間の単一クライアントからのリクエストで、有効なチャレンジトークンが含まれていないものが 5 つ以上あるかどうかを確認します。トークンの詳細については、「AWS WAF インテリジェントな脅威の軽減におけるトークンの使用」を参照してください。 **Note** 同じクライアントからのリクエストで、最近トークンの欠落が発生するようになったという場合は、このルールがトークンを有するリクエストに一致する可能性があります。 このルールが適用されるしきい値は、レイテンシーによって若干異なる場合があります。 このルールは、トークンラベル `awswaf:managed:token:absent` とは異なる方法で欠落したトークンを処理します。トークンラベルは、トークンがない個々のリクエストにラベルを付けます。このルールは、各クライアント IP のトークンが欠落しているリクエスト数を把握し、制限を超過するクライアントに一致させます。 ルールアクション: Challenge ラベル: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:ip:token_absent` および

ルール名	説明
	awswaf:managed:aws:bot-control:TGT_VolumetricIpTokenAbsent
TGT_TokenAbsent	有効なチャレンジトークンを含まない検証済みのボットからのリクエストを検査します。トークンの詳細については、「AWS WAF インテリジェントな脅威の軽減におけるトークンの使用」を参照してください。 ルールアクション: Count ラベル: awswaf:managed:aws:bot-control:TGT_TokenAbsent

ルール名	説明
TGT_VolumetricSession	5 分間で、単一クライアントセッションの検証済みのボットからではないリクエスト数が異常に多いかどうかを検査します。評価は、履歴トラフィックパターンを使用して が AWS WAF 維持する標準ボリューメトリックベースラインとの比較に基づいています。 この検査は、ウェブリクエストにトークンがある場合にのみ適用されます。トークンは、アプリケーション統合 SDK、ならびに CAPTCHA および Challenge のルールアクションによってリクエストに追加されます。詳細については、「AWS WAF インテリジェントな脅威の軽減におけるトークンの使用」を参照してください。 **Note** このルールは、有効にしてから有効になるまでに 5 分かかることがあります。Bot Control は、現在のトラフィックを が AWS WAF 計算するトラフィックベースラインと比較することで、ウェブトラフィックの異常な動作を識別します。 ルールアクション: CAPTCHA ラベル: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:high` および `awswaf:managed:aws:bot-control:TGT_VolumetricSession`

ルール名	説明
	ルールグループは、最小しきい値を超える中規模および低ボリュームのリクエストに次のラベルを適用します。これらのレベルでは、クライアントが検証されているかどうかにかかわらず、ルールは何も実行しません。すなわち、`awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:medium` および `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:low` 。

ルール名	説明
TGT_VolumetricSessionMaximum	5 分間で、単一クライアントセッションの検証済みのボットからではないリクエスト数が異常に多いかどうかを検査します。評価は、履歴トラフィックパターンを使用して が AWS WAF 維持する標準ボリューメトリックベースラインとの比較に基づいています。 このルールは、評価における最大の信頼度を示します。 この検査は、ウェブリクエストにトークンがある場合にのみ適用されます。トークンは、アプリケーション統合 SDK、ならびに CAPTCHA および Challenge のルールアクションによってリクエストに追加されます。詳細については、「AWS WAF インテリジェントな脅威の軽減におけるトークンの使用」を参照してください。 **Note** このルールは、有効にしてから有効になるまでに 5 分かかることがあります。Bot Control は、現在のトラフィックを が AWS WAF 計算するトラフィックベースラインと比較することで、ウェブトラフィックの異常な動作を識別します。 ルールアクション: Block ラベル: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:maximum` および `awswaf:managed:aws:bot-cont`

ルール名	説明
	rol:TGT_VolumetricSessionMaximum
TGT_SignalAutomatedBrowser	クライアントブラウザが自動化されている可能性があることを示す要素がないか、リクエストのトークンを検査します。詳細については、「AWS WAF トークンの特性」を参照してください。 この検査は、ウェブリクエストにトークンがある場合にのみ適用されます。トークンは、アプリケーション統合 SDK、ならびに CAPTCHA および Challenge のルールアクションによってリクエストに追加されます。詳細については、「AWS WAF インテリジェントな脅威の軽減におけるトークンの使用」を参照してください。 ルールアクション: CAPTCHA ラベル: awswaf:managed:aws:bot-control:targeted:signal:automated_browser および awswaf:managed:aws:bot-control:TGT_SignalAutomatedBrowser

ルール名	説明
`TGT_SignalBrowserAutomationExtension`	Selenium IDE などの自動化を支援するブラウザ拡張機能の存在を示す検証済みのボットからではないリクエストを検査します。このルールの一致は、ユーザーがこのタイプの拡張をインストールすると、ユーザーが自発的に使用していない場合でも追加されます。 この検査は、ウェブリクエストにトークンがある場合にのみ適用されます。トークンは、アプリケーション統合 SDK、ならびに CAPTCHA および Challenge のルールアクションによってリクエストに追加されます。詳細については、「AWS WAF インテリジェントな脅威の軽減におけるトークンの使用」を参照してください。 ルールアクション: CAPTCHA ラベル: `awswaf:managed:aws:bot-control:targeted:signal:browser_automation_extension` および `awswaf:managed:aws:bot-control:TGT_SignalBrowserAutomationExtension`

ルール名	説明
TGT_SignalBrowserInconsistency	検証済みボットからではないリクエストを検査し、一貫性のないブラウザインテロゲーションデータがないかを確認します。詳細については、「AWS WAF トークンの特性」を参照してください。 この検査は、ウェブリクエストにトークンがある場合にのみ適用されます。トークンは、アプリケーション統合 SDK、ならびに CAPTCHA および Challenge のルールアクションによってリクエストに追加されます。詳細については、「AWS WAF インテリジェントな脅威の軽減におけるトークンの使用」を参照してください。 ルールアクション: CAPTCHA ラベル: awswaf:managed:aws:bot-control:targeted:signal:browser_inconsistency および awswaf:managed:aws:bot-control:TGT_SignalBrowserInconsistency

ルール名	説明
`TGT_ML_CoordinatedActivityLow` , `TGT_ML_CoordinatedActivityMedium` , `TGT_ML_CoordinatedActivityHigh`	検証済みボットからではないリクエストを検査し、分散、および調整されたボットアクティビティと一致する異常な動作があるかどうかを確認します。ルールレベルは、リクエストのグループが協調攻撃に参加しているかどうかの信頼度のレベルを示します。 **Note** これらのルールは、ルールグループが機械学習 (ML) を使用するように設定されている場合にのみ実行されます。この場合の設定については、「AWS WAF Bot Control マネージドルールグループをウェブ ACL に追加する」を参照してください。 **Note** このルールが適用するしきい値は、レイテンシーによって若干異なる場合があります。ルールアクションが適用される前に、いくつかのリクエストが制限を超えることがあります。 AWS WAF は、ウェブサイトトラフィック統計の機械学習分析を通じてこの検査を実行します。 は、数分ごとにウェブトラフィック AWS WAF を分析し、多くの IP アドレスに分散されている低強度で長期間のボットを検出するための分析を最適化します。

ルール名	説明
	これらのルールは、協調攻撃が進行中ではないと判断される前に、ごく少数のリクエストに一致する場合があります。そのため、表示された一致が 1 つか 2 つしかない場合は、結果が誤検出である可能性があります。ただし、これらのルールからの一致が多数表示されている場合は、協調攻撃を受けていると考えられます。 **Note** ML オプションで Bot Control ターゲットルールを有効にしてから、これらのルールが有効になるまでに最大 24 時間かかることがあります。Bot Control は、現在のトラフィックを が計算した AWS WAF トラフィックベースラインと比較することで、ウェブトラフィックの異常な動作を識別します。は、Bot Control のターゲットルールを ML オプションで使用している間 AWS WAF のみベースラインを計算し、意味のあるベースラインを確立するまでに最大 24 時間かかる場合があります。 これらのルールの機械学習モデルを定期的に更新して、ボットの予測を改善します。これらのルールによってボット予測が突然大幅に変更された場合は、アカウントマネージャーに連絡するか、「AWS サポート センター」でケースを開きます。 ルールのアクション: • 低: Challenge • ミディアム: CAPTCHA

ルール名	説明
	• 高: CAPTCHA ラベル: `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:` *`low|medium|high`* および `awswaf:managed:aws:bot-control:TGT_ML_CoordinatedActivity` *`Low|Medium|High`*

ルール名	説明
`TGT_TokenReuseIpLow` , `TGT_TokenReuseIpMedium` , `TGT_TokenReuseIpHigh`	過去 5 分間に、検証済みのボットからではないリクエストを検査し、複数の IP 間で単一のトークンが使用されているかを確認します。各レベルには、個別の IP 数制限があります。 • 低: 2 つ以上 • 中: 5 以上 • 高: 8 つ以上 **Note** このルールが適用するしきい値は、レイテンシーによって若干異なる場合があります。ルールアクションが適用される前に、いくつかのリクエストが制限を超えることがあります。 ルールのアクション: • 低: Count • ミディアム: CAPTCHA • 高: Block ラベル: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:token_reuse:ip:` *`low|medium|high`* および `awswaf:managed:aws:bot-control:TGT_TokenReuseIp` *`Low|Medium|High`*

ルール名	説明
`TGT_TokenReuseCountryLow` , `TGT_TokenReuseCountryMedium` , `TGT_TokenReuseCountryHigh`	過去 5 分間に、検証済みのボットからではないリクエストを検査し、複数の国/地域で 1 つのトークンを使用しているかどうかを確認します。各レベルには、個別の国/地域の数に制限があります: • 低: 1 つ以上 • 中: 2 つ以上 • 高: 3 つ以上 **Note** このルールが適用するしきい値は、レイテンシーによって若干異なる場合があります。ルールアクションが適用される前に、いくつかのリクエストが制限を超えることがあります。 ルールのアクション: • 低: Count • ミディアム: CAPTCHA • 高: Block ラベル: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:token_reuse:country:` *`low|medium|high`* および `awswaf:managed:aws:bot-control:TGT_TokenReuseCountry` *`Low|Medium|High`*

ルール名	説明
`TGT_TokenReuseAsnLow` , `TGT_TokenReuseAsnMedium` , `TGT_TokenReuseAsnHigh`	検証済みボットからのものではないリクエストを検査し、過去 5 分間に、複数のネットワーク AS 番号 (ASN) で 1 つのトークンが使用されるかどうかを確認します。各レベルには、個別の ASN 数制限があります: • 低: 1 つ以上 • 中: 2 つ以上 • 高: 3 つ以上 **Note** このルールが適用するしきい値は、レイテンシーによって若干異なる場合があります。ルールアクションが適用される前に、いくつかのリクエストが制限を超えることがあります。 ルールのアクション: • 低: Count • ミディアム: CAPTCHA • 高: Block ラベル: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:token_reuse:asn:` *`low|medium|high`* および `awswaf:managed:aws:bot-control:TGT_TokenReuseAsn` *`Low|Medium|High`*

AWS WAF 分散サービス拒否 (DDoS) 防止ルールグループ

このセクションでは、分散型サービス拒否 (DDoS) 攻撃に対する保護の AWS WAF マネージドルールグループについて説明します。

VendorName: `AWS`、名前: `AWSManagedRulesAntiDDoSRuleSet`、WCU: 50

> **Note**
>
> このドキュメントでは、このマネージドルールグループの最新の静的バージョンリリースについて説明します。バージョンの変更は、AWS マネージドルールの変更ログ の変更ログにレポートされます。他のバージョンの情報については、API コマンド DescribeManagedRuleGroup を使用してください。
> AWS マネージドルールのルールグループでルール用に公開する情報は、ルールを回避するために必要なものを不正なアクターに与えることなく、ルールを使用するために必要なものを提供することを目的としています。
> ここに記載されている以上の情報が必要な場合は、AWS サポート センター にお問い合わせください。

DDoS 対策マネージドルールグループは、DDoS 攻撃に関与しているか、その可能性が高いリクエストを検出して管理するルールを提供します。さらに、ルールグループは、可能性の高いイベント中に評価されるすべてのリクエストにラベルを付けます。

このルールグループの使用に関する考慮事項

このルールグループは、DDoS 攻撃を受けているリソースに送信されるウェブリクエストをソフトかつハードに軽減します。さまざまな脅威レベルを検出するには、両方の緩和タイプの機密性を高、中、または低の疑惑レベルに調整できます。

- ソフトな軽減 — ルールグループは、チャレンジインタースティシャルを処理できるリクエストに応答して、サイレントブラウザチャレンジを送信できます。チャレンジを実行するための要件については、「CAPTCHA および Challenge アクション動作」を参照してください。
- ハードな軽減 — ルールグループはリクエストを完全にブロックできます。

ルールグループの動作方法とその設定方法の詳細については、「Anti-DDoS マネージドルールグループを使用した高度な AWS WAF Anti-DDoS 保護」を参照してください。

> **Note**
>
> このマネージドルールグループを使用する場合、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

このルールグループは、 AWS WAFでのインテリジェントな脅威の軽減保護の一部です。詳細については、「でのインテリジェントな脅威の軽減 AWS WAF」を参照してください。

コストを最小限に抑え、トラフィック管理を最適化するには、ベストプラクティスガイドラインに従ってこのルールグループを使用します。「でのインテリジェントな脅威軽減のベストプラクティス AWS WAF」を参照してください。

このルールグループによって追加されるラベル

このマネージドルールグループは、評価対象のウェブリクエストに保護パック (ウェブ ACL) 内のこのルールグループの後に実行されるルールでも使用できるラベルを追加します。 AWS WAF は、Amazon CloudWatch メトリクスにもラベルを記録します。ラベルとラベルメトリクスに関する一般的な情報については、「ウェブリクエストのラベル付け」および「ラベルメトリクスとディメンション」を参照してください。

トークンラベル

このルールグループは、 AWS WAF トークン管理を使用して、 AWS WAF トークンのステータスに従ってウェブリクエストを検査し、ラベル付けします。 は、クライアントセッションの追跡と検証にトークン AWS WAF を使用します。

トークンおよびトークンの管理の詳細については、「AWS WAF インテリジェントな脅威の軽減におけるトークンの使用」を参照してください。

ここで説明するラベルコンポーネントについては、「でのラベル構文と命名要件 AWS WAF」を参照してください。

クライアントセッションラベル

ラベルには、 AWS WAF トークン管理がクライアントセッションを識別するために使用する一意の識別子`awswaf:managed:token:id:`*`identifier`*が含まれています。この識別子は、クライアントが使用していたトークンを破棄した後など、新しいトークンを取得すると変わる可能性があります。

> **Note**
>
> AWS WAF はこのラベルの Amazon CloudWatch メトリクスを報告しません。

ブラウザフィンガープリントラベル

ラベルには、 AWS WAF トークン管理がさまざまなクライアントブラウザシグナルから計算する堅牢なブラウザフィンガープリント識別子`awswaf:managed:token:fingerprint:`*`fingerprint-identifier`*が含まれています。この識別子は、複数のトークン取得の試行全体で同じままです。フィンガープリント識別子は、単一のクライアントに対して一意ではありません。

> **Note**
>
> AWS WAF はこのラベルの Amazon CloudWatch メトリクスを報告しません。

トークンステータスラベル: ラベル名前空間プレフィックス

トークンステータスラベルは、トークン、チャレンジのステータス、およびそれに含まれる CAPTCHA 情報を報告します。

各トークンステータスラベルは、次のプレフィクスの 1 つで始まります。

- `awswaf:managed:token:` — トークンの一般的なステータスを報告したり、トークンのチャレンジ情報のステータスを報告したりするために使用されます。
- `awswaf:managed:captcha:` — トークンの CAPTCHA 情報のステータスを報告するために使用されます。

トークンステータスラベル: ラベル名

プレフィックスに続いて、ラベルの残りの部分には詳細なトークンステータス情報が表示されます。

- `accepted` - リクエストトークンが存在し、以下の内容が含まれています。
  - 有効なチャレンジまたは CAPTCHA ソリューション。
  - 有効期限が切れていないチャレンジまたは CAPTCHA タイムスタンプ。
  - 保護パック (ウェブ ACL) に有効なドメイン仕様。

例: ラベル awswaf:managed:token:accepted には、ウェブリクエストのトークンに有効なチャレンジソリューション、有効期限が切れていないチャレンジタイムスタンプ、および有効なドメインがあることが示されています。

- rejected - リクエストトークンは存在するが、承認基準を満たしていない。

  トークン管理では、拒否されたラベルに加えて、理由を示すカスタムラベル名前空間と名前が追加されます。

  - rejected:not_solved — トークンにチャレンジまたは CAPTCHA ソリューションがない。
  - rejected:expired — 保護パック (ウェブ ACL) に設定されているトークンイミュニティ時間によると、トークンのチャレンジまたは CAPTCHA タイムスタンプの有効期限が切れている。
  - rejected:domain_mismatch — トークンのドメインが、保護パック (ウェブ ACL) のトークンドメイン設定と一致しない。
  - rejected:invalid – 指定されたトークンを読み取ることが AWS WAF できませんでした。

  例: ラベル awswaf:managed:captcha:rejected と awswaf:managed:captcha:rejected:expired とともに、トークンの CAPTCHA タイムスタンプがウェブ ACL で設定されている CAPTCHA トークンのイミュニティ時間を超えたために、リクエストには有効な CAPTCHA 解決がなかったことが示されています。

- absent — リクエストにトークンがないか、トークンマネージャーがそれを読み取れなかった。

  例: ラベル awswaf:managed:captcha:absent には、リクエストにトークンがないことが示されています。

DDoS 対策ラベル

DDoS 対策マネージドルールグループは、名前空間プレフィックス awswaf:managed:aws:anti-ddos: が付いたラベルを生成し、その後にカスタム名前空間およびラベル名が付いたラベルを生成します。各ラベルには、DDoS 対策の検出結果の一部が反映されています。

ルールグループは、個々のルールによって追加されるラベルに加えて、次のラベルをリクエストに複数追加できます。

- awswaf:managed:aws:anti-ddos:event-detected – マネージドルールグループが DDoS イベントを検出する保護されたリソースにリクエストが送信されることを示します。マネージドルールグループは、リソースへのトラフィックがリソースのトラフィックベースラインから大幅に逸脱した場合にイベントを検出します。

ルールグループは、この状態のリソースに送信されるすべてのリクエストにこのラベルを追加するため、正当なトラフィックと攻撃トラフィックはこのラベルを取得します。

- `awswaf:managed:aws:anti-ddos:ddos-request` – リクエストがイベントに参加している疑いのあるソースからのものであることを示します。

  ルールグループは、一般ラベルに加えて、信頼度を示す次のラベルを追加します。

  `awswaf:managed:aws:anti-ddos:low-suspicion-ddos-request` – DDoS 攻撃の可能性があるリクエストを示します。

  `awswaf:managed:aws:anti-ddos:medium-suspicion-ddos-request` – DDoS 攻撃の可能性が高いリクエストを示します。

  `awswaf:managed:aws:anti-ddos:high-suspicion-ddos-request` – DDoS 攻撃の可能性が非常に高いリクエストを示します。

- `awswaf:managed:aws:anti-ddos:challengeable-request` – リクエスト URI が Challenge アクションを処理できることを示します。マネージドルールグループは、URI が除外されていないすべてのリクエストにこれを適用します。URI は、ルールグループの除外 URI 正規表現と一致する場合、除外されます。

  サイレントブラウザチャレンジを実行できるリクエストの要件については、「CAPTCHA および Challenge アクション動作」を参照してください。

`DescribeManagedRuleGroup` を呼び出すことにより、API を介してルールグループのすべてのラベルを取得できます。ラベルは、応答の `AvailableLabels` プロパティにリストされています。

DDoS 対策マネージドルールグループは、リクエストにラベルを適用しますが、必ずしもそれらに対して対応するとは限りません。リクエスト管理は、ルールグループが攻撃への参加を決定する信頼度によって異なります。必要に応じて、ルールグループの後に実行されるラベル一致ルールを追加して、ルールグループがラベル付けするリクエストを管理できます。これと例の詳細については、「AWS WAF 分散サービス拒否 (DDoS) の防止」を参照してください。

DDoS 対策ルールのリスト

このセクションでは、DDoS 対策ルールを一覧表示します。

> **Note**
>
> このドキュメントでは、このマネージドルールグループの最新の静的バージョンリリースについて説明します。バージョンの変更は、AWS マネージドルールの変更ログ の変更ログにレポートされます。他のバージョンの情報については、API コマンド DescribeManagedRuleGroup を使用してください。
> AWS マネージドルールのルールグループでルール用に公開する情報は、ルールを回避するために必要なものを不正なアクターに与えることなく、ルールを使用するために必要なものを提供することを目的としています。
> ここに記載されている以上の情報が必要な場合は、AWS サポート センター にお問い合わせください。

ルール名	説明
`ChallengeAllDuringEvent`	現在攻撃を受けている保護されたリソースのラベル `awswaf:managed:aws:anti-ddos:challengeable-request` を持つリクエストに一致します。 ルールアクション: Challenge このルールアクションは、Allow または Count にのみオーバーライドできます。Allow の使用はお勧めしません。ルールアクション設定では、ルールは `challengeable-request` ラベルを持つリクエストのみに一致します。 このルールの設定は、次のルールの評価に影響しますChallengeDDoSRequests 。 は、マネージドルールグループのウェブ ACL の設定で、このルールのアクションにオーバーライドが に設定されている場合にのみCount、そのルール AWS WAF を評価します。 ワークロードが予期しないリクエストボリュームの変更に対して脆弱である場合は、デフォルトのアクション設定を Challenge のままに

ルール名	説明
	して、すべてのチャレンジ可能なリクエストにチャレンジすることをお勧めします。機密性の低いアプリケーションでは、このルールに対するアクションを Count に設定し、ルール ChallengeDDoSRequests を使用して Challenge レスポンスの感度を調整できます。 ラベル: awswaf:managed:aws:anti-ddos:ChallengeAllDuringEvent
ChallengeDDoSRequests	リソースが攻撃を受けている期間中に、ルールグループで設定されたチャレンジ感度のしきい値以上を満たす、保護対象リソースへのリクエストに一致します。 ルールアクション: Challenge このルールアクションは、Allow または Count にのみオーバーライドできます。Allow の使用はお勧めしません。いずれの場合も、ルールは challengeable-request ラベルを持つリクエストのみに一致します。 AWS WAF は、前のルール Countで アクションを に上書きする場合にのみ、このルールを評価しますChallengeAllDuringEvent 。 ラベル: awswaf:managed:aws:anti-ddos:ChallengeDDoSRequests

ルール名	説明
DDoSRequests	リソースが攻撃されている間に、ルールグループの設定されたブロック感度設定を満たすか超える保護されたリソースのリクエストに一致します。 ルールアクション: Block ラベル: awswaf:managed:aws:anti-ddos:DDoSRequests

バージョニングされた AWS マネージドルールルールグループのデプロイ

このセクションでは、 が AWS マネージドルールのルールグループに更新を AWS デプロイする方法について説明します。

AWS は、リリース候補、静的バージョン、デフォルトバージョンの 3 つの標準デプロイで、バージョン管理ルール AWS ルールグループに変更をデプロイします。さらに、例外デプロイをリリースするか、デフォルトバージョンのデプロイをロールバックする必要がある AWS 場合があります。

> **Note**
>
> このセクションは、バージョニングされた AWS マネージドルールのルールグループにのみ適用されます。バージョニングされていないルールグループは、IP 評価ルールグループのみです。

トピック

- AWS マネージドルールのルールグループのデプロイに関する通知
- AWS マネージドルールの標準デプロイの概要
- AWS マネージドルールの一般的なバージョン状態
- AWS マネージドルールの候補デプロイをリリースする
- AWS マネージドルールの静的バージョンデプロイ
- AWS マネージドルールのデフォルトバージョンのデプロイ
- AWS マネージドルールの例外デプロイ

- AWS マネージドルールのデフォルトのデプロイのロールバック

AWS マネージドルールのルールグループのデプロイに関する通知

このセクションでは、Amazon SNS 通知が AWS Managed Rules ルールグループと連携する方法について説明します。

バージョニングされた AWS マネージドルールのルールグループはすべてデプロイの SNS 更新通知を提供し、すべて同じ SNS トピック Amazon リソースネーム (ARN) を使用します。バージョニングされていないルールグループは、IP 評価ルールグループのみです。

保護に影響するデプロイ (デフォルトバージョンへの変更など) の場合、 AWS は SNS 通知を提供して、計画されたデプロイについて通知し、デプロイが開始されるタイミングを知らせます。保護に影響しないデプロイ (リリース候補や静的バージョンのデプロイなど) の場合、 AWS は、デプロイが開始された後や完了した後でも通知を行う場合があります。新しい静的バージョンのデプロイが完了すると、 はこのガイドを の変更ログで更新AWS マネージドルールの変更ログし、 のドキュメント履歴ページで AWS 更新しますドキュメント履歴。

AWS マネージドルールルールグループに AWS が提供するすべての更新を受け取るには、このガイドの任意の HTML ページから RSS フィードにサブスクライブし、 AWS マネージドルールルールグループの SNS トピックにサブスクライブします。SNS 通知のサブスクライブの詳細については、マネージドルールグループに対する新しいバージョンと更新の通知を受け取る を参照してください。

SNS 通知のコンテンツ

Amazon SNS 通知のフィールドには常に題名、本文、メッセージ属性が含まれます。追加のフィールドは、メッセージのタイプと通知対象のマネージドルールグループによって異なります。`AWSManagedRulesCommonRuleSet` の通知リストの例を次に示します。

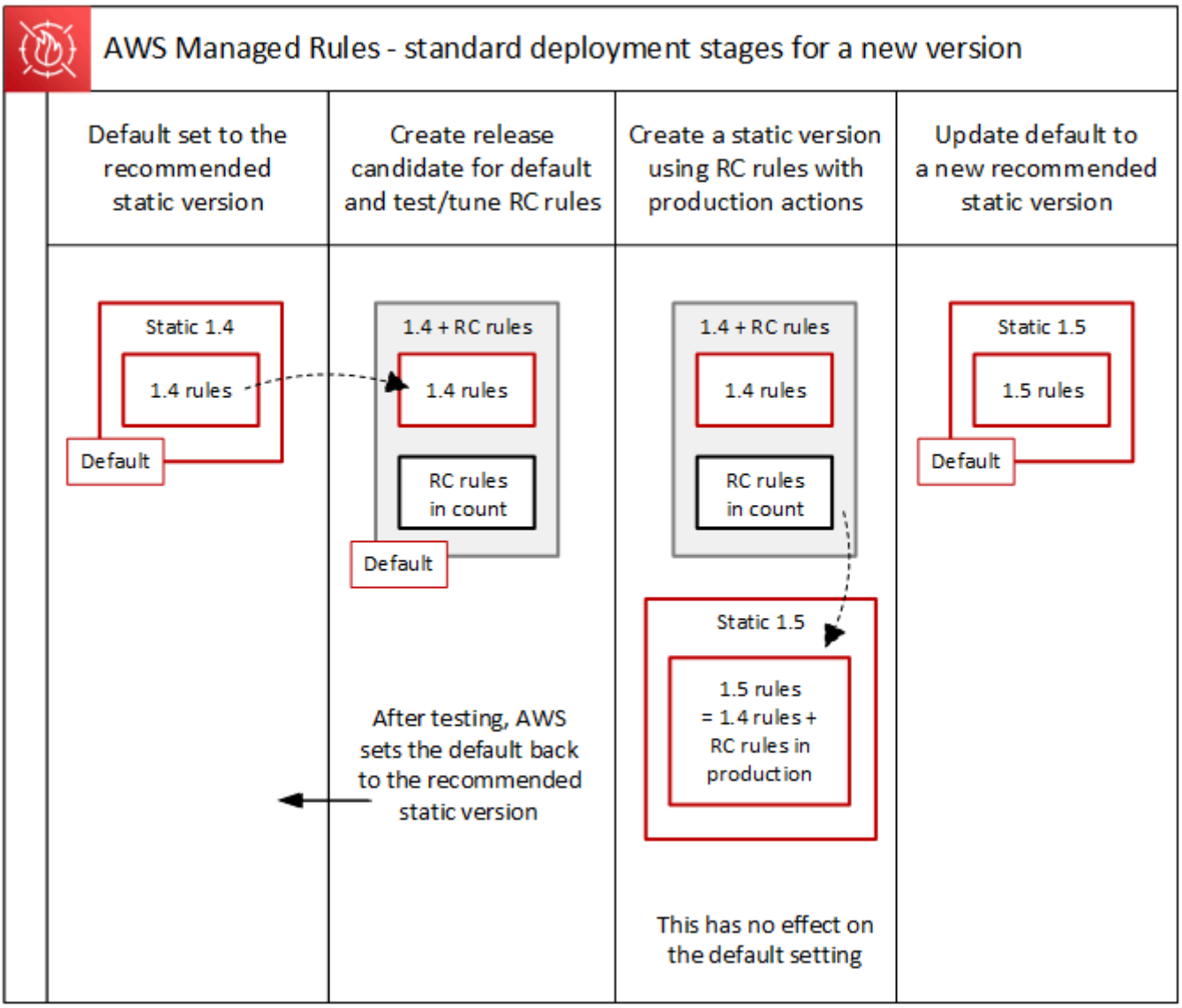
```
{
    "Type": "Notification",
    "MessageId": "4286b830-a463-5e61-bd15-e1ae72303868",
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:MyTopic",
    "Subject": "New version available for rule group AWSManagedRulesCommonRuleSet",
    "Message": "Welcome to AWSManagedRulesCommonRuleSet version 1.5! We've updated
 the regex specification in this version to improve protection coverage, adding
 protections against insecure deserialization. For details about this change, see
 http://updatedPublicDocs.html. Look for more exciting updates in the future! ",
    "Timestamp": "2021-08-24T11:12:19.810Z",
    "SignatureVersion": "1",
```

```
    "Signature": "EXAMPLEHXgJm...",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
f3ecfb7224c7233fe7bb5f59f96de52f.pem",
    "SubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=ConfirmSubscription&TopicArn=arn:aws:sns:us-
west-2:123456789012:MyTopic&Token=2336412f37...",
    "MessageAttributes": {
        "major_version": {
            "Type": "String",
            "Value": "v1"
        },
        "managed_rule_group": {
            "Type": "String",
            "Value": "AWSManagedRulesCommonRuleSet"
        }
    }
}
```

AWS マネージドルールの標準デプロイの概要

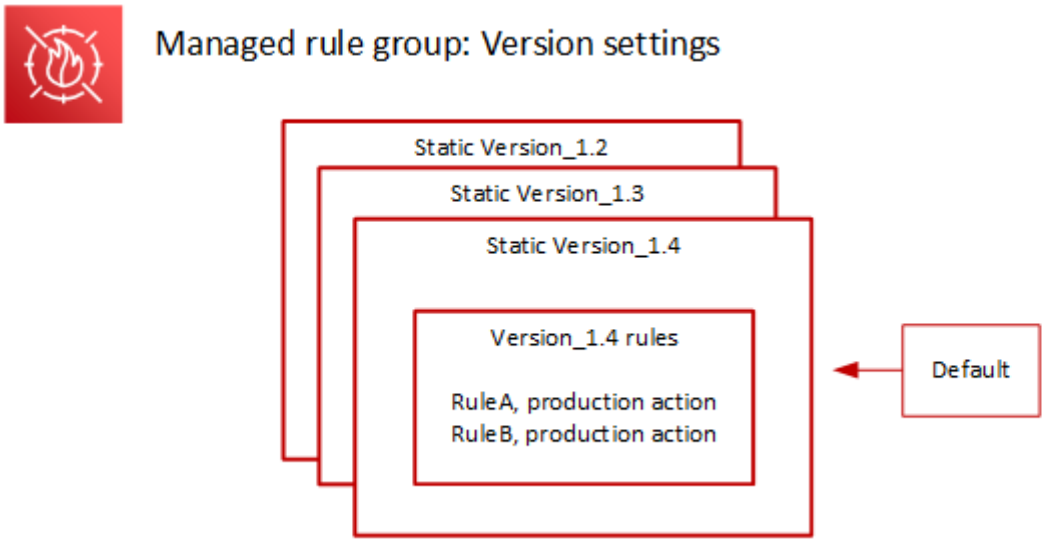
AWS は、リリース候補、静的バージョン、デフォルトバージョンの 3 つの標準デプロイステージを使用して、新しい AWS マネージドルール機能をロールアウトします。

次の図は、これらの標準的なデプロイを示しています。それぞれについて、以降のセクションで詳しく説明します。



AWS マネージドルールの一般的なバージョン状態

通常、バージョニングされたマネージドルールグループには有効期限が切れていない静的バージョンが多数あり、デフォルトバージョンは が AWS 推奨する静的バージョンを指します。次の図は、典型的な一連の静的バージョンとデフォルトバージョンの設定における例を示しています。



静的バージョンにおけるほとんどのルールの稼働アクションは Block ですが、別のアクションにセットされる場合があります。ルールアクション設定の詳細については、「AWS マネージドルールのルールグループリスト」で各ルールグループに関するルールのリストを参照してください。

AWS マネージドルールの候補デプロイをリリースする

このセクションでは、一時リリース候補デプロイの仕組みについて説明します。

AWS にマネージドルールグループのルール変更の候補セットがある場合、一時的なリリース候補デプロイでテストします。 AWS は、本番トラフィックに対してカウントモードで候補ルールを評価し、誤検出の軽減を含む最終的な調整アクティビティを実行します。 は、ルールグループのデフォルトバージョンを使用するすべての顧客に対して、この方法でリリース候補ルールを AWS テストします。リリース候補のデプロイは、ルールグループの静的バージョンを使用するお客様には適用されません。

デフォルトバージョンを使用する場合、リリース候補のデプロイは、ルールグループによるウェブトラフィックの管理方法を変更しません。候補ルールがテストされている間、次のことに気づくかもしれません。

- デフォルトバージョン名が `Default (using Version_X.Y)` から `Default (using Version_X.Y_PLUS_RC_COUNT)` に変更された。
- 名前に `RC_COUNT` が含まれる Amazon CloudWatch の追加のカウントメトリクス。これらはリリース候補ルールによって生成されます。

AWS はリリース候補を約 1 週間テストし、それを削除してデフォルトバージョンを現在の推奨静的バージョンにリセットします。

AWS は、リリース候補のデプロイに対して次のステップを実行します。

1. リリース候補を作成する – 現在の推奨静的バージョンに基づいてリリース候補 AWS を追加します。これは、デフォルトが指しているバージョンです。

   リリース候補の名前は、静的バージョン名に _PLUS_RC_COUNT が付加されたものです。例えば、現在推奨されている静的バージョンが Version_2.1 である場合、リリース候補の名前は Version_2.1_PLUS_RC_COUNT になります。

   リリース候補には次のルールが含まれています。

   - ルール設定を変更せずに、現在推奨されている静的バージョンから正確にコピーされたルール。
   - ルールアクションが Count に設定され、名前が _RC_COUNT で終わる候補の新しいルール。

     ほとんどの候補ルールは、ルールグループに既に存在するルールに対して提案された改善を提供します。これらの各ルールの名前は、既存のルールの名前に _RC_COUNT が付加されたものです。
2. デフォルトバージョンをリリース候補に設定し、テストする – 本番トラフィックに対してテストを実行するために、新しいリリース候補を指すようにデフォルトバージョン AWS を設定します。通常、テストには約 1 週間かかります。

   デフォルトバージョンの名前が、静的バージョンのみを示すもの (Default（using Version_1.4) など) から、静的バージョンとリリース候補ルールを示すもの (Default (using Version_1.4_PLUS_RC_COUNT) など) に変更されます。この命名スキームにより、ウェブトラフィックの管理に使用している静的バージョンを特定できます。

   次の図は、この時点でのサンプルルールグループバージョンの状態を示しています。
   図の上部には、スタックされた静的バージョンが 3 つ表示され、Version_1.4 が一番上にあります。静的バージョンスのタックとは別に、Version_1.4_PLUS_RC_COUNT バージョンがあります。このバージョンには、Version_1.4 のルールが含まれており、RuleB_RC_COUNT と RuleZ_RC_COUNT の 2 つのリリース候補ルールも含まれ、どちらもカウントアクションがあります。デフォルトのバージョンインジケータは Version_1.4_PLUS_RC_COUNT を指します。

   リリース候補ルールは常に Count アクションで設定されているため、ルールグループがウェブトラフィックを管理する方法が変更されることはありません。

リリース候補ルールは、 AWS が動作を検証し、誤検出を特定するために使用する Amazon CloudWatch カウントメトリクスを生成します。必要に応じて AWS 調整を行い、リリース候補カウントルールの動作を調整します。

リリース候補バージョンは静的バージョンではないため、静的ルールグループバージョンのリストから選択することはできません。デフォルトバージョンの仕様では、リリース候補バージョンの名前のみが表示されます。

3. デフォルトバージョンを推奨静的バージョンに戻す – リリース候補ルールをテストした後、AWS はデフォルトバージョンを現在の推奨静的バージョンに戻します。デフォルトバージョン名の設定では _PLUS_RC_COUNT の末尾が削除され、ルールグループはリリース候補ルールの CloudWatch カウントメトリクスの生成を停止します。これはサイレント変更であり、デフォルトバージョンロールバックのデプロイとは異なります。

   次の図は、リリース候補のテストが完了した後のサンプルルールグループのバージョンの状態を示しています。
   これは典型的なバージョンの状態図です。Version_1.2、Version_1.3、および Version_1.4 の 3 つの静的バージョンがスタックされ、Version_1.4 が一番上に表示されます。Version_1.4 には、RuleA と RuleB という 2 つのルールがあり、どちらも稼働アクションがあります。デフォルトのバージョンインジケータは Version_1.4 を指します。

タイミングと通知

AWS は、ルールグループの改善をテストするために、必要に応じてリリース候補バージョンをデプロイします。

- SNS – デプロイの開始時に SNS 通知 AWS を送信します。通知には、リリース候補がテストされる推定時間が表示されます。テストが完了すると、 は 2 回目の通知なしで、デフォルトを静的バージョン設定に AWS サイレントに返します。
- 変更ログ – このタイプのデプロイでは、変更ログやこのガイドの他の部分を更新 AWS しません。

AWS マネージドルールの静的バージョンデプロイ

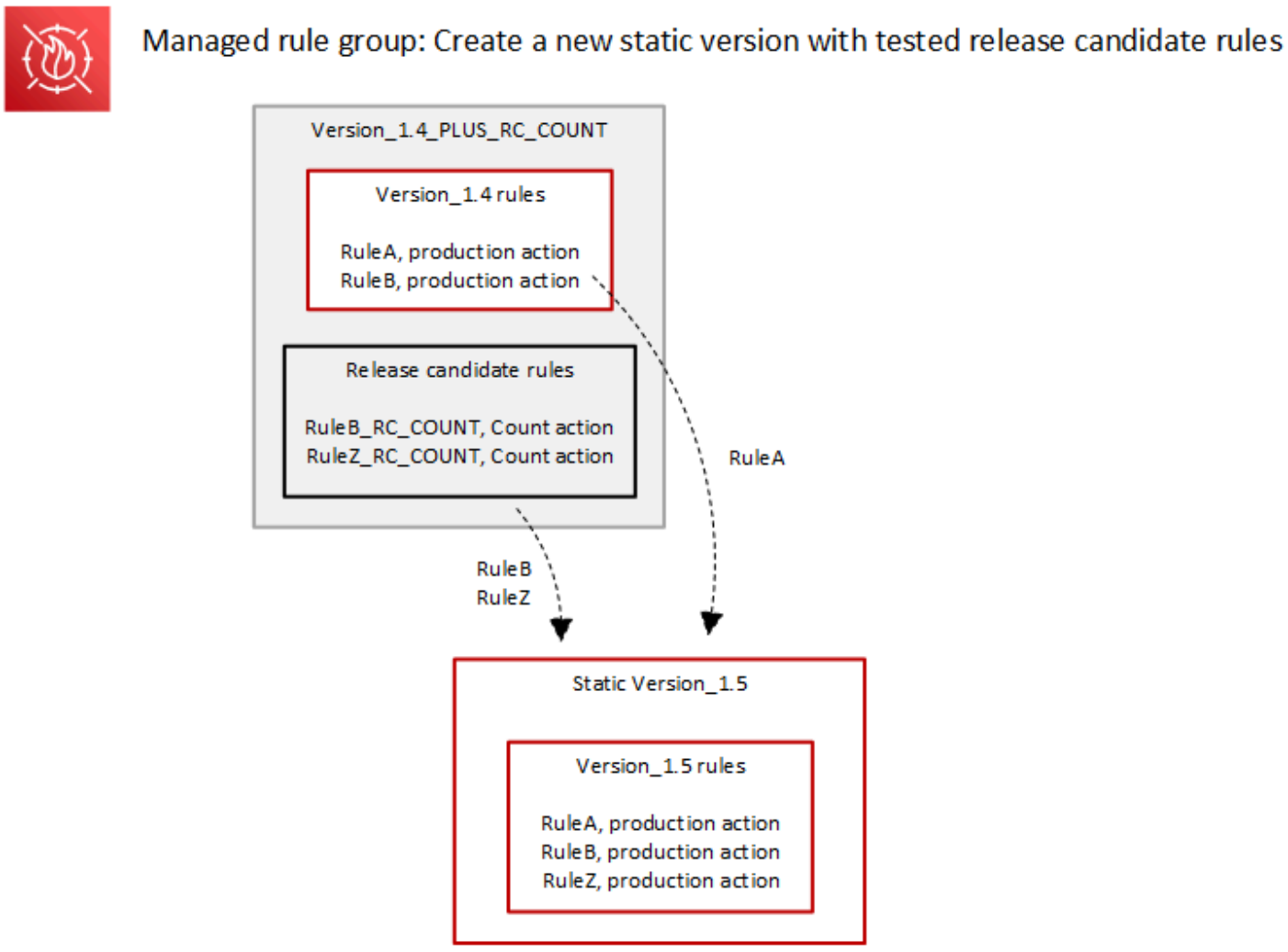
がリリース候補がルールグループに重要な変更を提供する AWS と判断した場合、 はリリース候補に基づいてルールグループの新しい静的バージョンを AWS デプロイします。このデプロイでは、ルールグループのデフォルトバージョンは変更されません。

新しい静的バージョンには、リリース候補からの次のルールが含まれています。

- リリース候補ルールの中に置換候補がない、以前の静的バージョンのルール。
- 次の変更を加えて、候補ルールをリリースします。
  - AWS は、リリース候補のサフィックス を削除してルール名を変更します_RC_COUNT。
  - AWS は、ルールアクションを から実稼働ルールアクションCountに変更します。

  以前の既存のルールを置き換えるリリース候補ルールの場合、これは新しい静的バージョンの以前のルールの機能を置き換えます。

次の図は、リリース候補から新しい静的バージョンを作成する方法を示しています。



デプロイ後、新しい静的バージョンをテストして、必要に応じて保護に使用できます。AWS マネージドルールのルールグループリスト のルールグループのルールリストで、新規および更新されたルールアクションと説明を確認できます。

静的バージョンはデプロイ後に変更できず、 AWS が期限切れになったときにのみ変更されます。バージョンのライフサイクルについては、「でのバージョニングされたマネージドルールグループの使用 AWS WAF」を参照してください。

タイミングと通知

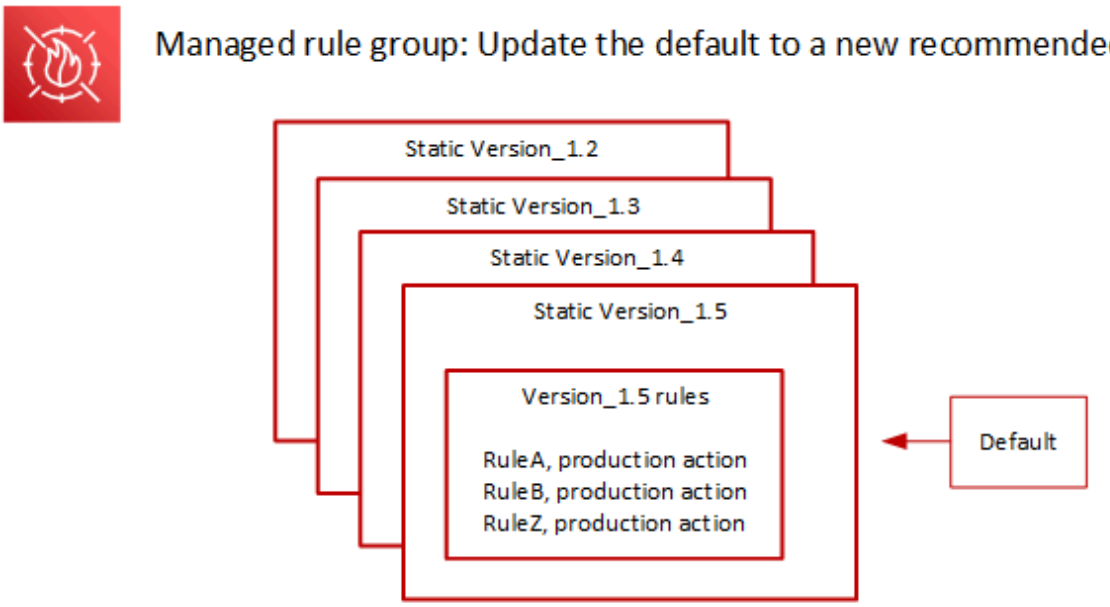
AWS は、ルールグループ機能の改善をデプロイするために、必要に応じて新しい静的バージョンをデプロイします。静的バージョンのデプロイは、デフォルトのバージョン設定には影響しません。

- SNS – デプロイが完了すると SNS 通知 AWS を送信します。
- 変更ログ – 利用可能なすべての場所でデプロイが完了すると、 AWS WAF は必要に応じてこのガイドのルールグループ定義 AWS を更新し、 AWS マネージドルールのルールグループ変更ログとドキュメント履歴ページでリリースを発表します。

AWS マネージドルールのデフォルトバージョンのデプロイ

新しい静的バージョンが現在のデフォルトと比較してルールグループの保護を改善すると が AWS 判断した場合、 はデフォルトバージョンを新しい静的バージョン AWS に更新します。ルールグループのデフォルトバージョンに昇格する前に、複数の静的バージョンをリリース AWS する可能性があります。

次の図は、 がデフォルトバージョン設定を新しい静的バージョン AWS に移行した後のルールグループバージョンの例の状態を示しています。



この変更をデフォルトバージョンにデプロイする前に、 は今後の変更をテストして準備できるように通知 AWS を提供します。デフォルトバージョンを使用する場合は、何も実行せずに、更新後もそのバージョンに留まることができます。デフォルトバージョンのデプロイの計画された開始の前に、代わりに新しいバージョンへの切り替えを遅らせたい場合、デフォルトが設定されている静的バージョンを使用するように、ルールグループを明示的に設定できます。

タイミングと通知

AWS は、現在使用されているものとは異なる静的バージョンをルールグループに推奨する場合、デフォルトバージョンを更新します。

- SNS – ターゲットデプロイ日の少なくとも 1 週間前に SNS 通知を送信し、デプロイ日のデプロイ開始時に別の SNS 通知 AWS を送信します。各通知には、ルールグループ名、デフォルトバージョンの更新先の静的バージョン、デプロイ日、更新が実行されている各 AWS リージョンのデプロイのスケジュールされたタイミングが含まれます。
- 変更ログ – このタイプのデプロイでは、変更ログやこのガイドの他の部分を更新 AWS しません。

AWS マネージドルールの例外デプロイ

AWS は、重要なセキュリティリスクに対処する更新を迅速にデプロイするために、標準のデプロイステージをバイパスすることがあります。例外デプロイには、標準デプロイタイプのいずれかが含まれる場合があり、 AWS リージョン間で迅速にデプロイされる可能性があります。

AWS は、例外デプロイについて可能な限り多くの事前通知を提供します。

タイミングと通知

AWS は、必要な場合にのみ例外デプロイを実行します。

- SNS – ターゲットデプロイ日のできるだけ前に SNS 通知 AWS を送信し、デプロイの開始時に別の通知を送信します。各通知には、ルールグループ名、行われる変更、およびデプロイ日が含まれます。
- 変更ログ – デプロイが静的バージョンの場合、利用可能なすべての場所でデプロイが完了した後、 AWS WAF は必要に応じてこのガイドのルールグループ定義 AWS を更新し、 AWS マネージドルールのルールグループ変更ログとドキュメント履歴ページでリリースを発表します。

AWS マネージドルールのデフォルトのデプロイのロールバック

特定の条件下で AWS は、デフォルトバージョンを以前の設定にロールバックすることがあります。ロールバックには通常、すべての AWS リージョンで 10 分未満かかります。

AWS は、許容できないほど高いレベルの誤検出など、静的バージョンの重大な問題を軽減するためにのみロールバックを実行します。

デフォルトバージョン設定のロールバック後、 は、問題のある静的バージョンの有効期限と、問題に対処するための新しい静的バージョンのリリースの両方を AWS 迅速化します。

タイミングと通知

AWS は、必要な場合にのみデフォルトバージョンのロールバックを実行します。

- SNS – ロールバック時に単一の SNS 通知 AWS を送信します。通知には、ルールグループ名、デフォルトバージョンが設定されるバージョン、およびデプロイ日が含まれます。このデプロイタイプは非常に高速なので、通知はリージョンのタイミング情報を提供しません。
- 変更ログ – このタイプのデプロイでは、変更ログやこのガイドの他の部分を更新 AWS しません。

AWS マネージドルールの変更ログ

このセクションでは、2019 年 11 月のリリース AWS WAF 以降の の AWS マネージドルールの変更を一覧表示します。

> **Note**
>
> この変更ログは、 AWS マネージドルールのルールとルールグループの変更を報告します AWS WAF。
> IP 評価ルールグループ において、この変更ログはルールとルールグループの変更を報告し、ルールが使用する IP アドレスリストのソースに大きな変更を報告します。このルールで使用されている IP アドレスリストは動的であるため、これらのリストの変更は報告されません。IP アドレスリストについて質問がある場合は、アカウントマネージャーに連絡するか、AWS サポート センターでケースを開きます。

ルールグループおよびルール	説明	日付
SQL データベースマネージドルールグループ このリリースでは、次のルールが更新されます。 • SQLi_COOKIE • SQLi_URIPATH • SQLi_QUERYARGUMENTS • SQLi_BODY • SQLiExtendedPatterns_QUERYARGUMENTS • SQLiExtendedPatterns_BODY • SQLiExtendedPatterns_HEADER • SQLiExtendedPatterns_URIPATH	このルールグループの静的バージョン 2.4 をリリースしました。 このリリースでは、SQL インジェクション検出ロジックを改善するためにすべてのルールが更新されました。	2026-08-12
AWS WAF Bot Control ルールグループ	このルールグループの静的バージョン 6.1 をリリースしました。 広告、AI、コンテンツフェッチャー、スクレイピングフレームワーク、検索エンジン、セキュリティ、SEO、ソーシャルメディアなど、複数のカ	2026-07-24

ルールグループおよびルール	説明	日付
	テゴリにまたがる新しいボット検出署名を追加しました。	
コアルールセット (CRS) マネージドルールグループ • GenericLFI_QUERYARGUMENTS • GenericLFI_URIPATH • GenericLFI_BODY	このルールグループの静的バージョン 1.22 をリリースしました。 汎用 LFI ルールの検出署名が改善されました。	2026-07-20
既知の不正な入力マネージドルールグループ • ReactJSRCE_BODY	このルールグループの静的バージョン 1.26 をリリースしました。 リストされたルールにREMOVE_NULLS テキスト変換を追加しました。	2026-07-15

ルールグループおよびルール	説明	日付
Windows オペレーティングシステムマネージドルールグループ • WindowsShellCommands_HEADER • WindowsShellCommands_URIPATH • WindowsShellCommands_BODY • WindowsShellCommands_QUERYARGUMENTS • WindowsShellCommands_QUERYSTRING	このルールグループの静的バージョン 2.5 をリリースしました。 WindowsShellCommands_QUERYARGUMENTS を削除し、WindowsShellCommands_QUERYSTRING で置き換えました。 検出ロジックを改善するために WindowsShellCommands ルールを更新しました。	2026-06-01

ルールグループおよびルール	説明	日付
AWS WAF Bot Control ルールグループ	このルールグループの静的バージョン 6.0 をリリースしました。 広告、コンテンツフェッチャー、検索エンジンなど、複数のカテゴリにまたがる新しいボット検出署名を追加しました。 Web Bot Auth のサポートを商用パーティションのリージョン AWS WAF 統合に拡張しました。 Web Bot Auth 検証済みボットの動作を、AI カテゴリだけでなく、すべてのカテゴリで標準検証済みボットとして扱うように変更しました。 この静的バージョンは、デフォルトのバージョン動作を変更しません。	2026-05-22

ルールグループおよびルール	説明	日付
SQL データベースマネージドルールグループ • SQLi_COOKIE • SQLi_URIPATH • SQLi_QUERYARGUMENTS • SQLi_BODY • SQLiExtendedPatterns_QUERYARGUMENTS • SQLiExtendedPatterns_BODY • SQLiExtendedPatterns_HEADER • SQLiExtendedPatterns_URIPATH	このルールグループの静的バージョン 2.3 をリリースしました。 新しいルール SQLiExtendedPatterns_HEADER とを追加しましたSQLiExtendedPatterns_URIPATH 。 すべてのルールにREPLACE_COMMENTS テキスト変換を追加しました。 SQLi_COOKIE 、、SQLi_URIPATH およびのすべての新しいルールにJS_DECODE テキスト変換を追加しました。 検出ロジックを改善するために、すべてのルールを更新しました。 Version_2.3 は Version_2.0 ではなく Version_1.3 の後継です。これらは、検出のトレードオフが異なる個別の系統です。Version_2.0 の検出動作に依存するお客様は、そのバージョンを明示的に固定する必要があります。	2026-04-29

ルールグループおよびルール	説明	日付
Windows オペレーティングシステムマネージドルールグループ • WindowsShellCommands_HEADER • WindowsShellCommands_COOKIE • WindowsShellCommands_URIPATH • WindowsShellCommands_BODY • WindowsShellCommands_QUERYARGUMENTS	このルールグループの静的バージョン 2.4 をリリースしました。 を削除WindowsShellCommands_COOKIE し、すべてのヘッダーWindowsShellCommands_HEADER に一致する に置き換えました。 新しいルール を追加しましたWindowsShellCommands_URIPATH 。 JSON 本文検査を に追加しましたWindowsShellCommands_BODY 。 WindowsShellCommands ルールに二重変換URL_DECODE_UNI とJS_DECODE テキスト変換を追加しました。 誤検出を減らすために WindowsShellCommands ルールを更新しました。	2026-04-28

ルールグループおよびルール	説明	日付
コアルールセット (CRS) マネージドルールグループ • RestrictedExtensions_QUERYARGUMENTS • RestrictedExtensions_URIPATH	このルールグループの静的バージョン 1.21 をリリースしました。 これらのルールの検出署名が改善されました。	2026-04-06
PHP アプリケーションマネージドルールグループ • PHPHighRiskMethodsVariables_BODY • PHPHighRiskMethodsVariables_QUERYSTRING • PHPHighRiskMethodsVariables_HEADER • PHPHighRiskMethodsVariables_URIPATH	このルールグループの静的バージョン 2.2 をリリースしました。 検出が改善され、PHPHighRiskMethodsVariables_URIPATH ルールが追加されました。	2026-03-24

ルールグループおよびルール	説明	日付
AWS WAF Bot Control ルールグループ 新しいルール: • `CategoryPagePreview` • `CategoryWebhooks`	このルールグループの静的バージョン 5.0 をリリースしました。 ページプレビューとウェブフックの 2 つの新しいボットカテゴリとそれぞれのルールを含む、複数のカテゴリにまたがる 400 以上の新しいボットを追加しました。 主な改善点 ボット検出シグナルと汎用ボットパターンマッチングの精度が向上し、トラフィック分類の精度が向上しました。 この更新により、マネージドルールグループがボット検出を優先する方法が変更されます。特定の未検証のボットパターンが、一般的なパターンと検出シグナルの前に評価されるようになりました。つまり、リクエストは一般的な指標ではなく、最も具体的な特性に基づいて分類される可能性が高くなります。 これはトラフィックにとって何を意味しますか。 一般的なボットパターンの一致頻度が低くなりました。これらのパターンは、より具	2026-02-25

ルールグループおよびルール	説明	日付
	体的なボットルールがまだトラフィックを特定していない場合にのみ適用されます。これにより、過剰分類が軽減され、利用可能な最も正確なボット識別でリクエストにラベルが付けられます。 リクエストがクラウドサービスプロバイダー、既知のボットデータセンターから発信された、またはブラウザ以外のユーザーエージェントを使用していることを示すインジケータなどの検出シグナルが、ボット識別ルールの後に適用されるようになりました。これにより、特定のボット分類が一般的なトラフィックシグナルよりも優先されます。 影響: リクエストが特定のボットルールによってより正確に分類されるようになったため、トラフィックログに表示される一般的なボットパターンのラベルが少なくなる場合があります。これにより、自動トラフィックの実際の性質をより明確に把握でき、過度に広範なパターンマッチングによるノイズが軽減されます。未検証のボット分類は、より目立つ正確なものになり、アプ	

ルールグループおよびルール	説明	日付
	リケーションへの自動リクエストをよりよく理解し、管理するのに役立ちます。 注: このバージョンには Version_4.0 からの`awswaf:managed:aws:bot-control:bot:web_bot_auth` ラベルとルールの更新が含まれていますが、Web Bot Auth この機能は引き続き CloudFront でのみ使用できます。	
POSIX オペレーティングシステムマネージドルールグループ	このルールグループの静的バージョン 3.2 をリリースしました。 すべてのルールの検出署名が改善されました。	2026-01-15
既知の不正な入力マネージドルールグループ • `ReactJSRCE_BODY`	このルールグループの静的バージョン 1.25 をリリースしました。 検出を改善する`ReactJSRCE_BODY` ために を更新しました。	2025-12-08
POSIX オペレーティングシステムマネージドルールグループ	このルールグループの静的バージョン 3.1 をリリースしました。 すべてのルールの検出署名が改善されました。	2025-12-08

ルールグループおよびルール	説明	日付
既知の不正な入力マネージドルールグループ • ReactJSRCE_BODY	このルールグループの静的バージョン 1.24 をリリースしました。 検出を改善するReactJSRCE_BODY ために を更新しました。	2025-12-04

ルールグループおよびルール	説明	日付

AWS WAF Bot Control ルールグループ
 	
新しいラベル:
 	
• awswaf:managed:aws:bot-control:bot:web_bot_auth<status>
  • verified – 検証に成功
  • invalid – 検証の試行に失敗しました
  • expired – 期限切れのキー使用量
  • unknown_bot – 認識されないキーの使用法
• awswaf:managed:aws:bot-control:bot:vendor<vendor_name> – ボットベンダーまたはオペレーター
• awswaf:managed:aws:bot-control:bot:name<rfc_name> – ボット名 (WBA からの RFC トークン)
• awswaf:managed:aws:bot-control:bot:a
	Web Bot Authentication (WBA) で暗号化ボット検証をサポートする新しい静的バージョン AWSManagedRulesBotControlRuleSet Version_4.0 をデプロイしました。このバージョンは明示的に選択する必要があり、デフォルトバージョンを使用して既存のデプロイを自動的に更新することはありません。
	
	新機能:
	
	• AI ボットとエージェントのウェブボット認証 (WBA) 暗号化検証
	• カテゴリ AI ルールの検証済み WBA ボットの自動許可リスト
	• ベンダー、名前、アカウントラベルによるボット識別の強化
	• Amazon Bedrock Agent Core ボット検出のサポート
	
	ルールの更新:
	
	•
		2025-11-20

ルールグループおよびルール	説明	日付
ccount<hash> – AWS アカウント識別子。(Amazon Bedrock エージェントコアエージェントのみ) スコープ: CloudFront	Category AI (アクション: ブロック) • web_bot_auth:verified ラベル付きのリクエストと一致しないように更新します。 • 検証済みの WBA ボットは自動的に許可されます • TGT_TokenAbsent (アクション: カウント) • リクエストとweb_bot_auth:verified ラベルが一致しないように更新されました **Important** Version_4.0 は静的バージョンのみであり、デフォルトのバージョン動作は変更されません。WBA 機能を使用するには、ウェブ ACL を設定するときにバージョン _4.0 を明示的に選択します。	

ルールグループおよびルール	説明	日付
AWS WAF Bot Control ルールグループ 新しい検証済みボットラベル: 広告: • `awswaf:managed:aws:bot-control:bot:name:meta-externalads` – メタ広告ボット • `awswaf:managed:aws:bot-control:bot:organization:facebook` – メタ組織 AI: • `awswaf:managed:aws:bot-control:bot:name:meta-webindexer` – メタウェブインデクサー • `awswaf:managed:aws:bot-control:bot:name:perplexity-user` – Perplexity ユーザーボット • `awswaf:managed:aws:bot-control:bot:n`	主な改善点: • 検証済みボットの検出を複数のカテゴリ (広告、AI、コンテンツフェッチャー、ソーシャルメディア) に拡張 • Meta、Facebook ボットの組織レベルのラベルを追加 • Perplexity、Bytespider、DuckDuckGo ボットを含む AI ボット検出の強化 • TikTok ソーシャルメディアボット検出を追加 **Important** Bot Control のボットカテゴリルールは、検証されていないボットでのみトリガーされます。ただし、検証済みのボットでもトリガーされる CategoryAI は除きます。Version_3.3 は静的バージョンのみであり、デフォルトのバージョ	2025-11-17

ルールグループおよびルール	説明	日付
ame:perplexitybot – Perplexity ボット • awswaf:managed:aws:bot-control:bot:name:bytespider – Bytespider ボット • awswaf:managed:aws:bot-control:bot:name:duckassistbot – DuckDuckGo アシスタントボット • awswaf:managed:aws:bot-control:bot:organization:facebook – メタ組織 コンテンツフェッチャー: • awswaf:managed:aws:bot-control:bot:name:meta-externalfetcher – メタコンテンツフェッチャー • awswaf:managed:aws:bot-control:bot:organization:facebook-externalfetcher – メタ組織 ソーシャルメディア:	ン動作は変更されません。	

ルールグループおよびルール	説明	日付
• awswaf:managed:aws:bot-control:bot:name:tiktok – TikTok ボット		
コアルールセット (CRS) マネージドルールグループ • EC2MetaDataSSRF_BODY • EC2MetaDataSSRF_COOKIE • EC2MetaDataSSRF_URIPATH • EC2MetaDataSSRF_QUERYARGUMENTS	このルールグループの静的バージョン 1.20 をリリースしました。 Server Side Request Forgery (SSRF) ルールの検出署名が改善されました。	2025-10-02
コアルールセット (CRS) マネージドルールグループ • CrossSiteScripting_BODY • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_URIPATH	このルールグループの静的バージョン 1.19 をリリースしました。 クロスサイトスクリプティングルールの検出シグネチャが改善されました。	2025-08-14

ルールグループおよびルール	説明	日付
コアルールセット (CRS) マネージドルールグループ • CrossSiteScripting_BODY • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_URIPATH	このルールグループの静的バージョン 1.18 をリリースしました。 クロスサイトスクリプティングルールの検出シグネチャが改善されました。	2025-06-18

ルールグループおよびルール	説明	日付

AWS WAF Bot Control ルールグループ
 	
新しいラベル:
 	
• 検索エンジンボット:
  • awswaf:managed:aws:bot-control:bot:name:evensi
  • awswaf:managed:aws:bot-control:bot:name:yisouspider
• AI ボット:
  • awswaf:managed:aws:bot-control:bot:name:searchbot
  • awswaf:managed:aws:bot-control:bot:name:nova_act
• AI ボットの組織ラベル:
  • awswaf:managed:aws:bot-control:bot:o
	このルールグループの静的バージョン 3.2 をリリースしました。
	
	リストされている新しいラベルを追加しました。
		2025-05-29

ルールグループおよびルール	説明	日付
rganizati on:openai • awswaf:ma naged:aws:bot- control:bot:o rganizati on:marfeel • awswaf:ma naged:aws:bot- control:bot:o rganizati on:facebook • awswaf:ma naged:aws:bot- control:bot:o rganizati on:metaex ternalagent • awswaf:ma naged:aws:bot- control:bot:o rganizati on:amazon		
• コンテンツフェッチャーボット: • awswaf:ma naged:aws:bot- control:bot:n ame:googl		

ルールグループおよびルール	説明	日付
e_cloud_v ertex_bot • クラウドサービスプロバイダーのシグナル: • awswaf:ma naged:aws:bot-control:signa l:cloud_s ervice_pr ovider:alibaba		
コアルールセット (CRS) マネージドルールグループ • CrossSiteScripting _BODY • CrossSiteScripting _COOKIE • CrossSiteScripting _QUERYARGUMENTS • CrossSiteScripting _URIPATH	このルールグループの静的バージョン 1.17 をリリースしました。 クロスサイトスクリプティングルールの検出シグネチャが改善されました。	2025-03-03

ルールグループおよびルール	説明	日付
SQL データベースマネージドルールグループ • SQLi_COOKIE • SQLi_URIPATH • SQLi_QUERYARGUMENTS • SQLi_BODY	このルールグループの静的バージョン 1.3 をリリースしました。 リストされたルールにダブル URL_DECODE_UNI テキスト変換を追加しました。	2025-01-24
Linux オペレーティングシステムマネージドルールグループ • LFI_HEADER • LFI_URIPATH • LFI_QUERYSTRING	このルールグループの静的バージョン 2.6 をリリースしました。 検出の向上を図るために署名を追加しました。	2025-01-24
AWS WAF Bot Control ルールグループ Bot Control ラベルの新しいボット名ラベル: awswaf:managed:aws:bot-control:bot::name:nytimes	このルールグループの静的バージョン 3.1 をリリースしました。 ボット名ラベルのリストに New York Times ラベルを追加しました。	2024-11-07

ルールグループおよびルール	説明	日付
コアルールセット (CRS) マネージドルールグループ • CrossSiteScripting_BODY • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_URIPATH	このルールグループの静的バージョン 1.16 をリリースしました。 クロスサイトスクリプティングルールの検出シグネチャが改善されました。	2024-10-16

ルールグループおよびルール	説明	日付
AWS WAF Bot Control ルールグループ 新しいルール: • TGT_TokenAbsent • TGT_VolumetricSessionMaximum • TGT_SignalBrowserAutomationExtension • TGT_ML_CoordinatedActivityLow 、TGT_ML_CoordinatedActivityMedium 、および TGT_ML_CoordinatedActivityHigh • TGT_TokenReuseIpLow 、TGT_TokenReuseIpMedium 、および TGT_TokenReuseIpHigh • TGT_TokenReuseAsnLow 、TGT_TokenReuseAsnMedium 、および TGT_TokenReuseAsnHigh • TGT_TokenReuseCountryLow 、TGT_TokenReuseCountryMedium 、および TGT_TokenReuseCountryHigh	このルールグループの静的バージョン 2.0 および 3.0 をリリースしました。バージョン 2.0 はバージョン 3.0 と同じですが、すべての新しいルールのルールアクションは Count に設定されています。このガイドは、各ルールグループの最新バージョンについて記録します。 リストされている新しいルールを追加しました。 すべてのルールがパターン awswaf:managed:aws:bot-control: *<RuleName>* を持つラベルを適用するようにラベルを更新しました。 Bot Control シグナルラベルにクラウドサービスプロバイダーラベルを追加しました。 ボットカテゴリルールによって検査される新しいボット名ラベルを追加しました。	2024-09-13

ルールグループおよびルール	説明	日付
削除されたルール: • TGT_TokenReuseIp 。新たな低、中、高ルールに対応するものに置き換わりました。 新しいラベル: • HTTP Library ボット: • awswaf:managed:aws:bot-control:bot:name:fasthttp • AI ボット: • awswaf:managed:aws:bot-control:bot:name:bedrockbot • awswaf:managed:aws:bot-control:bot:name:claudebot • awswaf:managed:aws:bot-control:bot:name:anthropic • awswaf:managed:aws:bot-control:bot:name:metaexternalagent		

ルールグループおよびルール	説明	日付
• awswaf:managed:aws:bot-control:bot:name:bytespider • awswaf:managed:aws:bot-control:bot:name:omgili • awswaf:managed:aws:bot-control:bot:name:diffbot • awswaf:managed:aws:bot-control:bot:name:perplexitybot • awswaf:managed:aws:bot-control:bot:name:timpibot • awswaf:managed:aws:bot-control:bot:name:cohere • 検索エンジンボット: • awswaf:managed:aws:bot-control:bot:name:naver • 広告ボット: • awswaf:managed:aws:bot-		

ルールグループおよびルール	説明	日付
control:bot:name:naver_ads • ソーシャルメディアボット: • awswaf:managed:aws:bot-control:bot:name:snapchat • コンテンツフェッチャーボット: • awswaf:managed:aws:bot-control:bot:name:naver_preview • awswaf:managed:aws:bot-control:bot:name:censys • awswaf:managed:aws:bot-control:bot:name:imessage_preview • awswaf:managed:aws:bot-control:bot:name:imagesift • クラウドサービスプロバイダーのシグナル: • awswaf:managed:aws:bot-control:signal:cloud_s		

ルールグループおよびルール	説明	日付
ervice_pr ovider:aws • awswaf:ma naged:aws:bot- control:signa l:cloud_s ervice_pr ovider:azure • awswaf:ma naged:aws:bot- control:signa l:cloud_s ervice_pr ovider:gcp • awswaf:ma naged:aws:bot- control:signa l:cloud_s ervice_pr ovider:oracle • awswaf:ma naged:aws:bot- control:signa l:cloud_s ervice_pr ovider:di gital_ocean • awswaf:ma naged:aws:bot- control:signa l:cloud_s ervice_pr ovider:akamai		

ルールグループおよびルール	説明	日付
• awswaf:managed:aws:bot-control:signal:cloud_service_provider:cloudflare • awswaf:managed:aws:bot-control:signal:cloud_service_provider:ibm_cloud 既存のルールの追加ラベル付け。		
AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループ すべてのルール	このルールグループの静的バージョン 1.1 をリリースしました。 すべてのルールがパターン awswaf:managed:aws:atp: *<RuleName>* を持つラベルを適用するようにラベルを更新しました。	2024-09-13

ルールグループおよびルール	説明	日付
AWS WAF Fraud Control アカウント作成不正防止 (ACFP) ルールグループ すべてのルール	このルールグループの静的バージョン 1.1 をリリースしました。 すべてのルールがパターン `awswaf:managed:aws:acfp:` *`<RuleName>`* を持つラベルを適用するようにラベルを更新しました。	2024-09-13
Linux オペレーティングシステムマネージドルールグループ すべてのルール	このルールグループの静的バージョン 2.5 をリリースしました。 検出の向上を図るために署名を追加しました。	2024-09-02
コアルールセット (CRS) マネージドルールグループ • `GenericLFI_QUERYARGUMENTS` • `GenericLFI_URIPATH` • `GenericLFI_BODY`	このルールグループの静的バージョン 1.15 をリリースしました。 汎用 LFI ルールの検出署名が改善されました。	2024-08-30

ルールグループおよびルール	説明	日付
Windows オペレーティングシステムマネージドルールグループ • WindowsShellCommands_QUERYARGUMENTS • WindowsShellCommands_BODY • WindowsShellCommands_COOKIE	このルールグループの静的バージョン 2.3 をリリースしました。 リストされたルールでは、誤検出を減らすために検出シグネチャをチューニングしました。	2024-08-28
WordPress アプリケーションマネージドルールグループ • WordPressExploitableCommands_QUERYSTRING	このルールグループの静的バージョン 1.3 をリリースしました。 リストされたルールに JS_DECODE テキスト変換を追加しました。	2024-07-15
Linux オペレーティングシステムマネージドルールグループ • LFI_QUERYSTRING	このルールグループの静的バージョン 2.4 をリリースしました。 リストされたルールに JS_DECODE テキスト変換を追加しました。	2024-07-12

ルールグループおよびルール	説明	日付
コアルールセット (CRS) マネージドルールグループ • EC2MetaDataSSRF_BODY • EC2MetaDataSSRF_QUERYARGUMENTS • GenericLFI_QUERYARGUMENTS • GenericLFI_BODY • RestrictedExtensions_QUERYARGUMENTS • GenericRFI_QUERYARGUMENTS • GenericRFI_BODY • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_COOKIE • CrossSiteScripting_URIPATH	このルールグループの静的バージョン 1.14 をリリースしました。 リストされているルールに JS_DECODE テキスト変換を追加しました。	2024-07-09

ルールグループおよびルール	説明	日付
PHP アプリケーションマネージドルールグループ • PHPHighRiskMethodsVariables_BODY • PHPHighRiskMethodsVariables_QUERYSTRING	このルールグループの静的バージョン 2.1 をリリースしました。 リストされているルールに JS_DECODE テキスト変換を追加しました。	2024-07-03
Windows オペレーティングシステムマネージドルールグループ • WindowsShellCommands_QUERYARGUMENTS • WindowsShellCommands_BODY • PowerShellCommands_QUERYARGUMENTS • PowerShellCommands_BODY	このルールグループの静的バージョン 2.2 をリリースしました。 リストされているルールに JS_DECODE テキスト変換を追加しました。	2024-07-03
Linux オペレーティングシステムマネージドルールグループ すべてのルール	このルールグループの静的バージョン 2.3 をリリースしました。 検出の向上を図るために署名を追加しました。	2024-06-06

ルールグループおよびルール	説明	日付
AWS WAF Bot Control ルールグループ AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループ AWS WAF Fraud Control アカウント作成不正防止 (ACFP) ルールグループ	ボットおよび不正ルールグループがバージョン管理されるようになりました。これらのルールグループを使用している場合、この更新によってウェブトラフィックの処理方法が変更されることはありません。 この更新では、現在のルールグループバージョンを静的バージョン 1.0 に設定し、それを指すデフォルトバージョンを設定します。 バージョンで管理されたルールの詳細については、以下の内容を参照してください。 • でのバージョニングされたマネージドルールグループの使用 AWS WAF • バージョニングされた AWS マネージドルールルールグループのデプロイ • マネージドルールグループに対する新しいバージョンと更新の通知を受け取る	2024-05-29

ルールグループおよびルール	説明	日付
POSIX オペレーティングシステムマネージドルールグループ • UNIXShellCommandsVariables_QUERYARGUMENTS • UNIXShellCommandsVariables_QUERYSTRING • UNIXShellCommandsVariables_HEADER • UNIXShellCommandsVariables_BODY	このルールグループの静的バージョン 3.0 をリリースしました。 UNIXShellCommandsVariables_QUERYARGUMENTS を削除し、UNIXShellCommandsVariables_QUERYSTRING で置き換えました。UNIXShellCommandsVariables_QUERYARGUMENTS のラベルに一致するルールがある場合、このバージョンを使用する場合は、UNIXShellCommandsVariables_QUERYSTRING のラベルと一致するように切り替えます。新しいラベルは awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_QueryString です。 すべてのヘッダーに一致するルール UNIXShellCommandsVariables_HEADER を追加しました。 改善された検出ロジックで管理ルールグループのすべてのルールを更新しました。 UNIXShellCommandsVariables_BODY のラベル	2024-05-28

ルールグループおよびルール	説明	日付
	の大文字が文書化されている箇所を修正しました。	
コアルールセット (CRS) マネージドルールグループ • CrossSiteScripting*	このルールグループの静的バージョン 1.12 をリリースしました。 検出の向上と誤検出の低減のため、クロスサイトのスクリプティングルール全体にシグネチャーを追加しました。	2024-05-21
SQL データベースマネージドルールグループ • SQLi_BODY • SQLi_QUERYARGUMENTS • SQLiExtendedPatterns_QUERYARGUMENTS	このルールグループの静的バージョン 1.2 をリリースしました。 リストされたルールに JS_DECODE テキスト変換を追加しました。	2024-05-14
既知の不正な入力マネージドルールグループ • JavaDeserializationRCE_BODY • JavaDeserializationRCE_QUERYSTRING • Log4JRCE_QUERYSTRING • Log4JRCE_BODY • Log4JRCE_HEADER	このルールグループの静的バージョン 1.22 をリリースしました。 リストされたルールに JS_DECODE テキスト変換を追加しました。	2024-05-08

ルールグループおよびルール	説明	日付
POSIX オペレーティングシステムマネージドルールグループ	このルールグループの静的バージョン 2.2 をリリースしました。 2 つのルールに JS_DECODE テキスト変換を追加しました。	2024-05-08
Windows オペレーティングシステムマネージドルールグループ • PowerShellCommands_BODY	このルールグループの静的バージョン 2.1 をリリースしました。 検出結果の改善を図るために署名を PowerShellCommands_BODY に追加しました。	2024-05-03
Amazon IP 評価リストマネージドルールグループ • AWSManagedIPReputationList	IP 評価リストのソースを更新し、悪意のあるアクティビティに積極的に関与しているアドレスの特定を改善し、誤検出を減らしました。 このルールグループはバージョン化されていないため、この更新には新しいバージョンは含まれません。	2024-03-13
既知の不正な入力マネージドルールグループ	このルールグループの静的バージョン 1.21 をリリースしました。 検出を改善し、誤検出を減らすためにシグネチャを追加しました。	2023-12-16

ルールグループおよびルール	説明	日付
既知の不正な入力マネージドルールグループ • ExploitablePaths_URIPATH	このルールグループの静的バージョン 1.20 をリリースしました。 Atlassian Confluence CVE-2023-22518 の不適切な認可の脆弱性に一致するリクエストの検出を追加するように ExploitablePaths_URIPATH ルールを更新しました。この脆弱性は Confluence Data Center および Server のすべてのバージョンに影響します。詳細については、「NIST: National Vulnerability Database: CVE-2023-22518 Detail」を参照してください。	2023-12-14
コアルールセット (CRS) マネージドルールグループ • CrossSiteScripting*	このルールグループの静的バージョン 1.11 をリリースしました。 検出の向上と誤検出の低減のため、クロスサイトのスクリプティングルール全体にシグネチャーを追加しました。	2023-12-06

ルールグループおよびルール	説明	日付
AWS WAF Bot Control ルールグループ • 新しいラベル: `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:low`	ルールグループの対象保護レベルラベルに調整されたアクティビティの下限ラベルを追加しました。このラベルはいずれのルールにも関連付けられていません。このラベルは、中レベルおよび高レベルのルールとラベルに追加されるものです。	2023-12-05
Bot Control ラベル • ラベル: `awswaf:managed:aws:bot-control:targeted:signal:browser_automation_extension`	自動化を支援するブラウザ拡張機能が検出されたことを示すシグナルラベルをルールグループに追加しました。このラベルは個々のルールに固有のものではありません。	2023-11-14
コアルールセット (CRS) マネージドルールグループ • `EC2MetaDataSSRF_QUERYARGUMENTS`	このルールグループの静的バージョン 1.10 をリリースしました。 1 つのルールを更新し、検出の向上と誤検出の低減を実現しました。	2023-11-02

ルールグループおよびルール	説明	日付
コアルールセット (CRS) マネージドルールグループ • EC2MetaDataSSRF_BODY • EC2MetaDataSSRF_COOKIE • EC2MetaDataSSRF_URIPATH • EC2MetaDataSSRF_QUERYARGUMENTS	このルールグループの静的バージョン 1.9 をリリースしました。 ルールが更新され、検出の向上と誤検出の低減を実現しました。	2023-10-30
POSIX オペレーティングシステムマネージドルールグループ • UNIXShellCommandsVariables_QUERYARGUMENTS	このルールグループの静的バージョン 2.1 をリリースしました。 クエリ引数ルールを更新して、検出を改善しました。	2023-10-12

ルールグループおよびルール	説明	日付
コアルールセット (CRS) マネージドルールグループ • GenericLFI_QUERYARGUMENTS • GenericLFI_URIPATH • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS	このルールグループの静的バージョン 1.8 をリリースしました。 ルールを更新して検出を改善しました。	2023-10-11

ルールグループおよびルール	説明	日付
既知の不正な入力マネージドルールグループ • ExploitablePaths_URIPATH	例外のデプロイ: このルールグループの静的バージョン 1.19 をリリースしました。バージョン 1.19 を使用するようにデフォルトバージョンを更新しました。 Atlassian Confluence CVE-2023-22515 の権限昇格の脆弱性に一致するリクエストの検出を追加するように ExploitablePaths_URIPATH ルールを更新しました。この脆弱性は、Atlassian Confluence の一部のバージョンに影響を及ぼします。詳細については、「NIST: National Vulnerability Database: CVE-2023-22515 Detail」および「Atlassian Support: FAQ for CVE-2023-22515」を参照してください。 デプロイタイプの詳細については、「AWS マネージドルールの例外デプロイ」を参照してください。	2023-10-04

ルールグループおよびルール	説明	日付
既知の不正な入力マネージドルールグループ • Host_localhost_HEADER • Log4J* • JavaDeserialization*	例外のデプロイ: このルールグループの静的バージョン 1.18 をリリースしました。これは、この静的バージョンの迅速なロールアウトであり、バージョン 1.19 の作成とロールアウトに対応するためのものです。 検出を改善するため、Host_localhost_HEADER ルールとすべての Log4J および Java 逆シリアル化ルールを更新しました。 デプロイタイプの詳細については、「AWS マネージドルールの例外デプロイ」を参照してください。	2023-10-04

ルールグループおよびルール	説明	日付
AWS WAF Bot Control ルールグループ • TGT_TokenReuseIp • TGT_ML_CoordinatedActivityMedium • TGT_ML_CoordinatedActivityHigh	Count アクションでルールグループにルールを追加しました。 トークン再利用 IP ルールは、IP アドレス間でのトークンの共有を検出してカウントします。 調整されたアクティビティルールは、ウェブサイトのトラフィックを機械学習 (ML) で自動的に分析し、ボット関連のアクティビティを検出します。ルールグループ設定で、ML の使用をオプトアウトできます。このリリースでは、ターゲットを絞った保護レベルを現在使用しているユーザーが ML の使用にオプトインされます。オプトアウトすると、調整されたアクティビティルールが無効になります。	2023-09-06
AWS WAF Bot Control ルールグループ • CategoryAI	ルール CategoryAI をルールグループに追加しました。	2023-08-30

ルールグループおよびルール	説明	日付
コアルールセット (CRS) マネージドルールグループ • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS • EC2MetaDataSSRF_COOKIE • EC2MetaDataSSRF_QUERYARGUMENTS • EC2MetaDataSSRF_BODY • EC2MetaDataSSRF_URIPATH	このルールグループの静的バージョン 1.7 をリリースしました。 制限付き拡張ルールおよび EC2 メタデータ SSRF ルールを更新し、検出の向上と誤検出の低減を実現しました。	2023-07-26
AWS WAF Fraud Control アカウント作成不正防止 (ACFP) ルールグループ 新しいルールグループ内のすべてのルール	ルールグループ AWSManagedRulesACFPRuleSet を追加しました。	2023-06-13

ルールグループおよびルール	説明	日付
Linux オペレーティングシステムマネージドルールグループ • LFI_HEADER • LFI_URIPATH • LFI_QUERYSTRING	このルールグループの静的バージョン 2.2 をリリースしました。 検出の向上を図るために署名を追加しました。	2023-05-22
コアルールセット (CRS) マネージドルールグループ • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	このルールグループの静的バージョン 1.6 をリリースしました。 クロスサイトスクリプティング (XSS) および制限付き拡張ルールを更新し、検出の向上と誤検出の低減を実現しました。	2023-04-28

ルールグループおよびルール	説明	日付
PHP アプリケーションマネージドルールグループ • PHPHighRiskMethodsVariables_BODY を更新 • 「PHPHighRiskMethodsVariables_QUERYARGUMENTS 」を削除 • 「PHPHighRiskMethodsVariables_QUERYSTRING 」を追加 • 「PHPHighRiskMethodsVariables_HEADER 」を追加	このルールグループの静的バージョン 2.0 をリリースしました。 すべてのルールで検出を改善するために署名を追加しました。 ルール PHPHighRiskMethodsVariables_QUERYARGUMENTS を、クエリ引数だけでなくクエリ文字列全体を検査する PHPHighRiskMethodsVariables_QUERYSTRING に置き換えました。 ルール PHPHighRiskMethodsVariables_HEADER を追加し、すべてのヘッダーを含むようにカバレッジを拡張しました。 標準の AWS マネージドルールのラベル付けに合わせて、次のラベルを更新しました。 • 現在の名前: PHPHighRiskMethodsVariables_BODY 新しい名前: PHPHighRiskMethodsVariables_Body • 現在の名前: PHPHighRiskMethodsVariables_QUERYARGUMENTS 新しい名前: PHPHighRi	2023-02-27

ルールグループおよびルール	説明	日付
	skMethodsVariables_QueryString	
AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループ • VolumetricIpFailedLoginResponseHigh • VolumetricSessionFailedLoginResponseHigh	保護されている Amazon CloudFront ディストリビューションで使用するためのログインレスポンス検査ルールを追加しました。これらのルールは、最近のログイン試行の失敗回数が過度に多い IP アドレスやクライアントセッションからの新たなログイン試行をブロックします。	2023-02-15
コアルールセット (CRS) マネージドルールグループ • NoUserAgent_HEADER • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	このルールグループの静的バージョン 1.5 をリリースしました。 検出を改善するため、クロスサイトスクリプティング (XSS) フィルターを更新しました。	2023-01-25

ルールグループおよびルール	説明	日付
Linux オペレーティングシステムマネージドルールグループ • LFI_COOKIE - 削除済み • LFI_HEADER - 追加済み • LFI_URIPATH • LFI_QUERYSTRING	このルールグループの静的バージョン 2.1 をリリースしました。 ルール LFI_COOKIE およびそのラベル awswaf:managed:aws:linux-os:LFI_Cookie を削除し、新しいルール LFI_HEADER およびそのラベル awswaf:managed:aws:linux-os:LFI_Header に置き換えました。この変更により、検査が複数のヘッダーに拡張されます。 検出を改善するため、すべてのルールにテキスト変換および署名を追加しました。	2022-12-15

ルールグループおよびルール	説明	日付
コアルールセット (CRS) マネージドルールグループ • NoUserAgent_HEADER • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	このルールグループの静的バージョン 1.4 をリリースしました。 すべての NULL バイトを削除するため、テキスト変換を NoUserAgent_HEADER に追加しました。検出を改善するため、クロスサイトのスクリプティングルールのフィルターを更新しました。	2022-12-05

ルールグループおよびルール	説明	日付
既知の不正な入力マネージドルールグループ • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URIPATH • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_QUERYSTRING • Host_localhost_HEADER	このルールグループの静的バージョン 1.17 をリリースしました。 Java 逆シリアル化ルールを更新し、1.10.0 以前の Apache Commons Text バージョンのリモートコード実行 (RCE) 脆弱性である Apache CVE-2022-42889 に一致するリクエストの検出を追加しました。詳細については、「NIST: National Vulnerability Database: CVE-2022-42889 Detail」(NIST: 国家脆弱性データベース: CVE-2022-42889 詳細) および「CVE-2022-42889: Apache Commons Text prior to 1.10.0 allows RCE when applied to untrusted input due to insecure interpolation defaults」(CVE-2022-42889: 信頼されない入力に適用された場合にセキュアでない補間デフォルトが原因で 1.10.0 以前の Apache Commons Text で RCE が許可される) を参照してください。 Host_localhost_HEADER での検出を改善しました。	2022-10-20

ルールグループおよびルール	説明	日付
既知の不正な入力マネージドルールグループ • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URIPATH • Log4JRCE_BODY	このルールグループの静的バージョン 1.16 をリリースしました。 バージョン 1.15 で AWS 識別された誤検出を削除しました。	2022-10-05
POSIX オペレーティングシステムマネージドルールグループ PHP アプリケーションマネージドルールグループ WordPress アプリケーションマネージドルールグループ	記載されているラベル名を修正しました。	2022-09-19
IP 評価ルールグループ • AWSManagedIPDDoSList	この変更により、ルールグループがウェブトラフィックを処理する方法が変更されることはありません。 Amazon 脅威インテリジェンスに従い、DDoS アクティビティに積極的に関与している IP アドレスを検査する Count アクションを含む新しいルールが追加されました。	2022-08-30

ルールグループおよびルール	説明	日付
既知の不正な入力マネージドルールグループ • Log4JRCE • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URIPATH • Log4JRCE_BODY • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URIPATH • JavaDeserializationRCE_QUERYSTRING • Host_localhost_HEADER • PROPFIND_METHOD	このルールグループの静的バージョン 1.15 をリリースしました。 誤検出のよりきめ細かにモニタリングと管理を行うため、Log4JRCE を削除して Log4JRCE_HEADER 、Log4JRCE_QUERYSTRING 、Log4JRCE_URI 、Log4JRCE_BODY に置き換えました。 PROPFIND_METHOD とすべての JavaDeserializationRCE* と Log4JRCE* ルールに対する検出とブロックを改善するため、署名を追加しました。 Host_localhost_HEADER と全ての JavaDeserialization RCE* ルールにおける大文字化の修正をするためにラベルを更新しました。 JavaDeserializationRCE_HEADER の記述を修正しました。	2022-08-22

ルールグループおよびルール	説明	日付
AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループ • UnsupportedCognitoIDP	Amazon Cognito ユーザープールのウェブトラフィック用のアカウント乗っ取り防止マネージドルールグループの使用を防止するルールを追加しました。	2022-08-11
コアルールセット (CRS) マネージドルールグループ	AWS には、ルールグループのバージョン Version_1.2 と Version_2.0 の有効期限がスケジュールされています。このバージョンの有効期限は 2022 年 9 月 9 日に失効します。バージョンの有効期限の詳細については、「でのバージョニングされたマネージドルールグループの使用 AWS WAF」を参照してください。	2022-06-09
コアルールセット (CRS) マネージドルールグループ • GenericLFI_URIPATH GenericRFI_URIPATH	このルールグループのバージョン 1.3 をリリースしました。このリリースでは、検出を改善するため、GenericLFI_URIPATH および GenericRFI_URIPATH のルールにある一致する署名が更新されます。	2022-05-24
AWS WAF Bot Control ルールグループ • CategoryEmailClient	ルール CategoryEmailClient をルールグループに追加しました。	2022-04-06

ルールグループおよびルール	説明	日付
既知の不正な入力マネージドルールグループ • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URI • JavaDeserializationRCE_QUERYSTRING	このルールグループのバージョン 1.14 をリリースしました。4 つの JavaDeserializtionRCE ルールが Block モードに移行します。	2022-03-31
既知の不正な入力マネージドルールグループ • JavaDeserializationRCE_HEADER_RC_COUNT • JavaDeserializationRCE_BODY_RC_COUNT • JavaDeserializationRCE_URI_RC_COUNT • JavaDeserializationRCE_QUERYSTRING_RC_COUNT	このルールグループのバージョン 1.13 をリリースしました。Spring Core および Cloud Function RCE 脆弱性のテキスト変換を更新しました。これらのルールは、メトリクスを収集して一致したパターンを評価するため、カウントモードになっています。ラベルは、カスタムルール内のリクエストをブロックするために使用できます。後続のバージョンは、これらのルールがブロックモードになった状態でデプロイされます。	2022-03-31

ルールグループおよびルール	説明	日付
既知の不正な入力マネージドルールグループ • JavaDeserializationRCE_HEADER_RC_COUNT • JavaDeserializationRCE_BODY_RC_COUNT • JavaDeserializationRCE_URI_RC_COUNT • JavaDeserializationRCE_QUERYSTRING_RC_COUNT • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URI • Log4JRCE_BODY • Log4JRCE	このルールグループのバージョン 1.12 をリリースしました。Spring Core および Cloud Function RCE の脆弱性の署名を追加しました。これらのルールは、メトリクスを収集して一致したパターンを評価するため、カウントモードになっています。ラベルは、カスタムルール内のリクエストをブロックするために使用できます。後続のバージョンは、これらのルールがブロックモードになった状態でデプロイされます。 ルール Log4JRCE_HEADER 、Log4JRCE_QUERYSTRING 、Log4JRCE_URI 、Log4JRCE_BODY を削除してルール Log4JRCE に置き換えました。	2022-03-30
IP 評価ルールグループ • AWSManagedReconnaissanceList	アクションをカウントからブロックに変更するように AWSManagedReconnaissanceList ルールを更新しました。	2022-02-15

ルールグループおよびルール	説明	日付
AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループ 新しいルールグループ内のすべてのルール	ルールグループ AWSManagedRulesATPRuleSet を追加しました。	2022-02-11
既知の不正な入力マネージドルールグループ • Log4JRCE • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URI • Log4JRCE_BODY	このルールグループのバージョン 1.9 をリリースしました。この機能を柔軟に使用できるように、ルール Log4JRCE を削除し、ルール Log4JRCE_HEADER 、Log4JRCE_QUERYSTRING 、Log4JRCE_URI 、および Log4JRCE_BODY に置き換えました。検出とブロックを改善するために署名を追加しました。	2022-01-28
コアルールセット (CRS) • CrossSiteScripting_URIPATH • CrossSiteScripting_BODY • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_COOKIE	このルールグループのバージョン 2.0 をリリースしました。これらのルールでは、誤検出を減らすために検出シグネチャをチューニングしました。URL_DECODE テキスト変換をダブル URL_DECODE_UNI テキスト変換に置き換えました。HTML_ENTITY_DECODE テキスト変換を追加しました。	2022-01-10

ルールグループおよびルール	説明	日付
コアルールセット (CRS) • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS	このルールグループのバージョン 2.0 のリリースの一部として、URL_DECODE_UNI テキスト変換が追加されました。RestrictedExtensions_URIPATH から URL_DECODE テキスト変換を削除しました。	2022-01-10
SQL データベース • SQLi_BODY • SQLi_QUERYARGUMENTS • SQLi_COOKIE • SQLi_URIPATH • SQLiExtendedPatterns_BODY • SQLiExtendedPatterns_QUERYARGUMENTS	このルールグループのバージョン 2.0 をリリースしました。URL_DECODE テキスト変換をダブル URL_DECODE_UNI テキスト変換に置き換え、COMPRESS_WHITE_SPACE テキスト変換を追加しました。 検出シグネチャを SQLiExtendedPatterns_QUERYARGUMENTS に追加しました。 SQLi_BODY に JSON 検査を追加しました。 ルール SQLiExtendedPatterns_BODY を追加しました。 ルール SQLi_URIPATH を削除しました。	2022-01-10

ルールグループおよびルール	説明	日付
既知の不正な入力 • Log4JRCE	ヘッダーの検査と一致基準を改善するために、ルール Log4JRCE のバージョン 1.8 をリリースしました。	2021-12-17
既知の不正な入力 • Log4JRCE	一致基準をチューニングし、追加のヘッダーを検査するために、ルール Log4JRCE のバージョン 1.4 をリリースしました。バージョン 1.5 をリリースし、一致条件をチューニングしました。	2021-12-11
既知の不正な入力 • Log4JRCE • BadAuthToken_COOKIE_AUTHORIZATION	Log4j 内で最近公開されたセキュリティ問題に対応して、ルール Log4JRCE バージョン 1.2 を追加しました。詳細については、「CVE-2021-44228」を参照してください。このルールは、共通の URI パス、クエリ文字列、リクエストボディの最初の 8 KB、および共通ヘッダーを検査します。ルールはダブル URL_DECODE_UNI テキスト変換を使用します。一致基準をチューニングし、追加のヘッダーを検査するために、Log4JRCE のバージョン 1.3 をリリースしました。 ルール BadAuthToken_COOKIE_AUTHORIZATION を削除しました。	2021-12-10

次の表には、2021 年 12 月よりも前の変更が記載されています。

ルールグループおよびルール	説明	Date	
Amazon IP 評価リスト	`AWSManagedReconnaissanceList`	モニタリング/カウントモードの `AWSManagedReconnaissanceList` ルールを追加しました。このルールには、AWS リソースに対して偵察を実行している IP アドレスが含まれています。	2021-11-23

Windows オペレーティングシステム	`WindowsShellCommands`
	
	`PowerShellCommands`
		WindowsShell コマンド用に 3 つの新しいルールを追加しました: `WindowsShellCommands_COOKIE` 、`WindowsShellCommands_QUERYARGUMENTS` 、および `WindowsShellCommands_BODY` 。
		
		新しい PowerShell ルールを追加しました: `PowerShellCommands_COOKIE` 。
			2021-11-23

ルールグループおよびルール	説明	Date	
		文字列 _Set1 と _Set2 を削除して、PowerShellComands ルールの命名を再構築しました。 より包括的な検出シグネチャを PowerShellRules に追加しました。 すべての Windows オペレーティングシステムのルールに URL_DECODE_UNI テキスト変換を追加しました。	

ルールグループおよびルール	説明	Date	
Linux オペレーティングシステム	LFI_URIPATH LFI_QUERYSTRING LFI_BODY LFI_COOKIE	ダブル URL_DECODE テキスト変換をダブル URL_DECODE_UNI に置き換えました。 2 つ目のテキスト変換として NORMALIZE_PATH_WIN を追加しました。 LFI_BODY ルールを LFI_COOKIE ルールに置き換えました。 すべての LFI ルールに、より包括的な検出シグネチャを追加しました。	2021-11-23
コアルールセット (CRS)	SizeRestrictions_BODY	8 KB を超える本文ペイロードを持つウェブリクエストをブロックするためのサイズ制限を縮小しました。これまでは、制限は 10 KB でした。	2021-10-27

ルールグループおよびルール	説明	Date	

コアルールセット (CRS)	`EC2MetaDataSSRF_BODY`
	`EC2MetaDataSSRF_COOKIE`
	`EC2MetaDataSSRF_URIPATH`
	`EC2MetaDataSSRF_QUERYARGUMENTS`
		検出シグネチャを追加しました。ブロックを改善するためにダブルユニコード URL デコードを追加しました。	2021-10-27

コアルールセット (CRS)	`GenericLFI_QUERYARGUMENTS`
	`GenericLFI_URIPATH`
	`RestrictedExtensions_URIPATH`
	`RestrictedExtensions_QUERYARGUMENTS`
		ブロックを改善するためにダブルユニコード URL デコードを追加しました。	2021-10-27

ルールグループおよびルール	説明	Date	

コアルールセット (CRS)	`GenericRFI_QUERYARGUMENTS`
	
	`GenericRFI_BODY`
	
	`GenericRFI_URIPATH`
		お客様からのフィードバックに基づいて、誤検出を減らすためにルールシグネチャを更新しました。ブロックを改善するためにダブルユニコード URL デコードを追加しました。	2021-10-27

すべて	すべてのルール	AWS WAF ラベル付けをまだサポートしていないすべてのルールにラベルのサポートを追加しました。	2021-10-25
Amazon IP 評価リスト	`AWSManagedIPReputationList_xxxx`	IP 評価リストを再構築し、ルール名からサフィックスを削除し、 AWS WAF ラベルのサポートを追加しました。	2021-05-04

匿名 IP リスト	`AnonymousIPList`
	
	`HostingProviderList`
		AWS WAF ラベルのサポートが追加されました。	2021-05-04

Bot Control	すべて	Bot Control ルールセットを追加しました。	2021-04-01

ルールグループおよびルール	説明	Date	
コアルールセット (CRS)	GenericRFI_QUERYARGUMENTS	二重 URL デコードを追加しました。	2021-03-03
コアルールセット (CRS)	RestrictedExtensions_URIPATH	ルールの設定を改善し、追加の URL デコードを追加しました。	2021-03-03
管理者保護	AdminProtection_URIPATH	二重 URL デコードを追加しました。	2021-03-03
既知の不正な入力	ExploitablePaths_URIPATH	ルールの設定を改善し、追加の URL デコードを追加しました。	2021-03-03
Linux オペレーティングシステム	LFI_QUERYARGUMENTS	ルールの設定を改善し、追加の URL デコードを追加しました。	2021-03-03
Windows オペレーティングシステム	すべて	ルールの設定を改善しました。	2020-09-23
PHP アプリケーション	PHPHighRiskMethodsVariables_QUERYARGUMENTS PHPHighRiskMethodsVariables_BODY	ブロックを改善するために、テキスト変換を HTML デコードから URL デコードに変更しました。	2020-09-16

ルールグループおよびルール	説明	Date	

POSIX オペレーティングシステム	`UNIXShellCommandsVariables_QUERYARGUMENTS`
	
	`UNIXShellCommandsVariables_BODY`
		ブロックを改善するために、テキスト変換を HTML デコードから URL デコードに変更しました。	2020-09-16

コアルールセット	`GenericLFI_QUERYARGUMENTS`
	
	`GenericLFI_URIPATH`
	
	GenericLFI_BODY
		ブロックを改善するために、テキスト変換を HTML デコードから URL デコードに変更しました。	2020-08-07

Linux オペレーティングシステム	`LFI_URIPATH`
	
	`LFI_QUERYARGUMENTS`
	
	`LFI_BODY`
		検出とブロックを改良するために、テキスト変換を HTML エンティティデコードから URL デコードに変更しました。	2020-05-19

匿名 IP リスト	すべて	ビューワー ID の難読化を許可するサービスからのリクエストをブロックする IP 評価ルールグループ の新しいルールグループは、ボットや地理的制限の回避に対する軽減に役立ちます。	2020-03-06

ルールグループおよびルール	説明	Date	
WordPress アプリケーション	`WordPressExploitableCommands_QUERYSTRING`	クエリ文字列内の悪用の対象となるコマンドをチェックする新しいルール。	2020-03-03

コアルールセット (CRS)	`SizeRestrictions_QUERYSTRING`
	
	`SizeRestrictions_Cookie_HEADER`
	
	`SizeRestrictions_BODY`
	
	`SizeRestrictions_URIPATH`
		精度を向上させるために、サイズ値の制約を調整しました。	2020-03-03

SQL データベース	`SQLi_URIPATH`	ルールは、メッセージ URI をチェックするようになりました。	2020-01-23

SQL データベース	`SQLi_BODY`
	
	`SQLi_QUERYARGUMENTS`
	
	`SQLi_COOKIE`
		テキスト変換を更新しました。	2019-12-20

ルールグループおよびルール	説明	Date	
コアルールセット (CRS)	CrossSite Scripting _URIPATH CrossSite Scripting_BODY CrossSite Scripting _QUERYARG UMENTS CrossSite Scripting _COOKIE	テキスト変換を更新しました。	2019-12-20

独自のルールグループの管理

独自のルールグループを作成して、マネージドルールグループサービスに見つからないルールのコレクションや、自分で処理したいルールのコレクションを再利用できます。

作成したルールグループは、保護パック (ウェブ ACL) と同じようにルールを保持し、保護パック (ウェブ ACL) と同じようにルールグループにルールを追加します。独自のルールグループを作成する場合は、そのルールにイミュータブルな最大容量を設定する必要があります。

トピック

- ルールグループの作成
- ルールグループの編集
- 保護パック (ウェブ ACL) でのルールグループの使用
- ルールグループの削除
- ルールグループの共有

ルールグループの作成

新しいルールグループを作成するには、このページにある手順に従います。

ルールグループを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで、[Rule groups] (ルールグループ)、[Create rule group] (ルールグループの作成) の順に選択します。
3. ルールの名前と説明を入力します。これらを使用して、ルールセットを識別して管理し、使用します。

   `AWS`、`Shield`、`PreFM`、または `PostFM` で始まる名前は使用しないでください。これらの文字列は、予約されているか、他のサービスが管理するルールグループと混同される可能性があります。「他のサービスによって提供されるルールグループを識別する」を参照してください。

   > **Note**
   >
   > ウェブ ACL の作成後は、名前を変更できません。

4. [Region] (リージョン) で、ルールグループを保存するリージョンを選択します。Amazon CloudFront ディストリビューションを保護する保護パック (ウェブ ACL) でルールグループを使用するには、グローバル設定を使用する必要があります。リージョン別アプリケーションにもグローバル設定を使用できます。
5. [次へ] を選択します。
6. 保護パック (ウェブ ACL) 管理の場合と同様に、[Rule builder (ルールビルダー)] ウィザードを使用してルールグループにルールを追加します。唯一の違いは、ルールグループを別のルールグループに追加できないことです。
7. [Capacity] (容量) で、ルールグループによる保護パック (ウェブ ACL) 容量ユニット (WCU) の使用の最大値を設定します。この設定はイミュータブルです。WCU の詳細については、「のウェブ ACL キャパシティユニット (WCUs) AWS WAF」を参照してください。

   ルールグループにルールを追加すると、[Add rules and set capacity] (ルールの追加と容量の設定) ペインに、追加済みのルールに基づいて、必要な最小容量が表示されます。これとルールグループの将来の計画を使用して、ルールグループに必要な容量を見積もることができます。
8. ルールグループの設定を確認し、[Create] (作成) を選択します。

ルールグループの編集

ルールグループを追加、削除、あるいは設定を変更するには、このページの手順を使用してルールグループにアクセスします。

> **本番稼働トラフィックのリスク**
>
> 保護パック (ウェブ ACL) で現在使用しているルールグループを変更すると、その変更は、使用されている場所に関係なく保護パック (ウェブ ACL) の動作に影響します。トラフィックへの潜在的な影響に納得がいくまで、すべての変更をステージング環境またはテスト環境でテストし、調整するようにしてください。その後、更新したルールを有効にする前に、本番稼働用トラフィックでカウントモードでルールをテストしてチューニングします。ガイダンスについては、「AWS WAF 保護のテストとチューニング」を参照してください。

ルールグループを編集するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで、[Rule groups] (ルールグループ) を選択します。
3. 編集するルールグループ名を選択します。コンソールにルールグループのページが表示されます。

   > **Note**
   >
   > 編集するルールグループが表示されない場合は、[ルールグループ] セクション内に選択されたリージョンを確認してください。Amazon CloudFront ディストリビューションの保護に使用されるルールグループの場合は、[グローバル (CloudFront)] 設定を使用します。

4. 必要に応じてルールグループを編集します。ルールグループの変更可能なプロパティは、作成時と同様に編集できます。変更内容は、実行中にコンソールに保存されます。

   > **Note**
   >
   > ルールの名前を変更し、ルールのメトリクス名に変更を反映する場合は、メトリクス名も更新する必要があります。ルール名を変更しても、ルールのメトリクス名は自動的に更新 AWS WAF されません。ルールの JSON エディターを使用して、コンソールで

ルールを編集するときに、メトリック名を変更できます。API や、保護パック (ウェブ ACL) またはルールグループの定義に使用する JSON リストを使用して、両方の名前を変更することもできます。

更新中の一時的な不一致

保護パック (ウェブ ACL) または他の AWS WAF リソースを作成または変更すると、リソースが保存されているすべての領域にその変更が反映されるまでに少し時間がかかります。伝播時間は、数秒から数分までかかります。

次の内容では、変更伝播中に直面する一時的な不整合性の例を紹介します。

- 保護パック (ウェブ ACL) を作成した後、それをリソースに関連付けようとすると、保護パック (ウェブ ACL) が利用できないことを示す例外が表示される場合があります。
- ルールグループを保護パック (ウェブ ACL) に追加した後、新しいルールグループのルールは、保護パック (ウェブ ACL) が使用されるエリアで有効になり、別のエリアでは有効にならない場合があります。
- ルールのアクション設定を変更した後、古いアクションを一部のエリアで確認され、新しいアクションを別のエリアで確認される場合があります。
- ブロックルールで使用されている IP セットに IP アドレスを追加した後、新しいアドレスはあるエリアではブロックされ、別のエリアでは許可される場合があります。

保護パック (ウェブ ACL) でのルールグループの使用

保護パック (ウェブ ACL) でルールグループを使用するには、ルールグループリファレンスステートメントの保護パック (ウェブ ACL) にルールグループを追加します。

⚠ 本番稼働トラフィックのリスク

本番稼働トラフィックの保護パック (ウェブ ACL) に変更をデプロイする前に、ステージング環境またはテスト環境でテストおよびチューニングしてトラフィックへの潜在的な影響を確認します。その後、更新したルールを有効にする前に、本番稼働用トラフィックでカウントモードでルールをテストしてチューニングします。ガイダンスについては、「AWS WAF 保護のテストとチューニング」を参照してください。

> **Note**
>
> 保護パック (ウェブ ACL) で 1,500 WCU を超える容量を使用すると、保護パック (ウェブ ACL) の基本料金を超えるコストが発生します。詳細については、「のウェブ ACL キャパシティユニット (WCUs) AWS WAF」と「AWS WAF 料金表」を参照してください。

ルールグループを使用するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで、[Rule groups] (ルールグループ) を選択します。
3. 使用するルールグループ名を選択します。
4. [ルールの追加] を選択してから [独自のルールとルールグループの追加] を選択します。
5. [ルールグループ] を選択し、リストからルールグループを選択します。

保護パック (ウェブ ACL) では、個々のルールアクションが Count またはその他のアクションを起こすように設定することで、ルールグループおよびそのルールの動作を変更できます。これは、ルールグループのテスト、ルールグループ内のルールからの誤検出の特定、マネージドルールグループによるリクエストの処理方法のカスタマイズなどを行うのに役立ちます。詳細については、「でのルールグループアクションの上書き AWS WAF」を参照してください。

ルールグループにレートベースのステートメントが含まれている場合、ルールグループを使用する各保護パック (ウェブ ACL) は、ルールグループを使用する他の保護パック (ウェブ ACL) とは無関係に、レートベースのルールについて独自のレートトラッキングと管理を行います。詳細については、「でのレートベースのルールステートメントの使用 AWS WAF」を参照してください。

更新中の一時的な不一致

保護パック (ウェブ ACL) または他の AWS WAF リソースを作成または変更すると、リソースが保存されているすべての領域にその変更が反映されるまでに少し時間がかかります。伝播時間は、数秒から数分までかかります。

次の内容では、変更伝播中に直面する一時的な不整合性の例を紹介します。

- 保護パック (ウェブ ACL) を作成した後、それをリソースに関連付けようとすると、保護パック (ウェブ ACL) が利用できないことを示す例外が表示される場合があります。

- ルールグループを保護パック (ウェブ ACL) に追加した後、新しいルールグループのルールは、保護パック (ウェブ ACL) が使用されるエリアで有効になり、別のエリアでは有効にならない場合があります。
- ルールのアクション設定を変更した後、古いアクションを一部のエリアで確認され、新しいアクションを別のエリアで確認される場合があります。
- ブロックルールで使用されている IP セットに IP アドレスを追加した後、新しいアドレスはあるエリアではブロックされ、別のエリアでは許可される場合があります。

ルールグループの削除

ルールグループを削除するには、このセクションのガイダンスに従います。

参照セットとルールグループの削除

IP セット、正規表現パターンセット、ルールグループなど、保護パック (ウェブ ACL) で使用できるエンティティを削除すると、 はエンティティが保護パック (ウェブ ACL) で現在使用されている AWS WAF かどうかを確認します。使用中であることがわかった場合、 は AWS WAF 警告します。AWS WAF はほとんどの場合、エンティティが保護パック (ウェブ ACL) によって参照されているかどうかを判断できます。ただし、まれに判別できないことがあります。エンティティが現在使用中でないことを確認する必要がある場合は、削除する前に保護パック (ウェブ ACL) でそのエンティティを確認してください。エンティティが参照されているセットである場合は、ルールグループでエンティティが使用されていないことも確認してください。

ルールグループを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで、[Rule groups] (ルールグループ) を選択します。
3. 削除するスナップショットを選択し、[Delete] (削除) を選択します。

> **Note**
>
> 削除したいルールグループが表示されない場合は、[ルールグループ] セクション内のリージョンの選択を確認してください。Amazon CloudFront ディストリビューションの保護に使用されるルールグループの場合は、[グローバル (CloudFront)] 設定を使用します。

ルールグループの共有

ルールグループを別のアカウントと共有して、そのアカウントで使用することができます。

ルールグループの共有

1 つ以上の特定のアカウントと共有でき、組織内のすべてのアカウントと共有できます。

ルールグループを共有するには、 AWS WAF API を使用して、必要なルールグループ共有のポリシーを作成します。詳細については、「AWS WAF API リファレンス」の「PutPermissionPolicy」を参照してください。

共有されているルールグループの使用

ルールグループがアカウントと共有されている場合は、API 経由でアクセスでき、API 経由で保護パック (ウェブ ACL) を作成または更新するときに参照できます。詳細については、AWS WAF API リファレンスの「GetRuleGroup」、「CreateWebACL」、および「UpdateWebACL」を参照してください。共有されているルールグループは、 AWS WAF コンソールのルールグループリストに表示されません。

AWS Marketplace ルールグループ

このセクションでは、 AWS Marketplace ルールグループを使用する方法について説明します。

AWS Marketplace ルールグループは、 の AWS Marketplace コンソールからサブスクリプションで使用できますAWS Marketplace。 AWS Marketplace ルールグループをサブスクライブしたら、 で使用できます AWS WAF。 AWS Firewall Manager AWS WAF ポリシーで AWS Marketplace ルールグループを使用するには、組織内の各アカウントがルールグループをサブスクライブする必要があります。

さまざまなタイプのルールグループをサブスクライブするには、以下を使用します AWS Marketplace。

- AWS WAF パートナーマネージドルールグループ
- クライアント側の保護

本番トラフィックに使用する前に、 AWS WAF 保護の変更をテストして調整します。詳細については、「AWS WAF 保護のテストとチューニング」を参照してください。

AWS Marketplace ルールグループの料金

AWS Marketplace ルールグループは、長期契約や最低契約金なしで使用できます。ルールグループをサブスクライブすると、月額料金 (時間単位の日割り計算) と、ボリュームに基づく継続的なリクエスト料金が課金されます。ただし、サブスクライブされたルールグループをウェブ ACL に追加して使用を開始した場合にのみ、サブスクリプション料金が課金されます。詳細については、「」のAWS WAF 「料金表」と「各 AWS Marketplace ルールグループの説明」を参照してくださいAWS Marketplace。

AWS Marketplace ルールグループについて質問がありますか?

AWS Marketplace 販売者が管理するルールグループに関する質問や機能の変更をリクエストするには、プロバイダーのカスタマーサポートチームにお問い合わせください。連絡先情報を検索するには、「AWS Marketplace」のプロバイダーのリストを参照してください。

AWS Marketplace ルールグループプロバイダーは、ルールグループを更新する方法や、ルールグループがバージョニングされているかどうかなど、ルールグループを管理する方法を決定します。プロバイダーは、ルール、ルールアクション、ルールが一致するウェブリクエストに追加するラベルなど、ルールグループの詳細も決定します。

AWS Marketplace ルールグループのサブスクライブ

AWS WAF コンソールで AWS Marketplace ルールグループをサブスクライブまたはサブスクライブ解除できます。

> **Important**
>
> AWS Firewall Manager ポリシーで AWS Marketplace ルールグループを使用するには、まず組織内の各アカウントがそのルールグループにサブスクライブする必要があります。

AWS Marketplace ルールグループをサブスクライブするには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで、[アドオン保護] を選択します。
3. AWS Marketplace セクションで、ルールグループの名前を選択して、詳細と料金情報を表示します。

> **Tip**
>
> フィルターを使用して、最も関心のあるルールをすばやくソートします。例えば、カテゴリ フィルターを使用して、クライアント側の保護のみを表示できます。

4. AWS Marketplace ルールグループにサブスクライブするには:

   a. ルールグループに移動し、[Marketplace 経由でサブスクライブ] を選択します。

   b. 開いた Marketplace ページで、[購入オプションを表示] を選択し、[サブスクライブ] を選択します。

> **Note**
>
> ルールグループをサブスクライブしない場合は、ポップアップを閉じます。

AWS Marketplace ルールグループをサブスクライブしたら、他のマネージドルールグループと同様に保護パック (ウェブ ACLs) で使用します。詳細については、「で保護パック (ウェブ ACL) を作成する AWS WAF」を参照してください。

ルールグループを保護パック (ウェブ ACL) に追加する場合、ルールグループ内のルールおよびルールグループの結果のアクションをオーバーライドできます。詳細については、「でのルールグループアクションの上書き AWS WAF」を参照してください。

AWS Marketplace ルールグループからのサブスクリプション解除

AWS Marketplace コンソールで AWS Marketplace ルールグループのサブスクリプションを解除できます。

> **Important**
>
> AWS Marketplace ルールグループのサブスクリプション料金を停止するには、ルールグループのサブスクリプションを解除するだけでなく、Firewall Manager AWS WAF ポリシー AWS WAF のすべての保護パック (ウェブ ACLs) から削除する必要があります。 AWS Marketplace ルールグループからサブスクリプションを解除しても、保護パック (ウェブ ACLs) から削除しない場合は、サブスクリプションに対して引き続き課金されます。

AWS Marketplace ルールグループのサブスクリプションを解除するには

1. すべての保護パック (ウェブ ACL) からルールグループを削除します。詳細については、「での保護パック (ウェブ ACL) の編集 AWS WAF」を参照してください。
2. https://console.aws.amazon.com/marketplace で AWS コンソールを開きます。

   [サブスクリプションを管理] ページが表示されます。
3. [配信方法] リストを開き、[SaaS] を選択します。
4. [契約] で、[アクションリスト] を開き、サブスクリプションを解除するルールグループの名前の横にある [サブスクリプションをキャンセル] を選択します。
5. [サブスクリプションをキャンセル] ダイアログボックスで、**confirm** と入力し、[はい、サブスクリプションをキャンセルします] を選択します。

AWS Marketplace ルールグループのトラブルシューティング

AWS Marketplace ルールグループが正当なトラフィックをブロックしていることがわかった場合は、次の手順を実行して問題をトラブルシューティングできます。

AWS Marketplace ルールグループのトラブルシューティングを行うには

1. アクションをオーバーライドして、正当なトラフィックをブロックしているルールをカウントします。 AWS WAF サンプリングされたリクエストまたは AWS WAF ログを使用して、特定のリクエストをブロックしているルールを特定できます。ログの `ruleGroupId` フィールドまたはサンプリングされたリクエストの `RuleWithinRuleGroup` フィールドを調べることによって、ルールを識別できます。パターン `<Seller Name>#<RuleGroup Name>#<Rule Name>` 内のルールを識別できます。
2. リクエストのみをカウントするように特定のルールを設定しても問題が解決しない場合は、すべてのルールアクションを上書きするか、 AWS Marketplace ルールグループ自体のアクションを上書きなしから上書きしてカウントするように変更できます。これにより、ルールグループ内の個々のルールアクションに関係なく、ウェブリクエストが通過します。
3. 個々のルールアクションまたは AWS Marketplace ルールグループアクション全体を上書きした後、ルールグループプロバイダーのカスタマーサポートチームに連絡して、問題のトラブルシューティングをさらに行ってください。連絡先については、「 AWS Marketplace」の製品リストページのルールグループリストを参照してください。

AWS サポートへのお問い合わせ

AWS WAF または が管理するルールグループに関する問題については AWS、 にお問い合わせください AWS サポート。 AWS Marketplace 販売者が管理するルールグループに関する問題については、プロバイダーのカスタマーサポートチームにお問い合わせください。連絡先情報を確認するには、プロバイダーのリストを参照してください AWS Marketplace。

他のサービスによって提供されるルールグループを識別する

ユーザーまたは組織の管理者が AWS Firewall Manager または を使用してリソース保護 AWS Shield Advanced を管理する場合 AWS WAF、アカウントの保護パック (ウェブ ACLs) に追加されたルールグループのリファレンスステートメントが表示されることがあります。

これらのルールグループの名前は、次の文字列で始まります。

- **`ShieldMitigationRuleGroup`** – これらのルールグループは によって管理 AWS Shield Advanced され、保護されたアプリケーションレイヤー (レイヤー 7) リソースにアプリケーションレイヤー DDoS の自動緩和を提供するために使用されます。

  保護されたリソースでアプリケーションレイヤー DDoS 自動緩和を有効にすると、Shield Advanced は、リソースに関連付けた保護パック (ウェブ ACL) に、これらのルールグループの 1 つを追加します。Shield Advanced は、ルールグループ参照ステートメントに優先順位の設定として 10,000,000 を割り当て、ユーザーが保護パック (ウェブ ACL) で設定したルールの後に実行されるようにします。これらのルールタイプの詳細については、「Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和」を参照してください。

  > **Warning**
  >
  > 保護パック (ウェブ ACL) 内のこのルールグループを手動で管理しないでください。特に、`ShieldMitigationRuleGroup` ルールグループ参照ステートメントを保護パック (ウェブ ACL) から手動で削除しないでください。これにより、保護パック (ウェブ ACL) に関連付けられているすべてのリソースに意図しない結果が生じていた可能性もあります。代わりに、Shield Advanced を使用して、保護パック (ウェブ ACL) に関連付けられているリソースの自動緩和を無効にします。Shield Advanced は、ルールグループが自動緩和に必要でない場合に、ユーザーに代わって削除します。

- **`PREFMManaged`** および **`POSTFMManaged`** – これらのルールグループは、Firewall Manager AWS WAF ポリシー設定 AWS Firewall Manager に基づいて によって管理されます。Firewall Manager

は、Firewall Manager が管理する保護パック (ウェブ ACL) 内にそれらのルールグループを提供します。

Firewall Manager は、FMManagedWebACLV2 で始まる名前で保護パック (ウェブ ACL) を作成します。既存の保護パック (ウェブ ACL) を改良するように Firewall Manager を設定することもできます。その場合、保護パック (ウェブ ACL) 名は作成時に指定した名前です。いずれの場合も、Firewall Manager はこれらのルールグループを保護パック (ウェブ ACL) に追加します。詳細については、「Firewall Manager での AWS WAF ポリシーの使用」を参照してください。

のウェブ ACL キャパシティユニット (WCUs) AWS WAF

このセクションでは、ウェブ ACL キャパシティーユニット (WCU) とは何か、およびそれらの仕組みについて説明します。

AWS WAF は WCUs を使用して、ルール、ルールグループ、およびウェブ ACLs の実行に必要な運用リソースを計算および制御します。 は、ルールグループとウェブ ACL を設定するときに WCU ACLs 制限 AWS WAF を適用します。WCUs がウェブトラフィックを AWS WAF 検査する方法には影響しません。

AWS WAF は、ルール、ルールグループ、およびウェブ ACLs容量を管理します。

ルール WCU

AWS WAF は、ルールを作成または更新するときにルール容量を計算します。 は、各ルールの相対コストを反映するために、ルールタイプごとに異なる容量を AWS WAF 計算します。実行コストがほとんどない単純なルールでは、処理能力が大きい複雑なルールよりも使用される WCU が少なくなります。例えば、サイズ制約ルールステートメントでは、正規表現パターンセットを使用して検査するステートメントよりも使用する WCU が少なくなります。

ルール容量要件は通常、ルールタイプの基本コストに始まり、検査前にテキスト変換を追加する場合や JSON 本文を検査する場合など、複雑になるほど増えていきます。ルール容量要件については、「でのルールステートメントの使用 AWS WAF」にあるルールステートメントのリストを参照してください。

ルールグループ WCU

ルールグループの WCU 要件は、ルールグループ内で定義したルール数によって決まります。ルールグループの最大容量は 5,000 WCU です。

各ルールグループには、所有者が作成時に割り当てるイミュータブルな容量設定があります。これは、 で作成するマネージドルールグループとルールグループに当てはまります AWS WAF。ルールグループを変更する場合、それらの変更に伴うルールグループの WCU を容量内に収める必要があります。そうすることで、ルールグループを使用している保護パック (ウェブ ACL) が確実に容量要件内にとどまります。

ルールグループで使用されている WCUs は、ルールの WCUs の合計から、ルールの動作を組み合わせることで取得 AWS WAF できる処理の最適化を引いたものです。たとえば、同じウェブリクエストコンポーネントを調べるために 2 つのルールを定義し、各ルールが検査する前にコンポーネントに特定の変換を適用する場合、変換の適用に対して 1 回だけ課金できる AWS WAF 可能性があります。保護パック (ウェブ ACL) のルールグループを使用するための WCU コストは、常にルールグループ作成時に定義した固定の WCU 設定です。

ルールグループを作成するときは、ルールグループの有効期間中に使用するルール数に対応できる十分な容量を設定するように注意してください。

保護パック (ウェブ ACL) WCU

保護パック (ウェブ ACL) の WCU 要件は、保護パック (ウェブ ACL) 内で使用するルールとルールグループの数によって決まります。

- 保護パック (ウェブ ACL) のルールグループの使用コストは、ルールグループの容量設定に基づきます。
- ルールを使用するコストは、ルールの計算された WCUs から、保護パック (ウェブ ACL) のルールの組み合わせから取得 AWS WAF できる処理の最適化を引いたものです。たとえば、同じウェブリクエストコンポーネントを調べるために 2 つのルールを定義し、各ルールが検査する前にコンポーネントに特定の変換を適用する場合、変換の適用に対して 1 回だけ課金できる AWS WAF 可能性があります。

保護パック (ウェブ ACL) の基本料金には、最大 1,500 WCU の容量が含まれます。階層型料金モデルに従って、1,500 を超える WCUs を使用すると、追加料金が発生します。 は、保護パック (ウェブ ACL) の WCU 使用量の変化に応じて、保護パック (ウェブ ACL) の料金 AWS WAF を自動的に調整します。料金の詳細については、「AWS WAF の料金」を参照してください。

保護パック (ウェブ ACL) の最大容量は 5,000 WCU です。

ルールグループまたは保護パック (ウェブ ACL) の WCU を決定する

前のセクションで説明したように、ルールグループまたは保護パック (ウェブ ACL) で使用される WCU の合計は、ルールグループまたは保護パック (ウェブ ACL) で定義されているすべてのルールの WCU の合計と同じか それ以下 になります。

AWS WAF コンソールでは、保護パック (ウェブ ACL)、ウェブ ACL、またはルールグループにルールを追加するときに消費される容量を確認できます。ルールを追加するときに使用された現在のキャパシティユニットがコンソールに表示されます。

API を介して、保護パック (ウェブ ACL) またはルールグループで使用するルールの最大容量要件を確認できます。確認する場合は、チェックキャパシティコールでルールの JSON リストを指定します。詳細については、「AWS WAF V2 API リファレンス」の「CheckCapacity」を参照してください。

でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF

このセクションでは、 AWS WAFでウェブリクエストのボディ、ヘッダー、および cookie を検査する際のサイズ制限を管理する方法を説明します。

AWS WAF は、ウェブリクエストコンポーネント本文、ヘッダー、または Cookie の非常に大きなコンテンツの検査をサポートしていません。基盤となるホストサービスには、検査 AWS WAF のために転送されるホストサービスの数とサイズの制限があります。たとえば、ホストサービスは 200 個を超えるヘッダーを に送信しないため AWS WAF、205 個のヘッダーを持つウェブリクエストの場合、 AWS WAF は最後の 5 個のヘッダーを検査できません。

がウェブリクエストを保護されたリソースに進めること AWS WAF を許可すると、ウェブリクエスト全体が送信されます。これには、検査 AWS WAF できたカウントとサイズの制限外のコンテンツも含まれます。

コンポーネント検査のサイズ制限

コンポーネント検査のサイズ制限は次のとおりです。

- **`Body`** および **`JSON Body`** – Application Load Balancer および の場合 AWS AppSync、リクエストの本文の最初の 8 KB を検査 AWS WAF できます。CloudFront、API Gateway、Amazon Cognito、App Runner、Verified Access、Amazon Bedrock AgentCore Gateway では、デフォル

トで最初の 16 KB を検査 AWS WAF でき、保護パック (ウェブ ACL) 設定で制限を最大 64 KB まで増やすことができます。詳細については、「でのボディ検査の管理に関する考慮事項 AWS WAF」を参照してください。

- **`Headers`** – は、リクエストヘッダーの最初の 8 KB (8,192 バイト) まで、および最初の 200 個のヘッダーまで検査 AWS WAF できます。コンテンツは、最初の制限に達する AWS WAF まで検査できます。

  これらの制限は、リクエスト内のすべてのヘッダーを検査する場合に適用されます。1 つのヘッダーを検査する場合、 はこれらのサイズや数の制限なしに、そのヘッダーの全内容を検査 AWS WAF できます。
- **`Cookies`** – は、リクエスト Cookie の最初の 8 KB (8,192 バイト) まで、および最初の 200 個の Cookie まで検査 AWS WAF できます。コンテンツは、最初の制限に達する AWS WAF まで検査できます。

ルールステートメントのオーバーサイズの処理オプション

これらのリクエストコンポーネントタイプのいずれかを検査するルールステートメントを記述するときは、オーバーサイズコンポーネントの処理方法を指定します。オーバーサイズ処理は、ルールが検査するリクエストコンポーネントがサイズ制限を超えた場合に、ウェブリクエストの処理 AWS WAF 方法を指示します。

オーバーサイズコンポーネントを処理するためのオプションは次のとおりです。

- Continue – ルール検査基準に従って、リクエストコンポーネントを正常に検査します。 AWS WAF は、サイズ制限内にあるリクエストコンポーネントのコンテンツを検査します。
- Match – ウェブリクエストをルールステートメントに一致するものとして扱います。 は、ルールの検査基準に照らして評価することなく、ルールアクションをリクエスト AWS WAF に適用します。
- No match – ウェブリクエストは、ルールの検査基準に照らして評価せずに、ルールステートメントと一致しないものとして扱います。 は、一致しないルールの場合と同様に、保護パック (ウェブ ACL) の残りのルールを使用してウェブリクエストの検査 AWS WAF を続行します。

AWS WAF コンソールでは、これらの処理オプションのいずれかを選択する必要があります。コンソールの外では、デフォルトのオプションは Continue です。

Block に設定されたアクションを含むルールで Match オプションを使用する場合、そのルールは、検査したコンポーネントがオーバーサイズであるリクエストをブロックします。その他の設定では、リ

クエストの最終的な処理は、保護パック (ウェブ ACL) 内の他のルールの設定や、保護パック (ウェブ ACL) のデフォルトのアクション設定など、さまざまな要因によって異なります。

ユーザーが所有していないルールグループでのオーバーサイズの処理

コンポーネントのサイズと数の制限は、保護パック (ウェブ ACL) で使用するすべてのルールに適用されます。これには、マネージドルールグループ内および別のアカウントと共有しているルールグループ内にある、使用しているが管理されていないルールが含まれます。

ユーザーが管理していないルールグループを使用する場合、ルールグループに制限されたリクエストコンポーネントを検査するルールがあっても、そのルールではオーバーサイズのコンテンツが必要な方法で処理されない場合があります。 AWS マネージドルールがオーバーサイズコンポーネントを管理する方法については、「」を参照してくださいAWS マネージドルールのルールグループリスト。他のルールグループの詳細については、ルールグループプロバイダーにお問い合わせください。

保護パック (ウェブ ACL) 内のオーバーサイズコンポーネントを管理するためのガイドライン

保護パック (ウェブ ACL) でオーバーサイズのコンポーネントを処理する方法は、リクエストコンポーネントのコンテンツの予想サイズ、保護パック (ウェブ ACL) のデフォルトリクエスト処理、保護パック (ウェブ ACL) 内の他のルールがリクエストと一致して処理する方法など、さまざまな要因によって異なります。

オーバーサイズのウェブリクエストコンポーネントを管理するための一般的なガイドラインは、以下のとおりです。

- オーバーサイズのコンポーネントコンテンツを含む一部のリクエストを許可する必要がある場合は、可能な場合は、それらのリクエストのみを明示的に許可するルールを追加します。同じコンポーネントタイプを検査する保護パック (ウェブ ACL) 内の他のルールより先に実行されるように、これらのルールの優先度を上げます。この方法では、 AWS WAF を使用して、保護されたリソースに渡すことを許可するオーバーサイズコンポーネントのコンテンツ全体を検査することはできません。
- 他のすべてのリクエストでは、次のように、制限を超えるリクエストをブロックすることで、余計なバイトが通過するのを防ぐことができます。
  - ルールとルールグループ – サイズ制限のあるコンポーネントを検査するルールで、制限を超過するリクエストをブロックするようにオーバーサイズの処理を設定します。例えば、ルールで特定のヘッダーコンテンツを含むリクエストをブロックする場合、オーバーサイズのヘッダーコンテンツを持つリクエストと一致するようにオーバーサイズの処理を設定できます。別の例として、保護パック (ウェブ ACL) によりデフォルトでリクエストがブロックされ、かつルールで特

定のヘッダーコンテンツが許可されている場合、オーバーサイズのヘッダーコンテンツを持つすべてのリクエストと一致しないように、ルールのオーバーサイズ処理を設定できます。

- 管理していないルールグループ – 管理していないルールグループでオーバーサイズのリクエストコンポーネントを許可しないようにするには、リクエストコンポーネントタイプを検査して制限を超えるリクエストをブロックする別のルールを追加します。保護パック (ウェブ ACL) でそのルールがルールグループより先に実行されるように、ルールの優先度を上げます。例えば、保護パック (ウェブ ACL) で本文検査ルールを実行する前に、オーバーサイズの本文コンテンツを含むリクエストをブロックできます。次の手順では、このタイプのルールを追加する方法について説明します。

オーバーサイズのウェブリクエストコンポーネントのブロック

保護パック (ウェブ ACL) にルールを追加して、オーバーサイズのコンポーネントを使用したリクエストをブロックできます。

オーバーサイズのコンテンツをブロックするルールを追加するには

1. 保護パック (ウェブ ACL) を作成または編集するときは、ルール設定で、[Add rules] (ルールを追加)、[Add my own rules and rule groups] (独自のルールとルールグループを追加)、[Rule builder] (ルールビルダー)、[Rule visual editor] (ルールビジュアルエディタ) の順に選択します。保護パック (ウェブ ACL) の作成または編集に関するガイダンスについては、「でのウェブトラフィックメトリクスの表示 AWS WAF」を参照してください。
2. ルールの名前を入力し、[Type] (タイプ) 設定を [Regular rule] (通常のルール) のままにします。
3. 次の一致設定をデフォルトから変更します。

   a. [Statement] (ステートメント) の [Inspect] (検査) で、ドロップダウンを開き、必要なウェブリクエストコンポーネント ([Body] (本文)、[Headers] (ヘッダー)、[Cookies] (cookie) のいずれか) を選択します。

   b. [Match type] (一致タイプ) で、[Size greater than] (次より大きいサイズ:) を選択します。

   c. [サイズ] で、コンポーネントタイプの最小サイズ以上の数値を入力します。ヘッダーと Cookie の場合は、8192 を入力します。Application Load Balancer または AWS AppSync 保護パック (ウェブ ACLs) で、本文に と入力します8192。CloudFront、API Gateway、Amazon Cognito、App Runner、Verified Access、または Amazon Bedrock AgentCore Gateway 保護パック (ウェブ ACLs「」と入力します16384。それ以外の場合は、護パック (ウェブ ACL) のために定義した本文のサイズ制限を入力します。

   d. [Oversize handling] (オーバーサイズ処理) で、[Match] (一致) を選択します。

4. [Action] (アクション) で、[Block] (ブロック) を選択します。
5. [Add Rule] (ルールの追加) を選択します。
6. ルールを追加したら、[Set rule priority] (ルールの優先度の設定) ページで、同じコンポーネントタイプを検査する護パック (ウェブ ACL) 内のルールまたはルールグループよりも上に移動します。これにより、新しいルールの優先順位が低くなり、 AWS WAF が最初に評価します。詳細については、「ルールの優先度を設定する」を参照してください。

でサポートされている正規表現構文 AWS WAF

AWS WAF は、PCRE ライブラリ で使用される正規表現パターン構文をサポートしますlibpcre。ライブラリは、「PCRE - Perl Compatible Regular Expressions」で文書化されています。

AWS WAF は、ライブラリのすべてのコンストラクトをサポートしているわけではありません。例えば、一部のゼロ幅アサーションをサポートしますが、すべてではありません。サポートされているコンストラクトの包括的なリストはありません。ただし、無効な正規表現パターンを指定したり、サポートされていないコンストラクトを使用したりすると、 AWS WAF API は失敗を報告します。

AWS WAF は、次の PCRE パターンをサポートしていません。

- 後方参照と部分式取得
- サブルーチン参照と再帰パターン
- 条件付きパターン
- バックトラック制御動詞
- \C シングルバイトディレクティブ
- \R 改行一致ディレクティブ
- \K 一致開始位置リセットディレクティブ
- コールアウトと埋め込みコード
- アトミックグループと所有格量指定子

の IP セットと正規表現パターンセット AWS WAF

このセクションでは、IP セットと正規表現パターンセットのトピックについて説明します。

AWS WAF は、より複雑な情報をルールで参照して使用するセットに保存します。これらのセットにはそれぞれ名前があり、作成時に Amazon リソースネーム (ARN) が割り当てられます。これらの

セットは、ルールステートメント内から管理でき、コンソールのナビゲーションペインから単独でアクセスして管理できます。

ルールグループまたは保護パック (ウェブ ACL) で管理セットを使用できます。

- IP セットを使用するには、IP セット一致ルールステートメント を参照してください。
- 正規表現パターンセットを使用するには、正規表現パターンセット一致ルールステートメント を参照してください。

更新中の一時的な不一致

保護パック (ウェブ ACL) または他の AWS WAF リソースを作成または変更すると、リソースが保存されているすべての領域にその変更が反映されるまでに少し時間がかかります。伝播時間は、数秒から数分までかかります。

次の内容では、変更伝播中に直面する一時的な不整合性の例を紹介します。

- 保護パック (ウェブ ACL) を作成した後、それをリソースに関連付けようとすると、保護パック (ウェブ ACL) が利用できないことを示す例外が表示される場合があります。
- ルールグループを保護パック (ウェブ ACL) に追加した後、新しいルールグループのルールは、保護パック (ウェブ ACL) が使用されるエリアで有効になり、別のエリアでは有効にならない場合があります。
- ルールのアクション設定を変更した後、古いアクションを一部のエリアで確認され、新しいアクションを別のエリアで確認される場合があります。
- ブロックルールで使用されている IP セットに IP アドレスを追加した後、新しいアドレスはあるエリアではブロックされ、別のエリアでは許可される場合があります。

トピック

- での IP セットの作成と管理 AWS WAF
- での正規表現パターンセットの作成と管理 AWS WAF

での IP セットの作成と管理 AWS WAF

IP セットは、ルールステートメントで一緒に使用する IP アドレスと IP アドレス範囲のコレクションを提供します。IP セットは AWS リソースです。

保護パック (ウェブ ACL) またはルールグループで IP セットを使用するには、まずアドレス仕様IPSetで AWS リソースを作成します。その後、IP セットルールステートメントを保護パック (ウェブ ACL) またはルールグループに追加するときに、このセットを参照します。

IP セットの作成

新しい IP セットを作成するには、このセクションの手順に従います。

> **Note**
>
> このセクションの手順に加えて、IP 一致ルールを保護パック (ウェブ ACL) またはルールグループに追加するときに、新しい IP セットを追加するオプションがあります。このオプションを選択する場合は、この手順で必要な設定と同じ設定を指定する必要があります。

IP セットを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで、[IP sets] (IP セット) を選択し、[Create IP set] (IP セットの作成) を選択します。
3. IP セットの名前と説明を入力します。これらを使用して、セットを使用するときにそのセットを識別します。

   > **Note**
   >
   > IP セットの作成後は、名前を変更できません。

4. [Region] (リージョン) で、Global (CloudFront)、または IP セットを保存するリージョンを選択します。リージョン IP セットは、リージョンのリソースを保護する保護パック (ウェブ ACL) でのみ使用できます。Amazon CloudFront ディストリビューションを保護する保護パック (ウェブ ACL) で IP セットを使用するには、グローバル (CloudFront) を使用する必要があります。
5. [IP version] (IP バージョン) で、使用するバージョンを選択します。
6. IP アドレステキストボックスに、CIDR 表記に 1 行あたり 1 つの IP アドレスまたは IP アドレス範囲を入力します。 は、 を除くすべての IPv4 および IPv6 CIDR 範囲 AWS WAF をサポートします/0。CIDR 表記の詳細については、Wikipedia の「Classless Inter-Domain Routing」(クラスレスドメイン間ルーティング) 記事を参照してください。

次に例を示します。

- IPv4 アドレス 192.0.2.44 を指定するには、192.0.2.44/32 と入力します。
- IPv6 アドレス 2620:0:2d0:200:0:0:0:0 を指定するには、2620:0:2d0:200:0:0:0:0/128 と入力します。
- IPv4 アドレス範囲 192.0.2.0 ~ 192.0.2.255 を指定するには、192.0.2.0/24 と入力します。
- IPv6 アドレス範囲の 2620:0:2d0:200:0:0:0:0 ~ 2620:0:2d0:200:ffff:ffff:ffff:ffff を指定するには、2620:0:2d0:200::/64 と入力します。

7. IP セットの設定を確認し、[Create IP set] (IP セットの作成) を選択します。

IP セットの削除

参照セットを削除するには、このセクションのガイダンスに従います。

参照セットとルールグループの削除

IP セット、正規表現パターンセット、ルールグループなど、保護パック (ウェブ ACL) で使用できるエンティティを削除すると、 はエンティティが保護パック (ウェブ ACL) で現在使用されている AWS WAF かどうかを確認します。使用中であることがわかった場合、 は AWS WAF 警告します。AWS WAF はほとんどの場合、エンティティが保護パック (ウェブ ACL) によって参照されているかどうかを判断できます。ただし、まれに判別できないことがあります。エンティティが現在使用中でないことを確認する必要がある場合は、削除する前に保護パック (ウェブ ACL) でそのエンティティを確認してください。エンティティが参照されているセットである場合は、ルールグループでエンティティが使用されていないことも確認してください。

IP セットを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで [IP sets] (IP セット) を選択します。
3. 削除する IP セットを選択し、[Delete] (削除) を選択します。

での正規表現パターンセットの作成と管理 AWS WAF

正規表現パターンセットは、ルールステートメントで一緒に使用する正規表現のコレクションを提供します。正規表現パターンセットは AWS リソースです。

保護パック (ウェブ ACL) またはルールグループで正規表現パターンセットを使用するには、まず正規表現パターン仕様RegexPatternSetを使用して AWS リソースを作成します。その後、正規表現パターンセットルールステートメントを保護パック (ウェブ ACL) またはルールグループに追加するときに、このセットを参照します。正規表現パターンセットには、少なくとも1つの正規表現パターンが含まれている必要があります。

正規表現パターンセットに複数の正規表現パターンが含まれている場合、ルールで使用される場合、パターン一致は OR ロジックと組み合わされます。つまり、リクエストコンポーネントがセット内のいずれかのパターンに一致する場合、ウェブリクエストはパターンセットルールステートメントと一致します。

AWS WAF は、いくつかの例外libpcreを除いて、PCRE ライブラリで使用されるパターン構文をサポートします。ライブラリは、「PCRE - Perl Compatible Regular Expressions」で文書化されています。 AWS WAF サポートの詳細については、「」を参照してくださいでサポートされている正規表現構文 AWS WAF。

正規表現パターンセットの作成

新しい正規表現パターンセットを作成するには、このセクションの手順に従います。

正規表現パターンセットを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで、[Regex pattern sets] (正規表現パターンセット) を選択し、[Create regex pattern set] (正規表現パターンセットを作成) を選択します。
3. 正規表現パターンセットの名前と説明を入力します。これらを使用して、セットを使用するときに識別します。

   > **Note**
   >
   > 正規表現パターンセットの作成後は、名前を変更できません。

4. [Region] (リージョン) で、Global (CloudFront)、または正規表現パターンセットを保存するリージョンを選択します。正規表現パターンセットは、リージョンのリソースを保護する保護パック (ウェブ ACL) でのみ使用できます。Amazon CloudFront ディストリビューションを保護する保護パック (ウェブ ACL) で正規表現パターンセットを使用するには、グローバル (CloudFront) を使用する必要があります。

5. [Regular expressions] (正規表現) テキストボックスに、1 行につき 1 つの正規表現パターンを入力します。

   例えば、正規表現 `I[a@]mAB[a@]dRequest` は、`IamABadRequest`、`IamAB@dRequest`、`I@mABadRequest`、および `I@mAB@dRequest` の文字列に一致します。

   AWS WAF は、いくつかの例外`libpcre`を除いて、PCRE ライブラリで使用されるパターン構文をサポートします。ライブラリは、「PCRE - Perl Compatible Regular Expressions」で文書化されています。 AWS WAF サポートの詳細については、「」を参照してくださいでサポートされている正規表現構文 AWS WAF。

6. 正規表現パターンセットの設定を確認し、[Create regex pattern set] (正規表現パターンセットを作成) を選択します。

正規表現パターンセットの削除

参照セットを削除するには、このセクションのガイダンスに従います。

参照セットとルールグループの削除

IP セット、正規表現パターンセット、ルールグループなど、保護パック (ウェブ ACL) で使用できるエンティティを削除すると、 はエンティティが保護パック (ウェブ ACL) で現在使用されている AWS WAF かどうかを確認します。使用中であることがわかった場合、 は AWS WAF 警告します。AWS WAF はほとんどの場合、エンティティが保護パック (ウェブ ACL) によって参照されているかどうかを判断できます。ただし、まれに判別できないことがあります。エンティティが現在使用中でないことを確認する必要がある場合は、削除する前に保護パック (ウェブ ACL) でそのエンティティを確認してください。エンティティが参照されているセットである場合は、ルールグループでエンティティが使用されていないことも確認してください。

正規表現パターンセットを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで、[Regex pattern sets] (正規表現パターンセット) を選択します。
3. 削除する正規表現パターンセットを選択し、[Delete] (削除) を選択します。

でカスタマイズされたウェブリクエストとレスポンス AWS WAF

このセクションでは、 AWS WAF ルールアクションとデフォルト保護パック (ウェブ ACL) アクションにカスタムウェブリクエストとレスポンスの処理動作を追加する方法について説明します。カスタム設定は、アタッチ先のアクションが適用されるたびに適用されます。

ウェブリクエストとレスポンスは、次の方法でカスタマイズできます。

- Allow、Count、CAPTCHA、Challenge アクションを使用すると、カスタムヘッダーをウェブリクエストに挿入できます。 AWS WAF がウェブリクエストを保護されたリソースに転送する場合、リクエストには、元のリクエスト全体と、挿入したカスタムヘッダーが含まれます。CAPTCHA および Challenge アクションの場合、リクエストが CAPTCHA またはチャレンジトークン検査に合格した場合のみに、 AWS WAF がカスタマイズを適用します。

- Block アクションを使用すると、レスポンスコード、ヘッダー、本文を含めた完全なカスタムレスポンスを定義できます。保護されたリソースは、 が提供するカスタムレスポンスを使用してリクエストに応答します AWS WAF。カスタムレスポンスは、`403 (Forbidden)` のデフォルトの Block アクションレスポンスを置き換えます。

カスタマイズできるアクション設定

次のアクション設定を定義する際に、カスタムリクエストまたはレスポンスを指定できます。

- ルールアクション。詳細については、「でのルールアクションの使用 AWS WAF」を参照してください。
- 保護パック (ウェブ ACL) のデフォルトアクション。詳細については、「で保護パック (ウェブ ACL) のデフォルトアクションを設定する AWS WAF」を参照してください。

カスタマイズできないアクション設定

保護パック (ウェブ ACL) で使用するルールグループについては、オーバーライドアクションでカスタムリクエスト処理を指定することは できません。「のルールとルールグループで保護パック (ウェブ ACLs) を使用する AWS WAF」を参照してください。「でのマネージドルールグループステートメントの使用 AWS WAF」および「でのルールグループステートメントの使用 AWS WAF」も参照してください。

更新中の一時的な不一致

保護パック (ウェブ ACL) または他の AWS WAF リソースを作成または変更すると、リソースが保存されているすべての領域にその変更が反映されるまでに少し時間がかかります。伝播時間は、数秒から数分までかかります。

次の内容では、変更伝播中に直面する一時的な不整合性の例を紹介します。

- 保護パック (ウェブ ACL) を作成した後、それをリソースに関連付けようとすると、保護パック (ウェブ ACL) が利用できないことを示す例外が表示される場合があります。
- ルールグループを保護パック (ウェブ ACL) に追加した後、新しいルールグループのルールは、保護パック (ウェブ ACL) が使用されるエリアで有効になり、別のエリアでは有効にならない場合があります。
- ルールのアクション設定を変更した後、古いアクションを一部のエリアで確認され、新しいアクションを別のエリアで確認される場合があります。
- ブロックルールで使用されている IP セットに IP アドレスを追加した後、新しいアドレスはあるエリアではブロックされ、別のエリアでは許可される場合があります。

カスタムリクエストとレスポンスの使用制限

AWS WAF は、カスタムリクエストとレスポンスを使用するための最大設定を定義します。保護パック (ウェブ ACL) またはルールグループあたりのリクエストヘッダーの最大数、および単一のカスタムレスポンス定義のカスタムヘッダーの最大数はその一例です。詳細については、「AWS WAF クォータ」を参照してください。

トピック

- ノンブロッキングアクションのためのカスタムリクエストヘッダーの挿入
- 動的ラベル補間
- Block アクションのカスタムレスポンスの送信
- カスタムレスポンスでサポートされるステータスコード

ノンブロッキングアクションのためのカスタムリクエストヘッダーの挿入

このセクションでは、ルールアクションがリクエストをブロックしない場合に、 AWS WAF にカスタムヘッダーを元の HTTP リクエストに挿入するように指示する方法について説明します。このオプションでは、リクエストにのみ追加します。元のリクエストの一部を変更したり、置き換えたりすることはできません。カスタムヘッダー挿入のユースケースには、挿入されたヘッダーに基づいてリ

クエストを異なる方法で処理するようにダウンストリームアプリケーションに通知し、分析のためにリクエストのフラグを立てることが含まれます。

> **Important**
>
> このオプションは、ルールアクション Allow、Count、CAPTCHA、Challenge に適用され、Allow に設定されている保護パック (ウェブ ACL) のデフォルトアクションにも適用されます。ルールアクションの詳細については、「でのルールアクションの使用 AWS WAF」を参照してください。デフォルトの保護パック (ウェブ ACL) アクションの詳細については、「で保護パック (ウェブ ACL) のデフォルトアクションを設定する AWS WAF」を参照してください。

カスタムリクエストヘッダー名を使用する場合の考慮事項

リクエストヘッダーに追加されたプレフィックス

AWS WAF は、リクエストにすでに存在するヘッダーとの混同を避けるために`x-amzn-waf-`、 で挿入するすべてのリクエストヘッダーにプレフィックスを付けます。たとえば、ヘッダー名 を指定すると`sample`、 はヘッダー AWS WAF を挿入します`x-amzn-waf-sample`。

> **Important**
>
> セキュリティプラクティスとして、ヘッダーがすでに `x-amzn-waf-` で始まるリクエストをブロックする文字列一致ルールを追加できます。これにより、カスタムリクエストヘッダーを処理するときに によって AWS WAF 挿入される`x-amzn-waf-`プレフィックス文字列を模倣する非AWS WAF ソースからのリクエストがブロックされます。

次の例は、`x-amzn-waf-`プレフィックスが挿入されなかったトラフィックをブロックするように設定された文字列一致ルールを示しています AWS WAF。

```
"Rules": [
    {
      "Name": "CustomHeader",
      "Priority": 0,
      "Statement": {
        "ByteMatchStatement": {
          "SearchString": " x-amzn-waf-",
          "FieldToMatch": {
```

```
            "Headers": {
              "MatchPattern": {
                "All": {}
              },
              "MatchScope": "KEY",
              "OversizeHandling": "MATCH"
            }
          },
          "TextTransformations": [
            {
              "Priority": 0,
              "Type": "NONE"
            }
          ],
          "PositionalConstraint": "STARTS_WITH"
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "CustomHeader"
      }
    }
  ]
```

文字列一致ルールの使用については、「文字列一致ルールステートメント」を参照してください。

同じ名前のヘッダー

リクエストに既に挿入されているのと同じ名前のヘッダーがある場合、 AWS WAF はヘッダーを AWS WAF 上書きします。したがって、同じ名前の複数のルールでヘッダーを定義すると、リクエストを検査して一致を見つける最後のルールにはヘッダーが追加され、それよりも前のルールには追加されません。

終了しないルールアクションを含むカスタムヘッダーの使用

Allow アクションとは異なり、Countアクションは保護パック (ウェブ ACL) の残りのルールを使用したウェブリクエストの処理 AWS WAF を停止しません。同様に、 CAPTCHAおよび がリクエストトークンが有効であるChallengeと判断した場合、これらのアクションはウェブリクエストの処理 AWS WAF を停止しません。したがって、これらのアクションを使用するルールでカスタムヘッ

ダーを挿入する場合、後続のルールもカスタムヘッダーを挿入することがあります。ルールアクションの動作については、「でのルールアクションの使用 AWS WAF」を参照してください。

例えば、表示された順序で優先順位付けされた次のルールがあるとします。

1. Count アクションと RuleAHeader という名前のカスタマイズされたヘッダーを持つ RuleA。
2. Allow アクションと RuleBHeader という名前のカスタマイズされたヘッダーを持つ RuleB。

リクエストが RuleA と RuleB の両方に一致する場合、 はヘッダーと x-amzn-waf-RuleAHeader AWS WAF を挿入しx-amzn-waf-RuleBHeader、保護されたリソースにリクエストを転送します。

AWS WAF は、リクエストの検査が完了すると、カスタムヘッダーをウェブリクエストに挿入します。したがって、アクションが Count に設定されているルールでカスタムリクエスト処理を使用する場合、追加するカスタムヘッダーは後続のルールによって検査されません。

カスタムリクエスト処理の例

ルールのアクションまたは保護パック (ウェブ ACL) のデフォルトアクション用に、カスタムリクエスト処理を定義します。次のリストは、保護パック (ウェブ ACL) のデフォルトアクションに追加されたカスタム処理用の JSON を示しています。

```
{
 "Name": "SampleWebACL",
 "Scope": "REGIONAL",
 "DefaultAction": {
  "Allow": {
   "CustomRequestHandling": {
    "InsertHeaders": [
     {
      "Name": "fruit",
      "Value": "watermelon"
     },
     {
      "Name": "pie",
      "Value": "apple"
     }
    ]
   }
  }
 },
```

```
  "Description": "Sample protection pack (web ACL) with custom request handling
  configured for default action.",
  "Rules": [],
  "VisibilityConfig": {
   "SampledRequestsEnabled": true,
   "CloudWatchMetricsEnabled": true,
   "MetricName": "SampleWebACL"
  }
 }
```

動的ラベル補間

動的ラベル補間を使用すると、${namespace:}構文を使用してカスタムリクエストヘッダー、カスタムレスポンスヘッダー、カスタムレスポンス本文にラベル値を直接埋め込むことができます。は、評価時に各プレースホルダーをリクエストにアタッチされたラベルに対して AWS WAF 解決するため、ラベル値ごとに個別のルールを記述する必要はありません。

補間は既存の AWS WAF API 内で機能し、新しいフィールドや設定ステップはありません。プレースホルダー構文は、既存の文字列値で使用します。既存の静的ヘッダー値は引き続き変更されません。補間は、値に ${namespace:}句が含まれている場合にのみアクティブ化されます。

補間がサポートされている場所

補${namespace:}間は、次の場所で使用できます。

- カスタムリクエストヘッダー – オリジンに転送されたヘッダーに解決済みラベル値を挿入します。ヘッダー値フィールドで ${namespace:}構文を使用します。
- カスタムレスポンス本文 – ブロックページ、チャレンジページ、およびその他のカスタムレスポンスにラベル値と合成ラベルを埋め込みます。レスポンス本文のコンテンツフィールドで ${namespace:}構文を使用します。
- カスタムレスポンスヘッダー – リダイレクトのヘッダーなど、レスポンスLocationヘッダーにラベル値を挿入します。レスポンスヘッダー値フィールドで ${namespace:}構文を使用します。

補間構文と解決

補間を使用するには、ヘッダー値またはカスタムレスポンス本文コンテンツに ${namespace:}句を含めます。末尾のコロンは重要です。1 つのラベルを文字通り一致させるのではなく、その名前空間内のすべてのラベルを解決 AWS WAF するように に指示します。

AWS WAF は、次のルールを使用して、評価時に各句を解決します。

1. 単一ラベル一致 – 句はラベルのターミナル値に解決されます。たとえば、リクエストにラベル があるawswaf:managed:aws:bot-control:bot:category:scraping、 句はに${awswaf:managed:aws:bot-control:bot:category:}解決されますscraping。
2. 複数のラベル – 複数のラベルが名前空間に一致する場合、値はカンマ区切りリストとして返され、名前空間プレフィックスは削除されます。例えば、scraping,advertising。
3. 一致なし – 句は空の文字列に解決されます。

> **Note**
>
> 単一の文字列値は、最大 10 個の${namespace:}プレースホルダーをサポートします。値に 10 個を超えるプレースホルダーが含まれている場合、 は最初の 10 個を AWS WAF 解決し、出力に追加のプレースホルダーをリテラル${namespace:}テキストとして残します。この制限は、各リクエストではなく、各文字列値に適用されます。複数のヘッダーごとに最大 10 個のプレースホルダーを問題なく使用できます。

> **Important**
>
> カスタムラベルは、 で短縮名を使用しますruleLabels。例えば、app:tier:enterprise。ただし、 は短縮名に保護パック (ウェブ ACL) コンテキスト AWS WAF を自動的にプレフィックスし、完全修飾ラベルを生成します。例えば、awswaf:*ACCOUNT_ID*:webacl:*WEBACL_NAME*:app:tier:enterprise。ラベル一致ステートメントは短い名前空間で機能しますが、補間参照は常に完全修飾名前空間を使用する必要があります。

合成ラベル

補間は合成ラベルもサポートしています。これらは、ラベルストアからではなくリクエストコンテキストから解決される AWS WAF 組み込み値です。合成ラベルを同じ値文字列内の名前空間ベースのラベルと組み合わせることができます。

合成ラベル	説明
${awswaf:request_id:}	一意の AWS WAF リクエスト識別子。

合成ラベル	説明
${awswaf:ip:}	クライアントの IP アドレス。
${awswaf:ja3:}	JA3 TLS フィンガープリント。
${awswaf:ja4:}	JA4 TLS フィンガープリント。

動的ラベル補間の例

動的ヘッダーを使用したアプリケーションシグナリング

次のルールは、複数の Bot Control シグナル名前空間を個別のヘッダーとしてオリジンに転送します。1 つのルールは名前空間全体を対象とするため、マネージドルールグループが新しいラベルを追加するときにルールを更新する必要はありません。

```
{
  "Name": "forward-waf-signals",
  "Statement": {
    "LabelMatchStatement": {
      "Scope": "NAMESPACE",
      "Key": "awswaf:managed:aws:bot-control:bot:category:"
    }
  },
  "RuleAction": {
    "Count": {
      "CustomRequestHandling": {
        "InsertHeaders": [
          { "Name": "bot-category",
            "Value": "${awswaf:managed:aws:bot-control:bot:category:}" },
          { "Name": "bot-name",
            "Value": "${awswaf:managed:aws:bot-control:bot:name:}" },
          { "Name": "bot-signals",
            "Value": "${awswaf:managed:aws:bot-control:signal:}" },
          { "Name": "client-ip",
            "Value": "${awswaf:ip:}" }
        ]
      }
    }
  }
}
```

bot-signals ヘッダー (出力: x-amzn-waf-bot-signals) は、複数値の解決を示します。signal: 名前空間には、カンマ区切りリストに解決される などnon_browser_user_agent,automated_browser、複数のラベルを含めることができます。client-ip ヘッダー (出力: x-amzn-waf-client-ip) は合成ラベルを使用します。

デバッグ情報を含むカスタムブロックページ

合成ラベルを使用すると、リクエスト固有のコンテキストを含むブロックページを構築できます。クライアントの IP アドレスと AWS WAF リクエスト ID をレスポンス本文に直接埋め込み、ユーザーが誤検出をレポートしたときに共有する内容を提供します。

```
{
  "CustomResponseBodies": {
    "BlockPage": {
      "Content": "Your request was blocked.\n\nIP: ${awswaf:ip:}\nRequest ID:
 ${awswaf:request_id:}\n\nIf you believe this is an error, contact support with the
 Request ID above.",
      "ContentType": "TEXT_PLAIN"
    }
  }
}
```

カスタムラベル補間

補間は、独自のルールで定義したカスタムラベルなど、任意のラベル名前空間で機能します。次の例では、API キーでリクエストを分類し、階層値をオリジンに転送します。

ルール 1: API キーに基づいて階層を分類する

このルールは、リクエストをエンタープライズ API キーと照合し、カスタムラベルを適用します。

```
{
{
  "Name": "classify-tier",
  "Priority": 100,
  "Statement": {
    "ByteMatchStatement": {
      "SearchString": "pk_enterprise_",
      "FieldToMatch": { "SingleHeader": { "Name": "x-api-key" } },
      "PositionalConstraint": "STARTS_WITH",
      "TextTransformations": [{ "Priority": 0, "Type": "NONE" }]
    }
```

```
  },
  "RuleLabels": [{ "Name": "app:tier:enterprise" }],
  "Action": { "Count": {} }
}

}
```

ルール 2: 解決された階層値を転送

このルールは、app:tier名前空間内の任意のラベルに一致し、解決された値をヘッダーとして転送します。

```
{
{
  "Name": "forward-tier",
  "Priority": 200,
  "Statement": {
    "LabelMatchStatement": {
      "Scope": "NAMESPACE",
      "Key": "app:tier:"
    }
  },
  "Action": {
    "Count": {
      "CustomRequestHandling": {
        "InsertHeaders": [{
          "Name": "customer-tier",
          "Value": "${awswaf:ACCOUNT_ID:webacl:WEBACL_NAME:app:tier:}"
        }]
      }
    }
  }
}
```

最初のルールはラベル を適用しますapp:tier:enterprise。2 番目のルールは、app:tier名前空間内の任意のラベルに一致し、解決された値を customer-tierヘッダーとして転送します。出力ヘッダー名は ですx-amzn-waf-customer-tier。app:tier:standard や など、他の階層の分類ルールを追加できますapp:tier:trial。転送ルールは、変更なしでそれらを取得します。

これらのパターンをすべて示すデプロイ可能なサンプルについては、GitHub のAWS WAF 「動的ラベル補間サンプル」を参照してください。

Block アクションのカスタムレスポンスの送信

このセクションでは、 に設定されたルールアクションまたは保護パック (ウェブ ACL) のデフォルトアクションのためにカスタム HTTP レスポンスをクライアントに送信する AWS WAF ように に指示する方法について説明しますBlock。ルールアクションの詳細については、「でのルールアクションの使用 AWS WAF」を参照してください。デフォルトの保護パック (ウェブ ACL) アクションの詳細については、「で保護パック (ウェブ ACL) のデフォルトアクションを設定する AWS WAF」を参照してください。

Block アクションのカスタムレスポンス処理を定義すると、ステータスコード、ヘッダー、レスポンス本文を定義します。で使用できるステータスコードのリストについては AWS WAF、次のセクション「」を参照してくださいカスタムレスポンスでサポートされるステータスコード。

ユースケース

カスタムレスポンスのユースケースには、次が含まれます。

- 非デフォルトのステータスコードをクライアントに送り返します。
- カスタムレスポンスヘッダーをクライアントに送り返します。`content-type` を除き、任意のヘッダー名を指定できます。
- 静的エラーページをクライアントに送り返します。
- クライアントを別の URL にリダイレクトします。これを行うには、`301` (`Moved Permanently`) または `302` (`Found`) などの `3xx` リダイレクトステータスコードのいずれかを指定してから、新しい URL で `Location` という名前が付けられた新しいヘッダーを指定します。

保護されたリソースで定義したレスポンスとのインタラクション

アクションに AWS WAF Block指定したカスタムレスポンスは、保護されたリソースで定義したレスポンス仕様よりも優先されます。

で保護する AWS リソースのホストサービスは、ウェブリクエストのカスタムレスポンス処理を許可する AWS WAF 場合があります。次に例を示します。

- Amazon CloudFront を使用して、ステータスコードに基づいてエラーページをカスタマイズできます。カスタムエラーページの詳細については、「Amazon CloudFront デベロッパーガイド」の「カスタムエラーレスポンスの生成」を参照してください。

- Amazon API Gateway では、ゲートウェイのレスポンスおよびステータスコードを定義できます。詳細については、「Amazon API Gateway デベロッパーガイド」の「API Gateway でのゲートウェイレスポンス」を参照してください。

保護された AWS リソースの AWS WAF カスタムレスポンス設定とカスタムレスポンス設定を組み合わせることはできません。個々のウェブリクエストの応答の仕様は、 AWS WAF または保護されたリソースから、そのすべてが取得されます。

が AWS WAF ブロックするウェブリクエストの場合、優先順位を次に示します。

1. AWS WAF カスタムレスポンス – AWS WAF Blockアクションでカスタムレスポンスが有効になっている場合、保護されたリソースは設定されたカスタムレスポンスをクライアントに送り返します。保護されたリソース自体で定義する応答設定は、効果がありません。
2. 保護されたリソースで定義されているカスタムレスポンス - それ以外の場合、保護されたリソースにカスタムレスポンス設定が指定されているときは、保護されたリソースはそれらの設定を使用してクライアントに応答します。
3. AWS WAF デフォルトBlockレスポンス – それ以外の場合、保護されたリソースは AWS WAF デフォルトのレスポンス でクライアントにBlock応答します`403 (Forbidden)`。

が AWS WAF 許可するウェブリクエストの場合、保護されたリソースの設定によって、クライアントに返送するレスポンスが決まります。許可されたリクエスト AWS WAF に対して でレスポンス設定を構成することはできません。許可されたリクエスト AWS WAF に対して で設定できる唯一のカスタマイズは、リクエストを保護されたリソースに転送する前に、元のリクエストにカスタムヘッダーを挿入することです。このオプションについては、前のセクション「ノンブロッキングアクションのためのカスタムリクエストヘッダーの挿入」で説明しました。

カスタムレスポンスヘッダー

`content-type` を除き、任意のヘッダー名を指定できます。

カスタムレスポンス本文

カスタムレスポンスの本文は、それを使用する保護パック (ウェブ ACL) またはルールグループのコンテキスト内で定義します。カスタムレスポンスボディの定義後、それを作成した保護パック (ウェブ ACL) またはルールグループの他の場所を参照して使用できます。個々の Block アクション設定では、使用するカスタム本文を参照し、カスタムレスポンスのステータスコードおよびヘッダーを定義します。

コンソールでカスタムレスポンスを作成するときは、既に定義したレスポンス本文から選択するか、新しい本文を作成できます。コンソールの外部では、保護パック (ウェブ ACL) またはルールグループレベルでカスタムレスポンス本文を定義し、保護パック (ウェブ ACL) またはルールグループ内のアクション設定から参照します。これは、次のセクションの JSON の例で示されます。

カスタムレスポンスの例

次の例は、カスタムレスポンス設定を持つルールグループの JSON をリストします。カスタムレスポンス本文は、ルールグループ全体のために定義され、ルールアクションでキーによって参照されます。

```
{
 "ARN": "test_rulegroup_arn",
 "Capacity": 1,

 "CustomResponseBodies": {
  "CustomResponseBodyKey1": {
   "Content": "This is a plain text response body.",
   "ContentType": "TEXT_PLAIN"
  }
 },

 "Description": "This is a test rule group.",
 "Id": "test_rulegroup_id",
 "Name": "TestRuleGroup",

 "Rules": [
  {
   "Action": {
    "Block": {
     "CustomResponse": {
      "CustomResponseBodyKey": "CustomResponseBodyKey1",
      "ResponseCode": 404,
      "ResponseHeaders": [
       {
        "Name": "BlockActionHeader1Name",
        "Value": "BlockActionHeader1Value"
       }
      ]
     }
    }
   },
   "Name": "GeoMatchRule",
```

```
    "Priority": 1,
    "Statement": {
     "GeoMatchStatement": {
      "CountryCodes": [
       "US"
      ]
     }
    },
    "VisibilityConfig": {
     "CloudWatchMetricsEnabled": true,
     "MetricName": "TestRuleGroupReferenceMetric",
     "SampledRequestsEnabled": true
    }
   }
  ],
  "VisibilityConfig": {
   "CloudWatchMetricsEnabled": true,
   "MetricName": "TestRuleGroupMetric",
   "SampledRequestsEnabled": true
  }
 }
```

カスタムレスポンスでサポートされるステータスコード

このセクションでは、カスタムレスポンスで使用できるステータスコードを一覧表示します。HTTP ステータスコードの詳細については、Internet Engineering Task Force (IETF) による「Status Codes」(ステータスコード) およびウィキペディアの「List of HTTP status codes」(HTTP ステータスコードのリスト) を参照してください。

カスタムレスポンスで が AWS WAF サポートする HTTP ステータスコードは次のとおりです。

- 2xx Successful
  - 200 – OK
  - 201 – Created
  - 202 – Accepted
  - 204 – No Content
  - 206 – Partial Content
- 3xx Redirection
  - 300 – Multiple Choices

  - 301 – Moved Permanently
  - 302 – Found
  - 303 –See Other
  - 304 – Not Modified
  - 307 – Temporary Redirect
  - 308 – Permanent Redirect
- 4xx Client Error
  - 400 – Bad Request
  - 401 – Unauthorized
  - 403 – Forbidden
  - 404 – Not Found
  - 405 – Method Not Allowed
  - 408 – Request Timeout
  - 409 – Conflict
  - 411 – Length Required
  - 412 – Precondition Failed
  - 413 – Request Entity Too Large
  - 414 – Request-URI Too Long
  - 415 – Unsupported Media Type
  - 416 – Requested Range Not Satisfiable
  - 421 – Misdirected Request
  - 429 – Too Many Requests
- 402 (支払いが必要) – AI エージェントに価格マニフェストを返すために Monetize アクションによって使用されます。レスポンス本文には、JSON 形式の機械読み取り可能な料金、承認された支払い方法、ライセンス条項が含まれています。
- 5xx Server Error
  - 500 – Internal Server Error
  - 501 – Not Implemented
  - 502 – Bad Gateway
  - 503 – Service Unavailable

- 504 – Gateway Timeout
- 505 – HTTP Version Not Supported

でのウェブリクエストのラベル付け AWS WAF

このセクションでは、 AWS WAF ラベルについて説明します。

ラベルは、ルールがリクエストと一致するときに、ルールによってウェブリクエストに追加されるメタデータです。追加された場合、保護パック (ウェブ ACL) 評価が終了するまで、ラベルはリクエストに引き続き存在します。保護パック (ウェブ ACL) の評価で後から実行されるルール内のラベルには、ラベル照合ステートメントを使用してアクセスできます。詳細については、「ラベル一致ルールステートメント」を参照してください。

ウェブリクエストのラベルは Amazon CloudWatch ラベルメトリクスを生成します。メトリクスとディメンションのリストについては、「ラベルメトリクスとディメンション」を参照してください。CloudWatch および AWS WAF コンソールからメトリクスとメトリクスの概要にアクセスする方法については、「AWS WAF 保護のモニタリングと調整」を参照してください。

ラベリングのユースケース

AWS WAF ラベルの一般的なユースケースは次のとおりです。

- リクエストに対してアクションを実行する前に、複数のルールステートメントに対するウェブリクエストを評価する – 保護パック (ウェブ ACL) 内のルールで一致が見つかった後、ルールアクションが保護パック (ウェブ ACL) 評価を終了しない場合、 は保護パック (ウェブ ACL) に対するリクエストの評価 AWS WAF を続行します。リクエストを許可または拒否するか判断する前、ラベルを使用して複数のルールから情報を評価および収集できます。これを行うには、既存のルールのアクションを Count に変更し、ラベルを一致リクエストに追加するように設定します。その後、他のルールの後に実行する新しいルールを 1 つ以上追加し、ラベルを評価してラベル一致の組み合わせに応じてリクエストを管理するように設定します。
- 地域別のウェブリクエストの管理 – 地理的一致ルールを単独で使用して、ウェブリクエストを発信国別に管理できます。地域レベルの精度で場所を微調整するには、地理一致ルールを Count アクションと一緒に使用し、それに続いてラベルマッチルールを使用します。地理一致ルールの情報については、「地理的一致ルールステートメント」を参照してください。
- 複数のルール間でロジックを再利用する – 複数のルールで同じロジックを再利用する必要がある場合は、ラベルを使用してそのロジックを単一のソースにして、結果をテストします。ネストされたルールステートメントの共通のサブセットを使用する複雑なルールが複数ある場合、複雑なルー

ル間で共通ルールセットを複製すると、時間がかかり、エラーが発生しやすくなります。ラベルを使用すると、一致するリクエストをカウントし、それらにラベルを追加する共通ルールサブセットを使用して新しいルールを作成できます。新しいルールを保護パック (ウェブ ACL) に追加して、元の複雑なルールの前に実行されるようにします。その後、元のルールで、共有ルールサブセットを、ラベルをチェックする単一のルールに置き換えます。

例えば、ログインパスにのみ適用する複数のルールがあるとします。各ルールで潜在的なログインパスと一致する同じロジックを指定するのではなく、そのロジックを含む 1 つの新しいルールを実装できます。新しいルールで、一致するリクエストにラベルを追加して、リクエストがログインパス上にあることを示します。保護パック (ウェブ ACL) で、この新しいルールの優先順位の数値設定を、元のルールの数値よりも小さく設定して、最初に実行されるようにします。その後、元のルールで、共有ロジックをラベルの存在のチェックに置き換えます。ジョブの優先順位の設定については、「ルールの優先度を設定する」を参照してください。

- ルールグループ内のルールに対する例外を作成する – このオプションは、表示または変更できないマネージドルールグループに特に役立ちます。多くのマネージドルールグループのルールはウェブリクエストにラベルを追加して一致したルールを示し、場合によってはその一致に関する追加情報を提供します。リクエストにラベルを追加するルールグループを使用すると、ルールグループのルールが一致をカウントするようにオーバーライドし、その後にルールグループラベルに基づいたウェブリクエストを処理するルールグループの後にルールを実行できます。すべての AWS マネージドルールは、一致するウェブリクエストにラベルを追加します。詳細については、「AWS マネージドルールのルールグループリスト」のルールの説明を参照してください。
- ラベルメトリクスの使用によるトラフィックパターンの監視 — ルールを使用して追加したラベルのメトリクスや、保護パック (ウェブ ACL) で使用するマネージドルールグループによって追加されたメトリクスのメトリクスにアクセスできます。 AWS マネージドルールのルールグループのすべては、評価するウェブリクエストにラベルを追加します。ラベルメトリクスとディメンションのリストについては、「ラベルメトリクスとディメンション」を参照してください。メトリクスとメトリクスの概要には、CloudWatch および AWS WAF コンソールの保護パック (ウェブ ACL) ページからアクセスできます。詳細については、「AWS WAF 保護のモニタリングと調整」を参照してください。
- 動的ラベル補間 – `${namespace:}`構文を使用して、カスタムリクエストヘッダー、カスタムレスポンスヘッダー、カスタムレスポンス本文の評価時にラベル値を解決できます。補間を使用する 1 つのルールは名前空間全体を対象とするため、ラベル値ごとに個別のルールは必要ありません。これは、Bot Control カテゴリなどのマネージドルールグループラベルをリクエストヘッダーとしてオリジンに転送する場合に便利です。詳細については、「動的ラベル補間」を参照してください。

でのラベル付けの仕組み AWS WAF

このセクションでは、 AWS WAF ラベルの仕組みについて説明します。

ルールがウェブリクエストに一致すると、ルールにラベルが定義されている場合、 はルール評価の最後にラベルをリクエスト AWS WAF に追加します。保護パック (ウェブ ACL) 内のルール一致後に評価されるルールは、ルールが追加したラベルと照合できます。

何によってリクエストにラベルが追加されるのか

リクエストを評価する保護パック (ウェブ ACL) コンポーネントは、リクエストにラベルを追加できます。

- ルールグループ参照ステートメントではないルールは、一致するウェブリクエストにラベルを追加できます。ラベル付け基準はルール定義の一部であり、ウェブリクエストがルールと一致すると、はルールのラベルをリクエスト AWS WAF に追加します。詳細については、「the section called “ラベルを追加するルール”」を参照してください。
- 地理照合ステートメントは、ステートメントの結果が一致するかどうかに関係なく、検査するすべてのリクエストに国と地域のラベルを追加します。詳細については、「the section called “地理的一致”」を参照してください。
- AWS WAF すべての AWS の管理ルールは、検査するリクエストにラベルを追加します。ルールグループ内のルールの一致に基づいてラベルを追加します。また、インテリジェントな脅威軽減ルールグループを使用すると追加されるトークンラベルなど、マネージドルールグループが使用する AWS プロセスに基づいてラベルを追加します。各マネージドルールグループが追加するラベルの詳細については、「the section called “AWS マネージドルールのルールグループリスト”」を参照してください。

がラベル AWS WAF を管理する方法

AWS WAF は、ルールによるリクエストの検査の最後に、ルールのラベルをリクエストに追加します。ラベル付けは、アクションと同様にルールの照合アクティビティの一部です。

保護パック (ウェブ ACL) 評価が終了した後、ラベルはウェブリクエストに保持されません。ルールが追加するラベルに照らして他のルールが照合するためには、ルールアクションが保護パック (ウェブ ACL) によるウェブリクエストの評価を終了してはなりません。ルールアクションは Count、CAPTCHA、Challenge に設定する必要があります。保護パック (ウェブ ACL) の評価が終了しない場合、保護パック (ウェブ ACL) 内の後続のルールは、リクエストに対してラベル一致基準を実行できます。ルールアクションの詳細については、「でのルールアクションの使用 AWS WAF」を参照してください。

保護パック (ウェブ ACL) 評価中のラベルにアクセスする

追加すると、 AWS WAF が保護パック (ウェブ ACL) に対してリクエストを評価する限り、ラベルはリクエストで使用できます。保護パック (ウェブ ACL) 内のすべてのルールは、同じ保護パック (ウェブ ACL) で既に実行されているルールによって追加されたラベルにアクセスできます。これには、保護パック (ウェブ ACL) 内で直接定義されたルールと、保護パック (ウェブ ACL) で使用されるルールグループ内の手以後されたルールが含まれます。

- ラベル一致ステートメントを使用してルールのリクエスト検査基準のラベルと照合できます。リクエストに添付されているどのラベルとも照合できます。ステートメントの詳細については、「ラベル一致ルールステートメント」を参照してください。
- 地理的照合ステートメントは、一致の有無にかかわらずラベルを追加しますが、ステートメントに含まれる保護パック (ウェブ ACL) ルールがリクエストの評価を完了して初めて使用できるようになります。
  - 論理 AND ステートメントなどの単一のルールを使用して、地理的ラベルに対して地域照合ステートメントの後にラベル照合チステートメントを実行することはできません。ラベル照合ステートメントは、地理的照合ステートメントを含むルールの後に実行される別のルールに記述する必要があります。
  - 地理的照合ステートメントをレートベースのルールステートメント、またはマネージドルールグループ参照ステートメント内のスコープダウンステートメントとして使用する場合、地理的照合ステートメントによって追加されたラベルは、包含ルールステートメントでは検査用に使用できません。レートベースのルールステートメントまたはルールグループの地理的ラベルを調べる必要がある場合は、事前に実行される別のルールで地理的照合ステートメントを実行する必要があります。

保護パック (ウェブ ACL) 評価対象外のラベル情報にアクセスする

保護パック (ウェブ ACL) 評価が終了した後、ラベルはウェブリクエストに保持されませんが、 AWS WAF はラベル情報を口グとメトリクスに記録します。

- AWS WAF は、1 つのリクエストで最初の 100 個のラベルの Amazon CloudWatch メトリクスを保存します。ラベルメトリクスへのアクセスの詳細については、「Amazon CloudWatch によるモニタリング」および「ラベルメトリクスとディメンション」を参照してください。
- AWS WAF は、 AWS WAF コンソールの保護パック (ウェブ ACL) トラフィック概要ダッシュボードの CloudWatch ラベルメトリクスを要約します。ダッシュボードにはどの保護パック (ウェブ ACL) ページからでもアクセスできます。詳細については、「保護パック (ウェブ ACL) のトラフィック概要ダッシュボード」を参照してください。

- AWS WAF は、リクエストの最初の 100 個のラベルのラベルをログに記録します。ルールアクションとともにラベルを使用して、 AWS WAF が記録するログをフィルタリングできます。詳細については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。

保護パック (ウェブ ACL) の評価では、ウェブリクエストに 100 個を超えるラベルを適用し、100 個を超えるラベルと照合できますが、ログとメトリクスには最初の 100 個 AWS WAF のみが記録されます。

でのラベル構文と命名要件 AWS WAF

このセクションでは、 AWS WAF ラベルを構築して照合する方法について説明します。

ラベルは、プレフィックス、オプションの名前空間、および名前で構成される文字列です。ラベルのコンポーネントはコロンで区切られます。ラベルには次の要件と特性があります。

- ラベルでは、大文字と小文字が区別されます。
- 各ラベル名前空間またはラベル名には、最大 128 文字を使用できます。
- ラベルには、最大 5 つの名前空間を指定できます。
- ラベルのコンポーネントはコロン (:) で区切られます。
- ラベルに指定する名前空間または名前で次の予約済み文字列を使用することはできません: `awswaf`、`aws`、`waf`、`rulegroup`、`webacl`、`regexpatternset`、`ipset`、および `managed`。

ラベル構文

完全修飾ラベルには、プレフィックス、オプションの名前空間、およびラベル名があります。プレフィックスは、ラベルを追加したルールのルールグループまたは保護パック (ウェブ ACL) コンテキストを識別します。名前空間は、ラベルのコンテキストを追加するために使用されることがあります。ラベル名は、ラベルの詳細レベルが最も低いレベルになります。多くの場合、リクエストにラベルを追加した特定のルールを示します。

ラベルのプレフィックスは、そのオリジンによって異なります。

- ラベル – 保護パック (ウェブ ACL) およびルールグループのルールで作成するラベルの完全なラベル構文を次に示します。エンティティタイプは `rulegroup` と `webacl` です。

```
awswaf:<entity owner account id>:<entity type>:<entity name>:<custom
 namespace>:...:<label name>
```

- ラベル名前空間プレフィックス: `awswaf:<entity owner account id>:<entity type>:<entity name>:`
- カスタム名前空間の追加: `<custom namespace>:…:`

ルールグループまたは保護パック (ウェブ ACL) でルールのラベルを定義する場合は、カスタム名前空間文字列とラベル名をコントロールします。残りは によって生成されます AWS WAF。 は、すべてのラベルに とアカウントawswafおよび保護パック (ウェブ ACL) またはルールグループのエンティティ設定 AWS WAF を自動的にプレフィックスします。

- マネージドルールグループのラベル – マネージドルールグループのルールによって作成されるラベルの完全なラベル構文を次に示します。

```
awswaf:managed:<vendor>:<rule group name>:<custom namespace>:...:<label name>
```

- ラベル名前空間プレフィックス: `awswaf:managed:<vendor>:<rule group name>:`
- カスタム名前空間の追加: `<custom namespace>:…:`

すべての AWS マネージドルールルールグループはラベルを追加します。マネージドルールグループの詳細については、「でのマネージドルールグループの使用 AWS WAF」を参照してください。

- 他の AWS プロセスのラベル – これらのプロセスは AWS マネージドルールルールグループによって使用されるため、マネージドルールグループを使用して評価するウェブリクエストに追加されます。マネージドルールグループによって呼び出されるプロセスが作成するラベルの完全なラベル構文を次に示します。

```
awswaf:managed:<process>:<custom namespace>:...:<label name>
```

- ラベル名前空間プレフィックス: `awswaf:managed:<process>:`
- カスタム名前空間の追加: `<custom namespace>:…:`

このタイプのラベルは、 AWS プロセスを呼び出すマネージドルールグループ用に一覧表示されます。マネージドルールグループの詳細については、「でのマネージドルールグループの使用 AWS WAF」を参照してください。

ルールの例にラベルを付ける

次のラベルの例は、アカウント 111122223333 に属する testRules という名前のルールグループのルールによって定義されています。

```
awswaf:111122223333:rulegroup:testRules:testNS1:testNS2:LabelNameA
```

```
awswaf:111122223333:rulegroup:testRules:testNS1:LabelNameQ
```

```
awswaf:111122223333:rulegroup:testRules:LabelNameZ
```

次のリストは、JSON のラベル指定の例を示しています。これらのラベル名には、末尾のラベル名の前にカスタム名前空間文字列が含まれます。

```
Rule: {
    Name: "label_rule",
    Statement: {...}
    RuleLabels: [
        Name: "header:encoding:utf8",
        Name: "header:user_agent:firefox"
    ],
    Action: { Count: {} }
}
```

> **Note**
>
> このタイプのリストには、ルール JSON エディタを通じてコンソールでアクセスできます。

前述のラベルの例と同じルールグループおよびアカウントで前述のルールを実行すると、結果として生じる完全修飾ラベルは次のようになります。

```
awswaf:111122223333:rulegroup:testRules:header:encoding:utf8
```

```
awswaf:111122223333:rulegroup:testRules:header:user_agent:firefox
```

マネージドルールグループのラベル例

マネージド AWS ルールのルールグループとプロセスから呼び出すラベルの例を次に示します。

```
awswaf:managed:aws:core-rule-set:NoUserAgent_Header
```

```
awswaf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments
```

```
awswaf:managed:aws:atp:aggregate:attribute:compromised_credentials
```

```
awswaf:managed:token:accepted
```

AWS WAF ラベルを追加する ルール

ほぼすべてのルールで、ラベルを定義し AWS WAF 、一致するリクエストに適用できます。

次のルールタイプが唯一の例外です。

- レートベースのルールは、レート制限中のみラベルを付与します – レートベースのルールは、特定の集計インスタンスが AWS WAFによってレート制限されている間のみ、ウェブリクエストにラベルを追加します。レートベースルールの詳細については、「でのレートベースのルールステートメントの使用 AWS WAF」を参照してください。
- ルールグループ参照ステートメントではラベル付けは許可されません – コンソールは、ルールグループステートメントまたはマネージドルールグループステートメントのラベルを受け付けません。API を使用して、いずれかのステートメントタイプのラベルを指定すると、検証例外が発生します。これらのステートメントのタイプについては、「でのマネージドルールグループステートメントの使用 AWS WAF」および「でのルールグループステートメントの使用 AWS WAF」を参照してください。

WCU – 保護パック (ウェブ ACL) またはルールグループのルールで定義する 5 つのラベルごとに 1 つの WCU。

ステートメントの場所

- コンソールのルールビルダー – ルールの [Action] (アクション) 設定の [Label] (ラベル) の下。
- API データタイプ – `Rule` `RuleLabels`

ルールでラベルを定義するには、ラベル名前空間プレフィックスに追加するカスタム名前空間文字列と名前を指定します。 は、ルールを定義するコンテキストからプレフィックス AWS WAF を取得し

ます。これについては、「でのラベル構文と命名要件 AWS WAF」の下のラベル構文情報を参照してください。

AWS WAF ラベルに一致する ルール

このセクションでは、ラベル一致ステートメントを使用して、ウェブリクエストラベルを評価する方法について説明します。ラベル名が必要な [Label] (ラベル)、または名前空間の指定が必要な [Namespace] (名前空間) と照合できます。ラベルまたは名前空間のいずれの場合も、オプションで、前述の名前空間とプレフィックスを指定に含めることができます。このステートメントタイプの一般的な情報については、「ラベル一致ルールステートメント」を参照してください。

ラベルのプレフィクスは、ラベルのルールが定義されているルールグループまたは保護パック (ウェブ ACL) のコンテキストを定義します。ルールのラベル一致ステートメントで、ラベルまたは名前空間一致文字列でプレフィックスが指定されていない場合、 はラベル一致ルールのプレフィックス AWS WAF を使用します。

- 保護パック (ウェブ ACL) 内で直接定義されたルールのラベルには、保護パック (ウェブ ACL) コンテキストを指定するプレフィックスが付いています。
- ルールグループ内にあるルールのラベルには、ルールグループコンテキストを指定するプレフィクスがあります。これは、独自のルールグループでも、マネージドルールグループでもかまいません。

これについては、「でのラベル構文と命名要件 AWS WAF」のラベル構文を参照してください。

> **Note**
>
> 一部のマネージドルールグループは、ラベルを追加します。`DescribeManagedRuleGroup` を呼び出すことにより、API を介してこれらを取得できます。ラベルは、応答の `AvailableLabels` プロパティにリストされています。

ルールのコンテキストとは異なるコンテキストにあるルールと照合する場合は、一致文字列にプレフィックスを指定する必要があります。例えば、マネージドルールグループのルールによって追加されたラベルと照合する場合は、一致文字列でルールグループのプレフィクスとその後に追加の一致基準が指定されるラベル一致ステートメントを使用して、保護パック (ウェブ ACL) にルールを追加できます。

ラベル一致ステートメントの一致文字列で、ラベルまたは名前空間のいずれかを指定します。

- ラベル – 一致のラベルの指定は、ラベルの終了部分で構成されます。ラベル名の直前に、連続するネームスペースをいくつでも含めて、その後に名前を含めることができます。指定の先頭をプレフィックスにして、完全修飾ラベルを指定することもできます。

  指定の例:

  - `testNS1:testNS2:LabelNameA`
  - `awswaf:managed:aws:managed-rule-set:testNS1:testNS2:LabelNameA`
- 名前空間 – 一致の名前空間の指定は、名前を除くラベルの指定の連続するサブセットで構成されます。プレフィックスを含めることができ、1 つ以上の名前空間文字列を含めることができます。

  指定の例:

  - `testNS1:testNS2:`
  - `awswaf:managed:aws:managed-rule-set:testNS1:`

AWS WAF ラベル一致の例

このセクションは、ラベル一致ルールステートメントの一致の指定の例を示します。

> **Note**
>
> これらの JSON リストは、ラベル一致指定を使用して保護パック (ウェブ ACL) にルールを追加し、ルールを編集して Rule JSON エディタに切り替えることでコンソールで作成されました。API またはコマンドラインインターフェイスを通じて、ルールグループまたは保護パック (ウェブ ACL) の JSON を取得することもできます。

トピック

- ローカルラベルと照合する
- 別のコンテキストのラベルと照合する
- マネージドルールグループラベルと照合する
- ローカル名前空間と照合する
- マネージドルールグループ名前空間と照合する

ローカルラベルと照合する

次の JSON リストは、このルールと同じコンテキストで、ウェブリクエストにローカルに追加されたラベルのラベル一致ステートメントを示しています。

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "header:encoding:utf8"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

アカウント 111122223333 でこの一致ステートメントを使用する場合、保護パック (ウェブ ACL) `testWebACL` のために定義するルールで、次のラベルと照合します。

```
awswaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

```
awswaf:111122223333:webacl:testWebACL:testNS1:testNS2:header:encoding:utf8
```

ラベル文字列が完全に一致しないため、次のラベルには一致しません。

```
awswaf:111122223333:webacl:testWebACL:header:encoding2:utf8
```

コンテキストが同じではないため、次のラベルには一致せず、したがってプレフィックスは一致しません。これは、ルールが定義されている保護パック (ウェブ ACL) `testWebACL` にルールグループ `productionRules` を追加した場合であっても当てはまります。

```
awswaf:111122223333:rulegroup:productionRules:header:encoding:utf8
```

別のコンテキストのラベルと照合する

次の JSON リストは、ユーザーが作成したルールグループ内のルールのラベルと照合するラベル一致ルールを示しています。名前が挙げられるルールグループに属さない保護パック (ウェブ ACL) で

実行されているすべてのルールの指定では、プレフィックスが必要です。このラベル指定の例では、正確なラベルのみと一致します。

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "awswaf:111122223333:rulegroup:testRules:header:encoding:utf8"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

マネージドルールグループラベルと照合する

これは、一致ルールのコンテキストとは別のコンテキストからのラベルとの一致の特殊なケースです。次の JSON リストは、マネージドルールグループラベルのラベル一致ステートメントを示しています。これは、ラベル一致ステートメントのキー設定で指定された正確なラベルのみと一致します。

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "awswaf:managed:aws:managed-rule-set:header:encoding:utf8"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

ローカル名前空間と照合する

次の JSON リストは、ローカル名前空間のラベル一致ステートメントを示しています。

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "NAMESPACE",
            Key: "header:encoding:"
        }
    },
    Labels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

ローカル Label 一致と同様に、アカウント 111122223333 でこのステートメントを使用する場合、保護パック (ウェブ ACL) testWebACL のために定義するルールで、次のラベルと照合します。

```
awswaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

アカウントが同じではないため、次のラベルには一致せず、したがってプレフィックスは一致しません。

```
awswaf:444455556666:webacl:testWebACL:header:encoding:utf8
```

プレフィックスは、次のようなマネージドルールグループによって適用されるラベルにも一致しません。

```
awswaf:managed:aws:managed-rule-set:header:encoding:utf8
```

マネージドルールグループ名前空間と照合する

次の JSON リストは、マネージドルールグループ名前空間のラベル一致ステートメントを示しています。所有しているルールグループの場合、ルールのコンテキスト外にある名前空間と照合するために、プレフィックスを指定する必要もあります。

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
```

```
            Scope: "NAMESPACE",
            Key: "awswaf:managed:aws:managed-rule-set:header:"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

この指定は、次のサンプルラベルと照合します。

```
awswaf:managed:aws:managed-rule-set:header:encoding:utf8
```

```
awswaf:managed:aws:managed-rule-set:header:encoding:unicode
```

次のラベルとは一致しません。

```
awswaf:managed:aws:managed-rule-set:query:badstring
```

でのインテリジェントな脅威の軽減 AWS WAF

このセクションでは、 が提供するマネージド型のインテリジェントな脅威軽減機能について説明します AWS WAF。これらは、悪意のあるボットやアカウント乗っ取りの試みなどの脅威から保護するために実装できる、高度で特殊な保護機能です。

> **Note**
>
> ここで説明する機能には、 の使用の基本料金を超える追加コストが発生します AWS WAF。詳細については、AWS WAF の料金を参照してください。

このセクションで提供されるガイダンスは、 AWS WAF ウェブ ACLs、およびルールグループの作成と管理の一般的な方法を知っているユーザーを対象としています。これらのトピックは、このガイドの前のセクションでカバーされています。

トピック

- でのインテリジェントな脅威軽減のオプション AWS WAF

- でのインテリジェントな脅威軽減のベストプラクティス AWS WAF
- AWS WAF インテリジェントな脅威の軽減におけるトークンの使用
- AWS WAF Fraud Control アカウント作成不正防止 (ACFP)
- AWS WAF Fraud Control アカウント乗っ取り防止 (ATP)
- AWS WAF ボットコントロール
- AWS WAF 分散サービス拒否 (DDoS) の防止
- でのクライアントアプリケーション統合 AWS WAF
- CAPTCHA および Challengeの AWS WAF

でのインテリジェントな脅威軽減のオプション AWS WAF

このセクションでは、インテリジェントな脅威の軽減を実装するためのオプションを詳細に比較します。

AWS WAF は、インテリジェントな脅威の軽減のために次のタイプの保護を提供します。

- AWS WAF Fraud Control Account Creation Fraud Prevention (ACFP) – アプリケーションのサインアップページで悪意のあるアカウント作成の試みを検出および管理します。コア機能は、ACFP マネージドルールグループによって提供されます。詳細については、「AWS WAF Fraud Control アカウント作成不正防止 (ACFP)」および「AWS WAF Fraud Control アカウント作成不正防止 (ACFP) ルールグループ」を参照してください。
- AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) – アプリケーションのログインページで悪意のある乗っ取りの試みを検出および管理します。コア機能は、ATP マネージドルールグループによって提供されます。詳細については、「AWS WAF Fraud Control アカウント乗っ取り防止 (ATP)」および「AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループ」を参照してください。
- AWS WAF Bot Control – フレンドリボットと悪意のあるボットの両方を識別、ラベル付け、管理します。この機能により、アプリケーション間で一意のシグネチャを持つ一般的なボットや、アプリケーション固有のシグネチャを持つターゲットしたボットを管理できます。コア機能は、Bot Control マネージドルールグループによって提供されます。詳細については、「AWS WAF ボットコントロール」および「AWS WAF Bot Control ルールグループ」を参照してください。
- クライアントアプリケーション統合 SDKs – ウェブページでクライアントセッションとエンドユーザーを検証し、クライアントがウェブリクエストで使用する AWS WAF トークンを取得します。ACFP、ATP、または Bot Control を使用する場合、可能であればクライアントアプリケーションにアプリケーション統合 SDK を実装し、ルールグループのすべての機能を最大限に活用し

てください。重大なリソースを迅速に保護する必要があり、SDK 統合に十分な時間がないときにのみ、一時的な対策として SDK を統合せずにこれらのルールグループを使用することをお勧めします。SDK を実装する情報については、「でのクライアントアプリケーション統合 AWS WAF」を参照してください。

- Challenge および CAPTCHAルールアクション – クライアントセッションとエンドユーザーを検証し、クライアントがウェブリクエストで使用する AWS WAF トークンを取得します。これらは、ルールアクションを指定する任意の場所、ルール内、使用するルールグループのオーバーライドとして実装できます。これらのアクションは AWS WAF JavaScript インタースティシャルを使用してクライアントまたはエンドユーザーを調査し、JavaScript をサポートするクライアントアプリケーションを必要とします。詳細については、「CAPTCHA および Challengeの AWS WAF」を参照してください。

インテリジェントな脅威軽減 AWS マネージドルールルールグループは、ACFP、ATP、および Bot Control のトークンを使用して高度な検出を行います。トークンがルールグループで有効にする機能については、「ACFP でのアプリケーション統合 SDK の使用」、「ATP でアプリケーション統合 SDK を使用」、「Bot Control のアプリケーション統合 SDK の使用」を参照してください。

インテリジェントな脅威軽減を実装するためのオプションは、チャレンジを実行し、トークン取得を強制するルールアクションの基本的な使用から、インテリジェントな脅威軽減 AWS マネージドルールルールグループが提供する高度な機能まで多岐にわたります。

次の表では、基本および高度な機能のオプションを詳細に比較します。

トピック

- チャレンジおよびトークン取得のオプション
- インテリジェントな脅威を軽減するマネージドルールグループのオプション
- レートベースのルールとターゲットを絞った Bot Control ルールにおけるレート制限のオプション

チャレンジおよびトークン取得のオプション

このセクションでは、チャレンジ管理オプションとトークン管理オプションを比較します。

AWS WAF アプリケーション統合 SDKsまたはルールアクション Challengeおよび を使用して、チャレンジを提供し、トークンを取得できますCAPTCHA。大まかに言うと、ルールアクションは実装がより簡単ですが、追加コストが発生してカスタマーエクスペリエンスへの悪影響が大きくなり、JavaScript が必要になります。SDK はクライアントアプリケーションでプログラミングする必要がありますが、より優れたカスタマーエクスペリエンスを提供できます。さらに無料で使用でき

て JavaScript で使用、あるいは Android または iOS アプリケーションで使用できます。アプリケーション統合 SDK は、次のセクションで説明する有料のインテリジェント脅威軽減のマネージドルールグループをいずれか 1 つ使用する保護パック (ウェブ ACL) でのみ使用できます。

チャレンジおよびトークン取得のオプション比較

	Challenge ルールアクション	CAPTCHA ルールアクション	JavaScript SDK チャレンジ	モバイル SDK チャレンジ
その内容とは	ブラウザクライアントにサイレントチャレンジインタースティシャルを提示することで AWS WAF トークンの取得を強制するルールアクション	クライアントエンドユーザーにビジュアルまたはオーディオチャレンジインタースティシャルを提示することで AWS WAF トークンの取得を強制するルールアクション	JavaScript を実行するクライアントブラウザおよびその他のデバイス向けのアプリケーション統合レイヤー。サイレントチャレンジをレンダリングし、トークンを取得します。	Android および iOS アプリケーション向けのアプリケーション統合レイヤー。サイレントチャレンジをネイティブにレンダリングし、トークンを取得します
こんなことにお勧めします	ボットセッションに対するサイレント検証および JavaScript をサポートするクライアントにトークン取得の強制	JavaScript をサポートするクライアントに、ボットセッションに対するエンドユーザーおよびサイレント検証、ならびにトークン取得の強制	ボットセッションに対するサイレント検証および JavaScript をサポートするクライアントにトークン取得の強制。 SDK はレイテンシーを最小限に抑え、アプリケーション内で実行されるチャレンジスクリプ	ボットセッションに対するサイレント検証および Android iOS のネイティブモバイルアプリケーションにトークン取得の強制。 SDK はレイテンシーを最小限に抑え、アプリケーション内で実行されるチャレンジスクリプ

	Challenge ルールアクション	CAPTCHA ルールアクション	JavaScript SDK チャレンジ	モバイル SDK チャレンジ
			トの場所を最適に制御します。	トの場所を最適に制御します。
実装の考慮事項	ルールアクション設定として実装済	ルールアクション設定として実装済	保護パック (ウェブ ACL) の ACFP、ATP、または Bot Control の有料ルールグループの 1 つが必要です。 クライアントアプリケーションでのコーディングが必要です。	保護パック (ウェブ ACL) の ACFP、ATP、または Bot Control の有料ルールグループの 1 つが必要です。 クライアントアプリケーションでのコーディングが必要です。
ランタイムの考慮事項	有効なトークンがないリクエストの侵入的なフロー。クライアントは AWS WAF チャレンジインタースティシャルにリダイレクトされます。ネットワークラウンドトリップを追加し、ウェブリクエストの 2 次評価が必要とします。	有効なトークンがないリクエストの侵入的なフロー。クライアントは AWS WAF CAPTCHA インタースティシャルにリダイレクトされます。ネットワークラウンドトリップを追加し、ウェブリクエストの 2 次評価が必要とします。	舞台裏で実行できます。チャレンジ体験をより広範囲に制御できます。	舞台裏で実行できます。チャレンジ体験をより広範囲に制御できます。
JavaScript が必要	はい	はい	あり	なし

	Challenge ルールアクション	CAPTCHA ルールアクション	JavaScript SDK チャレンジ	モバイル SDK チャレンジ
サポートされているクライアント	Javascript を実行するブラウザおよびデバイス	Javascript を実行するブラウザおよびデバイス	Javascript を実行するブラウザおよびデバイス	Android および iOS デバイス
単一ページアプリケーション (SPA) をサポート	強制適用のみ。 Challenge アクションを SDK と組み合わせて使用することで、リクエストが有効なチャレンジトークンを確実に持つようにできます。このルールアクションを使用してチャレンジスクリプトをページに配信することはできません。	強制適用のみ。 CAPTCHA アクションを SDK と組み合わせて使用することで、リクエストが有効な CAPTCHA トークンを確実に持つようにできます。このルールアクションを使用して CAPTCHA スクリプトをページに配信することはできません。	はい	該当なし
追加料金	はい。定義したルールまたは使用するルールグループのルールアクションのオーバーライドとして明示的に指定するアクション設定に適用されます。それ以外の場合は、いいえ。	はい。定義したルールまたは使用するルールグループのルールアクションのオーバーライドとして明示的に指定するアクション設定に適用されます。それ以外の場合は、いいえ。	いいえ。 ただし、ACFP、ATP、または Bot Control のいずれかの有料ルールグループが必要です。	いいえ。 ただし、ACFP、ATP、または Bot Control のいずれかの有料ルールグループが必要です。

これらのオプションに関連するコストの詳細については、「AWS WAF の料金表」のインテリジェントな脅威の軽減情報を参照してください。

Challenge または CAPTCHA アクションを含むルールを追加するだけで、チャレンジを実行して基本的なトークンの強制がより簡単にできます。アプリケーションコードにアクセスできない場合など、ルールアクションの使用が必要になる場合があります。

ただし、SDK を実装できれば、Challenge アクションを使用する場合と比較し、クライアントのウェブリクエストの保護パック (ウェブ ACL) 評価におけるコストを節約し、レイテンシーを低減できます。

- アプリケーションの任意の時点でチャレンジを実行するように SDK 実装を記述できます。保護されたリソースにウェブリクエストを送信するカスタマーアクションの前、トークンをバックグラウンドで取得できます。これにより、クライアントの最初のリクエストでトークンを送信できるようになります。
- 代わりに、Challenge アクションを含むルールを実装してトークンを取得する場合、クライアントが最初にリクエストを送信、ならびにトークンの有効期限が切れるとき、ルールおよびアクションに追加のウェブリクエスト評価と処理が必要になります。Challenge アクションは、有効期限が切れていない有効なトークンがないリクエストをブロックし、チャレンジインタースティシャルをクライアントに送り返します。クライアントがチャレンジの応答に成功した後、インタースティシャルは元のウェブリクエストを有効なトークンで再送信し、そのトークンが保護パック (ウェブ ACL) によって再度評価されます。

インテリジェントな脅威を軽減するマネージドルールグループのオプション

このセクションでは、マネージドルールグループのオプションを比較します。

インテリジェントな脅威軽減 AWS マネージドルールルールグループは、基本的なボットの管理、高度な悪意のあるボットの検出と緩和、アカウント乗っ取りの試みの検出と緩和、不正なアカウント作成の試みの検出と緩和を提供します。これらのルールグループは、前のセクションで説明したアプリケーション統合 SDK と組み合わせると、最も高度な保護およびクライアントアプリケーションとの安全な連携が可能になります。

マネージドルールのグループオプションの比較

	ACFP	ATP	Bot Control の共通レベル	Bot Control の目標レベル
その内容とは	アプリケーションの登録ページおよびサインアップページでのアカウントの不正な作成の試みの一環である可能性のあるリクエストを管理します。 ボットを管理しません。 「AWS WAF Fraud Control アカウント作成不正防止 (ACFP) ルールグループ」を参照してください。	アプリケーションのログインページで、悪意のある乗っ取りの試みの一部である可能性があるリクエストを管理します。 ボットを管理しません。 「AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループ」を参照してください。	アプリケーション間で一意のシグネチャで自己識別を行う一般的なボットを管理します。 「AWS WAF Bot Control ルールグループ」を参照してください。	アプリケーション固有のシグネチャで自己識別を行わないターゲットしたボットを管理します。 「AWS WAF Bot Control ルールグループ」を参照してください。
こんなことにお勧めします	ユーザー名トラバーサルによる作成の試みや、単一の IP アドレスから作成された多数の新しいアカウントなど、不正なアカウント作成攻撃がないかを確認するための、ア	パスワードトラバーサルによるログイン試行や同じ IP アドレスから多数のログイン試行など、アカウント乗っ取り攻撃におけるログイントラフィックの検査。トークンと	一般的な自動ボットトラフィックの基本的なボット保護およびラベル付け。	クライアントセッションレベルでのレート制限、ならびに Selenium や Puppeteer などのブラウザ自動化ツールの検出と軽減を含め、高度なボットに対するターゲ

	ACFP	ATP	Bot Control の共通レベル	Bot Control の目標レベル
	カウント作成トラフィックの検査。	併用すると、大量の失敗したログイン試行の IP およびクライアントセッションにおけるレート制限などの総合的な保護も提供されます。		ットを絞った保護。
評価結果を示すラベルを追加します	はい	はい	はい	はい
トークンラベルを追加します	はい	はい	はい	はい
有効なトークンがないリクエストのブロック	含まれません。 「有効な AWS WAF トークンを持たないリクエストのブロック」を参照してください。	含まれません。 「有効な AWS WAF トークンを持たないリクエストのブロック」を参照してください。	含まれません。 「有効な AWS WAF トークンを持たないリクエストのブロック」を参照してください。	トークンなしで 5 回のリクエストを送信するクライアントセッションをブロックします。
AWS WAF トークンが必要です `aws-waf-token`	すべてのルールで必須です。 「ACFP でのアプリケーション統合 SDK の使用」を参照してください。	多くのルールに必要です。 「ATP でアプリケーション統合 SDK を使用」を参照してください。	いいえ	はい

	ACFP	ATP	Bot Control の共通レベル	Bot Control の目標レベル
AWS WAF トークンを取得します。 `aws-waf-token`	はい。ルール `AllRequests` によって強制されます	いいえ	いいえ	トークンを取得する Challenge または CAPTCHA ルールアクションを使用するルールがあります。

これらのオプションに関連するコストの詳細については、「AWS WAF の料金表」のインテリジェントな脅威の軽減情報を参照してください。

アプリケーションが IP アドレスをローテーションし、ブラウザの動作を模倣するボットに直面した場合、一般的な保護レベルだけでは検出されません。これらのボットは自己識別を行わず、ターゲットを絞った保護が提供する動作分析と機械学習を必要としません。特定のアプリケーションに適した保護レベルを選択するガイダンスについては、「」を参照してくださいユースケースの Bot Control の選択と設定。

レートベースのルールとターゲットを絞った Bot Control ルールにおけるレート制限のオプション

このセクションでは、レートベースの緩和オプションを比較します。

AWS WAF Bot Control ルールグループのターゲットレベルと AWS WAF レートベースのルールステートメントの両方がウェブリクエストレート制限を提供します。以下の表は、これら 2 つのオプションを比較したものです。

レートベースの検出と緩和のためのオプションの比較

	AWS WAF レートベースのルール	AWS WAF Bot Control のターゲットルール	
レート制限の適用方法	レートが高すぎるリクエストのグループ	リクエストトークンの使用を通じて、人	

	AWS WAF レートベースのルール	AWS WAF Bot Control のターゲットルール	
	に対して動作します。Allow 以外のアクションを適用できます。	間のようなアクセスパターンを実施し、動的なレート制限を適用します。	
履歴的なトラフィックベースラインに基づく	いいえ	はい	
履歴的なトラフィックベースラインを蓄積するために要する時間	該当なし	動的しきい値の場合は 5 分。トークンがない場合は該当なし。	
軽減までの時間差	通常は 30 ~ 50 秒。最大で数分かかる場合もあります。	通常は 10 秒未満。最大で数分かかる場合もあります。	
緩和の対象	設定可能です。スコープダウンステートメントと、IP アドレス、HTTP メソッド、クエリ文字列などの 1 つ以上の集約キーを使用してリクエストをグループ化できます。	IP アドレスとクライアントセッション	
緩和をトリガーするために必要なトラフィック量のレベル	中 – 指定された時間枠で 10 リクエストまで設定できます	低 – 低速なスクレイパーなどのクライアントパターンを検出するためのもの	

	AWS WAF レートベースのルール	AWS WAF Bot Control のターゲットルール	
カスタマイズ可能なしきい値	はい	なし	
デフォルトの緩和アクション	コンソールのデフォルトは Block です。API にデフォルト設定はなく、設定が必要です。 これは、Allow 以外の任意の有効なルールアクションに設定できます。	ルールグループのルールアクション設定は、トークンがない場合には Challenge、単一のクライアントセッションからの大量のトラフィックの場合には CAPTCHA になります。 これらのルールのいずれかを、任意の有効なルールアクションに設定できます。	
高度に分散された攻撃に対する耐久性	中 – 単独で IP アドレスを制限する場合は最大 10,000 の IP アドレス	中程度 – IP アドレスとトークン間の合計で 50,000 個に制限されます	
AWS WAF 料金	の標準料金に含まれています AWS WAF。	Bot Control のインテリジェントな脅威軽減のターゲットレベル料金に含まれています。	
詳細情報	でのレートベースのルールステートメントの使用 AWS WAF	AWS WAF Bot Control ルールグループ	

でのインテリジェントな脅威軽減のベストプラクティス AWS WAF

インテリジェントな脅威の軽減機能の最も効果的でコスト効率性に優れた実装については、このセクションのベストプラクティスに従ってください。

- JavaScript とモバイルアプリケーション統合 SDK を実装する – アプリケーション統合を実装して、可能な限り最も効果的な方法で ACFP、ATP、または Bot Control 機能のすべて有効にします。マネージドルールグループは、SDK が提供するトークンを使用して、セッションレベルで正規のクライアントトラフィックを望ましくないトラフィックから分離させます。アプリケーション統合 SDK は、これらのトークンが常に利用可能であることを確実にします。詳細については、以下を参照してください。
  - ACFP でのアプリケーション統合 SDK の使用
  - ATP でアプリケーション統合 SDK を使用
  - Bot Control のアプリケーション統合 SDK の使用

  クライアントにチャレンジを実装したり、JavaScript の場合は CAPTCHA パズルがエンドユーザーに提示される方法をカスタマイズしたりするために、統合を使用します。詳細については、「でのクライアントアプリケーション統合 AWS WAF」を参照してください。

  JavaScript API を使用して CAPTCHA パズルをカスタマイズし、保護パック (ウェブ ACL) の任意の場所でCAPTCHAルールアクションを使用する場合は、 のクライアントで AWS WAF CAPTCHA レスポンスを処理するためのガイダンスに従ってくださいからの CAPTCHA レスポンスの処理 AWS WAF。このガイダンスは、ACFP マネージドルールグループや Bot Control マネージドルールグループのターゲットを絞った保護レベルなど、CAPTCHA アクションを使用するすべてのルールに適用されます。
- ACFP、ATP、Bot Control ルールグループに送信するリクエストを制限する – インテリジェントな脅威軽減 AWS マネージドルールルールグループの使用には追加料金が発生します。ACFP ルールグループは、指定したアカウント登録エンドポイントと作成エンドポイントに対するリクエストを検査します。ATP ルールグループは、指定したログインエンドポイントに対するリクエストを検査します。Bot Control ルールグループは、保護パック (ウェブ ACL) 評価で、到達するすべてのリクエストを検査します。

  これらのルールグループの使用を減らすため、以下のアプローチを検討してください。
  - マネージドルールグループステートメント内のスコープダウンステートメントを使用して、検査からリクエストを除外します。これは、ネスト可能なステートメントならどれでも実行できます。詳細については、「でのスコープダウンステートメントの使用 AWS WAF」を参照してください。

- ルールグループの前にルールを追加することで、検査からリクエストを除外します。スコープダウンステートメントで使用できないルール、およびラベル付けの後にラベルの照合が行われるような複雑な状況については、ルールグループの前に実行されるルールを追加する必要があるかもしれません。詳細については、「でのスコープダウンステートメントの使用 AWS WAF」および「でのルールステートメントの使用 AWS WAF」を参照してください。
- 低料金のルールを実行してからルールグループを実行します。何らかの理由でリクエストをブロックする他の標準 AWS WAF ルールがある場合は、これらの有料ルールグループの前に実行します。ルールとルール管理の詳細については、「でのルールステートメントの使用 AWS WAF」を参照してください。
- インテリジェントな脅威の軽減のためのマネージドルールグループを複数使用している場合は、Bot Control、ATP、ACFP の順に実行すると、コストを抑えることができます。

  料金の詳細については、「AWS WAF の料金表」を参照してください。

  Bot Control の前に安価なルール (IP 評価、ジオブロッキング) を配置して、より安価なルールでブロックされたリクエストが有料検査に到達しないようにすることもできます。コスト管理ガイダンスの詳細については、「」を参照してくださいのコスト管理。

- DDoS 対策ルールグループに送信するリクエストを制限しない – このルールグループは、明示的に許可していないすべてのウェブトラフィックをモニタリングするように設定する場合に最適です。ウェブ ACL に配置して、Allow ルールアクションを持つルールの後、および他のすべてのルールの前にのみ評価されるようにします。
- 分散型サービス拒否 (DDoS) の保護では、DDoS 対策または Shield Advanced のアプリケーションレイヤー DDoS 自動緩和を使用する – 他のインテリジェントな脅威の軽減ルールグループは DDoS 保護を提供しません。ACFP は、アプリケーションのサインアップページに対するアカウントの不正な作成の試みから保護します。ATP は、ログインページに対するアカウント乗っ取りの試みを防ぎます。Bot Control は、トークンとクライアントセッションに対する動的なレート制限を使用して、人間のようなアクセスパターンを実施することに重点を置いています。

  DDoS 対策を使用すると、DDoS 攻撃をモニタリングおよび制御できるため、脅威に迅速に対応して軽減できます。自動アプリケーションレイヤー DDoS 緩和機能を備えた Shield Advanced は、ユーザーに代わってカスタム AWS WAF 緩和を作成、評価、デプロイすることで、検出された DDoS 攻撃に自動的に応答します。

  Shield Advanced の詳細については、「AWS Shield Advanced の概要」および「AWS Shield Advanced および を使用したアプリケーションレイヤー (レイヤー 7) の保護 AWS WAF」を参照してください。

分散型サービス拒否 (DDoS) の防止の詳細については、「DDoS 対策ルールグループ」および「分散型サービス拒否 (DDoS) の防止」を参照してください。

- 通常のウェブトラフィック中に DDoS 対策ルールグループと Bot Control ルールグループのターゲットを絞った保護レベルを有効にする – これらのルールカテゴリには、通常のトラフィックのベースラインを確立する時間が必要です。

  通常のウェブトラフィック中に Bot Control ルールグループのターゲットを絞った保護レベルを有効にする – ターゲットを絞った保護レベルのルールの一部では、通常のトラフィックパターンのベースラインを確立してからでないと、不規則なトラフィックパターンや悪意のあるトラフィックパターンに対する認識と対応が行えません。例えば、`TGT_ML_*` ルールのウォームアップには最大 24 時間かかります。

  攻撃を受けていないときにこれらの保護を追加し、ルールが適切に対応することを期待する前に、トラフィックパターンのベースラインを確立するための猶予時間を与えます。攻撃中にこれらのルールを追加する場合は、カウントモードで DDoS 対策ルールグループを有効にする必要があります。攻撃が収まった後、ベースラインを確立するまでにかかる時間は通常の 2 倍から 3 倍になります。これは、攻撃トラフィックによって歪みが生じるためです。ルールとルールのウォームアップに必要な時間に関する詳細については、「ルールの一覧」を参照してください。

- 分散型サービス拒否 (DDoS) からの保護には、Shield Advanced のアプリケーションレイヤー DDoS 自動緩和を使用する – インテリジェントな脅威の軽減ルールグループは DDoS 保護を提供しません。ACFP は、アプリケーションのサインアップページに対するアカウントの不正な作成の試みから保護します。ATP は、ログインページに対するアカウント乗っ取りの試みを防ぎます。Bot Control は、トークンとクライアントセッションに対する動的なレート制限を使用して、人間のようなアクセスパターンを実施することに重点を置いています。

  自動アプリケーションレイヤー DDoS 緩和を有効にして Shield Advanced を使用すると、Shield Advanced はユーザーに代わってカスタム AWS WAF 緩和を作成、評価、デプロイすることで、検出された DDoS 攻撃に自動的に応答します。Shield Advanced の詳細については、「AWS Shield Advanced の概要」および「AWS Shield Advanced および を使用したアプリケーションレイヤー (レイヤー 7) の保護 AWS WAF」を参照してください。

- DDoS 対策ルールグループのベースラインを確立するときに本番トラフィック負荷を使用する – 人工テストトラフィックを使用して他のルールグループをテストするのが一般的です。ただし、DDoS 対策ルールグループのベースラインをテストして確立する場合は、本番環境の負荷を反映するトラフィックフローを使用することをお勧めします。一般的なトラフィックを使用して DDoS 対策ベースラインを確立することは、ルールグループが本番環境で有効になっているときにリソースを保護する最善の方法です。

- トークン処理を調整および設定する – 最高のユーザーエクスペリエンスが得られるように、保護パック (ウェブ ACL) のトークン処理を調整します。
  - 運用コストを削減し、エンドユーザーエクスペリエンスを改善するには、トークン管理のイミュニティ時間をセキュリティ要件が許容する最大時間に調整します。これにより、CAPTCHA パズルやサイレントチャレンジの使用を最小限に抑えることができます。詳細については、「でのタイムスタンプの有効期限とトークンイミュニティ時間の設定 AWS WAF」を参照してください。
  - 保護されたアプリケーション間でトークン共有を有効にするには、保護パック (ウェブ ACL) のトークンドメインリストを設定します。詳細については、「でのトークンドメインとドメインリストの指定 AWS WAF」を参照してください。
- 任意のホスト仕様を持つリクエストを拒否する – ウェブリクエストの `Host` ヘッダーがターゲットリソースに一致することを必須とするように保護対象リソースを設定します。ホストについて、1 つの値、または特定の値セット (`myExampleHost.com` および `www.myExampleHost.com` など) を受け入れることはできますが、任意の値は受け入れないでください。
- CloudFront ディストリビューションのオリジンである Application Load Balancer の場合、適切なトークン処理 AWS WAF のために CloudFront と を設定します – 保護パック (ウェブ ACL) を Application Load Balancer に関連付け、Application Load Balancer を CloudFront ディストリビューションのオリジンとしてデプロイする場合は、「」を参照してくださいCloudFront からの Application Load Balancers に必要な設定。
- デプロイ前にテストして調整する – 保護パック (ウェブ ACL) に変更を実装する前に、本ガイドのテストおよび調整手順に従って、期待通りの動作が得られることを確認してください。これらの有料機能を使用する場合は特に重要です。一般的なガイダンスについては、「AWS WAF 保護のテストとチューニング」を参照してください。有料マネージドルールグループ固有の情報については、「ACFP のテストとデプロイ」、「ATP のテストとデプロイ」、「AWS WAF Bot Control のテストとデプロイ」を参照してください。

AWS WAF インテリジェントな脅威の軽減におけるトークンの使用

このセクションでは、 AWS WAF トークンの動作について説明します。

AWS WAF トークンは、 AWS WAF インテリジェントな脅威の軽減によって提供される強化された保護の不可欠な部分です。トークンは、フィンガープリントとも呼ばれ、クライアントが保存し、送信するすべてのウェブリクエストに提供する単一のクライアントセッションに関する情報のコレクションです。 はトークン AWS WAF を使用して、悪意のあるクライアントセッションを 1 つの IP アドレスから発信した場合でも、正当なセッションから識別して分離します。トークンの使用による

コストは、正規ユーザーにとってはごくわずかですが、ボットネットにとってはかなり高額になります。

AWS WAF はトークンを使用して、アプリケーション統合 SDKs とルールアクション Challenge および によって提供されるブラウザおよびエンドユーザーチャレンジ機能をサポートします CAPTCHA。さらに、トークンは AWS WAF Bot Control とアカウント乗っ取り防止マネージドルールグループの機能を有効にします。

AWS WAF は、サイレントチャレンジや CAPTCHA パズルに正常に応答するクライアントのトークンを作成、更新、暗号化します。トークンを持つクライアントがウェブリクエストを送信すると、暗号化されたトークンが含まれ、トークンを AWS WAF 復号してその内容を検証します。

トピック

- がトークン AWS WAF を使用する方法
- AWS WAF トークンの特性
- でのタイムスタンプの有効期限とトークンイミュニティ時間の設定 AWS WAF
- でのトークンドメインとドメインリストの指定 AWS WAF
- のトークンラベルのタイプ AWS WAF
- 有効な AWS WAF トークンを持たないリクエストのブロック
- CloudFront からの Application Load Balancers に必要な設定

がトークン AWS WAF を使用する方法

このセクションでは、 がトークン AWS WAF を使用する方法について説明します。

AWS WAF はトークンを使用して、次のタイプのクライアントセッション検証を記録および検証します。

- CAPTCHA — CAPTCHA パズルは、ボットと人間のユーザーを区別するうえで役立ちます。CAPTCHA は CAPTCHA ルールアクションによってのみ実行されます。パズルの完了が成功すると、CAPTCHA スクリプトはトークンの CAPTCHA タイムスタンプを更新します。詳細については、「CAPTCHA および Challengeの AWS WAF」を参照してください。
- チャレンジ — 通常のクライアントセッションとボットセッションを区別しやすくし、ボットの運用コストを高めるために、チャレンジはサイレントで実行されます。チャレンジが正常に完了すると、チャレンジスクリプトは AWS WAF 必要に応じて から新しいトークンを自動的に取得し、トークンのチャレンジタイムスタンプを更新します。

AWS WAF は、次の状況でチャレンジを実行します。

- アプリケーション統合 SDK — アプリケーション統合 SDK は、クライアントアプリケーションセッション内で実行され、クライアントがチャレンジの応答に成功した後にのみログイン試行が許可されるようにします。詳細については、「でのクライアントアプリケーション統合 AWS WAF」を参照してください。
- Challenge ルールアクション – 詳細については、「CAPTCHA および Challengeの AWS WAF」を参照してください。
- CAPTCHA — CAPTCHA インタースティシャルを実行するときにクライアントがまだトークンを持っていない場合、スクリプトは最初に自動的にチャレンジを実行し、クライアントセッションを検証してトークンを初期化します。

トークンは、インテリジェントな脅威の AWS Managed Rules ルールグループの多くのルールで必要です。このルールは、セッションレベルでのクライアントの区別、ブラウザの特性の判断、アプリケーションウェブページにおける人間のインタラクティビティのレベルの理解などを行うためにトークンを使用します。これらのルールグループは AWS WAF トークン管理を呼び出し、ルールグループが検査するトークンのラベル付けを適用します。

- AWS WAF Fraud Control Account Creation Fraud Prevention (ACFP) – ACFP ルールには、有効なトークンを含むウェブリクエストが必要です。ルールの詳細については、「AWS WAF Fraud Control アカウント作成不正防止 (ACFP) ルールグループ」を参照してください。
- AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) – 大量のクライアントセッションや長時間のクライアントセッションを防ぐ ATP ルールには、有効期限が切れていないチャレンジタイムスタンプを持つ有効なトークンを持つウェブリクエストが必要です。詳細については、「AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループ」を参照してください。
- AWS WAF Bot Control – このルールグループのターゲットルールは、有効なトークンなしでクライアントが送信できるウェブリクエストの数を制限し、セッションレベルのモニタリングと管理にトークンセッション追跡を使用します。必要に応じて、ルールは Challenge および CAPTCHA ルールアクションを適用して、トークン取得および有効なクライアント動作を強制します。詳細については、「AWS WAF Bot Control ルールグループ」を参照してください。

AWS WAF トークンの特性

各トークンには次の特徴があります。

- トークンは、`aws-waf-token` という名前のクッキーに保存されます。

- トークンは暗号化されます。
- トークンは、次の情報を含む精度の高い識別子でクライアントセッションをフィンガープリントします。
  - クライアントがサイレントチャレンジに対して最後に成功した応答のタイムスタンプ。
  - エンドユーザーが CAPTCHA に対して最後に成功した応答のタイムスタンプ。これは保護機能で CAPTCHA を使用している場合にのみ表示されます。
  - 正規のクライアントを迷惑なトラフィックから切り離すうえで役立つクライアントおよびクライアント行動に関する追加情報。この情報には、自動化されたアクティビティを検出するために使用可能なさまざまなクライアント識別子およびクライアント側の信号が含まれます。収集される情報は一意ではなく、個別の人間を特定することはできません。
    - すべてのトークンには、オートメーションやブラウザ設定の不整合を示唆する要素など、クライアントブラウザの問い合わせから得られたデータが含まれています。この情報は、Challenge アクションによって実行されるスクリプトおよびクライアントアプリケーション SDK によって取得されます。スクリプトはブラウザに積極的に問い合わせて、結果をトークンに含めます。
    - さらに、クライアントアプリケーション統合 SDK を実装すると、トークンには、アプリケーションページとのエンドユーザーのインタラクティビティについて受動的に収集された情報が含まれます。インタラクティビティには、マウスの動き、キーの押下、およびページ上に存在する HTML フォームとのインタラクションが含まれます。この情報は、 AWS WAF がクライアントにおける人間のインタラクティビティのレベルを検出し、人間ではないように見えるユーザーにチャレンジを提示するのに役立ちます。クライアント側の統合については、「でのクライアントアプリケーション統合 AWS WAF」を参照してください。

セキュリティ上の理由から、 AWS トークンの内容の完全な説明や AWS WAF トークン暗号化プロセスに関する詳細情報は提供しません。

でのタイムスタンプの有効期限とトークンイミュニティ時間の設定 AWS WAF

このセクションでは、チャレンジと CAPTCHA タイムスタンプの有効期限について説明します。

AWS WAF はチャレンジと CAPTCHA イミュニティ時間を使用して、1 つのクライアントセッションにチャレンジまたは CAPTCHA を提示できる頻度を制御します。エンドユーザーが CAPTCHA に応答に成功した後、そのエンドユーザーに対して別の CAPTCHA が表示されない期間は、CAPTCHA イミュニティ時間によって決まります。同様に、チャレンジのイミュニティ時間は、チャレンジへの応答に成功した後、クライアントセッションが再度チャレンジを受けない期間を決定します。

AWS WAF トークンイミュニティ時間の仕組み

AWS WAF は、トークン内の対応するタイムスタンプを更新することで、チャレンジまたは CAPTCHA への正常な応答を記録します。がトークンにチャレンジまたは CAPTCHA がないか AWS WAF 検査すると、現在の時刻からタイムスタンプが減算されます。結果が設定されたイミュニティ時間よりも大きい場合、タイムスタンプは期限切れになります。

AWS WAF トークンイミュニティ時間の設定可能な側面

チャレンジおよび CAPTCHA のイミュニティ時間は、保護パック (ウェブ ACL) および CAPTCHA または Challenge ルールアクションを使用する任意のルールで設定できます。

- 両方のイミュニティ時間におけるデフォルトの保護パック (ウェブ ACL) 設定は 300 秒です。
- CAPTCHA または Challenge アクションを使用するすべてのルールにイミュニティ時間を指定できます。ルールにイミュニティ時間を指定しない場合、保護パック (ウェブ ACL) の設定が継承されます。
- CAPTCHA または Challenge アクションを使用するルールグループ内のルールには、ルールのイミュニティ時間を定義しない場合、ルールグループを使用する各保護パック (ウェブ ACL) から設定が継承されます。
- アプリケーション統合 SDK は、保護パック (ウェブ ACL) のチャレンジイミュニティ時間を使用します。
- チャレンジイミュニティ時間の最小値は 300 秒です。CAPTCHA イミュニティ時間の最小値は 60 秒です。両方のイミュニティ時間の最大値は 259,200 秒、または 3 日間です。

保護パック (ウェブ ACL) およびルールレベルのイミュニティ時間設定を使用して、CAPTCHA アクション、Challenge、SDK チャレンジ管理の動作を調整できます。たとえば、機密性の高いデータへのアクセスを制御するルールを低いイミュニティ時間で設定し、その後に保護パック (ウェブ ACL) 内で他のルールや SDK が承継するより高いイミュニティ時間を設定できます。

特に CAPTCHA の場合、パズルを解くことは顧客のウェブサイトエクスペリエンスを低下させる恐れがあるため、CAPTCHA のイミュニティ時間を調整すると必要な保護を提供し続けながら、顧客エクスペリエンスへの影響を軽減することに役立ちます。

Challenge および CAPTCHA ルールアクションを使用する際にイミュニティ時間の調整に関する詳細については、「CAPTCHA および Challenge アクションを使用するベストプラクティス」を参照してください。

AWS WAF トークンのイミュニティ時間を設定する場所

イミュニティ時間は、保護パック (ウェブ ACL) および Challenge や CAPTCHA ルールアクションを使用するルールで設定できます。

保護パック (ウェブ ACL) およびそのルールの管理に関する一般情報については、「でのウェブトラフィックメトリクスの表示 AWS WAF」を参照してください。

保護パック (ウェブ ACL) のイミュニティ時間を設定する場所

- コンソール — 保護パック (ウェブ ACL) を編集するとき、[Rules] (ルール) タブで、[保護パック (ウェブ ACL) の CAPTCHA 設定] および [保護パック (ウェブ ACL) のチャレンジ設定] ペインの設定を編集して変更します。コンソールでは、保護パック (ウェブ ACL) を作成した後にのみ、保護パック (ウェブ ACL) の CAPTCHA およびチャレンジのイミュニティ時間を設定できます。
- コンソールの外部 – 保護パック (ウェブ ACL) のデータタイプには CAPTCHA およびチャレンジの設定パラメータがあり、保護パック (ウェブ ACL) の作成および更新操作に設定して提供できます。

ルールのイミュニティ時間を設定する場所

- コンソール – ルールを作成または編集して CAPTCHA または Challenge アクションを指定すると、ルールのイミュニティ時間設定を変更できます。
- コンソールの外部 – ルールのデータタイプには CAPTCHA およびチャレンジの設定パラメータがあり、ルールを定義するときに設定できます。

でのトークンドメインとドメインリストの指定 AWS WAF

このセクションでは、 がトークンで AWS WAF 使用し、 がトークンで受け入れるドメインを設定する方法について説明します。

がクライアントのトークン AWS WAF を作成すると、トークンドメインで設定されます。 AWS WAF がウェブリクエスト内のトークンを検査するとき、そのドメインが保護パック (ウェブ ACL) で有効と見なされるドメインと一切一致しない場合、そのトークンは無効として拒否されます。

デフォルトでは、 は、ドメイン設定が保護パック (ウェブ ACL) に関連付けられているリソースのホストドメインと完全に一致するトークン AWS WAF のみを受け入れます。これはウェブリクエスト内の `Host` ヘッダーの値です。ブラウザでは、このドメインは JavaScript `window.location.hostname` プロパティ、ならびにユーザーのアドレスバーに表示されるアドレスに含まれます。

次のセクションで説明するように、保護パック (ウェブ ACL) 設定で許容されるトークンドメインを指定することもできます。この場合、 はホストヘッダーと完全一致とトークンドメインリストのドメインの両方 AWS WAF を受け入れます。

ドメインを設定するとき AWS WAF 、および保護パック (ウェブ ACL) でトークンを評価するときに使用する のトークンドメインを指定できます。指定するドメインには gov.au など、パブリックサフィックスを使用できません。使用できないドメインについては、「パブリックサフィックスリスト」のリスト (https://publicsuffix.org/list/public_suffix_list.dat) を参照してください。

AWS WAF 保護パック (ウェブ ACL) トークンドメインリスト設定

トークンドメインリストに AWS WAF 受け入れる追加のドメインを指定することで、複数の保護されたリソース間でトークンを共有するように保護パック (ウェブ ACL) を設定できます。トークンドメインリストを使用して、 AWS WAF はリソースのホストドメインを受け入れます。さらに、プレフィックス付きのサブドメインを含め、トークンドメインリスト内のすべてのドメインを受け入れます。

たとえば、トークンドメインリスト内のドメイン仕様 example.com は example.com (http://example.com/ から)、api.example.com (http://api.example.com/ から)、www.example.com (http://www.example.com/ から) と一致します。example.api.com (http://example.api.com/ から) または apiexample.com (http://apiexample.com/ から) と一致しません。

トークンドメインリストは、作成または編集するときに保護パック (ウェブ ACL) で設定できます。保護パック (ウェブ ACL) の管理に関する一般情報については、「でのウェブトラフィックメトリクスの表示 AWS WAF」を参照してください。

AWS WAF トークンドメイン設定

AWS WAF は、アプリケーション統合 SDKs と ChallengeおよびCAPTCHAルールアクションによって実行されるチャレンジスクリプトのリクエストでトークンを作成します。

がトークン AWS WAF に設定するドメインは、トークンをリクエストするチャレンジスクリプトのタイプと、指定した追加のトークンドメイン設定によって決まります。 AWS WAF は、トークンのドメインを、設定で確認できる最も短く、最も一般的な設定に設定します。

- JavaScript SDK — JavaScript SDK は、1 つ以上のドメインを含むことができるトークンドメイン仕様で構成できます。設定するドメインは、保護されたホストドメインと保護パック (ウェブ ACL) のトークンドメインリストに基づいて、 AWS WAF が受け入れるドメインである必要があります。

がクライアントのトークン AWS WAF を発行すると、ホストドメインと設定済みリスト内のドメインの中から、トークンドメインをホストドメインに一致する最短のトークンドメインに設定します。たとえば、ホストドメインが `api.example.com`で、トークンドメインリストに がある場合`example.com`、 はトークン`example.com`で AWS WAF を使用します。これは、ホストドメインと一致し、短いためです。JavaScript API 設定でトークンドメインリストを指定しない場合、 は保護されたリソースのホストドメインにドメイン AWS WAF を設定します。

詳細については、「トークンで使用するドメインの提供」を参照してください。

- モバイル SDK — アプリケーションコードでは、トークンドメインプロパティでモバイル SDK を設定する必要があります。このプロパティは、保護されたホストドメインおよび保護パック (ウェブ ACL) のトークンドメインリストに基づき、 AWS WAF が受け入れるドメインでなければなりません。

  がクライアントのトークン AWS WAF を発行する場合、このプロパティをトークンドメインとして使用します。 は、モバイル SDK AWS WAF クライアントに対して発行するトークンでホストドメインを使用しません。

  詳細については、「AWS WAF モバイル SDK 仕様」で `WAFConfiguration domainName` 設定を参照してください。
- Challenge アクション – 保護パック (ウェブ ACL) でトークンドメインリストを指定すると、 は、ホストドメインとリスト内のドメインの中から、 AWS WAF トークンドメインをホストドメインと一致するものに設定します。たとえば、ホストドメインが `api.example.com`で、トークンドメインリストに がある場合`example.com`、 はトークン`example.com`で AWS WAF を使用します。これは、ホストドメインと一致し、短いためです。保護パック (ウェブ ACL) にトークンドメインリストを指定しない場合、 は保護されたリソースのホストドメインにドメイン AWS WAF を設定します。

のトークンラベルのタイプ AWS WAF

このセクションでは、 AWS WAF トークン管理がウェブリクエストに追加するラベルについて説明します。ラベルの一般情報については、でのウェブリクエストのラベル付け AWS WAFを参照してください。

AWS WAF ボットまたは不正コントロールマネージドルールグループを使用する場合、ルールグループは AWS WAF トークン管理を使用してウェブリクエストトークンを検査し、リクエストにトークンラベルを適用します。マネージドルールグループの詳細については、「AWS WAF Fraud Control アカウント作成不正防止 (ACFP) ルールグループ」、「AWS WAF Fraud Control アカウント

乗っ取り防止 (ATP) ルールグループ」、「AWS WAF Bot Control ルールグループ」を参照してください。

> **Note**
>
> AWS WAF は、これらのインテリジェントな脅威軽減マネージドルールグループのいずれかを使用する場合にのみトークンラベルを適用します。

トークン管理では、以下のラベルをウェブリクエストに追加できます。

クライアントセッションラベル

ラベルには、 AWS WAF トークン管理がクライアントセッションを識別するために使用する一意の識別子`awswaf:managed:token:id:`*`identifier`*が含まれています。この識別子は、クライアントが使用していたトークンを破棄した後など、新しいトークンを取得すると変わる可能性があります。

> **Note**
>
> AWS WAF は、このラベルの Amazon CloudWatch メトリクスを報告しません。

ブラウザフィンガープリントラベル

ラベルには、 AWS WAF トークン管理がさまざまなクライアントブラウザシグナルから計算する堅牢なブラウザフィンガープリント識別子`awswaf:managed:token:fingerprint:`*`fingerprint-identifier`*が含まれています。この識別子は、複数のトークン取得の試行全体で同じままです。フィンガープリント識別子は、単一のクライアントに対して一意ではありません。

> **Note**
>
> AWS WAF は、このラベルの Amazon CloudWatch メトリクスを報告しません。

トークンステータスラベル: ラベル名前空間プレフィックス

トークンステータスラベルは、トークン、チャレンジのステータス、およびそれに含まれる CAPTCHA 情報を報告します。

各トークンステータスラベルは、次のプレフィクスの 1 つで始まります。

- awswaf:managed:token:— トークンの一般的なステータスを報告したり、トークンのチャレンジ情報のステータスを報告したりするために使用されます。
- awswaf:managed:captcha:— トークンの CAPTCHA 情報のステータスを報告するために使用されます。

トークンステータスラベル: ラベル名

プレフィックスに続いて、ラベルの残りの部分には詳細なトークンステータス情報が表示されます。

- accepted - リクエストトークンが存在し、以下の内容が含まれています。
  - 有効なチャレンジまたは CAPTCHA ソリューション。
  - 有効期限が切れていないチャレンジまたは CAPTCHA タイムスタンプ。
  - 保護パック (ウェブ ACL) に有効なドメイン仕様。

  例: ラベル awswaf:managed:token:accepted には、ウェブリクエストのトークンに有効なチャレンジソリューション、有効期限が切れていないチャレンジタイムスタンプ、および有効なドメインがあることが示されています。
- rejected - リクエストトークンは存在するが、承認基準を満たしていない。

  トークン管理では、拒否されたラベルに加えて、理由を示すカスタムラベル名前空間と名前が追加されます。
  - rejected:not_solved — トークンにチャレンジまたは CAPTCHA ソリューションがない。
  - rejected:expired — 保護パック (ウェブ ACL) に設定されているトークンイミュニティ時間によると、トークンのチャレンジまたは CAPTCHA タイムスタンプの有効期限が切れている。
  - rejected:domain_mismatch — トークンのドメインが、保護パック (ウェブ ACL) のトークンドメイン設定と一致しない。
  - rejected:invalid – 指定されたトークンを読み取ることが AWS WAF できませんでした。

  例: ラベル awswaf:managed:captcha:rejected と awswaf:managed:captcha:rejected:expired とともに、トークンの CAPTCHA タイムスタンプがウェブ ACL で設定されている CAPTCHA トークンのイミュニティ時間を超えたために、リクエストには有効な CAPTCHA 解決がなかったことが示されています。
- absent — リクエストにトークンがないか、トークンマネージャーがそれを読み取れなかった。

  例: ラベル awswaf:managed:captcha:absent には、リクエストにトークンがないことが示されています。

有効な AWS WAF トークンを持たないリクエストのブロック

このセクションでは、 AWS WAF モバイル SDK の使用時にトークンが欠落しているログインリクエストをブロックする方法について説明します。

インテリジェントな脅威の AWS Managed Rules ルールグループ `AWSManagedRulesACFPRuleSet`、`AWSManagedRulesATPRuleSet`、および を使用するとAWSManagedRulesBotControlRuleSet、ルールグループは AWS WAF トークン管理を呼び出してウェブリクエストトークンのステータスを評価し、それに応じてリクエストにラベルを付けます。

> **Note**
>
> トークンのラベル付けは、これらのマネージドルールグループのいずれかを使用して評価したウェブリクエストにのみ適用されます。

適用されるトークン管理のラベル付けについては、前述の「のトークンラベルのタイプ AWS WAF」セクションを参照してください。

その後、インテリジェントな脅威軽減マネージドルールグループは、トークンの要件を次のように処理します。

- `AWSManagedRulesACFPRuleSet` `AllRequests` ルールは、すべてのリクエストに対して Challenge アクションを実行するように設定されており、`accepted` トークンラベルのないリクエストは効果的にブロックされます。
- `AWSManagedRulesATPRuleSet` は、`rejected` トークンラベルを持つリクエストをブロックしますが、`absent` トークンラベルを持つリクエストはブロックしません。
- `accepted`トークンラベルなしでリクエストを 5 回送信すると、`AWSManagedRulesBotControlRuleSet` のターゲットを絞った保護レベルが、クライアントにチャレンジを送信します。有効なトークンを持たない個別のリクエストはブロックされません。ルールグループの共通の保護レベルでは、トークンの要件は管理されません。

インテリジェントな脅威ルールグループの詳細については、「AWS WAF Fraud Control アカウント作成不正防止 (ACFP) ルールグループ」、「AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループ」、および「AWS WAF Bot Control ルールグループ」を参照してください。

Bot Control または ATP マネージドルールグループの使用時にトークンを持たないリクエストをブロックするには

Bot Control と ATP ルールグループを使用すると、有効なトークンを持たないリクエストがルールグループの評価を終了し、保護パック (ウェブ ACL) によって引き続き評価される可能性があります。

トークンが不足しているリクエスト、あるいはトークンが拒否されたリクエストをすべてブロックするには、マネージドルールグループの直後に実行するルールを追加し、ルールグループがユーザーに代わって処理しないリクエストをキャプチャしてブロックします。

次の内容では、ATP マネージドルールグループを使用する保護パック (ウェブ ACL) の JSON リストの例を示します。保護パック (ウェブ ACL) には、`awswaf:managed:token:absent` ラベルをキャプチャして処理するルールが追加されています。このルールは、ATP ルールグループの範囲に合わせて、ログインエンドポイントに送信されるウェブリクエストに評価を絞り込みます。追加されたルールは太字で表示されます。

```
{
  "Name": "exampleWebACL",
  "Id": "55555555-6666-7777-8888-999999999999",
  "ARN": "arn:aws:wafv2:us-east-1:111111111111:regional/webacl/
exampleWebACL/55555555-4444-3333-2222-111111111111",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesATPRuleSet",
      "Priority": 1,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesATPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesATPRuleSet": {
                "LoginPath": "/web/login",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
```

```
                "PasswordField": {
                  "Identifier": "/form/password"
                }
              },
              "ResponseInspection": {
                "StatusCode": {
                  "SuccessCodes": [
                    200
                  ],
                  "FailureCodes": [
                    401,
                    403,
                    500
                  ]
                }
              }
            }
          }
        ]
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSManagedRulesATPRuleSet"
    }
  },
  {
    "Name": "RequireTokenForLogins",
    "Priority": 2,
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:token:absent"
              }
            }
          },
```

```
            {
              "ByteMatchStatement": {
                "SearchString": "/web/login",
                "FieldToMatch": {
                  "UriPath": {}
                },
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                 }
                ],
                "PositionalConstraint": "STARTS_WITH"
              }
            },
            {
              "ByteMatchStatement": {
                "SearchString": "POST",
                "FieldToMatch": {
                  "Method": {}
                },
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ],
                "PositionalConstraint": "EXACTLY"
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "RequireTokenForLogins"
      }
    }
  ],
  "VisibilityConfig": {
```

```
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "exampleWebACL"
  },
  "Capacity": 51,
  "ManagedByFirewallManager": false,
  "RetrofittedByFirewallManager": false,
  "LabelNamespace": "awswaf:111111111111:webacl:exampleWebACL:"
}
```

CloudFront からの Application Load Balancers に必要な設定

保護パック (ウェブ ACL) を Application Load Balancer に関連付けし、その Application Load Balancer を CloudFront ディストリビューションのオリジンとしてデプロイする場合、このセクションをお読みください。

このアーキテクチャでは、トークン情報が正しく処理されるには、次の追加設定を行う必要があります。

- `aws-waf-token` クッキーを Application Load Balancer に転送するように CloudFront を設定します。デフォルトでは、CloudFront はウェブリクエストをオリジンに転送する前にクッキーを削除します。トークンクッキーをウェブリクエストに含めるには、トークンキッキーのみまたはすべてのクッキーを含むように CloudFront キャッシュ動作を設定します。これを行う方法の情報については、「Amazon CloudFront デベロッパーガイド」の「クッキーに基づくコンテンツのキャッシュ」を参照してください。
- CloudFront ディストリビューションのドメインを有効なトークンドメインとして認識 AWS WAF するように を設定します。デフォルトでは、CloudFront は `Host`ヘッダーを Application Load Balancer オリジンに設定し、保護されたリソースのドメイン AWS WAF として使用します。ただし、クライアントブラウザは CloudFront ディストリビューションをホストドメインとして見なし、クライアント用に生成されたトークンは CloudFront ドメインをトークンドメインとして使用します。追加の設定がない場合、 が保護されたリソースドメインをトークンドメインと AWS WAF 照合すると、不一致が発生します。これを修正するには、CloudFront ディストリビューションのドメイン名を保護パック (ウェブ ACL) 設定のトークンドメインリストに追加します。これを行う方法については、「AWS WAF 保護パック (ウェブ ACL) トークンドメインリスト設定」を参照してください。

AWS WAF Fraud Control アカウント作成不正防止 (ACFP)

このセクションでは、 AWS WAF Fraud Control アカウント作成不正防止 (ACFP) の機能について説明します。

アカウント作成の不正行為は、攻撃者が 1 つ以上の偽のアカウントの作成を試みるオンライン上の違法行為です。攻撃者は、プロモーションやサインアップボーナスの濫用、なりすまし、フィッシングなどのサイバー攻撃などの不正行為のために偽のアカウントを使用します。偽のアカウントの存在は、顧客からの評判に傷をつけたり、金銭的な被害を伴う不正行為のリスクを生じさせたりするものであり、ビジネスに悪影響を及ぼす可能性があります。

ACFP 機能を実装することで、アカウント作成の不正試行をモニタリングおよび制御できます。この機能は、コンパニオンアプリケーション統合 SDKs `AWSManagedRulesACFPRuleSet`を備えた AWS Managed Rules ルールグループで AWS WAF 提供されます。

ACFP マネージドルールグループは、悪意のあるアカウント作成の試みの一部である可能性があるリクエストにラベルを付けて管理します。ルールグループは、クライアントでアプリケーションのアカウントサインアップエンドポイントに送信するアカウント作成の試みを検査することでこれを行います。

ACFP は、アカウントのサインアップリクエストをモニタリングして異常なアクティビティがないかを確認し、疑わしいリクエストを自動的にブロックすることで、アカウントサインアップページを保護します。ルールグループは、リクエスト ID、行動分析、機械学習を使用して不正なリクエストを検出します。

- 検査のリクエスト– ACFP を使用すると、アカウントの異常な作成の試みや、盗まれた認証情報を使用する試みを可視化して制御でき、不正なアカウントの作成を防止できます。ACFP は、盗まれた認証情報のデータベースに照らして E メールとパスワードの組み合わせをチェックします。このデータベースは、漏えいされた認証情報がダークウェブ上で新しく見つかると定期的に更新されます。ACFP は、メールアドレスで使用されているドメインを評価し、電話番号や住所のフィールドの使用をモニタリングして、エントリを検証するとともに、不正行為を検出します。ACFP は、IP アドレスやクライアントセッションごとにデータを集約し、不審なリクエストを大量に送信するクライアントを検出してブロックします。
- レスポンス検査 – CloudFront ディストリビューションの場合、ACFP ルールグループは、受信したアカウント作成リクエストを検査するだけでなく、アカウント作成の試みに対するアプリケーションのレスポンスも検査して、成功率と失敗率を追跡します。この情報を使用して、ACFP は失敗した試行回数が過度に多いクライアントセッションまたは IP アドレスを一時的にブロックできます。 AWS WAF は、レスポンス検査を非同期で実行するため、ウェブトラフィックのレイテンシーが大きくなることはありません。

> **Note**
>
> このマネージドルールグループを使用する場合、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

> **Note**
>
> ACFP 機能は、Amazon Cognito ユーザープールでは使用できません。

トピック

- AWS WAF ACFP コンポーネント
- ACFP でのアプリケーション統合 SDK の使用
- ACFP マネージドルールグループをウェブ ACL に追加
- ACFP のテストとデプロイ
- AWS WAF Fraud Control アカウント作成不正防止 (ACFP) の例

AWS WAF ACFP コンポーネント

AWS WAF Fraud Control Account Creation Fraud Prevention (ACFP) の主なコンポーネントは次のとおりです。

- **`AWSManagedRulesACFPRuleSet`** – この AWS マネージドルールルールグループのルールは、さまざまなタイプの不正なアカウント作成アクティビティを検出、ラベル付け、処理します。ルールグループは、指定されたアカウント登録エンドポイントにクライアントが送信する HTTP GET テキスト/HTML リクエストと、指定されたアカウントサインアップエンドポイントにクライアントが送信する POST ウェブリクエストを検査します。保護された CloudFront ディストリビューションでは、ルールグループはディストリビューションがアカウント作成リクエストに送り返すレスポンスも検査します。このルールグループのルールのリストについては、「AWS WAF Fraud Control アカウント作成不正防止 (ACFP) ルールグループ」を参照してください。マネージドルールグループ参照ステートメントを使用して、このルールグループを保護パック (ウェブ ACL) に含めます。このルールグループの使用については、「ACFP マネージドルールグループをウェブ ACL に追加」を参照してください。

> **Note**
>
> このマネージドルールグループを使用する場合、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

- アプリケーションのアカウント登録ページと作成ページに関する詳細 – 保護パック (ウェブ ACL) に `AWSManagedRulesACFPRuleSet` ルールグループを追加する際には、アカウント登録ページと作成ページに関する情報を提供する必要があります。これにより、ルールグループは検査するリクエストの範囲を絞り込み、アカウント作成ウェブリクエストを適切に検証できます。登録ページは `GET` テキスト/HTML リクエストを受け入れる必要があります。アカウント作成パスは `POST` リクエストを受け入れる必要があります。ACFP ルールグループは、電子メール形式のユーザー名に対応します。詳細については、「ACFP マネージドルールグループをウェブ ACL に追加」を参照してください。
- (保護された CloudFront ディストリビューションの場合) アカウント作成の試みに対するアプリケーションのレスポンスに関する詳細 – アカウント作成の試みに対するアプリケーションのレスポンスに関する詳細を提供すると、ACFP ルールグループは、単一の IP アドレスまたは単一のクライアントセッションからのアカウントの一括作成の試みを追跡および管理します。このオプションの設定については、「ACFP マネージドルールグループをウェブ ACL に追加」を参照してください。
- JavaScript とモバイルアプリケーションの統合 SDKs – ACFP 実装で AWS WAF JavaScript とモバイル SDKs を実装して、ルールグループが提供する機能の完全なセットを有効にします。ACFP ルールの多くは、セッションレベルのクライアント検証および動作集約に SDK から提供された情報を使用し、正規のクライアントトラフィックをボットトラフィックから分離するために必要です。SDK の詳細については、「でのクライアントアプリケーション統合 AWS WAF」を参照してください。

ACFP 実装を次と組み合わせて、保護のモニタリング、チューニング、およびカスタマイズに役立てることができます。

- ログ記録とメトリクス – 保護パック (ウェブ ACL) 用にログ、Amazon Security Lake データ収集と　Amazon CloudWatch メトリクスを設定して有効にすることで、トラフィックをモニタリングし、ACFP マネージドルールグループがトラフィックにどのように影響するのかを理解できます。`AWSManagedRulesACFPRuleSet` がウェブリクエストに追加するラベルは、データに含まれます。オプションの詳細については、ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック、Amazon CloudWatch によるモニタリング、及び「What is Amazon Security Lake?」を参照してください。

ニーズと確認できるトラフィックに応じて、AWSManagedRulesACFPRuleSet の実装をカスタマイズできます。例えば、ACFP 評価から一部のトラフィックを除外したり、スコープダウンステートメントやラベルマッチングルールなどの AWS WAF 機能を使用して、識別したアカウント作成の不正試行の処理方法を変更したりできます。

- ラベルとラベル一致ルール – AWSManagedRulesACFPRuleSet のどのルールでも、ブロック動作をカウントに切り替えて、ルールによって追加されたラベルと照合することができます。このアプローチを使用し、ACFP マネージドルールグループによって識別されるウェブリクエストの処理方法をカスタマイズします。ラベル付けおよびラベル一致ステートメントの使用の詳細については、「ラベル一致ルールステートメント」および「でのウェブリクエストのラベル付け AWS WAF」を参照してください。
- カスタムリクエストとレスポンス - 許可するリクエストにはカスタムヘッダーを追加し、ブロックするリクエストにはカスタムレスポンスを送信できます。これを行うには、ラベル一致を AWS WAF カスタムリクエストおよび応答機能とペアリングします。リクエストとレスポンスをカスタマイズする方法については、「でカスタマイズされたウェブリクエストとレスポンス AWS WAF」を参照してください。

ACFP でのアプリケーション統合 SDK の使用

ACFP ルールグループを最も効率的に使用するためにも、アプリケーション統合 SDK を実装することを強くお勧めします。

- 完全なルールグループ機能 – ACFP ルール SignalClientHumanInteractivityAbsentLow は、アプリケーション統合によって情報が提供されたトークンでのみ機能します。このルールは、アプリケーションページに対する人間の異常なインタラクションを検出および管理します。アプリケーション統合 SDK は、マウスの動き、キーの押下、その他の測定を通じて、人間の通常のインタラクティビティを検出できます。ルールアクション CAPTCHA および Challenge によって送信されるインタースティシャルは、このタイプのデータを提供できません。
- レイテンシーの短縮 – ルールグループのルール AllRequests は、チャレンジトークンをまだ持っていないリクエストに Challenge ルールアクションを適用します。これが発生すると、リクエストはルールグループによって 2 回評価されます。1 回目の評価はトークンなしで実行され、2 回目の評価は Challenge アクションインタースティシャルによってトークンが取得された後に実行されます。AllRequests ルールを使用するだけであれば追加料金は発生しませんが、このアプローチではウェブトラフィックに対するオーバーヘッドが大きくなり、エンドユーザーエクスペリエンスのレイテンシーが長くなります。アプリケーション統合を使用してクライアント側でトーク

ンを取得する場合、アカウント作成リクエストを送信する前に、ACFP ルールグループがリクエストを 1 回評価します。

ルールグループ機能の情報については、「AWS WAF Fraud Control アカウント作成不正防止 (ACFP) ルールグループ」を参照してください。

SDK の詳細については、「でのクライアントアプリケーション統合 AWS WAF」を参照してください。 AWS WAF トークンの詳細については、「」を参照してくださいAWS WAF インテリジェントな脅威の軽減におけるトークンの使用。ルールアクションの情報については、「CAPTCHA および Challengeの AWS WAF」を参照してください。

ACFP マネージドルールグループをウェブ ACL に追加

このセクションでは、AWSManagedRulesACFPRuleSet ルールグループを追加および設定する方法について説明します。

ウェブトラフィックのアカウントの不正な作成アクティビティを認識するように ACFP マネージドルールグループを設定するには、クライアントが登録ページにアクセスする方法、およびアプリケーションにアカウント作成リクエストを送信する方法に関する情報を入力します。保護された Amazon CloudFront ディストリビューションでは、アカウント作成リクエストに対するアプリケーションの応答方法に関する情報も指定します。この設定は、マネージドルールグループの通常の設定に追加されます。

ルールグループの説明とルールリストについては、「AWS WAF Fraud Control アカウント作成不正防止 (ACFP) ルールグループ」を参照してください。

> **Note**
>
> 盗まれた認証情報の ACFP データベースには、E メール形式のユーザー名のみが含まれています。

このガイダンスは、 AWS WAF 保護パック (ウェブ ACL)、ルール、およびルールグループを作成および管理する方法を一般的に認識しているユーザーを対象としています。これらのトピックは、このガイドの前のセクションでカバーされています。マネージドルールグループを保護パック (ウェブ ACL) に追加する方法の基本については、「コンソールを通じた保護パック (ウェブ ACL) へのマネージドルールグループの追加」を参照してください。

ベストプラクティスに従う

ACFP ルールグループは、「でのインテリジェントな脅威軽減のベストプラクティス AWS WAF」に記載されているベストプラクティスに従って使用してください。

保護パック (ウェブ ACL) で **AWSManagedRulesACFPRuleSet** ルールグループを使用するには

1. AWS マネージドルールグループを保護パック (ウェブ ACL) `AWSManagedRulesACFPRuleSet`に追加し、保存する前にルールグループ設定を編集します。

   > **Note**
   >
   > このマネージドルールグループを使用する場合、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

2. [ルールグループを設定] ペインで、ACFP ルールグループがアカウント作成リクエストの検査に使用する情報を入力します。

   a. 「パスで正規表現を使用する」で、登録およびアカウント作成ページのパス仕様に対して正規表現マッチング AWS WAF を実行する場合は、これをオンに切り替えます。

      AWS WAF は、いくつかの例外`libpcre`を除いて、PCRE ライブラリで使用されるパターン構文をサポートします。ライブラリは、「PCRE - Perl Compatible Regular Expressions」で文書化されています。 AWS WAF サポートの詳細については、「」を参照してくださいでサポートされている正規表現構文 AWS WAF。

   b. [登録ページのパス] で、アプリケーションの登録ページのエンドポイントのパスを指定します。このページは `GET` テキスト/HTML リクエストを受け入れる必要があります。ルールグループは、指定された登録ページのエンドポイントに対する HTTP `GET` テキスト/HTML リクエストのみを検査します。

      > **Note**
      >
      > エンドポイントの照会では大文字と小文字が区別されません。正規表現の仕様には、大文字と小文字を区別しない照合を無効にするフラグ (`?-i`) を含めてはいけません。文字列の指定はフォワードスラッシュ「`/`」で始まる必要があります。

      例えば、URL `https://example.com/web/registration` では、文字列パスの指定「`/web/registration`」を指定できます。指定したパスで始まる登録ページのパスは一致とみなされます。例えば、`/web/registration` は登録パス `/web/registration`、`/`

web/registration/、/web/registrationPage、および /web/registration/thisPage に一致しますが、パス /home/web/registration または /website/registration には一致しません。

> **Note**
>
> エンドユーザーがアカウント作成リクエストを送信する前に、登録ページをロードするようにします。これは、クライアントからのアカウント作成リクエストに、有効なトークンが確実に含まれているようにするのに役立ちます。

c. [アカウント作成パス]には、入力済みの新規ユーザー情報を受け入れるウェブサイトの URI を指定します。この URI は POST リクエストを受け入れる必要があります。

> **Note**
>
> エンドポイントの照会では大文字と小文字が区別されません。正規表現の仕様には、大文字と小文字を区別しない照合を無効にするフラグ (?-i) を含めてはいけません。文字列の指定はフォワードスラッシュ「/」で始まる必要があります。

例えば、URL https://example.com/web/newaccount では、文字列パスの指定「/web/newaccount」を指定できます。指定したパスで始まるアカウント作成パスは一致とみなされます。例えば、/web/newaccount はアカウント作成パス /web/newaccount、/web/newaccount/、/web/newaccountPage、および /web/newaccount/thisPage に一致しますが、パス /home/web/newaccount または /website/newaccount には一致しません。

d. [リクエスト検査] で、リクエストのペイロードタイプと、ユーザー名、パスワード、他のアカウント作成の詳細が指定されているリクエスト本文内のフィールドの名前を指定して、アプリケーションがアカウント作成の試みを受け入れる方法を指定します。

> **Note**
>
> 主な住所フィールドと電話番号フィールドについては、リクエストペイロードに表示される順にフィールドを指定します。

これらのフィールド名の指定は、ペイロードタイプによって異なります。

- JSON ペイロードタイプ – JSON Pointer 構文でフィールド名を指定します。JSON Pointer 構文の詳細については、インターネットエンジニアリングタスクフォース (IETF) ドキュメントの「JavaScript Object Notation (JSON) Pointer」を参照してください。

  例えば、次の JSON ペイロードの例では、ユーザー名フィールドの仕様は `/signupform/username` で、主な住所フィールドの仕様は `/signupform/addrp1`、`/signupform/addrp2`、および `/signupform/addrp3` です。

```
{
    "signupform": {
        "username": "THE_USERNAME",
        "password": "THE_PASSWORD",
        "addrp1": "PRIMARY_ADDRESS_LINE_1",
        "addrp2": "PRIMARY_ADDRESS_LINE_2",
        "addrp3": "PRIMARY_ADDRESS_LINE_3",
        "phonepcode": "PRIMARY_PHONE_CODE",
        "phonepnumber": "PRIMARY_PHONE_NUMBER"
    }
}
```

- FORM_ENCODED ペイロードタイプ – HTML 形式の名前を使用します。

  例えば、`username1` と `password1` という名前のユーザーおよびパスワードの入力要素を持つ HTML フォームの場合、ユーザー名フィールドの指定は `username1` で、パスワードフィールドの指定は `password1` です。

e. Amazon CloudFront ディストリビューションが保護されている場合、[レスポンス検査] で、アプリケーションがアカウント作成の試みに対するレスポンスで成功や失敗をどのように示すかを指定します。

> **Note**
>
> ACFP レスポンス検査は、CloudFront ディストリビューションを保護している保護パック (ウェブ ACL) でのみ使用できます。

ACFP で検査するアカウント作成レスポンスのコンポーネントを 1 つ指定します。Body および JSON コンポーネントタイプの場合、 AWS WAF はコンポーネントの最初の 65,536 バイト (64 KB) を検査できます。

インターフェイスに示されているように、コンポーネントタイプの検査基準を指定します。コンポーネント内で検査する成功基準と失敗基準の両方を指定する必要があります。

例えば、アプリケーションがアカウント作成の試みのステータスをレスポンスのステータスコードで示し、成功の場合は「200 OK」、失敗の場合は「401 Unauthorized」または「403 Forbidden」を使用するとします。レスポンス検査の [コンポーネントタイプ] を [ステータスコード] に設定し、[成功] テキストボックスに「200」と入力し、[失敗] テキストボックスの 1 行目に「401」、2 行目に「403」と入力します。

ACFP ルールグループは、成功または失敗の検査基準に一致するレスポンスのみをカウントします。ルールグループのルールは、アカウントの一括作成の試みを軽減するために、カウントされるレスポンスの成功率が高すぎるクライアントに対してアクションを実行します。ルールグループのルールが正確に動作するように、アカウント作成の試みの成功と失敗の両方に関する詳細な情報を必ず入力してください。

アカウント作成のレスポンスを検査するルールを確認するには、「AWS WAF Fraud Control アカウント作成不正防止 (ACFP) ルールグループ」のルールリストで VolumetricIPSuccessfulResponse と VolumetricSessionSuccessfulResponse を探します。

3. ルールグループに必要な追加設定を指定します。

   マネージドルールグループステートメントにスコープダウンステートメントを追加することで、ルールグループが検査するリクエストの範囲をさらに限定できます。例えば、特定のクエリ引数または cookie を持つリクエストのみを検査できます。ルールグループは、スコープダウンステートメントの基準に一致し、ルールグループ設定で指定したアカウント登録パスとアカウント作成パスに送信されたリクエストのみを検査します。スコープダウンステートメントの詳細については、「でのスコープダウンステートメントの使用 AWS WAF」を参照してください。

4. 変更を保護パック (ウェブ ACL) に保存します。

本番稼働トラフィックに ACFP 実装をデプロイする前に、トラフィックへの潜在的な影響に慣れるまで、ステージング環境またはテスト環境でテストおよびチューニングします。その後、ルールを有効にする前に、本番稼働用トラフィックでカウントモードでルールをテストしてチューニングします。ガイダンスについては、次のセクションを参照してください。

ACFP のテストとデプロイ

このセクションでは、サイトの AWS WAF Fraud Control Account Creation Fraud Prevention (ACFP) 実装を設定およびテストするための一般的なガイダンスを提供します。実行する具体的なステップは、ニーズ、リソース、および受け取るウェブリクエストによって異なります。

この情報は、AWS WAF 保護のテストとチューニング で提供されているテストおよび調整に関する一般情報とは別です。

> **Note**
>
> AWS マネージドルールは、一般的なウェブ脅威から保護するように設計されています。ドキュメントに従って使用すると、 AWS マネージドルールルールグループはアプリケーションに別のセキュリティレイヤーを追加します。ただし、 AWS マネージドルールルールグループは、選択した AWS リソースによって決定されるセキュリティ責任に代わるものではありません。責任共有モデルを参照して、 のリソースが適切に保護 AWS されていることを確認します。

> **本番稼働トラフィックのリスク**
>
> 本番稼働トラフィックに ACFP 実装をデプロイする前に、トラフィックへの潜在的な影響に慣れるまで、ステージング環境またはテスト環境でテストおよびチューニングします。その後、ルールを有効にする前に、本番稼働用トラフィックでカウントモードでルールをテストしてチューニングします。

AWS WAF は、ACFP 設定の検証に使用できるテスト認証情報を提供します。次の手順では、ACFP マネージドルールグループを使用するようにテスト保護パック (ウェブ ACL) を設定し、ルールグループによって追加されたラベルをキャプチャするルールを設定してから、これらのテスト認証情報を使用してアカウント作成の試みを実行します。アカウント作成の試みに関する Amazon CloudWatch メトリクスを確認して、保護パック (ウェブ ACL) が試行を正しく管理していることを検証します。

このガイダンスは、 AWS WAF 保護パック (ウェブ ACL)、ルール、およびルールグループを作成および管理する方法を一般的に認識しているユーザーを対象としています。これらのトピックは、このガイドの前のセクションでカバーされています。

Fraud Control Account Creation AWS WAF Fraud Prevention (ACFP) の実装を設定してテストするには

これらのステップを最初にテスト環境で実行し、次に本番環境で実行します。

1. AWS WAF Fraud Control アカウント作成不正防止 (ACFP) マネージドルールグループをカウントモードに追加する

   > **Note**
   >
   > このマネージドルールグループを使用する場合、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

   AWS マネージドルールルールグループ`AWSManagedRulesACFPRuleSet`を新規または既存の保護パック (ウェブ ACL) に追加し、現在の保護パック (ウェブ ACL) の動作を変更しないように設定します。このルールグループのルールとラベルの詳細については、「AWS WAF Fraud Control アカウント作成不正防止 (ACFP) ルールグループ」を参照してください。

   - マネージドルールグループを追加する際には、それを編集し、次の手順を実行します。
     - [ルールグループを設定] ペインで、アプリケーションのアカウント登録ページと作成ページの詳細を入力します。ACFP ルールグループは、この情報を使用してサインインアクティビティをモニタリングします。詳細については、「ACFP マネージドルールグループをウェブ ACL に追加」を参照してください。
     - [Rules] (ルール) ペインで、[Override all rule actions] (すべてのルールアクションをオーバーライド) ドロップダウンを開いて、[Count] を選択します。この設定では、 AWS WAF は、ルールグループ内のすべてのルールに対してリクエストを評価し、その結果の一致のみをカウントしつつ、引き続きリクエストにラベルを追加します。詳細については、「ルールグループ内のルールアクションのオーバーライド」を参照してください。

       このオーバーライドにより、ACFP マネージドルールの影響をモニタリングして、例外 (内部のユースケースの例外など) を追加するかどうか判断できます。
   - 保護パック (ウェブ ACL) の既存のルールの後に評価されるように、ルールグループを配置します。優先順位の設定の数値は、既に使用しているルールまたはルールグループよりも高くなります。詳細については、「ルールの優先度を設定する」を参照してください。

     これにより、現在のトラフィックの処理が中断されることはありません。例えば、SQL インジェクションやクロスサイトスクリプティングなどの悪意のあるトラフィックを検出するルー

ルがある場合、そのルールは引き続き検出し、それをログに記録します。または、既知の悪意のないトラフィックを許可するルールがある場合、ACFP マネージドルールグループによってブロックされるようにすることなく、そのトラフィックを許可し続けることができます。テストおよびチューニングのアクティビティ中に、処理順序を調整することもできます。

2. アプリケーション統合 SDK を実装する

AWS WAF JavaScript SDK をブラウザのアカウント登録パスとアカウント作成パスに統合します。 は、iOS デバイスと Android デバイスを統合するモバイル SDKs AWS WAF も提供します。統合 SDK の詳細については、「でのクライアントアプリケーション統合 AWS WAF」を参照してください。このレコメンデーションについては、「ACFP でのアプリケーション統合 SDK の使用」を参照してください。

> **Note**
>
> アプリケーション統合 SDK を使用できない場合は、保護パック (ウェブ ACL) で ACFP ルールグループを編集し、`AllRequests` ルールに設定したオーバーライドを削除することで、その ACFP ルールグループをテストできます。これにより、ルールの Challenge アクションの設定が有効になり、有効なチャレンジトークンが確実にリクエストに含まれるようになります。
> これは最初にテスト環境で実行し、その後に本番環境で細心の注意を払って実行してください。このアプローチは、ユーザーをブロックする可能性があります。例えば、登録ページのパスが `GET` テキスト/HTML リクエストを受け入れない場合、このルール設定は、登録ページですべてのリクエストを効果的にブロックできます。

3. 保護パック (ウェブ ACL) のサンプリング、ログ記録、およびメトリクスの有効化

必要に応じて、保護パック (ウェブ ACL) のログ記録、Amazon Security Lake データ収集、リクエストサンプリング、Amazon CloudWatch メトリクスを設定します。これらの可視化ツールを使用して ACFP マネージドルールグループとトラフィックとのインタラクションをモニタリングできます。

- ログ作成の詳細については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。
- Amazon Security Lake の詳細については、「Amazon Security Lake とは」および「Amazon Security Lake ユーザーガイド」の AWS 「サービスからデータを収集する」を参照してください。

- Amazon CloudWatch メトリクスの詳細については、「Amazon CloudWatch によるモニタリング」を参照してください。
- ウェブリクエストサンプリングの詳細については、「ウェブリクエストのサンプルの表示」を参照してください。

4. 保護パック (ウェブ ACL) をリソースに関連付ける

   保護パック (ウェブ ACL) がテストリソースに関連付けられていない場合は、関連付けます。詳細については、「AWS リソースとの保護の関連付けまたは関連付け解除」を参照してください。

5. トラフィックと ACFP ルールの一致をモニタリングする

   通常のトラフィックがフローしていることと、ACFP マネージドルールグループのルールが一致するウェブリクエストにラベルを追加していることを確認します。ログにラベルが表示され、Amazon CloudWatch メトリクスで ACFP とラベルのメトリクスを確認できます。ログでは、ルールグループでカウントするようにオーバーライドしたルールが、カウントに設定された `action` と、オーバーライドした設定済のルールアクションを示す `overriddenAction` とともに、`ruleGroupList` に表示されます。

6. ルールグループの認証情報チェック機能をテストする

   テスト用の侵害された認証情報を使用してアカウント作成を試行し、ルールグループが想定どおりに照合することを確認します。

   a. 保護されたリソースのアカウント登録ページにアクセスし、新しいアカウントの追加を試みます。次の AWS WAF テスト認証情報ペアを使用して、任意のテストを入力します。

      - ユーザー: `WAF_TEST_CREDENTIAL@wafexample.com`
      - パスワード: `WAF_TEST_CREDENTIAL_PASSWORD`

      これらのテスト認証情報は侵害された認証情報として分類され、ACFP マネージドルールグループはアカウント作成リクエストに `awswaf:managed:aws:acfp:signal:credential_compromised` ラベル (ログでの確認が可能) を追加します。

   b. 保護パック (ウェブ ACL) ログで、テストアカウント作成リクエストのログエントリの `labels` フィールドで `awswaf:managed:aws:acfp:signal:credential_compromised` ラベルを探しま

す。ログ作成の詳細については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。

侵害された認証情報をルールグループが想定どおりにキャプチャすることを検証したら、保護されたリソースに必要な実装を設定するステップを実行できます。

7. CloudFront ディストリビューションの場合、アカウントの一括作成の試みについてのルールグループによる管理をテストします。

   ACFP ルールグループに設定したレスポンスの成功基準それぞれに対してこのテストを実行します。テストとテストの間は 30 分以上あけてください。

   a. 成功基準ごとに、レスポンス内のその成功基準で成功するアカウント作成の試みを特定します。その後、単一のクライアントセッションから、30 分未満で少なくとも 5 回のアカウント作成の正常な試みを実行します。通常、ユーザーはサイトでアカウントを 1 つだけ作成します。

      最初のアカウント作成が成功した後、`VolumetricSessionSuccessfulResponse` ルールは他のアカウント作成レスポンスとの照合を開始し、ルールアクションのオーバーライドに基づいてそれらにラベル付けをしてカウントします。レイテンシーにより、ルールで最初の 1 回または 2 回が見逃される可能性があります。

   b. 保護パック (ウェブ ACL) ログで、テストアカウント作成ウェブリクエストのログエントリの `labels` フィールドで `awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_` ラベルを探します。ログ作成の詳細については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。

   これらのテストは、ルールによって集計された成功数がルールのしきい値を超えていることを確認することで、成功基準がレスポンスと一致していることを検証します。しきい値に達した後も同じセッションからアカウント作成リクエストを送信し続けると、成功率がしきい値を下回るまでルールによる一致が継続されます。しきい値を超えている間、ルールはセッションアドレスからの正常なアカウント作成の試みと失敗したアカウント作成の試みの両方に一致させます。

8. ACFP ウェブリクエストの処理をカスタマイズする

   必要に応じて、リクエストを明示的に許可またはブロックする独自のルールを追加して、ACFP ルールがそのリクエストを処理する方法を変更します。

例えば、ACFP ラベルを使用して、リクエストを許可またはブロックしたり、リクエスト処理をカスタマイズしたりできます。ACFP マネージドルールグループの後にラベル一致ルールを追加して、適用する処理のためにラベル付きリクエストをフィルタリングできます。テスト後、関連する ACFP ルールをカウントモードで維持し、カスタムルールでリクエストの処理に関する決定を維持します。例については、ACFP の例: 侵害された認証情報についてのカスタムレスポンスを参照してください。

9. テストルールを削除し、ACFP マネージドルールグループ設定を有効にする

   状況によっては、一部の ACFP ルールをカウントモードのままにすると判断していた可能性もあります。ルールグループ内で設定したとおりに実行するルールについては、保護パック (ウェブ ACL) ルールグループ設定でカウントモードを無効にします。テストが終了したら、テストラベル一致ルールを削除することもできます。

10. モニタリングおよびチューニング

    ウェブリクエストが希望どおりに処理されていることを確認するには、使用することを希望する ACFP 機能を有効にした後、トラフィックを注意深くモニタリングします。ルールグループに対するルールカウントの上書きと独自のルールを使用して、必要に応じて動作を調整します。

ACFP ルールグループの実装のテストが完了したら、 AWS WAF JavaScript SDK をブラウザのアカウント登録ページとアカウント作成ページにまだ統合していない場合は、統合することを強くお勧めします。また、 には、iOS デバイスと Android デバイスを統合するモバイル SDKs AWS WAF も用意されています。統合 SDK の詳細については、「でのクライアントアプリケーション統合 AWS WAF」を参照してください。このレコメンデーションについては、「ACFP でのアプリケーション統合 SDK の使用」を参照してください。

AWS WAF Fraud Control アカウント作成不正防止 (ACFP) の例

このセクションでは、 AWS WAF Fraud Control Account Creation Fraud Prevention (ACFP) の実装の一般的なユースケースに対応できる設定例を示します。

各例は、ユースケースの説明を提供し、カスタム設定ルールの JSON リストにそのソリューションを示します。

> **Note**
>
> これらの例に示されているような JSON リストは、コンソール保護パック (ウェブ ACL) JSON ダウンロードやルール JSON エディタを介して、または API やコマンドラインインターフェイスでの getWebACL オペレーションを介して取得できます。

トピック

- ACFP の例: シンプルな設定
- ACFP の例: 侵害された認証情報についてのカスタムレスポンス
- ACFP の例: レスポンス検査の設定

ACFP の例: シンプルな設定

次の JSON リストは、 AWS WAF Fraud Control アカウント作成不正防止 (ACFP) マネージドルールグループを使用した保護パック (ウェブ ACL) の例を示しています。検証するために、CreationPath および RegistrationPagePath の追加設定と、ペイロードタイプ、およびペイロード内の新しいアカウント情報を見つけるために必要な情報に注意してください。ルールグループはこの情報を使用して、アカウント作成リクエストをモニタリングおよび管理します。この JSON には、ラベル名前空間や保護パック (ウェブ ACL) のアプリケーション統合 URL など、保護パック (ウェブ ACL) の自動生成された設定が含まれます。

```
{
  "Name": "simpleACFP",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/simpleACFP/... ",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
```

```
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  },
                  "EmailField": {
                    "Identifier": "/form/email"
                  },
                  "PhoneNumberFields": [
                    {
                      "Identifier": "/form/country-code"
                    },
                    {
                      "Identifier": "/form/region-code"
                    },
                    {
                      "Identifier": "/form/phonenumber"
                    }
                  ],
                  "AddressFields": [
                    {
                      "Identifier": "/form/name"
                    },
                    {
                      "Identifier": "/form/street-address"
                    },
                    {
                      "Identifier": "/form/city"
                    },
                    {
                      "Identifier": "/form/state"
                    },
                    {
                      "Identifier": "/form/zipcode"
                    }
                  ]
                },
```

```
                "EnableRegexInPath": false
              }
            }
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "simpleACFP"
  },
  "Capacity": 50,
  "ManagedByFirewallManager": false,
  "RetrofittedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:simpleACFP:"
}
```

ACFP の例: 侵害された認証情報についてのカスタムレスポンス

デフォルトでは、ルールグループ AWSManagedRulesACFPRuleSet によって実行される認証情報チェックは、リクエストにラベル付けしてブロックすることで、侵害された認証情報を処理します。ルールグループとルールの動作の詳細については、「AWS WAF Fraud Control アカウント作成不正防止 (ACFP) ルールグループ」を参照してください。

ユーザーが提供したアカウント認証情報が侵害されたことをユーザーに通知するために、次を実行できます。

- **SignalCredentialCompromised** ルールを Count にオーバーライド — これにより、ルールは一致するリクエストをカウントしてラベル付けのみします。
- カスタム処理でラベル一致ルールの追加 – ACFP ラベルと照合し、カスタム処理を実行するようにルールを設定します。

次の保護パック (ウェブ ACL) リスティングは、SignalCredentialCompromised ルールアクションがカウントするようにオーバーライドされた状態で、前の例の ACFP マネージドルールグループを示しています。この設定では、このルールグループは、侵害された認証情報を使用するウェブリクエストを評価すると、リクエストにラベルを付けますが、ブロックすることはありません。

さらに、保護パック (ウェブ ACL) には aws-waf-credential-compromised という名前のカスタムレスポンスと AccountSignupCompromisedCredentialsHandling という名前の新しいルールが追加されました。ルールの優先順位にはルールグループよりも大きい数値が設定されているため、保護パック (ウェブ ACL) 評価では、ルールはルールグループの後に実行されます。新しいルールは、ルールグループの侵害された認証情報ラベルを持つすべてのリクエストと照合します。ルールは一致を見つけると、カスタムレスポンス本文を含むリクエストに Block アクションを適用します。カスタムレスポンス本文は、認証情報が侵害されたという情報をエンドユーザーに提供し、実行するアクションを提案します。

```
{
  "Name": "compromisedCreds",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/compromisedCreds/...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
```

```
                },
                "EmailField": {
                  "Identifier": "/form/email"
                },
                "PhoneNumberFields": [
                  {
                    "Identifier": "/form/country-code"
                  },
                  {
                    "Identifier": "/form/region-code"
                  },
                  {
                    "Identifier": "/form/phonenumber"
                  }
                ],
                "AddressFields": [
                  {
                    "Identifier": "/form/name"
                  },
                  {
                    "Identifier": "/form/street-address"
                  },
                  {
                    "Identifier": "/form/city"
                  },
                  {
                    "Identifier": "/form/state"
                  },
                  {
                    "Identifier": "/form/zipcode"
                  }
                ]
              },
              "EnableRegexInPath": false
            }
          }
        ],
        "RuleActionOverrides": [
          {
            "Name": "SignalCredentialCompromised",
            "ActionToUse": {
              "Count": {}
            }
          }
```

```
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
      }
    },
    {
      "Name": "AccountSignupCompromisedCredentialsHandling",
      "Priority": 1,
      "Statement": {
        "LabelMatchStatement": {
          "Scope": "LABEL",
          "Key": "awswaf:managed:aws:acfp:signal:credential_compromised"
        }
      },
      "Action": {
        "Block": {
          "CustomResponse": {
            "ResponseCode": 406,
            "CustomResponseBodyKey": "aws-waf-credential-compromised",
            "ResponseHeaders": [
              {
                "Name": "aws-waf-credential-compromised",
                "Value": "true"
              }
            ]
          }
        }
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AccountSignupCompromisedCredentialsHandling"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
```

```
    "CloudWatchMetricsEnabled": true,
    "MetricName": "compromisedCreds"
  },
  "Capacity": 51,
  "ManagedByFirewallManager": false,
  "RetrofittedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:compromisedCreds:",
  "CustomResponseBodies": {
    "aws-waf-credential-compromised": {
      "ContentType": "APPLICATION_JSON",
      "Content": "{\n  \"credentials-compromised\": \"The credentials you provided have
 been found in a compromised credentials database.\\n\\nTry again with a different
 username, password pair.\"\n}"
    }
  }
}
```

ACFP の例: レスポンス検査の設定

次の JSON リストは、オリジンレスポンスを検査するように設定された AWS WAF Fraud Control Account Creation Fraud Prevention (ACFP) マネージドルールグループを使用した保護パック (ウェブ ACL) の例を示しています。成功とレスポンスステータスコードを指定する応答検査設定を注意してください。ヘッダー、ボディ、ボディの JSON 一致に基づいて成功とレスポンスの設定を構成することもできます。この JSON には、ラベル名前空間や保護パック (ウェブ ACL) のアプリケーション統合 URL など、保護パック (ウェブ ACL) の自動生成された設定が含まれます。

> **Note**
>
> ATP レスポンス検査は、CloudFront ディストリビューションが保護されている保護パック (ウェブ ACL) でのみ使用できます。

```
{
  "Name": "simpleACFP",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/simpleACFP/... ",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
```

```
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  },
                  "EmailField": {
                    "Identifier": "/form/email"
                  },
                  "PhoneNumberFields": [
                    {
                      "Identifier": "/form/country-code"
                    },
                    {
                      "Identifier": "/form/region-code"
                    },
                    {
                      "Identifier": "/form/phonenumber"
                    }
                  ],
                  "AddressFields": [
                    {
                      "Identifier": "/form/name"
                    },
                    {
                      "Identifier": "/form/street-address"
                    },
                    {
                      "Identifier": "/form/city"
                    },
```

```
                    {
                      "Identifier": "/form/state"
                    },
                    {
                      "Identifier": "/form/zipcode"
                    }
                  ]
                },
                "ResponseInspection": {
                  "StatusCode": {
                    "SuccessCodes": [
                      200
                    ],
                    "FailureCodes": [
                      401
                    ]
                  }
                },
                "EnableRegexInPath": false
              }
            }
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "simpleACFP"
  },
  "Capacity": 50,
  "ManagedByFirewallManager": false,
  "RetrofittedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:simpleACFP:"
```

```
}
```

AWS WAF Fraud Control アカウント乗っ取り防止 (ATP)

このセクションでは、 AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) の機能について説明します。

アカウント乗っ取りは、攻撃者が個人のアカウントへの不正アクセスを得るオンラインの違法行為です。攻撃者は、盗まれた認証情報を使用したり、一連の試行を通じて被害者のパスワードを推測するなど、さまざまな方法でこれを行う可能性があります。攻撃者がアクセスできるようになると、被害者から金銭や情報を盗んだり、サービスを不正に利用したりする可能性があります。攻撃者は、被害者が所有する他のアカウントにアクセスしたり、他の人や組織のアカウントにアクセスしたりするために、被害者としてふるまう可能性があります。さらに、被害者であるユーザーが自分のアカウントからブロックされるようにするために、そのユーザーのパスワードを変更しようとする場合があります。

ATP 機能を実装することで、アカウント乗っ取りの試行をモニタリングおよび制御できます。 は、この機能を AWS マネージドルールのルールグループ`AWSManagedRulesATPRuleSet`およびコンパニオンアプリケーション統合 SDKs で AWS WAF 提供します。

ATP マネージドルールグループは、悪意のあるアカウント乗っ取りの試みの一部である可能性があるリクエストにラベルを付けて管理します。ルールグループは、クライアントでアプリケーションのログインエンドポイントに送信するログイン試行を検査することでこれを行います。

- リクエスト検査 – ATP を使用すると、異常なログイン試行や盗まれた認証情報を使用するログイン試行を可視化して制御できるため、不正行為につながる可能性のあるアカウントの乗っ取りを防ぐことができます。ATP は、盗まれた認証情報のデータベースに照らして E メールとパスワードの組み合わせをチェックします。このデータベースは、漏洩された認証情報がダークウェブ上で新しく見つかると定期的に更新されます。ATP は、IP アドレスやクライアントセッションごとにデータを集約し、不審なリクエストを大量に送信するクライアントを検出してブロックします。
- レスポンス検査 – CloudFront ディストリビューションの場合、ATP ルールグループは、受信したログインリクエストを検査するだけでなく、ログイン試行に対するアプリケーションの応答も検査して、成功率と失敗率を追跡します。この情報を使用して、ATP はログイン失敗の回数が過度に多いクライアントセッションまたは IP アドレスを一時的にブロックできます。 AWS WAF は、レスポンス検査を非同期で実行するため、ウェブトラフィックのレイテンシーが大きくなることはありません。

> **Note**
>
> このマネージドルールグループを使用する場合、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

> **Note**
>
> ATP 機能は、Amazon Cognito ユーザープールでは使用できません。

トピック

- AWS WAF ATP コンポーネント
- ATP でアプリケーション統合 SDK を使用
- ATP マネージドルールグループを保護パック (ウェブ ACL) に追加
- ATP のテストとデプロイ
- AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) の例

AWS WAF ATP コンポーネント

AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) の主なコンポーネントは次のとおりです。

- **`AWSManagedRulesATPRuleSet`** – この AWS マネージドルールルールグループのルールは、さまざまなタイプのアカウント乗っ取りアクティビティを検出、ラベル付け、処理します。ルールグループは、クライアントから指定したログインエンドポイントに送信される HTTP POST ウェブリクエストを検査します。保護された CloudFront ディストリビューションでは、ルールグループはディストリビューションがこれらのリクエストに送り返す応答も検査します。ルールグループのルールのリストについては、「AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループ」を参照してください。マネージドルールグループ参照ステートメントを使用して、このルールグループを保護パック (ウェブ ACL) に含めます。このルールグループの使用については、「ATP マネージドルールグループを保護パック (ウェブ ACL) に追加」を参照してください。

  > **Note**
  >
  > このマネージドルールグループを使用する場合、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

- アプリケーションのログインページに関する詳細 – AWSManagedRulesATPRuleSet ルールグループを保護パック (ウェブ ACL) に追加する際、ログインページに関する情報を提供する必要があります。これにより、ルールグループは検査するリクエストの範囲を絞り込み、ウェブリクエストで認証情報の使用状況を適切に検証できます。ATP ルールグループは、電子メール形式のユーザー名に対応します。詳細については、「ATP マネージドルールグループを保護パック (ウェブ ACL) に追加」を参照してください。
- 保護された CloudFront ディストリビューションの場合、ログイン試行に対するアプリケーションの応答方法に関する詳細 – ログイン試行に対するアプリケーションの応答に関する詳細を指定すると、ルールグループはログイン試行の失敗回数が過度に多いクライアントを追跡および管理します。このオプションの設定については、「ATP マネージドルールグループを保護パック (ウェブ ACL) に追加」を参照してください。
- JavaScript とモバイルアプリケーションの統合 SDKs – ATP 実装を使用して AWS WAF JavaScript とモバイル SDKs を実装し、ルールグループが提供する機能の完全なセットを有効にします。ATP ルールの多くは、セッションレベルのクライアント検証および動作集約に SDK から提供された情報を使用し、正規のクライアントトラフィックをボットトラフィックから分離するために必要です。SDK の詳細については、「でのクライアントアプリケーション統合 AWS WAF」を参照してください。

ATP 実装を次と組み合わせて、保護のモニタリング、チューニング、およびカスタマイズに役立てることができます。

- ログ記録とメトリクス – 保護パック (ウェブ ACL) 用にログ、Amazon Security Lake データ収集と　Amazon CloudWatch メトリクスを設定して有効にすることで、トラフィックをモニタリングし、ACFP マネージドルールグループがトラフィックにどのように影響するのかを理解できます。AWSManagedRulesATPRuleSet がウェブリクエストに追加するラベルは、データに含まれます。オプションの詳細については、ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック、Amazon CloudWatch によるモニタリング、及び「What is Amazon Security Lake?」を参照してください。

  ニーズと確認できるトラフィックに応じて、AWSManagedRulesATPRuleSet の実装をカスタマイズできます。たとえば、ATP 評価から一部のトラフィックを除外したり、スコープダウンステートメントやラベルマッチングルールなどの AWS WAF 機能を使用して、識別したアカウント乗っ取り試行の処理方法を変更したりできます。
- ラベルとラベル一致ルール – AWSManagedRulesATPRuleSet のどのルールでも、ブロック動作をカウントに切り替えて、ルールによって追加されたラベルと照合することができます。このアプローチを使用し、ATP マネージドルールグループによって識別されるウェブリクエストの処理方

法をカスタマイズします。ラベル付けおよびラベル一致ステートメントの使用の詳細については、「ラベル一致ルールステートメント」および「でのウェブリクエストのラベル付け AWS WAF」を参照してください。

- カスタムリクエストとレスポンス - 許可するリクエストにはカスタムヘッダーを追加し、ブロックするリクエストにはカスタムレスポンスを送信できます。これを行うには、ラベル一致を AWS WAF カスタムリクエストおよび応答機能とペアリングします。リクエストとレスポンスをカスタマイズする方法については、「でカスタマイズされたウェブリクエストとレスポンス AWS WAF」を参照してください。

ATP でアプリケーション統合 SDK を使用

このセクションでは、ATP でアプリケーション統合 SDK を使用する方法について説明します。

ATP マネージドルールグループには、アプリケーション統合 SDK が生成するチャレンジトークンが必要です。トークンは、ルールグループが提供するすべての保護を有効にします。

ATP ルールグループを最も効果的に使用するためにも、アプリケーション統合 SDK を実装することを強くお勧めします。チャレンジスクリプトが取得するトークンからのメリットを ATP ルールグループが得るには、ATP ルールグループの前にチャレンジスクリプトを実行する必要があります。アプリケーション統合 SDK を使用すると、これが自動的に行われます。SDK を使用できない場合は、代替手段として、ATP ルールグループが検査するすべてのリクエストに対して CAPTCHA または Challenge ルールアクションを実行するように保護パック (ウェブ ACL) を設定することができます。Challenge または CAPTCHA ルールアクションを使用すると、追加料金が発生する場合があります。料金の詳細については、「AWS WAF の料金」を参照してください。

トークンを必要としない ATP ルールグループの機能

ウェブリクエストにトークンが含まれていないときは、ATP マネージドルールグループ以下のタイプのトラフィックをブロックできます。

- 多数のログインリクエストを行う単一の IP アドレス。
- 短時間で多数の失敗したログインリクエストが行われた単一の IP アドレス。
- 同じユーザー名を使用してもパスワードを変更してパスワードトラバーサルでログイン試行。

トークンを必要とする ATP ルールグループの機能

チャレンジトークンで提供される情報により、ルールグループとクライアントアプリケーションセキュリティ全体の機能が拡張されます。

このトークンは、ウェブリクエストごとにクライアント情報を提供します。これにより、ATP ルールグループは、正規のクライアントセッションと動作の悪いクライアントセッションが両方とも単一の IP アドレスから発信された場合でも、前者を後者から分離できます。ルールグループは、トークン内の情報を使用してクライアントセッションリクエストの動作を集約し、微調整した検出および軽減を実現します。

トークンがウェブリクエストで使用可能な場合、ATP ルールグループは次の追加カテゴリのクライアントをセッションレベルで検出してブロックできます。

- SDK が管理するサイレントチャレンジに失敗するクライアントセッション。
- ユーザー名またはパスワードを経由するクライアントセッション。これはクレデンシャルスタッフィングとも呼ばれます。
- 盗まれた認証情報を繰り返し使用してログインするクライアントセッション。
- ログインに長時間かかるクライアントセッション。
- 多数のログインリクエストを行うクライアントセッション。ATP ルールグループは、IP アドレスでクライアントをブロックできる AWS WAF レートベースのルールよりも優れたクライアント分離を提供します。ATP ルールグループでは、より低いしきい値も使用されています。
- 短時間で多数の失敗したログインリクエストが行われたクライアントセッション。この機能は、保護されている Amazon CloudFront ディストリビューションで利用できます。

ルールグループ機能の情報については、「AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループ」を参照してください。

SDK の詳細については、「でのクライアントアプリケーション統合 AWS WAF」を参照してください。 AWS WAF トークンの詳細については、「」を参照してくださいAWS WAF インテリジェントな脅威の軽減におけるトークンの使用。ルールアクションの情報については、「CAPTCHA および Challengeの AWS WAF」を参照してください。

ATP マネージドルールグループを保護パック (ウェブ ACL) に追加

このセクションでは、`AWSManagedRulesATPRuleSet` ルールグループを追加および設定する方法について説明します。

ウェブトラフィックのアカウント乗っ取りアクティビティを認識するように ATP マネージドルールグループを設定するには、アプリケーションにログインリクエストを送信する方法に関する情報をクライアントで指定します。保護された Amazon CloudFront ディストリビューションでは、ログインリクエストに対するアプリケーションの応答方法に関する情報も指定します。この設定は、マネージドルールグループの通常の設定に追加されます。

ルールグループの説明とルールリストについては、「AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループ」を参照してください。

> **Note**
>
> 盗まれた認証情報の ATP データベースには、E メール形式のユーザー名のみが含まれています。

このガイダンスは、 AWS WAF 保護パック (ウェブ ACL)、ルール、およびルールグループを作成および管理する方法を一般的に認識しているユーザーを対象としています。これらのトピックは、このガイドの前のセクションでカバーされています。マネージドルールグループを保護パック (ウェブ ACL) に追加する方法の基本については、「コンソールを通じた保護パック (ウェブ ACL) へのマネージドルールグループの追加」を参照してください。

ベストプラクティスに従う

ATP ルールグループは、「でのインテリジェントな脅威軽減のベストプラクティス AWS WAF」に記載されているベストプラクティスに従って使用してください。

保護パック (ウェブ ACL) で **AWSManagedRulesATPRuleSet** ルールグループを使用するには

1. AWS マネージドルールグループを保護パック (ウェブ ACL) `AWSManagedRulesATPRuleSet`に追加し、保存する前にルールグループ設定を編集します。

   > **Note**
   >
   > このマネージドルールグループを使用する場合、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

2. [ルールグループを設定] ペインで、ATP ルールグループがログインリクエストの検査に使用する情報を入力します。

   a. 「パスで正規表現を使用する」で、ログインページパスの仕様に合わせて正規表現マッチング AWS WAF を実行する場合は、これをオンにします。

      AWS WAF は、いくつかの例外`libpcre`を除いて、PCRE ライブラリで使用されるパターン構文をサポートします。ライブラリは、「PCRE - Perl Compatible Regular Expressions」で文書化されています。 AWS WAF サポートの詳細については、「」を参照してくださいでサポートされている正規表現構文 AWS WAF。

b. [Login path] (ログインパス) で、アプリケーションのログインエンドポイントのパスを指定します。ルールグループは、指定されたログインエンドポイントに対する HTTP POST リクエストのみを検査します。

> **Note**
>
> エンドポイントの照会では大文字と小文字が区別されません。正規表現の仕様には、大文字と小文字を区別しない照合を無効にするフラグ (`?-i`) を含めてはいけません。文字列の指定はフォワードスラッシュ「/」で始まる必要があります。

例えば、URL `https://example.com/web/login` では、文字列パスの指定「`/web/login`」を指定できます。指定したパスで始まるログインパスは一致と見なされます。例えば、`/web/login` はログインパス `/web/login`、`/web/login/`、`/web/loginPage`、および `/web/login/thisPage` に一致しますが、ログインパス `/home/web/login` または `/website/login` には一致しません。

c. [リクエスト検査] で、リクエストのペイロードタイプと、ユーザー名とパスワードが指定されているリクエスト本文内のフィールドの名前を指定して、アプリケーションがログイン試行を受け入れる方法を指定します。これらのフィールド名の指定は、ペイロードタイプによって異なります。

- JSON ペイロードタイプ – JSON Pointer 構文でフィールド名を指定します。JSON Pointer 構文の詳細については、インターネットエンジニアリングタスクフォース (IETF) ドキュメントの「JavaScript Object Notation (JSON) Pointer」を参照してください。

  例えば、次の JSON ペイロードの例では、ユーザー名フィールドの指定は `/login/username` で、パスワードフィールドの指定は `/login/password` です。

  ```
  {
      "login": {
          "username": "THE_USERNAME",
          "password": "THE_PASSWORD"
      }
  }
  ```

- FORM_ENCODED ペイロードタイプ – HTML 形式の名前を使用します。

例えば、username1 と password1 という名前の入力要素を持つ HTML フォームの場合、ユーザー名フィールドの指定は username1 で、パスワードフィールドの指定は password1 です。

d. Amazon CloudFront ディストリビューションが保護されている場合、[レスポンス検査] で、アプリケーションがログイン試行に対する応答で成功や失敗をどのように示すかを指定します。

> **Note**
>
> ATP レスポンス検査は、CloudFront ディストリビューションが保護されている保護パック (ウェブ ACL) でのみ使用できます。

ATP で検査するログインレスポンスのコンポーネントを 1 つ指定します。本文および JSON コンポーネントタイプの場合、 AWS WAF はコンポーネントの最初の 65,536 バイト (64 KB) を検査できます。

インターフェイスに示されているように、コンポーネントタイプの検査基準を指定します。コンポーネント内で検査する成功基準と失敗基準の両方を指定する必要があります。

例えば、アプリケーションがログイン試行のステータスを応答のステータスコードで示し、成功の場合は「200 OK」、失敗の場合は「401 Unauthorized」または「403 Forbidden」を使用するとします。レスポンス検査の [コンポーネントタイプ] を [ステータスコード] に設定し、[成功] テキストボックスに「200」と入力し、[失敗] テキストボックスの 1 行目に「401」、2 行目に「403」と入力します。

ATP ルールグループは、成功または失敗の検査基準に一致する応答のみをカウントします。ルールグループのルールは、カウントされた応答の失敗率が過度に高いクライアントに適用されます。ルールグループのルールが正確に動作するように、ログイン試行の成功と失敗の両方に関する詳細な情報を必ず入力してください。

ログインレスポンスを検査するルールを確認するには、「AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループ」のルールリストで VolumetricIpFailedLoginResponseHigh と VolumetricSessionFailedLoginResponseHigh を探します。

3. ルールグループに必要な追加設定を指定します。

マネージドルールグループステートメントにスコープダウンステートメントを追加することで、ルールグループが検査するリクエストの範囲をさらに限定できます。例えば、特定のクエリ引数または cookie を持つリクエストのみを検査できます。ルールグループは、スコープダウンステートメントの基準に一致する、指定したログインエンドポイントへの HTTP POST リクエストのみを検査します。スコープダウンステートメントの詳細については、「でのスコープダウンステートメントの使用 AWS WAF」を参照してください。

4. 変更を保護パック (ウェブ ACL) に保存します。

本番稼働トラフィックに ATP 実装をデプロイする前に、トラフィックへの潜在的な影響に慣れるまで、ステージング環境またはテスト環境でテストおよびチューニングします。その後、ルールを有効にする前に、本番稼働用トラフィックでカウントモードでルールをテストしてチューニングします。ガイダンスについては、次のセクションを参照してください。

ATP のテストとデプロイ

このセクションでは、サイトの AWS WAF Fraud Control Account Takeover Prevention (ATP) 実装を設定およびテストするための一般的なガイダンスを提供します。実行する具体的なステップは、ニーズ、リソース、および受け取るウェブリクエストによって異なります。

この情報は、AWS WAF 保護のテストとチューニング で提供されているテストおよび調整に関する一般情報とは別です。

> **Note**
>
> AWS マネージドルールは、一般的なウェブ脅威から保護するように設計されています。ドキュメントに従って使用すると、 AWS マネージドルールルールグループはアプリケーションに別のセキュリティレイヤーを追加します。ただし、 AWS マネージドルールルールグループは、選択した AWS リソースによって決定されるセキュリティ責任に代わるものではありません。責任共有モデルを参照して、 のリソースが適切に保護 AWS されていることを確認します。

> **本番稼働トラフィックのリスク**
>
> 本番稼働トラフィックに ATP 実装をデプロイする前に、トラフィックへの潜在的な影響に慣れるまで、ステージング環境またはテスト環境でテストおよびチューニングします。その

後、ルールを有効にする前に、本番稼働用トラフィックでカウントモードでルールをテストしてチューニングします。

AWS WAF は、ATP 設定の検証に使用できるテスト認証情報を提供します。次の手順では、ATP マネージドルールグループを使用するようにテスト保護パック (ウェブ ACL) を設定し、ルールグループによって追加されたラベルをキャプチャするルールを設定してから、これらのテスト認証情報を使用してログイン試行を実行します。ログイン試行に関する Amazon CloudWatch メトリクスを確認して、ウェブ ACL が試行を正しく管理していることを検証します。

このガイダンスは、 AWS WAF 保護パック (ウェブ ACL)、ルール、およびルールグループを作成および管理する方法を一般的に認識しているユーザーを対象としています。これらのトピックは、このガイドの前のセクションでカバーされています。

AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) 実装を設定してテストするには

これらのステップを最初にテスト環境で実行し、次に本番環境で実行します。

1. Fraud AWS WAF Control アカウント乗っ取り防止 (ATP) マネージドルールグループをカウントモードに追加する

   > **Note**
   >
   > このマネージドルールグループを使用する場合、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

   AWS マネージドルールルールグループ`AWSManagedRulesATPRuleSet`を新規または既存の保護パック (ウェブ ACL) に追加し、現在の保護パック (ウェブ ACL) の動作を変更しないように設定します。このルールグループのルールとラベルの詳細については、「AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループ」を参照してください。

   - マネージドルールグループを追加する際には、それを編集し、次の手順を実行します。
     - [Rule group configuration] (ルールグループを設定) ペインで、アプリケーションのログインページの詳細を入力します。ATP ルールグループは、この情報を使用してサインインアクティビティをモニタリングします。詳細については、「ATP マネージドルールグループを保護パック (ウェブ ACL) に追加」を参照してください。

- [Rules] (ルール) ペインで、[Override all rule actions] (すべてのルールアクションをオーバーライド) ドロップダウンを開いて、[Count] を選択します。この設定では、 AWS WAF は、ルールグループ内のすべてのルールに対してリクエストを評価し、その結果の一致のみをカウントしつつ、引き続きリクエストにラベルを追加します。詳細については、「ルールグループ内のルールアクションのオーバーライド」を参照してください。

  このオーバーライドにより、ATP マネージドルールの影響をモニタリングして、例外 (内部のユースケースの例外など) を追加するかどうか判断できます。

- 保護パック (ウェブ ACL) の既存のルールの後に評価されるように、ルールグループを配置します。優先順位の設定の数値は、既に使用しているルールまたはルールグループよりも高くなります。詳細については、「ルールの優先度を設定する」を参照してください。

  これにより、現在のトラフィックの処理が中断されることはありません。例えば、SQL インジェクションやクロスサイトスクリプティングなどの悪意のあるトラフィックを検出するルールがある場合、そのルールは引き続き検出し、それをログに記録します。または、既知の悪意のないトラフィックを許可するルールがある場合、ATP マネージドルールグループによってブロックされるようにすることなく、そのトラフィックを許可し続けることができます。テストおよびチューニングのアクティビティ中に、処理順序を調整することもできます。

2. 保護パック (ウェブ ACL) のサンプリング、ログ記録、およびメトリクスの有効化

   必要に応じて、保護パック (ウェブ ACL) のログ記録、Amazon Security Lake データ収集、リクエストサンプリング、Amazon CloudWatch メトリクスを設定します。これらの可視化ツールを使用して ATP マネージドルールグループとトラフィックとのインタラクションをモニタリングできます。

   - ログ記録の設定と使用については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。
   - Amazon Security Lake の詳細については、「Amazon Security Lake とは」および「Amazon Security Lake ユーザーガイド」の AWS 「サービスからのデータ収集」を参照してください。
   - Amazon CloudWatch メトリクスの詳細については、「Amazon CloudWatch によるモニタリング」を参照してください。
   - ウェブリクエストサンプリングの詳細については、「ウェブリクエストのサンプルの表示」を参照してください。

3. 保護パック (ウェブ ACL) をリソースに関連付ける

   保護パック (ウェブ ACL) がテストリソースに関連付けられていない場合は、関連付けます。詳細については、「AWS リソースとの保護の関連付けまたは関連付け解除」を参照してください。

4. トラフィックと ATP ルールの一致をモニタリングする

   通常のトラフィックがフローしていることと、ATP マネージドルールグループのルールが一致するウェブリクエストにラベルを追加していることを確認します。ログにラベルが表示され、Amazon CloudWatch メトリクスで ATP とラベルのメトリクスを確認できます。ログでは、ルールグループでカウントするようにオーバーライドしたルールが、カウントに設定された `action` と、オーバーライドした設定済のルールアクションを示す `overriddenAction` とともに、`ruleGroupList` に表示されます。

5. ルールグループの認証情報チェック機能をテストする

   テスト用の侵害された認証情報を使用してログインを試行し、ルールグループが想定どおりに照合することを確認します。

   a. 次の AWS WAF テスト認証情報ペアを使用して、保護されたリソースのログインページにログインします。

      - ユーザー: `WAF_TEST_CREDENTIAL@wafexample.com`
      - パスワード: `WAF_TEST_CREDENTIAL_PASSWORD`

      これらのテスト認証情報は侵害された認証情報として分類され、ATP マネージドルールグループはログインリクエストに `awswaf:managed:aws:atp:signal:credential_compromised` ラベル (ログでの確認が可能) を追加します。

   b. 保護パック (ウェブ ACL) ログで、テストログインウェブリクエストのログエントリの `labels` フィールドで `awswaf:managed:aws:atp:signal:credential_compromised` ラベルを探します。ログ作成の詳細については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。

   侵害された認証情報をルールグループが想定どおりにキャプチャすることを検証したら、保護されたリソースに必要な実装を設定するステップを実行できます。

6. CloudFront ディストリビューションで、ルールグループのログイン失敗管理をテストする

   a. ATP ルールグループに設定した応答の失敗基準それぞれに対してテストを実行します。テストとテストの間は 10 分以上あけてください。

      単一の失敗基準をテストするには、その条件で失敗するログイン試行を応答内で特定します。次に、単一のクライアント IP アドレスからの失敗したログイン試行を、10 分以内に少なくとも 10 回実行します。

      最初の 6 回の試行が失敗した後、ボリューメトリックが失敗したログインルールが、残りのログイン試行に対する一致、ラベル付け、およびカウントを開始します。レイテンシーにより、ルールで最初の 1 回または 2 回が見逃される可能性があります。

   b. 保護パック (ウェブ ACL) ログで、テストログインウェブリクエストのログエントリの `labels` フィールドで `awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:high` ラベルを探します。ログ作成の詳細については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。

   これらのテストでは、失敗したログイン回数がルール `VolumetricIpFailedLoginResponseHigh` のしきい値を超えているかどうかをチェックして、失敗基準が応答に一致しているかどうかを検証します。しきい値に達した後も同じ IP アドレスからログインリクエストを送信し続けると、失敗率がしきい値を下回るまでルールによる一致が継続されます。しきい値を超えている間、ルールは IP アドレスからの成功したログインと失敗したログインの両方に一致させます。

7. ATP ウェブリクエストの処理をカスタマイズする

   必要に応じて、リクエストを明示的に許可またはブロックする独自のルールを追加して、ATP ルールがそのリクエストを処理する方法を変更します。

   例えば、ATP ラベルを使用して、リクエストを許可またはブロックしたり、リクエスト処理をカスタマイズしたりできます。ATP マネージドルールグループの後にラベル一致ルールを追加して、適用する処理のためにラベル付きリクエストをフィルタリングできます。テスト後、関連する ATP ルールをカウントモードで維持し、カスタムルールでリクエストの処理に関する決定を維持します。例については、ATP の例: 認証情報の不足および侵害された認証情報のカスタム処理を参照してください。

8. テストルールを削除し、ATP マネージドルールグループ設定を有効にする

   状況によっては、一部の ATP ルールをカウントモードのままにすると判断していた可能性もあります。ルールグループ内で設定したとおりに実行するルールについては、保護パック (ウェブ ACL) ルールグループ設定でカウントモードを無効にします。テストが終了したら、テストラベル一致ルールを削除することもできます。

9. モニタリングおよびチューニング

   ウェブリクエストが希望どおりに処理されていることを確認するには、使用することを希望する ATP 機能を有効にした後、トラフィックを注意深くモニタリングします。ルールグループに対するルールカウントの上書きと独自のルールを使用して、必要に応じて動作を調整します。

ATP ルールグループの実装のテストが終了した後、まだ行っていない場合は、検出機能を強化するために、 AWS WAF JavaScript SDK をブラウザのログインページに統合することを強くお勧めします。 には、iOS デバイスと Android デバイスを統合するモバイル SDKs AWS WAF も用意されています。統合 SDK の詳細については、「でのクライアントアプリケーション統合 AWS WAF」を参照してください。このレコメンデーションについては、「ATP でアプリケーション統合 SDK を使用」を参照してください。

AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) の例

このセクションでは、 AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) の実装の一般的なユースケースに対応できる設定例を示します。

各例は、ユースケースの説明を提供し、カスタム設定ルールの JSON リストにそのソリューションを示します。

> **Note**
>
> これらの例に示されているような JSON リストは、コンソール保護パック (ウェブ ACL) JSON ダウンロードやルール JSON エディタを介して、または API やコマンドラインインターフェイスでの `getWebACL` オペレーションを介して取得できます。

トピック

- ATP の例: シンプルな設定
- ATP の例: 認証情報の不足および侵害された認証情報のカスタム処理
- ATP の例: レスポンス検査の設定

ATP の例: シンプルな設定

次の JSON リストは、 AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) マネージドルールグループを使用した保護パック (ウェブ ACL) の例を示しています。追加のサインインページ設定は、ルールグループがログインリクエストをモニタリングおよび管理するために必要な情報を提供することにご注意ください。この JSON には、ラベル名前空間や保護パック (ウェブ ACL) のアプリケーション統合 URL など、保護パック (ウェブ ACL) の自動生成された設定が含まれます。

```
{
    "WebACL": {
        "LabelNamespace": "awswaf:111122223333:webacl:ATPModuleACL:",
        "Capacity": 50,
        "Description": "This is a test protection pack (web ACL) for ATP.",
        "Rules": [
            {
                "Priority": 1,
                "OverrideAction": {
                    "None": {}
                },
                "VisibilityConfig": {
                    "SampledRequestsEnabled": true,
                    "CloudWatchMetricsEnabled": true,
                    "MetricName": "AccountTakeOverValidationRule"
                },
                "Name": "DetectCompromisedUserCredentials",
                "Statement": {
                    "ManagedRuleGroupStatement": {
                        "VendorName": "AWS",
                        "Name": "AWSManagedRulesATPRuleSet",
                        "ManagedRuleGroupConfigs": [
                          {
                            "AWSManagedRulesATPRuleSet": {
                              "LoginPath": "/web/login",
                              "RequestInspection": {
                                "PayloadType": "JSON",
                                "UsernameField": {
                                  "Identifier": "/form/username"
                                },
                                "PasswordField": {
                                  "Identifier": "/form/password"
                                }
                              },
```

```
                            "EnableRegexInPath": false
                        }
                    }
                ]
            }
        }
    ],
    "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "ATPValidationAcl"
    },
    "DefaultAction": {
        "Allow": {}
    },
    "ManagedByFirewallManager": false,
    "RetrofittedByFirewallManager": false,
    "Id": "32q10987-65rs-4tuv-3210-98765wxyz432",
    "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
ATPModuleACL/32q10987-65rs-4tuv-3210-98765wxyz432",
    "Name": "ATPModuleACL"
},
"ApplicationIntegrationURL": "https://9z87abce34ea.us-
east-1.sdk.awswaf.com/9z87abce34ea/1234567a1b10/",
"LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
}
```

ATP の例: 認証情報の不足および侵害された認証情報のカスタム処理

デフォルトでは、ルールグループ AWSManagedRulesATPRuleSet によって実行される認証情報チェックは次のようにウェブリクエストを処理します。

- 認証情報の不足 – リクエストにラベルを付けてブロックします。
- [Compromised credentials] (侵害された認証情報) - リクエストにラベルを付けますが、ブロックしたりカウントしたりしません。

ルールグループとルールの動作の詳細については、「AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループ」を参照してください。

次の手順を実行して、認証情報が不足している、または侵害されたウェブリクエストのカスタム処理を追加できます。

- **MissingCredential** ルールを Count にオーバーライド — このルールアクションのオーバーライドにより、ルールは一致するリクエストをカウントしてラベル付けのみします。
- カスタム処理でラベル一致ルールの追加 – 両方の ATP ラベルと照合し、カスタム処理を実行するようにルールを設定します。例えば、顧客をサインアップページにリダイレクトできます。

次のルールは、MissingCredential ルールアクションがカウントするようにオーバーライドされた状態で、前の例の ATP マネージドルールグループを示しています。これにより、ルールはリクエストをブロックするのではなく、一致するリクエストにラベルを適用し、リクエストのみをカウントします。

```
"Rules": [
    {
        "Priority": 1,
        "OverrideAction": {
            "None": {}
        },
        "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "AccountTakeOverValidationRule"
        },
        "Name": "DetectCompromisedUserCredentials",
        "Statement": {
            "ManagedRuleGroupStatement": {
                "ManagedRuleGroupConfigs": [
                  {
                    "AWSManagedRulesATPRuleSet": {
                      "LoginPath": "/web/login",
                      "RequestInspection": {
                        "PayloadType": "JSON",
                        "UsernameField": {
                          "Identifier": "/form/username"
                        },
                        "PasswordField": {
                          "Identifier": "/form/password"
                        }
                      },
                      "EnableRegexInPath": false
                    }
                  }
                ]
```

```
                "VendorName": "AWS",
                "Name": "AWSManagedRulesATPRuleSet",
                "RuleActionOverrides": [
                  {
                    "ActionToUse": {
                      "Count": {}
                    },
                    "Name": "MissingCredential"
                  }
                ],
                "ExcludedRules": []
            }
        }
    }
],
```

この設定では、このルールグループは、認証情報が不足し、または侵害されたウェブリクエストを評価すると、リクエストにラベルを付けますが、ブロックすることはありません。

次のルールは、前のルールグループよりも優先順位が高く設定されています。 AWS WAF は、優先順位の低いルールから順番に評価するため、このルールはルールグループの後に評価されます。認証情報のラベルのどちらかと照合し、一致するリクエストにカスタムレスポンスを送信するようにルールが設定されています。

```
"Name": "redirectToSignup",
      "Priority": 10,
      "Statement": {
        "OrStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:atp:signal:missing_credential"
              }
            },
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:atp:signal:credential_compromised"
              }
            }
          ]
        }
```

```
      },
      "Action": {
        "Block": {
          "CustomResponse": {
             your custom response settings
          }
        }
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "redirectToSignup"
      }
```

ATP の例: レスポンス検査の設定

次の JSON リストは、オリジンレスポンスを検査するように設定された AWS WAF Fraud Control Account Takeover Prevention (ATP) マネージドルールグループを含む保護パック (ウェブ ACL) の例を示しています。成功とレスポンスステータスコードを指定する応答検査設定を注意してください。ヘッダー、ボディ、ボディの JSON 一致に基づいて成功とレスポンスの設定を構成することもできます。この JSON には、ラベル名前空間や保護パック (ウェブ ACL) のアプリケーション統合 URL など、保護パック (ウェブ ACL) の自動生成された設定が含まれます。

> **Note**
>
> ATP レスポンス検査は、CloudFront ディストリビューションが保護されている保護パック (ウェブ ACL) でのみ使用できます。

```
{
    "WebACL": {
        "LabelNamespace": "awswaf:111122223333:webacl:ATPModuleACL:",
        "Capacity": 50,
        "Description": "This is a test protection pack (web ACL) for ATP.",
        "Rules": [
            {
                "Priority": 1,
                "OverrideAction": {
                    "None": {}
                },
```

```
                "VisibilityConfig": {
                    "SampledRequestsEnabled": true,
                    "CloudWatchMetricsEnabled": true,
                    "MetricName": "AccountTakeOverValidationRule"
                },
                "Name": "DetectCompromisedUserCredentials",
                "Statement": {
                    "ManagedRuleGroupStatement": {
                        "VendorName": "AWS",
                        "Name": "AWSManagedRulesATPRuleSet",
                        "ManagedRuleGroupConfigs": [
                          {
                            "AWSManagedRulesATPRuleSet": {
                              "LoginPath": "/web/login",
                              "RequestInspection": {
                                "PayloadType": "JSON",
                                "UsernameField": {
                                  "Identifier": "/form/username"
                                },
                                "PasswordField": {
                                  "Identifier": "/form/password"
                                }
                              },
                              "ResponseInspection": {
                                "StatusCode": {
                                  "SuccessCodes": [
                                    200
                                  ],
                                  "FailureCodes": [
                                    401
                                  ]
                                }
                              },
                              "EnableRegexInPath": false
                            }
                          }
                        ]
                    }
                }
            }
        ],
        "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
```

```
            "MetricName": "ATPValidationAcl"
        },
        "DefaultAction": {
            "Allow": {}
        },
        "ManagedByFirewallManager": false,
        "RetrofittedByFirewallManager": false,
        "Id": "32q10987-65rs-4tuv-3210-98765wxyz432",
        "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
ATPModuleACL/32q10987-65rs-4tuv-3210-98765wxyz432",
        "Name": "ATPModuleACL"
    },
    "ApplicationIntegrationURL": "https://9z87abce34ea.us-
east-1.sdk.awswaf.com/9z87abce34ea/1234567a1b10/",
    "LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
}
```

AWS WAF ボットコントロール

このセクションでは、Bot Control の仕様について説明します。

Bot Control を使用すると、スクレーパー、スキャナ、クローラ、ステータスモニター、検索エンジンなどのボットを簡単にモニタリング、ブロック、レート制限の適用ができます。ルールグループの対象検査レベルを使用する場合、自己識別しないボットにチャレンジを仕掛けることができるため、悪意のあるボットがウェブサイトを狙うことが難しくなり、ボットの運用コストも高くなります。Bot Control マネージドルールグループのみを使用するか、他の AWS マネージドルールルールグループや独自のカスタム AWS WAF ルールと組み合わせてアプリケーションを保護することができます。

Bot Control は AI トラフィックの収益化も提供します。これにより、AI ボットとエージェントにコンテンツアクセスの料金を請求できます。Monetize アクションでルールを追加すると、Bot Control ラベルを使用して、ボットのアイデンティティと検証ステータスに基づいて料金を区別できます。詳細については、「AI トラフィック収益化」を参照してください。

> **Important**
>
> AI トラフィック収益化ポリシーを実装するために、動作シグナルやリスクベースのシステムなどの複数の検出手法を使用して、インバウンドトラフィックを検査および分類します。これらのメソッドは高い信頼性の分類を提供するように設計されていますが、確率的であり、すべてのボットトラフィックを正しく識別または分類できない場合があります。当社では、精度を高めるために分析方法を継続的にテストおよび更新しています。ライブ収益化を有効

にする前に、テストモードを使用してポリシーが期待される結果を生成することを確認することをお勧めします。

収益化

支払い手順を含む HTTP 402 Payment Required Challenge を返します。クライアントは支払いを完了し、アクセスを取得するためにリクエストを再送信できます。Monetize アクションを使用して、コンテンツアクセスの AI ボットに課金します。Monetize アクションは、Amazon CloudFront ディストリビューションに関連付けられたウェブ ACLs でのみ使用できます。このアクションを使用するには、ウェブ ACL に MonetizationConfig が設定されている必要があります。詳細については、「AI トラフィック収益化」を参照してください。

アクションパラメータの収益化

[Parameter] (パラメータ)	[Required] (必須)	説明
PriceMultiplier	いいえ	基本料金に適用される整数乗数 (1 ~ 100)。デフォルト: 1。

Bot Control には、リクエストサンプリングに基づいて、ボットからの現在のトラフィックの量を示すコンソールダッシュボードが含まれています。Bot Control マネージドルールグループを保護パック (ウェブ ACL) に追加すると、ボットトラフィックに対してアクションを実行したり、アプリケーションへの一般的なボットトラフィックに関する詳細なリアルタイム情報を受け取ったりすることができます。

> **Note**
>
> このマネージドルールグループを使用する場合、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

Bot Control マネージドルールグループには、自己識別ボットにラベルを追加、一般的に望ましいボットを検証、信頼度の高いボットシグネチャを検出する基本かつ共通の保護レベルが用意されています。これにより、ボットトラフィックの共通カテゴリをモニタリングおよび制御できます。

Bot Control ルールグループには、自己識別を行わない高度なボットに対する検出機能が追加された、ターゲットを絞った保護レベルも用意されています。ターゲットを絞った保護では、ブラウザ

調査、フィンガープリント、行動ヒューリスティックなどの検出技術を使用して不正なボットトラフィックを識別します。さらに、ターゲットを絞った保護では、ウェブサイトのトラフィック統計を機械学習で自動的に分析して、ボット関連のアクティビティを検出することもできます。機械学習を有効にすると、 AWS WAF はタイムスタンプ、ブラウザの特性、以前にアクセスした URL など、ウェブサイトのトラフィックに関する統計を使用して Bot Control の機械学習モデルを改善します。

が Bot Control マネージドルールグループに対してウェブリクエスト AWS WAF を評価すると、ボット関連として検出されたリクエストにラベルが付けられます。ラベルには、ボットカテゴリとボット名が含まれます。独自の AWS WAF ルールでこれらのラベルと照合して、処理をカスタマイズできます。Bot Control マネージドルールグループによって生成されるラベルは、Amazon CloudWatch メトリクスと保護パック (ウェブ ACL) ログに含まれます。

AWS Firewall Manager AWS WAF ポリシーを使用して、組織の一部である複数のアカウントのアプリケーション全体に Bot Control マネージドルールグループをデプロイすることもできます AWS Organizations。

Bot Control マネージドルールグループの詳細については、「AWS WAF Bot Control ルールグループ」を参照してください。

適切な保護レベルを選択し、特定のアプリケーションシナリオに対して Bot Control を設定する方法については、「」を参照してくださいユースケースの Bot Control の選択と設定。

AI エージェントのウェブボット認証

AWS WAF Bot Control は、ボットと AI エージェントの暗号化検証方法としてウェブボット認証 (WBA) をサポートするようになりました。WBA は、商用の CloudFront ディストリビューションとリージョンリソースに適用されます AWS リージョン。この機能により、正当な AI クローラとエージェントは、従来のチャレンジレスポンスメカニズムを必要とせずにアイデンティティを証明できます。

バージョン要件: `AWSManagedRulesBotControlRuleSet` Version_4.0 以降。(静的バージョンは明示的に選択する必要があります) 。ラベル分類とルールの動作の詳細については、以下を参照してください。

- AWS WAF Bot Control ルールグループ
- でのウェブリクエストのラベル付け AWS WAF
- AWS マネージドルールの変更ログ

ユースケースの Bot Control の選択と設定

Bot Control は、さまざまな自動脅威から保護します。適切な設定は、保護対象と直面する脅威によって異なります。このトピックでは、適切な保護レベルを選択し、一般的なアプリケーションシナリオに合わせて Bot Control を設定します。

Bot Control をアプリケーションに一致させる

ボットの脅威は通常、次の 3 つのカテゴリに分類されます。

- 不正の脅威 – 認証情報のスタッフィング、フェイクアカウント、自動購入。
- コンテンツの脅威 — 料金データ、製品カタログ、公開済みコンテンツのスクレイピング。
- 可用性の脅威 – パフォーマンスの低下やインフラストラクチャコストの増加につながるボットトラフィック量。

これらの脅威のほとんどについては、クライアントアプリケーション統合 SDKs でターゲットを絞った保護レベルをお勧めします。次のシナリオでは、 ごとに Bot Control を設定する方法について説明します。

ログインページとアカウントページの保護

認証情報スタッフィングとアカウント乗っ取り攻撃では、自動ツールを使用して、盗まれた認証情報をログインエンドポイントに対してテストします。アカウント作成の不正は、ボットを使用して大規模なフェイクアカウントを作成します。アプリケーション統合 SDK をサイト全体で統合し、ログインとアカウント作成の保護のために Bot Control を AWS WAF Fraud Control マネージドルールグループとペアリングします。

製品カタログと料金データの保護

アプリケーションが製品情報、料金、在庫レベル、またはその他の競合データを表示する場合、ボットはこのコンテンツをスクレイプして競合相手のインテリジェンスをフィードしたり、比較サイトを構築したり、料金を削減したりすることがあります。これらのスクレイパーは、多くの場合、実際のブラウザを模倣し、検出を避けるために住宅用 IP アドレスをローテーションします。Bot Control をチェックアウトだけでなく、製品ページとカタログページに適用します。これにより、ボットが通常のブラウザのように見えても、Bot Control は自動スクレイピングの動作パターンを検出できます。

公開されたコンテンツの保護

コンテンツパブリッシャー、ニュースサイト、メディアプラットフォームは、記事、イメージ、その他のオリジナルコンテンツをコピーするボットに直面します。このコンテンツの盗難により、検索

ランキングが減り、広告収益が減少し、競争力が損なわれる可能性があります。コンテンツページ全体に Bot Control を適用します。Bot Control ダッシュボードを使用して、コンテンツにアクセスしているボットをモニタリングし、各カテゴリの処理方法を決定します。詳細については、「AWS WAF Bot Control コンポーネント」を参照してください。

不要なクローラによるインフラストラクチャコストの削減

スクレイパー、クローラ、自動ツールは、ビジネス価値を提供することなく、大量のトラフィックを生成し、コンピューティングとデータ転送のコストを増やすことができます。Bot Control は、スクレイパー、HTTP ライブラリ、クローリングフレームワークなどのカテゴリ別に自己宣言ボットを識別します。その後、ラベルを使用して各カテゴリを個別にブロックまたはレート制限できます。回避的スクレイピングの場合、ターゲットを絞った保護は、住宅用プロキシやヘッドレスブラウザを使用しているボットなど、アイデンティティを偽装するボットを検出します。

高価値トランザクションの保護

チェックアウトフロー、限定在庫購入、チケット販売は、正当な顧客と競合する自動購入ボットのターゲットです。Bot Control は、Selenium や Puppeteer などの自動ブラウザを検出し、セッションレベルのレート制限を適用して、単一のクライアントがインベントリを独占しないようにします。トランザクションページに SDKs を統合して、最も強力な検出精度を実現します。

AI クローラの管理とデータスクレイパーのトレーニング

AI ボットはアプリケーションからコンテンツを収集して、AI アプリケーションのモデルをトレーニングしたり、データを表面化したりします。Bot Control は、既知の AI ボットを分類します。検証済み検索エンジンクローラなど、許可する特定の AI ボットを許可するカスタムルールを作成し、他のボットをブロックまたはレート制限します。ブラウザ自動化フレームワークを使用してアプリケーションとやり取りする AI エージェントの場合、Bot Control はこれらの自動セッションを検出してチャレンジします。Web Bot Authentication (WBA) を使用すると、正当な AI エージェントは自分のアイデンティティを暗号的に証明できます。これにより、認可されたエージェントと認可されていないエージェントを区別するための信頼性の高いシグナルが得られます。WBA の詳細については、「」を参照してくださいAI エージェントのウェブボット認証。

モバイルアプリケーションの保護

モバイルアプリケーションはウェブアプリケーションと同様のボットの脅威に直面しますが、トラフィックの特性は異なります。モバイルクライアントはブラウザ以外のユーザーエージェントを使用します。ネイティブモバイルアプリケーションフレームワークからの HTTP リクエストは Bot Control `SignalNonBrowserUserAgent`ルールから除外されますが、非標準の HTTP ライブラリとアプリケーション内ブラウザは除外されません。 AWS WAF Mobile SDK を iOS または Android ア

プリケーションに統合して、ターゲットを絞った保護が正確な検出に使用するクライアント側のトークンを提供します。

共通保護とターゲット保護の選択

Bot Control には 2 つの保護レベルがあります。以下のガイダンスは、アプリケーションに適したレベルを選択するのに役立ちます。

一般的な保護レベル

一般的な保護は、ユーザーエージェント文字列、IP アドレス、およびその他のリクエスト特性を通じて自分自身を識別するボットを検出します。既知の組織 (検索エンジンなど) からのボットであると主張するボットが実際にそれらの組織からのものであることを確認します。一般的な保護により、誰がアプリケーションにアクセスしているかを可視化し、各ボットカテゴリを個別に制御できます。SDKs は不要で、リクエストあたりのコストが低くなります。一般的な保護は、検索エンジンのクローラを許可しながら不要なスクレイパーをブロックするなど、既知のボットトラフィックを主に管理する必要がある場合の良い出発点です。

ターゲットを絞った保護レベル

ターゲットを絞った保護レベルは、一般的な保護レベルが検出するすべてを検出し、自己識別しないボットの検出を追加します。ブラウザ調査、TLS フィンガープリント、動作ヒューリスティック、機械学習を使用して、自動クライアントを人間と区別します。機械学習は、タイムスタンプ、ブラウザの特性、ナビゲーション動作など、特定のウェブサイトのトラフィックパターンを分析します。トラフィックの変化やボットの戦術の変化に応じて、検出を更新します。ターゲットを絞った保護は、認証情報のスタッフィング、高度なスクレイピング、自動購入、または攻撃者が検出を積極的に回避しようとするボットアクティビティに直面するアプリケーションに推奨されます。

ほとんどの本稼働ウェブアプリケーションでは、ターゲットを絞った保護をお勧めします。特定のシナリオのターゲットを絞った保護を設定するガイダンスについては、「」を参照してくださいBot Control をアプリケーションに一致させる。トラフィック量が多い場合のコスト管理のガイダンスについては、「」を参照してくださいのコスト管理。

	共通	Targeted
自己識別ボットを検出する	はい	はい
正当なボット (検索エンジン、モニタリングサービス) を検証する	はい	はい

	共通	Targeted
ID を非表示にするボットを検出します	いいえ	はい
トラフィックに合わせた機械学習	いいえ	はい
セッションレベルのレート制限	いいえ	はい
ブラウザ自動化ツールを検出する	はい (自己識別)	はい (回避的を含む)
クライアントアプリケーション統合 SDKs	不要	強く推奨

ルールグループバージョンの確認

Bot Control マネージドルールグループは、時間の経過とともに新しい検出機能で更新されます。現在使用しているバージョンと、新しい静的バージョンが使用可能かどうかを確認します。新しいバージョンには、新しいボットの脅威に対するカバレッジを向上させる追加の検出が含まれています。利用可能なバージョンとその変更については、「」を参照してくださいAWS マネージドルールの変更ログ。

Bot Control 検出の仕組み

Bot Control は、評価されるすべてのリクエストを、ボット名、カテゴリ、組織、検証ステータスなどの詳細な分類でラベル付けします。これらのラベルに一致するルールを記述して、ボットのタイプごとに実行するアクションを決定します。これにより、すべてのボットトラフィックに対する単一のallow-or-blockの決定ではなく、完全な制御が可能になります。

ターゲットを絞った保護レベルでは、Bot Control は複数の検出手法を組み合わせます。これには、署名マッチング、ブラウザ調査、TLS フィンガープリント、動作ヒューリスティック、ウェブサイトのトラフィックパターンに調整された機械学習が含まれます。ある手法を回避するボットは、別の手法でキャッチされる可能性があります。機械学習は、調整されたボットアクティビティも検出します。これは、個々のリクエスト分析が見逃す方法で複数のクライアントが連携するパターンです。すべての Bot Control コンポーネントの詳細については、「」を参照してくださいAWS WAF Bot Control コンポーネント。クライアントと 間の Challengeおよび CAPTCHAインタラクションの仕組みのチュートリアルについては AWS WAF、「」を参照してくださいCAPTCHA および ChallengeのAWS WAF。

のコスト管理

Bot Control マネージドルールグループの使用コストは、 がそれで AWS WAF 評価するウェブリクエストの数に応じて増加します。ほとんどのアプリケーションでは、Bot Control のコストは Bot Control が提供する保護によって正当化されます。ボットトラフィックをブロックすると、多くの場合、検査自体のコストよりもコンピューティング、帯域幅、データ転送のコストが削減されます。コストをさらに最適化する必要がある場合は、以下の戦略が役立ちます。

静的アセットを除外する

最も簡単なコスト最適化は、`.css`、、`.png`、 などの静的ファイルタイプのリクエストを `.jpg` `.svg` Bot Control 検査から除外することです。アプリケーションデータと機能をターゲットとするボットは、スタイルシートやイメージではなく、動的なエンドポイントにヒットします。これにより、検出効率を低下させることなく、検査されたリクエストが削減されます。例については、Bot Control の例: 動的コンテンツにのみ Bot Control を使用するを参照してください。

効率のための注文ルール

Bot Control マネージドルールグループの前に、より安価なルールを保護パック (ウェブ ACL) に配置します。IP 評価リスト、地理的制限、レートベースのルールなどのルールは、有料の Bot Control 検査に到達する前に、明らかに不要なトラフィックをブロックできます。以前のルールによってブロックされたリクエストは Bot Control によって評価されないため、リクエストごとの追加料金は発生しません。

必要に応じて特定のエンドポイントにスコープする

一部のアプリケーションでは、Bot Control をサイトの特定の部分にのみ適用できます。たとえば、アプリケーションに機密データや貴重なコンテンツが含まれていない公開情報セクションがある場合は、検査から除外できます。製品カタログ、料金データ、公開された記事など、保護する価値のあるコンテンツを含むページを除外しないように注意してください。例については、Bot Control の例: ログインページにのみ Bot Control を使用しますを参照してください。

クライアントアプリケーション統合 SDKsの統合

JavaScript と Mobile SDKs を使用して、ターゲットを絞った保護の効果を最大化します。SDKs は、ターゲットルールがセッションレベルの検出に使用するブラウザフィンガープリント、チャレンジトークン管理、動作テレメトリを提供します。ここでのセッションは、特定のブラウザまたはデバイスを表す SDK が取得するクライアントトークンによって識別されます。SDKs がない場合、ターゲットを絞った保護は操作するコンテキストがはるかに少なく、高度なボットを正当なユーザーと確実に区別することはできません。

最初から SDK を統合する

ターゲットを絞った保護をデプロイするときSDKs を同時に統合します。これは、本番環境にデプロイするか、テスト環境で Bot Control を評価するかにかかわらず適用されます。SDKs を使用せずにターゲットを絞った保護を評価しても、その検出機能を正確に把握することはできません。ターゲットを絞ったルールの多くは、SDKs だけが提供するクライアント側のシグナルに依存するためです。

広範な統合を推奨

最も強力な検出を行うには、ログインやチェックアウトだけでなく、動的コンテンツを提供するすべてのページで JavaScript SDK を統合します。Bot Control は、リクエストのタイミング、ページシーケンス、インタラクションパターンなど、クライアントがアプリケーションをナビゲートする方法から動作プロファイルを構築します。SDK が 1 ページのみに存在する場合、Bot Control の動作コンテキストは限られており、実際のユーザーを 1 ページのロードを模倣することを学習したボットと区別できます。統合を拡張することで、Bot Control は各クライアントセッションをより詳細に把握できるため、住宅用プロキシボットネットなどの高度なボットの検出が向上します。少なくとも、SDK を最も重要なページに統合しますが、これを終了状態ではなく開始点として扱います。

モバイルアプリケーション

iOS および Android アプリケーションの場合は、 AWS WAF Mobile SDK を使用します。Mobile SDK は、アプリ内のトークンの取得と更新を処理します。SDK の詳細については、「でのクライアントアプリケーション統合 AWS WAF」を参照してください。

一般的な設定調整

ほとんどの Bot Control デプロイでは、アプリケーショントラフィックの特定の特性に合わせて設定を調整する必要があります。以下は最も一般的な調整です。

モニタリングツールとヘルスチェックツールの許可

内部モニタリングツール、アップタイムチェッカー、ロードバランサーのヘルスチェックは、Bot Control がボットアクティビティとして識別する自動トラフィックを生成します。ソース IP アドレス範囲に一致するスコープダウンステートメントまたはモニタリングツールに含まれるカスタムヘッダーを使用して、これらのリクエストを Bot Control 検査から除外します。

アプリケーション内ブラウザと非標準 HTTP ライブラリの除外

ユーザーがソーシャルメディアアプリから開かれたリンクなど、アプリ内ブラウザを介してサイトにアクセスする場合、またはモバイルアプリが標準以外の HTTP ライブラリを使用している場合、

これらのクライアントがSignalNonBrowserUserAgentルールをトリガーすることがあります。標準のネイティブモバイルフレームワークはこのルールから除外されますが、ブラウザ以外の他のユーザーエージェントは除外されません。これらのクライアントの Bot Control ルールグループでユーザーエージェント例外を設定します。例については、Bot Control の例: ブロックされたユーザーエージェントの例外を作成するを参照してください。

検証済みボットクローラの管理

Bot Control では、検証済みボットがデフォルトで許可されます。検証済みのクローラもレート制限する場合は、例えば、攻撃的だが正当な検索エンジンのクローリングによる負荷を軽減するために、ボットラベルを使用して、特定の検証済みボットカテゴリのリクエストレートを制限するカスタムレートベースのルールを記述します。例については、Bot Control の例: 検証済みボットを明示的に許可するを参照してください。

ボットシグナルをオリジンに転送する

Bot Control 分類ラベルをカスタムリクエストヘッダーとしてアプリケーションに渡すことができます。その後、オリジンはラベルを使用して、疑わしいスクレイパーに簡略化されたコンテンツを提供したり、独自の分析でボットアクティビティを記録したり、誤検出レポートのためにブロックページにリクエスト識別子を含めることができます。 AWS WAF カスタムリクエストヘッダー機能を使用して、ラベル一致に基づいてヘッダーを挿入します。ヘッダーの動的ラベル値の詳細については、「」を参照してくださいでカスタマイズされたウェブリクエストとレスポンス AWS WAF。

ステップアップ認証のトリガー

疑わしいトラフィックを完全にブロックする代わりに、Bot Control シグナルをアプリケーションに転送し、それらを使用して追加の検証をトリガーできます。例えば、Bot Control がセッションを疑わしいものとしてラベル付けする場合、アプリケーションは多要素認証を要求したり、機密性の高いアクションを完了する前に追加の検証ステップを提示したりできます。ステップアップ認証は、自動脅威から保護しながら、誤検出の影響を軽減します。カスタムリクエストヘッダーを使用して、関連する Bot Control ラベルをオリジンに渡します。

強制前のテスト

最初に Bot Control をカウントモードでデプロイします。カウントモードでは、Bot Control はすべてのリクエストにラベルを付けますが、トラフィックをブロックしません。 AWS WAF ログのラベルを確認して、Bot Control がトラフィックで検出した内容を理解し、正当なトラフィックに誤ったラベルが付けられていないことを確認し、検出精度に確信が持てたらブロックモードに切り替えます。テストとデプロイの詳細については、「」を参照してくださいAWS WAF Bot Control のテストとデプロイ。

CDN またはリバースプロキシの背後へのデプロイ

アプリケーションがサードパーティー CDN の背後にある場合、 AWS WAF はデフォルトで CDN の IP アドレスをクライアントと見なします。Bot Control マネージドルールグループは、Amazon CloudFront、Cloudflare、および" からのトラフィックを自動的に認識し、代わりに CDN の標準クライアント IP ヘッダーから発信されたクライアント IP を使用します。一般的な保護レベルとターゲットを絞った保護レベルの両方で、セッションレベルのレート制限や、正確なクライアント ID に依存するターゲットを絞ったボット検出ルールなど、この検出が使用されます。これらの CDNs の Bot Control ルールグループで追加の転送された IP 設定は必要ありません。カスタム IP セット一致、地理的一致、ASN 一致、レートベースのルールなど、IP アドレスを使用する保護パック (ウェブ ACL) 内の他のルールステートメントについては、アップストリームクライアント IP を評価する場合は、転送された IP 設定で設定します。転送された IP アドレスの詳細については、「」を参照してくださいで転送された IP アドレスを使用する AWS WAF。アプリケーションが別のリバースプロキシまたは Bot Control が自動的に認識しない CDN の背後にある場合は、 などのヘッダーでクライアント IP を転送するようにリバースプロキシを設定し、IP アドレスを評価するルールステートメントで転送された IP 設定`X-Forwarded-For`を使用します。

AWS WAF Bot Control コンポーネント

Bot Control の実装の主なコンポーネントは次のとおりです。

- **`AWSManagedRulesBotControlRuleSet`** – さまざまなカテゴリのボットを検出して処理するルールを持つ Bot Control マネージドルールグループ。このルールグループは、ボットトラフィックとして検出されたウェブリクエストにラベルを追加します。

  > **Note**
  >
  > このマネージドルールグループを使用する場合、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

  Bot Control マネージドルールグループには、次の 2 レベルの保護から選択できます。

  - 共通 – ウェブスクレイピングフレームワーク、検索エンジン、自動ブラウザなど、さまざまな自己識別ボットを検出します。このレベルの Bot Control 保護は、静的リクエストデータ分析など、従来のボット検出技術を使用して一般的なボットを識別します。ルールはこれらのボットからのトラフィックにラベルを付け、検証できないものはブロックします。
  - ターゲットを絞った – 一般的な保護機能に加え、自己識別を行わない高度なボットに対するターゲットを絞った検出機能も追加されています。ターゲットを絞った保護は、レート制限と

CAPTCHA およびバックグラウンドブラウザのチャレンジの組み合わせを使用してボットアクティビティを軽減します。

- **TGT_** – ターゲットを絞った保護を提供するルールには、TGT_ で始まる名前が付いています。すべてのターゲットを絞った保護では、ブラウザ調査、フィンガープリント、行動ヒューリスティックなどの検出技術を使用して不正なボットトラフィックを識別します。
- **TGT_ML_** – 機械学習を使用するターゲットを絞った保護のルールには、TGT_ML_ で始まる名前が付いています。これらのルールでは、ウェブサイトトラフィック統計の自動機械学習分析を使用して、分散された調整されたボットアクティビティを示す異常な動作を検出します。 は、タイムスタンプ、ブラウザの特性、以前にアクセスした URL などのウェブサイトトラフィックに関する統計 AWS WAF を分析し、Bot Control 機械学習モデルを改善します。機械学習機能はデフォルトで有効になっていますが、ルールグループ設定で無効にすることができます。機械学習が無効になっている場合、 AWS WAF はこれらのルールを評価しません。

ルールグループルールに関する情報を含む詳細については、「AWS WAF Bot Control ルールグループ」を参照してください。

マネージドルールグループ参照ステートメントを使用して、このルールグループを保護パック (ウェブ ACL) に含め、使用する検査レベルを指定します。ターゲットレベルでは、機械学習を有効にするかどうかも指定します。このマネージドルールグループを保護パック (ウェブ ACL) に追加する方法については、「AWS WAF Bot Control マネージドルールグループをウェブ ACL に追加する」を参照してください。

- [Bot Control dashboard] (Bot Control ダッシュボード) – 保護パック (ウェブ ACL) のボットモニタリングダッシュボード。保護パック (ウェブ ACL) Bot Control のタブから利用できます。トラフィックをモニタリングし、さまざまなタイプのボットからのトラフィックの量を理解するために、このダッシュボードを使用します。これは、このトピックで説明するように、ボット管理をカスタマイズするための開始点とすることができます。また、これを使用して、変更を検証し、さまざまなボットやボットカテゴリのアクティビティをモニタリングすることもできます。
- AI トラフィック分析ダッシュボード – 詳細な AI ボットとエージェントのアクティビティ分析専用のダッシュボード。保護パック (ウェブ ACL) AI トラフィック分析タブから入手できます。標準の Bot Control メトリクスを超えた AI 固有のトラフィックパターン、ボットインテント、アクセス動作の可視性を強化します。
- JavaScript とモバイルアプリケーションの統合 SDKs – Bot Control ルールグループのターゲットを絞った保護レベルを使用する場合は、 AWS WAF JavaScript とモバイル SDKs を実装する必要があります。ターゲットルールは、クライアントトークン内で SDK から提供された情報を使用し、悪意のあるボットに対する検出を強化します。SDK の詳細については、「でのクライアントアプリケーション統合 AWS WAF」を参照してください。

- ログ記録とメトリクス – AWS WAF ログ、Amazon Security Lake、Amazon CloudWatch で保護パック (ウェブ ACL) 用に収集されたデータを調査することで、ボットトラフィックをモニタリングし、Bot Control マネージドルールグループがトラフィックを評価して処理する方法を理解できます。Bot Control がウェブリクエストに追加するラベルは、そのデータに含まれています。これらのオプションの詳細については、ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック、Amazon CloudWatch によるモニタリング、及び「What is Amazon Security Lake?」を参照してください。

  ニーズと確認できるトラフィックに応じて、Bot Control の実装をカスタマイズできます。最も一般的に使用されるオプションの一部は次のとおりです。

- スコープダウンステートメント – Bot Control マネージドルールグループの参照ステートメント内にスコープダウンステートメントを追加することにより、Bot Control マネージドルールグループが評価するウェブリクエストからの一部トラフィックを除外できます。スコープダウンステートメントは、ネスト可能なルールステートメントとすることができます。リクエストがスコープダウンステートメントと一致しない場合、 は、ルールグループに対して AWS WAF 評価せずに、ルールグループ参照ステートメントと一致していないと評価します。スコープダウンステートメントの詳細については、「でのスコープダウンステートメントの使用 AWS WAF」を参照してください。

  Bot Control マネージドルールグループを使用するためのコストは、 AWS WAF がルールグループを使用して評価するウェブリクエスト数に応じて上がります。スコープダウンステートメントを使用してルールグループが評価するリクエストを制限することで、これらのコストを削減できます。たとえば、ボットを含むすべてのユーザーにホームページのロードを許可し、その後にアプリケーション API に送信されるリクエスト、あるいは特定のタイプのコンテンツを含むリクエストにルールグループのルールを適用できます。

- ラベルとラベル一致ルール – Bot Control ルールグループが AWS WAF ラベル一致ルールステートメントを使用して識別するボットトラフィックの一部を処理する方法をカスタマイズできます。Bot Control ルールグループは、ウェブリクエストにラベルを追加します。Bot Control ラベルと一致する Bot Control ルールグループの後にラベル一致ルールを追加し、必要な処理を適用できます。ラベル付けおよびラベル一致ステートメントの使用の詳細については、「ラベル一致ルールステートメント」および「でのウェブリクエストのラベル付け AWS WAF」を参照してください。

- カスタムリクエストとレスポンス – カスタムヘッダーを許可したリクエストに追加し、ラベルマッチングをカスタムリクエストとレスポンス機能と組み合わせることで、ブロックしたリクエストに AWS WAF カスタムレスポンスを送信できます。動的ラベル補間では、${namespace:} 構文を使用して、評価時に Bot Control ラベル値を解決できます。その後、1 つのルールでラベル名前空間全体をヘッダー値として転送できます。ラベルごとに 1 つのルールは必要ありません。リクエストとレスポンスをカスタマイズする方法については、「でカスタマイズされたウェブリクエス

トとレスポンス AWS WAF」を参照してください。動的補間の詳細については、「」を参照してください動的ラベル補間。

Bot Control のアプリケーション統合 SDK の使用

このセクションでは、アプリケーション統合 SDK を Bot Control で使用する方法について説明します。

Bot Control マネージドルールグループのターゲット保護のほとんどには、アプリケーション統合 SDK が生成するチャレンジトークンが必要です。リクエストにチャレンジトークンを必要としないルールは、Bot Control の共通レベルの保護とターゲットレベルの機械学習ルールです。ルールグループの保護レベルとルールの説明については、「AWS WAF Bot Control ルールグループ」を参照してください。

Bot Control ルールグループを最も効果的に使用するためにも、アプリケーション統合 SDK を実装することを強くお勧めします。チャレンジスクリプトが取得するトークンからのメリットを Bot Control ルールグループが得るには、Bot Control ルールグループの前にチャレンジスクリプトを実行する必要があります。

少なくとも、ログイン、チェックアウト、アカウント作成などの最も重要なページに JavaScript チャレンジスクリプトタグを追加します。最も強力な検出を行うには、動的コンテンツを提供するページ間で SDK をより広範に統合します。Bot Control の動作データが多いほど、実際のユーザーを高度なボットと区別しやすくなります。統合ガイダンスの詳細については、「」を参照してくださいクライアントアプリケーション統合 SDKsの統合。

- アプリケーション統合 SDK では、スクリプトは自動的に実行されます。
- SDK を使用できない場合は、Bot Control ルールグループが検査するすべてのリクエストに対して Challenge または CAPTCHA ルールアクションを実行するように保護パック (ウェブ ACL) を設定することができます。Challenge または CAPTCHA ルールアクションを使用すると、追加料金が発生する場合があります。料金の詳細については、「AWS WAF の料金」を参照してください。

アプリケーション統合 SDK をクライアントに実装、またはチャレンジスクリプトを実行するルールアクションの 1 つを使用するときは、ルールグループと、クライアントアプリケーションセキュリティ全体の機能が拡張されます。

トークンは、各ウェブリクエストでクライアント情報を提供します。この追加情報により、Bot Control のルールグループは、正規のクライアントセッションと動作の悪いクライアントセッションが両方とも単一の IP アドレスから発信された場合でも、前者を後者から分離できます。ルールグ

ループは、トークン内の情報を使用してクライアントセッションリクエストの動作を集約し、ターゲットを絞った保護レベルが提供する微調整した検出および軽減を実現します。

SDK の詳細については、「でのクライアントアプリケーション統合 AWS WAF」を参照してください。 AWS WAF トークンの詳細については、「」を参照してくださいAWS WAF インテリジェントな脅威の軽減におけるトークンの使用。ルールアクションの情報については、「CAPTCHA および Challengeの AWS WAF」を参照してください。

AWS WAF Bot Control マネージドルールグループをウェブ ACL に追加する

このセクションでは、`AWSManagedRulesBotControlRuleSet` ルールグループを追加および設定する方法について説明します。

Bot Control マネージドルールグループ `AWSManagedRulesBotControlRuleSet` は、実装する保護レベルを特定するための追加設定が必要です。

ルールグループの説明とルールリストについては、「AWS WAF Bot Control ルールグループ」を参照してください。

このガイダンスは、 AWS WAF 保護パック (ウェブ ACL)、ルール、およびルールグループを作成および管理する方法を一般的に認識しているユーザーを対象としています。これらのトピックは、このガイドの前のセクションで力バーされています。マネージドルールグループを保護パック (ウェブ ACL) に追加する方法の基本については、「コンソールを通じた保護パック (ウェブ ACL) へのマネージドルールグループの追加」を参照してください。

ベストプラクティスに従う

Bot Control ルールグループは、「でのインテリジェントな脅威軽減のベストプラクティス AWS WAF」に記載されているベストプラクティスに従って使用してください。

保護パック (ウェブ ACL) で **`AWSManagedRulesBotControlRuleSet`** ルールグループを使用するには

1. AWS マネージドルールグループを保護パック (ウェブ ACL) `AWSManagedRulesBotControlRuleSet`に追加します。ルールグループの詳細な説明については、「the section called “Bot Control ルールグループ”」を参照してください。

> **Note**
>
> このマネージドルールグループを使用する場合、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

ルールグループを追加する際は、ルールグループの設定ページを開くように編集します。

2. ルールグループの設定ページの [Inspection level] (検査レベル) ペインで、使用する検査レベルを選択します。

   - 共通 – ウェブスクレイピングフレームワーク、検索エンジン、自動ブラウザなど、さまざまな自己識別ボットを検出します。このレベルの Bot Control 保護は、静的リクエストデータ分析など、従来のボット検出技術を使用して一般的なボットを識別します。ルールはこれらのボットからのトラフィックにラベルを付け、検証できないものはブロックします。
   - ターゲットを絞った – 一般的な保護機能に加え、自己識別を行わない高度なボットに対するターゲットを絞った検出機能も追加されています。ターゲットを絞った保護は、レート制限と CAPTCHA およびバックグラウンドブラウザのチャレンジの組み合わせを使用してボットアクティビティを軽減します。
     - **TGT_** – ターゲットを絞った保護を提供するルールには、TGT_ で始まる名前が付いています。すべてのターゲットを絞った保護では、ブラウザ調査、フィンガープリント、行動ヒューリスティックなどの検出技術を使用して不正なボットトラフィックを識別します。
     - **TGT_ML_** – 機械学習を使用するターゲットを絞った保護のルールには、TGT_ML_ で始まる名前が付いています。これらのルールでは、ウェブサイトトラフィック統計の自動機械学習分析を使用して、分散された調整されたボットアクティビティを示す異常な動作を検出します。 は、タイムスタンプ、ブラウザの特性、以前にアクセスした URL などのウェブサイトトラフィックに関する統計 AWS WAF を分析し、Bot Control 機械学習モデルを改善します。機械学習機能はデフォルトで有効になっていますが、ルールグループ設定で無効にすることができます。機械学習が無効になっている場合、 AWS WAF はこれらのルールを評価しません。
3. ターゲットを絞った保護レベルを使用していて、ウェブトラフィックの分析に機械学習 (ML) AWS WAF を使用しない場合は、機械学習オプションを無効にします。名前が TGT_ML_ で始まる Bot Control ルールでは機械学習が必要になります。これらのルールの詳細については、「Bot Control のルールリスト」を参照してください。
4. ルールグループの使用コストを抑えるスコープダウンステートメントを追加します。スコープダウンステートメントは、ルールグループが検査する一連のリクエストを絞り込みます。ユー

スケースの例として、Bot Control の例: ログインページにのみ Bot Control を使用します および Bot Control の例: 動的コンテンツにのみ Bot Control を使用する で始めてください。

5. ルールグループに必要な追加設定を指定します。
6. 変更を保護パック (ウェブ ACL) に保存します。

本番稼働トラフィックに Bot Control 実装をデプロイする前に、トラフィックへの潜在的な影響に慣れるまで、ステージング環境またはテスト環境でテストおよびチューニングします。その後、ルールを有効にする前に、本番稼働用トラフィックでカウントモードでルールをテストしてチューニングします。ガイダンスについては、次のセクションを参照してください。

AWS WAF Bot Control を使用した誤検出のシナリオ例

このセクションでは、 AWS WAF Bot Control で誤検出が発生する可能性のある状況の例を示します。

誤検出を最小限に抑えるために、 AWS WAF Bot Control マネージドルールグループのルールを慎重に選択しました。グローバルトラフィックに対してルールをテストし、テスト保護パック (ウェブ ACL) に対する影響をモニタリングします。ただし、トラフィックパターンの変化が原因で誤検出が引き続き検出されることがあります。さらに、一部のユースケースは誤検出を引き起こすことが知られており、ウェブトラフィックに特化したカスタマイズが必要になります。

誤検出が発生する可能性のある状況には、次のような例が含まれます。

- 通常、モバイルアプリにはブラウザ以外のユーザーエージェントがあり、`SignalNonBrowserUserAgent` ルールではデフォルトでブロックされます。モバイルアプリからのトラフィックや、ブラウザ以外のユーザーエージェントによるその他の正当なトラフィックが予想される場合は、例外を追加して許可する必要があります。
- アップタイムのモニタリング、統合テスト、マーケティングツールなど、特定のボットトラフィックに依拠する場合があります。許可するボットトラフィックを Bot Control が識別してブロックする場合は、独自のルールを追加して処理を変更する必要があります。これは必ずしもすべてのお客様の誤検出のシナリオではありませんが、誤検出のシナリオに該当する場合、誤検出の場合と同じ処理が必要になります。
- Bot Control マネージドルールグループは、IP アドレスを使用してボットを検証します AWS WAF。Bot Control を使用し、プロキシまたはロードバランサーを介してルーティングするボットを検証した場合は、カスタムルールを使用して明示的に許可する必要がある場合があります。このタイプのカスタムルールを作成する方法については、「で転送された IP アドレスを使用する AWS WAF」を参照してください。

- グローバルに誤検出率が低い Bot Control ルールが特定のデバイスまたはアプリケーションに大きな影響を与える可能性があります。例えば、テストや検証では、トラフィック量の少ないアプリケーションや、あまり一般的でないブラウザまたはデバイスからのリクエストが観察されなかった可能性があります。
- 以前から誤検出率が低い Bot Control ルールで有効なトラフィックの誤検出が増加している可能性があります。これは、新しいトラフィックパターンまたは有効なトラフィックを伴って出現するリクエスト属性が原因となっている可能性があります。これにより、以前は存在していなかったルールと一致するようになる可能性があります。これらの変更は、次のような状況によって発生する可能性があります。
  - ロードバランサーやコンテンツ配信ネットワーク (CDN) など、ネットワークアプライアンスを通じてトラフィックがフローする際に変更されたトラフィックの詳細。
  - トラフィックデータの新たな変化 (新しいブラウザや既存のブラウザの新しいバージョンなど)。

> **Important**
>
> モバイルアプリが標準以外の HTTP ライブラリを使用している場合、またはユーザーがアプリ内ブラウザ (ソーシャルメディアアプリから開かれたリンクなど) を介してサイトにアクセスする場合、これらのクライアントは`SignalNonBrowserUserAgent`ルールをトリガーすることがあります。標準のネイティブモバイルフレームワークはこのルールから除外されますが、ブラウザ以外の他のユーザーエージェントは除外されません。Bot Control をブロックモードで有効にする前に、例外をテストして追加する計画を立ててください。例については、Bot Control の例: ブロックされたユーザーエージェントの例外を作成するを参照してください。

AWS WAF Bot Control マネージドルールグループから発生する可能性のある誤検出を処理する方法については、後のセクション「AWS WAF Bot Control のテストとデプロイ」のガイダンスを参照してください。

AWS WAF Bot Control のテストとデプロイ

このセクションでは、サイトの AWS WAF Bot Control 実装を設定およびテストするための一般的なガイダンスを提供します。実行する具体的なステップは、ニーズ、リソース、受け取るウェブリクエストによって異なります。

この情報は、AWS WAF 保護のテストとチューニング で提供されているテストおよび調整に関する一般情報とは別です。

> **Note**
>
> AWS マネージドルールは、一般的なウェブ脅威から保護するように設計されています。ドキュメントに従って使用すると、 AWS マネージドルールルールグループはアプリケーションに別のセキュリティレイヤーを追加します。ただし、 AWS マネージドルールルールグループは、選択した AWS リソースによって決定されるセキュリティ責任に代わるものではありません。責任共有モデルを参照して、 のリソースが適切に保護 AWS されていることを確認します。

> **本番稼働トラフィックのリスク**
>
> 本番稼働トラフィックに Bot Control 実装をデプロイする前に、トラフィックへの潜在的な影響に慣れるまで、ステージング環境またはテスト環境でテストおよびチューニングします。その後、ルールを有効にする前に、本番稼働用トラフィックでカウントモードでルールをテストしてチューニングします。

このガイダンスは、 AWS WAF 保護パック (ウェブ ACL)、ルール、およびルールグループを作成および管理する方法を一般的に認識しているユーザーを対象としています。これらのトピックは、このガイドの前のセクションでカバーされています。

Bot Control の実装を設定およびテストするには

これらのステップを最初にテスト環境で実行し、次に本番環境で実行します。

1. Bot Control マネージドルールグループを追加する

   > **Note**
   >
   > このマネージドルールグループを使用する場合、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

   マネージド AWS ルールグループ`AWSManagedRulesBotControlRuleSet`を新規または既存の保護パック (ウェブ ACL) に追加し、現在の保護パック (ウェブ ACL) の動作を変更しないように設定します。

   - マネージドルールグループを追加する際には、それを編集し、次の手順を実行します。

- [Inspection level] (検査レベル) ペインで、使用する検査レベルを選択します。
  - 共通 – ウェブスクレイピングフレームワーク、検索エンジン、自動ブラウザなど、さまざまな自己識別ボットを検出します。このレベルの Bot Control 保護は、静的リクエストデータ分析など、従来のボット検出技術を使用して一般的なボットを識別します。ルールはこれらのボットからのトラフィックにラベルを付け、検証できないものはブロックします。
  - ターゲットを絞った – 一般的な保護機能に加え、自己識別を行わない高度なボットに対するターゲットを絞った検出機能も追加されています。ターゲットを絞った保護は、レート制限と CAPTCHA およびバックグラウンドブラウザのチャレンジの組み合わせを使用してボットアクティビティを軽減します。
    - **TGT_** – ターゲットを絞った保護を提供するルールには、TGT_ で始まる名前が付いています。すべてのターゲットを絞った保護では、ブラウザ調査、フィンガープリント、行動ヒューリスティックなどの検出技術を使用して不正なボットトラフィックを識別します。
    - **TGT_ML_** – 機械学習を使用するターゲットを絞った保護のルールには、TGT_ML_ で始まる名前が付いています。これらのルールでは、ウェブサイトトラフィック統計の自動機械学習分析を使用して、分散された調整されたボットアクティビティを示す異常な動作を検出します。 は、タイムスタンプ、ブラウザの特性、以前にアクセスした URL などのウェブサイトトラフィックに関する統計 AWS WAF を分析し、Bot Control 機械学習モデルを改善します。機械学習機能はデフォルトで有効になっていますが、ルールグループ設定で無効にすることができます。機械学習が無効になっている場合、 AWS WAF はこれらのルールを評価しません。

  この選択の詳細については、「AWS WAF Bot Control ルールグループ」を参照してください。
- [Rules] (ルール) ペインで、[Override all rule actions] (すべてのルールアクションをオーバーライド) ドロップダウンを開いて、[Count] を選択します。この設定では、 はルールグループ内のすべてのルールに対するリクエスト AWS WAF を評価し、その結果の一致のみをカウントしながら、リクエストにラベルを追加します。詳細については、「ルールグループ内のルールアクションのオーバーライド」を参照してください。

  このオーバーライドにより、Bot Control ルールがトラフィックに与える潜在的な影響をモニタリングでき、内部のユースケースや目的のボットなどの例外を追加するかどうか判断します。

- 保護パック (ウェブ ACL) で最後に評価されるように、ルールグループを配置します。優先順位の設定の数値は、既に使用している他のルールまたはルールグループよりも高くなります。詳細については、「ルールの優先度を設定する」を参照してください。

  これにより、現在のトラフィックの処理が中断されることはありません。たとえば、SQL インジェクションやクロスサイトスクリプティングなどの悪意のあるトラフィックを検出するルールがある場合、そのようなリクエストを継続的に検出してログ記録します。または、既知の悪意のないトラフィックを許可するルールがある場合、Bot Control マネージドルールグループによってブロックされるようにすることなく、そのトラフィックを許可し続けることができます。テストおよび調整アクティビティ中に処理順序を調整することができますが、開始する方法としてお勧めします。

2. 保護パック (ウェブ ACL) のサンプリング、ログ記録、およびメトリクスの有効化

   必要に応じて、保護パック (ウェブ ACL) のログ記録、Amazon Security Lake データ収集、リクエストサンプリング、Amazon CloudWatch メトリクスを設定します。これらの可視化ツールを使用して Bot Control マネージドルールグループとトラフィックとのインタラクションをモニタリングできます。

   - ログ作成の詳細については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。
   - Amazon Security Lake の詳細については、「Amazon Security Lake とは」および「Amazon Security Lake ユーザーガイド」の AWS 「サービスからのデータ収集」を参照してください。
   - Amazon CloudWatch メトリクスの詳細については、「Amazon CloudWatch によるモニタリング」を参照してください。
   - ウェブリクエストサンプリングの詳細については、「ウェブリクエストのサンプルの表示」を参照してください。

3. 保護パック (ウェブ ACL) をリソースに関連付ける

   保護パック (ウェブ ACL) がリソースに関連付けられていない場合は、関連付けます。詳細については、「AWS リソースとの保護の関連付けまたは関連付け解除」を参照してください。

4. トラフィックと Bot Control ルールの一致をモニタリングする

   トラフィックがフローしていることと、Bot Control マネージドルールグループのルールが一致するウェブリクエストにラベルを追加していることを確認します。ログにラベルが表示され、Amazon CloudWatch メトリクスでボットとラベルのメトリクスを確認できます。ログでは、ルールグループでカウントするようにオーバーライドしたルールが、カウントに設定された

`action` と、オーバーライドした設定済のルールアクションを示す `overriddenAction` とともに、`ruleGroupList` に表示されます。

> **Note**
>
> Bot Control マネージドルールグループは、 AWS WAFからの IP アドレスを使用してボットを検証します。Bot Control を使用し、プロキシまたはロードバランサーを介してルーティングするボットを検証した場合は、カスタムルールを使用して明示的に許可する必要がある場合があります。カスタムルールの作成方法については、「で転送された IP アドレスを使用する AWS WAF」を参照してください。ルールを使用して Bot Control ウェブリクエストの処理をカスタマイズする方法については、次のステップを参照してください。

ウェブリクエスト処理を詳細にレビューして、カスタム処理で軽減する必要のある誤検出があるかどうかを確認してください。誤検知の例については、「AWS WAF Bot Control を使用した誤検出のシナリオ例」を参照してください。

5. Bot Control ウェブリクエストの処理をカスタマイズする

   必要に応じて、リクエストを明示的に許可またはブロックする独自のルールを追加して、Bot Control ルールがそのリクエストを処理する方法を変更します。

   これをどのように実行するかはユースケースによって異なりますが、一般的な解決策は次のとおりです。

   - Bot Control マネージドルールグループの前に追加したルールを含むリクエストを明示的に許可します。これにより、許可されたリクエストが評価のためにルールグループに到達することはありません。これは、Bot Control マネージドルールグループの使用コストを抑えるのに役立ちます。
   - Bot Control マネージドルールグループのステートメント内のスコープダウンステートメントを追加し、Bot Control 評価からのリクエストを除外します。これは、前述のオプションと同じように機能します。スコープダウンステートメントと一致しないリクエストがルールグループの評価に到達することはないため、Bot Control マネージドルールグループの使用コストを抑えるのに役立ちます。スコープダウンステートメントの詳細については、「でのスコープダウンステートメントの使用 AWS WAF」を参照してください。

     例については、以下を参照してください。

     - ボット管理からの IP 範囲を除外する

- コントロールしているボットからのトラフィックを許可する

- リクエスト処理に Bot Control ラベルを使用して、リクエストを許可またはブロックします。Bot Control マネージドルールグループの後にラベル一致ルールを追加して、ブロックするリクエストから、許可するラベル付きリクエストをブロックするリクエストを除外します。

  テスト後、関連する Bot Control ルールをカウントモードで維持し、カスタムルールでリクエストの処理に関する決定を維持します。ラベル一致ステートメントの詳細については、「ラベル一致ルールステートメント」を参照してください。

  この種類のカスタマイズの例については、以下を参照してください。

  - ブロックされたユーザーエージェントの例外を作成する
  - 特定のブロックされたボットを許可する
  - 検証済みボットをブロックする

その他の例については、「AWS WAF Bot Control の例」を参照してください。

6. 必要に応じて、Bot Control マネージドルールグループ設定を有効にします

   状況によっては、一部の Bot Control ルールをカウントモードの状態で維持する、あるいは異なるアクションのオーバーライドに適用すると判断する場合があります。ルールグループ内で設定されているときに実行するルールについては、通常のルール設定を有効にします。これを行うには、保護パック (ウェブ ACL) のルールグループステートメントを編集し、[Rules] (ルール) ペインで変更を行います。

AWS WAF Bot Control の例

このセクションでは、 AWS WAF Bot Control 実装のさまざまな一般的なユースケースを満たす設定例を示します。

各例は、ユースケースの説明を提供し、カスタム設定ルールの JSON リストにそのソリューションを示します。

> **Note**
>
> これらの例に示されている JSON リストは、ルールを設定し、Rule JSON エディタを使用して編集することにより、コンソールで作成されました。

トピック

- Bot Control の例: 簡単な設定
- Bot Control の例: 検証済みボットを明示的に許可する
- Bot Control の例: 検証済みボットをブロックする
- Bot Control の例: 特定のブロックされたボットを許可する
- Bot Control の例: ブロックされたユーザーエージェントの例外を作成する
- Bot Control の例: ログインページにのみ Bot Control を使用します
- Bot Control の例: 動的コンテンツにのみ Bot Control を使用する
- Bot Control の例: ボット管理から IP 範囲を除外する
- Bot Control の例: コントロールしているボットからのトラフィックを許可する
- Bot Control の例: ターゲット検査レベルの有効化
- Bot Control の例: 2 つのステートメントを使用してターゲット検査レベルの使用を制限する

Bot Control の例: 簡単な設定

次の JSON リストは、 AWS WAF Bot Control マネージドルールグループを使用した保護パック (ウェブ ACL) の例を示しています。可視性設定に注意してください。これにより、 AWS WAF はモニタリング目的でリクエストサンプルとメトリクスを保存します。

```
{
  "Name": "Bot-WebACL",
  "Id": "...",
  "ARN": "...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "Bot-WebACL",
  "Rules": [
      {
        ...
      },
      {
         "Name": "AWS-AWSBotControl-Example",
         "Priority": 5,
         "Statement": {
            "ManagedRuleGroupStatement": {
               "VendorName": "AWS",
               "Name": "AWSManagedRulesBotControlRuleSet",
```

```
                "ManagedRuleGroupConfigs": [
                  {
                    "AWSManagedRulesBotControlRuleSet": {
                      "InspectionLevel": "COMMON"
                    }
                  }
                ],
                "RuleActionOverrides": [],
                "ExcludedRules": []
             },
             "VisibilityConfig": {
                "SampledRequestsEnabled": true,
                "CloudWatchMetricsEnabled": true,
                "MetricName": "AWS-AWSBotControl-Example"
              }
           }
       }
    ],
    "VisibilityConfig": {
      ...
    },
    "Capacity": 1496,
    "ManagedByFirewallManager": false,
    "RetrofittedByFirewallManager": false
}
```

Bot Control の例: 検証済みボットを明示的に許可する

AWS WAF Bot Control は、 が一般的 AWS で検証可能なボットであることがわかっているボットをブロックしません。Bot Control が検証済みボットからのウェブリクエストを識別すると、ボットに名前を付けるラベルと、検証済みボットであることを示すラベルが追加されます。Bot Control は、既知の正常なボットがブロックされないように、シグナルラベルなどの他のラベルを追加しません。

検証済みボットをブロックする他の AWS WAF ルールがある場合があります。検証済みのボットが確実に許可されるようにするには、Bot Control ラベルに基づいてそれらのボットを許可するカスタムルールを追加します。ラベルを照合できるように、新しいルールは Bot Control マネージドルールグループの後に実行される必要があります。

次のルールは、検証済みボットを明示的に許可します。

```
{
    "Name": "match_rule",
    "Statement": {
```

```
      "LabelMatchStatement": {
        "Scope": "LABEL",
        "Key": "awswaf:managed:aws:bot-control:bot:verified"
      }
    },
    "RuleLabels": [],
    "Action": {
      "Allow": {}
    }
}
```

Bot Control の例: 検証済みボットをブロックする

検証済みのボットをブロックするには、 AWS WAF Bot Control マネージドルールグループの後に実行されるボットをブロックするルールを追加する必要があります。これを行うには、ブロックするボット名を特定し、ラベル一致ステートメントを使用して、それらを識別してブロックします。検証済みのすべてのボットをブロックするだけの場合は、`bot:name:` ラベルとの照合を省略できます。

次のルールは、`bingbot` 検証済みボットのみをブロックします。このルールは、Bot Control マネージドルールグループの後に実行する必要があります。

```
{
    "Name": "match_rule",
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:bot:name:bingbot"
            }
          },
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:bot:verified"
            }
          }
        ]
      }
    },
    "RuleLabels": [],
    "Action": {
```

```
      "Block": {}
    }
  }
```

次のルールは、すべての検証済みボットをブロックします。

```
{
    "Name": "match_rule",
    "Statement": {
      "LabelMatchStatement": {
        "Scope": "LABEL",
        "Key": "awswaf:managed:aws:bot-control:bot:verified"
      }
    },
    "RuleLabels": [],
    "Action": {
      "Block": {}
    }
}
```

Bot Control の例: 特定のブロックされたボットを許可する

複数の Bot Control ルールによってボットがブロックされる可能性があります。各ブロッキングルールについて、次の手順を実行します。

AWS WAF Bot Control ルールがブロックしないボットをブロックしている場合は、次の操作を行います。

1. ログをチェックして、ボットをブロックしている Bot Control ルールを特定します。ブロックルールは、名前が `terminatingRule` で始まるフィールドのログで指定されます。保護パック (ウェブ ACL) ログの詳細については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。ルールがリクエストに追加するラベルに注意してください。
2. 保護パック (ウェブ ACL) で、ブロッキングルールのアクションをカウントするようにオーバーライドします。コンソールでこれを行うには、保護パック (ウェブ ACL) でルールグループのルールを編集し、ルールに Count のルールアクションオーバーライドを選択します。これにより、ボットがルールによってブロックされないようにしても、ルールは一致するリクエストにラベルを適用します。
3. Bot Control マネージドルールグループの後に、保護パック (ウェブ ACL) にラベル一致ルールを追加します。オーバーライドされたルールのラベルと照合し、ブロックしたくないボットを除くすべての一致するリクエストをブロックするようにルールを設定します。

これで、保護パック (ウェブ ACL) が設定され、許可するボットが、ログを通じて特定したブロックルールによってブロックされなくなります。

トラフィックとログをもう一度チェックして、ボットの通過が許可されていることを確認します。許可されていない場合は、上記の手順を再度実行してください。

例えば、pingdom を除くすべてのモニタリングボットをブロックするとします。この場合、CategoryMonitoring ルールがカウントするようにオーバーライドし、その後にボット名ラベル pingdom が付いているものを除くすべてのモニタリングボットをブロックするルールを記述します。

次のルールは、Bot Control マネージドルールグループを使用しますが、CategoryMonitoring のルールアクションがカウントするようにオーバーライドします。カテゴリモニタリングルールは、一致するリクエストに通常どおりラベルを適用しますが、通常のブロックアクションを実行するのではなく、カウントするだけです。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
   "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "CategoryMonitoring"
        }
      ],
      "ExcludedRules": []
    }
  },
```

```
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSBotControl-Example"
  }
}
```

次のルールは、前の CategoryMonitoring ルールが一致するウェブリクエストに追加するカテゴリモニタリングラベルと照合します。カテゴリモニタリングリクエストの中で、このルールはボット名 pingdom のラベルを持つものを除くすべてをブロックします。

次のルールは、保護パック (ウェブ ACL) の処理順序で、前の Bot Control マネージドルールグループの後に実行する必要があります。

```
{
      "Name": "match_rule",
      "Priority": 10,
      "Statement": {
        "AndStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
              }
            },
            {
              "NotStatement": {
                "Statement": {
                  "LabelMatchStatement": {
                    "Scope": "LABEL",
                    "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
                  }
                }
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
```

```
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "match_rule"
      }
}
```

Bot Control の例: ブロックされたユーザーエージェントの例外を作成する

一部のブラウザ以外のユーザーエージェントからのトラフィックが誤ってブロックされている場合は、問題のある AWS WAF Bot Control ルール`SignalNonBrowserUserAgent`をカウントに設定し、ルールのラベル付けを例外条件と組み合わせることで、例外を作成できます。

> **Note**
>
> 通常、モバイルアプリにはブラウザ以外のユーザーエージェントがあり、`SignalNonBrowserUserAgent` ルールではデフォルトでブロックされます。

次のルールは、Bot Control マネージドルールグループを使用しますが、`SignalNonBrowserUserAgent` のルールアクションがカウントするようにオーバーライドします。シグナルルールは、一致するリクエストに通常どおりラベルを適用しますが、通常のブロックアクションを実行するのではなく、カウントするだけです。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
   "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
```

```
          "Name": "SignalNonBrowserUserAgent"
        }
      ],
      "ExcludedRules": []
    }
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSBotControl-Example"
  }
}
```

次のルールは、Bot Control `SignalNonBrowserUserAgent` ルールが一致するウェブリクエストに追加したシグナルラベルと照合します。シグナルリクエストの中では、このルールは当社が許可するユーザーエージェントを持つものを除くすべてをブロックします。

次のルールは、保護パック (ウェブ ACL) の処理順序で、前の Bot Control マネージドルールグループの後に実行する必要があります。

```
{
    "Name": "match_rule",
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:signal:non_browser_user_agent"
            }
          },
          {
            "NotStatement": {
              "Statement": {
                "ByteMatchStatement": {
                  "FieldToMatch": {
                    "SingleHeader": {
                      "Name": "user-agent"
                    }
                  },
                  "PositionalConstraint": "EXACTLY",
                  "SearchString": "PostmanRuntime/7.29.2",
                  "TextTransformations": [
```

```
                    {
                      "Priority": 0,
                      "Type": "NONE"
                    }
                  ]
                }
              }
            }
          }
        ]
      }
    },
    "RuleLabels": [],
    "Action": {
      "Block": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "match_rule"
    }
}
```

Bot Control の例: ログインページにのみ Bot Control を使用します

次の例では、スコープダウンステートメントを使用して、URI パス によって識別されるウェブサイトのログインページに送信されるトラフィックにのみ AWS WAF Bot Control を適用しますlogin。ログインページへの URI パスは、アプリケーションや環境によっては、この例とは異なる場合があります。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
   "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
```

```
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "ByteMatchStatement": {
        "SearchString": "login",
        "FieldToMatch": {
          "UriPath": {}
        },
        "TextTransformations": [
          {
            "Priority": 0,
            "Type": "NONE"
          }
        ],
        "PositionalConstraint": "CONTAINS"
      }
    }
  }
}
```

Bot Control の例: 動的コンテンツにのみ Bot Control を使用する

この例では、スコープダウンステートメントを使用して、動的コンテンツにのみ AWS WAF Bot Control を適用します。

スコープダウンステートメントは、正規表現パターンセットの一致結果を否定することにより、静的コンテンツを除外します。

- 正規表現パターンセットは、静的コンテンツの拡張子と一致するように設定されています。例えば、正規表現パターンセットの指定は `(?i)\.(jpe?g|gif|png|svg|ico|css|js|woff2?)$` である場合があります。正規表現のパターンセットとステートメントの詳細については、「正規表現パターンセット一致ルールステートメント」を参照してください。
- スコープダウンステートメントでは、NOT ステートメント内に正規表現パターンセットのステートメントをネストすることにより、一致する静的コンテンツを除外します。NOT ステートメントについては、「NOT ルールステートメント」を参照してください。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
   "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "RegexPatternSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:123456789:regional/regexpatternset/
excludeset/00000000-0000-0000-0000-000000000000",
            "FieldToMatch": {
              "UriPath": {}
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        }
      }
    }
  }
}
```

Bot Control の例: ボット管理から IP 範囲を除外する

AWS WAF Bot Control 管理からウェブトラフィックのサブセットを除外し、ルールステートメントを使用してそのサブセットを識別できるようにする場合は、Bot Control マネージドルールグループステートメントにスコープダウンステートメントを追加して除外します。

次のルールは、特定の IP アドレス範囲からのウェブリクエストを除き、すべてのウェブトラフィックに対して通常の Bot Control ボット管理を実行します。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "IPSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:123456789:regional/ipset/
friendlyips/00000000-0000-0000-0000-000000000000"
          }
        }
      }
    }
  }
}
```

Bot Control の例: コントロールしているボットからのトラフィックを許可する

一部のサイトモニタリングボットとカスタムボットは、カスタムヘッダーを送信するように設定できます。このようなボットからのトラフィックを許可する場合、ヘッダーに共有シークレットを追加するように設定できます。その後、 AWS WAF Bot Control マネージドルールグループステートメントにスコープダウンステートメントを追加することで、 ヘッダーを持つメッセージを除外できます。

次のルール例は、シークレットヘッダーを持つトラフィックを Bot Control 検査から除外します。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "ByteMatchStatement": {
            "SearchString": "YSBzZWNyZXQ=",
            "FieldToMatch": {
              "SingleHeader": {
                "Name": "x-bypass-secret"
              }
            },
            "TextTransformations": [
              {
```

```
                "Priority": 0,
                "Type": "NONE"
              }
            ],
            "PositionalConstraint": "EXACTLY"
          }
        }
      }
    }
  }
}
```

Bot Control の例: ターゲット検査レベルの有効化

保護レベルを強化するために、 AWS WAF Bot Control マネージドルールグループでターゲット検査レベルを有効にできます。

次の例では、機械学習機能が有効になっています。`EnableMachineLearning` を `false` に設定することで、この動作をオプトアウトできます。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "TARGETED",
            "EnableMachineLearning": true
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    }
```

```
  }
}
```

Bot Control の例: 2 つのステートメントを使用してターゲット検査レベルの使用を制限する

コスト最適化として、保護パック (ウェブ ACL) で 2 つの AWS WAF Bot Control マネージドルールグループステートメントを使用し、個別の検査レベルとスコープを設定できます。例えば、より機密性の高いアプリケーションエンドポイントにのみ、ターゲット検査レベルのステートメントを評価できます。

次の例の 2 つのステートメントには、相互に排他的な評価があります。この設定がない場合、リクエストによって 2 つの Bot Control 評価が請求される可能性があります。

> **Note**
>
> コンソールのビジュアルエディターでは、複数のステートメントリファレンス `AWSManagedRulesBotControlRuleSet` はサポートされていません。代わりに、JSON エディターを使用します。

```
{
  "Name": "Bot-WebACL",
  "Id": "...",
  "ARN": "...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "Bot-WebACL",
  "Rules": [
      {
        ...
      },
      {
       "Name": "AWS-AWSBotControl-Common",
       "Priority": 5,
       "Statement": {
          "ManagedRuleGroupStatement": {
             "VendorName": "AWS",
             "Name": "AWSManagedRulesBotControlRuleSet",
             "ManagedRuleGroupConfigs": [
               {
                 "AWSManagedRulesBotControlRuleSet": {
```

```
                "InspectionLevel": "COMMON"
              }
            }
          ],
          "RuleActionOverrides": [],
          "ExcludedRules": []
        },
        "VisibilityConfig": {
          "SampledRequestsEnabled": true,
          "CloudWatchMetricsEnabled": true,
          "MetricName": "AWS-AWSBotControl-Common"
        },
        "ScopeDownStatement": {
          "NotStatement": {
            "Statement": {
              "ByteMatchStatement": {
                "FieldToMatch": {
                  "UriPath": {}
                },
                "PositionalConstraint": "STARTS_WITH",
                "SearchString": "/sensitive-endpoint",
                "TextTransformations": [
                  {
                    "Type": "NONE",
                    "Priority": 0
                  }
                ]
              }
            }
          }
        }
      }
    },
    {
      "Name": "AWS-AWSBotControl-Targeted",
      "Priority": 6,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesBotControlRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesBotControlRuleSet": {
                "InspectionLevel": "TARGETED",
```

```
                    "EnableMachineLearning": true
                  }
                }
              ],
              "RuleActionOverrides": [],
              "ExcludedRules": []
            },
            "VisibilityConfig": {
              "SampledRequestsEnabled": true,
              "CloudWatchMetricsEnabled": true,
              "MetricName": "AWS-AWSBotControl-Targeted"
             },
             "ScopeDownStatement": {
                "Statement": {
                  "ByteMatchStatement": {
                    "FieldToMatch": {
                      "UriPath": {}
                    },
                    "PositionalConstraint": "STARTS_WITH",
                    "SearchString": "/sensitive-endpoint",
                    "TextTransformations": [
                      {
                        "Type": "NONE",
                        "Priority": 0
                      }
                    ]
                  }
                }
              }
          }
        }
    ],
    "VisibilityConfig": {
      ...
    },
    "Capacity": 1496,
    "ManagedByFirewallManager": false,
    "RetrofittedByFirewallManager": false
}
```

AWS WAF 分散サービス拒否 (DDoS) の防止

AWS WAF は、 AWS リソース内の DDoS 攻撃に対する高度でカスタマイズ可能な保護を提供します。このセクションで説明されているオプションを確認し、セキュリティとビジネスニーズを満たす DDoS 対策保護のレベルを選択します。

AWS WAFでは、2 つの DDoS 保護階層から選択できます。

リソースレベルの DDoS 保護

標準階層は、Application Load Balancer 内で動作し、ホストフィルタリングを通じて既知の悪意のあるソースから保護します。潜在的な DDoS イベントに最もよく反応するように保護動作を設定できます。

リソースレベルの DDoS 保護:

- トラフィックパターンを自動的にモニタリングします。
- 脅威インテリジェンスをリアルタイムで更新します。
- 既知の悪意のあるソースから保護します。

Application Load Balancer のウェブ ACL リクエストコストを最適化するには

リソースレベルの保護を有効にするには、ウェブ ACL を Application Load Balancer に関連付ける必要があります。Application Load Balancer が設定のないウェブ ACL に関連付けられている場合、 AWS WAF リクエストに対して料金は発生しませんが、CloudWatch メトリクスの Application Load Balancer に対してサンプルリクエストやレポートを提供し AWS WAF ません。Application Load Balancer のオブザーバビリティ機能を有効にするには、次のアクションを実行できます。

- `DefaultAction` のカスタムリクエストヘッダーで `Allow` アクションまたは `Block` アクションを使用します。詳細については、「ノンブロッキングアクションのためのカスタムリクエストヘッダーの挿入」を参照してください。
- 任意のルールをウェブ ACL に追加します。詳細については、「AWS WAF ルール」を参照してください。
- ログ記録の送信先を有効にします。詳細については、「保護パック (ウェブ ACL) のログ記録の設定」を参照してください。
- ウェブ ACL を AWS Firewall Manager ポリシーに関連付けます。詳細については、「の AWS Firewall Manager ポリシーの作成 AWS WAF」を参照してください。

AWS WAF は、これらの設定がないと、サンプルリクエストを提供したり、CloudWatch メトリクスを発行したりしません。

AWS マネージドルールグループの DDoS 保護

DDoS 保護の高度な階層は、`AWSManagedRulesAntiDDoSRuleSet` を通じて提供されます。マネージドルールグループは、リソースレベルの保護階層を補完しますが、次の大きな違いがあります。

- 保護は Application Load Balancer と CloudFront ディストリビューションの両方に拡張されます
- トラフィックベースラインは、新しい攻撃パターンの検出を改善するために、保護されたリソース用に作成されます。
- 保護動作は、選択した感度レベルに応じてアクティブ化されます。
- DDoS イベントの発生時に、保護されたリソースへのリクエストを管理およびラベル付けします。

含まれているルールと機能の包括的なリストについては、「AWS WAF 分散サービス拒否 (DDoS) 防止ルールグループ」を参照してください。

Note

このマネージドルールグループを使用する場合、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

トピック

- Application Load Balancer のリソースレベルの DDoS 保護
- Anti-DDoS マネージドルールグループを使用した高度な AWS WAF Anti-DDoS 保護

Application Load Balancer のリソースレベルの DDoS 保護

リソースレベルの DDoS 保護は、 AWS WAF マネージドルールグループのデプロイ料金を発生させることなく、Application Load Balancer に即時の防御を追加します。この標準レベルのアンチ DDoS 保護では、 AWS 脅威インテリジェンスとトラフィックパターン分析を使用して Application Load

Balancer を保護します。既知の悪意のあるソースを特定するために、DDoS 対策保護は直接クライアント IP アドレスと X-Forwarded-For (XFF) ヘッダーの両方のオンホストフィルタリングを実行します。既知の悪意のあるソースが特定されると、次の 2 つのモードのいずれかで保護がアクティブ化されます。

DDoS 下でアクティブ はデフォルトの保護モードであり、ほとんどのユースケースで推奨されます。

このモードでは、以下を行います。

- 高負荷条件または潜在的な DDoS イベントを検出すると、保護を自動的にアクティブ化します
- 攻撃条件中にのみ既知の悪意のあるソースからのトラフィックをレート制限します。
- 通常のオペレーション中の正当なトラフィックへの影響を最小限に抑えます
- Application Load Balancer のヘルスメトリクスと AWS WAF レスポンスデータを使用して、いつ保護をエンゲージするかを判断します

常時オン はオプションモードであり、有効にすると常時アクティブになります。

このモードでは、以下を行います。

- 既知の悪意のあるソースに対する継続的な保護を維持します
- 既知の悪意のあるソースからのトラフィックをリアルタイムでレート制限します
- XFF ヘッダーの悪意のある IP を使用した直接接続とリクエストの両方に保護を適用します
- 正当なトラフィックに大きな影響を与える可能性がありますが、最大限のセキュリティを提供します

リソースレベルの DDoS 保護によってブロックされたリクエストは、CloudWatch ログに `LowReputationPacketsDropped`または `LowReputationRequestsDenied`メトリクスとして記録されます。詳細については、「AWS WAF コアメトリクスとディメンション」を参照してください。

既存の ウェブ ACL で標準 DDoS 保護を有効にします

ウェブ ACL を作成するとき、または Application Load Balancer に関連付けられた既存のウェブ ACL を更新するときに、DDoS 保護を有効にできます。

> **Note**
>
> Application Load Balancer に関連付けられている既存のウェブ ACL がある場合、DDoS 保護はデフォルトで DDoS モードでアクティブ で有効になります。

AWS WAF コンソールで DDoS 対策保護を有効にするには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで [ウェブ ACL] を選択し、Application Load Balancer に関連付けられているウェブ ACL を開きます。
3. 関連付けられた AWS リソースを選択します。
4. リソースレベルの DDoS 保護 で、編集 を選択します。
5. 次のいずれかのモードを選択します。
   - DDoS でアクティブ (推奨) - 保護は高負荷条件中でのみ機能します
   - 常時オン - 既知の悪意のあるソースに対する常時オンの保護
6. [Save changes] (変更の保存) をクリックします。

> **Note**
>
> ウェブ ACL の作成については、「で保護パック (ウェブ ACL) を作成する AWS WAF」を参照してください。

> **Application Load Balancer のウェブ ACL リクエストコストを最適化するには**
>
> リソースレベルの保護を有効にするには、ウェブ ACL を Application Load Balancer に関連付ける必要があります。Application Load Balancer が設定のないウェブ ACL に関連付けられている場合、 AWS WAF リクエストに対して料金は発生しませんが、CloudWatch メトリクスの Application Load Balancer に対してサンプルリクエストやレポートを提供し AWS WAF ません。Application Load Balancer のオブザーバビリティ機能を有効にするには、次のアクションを実行できます。

- `DefaultAction` のカスタムリクエストヘッダーで `Allow` アクションまたは `Block` アクションを使用します。詳細については、「ノンブロッキングアクションのためのカスタムリクエストヘッダーの挿入」を参照してください。
- 任意のルールをウェブ ACL に追加します。詳細については、「AWS WAF ルール」を参照してください。
- ログ記録の送信先を有効にします。詳細については、「保護パック (ウェブ ACL) のログ記録の設定」を参照してください。
- ウェブ ACL を AWS Firewall Manager ポリシーに関連付けます。詳細については、「の AWS Firewall Manager ポリシーの作成 AWS WAF」を参照してください。

AWS WAF は、これらの設定がないと、サンプルリクエストを提供したり、CloudWatch メトリクスを発行したりしません。

Anti-DDoS マネージドルールグループを使用した高度な AWS WAF Anti-DDoS 保護

`AWSManagedRulesAntiDDoSRuleSet` マネージドルールグループは、 で利用可能な DDoS 対策保護の最も高度な階層です AWS WAF。

> **Note**
>
> このマネージドルールグループを使用する場合、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

AWS WAF DDoS 対策コンポーネント

に高度なアンチ DDoS 保護を実装するための主なコンポーネント AWS WAF は次のとおりです。

`AWSManagedRulesAntiDDoSRuleSet` – DDoS 攻撃に参加している可能性が高いリクエストを検出、ラベル付け、チャレンジします。また、イベント中に保護されたリソースへのすべてのリクエストにラベル付けします。ルールグループのルールとラベルの詳細については、「AWS WAF 分散サービス拒否 (DDoS) 防止ルールグループ」を参照してください。このルールグループを使用するには、マネージドルールグループ参照ステートメントを使用して保護パック (ウェブ ACL) に含めます。詳細については、「DDoS 対策マネージドルールグループを保護パック (ウェブ ACL) に追加する」を参照してください。

- ウェブ ACL トラフィック概要ダッシュボード – コンソールで DDoS アクティビティと DDoS 対策レスポンスをモニタリングします。詳細については、「保護パック (ウェブ ACL) のトラフィック概要ダッシュボード」を参照してください。
- ログ記録とメトリクス – トラフィックをモニタリングし、DDoS 対策保護の効果を理解できます。保護パック (ウェブ ACL) のログ、Amazon Security Lake データ収集、Amazon CloudWatch メトリクスを設定します。これらのオプションの詳細については、ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック、Amazon CloudWatch によるモニタリング、及び「What is Amazon Security Lake?」を参照してください。
- ラベルとラベル一致ルール – DDoS 対策マネージドルールグループによって特定されるウェブリクエストの処理をカスタマイズできます。AWSManagedRulesAntiDDoSRuleSetのどのルールでも、カウントモードに切り替えて、追加されたラベルと照合できます。詳細については、「ラベル一致ルールステートメント」および「でのウェブリクエストのラベル付け AWS WAF」を参照してください。
- カスタムリクエストとレスポンス - 許可されたリクエストにカスタムヘッダーを追加し、ブロックされたリクエストではカスタムレスポンスを送信できます。ラベルマッチングを AWS WAF カスタムリクエストおよびレスポンス機能とペアリングします。詳細については、「でカスタマイズされたウェブリクエストとレスポンス AWS WAF」を参照してください。

DDoS 対策マネージドルールグループを保護パック (ウェブ ACL) に追加する

このセクションでは、AWSManagedRulesAntiDDoSRuleSet ルールグループを追加および設定する方法について説明します。

DDoS 対策マネージドルールグループを設定するには、DDoS 攻撃に対してルールグループがどれだけ機密であるかや、攻撃に参加している、または参加している可能性のあるリクエストに対してルールグループが実行するアクションを含む設定を指定します。この設定は、マネージドルールグループの通常の設定に追加されます。

ルールグループの説明およびルールとラベルのリストについては、「AWS WAF 分散サービス拒否 (DDoS) 防止ルールグループ」を参照してください。

このガイダンスは、 AWS WAF 保護パック (ウェブ ACL)、ルール、およびルールグループを作成および管理する方法を一般的に認識しているユーザーを対象としています。これらのトピックは、このガイドの前のセクションでカバーされています。マネージドルールグループを保護パック (ウェブ ACL) に追加する方法の基本については、「コンソールを通じた保護パック (ウェブ ACL) へのマネージドルールグループの追加」を参照してください。

ベストプラクティスに従う

DDoS 対策ルールグループは、「でのインテリジェントな脅威軽減のベストプラクティス AWS WAF」に記載されているベストプラクティスに従って使用してください。

保護パック (ウェブ ACL) で **AWSManagedRulesAntiDDoSRuleSet** ルールグループを使用するには

1. AWS マネージドルールグループを保護パック (ウェブ ACL) AWSManagedRulesAntiDDoSRuleSetに追加し、保存する前にルールグループ設定を編集します。

   > **Note**
   >
   > このマネージドルールグループを使用する場合、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

2. ルールグループ設定 ペインで、AWSManagedRulesAntiDDoSRuleSet ルールグループのカスタム設定を指定します。

   a. ブロックの機密性レベル では、ルールグループの DDoS 疑惑ラベル付けで一致するときに、ルール DDoSRequests をどれだけ機密にするかを指定します。機密性が高いほど、ルールが一致するラベル付けのレベルが低くなります。

      - 低い機密性では機密の程度が低く、高い疑惑ラベル awswaf:managed:aws:anti-ddos:high-suspicion-ddos-request がある、攻撃の最も明白な参加者でのみルールが一致します。
      - 中程度の機密性では、中程度と高い疑惑ラベルでルールが一致します。
      - 高い機密性では、ルールは低、中、高のすべての疑惑ラベルで一致します。

      このルールは、DDoS 攻撃に参加している疑いがあるウェブリクエストの最も重大な処理を提供します。

   b. チャレンジを有効にする では、ルール ChallengeDDoSRequests と ChallengeAllDuringEvent を有効にするかどうかを選択します。これにより、デフォルトで、一致するリクエストに Challenge アクションが適用されます。

      これらのルールは、正当なユーザーが DDoS 攻撃の参加者をブロックしながらリクエストを続行できるようにすることを目的としたリクエスト処理を提供します。アクション設定を Allow または Count にオーバーライドするか、完全に使用を無効にすることができます。

      これらのルールを有効にする場合は、必要な追加設定を指定します。

- チャレンジの機密レベル では、ルール `ChallengeDDoSRequests` をどれだけ機密にするかを指定します。

  機密性が高いほど、ルールが一致するラベル付けのレベルが低くなります。

  - 低い機密性では機密の程度が低く、高い疑惑ラベル `awswaf:managed:aws:anti-ddos:high-suspicion-ddos-request` がある、攻撃の最も明白な参加者でのみルールが一致します。
  - 中程度の機密性では、中程度と高い疑惑ラベルでルールが一致します。
  - 高い機密性では、ルールは低、中、高のすべての疑惑ラベルで一致します。

- 除外 URI 正規表現 では、サイレントブラウザチャレンジを処理できないウェブリクエストの URI に一致する正規表現を指定します。Challenge アクションは、サイレントブラウザチャレンジを処理できない限り、チャレンジトークンがない URI からのリクエストを効果的にブロックします。

  Challenge アクションは、HTML コンテンツを想定しているクライアントによってのみ適切に処理できます。アクションの仕組みの詳細については、「CAPTCHA および Challenge アクション動作」を参照してください。

  デフォルトの正規表現を確認し、必要に応じて更新します。ルールは、指定された正規表現を使用して、Challenge アクションを処理できないリクエスト URI を特定し、ルールがチャレンジを返さないようにします。この方法で除外するリクエストは、ルール `DDoSRequests` でルールグループによってのみブロックできます。

  コンソールで提供されるデフォルトの式は、ほとんどのユースケースを対象としていますが、アプリケーションに合わせて確認して調整する必要があります。

  AWS WAF は、いくつかの例外`libpcre`を除いて、PCRE ライブラリで使用されるパターン構文をサポートします。ライブラリは、「PCRE - Perl Compatible Regular Expressions」で文書化されています。 AWS WAF サポートの詳細については、「」を参照してくださいでサポートされている正規表現構文 AWS WAF。

3. ルールグループに必要な追加設定を指定し、ルールを保存します。

> **Note**
>
> AWS では、このマネージドルールグループでスコープダウンステートメントを使用しないことをお勧めします。スコープダウンステートメントは、ルールグループが監視するリクエストを制限するため、トラフィックベースラインが不正確になり、DDoS イベ

ント検出が低下する可能性があります。スコープダウンステートメントオプションは、すべてのマネージドルールグループステートメントで使用できますが、このステートメントには使用しないでください。スコープダウンステートメントの詳細については、「でのスコープダウンステートメントの使用 AWS WAF」を参照してください。

4. ルールの優先度の設定 ページで、新しい DDoS 対策マネージドルールグループルールを上に移動させ、持っている Allow アクションルールの後で他のルールの前にのみ実行されるようにします。これにより、ルールグループは DDoS 対策保護のトラフィックを最も多く追跡できます。
5. 変更を保護パック (ウェブ ACL) に保存します。

本番稼働トラフィックに DDoS 対策実装をデプロイする前に、トラフィックへの潜在的な影響に慣れるまで、ステージング環境またはテスト環境でテストおよびチューニングします。その後、ルールを有効にする前に、本番稼働用トラフィックでカウントモードでルールをテストしてチューニングします。ガイダンスについては、次のセクションを参照してください。

DDoS 対策のテストとデプロイ

機能をデプロイする前に、 AWS WAF 分散サービス拒否 (DDoS) 防止を設定してテストする必要があります。このセクションは設定とテストの一般的なガイダンスを提供しますが、実行する具体的なステップは、ニーズ、リソース、および受け取るウェブリクエストによって異なります。

この情報は、AWS WAF 保護のテストとチューニング で提供されているテストおよび調整に関する一般情報とは別です。

> **Note**
>
> AWS マネージドルールは、一般的なウェブ脅威から保護するように設計されています。ドキュメントに従って使用すると、 AWS マネージドルールルールグループはアプリケーションに別のセキュリティレイヤーを追加します。ただし、 AWS マネージドルールルールグループは、選択した AWS リソースによって決定されるセキュリティ責任に代わるものではありません。責任共有モデルを参照して、 のリソースが適切に保護 AWS されていることを確認します。

> **本番稼働トラフィックのリスク**
>
> トラフィックへの潜在的な影響に納得がいくまで、実装をステージング環境またはテスト環境でテストおよび調整します。その後、ルールを有効にする前に、本番稼働用トラフィックでカウントモードでルールをテストしてチューニングします。

このガイダンスは、 AWS WAF 保護パック (ウェブ ACL)、ルール、およびルールグループを作成および管理する方法を一般的に認識しているユーザーを対象としています。これらのトピックは、このガイドの前のセクションでカバーされています。

AWS WAF 分散サービス拒否 (DDoS) 防止実装を設定してテストするには

これらのステップを最初にテスト環境で実行し、次に本番環境で実行します。

1. AWS WAF 分散サービス拒否 (DDoS) 防止マネージドルールグループをカウントモードに追加する

   > **Note**
   >
   > このマネージドルールグループを使用する場合、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

   AWS マネージドルールルールグループ`AWSManagedRulesAntiDDoSRuleSet`を新規または既存の保護パック (ウェブ ACL) に追加し、現在の保護パック (ウェブ ACL) の動作を変更しないように設定します。このルールグループのルールとラベルの詳細については、「AWS WAF 分散サービス拒否 (DDoS) 防止ルールグループ」を参照してください。

   - マネージドルールグループを追加する際には、それを編集し、次の手順を実行します。
     - ルールグループ設定 ペインで、ウェブトラフィックの DDoS 対策アクティビティを実行するために必要な詳細を指定します。詳細については、「DDoS 対策マネージドルールグループを保護パック (ウェブ ACL) に追加する」を参照してください。
     - [Rules] (ルール) ペインで、[Override all rule actions] (すべてのルールアクションをオーバーライド) ドロップダウンを開いて、[Count] を選択します。この設定では、 AWS WAF は、ルールグループ内のすべてのルールに対してリクエストを評価し、その結果の一致のみをカウントしつつ、引き続きリクエストにラベルを追加します。詳細については、「ルールグループ内のルールアクションのオーバーライド」を参照してください。

このオーバーライドを使用すると、DDoS 対策マネージドルールの潜在的な影響をモニタリングして、サイレントブラウザチャレンジを処理できない URI の正規表現を拡張するなど、変更を加えるかどうかを判断できます。

- トラフィックを許可するルールの直後に、できるだけ早く評価されるようにルールグループを配置します。ルールは昇順の優先順位で評価されます。コンソールは、ルールリストの最上部から順番を設定します。詳細については、「ルールの優先度を設定する」を参照してください。

2. 保護パック (ウェブ ACL) のサンプリング、ログ記録、およびメトリクスの有効化

   必要に応じて、保護パック (ウェブ ACL) のログ記録、Amazon Security Lake データ収集、リクエストサンプリング、Amazon CloudWatch メトリクスを設定します。これらの可視化ツールを使用して DDoS 対策マネージドルールグループとトラフィックとのインタラクションをモニタリングできます。

   - ログ記録の設定と使用については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。
   - Amazon Security Lake の詳細については、「Amazon Security Lake ユーザーガイド」の「Amazon Security Lake とは」および AWS 「サービスからのデータの収集」を参照してください。
   - Amazon CloudWatch メトリクスの詳細については、「Amazon CloudWatch によるモニタリング」を参照してください。
   - ウェブリクエストサンプリングの詳細については、「ウェブリクエストのサンプルの表示」を参照してください。

3. 保護パック (ウェブ ACL) をリソースに関連付ける

   保護パック (ウェブ ACL) がテストリソースに関連付けられていない場合は、関連付けます。詳細については、「AWS リソースとの保護の関連付けまたは関連付け解除」を参照してください。

4. トラフィックと DDoS 対策ルールの一致をモニタリングする

   通常のトラフィックがフローしていることと、DDoS 対策マネージドルールグループのルールが一致するウェブリクエストにラベルを追加していることを確認します。ログにラベルが表示され、Amazon CloudWatch メトリクスで DDoS 対策とラベルのメトリクスを確認できます。ログでは、ルールグループでカウントするようにオーバーライドしたルールが、カウントに設定された `action` と、オーバーライドした設定済のルールアクションを示す `overriddenAction` とともに、`ruleGroupList` に表示されます。

5. DDoS 対策ウェブリクエストの処理をカスタマイズする

   必要に応じて、リクエストを明示的に許可またはブロックする独自のルールを追加して、DDoS 対策ルールがそのリクエストを処理する方法を変更します。

   例えば、DDoS 対策ラベルを使用して、リクエストを許可またはブロックしたり、リクエスト処理をカスタマイズしたりできます。DDoS 対策マネージドルールグループの後にラベル一致ルールを追加して、適用する処理のためにラベル付きリクエストをフィルタリングできます。テスト後、関連する DDoS 対策ルールをカウントモードで維持し、カスタムルールでリクエストの処理に関する決定を維持します。

6. テストルールを削除し、DDoS 対策設定を構成する

   テスト結果を確認して、モニタリングのみのためにカウントモードで保持する DDoS 対策ルールを決定します。アクティブな保護で実行するルールについては、保護パック (ウェブ ACL) ルールグループ設定でカウントモードを無効にして、設定されたアクションを実行できるようにします。これらの設定を確定したら、本番環境用に作成したカスタムルールを保持しながら、一時的なテストラベル一致ルールを削除します。DDoS 対策設定に関するその他の考慮事項については、「でのインテリジェントな脅威軽減のベストプラクティス AWS WAF」を参照してください。

7. モニタリングおよびチューニング

   ウェブリクエストが希望どおりに処理されていることを確認するには、使用することを希望する DDoS 対策機能を有効にした後、トラフィックを注意深くモニタリングします。ルールグループに対するルールカウントの上書きと独自のルールを使用して、必要に応じて動作を調整します。

DDoS 対策のベストプラクティス

- 通常のトラフィック期間中の保護を有効にする – これにより、保護は攻撃に対応する前にベーストラフィックパターンを確立できます。攻撃が発生していない場合は保護を追加し、ベースライン確立の時間を確保します。
- メトリクスを定期的にモニタリングする – CloudWatch メトリクスを確認して、トラフィックパターンと保護の有効性を理解します。
- 重要なアプリケーションにはプロアクティブモードを検討する – ほとんどのユースケースではリアクティブモードが推奨されますが、既知の脅威に対する継続的な保護を必要とするアプリケーションにはプロアクティブモードの使用を検討してください。
- ステージング環境でテストする – 本番環境で保護を有効にする前に、ステージング環境で設定をテストおよび調整して、正当なトラフィックへの影響を理解します。

でのクライアントアプリケーション統合 AWS WAF

このセクションでは、インテリジェントな脅威統合 APIsと JavaScript CAPTCHA 統合 API を AWS WAF の機能で使用する方法について説明します。

AWS WAF クライアントアプリケーション統合 APIs を使用して、クライアント側の保護と AWS サーバー側の保護パック (ウェブ ACL) 保護を組み合わせて、保護されたリソースにウェブリクエストを送信するクライアントアプリケーションが意図したクライアントであり、エンドユーザーが人間であることを確認します。

クライアント統合を使用して、サイレントブラウザのチャレンジと CAPTCHA パズルを管理し、ブラウザとエンドユーザーの応答が成功したことを証明するトークンを取得し、保護されたエンドポイントへのリクエストにこれらのトークンを含めます。 AWS WAF トークンの一般的な情報については、「」を参照してくださいAWS WAF インテリジェントな脅威の軽減におけるトークンの使用。

クライアント統合を、リソースへのアクセスに有効なトークンを必要とする保護パック (ウェブ ACL) 保護と組み合わせます。次のセクション インテリジェントな脅威統合と AWS マネージドルール に示されているような、チャレンジトークンをチェックおよびモニタリングするルールグループを使用できるため、「CAPTCHA および Challengeの AWS WAF」の説明に従い、CAPTCHA および Challenge ルールアクションを使用してチェックします。

AWS WAF SDK を使用して、Bot Control のターゲットを絞った保護レベルの検出精度を向上させます。キーページ (ログイン、チェックアウト、アカウント作成) にチャレンジ`script`タグを追加します。いつどのように統合するかに関する詳細なガイダンスについては、「」を参照してくださいクライアントアプリケーション統合 SDKsの統合。

AWS WAF は、JavaScript アプリケーションには 2 つのレベルの統合を提供し、モバイルアプリケーションには 1 つのレベルの統合を提供します。

- インテリジェントな脅威統合 – クライアントアプリケーションを検証し、 AWS トークンの取得と管理を提供します。これは、ルールアクションによって提供される機能に似ています AWS WAF Challenge。この機能により、クライアントアプリケーションは、`AWSManagedRulesACFPRuleSet` マネージドルールグループ、`AWSManagedRulesATPRuleSet` マネージドルールグループ、および `AWSManagedRulesBotControlRuleSet` マネージドルールグループのターゲットを絞った保護レベルと完全に統合されます。

  インテリジェントな脅威統合 APIs AWS WAF 、サイレントブラウザチャレンジを使用して、クライアントが有効なトークンを取得した後にのみ、保護されたリソースへのログイン試行やその他の呼び出しが許可されるようにします。API は、クライアントアプリケーションセッションのトーク

ン認可を管理し、クライアントに関する情報を収集して、ボットによる操作か、人間による操作かを判断します。

> **Note**
>
> JavaScript ならびに Android および iOS モバイルアプリケーションで使用できます。

- CAPTCHA 統合 – アプリケーションで管理するカスタマイズされた CAPTCHA パズルでエンドユーザーを検証します。これはルールアクションによって AWS WAF CAPTCHA提供される機能に似ていますが、パズルの配置と動作をさらに制御できます。

  この統合では、JavaScript のインテリジェントな脅威統合を活用してサイレントチャレンジを実行し、顧客のページに AWS WAF トークンを提供します。

  > **Note**
  >
  > これは JavaScript アプリケーションで使用できます。

トピック

- インテリジェントな脅威統合と AWS マネージドルール
- AWS WAF クライアントアプリケーション統合 APIs へのアクセス
- AWS WAF JavaScript 統合
- AWS WAF モバイルアプリケーションの統合

インテリジェントな脅威統合と AWS マネージドルール

このセクションでは、インテリジェントな脅威統合 APIs AWS Managed Rules ルールグループと連携する方法について説明します。

インテリジェントな脅威統合 API は、インテリジェントな脅威ルールグループを使用する保護パック (ウェブ ACL) と連携して、これらの高度なマネージドルールグループの全機能を有効にします。

- AWS WAF Fraud Control アカウント作成不正防止 (ACFP) マネージドルールグループ `AWSManagedRulesACFPRuleSet`。

  アカウント作成の不正行為は、サインアップボーナスの受け取りやなりすましなどの目的で、攻撃者がアプリケーションで無効なアカウントを作成するオンライン上の違法行為です。ACFP マネー

ジドルールグループには、不正なアカウント作成の試みの一部の可能性があるリクエストをブロック、ラベル付け、管理するためのルールが含まれています。API は、ACFP ルールが使用する微調整されたクライアントブラウザの検証および人間のインタラクティビティに関する情報を有効にし、有効なクライアントトラフィックを悪意のあるトラフィックから分離します。

詳細については、「AWS WAF Fraud Control アカウント作成不正防止 (ACFP) ルールグループ」および「AWS WAF Fraud Control アカウント作成不正防止 (ACFP)」を参照してください。

- AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) マネージドルールグループ `AWSManagedRulesATPRuleSet`。

  アカウント乗っ取りは、攻撃者が個人のアカウントへの不正アクセスを得るオンラインの違法行為です。ATP マネージドルールグループには、悪意のあるアカウント乗っ取りの試行の一部の可能性があるリクエストをブロック、ラベル付け、管理するためのルールが含まれています。API は、ATP ルールが使用する微調整されたクライアント検証および動作集約を有効にし、有効なクライアントトラフィックを悪意のあるトラフィックから分離します。

  詳細については、「AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループ」および「AWS WAF Fraud Control アカウント乗っ取り防止 (ATP)」を参照してください。

- AWS WAF Bot Control マネージドルールグループ のターゲットを絞った保護レベル`AWSManagedRulesBotControlRuleSet`。

  ボットには、ほとんどの検索エンジンやクローラーなど、自己識別型や便利なボットから、ウェブサイトを狙って動作し、自己識別を行わない悪意のあるものまでの範囲に及びます。Bot Control マネージドルールグループは、ウェブトラフィックのボットアクティビティをモニタリング、ラベル付け、管理するルールを提供します。このルールグループのターゲットを絞った保護レベルを使用すると、ターゲットルールは API が提供するクライアントセッション情報を使用し、悪意のあるボットをより適切に検出します。

  詳細については、「AWS WAF Bot Control ルールグループ」および「AWS WAF ボットコントロール」を参照してください。

これらのマネージドルールグループのいずれかを保護パック (ウェブ ACL) に追加するには、手順 ACFP マネージドルールグループをウェブ ACL に追加、ATP マネージドルールグループを保護パック (ウェブ ACL) に追加、AWS WAF Bot Control マネージドルールグループをウェブ ACL に追加する を参照してください。

> **Note**
>
> マネージドルールグループは現在、トークンが不足しているリクエストをブロックしていません。トークンが不足しているリクエストをブロックするには、アプリケーション統合 API を実装した後、有効な AWS WAF トークンを持たないリクエストのブロック のガイダンスに従ってください。

AWS WAF クライアントアプリケーション統合 APIs へのアクセス

このセクションでは、 AWS WAF コンソールでアプリケーション統合 APIsを見つける場所について説明します。

JavaScript 統合 API は一般利用可能で、JavaScript を実行するブラウザや他のデバイスに使用できます。

AWS WAF は、Android および iOS モバイルアプリ用のカスタムのインテリジェントな脅威統合 SDKs を提供します。

- Android モバイルと TV アプリの場合、 SDK は Android API バージョン 23 (Android バージョン 6) 以降で動作します。Android バージョンの詳細については、「SDK Platform リリースノート」を参照してください。
- iOS モバイルアプリの場合、 SDK は iOS バージョン 13 以降で動作します。iOS バージョンの詳細については、「iOS と iPadOS のリリースノート」を参照してください。
- Apple TV アプリの場合、SDK は tvOS バージョン 14 以降で動作します。tvOS バージョンの詳細については、「tvOS のリリースノート」を参照してください。

コンソールで統合 API にアクセスするには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインの [アプリケーション統合] を選択してから、関心のあるタブを選択します。

   - インテリジェントな脅威に対応した統合 は、JavaScript とモバイルアプリケーションで使用できます。

     タブには次のものが含まれています。

- インテリジェントな脅威に対応したアプリケーション統合が有効になっている保護パック (ウェブ ACL) のリスト。リストには、`AWSManagedRulesACFPRuleSet` マネージドルールグループ、`AWSManagedRulesATPRuleSet` マネージドルールグループ、または `AWSManagedRulesBotControlRuleSet` マネージドルールグループのターゲットを絞った保護レベルを使用する各保護パック (ウェブ ACL) が含まれます。インテリジェントな脅威に対応した API を実装するときは、統合する保護パック (ウェブ ACL) の統合 URL を使用します。
- ユーザーがアクセスできる API。JavaScript API は常に利用可能です。モバイル SDK にアクセスするには、「AWSへのお問い合わせ」にてサポート担当者までお問い合わせください。

- CAPTCHA 統合は、JavaScript アプリケーションで使用できます。

  タブには次のものが含まれています。

  - 統合で使用する統合 URL。
  - クライアントアプリケーションドメイン用に作成した API キー。CAPTCHA API を使用するには、暗号化された API キーが必要です。これにより、クライアントは自分のドメインから AWS WAF CAPTCHA にアクセスできるようになります。統合するクライアントごとに、クライアントのドメインを含む API キーを使用します。これらの要件とキーの管理の詳細については、「JS CAPTCHA API の API キーの管理」を参照してください。

AWS WAF JavaScript 統合

このセクションでは、 AWS WAF JavaScript 統合を使用する方法について説明します。

JavaScript 統合 APIs を使用して、JavaScript を実行するブラウザやその他のデバイスに AWS WAF アプリケーション統合を実装できます。

CAPTCHA パズルとサイレントチャレンジは、ブラウザが HTTPS エンドポイントにアクセスしている場合にのみ実行できます。トークンを取得するには、ブラウザクライアントが安全なコンテキストで実行されている必要があります。

- インテリジェントな脅威に対応した API を使用すると、クライアント側のサイレントブラウザのチャレンジを通じてトークン認可を管理し、保護されたリソースに送信するリクエストにトークンを含めることができます。
- CAPTCHA 統合 API にインテリジェントな脅威に対応した API が追加され、クライアントアプリケーションでの CAPTCHA パズルの配置と特性をカスタマイズすることができるようにな

りました。この API は、インテリジェントな脅威に対応した API を活用し、エンドユーザーが CAPTCHA パズルの完成に成功した後にページで使用する AWS WAF トークンを取得します。

これらの統合を使用すると、クライアントによるリモートプロシージャコールに有効なトークンが含まれていることを確認できます。これらの統合 API がアプリケーションのページで実行されている場合、有効なトークンを含まないリクエストをブロックするなどの緩和ルールを保護パック (ウェブ ACL) で実装できます。ルール内の Challenge または CAPTCHA アクションを使用して、クライアントアプリケーションが取得したトークンの使用を強制するルールを実装することもできます。

インテリジェントな脅威 API の実施例

次のリストは、ウェブアプリケーションページでのインテリジェントな脅威に対応した API の一般的な実装の基本コンポーネントを示しています。

```
<head>
<script type="text/javascript" src="protection pack (web ACL) integration URL/
challenge.js" defer></script>
</head>
<script>
const login_response = await AwsWafIntegration.fetch(login_url, {
    method: 'POST',
    headers: {
      'Content-Type': 'application/json'
    },
    body: login_body
  });
</script>
```

CAPTCHA JavaScript API の実施例

CAPTCHA 統合 API を使用すると、エンドユーザーの CAPTCHA パズルエクスペリエンスをカスタマイズできます。CAPTCHA 統合では、ブラウザの検証とトークン管理用に JavaScript のインテリジェントな脅威に対応した統合が活用されているだけでなく、CAPTCHA パズルの設定とレンダリング用の機能も追加されています。

次のリストは、ウェブアプリケーションページでの CAPTCHA JavaScript API の一般的な実装の基本コンポーネントを示しています。

```
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
```

```
</head>

<script type="text/javascript">
    function showMyCaptcha() {
        var container = document.querySelector("#my-captcha-container");

        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            ...other configuration parameters as needed...
        });
    }

    function captchaExampleSuccessFunction(wafToken) {
        // Use WAF token to access protected resources
        AwsWafIntegration.fetch("...WAF-protected URL...", {
            method: "POST",
            ...
        });
    }

    function captchaExampleErrorFunction(error) {
        /* Do something with the error */
    }
</script>

<div id="my-captcha-container">
    <!-- The contents of this container will be replaced by the captcha widget -->
</div>
```

トピック

- トークンで使用するドメインの提供
- コンテンツセキュリティポリシーでの JavaScript API の使用
- インテリジェントな脅威に対応した JavaScript API の使用
- CAPTCHA JavaScript API を使用する

トークンで使用するドメインの提供

このセクションでは、トークンに追加のドメインを提供する方法について説明します。

デフォルトでは、 がトークン AWS WAF を作成すると、保護パック (ウェブ ACL) に関連付けられているリソースのホストドメインが使用されます。 AWS WAF が JavaScript API 用に作成するトークンには、追加のドメインを指定できます。これを行うには、グローバル変数 `window.awsWafCookieDomainList` に 1 つ以上のトークンドメインを設定します。

がトークン AWS WAF を作成すると、 のドメイン`window.awsWafCookieDomainList`と、保護パック (ウェブ ACL) に関連付けられているリソースのホストドメインの組み合わせの中から、最も適切で最短のドメインが使用されます。

設定の例

```
window.awsWafCookieDomainList = ['.aws.amazon.com']
```

```
window.awsWafCookieDomainList = ['.aws.amazon.com', 'abc.aws.amazon.com']
```

このリストではパブリックサフィックスを使用できません。例えば、`gov.au` または `co.uk` をリストでトークンドメインとして使用することはできません。

このリストで指定するドメインは、他のドメインやドメイン設定と互換性がある必要があります。

- ドメインは、保護されたホストドメインと、保護パック (ウェブ ACL) 用に設定されたトークンドメインリストに基づいて、 が AWS WAF 受け入れるドメインである必要があります。詳細については、「AWS WAF 保護パック (ウェブ ACL) トークンドメインリスト設定」を参照してください。
- JavaScript CAPTCHA API を使用する場合、CAPTCHA API キー内の少なくとも 1 つのドメインが、`window.awsWafCookieDomainList` のトークンドメインの 1 つと完全に一致するか、いずれかのトークンドメインの apex ドメインである必要があります。

  例えば、トークンドメイン `mySubdomain.myApex.com` の場合、API キー `mySubdomain.myApex.com` は完全に一致し、API キー `myApex.com` は apex ドメインです。どちらかのキーがトークンドメインに一致します。

  API キーの詳細については、「JS CAPTCHA API の API キーの管理」を参照してください。

`AWSManagedRulesACFPRuleSet` マネージドルールグループを使用する場合、ルールグループ設定に指定したアカウント作成パスのドメインと一致するドメインを設定できます。この設定の詳細については、「ACFP マネージドルールグループをウェブ ACL に追加」を参照してください。

AWSManagedRulesATPRuleSet マネージドルールグループを使用する場合、ルールグループ設定に指定したログインパスのドメインと一致するドメインを設定できます。この設定の詳細については、「ATP マネージドルールグループを保護パック (ウェブ ACL) に追加」を参照してください。

コンテンツセキュリティポリシーでの JavaScript API の使用

このセクションでは、apex AWS WAF ドメインを許可リストに登録するための設定例を示します。

コンテンツセキュリティポリシー (CSP) をリソースに適用し、JavaScript 実装を機能させるには、apex AWS WAF ドメイン を許可リストに登録する必要がありますawswaf.com。JavaScript SDK は異なる AWS WAF エンドポイントを呼び出すため、このドメインを許可リストに登録すると、SDK の動作に必要な権限が付与されます。

以下は、apex AWS WAF ドメインを許可リストに登録するための設定例です。

```
connect-src 'self' https://*.awswaf.com;
script-src 'self' https://*.awswaf.com;
script-src-elem 'self' https://*.awswaf.com;
```

CSP を使用するリソースで JavaScript SDKs を使用しようとしたときに、 AWS WAF ドメインを許可リストに登録していない場合は、次のようなエラーが表示されます。

```
Refused to load the script ...awswaf.com/<> because it violates the following Content
 Security Policy directive: “script-src ‘self’
```

インテリジェントな脅威に対応した JavaScript API の使用

このセクションでは、クライアントアプリケーションでインテリジェントな脅威 JavaScript API を使用する手順について説明します。

インテリジェントな脅威 APIsは、ユーザーのブラウザに対してサイレントチャレンジを実行するオペレーションと、チャレンジと CAPTCHA レスポンスが成功した証拠を提供する AWS WAF トークンを処理するオペレーションを提供します。

JavaScript 統合を最初にテスト環境で実装し、次に本番環境で実装します。追加のコーディングガイダンスについては、次のセクションを参照してください。

インテリジェントな脅威に対応した API を使用するには

1. API のインストール

CAPTCHA API を使用している場合は、このステップをスキップできます。CAPTCHA API をインストールすると、スクリプトはインテリジェントな脅威に対応した API を自動的にインストールします。

a. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。

b. ナビゲーションペインで、[Application integration] (アプリケーション統合) を選択します。[アプリケーション統合] ページに、タブ付きのオプションが表示されます。

c. [インテリジェントな脅威に対応した統合] を選択

d. タブで、統合する保護パック (ウェブ ACL) を選択します。保護パック (ウェブ ACL) リストには、`AWSManagedRulesACFPRuleSet` マネージドルールグループ、`AWSManagedRulesATPRuleSet` マネージドルールグループ、または `AWSManagedRulesBotControlRuleSet` マネージドルールグループのターゲットを絞った保護レベルを使用する保護パック (ウェブ ACL) のみが含まれます。

e. [JavaScript SDK] ペインを開き、統合で使用するスクリプトタグをコピーします。

f. <head> セクションのアプリケーションページコードに、保護パック (ウェブ ACL) 用にコピーしたスクリプトタグを挿入します。この包含により、クライアントアプリケーションは、ページをロードする際にバックグラウンドでトークンを自動的に取得します。

```
<head>
    <script type="text/javascript" src="protection pack (web ACL) integration
 URL/challenge.js” defer></script>
<head>
```

この `<script>` リストは `defer` 属性で設定されていますが、ページに別の動作が必要な場合は、設定を `async` に変更できます。

2. (オプション) クライアントのトークンにドメイン設定を追加する – デフォルトでは、 がトークン AWS WAF を作成すると、保護パック (ウェブ ACL) に関連付けられているリソースのホストドメインが使用されます。JavaScript API に追加のドメインを指定するには、「トークンで使用するドメインの提供」のガイダンスに従ってください。

3. インテリジェントな脅威に対応した統合をコーディングする – クライアントで保護されたエンドポイントにリクエストを送信する前に、トークンの取得が完了するようにコードを記述します。既に `fetch` API を使用して呼び出しを行っている場合は、 AWS WAF 統合 `fetch` ラッパーに置き換えることができます。`fetch` API を使用しない場合は、代わりに AWS WAF 統

合getTokenオペレーションを使用できます。コーディングガイダンスについては、次のセクションを参照してください。

4. 保護パック (ウェブ ACL) にトークン検証を追加する – クライアントで送信するウェブリクエスト内に有効なチャレンジトークンがないかチェックするルールを、保護パック (ウェブ ACL) に少なくとも 1 つ追加します。Bot Control マネージドルールグループのターゲットレベルのような、チャレンジトークンをチェックおよびモニタリングするルールグループを使用できるため、「CAPTCHA および Challengeの AWS WAF」の説明に従い、Challenge ルールアクションを使用してチェックします。

   保護パック (ウェブ ACL) を追加すると、保護されたエンドポイントへのリクエストに、クライアント統合で取得したトークンが含まれていることを確認できます。有効で期限が切れていないトークンを含むリクエストは、Challenge 検査に合格し、クライアントに別のサイレントチャレンジを送信することはありません。

5. (オプション) トークンが不足しているリクエストをブロックする – ACFP マネージドルールグループ、ATP マネージドルールグループまたは Bot Control ルールグループのターゲットを絞ったルールで API を使用する場合、これらのルールはトークンが不足しているリクエストをブロックしません。トークンが不足しているリクエストをブロックするには、有効な AWS WAF トークンを持たないリクエストのブロック のガイダンスに従ってください。

トピック

- インテリジェントな脅威に対応した API 仕様
- 統合 fetch ラッパーの使用方法
- 統合 getToken を使用する方法

インテリジェントな脅威に対応した API 仕様

このセクションでは、インテリジェントな脅威の軽減を目的とした JavaScript API のメソッドとプロパティの仕様を示します。インテリジェントな脅威に対応したこれらの API と CAPTCHA 統合を使用します。

`AwsWafIntegration.fetch()`

AWS WAF 統合実装を使用して HTTP fetchリクエストをサーバーに送信します。

`AwsWafIntegration.getToken()`

保存された AWS WAF トークンを取得しaws-waf-token、現在のページの という名前の Cookie に保存します。値はトークン値に設定されます。

`AwsWafIntegration.hasToken()`

有効期限が切れていないトークンが現在 `aws-waf-token` cookie で保持されているかどうかを示すブール値を返します。

CAPTCHA 統合も使用している場合は、「CAPTCHA JavaScript API 仕様」でその仕様を確認してください。

統合 **`fetch`** ラッパーの使用方法

このセクションでは、統合 `fetch` ラッパーを使用する手順について説明します。

`AwsWafIntegration` 名前空間の下で `fetch` API に対する通常の `fetch` 呼び出しを変更することにより、 AWS WAF `fetch` ラッパーを使用できます。 AWS WAF ラッパーは、標準の JavaScript `fetch` API コールと同じオプションをすべてサポートし、統合のトークン処理を追加します。このアプローチは、一般的に、アプリケーションを統合する最も簡単な方法です。

ラッパーの実装前

次のリスト例は、`AwsWafIntegration` `fetch` ラッパーを実装する前の標準コードを示しています。

```
const login_response = await fetch(login_url, {
     method: 'POST',
     headers: {
       'Content-Type': 'application/json'
     },
     body: login_body
   });
```

ラッパー実装後

次のリストは、`AwsWafIntegration` `fetch` ラッパー実装と同じコードを示しています。

```
const login_response = await AwsWafIntegration.fetch(login_url, {
     method: 'POST',
     headers: {
       'Content-Type': 'application/json'
     },
     body: login_body
   });
```

統合 **getToken** を使用する方法

このセクションでは、getToken オペレーションの使用方法について説明します。

AWS WAF では、保護されたエンドポイントへのリクエストに、現在のトークンの値aws-waf-tokenを持つ という名前の Cookie を含める必要があります。

getToken オペレーションとは、 AWS WAF トークンを取得し、名前を aws-waf-token にして、値をトークン値に設定し、現在のページの cookie に保存する非同期 API コールです。このトークン cookie は、必要に応じてページで使用できます。

getToken を呼び出すと、次が実行されます。

- 期限切れでないトークンが既に使用可能な場合、コールは直ちにそれを返します。
- それ以外の場合、コールは トークンプロバイダーから新しいトークンを取得します。トークン取得ワークフローが完了するまで最大で 2 秒間の猶予があり、この待機期間が経過するとタイムアウトします。オペレーションがタイムアウトすると、呼び出しコードが処理しなければならないエラーがスローされます。

getToken オペレーションには付随する hasToken オペレーションがあり、aws-waf-token cookie が現在有効期限が切れていないトークンを保持しているかどうかを示します。

AwsWafIntegration.getToken() は有効なトークンを取得し、それを Cookie として保存します。ほとんどのクライアント呼び出しは、この Cookie を自動的にアタッチしますが、アタッチしないクライアント呼び出しもあります。例えば、ホストドメイン間で行われた呼び出しは Cookie にアタッチしません。以下の実施詳細では、両方のタイプのクライアント呼び出しを操作する方法を示します。

aws-waf-token Cookie にアタッチする呼び出しの基本的な **getToken** 実施

次のリストの例は、ログインリクエストで getToken オペレーションを実装するための標準コードを示しています。

```
const login_response = await AwsWafIntegration.getToken()
     .catch(e => {
         // Implement error handling logic for your use case
     })
     // The getToken call returns the token, and doesn't typically require special
 handling
     .then(token => {
```

```
        return loginToMyPage()
    })

async function loginToMyPage() {
    // Your existing login code
}
```

トークンが **getToken** から利用可能になった後にのみフォームを送信する

次のリストは、有効なトークンが使用可能になるまで、フォーム送信をインターセプトするイベントリスナーを登録する方法を示しています。

```
<body>
   <h1>Login</h1>
   <p></p>
   <form id="login-form" action="/web/login" method="POST" enctype="application/x-www-
form-urlencoded">
     <label for="input_username">USERNAME</label>
     <input type="text" name="input_username" id="input_username"><br>
     <label for="input_password">PASSWORD</label>
     <input type="password" name="input_password" id="input_password"><br>
     <button type="submit">Submit<button>
   </form>

 <script>
   const form = document.querySelector("#login-form");

   // Register an event listener to intercept form submissions
   form.addEventListener("submit", (e) => {
       // Submit the form only after a token is available
       if (!AwsWafIntegration.hasToken()) {
           e.preventDefault();
           AwsWafIntegration.getToken().then(() => {
               e.target.submit();
           }, (reason) => { console.log("Error:"+reason) });
         }
     });
 </script>
 </body>
```

クライアントがデフォルトで **aws-waf-token** Cookie にアタッチしない場合のトークンとのアタッチ

`AwsWafIntegration.getToken()` は有効なトークンを取得し、それを Cookie として保存しますが、デフォルトの場合、すべてのクライアント呼び出しがこの Cookie にアタッチするわけではありません。例えば、ホストドメイン間で行われた呼び出しは Cookie にアタッチしません。

`fetch` ラッパーはこれらのケースを自動的に処理しますが、`fetch`ラッパーを使用できない場合は、Cookie から読み取るだけでなく、このヘッダーのカスタム `x-aws-waf-token` header. AWS WAF reads `aws-waf-token` トークンを使用して処理できます。次のコードは、ヘッダーの設定例を示しています。

```
const token = await AwsWafIntegration.getToken();
const result = await fetch('/url', {
    headers: {
        'x-aws-waf-token': token,
    },
});
```

デフォルトでは、 はリクエストされたホストドメインと同じドメインを含むトークン AWS WAF のみを受け入れます。クロスドメイントークンには、保護パック (ウェブ ACL) トークンドメインリストの対応するエントリが必要です。詳細については、「AWS WAF 保護パック (ウェブ ACL) トークンドメインリスト設定」を参照してください。

クロスドメイントークンの使用の詳細については、「aws-samples/aws-waf-bot-control-api-protection-with-captcha」を参照してください。

CAPTCHA JavaScript API を使用する

このセクションでは、CAPTCHA 統合 API を使用する手順について説明します。

CAPTCHA JavaScript API を使用すると、CAPTCHA パズルを設定し、クライアントアプリケーションの任意の場所に配置できます。この API は、インテリジェントな脅威の JavaScript APIs の機能を活用して、エンドユーザーが CAPTCHA パズルを正常に完了した後に AWS WAF トークンを取得して使用します。

JavaScript 統合を最初にテスト環境で実装し、次に本番環境で実装します。追加のコーディングガイダンスについては、次のセクションを参照してください。

CAPTCHA 統合 API を使用するには

1. API のインストール

a. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。

b. ナビゲーションペインで、[Application integration] (アプリケーション統合) を選択します。[アプリケーション統合] ページに、タブ付きのオプションが表示されます。

c. [CAPTCHA 統合] を選択します。

d. リストされている JavaScript 統合スクリプトタグをコピーして、統合で使用します。

e. <head> セクションのアプリケーションページコードに、コピーしたスクリプトタグを挿入します。これにより、CAPTCHA パズルの設定および使用が可能になります。

```
<head>
    <script type="text/javascript" src="integrationURL/jsapi.js" defer></
script>
</head>
```

この <script> リストは defer 属性で設定されていますが、ページに別の動作が必要な場合は、設定を async に変更できます。

また、CAPTCHA スクリプトは、インテリジェントな脅威に対応した統合のスクリプトがまだ存在しない場合は自動的にロードします。インテリジェントな脅威に対応した統合のスクリプトにより、クライアントアプリケーションは、ページをロードする際にバックグラウンドでトークンを自動的に取得し、CAPTCHA API の使用に必要なその他のトークン管理機能を提供します。

2. (オプション) クライアントのトークンにドメイン設定を追加する – デフォルトでは、 がトークン AWS WAF を作成すると、保護パック (ウェブ ACL) に関連付けられているリソースのホストドメインが使用されます。JavaScript API に追加のドメインを指定するには、「トークンで使用するドメインの提供」のガイダンスに従ってください。

3. クライアントの暗号化された API キーを取得する – CAPTCHA API には、有効なクライアントドメインのリストを含む暗号化された API キーが必要です。 はこのキー AWS WAF を使用して、統合で使用しているクライアントドメインが CAPTCHA AWS WAF の使用が承認されていることを確認します。API キーを生成するには、「JS CAPTCHA API の API キーの管理」のガイダンスに従ってください。

4. CAPTCHA ウィジェットの実装をコーディングする – renderCaptcha() API コールを、ページ内の使用したい場所に実装します。この機能の設定および使用方法については、以下のセクション「CAPTCHA JavaScript API 仕様」と「CAPTCHA パズルをレンダリングする方法」を参照してください。

CAPTCHA 実装は、トークン管理と AWS WAF トークンを使用するフェッチ呼び出しを実行するためのインテリジェントな脅威統合 APIs と統合されます。これらの API の使用に関するガイダンスについては、「インテリジェントな脅威に対応した JavaScript API の使用」を参照してください。

5. 保護パック (ウェブ ACL) にトークン検証を追加する – クライアントで送信するウェブリクエスト内に有効な CAPTCHA トークンがないかチェックするルールを、保護パック (ウェブ ACL) に少なくとも 1 つ追加します。「CAPTCHA および Challengeの AWS WAF」の説明に従い、CAPTCHA ルールアクションを使用してチェックします。

   保護パック (ウェブ ACL) の追加により、保護されたエンドポイントに送信されるリクエストに、クライアント統合で取得したトークンが含まれていることを確認できます。有効で期限が切れていない CAPTCHA トークンを含むリクエストは、CAPTCHA ルールアクション検査に合格し、エンドユーザーに別の CAPTCHA パズルを提示することはありません。

JavaScript API を実装したら、CAPTCHA パズルの試行とソリューションの CloudWatch メトリクスを確認できます。メトリクスとディメンションの詳細については、アカウントメトリクスとディメンション を参照してください。

トピック

- CAPTCHA JavaScript API 仕様
- CAPTCHA パズルをレンダリングする方法
- からの CAPTCHA レスポンスの処理 AWS WAF
- JS CAPTCHA API の API キーの管理

CAPTCHA JavaScript API 仕様

このセクションでは、CAPTCHA JavaScript API のメソッドとプロパティの仕様を一覧表示します。CAPTCHA JavaScript API を使用して、クライアントアプリケーションでカスタム CAPTCHA パズルを実行します。

この API は、 AWS WAF トークンの取得と使用を設定および管理するために使用するインテリジェントな脅威 APIs に基づいています。「インテリジェントな脅威に対応した API 仕様」を参照してください。

AwsWafCaptcha.renderCaptcha(container, configuration)

エンドユーザーに AWS WAF CAPTCHA パズルを提示し、成功すると、CAPTCHA 検証でクライアントトークンを更新します。これは CAPTCHA 統合でのみ使用できます。この呼び出しをインテリジェントな脅威に対応した API と組み合わせて使用すると、トークンの取得を管理したり、fetch コールでトークンを提供したりできます。インテリジェントな脅威に対応した API については、「インテリジェントな脅威に対応した API 仕様」を参照してください。

が AWS WAF 送信する CAPTCHA インタースティシャルとは異なり、この方法でレンダリングされた CAPTCHA パズルは、最初のタイトル画面なしですぐにパズルを表示します。

container

ページ上のターゲットとなるコンテナ要素の Element オブジェクト。これは通常、document.getElementById() または document.querySelector() を呼び出すことで取得できます。

必須: はい

タイプ: Element

設定

以下のような CAPTCHA 構成設定を含むオブジェクト。

apiKey

クライアントのドメインの許可を有効にする暗号化された API キー。 AWS WAF コンソールを使用して、クライアントドメインの API キーを生成します。1 つのキーを最大 5 つのドメインに使用できます。詳細については、「JS CAPTCHA API の API キーの管理」を参照してください。

必須: はい

タイプ: string

onSuccess: (wafToken: string) => void;

エンドユーザーが CAPTCHA パズルを正常に完了すると、有効な AWS WAF トークンで呼び出されます。 AWS WAF 保護パック (ウェブ ACL) で保護するエンドポイントに送信するリクエストでトークンを使用します。トークンは、パズルの完成に最後に成功したときの証明とタイムスタンプを提供します。

必須: はい

onError?: (error: CaptchaError) => void;

CAPTCHA 操作中にエラーが発生したときに、エラーオブジェクトとともに呼び出されます。

必須: いいえ

CaptchaError クラス定義 – onError ハンドラーは、次のクラス定義を使用してエラータイプを提供します。

```
CaptchaError extends Error {
    kind: "internal_error" | "network_error" | "token_error" | "client_error";
    statusCode?: number;
}
```

- kind – 返されたエラーの種類。
- statusCode – HTTP ステータスコード (利用可能な場合)。これは、エラーが HTTP エラーに起因する場合に network_error で使用されます。

onLoad?: () => void;

新しい CAPTCHA パズルがロードされると呼び出されます。

必須: いいえ

onPuzzleTimeout?: () => void;

CAPTCHA パズルが期限切れになる前に完成しなかった場合に呼び出されます。

必須: いいえ

onPuzzleCorrect?: () => void;

CAPTCHA パズルに正しい回答が入力されると呼び出されます。

必須: いいえ

onPuzzleIncorrect?: () => void;

CAPTCHA パズルに間違った回答が入力されると呼び出されます。

必須: いいえ

defaultLocale

CAPTCHA パズルに使用するデフォルトのロケール。CAPTCHA パズルの説明書は、アラビア語 (ar-SA)、簡体字中国語 (zh-CN)、オランダ語 (nl-NL)、英語 (en-US)、フランス語 (fr-FR)、ドイツ語 (de-DE)、イタリア語 (it-IT)、日本語 (ja-JP)、ブラジルポルトガル語 (pt-BR)、スペイン語 (es-ES)、およびトルコ語 (tr-TR) で提供されています。音声指示はすべての書かれた言語に対して提供されていますが、中国語と日本語の場合、デフォルトでは英語を使用します。デフォルト言語を変更するには、国際言語と ロケールコード (例: `ar-SA`) を指定します。

デフォルト: エンドユーザーのブラウザで現在使用されている言語

必須: いいえ

タイプ: `string`

disableLanguageSelector

`true` に設定すると、CAPTCHA パズルの言語セレクタが非表示になります。

デフォルト: `false`

必須: いいえ

タイプ: `boolean`

dynamicWidth

`true` に設定すると、CAPTCHA パズルの幅はブラウザウィンドウの幅に合わせて変更されます。

デフォルト: `false`

必須: いいえ

タイプ: `boolean`

skipTitle

`true` に設定すると、CAPTCHA パズルのパズルタイトルに「パズルを解く」という見出しが表示されません。

デフォルト: `false`

必須: いいえ

タイプ: boolean

CAPTCHA パズルをレンダリングする方法

このセクションでは、renderCaptcha の実施例を示します。

クライアントインターフェイスで使用する 呼び出しを使用できます AWS WAF renderCaptcha。呼び出しは、CAPTCHA パズルを から取得し AWS WAF、レンダリングして、検証 AWS WAF のために に送信します。呼び出しを行うときは、パズルのレンダリング設定と、エンドユーザーがパズルを完成させたときに実行するコールバックを指定します。オプションの詳細については、前のセクション「CAPTCHA JavaScript API 仕様」を参照してください。

この呼び出しは、インテリジェントな脅威に対応した統合 API のトークン管理機能と組み合わせて使用します。この呼び出しにより、CAPTCHA パズルの完成に成功したことを検証するトークンがクライアントに渡されます。インテリジェントな脅威統合 APIs を使用してトークンを管理し、AWS WAF 保護パック (ウェブ ACLs) で保護されているエンドポイントへのクライアントの呼び出しでトークンを提供します。インテリジェントな脅威に対応した API の詳細については、「インテリジェントな脅威に対応した JavaScript API の使用」を参照してください。

実装例

次のリスト例は、 <head>セクション AWS WAF の統合 URL の配置を含む、標準の CAPTCHA 実装を示しています。

このリストは、インテリジェントな脅威に対応した統合 API の AwsWafIntegration.fetch ラッパーを使用する成功コールバックを含む renderCaptcha 関数で構成されています。この関数については、「統合 fetch ラッパーの使用方法」を参照してください。

```
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>

<script type="text/javascript">
    function showMyCaptcha() {
        var container = document.querySelector("#my-captcha-container");

        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
```

```
            onError: captchaExampleErrorFunction,
            ...other configuration parameters as needed...
        });
    }

    function captchaExampleSuccessFunction(wafToken) {
        // Captcha completed. wafToken contains a valid WAF token. Store it for
        // use later or call AwsWafIntegration.fetch() to use it easily.
        // It will expire after a time, so calling AwsWafIntegration.getToken()
        // again is advised if the token is needed later on, outside of using the
        // fetch wrapper.

        // Use WAF token to access protected resources
        AwsWafIntegration.fetch("...WAF-protected URL...", {
            method: "POST",
            headers: {
                "Content-Type": "application/json",
            },
            body: "{ ... }" /* body content */
        });
    }

    function captchaExampleErrorFunction(error) {
        /* Do something with the error */
    }
</script>

<div id="my-captcha-container">
    <!-- The contents of this container will be replaced by the captcha widget -->
</div>
```

構成設定の例

次のリストの例は、幅とタイトルのオプションをデフォルト以外で設定した renderCaptcha を示しています。

```
        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            dynamicWidth: true,
            skipTitle: true
```

```
        });
```

設定オプションの詳細な情報については、「CAPTCHA JavaScript API 仕様」を参照してください。

からの CAPTCHA レスポンスの処理 AWS WAF

このセクションでは、CAPTCHA レスポンスを処理する例を示します。

CAPTCHA アクションを持つ AWS WAF ルールは、リクエストに有効な CAPTCHA タイムスタンプを持つトークンがない場合、一致するウェブリクエストの評価を終了します。リクエストが GET テキスト/HTML 呼び出しの場合、CAPTCHA アクションは CAPTCHA パズルを含むインタースティシャルをクライアントに提供します。CAPTCHA JavaScript API を統合しない場合、インタースティシャルはパズルを実行し、エンドユーザーが問題を正しく解決すると、自動的にリクエストを再送信します。

CAPTCHA JavaScript API を統合し、CAPTCHA 処理をカスタマイズする場合は、終了 CAPTCHA レスポンスを検出し、カスタム CAPTCHA を提供する必要があります。その後、エンドユーザーがパズルを正しく解決した場合は、クライアントのウェブリクエストを再送信します。

次のコード例は、これを実行する方法を説明しています。

> **Note**
>
> AWS WAF CAPTCHA アクションレスポンスのステータスコードは HTTP 405 で、このコードのCAPTCHAレスポンスを認識するために使用します。保護されたエンドポイントが HTTP 405 ステータスコードを使用して同じ呼び出しのために他の種類のレスポンスを通信する場合、このサンプルコードはそれらのレスポンスのためにも CAPTCHA パズルをレンダリングします。

```
<!DOCTYPE html>
<html>
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>
<body>
    <div id="my-captcha-box"></div>
    <div id="my-output-box"></div>

    <script type="text/javascript">
    async function loadData() {
```

```
        // Attempt to fetch a resource that's configured to trigger a CAPTCHA
        // action if the rule matches. The CAPTCHA response has status=HTTP 405.
        const result = await AwsWafIntegration.fetch("/protected-resource");

        // If the action was CAPTCHA, render the CAPTCHA and return

        // NOTE: If the endpoint you're calling in the fetch call responds with HTTP
 405
        // as an expected response status code, then this check won't be able to tell
 the
        // difference between that and the CAPTCHA rule action response.

        if (result.status === 405) {
            const container = document.querySelector("#my-captcha-box");
            AwsWafCaptcha.renderCaptcha(container, {
                apiKey: "...API key goes here...",
                onSuccess() {
                    // Try loading again, now that there is a valid CAPTCHA token
                    loadData();
                },
            });
            return;
        }

        const container = document.querySelector("#my-output-box");
        const response = await result.text();
        container.innerHTML = response;
    }

    window.addEventListener("load", () => {
        loadData();
    });
    </script>
</body>
</html>
```

JS CAPTCHA API の API キーの管理

このセクションでは、API キーを生成および削除する手順について説明します。

JavaScript API を使用して AWS WAF CAPTCHA をクライアントアプリケーションに統合するには、JavaScript API 統合タグと、CAPTCHA パズルを実行するクライアントドメインの暗号化された API キーが必要です。

JavaScript の CAPTCHA アプリケーション統合では、暗号化された API キーを使用して、クライアントアプリケーションドメインに CAPTCHA API AWS WAF を使用するアクセス許可があることを確認します。JavaScript クライアントから CAPTCHA API を呼び出すときは、現在のクライアントのドメインを含むドメインリストに API キーを含めます。1 つの暗号化キーに最大 5 つのドメインを列挙することができます。

API キー要件

CAPTCHA 統合で使用する API キーには、そのキーを使用するクライアントに適用されるドメインが含まれている必要があります。

- クライアントのインテリジェントな脅威に対応した統合で `window.awsWafCookieDomainList` を指定する場合、API キーの少なくとも 1 つのドメインが `window.awsWafCookieDomainList` のトークンドメインの 1 つと完全一致するか、いずれかのトークンドメインの apex ドメインである必要があります。

  例えば、トークンドメイン `mySubdomain.myApex.com` の場合、API キー `mySubdomain.myApex.com` は完全に一致し、API キー `myApex.com` は apex ドメインです。どちらかのキーがトークンドメインに一致します。

  トークンドメインリストの設定については、「トークンで使用するドメインの提供」を参照してください。
- それ以外の場合は、現在のドメインが API キーに含まれている必要があります。現在のドメインは、ブラウザのアドレスバーで確認できるドメインです。

使用するドメインは、保護されたホストドメインとウェブ ACL 用に設定されたトークンドメインリストに基づいて、 が AWS WAF 受け入れるドメインである必要があります。詳細については、「AWS WAF 保護パック (ウェブ ACL) トークンドメインリスト設定」を参照してください。

API キーのリージョンを選択する方法

AWS WAF は、 AWS WAF が利用可能な任意のリージョンで CAPTCHA API キーを生成できます。

原則として、保護パック (ウェブ ACL) に使用するのと同じリージョンを CAPTCHA API キーに使用する必要があります。ただし、リージョナル保護パック (ウェブ ACL) のグローバルオーディエンスが予想される場合は、CloudFront にスコープされた CAPTCHA JavaScript 統合タグと CloudFront にスコープされた API キーを取得し、リージョナル保護パック (ウェブ ACL) で使用できます。このアプローチにより、クライアントは自分に最も近いリージョンから CAPTCHA パズルをロードできるため、レイテンシーが短縮されます。

CloudFront 以外のリージョンに限定されている CAPTCHA API キーは、複数のリージョンでは使用できません。これらは、限定されたリージョンでのみ使用できます。

クライアントドメインの API キーを生成するには

統合 URL を取得し、コンソールを介して API キーを生成および取得するには。

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで、[Application integration] (アプリケーション統合) を選択します。
3. ペインで、[アプリケーション統合のために有効にする保護パック (ウェブ ACL)] で、API キーに使用したいリージョンを選択します。[CAPTCHA 統合] タブの [API キー] ペインでリージョンを選択することもできます。
4. タブ [CAPTCHA 統合] を選択します。このタブには、統合で使用できる CAPTCHA JavaScript 統合タグと API キーリストが表示されます。どちらも選択したリージョンに限定されます。
5. [API キー] ペインで、[キーを生成] を選択します。[キー生成] ダイアログが表示されます。
6. キーに含めるクライアントドメインを入力します。最大 5 つまで入力できます。完了したら、[キーを生成] を選択します。インターフェイスが CAPTCHA 統合タブに戻り、新しいキーが一覧表示されます。

   一度作成された API キーは、イミュータブルです。キーを変更する必要がある場合は、新しいキーを生成し、代わりにそれを使用します。
7. (オプション) 新しく生成されたキーをコピーして、統合で使用します。

この作業には、REST APIs または言語固有の AWS SDKsのいずれかを使用することもできます。REST API コールは 「CreateAPIKey」と「ListAPIKeys」です。

API を削除するには

API キーを削除するには、REST API または言語固有の AWS SDKsのいずれかを使用する必要があります。REST API コールは 「DeleteAPIKey」です。コンソールでキーを削除することはできません。

キーを削除すると、 がすべてのリージョンでキーの使用を禁止する AWS WAF までに最大 24 時間かかることがあります。

AWS WAF モバイルアプリケーションの統合

このセクションでは、 AWS WAF モバイル SDKs を使用して、Android および iOS モバイルアプリと TV アプリ用の AWS WAF インテリジェントな脅威統合 SDKs を実装するトピックを紹介します。TV アプリの場合、SDK は Android TV や Apple TV などの主要なスマート TV プラットフォームと互換性があります。

- Android モバイルと TV アプリの場合、 SDK は Android API バージョン 23 (Android バージョン 6) 以降で動作します。Android バージョンの詳細については、「SDK Platform リリースノート」を参照してください。
- iOS モバイルアプリの場合、 SDK は iOS バージョン 13 以降で動作します。iOS バージョンの詳細については、「iOS と iPadOS のリリースノート」を参照してください。
- Apple TV アプリの場合、SDK は tvOS バージョン 14 以降で動作します。tvOS バージョンの詳細については、「tvOS のリリースノート」を参照してください。

モバイル AWS WAF SDK を使用すると、トークン認可を管理し、保護されたリソースに送信するリクエストにトークンを含めることができます。SDK を使用すると、クライアントによるこれらのリモートプロシージャコールに有効なトークンが含まれていることを確認できます。さらに、この統合がアプリケーションのページで実行されている場合、有効なトークンを含まないリクエストをブロックするなど、保護パック (ウェブ ACL) で緩和ルールを実装できます。

モバイル SDK にアクセスするには、「AWSへのお問い合わせ」にてサポート担当者までお問い合わせください。

> **Note**
>
> AWS WAF モバイル SDKs は CAPTCHA のカスタマイズには使用できません。

SDK を使用するための基本的なアプローチは、設定オブジェクトを使用してトークンプロバイダーを作成し、トークンプロバイダーを使用してトークンを取得することです AWS WAF。デフォルトでは、トークンプロバイダーは、保護されたリソースに対するウェブリクエストに取得したトークンを含めます。

主要なコンポーネントを示す SDK 実装の一部を次に示します。詳細な例については、「AWS WAF モバイル SDK のコード例」を参照してください。

iOS

```
let url: URL = URL(string: "protection pack (web ACL) integration URL")!
 let configuration = WAFConfiguration(applicationIntegrationUrl: url, domainName:
 "Domain name")
 let tokenProvider = WAFTokenProvider(configuration)
 let token = tokenProvider.getToken()
```

Android

```
URL applicationIntegrationURL = new URL("protection pack (web ACL) integration
 URL");
 String domainName = "Domain name";
 WAFConfiguration configuration =
 WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL).domainName(
 WAFTokenProvider tokenProvider = new WAFTokenProvider(Application context,
 configuration);
 WAFToken token = tokenProvider.getToken();
```

AWS WAF モバイル SDK のインストール

このセクションでは、 AWS WAF モバイル SDK をインストールする手順について説明します。

モバイル SDK にアクセスするには、「AWSへのお問い合わせ」にてサポート担当者までお問い合わせください。

モバイル SDK を最初にテスト環境で実装し、次に本番環境で実装します。

AWS WAF モバイル SDK をインストールするには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで、[Application integration] (アプリケーション統合) を選択します。
3. [インテリジェントな脅威に対応した統合] タブで、次の操作を行います。
   a. [アプリケーション統合が有効になっている保護パック (ウェブ ACL)] ペインで、統合する保護パック (ウェブ ACL) を見つけます。実装で使用するアプリケーション統合が有効になっ

ている保護パック (ウェブ ACL) 統合 URL をコピーして保存します。この URL は、API コール GetWebACL を通じて取得することもできます。

b. モバイルデバイスのタイプとバージョンを選択してから、[Download] (ダウンロード) を選択します。任意のバージョンを選択できますが、最新バージョンを使用することをお勧めします。 はデバイスのzipファイルを標準のダウンロード場所に AWS WAF ダウンロードします。

4. アプリケーション開発環境で、ファイルを任意の作業場所に解凍します。zip ファイルの最上位ディレクトリで、README を見つけて開きます。ファイルの指示READMEに従って、 AWS WAF モバイルアプリコードで使用するモバイル SDK をインストールします。
5. 次のセクションのガイダンスに従って、アプリケーションをプログラムします。

AWS WAF モバイル SDK 仕様

このセクションでは、 AWS WAF モバイル SDK の利用可能な最新バージョンに対応する SDK オブジェクト、オペレーション、および構成設定を一覧表示します。構成設定のさまざまな組み合わせでトークンプロバイダーとオペレーションがどのように連携するかについては、「AWS WAF モバイル SDK の仕組み」を参照してください。

WAFToken

AWS WAF トークンを保持します。

getValue()

WAFToken の String 表現を取得します。

WAFTokenProvider

モバイルアプリケーションでトークンを管理します。WAFConfiguration オブジェクトを使用してこれを実装します。

getToken()

バックグラウンド更新が有効になっている場合、キャッシュされたトークンが返されます。バックグラウンド更新が無効になっている場合、 への同期呼び出しがブロック AWS WAF され、新しいトークンを取得します。

loadTokenIntoProvider(WAFToken)

指定されたトークンを WAFTokenProvider にロードし、プロバイダーが管理していたトークンを置き換えます。トークンプロバイダーは新しいトークンの所有権を取得し、今後の更新

を処理します。このオペレーションでは、WAFConfiguration で setTokenCookie が有効になっている場合、Cookie ストアのトークンも更新されます。

onTokenReady(WAFTokenResultCallback)

アクティブなトークンの準備ができたら、トークンを更新し、指定されたコールバックを呼び出すようにトークンプロバイダーに指示します。トークンプロバイダーは、トークンがキャッシュされて準備ができたときに、バックグラウンドスレッドでコールバックを呼び出します。アプリケーションが最初にロードされたときや、アクティブ状態に戻ったときにこれを呼び出します。アクティブ状態に戻ることの詳細については、「the section called “アプリケーションが非アクティブ状態になった後のトークンの取得”」を参照してください。

Android または iOS アプリケーションの場合、WAFTokenResultCallback を、リクエストされたトークンの準備ができたときにトークンプロバイダーが呼び出すオペレーションに設定できます。WAFTokenResultCallback の実装では、パラメータ WAFToken、SdkError を取得する必要があります。iOS アプリケーションでは、代わりにインライン関数を作成できます。

storeTokenInCookieStorage(WAFToken)

指定された AWS WAF トークンを SDK の Cookie マネージャーに保存WAFTokenProviderするように に指示します。デフォルトでは、トークンは最初に取得されたときと更新されたときのみ、Cookie ストアに追加されます。アプリケーションが何らかの理由で共有 Cookie ストアをクリアした場合、SDK は次回の更新まで AWS WAF トークンを自動的に追加しません。

WAFConfiguration

WAFTokenProvider の実装のための設定を保持します。これを実装すると、保護パック (ウェブ ACL) の統合 URL、トークンで使用するドメイン名、トークンプロバイダーが使用するデフォルト以外の設定を指定します。

次のリストは、WAFConfiguration オブジェクトで管理できる構成設定を示しています。

applicationIntegrationUrl

アプリケーション統合 URL。これを AWS WAF コンソールまたは getWebACL API コールから取得します。

必須: はい

タイプ: アプリケーション固有の URL。iOS の場合は、「iOS URL」を参照してください。Android の場合は、「java.net URL」を参照してください。

backgroundRefreshEnabled

トークンプロバイダーがバックグラウンドでトークンを更新するかどうかを示します。これを設定すると、トークンプロバイダーは、自動トークン更新アクティビティを管理する構成設定に従って、バックグラウンドでトークンを更新します。

必須: いいえ

タイプ: Boolean

デフォルト値: TRUE

domainName

トークンで使用するドメインは、トークン取得とクッキーの保存に使用されます。例えば、example.com、aws.amazon.com です。これは通常、保護パック (ウェブ ACL) に関連付けられているリソースのホストドメインであり、ウェブリクエストの送信先です。ACFP マネージドルールグループ AWSManagedRulesACFPRuleSet の場合、通常はルールグループ設定で指定したアカウント作成パスのドメインと一致する単一のドメインになります。ATP マネージドルールグループ AWSManagedRulesATPRuleSet の場合、通常はルールグループ設定で指定したログインパスのドメインと一致する単一のドメインになります。

パブリックサフィックスは許可されません。たとえば、gov.au または co.uk をトークンドメインとして使用することはできません。

ドメインは、保護されたホストドメインと保護パック (ウェブ ACL) のトークンドメインリストに基づいて、 AWS WAF が受け入れるドメインである必要があります。詳細については、「AWS WAF 保護パック (ウェブ ACL) トークンドメインリスト設定」を参照してください。

必須: はい

タイプ: String

maxErrorTokenRefreshDelayMsec

失敗した試行後にトークンの更新を繰り返すまでの待機時間の最大値 (ミリ秒)。失敗した試行の自動再試行ごとに、指定された入力遅延時間までエクスポネンシャルバックオフが追加されます。この値は、トークンの取得が失敗し、maxRetryCount 回再試行された後に使用されます。

必須: いいえ

タイプ: Integer

デフォルト値: 5000 (5 秒)

許容される最小値: 1 (1 ミリ秒)

許容される最大値: 30000 (30 秒)

maxRetryCount

トークンがリクエストされたときに、エクスポネンシャルバックオフで実行する最大再試行回数。

必須: いいえ

タイプ: Integer

デフォルト値: Infinity

許容される最小値: 0

許容される最大値: 100

setTokenCookie

SDK の Cookie マネージャーがリクエストに、およびその他のエリアにトークン Cookie を追加するかどうかを示します。

TRUE 値の場合:

- cookie マネージャーは、パスが tokenCookiePath で指定されたパスの下にあるすべてのリクエストにトークン Cookie を追加します。
- WAFTokenProvider オペレーションは、トークンプロバイダーにロードするだけでなく、Cookie ストアのトークン loadTokenIntoProvider() を更新します。

必須: いいえ

タイプ: Boolean

デフォルト値: TRUE

tokenCookiePath

setTokenCookie が TRUE の場合に使用されます。SDK の cookie マネージャーでトークン cookie を追加する最上位レベルのパスを示します。マネージャーは、このパスに送信するすべてのリクエストとすべての子パスにトークン cookie を追加します。

例えば、これを /web/login に設定すると、マネージャーには、/web/login に送信されるすべてのトークン cookie と、その子パスのいずれかが含まれます (/web/login/help など)。/、/web、/web/order などの他のパスに送信されたリクエストのトークンは含まれません。

必須: いいえ

タイプ: String

デフォルト値: /

tokenRefreshDelaySec

バックグラウンドの更新に使用されます。バックグラウンドトークンが更新されるまでの最大時間 (秒)。

必須: いいえ

タイプ: Integer

デフォルト値: 88

許容される最小値: 88

許容される最大値: 300 (5 分)

AWS WAF モバイル SDK エラー

このセクションでは、現在の AWS WAF モバイル SDK バージョンで発生する可能性のあるエラーを一覧表示します。

SdkError

トークンの取得に失敗した場合に返されるエラータイプ。Android と iOS SDK のエラータイプは同じです。

AWS WAF モバイル SDK には次のエラータイプがあります。

invalidChallenge

このエラーは、トークンサーバーが無効なチャレンジデータを返すか、レスポンス BLOB が攻撃者によって変更された場合に返されます。

errorInvokingGetChallengeEndpoint

このエラーは、トークンサーバーが成功しないレスポンスコードをクライアントに返すか、ネットワークエラーが発生したときに返されます。

invalidVerifyChallengeResponse

このエラーは、 AWS WAF サーバーの検証レスポンスaws-waf-tokenから を取得する際にエラーが発生した場合、またはサーバーレスポンスが改ざんされた場合に返されます。

errorInvokingVerifyEndpoint

このエラーは、クライアントが AWS WAF サーバーから不正な応答を受け取ったとき、または解決されたチャレンジを検証するときにネットワークエラーを受け取ったときに返されます。

internalError

このエラーは、SDK 自体の内部で発生する可能性のある他のすべてのエラーに対して返されます。

socketTimeoutException

このエラーは、トークンの取得中にネットワークエラーが発生したときに返されることがよくあります。

これにエラー、以下によって発生する可能性があります。

- 低ネットワーク帯域幅: ネットワーク接続設定を確認する
- ミューテーションされたアプリケーション統合 URL: AWS WAF コンソールに表示される内容から統合 URL が変更されていないことを確認します。

AWS WAF モバイル SDK の仕組み

このセクションでは、 AWS WAF モバイル SDK クラス、プロパティ、およびオペレーションがどのように連携するかについて説明します。

モバイル SDK は、トークンの取得と利用のために使用できる設定可能なトークンプロバイダーを提供します。トークンプロバイダーは、許可するリクエストが正規の顧客からのものであることを検証します。保護するリソースに AWS リクエストを送信するときは AWS WAF、Cookie にトークンを含めてリクエストを検証します。トークン cookie は手動で処理することも、トークンプロバイダーに処理させることもできます。

このセクションでは、モバイル SDK に含まれるクラス、プロパティ、およびメソッド間のインタラクションについて説明します。SDK の仕様については、「AWS WAF モバイル SDK 仕様」を参照してください。

トークンの取得とキャッシュ

モバイルアプリケーションでトークンプロバイダーインスタンスを作成するときに、トークンとトークンの取得を管理する方法を設定します。主に、アプリケーションのウェブリクエストで使用するための、有効で期限切れになっていないトークンを維持する方法を選択できます。

- [Background refresh enabled] (バックグラウンド更新が有効) - これがデフォルトのトランスコードプリセットです。トークンプロバイダーは、バックグラウンドでトークンを自動的に更新し、キャッシュします。バックグラウンド更新が有効になっている場合、`getToken()` を呼び出すと、オペレーションはキャッシュされたトークンを取得します。

  トークンプロバイダーは、設定可能な間隔でトークンの更新を実行します。これにより、アプリケーションがアクティブな間、期限切れでないトークンは常にキャッシュ内で利用可能な状態となります。アプリケーションが非アクティブ状態の間、バックグラウンドの更新が一時停止されます。詳細については、「アプリケーションが非アクティブ状態になった後のトークンの取得」を参照してください。
- [Background refresh disabled] (バックグラウンド更新が無効) - バックグラウンドトークンの更新を無効にして、オンデマンドでのみトークンを取得できます。オンデマンドで取得されたトークンはキャッシュされません。また、必要に応じて複数のトークンを取得できます。各トークンは、取得する他のトークンとは独立しており、有効期限を計算するために使用される独自のタイムスタンプを備えています。

  バックグラウンド更新が無効になっている場合のトークンの取得には、次の選択肢があります。
  - **`getToken()`** – バックグラウンド更新を無効に`getToken()`して を呼び出すと、呼び出しは同期的に新しいトークンを取得します AWS WAF。これは、メインスレッドで呼び出すと、アプリケーションの応答性に影響する可能性のあるブロッキング呼び出しである場合があります。
  - **`onTokenReady(WAFTokenResultCallback)`** - この呼び出しは、新しいトークンを非同期的に取得し、トークンの準備ができたときに提供された結果コールバックをバックグラウンドスレッドで呼び出します。

トークンプロバイダーが失敗したトークンの取得を再試行する方法

トークンプロバイダーは、取得に失敗したときにトークンの取得を自動的に再試行します。再試行は、開始の再試行の待ち時間が 100 ミリ秒のエクスポネンシャルバックオフを使用して最初に実行

されます。エクスポネンシャル再試行の詳細については、「AWSでのエラー再試行とエクスポネンシャルバックオフ」を参照してください。

再試行回数が設定された maxRetryCount に達すると、トークンプロバイダーは、トークン取得のタイプに応じて、試行を停止するか、maxErrorTokenRefreshDelayMsec ミリ秒ごとの試行に切り替えます。

- **onTokenReady()** – トークンプロバイダーは、試行間の待機時間を maxErrorTokenRefreshDelayMsec ミリ秒に切り替えて、トークン取得の試行を続行します。
- バックグラウンド更新 – トークンプロバイダーは、試行間の待機時間を maxErrorTokenRefreshDelayMsec ミリ秒に切り替えて、トークンの取得の試行を続行します。
- バックグラウンド更新が無効になっている場合のオンデマンド **getToken()** 呼び出し – トークンプロバイダーはトークンの取得の試行を停止し、前のトークン値を返します。前のトークンがない場合は null 値を返します。

トークン取得の再試行シナリオ

トークンプロバイダーがトークンを取得しようとすると、トークンの取得フローのどこでトークンの取得が失敗するかに応じて、自動再試行が発生する可能性があります。このセクションでは、自動再試行が表示される可能性のある場所を一覧表示します。

- /inputs または /verify による AWS WAF チャレンジの取得または検証:
  - AWS WAF チャレンジを取得して検証するリクエストが行われて失敗すると、自動再試行が発生する可能性があります。
  - ここで自動再試行が socketTimeoutException エラーとともに発生することがあります。これには、次のような複数の原因が考えられます。
    - 低ネットワーク帯域幅: ネットワーク接続設定を確認する
    - ミューテーションされたアプリケーション統合 URL: AWS WAF コンソールに表示される内容から統合 URL が変更されていないことを確認します。
  - 自動再試行カウントは、maxRetryCount() 関数で設定できます
- トークンの更新:
  - トークンハンドラーを介してトークンの更新リクエストが行われると、自動再試行が発生する可能性があります。
  - ここでの自動再試行数は、maxRetryCount() 関数で設定できます。

自動再試行のない設定は、maxRetryCount(0) を設定することで可能です。

トークンイミュニティ時間とバックグラウンド更新

ウェブ ACL で設定したトークンイミュニティ時間は、 AWS WAF モバイル SDK で設定したトークン更新間隔とは無関係です。バックグラウンド更新を有効にすると、SDK は tokenRefreshDelaySec() を使用して指定した間隔でトークンを更新します。これにより、設定されたイミュニティ時間に応じて、複数の有効なトークンが同時に存在する可能性があります。

複数の有効なトークンを防ぐには、バックグラウンド更新を無効にし、getToken() 関数を使用してモバイルアプリでトークンのライフサイクルを管理できます。

アプリケーションが非アクティブ状態になった後のトークンの取得

バックグラウンド更新は、アプリケーションがアプリケーションタイプについてアクティブであるとみなされる場合にのみ実行されます。

- iOS – バックグラウンド更新は、アプリケーションがフォアグラウンドにあるときに実行されます。
- Android - バックグラウンドの更新は、アプリケーションがフォアグラウンドまたはバックグラウンドのいずれにあるかにかかわらず、アプリケーションが閉じられていないときに実行されます。

アプリケーションが設定された tokenRefreshDelaySec 秒より長くバックグラウンド更新をサポートしない状態のままである場合、トークンプロバイダーはバックグラウンド更新を一時停止します。例えば、iOS アプリケーションの場合、tokenRefreshDelaySec が 300 で、300 秒以を超える時間にわたって、アプリケーションが閉じられていたり、バックグラウンド状態になっていたりすると、トークンプロバイダーはトークンの更新を停止します。アプリケーションがアクティブな状態に戻ると、トークンプロバイダーは自動的にバックグラウンド更新を再開します。

アプリケーションがアクティブ状態に戻ったら、トークンプロバイダーが新しいトークンを取得してキャッシュしたときに通知を受け取ることができるように onTokenReady() を呼び出します。キャッシュには最新の有効なトークンがまだ含まれていない可能性があるため、単に getToken() を呼び出さないでください。

アプリケーション統合 URL

AWS WAF モバイル SDK アプリケーション統合 URL は、アプリケーション統合を有効にしたウェブ ACL を指します。この URL は、リクエストを正しいバックエンドサーバーにルーティングし、顧客に関連付けます。ハードセキュリティコントロールとして機能しないため、統合 URL を公開してもセキュリティリスクは生じません。

提供された統合 URL を技術的に変更しても、トークンを取得できます。ただし、チャレンジ解決率の可視性が失われたり、socketTimeoutException エラーによるトークンの取得の失敗が発生する可能性があるため、これはお勧めしません。

依存関係

ダウンロード可能な各 AWS WAF モバイル SDK には、SDK の特定バージョンの依存関係を一覧表示する README ファイルが含まれています。お使いのバージョンのモバイル SDK の依存関係については、README を参照してください。

難読化/ProGuard (Android SDK のみ)

ProGuard などの難読化または最小化製品を使用する場合は、モバイル SDK が正しく動作するように特定の名前空間を除外する必要がある場合があります。お使いのバージョンのモバイル SDK の README をチェックして、名前空間と除外ルールのリストを見つけます。

AWS WAF モバイル SDK のコード例

このセクションでは、モバイル SDK を使用するためのコード例を提供します。

トークンプロバイダーの初期化とトークンの取得

設定オブジェクトを使用して、トークンプロバイダーインスタンスを開始します。その後、使用可能なオペレーションを使用してトークンを取得できます。必要なコードの基本コンポーネントを次に示します。

iOS

```
let url: URL = URL(string: "protection pack (web ACL) integration URL")!
let configuration = WAFConfiguration(applicationIntegrationUrl: url, domainName:
 "Domain name")
let tokenProvider = WAFTokenProvider(configuration)

//onTokenReady can be add as an observer for
 UIApplication.willEnterForegroundNotification
self.tokenProvider.onTokenReady() { token, error in
 if let token = token {
 //token available
 }

 if let error = error {
 //error occurred after exhausting all retries
```

```
 }
}

//getToken()
let token = tokenProvider.getToken()
```

Android

Java の例:

```
String applicationIntegrationURL = "protection pack (web ACL) integration URL";
//Or
URL applicationIntegrationURL = new URL("protection pack (web ACL) integration
 URL");

String domainName = "Domain name";

WAFConfiguration configuration =
 WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL).domainName(
WAFTokenProvider tokenProvider = new WAFTokenProvider(Application context,
 configuration);

// implement a token result callback
WAFTokenResultCallback callback = (wafToken, error) -> {
 if (wafToken != null) {
 // token available
 } else {
 // error occurred in token refresh
 }
};

// Add this callback to application creation or activity creation where token will
 be used
tokenProvider.onTokenReady(callback);

// Once you have token in token result callback
// if background refresh is enabled you can call getToken() from same tokenprovider
 object
// if background refresh is disabled you can directly call getToken()(blocking call)
 for new token
WAFToken token = tokenProvider.getToken();
```

Kotlin の例:

```
import com.amazonaws.waf.mobilesdk.token.WAFConfiguration
import com.amazonaws.waf.mobilesdk.token.WAFTokenProvider

private lateinit var wafConfiguration: WAFConfiguration
private lateinit var wafTokenProvider: WAFTokenProvider

private val WAF_INTEGRATION_URL = "protection pack (web ACL) integration URL"
private val WAF_DOMAIN_NAME = "Domain name"

fun initWaf() {
 // Initialize the tokenprovider instance
 val applicationIntegrationURL = URL(WAF_INTEGRATION_URL)
 wafConfiguration =
  WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL)
   .domainName(WAF_DOMAIN_NAME).backgroundRefreshEnabled(true).build()
 wafTokenProvider = WAFTokenProvider(getApplication(), wafConfiguration)

  // getToken from tokenprovider object
  println("WAF: "+ wafTokenProvider.token.value)

  // implement callback for where token will be used
  wafTokenProvider.onTokenReady {
   wafToken, sdkError ->
  run {
   println("WAF Token:" + wafToken.value)
  }
 }
}
```

SDK による HTTP リクエストでのトークン cookie の提供の許可

`setTokenCookie` が `TRUE` である場合、トークンプロバイダーは、`tokenCookiePath` で指定されたパスの下のすべての場所に対するウェブリクエストにトークン cookie を含めます。デフォルトでは、`setTokenCookie` は `TRUE`、`tokenCookiePath` は `/` です。

トークン cookie のパスを指定することで、トークン cookie を含むリクエストの範囲を絞り込むことができます (例: `/web/login`)。これを行う場合は、他のパスに送信するリクエストのトークンが AWS WAF ルールで検査されていないことを確認します。`AWSManagedRulesACFPRuleSet` ルールグループを使用する場合、アカウントの登録パスと作成パスを設定すると、ルールグループはそれらのパスに送信されるリクエスト内のトークンをチェックします。詳細については、「ACFP マネージドルールグループをウェブ ACL に追加」を参照してください。同様

に、AWSManagedRulesATPRuleSet ルールグループを使用する場合は、ログインパスを設定し、ルールグループはそのパスに送信されるリクエストのトークンをチェックします。詳細については、「ATP マネージドルールグループを保護パック (ウェブ ACL) に追加」を参照してください。

iOS

setTokenCookie が の場合TRUE、トークンプロバイダーは AWS WAF トークンを に保存HTTPCookieStorage.sharedし、 で指定したドメインへのリクエストに Cookie を自動的に含めますWAFConfiguration。

```
let request = URLRequest(url: URL(string: domainEndpointUrl)!)
//The token cookie is set automatically as cookie header
let task = URLSession.shared.dataTask(with: request) { data, urlResponse, error  in
}.resume()
```

Android

setTokenCookie が の場合TRUE、トークンプロバイダーはアプリケーション全体で共有されているCookieHandlerインスタンスに AWS WAF トークンを保存します。トークンプロバイダーは、WAFConfiguration で指定したドメインへのリクエストに cookie を自動的に含めます。

Java の例:

```
URL url = new URL("Domain name");
//The token cookie is set automatically as cookie header
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
connection.getResponseCode();
```

Kotlin の例:

```
val url = URL("Domain name")
//The token cookie is set automatically as cookie header
val connection = (url.openConnection() as HttpsURLConnection)
connection.responseCode
```

CookieHandler デフォルトインスタンスが既に初期化されている場合、トークンプロバイダーは、それを使用して cookie を管理します。そうでない場合、トークンプロバイダーは AWS WAF トークンを使用して新しいCookieManagerインスタンスを初期化CookiePolicy.ACCEPT_ORIGINAL_SERVERし、この新しいインスタンスを のデフォルトインスタンスとして設定しますCookieHandler。

次のコードは、アプリケーションで使用できない場合に cookie マネージャーと cookie ハンドラーを SDK が初期化する方法を示しています。

Java の例:

```
CookieManager cookieManager = (CookieManager) CookieHandler.getDefault();
if (cookieManager == null) {
 // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
 cookieManager = new CookieManager();
 CookieHandler.setDefault(cookieManager);
}
```

Kotlin の例:

```
var cookieManager = CookieHandler.getDefault() as? CookieManager
if (cookieManager == null) {
 // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
 cookieManager = CookieManager()
 CookieHandler.setDefault(cookieManager)
}
```

HTTP リクエストにおけるトークン cookie の手動による提供

`setTokenCookie` を FALSE に設定した場合、保護されたエンドポイントに対するリクエストで、cookie HTTP リクエストヘッダーとしてトークン cookie を手動で提供する必要があります。次のコードは、これを実行する方法を説明しています。

iOS

```
var request = URLRequest(url: wafProtectedEndpoint)
request.setValue("aws-waf-token=token from token provider", forHTTPHeaderField:
 "Cookie")
request.httpShouldHandleCookies = true
URLSession.shared.dataTask(with: request) { data, response, error in }
```

Android

Java の例:

```
URL url = new URL("Domain name");
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
```

```
String wafTokenCookie = "aws-waf-token=token from token provider";
connection.setRequestProperty("Cookie", wafTokenCookie);
connection.getInputStream();
```

Kotlin の例:

```
val url = URL("Domain name")
val connection = (url.openConnection() as HttpsURLConnection)
val wafTokenCookie = "aws-waf-token=token from token provider"
connection.setRequestProperty("Cookie", wafTokenCookie)
connection.inputStream
```

CAPTCHA および Challengeの AWS WAF

このセクションでは、 CAPTCHA と Challengeの操作方法について説明します AWS WAF。

AWS WAF ルールの検査基準に一致するウェブリクエストに対して CAPTCHAまたは Challengeアクションを実行するようにルールを設定できます。また、CAPTCHA パズルやブラウザチャレンジをローカルで実行するように JavaScript クライアントアプリケーションをプログラムすることもできます。

CAPTCHA パズルとサイレントチャレンジは、ブラウザが HTTPS エンドポイントにアクセスしている場合にのみ実行できます。トークンを取得するには、ブラウザクライアントが安全なコンテキストで実行されている必要があります。

- CAPTCHA – エンドユーザーが CAPTCHA パズルを解いて、人間がリクエストを送信していることを証明する必要があります。CAPTCHA パズルは、人間にとっては非常に簡単かつ短時間で完了に成功できる一方、コンピュータにとっては完了に成功、あるいは有意義な成功率でランダムに完了させることを困難にすることを意図しています。

  保護パック (ウェブ ACL) ルールでは、Block アクションが正当なリクエストを多く止めてしまう場合によく CAPTCHA が使用されますが、すべてのトラフィックを許可すると、ボットなどからの望ましくないリクエストが非常に多くなる可能性があります。ルールアクションの動作については、AWS WAF CAPTCHA および Challenge ルールアクションの仕組み を参照してください。

  クライアントアプリケーション統合 API で CAPTCHA パズルの実装をプログラムすることもできます。パズルをクライアントアプリケーションにプログラムするときに、クライアントアプリケーションでパズルの動作と配置をカスタマイズできます。詳細については、「でのクライアントアプリケーション統合 AWS WAF」を参照してください。

- Challenge – サイレントチャレンジを実行して、クライアントセッションがボットではなく、ブラウザであることを検証する必要があります。検証は、エンドユーザーの関与なしでバックグラウンドで実行されます。これは、CAPTCHA パズルでエンドユーザーのエクスペリエンスに悪影響を与えることなく、無効だと思われるクライアントを検証する場合に適したオプションです。ルールアクションの動作については、AWS WAF CAPTCHA および Challenge ルールアクションの仕組み を参照してください。

  Challenge ルールアクションは、「でのクライアントアプリケーション統合 AWS WAF」で説明されている、インテリジェントな脅威に対応したクライアント統合 API が実行するチャレンジと似ています。

> **Note**
>
> CAPTCHA または Challenge ルールアクションを 1 つのルールで使用、あるいはルールグループでルールアクションのオーバーライドとして使用すると、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

すべてのルールアクションオプションの説明については、でのルールアクションの使用 AWS WAF を参照してください。

トピック

- AWS WAF CAPTCHA パズル
- AWS WAF CAPTCHA および Challenge ルールアクションの仕組み
- CAPTCHA および Challenge アクションを使用するベストプラクティス

AWS WAF CAPTCHA パズル

このセクションでは、 AWS WAF CAPTCHA パズルの特徴と機能について説明します。

AWS WAF は、ユーザーが人間であることを確認するように要求する標準の CAPTCHA 機能を提供します。CAPTCHA は、「Completely Automated Public Turing test to tell Computers and Humans Apart」(コンピューターと人間を区別する完全自動公開チューリングテスト) の略です。CAPTCHA パズルは、人間がリクエストを送信していることを検証し、ウェブスクレイピング、クレデンシャルスタッフィング、スパムなどのアクティビティを防ぐように設計されます。CAPTCHA パズルは望ましくないリクエストをすべて排除することはできません。機械学習と人工知能を駆使することによって多くの CAPTCHA パズルが解決されました。CAPTCHA を回避するため、一部の組織は人間

が介入した自動化技術で補完しています。それにもかかわらず、CAPTCHA は洗練度の低いボットトラフィックを防ぎ、大規模な運営に必要なリソースを増やすための便利なツールとして役割を果たし続けています。

AWS WAF は CAPTCHA パズルをランダムに生成し、ローテーションスルーして、ユーザーに固有の課題が提示されるようにします。 AWS WAF は定期的に新しいタイプのパズルとスタイルを追加して、自動化手法に対して効果的を維持します。 AWS WAF CAPTCHA スクリプトは、パズルに加えて、タスクが人間によって完了されていることを確認し、再生攻撃を防ぐために、クライアントに関するデータを収集します。

各 CAPTCHA パズルには、エンドユーザーが新しいパズルをリクエストしたり、音声パズルと視覚パズルを切り替えたり、追加の指示にアクセスしたり、パズルの解答を送信したりするための標準的なコントロールセットが含まれています。すべてのパズルには、スクリーンリーダー、キーボードコントロール、コントラスト色のサポートが含まれています。

AWS WAF CAPTCHA パズルは、ウェブコンテンツアクセシビリティガイドライン (WCAG) の要件を満たしています。詳細については、World Wide Web Consortium (W3C) ウェブサイトの「Web Content Accessibility Guidelines (WCAG) Overview」(Web Content Accessibility Guidelines (WCAG) の概要) を参照してください。

トピック

- CAPTCHA パズル言語へのサポート
- CAPTCHA パズルの例

CAPTCHA パズル言語へのサポート

このセクションでは、 AWS WAF CAPTCHA パズルでサポートされている言語を一覧表示します。

CAPTCHA パズルは、クライアントブラウザ言語での書面による指示、またはブラウザ言語がサポートされていない場合は英語で始まります。このパズルには、ドロップダウンメニューによって代替言語オプションを用意しています。

ユーザーは、ページの下部にあるヘッドフォンアイコンを選択して、音声指示に切り替えることができます。音声バージョンのパズルでは、ユーザーがテキストボックスに入力する必要があるテキストに関する指示に、バックグラウンドノイズを重ねて発信します。

次の表に、CAPTCHA パズルの書面的な手順と、各選択肢の音声サポートで選択できる言語を示します。

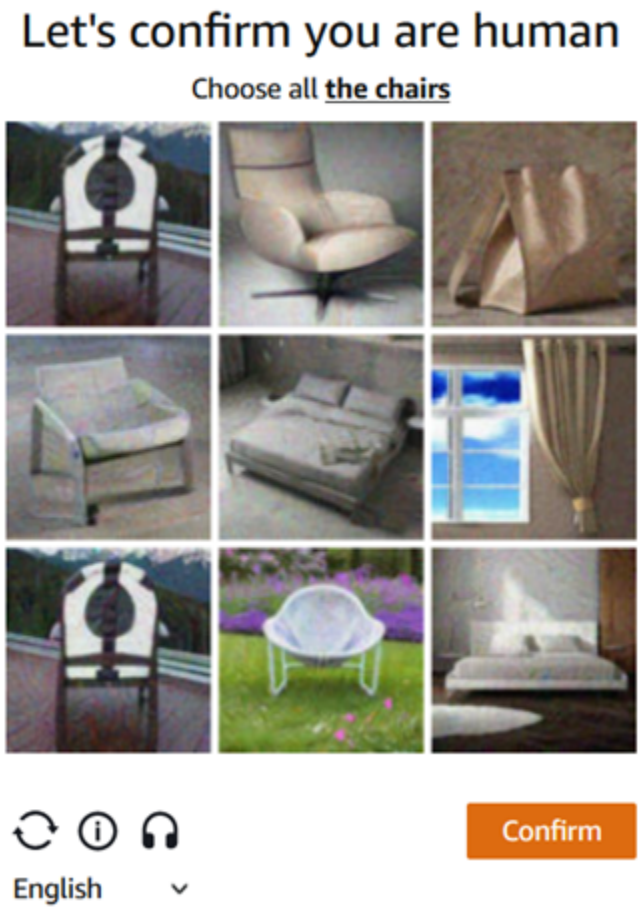
AWS WAF CAPTCHA パズルでサポートされている言語

書面的な指示のサポート	ロケールコード	音声指示のサポート
アラビア語	ar-SA	アラビア語
簡体字中国語	zh-CN	英語の音声
Dutch	nl-NL	Dutch
英語	en-US	英語
French	fr-FR	フランス語
ドイツ語	de-DE	German
Italian	it-IT	Italian
Japanese	ja-JP	英語の音声
ブラジルポルトガル語	pt-BR	ブラジルポルトガル語
Spanish	es-ES	Spanish
Turkish	tr-TR	Turkish

CAPTCHA パズルの例

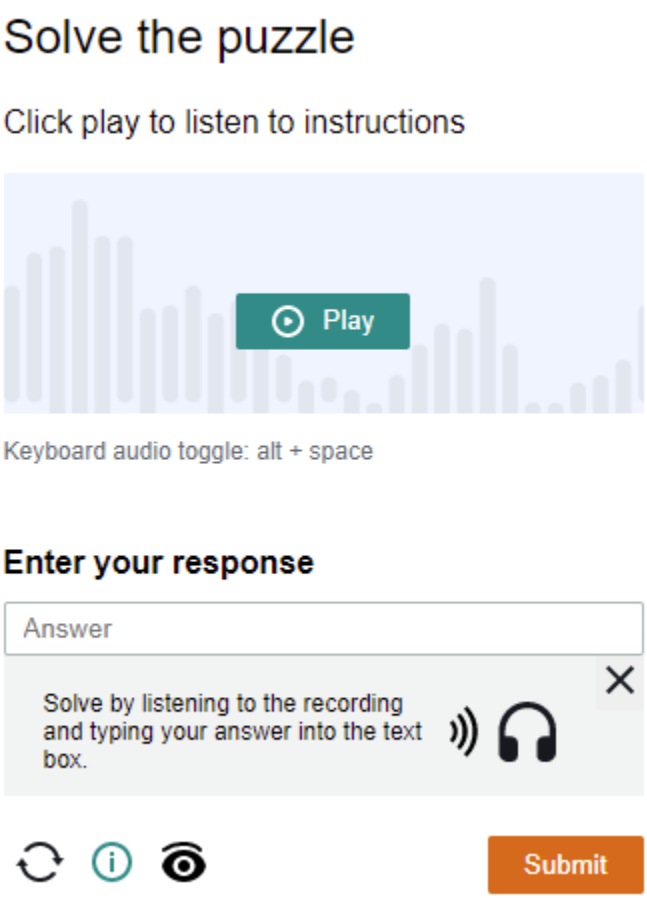
一般的なビジュアル CAPTCHA パズルでは、ユーザーが 1 つ以上のイメージを理解して操作できることを示すためのインタラクションが必要です。

次のスクリーンショットは、画像グリッドパズルの例を示しています。このパズルでは、特定のタイプのオブジェクトを含むグリッド内のすべての画像を選択する必要があります。



音声パズルオプションでは、ユーザーがテキストボックスに入力する必要があるテキストに関する発音指示に、バックグラウンドノイズを重ねて発信します。

次のスクリーンショットは、選択した音声パズルの表示内容を示しています。



AWS WAF CAPTCHA および Challenge ルールアクションの仕組み

このセクションでは、CAPTCHA と Challenge の仕組みについて説明します。

AWS WAF CAPTCHA と Challengeは標準のルールアクションであるため、実装は比較的簡単です。どちらかを使用するには、検査するリクエストを識別するルールの検査基準を作成し、2 つのルールアクションのうち 1 つを指定します。ルールアクションのオプションの一般的な情報については、「でのルールアクションの使用 AWS WAF」を参照してください。

サーバー側からサイレントチャレンジと CAPTCHA パズルを実装するだけでなく、サイレントチャレンジを JavaScript ならびに iOS および Android のクライアントアプリケーションに統合したり、JavaScript クライアントで CAPTCHA パズルをレンダリングしたりできます。これらの統合を使用すると、エンドユーザーがより良いパフォーマンスと CAPTCHA パズルエクスペリエンスを享受できるだけでなく、ルールアクションやインテリジェントな脅威の軽減を目的としたルールグループの使用に関連するコストを削減できます。これらのパラメータの詳細については「でのクライアントアプリケーション統合 AWS WAF」を参照してください。料金に関する情報については、[AWS WAF の料金]を参照してください。

トピック

- CAPTCHA および Challenge アクション動作
- ログとメトリクスの CAPTCHA および Challenge アクション

CAPTCHA および Challenge アクション動作

このセクションでは、CAPTCHA および Challenge アクションの役割について説明します。

ウェブリクエストが CAPTCHAまたは Challengeアクションでルールの検査基準に一致すると、 はトークンの状態とイミュニティ時間設定に従ってリクエストを処理する方法 AWS WAF を決定します。 は、リクエストが CAPTCHA パズルまたはチャレンジスクリプトインタースティシャルを処理できるかどうか AWS WAF も考慮します。スクリプトは HTML コンテンツとして処理されるように設計されており、HTML コンテンツを想定しているクライアントによってのみ適切に処理されることが可能です。

> **Note**
>
> CAPTCHA または Challenge ルールアクションを 1 つのルールで使用、あるいはルールグループでルールアクションのオーバーライドとして使用すると、追加料金が請求されます。詳細については、「AWS WAF 料金」を参照してください。

アクションがウェブリクエストを処理する方法

AWS WAF は、次のように CAPTCHAまたは Challengeアクションをウェブリクエストに適用します。

- 有効なトークン – アクションと同様にこれ AWS WAF を処理します。 は、ルールCountアクション用に設定したラベルとリクエストのカスタマイズ AWS WAF を適用し、保護パック (ウェブ ACL) の残りのルールを使用してリクエストの評価を続行します。
- トークンの欠落、無効、または期限切れ — リクエストの保護パック (ウェブ ACL) の評価 AWS WAF を中止し、意図した送信先への送信をブロックします。

  AWS WAF は、ルールアクションタイプに従って、クライアントに返されるレスポンスを生成します。

  - Challenge – AWS WAF はレスポンスに次のものが含まれます。
    - 値が `challenge` のヘッダー `x-amzn-waf-action`。

> **Note**
>
> クライアントブラウザで実行されている Javascript アプリケーションの場合、このヘッダーはアプリケーションのドメイン内でのみ使用できます。ヘッダーは、クロスドメイン取得には使用できません。詳細については、次のセクションを参照してください。

  - HTTP ステータスコード `202 Request Accepted`。
  - 値が `text/html` の `Accept` ヘッダーがリクエストに含まれている場合、応答にはチャレンジスクリプトを備えた JavaScript ページインタースティシャルが含まれます。
- CAPTCHA – レスポンスに以下 AWS WAF を含めます。
  - 値が `captcha` のヘッダー `x-amzn-waf-action`。

> **Note**
>
> クライアントブラウザで実行されている Javascript アプリケーションの場合、このヘッダーはアプリケーションのドメイン内でのみ使用できます。ヘッダーは、クロスドメイン取得には使用できません。詳細については、次のセクションを参照してください。

  - HTTP ステータスコード `405 Method Not Allowed`。
  - `text/html` の値の `Accept` ヘッダーがリクエストに含まれている場合、応答には CAPTCHA スクリプトを使った JavaScript ページのインタースティシャルが含まれます。

保護パック (ウェブ ACL) またはルールレベルでトークンの有効期限が切れるタイミングを設定するには、「でのタイムスタンプの有効期限とトークンイミュニティ時間の設定 AWS WAF」を参照してください。

ヘッダーは、クライアントブラウザで実行される JavaScript アプリケーションでは使用できません

が CAPTCHA またはチャレンジ AWS WAF レスポンスでクライアントリクエストに応答する場合、Cross-Origin Resource Sharing (CORS) ヘッダーは含まれません。CORS ヘッダーは、JavaScript アプリケーションがどのドメイン、HTTP メソッド、および HTTP ヘッダーを使用できるかをクライアントウェブブラウザに指示する一連のアクセスコントロールヘッダーです。CORS ヘッダーがないと、クライアントブラウザで実行されている JavaScript アプリケーションには

HTTP ヘッダーへのアクセスが許可されないため、CAPTCHA および Challenge 応答で提供される `x-amzn-waf-action` ヘッダーを読み取ることができません。

チャレンジと CAPTCHA インタースティシャルの機能

チャレンジインタースティシャルが実行されると、クライアントが応答に成功した後、まだトークンがない場合、インタースティシャルがトークンを初期化します。その後、チャレンジ解決のタイムスタンプでトークンを更新します。

CAPTCHA インタースティシャルを実行するとき、クライアントがまだトークンを持っていない場合、CAPTCHA インタースティシャルはまずチャレンジスクリプトを呼び出し、ブラウザにチャレンジしてトークンを初期化します。その後、インタースティシャルは CAPTCHA パズルを実行します。エンドユーザーがパズルの完成に成功すると、インタースティシャルはトークンを CAPTCHA 解決のタイムスタンプで更新します。

いずれの場合も、クライアントが応答に成功してスクリプトがトークンを更新した後、スクリプトは更新されたトークンを使用して元のウェブリクエストを再送信します。

がトークン AWS WAF を処理する方法を設定できます。詳細については、「AWS WAF インテリジェントな脅威の軽減におけるトークンの使用」を参照してください。

ログとメトリクスの CAPTCHA および Challenge アクション

このセクションでは、 が CAPTCHAおよび Challengeアクションのログ記録とメトリクス AWS WAF を処理する方法について説明します。

Challenge および CAPTCHA アクションは、Count のように終了しない場合もあれば、Block のように終了する場合もあります。結果は、リクエストがアクションタイプの有効期限が切れていない有効なトークンがあるかどうかによって異なります。

- 有効なトークン – アクションが有効なトークンを見つけてリクエストをブロックしない場合、 はメトリクスとログを次のように AWS WAF キャプチャします。
  - `CaptchaRequests` および `RequestsWithValidCaptchaToken` または `ChallengeRequests` および `RequestsWithValidChallengeToken` のいずれかのメトリクスを増分します。
  - CAPTCHA または Challenge のアクションで `nonTerminatingMatchingRules` エントリとして一致をログに記録します。次のリストは、CAPTCHA アクションを使ったこの一致タイプにおけるログのセクションを示しています。

```
    "nonTerminatingMatchingRules": [
```

```
    {
      "ruleId": "captcha-rule",
      "action": "CAPTCHA",
      "ruleMatchDetails": [],
      "captchaResponse": {
        "responseCode": 0,
        "solveTimestamp": 1632420429
      }
    }
  ]
```

- トークンの欠落、無効、または期限切れ – アクションがトークンの欠落または無効なためにリクエストをブロックすると、 はメトリクスとログを次のように AWS WAF キャプチャします。
  - CaptchaRequests または ChallengeRequests のメトリクスを増分させます。
  - 一致を HTTP 405 ステータスコードを含む CaptchaResponse エントリ、あるいは HTTP 202 ステータスコードを含む ChallengeResponse エントリとしてログ記録します。ログは、リクエストにトークンが不足しているか、トークンの有効期限が切れているか示します。ログには、がクライアントに CAPTCHA インタースティシャルページを送信したか、クライアントブラウザにサイレントチャレンジ AWS WAF を送信したかも示されます。次のリストは、CAPTCHA アクションを含むこのタイプの一致におけるログのセクションを示しています。

```
    "terminatingRuleId": "captcha-rule",
    "terminatingRuleType": "REGULAR",
    "action": "CAPTCHA",
    "terminatingRuleMatchDetails": [],
    ...
    "responseCodeSent": 405,
    ...
    "captchaResponse": {
      "responseCode": 405,
      "solveTimestamp": 0,
      "failureReason": "TOKEN_MISSING"
    }
```

AWS WAF ログの詳細については、「」を参照してくださいログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック。

AWS WAF メトリクスの詳細については、「」を参照してくださいAWS WAF メトリクスとディメンション。

ルールアクションのオプションの一般的な情報については、「でのルールアクションの使用 AWS WAF」を参照してください。

トークンのないリクエストは、ログとメトリクスに 2 回表示されるように見える

このセクションで説明されている CAPTCHA および Challenge アクション動作、ログ記録とメトリクスに基づいて、トークンのないリクエストは通常、ログとメトリクスに 2 回表示されます。これは、意図した 1 つのリクエストが実際にクライアントによって 2 回送信されるためです。

- トークンのない最初のリクエストは、欠落、無効、または期限切れのトークンについて、上記のログ記録とメトリクス処理を受け取ります。CAPTCHA または Challenge アクションはこの最初のリクエストを終了し、サイレントチャレンジまたは CAPTCHA パズルのいずれかでクライアントに応答します。
- クライアントはチャレンジまたはパズルを評価し、クライアントブラウザまたはエンドユーザーが正常に応答すると、新しく取得したトークンを使用してリクエストを再度送信します。この 2 番目のリクエストは、有効なトークンを持つリクエストについて、上記のログ記録とメトリクス処理を受け取ります。

CAPTCHA および Challenge アクションを使用するベストプラクティス

このセクションのガイダンスに従って、CAPTCHA AWS WAF またはチャレンジを計画および実装します。

CAPTCHA およびチャレンジの実装の計画

ウェブサイトの使用状況、保護するデータの機密性、リクエストのタイプに基づいて、CAPTCHA パズルまたはサイレントチャレンジを配置する場所を決定します。必要に応じてパズルを提示できるように、CAPTCHA に適用するリクエストを選択します。ただし、役に立たずにユーザーエクスペリエンスを低下させる可能性がある場合、パズルの提示を控えてください。Challenge アクションを使用してエンドユーザーへの影響が少ないサイレントチャレンジを実行しますが、リクエストが JavaScript 対応のブラウザから送信されていることを確認できます。

CAPTCHA パズルとサイレントチャレンジは、ブラウザが HTTPS エンドポイントにアクセスしている場合にのみ実行できます。トークンを取得するには、ブラウザクライアントが安全なコンテキストで実行されている必要があります。

クライアントで CAPTCHA パズルやサイレントチャレンジを実行する場所を決定

CSS や画像のリクエストなど、CAPTCHA による影響を受けたくないリクエストを特定します。CAPTCHA は必要な場合にのみ使用してください。たとえば、ログイン時に CAPTCHA チェッ

クを行う予定で、ユーザーが常にログインから別の画面に直接ダイレクトされる場合、2 つ目の画面で CAPTCHA チェックを要求することはおそらく不要であり、ユーザーエクスペリエンスを低下させる可能性があります。

がGETtext/htmlリクエストに応じて CAPTCHA パズルとサイレントチャレンジ AWS WAF のみを送信するように Challengeと CAPTCHAを設定します。POSTリクエスト、クロスオリジンリソース共有 (CORS) プリフライトOPTIONS要求、またはその他の非要求GETリクエストタイプに応答しても、パズルもチャレンジも実行することはできません。他のリクエストに対するブラウザの動作は異なる場合があり、インタースティシャルを適切に処理できない可能性があります。

クライアントが HTML を受け入れられても、CAPTCHA またはチャレンジインタースティシャルを処理できない場合があります。たとえば、小さな iFrame を持つウェブページ上のウィジェットは HTML を受け入れますが、CAPTCHA の表示またはその処理ができない場合があります。このようなタイプのリクエストのルールアクションは、HTML を受け入れないリクエストと同じように、設定しないでください。

以前に取得したトークンの確認に CAPTCHA または Challenge を使用

ルールアクションは、正規ユーザーが常にトークンを持っている必要がある場所で、有効なトークンの存在を確認する場合にのみ使用できます。このような状況では、リクエストでインタースティシャルを処理できるかどうかは問題ではありません。

例えば、JavaScript クライアントアプリケーションの CAPTCHA API を実装し、保護されたエンドポイントに最初のリクエストを送信する直前にクライアントで CAPTCHA パズルを実行する場合、最初のリクエストには、チャレンジと CAPTCHA の両方に有効なトークンが常に含まれている必要があります。JavaScript クライアントアプリケーション統合については、「AWS WAF JavaScript 統合」を参照してください。

この状況では、保護パック (ウェブ ACL) に、この最初の呼び出しと一致するルールを追加し、Challenge または CAPTCHA ルールアクションでルールを設定することができます。ルールが正規のエンドユーザーとブラウザに一致すると、アクションは有効なトークンを検索します。したがって、アクションがリクエストをブロックしたり、リクエストに応答してチャレンジや CAPTCHA パズルを送信したりすることはありません。ルールアクションの仕組みの詳細については、「CAPTCHA および Challenge アクション動作」を参照してください。

CAPTCHA および Challenge で機密性のある非 HTML データを保護する

次のアプローチで、API などの機密性の高い非 HTML データに CAPTCHA および Challenge 保護を使用できます。

1. HTML レスポンスを受け取り、機密性の高い HTML 以外のデータに対するリクエストの近くで実行されるリクエストを特定します。
2. HTML のリクエストと照合し、機密データのリクエストと照合する CAPTCHA または Challenge ルールを記述します。
3. CAPTCHA および Challenge イミュニティ時間の設定を調整し、通常のユーザーインタラクションで、クライアントが HTML リクエストから取得するトークンが、機密データのリクエストにおいて利用可能で有効期限が切れないようします。チューニングの情報については、「でのタイムスタンプの有効期限とトークンイミュニティ時間の設定 AWS WAF」を参照してください。

機密データのリクエストが CAPTCHA または Challenge ルールに一致すると、クライアントが以前のパズルまたはチャレンジからの有効なトークンをまだ持っている場合、そのリクエストはブロックされません。トークンが利用できない、あるいはタイムスタンプが有効期限が切れている場合、機密データをアクセスするリクエストは失敗します。ルールアクションの仕組みの詳細については、「CAPTCHA および Challenge アクション動作」を参照してください。

CAPTCHA および Challenge を使用して既存ルールの調整

既存のルールを確認し、変更するか追加するかを確認します。一般的なシナリオをいくつか次に示します。

- トラフィックをブロックするレートベースルールがあるものの、正規ユーザーのブロックを避けるためにレート制限を比較的高く維持する場合、ブロックルールの後に 2 つ目のレートベースルールを追加することを検討してください。2 つ目のルールにブロッキングルールよりも低い制限を設定し、ルールアクションを CAPTCHA また Challenge に設定します。ブロッキングルールは、高すぎるレートでリクエストを受け取らないように引き続きブロックします。新しいルールは、ほとんどの自動化トラフィックをさらに低いレートでブロックします。レートベースルールの詳細については、「でのレートベースのルールステートメントの使用 AWS WAF」を参照してください。
- リクエストをブロックするマネージドルールグループがある場合、一部またはすべてのルールの動作を Block から CAPTCHA または Challenge に切り替えることができます。これを行うには、マネージドルールグループの設定で、ルールアクション設定をオーバーライドします。ルールアクションのオーバーライドの情報については、「ルールグループのルールアクションの上書き」を参照してください。

デプロイする前に CAPTCHA およびチャレンジの実装をテストしてください

すべての新機能については、the section called “ 保護のテストと調整” のガイダンスに従ってください。

テストのとき、トークンタイムスタンプの有効期限要件を確認し、ウェブ ACL およびルールレベルのイミュニティ時間を設定して、ウェブサイトへのアクセスを制御および顧客に優れたエクスペリエンスを提供することのバランスが適切に維持できるようにします。詳細については、「でのタイムスタンプの有効期限とトークンイミュニティ時間の設定 AWS WAF」を参照してください。

AI トラフィック収益化

AI トラフィック収益化により、コンテンツプロバイダーと API プロバイダーは AI ボットとエージェントにエッジで保護されたリソースに直接アクセスするための料金を請求できます。クライアントが収益化されたリソースをリクエストすると、 は料金設定と承認された支払いネットワークを含む HTTP 402 Payment Required レスポンス AWS WAF を返します。クライアントは、選択した支払いネットワークで署名付き支払い認可を送信し、 AWS WAF 検証してコンテンツを取得し、サードパーティーのファシリテーターサービスと統合して支払いをチェーン上で決済し、応答を提供します。

AI トラフィック収益化は、machine-to-machine支払いにオープン支払いプロトコルを使用します。互換性のあるクライアントまたはエージェントのランタイムは、支払いを完了できます。

> **Note**
>
> AI トラフィック収益化はAmazon CloudFront でグローバルに利用でき、標準 AWS WAF 料金を超える追加料金はかかりません。

トピック

- AI トラフィック収益化の仕組み
- AI トラフィック収益化の開始方法
- 料金設定
- 支払いネットワークと決済
- 収益分析
- AI エージェントへのライセンス条項の伝達

AI トラフィック収益化の仕組み

AI トラフィック収益化では、machine-to-machine支払いに x402 オープンプロトコルを使用します。収益化されたリソースのリクエストライフサイクルを以下に示します。

1. リクエスト – クライアント (通常は AI エージェント) は、CloudFront ディストリビューション AWS WAF の保護対象リソースにリクエストを送信します。
2. ルール評価 – AWS WAF リクエストをルールに対して優先順位で評価します。Monetize アクションを持つルールが一致し、リクエストに有効な支払い承認が含まれていない場合、 は HTTP 402 Payment Required レスポンス AWS WAF を返します。詳細については、「ルールアクション」を参照してください。
3. Payment Required Challenge – HTTP 402 レスポンス (「Payment Required Challenge」) AWS WAF を返します。レスポンスには、以下を含む支払い指示が含まれます。
   a. USDC でのコンテンツ料金 (リクエストごと)
   b. 承認された支払いネットワーク (Base、Solana)
   c. パブリッシャーウォレットアドレス (payTo)
   d. 最大タイムアウト
   e. 支払いスキーム
4. 支払い承認 – クライアントは、ウォレットのプライベートキーまたはサーバーウォレット API を使用して支払い承認に署名します。クライアントは、署名付き認可を含む`payment-signature`ヘッダーを使用して元のリクエストを再送信します。
5. 検証 – 支払い認証情報 AWS WAF を検証し、十分な資金の移管と有効な認可を確認します。これは、リクエストパスで同期的に発生します。検証が失敗した場合、クライアントには 402 が提供され、コンテンツは提供されません。
6. コンテンツフェッチ — 検証に成功すると、コンテンツのリクエストが許可されます。
7. 決済 – コンテンツの取得が成功した場合 (2xx ステータスコード) 、支払いは Coinbase 開発者プラットフォームの x402 ファシリテーターサービスを介してブロックチェーンで決済されます。決済は同期的に行われます。コンテンツは確認済みの支払い後に提供されます。支払い決済が失敗した場合、クライアントには 402 が提供され、コンテンツは提供されません。
8. レスポンス – コンテンツは、決済確認の詳細を含む`payment-response`ヘッダーとともにクライアントに提供されます。

主な動作:

- 失敗したオリジンに対する支払いなし – オリジンが 4xx または 5xx を返した場合、決済はスキップされ、クライアントは課金されません。
- べき等性 – x402 プロトコルは、クライアントが二重支払いなしで最大 15 分間リクエストを再試行できるようにする支払い識別子拡張をサポートしています。ただし、拡張がクライアントによって使用されている場合に限ります。

- 再生保護 – 支払い承認はシングルユースです。有効な支払い識別子なしで支払いヘッダーを再利用すると、新しい 402 レスポンスになります。

x402 オープン支払いプロトコルの詳細については、「x402 ドキュメント」を参照してください。

サポートされているリソースタイプ

AI トラフィック収益化は、Amazon CloudFront ディストリビューションのリソースを保護します。CloudFront を通じて提供されるパスまたはコンテンツゾーンを収益化できます。これには、以下が含まれます。

- ウェブページと記事
- API エンドポイント
- データフィード
- メディアアセット
- 構造化データセット

AI トラフィック収益化の開始方法

前提条件

- Amazon CloudFront ディストリビューションに関連付けられた AWS WAF 保護パック (ウェブ ACL)
- 支払いを受け取るための Base、Solana、またはその両方の USDC ウォレットアドレス。
- (推奨)Bot AWS WAF Control を有効にして AI ボットトラフィックを ID で分類する

クイックスタート

1. Bot Control を有効にする – まだ有効になっていない場合は、AWS WAF Bot Control マネージドルールグループをウェブ ACL に追加します。
2. 保護パックの作成 (webACL) – AWS WAF コンソールで、Cloudfront (グローバル) リージョンの Protection Pack (webACL) に移動し、料金、ボットとエージェントのポリシー、および支払い設定を使用して新しいパックを作成します。CloudFront ディストリビューションに関連付けます。

3. MonetizationConfig の設定 – AI トラフィックの収益化を使用するには、ウェブ ACL `MonetizationConfig`で を設定します。この設定では、承諾する支払いネットワークと、収益化されたリクエストの基本料金を定義します。

MonetizationConfig には以下が含まれます。

- CurrencyMode – REAL 本番稼働用支払いまたはテストネットワーク支払いTEST用。
- CryptoConfig – チェーン、ウォレットアドレス、料金などの支払いネットワーク設定。

MonetizationConfig 構造

```
{
  "MonetizationConfig": {
    "CryptoConfig": {
      "PaymentNetworks": [
        {
          "Chain": "BASE",
          "WalletAddress": "0x1234567890abcdef1234567890abcdef12345678",
          "Prices": [
            {
              "Amount": "0.001",
              "Currency": "USDC"
            }
          ]
        },
        {
          "Chain": "SOLANA",
          "WalletAddress": "7xKXtg2CW87d97TXJSDpbD5jBkheTqA83TZRuJosgAsU",
          "Prices": [
            {
              "Amount": "0.001",
              "Currency": "USDC"
            }
          ]
        }
      ]
    }
  }
}
```

> **Important**
>
> `Amount` は、小数点以下第 3 位までの 10 進文字列として USDC で指定されます (例: `"0.001"` = リクエストあたり 0.001 USDC)。

サポートされている支払いネットワーク

Chain	Network	通貨	ユースケース
ベース	ベースメインネット (EVM L2)	USDC	本番稼働用支払い
ソラナ	Solana のメインネット	USDC	本番稼働用支払い
BASE_SEPOLIA	ベースセポリアテストネット	USDC	テストモード
SOLANA_DEVNET	Solana Devnet	USDC	テストモード

テストモード

テストモード (`CurrencyMode: TEST`) を使用すると、実際の支払いを開始する前に、テストブロックチェーンネットワークを使用して収益化設定を検証できます。この設定は、保護パック (ウェブ ACL) (ウェブ ACL) 全体に適用されます。

> **Important**
>
> AI トラフィック収益化ポリシーを実装するために、動作シグナルやリスクベースのシステムなどの複数の検出手法を使用して、インバウンドトラフィックを検査および分類します。これらのメソッドは高い信頼性の分類を提供するように設計されていますが、確率的であり、すべてのボットトラフィックを正しく識別または分類できない場合があります。当社では、精度を高めるために分析方法を継続的にテストおよび更新しています。ライブ収益化を有効にする前に、テストモードを使用してポリシーが期待される結果を生成することを確認することをお勧めします。

テストモードの有効化

MonetizationConfig TESTで CurrencyModeを に設定し、テストネットワークチェーンを設定します。

テストモードの動作

テストモードの場合:

- 支払いではテストネットワークを使用: Base Sepolia と Solana Devnet
- 実際の USDC の代わりに Testnet 蛇口 (パブリック蛇口から利用可能) などのテスト資金を使用する
- 完全な支払いフローは本番環境と同じように実行されます。検証、オリジンフェッチ、決済はすべてテストブロックチェーンで行われます。
- すべてのイベントは でログに記録されます。 CurrencyMode: TEST
- 収益分析はCurrencyMode: ["TEST"]フィルターでクエリ可能

> **Important**
>
> 本番環境で収益化ポリシーを適用する前に、内部検証のために非本番環境トラフィックにのみテストモードを使用します。

設定の検証

テストモードを使用して以下を確認します。

- さまざまなルールとコンテンツパスの正しい料金
- 支払いフローend-to-end (402 → 支払い承認 → 検証 → 決済)
- ウォレットアドレスの正確性 (テストウォレットに資金が到着)
- 分析フィールドとログフィールドが正しく入力されている

問題がなければ、MonetizationConfig を に更新CurrencyMode: REALし、実際の支払いの処理を開始するようにプロダクションチェーン (BASE、SOLANA) を設定します。

- 初期テストCurrencyMode: TESTのために から開始することも、 を使用して直接収益化を開始することもできますCurrencyMode: REAL。

- 収益化ルールの追加 – 収益化アクションを使用してルールを作成します。一致ステートメントを使用して、特定のパス、Bot Control ラベル、またはその他のリクエスト特性をターゲットにします。
- テスト – CloudFront ディストリビューションにテストリクエストを送信します。Monetize ルールに一致するリクエストは、支払いが必要なチャレンジ (402 レスポンス) を受け取ります。互換性のある支払いクライアントを使用してフローを完了します。
- Go Live – 本番稼働用支払いネットワーク (BASE、SOLANA) `CurrencyMode`を更新`REAL`して設定します。本番トラフィックを開く前に、テストウォレットに資金を提供しend-to-endを検証します。

次の手順

- AI トラフィック分析ダッシュボードを確認して、料金を設定する前に現在のボットトラフィックを理解します。
- エージェント層とコンテンツパスに基づいて差別化された料金を設定します。
- 収益分析を設定して収益をモニタリングします。

料金設定

基本料金

MonetizationConfig でリクエストごとに基本価格を設定します。料金は、小数点以下 3 桁までの 10 進 USD 文字列として指定されます。リクエストあたりの最低料金は 0.001 USDC です。

料金乗数

個々の Monetize ルールアクションで `PriceMultiplier`パラメータを使用して、ルールあたりの料金を調整します。実効価格は、基本価格にこの値を乗じたものです。

たとえば、基本料金が `"0.001"` (0.001 USD) で、ルールに PriceMultiplier がある場合`"3"`、そのルールに一致するリクエストの有効料金は 0.003 USD です。

インテント別の料金設定

検証階層ごとに異なる料金を設定できます。一般的なパターンは次のとおりです。

- 紹介トラフィックを駆動する検証済み AI 検索クローラの低価格

- RAG または要約を実行する既知のエージェントの標準料金
- 不明または未検証のエージェントの料金が高い
- トレーニングクローラ全体またはプレミアム料金でのブロック

> **Important**
>
> AI トラフィック収益化ポリシーを実装するために、動作シグナルやリスクベースのシステムなどの複数の検出手法を使用して、インバウンドトラフィックを検査および分類します。これらのメソッドは高い信頼性の分類を提供するように設計されていますが、確率的であり、すべてのボットトラフィックを正しく識別または分類できない場合があります。当社では、精度を高めるために分析方法を継続的にテストおよび更新しています。ライブ収益化を有効にする前に、テストモードを使用してポリシーが期待される結果を生成することを確認することをお勧めします。

ルールアクションの設定

階層ごとに、次のいずれかのアクションを設定できます。

- 収益化 – 終了アクション。Monetize アクションを持つルールが一致すると、 は後続のルールの評価 AWS WAF を停止します。リクエストに有効な支払い承認が含まれていない場合、 は HTTP 402 レスポンスを直接 AWS WAF 返し、リクエストはブロックされます。
- 許可 – 無料アクセス (紹介契約に基づく検証済み検索クローラなど) を付与します。
- ブロック – アクセスを完全に拒否します。
- カウント – アクセスを許可し、課金なしでリクエストをログに記録します。
- Captcha – エンドユーザーは、人間がリクエストを送信していることを証明するために CAPTCHA パズルを解決する必要があります。
- チャレンジ – クライアントセッションがボットではなくブラウザであることを確認する必要があるサイレントチャレンジを実行します。

重要: アクションと人的トラフィックを収益化する

Monetize アクションは、自動 AI エージェントトラフィック用に設計されています。リクエストが Monetize ルールと一致すると、 は、x402 プロトコル形式で機械読み取り可能な支払い指示を含む HTTP 402 Payment Required レスポンス AWS WAF を返します。標準ウェブブラウザとヒューマン

ユーザーは、この支払いフローを解釈または完了できません。402 レスポンスは、自動化されていないクライアントのアクセスを効果的にブロックします。

人間の訪問者を誤ってブロックしないようにするには、自動として識別されたトラフィックに対してのみ Monetize アクションを使用します。Monetize アクションを AWS WAF Bot Control ラベルと組み合わせることをお勧めします。これにより、ボットトラフィックのみが 402 チャレンジを受信し、人間のユーザーは引き続き通常どおりコンテンツにアクセスできます。

例: Bot Control ラベルを使用してボットトラフィックのみを収益化する

次のルール設定では、まず Bot Control を使用してトラフィックを分類し、次に Monetize アクションをボットとしてラベル付けされたリクエストにのみ適用されます。

```
{
  "Name": "MonetizeBotTrafficOnly",
  "Priority": 5,
  "Statement": {
    "LabelMatchStatement": {
      "Scope": "LABEL",
      "Key": "awswaf:managed:aws:bot-control:bot"
    }
  },
  "Action": {
    "Monetize": {
    }
  },
  "VisibilityConfig": {
    "CloudWatchMetricsEnabled": true,
    "MetricName": "MonetizeBotTrafficOnly",
    "SampledRequestsEnabled": true
  }
}
```

この例では、人間のユーザー (`awswaf:managed:aws:bot-control:bot`ラベルを付けない) からのリクエストは、一致せずにこのルールを通過し、後続のルールに進みます。Bot Control によってボットとして分類されたリクエストのみが、402 Payment Required Challenge を受け取ります。

このパターンをさらに絞り込むには、ボット階層ごとに個別のルールを作成します。たとえば、検証済みボットをより高い料金乗数で収益化しながら、検証済み検索クローラを無料で許可します。

レイテンシー特性

AI トラフィック収益化は、支払い処理を必要とするリクエストに数秒のレイテンシーを追加します。このオーバーヘッドには、支払い承認の検証とオンチェーン決済が含まれます。追加のレイテンシーは、トランザクションが試行されているリクエストにのみ適用されます。Monetize アクションと一致しないリクエストや、支払い署名がアタッチされていないリクエストは影響を受けません。

正確なレイテンシーは、決済時のブロックチェーンネットワークの状態によって異なります。

支払い処理エラーとスロットリング

AI トラフィックの収益化はサードパーティーのブロックチェーン決済サービスに依存するため、支払い処理が当社の管理外の理由で失敗することがあります。考えられる原因には、Coinbase 開発者プラットフォームの x402 ファシリテーターサービスの一時的な利用不能、ブロックチェーンネットワークの輻輳、チェーン上の決済中の一時的なエラーなどがあります。支払い処理が失敗した場合、コンテンツはクライアントに提供されません。クライアントは失敗を示すレスポンスを受け取り、リクエストを再試行できます。

さらに、過度に大量の支払いトラフィックをスロットリングして、支払い処理インフラストラクチャの整合性を保護し、不正使用を防ぐ AWS 可能性があります。スロットリングすると、支払いリクエストはエラーレスポンスを受け取り、短いバックオフ後に再試行する必要があります。通常のリクエストボリュームはスロットリングの影響を受けません。

支払いネットワークと決済

MonetizationConfig でウォレットアドレスを設定して、支払いを受け取る方法を選択します。支払いはウォレットに直接決済されます。 AWS は、受け取った支払いの資金の流れまたは資金の流れの当事者ではありません。

決済の仕組み

1. クライアントの支払い承認は、コンテンツがオリジンから取得される前に検証されます。
2. オリジンが正常なレスポンスを返した後、支払いはブロックチェーンで決済されます。
3. USDC は、クライアントのウォレットから設定されたウォレットアドレスに転送されます。
4. 決済確認は、クライアントへのレスポンスに含まれます。

支払い決済は、Coinbase Developer Platform の x402 ファシリテーターによって提供されます。Coinbase の利用規約に同意します。料金および支払い設定情報を Coinbase および関連するクライアントと共有するよう指示します。

収益分析

収益ダッシュボード

収益ダッシュボードには、以下が表示されます。

- 収益概要 – 合計収益、検証済みと未検証の収益内訳、合計決済数、合計 402 件の応答数 (GetRevenueStatisticsSummary)
- 収益別の上位のソース – 収益額でランク付けされた AI ボットを名前、カテゴリ、インテント、または組織別にグループ化 (TOP_SOURCES_BY_REVENUE を使用した GetRevenueStatistics)
- 収益別の上位パス – 収益額別のランク付けされたコンテンツパス (TOP_PATHS_BY_REVENUE を使用した GetRevenueStatistics)
- 経時的な収益 – 分単位、5 分単位、時間単位、または日単位の時系列グラフ (DATE_HISTOGRAM を使用した GetRevenueStatisticsTimeSeries)
- 経時的な支払いトラフィック – 経時的な支払い試行量 (GetRevenueStatisticsTimeSeries with PAYMENT_TRAFFIC)
- 決済レコード – ステータス (SETTLED、PENDING、FAILED、SERVICE_ERROR、SKIPPED_ORIGIN_ERROR)、支払者の住所、金額、ブロックチェーントランザクション ID (ListSettlementRecords) を含む個々のトランザクションの詳細

すべての収益データは、ソース名、カテゴリ、組織、インテントでフィルタリングできます。デフォルトでは、実通貨 (REAL) トランザクションのみが表示されます。CurrencyMode フィルターを使用してテストトランザクションを表示します。

ログフィールド

AWS WAF ログ記録を有効にすると、収益化イベントには次の追加フィールドが含まれます。

フィールド	説明
`action`	リクエスト時に実行される WAF アクション
`monetizeVerifyResponse.verificationStatus`	検証結果: VERIFIED、INSUFFICIENT_FUNDS、INVALID_PAYLOAD、INVALID_PAYMENT_REQUIREMENTS、SERVICE_ERROR

フィールド	説明
monetizeVerifyResponse.failureReason	検証失敗の理由 (成功時に空)
monetizeVerifyResponse.chainName	使用するブロックチェーンチェーン
monetizeVerifyResponse.network	CAIP-2 形式のブロックチェーンネットワーク識別子
monetizeVerifyResponse.amount	アトミックトークン単位の支払い額
monetizeVerifyResponse.currency	支払い通貨 (USDC など)
monetizeVerifyResponse.asset	トークン契約住所
monetizeVerifyResponse.payerAddress	クライアントのウォレットアドレスの支払い
monetizeVerifyResponse.idempotencyKey	再試行相関用の x402 支払いべき等性キー
monetizeVerifyResponse.currencyMode	通貨モード: REAL または TEST

詳細については、「the section called “ログ記録”」を参照してください。

メトリクス

メトリクスは Amazon CloudWatch の名前空間 で公開されますAWS/WAFV2。

メトリクス名	説明
MonetizeRequests	終了ルールにアクション Monetize がある場合に発行されます
MonetizeRequestsFailedVerification	終了ルールにアクション Monetize があり、検証ステータスが VERIFIED でない場合に発行されます

これらのメトリクスには、リージョン、ルール、WebACL、リソース、ResourceType、デバイス、国というディメンションがあります。

詳細については、「the section called “AWS WAF メトリクスとディメンション”」を参照してください。

AI エージェントへのライセンス条項の伝達

AI トラフィックの収益化は、エージェントに支払う金額を伝えますが、コンテンツに対して許可される金額は伝えません。機械読み取り可能な使用条件を伝えるには、RSL (Really Simple Licensing) を使用します。これは、機械読み取り可能なコンテンツライセンスのオープンスタンダードです。

RSL は、AI エージェントがライセンス条項を見つけるためのいくつかの検出メカニズムを定義します。

- robots.txt – 既存の robots.txt ファイルに RSL ディレクティブを追加します。エージェントは、標準のクロールプリフライト中に用語を検出します。
- HTTP リンクヘッダー – RSL ライセンス URL を参照するLinkヘッダーを HTTP レスポンスに挿入します。CloudFront で設定できます (以下を参照) 。
- HTML リンク要素 – HTML ページに<link rel="license">タグを埋め込みます。ウェブコンテンツに適していますが、API または非 HTML レスポンスには適用されません。
- RSS/Atom モジュール – ライセンスメタデータをフィードエントリにアタッチします。

RSL での CloudFront レスポンスヘッダーポリシーの使用

HTTP Linkヘッダー検出の場合、レスポンスに RSL ライセンスリファレンスを挿入するように CloudFront を設定できます。

1. 使用条件を説明する RSL ライセンス XML ファイルを作成し、安定した HTTPS URL (例:) でホストしますhttps://example.com/license.xml。RSL Collective の標準ライセンスを使用するか、カスタム用語を定義できます。
2. カスタムヘッダーを使用して CloudFront レスポンスヘッダーポリシーを作成します。
   - ヘッダー名: Link
   - 値: <https://example.com/license.xml>; rel="license"; type="application/rsl+xml"
3. このポリシーを、収益化されたコンテンツを提供するキャッシュ動作に関連付けます。

RSL をサポートする AI エージェントは、オリジンレスポンスごとに用語を自動的に検出します。

> **Note**
>
> CloudFront レスポンスヘッダーポリシーは、オリジンから提供されるレスポンスに適用されます。Monetize アクションによって提供される 402 Payment Required Challenge には、このヘッダーは含まれません。

レスポンスヘッダーポリシーの詳細については、「Amazon CloudFront デベロッパーガイド」の「CloudFront を使用した HTTP レスポンスヘッダーの追加」を参照してください。 Amazon CloudFront

RSL 仕様については、https://rslstandard.org/rsl を参照してください。

保護 AWS WAF パック (ウェブ ACL) トラフィックのデータ保護とログ記録

このセクションでは、 で使用できるデータログ記録、収集、保護オプションについて説明します AWS WAF。オプションは次のとおりです。

- ログ記録 – ウェブリクエストトラフィックのログを任意のログ記録先に送信するように保護パック (ウェブ ACL) を設定できます。この選択では、フィールドの秘匿化とフィルタリングを設定できます。ログ記録では、データ保護設定の適用後に使用可能なデータを使用します。

  このオプションについては、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。
- リクエストサンプリング – 評価対象のウェブリクエストをサンプリングするように保護パック (ウェブ ACL) を設定して、アプリケーションが受信するトラフィックのタイプを把握できます。リクエストサンプリングでは、データ保護設定の適用後に使用可能なデータを使用します。

  このオプションについては、「ウェブリクエストのサンプルの表示」を参照してください。
- Amazon Security Lake – Security Lake を設定して、保護パック (ウェブ ACL) データを収集できます。Security Lake は、正規化、分析、管理のためにさまざまな AWS ソースからログとイベントデータを収集します。Security Lake は、データ保護設定の適用後に使用可能なデータから収集します。

このオプションの詳細については、「Amazon Security Lake ユーザーガイド」の「Amazon Security Lake とは」および「 AWS のサービスからデータを収集する」を参照してください。

AWS WAF は、このオプションの使用に対して課金しません。料金については、「Amazon Security Lake ユーザーガイド」の「Security Lake Pricing」と「How Security Lake pricing is determined」を参照してください。

- データ保護 – ウェブトラフィックデータのデータ保護は、次の 2 つのレベルで設定できます。
  - 保護パック (ウェブ ACL) のデータ保護 – 保護パック (ウェブ ACL) ごとにデータ保護を設定できます。これにより、特定のウェブトラフィックデータを静的文字列または暗号化ハッシュに置き換えることができます。このレベルでのデータ保護は一元的に設定でき、すべてのログ記録とデータコレクションオプションに適用されます。

    このオプションについては、「データ保護」を参照してください。
  - ログ記録の秘匿化とフィルタリング – ログ記録のみの場合、ウェブトラフィックデータの一部をログから秘匿化するように設定し、ログに記録するデータをフィルタリングできます。このオプションは、設定したデータ保護設定に加えて、 が設定したログ記録先 AWS WAF に送信するデータにのみ影響します。

トピック

- ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック
- データ保護

ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック

このセクションでは、 AWS WAF 保護パック (ウェブ ACLs) のログ記録オプションについて説明します。

ログ記録を有効にして、ウェブ ACL で分析されるトラフィックに関する詳細情報を取得できます。ログに記録された情報には、 AWS がリソースからウェブリクエストを AWS WAF 受信した時間、リクエストに関する詳細情報、およびリクエストが一致したルールに関する詳細が含まれます。保護パック (ウェブ ACL) ログは、Amazon CloudWatch Logs ロググループ、Amazon Simple Storage Service (Amazon S3) バケット、または Amazon Data Firehose 配信ストリームに送信できます。

は、保護パック (ウェブ ACLs) に対して有効にできるログに加えて、 によって処理されたウェブサイトまたはアプリケーショントラフィックのサービスログ AWS も使用 AWS WAF して、 AWS 顧客およびサービスのセキュリティをサポートし、保護します。

> **Note**
>
> 保護パック (ウェブ ACL) のログ記録設定は、 AWS WAF ログにのみ影響します。特に、ログ記録用に編集されたフィールド設定は、リクエストサンプリングや Security Lake データ収集には影響しません。保護パック (ウェブ ACL) データ保護を設定することで、収集またはサンプリングからフィールドを除外できます。データ保護以外に、Security Lake データ収集は、Security Lake サービスを通じて完全に設定されます。

トピック

- 保護パック (ウェブ ACL) トラフィックのログ記録の料金に関する情報
- AWS WAF ログ記録の送信先
- 保護パック (ウェブ ACL) のログ記録の設定
- 保護パック (ウェブ ACL) レコードの検索
- 保護パック (ウェブ ACL) トラフィックのログフィールド
- 保護パック (ウェブ ACL) トラフィックのログ例

その他のデータ収集および分析オプション

ログ記録に加えて、データ収集と分析のために以下のオプションを有効にすることができます。

- Amazon Security Lake – Security Lake を設定して、保護パック (ウェブ ACL) データを収集できます。Security Lake は、正規化、分析、管理のためにさまざまな ソースからログとイベントデータを収集します。このオプションの詳細については、「Amazon Security Lake ユーザーガイド」の「Amazon Security Lake とは」および「 AWS のサービスからデータを収集する」を参照してください。

  AWS WAF は、このオプションの使用に対して課金しません。料金については、「Amazon Security Lake ユーザーガイド」の「Security Lake Pricing」と「How Security Lake pricing is determined」を参照してください。
- リクエストサンプリング – 評価対象のウェブリクエストをサンプリングするように保護パック (ウェブ ACL) を設定して、アプリケーションが受信するトラフィックのタイプを把握できます。このオプションについては、「ウェブリクエストのサンプルの表示」を参照してください。

保護パック (ウェブ ACL) トラフィックのログ記録の料金に関する情報

このセクションで、保護パック (ウェブ ACL) トラフィックログの使用についての料金に関する考慮事項について説明します。

保護パック (ウェブ ACL) トラフィックに関する情報のログ記録について、各ログの宛先タイプに関連するコストに応じて請求されます。これらの料金は、 AWS WAFの使用料に加算されます。コストは、選択した宛先タイプやログに記録するデータ量などの要因によって異なる場合があります。

各ログ記録の宛先タイプの料金に関する情報へのリンクを次に示します。

- CloudWatch Logs – 料金は公開ログ配信についてのものです。「Amazon CloudWatch Logs の料金」を参照してください。[Paid Tier] (有料の階層) で [Logs] (ログ) タブを選択し、[Vended Logs] (公開ログ) で [Delivery to CloudWatch Logs] (CloudWatch Logs に配信) の情報を確認します。
- Amazon S3 バケット – Amazon S3 の料金は、CloudWatch Logs が Amazon S3 バケットに公開ログ配信した料金と Amazon S3 を使用した料金を合計したものです。
  - Amazon S3 については、「Amazon S3 の料金」を参照してください。
  - CloudWatch Logs が Amazon S3 に提供する公開ログ配信については、「Amazon CloudWatch Logs の料金」を参照してください。[Paid Tier] (有料の階層) で [Logs] (ログ) タブを選択し、[Vended Logs] (公開ログ) で [Delivery to S3] (S3 に配信) の情報を確認します。
- Firehose –「Amazon Data Firehose Pricing」を参照してください。

AWS WAF 料金の詳細については、AWS WAF 「料金表」を参照してください。

AWS WAF ログ記録の送信先

このセクションでは、 AWS WAF ログ用に選択できるログ記録のオプションについて説明します。各セクションでは、ログを設定するためのガイダンスと、送信先の種類に固有の動作に関する情報を提供します。ログ記録の送信先を設定したら、保護パック (ウェブ ACL) ログ記録設定にその指定を入力して、送信先へのログ記録を開始することができます。

トピック

- Amazon CloudWatch Logs ロググループへの保護パック (ウェブ ACL) トラフィックログの送信
- Amazon Simple Storage Service バケットへの保護パック (ウェブ ACL) トラフィックログの送信
- Amazon Data Firehose 配信ストリームへの保護パック (ウェブ ACL) トラフィックログ送信

Amazon CloudWatch Logs ロググループへの保護パック (ウェブ ACL) トラフィックログの送信

このトピックは、保護パック (ウェブ ACL) トラフィックログの CloudWatch Logs ロググループへの送信に関する情報を提供します。

> **Note**
>
> AWS WAFの使用料金に加えて、ログ記録の料金が請求されます。詳細については、「保護パック (ウェブ ACL) トラフィックのログ記録の料金に関する情報」を参照してください。

Amazon CloudWatch Logs にログを送信するには、CloudWatch Logs ロググループを作成します。ログインを有効にするときは AWS WAF、ロググループ ARN を指定します。保護パック (ウェブ ACL) のログ記録を有効にすると、 はログストリームの CloudWatch Logs ロググループにログを AWS WAF 配信します。

CloudWatch Logs を使用すると、 AWS WAF コンソールで保護パック (ウェブ ACL) のログを調べることができます。保護パック (ウェブ ACL) ページで、[Logging insights] (ログ記録のインサイト) タブを選択します。このオプションは、CloudWatch コンソールで CloudWatch Logs に提供されるログ記録インサイトに追加されるものです。

AWS WAF 保護パック (ウェブ ACL) と同じリージョンで、保護パック (ウェブ ACL) の管理に使用するのと同じアカウントを使用して、保護パック (ウェブ ACL) ログのロググループを設定します。CloudWatch Logs ロググループの設定については、「ロググループとログストリームの操作」を参照してください。

CloudWatch Logs のロググループに関する配分

CloudWatch Logs には、スループットのデフォルトの最大クォータがあり、リージョン内のすべてのロググループで共有されます。これに対して、増加をリクエストできます。ログ記録の要件が既存のスループット設定に対して高すぎる場合は、アカウントの `PutLogEvents` のスロットリングメトリクスが表示されます。Service Quotas コンソールで制限を表示して引き上げをリクエストするには、「CloudWatch Logs PutLogEvents quota」を参照してください。

ロググループの命名

ロググループ名は `aws-waf-logs-` で始まる必要があり、末尾を任意のサフィックスにすることができます (例: `aws-waf-logs-testLogGroup2`)。

結果として生じる ARN 形式は次のとおりです。

```
arn:aws:logs:Region:account-id:log-group:aws-waf-logs-log-group-suffix
```

ログストリームの命名形式は次のとおりです。

```
Region_web-acl-name_log-stream-number
```

リージョン us-east-1 の保護パック (ウェブ ACL) TestWebACL のログストリームの例を次に示します。

```
us-east-1_TestWebACL_0
```

CloudWatch Logs にログを発行するために必須のアクセス許可

CloudWatch Logs ロググループの保護パック (ウェブ ACL) トラフィックログ記録を設定するには、このセクションで説明する許可設定が必要です。アクセス許可は、 AWS WAF フルアクセス管理ポリシーの 1 つ、AWSWAFConsoleFullAccessまたは を使用する場合に設定されますAWSWAFFullAccess。ログ記録と AWS WAF リソースへのよりきめ細かなアクセスを管理する場合は、アクセス許可を自分で設定できます。アクセス許可の管理の詳細については、IAM ユーザーガイドのAWS 「リソースのアクセス管理」を参照してください。 AWS WAF マネージドポリシーの詳細については、「AWS の 管理ポリシー AWS WAF」を参照してください。

これらの許可を使用すると、保護パック (ウェブ ACL) ログ記録設定の変更、CloudWatch Logs のログ配信の設定、およびロググループに関する情報の取得が可能となります。これらの許可は、 AWS WAFの管理に使用するユーザーにアタッチされる必要があります。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "wafv2:PutLoggingConfiguration",
                "wafv2:DeleteLoggingConfiguration"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow",
```

```
            "Sid": "LoggingConfigurationAPI"
        },
        {
            "Sid": "WebACLLoggingCWL",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:PutResourcePolicy",
                "logs:DescribeResourcePolicies",
                "logs:DescribeLogGroups"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

すべての AWS リソースでアクションが許可されている場合、ポリシーに "Resource"の設定で示されます"*"。つまり、各アクションがサポートするすべての AWS リソースでアクションが許可されます。 例えば、アクション wafv2:PutLoggingConfiguration は、wafv2 のログ記録設定リソースでのみサポートされます。

Amazon Simple Storage Service バケットへの保護パック (ウェブ ACL) トラフィックログの送信

このトピックは、保護パック (ウェブ ACL) トラフィックログの Amazon S3 バケットへの送信に関する情報を提供します。

> **Note**
>
> AWS WAFの使用料金に加えて、ログ記録の料金が請求されます。詳細については、「保護パック (ウェブ ACL) トラフィックのログ記録の料金に関する情報」を参照してください。

保護パック (ウェブ ACL) トラフィックログを Amazon S3 に送信するには、保護パック (ウェブ ACL) を管理するのと同じアカウントから Amazon S3 バケットを設定し、バケットに aws-waf-logs- で始まる名前を付けます。ログインを有効にするときは AWS WAF、バケット名を指定します。ロギングバケットの作成については、「Amazon Simple Storage Service ユーザーガイド」の「バケットの作成」を参照してください。

Amazon Athena インタラクティブクエリサービスを使用して、Amazon S3 ログにアクセスし、分析することができます。Athena を使用すれば、標準 SQL を使用した Amazon S3 内のデータを直接分析しやすくなります。のいくつかのアクションを使用すると AWS マネジメントコンソール、Amazon S3 に保存されているデータを Athena にポイントし、標準 SQL を使用してアドホッククエリを実行し、結果を取得できます。詳細については、「Amazon Athena ユーザーガイド」の AWS WAF 「ログのクエリ」を参照してください。 Amazon Athena その他のサンプル Amazon Athena クエリについては、GitHub ウェブサイトのaws-samples/waf-log-sample-athena-queriesを参照してください。

> **Note**
>
> AWS WAF は、キータイプの Amazon S3 キー (SSE-S3) と for AWS Key Management Service (SSE-KMS) の Amazon S3 バケットによる暗号化をサポートしています AWS KMS keys。 AWS WAF は、 によって管理される AWS Key Management Service キーの暗号化をサポートしていません AWS。

保護パック (ウェブ ACL) からのログファイルは、5 分間隔で Amazon S3 バケットに発行されます。各ログファイルには、前の 5 分間に記録されたトラフィックのログレコードが含まれています。

5 分以内に複数のログファイルを発行できます。ログファイルには、過去 5 分間に記録されたトラフィックの AWS WAF ログレコードの一部またはすべてが含まれている場合があります。

ログファイルは圧縮されます。Amazon S3 コンソールを使用してファイルを開くと、Amazon S3 はログレコードを解凍して表示します。ログファイルをダウンロードする場合、レコードを表示するには解凍する必要があります。

1 つのログファイルには、複数のレコードを含むインターリーブされたエントリが含まれます。保護パック (ウェブ ACL) のすべてのログファイルを表示するには、 保護パック (ウェブ ACL) 名、リージョン、およびアカウント ID で集約されたエントリを探します。

命名要件と構文

AWS WAF ログ記録用のバケット名は で始まりaws-waf-logs-、任意のサフィックスで終わることができます。例えば、aws-waf-logs-*LOGGING-BUCKET-SUFFIX*。

バケットの場所

バケットの場所は次の構文を使用します。

```
s3://aws-waf-logs-LOGGING-BUCKET-SUFFIX/
```

バケット ARN

バケットの Amazon リソースネーム (ARN) の形式は次のとおりです。

```
arn:aws:s3:::aws-waf-logs-LOGGING-BUCKET-SUFFIX
```

プレフィックスを使用したバケットの場所

オブジェクトキー名にプレフィックスを使用してバケットに保存するデータを整理する場合は、ロギングバケット名にプレフィックスを指定できます。

> **Note**
>
> このオプションはコンソールからは使用できません。 AWS WAF APIs、CLI、または を使用します AWS CloudFormation。

Amazon S3 でのプレフィックスの使用については、「Amazon Simple Storage Service ユーザーガイド」の「プレフィックスを使用してオブジェクトを整理する」を参照してください。

プレフィックスを使用したバケットの場所には、次の構文が使用されます。

```
s3://aws-waf-logs-LOGGING-BUCKET-SUFFIX/KEY-NAME-PREFIX/
```

バケットフォルダとファイル名

バケット内で、指定したプレフィックスに従って、 AWS WAF ログはアカウント ID、リージョン、保護パック (ウェブ ACL) 名、および日時によって決定されるフォルダ構造で書き込まれます。

```
AWSLogs/account-id/WAFLogs/Region/web-acl-name/YYYY/MM/dd/HH/mm
```

フォルダ内では、ログファイル名は同様の形式になります。

```
account-id_waflogs_Region_web-acl-name_timestamp_hash.log.gz
```

フォルダ構造およびログファイル名で使用される時間の指定は、タイムスタンプ形式の仕様 YYYYMMddTHHmmZ に準拠しています。

aws-waf-logs-*LOGGING-BUCKET-SUFFIX* という名前のバケット用の Amazon S3 バケットに存在するログファイルの例を次に示します。 AWS アカウント は です11111111111。保護パック (ウェブ ACL) は TEST-WEBACL で、リージョンは us-east-1 です。

```
s3://aws-waf-logs-LOGGING-BUCKET-SUFFIX/AWSLogs/11111111111/WAFLogs/us-
east-1/TEST-WEBACL/2021/10/28/19/50/11111111111_waflogs_us-east-1_TEST-
WEBACL_20211028T1950Z_e0ca43b5.log.gz
```

> **Note**
>
> AWS WAF ログ記録用のバケット名は で始まりaws-waf-logs-、任意のサフィックスで終わることができます。

Amazon S3 にログを発行するために必須のアクセス許可

Amazon S3 バケットの保護パック (ウェブ ACL) トラフィックログ記録を設定するには、次の許可設定が必要です。 AWS WAF フルアクセスマネージドポリシーのいずれか (AWSWAFConsoleFullAccess または AWSWAFFullAccess) を使用すると、これらの許可が設定されます。ログ記録と AWS WAF リソースへのアクセスをさらに管理する場合は、これらのアクセス許可を自分で設定できます。アクセス許可の管理については、「IAM ユーザーガイド」の「AWS リソースのアクセス管理」を参照してください。 AWS WAF 管理ポリシーの詳細については、「」を参照してくださいAWS の 管理ポリシー AWS WAF。

次の許可を使用すると、保護パック (ウェブ ACL) ログ記録設定を変更し、Amazon S3 バケットへのログ配信を設定できます。これらの許可は、 AWS WAFの管理に使用するユーザーにアタッチされる必要があります。

> **Note**
>
> 以下に示すアクセス許可を設定すると、アクセスが拒否されたことを示すエラーが AWS CloudTrail ログに表示されることがありますが、 AWS WAF ログ記録のアクセス許可は正確です。

JSON

```
{
```

```
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "wafv2:PutLoggingConfiguration",
            "wafv2:DeleteLoggingConfiguration"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow",
         "Sid":"LoggingConfigurationAPI"
      },
    {


       "Sid":"WebACLLogDelivery",


       "Action":[


          "logs:CreateLogDelivery",


          "logs:DeleteLogDelivery"


       ],


       "Resource": "*",


       "Effect":"Allow"


    },
      {
         "Sid":"WebACLLoggingS3",
         "Action":[
            "s3:PutBucketPolicy",
            "s3:GetBucketPolicy"
         ],
```

```
            "Resource": [
            "arn:aws:s3:::aws-waf-logs-amzn-s3-demo-destination-bucket-suffix"
            ],
            "Effect":"Allow"
        }
    ]
}
```

すべての AWS リソースでアクションが許可されている場合、ポリシーに "Resource"の設定で示されます"*"。つまり、各アクションがサポートするすべての AWS リソースでアクションが許可されます。 例えば、アクション wafv2:PutLoggingConfiguration は、wafv2 のログ記録設定リソースでのみサポートされます。

デフォルトでは、Amazon S3 バケットとそれに含まれているオブジェクトはプライベートです。バケット所有者のみが、そのバケットとそれに含まれているオブジェクトにアクセスできます。ただし、バケット所有者は、アクセスポリシーを記述することで他のリソースおよびユーザーに許可を付与することができます。

フローログを作成しているユーザーがバケットを所有している場合、そのバケットにログを発行する許可をフローログに付与するため、サービスは次のポリシーを自動的にバケットにアタッチします。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::aws-waf-logs-amzn-s3-demo-destination-bucket-
suffix/AWSLogs/123456789012/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "aws:SourceAccount": ["123456789012"]
        },
```

```
        "ArnLike": {
        "aws:SourceArn": ["arn:aws:logs:us-east-2:123456789012:*"]
        }
      }
    },
    {
      "Sid": "AWSLogDeliveryAclCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::aws-waf-logs-amzn-s3-demo-destination-bucket-
suffix",
      "Condition": {
        "StringEquals": {
        "aws:SourceAccount": ["123456789012"]
        },
        "ArnLike": {
        "aws:SourceArn": ["arn:aws:logs:us-east-2:123456789012:*"]
        }
      }
    }
  ]
}
```

> **Note**
>
> AWS WAF ログ記録用のバケット名は で始まりaws-waf-logs-、任意のサフィックスで終わることができます。

ログを作成しているユーザーがバケットを所有していないか、バケットに対する GetBucketPolicy および PutBucketPolicy 許可がない場合、ログの作成は失敗します。この場合、バケット所有者はバケットに手動で前述のポリシーを追加して、ログ作成者の AWS アカウント ID を指定する必要があります。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「S3 バケットポリシーを追加する方法」を参照してください。バケットが複数のアカウントからログを受け取る場合は、各アカウントの AWSLogDeliveryWrite ポリシーステートメントに Resource エレメントエントリを追加します。

たとえば、次のバケットポリシーでは AWS アカウント 、 111122223333が という名前のバケットにログを発行できるようにしますaws-waf-logs-*LOGGING-BUCKET-SUFFIX*。

JSON

```
{
    "Version":"2012-10-17",
    "Id": "AWSLogDeliveryWrite20150319",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::aws-waf-logs-amzn-s3-demo-destination-
bucket-suffix/AWSLogs/111122223333/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": ["111122223333"]
                },
                "ArnLike": {
                    "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::aws-waf-logs-amzn-s3-demo-destination-
bucket-suffix",
            "Condition": {
                "StringEquals": {
                "aws:SourceAccount": ["111122223333"]
                },
                "ArnLike": {
                "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]
```

```
                }
            }
        }
    ]
}
```

> **Note**
>
> s3:ListBucket アクセス許可が delivery.logs.amazonaws.com に付与されていないと、 AWS CloudTrail で AccessDenied エラーが表示される場合があります。CloudTrail ログにこのようなエラーが表示されないようにするには、s3:ListBucket が delivery.logs.amazonaws.com にアクセスアクセス許可を付与し、前述のバケットポリシーで設定された s3:GetBucketAcl アクセス許可で示されている Condition パラメータを含める必要があります。これを簡単にするには、新しい Statement を作成する代わりに、AWSLogDeliveryAclCheck を "Action": ["s3:GetBucketAcl", "s3:ListBucket"] であるように直接更新することができます。

KMS キー AWS Key Management Service で を使用するためのアクセス許可

ログ記録先が AWS Key Management Service (SSE-KMS) に保存されているキーによるサーバー側の暗号化を使用していて、カスタマーマネージドキー (KMS キー) を使用する場合は、KMS キーを使用するアクセス AWS WAF 許可を付与する必要があります。そのためには、選択した送信先の KMS キーにキーポリシーを追加します。これにより、 AWS WAF ロギングがログファイルを送信先に書き込むことができます。

次のキーポリシーを KMS キーに追加して、 AWS WAF が Amazon S3 バケットにログ記録できるようにします。

```
{
    "Sid": "Allow AWS WAF to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
        ]
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*"
```

```
}
```

Amazon S3 ログファイルへのアクセスに必要なアクセス許可

Amazon S3 は、アクセスコントロールリスト (ACL) を使用して、 AWS WAF ログによって作成されたログファイルへのアクセスを管理します。デフォルトでは、バケット所有者が各ログファイルで FULL_CONTROL 許可を持ちます。ログ配信の所有者 (バケット所有者とは異なる場合) は、許可を持ちません。ログ配信アカウントには、READ および WRITE 許可があります。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「アクセスコントロールリスト (ACL) の概要」を参照してください。

Amazon Data Firehose 配信ストリームへの保護パック (ウェブ ACL) トラフィックログ送信

このセクションは、保護パック (ウェブ ACL) トラフィックログの Amazon Data Firehose 配信ストリームへの送信に関する情報を提供します。

> **Note**
>
> AWS WAFの使用料金に加えて、ログ記録の料金が請求されます。詳細については、「保護パック (ウェブ ACL) トラフィックのログ記録の料金に関する情報」を参照してください。

ログを Amazon Data Firehose に送信するには、保護パック (ウェブ ACL) から Firehose で設定した Amazon Data Firehose 配信ストリームにログを送信します。ログ記録を有効にすると、 は Firehose の HTTPS エンドポイントを介してストレージ宛先にログを AWS WAF 配信します。

1 つの AWS WAF ログは、1 つの Firehose レコードに相当します。通常、1 秒あたり 10,000 件のリクエストを受信していて、完全なログを有効にする場合、Firehose には 1 秒あたり 10,000 件のレコード設定を行う必要があります。Firehose を正しく設定しない場合、すべてのログは記録 AWS WAF されません。詳細については、「Amazon Kinesis Data Firehose quotas」を参照してください。

Amazon Data Firehose 配信ストリームを作成し、保存されているログを確認する方法については、「What Is Amazon Data Firehose?」を参照してください。

配信ストリームの作成の詳細については、「Creating an Amazon Data Firehose delivery stream」を参照してください。

保護パック (ウェブ ACL) の Amazon Data Firehose 配信ストリームを設定する

保護パック (ウェブ ACL) の Amazon Data Firehose 配信ストリームを次のように設定します。

- 保護パック (ウェブ ACL) の管理に使用するアカウントと同じアカウントを使用して作成します。
- 保護パック (ウェブ ACL) と同じリージョンに作成します。Amazon CloudFront のログをキャプチャしている場合は、米国東部 (バージニア北部) リージョン `us-east-1` に Firehose を作成します。
- データ Firehose にプレフィックス `aws-waf-logs-` で始まる名前を付けます。例えば、`aws-waf-logs-us-east-2-analytics`。
- Direct PUT 用に設定し、アプリケーションが配信ストリームに直接アクセスできるようにします。「Amazon Data Firehose コンソール」で、配信ストリームの [ソース] の設定に [Direct PUT または他のソース] を選択します。API を通じて、配信ストリームのプロパティ `DeliveryStreamType` を `DirectPut` に設定します。

> **Note**
>
> `Kinesis stream` をソースとして使用しないでください。

Amazon Data Firehose にログを発行するために必須のアクセス権限

Kinesis Data Firehose の設定に必要な許可を理解するには、「Controlling Access with Amazon Kinesis Data Firehose」(Amazon Kinesis Data Firehose によるアクセスの制御) を参照してください。

Amazon Data Firehose 配信ストリームを使用して保護パック (ウェブ ACL) のログ記録を正常に有効化するには、次のアクセス権限が付与されている必要があります。

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

サービスにリンクされたロールおよび `iam:CreateServiceLinkedRole` 許可の詳細については、「のサービスにリンクされたロールの使用 AWS WAF」を参照してください。

保護パック (ウェブ ACL) のログ記録の設定

このセクションでは、保護パック (ウェブ ACL) のデータ保護を設定する手順について説明します。

> **Note**
>
> AWS WAFの使用料金に加えて、ログ記録の料金が請求されます。詳細については、「保護パック (ウェブ ACL) トラフィックのログ記録の料金に関する情報」を参照してください。

保護パック (ウェブ ACL) のログ記録を有効にするには、使用するログ記録の送信先を既に設定しておく必要があります。ターゲットの選択肢とそれぞれの要件については、「AWS WAF ログ記録の送信先」を参照してください。

保護パック (ウェブ ACL) のログ記録を設定するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで、[保護パック (ウェブ ACL)] を選択します。
3. ログ記録を有効にする保護パック (ウェブ ACL) の名前を選択します。コンソールで保護パック (ウェブ ACL) の説明が表示され、そこで編集できます。
4. [ログ記録] タブで [ログ記録を有効にする] を選択します。
5. ログ記録の送信先タイプを選択し、設定したログ記録先を選択します。名前が `aws-waf-logs-` で始まるログ記録先を選択する必要があります。
6. (オプション) ログに一部のフィールドを含めたくない場合は、それらをマスキングします。マスキングするフィールドを選び、[Add] (追加) を選択します。必要に応じて手順を繰り返し、追加のフィールドをマスキングします。マスキングされたフィールドは、ログに `xxx` と表示されます。

   > **Note**
   >
   > この設定は、リクエストサンプリングには影響しません。保護パック (ウェブ ACL) データ保護を設定するか、保護パック (ウェブ ACL) のサンプリングを無効にすることで、リクエストサンプリングからフィールドを除外できます。

7. (オプション) すべてのリクエストをログに送信しない場合は、フィルタリング条件と動作を追加します。[Filter logs] (ログをフィルタリング) で、適用する各フィルターについて [Add filter] (フィルターを追加) を選択し、次にフィルター基準を選択して、基準に一致するリクエストを保持するかドロップするかを指定します。フィルターの追加が完了したら、必要に応じて、[Default logging behavior] (デフォルトのログ記録動作) を変更します。

> **Note**
>
> 複数のフィルターを追加すると、 AWS WAF はそれらを上部から評価します。

8. [Enable logging] (ログの有効化) を選択します。

> **Note**
>
> ログ記録を正常に有効にすると、 AWS WAF はログ記録の送信先にログを書き込むために必要なアクセス許可を持つサービスにリンクされたロールを作成します。詳細については、「のサービスにリンクされたロールの使用 AWS WAF」を参照してください。

保護パック (ウェブ ACL) レコードの検索

このセクションでは、保護パック (ウェブ ACL) レコードを検索する方法について説明します。

> **Note**
>
> AWS WAFの使用料金に加えて、ログ記録の料金が請求されます。詳細については、「保護パック (ウェブ ACL) トラフィックのログ記録の料金に関する情報」を参照してください。

ログにログレコードが見つからない場合

まれに、 AWS WAF ログ配信が 100% を下回ることがあり、ログはベストエフォートベースで配信されます。この AWS WAF アーキテクチャは、他のすべての考慮事項よりもアプリケーションのセキュリティを優先します。ロギングフローでトラフィックスロットリングが発生する場合など、状況によってはレコードがドロップされることがあります。影響するレコードは数件に限られます。ログエントリがいくつか欠落していることに気付いた場合は、AWS サポート センターに連絡してください。

保護パック (ウェブ ACL) のログ記録設定で、 AWS WAF がログに送信する内容をカスタマイズできます。

- フィールドのマスキング – 対応する一致設定を使用するルールのログレコードの次のフィールドをマスキングできます: [URI パス]、[クエリ文字列]、[単一ヘッダー]、および [HTTP メソッド]。マスキングされたフィールドは、ログに REDACTED と表示されます。例えば、ログ内の [クエリ

文字列] フィールドをマスキングすると、[クエリ文字列] 一致コンポーネント設定を使用するすべてのルールで REDACTED としてリストされます。マスキングは、ルールで一致するように指定したリクエストコンポーネントにのみ適用されるため、[単一ヘッダー] コンポーネントのマスキングは、[ヘッダー] で照合するルールには適用されません。ログフィールドのリストについては、「保護パック (ウェブ ACL) トラフィックのログフィールド」を参照してください。

> **Note**
>
> この設定は、リクエストサンプリングには影響しません。保護パック (ウェブ ACL) データ保護を設定するか、保護パック (ウェブ ACL) のサンプリングを無効にすることで、リクエストサンプリングからフィールドを除外できます。

- ログのフィルタリング – フィルタリングを追加して、ログに保持されるウェブリクエストとドロップされるウェブリクエストを指定できます。ウェブリクエストの評価中 AWS WAF に適用される設定をフィルタリングします。次の設定でフィルタリングできます。
  - 完全修飾ラベル – 完全修飾ラベルには、プレフィックス、オプションの名前空間、およびラベル名があります。プレフィクスは、ラベルを追加したルールのルールグループまたは保護パック (ウェブ ACL) コンテキストを識別します。ラベルの詳細については、「でのウェブリクエストのラベル付け AWS WAF」を参照してください。
  - ルールアクション – 通常のルールアクション設定だけでなく、ルールグループのルールのレガシー EXCLUDED_AS_COUNT オーバーライドオプションをフィルタリングできます。ルールアクションの設定については、「でのルールアクションの使用 AWS WAF」を参照してください。ルールグループのルールの現在のルールアクションオーバーライドとレガシールールアクションオーバーライドについては、「でのルールグループアクションの上書き AWS WAF」を参照してください。
    - 通常のルールアクションフィルターは、ルールで設定されたアクションだけでなく、ルールグループのルールアクションをオーバーライドするための現在のオプションを使用して設定されたアクションにも適用されます。
    - EXCLUDED_AS_COUNT ログフィルターは、Count アクションログフィルターと重複しています。EXCLUDED_AS_COUNT は、ルールグループのルールアクションを Count にオーバーライドするための現在のオプションとレガシーオプションの両方をフィルタリングします。

ログをフィルタリングして、収益化イベントを含めたり除外したりできます。

- 収益化アクティビティのみをログに記録するには: フィルターオン `action = MONETIZE`
- 収益化を除外するには: `monetization`フィールドが存在しないフィルター

保護パック (ウェブ ACL) トラフィックのログフィールド

次のリストは、可能なログフィールドについて説明しています。

action

がリクエスト AWS WAF に適用した終了アクション。これは許可、ブロック、CAPTCHA、チャレンジのいずれかを示します。ウェブリクエストに有効なトークンが含まれていないとき、CAPTCHA および Challenge アクションは終了します。

args

クエリ文字列。

captchaResponse

CAPTCHA アクションがリクエストに適用されたときに入力される、リクエストの CAPTCHA アクションステータス。このフィールドは、終了の有無にかかわらず、すべての CAPTCHA アクションに入力されます。リクエストに CAPTCHA アクションが複数回適用されている場合、このフィールドはアクションが最後に適用された時点から入力されます。

リクエストにトークンが含まれていない、あるいはトークンが無効または有効期限切れているとき、CAPTCHA アクションはウェブリクエストの検査を終了します。CAPTCHA アクションが終了している場合、このフィールドにはレスポンスコードと失敗の理由が含まれます。アクションが非終了型の場合、このフィールドには解決タイムスタンプが含まれます。終了アクションと非終了アクションを区別するには、このフィールドで空でない `failureReason` 属性をフィルタリングできます。

cfDistributionTenantId

ウェブリクエストに関連付けられた CloudFront ディストリビューションテナントの識別子。このフィールドはオプションであり、CloudFront ディストリビューションテナントに関連付けられた保護パック (ウェブ ACL) にのみ適用されます。

challengeResponse

Challenge アクションがリクエストに適用されたときに入力される、リクエストのチャレンジアクションステータス。このフィールドは、終了の有無にかかわらず、すべての Challenge アクションに入力されます。リクエストに Challenge アクションが複数回適用されている場合、このフィールドはアクションが最後に適用された時点から入力されます。

リクエストにトークンが含まれていない、あるいはトークンが無効または有効期限切れているとき、Challenge アクションはウェブリクエストの検査を終了します。Challenge アクションが終

了している場合、このフィールドにはレスポンスコードと失敗の理由が含まれます。アクションが非終了型の場合、このフィールドには解決タイムスタンプが含まれます。終了アクションと非終了アクションを区別するには、このフィールドで空でない `failureReason` 属性をフィルタリングできます。

clientAsn

ウェブリクエストのオリジンの IP アドレスに関連付けられた AS 番号 (ASN)。

> **Note**
>
> clientAsn は、ASN 一致ステートメントが使用されている場合にのみ AWS WAF ログに記録されます。このフィールドは、それ以外の場合はログに記録されません。

clientIp

リクエストを送信するクライアントの IP アドレス。

country

リクエストの送信国。 AWS WAF が原産国を特定できない場合、このフィールドは に設定されます-。

country

リクエストの送信国。 AWS WAF が原産国を特定できない場合、このフィールドは に設定されます-。

excludedRules

ルールグループのルールにのみ使用されます。除外されているルールグループ内のルールのリスト。これらのルールのアクションは Count に設定されています。

オーバーライドルールアクションのオプションを使用してルールがカウントするようにオーバーライドする場合、一致するものはここには一覧表示されません。アクションペア `action` および `overriddenAction` として一覧表示されています。

exclusionType

除外されたルールにアクション Count があることを示すタイプ。

ruleId

除外されたルールグループ内のルールの ID。

formatVersion

ログの形式バージョン。

forwardedAsn

ウェブリクエストを転送したエンティティの の IP アドレスに関連付けられた AS 番号 (ASN)。

headers

ヘッダーの一覧。

httpMethod

リクエストの HTTP メソッド。

httpRequest

リクエストに関するメタデータです。

httpSourceId

関連付けられたリソースの ID。

- Amazon CloudFront ディストリビューションの場合、ID は ARN 構文で *distribution-id* です。

  arn:*partition*cloudfront::*account-id*:distribution/*distribution-id*
- Application Load Balancer の場合、ID は ARN 構文で *load-balancer-id* です。

  arn:*partition*:elasticloadbalancing:*region*:*account-id*:loadbalancer/app/*load-balancer-name/load-balancer-id*
- Amazon API Gateway REST API の場合、ID は ARN 構文で *api-id* です。

  arn:*partition*:apigateway:*region*::/restapis/*api-id*/stages/*stage-name*
- AWS AppSync GraphQL API の場合、ID は ARN 構文*GraphQLApiId*の です。

  arn:*partition*:appsync:*region*:*account-id*:apis/*GraphQLApiId*
- Amazon Cognito ユーザープールの場合、ID は ARN 構文で *user-pool-id* です。

  arn:*partition*:cognito-idp:*region*:*account-id*:userpool/*user-pool-id*
- AWS App Runner サービスの場合、ID は ARN 構文*apprunner-service-id*の です。

  arn:*partition*:apprunner:*region*:*account-id*:service/*apprunner-service-name/apprunner-service-id*

httpSourceName

リクエストの送信元。指定できる値: Amazon CloudFront `CF` の場合、`APIGW`Amazon API Gateway `ALB` の場合、Application Load Balancer `APPSYNC`の場合、Amazon Cognito AWS AppSync`COGNITOIDP` の場合、App Runner `APPRUNNER` の場合、Verified Access `VERIFIED_ACCESS` の場合。

httpVersion

HTTP のバージョン。

ja3Fingerprint

リクエストの JA3 フィンガープリント。

> **Note**
>
> JA3 フィンガープリント検査は、Amazon CloudFront ディストリビューションと Application Load Balancer でのみ利用可能です。

JA3 フィンガープリントは、受信リクエストの TLS Client Hello から生成される 32 文字のハッシュです。このフィンガープリントは、クライアントの TLS 設定の一意の識別子として機能します。 AWS WAF は、計算に十分な TLS Client Hello 情報を持つリクエストごとに、このフィンガープリントを計算してログに記録します。

この値は、保護パック (ウェブ ACL) ルールで JA3 フィンガープリントの一致を設定するときに指定します。JA3 フィンガープリントとの一致を作成する方法については、「でコンポーネントをリクエストする AWS WAF」の「JA3 フィンガープリント」に記載されているルールステートメントを参照してください。

ja4Fingerprint

リクエストの JA4 フィンガープリント。

> **Note**
>
> JA4 フィンガープリント検査は、Amazon CloudFront ディストリビューションと Application Load Balancer でのみ使用できます。

JA4 フィンガープリントは、受信リクエストの TLS Client Hello から派生した 36 文字のハッシュです。このフィンガープリントは、クライアントの TLS 設定の一意の識別子として機能します。AWS WAF は、計算に十分な TLS Client Hello 情報を持つリクエストごとに、このフィンガープリントを計算してログに記録します。

この値は、保護パック (ウェブ ACL) ルールで JA4 フィンガープリントの一致を設定するときに指定します。JA4 フィンガープリントとの一致の作成については、ルールステートメントでコンポーネントをリクエストする AWS WAFの JA4 フィンガープリントの「」を参照してください。

ラベル

ウェブリクエストのラベル。これらのラベルは、最初の 100 AWS WAF 個のラベルの評価に使用されたルールによって適用されました。

nonTerminatingMatchingRules

リクエストに一致した非終了型ルールのリスト。各リスト項目には、次の情報が含まれています。

action

がリクエスト AWS WAF に適用したアクション。カウント、CAPTCHA、チャレンジのいずれかを示します。ウェブリクエストに有効なトークンが含まれていると、CAPTCHA および Challenge は終了処理しません。

ruleId

リクエストに一致し、非終了ルールの ID。

ruleMatchDetails

リクエストに一致したルールに関する詳細情報。このフィールドは、SQL インジェクションおよびクロスサイトスクリプティング (XSS) 一致ルールステートメントに対してのみ設定されます。一致ルールでは、複数の検査基準の一致が必要になる場合があるため、これらの一致の詳細は、一致基準の配列として提供されます。

各ルールに提供される追加情報は、ルール設定、ルール一致タイプ、一致の詳細などの要因によって異なります。たとえば、CAPTCHA または Challenge アクションを持つルールの場合、`captchaResponse` または`challengeResponse` が一覧表示されます。一致するルールがルールグループにあり、その設定済みルールアクションをオーバーライドした場合、設定済みアクションは `overriddenAction` で提供されます。

oversizeFields

保護パック (ウェブ ACL) によって検査され、 AWS WAF 検査制限を超えているウェブリクエスト内のフィールドのリスト。フィールドがオーバーサイズであっても、保護パック (ウェブ ACL) が検査しない場合、ここには表示されません。

このリストには、REQUEST_BODY、REQUEST_JSON_BODY、REQUEST_HEADERS、および REQUEST_COOKIES の値が何個か含まれることも、含まれないこともあります。オーバーサイズフィールドの詳細については、「でのウェブリクエストコンポーネントのオーバーサイズ化 AWS WAF」を参照してください。

rateBasedRuleList

リクエストに対して評価されたウェブ ACL 内のすべてのレートベースのルールのリスト。これには、完全に評価できなかったルールが含まれます。レートベースルールの詳細については、「でのレートベースのルールステートメントの使用 AWS WAF」を参照してください。

rateBasedRuleId

レートベースのルールの ID。これがリクエストを終了した場合、rateBasedRuleId の ID は、terminatingRuleId の ID と同じです。このフィールドは、ルールが評価できなかったNO_EVALUATION_PERFORMED場合に に設定されます。これは、集約に必要なヘッダーや Cookie などのカスタムCUSTOMKEYS集約キーがリクエストにない場合に発生する可能性があります。

rateBasedRuleName

レートベースのルールの名前。

limitKey

ルールが使用している集約のタイプ。指定できる値は、ウェブリクエストの発信元用の IP、リクエストのヘッダーで転送された IP 用の FORWARDED_IP、カスタム集約キー設定用の CUSTOMKEYS、および集約なしですべてのリクエストをまとめてカウントする用の CONSTANT です。

limitValue

単一の IP アドレスタイプでレート制限を行う場合にのみ使用される。リクエストに有効ではない IP アドレスが含まれている場合、limitvalue は INVALID です。

maxRateAllowed

特定の集約インスタンスに対して指定された時間枠で許可されるリクエストの最大数。集約インスタンスは、limitKey およびレートベースのルール設定で提供される追加のキー仕様によって定義されます。

evaluationWindowSec

がリクエストに AWS WAF 含めた時間を秒単位でカウントします。

customValues

リクエスト内のレートベースのルールによって識別される一意の値。文字列値の場合、ログは文字列値の最初の 32 文字を出力します。キータイプに応じて、これらの値は HTTP メソッドやクエリ文字列といったキーだけの場合もあれば、ヘッダーやヘッダー名のようなキーと名前の場合もあります。

requestHeadersInserted

カスタムリクエストの処理用に挿入されるヘッダーのリスト。

requestId

基盤となるホストサービスによって生成されるリクエストの ID。Application Load Balancer では、これはトレース ID です。その他すべての場合、これはリクエスト ID です。

responseCodeSent

カスタムレスポンスで送信されるレスポンスコード。

ruleGroupId

ルールグループの ID ルールがリクエストをブロックした場合、ruleGroupID の ID は、terminatingRuleId の ID と同じです。

ruleGroupList

このリクエストに対して動作したルールグループのリスト (一致情報を含む)。

terminatingRule

リクエストを終了したルール。これが存在する場合、次の情報が含まれます。

action

がリクエスト AWS WAF に適用した終了アクション。これは許可、ブロック、CAPTCHA、チャレンジのいずれかを示します。ウェブリクエストに有効なトークンが含まれていないとき、CAPTCHA および Challenge アクションは終了します。

ruleId

リクエストに一致したルールの ID。

ruleMatchDetails

リクエストに一致したルールに関する詳細情報。このフィールドは、SQL インジェクションおよびクロスサイトスクリプティング (XSS) 一致ルールステートメントに対してのみ設定されます。一致ルールでは、複数の検査基準の一致が必要になる場合があるため、これらの一致の詳細は、一致基準の配列として提供されます。

各ルールに提供される追加情報は、ルール設定、ルール一致タイプ、一致の詳細などの要因によって異なります。たとえば、CAPTCHA または Challenge アクションを持つルールの場合、`captchaResponse` または`challengeResponse` が一覧表示されます。一致するルールがルールグループにあり、その設定済みルールアクションをオーバーライドした場合、設定済みアクションは `overriddenAction` で提供されます。

terminatingRuleId

リクエストを終了したルールの ID。リクエストを終了したものがない場合、この値は `Default_Action` となります。

terminatingRuleMatchDetails

リクエストに一致した終了ルールに関する詳細情報。終了ルールには、ウェブリクエストに対する検査プロセスを終了するアクションがあります。終了ルールに可能なアクションには、Allow、Block、CAPTCHA、Challenge が含まれます。ウェブリクエストの検査中に、リクエストに一致し、終了アクションを持つ最初のルールで、 は検査 AWS WAF を停止し、アクションを適用します。ウェブリクエストには、一致する終了ルールのログで報告された脅威に加えて、他の脅威が含まれている可能性があります。

これは、SQL インジェクションおよびクロスサイトスクリプティング (XSS) 一致ルールステートメントに対してのみ設定されます。一致ルールでは、複数の検査基準の一致が必要になる場合があるため、これらの一致の詳細は、一致基準の配列として提供されます。

terminatingRuleType

リクエストを終了したルールのタイプ。可能な値: RATE_BASED、REGULAR、GROUP、MANAGED_RULE_GROUP。

timestamp

タイムスタンプ (ミリ秒単位)。

uri

リクエストの URI。

fragment

「#」記号の後に続く URL の一部で、#section2 など、リソースに関する追加情報を提供します。

webaclId

保護パック (ウェブ ACL) の GUID。

monetizeVerifyResponse

Monetize アクションが支払い検証をトリガーするときに表示されます。検証結果と支払いの詳細が含まれます。

monetizeVerifyResponse.verificationStatus

支払い検証の結果。指定できる値:
`VERIFIED`、`INSUFFICIENT_FUNDS`、`INVALID_PAYLOAD`、`INVALID_PAYMENT_REQUIREMENTS`、

monetizeVerifyResponse.failureReason

検証が失敗した場合、失敗の理由。

monetizeVerifyResponse.chainName

支払いに使用されるブロックチェーンチェーン。指定できる値:
`BASE`、`SOLANA`、`BASE_SEPOLIA`、`SOLANA_DEVNET`。

monetizeVerifyResponse.network

ブロックチェーンネットワーク識別子 (`eip155:84532`Base Sepolia など) 。

monetizeVerifyResponse.amount

小数文字列としての支払い額。

monetizeVerifyResponse.currency

支払いに使用される暗号通貨。現在 `USDC`。

monetizeVerifyResponse.asset

ブロックチェーンのトークン契約アドレス (たとえば、指定されたチェーンの USDC 契約アドレス) 。

monetizeVerifyResponse.payerAddress

支払い AI エージェントのウォレットアドレス。

monetizeVerifyResponse.idempotencyKey

支払いトランザクションの一意のキー。重複処理の防止に使用されます。

monetizeVerifyResponse.currencyMode

実通貨とテスト通貨のどちらが使用されたか。指定できる値: REAL、TEST。

保護パック (ウェブ ACL) トラフィックのログ例

このセクションでは、保護パック (ウェブ ACL) トラフィックをログに記録する例を示します。

Exampleレートベースのルール 1: キーが 1 つで、Header:dogname に設定されたルール設定

```
{
  "Name": "RateBasedRule",
  "Priority": 1,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "AggregateKeyType": "CUSTOM_KEYS",
      "CustomKeys": [
        {
          "Header": {
            "Name": "dogname",
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        }
      ]
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
```

```
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "RateBasedRule"
      }
    }
```

Exampleレートベースのルール 1: レートベースのルールによってブロックされたリクエストのログエントリ

```
{
   "timestamp":1683355579981,
   "formatVersion":1,
   "webaclId": ...,
   "terminatingRuleId":"RateBasedRule",
   "terminatingRuleType":"RATE_BASED",
   "action":"BLOCK",
   "terminatingRuleMatchDetails":[

   ],
   "httpSourceName":"APIGW",
   "httpSourceId":"EXAMPLE11:rjvegx5guh:CanaryTest",
   "ruleGroupList":[

   ],
   "rateBasedRuleList":[
      {
         "rateBasedRuleId": ...,
         "rateBasedRuleName":"RateBasedRule",
         "limitKey":"CUSTOMKEYS",
         "maxRateAllowed":100,
         "evaluationWindowSec":"120",
         "customValues":[
            {
               "key":"HEADER",
               "name":"dogname",
               "value":"ella"
            }
         ]
      }
   ],
   "nonTerminatingMatchingRules":[

   ],
```

```
    "requestHeadersInserted":null,
    "responseCodeSent":null,
    "httpRequest":{
       "clientIp":"52.46.82.45",
       "country":"FR",
       "headers":[
          {
             "name":"X-Forwarded-For",
             "value":"52.46.82.45"
          },
          {
             "name":"X-Forwarded-Proto",
             "value":"https"
          },
          {
             "name":"X-Forwarded-Port",
             "value":"443"
          },
          {
             "name":"Host",
             "value":"rjvegx5guh.execute-api.eu-west-3.amazonaws.com"
          },
          {
             "name":"X-Amzn-Trace-Id",
             "value":"Root=1-645566cf-7cb058b04d9bb3ee01dc4036"
          },
          {
             "name":"dogname",
             "value":"ella"
          },
          {
             "name":"User-Agent",
             "value":"RateBasedRuleTestKoipOneKeyModulePV2"
          },
          {
             "name":"Accept-Encoding",
             "value":"gzip,deflate"
          }
       ],
       "uri":"/CanaryTest",
       "args":"",
       "httpVersion":"HTTP/1.1",
       "httpMethod":"GET",
       "requestId":"Ed0AiHF_CGYF-DA="
```

```
    }
}
```

Exampleレートベースのルール 2: キーが 2 つで、Header:dogname および Header:catname に設定されたルール設定

```
    {
      "Name": "RateBasedRule",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 100,
          "AggregateKeyType": "CUSTOM_KEYS",
          "CustomKeys": [
            {
              "Header": {
                "Name": "dogname",
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            },
            {
              "Header": {
                "Name": "catname",
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
```

```
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "RateBasedRule"
      }
    }
```

Exampleレートベースのルール 2: レートベースのルールによってブロックされたリクエストのログエントリ

```
{
   "timestamp":1633322211194,
   "formatVersion":1,
   "webaclId":...,
   "terminatingRuleId":"RateBasedRule",
   "terminatingRuleType":"RATE_BASED",
   "action":"BLOCK",
   "terminatingRuleMatchDetails":[

   ],
   "httpSourceName":"APIGW",
   "httpSourceId":"EXAMPLE11:rjvegx5guh:CanaryTest",
   "ruleGroupList":[

   ],
   "rateBasedRuleList":[
      {
         "rateBasedRuleId":...,
         "rateBasedRuleName":"RateBasedRule",
         "limitKey":"CUSTOMKEYS",
         "maxRateAllowed":100,
         "evaluationWindowSec":"120",
         "customValues":[
            {
               "key":"HEADER",
               "name":"dogname",
               "value":"ella"
            },
            {
               "key":"HEADER",
               "name":"catname",
               "value":"goofie"
            }
         ]
```

```
      }
   ],
   "nonTerminatingMatchingRules":[

   ],
   "requestHeadersInserted":null,
   "responseCodeSent":null,
   "httpRequest":{
      "clientIp":"52.46.82.35",
      "country":"FR",
      "headers":[
         {
            "name":"X-Forwarded-For",
            "value":"52.46.82.35"
         },
         {
            "name":"X-Forwarded-Proto",
            "value":"https"
         },
         {
            "name":"X-Forwarded-Port",
            "value":"443"
         },
         {
            "name":"Host",
            "value":"23llbyn8v3.execute-api.eu-west-3.amazonaws.com"
         },
         {
            "name":"X-Amzn-Trace-Id",
            "value":"Root=1-64556629-17ac754c2ed9f0620e0f2a0c"
         },
         {
            "name":"catname",
            "value":"goofie"
         },
         {
            "name":"dogname",
            "value":"ella"
         },
         {
            "name":"User-Agent",
            "value":"Apache-HttpClient/UNAVAILABLE (Java/11.0.19)"
         },
         {
```

```
            "name":"Accept-Encoding",
            "value":"gzip,deflate"
         }
      ],
      "uri":"/CanaryTest",
      "args":"",
      "httpVersion":"HTTP/1.1",
      "httpMethod":"GET",
      "requestId":"EdzmlH5OCGYF1vQ="
   }
}
```

Example SQLi 検出 (終了) でトリガーされたルールのログ出力

```
{
    "timestamp": 1576280412771,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-southeast-2:111122223333:regional/webacl/
STMTest/1EXAMPLE-2ARN-3ARN-4ARN-123456EXAMPLE",
    "terminatingRuleId": "STMTest_SQLi_XSS",
    "terminatingRuleType": "REGULAR",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [
        {
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "HIGH",
            "location": "HEADER",
            "matchedData": [
                "10",
                "AND",
                "1"
            ]
        }
    ],
    "httpSourceName": "-",
    "httpSourceId": "-",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [],
    "httpRequest": {
        "clientIp": "1.1.1.1",
        "country": "AU",
        "headers": [
```

```
            {
                "name": "Host",
                "value": "localhost:1989"
            },
            {
                "name": "User-Agent",
                "value": "curl/7.61.1"
            },
            {
                "name": "Accept",
                "value": "*/*"
            },
            {
                "name": "x-stm-test",
                "value": "10 AND 1=1"
            }
        ],
        "uri": "/myUri",
        "args": "",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "GET",
        "requestId": "rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example SQLi 検出 (非終了) でトリガーされたルールのログ出力

```
{
    "timestamp":1592357192516
    ,"formatVersion":1
    ,"webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-
world/5933d6d9-9dde-js82-v8aw-9ck28nv9"
    ,"terminatingRuleId":"Default_Action"
    ,"terminatingRuleType":"REGULAR"
    ,"action":"ALLOW"
    ,"terminatingRuleMatchDetails":[]
    ,"httpSourceName":"-"
    ,"httpSourceId":"-"
```

```
    ,"ruleGroupList":[]
    ,"rateBasedRuleList":[]
    ,"nonTerminatingMatchingRules":
    [{
        "ruleId":"TestRule"
        ,"action":"COUNT"
        ,"ruleMatchDetails":
        [{
            "conditionType":"SQL_INJECTION"
            ,"sensitivityLevel": "HIGH"
            ,"location":"HEADER"
            ,"matchedData":[
                "10"
                ,"and"
                ,"1"]
            }]
    }]
    ,"httpRequest":{
        "clientIp":"3.3.3.3"
        ,"country":"US"
        ,"headers":[
            {"name":"Host","value":"localhost:1989"}
            ,{"name":"User-Agent","value":"curl/7.61.1"}
            ,{"name":"Accept","value":"*/*"}
            ,{"name":"myHeader","myValue":"10 AND 1=1"}
            ]
            ,"uri":"/myUri","args":""
            ,"httpVersion":"HTTP/1.1"
            ,"httpMethod":"GET"
            ,"requestId":"rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Exampleルールグループ内でトリガーされた複数のルールのログ出力 (RuleA-XSS は終了、Rule-B は非終了)

```
{
    "timestamp":1592361810888,
```

```
    "formatVersion":1,
    "webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-
world/5933d6d9-9dde-js82-v8aw-9ck28nv9"
    ,"terminatingRuleId":"RG-Reference"
    ,"terminatingRuleType":"GROUP"
    ,"action":"BLOCK",
    "terminatingRuleMatchDetails":
    [{
        "conditionType":"XSS"
        ,"location":"HEADER"
        ,"matchedData":["<","frameset"]
    }]
    ,"httpSourceName":"-"
    ,"httpSourceId":"-"
    ,"ruleGroupList":
    [{
        "ruleGroupId":"arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/hello-
world/c05lb698-1f11-4m41-aef4-99a506d53f4b"
        ,"terminatingRule":{
            "ruleId":"RuleA-XSS"
            ,"action":"BLOCK"
            ,"ruleMatchDetails":null
            }
        ,"nonTerminatingMatchingRules":
        [{
            "ruleId":"RuleB-SQLi"
            ,"action":"COUNT"
            ,"ruleMatchDetails":
            [{
                "conditionType":"SQL_INJECTION"
                ,"sensitivityLevel": "LOW"
                ,"location":"HEADER"
                ,"matchedData":[
                    "10"
                    ,"and"
                    ,"1"]
            }]
        }]
        ,"excludedRules":null
    }]
    ,"rateBasedRuleList":[]
    ,"nonTerminatingMatchingRules":[]
    ,"httpRequest":{
        "clientIp":"3.3.3.3"
```

```
        ,"country":"US"
        ,"headers":
        [
            {"name":"Host","value":"localhost:1989"}
            ,{"name":"User-Agent","value":"curl/7.61.1"}
            ,{"name":"Accept","value":"*/*"}
            ,{"name":"myHeader1","value":"<frameset onload=alert(1)>"}
            ,{"name":"myHeader2","value":"10 AND 1=1"}
            ]
        ,"uri":"/myUri"
        ,"args":""
        ,"httpVersion":"HTTP/1.1"
        ,"httpMethod":"GET"
        ,"requestId":"rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Exampleコンテンツタイプ JSON を使用したリクエストボディの検査のためにトリガーされたルールのログ出力

AWS WAF は現在、JSON 本文検査の場所を として報告していますUNKNOWN。

```
{
    "timestamp": 1576280412771,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-southeast-2:123456789012:regional/webacl/test/111",
    "terminatingRuleId": "STMTest_SQLi_XSS",
    "terminatingRuleType": "REGULAR",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [
        {
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "LOW",
            "location": "UNKNOWN",
            "matchedData": [
                "10",
                "AND",
                "1"
```

```
            ]
        }
    ],
    "httpSourceName": "ALB",
    "httpSourceId": "alb",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [],
    "requestHeadersInserted":null,
    "responseCodeSent":null,
    "httpRequest": {
        "clientIp": "1.1.1.1",
        "country": "AU",
        "headers": [],
        "uri": "",
        "args": "",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "POST",
        "requestId": "null"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example有効期限が切れていない有効な CAPTCHA トークンを使用したウェブリクエストに対する CAPTCHA ルールのログ出力

次のログリストは、CAPTCHA アクションを持つルールと一致したウェブリクエストについてのものです。ウェブリクエストには有効で有効期限が切れていない CAPTCHA トークンがあり、Count アクションの動作と同様に AWS WAF、 による CAPTCHA 一致としてのみ記録されます。この CAPTCHA の一致については、nonTerminatingMatchingRules に記載されています。

```
{
  "timestamp": 1632420429309,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/captcha-web-
acl/585e38b5-afce-4d2a-b417-14fb08b66c67",
  "terminatingRuleId": "Default_Action",
  "terminatingRuleType": "REGULAR",
  "action": "ALLOW",
```

```
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "123456789012:b34myvfw0b:pen-test",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [
    {
      "ruleId": "captcha-rule",
      "action": "CAPTCHA",
      "ruleMatchDetails": [],
      "captchaResponse": {
        "responseCode": 0,
        "solveTimestamp": 1632420429
      }
    }
  ],
  "requestHeadersInserted": [
    {
      "name": "x-amzn-waf-test-header-name",
      "value": "test-header-value"
    }
  ],
  "responseCodeSent": null,
  "httpRequest": {
    "clientIp": "72.21.198.65",
    "country": "US",
    "headers": [
      {
        "name": "X-Forwarded-For",
        "value": "72.21.198.65"
      },
      {
        "name": "X-Forwarded-Proto",
        "value": "https"
      },
      {
        "name": "X-Forwarded-Port",
        "value": "443"
      },
      {
        "name": "Host",
        "value": "b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com"
      },
      {
```

```
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-614cc24d-5ad89a09181910c43917a888"
      },
      {
        "name": "cache-control",
        "value": "max-age=0"
      },
      {
        "name": "sec-ch-ua",
        "value": "\"Chromium\";v=\"94\", \"Google Chrome\";v=\"94\", \";Not A Brand
\";v=\"99\""
      },
      {
        "name": "sec-ch-ua-mobile",
        "value": "?0"
      },
      {
        "name": "sec-ch-ua-platform",
        "value": "\"Windows\""
      },
      {
        "name": "upgrade-insecure-requests",
        "value": "1"
      },
      {
        "name": "user-agent",
        "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/94.0.4606.54 Safari/537.36"
      },
      {
        "name": "accept",
        "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
      },
      {
        "name": "sec-fetch-site",
        "value": "same-origin"
      },
      {
        "name": "sec-fetch-mode",
        "value": "navigate"
      },
      {
        "name": "sec-fetch-user",
```

```
        "value": "?1"
      },
      {
        "name": "sec-fetch-dest",
        "value": "document"
      },
      {
        "name": "referer",
        "value": "https://b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com/pen-
test/pets"
      },
      {
        "name": "accept-encoding",
        "value": "gzip, deflate, br"
      },
      {
        "name": "accept-language",
        "value": "en-US,en;q=0.9"
      },
      {
        "name": "cookie",
        "value": "aws-waf-token=51c71352-41f5-4f6d-b676-c24907bdf819:EQoAZ/J
+AAQAAAAA:t9wvxbw042wva7E2Y6lgud/
bS6YG0CJKVAJqaRqDZ140ythKW0Zj9wKB2O8lSkYDRqf1yONcVBFo5u0eYi0tvT4rtQCXsu
+KanAardW8go4QSLw4yoED59lgV7oAhGyCalAzE7ra29j+RvvZPsQyoQuDCrtoY/TvQyMTXIXzGPDC/rKBbg=="
      }
    ],
    "uri": "/pen-test/pets",
    "args": "",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "GINMHHUgoAMFxug="
  }
}
```

Example CAPTCHA トークンがないウェブリクエストに対する CAPTCHA ルールのログ出力

次のログリストは、CAPTCHA アクションを持つルールと一致したウェブリクエストについてのものです。ウェブリクエストに CAPTCHA トークンがなく、 によってブロックされました AWS WAF。

```
{
  "timestamp": 1632420416512,
```

```
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/captcha-web-
acl/585e38b5-afce-4d2a-b417-14fb08b66c67",
  "terminatingRuleId": "captcha-rule",
  "terminatingRuleType": "REGULAR",
  "action": "CAPTCHA",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "123456789012:b34myvfw0b:pen-test",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [],
  "requestHeadersInserted": null,
  "responseCodeSent": 405,
  "httpRequest": {
    "clientIp": "72.21.198.65",
    "country": "US",
    "headers": [
      {
        "name": "X-Forwarded-For",
        "value": "72.21.198.65"
      },
      {
        "name": "X-Forwarded-Proto",
        "value": "https"
      },
      {
        "name": "X-Forwarded-Port",
        "value": "443"
      },
      {
        "name": "Host",
        "value": "b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com"
      },
      {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-614cc240-18b57ff33c10e5c016b508c5"
      },
      {
        "name": "sec-ch-ua",
        "value": "\"Chromium\";v=\"94\", \"Google Chrome\";v=\"94\", \";Not A Brand
\";v=\"99\""
      },
      {
```

```
        "name": "sec-ch-ua-mobile",
        "value": "?0"
      },
      {
        "name": "sec-ch-ua-platform",
        "value": "\"Windows\""
      },
      {
        "name": "upgrade-insecure-requests",
        "value": "1"
      },
      {
        "name": "user-agent",
        "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/94.0.4606.54 Safari/537.36"
      },
      {
        "name": "accept",
        "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
      },
      {
        "name": "sec-fetch-site",
        "value": "cross-site"
      },
      {
        "name": "sec-fetch-mode",
        "value": "navigate"
      },
      {
        "name": "sec-fetch-user",
        "value": "?1"
      },
      {
        "name": "sec-fetch-dest",
        "value": "document"
      },
      {
        "name": "accept-encoding",
        "value": "gzip, deflate, br"
      },
      {
        "name": "accept-language",
        "value": "en-US,en;q=0.9"
```

```
      }
    ],
    "uri": "/pen-test/pets",
    "args": "",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "GINKHEssoAMFsrg="
  },
  "captchaResponse": {
    "responseCode": 405,
    "solveTimestamp": 0,
    "failureReason": "TOKEN_MISSING"
  }
}
```

データ保護

AWS WAF データ保護設定を使用すると、ヘッダー、パラメータ、本文コンテンツなどの特定のデータフィールドに、機密情報 (パスワード、API キー、認証トークン、その他の機密データ) のカスタマイズされたきめ細かな保護を実装できます。

データ保護は、次のいずれかで設定できます。

- すべての出力先に適用される保護パック (ウェブ ACL) レベル。
- ログ記録のみ。これは、 が設定されたログ記録先 AWS WAF に送信するデータにのみ影響します。

データ保護は、置換またはハッシュとして指定できます。

置換とは、コンテンツを REDACTED という単語に置き換えることを指します。

ハッシュとは、文字列から Base64 への SHA-256 バイナリにコンテンツを置き換えることを指します。

1. まず、アルゴリズムは account_number とコンテンツから文字列を構築します。
2. 次に、SHA-256 を適用してバイナリハッシュを生成します。
3. 最後に、Base64 を使用してこれらのバイトをエンコードします。

> **Tip**
>
> 適切なデータ保護方法を選択する前に、SHA-256 ハッシュの特性を確認して、要件を満たしているかどうかを判断する必要があります。暗号化またはトークン化と同等の結果を実現する場合は、SHA-256 ハッシュを使用することはお勧めしません。

トピック

- データ保護の有効化
- データ保護の例外
- データ保護制限
- データ保護の例
- 保護パック (ウェブ ACL) のデータ保護の設定

データ保護の有効化

このセクションでは、 コンソールから選択できるデータ保護とログ設定オプションについて説明します。特定のフィールドでデータ保護を有効にすることで、ログに表示されるデータを保護できます。データ保護を適用して、フルログ、サンプルリクエスト、Security Lake など、さまざまなタイプの出力で機密情報を変換できます。

AWS WAF コンソールでデータ保護を有効にするには

コンソールで 保護パック (ウェブ ACL) ページに移動して、保護設定の有効化 を行います。ログのデータ保護を有効にするには、それをすべてのログに適用するか、特定のログ送信先に適用するかを選択します。詳細については、「保護パック (ウェブ ACL) トラフィックのログフィールド」を参照してください。

> **Note**
>
> すべてのログ記録にデータ保護を適用するために、ログ記録を有効にする必要はありません。データ保護は、ログ記録が有効になっているかどうかにかかわらず、すべての出力先に適用されます。

[保護設定の有効化] ページの下部で、[データ保護] フィールドパネルの [フィールドの追加] ボタンを選択します。ドロップダウンメニューからフィールドタイプを選択します。各フィールドのデータがデータ保護でどのように保護されるかについては、以下の表を参照してください。

フィールドタイプ	詳細
`Single header`	指定されたオプション (ハッシュまたは部分配置) に従って、指定されたヘッダーキー値を永続的に変換します。変換された値は完全なログにも反映されます。
`Body`	本文の値を永続的に変換します。ログ内の `RuleMatchDetails` にのみ適用できます。
`Query string`	指定されたオプション (ハッシュまたは部分配置) に従って、クエリ文字列を永続的に変換します。変換された値は完全なログにも反映されます。
`Single query argument`	指定されたオプション (ハッシュまたは部分配置) に従って、指定されたクエリ引数値を永続的に変換します。変換された値は完全なログにも反映されます。
`Single cookie`	指定されたオプション (ハッシュまたは部分配置) に従って、Cookie 値を永続的に変換します。変換された値は完全なログにも反映されます。

データ保護の例外

有効にすると、`RuleMatchDetails` や `rateBasedRuleList` など、有効になっているフィールドにデータ保護が適用されます。ただし、トラブルシューティングと可視性の目的で、保護されたデータとコンテンツを `RuleMatchDetails` および `rateBasedRuleList` に含める必要がある場合があります。これらのシナリオでは、そのフィールドのデータ保護に例外を指定できます。

- **`ExcludeRuleMatchDetails`**: 特定のフィールドにこの例外を指定すると、`RuleMatchDetails` は フィールドの値を表示し、データ保護の対象外になります。

- **`ExcludeRateBasedDetails`**: 特定のフィールドにこの例外を指定すると、`rateBasedRuleList` は フィールドの値を表示し、データ保護の対象外になります。

  例: `ExcludeRateBasedDetails` ルールは「dogname」の SINGLE_HEADER と HEADER_NAME で有効になっています。

  ルールに例外が適用されない場合、「dogname」の値は `REDACTED` として表示されます。

```
"rateBasedRuleList":[ {"rateBasedRuleId": ...,
                       "rateBasedRuleName":"RateBasedRule", "limitKey":"CUSTOMKEYS",
                       "maxRateAllowed":100, "evaluationWindowSec":"120",
 "customValues":[
                       {"key":"HEADER", "name":"dogname", "value":"REDACTED" } ] } ]
```

  ルールで例外が有効になっている場合、「dogname」値がログに表示されます。

```
 "rateBasedRuleList":[ {"rateBasedRuleId": ...,
                       "rateBasedRuleName":"RateBasedRule", "limitKey":"CUSTOMKEYS",
                       "maxRateAllowed":100, "evaluationWindowSec":"120",
 "customValues":[
                       {"key":"HEADER", "name":"dogname", "value":"ELLA" } ] } ]
```

> **Warning**
>
> データ保護機能は、トラブルシューティング AWS WAF 機能に影響を与える可能性があります。これらの設定により、予期しない検出および緩和動作が発生する可能性があります。特定のパラメータのデータ保護を、絶対に必要なパラメータのみに制限します。

データ保護制限

以下は、データ保護を使用する際に考慮すべき制限です。

QueryString と SingleQueryArg

QueryString の保護

- `QueryString` のデータ保護は、すべてのクエリ引数に適用され、指定された設定に従ってキーと値の両方を置換/ハッシングします。

RuleMatch の詳細と RateBased ルールリストの QueryString

- データ保護が単一クエリ引数に適用される場合、クエリ文字列全体が完全なログの RuleMatchDetails および RateBasedRule セクションで置換/ハッシングされます。
- 複数の単一クエリ引数で異なる保護方法 (置換とハッシング) が指定されている場合、より厳密なメソッドである置換は、完全なログの RuleMatchDetails および RateBasedRule セクションのクエリ文字列全体に適用されます。

cookie

> **Note**
>
> データ保護は、単一ヘッダー Cookie が保護されている場合にのみ、 Cookie の値に適用されます。

RuleMatchDetails および **RateBasedRule** リストの単一 Cookie

- データ保護が 1 つの Cookie に適用される場合、Cookie ヘッダー全体が完全なログの RuleMatchDetails および RateBasedRule セクションで置換/ハッシングされます。
- 異なる保護方法 (置換とハッシング) が指定されている場合、より厳密なメソッドである置換は、完全なログの RuleMatchDetails および RateBasedRule セクションの Cookie 全体に適用されます。

データ保護の例

このセクションでは、保護パック (ウェブ ACL) トラフィックのデータ保護ログ記録のログ例を示します。

DataProtection ハッシング

Webacl 設定

```
"data_protection_config": {
            "data_protections": [
                {
                    "field": {
                        "field_type": "SINGLE_QUERY_ARGUMENT",
                        "field_keys": [
```

```
                            "hoppy"
                        ]
                    },
                    "action": "HASH",
                    "exclude_rule_match_details": false,
                    "exclude_rate_based_details": false
                }
            ]
        }
```

DataProtection ハッシングの例: SingleQuery 引数「hoppy」が保護されたログエントリ。

```
{
    "timestamp": 1738705092889,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
DataProtectionhashACL/4eede063-e611-44f5-b357-ffc9d7b7fed5",
    "terminatingRuleId": "Default_Action",
    "terminatingRuleType": "REGULAR",
    "action": "ALLOW",
    "terminatingRuleMatchDetails": [],
    "httpSourceName": "APIGW",
    "httpSourceId": "746533260405:xt7v59bhn7:ABC",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [{
        "ruleId": "ProtectedSQLIHeadersVisibleInSTM",
        "action": "COUNT",
        "ruleMatchDetails": [{
                "conditionType": "SQL_INJECTION",
                "sensitivityLevel": "HIGH",
                "location": "SINGLE_QUERY_ARG",
                "matchedData": [ "z6hpYAFaMYdtiTeHhxnN5ydgRE5E1WgyVIdgqH0D3iM=" ],
                "matchedFieldName": "hoppy"
        }]
    }],
"requestHeadersInserted": null,
"responseCodeSent": null,
"httpRequest": {
    "clientIp": "54.239.98.137",
    "country": "US",
    "headers": [{
        "name": "X-Forwarded-For",
```

```
        "value": "54.239.98.137"
    }, {
        "name": "X-Forwarded-Proto",
        "value": "https"
    }, {
        "name": "X-Forwarded-Port",
        "value": "443"
    }, {
        "name": "Host",
        "value": "xt7xxx9bhn7.gamma.execute-api.us-east-1.amazonaws.com"
    }, {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-67a288c4-27acb3cd5795dd8456b7e3c3"
    }, {
        "name": "Accept-Encoding",
        "value": "gzip"
    }, {
        "name": "User-Agent",
        "value": "okhttp/3.12.1"
    }],
    "uri": "/CanaryTest",
    "args": "hoppy=z6hpYAFaMYdtiTeHhxnN5ydgRE5E1WgyVIdgqH0D3iM=&yellow=hello&x-hoppy-
extra=generic-%3Cwords%3E-in-angle-brackets",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "FepO0F8fIAMEqoQ="
},
"labels": [{
    "name": "awswaf:forwardedip:geo:country:US"
}, {
    "name": "awswaf:forwardedip:geo:region:US-VA"
}]
}
```

DataProtection の置換

Webacl 設定

```
"data_protection_config": {
            "data_protections": [
                {
                    "field": {
                        "field_type": "SINGLE_QUERY_ARGUMENT",
                        "field_keys": [
```

```
                        "hoppy"
                    ]
                },
                "action": "SUBSTITUTION",
                "exclude_rule_match_details": false,
                "exclude_rate_based_details": false
            }
        ]
    }
```

DataProtection 置換の例: 単一クエリ引数「ホッピー」が保護されたログエントリ

```
{
    "timestamp": 1738705092889,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
DataProtectionhashACL/4eede063-e611-44f5-b357-ffc9d7b7fed5",
    "terminatingRuleId": "Default_Action",
    "terminatingRuleType": "REGULAR",
    "action": "ALLOW",
    "terminatingRuleMatchDetails": [],
    "httpSourceName": "APIGW",
    "httpSourceId": "746533260405:xt7v59bhn7:ABC",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": []
"requestHeadersInserted": null,
"responseCodeSent": null,
"httpRequest": {
    "clientIp": "54.239.98.137",
    "country": "US",
    "headers": [{
        "name": "X-Forwarded-For",
        "value": "54.239.98.137"
    }, {
        "name": "X-Forwarded-Proto",
        "value": "https"
    }, {
        "name": "X-Forwarded-Port",
        "value": "443"
    }, {
        "name": "Host",
        "value": "xt7xxx9bhn7.gamma.execute-api.us-east-1.amazonaws.com"
```

```
    }, {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-67a288c4-27acb3cd5795dd8456b7e3c3"
    }, {
        "name": "Accept-Encoding",
        "value": "gzip"
    }, {
        "name": "User-Agent",
        "value": "okhttp/3.12.1"
    }],
    "uri": "/CanaryTest",
    "args": "hoppy=REDACTED&yellow=hello&x-hoppy-extra=generic-%3Cwords%3E-in-angle-
brackets",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "FepO0F8fIAMEqoQ="
},
"labels": [{
    "name": "awswaf:forwardedip:geo:country:US"
}, {
    "name": "awswaf:forwardedip:geo:region:US-VA"
}]
}
```

RuleMatchDetails でのデータの保持

Webacl 設定

```
"data_protection_config": {
            "data_protections": [
                {
                    "field": {
                        "field_type": "SINGLE_HEADER",
                        "field_keys": [
                            "hoppy"
                        ]
                    },
                    "action": "HASH",
                    "exclude_rule_match_details": true,
                    "exclude_rate_based_details": false
                }
             ]
           }
```

RuleMatchDetails でデータを保持する例: 単一のHeader「ホッピー」が保護されているが、値は でのみ保持されるログエントリRuleMatchDetails。

```
{
    "timestamp": 1738705092889,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
DataProtectionhashACL/4eede063-e611-44f5-b357-ffc9d7b7fed5",
    "terminatingRuleId": "Default_Action",
    "terminatingRuleType": "REGULAR",
    "action": "ALLOW",
    "terminatingRuleMatchDetails": [],
    "httpSourceName": "APIGW",
    "httpSourceId": "746533260405:xt7v59bhn7:ABC",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [{
        "ruleId": "ProtectedSQLIHeadersVisibleInSTM",
        "action": "COUNT",
        "ruleMatchDetails": [{
                "conditionType": "SQL_INJECTION",
                "sensitivityLevel": "HIGH",
                "location": "HEADER",
                "matchedData": [ "10", "AND", "1" ],
                "matchedFieldName": "hoppy"
        }]
    }],
"requestHeadersInserted": null,
"responseCodeSent": null,
"httpRequest": {
    "clientIp": "54.239.98.137",
    "country": "US",
    "headers": [{
        "name": "X-Forwarded-For",
        "value": "54.239.98.137"
    }, {
        "name": "X-Forwarded-Proto",
        "value": "https"
    }, {
        "name": "X-Forwarded-Port",
        "value": "443"
    }, {
        "name": "Host",
```

```
        "value": "xt7xxx9bhn7.gamma.execute-api.us-east-1.amazonaws.com"
    }, {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-67a288c4-27acb3cd5795dd8456b7e3c3"
    }, {
        "name": "hoppy",
        "value": "zuomr2mxQxofg6EI6f7hMNGaJhhPxt0rFVAXog6FLxE="
    }, {
        "name": "Accept-Encoding",
        "value": "gzip"
    }, {
        "name": "User-Agent",
        "value": "okhttp/3.12.1"
    }, {
        "name": "hoppy",
        "value": "z6hpYAFaMYdtiTeHhxnN5ydgRE5E1WgyVIdgqH0D3iM="
    }],
    "uri": "/CanaryTest",
    "args": "happy=true",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "FepO0F8fIAMEqoQ="
},
"labels": [{
    "name": "awswaf:forwardedip:geo:country:US"
}, {
    "name": "awswaf:forwardedip:geo:region:US-VA"
}]
}
```

rateBasedRule でのデータの保持

```
 "data_protection_config": {
            "data_protections": [
                {
                    "field": {
                        "field_type": "SINGLE_HEADER",
                        "field_keys": [
                            "hoppy"
                        ]
                    },
                    "action": "HASH",
                    "exclude_rule_match_details": false,
```

```
                    "exclude_rate_based_details": true
                }
            ]
        }
```

rateBasedRuleList でのデータの保持例: 単一のHeader「ホピー」が保護されているが、値が でのみ保持されるログエントリ rateBasedRuleList

```
{
    "timestamp": 1683355579981,
    "formatVersion": 1,
    "webaclId": ...,
    "terminatingRuleId": "RateBasedRule",
    "terminatingRuleType": "RATE_BASED",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [],
    "httpSourceName": "APIGW",
    "httpSourceId": "EXAMPLE11:rjvegx5guh:CanaryTest",
    "ruleGroupList": [],
    "rateBasedRuleList": [{
        "rateBasedRuleId": ...,
        "rateBasedRuleName": "RateBasedRule",
        "limitKey": "CUSTOMKEYS",
        "maxRateAllowed": 100,
        "evaluationWindowSec": "120",
        "customValues": [{
            "key": "HEADER",
            "name": "hoppy",
            "value": "ella"
        }]
    }],
    "nonTerminatingMatchingRules": [],
    "requestHeadersInserted": null,
    "responseCodeSent": null,
    "httpRequest": {
        "clientIp": "52.46.82.45",
        "country": "FR",
        "headers": [{
            "name": "X-Forwarded-For",
            "value": "52.46.82.45"
        }, {
            "name": "X-Forwarded-Proto",
            "value": "https"
```

```
        }, {
            "name": "X-Forwarded-Port",
            "value": "443"
        }, {
            "name": "Host",
            "value": "rjvegx5guh.execute-api.eu-west-3.amazonaws.com"
        }, {
            "name": "X-Amzn-Trace-Id",
            "value": "Root=1-645566cf-7cb058b04d9bb3ee01dc4036"
        }, {
            "name": "hoppy",
            "value": "zuomr2mxQxofg6EI6f7hMNGaJhhPxt0rFVAXog6FLxE="
        }, {
            "name": "User-Agent",
            "value": "RateBasedRuleTestKoipOneKeyModulePV2"
        }, {
            "name": "Accept-Encoding",
            "value": "gzip,deflate"
        }],
        "uri": "/CanaryTest",
        "args": "",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "GET",
        "requestId": "Ed0AiHF_CGYF-DA="
    }
}
```

本文のデータ保護

AWS WAF の本文のサブセットのみを口グに記録しますRuleMatchDetails。

Webacl 設定

```
 "data_protection_config": {
            "data_protections": [
                {
                    "field": {
                        "field_type": "BODY"
                    },
                    "action": "SUBSTITUTE",
                    "exclude_rule_match_details": false,
                    "exclude_rate_based_details": false
                }
             ]
```

```
            }
```

本文の DataProtection の例: 本文が `ruleMatchDetails` にサブセットされたログエントリ。

```
{
    "timestamp": 1738705092889,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
DataProtectionhashACL/4eede063-e611-44f5-b357-ffc9d7b7fed5",
    "terminatingRuleId": "Default_Action",
    "terminatingRuleType": "REGULAR",
    "action": "ALLOW",
    "terminatingRuleMatchDetails": [],
    "httpSourceName": "APIGW",
    "httpSourceId": "746533260405:xt7v59bhn7:ABC",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [{
        "ruleId": "ProtectedSQLIBody",
        "action": "COUNT",
        "ruleMatchDetails": [{
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "HIGH",
            "location": "BODY",
            "matchedData": ["REDACTED"]
        }]
    }],
    "requestHeadersInserted": null,
    "responseCodeSent": null,
    "httpRequest": {
        "clientIp": "54.239.98.137",
        "country": "US",
        "headers": [{
            "name": "X-Forwarded-For",
            "value": "54.239.98.137"
        }, {
            "name": "X-Forwarded-Proto",
            "value": "https"
        }, {
            "name": "X-Forwarded-Port",
            "value": "443"
        }, {
            "name": "Host",
```

```
            "value": "xt7xxx9bhn7.gamma.execute-api.us-east-1.amazonaws.com"
        }, {
            "name": "X-Amzn-Trace-Id",
            "value": "Root=1-67a288c4-27acb3cd5795dd8456b7e3c3"
        }, {
            "name": "Accept-Encoding",
            "value": "gzip"
        }, {
            "name": "User-Agent",
            "value": "okhttp/3.12.1"
        }, {
            "name": "cookie",
            "value": "hoppy=dog;"
        }],
        "uri": "/CanaryTest",
        "args": "baloo=abc&hoppy-query=xyz&x-hoppy-extra=generic-%3Cwords%3E-in-angle-
brackets",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "GET",
        "requestId": "FepO0F8fIAMEqoQ="
    },
    "labels": [{
        "name": "awswaf:forwardedip:geo:country:US"
    }, {
        "name": "awswaf:forwardedip:geo:region:US-VA"
    }]
}
```

SINGLE_COOKIE のデータ保護

Webacl 設定

```
 "data_protection_config": {
            "data_protections": [
                {
                    "field": {
                        "field_type": "SINGLE_COOKIE",
                        "field_keys": [
                            "MILO"
                        ]
                    },
                    "action": "HASH",
                    "exclude_rule_match_details": false,
                    "exclude_rate_based_details": false
```

```
                }
            ]
        }
```

SINGLE_COOKIE の DataProtection の例: 保護された「MILO」という名前の SINGLE_COOKIE ログエントリ。

完全なログには、MILO という名前の Cookie が ruleMatchDetails で保護され、Cookie ヘッダーが表示されます。Cookie 値のみが保護され、キー名は除外されます。

> **Note**
>
> すべての保護されたフィールド (単一ヘッダー、Cookie、クエリ引数) では、大文字と小文字は区別されません。したがって、この例では、「MILO」は「milo」と一致します。

```
{
    "timestamp": 1738705092889,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
DataProtectionhashACL/4eede063-e611-44f5-b357-ffc9d7b7fed5",
    "terminatingRuleId": "Default_Action",
    "terminatingRuleType": "REGULAR",
    "action": "ALLOW",
    "terminatingRuleMatchDetails": [],
    "httpSourceName": "APIGW",
    "httpSourceId": "746533260405:xt7v59bhn7:ABC",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [{
        "ruleId": "ProtectedSQLIHeadersVisibleInSTM",
        "action": "COUNT",
        "ruleMatchDetails": [{
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "HIGH",
            "location": "COOKIE",
            "matchedData": ["zuomr2mxQxofg6EI6f7hMNGaJhhPxt0rFVAXog6FLxE="],
            "matchedFieldName": "milo"
        }]
    }],
    "requestHeadersInserted": null,
    "responseCodeSent": null,
```

```
    "httpRequest": {
        "clientIp": "54.239.98.137",
        "country": "US",
        "headers": [{
            "name": "X-Forwarded-For",
            "value": "54.239.98.137"
        }, {
            "name": "X-Forwarded-Proto",
            "value": "https"
        }, {
            "name": "X-Forwarded-Port",
            "value": "443"
        }, {
            "name": "Host",
            "value": "xt7xxx9bhn7.gamma.execute-api.us-east-1.amazonaws.com"
        }, {
            "name": "X-Amzn-Trace-Id",
            "value": "Root=1-67a288c4-27acb3cd5795dd8456b7e3c3"
        }, {
            "name": "Accept-Encoding",
            "value": "gzip"
        }, {
            "name": "User-Agent",
            "value": "okhttp/3.12.1"
        }, {
            "name": "cookie",
            "value": "hoppy=dog;milo=zuomr2mxQxofg6EI6f7hMNGaJhhPxt0rFVAXog6FLxE=;aws-
waf-token=51c71352-41f5-4f6d-b676-c24907bdf819:EQoAZ/J+AAQAAAAA:t9wvxbw042wva7E2Y6lgud/
bS6YG0CJKVAJqaRqDZ140ythKW0Zj9wKB2O8lSkYDRqf1yONcVBFo5u0eYi0tvT4rtQCXsu
+KanAardW8go4QSLw4yoED59lgV7oAhGyCalAzE7ra29j+RvvZPsQyoQuDCrtoY/TvQyMTXIXzGPDC/rKBbg=="
        }],
        "uri": "/CanaryTest",
        "args": "baloo=abc&hoppy-query=xyz&x-hoppy-extra=generic-%3Cwords%3E-in-angle-
brackets",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "GET",
        "requestId": "FepO0F8fIAMEqoQ="
    },
    "labels": [{
        "name": "awswaf:forwardedip:geo:country:US"
    }, {
        "name": "awswaf:forwardedip:geo:region:US-VA"
    }]
```

```
}
```

すべての Cookie のデータ保護

SINGLE_HEADER を使用して Cookie のデータ保護を設定できます。Cookie 値のみが保護され、キー名は除外されます。

```
"DataProtectionConfig": {
    "DataProtections": [
        {
            "Field": {
                "FieldType": "SINGLE_HEADER",
                "FieldKeys": ["cookie"]
            },
            "Action": "SUBSTITUTION",
            "ExcludeRuleMatchDetails": false,
            "ExcludeRateBasedDetails": false
        }
    ]
}
```

header 「COOKIE」の DataProtection の例: Cookie ヘッダーが保護されたログエントリ。

> **Note**
>
> Cookie 名 AWS-WAF-TOKEN はデータ保護の対象外です。

```
{
    "timestamp": 1738705092889,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
DataProtectionhashACL/4eede063-e611-44f5-b357-ffc9d7b7fed5",
    "terminatingRuleId": "Default_Action",
    "terminatingRuleType": "REGULAR",
    "action": "ALLOW",
    "terminatingRuleMatchDetails": [],
    "httpSourceName": "APIGW",
    "httpSourceId": "746533260405:xt7v59bhn7:ABC",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [],
```

```
    "requestHeadersInserted": null,
    "responseCodeSent": null,
    "httpRequest": {
        "clientIp": "54.239.98.137",
        "country": "US",
        "headers": [{
            "name": "X-Forwarded-For",
            "value": "54.239.98.137"
        }, {
            "name": "X-Forwarded-Proto",
            "value": "https"
        }, {
            "name": "X-Forwarded-Port",
            "value": "443"
        }, {
            "name": "Host",
            "value": "xt7xxx9bhn7.gamma.execute-api.us-east-1.amazonaws.com"
        }, {
            "name": "X-Amzn-Trace-Id",
            "value": "Root=1-67a288c4-27acb3cd5795dd8456b7e3c3"
        }, {
            "name": "Accept-Encoding",
            "value": "gzip"
        }, {
            "name": "User-Agent",
            "value": "okhttp/3.12.1"
        }, {
            "name": "cookie",
            "value": "hoppy=REDACTED;milo=REDACTED;aws-waf-
token=51c71352-41f5-4f6d-b676-c24907bdf819:EQoAZ/J+AAQAAAAA:t9wvxbw042wva7E2Y6lgud/
bS6YG0CJKVAJqaRqDZ140ythKW0Zj9wKB2O8lSkYDRqf1yONcVBFo5u0eYi0tvT4rtQCXsu
+KanAardW8go4QSLw4yoED59lgV7oAhGyCalAzE7ra29j+RvvZPsQyoQuDCrtoY/TvQyMTXIXzGPDC/rKBbg=="
        }],
        "uri": "/CanaryTest",
        "args": "baloo=xyz=&hoppy-query=abc&x-hoppy-extra=abc",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "GET",
        "requestId": "FepO0F8fIAMEqoQ="
    },
    "labels": [{
        "name": "awswaf:forwardedip:geo:country:US"
    }, {
        "name": "awswaf:forwardedip:geo:region:US-VA"
    }]
```

```
}
```

単一クエリ引数のデータ保護

SINGLE_QUERY_ARGUMENT を使用して、クエリ文字列のデータ保護を設定できます。これは、すべてのクエリ引数のキーと値に影響します。次の例では、元のクエリ文字列は baloo=10 AND 1=1&hoppy=10 AND 1=1&x-hoppy-extra=generic-%3Cwords でした。

Webacl 設定

```
"DataProtectionConfig": {
   "DataProtections": [
        {
            "Field": {
                "FieldType": "SINGLE_QUERY_ARGUMENT",
                "FieldKeys": ["hoppy"]
            },
            "Action": "SUBSTITUTION",
            "ExcludeRuleMatchDetails": false,
            "ExcludeRateBasedDetails": false
        }
    ]
}
```

SINGLE_QUERY_ARGUEMENT の DataProtection の例: 置換で保護された「hoppy」クエリ文字列を含むログエントリ。

```
{
    "timestamp": 1738705092889,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
DataProtectionSubstituteQueryString/4eede063-e611-44f5-b357-ffc9d7b7fed5",
    "terminatingRuleId": "Default_Action",
    "terminatingRuleType": "REGULAR",
    "action": "ALLOW",
    "terminatingRuleMatchDetails": [],
    "httpSourceName": "APIGW",
    "httpSourceId": "746533260405:xt7v59bhn7:ABC",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [
      {
        "ruleId": "ProtectedHoppyQueryArg",
```

```
        "action": "COUNT",
        "ruleMatchDetails": [
            {
                "conditionType": "SQL_INJECTION",
                "sensitivityLevel": "HIGH",
                "location": "SINGLE_QUERY_ARG",
                "matchedData": ["REDACTED"],
                "matchedFieldName": "hoppy"
            }]
      },
      {
        "ruleId":
 "FullQueryStringInspectionWhichDetectsTheFirstFieldWithSQLi_Baloo_IsAlsoMaskedMasked",
        "action": "COUNT",
        "ruleMatchDetails": [
            {
                "conditionType": "SQL_INJECTION",
                "sensitivityLevel": "HIGH",
                "location": "QUERY_ARGS",
                "matchedData": ["REDACTED"],
            }]
      },
      {
        "ruleId": "ProtectedBalooQueryArg",
        "action": "COUNT",
        "ruleMatchDetails": [
            {
                "conditionType": "SQL_INJECTION",
                "sensitivityLevel": "HIGH",
                "location": "SINGLE_QUERY_ARG",
                "matchedData": [ "10", "AND", "1" ],
                "matchedFieldName": "baloo"
            }]
      }
    ],
    "requestHeadersInserted": null,
    "responseCodeSent": null,
    "httpRequest": {
        "clientIp": "54.239.98.137",
        "country": "US",
        "headers": [{
            "name": "X-Forwarded-For",
            "value": "54.239.98.137"
        }, {
```

```
            "name": "X-Forwarded-Proto",
            "value": "https"
        }, {
            "name": "X-Forwarded-Port",
            "value": "443"
        }, {
            "name": "Host",
            "value": "xt7xxx9bhn7.gamma.execute-api.us-east-1.amazonaws.com"
        }, {
            "name": "X-Amzn-Trace-Id",
            "value": "Root=1-67a288c4-27acb3cd5795dd8456b7e3c3"
        }, {
            "name": "Accept-Encoding",
            "value": "gzip"
        }, {
            "name": "User-Agent",
            "value": "okhttp/3.12.1"
        }],
        "uri": "/CanaryTest",
        "args": "baloo=10 AND 1=1&hoppy=REDACTED&x-hoppy-extra=generic-%3Cwords",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "GET",
        "requestId": "FepO0F8fIAMEqoQ="
    },
    "labels": [{
        "name": "awswaf:forwardedip:geo:country:US"
    }, {
        "name": "awswaf:forwardedip:geo:region:US-VA"
    }]
}
```


クエリ文字列のデータ保護

QUERY_STRING を使用して、クエリ文字列のデータ保護を設定できます。これは、すべてのクエリ引数のキーと値に影響します。次の例では、元のクエリ文字列は baloo=10 AND 1=1&hoppy-query=10 AND 1=1&x-hoppy-extra=generic-%3Cwords でした。

Webacl 設定


```
"DataProtectionConfig": {
 "DataProtections": [
 {
 "Field": {
```

```
 "FieldType": "QUERY_STRING"
 },
 "Action": "SUBSTITUTION",
 "ExcludeRuleMatchDetails": false,
 "ExcludeRateBasedDetails": false
 }
 ]
}
```

QUERY_STRING の DataProtection の例: 置換で保護されたクエリ文字列を含むログエントリ。

```
{
    "timestamp": 1738705092889,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
DataProtectionSubstituteQueryString/4eede063-e611-44f5-b357-ffc9d7b7fed5",
    "terminatingRuleId": "Default_Action",
    "terminatingRuleType": "REGULAR",
    "action": "ALLOW",
    "terminatingRuleMatchDetails": [],
    "httpSourceName": "APIGW",
    "httpSourceId": "746533260405:xt7v59bhn7:ABC",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [
      {
        "ruleId": "ProtectedHoppyQueryArg",
        "action": "COUNT",
        "ruleMatchDetails": [
            {
                "conditionType": "SQL_INJECTION",
                "sensitivityLevel": "HIGH",
                "location": "QUERY_STRING",
                "matchedData": ["REDACTED"]
            }]
      },
      {
        "ruleId": "ProtectedBalooQueryArg",
        "action": "COUNT",
        "ruleMatchDetails": [
            {
                "conditionType": "SQL_INJECTION",
                "sensitivityLevel": "HIGH",
```

```
                "location": "SINGLE_QUERY_ARG",
                "matchedData": [ "REDACTED" ],
                "matchedFieldName": "REDACTED"
            }]
      }
    ],
    "requestHeadersInserted": null,
    "responseCodeSent": null,
    "httpRequest": {
        "clientIp": "54.239.98.137",
        "country": "US",
        "headers": [{
            "name": "X-Forwarded-For",
            "value": "54.239.98.137"
        }, {
            "name": "X-Forwarded-Proto",
            "value": "https"
        }, {
            "name": "X-Forwarded-Port",
            "value": "443"
        }, {
            "name": "Host",
            "value": "xt7xxx9bhn7.gamma.execute-api.us-east-1.amazonaws.com"
        }, {
            "name": "X-Amzn-Trace-Id",
            "value": "Root=1-67a288c4-27acb3cd5795dd8456b7e3c3"
        }, {
            "name": "Accept-Encoding",
            "value": "gzip"
        }, {
            "name": "User-Agent",
            "value": "okhttp/3.12.1"
        }],
        "uri": "/CanaryTest",
        "args": "REDACTED",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "GET",
        "requestId": "FepO0F8fIAMEqoQ="
    },
    "labels": [{
        "name": "awswaf:forwardedip:geo:country:US"
    }, {
        "name": "awswaf:forwardedip:geo:region:US-VA"
    }]
```

```
}
```

複数のクエリ引数のデータ保護

SINGLE_QUERY_ARGUMENT を使用して、個々のクエリ引数のデータ保護を設定できます。ローカル情報を報告する際は、ローカル保護を使用します。ただし、クエリ文字列と Cookie ヘッダーで一致した文字列には、適用される可能性のある多くの保護設定があります。簡素化するために、RuleMatchDetails の最も厳密な保護が適用されます。これは、一致した特定のデータ範囲と重複していない場合でも適用されます。

次の例では、元のクエリ文字列は baloo=is_a_good_boy&hoppy=likes_to_sleep&x-hoppy-extra=10 AND 1=1 でした。

```
"DataProtectionConfig": {
    "DataProtections": [
        {
            "Field": {
                "FieldType": "SINGLE_QUERY_ARGUMENT",
                "FieldKeys": ["hoppy"]
            },
            "Action": "SUBSTITUTION",
            "ExcludeRuleMatchDetails": false,
            "ExcludeRateBasedDetails": false
        },
        {
            "Field": {
                "FieldType": "SINGLE_QUERY_ARGUMENT",
                "FieldKeys": ["baloo"]
            },
            "Action": "HASH",
            "ExcludeRuleMatchDetails": false,
            "ExcludeRateBasedDetails": false
        }
    ]
}
```

複数のクエリ引数の DataProtection の例。

```
{
    "timestamp": 1738705092889,
    "formatVersion": 1,
```

```
    "webaclId": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
DataProtectionSubstituteQueryString/4eede063-e611-44f5-b357-ffc9d7b7fed5",
    "terminatingRuleId": "Default_Action",
    "terminatingRuleType": "REGULAR",
    "action": "ALLOW",
    "terminatingRuleMatchDetails": [],
    "httpSourceName": "APIGW",
    "httpSourceId": "746533260405:xt7v59bhn7:ABC",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [
      {
        "ruleId": "ProtectedHoppyQueryArg",
        "action": "COUNT",
        "ruleMatchDetails": [
            {
                "conditionType": "SQL_INJECTION",
                "sensitivityLevel": "HIGH",
                "location": "SINGLE_QUERY_ARG",
                "matchedData": ["REDACTED"],
                "matchedFieldName": "hoppy"
            }]
      },
      {
        "ruleId": "ProtectedBalooQueryArg",
        "action": "COUNT",
        "ruleMatchDetails": [
            {
                "conditionType": "SQL_INJECTION",
                "sensitivityLevel": "HIGH",
                "location": "SINGLE_QUERY_ARG",
                "matchedData": ["zuomr2mxQxofg6EI6f7hMNGaJhhPxt0rFVAXog6FLxE="],
                "matchedFieldName": "baloo"
            }]
      },
      {
        "ruleId": "FullQueryStringDetects_x-hoppy-extra_IsSubstituted",
        "action": "COUNT",
        "ruleMatchDetails": [
            {
                "conditionType": "SQL_INJECTION",
                "sensitivityLevel": "HIGH",
                "location": "QUERY_ARGS",
                "matchedData": ["REDACTED"],  // Harshest of Protection Config
```

```
            }]
      }
    ],
    "requestHeadersInserted": null,
    "responseCodeSent": null,
    "httpRequest": {
        "clientIp": "54.239.98.137",
        "country": "US",
        "headers": [{
            "name": "X-Forwarded-For",
            "value": "54.239.98.137"
        }, {
            "name": "X-Forwarded-Proto",
            "value": "https"
        }, {
            "name": "X-Forwarded-Port",
            "value": "443"
        }, {
            "name": "Host",
            "value": "xt7xxx9bhn7.gamma.execute-api.us-east-1.amazonaws.com"
        }, {
            "name": "X-Amzn-Trace-Id",
            "value": "Root=1-67a288c4-27acb3cd5795dd8456b7e3c3"
        }, {
            "name": "Accept-Encoding",
            "value": "gzip"
        }, {
            "name": "User-Agent",
            "value": "okhttp/3.12.1"
        }],
        "uri": "/CanaryTest",
        "args": "baloo=zuomr2mxQxofg6EI6f7hMNGaJhhPxt0rFVAXog6FLxE=&hoppy=REDACTED&x-
hoppy-extra=10 AND 1=1",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "GET",
        "requestId": "FepO0F8fIAMEqoQ="
    },
    "labels": [{
        "name": "awswaf:forwardedip:geo:country:US"
    }, {
        "name": "awswaf:forwardedip:geo:region:US-VA"
    }]
}
```

> **Note**
>
> 同じ ウェブ ACL で QueryString マスキング と シングルクエリ配列マスキング の両方を指定することはできません。

保護パック (ウェブ ACL) のデータ保護の設定

このセクションでは、保護パック (ウェブ ACL) のデータ保護を設定する手順について説明します。

保護パック (ウェブ ACL) のデータ保護を設定するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで、[保護パック (ウェブ ACL)] を選択します。
3. データ保護を有効にする保護パック (ウェブ ACL) の名前を選択します。コンソールで保護パック (ウェブ ACL) の説明が表示され、そこで編集できます。
4. [ログ記録とメトリクス] タブの [データ保護設定] ペインで、[有効化] または [編集] を選択します。
5. 範囲 [グローバル] を選択し、フィールドデータ保護選択を行います。フィールドデータ保護設定ごとに、保護動作から除外する例外を指定することもできます。
6. 選択が完了したら、[保存] を選択します。インターフェイスは、選択内容が要約されている ログ記録とメトリクス タブに戻ります。

AWS WAF 保護のテストとチューニング

このセクションでは、 AWS WAF 保護パック (ウェブ ACLs)、ルール、ルールグループ、IP セット、正規表現パターンセットをテストおよびチューニングするためのガイダンスを提供します。

ウェブサイトまたはウェブアプリケーショントラフィックに適用する前に、 AWS WAF 保護パック (ウェブ ACL) の変更をテストして調整することをお勧めします。

> **本番稼働トラフィックのリスク**
>
> 本番稼働トラフィックに保護パック (ウェブ ACL) 実装をデプロイする前に、トラフィックへの潜在的な影響に慣れるまで、ステージング環境またはテスト環境でテストおよびチューニ

ングします。その後、ルールを有効にする前に、本番稼働用トラフィックでカウントモードでルールをテストしてチューニングします。

また、このセクションでは、他のユーザーによって管理されているルールグループの使用をテストするための一般的なガイダンスも提供します。これには、 AWS マネージドルールルールグループ、AWS Marketplace マネージドルールグループ、および別のアカウントによって共有されるルールグループが含まれます。これらのルールグループについては、ルールグループプロバイダーから取得したガイダンスにも従ってください。

- Bot Control AWS マネージドルールのルールグループについては、「」も参照してくださいAWS WAF Bot Control のテストとデプロイ。
- アカウント乗っ取り防止 AWS マネージドルールのルールグループについては、「」も参照してくださいATP のテストとデプロイ。
- アカウント作成の不正防止 AWS マネージドルールのルールグループについては、「」も参照してくださいACFP のテストとデプロイ。

更新中の一時的な不一致

保護パック (ウェブ ACL) または他の AWS WAF リソースを作成または変更すると、リソースが保存されているすべての領域にその変更が反映されるまでに少し時間がかかります。伝播時間は、数秒から数分までかかります。

次の内容では、変更伝播中に直面する一時的な不整合性の例を紹介します。

- 保護パック (ウェブ ACL) を作成した後、それをリソースに関連付けようとすると、保護パック (ウェブ ACL) が利用できないことを示す例外が表示される場合があります。
- ルールグループを保護パック (ウェブ ACL) に追加した後、新しいルールグループのルールは、保護パック (ウェブ ACL) が使用されるエリアで有効になり、別のエリアでは有効にならない場合があります。
- ルールのアクション設定を変更した後、古いアクションを一部のエリアで確認され、新しいアクションを別のエリアで確認される場合があります。
- ブロックルールで使用されている IP セットに IP アドレスを追加した後、新しいアドレスはあるエリアではブロックされ、別のエリアでは許可される場合があります。

ハイレベルステップのテストとチューニング

このセクションでは、ウェブ ACL が使用するルールまたはルールグループなど、ウェブ ACL に対する変更をテストするための手順のチェックリストを示します。

> **Note**
>
> このセクションのガイダンスに従うには、保護パック (ウェブ ACL)、ルール、ルールグループなどの AWS WAF 保護の作成および管理方法を理解する必要があります。この情報は、このガイドの前のセクションで説明しています。

保護パック (ウェブ ACL) をテストおよび調整するには

これらのステップを最初にテスト環境で実行し、次に本番環境で実行します。

1. テストの準備

   モニタリング環境を準備し、新しい AWS WAF 保護をテスト用のカウントモードに切り替え、必要なリソースの関連付けを作成します。

   「AWS WAF 保護のテストの準備」を参照してください。
2. テスト環境および本番環境での監視とチューニング

   最初にテスト環境またはステージング環境で、次に本番環境で、必要に応じてトラフィックを処理できることを確認するまで、 AWS WAF 保護を監視および調整します。

   「AWS WAF 保護のモニタリングと調整」を参照してください。
3. 本番環境で保護を有効にする

   テスト保護に納得できたら、それらを本番モードに切り替え、不要なテストアーティファクトをクリーンアップして、監視を続行します。

   「本番環境で保護の有効化」を参照してください。

変更の実装が完了したら、本番環境でウェブトラフィックと保護を監視し、必要に応じて動作していることを確認します。Web トラフィックパターンは時間の経過とともに変化することがあるため、時々保護を調整する必要がある場合があります。

AWS WAF 保護のテストの準備

このセクションでは、 をセットアップして AWS WAF 保護をテストおよび調整する方法について説明します。

> **Note**
>
> このセクションのガイダンスに従うには、 AWS WAF 保護パック (ウェブ ACLs)、ルール、ルールグループなどの保護を作成および管理する方法を一般的に理解する必要があります。この情報は、このガイドの前のセクションで説明しています。

テストを準備するには

1. 保護パック (ウェブ ACL) のログ記録、Amazon CloudWatch メトリクス、および保護パック (ウェブ ACL) のウェブリクエストサンプリングを有効にする

   ログ記録、メトリクス、およびサンプリングを使用して、保護パック (ウェブ ACL) ルールとウェブトラフィックとの相互作用を監視します。

   - ログ記録 – 保護パック (ウェブ ACL) が評価するウェブリクエストをログ AWS WAF に記録するように を設定できます。ログを、CloudWatch ログ、Amazon S3 バケット、または Amazon Data Firehose 配信ストリームに送信できます。フィールドの修正やフィルタリングの適用も可能です。詳細については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。
   - Amazon Security Lake – Security Lake を設定して、保護パック (ウェブ ACL) データを収集できます。Security Lake は、正規化、分析、管理のためにさまざまな ソースからログとイベントデータを収集します。このオプションの詳細については、「Amazon Security Lake ユーザーガイド」の「Amazon Security Lake とは」および「 AWS のサービスからデータを収集する」を参照してください。
   - Amazon CloudWatch メトリクス — 保護パック (ウェブ ACL) 設定で、監視するすべてのメトリック仕様を指定します。および AWS WAF CloudWatch コンソールを使用してメトリクスを表示できます。詳細については、「Amazon CloudWatch によるモニタリング」を参照してください。
   - ウェブリクエストサンプリング — 保護パック (ウェブ ACL) が評価するすべてのウェブリクエストのサンプルを表示できます。ウェブリクエストサンプリングの詳細については、「ウェブリクエストのサンプルの表示」を参照してください。

2. 保護を Count モードに設定します。

   保護パック (ウェブ ACL) 設定で、テストするものをカウントモードに切り替えます。これにより、テスト保護は、リクエストの処理方法を変更することなく、ウェブリクエストに対する一致を記録します。メトリクス、ログ、およびサンプリングされたリクエストで一致を確認し、一致条件を検証し、ウェブトラフィックにどのような影響があるかを理解することができます。一致するリクエストにラベルを追加するルールは、ルールのアクションに関係なくラベルを追加します。

   - 保護パック (ウェブ ACL) で定義されているルール — 保護パック (ウェブ ACL) のルールを編集し、アクションを Count に設定します。
   - ルールグループ — 保護パック (ウェブ ACL) 設定で、ルールグループのルールステートメントを編集し、[Rules] (ルール) ペインで [Override all rule actions] (すべてのルールアクションをオーバーライド) ドロップダウンを開いて [Count] 選択します。JSON で保護パック (ウェブ ACL) を管理する場合、ルールグループ参照ステートメントで `RuleActionOverrides` 設定にリールを追加し、`ActionToUse` を Count に設定します。次のリスト例は、`AWSManagedRulesAnonymousIpList` AWS マネージドルールルールグループの 2 つのルールのオーバーライドを示しています。

```
"ManagedRuleGroupStatement": {
  "VendorName": "AWS",
  "Name": "AWSManagedRulesAnonymousIpList",
    "RuleActionOverrides": [
      {
        "ActionToUse": {
          "Count": {}
        },
        "Name": "AnonymousIPList"
      },
      {
        "ActionToUse": {
          "Count": {}
        },
        "Name": "HostingProviderIPList"
      }
    ],
    "ExcludedRules": []
  }
},
```

ルールアクションのオーバーライドの詳細については、「ルールグループ内のルールアクションのオーバーライド」を参照してください。

独自のルールグループについては、ルールグループ自体のルールアクションを変更しないでください。ルールグループルールCountアクションは、テストに必要なメトリクスやその他のアーティファクトを生成しません。さらに、ルールグループを変更すると、それを使用するすべての保護パック (ウェブ ACL) に影響しますが、保護パック (ウェブ ACL) 設定内の変更は単一の保護パック (ウェブ ACL) にのみ影響します。

- 保護パック (ウェブ ACL) — 新しい保護パック (ウェブ ACL) をテストする場合は、リクエストを許可する保護パック (ウェブ ACL) のデフォルトのアクションを設定します。これにより、トラフィックに影響を与えずにウェブ ACL を試すことができます。

一般的に、カウントモードは本番稼働よりも多くの一致が生成されます。これは、リクエストをカウントするルールが保護パック (ウェブ ACL) によるリクエストの評価を停止しないため、保護パック (ウェブ ACL) で後で実行されるルールもリクエストと一致する場合があるためです。ルールアクションを本番設定に変更すると、リクエストを許可またはブロックするルールは、一致するリクエストの評価を終了します。その結果、一致するリクエストは通常、保護パック (ウェブ ACL) 内のより少ないルールで検査されます。ウェブリクエストの全体的な評価に対するルールアクションの影響の詳細については、「でのルールアクションの使用 AWS WAF」を参照してください。。

これらの設定を使用すると、新しい保護によってウェブトラフィックは変更されませんが、メトリクス、保護パック (ウェブ ACL) ログ、およびリクエストサンプルで一致情報が生成されます。

3. 保護パック (ウェブ ACL) をリソースに関連付ける

   保護パック (ウェブ ACL) がリソースに関連付けられていない場合は、関連付けます。

   「AWS リソースとの保護の関連付けまたは関連付け解除」を参照してください。

これで、保護パック (ウェブ ACL) を監視してチューニングする準備ができました。

AWS WAF 保護のモニタリングと調整

AWS WAF 保護を監視および調整します。

> **Note**
>
> このセクションのガイダンスに従うには、AWS WAF 保護パック (ウェブ ACLs)、ルール、ルールグループなどの保護を作成および管理する方法を一般的に理解する必要があります。この情報は、このガイドの前のセクションで説明しています。

ウェブトラフィックとルールの一致をモニタリングして、保護パック (ウェブ ACL) の動作を確認します。問題が見つかった場合は、ルールを調整して修正し、モニタリングして調整を確認します。

保護パック (ウェブ ACL) が必要に応じてウェブトラフィックを管理するまで、次の手順を繰り返します。

モニタリングおよびチューニング

1. トラフィックとルールの一致をモニタリングする

   トラフィックがフローしていることと、テストルールで一致するリクエストが検出されていることを確認します。

   テストしている保護については、次の情報を参照してください。

   - ログ — 以下はウェブリクエストに一致するルールに関するアクセス情報です。
     - ルール - Count アクションがある保護パック (ウェブ ACL) のルールは、`nonTerminatingMatchingRules` にリストされます。Allow または Block を持つルールは、`terminatingRule` として一覧表示されます。CAPTCHA または Challenge を持つルールは、終了する場合と終了しない場合があり、そのためにルール一致の結果に応じて、2 つのカテゴリのいずれかに一覧表示されます。
     - ルールグループ - ルールグループは `ruleGroupId` フィールドで識別され、そのルールに一致するルールはスタンドアロンルールと同様に分類されます。
     - ラベル - ルールがリクエストに適用したラベルが `Labels` フィールドに一覧表示されます。

     詳細については、「保護パック (ウェブ ACL) トラフィックのログフィールド」を参照してください。
   - Amazon CloudWatch メトリクス – 保護パック (ウェブ ACL) リクエスト評価の次のメトリクスにアクセスできます。

- ルール – メトリクスはルールアクションによってグループ化されます。例えば、Count モードでルールをテストする場合、一致したルールが保護パック (ウェブ ACL) の Count メトリクスとして一覧表示されます。
- ルールグループ – ルールグループのメトリクスは、ルールグループメトリクスの下に一覧表示されます。
- 別のアカウントが所有するルールグループ – ルールグループメトリクスは、通常、ルールグループの所有者にのみ表示されます。ただし、ルールのルールアクションを上書きすると、そのルールのメトリクスが保護パック (ウェブ ACL) メトリクスの下に一覧表示されます。さらに、ルールグループによって追加されたラベルは、保護パック (ウェブ ACL) メトリクスに一覧表示されます。

  ルールグループのカウントアクションルールは、ウェブ ACL ディメンションメトリクスを出力しません - Rule、RuleGroup、およびリージョンディメンションのみ。これは、ルールグループがウェブ ACL で参照されている場合でも適用されます。

  このカテゴリにあるルールグループは AWS の マネージドルール AWS WAF、AWS Marketplace ルールグループ、他のサービスによって提供されるルールグループを識別する、また、他のアカウントから共有されたルールグループも含まれます。Firewall Manager を介して保護パック (ウェブ ACL) がデプロイされると、カウントアクションを持つ WebACL 内のルールはメンバーアカウントにメトリクスを表示しません。
- ラベル – 評価中にウェブリクエストに追加されたラベルは、保護パック (ウェブ ACL) のラベルメトリクスに一覧表示されます。自分のルールやルールグループによって追加されたか、他のアカウントが所有するルールグループのルールによって追加されたかにかかわらず、すべてのラベルのメトリクスにアクセスできます。

詳細については、「ウェブ ACL のメトリクスの表示」を参照してください。

- 保護パック (ウェブ ACL) トラフィック概要ダッシュボード – AWS WAF コンソールで保護パック (ウェブ ACL) のページに移動し、トラフィック概要タブを開いて、保護パック (ウェブ ACL) が評価したウェブトラフィックの概要にアクセスします。

  トラフィック概要ダッシュボードには、アプリケーションのウェブトラフィックを評価するときに が AWS WAF 収集する Amazon CloudWatch メトリクスのほぼリアルタイムの概要が表示されます。

  詳細については、「保護パック (ウェブ ACL) のトラフィック概要ダッシュボード」を参照してください。

- ウェブリクエストのサンプル — ウェブリクエストのサンプルと一致するルールのアクセス情報。サンプル情報では、保護パック (ウェブ ACL) 内のルールのメトリクス名で一致するルールを識別します。ルールグループの場合、メトリックはルールグループ参照ステートメントを識別します。ルールグループ内のルールの場合、サンプルは `RuleWithinRuleGroup` の一致ルール名をリストします。

  詳細については、「ウェブリクエストのサンプルの表示」を参照してください。

2. 誤検知に対処するための緩和を構成する

   ルールが、本来は一致しないはずのウェブリクエストに一致して、誤検出を発生させていると判断した場合、次のオプションを使用して保護パック (ウェブ ACL) 保護を調整して緩和できます。

   ルールの検査基準の修正

   自分のルールについては、多くの場合、ウェブリクエストを検査するために使用する設定を調整する必要があります。例としては、正規表現パターンセット内の仕様の変更、検査前にリクエストコンポーネントに適用するテキスト変換の調整、転送 IP アドレスへの切り替えなどがあります。「でのルールステートメントの使用 AWS WAF」にある問題の原因となっているルールタイプのガイダンスを参照してください。

   より複雑な問題の修正

   制御しない検査基準や複雑なルールについては、要求を明示的に許可またはブロックするルールを追加したり、問題のあるルールによる評価から要求を排除したりするなど、その他の変更が必要になることがあります。管理ルールグループでは、通常、このタイプの緩和策が必要ですが、他のルールも可能です。例としては、レートベースのルールステートメントと SQL インジェクション攻撃ルールステートメントなどがあります。

   誤検出を軽減するために行う方法は、ユースケースによって異なります。一般的なアプローチは以下のとおりです。

   - 緩和ルールの追加：新しいルールの前に実行され、誤検出の原因となっているリクエストを明示的に許可するルールを追加します。ウェブ ACL でのルールの評価順序の詳細については、「ルールの優先度を設定する」を参照してください。

     この方法では、許可されたリクエストは保護されたリソースに送信されるため、評価のために新しいルールに到達することはありません。新しいルールが有料管理ルールグループである場合、このアプローチはルールグループの使用コストを抑えるのにも役立ちます。

- 緩和ルールで論理ルールを追加する：論理ルールステートメントを使用して、新しいルールと誤検出を除外するルールを組み合わせます。詳細については、「での論理ルールステートメントの使用 AWS WAF」を参照してください。

  たとえば、リクエストのカテゴリに対して誤検出を生成する SQL インジェクションアタック match ステートメントを追加するとします。これらの要求に一致するルールを作成し、論理ルールステートメントを使用してルールを組み合わせて、両方が誤検出条件に一致せず、SQL インジェクション攻撃条件に一致するリクエストに対してのみ一致するようにします。

- スコープダウンステートメントを追加する：レートベースのステートメントおよび管理ルールグループ参照ステートメントの場合、メインステートメント内にスコープダウンステートメントを追加して、誤検出の原因となるリクエストを評価から除外します。

  スコープダウンステートメントと一致しないリクエストは、ルールグループまたはレートベースの評価に到達することはありません。スコープダウンステートメントの詳細については、「でのスコープダウンステートメントの使用 AWS WAF」を参照してください。例については、ボット管理からの IP 範囲を除外するを参照してください。

- ラベルマッチルールを追加する— ラベリングを使用するルールグループでは、問題のあるルールがリクエストに適用されているラベルを特定します。ルールグループのルールをまだカウントモードに設定していない場合は、最初にカウントモードに設定する必要がある場合があります。問題のあるルールによって追加されているラベルと一致するラベル一致ルールを、ルールグループの後に実行するように追加します。ラベル一致ルールでは、ブロックするリクエストから許可するリクエストをフィルタリングできます。

  この方法を使用する場合、テストが終了したら、問題のあるルールをルールグループ内でカウントモードで保持し、カスタムラベルマッチルールをそのまま維持します。ラベル一致ステートメントの詳細については、「ラベル一致ルールステートメント」を参照してください。例については、「特定のブロックされたボットを許可する」および「ATP の例: 認証情報の不足および侵害された認証情報のカスタム処理」を参照してください。

- マネージドルールグループのバージョンの変更— バージョン対応管理ルールグループの場合、使用しているバージョンを変更します。たとえば、正常に使用していた最後の静的バージョンに戻すことができます。

  これは通常、一時的な修正です。テスト環境またはステージング環境で最新バージョンのテストを継続している間、またはプロバイダーから互換性が高いバージョンを待っている間に、本番トラフィックのバージョンを変更する場合があるかもしれません。マネージドルールグループの詳細については、「でのマネージドルールグループの使用 AWS WAF」を参照してください。

新しいルールが必要なリクエストと一致していることに納得できたら、テストの次の段階に進み、この手順を繰り返します。テストと調整の最終段階は、本番稼働環境で実行します。

ウェブ ACL のメトリクスの表示

このセクションでは、保護パック (ウェブ ACL) のメトリクスを表示する方法について説明します。

保護パック (ウェブ ACL) を 1 つ以上の AWS リソースに関連付けると、関連付けの結果メトリクスを Amazon CloudWatch グラフで表示できます。

AWS WAF メトリクスの詳細については、「」を参照してくださいAWS WAF メトリクスとディメンション。Amazon CloudWatch メトリクスの詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。

保護パック (ウェブ ACL) の各ルールと、関連付けられたリソースが保護パック (ウェブ ACL) AWS WAF の に転送するすべてのリクエストについて、CloudWatch では以下を実行できます。

- 1 時間前または 3 時間前のデータを表示する
- データポイント間の間隔を変更する
- CloudWatch がデータに対して実行する計算 (最大、最小、平均、合計など) を変更する

> **Note**
>
> AWS WAF CloudFront を使用した はグローバルサービスであり、メトリクスは で米国東部 (バージニア北部) リージョンを選択した場合にのみ使用できます AWS マネジメントコンソール。別のリージョンを選択した場合、 AWS WAF メトリクスは CloudWatch コンソールに表示されません。

保護パック (ウェブ ACL) でルールのデータを表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. 必要に応じて、リージョンを AWS リソースがあるリージョンに変更します。CloudFront の場合、米国東部 (バージニア北部) リージョンを選択する必要があります。
3. ナビゲーションペインの [Metrics] (メトリクス) で、[All metrics] (すべてのメトリクス) を選択し、[Browse] (参照) タブで `AWS::WAFV2` メトリクスを検索します。

4. データを表示する保護パック (ウェブ ACL) のチェックボックスをオンにします。
5. 該当する設定を変更します。

[Statistic] (統計)

CloudWatch がデータに対して実行する計算内容を選択します。

[Time range] (時間範囲)

前の 1 時間のデータを表示するか、前の 3 時間のデータを表示するかを選択します。

[Period] (期間)

グラフでのデータポイント間の間隔を変更します。

[Rules] (ルール)

データを表示するルールを選択します。

> **Note**
>
> ルールの名前を変更し、ルールのメトリクス名に変更を反映する場合は、メトリクス名も更新する必要があります。ルール名を変更しても、ルールのメトリクス名は自動的に更新 AWS WAF されません。ルールの JSON エディターを使用して、コンソールでルールを編集するときに、メトリック名を変更できます。API や、保護パック (ウェブ ACL) またはルールグループの定義に使用する JSON リストを使用して、両方の名前を変更することもできます。

次の点に注意してください。

- 最近保護パック (ウェブ ACL) を AWS リソースに関連付けた場合、データがグラフに表示され、保護パック (ウェブ ACL) のメトリクスが使用可能なメトリクスのリストに表示されるまで数分待つ必要がある場合があります。
- 複数のリソースを保護パック (ウェブ ACL) に関連付けると、CloudWatch データにはそれらすべてのリクエストが含まれます。
- データポイントの上にマウスカーソルを置くと、詳細情報が表示されます。
- グラフは自動的には更新されません。表示を更新するには、更新 () アイコンを選択します。

CloudWatch のメトリクスの詳細については、「Amazon CloudWatch によるモニタリング」を参照してください。

保護パック (ウェブ ACL) のトラフィック概要ダッシュボード

このセクションでは、 AWS WAF コンソールの保護パック (ウェブ ACL) トラフィック概要ダッシュボードについて説明します。保護パック (ウェブ ACL) を 1 つ以上の AWS リソースに関連付け、保護パック (ウェブ ACL) のメトリクスを有効にすると、 AWS WAF コンソールの 保護パック (ウェブ ACL) のトラフィック概要タブに移動して、保護パック (ウェブ ACL) が評価するウェブトラフィックの概要にアクセスできます。ダッシュボードには、特殊な AI ボットやエージェントのアクティビティ分析など、アプリケーションのウェブトラフィックを評価するときに が AWS WAF 収集する Amazon CloudWatch メトリクスのほぼリアルタイムの概要が含まれています。

> **Note**
>
> ダッシュボードに何も表示されない場合は、保護パック (ウェブ ACL) でメトリクスが有効になっていることを確認してください。

保護パック (ウェブ ACL) の [トラフィック概要] タブには、次のカテゴリの情報を含むタブ付きダッシュボードがあります。

- トップセキュリティインサイト – Amazon CloudWatch logsを直接クエリすることで が AWS WAF 取得する AWS WAF 保護に関するインサイト。ダッシュボードの残りの部分では、CloudWatch メトリクスを使用します。これらのインサイトはより豊富な情報を提供しますが、CloudWatch ログのクエリに追加のコストが発生します。追加コストの詳細については、「Amazon CloudWatch Logs の料金」を参照してください。
- AI トラフィック分析 – ボットの識別、インテント分類、アクセスパターン、一時的な傾向など、AI ボットとエージェントのアクティビティについて分析されたウェブリクエスト。このタブは、保護パック (ウェブ ACL) が AI ボットトラフィックを受信したときに使用できます。
- [すべてのトラフィック] — 保護パック (ウェブ ACL) で評価されるすべてのウェブリクエスト。

  ダッシュボードではアクションの終了に重点が置かれていますが、以下の場所でカウントルールに一致するものを確認できます。

  - このダッシュボードの [上位 10 件のルール] ペイン。[カウントアクションに切り替える] をオンにすると、一致するカウントルールが表示されます。

- 保護パック (ウェブ ACL) ページの [サンプルリクエスト] タブ。この新しいタブには、ルールに一致したすべてのグラフが含まれています。詳細については、「ウェブリクエストのサンプルの表示」を参照してください。

- DDoS 対策 – `AntiDDoSRuleSet` DDoS 対策マネージドルールグループを使用して保護パック (ウェブ ACL) が評価するウェブリクエスト。

  このタブは、保護パック (ウェブ ACL) 内のこのルールグループを使用している場合にのみ使用できます。

- [Bot Control] — Bot Control マネージドルールグループを使用して保護パック (ウェブ ACL) で評価されるウェブリクエスト。

- 保護パック (ウェブ ACL) でこのルールグループを使用していない場合、このタブにはウェブトラフィックのサンプリングを Bot Control ルールと照合して評価した結果が表示されます。これにより、アプリケーションが受信するボットトラフィックがわかり、この機能は無料でご利用いただけます。

  このルールグループは、 AWS WAF が提供するインテリジェントな脅威軽減オプションの一部です。詳細については、「AWS WAF ボットコントロール」および「AWS WAF Bot Control ルールグループ」を参照してください。

- アカウント乗っ取り防止 – AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) マネージドルールグループを使用して保護パック (ウェブ ACL) が評価するウェブリクエスト。このタブは、保護パック (ウェブ ACL) 内のこのルールグループを使用している場合にのみ使用できます。

  ATP ルールグループは、 AWS WAF インテリジェントな脅威の軽減保護の一部です。詳細については、「AWS WAF Fraud Control アカウント乗っ取り防止 (ATP)」および「AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループ」を参照してください。

- アカウント作成不正防止 – Fraud Control Account Creation AWS WAF Fraud Prevention (ACFP) マネージドルールグループを使用して保護パック (ウェブ ACL) が評価するウェブリクエスト。このタブは、保護パック (ウェブ ACL) 内のこのルールグループを使用している場合にのみ使用できます。

  ACFP ルールグループは、 AWS WAF のインテリジェントな脅威の緩和保護機能の一部です。詳細については、「AWS WAF Fraud Control アカウント作成不正防止 (ACFP)」および「AWS WAF Fraud Control アカウント作成不正防止 (ACFP) ルールグループ」を参照してください。

ダッシュボードは保護パック (ウェブ ACL) の CloudWatch メトリクスに基づいており、グラフが CloudWatch の対応するメトリクスへのアクセスを提供します。Bot Control のようなインテリジェントな脅威軽減ダッシュボードでは、使用されるメトリクスは主にラベルメトリクスです。

- AWS WAF が提供するメトリクスのリストについては、「」を参照してくださいAWS WAF メトリクスとディメンション。
- Amazon CloudWatch メトリクスの詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。

ダッシュボードには、選択した終了アクションと日付範囲のトラフィックパターンの概要が表示されます。インテリジェント脅威軽減ダッシュボードには、マネージドルールグループ自体が終了アクションを適用したかどうかに関係なく、対応するマネージドルールグループが評価したリクエストが含まれます。たとえば、Block が選択されている場合、[Account Takeover Prevention] ダッシュボードには、ATP マネージドルールグループによって評価されたものと、保護パック (ウェブ ACL) 評価中のある時点でブロックされたものの両方のすべてのウェブリクエストの情報が表示されます。リクエストは ATP マネージドルールグループ、保護パック (ウェブ ACL) のルールグループの後に実行されたルール、または保護パック (ウェブ ACL) のデフォルトアクションによってブロックされる場合があります。

保護パック (ウェブ ACL) のダッシュボードを表示する

保護パック (ウェブ ACL) ダッシュボードにアクセスし、データフィルタリング条件を設定するには、このセクションの手順に従います。最近 AWS リソースに保護パック (ウェブ ACL) を関連付けた場合、ダッシュボードでデータが利用可能になるまで数分かかることがあります。

ダッシュボードには、保護パック (ウェブ ACL) に関連付けたすべてのリソースのリクエストが含まれます。

保護パック (ウェブ ACL) の [トラフィックの概要] ダッシュボードを表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで、[保護パック (ウェブ ACL)] を選択し、目的のウェブ ACL を検索します。
3. 保護パック (ウェブ ACL) を選択します。コンソールで保護パック (ウェブ ACL) のページが表示されます。[トラフィックの概要] タブがデフォルトで選択されています。
4. [データフィルター] の設定を必要に応じて変更します。

- [終了ルールアクション] — ダッシュボードに含める終了アクションを選択します。保護パック (ウェブ ACL) 評価によって選択されたアクションが適用されたウェブリクエストのメトリクスがダッシュボードに要約されます。実行可能なアクションをすべて選択すると、ダッシュボードには評価されたウェブリクエストがすべて含まれます。アクションの詳細については、「がルールとルールグループのアクション AWS WAF を処理する方法」を参照してください。
- [時間範囲] — ダッシュボードに表示する時間間隔を選択します。過去 3 時間や過去 1 週間など、現在を基準にした時間枠を表示したり、カレンダーから絶対的な時間範囲を選択したりできます。
- [タイムゾーン] — この設定は、絶対時間で範囲を指定した場合に適用されます。ブラウザのローカルタイムゾーンまたは UTC (協定世界時) を使用できます。

関心があるタブの情報を確認します。データフィルターの選択は、すべてのダッシュボードに適用されます。グラフペインでは、データポイントまたは領域の上にカーソルを置くと、その他の詳細が表示されます。

Count アクションルール

カウントアクションの一致に関する情報は、2 つの場所のいずれかで表示できます。

- この [トラフィック概要] タブの [すべてのトラフィック] ダッシュボードで、[トップ 10 ルール] ペインを見つけ、[カウントアクションに切り替え] をオンにします。このトグルをオンにすると、ペインには一致したルールだけでなく、一致したルールも表示されます。
- 保護パック (ウェブ ACL) の [サンプルリクエスト] タブで、[トラフィック概要] で設定した期間のルールの一致とアクションの全グラフを参照します。[サンプルリクエスト] タブについて詳細は、「ウェブリクエストのサンプルの表示」を参照してください。

Amazon CloudWatch メトリクス

ダッシュボードのグラフペインでは、グラフ化されたデータの CloudWatch メトリクスにアクセスできます。グラフペインの上部またはペイン右上の [⋮] (垂直省略記号) ドロップダウンメニューからオプションを選択します。

ダッシュボードの更新

ダッシュボードは自動的には更新されません。表示を更新するには、更新



アイコンを選択します。

保護パック (ウェブ ACL) のトラフィックの概要ダッシュボード例

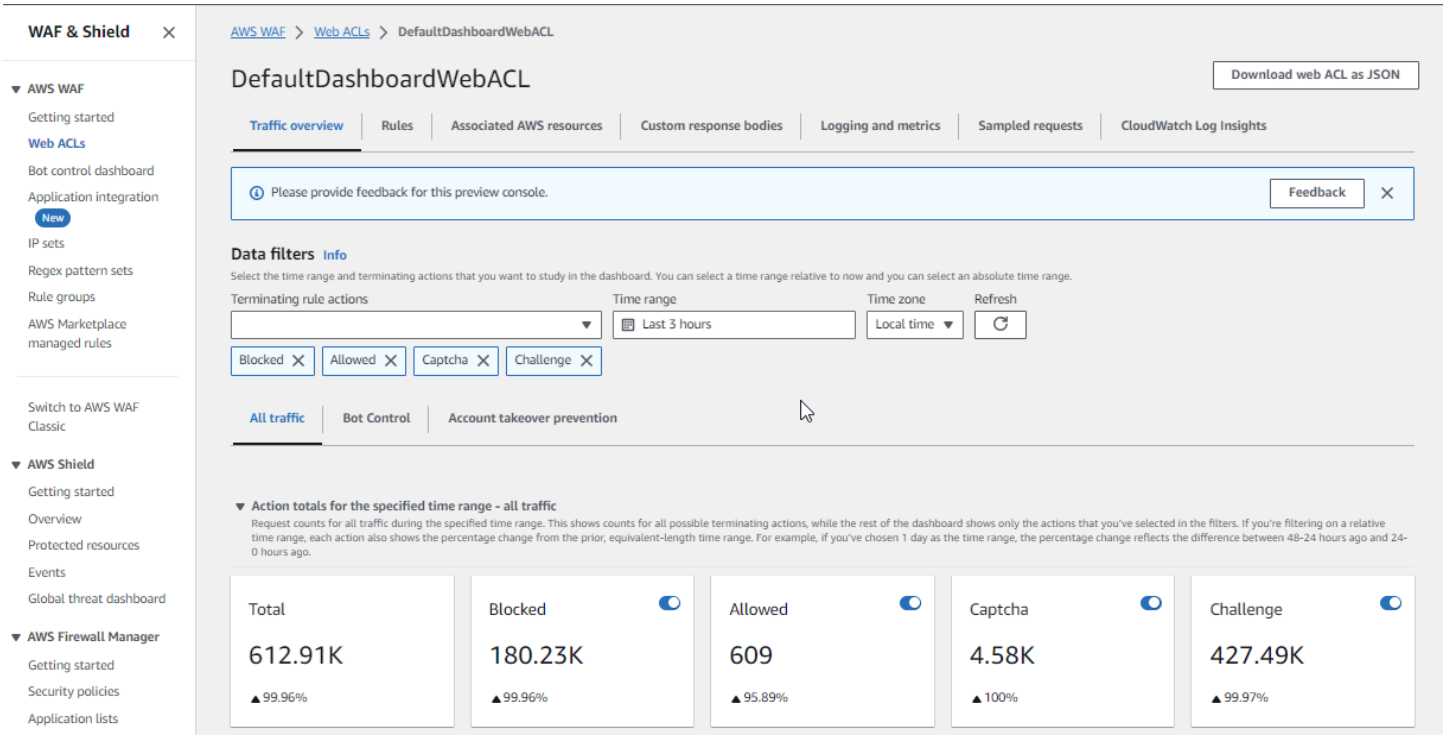
このセクションでは、保護パック (ウェブ ACL) のトラフィック概要ダッシュボードの画面例を示しています。

> **Note**
>
> すでに AWS WAF を使用してアプリケーションリソースを保護している場合は、 AWS WAF コンソールのページで任意の保護パック (ウェブ ACLs) のダッシュボードを表示できます。詳細については、「保護パック (ウェブ ACL) のダッシュボードを表示する」を参照してください。

画面例: データフィルターと [すべてのトラフィック] ダッシュボードのアクション数

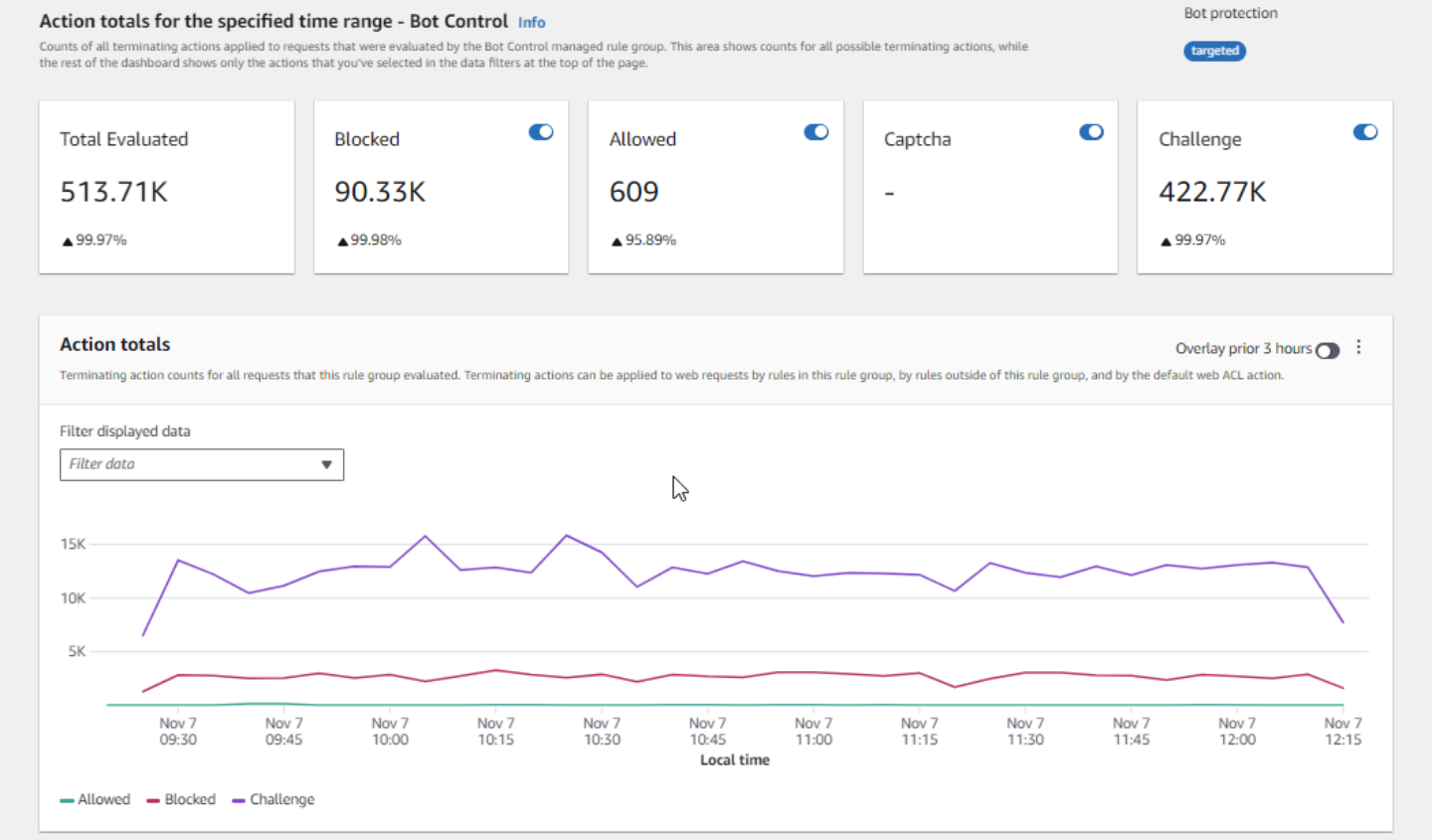
次のスクリーンショットは、[すべてのトラフィック] タブが選択された状態で、保護パック (ウェブ ACL) のトラフィック概要を示しています。データフィルターはデフォルトに設定されており、過去 3 時間のすべての終了アクションを示しています。

すべてのトラフィックダッシュボードには、さまざまな終了アクションのアクション合計が表示されます。各ペインにはリクエスト数が一覧表示され、過去 3 時間の時間範囲からの変化を示す上向き/下向きの矢印が表示されます。



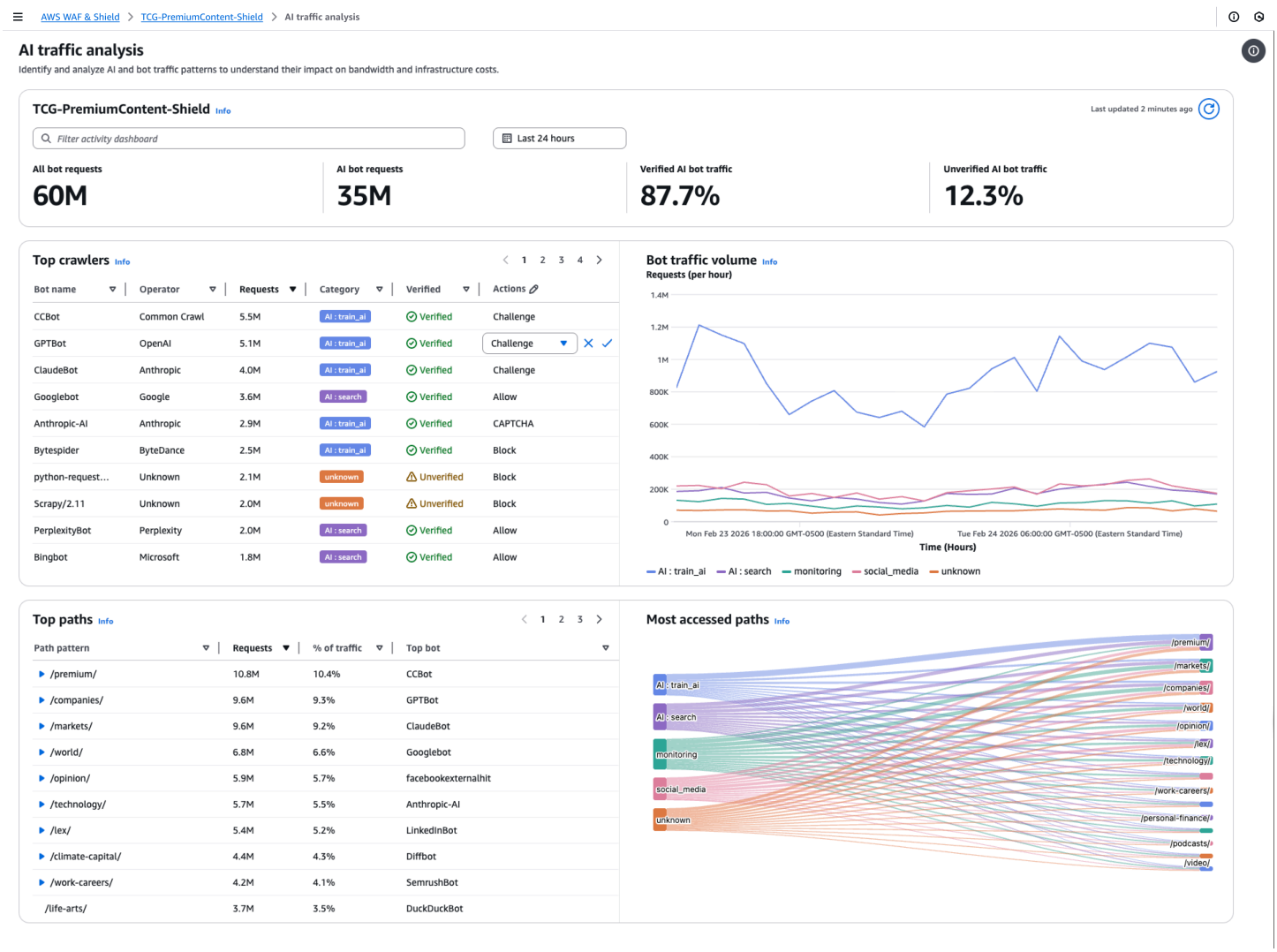
画面の例: [Bot Control] ダッシュボードのアクション数

次のスクリーンショットは、Bot Control ダッシュボードのアクション数を示しています。これは時間範囲で同じ合計ペインを表示していますが、この数は Bot Control ルールグループが評価したリクエストのみを対象としています。さらに下の [アクション合計] ペインには、指定した 3 時間の時間範囲におけるアクション数が表示されます。この時間範囲では、ルールグループが評価したどのリクエストにも CAPTCHA アクションは適用されませんでした。



画面の例: AI トラフィック分析ダッシュボードのアクション数

次のスクリーンショットは、保護パック (ウェブ ACL) の AI トラフィック分析ダッシュボードを示しています。ダッシュボードには、選択した時間範囲における AI ボットアクティビティと、ボットの組織、インテントタイプ、検証ステータスのフィルターが表示されます。



ダッシュボードには以下が含まれます。

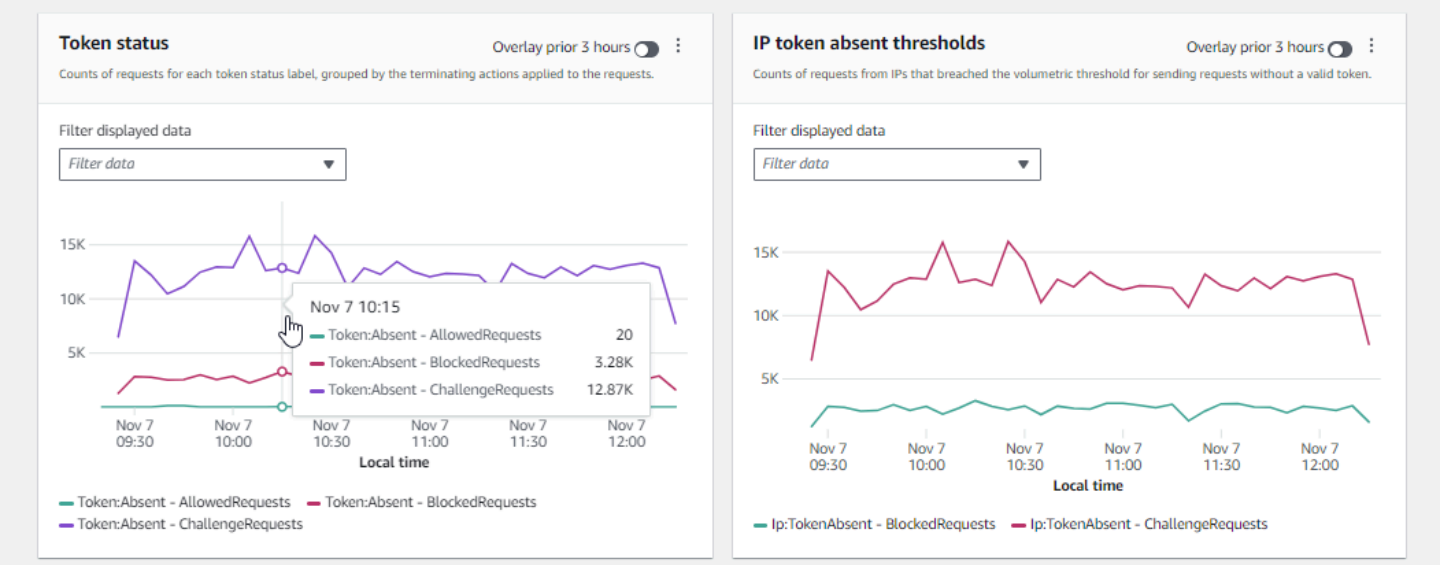
- Bot Identity パネル – 検出された AI ボットを名前と組織で一覧表示します
- 目的分類 – ボットの目的 (クローリング、インデックス作成、調査など) を分類します。
- アクセスパターン – リクエスト数を持つ AI エージェントによってアクセスされた上位 URLs
- 時間分析 – 14 日間の履歴ビューを含む時間単位および日単位のアクティビティの傾向
- 組織の内訳 — ボット所有者組織別のトラフィック量

画面の例: [Bot Control] ダッシュボードのトークンステータスの概要グラフ

次のスクリーンショットは、Bot Control ダッシュボードに表示される 2 つの概要グラフィックを示しています。[トークンステータス] ペインには、さまざまなトークンステータスラベルの数と、リ

クエストに適用されたルールアクションが表示されます。[IP トークン不在しきい値] ペインには、トークンなしで大量のリクエストを送信していた IP からのリクエストのデータが表示されます。

グラフの任意の領域にカーソルを合わせると、利用可能な情報の詳細が表示されます。このスクリーンショットの [トークンステータス] ペインでは、マウスはグラフの線上にない特定の時点にカーソルを合わせているので、コンソールにはその時点のすべての線のデータが表示されます。



このセクションには、保護パック (ウェブ ACL) トラフィック概要ダッシュボードに表示されるトラフィックの概要の一部だけが表示されます。保護パック (ウェブ ACL) のダッシュボードを表示するには、コンソールで保護パック (ウェブ ACL) のページを開きます。これを行う方法については、「保護パック (ウェブ ACL) のダッシュボードを表示する」でガイダンスを参照してください。

ウェブリクエストのサンプルの表示

このセクションでは、 AWS WAF コンソールの保護パック (ウェブ ACL) のサンプルリクエストタブについて説明します。このタブでは、 AWS WAF が検査したウェブリクエストのすべてのルール一致のグラフを表示できます。さらに、保護パック (ウェブ ACL) に対してリクエストサンプリングが有効になっている場合は、 AWS WAF が検査したウェブリクエストのサンプルのテーブルビューが表示されます。また、API コールを通じてサンプルリクエスト情報を取得することもできます `GetSampledRequests`。

リクエストのサンプルには、保護パック (ウェブ ACL) のルールの基準に一致した最大 100 件のリクエストと、いずれのルールにも一致せず、保護パック (ウェブ ACL) のデフォルトアクションが適用されたリクエストの別の 100 件のリクエストが含まれます。サンプルのリクエストは、過去 3 時間にコンテンツについてのリクエストを受け取ったすべての保護されたリソースからのものです。

ウェブリクエストがルールの基準に一致し、そのルールのアクションがリクエスト評価を終了しない場合、 は保護パック (ウェブ ACL) の後続のルールを使用してウェブリクエストの検査を AWS WAF 続行します。このため、ウェブリクエストが複数回表示される可能性があります。ルールアクションの動作については、「でのルールアクションの使用 AWS WAF」を参照してください。

すべてのルールグラフとサンプルされたリクエストを表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. ナビゲーションペインで、[保護パック (ウェブ ACL)] を選択します。
3. リクエストを表示する保護パック (ウェブ ACL) の名前を選択します。コンソールで保護パック (ウェブ ACL) の説明が表示され、そこで編集できます。
4. [サンプルリクエスト] タブには、次の内容が表示されます。

   - [すべてのルールグラフ] — このグラフには、指定した期間中に実行されたすべての Web リクエスト評価の一致ルールとルールアクションが表示されます。

     > **Note**
     >
     > このグラフの時間範囲は、保護パック (ウェブ ACL) の [トラフィック概要] タブの [データフィルター] セクションで設定されます。詳細については、「保護パック (ウェブ ACL) のダッシュボードを表示する」を参照してください。

   - サンプルリクエストテーブル — このテーブルには、過去 3 時間のサンプルリクエストデータが表示されます。

     > **Note**
     >
     > マネージドルールグループで期待されるサンプルが表示されない場合は、この手順の下のセクションを参照してください。

     この表には、エントリごとに以下のデータが表示されます。

     メトリクス名

     リクエストに一致した保護パック (ウェブ ACL) 内のルールの CloudWatch メトリクス名。ウェブリクエストが保護パック (ウェブ ACL) のルールと一致しない場合、この値はデフォルト。

> **Note**
>
> ルールの名前を変更し、ルールのメトリクス名に変更を反映する場合は、メトリクス名も更新する必要があります。ルール名を変更しても、ルールのメトリクス名は自動的に更新 AWS WAF されません。ルールの JSON エディターを使用して、コンソールでルールを編集するときに、メトリック名を変更できます。API や、保護パック (ウェブ ACL) またはルールグループの定義に使用する JSON リストを使用して、両方の名前を変更することもできます。

[Source IP] (送信元 IP)

リクエストの発生元の IP アドレス (ビューワーが HTTP プロキシまたは Application Load Balancer を使用してリクエストを送信した場合は、そのプロキシまたは Application Load Balancer の IP アドレス)。

[URI]

URL 内でリソースを識別する部分 (`/images/daily-ad.jpg` など)。

ルールグループ内のルール

メトリック名がルールグループ参照ステートメントを識別する場合、これにより、リクエストに一致するルールグループ内のルールが識別されます。

Action

対応するルールのアクションを示します。取りうるルールアクションの情報については、「でのルールアクションの使用 AWS WAF」を参照してください。

> **Note**
>
> ルールグループでカウントアクションを使用するルールのサンプルリクエストは、ウェブ ACL ビューでは使用できません。ルールグループルールのカウントメトリクスとサンプリングされたリクエストは、ルールグループの所有者にのみ表示されます。

Time

が保護されたリソースからリクエストを AWS WAF 受信した時間。

ウェブリクエストのコンポーネントに関する追加情報を表示するには、リクエストの行にある URI の名前を選択します。

マネージドルールグループのルールのサンプリングされたリクエスト

コンソールには、トリガーされたルールを指定する「ルールグループ内のルール」を含むルールグループのメトリクスが表示されます。最新のRuleActionOverrides設定を使用して、デフォルトのアクションルールセットとルールのメトリクスを表示できます。古いExcludedRules設定を使用するルールの場合、Sampled Requests メトリクスルールドロップダウンからルールセット内から特定のルールを選択します。

古い設定が表示された場合は、それらを新しい設定に置き換えて、サンプルリクエストをコンソールで使用可能にします。これを行うには、保護パック (ウェブ ACL) のマネージドルールグループを編集して保存します。 AWS WAF は古い設定を自動的に RuleActionOverrides 設定に置き換え、ルールアクションオーバーライドを Count に設定します。これらの 2 つの設定の詳細については、「JSON リスト: RuleActionOverrides を ExcludedRules に置き換えます」を参照してください。

AWS WAF REST API、SDKs、またはコマンドラインを使用して、古いオーバーライドが設定されているルールのサンプルリクエストにアクセスできます。詳細については、「AWS WAF API リファレンス」の GetSampledRequests を参照してください。

コマンドラインリクエストの構文を次に示します。

```
aws wafv2 get-sampled-requests \
  --web-acl-arn webACL ARN \
  --rule-metric-name Metric name of the rule in the managed rule group \
  --scope=REGIONAL or CLOUDFRONT \
  --time-window StartTime=UTC timestamp,EndTime=UTC timestamp \
  --max-items 100
```

本番環境で保護の有効化

このセクションでは、本番稼働でチューニングされた保護を有効にする手順について説明します。

本番環境でのテストとチューニングの最終段階が終了したら、本番モードで保護を有効にします。

> **本番稼働トラフィックのリスク**
>
> 本番稼働トラフィックに保護パック (ウェブ ACL) 実装をデプロイする前に、トラフィックへの潜在的な影響に慣れるまで、テスト環境でテストおよびチューニングします。また、本番稼働用トラフィックの保護を有効にする前に、本番稼働用トラフィックでカウントモードでテストおよびチューニングします。

> **Note**
>
> このセクションのガイダンスに従うには、 AWS WAF 保護パック (ウェブ ACLs)、ルール、ルールグループなどの保護を作成および管理する方法を一般的に理解する必要があります。この情報は、このガイドの前のセクションで説明しています。

これらのステップを最初にテスト環境で実行し、次に本番環境で実行します。

本番環境で AWS WAF 保護を有効にする

1. 本番環境保護に切り替える

   保護パック (ウェブ ACL) を更新し、本番環境の設定を切り替えます。

   a. 不要なテストルールをすべて削除する

      本番環境では必要ないテストルールを追加した場合は、それらを削除します。ラベル一致ルールを使用して管理ルールグループルールの結果をフィルタリングする場合は、必ずそれらのルールをそのままにしておいてください。

   b. 本番用アクションに切り替える

      新しいルールのアクション設定を、意図したプロダクション設定に変更します。

      - 保護パック (ウェブ ACL) で定義されているルール — 保護パック (ウェブ ACL) のルールを編集し、Count からのそれらのアクションを本番環境のアクションに変更します。
      - ルールグループ — ルールグループの保護パック (ウェブ ACL) 設定で、独自のアクションを使用するようにルールを切り替えるか、テストおよびチューニングのアクティビティの結果に応じて、Count アクションオーバーライドがあるままにします。ラベル一致ルール

を使用してルールグループルールの結果をフィルタリングする場合は、必ずそのルールのオーバーライドをそのまま残してください。

ルールのアクションの使用に切り替えるには、保護パック (ウェブ ACL) 設定で、ルールグループのルールステートメントを編集し、ルールの Count オーバーライドを削除します。JSON で保護パック (ウェブ ACL) を管理する場合、ルールグループ参照ステートメントで `RuleActionOverrides` リストからルールのエントリを削除します。

- 保護パック (ウェブ ACL) — 保護パック (ウェブ ACL) のデフォルトアクションをテスト用に変更した場合は、本番用の設定に切り替えます。

これらの設定により、意図したとおりに新しい保護がウェブトラフィックを管理します。

保護パック (ウェブ ACL) を保存すると、それが関連付けられているリソースは本番設定を使用します。

2. モニタリングおよびチューニング

ウェブリクエストが希望どおりに処理されていることを確認するには、新しい機能を有効にした後、トラフィックを注意深く監視します。チューニング作業で監視していたカウントアクションではなく、本番ルールアクションのメトリクスとログを監視します。ウェブトラフィックの変化に適応するために、必要に応じて動作を監視し、調整してください。

Amazon CloudFront AWS WAF での の使用

Amazon CloudFront 機能 AWS WAF で を使用する方法について説明します。

保護パック (ウェブ ACL) を作成するときに、 AWS WAF で検査する 1 つ以上の CloudFront ディストリビューションを指定できます。CloudFront は、個々のテナントを保護する標準ディストリビューションと、単一の共有設定テンプレートを使用して複数のテナントを保護するマルチテナントディストリビューションの 2 種類のディストリビューションをサポートしています。 AWS WAF は、保護パック (ウェブ ACL) で定義したルールに基づいて、両方のディストリビューションタイプのウェブリクエストを検査し、タイプごとに実装パターンが異なります。

トピック

- がさまざまなディストリビューションタイプと AWS WAF 連携する方法
- CloudFront 定額料金プラン AWS WAF での の使用
- CloudFront による AI トラフィックの収益化

- で CloudFront ディストリビューションを保護するための一般的なユースケース AWS WAF

がさまざまなディストリビューションタイプと AWS WAF 連携する方法

ディストリビューションタイプ

AWS WAF は、標準およびマルチテナントディストリビューション CloudFront ディストリビューションの両方にウェブアプリケーションファイアウォール機能を提供します。

標準ディストリビューション

標準ディストリビューションの場合、 はディストリビューションごとに 1 つの保護パック (ウェブ ACL) を使用して保護 AWS WAF を追加します。この保護を有効にするには、既存の保護パック (ウェブ ACL) を CloudFront ディストリビューションに関連付けるか、CloudFront コンソールでワンクリック保護を使用します。これにより、保護パック (ウェブ ACL) を変更すると、それに関連付けられたディストリビューションにのみ影響するため、各ディストリビューションのセキュリティコントロールを個別に管理できます。

CloudFront ディストリビューションを保護するこの簡単な方法は、個々のドメインに単一の保護パック (ウェブ ACL) からの特定の保護を提供するのに最適です。

標準ディストリビューションに関する考慮事項

- 保護パック (ウェブ ACL) の変更は、関連付けられたディストリビューションにのみ影響します
- 各ディストリビューションには、独立した保護パック (ウェブ ACL) 設定が必要です
- ルールとルールグループはディストリビューションごとに個別に管理されます

マルチテナントディストリビューション

マルチテナントディストリビューションの場合、 は単一の保護パック (ウェブ ACL) を使用して複数のドメインに保護 AWS WAF を追加します。マルチテナントディストリビューションによって管理されるドメインは、ディストリビューションテナントと呼ばれます。マルチテナントディストリビューション AWS WAF の保護は、マルチテナントディストリビューションの作成プロセス中または作成後に、CloudFront コンソールでのみ有効にできます。ただし、保護パック (ウェブ ACL) への変更は、引き続き AWS WAF コンソールまたは API を通じて管理されます。

マルチテナントディストリビューションは、次の 2 つのレベルで AWS WAF 保護を可能にする柔軟性を提供します。

- マルチテナントディストリビューションレベル – 関連付けられた保護パック (ウェブ ACL) は、そのディストリビューションを共有するすべてのアプリケーションに適用されるベースラインセキュリティコントロールを提供します
- ディストリビューションテナントレベル – マルチテナントディストリビューション内の個々のテナントは、追加のセキュリティコントロールを実装したり、マルチテナントディストリビューション設定をオーバーライドしたりするために、独自の保護パック (ウェブ ACL) を持つことができます

これらの 2 つの階層により、マルチテナントディストリビューションは、個々のディストリビューションのセキュリティをカスタマイズする能力を失うことなく、複数のドメイン間で AWS WAF 保護を共有するのに最適です。

マルチテナントディストリビューションに関する考慮事項

- 個々のディストリビューションテナントは、関連するマルチテナントディストリビューションに関連付けられている保護パック (ウェブ ACL) に加えられた変更を継承します
- 特定のディストリビューションテナントに関連付けられた保護パック (ウェブ ACL) は、マルチテナント保護パック (ウェブ ACL) レベルで設定された設定をオーバーライドできます
- マネージドルールグループは、ディストリビューションレベルとディストリビューションテナントレベルの両方で実装できます
- アプリケーション識別子をログに保存して、ディストリビューション別にセキュリティイベントを追跡できます

AWS WAF ディストリビューションタイプ別の機能

保護パック (ウェブ ACL) の実装を比較する

AWS WAF 機能	標準ディストリビューション	マルチテナントディストリビューション
保護パック (ウェブ ACL) の関連付け	ディストリビューションごとに 1 つの保護パック (ウェブ ACL)	オプションでテナント固有の保護パック (ウェブ ACL) を使用して、テナント間で保護パック (ウェブ ACL) を共有できます

AWS WAF 機能	標準ディストリビューション	マルチテナントディストリビューション
ルールの管理	ルールが 1 つのディストリビューションに影響する	マルチテナントディストリビューションルールは、関連付けられたすべてのテナントに影響します。ディストリビューションテナント固有のルールは、そのテナントにのみ影響します
マネージドルールグループ	個々のディストリビューションに適用	すべてのテナントにマルチテナントディストリビューションレベルで、または特定のアプリケーションにテナントレベルで適用できます
ログ記録	標準 AWS WAF ログ	ログには、セキュリティイベント属性のテナント識別子が含まれます

CloudFront 定額料金プラン AWS WAF での の使用

CloudFront 定額料金プランは、Amazon CloudFront グローバルコンテンツ配信ネットワーク (CDN) と複数の AWS のサービス および 機能を、トラフィックの急増や攻撃に関係なく、超過料金なしで月額料金にまとめます。

定額料金プランには、シンプルな月額料金の以下の AWS のサービス および 機能が含まれます。

- CloudFront CDN
- AWS WAF および DDoS 保護
- ボット管理と分析
- Amazon Route 53 DNS
- Amazon CloudWatch Logs の取り込み
- TLS 証明書
- サーバーレスエッジコンピューティング

- 毎月の Amazon S3 ストレージクレジット

プランは、アプリケーションのニーズに合わせて、無料、プロ、ビジネス、プレミアムの各階層で利用できます。プランでは、ベストレートを取得するために年間コミットメントは必要ありません。無料プランから始めて、より多くの機能や使用量にアップグレードできます。

プランと機能の詳細なリストについては、「Amazon CloudFront デベロッパーガイド」の「CloudFront 定額料金プラン」を参照してください。 Amazon CloudFront

> **Important**
>
> 料金プランを使用する場合は、有効な AWS WAF 保護パック (ウェブ ACL) を CloudFront ディストリビューションに関連付ける必要があります。pay-as-you-goに切り替えない限り、保護パック (ウェブ ACL) の関連付けを削除することはできません。
> AWS WAF ウェブ ACL はディストリビューションに関連付けられている必要がありますが、セキュリティ設定を完全に制御できます。ウェブ ACL で有効または無効にするルールを調整して保護をカスタマイズし、セキュリティ要件に合わせてルール設定を変更できます。ウェブ ACL ルールの管理については、AWS WAF 「 ルール」を参照してください。

CloudFront による AI トラフィックの収益化

AI トラフィック収益化は、Amazon CloudFront ディストリビューションに関連付けられた AWS WAF ウェブ ACL リソースでのみ使用できます。支払いの検証と決済は CloudFront エッジロケーションで行われ、世界中のエージェントのレイテンシーを最小限に抑えます。

CloudFront Functions と Lambda@Edge で AI トラフィック収益化を使用する場合の考慮事項

Monetize ルールがあるディストリビューションで CloudFront Functions または Lambda@Edge を使用する場合は AWS WAF、 AWS WAF生成されたレスポンスに対して次の動作に注意してください。

AWS WAFが生成したレスポンス (402 Payment Required Challenge)

ビューワーレスポンス関数 (CloudFront Functions および Lambda@Edge) は AWS WAF、生成された 402 レスポンスでは実行されません。これらの関数を使用して、支払いが必要なチャレンジをカスタマイズすることはできません。また、ヘッダーを追加したり変更したりすることもできま

せん。402 レスポンスにカスタムヘッダー (CORS や分析ヘッダーなど) を追加する必要がある場合は、代わりにレスポンスヘッダーポリシーを使用します。レスポンスヘッダー ポリシーは AWS WAF、生成されたレスポンスに適用されます。

CloudFront Functions とレスポンスヘッダーポリシーの詳細については、以下を参照してください。

- ビューワーレスポンス関数は、HTTP ステータスコード 400 以降では実行されません。エッジ関数の制限の詳細については、「HTTP ステータスコード」を参照してください。
- レスポンスヘッダーポリシーの詳細については、「レスポンスヘッダーポリシーについて」を参照してください。

有料レスポンス (決済後 200)

支払い決済が成功すると、オリジンレスポンスはビューワーレスポンス関数を含む通常の CloudFront レスポンスパイプラインを通過します。ビューワーレスポンス関数は、支払い後にエージェントが受け取るレスポンスを変更できます。たとえば、ステータスコードを変更したり、ヘッダーを削除したりできます。

で CloudFront ディストリビューションを保護するための一般的なユースケース AWS WAF

以下の AWS WAF 機能は、すべての CloudFront ディストリビューションで同じように機能します。マルチテナントディストリビューションに関する考慮事項は、各機能シナリオの後に一覧表示されます。

CloudFront カスタムエラーページ AWS WAF での の使用

デフォルトでは、 が指定した条件に基づいてウェブリクエストを AWS WAF ブロックすると、HTTP ステータスコードを CloudFront `403 (Forbidden)`に返し、CloudFront はそのステータスコードをビューワーに返します。ビューワーには、次のような簡潔で特に書式設定されていないデフォルトメッセージが表示されます。

```
Forbidden: You don't have permission to access /myfilename.html on this server.
```

カスタムレスポンスを定義することで、 AWS WAF 保護パック (ウェブ ACL) ルールでこの動作を上書きできます。 AWS WAF ルールを使用したレスポンス動作のカスタマイズの詳細については、「」を参照してくださいBlock アクションのカスタムレスポンスの送信。

> **Note**
>
> AWS WAF ルールを使用してカスタマイズしたレスポンスは、CloudFront カスタムエラーページで定義したレスポンス仕様よりも優先されます。

場合によってウェブサイトの他の部分と同じフォーマットを使用して、CloudFront を介してカスタムエラーメッセージを表示したい場合は、カスタムエラーメッセージを含むオブジェクト (HTML ファイルなど) をビューワーに返すように CloudFront を設定できます 。

> **Note**
>
> CloudFront は、オリジンによって返される HTTP ステータスコード 403 と、リクエストがブロックされた AWS WAF ときに によって返される HTTP ステータスコード 403 を区別できません。つまり、HTTP ステータスコード 403 のさまざまな原因に基づいて、異なるカスタムエラーページを返すことはできません。

CloudFront カスタムエラーページの詳細については、「Amazon CloudFront デベロッパーガイド」の「カスタムエラーレスポンスの生成」を参照してください。

マルチテナントディストリビューションのカスタムエラーページ

CloudFront マルチテナントディストリビューションでは、次の方法でカスタムエラーページを設定できます。

- マルチテナントレベル - これらの設定は、マルチテナントディストリビューションテンプレートを使用するすべてのテナントディストリビューションに適用されます。
- AWS WAF ルール経由 - 保護パック (ウェブ ACLsマルチテナントディストリビューションとテナントレベルのカスタムエラーページの両方よりも優先されます。

独自の HTTP サーバーで実行されているアプリケーションに CloudFront AWS WAF で を使用する

CloudFront AWS WAF で を使用すると、Amazon Elastic Compute Cloud (Amazon EC2) で実行されているウェブサーバーでも、プライベートに管理するウェブサーバーでも、任意の HTTP ウェブサーバーで実行されているアプリケーションを保護できます。CloudFront と独自のウェブサーバー

間、およびビューワーと CloudFront の間で HTTPS が必須になるように CloudFront を設定することもできます。

CloudFront と独自のウェブサーバー間での HTTPS の必須化

CloudFront と独自のウェブサーバー間で HTTPS を必須にするには、CloudFront カスタムオリジン機能を使用し、特定のオリジンの [Origin Protocol Policy] (オリジンプロトコルポリシー) および [Origin Domain Name] (オリジンドメイン名) の設定を構成します。CloudFront 設定では、オリジンからオブジェクトをフェッチするとき CloudFront で使用するポートとプロトコルとともに、サーバーの DNS 名を指定できます。また、カスタムオリジンサーバー上の SSL/TLS 証明書が、設定したオリジンドメイン名と一致することを確認する必要もあります。の外部で独自の HTTP ウェブサーバーを使用する場合は AWS、信頼できるサードパーティー認証機関 (CA) によって署名された証明書を使用する必要があります。例えば、Comodo、DigiCert、Symantec などです。CloudFront と独自のウェブサーバー間の通信に HTTPS を要求する方法の詳細については、「Amazon CloudFront デベロッパーガイド」の「CloudFront とカスタムオリジン間の通信で HTTPS を必須にする」のトピックを参照してください。

ビューワーと CloudFront との間での HTTPS の必須化

ビューワーと CloudFront の間に HTTPS を要求するために、CloudFront ディストリビューションの 1 つ以上のキャッシュ動作のビューワープロトコルポリシーを変更できます。ビューワーと CloudFront 間での HTTPS の使用の詳細については、「Amazon CloudFront デベロッパーガイド」の「ビューワーと CloudFront 間の通信で HTTPS を必須にする」のトピックを参照してください。独自の SSL 証明書を使用して、ビューワーが独自のドメイン名を使用して HTTPS 経由で CloudFront ディストリビューションに接続できるようにすることもできます (例: https://www.mysite.com)。詳細については、「Amazon CloudFront デベロッパーガイド」の「代替ドメイン名とHTTPS を使用する」のトピックを参照してください。

マルチテナントディストリビューションの場合、HTTP メソッド設定は次の階層に従います。

- テンプレートレベルの設定は、すべてのテナントディストリビューションで許可されるベースライン HTTP メソッドを定義します。
- テナントディストリビューションは、これらの設定を次のようにオーバーライドできます。
  - マルチテナントディストリビューションよりも少ないメソッドを許可する (AWS WAF ルールを使用して追加のメソッドをブロックする)
  - マルチテナントディストリビューションがサポートするように設定されている場合、より多くのメソッドを許可する

- AWS WAF マルチテナントディストリビューションレベルとテナントレベルの両方の ルールは、CloudFront 設定に関係なく HTTP メソッドをさらに制限できます。

CloudFront が応答する HTTP メソッドの選択

Amazon CloudFront のウェブディストリビューションを作成するときは、CloudFront によって処理されてオリジンに転送される HTTP メソッドを選択します。次のオプションから選択できます。

- **GET、HEAD** – CloudFront を使用して、オリジンからのオブジェクトの取得またはオブジェクトヘッダーの取得のみを行うことができます。
- **GET、HEAD、OPTIONS** – CloudFront を使用して、オリジンからのオブジェクトの取得、オブジェクトヘッダーの取得、またはオリジンサーバーがサポートするオプションのリスト取得のみを行うことができます。
- **GET、HEAD、OPTIONS、PUT、POST、PATCH、DELETE** – CloudFront を使用して、オブジェクトの取得、追加、更新、削除、およびオブジェクトヘッダーの取得を行うことができます。また、ウェブフォームからのデータの送信など、その他の POST オペレーションも実行できます。

「」で説明されているように、 AWS WAF バイト一致ルールステートメントを使用して、HTTP メソッドに基づいてリクエストを許可またはブロックすることもできます文字列一致ルールステートメント。GET や など、CloudFront がサポートするメソッドの組み合わせを使用する場合はHEAD、他のメソッドを使用するリクエストをブロック AWS WAF するように を設定する必要はありません。GET、、 など、CloudFront がサポートしていないメソッドの組み合わせを許可する場合はPOST、すべてのメソッドに応答するように CloudFront HEADを設定し、 を使用して他のメソッドを使用するリクエスト AWS WAF をブロックできます。

が応答するメソッドの選択の詳細については、「Amazon CloudFront デベロッパーガイド」で「ウェブディストリビューションを作成または更新する場合に指定する値」トピックの「許可される HTTP メソッド」を参照してください。

HTTP メソッド設定がマルチテナントディストリビューションで許可されている

マルチテナントディストリビューションの場合、マルチテナントディストリビューションレベルで設定された HTTP メソッド設定は、デフォルトですべてのテナントディストリビューションに適用されます。テナントディストリビューションは、必要に応じてこれらの設定をオーバーライドできます。

- GET や など、CloudFront がサポートするメソッドの組み合わせを使用する場合はHEAD、他のメソッドを使用するリクエストをブロック AWS WAF するように を設定する必要はありません。

- GET、、 など、CloudFront がデフォルトでサポートしていないメソッドの組み合わせを許可する場合はPOST、すべてのメソッドに応答するように CloudFront HEADを設定し、 を使用して他のメソッドを使用するリクエスト AWS WAF をブロックできます。

マルチテナントディストリビューションにセキュリティヘッダーを実装する場合は、次の点を考慮してください。

- テンプレートレベルのセキュリティヘッダーは、すべてのテナントディストリビューションでベースライン保護を提供します
- テナントディストリビューションは次のことができます。
  - マルチテナントディストリビューションで定義されていない新しいセキュリティヘッダーを追加する
  - テナント固有のヘッダーの値を変更する
  - マルチテナントディストリビューションレベルで設定されたセキュリティヘッダーを削除またはオーバーライドすることはできません
- すべてのテナントに適用する必要がある重要なセキュリティコントロールには、マルチテナントディストリビューションレベルのヘッダーを使用することを検討してください。

ログ記録に関する考慮事項

標準ディストリビューションとマルチテナントディストリビューションの両方が AWS WAF ログ記録をサポートしていますが、ログの構造と管理方法には重要な違いがあります。

ログ記録の比較

標準ディストリビューション	マルチテナントディストリビューション
ディストリビューションごとに 1 つのログ設定	テンプレートとテナントレベルのログ記録オプション
標準ログフィールド	追加のテナント識別子フィールド
ディストリビューションごとに 1 つの送信先	マルチテナントディストリビューションとテナントログに可能な別々の送信先

その他のリソース

- マルチテナントディストリビューションの詳細については、「Amazon CloudFront デベロッパーガイド」の「ディストリビューションの設定」を参照してください。
- CloudFront AWS WAF での の使用の詳細については、Amazon CloudFront デベロッパーガイド」の AWS WAF 「保護の使用」を参照してください。
- AWS WAF ログの詳細については、「」を参照してください保護パック (ウェブ ACL) トラフィックのログフィールド。

AWS WAF サービスの使用におけるセキュリティ

このセクションでは、 責任共有モデルがどのように適用されるかについて説明します AWS WAF。

でのクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを活用できます。

> **Note**
>
> このセクションでは、 AWS WAF 保護パック (ウェブ ACLs) やルールグループなど、 AWS WAF サービスとその AWS リソースの使用に関する標準的な AWS セキュリティガイダンスを提供します。
> を使用して AWS リソースを保護する方法については AWS WAF、この AWS WAF ガイドの残りの部分を参照してください。

セキュリティは、 AWS お客様とお客様の間の責任共有です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ – AWS は、 で AWS サービスを実行するインフラストラクチャを保護する責任を担います AWS クラウド。 は、お客様が安全に使用できるサービス AWS も提供します。セキュリティの有効性は、AWS コンプライアンスプログラムの一環として、サードパーティーの審査機関によって定期的にテストおよび検証されています。が適用されるコンプライアンスプログラムの詳細については AWS WAF、AWS「コンプライアンスプログラムによる対象範囲内のサービス」を参照してください。

- クラウドのセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、お客様のデータの機密性、組織の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、 を使用する際の責任共有モデルの適用方法を理解するのに役立ちます AWS WAF。以下のトピックでは、セキュリティとコンプライアンスの目的を達成する AWS WAF ようにを設定する方法を示します。また、 AWS WAF リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

- でのデータの保護 AWS WAF
- での IAM の使用 AWS WAF
- でのログ記録とモニタリング AWS WAF
- でのコンプライアンスの検証 AWS WAF
- でのレジリエンスの構築 AWS WAF
- のインフラストラクチャセキュリティ AWS WAF

でのデータの保護 AWS WAF

AWS 責任共有モデル は、 AWS WAFでのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「 AWS のサービス 」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「Data Privacy FAQChina」を参照してください。 欧州におけるデータ保護に関する情報については、General Data Protection Regulation (GDPR) Center を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM アイデンティティセンターまたは AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須ですが、TLS 1.3 を推奨します。

- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール AWS WAF 、API、または SDK を使用して AWS CLIまたは他の AWS のサービス を操作する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

AWS WAF 保護パック (ウェブ ACLs)、ルールグループ、IP セットなどの エンティティは、中国 (北京) や中国 (寧夏) など、暗号化が利用できない特定のリージョンを除き、保管時に暗号化されます。リージョンごとに一意の暗号化キーが使用されます。

AWS WAF リソースの削除

AWS WAFで作成したリソースは削除できます。次のセクションの各リソースタイプのガイダンスを参照してください。

- 保護パック (ウェブ ACL) の削除
- ルールグループの削除
- IP セットの削除
- 正規表現パターンセットの削除

での IAM の使用 AWS WAF

このセクションでは、 で IAM を使用する方法について説明します AWS WAF。

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に AWS WAF リソースの使用を許可する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで使用できる AWS のサービス です。

トピック

- オーディエンス
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- が IAM と AWS WAF 連携する方法
- のアイデンティティベースのポリシーの例 AWS WAF
- AWS の 管理ポリシー AWS WAF
- AWS WAF ID とアクセスのトラブルシューティング
- のサービスにリンクされたロールの使用 AWS WAF

オーディエンス

AWS Identity and Access Management (IAM) の使用方法は、ロールによって異なります。

- サービスユーザー - 機能にアクセスできない場合は、管理者にアクセス許可をリクエストします (「AWS WAF ID とアクセスのトラブルシューティング」を参照)。
- サービス管理者 - ユーザーアクセスを決定し、アクセス許可リクエストを送信します (「が IAM と AWS WAF 連携する方法」を参照)
- IAM 管理者 - アクセスを管理するためのポリシーを作成します (「のアイデンティティベースのポリシーの例 AWS WAF」を参照)

アイデンティティを使用した認証

認証は、ID 認証情報 AWS を使用して にサインインする方法です。、IAM ユーザー AWS アカウントのルートユーザー、または IAM ロールを引き受けることで認証される必要があります。

AWS IAM アイデンティティセンター (IAM Identity Center)、シングルサインオン認証、Google/Facebook 認証情報などの ID ソースからの認証情報を使用して、フェデレーティッド ID としてサインインできます。サインインの詳細については、「AWS サインイン ユーザーガイド」の「AWS アカウントにサインインする方法」を参照してください。

プログラムによるアクセスの場合、 は SDK と CLI AWS を提供してリクエストを暗号化して署名します。詳細については、「IAM ユーザーガイド」の「API リクエストに対するAWS 署名バージョン 4」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、まず、すべての AWS のサービス および リソースへの完全なアクセス権を持つ AWS アカウント root ユーザーと呼ばれる 1 つのサインイン ID から始めます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザー認証情報を必要とするタスクについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーテッドアイデンティティ

ベストプラクティスとして、人間のユーザーが一時的な認証情報 AWS のサービス を使用して にアクセスするには、ID プロバイダーとのフェデレーションを使用する必要があります。

フェデレーティッド ID は、エンタープライズディレクトリ、ウェブ ID プロバイダー、または ID Directory Service ソースの認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーテッドアイデンティティは、一時的な認証情報を提供するロールを引き受けます。

アクセスを一元管理する場合は、 AWS IAM アイデンティティセンターをお勧めします。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「IAM アイデンティティセンターとは」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、特定の個人やアプリケーションに対する特定のアクセス許可を持つアイデンティティです。長期認証情報を持つ IAM ユーザーの代わりに一時的な認証情報を使用することをお勧めします。詳細については、IAM ユーザーガイドの「ID プロバイダーとのフェデレーションを使用して にアクセスする必要がある AWS」を参照してください。

IAM グループは、IAM ユーザーの集合を指定し、大量のユーザーに対するアクセス許可の管理を容易にします。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可を持つアイデンティであり、一時的な認証情報を提供します。ユーザーから IAM ロール (コンソール) に切り替えるか、 または API オペレーションを呼び出すことで、ロールを引き受けることができます。 AWS CLI AWS 詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールは、フェデレーションユーザーアクセス、一時的な IAM ユーザーのアクセス許可、クロスアカウントアクセス、クロスサービスアクセス、および Amazon EC2 で実行するアプリケーションに役立ちます。詳細については、IAM ユーザーガイド の IAM でのクロスアカウントリソースアクセス を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは、ID またはリソースに関連付けられている場合のアクセス許可を定義します。 は、プリンシパルがリクエストを行うときに、これらのポリシー AWS を評価します。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は、ポリシーを使用して、どのプリンシパルがどのリソースに対して、どのような条件でアクションを実行できるかを定義することで、誰が何にアクセスできるかを指定します。

デフォルトでは、ユーザーやロールにアクセス許可はありません。IAM 管理者は IAM ポリシーを作成してロールに追加し、このロールをユーザーが引き受けられるようにします。IAM ポリシーは、オペレーションの実行方法を問わず、アクセス許可を定義します。

アイデンティティベースのポリシー

アイデンティティベースのポリシーは、アイデンティティ (ユーザー、グループ、またはロール) にアタッチできる JSON アクセス許可ポリシードキュメントです。これらのポリシーは、アイデンティティがどのリソースに対してどのような条件下でどのようなアクションを実行できるかを制御します。アイデンティティベースポリシーの作成方法については、IAM ユーザーガイド の カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する を参照してください。

アイデンティティベースのポリシーは、インラインポリシー (単一の ID に直接埋め込む) または管理ポリシー (複数の ID にアタッチされたスタンドアロンポリシー) にすることができます。管理ポリシーとインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。例としては、IAM ロール信頼ポリシーや Amazon S3 バケットポリシーなどがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

その他のポリシータイプ

AWS は、より一般的なポリシータイプによって付与されるアクセス許可の最大数を設定できる追加のポリシータイプをサポートしています。

- アクセス許可の境界 – アイデンティティベースのポリシーで IAM エンティティに付与することのできるアクセス許可の数の上限を設定します。詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可境界」を参照してください。
- サービスコントロールポリシー (SCP) - AWS Organizations内の組織または組織単位の最大のアクセス許可を指定します。詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」を参照してください。
- リソースコントロールポリシー (RCP) – は、アカウント内のリソースで利用できる最大数のアクセス許可を定義します。詳細については、「AWS Organizations ユーザーガイド」の「リソースコントロールポリシー (RCP)」を参照してください。
- セッションポリシー – ロールまたはフェデレーションユーザーの一時セッションを作成する際にパラメータとして渡される高度なポリシーです。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成されるアクセス許可を理解するのがさらに難しくなります。が複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、「IAM ユーザーガイド」の「ポリシー評価ロジック」を参照してください。

が IAM と AWS WAF 連携する方法

このセクションでは、 で IAM の機能を使用する方法について説明します AWS WAF。

> **Note**
>
> Application Load Balancer および のウェブ ACL 関連付け関連オペレーションを呼び出すときに、より詳細な制御を可能にする新しいアクションを IAM ポリシーに導入します AWS AppSync。「追加のアクセス許可設定が必要なアクション」を参照してください。

IAM を使用して へのアクセスを管理する前に AWS WAF、 で使用できる IAM 機能を確認してください AWS WAF。

で使用できる IAM 機能 AWS WAF

IAM 機能	AWS WAF サポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	はい
ポリシーアクション	あり
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	はい
ACL	なし
ABAC (ポリシー内のタグ)	部分的
一時認証情報	あり
転送アクセスセッション (FAS)	あり
サービスロール	あり
サービスリンクロール	はい

AWS WAF およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要については、IAM ユーザーガイドのAWS 「IAM と連携する のサービス」を参照してください。

のアイデンティティベースのポリシー AWS WAF

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティ

ベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

AWS WAF アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいのアイデンティティベースのポリシーの例 AWS WAF。

内のリソースベースのポリシー AWS WAF

リソースベースのポリシーのサポート: あり

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシー や Amazon S3 バケットポリシー があげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーで、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、全体のアカウント、または別のアカウントの IAM エンティティを、リソースベースのポリシーのプリンシパルとして指定します。詳細については、IAM ユーザーガイドのIAM でのクロスアカウントリソースアクセスを参照してください。

AWS WAF はリソースベースのポリシーを使用して、アカウント間のルールグループの共有をサポートします。リソースベースのポリシー設定を AWS WAF API コール、`PutPermissionPolicy`または同等の CLI または SDK コールに提供することで、所有するルールグループを別の AWS アカウントと共有します。その他の利用可能な言語の例やドキュメントへのリンクなど、追加情報については、 AWS WAF API リファレンスのPutPermissionPolicy」を参照してください。この機能は、コンソールや CloudFormationなどの他の方法では使用できません。

のポリシーアクション AWS WAF

ポリシーアクションのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action` 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

それぞれの AWS WAF アクションとアクセス許可のリストを確認するには、「サービス認可リファレンス」のAWS WAF V2 で定義されるアクション」を参照してください。

のポリシーアクションは、アクションの前に次のプレフィックス AWS WAF を使用します。

```
wafv2
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "wafv2:action1",
      "wafv2:action2"
         ]
```

ワイルドカード (*) を使用すると、複数のアクションを指定することができます。たとえば、 で始 AWS WAF まる のすべてのアクションを指定するには`List`、次のアクションを含めます。

```
"Action": "wafv2:List*"
```

AWS WAF アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいのアイデンティティベースのポリシーの例 AWS WAF。

追加のアクセス許可設定が必要なアクション

一部のアクションには、「サービス認可リファレンス」のAWS WAF V2 で定義されるアクション」で完全に説明できないアクセス許可が必要です。このセクションは、追加のアクセス許可に関する情報を説明します。

トピック

- AssociateWebACL のアクセス権限
- DisassociateWebACL のアクセス権限

- GetWebACLForResource のアクセス権限
- ListResourcesForWebACL のアクセス権限

`AssociateWebACL` のアクセス権限

このセクションでは、 AWS WAF アクションAssociateWebACL を使用してウェブ ACL をリソースに関連付けるために必要なアクセス許可の一覧を示します。

Amazon CloudFront ディストリビューションでは、このアクションの代わりに CloudFront アクション UpdateDistribution を使用してください。詳細については、「Amazon CloudFront API リファレンス」の「UpdateDistribution」を参照してください。

Amazon API Gateway REST API

REST API リソースタイプSetWebACLで API Gateway を呼び出し、保護パック (ウェブ ACL) で を呼び AWS WAF AssociateWebACL出すアクセス許可が必要です。

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "apigateway:SetWebACL"
    ],
    "Resource": [
        "arn:aws:apigateway:*::/restapis/*/stages/*"
    ]
}
```

Application Load Balancer

古いアクセス許可の設定

Application Load Balancer リソースタイプで elasticloadbalancing:SetWebACLアクションを呼び出し、保護パック (ウェブ ACL) AssociateWebACLで を呼び AWS WAF 出すアクセス許可が必要です。

```
{
                    "Sid": "AssociateWebACL1",
                    "Effect": "Allow",
                    "Action": [
                       "wafv2:AssociateWebACL"
                    ],
                    "Resource": [
                       "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
                    ]
                },
                {
                    "Sid": "AssociateWebACL2",
                    "Effect": "Allow",
                    "Action": [
                       "elasticloadbalancing:SetWebACL"
                    ],
                    "Resource": [
                       "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
                    ]
                }
```

新しいアクセス許可の設定

Application Load Balancer リソースタイプで elasticloadbalancing:CreateWebACLAssociationアクションを呼び出し、保護パック (ウェブ ACL) AssociateWebACLで を呼び AWS WAF 出すアクセス許可が必要です。

```
{
   "Sid": "AssociateWebACL1",
   "Effect": "Allow",
   "Action": [
      "wafv2:AssociateWebACL"
   ],
   "Resource": [
      "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
   ]
},
{
```

```
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
       "elasticloadbalancing:CreateWebACLAssociation"
    ],
    "Resource": [
          "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
    ]
}
```

AWS AppSync GraphQL API

古いアクセス許可の設定

GraphQL API リソースタイプで を呼び出し AWS AppSync SetWebACL、保護パック (ウェブ ACL) で を呼び AWS WAF AssociateWebACL出すアクセス許可が必要です。

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "appsync:SetWebACL"
    ],
    "Resource": [
        "arn:aws:appsync:*:account-id:apis/*"
    ]
}
```

新しいアクセス許可の設定

GraphQL API リソースタイプで appsync:AssociateWebACLアクションを呼び出し、保護パック (ウェブ ACL) で を呼び AWS WAF AssociateWebACL出すアクセス許可が必要です。

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "appsync:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:appsync:*:account-id:apis/*"
    ]
}
```

Amazon Cognito ユーザープール

ユーザープールリソースタイプで Amazon Cognito `AssociateWebACL`アクションを呼び出し、保護パック (ウェブ ACL) で を呼び AWS WAF `AssociateWebACL`出すアクセス許可が必要です。

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:AssociateWebACL"
    ],
    "Resource": [
```

```
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner サービス

App Runner サービスリソースタイプで App Runner `AssociateWebACL`アクションを呼び出し、ウェブ ACL で を呼び AWS WAF `AssociateWebACL`出すアクセス許可が必要です。

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:AssociateWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

Amazon Bedrock AgentCore Gateway

Bedrock AgentCore Gateway リソースタイプで `bedrock-agentcore:GatewayAssociateWebACL`アクションを呼び出し、ウェブ ACL を呼び出す AWS WAF `AssociateWebACL`アクセス許可が必要です。

```
{
  "Sid": "AssociateWebACL1",
  "Effect": "Allow",
  "Action": [
    "wafv2:AssociateWebACL"
  ],
```

```
  "Resource": [
    "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
  ]
},
{
  "Sid": "AssociateWebACL2",
  "Effect": "Allow",
  "Action": [
    "bedrock-agentcore:GatewayAssociateWebACL"
  ],
  "Resource": [
    "arn:aws:bedrock-agentcore:*:account-id:gateway/*"
  ]
}
```

AWS Verified Access インスタンス

Verified Access インスタンスリソースタイプで `ec2:AssociateVerifiedAccessInstanceWebAcl`アクションを呼び出し、ウェブ ACL で を呼び AWS WAF `AssociateWebACL`出すアクセス許可が必要です。

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "ec2:AssociateVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

`DisassociateWebACL` のアクセス権限

このセクションでは、 AWS WAF アクション `DisassociateWebACL` を使用して保護パック (ウェブ ACL) とリソースの関連付けを解除するために必要なアクセス許可を一覧表示します。

Amazon CloudFront ディストリビューションでは、このアクションの代わりに、空の保護パック (ウェブ ACL) ID を持つ CloudFront アクション `UpdateDistribution` を使用してください。詳細については、「Amazon CloudFront API リファレンス」の「UpdateDistribution」を参照してください。

Amazon API Gateway REST API

REST API リソースタイプで API ゲートウェイ `SetWebACL` を呼び出すアクセス許可が必要です。を呼び出すアクセス許可は必要ありません AWS WAF `DisassociateWebACL`。

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "apigateway:SetWebACL"
    ],
    "Resource": [
        "arn:aws:apigateway:*::/restapis/*/stages/*"
    ]
}
```

Application Load Balancer

古いアクセス許可の設定

Application Load Balancer リソースタイプで `elasticloadbalancing:SetWebACL` アクションを呼び出すアクセス許可が必要です。を呼び出すアクセス許可は必要ありません AWS WAF `DisassociateWebACL`。

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "elasticloadbalancing:SetWebACL"
    ],
    "Resource": [
```

```
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
    ]
}
```

新しいアクセス許可の設定

Application Load Balancer リソースタイプで `elasticloadbalancing:DeleteWebACLAssociation` アクションを呼び出すアクセス許可が必要です。また、 を呼び出すアクセス許可も必要です AWS WAF `DisassociateWebACL`。

```
{
      "Sid": "DisassociateWebACL",
      "Effect": "Allow",
      "Action": "wafv2:DisassociateWebACL",
      "Resource": "*"
    },
    {
      "Sid": "DisassociateWebACL2",
      "Effect": "Allow",
      "Action": [
         "elasticloadbalancing:DeleteWebACLAssociation"
      ],
      "Resource": [
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
      ]
   }
}
```

AWS AppSync GraphQL API

古いアクセス許可の設定

GraphQL API リソースタイプで を呼び AWS AppSync `SetWebACL`出すアクセス許可が必要です。AWS WAF `DisassociateWebACL` の呼び出しにはアクセス許可は必要ありません。

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "appsync:SetWebACL"
    ],
    "Resource": [
```

```
        "arn:aws:appsync:*:account-id:apis/*"
    ]
}
```

新しいアクセス許可の設定

GraphQL API リソースタイプで appsync:DisassociateWebACLアクションを呼び出すアクセス許可が必要です。また、 を呼び出すアクセス許可も必要です AWS WAF DisassociateWebACL。

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "appsync:DisassociateWebACL"
    ],
    "Resource": [
        "arn:aws:appsync:*:account-id:apis/*"
    ]
}
```

Amazon Cognito ユーザープール

ユーザープールリソースタイプで Amazon Cognito DisassociateWebACLアクションを呼び出し、を呼び出すアクセス許可が必要です AWS WAF DisassociateWebACL。

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:DisassociateWebACL"
```

```
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner サービス

App Runner サービスリソースタイプで App Runner `DisassociateWebACL`アクションを呼び出し、 を呼び出すアクセス許可が必要です AWS WAF `DisassociateWebACL`。

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:DisassociateWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

Amazon Bedrock AgentCore Gateway

Bedrock AgentCore Gateway リソースタイプで `bedrock-agentcore:GatewayDisassociateWebACL`アクションを呼び出し、 を呼び出すアクセス許可が必要です AWS WAF `DisassociateWebACL`。

```
{
  "Sid": "DisassociateWebACL",
  "Effect": "Allow",
  "Action": [
    "wafv2:DisassociateWebACL"
  ],
  "Resource": "*"
},
```

```
{
  "Sid": "DisassociateWebACL2",
  "Effect": "Allow",
  "Action": [
    "bedrock-agentcore:GatewayDisassociateWebACL"
  ],
  "Resource": [
    "arn:aws:bedrock-agentcore:*:account-id:gateway/*"
  ]
}
```

AWS Verified Access インスタンス

Verified Access インスタンスリソースタイプで `ec2:DisassociateVerifiedAccessInstanceWebAcl`アクションを呼び出し、 を呼び出すアクセス許可が必要です AWS WAF `DisassociateWebACL`。

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "ec2:DisassociateVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

`GetWebACLForResource` のアクセス権限

このセクションでは、 AWS WAF アクション `GetWebACLForResource` を使用して保護対象リソースの保護パック (ウェブ ACL) を取得するために必要なアクセス許可の一覧を示します。

Amazon CloudFront ディストリビューションでは、このアクションの代わりに CloudFront アクション `GetDistributionConfig` を使用してください。詳細については、「Amazon CloudFront API リファレンス」の「GetDistributionConfig」を参照してください。

> **Note**
>
> GetWebACLForResource によって GetWebACL を呼び出すにはアクセス許可が必要です。このコンテキストでは、 は、 がGetWebACLForResource返す保護パック (ウェブ ACL) にアクセスするために必要なアクセス許可がアカウントにあることを検証するためにGetWebACLのみ AWS WAF 使用します。を呼び出すとGetWebACLForResource、アカウントが resource wafv2:GetWebACLに対して実行する権限がないことを示すエラーが表示されることがあります。このタイプのエラーは AWS CloudTrail イベント履歴に追加 AWS WAF されません。

Amazon API Gateway REST API

保護パック (ウェブ ACL) GetWebACL の と を呼び AWS WAF GetWebACLForResource出すアクセス許可が必要です。

```
{
    "Sid": "GetWebACLForResource",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
}
```

Application Load Balancer

古いアクセス許可の設定

保護パック (ウェブ ACL) GetWebACL の と を呼び AWS WAF GetWebACLForResource出すアクセス許可が必要です。

```
{
    "Sid": "GetWebACLForResource",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
```

```
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
}
```

新しいアクセス許可の設定

保護パック (ウェブ ACL) GetWebACL の と を呼び AWS WAF GetWebACLForResource出すアクセス許可が必要です。また、 を呼び出すには アクセス許可も必要ですelasticloadbalancing:GetLoadBalancerWebACL。

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
   "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "elasticloadbalancing:GetLoadBalancerWebACL"
    ],
    "Resource": [
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
    ]
}
```

AWS AppSync GraphQL API

古いアクセス許可の設定

保護パック (ウェブ ACL) GetWebACL の と を呼び AWS WAF GetWebACLForResource出すアクセス許可が必要です。

```
{
```

```
    "Sid": "GetWebACLForResource",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
}
```

新しいアクセス許可の設定

保護パック (ウェブ ACL) GetWebACL の と を呼び AWS WAF GetWebACLForResource出すアクセス許可が必要です。また、 を呼び出すには アクセス許可も必要ですappsync:GetWebACLForResource。

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
   "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "appsync:GetWebACLForResource"
    ],
    "Resource": [
        "arn:aws:appsync:*:account-id:apis/*"
    ]
}
```

Amazon Cognito ユーザープール

ユーザープールリソースタイプで Amazon Cognito GetWebACLForResourceアクションを呼び出し、 と を呼び AWS WAF GetWebACLForResource出すアクセス許可が必要ですGetWebACL。

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:GetWebACLForResource"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner サービス

App Runner サービスリソースタイプで App Runner `DescribeWebAclForService`アクションを呼び出し、 `GetWebACLForResource` と を呼び AWS WAF 出すアクセス許可が必要です`GetWebACL`。

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
```

```
            "apprunner:DescribeWebAclForService"
        ],
        "Resource": [
            "arn:aws:apprunner:*:account-id:service/*/*"
        ]
}
```

Amazon Bedrock AgentCore Gateway

Bedrock AgentCore Gateway リソースタイプで bedrock-agentcore:GatewayGetWebACLForResourceアクションを呼び出し、ウェブ ACL GetWebACLで および を呼び AWS WAF GetWebACLForResource出すアクセス許可が必要です。

```
{
  "Sid": "GetWebACLForResource1",
  "Effect": "Allow",
  "Action": [
    "wafv2:GetWebACLForResource",
    "wafv2:GetWebACL"
  ],
  "Resource": [
    "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
  ]
},
{
  "Sid": "GetWebACLForResource2",
  "Effect": "Allow",
  "Action": [
    "bedrock-agentcore:GatewayGetWebACLForResource"
  ],
  "Resource": [
    "arn:aws:bedrock-agentcore:*:account-id:gateway/*"
  ]
}
```

AWS Verified Access インスタンス

Verified Access インスタンスリソースタイプで ec2:GetVerifiedAccessInstanceWebAclアクションを呼び出し、 と を呼び AWS WAF GetWebACLForResource出すアクセス許可が必要ですGetWebACL。

```
{
```

```
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "ec2:GetVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

`ListResourcesForWebACL` のアクセス権限

このセクションには、 AWS WAF アクション `ListResourcesForWebACL` を使用して保護パック (ウェブ ACL) の保護対象リソースのリストを取得するために必要なアクセス許可の一覧が記載されています。

Amazon CloudFront ディストリビューションでは、このアクションの代わりに CloudFront アクション `ListDistributionsByWebACLId` を使用してください。詳細については、「Amazon CloudFront API リファレンス」の「ListDistributionsByWebACLId」を参照してください。

Amazon API Gateway REST API

ウェブ ACL の を呼び AWS WAF `ListResourcesForWebACL`出すアクセス許可が必要です。

```
{
    "Sid": "ListResourcesForWebACL",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
```

```
    ]
}
```

Application Load Balancer

古いアクセス許可の設定

保護パック (ウェブ ACL) の を呼び AWS WAF `ListResourcesForWebACL`出すアクセス許可が必要です。

```
{
    "Sid": "ListWebACLForResource",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
}
```

新しいアクセス許可の設定

保護パック (ウェブ ACL) の を呼び AWS WAF `ListResourcesForWebACL`出すアクセス許可が必要です。また、 を呼び出すには アクセス許可も必要です`elasticloadbalancing:DescribeWebACLAssociation`。

```
{
    "Sid": "ListResourcesForWebACL",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL",
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
   "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "elasticloadbalancing:DescribeWebACLAssociation"
```

```
    ],
    "Resource": "*"
}
```

AWS AppSync GraphQL API

古いアクセス許可の設定

保護パック (ウェブ ACL) の を呼び AWS WAF `ListResourcesForWebACL`出すアクセス許可が必要です。

```
{
    "Sid": "ListResourcesForWebACL",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL",
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
}
```

新しいアクセス許可の設定

保護パック (ウェブ ACL) の を呼び AWS WAF `ListResourcesForWebACL`出すアクセス許可が必要です。また、 を呼び出すには アクセス許可も必要です`appsync:ListResourcesForWebACL`。

```
{
    "Sid": "ListResourcesForWebACL",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "appsync:ListResourcesForWebACL"
    ],
```

```
    "Resource": "*"
}
```

Amazon Cognito ユーザープール

ユーザープールリソースタイプで Amazon Cognito `ListResourcesForWebACL` アクションを呼び出し、 AWS WAF `ListResourcesForWebACL` を呼び出すためのアクセス許可が必要です。

```
{
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner サービス

App Runner サービスリソースタイプで App Runner `ListAssociatedServicesForWebAcl`アクションを呼び出し、 を呼び出すアクセス許可が必要です AWS WAF `ListResourcesForWebACL`。

```
{
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
```

```
    ]
},
{
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:ListAssociatedServicesForWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

Amazon Bedrock AgentCore Gateway

bedrock-agentcore:GatewayListResourcesForWebACL アクションを呼び出し、ウェブ ACL を呼び出す AWS WAF ListResourcesForWebACLアクセス許可が必要です。

```
{
  "Sid": "ListResourcesForWebACL",
  "Effect": "Allow",
  "Action": [
    "wafv2:ListResourcesForWebACL"
  ],
  "Resource": [
    "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
  ]
},
{
  "Sid": "ListResourcesForWebACL2",
  "Effect": "Allow",
  "Action": [
    "bedrock-agentcore:GatewayListResourcesForWebACL"
  ],
  "Resource": "*"
}
```

AWS Verified Access インスタンス

検証済みアクセス インスタンスのリソース タイプで ec2:DescribeVerifiedAccessInstanceWebAclAssociations アクションを呼び出すには、AWS WAF ListResourcesForWebACL を呼び出すためのアクセス許可が必要です。

```
{
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

のポリシーリソース AWS WAF

ポリシーリソースのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Resource JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。リソースレベルのアクセス許可をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

AWS WAF リソースタイプとその ARNsAWS WAF V2 で定義されるリソース」を参照してください。 各リソースの ARN を指定できるアクションについては、AWS WAF V2 で定義されるアクション」を参照してください。 AWS WAF リソースのサブセットへのアクセスを許可または拒否するには、ポリシーの resource要素にリソースの ARN を含めます。

リソースの AWS WAF wafv2 ARNs の形式は次のとおりです。

```
arn:partition:wafv2:region:account-id:scope/resource-type/resource-name/resource-id
```

ARN の仕様に関する一般情報については、「 Amazon Web Services 全般のリファレンス」の「Amazon リソースネーム (ARN)」を参照してください。

wafv2 リソースの ARN に固有の要件は以下の通りです。

- *region*: Amazon CloudFront ディストリビューションの保護に使用する AWS WAF リソースの場合は、これを に設定しますus-east-1。それ以外の場合は、保護されたリージョンリソースで使用している領域を設定します。
- *####*: Amazon CloudFront ディストリビューションglobalで使用するスコープ、または が AWS WAF サポートするリージョンリソースregionalで使用するスコープを に設定します。リージョンリソースは、Amazon API Gateway REST API、Application Load Balancer、 AWS AppSync GraphQL API、Amazon Cognito ユーザープール、 AWS App Runner サービス、Amazon Bedrock AgentCore Gateway、 AWS Verified Access インスタンスです。
- *#######*: 次の値のいずれかを指定します。webacl、rulegroup、ipset、regexpatternset、managedruleset。
- *resource-name*: AWS WAF リソースに付けた名前を指定、あるいは ARN の他の仕様を満たすすべてのリソースを示すワイルドカード (*) を指定します。リソース名とリソース ID のどちらかを指定するか、両方にワイルドカードを指定する必要があります。
- *resource-id*: AWS WAF リソースの ID を指定、あるいは ARN の他の仕様を満たすすべてのリソースを示すワイルドカード (*) を指定します。リソース名とリソース ID のどちらかを指定するか、両方にワイルドカードを指定する必要があります。

例えば、次の ARN は、リージョン us-west-1 におけるアカウント 111122223333 のリージョンレベルの範囲のすべての保護パック (ウェブ ACL) を指定します。

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

次の ARN は、リージョン us-east-1 のアカウント 111122223333 に対して、グローバルスコープを持つ MyIPManagementRuleGroup というルールグループを指定します。

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

AWS WAF アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいのアイデンティティベースのポリシーの例 AWS WAF。

AWS WAF向けのポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Condition 要素は、定義された基準に基づいてステートメントが実行される時期を指定します。イコールや未満などの条件演算子を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「グローバル条件コンテキストキー」を参照してください。

さらに、 は IAM ポリシーにきめ細かなフィルタリングを提供するために使用できる以下の条件キー AWS WAF をサポートしています。

- wafv2:LogDestinationResource

  この条件キーは、ログ記録の送信先の Amazon リソースネーム (ARN) 仕様を取得します。これは、REST API コール PutLoggingConfiguration を使用する際に、ログ送信先として指定する ARN です。

  ARN を明示的に指定し、ARN のフィルタリングを指定できます。次の例では、特定の位置とプレフィックスを持つ Amazon S3 バケット ARN のフィルタリングを指定します。

  ```
  "Condition": { "ArnLike": { "wafv2:LogDestinationResource": "arn:aws:s3:::aws-waf-logs-suffix/custom-prefix/*" } }
  ```

- wafv2:LogScope

  この条件キーは、文字列内のログ記録設定のソースを定義します。現在、これは常に のデフォルトに設定されています。これは Customer、ログ記録の送信先がユーザーによって所有および管理されていることを示します。

AWS WAF 条件キーのリストを確認するには、「サービス認可リファレンス」の AWS WAF V2 の条件キー」を参照してください。条件キーを使用できるアクションとリソースについては、AWS WAF V2 で定義されるアクション」を参照してください。

AWS WAF アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいのアイデンティティベースのポリシーの例 AWS WAF。

ACLs AWS WAF

ACL のサポート: なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするためのアクセス許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

を使用した ABAC AWS WAF

ABAC (ポリシー内のタグ) のサポート: 一部

属性ベースのアクセス制御 (ABAC) は、タグと呼ばれる属性に基づいてアクセス許可を定義する認可戦略です。IAM エンティティと AWS リソースにタグをアタッチし、プリンシパルのタグがリソースのタグと一致するときにオペレーションを許可するように ABAC ポリシーを設計できます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/`*`key-name`*、`aws:RequestTag/`*`key-name`*、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM ユーザーガイド」の「属性ベースのアクセス制御 (ABAC) を使用する」を参照してください。

での一時的な認証情報の使用 AWS WAF

一時的な認証情報のサポート: あり

一時的な認証情報は、 AWS リソースへの短期的なアクセスを提供し、フェデレーションまたはスイッチロールを使用する場合に自動的に作成されます。長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成 AWS することをお勧めします。詳細については、「IAM ユーザーガイド」の「IAM の一時的な認証情報」および「AWS のサービス と IAM との連携」を参照してください。

サービスの転送アクセスセッション AWS WAF

転送アクセスセッション (FAS) のサポート: あり

転送アクセスセッション (FAS) は、 を呼び出すプリンシパルのアクセス許可と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする を使用します。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

のサービスロール AWS WAF

サービスロールのサポート: あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、IAM ユーザーガイドの AWS のサービスに許可を委任するロールを作成するを参照してください。

> **Warning**
>
> サービスロールのアクセス許可を変更すると、 AWS WAF 機能が破損する可能性があります。 AWS WAF が指示する場合にのみ、サービスロールを編集します。

のサービスにリンクされたロール AWS WAF

サービスリンクロールのサポート: あり

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。

AWS WAF サービスにリンクされたロールの作成または管理の詳細については、「」を参照してくださいのサービスにリンクされたロールの使用 AWS WAF。

のアイデンティティベースのポリシーの例 AWS WAF

このセクションでは、アイデンティティベースのポリシーの例を示します AWS WAF。

デフォルトでは、 ユーザーおよびロールには、 AWS WAF リソースを作成または変更する権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。

これらのサンプルの JSON ポリシードキュメントを使用して IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーを作成する (コンソール)」を参照してください。

各リソースタイプの ARN の形式など AWS WAF、 で定義されるアクションとリソースタイプの詳細については、「サービス認可リファレンス」のAWS WAF V2 のアクション、リソース、および条件キー」を参照してください。 ARNs

トピック

- ポリシーに関するベストプラクティス
- AWS WAF コンソールの使用
- 自分の権限の表示をユーザーに許可する
- 、CloudFront AWS WAF、および CloudWatch への読み取り専用アクセスを付与する
- 、CloudFront AWS WAF、および CloudWatch へのフルアクセスを付与する
- 単一の へのアクセスを許可する AWS アカウント
- 単一の保護パック (ウェブ ACL) へのアクセスを付与する
- 保護パック (ウェブ ACL) およびルールグループに対して、CLI アクセス権を付与

ポリシーに関するベストプラクティス

ID ベースのポリシーは、アカウント内の AWS WAF リソースを作成、アクセス、または削除できるかどうかを決定します。これらのアクションでは、 AWS アカウントに費用が発生する場合があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、IAM ユーザーガイド の AWS マネージドポリシー または ジョブ機能のAWS マネージドポリシー を参照してください。

- 最小特権を適用する – IAM ポリシーでアクセス許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、IAM ユーザーガイド の IAM でのポリシーとアクセス許可 を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。たとえば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用されている場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます CloudFormation。詳細については、IAM ユーザーガイド の IAM JSON ポリシー要素:条件 を参照してください。
- IAM アクセスアナライザー を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM アクセスアナライザー は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイド の IAM Access Analyzer でポリシーを検証する を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイド の MFA を使用した安全な API アクセス を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイド の IAM でのセキュリティのベストプラクティス を参照してください。

AWS WAF コンソールの使用

AWS WAF コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 の AWS WAF リソースの詳細を一覧表示および表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

ユーザーとロールが AWS WAF コンソールを使用できるようにするには、少なくとも AWS WAF `AWSWAFConsoleReadOnlyAccess` AWS 管理ポリシーをエンティティにアタッチします。このマネージドポリシーの情報については、「AWS マネージドポリシー: AWSWAFConsoleReadOnlyAccess」を参照してください。マネージドポリシーをユーザーにアタッチする方法の詳細については、「IAM ユーザーガイド」の「Adding permissions to a user」(ユーザーに許可の追加) を参照してください。

自分の権限の表示をユーザーに許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

、CloudFront AWS WAF、および CloudWatch への読み取り専用アクセスを付与する

次のポリシーは、 AWS WAF リソース、Amazon CloudFront ウェブディストリビューション、および Amazon CloudWatch メトリクスへの読み取り専用アクセスをユーザーに付与します。これは、AWS WAF 条件、ルール、保護パック (ウェブ ACLs) で設定を表示し、保護パック (ウェブ ACL) に関連付けられているディストリビューションを確認し、CloudWatch でメトリクスとリクエストのサンプルを監視するアクセス許可が必要なユーザーに役立ちます。これらのユーザーは、 AWS WAF リソースを作成、更新、または削除することはできません。

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Action": [
               "wafv2:Get*",
               "wafv2:List*",
               "cloudfront:GetDistribution",
               "cloudfront:GetDistributionConfig",
               "cloudfront:ListDistributions",
               "cloudfront:ListDistributionsByWebACLId",
               "cloudfront:ListDistributionTenantsByCustomization",
               "cloudfront:ListDistributionTenants",
               "cloudfront:GetDistributionTenant",
               "cloudwatch:GetMetricData",
               "cloudwatch:ListMetrics",
               "cloudwatch:GetMetricStatistics",
               "ec2:DescribeRegions",
               "pricingplanmanager:GetSubscription",
               "pricingplanmanager:ListSubscriptions",
               "route53:ListHostedZones",
               "route53:GetHostedZone"
           ],
           "Effect": "Allow",
           "Resource": "*"
       }
   ]
}
```

、CloudFront AWS WAF、および CloudWatch へのフルアクセスを付与する

次のポリシーでは、ユーザーは任意の AWS WAF オペレーションを実行し、CloudFront ウェブディストリビューションに対して任意のオペレーションを実行し、CloudWatch でメトリクスとリクエストのサンプルを監視できます。これは、 AWS WAF 管理者であるユーザーにとって便利です。

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Action": [
               "wafv2:*",
               "cloudfront:CreateDistribution",
               "cloudfront:ListDistributions",
               "cloudfront:ListDistributionsByWebACLId",
               "cloudfront:UpdateDistribution",
               "cloudfront:GetDistributionConfig",
               "cloudfront:GetDistribution",
               "cloudfront:DisassociateDistributionTenantWebACL",
               "cloudfront:DisassociateDistributionWebACL",
               "cloudfront:AssociateDistributionTenantWebACL",
               "cloudfront:AssociateDistributionWebACL",
               "cloudfront:ListDistributionTenantsByCustomization",
               "cloudfront:ListDistributionTenants",
               "cloudfront:DeleteDistribution",
               "cloudfront:GetDistributionTenant",
               "cloudfront:DeleteDistributionTenant",
               "cloudwatch:GetMetricData",
               "cloudwatch:ListMetrics",
               "cloudwatch:GetMetricStatistics",
               "ec2:DescribeRegions",
               "pricingplanmanager:GetSubscription",
               "pricingplanmanager:ListSubscriptions",
               "pricingplanmanager:UpdateSubscription",
               "pricingplanmanager:CancelSubscription",
               "pricingplanmanager:CancelSubscriptionChange",
               "pricingplanmanager:AssociateResourcesToSubscription",
               "pricingplanmanager:DisassociateResourcesFromSubscription",
               "route53:ListHostedZones",
               "route53:GetHostedZone"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

管理者許可を持つユーザーに対しては多要素認証 (MFA) を設定することを強くお勧めします。詳細については、「IAM ユーザーガイド」の「AWSでの多要素認証 (MFA) デバイスの使用」を参照してください。

単一の へのアクセスを許可する AWS アカウント

このポリシーは、アカウント 444455556666 に次の許可を付与します。

- すべての AWS WAF オペレーションとリソースへのフルアクセス。
- 保護パック (ウェブ ACL) と CloudFront ディストリビューションを関連付けるための、すべての CloudFront ディストリビューションへの読み取りおよび更新アクセス。
- すべての CloudWatch メトリクスとメトリクス統計への読み取りアクセスにより、 AWS WAF コンソールで CloudWatch データおよびリクエストのサンプルを表示できます。

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "wafv2:*"
         ],
         "Resource": [
            "arn:aws:wafv2:us-east-1:444455556666:*"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "cloudfront:GetDistribution",
```

```
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionsByWebACLId",
            "cloudfront:UpdateDistribution",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics",
            "ec2:DescribeRegions"
         ],
         "Resource": [
            "*"
         ]
      }
   ]
}
```

単一の保護パック (ウェブ ACL) へのアクセスを付与する

次のポリシーでは、ユーザーは、アカウント 内の特定の保護パック (ウェブ ACL) で コンソールを介して任意の AWS WAF オペレーションを実行できます444455556666。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wafv2:*"
            ],
            "Resource": [
                "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example"
            ]
        },
        {
            "Sid": "consoleAccess",
            "Effect": "Allow",
            "Action": [
                "wafv2:ListWebACLs",
                "ec2:DescribeRegions"
```

```
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

保護パック (ウェブ ACL) およびルールグループに対して、CLI アクセス権を付与

次のポリシーでは、ユーザーは、アカウント 内の特定の保護パック (ウェブ ACL) と特定のルールグループに対して CLI を介して任意の AWS WAF オペレーションを実行できます444455556666。

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "wafv2:*"
         ],
         "Resource": [
        "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example",
        "arn:aws:wafv2:us-east-1:444455556666:regional/rulegroup/
test123rulegroup/555555555-6666-1234-abcd-00d11example"
         ]
      }
   ]
}
```

次のポリシーでは、ユーザーは、アカウント 内の特定の保護パック (ウェブ ACL) で コンソールを介して任意の AWS WAF オペレーションを実行できます444455556666。

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wafv2:*"
            ],
            "Resource": [
                "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example"
            ]
        },
        {
            "Sid": "consoleAccess",
            "Effect": "Allow",
            "Action": [
                "wafv2:ListWebACLs",
                "ec2:DescribeRegions"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS の 管理ポリシー AWS WAF

このセクションでは、 の AWS 管理ポリシーを使用する方法について説明します AWS WAF。

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できるように、多くの一般的なユースケースにアクセス許可を付与するように設計されています。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS 管理ポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) に影響します。 AWS は、新しい が起動されるか、新しい API オペ

レーション AWS のサービス が既存のサービスで使用できるようになったときに、 AWS 管理ポリシーを更新する可能性が高くなります。

詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

AWS マネージドポリシー: AWSWAFReadOnlyAccess

このポリシーは、Amazon CloudFront、Amazon API Gateway、Application Load Balancer、Amazon Cognito、、 AWS AppSync Amazon AWS App Runner AWS Amplify Amazon CloudWatch、Amazon Bedrock AgentCore Gateway、 AWS Verified Access などの統合サービスの AWS WAF リソースとリソースにユーザーがアクセスできるようにする読み取り専用アクセス許可を付与します。このポリシーを IAM ID にアタッチできます。 は、ユーザーに代わって がアクションを実行できるようにするサービスロール AWS WAF にもこのポリシー AWS WAF をアタッチします。

このポリシーの詳細については、IAM コンソールで「AWSWAFReadOnlyAccess」を参照してください。

AWS マネージドポリシー: AWSWAFFullAccess

このポリシーは、Amazon CloudFront、Amazon API Gateway、Application Load Balancer、、 AWS AppSync Amazon Cognito、 AWS App Runner、 AWS Amplify Amazon CloudWatch、Amazon Bedrock AgentCore Gateway、 AWS Verified Access などの統合サービスの AWS WAF リソースとリソースへのフルアクセスを許可します。このポリシーを IAM ID にアタッチできます。 は、ユーザーに代わって がアクションを実行できるようにするサービスロール AWS WAF にもこのポリシー AWS WAF をアタッチします。

このポリシーの詳細については、IAM コンソールで「AWSWAFFullAccess」を参照してください。

AWS マネージドポリシー: AWSWAFConsoleReadOnlyAccess

このポリシーは、Amazon CloudFront、Amazon API Gateway、Application Load Balancer、Amazon Cognito、 AWS AppSync、Amazon AWS App Runner AWS Amplify Amazon CloudWatch、Amazon Bedrock AgentCore Gateway、 AWS Verified Access などの AWS WAF 統合サービスの および リソースを含む読み取り専用アクセス許可を AWS WAF コンソールに付与します。 Amazon Cognito このポリシーは IAM アイデンティティにアタッチできます。

このポリシーの詳細については、IAM コンソールで「AWSWAFConsoleReadOnlyAccess」を参照してください。

AWS マネージドポリシー: AWSWAFConsoleFullAccess

このポリシーは、コンソールへのフルアクセスを許可します。 AWS WAF コンソールには、Amazon CloudFront、Amazon API Gateway、Application Load Balancer、 AWS AppSync Amazon Cognito、AWS App Runner、 AWS Amplify Amazon CloudWatch、Amazon Bedrock AgentCore Gateway、AWS Verified Access などの AWS WAF 統合サービスのリソースとリソースが含まれます。このポリシーを IAM ID にアタッチできます。 は、ユーザーに代わって がアクションを実行できるようにするサービスロール AWS WAF にもこのポリシー AWS WAF をアタッチします。

このポリシーの詳細については、IAM コンソールで「AWSWAFConsoleFullAccess」を参照してください。

AWS マネージドポリシー: WAFV2LoggingServiceRolePolicy

このポリシーにより、 AWS WAF は Amazon Data Firehose にログを書き込むことができます。このポリシーは、ログインを有効にした場合にのみ使用されます AWS WAF。このポリシーは、`AWSServiceRoleForWAFV2Logging` サービスにリンクされたロールにアタッチされます。サービスにリンクされたロールの詳細については、「のサービスにリンクされたロールの使用 AWS WAF」を参照してください。

このポリシーの詳細については、IAM コンソールで「WAFV2LoggingServiceRolePolicy」を参照してください。

AWS WAF AWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始 AWS WAF してからの の AWS 管理ポリシーの更新に関する詳細を表示します。このページの変更に関する自動アラートについては、 の AWS WAF ドキュメント履歴ページの RSS フィードにサブスクライブしてくださいドキュメント履歴。

ポリシー	変更点の説明	日付
`AWSWAFConsoleFullAccess` このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS コンソール	CloudFront 料金プランに次のアクセス許可を追加しました。詳細については、「」を参照してください。CloudFront 定額料金プラン AWS WAF での の使用	2025-11-18

ポリシー	変更点の説明	日付
リソースやその他の AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFConsoleFullAccess。	• pricingplanmanager:GetSubscription – に関連付けられた料金プランのサブスクリプション情報を取得するアクセス許可を付与します AWS アカウント • pricingplanmanager:ListSubscriptions – に関連付けられた料金プランサブスクリプションを一覧表示するアクセス許可を付与します AWS アカウント • pricingplanmanager:UpdateSubscription – に関連付けられた料金プランサブスクリプションを更新するアクセス許可を付与します AWS アカウント • pricingplanmanager:CancelSubscription – に関連付けられた料金プランサブスクリプションをキャンセルするアクセス許可を付与します AWS アカウント • pricingplanmanager:CancelSubscriptionChange – に関連付けられた料金プランのサブスクリプション変更をキャンセ	

ポリシー	変更点の説明	日付
	ルするアクセス許可を付与します AWS アカウント • `route53:ListHostedZones` – に関連付けられている Route 53 ホストゾーンを一覧表示するアクセス許可を付与します AWS アカウント • `route53:GetHostedZone` – に関連付けられている Route 53 ホストゾーンの詳細を表示するアクセス許可を付与します AWS アカウント • `cloudfront:GetDistribution` – に関連付けられている CloudFront ディストリビューションの詳細を表示するアクセス許可を付与します AWS アカウント	

ポリシー	変更点の説明	日付
AWSWAFConsoleReadOnlyAccess このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS コンソールリソースやその他の AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFConsoleReadOnlyAccess。	CloudFront 料金プランに次のアクセス許可を追加しました。詳細については、「」を参照してください。CloudFront 定額料金プラン AWS WAF での の使用 • pricingplanmanager:GetSubscription – に関連付けられた料金プランのサブスクリプション情報を取得するアクセス許可を付与します AWS アカウント • pricingplanmanager:ListSubscriptions – に関連付けられた料金プランサブスクリプションを一覧表示するアクセス許可を付与します AWS アカウント • route53:ListHostedZones – に関連付けられている Route 53 ホストゾーンを一覧表示するアクセス許可を付与します AWS アカウント • route53:GetHostedZone – に関連付けられている Route 53 ホストゾーンの詳細を表示するアクセス許可を付与します AWS アカウント	2025-11-18

ポリシー	変更点の説明	日付
	• `cloudfront:GetDistribution` – に関連付けられている CloudFront ディストリビューションの詳細を表示するアクセス許可を付与します AWS アカウント	

ポリシー	変更点の説明	日付
`AWSWAFConsoleReadOnlyAccess` このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS コンソールリソースやその他の AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFConsoleReadOnlyAccess。	以下のアクセス許可が更新されました。 • `apigateway:GET` – リソースの範囲を更新して、取得可能なリソースを Amazon API Gateway リソースのみに制限しました 以下の権限を追加しました。 AWS AppSync • `appsync:ListApis` – アカウント内の AWS AppSync APIsを取得するアクセス許可を付与します AWS Amazon CloudWatch • `logs:StartQuery` – 1 つ以上の Amazon CloudWatch Logs インサイトロググループのクエリを開始するアクセス許可を付与します • `logs:DescribeQueryDefinitions` – Amazon CloudWatch Logs インサイトクエリ定義のリストを取得し、 AWS またはソース AWS アカウントに保存するアクセス許可を付与します • `logs:GetQueryResults` – 指定された Amazon	2025-11-03

ポリシー	変更点の説明	日付
	CloudWatch Logs インサイトクエリから結果を取得するアクセス許可を付与します Amazon Data Firehose • `firehose:ListDeliveryStreams` – AWS アカウントの Firehose ストリームを取得するアクセス許可を付与します AWS の料金表 • `pricing:GetPriceListFileUrl` – から Price List ファイルを取得するために使用される URL を取得するアクセス許可を付与します AWS の料金表 • `pricing:ListPriceLists` – から Price List リファレンスのリストを取得するアクセス許可を付与します AWS の料金表 AWS Marketplace • `aws-marketplace:ViewSubscriptions` – AWS アカウントに関連付けられた AWS Marketplace ソフトウェアサブスクリプ	

ポリシー	変更点の説明	日付
	ションを表示するアクセス許可を付与します	

ポリシー	変更点の説明	日付
AWSWAFConsoleFullAccess このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS コンソールリソースやその他の AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFConsoleFullAccess。	以下のアクセス許可が更新されました。 • apigateway:GET – リソースの範囲を更新して、取得可能なリソースを Amazon API Gateway リソースのみに制限しました 以下の権限を追加しました。 AWS AppSync • appsync:ListApis – アカウント内の AWS AppSync APIsを取得するアクセス許可を付与します AWS Amazon CloudWatch • logs:StartQuery – 1 つ以上の Amazon CloudWatch Logs インサイトロググループのクエリを開始するアクセス許可を付与します • logs:DescribeQueryDefinitions – Amazon CloudWatch Logs インサイトクエリ定義のリストを取得し、 AWS またはソース AWS アカウントに保存するアクセス許可を付与します • logs:GetQueryResults – 指定された Amazon	2025-11-03

ポリシー	変更点の説明	日付
	CloudWatch Logs インサイトクエリから結果を取得するアクセス許可を付与します Amazon Data Firehose • `firehose:ListDeliveryStreams` – AWS アカウントの Firehose ストリームを取得するアクセス許可を付与します AWS の料金表 • `pricing:GetPriceListFileUrl` – から Price List ファイルを取得するために使用される URL を取得するアクセス許可を付与します AWS の料金表 • `pricing:ListPriceLists` – から Price List リファレンスのリストを取得するアクセス許可を付与します AWS の料金表 AWS Marketplace • `aws-marketplace:ViewSubscriptions` – AWS アカウントに関連付けられた AWS Marketplace ソフトウェアサブスクリプ	

ポリシー	変更点の説明	日付
	ションを表示するアクセス許可を付与します	
`AWSWAFFullAccess` このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFFullAccess。	に必要なアクセス許可 AssociateWebACL、DisassociateWebACL、GetWebACLForResource、および ListResourcesForWebACL を追加しました AWS Amplify。	2025-05-05
`AWSWAFReadOnlyAccess` このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS リソースを管理できます。 このポリシーの詳細については、IAM コンソールで「AWSWAFReadOnlyAccess」を参照してください。	に必要な GetWebACLForResource および ListResourcesForWebACL のアクセス許可を追加しました AWS Amplify。	2025-05-05

ポリシー	変更点の説明	日付
AWSWAFConsoleReadOnlyAccess このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS コンソールリソースやその他の AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFConsoleReadOnlyAccess。	以下の権限を追加しました。 Amplify • amplify:GetWebACLForResource – Amplify リソースに関連付けられた AWS WAF 保護パック (ウェブ ACL) を取得する許可を付与 • amplify:ListApps – の Amplify アプリを取得するアクセス許可を付与します AWS アカウント • amplify:ListResourcesForWebACL – AWS WAF 保護パック (ウェブ ACL) に関連付けられた Amplify アプリを取得するアクセス許可を付与します CloudFront • cloudfront:GetDistributionConfig – CloudFront ディストリビューションに関する設定情報を取得するアクセス許可を付与します • cloudfront:GetDistributionTenant – CloudFront ディストリビューションテナントに関	2025-05-05

ポリシー	変更点の説明	日付
	する情報を取得するアクセス許可を付与します • `cloudfront:ListDistributionTenants` – に関連付けられている CloudFront ディストリビューションテナントを一覧表示するアクセス許可を付与します AWS アカウント • `cloudfront:ListDistributionTenantsByCustomization` – に関連付けられたフィルタリングされた CloudFront ディストリビューションテナントを一覧表示するアクセス許可を付与します AWS アカウント	

ポリシー	変更点の説明	日付
AWSWAFConsoleFullAccess このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS コンソールリソースやその他の AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFConsoleFullAccess。	以下の権限を追加しました。 Amplify • amplify:AssociateWebACL – AWS WAF 保護パック (ウェブ ACL) を Amplify リソースに関連付けるアクセス許可を付与します • amplify:DisassociateWebACL – Amplify リソースから AWS WAF 保護パック (ウェブ ACL) の関連付けを解除するアクセス許可を付与します • amplify:GetWebACLForResource – Amplify リソースに関連付けられた AWS WAF 保護パック (ウェブ ACL) を取得する許可を付与 • amplify:ListApps – の Amplify アプリを取得するアクセス許可を付与します AWS アカウント • amplify:ListResourcesForWebACL – AWS WAF 保護パック (ウェブ ACL) に関連付けられた Amplify アプリを取得するアクセス許可を付与します	2025-05-05

ポリシー	変更点の説明	日付
	CloudFront • `cloudfront:AssociateDistributionTenantWebACL` – AWS WAF 保護パック (ウェブ ACL) を CloudFront ディストリビューションテナントに関連付けるアクセス許可を付与します • `cloudfront:AssociateDistributionWebACL` – AWS WAF 保護パック (ウェブ ACL) を CloudFront ディストリビューションに関連付けるアクセス許可を付与します • `cloudfront:DisassociateDistributionTenantWebACL` – AWS WAF 保護パック (ウェブ ACL) と CloudFront ディストリビューションテナントの関連付けを解除するアクセス許可を付与します • `cloudfront:DisassociateDistributionWebACL` – AWS WAF 保護パック (ウェブ ACL) と CloudFront ディストリビューションの関連付けを解除するアクセス許可を付与します	

ポリシー	変更点の説明	日付
	• `cloudfront:GetDistributionConfig` – CloudFront ディストリビューションに関する設定情報を取得するアクセス許可を付与します • `cloudfront:GetDistributionTenant` – CloudFront ディストリビューションテナントに関する情報を取得するアクセス許可を付与します • `cloudfront:ListDistributionTenants` – に関連付けられている CloudFront ディストリビューションテナントを一覧表示するアクセス許可を付与します AWS アカウント • `cloudfront:ListDistributionTenantsByCustomization` – に関連付けられたフィルタリングされた CloudFront ディストリビューションテナントを一覧表示するアクセス許可を付与します AWS アカウント	

ポリシー	変更点の説明	日付
`WAFV2LoggingServiceRolePolicy` このポリシーにより、AWS WAF は Amazon Data Firehose にログを書き込むことができます。これは、ログ記録を有効にする場合にのみ使用されます。 IAM コンソールの詳細: WAFV2LoggingServiceRolePolicy。	このポリシーがアタッチされているサービスにリンクされたロールのアクセス権限設定にステートメント ID (Sid) を追加しました。	2024-06-03
`AWSServiceRoleForWAFV2Logging` このサービスにリンクされたロールは、 が Amazon Data Firehose AWS WAF にログを書き込むことを許可するアクセス許可ポリシーを提供します。 IAM コンソールの詳細: AWSServiceRoleForWAFV2Logging。	アクセス権限設定にステートメント ID (Sid) を追加しました。	2024-06-03
AWS WAF 変更追跡への の追加	AWS WAF は、管理ポリシー `WAFV2LoggingServiceRolePolicy` とサービスにリンクされたロール の変更の追跡を開始しましたAWSServiceRoleForWAFV2Logging 。	2024-06-03

ポリシー	変更点の説明	日付
`AWSWAFFullAccess` このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFFullAccess。	保護できるリソースタイプに AWS Verified Access インスタンスを追加するアクセス許可を拡張しました AWS WAF。	2023-06-17
`AWSWAFReadOnlyAccess` このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS リソースを管理できます。 IAM コンソールの詳細: 「AWSWAFReadOnlyAccess」	保護できるリソースタイプに AWS Verified Access インスタンスを追加するアクセス許可を拡張しました AWS WAF。	2023-06-17
`AWSWAFConsoleFullAccess` このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS コンソールリソースやその他の AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFConsoleFullAccess。	保護できるリソースタイプに AWS Verified Access インスタンスを追加するアクセス許可を拡張しました AWS WAF。	2023-06-17

ポリシー	変更点の説明	日付
`AWSWAFConsoleReadOnlyAccess` このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS コンソールリソースやその他の AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFConsoleReadOnlyAccess。	保護できるリソースタイプに AWS Verified Access インスタンスを追加するアクセス許可を拡張しました AWS WAF。	2023-06-17
`AWSWAFFullAccess` このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFFullAccess。	AWS App Runner サービスのアクセス設定を修正するためのアクセス許可を拡張しました。	2023-06-06
`AWSWAFReadOnlyAccess` このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS リソースを管理できます。 IAM コンソールの詳細: 「AWSWAFReadOnlyAccess」	AWS App Runner サービスのアクセス設定を修正するためのアクセス許可を拡張しました。	2023-06-06

ポリシー	変更点の説明	日付
`AWSWAFConsoleFullAccess` このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS コンソールリソースやその他の AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFConsoleFullAccess。	AWS App Runner サービスのアクセス設定を修正するためのアクセス許可を拡張しました。	2023-06-06
`AWSWAFConsoleReadOnlyAccess` このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS コンソールリソースやその他の AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFConsoleReadOnlyAccess。	AWS App Runner サービスのアクセス設定を修正するためのアクセス許可を拡張しました。	2023-06-06

ポリシー	変更点の説明	日付
`AWSWAFFullAccess` このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFFullAccess。	保護できるリソースタイプに AWS App Runner サービスを追加するためのアクセス許可を拡張しました AWS WAF。	2023-03-30
`AWSWAFReadOnlyAccess` このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS リソースを管理できます。 IAM コンソールの詳細: 「AWSWAFReadOnlyAccess」	保護できるリソースタイプに AWS App Runner サービスを追加するためのアクセス許可を拡張しました AWS WAF。	2023-03-30
`AWSWAFConsoleFullAccess` このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS コンソールリソースやその他の AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFConsoleFullAccess。	保護できるリソースタイプに AWS App Runner サービスを追加するためのアクセス許可を拡張しました AWS WAF。	2023-03-30

ポリシー	変更点の説明	日付
`AWSWAFConsoleReadOnlyAccess` このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS コンソールリソースやその他の AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFConsoleReadOnlyAccess。	保護できるリソースタイプに AWS App Runner サービスを追加するためのアクセス許可を拡張しました AWS WAF。	2023-03-30
`AWSWAFFullAccess` このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFFullAccess。	保護できるリソースタイプに Amazon Cognito ユーザープールを追加するアクセス許可を拡張しました AWS WAF。	2022-08-25
`AWSWAFReadOnlyAccess` このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS リソースを管理できます。 IAM コンソールの詳細: 「AWSWAFReadOnlyAccess」	保護できるリソースタイプに Amazon Cognito ユーザープールを追加するアクセス許可を拡張しました AWS WAF。	2022-08-25

ポリシー	変更点の説明	日付
`AWSWAFConsoleFullAccess` このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS コンソールリソースやその他の AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFConsoleFullAccess。	保護できるリソースタイプに Amazon Cognito ユーザープールを追加するアクセス許可を拡張しました AWS WAF。	2022-08-25
`AWSWAFConsoleReadOnlyAccess` このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS コンソールリソースやその他の AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFConsoleReadOnlyAccess。	保護できるリソースタイプに Amazon Cognito ユーザープールを追加するアクセス許可を拡張しました AWS WAF。	2022-08-25

ポリシー	変更点の説明	日付
AWSWAFFullAccess このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFFullAccess。	Amazon Simple Storage Service (Amazon S3) と Amazon CloudWatch Logs のログ配信の許可設定を修正しました。この変更により、ログ記録設定中に発生していたアクセス拒否エラーが解決されます。保護パック (ウェブ ACL) トラフィックのログ記録の詳細については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。	2022-01-11
AWSWAFConsoleFullAccess このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS コンソールリソースやその他の AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFConsoleFullAccess。	Amazon Simple Storage Service (Amazon S3) と Amazon CloudWatch Logs のログ配信の許可設定を修正しました。この変更により、ログ記録設定中に発生していたアクセスエラーが解決されます。保護パック (ウェブ ACL) トラフィックのログ記録の詳細については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。	2022-01-11

ポリシー	変更点の説明	日付
AWSWAFFullAccess このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFFullAccess。	拡張ログ記録オプション用の新しい許可を追加しました。 この変更により、追加のログ記録先 Amazon Simple Storage Service (Amazon S3) と Amazon CloudWatch Logs AWS WAF にアクセスできます。保護パック (ウェブ ACL) トラフィックのログ記録の詳細については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。	2021-11-15
AWSWAFConsoleFullAccess このポリシーにより AWS WAF 、 は AWS WAF および統合サービスでユーザーに代わって AWS コンソールリソースやその他の AWS リソースを管理できます。 IAM コンソールの詳細: AWSWAFConsoleFullAccess。	拡張ログ記録オプション用の新しい許可を追加しました。 この変更により、追加のログ記録先 Amazon Simple Storage Service (Amazon S3) と Amazon CloudWatch Logs AWS WAF にアクセスできます。保護パック (ウェブ ACL) トラフィックのログ記録の詳細については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。	2021-11-15
AWS WAF が変更の追跡を開始しました	AWS WAF は、 AWS 管理ポリシーの変更の追跡を開始しました。	2021-3-01

AWS WAF ID とアクセスのトラブルシューティング

以下の情報は、 および IAM の使用時に発生する可能性がある一般的な問題の診断 AWS WAF と修正に役立ちます。

トピック

- でアクションを実行する権限がありません AWS WAF
- iam:PassRole を実行する権限がありません
- 自分の 以外のユーザーに自分の AWS WAF リソース AWS アカウント へのアクセスを許可したい

でアクションを実行する権限がありません AWS WAF

アクションを実行する権限がないというエラーが表示された場合は、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要な wafv2:*GetWidget* アクセス許可を持っていない場合に発生するものです。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 wafv2:GetWidget on resource: my-example-widget
```

この場合、wafv2:*GetWidget* アクションを使用して *my-example-widget* リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

iam:PassRole を実行する権限がありません

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して AWS WAFにロールを渡すことができるようにする必要があります。

一部の AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、既存のロールをそのサービスに渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

以下の例のエラーは、marymajor という IAM ユーザーがコンソールを使用して AWS WAFでアクションを実行しようとする場合に発生します。ただし、このアクションをサービスが実行するには、

サービスロールから付与された権限が必要です。Mary には、ロールをサービスに渡すアクセス許可がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに `iam:PassRole` アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン資格情報を提供した担当者が管理者です。

自分の 以外のユーザーに自分の AWS WAF リソース AWS アカウント へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- がこれらの機能 AWS WAF をサポートしているかどうかを確認するには、「」を参照してくださいが IAM と AWS WAF 連携する方法。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイド の 外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可 を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

のサービスにリンクされたロールの使用 AWS WAF

このセクションでは、サービスにリンクされたロールを使用して、アカウント AWS 内のリソース AWS WAF へのアクセスを許可する方法について説明します。

AWS WAF は AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスにリンクされたロールは、直接リンクされた一意のタイプの IAM ロールです AWS WAF。サービスにリンクされたロールは によって事前定義 AWS WAF されており、サービスがユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、 の設定 AWS WAF が簡単になります。 は、サービスにリンクされたロールのアクセス許可 AWS WAF を定義し、特に定義されている場合を除き、 のみがその ロールを引き受け AWS WAF ることができます。定義された許可には、信頼ポリシーと許可ポリシーが含まれます。この許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスにリンクされたロールを削除するには、まずその ロールの関連リソースを削除します。これにより、 AWS WAF リソースへのアクセス許可が誤って削除されないため、リソースが保護されます。

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連携するAWS サービス」を参照して、サービスにリンクされたロール列がはいになっているサービスを見つけてください。サービスにリンクされた役割に関するドキュメントをサービスで表示するには[はい] リンクを選択してください。

のサービスにリンクされたロールのアクセス許可 AWS WAF

AWS WAF は、サービスにリンクされたロールAWSServiceRoleForWAFV2Loggingを使用して Amazon Data Firehose にログを書き込みます。このロールは、ログインを有効にした場合にのみ使用されます AWS WAF。ログ作成の詳細については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。

このサービスにリンクされたロールは、 AWS マネージドポリシー にアタッチされますWAFV2LoggingServiceRolePolicy。管理ポリシーの詳細については、「AWS マネージドポリシー: WAFV2LoggingServiceRolePolicy」を参照してください。

AWSServiceRoleForWAFV2Logging サービスにリンクされたロールは、ロール wafv2.amazonaws.com を引き受けるためにサービスを信頼します。

ロールのアクセス許可ポリシーにより AWS WAF 、 は指定されたリソースに対して次のアクションを実行できます。

- Amazon Data Firehose のアクション: aws-waf-logs- で始まる名前を持つ PutRecord および PutRecordBatch は Firehose データストリームリソースに対するアクション。例えば、aws-waf-logs-us-east-2-analytics。
- AWS Organizations アクション: Organizations 組織のリソースDescribeOrganization。
- AWS Key Management Service アクション: GenerateDataKeyおよび Decryptを使用して、Amazon Data Firehose がカスタマーマネージド AWS KMS キーを使用してデータを暗号化できるようにします。

IAM コンソールのサービスにリンクされたロール全体を参照してください: AWSServiceRoleForWAFV2Logging。

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するにはアクセス許可を設定する必要があります。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの許可」を参照してください。

のサービスにリンクされたロールの作成 AWS WAF

サービスリンクロールを手動で作成する必要はありません。で AWS WAF ログ記録を有効にするか AWS マネジメントコンソール、 AWS WAF CLI または AWS WAF API でPutLoggingConfigurationリクエストを行うと、 によってサービスにリンクされたロールが自動的に AWS WAF 作成されます。

ログ記録を有効化するためには、iam:CreateServiceLinkedRole 許可が必要です。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は同じ方法でアカウントにロールを再作成できます。 AWS WAF ログ記録を有効にすると、 によってサービスにリンクされたロールが再度 AWS WAF 作成されます。

のサービスにリンクされたロールの編集 AWS WAF

AWS WAF では、AWSServiceRoleForWAFV2Loggingサービスにリンクされたロールを編集することはできません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロール記述の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

のサービスにリンクされたロールの削除 AWS WAF

サービスリンクロールを必要とする機能やサービスが不要になった場合は、ロールを削除することをお勧めします。そうすることで、積極的にモニタリングまたは保守されていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

> **Note**
>
> リソースを削除しようとしたときに AWS WAF サービスがロールを使用している場合は、削除が失敗する可能性があります。失敗した場合は数分待ってから操作を再試行してください。

で使用される AWS WAF リソースを削除するには **`AWSServiceRoleForWAFV2Logging`**

1. AWS WAF コンソールで、すべてのウェブ ACL からログ記録を削除します。詳細については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。
2. API または CLI を使用して、ログ記録が有効化されている各ウェブ ACL に `DeleteLoggingConfiguration` リクエストを送信します。詳細については、「AWS WAF API リファレンス」を参照してください。

IAM を使用して、サービスにリンクされたロールを手動で削除するには

`AWSServiceRoleForWAFV2Logging` サービスにリンクされたロールを削除するには、IAM コンソール、IAM CLI、または IAM API を使用します。詳細については、IAM ユーザーガイドの「サービスにリンクされたロールの削除」を参照してください。

AWS WAF サービスにリンクされたロールでサポートされているリージョン

AWS WAF は、サービスが利用可能なすべてのリージョンでサービスにリンクされたロールの使用をサポートします。詳細については、「AWS WAF エンドポイントとクォータ」を参照してください。

でのログ記録とモニタリング AWS WAF

このセクションでは、 でイベントをモニタリングおよび応答するための AWS ツールを使用する方法について説明します AWS WAF。

モニタリングは、 および AWS WAF AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、 AWS ソリューションのすべての部分からモニタリングデータを収集する必要があります。 には、 AWS WAF リソースをモニタリングし、潜在的なイベントに対応するための複数のツール AWS が用意されています。

Amazon CloudWatch アラーム

Amazon CloudWatch アラームを使用して、指定した期間にわたって 1 つのメトリクスを確認します。メトリクスが指定されたしきい値を超えると、CloudWatch は Amazon SNS トピックまたは AWS Auto Scaling ポリシーに通知を送信します。詳細については、「Amazon CloudWatch によるモニタリング」を参照してください。

AWS CloudTrail ログ

CloudTrail は、ユーザー、ロール、または AWS のサービスによって実行されたアクションの記録を提供します AWS WAF。CloudTrail によって収集された情報を使用して、リクエストの実行元の IP アドレス AWS WAF、リクエストの実行者、リクエストの実行日時などの詳細を確認できます。詳細については、「での AWS CloudTrail API コールのログ記録」を参照してください。

AWS WAF 保護パック (ウェブ ACL) トラフィックのログ記録

AWS WAF は、保護パック (ウェブ ACLs) が分析するトラフィックのログ記録を提供します。ログには、保護された AWS リソースからリクエスト AWS WAF を受信した時間、リクエストに関する詳細情報、リクエストが一致したルールのアクション設定などの情報が含まれます。詳細については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。

でのコンプライアンスの検証 AWS WAF

このセクションでは、 を使用する際のコンプライアンス責任について説明します AWS WAF。

新しい AWS サインアップエクスペリエンスは、規制されたワークロード向けには設計されていません。新しい AWS サインアップエクスペリエンスを使用しているが、規制対象のワークロード AWS に を使用する場合は、 AWS (アドバンスド) にサインアップするか、 AWS 環境の高度な機能をアクティブ化できます。

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、「コンプライアンスAWS のサービス プログラムによるスコープ」の「コンプライアンス」を参照して、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「Downloading Reports in AWS Artifact」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。を使用する際のコンプライアンス責任の詳細については AWS のサービス、AWS 「 セキュリティドキュメント」を参照してください。

でのレジリエンスの構築 AWS WAF

このセクションでは、 AWS アーキテクチャが のデータ冗長性をサポートする方法について説明します AWS WAF。

AWS グローバルインフラストラクチャは、 AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。 は、低レイテンシー、高スループット、高度に冗長なネットワークで接続された、物理的に分離および分離された複数のアベイラビリティーゾーン AWS リージョン を提供します。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断せずに、自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、およびスケーラビリティが優れています。

AWS リージョン およびアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

のインフラストラクチャセキュリティ AWS WAF

このセクションでは、 がサービストラフィックを AWS WAF 分離する方法について説明します。

マネージドサービスである AWS WAF は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して環境を AWS 設計するには、「Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

AWS が公開した API コールを使用して、ネットワーク AWS WAF 経由で にアクセスします。クライアントは以下をサポートする必要があります。

- Transport Layer Security (TLS)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

AWS WAF クォータ

> **Note**
>
> これは の最新バージョンです AWS WAF。 AWS WAF Classic については、「」を参照してくださいAWS WAF クラシック。

AWS WAF には、次のクォータが適用されます (以前は制限と呼ばれていました)。これらのクォータは、 が利用可能なすべてのリージョンで同じ AWS WAF です。各リージョンでは、これらのクォータが個別に適用されます。クォータは、リージョンにまたがって累積されません。

AWS WAF には、アカウントごとに保持できるエンティティの最大数に対するデフォルトのクォータがあります。このクォータの引き上げをリクエストできます。

リソース	1 リージョン、1 アカウントあたりのデフォルトのクォータ
保護パック (ウェブ ACL) の最大数	100
ルールグループの最大数	100
IP セットの最大数	100
保護パック (ウェブ ACL) ごとの 1 秒あたりの最大リクエスト数	100,000
保護パック (ウェブ ACL) またはルールグループあたりのカスタムリクエストヘッダーの最大数	100
保護パック (ウェブ ACL) またはルールグループあたりのカスタムレスポンスヘッダーの最大数	100
保護パック (ウェブ ACL) またはルールグループあたりのカスタムレスポンス本文の最大数	50
保護パック (ウェブ ACL) トークンドメインリストのトークンドメインの最大数	10

リソース	1 リージョン、1 アカウントあたりのデフォルトのクォータ
正規表現パターンセットの最大数	10
保護パック (ウェブ ACL) あたりの Application Load Balancer の関連付けの最大数	100
保護パックあたりの Amazon API Gateway REST API 関連付けの最大数 (ウェブ ACL)	100
保護パックあたりの Amazon Cognito ユーザープールの関連付けの最大数 (ウェブ ACL)	100
保護パックあたりの AWS AppSync GraphQL API 関連付けの最大数 (ウェブ ACL)	100
保護パックあたりの AWS App Runner サービス関連付けの最大数 (ウェブ ACL)	100
保護パックあたりの AWS Verified Access インスタンスの関連付けの最大数 (ウェブ ACL)	100
保護パックあたりの AWS Amplify 関連付けの最大数 (ウェブ ACL)	100
保護パックあたりの Amazon Bedrock AgentCore Gateway 関連付けの最大数 (ウェブ ACL)	100

CloudFront AWS WAF で に許可される 1 秒あたりの最大リクエスト数 (RPS) はCloudFront によって設定され、CloudFront デベロッパーガイド」で説明されています。

AWS WAF には、リージョンごとにアカウントごとに次のエンティティ設定に対する固定クォータがあります。これらのクォータは変更できません。

リソース	1 アカウント、1 リージョンあたりのクォータ
保護パック (ウェブ ACL) あたりの最大保護パック (ウェブ ACL) キャパシティーユニット (WCU)*	5,000
ルールグループあたりの最大 WCU	5,000
ルールグループあたりの参照ステートメントの最大数。ルールグループでは、参照ステートメントは IP セットまたは正規表現パターンセットを参照できます。	50
保護パック (ウェブ ACL) あたりの参照ステートメントの最大数。保護パック (ウェブ ACL) では、参照ステートメントはルールグループ、IP セット、または正規表現パターンセットを参照できます。	50
IP セットあたりの CIDR 表記の IP アドレスの最大数	10,000
保護パック (ウェブ ACL) あたりのレートベースのルールの最大数	10
ルールグループあたりのレートベースのルールの最大数	4
レートベースのルールに対して定義できる最小リクエスト率	10
レートベースのルールごとにレート制限できる一意の IP アドレスの最大数	10,000
文字列一致ステートメントの最大文字数	200
各正規表現パターンの最大文字数	200
正規表現パターンセットあたりの一意の正規表現パターンの最大数	10
Application Load Balancer と AWS AppSync 保護を検査できるウェブリクエストボディの最大サイズ	8 KB
Amazon Bedrock AgentCore Gateway 保護を検査できるウェブリクエストボディの最大サイズ	16 KB

リソース	1 アカウント、1 リージョンあたりのクォータ
CloudFront、API Gateway、Amazon Cognito、App Runner、Verified Access、Amazon Bedrock AgentCore Gateway 保護について検査できるウェブリクエストボディの最大サイズ**	64 KB
ルールステートメントあたりのテキスト変換の最大数	10
単一のカスタムレスポンス定義のカスタムレスポンス本文コンテンツの最大サイズ	4 KB
1 つのカスタムレスポンス定義のカスタムヘッダーの最大数	10
1 つのカスタムリクエスト定義のカスタムヘッダーの最大数	10
単一のルールグループまたは単一の保護パック (ウェブ ACL) 用のすべてのレスポンス本文コンテンツの最大合計サイズ	50 KB
1 つのルール内の地域一致国コードの最大数	50

*保護パック (ウェブ ACL) で 1,500 WCU を超える容量を使用すると、保護パック (ウェブ ACL) の基本料金を超えるコストが発生します。詳細については、「のウェブ ACL キャパシティユニット (WCUs) AWS WAF」と「AWS WAF 料金表」を参照してください。

**デフォルトでは、CloudFront、API Gateway、Amazon Cognito、App Runner、Verified Access、Amazon Bedrock AgentCore Gateway リソースのボディ検査制限は 16 KB に設定されていますが、保護パック (ウェブ ACL) 設定でこれらのリソースのいずれかに対して、リストされている最大値まで引き上げることができます。詳細については、「でのボディ検査の管理に関する考慮事項 AWS WAF」を参照してください。

AWS WAF には、リージョンごとのアカウントごとの呼び出しに対して次の固定クォータがあります。これらのクォータは、コンソール、CLI、 AWS CloudFormation、REST API、SDK など、利用可能な手段を通じてサービスへのコールの合計に適用されます。これらのクォータは変更できません。

コールタイプ	1 アカウント、1 リージョンあたりのクォータ
`AssociateWebACL` へのコールの最大数	2 秒あたり 1 回のリクエスト
`DisassociateWebACL` へのコールの最大数	2 秒あたり 1 回のリクエスト
`GetWebACLForResource` へのコールの最大数	1 秒あたり 1 回のリクエスト
`ListResourcesForWebACL` へのコールの最大数	1 秒あたり 1 回のリクエスト
`GetDecryptedAPIKey` へのコールの最大数	2 秒あたり 1 回のリクエスト
個々の `Get` または `List` アクションに対するコールの最大数 (他にクォータが定義されていない場合)	1 秒あたり 5 回のリクエスト
個々の `Create`、`Put`、または `Update` アクションへのコールの最大数 (他にクォータが定義されていない場合)	1 秒あたり 1 回のリクエスト

AWS WAF には、 の 1 つの組織内のすべてのアカウントによる呼び出しに対して次の固定クォータがあります AWS Organizations。これらのクォータは、コンソール、CLI、 AWS CloudFormation、REST API、SDK など、利用可能な手段を通じてサービスへのコールの合計に適用されます。これらのクォータは変更できません。

コールタイプ	1 つのリージョンの組織あたりの配分
組織内のすべてのアカウントから `ListResourcesForWebACL` への呼び出しの最大数。米国東部 (バージニア北部) (us-east-1)、米国西部 (オレゴン)	1 秒あたり 12 リクエスト

コールタイプ	1 つのリージョンの組織あたりの配分
(us-west-2)、欧州 (アイルランド) (eu-west-1) の任意の 1 つのリージョンで使用できます。	
このテーブルに異なるクォータがリストされていない 1 つのリージョンにおける、組織内のすべてのアカウントから `ListResourcesForWebACL` への呼び出しの最大数。	1 秒あたり 6 リクエスト

AWS WAF には、AI トラフィック収益化機能の次のクォータがあります。調整可能とマークされたクォータは、クォータ引き上げリクエストを通じて引き上げることができます。

[リソース]	デフォルトのクォータ	引き上げ可能
アカウントあたりの保護パック	25	はい
保護パックあたりの保護パック (ウェブ ACL)	10	[Yes (はい)]
保護パックあたりの料金階層	20	いいえ
保護パックあたりのコンテンツゾーン	50	はい
保護パックあたりの支払いプロバイダー	3	いいえ
リクエストあたりの最低料金	0.00001 USD (10^-5 USD)	いいえ
リクエストあたりの上限価格	100 USD	いいえ
アクセストークンの TTL 範囲	60 ~ 86400 秒	いいえ

AWS WAF Classic リソースの への移行 AWS WAF

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは、AWS WAF ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

このセクションでは、2019 年 11 月に AWS WAF AWS WAF リリースされた AWS WAF Classic から にルールと保護パック (ウェブ ACLs) を移行するためのガイダンスを提供します。 AWS WAF Classic を使用してルールや保護パック (ウェブ ACLs) などのリソースを作成した場合は、 AWS WAF Classic を使用してリソースを操作するか、この最新バージョンに移行する必要があります。

> **Warning**
>
> AWS WAF クラシックサポートは 2025 年 9 月 30 日に終了します。

移行作業を開始する前に、 AWS WAF 「」の「」を参照してくださいAWS WAF。

トピック

- に移行する理由 AWS WAF
- 移行に関する注意事項と制限事項
- 移行の仕組み
- AWS WAF Classic から への保護パック (ウェブ ACL) の移行 AWS WAF

に移行する理由 AWS WAF

の最新バージョン AWS WAF では、以前のバージョンよりも多くの改善が加えられていますが、慣れている概念と用語のほとんどは維持されています。

最新の AWS WAFの主な変更点を次に示します。移行を続行する前に、このリストを確認し、残りの AWS WAF ガイドをよく理解してください。

- AWS WAF Classic のサポートは 2025 年 9 月 30 日に終了します。
- AWS のマネージドルール AWS WAF – AWS マネージドルールを通じて利用できるルールグループは、一般的なウェブ脅威に対する保護を提供します。これらのルールグループのほとんどは、に無料で含まれています AWS WAF。詳細については、AWS マネージドルールのルールグループリスト「」およびブログ記事「 AWS マネージドルールの発表 AWS WAF」を参照してください。
- 新しい AWS WAF API – 新しい API では、単一の APIs セットを使用してすべての AWS WAF リソースを設定できます。リージョン別アプリケーションとグローバルアプリケーションを区別するために、新しい API には scope 設定が含まれています。API の詳細については、「AWS WAFV2 アクション」および「AWS WAFV2 データ型」を参照してください。

  APIs では、SDKs、CLIs、および AWS CloudFormation、 AWS WAF Classic は命名スキームを保持し、この最新バージョンの AWS WAF はv2、コンテキストに応じて、 V2または で参照されます。
- サービスクォータ (制限) の簡素化 – AWS WAF 保護パック (ウェブ ACL) ごとにより多くのルールを許可し、より長い正規表現パターンを表現できるようになりました。詳細については、「AWS WAF クォータ」を参照してください。
- コンピューティングニーズが容量制限を決定する – 保護パック (ウェブ ACLs) の制限は、保護パック (ウェブ ACL) 容量ユニット (WCUs) に基づくようになりました。 は、必要な運用容量に従ってルールの WCUs AWS WAF を計算します。保護パック (ウェブ ACL) の合計 WCU は、すべてのルールとルールグループからの WCU の合計に等しくなります。

  WCU の一般情報については、「の AWS WAF 仕組み」を参照してください。各ルールの WCU の使用量については、「でのルールステートメントの使用 AWS WAF」を参照してください。
- ドキュメントベースのルールの記述 – ルール、ルールグループ、保護パック (ウェブ ACL) を JSON 形式で記述および表現できるようになりました。個々の API コールを使用してさまざまな条件を作成し、その条件をルールに関連付ける必要がなくなりました。これにより、コードの記述方法と保守方法が大幅に簡素化されます。保護パック (ウェブ ACL) を表示しているときに、[保護パック (ウェブ ACL) を JSON としてダウンロード] を選択することで、コンソールから保護パッ

ク (ウェブ ACL) の JSON 形式にアクセスできます。独自のルールを作成する場合は、[Rule JSON editor] (ルール JSON エディタ) を選択することで、その JSON 表現にアクセスできます。

- ルールのネストと完全な論理オペレーションのサポート - 論理ルールステートメントとネストを使用して、複雑な結合ルールを記述できます。`[A AND NOT(B OR C)]` などのステートメントを作成できます。詳細については、「での論理ルールステートメントの使用 AWS WAF」を参照してください。
- レートベースのルールの改善 – の最新バージョンでは AWS WAF、ルールが評価する時間枠と、ルールがリクエストを集約する方法をカスタマイズできます。多数のウェブリクエスト特性を組み合わせて集計をカスタマイズできます。さらに、最新のレートベースのルールは、トラフィックの変化により迅速に対応します。詳細については、「でのレートベースのルールステートメントの使用 AWS WAF」を参照してください。
- IP セットに対する可変 CIDR 範囲のサポート - IP セット指定における IP 範囲の柔軟性が向上しました。IPv4 の場合、 は /1 AWS WAF をサポートします/32。IPv6 の場合、 は /1 AWS WAF をサポートします/128。IP セットの詳細については、「IP セット一致ルールステートメント」を参照してください。
- 連鎖可能なテキスト変換 – AWS WAF ウェブリクエストコンテンツを調べる前に、ウェブリクエストコンテンツに対して複数のテキスト変換を実行できます。詳細については、「でのテキスト変換の使用 AWS WAF」を参照してください。
- コンソールエクスペリエンスの向上 – 新しい AWS WAF コンソールは、ビジュアルルールビルダーとより直感的なコンソール設計を備えています。
- Firewall Manager AWS WAF ポリシーの拡張オプション – Firewall Manager による AWS WAF 保護パックの管理 (ウェブ ACLs) で、最初に AWS WAF 処理するルールグループのセットと、最後に AWS WAF 処理するルールグループのセットを作成できるようになりました。 AWS WAF ポリシーを適用すると、ローカルアカウントの所有者は、これら 2 つのセットの間に が AWS WAF 処理する独自のルールグループを追加できます。Firewall Manager の AWS WAF ポリシーの詳細については、「Firewall Manager での AWS WAF ポリシーの使用」を参照してください。
- AWS CloudFormation はすべてのルールステートメントタイプのサポート – AWS WAF の AWS CloudFormation は、 AWS WAF コンソールと API がサポートするすべてのルールステートメントタイプをサポートします。さらに、JSON 形式で記述したルールを YAML 形式に簡単に変換できます。

移行に関する注意事項と制限事項

移行では保護パック (ウェブ ACL) 設定のみが処理され、保護パック (ウェブ ACL) の移行では AWS WAF 、 Classic とまったく同じようにすべての設定が引き継がれるわけではありません。一部の設定項目では、 AWS WAF (v2) で手動設定が必要です。2 つのバージョン間で正確にマッピングされない点がいくつかあります。また、 AWS WAF (v2) で機能を設定する方法を決定する必要があります。保護パック (ウェブ ACL) の AWS リソースとの関連付けなどの一部の設定は、新しいバージョンでは最初は無効になっているため、準備ができたら追加できます。

次のリストでは、移行の注意事項と、対処が必要となる可能性があるステップについて説明します。この概要を使用して、移行を計画してください。後述する移行の詳細なステップでは、推奨される緩和ステップについて順を追って説明します。

- 単一アカウントの移行 – どのアカウントの AWS WAF Classic リソースも、同じアカウントの AWS WAF リソースにのみ移行できます。
- 保護パック (ウェブ ACL) 設定のみ - 移行では、保護パック (ウェブ ACL) と、保護パック (ウェブ ACL) が使用しているリソースのみが移行されます。移行されたウェブ ACL で使用されていないルールグループや IP セットなどのリソースを移行するには、 AWS WAF (v2) でリソースを手動で作成します。
- AWS Marketplace マネージドルールなし – 移行では、 AWS Marketplace 販売者からのマネージドルールは引き継がれません。一部の AWS Marketplace 販売者には、再度サブスクライブ AWS WAF できる同等の マネージドルールがあります。これを行う前に、 の最新バージョンで提供されている AWS マネージドルールを確認してください AWS WAF。これらの大部分は AWS WAF ユーザーには無料です。マネージドルールの詳細については、「でのマネージドルールグループの使用 AWS WAF」を参照してください。
- 保護パック (ウェブ ACL) の関連付けなし - 移行では、保護パック (ウェブ ACL) と保護されたリソース間の関連付けは引き継がれません。これは仕様です。本番環境のワークロードに影響を与えないようにするためのものです。すべて正しく移行されたことを検証したら、新しい保護パック (ウェブ ACL) をリソースに関連付けます。
- ログ記録無効 - 移行された保護パック (ウェブ ACL)L のログ記録は、デフォルトで無効になっています。これは仕様です。 AWS WAF Classic から に切り替える準備ができたら、ログ記録を有効にします AWS WAF。
- AWS Firewall Manager ルールグループなし – 移行では、Firewall Manager によって管理されるルールグループは処理されません。Firewall Manager によって管理されている保護パック (ウェブ ACL) を移行することはできますが、移行でルールグループは引き継がれません。このような保護

パック (ウェブ ACL) には、移行ツールを使用するのではなく、Firewall Manager で新しい AWS WAF のポリシーを再作成します。

> **Note**
>
> Firewall Manager が AWS WAF Classic 用に管理したルールグループは、Firewall Manager ルールグループでした。の新しいバージョンでは AWS WAF、ルールグループは AWS WAF ルールグループです。機能的には、これらは同じです。

- AWS WAF セキュリティオートメーションの注意 — AWS WAF セキュリティオートメーションの移行を試みないでください。移行では、オートメーションにより使用される可能性がある Lambda 関数が変換されません。代わりに、最新バージョンのオートメーションのデプロイを検討してください。詳細については、「AWS WAF セキュリティオートメーション」を参照してください。

移行の仕組み

複数の方法を使用してACLs AWS WAF Classic を から AWS WAF v2 に移行できます。移行を完了するには、次の手順に従います。

から v2 AWS WAF Classic AWS WAF に移行するには

1. AWS WAF Classic ウェブ ACLs を特定します。
   - AWS Health ダッシュボードでウェブ ACLs のリストを表示します。
   - AWS WAF Classic ウェブ ACL クリーンアップスクリプト を使用して、すべてのウェブ ACL とその関連付けのリストを取得します。これにより、どのウェブ ACL リソースを積極的に保護しているかを特定し、未使用のウェブ ACL を削除できます。
2. 個々のウェブ ACL:
   - 「AWS WAF デベロッパーガイド」の「移行プロセス」に従ってください。
   - 移行ウィザードを使用してウェブ AWS WAF Classic ACL を解析し、 AWS CloudFormation テンプレートを生成します。
   - 生成されたテンプレートを使用して同等の AWS WAF v2 ウェブ ACL を作成し、移行を完了します。
3. 複数の対象となるウェブ ACL:
   - AWS WAF 一括移行スクリプトを使用して、複数の適格な AWS WAF Classic ウェブ ACLs。

4. によって管理ACLs の場合 AWS Firewall Manager:

   - Firewall Manager ポリシーは、 AWS WAF Classic ポリシーで AWS WAF Classic ウェブ ACL を使用します。 ACLs 2022 年 1 月より前に作成された Shield Advanced ポリシーの場合、Firewall Manager は AWS WAF Classic ウェブ ACLs も使用します。v2 ウェブ ACLs AWS WAF を使用するには、これらのポリシーを移行する必要があります。

     Firewall Manager での AWS WAF Classic ウェブ ACLs移行 の指示に従います。

> **Important**
>
> リソースに関連付ける前に、移行された各ウェブ ACL を確認して、セキュリティ要件を満たしていることを確認することをお勧めします。

AWS WAF Classic から への保護パック (ウェブ ACL) の移行 AWS WAF

自動移行では、 AWS WAF Classic 保護パック (ウェブ ACL) 設定のほとんどが引き継がれ、手動で処理する必要があるものが残ります。

> **Note**
>
> 一部の保護設定は自動的に移行できず、 AWS WAF (v2) で手動設定が必要です。移行に関する注意事項と制限事項 のリストを参照してください。

保護パック (ウェブ ACL) を移行するためのステップの概要を次に示します。

1. 自動移行は、 AWS WAF Classic で何も変更または削除することなく、既存の保護パック (ウェブ ACL) に関連するすべてを読み込みます。ウェブ ACL と互換性のある関連リソースの表現を作成します AWS WAF。新しい保護パック (ウェブ ACL) の CloudFormation テンプレートを生成し、Amazon S3 バケットに保存します。
2. テンプレートを にデプロイして CloudFormation、 で保護パック (ウェブ ACL) と関連リソースを再作成します AWS WAF。
3. 保護パック (ウェブ ACL) を確認して手動で移行を完了し、新しい保護パック (ウェブ ACL) が最新の AWS WAFの機能を最大限に活用するようにします。
4. 保護されたリソースを新しい保護パック (ウェブ ACL) に手動で切り替えます。

トピック

- 保護パック (ウェブ ACL) の移行: 自動移行
- 保護パック (ウェブ ACL) の移行: 手動フォローアップ
- 保護パック (ウェブ ACL) の移行: その他の考慮事項
- 保護パック (ウェブ ACL): スイッチオーバー

保護パック (ウェブ ACL) の移行: 自動移行

保護パック (ウェブ ACL) 設定を AWS WAF Classic から に自動的に移行するには AWS WAF

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. AWS WAF Classic に切り替えを選択し、保護パック (ウェブ ACL) の設定を確認します。前のセクション「移行に関する注意事項と制限事項」で説明した注意事項と制限事項を考慮して、設定をメモしておきます。
3. 上部の情報ダイアログで、「保護パック (ウェブ ACL) を移行する」で始まる文を見つけて、移行ウィザード へのリンクを選択します。移行ウィザードが起動します。

   情報ダイアログが表示されない場合は、 AWS WAF Classic コンソールを起動してから閉じた可能性があります。ナビゲーションバーで、「新規に切り替える AWS WAF」を選択し、 AWS WAF 「クラシックに切り替える」を選択すると、情報ダイアログが再び表示されます。
4. 移行する保護パック (ウェブ ACL) を選択します。
5. [Migration configuration] (移行設定) では、テンプレートに使用する Amazon S3 バケットを指定します。生成する AWS CloudFormation テンプレートを保存するには、移行 API 用に適切に設定された Amazon S3 バケットが必要です。

   - バケットが暗号化されている場合、暗号化は Amazon S3 (SSE-S3) キーを使用する必要があります。移行では、 AWS Key Management Service (SSE-KMS) キーを使用した暗号化はサポートされていません。
   - バケット名の先頭は `aws-waf-migration-` にする必要があります。例えば、`aws-waf-migration-my-web-acl`。
   - バケットは、テンプレートをデプロイするリージョンに存在する必要があります。例えば、`us-west-2` の保護パック (ウェブ ACL) の場合、`us-west-2` で Amazon S3 バケットを使用し、テンプレートスタックを `us-west-2` にデプロイする必要があります。

6. S3 バケットポリシーの場合、[Auto apply the bucket policy required for migration] (移行に必要なバケットポリシーを自動的に適用する) を選択することをお勧めします。または、自分でバケットを管理する場合は、次のバケットポリシーを手動で適用する必要があります。

   - グローバル Amazon CloudFront アプリケーションの場合 (`waf`):

     JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "apiv2migration.waf.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>/AWSWAF/
<CUSTOMER_ACCOUNT_ID>/*"
        }
    ]
}
```

   - リージョンレベルの Amazon API Gateway または Application Load Balancer アプリケーションの場合 (`waf-regional`):

     JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "apiv2migration.waf-regional.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>/AWSWAF/
<CUSTOMER_ACCOUNT_ID>/*"
        }
    ]
```

```
}
```

7. [Choose how to handle rules that cannot be migrated] (移行できないルールの処理方法を選択してください) で、移行できないルールを除外するか、移行を停止するかを選択します。移行できないルールの詳細については、「移行に関する注意事項と制限事項」を参照してください。
8. [次へ] を選択します。
9. CloudFormation テンプレートの作成 で設定を確認し、 CloudFormation テンプレートの作成を開始する を選択して移行プロセスを開始します。保護パック (ウェブ ACL) の複雑さによっては、この処理に数分かかる場合があります。
10. CloudFormation スタックの作成と実行で移行を完了するには、 AWS CloudFormation コンソールに移動してテンプレートからスタックを作成し、新しい保護パック (ウェブ ACL) とそのリソースを作成できます。これを行うには、 CloudFormation スタックの作成を選択します。

自動移行プロセスが完了したら、手動でのフォローアップステップに進む準備が整います。「保護パック (ウェブ ACL) の移行: 手動フォローアップ」を参照してください。

保護パック (ウェブ ACL) の移行: 手動フォローアップ

自動移行が完了したら、新しく作成した保護パック (ウェブ ACL) を確認し、移行によって引き継がれないコンポーネントを入力します。次の手順では、移行によって処理されない保護パック (ウェブ ACL) 管理の側面について説明します。リストについては、「移行に関する注意事項と制限事項」を参照してください。

基本的な移行を完了するには - 手動ステップ

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/homev2 で AWS WAF コンソールを開きます。
2. コンソールは、 の最新バージョンを自動的に使用する必要があります AWS WAF。これを確認するには、ナビゲーションペインで、 AWS WAF 「クラシックに切り替える」オプションが表示されていることを確認します。新しい に切り替える AWS WAF が表示された場合は、それを選択して最新バージョンに切り替えます。
3. ナビゲーションペインで、[保護パック (ウェブ ACL)] を選択します。
4. [保護パック (ウェブ ACL)] ページで、作成したリージョンのリストで新しい保護パック (ウェブ ACL) を見つけます。保護パック (ウェブ ACL) の名前を選択して、保護パック (ウェブ ACL) の設定を表示します。

5. 以前の AWS WAF Classic ウェブ ACL に対して、新しい保護パック (ウェブ ACL) のすべての設定を確認します。デフォルトでは、ログ記録と保護されたリソースの関連付けは無効になっています。切り替えの準備ができたら有効にします。
6. AWS WAF Classic 保護パック (ウェブ ACL) にマネージドルールグループがある場合、ルールグループの包含は移行に引き継がれませんでした。マネージドルールグループを新しい保護パック (ウェブ ACL) に追加できます。で、新しいバージョンの で利用可能なマネージドルールのリストなど AWS WAF、 AWS マネージドルールグループに関する情報を確認しますでのマネージドルールグループの使用 AWS WAF。マネージドルールグループを追加するには、次の手順を実行します。

   a. 保護パック (ウェブ ACL) 設定ページで、保護パック (ウェブ ACL) ルール タブを選択します。
   b. [Add rules] (ルールの追加) を選択し、[Add managed rule groups] (マネージドルールグループの追加) を選択します。
   c. 選択したベンダーのリストを展開し、追加するルールグループを選択します。 AWS Marketplace 販売者の場合、ルールグループにサブスクライブする必要がある場合があります。保護パック (ウェブ ACL) でのマネージドルールグループの使用の詳細については、「でのマネージドルールグループの使用 AWS WAF」および「のルールとルールグループで保護パック (ウェブ ACLs) を使用する AWS WAF」を参照してください。

基本的な移行プロセスを完了したら、ニーズを見直して追加のオプションを検討することにより、新しい設定の効率が可能な限り高いことと、利用可能な最新のセキュリティオプションを使用していることを確認することをお勧めします。「保護パック (ウェブ ACL) の移行: その他の考慮事項」を参照してください。

保護パック (ウェブ ACL) の移行: その他の考慮事項

新しい保護パック (ウェブ ACL) を確認し、新しい で使用可能なオプションを検討 AWS WAF して、設定ができるだけ効率的であり、利用可能な最新のセキュリティオプションを使用していることを確認します。

その他の AWS マネージドルール

アプリケーションのセキュリティ体制を強化するために、追加の AWS マネージドルールを保護パック (ウェブ ACL) に実装することを検討してください。これらは追加料金 AWS WAF なしで に含まれます。 AWS マネージドルールには、次のタイプのルールグループがあります。

- ベースラインルールグループは、既知の不正な入力がアプリケーションに入らないようにしたり、管理ページへのアクセスを防ぐなど、さまざまな一般的な脅威に対して全般的な保護を提供します。
- ユースケース固有のルールグループは、多種多様なユースケースに対して段階的な保護を提供します。
- IP 評価レピュテーションリストは、クライアントの送信元 IP に基づく脅威インテリジェンスを提供します。

詳細については、「AWS の マネージドルール AWS WAF」を参照してください。

ルールの最適化とクリーンアップ

古いルールを再検討し、それらを書き換えたり、古いルールを削除して最適化することを検討してください。例えば、過去に OWASP Top 10 Web Application Vulnerabilities のテクニカルペーパーの AWS CloudFormation テンプレートをデプロイしたことがある場合は、と新しいホワイトペーパーを使用して AWS WAF OWASP Top 10 Web Application Vulnerabilities に備えてください。これを AWS マネージドルールに置き換えることを検討してください。ドキュメント内の概念は依然として適用可能であり、独自のルールの作成に役立つ場合がありますが、テンプレートによって作成されたルールは主に AWS マネージドルールに置き換えられています。

Amazon CloudWatch メトリクスおよびアラーム

Amazon CloudWatch メトリクスに再度アクセスして、必要に応じてアラームを設定します。移行では CloudWatch アラームが引き継がれないため、メトリクス名が目的のものとは異なる可能性があります。

アプリケーションチームとの確認

アプリケーションチームと協力して、セキュリティ体制を確認してください。アプリケーションによって頻繁に解析されるフィールドを調べ、それに応じて入力をサニタイズするルールを追加します。エッジケースをチェックし、アプリケーションのビジネスロジックがケースを処理できない場合にこれらのケースをキャッチするルールを追加します。

切り替えの計画

アプリケーションチームと切り替えのタイミングを計画します。古い保護パック (ウェブ ACL) の関連付けから新しいものへの切り替えは、リソースが保存されているすべての領域に反映されるまで、少し時間がかかる場合があります。伝播時間は、数秒から数分までかかります。この際、一部のリクエストは古い保護パック (ウェブ ACL) で処理される一方、他のものは新しい保護パック (ウェブ

ACL) で処理されます。リソースは切り替え作業を通して保護されますが、その過程中にリクエスト処理に一貫性がないことに気付く場合があります。

切り替えの準備ができたら、「保護パック (ウェブ ACL): スイッチオーバー」の手順に従います。

保護パック (ウェブ ACL): スイッチオーバー

新しい保護パック (ウェブ ACL) 設定を検証したら、 AWS WAF Classic 保護パック (ウェブ ACL) の代わりに使用を開始できます。

新しい AWS WAF 保護パックの使用を開始するには (ウェブ ACL)

1. 「」のガイダンスに従って、 AWS WAF 保護パック (ウェブ ACL) を保護対象のリソースに関連付けますAWS リソースとの保護の関連付けまたは関連付け解除。これにより、古い保護パック (ウェブ ACL) からリソースの関連付けが自動的に解除されます。

   切り替えは、伝播するために数秒から数分までかかります。この際、一部のリクエストは古いウェブ ACL で処理される可能性がある一方、他のものは新しい保護パック (ウェブ ACL) で処理される可能性があります。リソースは切り替え作業を通して保護されますが、終了するまでリクエスト処理に一貫性がないことに気付く場合があります。
2. 「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」のガイダンスに従って、新しい保護パック (ウェブ ACL) のログ記録を設定します。
3. (オプション) AWS WAF Classic 保護パック (ウェブ ACL) がリソースに関連付けられなくなった場合は、 AWS WAF Classic から完全に削除することを検討してください。詳細については、「ウェブ ACL の削除」を参照してください。

AWS WAF クラシック

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

AWS WAF Classic は、Amazon API Gateway API、Amazon CloudFront、または Application Load Balancer に転送される HTTP および HTTPS リクエストをモニタリングできるウェブアプリケーションファイアウォールです。 AWS WAF Classic では、コンテンツへのアクセスを制御することもできます。リクエストの送信元の IP アドレスやクエリ文字列の値などの、指定した条件に基づいて、API Gateway、CloudFront、または Application Load Balancer はリクエストされたコンテンツまたは HTTP 403 ステータスコード (Forbidden) (禁止) のリクエストのいずれかに対応します。リクエストがブロックされたときにカスタムエラーを返すように CloudFront を設定することもできます。

トピック

- AWS WAF Classic のセットアップ
- AWS WAF Classic の仕組み
- AWS WAF クラシック料金
- AWS WAF Classic の開始方法
- ウェブアクセスコントロールリスト (ウェブ ACL) の作成と設定
- で使用する AWS WAF Classic ルールグループの使用 AWS Firewall Manager
- AWS WAF Classic ルールを有効にする AWS Firewall Manager ための の開始方法
- チュートリアル: 階層ルールによる AWS Firewall Manager ポリシーの作成

- ウェブ ACL トラフィック情報のログ記録
- レートベースのルールごとにブロックされている IP アドレスの一覧表示
- AWS WAF Classic が Amazon CloudFront 機能と連携する方法
- AWS WAF Classic のセキュリティ
- AWS WAF クラシッククォータ

AWS WAF Classic のセットアップ

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、まだ最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

このトピックでは、 AWS WAF Classic を使用する準備をするためのユーザーアカウントの作成などの準備手順について説明します。これらに対しては請求されません。使用した AWS サービスに対してのみ課金されます。

> **Note**
>
> を初めて使用する場合は AWS WAF、 AWS WAF Classic のセットアップ手順を実行しないでください。代わりに、 の最新バージョンの手順に従います AWS WAFアカウントを設定してサービスを使用する。

これらのステップを完了したら、AWS WAF Classic の開始方法「」を参照して AWS WAF Classic の使用を続行します。

> **Note**
>
> AWS Shield Standard は AWS WAF Classic に含まれており、追加のセットアップは必要ありません。詳細については、「AWS Shield と Shield Advanced の仕組み」を参照してください。

AWS WAF Classic または AWS Shield Advanced を初めて使用する前に、このセクションの手順を完了してください。

トピック

- にサインアップする AWS アカウント
- ツールをダウンロード

にサインアップする AWS アカウント

の使用を開始するには AWS、 が必要です AWS アカウント。の作成の詳細については AWS アカウント、「 AWS アカウント管理 リファレンスガイド」の「 の開始方法 AWS アカウント」を参照してください。

ツールをダウンロード

には AWS WAF Classic のコンソール AWS マネジメントコンソール が含まれていますが、プログラムで AWS WAF Classic にアクセスする場合は、以下を参照してください。

- raw HTTP リクエストの組み立てなどの低レベルの詳細を処理せずに AWS WAF Classic API を呼び出す場合は、 AWS SDK を使用できます。 AWS SDKs は、 AWS WAF Classic およびその他の AWS サービスの機能をカプセル化する関数とデータ型を提供します。 AWS SDK をダウンロードするには、該当するページを参照してください。このページには、前提条件とインストール手順も含まれています。
  - Java
  - JavaScript
  - .NET
  - Node.js
  - PHP
  - Python

- Ruby

AWS SDKs「Amazon Web Services のツール」を参照してください。

- が SDK を提供し AWS ないプログラミング言語を使用している場合、 AWS WAF API リファレンスは AWS WAF Classic がサポートするオペレーションを文書化します。
- AWS Command Line Interface (AWS CLI) は AWS WAF Classic をサポートしています。 AWS CLI を使用すると、コマンドラインから複数の AWS サービスを制御したり、スクリプトを使用して自動化したりできます。詳細については、「AWS Command Line Interface」を参照してください。
- AWS Tools for Windows PowerShell は AWS WAF Classic をサポートしています。詳細については、「AWS Tools for PowerShell コマンドレットリファレンス」(Cmdlet リファレンス) を参照してください。

AWS WAF Classic の仕組み

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

AWS WAF Classic を使用して、API Gateway、Amazon CloudFront、または Application Load Balancer がウェブリクエストにどのように応答するかを制御します。まず、条件、ルール、ウェブアクセスコントロールリスト (ウェブ ACL) を作成します。条件を定義し、ルールに追加したら、ルールをウェブ ACL に結合します。

> **Note**
>
> AWS WAF Classic を使用して、Amazon Elastic Container Service (Amazon ECS) コンテナでホストされているアプリケーションを保護することもできます。Amazon ECS は、クラスターで Docker コンテナを簡単に実行、停止、管理できる非常にスケーラブルで高速なコンテナ管理サービスです。このオプションを使用するには、 AWS WAF Classic が有効な Application Load Balancer を使用して、サービスのタスク間で HTTP/HTTPS (レイヤー 7) トラフィックをルーティングおよび保護するように Amazon ECS を設定します。詳細については、「Amazon Elastic Container Service デベロッパーガイド」の「Service load balancing」(サービスのロードバランシング) のトピックを参照してください。

条件

条件では、ウェブリクエストで AWS WAF Classic が監視する基本的な特徴を定義します。

- 悪意のある可能性が高いスクリプト。攻撃者は、ウェブアプリケーションの脆弱性を悪用できるスクリプトを埋め込みます。これはクロスサイトスクリプティングと呼ばれます。
- リクエストの発生元の IP アドレスまたはアドレス範囲。
- リクエスト送信元の国または地理的場所。
- クエリ文字列など、リクエストの指定された部分の長さ。
- 悪意のある可能性が高い SQL コード。攻撃者は、ウェブリクエストに悪意のある SQL コードを埋め込むことで、データベースからデータを抽出しようとします。これは SQL インジェクションと呼ばれます。
- リクエストに表示される文字列。例えば、`User-Agent` ヘッダーに表示される値、またはクエリ文字列に表示されるテキスト文字列です。正規表現を使用してこれらの文字列を指定することもできます。

条件によっては、複数の値を指定できる場合があります。例えば、IP 条件では最大 10,000 個の IP アドレスまたは IP アドレス範囲を指定できます。

Rules

条件をルールに結合して、許可、ブロック、またはカウントするリクエストを正確にターゲットにします。 AWS WAF Classic には、次の 2 種類のルールがあります。

通常ルール

通常ルールでは、特定のリクエストを対象とするための条件のみが使用されます。例えば、攻撃者からの最近のリクエストに基づいて、次の条件を含むルールを作成できます。

- リクエストが 192.0.2.44 から発生した。
- リクエストの User-Agent ヘッダーに BadBot 値が含まれる。
- それらのクエリ文字列には、SQL などのコードが含まれる。

ルールに複数の条件をすべて含めると、この例のように AWS WAF Classic によってすべての条件に一致するリクエストが検索されます。つまり、これらの条件を AND で連結したことになります。

少なくとも 1 つの条件を通常ルールに追加します。条件のない通常のルールはどのリクエストにも一致しないため、ルールのアクション (許可、カウント、またはブロック) はトリガーされません。

レートベースのルール

レートベースのルールは、レート制限が追加された通常のルールに似ています。レートベースのルールは、ルールの条件を満たす IP アドレスから到着したリクエストをカウントします。IP アドレスからのリクエストが 5 分間でレート制限を超えた場合、ルールはアクションをトリガーできます。アクションがトリガーされるまで、1~2 分かかることがあります。

レートベースのルールの条件はオプションです。レートベースのルールに条件を追加しない場合、レート制限はすべての IP アドレスに適用されます。条件をレート制限と組み合わせると、レート制限は条件に一致する IP アドレスに適用されます。

例えば、攻撃者からの最近のリクエストに基づいて、次の条件を含むレートベースのルールを作成できます。

- リクエストが 192.0.2.44 から発生した。
- リクエストの User-Agent ヘッダーに BadBot 値が含まれる。

このレートベースのルールでは、レート制限を定義することもできます。この例では、1,000 のレート制限を作成します。前述の条件の両方を満たし、5 分間に 1,000 リクエストを超えるリクエストは、ウェブ ACL で定義されたルールのアクション (ブロックまたはカウント) をトリガーします。

両方の条件を満たさないリクエストは、レート制限に対してカウントされないため、このルールの影響を受けません。

2 つ目の例では、ウェブサイトの特定のページにリクエストを制限します。これを行うには、次の文字列一致条件をレートベースのルールに追加します。

- [Part of the request to filter on] (フィルタリングするリクエストの一部) は、URI です。

- [Match Type] (一致タイプ) は `Starts with` です。
- [Value to match] (一致する値) は、`login` です。

さらに、1,000 の `RateLimit` を指定します。

このレートベースのルールをウェブ ACL に追加することで、残りのサイトに影響を与えることなく、ログインページへのリクエストを制限することができます。

ウェブ ACL

条件を組み合わせてルールを作成した後、ルールを組み合わせてウェブ ACL を作成します。ここで、各ルールのアクション (許可、ブロック、カウント) とデフォルトアクションを定義します。

各ルールのアクション

ウェブリクエストがルールのすべての条件に一致すると、 AWS WAF Classic はリクエストをブロックするか、リクエストを API Gateway API、CloudFront ディストリビューション、または Application Load Balancer に転送できるようにします。 AWS WAF Classic が各ルールに対して実行するアクションを指定します。

AWS WAF Classic は、ルールを一覧表示した順序でリクエストをウェブ ACL のルールと比較します。 AWS WAF 次に Classic は、リクエストが一致する最初のルールに関連付けられているアクションを実行します。たとえば、ウェブリクエストがリクエストを許可する 1 つのルールとリクエストをブロックする別のルールに一致する場合、 AWS WAF Classic は、最初にリストされているルールに応じてリクエストを許可または拒否します。

使用を開始する前に新しいルールをテストする場合は、ルールのすべての条件を満たすリクエストをカウントするように AWS WAF Classic を設定することもできます。リクエストを許可またはブロックするルールと同様に、リクエストをカウントするルールも、ウェブ ACL でリストされている順番によって影響を受けます。例えば、ウェブリクエストが、リクエストを許可する 1 つのルールと一致し、リクエストをカウントする別のルールと一致する場合、リクエストを許可するルールが最初にリストされていると、リクエストはカウントされません。

デフォルトアクション

デフォルトのアクションは、 AWS WAF Classic がウェブ ACL のルールのすべての条件に一致しないリクエストを許可するかブロックするかを決定します。例えば、ウェブ ACL を作成し、前に定義したルールのみを追加するとします。

- リクエストが 192.0.2.44 から発生した。
- リクエストの `User-Agent` ヘッダーに `BadBot` 値が含まれる。

- それらのリクエストのクエリ文字列に悪意のある可能性がある SQL コードが含まれる。

リクエストがルールの 3 つの条件をすべて満たしておらず、デフォルトのアクションがの場合ALLOW、 AWS WAF Classic はリクエストを API Gateway、CloudFront、または Application Load Balancer に転送し、サービスはリクエストされたオブジェクトで応答します。

ウェブ ACL に 2 つ以上のルールを追加すると、リクエストがルールのすべての条件を満たさない場合にのみ、 AWS WAF Classic はデフォルトのアクションを実行します。例えば、以下の 1 つの条件を含む 2 つ目のルールを追加するとします。

- `User-Agent` ヘッダーに `BIGBadBot` 値が含まれるリクエスト。

AWS WAF Classic は、リクエストが最初のルールの 3 つの条件をすべて満たしておらず、2 番目のルールの 1 つの条件を満たさない場合にのみ、デフォルトのアクションを実行します。

場合によっては、リクエストを許可またはブロックするかどうかについて、Amazon API Gateway、Amazon CloudFront、または Application Load Balancer への応答を遅らせる内部エラーが発生する AWS WAF ことがあります。そのような場合は通常、CloudFront はリクエストを許可またはコンテンツを提供します。API Gateway および Application Load Balancer は、通常、リクエストを拒否し、コンテンツを提供しません。

AWS WAF クラシック料金

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

AWS WAF Classic では、作成したウェブ ACLs とルール、および AWS WAF Classic が検査する HTTP リクエストの数に対してのみ料金が発生します。詳細については、「AWS WAF Classic の料金」を参照してください。

AWS WAF Classic の開始方法

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

このチュートリアルでは、 AWS WAF Classic を使用して以下のタスクを実行する方法を示します。

- AWS WAF Classic をセットアップします。
- AWS WAF Classic コンソールを使用してウェブアクセスコントロールリスト (ウェブ ACL) を作成し、ウェブリクエストのフィルタリングに使用する条件を指定します。例えば、リクエストの発生元の IP アドレスと、攻撃者によってのみ使用されるリクエスト内の値を指定できます。
- 条件をルールに追加します。ルールでは、ブロックまたは許可するウェブリクエストを対象にすることができます。ウェブリクエストは、 AWS WAF Classic が指定した条件に基づいてリクエストをブロックまたは許可する前に、ルールのすべての条件と一致する必要があります。
- ルールをウェブ ACL に追加します。ウェブ ACL では、各ルールに追加する条件に基づいて、ウェブリクエストをブロックするか許可するかを指定します。
- ブロックまたは許可のいずれかのデフォルトアクションを指定します。これは、ウェブリクエストがどのルールとも一致しない場合に AWS WAF Classic が実行するアクションです。
- AWS WAF Classic がウェブリクエストを検査する Amazon CloudFront ディストリビューションを選択します。このチュートリアルでは、CloudFront のステップのみについて説明します

が、Application Load Balancer と Amazon API Gateway APIsのプロセスは基本的に同じです。CloudFront の AWS WAF Classic はすべての で使用できます AWS リージョン。API Gateway で使用する AWS WAF Classic または Application Load Balancer は、AWS サービスエンドポイントにリストされているリージョンで使用できます。

> **Note**
>
> AWS 通常、 は、このチュートリアルで作成したリソースに対して 1 日あたり 0.25 USD 未満を請求します。チュートリアルを終了したら、不要な料金が発生しないようにリソースを削除することをお勧めします。

トピック

- ステップ 1: AWS WAF Classic をセットアップする
- ステップ 2: ウェブ ACL を作成する
- ステップ 3: IP 一致条件を作成する
- ステップ 4: Geo 一致条件を作成する
- ステップ 5: 文字列一致条件を作成する
- ステップ 5A: (オプション) 正規表現条件を作成する
- ステップ 6: SQL インジェクション一致条件を作成する
- ステップ 7: (オプション) 追加の条件を作成する
- ステップ 8: ルールを作成して条件を追加する
- ステップ 9: ルールをウェブ ACL に追加する
- ステップ 10: リソースをクリーンアップする

ステップ 1: AWS WAF Classic をセットアップする

AWS WAF Classic のセットアップ の一般的なセットアップ手順をまだ実行していない場合、今すぐ実行してください。

ステップ 2: ウェブ ACL を作成する

AWS WAF Classic コンソールは、リクエストの送信元の IP アドレスやリクエストの値など、指定した条件に基づいてウェブリクエストをブロックまたは許可するように AWS WAF Classic を設定するプロセスをガイドします。このステップでは、ウェブ ACL を作成します。

ウェブ ACL を作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示されている場合は、それを選択します。

2. AWS WAF Classic を初めて使用する場合は、 AWS WAF 「クラシックに移動」を選択し、「ウェブ ACL の設定」を選択します。

   AWS WAF Classic を以前に使用したことがある場合は、ナビゲーションペインでウェブ ACLs を選択し、ウェブ ACL の作成を選択します。

3. [Name web ACL] (ウェブ ACL に名前を付ける) ページで、[Web ACL name] (ウェブ ACL の名前) に名前を入力します。

   > **Note**
   >
   > ウェブ ACL の作成後は、名前を変更することはできません。

4. [CloudWatch metric name] (CloudWatch メトリクス名)で、名前を入力します。名前には、英数字のみ (A～Z、a～z、0～9) を使用できます。空白を含めることはできません。

   > **Note**
   >
   > ウェブ ACL の作成後は、名前を変更することはできません。

5. [Region] (リージョン) で、リージョンを選択します。このウェブ ACL を CloudFront ディストリビューションに関連付ける場合は、[Global (CloudFront)] (グローバル (CloudFront)) を選択します。

6. [AWS resource to associate (関連付けるリソース)] で、ウェブ ACL に関連付けるリソースを選択し、[Next (次へ)] を選択します。

ステップ 3: IP 一致条件を作成する

IP 一致条件では、リクエストの発生元の IP アドレスまたは IP アドレス範囲を指定します。このステップでは、IP 一致条件を作成します。後のステップで、指定した IP アドレスからのリクエストを許可するかブロックするかを指定します。

> **Note**
>
> IP 一致条件の詳細については、「IP 一致条件の使用」を参照してください。

IP 一致条件を作成するには

1. [Create conditions] (条件を作成) ページの [IP match conditions] (IP 一致条件) で、[Create condition] (条件を作成) を選択します。
2. [Create IP match condition] (IP 一致条件の作成) ダイアログボックスの [Name] (名前) に名前を入力します。名前に使用できるのは英数字 (A～Z、a～z、0～9) または特殊文字 _-!"#`+*},./ です。
3. [Address] (アドレス) で、192.0.2.0/24 と入力します。この IP アドレス範囲は、CIDR 表記で指定しており、192.0.2.0 から 192.0.2.255 までの IP アドレスが含まれます (192.0.2.0/24 の IP アドレス範囲は例のために予約されているため、ウェブリクエストはこれらの IP アドレスから発生しません)。

   AWS WAF Classic は IPv4 アドレス範囲 /8、および /16 から /32 までの任意の範囲をサポートします。 AWS WAF Classic は IPv6 アドレス範囲 /24、/32、/48、/56、/64、および /128 をサポートします。(192.0.2.44 など 1 つの IP アドレスを指定するには、192.0.2.44/32 と入力します)。他の範囲はサポートされていません。

   CIDR 表記の詳細については、Wikipedia の「Classless Inter-Domain Routing」(クラスレスドメイン間ルーティング) 記事を参照してください。
4. [Create] (作成) を選択します。

ステップ 4: Geo 一致条件を作成する

Geo 一致条件では、リクエスト送信元の 1 つ以上の国を指定します。このステップでは、Geo 一致条件を作成します。後のステップで、指定した国から送信されたリクエストを許可するかブロックするかを指定します。

> **Note**
>
> Geo 一致条件の詳細については、「Geo (地理的) 一致条件の使用」を参照してください。

Geo 一致条件を作成するには

1. [Create conditions] (条件を作成) ページの [Geo match conditions] (Geo 一致条件) で、[Create condition] (条件を作成) を選択します。
2. [Create geo match condition] (geo 一致条件の作成) ダイアログボックスの [Name] (名前) に名前を入力します。名前に使用できるのは英数字 (A ~ Z、a ~ z、0 ~ 9) または特殊文字 _-!"#`+*},./ です。
3. [Location type] (場所のタイプ) と国を選択します。現時点では、[Location type] (場所のタイプ) は [Country] (国) にのみ設定できます。
4. [Add location] (場所を追加) を選択します。
5. [Create] (作成) を選択します。

ステップ 5: 文字列一致条件を作成する

文字列一致条件は、ヘッダーまたはクエリ文字列の指定された値など、リクエストで AWS WAF Classic が検索する文字列を識別します。通常、文字列は印刷可能な ASCII 文字で構成されますが、16 進数 0x00 ～ 0xFF (10 進数 0 ～ 255) の任意の文字を指定できます。このステップでは、文字列一致条件を作成します。後のステップで、指定した文字列を含むリクエストを許可するかブロックするかを指定します。

> **Note**
>
> 文字列一致条件の詳細については、「文字列一致条件の使用」を参照してください。

文字列一致条件を作成するには

1. [Create conditions] (条件を作成) ページの [String and regex match conditions] (文字列および正規表現の一致条件) で、[Create condition] (条件を作成) を選択します。
2. [Create string match condition] (文字列一致条件の作成) ダイアログボックスで、次の値を入力します。

[Name] (名前)

名前を入力します。名前に使用できるのは英数字 (A～Z、a～z、0～9) または特殊文字 _-!"#`+*},./ です。

[Type] (タイプ)

[String match] (文字列の一致) を選択します。

[Part of the request to filter on] (フィルタリングするリクエストの一部)

AWS WAF Classic で指定された文字列を検査するウェブリクエストの部分を選択します。

この例では、[Header] (ヘッダー) を選択します。

> **Note**
>
> [Part of the request to filter on] (フィルタリングするリクエストの一部) の値として [Body] (本文) を選択した場合、CloudFront によって最初の 8,192 バイトのみが検査のために転送されるため、 AWS WAF Classic によって最初の 8,192 バイト (8 KB) のみが検査されます。本文が 8,192 バイトより長いリクエストを許可またはブロックするには、サイズ制約条件を作成します。(AWS WAF Classic はリクエストヘッダーから本文の長さを取得します) 。詳細については、「サイズ制約条件の使用」を参照してください。

[Header] (ヘッダー) ([Part of the request to filter on] (フィルタリングするリクエストの一部) が [Header] (ヘッダー) の場合は必須)

フィルタリングするリクエストの一部にヘッダーを選択しているため、 AWS WAF Classic で検査するヘッダーを指定する必要があります。[User-Agent] を入力します。(この値は大文字と小文字が区別されません。)

[Match type] (一致タイプ)

指定した文字列が [User-Agent] ヘッダーに表示される場所 (文字列の先頭、末尾、または任意の場所など) を選択します。

この例では、完全一致を選択します。これは、 AWS WAF Classic が指定した値と同じヘッダー値についてウェブリクエストを検査することを示します。

変換

AWS WAF Classic をバイパスするために、攻撃者は空白を追加したり、リクエストの一部またはすべてを URL エンコードしたりするなどして、ウェブリクエストで異常な形式を使用します。[Transformation] (変換) を有効にすることで、ウェブリクエストはより標準的な形式に変換されます。そのために、空白が削除されたり、リクエストが URL デコードされたり、攻撃者がよく使用する特殊な形式の多くが排除されたりします。

1 種類のテキスト変換しか指定できません。

この例では、[None] (なし) を選択します。

[Value is base64 encoded] (値が base64 エンコードされている)

[Value to match] (一致する値) に入力した値が既に base64 でエンコードされている場合は、このチェックボックスをオンにします。

この例では、このチェックボックスをオンにしないでください。

[Value to match] (照合する値)

Classic で AWS WAF 検索する値を、フィルタリングするリクエストのパートで指定したウェブリクエストのパートで指定します。

この例では、BadBot. AWS WAF Classic はウェブリクエストの `User-Agent` ヘッダーに BadBot の値がないか検査します。」と入力します。

[Value to match] (一致する値) は最大 50 文字です。base64 でエンコードされた値を指定する場合、エンコード前の長さで最大 50 文字指定できます。

3. AWS WAF Classic で を含む`User-Agent`ヘッダー`BadBot`や を含むクエリ文字列など、複数の値についてウェブリクエストを検査する場合は`BadParameter`、次の 2 つの選択肢があります。

   - 両方の値が含まれているときにのみ (AND)、ウェブリクエストを許可またはブロックする場合は、値ごとに 1 つの文字列一致条件を作成します。
   - 一方か両方の値が含まれているときに (OR)、ウェブリクエストを許可またはブロックする場合は、両方の値を同じ文字列一致条件に追加します。

   この例では、[Create] (作成) を選択します。

ステップ 5A: (オプション) 正規表現条件を作成する

正規表現条件は文字列一致条件の一種であり、ヘッダーやクエリ文字列の指定された値など、リクエストで AWS WAF Classic が検索する文字列を識別する点で似ています。主な違いは、正規表現 (regex) を使用して AWS WAF Classic で検索する文字列パターンを指定することです。このステップでは、正規表現一致条件を作成します。後のステップで、指定した文字列を含むリクエストを許可するかブロックするかを指定します。

> **Note**
>
> 正規表現一致条件の詳細については、「正規表現一致条件の使用」を参照してください。

正規表現一致条件を作成するには

1. [Create conditions] (条件を作成) ページの [String match and regex conditions] (文字列の一致および正規表現の条件)で、[Create condition] (条件を作成) を選択します。
2. [Create string match condition] (文字列一致条件の作成) ダイアログボックスで、次の値を入力します。

   [Name] (名前)

   名前を入力します。名前に使用できるのは英数字 (A ~ Z、a ~ z、0 ~ 9) または特殊文字 _-!"#`+*},./ です。

   [Type] (タイプ)

   [Regex match] (正規表現の一致) を選択します。

   [Part of the request to filter on] (フィルタリングするリクエストの一部)

   AWS WAF Classic で指定された文字列を検査するウェブリクエストの部分を選択します。

   この例では、[Body] (本文) を選択します。

   > **Note**
   >
   > [Part of the request to filter on] (フィルタリングするリクエストの一部) の値として [Body] (本文) を選択した場合、CloudFront によって最初の 8,192 バイトのみが検査のために転送されるため、 AWS WAF Classic によって最初の 8,192 バイト (8 KB) のみが検査されます。本文が 8,192 バイトより長いリクエストを許可またはブロッ

クするには、サイズ制約条件を作成します。(AWS WAF Classic はリクエストヘッダーから本文の長さを取得します) 。詳細については、「サイズ制約条件の使用」を参照してください。

変換

AWS WAF Classic をバイパスするために、攻撃者は空白を追加したり、リクエストの一部またはすべてを URL エンコードしたりするなどして、ウェブリクエストで異常な形式を使用します。[Transformation] (変換) を有効にすることで、ウェブリクエストはより標準的な形式に変換されます。そのために、空白が削除されたり、リクエストが URL デコードされたり、攻撃者がよく使用する特殊な形式の多くが排除されたりします。

1 種類のテキスト変換しか指定できません。

この例では、[None] (なし) を選択します。

Regex patterns to match to request (リクエストに一致する正規表現パターン)

[Create regex pattern set] (正規表現パターンセットを作成) を選択します。

New pattern set name (新しいパターンセット名)

名前を入力し、 AWS WAF Classic で検索する正規表現パターンを指定します。

次に、正規表現 I[a@]mAB[a@]dRequest. AWS WAF Classic を入力します。 はウェブリクエストの `User-Agent` ヘッダーに値がないか検査します。

- IamABadRequest
- IamAB@dRequest
- I@mABadRequest
- I@mAB@dRequest

3. [Create pattern set and add filter] (パターンセットを作成してフィルターを追加) を選択します。
4. [Create] (作成) を選択します。

ステップ 6: SQL インジェクション一致条件を作成する

SQL インジェクション一致条件は、 AWS WAF Classic が悪意のある SQL コードを検査するヘッダーやクエリ文字列などのウェブリクエストの部分を識別します。攻撃者は SQL クエリを使用してデータベースからデータを抽出します。このステップでは、SQL インジェクション一致条件を作成

します。後のステップで、悪意のある可能性がある SQL コードを含むリクエストを許可するかブロックするかを指定します。

> **Note**
>
> 文字列一致条件の詳細については、「SQL インジェクション一致条件の使用」を参照してください。

ステップ 5: SQL インジェクション一致条件を作成するには

1. [Create conditions] (条件を作成) ページの [SQL injection match conditions] (SQL インジェクション一致条件) で、[Create condition] (条件を作成) を選択します。
2. [Create SQL injection match condition] (SQL インジェクション一致条件の作成) ダイアログボックスで、次の値を入力します。

   [Name] (名前)

   名前を入力します。

   [Part of the request to filter on] (フィルタリングするリクエストの一部)

   AWS WAF Classic で悪意のある SQL コードを検査するウェブリクエストの部分を選択します。

   この例では、[Query string] (クエリ文字列) を選択します。

   > **Note**
   >
   > [Part of the request to filter on] (フィルタリングするリクエストの一部) の値として [Body] (本文) を選択した場合、CloudFront によって最初の 8,192 バイトのみが検査のために転送されるため、 AWS WAF Classic によって最初の 8,192 バイト (8 KB) のみが検査されます。本文が 8,192 バイトより長いリクエストを許可またはブロックするには、サイズ制約条件を作成します。(AWS WAF Classic はリクエストヘッダーから本文の長さを取得します) 。詳細については、「サイズ制約条件の使用」を参照してください。

[Transformation] (変換)

この例では、[URL decode] (URL デコード) を選択します。

攻撃者は Classic をバイパスするために URL エンコードなどの異常な形式を使用します AWS WAF 。[URL decode] (URL デコード) オプションを選択すると、 AWS WAF Classic によってリクエストが検査される前に、ウェブリクエストでその形式の部分が削除されます。

1 種類のテキスト変換しか指定できません。

3. [Create] (作成) を選択します。
4. [Next] (次へ) を選択します。

ステップ 7: (オプション) 追加の条件を作成する

AWS WAF Classic には、以下を含む他の条件が含まれます。

- サイズ制約条件 – AWS WAF Classic で長さを確認するヘッダーやクエリ文字列などのウェブリクエストの部分を識別します。詳細については、「サイズ制約条件の使用」を参照してください。
- クロスサイトスクリプト一致条件 – 悪意のあるスクリプトを検査 AWS WAF するヘッダーやクエリ文字列などのウェブリクエストの一部を識別します。詳細については、「クロスサイトスクリプティング一致条件の使用」を参照してください。

この時点で、必要に応じてこれらの条件を作成するか、「ステップ 8: ルールを作成して条件を追加する」に進むことができます。

ステップ 8: ルールを作成して条件を追加する

Classic がウェブリクエストで AWS WAF 検索する条件を指定するルールを作成します。ルールに複数の条件を追加する場合、 AWS WAF Classic がそのルールに基づいてリクエストを許可またはブロックするには、ウェブリクエストがルールのすべての条件と一致する必要があります。

> **Note**
>
> ルールの詳細については、「ルールの使用」を参照してください。

ルールを作成して条件を追加するには

1. [Create rules] (ルールの作成) ページで、[Create rule] (ルールの作成) を選択します。
2. [Create rule] (ルールの作成) ダイアログボックスで、次の値を入力します。

   [Name] (名前)

   名前を入力します。

   [CloudWatch metric name] (CloudWatch メトリクス名)

   AWS WAF Classic が作成し、ルールに関連付ける CloudWatch メトリクスの名前を入力します。名前には、英数字のみ (A ~ Z、a ~ z、0 ~ 9) を使用できます。空白を含めることはできません。

   [Rule type] (ルールタイプ)

   [Regular rule] (通常ルール) または [Rate-based rule] (レートベースのルール) を選択します。レートベースのルールは通常ルールと同じですが、5 分間に識別された IP アドレスから着信したリクエストの数も考慮に入れます。ルールタイプの詳細については、「AWS WAF Classic の仕組み」を参照してください。この例では、[Regular rule] を選択します。

   [Rate limit] (レート制限)

   レートベースのルールの場合、ルールの条件に一致する IP アドレスから 5 分間に許可するリクエストの最大数を入力します。
3. ルールに追加する最初の条件として、次の設定を指定します。

   - ウェブリクエストが条件の設定と一致するかどうかに基づいて、 AWS WAF Classic がリクエストを許可またはブロックするかどうかを選択します。

     この例では、[does] (条件に該当) を選択します。
   - ルールに追加する条件のタイプ (IP 一致セット条件、文字列一致セット条件、または SQL インジェクション一致セット条件) を選択します。

     この例では、[originate from IP addresses in] (次の IP アドレスから発信) を選択します。
   - ルールに追加する条件を選択します。

     この例では、前のタスクで作成した IP 一致条件を選択します。
4. [Add condition] (条件を追加) を選択します。
5. 前に作成した Geo 一致条件を追加します。次の値を指定します。

- [When a request does] (リクエストが条件に該当する場合)
- [originate from a geographic location in] (発生元の地理的場所)
- Geo 一致条件を選択します。

6. [Add another condition] (別の条件を追加) を選択します。
7. 前に作成した文字列一致条件を追加します。次の値を指定します。
   - [When a request does] (リクエストが条件に該当する場合)
   - [match at least one of the filters in the string match condition] (文字列一致条件のフィルターの少なくとも 1 つに一致)
   - 文字列一致条件を選択します。
8. [Add condition] (条件を追加) を選択します。
9. 前に作成した SQL インジェクション一致条件を追加します。次の値を指定します。
   - [When a request does] (リクエストが条件に該当する場合)
   - [match at least one of the filters in the SQL injection match condition] (SQL インジェクション一致条件のフィルターの少なくとも 1 つに一致)
   - SQL インジェクション一致条件を選択します。
10. [Add condition] (条件を追加) を選択します。
11. 前に作成したサイズ制約条件を追加します。次の値を指定します。
    - [When a request does] (リクエストが条件に該当する場合)
    - [match at least one of the filters in the size constraint condition] (サイズ制約条件のフィルターの少なくとも 1 つに一致)
    - サイズ制約条件を選択します。
12. 正規表現条件など、他の条件を作成した場合は、同様の方法でそれらの条件を追加します。
13. [Create] (作成) を選択します。
14. [Default action] (デフォルトのアクション) で、[Allow all requests that don't match any rules] (ルールに一致しないすべてのリクエストを許可) を選択します。
15. [Review and create] (確認および作成) を選択します。

ステップ 9: ルールをウェブ ACL に追加する

ルールをウェブ ACL に追加するときは、次の設定を指定します。

- Classic がルールのすべての条件に一致するウェブリクエストに対して AWS WAF 実行するアクション: リクエストを許可、ブロック、またはカウントします。
- ウェブ ACL のデフォルトアクション。これは、ルールのすべての条件に一致しないウェブリクエストに対して AWS WAF Classic が実行するアクションです。リクエストを許可または拒否します。

AWS WAF Classic は、以下のすべての条件 (および追加した可能性のある他の条件) に一致する CloudFront ウェブリクエストのブロックを開始します。

- `User-Agent` ヘッダーの値が `BadBot`
- (正規表現条件を作成して追加した場合) Body の値がパターン `I[a@]mAB[a@]dRequest` と一致する 4 つの文字列のいずれか
- リクエストの発生元が 192.0.2.0 ~ 192.0.2.255 の範囲の IP アドレス
- リクエストの送信元が Geo 一致条件で選択した国
- リクエスト内のクエリ文字列に悪意のある可能性がある SQL コードが含まれる

AWS WAF Classic を使用すると、CloudFront はこれらの 3 つの条件をすべて満たしていないリクエストに応答できます。

ステップ 10: リソースをクリーンアップする

これでチュートリアルは完了です。アカウントに AWS WAF Classic の追加料金が発生しないようにするには、作成した AWS WAF Classic オブジェクトをクリーンアップする必要があります。または、許可、ブロック、カウントするウェブリクエストに合わせて設定を変更することもできます。

> **Note**
>
> AWS 通常、 は、このチュートリアルで作成したリソースに対して 1 日あたり 0.25 USD 未満を請求します。終了したら、不要な料金が発生しないようにリソースを削除することをお勧めします。

AWS WAF Classic が請求するオブジェクトを削除するには

1. CloudFront ディストリビューションからウェブ ACL の関連付けを解除します。

a. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。

b. 削除するウェブ ACL の名前を選択します。これにより、右ペインで、ウェブ ACL の詳細を含むページが開きます。

c. 右ペインの [Rules] (ルール) タブで、[AWS resources using this web ACL] (このウェブ ACL を使用する リソース) セクションに移動します。ウェブ ACL を関連付けた CloudFront ディストリビューションに対して、[Type] (タイプ) 列の [x] を選択します。

2. ルールから条件を削除する:

   a. ナビゲーションペインで [Rules] (ルール) を選択します。

   b. チュートリアルで作成したルールを選択します。

   c. [Edit rule] (ルールの編集) を選択します。

   d. 各条件見出しの右にある [x] を選択します。

   e. [Update] (更新) を選択します。

3. ウェブ ACL からルールを削除し、ウェブ ACL を削除する:

   a. ナビゲーションペインで [Web ACLs] (ウェブ ACL) を選択します。

   b. チュートリアルで作成したウェブ ACL の名前を選択します。これにより、右ペインで、ウェブ ACL の詳細を含むページが開きます。

   c. [Rules] (ルール) タブで、[Edit web ACL] (ウェブ ACL を編集) を選択します。

   d. 各ルール見出しの右にある [x] を選択します。

   e. [Actions] (アクション) を選択してから、[Delete web ACL] (ウェブ ACL を削除) を選択します。

4. ルールを削除する:

   a. ナビゲーションペインで [Rules] (ルール) を選択します。

   b. チュートリアルで作成したルールを選択します。

   c. [Delete] (削除) を選択します。

   d. [Delete] (削除) のダイアログボックスで、再度 [Delete] (削除) を選択して確認します。

AWS WAF Classic は条件に対して課金しませんが、クリーンアップを完了する場合は、次の手順を実行して条件からフィルターを削除し、条件を削除します。

フィルターと条件を削除するには

1. IP 一致条件で IP アドレス範囲を削除し、IP 一致条件を削除します。
   a. AWS WAF Classic コンソールのナビゲーションペインで、IP アドレスを選択します。
   b. チュートリアルで作成した IP 一致条件を選択します。
   c. 追加した IP アドレス範囲のチェックボックスをオンにします。
   d. [Delete IP address or range] (IP アドレスまたは範囲を削除) を選択します。
   e. [IP match conditions] (IP 一致条件) ペインで、[Delete] (削除) を選択します。
   f. [Delete] (削除) のダイアログボックスで、再度 [Delete] (削除) を選択して確認します。
2. SQL インジェクションでフィルターを削除し、SQL インジェクション一致条件を削除する:
   a. ナビゲーションペインで、[SQL injection] (SQL インジェクション) を選択します。
   b. チュートリアルで作成した SQL インジェクション一致条件を選択します。
   c. 追加したフィルターのチェックボックスをオンにします。
   d. [Delete filter] (フィルターを削除) を選択します。
   e. [SQL injection match conditions] (SQL インジェクション一致条件) ペインで、[Delete] (削除) を選択します。
   f. [Delete] (削除) のダイアログボックスで、再度 [Delete] (削除) を選択して確認します。
3. 文字列一致条件でフィルターを削除し、文字列一致条件を削除します。
   a. ナビゲーションペインで、[String and regex matching] (文字列および正規表現の一致) を選択します。
   b. チュートリアルで作成した文字列一致条件を選択します。
   c. 追加したフィルターのチェックボックスをオンにします。
   d. [Delete filter] (フィルターを削除) を選択します。
   e. [String match conditions] (文字列一致条件) ペインで、[Delete] (削除) を選択します。
   f. [Delete] (削除) のダイアログボックスで、再度 [Delete] (削除) を選択して確認します。
4. フィルターを作成した場合は、正規表現一致条件でフィルタを削除してから、正規表現一致条件を削除します。

a. ナビゲーションペインで、[String and regex matching] (文字列および正規表現の一致) を選択します。
b. チュートリアルで作成した正規表現一致条件を選択します。
c. 追加したフィルターのチェックボックスをオンにします。
d. [Delete filter] (フィルターを削除) を選択します。
e. [Regex match conditions] (正規表現一致条件) ペインで、[Delete] (削除) を選択します。
f. [Delete] (削除) のダイアログボックスで、再度 [Delete] (削除) を選択して確認します。

5. サイズ制約条件でフィルターを削除し、サイズ制約条件を削除します。

a. ナビゲーションペインで、[Size constraints] (サイズ制約) を選択します。
b. チュートリアルで作成したサイズ制約条件を選択します。
c. 追加したフィルターのチェックボックスをオンにします。
d. [Delete filter] (フィルターを削除) を選択します。
e. [Size constraint conditions] (サイズ制約の条件) ペインで、[Delete] (削除) を選択します。
f. [Delete] (削除) のダイアログボックスで、再度 [Delete] (削除) を選択して確認します。

ウェブアクセスコントロールリスト (ウェブ ACL) の作成と設定

Warning

AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

Note

これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

ウェブアクセスコントロールリスト (ウェブ ACL) を使用すると、Amazon API Gateway API、Amazon CloudFront ディストリビューション、または Application Load Balancer が応答するウェブリクエストをきめ細かく制御できます。次の種類のリクエストを許可またはブロックすることができます。

- 特定の IP アドレスまたは IP アドレス範囲が送信元である
- 特定の国が送信元である
- リクエストの特定の部分が、指定した文字列を含むか、正規表現パターンと一致する
- 指定した長さを超えている
- 悪意のある SQL コード (通称 SQL インジェクション) が含まれている可能性がある
- 悪意のあるスクリプト (通称クロスサイトスクリプティング) が含まれている可能性がある

また、これらの条件の組み合わせをテストしたり、指定された条件を満たすだけでなく、5 分間にわたって指定された数のリクエストを超えるウェブリクエストをブロックまたはカウントすることもできます。

コンテンツへのアクセスを許可またはブロックするリクエストを選り分けるには、次のタスクを実行します。

1. ウェブリクエストが指定条件のいずれとも一致しない場合のデフォルトアクション (許可またはブロック) を選択します。詳細については、「ウェブ ACL のデフォルトアクションの決定」を参照してください。
2. リクエストを許可またはブロックする条件を指定します。
   - 悪意のあるスクリプトが含まれている可能性があるかどうかに基づいてリクエストを許可またはブロックするには、クロスサイトスクリプティング一致条件を作成します。詳細については、「クロスサイトスクリプティング一致条件の使用」を参照してください。
   - 送信元の IP アドレスに基づいてリクエストを許可またはブロックするには、IP 一致条件を作成します。詳細については、「IP 一致条件の使用」を参照してください。
   - 送信元の国に基づいてリクエストを許可またはブロックするには、Geo 一致条件を作成します。詳細については、「Geo (地理的) 一致条件の使用」を参照してください。
   - 指定した長さを超えているかどうかに基づいてリクエストを許可またはブロックするには、サイズ制約条件を作成します。詳細については、「サイズ制約条件の使用」を参照してください。

- 悪意のある SQL コードが含まれている可能性があるかどうかに基づいてリクエストを許可またはブロックするには、SQL インジェクション一致条件を作成します。詳細については、「SQL インジェクション一致条件の使用」を参照してください。
- 含まれている文字列に基づいてリクエストを許可またはブロックするには、文字列一致条件を作成します。詳細については、「文字列一致条件の使用」を参照してください。
- リクエストに含まれる正規表現パターンと一致する文字列に基づいてリクエストを許可またはブロックするには、正規表現一致条件を作成します。詳細については、「正規表現一致条件の使用」を参照してください。

3. 条件を 1 つまたは複数のルールに追加します。同じルールに複数の条件を追加する場合、ウェブリクエストは AWS WAF Classic がルールに基づいてリクエストを許可またはブロックするすべての条件と一致する必要があります。詳細については、「ルールの使用」を参照してください。必要に応じて、通常のルールの代わりにレートベースのルールを使用して、条件を満たす IP アドレスからのリクエスト数を制限できます。
4. ルールをウェブ ACL に追加します。ルールごとに、ルールに追加した条件に基づいて AWS WAF Classic がリクエストを許可するかブロックするかを指定します。ウェブ ACL に複数のルールを追加すると、 AWS WAF Classic はウェブ ACL にリストされている順序でルールを評価します。詳細については、「ウェブ ACL の使用」を参照してください。

   新しいルールを追加したり、既存のルールを更新したりすると、該当するすべてのウェブ ACL およびリソースでそれらの変更がアクティブになるまでに、最大 1 分かかることがあります。

トピック

- 条件の使用
- ルールの使用
- ウェブ ACL の使用

条件の使用

> **Warning**
>
> AWS WAF Classic は計画されたend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

リクエストを許可またはブロックする場合に条件を指定します。

- 悪意のあるスクリプトが含まれている可能性があるかどうかに基づいてリクエストを許可またはブロックするには、クロスサイトスクリプティング一致条件を作成します。詳細については、「クロスサイトスクリプティング一致条件の使用」を参照してください。
- 送信元の IP アドレスに基づいてリクエストを許可またはブロックするには、IP 一致条件を作成します。詳細については、「IP 一致条件の使用」を参照してください。
- 送信元の国に基づいてリクエストを許可またはブロックするには、Geo 一致条件を作成します。詳細については、「Geo (地理的) 一致条件の使用」を参照してください。
- 指定した長さを超えているかどうかに基づいてリクエストを許可またはブロックするには、サイズ制約条件を作成します。詳細については、「サイズ制約条件の使用」を参照してください。
- 悪意のある SQL コードが含まれている可能性があるかどうかに基づいてリクエストを許可またはブロックするには、SQL インジェクション一致条件を作成します。詳細については、「SQL インジェクション一致条件の使用」を参照してください。
- 含まれている文字列に基づいてリクエストを許可またはブロックするには、文字列一致条件を作成します。詳細については、「文字列一致条件の使用」を参照してください。
- リクエストに含まれる正規表現パターンと一致する文字列に基づいてリクエストを許可またはブロックするには、正規表現一致条件を作成します。詳細については、「正規表現一致条件の使用」を参照してください。

トピック

- クロスサイトスクリプティング一致条件の使用
- IP 一致条件の使用
- Geo (地理的) 一致条件の使用
- サイズ制約条件の使用

- SQL インジェクション一致条件の使用
- 文字列一致条件の使用
- 正規表現一致条件の使用

クロスサイトスクリプティング一致条件の使用

> **Warning**
>
> AWS WAF Classic は計画されたend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

攻撃者は、ウェブアプリケーションの脆弱性を悪用するために、ウェブリクエスト内にスクリプトを挿入する場合があります。1 つ以上のクロスサイトスクリプティング一致条件を作成して、 URI やクエリ文字列など、 AWS WAF Classic で悪意のあるスクリプトがないか検査するウェブリクエストの部分を特定できます。後でウェブ ACL を作成するときに、悪意のあるスクリプトが含まれている可能性があるリクエストを許可するかブロックするかを指定します。

トピック

- クロスサイトスクリプティング一致条件の作成
- クロスサイトスクリプティング一致条件の作成時または編集時に指定する値
- クロスサイトスクリプティング一致条件のフィルターの追加と削除
- クロスサイトスクリプティング一致条件の削除

クロスサイトスクリプティング一致条件の作成

クロスサイトスクリプティング一致条件を作成する場合は、フィルターを指定します。フィルタは、AWS WAF Classic が URI やクエリ文字列などの悪意のあるスクリプトを検査するウェブリクエストの部分を示します。クロスサイトスクリプティング一致条件には複数のフィルターを追加できます。条件ごとに 1 つのフィルターを設定することもできます。各設定が AWS WAF Classic の動作にどのように影響するかを次に示します。

- クロスサイトスクリプティング一致条件ごとに複数のフィルター (推奨) – 複数のフィルターを含むクロスサイトスクリプティング一致条件をルールに追加し、そのルールをウェブ ACL に追加する場合、ウェブリクエストはクロスサイトスクリプティング一致条件のフィルターの 1 つにのみ一致する必要があり、 AWS WAF Classic はその条件に基づいてリクエストを許可またはブロックします。

  例えば、1 つのクロスサイトスクリプティング一致条件を作成し、その条件に 2 つのフィルターを含めたとします。1 つのフィルターは URI に悪意のあるスクリプトがないか検査するように AWS WAF Classic に指示し、もう 1 つのフィルターはクエリ文字列を検査するように AWS WAF Classic に指示します。 AWS WAF Classic は、URI またはクエリ文字列に悪意のあるスクリプトが含まれているように見えるリクエストを許可またはブロックします。
- クロスサイトスクリプティング一致条件ごとに 1 つのフィルター – 個別のクロスサイトスクリプティング一致条件をルールに追加し、ウェブ ACL にルールを追加する場合、ウェブリクエストは Classic が条件に基づいてリクエストを許可またはブロック AWS WAF するすべての条件と一致する必要があります。

  2 つの条件を作成し、各条件に前の例で示した 2 つのフィルターの 1 つを別個に含めたとします。両方の条件を同じルールに追加し、そのルールをウェブ ACL に追加すると、 AWS WAF Classic は URI とクエリ文字列の両方に悪意のあるスクリプトが含まれているように見える場合にのみリクエストを許可または拒否します。

> **Note**
>
> クロスサイトスクリプト一致条件をルールに追加すると、悪意のあるスクリプトが含まれていないように見えるウェブリクエストを許可またはブロックするように AWS WAF Classic を設定することもできます。

クロスサイトスクリプティング一致条件を作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示されている場合は、それを選択します。
2. ナビゲーションペインで、[Cross-site scripting] (クロスサイトスクリプティング) を選択します。
3. [Create condition] (条件を作成) を選択します。
4. 適用するフィルター設定を指定します。詳細については、「クロスサイトスクリプティング一致条件の作成時または編集時に指定する値」を参照してください。
5. [Add another filter] (別のフィルターを追加) を選択します。
6. 別のフィルターを追加する場合は、ステップ 4～5 を繰り返します。
7. フィルターの追加が完了したら、[Create] (作成) を選択します。

クロスサイトスクリプティング一致条件の作成時または編集時に指定する値

クロスサイトスクリプティング一致条件を作成または更新するときに、次の値を指定します。

[Name] (名前)

クロスサイトスクリプティング一致条件の名前。

名前に使用できるのは A～Z、a～z、0～9 の英数字と特殊文字 _-!"#`+*},./ です。一度作成した条件の名前は変更できません。

[Part of the request to filter on] (フィルタリングするリクエストの一部)

AWS WAF Classic で悪意のあるスクリプトを検査する各ウェブリクエストの部分を選択します。

ヘッダー

指定したリクエストヘッダー (`User-Agent` や `Referer` など)。[Header] (ヘッダー) を選択した場合は、[Header] (ヘッダー) フィールドにヘッダー名を指定します。

[HTTP method] (HTTP メソッド)

リクエストがオリジンに実行を要求しているオペレーションのタイプを示す HTTP メソッド。CloudFront がサポートしているメソッドは、DELETE、GET、HEAD、OPTIONS、PATCH、POST、および PUT です。

[Query string] (クエリ文字列)

URL 内で ? 文字の後に続く部分 (ある場合)。

> **Note**
>
> クロスサイトスクリプティングの一致条件については、[Part of the request to filter on] (フィルタリングするリクエストの一部) に [Query string] (クエリ文字列) ではなく、[All query parameters (values only)] (すべてのクエリパラメータ (値のみ)) を選択することをお勧めします。

[URI]

リクエストの URI パス。リソースを識別します (例: /images/daily-ad.jpg)。これには、URI のクエリ文字列またはフラグメントコンポーネントは含まれません。詳細については、「Uniform Resource Identifier (URI): 一般的な構文」を参照してください。

変換が指定されていない限り、URI は正規化されず、リクエストの一部としてクライアントから AWS 受け取ったのと同じように検査されます。[Transformation] (変換) が指定されている場合、URI はその指定に従って形式が再設定されます。

[Body] (本文)

リクエスト内で、HTTP リクエストの本文としてウェブサーバーに送信する追加データ (フォームのデータなど) を含む部分。

> **Note**
>
> [Part of the request to filter on] (フィルタリングするリクエストの一部) の値として [Body] (本文) を選択した場合、 AWS WAF Classic によって最初の 8,192 バイト (8 KB) のみが検査されます。本文が 8,192 バイトより長いリクエストを許可またはブロックするには、サイズ制約条件を作成します。(AWS WAF Classic はリクエストヘッダーから本文の長さを取得します) 。詳細については、「サイズ制約条件の使用」を参照してください。

[Single query parameter (value only)] (単一クエリパラメータ (値のみ))

クエリ文字列の一部として定義されているすべてのパラメータです。例えば、URL が「www.xyz.com?UserName=abc&SalesRegion=seattle」である場合、UserName または SalesRegion パラメータにフィルターを追加できます。

[Single query parameter (value only)] (単一クエリパラメータ (値のみ)) を選択する場合は、[Query parameter name] (クエリパラメータ名) も指定します。これは検査するクエリ文字列のパラメータです (UserName や SalesRegion など)。[Query parameter name] (クエリパラメータ名) の最大長は 30 文字です。[Query parameter name] (クエリパラメータ名) では、大文字と小文字は区別されません。例えば、UserName を [Query parameter name] (クエリパラメータ名) として指定すると、username や UsERName など UserName のすべてのバリエーションに一致します。

[All query parameters (values only)] (すべてのクエリパラメータ (値のみ))

単一クエリパラメータ (値のみ) に似ていますが、単一パラメータの値を検査するのではなく、 AWS WAF Classic はクエリ文字列内のすべてのパラメータ値に悪意のあるスクリプトがないか検査します。例えば、URL が「www.xyz.com?UserName=abc&SalesRegion=seattle」の場合、[All query parameters (values only)] (すべてのクエリパラメータ (値のみ)) を選択すると、UserName または SalesRegion のいずれかの値に悪意のある可能性があるスクリプトが含まれている場合、 AWS WAF Classic によって一致がトリガーされます。

ヘッダー

フィルタリングするリクエストの一部のヘッダーを選択した場合は、一般的なヘッダーのリストからヘッダーを選択するか、 AWS WAF Classic で悪意のあるスクリプトを検査するヘッダーの名前を入力します。

変換

Classic がリクエストを AWS WAF 検査する前に、変換によってウェブリクエストが再フォーマットされます。これにより、攻撃者が AWS WAF Classic をバイパスするためにウェブリクエストで使用する異常なフォーマットの一部が排除されます。

1 種類のテキスト変換しか指定できません。

変換では次の操作を実行できます。

なし

AWS WAF Classic は、値の文字列が一致するかどうかを検査する前に、ウェブリクエストに対してテキスト変換を実行しません。

[Convert to lowercase] (小文字に変換)

AWS WAF Classic は、大文字 (A ~ Z) を小文字 (a ~ z) に変換します。

[HTML decode] (HTML デコード)

AWS WAF Classic は、HTML エンコード文字をエンコードされていない文字に置き換えます。

- " を & に置き換えます。
-   を改行なしスペースに置き換えます。
- < を < に置き換えます。
- > を > に置き換えます。
- 16 進数形式の文字 (&#xhhhh;) を対応する文字に置き換えます。
- 10 進数形式の文字 (&#nnnn;) を対応する文字に置き換えます。

[Normalize white space] (空白の正規化)

AWS WAF Classic は、次の文字をスペース文字 (10 進数 32) に置き換えます。

- \f、フォームフィード、10 進数 12
- \t、タブ、10 進数 9
- \n、改行、10 進数 10
- \r、キャリッジリターン、10 進数 13
- \v、垂直タブ、10 進数 11
- 改行なしスペース、10 進数 160

さらに、このオプションでは複数のスペースを 1 つのスペースに置き換えます。

[Simplify command line] (コマンドラインを簡素化)

オペレーティングシステムのコマンドラインのコマンドが含まれているリクエストの場合、このオプションを使用して次の変換を行います。

- 次の文字を削除します: \ " ' ^
- 次の文字の前にあるスペースを削除します: / (
- 次の文字をスペースに置き換えます: , ;
- 複数のスペースを 1 つのスペースに置き換えます。
- 大文字 (A〜Z) を小文字 (a〜z) に変換します。

[URL decode] (URL デコード)

URL エンコードされたリクエストをデコードします。

クロスサイトスクリプティング一致条件のフィルターの追加と削除

クロスサイトスクリプティング一致条件のフィルターを追加または削除できます。フィルターを変更するには、新しいフィルターを追加して古いフィルターを削除します。

クロスサイトスクリプティング一致条件のフィルターを追加または削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. ナビゲーションペインで、[Cross-site scripting] (クロスサイトスクリプティング) を選択します。
3. フィルターを追加または削除する対象の条件を選択します。
4. フィルターを追加するには、次のステップを実行します。

   a. [Add filter] (フィルターを追加) を選択します。

   b. 適用するフィルター設定を指定します。詳細については、「クロスサイトスクリプティング一致条件の作成時または編集時に指定する値」を参照してください。

   c. [Add] (追加) を選択します。
5. フィルターを削除するには、次のステップを実行します。

   a. 削除するフィルターを選択します。

   b. [Delete filter] (フィルターを削除) を選択します。

クロスサイトスクリプティング一致条件の削除

クロスサイトスクリプティング一致条件を削除するには、最初にその条件からすべてのフィルターを削除し、その条件を使用しているすべてのルールから条件自体を削除します。次に手順を示します。

クロスサイトスクリプティング一致条件を削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。

2. ナビゲーションペインで、[Cross-site scripting] (クロスサイトスクリプティング) を選択します。
3. [Cross-site scripting match conditions] (クロスサイトスクリプティング一致条件) ペインで、削除するクロスサイトスクリプティング一致条件を選択します。
4. 右ペインで、[Associated rules] (関連付けられたルール) タブを選択します。

   このクロスサイトスクリプティング一致条件を使用しているルールのリストが空の場合は、ステップ 6 に進みます。リストにルールが含まれている場合は、ルールを書き留めて、ステップ 5 に進みます。

5. クロスサイトスクリプティング一致条件を使用しているルールから、この条件を削除するには、次のステップを実行します。

   a. ナビゲーションペインで [Rules] (ルール) を選択します。
   b. 削除するクロスサイトスクリプティング一致条件を使用しているルールの名前を選択します。
   c. 右ペインで、ルールから削除するクロスサイトスクリプティング一致条件を選択し、[Remove selected condition] (選択した条件を削除) を選択します。
   d. 削除するクロスサイトスクリプティング一致条件を使用しているすべての残りのルールに対してステップ b とステップ c を繰り返します。
   e. ナビゲーションペインで、[Cross-site scripting] (クロスサイトスクリプティング) を選択します。
   f. [Cross-site scripting match conditions] (クロスサイトスクリプティング一致条件) ペインで、削除するクロスサイトスクリプティング一致条件を選択します。

6. [Delete] (削除) を選択して、選択した条件を削除します。

IP 一致条件の使用

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

リクエストの送信元の IP アドレスに基づいてウェブリクエストを許可またはブロックする場合は、IP 一致条件を作成します。IP 一致条件は、リクエストの送信元の IP アドレスまたは IP アドレス範囲を 10,000 件までリストアップします。後でウェブ ACL を作成するときに、これらの IP アドレスからのリクエストを許可するかブロックするかを指定します。

トピック

- IP 一致条件の作成
- IP 一致条件の編集
- IP 一致条件の削除

IP 一致条件の作成

リクエストの送信元の IP アドレスに基づいて許可またはブロックするウェブリクエストを選り分けるには、許可する IP アドレス用に 1 つの IP 一致条件を作成し、ブロックする IP アドレス用に別の IP 一致条件を作成します。

> **Note**
>
> IP 一致条件をルールに追加すると、条件で指定した IP アドレスから発信されないウェブリクエストを許可またはブロックするように AWS WAF Classic を設定することもできます。

IP 一致条件を作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. ナビゲーションペインで、[IP addresses] (IP アドレス) を選択します。
3. [Create condition] (条件を作成) を選択します。
4. [Name] (名前) フィールドに名前を入力します。

   名前に使用できるのは英数字 (A～Z、a～z、0～9) または特殊文字 _-!"#`+*},./ です。一度作成した条件の名前は変更できません。
5. 正しい IP バージョンを選択し、IP アドレスまたは IP アドレス範囲を CIDR 表記で指定します。次に例を示します。

   - IPv4 アドレス 192.0.2.44 を指定するには、192.0.2.44/32 と入力します。
   - IPv6 アドレス 0:0:0:0:0:ffff:c000:22c を指定するには、0:0:0:0:0:ffff:c000:22c/128 と入力します。
   - IPv4 アドレス範囲 192.0.2.0～192.0.2.255 を指定するには、192.0.2.0/24 と入力します。
   - IPv6 アドレス範囲の 2620:0:2d0:200:0:0:0:0～2620:0:2d0:200:ffff:ffff:ffff:ffff を指定するには、2620:0:2d0:200::/64 と入力します。

   AWS WAF Classic は IPv4 アドレス範囲 /8 および /16 から /32 までの任意の範囲をサポートします。 AWS WAF Classic は IPv6 アドレス範囲 /24、/32、/48、/56、/64、/128 をサポートしています。CIDR 表記の詳細については、Wikipedia の「Classless Inter-Domain Routing」(クラスレスドメイン間ルーティング) を参照してください。
6. [Add another IP address or range] (別の IP アドレスまたは範囲を追加) を選択します。
7. 別の IP アドレスまたは IP アドレス範囲を追加する場合は、ステップ 5～6 を繰り返します。
8. 値の追加が終了したら、[Create IP match condition] (IP 一致条件を作成) を選択します。

IP 一致条件の編集

IP 一致条件の IP アドレス範囲を追加または削除できます。範囲を変更するには、新しい範囲を追加して古い範囲を削除します。

IP 一致条件を編集するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. ナビゲーションペインで、[IP addresses] (IP アドレス) を選択します。
3. [IP match conditions] (IP 一致条件) ペインで、編集する IP 一致条件を選択します。
4. IP アドレス範囲を追加するには:

   a. ナビゲーションペインで、[Add IP address or range] (IP アドレスまたは範囲を追加) を選択します。

   b. 正しい IP バージョンを選択し、IP アドレス範囲を CIDR 表記で入力します。次に例を示します。

      - IPv4 アドレス 192.0.2.44 を指定するには、192.0.2.44/32 と入力します。
      - IPv6 アドレス 0:0:0:0:0:ffff:c000:22c を指定するには、0:0:0:0:0:ffff:c000:22c/128 と入力します。
      - IPv4 アドレス範囲 192.0.2.0 ~ 192.0.2.255 を指定するには、192.0.2.0/24 と入力します。
      - IPv6 アドレス範囲の 2620:0:2d0:200:0:0:0:0 ~ 2620:0:2d0:200:ffff:ffff:ffff:ffff を指定するには、2620:0:2d0:200::/64 と入力します。

      AWS WAF Classic は IPv4 アドレス範囲 /8 および /16 から /32 までの任意の範囲をサポートします。 AWS WAF Classic は IPv6 アドレス範囲 /24、/32、/48、/56、/64、/128 をサポートしています。CIDR 表記の詳細については、Wikipedia の「Classless Inter-Domain Routing」(クラスレスドメイン間ルーティング) を参照してください。

   c. IP アドレスをさらに追加するには、[Add another IP address] (別の IP アドレスの追加) を選択して、その値を入力します。

   d. [Add] (追加) を選択します。
5. IP アドレスまたは IP アドレス範囲を削除するには:

   a. 右ペインで、削除する値を選択します。

   b. [Delete IP address or range] (IP アドレスまたは範囲を削除) を選択します。

IP 一致条件の削除

IP 一致条件を削除するには、最初にすべての IP アドレスおよび IP アドレス範囲を条件から削除し、その条件を使用しているすべてのルールから条件自体を削除します。次に手順を示します。

IP 一致条件を削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. ナビゲーションペインで、[IP addresses] (IP アドレス) を選択します。
3. [IP match conditions] (IP 一致条件) ペインで、削除する IP 一致条件を選択します。
4. 右ペインで、[Rules] (ルール) タブを選択します。

   この IP 一致条件を使用しているルールのリストが空の場合は、ステップ 6 に進みます。リストにルールが含まれている場合は、ルールを書き留めて、ステップ 5 に進みます。
5. IP 一致条件を使用しているルールから、この条件を削除するには、次のステップを実行します。

   a. ナビゲーションペインで [Rules] (ルール) を選択します。

   b. 削除する IP 一致条件を使用しているルールの名前を選択します。

   c. 右ペインで、ルールから削除する IP 一致条件を選択し、[Remove selected condition] (選択した条件を削除) を選択します。

   d. 削除する IP 一致条件を使用しているすべての残りのルールに対してステップ b とステップ c を繰り返します。

   e. ナビゲーションペインで、[IP match conditions] (IP 一致条件) を選択します。

   f. [IP match conditions] (IP 一致条件) ペインで、削除する IP 一致条件を選択します。
6. [Delete] (削除) を選択して、選択した条件を削除します。

Geo (地理的) 一致条件の使用

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

リクエスト送信元の国に基づいてウェブリクエストを許可またはブロックする場合は、Geo 一致条件を作成します。Geo 一致条件は、リクエスト送信元の国のリストを返します。後でウェブ ACL を作成するときに、それらの国からのリクエストを許可するかブロックするかを指定します。

地理的一致条件を他の AWS WAF Classic 条件またはルールとともに使用して、高度なフィルタリングを構築できます。例えば、特定の国をブロックするがその国の特定の IP アドレスを許可する場合は、Geo 一致条件と IP 一致条件を含むルールを作成できます。その国から送信され、かつ承認済みの IP アドレスと一致しないリクエストをブロックするようにルールを設定します。別の例として、特定の国のユーザーのリソースを優先させる場合は、2 つの異なるレートベースのルールに Geo 一致条件を含めることができます。優先させる国のユーザーのレート制限をより高く設定し、他のすべてのユーザーのレート制限をより低く設定します。

> **Note**
>
> CloudFront の地理制限機能を使用して国がコンテンツにアクセスするのをブロックしている場合、その国からのリクエストはブロックされ、 AWS WAF Classic に転送されません。したがって、地理的条件とその他の AWS WAF Classic 条件に基づいてリクエストを許可またはブロックする場合は、CloudFront の地理的制限機能を使用しないでください。代わりに、AWS WAF Classic の地理的一致条件を使用する必要があります。

トピック

- Geo 一致条件の作成
- Geo 一致条件の編集
- Geo 一致条件の削除

Geo 一致条件の作成

リクエスト送信元の国に基づいて許可またはブロックするウェブリクエストを選り分けるには、許可する国用に 1 つの Geo 一致条件を作成し、ブロックする国用に別の Geo 一致条件を作成します。

> **Note**
>
> ルールに地理的一致条件を追加すると、条件で指定した国から発信されていないウェブリクエストを許可またはブロックするように AWS WAF Classic を設定することもできます。

Geo 一致条件を作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示されている場合は、それを選択します。
2. ナビゲーションペインで、[Geo match] (Geo 一致) を選択します。
3. [Create condition] (条件を作成) を選択します。
4. [Name] (名前) フィールドに名前を入力します。

   名前に使用できるのは英数字 (A～Z、a～z、0～9) または特殊文字 _-!"#`+*},./ です。一度作成した条件の名前は変更できません。
5. [Region] (リージョン) を選択します。
6. [Location type] (場所のタイプ) と国を選択します。現時点では、[Location type] (場所のタイプ) は [Country] (国) にのみ設定できます。
7. [Add location] (場所を追加) を選択します。
8. [Create] (作成) を選択します。

Geo 一致条件の編集

Geo 一致条件に対して国を追加したり削除したりできます。

Geo 一致条件を編集するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. ナビゲーションペインで、[Geo match] (Geo 一致) を選択します。
3. [Geo match conditions] (Geo 一致条件) ペインで、編集する Geo 一致条件を選択します。
4. 国を追加するには:

   a. 右側のペインで、[Add filter] (フィルターを追加) を選択します。

   b. [Location type] (場所のタイプ) と国を選択します。現時点では、[Location type] (場所のタイプ) は [Country] (国) にのみ設定できます。

   c. [Add] (追加) を選択します。
5. 国を削除するには:

   a. 右ペインで、削除する値を選択します。

   b. [Delete filter] (フィルターを削除) を選択します。

Geo 一致条件の削除

Geo 一致条件を削除するには、まずその条件からすべての国を削除し、その条件を使用しているすべてのルールから条件自体を削除します。その手順を次に示します。

Geo 一致条件を削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. Geo 一致条件を使用しているルールからその条件を削除します。

a. ナビゲーションペインで [Rules] (ルール) を選択します。
b. 削除する Geo 一致条件を使用しているルールの名前を選択します。
c. 右側のペインで、[Edit rule] (ルールを編集) を選択します。
d. 削除する条件の横にある [X] を選択します。
e. [Update] (更新) を選択します。
f. 削除する Geo 一致条件を使用している残りのすべてのルールに対してこの同じ手順を繰り返します。

3. 削除する条件からフィルターを削除します。
   a. ナビゲーションペインで、[Geo match] (Geo 一致) を選択します。
   b. 削除する Geo 一致条件の名前を選択します。
   c. 右側のペインで、[Filter] (フィルター) の横にあるチェックボックスをオンにして、すべてのフィルターを選択します。
   d. [Delete filter] (フィルターを削除) を選択します。
4. ナビゲーションペインで、[Geo match] (Geo 一致) を選択します。
5. [Geo match conditions] (Geo 一致条件) ペインで、削除する Geo 一致条件を選択します。
6. [Delete] (削除) を選択して、選択した条件を削除します。

サイズ制約条件の使用

Warning

AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

Note

これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

指定したウェブリクエスト部分の長さに基づいてリクエストを許可またはブロックする場合は、サイズ制約条件を作成します。サイズ制約条件は、 AWS WAF Classic が参照するウェブリクエストの部分、 AWS WAF Classic が検索するバイト数、および大なり (>) や小なり (<) などの演算子を識別します。例えば、サイズ制約条件を使用して 100 バイトよりも長いクエリ文字列を探すことができます。後でウェブ ACL を作成するときに、これらの設定に基づいてリクエストを許可するかブロックするかを指定します。

例えば、指定した文字列の本文を検索してリクエスト本文を検査するように AWS WAF Classic を設定すると、 AWS WAF Classic は最初の 8192 バイト (8 KB) のみを検査することに注意してください。ウェブリクエストの本文が 8192 バイトを超えない場合は、サイズ制約条件を作成して、8192 バイトを超える本文を持つリクエストをブロックできます。

トピック

- サイズ制約条件の作成
- サイズ制約条件の作成時または編集時に指定する値
- サイズ制約条件のフィルターの追加と削除
- サイズ制約条件の削除

サイズ制約条件の作成

サイズ制約条件を作成するときは、 AWS WAF Classic で長さを評価するウェブリクエストの部分を識別するフィルターを指定します。サイズ制約条件には複数のフィルターを追加できます。条件ごとに 1 つのフィルターを設定することもできます。各設定が AWS WAF Classic の動作にどのように影響するかを次に示します。

- サイズ制約条件ごとに 1 つのフィルター – ルールに個別のサイズ制約条件を追加し、ウェブ ACL にルールを追加する場合、ウェブリクエストは AWS WAF Classic が条件に基づいてリクエストを許可またはブロックするすべての条件と一致する必要があります。

  例えば、2 つの条件を作成するとします。1 つの条件は、クエリ文字列が 100 バイトを超えるウェブリクエストに一致します。もう 1 つの条件は、リクエストボディが 1024 バイトを超えるウェブリクエストに一致します。両方の条件を同じルールに追加し、そのルールをウェブ ACL に追加すると、 AWS WAF Classic は両方の条件が true の場合にのみリクエストを許可または拒否します。
- サイズ制約条件ごとに複数のフィルター – ルールに複数のフィルターを含むサイズ制約条件を追加し、ウェブ ACL にルールを追加する場合、ウェブリクエストはサイズ制約条件のフィルターの

1 つと一致するだけで、 AWS WAF Classic はその条件に基づいてリクエストを許可またはブロックします。

2 つの条件ではなく 1 つの条件を作成し、1 つの条件に前の例と同じ 2 つのフィルターが含まれているとします。 AWS WAF Classic は、クエリ文字列が 100 バイトより大きいか、リクエスト本文が 1024 バイトより大きい場合にリクエストを許可またはブロックします。

> **Note**
>
> ルールにサイズ制約条件を追加すると、条件の値と一致しないウェブリクエストを許可またはブロックするように AWS WAF Classic を設定することもできます。

サイズ制約条件を作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示されている場合は、それを選択します。
2. ナビゲーションペインで、[Size constraints] (サイズ制約) を選択します。
3. [Create condition] (条件を作成) を選択します。
4. 適用するフィルター設定を指定します。詳細については、「サイズ制約条件の作成時または編集時に指定する値」を参照してください。
5. [Add another filter] (別のフィルターを追加) を選択します。
6. 別のフィルターを追加する場合は、ステップ 4～5 を繰り返します。
7. フィルターの追加が完了したら、[Create size constraint condition] (サイズ制約の条件を作成) を選択します。

サイズ制約条件の作成時または編集時に指定する値

サイズ制約条件を作成または更新するときに、次の値を指定します。

[Name] (名前)

サイズ制約条件の名前を入力します。

名前に使用できるのは英数字 (A～Z、a～z、0～9) または特殊文字 _-!"#`+*},./ です。一度作成した条件の名前は変更できません。

[Part of the request to filter on] (フィルタリングするリクエストの一部)

AWS WAF Classic で長さを評価する各ウェブリクエストの部分を選択します。

ヘッダー

指定したリクエストヘッダー (`User-Agent` や `Referer` など)。[Header] (ヘッダー) を選択した場合は、[Header] (ヘッダー) フィールドにヘッダー名を指定します。

[HTTP method] (HTTP メソッド)

リクエストがオリジンに実行を要求しているオペレーションのタイプを示す HTTP メソッド。CloudFront がサポートしているメソッドは、`DELETE`、`GET`、`HEAD`、`OPTIONS`、`PATCH`、`POST`、および `PUT` です。

[Query string] (クエリ文字列)

URL 内で ? 文字の後に続く部分 (ある場合)。

[URI]

リクエストの URI パス。リソースを識別します (例: `/images/daily-ad.jpg`)。これには、URI のクエリ文字列またはフラグメントコンポーネントは含まれません。詳細については、「Uniform Resource Identifier (URI): 一般的な構文」を参照してください。

変換が指定されていない限り、URI は正規化されず、リクエストの一部としてクライアントから AWS 受け取ったのと同じように検査されます。[Transformation] (変換) が指定されている場合、URI はその指定に従って形式が再設定されます。

[Body] (本文)

リクエスト内で、HTTP リクエストの本文としてウェブサーバーに送信する追加データ (フォームのデータなど) を含む部分。

[Single query parameter (value only)] (単一クエリパラメータ (値のみ))

クエリ文字列の一部として定義されているすべてのパラメータです。例えば、URL が「www.xyz.com?UserName=abc&SalesRegion=seattle」である場合、UserName または SalesRegion パラメータにフィルターを追加できます。

[Single query parameter (value only)] (単一クエリパラメータ (値のみ)) を選択する場合は、[Query parameter name] (クエリパラメータ名) も指定します。これは検査するクエリ文

字列のパラメータです (UserName など)。[Query parameter name] (クエリパラメータ名) の最大長は 30 文字です。[Query parameter name] (クエリパラメータ名) では、大文字と小文字は区別されません。例えば、UserName を [Query parameter name] (クエリパラメータ名) として指定すると、username や UsERName など UserName のすべてのバリエーションに一致します。

[All query parameters (values only)] (すべてのクエリパラメータ (値のみ))

単一クエリパラメータ (値のみ) に似ていますが、単一パラメータの値を検査するのではなく、 AWS WAF Classic はクエリ文字列内のすべてのパラメータの値のサイズ制約を検査します。例えば、URL が「www.xyz.com?UserName=abc&SalesRegion=seattle」の場合、[All query parameters (values only)] (すべてのクエリパラメータ (値のみ)) を選択すると、UserName または SalesRegion のいずれかの値が指定されたサイズを超過している場合、 AWS WAF Classic によって一致がトリガーされます。

[Header] (ヘッダー) ([Part of the request to filter on] (フィルタリングするリクエストの一部) が [Header] (ヘッダー) の場合のみ)

フィルタリングするリクエストの一部のヘッダーを選択した場合は、一般的なヘッダーのリストからヘッダーを選択するか、 AWS WAF Classic で長さを評価するヘッダーの名前を入力します。

Comparison operator (比較演算子)

Classic で AWS WAF 、サイズに指定した値に関してウェブリクエストのクエリ文字列の長さを評価する方法を選択します。

例えば、比較演算子に Is greater than を選択し、サイズに 100 と入力すると、 AWS WAF Classic は 100 バイトを超えるクエリ文字列のウェブリクエストを評価します。

サイズ

AWS WAF Classic がクエリ文字列で監視する長さをバイト単位で入力します。

> **Note**
>
> [Part of the request to filter on] (フィルタリングするリクエストの一部) の値に [URI] を選択した場合、URI の / は 1 文字としてカウントされます。例えば、URI パスの `/logo.jpg` は 9 文字の長さになります。

変換

変換は、 AWS WAF Classic がリクエストの指定された部分の長さを評価する前にウェブリクエストを再フォーマットします。これにより、攻撃者が AWS WAF Classic をバイパスするためにウェブリクエストで使用する異常なフォーマットの一部が排除されます。

> **Note**
>
> フィルタリングするリクエストの一部の本文を選択した場合、最初の 8192 バイトのみが検査に転送されるため、変換を実行するように AWS WAF Classic を設定することはできません。ただし、HTTP リクエストボディのサイズに基づいてトラフィックをフィルタして、[None] (なし) の変換を指定することはできます。(AWS WAF Classic はリクエストヘッダーから本文の長さを取得します) 。

1 種類のテキスト変換しか指定できません。

変換では次の操作を実行できます。

なし

AWS WAF Classic は、長さをチェックする前にウェブリクエストに対してテキスト変換を実行しません。

[Convert to lowercase] (小文字に変換)

AWS WAF Classic は、大文字 (A ~ Z) を小文字 (a ~ z) に変換します。

[HTML decode] (HTML デコード)

AWS WAF Classic は、HTML エンコード文字をエンコードされていない文字に置き換えます。

- `"` を & に置き換えます。
- ` ` を改行なしスペースに置き換えます。
- `<` を < に置き換えます。
- `>` を > に置き換えます。
- 16 進数形式の文字 (`&#xhhhh;`) を対応する文字に置き換えます。
- 10 進数形式の文字 (`&#nnnn;`) を対応する文字に置き換えます。

[Normalize white space] (空白の正規化)

AWS WAF Classic は、次の文字をスペース文字 (10 進数 32) に置き換えます。

- \f、フォームフィード、10 進数 12
- \t、タブ、10 進数 9
- \n、改行、10 進数 10
- \r、キャリッジリターン、10 進数 13
- \v、垂直タブ、10 進数 11
- 改行なしスペース、10 進数 160

さらに、このオプションでは複数のスペースを 1 つのスペースに置き換えます。

[Simplify command line] (コマンドラインを簡素化)

オペレーティングシステムのコマンドラインのコマンドが含まれているリクエストの場合、このオプションを使用して次の変換を行います。

- 次の文字を削除します: \ " ' ^
- 次の文字の前にあるスペースを削除します: / (
- 次の文字をスペースに置き換えます: , ;
- 複数のスペースを 1 つのスペースに置き換えます。
- 大文字 (A〜Z) を小文字 (a〜z) に変換します。

[URL decode] (URL デコード)

URL エンコードされたリクエストをデコードします。

サイズ制約条件のフィルターの追加と削除

サイズ制約条件のフィルターを追加または削除できます。フィルターを変更するには、新しいフィルターを追加して古いフィルターを削除します。

サイズ制約条件のフィルターを追加または削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示されている場合は、それを選択します。
2. ナビゲーションペインで、[Size constraint] (サイズ制約) を選択します。
3. フィルターを追加または削除する対象の条件を選択します。

4. フィルターを追加するには、次のステップを実行します。

   a. [Add filter] (フィルターを追加) を選択します。

   b. 適用するフィルター設定を指定します。詳細については、「サイズ制約条件の作成時または編集時に指定する値」を参照してください。

   c. [Add] (追加) を選択します。

5. フィルターを削除するには、次のステップを実行します。

   a. 削除するフィルターを選択します。

   b. [Delete filter] (フィルターを削除) を選択します。

サイズ制約条件の削除

サイズ制約条件を削除するには、最初にその条件からすべてのフィルターを削除し、その条件を使用しているすべてのルールから条件自体を削除します。次に手順を示します。

サイズ制約条件を削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示されている場合は、それを選択します。

2. ナビゲーションペインで、[Size constraints] (サイズ制約) を選択します。

3. [Size constraint conditions] (サイズ制約の条件) ペインで、削除するサイズ制約の条件を選択します。

4. 右ペインで、[Associated rules] (関連付けられたルール) タブを選択します。

   このサイズ制約条件を使用しているルールのリストが空の場合は、ステップ 6 に進みます。リストにルールが含まれている場合は、ルールを書き留めて、ステップ 5 に進みます。

5. サイズ制約条件を使用しているルールから、この条件を削除するには、次のステップを実行します。

   a. ナビゲーションペインで [Rules] (ルール) を選択します。

   b. 削除するサイズ制約条件を使用しているルールの名前を選択します。

   c. 右ペインで、ルールから削除するサイズ制約条件を選択し、[Remove selected condition] (選択した条件を削除) を選択します。

d. 削除するサイズ制約条件を使用しているすべての残りのルールに対してステップ b とステップ c を繰り返します。

e. ナビゲーションペインで、[Size constraint] (サイズ制約) を選択します。

f. [Size constraint conditions] (サイズ制約の条件) ペインで、削除するサイズ制約の条件を選択します。

6. [Delete] (削除) を選択して、選択した条件を削除します。

SQL インジェクション一致条件の使用

> **Warning**
>
> AWS WAF Classic は計画されたend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

攻撃者は、データベースからデータを取り出そうとしてウェブリクエスト内に悪意のある SQL コードを挿入する場合があります。悪意のある SQL コードが含まれている可能性があるウェブリクエストを許可またはブロックするには、SQL インジェクション一致条件を作成します。SQL インジェクション一致条件は、 AWS WAF Classic が検査する URI パスやクエリ文字列などのウェブリクエストの一部を識別します。後でウェブ ACL を作成するときに、悪意のある SQL コードが含まれている可能性があるリクエストを許可するかブロックするかを指定します。

トピック

- SQL インジェクション一致条件の作成
- SQL インジェクション一致条件の作成時または編集時に指定する値
- SQL インジェクション一致条件のフィルターの追加と削除

- SQL インジェクション一致条件の削除

SQL インジェクション一致条件の作成

SQL インジェクション一致条件を作成するときは、 URI やクエリ文字列などの悪意のある SQL コードを AWS WAF Classic が検査するウェブリクエストの部分を示すフィルターを指定します。SQL インジェクション一致条件には複数のフィルターを追加できます。条件ごとに 1 つのフィルターを設定することもできます。各設定が AWS WAF Classic の動作にどのように影響するかを次に示します。

- SQL インジェクション一致条件ごとに複数のフィルター (推奨) – ルールに複数のフィルターを含む SQL インジェクション一致条件を追加し、ウェブ ACL にルールを追加する場合、ウェブリクエストは AWS WAF 、Classic がその条件に基づいてリクエストを許可またはブロックするために、SQL インジェクション一致条件のフィルターの 1 つと一致するだけで済みます。

  例えば、SQL インジェクション一致条件を 1 つ作成し、この条件に 2 つのフィルターを含めたとします。1 つのフィルターは URI に悪意のある SQL コードを検査するように AWS WAF Classic に指示し、もう 1 つのフィルターはクエリ文字列を検査するように AWS WAF Classic に指示します。 AWS WAF Classic は、URI またはクエリ文字列に悪意のある SQL コードが含まれているように見えるリクエストを許可またはブロックします。
- SQL インジェクション一致条件ごとに 1 つのフィルター – ルールに個別の SQL インジェクション一致条件を追加し、ウェブ ACL にルールを追加する場合、ウェブリクエストは AWS WAF Classic が条件に基づいてリクエストを許可またはブロックするすべての条件と一致する必要があります。

  2 つの条件を作成し、各条件に前の例で示した 2 つのフィルターの 1 つを別個に含めたとします。両方の条件を同じルールに追加し、そのルールをウェブ ACL に追加すると、 AWS WAF Classic は URI とクエリ文字列の両方に悪意のある SQL コードが含まれているように見える場合にのみリクエストを許可または拒否します。

> **Note**
>
> SQL インジェクション一致条件をルールに追加すると、悪意のある SQL コードが含まれていないように見えるウェブリクエストを許可またはブロックするように AWS WAF Classic を設定することもできます。

ステップ 5: SQL インジェクション一致条件を作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示されている場合は、それを選択します。
2. ナビゲーションペインで、[SQL injection] (SQL インジェクション) を選択します。
3. [Create condition] (条件を作成) を選択します。
4. 適用するフィルター設定を指定します。詳細については、「SQL インジェクション一致条件の作成時または編集時に指定する値」を参照してください。
5. [Add another filter] (別のフィルターを追加) を選択します。
6. 別のフィルターを追加する場合は、ステップ 4～5 を繰り返します。
7. フィルターの追加が終了したら、[Create] (作成) を選択します。

SQL インジェクション一致条件の作成時または編集時に指定する値

SQL インジェクション一致条件を作成または更新するときに、次の値を指定します。

[Name] (名前)

SQL インジェクション一致条件の名前。

名前に使用できるのは英数字 (A～Z、a～z、0～9) または特殊文字 _-!"#`+*},./ です。一度作成した条件の名前は変更できません。

[Part of the request to filter on] (フィルタリングするリクエストの一部)

AWS WAF Classic が悪意のある SQL コードを検査する各ウェブリクエストの部分を選択します。

ヘッダー

指定したリクエストヘッダー (`User-Agent` や `Referer` など)。[Header] (ヘッダー) を選択した場合は、[Header] (ヘッダー) フィールドにヘッダー名を指定します。

[HTTP method] (HTTP メソッド)

リクエストがオリジンに実行を要求しているオペレーションのタイプを示す HTTP メソッド。CloudFront がサポートしているメソッドは、`DELETE`、`GET`、`HEAD`、`OPTIONS`、`PATCH`、`POST`、および `PUT` です。

[Query string] (クエリ文字列)

URL 内で ? 文字の後に続く部分 (ある場合)。

> **Note**
>
> SQL インジェクションの一致条件については、[Part of the request to filter on] (フィルタリングするリクエストの一部) に [Query string] (クエリ文字列) ではなく、[All query parameters (values only)] (すべてのクエリパラメータ (値のみ)) を選択することをお勧めします。

[URI]

リクエストの URI パス。リソースを識別します (例: `/images/daily-ad.jpg`)。これには、URI のクエリ文字列またはフラグメントコンポーネントは含まれません。詳細については、「Uniform Resource Identifier (URI): 一般的な構文」を参照してください。

変換が指定されていない限り、URI は正規化されず、リクエストの一部としてクライアントから AWS 受け取ったのと同じように検査されます。[Transformation] (変換) が指定されている場合、URI はその指定に従って形式が再設定されます。

[Body] (本文)

リクエスト内で、HTTP リクエストの本文としてウェブサーバーに送信する追加データ (フォームのデータなど) を含む部分。

> **Note**
>
> [Part of the request to filter on] (フィルタリングするリクエストの一部) の値として [Body] (本文) を選択した場合、 AWS WAF Classic によって最初の 8,192 バイト (8 KB) のみが検査されます。本文が 8,192 バイトより長いリクエストを許可またはブロックするには、サイズ制約条件を作成します。(AWS WAF Classic はリクエストヘッダーから本文の長さを取得します) 。詳細については、「サイズ制約条件の使用」を参照してください。

[Single query parameter (value only)] (単一クエリパラメータ (値のみ))

クエリ文字列の一部として定義されているすべてのパラメータです。例えば、URL が「www.xyz.com?UserName=abc&SalesRegion=seattle」である場合、UserName または SalesRegion パラメータにフィルターを追加できます。

[Single query parameter (value only)] (単一クエリパラメータ (値のみ)) を選択する場合は、[Query parameter name] (クエリパラメータ名) も指定します。これは検査するクエリ文字列のパラメータです (UserName や SalesRegion など)。[Query parameter name] (クエリパラメータ名) の最大長は 30 文字です。[Query parameter name] (クエリパラメータ名) では、大文字と小文字は区別されません。例えば、UserName を [Query parameter name] (クエリパラメータ名) として指定すると、username や UsERName など UserName のすべてのバリエーションに一致します。

[All query parameters (values only)] (すべてのクエリパラメータ (値のみ))

単一クエリパラメータ (値のみ) に似ていますが、単一パラメータの値を検査するのではなく、 AWS WAF Classic はクエリ文字列内のすべてのパラメータの値を検査して、悪意のある SQL コードがないかを確認します。例えば、URL が「www.xyz.com?UserName=abc&SalesRegion=seattle」の場合、[All query parameters (values only)] (すべてのクエリパラメータ (値のみ)) を選択すると、UserName または SalesRegion のいずれかの値に悪意のある可能性がある SQL コードが含まれている場合、 AWS WAF Classic によって一致がトリガーされます。

ヘッダー

フィルタリングするリクエストの一部のヘッダーを選択した場合は、一般的なヘッダーのリストからヘッダーを選択するか、 AWS WAF Classic で悪意のある SQL コードを検査するヘッダーの名前を入力します。

変換

Classic がリクエストを AWS WAF 検査する前に、変換によってウェブリクエストが再フォーマットされます。これにより、攻撃者が AWS WAF Classic をバイパスするためにウェブリクエストで使用する異常なフォーマットの一部が排除されます。

1 種類のテキスト変換しか指定できません。

変換では次の操作を実行できます。

なし

AWS WAF Classic は、値の文字列が一致するかどうかを検査する前に、ウェブリクエストに対してテキスト変換を実行しません。

[Convert to lowercase] (小文字に変換)

AWS WAF Classic は、大文字 (A ~ Z) を小文字 (a ~ z) に変換します。

[HTML decode] (HTML デコード)

AWS WAF Classic は、HTML エンコード文字をエンコードされていない文字に置き換えます。

- `"` を & に置き換えます。
- ` ` を改行なしスペースに置き換えます。
- `<` を < に置き換えます。
- `>` を > に置き換えます。
- 16 進数形式の文字 (`&#xhhhh;`) を対応する文字に置き換えます。
- 10 進数形式の文字 (`&#nnnn;`) を対応する文字に置き換えます。

[Normalize white space] (空白の正規化)

AWS WAF Classic は、次の文字をスペース文字 (10 進数 32) に置き換えます。

- \f、フォームフィード、10 進数 12
- \t、タブ、10 進数 9
- \n、改行、10 進数 10
- \r、キャリッジリターン、10 進数 13
- \v、垂直タブ、10 進数 11
- 改行なしスペース、10 進数 160

さらに、このオプションでは複数のスペースを 1 つのスペースに置き換えます。

[Simplify command line] (コマンドラインを簡素化)

オペレーティングシステムのコマンドラインのコマンドが含まれているリクエストの場合、このオプションを使用して次の変換を行います。

- 次の文字を削除します: \ " ' ^
- 次の文字の前にあるスペースを削除します: / (

- 次の文字をスペースに置き換えます: , ;
- 複数のスペースを 1 つのスペースに置き換えます。
- 大文字 (A〜Z) を小文字 (a〜z) に変換します。

[URL decode] (URL デコード)

URL エンコードされたリクエストをデコードします。

SQL インジェクション一致条件のフィルターの追加と削除

SQL インジェクション一致条件のフィルターを追加または削除できます。フィルターを変更するには、新しいフィルターを追加して古いフィルターを削除します。

SQL インジェクション一致条件のフィルターを追加または削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. ナビゲーションペインで、[SQL injection] (SQL インジェクション) を選択します。
3. フィルターを追加または削除する対象の条件を選択します。
4. フィルターを追加するには、次のステップを実行します。

   a. [Add filter] (フィルターを追加) を選択します。

   b. 適用するフィルター設定を指定します。詳細については、「SQL インジェクション一致条件の作成時または編集時に指定する値」を参照してください。

   c. [Add] (追加) を選択します。
5. フィルターを削除するには、次のステップを実行します。

   a. 削除するフィルターを選択します。

   b. [Delete filter] (フィルターを削除) を選択します。

SQL インジェクション一致条件の削除

SQL インジェクション一致条件を削除するには、最初にその条件からすべてのフィルターを削除し、その条件を使用しているすべてのルールから条件自体を削除します。次に手順を示します。

SQL インジェクション一致条件を削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. ナビゲーションペインで、[SQL injection] (SQL インジェクション) を選択します。
3. [SQL injection match conditions] (SQL インジェクション一致条件) ペインで、削除する SQL インジェクション一致条件を選択します。
4. 右ペインで、[Associated rules] (関連付けられたルール) タブを選択します。

   この SQL インジェクション一致条件を使用しているルールのリストが空の場合は、ステップ 6 に進みます。リストにルールが含まれている場合は、ルールを書き留めて、ステップ 5 に進みます。
5. SQL インジェクション一致条件を使用しているルールから、この条件を削除するには、次のステップを実行します。

   a. ナビゲーションペインで [Rules] (ルール) を選択します。
   b. 削除する SQL インジェクション一致条件を使用しているルールの名前を選択します。
   c. 右ペインで、ルールから削除する SQL インジェクション一致条件を選択し、[Remove selected condition] (選択した条件を削除) を選択します。
   d. 削除する SQL インジェクション一致条件を使用しているすべての残りのルールに対してステップ b とステップ c を繰り返します。
   e. ナビゲーションペインで、[SQL injection] (SQL インジェクション) を選択します。
   f. [SQL injection match conditions] (SQL インジェクション一致条件) ペインで、削除する SQL インジェクション一致条件を選択します。
6. [Delete] (削除) を選択して、選択した条件を削除します。

文字列一致条件の使用

> **Warning**
>
> AWS WAF Classic は計画されたend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

ウェブリクエストに表示される文字列に基づいてリクエストを許可またはブロックする場合は、文字列一致条件を作成します。文字列一致条件は、検索する文字列と、指定されたヘッダーやクエリ文字列など、 AWS WAF Classic が文字列を検査するウェブリクエストの一部を識別します。後でウェブ ACL を作成するときに、文字列を含むリクエストを許可するかブロックするかを指定します。

トピック

- 文字列一致条件の作成
- 文字列一致条件の作成時または編集時に指定する値
- 文字列一致条件のフィルターの追加と削除
- 文字列一致条件の削除

文字列一致条件の作成

文字列一致条件を作成するときは、検索する文字列と、URI やクエリ文字列など、 AWS WAF Classic がその文字列を検査するウェブリクエストの部分を識別するフィルターを指定します。文字列一致条件には複数のフィルターを追加できます。文字列一致条件ごとに 1 つのフィルターを設定することもできます。各設定が AWS WAF Classic の動作にどのように影響するかを次に示します。

- 文字列一致条件ごとに 1 つのフィルター – 個別の文字列一致条件をルールに追加し、ウェブ ACL にルールを追加する場合、 AWS WAF ウェブリクエストは Classic が条件に基づいてリクエストを許可またはブロックするすべての条件と一致する必要があります。

  例えば、2 つの条件を作成するとします。1 つの条件は、`User-Agent` ヘッダーに値 `BadBot` が含まれているウェブリクエストに一致します。もう 1 つの条件は、クエリ文字列に値 `BadParameter` が含まれているウェブリクエストに一致します。両方の条件を同じルールに追加し、そのルールをウェブ ACL に追加すると、 AWS WAF Classic は両方の値が含まれている場合にのみリクエストを許可または拒否します。

- 文字列一致条件ごとに複数のフィルタ – 複数のフィルタを含む文字列一致条件をルールに追加し、そのルールをウェブ ACL に追加すると、ウェブリクエストは、1 つの条件に基づいて AWS WAF Classic がリクエストを許可またはブロックするために、文字列一致条件のいずれかのフィルタと一致するだけで済みます。

  2 つの条件ではなく 1 つの条件を作成し、1 つの条件に前の例と同じ 2 つのフィルターが含まれているとします。 AWS WAF Classic は`User-Agent`、ヘッダーまたはクエリ文字列`BadBot`のいずれかに が含まれている場合、リクエストを許可またはブロック`BadParameter`します。

> **Note**
>
> 文字列一致条件をルールに追加すると、条件の値と一致しないウェブリクエストを許可またはブロックするように AWS WAF Classic を設定することもできます。

文字列一致条件を作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. ナビゲーションペインで、[String and regex matching] (文字列および正規表現の一致) を選択します。
3. [Create condition] (条件を作成) を選択します。
4. 適用するフィルター設定を指定します。詳細については、「文字列一致条件の作成時または編集時に指定する値」を参照してください。
5. [Add filter] (フィルターを追加) を選択します。
6. 別のフィルターを追加する場合は、ステップ 4～5 を繰り返します。
7. フィルターの追加が終了したら、[Create] (作成) を選択します。

文字列一致条件の作成時または編集時に指定する値

文字列一致条件を作成または更新するときに、次の値を指定します。

[Name] (名前)

文字列一致条件の名前を入力します。名前に使用できるのは英数字 (A～Z、a～z、0～9) または特殊文字 _-!"#`+*},./ です。一度作成した条件の名前は変更できません。

[Type] (タイプ)

[String match] (文字列の一致) を選択します。

[Part of the request to filter on] (フィルタリングするリクエストの一部)

AWS WAF Classic が検査する各ウェブリクエストの部分を選択し、一致する値で指定した文字列を探します。

ヘッダー

指定したリクエストヘッダー (`User-Agent` や `Referer` など)。[Header] (ヘッダー) を選択した場合は、[Header] (ヘッダー) フィールドにヘッダー名を指定します。

[HTTP method] (HTTP メソッド)

リクエストがオリジンに実行を要求しているオペレーションのタイプを示す HTTP メソッド。CloudFront がサポートしているメソッドは、`DELETE`、`GET`、`HEAD`、`OPTIONS`、`PATCH`、`POST`、および `PUT` です。

[Query string] (クエリ文字列)

URL 内で ? 文字の後に続く部分 (ある場合)。

[URI]

リクエストの URI パス。リソースを識別します (例: `/images/daily-ad.jpg`)。これには、URI のクエリ文字列またはフラグメントコンポーネントは含まれません。詳細については、「Uniform Resource Identifier (URI): 一般的な構文」を参照してください。

変換が指定されていない限り、URI は正規化されず、リクエストの一部としてクライアントから AWS 受け取ったのと同じように検査されます。[Transformation] (変換) が指定されている場合、URI はその指定に従って形式が再設定されます。

[Body] (本文)

リクエスト内で、HTTP リクエストの本文としてウェブサーバーに送信する追加データ (フォームのデータなど) を含む部分。

> **Note**
>
> [Part of the request to filter on] (フィルタリングするリクエストの一部) の値として [Body] (本文) を選択した場合、 AWS WAF Classic によって最初の 8,192 バイト (8 KB) のみが検査されます。本文が 8,192 バイトより長いリクエストを許可またはブロックするには、サイズ制約条件を作成します。(AWS WAF Classic はリクエストヘッダーから本文の長さを取得します) 。詳細については、「サイズ制約条件の使用」を参照してください。

[Single query parameter (value only)] (単一クエリパラメータ (値のみ))

クエリ文字列の一部として定義されているすべてのパラメータです。例えば、URL が「www.xyz.com?UserName=abc&SalesRegion=seattle」である場合、UserName または SalesRegion パラメータにフィルターを追加できます。

重複したパラメータがクエリ文字列に記述される場合、値は「OR」として評価されます。つまり、いずれかの値によって一致がトリガーされます。例えば、「www.xyz.com?SalesRegion=boston&SalesRegion=seattle」という URL では、[Value to match] (一致する値) に「boston」または「seattle」を指定すると、一致がトリガーされます。

[Single query parameter (value only)] (単一クエリパラメータ (値のみ)) を選択する場合は、[Query parameter name] (クエリパラメータ名) も指定します。これは検査するクエリ文字列のパラメータです (UserName や SalesRegion など)。[Query parameter name] (クエリパラメータ名) の最大長は 30 文字です。[Query parameter name] (クエリパラメータ名) では、大文字と小文字は区別されません。例えば、UserName を [Query parameter name] (クエリパラメータ名) として指定すると、username や UsERName など UserName のすべてのバリエーションに一致します。

[All query parameters (values only)] (すべてのクエリパラメータ (値のみ))

単一クエリパラメータ (値のみ) に似ていますが、単一パラメータの値を検査するのではなく、 AWS WAF Classic はクエリ文字列内のすべてのパラメータの値を検査して、一致する値を探します。例えば、URL が「www.xyz.com?UserName=abc&SalesRegion=seattle」の場合、[All query parameters (values only)] (すべてのクエリパラメータ (値のみ)) を選択すると、UserName または SalesRegion のいずれかの値が [Value to match] (一致する値) として指定されている場合、 AWS WAF Classic によって一致がトリガーされます。

[Header] (ヘッダー) ([Part of the request to filter on] (フィルタリングするリクエストの一部) が [Header] (ヘッダー) の場合のみ)

リストからフィルタリングするリクエストのパートからヘッダーを選択した場合は、一般的なヘッダーのリストからヘッダーを選択するか、 AWS WAF Classic が検査するヘッダーの名前を入力します。

[Match type] (一致タイプ)

AWS WAF Classic が検査するリクエストの部分内で、一致する値の文字列がこのフィルターと一致するように表示する必要がある場所を選択します。

[Contains] (次を含む)

文字列は、指定したリクエスト部分内の任意の場所に表示されます。

[Contains word] (単語を含む)

指定したウェブリクエスト部分には [Value to match] (一致する値) が含まれていること、[Value to match] (一致する値) には英数字または下線 (A〜Z、a〜z、0〜9、_) のみが含まれていることが必要です。さらに、[Value to match] (一致する値) は単語であること、つまり、次のいずれかであることが必要です。

- [Value to match] (一致する値) は、指定したウェブリクエスト部分 (ヘッダーの値など) の値と正確に一致する。
- [Value to match] (一致する値) は、指定したウェブリクエスト部分の先頭にあり、英数字または下線 (_) 以外の文字が続く (例: `BadBot;`)。
- [Value to match] (一致する値) は、指定したウェブリクエスト部分の末尾にあり、英数字または下線 (_) 以外の文字が続く (例: `;BadBot`)。
- [Value to match] (一致する値) は、指定したウェブリクエスト部分の中央にあり、英数字または下線 (_) 以外の文字が前後にある (例: `-BadBot;`)。

[Exactly matches] (完全に一致)

文字列と指定したリクエスト部分の値が正確に一致します。

[Starts with] (次で開始)

文字列は指定したリクエスト部分の先頭にあります。

[Ends with] (次で終了)

文字列は指定したリクエスト部分の末尾にあります。

変換

Classic がリクエストを AWS WAF 検査する前に、変換によってウェブリクエストが再フォーマットされます。これにより、攻撃者が AWS WAF Classic をバイパスするためにウェブリクエストで使用する異常なフォーマットの一部が排除されます。

1 種類のテキスト変換しか指定できません。

変換では次の操作を実行できます。

なし

AWS WAF Classic は、値の文字列が一致するかどうかを検査する前に、ウェブリクエストに対してテキスト変換を実行しません。

[Convert to lowercase] (小文字に変換)

AWS WAF Classic は、大文字 (A ~ Z) を小文字 (a ~ z) に変換します。

[HTML decode] (HTML デコード)

AWS WAF Classic は、HTML エンコード文字をエンコードされていない文字に置き換えます。

- `"` を & に置き換えます。
- ` ` を改行なしスペースに置き換えます。
- `<` を < に置き換えます。
- `>` を > に置き換えます。
- 16 進数形式の文字 (`&#xhhhh;`) を対応する文字に置き換えます。
- 10 進数形式の文字 (`&#nnnn;`) を対応する文字に置き換えます。

[Normalize white space] (空白の正規化)

AWS WAF Classic は、次の文字をスペース文字 (10 進数 32) に置き換えます。

- \f、フォームフィード、10 進数 12
- \t、タブ、10 進数 9
- \n、改行、10 進数 10
- \r、キャリッジリターン、10 進数 13
- \v、垂直タブ、10 進数 11
- 改行なしスペース、10 進数 160

さらに、このオプションでは複数のスペースを 1 つのスペースに置き換えます。

[Simplify command line] (コマンドラインを簡素化)

攻撃者がオペレーティングシステムのコマンドラインのコマンドを挿入し、通常と異なるフォーマットを使用してコマンドの一部または全部を偽装するおそれがある場合は、このオプションを使用して次の変換を行います。

- 次の文字を削除します: \ " ' ^
- 次の文字の前にあるスペースを削除します: / (
- 次の文字をスペースに置き換えます: , ;
- 複数のスペースを 1 つのスペースに置き換えます。
- 大文字 (A〜Z) を小文字 (a〜z) に変換します。

[URL decode] (URL デコード)

URL エンコードされたリクエストをデコードします。

[Value is base64 encoded] (値が base64 エンコードされている)

[Value to match] (一致する値) の値が base64 でエンコードされている場合は、このチェックボックスをオンにします。Base64 エンコーディングを使用して、攻撃者がリクエストに含める表示不可能な文字 (タブや改行など) を指定します。

[Value to match] (照合する値)

AWS WAF Classic がウェブリクエストで検索する値を指定します。最大長は 50 バイトです 値を Base 64 でエンコードする場合は、エンコードする前の値に 50 バイトの最大長が適用されます。

文字列一致条件のフィルターの追加と削除

文字列一致条件のフィルターを追加または削除できます。フィルターを変更するには、新しいフィルターを追加して古いフィルターを削除します。

文字列一致条件のフィルターを追加または削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. ナビゲーションペインで、[String and regex matching] (文字列および正規表現の一致) を選択します。

3. フィルターを追加または削除する対象の条件を選択します。
4. フィルターを追加するには、次のステップを実行します。

   a. [Add filter] (フィルターを追加) を選択します。
   b. 適用するフィルター設定を指定します。詳細については、「文字列一致条件の作成時または編集時に指定する値」を参照してください。
   c. [Add] (追加) を選択します。
5. フィルターを削除するには、次のステップを実行します。

   a. 削除するフィルターを選択します。
   b. [Delete filter] (フィルターを削除) を選択します。

文字列一致条件の削除

文字列一致条件を削除するには、最初にその条件からすべてのフィルターを削除し、その条件を使用しているすべてのルールから条件自体を削除します。次に手順を示します。

文字列一致条件を削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. 文字列一致条件を使用しているルールからその条件を削除します。

   a. ナビゲーションペインで [Rules] (ルール) を選択します。
   b. 削除する文字列一致条件を使用しているルールの名前を選択します。
   c. 右側のペインで、[Edit rule] (ルールを編集) を選択します。
   d. 削除する条件の横にある [X] を選択します。
   e. [Update] (更新) を選択します。
   f. 削除する文字列一致条件を使用している残りのすべてのルールに対してこの同じ手順を繰り返します。
3. 削除する条件からフィルターを削除します。

   a. ナビゲーションペインで、[String and regex matching] (文字列および正規表現の一致) を選択します。

b. 削除する文字列一致条件の名前を選択します。

c. 右側のペインで、[Filter] (フィルター) の横にあるチェックボックスをオンにして、すべてのフィルターを選択します。

d. [Delete filter] (フィルターを削除) を選択します。

4. ナビゲーションペインで、[String and regex matching] (文字列および正規表現の一致) を選択します。

5. [String and regex match conditions] (文字列および正規表現の一致条件) ペインで、削除する文字列一致条件を選択します。

6. [Delete] (削除) を選択して、選択した条件を削除します。

正規表現一致条件の使用

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

リクエストに含まれる正規表現パターンと一致する文字列に基づいてウェブリクエストを許可またはブロックする場合は、1 つ以上の正規表現一致条件を作成します。正規表現一致条件は、検索するパターンと、指定されたヘッダーやクエリ文字列など、 AWS WAF Classic でパターンを検査するウェブリクエストの部分を識別する文字列一致条件の一種です。後でウェブ ACL を作成するときに、そのパターンを含むリクエストを許可するかブロックするかを指定します。

トピック

- 正規表現一致条件の作成

- 正規表現一致条件の作成時または編集時に指定する値
- 正規表現一致条件の編集

正規表現一致条件の作成

正規表現一致条件を作成するときは、検索する文字列 (正規表現を使用) を識別するパターンセットを指定します。次に、URI やクエリ文字列など、 AWS WAF Classic がそのパターンセットを検査するウェブリクエストの部分を指定するフィルターに、これらのパターンセットを追加します。

1 つのパターンセットに複数の正規表現を追加できます。その場合、それらの表現は OR を使用して結合します。つまり、リクエストの該当する部分が、指定した式のいずれかと一致する場合、ウェブリクエストはパターンセットと一致することになります。

正規表現一致条件をルールに追加すると、条件の値と一致しないウェブリクエストを許可またはブロックするように AWS WAF Classic を設定することもできます。

AWS WAF Classic は、ほとんどの標準の Perl 互換正規表現 (PCRE) をサポートしています。ただし、次はサポートしていません。

- 後方参照と部分式取得
- 任意のゼロ幅アサーション
- サブルーチン参照と再帰パターン
- 条件付きパターン
- バックトラック制御動詞
- \C シングルバイトディレクティブ
- \R 改行一致ディレクティブ
- \K 一致開始位置リセットディレクティブ
- コールアウトと埋め込みコード
- アトミックグループと所有格量指定子

正規表現一致条件を作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示されている場合は、それを選択します。

2. ナビゲーションペインで、[String and regex matching] (文字列および正規表現の一致) を選択します。
3. [Create condition] (条件を作成) を選択します。
4. 適用するフィルター設定を指定します。詳細については、「正規表現一致条件の作成時または編集時に指定する値」を参照してください。
5. [Create pattern set and add filter] (パターンセットを作成してフィルターを追加) を選択するか (新しいパターンセットを作成した場合)、[Add filter] (フィルターを追加) を選択します (既存のパターンセットを使用した場合)。
6. [Create] (作成) を選択します。

正規表現一致条件の作成時または編集時に指定する値

正規表現一致条件を作成または更新するときに、次の値を指定します。

[Name] (名前)

正規表現一致条件の名前を入力します。名前に使用できるのは英数字 (A ~ Z、a ~ z、0 ~ 9) または特殊文字 _-!"#`+*},./ です。一度作成した条件の名前は変更できません。

[Type] (タイプ)

[Regex match] (正規表現の一致) を選択します。

[Part of the request to filter on] (フィルタリングするリクエストの一部)

AWS WAF Classic が一致する値で指定したパターンを検査する各ウェブリクエストの部分を選択します。

ヘッダー

指定したリクエストヘッダー (`User-Agent` や `Referer` など)。[Header] (ヘッダー) を選択した場合は、[Header] (ヘッダー) フィールドにヘッダー名を指定します。

[HTTP method] (HTTP メソッド)

リクエストがオリジンに実行を要求しているオペレーションのタイプを示す HTTP メソッド。CloudFront がサポートしているメソッドは、`DELETE`、`GET`、`HEAD`、`OPTIONS`、`PATCH`、`POST`、および `PUT` です。

[Query string] (クエリ文字列)

URL 内で ? 文字の後に続く部分 (ある場合)。

[URI]

リクエストの URI パス。リソースを識別します (例: `/images/daily-ad.jpg`)。これには、URI のクエリ文字列またはフラグメントコンポーネントは含まれません。詳細については、「Uniform Resource Identifier (URI): 一般的な構文」を参照してください。

変換が指定されていない限り、URI は正規化されず、リクエストの一部としてクライアントから AWS 受け取ったのと同じように検査されます。[Transformation] (変換) が指定されている場合、URI はその指定に従って形式が再設定されます。

[Body] (本文)

リクエスト内で、HTTP リクエストの本文としてウェブサーバーに送信する追加データ (フォームのデータなど) を含む部分。

> **Note**
>
> [Part of the request to filter on] (フィルタリングするリクエストの一部) の値として [Body] (本文) を選択した場合、 AWS WAF Classic によって最初の 8,192 バイト (8 KB) のみが検査されます。本文が 8,192 バイトより長いリクエストを許可またはブロックするには、サイズ制約条件を作成します。(AWS WAF Classic はリクエストヘッダーから本文の長さを取得します) 。詳細については、「サイズ制約条件の使用」を参照してください。

[Single query parameter (value only)] (単一クエリパラメータ (値のみ))

クエリ文字列の一部として定義されているすべてのパラメータです。例えば、URL が「www.xyz.com?UserName=abc&SalesRegion=seattle」である場合、UserName または SalesRegion パラメータにフィルターを追加できます。

重複したパラメータがクエリ文字列に記述される場合、値は「OR」として評価されます。つまり、いずれかの値によって一致がトリガーされます。例えば、「www.xyz.com?SalesRegion=boston&SalesRegion=seattle」という URL では、[Value to match] (一致する値) の「boston」または「seattle」に一致するパターンによって、一致がトリガーされます。

[Single query parameter (value only)] (単一クエリパラメータ (値のみ)) を選択する場合は、[Query parameter name] (クエリパラメータ名) も指定します。これは検査するクエリ文字列のパラメータです (UserName や SalesRegion など)。[Query parameter name] (クエリパラメータ名) の最大長は 30 文字です。[Query parameter name] (クエリパラメータ名) では、

大文字と小文字は区別されません。例えば、UserName を [Query parameter name] (クエリパラメータ名) として指定すると、username や UsERName など UserName のすべてのバリエーションに一致します。

[All query parameters (values only)] (すべてのクエリパラメータ (値のみ))

単一クエリパラメータ (値のみ) に似ていますが、単一パラメータの値を検査するのではなく、 AWS WAF Classic はクエリ文字列内のすべてのパラメータの値を、一致する値で指定されたパターンで検査します。例えば、「www.xyz.com?UserName=abc&SalesRegion=seattle」という URL の UserName または SalesRegion のいずれかの値に一致する [Value to match] (一致する値) のパターンによって、一致がトリガーされます。

[Header] (ヘッダー) ([Part of the request to filter on] (フィルタリングするリクエストの一部) が [Header] (ヘッダー) の場合のみ)

リストからフィルタリングするリクエストのパートからヘッダーを選択した場合は、一般的なヘッダーのリストからヘッダーを選択するか、 AWS WAF Classic で検査するヘッダーの名前を入力します。

変換

Classic がリクエストを AWS WAF 検査する前に、変換によってウェブリクエストが再フォーマットされます。これにより、攻撃者が AWS WAF Classic をバイパスするためにウェブリクエストで使用する異常なフォーマットの一部が排除されます。

1 種類のテキスト変換しか指定できません。

変換では次の操作を実行できます。

なし

AWS WAF Classic は、値の文字列が一致するかどうかを検査する前に、ウェブリクエストに対してテキスト変換を実行しません。

[Convert to lowercase] (小文字に変換)

AWS WAF Classic は、大文字 (A ~ Z) を小文字 (a ~ z) に変換します。

[HTML decode] (HTML デコード)

AWS WAF Classic は、HTML エンコード文字をエンコードされていない文字に置き換えます。

- `"` を `&` に置き換えます。

-   を改行なしスペースに置き換えます。
- < を < に置き換えます。
- > を > に置き換えます。
- 16 進数形式の文字 (&#xhhhh;) を対応する文字に置き換えます。
- 10 進数形式の文字 (&#nnnn;) を対応する文字に置き換えます。

[Normalize white space] (空白の正規化)

AWS WAF Classic は、次の文字をスペース文字 (10 進数 32) に置き換えます。

- \f、フォームフィード、10 進数 12
- \t、タブ、10 進数 9
- \n、改行、10 進数 10
- \r、キャリッジリターン、10 進数 13
- \v、垂直タブ、10 進数 11
- 改行なしスペース、10 進数 160

さらに、このオプションでは複数のスペースを 1 つのスペースに置き換えます。

[Simplify command line] (コマンドラインを簡素化)

攻撃者がオペレーティングシステムのコマンドラインのコマンドを挿入し、通常と異なるフォーマットを使用してコマンドの一部または全部を偽装するおそれがある場合は、このオプションを使用して次の変換を行います。

- 次の文字を削除します: \ " ' ^
- 次の文字の前にあるスペースを削除します: / (
- 次の文字をスペースに置き換えます: , ;
- 複数のスペースを 1 つのスペースに置き換えます。
- 大文字 (A～Z) を小文字 (a～z) に変換します。

[URL decode] (URL デコード)

URL エンコードされたリクエストをデコードします。

[Regex pattern to match to request] (リクエストに一致する正規表現パターン)

既存のパターンセットを選択するか、新しいパターンセットを作成できます。新しいパターンセットを作成する場合は、次のように指定します。

New pattern set name (新しいパターンセット名)

名前を入力し、 AWS WAF Classic で検索する正規表現パターンを指定します。

パターンセットに複数の正規表現を追加すると、それらの表現は OR を使用して結合されます。つまり、リクエストの該当する部分が、指定した式のいずれかと一致する場合、ウェブリクエストはパターンセットと一致することになります。

[Value to match] (一致する値) は最大 70 文字です。

正規表現一致条件の編集

既存の正規表現一致条件に次の変更を加えることができます。

- 既存のパターンセットからパターンを削除する
- 既存のパターンセットにパターンを追加する
- 既存正規表現一致条件からフィルターを削除する
- 既存の正規表現一致条件にフィルターを追加する (正規表現一致条件には 1 つのフィルターのみを含めることができます。したがって、フィルターを追加するには、まず既存のフィルターを削除する必要があります。)
- 既存の正規表現一致条件を削除する

> **Note**
>
> 既存のフィルターに対してパターンセットを追加したり削除したりはできません。パターンセットを編集するか、または、フィルターを削除して新しいパターンセットで新しいフィルターを作成する必要があります。

既存のパターンセットからパターンを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示されている場合は、それを選択します。
2. ナビゲーションペインで、[String and regex matching] (文字列および正規表現の一致) を選択します。

3. [View regex pattern sets] (正規表現パターンセットを表示) を選択します。
4. 編集するパターンセットの名前を選択します。
5. [Edit] (編集) を選択します。
6. 削除するパターンの横にある [X] を選択します。
7. [Save] (保存) を選択します。

既存のパターンセットにパターンを追加するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. ナビゲーションペインで、[String and regex matching] (文字列および正規表現の一致) を選択します。
3. [View regex pattern sets] (正規表現パターンセットを表示) を選択します。
4. 編集するパターンセットの名前を選択します。
5. [Edit] (編集) を選択します。
6. 新しい正規表現パターンを入力します。
7. 新しいパターンの横にある [+] を選択します。
8. [Save] (保存) を選択します。

既存の正規表現一致条件からフィルターを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. ナビゲーションペインで、[String and regex matching] (文字列および正規表現の一致) を選択します。
3. 削除するフィルターを含む条件の名前を選択します。
4. 削除するフィルターの横にあるボックスを選択します。
5. [Delete filter] (フィルターを削除) を選択します。

正規表現一致条件を削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. 正規表現条件からフィルターを削除します。その手順については、「既存の正規表現一致条件からフィルターを削除するには」を参照してください。
3. 正規表現一致条件を使用しているルールから条件自体を削除します。

   a. ナビゲーションペインで [Rules] (ルール) を選択します。

   b. 削除する正規表現一致条件を使用しているルールの名前を選択します。

   c. 右側のペインで、[Edit rule] (ルールを編集) を選択します。

   d. 削除する条件の横にある [X] を選択します。

   e. [Update] (更新) を選択します。

   f. 削除する正規表現一致条件を使用している残りのすべてのルールに対してこの同じ手順を繰り返します。
4. ナビゲーションペインで、[String and regex matching] (文字列および正規表現の一致) を選択します。
5. 削除する条件の横にあるボタンを選択します。
6. [Delete] (削除) を選択します。

既存の正規表現一致条件に対してフィルターを追加または変更するには

正規表現一致条件には 1 つのフィルターのみ含めることができます。フィルターを追加または変更するには、まず既存のフィルターを削除する必要があります。

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. 変更する正規表現条件からフィルターを削除します。その手順については、「既存の正規表現一致条件からフィルターを削除するには」を参照してください。

3. ナビゲーションペインで、[String and regex matching] (文字列および正規表現の一致) を選択します。
4. 変更する条件の名前を選択します。
5. [Add filter] (フィルターを追加) を選択します。
6. 新しいフィルターに適切な値を入力し、[Add] (追加) を選択します。

ルールの使用

> **Warning**
>
> AWS WAF Classic は計画されたend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

ルールを使用すると、 AWS WAF Classic が監視する正確な条件を指定して、 AWS WAF Classic が許可またはブロックするウェブリクエストを正確にターゲットにできます。たとえば、 AWS WAF Classic は、リクエストの送信元の IP アドレス、リクエストに含まれる文字列と文字列が表示される場所、リクエストに悪意のある SQL コードが含まれているように見えるかどうかを監視できます。

トピック

- ルールの作成と条件の追加
- ルールの条件の追加と削除
- ルールの削除
- AWS Marketplace ルールグループ

ルールの作成と条件の追加

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

ルールに複数の条件を追加する場合、そのルールに基づいて AWS WAF Classic がリクエストを許可またはブロックするには、ウェブリクエストがすべての条件と一致する必要があります。

ルールを作成して条件を追加するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. ナビゲーションペインで [ルール] を選択します。
3. [Create rule] (ルールの作成) を選択します。
4. 次の値を入力します。

   [Name] (名前)

   名前を入力します。

   [CloudWatch metric name] (CloudWatch メトリクス名)

   AWS WAF Classic が作成し、ルールに関連付ける CloudWatch メトリクスの名前を入力します。名前には英数字 (A～Z、a～z、0～9) のみを使用することができ、最大 128 文字、最

小 1 文字です。「All」や「Default_Action」など、 AWS WAF Classic 用に予約されている空白やメトリクス名を含めることはできません。

[Rule type] (ルールタイプ)

[Regular rule] または [Rate-based rule] のいずれかを選択します。レートベースのルールは通常ルールと同じですが、5 分間に IP アドレスから着信したリクエストの数も考慮に入れます。これらのルールタイプの詳細については、「AWS WAF Classic の仕組み」を参照してください。

[Rate limit] (レート制限)

レートベースのルールの場合、ルールの条件に一致する IP アドレスから 5 分間に許可するリクエストの最大数を入力します。レート制限は 100 以上にする必要があります。

レート制限を単独で指定することも、レート制限と条件を指定することもできます。レート制限のみを指定すると、 は制限をすべての IP アドレス AWS WAF に配置します。レート制限と条件を指定すると、 は条件に一致する IP アドレスに制限 AWS WAF を配置します。

IP アドレスがレート制限のしきい値に達すると、 は割り当てられたアクション (ブロックまたはカウント) をできるだけ早く、通常は 30 秒以内に AWS WAF 適用します。アクションが実行されると、IP アドレスからのリクエストなしで 5 分が経過すると、 はカウンターをゼロに AWS WAF リセットします。

5. ルールに条件を追加するには、次の値を指定します。

[When a request does/does not] (リクエストが次の条件内/条件外)

AWS WAF Classic で条件内のフィルターに基づいてリクエストを許可またはブロックする場合は、 を選択します。例えば、IP 一致条件に IP アドレス範囲 192.0.2.0/24 が含まれていて、それらの IP アドレスからのリクエストを AWS WAF Classic で許可またはブロックする場合は、 を選択します。

AWS WAF Classic で条件内のフィルターの逆数に基づいてリクエストを許可またはブロックする場合は、そうしないを選択します。例えば、IP 一致条件に IP アドレス範囲 192.0.2.0/24 が含まれていて、それらの IP アドレスから来ないリクエストを AWS WAF Classic で許可またはブロックする場合は、そうしないを選択します。

[match/originate from] (一致/次から生じている)

ルールに追加する条件のタイプを選択します。

- クロスサイトスクリプティング一致条件 - [match at least one of the filters in the cross-site scripting match condition] (クロスサイトスクリプティング一致条件の少なくとも 1 つのフィルターに一致する) を選択します。
- IP 一致条件 - [originate from an IP address in] (IP アドレスより送信) を選択します
- Geo 一致条件 - [originate from a geographic location in] (地理的場所より送信) を選択します
- サイズ制約条件 - [match at least one of the filters in the size constraint condition] (サイズ制約条件の少なくとも 1 つのフィルターに一致する) を選択します
- SQL インジェクション一致条件 - [match at least one of the filters in the SQL injection match condition] (SQL インジェクション一致条件の少なくとも 1 つのフィルターに一致する) を選択します
- 文字列一致条件 - [match at least one of the filters in the string match condition] (文字列一致条件の少なくとも 1 つのフィルターに一致する) を選択します
- 正規表現一致条件 - [match at least one of the filters in the regex match condition] (正規表現一致条件の少なくとも 1 つのフィルターに一致する) を選択します

[condition name] (条件名)

ルールに追加する条件を選択します。リストには、前のステップで選択したタイプの条件のみが表示されます。

6. ルールに別の条件を追加するには、[Add another condition] (別の条件を追加) を選択して、ステップ 4〜5 を繰り返します。次の点に注意してください。

   - 複数の条件を追加する場合、 AWS WAF Classic がそのルールに基づいてリクエストを許可または拒否するには、ウェブリクエストがすべての条件で少なくとも 1 つのフィルターと一致する必要があります。
   - 同じルールに 2 つの IP 一致条件を追加すると、 AWS WAF Classic は両方の IP 一致条件に表示される IP アドレスからのリクエストのみを許可または拒否します。

7. 条件の追加が終了したら、[Create] (作成) を選択します。

ルールの条件の追加と削除

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

条件を追加または削除することでルールを変更できます。

ルールの条件を追加または削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示されている場合は、それを選択します。
2. ナビゲーションペインで [Rules] (ルール) を選択します。
3. 条件を追加または削除するルールの名前を選択します。
4. [Add Rule] (ルールの追加) を選択します。
5. 条件を追加するには、[Add condition] (条件を追加) を選択して次の値を指定します。

   [When a request does/does not] (リクエストが次の条件内/条件外)

   AWS WAF Classic で、IP アドレス 192.0.2.0/24 の範囲から送信されるウェブリクエストなど、条件内のフィルターに基づいてリクエストを許可またはブロックする場合は、 を選択します。

AWS WAF Classic で条件内のフィルターの逆数に基づいてリクエストを許可またはブロックする場合は、 なしを選択します。例えば、IP 一致条件に IP アドレス範囲 192.0.2.0/24 が含まれていて、それらの IP アドレスから来ないリクエストを AWS WAF Classic で許可またはブロックする場合は、そうしないを選択します。

[match/originate from] (一致/次から生じている)

ルールに追加する条件のタイプを選択します。

- クロスサイトスクリプティング一致条件 - [match at least one of the filters in the cross-site scripting match condition] (クロスサイトスクリプティング一致条件の少なくとも 1 つのフィルターに一致する) を選択します。
- IP 一致条件 - [originate from an IP address in] (IP アドレスより送信) を選択します
- Geo 一致条件 - [originate from a geographic location in] (地理的場所より送信) を選択します
- サイズ制約条件 - [match at least one of the filters in the size constraint condition] (サイズ制約条件の少なくとも 1 つのフィルターに一致する) を選択します
- SQL インジェクション一致条件 - [match at least one of the filters in the SQL injection match condition] (SQL インジェクション一致条件の少なくとも 1 つのフィルターに一致する) を選択します
- 文字列一致条件 - [match at least one of the filters in the string match condition] (文字列一致条件の少なくとも 1 つのフィルターに一致する) を選択します
- 正規表現一致条件 - [match at least one of the filters in the regex match condition] (正規表現一致条件の少なくとも 1 つのフィルターに一致する) を選択します

[condition name] (条件名)

ルールに追加する条件を選択します。リストには、前のステップで選択したタイプの条件のみが表示されます。

6. 条件を削除するには、条件名の右側にある [X] を選択します。
7. [更新] を選択します。

ルールの削除

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

ルールを削除する場合は、最初にそのルールを使用しているウェブ ACL からルールを削除し、次にルール内に含まれている条件を削除します。

ルールを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. ルールを使用しているウェブ ACL から、このルールを削除するには、ウェブ ACL のそれぞれについて、次のステップを実行します。

   a. ナビゲーションペインで [Web ACLs] (ウェブ ACL) を選択します。

   b. 削除するルールを使用しているウェブ ACL の名前を選択します。

   > **Note**
   >
   > ウェブ ACL が表示されない場合は、リージョンの選択が正しいことを確認してください。Amazon CloudFront ディストリビューションを保護するウェブ ACL は [グローバル (CloudFront)] にあります。

c. [Rules] (ルール) タブを選択します。

d. [Edit web ACL] (ウェブ ACL を編集) を選択します。

e. 削除するルールの右側にある [X] を選択してから、[Update] (更新) を選択します。

3. ナビゲーションペインで [Rules] (ルール) を選択します。

4. 削除するルールの名前を選択します。

> **Note**
>
> ルールが表示されない場合は、リージョンの選択が正しいことを確認してください。Amazon CloudFront ディストリビューションを保護するルールは、[グローバル (CloudFront)] にあります。

5. [Delete] (削除) をクリックします。

AWS Marketplace ルールグループ

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

AWS WAF Classic は、 リソースの保護に役立つAWS Marketplace ルールグループを提供します。AWS Marketplace ルールグループは、 ready-to-useルールのコレクションです。 AWS AWS

一部の AWS Marketplace ルールグループは、WordPress、Joomla、PHP などの特定のタイプのウェブアプリケーションを保護するように設計されています。他の AWS Marketplace ルールグルー

プは、OWASP Top 10 に記載されているような既知の脅威や一般的なウェブアプリケーションの脆弱性に対して広範な保護を提供します。

優先 AWS パートナーから 1 つの AWS Marketplace ルールグループをインストールでき、独自のカスタマイズされた AWS WAF Classic ルールを追加して保護を強化することもできます。PCI や HIPAA などの規制の遵守が必要な場合は、 AWS Marketplace ルールグループを使用してウェブアプリケーションファイアウォールの要件を満たすことができます。

AWS Marketplace ルールグループは、長期契約や最低契約金なしで利用できます。ルールグループをサブスクライブすると、月額料金 (時間数で按分) およびボリュームに基づく継続中のリクエスト料金が課金されます。詳細については、AWS WAF 「 Classic Pricing」と「 の各 AWS Marketplace ルールグループの説明」を参照してください AWS Marketplace。

自動更新

絶えず変化する脅威の状況を常に把握しておくと、時間がかかり、コストがかかる可能性があります。 AWS Marketplace ルールグループを使用すると、 AWS WAF Classic を実装して使用する時間を短縮できます。もう 1 つの利点は、新しい脆弱性や脅威が発生したときに AWS 、 と当社の AWS パートナーが AWS Marketplace ルールグループを自動的に更新することです。

新しい脆弱性が公開前にパートナーの多くに通知されます。新しい脅威が広く知られる前でも、パートナーはルールグループを更新してお客様にデプロイできます。また、最新の脅威を調査して分析して最も関連性の高いルールを作成する脅威調査チームも数多くあります。

ルールグループの AWS Marketplace ルールへのアクセス

各 AWS Marketplace ルールグループは、保護するように設計されている攻撃のタイプと脆弱性の包括的な説明を提供します。ルールグループプロバイダーの知的財産を保護するために、ルールグループ内の個々のルールを表示することはできません。この制限は、悪意のあるユーザーが公開されたルールを特に回避する脅威を設計するのを防ぐのにも役立ちます。

ルールグループ内の個々の AWS Marketplace ルールを表示できないため、ルールグループ内の AWS Marketplace ルールを編集することもできません。ただし、ルールグループから特定のルールを除外できます。これは、「ルールグループ例外」と呼ばれます。ルールの除外は、これらのルールを削除しません。むしろ、ルールのアクションを COUNT に変更します。そのため、除外されたルールと一致するリクエストはカウントされますが、ブロックされません。除外されたルールごとに COUNT メトリクスを受信します。

予期せずにトラフィックをブロックしているルールグループのトラブルシューティングを行う場合、ルールを除外することが役立ちます (誤検出)。トラブルシューティングの手法の 1 つは、目的のト

ラフィックをブロックしているルールグループ内の特定のルールを識別し、その特定のルールを無効にする (除外する) ことです。

特定のルールを除外することに加えて、ルールグループ全体を有効または無効にすることで保護を絞り込むか、実行するルールグループアクションを選択できます。詳細については、「AWS Marketplace ルールグループの使用」を参照してください。

クォータ

有効にできる AWS Marketplace ルールグループは 1 つだけです。を使用して作成した 1 つのカスタムルールグループを有効にすることもできます AWS Firewall Manager。これらのルールグループは、ウェブ ACL ごとの 10 ルールの最大クォータにカウントされます。したがって、1 つの AWS Marketplace ウェブ ACL に 1 つのルールグループ、1 つのカスタムルールグループ、および最大 8 つのカスタムルールを含めることができます。

料金

AWS Marketplace ルールグループの料金については、AWS WAF 「 Classic Pricing」および「各 AWS Marketplace ルールグループの説明」を参照してください AWS Marketplace。

AWS Marketplace ルールグループの使用

AWS WAF Classic コンソールで AWS Marketplace ルールグループをサブスクライブおよびサブスクライブ解除できます。ルールグループから特定のルールを除外することもできます。

AWS Marketplace ルールグループをサブスクライブして使用するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. ナビゲーションペインで [Marketplace] を選択します。
3. [Available marketplace products] (利用可能な Marketplace 製品) セクションで、ルールグループの名前を選択して、詳細と料金情報を表示します。
4. ルールグループにサブスクライブする場合は、[Continue] (続行) を選択します。

> **Note**
>
> このルールグループをサブスクライブしたくない場合は、ブラウザでこのページを閉じるだけです。

5. [Set up your account] (アカウントをセットアップ) を選択します。
6. 個々のルールを追加するのと同様の方法で、ウェブ ACL にルールグループを追加します。詳細については、「ウェブ ACL の作成」または「ウェブ ACL の編集」を参照してください。

> **Note**
>
> ウェブ ACL にルールグループを追加するときに、ルールグループ ([No override] (上書きしない) または [Override to count] (カウントに上書き) に設定したアクションは、ルールグループ上書きアクションと呼びます。詳細については、「ルールグループの上書き」を参照してください。

AWS Marketplace ルールグループのサブスクリプションを解除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. すべてのウェブ ACL からルールグループを削除します。詳細については、「ウェブ ACL の編集」を参照してください。
3. ナビゲーションペインで [Marketplace] を選択します。
4. [Manage your subscriptions] (サブスクリプションを管理) を選択します。
5. サブスクリプションを解除するルールグループの名前の横にある [Cancel subscription] (サブスクリプションをキャンセル) を選択します。
6. [Yes, cancel subscription] (はい、サブスクリプションをキャンセルします) を選択します。

ルールグループからルールを除外するには (ルールグループ例外)

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。

2. まだ有効になっていない場合は、 AWS WAF Classic ログ記録を有効にします。詳細については、「ウェブ ACL トラフィック情報のログ記録」を参照してください。 AWS WAF Classic ログを使用して、除外するルールの IDs を識別します。これらは通常、正規のリクエストをブロックしているルールです。
3. ナビゲーションペインで [Web ACLs] (ウェブ ACL) を選択します。
4. 編集するウェブ ACL の名前を選択します。これにより、右ペインで、ウェブ ACL の詳細を含むページが開きます。

> **Note**
>
> 編集するルールグループは、そのルールグループからルールを除外する前にウェブ ACL に関連付ける必要があります。

5. 右ペインの [Rules] (ルール) タブで、[Edit web ACL] (ウェブ ACL を編集) を選択します。
6. [Rule group exceptions] (ルールグループ例外) セクションに、編集するルールグループを展開します。
7. 除外するルールの隣にある [X] を選択します。 AWS WAF Classic ログを使用して、正しいルール ID を特定できます。
8. [更新] を選択します。

ルールの除外は、ルールグループからこれらのルールを削除しません。むしろ、ルールのアクションを COUNT に変更します。そのため、除外されたルールと一致するリクエストはカウントされますが、ブロックされません。除外されたルールごとに COUNT メトリクスを受信します。

> **Note**
>
> この同じ手順を使用して、 AWS Firewall Managerで作成したカスタムルールグループからルールを除外できます。ただし、これらのステップを使用してカスタムルールグループからルールを除外するよりも、「AWS WAF Classic ルールグループへのルールの追加と削除」で説明されているステップを使用してカスタムルールグループを編集することもできます。

ルールグループの上書き

AWS Marketplace ルールグループには、オーバーライドなしとカウントするオーバーライドの 2 つのアクションがあります。ルールグループをテストする場合は、アクションを [Override to count] (カウントに上書き) に設定します。このルールグループアクションは、グループに含まれる個々のルールで指定された BLOCK アクションを上書きします。つまり、ルールグループのアクションが [Override to count] (カウントに上書き) に設定されている場合は、グループ内の個々のルールのアクションに基づいて一致するリクエストをブロックするのではなく、それらのリクエストがカウントされます。逆に、ルールグループのアクションを [No override] (上書きしない) に設定すると、グループ内の個々のルールのアクションが使用されます。

AWS Marketplace ルールグループのトラブルシューティング

AWS Marketplace ルールグループが正当なトラフィックをブロックしていることがわかった場合は、次の手順を実行します。

AWS Marketplace ルールグループのトラブルシューティングを行うには

1. 正当なトラフィックをブロックしている特定のルールを除外します。 AWS WAF Classic ログを使用して、どのルールがどのリクエストをブロックしているかを特定できます。ルールの除外の詳細については、ルールグループからルールを除外するには (ルールグループ例外) を参照してください。
2. 特定のルールを除外しても問題が解決しない場合は、 AWS Marketplace ルールグループのアクションをオーバーライドなしからオーバーライドしてカウントするように変更できます。これにより、ルールグループ内の個々のルールアクションに関係なく、ウェブリクエストが通過します。また、ルールグループに Amazon CloudWatch メトリクスも使用できるようになります。
3. AWS Marketplace ルールグループアクションをカウントに上書きに設定したら、ルールグループプロバイダーのカスタマーサポートチームに連絡して問題のトラブルシューティングをさらに行います。連絡先については、 AWS Marketplaceの製品リストページのルールグループリストを参照してください。

カスタマーサポートへの問い合わせ

AWS WAF Classic または によって管理されるルールグループに関する問題については AWS、 にお問い合わせください AWS サポート。 AWS パートナーによって管理されるルールグループに関する問題については、そのパートナーのカスタマーサポートチームにお問い合わせください。パートナーの連絡先情報を確認するには、パートナーのリストを参照してください AWS Marketplace。

AWS Marketplace ルールグループの作成と販売

AWS Marketplace ルールグループを販売する場合は AWS Marketplace、「ソフトウェアの販売方法 AWS Marketplace」を参照してください。

ウェブ ACL の使用

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

ウェブ ACL にルールを追加するときは、ルールの条件に基づいて AWS WAF Classic がリクエストを許可するかブロックするかを指定します。ウェブ ACL に複数のルールを追加すると、 AWS WAF Classic は各リクエストをウェブ ACL にリストした順序でルールに対して評価します。ウェブリクエストがルールのすべての条件に一致すると、 AWS WAF Classic は直ちに対応するアクションを許可またはブロックし、ウェブ ACL の残りのルールに対してリクエストを評価しません。

ウェブリクエストがウェブ ACL のルールのいずれとも一致しない場合、 AWS WAF Classic はウェブ ACL に指定したデフォルトのアクションを実行します。詳細については、「ウェブ ACL のデフォルトアクションの決定」を参照してください。

リクエストを許可またはブロックする前にルールをテストする場合は、ルールの条件に一致するウェブリクエストをカウントするように AWS WAF Classic を設定できます。詳細については、「ウェブ ACL のテスト」を参照してください。

トピック

- ウェブ ACL のデフォルトアクションの決定

- ウェブ ACL の作成
- ウェブ ACL と Amazon API Gateway API、CloudFront ディストリビューション、または Application Load Balancer との関連付けまたは関連付けの解除
- ウェブ ACL の編集
- ウェブ ACL の削除
- ウェブ ACL のテスト

ウェブ ACL のデフォルトアクションの決定

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

ウェブ ACL を作成して設定する場合、最初に行う必要がある最も重要な決定は、 AWS WAF Classic がウェブリクエストを許可するか、ウェブリクエストをブロックするかです。デフォルトのアクションは、指定したすべての条件についてウェブリクエストを検査し、ウェブリクエストがそれらの条件のいずれにも一致しない後に AWS WAF Classic が実行する内容を示します。

- [Allow] (許可) 大部分のユーザーに対してはウェブサイトへのアクセスを許可する一方、指定した IP アドレスからのリクエストまたは悪意のある SQL コードや指定した値が含まれている可能性があるリクエストを行う攻撃者に対してアクセスをブロックする場合は、デフォルトアクションとして [Allow] (許可) を選択します。
- [Block] (ブロック) 大部分の自称ユーザーに対してはウェブサイトへのアクセスを拒否する一方、指定した IP アドレスからのリクエストや指定した値が含まれているリクエストのユーザーに対してアクセスを許可する場合は、デフォルトアクションとして [Block] (ブロック) を選択します。

デフォルトアクションを決めた後は、通常、大部分のウェブリクエストを許可するかブロックするかで条件を決めます。例えば、大部分のウェブリクエストを許可する場合は、通常、次のようなウェブリクエストをブロックする一致条件を作成します。

- リクエスト数が不当に多い IP アドレスからのリクエスト
- お客様がビジネスを行っていない国、または頻繁に攻撃元になっている国からのリクエスト
- [User-Agent] ヘッダーに不正な値が含まれているリクエスト
- 悪意のある SQL コードが含まれている可能性があるリクエスト

ウェブ ACL の作成

> **Warning**
>
> AWS WAF Classic は計画されたend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

ウェブ ACL を作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示されている場合は、それを選択します。
2. AWS WAF Classic を初めて使用する場合は、 AWS WAF 「クラシックに移動」を選択し、「ウェブ ACL の設定」を選択します。 AWS WAF Classic を以前に使用したことがある場合は、ナビゲーションペインでウェブ ACLs を選択し、ウェブ ACL の作成を選択します。
3. [Web ACL name] (ウェブ ACL の名前) に名前を入力します。

> **Note**
>
> ウェブ ACL の作成後は、名前を変更することはできません。

4. [CloudWatch metric name] (CloudWatch メトリクス名) で、必要に応じてデフォルト名を変更します。名前には英数字 (A～Z、a～z、0～9) のみを使用することができ、最大 128 文字、最小 1 文字です。「All」や「Default_Action」など、 AWS WAF Classic 用に予約されている空白やメトリクス名を含めることはできません。

> **Note**
>
> ウェブ ACL の作成後は、名前を変更することはできません。

5. [Region] (リージョン) で、リージョンを選択します。
6. [AWS resource (リソース)] で、ウェブ ACL に関連付けるリソースを選択し、[Next (次へ)] を選択します。
7. AWS WAF Classic がウェブリクエストを検査するために使用する条件をすでに作成している場合は、次へを選択し、次のステップに進みます。

   条件をまだ作成していない場合は、ここで作成します。詳細については、次のトピックを参照してください。

   - クロスサイトスクリプティング一致条件の使用
   - IP 一致条件の使用
   - Geo (地理的) 一致条件の使用
   - サイズ制約条件の使用
   - SQL インジェクション一致条件の使用
   - 文字列一致条件の使用
   - 正規表現一致条件の使用
8. このウェブ ACL に追加するルールまたはルールグループ (または AWS Marketplace ルールグループをサブスクライブ) を既に作成している場合は、ウェブ ACL にルールを追加します。

   a. [Rules] (ルール) リストで、ルールを選択します。

   b. [Add rule to web ACL] (ウェブ ACL にルールを追加) を選択します。

c. このウェブ ACL に関連付けるすべてのルールを追加するまでステップ a とステップ b を繰り返します。

d. ステップ 10 に進んでください。

9. ルールをまだ作成していない場合は、ここでルールを追加できます。

a. [Create rule] (ルールの作成) を選択します。

b. 次の値を入力します。

[Name] (名前)

名前を入力します。

[CloudWatch metric name] (CloudWatch メトリクス名)

AWS WAF Classic が作成し、ルールに関連付ける CloudWatch メトリクスの名前を入力します。名前には英数字 (A～Z、a～z、0～9) のみを使用することができ、最大 128 文字、最小 1 文字です。空白や、「All」および「Default_Action」など AWS WAF Classic 用に予約されたメトリクス名は使用できません。

> **Note**
> ルールの作成後はメトリクス名を変更できません。

c. ルールに条件を追加するには、次の値を指定します。

[When a request does/does not] (リクエストが次の条件内/条件外)

AWS WAF Classic で、IP アドレス 192.0.2.0/24 の範囲から送信されるウェブリクエストなど、条件内のフィルターに基づいてリクエストを許可またはブロックする場合は、を選択します。

AWS WAF Classic で条件内のフィルターの逆数に基づいてリクエストを許可またはブロックする場合は、そうしないを選択します。例えば、IP 一致条件に IP アドレス範囲 192.0.2.0/24 が含まれていて、それらの IP アドレスから来ないリクエストを AWS WAF Classic で許可またはブロックする場合は、そうしないを選択します。

[match/originate from] (一致/次から生じている)

ルールに追加する条件のタイプを選択します。

- クロスサイトスクリプティング一致条件 - [match at least one of the filters in the cross-site scripting match condition] (クロスサイトスクリプティング一致条件の少なくとも 1 つのフィルターに一致する) を選択します。
- IP 一致条件 - [originate from an IP address in] (IP アドレスより送信) を選択します
- Geo 一致条件 - [originate from a geographic location in] (地理的場所より送信) を選択します
- サイズ制約条件 - [match at least one of the filters in the size constraint condition] (サイズ制約条件の少なくとも 1 つのフィルターに一致する) を選択します
- SQL インジェクション一致条件 - [match at least one of the filters in the SQL injection match condition] (SQL インジェクション一致条件の少なくとも 1 つのフィルターに一致する) を選択します
- 文字列一致条件 - [match at least one of the filters in the string match condition] (文字列一致条件の少なくとも 1 つのフィルターに一致する) を選択します
- 正規表現一致条件 - [match at least one of the filters in the regex match condition] (正規表現一致条件の少なくとも 1 つのフィルターに一致する) を選択します

[condition name] (条件名)

ルールに追加する条件を選択します。リストには、前のリストで選択したタイプの条件のみが表示されます。

d. ルールに別の条件を追加するには、[Add another condition] (別の条件を追加) を選択し、ステップ b とステップ c を繰り返します。次の点に注意してください。

- 複数の条件を追加する場合、 AWS WAF Classic がそのルールに基づいてリクエストを許可またはブロックするには、ウェブリクエストがすべての条件の少なくとも 1 つのフィルターと一致する必要があります。
- 同じルールに 2 つの IP 一致条件を追加すると、 AWS WAF Classic は両方の IP 一致条件に表示される IP アドレスからのリクエストのみを許可または拒否します。

e. ステップ 9 を繰り返して、このウェブ ACL に追加するすべてのルールを作成します。

f. [Create] (作成) を選択します。

g. ステップ 10 に進みます。

10. ウェブ ACL 内のルールまたはルールグループごとに、 AWS WAF Classic が提供する管理の種類を次のように選択します。

- ルールごとに、ルールの条件に基づいて AWS WAF Classic がウェブリクエストを許可、ブロック、またはカウントするかどうかを選択します。

- [Allow] (許可) - API Gateway、CloudFront、または Application Load Balancer は、リクエストされたオブジェクトを返します。CloudFront の場合、オブジェクトがエッジキャッシュ内になければ、CloudFront により、リクエストはオリジンに転送されます。
- [Block] (ブロック) - API Gateway、CloudFront、または Application Load Balancer は、「HTTP 403 (Forbidden)」(HTTP 403 (禁止) ステータスコードを返します。CloudFront はカスタムエラーページを返すこともできます。詳細については、「CloudFront カスタムエラーページでの AWS WAF Classic の使用」を参照してください。
- カウント – AWS WAF Classic は、ルールの条件に一致するリクエストのカウンターを増分し、引き続きウェブ ACL の残りのルールに基づいてウェブリクエストを検査します。

  ウェブ ACL を使用してウェブリクエストを許可またはブロックする前に、[Count] (カウント) でウェブ ACL をテストする方法については、「ウェブ ACL のルールに一致するウェブリクエストのカウント」を参照してください。

- ルールグループごとに、ルールグループの上書きアクションを設定します。
  - [No override] (上書きなし) - ルールグループ内の個々のルールのアクションが使用されます。
  - [Override to count] (カウントに上書き) - グループ内の個々のルールによって指定されたブロックアクションを上書きし、一致するリクエストのみがすべてカウントされるようにします。

  詳細については、「ルールグループの上書き」を参照してください。

11. ウェブ ACL のルールの順序を変更する場合は、順序列の矢印を使用します。 AWS WAF Classic は、ルールがウェブ ACL に表示される順序に基づいてウェブリクエストを検査します。
12. ウェブ ACL に追加したルールを削除する場合は、ルールの行にある [x] を選択します。
13. ウェブ ACL のデフォルトアクションを選択します。これは、ウェブリクエストがこのウェブ ACL のルールの条件と一致しない場合に AWS WAF Classic が実行するアクションです。詳細については、「ウェブ ACL のデフォルトアクションの決定」を参照してください。
14. [Review and create] (確認および作成) を選択します。
15. ウェブ ACL の設定を確認し、[Confirm and create] (確認して作成) を選択します。

ウェブ ACL と Amazon API Gateway API、CloudFront ディストリビューション、または Application Load Balancer との関連付けまたは関連付けの解除

> **Warning**
>
> AWS WAF Classic は計画されたend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

ウェブ ACL の関連付けまたは関連付けの解除を行うには、該当する手順を実行します。ウェブ ACL と CloudFront ディストリビューションとの関連付けは、ディストリビューションの作成時または更新時に行うこともできます。詳細については、Amazon CloudFront デベロッパーガイド」のAWS WAF 「Classic を使用してコンテンツへのアクセスを制御する」を参照してください。

ウェブ ACL を関連付けるとき、次の制限が適用されます。

- 各 API Gateway API、Application Load Balancer、CloudFront ディストリビューションは、1 つのウェブ ACL にのみ関連付けることができます。
- CloudFront ディストリビューションに関連付けられたウェブ ACL を、Application Load Balancer または API Gateway API に関連付けることはできません。ただし、ウェブ ACL は、他の CloudFront ディストリビューションに関連付けることはできます。

ウェブ ACL を API Gateway API、CloudFront ディストリビューション、または Application Load Balancer に関連付けるには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。

2. ナビゲーションペインで [Web ACLs] (ウェブ ACL) を選択します。
3. API Gateway API、CloudFront ディストリビューション、または Application Load Balancer に関連付けるウェブ ACL の名前を選択します。これにより、右ペインで、ウェブ ACL の詳細を含むページが開きます。
4. [ルール] タブの [このウェブ ACL を使用するAWS リソース] で、[関連付けを追加] を選択します。
5. プロンプトが表示されたら、[Resource] (リソース) リストを使用して、このウェブ ACL を関連付ける API Gateway API、CloudFront ディストリビューション、または Application Load Balancer を選択します。Application Load Balancer を選択した場合は、リージョンも指定する必要があります。
6. [Add] (追加) を選択します。
7. このウェブ ACL を追加の API Gateway API、CloudFront ディストリビューション、または別の Application Load Balancer に関連付けるには、ステップ 4〜6 を繰り返します。

ウェブ ACL と API Gateway API、CloudFront ディストリビューション、または Application Load Balancer との関連付けを解除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. ナビゲーションペインで [Web ACLs] (ウェブ ACL) を選択します。
3. API Gateway API、CloudFront ディストリビューション、または Application Load Balancer との関連付けを解除するウェブ ACL の名前を選択します。これにより、右ペインで、ウェブ ACL の詳細を含むページが開きます。
4. [ルール] タブの [このウェブ ACL を使用するAWS リソース] で、このウェブ ACL との関連を解除する API Gateway API、CloudFront ディストリビューション、または Application Load Balancer のそれぞれに [x] を選択します。

ウェブ ACL の編集

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

ウェブ ACL のルールを追加または削除したり、デフォルトアクションを変更したりするには、次の手順を実行します。

ウェブ ACL を編集するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示されている場合は、それを選択します。
2. ナビゲーションペインで [Web ACLs] (ウェブ ACL) を選択します。
3. 編集するウェブ ACL の名前を選択します。これにより、右ペインで、ウェブ ACL の詳細を含むページが開きます。
4. 右ペインの [Rules] (ルール) タブで、[Edit web ACL] (ウェブ ACL を編集) を選択します。
5. ウェブ ACL にルールを追加するには、次のステップを実行します。

   a. [Rules] (ルール) リストで、追加するルールを選択します。

   b. [Add rule to web ACL] (ウェブ ACL にルールを追加) を選択します。

   c. ステップ a とステップ b を繰り返して、すべての必要なルールを追加します。

6. ウェブ ACL のルールの順序を変更する場合は、順序列の矢印を使用します。 AWS WAF Classic は、ルールがウェブ ACL に表示される順序に基づいてウェブリクエストを検査します。
7. ウェブ ACL からルールを削除するには、そのルールの行の右にある [x] を選択します。これにより AWS WAF 、 Classic からルールが削除されるのではなく、このウェブ ACL からルールが削除されます。
8. ルールのアクションまたはウェブ ACL のデフォルトアクションを変更するには、希望するオプションを選択します。

> **Note**
>
> (単一のルールではなく) ルールグループまたは AWS Marketplace ルールグループのアクションを設定する場合、ルールグループに設定したアクション (オーバーライドなしまたはカウントに上書き) はオーバーライドアクションと呼ばれます。詳細については、ルールグループの上書きを参照してください。

9. [Save changes] (変更の保存) をクリックします。

ウェブ ACL の削除

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

> **Important**
>
> ウェブ ACL の削除は永続的であり、元に戻すことはできません。選択したウェブ ACL にルールが含まれているか、CloudFront ディストリビューション、Application Load Balancer、または API Gateway に関連付けられている場合は、削除する前にルールと関連付けを削除します。そうしないと、削除は失敗します。

ウェブ ACL を削除するには、ウェブ ACL に含まれているルールを削除し、ウェブ ACL からすべての CloudFront ディストリビューションおよび Application Load Balancer の関連付けを解除する必要があります。次の手順を実行します。

ウェブ ACL を削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. ナビゲーションペインで [Web ACLs] (ウェブ ACL) を選択します。
3. 削除するウェブ ACL の名前を選択します。これにより、右ペインで、ウェブ ACL の詳細を含むページが開きます。

   > **Note**
   >
   > ウェブ ACL が表示されない場合は、リージョンの選択が正しいことを確認してください。Amazon CloudFront ディストリビューションを保護するウェブ ACL は [グローバル (CloudFront)] にあります。
4. 右ペインの [Rules] (ルール) タブで、[Edit web ACL] (ウェブ ACL を編集) を選択します。
5. ウェブ ACL からすべてのルールを削除するには、各ルールの行の右にある [x] を選択します。これにより AWS WAF Classic からルールが削除されるのではなく、このウェブ ACL からルールが削除されます。
6. [更新] を選択します。
7. すべての CloudFront ディストリビューションと Application Load Balancer からウェブ ACL の関連付けを解除します。[ルール] タブの [このウェブ ACL を使用するAWS リソース] で、API

Gateway API、CloudFront ディストリビューション、または Application Load Balancer のそれぞれに [x] を選択します。

8. [Web ACLs] (ウェブ ACL) ページで、削除するウェブ ACL が選択されていることを確認し、[Delete] (削除) を選択します。

ウェブ ACL のテスト

> **Warning**
>
> AWS WAF Classic は計画されたend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

許可または拒否するリクエストをブロックするように AWS WAF Classic を誤って設定しないようにするには、ウェブサイトまたはウェブアプリケーションでウェブ ACL の使用を開始する前に、ウェブ ACL を徹底的にテストすることをお勧めします。

トピック

- ウェブ ACL のルールに一致するウェブリクエストのカウント
- API Gateway CloudFront または Application Load Balancer が AWS WAF Classic に転送したウェブリクエストのサンプルの表示

ウェブ ACL のルールに一致するウェブリクエストのカウント

ウェブ ACL にルールを追加するときは、 AWS WAF そのルールのすべての条件に一致するウェブリクエストを許可、ブロック、またはカウントするかどうかを指定します。次の設定から始めることをお勧めします。

- ウェブリクエストをカウントするようにウェブ ACL のすべてのルールを設定する
- リクエストを許可するウェブ ACL のデフォルトアクションを設定する

この設定では、 AWS WAF Classic は最初のルールの条件に基づいて各ウェブリクエストを検査します。ウェブリクエストがそのルールのすべての条件に一致する場合、 AWS WAF Classic はそのルールのカウンターを増分します。次に、 AWS WAF Classic は次のルールの条件に基づいてウェブリクエストを検査します。リクエストがそのルールのすべての条件に一致する場合、 AWS WAF Classic はルールのカウンターを増分します。これは、 AWS WAF Classic がすべてのルールの条件に基づいてリクエストを検査するまで続きます。

リクエストをカウントするようにウェブ ACL のすべてのルールを設定し、ウェブ ACL を Amazon API Gateway、CloudFront ディストリビューション、または Application Load Balancer と関連付けたら、結果として生じるカウントを Amazon CloudWatch グラフで表示できます。ウェブ ACL の各ルールと、API Gateway、CloudFront、または Application Load Balancer がウェブ ACL の AWS WAF Classic に転送するすべてのリクエストについて、CloudWatch では以下を実行できます。

- 1 時間前または 3 時間前のデータを表示する
- データポイント間の間隔を変更する
- CloudWatch がデータに対して実行する計算 (最大、最小、平均、合計など) を変更する

> **Note**
>
> AWS WAF Classic with CloudFront はグローバルサービスであり、メトリクスは で米国東部 (バージニア北部) リージョンを選択した場合にのみ使用できます AWS マネジメントコンソール。別のリージョンを選択した場合、 AWS WAF Classic メトリクスは CloudWatch コンソールに表示されません。

ウェブ ACL でルールのデータを表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. ナビゲーションペインの [Metrics] (メトリクス) で、[WAF] を選択します。
3. データを表示するウェブ ACL のチェックボックスをオンにします。
4. 該当する設定を変更します。

[Statistic] (統計)

CloudWatch がデータに対して実行する計算内容を選択します。

[Time range] (時間範囲)

前の 1 時間のデータを表示するか、前の 3 時間のデータを表示するかを選択します。

[Period] (期間)

グラフでのデータポイント間の間隔を変更します。

[Rules] (ルール)

データを表示するルールを選択します。

次の点に注意してください。

- ウェブ ACL を API Gateway API、CloudFront ディストリビューション、または Application Load Balancer に関連付けただけの場合は、グラフにデータが表示され、使用可能なメトリクスのリストにウェブ ACL のメトリクスが表示されるまでに数分かかることがあります。
- 複数の API Gateway API、CloudFront ディストリビューション、または Application Load Balancer をウェブ ACL に関連付ける場合、CloudWatch データには、ウェブ ACL に関連付けられるすべてのディストリビューションに対するすべてのリクエストが含まれます。
- データポイントの上にマウスカーソルを置くと、詳細情報が表示されます。
- グラフは自動的には更新されません。表示を更新するには、更新 () アイコンを選択します。

5. (オプション) API Gateway CloudFront または Application Load Balancer が AWS WAF Classic に転送した個々のリクエストに関する詳細情報を表示します。詳細については、「API Gateway CloudFront または Application Load Balancer が AWS WAF Classic に転送したウェブリクエストのサンプルの表示」を参照してください。
6. ルールにより、傍受する必要のないリクエストが傍受されていると判断した場合は、該当する設定を変更します。詳細については、「ウェブアクセスコントロールリスト (ウェブ ACL) の作成と設定」を参照してください。

すべてのルールにより、正しいリクエストのみが傍受されていることを確認したら、各ルールのアクションを [Allow] (許可) または [Block] (ブロック) に変更します。詳細については、「ウェブ ACL の編集」を参照してください。

API Gateway CloudFront または Application Load Balancer が AWS WAF Classic に転送したウェブリクエストのサンプルの表示

AWS WAF Classic コンソールでは、API Gateway CloudFront または Application Load Balancer が検査のために AWS WAF Classic に転送したリクエストのサンプルを表示できます。サンプリングされたリクエストごとに、発生元の IP アドレスやリクエストに含まれるヘッダーなど、リクエストに関する詳細なデータを表示できます。また、リクエストが一致したルールを表示したり、ルールがリクエストを許可するように設定されているかブロックするように設定されているかを確認したりもできます。

リクエストのサンプルには、各ルールのすべての条件に一致した最大 100 件のリクエストと、デフォルトアクションが適用された別の 100 件のリクエストが含まれます。デフォルトアクションは、すべてのルールのすべての条件に一致しなかったリクエストに適用されます。サンプルのリクエストは、過去 15 分間にコンテンツに対するリクエストを受信したすべての API Gateway API、CloudFront エッジロケーション、または Application Load Balancer からのものです。

API Gateway、CloudFront、または Application Load Balancer が AWS WAF Classic に転送したウェブリクエストのサンプルを表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。
2. ナビゲーションペインで、リクエストを表示するウェブ ACL を選択します。
3. 右ペインで、[Requests] (リクエスト) タブを選択します。

   [Sampled requests] (サンプリングされたリクエスト) テーブルには、リクエストごとに次の値が表示されます。

   [Source IP] (送信元 IP)

   リクエストの発生元の IP アドレス (ビューワーが HTTP プロキシまたは Application Load Balancer を使用してリクエストを送信した場合は、そのプロキシまたは Application Load Balancer の IP アドレス)。

[URI]

リクエストの URI パス。リソースを識別します (例: `/images/daily-ad.jpg`)。これには、URI のクエリ文字列またはフラグメントコンポーネントは含まれません。詳細については、「Uniform Resource Identifier (URI): 一般的な構文」を参照してください。

[Matches rule] (一致ルール)

ウェブリクエストがすべての条件に一致したウェブ ACL の最初のルールを識別します。ウェブリクエストがウェブ ACL のすべてのルールのすべての条件に一致しない場合、[Matches rule] (ルールに一致) の値は [Default] (デフォルト) です。

ウェブリクエストがルールのすべての条件に一致し、そのルールのアクションが Count の場合、 AWS WAF Classic はウェブ ACL の後続のルールに基づいてウェブリクエストの検査を続行します。この場合、ウェブリクエストはサンプリングされたリクエストのリストに 2 回表示されることがあります。1 回は、アクションが [Count] (カウント) のルールに対応し、もう 1 回は、後続のルールまたはデフォルトアクションに対応します。

[Action] (アクション)

対応するルールのアクションが [Allow] (許可)、[Block] (ブロック)、[Count] (カウント) のいずれかであるかを示します。

[Time] (時間)

AWS WAF Classic が API Gateway、CloudFront、または Application Load Balancer からリクエストを受信した時刻。

4. リクエストに関する追加情報を表示するには、そのリクエストの IP アドレスの左側にある矢印を選択します。 AWS WAF Classic は次の情報を表示します。

[Source IP] (送信元 IP)

テーブルの [Source IP] (ソース IP) 列の値と同じ IP アドレス。

[Country] (国)

リクエスト送信元の国の 2 文字の国コード。ビューワーが HTTP プロキシまたは Application Load Balancer を使用してリクエストを送信する場合、これは HTTP プロキシまたは Application Load Balancer が存在する国の 2 文字の国コードです。

2 文字の国コードと対応する国名のリストについては、Wikipedia の「ISO 3166-1 alpha-2」記事を参照してください。

[Method] (メソッド)

リクエストの HTTP リクエストメソッド:
`GET`、`HEAD`、`OPTIONS`、`PUT`、`POST`、`PATCH`、`DELETE`。

[URI]

テーブルの [URI] 列の値と同じ URI。

[Request headers] (リクエストヘッダー)

リクエストのヘッダーとヘッダー値。

5. サンプルのリクエストのリストを更新するには、[Get new samples] (新しいサンプルを取得) を選択します。

で使用する AWS WAF Classic ルールグループの使用 AWS Firewall Manager

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

AWS WAF Classic ルールグループは、 AWS WAF Classic AWS Firewall Manager ポリシーに追加する一連のルールです。独自のルールグループを作成することも、マネージドルールグループを購入することもできます AWS Marketplace。

Important

Firewall Manager ポリシーに AWS Marketplace ルールグループを追加する場合は、まず組織内の各アカウントがそのルールグループにサブスクライブする必要があります。すべてのアカウントをサブスクライブしたら、ルールグループをポリシーに追加できます。詳細については、「AWS Marketplace ルールグループ」を参照してください。

トピック

- AWS WAF Classic ルールグループの作成
- AWS WAF Classic ルールグループへのルールの追加と削除

AWS WAF Classic ルールグループの作成

Warning

AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

Note

これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

で使用する AWS WAF Classic ルールグループを作成するときは AWS Firewall Manager、グループに追加するルールを指定します。

ルールグループを作成するには (コンソール)

1. 前提条件で設定した AWS Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fms。

> **Note**
>
> Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager デフォルトの管理者アカウントの作成」を参照してください。

2. ナビゲーションペインで、 AWS WAF クラシックに切り替えるを選択します。
3. AWS WAF Classic ナビゲーションペインで、ルールグループを選択します。
4. [Create rule group] (ルールグループの作成) を選択します。

> **Note**
>
> ルールグループにレートベースのルールを追加することはできません。

5. ルールグループに追加するルールを既に作成している場合は、[Use existing rules for this rule group] (このルールグループに既存のルールを使用する) を選択します。ルールグループに追加する新しいルールを作成する場合は、[Create rules and conditions for this rule group] (このルールグループにルールと条件を作成する) を選択します。
6. [Next] (次へ) を選択します。
7. ルールの作成を選択した場合は、「ルールの作成と条件の追加」のステップに従ってルールを作成します。

> **Note**
>
> AWS WAF Classic コンソールを使用してルールを作成します。

   必要なルールをすべて作成したら、次のステップに進みます。
8. ルールグループ名を入力します。
9. ルールグループにルールを追加するには、ルールを選択し、[Add rule] (ルールの追加) を選択します。ルールの条件に一致するリクエストを許可するか、ブロックするか、カウントするかを選択します。選択の詳細については、「AWS WAF Classic の仕組み」を参照してください。
10. ルールの追加が完了したら、[Create] (作成) を選択します。

AWS WAF WebACL に追加し、WebACL アクションを Override to Count に設定することで、ルールグループをテストできます。このアクションは、グループに含まれるルールに対して選択したアク

ションを上書きし、一致するリクエストのみカウントします。詳細については、「ウェブ ACL の作成」を参照してください。

AWS WAF Classic ルールグループへのルールの追加と削除

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

AWS WAF Classic ルールグループでルールを追加または削除できます。

ルールグループからルールを削除しても、ルール自体は削除されません。ルールグループからルールが削除されるだけです。

ルールグループにルールを追加または削除するには (コンソール)

1. 前提条件で設定した AWS Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fms。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager デフォルトの管理者アカウントの作成」を参照してください。

2. ナビゲーションペインで、 AWS WAF クラシックに切り替えるを選択します。
3. AWS WAF Classic ナビゲーションペインで、ルールグループを選択します。

4. 編集するルールグループを選択します。

> **Note**
>
> 編集したいルールグループが表示されない場合は、正しいリージョンが選択されていることを確認してください。Amazon CloudFront ディストリビューションの保護に使用されるルールグループの場合は、[グローバル (CloudFront)] 設定を使用します。

5. [Edit rule group] (ルールグループの編集) を選択します。
6. ルールを追加するには、次のステップを実行します。

   a. ルールを選択し、[Add rule to rule group] (ルールグループへのルールの追加) を選択します。ルールの条件に一致するリクエストを許可するか、ブロックするか、カウントするかを選択します。選択の詳細については、「AWS WAF Classic の仕組み」を参照してください。ルールグループにさらにルールを追加するには、この操作を繰り返します。

   > **Note**
   >
   > レートベースのルールをルールグループに追加することはできません。

   b. [Update] (更新) を選択します。
7. ルールを削除するには、次のステップを実行します。

   a. 削除するルールの横にある [X] を選択します。ルールグループからさらにルールを削除するには、この操作を繰り返します。

   b. [Update] (更新) を選択します。

AWS WAF Classic ルールを有効にする AWS Firewall Manager ための の開始方法

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

AWS Firewall Manager を使用して、 AWS WAF ルール、 AWS WAF Classic ルール、 AWS Shield Advanced 保護、Amazon VPC セキュリティグループを有効にできます。セットアップのステップはそれぞれ少し異なります。

- Firewall Manager を使用して の最新バージョンを使用するルールを有効にするには AWS WAF、このトピックを使用しないでください。代わりに、「AWS Firewall Manager AWS WAF ポリシーの設定」のステップに従います。
- Firewall Manager を使用して AWS Shield Advanced 保護を有効にするには、「」の手順に従いますAWS Firewall Manager AWS Shield Advanced ポリシーの設定。
- Firewall Manager を使用して Amazon VPC セキュリティグループを有効にするには、「AWS Firewall Manager Amazon VPC セキュリティグループポリシーの設定」のステップに従います。

Firewall Manager を使用して AWS WAF Classic ルールを有効にするには、次の手順を順番に実行します。

トピック

- ステップ 1: 前提条件を満たす
- ステップ 2: ルールを作成する
- ステップ 3: ルールグループを作成する
- ステップ 4: AWS Firewall Manager AWS WAF Classic ポリシーを作成して適用する

ステップ 1: 前提条件を満たす

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

AWS Firewall Managerのアカウントを準備するには、いくつかの必須のステップがあります。それらのステップは、AWS Firewall Manager 前提条件 で説明されています。「ステップ 2: ルールを作成する」に進む前に、すべての前提条件を満たしてください。

ステップ 2: ルールを作成する

> **Warning**
>
> AWS WAF Classic は計画されたend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

このステップでは、 AWS WAF Classic を使用してルールを作成します。使用する AWS WAF Classic ルールがすでにある場合は AWS Firewall Manager、このステップをスキップして に進みますステップ 3: ルールグループを作成する。

> **Note**
>
> AWS WAF Classic コンソールを使用してルールを作成します。

AWS WAF Classic ルールを作成するには (コンソール)

- ルールを作成し、ルールに条件を追加します。詳細については、「ルールの作成と条件の追加」を参照してください。

これで「ステップ 3: ルールグループを作成する」に進む準備ができました。

ステップ 3: ルールグループを作成する

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

ルールグループは、特定の一連の条件が満たされたときに実行するアクションを定義する一連のルールです。マネージドルールグループは から使用でき AWS Marketplace、独自のルールグループを作成できます。マネージドルールグループの詳細については、「AWS Marketplace ルールグループ」を参照してください。

独自のルールグループを作成するには、次の手順を実行します。

ルールグループを作成するには (コンソール)

1. 前提条件で設定した AWS Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fms。
2. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
3. 前提条件を満たしていない場合、問題を修正する方法についての指示がコンソールに表示されます。指示に従った後、このステップ (ルールグループを作成) を再試行します。前提条件を満たしている場合は、[Close] (閉じる) を選択します。
4. [Create policy] (ポリシーの作成) を選択します。

   [Policy type (ポリシータイプ)] で、[AWS WAF Classic] を選択します。
5. AWS Firewall Manager ポリシーの作成 を選択し、新しいルールグループを追加します。
6. を選択し AWS リージョン、次へを選択します。
7. 既にルールを作成しているため、条件を作成する必要はありません。[Next] (次へ) を選択します。
8. 既にルールを作成しているため、ルールを作成する必要はありません。[Next] (次へ) を選択します。
9. [Create rule group] (ルールグループの作成) を選択します。
10. [Name] (名前) で、わかりやすい名前を入力します。
11. AWS WAF Classic が作成し、ルールグループに関連付ける CloudWatch メトリクスの名前を入力します。名前に使用できるのは英数字 (A～Z、a～z、0～9) または特殊文字 _-!"#`+*},./ です。空白を含めることはできません。
12. ルールを選択してから、[Add rule] (ルールの追加) を選択します。ルールには、ルールの条件に一致するリクエストを許可するか、ブロックするか、カウントするかを選択できるアクション設定があります。このチュートリアルでは、[Count] (カウント) を選択します。ルールグループに必要なすべてのルールを追加するまで、ルールの追加を繰り返します。
13. [Create] (作成) を選択します。

これで「ステップ 4: AWS Firewall Manager AWS WAF Classic ポリシーを作成して適用する」に進む準備ができました。

ステップ 4: AWS Firewall Manager AWS WAF Classic ポリシーを作成して適用する

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

ルールグループを作成したら、 AWS Firewall Manager AWS WAF ポリシーを作成します。Firewall Manager AWS WAF ポリシーには、リソースに適用するルールグループが含まれます。

Firewall Manager AWS WAF ポリシーを作成するには (コンソール)

1. ルールグループを作成すると (前の手順の最後のステップ「ステップ 3: ルールグループを作成する」)、[Rule group summary] (ルールグループの概要) ページがコンソールに表示されます。[Next] (次へ) を選択します。
2. [Name] (名前) で、わかりやすい名前を入力します。
3. [Policy type] (ポリシータイプ) で、[WAF] を選択します。
4. リージョンで、 を選択します AWS リージョン。Amazon CloudFront のリソースを保護するには、[Global] (グローバル) を選択します。

   複数のリージョンのリソース (CloudFront リソースを除く) を保護するには、各リージョンに別々の Firewall Manager ポリシーを作成する必要があります。
5. 追加するルールグループを選択して、[Add rule group] (ルールグループの追加) を選択します。
6. ポリシーには、[Action set by rule group] (ルールグループによって設定されたアクション) と [Count] (カウント) の 2 つのアクションがあります。ポリシーをテストする場合は、アクション

を [Count] (カウント) に設定します。このアクションは、ポリシーに含まれるルールグループで指定されたブロックアクションを上書きします。つまり、ポリシーのアクションが [Count] (カウント) に設定されている場合、リクエストはカウントされ、ブロックされません。逆に、ポリシーのアクションを [Action set by rule group] (ルールグループによって設定されたアクション) に設定すると、ポリシー内のルールグループのアクションが使用されます。このチュートリアルでは、[Count] (カウント) を選択します。

7. [Next] (次へ) を選択します。
8. ポリシーに特定のアカウントのみを含める場合やポリシーから特定のアカウントを除外する場合には、[Select accounts to include/exclude from this policy (optional)] (このポリシーに含める/除外するアカウントを選択する (オプション)) を選択します。[Include only these accounts in this policy] (このアカウントのみをこのポリシーに含める) あるいは [Exclude these accounts from this policy](このアカウントをこのポリシーから除外する) のどちらかを選択します 1 つのオプションのみを選択できます。[Add] (追加) を選択します。含めるアカウント番号または除外するアカウント番号を選び、[OK] を選択します。

   > **Note**
   >
   > このオプションを選択しない場合、Firewall Manager は AWS Organizationsの組織内のすべてのアカウントにポリシーを適用します。組織に新しいアカウントを追加すると、Firewall Manager はそのアカウントにポリシーを自動的に適用します。

9. 保護するリソースのタイプを選択します。
10. 特定のタグを持つリソースのみを保護する場合、または特定のタグを持つリソースを除外する場合は、[Use tags to include/exclude resources] (タグを使用してリソースを含める/除外する) を選択し、タグを入力してから、[Include] (含める) または [Exclude] (除外) を選択します。1 つのオプションのみを選択できます。

    複数のタグをコンマで区切って入力する場合、リソースにこれらのタグのいずれかがある場合は一致するとみなされます。

    タグの詳細については、「タグエディタの使用」を参照してください。
11. [Create and apply this policy to existing and new resources] (既存および新規のリソースにこのポリシーを作成して適用する) を選択します。

    このオプションでは、 の組織内の該当する各アカウントにウェブ ACL を作成し AWS Organizations、そのウェブ ACL をアカウント内の指定されたリソースに関連付けます。このオプションは、前述の基準 (リソースタイプとタグ) に一致するすべての新しいリソースにもポリ

シーを適用します。また、[Create but do not apply this policy to existing or new resources] (作成するが既存および新規のリソースにこのポリシーを適用しない) を選択する場合は、Firewall Manager により組織内の各関連アカウントにウェブ ACL が作成されますが、ウェブ ACL はいずれのリソースにも適用されません。ポリシーは後でリソースに適用する必要があります。

12. [Replace existing associated web ACLs] (既存の関連付けられたウェブ ACL を置換) の選択肢は、デフォルト設定のままにします。

    このオプションを選択すると、Firewall Manager は、新しいポリシーのウェブ ACL を関連付ける前に、範囲内のリソースから既存のウェブ ACL の関連付けをすべて削除します。

13. [Next] (次へ) を選択します。

14. 新しいポリシーを確認します。設定を変更するには、[Edit] (編集) を選択します。ポリシーが完成したら、[Create policy] (ポリシーの作成) を選択します。

チュートリアル: 階層ルールによる AWS Firewall Manager ポリシーの作成

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

を使用すると AWS Firewall Manager、階層ルールを含む AWS WAF Classic 保護ポリシーを作成して適用できます。つまり、特定のルールを一元的に作成および適用し、アカウント固有ルールの作成やメンテナンスを個々のユーザーに委任できるということです。一元的に適用する (共通) ルールを常に一貫して適用するために、誤操作による削除やその他の処理が行われないようモニタリングでき

ます。アカウント固有のルールでは、個々のチームのニーズに合わせてカスタマイズされた保護をさらに追加できます。

> **Note**
>
> の最新バージョンでは AWS WAF、この機能は組み込まれており、特別な処理は必要ありません。 AWS WAF Classic をまだ使用していない場合は、代わりに最新バージョンを使用してください。「の AWS Firewall Manager ポリシーの作成 AWS WAF」を参照してください。

次のチュートリアルでは、保護ルールの階層セットを作成する方法について説明します。

トピック

- ステップ 1: Firewall Manager 管理者アカウントを指定する
- ステップ 2: Firewall Manager 管理者アカウントを使用してルールグループを作成する
- ステップ 3: Firewall Manager ポリシーを作成して共通のルールグループをアタッチする
- ステップ 4: アカウント固有のルールを追加する
- 結論

ステップ 1: Firewall Manager 管理者アカウントを指定する

を使用するには AWS Firewall Manager、組織内のアカウントを Firewall Manager 管理者アカウントとして指定する必要があります。このアカウントは、組織内の管理アカウントまたはメンバーアカウントのいずれでもかまいません。

Firewall Manager 管理者アカウントを使用すると、組織内の他のアカウントに適用する一連の共通ルールを作成できます。組織内の他のアカウントでは、このように一元的に適用されたルールを変更することはできません。

アカウントを Firewall Manager 管理者アカウントに指定して、Firewall Manager を使用するための外の前提条件を満たすには、「AWS Firewall Manager 前提条件」の説明を参照してください。前提条件を既に満たしている場合は、このチュートリアルのステップ 2 に進むことができます。

このチュートリアルでは、この管理者アカウントを **`Firewall-Administrator-Account`** と呼びます。

ステップ 2: Firewall Manager 管理者アカウントを使用してルールグループを作成する

次に、**Firewall-Administrator-Account** を使用してルールグループを作成します。このルールグループには、次のステップで作成するポリシーで管理されるすべてのメンバーアカウントに適用する共通ルールを指定します。これらのルールとコンテナルールグループを変更できるのは、**Firewall-Administrator-Account** のみです。

このチュートリアルでは、このコンテナルールグループを **Common-Rule-Group** と呼びます。

ルールグループを作成するには、「AWS WAF Classic ルールグループの作成」の手順を参照してください。これらの手順に従う際には、Firewall Manager 管理者アカウント (**Firewall-Administrator-Account**) を使用してコンソールにサインインしておいてください。

ステップ 3: Firewall Manager ポリシーを作成して共通のルールグループをアタッチする

Firewall-Administrator-Account を使用して、Firewall Manager ポリシーを作成します。このポリシーを作成する場合は、次を実行する必要があります。

- 新しいポリシーに **Common-Rule-Group** を追加する。
- **Common-Rule-Group** を適用する組織内のすべてのアカウントを含める。
- **Common-Rule-Group** を適用するすべてのリソースを追加する。

ポリシーの作成手順については、「AWS Firewall Manager ポリシーの作成」を参照してください。

これにより、指定された各アカウントにウェブ ACL が作成され、各ウェブ ACL に **Common-Rule-Group** が追加されます。ポリシーの作成後、このウェブ ACL および共通ルールは、指定されたすべてのアカウントにデプロイされます。

このチュートリアルでは、このウェブ ACL を **Administrator-Created-ACL** と呼びます。これで、組織内の指定されたメンバーアカウントごとに、一意の **Administrator-Created-ACL** が作成されます。

ステップ 4: アカウント固有のルールを追加する

組織内の各メンバーアカウントは、アカウントに存在する **Administrator-Created-ACL** に、アカウント固有のルールを自分で追加できます。にすでに存在する一般的なルールは、新しいアカ

ウント固有のルールとともに**Administrator-Created-ACL**引き続き適用されます。 は、ルールがウェブ ACL に表示される順序に基づいてウェブリクエスト AWS WAF を検査します。これは、**Administrator-Created-ACL** とアカウント固有のルールの両方に当てはまります。

ルールを **Administrator-Created-ACL** に追加するには、[での保護パック (ウェブ ACL) の編集 AWS WAF] を参照してください。

結論

これで、Firewall Manager 管理者が管理する共通ルールが含まれたウェブ ACL と、各メンバーアカウントで管理するアカウント固有のルールを作成できました。

各アカウントの **Administrator-Created-ACL** は、1 つの **Common-Rule-Group** を参照しています。このため、今後 Firewall Manager 管理者アカウントによって **Common-Rule-Group** が変更されると、各メンバーアカウントに直ちに反映されます。

メンバーアカウントでは、**Common-Rule-Group** に指定されている共通ルールを変更または削除することはできません。

アカウント固有のルールは、他のアカウントに影響しません。

ウェブ ACL トラフィック情報のログ記録

> **Warning**
>
> AWS WAF Classic は計画されたend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、[AWS WAF Classic リソースの への移行 AWS WAF] を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

> **Note**
>
> Amazon Security Lake を使用して AWS WAF Classic データを収集することはできません。

ログ記録を有効にして、ウェブ ACL で分析されるトラフィックに関する詳細情報を取得できます。ログに含まれる情報には、 AWS WAF Classic が AWS リソースからリクエストを受信した時間、リクエストに関する詳細情報、および各リクエストが一致したルールのアクションが含まれます。

開始するには、Amazon Kinesis Data Firehose をセットアップします。このプロセスの一環として、ログの保存先を選択します。次に、ログ記録を有効にするウェブ ACL を選択します。ログ記録を有効にすると、 は Firehose を介してストレージ宛先にログを AWS WAF 配信します。

Amazon Kinesis Data Firehose を作成し、保存されているログを確認する方法については、「What Is Amazon Data Firehose?」を参照してください。Kinesis Data Firehose の設定に必要な許可を理解するには、「Controlling Access with Amazon Kinesis Data Firehose」(Amazon Kinesis Data Firehose によるアクセスの制御) を参照してください。

ログ記録を正常に有効化するには、次の許可がある必要があります。

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `waf:PutLoggingConfiguration`

サービスにリンクされたロールおよび `iam:CreateServiceLinkedRole` 許可の詳細については、「AWS WAF Classic のサービスにリンクされたロールの使用」を参照してください。

ウェブ ACL でログ記録を有効にするには

1. Amazon Kinesis Data Firehose を「aws-waf-logs-」で始まるプレフィックスを使用して作成します (例: `aws-waf-logs-us-east-2-analytics`)。PUT ソースを使用して、動作しているリージョンでデータ Firehose を作成します。Amazon CloudFront のログをキャプチャしている場合は、米国東部 (バージニア北部) に Firehose を作成します。詳細については、「Amazon Data Firehose 配信ストリームの作成」を参照してください。

   > **Important**
   >
   > ソースとして `Kinesis stream` を選択しないでください。

1 つの AWS WAF Classic ログは、1 つの Firehose レコードに相当します。通常、1 秒あたり 10,000 件のリクエストを受信していて、完全なログを有効にする場合、Firehose には 1 秒あたり 10,000 件のレコード設定を行う必要があります。Firehose を正しく設定しないと、 AWS WAF Classic はすべてのログを記録しません。詳細については、「Amazon Kinesis Data Firehose Quotas」(Amazon Kinesis Data Firehose のクォータ) を参照してください。

2. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示される場合は、それを選択します。

3. ナビゲーションペインで [Web ACLs] (ウェブ ACL) を選択します。
4. ログ記録を有効にするウェブ ACL の名前を選択します。これにより、右ペインで、ウェブ ACL の詳細を含むページが開きます。
5. [Logging] (ログ記録) タブで [Enable logging] (ログの有効化) を選択します。
6. 最初のステップで作成した Kinesis Data Firehose を選択します。「aws-waf-logs-」ではじまる Firehose を選択する必要があります。
7. (オプション) 特定のフィールドとその値がログに含まれることを希望しない場合には、このフィールドをマスキングします。マスキングするフィールドを選び、[Add] (追加) を選択します。必要に応じて手順を繰り返し、追加のフィールドをマスキングします。マスキングされたフィールドは、ログに REDACTED と表示されます。例えば、[cookie] フィールドをマスキングした場合、ログ内の [cookie] フィールドは REDACTED となります。
8. [Enable logging] (ログの有効化) を選択します。

> **Note**
>
> ログ記録を正常に有効にすると、 AWS WAF Classic は Amazon Kinesis Data Firehose にログを書き込むために必要なアクセス許可を持つサービスにリンクされたロールを作成します。詳細については、「AWS WAF Classic のサービスにリンクされたロールの使用」を参照してください。

ウェブ ACL でログ記録を無効にするには

1. ナビゲーションペインで [Web ACLs] (ウェブ ACL) を選択します。

2. ログ記録を無効にするウェブ ACL の名前を選択します。これにより、右ペインで、ウェブ ACL の詳細を含むページが開きます。
3. [Logging] (ログ記録) タブで [Disable logging] (ログの無効化) を選択します。
4. 確認ダイアログボックスで、[Disable logging] (ログの無効化) を選択します。

Exampleログの例

```
{

 "timestamp":1533689070589,
 "formatVersion":1,
 "webaclId":"385cb038-3a6f-4f2f-ac64-09ab912af590",
 "terminatingRuleId":"Default_Action",
 "terminatingRuleType":"REGULAR",
 "action":"ALLOW",
 "httpSourceName":"CF",
 "httpSourceId":"i-123",
 "ruleGroupList":[
                         {
                          "ruleGroupId":"41f4eb08-4e1b-2985-92b5-e8abf434fad3",
                          "terminatingRule":null,
                          "nonTerminatingMatchingRules":[
                                                          {"action" : "COUNT",
                                                          "ruleId" :
 "4659b169-2083-4a91-bbd4-08851a9aaf74"}
                                                         ],
                          "excludedRules":               [
                                                          {"exclusionType" :
 "EXCLUDED_AS_COUNT",
                                                           "ruleId" :
 "5432a230-0113-5b83-bbb2-89375c5bfa98"}
                                                         ]
                         }
                        ],

 "rateBasedRuleList":[
                             {
                              "rateBasedRuleId":"7c968ef6-32ec-4fee-96cc-51198e412e7f",

                              "limitKey":"IP",
```

```
                                "maxRateAllowed":100

                               },
                               {
                                "rateBasedRuleId":"462b169-2083-4a93-bbd4-08851a9aaf30",
                                "limitKey":"IP",
                                "maxRateAllowed":100
                                }
                                ],

 "nonTerminatingMatchingRules":[
                                        {"action" : "COUNT",

                                        "ruleId" : "4659b181-2011-4a91-
bbd4-08851a9aaf52"}
                                       ],

 "httpRequest":{
                        "clientIp":"192.10.23.23",

                        "country":"US",

                        "headers":[

                                   {
                                    "name":"Host",
                                    "value":"127.0.0.1:1989"
                                   },
                                   {
                                    "name":"User-Agent",
                                    "value":"curl/7.51.2"
                                   },
                                   {
                                    "name":"Accept",
                                    "value":"*/*"
                                   }
                                 ],
                      "uri":"REDACTED",
                      "args":"usernam=abc",
                      "httpVersion":"HTTP/1.1",
                      "httpMethod":"GET",
                      "requestId":"cloud front Request id"
                      }
```

```
}
```

以下ではこれらのログに示されている各項目について説明しています。

timestamp

タイムスタンプ (ミリ秒単位)。

formatVersion

ログの形式バージョン。

webaclId

ウェブ ACL の GUID。

terminatingRuleId

リクエストを終了したルールの ID。リクエストを終了したものがない場合、この値は `Default_Action` となります。

terminatingRuleType

リクエストを終了したルールのタイプ。可能な値は、RATE_BASED、REGULAR、GROUP です。

action

アクション。終了ルールの可能な値は、ALLOW および BLOCK です。COUNT は、終了ルールの有効な値ではありません。

terminatingRuleMatchDetails

リクエストに一致した終了ルールに関する詳細情報。終了ルールには、ウェブリクエストに対する検査プロセスを終了するアクションがあります。終了ルールに対して実行できるアクションは、ALLOW および BLOCK です。これは、SQL インジェクションおよびクロスサイトスクリプティング (XSS) 一致ルールステートメントに対してのみ設定されます。複数の対象を検査するすべてのルールステートメントと同様、 AWS WAF は最初の一致にアクションを適用し、ウェブリクエストの検査を停止します。終了アクションを伴うウェブリクエストには、ログで報告された脅威に加えて、他の脅威が含まれている可能性があります。

httpSourceName

リクエストの送信元。有効な値: CF (ソースが Amazon CloudFront である場合)、APIGW (ソースが Amazon API Gateway である場合)、および ALB (ソースが Application Load Balancer である場合)。

httpSourceId

ソース ID。このフィールドには、関連する Amazon CloudFront ディストリビューションの ID、API Gateway の REST API、または Application Load Balancer の名前が表示されます。

ruleGroupList

このリクエストで動作したルールグループのリスト。前述のコード例では、1 つのみです。

ruleGroupId

ルールグループの ID ルールがリクエストをブロックした場合、`ruleGroupID` の ID は、`terminatingRuleId` の ID と同じです。

terminatingRule

リクエストを終了したルールグループ内のルール。これが Null 以外の値の場合、[ruleid] および [action] (アクション) も含まれます。この場合、アクションは常に BLOCK です。

nonTerminatingMatchingRules

リクエストに一致するルールグループ内のルールのリスト。これは常に COUNT ルール (一致する非終了ルール) です。

action (nonTerminatingMatchingRules group)

これは常に COUNT (一致する非終了ルール) です。

ruleId (nonTerminatingMatchingRules group)

リクエストに一致する非終了ルールグループ内のルールの ID。これが COUNT ルールです。

excludedRules

除外されているルールグループ内のルールのリスト。これらのルールのアクションは [COUNT] に設定されます。

exclusionType (excludedRules group)

除外されたルールにアクション COUNT があることを示すタイプ。

ruleId (excludedRules group)

除外されたルールグループ内のルールの ID。

rateBasedRuleList

このリクエストで動作したレートベースのルールのリスト。

rateBasedRuleId

このリクエストで動作したレートベースのルールの ID。これがリクエストを終了した場合、`rateBasedRuleId` の ID は、`terminatingRuleId` の ID と同じです。

limitKey

が 1 つのソースからリクエストが到着する可能性が高く、レートモニタリングの対象となるかどうかを判断するために AWS WAF 使用する フィールド。可能性のある値は IP です。

maxRateAllowed

5 分間に許可される `limitKey` で指定されたフィールドに同じ値を持つ、リクエストの最大数。リクエストの数が を超え`maxRateAllowed`、ルールで指定された他の述語も満たされた場合、はこのルールに指定されたアクションを AWS WAF トリガーします。

httpRequest

リクエストに関するメタデータです。

clientIp

リクエストを送信するクライアントの IP アドレス。

country

リクエストの送信国。 AWS WAF が原産国を特定できない場合は、このフィールドを に設定します-。

headers

ヘッダーの一覧。

uri

リクエストの URI。上記のコードの例では、このフィールドがマスキングされた場合の値を示しています。

args

クエリ文字列。

httpVersion

HTTP のバージョン。

httpMethod

リクエストの HTTP メソッド。

requestId

リクエストの ID。

レートベースのルールごとにブロックされている IP アドレスの一覧表示

> **Warning**
>
> AWS WAF Classic は計画されたend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

AWS WAF Classic は、レートベースのルールによってブロックされている IP アドレスのリストを提供します。

レートベースのルールごとにブロックされているアドレスを表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF コンソールを開きます。

   ナビゲーションペインに AWS WAF 「クラシックに切り替える」と表示されている場合は、それを選択します。
2. ナビゲーションペインで [Rules] (ルール) を選択します。
3. [Name] (名前) 列で、レートベースのルールを選択します。

一覧には、ルールによって現在ブロックされている IP アドレスが表示されます。

AWS WAF Classic が Amazon CloudFront 機能と連携する方法

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

ウェブ ACL を作成するときに、 AWS WAF Classic が検査する 1 つ以上の CloudFront ディストリビューションを指定できます。 AWS WAF Classic は、ウェブ ACL で識別した条件に基づいて、それらのディストリビューションのウェブリクエストを許可、ブロック、またはカウントし始めます。CloudFront には、 AWS WAF Classic の機能を強化する機能がいくつか用意されています。この章では、CloudFront と AWS WAF Classic の連携を改善するように CloudFront を設定するいくつかの方法について説明します。

トピック

- CloudFront カスタムエラーページでの AWS WAF Classic の使用
- 独自の HTTP サーバーで実行されているアプリケーションに CloudFront で AWS WAF Classic を使用する
- CloudFront が応答する HTTP メソッドの選択

CloudFront カスタムエラーページでの AWS WAF Classic の使用

AWS WAF Classic は、指定した条件に基づいてウェブリクエストをブロックすると、HTTP ステータスコード 403 (禁止) を CloudFront に返します。次に、CloudFront はそのステータスコードをビューワーに返します。ビューワーには、以下のような簡潔で特に書式設定されていないデフォルトメッセージが表示されます。

```
Forbidden: You don't have permission to access /myfilename.html on this server.
```

デフォルトメッセージはなく、お客様のウェブサイトの他のページと同じ書式設定のカスタムエラーメッセージを表示することを希望する場合は、カスタムエラーメッセージを含むオブジェクト (HTML ファイルなど) をビューワーに返すように CloudFront を設定できます。

> **Note**
>
> CloudFront は、オリジンから返される HTTP ステータスコード 403 と、リクエストがブロックされたときに AWS WAF Classic から返される HTTP ステータスコード 403 を区別できません。つまり、HTTP ステータスコード 403 のさまざまな原因に基づいて、異なるカスタムエラーページを返すことはできません。

CloudFront カスタムエラーページの詳細については、「Amazon CloudFront デベロッパーガイド」の「エラーレスポンスのカスタマイズ」を参照してください。

独自の HTTP サーバーで実行されているアプリケーションに CloudFront で AWS WAF Classic を使用する

CloudFront で AWS WAF Classic を使用すると、Amazon Elastic Compute Cloud (Amazon EC2) で実行されているウェブサーバーでも、プライベートに管理するウェブサーバーでも、任意の HTTP ウェブサーバーで実行されているアプリケーションを保護できます。CloudFront と独自のウェブサーバー間、およびビューワーと CloudFront の間で HTTPS が必須になるように CloudFront を設定することもできます。

CloudFront と独自のウェブサーバー間での HTTPS の必須化

CloudFront と独自のウェブサーバー間で HTTPS を必須にするには、CloudFront カスタムオリジン機能を使用し、特定のオリジンの [Origin Protocol Policy] (オリジンプロトコルポリシー) お

よび [Origin Domain Name] (オリジンドメイン名) の設定を構成します。CloudFront 設定では、オリジンからオブジェクトをフェッチするとき CloudFront で使用するポートとプロトコルとともに、サーバーの DNS 名を指定できます。また、カスタムオリジンサーバー上の SSL/TLS 証明書が、設定したオリジンドメイン名と一致することを確認する必要もあります。の外部で独自の HTTP ウェブサーバーを使用する場合は AWS、信頼できるサードパーティー認証機関 (CA) によって署名された証明書を使用する必要があります。例えば、Comodo、DigiCert、Symantec などです。CloudFront と独自のウェブサーバー間の通信に HTTPS を要求する方法の詳細については、「Amazon CloudFront デベロッパーガイド」の「CloudFront とカスタムオリジン間の通信で HTTPS を必須にする」のトピックを参照してください。

ビューワーと CloudFront との間での HTTPS の必須化

ビューワーと CloudFront の間に HTTPS を要求するために、CloudFront ディストリビューションの 1 つ以上のキャッシュ動作のビューワープロトコルポリシーを変更できます。ビューワーと CloudFront 間での HTTPS の使用の詳細については、「Amazon CloudFront デベロッパーガイド」の「ビューワーと CloudFront 間の通信で HTTPS を必須にする」のトピックを参照してください。独自の SSL 証明書を使用して、ビューワーが独自のドメイン名を使用して HTTPS 経由で CloudFront ディストリビューションに接続できるようにすることもできます (例: https://www.mysite.com)。詳細については、「Amazon CloudFront デベロッパーガイド」の「代替ドメイン名とHTTPS を使用する」のトピックを参照してください。

CloudFront が応答する HTTP メソッドの選択

Amazon CloudFront のウェブディストリビューションを作成するときは、CloudFront によって処理されてオリジンに転送される HTTP メソッドを選択します。次のオプションから選択できます。

- [GET, HEAD] - CloudFront を使用して、オリジンからのオブジェクトの取得またはオブジェクトヘッダーの取得のみを行うことができます。
- [GET, HEAD, OPTIONS] - CloudFront を使用して、オリジンからのオブジェクトの取得、オブジェクトヘッダーの取得、またはオリジンサーバーがサポートするオプションのリスト取得のみを行うことができます。
- [GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE] - CloudFront を使用して、オブジェクトの取得、追加、更新、削除、およびオブジェクトヘッダーの取得を行うことができます。また、ウェブフォームからのデータの送信など、その他の POST 操作も実行できます。

で説明されているように、 AWS WAF Classic 文字列一致条件を使用して、HTTP メソッドに基づいてリクエストを許可またはブロックすることもできます文字列一致条件の使用。GET や な

ど、CloudFront がサポートするメソッドの組み合わせを使用する場合はHEAD、他のメソッドを使用するリクエストをブロックするように AWS WAF Classic を設定する必要はありません。GET、、など、CloudFront がサポートしていないメソッドの組み合わせを許可する場合はPOST、すべてのメソッドに応答するように CloudFront HEADを設定し、 AWS WAF Classic を使用して他のメソッドを使用するリクエストをブロックできます。

が応答するメソッドの選択の詳細については、「Amazon CloudFront デベロッパーガイド」で「ウェブディストリビューションを作成または更新する場合に指定する値」トピックの「許可される HTTP メソッド」を参照してください。

AWS WAF Classic のセキュリティ

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

でのクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを活用できます。

セキュリティは、 AWS お客様とお客様の間の責任共有です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ – AWS は、 で AWS サービスを実行するインフラストラクチャを保護する責任を担います AWS クラウド。 は、お客様が安全に使用できるサービス AWS も提供します。セキュリティの有効性は、AWS コンプライアンスプログラムの一環として、サードパーティーの審査機関によって定期的にテストおよび検証されています。 AWS WAF Classic に適用されるコン

プライアンスプログラムの詳細については、AWS「コンプライアンスプログラムによる対象範囲内のサービス」を参照してください。

- クラウド内のセキュリティ — お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、お客様のデータの機密性、組織の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、 AWS WAF Classic を使用する際の責任共有モデルの適用方法を理解するのに役立ちます。以下のトピックでは、セキュリティとコンプライアンスの目的を達成するように AWS WAF Classic を設定する方法について説明します。また、 AWS WAF Classic リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

- AWS WAF Classic でのデータ保護
- AWS WAF Classic の Identity and Access Management
- AWS WAF Classic でのログ記録とモニタリング
- AWS WAF Classic のコンプライアンス検証
- AWS WAF Classic の耐障害性
- AWS WAF Classic のインフラストラクチャセキュリティ

AWS WAF Classic でのデータ保護

> **Warning**
>
> AWS WAF Classic は計画されたend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

AWS WAF Classic AWS でのデータ保護には、 責任共有モデルが適用されます。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「 AWS のサービス 」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「Data Privacy FAQChina」を参照してください。 欧州におけるデータ保護に関する情報については、General Data Protection Regulation (GDPR) Center を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM アイデンティティセンターまたは AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須ですが、TLS 1.3 を推奨します。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール、API、または SDK を使用して AWS WAF Classic AWS CLIまたは他の AWS のサービス を使用する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

AWS WAF ウェブ ACLs、ルール、条件などのクラシックエンティティは、中国 (北京) や中国 (寧夏) など、暗号化が利用できない特定のリージョンを除き、保管時に暗号化されます。リージョンごとに一意の暗号化キーが使用されます。

AWS WAF Classic リソースの削除

AWS WAF Classic で作成したリソースを削除できます。次のセクションの各リソースタイプのガイダンスを参照してください。

- ウェブ ACL の削除
- AWS WAF Classic ルールグループへのルールの追加と削除
- ルールの削除

AWS WAF Classic の Identity and Access Management

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、まだ最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に AWS WAF Classic リソースの使用を許可する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで使用できる AWS のサービス です。

トピック

- オーディエンス
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- AWS WAF Classic と IAM の連携方法
- AWS WAF Classic のアイデンティティベースのポリシーの例
- AWS WAF Classic のアイデンティティとアクセスのトラブルシューティング
- AWS WAF Classic のサービスにリンクされたロールの使用

オーディエンス

AWS Identity and Access Management (IAM) の使用方法は、 AWS WAF Classic で行う作業によって異なります。

サービスユーザー – AWS WAF Classic サービスを使用してジョブを実行する場合、管理者は必要な認証情報とアクセス許可を提供します。さらに多くの AWS WAF Classic 機能を使用して作業を行う場合は、追加のアクセス許可が必要になる場合があります。アクセスの管理方法を理解すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。 AWS WAF Classic の特徴にアクセスできない場合は、「AWS WAF Classic のアイデンティティとアクセスのトラブルシューティング」を参照してください。

サービス管理者 – 社内の AWS WAF Classic リソースを担当している場合は、通常 Classic AWS WAF へのフルアクセスがあります。サービスユーザーがどの AWS WAF Classic 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。会社が AWS WAF Classic で IAM を使用する方法の詳細については、「」を参照してくださいAWS WAF Classic と IAM の連携方法。

IAM 管理者 – IAM 管理者は、 AWS WAF Classic へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できる AWS WAF Classic アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS WAF Classic のアイデンティティベースのポリシーの例。

アイデンティティを使用した認証

認証は、ID 認証情報 AWS を使用して にサインインする方法です。、IAM ユーザー AWS アカウントのルートユーザー、または IAM ロールを引き受けることで認証される必要があります。

AWS IAM アイデンティティセンター (IAM Identity Center)、シングルサインオン認証、Google/Facebook 認証情報などの ID ソースからの認証情報を使用して、フェデレーティッド ID としてサインインできます。サインインの詳細については、「AWS サインイン ユーザーガイド」の「AWS アカウントにサインインする方法」を参照してください。

プログラムによるアクセスの場合、 は SDK と CLI AWS を提供してリクエストを暗号化して署名します。詳細については、「IAM ユーザーガイド」の「API リクエストに対するAWS 署名バージョン 4」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、まず、すべての AWS のサービス および リソースへの完全なアクセス権を持つ AWS アカウント root ユーザーと呼ばれる 1 つのサインインアイデンティティから始めます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザー認証情報を必要とするタスクについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーテッドアイデンティティ

ベストプラクティスとして、人間のユーザーが一時的な認証情報 AWS のサービス を使用して にアクセスするには、ID プロバイダーとのフェデレーションを使用する必要があります。

フェデレーティッド ID は、エンタープライズディレクトリ、ウェブ ID プロバイダー、または ID ソースの認証情報 AWS のサービス を使用して Directory Service にアクセスするユーザーです。フェデレーテッドアイデンティティは、一時的な認証情報を提供するロールを引き受けます。

アクセスを一元管理する場合は、 AWS IAM アイデンティティセンターをお勧めします。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「IAM アイデンティティセンターとは」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、特定の個人やアプリケーションに対する特定のアクセス許可を持つアイデンティティです。長期認証情報を持つ IAM ユーザーの代わりに一時的な認証情報を使用することをお勧めします。詳細については、IAM ユーザーガイドの「ID プロバイダーとのフェデレーションを使用して にアクセスする必要がある AWS」を参照してください。

IAM グループは、IAM ユーザーの集合を指定し、大量のユーザーに対するアクセス許可の管理を容易にします。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可を持つアイデンティであり、一時的な認証情報を提供します。ユーザーから IAM ロール (コンソール) に切り替えるか、 または API オペレーションを呼び出すことで、ロールを引き受けることができます。 AWS CLI AWS 詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールは、フェデレーションユーザーアクセス、一時的な IAM ユーザーのアクセス許可、クロスアカウントアクセス、クロスサービスアクセス、および Amazon EC2 で実行するアプリケーションに役立ちます。詳細については、IAM ユーザーガイド の IAM でのクロスアカウントリソースアクセス を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは、ID またはリソースに関連付けられている場合のアクセス許可を定義します。 は、プリンシパルがリクエストを行うときに、これらのポリシー AWS を評価します。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は、ポリシーを使用して、どのプリンシパルがどのリソースに対して、どのような条件でアクションを実行できるかを定義することで、誰が何にアクセスできるかを指定します。

デフォルトでは、ユーザーやロールにアクセス許可はありません。IAM 管理者は IAM ポリシーを作成してロールに追加し、このロールをユーザーが引き受けられるようにします。IAM ポリシーは、オペレーションの実行方法を問わず、アクセス許可を定義します。

アイデンティティベースのポリシー

アイデンティティベースのポリシーは、アイデンティティ (ユーザー、グループ、またはロール) にアタッチできる JSON アクセス許可ポリシードキュメントです。これらのポリシーは、アイデンティティがどのリソースに対してどのような条件下でどのようなアクションを実行できるかを制御します。アイデンティティベースポリシーの作成方法については、IAM ユーザーガイド の カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する を参照してください。

アイデンティティベースのポリシーは、インラインポリシー (単一の ID に直接埋め込む) または管理ポリシー (複数の ID にアタッチされたスタンドアロンポリシー) にすることができます。管理ポリシーとインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。例としては、IAM ロール信頼ポリシーや Amazon S3 バケットポリシーなどがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするためのアクセス許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、および Amazon VPC は AWS WAF、ACLs。ACL の詳細については、Amazon Simple Storage Service デベロッパーガイド の アクセスコントロールリスト (ACL) の概要 を参照してください。

その他のポリシータイプ

AWS は、より一般的なポリシータイプによって付与されるアクセス許可の最大数を設定できる追加のポリシータイプをサポートしています。

- アクセス許可の境界 – アイデンティティベースのポリシーで IAM エンティティに付与することのできるアクセス許可の数の上限を設定します。詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可境界」を参照してください。
- サービスコントロールポリシー (SCP) - AWS Organizations内の組織または組織単位の最大のアクセス許可を指定します。詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」を参照してください。
- リソースコントロールポリシー (RCP) – は、アカウント内のリソースで利用できる最大数のアクセス許可を定義します。詳細については、「AWS Organizations ユーザーガイド」の「リソースコントロールポリシー (RCP)」を参照してください。
- セッションポリシー – ロールまたはフェデレーションユーザーの一時セッションを作成する際にパラメータとして渡される高度なポリシーです。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成されるアクセス許可を理解するのがさらに難しくなります。が複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、「IAM ユーザーガイド」の「ポリシー評価ロジック」を参照してください。

AWS WAF Classic と IAM の連携方法

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

IAM を使用して AWS WAF Classic へのアクセスを管理する前に、 AWS WAF Classic で使用できる IAM 機能を確認してください。

AWS WAF Classic で使用できる IAM 機能

IAM 機能	AWS WAF クラシックサポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	はい

IAM 機能	AWS WAF クラシックサポート
ポリシー条件キー (サービス固有)	はい
ACL	なし
ABAC (ポリシー内のタグ)	部分的
一時認証情報	あり
転送アクセスセッション (FAS)	あり
サービスロール	あり
サービスにリンクされたロール	はい

AWS WAF Classic およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要については、IAM ユーザーガイドのAWS 「IAM と連携する のサービス」を参照してください。

AWS WAF Classic のアイデンティティベースのポリシー

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

AWS WAF Classic アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS WAF Classic のアイデンティティベースのポリシーの例。

AWS WAF Classic 内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーで、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、全体のアカウント、または別のアカウントの IAM エンティティを、リソースベースのポリシーのプリンシパルとして指定します。詳細については、IAM ユーザーガイドのIAM でのクロスアカウントリソースアクセスを参照してください。

AWS WAF Classic のポリシーアクション

ポリシーアクションのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action` 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

AWS WAF Classic アクションのリストを確認するには、「サービス認可リファレンス」の「 で定義されるアクション AWS WAF」およびAWS WAF 「リージョンで定義されるアクション」を参照してください。

AWS WAF Classic のポリシーアクションは、アクションの前に次のプレフィックスを使用します。

```
waf
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "waf:action1",
      "waf:action2"
         ]
```

ワイルドカード (*) を使用すると、複数のアクションを指定することができます。たとえば、 で始まる AWS WAF Classic のすべてのアクションを指定するにはList、次のアクションを含めます。

```
"Action": "waf:List*"
```

AWS WAF Classic アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS WAF Classic のアイデンティティベースのポリシーの例。

AWS WAF Classic のポリシーリソース

ポリシーリソースのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Resource JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。リソースレベルのアクセス許可をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

AWS WAF Classic リソースタイプとその ARNs「 で定義されるリソース AWS WAF」およびAWS WAF 「リージョンで定義されるリソース」を参照してください。 各リソースの ARN を指定できるアクションについては、「 で定義されるアクション AWS WAF」およびAWS WAF 「 リージョンで定義されるアクション」を参照してください。 AWS WAF Classic リソースのサブセットへのアクセスを許可または拒否するには、ポリシーの resource要素にリソースの ARN を含めます。

AWS WAF Classic では、リソースはウェブ ACLsとルールです。 AWS WAF Classic は、バイト一致、IP 一致、サイズ制約などの条件もサポートしています。

これらのリソースと条件には、次の表に示すとおり、一意の Amazon リソースネーム (ARN) が関連付けられています。

AWS WAF コンソールの名前	AWS WAF SDK/CLI の名前	ARN 形式	
ウェブ ACL	WebACL	arn:aws:waf:: *account*:*webacl*/*ID*	

AWS WAF コンソールの名前	AWS WAF SDK/CLI の名前	ARN 形式
ルール	Rule	arn:aws:waf:: *account*:*rule*/*ID*
文字列一致条件	ByteMatchSet	arn:aws:waf:: *account*:*bytematchset* /*ID*
SQL のインジェクション一致の状態	SqlInjectionMatchSet	arn:aws:waf:: *account*:*sqlinjectionset* /*ID*
サイズ制約条件	SizeConstraintSet	arn:aws:waf:: *account*:*sizeconstraintset* /*ID*
IP 一致条件	IPSet	arn:aws:waf:: *account*:*ipset*/*ID*
クロスサイトスクリプティング一致条件	XssMatchSet	arn:aws:waf:: *account*:*xssmatchset* /*ID*

AWS WAF Classic リソースのサブセットへのアクセスを許可または拒否するには、ポリシーの `resource`要素にリソースの ARN を含めます。 AWS WAF Classic ARNs の形式は次のとおりです。

```
arn:aws:waf::account:resource/ID
```

[account] (アカウント)、*[resource]* (リソース)、および *[ID]* 変数を有効な値に置き換えます。有効な値は次のとおりです。

- *#####*: の ID AWS アカウント。値を指定する必要があります。
- *resource*: AWS WAF Classic リソースのタイプ。
- *ID*: AWS WAF Classic リソースの ID、または指定された に関連付けられている指定されたタイプのすべてのリソースを示すワイルドカード (*) AWS アカウント。

例えば、次の ARN はアカウント 111122223333 のすべてのウェブ ACL を指定します。

```
arn:aws:waf::111122223333:webacl/*
```

AWS WAF Classic のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Condition 要素は、定義された基準に基づいてステートメントが実行される時期を指定します。イコールや未満などの条件演算子を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「グローバル条件コンテキストキー」を参照してください。

AWS WAF Classic 条件キーのリストを確認するには、「サービス認可リファレンス」の「AWS WAF Regional」で定義される および リソースの条件キー AWS WAF」を参照してください。条件キーを使用できるアクションとリソースについては、「 で定義されるアクション AWS WAF」およびAWS WAF 「リージョンで定義されるアクション」を参照してください。

AWS WAF Classic アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS WAF Classic のアイデンティティベースのポリシーの例。

AWS WAF Classic ACLs

ACL のサポート: なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするためのアクセス許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

AWS WAF Classic での ABAC

ABAC (ポリシー内のタグ) のサポート: 一部

属性ベースのアクセスコントロール (ABAC) は、タグと呼ばれる属性に基づいてアクセス許可を定義する認可戦略です。IAM エンティティと AWS リソースにタグをアタッチし、プリンシパルのタグがリソースのタグと一致するときにオペレーションを許可するように ABAC ポリシーを設計できます。

タグに基づいてアクセスを管理するには、aws:ResourceTag/*key-name*、aws:RequestTag/*key-name*、または aws:TagKeys の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用する」を参照してください。

AWS WAF Classic での一時的な認証情報の使用

一時的な認証情報のサポート: あり

一時的な認証情報は、 AWS リソースへの短期的なアクセスを提供し、フェデレーションまたはスイッチロールの使用時に自動的に作成されます。 AWS では、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することをお勧めします。詳細については、「IAM ユーザーガイド」の「IAM の一時的な認証情報」および「AWS のサービス と IAM との連携」を参照してください。

AWS WAF Classic の転送アクセスセッション

転送アクセスセッション (FAS) のサポート: あり

転送アクセスセッション (FAS) は、 を呼び出すプリンシパルのアクセス許可と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする を使用します。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

AWS WAF Classic のサービスロール

サービスロールのサポート: あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、IAM ユーザーガイドの AWS のサービスに許可を委任するロールを作成するを参照してください。

> **Warning**
>
> サービスロールのアクセス許可を変更すると、 AWS WAF Classic の機能が破損する可能性があります。 AWS WAF Classic が指示する場合にのみ、サービスロールを編集します。

AWS WAF Classic のサービスにリンクされたロール

サービスリンクロールのサポート: あり

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。

AWS WAF Classic サービスにリンクされたロールの作成または管理の詳細については、「」を参照してくださいAWS WAF Classic のサービスにリンクされたロールの使用。

AWS WAF Classic のアイデンティティベースのポリシーの例

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

デフォルトでは、ユーザーとロールには AWS WAF Classic リソースを作成または変更するアクセス許可はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。

これらのサンプルの JSON ポリシードキュメントを使用して IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーを作成する (コンソール)」を参照してください。

各リソースタイプの ARN の形式など、 AWS WAF Classic で定義されるアクションとリソースタイプの詳細については、「サービス認可リファレンス」の「Actions, resources, and condition keys for AWS WAF and Actions, resources, and condition keys for AWS WAF Regional」を参照してください。 ARNs

トピック

- ポリシーに関するベストプラクティス
- AWS WAF Classic コンソールの使用
- 自分の権限の表示をユーザーに許可する

ポリシーに関するベストプラクティス

ID ベースのポリシーは、アカウント内の AWS WAF Classic リソースを作成、アクセス、または削除できるかどうかを決定します。これらのアクションでは、 AWS アカウントに費用が発生する場合があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、IAM ユーザーガイド の AWS マネージドポリシー または ジョブ機能のAWS マネージドポリシー を参照してください。
- 最小特権を適用する – IAM ポリシーでアクセス許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、IAM ユーザーガイド の IAM でのポリシーとアクセス許可 を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。たとえば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用されている場合に AWS のサービス、サービスアクションへのアクセス

を許可することもできます CloudFormation。詳細については、IAM ユーザーガイド の IAM JSON ポリシー要素:条件 を参照してください。

- IAM アクセスアナライザー を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM アクセスアナライザー は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイド の IAM Access Analyzer でポリシーを検証する を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイド の MFA を使用した安全な API アクセス を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイド の IAM でのセキュリティのベストプラクティス を参照してください。

AWS WAF Classic コンソールの使用

AWS WAF Classic コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 の AWS WAF Classic リソースの詳細を一覧表示および表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

AWS コンソールにアクセスして使用できるユーザーは、 AWS WAF Classic コンソールにもアクセスできます。追加のアクセス許可は必要ありません。

自分の権限の表示をユーザーに許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS WAF Classic のアイデンティティとアクセスのトラブルシューティング

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

以下の情報は、 AWS WAF Classic と IAM の使用時に発生する可能性がある一般的な問題の診断と修正に役立ちます。

トピック

- AWS WAF Classic でアクションを実行する権限がありません
- iam:PassRole を実行する権限がありません
- 自分の 以外のユーザーに AWS WAF Classic リソース AWS アカウント へのアクセスを許可したい

AWS WAF Classic でアクションを実行する権限がありません

アクションを実行する権限がないというエラーが表示された場合は、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要な waf:*GetWidget* アクセス許可を持っていない場合に発生するものです。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 waf:GetWidget on resource: my-example-widget
```

この場合、waf:*GetWidget* アクションを使用して *my-example-widget* リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

iam:PassRole を実行する権限がありません

`iam:PassRole` アクションを実行する権限がないというエラーが表示された場合は、 AWS WAF Classic にロールを渡すことができるようにポリシーを更新する必要があります。

一部の AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、既存のロールをそのサービスに渡すことができます。そのためには、サービスにロールを渡すアクセス許可が必要です。

以下の例のエラーは、 `marymajor` という IAM ユーザーがコンソールを使用して AWS WAF Classic でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与されたアクセス許可が必要です。Mary には、ロールをサービスに渡すアクセス許可がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに `iam:PassRole` アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン資格情報を提供した担当者が管理者です。

自分の 以外のユーザーに AWS WAF Classic リソース AWS アカウント へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- AWS WAF Classic がこれらの機能をサポートしているかどうかを確認するには、「」を参照してくださいAWS WAF Classic と IAM の連携方法。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、「IAM ユーザーガイド」の「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。

- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイドの外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いの詳細については、IAM ユーザーガイドのIAM ロールとリソースベースのポリシーとの相違点を参照してください。

AWS WAF Classic のサービスにリンクされたロールの使用

> **Warning**
>
> AWS WAF Classic は計画されたend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

AWS WAF Classic は AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスにリンクされたロールは、 AWS WAF Classic に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは AWS WAF Classic によって事前定義されており、サービスがユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、 AWS WAF Classic の設定が簡単になります。 AWS WAF Classic はサービスにリンクされたロールのアクセス許可を定義し、特に定義されている場合を除き、 AWS WAF Classic のみがそのロールを引き受けることができます。定義された許可には、信頼ポリシーと許可ポリシーが含まれます。この許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスにリンクされたロールを削除するには、まずその ロールの関連リソースを削除します。これにより、リソースへのアクセス許可が誤って削除されないため、 AWS WAF Classic リソースが保護されます。

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連携するAWS サービス」を参照して、サービスにリンクされたロール列がはいになっているサービスを見つけてください。サービスにリンクされた役割に関するドキュメントをサービスで表示するには[はい] リンクを選択してください。

AWS WAF Classic のサービスにリンクされたロールのアクセス許可

AWS WAF Classic は、以下のサービスにリンクされたロールを使用します。

- `AWSServiceRoleForWAFLogging`
- `AWSServiceRoleForWAFRegionalLogging`

AWS WAF Classic は、これらのサービスにリンクされたロールを使用して Amazon Data Firehose にログを書き込みます。これらのロールは、ログインを有効にした場合にのみ使用されます AWS WAF。詳細については、「ウェブ ACL トラフィック情報のログ記録」を参照してください。

`AWSServiceRoleForWAFLogging` および `AWSServiceRoleForWAFRegionalLogging` のサービスにリンクされたロールは、ロールを引き受ける上でそれぞれに対応する次のサービスを信頼します。

- `waf.amazonaws.com`

  `waf-regional.amazonaws.com`

ロールのアクセス許可ポリシーにより、 AWS WAF Classic は指定されたリソースに対して次のアクションを実行できます。

- アクション: 名前が「aws-waf-logs-」で始まる Amazon Data Firehose データストリームリソースで `firehose:PutRecord` および `firehose:PutRecordBatch`。例えば、`aws-waf-logs-us-east-2-analytics`。
- アクション: Amazon Data Firehose AWS Key Management Service がカスタマーマネージド AWS KMS キーを使用してデータを暗号化できるようにする `kms:GenerateDataKey`および `kms:Decrypt`。

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するにはアクセス許可を設定する必要があります。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの許可」を参照してください。

AWS WAF Classic のサービスにリンクされたロールの作成

サービスリンクロールを手動で作成する必要はありません。で AWS WAF Classic ログ記録を有効にするか AWS マネジメントコンソール、 AWS WAF Classic CLI または AWS WAF Classic API でPutLoggingConfigurationリクエストを行うと、 AWS WAF Classic によってサービスにリンクされたロールが作成されます。

ログ記録を有効化するためには、iam:CreateServiceLinkedRole 許可が必要です。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は同じ方法でアカウントにロールを再作成できます。 AWS WAF Classic ログ記録を有効にすると、 AWS WAF Classic はサービスにリンクされたロールを再度作成します。

AWS WAF Classic のサービスにリンクされたロールの編集

AWS WAF Classic では、 AWSServiceRoleForWAFLoggingおよびAWSServiceRoleForWAFRegionalLoggingサービスにリンクされたロールを編集することはできません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロール記述の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

AWS WAF Classic のサービスにリンクされたロールの削除

サービスリンクロールを必要とする機能やサービスが不要になった場合は、ロールを削除することをお勧めします。そうすることで、積極的にモニタリングまたは保守されていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

> **Note**
>
> リソースを削除しようとしたときに AWS WAF Classic サービスがロールを使用している場合、削除が失敗する可能性があります。失敗した場合は数分待ってから操作を再試行してください。

AWSServiceRoleForWAFLogging および で使用される AWS WAF Classic リソースを削除するには AWSServiceRoleForWAFRegionalLogging

1. AWS WAF Classic コンソールで、すべてのウェブ ACL からログ記録を削除します。詳細については、「ウェブ ACL トラフィック情報のログ記録」を参照してください。
2. API または CLI を使用して、ログ記録が有効化されている各ウェブ ACL に DeleteLoggingConfiguration リクエストを送信します。詳細については、「AWS WAF Classic API リファレンス」を参照してください。

IAM を使用して、サービスにリンクされたロールを手動で削除するには

AWSServiceRoleForWAFLogging および AWSServiceRoleForWAFRegionalLogging サービスにリンクされたロールを削除するには、IAM コンソール、IAM CLI、または IAM API を使用します。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの削除」を参照してください。

AWS WAF Classic サービスにリンクされたロールでサポートされているリージョン

AWS WAF Classic は、以下のサービスにリンクされたロールの使用をサポートしています AWS リージョン。

リージョン名	リージョンアイデンティティ	AWS WAF Classic でのサポート
米国東部 (バージニア北部)	us-east-1	あり
米国東部 (オハイオ)	us-east-2	あり
米国西部 (北カリフォルニア)	us-west-1	あり
米国西部 (オレゴン)	us-west-2	あり
アジアパシフィック (ムンバイ)	ap-south-1	あり
アジアパシフィック (大阪)	ap-northeast-3	あり
アジアパシフィック (ソウル)	ap-northeast-2	あり
アジアパシフィック (シンガポール)	ap-southeast-1	あり

リージョン名	リージョンアイデンティティ	AWS WAF Classic でのサポート
アジアパシフィック (シドニー)	ap-southeast-2	あり
アジアパシフィック (東京)	ap-northeast-1	あり
カナダ (中部)	ca-central-1	あり
欧州 (フランクフルト)	eu-central-1	あり
欧州 (アイルランド)	eu-west-1	あり
欧州 (ロンドン)	eu-west-2	あり
欧州 (パリ)	eu-west-3	あり
南米 (サンパウロ)	sa-east-1	あり

AWS WAF Classic でのログ記録とモニタリング

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

モニタリングは、 AWS WAF Classic と AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、 AWS ソリューションのすべての部分からモニタリングデータを収集する必要があります。 には、 AWS WAF Classic リソースをモニタリングし、潜在的なイベントに対応するための複数のツール AWS が用意されています。

Amazon CloudWatch アラーム

Amazon CloudWatch アラームを使用して、指定した期間にわたって 1 つのメトリクスを確認します。メトリクスが指定されたしきい値を超えると、CloudWatch は Amazon SNS トピックまたは AWS Auto Scaling ポリシーに通知を送信します。詳細については、「Amazon CloudWatch によるモニタリング」を参照してください。

AWS CloudTrail ログ

CloudTrail は、 AWS WAF Classic のユーザー、ロール、または AWS のサービスによって実行されたアクションの記録を提供します。CloudTrail で収集された情報を使用して、 AWS WAF Classic に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。詳細については、「での AWS CloudTrail API コールのログ記録」を参照してください。

AWS WAF Classic のコンプライアンス検証

> **Warning**
>
> AWS WAF Classic は計画されたend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

新しい AWS サインアップエクスペリエンスは、規制されたワークロード向けには設計されていません。新しい AWS サインアップエクスペリエンスを使用しているが、規制対象のワークロード AWS に を使用する場合は、 AWS (アドバンスド) にサインアップするか、 AWS 環境の高度な機能をアクティブ化できます。

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、AWS のサービス「コンプライアンスプログラムによる対象範囲内のコンプライアンス範囲内の」を参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「Downloading Reports in AWS Artifact」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。を使用する際のコンプライアンス責任の詳細については AWS のサービス、AWS 「 セキュリティドキュメント」を参照してください。

AWS WAF Classic の耐障害性

> **Warning**
>
> AWS WAF Classic は計画されたend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

AWS グローバルインフラストラクチャは、 AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。 は、低レイテンシー、高スループット、高度に冗長なネットワークで接続された、物理的に分離および分離された複数のアベイラビリティーゾーン AWS リージョン を提供します。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断せずに、自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、およびスケーラビリティが優れています。

AWS リージョン およびアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

AWS WAF Classic のインフラストラクチャセキュリティ

> **Warning**
>
> AWS WAF Classic は計画的なend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。
> の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

マネージドサービスである AWS WAF Classic は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して環境を AWS 設計するには、「Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

AWS 公開された API コールを使用して、ネットワーク経由で AWS WAF Classic にアクセスします。クライアントは以下をサポートする必要があります。

- Transport Layer Security (TLS)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

AWS WAF クラシッククォータ

> **Warning**
>
> AWS WAF Classic は計画されたend-of-lifeプロセスを進めています。リージョン固有のマイルストーンと日付については、 AWS Health ダッシュボードを参照してください。

> **Note**
>
> これは AWS WAF Classic ドキュメントです。このバージョンは、2019 年 11 月 AWS WAF より前にルールやウェブ ACLs などのリソースを作成し AWS WAF 、最新バージョンに移行していない場合にのみ使用してください。Web ACL を移行するには、AWS WAF Classic リソースの への移行 AWS WAF を参照してください。

の最新バージョンについては、 AWS WAF「」を参照してくださいAWS WAF。

AWS WAF Classic には、次のクォータが適用されます (以前は制限と呼ばれていました)。

AWS WAF Classic には、リージョンごとのアカウントあたりのエンティティ数に対するデフォルトのクォータがあります。このクォータの引き上げをリクエストすることができます。

リソース	1 リージョン、1 アカウントあたりのデフォルトのクォータ
ウェブ ACL	50
[Rules] (ルール)	100
レートベースのルール	5
アカウントあたり、リージョンあたりの条件	正規表現一致と Geo 一致を除くすべての条件で、100 個の各条件タイプ。100 のサイズ制約条件と 100 の IP 一致条件はその一例です。正規表現一致条件については、次の表を参照してください。
1 秒あたりのリクエスト	ウェブ ACL あたり 25,000*

*このクォータは、Application Load Balancer の AWS WAF Classic にのみ適用されます。CloudFront での AWS WAF Classic の 1 秒あたりのリクエスト (RPS) クォータは、CloudFront デベロッパーガイドで説明されている CloudFront による RPS クォータサポートと同じです。

AWS WAF Classic エンティティの次のクォータは変更できません。

[リソース]	1 アカウント、1 リージョンあたりのクォータ
ウェブ ACL あたりのルールグループ	2: お客様が作成した 1 つのルールグループと 1 つの AWS Marketplace ルールグループ
ウェブ ACL あたりのルールの数	10
ルールあたりの条件の数	10
IP 一致条件ごとの IP アドレス範囲 (CIDR 表記)	10,000 一度に更新できるアドレスは最大で 1,000 個です。API コール `UpdateIPSet` は、1 回のリクエストで最大 1,000 個のアドレスを受け入れます。
レートベースのルールごとにブロックされている IP アドレス	10,000
5 分間あたりの最小レートベースのルール制限	100
クロスサイトスクリプティング一致条件あたりのフィルターの数	10

[リソース]	1 アカウント、1 リージョンあたりのクォータ
サイズ制約条件あたりのフィルターの数	10
SQL インジェクション一致条件あたりのフィルターの数	10
文字列一致条件あたりのフィルターの数	10
文字列一致条件では、指定した値についてウェブリクエストのヘッダーを検査するように AWS WAF Classic を設定した場合の、HTTP ヘッダー名の文字数	40
文字列一致条件では、 AWS WAF Classic が検索する値の文字数	50
正規表現一致条件	10
正規表現一致条件では、 AWS WAF Classic が検索するパターンの文字数	70
正規表現一致条件で、1 パターンセットあたりのパターンの数	10
正規表現一致条件で、1 正規表現条件あたりのパターンセットの数	1
パターンセット	5
Geo 一致条件	50
Geo 一致条件ごとの場所	50

AWS WAF Classic には、リージョンごとのアカウントごとの呼び出しに対して次の固定クォータがあります。これらのクォータは、コンソール、CLI、REST API、SDKs など AWS CloudFormation、利用可能なあらゆる手段によるサービスへの合計呼び出しに適用されます。これらのクォータは変更できません。

コールタイプ	1 アカウント、1 リージョンあたりのクォータ
AssociateWebACL へのコールの最大数	2 秒あたり 1 個のリクエスト
DisassociateWebACL へのコールの最大数	2 秒あたり 1 個のリクエスト
GetWebACLForResource へのコールの最大数	1 秒あたり 1 個のリクエスト
ListResourcesForWebACL へのコールの最大数	1 秒あたり 1 個のリクエスト
CreateWebACLMigrationStack へのコールの最大数	1 秒あたり 1 個のリクエスト
GetChangeToken へのコールの最大数	1 秒あたり 10 個のリクエスト
GetChangeTokenStatus へのコールの最大数	1 秒あたり 1 個のリクエスト
個々の List アクションへのコールの最大数 (他にクォータが定義されていない場合)	1 秒あたり 5 個のリクエスト
個々の Create、Put、Get、または Update アクションへのコールの最大数 (他にクォータが定義されていない場合)	1 秒あたり 1 個のリクエスト

AWS Shield

Distributed Denial of Service (DDoS) 攻撃から保護することは、インターネットに直接接続するアプリケーションにとって極めて重要です。でアプリケーションを構築する場合 AWS、 AWS が提供する保護を追加料金なしで使用できます。さらに、 AWS Shield Advanced マネージド脅威保護サービスを使用して、DDoS 検出、緩和、対応機能を追加してセキュリティ体制を改善できます。

AWS は、インターネット上の不正行為者に対する防御において高可用性、セキュリティ、回復性を確保するためのツール、ベストプラクティス、およびサービスを提供することに全力を注いでいます。このガイドは、IT 関連事項の意思決定者やセキュリティエンジニアが、Shield と Shield Advanced を使用して DDoS 攻撃や他の外部の脅威からアプリケーションをより適切に保護する方法を理解できるように提供されています。

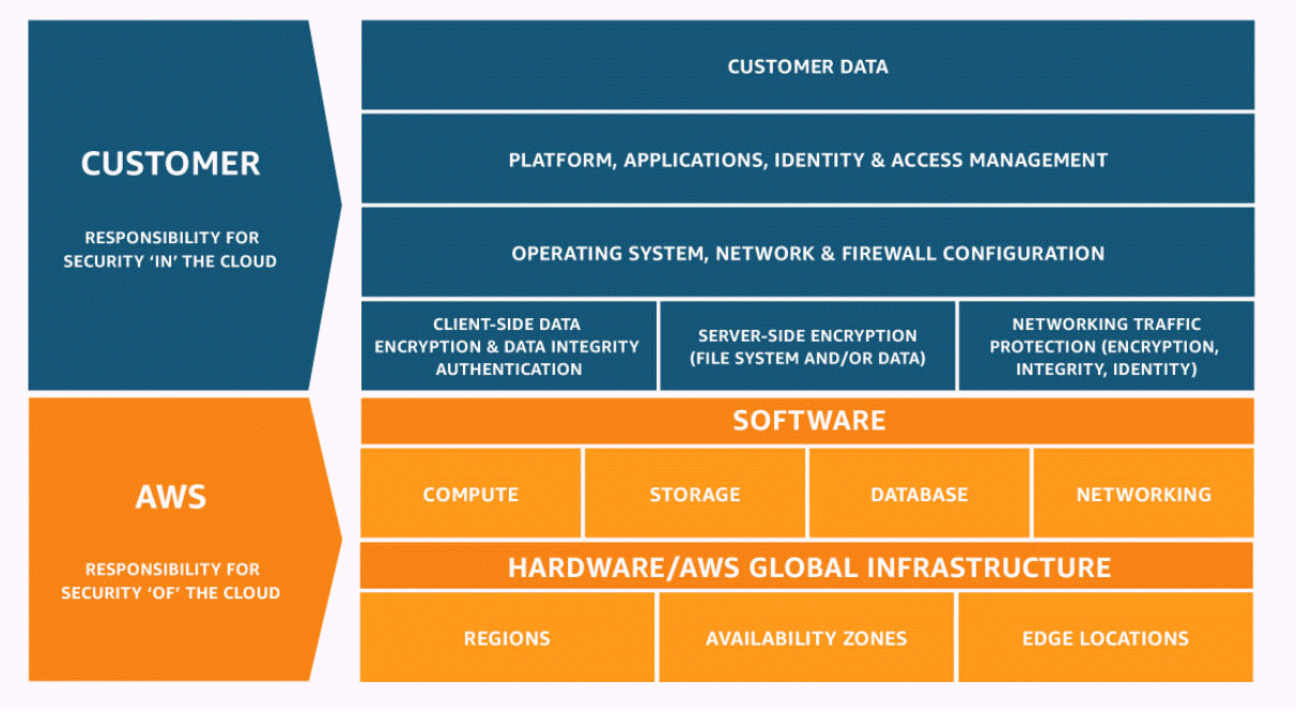
でアプリケーションを構築すると AWS、UDP リフレクション攻撃や TCP SYN フラッドなどの一般的なボリューメトリック DDoS 攻撃ベクトル AWS に対して、 によって自動的に保護されます。これらの保護を活用して、DDoS 回復性のためにアーキテクチャを設計および設定 AWS することで、で実行するアプリケーションの可用性を確保できます。

このガイドでは、DDoS レジリエンシーを実現するためのアプリケーションアーキテクチャの設計、作成、および設定に役立つ推奨事項について説明します。このガイドで提供されるベストプラクティスに準拠するアプリケーションは、大規模な DDoS 攻撃や広範囲の DDoS 攻撃ベクトルによってターゲットとされた場合に、改善された可用性の維持の恩恵を受けることができます。さらに、このガイドでは、Shield Advanced を使用して、重要なアプリケーション向けに最適化された DDoS 保護体制を実装する方法について説明します。これには、特定のレベルの可用性を顧客に保証しているアプリケーションや、DDoS イベント AWS 中に からの運用サポートを必要とするアプリケーションが含まれます。

セキュリティは、 AWS とお客様の間の責任共有です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ – AWS は、 で AWS サービスを実行するインフラストラクチャを保護する責任を担います AWS クラウド。 は、お客様が安全に使用できるサービス AWS も提供します。セキュリティの有効性は、AWS コンプライアンスプログラムの一環として、サードパーティーの審査機関によって定期的にテストおよび検証されています。AWSServiceRoleForAWSShield に適用されるコンプライアンスプログラムについては、「コンプライアンスプログラムによる対象範囲内のAWS のサービス」を参照してください。

- クラウド内のセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、お客様のデータの機密性、組織の要件、および適用可能な法律および規制などの他の要因についても責任を担います。



AWS Shield と Shield Advanced の仕組み

このページでは、 AWS Shield Standard と の違いについて説明します AWS Shield Advanced。また、Shield が検出する攻撃のクラスについても説明します。

AWS Shield Standard と は、ネットワークレイヤーとトランスポートレイヤー (レイヤー 3 と 4) およびアプリケーションレイヤー (レイヤー 7) のリソースに対する AWS 分散型サービス拒否 (DDoS) 攻撃に対する保護 AWS Shield Advanced を提供します。DDoS 攻撃は、侵害された複数のシステムが、ターゲットに対してトラフィックでフラッディングを試みる攻撃です。DDoS 攻撃は正当なエンドユーザーがターゲットのサービスにアクセスするのを妨げ、圧倒的なトラフィック量のためにターゲットがクラッシュする可能性があります。

AWS Shield は、幅広い既知の DDoS 攻撃ベクトルとゼロデイ攻撃ベクトルに対する保護を提供します。Shield の検出および緩和は、検出時において、サービスにとって明示的に既知でなくても、脅威に対するカバレッジを提供するように設計されています。

Shield Standard は、 AWSの使用時に自動的に提供され、追加料金はかかりません。攻撃に対するより高いレベルの保護のために、 AWS Shield Advancedサブスクライブすることができます。

Shield が検出する攻撃のクラスには、次のものが含まれます。

- [Network volumetric attacks (layer 3)] (ネットワークボリューム攻撃 (レイヤー 3)) – これは、インフラストラクチャレイヤー攻撃のベクトルのサブカテゴリです。これらのベクトルは、正当なユーザーへのサービスを拒否するために、ターゲットネットワークまたはリソースの容量を飽和させることを試みます。
- [Network protocol attacks (layer 4)] (ネットワークプロトコル攻撃 (レイヤー 4)) – これは、インフラストラクチャレイヤー攻撃のベクトルのサブカテゴリです。これらのベクトルは、プロトコルを悪用してターゲットリソースへのサービスを拒否します。ネットワークプロトコル攻撃の一般的な例は TCP SYN フラッドです。TCP SYN フラッドは、サーバー、ロードバランサー、ファイアウォールなどのリソースの接続状態を使い果たす可能性があります。ネットワークプロトコル攻撃は、帯域幅消費型である場合もあります。例えば、大規模な TCP SYN フラッドには、ターゲットリソースまたは中間リソースの状態を使い果たしながら、ネットワークの容量を飽和させる意図があるかもしれません。
- アプリケーションレイヤー攻撃 (レイヤー 7) - このカテゴリの攻撃ベクトルは、ウェブリクエストのフラッドなど、ターゲットに対して有効なクエリをアプリケーションにフラッディングすることによって、正当なユーザーへのサービス提供の拒否を試みます。

目次

- AWS Shield Standard の概要
- AWS Shield Advanced の概要
- が AWS Shield Advanced 保護する AWS リソースのリスト
- AWS Shield Advanced 機能とオプション
- 追加の保護をサブスクライブ AWS Shield Advanced して適用するかどうかを決定する
- DDoS 攻撃の例
- がイベント AWS Shield を検出する方法
  - AWS Shield インフラストラクチャレイヤーの脅威の検出ロジック (レイヤー 3 とレイヤー 4)
  - アプリケーションレイヤーの脅威に対する Shield Advanced 検出ロジック (レイヤー 7)
  - アプリケーション内の複数のリソースの Shield Advanced 検出ロジック
- がイベント AWS Shield を軽減する方法
  - AWS Shield DDoS 緩和機能のリスト

- AWS Shield CloudFront と Route 53 の緩和ロジック
- AWS Shield AWS リージョンの緩和ロジック
- AWS Shield AWS Global Accelerator 標準アクセラレーターの緩和ロジック
- AWS Shield Advanced Elastic IPs の緩和ロジック
- AWS Shield Advanced ウェブアプリケーションの緩和ロジック

AWS Shield Standard の概要

AWS Shield は、アプリケーションの境界を保護するマネージド脅威保護サービスです。境界は、AWS ネットワーク外からのアプリケーショントラフィックの最初のエントリポイントです。

アプリケーションの境界がどこにあるかを判断するには、ユーザーがインターネットからアプリケーションにどのようにアクセスするかを検討します。最初のエントリポイントが AWS リージョンにある場合、アプリケーション境界は Amazon Virtual Private Cloud (VPC) です。ユーザーが Amazon Route 53 によってアプリケーションに誘導され、最初に Amazon CloudFront または を使用してアプリケーションにアクセスする場合 AWS Global Accelerator、アプリケーション境界は AWS ネットワークのエッジから始まります。

Shield は、 で実行されているすべてのアプリケーションに DDoS 検出と緩和の利点を提供しますが AWS、アプリケーションアーキテクチャを設計するときに行う決定は、DDoS の耐障害性のレベルに影響します。DDoS Resiliency は、攻撃を受けている最中に、想定されるパラメータ内でアプリケーションが動作し続ける能力です。

すべての AWS お客様は、Shield Standard の自動保護を追加料金なしで利用できます。Shield Standard は、お客様のウェブサイトやアプリケーションを標的として一般的かつ頻繁に発生するネットワークおよび転送レイヤーの DDoS 攻撃に対して防御します。Shield Standard はすべての AWS お客様を保護するのに役立ちますが、Amazon Route 53 ホストゾーン、Amazon CloudFront ディストリビューション、および AWS Global Accelerator 標準アクセラレーターには特に利点があります。これらのリソースは、既知のすべてのネットワークおよびトランスポートレイヤー攻撃に対して、可用性についての包括的な保護を受けます。

AWS Shield Advanced の概要

AWS Shield Advanced は、DDoS 攻撃、ボリューメトリックボット、脆弱性悪用の試みなどの外部脅威からアプリケーションを保護するのに役立つマネージドサービスです。攻撃に対するより高いレベルの保護のために、 AWS Shield Advancedサブスクライブすることができます。

Shield Advanced をサブスクライブしてリソースに保護を追加すると、Shield Advanced は、それらのリソースのために拡張された DDoS 攻撃保護を提供します。Shield Advanced から受ける保護は、アーキテクチャと設定の選択内容によって異なります。このガイドの情報を参照して、Shield Advanced を使用して回復力のあるアプリケーションを構築して保護し、エキスパートのサポートが必要なときにエスカレーションできます。

Shield Advanced サブスクリプションと AWS WAF コスト

Shield Advanced サブスクリプションは、Shield Advanced で保護するリソースに標準 AWS WAF 機能を使用するコストをカバーします。Shield Advanced 保護の対象となる標準 AWS WAF 料金は、保護パック (ウェブ ACL) あたりのコスト、ルールあたりのコスト、ウェブリクエスト検査の 100 万リクエストあたりの基本料金、最大 1,500 WCUs、およびデフォルトの本文サイズです。

Shield Advanced 自動アプリケーションレイヤー DDoS 緩和を有効にすると、150 個の保護パック (ウェブ ACL) キャパシティユニット (WCU) はルールグループに追加されます。これらの WCU は、保護パック (ウェブ ACL) 内の WCU の使用量に対してカウントされます。詳細については[Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和]、[Shield Advanced ルールグループによるアプリケーションレイヤーの保護]、および[のウェブ ACL キャパシティユニット (WCUs) AWS WAF]を参照してください。

Shield Advanced のサブスクリプションでは、Shield Advanced を使用して保護しないリソース AWS WAF の の使用はカバーされません。また、保護されたリソースの標準以外の追加 AWS WAF コストもカバーしません。標準以外の AWS WAF コストの例としては、Bot Control、CAPTCHA ルールアクション、1,500 WCUs を超えるウェブ ACLs、およびデフォルトの本文サイズを超えるリクエスト本文の検査などがあります。完全なリストは AWS WAF 料金ページに記載されています。Shield Advanced へのサブスクリプションには、 Layer 7 Anti-DDoS Amazon Managed Rule グループへのアクセスが含まれます。サブスクリプションの一環として、Shield Advanced で保護された AWS WAF リソースに対するリクエストは 1 か月あたり最大 500 億件になります。500 億を超えるリクエストは、 AWS Shield Advanced 料金ページに従って請求されます。

詳細情報および料金の例については、「[Shield の料金]」および「[AWS WAF の料金]」を参照してください。

Shield Advanced サブスクリプションの請求

AWS チャネルリセラーの場合は、アカウントチームに情報とガイダンスを求めてください。この請求情報は、 AWS チャネルリセラーではないお客様を対象としています。

他のすべてについては、次のサブスクリプションと請求のガイドラインが適用されます。

- AWS Organizations 組織のメンバーであるアカウントの場合、 は、支払者アカウント自体がサブスクライブされているかどうかにかかわらず、組織の支払者アカウントに対して Shield Advanced サブスクリプションを AWS 請求します。
- 同じ AWS Organizations 一括請求 (コンソリデーティッドビリング) アカウントファミリー に属する複数のアカウントをサブスクライブする場合、1 つのサブスクリプション料金はファミリー内のすべてのサブスクライブアカウントに対するものです。組織は、すべての AWS アカウント とそのすべてのリソースを所有している必要があります。
- 複数の組織のために複数のアカウントをサブスクライブする場合でも、すべてを所有しているのであれば、すべての組織、アカウント、リソースのサブスクリプション料金の支払いを引き続き 1 回で行うことができます。アカウントマネージャーまたは AWS サポートに連絡して、組織の 1 つを除くすべての AWS Shield Advanced サブスクリプション料金の免除をリクエストしてください。

詳細な料金情報と例については、「AWS Shield の料金表」を参照してください。

が AWS Shield Advanced 保護する AWS リソースのリスト

> **Note**
>
> Shield Advanced 保護は、Shield Advanced で明示的に指定したリソース、または Shield AWS Firewall Manager Advanced ポリシーで保護するリソースに対してのみ有効になります。Shield Advanced は、リソースを自動的に保護しません。

Shield Advanced を使用すると、次のリソースタイプで高度なモニタリングと保護を行うことができます。

- Amazon CloudFront ディストリビューション。CloudFront の継続的デプロイでは、Shield Advanced は保護対象のプライマリディストリビューションに関連付けられているすべてのステージングディストリビューションを保護します。
- Amazon Route 53 ホストゾーン。
- AWS Global Accelerator 標準アクセラレーター。
- Amazon EC2 Elastic IP アドレス。Shield Advanced は、保護された Elastic IP アドレスに関連付けられているリソースを保護します。
- Amazon EC2 インスタンス (Amazon EC2 Elastic IP アドレスへの関連付け経由)
- 次の Elastic Load Balancing (ELB) ロードバランサー:

- Application Load Balancer。
- Classic Load Balancer。
- Network Load Balancer (Amazon EC2 Elastic IP アドレスへの関連付け経由)。

これらのリソースタイプの保護に関する追加情報については、「が AWS Shield Advanced 保護するリソースのリスト」を参照してください。

AWS Shield Advanced 機能とオプション

AWS Shield Advanced サブスクリプションには、次の機能とオプションが含まれています。これらは、既に提供されている DDoS 検出および緩和機能を補完します AWS。

- AWS WAF 統合 – Shield Advanced は、アプリケーションレイヤー保護の一部として AWS WAF ウェブ ACLs、ルール、およびルールグループを使用します。詳細については AWS WAF、「」を参照してくださいの AWS WAF 仕組み。

> **Note**
>
> Shield Advanced サブスクリプションは、Shield Advanced で保護するリソースに標準 AWS WAF 機能を使用するコストをカバーします。Shield Advanced 保護の対象となる標準 AWS WAF 料金は、保護パック (ウェブ ACL) あたりのコスト、ルールあたりのコスト、ウェブリクエスト検査の 100 万リクエストあたりの基本料金、最大 1,500 WCUs、およびデフォルトの本文サイズです。
> Shield Advanced 自動アプリケーションレイヤー DDoS 緩和を有効にすると、150 個の保護パック (ウェブ ACL) キャパシティユニット (WCU) はルールグループに追加されます。これらの WCU は、保護パック (ウェブ ACL) 内の WCU の使用量に対してカウントされます。詳細については Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和、Shield Advanced ルールグループによるアプリケーションレイヤーの保護、およびのウェブ ACL キャパシティユニット (WCUs) AWS WAF を参照してください。
> Shield Advanced のサブスクリプションは、Shield Advanced を使用して保護しないリソース AWS WAF の の使用を対象としていません。また、保護されたリソースの標準以外の追加 AWS WAF コストもカバーしません。標準以外の AWS WAF コストの例としては、Bot Control、CAPTCHAルールアクション、1,500 WCUs を超えるウェブ ACLs、およびデフォルトの本文サイズを超えるリクエスト本文の検査などがあります。完全なリストは AWS WAF 料金ページに記載されています。Shield Advanced へのサブスクリプションには、 Layer 7 Anti-DDoS Amazon Managed Rule グループへのアクセスが含まれます。サブスクリプションの一環として、Shield Advanced で保護された AWS WAF リソースに

対するリクエストは 1 か月あたり最大 500 億件になります。500 億を超えるリクエストは、 AWS Shield Advanced 料金ページに従って請求されます。
詳細情報および料金の例については、「Shield の料金」および「AWS WAF の料金」を参照してください。

- アプリケーションレイヤーの DDoS の自動緩和 - Shield Advanced は、保護されたリソースに対するアプリケーションレイヤー (レイヤー 7) 攻撃を自動的に緩和して対応するように設定できます。自動緩和により、Shield Advanced は既知の DDoS ソースからのリクエストに AWS WAF レート制限を適用し、検出された DDoS 攻撃に応じてカスタム AWS WAF 保護を自動的に追加および管理します。攻撃の一部であるウェブリクエストをカウントまたはブロックするように自動緩和を設定できます。

  詳細については、「Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和」を参照してください。

- ヘルスベースの検出 – Shield Advanced で Amazon Route 53 ヘルスチェックを使用して、イベントの検出と緩和の通知を受けることができます。ヘルスチェックは、仕様に従ってアプリケーションをモニタリングし、仕様が満たされた場合は正常、そうでない場合は異常を報告します。Shield Advanced でヘルスチェックを使用すると、誤検出を防止するのに役立つともに、保護されたリソースが異常な場合により迅速に検出および緩和できます。Route 53 ホストゾーンを除くリソースタイプのために、ヘルスベースの検出を使用できます。Shield Advanced のプロアクティブエンゲージメントは、ヘルスベースの検出が有効になっているリソースでのみ使用できます。

  詳細については、「Shield Advanced と Route 53 を使用したヘルスチェックを使用したヘルスベースの検出」を参照してください。

- 保護グループ – 保護グループを使用して、保護されたリソースの論理グループを作成し、グループ全体の検出と緩和を強化できます。新しく保護されたリソースを自動的に含めるように、保護グループのメンバーシップの条件を定義できます。保護されたリソースは、複数の保護グループに所属できます。

  詳細については、「AWS Shield Advanced 保護のグループ化」を参照してください。

- DDoS イベントと攻撃の可視性の向上 – Shield Advanced を使用すると、高度なリアルタイムのメトリクスとレポートにアクセスして、保護された AWS のリソースに対するイベントと攻撃の可視性を高めることができます。この情報には、Shield Advanced API とコンソール、および Amazon CloudWatch メトリクスを通じてアクセスできます。

  詳細については、「Shield Advanced による DDoS イベントの可視性」を参照してください。

- AWS Firewall Managerによる Shield Advanced 保護の一元管理 – Firewall Manager を使用して、新しいアカウントとリソースに Shield Advanced 保護を自動的に適用し、ウェブ ACL に AWS WAF ルールをデプロイできます。Firewall Manager Shield Advanced 保護ポリシーは、Shield Advanced のお客様に追加料金なしでご利用いただけます。また、Amazon Simple Notification Service (SNS) トピックまたは AWS Security Hub CSPMで Firewall Manager を使用して、アカウントの Shield Advanced モニタリングアクティビティを一元化することもできます。

  Firewall Manager を使用して Shield Advanced 保護機能を管理する方法については、「AWS Firewall Manager」および「Firewall Manager での AWS Shield Advanced ポリシーの使用」を参照してください。Firewall Manager の料金については、「AWS Firewall Manager の料金」を参照してください。

- AWS Shield Response Team (SRT) – SRT は AWS、、Amazon.com、およびその子会社の保護において豊富な経験を持っています。 AWS Shield Advanced のお客様は、アプリケーションの可用性に影響を与える DDoS 攻撃を受けている最中に、いつでも SRT に連絡してサポートを求めることができます。SRT と連携して、リソースのカスタム緩和策を作成および管理することもできます。SRT のサービスを使用するには、ビジネスサポートプランまたはエンタープライズサポートプランをサブスクライブする必要もあります。

  詳細については、「Shield Response Team (SRT) サポートによるマネージド DDoS イベントレスポンス」を参照してください。

- プロアクティブな関与 – Shield Advanced が検出したイベントの発生中に、保護されたリソースに関連付けられた Amazon Route 53 ヘルスチェックが異常になった場合、プロアクティブな関与によって、Shield Response Team (SRT) はお客様に直接ご連絡します。これにより、アプリケーションの可用性に影響を及ぼす可能性のある攻撃が疑われる場合に、エキスパートとより迅速に連携することができます。

  詳細については、「SRT が直接連絡するためのプロアクティブエンゲージメントの設定」を参照してください。

- コスト保護の機会 – Shield Advanced は、保護されたリソースに対する DDoS 攻撃に起因する可能性のある AWS 請求の急増に対するコスト保護を提供します。これには、Shield Advanced データ転送アウト (DTO) 使用料の急増に対する補償が含まれる場合があります。Shield Advanced は、Shield Advanced サービスクレジットという形であらゆるコスト保護を提供します。

  詳細については、「攻撃 AWS Shield Advanced 後の でのクレジットのリクエスト」を参照してください。

追加の保護をサブスクライブ AWS Shield Advanced して適用するかどうかを決定する

AWS Shield Advanced をサブスクライブするアカウントと追加の保護を適用する場合を判断するのに役立てるため、このセクションのシナリオを確認してください。Shield Advanced では、一括請求 (コンソリデーティッドビリング) の支払いアカウントで作成されたすべてのアカウントについて、1 つの月額サブスクリプション料金をお支払いいただきます。さらに、転送されたデータの GB (OUT) に基づく使用料金もお支払いいただきます。Shield Advanced の料金については、「AWS Shield Advanced の料金」を参照してください。

Shield Advanced でアプリケーションとそのリソースを保護するには、アプリケーションを管理するアカウントを Shield Advanced にサブスクライブし、アプリケーションのリソースに保護を追加します。アカウントのサブスクライブとリソースの保護については、「セットアップ AWS Shield Advanced」を参照してください。

Shield Advanced サブスクリプションと AWS WAF コスト

Shield Advanced サブスクリプションは、Shield Advanced で保護するリソースに標準 AWS WAF 機能を使用するコストをカバーします。Shield Advanced 保護の対象となる標準 AWS WAF 料金は、保護パック (ウェブ ACL) あたりのコスト、ルールあたりのコスト、ウェブリクエスト検査の 100 万リクエストあたりの基本料金、最大 1,500 WCUs、およびデフォルトの本文サイズです。

Shield Advanced 自動アプリケーションレイヤー DDoS 緩和を有効にすると、150 個の保護パック (ウェブ ACL) キャパシティユニット (WCU) はルールグループに追加されます。これらの WCU は、保護パック (ウェブ ACL) 内の WCU の使用量に対してカウントされます。詳細については Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和、Shield Advanced ルールグループによるアプリケーションレイヤーの保護、および のウェブ ACL キャパシティユニット (WCUs) AWS WAF を参照してください。

Shield Advanced のサブスクリプションでは、Shield Advanced を使用して保護しないリソース AWS WAF の の使用はカバーされません。また、保護されたリソースの標準以外の追加 AWS WAF コストもカバーしません。標準以外の AWS WAF コストの例としては、Bot Control、CAPTCHA ルールアクション、1,500 WCUs を超えるウェブ ACLs、およびデフォルトの本文サイズを超えるリクエスト本文の検査などがあります。完全なリストは AWS WAF 料金ページに記載されています。Shield Advanced へのサブスクリプションには、 Layer 7 Anti-DDoS Amazon Managed Rule グループへのアクセスが含まれます。サブスクリプションの一環として、Shield Advanced で保護された AWS WAF リソースに対するリクエストは 1 か月あたり最大 500 億件になります。500 億を超えるリクエストは、 AWS Shield Advanced 料金表ページに従って請求されます。

詳細情報および料金の例については、「Shield の料金」および「AWS WAF の料金」を参照してください。

Shield Advanced サブスクリプションの請求

AWS チャネルリセラーの場合は、アカウントチームに情報とガイダンスを求めてください。この請求情報は、 AWS チャネルリセラーではないお客様を対象としています。

他のすべてについては、次のサブスクリプションと請求のガイドラインが適用されます。

- AWS Organizations 組織のメンバーであるアカウントの場合、 は、支払者アカウント自体がサブスクライブされているかどうかにかかわらず、組織の支払者アカウントに対して Shield Advanced サブスクリプションを AWS 請求します。
- 同じ AWS Organizations 一括請求 (コンソリデーティッドビリング) アカウントファミリー に属する複数のアカウントをサブスクライブする場合、1 つのサブスクリプション料金はファミリー内のすべてのサブスクライブアカウントに対するものです。組織は、すべての AWS アカウント とそのすべてのリソースを所有している必要があります。
- 複数の組織のために複数のアカウントをサブスクライブする場合でも、すべてを所有しているのであれば、すべての組織、アカウント、リソースのサブスクリプション料金の支払いを引き続き 1 回で行うことができます。アカウントマネージャーまたは AWS サポートに連絡して、組織の 1 つを除くすべての AWS Shield Advanced サブスクリプション料金の免除をリクエストしてください。

詳細な料金情報と例については、「AWS Shield の料金表」を参照してください。

保護するアプリケーションの特定

次のいずれかが必要なアプリケーションには、Shield Advanced 保護を実装することを検討してください。

- アプリケーションのユーザーに保証された可用性。
- DDoS 攻撃によってアプリケーションが影響を受ける場合における、DDoS 緩和のエキスパートへの迅速なアクセス。
- アプリケーション AWS が DDoS 攻撃の影響を受ける可能性があることを認識し、セキュリティチームまたは運用チームからの攻撃 AWS の通知とエスカレーション。
- クラウドコストの予測可能性 (DDoS 攻撃が AWS のサービスの利用に影響を与える場合を含む)。

アプリケーションまたはそのリソースが上記のいずれかを必要とする場合は、関連アカウントのサブスクリプションを作成することを検討してください。

保護するリソースの特定

サブスクライブした各アカウントについて、次のいずれかの特性を持つ各リソースに Shield Advanced 保護を追加することを検討してください。

- このリソースは、インターネット上の外部ユーザーにサービスを提供します。
- リソースはインターネットに公開されます。また、重要なアプリケーションの一部でもあります。インターネット上のユーザーがアクセスするかどうかにかかわらず、公開されているすべてのリソースを検討してください。
- リソースは AWS WAF ウェブ ACL によって保護されます。

リソースの保護の作成と管理の詳細については、「でのリソース保護 AWS Shield Advanced」を参照してください。

さらに、このガイドの推奨事項は、DDoS レジリエンシーを考慮してアプリケーションを設計し、最適な保護を実現するために Shield Advanced の機能を適切に設定するのに役立ちます。

DDoS 攻撃の例

AWS Shield Advanced は、さまざまなタイプの攻撃に対する保護を拡張します。

次のリストでは、いくつかの一般的な攻撃の種類について説明します。

User Datagram Protocol (UDP) リフレクション攻撃

UDP リフレクション攻撃では、攻撃者はリクエストの発生元を偽装し、UDP を使用してサーバーから大量のレスポンスを引き出すことができます。攻撃対象の偽装 IP アドレスに向かう追加のネットワークトラフィックにより、対象のサーバーは遅くなり、正当なエンドユーザーが必要なリソースにアクセスできなくなります。

TCP SYN フラッド

TCP SYN フラッド攻撃の目的は、接続を半開状態にして、システムの利用可能なリソースを枯渇させることです。ユーザーがウェブサーバーのような TCP サービスに接続すると、クライアントは TCP SYN パケットを送信します。サーバーが肯定応答を返し、クライアントがそれ自体

の肯定応答を返すことで、3 ウェイハンドシェイクが完了します。TCP SYN フラッドでは、3 回目の肯定応答が返されることはなく、サーバーはレスポンスを待ったままになります。このため、他のユーザーはサーバーに接続できなくなります。

DNS クエリフラッド

DNS クエリフラッドでは、攻撃者は複数の DNS クエリを使用して DNS サーバーのリソースを使い果たします。 AWS Shield Advanced は、Route 53 DNS サーバーの DNS クエリフラッド攻撃に対する保護を提供します。

HTTP フラッド/キャッシュ無効化 (レイヤー 7) 攻撃

GET および POST フラッドを含む HTTP フラッドにより、攻撃者はウェブアプリケーションの実際のユーザーからのように見せかけて多数の HTTP リクエストを送信します。キャッシュ無効化攻撃は、HTTP フラッドの一種です。HTTP リクエストのクエリ文字列のバリエーションを使用して、エッジでキャッシュされているコンテンツが使用されないようにし、オリジンウェブサーバーからコンテンツが送信されるようにすることで、オリジンウェブサーバーに損害につながる可能性があるほどの負荷をかけます。

がイベント AWS Shield を検出する方法

AWS は AWS 、ネットワークおよび個々の AWS サービスのサービスレベル検出システムを運用し、DDoS 攻撃中にそれらが引き続き利用可能であることを確認します。さらに、リソースレベルの検出システムは、個々の AWS リソースをモニタリングして、リソースへのトラフィックが予想されるパラメータ内に留まるようにします。この組み合わせは、既知の不正なパケットを削除し、悪意のある可能性のあるトラフィックを強調し、エンドユーザーからのトラフィックに優先順位を付ける緩和策を適用することで、ターゲット AWS リソースと AWS サービスの両方を保護します。

イベントは、Shield Advanced のイベントの概要、攻撃の詳細、Amazon CloudWatch メトリクスに、DDoS 攻撃ベクトルの名前として、または評価がシグネチャではなくトラフィック量に基づいている場合は `Volumetric` として表示されます。`DDoSDetected` CloudWatch メトリクス内で利用可能な攻撃ベクトルのディメンションの詳細については、AWS Shield Advanced メトリクス を参照してください。

トピック

- AWS Shield インフラストラクチャレイヤーの脅威の検出ロジック (レイヤー 3 とレイヤー 4)
- アプリケーションレイヤーの脅威に対する Shield Advanced 検出ロジック (レイヤー 7)
- アプリケーション内の複数のリソースの Shield Advanced 検出ロジック

AWS Shield インフラストラクチャレイヤーの脅威の検出ロジック (レイヤー 3 とレイヤー 4)

このページでは、インフラストラクチャ (ネットワークと移転) レイヤーでイベント検出がどのように機能するかについて説明します。

インフラストラクチャレイヤー (レイヤー 3 とレイヤー 4) の DDoS 攻撃からターゲット AWS リソースを保護するために使用される検出ロジックは、リソースタイプとリソースが保護されているかどうかによって異なります AWS Shield Advanced。

Amazon CloudFront と Amazon Route 53 の検出

CloudFront および Route 53 でウェブアプリケーションを提供すると、アプリケーションへのすべてのパケットが完全インライン DDoS 緩和システムによって検査されます。これにより、観測可能なレイテンシーが発生することはありません。CloudFront ディストリビューションおよび Route 53 ホストゾーンに対する DDoS 攻撃は、リアルタイムで緩和されます。これらの保護は、 AWS Shield Advancedを使用するかどうかにかかわらず適用されます。

DDoS イベントの迅速な検出と緩和のために、可能な場合は常に、ウェブアプリケーションのエントリポイントとしての CloudFront と Route 53 の利用に関するベストプラクティスに従います。

AWS Global Accelerator および リージョンのサービスの検出

リソースレベルの検出は、Classic Load Balancer、Application Load Balancer、Elastic IP アドレス (EIPs) などの AWS リージョンで起動される AWS Global Accelerator 標準アクセラレーターとリソースを保護します。これらのリソースタイプは、緩和が必要な DDoS 攻撃の存在を示している可能性のあるトラフィックの増加をモニタリングします。毎分、各 AWS リソースへのトラフィックが評価されます。リソースへのトラフィックが上昇した場合は、リソースの容量を測定するために追加のチェックが実行されます。

Shield は次の標準チェックを実行します。

- Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、Amazon EC2 インスタンスにアタッチされた EIP – Shield は保護されたリソースから容量を取得します。容量は、ターゲットのインスタンスタイプ、インスタンスサイズ、およびインスタンスが拡張ネットワークを使用しているかどうかなどの他の要因によって異なります。
- Classic Load Balancer と Application Load Balancer – Shield はターゲットのロードバランサーノードから容量を取得します。
- Network Load Balancer にアタッチされた EIP – Shield はターゲットのロードバランサーから容量を取得します。容量は、ターゲットのロードバランサーのグループ設定とは無関係です。

- AWS Global Accelerator 標準アクセラレーター – Shield は、エンドポイント設定に基づいて容量を取得します。

これらの評価は、ポートやプロトコルなど、ネットワークトラフィックの複数のディメンションにわたって行われます。ターゲットリソースの容量を超えると、Shield は DDoS 緩和策を実行します。Shield によって実施された緩和策は DDoS トラフィックを削減しますが、完全に排除することはできない場合があります。Shield は、既知の DDoS 攻撃ベクトルと一致するトラフィックディメンションでリソースの容量がわずかに超過した場合も、緩和策を講じることがあります。Shield は、この緩和策を有効期限 (TTL) を設けて実施し、攻撃が続く限り延長されます。

> **Note**
>
> Shield によって実施された緩和策は DDoS トラフィックを削減しますが、完全に排除することはできない場合があります。Shield を のようなソリューション AWS Network Firewall や のようなホスト上のファイアウォールで強化iptablesすることで、アプリケーションがアプリケーションに有効でないか、正当なエンドユーザーによって生成されなかったトラフィックを処理できないようにすることができます。

Shield Advanced の保護では、既存の Shield の検出アクティビティに次が追加されます。

- [Lower detection thresholds] (検出しきい値を下げる) – Shield Advanced は、計算された容量の半分に緩和策を実施します。これにより、ゆっくり増加する攻撃をより迅速に緩和し、より曖昧なボリュームシグネチャを持つ攻撃を緩和できます。
- [Intermittent attack protection] (断続的な攻撃からの保護) – Shield Advanced は、攻撃の頻度と期間に基づいて、指数関数的に増加する有効期限 (TTL) で緩和策を実施します。これにより、リソースが頻繁にターゲットとなり、短いバーストで攻撃が発生する際に、緩和策が長く維持されます。
- [Health-based detection] (ヘルスベースの検出) – Route 53 ヘルスチェックを Shield Advanced で保護されたリソースに関連付けると、ヘルスチェックのステータスが検出ロジックで使用されます。検出されたイベント中、ヘルスチェックが正常である場合、Shield Advanced では、緩和策を行う前に、そのイベントが攻撃であるというより強力な確信が必要です。代わりにヘルスチェックが異常な場合は、信頼が確立される前でも Shield Advanced が緩和策を講じることがあります。この機能は、誤検出を回避するのに役立つとともに、アプリケーションに影響する攻撃への迅速な対応を提供します。Shield Advanced を使用したヘルスチェックの詳細については、「Shield Advanced と Route 53 を使用したヘルスチェックを使用したヘルスベースの検出」を参照してください。

アプリケーションレイヤーの脅威に対する Shield Advanced 検出ロジック (レイヤー 7)

このページでは、アプリケーション層におけるイベント検出の仕組みについて説明します。

AWS Shield Advanced は、保護された Amazon CloudFront ディストリビューションと Application Load Balancer のウェブアプリケーションレイヤー検出を提供します。これらのリソースタイプを Shield Advanced で保護する場合、 AWS WAF ウェブ ACL を保護に関連付けて、ウェブアプリケーションレイヤーの検出を有効にすることができます。Shield Advanced は、関連付けられたウェブ ACL のリクエストデータを消費し、アプリケーションのトラフィックベースラインを構築します。ウェブアプリケーションレイヤーの検出は、Shield Advanced と AWS WAFのネイティブ統合に依存しています。 AWS WAF ウェブ ACL を Shield Advanced で保護されたリソースに関連付けるなど、アプリケーションレイヤーの保護の詳細については、「」を参照してくださいAWS Shield Advanced および を使用したアプリケーションレイヤー (レイヤー 7) の保護 AWS WAF。

ウェブアプリケーションレイヤーの検出では、Shield Advanced はアプリケーショントラフィックをモニタリングし、異常を検出する過去のベースラインと比較します。このモニタリングは、トラフィックの総量と構成をカバーします。DDoS 攻撃を受けている最中、トラフィックの量と構成の両方が変化することが想定され、Shield Advanced では、イベントを宣言するために両方における統計的に有意な偏差が必要です。

Shield Advanced は、過去のタイムウィンドウに照らして測定を実行します。このアプローチを使用すると、トラフィック量の正当な変化や、毎日同じ時間に提供される販売など、想定されるパターンに一致するトラフィックの変化による誤検出の通知が減少します。

> **Note**
>
> Shield Advanced が通常の正当なトラフィックパターンを表すベースラインを確立する時間を与えることで、Shield Advanced 保護の誤検出を回避できます。Shield Advanced は、ウェブ ACL を保護されたリソースに関連付けると、ベースラインの情報を収集し始めます。ウェブトラフィックに異常なパターンを引き起こす可能性のある予定イベントの少なくとも 24 時間前に、ウェブ ACL を保護リソースに関連付けます。Shield Advanced のウェブアプリケーションレイヤー検出は、30 日間の通常のトラフィックが観測された場合に最も正確です。

Shield Advanced がイベントを検出するのにかかる時間は、トラフィック量で見られる変化の量の影響を受けます。量の変化が少ない場合、Shield Advanced は、イベントが発生していることについて

のより強い確信を持つために、トラフィックをより長い期間にわたって観察します。量の変化が大きい場合、Shield Advanced はイベントをより迅速に検出してレポートします。

ウェブ ACL のレートベースのルールは、ユーザーによって追加されるか、Shield Advanced 自動アプリケーションレイヤー緩和機能によって追加されるかにかかわらず、検出可能なレベルに達する前に攻撃を軽減できます。アプリケーションレイヤー DDoS の自動緩和の詳細については、Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和 を参照してください。

> **Note**
>
> トラフィックの増加やロードに対応してスケールするようにアプリケーションを設計して、小規模なリクエストフラッドの影響を受けないようにすることができます。Shield Advanced を使用すると、保護されたリソースはコスト保護の対象となります。これは、DDoS 攻撃の結果として発生する可能性のあるクラウド料金の想定外の増加を防ぐのに役立ちます。Shield Advanced のコスト保護の詳細については、「攻撃 AWS Shield Advanced 後の でのクレジットのリクエスト」を参照してください。

アプリケーション内の複数のリソースの Shield Advanced 検出ロジック

このページでは、アプリケーション内の複数のリソースのためにイベント検出の仕組みについて説明します。

AWS Shield Advanced 保護グループを使用して、同じアプリケーションの一部である保護されたリソースのコレクションを作成できます。グループに配置する保護されたリソースを選択するか、同じタイプのすべてのリソースを 1 つのグループとして扱うことを指定できます。例えば、すべての Application Load Balancer のグループを作成できます。保護グループを作成すると、Shield Advanced 検出は、グループ内の保護されたリソースに関するすべてのトラフィックを集約します。これは、トラフィック量は少ないが、集約されたボリュームが大きいリソースが多数ある場合に有益です。また、保護されたリソース間でトラフィックが転送されるブルーグリーンデプロイメント向けに、保護グループを使用してアプリケーションベースラインを保持することもできます。

次のいずれかの方法で保護グループ内のトラフィックを集約することを選択できます。

- [Sum] (合計) – この集計は、保護グループ内のリソース全体のすべてのトラフィックを合計します。この集約を使用して、新しく作成されたリソースに既存のベースラインが確実に存在しているようにしたり、検出の感度を下げて、誤検出を防いだりすることができます。

- [Mean] (平均) – この集計は、保護グループ全体のすべてのトラフィックの平均を使用します。この集約は、ロードバランサーのように、リソース間のトラフィックが均一であるアプリケーションに使用できます。
- [Max] (最大) – この集約は、保護グループ内のリソースの中で最も高いトラフィックを使用します。この集約は、保護グループにアプリケーションの階層が複数ある場合に使用できます。例えば、CloudFront ディストリビューション、その Application Load Balancer のオリジン、および Application Load Balancer の Amazon EC2 インスタンスターゲットを含む保護グループがあるとします。

また、保護グループを使用して、複数のインターネットに接続する Elastic IP または AWS Global Accelerator 標準のアクセラレーターをターゲットとする攻撃に対して、Shield Advanced が緩和策を実施する速度を向上させることもできます。保護グループ内の 1 つのリソースがターゲットになると、Shield Advanced は、グループ内の他のリソースについての信頼を確立します。これにより、Shield Advanced 検出がアラート状態になり、追加の緩和策の作成に必要な時間を短縮できます。

保護グループの詳細については、「AWS Shield Advanced 保護のグループ化」を参照してください。

がイベント AWS Shield を軽減する方法

このページでは、 AWS Shield イベント緩和の仕組みについて説明します。

アプリケーションを保護する緩和ロジックは、アプリケーションのアーキテクチャによって異なります。Amazon CloudFront および Amazon Route 53 でウェブアプリケーションを保護する場合、ウェブおよび DNS ユースケースに固有の緩和策と、サービスのすべてのトラフィックを保護する緩和策の恩恵を受けることができます。アプリケーションのエントリポイントが リージョンで AWS 実行されるリソースである場合、緩和ロジックはサービス、リソースタイプ、および の使用によって異なります AWS Shield Advanced。

AWS DDoS 緩和システムは Shield エンジニアによって開発され、 AWS サービスと緊密に統合されています。エンジニアは、ターゲットリソースの容量や健全性など、アーキテクチャの側面を考慮に入れます。Shield エンジニアは、DDoS 緩和システムの有効性とパフォーマンスを継続的に監視し、新しい脅威が発見または予測されたときに迅速に対応できます。

トラフィックの増加やロードに対応してスケールするようにアプリケーションを設計して、小規模なリクエストフラッドの影響を受けないようにする手助けをします。Shield Advanced を使用してリ

ソースを保護すると、DDoS 攻撃の結果として発生する可能性のあるクラウド料金の予想外の増加を防ぐことができます。

インフラストラクチャの緩和

インフラストラクチャレイヤー攻撃の場合、 AWS Shield DDoS 緩和システムは AWS ネットワーク境界と AWS エッジロケーションに存在します。 AWS インフラストラクチャ全体に複数のレベルのセキュリティコントロールを配置することで、クラウドアプリケーションにdefense-in-depthを提供します。

Shield により、インターネットからの進入のすべてのポイントで DDoS 軽減システムを維持されます。Shield は DDoS 攻撃を検出すると、進入ポイントごとに、同じ場所にある DDoS 緩和システムを介してトラフィックを再ルーティングします。これにより、観測可能なレイテンシーがさらに発生することはなく、すべての AWS リージョンとすべてのエッジロケーションにおいて、100 テラビット/秒 (Tbps) を超える緩和能力を実現します。Shield は、トラフィックを外部またはリモートのスクラビングセンターに再ルーティングすることなく、リソースの可用性を保護します。これにより、レイテンシーが増加する可能性があります。

- AWS ネットワーク境界では、あらゆる AWS サービスまたはリソースについて、DDoS 緩和システムはインターネットからのインフラストラクチャレイヤー攻撃を軽減します。Shield による検出または Shield Response Team (SRT) のエンジニアによる通知があると、システムは緩和を実行します。
- AWS エッジロケーションでは、DDoS 緩和システムは、オリジンに関係なく、Amazon CloudFront ディストリビューションと Amazon Route 53 ホストゾーンに転送されるすべてのパケットを継続的に検査します。必要な場合、システムはウェブおよび DNS トラフィック向けに特別に設計された緩和策を適用します。Amazon CloudFront と Amazon Route 53 を使用してウェブアプリケーションを保護することで付加される利点の 1 つは、Shield 検出からのシグナルを必要とせずに DDoS 攻撃を即座に軽減できることです。

アプリケーションレイヤーの緩和

Shield Advanced は、Shield Advanced 保護を有効にした Amazon CloudFront ディストリビューションと Application Load Balancer 向けに、ウェブアプリケーションレイヤー緩和を提供します。保護を有効にすると、 AWS WAF ウェブ ACL をリソースに関連付けて、ウェブアプリケーションレイヤーの検出を有効にします。さらに、自動アプリケーションレイヤー軽減を有効にするオプションがあります。これは、DDoS 攻撃中に保護を管理するよう Shield Advanced に指示します。

Shield は、Shield Advanced と自動アプリケーションレイヤー緩和を有効にしたリソースに対するアプリケーションレイヤー攻撃に対してのみカスタム緩和策を提供します。自動緩和により、Shield

Advanced は既知の DDoS ソースからのリクエストに AWS WAF レート制限を適用し、検出された DDoS 攻撃に応じてカスタム AWS WAF 保護を自動的に追加および管理します。このタイプの緩和の詳細については、「Shield Advanced が自動緩和を管理する方法」を参照してください。。

ウェブ ACL のレートベースのルールは、ユーザーが追加した場合でも、Shield Advanced 自動アプリケーションレイヤー緩和機能によって追加された場合でも、検出可能なレベルに達する前に攻撃を軽減できます。検知の詳細については、アプリケーションレイヤーの脅威に対する Shield Advanced 検出ロジック (レイヤー 7) を参照してください。

トピック

- AWS Shield DDoS 緩和機能のリスト
- AWS Shield CloudFront と Route 53 の緩和ロジック
- AWS Shield AWS リージョンの緩和ロジック
- AWS Shield AWS Global Accelerator 標準アクセラレーターの緩和ロジック
- AWS Shield Advanced Elastic IPs の緩和ロジック
- AWS Shield Advanced ウェブアプリケーションの緩和ロジック

AWS Shield DDoS 緩和機能のリスト

AWS Shield DDoS 緩和の主な機能は次のとおりです。

- パケット検証 — これにより、検査されたすべてのパケットが期待される構造に適合し、そのプロトコルに対して有効であることが保証されます。サポートされているプロトコル検証には、IP、TCP (ヘッダーとオプションを含む)、UDP、ICMP、DNS、および NTP が含まれます。
- アクセスコントロールリスト (ACL) と Shaper — ACL は特定の属性に対してトラフィックを評価し、一致するトラフィックをドロップするか、シェーパーにマッピングします。シェーパーは、一致するトラフィックのパケットレートを制限し、送信先に到達するボリュームを含めるために余分なパケットをドロップします。 AWS Shield detection and Shield Response Team (SRT) エンジニアは、予想されるトラフィックへの専用レート割り当てと、既知の DDoS 攻撃ベクトルに一致する属性を持つトラフィックへのより制限的なレート割り当てを提供できます。ACL が照合できる属性には、パケットペイロード内のポート、プロトコル、TCP フラグ、宛先アドレス、送信元の国、および任意のパターンが含まれます。
- 疑惑のスコアリング — これにより、Shield が期待するトラフィックに関する知識を使用して、すべてのパケットにスコアを適用されます。既知の正常なトラフィックのパターンに近いパケットには、より低い疑惑スコアが割り当てられます。既知の不良トラフィック属性を観察すると、パケッ

トの疑惑スコアが高まる可能性があります。レート制限パケットが必要な場合、Shield は疑惑スコアが高いパケットからドロップします。これは、Shield が誤検知を回避しながら、既知の DDoS 攻撃とゼロデイ攻撃の両方を軽減するのに役立ちます。

- TCP SYN プロキシ — これにより、TCP SYN Cookie が保護されたサービスに渡すのを許可する前に新しい接続に挑戦するために TCP SYN Cookie を送信することで、TCP SYN フラッドに対する保護が提供されます。Shield DDoS 緩和によって提供される TCP SYN プロキシはステートレスであり、ステートを使い果たすことなく、既知の最大の TCP SYN フラッド攻撃を軽減できます。これは、クライアントと保護された AWS サービス間の継続的なプロキシを維持するのではなく、 サービスと統合して接続状態を渡すことによって実現されます。TCP SYN プロキシは現在、Amazon CloudFront、Amazon Route 53、および で使用できます AWS Global Accelerator。
- レートの分布 — これにより、保護されたリソースへのトラフィックの入力パターンに基づいて、ロケーションシェーパーの値を継続的に調整します。これにより、 AWS ネットワークに均等に進まない可能性のある顧客トラフィックのレート制限を防ぐことができます。

AWS Shield CloudFront と Route 53 の緩和ロジック

このページでは、Shield DDoS 緩和が Cloud Front および Route 53 のトラフィックを継続的に検査する仕組みについて説明します。これらのサービスは、 AWS エッジロケーションのグローバルに分散されたネットワークから動作し、Shield の DDoS 緩和容量への広範なアクセスを提供し、エンドユーザーに近いインフラストラクチャからアプリケーションを提供します。

> **Important**
>
> AWS Shield Advanced は CloudFront テナントをサポートしていません。

- CloudFront — Shield DDoS 緩和では、Web アプリケーションがサービスへのパススルーに有効なトラフィックのみを許可します。これにより、UDP リフレクション攻撃など、多くの一般的な DDoS ベクトルに対して自動的に保護されます。

  CloudFront はアプリケーションオリジンへの永続的な接続を維持し、Shield TCP SYN プロキシ機能との統合によって TCP SYN フラッドが自動的に緩和され、Transport Layer Security (TLS) はエッジで終了します。これらの機能を組み合わせることで、アプリケーションオリジンは整形式のウェブリクエストのみを受信し、下位層の DDoS 攻撃、接続フラッド、および TLS 不正使用から保護されます。

CloudFront は DNS トラフィック方向とエニーキャストルーティングの組み合わせを使用します。これらの手法は、ソースに近い攻撃を緩和し、障害を分離し、容量へのアクセスを確保して既知の最大の攻撃を軽減することで、アプリケーションの復元力を向上させます。

- Route 53 — Shield 緩和では、有効な DNS リクエストのみがサービスに到達することを許可します。Shield は、既知の正常なクエリに優先順位を付け、疑わしいまたは既知の DDoS 攻撃属性を含むクエリの優先度を下げる、疑わしいスコアリングを使用して DNS クエリのフラッドを軽減します。

  Route 53 は、シャッフルシャーディングを使用して、IPv4 と IPv6 の両方のホストゾーンに 4 つのリゾルバー IP アドレスの一意のセットを提供します。各 IP アドレスは、Route 53 ロケーションの異なるサブセットに対応します。各ロケーションサブセットは、他のサブセットのインフラストラクチャと部分的にしか重複しない権限を持つ DNS サーバーで構成されます。これにより、何らかの理由でユーザークエリが失敗した場合、再試行時に正常に処理されるようになります。

  Route 53 は、エニーキャストルーティングを使用して、ネットワークの近接度に基づいて DNS クエリを最も近いエッジロケーションに送信します。エニーキャストはまた、DDoS トラフィックを多くのエッジロケーションにファンアウトし、攻撃が単一のロケーションに集中するのを防ぎます。

緩和の速度に加えて、CloudFront と Route 53 は Shield のグローバルに分散された容量への幅広いアクセスを提供します。これらの機能を活用するには、これらのサービスを動的または静的ウェブアプリケーションのエントリーポイントとして使用します。

CloudFront と Route 53 を使用してウェブアプリケーションを保護する方法の詳細については、「How to Help Protect Dynamic Web Applications Against DDoS Attacks by Using Amazon CloudFront and Amazon Route 53」(Amazon CloudFront と Amazon Route 53 を使用して DDoS 攻撃から動的ウェブアプリケーションを保護する方法) を参照してください。Route 53 での障害分離の詳細については、「グローバルフォールトアイソレーションのケーススタディ」を参照してください。

AWS Shield AWS リージョンの緩和ロジック

このページでは、Shield イベント緩和ロジックが AWS リージョンでどのように機能するかについて説明します。

AWS リージョンで起動されるリソースは、Shield リソースレベル検出によって配置される AWS Shield DDoS 緩和システムによって保護されます。リージョンリソースには、Elastic IP (EIP)、クラシックロードバランサー、アプリケーションロードバランサーなどがあります。

緩和を実施する前に、Shield はターゲットリソースとその容量を特定します。Shield は、キャパシティを使用して、緩和がリソースに転送できる最大合計トラフィックを決定します。アクセスコントロールリスト（ACL）および緩和策内のその他のシェーパによって、既知の DDoS 攻撃ベクトルに一致するトラフィックや、大量の受信が予想されないトラフィックなど、一部のトラフィックで許可されるボリュームが減少する可能性があります。これにより、UDP リフレクション攻撃や TCP SYN フラグまたは FIN フラグを持つ TCP トラフィックに対して、緩和によって許可されるトラフィック量がさらに制限されます。

Shield は、リソースタイプごとにキャパシティを決定し、緩和を別々に配置します。

- Amazon EC2 インスタンス、または Amazon EC2 インスタンスにアタッチされている EIP の場合、Shield はインスタンスタイプおよびその他のインスタンス属性 (インスタンスで拡張ネットワーキングが有効になっているかどうかなど) に基づいて容量を計算します。
- Application Load Balancer または Classic Load Balancer の場合、Shield はロードバランサーのターゲットノードごとに個別に容量を計算します。これらのリソースに対する DDoS 攻撃の緩和は、Shield DDoS 緩和とロードバランサーによる自動スケーリングの組み合わせによって提供されます。Shield Response Team (SRT) がApplication Load Balancer またはClassic Load Balancer のリソースに対する攻撃に従事している場合、追加の保護対策としてスケーリングを加速する可能性があります。
- Shield は、基盤となる AWS インフラストラクチャの使用可能な容量に基づいて、一部の AWS リソースの容量を計算します。これらのリソースタイプには、Network Load Balancer (NLBs と、Gateway Load Balancer または を介してトラフィックをルーティングするリソースが含まれます AWS Network Firewall。

> **Note**
>
> Shield Advanced で保護されている EIP をアタッチして、ネットワークロードバランサーを保護します。SRT と連携して、基盤となるアプリケーションの予想されるトラフィックと容量に基づくカスタム緩和を構築できます。

Shield が緩和策を設定すると、Shield が緩和ロジックで定義した初期レート制限が、すべての Shield DDoS 緩和システムに等しく適用されます。たとえば、Shield が 100,000 パケット/秒 (pps) の制限で緩和を設定した場合、最初はすべてのロケーションで 100,000 pps を許可します。次に、Shield は継続的に緩和メトリクスを集約してトラフィックの実際の比率を決定し、その比率を使用して各ロケーションのレート制限を調整します。これにより、誤検出を防ぎ、緩和が過度に許容されないようにします。

AWS Shield AWS Global Accelerator 標準アクセラレーターの緩和ロジック

このページでは、Shield イベント緩和ロジックが AWS Global Accelerator 標準アクセラレーターでどのように機能するかについて説明します。Shield 緩和は、有効なトラフィックがグローバルアクセラレータの標準アクセラレータのリスナーエンドポイントに到達することのみを許可します。

標準アクセラレーターはグローバルにデプロイされ、任意の AWS リージョンの AWS リソースにトラフィックをルーティングするために使用できる IP アドレスを提供します。Shield が Global Accelerator への緩和に対して適用するレート制限は、標準アクセラレータがトラフィックをルーティングするリソースの容量に基づいています。Shield は、総トラフィックが決められたレートを超えたとき、および既知の DDoS ベクトルに対してそのレートの割合を超えた場合に、緩和を実行します。

標準アクセラレータを設定するときは、アプリケーションのトラフィックをルーティングする AWS リージョンごとにエンドポイントグループを定義します。Shield が緩和策を設定すると、各エンドポイントグループの容量が計算され、それに応じて各 Shield DDoS 緩和システムのレート制限が更新されます。レートは、トラフィックがインターネットから AWS リソースにルーティングされる方法について Shield が行った仮定に基づいて、場所によって異なります。エンドポイントグループのキャパシティは、グループ内のリソースの数に、グループ内の任意のリソースの最小容量を乗じて計算されます。一定の間隔で、Shield はアプリケーションの容量を再計算し、必要に応じてレート制限を更新します。

> **Note**
>
> トラフィックダイヤルを使用してエンドポイントグループに誘導されるトラフィックの割合を変更しても、Shield DDoS 軽減システムに対してレート制限を計算または配布する方法は変わりません。トラフィックダイヤルを使用する場合は、リソースタイプと数量について相互にミラーリングするようにエンドポイントグループを構成します。これにより、Shield によって計算されたキャパシティが、アプリケーションのトラフィックを処理しているリソースを代表するようにできます。

Global Accelerator のエンドポイントグループとトラフィックダイヤルの詳細については、「AWS Global Accelerator 標準アクセラレーターのエンドポイントグループ」を参照してください。

AWS Shield Advanced Elastic IPs の緩和ロジック

このページでは、 で Shield イベント緩和ロジックが Elastic IPs に対してどのように機能するかについて説明します AWS Shield Advanced。で Elastic IP (EIP) を保護すると AWS Shield Advanced、Shield Advanced は Shield が DDoS イベント中に導入する緩和策を強化します。

Shield Advanced DDoS 緩和システムは、EIP が関連付けられているパブリックサブネットのネットワーク ACL (NACL) 設定を複製します。たとえば、NACL がすべての UDP トラフィックをブロックするように設定されている場合、Shield Advanced はそのルールを Shield が配置する緩和にマージします。

この追加機能は、アプリケーションに対して有効ではないトラフィックによる可用性リスクを回避するのに役立ちます。NACL を使用して、個々の送信元 IP アドレスまたは送信元 IP アドレス CIDR 範囲をブロックすることもできます。これは、分散されていない DDoS 攻撃の緩和ツールとして役立ちます。また、 AWS エンジニアの介入に頼ることなく、独自の許可リストを簡単に管理したり、アプリケーションと通信すべきではない IP アドレスをブロックしたりできます。

AWS Shield Advanced ウェブアプリケーションの緩和ロジック

AWS Shield Advanced は AWS WAF を使用してウェブアプリケーションレイヤー攻撃を軽減します。 AWS WAF は、追加コストなしで Shield Advanced に含まれています。

アプリケーションレイヤー標準保護

Amazon CloudFront ディストリビューションまたは Application Load Balancer を Shield Advanced で保護する場合、Shield Advanced を使用して AWS WAF ウェブ ACL を保護されたリソースにまだ関連付けていない場合は、関連付けることができます。ウェブ ACL をまだ設定していない場合は、Shield Advanced コンソールウィザードを使用して作成して、レートベースのルールを追加できます。レートベースのルールは、各 IP アドレスの 5 分間の時間枠あたりの要求数を制限し、ウェブアプリケーション層のリクエストのフラッドに対する基本的な保護を提供します。レートは 10 から設定できます。詳細については、「AWS WAF ウェブ ACLs と Shield Advanced によるアプリケーションレイヤーの保護」を参照してください。

AWS WAF サービスを使用してウェブ ACL を管理することもできます。を通じて AWS WAF、ウェブ ACL 設定を拡張して、特定のウェブリクエストコンポーネントの文字列一致やパターンの検査、カスタムリクエストとレスポンスの処理の追加、リクエストオリジンの位置情報との照合などを行うことができます。 AWS WAF ルールの詳細については、「」を参照してくださいAWS WAF ルール。

アプリケーションレイヤーの自動緩和

保護を強化するには、Shield Advanced アプリケーションレイヤーの自動緩和を有効にします。このオプションを使用すると、Shield Advanced は既知の DDoS ソースからのリクエストの AWS WAF レート制限ルールを維持し、検出された DDoS 攻撃のカスタム緩和を提供します。

Shield Advanced は、保護されたリソースに対する攻撃を検出すると、アプリケーションへの通常のトラフィックから攻撃トラフィックを分離する攻撃シグネチャの特定を試みます。Shield Advanced は、識別された攻撃シグネチャを攻撃対象のリソースおよび同じウェブ ACL に関連付けられている他のリソースについての過去のトラフィックパターンに照らして評価します。

Shield Advanced は、攻撃シグネチャが DDoS 攻撃に関与しているトラフィックのみを分離していると判断した場合、関連付けられたウェブ ACL 内の AWS WAF ルールにシグネチャを実装します。Shield Advanced に、一致したトラフィックのみをカウントする、またはブロックする緩和を配置するように指示できます。この設定はいつでも変更できます。Shield Advanced は、緩和ルールが不要になったと判断すると、そのルールをウェブ ACL から削除します。アプリケーションレイヤーイベントの緩和の詳細については、「Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和」を参照してください。

Shield Advanced アプリケーションレイヤー の緩和の詳細については、「AWS Shield Advanced および を使用したアプリケーションレイヤー (レイヤー 7) の保護 AWS WAF」を参照してください。

Shield Advanced を使用した基本的な DDoS 耐障害性アーキテクチャの構築

このページでは、分散型サービス拒否 (DDoS) の障害耐性について説明し、2 つのアーキテクチャ例を紹介します。

DDoS 耐障害性とは、正規ユーザーに引き続きサービスを提供しながら、分散型サービス拒否 (DDoS) 攻撃に耐えるアプリケーションアーキテクチャの機能です。高い耐障害性を持つアプリケーションは、エラーやレイテンシーなどのパフォーマンスメトリクスへの影響を最小限に抑えながら、攻撃を受けている最中も引き続き利用可能な状態を維持できます。このセクションでは、いくつかの一般的なアーキテクチャの例を示し、 AWS および Shield Advanced によって提供される DDoS 検出および緩和機能を使用して DDoS レジリエンシーを高める方法について説明します。

このセクションのアーキテクチャの例では、デプロイされたアプリケーションに DDoS レジリエンシーの最大のメリットを提供する AWS のサービスに焦点を当てています。主なサービスには、次のようなメリットがあります。

- グローバルに分散されたネットワーク容量へのアクセス – Amazon CloudFront、および Amazon Route 53 のサービスにより AWS Global Accelerator、 AWS グローバルエッジネットワーク全体

のインターネットおよび DDoS 緩和容量にアクセスできます。これは、大規模にテラビットに達する可能性がある、比較的大きなボリューム攻撃を緩和するのに有益です。アプリケーションを任意の AWS リージョンで実行し、これらのサービスを使用して可用性を保護し、正当なユーザーのパフォーマンスを最適化できます。

- ウェブアプリケーションレイヤーの DDoS 攻撃のベクトルに対する保護 – ウェブアプリケーションレイヤーの DDoS 攻撃は、アプリケーションのスケールとウェブアプリケーションファイアウォール (WAF) の組み合わせを使用することによって最も効果的に緩和されます。Shield Advanced は、 からのウェブリクエスト検査ログ AWS WAF を使用して、自動で、または Shield Response Team (SRT) とのエンゲージメントを通じて軽減できる異常を検出します AWS 。自動緩和は、デプロイされた AWS WAF レートベースのルールと、Shield Advanced アプリケーションレイヤー DDoS 自動緩和を通じて利用できます。

これらの例を確認することに加えて、「AWS Best Practices for DDoS Resiliency」(DDoS レジリエンシーに関するのベストプラクティス) で該当するベストプラクティスを確認し、それに従います。

トピック

- 一般的なウェブアプリケーションの Shield Advanced DDoS 耐障害性アーキテクチャの例
- TCP および UDP アプリケーションの Shield Advanced DDoS 耐障害性アーキテクチャの例

一般的なウェブアプリケーションの Shield Advanced DDoS 耐障害性アーキテクチャの例

このページでは、 AWS ウェブアプリケーションによる DDoS 攻撃に対する耐障害性を最大化するためのアーキテクチャの例を示します。

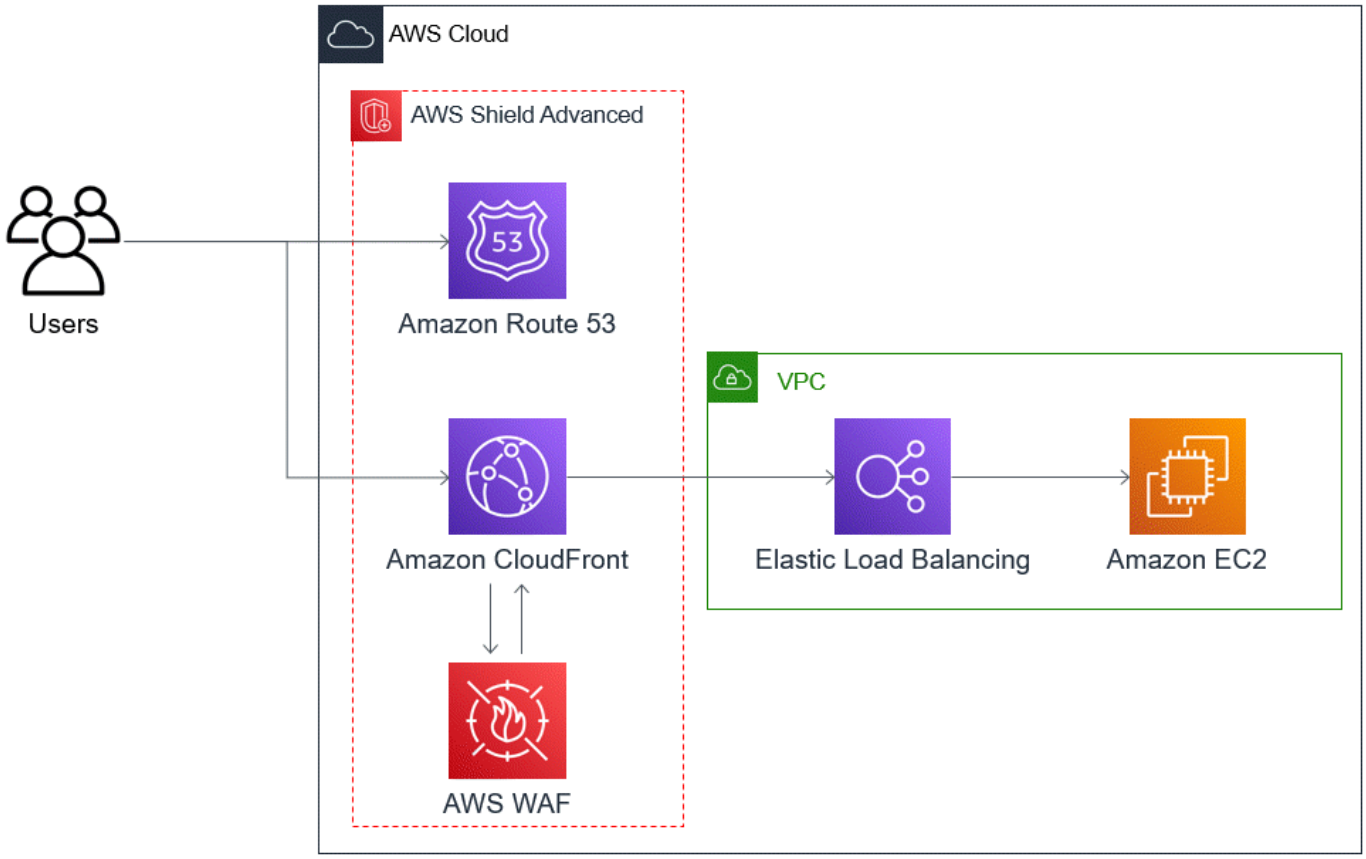
任意の AWS リージョンにウェブアプリケーションを構築し、そのリージョンで AWS が提供する検出および緩和機能から DDoS の自動保護を受けることができます。

この例は、Classic Load Balancer、Application Load Balancer、Network Load Balancer、 AWS Marketplace ソリューション、または独自のプロキシレイヤーなどのリソースを使用して、エンドユーザーをウェブアプリケーションにルーティングするアーキテクチャ向けです。これらの AWS WAF ウェブアプリケーションリソースとユーザーの間に Amazon Route 53 ホストゾーン、Amazon CloudFront ディストリビューション、ウェブ ACLs を挿入することで、DDoS の耐障害性を向上させることができます。これらの挿入により、アプリケーションのオリジンが難読化され、エンドユーザーにより近いリクエストを処理し、アプリケーションレイヤーのリクエストのフラッドを検出して緩和できます。CloudFront および Route 53 を使用してエンドユーザーに静的または動的コンテンツ

を提供するアプリケーションは、インフラストラクチャレイヤー攻撃をリアルタイムで緩和する、統合された完全インライン DDoS 緩和システムによって保護されます。

これらのアーキテクチャの改善を実施することにより、Shield Advanced を使用して Route 53 ホストゾーンと CloudFront ディストリビューションを保護できます。CloudFront ディストリビューションを保護すると、Shield Advanced は AWS WAF ウェブ ACLs関連付けてレートベースのルールを作成するように促し、アプリケーションレイヤー DDoS 自動緩和またはプロアクティブエンゲージメントを有効にするオプションを提供します。プロアクティブなエンゲージメントとアプリケーションレイヤー DDoS 自動緩和では、リソースに関連付ける Route 53 ヘルスチェックを使用します。これらのオプションの詳細については、「でのリソース保護 AWS Shield Advanced」を参照してください。

次の参照図は、ウェブアプリケーション用のこの DDoS 回復アーキテクチャを示しています。



このアプローチがウェブアプリケーションに提供するメリットには、次のものがあります。

- 頻繁に使用されるインフラストラクチャレイヤー (レイヤー 3 およびレイヤー 4) の DDoS 攻撃に対する保護。検出の遅延はありません。さらに、リソースが頻繁にターゲットになっている場合、Shield Advanced はより長期にわたって緩和策を実施します。また、Shield Advanced

は、Network ACL (NACL) から推測されるアプリケーションコンテキストを使用して、望ましくないトラフィックがさらにアップストリームするのをブロックします。これにより、ソースにより近い障害を隔離でき、正当なエンドユーザーへの影響が最小限に抑えられます。

- TCP SYN フラッドに対する保護。CloudFront、Route 53 と統合され、新しい接続試行にチャレンジし、正当なユーザーのみを提供する TCP SYN プロキシ機能 AWS Global Accelerator を提供する DDoS 緩和システム。
- DNS アプリケーションレイヤー攻撃に対する保護 (Route 53 は権威 DNS レスポンスを処理する責任があるため)。
- ウェブアプリケーションレイヤーリクエストのフラッドに対する保護。 AWS WAF ウェブ ACL で設定したレートベースのルールは、ルールで許可されているよりも多くのリクエストを送信するときにソース IPs をブロックします。
- CloudFront ディストリビューションのアプリケーションレイヤー DDoS 自動緩和機能 (このオプションを有効にした場合)。自動 DDoS 緩和により、Shield Advanced は、既知の DDoS ソースからのリクエストの量を制限するレートベースのルールをディストリビューションに関連付けられた AWS WAF ウェブ ACL に維持します。さらに、Shield Advanced は、アプリケーションのヘルスに影響を及ぼすイベントを検出すると、ウェブ ACL の緩和ルールを自動的に作成、テスト、および管理します。
- Shield Response Team (SRT) とのプロアクティブなエンゲージメント (このオプションを有効にした場合)。Shield Advanced がアプリケーションのヘルスに影響を与えるイベントを検出すると、SRT は、提供された連絡先情報を使用して、お客様のセキュリティチームまたはオペレーションチームとプロアクティブに対応します。SRT はトラフィックのパターンを分析し、 AWS WAF ルールを更新して攻撃をブロックできます。

TCP および UDP アプリケーションの Shield Advanced DDoS 耐障害性アーキテクチャの例

この例は、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは Elastic IP (EIP) アドレスを使用する AWS リージョンの TCP および UDP アプリケーション向けの DDoS に対する耐性の高いアーキテクチャを示しています。

この一般的な例に従って、次のアプリケーションタイプの DDoS レジリエンシーを改善できます。

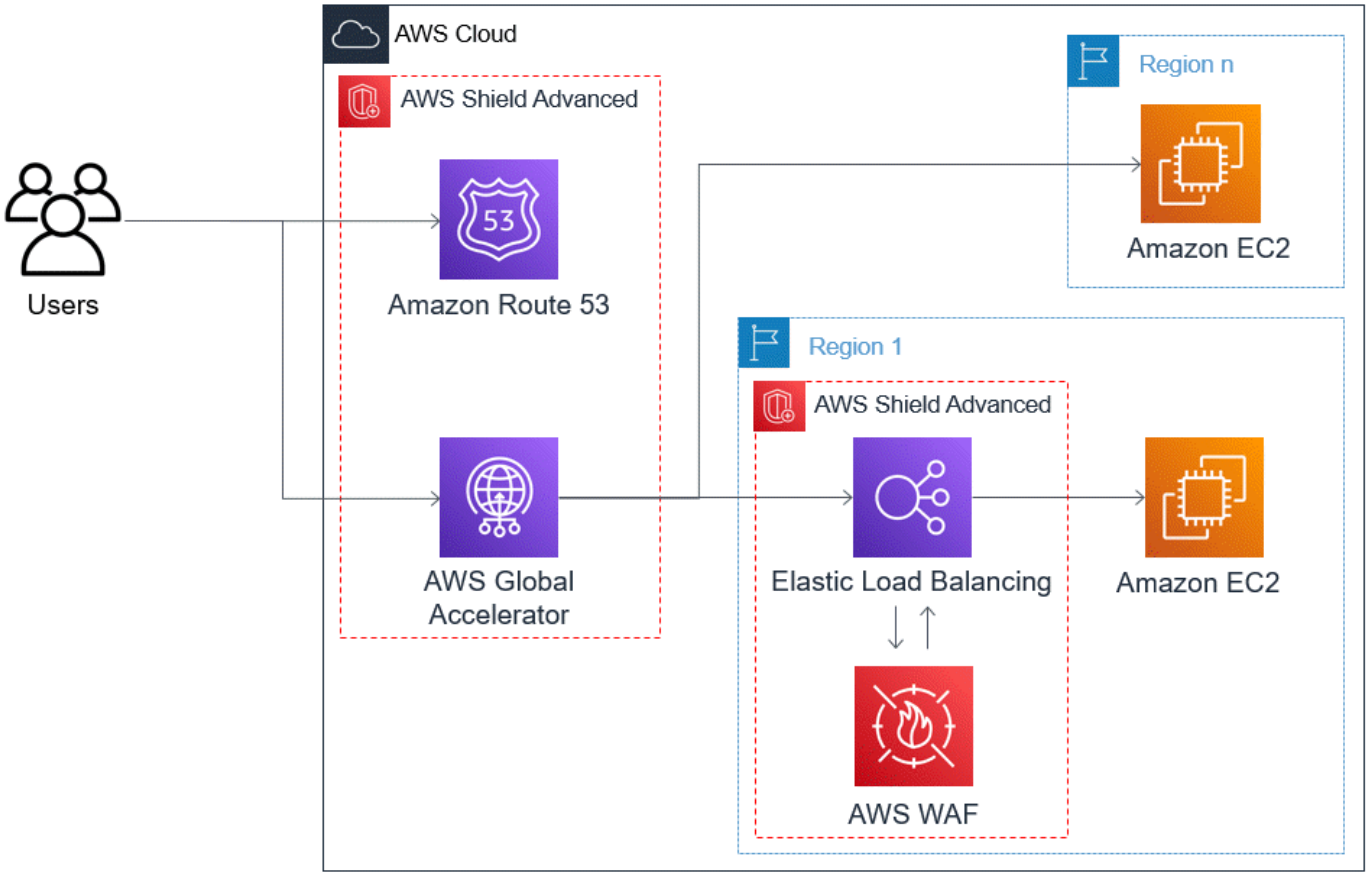
- TCP または UDP アプリケーション。ゲーム、IoT、およびボイスオーバー IP に使用されるアプリケーションはその一例です。
- 静的 IP アドレスを必要とするウェブアプリケーション、または Amazon CloudFront がサポートしていないプロトコルを使用するウェブアプリケーション。たとえば、アプリケーションでは、ユー

ザーがファイアウォール許可リストに追加でき、他の AWS お客様が使用していない IP アドレスが必要になる場合があります。

Amazon Route 53 および AWS Global Acceleratorを導入することで、これらのアプリケーションタイプの DDoS レジリエンシーを改善できます。これらのサービスは、エンドユーザーをアプリケーションにルーティングでき、 AWS グローバルエッジネットワークを介してルーティングされるエニーキャストである静的 IP アドレスをアプリケーションに提供できます。Global Accelerator 標準アクセラレーターは、エンドユーザーのレイテンシーを最大 60% 改善できます。ウェブアプリケーションがある場合は、Application Load Balancer でアプリケーションを実行し、ウェブ ACL で Application Load Balancer を保護することで、 AWS WAF ウェブアプリケーションレイヤーリクエストのフラッドを検出して軽減できます。

アプリケーションの構築後、Shield Advanced を使用して、Route 53 ホストゾーン、Global Accelerator 標準アクセラレーター、および Application Load Balancer を保護します。Application Load Balancer を保護すると、 AWS WAF ウェブ ACLs関連付けてレートベースのルールを作成できます。新規または既存の Route 53 ヘルスチェックを関連付けることで、Global Accelerator 標準アクセラレーターと Application Load Balancerの両方のために、SRT とのプロアクティブエンゲージメントを設定できます。オプションの詳細については、「でのリソース保護 AWS Shield Advanced」を参照してください。

次の図は、TCP および UDP アプリケーションの DDoS に対する耐性が高いアーキテクチャの例を示しています。



このアプローチがアプリケーションに提供するメリットには、次のものがあります。

- 最大の既知のインフラストラクチャレイヤー (レイヤー 3 およびレイヤー 4) の DDoS 攻撃に対する保護。攻撃の量によって の上流で輻輳が発生した場合 AWS、障害はソースの近くで分離され、正当なユーザーへの影響は最小限に抑えられます。
- DNS アプリケーションレイヤー攻撃に対する保護 (Route 53 は権威 DNS レスポンスを処理する責任があるため)。
- ウェブアプリケーションがある場合、このアプローチはウェブアプリケーションレイヤーのリクエストのフラッドに対する保護を提供します。 AWS WAF ウェブ ACL で設定したレートベースのルールは、ルールで許可されているよりも多くのリクエストを送信している間、ソース IPs をブロックします。
- Shield Response Team (SRT) とのプロアクティブなエンゲージメント (対象リソースのためにこのオプションを有効にした場合)。Shield Advanced がアプリケーションのヘルスに影響を与えるイベントを検出すると、SRT は、提供された連絡先情報を使用して、お客様のセキュリティチームまたはオペレーションチームとプロアクティブに対応します。

Shield Advanced と他の の組み合わせ AWS のサービス

Shield Advanced を使用すると、さまざまなシナリオでリソースを保護できます。ただし、場合によっては、他のサービスを使用するか、他のサービスと Shield Advanced を組み合わせて最高の保護を提供する必要があります。以下は、Shield Advanced または他の AWS のサービスを使用してリソースを保護する方法の例です。

目標	推奨するサービス	関連サービスドキュメント
DDoS 攻撃からウェブアプリケーションと RESTful API を保護する	Amazon CloudFront ディストリビューションと Application Load Balancer を保護する Shield Advanced	Elastic Load Balancing ドキュメント、Amazon CloudFront ドキュメント
DDoS 攻撃から TCP ベースのアプリケーションを保護する	AWS Global Accelerator 標準アクセラレーターを保護する Shield Advanced、Elastic IP アドレスにアタッチ	AWS Global Accelerator ドキュメント、Elastic Load Balancing ドキュメント
DDoS 攻撃から UDP ベースのゲームサーバーを保護する	Elastic IP アドレスにアタッチされた Amazon EC2 インスタンスを保護する Shield Advanced	Amazon Elastic Compute Cloud のドキュメント

例えば、Shield Advanced を使用して Elastic IP アドレスを保護する場合、Shield Advanced はそれに関連付けられているすべてのリソースを保護します。攻撃中、Shield Advanced はネットワーク ACLsを AWS ネットワークの境界に自動的にデプロイします。ネットワーク ACL がネットワークの境界にある場合、Shield Advanced はより大きな DDoS イベントに対する保護を提供できます。通常、ネットワーク ACL は Amazon VPC 内の Amazon EC2 インスタンスの近くで適用されます。ネットワーク ACL は、Amazon VPC とインスタンスが処理できるだけの大きさの攻撃を緩和できます。Amazon EC2 インスタンスにアタッチされたネットワークインターフェイスが最大 10 Gbps を処理できる場合、10 Gbps を超えるボリュームは遅くなり、そのインスタンスへのトラフィックがブロックされる可能性があります。攻撃を受けている最中に、Shield Advanced はネットワーク ACL を AWS 境界に昇格させ、数テラバイトのトラフィックを処理できます。ネットワーク ACL は、典型的なネットワークの容量を超えてリソースを十分に保護することができます。ネットワーク ACL の詳細については、「ネットワーク ACL」を参照してください。

セットアップ AWS Shield Advanced

このチュートリアルでは、Shield Advanced コンソール AWS Shield Advanced を使用した の開始方法について説明します。

> **Note**
>
> Shield Advanced にはサブスクリプションが必要ですが、そう AWS Shield Standard ではありません。Shield Standard で提供される保護は、すべての AWS のお客様に無料でご利用いただけます。

Shield Advanced では、ネットワークレイヤー (レイヤー 3)、トランスポートレイヤー (レイヤー 4)、およびアプリケーションレイヤー (レイヤー 7) 攻撃に対して、高度な DDoS 検出、緩和、保護が可能です。Shield Advanced の詳細については、「AWS Shield Advanced の概要」を参照してください。

AWS 技術コミュニティは、Infrastructure as Code (IaC) ツール AWS CloudFormation と Terraform を使用して Shield Advanced を設定するための自動プロセスの例を公開しました。アカウントがの組織の一部であり AWS Organizations 、Amazon Route 53 または 以外のリソースタイプを保護している場合は、このソリューション AWS Firewall Manager で を使用できます AWS Global Accelerator。このオプションの詳細については、「aws-samples / aws-shield-advanced-one-click-deployment」のコードリポジトリと「Shield Advanced のワンクリックデプロイ」のチュートリアルを参照してください。

> **Note**
>
> Distributed Denial of Service (DDoS) イベントが発生する前に Shield Advanced の設定を完了することが重要です。設定を完了すると、アプリケーションが保護され、アプリケーションが DDoS 攻撃の影響を受けた場合に対応する準備ができているようにします。

Shield Advanced の使用を開始するには、次の手順を順番に実行します。

目次

- へのサブスクライブ AWS Shield Advanced
- Shield Advanced を使用したリソース保護の追加と設定

- を使用したアプリケーションレイヤー (レイヤー 7) DDoS 保護の設定 AWS WAF
- Shield Advanced と Route 53 による保護のためのヘルスベースの検出の設定
- Shield Advanced と Amazon SNS を使用したアラームと通知の設定
- Shield Advanced で保護構成の確認および終了
- DDoS AWS イベントレスポンスの Shield Response Team (SRT) サポートの設定
- CloudWatch で DDoS ダッシュボードを作成し、CloudWatch アラームを設定する

へのサブスクライブ AWS Shield Advanced

このページでは、Shield Advanced にアカウントをサブスクライブし、サービスの使用を開始する方法について説明します。

保護 AWS アカウント する ごとに Shield Advanced をサブスクライブする必要があります。Shield Standard に登録する必要はありません。

Shield Advanced サブスクリプションの請求

AWS チャネルリセラーの場合は、アカウントチームに情報とガイダンスを求めてください。この請求情報は、 AWS チャネルリセラーではないお客様を対象としています。

他のすべてについては、次のサブスクリプションと請求のガイドラインが適用されます。

- AWS Organizations 組織のメンバーであるアカウントの場合、 は、支払者アカウント自体がサブスクライブされているかどうかにかかわらず、組織の支払者アカウントに対して Shield Advanced サブスクリプションを AWS 請求します。
- 同じ AWS Organizations 一括請求 (コンソリデーティッドビリング) アカウントファミリー に属する複数のアカウントをサブスクライブする場合、1 つのサブスクリプション料金はファミリー内のすべてのサブスクライブアカウントに対するものです。組織は、すべての AWS アカウント とそのすべてのリソースを所有している必要があります。
- 複数の組織のために複数のアカウントをサブスクライブする場合でも、すべてを所有しているのであれば、すべての組織、アカウント、リソースのサブスクリプション料金の支払いを引き続き 1 回で行うことができます。アカウントマネージャーまたは AWS サポートに連絡して、組織の 1 つを除くすべての AWS Shield Advanced サブスクリプション料金の免除をリクエストしてください。

詳細な料金情報と例については、「AWS Shield の料金表」を参照してください。

でサブスクリプションを簡素化することを検討する AWS Firewall Manager

アカウントが組織の一部である場合は、できればその組織のサブスクリプションと保護を自動化するために AWS Firewall Manager を使用することをおすすめします。Firewall Manager は、Amazon Route 53 および AWS Global Acceleratorを除くすべての保護されたリソースタイプをサポートします。Firewall Manager を使用するには、「AWS Firewall Manager」と「AWS Firewall Manager AWS Shield Advanced ポリシーの設定」を参照してください。

Firewall Manager を使用しない場合は、保護するリソースを持つアカウントごとに、次の手順を使用してサブスクライブし、保護を追加します。

アカウントを にサブスクライブするには AWS Shield Advanced

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF & Shield コンソールを開きます。
2. AWS Shield ナビゲーションバーで、[Getting started] (はじめに) を選択します。[Subscribe to Shield Advanced] (Shield Advanced をサブスクライブ) を選択します。
3. [Subscribe to Shield Advanced] (Shield Advanced をサブスクライブ) ページで、契約の各条件を読み、条件を承諾する意思を表示するために、すべてのチェックボックスを選択します。一括請求 (コンソリデーティッドビリング) ファミリーのアカウントについては、各アカウントの条件に同意する必要があります。

   > **Important**
   >
   > サブスクライブされている場合、サブスクライブを解除するには、AWS サポート に連絡する必要があります。
   > サブスクリプションの自動更新を無効にするには、Shield API オペレーション UpdateSubscription または CLI コマンド update-subscription を使用する必要があります。

   [Subscribe to Shield Advanced] (Shield Advanced をサブスクライブ) を選択します。これにより、アカウントが Shield Advanced にサブスクライブされ、サービスが有効になります。

お客様のアカウントはサブスクライブされています。次のステップを続行して、Shield Advanced でアカウントのリソースを保護します。

> **Note**
>
> サブスクライブ後、Shield Advanced はリソースを自動的に保護しません。Shield Advanced で保護するリソースを指定する必要があります。

Shield Advanced を使用したリソース保護の追加と設定

このページでは、リソースの保護を追加および設定する手順を説明します。

Shield Advanced は、Shield Advanced を通じて、または Firewall Manager Shield Advanced ポリシーで指定したリソースのみを保護します。サブスクライブアカウントのリソースは自動的に保護されません。

> **Note**
>
> 保護に Shield Advanced AWS Firewall Manager ポリシーを使用する場合は、このステップを実行する必要はありません。保護するリソースタイプを指定してポリシーを設定すると、Firewall Manager はポリシーの範囲内にあるリソースに自動的に保護を追加します。

Firewall Manager を使用しない場合は、保護するリソースを持つアカウントごとに次の手順を実行します。

Shield Advanced を使用して保護するリソースを選択するには

1. 前の手順のサブスクリプション確認ページから、または [Protected resources] (保護されたリソース) または [Overview] (概要) ページから、[Add resources to protect] (保護するリソースを追加) を選択します。
2. [Choose resources to protect with Shield Advanced] (Shield Advanced で保護するリソースの選択) ページの [Specify the Region and resource types] (リージョンとリソースタイプの指定) で、保護するリソースのリージョンとリソースタイプの仕様を指定します。[All Regions] (すべてのリージョン) を選択すると複数のリージョンのリソースを保護でき、[Global] (グローバル) を選択すると選択範囲をグローバルリソースに絞り込むことができます。保護しないリソースタイプは、すべて選択解除できます。リソースタイプの保護については、「が AWS Shield Advanced 保護するリソースのリスト」を参照してください。
3. [Load resources] (リソースをロード) を選択します。Shield Advanced は、[Select Resources] (リソースの選択) セクションに条件に一致する AWS リソースを入力します。

4. [Select Resources] (リソースの選択) セクションでは、リソースリストで検索する文字列を入力して、リソースのリストをフィルタリングできます。

   保護するリソースを選択します。

5. 作成しようとしている Shield Advanced 保護にタグを追加する場合は、[Tags] (タグ) セクションでそれらを指定します。 AWS リソースのタグ付けの詳細については、「タグエディタの使用」を参照してください。

6. [Protect with Shield Advanced] (Shield Advanced で保護) を選択します。これにより、Shield Advanced 保護がリソースに追加されます。

コンソールウィザードの画面を続行して、リソース保護の設定を完了します。

トピック

- を使用したアプリケーションレイヤー (レイヤー 7) DDoS 保護の設定 AWS WAF
- Shield Advanced と Route 53 による保護のためのヘルスベースの検出の設定
- Shield Advanced と Amazon SNS を使用したアラームと通知の設定
- Shield Advanced で保護構成の確認および終了

を使用したアプリケーションレイヤー (レイヤー 7) DDoS 保護の設定 AWS WAF

このページでは、 AWS WAF ウェブ ACLs でアプリケーションレイヤー保護を設定する手順について説明します。

アプリケーションレイヤーリソースを保護するために、Shield Advanced はレートベースのルールを持つ AWS WAF ウェブ ACL を出発点として使用します。 AWS WAF は、アプリケーションレイヤーリソースに転送される HTTP および HTTPS リクエストをモニタリングし、リクエストの特性に基づいてコンテンツへのアクセスを制御できるウェブアプリケーションファイアウォールです。レートベースのルールは、リクエスト集約条件に基づいてトラフィックの量を制限し、アプリケーションに基本的な DDoS 防御を提供します。詳細については、「の AWS WAF 仕組み」および「でのレートベースのルールステートメントの使用 AWS WAF」を参照してください。

また、オプションで Shield Advanced の自動アプリケーションレイヤーの DDoS 談話を有効にして、既知の DDoS ソースから Shield Advanced レート制限リクエストを受け取り、インシデント固有の保護を自動的に提供することもできます。

> **Important**
>
> Shield Advanced ポリシー AWS Firewall Manager を使用して を通じて Shield Advanced 保護を管理する場合、ここではアプリケーションレイヤー保護を管理することはできません。Firewall Manager Shield Advanced ポリシーで管理する必要があります。

Shield Advanced サブスクリプションと AWS WAF コスト

Shield Advanced サブスクリプションは、Shield Advanced で保護するリソースに標準 AWS WAF 機能を使用するコストをカバーします。Shield Advanced 保護の対象となる標準 AWS WAF 料金は、保護パック (ウェブ ACL) あたりのコスト、ルールあたりのコスト、ウェブリクエスト検査の 100 万リクエストあたりの基本料金、最大 1,500 WCUs、デフォルトの本文サイズです。

Shield Advanced 自動アプリケーションレイヤー DDoS 緩和を有効にすると、150 個の保護パック (ウェブ ACL) キャパシティユニット (WCU) はルールグループに追加されます。これらの WCU は、保護パック (ウェブ ACL) 内の WCU の使用量に対してカウントされます。詳細については[Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和]、[Shield Advanced ルールグループによるアプリケーションレイヤーの保護]、および[のウェブ ACL キャパシティユニット (WCUs) AWS WAF]を参照してください。

Shield Advanced へのサブスクリプションは、Shield Advanced を使用して保護しないリソース AWS WAF の の使用には適用されません。また、保護されたリソースの標準以外の追加 AWS WAF コストもカバーしません。標準以外の AWS WAF コストの例としては、Bot Control、CAPTCHA ルールアクション、1,500 WCUs を超えるウェブ ACLs、およびデフォルトの本文サイズを超えるリクエスト本文の検査などがあります。完全なリストは AWS WAF 料金ページに記載されています。Shield Advanced へのサブスクリプションには、 Layer 7 Anti-DDoS Amazon Managed Rule グループへのアクセスが含まれます。サブスクリプションの一環として、Shield Advanced で保護された AWS WAF リソースに対するリクエストは 1 か月あたり最大 500 億件になります。500 億を超えるリクエストは、 AWS Shield Advanced 料金表ページに従って請求されます。

詳細情報および料金の例については、「[Shield の料金]」および「[AWS WAF の料金]」を参照してください。

リージョン用にレイヤー 7 DDoS 保護を設定するには

Shield Advanced では、選択したリソースが配置されている各リージョンについて、レイヤー 7 DDoS 緩和策を設定するオプションを使用できます。複数のリージョンに保護を追加する場合、ウィザードはリージョンごとに次の手順を説明します。

1. [Configure layer 7 DDoS protections] (レイヤー 7 DDoS 保護の設定) ページには、ウェブ ACL にまだ関連付けられていない各リソースが一覧表示されます。これらのそれぞれについて、既存のウェブ ACL を選択するか、新しいウェブ ACL を作成します。ウェブ ACL が既に関連付けられているリソースについては、まず現在のウェブ ACL の関連付けを解除することでウェブ ACLs を変更できます AWS WAF。詳細については、「AWS リソースとの保護の関連付けまたは関連付け解除」を参照してください。

   レートベースのルールがまだないウェブ ACL の場合、設定ウィザードでルールを追加するよう求められます。レートベースのルールは、大量のリクエストを送信している IP アドレスからのトラフィックを制限します。レートベースのルールは、ウェブリクエストのフラッドからアプリケーションを保護するのに役立つとともに、DDoS 攻撃の可能性を示していることがあるトラフィックの急増についてアラートを出すことができます。[Add rate limit rule] (レート制限ルールを追加) を選択し、レート制限とルールアクションを指定して、レートベースのルールをウェブ ACL に追加します。を介してウェブ ACL で追加の保護を設定できます AWS WAF。

   レートベースのルールの追加設定オプションを含む、Shield Advanced 保護でのウェブ ACL およびレートベースのルールの使用方法については、「AWS WAF ウェブ ACLs と Shield Advanced によるアプリケーションレイヤーの保護」を参照してください。

2. 自動アプリケーションレイヤー DDoS 緩和では、Shield Advanced がアプリケーションレイヤーリソースに対する DDoS 攻撃を自動的に軽減する場合は、有効化を選択し、Shield Advanced がカスタム AWS WAF ルールで使用するルールアクションを選択します。この設定は、このウィザードセッションで管理しているリソースのすべてのウェブ ACL に適用されます。

   アプリケーションレイヤー DDoS 自動緩和により、Shield Advanced は、既知の DDoS ソースからのリクエストの量を制限するレートベースのルールをリソースの AWS WAF ウェブ ACL に維持します。さらに、Shield Advanced は、現在のトラフィックパターンと過去のトラフィックベースラインを比較して、DDoS 攻撃を示している可能性のある逸脱を検出します。Shield Advanced が DDoS 攻撃を検出すると、応答するカスタム AWS WAF ルールを作成、評価、デプロイして応答します。カスタムルールが、ユーザーに代わって攻撃に対してカウントまたはブロックするかどうかを指定します。

   > **Note**
   >
   > 自動アプリケーションレイヤー DDoS 緩和は、最新バージョンの (v2) を使用して作成された保護パック AWS WAF (ウェブ ACLs) でのみ機能します。

この機能を使用するための注意点やベストプラクティスなど、Shield Advanced 自動アプリケーションレイヤー DDoS 緩和の詳細については、Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和 を参照してください。

3. [次へ] を選択します。コンソールウィザードは、ヘルスベースの検出のページに進みます。

Shield Advanced と Route 53 による保護のためのヘルスベースの検出の設定

このページでは、ヘルスベースの検出を使用するように Shield Advanced を設定する手順を説明します。これにより、攻撃の検出と緩和における応答性と精度を向上させることができます。

イベントを正確に検出するには、適切に設定されたヘルスチェックが不可欠です。Route 53 ホストゾーンを除くリソースタイプのために、ヘルスベースの検出を設定できます。

ヘルスベースの検出を使用するには、まず Route 53 でリソースのヘルスチェックを定義してから、ヘルスチェックを Shield Advanced の保護に関連する必要があります。設定するヘルスチェックがリソースの正常性を正確に反映していることが重要です。Shield Advanced で使用するヘルスチェックの設定に関する情報と例については、「Shield Advanced と Route 53 を使用したヘルスチェックを使用したヘルスベースの検出」を参照してください。

Shield Response Team (SRT) のプロアクティブなエンゲージメントサポートには、ヘルスチェックが必要です。プロアクティブなエンゲージメントの詳細については、「SRT が直接連絡するためのプロアクティブエンゲージメントの設定」を参照してください。

> **Note**
>
> ヘルスチェックを Shield Advanced 保護に関連付ける場合、正常であることが報告されている必要があります。

ヘルスベースの検出を設定するには

1. [Associated Health Check] (ヘルスチェックを関連付ける) で、保護に関連付けるヘルスチェックの ID を選択します。

> **Note**
>
> 必要なヘルスチェックが表示されない場合は、Route 53 コンソールに移動して、ヘルスチェックとその ID を検証します。詳細については、「ヘルスチェックの作成と更新」を参照してください。

2. [Next] (次へ) を選択します。コンソールウィザードは、アラームと通知のページに進みます。

Shield Advanced と Amazon SNS を使用したアラームと通知の設定

このページでは、必要に応じて、検出された Amazon CloudWatch アラームとレートベースのルールアクティビティに対する Amazon Simple Notification Service 通知の設定について説明します。これらを使用すると、Shield が保護対象リソースでイベントを検出したとき、またはレートベースのルールで設定されたレート制限を超えたときに通知を受け取ることができます。

Shield Advanced CloudWatch のメトリクスについては、「AWS Shield Advanced メトリクス」を参照してください。Amazon SNS の詳細については、「Amazon Simple Notification Service デベロッパーガイド」を参照してください。

アラームと通知を設定するには

1. 通知の対象となる Amazon SNS トピックを選択します。すべての保護されたリソースとレートベースのルールに単一の Amazon SNSトピックを使用することも、組織に合わせてカスタマイズされた異なるトピックを選択することもできます。例えば、特定のリソースセットのインシデント対応を担当するチームごとに SNS トピックを作成できます。
2. [次へ] を選択します。コンソールウィザードは、リソース保護の確認ページに進みます。

Shield Advanced で保護構成の確認および終了

設定を確認および終了するには

1. [Review and configure DDoS mitigation and visibility] (DDoS の緩和と可視性を確認および設定) ページで、設定を確認します。変更するには、変更する部分で [Edit] (編集) を選択します。これにより、コンソールウィザードの関連するページに戻ります。変更を加えた後、[Review and configure DDoS mitigation and visibility] (DDoS の緩和と可視性を確認および設定) ページに戻るまで、後続のページで [Next] (次へ) を選択します。

2. [Finish configuration] (設定を終了) を選択します。[Protected resources] (保護されたリソース) ページには、新しく保護されたリソースが一覧表示されます。

DDoS AWS イベントレスポンスの Shield Response Team (SRT) サポートの設定

このページでは、Shield Response Team (SRT) サポートを設定する手順について説明します。

SRT は DDoS イベントへの対応を専門とするセキュリティエンジニアの集団です。必要に応じて、DDoS イベント中に SRT がユーザーに代わってリソースを管理できるようにするアクセス許可を追加できます。さらに、保護対象リソースに関連する Route 53 ヘルスチェックが検出されたイベント中に異常が発生した場合に、事前に対処するように SRT を設定できます。この両方の保護機能を追加することで、DDoS イベントへの迅速な対応が可能になります。

> **Note**
>
> Shield Response Team (SRT) のサービスを使用するには、ビジネスサポートプランまたはエンタープライズサポートプランをサブスクライブする必要があります。

SRT は、アプリケーションレイヤーイベント中に AWS WAF リクエストデータとログをモニタリングして、異常なトラフィックを特定できます。これらは、問題のあるトラフィックソースを軽減するためのカスタム AWS WAF ルールの作成に役立ちます。必要に応じて、SRT は、リソースをレコメンデーションとより適切に一致させるために、アーキテクチャに関するレコメンデ AWS ーションを作成する場合があります。

SRT 関数の詳細については、「Shield Response Team (SRT) サポートによるマネージド DDoS イベントレスポンス」を参照してください。

SRT にアクセス許可を付与するには

1. AWS Shield コンソールの概要ページの「SRT サポートの設定 AWS 」で、「SRT アクセスの編集」を選択します。Edit AWS Shield Response Team (SRT) アクセスページが開きます。
2. SRT アクセス設定には、次のいずれかのオプションを選択します。
   - アカウントへのアクセス権を SRT に付与しない – Shield は、アカウントとリソースにアクセスするために以前に SRT に付与したすべての許可を削除します。

- [Create a new role for the SRT to access my account] (SRT が自分のアカウントにアクセスするための新しいロールを作成する) — Shield は、SRT を表すサービスプリンシパル `drt.shield.amazonaws.com` を信頼するロールを作成し、マネージドポリシー `AWSShieldDRTAccessPolicy` をそれにアタッチします。管理ポリシーは、SRT がユーザーに代わって および AWS WAF API コールを行い AWS Shield Advanced 、ログにアクセスすることを許可します AWS WAF 。管理ポリシーの詳細については、「AWS マネージドポリシー: AWSShieldDRTAccessPolicy」を参照してください。
- SRT がアカウントにアクセスするための既存のロールを選択する – このオプションでは、AWS Identity and Access Management 次のように (IAM) でロールの設定を変更する必要があります。
  - マネージドポリシー `AWSShieldDRTAccessPolicy` をロールにアタッチします。この管理ポリシーにより、SRT はユーザーに代わって および AWS WAF API コールを行い AWS Shield Advanced 、ログにアクセスできるようになります AWS WAF 。管理ポリシーの詳細については、「AWS マネージドポリシー: AWSShieldDRTAccessPolicy」を参照してください。マネージドポリシーをロールにアタッチする方法については、「Attaching and Detaching IAM Policies」(IAM ポリシーのアタッチとデタッチ) を参照してください。
  - サービスプリンシパル `drt.shield.amazonaws.com` を信頼するようにロールを変更します。これは、SRT を表すサービスプリンシパルです。詳細については、「IAM JSON ポリシーエレメント: プリンシパル」を参照してください。

3. [保存] を選択して変更を保存します。

SRT に保護とデータへのアクセスを許可する方法の詳細については、「SRT へのアクセスの許可」を参照してください。

SRT のプロアクティブな関与を有効にするには

1. AWS Shield コンソールの概要ページの「プロアクティブエンゲージメントとコンタクト」の「コンタクトエリア」で、「編集」を選択します。

   [Edit contacts] (連絡先を編集) ページで、SRT がプロアクティブな関与のために連絡する担当者の連絡先情報を入力します。

   複数の連絡先を提供する場合は、[Notes] (備考) に、各連絡先を使用する必要がある状況を記載してください。プライマリおよびセカンダリの連絡先指定を含めて、各連絡先の空き時間およびタイムゾーンを指定します。

   問い合わせメモの例:

- これは、24 時間年中無休でスタッフが対応するホットラインです。応答するアナリストにご協力ください。この担当者は、適切な担当者を呼び出します。
- 5 分以内にホットラインが応答しない場合は、私までお問い合わせください。

2. [Save] (保存) を選択します。

   [Overview] (概要) ページには、更新された連絡先情報が反映されます。

3. [Edit proactive engagement feature] (プロアクティブな関与機能を編集) を選択し、[Enable] (有効化) を選択してから、[Save] (保存) を選択してプロアクティブな関与を有効にします。

プロアクティブな関与の詳細については、「SRT が直接連絡するためのプロアクティブエンゲージメントの設定」を参照してください。

CloudWatch で DDoS ダッシュボードを作成し、CloudWatch アラームを設定する

このページでは、CloudWatch で DDoS ダッシュボードを作成し、CloudWatch アラームの設定について説明します。

Amazon CloudWatch を使用して潜在的な DDoS アクティビティをモニタリングすることで、Shield Advanced から未加工データを収集し、リアルタイムに近い読み取り可能なメトリクスとして加工できます。CloudWatch の統計を使用して、ウェブアプリケーションやサービスの動作状況を把握できます。CloudWatch の詳細については、「Amazon CloudWatch ユーザーガイド」の「What is CloudWatch」(CloudWatch とは) を参照してください。

- CloudWatch ダッシュボードを作成する手順については、「Amazon CloudWatch によるモニタリング」を参照してください。
- ダッシュボードに追加できる Shield Advanced メトリクスの説明については、「AWS Shield Advanced メトリクス」を参照してください。

Shield Advanced は、リソースメトリクスを、進行中のイベントがないときと比較して、DDoS イベント中により頻繁に CloudWatch にレポートします。Shield Advanced は、イベント中は 1 分ごとに、およびイベント終了直後に 1 回、メトリクスをレポートします。イベントが発生していない間、Shield Advanced は 1 日に 1 回、リソースに割り当てられた時間にメトリクスを報告します。この定期的なレポートにより、メトリクスをアクティブに保ち、ユーザーのカスタム CloudWatch アラームで使用できるようにします。

これで、Shield Advanced の開始方法のチュートリアルは完了です。選択した保護機能を最大限に活用するには、Shield Advanced の機能とオプションの検索を続けてください。まず、Shield Advanced による DDoS イベントの可視性 および での DDoS イベントへの対応 AWS でイベントを表示して対応するためのオプションをよく理解してください。

Shield Response Team (SRT) サポートによるマネージド DDoS イベントレスポンス

このページでは、Shield Response Team (SRT) の機能について説明します。

SRT は、Shield Advanced のお客様に追加のサポートを提供します。SRT は DDoS イベントへの対応を専門とするセキュリティエンジニアの集団です。 AWS サポート プランに対するサポートの追加レイヤーとして、SRT と直接やり取りして、イベント対応ワークフローの一環として SRT の専門知識を活用できます。オプションの詳細および設定ガイダンスについては、次のトピックを参照してください。

> **Note**
>
> - Shield Response Team (SRT) のサービスを使用するには、ビジネスサポートプランまたはエンタープライズサポートプランをサブスクライブする必要があります。
> - Shield Response Team (SRT) は、Shield Advanced が利用可能なリージョン、および GovCloud リージョン、 AWS GovCloud (米国東部) 、 AWS GovCloud (米国西部) のお客様にサービスを提供しています。

SRT のサポートアクティビティ

SRT との連携の主な目標は、アプリケーションの可用性とパフォーマンスを保護することです。DDoS イベントのタイプとアプリケーションのアーキテクチャに応じて、SRT は次のいずれかまたは複数のアクションを実行することがあります。

- AWS WAF ログ分析とルール – AWS WAF ウェブ ACL を使用するリソースの場合、SRT は AWS WAF ログを分析してアプリケーションウェブリクエストの攻撃特性を特定できます。エンゲージメント中に承認を得た場合、SRT はウェブ ACL に変更を適用して、特定した攻撃をブロックできます。
- カスタムネットワーク緩和策の構築 – SRT は、インフラストラクチャレイヤーの攻撃に対して、お客様のためにカスタム緩和策を作成できます。SRT はユーザーと連携して、アプリケーション

について想定されるトラフィックを理解し、予期しないトラフィックをブロックし、パケット/秒のレート制限を最適化できます。詳細については、「SRT による DDoS 攻撃に対するカスタム緩和策の設定」を参照してください。

- ネットワークトラフィックエンジニアリング – SRT は AWS ネットワークチームと密接に連携して Shield Advanced のお客様を保護します。必要に応じて、インターネットトラフィックが AWS ネットワークに到達する方法 AWS を変更して、アプリケーションにより多くの緩和キャパシティを割り当てることができます。
- アーキテクチャの推奨事項 – SRT は、攻撃の最善の緩和策として、 AWS ベストプラクティスにより合致するアーキテクチャの変更が必要であると判断し、これらのプラクティスの実装をサポートします。詳細については、「DDoS 耐性向上のためのAWS のベストプラクティス」を参照してください。

以下のセクションでは、SRT を利用する手順について説明します。

トピック

- SRT へのアクセスの許可
- SRT が直接連絡するためのプロアクティブエンゲージメントの設定
- 疑わしい DDoS イベントに関する SRT への問い合わせ
- SRT による DDoS 攻撃に対するカスタム緩和策の設定

SRT へのアクセスの許可

このページでは、SRT が AWS WAF ログにアクセスし、 AWS Shield Advanced および AWS WAF APIs を呼び出して保護を管理できるように、ユーザーに代わって動作するアクセス許可を SRT に付与する手順を示します。

アプリケーションレイヤー DDoS イベント中、SRT は AWS WAF リクエストをモニタリングして異常なトラフィックを特定し、問題のあるトラフィックソースを軽減するためのカスタム AWS WAF ルールを作成できます。

さらに、Application Load Balancer、Amazon CloudFront、またはサードパーティーのソースからのパケットキャプチャや口グなど、Amazon S3 バケットに保存されている他のデータへのアクセス権を SRT に付与することもできます。

> **Note**
>
> Shield Response Team (SRT) のサービスを使用するには、ビジネスサポートプランまたはエンタープライズサポートプランをサブスクライブする必要があります。

SRT の許可を管理するには

1. AWS Shield コンソールの概要ページの「SRT サポートの設定 AWS 」で、「SRT アクセスの編集」を選択します。Edit AWS Shield Response Team (SRT) アクセスページが開きます。
2. SRT アクセス設定には、次のいずれかのオプションを選択します。

   - アカウントへのアクセス権を SRT に付与しない – Shield は、アカウントとリソースにアクセスするために以前に SRT に付与したすべての許可を削除します。
   - [Create a new role for the SRT to access my account] (SRT が自分のアカウントにアクセスするための新しいロールを作成する) — Shield は、SRT を表すサービスプリンシパル `drt.shield.amazonaws.com` を信頼するロールを作成し、マネージドポリシー `AWSShieldDRTAccessPolicy` をそれにアタッチします。管理ポリシーは、SRT がユーザーに代わって および AWS WAF API コールを行い AWS Shield Advanced 、ログにアクセスすることを許可します AWS WAF 。管理ポリシーの詳細については、「AWS マネージドポリシー: AWSShieldDRTAccessPolicy」を参照してください。
   - SRT がアカウントにアクセスするための既存のロールを選択する – このオプションでは、AWS Identity and Access Management 次のように (IAM) でロールの設定を変更する必要があります。
     - マネージドポリシー `AWSShieldDRTAccessPolicy` をロールにアタッチします。この管理ポリシーにより、SRT はユーザーに代わって および AWS WAF API コールを行い AWS Shield Advanced 、ログにアクセスできるようになります AWS WAF 。管理ポリシーの詳細については、「AWS マネージドポリシー: AWSShieldDRTAccessPolicy」を参照してください。マネージドポリシーをロールにアタッチする方法については、「Attaching and Detaching IAM Policies」(IAM ポリシーのアタッチとデタッチ) を参照してください。
     - サービスプリンシパル `drt.shield.amazonaws.com` を信頼するようにロールを変更します。これは、SRT を表すサービスプリンシパルです。詳細については、「IAM JSON ポリシーエレメント: プリンシパル」を参照してください。
3. (オプション): Amazon S3 バケットへの SRT アクセスを付与します。 AWS WAF ウェブ ACL ログにないデータを共有する必要がある場合は、これを設定します。Application Load Balancer

アクセスログ、Amazon CloudFront ログ、またはサードパーティーのソースからのログはその一例です。

> **Note**
>
> AWS WAF ウェブ ACL ログに対してこれを行う必要はありません。SRT は、アカウントへのアクセス権が付与されると、それらにアクセスできるようになります。

a. 次のガイドラインに従って Amazon S3 バケットを設定します。

- バケットの場所は、前のステップの AWS Shield Response Team (SRT) アクセスで SRT に一般アクセス権を付与したもの AWS アカウント と同じ にある必要があります。
- バケットは、プレーンテキストまたは SSE-S3 暗号化のいずれかです。Amazon S3 SSE-S3 暗号化の詳細については、「Amazon S3 ユーザーガイド」の「Amazon S3 が管理する暗号化キーによるサーバー側の暗号化 (SSE-S3) を使用したデータの保護」を参照してください。

  SRT は、 AWS Key Management Service () に保存されているキーで暗号化されたバケットに保存されているログを表示または処理することはできませんAWS KMS。

b. Shield Advanced の [(Optional): Grant SRT access to an Amazon S3 bucket] ((オプション): Amazon S3 バケットへのアクセス権を SRT に付与) セクションで、データまたはログが保存されている各 Amazon S3 バケットについてバケットの名前を入力し、[Add Bucket] (バケットを追加) を選択します。バケットは最大 10 個まで追加できます。

これにより、SRT に各バケットに対する次の `s3:GetBucketLocation`、`s3:GetObject`、および `s3:ListBucket` 許可が付与されます。

10 個を超えるバケットにアクセスする許可を SRT に付与する場合は、追加のバケットポリシーを編集し、SRT についてここにリストされている許可を手動で付与することで、これを実行できます。

ポリシーリストの例を以下に示します。

```
{
    "Sid": "AWSDDoSResponseTeamAccessS3Bucket",
    "Effect": "Allow",
    "Principal": {
```

```
            "Service": "drt.shield.amazonaws.com"
        },
        "Action": [
            "s3:GetBucketLocation",
            "s3:GetObject",
            "s3:ListBucket"
        ],
        "Resource": [
            "arn:aws:s3:::bucket-name",
            "arn:aws:s3:::bucket-name/*"
        ]
}
```

4. [保存] を選択して変更を保存します。

また、IAM ロールを作成してポリシー AWSShieldDRTAccessPolicy をアタッチしてから、そのロールをオペレーション AssociateDRTRole に渡すことで、API を通じて SRT を承認することもできます。

SRT が直接連絡するためのプロアクティブエンゲージメントの設定

このページでは、SRT とのプロアクティブエンゲージメントを設定する手順について説明します。

プロアクティブなエンゲージメントにより、攻撃の可能性があるためにアプリケーションの可用性またはパフォーマンスが影響を受ける場合は、SRT から直接連絡します。このエンゲージメントモデルでは、SRT による最も迅速な対応が提供され、SRT がお客様と連絡を取り合う前であってもトラブルシューティングを開始できるため、推奨されています。

プロアクティブエンゲージメントは、Elastic IP アドレスと AWS Global Accelerator 標準アクセラレーターでのネットワークレイヤーイベントとトランスポートレイヤーイベント、および Amazon CloudFront ディストリビューションと Application Load Balancer でのウェブリクエストフラッドに使用できます。プロアクティブエンゲージメントは、Amazon Route 53 ヘルスチェックが関連付けられている Shield Advanced リソース保護でのみ利用できます。ヘルスチェックの管理と使用の詳細については、「Shield Advanced と Route 53 を使用したヘルスチェックを使用したヘルスベースの検出」を参照してください。

Shield Advanced によって検出されたイベント中、SRT はヘルスチェックの状態を使用して、イベントがプロアクティブなエンゲージメントの対象となるかどうかを判断します。その場合は、プロアクティブな関与の設定で提供された連絡ガイダンスに従って、SRT から連絡が送られます。

プロアクティブな関与のために最大 10 件の連絡先を設定でき、SRT がお客様に連絡する際に参考となるメモを入力できます。イベント中、お客様側のプロアクティブな関与の連絡先は、SRT と対話が可能な状態になっている必要があります。24 時間年中無休のオペレーションセンターがない場合は、ポケットベルの連絡先を提供し、連絡先メモにこの連絡先設定を記載できます。

プロアクティブなエンゲージメントのために、次を実行する必要があります。

- ビジネスサポートプランまたはエンタープライズサポートプランに加入している必要があります。
- Amazon Route 53 ヘルスチェックは、プロアクティブなエンゲージメントで保護するリソースに関連付ける必要があります。SRT は、イベントにプロアクティブなエンゲージメントが必要かどうかを判断するのをサポートするために、ヘルスチェックのステータスを使用します。したがって、ヘルスチェックが保護されたリソースの状態を正確に反映していることが重要です。詳細とガイダンスについては、「Shield Advanced と Route 53 を使用したヘルスチェックを使用したヘルスベースの検出」を参照してください。
- AWS WAF ウェブ ACL が関連付けられているリソースの場合、最新バージョンの AWS WAF (v2) を使用してウェブ ACL を作成する必要があります AWS WAF。
- イベント中、プロアクティブなエンゲージメントのために、SRT による使用を目的として、少なくとも 1 名の連絡先を提供する必要があります。連絡先情報を完全かつ最新の状態に保ちます。

SRT のプロアクティブな関与を有効にするには

1. AWS Shield コンソールの概要ページの「プロアクティブエンゲージメントと問い合わせ」の「問い合わせエリア」で、「編集」を選択します。

   [Edit contacts] (連絡先を編集) ページで、SRT がプロアクティブな関与のために連絡する担当者の連絡先情報を入力します。

   複数の連絡先を提供する場合は、[Notes] (備考) に、各連絡先を使用する必要がある状況を記載してください。プライマリおよびセカンダリの連絡先指定を含めて、各連絡先の空き時間およびタイムゾーンを指定します。

   問い合わせメモの例:

   - これは、24 時間年中無休でスタッフが対応するホットラインです。応答するアナリストにご協力ください。この担当者は、適切な担当者を呼び出します。
   - 5 分以内にホットラインが応答しない場合は、私までお問い合わせください。
2. [Save] (保存) を選択します。

[Overview] (概要) ページには、更新された連絡先情報が反映されます。

3. [Edit proactive engagement feature] (プロアクティブな関与機能を編集) を選択し、[Enable] (有効化) を選択してから、[Save] (保存) を選択してプロアクティブな関与を有効にします。

疑わしい DDoS イベントに関する SRT への問い合わせ

次のいずれかの方法で SRT に連絡できます。

サポートケース

[AWS サポートセンター] コンソールの [AWS Shield] でケースを開くことができます。

サポートケースの作成に関するガイダンスについては、「AWS サポート センター」を参照してください。

状況に適した重要度を選択し、連絡先の詳細を入力します。説明では、可能な限り詳細に入力します。影響を受ける可能性があると思われる保護されたリソースと、エンドユーザーエクスペリエンスの現在の状態に関する情報を入力してください。例えば、ユーザーエクスペリエンスが低下したり、アプリケーションの一部が現在利用できない場合は、その情報を提供してください。

- DDoS 攻撃が疑われる状況 –アプリケーションの可用性またはパフォーマンスが DDoS 攻撃の可能性がある現象によって現在影響を受けている場合は、次の重要度と連絡先のオプションを選択します。
  - 重要度については、サポートプランで使用可能な最も高い重要度を選択します。
    - ビジネスサポートの場合、これは [Production system down: < 1 hour] (本番稼働用システムのダウン: 1 時間未満) です。
    - エンタープライズサポートの場合、これは [Business-critical system down: < 15 minutes] (ビジネスクリティカルなシステムのダウン: 15 分未満) です。
  - 連絡先オプションについては、[Phone] (電話) または [Chat] (チャット) のいずれかを選択し、詳細を入力してください。ライブのお問い合わせ方法を使用すると、最速で応答が得られます。

プロアクティブな関与

AWS Shield Advanced プロアクティブエンゲージメントでは、検出されたイベント中に保護されたリソースに関連付けられた Amazon Route 53 ヘルスチェックが異常になった場合、SRT から直接連絡されます。このオプションの詳細については、「SRT が直接連絡するためのプロアクティブエンゲージメントの設定」を参照してください。

SRT による DDoS 攻撃に対するカスタム緩和策の設定

このページでは、SRT を使用して DDoS 攻撃に対するカスタム緩和策を構築する手順を示します。

Elastic IPs (EIPs) と AWS Global Accelerator 標準アクセラレーターについては、SRT を使用してカスタム緩和策を設定できます。これは、緩和の導入時に適用すべき特定のロジックがわかっている場合に便利です。例えば、特定の国からのトラフィックのみを許可する、特定のレート制限を適用する、オプションの検証を設定する、フラグメントを許可しない、パケットペイロードの特定のパターンに一致するトラフィックのみを許可する、などの設定が可能です。

一般的なカスタム緩和の例には、次のようなものがあります。

- パターンが一致 - クライアントサイドアプリケーションとやり取りするサービスを運用する場合、それらのアプリケーションに固有の既知のパターンを照合するように選択できます。例えば、お客様が配布する特定のソフトウェアをエンドユーザーがインストールする必要があるゲームまたは通信サービスを運用する場合があります。アプリケーションがサービスに送信するすべてのパケットにマジックナンバーを含めることができます。フラグメント化されていない TCP または UDP パケットペイロードおよびヘッダーを最大 128 バイト (個別または連続) まで照合できます。一致は、パケットペイロードの先頭からの特定のオフセット、または既知の値に続くダイナミックオフセットとして 16 進表記で表すことができます。たとえば、緩和はバイト `0x01` を探すことができ、次の 4 バイトとして `0x12345678` が予測されます。
- DNS 固有 — グローバルアクセラレータや Amazon Elastic Compute Cloud (Amazon EC2) などのサービスを使用して独自の権威ある DNS サービスを運用する場合、パケットが有効な DNS クエリであることを確認し、DNS トラフィックに固有の特定の属性を評価する疑惑スコアリングを適用するパケットを検証するカスタム緩和をリクエストできます。

SRT でのカスタム緩和策の構築に関する問い合わせは、 AWS Shieldでサポートケースを作成します。 AWS サポート ケースの作成の詳細については、「 の開始方法 AWS サポート」を参照してください。

でのリソース保護 AWS Shield Advanced

リソース AWS Shield Advanced の保護を追加および設定できます。1 つのリソースのための保護を管理でき、保護されたリソースを論理コレクションにグループ化して、イベント管理を改善できます。を使用して Shield Advanced 保護の変更を追跡することもできます AWS Config。

> **Note**
>
> Shield Advanced は、Shield Advanced または Shield Advanced AWS Firewall Manager ポリシーを通じて指定したリソースのみを保護します。リソースは自動的に保護されません。

AWS Firewall Manager Shield Advanced ポリシーを使用している場合は、ポリシーの範囲内にあるリソースの保護を管理する必要はありません。Firewall Manager は、ポリシーの設定に従って、ポリシーの範囲内にあるアカウントおよびリソースの保護を自動的に管理します。詳細については、「Firewall Manager での AWS Shield Advanced ポリシーの使用」を参照してください。

トピック

- が AWS Shield Advanced 保護するリソースのリスト
- Shield Advanced を使用した Amazon EC2 インスタンスおよび Network Load Balancer の保護
- AWS Shield Advanced および を使用したアプリケーションレイヤー (レイヤー 7) の保護 AWS WAF
- Shield Advanced と Route 53 を使用したヘルスチェックを使用したヘルスベースの検出
- AWS リソースへの AWS Shield Advanced 保護の追加
- AWS Shield Advanced 保護の編集
- Shield Advanced で保護されたリソースのアラームと通知の作成
- AWS リソースからの AWS Shield Advanced 保護の削除
- AWS Shield Advanced 保護のグループ化
- での Shield Advanced リソース保護の変更の追跡 AWS Config

が AWS Shield Advanced 保護するリソースのリスト

このセクションは、各リソースタイプの Shield Advanced 保護に関する情報を提供します。

Shield Advanced は、ネットワークレイヤーとトランスポートレイヤー (レイヤー 3 と 4) とアプリケーションレイヤー (レイヤー 7) の AWS リソースを保護します。一部のリソースを直接保護し、他のリソースを保護されたリソースとの関連付けを通じて保護することができます。Shield Advanced は IPv4 をサポートしていますが、IPv6 はサポートしていません。

> **Note**
>
> Shield Advanced は、Shield Advanced で、または AWS Firewall Manager Shield Advanced ポリシーを通じて指定したリソースのみを保護します。リソースは自動的に保護されません。

Shield Advanced を使用すると、次のリソースタイプで高度なモニタリングと保護を行うことができます。

- Amazon CloudFront ディストリビューション。CloudFront の継続的デプロイでは、Shield Advanced は保護対象のプライマリディストリビューションに関連付けられているすべてのステージングディストリビューションを保護します。
- Amazon Route 53 ホストゾーン。
- AWS Global Accelerator 標準アクセラレーター。
- Amazon EC2 Elastic IP アドレス。Shield Advanced は、保護された Elastic IP アドレスに関連付けられているリソースを保護します。
- Amazon EC2 インスタンス (Amazon EC2 Elastic IP アドレスへの関連付け経由)
- 次の Elastic Load Balancing (ELB) ロードバランサー:
  - Application Load Balancer。
  - Classic Load Balancer。
  - Network Load Balancer (Amazon EC2 Elastic IP アドレスへの関連付け経由)。

> **Note**
>
> Shield Advanced を使用して他のリソースタイプを保護することはできません。例えば、AWS Global Accelerator カスタムルーティングアクセラレータや Gateway Load Balancer を保護することはできません。

> **Note**
>
> NAT ゲートウェイはアウトバウンドトラフィックのみを処理しますが、Shield Advanced はインバウンド DDoS から保護します。アウトバウンドトラフィックの保護には、 を使用しますAWS Network Firewall。

AWS アカウントあたり各リソースタイプについて最大 1,000 のリソースをモニタリングおよび保護できます。例えば、1 つのアカウントで、1,000 の Amazon EC2 Elastic IP アドレス、1,000 の CloudFront ディストリビューション、および 1,000 の Application Load Balancer を保護できます。https://console.aws.amazon.com/servicequotas/ の Service Quotas コンソールで、Shield Advanced で保護できるリソースの数の増加をリクエストできます。

Shield Advanced を使用した Amazon EC2 インスタンスおよび Network Load Balancer の保護

このページでは、Amazon EC2 インスタンスと Network Load Balancer AWS Shield Advanced の保護を使用する方法について説明します。

Amazon EC2 インスタンスおよび Network Load Balancer を保護するには、まずこれらのリソースを Elastic IP アドレスにアタッチし、次に Shield Advanced で Elastic IP アドレスを保護します。

Elastic IP アドレスを保護すると、Shield Advanced は、それらがアタッチされているリソースを識別して保護します。Shield Advanced は、Elastic IP アドレスにアタッチされているリソースのタイプを自動的に識別し、そのリソースのために適切な検出および緩和策を適用します。これには、その Elastic IP アドレスに固有のネットワーク ACL を設定することが含まれます。 AWS リソースでの Elastic IP アドレスの使用の詳細については、Amazon Elastic Compute Cloud のドキュメントまたは Elastic Load Balancing のドキュメントのガイドを参照してください。

攻撃中、Shield Advanced はネットワーク ACLsを AWS ネットワークの境界に自動的にデプロイします。ネットワーク ACL がネットワークの境界にある場合、Shield Advanced はより大きな DDoS イベントに対する保護を提供できます。通常、ネットワーク ACL は Amazon VPC 内の Amazon EC2 インスタンスの近くで適用されます。ネットワーク ACL は、Amazon VPC とインスタンスが処理できるだけの大きさの攻撃を緩和できます。例えば、Amazon EC2 インスタンスに接続されたネットワークインターフェイスが最大 10 Gbps を処理できる場合、10 Gbps を超えるボリュームは遅くなり、そのインスタンスへのトラフィックをブロックする可能性があります。攻撃を受けている最中に、Shield Advanced はネットワーク ACL を AWS 境界に昇格させ、数テラバイトのトラフィックを処理できます。ネットワーク ACL は、典型的なネットワークの容量を超えてリソースを

十分に保護することができます。ネットワーク ACL の詳細については、「ネットワーク ACL」を参照してください。

などの一部のスケーリングツールでは AWS Elastic Beanstalk、Network Load Balancer に Elastic IP アドレスを自動的にアタッチすることはできません。このような場合、Elastic IP アドレスを手動でアタッチする必要があります。

AWS Shield Advanced および を使用したアプリケーションレイヤー (レイヤー 7) の保護 AWS WAF

このページでは、Shield Advanced と AWS WAF が連携してアプリケーションレイヤー (レイヤー 7) のリソースを保護する方法について説明します。

Shield Advanced を使用してアプリケーションレイヤーのリソースを保護するには、まず AWS WAF ウェブ ACL をリソースに関連付けて、それに 1 つ以上のレートベースのルールを追加します。さらに、アプリケーションレイヤー DDoS 自動緩和を有効にすることもできます。これにより、DDoS 攻撃への対応として、Shield Advanced がユーザーのために自動的にウェブ ACL ルールを作成および管理するようになります。

Shield Advanced を使用してアプリケーションレイヤーリソースを保護する場合、Shield Advanced は、トラフィックを時間の経過に合わせて分析し、ベースラインを確立して維持します。Shield Advanced は、DDoS 攻撃を示している可能性のあるトラフィックパターンの異常を検出するために、これらのベースラインを使用します。Shield Advanced が攻撃を検出するポイントは、Shield Advanced が攻撃前にモニタリングできる状態になっていたトラフィックと、ウェブアプリケーションで使用するアーキテクチャによって異なります。Shield Advanced の動作に影響を与える可能性があるアーキテクチャのバリエーションには、使用するインスタンスのタイプ、インスタンスのサイズ、該当するインスタンスのタイプが拡張ネットワーキングをサポートするかどうかなどがあります。Shield Advanced を設定して、アプリケーションレイヤー攻撃に対して自動的に緩和策を実施することもできます。

Shield Advanced サブスクリプションと AWS WAF コスト

Shield Advanced サブスクリプションは、Shield Advanced で保護するリソースの標準 AWS WAF 機能を使用するコストをカバーします。Shield Advanced 保護の対象となる標準 AWS WAF 料金は、保護パック (ウェブ ACL) あたりのコスト、ルールあたりのコスト、ウェブリクエスト検査の 100 万リクエストあたりの基本料金、最大 1,500 WCUs、およびデフォルトの本文サイズです。

Shield Advanced 自動アプリケーションレイヤー DDoS 緩和を有効にすると、150 個の保護パック (ウェブ ACL) キャパシティユニット (WCU) はルールグループに追加されます。これらの WCU は、

保護パック (ウェブ ACL) 内の WCU の使用量に対してカウントされます。詳細については[Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和]、[Shield Advanced ルールグループによるアプリケーションレイヤーの保護]、および[のウェブ ACL キャパシティユニット (WCUs) AWS WAF]を参照してください。

Shield Advanced のサブスクリプションでは、Shield Advanced を使用して保護しないリソース AWS WAF の の使用はカバーされません。また、保護されたリソースの標準以外の追加 AWS WAF コストもカバーしません。標準以外の AWS WAF コストの例としては、Bot Control、CAPTCHA ルールアクション、1,500 WCUs を超えるウェブ ACLs、およびデフォルトの本文サイズを超えるリクエスト本文の検査などがあります。完全なリストは AWS WAF 料金ページに記載されています。Shield Advanced へのサブスクリプションには、 Layer 7 Anti-DDoS Amazon Managed Rule グループへのアクセスが含まれます。サブスクリプションの一環として、Shield Advanced で保護された AWS WAF リソースへのリクエストは 1 か月あたり最大 500 億件になります。500 億を超えるリクエストは、 AWS Shield Advanced 料金ページに従って請求されます。

詳細情報および料金の例については、「[Shield の料金]」および「[AWS WAF の料金]」を参照してください。

トピック

- [Shield Advanced によるアプリケーションレイヤーのイベント検出と緩和に影響する要因のリスト]
- [AWS WAF ウェブ ACLs と Shield Advanced によるアプリケーションレイヤーの保護]
- [AWS WAF レートベースのルールと Shield Advanced によるアプリケーションレイヤーの保護]
- [Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和]

Shield Advanced によるアプリケーションレイヤーのイベント検出と緩和に影響する要因のリスト

このセクションでは、Shield Advanced によるアプリケーションレイヤーイベントの検出と緩和に影響する要因について説明します。

ヘルスチェック

アプリケーションの全体的な状態を正確に報告するヘルスチェックは、アプリケーションが経験しているトラフィック条件に関する情報を Shield Advanced に提供します。Shield Advanced では、アプリケーションが異常を報告している場合に潜在的な攻撃を指している情報が少なくなり、アプリケーションが正常を報告している場合に攻撃の証拠がさらに必要になります。

アプリケーションの状態を正確にレポートするには、ヘルスチェックを設定することが重要です。詳細とガイダンスについては、「Shield Advanced と Route 53 を使用したヘルスチェックを使用したヘルスベースの検出」を参照してください。

トラフィックのベースライン

トラフィックのベースラインは、アプリケーションの通常のトラフィックの特性に関する Shield Advanced 情報を提供します。Shield Advanced は、これらのベースラインを使用して、アプリケーションが通常のトラフィックを受信していないタイミングを認識します。そのため、アプリケーションは通知を行い、設定に従って、潜在的な攻撃に対抗するための緩和オプションの考案とテストを開始できます。Shield Advanced がトラフィックベースラインを使用して潜在的なイベントを検出する方法の詳細については、概要セクション アプリケーションレイヤーの脅威に対する Shield Advanced 検出ロジック (レイヤー 7) を参照してください。

Shield Advanced は、保護されたリソースに関連付けられているウェブ ACL によって提供される情報からベースラインを作成します。ウェブ ACL は、Shield Advanced がアプリケーションのベースラインを確実に決定できるようになるまで、少なくとも 24 時間から最大 30 日間、リソースに関連付ける必要があります。必要な時間は、Shield Advanced または AWS WAFを介してウェブ ACL を関連付けたときに開始されます。

Shield Advanced アプリケーションレイヤー保護でウェブ ACL を使用する方法の詳細については、AWS WAF ウェブ ACLs と Shield Advanced によるアプリケーションレイヤーの保護 を参照してください。

レートベースのルール

レートベースのルールは、攻撃の軽減に役立ちます。また、攻撃が通常のトラフィックのベースラインやヘルスチェックのステータスレポートに現れるほど大きな問題になる前に対処することで、攻撃を目立たなくすることもできます。

Shield Advanced でアプリケーションリソースを保護する場合は、ウェブ ACL でレートベースのルールを使用することをお勧めします。緩和策によって潜在的な攻撃を目立たなくすることはありますが、これらは貴重な第一の防御線であり、正当な顧客に対してアプリケーションの利用可能性を確保するのに役立ちます。レートベースのルールが検出するトラフィックとレート制限は、 AWS WAF メトリクスに表示されます。

独自のレートベースのルールに加えて、自動アプリケーションレイヤー DDoS 緩和を有効にすると、Shield Advanced は攻撃の軽減に使用するルールグループをウェブ ACL に追加します。このルールグループで、Shield Advanced は常に、DDoS 攻撃のソースであることが判明している IP ア

ドレスからのリクエストの量を制限するレートベースのルールを保持しています。Shield Advanced ルールが緩和するトラフィックのメトリクスは表示できません。

レートベースのルールの詳細については、「でのレートベースのルールステートメントの使用 AWS WAF」を参照してください。Shield Advanced アプリケーションレイヤー DDoS 自動緩和の詳細については、Shield Advanced ルールグループによるアプリケーションレイヤーの保護 を参照してください。

Shield Advanced と AWS WAF メトリクスの詳細については、「」を参照してくださいAmazon CloudWatch によるモニタリング。

AWS WAF ウェブ ACLs と Shield Advanced によるアプリケーションレイヤーの保護

このページでは、 AWS WAF ウェブ ACL と Shield Advanced が連携して基本的なアプリケーションレイヤー保護を作成する方法について説明します。 ACLs

Shield Advanced でアプリケーションレイヤーリソースを保護するには、まずウェブ ACL を AWS WAF リソースに関連付けることから始めます。 AWS WAF は、アプリケーションレイヤーリソースに転送される HTTP および HTTPS リクエストをモニタリングし、リクエストの特性に基づいてコンテンツへのアクセスを制御できるウェブアプリケーションファイアウォールです。リクエストの発信元、クエリ文字列とクッキーのコンテンツ、単一の IP アドレスからのリクエストのレートなどの要因に基づいて、リクエストをモニタリングおよび管理するウェブ ACL を設定できます。少なくとも、Shield Advanced 保護では、ウェブ ACL をレートベースのルールに関連付けて、各 IP アドレスのリクエストのレートを制限する必要があります。

関連付けられたウェブ ACL にレートベースのルールが定義されていない場合、Shield Advanced から少なくとも 1 つ定義するように求められます。レートベースのルールは、定義したしきい値を超えると、ソース IP からのトラフィックを自動的にブロックします。これらは、ウェブリクエストのフラッドからアプリケーションを保護するのに役立つとともに、DDoS 攻撃の可能性を示していることがあるトラフィックの急増についてアラートを出すことができます。

> **Note**
>
> レートベースのルールは、ルールがモニタリングしているトラフィックの急増に非常に迅速に応答します。このため、レートベースのルールは、攻撃だけでなく、Shield Advanced 検出によって、潜在的な攻撃も検出できます。このトレードオフは、攻撃パターンを完全に可視化するよりも防止を優先します。攻撃に対する防御の最前線として、レートベースのルールを使用することをお勧めします。

ウェブ ACL を設定すると、DDoS 攻撃が発生した場合、ウェブ ACL にルールを追加して管理することで緩和策を適用します。これは、直接行うことができるほか、Shield レスポンスチーム (SRT、Shield Response Team) のサポートを受けて、またはアプリケーションレイヤー DDoS 自動緩和を通じて自動的に行うこともできます。

> **Important**
>
> 自動アプリケーションレイヤー DDoS 緩和も使用する場合は、アプリケーションレイヤー DDoS 自動緩和機能を使用するためのベストプラクティス。 でウェブ ACL を管理するためのベストプラクティスを参照してください。

AWS WAF を使用してウェブリクエストのモニタリングおよび管理ルールを管理する方法については、「」を参照してください[で保護パック (ウェブ ACL) を作成する AWS WAF](#)。

AWS WAF レートベースのルールと Shield Advanced によるアプリケーションレイヤーの保護

このページでは、 AWS WAF レートベースのルールと Shield Advanced が連携して基本的なアプリケーションレイヤー保護を作成する方法について説明します。

デフォルト設定でレートベースのルールを使用すると、 は過去 5 分間の時間枠のトラフィック AWS WAF を定期的に評価します。 は、リクエストレートが許容レベルに低下するまで、ルールのしきい値を超える IP アドレスからのリクエストを AWS WAF ブロックします。Shield Advanced を通じてレートベースのルールを設定する際は、任意の 5 分間の時間枠内で期待される通常のトラフィックレートを超える値にレートしきい値を設定してください。

ウェブ ACL で複数のレートベースのルールを使用したい場合があります。例えば、高いしきい値を持つすべてのトラフィックについて 1 つのレートベースのルールを指定するとともに、ウェブアプリケーションの特定の部分と一致するように設定され、しきい値が低い追加のルールを 1 つ以上指定できます。例えば、ログインページに対する不正を緩和するために、しきい値を低くして URI `/login.html` に対する照合を行うことができます。

別の評価時間枠を使用し、ヘッダー値、ラベル、クエリ引数などの多数のリクエストコンポーネントによってリクエストを集約するように、レートベースのルールを設定できます。詳細については、「[でのレートベースのルールステートメントの使用 AWS WAF](#)」を参照してください。

追加情報とガイダンスについては、セキュリティブログ記事「[The three most important AWS WAF rate-based rules](#)」を参照してください。

を使用して設定オプションを拡張 AWS WAF

Shield Advanced コンソールでは、レートベースのルールを追加し、基本のデフォルト設定で構成できます。レートベースのルールを管理することで、追加の設定オプションを定義できます AWS WAF。例えば、転送された IP アドレス、クエリ文字列、およびラベルなどのキーに基づく集約リクエストのルールを設定できます。また、ルールにスコープダウンステートメントを追加して、一部のリクエストを評価およびレート制限から除外することも可能です。詳細については、「でのレートベースのルールステートメントの使用 AWS WAF」を参照してください。

Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和

> **Note**
>
> 2026 年 3 月 26 日以降、 の Anti-DDoS Managed Rule Group (Anti-DDOS AMR) が HTTP リクエストフラッド攻撃に対する保護のデフォルトソリューション AWS WAF になります (Anti-DDoS AMR 起動ブログを参照) 。Layer 7 Auto Mitigation (L7AM) 機能よりも優先されます。既存の Shield Advanced のお客様は、既存のアカウントまたは新しい AWS アカウントでレガシーソリューションを引き続き使用できます。ただし、DDoS 対策 DDoS マネージドルールグループを採用することをお勧めします。Anti-DDoS Managed Rule Group は、攻撃を数分ではなく数秒以内に検出して軽減します。Shield Advanced の新規のお客様で、レガシーソリューションへのアクセスが必要な場合は、 AWS サポートにお問い合わせください。

このページでは、アプリケーションレイヤーの自動 DDoS 緩和のトピックを紹介し、関連する規制を一覧表示します。

攻撃の一部であるウェブリクエストをカウントまたはブロックすることで、保護されたアプリケーションレイヤーリソースに対するアプリケーションレイヤー (レイヤー 7) 攻撃を自動的に緩和して対応するよう Shield Advanced を設定できます。このオプションは、 AWS WAF ウェブ ACL と独自のレートベースのルールを使用して Shield Advanced を介して追加するアプリケーションレイヤー保護に追加されます。

リソースの自動緩和が有効になっている場合、Shield Advanced はリソースの関連するウェブ ACL にルールグループを管理し、リソースに代わって緩和ルールを管理します。ルールグループには、DDoS 攻撃のソースであることが判明している IP アドレスからのリクエストの量を追跡するレートベースのルールが含まれています。

さらに、Shield Advanced は、現在のトラフィックパターンと過去のトラフィックベースラインを比較して、DDoS 攻撃を示している可能性のある逸脱を検出します。Shield Advanced は、ルールグループに追加のカスタム AWS WAF ルールを作成、評価、デプロイすることで、検出された DDoS 攻撃に応答します。

自動アプリケーションレイヤー DDoS 緩和の使用に関する規制

次のリストでは、Shield Advanced アプリケーションレイヤー DDoS 自動緩和の注意事項と、対応が必要となる可能性があるステップについて説明します。

- 自動アプリケーションレイヤー DDoS 緩和は、最新バージョンの (v2) を使用して作成された保護パック AWS WAF (ウェブ ACLs) でのみ機能します。
- Shield Advanced には、アプリケーションの通常の履歴トラフィックのベースラインを確立する時間が必要です。これを活用して、攻撃トラフィックを検出して通常のトラフィックから分離し、攻撃トラフィックを軽減します。ベースラインを確立する時間は、ウェブ ACL を保護されたアプリケーションリソースに関連付ける時点から 24 時間から 30 日の間です。トラフィックベースラインの詳細については、Shield Advanced によるアプリケーションレイヤーのイベント検出と緩和に影響する要因のリスト を参照してください。
- 自動アプリケーションレイヤー DDoS 緩和を有効にすると、150 個の保護パック (ウェブ ACL) キャパシティユニット (WCU)。これらの WCU は、保護パック (ウェブ ACL) 内の WCU の使用量に対してカウントされます。詳細については「Shield Advanced ルールグループによるアプリケーションレイヤーの保護」および「のウェブ ACL キャパシティユニット (WCUs) AWS WAF」を参照してください。
- Shield Advanced ルールグループは AWS WAF メトリクスを生成しますが、表示することはできません。これは、 AWS マネージドルールルールグループなど、保護パック (ウェブ ACL) で使用する他のルールグループと同じですが、所有していません。 AWS WAF メトリクスの詳細については、「」を参照してくださいAWS WAF メトリクスとディメンション。Shield Advanced 保護オプションの機能については、Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和 を参照してください。
- 複数のリソースを保護するウェブ ACL の場合、自動緩和は、どのリソースにも悪影響をおよぼさないカスタム緩和策のみを展開します。
- DDoS 攻撃の開始から Shield Advanced がカスタム自動緩和ルールを実行するまでの時間は、各イベントによって異なります。一部の DDoS 攻撃は、カスタムルールがデプロイされる前に終了することがあります。他の攻撃は、緩和策が既に実施されている場合に発生する可能性があるため、これらのルールによってイベントの開始時から緩和される可能性があります。さらに、ウェブ ACL および Shield Advanced ルールグループのレートベースのルールは、潜在的なイベントとして検出される前に、攻撃トラフィックを軽減する可能性があります。

- Amazon CloudFront などのコンテンツ配信ネットワーク (CDN) を介してトラフィックを受信する Application Load Balancer では、それらの Application Load Balancer リソース向けの Shield Advanced のアプリケーションレイヤーの自動緩和機能は低減します。Shield Advanced は、クライアントトラフィック属性を使用して、アプリケーションへの通常のトラフィックから攻撃トラフィックを識別および分離します。CDN は、元のクライアントトラフィック属性を保持または転送しない場合があります。CloudFront を使用する場合は、CloudFront ディストリビューションで自動緩和策を有効にすることをお勧めします。
- アプリケーションレイヤー DDoS 自動緩和は、保護グループとインタラクションしません。保護グループに含まれるリソースのために自動緩和を有効にできますが、Shield Advanced は、保護グループの検出結果に基づいて攻撃の緩和策を自動的に適用しません。Shield Advanced は、個々のリソースのために攻撃の自動緩和を適用します。

目次

- アプリケーションレイヤー DDoS 自動緩和機能を使用するためのベストプラクティス。
- アプリケーションレイヤー DDoS 自動緩和の有効化
  - 自動緩和を有効にした場合の実行内容
- Shield Advanced が自動緩和を管理する方法
  - Shield Advanced が自動緩和機能で DDoS 攻撃に対応する方法
  - Shield Advanced がルールアクション設定を管理する方法
  - 攻撃が沈静化した場合に Shield Advanced が緩和を管理する方法
  - 自動緩和を無効にした場合の実行内容
- Shield Advanced ルールグループによるアプリケーションレイヤーの保護
- リソースのアプリケーションレイヤー DDoS 自動緩和設定の表示
- アプリケーションレイヤー DDoS 自動緩和の有効化と無効化
- アプリケーションレイヤー DDoS 自動緩和に使用されるアクションの変更
- アプリケーションレイヤー DDoS 自動緩和 AWS CloudFormation での の使用

アプリケーションレイヤー DDoS 自動緩和機能を使用するためのベストプラクティス。

自動緩和機能を使用する場合は、このセクションに記載されているガイダンスを遵守してください。

一般的な保護管理

自動緩和保護を計画および実装する場合は、以下のガイドラインに従ってください。

- Shield Advanced を通じて、または AWS Firewall Manager を使用して Shield Advanced 自動緩和設定を管理している場合は Firewall Manager を通じて、すべての自動緩和保護を管理します。これらの保護を管理するために Shield Advanced と Firewall Manager を合わせて使用しないでください。
- 同一のウェブ ACL と保護設定を使用して類似のリソースを管理し、別々のウェブ ACL を使用して類似していないリソースを管理してください。Shield Advanced は、保護されたリソースに対する DDoS 攻撃を緩和する場合、リソースに関連付けられているウェブ ACL のルールを定義し、ウェブ ACL に関連付けられているすべてのリソースのトラフィックに対してルールをテストします。Shield Advanced は、関連付けられたリソースに悪影響を及ぼさない場合にのみルールを適用します。詳細については、「Shield Advanced が自動緩和を管理する方法」を参照してください。
- Amazon CloudFront ディストリビューションを介してすべてのインターネットトラフィックがプロキシされる Application Load Balancer では、CloudFront ディストリビューションでの自動緩和のみを有効にします。CloudFront ディストリビューションが持つ元のトラフィック属性の数は常に最大となります。これは、Shield Advanced が攻撃を緩和するために活用します。

検出と緩和の最適化

自動緩和が保護されたリソースに提供する保護を最適化するには、以下のガイドラインに従ってください。アプリケーションレイヤーの検出と緩和の概要については、Shield Advanced によるアプリケーションレイヤーのイベント検出と緩和に影響する要因のリスト を参照してください。

- 保護されたリソースのヘルスチェックを設定し、それを使用して Shield Advanced 保護でヘルスベースの検出を有効にします。ガイダンスについては、「Shield Advanced と Route 53 を使用したヘルスチェックを使用したヘルスベースの検出」を参照してください。
- Shield Advanced が通常の履歴トラフィックのベースラインを確立するまで、Count モードで自動緩和を有効にします。Shield Advanced では、ベースラインを確立するのに 24 時間から 30 日かかります。

  通常のトラフィックパターンのベースラインを確立するには、以下が必要です:

  - ウェブ ACL と保護されたリソースとの関連。を使用してウェブ ACL AWS WAF を直接関連付けるか、Shield Advanced アプリケーションレイヤー保護を有効にして使用するウェブ ACL を指定するときに Shield Advanced に関連付けさせることができます。
  - 保護されたアプリケーションの通常のトラフィックフロー。アプリケーションの起動前など、アプリケーションに通常のトラフィックが発生していない場合や、本番環境のトラフィックが長期間不足している場合、履歴データを収集することはできません。

ウェブ ACL 管理

自動緩和で使用されるウェブ ACL を管理するには、以下のガイドラインに従ってください。

- 保護されたリソースに関連付けられているウェブ ACL を置き換える必要がある場合は、次の変更を順番に行います。

  1. Shield Advanced が自動緩和を管理する方法。
  2. で AWS WAF、古いウェブ ACL の関連付けを解除し、新しいウェブ ACL を関連付けます。
  3. Shield Advanced で自動緩和を管理します。

  Shield Advanced は、古いウェブ ACL から新しいウェブ ACL に自動緩和を自動的に転送しません。
- 名前が `ShieldMitigationRuleGroup` で始まるウェブ ACL からルールグループルールを削除しないでください。このルールグループを削除すると、ウェブ ACL に関連付けられているすべてのリソースについて、Shield Advanced 自動緩和機能によって提供される保護が無効になります。さらに、Shield Advanced が変更の通知を受け取り、設定を更新するのに時間がかかることがあります。この間、Shield Advanced コンソールページには誤った情報が表示されます。

  ルールグループの詳細については、「Shield Advanced ルールグループによるアプリケーションレイヤーの保護」を参照してください。
- 名前が `ShieldMitigationRuleGroup` で始まるルールグループルールの名前を変更しないでください。変更すると、ウェブ ACL を介して Shield Advanced 自動緩和機能によって提供される保護が妨げられる可能性があります。
- ルールとルールグループを作成するときには、`ShieldMitigationRuleGroup` で始まる名前を使用しないでください。この文字列は、Shield Advanced が自動緩和を管理するために使用します。
- ウェブ ACL ルールの管理では、優先順位の設定として 10,000,000 を割り当てないでください。Shield Advanced は、自動緩和ルールグループルールを追加するときに、この優先順位設定をそのルールグループルールに割り当てます。
- `ShieldMitigationRuleGroup` ルールの優先順位を維持し、ウェブ ACL 内の他のルールと関連して必要なときに実行できるようにします。Shield Advanced は、優先順位を 10,000,000 に設定したルールグループルールをウェブ ACL に追加し、他のルールよりも後に実行します。 AWS WAF コンソールウィザードを使用してウェブ ACL を管理する場合は、ウェブ ACL にルールを追加した後、必要に応じて優先度設定を調整します。
- AWS CloudFormation を使用してウェブ ACLs を管理する場合、`ShieldMitigationRuleGroup`ルールグループルールを管理する必要はありません。「アプ

リケーションレイヤー DDoS 自動緩和 AWS CloudFormation での の使用」のガイダンスに従います。

アプリケーションレイヤー DDoS 自動緩和の有効化

このページでは、アプリケーションレイヤー攻撃に自動的に対応するように Shield Advanced を設定する方法について説明します。

Shield Advanced 自動緩和機能は、リソースのためのアプリケーションレイヤーの DDoS 保護の一部として有効にします。コンソールからこれを実行する方法については、「アプリケーションレイヤー DDoS 保護を設定する」を参照してください。

自動緩和機能を使用するには、次の操作を行う必要があります。

- [Associate a web ACL with the resource] (ウェブ ACL をリソースに関連付ける) – これは、Shield Advanced アプリケーションレイヤー保護のために必須です。複数のリソースに同じウェブ ACL を使用できます。同様のトラフィックを持つリソースについてのみ、これを行うことをお勧めします。ウェブ ACL を複数のリソースで使用するための要件など、ウェブ ACL の詳細については、「の AWS WAF 仕組み」を参照してください。
- [Enable and configure Shield Advanced automatic application layer DDoS mitigation] (Shield Advanced アプリケーションレイヤー DDoS 自動緩和を有効にして設定する) – これを有効にする際に、Shield Advanced が DDoS 攻撃の一部であると判断したウェブリクエストを自動的にブロックまたはカウントするかどうかを指定します。Shield Advanced は、関連付けられたウェブ ACL にルールグループを追加し、それを使用して、リソースに対する DDoS 攻撃に対する対応を動的に管理します。ルールアクションのオプションについては、「でのルールアクションの使用 AWS WAF」を参照してください。
- (オプションですが、推奨されます) ウェブ ACL にレートベースのルールを追加する – デフォルトでは、レートベースのルールは、個々の IP アドレスによる短時間の大量リクエスト送信を防ぐことで、DDoS 攻撃に対する基本的な保護をリソースに提供します。カスタムリクエストの集約オプションや例など、レートベースのルールの詳細については、「でのレートベースのルールステートメントの使用 AWS WAF」を参照してください。

自動緩和を有効にした場合の実行内容

Shield Advanced は、自動緩和を有効にすると、次の処理を実行します。

- 必要に応じて、 は Shield Advanced 用のルールグループを追加します – リソースに関連付けられた AWS WAF ウェブ ACL に、アプリケーションレイヤー DDoS 自動緩和専用の AWS WAF ルールグループルールがまだない場合、Shield Advanced はルールグループを追加します。

  グループルールのルール名は `ShieldMitigationRuleGroup` で始まります。ルールグループには常に `ShieldKnownOffenderIPRateBasedRule` という名前のレートベースのルールが含まれており、DDoS 攻撃のソースであることが判明している IP アドレスからのリクエストの量を制限します。Shield Advanced ルールグループと参照するウェブ ACL ルールの詳細については、「Shield Advanced ルールグループによるアプリケーションレイヤーの保護」を参照してください。

- [Starts responding to DDoS attacks against the resource] (リソースに対する DDoS 攻撃への対応を開始) – Shield Advanced は、保護されたリソースに対する DDoS 攻撃に自動的に対応します。常に存在するレートベースのルールに加えて、Shield Advanced はルールグループを使用して DDoS 攻撃の軽減のためのカスタム AWS WAF ルールをデプロイします。Shield Advanced は、これらのルールをアプリケーションとアプリケーションが経験する攻撃に合わせて調整し、デプロイする前にリソースの過去のトラフィックに照らし合わせてテストします。

Shield Advanced は、自動緩和に使用するウェブ ACL で単一のルールグループルールを使用します。Shield Advanced が、別の保護されたリソースのルールグループを追加している場合、ウェブ ACL には別のルールグループを追加しません。

アプリケーションレイヤー DDoS 自動緩和は、攻撃を緩和するためのルールグループの存在によって異なります。何らかの理由でルールグループが AWS WAF ウェブ ACL から削除された場合、削除はウェブ ACL に関連付けられているすべてのリソースの自動緩和を無効にします。

Shield Advanced が自動緩和を管理する方法

このセクションのトピックでは、Shield Advanced がアプリケーションレイヤー DDoS 自動緩和の設定変更をどのように処理するか、および自動緩和が有効になっている場合の DDoS 攻撃の処理方法について説明します。

トピック

- Shield Advanced が自動緩和機能で DDoS 攻撃に対応する方法
- Shield Advanced がルールアクション設定を管理する方法
- 攻撃が沈静化した場合に Shield Advanced が緩和を管理する方法
- 自動緩和を無効にした場合の実行内容

Shield Advanced が自動緩和機能で DDoS 攻撃に対応する方法

保護対象リソースで自動軽減機能を有効にすると、Shield Advanced ルールグループのレートベースのルール `ShieldKnownOffenderIPRateBasedRule` は、既知の DDoS ソースからのトラフィックの量の増加に自動的に応答します。このレート制限は迅速に適用され、攻撃に対する最前線の防御として機能します。

Shield Advanced が攻撃を検出すると、次の処理が実行されます。

1. アプリケーションへの通常のトラフィックから攻撃トラフィックを分離する攻撃シグネチャの特定を試みます。目標は、攻撃トラフィックにのみ影響し、アプリケーションへの通常のトラフィックに影響を与えない、質の高い DDoS 緩和ルールを作成することです。
2. 識別された攻撃シグネチャを、攻撃対象のリソースおよび同じウェブ ACL に関連付けられている他のリソースについての過去のトラフィックパターンに照らして評価します。Shield Advanced は、イベントに対応してルールをデプロイする前にこれを実行します。

   Shield Advanced は、評価結果に応じて、次のいずれかを実行します。

   - Shield Advanced は、攻撃シグネチャが DDoS 攻撃に関与するトラフィックのみを隔離すると判断した場合、ウェブ ACL の Shield Advanced 緩和ルールグループの AWS WAF ルールにシグネチャを実装します。Shield Advanced は、これらのルールに、リソースの自動緩和のために設定したアクション設定 (Count または Block) を提供します。
   - その他の場合、Shield Advanced は緩和策を講じません。

攻撃全体を通じて、Shield Advanced は、基本的な Shield Advanced アプリケーションレイヤー保護と同じ通知を送信し、同じイベント情報を提供します。Shield Advanced イベントコンソールで、イベントと DDoS 攻撃に関する情報、および攻撃に対する Shield Advanced の緩和策に関する情報を確認できます。詳細については、「Shield Advanced による DDoS イベントの可視性」を参照してください。

Block ルールアクションを使用するように自動緩和を設定し、Shield Advanced がデプロイした緩和ルールからの誤検出が発生した場合は、ルールアクションを Count に変更できます。これを行う方法については、「アプリケーションレイヤー DDoS 自動緩和に使用されるアクションの変更」を参照してください。

Shield Advanced がルールアクション設定を管理する方法

自動緩和策のルールアクションは Block または Count に設定できます。

保護されたリソースの自動緩和ルールアクション設定を変更すると、Shield Advanced は、リソースのすべてのルール設定を更新します。Sheild Advanced ルールグループのリソースに現在適用されているルールが更新され、新しいルールの作成時に新しいアクション設定が使用されます。

同じウェブ ACL を使用するリソースに対して異なるアクションを指定すると、Shield Advanced はルールグループのレートベースのルール `ShieldKnownOffenderIPRateBasedRule` の Block アクション設定を使用します。Shield Advanced は、特定の保護対象リソースに代わってルールグループ内の他のルールを作成および管理し、リソースに指定したアクション設定を使用します。ウェブ ACL 内の Shield Advanced ルールグループのすべてのルールは、関連するすべてのリソースのウェブトラフィックに適用されます。

アクション設定を変更すると、反映されるまでに数秒かかる場合があります。この間、ルールグループが使用されている場所によっては古い設定が表示され、他の場所では新しい設定が表示される場合があります。

自動緩和設定のルールアクション設定は、コンソールのイベントページ、およびアプリケーションレイヤー設定ページで変更できます。イベントページの詳細については、「での DDoS イベントへの対応 AWS」を参照してください。設定ページについては、「アプリケーションレイヤー DDoS 保護を設定する」を参照してください。

攻撃が沈静化した場合に Shield Advanced が緩和を管理する方法

Shield Advanced は、特定の攻撃に対してデプロイされた緩和ルールが不要になったと判断すると、そのルールを Shield Advanced 緩和ルールグループから削除します。

緩和ルールの削除は、必ずしも攻撃の終了と一致しません。Shield Advanced は、保護されたリソースで検出された攻撃のパターンをモニタリングします。攻撃の最初の発生に対してデプロイしたルールを所定の位置に保持することで、特定のシグネチャを使用した攻撃の再発を先回りして防御できる場合があります。必要に応じて、Shield Advanced はルールを保持する時間枠を拡大します。このようにして、Shield Advanced は、保護されたリソースに影響が及ぶ前に、特定のシグネチャで繰り返される攻撃を緩和する場合があります。

Shield Advanced が、DDoS 攻撃のソースであることが判明している IP アドレスからのリクエストの量を制限するレートベースのルール `ShieldKnownOffenderIPRateBasedRule` を削除することはありません。

自動緩和を無効にした場合の実行内容

Shield Advanced は、リソースのための自動緩和を無効にすると、次の処理を実行します。

- [Stops automatically responding to DDoS attacks] (DDoS 攻撃への自動対応を停止) – Shield Advanced は、リソースのための自動応答アクティビティを中止します。
- [Removes unneeded rules from the Shield Advanced rule group] (Shield Advanced ルールグループから不要なルールを削除) – Shield Advanced が保護されたリソースのためにマネージドルールグループ内のルールを維持している場合、それらを削除します。
- [Removes the Shield Advanced rule group, if it's no longer in use] (Shield Advanced ルールグループが使用されなくなった場合は削除) – リソースに関連付けたウェブ ACL が、自動緩和が有効になっている他のリソースに関連付けられていない場合、Shield Advanced は、そのルールグループルールをウェブ ACL から削除します。

Shield Advanced ルールグループによるアプリケーションレイヤーの保護

このページでは、ウェブ ACL での Shield Advanced ルールグループの仕組みについて説明します。

Shield Advanced は、所有および管理するルールグループ内のルールを使用して、自動緩和アクティビティを管理します。Shield Advanced は、保護されたリソースに関連付けたウェブ ACL 内のルールを使用してルールグループを参照します。

ウェブ ACL におけるルールグループルール

ウェブ ACL の Shield Advanced ルールグループルールには、次のプロパティがあります。

- [Name] (名前) – `ShieldMitigationRuleGroup_`*`account-id`*`_`*`web-acl-id`*`_`*`unique-identifier`*
- [Web ACL capacity units (WCU)] (ウェブ ACL キャパシティーユニット (WCU)) – 150。これらの WCU は、ウェブ ACL 内の WCU の使用量に対してカウントされます。

Shield Advanced は、優先度設定が 10,000,000 のウェブ ACL にこのルールを作成します。このルールは、ウェブ ACL の他のルールとルールグループがウェブ ACL のルールを、 上の最も低い数値優先度設定から AWS WAF 実行した後に実行されます。ウェブ ACL の管理中に、この優先順位の設定が変更される場合があります。

自動緩和機能は、ウェブ ACL のルール グループによって使用される WCU を除き、アカウント内の追加の AWS WAF リソースを消費しません。例えば、Shield Advanced ルールグループは、アカウントのルールグループの 1 つとしてカウントされません。のアカウント制限の詳細については AWS WAF、「」を参照してくださいAWS WAF クォータ。

ルールグループ内のルール

参照先の Shield Advanced ルールグループ内では、Shield Advanced が DDoS 攻撃のソースであることが判明している IP アドレスからのリクエストの量を制限するレートベースのルール `ShieldKnownOffenderIPRateBasedRule` を維持します。このルールは常にルールグループに存在し、トラフィックパターンの分析に頼らずに攻撃を封じ込めるため、あらゆる攻撃に対する防御の最前線として機能します。このルールのアクションは、ルールグループの他のルールと同様に、自動緩和策で選択したアクションに設定されます。レートベースルールの詳細については、「でのレートベースのルールステートメントの使用 AWS WAF」を参照してください。

> **Note**
>
> レートベースのルール `ShieldKnownOffenderIPRateBasedRule` の動きは、Shield Advanced イベント検出とは無関係です。自動緩和が有効になっている間、このルールレートは DDoS 攻撃のソースとして知られている IP アドレスを制限します。これらの IP アドレスの場合、ルールのレート制限により、攻撃を防止し、Shield Advanced 検出情報に攻撃が表示されないようにすることができます。このトレードオフは、攻撃パターンを完全に可視化するよりも防止を優先します。

上記の永久レートベースのルールに加えて、ルールグループには、Shield Advanced が現在 DDoS 攻撃を軽減するために使用しているすべてのルールが含まれます。Shield Advanced は、必要に応じてこれらのルールを追加、変更、削除します。詳細については、「Shield Advanced が自動緩和を管理する方法」を参照してください。

メトリクス

ルールグループは AWS WAF メトリクスを生成しますが、このルールグループは Shield Advanced によって所有されているため、これらのメトリクスを表示することはできません。詳細については、「AWS WAF メトリクスとディメンション」を参照してください。

リソースのアプリケーションレイヤー DDoS 自動緩和設定の表示

リソースのアプリケーションレイヤー DDoS 自動緩和設定は、[保護リソース] ページと個々の保護ページで表示できます。

リソースのアプリケーションレイヤー DDoS 自動緩和設定を表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF & Shield コンソールを開きます。

2. AWS Shield ナビゲーションペインで、保護されたリソースを選択します。保護対象リソースのリストの [アプリケーションレイヤー DDoS 自動緩和] 列は、自動緩和が有効になっているかどうか、また有効になっている場合は緩和で Shield Advanced が使用するアクションを示します。

   任意のアプリケーションレイヤーリソースを選択することによっても、リソースの保護ページにリストされているのと同じ情報を表示することもできます。

アプリケーションレイヤー DDoS 自動緩和の有効化と無効化

次の手順では、保護されたリソースのための自動対応を有効または無効にする方法を示しています。

単一のリソースのアプリケーションレイヤー DDoS 自動緩和を有効または無効にするには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF & Shield コンソールを開きます。
2. AWS Shield ナビゲーションペインで、保護されたリソースを選択します。
3. [Protections] (保護) タブで、自動緩和を有効にするアプリケーションレイヤーリソースを選択します。リソースの保護ページが開きます。
4. リソースの保護ページで、[Edit] (編集) を選択します。
5. [グローバルリソース用のレイヤー 7 DDoS 緩和を設定 - オプション] ページの [アプリケーションレイヤー DDoS 自動緩和] で、自動緩和に使用するオプションを選択します。コンソールのオプションを以下に示します。

   - [Keep current settings] (現在の設定を保持) — 保護されたリソースの自動緩和設定は変更されません。
   - [Enable] (有効化) — 保護されたリソースの自動緩和を有効にします。このオプションを選択する場合、ウェブ ACL ルールで使用するルールアクションも選択します。ルールアクションの設定については、「でのルールアクションの使用 AWS WAF」を参照してください。

     保護されたリソースに通常のアプリケーショントラフィックの履歴がまだない場合は、Shield Advanced がベースラインを確立できるようになるまで、Count モードで自動緩和を有効にします。Shield Advanced は、ウェブ ACL を保護されたリソースに関連付けると、ベースラインの情報を収集し始めます。通常のトラフィックの適切なベースラインを確立するには 24 時間から 30 日間までかかる場合があります。
   - [Disable] (無効化) — 保護されたリソースの自動緩和を無効にします。
6. 残りのページを最後まで順を追って確認し、設定を保存します。

[Protections] (保護) ページで、リソースの自動軽減設定が更新されます。

アプリケーションレイヤー DDoS 自動緩和に使用されるアクションの変更

コンソール内の複数の場所で、Shield Advanced がアプリケーションレイヤーの自動対応に使用するアクションを変更できます。

- [Automatic mitigation configuration] (自動緩和設定) - リソースのための自動緩和を設定するときに、アクションを変更します。手順については、前のセクションの「アプリケーションレイヤー DDoS 自動緩和の有効化と無効化」を参照してください。
- [Event details page] (イベントの詳細ページ) – コンソールでイベント情報を表示しているときに、イベントの詳細ページでアクションを変更します。詳細については、「AWS Shield Advanced イベントの詳細の表示」を参照してください。

ウェブ ACL を共有する保護対象リソースが 2 つあり、一方のアクションを Count に、他方のアクションを Block に設定した場合、Shield Advanced はルールグループのレートベースのルール `ShieldKnownOffenderIPRateBasedRule` のアクションを Block に設定します。

アプリケーションレイヤー DDoS 自動緩和 AWS CloudFormation での の使用

このページでは、 CloudFormation を使用して保護と AWS WAF ウェブ ACLs を管理する方法について説明します。

アプリケーションレイヤー DDoS 自動緩和の有効化または無効化

`AWS::Shield::Protection` リソースを使用して AWS CloudFormation、 を通じてアプリケーションレイヤー DDoS 自動緩和を有効または無効にできます。コンソールやその他のインターフェイスからでも、同じようにこの機能を有効または無効にできます。 CloudFormation リソースの詳細については、 AWS CloudFormation ユーザーガイドのAWS::Shield::Protection」を参照してください。

自動緩和で使用されるウェブ ACL の管理

Shield Advanced は、保護されたリソースの AWS WAF ウェブ ACL のルールグループルールを使用して、保護されたリソースの自動緩和を管理します。 AWS WAF コンソールと APIs を通じて、ウェブ ACL ルールに で始まる名前でリストされているルールが表示されますShieldMitigationRuleGroup。このルールはアプリケーションレイヤー DDoS 自動緩和専用で、Shield Advanced と AWS WAFがユーザーに代わって管理します。詳細については、「Shield Advanced ルールグループによるアプリケーションレイヤーの保護」および「Shield Advanced が自動緩和を管理する方法」を参照してください。

CloudFormation を使用してウェブ ACLs を管理する場合は、Shield Advanced ルールグループルールをウェブ ACL テンプレートに追加しないでください。自動緩和保護で使用されているウェブ ACL を更新すると、 はウェブ ACL のルールグループルール AWS WAF を自動的に管理します。

管理する他のウェブ ACLs と比較して、次の違いがあります CloudFormation。

- CloudFormation は、Shield Advanced ルールグループルールを使用したウェブ ACL の実際の設定と、ルールを使用しないウェブ ACL テンプレートの間のスタックドリフトステータスのドリフトを報告しません。Shield Advanced ルールは、ドリフト詳細でリソースの実際のリストには表示されません。

  Shield Advanced ルールグループルールは AWS WAF、コンソールや AWS WAF APIs など、AWS WAF から取得したウェブ ACL リストで確認できます。
- スタックでウェブ ACL テンプレートを変更 AWS WAF し、Shield Advanced が更新されたウェブ ACL で Shield Advanced 自動緩和ルールを自動的に維持する場合。Shield Advanced が提供する自動緩和保護は、ウェブ ACL を更新しても中断されることはありません。

CloudFormation ウェブ ACL テンプレートで Shield Advanced ルールを管理しないでください。ウェブ ACL テンプレートで Shield Advanced ルールを表示しないでください。「アプリケーションレイヤー DDoS 自動緩和機能を使用するためのベストプラクティス。」のウェブ ACL 管理のベストプラクティスに従ってください。

Shield Advanced と Route 53 を使用したヘルスチェックを使用したヘルスベースの検出

ヘルスベースの検出を使用するように Shield Advanced を設定することで、攻撃の検出と緩和策の応答性と精度を改善できます。このオプションは、Route 53 ホストゾーンを除くすべてのリソースタイプで使用できます。

ヘルスベースの検出を設定するには、Route 53 でリソースのヘルスチェックを定義し、正常であると報告されていることを検証してから、Shield Advanced 保護と関連付けます。Route 53 ヘルスチェックの詳細については、「Amazon Route 53 デベロッパーガイド」の「Amazon Route 53 がリソースのヘルスをチェックする方法」および「ヘルスチェックの作成、更新、削除」を参照してください。

> **Note**
>
> Shield Response Team (SRT) のプロアクティブなエンゲージメントサポートには、ヘルスチェックが必要です。プロアクティブなエンゲージメントの詳細については、「SRT が直接連絡するためのプロアクティブエンゲージメントの設定」を参照してください。

ヘルスチェックでは、定義した要件に基づいて、リソースのヘルスを測定します。ヘルスチェックのステータスは、Shield Advanced 検出メカニズムに重要な入力を提供します。これにより、特定のアプリケーションの現在の状態に対する感度が向上します。

Route 53 ホストゾーンを除くリソースタイプのために、ヘルスベースの検出を有効にできます。

- ネットワークおよびトランスポートレイヤー (レイヤー 3 /レイヤー 4) のリソース – ヘルスベースの検出により、ネットワークレイヤーおよびトランスポートレイヤーのイベント検出の精度と、Network Load Balancer、Elastic IP アドレス、および Global Accelerator 標準アクセラレーターのための緩和が改善されます。Shield Advanced を使用してこれらのリソースタイプを保護する場合、Shield Advanced は、トラフィックがアプリケーションの容量内である場合でも、小規模な攻撃の緩和と、攻撃のより迅速な緩和を行うことができます。

  ヘルスベースの検出を追加する場合、関連付けられたヘルスチェックが異常な期間中に、Shield Advanced を使用してより迅速に、低いしきい値で緩和策を行えます。
- アプリケーションレイヤー (レイヤー 7) リソース - ヘルスベースの検出により、CloudFront ディストリビューションおよび Application Load Balancer のウェブリクエストのフラッド検出の精度が向上します。Shield Advanced を使用してこれらのリソースタイプを保護する場合、リクエストの特性に基づいて、トラフィックパターンの大幅な変化を伴うトラフィック量の統計的に有意な偏差がある場合に、ウェブリクエストのフラッド検出アラートが送信されます。

  ヘルスベースの検出では、関連付けられた Route 53 ヘルスチェックが異常な期間中に、Shield Advanced は、アラートするためにより小さな偏差を必要とし、より迅速にイベントを報告します。逆に、関連付けられた Route 53 ヘルスチェックが正常である場合、Shield Advanced では、アラートするためにより大きな偏差が必要です。

アプリケーションが許容可能なパラメータ内で実行されている場合にのみヘルスチェックが正常であることを報告し、そうでないときにのみ異常であることを報告する場合に、Shield Advanced におけるヘルスチェックの使用から最も大きな恩恵を受けることができます。このセクションのガイダンスを使用して、Shield Advanced でヘルスチェックの関連付けを管理します。

> **Note**
>
> Shield Advanced は、ヘルスチェックを自動的に管理しません。

Shield Advanced でヘルスチェックを使用するには、次が必要です。

- ヘルスチェックは、Shield Advanced 保護に関連付けるときに、正常であると報告するものである必要があります。
- ヘルスチェックは、保護されたリソースのヘルスに関連している必要があります。お客様は、アプリケーションの特定の要件に基づいて、アプリケーションのヘルスを正確に報告するヘルスチェックを定義し、維持する責任があります。
- ヘルスチェックは、Shield Advanced 保護で使用できるようにしておく必要があります。Shield Advanced 保護に使用している Route 53 のヘルスチェックを削除しないでください。

目次

- Shield Advanced でヘルスチェックを使用するためのベストプラクティス
- Shield Advanced によるヘルスチェックに一般的に使用される CloudWatch メトリクス
  - アプリケーションのヘルスをモニタリングするために使用されるメトリクス
  - 各リソースタイプの Amazon CloudWatch メトリクス
- Shield Advanced で保護されたリソースにヘルスチェックを関連付ける
- Shield Advanced で保護されたリソースとヘルスチェックの関連解除する
- Shield Advanced でのヘルスチェックの関連ステータスの表示
- Shield Advanced のヘルスチェックの例
  - Amazon CloudFront ディストリビューション
  - ロードバランサー
  - Amazon EC2 Elastic IP アドレス (EIP)

Shield Advanced でヘルスチェックを使用するためのベストプラクティス

Shield Advanced でヘルスチェックを作成して使用する場合は、このセクションのベストプラクティスに従います。

- モニタリングするインフラストラクチャのコンポーネントを特定して、ヘルスチェックを計画します。ヘルスチェックでは、次のリソースタイプを検討してください。
  - 重要なリソース。
  - Shield Advanced の検出と緩和で高感度が必要なリソース。
  - Shield Advanced からプロアクティブに通知を受けたいリソース。プロアクティブなエンゲージメントは、ヘルスチェックのステータスによって通知されます。

  モニタリングする可能性のあるリソースの例には、Amazon CloudFront ディストリビューション、インターネット向けロードバランサー、Amazon EC2 インスタンスが含まれます。
- 可能な限り少ない通知で、アプリケーションオリジンのヘルスを正確に反映するヘルスチェックを定義します。
  - アプリケーションが利用できない場合や許容可能なパラメータ内で動作しない場合のみ異常になるようにヘルスチェックを記述します。お客様は、アプリケーションの特定の要件に基づいてヘルスチェックを定義し、維持する責任があります。
  - アプリケーションのヘルスを引き続き正確に報告しながら、できる限り少ないヘルスチェックを使用します。例えば、すべてが同じ問題を報告するアプリケーションの複数の領域からの複数のアラームは、情報価値をもたらすことなく、レスポンスアクティビティにオーバーヘッドを追加する可能性があります。
  - 計算されたヘルスチェックを使用して、Amazon CloudWatch メトリクスの組み合わせを用いてアプリケーションのヘルスをモニタリングします。例えば、アプリケーションサーバーのレイテンシーと 5xx エラー率に基づいて、複合ヘルスを計算できます。これは、オリジンサーバーがリクエストを満たしていないことを示唆します。
  - 必要に応じて、独自のアプリケーションヘルスインジケーターを作成し、CloudWatch カスタムメトリクスに発行して、計算されたヘルスチェックで使用します。
- ヘルスチェックを実装および管理して、検出を改善し、不要なメンテナンス作業を減らします。
  - ヘルスチェックを Shield Advanced 保護に関連付ける前に、ヘルスチェックが正常な状態であることを確認してください。異常を報告しているヘルスチェックを関連付けると、保護されたリソースに関する Shield Advanced 検出メカニズムが歪む可能性があります。
  - ヘルスチェックは Shield Advanced で使用できるようにしておきます。Shield Advanced 保護に使用している Route 53 のヘルスチェックを削除しないでください。
  - ステージング環境とテスト環境は、ヘルスチェックのテストにのみ使用します。本番稼働レベルのパフォーマンスと可用性を必要とする環境のヘルスチェックの関連付けのみを維持します。ステージングおよびテスト環境のために、Shield Advanced でヘルスチェックの関連付けを維持しないでください。

Shield Advanced によるヘルスチェックに一般的に使用される CloudWatch メトリクス

このセクションには、Distributed Denial of Service (DDoS) イベント中のアプリケーションのヘルスを測定するためのヘルスチェックで一般的に使用される Amazon CloudWatch メトリクスが記載されています。各リソースタイプの CloudWatch メトリクスに関する詳細については、表の後のリストを参照してください。

トピック

- アプリケーションのヘルスをモニタリングするために使用されるメトリクス
- 各リソースタイプの Amazon CloudWatch メトリクス

アプリケーションのヘルスをモニタリングするために使用されるメトリクス

リソース	メトリクス	説明
Route 53	`HealthCheckStatus`	ヘルスチェックエンドポイントのステータス。
CloudFront	`5xxErrorRate`	HTTP ステータスコードが 5xx であるすべてのリクエストの割合。これは、アプリケーションに影響を与えている攻撃を示しています。
Application Load Balancer	`HTTPCode_ELB_5XX_Count`	ロードバランサーによって生成された HTTP 5xx クライアントエラーコードの数。
Application Load Balancer	`RejectedConnectionCount`	ロードバランサーが接続の最大数に達したため、拒否された接続の数。
Application Load Balancer	`TargetConnectionErrorCount`	ロードバランサーとターゲット間で正常に確立されなかった接続数。
Application Load Balancer	`TargetResponseTime`	

リソース	メトリクス	説明
		リクエストがロードバランサーを離れてから、ターゲットからの応答を受信するまでの経過時間 (秒)。
Application Load Balancer	`UnHealthyHostCount`	異常とみなされるターゲットの数。
Amazon EC2	`CPUUtilization`	割り当てられた EC2 コンピューティングユニットのうち、現在使用されているものの割合。

各リソースタイプの Amazon CloudWatch メトリクス

保護されたリソースのために使用できるメトリクスの詳細については、リソースガイドの次のセクションを参照してください。

- Amazon Route 53 – 「Amazon Route 53 デベロッパーガイド」の「Amazon Route 53 のヘルスチェックと Amazon CloudWatch を使用したリソースのモニタリング」。
- Amazon CloudFront – 「Amazon CloudFront デベロッパーガイド」の「Amazon CloudWatch による CloudFront のモニタリング」。
- Application Load Balancer – 「Application Load Balancer のユーザーガイド」の「Application Load Balancer の CloudWatch メトリクス」。
- Network Load Balancer – 「Network Load Balancer のユーザーガイド」の「Network Load Balancer の CloudWatch メトリクス」。
- AWS Global Accelerator – デベロッパーガイドの「 での Amazon CloudWatch AWS Global Accelerator の使用」。 AWS Global Accelerator
- Amazon Elastic Compute Cloud – https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ の「インスタンスの利用可能な CloudWatch メトリクスのリスト表示」。
- Amazon EC2 Auto Scaling – 「Amazon EC2 Auto Scaling ユーザーガイド」の「Monitoring CloudWatch metrics for your Auto Scaling groups and instances」(オートスケーリンググループおよびインスタンス用の CloudWatch メトリクスのモニタリング)。

Shield Advanced で保護されたリソースにヘルスチェックを関連付ける

次の手順は、Amazon Route 53 ヘルスチェックを保護されたリソースに関連付ける方法を示しています。

> **Note**
>
> ヘルスチェックを Shield Advanced 保護に関連付ける前に、ヘルスチェックが正常な状態であることを確認してください。詳細については、「Amazon Route 53 デベロッパーガイド」の「ヘルスチェックのステータスモニタリングと通知の受信」を参照してください。

ヘルスチェックを関連付けるには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF & Shield コンソールを開きます。
2. AWS Shield ナビゲーションペインで、保護されたリソースを選択します。
3. [Protections] (保護) タブで、ヘルスチェックに関連付けるリソースを選択します。
4. [Configure protections] (保護を設定) を選択します。
5. [Configure health check based DDoS detection - optional] (ヘルスチェックベースの DDoS 検出を設定 - オプション) ページが表示されるまで [Next] (次へ) を選択します。
6. [Associated Health Check] (ヘルスチェックを関連付ける) で、保護に関連付けるヘルスチェックの ID を選択します。

   > **Note**
   >
   > 必要なヘルスチェックが表示されない場合は、Route 53 コンソールに移動して、ヘルスチェックとその ID を検証します。詳細については、「ヘルスチェックの作成と更新」を参照してください。

7. 設定を完了するまで残りのページを順を追って確認します。[Protections] (保護) ページに、リソースについて、更新されたヘルスチェックの関連付けが一覧表示されます。
8. [Protections] (保護) ページで、新しく関連付けられたヘルスチェックが正常であるとレポートされていることを確認します。

   ヘルスチェックが異常を報告している間は、Shield Advanced でヘルスチェックの使用を正常に開始することはできません。そうすることで、Shield Advanced は非常に低いしきい値で誤検出

を検出し、Shield Response Team (SRT) がリソースにプロアクティブなエンゲージメントを提供する能力にも悪影響を及ぼす可能性があります。

新しく関連付けられたヘルスチェックで異常が報告されている場合は、次の手順を実行します。

a. Shield Advanced で、ヘルスチェックと保護機能の関連付けを解除します。

b. Amazon Route 53 のヘルスチェックの仕様を再確認し、アプリケーション全体のパフォーマンスと可用性を検証します。

c. アプリケーションが良好なヘルスのためのパラメータ内で実行され、ヘルスチェックが正常であると報告している場合は、Shield Advanced でのヘルスチェックの関連付けをもう一度お試しください。

ヘルスチェックの関連付け手順は、新しいヘルスチェックの関連付けを確立し、Shield Advanced で正常であると報告されると完了します。

Shield Advanced で保護されたリソースとヘルスチェックの関連解除する

次の手順は、保護されたリソースから Amazon Route 53 ヘルスチェックの関連付けを解除する方法を示しています。

ヘルスチェックの関連付けを解除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF & Shield コンソールを開きます。
2. AWS Shield ナビゲーションペインで、保護されたリソースを選択します。
3. [Protections] (保護) タブで、ヘルスチェックから関連付けを解除するリソースを選択します。
4. [Configure protections] (保護を設定) を選択します。
5. [Configure health check based DDoS detection - optional] (ヘルスチェックベースの DDoS 検出を設定 - オプション) ページが表示されるまで [Next] (次へ) を選択します。
6. [Associated Health Check] (関連付けられたヘルスチェック) で、- としてリストされている空のオプションを選択します。
7. 設定を完了するまで残りのページを順を追って確認します。

[Protections] (保護) ページでは、リソースのヘルスチェックフィールドが - に設定されます。これは、ヘルスチェックの関連付けがないことを示しています。

Shield Advanced でのヘルスチェックの関連ステータスの表示

保護に関連付けられているヘルスチェックのステータスは、 AWS WAF & Shield コンソールの [Protected resources] (保護されたリソース) ページと各リソースの詳細ページで確認できます。

- [Healthy] (正常) - ヘルスチェックが使用可能で、正常であると報告されています。
- [Unhealthy] (異常) - ヘルスチェックが使用可能で、異常があると報告されています。
- [Unavailable] (使用不可) - Shield Advanced によるヘルスチェックは使用できません。

[Unavailable] (使用不可) のヘルスチェックを解決するには

新しいヘルスチェックを作成して使用します。Shield Advanced でステータスが使用不可になった後、ヘルスチェックを再度関連付けないでください。

これらのステップの実行に関する詳細なガイダンスについては、前のトピックを参照してください。

1. Shield Advanced で、リソースからヘルスチェックの関連付けを解除します。
2. Route 53 で、リソースの新しいヘルスチェックを作成し、その ID を記録します。詳細については、「Amazon Route 53 デベロッパーガイド」の「ヘルスチェックの作成と更新」を参照してください。
3. Shield Advanced で、新しいヘルスチェックをリソースに関連付けます。

Shield Advanced のヘルスチェックの例

このセクションは、計算されたヘルスチェックで使用できるヘルスチェックの例を示します。計算されたヘルスチェックでは、多数の個別のヘルスチェックを使用して、組み合わせたステータスを決定します。個々のヘルスチェックのステータスは、エンドポイントのヘルスまたは Amazon CloudWatch メトリクスの状態に基づきます。ヘルスチェックを計算されたヘルスチェックに組み込んでから、個々のヘルスチェックの組み合わせられたヘルスステータスに基づいてヘルスをレポートするように、計算されたヘルスチェックを設定します。アプリケーションのパフォーマンスと可用性の要件に応じて、計算されたヘルスチェックの感度をチューニングします。

計算されたヘルスチェックの詳細については、「Amazon Route 53 デベロッパーガイド」の「他のヘルスチェック (算出したヘルスチェック) のモニタリング」を参照してください。詳細については、「Route 53 Improvements – Calculated Health Checks and Latency Checks」(Route 53 の改善 – 計算されたヘルスチェックとレイテンシーチェック) のブログ記事を参照してください。

トピック

- Amazon CloudFront ディストリビューション
- ロードバランサー
- Amazon EC2 Elastic IP アドレス (EIP)

Amazon CloudFront ディストリビューション

次の例では、CloudFront ディストリビューションの計算されたヘルスチェックと組み合わせることができるヘルスチェックについて説明します。

- 動的コンテンツを提供するディストリビューション上のパスへのドメイン名を指定して、エンドポイントをモニタリングします。正常な応答には、HTTP レスポンスコード 2xx と 3xx が含まれます。
- CloudFront オリジンのヘルスを測定する CloudWatch アラームの状態をモニタリングします。例えば、Application Load Balancer メトリクス `TargetResponseTime` で CloudWatch アラームを維持し、アラームのステータスを反映するヘルスチェックを作成できます。ヘルスチェックは、応答時間 (リクエストがロードバランサーから発信されてから、ロードバランサーがターゲットから応答を受け取るまでの時間) がアラームで設定されたしきい値を超えると、異常になることがあります。
- レスポンスの HTTP ステータスコードが 5xx であるリクエストの割合を測定する CloudWatch アラームの状態をモニタリングします。CloudFront ディストリビューションの 5xx エラーレートが CloudWatch アラームで定義されたしきい値よりも高い場合、このヘルスチェックのステータスは異常に切り替わります。

ロードバランサー

次の例では、Application Load Balancer、Network Load Balancer、または Global Accelerator 標準アクセラレーターの計算されたヘルスチェックで使用できるヘルスチェックについて説明します。

- クライアントがロードバランサーに対して確立した新しい接続の数を測定する CloudWatch アラームの状態をモニタリングします。新しい接続の平均数に関するアラームのしきい値は、毎日の平均よりある程度高い値に設定できます。各リソースタイプのメトリクスは次のとおりです。
  - Application Load Balancer: `NewConnectionCount`
  - Network Load Balancer: `ActiveFlowCount`
  - Global Accelerator: `NewFlowCount`
- Application Load Balancer および Network Load Balancer では、正常とみなされるロードバランサーの数を測定する CloudWatch アラームの状態をモニタリングします。アラームのしきい値は、

アベイラビリティーゾーン、またはロードバランサーが必要とする最小数の正常なホストで設定できます。ロードバランサーのリソースで使用可能なメトリクスは次のとおりです。

- Application Load Balancer: `HealthyHostCount`
- Network Load Balancer: `HealthyHostCount`

- Application Load Balancer では、ロードバランサーのターゲットによって生成された HTTP 5xx レスポンスコードの数を測定する CloudWatch アラームの状態をモニタリングします。Application Load Balancer の場合、メトリクス `HTTPCode_Target_5XX_Count` を使用して、ロードバランサーのすべての 5xx エラーの合計に基づいてアラームしきい値を設定できます。

Amazon EC2 Elastic IP アドレス (EIP)

次のヘルスチェックの例を、Amazon EC2 Elastic IP アドレスの計算されたヘルスチェックに組み合わせることができます。

- Elastic IP アドレスへの IP アドレスを指定して、エンドポイントをモニタリングします。IP アドレスの背後にあるリソースと TCP 接続を確立できる限り、ヘルスチェックは正常なままです。
- 割り当てられた Amazon EC2 コンピューティングユニットのうち、現在インスタンス上で使用されているものが占める割合を測定する CloudWatch アラームの状態をモニタリングします。Amazon EC2 メトリクス `CPUUtilization` を使用して、高いと考えるアプリケーションの CPU 使用率 (90% など) に基づいてアラームしきい値を設定できます。

AWS リソースへの AWS Shield Advanced 保護の追加

Shield Advanced 保護を 1 つ以上のリソースに追加するには、このセクションのガイダンスに従います。

AWS リソースの保護を追加するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF & Shield コンソールを開きます。
2. ナビゲーションペインで、保護されたリソース AWS Shield を選択します。
3. [Add resources to protect] (保護するリソースを追加) を選択します。
4. [Choose resources to protect with Shield Advanced] (Shield Advanced で保護するリソースの選択) ページの [Specify the Region and resource types] (リージョンとリソースタイプの指定) で、保護するリソースのリージョンとリソースタイプの仕様を指定します。[All Regions] (すべてのリージョン) を選択すると複数のリージョンのリソースを保護でき、[Global] (グローバル) を選

択すると選択範囲をグローバルリソースに絞り込むことができます。保護しないリソースタイプは、すべて選択解除できます。リソースタイプの保護については、「が AWS Shield Advanced 保護するリソースのリスト」を参照してください。

5. [Load resources] (リソースをロード) を選択します。Shield Advanced は、[Select Resources] (リソースの選択) セクションに条件に一致する AWS リソースを入力します。
6. [Select Resources] (リソースの選択) セクションでは、リソースリストで検索する文字列を入力して、リソースのリストをフィルタリングできます。

   保護するリソースを選択します。
7. 作成しようとしている Shield Advanced 保護にタグを追加する場合は、[Tags] (タグ) セクションでそれらを指定します。 AWS リソースのタグ付けの詳細については、「タグエディタの使用」を参照してください。
8. [Protect with Shield Advanced] (Shield Advanced で保護) を選択します。これにより、Shield Advanced 保護がリソースに追加されます。

AWS Shield Advanced 保護の編集

AWS Shield Advanced 保護の設定はいつでも変更できます。これを行うには、選択した保護のオプションを確認し、変更する必要がある設定を変更します。

保護されたリソースを管理するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF & Shield コンソールを開きます。
2. AWS Shield ナビゲーションペインで、保護されたリソースを選択します。
3. [Protections] (保護) タブで、保護するリソースを選択します。
4. 必要な [Configure protections] (保護を設定) とリソース指定オプションを選択します。
5. 各リソース保護オプションを順を追って確認し、必要に応じて変更を行います。

アプリケーションレイヤー DDoS 保護を設定する

Amazon CloudFront および Application Load Balancer リソースに対する攻撃から保護するために、AWS WAF ウェブ ACLs を追加したり、レートベースのルールを追加したりできます。詳細については、「AWS WAF ウェブ ACLs と Shield Advanced によるアプリケーションレイヤーの保護」を参照してください。

Shield Advanced アプリケーションレイヤー DDoS 自動緩和機能を有効にすることもできます。の AWS WAF 仕組みについては、「」を参照してくださいAWS WAF。自動緩和機能の詳細については、「Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和」を参照してください。

> **Important**
>
> Shield Advanced ポリシー AWS Firewall Manager を使用して を通じて Shield Advanced 保護を管理する場合、ここではアプリケーションレイヤー保護を管理することはできません。他のすべてのリソースについては、ウェブ ACL にルールが含まれていない場合でも、少なくとも各リソースにウェブ ACL をアタッチすることをお勧めします。

> **Note**
>
> リソースのためにアプリケーションレイヤー DDoS 自動緩和を有効にすると、必要に応じて、オペレーションは、サービスにリンクされたロールをアカウントに自動的に追加し、ウェブ ACL 保護の管理に必要な許可を Shield Advanced に付与します。詳細については、「Shield Advanced のサービスにリンクされたロールの使用」を参照してください。

アプリケーションレイヤー DDoS 保護を設定するには

1. [Configure layer 7 DDoS protections] (レイヤー 7 DDoS 保護を設定) ページで、リソースがまだウェブ ACL に関連付けられていない場合は、既存のウェブ ACL を選択するか、独自のウェブ ACL を作成できます。

   ウェブ ACL を作成するには、次のステップに従います。

   a. [Create web ACL] (ウェブ ACL の作成) を選択します。
   b. 名前を入力します。ウェブ ACL の作成後は、名前を変更することはできません。
   c. [Create] (作成) を選択します。

   > **Note**
   >
   > リソースが既にウェブ ACL に関連付けられている場合、別のウェブ ACL に変更することはできません。ACL を変更する場合は、最初にリソースから関連するウェブ ACL を

削除します。詳細については、「AWS リソースとの保護の関連付けまたは関連付け解除」を参照してください。

2. ウェブ ACL にレートベースのルールが定義されていない場合は、[Add rate limit rule] (レート制限ルールを追加) を選択し、次のステップを実行してルールを追加できます。

   a. 名前を入力します。

   b. レート制限を入力します。これは、レートベースのルールアクションが IP アドレスに適用される前の任意の 5 分間に許可される、単一の IP アドレスからのリクエストの最大数です。IP アドレスからのリクエストが制限を下回ると、アクションは中止されます。

   c. リクエストの数が制限を超えている間に IP アドレスからのリクエストをカウントまたはブロックするルールアクションを設定します。ルールアクションの適用と削除は、IP アドレスのリクエストレートが変更されてから有効になるまでに 1 ~ 2 分かかる場合があります。

   d. [Add Rule] (ルールの追加) を選択します。

3. [Automatic application layer DDoS mitigation] (アプリケーションレイヤー DDoS 自動緩和) の場合、次のように、Shield Advanced がユーザーのために DDoS 攻撃を自動的に緩和するかどうかを選択します。

   - 自動緩和を有効にするには、有効化 を選択し、Shield Advanced がカスタム AWS WAF ルールで使用するルールアクションを選択します。選択内容は Count と Block です。これらの AWS WAF ルールアクションの詳細については、「」を参照してくださいでのルールアクションの使用 AWS WAF。Shield Advanced がこのアクション設定を管理する方法については、「Shield Advanced がルールアクション設定を管理する方法」を参照してください。
   - 自動緩和を無効にするには、[Disable] (無効化) を選択します。
   - 管理しているリソースの自動緩和設定を変更しない場合は、デフォルトの選択である [Keep current settings] (現在の設定を保持) のままにします。

   Shield Advanced アプリケーションレイヤー DDoS 自動緩和の詳細については、「Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和」を参照してください。

4. [次へ] を選択します。

Shield Advanced で保護されたリソースのアラームと通知の作成

次の手順では、保護されたリソースに関する CloudWatch アラームを管理する方法を示します。

> **Note**
>
> CloudWatch には追加料金が発生します。CloudWatch の料金については、「Amazon CloudWatch の料金」を参照してください。

アラームと通知を作成するには

1. 保護に関する [Create alarms and notifications - optional] (アラームと通知を作成 - オプション) ページで、受け取るアラームと通知の SNS トピックを設定します。通知が不要なリソースでは、[No topic] (トピックなし) を選択します。Amazon SNS トピックを追加するか、新しいトピックを作成できます。
2. Amazon SNS トピックを作成するには、次のステップに従います。
   a. ドロップダウンリストで、[Create an SNS topic] (SNS トピックを作成) を選択します。
   b. トピック名を入力します。
   c. オプションで、Amazon SNS メッセージの送信先メールアドレスを入力し、[Add email] (E メールの追加) を選択します。複数入力できます。
   d. [Create] (作成) を選択します。
3. [次へ] を選択します。

AWS リソースからの AWS Shield Advanced 保護の削除

任意の AWS リソースからいつでも AWS Shield Advanced 保護を削除できます。

> **Important**
>
> AWS リソースを削除しても、リソースは削除されません AWS Shield Advanced。また、この手順で説明されているように AWS Shield Advanced、 からリソースに対する保護を削除する必要があります。

AWS リソースから AWS Shield Advanced 保護を削除する

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF & Shield コンソールを開きます。
2. AWS Shield ナビゲーションペインで、保護されたリソースを選択します。

3. [Protections] (保護) タブで、保護を削除するリソースを選択します。
4. [Delete protections] (保護を削除) を選択します。
    - この保護用に設定された Amazon CloudWatch アラームがある場合は、このアラームを保護と一緒に削除するオプションが与えられます。この時点でアラームを削除しない場合は、代わりに CloudWatch コンソールを使用してアラームを後で削除することができます。

> **Note**
>
> Amazon Route 53 ヘルスチェックが設定されている保護は、後から再度追加した場合でも、保護にヘルスチェックが含まれます。

前述のステップでは、特定の AWS リソースから AWS Shield Advanced 保護を削除します。 AWS Shield Advanced サブスクリプションはキャンセルされません。このサービスに対しては引き続き料金が発生します。 AWS Shield Advanced サブスクリプションの詳細については、 AWS サポート センターにお問い合わせください。

CloudWatch アラームの Shield Advanced 保護からの削除

CloudWatch アラームを Shield Advanced 保護から削除するには、次のいずれかの操作を行います。

- 「AWS リソースからの AWS Shield Advanced 保護の削除」の説明に従って保護を削除します。[Also delete related DDoSDetection alarm] (関連する DDoSDetection アラームも削除する) の横にあるチェックボックスをオンにしてください。
- CloudWatch コンソールを使用してアラームを削除します。削除するアラームの名前は、DDoSDetectedAlarmForProtection で始まります。

AWS Shield Advanced 保護のグループ化

保護グループを使用して、保護されたリソースの論理コレクションを作成し、その保護をグループとして管理します。リソース保護の管理の詳細については、「AWS Shield Advanced 保護の編集」を参照してください。

> **Note**
>
> アプリケーションレイヤー DDoS 自動緩和は、保護グループとインタラクションしません。保護グループに含まれるリソースのために自動緩和を有効にできますが、Shield Advanced は、保護グループの検出結果に基づいて攻撃の緩和策を自動的に適用しません。Shield Advanced は、個々のリソースのために攻撃の自動緩和を適用します。

AWS Shield Advanced 保護グループを使用すると、複数の保護されたリソースを 1 つのユニットとして扱うことで、検出と緩和の範囲をセルフサービスでカスタマイズできます。リソースのグループ化は、多くのメリットをもたらす場合があります。

- 検出の精度を向上させます。
- 実行不可能なイベントの通知を減らします。
- イベント中に影響を受ける可能性のある保護されたリソースを含めるように、緩和アクションの対象範囲を拡大します。
- 複数の類似ターゲットに対する攻撃の緩和にかかる時間を短縮します。
- 新しく作成された保護対象リソースの自動保護を容易にします。

保護グループは、リソースがゼロ負荷に近い状態と完全に負荷がかかっている状態を交互に繰り返すブルー/グリーンスワップなどの状況で誤検出を減らすのに役立ちます。もう 1 つの例は、グループのメンバー間で共有されるロードレベルを維持しながら、リソースを頻繁に作成および削除する場合です。このような状況では、個々のリソースをモニタリングすると誤検出が発生する可能性がありますが、リソースグループのヘルスのモニタリングでは発生しません。

保護グループを設定して、すべての保護されたリソース、特定のリソースタイプのすべてのリソース、または個別に指定したリソースを含めることができます。保護グループの基準を満たす新しく保護されたリソースは、自動的に保護グループに含まれます。保護されたリソースは、複数の保護グループに所属できます。

Shield Advanced 保護グループの作成

保護グループを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF & Shield コンソールを開きます。
2. AWS Shield ナビゲーションペインで、保護されたリソースを選択します。

3. [Protection groups] (保護グループ) タブを選択してから、[Create protection group] (保護グループを作成) を選択します。
4. [Create protection group] (保護グループを作成) ページで、グループの名前を入力します。この名前を使用して、保護されたリソースのリスト内のグループを識別します。保護グループの作成後にその名前を変更することはできません。
5. [Protection grouping criteria] (保護のグループ化の基準) で、Shield Advanced がグループに含める保護されたリソースを識別するために使用する基準を選択します。選択した基準に基づいて追加の選択を行います。
6. [Aggregation] (集約) で、イベントの検出、緩和、およびレポートのために、Shield Advanced がグループのリソースデータをどのように組み合わせるかを選択します。

   - [Sum] (合計) – グループ全体のトラフィックの合計を使用します。これは、ほとんどの場合に適切な選択です。例には、手動または自動でスケールする Amazon EC2 インスタンスの Elastic IP アドレスが含まれます。
   - [Mean] (平均) – グループ全体のトラフィックの平均を使用します。これは、トラフィックを均一に共有するリソースに適した選択です。例には、アクセラレーターとロードバランサーが含まれます。
   - [Max] (最大) – 各リソースからの最大のトラフィックを使用します。これは、トラフィックを共有しないリソースや、不均一な方法でトラフィックを共有するリソースに有益です。例には、Amazon CloudFront ディストリビューションと CloudFront ディストリビューションのオリジンリソースが含まれます。
7. [Save] (保存) を選択して保護グループを保存し、[Protected resources] (保護されたリソース) ページに戻ります。

[Shield Events] (Shield イベント) ページでは、保護グループのイベントを表示し、ドリルダウンして、グループ内の保護されたリソースに関する追加情報を確認できます。

Shield Advanced 保護グループの更新

保護グループを更新するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF & Shield コンソールを開きます。
2. AWS Shield ナビゲーションペインで、保護されたリソースを選択します。
3. [Protection groups] (保護グループ) タブで、変更する保護グループの横にあるチェックボックスを選択します。

4. 保護グループのページで、[Edit] (編集) を選択します。保護グループの設定を変更します。
5. [Save] (保存) を選択して変更を保存します。

Shield Advanced 保護グループの削除

保護グループを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF & Shield コンソールを開きます。
2. AWS Shield ナビゲーションペインで、保護されたリソースを選択します。
3. [Protection groups] (保護グループ) タブで、削除する保護グループの横にあるチェックボックスを選択します。
4. 保護グループのページで、[Delete] (削除) を選択し、アクションを確認します。

での Shield Advanced リソース保護の変更の追跡 AWS Config

このページでは、 を使用してリソース AWS Shield Advanced の保護に対する変更を記録する方法について説明します AWS Config。この情報を使用して、監査およびトラブルシューティングのために設定変更履歴を維持することができます。

保護の変更を記録するには、追跡するリソース AWS Config ごとに を有効にします。詳細については、「AWS Config デベロッパーガイド」の」「AWS Configの使用開始」を参照してください。

追跡されたリソース AWS リージョン を含む各 AWS Config に対して を有効にする必要があります。 AWS Config 手動で を有効にすることも、 CloudFormation ユーザーガイドの StackSets サンプルテンプレートで CloudFormation テンプレート「有効化 AWS Config」を使用することもできます。 CloudFormation StackSets

有効にすると AWS Config、AWS Config 料金表ページの説明に従って課金されます。

> **Note**
>
> 必要なリージョンとリソースに対して を既に AWS Config 有効にしている場合は、リソースに対する保護の変更に関する . AWS Config logs が自動的に入力され始めます。

有効にしたら AWS Config、 AWS Config コンソールで米国東部 (バージニア北部) リージョンを使用して、 AWS Shield Advanced グローバルリソースの設定変更履歴を表示します。

米国東部 (バージニア北部)、米国東部 (オハイオ)、米国西部 (オレゴン)、米国西部 (北カリフォルニア)、欧州 (アイルランド)、欧州 (フランクフルト)、アジアパシフィック (東京)、アジアパシフィック (シドニー) の各リージョンで、 AWS Config コンソールを使用して AWS Shield Advanced リージョンリソースの変更履歴を表示します。

Shield Advanced による DDoS イベントの可視性

AWS Shield は、以下のカテゴリのイベントとイベントアクティビティを可視化します。

- グローバル – すべてのお客様は、直近 2 週間のグローバル脅威アクティビティの集約ビューにアクセスできます。この情報は、 AWS Shield コンソールの「開始方法」ページと「グローバル脅威ダッシュボード」ページに表示されます。詳細については、「AWS Shield グローバルアクティビティとアカウントアクティビティの表示」を参照してください。
- アカウント - すべてのお客様は、前年度のアカウントのイベントの概要にアクセスできます。この情報は、 AWS Shield コンソールの開始方法ページに表示されます。詳細については、「AWS Shield グローバルアクティビティとアカウントアクティビティの表示」を参照してください。

Shield Advanced をサブスクライブしてリソースに保護を追加すると、保護されたリソースに対するイベントや DDoS 攻撃に関する追加情報にアクセスできます。

- 保護されたリソースのイベント – Shield Advanced は、 AWS Shield コンソールのイベントページを通じて各イベントの詳細情報を提供します。詳細については、「AWS Shield Advanced イベントの表示」を参照してください。
- 保護されたリソースのイベントメトリクス – Shield Advanced は、保護するすべてのリソースの検出、緩和、上位寄稿者の Amazon CloudWatch メトリクスを発行します。これらのメトリクスを使用して、CloudWatch ダッシュボードとアラームを設定できます。詳細については、「AWS Shield Advanced メトリクス」を参照してください。
- 保護されたリソースのクロスアカウントイベントの可視性 – AWS Firewall Manager を使用して Shield Advanced 保護を管理する場合、Firewall Manager を組み合わせて使用することで、複数のアカウントにわたる保護の可視性を有効にできます AWS Security Hub CSPM。詳細については、「AWS Firewall Manager と AWS アカウント を使用して複数の にまたがる Shield Advanced イベントを表示する AWS Security Hub CSPM」を参照してください。

アプリケーションレイヤー保護の自動アプリケーションレイヤー DDoS 緩和を有効にすると、Shield Advanced は自動保護の管理に使用するルールグループを保護パック (ウェブ ACL) に追加します。このルールグループは AWS WAF メトリクスを生成しますが、表示することはできません。これ

は、 AWS マネージドルールルールグループなど、保護パック (ウェブ ACL) で使用する他のルールグループと同じですが、所有していません。 AWS WAF メトリクスの詳細については、「」を参照してくださいAWS WAF メトリクスとディメンション。Shield Advanced 保護オプションの機能については、Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和 を参照してください。

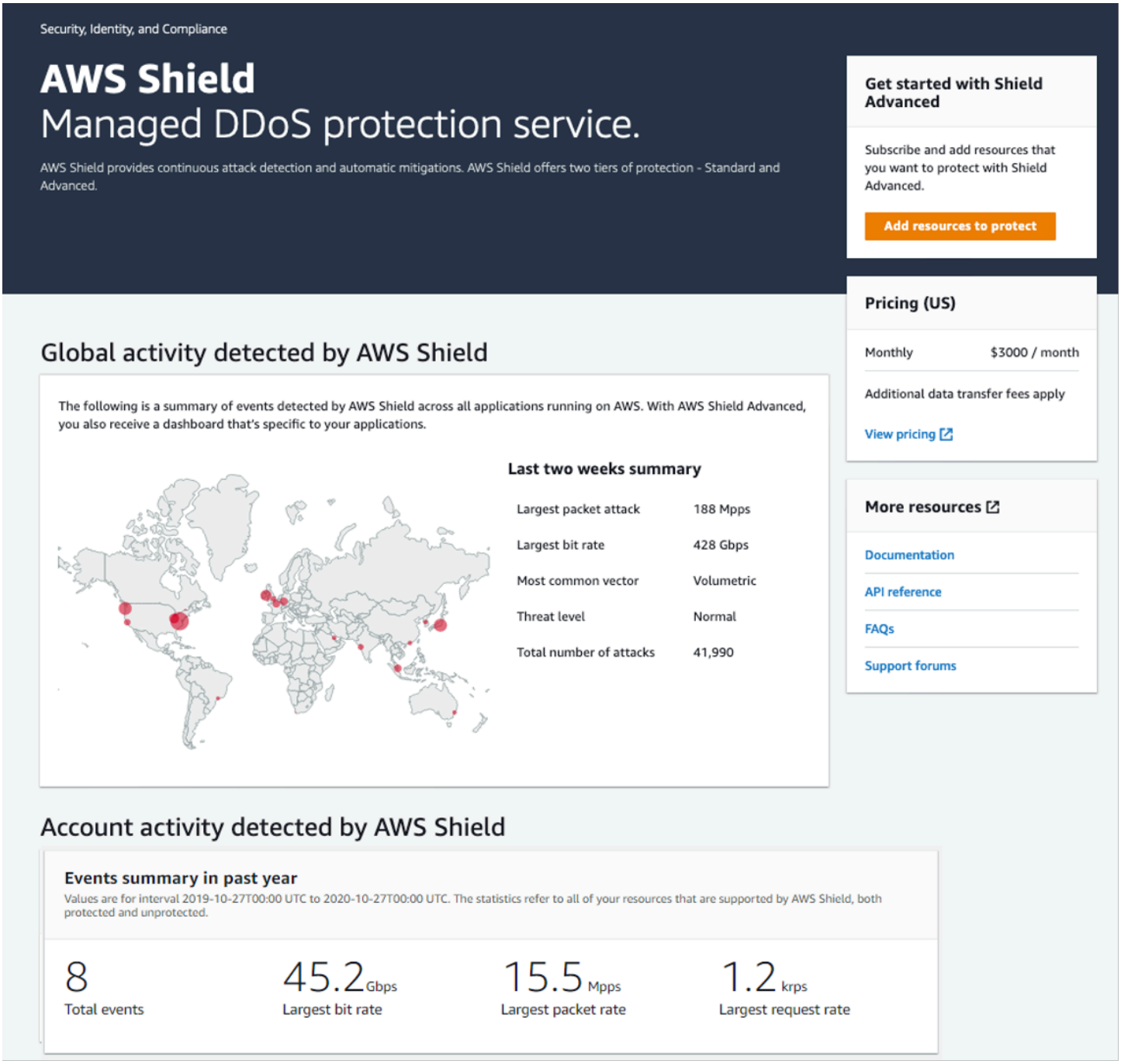
トピック

- AWS Shield グローバルアクティビティとアカウントアクティビティの表示
- AWS Shield Advanced イベントの表示
- AWS Firewall Manager と AWS アカウント を使用して複数の にまたがる Shield Advanced イベントを表示する AWS Security Hub CSPM

AWS Shield グローバルアクティビティとアカウントアクティビティの表示

このページでは、 AWS Shield コンソールの「開始方法」ページと「グローバル脅威ダッシュボード」ページで、グローバル脅威アクティビティの集約ビューとアカウントごとのイベント概要にアクセスする手順について説明します。

次のスクリーンショットは、[Getting Started] (開始方法) ページの例を示しています。



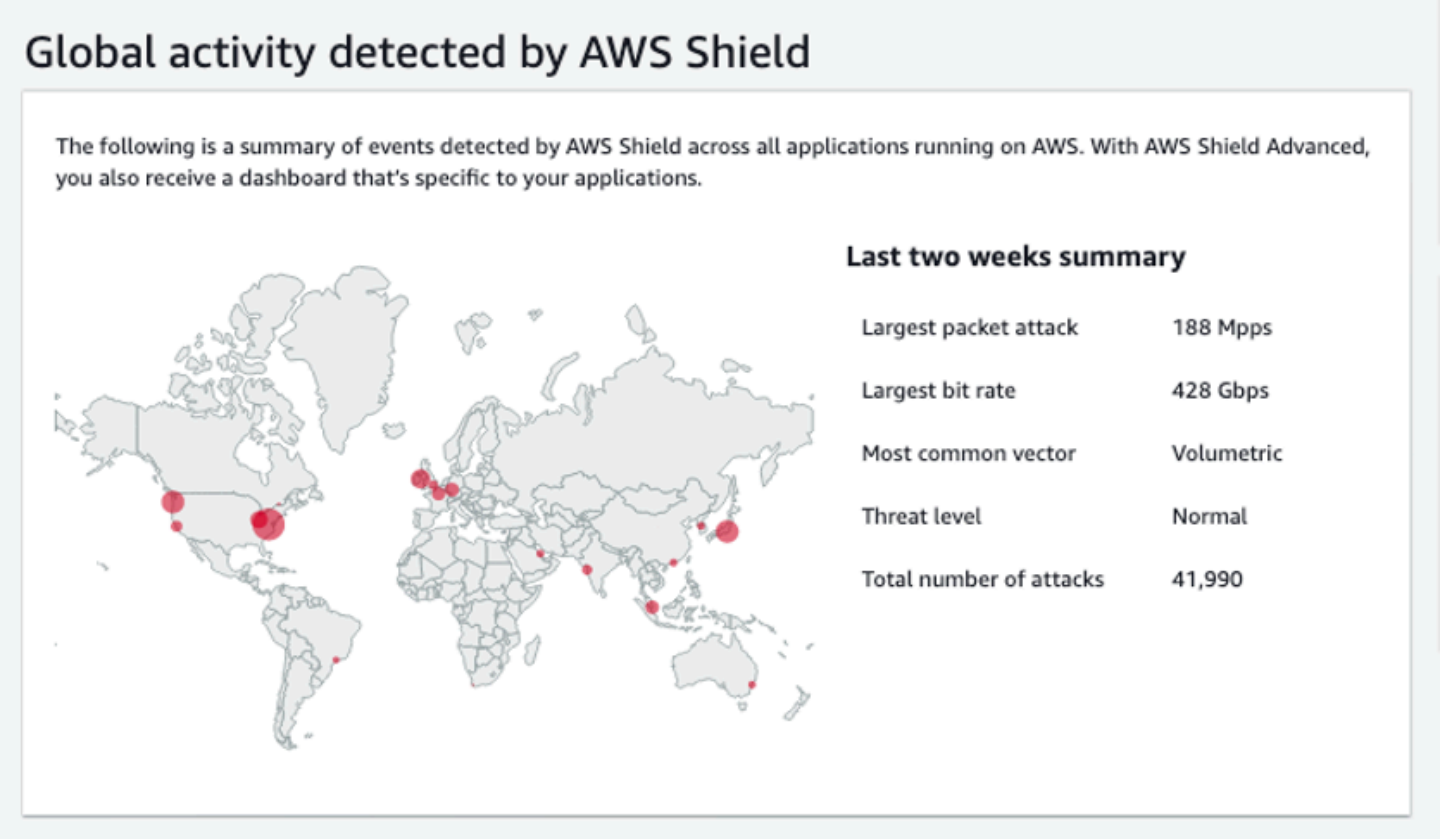
AWS Shield コンソールにアクセスするには

- にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF & Shield コンソールを開きます。

グローバルアクティビティとアカウントイベントの概要情報にアクセスするために、Shield Advanced のサブスクリプションは必要ありません。

グローバルアクティビティ

この情報は、 AWS Shield コンソールのグローバル脅威ダッシュボードと開始方法ページから入手できます。次のスクリーンショットは、グローバルアクティビティペインの例を示しています。



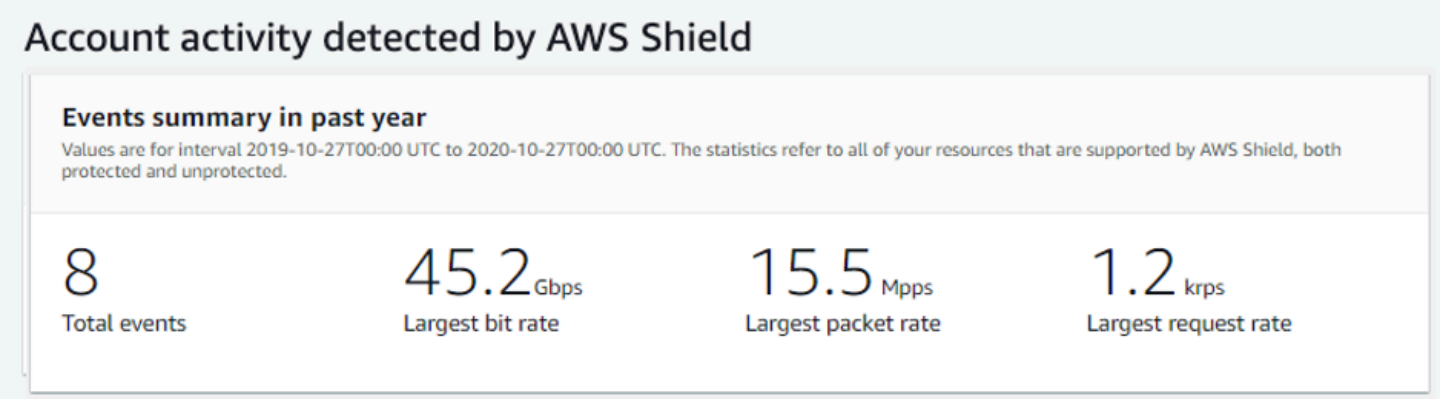
グローバルアクティビティは、すべての AWS お客様に見られる DDoS イベントを記述します。1 時間に 1 回、 は過去 2 週間の情報 AWS を更新します。コンソールペインで、 AWS リージョンごとにパーティション分割され、ワールドヒートマップに表示される結果を確認できます。マップの横には、最大パケット攻撃、最大ビットレート、最も一般的なベクトル、Shield の総数、脅威レベルなどの概要情報が表示されます。脅威レベルは、 AWS が通常観察するものと比較した現在のグローバルアクティビティの評価です。デフォルトの脅威レベル値は [Normal] (通常) です。 AWS は、昇格された DDoS アクティビティの値を自動的に [High] (高) に更新します。

[Global threat dashboard] (グローバル脅威ダッシュボード) は、時系列メトリクスも提供し、期間の変更を可能にします。重大な DDoS 攻撃の履歴を表示するには、ダッシュボードをカスタマイズして、最終日から過去 2 週間までを表示できます。時系列メトリクスは、選択した時間枠 AWS 内にで実行されている AWS Shield アプリケーションについて、 によって検出されたすべてのイベントの最大ビットレート、パケットレート、またはリクエストレートを表示します。

アカウントアクティビティ

この情報は、 AWS Shield コンソールの開始方法ページで確認できます。

次のスクリーンショットは、アカウントアクティビティペインの例を示しています。



アカウントアクティビティは、Shield Advanced による保護の対象となるリソースに関して Shield が検出した DDoS イベントを明らかにします。毎日、Shield は前日の 00:00 UTC で終わる 1 年の概要メトリクスを作成し、イベントの合計、最大ビットレート、最大パケットレート、および最大リクエストレートを表示します。

- Shield がアプリケーションを宛先とするトラフィックで疑わしい属性を観察するたびに、合計イベントメトリクスで反映されます。疑わしい属性には、通常のボリュームよりも大きいトラフィック、アプリケーションの過去のプロファイルに一致しないトラフィック、有効なアプリケーショントラフィック用に Shield で定義されているヒューリスティックに一致しないトラフィックが含まる場合があります。
- すべてのリソースで、最大ビットレートと最大のパケットレートの統計情報を使用できます。
- 最大リクエストレート統計は、 AWS WAF ウェブ ACL が関連付けられている Amazon CloudFront ディストリビューションと Application Load Balancer でのみ使用できます。

> **Note**
>
> AWS Shield API オペレーション DescribeAttackStatistics を使用して、アカウントレベルのイベント概要にアクセスすることもできます。

AWS Shield Advanced イベントの表示

このページでは、Shield Advanced のイベントに関する情報にアクセスする手順について説明します。

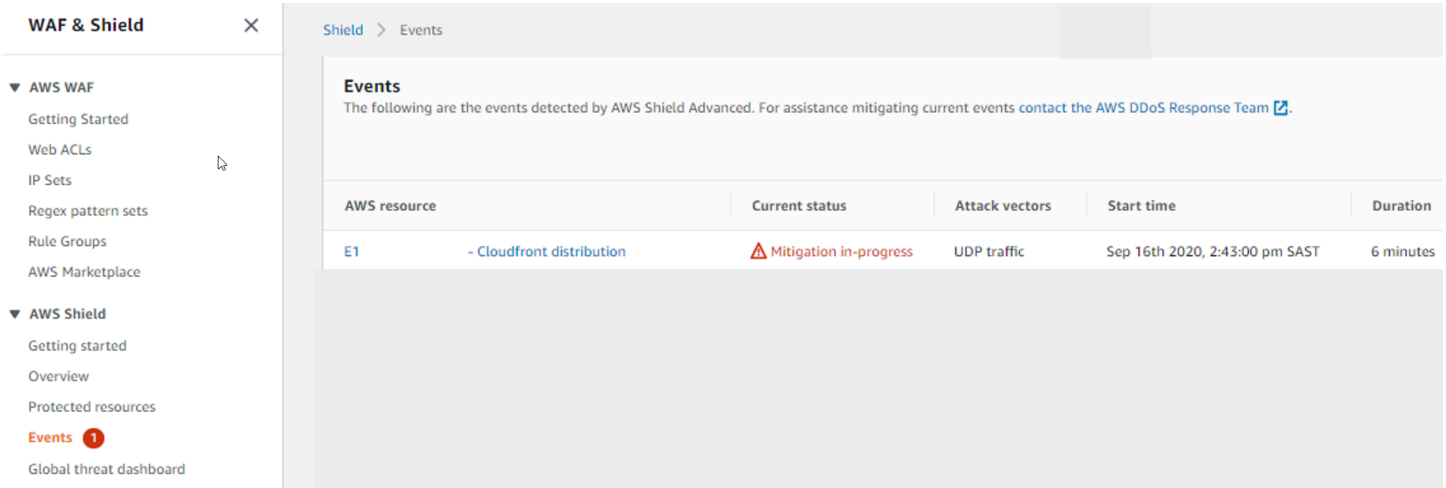
Shield Advanced をサブスクライブしてリソースを保護すると、リソースの追加の可視性機能にアクセスできます。これには、Shield Advanced によって検出されたイベントのほぼリアルタイムの通知や、検出されたイベントおよび緩和に関する追加情報が含まれます。

> **Note**
>
> Shield Advanced コンソールのイベント情報は、Shield Advanced メトリクスに基づいています。Shield Advanced メトリクスについては、AWS Shield Advanced メトリクス を参照してください。

AWS Shield は、複数のディメンションに沿って保護されたリソースへのトラフィックを評価します。異常が検出されると、Shield Advanced は影響を受けるリソースごとに個別のイベントを作成します。

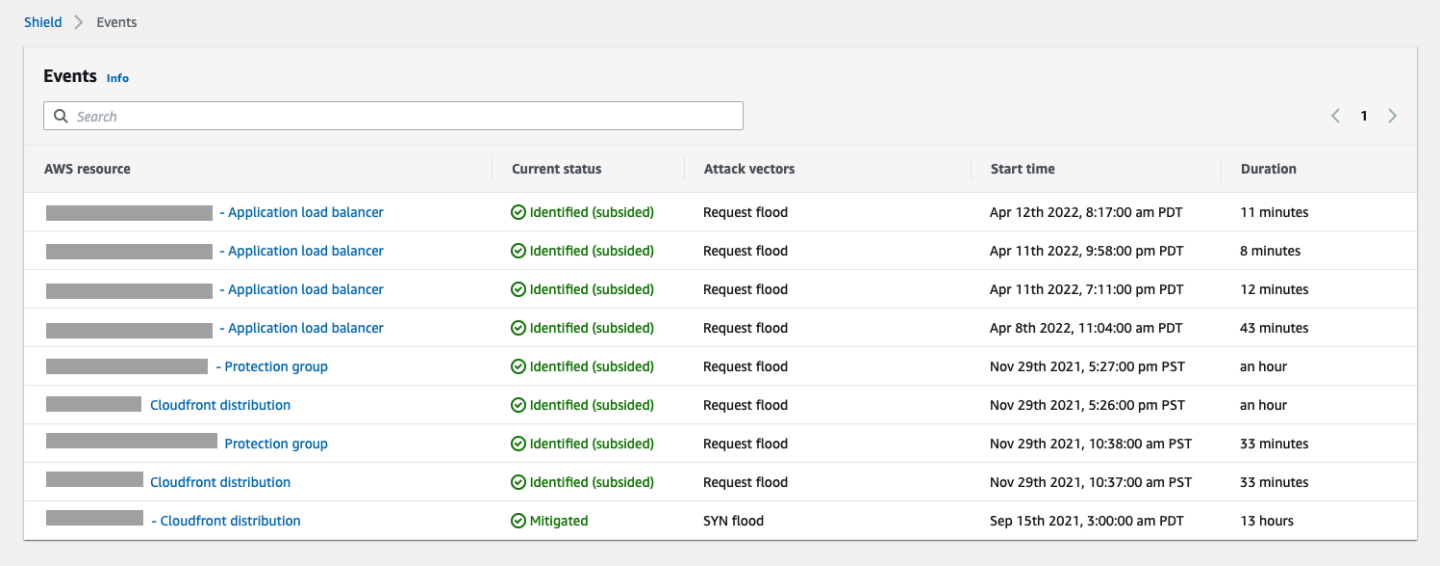
Shield コンソールの [Events] (イベント) ページからイベントの概要と詳細にアクセスできます。上位レベルの [Events] (イベント) ページには、現在および過去のイベントの概要が表示されます。

次のスクリーンショットは、単一の進行中のイベントを含む [Events] (イベント) ページの例を示しています。このアクティブなイベントには、左側のナビゲーションペインにもフラグが立てられます。



また、Shield Advanced は、トラフィックの種類と設定された保護に応じて、攻撃に対する緩和策を自動的に実施する場合があります。これらの緩和策により、過剰なトラフィックを受信したり、既知の DDoS 攻撃シグネチャに一致するトラフィックを受信したりしないようにリソースを保護できます。

次のスクリーンショットは、すべてのイベントが Shield Advanced によって緩和されたか、自然に沈静化した [Events] (イベント) のリストの例を示しています。



イベントが発生する前にリソースを保護する

DDoS 攻撃の対象となる前に、通常の予想トラフィックを受信している間に Shield Advanced でリソースを保護することで、イベント検出の精度を向上させます。

保護されたリソースのイベントを正確に報告するには、Shield Advanced はまずそのリソースの想定されるトラフィックパターンのベースラインを確立する必要があります。

- Shield Advanced は、少なくとも 15 分間保護されたリソースのインフラストラクチャレイヤーイベントをレポートします。
- Shield Advanced は、少なくとも 24 時間保護されたリソースのウェブアプリケーションレイヤーイベントをレポートします。アプリケーションレイヤーのイベントの検出精度は、Shield Advanced が 30 日間にわたって想定されるトラフィックをモニタリングした後に最適となります。

AWS Shield コンソールでイベント情報にアクセスするには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/ で AWS WAF & Shield コンソールを開きます。
2. AWS Shield ナビゲーションペインで、イベントを選択します。コンソールに [Events] (イベント) ページが表示されます。

3. [Events] (イベント) ページから、リスト内の任意のイベントを選択して、イベントの追加の概要情報と詳細を表示できます。

トピック

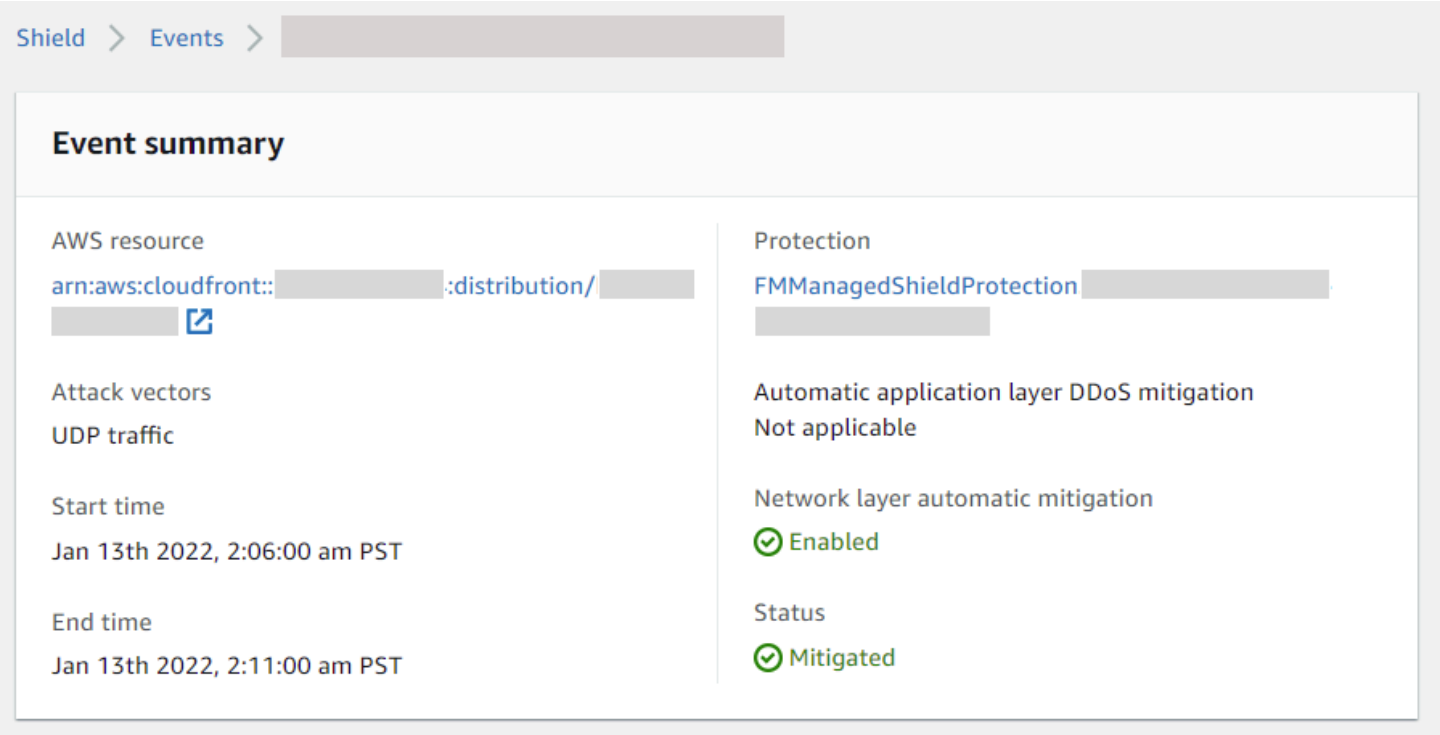
- AWS Shield Advanced イベント概要のフィールドのリスト
- AWS Shield Advanced イベントの詳細の表示

AWS Shield Advanced イベント概要のフィールドのリスト

このページでは、Shield Advanced イベント概要のフィールドを一覧表示して定義します。

イベントの概要と詳細情報は、イベントのコンソールページに表示できます。イベントのページを開くには、イベントページリストからその AWS リソース名を選択します。

次のスクリーンショットは、ネットワークレイヤーイベントのイベント概要の例を示しています。



イベントページの概要に関する情報には次が含まれます。

- [Current status] (現在のステータス) - イベントの状態と Shield Advanced がイベントに対して実行したアクションを示す値。ステータス値は、インフラストラクチャレイヤー (レイヤー 3 または 4) およびアプリケーションレイヤー (レイヤー 7) のイベントに適用されます。

  - [Identified (ongoing)] (識別済み (進行中)) および [Identified (subsided)] (識別済み (沈静化済み)) – これらは、Shield Advanced がイベントを検出したが、これまでのところアクションを実行していないことを示します。[Identified (subsided)] (識別済み (沈静化済み)) は、Shield が検出した疑わしいトラフィックが介入なしに停止したことを示します。
  - [Mitigation in progress] (緩和中) および [Mitigated] (緩和済み) – これらは、Shield Advanced がイベントを検出し、それに対してアクションが実行されたことを示します。[Mitigated] (緩和済み) は、ターゲットリソースが Amazon CloudFront ディストリビューションまたは Amazon Route 53 ホストゾーンであり、独自の自動インライン緩和機能がある場合にも使用されます。
- [Attack vectors] (攻撃ベクトル) - TCP SYN フラッドや Shield Advanced 検出ヒューリスティックなどの DDoS 攻撃ベクトル (リクエストフラッドなど)。これらは DDoS 攻撃を示している場合があります。
- [Start time] (開始時刻) – 最初の異常なトラフィックデータポイントが検出された日時。
- [Duration or end time] (期間または終了時刻) – イベントの開始時刻から Shield Advanced が最後に観察した異常なデータポイントまでの経過時間を示します。イベントが進行中であっても、これらの値は引き続き増加します。
- [Protection] (保護) – リソースに関連付けられている Shield Advanced 保護に名前を付け、その保護ページへのリンクを提供します。これは、個々のイベントのページで確認できます。
- [Automatic application layer DDoS mitigation] (アプリケーションレイヤーの DDoS の自動緩和) - Shield Advanced アプリケーションレイヤー DDoS 自動緩和がリソースのために有効になっているかどうかを示すために、アプリケーションレイヤーの保護に使用されます。有効になっている場合、これは、設定にアクセスして管理するためのリンクを提供します。これは、個々のイベントのページで確認できます。
- [Network layer automatic mitigation] (ネットワークレイヤーの自動緩和) – リソースがネットワークレイヤーで自動緩和されているかどうかを示します。リソースにネットワークレイヤーコンポーネントがある場合、これは有効になります。この情報は、個々のイベントのページで入手できます。

頻繁にターゲットが設定されるリソースの場合、Shield は、さらに繰り返し発生するイベントを防ぐために、過剰なトラフィックが沈静化した後も緩和策をそのままにすることができます。

> **Note**
>
> AWS Shield API オペレーション ListAttacks を通じて、保護されたリソースに関するイベントの概要にアクセスすることもできます。

AWS Shield Advanced イベントの詳細の表示

イベントのコンソールページの下部のセクションで、イベントの検出、緩和策、および上位の寄稿者に関する詳細を確認できます。このセクションには、正当なトラフィックと望ましくないものである可能性があるトラフィックが混在している可能性があり、保護されたリソースに渡されたトラフィックと Shield 緩和によってブロックされたトラフィックの両方が表われている場合があります。

- [検出と緩和] – 観察されたイベントと、それに対して適用された緩和策に関する情報を提供します。イベントの緩和については、「での DDoS イベントへの対応 AWS」を参照してください。
- [上位の寄稿者] – イベントに関係するトラフィックを分類し、Shield がカテゴリごとに特定したトラフィックの主要なソースを一覧表示します。アプリケーションレイヤーイベントの場合、上位の寄稿者情報を使用してイベントの性質に関する一般的なアイデアを取得しますが、セキュリティ上の意思決定には AWS WAF ログを使用します。詳細については、次のセクションを参照してください。

Shield Advanced コンソールのイベント情報は、Shield Advanced メトリクスに基づいています。Shield Advanced メトリクスについては、AWS Shield Advanced メトリクス を参照してください。

Amazon CloudFront または Amazon Route 53 リソースには緩和メトリクスは含まれません。これらのサービスは、常に有効になっている緩和システムによって保護されており、個別のリソース用の緩和策を必要としないためです。

詳細セクションは、情報がインフラストラクチャ層またはアプリケーションレイヤーイベントのどちらに関するものであるかによって異なります。

トピック

- Shield Advanced でのアプリケーションレイヤー (レイヤー 7) イベントの詳細の表示
- Shield Advanced でのインフラストラクチャレイヤー (レイヤー 3 または 4) イベントの詳細の表示

Shield Advanced でのアプリケーションレイヤー (レイヤー 7) イベントの詳細の表示

イベントの検出、緩和策、および上位の寄稿者に関する詳細は、イベントのコンソールページの下部のセクションで確認できます。このセクションには、正当なトラフィックと潜在的に望ましくないトラフィックの両方が含まれる可能性があり、保護対象のリソースに渡されたトラフィックと、Shield Advanced の緩和措置によってブロックされたトラフィックの両方を表す場合があります。

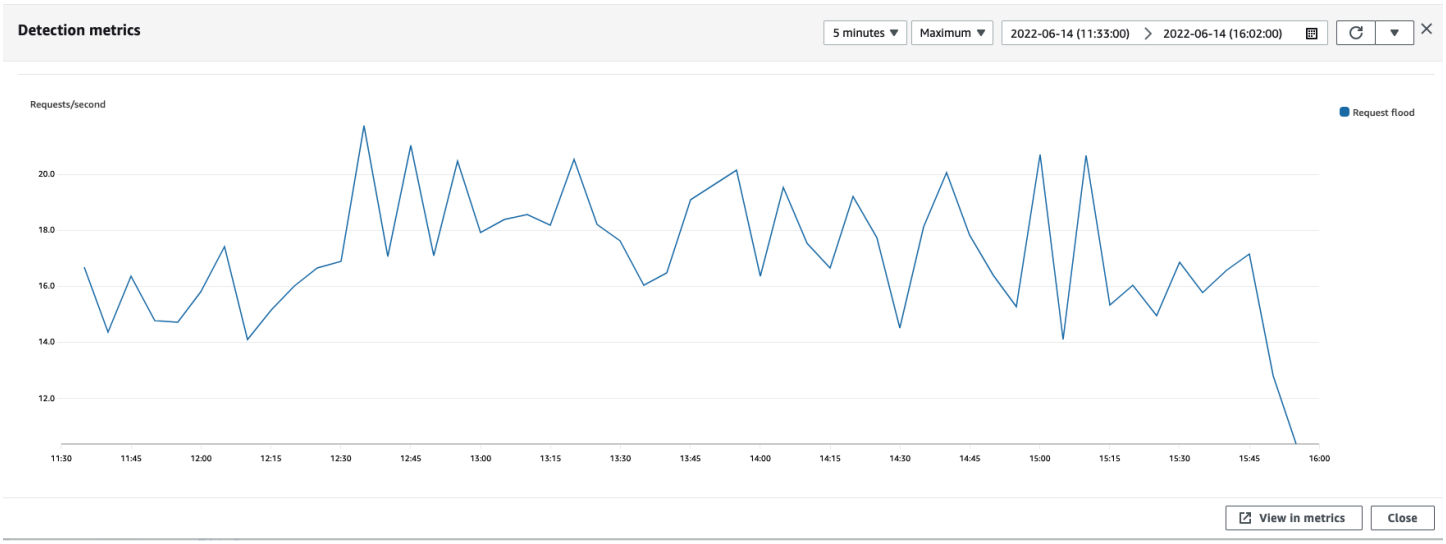
緩和策の詳細は、ウェブ ACL で定義されている攻撃やレートベースのルールに応じて特にデプロイされるルールなど、リソースに関連付けられているウェブ ACL 内のすべてのルールに関するものです。アプリケーションのアプリケーションレイヤー DDoS の自動緩和を有効にすると、緩和メトリクスにはこれらの追加ルールのメトリクスが含まれます。これらのアプリケーションレイヤー保護の詳細については、AWS Shield Advanced および を使用したアプリケーションレイヤー (レイヤー 7) の保護 AWS WAF を参照してください。

検出と緩和

アプリケーションレイヤー (レイヤー 7) イベントの場合、検出と緩和タブには、 AWS WAF ログから取得した情報に基づく検出メトリクスが表示されます。緩和メトリクスは、望ましくないトラフィックをブロックするように設定された、関連付けられたウェブ ACL の AWS WAF ルールに基づいています。

Amazon CloudFront ディストリビューションでは、自動緩和を適用するように Shield Advanced を設定できます。任意のアプリケーションレイヤーリソースを使用して、ウェブ ACL で独自の緩和ルールを定義することを選択したり、Shield レスポンスチーム (SRT、Shield Response Team) にサポートをリクエストしたりできます。これらのオプションについては、「での DDoS イベントへの対応 AWS」を参照してください。

次のスクリーンショットは、数時間後に沈静化したアプリケーションレイヤーイベントの検出メトリクスの例を示しています。



緩和ルールが有効になる前に沈静化するイベントトラフィックは、緩和メトリクスに表れません。これにより、検出グラフに表示されるウェブリクエストのトラフィックと、緩和グラフに表示される許可およびブロックメトリクスが異なることがあります。

上位の寄稿者

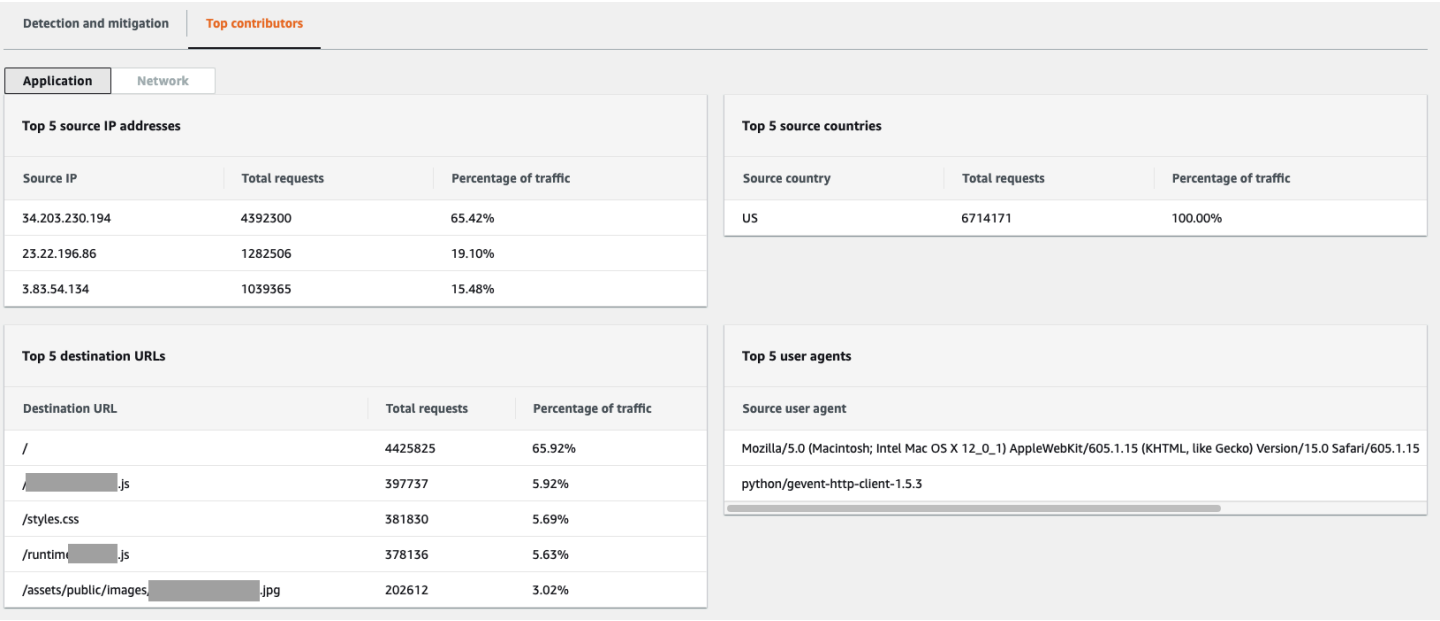
アプリケーションレイヤーイベントの上位寄与要因タブには、Shield が取得した AWS WAF ログに基づいてイベントで特定した上位 5 つの寄与要因が表示されます。Shield は、上位の寄稿者情報をソースIP、送信元国、送信先 URLなどのディメンションで分類します。

> **Note**
>
> アプリケーションレイヤーイベントに寄与しているトラフィックに関する最も正確な情報については、 AWS WAF ログを使用します。

Shield アプリケーションレイヤーの上位の寄稿者情報は、攻撃の性質を大まかに把握するためにのみ使用し、それに基づいてセキュリティ上の決定を行うべきではありません。アプリケーションレイヤーイベントの場合、 AWS WAF ログは攻撃の寄与要因を理解し、緩和戦略を考案するための最適な情報源です。

Shield の上位寄与要因情報は、必ずしも AWS WAF ログにデータを完全に反映しているとは限りません。Shield は、ログを取り込む際に、ログから完全なデータを取得することよりも、システムパフォーマンスへの影響を減らすことを優先します。その結果、Shield で分析に使用できるデータの粒度が失われる可能性があります。ほとんどの場合、情報の大部分は入手可能ですが、上位の寄稿者のデータは、攻撃によってはある程度偏る可能性があります。

次のスクリーンショットは、アプリケーションレイヤーイベントの [上位の寄稿者] タブの例を示しています。



コントリビューターに関する情報は、正当なトラフィックと望ましくない可能性があるトラフィックの両方に対するリクエストに基づいています。大量のイベントやリクエストソースが高度に分散されていないイベントは、識別可能な上位の寄稿者を持っている可能性が比較的高いです。大幅に分散した攻撃では、任意の数のソースが存在する可能性があり、攻撃の上位の寄稿者を特定することが困難です。Shield Advanced が特定のカテゴリの重要な寄稿者を特定しない場合、データは利用不可として表示されます。

Shield Advanced でのインフラストラクチャレイヤー (レイヤー 3 または 4) イベントの詳細の表示

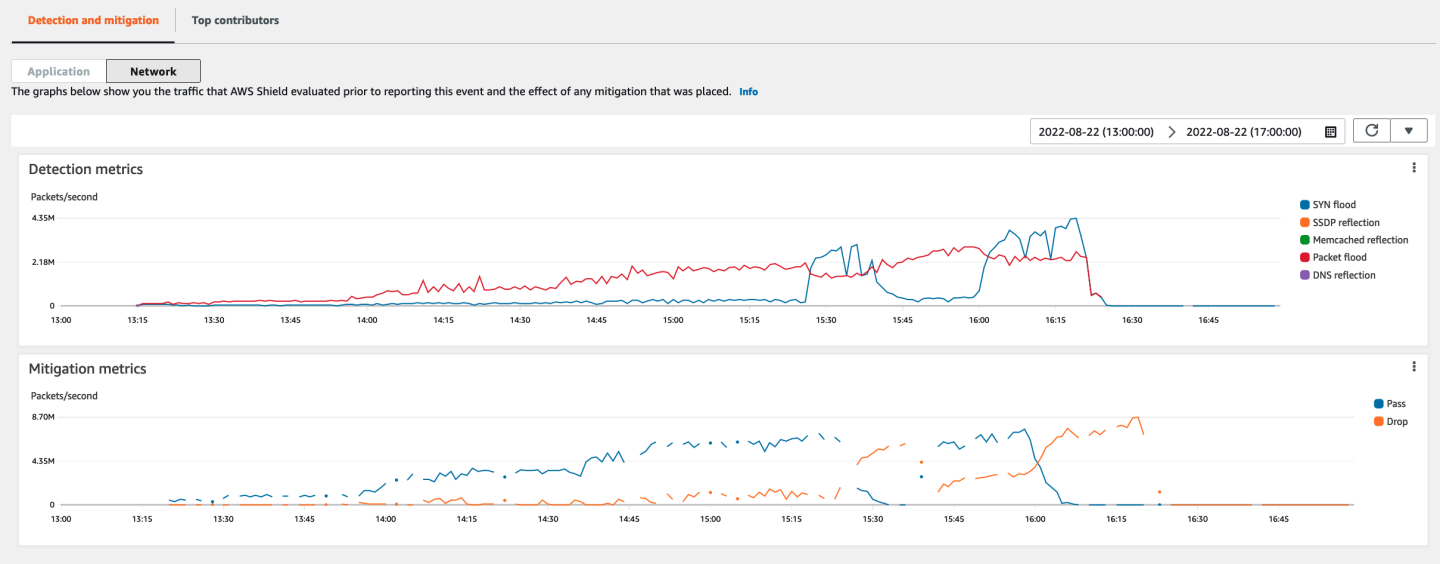
イベントのコンソールページの下部のセクションで、イベントの検出、緩和策、および上位の寄稿者に関する詳細を確認できます。このセクションには、正当なトラフィックと望ましくないものである可能性があるトラフィックが混在している可能性があり、保護されたリソースに渡されたトラフィックと Shield 緩和によってブロックされたトラフィックの両方が表われている場合があります。

検出と緩和

インフラストラクチャレイヤー (レイヤー 3 または 4) イベントの場合、[Detection and mitigation] (検出と緩和) タブには、サンプリングされたネットワークフローに基づく検出メトリクスと、緩和システムによって観察されたトラフィックに基づく緩和メトリクスが表示されます。緩和メトリクスは、リソースへのトラフィックをより正確に測定します。

Shield は、保護されたリソースタイプの緩和策 Elastic IP (EIP)、Classic Load Balancer (CLB)、Application Load Balancer (ALB)、および AWS Global Accelerator 標準アクセラレーターを自動的に作成します。EIP アドレスと AWS Global Accelerator 標準アクセラレーターの緩和メトリクスは、渡されたパケットとドロップされたパケットの数を示します。

次のスクリーンショットは、インフラストラクチャレイヤーイベントの [Detection and mitigation] (検出と緩和) タブの例を示しています。

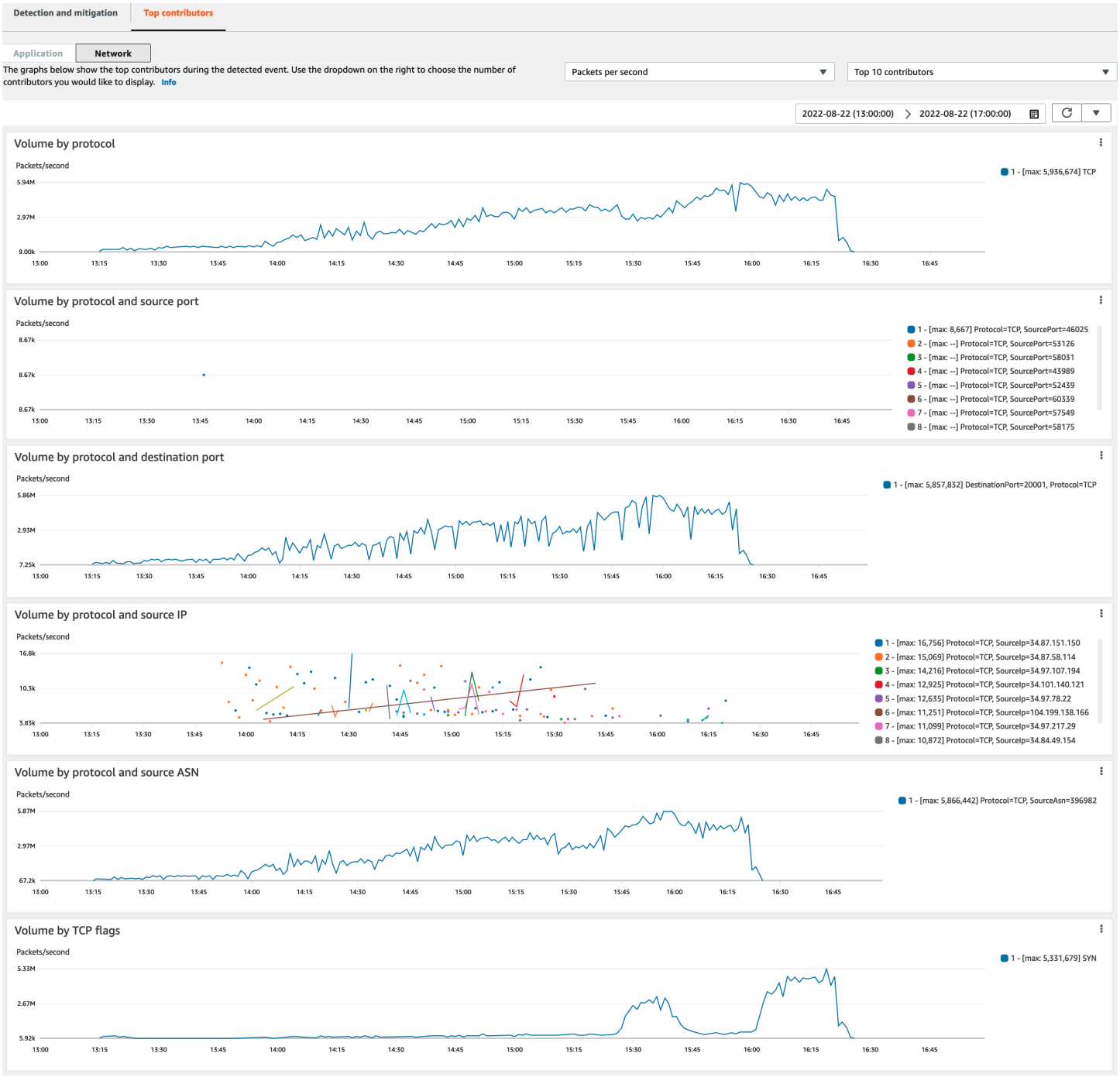


Shield が緩和策を行う前に沈静化するイベントトラフィックは、緩和メトリクスに表れません。これにより、検出グラフに表示されるトラフィックと、緩和グラフに表示されるパスおよびドロップメトリクスが異なることがあります。

上位の寄稿者

インフラストラクチャレイヤーイベントの [上位の寄稿者] タブには、いくつかのトラフィックディメンションで最大 100 の上位の寄稿者に関するメトリクスが一覧表示されます。詳細には、少なくとも 5 つの重要なトラフィックソースを特定できる任意のディメンションのネットワークレイヤープロパティが含まれます。トラフィックのソースの例としては、ソース IP とソース ASN があります。

次のスクリーンショットは、インフラストラクチャレイヤーイベントの [上位の寄稿者] タブの例を示しています。



コントリビューターメトリクスは、正当なトラフィックと望ましくない可能性があるトラフィックの両方についてサンプリングされたネットワークフローに基づいています。大量のイベントやトラフィックソースが高度に分散されていないイベントは、識別可能な上位の寄稿者を持っている可能性が比較的高いです。大幅に分散した攻撃では、任意の数のソースが存在する可能性があり、攻撃に対する上位の寄稿者を特定することが困難です。Shield が特定のメトリクスまたはカテゴリの重要な寄稿者を特定しない場合、データは利用不可として表示されます。

インフラストラクチャレイヤー DDoS 攻撃では、トラフィックソースがスプーフィングまたはリフレクトされる可能性があります。スプーフィングされたソースは、攻撃者によって意図的に偽造されます。反映されたソースは、検出されたトラフィックの実際のソースですが、攻撃に積極的に参加しているわけではありません。例えば、攻撃者は、通常は正当なインターネット上のサービスの攻撃を反射して、ターゲットに対する大規模で増幅されたトラフィックのフラッドを生成する可能性があります。この場合、ソース情報は、有効ではあるものの、実際の攻撃元ではない可能性があります。これらの要因により、パケットヘッダーに基づいてソースをブロックする緩和技術の実行可能性が制限される可能性があります。

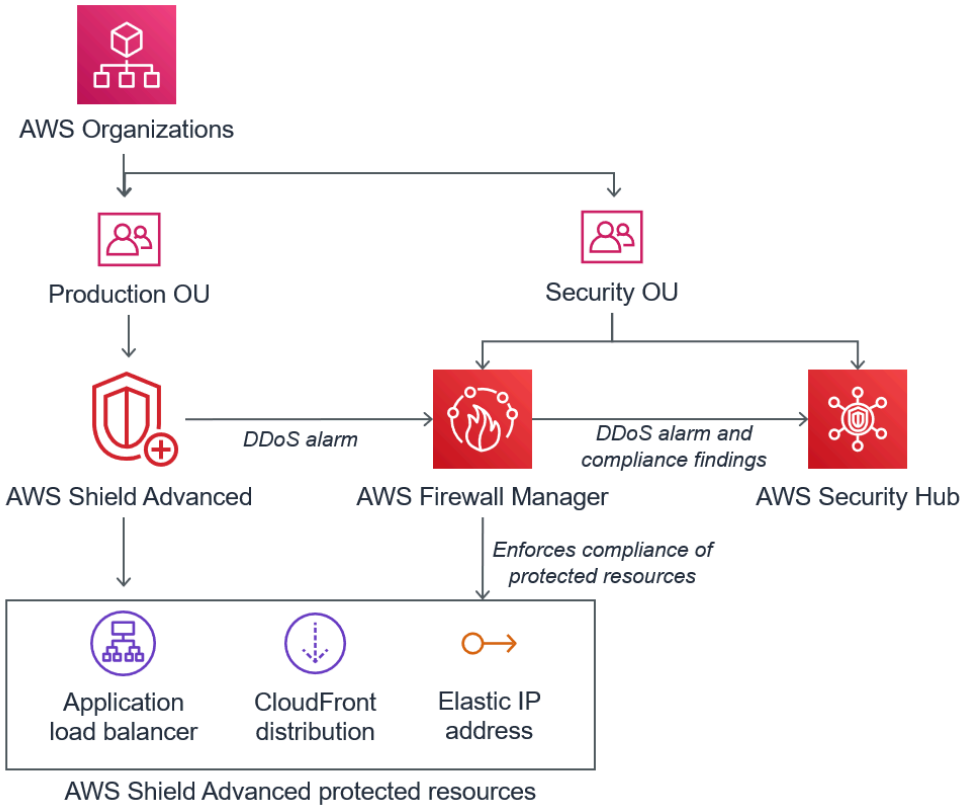
AWS Firewall Manager と AWS アカウント を使用して複数の にまたがる Shield Advanced イベントを表示する AWS Security Hub CSPM

AWS Firewall Manager と を使用して AWS Security Hub CSPM 、複数のアカウントで AWS Shield Advanced 保護されたリソースを管理およびモニタリングできます。

Firewall Manager を使用すると、すべてのアカウントで DDoS 保護のコンプライアンスを報告および適用する Shield Advanced セキュリティポリシーを作成できます。Firewall Manager は、Shield Advanced ポリシーの対象となる新しいリソースへの保護の追加を含め、保護されたリソースをモニタリングします。

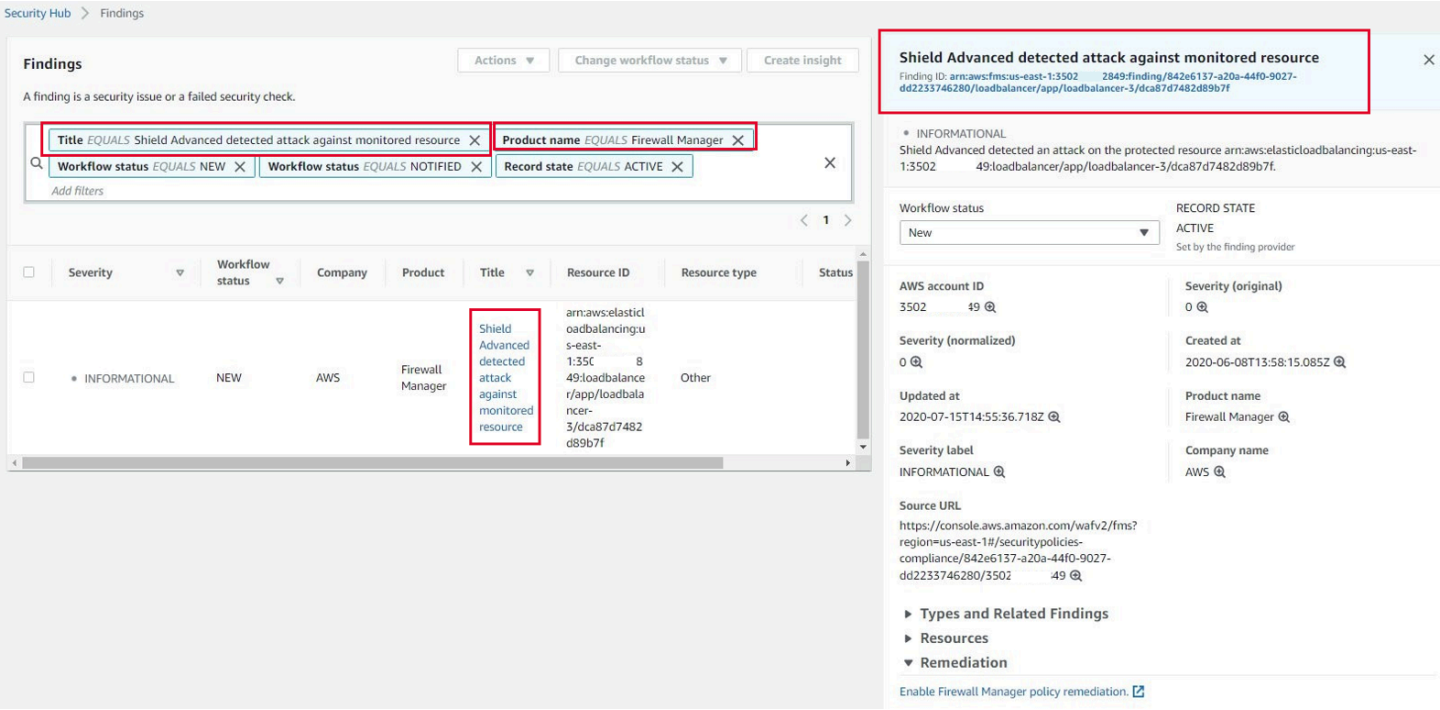
Firewall Manager を と統合 AWS Security Hub CSPM すると、Shield Advanced のセキュリティポリシーに準拠していないリソースを Firewall Manager が特定したときに、Shield Advanced と Firewall Manager のコンプライアンス検出結果によって検出された DDoS イベントを報告する単一のダッシュボードを取得できます。

次の図は、Firewall Manager と Security Hub CSPM を使用して Shield Advanced で保護されたリソースをモニタリングするための一般的なアーキテクチャを示しています。



Firewall Manager を Security Hub CSPM と統合すると、実行するアプリケーションの他のアラートやコンプライアンスステータス情報とともに、セキュリティ検出結果を 1 か所で表示できます AWS。

次のスクリーンショットは、このタイプの統合がある場合に Security Hub CSPM コンソール内で Shield Advanced イベントに表示される情報を示しています。



Firewall Manager と Security Hub CSPM を Shield Advanced と統合して、保護されたアカウント間でイベントとコンプライアンスのモニタリングを一元化する方法については、 AWS 「セキュリティブログ」のDDoS イベントの集中モニタリングのセットアップ」および「非準拠リソースの自動修復」を参照してください。

Shield Advanced 攻撃フローログ

フローログを使用すると、Shield Advanced で保護されたリソースのネットワークインターフェイスに送信されるトラフィックに関する情報をキャプチャできます。フローログデータは Amazon S3、Amazon CloudWatch Logs、または Amazon Data Firehose に発行され、フローログを有効にした後でデータを取得して表示できます。

> **Note**
>
> 米国東部 (バージニア北部) リージョンの Shield Advanced で保護されたリソースの CloudWatch メトリクスとログを表示する必要があります。これは、 コンソールと の両方に適用されます AWS CLI。を使用する場合は AWS CLI、次のパラメータを含めます。 `--region us-east-1`

> **Note**
>
> CloudWatch Logs の料金は、ログが Amazon S3 に直接公開されている場合でも、フローログを使用する場合に適用されます。詳細については、Amazon CloudWatch 料金表」の「ログ」タブの「Vended Logs」を参照してください。

フローログを Amazon S3 に発行できるようにする

Amazon S3 にフローログを発行するには、ログ配信アクションと Shield サービスの IAM アクセス許可を設定する必要があります。

フローログを発行するための IAM アクセス許可

フローログを Amazon S3 バケットに発行するには、IAM プリンシパル (例: IAM ロールまたはユーザー) に十分なアクセス許可が付与されている必要があります。IAM ポリシーには以下のアクセス許可が含まれています:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:GetDelivery",
                "logs:GetDeliverySource",
                "logs:PutDeliveryDestination",
                "logs:GetDeliveryDestinationPolicy",
                "logs:DeleteDeliverySource",
                "logs:PutDeliveryDestinationPolicy",
                "logs:CreateDelivery",
                "logs:GetDeliveryDestination",
                "logs:PutDeliverySource",
                "logs:DeleteDeliveryDestination",
                "logs:DeleteDeliveryDestinationPolicy",
                "logs:DeleteDelivery",
                "logs:UpdateDeliveryConfiguration"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:accountID:delivery:*",
                "arn:aws:logs:us-east-1:accountID:delivery-source:*",
```

```
                "arn:aws:logs:us-east-1:accountID:delivery-destination:*"
            ]
        },
        {
            "Sid": "ListAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeDeliveryDestinations",
                "logs:DescribeDeliverySources",
                "logs:DescribeDeliveries",
                "logs:DescribeConfigurationTemplates"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUpdatesToResourcePolicyS3",
            "Effect": "Allow",
            "Action": [
                "s3:PutBucketPolicy",
                "s3:GetBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::bucket-name"
        }
    ]
}
```

前述のポリシーでは、*accountID* を AWS アカウント ID に置き換え、*bucket-name* を Amazon S3 バケットの名前に置き換えます。

Shield サービス固有のアクセス許可

では、送信先固有のアクセス許可に加えて、リソースからログを送信できる明示的な認可 AWS Shield が必要です。これにより、追加のセキュリティレイヤーが提供されます。Shield は、ログを提供する保護リソースのAllowVendedLogDeliveryForResourceアクションを承認します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ServiceLevelAccessForLogDelivery",
            "Effect": "Allow",
            "Action": [
                "shield:AllowVendedLogDeliveryForResource"
```

```
            ],
            "Resource": "arn:aws:shield::accountID:protection/*"
        }
    ]
}
```

accountID を自分の AWS アカウント ID に置き換えます。

フローログ配信を有効にするには

作業ログ配信は 3 つの要素で構成されます。を使用して各要素を設定するには、次の手順に従いますAWS CLI。

1. ログを送信するリソースを表す論理オブジェクトDeliverySourceである を作成します。次のコマンドを実行します。

   ```
   aws logs put-delivery-source \
     --name delivery-source-name \
     --resource-arn "arn:aws:shield::accountID:protection/protectionID" \
     --log-type FLOW_LOGS \
     --region us-east-1
   ```

   delivery-source-name を配信ソースの名前に、*accountID* を AWS アカウント ID に、*protectionID* を Shield Advanced 保護 ID に置き換えます。

   このコマンドを発行するユーザーにサービスレベルのアクセス許可 があることを確認しますshield:AllowVendedLogDeliveryForResource。
2. 実際の配信先を表す論理オブジェクトDeliveryDestinationである を作成します。次のコマンドを実行します。

   ```
   aws logs put-delivery-destination \
     --name delivery-destination-name \
     --output-format json \
     --delivery-destination-configuration "destinationResourceArn=arn:aws:s3:::bucket-name" \
     --region us-east-1
   ```

   delivery-destination-name を配信先の名前に、*bucket-name* を Amazon S3 バケットの名前に置き換えます。
3. 配信ソースを配信先Deliveryに接続する を作成します。次のコマンドを実行します。

```
aws logs create-delivery \
  --delivery-source-name delivery-source-name-from-step1 \
  --delivery-destination-arn "arn-returned-in-step2" \
  --region us-east-1
```

delivery-source-name-from-step1 をステップ 1 の配信ソース名に置き換え、*arn-returned-in-step2* をステップ 2 で返された ARN に置き換えます。

フローログファイル

Shield 保護からのフローログは、攻撃中に 5 分間隔で Amazon S3 バケットに発行されます。ログファイルは 5 分ごとに書き込まれ、各ログファイルには、過去 5 分間に記録された IP アドレストラフィックのフローログレコードが含まれます。

ログファイルの最大ファイルサイズは 75 MB です。ログファイルが 5 分以内にこの制限に達すると、フローログはレコードの追加を停止します。その後、フローログはファイルを Amazon S3 バケットに発行し、新しいログファイルを作成します。

ログファイルは圧縮されます。Amazon S3 コンソールを使用してファイルを開くと、Amazon S3 はログレコードを解凍して表示します。ログファイルをダウンロードする場合、レコードを表示するには解凍する必要があります。

1 つのログファイルには、複数のレコードを含むインターリーブされたエントリが含まれます。保護のすべてのログファイルを表示するには、保護名、リージョン、アカウント ID で集計されたエントリを探します。

フローログレコードの構文

フローログレコードは、次のフィールドを含むスペース区切りの文字列です。

フィールド	説明
version	フローログのバージョン番号。
protection_arn	AWS Shield Advanced で保護されたリソースを識別する保護 ARN。
srcaddr	パケットの送信元 IP アドレス。

フィールド	説明
dstaddr	パケットの送信先 IP アドレス。
srcport	パケットのソースポート。
dstport	パケットの送信先ポート。
protocol	パケットのプロトコル。
packets	集約ウィンドウ内のパケットの数。
bytes	集約ウィンドウ内のバイト数。
starttime	集計ウィンドウの開始時刻。
endtime	集計ウィンドウの終了時刻。
action	Shield Advanced によって実行されたアクション。
tcp_flags	パケットの TCP フラグフィールド。
sampling_rate	パケット処理中に使用されるサンプリングレート。
location	AWS Ingress の場所。
srccountry	進入トラフィックの国を表す 2 文字の国コード。

での DDoS イベントへの対応 AWS

このページでは、 が DDoS 攻撃にどのように AWS 応答するかを説明し、さらに応答する方法のオプションを提供します。

AWS は、ネットワークレイヤーとトランスポートレイヤー (レイヤー 3 とレイヤー 4) の DDoS 攻撃を自動的に軽減します。Shield Advanced を使用して Amazon EC2 インスタンスを保護する場合、攻撃を受けている最中に、Shield Advanced は、Amazon VPC ネットワーク ACL を AWS ネットワークの境界に自動的にデプロイします。これにより、Shield Advanced は、大規模な DDoS イベントに対する保護を提供できます。ネットワーク ACL の詳細については、「ネットワーク ACL」を参照してください。

アプリケーションレイヤー (レイヤー 7) DDoS 攻撃の場合、CloudWatch AWS アラームを通じて AWS Shield Advanced 顧客を検出して通知しようとします。デフォルトでは、有効なユーザートラフィックが誤ってブロックされないように、緩和策は自動的に適用されません。

アプリケーションレイヤー (レイヤー 7) リソースでは、攻撃に対応するために次のオプションを使用できます。

- [Provide your own mitigations] (独自の緩和策を提供する) – 独自に攻撃を調査して緩和することができます。詳細については、「アプリケーションレイヤー DDoS 攻撃の手動による緩和」を参照してください。
- [Contact support] (サポートに問い合わせる) – Shield Advanced をご利用の場合は、AWS サポートセンター に問い合わせて緩和に関するサポートを受けることができます。重大かつ緊急のケースは DDoS エキスパートに直接、ルーティングされます。詳細については、「アプリケーションレイヤー DDoS 攻撃を受けている最中のサポートセンターへの問い合わせ」を参照してください。

さらに、攻撃が発生する前に、次の緩和オプションをプロアクティブに有効にできます。

- [Automatic mitigations on Amazon CloudFront distributions] (Amazon CloudFront ディストリビューションでの自動緩和) - このオプションを使用すると、Shield Advanced は、ウェブ ACL で緩和ルールを定義および管理します。アプリケーションレイヤーの自動緩和の詳細については、「Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和」を参照してください。
- プロアクティブエンゲージメント – がアプリケーションの 1 つに対する大規模なアプリケーションレイヤー攻撃 AWS Shield Advanced を検出すると、SRT はプロアクティブに連絡できます。SRT は DDoS イベントをトリアージし、 AWS WAF 緩和策を作成します。SRT はお客様に連絡し、お客様の同意を得て、 AWS WAF ルールを適用することができます。このオプションの詳細については、「SRT が直接連絡するためのプロアクティブエンゲージメントの設定」を参照してください。

アプリケーションレイヤー DDoS 攻撃を受けている最中のサポートセンターへの問い合わせ

このページでは、アプリケーションレイヤー DDoS 攻撃を受けている最中のサポートセンターへの問い合わせについて説明します。

AWS Shield Advanced のお客様は、 AWS サポート センターに連絡して緩和策についてサポートを受けることができます。重大かつ緊急のケースは DDoS エキスパートに直接、ルーティングされます。では AWS Shield Advanced、複雑なケースを AWS Shield Response Team (SRT) にエスカレー

ションできます。SRT は AWS、、Amazon.com とその子会社の保護において豊富な経験を持っています。SRT 関数の詳細については、「Shield Response Team (SRT) サポートによるマネージド DDoS イベントレスポンス」を参照してください。

Shield Response Team (SRT) のサポートを受けるには、AWS サポート Center に問い合わせてください。ケースへの応答時間は、選択した重要度と応答回数によって異なります (「AWS サポート プラン」ページを参照)。

次のオプションを選択してください。

- ケースタイプ: テクニカルサポート
- サービス: Distributed Denial of Service (DDoS)
- カテゴリ: へのインバウンド AWS
- 重要度: 適切なオプションを選択してください

担当者と話し合うときは、お客様が DDoS 攻撃の可能性がある AWS Shield Advanced と説明してください。担当者がお客様の問い合わせを適切な DDoS エキスパートに取り次ぎます。[Distributed Denial of Service (DDoS)] サービスタイプを使用して AWS サポート Center でケースを開いた場合は、チャットや電話で DDoS エキスパートと直接お話しいただけます。DDoS サポートエンジニアは、攻撃の特定、 AWS アーキテクチャの改善の推奨、DDoS 攻撃の軽減のための AWS サービスの使用に関するガイダンスの提供を支援します。

アプリケーションレイヤー攻撃の場合、SRT は疑わしいアクティビティを分析するのをサポートします。リソースについて自動緩和が有効になっている場合、SRT は Shield Advanced が攻撃に対して自動的に実施している緩和策を確認できます。いずれの場合でも、SRT は問題の確認と緩和をサポートできます。SRT が推奨する緩和策では、多くの場合、SRT がアカウントで AWS WAF ウェブアクセスコントロールリスト (ウェブ ACLs) を作成または更新する必要があります。SRT がこの作業を行うには、お客様の許可が必要となります。

> **Important**
>
> 有効化の一環として AWS Shield Advanced、SRT へのアクセスの許可「」の手順に従って、攻撃中に支援するために必要なアクセス許可を SRT に事前に提供することをお勧めします。事前に許可を付与することで、実際に攻撃が発生した場合の遅延を防ぐことができます。

SRT は、DDoS 攻撃を分類して、攻撃シグネチャとパターンを識別できるようにお客様を支援します。お客様の同意を得て、SRT は攻撃を軽減するための AWS WAF ルールを作成してデプロイします。

また、緩和策を確認したり、カスタム緩和策を開発してデプロイしたりするために、攻撃の可能性が生じる前であっても、または生じている最中に SRT に問い合わせることもできます。例えば、ウェブアプリケーションを実行していて、ポート 80 と 443 だけを開く必要がある場合は、SRT と連携してポート 80 と 443 だけを [Allow] (許可) するようにウェブ ACL を事前設定できます。

SRT への連絡と承認はアカウントレベルで行います。つまり、Firewall Manager Shield Advanced ポリシー内で Shield Advanced を使用する場合、アカウント所有者 (Firewall Manager 管理者ではない) は SRT にサポートを依頼する必要があります。Firewall Manager 管理者は、所有しているアカウントに関してのみ SRT に問い合わせることができます。

アプリケーションレイヤー DDoS 攻撃の手動による緩和

このページでは、アプリケーションレイヤーの DDoS 攻撃を手動で軽減する手順について説明します。

リソースのイベントページのアクティビティが DDoS 攻撃を表していると判断した場合は、ウェブ ACL に独自の AWS WAF ルールを作成して攻撃を軽減できます。これは、Shield Advanced のお客様でない場合に使用できる唯一のオプションです。 AWS WAF は追加料金なしで AWS Shield Advanced に含まれています。ウェブ ACL でのルール作成の詳細については、「での保護の設定 AWS WAF」を参照してください。

を使用する場合は AWS Firewall Manager、Firewall Manager AWS WAF ポリシーに AWS WAF ルールを追加できます。

アプリケーションレイヤー DDoS 攻撃の可能性がある状況を手動で緩和するには

1. 異常な動作に一致する条件を使用して、ウェブ ACL にルールステートメントを作成します。まず、一致するリクエストをカウントするように設定します。ウェブ ACL およびルールステートメントの設定については、「のルールとルールグループで保護パック (ウェブ ACLs) を使用する AWS WAF」および「AWS WAF 保護のテストとチューニング」を参照してください。

> **Note**
>
> 最初に Block の代わりにルールアクション Count を使用して、常に最初にルールをテストしてください。新しいルールが正しいリクエストを識別していることを確認した後、リクエストをブロックするためにそれらを変更できます。

2. リクエスト数をモニタリングして、一致するリクエストをブロックするかどうかを決定します。リクエストの量が異常に多い状況が継続しており、そのような状況を引き起こしているリクエストをルールがキャプチャしていると確信できる場合は、ウェブ ACL のルールを変更してそのリクエストをブロックします。
3. イベントページのモニタリングを続行して、トラフィックが希望どおりに処理されるようにします。

AWS には、すぐに使用を開始できるように事前設定されたテンプレートが用意されています。テンプレートには、一般的なウェブベースの攻撃をブロックするためにカスタマイズして使用できる一連の AWS WAF ルールが含まれています。詳細については、「AWS WAF セキュリティオートメーション」を参照してください。

攻撃 AWS Shield Advanced 後の でのクレジットのリクエスト

にサブスクライブ AWS Shield Advanced していて、Shield Advanced で保護されたリソースの使用率を高める DDoS 攻撃が発生した場合は、Shield Advanced によって軽減されない範囲で、使用率の増加に関連する料金に対して Shield Advanced サービスクレジットをリクエストできます。

> **Note**
>
> このプロセスを通じて受け取ったクレジットは、Shield Advanced の使用にのみ適用できます。Shield Advanced クレジットは、他のサービスでは使用できません。

クレジットは、次のタイプの請求でのみ使用できます。

- Shield Advanced データ転送アウト
- Amazon CloudFront HTTP/HTTPS リクエスト
- CloudFront データ転送アウト
- Amazon Route 53 クエリ

- AWS Global Accelerator 標準アクセラレーターデータ転送
- Application Load Balancer のロードバランサー容量ユニット
- 攻撃に対応して自動スケーリングポリシーによって作成、保護された Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのインスタンスコスト

クレジットをリクエストするための前提条件

クレジットの付与を受けるための要件を満たすには、攻撃が始まる前に、次のことを完了している必要があります。

- クレジットをリクエストするリソースに Shield Advanced 保護を追加しておく必要があります。攻撃を受けている最中に追加された保護対象リソースは、コスト保護の対象外です。

  > **Note**
  >
  > で Shield Advanced を有効に AWS アカウント しても、個々のリソースに対して Shield Advanced 保護が自動的に有効になるわけではありません。

  Shield Advanced を使用して AWS リソースを保護する方法の詳細については、「」を参照してくださいAWS リソースへの AWS Shield Advanced 保護の追加。
- 該当する CloudFront および Application Load Balancer で保護されたリソースについては、 AWS WAF ウェブ ACL を関連付け、 Block モードでウェブ ACL にレートベースのルールを実装している必要があります。 AWS WAF のレートベースルールの詳細については、「でのレートベースのルールステートメントの使用 AWS WAF」を参照してください。ウェブ ACLs「」を参照してくださいでの保護の設定 AWS WAF。 AWS
- DDoS 攻撃を受けている最中のコストを最小限に抑えるようにアプリケーションを設定するには、「DDoS レジリエンシーに関するAWS のベストプラクティス」の適切なベストプラクティスを実装しておく必要があります。

クレジットの申請方法

クレジットの付与を受けるために要件を満たすには、攻撃が発生した請求月の直後から 15 日以内にクレジットリクエストを送信する必要があります。

クレジットを申請するには、AWS サポート Center を通じて請求ケースを提出してください。リクエストには次の内容を含めます。

- 件名の「DDoS Concession」という文字
- クレジットをリクエストしている各イベントまたは可用性の中断の日時
- 影響を受けた AWS サービスと特定のリソース

リクエストを送信すると、Shield Response Team (SRT) AWS は DDoS 攻撃が発生したかどうか、発生した場合は、保護されたリソースが DDoS 攻撃を吸収するためにスケーリングされたかどうかを検証します。が、 AWS 保護されたリソースが DDoS 攻撃を吸収するためにスケールされたと判断した場合、 AWS は が DDoS 攻撃によって引き起こされた AWS と判断したトラフィックのその部分にクレジットを発行します。クレジットは 12 か月間有効です。

AWS Shield サービスの使用におけるセキュリティ

このセクションでは、 責任共有モデルがどのように適用されるかについて説明します AWS Shield。

でのクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを活用できます。

> **Note**
>
> このセクションでは、Shield Advanced 保護など、 AWS Shield サービスとその AWS リソースの使用に関する標準的な AWS セキュリティガイダンスを提供します。
> Shield と Shield Advanced を使用して AWS リソースを保護する方法については、この AWS Shield ガイドの残りの部分を参照してください。

セキュリティは、 AWS とお客様の間の責任共有です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ – AWS は、 で AWS サービスを実行するインフラストラクチャを保護する責任を担います AWS クラウド。 は、お客様が安全に使用できるサービス AWS も提供します。セキュリティの有効性は、AWS コンプライアンスプログラムの一環として、サードパーティーの審査機関によって定期的にテストおよび検証されています。Shield に適用するコンプライアンスプログラムの詳細については、「コンプライアンスプログラムによる対象範囲内のAWS のサービス」を参照してください。

- クラウドのセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、お客様のデータの機密性、組織の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、Shield を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます。次のトピックでは、セキュリティとコンプライアンスの目的を達成するために Shield を設定する方法を示します。また、Shield リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

- Shield でのデータの保護
- での IAM の使用 AWS Shield
- Shield でのログ記録とモニタリング
- Shield でのコンプライアンス検証
- Shield での耐障害性の構築
- のインフラストラクチャセキュリティ AWS Shield

Shield でのデータの保護

このセクションでは、Shield でのデータ保護に 責任 AWS 共有モデルがどのように適用されるかについて説明します。

AWS 責任共有モデル は、 AWS Shieldでのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「 AWS のサービス 」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「Data Privacy FAQChina」を参照してください。 欧州におけるデータ保護に関する情報については、General Data Protection Regulation (GDPR) Center を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM アイデンティティセンター または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。

- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須ですが、TLS 1.3 を推奨します。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール、API、または SDK を使用して Shield AWS CLIまたは他の AWS のサービス を使用する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

Shield のエンティティ (保護など) は、中国 (北京) や中国 (寧夏) など、暗号化が利用できない特定のリージョンを除き、保管時に暗号化されます。リージョンごとに一意の暗号化キーが使用されます。

での IAM の使用 AWS Shield

このセクションでは、 で IAM を使用する方法について説明します AWS Shield。

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、Shield リソースを使用するための、認証 (サインイン) および認可 (アクセス許可を持つ) ができるユーザーを制御します。IAM は、追加料金なしで使用できる AWS のサービス です。

トピック

- オーディエンス
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理

- が IAM と AWS Shield 連携する方法
- のアイデンティティベースのポリシーの例 AWS Shield
- AWS の 管理ポリシー AWS Shield
- AWS Shield ID とアクセスのトラブルシューティング
- Shield Advanced のサービスにリンクされたロールの使用

オーディエンス

AWS Identity and Access Management (IAM) の使用方法は、Shield で行う作業によって異なります。

サービスユーザー - Shield サービスを使用してジョブを実行する場合は、必要なアクセス許可と認証情報を管理者が用意します。作業を実行するためにさらに多くの Shield 機能を使用するとき、追加の許可が必要になる場合があります。アクセスの管理方法を理解すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。Shield の特徴にアクセスできない場合は、「AWS Shield ID とアクセスのトラブルシューティング」を参照してください。

サービス管理者 - 社内の Shield リソースを担当している場合は、通常、Shield へのフルアクセスがあります。サービスのユーザーがどの Shield 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。お客様の会社にて Shield により IAM を利用する方法の詳細については、が IAM と AWS Shield 連携する方法 をご参照ください。

IAM 管理者 - IAM 管理者は、Shield へのアクセスを管理するためのポリシーの作成方法について、詳細を知りたい場合があります。IAM で使用できる Shield アイデンティティベースのポリシーの例を表示するには、「のアイデンティティベースのポリシーの例 AWS Shield」を参照してください。

アイデンティティを使用した認証

認証は、ID 認証情報 AWS を使用して にサインインする方法です。、IAM ユーザー AWS アカウントのルートユーザー、または IAM ロールを引き受けることで認証される必要があります。

AWS IAM アイデンティティセンター (IAM Identity Center)、シングルサインオン認証、Google/Facebook 認証情報などの ID ソースからの認証情報を使用して、フェデレーティッド ID としてサインインできます。サインインの詳細については、「AWS サインイン ユーザーガイド」の「AWS アカウントにサインインする方法」を参照してください。

プログラムによるアクセスの場合、 は SDK と CLI AWS を提供してリクエストを暗号化して署名します。詳細については、「IAM ユーザーガイド」の「API リクエストに対するAWS 署名バージョン 4」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、まず、すべての AWS のサービス および リソースへの完全なアクセス権を持つ AWS アカウント root ユーザーと呼ばれる 1 つのサインイン ID から始めます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザー認証情報を必要とするタスクについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーテッドアイデンティティ

ベストプラクティスとして、人間のユーザーが一時的な認証情報 AWS のサービス を使用して にアクセスするには、ID プロバイダーとのフェデレーションを使用する必要があります。

フェデレーティッド ID は、エンタープライズディレクトリ、ウェブ ID プロバイダー、または ID Directory Service ソースの認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーテッドアイデンティティは、一時的な認証情報を提供するロールを引き受けます。

アクセスを一元管理する場合は、 AWS IAM アイデンティティセンターをお勧めします。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「IAM アイデンティティセンターとは」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、特定の個人やアプリケーションに対する特定のアクセス許可を持つアイデンティティです。長期認証情報を持つ IAM ユーザーの代わりに一時的な認証情報を使用することをお勧めします。詳細については、IAM ユーザーガイドの「ID プロバイダーとのフェデレーションを使用して にアクセスする必要がある AWS」を参照してください。

IAM グループは、IAM ユーザーの集合を指定し、大量のユーザーに対するアクセス許可の管理を容易にします。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可を持つアイデンティであり、一時的な認証情報を提供します。ユーザーから IAM ロール (コンソール) に切り替えるか、 または API オペレーションを呼び出すこ

とで、ロールを引き受けることができます。 AWS CLI AWS 詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールは、フェデレーションユーザーアクセス、一時的な IAM ユーザーのアクセス許可、クロスアカウントアクセス、クロスサービスアクセス、および Amazon EC2 で実行するアプリケーションに役立ちます。詳細については、IAM ユーザーガイド の IAM でのクロスアカウントリソースアクセス を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは、ID またはリソースに関連付けられている場合のアクセス許可を定義します。 は、プリンシパルがリクエストを行うときに、これらのポリシー AWS を評価します。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は、ポリシーを使用して、どのプリンシパルがどのリソースに対して、どのような条件でアクションを実行できるかを定義することで、誰が何にアクセスできるかを指定します。

デフォルトでは、ユーザーやロールにアクセス許可はありません。IAM 管理者は IAM ポリシーを作成してロールに追加し、このロールをユーザーが引き受けられるようにします。IAM ポリシーは、オペレーションの実行方法を問わず、アクセス許可を定義します。

アイデンティティベースのポリシー

アイデンティティベースのポリシーは、アイデンティティ (ユーザー、グループ、またはロール) にアタッチできる JSON アクセス許可ポリシードキュメントです。これらのポリシーは、アイデンティティがどのリソースに対してどのような条件下でどのようなアクションを実行できるかを制御します。アイデンティティベースポリシーの作成方法については、IAM ユーザーガイド の カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する を参照してください。

アイデンティティベースのポリシーは、インラインポリシー (単一の ID に直接埋め込む) または管理ポリシー (複数の ID にアタッチされたスタンドアロンポリシー) にすることができます。管理ポリシーとインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。例としては、IAM ロール信頼ポリシーや Amazon S3 バケットポリシーなどがあります。リソースベースのポ

リシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするためのアクセス許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、および Amazon VPC は AWS WAF、ACLs。ACL の詳細については、Amazon Simple Storage Service デベロッパーガイド の アクセスコントロールリスト (ACL) の概要 を参照してください。

その他のポリシータイプ

AWS は、より一般的なポリシータイプによって付与されるアクセス許可の最大数を設定できる追加のポリシータイプをサポートしています。

- アクセス許可の境界 – アイデンティティベースのポリシーで IAM エンティティに付与することのできるアクセス許可の数の上限を設定します。詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可境界」を参照してください。
- サービスコントロールポリシー (SCP) - AWS Organizations内の組織または組織単位の最大のアクセス許可を指定します。詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」を参照してください。
- リソースコントロールポリシー (RCP) – は、アカウント内のリソースで利用できる最大数のアクセス許可を定義します。詳細については、「AWS Organizations ユーザーガイド」の「リソースコントロールポリシー (RCP)」を参照してください。
- セッションポリシー – ロールまたはフェデレーションユーザーの一時セッションを作成する際にパラメータとして渡される高度なポリシーです。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成されるアクセス許可を理解するのがさらに難しくなります。が複数のポリシータイプが関与する場合にリクエストを許可す

るかどうか AWS を決定する方法については、「IAM ユーザーガイド」の「ポリシー評価ロジック」を参照してください。

が IAM と AWS Shield 連携する方法

このセクションでは、 で IAM の機能を使用する方法について説明します AWS Shield。

IAM を使用して Shield へのアクセスを管理する前に、Shield で利用できる IAM の機能について学びます。

で使用できる IAM 機能 AWS Shield

IAM 機能	Shield のサポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	はい
ACL	なし
ABAC (ポリシー内のタグ)	部分的
一時認証情報	あり
転送アクセスセッション (FAS)	あり
サービスロール	あり
サービスにリンクされたロール	はい

Shield およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要については、「IAM ユーザーガイド」のAWS 「IAM と連携する のサービス」を参照してください。

Shield のアイデンティティベースのポリシー

このセクションでは、アイデンティティベースのポリシーの例を示します AWS Shield。

ID ベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

Shield アイデンティティベースのポリシーの例を表示するには、「のアイデンティティベースのポリシーの例 AWS Shield」を参照してください。

Shield 内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシー や Amazon S3 バケットポリシー があげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーで、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、全体のアカウント、または別のアカウントの IAM エンティティを、リソースベースのポリシーのプリンシパルとして指定します。詳細については、IAM ユーザーガイドのIAM でのクロスアカウントリソースアクセスを参照してください。

Shield のポリシーアクション

ポリシーアクションのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action` 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

Shield アクションのリストを確認するには、「Service Authorization Reference」の「AWS Shieldで定義されるアクション」を参照してください。

Shield のポリシーアクションは、アクションの前に以下のプレフィックス を使用します。

```
shield
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "shield:action1",
      "shield:action2"
         ]
```

ワイルドカード (*) を使用すると、複数のアクションを指定することができます。たとえば、Shield で `List` で始まるすべてのアクションを指定するには、次のアクションを含めます。

```
"Action": "shield:List*"
```

Shield アイデンティティベースのポリシーの例を表示するには、「のアイデンティティベースのポリシーの例 AWS Shield」を参照してください。

Shield のポリシーリソース

ポリシーリソースのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

`Resource` JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。リソースレベ

ルのアクセス許可をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

Shield リソースタイプとそれらの ARN のリストを確認するには、「Service Authorization Reference」の「AWS Shieldで定義されるリソース」を参照してください。どのアクションで各リソースの ARN を指定できるかについては、「AWS Shieldで定義されるアクション」を参照してください。Shield リソースのサブセットへのアクセスを許可または拒否するには、ポリシーの `resource` 要素にリソースの ARN を含めます。

では AWS Shield、リソースは保護と攻撃です。これらのリソースには、次の表に示すとおり、一意の Amazon リソースネーム (ARN) が関連付けられています。

AWS Shield コンソールの名前	AWS Shield SDK/CLI の名前	ARN 形式
イベントまたは攻撃	`AttackDetail`	`arn:aws:shield::` *`account`*`:attack/`*`ID`
保護	`Protection`	`arn:aws:shield::` *`account`*`:protection/`*` ID`

Shield リソースのサブセットへのアクセスを許可または拒否するには、ポリシーの `resource` 要素にリソースの ARN を含めます。Shield の ARN の形式は次のとおりです。

```
arn:partition:shield::account:resource/ID
```

`[account]` (アカウント)、*`[resource]`* (リソース)、および *`[ID]`* 変数を有効な値に置き換えます。有効な値は次のとおりです。

- *`#####`*: の ID AWS アカウント。値を指定する必要があります。
- *`resource`*: Shield リソースのタイプ (`attack` または `protection` のいずれか)。
- *`ID`*: Shield リソースの ID、または ワイルドカード (*)。ワイルドカードは、指定した AWS アカウントに関連付けられている、指定したタイプのすべてのリソースを示します。

例えば、次の ARN はアカウント 111122223333 のすべての保護を指定します。

```
arn:aws:shield::111122223333:protection/*
```

Shield リソースの ARN の形式は次のとおりです。

```
arn:partition:shield:region:account-id:scope/resource-type/resource-name/resource-id
```

ARN の仕様に関する一般情報については、「 Amazon Web Services 全般のリファレンス」の「Amazon リソースネーム (ARN)」を参照してください。

wafv2 リソースの ARN に固有の要件は以下の通りです。

- *region*: Amazon CloudFront ディストリビューションを保護するために使用する Shield リソースの場合は、これを us-east-1 に設定します。それ以外の場合は、保護されたリージョンリソースで使用している領域を設定します。
- *####*: Amazon CloudFront ディストリビューションglobalで使用するか、 が AWS WAF サポートするリージョンリソースregionalで使用するスコープを に設定します。リージョンリソースは、Amazon API Gateway REST API、Application Load Balancer、 AWS AppSync GraphQL API、Amazon Cognito ユーザープール、 AWS App Runner サービス、Amazon Bedrock AgentCore Gateway、 AWS Verified Access インスタンスです。
- *resource-type*: イベント用または攻撃用の attack、保護用の protection のいずれかの値を指定します。
- *resource-name*: Shield リソースに付けた名前を指定するか、ARN の他の仕様を満たすすべてのリソースを示すワイルドカード (*) を指定します。リソース名とリソース ID のどちらかを指定するか、両方にワイルドカードを指定する必要があります。
- *resource-id*: Shield リソースの ID を指定するか、ワイルドカード (*) を指定して ARN の他の仕様を満たすすべてのリソースを指定します。リソース名とリソース ID のどちらかを指定するか、両方にワイルドカードを指定する必要があります。

例えば、次の ARN は、リージョン us-west-1 におけるアカウント 111122223333 のリージョンレベルの範囲のすべてのウェブ ACL を指定します。

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

次の ARN は、リージョン us-east-1 のアカウント 111122223333 に対して、グローバルスコープを持つ MyIPManagementRuleGroup というルールグループを指定します。

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

Shield アイデンティティベースのポリシーの例を表示するには、「のアイデンティティベースのポリシーの例 AWS Shield」を参照してください。

Shield のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Condition 要素は、定義された基準に基づいてステートメントが実行される時期を指定します。イコールや未満などの条件演算子を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「グローバル条件コンテキストキー」を参照してください。

Shield の条件キーのリストを確認するには、「Service Authorization Reference」の「AWS Shieldの条件キー」を参照してください。条件キーを使用できるアクションとリソースについては、「 で定義されるアクション AWS Shield」を参照してください。

Shield アイデンティティベースのポリシーの例を表示するには、「のアイデンティティベースのポリシーの例 AWS Shield」を参照してください。

Shield の ACL

ACL のサポート: なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするためのアクセス許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Shield 付き ABAC

ABAC (ポリシー内のタグ) のサポート: 一部

属性ベースのアクセス制御 (ABAC) は、タグと呼ばれる属性に基づいてアクセス許可を定義する認可戦略です。IAM エンティティと AWS リソースにタグをアタッチし、プリンシパルのタグがリソースのタグと一致するときにオペレーションを許可するように ABAC ポリシーを設計できます。

タグに基づいてアクセスを管理するには、aws:ResourceTag/*key-name*、aws:RequestTag/*key-name*、または aws:TagKeys の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM ユーザーガイド」の「属性ベースのアクセス制御 (ABAC) を使用する」を参照してください。

Shield での一時的な認証情報の使用

一時的な認証情報のサポート: あり

一時的な認証情報は AWS 、リソースへの短期的なアクセスを提供し、フェデレーションまたは切り替えロールを使用する場合に自動的に作成されます。長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成 AWS することをお勧めします。詳細については、「IAM ユーザーガイド」の「IAM の一時的な認証情報」および「AWS のサービス と IAM との連携」を参照してください。

Shield の転送アクセスセッション

転送アクセスセッション (FAS) のサポート: あり

転送アクセスセッション (FAS) は、 を呼び出すプリンシパルのアクセス許可と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする を使用します。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

Shield のサービスロール

サービスロールのサポート: あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、IAM ユーザーガイドの AWS のサービスに許可を委任するロールを作成するを参照してください。

> **Warning**
>
> サービスロールの許可を変更すると、Shield の機能が破損する可能性があります。Shield が指示する場合以外は、サービスロールを編集しないでください。

Shield のサービスリンクロール

サービスリンクロールのサポート: あり

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、 サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。

Shield サービスにリンクされたロールの作成または管理の詳細については、「Shield Advanced のサービスにリンクされたロールの使用」を参照してください。

のアイデンティティベースのポリシーの例 AWS Shield

デフォルトでは、ユーザーおよびロールには、Shield リソースを作成または変更するアクセス許可はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。

これらのサンプルの JSON ポリシードキュメントを使用して IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーを作成する (コンソール)」を参照してください。

Shield が定義するアクションとリソースタイプ (リソースタイプごとの ARN の形式を含む) の詳細については、「Service Authorization Reference」の「Actions, resources, and condition keys for AWS Shield」を参照してください。

トピック

- ポリシーに関するベストプラクティス
- Shield コンソールの使用
- 自分の権限の表示をユーザーに許可する
- Shield Advanced の保護機能に対する読み取りアクセスの許可
- Shield、CloudFront、CloudWatch に読み取り専用のアクセス権を付与する

- Shield、CloudFront、CloudWatch へのフルアクセス権を付与する

ポリシーに関するベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが Shield リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションでは、 AWS アカウントに費用が発生する場合があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、IAM ユーザーガイド の AWS マネージドポリシー または ジョブ機能のAWS マネージドポリシー を参照してください。
- 最小特権を適用する – IAM ポリシーでアクセス許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、IAM ユーザーガイド の IAM でのポリシーとアクセス許可 を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。たとえば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用されている場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます CloudFormation。詳細については、IAM ユーザーガイド の IAM JSON ポリシー要素:条件 を参照してください。
- IAM アクセスアナライザー を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM アクセスアナライザー は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイド の IAM Access Analyzer でポリシーを検証する を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、MFA をオンにしてセキュリティを強化します。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイド の MFA を使用した安全な API アクセス を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイド の IAM でのセキュリティのベストプラクティス を参照してください。

Shield コンソールの使用

AWS Shield コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 の Shield リソースの詳細を一覧表示および表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

AWS コンソールにアクセスして使用できるユーザーは、 AWS Shield コンソールにアクセスすることもできます。追加のアクセス許可は必要ありません。

コンソールのみの API

コンソールでは、次の分散型サービス拒否 (DDoS) 攻撃情報にアクセスできます。特定のアクションを許可または拒否するには、IAM ポリシーで次の API アクセス許可を指定します。

アクション	説明
`DescribeAttackContributors`	特定の DDoS 攻撃の寄与者に関する詳細情報を取得するアクセス許可を付与します。
`ListMitigations`	DDoS 攻撃中に適用された緩和アクションのリストを取得するアクセス許可を付与します。
`GetGlobalThreatData`	Shield AWS の脅威モニタリングシステムからグローバルな脅威インテリジェンスデータと傾向を取得するアクセス許可を付与します。

この例では、コンソールで DDoS 攻撃情報を表示できるようにするポリシーを作成する方法を示します。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "shield:DescribeAttackContributors"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "shield:ListMitigations"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "shield:GetGlobalThreatData"
            ],
            "Resource": "*"
        }
    ]
}
```

自分の権限の表示をユーザーに許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
```

```
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Shield Advanced の保護機能に対する読み取りアクセスの許可

AWS Shield はクロスアカウントリソースアクセスを許可しますが、クロスアカウントリソース保護を作成することはできません。リソースの保護は、それらのリソースを所有するアカウント内からのみ作成できます。

すべてのリソースの `shield:ListProtections` アクションの許可を付与するポリシーの例を次に示します。Shield は、一部の API アクションについて、リソース ARN (リソースレベルの許可と呼ばれる) を使用した特定のリソースの識別をサポートしていません。そのため、ワイルドカード文字 (*) を指定する必要があります。これは、アクション `ListProtections` を通して取得できるリソースへのアクセスのみを許可するものです。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ListProtections",
            "Effect": "Allow",
            "Action": [
                "shield:ListProtections"
            ],
            "Resource": "*"
        }
    ]
}
```

Shield、CloudFront、CloudWatch に読み取り専用のアクセス権を付与する

次のポリシーでは、Amazon CloudFront リソースや Amazon CloudWatch メトリクスなど、Shield の関連付けられたリソースへの読み取り専用アクセスをユーザーに付与します。これは、Shield 保護と攻撃の設定を表示したり、CloudWatch でメトリクスをモニタリングする許可が必要なユーザーにとって役立ちます。これらのユーザーは、Shield リソースを作成、更新、または削除することはできません。

JSON

```
{
        "Version":"2012-10-17",
        "Statement": [
            {
                "Sid": "ProtectedResourcesReadAccess",
                "Effect": "Allow",
                "Action": [
                    "cloudfront:List*",
                    "route53:List*",
                    "cloudfront:Describe*",
                    "elasticloadbalancing:Describe*",
                    "cloudwatch:Describe*",
                    "cloudwatch:Get*",
                    "cloudwatch:List*",
```

```
                "cloudfront:GetDistribution*",
                "globalaccelerator:ListAccelerators",
                "globalaccelerator:DescribeAccelerator"
            ],
            "Resource": [
                "arn:aws:elasticloadbalancing:*:*:*",
                "arn:aws:cloudfront::*:*",
                "arn:aws:route53:::hostedzone/*",
                "arn:aws:cloudwatch:*:*:*:*",
                "arn:aws:globalaccelerator::*:*"
            ]
        },
        {
            "Sid": "ShieldReadOnly",
            "Effect": "Allow",
            "Action": [
                "shield:List*",
                "shield:Describe*",
                "shield:Get*"
            ],
            "Resource": "*"
        }
    ]
}
```

Shield、CloudFront、CloudWatch へのフルアクセス権を付与する

次のポリシーにより、ユーザーは Shield オペレーションを実行し、CloudFront ウェブディストリビューションで任意のオペレーションを実行して、CloudWatch でメトリクスとリクエストのサンプルをモニタリングできます。これは、Shield の管理者であるユーザーにとって便利です。

JSON

```
{
        "Version":"2012-10-17",
        "Statement": [
            {
                "Sid": "ProtectedResourcesReadAccess",
                "Effect": "Allow",
                "Action": [
                    "cloudfront:List*",
```

```
                "route53:List*",
                "cloudfront:Describe*",
                "elasticloadbalancing:Describe*",
                "cloudwatch:Describe*",
                "cloudwatch:Get*",
                "cloudwatch:List*",
                "cloudfront:GetDistribution*",
                "globalaccelerator:ListAccelerators",
                "globalaccelerator:DescribeAccelerator"
            ],
            "Resource": [
                "arn:aws:elasticloadbalancing:*:*:*",
                "arn:aws:cloudfront::*:*",
                "arn:aws:route53:::hostedzone/*",
                "arn:aws:cloudwatch:*:*:*:*",
                "arn:aws:globalaccelerator::*:*"
            ]
        },
        {
            "Sid": "ShieldFullAccess",
            "Effect": "Allow",
            "Action": [
                "shield:*"
            ],
            "Resource": "*"
        }
    ]
}
```

管理者許可を持つユーザーに対しては多要素認証 (MFA) を設定することを強くお勧めします。詳細については、「IAM ユーザーガイド」の「AWSでの多要素認証 (MFA) デバイスの使用」を参照してください。

AWS の 管理ポリシー AWS Shield

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できるように、多くの一般的なユースケースにアクセス許可を付与するように設計されています。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS 管理ポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) に影響します。 AWS は、新しい が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、 AWS 管理ポリシーを更新する可能性が高くなります。

詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

AWS マネージドポリシー: AWSShieldDRTAccessPolicy

このセクションでは、Shield の AWS 管理ポリシーを使用する方法について説明します。

AWS Shield は、Shield Response Team (SRT) にユーザーに代わって行動するためのアクセス許可を付与するときに、この管理ポリシーを使用します。このポリシーは、重大度の高いイベント中の DDoS 攻撃の軽減を支援するために、SRT に AWS アカウントへの制限付きアクセスを許可します。このポリシーにより、SRT は AWS WAF ルールと Shield Advanced 保護を管理し、 AWS WAF ログにアクセスできます。

SRT に代行操作を許可する方法については、「SRT へのアクセスの許可」を参照してください。

ポリシーの詳細については、IAM コンソールの「AWSShieldDRTAccessPolicy」を参照してください。

AWS マネージドポリシー: AWSShieldServiceRolePolicy

Shield Advanced は、アプリケーションレイヤーの自動 DDoS 軽減を有効にする際に、この管理ポリシーを使用して、アカウントのリソース管理に必要な権限を設定します。このポリシーにより、Shield Advanced は、保護されたリソースに関連付けたウェブ ACLs に AWS WAF ルールとルールグループを作成して適用し、DDoS 攻撃に自動的に対応できます。

お客様の IAM エンティティに、AWSShieldServiceRolePolicy をアタッチすることはできません。Shield はこのポリシーをサービス連動ロール `AWSServiceRoleForAWSShield` に添付し、Shield が代わりにアクションを実行できるようにします。

アプリケーションレイヤーの DDoS 自動緩和機能を有効にすると、Shield Advanced でこのポリシーの使用が可能になります。このポリシーの使用の詳細については、Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和 を参照してください。

このポリシーを使用するサービス連携ロール AWSServiceRoleForAWSShield の詳細は、「Shield Advanced のサービスにリンクされたロールの使用」を参照してください。

ポリシーの詳細については、IAM コンソールで「AWSShieldServiceRolePolicy」を参照してください。

AWS マネージドポリシーへの Shield 更新

このサービスがこれらの変更の追跡を開始してからの Shield の AWS マネージドポリシーの更新に関する詳細を表示します。このページの変更に関する自動通知については、ドキュメント履歴 の Shield ドキュメントの履歴ページの RSS フィードをサブスクライブしてください。

ポリシー	変更点の説明	日付
`AWSShieldServiceRolePolicy` このポリシーにより、Shield はユーザーに代わってアプリケーションレイヤー DDoS 攻撃に自動的に対応するために、 AWS リソースにアクセスして管理できます。 IAM コンソールの詳細: AWSShieldServiceRolePolicy サービスにリンクされたロール `AWSServiceRoleForAWSShield` はこのポリシーを使用します。詳細については、「Shield Advanced のサービスにリンクされたロールの使用」を参照してください。	アプリケーションレイヤー DDoS 自動緩和機能に必要な許可を Shield Advanced に提供するため、このポリシーを追加しました。この機能については、「Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和」を参照してください。	2021 年 12 月 1 日

ポリシー	変更点の説明	日付
Shield は変更の追跡を開始しました	Shield は、 AWS 管理ポリシーの変更の追跡を開始しました。	2021 年 3 月 3 日

AWS Shield ID とアクセスのトラブルシューティング

次の情報は、Shield と IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復に役立ちます。

トピック

- Shield でアクションを実行する権限がない
- iam:PassRole を実行する権限がありません
- 自分の 以外のユーザーに Shield リソース AWS アカウント へのアクセスを許可したい

Shield でアクションを実行する権限がない

あるアクションを実行する権限がないというエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要な shield:*GetWidget* アクセス許可を持っていない場合に発生するものです。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 shield:GetWidget on resource: my-example-widget
```

この場合、shield:*GetWidget* アクションを使用して *my-example-widget* リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

iam:PassRole を実行する権限がありません

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Shield にロールを渡せるようにする必要があります。

一部の AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡すアクセス許可が必要です。

以下の例のエラーは、marymajor という IAM ユーザーがコンソールを使用して Shield でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与されたアクセス許可が必要です。Mary には、ロールをサービスに渡すアクセス許可がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン資格情報を提供した担当者が管理者です。

自分の 以外のユーザーに Shield リソース AWS アカウント へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- Shield でこれらの特徴がサポートされるかどうかを確認するには、「が IAM と AWS Shield 連携する方法」を参照してください。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、「IAM ユーザーガイド」の「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイドの外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可を参照してください。

- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いの詳細については、IAM ユーザーガイドのIAM ロールとリソースベースのポリシーとの相違点を参照してください。

Shield Advanced のサービスにリンクされたロールの使用

このセクションでは、サービスにリンクされたロールを使用して、Shield Advanced に AWS アカウントのリソースへのアクセスを許可する方法について説明します。

AWS Shield Advanced は AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスにリンクされたロールは、Shield Advanced に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは Shield Advanced によって事前定義されており、サービスがユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用することで、必要な許可を手動で追加する必要がなくなるため、Shield Advanced の設定が簡単になります。Shield Advanced は、サービスにリンクされたロールの許可を定義します。特に定義されている場合を除き、Shield Advanced のみがそのロールを引き受けることができます。定義される許可には、信頼ポリシーと許可ポリシーが含まれており、その許可ポリシーを他のIAM エンティティにアタッチすることはできません。

サービスにリンクされたロールは、まずその関連リソースを削除しなければ削除できません。これにより、リソースへの意図しないアクセスによる許可の削除が防止され、Shield Advanced リソースは保護されます。

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連携するAWS サービス」を参照して、サービスにリンクされたロール列がはいになっているサービスを見つけてください。そのサービスに関するサービスにリンクされたロールに関するドキュメントを表示するには、リンクが設定されている [Yes] (はい) を選択します。

Shield Advanced のサービスにリンクされたロールの許可

Shield Advanced は、AWSServiceRoleForAWSShield という名前のサービスにリンクされたロールを使用します。このロールにより、Shield Advanced はユーザーに代わってアプリケーションレイヤー DDoS 攻撃に自動的に対応するために、 AWS リソースにアクセスして管理できます。この関数の詳細については、「Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和」を参照してください。

サービスにリンクされたロール AWSServiceRoleForAWSShield は、次のサービスを信頼してロールを引き受けます。

- shield.amazonaws.com

AWSShieldServiceRolePolicy という名前のロールアクセス許可ポリシーにより、Shield Advanced はすべての AWS リソースに対して次のアクションを実行できます。

- wafv2:GetWebACL
- wafv2:UpdateWebACL
- wafv2:GetWebACLForResource
- wafv2:ListResourcesForWebACL
- cloudfront:ListDistributions
- cloudfront:GetDistribution

すべての AWS リソースでアクションが許可されている場合、これはポリシーに と表示されます"Resource": "*"。これは、サービスにリンクされたロールが、アクションがサポートするすべての AWS リソースに対して、指定された各アクションを実行できることを意味します。例えば、アクション wafv2:GetWebACL は wafv2 ウェブ ACL リソースでのみサポートされます。

Shield Advanced は、アプリケーションレイヤー保護機能を有効にしている保護されたリソースと、それらの保護されたリソースに関連付けられているウェブ ACL についてのみ、リソースレベルの API コールを実行します。

サービスにリンクされたロールの作成、編集、削除をIAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、許可を設定する必要があります。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの許可」を参照してください。

Shield Advanced のサービスにリンクされたロールの作成

サービスリンクロールを手動で作成する必要はありません。 AWS マネジメントコンソール、、AWS CLIまたは AWS API でリソースのアプリケーションレイヤー DDoS 自動緩和を有効にすると、Shield Advanced によってサービスにリンクされたロールが作成されます。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は同じ方法でアカウントにロールを再作成できます。リソースのためにアプリケーションレイヤー DDoS 自動緩和を有効にすると、Shield Advanced は、サービスにリンクされたロールを再作成します。

Shield Advanced のサービスにリンクされたロールの編集

Shield Advanced で、AWSServiceRoleForAWSShield のサービスにリンクされたロールを編集することはできません。サービスにリンクされたロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用してロールの説明を編集することはできます。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの編集」を参照してください。

Shield Advanced のサービスにリンクされたロールの削除

サービスにリンクされたロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、積極的にモニタリングまたは保守されていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスにリンクされたロールのリソースをクリーンアップする必要があります。

> **Note**
>
> リソースを削除する際に、Shield Advanced でロールが使用されている場合、削除は失敗することがあります。失敗した場合は、数分待ってからオペレーションを再試行してください。

AWSServiceRoleForAWSShield で使用されている Shield Advanced リソースを削除するには

アプリケーションレイヤー DDoS 保護が設定されているすべてのリソースについて、アプリケーションレイヤー DDoS 自動緩和を無効にします。コンソールの手順については、「アプリケーションレイヤー DDoS 保護を設定する」を参照してください。

IAM を使用して、サービスにリンクされたロールを手動で削除するには

IAM コンソール、 AWS CLI、または AWS API を使用して、AWSServiceRoleForAWSShield サービスにリンクされたロールを削除します。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの削除」を参照してください。

Shield Advanced のサービスにリンクされたロールをサポートするリージョン

Shield Advanced では、このサービスが利用可能なすべての リージョンで、サービスにリンクされたロールの使用をサポートしています。詳細については、「Shield Advanced エンドポイントとクォータ」を参照してください。

Shield でのログ記録とモニタリング

このセクションでは、 でイベントをモニタリングおよび応答するための AWS ツールを使用する方法について説明します AWS Shield。

モニタリングは、Shield と AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、 AWS ソリューションのすべての部分からモニタリングデータを収集する必要があります。 には、Shield リソースをモニタリングし、潜在的なイベントに対応するための複数のツール AWS が用意されています。

Amazon CloudWatch アラーム

Amazon CloudWatch アラームを使用して、指定した期間にわたって 1 つのメトリクスを確認します。メトリクスが指定されたしきい値を超えると、CloudWatch は Amazon SNS トピックまたは AWS Auto Scaling ポリシーに通知を送信します。詳細については、「Amazon CloudWatch によるモニタリング」を参照してください。

AWS CloudTrail ログ

CloudTrail は、Shield のユーザー、ロール、または AWS のサービスによって実行されたアクションの記録を提供します。CloudTrail で収集された情報を使用して、Shield に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。詳細については、「での AWS CloudTrail API コールのログ記録」を参照してください。

Shield でのコンプライアンス検証

このセクションでは、 を使用する際のコンプライアンス責任について説明します AWS Shield。

新しい AWS サインアップエクスペリエンスは、規制されたワークロード向けには設計されていません。新しい AWS サインアップエクスペリエンスを使用しているが、規制対象のワークロード AWS に を使用する場合は、 AWS (アドバンスド) にサインアップするか、 AWS 環境の高度な機能をアクティブ化できます。

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、「コンプライアンスAWS のサービス プログラムによるスコープ」の「コンプライアンス」を参照して、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「Downloading Reports in AWS Artifact」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。を使用する際のコンプライアンス責任の詳細については AWS のサービス、AWS 「 セキュリティドキュメント」を参照してください。

Shield での耐障害性の構築

このセクションでは、 AWS アーキテクチャが のデータ冗長性をサポートする方法について説明します AWS Shield。

AWS グローバルインフラストラクチャは、 AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。 は、低レイテンシー、高スループット、高度に冗長なネットワークで接続された、物理的に分離および分離された複数のアベイラビリティーゾーン AWS リージョン を提供します。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断せずに、自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、およびスケーラビリティが優れています。

AWS リージョン およびアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

のインフラストラクチャセキュリティ AWS Shield

このセクションでは、 がサービストラフィックを AWS Shield 分離する方法について説明します。

マネージドサービスである AWS Shield は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して環境を AWS 設計するには、「Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

AWS 公開された API コールを使用して、ネットワーク経由で Shield にアクセスします。クライアントは以下をサポートする必要があります。

- Transport Layer Security (TLS)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

AWS Shield Advanced クォータ

AWS Shield Advanced には、リージョンあたりのエンティティ数に対するデフォルトのクォータがあります。このクォータの引き上げをリクエストできます。

[リソース]	デフォルトのクォータ
アカウントごとに、 が保護 AWS Shield Advanced を提供するリソースタイプごとの保護されたリソースの最大数。	1,000
アカウントごとの保護グループの最大数。	100
保護グループに具体的に含めることができる個別の保護されたリソースの最大数。API では、これは保護グループ `Pattern` を `ARBITRARY` に設定するときに指定する `Members` に適用されます。コンソールでは、これは保護グループのために選択するリソースに適用されます [Choose from protected resources] (保護されたリソースから選択)	1,000

AWS Shield ネットワークセキュリティディレクター (プレビュー)

> **Note**
>
> AWS Shield ネットワークセキュリティディレクターはパブリックプレビューリリースであり、変更される可能性があります。

AWS Shield ネットワークセキュリティディレクターは、 アカウント全体でコンピューティング、ネットワーク、およびネットワークセキュリティリソースを検出して AWS 環境を保護するのに役立ちます。 ネットワークセキュリティディレクターは、 AWS ベストプラクティスと脅威インテリジェンスに照らしてネットワークトポロジとセキュリティ設定を分析することで、各リソースのセキュリティ設定を評価します。セキュリティを強化するために、ネットワークセキュリティディレクターは検出結果を低い重要度から重大な重要度で評価し、Amazon Q Developer を通じて自然言語クエリを使用して調べることができる特定の修復手順を共有します。

AWS Shield ネットワークセキュリティディレクターの料金

AWS は現在、ネットワークセキュリティディレクターの使用には課金されません。ただし、 AWS WAFなど、使用する基盤となるサービスに対して発生する料金はお客様の負担となります。ネットワークセキュリティディレクターが一般公開されると、料金はプレビューリリースとは異なります。

AWS Shield ネットワークセキュリティディレクターのユースケース

> **Note**
>
> AWS Shield Network Security Director はパブリックプレビューリリースであり、変更される可能性があります。

AWS Shield ネットワークセキュリティディレクターは、アカウント全体でコンピューティング、ネットワーク、およびネットワークセキュリティリソースを検出することで AWS 、環境を保護するのに役立ちます。 ネットワークセキュリティディレクターは、 AWS ベストプラクティスと脅威イ

ンテリジェンスに照らしてネットワークトポロジとセキュリティ設定を分析することで、各リソースのセキュリティ設定を評価します。セキュリティを強化するために、ネットワークセキュリティディレクターは検出結果を低い重要度から重大な重要度で評価し、Amazon Q Developer を通じて自然言語クエリを使用して調べることができる特定の修復手順を共有します。

ネットワークセキュリティディレクターと Amazon Q Developer は、ネットワークセキュリティ設定のセキュリティ問題を特定し、緩和オプションを提供するのに役立ちます。

- EC2 インスタンスへの過剰なアクセス – VPCs および Amazon Elastic Compute Cloud インスタンスに関連付けられているセキュリティグループとネットワーク ACLs (NACLs) を特定し、ポート 22 や 3389 などの高リスクポートへの無制限アクセスを許可します。セキュリティグループまたは NACLs に適切なルールを実装して、これらの高リスクポートへのアクセスを制限するには、step-by-stepの手順に従います。
- インターネットに開かれているコンピューティングリソースとネットワークリソース — インターネットゲートウェイとの接続を介してインターネットから到達可能なリソースを特定します。
- で完全に保護されていないインターネット向けリソース AWS WAF — インターネットから到達可能なリソースを特定し、その AWS WAF 保護のステータスを理解します。レート制限ルールや AWS Managed Rules ルールグループなどのルールを使用するための推奨事項など AWS WAF、設定とデプロイのstep-by-stepの手順に従います。
- 既知の脅威にさらされているリソース – 分散型サービス拒否 (DDoS) 攻撃、SQL インジェクション攻撃、クロスサイトスクリプティング (XSS) 攻撃など、既知の脅威にさらされているリソースを特定します。カスタムルールまたは AWS WAF AWS マネージドルールルールグループを実装するstep-by-stepの手順に従って、これらの脅威から保護します。
- 有効になっているが、コンピューティングまたはネットワークリソースにアタッチされていないネットワークセキュリティサービス — 現在、コンピューティングまたはネットワークリソースを保護していない AWS WAF ウェブ ACLs と VPC セキュリティグループ、および NACLs を特定します。今後コンピューティングリソースまたはネットワークリソースに関連付ける場合は、それらを削除するか、推奨ルールを追加して保護を改善する手順に従います。

ネットワークセキュリティディレクターの主な概念

> **Note**
>
> AWS Shield Network Security Director はパブリックプレビューリリースであり、変更される可能性があります。

リソース

アプリケーショントラフィックを処理するコンピューティング、ネットワーキング、およびセキュリティリソース:

- コンピューティング — Amazon Elastic Compute Cloud インスタンス
- ネットワーキング — Application Load Balancer、Amazon API Gateway、Amazon CloudFront ディストリビューション、VPC サブネット、VPC Elastic Network Interface (ENI)
- セキュリティ – AWS WAF ウェブ ACLs、VPC セキュリティグループ、VPC ネットワークアクセスコントロールリスト (NACLs)

検出結果

重要度レベルが NONE、 INFORMATIONAL、LOW、MEDIUM、HIGH、または CRITICAL であるネットワークセキュリティサービスの欠落または誤設定に関するアラート。 ネットワークセキュリティディレクターは、各リソースの設定と脅威インテリジェンスを評価することで検出結果を生成します。

緊急度

AWS ベストプラクティスと脅威インテリジェンスに基づく、潜在的なセキュリティイベントに対するリソースの脆弱性の尺度。重要度評価では、潜在的な脆弱性と既存の保護の両方を考慮します。リソースの重要度レベルは、最も重大な検出結果と一致するか、検出結果がない場合は「なし」と表示されます。

ネットワークトポロジ

リソース接続、インターネットへの公開、タグベースの関係を示すネットワークの視覚的表現。トポロジビューを使用して、リソースとその検出結果を調査します。

ネットワークセキュリティディレクターの検出結果を理解する

> **Note**
>
> AWS Shield Network Security Director はパブリックプレビューリリースであり、変更される可能性があります。

ネットワークセキュリティディレクターは、分析するリソースのタイプごとに特定の検出結果を生成します。これらの検出結果は、セキュリティの問題を特定し、適切なアクションを実行するのに役立ちます。次の表に、考えられるすべての検出結果をリソースタイプ別に一覧表示します。

リソースタイプ別のネットワークセキュリティディレクターの検出結果は

リソースタイプ	結果の説明
Application Load Balancer	• CloudFront オリジンはCloudFront 保護なしでインターネットにアクセス可能 • AWS WAF 欠落しているボットとスクレイパーのルール • 検出された DDoS アクティビティ • リソースには保護用のファイアウォールがアタッチされていません • AWS WAF すべてのルールが欠落 - 保護なし、設定ミスの可能性 • AWS WAF キーの欠落 AWS マネージドルール (IP 評価、一般的なルール、または不正な入力)
Amazon API Gateway	• AWS WAF 欠落しているボットとスクレイパーのルール • リソースには保護用のファイアウォールがアタッチされていません • AWS WAF すべてのルールが欠落 - 保護なし、設定ミスの可能性 • AWS WAF キーの欠落 AWS マネージドルール (IP 評価、一般的なルール、または不正な入力)
Amazon CloudFront	• AWS WAF 欠落しているボットとスクレイパーのルール • 検出された DDoS アクティビティ • リソースには保護用のファイアウォールがアタッチされていません • AWS WAF すべてのルールが欠落 - 保護なし、設定ミスの可能性 • AWS WAF キーの欠落 AWS マネージドルール (IP 評価、一般的なルール、または不正な入力)
Amazon Elastic Compute Cloud (EC2) インスタンス	• すべてのポートで無制限のインバウンドアクセス (0.0.0.0/0) を許可する

リソースタイプ	結果の説明
	• RDP ポート 3389 への無制限のインバウンドアクセス (0.0.0.0/0) を許可する • SSH ポート 22 への無制限のインバウンドアクセス (0.0.0.0/0) を許可する • すべてのポートで無制限のアウトバウンドアクセス (0.0.0.0/0) を許可する • リソースには保護用のファイアウォールがアタッチされていません • CloudFront オリジンはCloudFront 保護なしでインターネットにアクセス可能 • リソースには保護用のファイアウォールがアタッチされていません • AWS WAF 欠落しているボットとスクレイパーのルール • AWS WAF すべてのルールが欠落 - 保護なし、設定ミスの可能性 • AWS WAF キーの欠落 AWS マネージドルール (IP 評価、一般的なルール、または不正な入力)
VPC セキュリティグループ	• すべてのポートで無制限のインバウンドアクセス (0.0.0.0/0) を許可する • RDP ポート 3389 への無制限のインバウンドアクセス (0.0.0.0/0) を許可する • SSH ポート 22 への無制限のインバウンドアクセス (0.0.0.0/0) を許可する • すべてのポートで無制限のアウトバウンドアクセス (0.0.0.0/0) を許可する

リソースタイプ	結果の説明
VPC ネットワークアクセスコントロールリスト (NACL)	• すべてのポートで無制限のインバウンドアクセス (0.0.0.0/0) を許可する • RDP ポート 3389 への無制限のインバウンドアクセス (0.0.0.0/0) を許可する • SSH ポート 22 への無制限のインバウンドアクセス (0.0.0.0/0) を許可する • すべてのポートで無制限のアウトバウンドアクセス (0.0.0.0/0) を許可する
AWS WAF ウェブ ACL	• ボットアクティビティが検出されました • AWS WAF 欠落しているボットとスクレイパーのルール • AWS WAF WebACL はどのリソースにも関連付けられていません • AWS WAF すべてのルールが欠落 - 保護なし、設定ミスの可能性 • AWS WAF キーの欠落 AWS マネージドルール (IP 評価、一般的なルール、または不正な入力)

AWS Shield ネットワークセキュリティディレクターを使用するようにアカウントを設定する

> **Note**
>
> AWS Shield Network Security Director はパブリックプレビューリリースであり、変更される可能性があります。

AWS Shield ネットワークセキュリティディレクターは、 AWS 組織内の複数のアカウントでセキュリティを管理することを Organizations に要求します。このトピックでは、Organizations の設定、委任管理者の指定、必要な IAM アクセス許可の設定など、 AWS 環境を準備するための準備手順について説明します。これらの事前セットアップステップには料金はかかりません。使用した AWS サービスに対してのみ課金されます。

前提条件

AWS Shield Network Security Director を使用する前に、以下を設定する必要があります。

- AWS Organizations - AWS Shield ネットワークセキュリティディレクターは AWS 、Organizations とのみ連携し、複数のアカウントにわたるセキュリティ分析を提供します。単一のスタンドアロンアカウントで AWS Shield Network Security Director を使用することはできません。
- 管理アカウントアクセス - AWS Shield ネットワークセキュリティディレクターの委任管理者を指定するには、 AWS Organizations 管理アカウントにアクセスする必要があります。
- 委任管理者アカウント - AWS Shield ネットワークセキュリティディレクターの委任管理者として機能するアカウントを特定または作成する必要があります。これは Organizations 管理アカウントにすることはできません。

> **Important**
>
> AWS Shield Network Security Director は、スタンドアロン AWS アカウントでは使用できません。 AWS Organizations には、管理アカウントに加えて、少なくとも 1 つのメンバーアカウントを設定する必要があります。

AWS Organizations の統合について

AWS Organizations は、 AWS 管理者が複数のアカウントを統合して管理できるようにするグローバル AWS アカウント管理サービスです。 AWS Shield ネットワークセキュリティディレクターは Organizations と統合して、組織全体で一元的なセキュリティ分析と管理を提供します。

AWS Shield ネットワークセキュリティディレクターを AWS Organizations と統合する場合:

- Organizations 管理アカウントは、 AWS Shield ネットワークセキュリティディレクターの委任管理者を指定します。
- 委任管理者は、複数のアカウントとリージョンで AWS Shield ネットワークセキュリティディレクターを有効にできます。
- セキュリティ分析と検出結果は、委任管理者アカウントを通じて一元管理されます。
- サービスにリンクされたロールは、分析を有効にするためにメンバーアカウントで自動的に作成されます。

このアプローチは、 AWS Security Hub などの他の AWS セキュリティサービスに似ており、セキュリティツール全体で一貫したガバナンスを提供します。

委任管理者の選択

委任管理者は、組織に代わって AWS Shield ネットワークセキュリティディレクターを管理するアクセス許可が付与された組織内の AWS アカウントです。委任管理者は、サービスを有効にし、ポリシーを作成し、すべてのメンバーアカウントでセキュリティ検出結果を管理できます。

委任された管理者の要件:

- AWS Organizations 構造のメンバーアカウントである必要があります
- Organizations 管理アカウントにすることはできません
- 適切な IAM アクセス許可を設定する必要があります (次のセクションを参照)

> **Note**
>
> ベストプラクティスとして、一貫したガバナンスと管理の簡素化のために、 AWS セキュリティサービス (Security Hub、GuardDuty、 AWS Shield ネットワークセキュリティディレクターなど) 全体で同じ委任管理者アカウントを使用することをお勧めします。

委任管理者の IAM 要件

委任管理者アカウントには、 AWS Shield ネットワークセキュリティディレクターを効果的に管理するための特定の IAM アクセス許可が必要です。委任管理者アカウントの AWS Shield ネットワークセキュリティディレクターを管理する IAM ユーザーまたはロールに、次のポリシーをアタッチする必要があります。

AWS Shield ネットワークセキュリティディレクターの委任管理者に必要な IAM ポリシー:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "network-security-director:*"
            ],
```

```
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": [
                "arn:aws:iam:::role/aws-service-role/
AWSServiceRoleForNetworkSecurityDirector"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListRoots",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListDelegatedAdministrators",
                "organizations:DescribeOrganization",
                "organizations:CreatePolicy",
                "organizations:UpdatePolicy",
                "organizations:DeletePolicy",
                "organizations:AttachPolicy",
                "organizations:DetachPolicy",
                "organizations:EnablePolicyType",
                "organizations:DisablePolicyType",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListRoots",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListTagsForResource",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListHandshakesForAccount",
```

```
                "organizations:DescribePolicy",
                "organizations:DescribeEffectivePolicy",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

ポリシーの説明:

- network-security-director:* - サービスの有効化、ポリシーの作成、検出結果の管理など、すべての AWS Shield ネットワークセキュリティディレクターオペレーションへのフルアクセスを許可します。
- IAM アクセス許可 - 委任された管理者が、 AWS Shield ネットワークセキュリティディレクターがメンバーアカウント間で分析を実行するために使用するサービスにリンクされたロールを管理できるようにします。

IAM ポリシーを作成してアタッチするには

1. 委任管理者アカウントを使用して AWS マネジメントコンソールにサインインします。
2. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
3. ナビゲーションペインで、[ポリシー]、[ポリシーの作成] の順に選択します。
4. JSON タブを選択し、上記のポリシードキュメントを貼り付けます。
5. 次へ: タグ、次へ: レビューを選択します。
6. [Name] (名前) に **`NetworkSecurityDirectorDelegatedAdminPolicy`** と入力します。
7. [ポリシーの作成] を選択します。
8. このポリシーを、委任管理者アカウントの AWS Shield ネットワークセキュリティディレクターを管理する IAM ユーザーまたはロールにアタッチします。

セットアップチェックリスト

AWS Shield Network Security Director を有効にする前に、次のセットアップタスクが完了していることを確認してください。

- AWS ✓組織は管理アカウントと少なくとも 1 つのメンバーアカウントで設定されています
- ✓ 委任管理者アカウントを特定しました (管理アカウントは使用できません)
- ✓ 必要な IAM ポリシーが作成され、委任管理者アカウントにアタッチされました
- ✓ Organizations 管理アカウントと委任管理者アカウントの両方にアクセスできます

これらのセットアップタスクが完了したら、AWS Shield ネットワークセキュリティディレクターの有効化 に進み、組織の AWS Shield ネットワークセキュリティディレクターを有効にできます。

AWS Shield ネットワークセキュリティディレクターの有効化

> **Note**
>
> AWS Shield ネットワークセキュリティディレクターはパブリックプレビューリリースであり、変更される可能性があります。

AWS Shield ネットワークセキュリティディレクターは、 AWS Organizations を通じて AWS アカウントに対して有効になっています。ドキュメントのこのセクションでは、 AWS 組織の AWS Shield ネットワークセキュリティディレクターを有効にするために必要なすべての手順について説明します。

このセクションでは、ネットワークセキュリティディレクターのセットアップを完了するために必要な 2 つのステップについて説明します。

1. Organization AWS 管理アカウントは、 AWS Shield ネットワークセキュリティディレクターを有効にし、組織の委任管理者を指定し、対応する委任管理者ポリシーを作成します。
2. 組織の委任管理者は、組織内のユーザーが選択したリージョンとターゲットメンバーアカウントの AWS Shield ネットワークセキュリティディレクターを有効にするポリシーを作成します。

AWS Shield ネットワークセキュリティディレクターの有効化とサービス管理者の委任

AWS Shield ネットワークセキュリティディレクターに委任管理者アカウントを割り当てるときに、Security AWS Hub などの別のセキュリティサービス用にすでに設定されている場合、 AWS Shield ネットワーク AWS セキュリティディレクターは既存の委任管理者を推奨します。委任された管理者が存在しない場合は、組織からメンバーアカウントを選択するように求められます。組織の管理アカウントを委任管理者として指定することはできません。

AWS Shield ネットワークセキュリティディレクターの管理者を指定するには

1. AWS Organization 管理 AWS アカウントの認証情報を使用してアカウントにサインインし、https://console.aws.amazon.com/wafv2/network-security-director/ で AWS Shield ネットワークセキュリティディレクターコンソールを開きます。
2. ネットワークセキュリティディレクターのホームページから、開始方法 を選択します。
3. 委任管理者アカウントでは、提供されたオプションに基づいて管理者アカウントを選択します。ベストプラクティスとして、一貫したガバナンスのために、すべてのセキュリティサービスで同じ委任管理者を使用することをお勧めします。
4. 委任管理者ポリシーで、次のいずれかのオプションを選択してポリシーステートメントを追加します。

    a. (オプション 1) [これを更新する] を選択します。ポリシーステートメントの下にあるチェックボックスをオンにして、 AWS Shield ネットワークセキュリティディレクターが委任管理者に必要なすべてのアクセス許可を付与する委任ポリシーを自動的に作成することを確認します。

    b. (オプション 2) [手動でアタッチする] を選択します。[コピーしてアタッチ] を選択します。AWS Organizations コンソールの AWS 「Organizations の委任管理者」で、「委任」を選択し、委任ポリシーエディタでリソースポリシーを貼り付け、「ポリシーの作成」を選択します。 AWS Shield ネットワークセキュリティディレクターコンソールにあるタブを開きます。
5. Complete get started を選択します。

このステップの最後に、以下のアクションが完了します。

- AWS Shield ネットワークセキュリティディレクターの信頼されたアクセスの有効化。これにより、ネットワークセキュリティディレクターは、ポリシーの範囲内のメンバーアカウント内にサービスにリンクされたロールを作成できます。
- 組織の管理アカウントのサービスにリンクされたロール AWSServiceRoleForNetworkSecurityDirector の作成。
- AWS Shield ネットワークセキュリティディレクターの委任管理者の登録。
- リソースポリシーを更新し、 AWS Shield ネットワークセキュリティディレクターの委任管理者が AWS Organizations APIsに必要な呼び出しを実行できるようにします。

セットアップが完了すると、設定ページにリダイレクトされます。このページでは、委任管理者の更新または削除、委任ポリシーの管理、サービスとしてのネットワークセキュリティディレクターの無効化を行うことができます。組織の管理アカウントを使用して今後この設定ページにアクセスするには、ネットワークセキュリティディレクターコンソールに移動し、設定の管理を選択します。

委任された管理者を持つメンバーアカウントの AWS Shield ネットワークセキュリティディレクターの有効化

このステップは、委任された管理者が完了する必要があります。 AWS 組織の管理アカウントが委任管理者を指定すると、その管理者は組織内のリージョンを有効にするアクセス許可を付与するポリシーを作成する必要があります。設定されているすべてのポリシーは、 AWS Shield ネットワークセキュリティディレクターコンソールのリージョンとアカウントポリシーセクションで使用できます。以下の手順では、このポリシーを作成する方法の概要を説明します。

ターゲットアカウントのリージョンを有効にするポリシーを作成してアタッチするには

1. 委任管理者認証情報を使用して AWS アカウントにサインインし、https://console.aws.amazon.com/wafv2/network-security-director/ で AWS Shield ネットワークセキュリティディレクターコンソールを開きます。
2. AWS Shield ネットワークセキュリティディレクターのホームページから、有効化を選択します。
3. 詳細 に、ポリシーの名前とオプションの説明を入力します。
4. [アカウントの選択] では、次のいずれかのオプションを選択します。ポリシーをすべての組織単位とアカウントに適用する場合は、[すべての組織単位とアカウントに適用] を選択します。特定の組織単位とアカウントにポリシーを適用する場合は、[特定の組織単位とアカウントに適用] を選択します。検索バーまたは組織構造ツリーを使用して、ポリシーが適用される組織単位とアカウントを指定します。

5. リージョンでは、このポリシーで有効または無効にするリージョンを選択します。選択を完了するパフォーマンスに関する考慮事項前に、「」を参照してください。
6. 変更を確認し、ネットワークセキュリティディレクターを有効にするを選択します。

このステップの最後に、以下のアクションが完了します。

- 現在の委任管理者アカウントのサービスにリンクされたロール AWSServiceRoleForNetworkSecurityDirector の作成。
- AWS Shield ネットワークセキュリティディレクターが有効なリージョンとアタッチされたターゲットでスキャンを実行できるようにするポリシーの作成。
- 概要ダッシュボードへのリダイレクト。組織全体のインサイトと、各アカウントのリソースレベルの詳細を表示できます。

セットアップが完了すると、概要ダッシュボードページにリダイレクトされ、組織全体のインサイトと各アカウントのリソースレベルの詳細を表示できます。今後、委任管理者アカウントでポリシーを管理するには、ネットワークセキュリティディレクターコンソールに移動し、設定の管理を選択します。

リソースと検出結果の調査

AWS Shield ネットワークセキュリティディレクターダッシュボードには、最も重大な検出結果の概要、含まれているリージョン別の検出結果の比較、分析されたアカウントのテーブル、アカウントの選択時に表示されるパネル、そのパネル内のリソースが選択されると入力されるネットワークトポロジが表示されます。

> **Note**
>
> ネットワークセキュリティディレクターダッシュボードでリソースと検出結果を表示するには、委任管理者認証情報を使用してサインインする必要があります。

検出結果があるアカウントを特定するには

1. 委任管理者アカウントでサインインし、https://console.aws.amazon.com/wafv2/network-security-director/ で AWS Shield ネットワークセキュリティディレクターコンソールを開きます。

2. ナビゲーションペインのネットワークセキュリティディレクターで、ダッシュボードを選択します。
3. 概要ダッシュボードには、次のウィジェットが表示されます。

リージョンウィジェット

リージョンウィジェットは、最も重要な検出結果を強調表示します。これは、リソースに関するすべての検出結果と、それらを組み合わせた重要度を表します。その横には、現在のリージョンが含まれ、有効なすべてのリージョンで重要度の検出結果の比較の概要を示すグラフがあります。これにより、リージョンごとに重要な問題をすばやく特定し、そのリージョンにレビューすべき結果がある場合にリージョンを切り替える必要があることを示す指標が得られます。

アカウントウィジェット

現在のリージョンで分析されたアカウントは、複合検出結果の重要度が最も高いリソースを持つアカウントを表示するように設定されたデフォルトのソートがテーブルに表示されます。アカウントを選択して、複合結果の重要度別にリソースを表示するパネルを開くことができます。

検出結果があるリソースを特定するには

1. ネットワークセキュリティディレクターダッシュボードから、アカウントウィジェットに移動します。
2. 複合重要度の検出結果の数を示すアカウントを選択します。
3. これにより、アカウントとトポロジのエクスプローラーパネルウィジェットでリソースが開きます。

影響を受けるリソースを特定し、特定の修復推奨事項を見つけるには、以下のセクションを参照してください。

ネットワーク分析が完了すると、ネットワークセキュリティディレクターは、リソースの検出結果で特定された脆弱性を修正するための詳細な推奨事項を提供します。リソース ID、重要度レベル、リソースタイプ、または関連する 検出結果 に基づいて、脆弱なリソースについてフィルタリングできます。デフォルトでは、リソース テーブルには、最も高い重要度から最も低い重要度の順にリソースが表示されます。

アカウントとトポロジエクスプローラーパネルウィジェット

アカウントを選択すると、アカウントとトポロジエクスプローラーパネルウィジェットが開き、そのアカウント内のリソースと結果が表示されます。内のテーブルをフィルタリングして特定のリソースまたは検出結果を検索するか、フィルターを削除してリソースタイプと検出結果タイプの概要を表示します。

AWS Shield Network Security Director は、最新のネットワーク分析の各検出結果に重要度レベルを割り当てます。リソースには、None、Informational、Low、Medium、High、または Critical を割り当てることができます。この重要度レベルは、リソースで特定された最も重大な検出結果の重要度レベルを表します。例えば、最新のネットワーク分析で Amazon EC2 インスタンスに 1 つの中重要度検出結果と 2 つの低重要度検出結果があると判断された場合、そのリソースには中複合検出結果の重要度レベルが割り当てられます。

アカウントおよびトポロジエクスプローラーパネルウィジェット内の検出結果の概要ウィジェットには、リソースフィルターまたは検出結果タイプフィルターを削除してアクセスでき、ネットワークセキュリティディレクターがリソースで検出した検出結果を理解する 2 つの方法があります。

- 最も高い重要度のリソース から、すべてのネットワークリソースでどの重要度レベルが最も重要度が高いかをすばやく把握できます。また、影響を受けるリソースの数と、ネットワークセキュリティディレクターによって各重要度レベルに割り当てられたリソースの数のリストを表示することもできます。
- 重要度分布 から、各リソースタイプの特定の重要度レベルを持つリソースの数を表示し、他のリソースタイプのリソースと比較できます。

ネットワークトポロジを調べるには

1. ナビゲーションペインのネットワークセキュリティディレクターで、ダッシュボードを選択します。
2. ネットワークセキュリティディレクターダッシュボードから、アカウントウィジェットに移動します。
3. 複合重要度の検出結果の数を示すアカウントを選択します。
4. これにより、アカウントとトポロジエクスプローラーパネルウィジェットのリソースが開きます。

AWS Shield Network Security Director は、分析中にリソースの接続をマッピングします。これらの接続は、アカウントウィジェットの下のダッシュボードのウィジェットに表示されるネットワークト

ポロジで視覚化されます。アカウントを選択し、アカウントとトポロジエクスプローラーパネルウィジェットでリソースを選択すると、選択したリソースのコンテキストにネットワークトポロジの視覚化が表示されます。

ネットワークトポロジウィジェット

ネットワークトポロジは、アカウントおよびトポロジエクスプローラーパネルウィジェットで特定のリソースが選択されるまで空の状態で存在します。これは、アカウントテーブルウィジェットでアカウントが選択されたときに表示されます。ネットワークトポロジは、キャンバスをドラッグするか、コンテナの右下隅にあるズームコントロールを使用してナビゲートできます。キャンバスのズームと位置をリセットし、その内容をエクスポートするコントロールもあります。トポロジは、更新された分析結果の場合に更新でき、そのビューを拡張して画面全体にトポロジを表示することもできます。トポロジーでリソースを選択すると、アカウントとトポロジーエクスプローラーパネルウィジェットでその詳細が表示されます。リソースエッジ接続を選択すると、トポロジ内の 2 つのリソース間の関係の性質の詳細が表示されます。

> **Note**
>
> ネットワークトポロジは、選択したリソースから接続されたネットワークリソースにトラバースすることで構築されます。トポロジの視覚化には、接続された最初の 100 個のリソースのみが重要度別にソートされて表示されます。このソートは、取得された 100 件の結果の最初のセットにのみ適用され、データセット全体には適用されません。

セキュリティを改善するための推奨事項を見つけるには

1. ネットワークセキュリティディレクターダッシュボードから、アカウントウィジェットに移動します。
2. 複合重要度の検出結果の数を示すアカウントを選択します。
3. これにより、アカウントとトポロジのエクスプローラーパネルウィジェットでリソースが開きます。
4. ウィジェットでリソースを選択すると、その詳細が表示され、詳細な調査のためにリソースの詳細ページに直接移動するオプションが表示されます。

リソースには、ネットワークセキュリティディレクターによって特定された複数の検出結果を含めることができます。各検出結果は、最新のネットワーク分析中に見つかったセキュリティ上の問題を表します。

- 検出結果の修復の推奨事項を展開して、詳細を確認します。
- 詳細については、ネットワークセキュリティディレクターが推奨するステップに従うか、含まれているドキュメントリンクを選択してください。

影響を受けるリソースの修復の推奨事項を確認して実装したら、全体的なセキュリティ設定に関する追加のインサイトを取得できます。Amazon Q Developer を使用して詳細な分析を行う方法については、「Amazon Q Developer でネットワークセキュリティを分析する」に進みます。

Amazon Q Developer でネットワークセキュリティを分析する

Amazon Q Developer は、生成人工知能 (生成 AI) を活用したアシスタントであり、ネットワークセキュリティディレクターと連携して、質問に答え、ネットワークセキュリティと修復オプションに関するレコメンデーションを提供するのに役立ちます。

Amazon Q Developer を操作するには、Q ボタンを選択するか、ネットワークセキュリティディレクターコンソールに表示される任意の場所で [Amazon Q Developer を試す] を選択します。このセクションでは、ネットワークセキュリティディレクター ダッシュボード から Q に質問する手順について説明します。

Amazon Q Developer と連携するには

> **Note**
>
> Amazon Q Developer とチャットする前に、ネットワーク分析を完了しておく必要があります。

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/wafv2/network-security-director/ で AWS Shield ネットワークセキュリティディレクターコンソールを開きます。
2. ネットワークセキュリティディレクターのホームページから、ダッシュボード を選択します。
3. Amazon Q Developer に質問する ウィジェットで、Amazon Q Developer チャットインターフェイスでプロンプトとして使用する質問を選択します。
4. Amazon Q Developer チャットインターフェイスで、リクエストを送信します。

質問例

以下は、ネットワークセキュリティについて Amazon Q Developer に尋ねることができる質問の例です。

- 上位のネットワークセキュリティ検出結果を特定して
- アカウント 123456789010 のネットワークセキュリティに関する上位の検出結果を特定する
- us-west-2 で上位のネットワークセキュリティの検出結果を特定する
- 環境内のネットワークセキュリティを要約して
- システムに DDoS 攻撃のリスクはありますか？
- ネットワークセキュリティを強化するにはどうすればよいですか?
- WAF で保護されていないリソースはありますか?
- 一般的なウェブの脆弱性から保護されていないリソースはどれですか?
- EC2 インスタンスに共通するネットワークセキュリティの問題は何ですか?
- 何も保護していない WAF ウェブ ACL はありますか?

データ保護に関する考慮事項

Amazon Q Developer が会話を保存する方法については、「Amazon Q Developer ユーザーガイド」の「Amazon Q Developer でのデータ保護」を参照してください。

Amazon Q Developer がクロスリージョン処理を使用する方法については、「Amazon Q Developer ユーザーガイド」の「Amazon Q Developer でのクロスリージョン処理」を参照してください。

AWS Shield ネットワークセキュリティディレクターのクォータ

AWS アカウントには、 AWS サービスごとに、以前は制限と呼ばれていたデフォルトのクォータがあります。次の表に、ネットワークセキュリティディレクターのクォータを示します。変更可能なクォータの詳細については、「Service Quotas」を参照してください。

[リソース]	デフォルトのクォータ
スキャンごとに処理されるリソースの最大数	300,000
リソースあたりのエッジの最大数	200

[リソース]	デフォルトのクォータ
組織ごとにリージョンごとに有効になるアカウントの最大数	15,000
組織あたりの 1 か月あたりの最大 Q プロンプト数	200

ネットワークセキュリティディレクターがネットワーク分析で処理できるリソースの最大数またはリソースあたりのエッジの最大数に達すると、ネットワーク分析は失敗します。失敗したネットワーク分析に対しては課金されません。

AWS Shield ネットワークセキュリティディレクターのトラブルシューティング

サポートされていないクロスアカウント共有リソース

AWS Shield Network Security Director は、特定のクロスアカウント共有リソースをサポートしていません。これらのリソースをスキャンしようとすると、リソースを分析できないことを示すエラーメッセージが表示されます。

サポートされていない共有リソースとエラーメッセージ

リソースタイプ	エラーメッセージ
Network Firewall FirewallPolicy	network-firewall:DescribeFirewallPolicy は共有リソースではサポートされていません
Network Firewall Stateful ルールグループ	network-firewall:DescribeRuleGroup は共有リソースではサポートされていません
Network Firewall Stateless ルールグループ	network-firewall:DescribeRuleGroup は共有リソースではサポートされていません
EC2 PrefixList	ec2:GetManagedPrefixListEntries は共有リソースではサポートされていません

リソース、結果、および抑制の可用性

アカウントが組織を離れるか、アカウントでネットワークセキュリティディレクターが無効になっている場合、以下が発生します。

- 結果とリソース: アカウントでサービスが無効になると、アカウントからの結果は削除されます。このプロセスには通常数分かかりますが、時間がかかる場合があります。
- 抑制: 抑制は、アカウントのサービスを無効にしてから 90 日以内に削除されます。この 90 日以内にアカウントに対してサービスを再度有効にしても、既存のサプレッションは引き続き利用可能になる可能性がありますが、可用性は保証されません。この不確実性を回避するには、アカウントのサービスを無効にする前に抑制を削除する必要があります。

パフォーマンスに関する考慮事項

AWS Shield Network Security Director は、組織のネットワーク分析に毎日のデータ更新を提供するように設計されています。ただし、パフォーマンスは組織のサイズとリージョンによって異なる場合があります。

アカウント数が多い組織では、更新サイクルが長くなり、個々のアカウントで数日後にデータ更新が発生する可能性があります。さらに、パフォーマンスはリージョンによって大きく異なる場合があります。特にオプトインリージョンではパフォーマンスが低下し、更新時間が長くなります。

パフォーマンスを向上させ、データ更新の頻度を高めるには、各リージョンに特に関連するアカウントのネットワークセキュリティディレクターを有効にすることをお勧めします。この推奨事項は、オプトインリージョンでは特に重要です。

その他のリソース

このトラブルシューティングガイドで対処されていない問題が発生した場合は、 AWS サポートにお問い合わせください。

AWS Shield ネットワークセキュリティディレクターの使用におけるセキュリティ

> **Note**
>
> AWS Shield Network Security Director はパブリックプレビューリリースであり、変更される可能性があります。

このセクションでは、このネットワークセキュリティディレクタープレビューを使用する際のセキュリティに関する重要な考慮事項について説明します。

データソース

分析を実行すると、Network Security Director はパブリック AWS API エンドポイントを使用してAWS リソースに関する情報を取得します。取得される情報には、 AWS APIs を通じてアカウントで使用できるリソース属性が含まれます。

AWS Shield ネットワークセキュリティディレクターは、内部 AWS データソースと脅威インテリジェンスを使用して検出結果を特定し、修復を推奨します。

データ暗号化

ネットワークセキュリティディレクターを使用する場合は、次の暗号化に関する考慮事項を確認してください。

- 保管時の暗号化 – すべてのデータは保管時に保護されます。
- 転送中の暗号化 – 転送中のすべてのデータは、Transport Layer Security (TLS) 暗号化を使用して保護されます。すべての通信は、Amazon Simple Storage Service AWS 署名バージョン 4 (SigV4) を使用して認証されます。SigV4 の詳細については、Amazon S3 ユーザーガイド」の「リクエストの認証 (AWS 署名バージョン 4)」を参照してください。
- キー管理 – カスタマーマネージドキーは、現在サポートされていません。

トピック

- AWS Shield ネットワークセキュリティディレクターの Identity and Access Management
- AWS Shield ネットワークセキュリティディレクターのアイデンティティベースのポリシーの例
- AWS Shield ネットワークセキュリティディレクターのサービスにリンクされたロールの使用

AWS Shield ネットワークセキュリティディレクターの Identity and Access Management

> **Note**
>
> AWS Shield ネットワークセキュリティディレクターはパブリックプレビューリリースであり、変更される可能性があります。

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に AWS Shield ネットワークセキュリティディレクターリソースの使用を許可する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで使用できる AWS のサービス です。

このセクションのガイダンスを確認して、 AWS Shield ネットワークセキュリティディレクターでサポートされているポリシーとロールを使用する方法を理解します。

AWS Shield ネットワークセキュリティディレクターと IAM の連携方法

このセクションでは、 AWS Shield ネットワークセキュリティディレクターで IAM の機能を使用する方法について説明します。

IAM を使用してネットワークセキュリティディレクターへのアクセスを管理する前に、ネットワークセキュリティディレクターで使用できる IAM 機能を確認してください。

AWS Shield ネットワークセキュリティディレクターで使用できる IAM 機能

IAM 機能	AWS Shield ネットワークセキュリティディレクターのサポート
アイデンティティベースのポリシー	はい
サービスにリンクされたロール	はい

ネットワークセキュリティディレクターやその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要については、IAM ユーザーガイドのAWS 「IAM と連携する のサービス」を参照してください。

ネットワークセキュリティディレクターのアイデンティティベースのポリシー

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

AWS Shield ネットワークセキュリティディレクターのアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS Shield ネットワークセキュリティディレクターのアイデンティティベースのポリシーの例。

ネットワークセキュリティディレクターのサービスにリンクされたロール

サービスリンクロールのサポート: あり

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。

ネットワークセキュリティディレクターのサービスリンクロールの作成または管理の詳細については、「AWS Shield ネットワークセキュリティディレクターのサービスにリンクされたロールの使用」を参照してください。

AWS Shield ネットワークセキュリティディレクターのアイデンティティベースのポリシーの例

> **Note**
>
> AWS Shield ネットワークセキュリティディレクターの使用を開始すると、すべての最小アクセス許可要件を満たすサービスにリンクされたロールが自動的に作成されます。独自のアイデンティティベースのポリシーの作成と管理はオプションです。

ネットワークセキュリティディレクターに適切なアクセスを提供するために、管理アクセスと読み取り専用アクセスに必要なアクセス許可を付与するアイデンティティベースのポリシーを作成できます。

IAM ポリシーの作成と管理の詳細については、「IAM ユーザーガイド」の「マネージドポリシーとインラインポリシー」を参照してください。

これらのアクセス許可により、 AWS Shield ネットワークセキュリティディレクターは包括的なセキュリティ分析を実行し、正確なネットワークセキュリティの推奨事項を提供できます。このガイドで提供されるポリシーの例は、一般的なユースケース向けに設計されています。これらのポリシーを出発点として使用し、特定の要件を満たすように必要に応じて変更することができます。

このガイドのポリシーの例

- 管理アクセスアイデンティティベースのポリシー
- 読み取り専用アクセスアイデンティティベースのポリシー

ポリシーに関するベストプラクティス

ID ベースのポリシーは、あるユーザーがアカウント内でネットワークセキュリティディレクターリソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションでは、 AWS アカウントに費用が発生する場合があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、IAM ユーザーガイド の AWS マネージドポリシー または ジョブ機能のAWS マネージドポリシー を参照してください。
- 最小特権を適用する – IAM ポリシーでアクセス許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、IAM ユーザーガイド の IAM でのポリシーとアクセス許可 を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。たとえば、ポリシー条件を記述して、すべてのリクエ

ストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用されている場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます CloudFormation。詳細については、IAM ユーザーガイド の IAM JSON ポリシー要素:条件 を参照してください。

- IAM アクセスアナライザー を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM アクセスアナライザー は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイド の IAM Access Analyzer でポリシーを検証する を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイド の MFA を使用した安全な API アクセス を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイド の IAM でのセキュリティのベストプラクティス を参照してください。

アイデンティティベースのポリシーの更新

ネットワークセキュリティディレクターに更新と機能が追加されると、追加のアクセス許可を含めるようにアイデンティティベースのポリシーを更新する必要がある場合があります。このガイドでは、必要となる可能性がある新しいアクセス許可について説明します。

AWS 管理ポリシーとは異なり、カスタマー管理ポリシーは自動的に更新されません。必要に応じて、お客様はこれらのポリシーを維持および更新する責任があります。

詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

管理アクセスアイデンティティベースのポリシー

次の例を使用してアイデンティティベースのポリシーを作成し、ネットワークセキュリティディレクターオペレーションへのフル管理アクセスと、必要なサービスにリンクされたロールを作成する機能を提供します。

ポリシー名: NetworkSecurityDirectorAdminPolicy

ポリシーの説明: Network AWS Shield Security Director オペレーションへの完全な管理アクセスを許可し、Network Security Director のサービスにリンクされたロールを作成または削除するためのアクセスを提供します。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "network-security-director:*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/network-security-
director.amazonaws.com/AWSServiceRoleForNetworkSecurityDirector"
    }
  ]
}
```

読み取り専用アクセスアイデンティティベースのポリシー

次のポリシー例を使用してアイデンティティベースのポリシーを作成して、ネットワークセキュリティディレクターオペレーションへの読み取り専用アクセスを提供します。

ポリシー名: NetworkSecurityDirectorReadOnlyPolicy

ポリシーの説明: AWS Shield ネットワークセキュリティディレクターへの読み取り専用アクセスを許可します。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "network-security-director:Get*",
        "network-security-director:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Shield ネットワークセキュリティディレクターのサービスにリンクされたロールの使用

このセクションでは、サービスにリンクされたロールを使用して、 AWS Shield ネットワークセキュリティディレクターに AWS アカウントのリソースへのアクセスを許可する方法について説明します。

AWS Shield ネットワークセキュリティディレクターは AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスにリンクされたロールは、 AWS Shield ネットワークセキュリティディレクターに直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは、 AWS Shield ネットワークセキュリティディレクターによって事前定義されており、サービスがユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、 AWS Shield ネットワークセキュリティディレクターの設定が簡単になります。 AWS Shield ネットワークセキュリティディレクターは、サービスにリンクされたロールのアクセス許可を定義し、特に定義されている場合を除き、 AWS Shield ネットワークセキュリティディレクターのみがそのロールを引き受けることができます。定義された許可には、信頼ポリシーと許可ポリシーが含まれます。この許可ポリシーを他の IAM エンティティにアタッチすることはできません。

IAM コンソールで、完全にサービスにリンクされたロール: NetworkSecurityDirectorServiceLinkedRolePolicy を参照してください。

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するにはアクセス許可を設定する必要があります。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの許可」を参照してください。

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連携するAWS サービス」を参照して、サービスにリンクされたロール列がはいになっているサービスを見つけてください。サービスにリンクされた役割に関するドキュメントをサービスで表示するには[はい] リンクを選択してください。

AWS Shield ネットワークセキュリティディレクターのサービスにリンクされたロールのアクセス許可

NetworkSecurityDirectorServiceLinkedRolePolicy サービスリンクロールは、以下のサービスを信頼してロールを引き受けます。

- network-director.amazonaws.com

は、ユーザーに代わってさまざまな AWS リソースやサービスにアクセスして分析するためのアクセス許可を AWS Shield ネットワークセキュリティディレクターにNetworkSecurityDirectorServiceLinkedRolePolicy付与します。これには、以下が含まれます。

- Amazon EC2 リソースからネットワーク設定とセキュリティ設定を取得する
- CloudWatch メトリクスにアクセスしてネットワークトラフィックパターンを分析する
- ロードバランサーとターゲットグループに関する情報を収集する
- AWS WAF 設定とルールの収集
- AWS Direct Connect ゲートウェイ情報へのアクセス
- さらに、以下のアクセス許可リストで詳しく説明しています

次のリストは、特定のリソースへのダウンスコープをサポートしていないアクセス許可を対象としています。残りは、指定されたサービスリソースに対してダウンスコープされます。

```
{
 "Sid": "ResourceLevelPermissionNotSupported",
```

```
  "Effect": "Allow",
  "Action": [
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeManagedPrefixLists",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribePrefixLists",
    "ec2:DescribeRegions",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribeTransitGatewayAttachments",
    "ec2:DescribeTransitGatewayPeeringAttachments",
    "ec2:DescribeTransitGatewayRouteTables",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetTransitGatewayRouteTablePropagations",
    "ec2:GetManagedPrefixListEntries",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeTargetHealth",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeLoadBalancencerAttributes",
    "wafv2:ListWebACLs",
    "cloudfront:ListDistributions",
    "cloudfront:ListTagsForResource",
    "directconnect:DescribeDirectConnectGateways",
    "directconnect:DescribeVirtualInterfaces"
  ],
```

```
  "Resource": "*"
}
```

NetworkSecurityDirectorServiceLinkedRolePolicy サービスにリンクされたロールのアクセス許可

次のリストは、NetworkSecurityDirectorServiceLinkedRolePolicy サービスにリンクされたロールによって有効になっているすべてのアクセス許可を対象としています。

Amazon CloudFront

```
{
 "Sid": "cloudfront",
 "Effect": "Allow",
 "Action": [
   "cloudfront:GetDistribution"
 ],
 "Resource": "arn:aws:cloudfront::*:distribution/*"
}
```

AWS WAF

```
{
 "Sid": "wafv2",
 "Effect": "Allow",
 "Action": [
   "wafv2:ListResourcesForWebACL",
   "wafv2:ListRuleGroups",
   "wafv2:ListAvailableManagedRuleGroups",
   "wafv2:GetRuleGroup",
   "wafv2:DescribeManagedRuleGroup",
   "wafv2:GetWebACL"
 ],
 "Resource": [
   "arn:aws:wafv2:*:*:global/rulegroup/*",
   "arn:aws:wafv2:*:*:regional/rulegroup/*",
   "arn:aws:wafv2:*:*:global/managedruleset/*",
   "arn:aws:wafv2:*:*:regional/managedruleset/*",
   "arn:aws:wafv2:*:*:global/webacl/*/*",
```

```
    "arn:aws:wafv2:*:*:regional/webacl/*/*",
    "arn:aws:apprunner:*:*:service/*",
    "arn:aws:cognito-idp:*:*:userpool/*",
    "arn:aws:ec2:*:*:verified-access-instance/*"
  ]
 }
```

AWS WAF クラシック

```
 {
  "Sid": "classicWaf",
  "Effect": "Allow",
  "Action": [
    "waf:ListWebACLs",
    "waf:GetWebACL"
  ],
  "Resource": [
    "arn:aws:waf::*:webacl/*",
    "arn:aws:waf-regional:*:*:webacl/*"
  ]
}
```

AWS Direct Connect

```
 {
  "Sid": "directconnect",
  "Effect": "Allow",
  "Action": [
    "directconnect:DescribeConnections",
    "directconnect:DescribeDirectConnectGatewayAssociations",
    "directconnect:DescribeDirectConnectGatewayAttachments",
    "directconnect:DescribeVirtualGateways"
  ],
  "Resource": [
    "arn:aws:directconnect::*:dx-gateway/*",
    "arn:aws:directconnect:*:*:dxcon/*",
    "arn:aws:directconnect:*:*:dxlag/*",
    "arn:aws:directconnect:*:*:dxvif/*"
  ]
```

```
 }
```

AWS Transit Gateway ルート

```
{
 "Sid": "ec2Get",
 "Effect": "Allow",
 "Action": [
   "ec2:SearchTransitGatewayRoutes"
 ],
 "Resource": [
   "arn:aws:ec2:*:*:transit-gateway-route-table/*"
 ]
}
```

AWS Network Firewall

```
{
 "Sid": "networkFirewall",
 "Effect": "Allow",
 "Action": [
   "network-firewall:ListFirewalls",
   "network-firewall:ListFirewallPolicies",
   "network-firewall:ListRuleGroups",
   "network-firewall:DescribeFirewall",
   "network-firewall:DescribeFirewallPolicy",
   "network-firewall:DescribeRuleGroup"
 ],
 "Resource": [
   "arn:aws:network-firewall:*:*:*/*"
 ]
}
```

Amazon API Gateway

```
{
```

```
    "Sid": "apiGatewayGetAPI",
    "Effect": "Allow",
    "Action": [
      "apigateway:GET"
    ],
   "Resource": [
     "arn:aws:apigateway:*::/restapis",
     "arn:aws:apigateway:*::/restapis/*",
     "arn:aws:apigateway:*::/apis",
     "arn:aws:apigateway:*::/apis/*",
     "arn:aws:apigateway:*::/tags/*",
     "arn:aws:apigateway:*::/vpclinks",
     "arn:aws:apigateway:*::/vpclinks/*"
   ]
  }
```

AWS Shield ネットワークセキュリティディレクターのサービスにリンクされたロールの作成

サービスリンクロールを手動で作成する必要はありません。最初のネットワーク分析を実行すると、AWS Shield Network Security Director がサービスにリンクされたロールを作成します。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は同じ方法でアカウントにロールを再作成できます。 AWS Shield ネットワークセキュリティディレクターのログ記録を有効にすると、 AWS Shield ネットワークセキュリティディレクターはサービスにリンクされたロールを再度作成します。

AWS Shield ネットワークセキュリティディレクターのサービスにリンクされたロールの編集

AWS Shield Network Security Director では、`NetworkSecurityDirectorServiceLinkedRolePolicy`サービスにリンクされたロールを編集することはできません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロール記述の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

AWS Shield ネットワークセキュリティディレクターのサービスにリンクされたロールの削除

サービスリンクロールを必要とする機能やサービスが不要になった場合は、ロールを削除することをお勧めします。そうすることで、積極的にモニタリングまたは保守されていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

これにより、 リソースへのアクセス許可が誤って削除されないため、 AWS Shield ネットワークセキュリティディレクターのリソースが保護されます。

> **Note**
>
> リソースを削除しようとしたときに AWS Shield ネットワークセキュリティディレクターサービスがロールを使用している場合、削除が失敗する可能性があります。その場合は、数分待ってからオペレーションを再試行してください。

IAM を使用してサービスリンクロールを手動で削除するには

`NetworkSecurityDirectorServiceLinkedRolePolicy` サービスにリンクされたロールを削除するには、IAM コンソール、IAM CLI、または IAM API を使用します。詳細については、IAM ユーザーガイドの「サービスにリンクされたロールの削除」を参照してください。

AWS Shield ネットワークセキュリティディレクターのサービスにリンクされたロールでサポートされているリージョン

> **Note**
>
> AWS Shield ネットワークセキュリティディレクターはパブリックプレビューリリースであり、変更される可能性があります。

AWS Shield Network Security Director は、以下のリージョンでサービスにリンクされたロールの使用をサポートし、これらのリージョンのリソースに関するデータのみを取得できます。

リージョン名	リージョン
米国東部 (バージニア北部)	us–east–1

リージョン名	リージョン
欧州 (ストックホルム)	eu-north-1
アジアパシフィック (タイ)	ap-southeast-7
アフリカ (ケープタウン)	ap-south-1
米国東部 (オハイオ)	us-east-2
アジアパシフィック (マレーシア)	ap-southeast-5
アジアパシフィック (東京)	ap-northeast-1
米国西部 (オレゴン)	us-west-2
欧州 (スペイン)	eu-south-2
欧州 (アイルランド)	eu-west-1
欧州 (フランクフルト)	eu-central-1
アジアパシフィック (香港)	ap-east-1
アジアパシフィック (シンガポール)	ap-southeast-1
アジアパシフィック (シドニー)	ap-southeast-2

を使用した AWS Shield Network Security Director API コールのログ記録 AWS CloudTrail

AWS Shield Network Security Director は と統合 AWS CloudTrail して、すべての API コールをイベントとして記録します。この統合は、ネットワークセキュリティディレクターコンソールからの呼び出し、ネットワークセキュリティディレクター APIs、および他の AWS サービスからの呼び出しをキャプチャします。

CloudTrail を使用すると、イベント履歴で最近のイベントを表示したり、証跡を作成して Amazon Simple Storage Service バケットに継続的なログを配信したりできます。これらのログは、発信者の ID、時刻、リクエストパラメータ、レスポンスなど、各リクエストに関する詳細を提供します。

CloudTrail の詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

CloudTrail のネットワークセキュリティディレクター情報

CloudTrail は AWS アカウントで自動的に有効になります。ネットワークセキュリティディレクターでアクティビティが発生すると、CloudTrail にイベントとして記録されます。イベントの継続的な記録については、ログファイルを Amazon S3 バケットに配信する証跡を作成します。

証跡の作成と管理に関する詳細については、以下を参照してください。

- AWS アカウントの証跡の作成
- AWS CloudTrail Logs とのサービス統合
- 複数のリージョンとアカウントから CloudTrail ログファイルを受け取る

CloudTrail によってログに記録されるネットワークセキュリティディレクター API オペレーション

すべてのネットワークセキュリティディレクター API オペレーションは CloudTrail によってログに記録され、 API リファレンスに文書化されます。以下のオペレーションが含まれています。

- ListResources: サービスで使用可能なリソースを一覧表示します
- GetResource: 特定のリソースに関する詳細情報を取得します
- ListFindings: セキュリティ検出結果を一覧表示します
- GetFinding: 特定の検出結果に関する詳細情報を取得します
- UpdateFinding: 検出結果のステータスまたはその他の属性を更新します
- ListRemediations: 検出結果の修正推奨事項を一覧表示します
- ListInsights: 検出結果とリソースに基づいてインサイトを一覧表示します
- ListAccountSummaries: 組織のアカウント概要を一覧表示します

ネットワークセキュリティディレクターのログファイルエントリについて

CloudTrail ログエントリには、リクエストを行ったユーザー、リクエストが行われた日時、使用されたパラメータに関する情報が含まれます。ListAccountSummaries アクションの例を次に示します。

```
{
```

```
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111122223333:user/janedoe",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/janedoe",
        "accountId": "111122223333",
        "userName": "janedoe"
      },
      "attributes": {
        "creationDate": "2025-11-11T02:57:20Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2025-11-11T02:59:53Z",
  "eventSource": "network-security-director.amazonaws.com",
  "eventName": "ListAccountSummaries",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/1.18.147 Python/2.7.18 Linux/5.10.244-220.970.amzn2int.x86_64
 botocore/1.18.6",
  "requestParameters": {
    "status": "ACTIVE",
    "sortBy": "SEVERITY",
    "maxResults": 2
  },
  "responseElements": null,
  "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management"
}
```

Amazon CloudWatch による CloudTrail ログのモニタリング

Amazon CloudWatch を使用して、CloudTrail ログの特定の API アクティビティをモニタリングおよびアラートできます。これにより、不正アクセスの試み、設定の変更、異常なアクティビティパターンを検出できます。

CloudWatch モニタリングを設定するには:

1. CloudWatch Logs にログを送信する CloudTrail 証跡を設定する
2. ログイベントから特定の情報を抽出するメトリクスフィルターを作成する
3. これらのメトリクスに基づいてアラームを作成する

詳細な手順については、「Amazon CloudWatch Logs による CloudTrail ログファイルのモニタリング」を参照してください。

ネットワークセキュリティディレクターを使用した CloudTrail のベストプラクティス

CloudTrail でセキュリティと監査可能性を最大化するには:

- 包括的なカバレッジのために、すべてのリージョンで CloudTrail を有効にする
- 不正な変更を検出するために、ログファイルの整合性検証を有効にする
- 最小特権の原則に従って、IAM を使用して CloudTrail ログへのアクセスを制御する
- CloudWatch アラームを使用して、重要なイベントのアラートをセットアップする
- 異常なアクティビティを特定するために、CloudTrail ログを定期的に確認する

AWS Firewall Manager

AWS Firewall Manager は、Amazon VPC セキュリティグループとネットワーク ACLs、 AWS Shield Advanced Amazon Route 53 Resolver DNS Firewall AWS WAFなど、さまざまな保護のために AWS Network Firewall、複数のアカウントとリソースにわたる管理およびメンテナンスタスクを簡素化します。Firewall Manager を使用すると、保護を 1 回設定するだけで、アカウントとリソースに (追加する新しいアカウントとリソースにも) その保護が自動的に適用されます。

Firewall Manager には、次のような利点があります。

- アカウント間でリソースを保護するのに役立ちます
- すべての Amazon CloudFront ディストリビューションなど、特定のタイプのすべてのリソースを保護するのに役立ちます
- 特定のタグですべてのリソースを保護するのに役立ちます
- アカウントに追加されたリソースへの保護を自動的に追加します
- AWS Organizations 組織内のすべてのメンバーアカウントを にサブスクライブし AWS Shield Advanced、組織に参加する新しいスコープ内アカウントを自動的にサブスクライブできます。
- AWS Organizations 組織内のすべてのメンバーアカウントまたはアカウントの特定のサブセットにセキュリティグループルールを適用し、組織に参加する新しい範囲内アカウントにルールを自動的に適用できます。
- 独自のルールを使用するか、 から マネージドルールを購入できます。 AWS Marketplace

Firewall Manager は、少数の特定のアカウントやリソースではなく、組織全体を保護したい場合や、保護したい新しいリソースを頻繁に追加する場合に、特に有効です。Firewall Manager では、組織全体の DDoS 攻撃を一元的にモニタリングすることもできます。

> **Note**
>
> で発生する料金は、 AWS WAF や などの基盤となるサービスに対して AWS Firewall Manager 発生します AWS Config。詳細については、「AWS Firewall Manager 料金」を参照してください。

トピック

- AWS Firewall Manager 前提条件

- AWS Firewall Manager 管理者の使用
- AWS Firewall Manager ポリシーの設定
- AWS Firewall Manager ポリシーの使用
- Firewall Manager のマネージドリストの使用
- Firewall Manager でのリソースのグループ化する
- AWS Firewall Manager ポリシーのコンプライアンス情報の表示
- AWS Firewall Manager との統合 AWS Security Hub CSPM
- AWS Firewall Manager サービスの使用におけるセキュリティ
- AWS Firewall Manager クォータ
- Firewall Manager での AWS WAF Classic ウェブ ACLs移行

AWS Firewall Manager 前提条件

このトピックでは、 を管理する準備をする方法について説明します AWS Firewall Manager。 AWS Organizationsで組織のすべてのための Firewall Manager セキュリティポリシーを管理するには、1 つの Firewall Manager 管理者アカウントを使用します。特に記載がない限り、Firewall Manager 管理者として使用するアカウントを使用して、前提条件となるステップを実行します。

Firewall Manager を初めて使用する前に、次のステップを順番に実行してください。

トピック

- Firewall Manager を使用する AWS Organizations ための結合と設定
- AWS Firewall Manager デフォルトの管理者アカウントの作成
- Firewall Manager の使用 AWS Config の有効化
- AWS Marketplace でサブスクライブし、Firewall Manager サードパーティーポリシーのサードパーティー設定を構成する
- を使用した Network Firewall および DNS Firewall ポリシーのリソース共有の有効化 AWS RAM
- デフォルトでは無効になっているリージョン AWS Firewall Manager での の使用

Firewall Manager を使用する AWS Organizations ための結合と設定

Firewall Manager を使用するには、アカウントが Firewall Manager ポリシーを使用する AWS Organizations のサービスの組織のメンバーである必要があります。

> **Note**
>
> Organizations の詳細については、「AWS Organizations ユーザーガイド」を参照してください。

必要な AWS Organizations メンバーシップと設定を確立するには

1. Organizations で組織の Firewall Manager 管理者として使用するアカウントを選択します。
2. 選択したアカウントがまだ組織のメンバーでない場合は、そのアカウントに参加させてください。「 AWS アカウント を組織に招待する」のガイダンスに従ってください。
3. AWS Organizations には、一括請求機能とすべての機能という 2 つの機能セットがあります。Firewall Manager を使用するには、組織ですべての機能を有効にする必要があります。組織が一括請求 (コンソリデーティッドビリング) のためにのみ設定されている場合は、「組織内のすべての機能の有効化」のガイダンスに従ってください。

AWS Firewall Manager デフォルトの管理者アカウントの作成

このページでは、 AWS Firewall Manager デフォルトの管理者アカウントを作成する手順について説明します。

> **Note**
>
> この手順では、前のステップで選択および設定したアカウントと組織を使用します。

Firewall Manager のデフォルト管理者アカウントを作成できるのは、組織の管理アカウントのみです。デフォルトの管理者 アカウントは、最初に作成する管理者アカウントです。デフォルトの管理者アカウントはサードパーティのファイアウォールを管理でき、完全な管理権限範囲を持ちます。デフォルトの管理者アカウントを設定すると、Firewall Manager はそれを Firewall Manager の AWS Organizations 委任管理者として自動的に設定します。これにより、Firewall Manager は、対象の組織内の組織単位 (OU) に関する情報にアクセスできます。OU を使用して、Firewall Manager ポリシーの範囲を指定できます。ポリシーの範囲の設定の詳細については、「AWS Firewall Manager ポリシーの作成」の個々のポリシータイプに関するガイダンスを参照してください。組織と管理アカウントの詳細については、「組織の AWS アカウントの管理」を参照してください。

組織の管理アカウントに必須な設定

組織を Firewall Manager にオンボーディングし、さらにデフォルト管理者を作成するためには、組織の管理アカウントに以下の設定が必要です。

- Firewall Manager ポリシー AWS Organizations を適用する の組織のメンバーである必要があります。

デフォルトの管理者アカウントを設定するには

1. 既存の AWS Organizations 管理アカウント AWS マネジメントコンソール を使用して Firewall Manager にサインインします。
2. Firewall Manager コンソール (https://console.aws.amazon.com/wafv2/fmsv2) を開きます。
3. ナビゲーションペインで [設定] を選択します。
4. Firewall Manager 管理者として使用するように選択した AWS アカウントのアカウント ID を入力します。

   > **Note**
   >
   > デフォルトの管理者は完全な管理権限範囲を保持します。完全な管理権限範囲とは、このアカウントが組織内のすべてのアカウントと組織単位 (OU) にポリシーを適用でき、すべてのリージョンでアクションの実行が可能で、また、Firewall Manager のすべてのポリシータイプを管理できることを意味します。

5. [管理者アカウントを作成] を選択してアカウントを作成します。

Firewall Manager 管理者アカウントの管理の詳細については、「AWS Firewall Manager 管理者の使用」を参照してください。

Firewall Manager の使用 AWS Config の有効化

Firewall Manager を使用するには、 AWS Configを有効にする必要があります。

> **Note**
>
> AWS Config 料金に応じて、 AWS Config 設定に対して料金が発生します。詳細については、「 の開始方法 AWS Config」を参照してください。

> **Note**
>
> Firewall Manager がポリシーコンプライアンスをモニタリングするには、保護されたリソースの設定変更を継続的に記録 AWS Config する必要があります。 AWS Config 設定では、記録頻度をデフォルト設定である Continuous に設定する必要があります。

Firewall Manager AWS Config で を有効にするには

1. Firewall Manager 管理者アカウントを含め、 AWS Organizations メンバーアカウント AWS Config ごとに を有効にします。詳細については、「 の開始方法 AWS Config」を参照してください。
2. 保護するリソース AWS リージョン を含む各 AWS Config に対して を有効にします。 AWS Config を手動で有効にすることも、StackSets サンプル CloudFormation テンプレートでテンプレート「有効化 AWS Config」を使用することもできます。 AWS CloudFormation StackSets

   すべてのリソース AWS Config に対して を有効にしない場合は、使用する Firewall Manager ポリシーのタイプに応じて以下を有効にする必要があります。

   - WAF ポリシー – CloudFront Distribution、Application Load Balancer (リストから [ElasticLoadBalancingV2] を選択)、API Gateway、WAF WebACL、WAF Regional WebACL、および WAFv2 WebACL のリソースタイプについて Config を有効にします。 AWS Config が CloudFront ディストリビューションを保護できるようにするには、米国東部 (バージニア北部) リージョンに存在している必要があります。他のリージョンにはオプションとしての CloudFront がありません。
   - Shield ポリシー – Shield Protection、ShieldRegional Protection、Application Load Balancer、EC2 EIP、WAF WebACL、WAF Regional WebACL、および WAFv2 WebACL のリソースタイプについて Config を有効にします。
   - 共通セキュリティグループポリシー – Amazon EC2 SecurityGroup と Amazon EC2 VPC のリソースタイプと、ポリシーのリソースタイプリスト (通常は Amazon EC2 インスタンスと Amazon EC2 NetworkInterface) のリソースタイプに対して Config を有効にします。ポリシーでセキュリティグループ参照のディストリビューションを有効にする場合は、Amazon EC2 VPCPeeringConnection も有効にします。
   - セキュリティグループコンテンツ監査ポリシー – Amazon EC2 SecurityGroup、Amazon EC2 NetworkInterface、および Amazon EC2 インスタンスのリソースタイプの Config を有効にします。

- セキュリティグループ使用状況監査ポリシー – リソースタイプ Amazon EC2 SecurityGroup の Config を有効にします。
- ネットワーク ACL ポリシー — リソースタイプの Amazon EC2 サブネットと Amazon EC2 ネットワーク ACL の Config を有効にします。
- Network Firewall ポリシー – NetworkFirewall FirewallPolicy、NetworkFirewall RuleGroup、EC2 VPC、EC2 InternetGateway、EC2 RouteTable、および EC2 Subnetのリソースタイプについて Config を有効にします。
- DNS ファイアウォールポリシー – リソースタイプ EC2 VPC と Amazon Route 53 FirewallRuleGroupAssociation の Config を有効にします。
- サードパーティーファイアウォールポリシー - Amazon EC2 VPC、Amazon EC2 InternetGateway、Amazon EC2 RouteTable、Amazon EC2 サブネット、Amazon EC2 VPCEndpoint のリソースタイプについて Config を有効にします。

> **Note**
>
> カスタム IAM ロールを使用するように AWS Config レコーダーを設定する場合は、IAM ポリシーに Firewall Manager ポリシーに必要なリソースタイプを記録するための適切なアクセス許可があることを確認する必要があります。適切なアクセス許可がないと、必要なリソースが記録されず、Firewall Manager がリソースを適切に保護できなくなる可能性があります。Firewall Manager では、これらのアクセス許可の設定ミスを可視化することはできません。で IAM を使用する方法については AWS Config、「IAM forAWS Config」を参照してください。

AWS Marketplace でサブスクライブし、Firewall Manager サードパーティーポリシーのサードパーティー設定を構成する

Firewall Manager のサードパーティファイアウォールポリシーを開始するには、次の前提条件を満たします。

Fortigate Cloud Native Firewall (CNF) as a Service ポリシーの前提条件

Fortigate CNF を Firewall Manager で使用するには

1. AWS Marketplace のサービスとしての Fortigate Cloud Native Firewall (CNF) にサブスクライブします。

2. まず、Fortigate CNF 製品ポータルにテナントを登録します。次に、Fortigate CNF 製品ポータルのテナントの下に Firewall Manager の管理者アカウントを追加します。詳細については、「Fortigate CNF documentation」(Fortigate CNF ドキュメント) を参照してください。

Fortigate CNF ポリシーの操作については、「Firewall Manager に Fortigate Cloud Native Firewall (CNF) as a Service ポリシーを使用する」を参照してください。

Palo Alto Networks Cloud Next Generation Firewall ポリシーの要件

Palo Alto Networks Cloud NGFW を Firewall Manager で使用するには

1. AWS Marketplace で Palo Alto Networks Cloud Next Generation Firewall Pay-As-You-Go サービスをサブスクライブします。
2. Palo Alto Networks Cloud NGFW デプロイガイドの「Deploy Palo Alto Networks Cloud NGFW for AWSAWS Firewall Manager」トピックに記載されている Palo Alto Networks Cloud Next Generation Firewall for AWS デプロイステップを完了します。

Palo Alto Networks Cloud NGFW ポリシーの操作については、「Palo Alto Networks Cloud NGFW ポリシーを Firewall Manager で使用する」を参照してください。

を使用した Network Firewall および DNS Firewall ポリシーのリソース共有の有効化 AWS RAM

Firewall Manager Network Firewall および DNS Firewall ポリシーを管理するには、 AWS Organizations で との共有を有効にする必要があります AWS Resource Access Manager。これにより、Firewall Manager は、これらのポリシータイプを作成するときに、アカウント全体で保護をデプロイできます。

AWS Organizations で との共有を有効にするには AWS Resource Access Manager

- 「AWS Resource Access Manager ユーザーガイド」の「AWS Organizations内でリソース共有を有効にする」のガイダンスに従ってください。

リソース共有で問題が発生した場合は、「Network Firewall ポリシーと DNS Firewall ポリシーのリソース共有」のガイダンスを参照してください。

デフォルトでは無効になっているリージョン AWS Firewall Manager での の使用

デフォルトでは無効になっているリージョンで Firewall Manager を使用するには、 AWS 組織の管理アカウントと Firewall Manager のデフォルトの管理者アカウントの両方でリージョンを有効にする必要があります。デフォルトで無効になっているリージョンとそれを有効にする方法については、「AWS 全般のリファレンス」の「AWS リージョンの管理」を参照してください。

無効にしたリージョンを有効にするには

- Organizations の管理アカウントと Firewall Manager のデフォルトの管理者アカウントの両方について、「AWS 全般のリファレンス」の「リージョンを有効にする」のガイダンスに従います。

次のステップを実行した後、Firewall Manager を設定してリソースの保護を開始できます。詳細については、「AWS Firewall Manager AWS WAF ポリシーの設定」を参照してください。

AWS Firewall Manager 管理者の使用

このページでは、Firewall Manager 管理者とは何かを説明し、また、それと関連する用語を定義します。

AWS Firewall Manager では、組織のファイアウォールリソースを管理できる管理者を 1 人または複数持つことができます。組織内で複数の Firewall Manager 管理者を配置する場合は、各管理者の管理権限範囲の条件を適用することで、それぞれが管理できるリソースを定義できます。これにより、組織内のさまざまな管理者に役割を割り当てる上での柔軟性が提供され、最小権限の原則を維持しやすくなります。例えば、組織の一連の組織単位 (OU) を 1 人の管理者に管理させ、別の管理者には、特定の Firewall Manager ポリシータイプのみの管理を任せるといったことが可能です。Organizations と管理アカウントの詳細については、「組織の AWS アカウントの管理」を参照してください。

組織ごとに設定できる管理者の最大数については、「AWS Firewall Manager クォータ」を参照してください。

Firewall Manager 管理者の使用開始

Firewall Manager 管理者の使用を開始する前に、「AWS Firewall Manager 前提条件」に記載されている前提条件を完了する必要があります。前提条件では、 AWS Organizations 組織を Firewall

Manager にオンボードし、Firewall Manager のデフォルトの管理者アカウントを作成します。デフォルトの管理者アカウントは完全な管理権限範囲を持ち、サードパーティのファイアウォールを管理することができます。

管理権限範囲

管理権限範囲により、Firewall Manager 管理者が管理できるリソースが定義されます。 AWS Organizations 管理アカウントが組織を Firewall Manager にオンボーディングすると、管理アカウントは異なる管理スコープを持つ追加の Firewall Manager 管理者を作成できます。 AWS Organizations 管理アカウントは、管理者にフルまたは制限された管理範囲を付与できます。完全な管理権限範囲を持つ管理者は、前述のすべてのリソースタイプに対し完全なアクセスが可能です。制限付きの管理権限範囲とは、前述のリソースに関して部分的な管理者権限が付与されることを指します。各管理者には、それぞれの役割の遂行に必要な権限のみを付与することをお勧めします。以下の管理権限範囲の条件は、任意に組み合わせて管理者に適用できます。

- 管理者がポリシーを適用できる組織内のアカウントまたは OU。
- 管理者がアクションを実行できるリージョン。
- 管理者が管理できる Firewall Manager のポリシータイプ。

管理者のロール

Firewall Manager には、デフォルト管理者 とFirewall Manager 管理者の 2 種類の管理者ロールがあります。

- デフォルト管理者 – 組織の管理アカウントは、組織を Firewall Manager にオンボーディングする際に、AWS Firewall Manager 前提条件 を完了する段階で、Firewall Manager のデフォルト管理者アカウントを作成します。デフォルトの管理者はサードパーティのファイアウォールを管理でき、完全な管理権限範囲を持ちます。ただし、他に複数の管理者を配置する場合には、他の管理者と同じレベルの権限にもできます。
- Firewall Manager 管理者 – Firewall Manager 管理者は、 AWS Organizations の管理アカウントが管理権限範囲の設定で指定したリソースを管理できます。組織ごとに配置できる管理者の最大数については、「AWS Firewall Manager クォータ」を参照してください。Firewall Manager 管理者アカウントを作成すると、サービスは にチェック AWS Organizations して、アカウントが組織内の Firewall Manager の委任管理者として既にあるかどうかを確認します。そうでない場合、Firewall Manager は Organizations を呼び出して、対象のアカウントに Firewall Manager の管理者を委任します。Organizations での委任された管理者の詳細については、「AWS Organizations ユーザーガイド」の「AWS Organizations の用語と概念」を参照してください。

既存の管理者

現在 Firewall Manager をご利用のお客様で、すでに管理者を設定している場合には、この既存の管理者が Firewall Manager のデフォルト管理者になります。既存のフローには、特に影響を与えません。さらに管理者を追加したい場合は、この章の手順に従って設定します。

Firewall Manager 管理者アカウントの作成。

次の手順は、Firewall Manager コンソールを使用して、Firewall Manager 管理者アカウントを作成する方法を説明します。

> **Note**
>
> 組織の管理アカウントのみが、Firewall Manager 管理者アカウントを作成できます。

Firewall Manager 管理者アカウントを作成するには

1. 既存の AWS Organizations 管理アカウント AWS マネジメントコンソール を使用して Firewall Manager にサインインします。
2. Firewall Manager コンソール (https://console.aws.amazon.com/wafv2/fmsv2) を開きます。
3. ナビゲーションペインで [設定] を選択します。
4. [管理者アカウントを作成] を選択します。
5. [詳細] ペインの [AWS アカウント ID] に、Firewall Manager 管理者として追加するメンバーアカウントの AWS ID を入力します。
6. [管理権限範囲] では、以下のいずれかのオプションを選択します。

   - [完全] – これにより、管理者は組織内のすべてのアカウントと組織単位 (OU) にポリシーを適用したり、すべてのリージョンでアクションを実行したりできます。また、サードパーティのファイアウォールを除くすべてのFirewall Manager ポリシータイプを適用できます。デフォルトの管理者のみが、サードパーティのファイアウォールを作成および管理できます。このレベルのアクセス許可を管理者に付与する場合は注意が必要です。最小特権の原則を考慮した場合、管理者にはその役割の遂行に必要なアクセス許可のみを付与することが推奨されます。
   - 制限付き – 制限付きの管理権限の範囲を適用する場合は、[管理権限範囲を設定] で、そのアカウントで管理が可能なアカウントと組織単位、リージョン、ポリシータイプを設定します。

     [アカウントと組織単位] では、以下のようにオプションを選択します。

- 組織内のすべてのアカウントまたは組織単位にポリシーを適用する場合は、 AWS 組織内のすべてのアカウントを含めるを選択します。
- 特定の AWS Organizations 組織単位 (OUs) にある特定のアカウントまたはアカウントにのみポリシーを適用する場合は、指定されたアカウントと組織単位のみを含めるを選択し、含めるアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。
- 特定のアカウントまたは AWS Organizations 組織単位 (OUs) のセットを除くすべてのアカウントにポリシーを適用する場合は、指定されたアカウントと組織単位を除外し、その他をすべて含めてから、除外するアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。

[リージョン] で、以下のようにオプションを選択します。

- 使用可能なすべてのリージョンで管理者がアクションを実行できるようにするには、[すべてのリージョンを含める] を選択します。
- 管理者に特定のリージョンでのみアクションを実行させたい場合は、[指定したリージョンのみを含める] を選択した後、含めるリージョンを指定します。

> **Note**
>
> デフォルトでは無効になっているリージョンを含めるには、 AWS Organizations 組織管理アカウントとデフォルトの管理アカウントの両方でリージョンを有効にする必要があります。アカウントのリージョンを有効にする方法については、「Amazon Web Services 全般のリファレンス」の「リージョンを有効にする」を参照してください。

[ポリシータイプ] で、以下のようにオプションを選択します。

- すべてのポリシータイプの管理を管理者に許可するには、[すべてのポリシータイプを含める] を選択します。
- 管理者に特定のポリシータイプのみを管理させたい場合は、[指定したポリシータイプのみを含める] を選択し、対象のポリシータイプを指定します。

7. [管理者アカウントを作成] を選択し、管理者アカウントを作成します。作成時に、Firewall Manager は AWS Organizations を呼び出して、管理者が既に組織の委任管理者かどうかを確認します。そうでない場合、Firewall Manager は対象のアカウントを委任された管理者として指定

します。Organizations の委任された管理者の詳細については、「AWS Organizations ユーザーガイド」の「AWS Organizations の用語と概念」を参照してください。

[制限付き] の管理権限範囲を適用している場合、Firewall Manager は、設定に対応させながら新しいリソースを自動的に評価します。例えば、特定のアカウントのみを含めると、Firewall Manager は新しいアカウントにポリシーを適用しません。別の例として OU を使用しており、その OU またはその子である任意の OU にアカウントを追加した場合、Firewall Manager は、そのアカウントを対応した管理権限範囲に自動的に含めます。

Firewall Manager 管理者アカウントの更新

以下で、Firewall Manager コンソールを使用してFirewall Manager 管理者アカウントを更新するための手順について説明します。

> **Note**
>
> デフォルトでは無効になっているリージョンを含めるように管理者の範囲を更新するには、AWS Organizations 組織管理アカウントとデフォルトの管理アカウントの両方でリージョンを有効にする必要があります。アカウントのリージョンを有効にする方法については、「Amazon Web Services 全般のリファレンス」の「リージョンを有効にする」を参照してください。
> Firewall Manager 管理者アカウントの作成および更新は、組織の管理アカウントのみが実行できます。

管理者アカウントを更新するには (コンソール)

1. 既存の AWS Organizations 管理アカウント AWS マネジメントコンソール を使用して Firewall Manager にサインインします。
2. Firewall Manager コンソール (https://console.aws.amazon.com/wafv2/fmsv2) を開きます。
3. ナビゲーションペインで [設定] を選択します。
4. [Firewall Manager 管理者テーブル] で、更新する対象のアカウントを選択します。
5. 管理者アカウントの詳細を変更するには、[編集] を選択します。[アカウント ID] を変更することはできません。
6. [保存] を選択して変更を保存します。

Firewall Manager 管理者アカウントを取り消す

以下で、Firewall Manager 管理者アカウントを取り消す手順について説明します。デフォルト管理者がアカウントを取り消せるようになるためには、組織内のすべての Firewall Manager 管理者アカウントが、まず自分のアカウントを取り消す必要があります。

> **Note**
>
> 個々の Firewall Manager の管理者のみが、その Firewall Manager の管理者アカウントを取り消すことができます。

管理者アカウントを取り消すには (コンソール)

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。
2. ナビゲーションペインで [設定] を選択します。
3. [管理者アカウント] ペインで、「管理者アカウントを取り消す] を選択して、アカウントを取り消します。

> **Important**
>
> 管理者アカウントから管理者権限を取り消すと、そのアカウントによって作成されたすべての Firewall Manager ポリシーが削除されます。

デフォルトな Firewall Manager 管理者アカウントを変更する

以下で、Firewall Manager 管理者アカウントを取り消すための手順について説明します。

組織内では、1 つのアカウントのみをデフォルトの Firewall Manager 管理者アカウントとして指定できます。デフォルトの管理者アカウントは、先入れ後出しの原則に従います。異なるデフォルト管理者アカウントを指定する場合には、まず個々の管理者アカウントが自分のアカウントを取り消す必要があります。その後、既存のデフォルト管理者は自分のアカウントを取り消すことが可能になります。これにより、組織は Firewall Manager からオフボーディングされます。管理者が自分のアカウ

ントを取り消すと、そのアカウントによって作成されたすべての Firewall Manager ポリシーが削除されます。新しいデフォルトの管理者アカウントを指定するには、 AWS Organizations 管理アカウントを使用して Firewall Manager にサインインし、新しい管理者アカウントを指定する必要があります。組織のデフォルトの管理者アカウントを変更するには、次の手順を実行します。

デフォルトの管理者アカウントを変更するには

1. 既存の AWS Organizations 管理アカウント AWS マネジメントコンソール を使用して Firewall Manager にサインインします。
2. Firewall Manager コンソール (https://console.aws.amazon.com/wafv2/fmsv2) を開きます。
3. ナビゲーションペインで [設定] を選択します。
4. Firewall Manager 管理者として使用するように選択したアカウントの ID を入力します。

> **Note**
>
> このアカウントには、組織内のすべてのアカウントで Firewall Manager ポリシーを作成および管理するための許可が付与されます。

5. [管理者アカウントを作成] を選択します。
6. Firewall Manager 管理者として使用するように選択したアカウントの AWS ID を入力します。

> **Note**
>
> このアカウントには完全な管理権限範囲が与えられます。完全な管理権限範囲とは、このアカウントが組織内のすべてのアカウントと組織単位 (OU) にポリシーを適用でき、すべてのリージョンでアクションの実行が可能で、また、Firewall Manager のすべてのポリシータイプを管理できることを意味します。

7. [管理者アカウントを作成] を選択して、デフォルトの管理者アカウントを作成します。

Firewall Manager 管理者アカウントに対する変更の却下

管理者アカウントに加えられた変更の一部が却下され、管理者アカウントが維持できないことがあります。

このセクションでは、管理者アカウントを失格にする可能性がある変更と、 AWS と Firewall Manager がこれらの変更を処理する方法について説明します。

で組織から削除されたアカウント AWS Organizations

AWS Firewall Manager 管理者アカウントが の組織から削除されると AWS Organizations、組織のポリシーを管理できなくなります。Firewall Manager は、次のいずれかのアクションを実行します。

- ポリシーのないアカウント - Firewall Manager 管理者アカウントに Firewall Manager ポリシーがない場合、Firewall Manager は管理者アカウントを取り消します。
- Firewall Manager ポリシーを使用したアカウント – Firewall Manager 管理者アカウントに Firewall Manager ポリシーがある場合、Firewall Manager は AWS 、販売アカウント担当者の助けを借りて、状況を知らせ、実行できるオプションを提供するために E メールを送信します。

アカウントが閉鎖された

AWS Firewall Manager 管理者に使用しているアカウントを閉鎖 AWS し、Firewall Manager が閉鎖を次のように処理する場合:

- AWS は Firewall Manager からのアカウントの管理者アクセスを取り消し、Firewall Manager は管理者アカウントによって管理されたポリシーを無効にします。それらのポリシーによって提供された保護は、組織全体で停止されます。
- AWS は、管理者アカウントの閉鎖の発効日から 90 日間、アカウントの Firewall Manager ポリシーデータを保持します。この 90 日間の期間中、閉鎖したアカウントを再開できます。
  - 90 日間に閉鎖されたアカウントを再開すると、 はアカウントを Firewall Manager 管理者として AWS 再割り当てし、アカウントの Firewall Manager ポリシーデータを復元します。
  - それ以外の場合、90 日間の終了時に、 はアカウントのすべての Firewall Manager ポリシーデータ AWS を完全に削除します。

AWS Firewall Manager ポリシーの設定

AWS Firewall Manager を使用して、さまざまなタイプのセキュリティポリシーを有効にできます。セットアップのステップはそれぞれ少し異なります。

トピック

- AWS Firewall Manager AWS WAF ポリシーの設定
- AWS Firewall Manager AWS Shield Advanced ポリシーの設定
- AWS Firewall Manager Amazon VPC セキュリティグループポリシーの設定

- AWS Firewall Manager Amazon VPC ネットワーク ACL ポリシーの設定
- AWS Firewall Manager AWS Network Firewall ポリシーの設定
- AWS Firewall Manager DNS Firewall ポリシーの設定
- AWS Firewall Manager Palo Alto Networks Cloud Next Generation Firewall ポリシーの設定
- CNF ポリシー AWS Firewall Managerの強制設定

AWS Firewall Manager AWS WAF ポリシーの設定

を使用して組織全体 AWS Firewall Manager の AWS WAF ルールを有効にするには、次の手順を順番に実行します。

トピック

- ステップ 1: 前提条件を満たす
- ステップ 2: AWS WAF ポリシーを作成して適用する
- ステップ 3: クリーンアップする

ステップ 1: 前提条件を満たす

AWS Firewall Managerのアカウントを準備するには、いくつかの必須のステップがあります。それらのステップは、AWS Firewall Manager 前提条件 で説明されています。「ステップ 2: AWS WAF ポリシーを作成して適用する」に進む前に、すべての前提条件を満たしてください。

ステップ 2: AWS WAF ポリシーを作成して適用する

Firewall Manager AWS WAF ポリシーには、リソースに適用するルールグループが含まれます。Firewall Manager は、ポリシーを適用する各アカウントに Firewall Managerウェブ ACL を作成します。各アカウントマネージャーは、生成されたウェブ ACL に、お客様がここで定義するルールグループに加えて、ルールとルールグループを追加できます。Firewall Manager AWS WAF ポリシーの詳細については、「」を参照してくださいFirewall Manager での AWS WAF ポリシーの使用。

> **Note**
>
> Firewall Manager が作成するウェブ ACLs は、CloudFront の定額料金プランに参加できません。CloudFront 定額料金プランの一部であるウェブ ACL を管理しようとすると、Firewall Manager は CloudFront ディストリビューションと Firewall Manager ポリシーの両方のコン

プライアンスステータスを報告しません。この状態は、Firewall Manager やその他のアクションでは修復できません。

Firewall Manager AWS WAF ポリシーを作成するには (コンソール)

Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

1. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
2. [Create policy] (ポリシーの作成) を選択します。
3. [Policy type] (ポリシータイプ) では [AWS WAF] を選択します。
4. リージョンで、 を選択します AWS リージョン。Amazon CloudFront ディストリビューションを保護するには、[Global] (グローバル) を選択します。

   複数のリージョンのリソース (CloudFront ディストリビューションを除く) を保護するには、各リージョンに別々の Firewall Manager ポリシーを作成する必要があります。
5. [Next] (次へ) を選択します。
6. [Policy name] (ポリシー名) で、わかりやすい名前を入力します。Firewall Manager は、管理するウェブ ACL の名前にポリシー名を含めます。ウェブ ACL 名の後に、`FMManagedWebACLV2-`、ここに入力するポリシー名、`-`、およびウェブ ACL 作成タイムスタンプ (UTC ミリ秒) が続きます。例えば、`FMManagedWebACLV2-MyWAFPolicyName-1621880374078`。

   > **Important**
   >
   > ウェブ ACL 名は作成後に変更できません。ポリシー名を更新しても、Firewall Manager は関連するウェブ ACL 名を更新しません。Firewall Manager で別の名前のウェブ ACL を作成できるようにするには、新しいポリシーを作成する必要があります。
7. [Policy rules (ポリシールール)] の [First rule groups (最初のルールグループ)] で、[Add rule groups (ルールグループの追加)] を選択します。[AWS managed rule groups] (マネージドルールグループ) を展開します。[Core rule set] (コアルールセット) で、[Add to web ACL] (ウェブ ACL に追加) に切り替えます。[AWS の既知の不正な入力] で、[ウェブ ACL に追加] に切り替えます。[Add rules] (ルールの追加) を選択します。

[Last rule groups] (最後のルールグループ) で、[Add rule groups] (ルールグループの追加) を選択します。[AWS マネージドルールグループ] を展開し、[Amazon IP 評価リスト] で [ウェブ ACL に追加] に切り替えます。[Add rules] (ルールの追加) を選択します。

最初のルールグループで、 Core ルールセットを選択し、Move down を選択します。 は、 Core ルールセットに対して評価する前に、AWS 既知の不正な入力ルールグループに対してウェブリクエスト AWS WAF を評価します。

AWS WAF コンソールを使用して、必要に応じて独自の AWS WAF ルールグループを作成することもできます。作成したルールグループは、[Describe policy : Add rule groups page] (ポリシーを記述: ルールグループの追加ページ) の [Your rule groups] (ルールグループ) の下に表示されます。

Firewall Manager で管理する最初と最後の AWS WAF ルールグループの名前はPOSTFMManaged-、それぞれ PREFMManaged-または で始まり、その後に Firewall Manager ポリシー名とルールグループ作成タイムスタンプが UTC ミリ秒単位で続きます。例えば、PREFMManaged-MyWAFPolicyName-1621880555123。

8. ウェブ ACL のデフォルトアクションは [Allow] (許可) のままにします。
9. [Policy action] (ポリシーアクション) はデフォルトのままにして、準拠していないリソースが自動的に修復されないようにします。このオプションは後で変更できます。
10. [Next] (次へ) を選択します。
11. [Policy scope] (ポリシーの範囲) で、ポリシーを適用するリソースを識別するアカウント、リソースタイプ、タグを設定します。このチュートリアルでは、[AWS アカウント] と [Resources] (リソース) の設定はそのままにし、1 つ以上のリソースタイプを選択します。
12. [リソース] では、指定したタグでリソースを含めるか除外するかによって、タグ付けを使用してポリシーの範囲を絞り込むことができます。包含または除外は使用できますが、両方を使用することはできません。ポリシーの範囲を定義するタグの詳細については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

    リソースタグには NULL 以外の値のみを含めることができます。タグの値を省略すると、Firewall Manager は空の文字列値 "" でタグを保存します。リソースタグは、同じキーと値を持つタグのみと一致します。
13. [次へ] を選択します。
14. [ポリシータグ] で、Firewall Manager ポリシーリソースに必要な識別タグを追加します。タグの詳細については、「タグエディタの使用」を参照してください。
15. [次へ] を選択します。

16. 新しいポリシー設定を確認し、調整が必要なページに戻ります。

    [Policy actions] (ポリシーアクション) が [Identify resources that don't comply with the policy rules, but don't auto remediate] (ポリシールールに準拠していないリソースを特定するが、自動修復しない) に設定されていることを確認します。これにより、ポリシーを有効にする前に、ポリシーが行う変更を確認できます。

17. ポリシーが完成したら、[ポリシーの作成] を選択します。

    [AWS Firewall Manager ポリシー] ペインにポリシーが一覧表示されます。アカウントのヘッダーの下に [保留中] と表示され、[自動修復] のステータスが示されます。ポリシーの作成には数分かかることがあります。[Pending] (保留中) ステータスがアカウント数に置き換えられたら、ポリシー名を選択して、アカウントとリソースの準拠ステータスを調べることができます。詳細については、「AWS Firewall Manager ポリシーのコンプライアンス情報の表示」を参照してください。

ステップ 3: クリーンアップする

余分な料金が発生しないようにするには、不要なポリシーとリソースを削除します。

ポリシーを削除するには (コンソール)

1. [AWS Firewall Manager ポリシー] ページで、ポリシー名の横にあるラジオボタンを選択し、[削除] を選択します。
2. [Delete] (削除) 確認ボックスで [Delete all policy resources] (すべてのポリシーリソースの削除) を選択してから、もう一度 [Delete] (削除) を選択します。

   AWS WAF は、アカウントで作成したポリシーおよびウェブ ACLs などの関連リソースを削除します。変更がすべてのアカウントに反映されるまでに数分かかる場合があります。

AWS Firewall Manager AWS Shield Advanced ポリシーの設定

を使用して AWS Firewall Manager 、組織全体 AWS Shield Advanced の保護を有効にできます。

> **Important**
>
> Firewall Manager は、Amazon Route 53 または AWS Global Acceleratorをサポートしていません。Shield Advanced を使用してこれらのリソースを保護する必要がある場

合、Firewall Manager ポリシーは使用できません。代わりに、「AWS リソースへの AWS Shield Advanced 保護の追加」の手順に従ってください。

Firewall Manager を使用して Shield Advanced 保護を有効にするには、次のステップを実行します。

トピック

- ステップ 1: 前提条件を満たす
- ステップ 2: Shield Advanced ポリシーを作成して適用する
- ステップ 3: (利用可能) Shield Response Team (SRT) に権限を付与する
- ステップ 4: Amazon SNS 通知と Amazon CloudWatch アラームを設定する

ステップ 1: 前提条件を満たす

AWS Firewall Managerのアカウントを準備するには、いくつかの必須のステップがあります。それらのステップは、AWS Firewall Manager 前提条件 で説明されています。「ステップ 2: Shield Advanced ポリシーを作成して適用する」に進む前に、すべての前提条件を満たしてください。

ステップ 2: Shield Advanced ポリシーを作成して適用する

前提条件を完了したら、Shield Advanced AWS Firewall Manager ポリシーを作成します。Firewall Manager Shield Advanced ポリシーには、Shield Advanced で保護するアカウントおよびリソースが含まれています。

> **Important**
>
> Firewall Manager は、Amazon Route 53 または AWS Global Acceleratorをサポートしていません。Shield Advanced を使用してこれらのリソースを保護する必要がある場合、Firewall Manager ポリシーは使用できません。代わりに、「AWS リソースへの AWS Shield Advanced 保護の追加」の手順に従ってください。

Firewall Manager Shield Advanced ポリシーを作成するには (コンソール)

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

> **Note**
>
> Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
3. [Create policy] (ポリシーの作成) を選択します。
4. [Policy type] (ポリシータイプ) で、[Shield Advanced] を選択します。

   Shield Advanced ポリシーを作成するには、Firewall Manager 管理者アカウントが Shield Advanced にサブスクライブしている必要があります。登録されていない場合は、登録するよう求められます。サブスクリプションの費用については、「AWS Shield Advanced の料金」を参照してください。

   > **Note**
   >
   > Shield Advanced に各メンバーアカウントを手動でサブスクライブさせる必要はありません。Firewall Manager は、ポリシーの作成時にこれを行います。各アカウント内のリソースを引き続き保護するには、アカウントが Firewall Manager と Shield Advanced に登録されている必要があります。

5. リージョンで、 を選択します AWS リージョン。Amazon CloudFront のリソースを保護するには、[Global] (グローバル) を選択します。

   複数のリージョンのリソース (CloudFront リソースを除く) を保護するには、各リージョンに別々の Firewall Manager ポリシーを作成する必要があります。
6. [Next] (次へ) を選択します。
7. [Name] (名前) で、わかりやすい名前を入力します。
8. (グローバルリージョンのみ) [Global] (グローバル) リージョンポリシーの場合、Shield Advanced アプリケーションレイヤー DDoS 自動緩和を管理するかどうかを選択できます。このチュートリアルでは、この選択をデフォルト設定の [Ignore] (無視) のままにします。
9. [Policy action] (ポリシーアクション) で、自動的に修復されないオプションを選択します。
10. [次へ] を選択します。

11. AWS アカウント このポリシーは に適用され、包含または除外するアカウントを指定してポリシーの範囲を絞り込むことができます。このチュートリアルでは、[Include all accounts under my organization] (組織のすべてのアカウントを含める) を選択します。
12. 保護するリソースのタイプを選択します。

    Firewall Manager は、Amazon Route 53 または AWS Global Acceleratorをサポートしていません。Shield Advanced を使用してこれらのリソースを保護する必要がある場合、Firewall Manager ポリシーは使用できません。代わりに、「AWS リソースへの AWS Shield Advanced 保護の追加」の Shield Advanced のガイダンスに従ってください。
13. [リソース] では、指定したタグでリソースを含めるか除外するかによって、タグ付けを使用してポリシーの範囲を絞り込むことができます。包含または除外は使用できますが、両方を使用することはできません。ポリシーの範囲を定義するタグの詳細については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

    リソースタグには NULL 以外の値のみを含めることができます。タグの値を省略すると、Firewall Manager は空の文字列値 "" でタグを保存します。リソースタグは、同じキーと値を持つタグのみと一致します。
14. [次へ] を選択します。
15. [ポリシータグ] で、Firewall Manager ポリシーリソースに必要な識別タグを追加します。タグの詳細については、「タグエディタの使用」を参照してください。
16. [次へ] を選択します。
17. 新しいポリシー設定を確認し、調整が必要なページに戻ります。

    [Policy actions] (ポリシーアクション) が [Identify resources that don't comply with the policy rules, but don't auto remediate] (ポリシールールに準拠していないリソースを特定するが、自動修復しない) に設定されていることを確認します。これにより、ポリシーを有効にする前に、ポリシーが行う変更を確認できます。
18. ポリシーが完成したら、[ポリシーの作成] を選択します。

    [AWS Firewall Manager ポリシー] ペインにポリシーが一覧表示されます。アカウントのヘッダーの下に [保留中] と表示され、[自動修復] のステータスが示されます。ポリシーの作成には数分かかることがあります。[Pending] (保留中) ステータスがアカウント数に置き換えられたら、ポリシー名を選択して、アカウントとリソースの準拠ステータスを調べることができます。詳細については、「AWS Firewall Manager ポリシーのコンプライアンス情報の表示」を参照してください。

「ステップ 3: (利用可能) Shield Response Team (SRT) に権限を付与する」に進みます。

ステップ 3: (利用可能) Shield Response Team (SRT) に権限を付与する

の利点の 1 つは、Shield Response Team (SRT) からのサポート AWS Shield Advanced です。DDoS 攻撃の兆候を見つけた場合は、AWS サポート センターにお問い合わせください。必要に応じて、サポートセンターがお客様の問題を SRT にエスカレートします。SRT は疑わしいアクティビティを分析し、お客様に問題の緩和策を提供します。この緩和策では、多くの場合、アカウントで AWS WAF ルールとウェブ ACLs を作成または更新します。SRT は AWS WAF 設定を検査し、 AWS WAF ルールとウェブ ACLs を作成または更新できますが、そのためにはチームの承認が必要です。セットアップの一環として AWS Shield Advanced、必要な認可を SRT に事前に提供することをお勧めします。事前に権限を付与することで、実際に攻撃が発生した場合の遅延を防ぐことができます。

SRT への連絡と承認はアカウントレベルで行います。つまり、攻撃を緩和する権限を SRT に付与するには、Firewall Manager 管理者ではなくアカウント所有者が次のステップを実行する必要があります。Firewall Manager 管理者は、所有しているアカウントに関してのみ SRT に権限を付与することができます。同様に、SRT に連絡してサポートを依頼できるのは、アカウントの所有者のみです。

> **Note**
>
> SRT のサービスを使用するには、ビジネスサポートプランまたはエンタープライズサポートプランをサブスクライブする必要があります。

ユーザーに代わって攻撃を緩和する権限を SRT に付与するには、「Shield Response Team (SRT) サポートによるマネージド DDoS イベントレスポンス」の手順に従ってください。SRT の許可と許可は、同じステップを使用していつでも変更できます。

「ステップ 4: Amazon SNS 通知と Amazon CloudWatch アラームを設定する」に進みます。

ステップ 4: Amazon SNS 通知と Amazon CloudWatch アラームを設定する

Amazon SNS 通知や CloudWatch アラームを設定することなく、このステップから続けることもできます。しかし、これらのアラームと通知を設定することで、潜在的な DDoS イベントの可視性が大幅に上昇します。

Amazon SNS を使用すると、潜在的な DDoS アクティビティから保護されたリソースをモニタリングできます。潜在的な攻撃の通知を受け取るには、リージョンごとに Amazon SNS トピックを作成します。

> **Important**
>
> 潜在的な DDoS アクティビティに関する Amazon SNS 通知はリアルタイムで送信されず、遅延する可能性があります。さらに、各アカウントのリソースタイプごとに Shield Advanced の保護されたリソースのクォータである 1,000 を超えると、Firewall Manager のパフォーマンスの制約により、DDoS 攻撃通知の正常な配信が完全に妨げられる可能性があります。詳細については、「AWS Shield Advanced クォータ」を参照してください。
> 潜在的な DDoS アクティビティのリアルタイム通知を有効にするには、CloudWatch アラームを使用できます。アラームは、保護されたリソースが存在するアカウントの `DDoSDetected` メトリクスに基づいている必要があります。

Firewall Manager で Amazon SNS トピックを作成するには (コンソール)

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで [AWS FMS] の [Settings] (設定) を選択します。
3. [Create new topic] (新しいトピックを作成) を選択します。
4. トピック名を入力します。
5. Amazon SNS メッセージの送信先となる E メールアドレスを入力し、[Add email address] (E メールアドレスの追加) を選択します。
6. [Update SNS configuration] (SNS 設定の更新) を選択します。

Amazon CloudWatch アラームの設定

Shield Advanced は、モニタリングできる CloudWatch の検出、緩和、上位寄稿者のメトリクスを記録します。詳細については、「AWS Shield Advanced メトリクス」を参照してください。CloudWatch では、追加料金が発生します。CloudWatch の料金については、「Amazon CloudWatch の料金」を参照してください。

CloudWatch アラームを作成するには、「Amazon CloudWatch アラームの使用」の指示に従ってください。デフォルトでは、Shield Advanced は CloudWatch を設定して潜在的な DDoS イベントを示す 1 つのインジケーターの検出後に警告します。必要であれば、複数のインジケーターが検出された後にのみ警告が表示されるように、CloudWatch コンソールを使用して設定を変更することもできます。

> **Note**
>
> アラームに加えて、DDoS アクティビティをモニタリングする CloudWatch ダッシュボードを使用することもできます。ダッシュボードは Shield Advanced から raw データを収集し、ほぼリアルタイムの読み取り可能なメトリクスに加工します。Amazon CloudWatch の統計を使用して、ウェブアプリケーションやサービスの動作状況を把握できます。詳細については、「Amazon CloudWatch ユーザーガイド」の「CloudWatch とは」を参照してください。CloudWatch ダッシュボードを作成する手順については、「Amazon CloudWatch によるモニタリング」を参照してください。ダッシュボードに追加できる特定の Shield Advanced メトリクスの詳細については、「AWS Shield Advanced メトリクス」を参照してください。

Shield Advanced の設定が完了したら、Shield Advanced による DDoS イベントの可視性 でイベントを表示するためのオプションをよく理解してください。

AWS Firewall Manager Amazon VPC セキュリティグループポリシーの設定

AWS Firewall Manager を使用して組織全体で Amazon VPC セキュリティグループを有効にするには、次の手順を順番に実行します。

トピック

- ステップ 1: 前提条件を満たす
- ステップ 2: ポリシーで使用するセキュリティグループを作成する
- ステップ 3: 一般セキュリティグループポリシーを作成して適用する

ステップ 1: 前提条件を満たす

AWS Firewall Managerのアカウントを準備するには、いくつかの必須のステップがあります。それらのステップは、AWS Firewall Manager 前提条件 で説明されています。「ステップ 2: ポリシーで使用するセキュリティグループを作成する」に進む前に、すべての前提条件を満たしてください。

ステップ 2: ポリシーで使用するセキュリティグループを作成する

このステップでは、Firewall Manager を使用して組織全体に適用できるセキュリティグループを作成します。

> **Note**
>
> このチュートリアルでは、セキュリティグループポリシーを組織内のリソースに適用しません。ポリシーを作成し、ポリシーのセキュリティグループをリソースに適用した場合どうなるかを確認するだけです。これを行うには、ポリシーの自動修復を無効にします。

一般的なセキュリティグループが既に定義されている場合は、このステップを省略して「ステップ 3: 一般セキュリティグループポリシーを作成して適用する」に進みます。

Firewall Manager 共通のセキュリティグループポリシーで使用するセキュリティグループを作成するには

- 「Amazon VPC ユーザーガイド」の「Security Groups for Your VPC」(VPC のセキュリティグループ) のガイダンスに従って、組織内のすべてのアカウントとリソースに適用できるセキュリティグループを作成します。

  セキュリティグループルールオプションの詳細については、「セキュリティグループのルールのリファレンス」を参照してください。

これで「ステップ 3: 一般セキュリティグループポリシーを作成して適用する」に進む準備ができました。

ステップ 3: 一般セキュリティグループポリシーを作成して適用する

前提条件を完了したら、 AWS Firewall Manager 共通のセキュリティグループポリシーを作成します。共通セキュリティグループポリシーは、 AWS 組織全体に一元管理されたセキュリティグループを提供します。また、セキュリティグループが適用される AWS アカウント および リソースも定義します。Firewall Manager では、共通セキュリティグループポリシーに加えて、組織内で使用中のセキュリティグループルールを管理するためのコンテンツ監査セキュリティグループポリシーと、未使用および冗長セキュリティグループを管理するための使用状況監査セキュリティグループポリシーがサポートされています。詳細については、「Firewall Manager のセキュリティグループポリシーを使用して Amazon VPC セキュリティグループを管理する」を参照してください。

このチュートリアルでは、共通セキュリティグループポリシーを作成し、そのアクションを自動的に修復しないように設定します。これにより、 AWS 組織を変更せずにポリシーがどのような影響を与えるかを確認できます。

Firewall Manager の一般的なセキュリティグループポリシーを作成するには (コンソール)

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
3. 前提条件を満たしていない場合、問題を修正する方法についての指示がコンソールに表示されます。指示に従ってから、このステップに戻り、共通セキュリティグループポリシーを作成します。
4. [Create policy] (ポリシーの作成) を選択します。
5. [Policy type] (ポリシータイプ) で、[Security group] (セキュリティグループ) を選択します。
6. [Security group policy type] (セキュリティグループポリシータイプ) で、[Common security groups] (共通セキュリティグループ) を選択します。
7. リージョンで、 を選択します AWS リージョン。
8. [次へ] を選択します。
9. [Policy name] (ポリシー名) で、わかりやすい名前を入力します。
10. [Policy rules] (ポリシールール) を使用すると、このポリシーのセキュリティグループの適用方法と保守方法を選択できます。このチュートリアルでは、オプションのチェックをオフのままにします。
11. [Add primary security group] (プライマリセキュリティグループの追加) を選択し、このチュートリアル用に作成したセキュリティグループを選択して、[Add security group] (セキュリティグループの追加) を選択します。
12. [Policy action] (ポリシーアクション) で、[Identify resources that don't comply with the policy rules, but don't auto remediate] (ポリシールールに準拠していないリソースを特定するが、自動修復しない) を選択します。

13. [次へ] を選択します。
14. AWS アカウント このポリシーの影響を受ける では、包含または除外するアカウントを指定することで、ポリシーの範囲を絞り込むことができます。このチュートリアルでは、[Include all accounts under my organization] (組織のすべてのアカウントを含める) を選択します。
15. リソースタイプで、 AWS 組織に定義したリソースに応じて、1 つ以上のタイプを選択します。
16. [リソース] では、指定したタグでリソースを含めるか除外するかによって、タグ付けを使用してポリシーの範囲を絞り込むことができます。包含または除外は使用できますが、両方を使用することはできません。ポリシーの範囲を定義するタグの詳細については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

    リソースタグには NULL 以外の値のみを含めることができます。タグの値を省略すると、Firewall Manager は空の文字列値 "" でタグを保存します。リソースタグは、同じキーと値を持つタグのみと一致します。
17. [次へ] を選択します。
18. [ポリシータグ] で、Firewall Manager ポリシーリソースに必要な識別タグを追加します。タグの詳細については、「タグエディタの使用」を参照してください。
19. [次へ] を選択します。
20. 新しいポリシー設定を確認し、調整が必要なページに戻ります。

    [Policy actions] (ポリシーアクション) が [Identify resources that don't comply with the policy rules, but don't auto remediate] (ポリシールールに準拠していないリソースを特定するが、自動修復しない) に設定されていることを確認します。これにより、ポリシーを有効にする前に、ポリシーが行う変更を確認できます。
21. ポリシーが完成したら、[ポリシーの作成] を選択します。

    [AWS Firewall Manager ポリシー] ペインにポリシーが一覧表示されます。アカウントのヘッダーの下に [保留中] と表示され、[自動修復] のステータスが示されます。ポリシーの作成には数分かかることがあります。[Pending] (保留中) ステータスがアカウント数に置き換えられたら、ポリシー名を選択して、アカウントとリソースの準拠ステータスを調べることができます。詳細については、「AWS Firewall Manager ポリシーのコンプライアンス情報の表示」を参照してください。
22. 調べ終わったら、このチュートリアルで作成したポリシーを保持しない場合は、ポリシー名を選択して [Delete] (削除) を選択し、[Clean up resources created by this policy.] (このポリシーによって作成されたリソースをクリーンアップします。) を選択して、最後に [Delete] (削除) を選択します。

Firewall Manager セキュリティグループポリシーの詳細については、「Firewall Manager のセキュリティグループポリシーを使用して Amazon VPC セキュリティグループを管理する」を参照してください。

AWS Firewall Manager Amazon VPC ネットワーク ACL ポリシーの設定

AWS Firewall Manager を使用して組織全体ACLs を有効にするには、このセクションのステップを順番に実行します。

ネットワーク ACL の詳細については、「Amazon VPC ユーザーガイド」の「ACL を使用して、サブネットのトラフィックを制御する」を参照してください。

トピック

- ステップ 1: 前提条件を満たす
- ステップ 2: ネットワーク ACL ポリシーを作成する

ステップ 1: 前提条件を満たす

AWS Firewall Managerのアカウントを準備するには、いくつかの必須のステップがあります。それらのステップは、AWS Firewall Manager 前提条件 で説明されています。「ステップ 2: ネットワーク ACL ポリシーを作成する」に進む前に、すべての前提条件を満たしてください。

ステップ 2: ネットワーク ACL ポリシーを作成する

前提条件を満たす後、Firewall Manager のネットワーク ACL ポリシーを作成します。ネットワーク ACL ポリシーは、 AWS 組織全体に一元管理されたネットワーク ACL 定義を提供します。また、ネットワーク ACL が適用される AWS アカウント および サブネットも定義します。

Firewall Manager のネットワーク ACL ポリシーの詳細について、ネットワーク ACL ポリシー を参照してください。

Firewall Manager の ネットワーク ACL ポリシーの一般情報については、ネットワーク ACL ポリシー を参照してください。

> **Note**
>
> このチュートリアルでは、ネットワーク ACL ポリシーを組織内のサブネットに適用しません。ポリシーを作成し、そのネットワークACLをサブネットに適用した場合に何が起こるかを確認するだけです。これを行うには、ポリシーの自動修復を無効にします。

Firewall Manager ネットワーク ACL ポリシーを作成するには (コンソールで)

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
3. 前提条件を満たしていない場合、問題を修正する方法についての指示がコンソールに表示されます。指示を従って、このステップに戻り、ネットワーク ACL ポリシーを作成します。
4. [Create policy] (ポリシーの作成) を選択します。
5. リージョンで、 を選択します AWS リージョン。
6. [ポリシータイプ] で、[ネットワーク ACL] を選択します。
7. [次へ] を選択します。
8. [Policy name] (ポリシー名) で、わかりやすい名前を入力します。
9. [ネットワーク ACL ポリシールール] では、インバウンドトラフィックとアウトバウンドトラフィックの両方の最初と最後のルールを定義します。

   Firewall Manager でネットワーク ACL ルールを定義する方法は、Amazon VPC を通じて定義する方法と同様です。唯一の違いは、ルール番号を自分で割り当てるのではなく、ルールの各セットを実行する順序を割り当て、ポリシーを保存するときに Firewall Manager が番号を割り当てることです。最大 5 つのインバウンドルールを定義し、最初と最後に任意の方法で分割できます。また、最大 5 つのアウトバウンドルールを定義できます。

   ネットワーク ACL ルールを指定するガイダンスについては、「Amazon VPC ユーザーガイド」の「ネットワーク ACL ルールの追加と削除」を参照してください。

   Firewall Manager ポリシーで定義するルールは、ネットワーク ACL がネットワーク ACL ポリシーに準拠する必要がある最小ルール設定を指定します。例えば、ネットワーク ACL のインバウンドルールは、ポリシーで指定されているのと同じ順序で、ポリシーの最初インバウンドルールとして始まる場合を除き、ポリシーに準拠することはできません。詳細については、「ネットワーク ACL ポリシー」を参照してください。

10. [Policy action] (ポリシーアクション) で、[Identify resources that don't comply with the policy rules, but don't auto remediate] (ポリシールールに準拠していないリソースを特定するが、自動修復しない) を選択します。
11. [次へ] を選択します。
12. AWS アカウント このポリシーの影響を受けると、包含または除外するアカウントを指定して、ポリシーの範囲を絞り込むことができます。このチュートリアルでは、[Include all accounts under my organization] (組織のすべてのアカウントを含める) を選択します。

    ネットワーク ACL ポリシーの [リソースタイプ] は常にサブネットです。
13. [リソース] では、指定したタグでリソースを含めるか除外するかによって、タグ付けを使用してポリシーの範囲を絞り込むことができます。包含または除外は使用できますが、両方を使用することはできません。ポリシーの範囲を定義するタグの詳細については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

    リソースタグには NULL 以外の値のみを含めることができます。タグの値を省略すると、Firewall Manager は空の文字列値 "" でタグを保存します。リソースタグは、同じキーと値を持つタグのみと一致します。
14. [次へ] を選択します。
15. [ポリシータグ] で、Firewall Manager ポリシーリソースに必要な識別タグを追加します。タグの詳細については、「タグエディタの使用」を参照してください。
16. [次へ] を選択します。
17. 新しいポリシー設定を確認し、調整が必要なページに戻ります。

    [Policy actions] (ポリシーアクション) が [Identify resources that don't comply with the policy rules, but don't auto remediate] (ポリシールールに準拠していないリソースを特定するが、自動修復しない) に設定されていることを確認します。これにより、ポリシーを有効にする前に、ポリシーが行う変更を確認できます。
18. ポリシーが完成したら、[ポリシーの作成] を選択します。

    [AWS Firewall Manager ポリシー] ペインにポリシーが一覧表示されます。アカウントのヘッダーの下に [保留中] と表示され、[自動修復] のステータスが示されます。ポリシーの作成には数分かかることがあります。[Pending] (保留中) ステータスがアカウント数に置き換えられたら、ポリシー名を選択して、アカウントとリソースの準拠ステータスを調べることができます。詳細については、「AWS Firewall Manager ポリシーのコンプライアンス情報の表示」を参照してください。

19. 調べ終わったら、このチュートリアルで作成したポリシーを保持しない場合は、ポリシー名を選択して [Delete] (削除) を選択し、[Clean up resources created by this policy.] (このポリシーによって作成されたリソースをクリーンアップします。) を選択して、最後に [Delete] (削除) を選択します。

Firewall Manager ネットワーク ACL ポリシーの詳細については、ネットワーク ACL ポリシー を参照してください。

AWS Firewall Manager AWS Network Firewall ポリシーの設定

AWS Firewall Manager を使用して組織全体で AWS Network Firewall ファイアウォールを有効にするには、次の手順を順番に実行します。Firewall Manager の Network Firewall ポリシーについては、「Firewall Manager での AWS Network Firewall ポリシーの使用」を参照してください。

トピック

- ステップ 1: 前提条件を満たす
- ステップ 2: ポリシーで使用するネットワーク Firewall ルールグループを作成する
- ステップ 3: Network Firewall ポリシーを作成して適用する

ステップ 1: 前提条件を満たす

AWS Firewall Managerのアカウントを準備するには、いくつかの必須のステップがあります。それらのステップは、AWS Firewall Manager 前提条件 で説明されています。次のステップに進む前に、すべての前提条件を満たしてください。

ステップ 2: ポリシーで使用するネットワーク Firewall ルールグループを作成する

このチュートリアルに従うには、ルールグループ AWS Network Firewall とファイアウォールポリシーの設定方法を理解しておく必要があります。

AWS Firewall Manager ポリシーで使用される Network Firewall には、少なくとも 1 つのルールグループが必要です。Network Firewall でルールグループをまだ作成していない場合は、ここで作成します。Network Firewall の使用については、「AWS Network Firewall デベロッパーガイド」を参照してください。

ステップ 3: Network Firewall ポリシーを作成して適用する

前提条件を満たしてから、 AWS Firewall Manager Network Firewall ポリシーを作成します。Network Firewall ポリシーは、組織全体に一元管理された AWS Network Firewall ファイアウォールを提供します AWS 。また、ファイアウォールが適用される AWS アカウント および リソースも定義します。

Firewall Manager が Network Firewall ポリシーを管理する方法の詳細については、「Firewall Manager での AWS Network Firewall ポリシーの使用」を参照してください。

Firewall Manager の Network Firewall ポリシーを作成するには (コンソール)

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
3. 前提条件を満たしていない場合、問題を修正する方法についての指示がコンソールに表示されます。指示を実行してから、このステップに戻り、Network Firewall ポリシーを作成します。
4. [Create security policy] (セキュリティポリシーを作成) を選択します。
5. [Policy type] (ポリシータイプ) では [AWS Network Firewall] を選択します。
6. リージョンで、 を選択します AWS リージョン。
7. [次へ] を選択します。
8. [Policy name] (ポリシー名) で、わかりやすい名前を入力します。
9. ポリシー設定では、ファイアウォールポリシーを定義できます。これは、 AWS Network Firewall コンソールで使用するプロセスと同じプロセスです。ポリシーで使用するルールグループを追加し、デフォルトのステートレスアクションを指定します。このチュートリアルでは、Network Firewall におけるファイアウォールポリシーと同様に、このポリシーを設定します。

> **Note**
>
> 自動修復は AWS Firewall Manager Network Firewall ポリシーに対して自動的に行われるため、ここで自動修復を選択しないオプションは表示されません。

10. [次へ] を選択します。
11. [Firewall endpoints] (ファイアウォールエンドポイント) で、[Multiple firewall endpoints] (複数のファイアウォールエンドポイント) を選択します。このオプションは、ファイアウォールについて高い可用性を実現します。ポリシーを作成すると、Firewall Manager は、保護するパブリックサブネットがある各アベイラビリティーゾーンにファイアウォールサブネットを作成します。
12. [AWS Network Firewall ルート設定] で [モニタリング] をクリックします。これにより、Firewall Manager が VPC のルート設定違反をモニタリングし、ルートのコンプライアンス準拠に役立つ改善策のアラートを発信します。オプションで、ルート設定を Firewall Manager でモニタリングしてこれらのアラートを受信したくない場合は、[Off] (オフ) を選択します。

> **Note**
>
> モニタリングにより、ルート設定の誤りが原因で非準拠となっているリソースに関する詳細が提供され、Firewall Manager `GetViolationDetails` API からの修復アクションが提案されます。例えば、Network Firewall は、ポリシーによって作成されたファイアウォールエンドポイントを通じてトラフィックがルーティングされない場合に警告します。

> **Warning**
>
> [Monitor] (モニタリング) を選択した場合、同じポリシーについて将来 [Off] (オフ) に変更することはできません。新しいポリシーを作成する必要があります。

13. [Traffic type] (トラフィックの種類) で、[Add to firewall policy] (ファイアウォールポリシーに追加) を選択して、インターネットゲートウェイを介してトラフィックをルーティングします。
14. AWS アカウント このポリシーの影響を受ける では、包含または除外するアカウントを指定することで、ポリシーの範囲を絞り込むことができます。このチュートリアルでは、[Include all accounts under my organization] (組織のすべてのアカウントを含める) を選択します。

    Network Firewall ポリシーの [Resource type] (リソースタイプ) は常に [VPC] です。

15. [リソース] では、指定したタグでリソースを含めるか除外するかによって、タグ付けを使用してポリシーの範囲を絞り込むことができます。包含または除外は使用できますが、両方を使用することはできません。ポリシーの範囲を定義するタグの詳細については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

    リソースタグには NULL 以外の値のみを含めることができます。タグの値を省略すると、Firewall Manager は空の文字列値 "" でタグを保存します。リソースタグは、同じキーと値を持つタグのみと一致します。

16. [次へ] を選択します。
17. [ポリシータグ] で、Firewall Manager ポリシーリソースに必要な識別タグを追加します。タグの詳細については、「タグエディタの使用」を参照してください。
18. [次へ] を選択します。
19. 新しいポリシー設定を確認し、調整が必要なページに戻ります。

    [Policy actions] (ポリシーアクション) が [Identify resources that don't comply with the policy rules, but don't auto remediate] (ポリシールールに準拠していないリソースを特定するが、自動修復しない) に設定されていることを確認します。これにより、ポリシーを有効にする前に、ポリシーが行う変更を確認できます。

20. ポリシーが完成したら、[ポリシーの作成] を選択します。

    [AWS Firewall Manager ポリシー] ペインにポリシーが一覧表示されます。アカウントのヘッダーの下に [保留中] と表示され、[自動修復] のステータスが示されます。ポリシーの作成には数分かかることがあります。[Pending] (保留中) ステータスがアカウント数に置き換えられたら、ポリシー名を選択して、アカウントとリソースの準拠ステータスを調べることができます。詳細については、「AWS Firewall Manager ポリシーのコンプライアンス情報の表示」を参照してください。

21. 調べ終わったら、このチュートリアルで作成したポリシーを保持しない場合は、ポリシー名を選択して [Delete] (削除) を選択し、[Clean up resources created by this policy.] (このポリシーによって作成されたリソースをクリーンアップします。) を選択して、最後に [Delete] (削除) を選択します。

Firewall Manager の Network Firewall ポリシーの詳細については、「Firewall Manager での AWS Network Firewall ポリシーの使用」を参照してください。

AWS Firewall Manager DNS Firewall ポリシーの設定

AWS Firewall Manager を使用して組織全体で Amazon Route 53 Resolver DNS Firewall を有効にするには、次の手順を順番に実行します。Firewall Manager の DNS Firewall ポリシーについては、「Firewall Manager の Amazon Route 53 Resolver DNS Firewall ポリシーを使用する」を参照してください。

トピック

- ステップ 1: 前提条件を満たす
- ステップ 2: ポリシーで使用する DNS Firewall ルールグループを作成する
- ステップ 3: DNS Firewall ポリシーを作成して適用する

ステップ 1: 前提条件を満たす

AWS Firewall Managerのアカウントを準備するには、いくつかの必須のステップがあります。それらのステップは、AWS Firewall Manager 前提条件 で説明されています。次のステップに進む前に、すべての前提条件を満たしてください。

ステップ 2: ポリシーで使用する DNS Firewall ルールグループを作成する

このチュートリアルの手順を実行するには、Amazon Route 53 Resolver DNS Firewall に精通しており、そのルールグループを設定する方法を理解している必要があります。

AWS Firewall Manager ポリシーで使用される DNS Firewall には少なくとも 1 つのルールグループが必要です。DNS Firewall でルールグループをまだ作成していない場合は、ここで作成します。DNS Firewall の使用方法については、「Amazon Route 53 デベロッパーガイド」の「Amazon Route 53 Resolver DNS Firewall」を参照してください。

ステップ 3: DNS Firewall ポリシーを作成して適用する

前提条件を完了したら、DNS Firewall AWS Firewall Manager ポリシーを作成します。DNS Firewall ポリシーは、 AWS 組織全体に対して一元管理された DNS Firewall ルールグループの関連付けのセットを提供します。また、ファイアウォールが適用される AWS アカウント とリソースも定義します。

Firewall Manager が DNS Firewall ルールグループの関連付けを管理する方法の詳細については、「Firewall Manager の Amazon Route 53 Resolver DNS Firewall ポリシーを使用する」を参照してください。

Firewall Manager の DNS Firewall ポリシーを作成するには (コンソール)

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。
2. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
3. 前提条件を満たしていない場合、問題を修正する方法についての指示がコンソールに表示されます。指示を実行してから、このステップに戻り、DNS Firewall ポリシーを作成します。
4. [Create security policy] (セキュリティポリシーを作成) を選択します。
5. [Policy type] (ポリシータイプ) で、[Amazon Route 53 Resolver DNS Firewall] を選択します。
6. リージョンで、 を選択します AWS リージョン。
7. [次へ] を選択します。
8. [Policy name] (ポリシー名) で、わかりやすい名前を入力します。
9. ポリシー設定を使用すると、Firewall Manager から管理する DNS Firewall ルールグループの関連付けを定義できます。ポリシーで使用するルールグループを追加します。VPC について、最初に評価する関連付けと、最後に評価する関連付けを定義できます。このチュートリアルでは、必要に応じて 1 つまたは 2 つのルールグループの関連付けを追加します。
10. [次へ] を選択します。
11. AWS アカウント このポリシーの影響を受けると、包含または除外するアカウントを指定して、ポリシーの範囲を絞り込むことができます。このチュートリアルでは、[Include all accounts under my organization] (組織のすべてのアカウントを含める) を選択します。

    DNS Firewall ポリシーの [Resource type] (リソースタイプ) は常に [VPC] です。
12. [リソース] では、指定したタグでリソースを含めるか除外するかによって、タグ付けを使用してポリシーの範囲を絞り込むことができます。包含または除外は使用できますが、両方を使用することはできません。ポリシーの範囲を定義するタグの詳細については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

    リソースタグには NULL 以外の値のみを含めることができます。タグの値を省略すると、Firewall Manager は空の文字列値 "" でタグを保存します。リソースタグは、同じキーと値を持つタグのみと一致します。
13. [次へ] を選択します。
14. [ポリシータグ] で、Firewall Manager ポリシーリソースに必要な識別タグを追加します。タグの詳細については、「タグエディタの使用」を参照してください。

15. [次へ] を選択します。
16. 新しいポリシー設定を確認し、調整が必要なページに戻ります。

    [Policy actions] (ポリシーアクション) が [Identify resources that don't comply with the policy rules, but don't auto remediate] (ポリシールールに準拠していないリソースを特定するが、自動修復しない) に設定されていることを確認します。これにより、ポリシーを有効にする前に、ポリシーが行う変更を確認できます。
17. ポリシーが完成したら、[ポリシーの作成] を選択します。

    [AWS Firewall Manager ポリシー] ペインにポリシーが一覧表示されます。アカウントのヘッダーの下に [保留中] と表示され、[自動修復] のステータスが示されます。ポリシーの作成には数分かかることがあります。[Pending] (保留中) ステータスがアカウント数に置き換えられたら、ポリシー名を選択して、アカウントとリソースの準拠ステータスを調べることができます。詳細については、「AWS Firewall Manager ポリシーのコンプライアンス情報の表示」を参照してください。
18. 調べ終わったら、このチュートリアルで作成したポリシーを保持しない場合は、ポリシー名を選択して [Delete] (削除) を選択し、[Clean up resources created by this policy.] (このポリシーによって作成されたリソースをクリーンアップします。) を選択して、最後に [Delete] (削除) を選択します。

Firewall Manager の DNS Firewall ポリシーの詳細については、「Firewall Manager の Amazon Route 53 Resolver DNS Firewall ポリシーを使用する」を参照してください。

AWS Firewall Manager Palo Alto Networks Cloud Next Generation Firewall ポリシーの設定

AWS Firewall Manager を使用して Palo Alto Networks Cloud Next Generation Firewall (NGFW) ポリシーを有効にするには、次の手順を順番に実行します。Palo Alto Networks Cloud NGFW ポリシーについては、「Palo Alto Networks Cloud NGFW ポリシーを Firewall Manager で使用する」を参照してください。

トピック

- ステップ 1: 一般的な前提条件を満たす
- ステップ 2: Palo Alto Networks Cloud NGFW ポリシーの前提条件を満たす
- ステップ 3: Palo Alto Networks Cloud NGFW ポリシーを作成して適用する

ステップ 1: 一般的な前提条件を満たす

AWS Firewall Managerのアカウントを準備するには、いくつかの必須のステップがあります。それらのステップは、AWS Firewall Manager 前提条件 で説明されています。次のステップに進む前に、すべての前提条件を満たしてください。

ステップ 2: Palo Alto Networks Cloud NGFW ポリシーの前提条件を満たす

Palo Alto Networks Cloud NGFW ポリシーを使用するには、いくつかの追加の必須ステップを完了する必要があります。それらのステップは、Palo Alto Networks Cloud Next Generation Firewall ポリシーの要件 で説明されています。次のステップに進む前に、すべての前提条件を満たしてください。

ステップ 3: Palo Alto Networks Cloud NGFW ポリシーを作成して適用する

前提条件を完了したら、 AWS Firewall Manager Palo Alto Networks Cloud NGFW ポリシーを作成します。

Firewall Manager の Palo Alto Networks Cloud NGFW ポリシーの詳細については、「Palo Alto Networks Cloud NGFW ポリシーを Firewall Manager で使用する」を参照してください。

Palo Alto Networks Cloud NGFW の Firewall Manager ポリシーを作成するには (コンソール)

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
3. [Create policy] (ポリシーの作成) を選択します。
4. [Policy type] (ポリシータイプ) で、[Palo Alto Networks Cloud NGFW] を選択します。 AWS Marketplace で Palo Alto Networks Cloud NGFW サービスをまだサブスクライブしていない場合は、まずサブスクライブする必要があります。 AWS Marketplace でサブスクライブするには、View AWS Marketplace の詳細を選択します。

5. [Deployment model] (デプロイモデル) で、[Distributed model] (分散モデル) または [Centralized model] (集約型モデル) のいずれかを選択します。デプロイモデルによって、Firewall Manager がポリシーのエンドポイントを管理する方法が決まります。分散モデルでは、Firewall Manager は、ポリシーの範囲内の各 VPC にファイアウォールエンドポイントを維持します。集約型モデルでは、Firewall Manager は検査 VPC に単一のエンドポイントを維持します。
6. リージョンで、 を選択します AWS リージョン。複数のリージョンのリソースを保護するには、各リージョンに別々の ポリシーを作成する必要があります。
7. [Next] (次へ) を選択します。
8. [Policy name] (ポリシー名) で、わかりやすい名前を入力します。
9. ポリシー設定で、このポリシーに関連付ける Palo Alto Networks Cloud NGFW ファイアウォールポリシーを選択します。Palo Alto Networks Cloud NGFW ファイアウォールポリシーの一覧には、Palo Alto Networks Cloud NGFW テナントに関連付けられているすべての Cloud NGFW ファイアウォールポリシーが含まれています。Palo Alto Networks Cloud NGFW ファイアウォールポリシーの作成と管理については、「Palo Alto Networks Cloud NGFW for デプロイガイド」の「Deploy Palo Alto Networks Cloud NGFW for AWSAWS Firewall Manager」トピックを参照してください。 AWS
10. [Palo Alto Networks Cloud NGFW logging ログ記録 - 選択可能]で、オプションで、ポリシーに関してログ記録する Cloud NGFW ログタイプを選択します。Palo Alto Networks Cloud NGFW ログタイプの詳細については、「Palo Alto Networks Cloud NGFW for deployment guide」の「Configure Logging AWS for Palo Alto Networks Cloud NGFW on」を参照してください。 AWS

    [log destination] (ログの宛先) で、Firewall Manager がログを書き込む場合を指定します。
11. [Next] (次へ) を選択します。
12. [Configure third-party firewall endpoint] (サードパーティーのファイアウォールエンドポイントを設定) で、ファイアウォールエンドポイントの作成に分散デプロイモデルと集約型デプロイモデルのいずれを使用しているかに応じて、次のいずれかを実行します。

    - このポリシーに分散デプロイモデルを使用している場合は、[Availability Zones] (アベイラビリティーゾーン) で、ファイアウォールエンドポイントを作成するアベイラビリティーゾーンを選択します。アベイラビリティーゾーンは、[Availability Zone name] (アベイラビリティーゾーン名) または [Availability Zone ID] (アベイラビリティーゾーン ID) で選択できます。
    - このポリシーに集約型デプロイモデルを使用している場合は、[Inspection VPC configuration] (検査 VPC 設定) の [AWS Firewall Manager endpoint configuration] (エンドポイント設定) で、検査 VPC の所有者の AWS アカウント ID と検査 VPC の VPC ID を入力します。

- [Availability Zones] (アベイラビリティーゾーン) で、ファイアウォールエンドポイントを作成するアベイラビリティーゾーンを選択します。アベイラビリティーゾーンは、[Availability Zone name] (アベイラビリティーゾーン名) または [Availability Zone ID] (アベイラビリティーゾーン ID) で選択できます。

13. [Next] (次へ) を選択します。
14. [Policy scope] (ポリシーの範囲) の [AWS アカウント this policy applies to] (このポリシーが適用される) で、次のようにオプションを選択します。

    - 組織内のすべてのアカウントにポリシーを適用する場合は、デフォルトの選択のままにし、AWS 組織内のすべてのアカウントを含めます。
    - ポリシーを特定の AWS Organizations 組織単位 (OUs) にある特定のアカウントにのみ適用する場合は、指定されたアカウントと組織単位のみを含めるを選択し、含めるアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。
    - 特定のアカウントまたは AWS Organizations 組織単位 (OUs) を除くすべてのアカウントにポリシーを適用する場合は、指定されたアカウントと組織単位を除外し、その他をすべて含めてから、除外するアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。

    選択できるオプションは 1 つのみです。

    ポリシーを適用すると、Firewall Manager は新しいアカウントを設定と照合して自動的に評価します。例えば、特定のアカウントのみを含めると、Firewall Manager は新しいアカウントにポリシーを適用しません。別の例として、OU を含めた場合、OU またはその子である OU にアカウントを追加すると、Firewall Manager は新しいアカウントにポリシーを自動的に適用します。

    Network Firewall ポリシーの [Resource type] (リソースタイプ) は [VPC] です。
15. [リソース] では、指定したタグでリソースを含めるか除外するかによって、タグ付けを使用してポリシーの範囲を絞り込むことができます。包含または除外は使用できますが、両方を使用することはできません。ポリシーの範囲を定義するタグの詳細については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

    リソースタグには NULL 以外の値のみを含めることができます。タグの値を省略すると、Firewall Manager は空の文字列値 "" でタグを保存します。リソースタグは、同じキーと値を持つタグのみと一致します。

16. [Grant cross-account access] (クロスアカウントアクセスを付与) で、[Download CloudFormation template] (テンプレートをダウンロード) を選択します。これにより、CloudFormation スタックの作成に使用できる CloudFormation テンプレートがダウンロードされます。このスタックは、Palo Alto Networks Cloud NGFW リソースを管理するためのクロスアカウントアクセス許可を Firewall Manager に付与する AWS Identity and Access Management ロールを作成します。スタックの詳細については、「CloudFormation ユーザーガイド」の「StackSets の操作」を参照してください。
17. [次へ] を選択します。
18. [ポリシータグ] で、Firewall Manager ポリシーリソースに必要な識別タグを追加します。タグの詳細については、「タグエディタの使用」を参照してください。
19. [次へ] を選択します。
20. 新しいポリシー設定を確認し、調整が必要なページに戻ります。

    [Policy actions] (ポリシーアクション) が [Identify resources that don't comply with the policy rules, but don't auto remediate] (ポリシールールに準拠していないリソースを特定するが、自動修復しない) に設定されていることを確認します。これにより、ポリシーを有効にする前に、ポリシーが行う変更を確認できます。
21. ポリシーが完成したら、[ポリシーの作成] を選択します。

    [AWS Firewall Manager ポリシー] ペインにポリシーが一覧表示されます。アカウントのヘッダーの下に [保留中] と表示され、[自動修復] のステータスが示されます。ポリシーの作成には数分かかることがあります。[Pending] (保留中) ステータスがアカウント数に置き換えられたら、ポリシー名を選択して、アカウントとリソースの準拠ステータスを調べることができます。詳細については、「AWS Firewall Manager ポリシーのコンプライアンス情報の表示」を参照してください。

Firewall Manager Palo Alto Networks Cloud NGFW ポリシーの詳細については、「Palo Alto Networks Cloud NGFW ポリシーを Firewall Manager で使用する」を参照してください。

CNF ポリシー AWS Firewall Managerの強制設定

Fortigate Cloud Native Firewall (CNF) as a Service は、 AWS Firewall Manager ポリシーに使用できるサードパーティーのファイアウォールサービスです。Fortigate CNF for Firewall Manager を使用すると、Fortigate CNF リソースとポリシーセットを作成し、すべての AWS アカウントに一元的にデプロイできます。 AWS Firewall Manager を使用して Fortigate CNF ポリシーを有効にするには、

次の手順を順番に実行します。Fortigate CNF ポリシーの詳細については、「Firewall Manager に Fortigate Cloud Native Firewall (CNF) as a Service ポリシーを使用する」を参照してください。

トピック

- ステップ 1: 一般的な前提条件を満たす
- ステップ 2: Fortigate CNF ポリシーの前提条件を満たす
- ステップ 3: Fortigate CNF ポリシーを作成して適用する

ステップ 1: 一般的な前提条件を満たす

AWS Firewall Managerのアカウントを準備するには、いくつかの必須のステップがあります。それらのステップは、AWS Firewall Manager 前提条件 で説明されています。次のステップに進む前に、すべての前提条件を満たしてください。

ステップ 2: Fortigate CNF ポリシーの前提条件を満たす

Fortigate CNF ポリシーを使用するには、追加の必須ステップを完了する必要があります。それらのステップは、Fortigate Cloud Native Firewall (CNF) as a Service ポリシーの前提条件 で説明されています。次のステップに進む前に、すべての前提条件を満たしてください。

ステップ 3: Fortigate CNF ポリシーを作成して適用する

前提条件を完了したら、Fortigate AWS Firewall Manager CNF ポリシーを作成します。

Fortigate CNF の Firewall Manager ポリシーの詳細については、「Firewall Manager に Fortigate Cloud Native Firewall (CNF) as a Service ポリシーを使用する」を参照してください。

Fortigate CNF の Firewall Manager ポリシーを作成するには (コンソール)

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
3. [Create policy] (ポリシーの作成) を選択します。
4. [Policy type] (ポリシータイプ) には、Fortigate CNF を選択してください。 AWS Marketplace で Fortigate CNF サービスをまだサブスクライブしていない場合は、まずサブスクライブする必要があります。 AWS Marketplace でサブスクライブするには、View AWS Marketplace の詳細を選択します。
5. [Deployment model] (デプロイモデル) で、[Distributed model] (分散モデル) または [Centralized model] (集約型モデル) のいずれかを選択します。デプロイモデルによって、Firewall Manager がポリシーのエンドポイントを管理する方法が決まります。分散モデルでは、Firewall Manager は、ポリシーの範囲内の各 VPC にファイアウォールエンドポイントを維持します。集約型モデルでは、Firewall Manager は検査 VPC に単一のエンドポイントを維持します。
6. リージョンで、 を選択します AWS リージョン。複数のリージョンのリソースを保護するには、各リージョンに別々の ポリシーを作成する必要があります。
7. [次へ] を選択します。
8.
9. ポリシー設定で、このポリシーに関連付ける Fortigate CNF ファイアウォールポリシーを選択します。Fortigate CNF ファイアウォールポリシーのリストには、Fortigate CNF テナントに関連付けられているすべての CNF ファイアウォールポリシーが含まれています。Fortigate CNF ファイアウォールポリシーの作成と管理については、「Fortigate CNF documentation」(Fortigate CNF のドキュメント) を参照してください。
10. [次へ] を選択します。
11. [Configure third-party firewall endpoint] (サードパーティーのファイアウォールエンドポイントを設定) で、ファイアウォールエンドポイントの作成に分散デプロイモデルと集約型デプロイモデルのいずれを使用しているかに応じて、次のいずれかを実行します。

    - このポリシーに分散デプロイモデルを使用している場合は、[Availability Zones] (アベイラビリティーゾーン) で、ファイアウォールエンドポイントを作成するアベイラビリティーゾーンを選択します。アベイラビリティーゾーンは、[Availability Zone name] (アベイラビリティーゾーン名) または [Availability Zone ID] (アベイラビリティーゾーン ID) で選択できます。
    - このポリシーに集約型デプロイモデルを使用している場合は、[Inspection VPC configuration] (検査 VPC 設定) の [AWS Firewall Manager endpoint configuration] (エンドポイント設定) で、検査 VPC の所有者の AWS アカウント ID と検査 VPC の VPC ID を入力します。
        - [Availability Zones] (アベイラビリティーゾーン) で、ファイアウォールエンドポイントを作成するアベイラビリティーゾーンを選択します。アベイラビリティーゾーンは、[Availability

Zone name] (アベイラビリティーゾーン名) または [Availability Zone ID] (アベイラビリティーゾーン ID) で選択できます。

12. [Next] (次へ) を選択します。
13. [Policy scope] (ポリシーの範囲) の [AWS アカウント this policy applies to] (このポリシーが適用される) で、次のようにオプションを選択します。

    - 組織内のすべてのアカウントにポリシーを適用する場合は、デフォルトの選択のままにし、AWS 組織内のすべてのアカウントを含めます。
    - ポリシーを特定の AWS Organizations 組織単位 (OUs) にある特定のアカウントにのみ適用する場合は、指定されたアカウントと組織単位のみを含めるを選択し、含めるアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。
    - 特定のアカウントまたは AWS Organizations 組織単位 (OUs) を除くすべてのアカウントにポリシーを適用する場合は、指定されたアカウントと組織単位を除外し、その他をすべて含めてから、除外するアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。

    選択できるオプションは 1 つのみです。

    ポリシーを適用すると、Firewall Manager は新しいアカウントを設定と照合して自動的に評価します。例えば、特定のアカウントのみを含めると、Firewall Manager は新しいアカウントにポリシーを適用しません。別の例として、OU を含めた場合、OU またはその子である OU にアカウントを追加すると、Firewall Manager は新しいアカウントにポリシーを自動的に適用します。

    Fortigate CNF ポリシーの [リソースタイプ] は [VPC] です。
14. [リソース] では、指定したタグでリソースを含めるか除外するかによって、タグ付けを使用してポリシーの範囲を絞り込むことができます。包含または除外は使用できますが、両方を使用することはできません。ポリシーの範囲を定義するタグの詳細については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

    リソースタグには NULL 以外の値のみを含めることができます。タグの値を省略すると、Firewall Manager は空の文字列値 "" でタグを保存します。リソースタグは、同じキーと値を持つタグのみと一致します。
15. [Grant cross-account access] (クロスアカウントアクセスを付与) で、[Download CloudFormation template] (テンプレートをダウンロード) を選択します。これにより、

CloudFormation スタックの作成に使用できる CloudFormation テンプレートがダウンロードされます。このスタックは、Fortigate CNF リソースを管理するためのクロスアカウントアクセス許可を Firewall Manager に付与する AWS Identity and Access Management ロールを作成します。スタックの詳細については、「CloudFormation ユーザーガイド」の「StackSets の操作」を参照してください。スタックを作成するには、Fortigate CNF ポータルのアカウント ID が必要です。

16. [次へ] を選択します。
17. [ポリシータグ] で、Firewall Manager ポリシーリソースに必要な識別タグを追加します。タグの詳細については、「タグエディタの使用」を参照してください。
18. [次へ] を選択します。
19. 新しいポリシー設定を確認し、調整が必要なページに戻ります。

    [Policy actions] (ポリシーアクション) が [Identify resources that don't comply with the policy rules, but don't auto remediate] (ポリシールールに準拠していないリソースを特定するが、自動修復しない) に設定されていることを確認します。これにより、ポリシーを有効にする前に、ポリシーが行う変更を確認できます。
20. ポリシーが完成したら、[ポリシーの作成] を選択します。

    [AWS Firewall Manager ポリシー] ペインにポリシーが一覧表示されます。アカウントのヘッダーの下に [保留中] と表示され、[自動修復] のステータスが示されます。ポリシーの作成には数分かかることがあります。[Pending] (保留中) ステータスがアカウント数に置き換えられたら、ポリシー名を選択して、アカウントとリソースの準拠ステータスを調べることができます。詳細については、「AWS Firewall Manager ポリシーのコンプライアンス情報の表示」を参照してください。

Firewall Manager Fortigate CNF ポリシーの詳細については、「Firewall Manager に Fortigate Cloud Native Firewall (CNF) as a Service ポリシーを使用する」を参照してください。

AWS Firewall Manager ポリシーの使用

AWS Firewall Manager には、次のタイプのポリシーが用意されています。ポリシータイプごとに、以下を定義します:

- AWS WAF policy – Firewall Manager は AWS WAF および AWS WAF Classic ポリシーをサポートしています。どちらのバージョンでも、ポリシーによって保護されるリソースを定義します。

  - AWS WAF ポリシータイプは、一連のルールグループをウェブ ACL で最初と最後に実行します。ウェブ ACL を適用するアカウントでは、アカウント所有者はルールとルールグループを追加して、2 つのセットの間で実行できます。
  - AWS WAF Classic ポリシータイプは、単一のルールグループをウェブ ACL で実行します。
- Shield Advanced ポリシー – このポリシータイプは、指定したリソースタイプに対して組織全体で Shield Advanced 保護を適用します。
- Amazon VPC セキュリティグループポリシー – このタイプのポリシーでは、組織全体で使用中のセキュリティグループを制御し、組織全体にルールのベースラインセットを適用できます。
- Amazon VPC ネットワークアクセスコントロールリスト (ACL) ポリシー – このポリシータイプでは、組織全体で使用されているネットワーク ACL を制御し、組織全体でベースラインのネットワーク ACL セットを適用できます。
- Network Firewall ポリシー – このポリシーは、組織の VPC に AWS Network Firewall 保護を適用します。
- Amazon Route 53 Resolver DNS Firewall ポリシー – このポリシーは、DNS Firewall 保護を組織の VPC に適用します。
- サードパーティーのファイアウォールポリシー – このポリシーは、サードパーティーのファイアウォール保護に適用します。サードパーティーのファイアウォールは、 Marketplace の AWS Marketplace コンソールからサブスクリプションで利用できますAWS。
  - Palo Alto Networks Cloud NGFW ポリシー – このポリシータイプは、Palo Alto Networks Cloud Next Generation Firewall (NGFW) 保護と Palo Alto Networks Cloud NGFW ルールスタックを組織の VPC に適用します。
  - Fortigate Cloud Native Firewall (CNF) as a Service ポリシー – このポリシータイプは、Fortigate Cloud Native Firewall (CNF) as a Service の保護に適用されます。Fortigate CNF は、ゼロデイ脅威をブロックし、業界をリードする高度な脅威防止、スマートなウェブアプリケーションファイアウォール (WAF) 、API によってクラウドインフラストラクチャを保護するクラウド中心のソリューションです。

Firewall Manager ポリシーは、個々のポリシータイプに固有です。アカウント間で複数のポリシータイプを適用する場合は、複数のポリシーを作成できます。タイプごとに複数のポリシーを作成できます。

で作成した組織に新しいアカウントを追加すると AWS Organizations、Firewall Manager はポリシーの範囲内にあるそのアカウントのリソースにポリシーを自動的に適用します。

AWS Firewall Manager ポリシーの一般設定

AWS Firewall Manager 管理ポリシーには、いくつかの一般的な設定と動作があります。すべてについて、名前を指定してポリシーの範囲を定義し、リソースのタグ付けを使用してポリシーの範囲を制御できます。修復処置を行わずに準拠していないアカウントとリソースを表示するか、非準拠リソースを自動的に修復するかを選択できます。

ポリシーの範囲については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

AWS Firewall Manager ポリシーの作成

ポリシーを作成するステップは、ポリシータイプによって異なります。必ず、必要なポリシーのタイプに対応する手順を使用してください。

> **Important**
>
> AWS Firewall Manager は Amazon Route 53 または をサポートしていません AWS Global Accelerator。Shield Advanced を使用してこれらのリソースを保護する場合、Firewall Manager ポリシーは使用できません。代わりに、「AWS リソースへの AWS Shield Advanced 保護の追加」の手順に従ってください。

トピック

- の AWS Firewall Manager ポリシーの作成 AWS WAF
- AWS WAF Classic の AWS Firewall Manager ポリシーの作成
- の AWS Firewall Manager ポリシーの作成 AWS Shield Advanced
- AWS Firewall Manager 共通セキュリティグループポリシーの作成
- AWS Firewall Manager コンテンツ監査セキュリティグループポリシーの作成
- AWS Firewall Manager 使用状況監査セキュリティグループポリシーの作成
- AWS Firewall Manager ネットワーク ACL ポリシーの作成
- の AWS Firewall Manager ポリシーの作成 AWS Network Firewall
- Amazon Route 53 Resolver DNS Firewall の AWS Firewall Manager ポリシーの作成
- Palo Alto Networks Cloud NGFW の AWS Firewall Manager ポリシーの作成
- サービスとしての Fortigate Cloud Native Firewall (CNF) の AWS Firewall Manager ポリシーの作成

の AWS Firewall Manager ポリシーの作成 AWS WAF

Firewall Manager AWS WAF ポリシーでは、マネージドルールグループを使用できます。このグループ AWS と AWS Marketplace 販売者はユーザーに代わって作成および維持します。独自のルールグループを作成して使用することもできます。ルールグループの詳細については、「AWS WAF ルールグループ」を参照してください。

独自のルールグループを使用する場合は、Firewall Manager AWS WAF ポリシーを作成する前にそれらのグループを作成します。ガイダンスについては、「独自のルールグループの管理」を参照してください。個々のカスタムルールを使用するには、独自のルールグループを定義し、その中にルールを定義してから、ポリシーでそのルールグループを使用する必要があります。

Firewall Manager AWS WAF ポリシーの詳細については、「」を参照してくださいFirewall Manager での AWS WAF ポリシーの使用。

の Firewall Manager ポリシーを作成するには AWS WAF (コンソール)

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
3. [Create policy] (ポリシーの作成) を選択します。
4. [Policy type] (ポリシータイプ) では [AWS WAF] を選択します。
5. リージョンで、 を選択します AWS リージョン。Amazon CloudFront ディストリビューションを保護するには、[Global] (グローバル) を選択します。

   複数のリージョンのリソース (CloudFront ディストリビューションを除く) を保護するには、各リージョンに別々の Firewall Manager ポリシーを作成する必要があります。
6. [Next] (次へ) を選択します。
7. [Policy name] (ポリシー名) で、わかりやすい名前を入力します。Firewall Manager は、管理するウェブ ACL の名前にポリシー名を含めます。ウェブ ACL 名の後

に、FMManagedWebACLV2-、ここに入力するポリシー名、-、およびウェブ ACL 作成タイムスタンプ (UTC ミリ秒) が続きます。例えば、FMManagedWebACLV2-MyWAFPolicyName-1621880374078。

8. [ウェブリクエストボディの検査] では、オプションで本文のサイズ制限を変更してください。価格に関する考慮事項など、ボディ検査のサイズ制限については、「AWS WAF デベロッパーガイド」の「でのボディ検査の管理に関する考慮事項 AWS WAF」を参照してください。
9. ポリシールールで、ウェブ ACL で最初と最後に AWS WAF 評価するルールグループを追加します。 AWS WAF マネージドルールグループのバージョニングを使用するには、バージョニングを有効にする に切り替えます。各アカウントマネージャーは、最初のルールグループと最後のルールグループの間にルールとルールグループを追加できます。Firewall Manager ポリシーで AWS WAF ルールグループを使用する方法の詳細については AWS WAF、「」を参照してくださいFirewall Manager での AWS WAF ポリシーの使用。

   (オプション)ウェブ ACL によるルールグループの使用方法をカスタマイズするには、[編集] を選択します。一般的なカスタマイズ設定は次のとおりです。

   - マネージドルールのグループの場合は、一部またはすべてのルールのルールアクションをオーバーライドします。ルールにオーバーライドアクションを定義しない場合、評価にはルールグループ内で定義されているルールアクションが使用されます。このオプションの詳細については、「AWS WAF デベロッパーガイド」の「でのルールグループアクションの上書き AWS WAF」を参照してください。
   - 一部のマネージドルールグループは追加の設定が必要です。マネージドルールグループのプロバイダーのドキュメントを参照してください。 AWS マネージドルールのルールグループに固有の情報については、「 AWS WAF デベロッパーガイドAWS の マネージドルール AWS WAF」の「」を参照してください。

   設定が完了したら、[Save rule] (ルールを保存) を選択します。
10. ウェブ ACL のデフォルトアクションを設定します。これは、ウェブリクエストがウェブ ACL のルールのいずれにも一致しない場合に AWS WAF が実行するアクションです。[Allow] (許可) アクションでカスタムヘッダーを追加することや、[Block] (ブロック) アクションのカスタムレスポンスを追加することができます。デフォルトのウェブ ACL アクションの詳細については、「で保護パック (ウェブ ACL) のデフォルトアクションを設定する AWS WAF」を参照してください。カスタムウェブリクエストを設定する方法については、「でカスタマイズされたウェブリクエストとレスポンス AWS WAF」を参照してください。
11. [ログ記録設定] で、[ログ記録を有効にする] を選択してログ記録をオンにします。ログ記録は、ウェブ ACL で分析されるトラフィックに関する詳細情報を提供します。[ログの出力先] を選択

し、設定したログ記録の送信先を選択します。名前が aws-waf-logs- で始まるログ記録先を選択する必要があります。 AWS WAF ログ記録先の設定については、「」を参照してくださいFirewall Manager での AWS WAF ポリシーの使用。

12. (オプション) 特定のフィールドとその値がログに含まれることを希望しない場合には、このフィールドをマスキングします。マスキングするフィールドを選び、[Add] (追加) を選択します。必要に応じて手順を繰り返し、追加のフィールドをマスキングします。マスキングされたフィールドは、ログに REDACTED と表示されます。例えば、[URI] フィールドをマスキングすると、ログの [URI] フィールドは REDACTED となります。

13. (オプション) すべてのリクエストをログに送信しない場合は、フィルタリング条件と動作を追加します。[Filter logs] (ログをフィルタリング) で、適用する各フィルターについて [Add filter] (フィルターを追加) を選択し、次にフィルター基準を選択して、基準に一致するリクエストを保持するかドロップするかを指定します。フィルターの追加が完了したら、必要に応じて、[Default logging behavior] (デフォルトのログ記録動作) を変更します。詳細については、「AWS WAF デベロッパーガイド」の 「保護パック (ウェブ ACL) レコードの検索」を参照してください。

14. [Token domain list] (トークンドメインリスト) を定義して、保護されたアプリケーション間でトークンの共有を有効にできます。トークンは、 AWS WAF 不正コントロールアカウント乗っ取り防止 (ATP) と AWS WAF Bot Control に AWS Managed Rules ルールグループを使用する場合に実装する CAPTCHAアクションと Challengeアクション、およびアプリケーション統合 SDKs によって使用されます。

    パブリックサフィックスは許可されません。たとえば、gov.au または co.uk をトークンドメインとして使用することはできません。

    デフォルトでは、 は保護されたリソースのドメインに対してのみトークン AWS WAF を受け入れます。このリストにトークンドメインを追加すると、 はリスト内のすべてのドメインと、関連付けられたリソースのドメインのトークン AWS WAF を受け入れます。詳細については、「AWS WAF デベロッパーガイド」の 「AWS WAF 保護パック (ウェブ ACL) トークンドメインリスト設定」を参照してください。

    ウェブ ACL の CAPTCHA およびチャレンジのイミュニティ時間を変更できるのは、既存のウェブ ACL を編集するときのみです。これらの設定は、Firewall Manager の [ポリシーの詳細] ページで確認できます。これらの設定については、「でのタイムスタンプの有効期限とトークンイミュニティ時間の設定 AWS WAF」を参照してください。既存のポリシー内で [関連付けの設定]、[CAPTCHA]、[チャレンジ]、または [トークンのドメインリスト] 設定を更新すると、Firewall Manager はローカルのウェブ ACL を新しい値でオーバーライドします。ただし、ポリシーの [関連付けの設定]、[CAPTCHA]、[チャレンジ]、または [トークンのドメインリス

ト] 設定を更新していない場合は、ローカルのウェブ ACL の値は変更されません。このオプションの詳細については、「AWS WAF デベロッパーガイド」の「CAPTCHA および Challenge の AWS WAF」を参照してください。

15. [ウェブ ACL 管理] で、Firewall Manager がウェブ ACL の作成とクリーンアップを管理する方法を選択します。

    a. [関連付けられていないウェブ ACL を管理する] では、Firewall Manager が関連付けられていないウェブ ACL を管理するかどうかを選択します。このオプションを使用すると、Firewall Manager は、少なくとも 1 つのリソースがウェブ ACL を使用する場合のみ、ポリシー範囲内のアカウントにウェブ ACL を作成します。アカウントがポリシー範囲内の対象になると、少なくとも 1 つのリソースがウェブ ACL を使用する場合に、Firewall Manager はアカウントにウェブ ACL を自動的に作成します。

       このオプションを有効にすると、Firewall Manager はアカウント内の関連付けられていないウェブ ACL に 1 回だけクリーンアップを実行します。このクリーンアッププロセスには、数時間かかることがあります。Firewall Manager がウェブ ACL を作成した後、リソースがポリシー範囲から外れた場合、Firewall Manager はそのリソースとウェブ ACL の関連付けを解除しますが、関連付けられていないウェブ ACL はクリーンアップしません。Firewall Manager は、関連付けられていないウェブ ACL の管理を、ポリシーで初めて有効にした場合のみ、関連付けられていないウェブ ACL をクリーンアップします。

    b. [ウェブ ACL ソース] の場合、スコープ内リソースのすべての新しいウェブ ACL を作成するか、可能であれば既存のウェブ ACL を改良するかを指定します。Firewall Manager は、対象範囲内のアカウントが所有するウェブ ACL を改良できます。

       デフォルトの動作は、すべての新しいウェブ ACL を作成することです。これを選択すると、Firewall Manager によって管理されるすべてのウェブ ACL には、`FMManagedWebACLV2` で始まる名前が付けられます。既存のウェブ ACL を改良することを選択した場合、改良されたウェブ ACL には元の名前が付けられ、Firewall Manager によって作成された名前には `FMManagedWebACLV2` で始まる名前が付けられます。

16. 組織内の該当する各アカウントにウェブ ACL を作成したいが、まだリソースにウェブ ACL を適用しない場合は、[ポリシーアクション] で、[ポリシールールに準拠していないリソースを特定するが、自動修復しない] を選択し、[関連付けられていないウェブ ACL の管理] を選択します。これらのオプションは後で変更できます。

    代わりに、ポリシーを既存の範囲内のリソースに自動的に適用する場合は、[Auto remediate any noncompliant resources] (準拠していないリソースを自動修復する) を選択します。[関連付けられていないウェブ ACL の管理]が無効になっている場合、[準拠していないリソースを自動修復

する]のオプションで、組織内の該当する各アカウントにウェブ ACL を作成し、そのウェブ ACL をアカウント内のリソースに関連付けます。[関連付けられていないウェブ ACL の管理]が有効になっている場合は、[準拠していないリソースを自動修復する]のオプションは、ウェブ ACL への関連付けの対象になるリソースを持つアカウントでのみウェブ ACL を作成して関連付けます。

[Auto remediate any noncompliant resources] (準拠していないリソースを自動修復) を選択すると、別のアクティブな Firewall Manager ポリシーによって管理されていないウェブ ACL に対して、範囲内のリソースから既存のウェブ ACL の関連付けを削除することもできます。このオプションを選択した場合、Firewall Manager は、まずポリシーのウェブ ACL をリソースに関連付けてから、以前の関連付けを削除します。リソースに、別のアクティブな Firewall Manager ポリシーによって管理されている別のウェブ ACL との関連付けがある場合、この選択はその関連付けには影響しません。

17. [Next] (次へ) を選択します。
18. [AWS アカウント this policy applies to] (このポリシーが適用される) で、次のようにオプションを選択します。

    - 組織内のすべてのアカウントにポリシーを適用する場合は、デフォルトの選択のままにし、AWS 組織内のすべてのアカウントを含めます。
    - ポリシーを特定の AWS Organizations 組織単位 (OUs) にある特定のアカウントにのみ適用する場合は、指定されたアカウントと組織単位のみを含めるを選択し、含めるアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。
    - 特定のアカウントや AWS Organizations の組織単位 (OU) 以外のすべてにポリシーを適用する場合は、[Exclude the specified accounts and organizational units, and include all others] (指定されたアカウントと組織単位を除外し、他のすべてを含める) を選択して、除外するアカウントと OU を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。

    選択できるオプションは 1 つのみです。

    ポリシーを適用すると、Firewall Manager は新しいアカウントを設定と照合して自動的に評価します。例えば、特定のアカウントのみを含めると、Firewall Manager は新しいアカウントにポリシーを適用しません。別の例として、OU を含めた場合、OU またはその子である OU にアカウントを追加すると、Firewall Manager は新しいアカウントにポリシーを自動的に適用します。
19. [Resource type] (リソースタイプ) で、保護するリソースのタイプを選択します。

20. [リソース] では、指定したタグでリソースを含めるか除外するかによって、タグ付けを使用してポリシーの範囲を絞り込むことができます。包含または除外は使用できますが、両方を使用することはできません。ポリシーの範囲を定義するタグの詳細については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

    リソースタグには NULL 以外の値のみを含めることができます。タグの値を省略すると、Firewall Manager は空の文字列値 "" でタグを保存します。リソースタグは、同じキーと値を持つタグのみと一致します。

21. [次へ] を選択します。
22. [ポリシータグ] で、Firewall Manager ポリシーリソースに必要な識別タグを追加します。タグの詳細については、「タグエディタの使用」を参照してください。
23. [次へ] を選択します。
24. 新しいポリシー設定を確認し、調整が必要なページに戻ります。

    ポリシーが完成したら、[ポリシーの作成] を選択します。[AWS Firewall Manager ポリシー] ペインにポリシーが一覧表示されます。アカウントのヘッダーの下に [保留中] と表示され、[自動修復] のステータスが示されます。ポリシーの作成には数分かかることがあります。[Pending] (保留中) ステータスがアカウント数に置き換えられたら、ポリシー名を選択して、アカウントとリソースの準拠ステータスを調べることができます。詳細については、「AWS Firewall Manager ポリシーのコンプライアンス情報の表示」を参照してください。

AWS WAF Classic の AWS Firewall Manager ポリシーの作成

AWS WAF Classic の Firewall Manager ポリシーを作成するには (コンソール)

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

    > **Note**
    >
    > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
3. [Create policy] (ポリシーの作成) を選択します。

4. [Policy type (ポリシータイプ)] で、[AWS WAF Classic] を選択します。
5. ポリシーに追加する AWS WAF Classic ルールグループを既に作成している場合は、 AWS Firewall Manager ポリシーの作成を選択し、既存のルールグループを追加します。新しいルールグループを作成する場合は、[Create a Firewall Manager policy and add a new rule group] (Firewall Manager ポリシーを作成して新しいルールグループを追加する) を選択します。
6. リージョンで、 を選択します AWS リージョン。Amazon CloudFront のリソースを保護するには、[Global] (グローバル) を選択します。

   複数のリージョンのリソース (CloudFront リソースを除く) を保護するには、各リージョンに別々の Firewall Manager ポリシーを作成する必要があります。
7. [Next] (次へ) を選択します。
8. ルールグループを作成する場合は、AWS WAF Classic ルールグループの作成 の手順に従います。ルールグループを作成したら、次のステップに進みます。
9. ポリシー名を入力します。
10. 既存のルールグループを追加する場合は、ドロップダウンメニューを使用して追加するルールグループを選択し、[Add rule group] (ルールグループの追加) を選択します。
11. ポリシーには、[Action set by rule group] (ルールグループによって設定されたアクション) と [Count] (カウント) の 2 つのアクションがあります。ポリシーをテストする場合は、アクションを [Count] (カウント) に設定します。このアクションは、ルールグループのルールで指定されたブロックアクションを上書きします。つまり、ポリシーのアクションが [Count] (カウント) に設定されている場合、リクエストはカウントされ、ブロックされません。逆に、ポリシーのアクションを [Action set by rule group] (ルールグループによって設定されたアクション) に設定すると、ルールグループルールのアクションが使用されます。適切なアクションを選択します。
12. [Next] (次へ) を選択します。
13. [AWS アカウント this policy applies to] (このポリシーが適用される) で、次のようにオプションを選択します。

    - 組織内のすべてのアカウントにポリシーを適用する場合は、デフォルトの選択のままにし、AWS 組織内のすべてのアカウントを含めます。
    - ポリシーを特定の AWS Organizations 組織単位 (OUs) にある特定のアカウントにのみ適用する場合は、指定されたアカウントと組織単位のみを含めるを選択し、含めるアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。
    - 特定のアカウントまたは AWS Organizations 組織単位 (OUs) を除くすべてのアカウントにポリシーを適用する場合は、指定されたアカウントと組織単位を除外し、その他をすべて含めて

から、除外するアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。

選択できるオプションは 1 つのみです。

ポリシーを適用すると、Firewall Manager は新しいアカウントを設定と照合して自動的に評価します。例えば、特定のアカウントのみを含めると、Firewall Manager は新しいアカウントにポリシーを適用しません。別の例として、OU を含めた場合、OU またはその子である OU にアカウントを追加すると、Firewall Manager は新しいアカウントにポリシーを自動的に適用します。

14. 保護するリソースのタイプを選択します。
15. [リソース] では、指定したタグでリソースを含めるか除外するかによって、タグ付けを使用してポリシーの範囲を絞り込むことができます。包含または除外は使用できますが、両方を使用することはできません。ポリシーの範囲を定義するタグの詳細については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

    リソースタグには NULL 以外の値のみを含めることができます。タグの値を省略すると、Firewall Manager は空の文字列値 "" でタグを保存します。リソースタグは、同じキーと値を持つタグのみと一致します。
16. 既存のリソースにポリシーを自動的に適用する場合は、[Create and apply this policy to existing and new resources] (既存および新規のリソースにこのポリシーを作成して適用する) を選択します。

    このオプションは、 AWS 組織内の各関連アカウントにウェブ ACL を作成し、アカウント内のリソースにウェブ ACL を関連付けます。このオプションは、前述の基準 (リソースタイプとタグ) に一致するすべての新しいリソースにもポリシーを適用します。また、[Create policy but do not apply the policy to existing or new resources] (ポリシーを作成するが既存および新規のリソースにポリシーを適用しない) を選択する場合は、Firewall Manager により組織内の各関連アカウントにウェブ ACL が作成されますが、ウェブ ACL はいずれのリソースにも適用されません。ポリシーは後でリソースに適用する必要があります。適切なオプションを選択します。
17. [Replace existing associated web ACLs] (既存の関連付けられたウェブ ACL を置換) では、範囲内のリソースに対して現在定義されているウェブ ACL の関連付けをすべて削除し、このポリシーで作成しているウェブ ACL への関連付けに置き換えることができます。デフォルトでは、Firewall Manager は、新しいウェブ ACL の関連付けを追加する前に既存のウェブ ACL の関連付けを削除しません。既存の関連付けを削除する場合は、このオプションを選択します。
18. [Next] (次へ) を選択します。

19. 新しいポリシーを確認します。設定を変更するには、[Edit] (編集) を選択します。ポリシーが完成したら、[Create and apply policy] (ポリシーの作成と適用) を選択します。

の AWS Firewall Manager ポリシーの作成 AWS Shield Advanced

Shield Advanced の Firewall Manager ポリシーを作成するには (コンソール)

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
3. [Create policy] (ポリシーの作成) を選択します。
4. [Policy type] (ポリシータイプ) で、[Shield Advanced] を選択します。

   Shield Advanced ポリシーを作成するには、Shield Advanced をサブスクライブする必要があります。登録されていない場合は、登録するよう求められます。サブスクリプションの費用については、「AWS Shield Advanced の料金」を参照してください。
5. リージョンで、 を選択します AWS リージョン。Amazon CloudFront ディストリビューションを保護するには、[Global] (グローバル) を選択します。

   [Global] (グローバル) 以外のリージョンを選択する場合、複数のリージョンでリソースを保護するには、各リージョン用に個別の Firewall Manager ポリシーを作成する必要があります。
6. [Next] (次へ) を選択します。
7. [Name] (名前) で、わかりやすい名前を入力します。
8. [Global] (グローバル) リージョンポリシーの場合のみ、Shield Advanced アプリケーションレイヤー DDoS 自動緩和を管理するかどうかを選択できます。Shield Advanced 機能については、「Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和」を参照してください。

   自動緩和を有効または無効にすることを選択でき、あるいは無視することを選択できます。無視することを選択した場合、Firewall Manager は、Shield Advanced 保護のために自動緩和をまっ

たく管理しません。これらのポリシーのオプションの詳細については、「Firewall Manager の Shield Advanced ポリシーでアプリケーションレイヤー DDoS 自動緩和を使用する」を参照してください 。

9. 関連付けられていないウェブ ACL を Firewall Manager に管理させたい場合は、[ウェブ ACL 管理]で、[関連付けられていないウェブ ACL の管理]を有効にしてください。このオプションを使用すると、Firewall Manager は、少なくとも 1 つのリソースがウェブ ACL を使用する場合のみ、ポリシー範囲内のアカウントにウェブ ACL を作成します。アカウントがポリシーの対象になるといつでも、少なくとも 1 つのリソースがウェブ ACL を使用する場合に、Firewall Manager はアカウントにウェブ ACL を自動的に作成します。このオプションを有効にすると、Firewall Manager はアカウント内の関連付けられていないウェブ ACL に 1 回だけクリーンアップを実行します。このクリーンアッププロセスには、数時間かかることがあります。Firewall Manager がウェブ ACL を作成した後、リソースがポリシーの範囲から外れても、Firewall Manager はそのリソースとウェブ ACL との関連付けを解除しません。ウェブ ACL を 1 回限りのクリーンアップに含めるには、まずリソースとウェブ ACL の関連付けを手動で解除してから、[関連付けられていないウェブ ACL の管理]を有効にする必要があります。

10. [Policy action] (ポリシーアクション) では、準拠していないリソースを自動的に修復しないオプションを使用してポリシーを作成することをお勧めします。自動修復を無効にすると、新しいポリシーを適用する前にその効果を評価できます。変更が適切であることを確認したら、ポリシーを編集し、ポリシーアクションを変更して、自動修復を有効にします。

    代わりに、ポリシーを既存の範囲内のリソースに自動的に適用する場合は、[Auto remediate any noncompliant resources] (準拠していないリソースを自動修復する) を選択します。このオプションは、 AWS 組織内の該当する各アカウントとアカウント内の該当する各リソースに Shield Advanced 保護を適用します。

    グローバルリージョンポリシーについてのみ、非準拠リソースの自動修復を選択した場合、Firewall Manager で既存の AWS WAF Classic ウェブ ACL 関連付けを、最新バージョンの AWS WAF (v2) を使用して作成されたウェブ ACLs への新しい関連付けに自動的に置き換えることもできます。これを選択すると、Firewall Manager は、ポリシー用にまだウェブ ACL を持っていない範囲内のアカウントに新しい空のウェブ ACL を作成した後、以前のバージョンのウェブ ACL との関連付けを削除し、最新バージョンのウェブ ACL との新しい関連付けを作成します。このオプションの詳細については、「AWS WAF Classic ウェブ ACLs最新バージョンのウェブ ACLs」をご参照ください。

11. [Next] (次へ) を選択します。

12. [AWS アカウント this policy applies to] (このポリシーが適用される) で、次のようにオプションを選択します。

- 組織内のすべてのアカウントにポリシーを適用する場合は、デフォルトの [Include all accounts under my AWS organization] (自分の組織の下にあるすべてのアカウントを含める) を選択したままにします。
- ポリシーを特定の AWS Organizations 組織単位 (OUs) にある特定のアカウントにのみ適用する場合は、指定されたアカウントと組織単位のみを含めるを選択し、含めるアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。
- 特定のアカウントまたは AWS Organizations 組織単位 (OUs) を除くすべてのアカウントにポリシーを適用する場合は、指定されたアカウントと組織単位を除外し、その他をすべて含めてから、除外するアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。

選択できるオプションは 1 つのみです。

ポリシーを適用すると、Firewall Manager は新しいアカウントを設定と照合して自動的に評価します。例えば、特定のアカウントのみを含めると、Firewall Manager は新しいアカウントにポリシーを適用しません。別の例として、OU を含めた場合、OU またはその子である OU にアカウントを追加すると、Firewall Manager は新しいアカウントにポリシーを自動的に適用します。

13. 保護するリソースのタイプを選択します。

    Firewall Manager は、Amazon Route 53 または AWS Global Acceleratorをサポートしていません。これらのサービスからリソースを保護するために Shield Advanced を使用する必要がある場合、Firewall Manager ポリシーを使用することはできません。代わりに、「AWS リソースへの AWS Shield Advanced 保護の追加」の Shield Advanced のガイダンスに従ってください。

14. [リソース] では、指定したタグでリソースを含めるか除外するかによって、タグ付けを使用してポリシーの範囲を絞り込むことができます。包含または除外は使用できますが、両方を使用することはできません。ポリシーの範囲を定義するタグの詳細については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

    リソースタグには NULL 以外の値のみを含めることができます。タグの値を省略すると、Firewall Manager は空の文字列値 "" でタグを保存します。リソースタグは、同じキーと値を持つタグのみと一致します。

15. [次へ] を選択します。

16. [ポリシータグ] で、Firewall Manager ポリシーリソースに必要な識別タグを追加します。タグの詳細については、「タグエディタの使用」を参照してください。
17. [次へ] を選択します。
18. 新しいポリシー設定を確認し、調整が必要なページに戻ります。

    ポリシーが完成したら、[ポリシーの作成] を選択します。[AWS Firewall Manager ポリシー] ペインにポリシーが一覧表示されます。アカウントのヘッダーの下に [保留中] と表示され、[自動修復] のステータスが示されます。ポリシーの作成には数分かかることがあります。[Pending] (保留中) ステータスがアカウント数に置き換えられたら、ポリシー名を選択して、アカウントとリソースの準拠ステータスを調べることができます。詳細については、「AWS Firewall Manager ポリシーのコンプライアンス情報の表示」を参照してください。

AWS Firewall Manager 共通セキュリティグループポリシーの作成

共通セキュリティグループポリシーの仕組みの詳細については、「Firewall Manager の一般的なセキュリティグループポリシーの使用」を参照してください。

共通セキュリティグループポリシーを作成するには、ポリシーのプライマリとして使用するセキュリティグループが Firewall Manager 管理者アカウントに既に作成されている必要があります。セキュリティグループは、Amazon Virtual Private Cloud (Amazon VPC) または Amazon Elastic Compute Cloud (Amazon EC2) を通じて管理できます。詳細については、「Amazon VPC ユーザーガイド」の「セキュリティグループの操作」を参照してください。

共通セキュリティグループポリシー (コンソール) を作成するには

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
3. [Create policy] (ポリシーの作成) を選択します。
4. [Policy type] (ポリシータイプ) で、[Security group] (セキュリティグループ) を選択します。

5. [Security group policy type] (セキュリティグループポリシータイプ) で、[Common security groups] (共通セキュリティグループ) を選択します。
6. リージョンで、 を選択します AWS リージョン。
7. [次へ] を選択します。
8. [Policy name](ポリシー名) で、フレンドリ名を入力します。
9. [Policy rules] (ポリシールール) で、次の操作を行います。

   a. ルールオプションから、セキュリティグループルールとポリシーの範囲内にあるリソースに対して適用する制限を選択します。[Distribute tags from the primary security group to the security groups created by this policy] (プライマリセキュリティグループからこのポリシーによって作成されたセキュリティグループにタグを配布) を選択した場合は、[Identify and report when the security groups created by this policy become non-compliant] (このポリシーによって作成されたセキュリティグループが非準拠になったときに識別して報告) も選択する必要があります。

   > **Important**
   >
   > Firewall Manager は、 AWS サービスによって追加されたシステムタグをレプリカセキュリティグループに配布しません。システムタグは `aws:` プレフィックスで始まります。また、ポリシーに組織のタグポリシーと矛盾するタグがある場合は、Firewall Manager が既存のセキュリティグループでのタグ更新や、新しいセキュリティグループの作成を行うことはありません。タグポリシーの詳細については、「 AWS Organizations ユーザーガイド」の「タグポリシー」を参照してください。

   [プライマリセキュリティグループからのセキュリティグループの参照をこのポリシーによって作成されたセキュリティグループに配布する] を選択した場合、Firewall Manager は Amazon VPC にアクティブなピア接続がある場合にのみセキュリティグループの参照を配布します。このオプションについては、「Firewall Manager の一般的なセキュリティグループポリシーの使用」を参照してください。

   b. [プライマリセキュリティグループ] で、[プライマリセキュリティグループを追加] を選択してから、使用するセキュリティグループを選択します。Firewall Manager は、Firewall Manager 管理者アカウント内におけるすべての Amazon VPC インスタンスからのセキュリティグループのリストを設定します。

ポリシーのプライマリセキュリティグループのデフォルト最大数は 3 です。この設定についての情報は、「AWS Firewall Manager クォータ」を参照してください。

c. [Policy action] (ポリシーアクション) では、自動的に修復されないオプションを使用してポリシーを作成することをお勧めします。これにより、新しいポリシーを適用する前にその効果を評価できます。変更が適切であることを確認したら、ポリシーを編集し、ポリシーアクションを変更して、準拠していないリソースの自動修復を有効にします。

10. [Next] (次へ) を選択します。

11. [AWS アカウント this policy applies to] (このポリシーが適用される) で、次のようにオプションを選択します。

- 組織内のすべてのアカウントにポリシーを適用する場合は、デフォルトの選択のままにし、AWS 組織内のすべてのアカウントを含めます。
- ポリシーを特定の AWS Organizations 組織単位 (OUs) にある特定のアカウントにのみ適用する場合は、指定されたアカウントと組織単位のみを含めるを選択し、含めるアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。
- 特定のアカウントまたは AWS Organizations 組織単位 (OUs) を除くすべてのアカウントにポリシーを適用する場合は、指定されたアカウントと組織単位を除外し、その他をすべて含めてから、除外するアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。

選択できるオプションは 1 つのみです。

ポリシーを適用すると、Firewall Manager は新しいアカウントを設定と照合して自動的に評価します。例えば、特定のアカウントのみを含めると、Firewall Manager は新しいアカウントにポリシーを適用しません。別の例として、OU を含めた場合、OU またはその子である OU にアカウントを追加すると、Firewall Manager は新しいアカウントにポリシーを自動的に適用します。

12. [Resource type] (リソースタイプ) で、保護するリソースのタイプを選択します。

リソースタイプ [EC2 インスタンス] では、すべての Amazon EC2 インスタンスを修復するか、デフォルトのプライマリ Elastic Network Interface (ENI) のみを持つインスタンスのみを修復するかを選択できます。後者のオプションでは、Firewall Manager は追加の ENI アタッチメントを持つインスタンスを修正しません。代わりに、自動修復が有効になっている場合、Firewall Manager はこれらの EC2 インスタンスのコンプライアンスステータスのみをマークし、修復

アクションは適用されません。Amazon EC2 リソースタイプのその他の規制と制限については、セキュリティグループポリシーの規制と制限 を参照してください。

13. [リソース] では、指定したタグでリソースを含めるか除外するかによって、タグ付けを使用してポリシーの範囲を絞り込むことができます。包含または除外は使用できますが、両方を使用することはできません。ポリシーの範囲を定義するタグの詳細については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

    リソースタグには NULL 以外の値のみを含めることができます。タグの値を省略すると、Firewall Manager は空の文字列値 "" でタグを保存します。リソースタグは、同じキーと値を持つタグのみと一致します。

14. [Shared VPC resources] (共有 VPC リソース) の場合、アカウントが所有する VPC に加えて、共有 VPC 内のリソースにポリシーを適用する場合は、[Include resources from shared VPCs] (共有 VPC からのリソースを含める) を選択します。
15. [Next] (次へ) を選択します。
16. ポリシー設定を見直して目的の設定になっていることを確認し、[Create policy] (ポリシーの作成) を選択します。

Firewall Manager は、範囲内のアカウントに含まれるすべての Amazon VPC インスタンスに、アカウントごとにサポートされる Amazon VPC の最大クォータまで、プライマリセキュリティグループのレプリカを作成します。Firewall Manager は、レプリカセキュリティグループを、範囲内の各アカウント用のポリシーの範囲内にあるリソースに関連付けます。このポリシーの仕組みの詳細については、「Firewall Manager の一般的なセキュリティグループポリシーの使用」を参照してください。

AWS Firewall Manager コンテンツ監査セキュリティグループポリシーの作成

コンテンツ監査セキュリティグループポリシーの仕組みの詳細については、「Firewall Manager のコンテンツ監査セキュリティグループポリシーの使用」を参照してください。

コンテンツ監査ポリシーの設定によっては、Firewall Manager がテンプレートとして使用するための監査セキュリティグループを指定する必要があります。例えば、どのセキュリティグループでも許可しないすべてのルールを含む監査セキュリティグループがあるとします。ポリシーでこれらの監査セキュリティグループを使用するには、Firewall Manager 管理者アカウントを使用してこれらの監査セキュリティグループを作成する必要があります。セキュリティグループは、Amazon Virtual Private Cloud (Amazon VPC) または Amazon Elastic Compute Cloud (Amazon EC2) を通じて管理できます。詳細については、「Amazon VPC ユーザーガイド」の「セキュリティグループの操作」を参照してください。

コンテンツ監査セキュリティグループポリシーを作成するには (コンソール)

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
3. [Create policy] (ポリシーの作成) を選択します。
4. [Policy type] (ポリシータイプ) で、[Security group] (セキュリティグループ) を選択します。
5. [Security group policy type] (セキュリティグループポリシータイプ) で、[Auditing and enforcement of security group rules] (セキュリティグループルールの監査と適用) を選択します。
6. リージョンで、 を選択します AWS リージョン。
7. [次へ] を選択します。
8. [Policy name](ポリシー名) で、フレンドリ名を入力します。
9. [Policy rules] (ポリシールール) で、使用するマネージドポリシールールオプションまたはカスタムポリシールールオプションを選択します。

   a. [Configure managed audit policy rules] (マネージド監査ポリシールールを設定) で、次の手順を実行します。

      i. [Configure security group rules to audit] (監査するセキュリティグループルールを設定) で、監査ポリシーを適用するセキュリティグループルールの種類を選択します。

      ii. セキュリティグループ内のプロトコル、ポート、CIDR 範囲設定に基づく監査ルールなどを実行する場合は、[過度に許容されるセキュリティグループルールを監査] を選択し、必要なオプションを選択します。

      [ルールですべてのトラフィックを許可する] を選択すると、カスタムアプリケーションリストを指定して、監査するアプリケーションを指定できます。カスタムアプリケーションリスト、およびポリシーでのアプリケーションリストの使用方法については、「マネージドリストの使用」および「マネージドリストの使用」を参照してください。

プロトコルリストを使用する選択では、既存のリストを使用したり、新しいリストを作成したりできます。プロトコルリスト、およびポリシーでのアプリケーションリストの使用方法については、「マネージドリストの使用」および「マネージドリストの使用」を参照してください。

iii. 予約済みまたは予約されていない CIDR 範囲へのアクセスに基づいて高リスクを監査する場合は、[高リスクアプリケーションを監査する] を選択し、必要なオプションを選択します。

[ローカル CIDR 範囲のみにアクセスできるアプリケーション] と [パブリック CIDR 範囲を使用できるアプリケーション] の選択は相互に排他的です。いずれのポリシーでも、選択できるのは最大 1 つです。

アプリケーションリストを使用する選択では、既存のリストを使用したり、新しいリストを作成したりできます。アプリケーションリスト、およびポリシーでのアプリケーションリストの使用方法については、「マネージドリストの使用」および「マネージドリストの使用」を参照してください。

iv. [Overrides] (上書き) 設定を使用して、ポリシー内の他の設定を明示的に上書きします。ポリシーに設定した他のオプションに準拠しているかどうかにかかわらず、特定のセキュリティグループルールを常に許可するか常に拒否するかを選択できます。

このオプションでは、許可されたルールまたは拒否されたルールテンプレートとして監査セキュリティグループを指定します。[Audit security groups] (監査セキュリティグループ) で、[Add audit security groups] (監査セキュリティグループを追加) を選択してから、使用するセキュリティグループを選択します。Firewall Manager は、Firewall Manager 管理者アカウント内におけるすべての Amazon VPC インスタンスからの監査セキュリティグループのリストを設定します。ポリシーの監査セキュリティグループ数のデフォルト最大クォータは 1 です。クォータを引き上げる方法については、「AWS Firewall Manager クォータ」を参照してください。

b. [Configure custom policy rules] (カスタムポリシールールを設定) で、次の手順を実行します。

i. ルールオプションから、監査セキュリティグループで定義されたルールのみを許可するか、すべてのルールを拒否するかを選択します。この選択の詳細については、「Firewall Manager のコンテンツ監査セキュリティグループポリシーの使用」を参照してください。

ii. [Audit security groups] (監査セキュリティグループ) で、[Add audit security groups] (監査セキュリティグループを追加) を選択してから、使用するセキュリティグループを選択します。Firewall Manager は、Firewall Manager 管理者アカウント内におけるすべての Amazon VPC インスタンスからの監査セキュリティグループのリストを設定します。ポリシーの監査セキュリティグループ数のデフォルト最大クォータは 1 です。クォータを引き上げる方法については、「AWS Firewall Manager クォータ」を参照してください。

iii. [Policy action] (ポリシーアクション) では、自動的に修復されないオプションを使用してポリシーを作成する必要があります。これにより、新しいポリシーを適用する前にその効果を評価できます。変更が適切であることを確認したら、ポリシーを編集し、ポリシーアクションを変更して、準拠していないリソースの自動修復を有効にします。

10. [Next] (次へ) を選択します。
11. [AWS アカウント this policy applies to] (このポリシーが適用される) で、次のようにオプションを選択します。

    - 組織内のすべてのアカウントにポリシーを適用する場合は、デフォルトの選択のままにし、AWS 組織内のすべてのアカウントを含めます。
    - ポリシーを特定の AWS Organizations 組織単位 (OUs) にある特定のアカウントにのみ適用する場合は、指定されたアカウントと組織単位のみを含めるを選択し、含めるアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。
    - 特定のアカウントまたは AWS Organizations 組織単位 (OUs) を除くすべてのアカウントにポリシーを適用する場合は、指定されたアカウントと組織単位を除外し、その他をすべて含めてから、除外するアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。

    選択できるオプションは 1 つのみです。

    ポリシーを適用すると、Firewall Manager は新しいアカウントを設定と照合して自動的に評価します。例えば、特定のアカウントのみを含めると、Firewall Manager は新しいアカウントにポリシーを適用しません。別の例として、OU を含めた場合、OU またはその子である OU にアカウントを追加すると、Firewall Manager は新しいアカウントにポリシーを自動的に適用します。
12. [Resource type] (リソースタイプ) で、保護するリソースのタイプを選択します。

13. [リソース] では、指定したタグでリソースを含めるか除外するかによって、タグ付けを使用してポリシーの範囲を絞り込むことができます。包含または除外は使用できますが、両方を使用することはできません。ポリシーの範囲を定義するタグの詳細については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

    リソースタグには NULL 以外の値のみを含めることができます。タグの値を省略すると、Firewall Manager は空の文字列値 "" でタグを保存します。リソースタグは、同じキーと値を持つタグのみと一致します。
14. [次へ] を選択します。
15. ポリシー設定を見直して目的の設定になっていることを確認し、[Create policy] (ポリシーの作成) を選択します。

Firewall Manager は、ポリシールールの設定に従って、監査セキュリティグループを AWS 組織内の範囲内セキュリティグループと比較します。ポリシーのステータスは、 AWS Firewall Manager ポリシーコンソールで確認できます。ポリシーを作成したら、ポリシーを編集して自動修復を有効にし、監査セキュリティグループポリシーを有効にすることができます。このポリシーの仕組みの詳細については、「Firewall Manager のコンテンツ監査セキュリティグループポリシーの使用」を参照してください。

AWS Firewall Manager 使用状況監査セキュリティグループポリシーの作成

使用状況監査セキュリティグループポリシーの仕組みの詳細については、「Firewall Manager の使用状況監査セキュリティグループポリシーの使用」を参照してください。

使用状況監査セキュリティグループポリシーを作成するには (コンソール)

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

    > **Note**
    >
    > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。
2. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
3. [Create policy] (ポリシーの作成) を選択します。

4. [Policy type] (ポリシータイプ) で、[Security group] (セキュリティグループ) を選択します。
5. [セキュリティグループポリシータイプ]で、[未使用および冗長セキュリティグループの監査とクリーンアップ]を選択します。
6. リージョンで、 を選択します AWS リージョン。
7. [次へ] を選択します。
8. [Policy name](ポリシー名) で、フレンドリ名を入力します。
9. [Policy rules] (ポリシールール) で、使用可能なオプションのいずれかまたは両方を選択します。

   - [このポリシーの範囲内のセキュリティグループは少なくとも 1 つのリソースによって使用される必要があります] を選択した場合、Firewall Manager は、未使用と判断されるセキュリティグループを削除します。このルールを有効にすると、Firewall Manager により、ポリシーの保存時に最後に実行されます。

     Firewall Manager が使用状況と修復のタイミングを決定する方法の詳細については、Firewall Manager の使用状況監査セキュリティグループポリシーの使用 を参照してください。

     > **Note**
     >
     > この使用状況監査セキュリティグループポリシータイプを使用する場合は、スコープ内のセキュリティグループの関連付けステータスを短時間で複数回変更しないでください。そうすると、Firewall Manager が対応するイベントを見逃す可能性があります。

     デフォルトでは、セキュリティグループが使用されていない場合、Firewall Manager はこのポリシールールに準拠していないとみなします。必要に応じて、セキュリティグループが非準拠とみなされる前に、未使用のセキュリティグループが存在できる時間を分単位で指定できます。最大は 525,600 分 (365 日) です。新しいセキュリティグループをリソースに関連付ける時間を確保するために、この設定をより高くすることができます。

     > **Important**
     >
     > デフォルト値の 0 以外の分間数を指定する場合は、 AWS Configで間接的な関係を有効にする必要があります。それ以外の場合、使用状況監査セキュリティグループポリシーは意図したとおりに機能しません。の間接的な関係については AWS Config、

AWS Config デベロッパーガイドの「 の間接的な関係 AWS Config」を参照してください。

- [このポリシーの範囲内のセキュリティグループは一意である必要があります] を選択した場合、Firewall Manager は、冗長なセキュリティグループを統合し、1 つのセキュリティグループのみがリソースに関連付けられるようにします。これを選択すると、Firewall Manager により、ポリシーの保存時に最初に実行されます。

10. [Policy action] (ポリシーアクション) では、自動的に修復されないオプションを使用してポリシーを作成することをお勧めします。これにより、新しいポリシーを適用する前にその効果を評価できます。変更が適切であることを確認したら、ポリシーを編集し、ポリシーアクションを変更して、準拠していないリソースの自動修復を有効にします。
11. [Next] (次へ) を選択します。
12. [AWS アカウント this policy applies to] (このポリシーが適用される) で、次のようにオプションを選択します。

    - 組織内のすべてのアカウントにポリシーを適用する場合は、デフォルトの選択のままにし、AWS 組織内のすべてのアカウントを含めます。
    - 特定の AWS Organizations 組織単位 (OUs) にある特定のアカウントまたはアカウントにのみポリシーを適用する場合は、指定されたアカウントと組織単位のみを含めるを選択し、含めるアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。
    - 特定のアカウントまたは AWS Organizations 組織単位 (OUs) を除くすべてのアカウントにポリシーを適用する場合は、指定されたアカウントと組織単位を除外し、その他をすべて含めてから、除外するアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。

    選択できるオプションは 1 つのみです。

    ポリシーを適用すると、Firewall Manager は新しいアカウントを設定と照合して自動的に評価します。例えば、特定のアカウントのみを含めると、Firewall Manager は新しいアカウントにポリシーを適用しません。別の例として、OU を含めた場合、OU またはその子である OU にアカウントを追加すると、Firewall Manager は新しいアカウントにポリシーを自動的に適用します。
13. [リソース] では、指定したタグでリソースを含めるか除外するかによって、タグ付けを使用してポリシーの範囲を絞り込むことができます。包含または除外は使用できますが、両方を使

用することはできません。ポリシーの範囲を定義するタグの詳細については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

リソースタグには NULL 以外の値のみを含めることができます。タグの値を省略すると、Firewall Manager は空の文字列値 "" でタグを保存します。リソースタグは、同じキーと値を持つタグのみと一致します。

14. [次へ] を選択します。
15. ポリシーの範囲から Firewall Manager 管理者アカウントを除外していない場合、Firewall Manager によりこれを行うよう求められます。これにより、セキュリティグループは Firewall Manager 管理者アカウントに残ります。このアカウントは、手動コントロール下で、共通セキュリティグループポリシーおよび監査セキュリティグループポリシーに使用します。このダイアログで目的のオプションを選択します。
16. ポリシー設定を見直して目的の設定になっていることを確認し、[Create policy] (ポリシーの作成) を選択します。

一意のセキュリティグループにする必要があることを選択した場合、Firewall Manager は各範囲内 Amazon VPC インスタンスで冗長セキュリティグループをスキャンします。その後、各セキュリティグループを少なくとも 1 つのリソースで使用するように選択した場合、Firewall Manager は、ルールで指定された時間 (単位: 分)、未使用のままのセキュリティグループをスキャンします。ポリシーのステータスは、 AWS Firewall Manager ポリシーコンソールで確認できます。このポリシーの仕組みの詳細については、「Firewall Manager の使用状況監査セキュリティグループポリシーの使用」を参照してください。

AWS Firewall Manager ネットワーク ACL ポリシーの作成

ネットワーク Firewall ポリシーの仕組みの詳細については、ネットワーク ACL ポリシー を参照してください。

ネットワーク ACL ポリシーを作成するには、Amazon VPC サブネットで使用するネットワーク ACL を定義する方法を知る必要があります。詳細については、「Amazon VPC ユーザーガイド」の「ACL を使用して、サブネットのトラフィックを制御する」および「ネットワーク ACL の動作」を参照してください。

ネットワーク ACL ポリシーを作成するには (コンソールで)

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/

fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

> **Note**
>
> Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
3. [Create policy] (ポリシーの作成) を選択します。
4. [ポリシータイプ] で、[ネットワーク ACL] を選択します。
5. リージョンで、 を選択します AWS リージョン。
6. [次へ] を選択します。
7. [Policy name] (ポリシー名) で、わかりやすい名前を入力します。
8. [ポリシールール] では、Firewall Manager が管理するネットワーク ACL で常に実行するルールを定義します。ネットワーク ACL インバウンドトラフィックとアウトバウンドトラフィックをモニタリングして処理するため、ポリシーでは両方の方向のルールを定義します。

   どちらの方向でも、常に最初に実行するルールと、最後に実行するルールを定義します。Firewall Manager が管理するネットワーク ACL では、アカウント所有者は、これらの最初と最後のルールの間で実行するカスタムルールを定義できます。
9. [ポリシーアクション] で、非準拠のサブネットとネットワーク ACL を識別したいが、まだ修正アクションを実行しない場合は、[ポリシールールに準拠していないが、自動修正しないリソースの特定] を選択します。これらのオプションは後で変更できます。

   代わりに、ポリシーを既存の範囲内のリソースに自動的に適用する場合は、[準拠していないリソースを自動修復する] を選択します。このオプションでは、ポリシールールのトラフィック処理動作がネットワーク ACL にあるカスタムルールと競合した場合に、強制的な修復を行うかどうかも指定します。Firewall Manager は、強制的な修復の有無にかかわらず、コンプライアンス違反で競合するルールを報告します。
10. [次へ] を選択します。
11. [AWS アカウント this policy applies to] (このポリシーが適用される) で、次のようにオプションを選択します。

    - 組織内のすべてのアカウントにポリシーを適用する場合は、デフォルトの選択のままにし、AWS 組織内のすべてのアカウントを含めます。

- ポリシーを特定の AWS Organizations 組織単位 (OUs) にある特定のアカウントにのみ適用する場合は、指定されたアカウントと組織単位のみを含めるを選択し、含めるアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。
- 特定のアカウントまたは AWS Organizations 組織単位 (OUs) を除くすべてのアカウントにポリシーを適用する場合は、指定されたアカウントと組織単位を除外し、その他をすべて含めてから、除外するアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。

選択できるオプションは 1 つのみです。

ポリシーを適用すると、Firewall Manager は新しいアカウントを設定と照合して自動的に評価します。例えば、特定のアカウントのみを含めると、Firewall Manager は新しい異なるアカウントにポリシーを適用しません。別の例として、OU を含めた場合、OU またはその子である OU にアカウントを追加すると、Firewall Manager は新しいアカウントにポリシーを自動的に適用します。

12. [リソースタイプ] の場合、設定は [サブネット] に固定されます。
13. [リソース] では、指定したタグでリソースを含めるか除外するかによって、タグ付けを使用してポリシーの範囲を絞り込むことができます。包含または除外は使用できますが、両方を使用することはできません。ポリシーの範囲を定義するタグの詳細については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

    リソースタグには NULL 以外の値のみを含めることができます。タグの値を省略すると、Firewall Manager は空の文字列値 "" でタグを保存します。リソースタグは、同じキーと値を持つタグのみと一致します。
14. [次へ] を選択します。
15. ポリシー設定を見直して目的の設定になっていることを確認し、[Create policy] (ポリシーの作成) を選択します。

Firewall Manager はポリシーを作成し、設定に従ってスコープ内ネットワーク ACL のモニタリングと管理を開始します。このポリシーの仕組みの詳細については、「ネットワーク ACL ポリシー」を参照してください。

の AWS Firewall Manager ポリシーの作成 AWS Network Firewall

Firewall Manager の Network Firewall ポリシーでは、 AWS Network Firewallで管理するルールグループを使用します。ルールグループの管理については、「Network Firewall デベロッパーガイド」の「AWS Network Firewall ルールグループ」を参照してください。

Firewall Manager の Network Firewall ポリシーについては、「Firewall Manager での AWS Network Firewall ポリシーの使用」を参照してください。

の Firewall Manager ポリシーを作成するには AWS Network Firewall (コンソール)

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
3. [Create policy] (ポリシーの作成) を選択します。
4. [Policy type] (ポリシータイプ) では [AWS Network Firewall] を選択します。
5. [Firewall management type] (ファイアウォールの管理タイプ) で、Firewall Manager にポリシーのファイアウォールをどのように管理させるか選択します。次のオプションから選択します。

   - [Distributed] (分散型) を使用すると、Firewall Manager は、ポリシーの範囲内の各 VPC でファイアウォールエンドポイントを作成および維持します。
   - [Centralized] (集約型) を使用すると、Firewall Manager は、単一の検査 VPC でエンドポイントを作成および維持します。
   - [Import existing firewalls] (既存のファイアウォールのインポート)- Firewall Manager は、リソースセットを使用して Network Firewall から既存のファイアウォールをインポートします。リソースセットの詳細については、「Firewall Manager でのリソースのグループ化する」を参照してください。

6. リージョンで、 を選択します AWS リージョン。複数のリージョンのリソースを保護するには、各リージョンに別々の ポリシーを作成する必要があります。

7. [Next] (次へ) を選択します。
8. [Policy name] (ポリシー名) で、わかりやすい名前を入力します。Firewall Manager は、Network Firewall のファイアウォールおよび作成するファイアウォールポリシーの名前にポリシー名を含めます。
9. [AWS Network Firewall policy configuration] (ポリシー設定) では、Network Firewall の場合と同じようにファイアウォールポリシーを設定します。ステートレスルールグループおよびステートフルルールグループを追加し、ポリシーのデフォルトアクションを指定します。オプションで、ポリシーのステートフルルール評価順序とデフォルトアクションを設定し、ログ記録設定を行うことができます。Network Firewall のファイアウォールポリシーの管理については、「AWS Network Firewall デベロッパーガイド」の「AWS Network Firewall ファイアウォールポリシー」を参照してください。

   Firewall Manager の Network Firewall ポリシーを作成すると、Firewall Manager は、範囲内にあるアカウント用にファイアウォールポリシーを作成します。個々のアカウントマネージャーは、ファイアウォールポリシーにルールグループを追加できますが、ここで指定する設定を変更することはできません。
10. [次へ] を選択します。
11. 前のステップで選択した [Firewall management type] (ファイアウォール管理タイプ) に応じて、次のいずれかを実行します。

    - [分散型] ファイアウォール管理タイプを使用している場合、[AWS Firewall Manager エンドポイント設定] 内の [ファイアウォールのエンドポイントの場所] で、以下のオプションのいずれかを選択します。
      - [Custom endpoint configuration] (カスタムエンドポイント設定) - Firewall Manager は、指定したアベイラビリティーゾーンに、ポリシー範囲内の各 VPC に対してファイアウォールを作成します。各ファイアウォールには、少なくとも 1 つのファイアウォールエンドポイントが含まれています。
        - [Availability Zones] (アベイラビリティーゾーン) で、ファイアウォールエンドポイントを作成するアベイラビリティーゾーンを選択します。アベイラビリティーゾーンは、[Availability Zone name] (アベイラビリティーゾーン名) または [Availability Zone ID] (アベイラビリティーゾーン ID) で選択できます。
        - Firewall Manager が VPC のファイアウォールサブネットに使用する CIDR ブロックを指定する場合、そのすべては /28 CIDR ブロックである必要があります。1 行に 1 つのブロックを入力します。これらを省略すると、Firewall Manager は、VPC で使用可能な IP アドレスから選択します。

> **Note**
>
> 自動修復は AWS Firewall Manager Network Firewall ポリシーに対して自動的に行われるため、ここで自動修復を選択しないオプションは表示されません。

- エンドポイントの自動設定 - Firewall Manager は、VPC 内のパブリックサブネットを持つアベイラビリティーゾーンにファイアウォールエンドポイントを自動的に作成します。
  - [Firewall endpoints] (ファイアウォールエンドポイント) の設定では、Firewall Manager によるファイアウォールエンドポイントの管理方法を指定します。高可用性を実現するために、複数のエンドポイントを使用することをお勧めします。
- このポリシーに [集約型] ファイアウォール管理タイプを使用している場合は、[AWS Firewall Manager エンドポイント設定] 内の [インスペクション VPC の設定] で、検査 VPC の所有者の AWS アカウント ID と検査 VPC の VPC ID を入力します。
  - [Availability Zones] (アベイラビリティーゾーン) で、ファイアウォールエンドポイントを作成するアベイラビリティーゾーンを選択します。アベイラビリティーゾーンは、[Availability Zone name] (アベイラビリティーゾーン名) または [Availability Zone ID] (アベイラビリティーゾーン ID) で選択できます。
  - Firewall Manager が VPC のファイアウォールサブネットに使用する CIDR ブロックを指定する場合、そのすべては /28 CIDR ブロックである必要があります。1 行に 1 つのブロックを入力します。これらを省略すると、Firewall Manager は、VPC で使用可能な IP アドレスから選択します。

> **Note**
>
> 自動修復は AWS Firewall Manager Network Firewall ポリシーに対して自動的に行われるため、ここで自動修復を選択しないオプションは表示されません。

- [Import existing firewalls] (既存のファイアウォールのインポート) のファイアウォール管理タイプを使用している場合は、[Resource sets] (リソースセット) で 1 つ以上のリソースセットを追加します。リソースセットは、このポリシーで一元管理したい組織のアカウントが所有する既存の Network Firewall を定義します。リソースセットをポリシーに追加するには、まずコンソールまたは「PutResourceSet」API を使用してリソースセットを作成する必要があります。リソースセットの詳細については、「Firewall Manager でのリソースのグループ化する」を参照してください。Network Firewall から既存のファイアウォールをインポートする方法の詳細については、「」を参照してくださいFirewall Manager がファイアウォールエンドポイントを作成する方法。

12. [次へ] を選択します。
13. ポリシーで分散型ファイアウォール管理タイプを使用している場合は、[Route management] (ルート管理) で、Firewall Manager がそれぞれのファイアウォールエンドポイントを経由してルーティングする必要のあるトラフィックをモニタリングおよびアラートするかどうかを選択します。

    > **Note**
    >
    > [Monitor] (モニタリング) を選択した場合、後日設定を [Off] (オフ) に変更することはできません。モニタリングは、ポリシーを削除するまで継続します。

14. [Traffic type] (トラフィックタイプ) で、ファイアウォール検査のためにトラフィックをルーティングするトラフィックエンドポイントをオプションで追加します。
15. [Allow required cross-AZ traffic] (必要なクロス AZ トラフィックを許可) で、このオプションを有効にすると、Firewall Manager は、独自のファイアウォールエンドポイントを持たないアベイラビリティーゾーンの場合、検査のためにアベイラビリティーゾーンからトラフィックを送信する準拠ルーティングとして扱います。エンドポイントを持つアベイラビリティーゾーンでは、常に独自のトラフィックを検査する必要があります。
16. [Next] (次へ) を選択します。
17. [Policy scope] (ポリシーの範囲) の [AWS アカウント this policy applies to] (このポリシーが適用される) で、次のようにオプションを選択します。

    - 組織内のすべてのアカウントにポリシーを適用する場合は、デフォルトの選択のままにし、AWS 組織内のすべてのアカウントを含めます。
    - ポリシーを特定の AWS Organizations 組織単位 (OUs) にある特定のアカウントにのみ適用する場合は、指定されたアカウントと組織単位のみを含めるを選択し、含めるアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。
    - 特定のアカウントまたは AWS Organizations 組織単位 (OUs) を除くすべてのアカウントにポリシーを適用する場合は、指定されたアカウントと組織単位を除外し、その他をすべて含めてから、除外するアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。

    選択できるオプションは 1 つのみです。

ポリシーを適用すると、Firewall Manager は新しいアカウントを設定と照合して自動的に評価します。例えば、特定のアカウントのみを含めると、Firewall Manager は新しいアカウントにポリシーを適用しません。別の例として、OU を含めた場合、OU またはその子である OU にアカウントを追加すると、Firewall Manager は新しいアカウントにポリシーを自動的に適用します。

18. Network Firewall ポリシーの [Resource type] (リソースタイプ) は [VPC] です。
19. [リソース] では、指定したタグでリソースを含めるか除外するかによって、タグ付けを使用してポリシーの範囲を絞り込むことができます。包含または除外は使用できますが、両方を使用することはできません。ポリシーの範囲を定義するタグの詳細については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

    リソースタグには NULL 以外の値のみを含めることができます。タグの値を省略すると、Firewall Manager は空の文字列値 "" でタグを保存します。リソースタグは、同じキーと値を持つタグのみと一致します。
20. [次へ] を選択します。
21. [ポリシータグ] で、Firewall Manager ポリシーリソースに必要な識別タグを追加します。タグの詳細については、「タグエディタの使用」を参照してください。
22. [次へ] を選択します。
23. 新しいポリシー設定を確認し、調整が必要なページに戻ります。

    ポリシーが完成したら、[ポリシーの作成] を選択します。[AWS Firewall Manager ポリシー] ペインにポリシーが一覧表示されます。アカウントのヘッダーの下に [保留中] と表示され、[自動修復] のステータスが示されます。ポリシーの作成には数分かかることがあります。[Pending] (保留中) ステータスがアカウント数に置き換えられたら、ポリシー名を選択して、アカウントとリソースの準拠ステータスを調べることができます。詳細については、「AWS Firewall Manager ポリシーのコンプライアンス情報の表示」を参照してください。

Amazon Route 53 Resolver DNS Firewall の AWS Firewall Manager ポリシーの作成

Firewall Manager の DNS Firewall ポリシーでは、Amazon Route 53 Resolver DNS Firewall で管理するルールグループを使用します。ルールグループの管理については、「Amazon Route 53 デベロッパーガイド」の「DNS Firewall でのルールグループおよびルールの管理」を参照してください。

Firewall Manager の DNS Firewall ポリシーについては、「Firewall Manager の Amazon Route 53 Resolver DNS Firewall ポリシーを使用する」を参照してください。

Amazon Route 53 Resolver DNS Firewall の Firewall Manager ポリシーを作成するには (コンソール)

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
3. [Create policy] (ポリシーの作成) を選択します。
4. [Policy type] (ポリシータイプ) で、[Amazon Route 53 Resolver DNS Firewall] を選択します。
5. リージョンで、 を選択します AWS リージョン。複数のリージョンのリソースを保護するには、各リージョンに別々の ポリシーを作成する必要があります。
6. [Next] (次へ) を選択します。
7. [Policy name] (ポリシー名) で、わかりやすい名前を入力します。
8. ポリシー設定で、VPC のルールグループの関連付けの中で DNS Firewall が最初と最後に評価するルールグループを追加します。ポリシーには最大 2 つのルールグループを追加できます。

   Firewall Manager の DNS Firewall ポリシーを作成すると、Firewall Manager は、指定した関連付けの優先順位を使用して、範囲内の VPC とアカウントのルールグループの関連付けを作成します。個々のアカウントマネージャーは、最初の関連付けと最後の関連付けの間にルールグループの関連付けを追加できますが、お客様がここで定義する関連付けを変更することはできません。詳細については、「Firewall Manager の Amazon Route 53 Resolver DNS Firewall ポリシーを使用する」を参照してください。
9. [Next] (次へ) を選択します。
10. [AWS アカウント this policy applies to] (このポリシーが適用される) で、次のようにオプションを選択します。

    - 組織内のすべてのアカウントにポリシーを適用する場合は、デフォルトの選択のままにし、AWS 組織内のすべてのアカウントを含めます。
    - ポリシーを特定の AWS Organizations 組織単位 (OUs) にある特定のアカウントにのみ適用する場合は、指定されたアカウントと組織単位のみを含めるを選択し、含めるアカウントと

OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。

- 特定のアカウントまたは AWS Organizations 組織単位 (OUs) を除くすべてのアカウントにポリシーを適用する場合は、指定されたアカウントと組織単位を除外し、その他をすべて含めてから、除外するアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。

選択できるオプションは 1 つのみです。

ポリシーを適用すると、Firewall Manager は新しいアカウントを設定と照合して自動的に評価します。例えば、特定のアカウントのみを含めると、Firewall Manager は新しいアカウントにポリシーを適用しません。別の例として、OU を含めた場合、OU またはその子である OU にアカウントを追加すると、Firewall Manager は新しいアカウントにポリシーを自動的に適用します。

11. DNS Firewall ポリシーの [Resource type] (リソースタイプ) は [VPC] です。
12. [リソース] では、指定したタグでリソースを含めるか除外するかによって、タグ付けを使用してポリシーの範囲を絞り込むことができます。包含または除外は使用できますが、両方を使用することはできません。ポリシーの範囲を定義するタグの詳細については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

    リソースタグには NULL 以外の値のみを含めることができます。タグの値を省略すると、Firewall Manager は空の文字列値 "" でタグを保存します。リソースタグは、同じキーと値を持つタグのみと一致します。
13. [次へ] を選択します。
14. [ポリシータグ] で、Firewall Manager ポリシーリソースに必要な識別タグを追加します。タグの詳細については、「タグエディタの使用」を参照してください。
15. [次へ] を選択します。
16. 新しいポリシー設定を確認し、調整が必要なページに戻ります。

    ポリシーが完成したら、[ポリシーの作成] を選択します。[AWS Firewall Manager ポリシー] ペインにポリシーが一覧表示されます。アカウントのヘッダーの下に [保留中] と表示され、[自動修復] のステータスが示されます。ポリシーの作成には数分かかることがあります。[Pending] (保留中) ステータスがアカウント数に置き換えられたら、ポリシー名を選択して、アカウントとリソースの準拠ステータスを調べることができます。詳細については、「AWS Firewall Manager ポリシーのコンプライアンス情報の表示」を参照してください。

Palo Alto Networks Cloud NGFW の AWS Firewall Manager ポリシーの作成

Palo Alto Networks Cloud Next Generation Firewall (Palo Alto Networks Cloud NGFW) の Firewall Manager ポリシーでは、Firewall Manager を使用して Palo Alto Networks Cloud NGFW リソースをデプロイし、すべての AWS アカウントで NGFW ルールスタックを一元的に管理します。

Firewall Manager Palo Alto Networks Cloud NGFW ポリシーの詳細については、「Palo Alto Networks Cloud NGFW ポリシーを Firewall Manager で使用する」を参照してください。Firewall Manager 用に Palo Alto Networks Cloud NGFW を設定および管理する方法については、Palo Alto Networks Palo Alto Networks Cloud NGFW on AWS のドキュメントを参照してください。

前提条件

AWS Firewall Managerのアカウントを準備するには、いくつかの必須のステップがあります。それらのステップは、AWS Firewall Manager 前提条件 で説明されています。次のステップに進む前に、すべての前提条件を満たしてください。

Palo Alto Networks Cloud NGFW の Firewall Manager ポリシーを作成するには (コンソール)

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
3. [Create policy] (ポリシーの作成) を選択します。
4. [Policy type] (ポリシータイプ) で、[Palo Alto Networks Cloud NGFW] を選択します。 AWS Marketplace で Palo Alto Networks Cloud NGFW サービスをまだサブスクライブしていない場合は、まずサブスクライブする必要があります。 AWS Marketplace でサブスクライブするには、View AWS Marketplace の詳細を選択します。
5. [Deployment model] (デプロイモデル) で、[Distributed model] (分散モデル) または [Centralized model] (集約型モデル) のいずれかを選択します。デプロイモデルによって、Firewall Manager がポリシーのエンドポイントを管理する方法が決まります。分散モデルでは、Firewall Manager

は、ポリシーの範囲内の各 VPC にファイアウォールエンドポイントを維持します。集約型モデルでは、Firewall Manager は検査 VPC に単一のエンドポイントを維持します。

6. リージョンで、 を選択します AWS リージョン。複数のリージョンのリソースを保護するには、各リージョンに別々の ポリシーを作成する必要があります。
7. [Next] (次へ) を選択します。
8. [Policy name] (ポリシー名) で、わかりやすい名前を入力します。
9. ポリシー設定で、このポリシーに関連付ける Palo Alto Networks Cloud NGFW ファイアウォールポリシーを選択します。Palo Alto Networks Cloud NGFW ファイアウォールポリシーの一覧には、Palo Alto Networks Cloud NGFW テナントに関連付けられているすべての Cloud NGFW ファイアウォールポリシーが含まれています。Palo Alto Networks Cloud NGFW ファイアウォールポリシーの作成と管理の詳細については、「Palo Alto Networks Cloud NGFW for deployment guide」の「Deploy Palo Alto Networks Cloud NGFW for AWSAWS Firewall Manager」トピックを参照してください。 AWS
10. [Palo Alto Networks Cloud NGFW logging ログ記録 - 選択可能]で、オプションで、ポリシーに関してログ記録する Cloud NGFW ログタイプを選択します。Palo Alto Networks Cloud NGFW ログタイプの詳細については、「Palo Alto Networks Cloud NGFW for deployment guide」の「Configure Logging AWS for Palo Alto Networks Cloud NGFW on」を参照してください。 AWS

    [log destination] (ログの宛先) で、Firewall Manager がログを書き込む場合を指定します。
11. [Next] (次へ) を選択します。
12. [Configure third-party firewall endpoint] (サードパーティーのファイアウォールエンドポイントを設定) で、ファイアウォールエンドポイントの作成に分散デプロイモデルと集約型デプロイモデルのいずれを使用しているかに応じて、次のいずれかを実行します。

    - このポリシーに分散デプロイモデルを使用している場合は、[Availability Zones] (アベイラビリティーゾーン) で、ファイアウォールエンドポイントを作成するアベイラビリティーゾーンを選択します。アベイラビリティーゾーンは、[Availability Zone name] (アベイラビリティーゾーン名) または [Availability Zone ID] (アベイラビリティーゾーン ID) で選択できます。
    - このポリシーに集約型デプロイモデルを使用している場合は、[Inspection VPC configuration] (検査 VPC 設定) の [AWS Firewall Manager endpoint configuration] (エンドポイント設定) で、検査 VPC の所有者の AWS アカウント ID と検査 VPC の VPC ID を入力します。
        - [Availability Zones] (アベイラビリティーゾーン) で、ファイアウォールエンドポイントを作成するアベイラビリティーゾーンを選択します。アベイラビリティーゾーンは、[Availability

Zone name] (アベイラビリティーゾーン名) または [Availability Zone ID] (アベイラビリティーゾーン ID) で選択できます。

13. Firewall Manager が VPC のファイアウォールサブネットに使用する CIDR ブロックを指定する場合、そのすべては /28 CIDR ブロックである必要があります。1 行に 1 つのブロックを入力します。これらを省略すると、Firewall Manager は、VPC で使用可能な IP アドレスから選択します。

> **Note**
>
> 自動修復は AWS Firewall Manager Network Firewall ポリシーに対して自動的に行われるため、ここで自動修復を選択しないオプションは表示されません。

14. [次へ] を選択します。
15. [Policy scope] (ポリシーの範囲) の [AWS アカウント this policy applies to] (このポリシーが適用される) で、次のようにオプションを選択します。

    - 組織内のすべてのアカウントにポリシーを適用する場合は、デフォルトの選択のままにし、AWS 組織内のすべてのアカウントを含めます。
    - ポリシーを特定の AWS Organizations 組織単位 (OUs) にある特定のアカウントにのみ適用する場合は、指定されたアカウントと組織単位のみを含めるを選択し、含めるアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。
    - 特定のアカウントまたは AWS Organizations 組織単位 (OUs) を除くすべてのアカウントにポリシーを適用する場合は、指定されたアカウントと組織単位を除外し、その他をすべて含めてから、除外するアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。

    選択できるオプションは 1 つのみです。

    ポリシーを適用すると、Firewall Manager は新しいアカウントを設定と照合して自動的に評価します。例えば、特定のアカウントのみを含めると、Firewall Manager は新しいアカウントにポリシーを適用しません。別の例として、OU を含めた場合、OU またはその子である OU にアカウントを追加すると、Firewall Manager は新しいアカウントにポリシーを自動的に適用します。
16. Network Firewall ポリシーの [Resource type] (リソースタイプ) は [VPC] です。

17. [リソース] では、指定したタグでリソースを含めるか除外するかによって、タグ付けを使用してポリシーの範囲を絞り込むことができます。包含または除外は使用できますが、両方を使用することはできません。ポリシーの範囲を定義するタグの詳細については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

    リソースタグには NULL 以外の値のみを含めることができます。タグの値を省略すると、Firewall Manager は空の文字列値 "" でタグを保存します。リソースタグは、同じキーと値を持つタグのみと一致します。

18. [Grant cross-account access] (クロスアカウントアクセスを付与) で、[Download CloudFormation template] (テンプレートをダウンロード) を選択します。これにより、CloudFormation スタックの作成に使用できる CloudFormation テンプレートがダウンロードされます。このスタックは、Palo Alto Networks Cloud NGFW リソースを管理するためのクロスアカウントアクセス許可を Firewall Manager に付与する AWS Identity and Access Management ロールを作成します。スタックの詳細については、「CloudFormation ユーザーガイド」の「StackSets の操作」を参照してください。
19. [次へ] を選択します。
20. [ポリシータグ] で、Firewall Manager ポリシーリソースに必要な識別タグを追加します。タグの詳細については、「タグエディタの使用」を参照してください。
21. [次へ] を選択します。
22. 新しいポリシー設定を確認し、調整が必要なページに戻ります。

    ポリシーが完成したら、[ポリシーの作成] を選択します。[AWS Firewall Manager ポリシー] ペインにポリシーが一覧表示されます。アカウントのヘッダーの下に [保留中] と表示され、[自動修復] のステータスが示されます。ポリシーの作成には数分かかることがあります。[Pending] (保留中) ステータスがアカウント数に置き換えられたら、ポリシー名を選択して、アカウントとリソースの準拠ステータスを調べることができます。詳細については、「AWS Firewall Manager ポリシーのコンプライアンス情報の表示」を参照してください。

サービスとしての Fortigate Cloud Native Firewall (CNF) の AWS Firewall Manager ポリシーの作成

Fortigate CNF の Firewall Manager ポリシーを使用すると、Firewall Manager を使用して、すべての AWS アカウントで Fortigate CNF リソースをデプロイおよび管理できます。

Firewall Manager Fortigate CNF ポリシーについては、「Firewall Manager に Fortigate Cloud Native Firewall (CNF) as a Service ポリシーを使用する」を参照してください。Fortigate CNF を Firewall

Manager で使用するための設定について詳しくは、「Fortinet のドキュメント」を参照してください。

前提条件

AWS Firewall Managerのアカウントを準備するには、いくつかの必須のステップがあります。それらのステップは、AWS Firewall Manager 前提条件 で説明されています。次のステップに進む前に、すべての前提条件を満たしてください。

Fortigate CNF の Firewall Manager ポリシーを作成するには (コンソール)

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
3. [Create policy] (ポリシーの作成) を選択します。
4. [Policy type] (ポリシータイプ) には、[Fortigate Cloud Native Firewall (CNF) as a Service] (サービスとしての Fortigate Cloud ネイティブファイアウォール (CNF)) を選択してください。AWS Marketplace で Fortigate CNF サービスをまだサブスクライブしていない場合は、まずサブスクライブする必要があります。 AWS Marketplace でサブスクライブするには、View AWS Marketplace の詳細を選択します。
5. [Deployment model] (デプロイモデル) で、[Distributed model] (分散モデル) または [Centralized model] (集約型モデル) のいずれかを選択します。デプロイモデルによって、Firewall Manager がポリシーのエンドポイントを管理する方法が決まります。分散モデルでは、Firewall Manager は、ポリシーの範囲内の各 VPC にファイアウォールエンドポイントを維持します。集約型モデルでは、Firewall Manager は検査 VPC に単一のエンドポイントを維持します。
6. リージョンで、 を選択します AWS リージョン。複数のリージョンのリソースを保護するには、各リージョンに別々の ポリシーを作成する必要があります。
7. [Next] (次へ) を選択します。
8. [Policy name] (ポリシー名) で、わかりやすい名前を入力します。

9. ポリシー設定で、このポリシーに関連付ける Fortigate CNF ファイアウォールポリシーを選択します。Fortigate CNF ファイアウォールポリシーのリストには、Fortigate CNF テナントに関連付けられているすべての CNF ファイアウォールポリシーが含まれています。Fortigate CNF テナントの作成と管理については、「Fortinet のドキュメント」を参照してください。
10. [次へ] を選択します。
11. [Configure third-party firewall endpoint] (サードパーティーのファイアウォールエンドポイントを設定) で、ファイアウォールエンドポイントの作成に分散デプロイモデルと集約型デプロイモデルのいずれを使用しているかに応じて、次のいずれかを実行します。

    - このポリシーに分散デプロイモデルを使用している場合は、[Availability Zones] (アベイラビリティーゾーン) で、ファイアウォールエンドポイントを作成するアベイラビリティーゾーンを選択します。アベイラビリティーゾーンは、[Availability Zone name] (アベイラビリティーゾーン名) または [Availability Zone ID] (アベイラビリティーゾーン ID) で選択できます。
    - このポリシーに集約型デプロイモデルを使用している場合は、[Inspection VPC configuration] (検査 VPC 設定) の [AWS Firewall Manager endpoint configuration] (エンドポイント設定) で、検査 VPC の所有者の AWS アカウント ID と検査 VPC の VPC ID を入力します。
        - [Availability Zones] (アベイラビリティーゾーン) で、ファイアウォールエンドポイントを作成するアベイラビリティーゾーンを選択します。アベイラビリティーゾーンは、[Availability Zone name] (アベイラビリティーゾーン名) または [Availability Zone ID] (アベイラビリティーゾーン ID) で選択できます。
12. Firewall Manager が VPC のファイアウォールサブネットに使用する CIDR ブロックを指定する場合、そのすべては /28 CIDR ブロックである必要があります。1 行に 1 つのブロックを入力します。これらを省略すると、Firewall Manager は、VPC で使用可能な IP アドレスから選択します。

    > **Note**
    >
    > 自動修復は AWS Firewall Manager Network Firewall ポリシーに対して自動的に行われるため、ここで自動修復を選択しないオプションは表示されません。

13. [次へ] を選択します。
14. [Policy scope] (ポリシーの範囲) の [AWS アカウント this policy applies to] (このポリシーが適用される) で、次のようにオプションを選択します。

    - 組織内のすべてのアカウントにポリシーを適用する場合は、デフォルトの選択のままにし、AWS 組織内のすべてのアカウントを含めます。

- ポリシーを特定の AWS Organizations 組織単位 (OUs) にある特定のアカウントにのみ適用する場合は、指定されたアカウントと組織単位のみを含めるを選択し、含めるアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。
- 特定のアカウントまたは AWS Organizations 組織単位 (OUs) を除くすべてのアカウントにポリシーを適用する場合は、指定されたアカウントと組織単位を除外し、その他をすべて含めてから、除外するアカウントと OUs を追加します。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。

選択できるオプションは 1 つのみです。

ポリシーを適用すると、Firewall Manager は新しいアカウントを設定と照合して自動的に評価します。例えば、特定のアカウントのみを含めると、Firewall Manager は新しいアカウントにポリシーを適用しません。別の例として、OU を含めた場合、OU またはその子である OU にアカウントを追加すると、Firewall Manager は新しいアカウントにポリシーを自動的に適用します。

15. Network Firewall ポリシーの [Resource type] (リソースタイプ) は [VPC] です。
16. [リソース] では、指定したタグでリソースを含めるか除外するかによって、タグ付けを使用してポリシーの範囲を絞り込むことができます。包含または除外は使用できますが、両方を使用することはできません。ポリシーの範囲を定義するタグの詳細については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

    リソースタグには NULL 以外の値のみを含めることができます。タグの値を省略すると、Firewall Manager は空の文字列値 "" でタグを保存します。リソースタグは、同じキーと値を持つタグのみと一致します。
17. [Grant cross-account access] (クロスアカウントアクセスを付与) で、[Download CloudFormation template] (テンプレートをダウンロード) を選択します。これにより、CloudFormation スタックの作成に使用できる CloudFormation テンプレートがダウンロードされます。このスタックは、Fortigate CNF リソースを管理するためのクロスアカウントアクセス許可を Firewall Manager に付与する AWS Identity and Access Management ロールを作成します。スタックの詳細については、「CloudFormation ユーザーガイド」の「StackSets の操作」を参照してください。スタックを作成するには、Fortigate CNF ポータルのアカウント ID が必要です。
18. [次へ] を選択します。

19. [ポリシータグ] で、Firewall Manager ポリシーリソースに必要な識別タグを追加します。タグの詳細については、「タグエディタの使用」を参照してください。
20. [次へ] を選択します。
21. 新しいポリシー設定を確認し、調整が必要なページに戻ります。

    ポリシーが完成したら、[ポリシーの作成] を選択します。[AWS Firewall Manager ポリシー] ペインにポリシーが一覧表示されます。アカウントのヘッダーの下に [保留中] と表示され、[自動修復] のステータスが示されます。ポリシーの作成には数分かかることがあります。[Pending] (保留中) ステータスがアカウント数に置き換えられたら、ポリシー名を選択して、アカウントとリソースの準拠ステータスを調べることができます。詳細については、「AWS Firewall Manager ポリシーのコンプライアンス情報の表示」を参照してください。

AWS Firewall Manager ポリシーの削除

次のステップを実行して、Firewall Manager ポリシーを削除できます。

ポリシーを削除するには (コンソール)

1. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
2. 削除するポリシーの横にあるオプションを選択します。
3. [Delete] (削除) を選択します。

> **Note**
>
> Firewall Manager 共通セキュリティグループポリシーを削除する場合、ポリシーのレプリカセキュリティグループを削除するには、ポリシーによって作成されたリソースをクリーンアップするオプションを選択します。それ以外の場合、プライマリが削除されても、レプリカはそのまま残り、各 Amazon VPC インスタンスで手動管理が必要です。

> **Important**
>
> Firewall Manager Shield Advanced ポリシーを削除すると、ポリシーは削除されますが、アカウントは Shield Advanced にサブスクライブされたままとなります。

AWS Firewall Manager ポリシースコープの使用

このページでは、Firewall Manager ポリシーの範囲とその仕組みについて説明します。

ポリシーの範囲は、ポリシーが適用される場所を定義するものです。一元管理ポリシーは、以下に適用できます。

- AWS Organizationsの組織内のすべてのアカウントとリソース。
- AWS Organizationsの組織内のアカウントとリソースのサブセット。

ポリシーの範囲の設定方法については、「AWS Firewall Manager ポリシーの作成」を参照してください。

のポリシースコープオプション AWS Firewall Manager

組織に新しいアカウントまたはリソースを追加すると、Firewall Manager は、各ポリシーの設定に対して自動的に評価し、これらの設定に基づいてポリシーを適用します。例えば、指定されたリストのアカウント番号を除くすべてのアカウントにポリシーを適用するように選択できます。リソースタグを使用してポリシーの範囲を定義することもできます。リスト内のすべてのタグを持つリソースを除外または含めることで、ポリシーを適用するように選択できます。または、リストで指定されたタグのいずれかを持つリソースにのみポリシーを適用することもできます。

AWS アカウント 範囲内

ポリシーの AWS アカウント 影響を受ける を定義するために指定する設定によって、ポリシーを適用する AWS 組織内のアカウントが決まります。次のいずれかの方法でポリシーを適用できます。

- 組織のすべてのアカウントに適用
- 含めたアカウント番号と AWS Organizations の組織単位 (OU) の特定のリストにのみ適用
- 除外したアカウント番号と AWS Organizations の組織単位 (OU) の特定のリストを除くすべてに適用

詳細については AWS Organizations、AWS Organizations 「 ユーザーガイド」を参照してください。

範囲内のリソース

範囲内のアカウントの設定と同様に、リソースに指定した設定によって、ポリシーを適用する範囲内のリソースタイプが決まります。次のいずれかを選択できます。

- すべてのリソース
- 指定したすべてのタグを持つリソース
- 指定したすべてのタグを持つリソースを除くすべてのリソース
- 指定したタグのいずれかを持つリソースのみ
- 指定したタグのいずれかを持つリソースのみを除くすべてのリソース

NULL 以外の値を持つリソースタグのみを指定できます。値に何も指定しない場合、Firewall Manager は空の文字列値 "" でタグを保存します。リソースタグは、同じキーと値を持つタグのみと一致します。

リソースのタグ付けの詳細については、「タグエディタの使用」を参照してください。

でのポリシースコープ管理 AWS Firewall Manager

ポリシーが設定されると、Firewall Manager はポリシーを継続的に管理し、ポリシーの範囲に従って、追加される新しい AWS アカウント およびリソースに適用します。

Firewall Manager が AWS アカウント および リソースを管理する方法

何らかの理由でアカウントまたはリソースがスコープ外になった場合、ポリシースコープを離れるリソースから保護を自動的に削除チェックボックスをオンにしない限り、 AWS Firewall Manager は保護を自動的に削除したり、Firewall Manager が管理するリソースを削除したりしません。

> **Note**
>
> オプション ポリシーの範囲を離れるリソースから自動的に保護を削除すると、 AWS Shield Advanced または AWS WAF Classic ポリシーでは使用できません。

このチェックボックスをオンにすると、 AWS Firewall Manager は、Firewall Manager がアカウントがポリシーの範囲を離れるときに管理するリソースを自動的にクリーンアップするように に指示します。例えば、カスタマーリソースがポリシーの範囲から外れた場合、Firewall Manager は、Firewall Manager で管理するウェブ ACL と保護されたカスタマーリソースとの関連付けを解除します。

カスタマーリソースがポリシーの範囲外になったときに保護から削除する必要があるリソースを決定するために、Firewall Manager は次のガイドラインに従います。

- デフォルトの動作

- 関連付けられた AWS Config マネージドルールが削除されます。この動作は、チェックボックスとは無関係です。
- リソースを含まない関連する AWS WAF ウェブアクセスコントロールリスト (ウェブ ACLs) はすべて削除されます。この動作は、チェックボックスとは無関係です。
- 範囲外となった保護されたリソースは、関連付けられ、保護されたままになります。例えば、ウェブ ACL に関連付けられた API Gateway からの Application Load Balancer または API は、ウェブ ACL に関連付けられたままになり、保護は維持されます。

- [Automatically remove protections from resources that leave the policy scope] (ポリシーの範囲を外れるリソースから保護を自動的に削除) のチェックボックスをオンにすると、次のようになります。
  - 関連付けられた AWS Config マネージドルールが削除されます。この動作は、チェックボックスとは無関係です。
  - リソースを含まない関連する AWS WAF ウェブアクセスコントロールリスト (ウェブ ACLs) はすべて削除されます。この動作は、チェックボックスとは無関係です。
  - 範囲外となった保護されたリソースは、ポリシーの範囲から外れると、自動的に関連付けが解除され、Firewall Manager 保護から削除されます。例えば、セキュリティグループポリシーの場合、Elastic Inference アクセラレーターまたは Amazon EC2 インスタンスは、レプリケートされたセキュリティグループがポリシーの範囲外になると、自動的に関連付けが解除されます。レプリケートされたセキュリティグループとそのリソースは、自動的に保護から削除されます。
  - Firewall Manager は、メンバーアカウントがスコープを離れたとき、またはポリシーが削除されたときに、リソースクリーンアップオプションの値に関係なくログ記録設定を削除します。

Firewall Manager での AWS WAF ポリシーの使用

このセクションでは、Firewall Manager で AWS WAF ポリシーを使用する方法について説明します。Firewall Manager AWS WAF ポリシーでは、ポリシー範囲内のすべてのリソースを保護するために使用する AWS WAF ルールグループを指定します。ポリシーを適用すると、Firewall Manager は、指定されたルールグループやその他のポリシー設定を使用して、対象範囲内のリソースのウェブ ACL の管理を開始します。

ポリシーを設定して、対象範囲内のリソースのすべての新しいウェブ ACL を作成および管理し、既に使用されているウェブ ACL を置き換えることができます。または、対象範囲内のリソースに既に関連付けられているウェブ ACL を保持するようにポリシーを設定し、ポリシーで使用できるように後付けすることもできます。この 2 番目のオプションでは、Firewall Manager は、ウェブ ACL とまだ関連していないリソースに対してのみ新しいウェブ ACL を作成します。

作成方法に関係なく、Firewall Manager が管理するウェブ ACL では、Firewall Manager ポリシーで定義したルールグループに加えて、各アカウントが独自のルールとルールグループを管理できます。

Firewall Manager AWS WAF ポリシーを作成する手順については、「」を参照してくださいの AWS Firewall Manager ポリシーの作成 AWS WAF。

AWS WAF ポリシーのルールグループ管理

Firewall Manager AWS WAF ポリシーによって管理されるウェブ ACLs には、3 つのルールセットが含まれています。これらのセットにより、ウェブ ACL 内のルールおよびルールグループの優先順位は上がります。

- Firewall Manager AWS WAF ポリシーで定義した最初のルールグループは、最初にこれらのルールグループ AWS WAF を評価します。
- アカウントマネージャーがウェブ ACL で定義したルールおよびルールグループ。 AWS WAF は次にアカウントマネージドルールまたはルールグループを評価します。
- Firewall Manager AWS WAF ポリシーで定義した最後のルールグループ。 は、これらのルールグループを最後に AWS WAF 評価します。

これらのルールの各セット内で、 はセット内の優先順位設定に従って、通常どおりルールとルールグループ AWS WAF を評価します。

ポリシーの最初と最後のルールグループセットでは、個別のルールではなく、ルールグループのみを追加できます。マネージドルールグループを使用できます。マネージドルールグループは、 AWS マネージドルールと AWS Marketplace 販売者が作成および維持します。独自のルールグループを管理して使用することもできます。これらのすべてのオプションの詳細については、「AWS WAF ルールグループ」を参照してください。

独自のルールグループを使用する場合は、Firewall Manager AWS WAF ポリシーを作成する前にそれらのグループを作成します。ガイダンスについては、「独自のルールグループの管理」を参照してください。個々のカスタムルールを使用するには、独自のルールグループを定義し、その中にルールを定義してから、ポリシーでそのルールグループを使用する必要があります。

Firewall Manager で管理する最初と最後の AWS WAF ルールグループの名前は`POSTFMManaged-`、それぞれ `PREFMManaged-`または で始まり、その後に Firewall Manager ポリシー名とルールグループ作成タイムスタンプが UTC ミリ秒単位で続きます。例えば、`PREFMManaged-MyWAFPolicyName-1621880555123`。

がウェブリクエスト AWS WAF を評価する方法については、「」を参照してくださいのルールとルールグループで保護パック (ウェブ ACLs) を使用する AWS WAF。

Firewall Manager は、 AWS WAF ポリシーのために定義したルールグループのサンプリングと Amazon CloudWatch メトリクスを有効にします。

個々のアカウント所有者は、ポリシーのマネージドウェブ ACL に追加するルールまたはルールグループのメトリクスとサンプリング設定を完全に制御できます。

> **Note**
>
> メンバーアカウントに AWS WAF マーケットプレイスルールグループへのサブスクリプションがない場合、Firewall Manager はそのアカウントにカスタムルールグループまたはマネージドルールグループを伝播できません。

AWS WAF ポリシーのウェブ ACL 管理

Firewall Manager は、設定と一般的なポリシー管理に従って、対象範囲内のリソースのウェブ ACL を作成および管理します。

> **Note**
>
> 別の Firewall Manager Shield ポリシーによって高度な自動アプリケーションレイヤー DDoS 緩和が設定されているリソースが、その Firewall Manager Shield AWS WAF ポリシーによってリソースのウェブ ACL が作成された ポリシーの範囲内にある場合、Firewall Manager は AWS WAF ポリシー保護をリソースに適用できず、リソースが非準拠としてマークされます。
> 顧客が顧客所有のウェブ ACL をリソースに手動で関連付けた場合でも、Firewall Manager AWS WAF ポリシーはその顧客ウェブ ACL を Firewall Manager AWS WAF ポリシーウェブ ACL で上書きします。

関連付けられていないウェブ ACL 設定の管理

Firewall Manager が、どのリソースでもウェブ ACL を使用しない場合に、アカウントのウェブ ACL を管理する方法を指定するポリシー設定。関連付けられていないウェブ ACL の管理を有効にした場合、Firewall Manager は、少なくとも 1 つのリソースがウェブ ACL を使用する場合のみ、ポリ

シー範囲内のアカウントにウェブ ACL を作成します。このオプションを有効にしない場合、Firewall Manager は、ウェブ ACL を使用するかどうかに関係なく、各アカウントにウェブ ACL が自動的に付与されるようにします。

これが有効にした場合、アカウントがポリシーの対象になると、少なくとも 1 つのリソースがウェブ ACL を使用する場合のみ、Firewall Manager はアカウントにウェブ ACL を自動的に作成します。

また、関連付けられていないウェブ ACL の管理を有効にすると、ポリシーの作成中に、Firewall Manager はアカウント内の関連付けられていないウェブ ACL に 1 回だけクリーンアップを実行します。このクリーンアップ中に、Firewall Manager は、作成後に変更したウェブ ACL をすべてスキップします。例えば、ルールグループをウェブ ACL に追加したり、その設定を変更したりした場合などです。このクリーンアッププロセスには、数時間かかることがあります。Firewall Manager がウェブ ACL を作成した後、リソースがポリシー範囲から外れた場合、Firewall Manager はそのリソースとウェブ ACL の関連付けを解除しますが、関連付けられていないウェブ ACL はクリーンアップしません。Firewall Manager は、関連付けられていないウェブ ACL の管理を、ポリシーで初めて有効にした場合のみ、関連付けられていないウェブ ACL をクリーンアップします。

API では、この設定は「SecurityServicePolicyData」データタイプにある `optimizeUnassociatedWebACL` です。例: `\"optimizeUnassociatedWebACL\":false`

ウェブ ACL ソース設定: すべて新規作成または既存のもの改良を行いますか？

Firewall Manager が対象範囲内のリソースに関連付けられている既存のウェブ ACL に対して行うことを指定するポリシー設定。

デフォルトでは、Firewall Manager は対象範囲内のリソースのすべての新しいウェブ ACL を作成します。Firewall Manager は、後付けにより、既に使用されている既存のウェブ ACL を使用し、まだ関連付けられていないリソースに対してのみ新しいウェブ ACL を作成します。

ポリシーが改良用に設定されている場合、範囲内のリソースに関連付けられているすべてのウェブ ACL は、レトロフィットまたは非準拠とマークされます。

Firewall Manager は、以下の要件を満たす場合にのみウェブ ACL を改良します。

- ウェブ ACL はカスタマーアカウントによって所有されています。
- ウェブ ACL は、範囲内のリソースにのみ関連付けられます。

> **Tip**
>
> 改良のために AWS WAF ポリシーを設定する前に、ポリシーの対象範囲内のリソースに関連付けられているウェブ ACLs がout-of-scopeリソースに関連付けられていないことを確認してください。

> **Tip**
>
> ウェブ ACL を削除するには、最初にすべてのリソースをウェブ ACL から分離します。範囲外のリソースとの関連付けが原因でウェブ ACL が準拠していない場合、まずウェブ ACL から関連付けを解除せずに範囲外のリソースを削除すると、ウェブ ACL が準拠し、Firewall Manager は修復を通じてウェブ ACL を改良できますが、この状況での修復は最大 24 時間遅延する可能性があります。

コンプライアンス違反の詳細へのアクセスについては、AWS Firewall Manager ポリシーのコンプライアンス情報の表示 を参照してください。

ウェブ ACL を改良できる場合、Firewall Manager はそれを次のように変更します:

- Firewall Manager は、ウェブ ACL の既存のルールの前に AWS WAF ポリシーの最初のルールグループを挿入し、最後に AWS WAF ポリシーの最後のルールグループを追加します。マネージドルールグループの詳細については、AWS WAF ポリシーのルールグループ管理 を参照してください。
- ポリシーにログ記録設定がある場合、Firewall Manager は、ウェブ ACL がログ記録用にまだ設定されていない場合にのみ、それをウェブ ACL に追加します。ウェブ ACL にアカウントによってログ記録が設定されている場合、Firewall Manager は、ポリシーのログ記録設定の改良中とその後の更新時の両方でそのログ記録を保持します。
- Firewall Manager は、他のウェブ ACL プロパティを検証または設定しません。例えば、Firewall Manager はウェブ ACL のデフォルトアクション、カスタムリクエストヘッダー、CAPTCHA または Challenge の設定、トークンドメインリストを変更しません。Firewall Manager は、Firewall Manager が作成するウェブ ACL に対してのみ、これらの他のプロパティを設定します。

Firewall Manager が既存の関連付けられているすべてのウェブ ACL をレトロフィットした後、ウェブ ACL を持たない範囲内のリソースについて、Firewall Manager はデフォルトのポリシー動作に

従ってリソースを処理します。が保護 AWS WAF できるリソースである場合、Firewall Manager はそのリソースに Firewall Manager ウェブ ACL を作成して関連付けます。

API では、ウェブ ACL ソース設定は「SecurityServicePolicyData」データタイプにある webACLSource です。例: \"webACLSource\":\"RETROFIT_EXISTING\"

サンプリングと CloudWatch メトリクス

AWS Firewall Manager は、 AWS WAF ポリシー用に作成するウェブ ACLs とルールグループのサンプリングと Amazon CloudWatch メトリクスを有効にします。

ウェブ ACL の命名

Firewall Manager が作成するウェブ ACL は、 AWS WAF ポリシーにちなんで という名前が付けられますFMManagedWebACLV2-*policy name*-*timestamp*。タイムスタンプは UTC (ミリ秒) です。例えば、FMManagedWebACLV2-MyWAFPolicyName-1621880374078。

Firewall Manager が改良するウェブ ACL には、作成時にカスタマアカウントが指定した名前があります。ウェブ ACL 名は作成後に変更できません。

> **Note**
>
> 高度な自動アプリケーションレイヤー DDoS 緩和で設定されたリソースが AWS WAF ポリシーの対象である場合、Firewall Manager は AWS WAF ポリシーによって作成されたウェブ ACL をリソースに関連付けることができません。

AWS WAF ポリシーのログ記録

AWS WAF ポリシーの集中ログ記録を有効にして、組織内のウェブ ACL によって分析されるトラフィックに関する詳細情報を取得できます。 は、このオプションを AWS WAF Classic ではなく AWS WAFV2で AWS Firewall Manager サポートします。

ログの情報には、保護された AWS リソースからリクエスト AWS WAF を受信した時間、リクエストに関する詳細情報、および各リクエストがすべての対象アカウントから一致したルールのアクションが含まれます。 AWS WAF ログ記録の詳細については、「 AWS WAF デベロッパーガイドログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」の「」を参照してください。

ログは、Amazon Data Firehose データストリーム、または Amazon Simple Storage Service (S3) バケットに送信することができます。各送信先タイプには、Firewall Manager が範囲内のリソースとア

カウント全体の AWS WAF ログ記録を管理できるようにするために追加の設定が必要です。詳細については次のセクションで説明します。

ポリシーでウェブ ACL のレトロフィットが有効になっている場合、Firewall Manager は既存のウェブ ACL に配置されているログ記録設定を上書きしません。後付けの詳細については、AWS WAF ポリシーのウェブ ACL 管理 のウェブ ACL ソース設定情報を参照してください。

> **Note**
>
> Firewall Manager ポリシーのログ記録は、Firewall Manager インターフェイスを介してのみ変更または無効にします。 AWS WAF を使用して Firewall Manager によって管理されるウェブ ACL のログ記録設定を更新または削除する場合、Firewall Manager は変更を自動的に検出しません。を使用した場合は AWS WAF、 AWS WAF ポリシーのルールを再評価することで、Firewall Manager ポリシーの更新を手動で求めることができます AWS Config。これを行うには、 AWS Config コンソールで Firewall Manager ポリシーの AWS Config ルールを見つけ、再評価アクションを選択します。

トピック

- ログ記録の送信先
- Firewall Manager で AWS WAF ポリシーのログ記録を有効にする
- Firewall Manager での AWS WAF ポリシーのログ記録の無効化

ログ記録の送信先

このセクションでは、 AWS WAF ポリシーログの送信先として選択できるログ記録先について説明します。各セクションでは、送信先の種類のログを設定するためのガイダンスと、送信先の種類に固有の動作に関する情報を提供します。ログ記録先を設定したら、Firewall Manager AWS WAF ポリシーにその仕様を指定して、ログ記録を開始できます。

Firewall Manager では、ログ記録設定を作成した後でログの失敗を可視化することはできません。ログ配信が意図したとおりに機能していることを確認するのはユーザーの責任になります。

Firewall Manager は、組織のメンバーアカウントの既存のログ記録設定を変更しません。

トピック

- Amazon Data Firehose データストリーム
- Amazon Simple Storage Service バケット

Amazon Data Firehose データストリーム

このトピックでは、ウェブ ACL トラフィックログの Amazon Data Firehose データストリームへの送信に関する情報を提供します。

Amazon Data Firehose のログ記録を有効化していると、Firewall Manager は、ストレージを出力先に設定した Amazon Data Firehose に対し、ポリシーのウェブ ACL からログを送信します。ログ記録を有効にすると、 は Kinesis Data Firehose の HTTPS エンドポイントを介して、設定された各ウェブ ACL のログを設定されたストレージ宛先に AWS WAF 配信します。それを使用する前に、配信ストリームをテストして、組織のログに対応するのに十分なスループットがあることを確認します。Amazon Kinesis Data Firehose を作成し、保存されているログを確認する方法の詳細については、「What Is Amazon Data Firehose?」を参照してください。

Kinesis によるログ記録を正常に有効化するには、以下の許可が付与されている必要があります。

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

AWS WAF ポリシーで Amazon Data Firehose ログ記録先を設定すると、Firewall Manager は Firewall Manager 管理者アカウントにポリシーのウェブ ACL を次のように作成します。

- Firewall Manager は、アカウントがポリシーの範囲内にあるかどうかにかかわらず、Firewall Manager 管理者アカウントにウェブ ACL を作成します。
- ウェブ ACL でログ記録が有効になり、`FMManagedWebACLV2-Logging`*`policy name`*`-`*`timestamp`* というログ名が付けられます。タイムスタンプは、ウェブ ACL 用にログが有効になった UTC 時間 (ミリ秒) です。例えば、`FMManagedWebACLV2-LoggingMyWAFPolicyName-1621880565180`。ウェブ ACL には、ルールグループおよび関連するリソースはありません。
- ウェブ ACL には、 AWS WAF 料金ガイドラインに従って課金されます。詳細については、「AWS WAF 料金」を参照してください。
- ポリシーを削除すると、Firewall Manager はウェブ ACL を削除します。

サービスにリンクされたロールおよび `iam:CreateServiceLinkedRole` 許可の詳細については、「のサービスにリンクされたロールの使用 AWS WAF」を参照してください。

配信ストリームの作成の詳細については、「Creating an Amazon Data Firehose Delivery Stream」を参照してください。

Amazon Simple Storage Service バケット

このトピックは、ウェブ ACL トラフィックログの Amazon S3 バケットへの送信に関する情報を提供します。

ログ記録の出力先として選択するバケットは、Firewall Manager の管理者アカウントが所有している必要があります。ログ記録用に Amazon S3 バケットを作成する際の要件、およびバケット命名における要件の情報については、「AWS WAF デベロッパーガイド」の「Amazon Simple Storage Service」を参照してください。

結果整合性

Amazon S3 ログ記録先で設定された AWS WAF ポリシーを変更すると、Firewall Manager はバケットポリシーを更新して、ログ記録に必要なアクセス許可を追加します。その際、Firewall Manager は、Amazon Simple Storage Service が採用している、最後の書き込みを優先するセマンティクスとデータ整合性モデルに従います。Firewall Manager コンソールまたは PutPolicy API を使用して、Amazon S3 内の送信先に対して同時に複数のポリシーを更新すると、一部のアクセス許可が保存されない場合があります。Amazon S3 におけるデータ整合性モデルの詳細については、「Amazon Simple Storage Service ユーザーガイド」の「 Amazon S3 のデータ整合性モデル」を参照してください。

Amazon S3 に対しログを発行するためのアクセス許可

AWS WAF ポリシーで Amazon S3 バケットのウェブ ACL トラフィックログ記録を設定するには、次のアクセス許可設定が必要です。Amazon S3 をログ記録の出力先として設定すると、Firewall Manager は、サービスがバケットに対しログを公開することを許可するために、これらのアクセス許可を Amazon S3 バケットに自動的にアタッチします。ログ記録と Firewall Manager リソースへのよりきめ細かいアクセスを管理したい場合は、自分でこれらの許可を設定できます。アクセス許可の管理については、「IAM ユーザーガイド」の「AWS リソースのアクセス管理」を参照してください。 AWS WAF 管理ポリシーの詳細については、「」を参照してくださいAWS の 管理ポリシー AWS WAF。

JSON

```
{
    "Version":"2012-10-17",
```

```
    "Id": "AWSLogDeliveryForFirewallManager",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheckFMS",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::aws-waf-logs-amzn-s3-demo-destination-
bucket-suffix"
        },
        {
            "Sid": "AWSLogDeliveryWriteFMS",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::aws-waf-logs-amzn-s3-demo-destination-
bucket-suffix/policy-id/AWSLogs/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

サービス間での混乱した代理問題を防ぐためには、aws:SourceArn および aws:SourceAccount グローバル条件コンテキストキーを、バケットのポリシーに追加できます。これらのキーを追加する場合は、ログの出力先を設定する際に Firewall Manager により作成されたポリシーを変更します。あるいは、よりきめ細かな制御が必要な場合には、独自のポリシーを作成することができます。これらの条件をログ記録出力先のポリシーに追加した場合、Firewall Manager は、混乱した代理に関する保護の検証またはモニタリングを行いません。混乱した代理問題の詳細については、「IAM ユーザーガイド」の「混乱する代理問題」を参照してください。

sourceAccount および sourceArn のプロパティを追加すると、バケットポリシーのサイズが増加します。sourceAccount および sourceArn プロパティから成る長いリストを追加する場合は、Amazon S3 のバケットポリシーのサイズが上限を超えないように注意してください。

次の例で、 ロールポリシーで aws:SourceArn および aws:SourceAccount のグローバル条件コンテキストを使用して、混乱した代理問題を防止する方法を示します。*member-account-id* を、組織内のメンバーのアカウント ID に置き換えます。

JSON

```
{
   "Version":"2012-10-17",
   "Id":"AWSLogDeliveryForFirewallManager",
   "Statement":[
      {
         "Sid":"AWSLogDeliveryAclCheckFMS",
         "Effect":"Allow",
         "Principal":{
            "Service":"delivery.logs.amazonaws.com"
         },
         "Action":"s3:GetBucketAcl",
         "Resource":"arn:aws:s3:::aws-waf-logs-amzn-s3-demo-destination-bucket-
suffix",
         "Condition":{
            "StringEquals":{
               "aws:SourceAccount":[
               "111122223333",
               "444455556666"
               ]
            },
            "ArnLike":{
               "aws:SourceArn":[
               "arn:aws:logs:*:111122223333:*",
               "arn:aws:logs:*:444455556666:*"
               ]
            }
         }
      },
      {
         "Sid":"AWSLogDeliveryWriteFMS",
         "Effect":"Allow",
         "Principal":{
            "Service":"delivery.logs.amazonaws.com"
         },
         "Action":"s3:PutObject",
```

```
            "Resource":"arn:aws:s3:::aws-waf-logs-amzn-s3-demo-destination-bucket-
suffix/policy-id/AWSLogs/*",
            "Condition":{
               "StringEquals":{
                  "s3:x-amz-acl":"bucket-owner-full-control",
                  "aws:SourceAccount":[
                  "111122223333",
                  "444455556666"
                  ]
               },
               "ArnLike":{
                  "aws:SourceArn":[
                  "arn:aws:logs:*:111122223333:*",
                  "arn:aws:logs:*:444455556666:*"
                  ]
               }
            }
         }
      ]
}
```

Amazon S3 バケットのサーバー側の暗号化

Amazon S3 サーバー側の暗号化を有効にするか、S3 バケットで AWS Key Management Service カスタマーマネージドキーを使用できます。 AWS WAF ログに Amazon S3 バケットでデフォルトの Amazon S3 暗号化を使用する場合は、特別なアクションを実行する必要はありません。ただし、お客様が用意した暗号化キーを使用して保管中の Amazon S3 データを暗号化する場合は、 AWS Key Management Service キーポリシーに次のアクセス許可ステートメントを追加する必要があります。

```
{
            "Sid": "Allow Logs Delivery to use the key",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
```

```
            "Resource": "*"
}
```

Amazon S3 でお客様が提供する暗号化キーの使用の詳細については、「Amazon Simple Storage Service ユーザーガイド」の「お客様が指定したキーによるサーバー側の暗号化 (SSE-C) の使用」を参照してください。

Firewall Manager で AWS WAF ポリシーのログ記録を有効にする

次の手順では、Firewall Manager コンソールで AWS WAF ポリシーのログ記録を有効にする方法について説明します。

AWS WAF ポリシーのログ記録を有効にするには

1. ログ記録を有効にする前に、次のようにログ記録の出力先リソースを設定する必要があります。

   - Amazon Kinesis Data Streams – Firewall Manager 管理者アカウントを使用して Amazon Data Firehose を作成します。プレフィックス `aws-waf-logs-` で始まる名前を使用します。例えば、`aws-waf-logs-firewall-manager-central`。自分が操作しているリージョン内で、PUT ソースを使用して Data Firehose を作成します。Amazon CloudFront のログをキャプチャしている場合は、米国東部 (バージニア北部) に Firehose を作成します。それを使用する前に、配信ストリームをテストして、組織のログに対応するのに十分なスループットがあることを確認します。詳細については、「Creating an Amazon Data Firehose Delivery Stream」を参照してください。
   - Amazon Simple Storage Service バケット – 「AWS WAF デベロッパーガイド」の「Amazon Simple Storage Service」トピックにあるガイドラインに従って、Amazon S3 バケットを作成します。また、Amazon S3 に対しログを発行するためのアクセス許可 に一覧されているアクセス許可を使用して、Amazon S3 バケットを設定する必要があります。
2. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

3. ナビゲーションペインで、[Security Policies] (セキュリティポリシー) を選択します。

4. ログ記録を有効にする AWS WAF ポリシーを選択します。 AWS WAF ログ記録の詳細については、「ログ記録 AWS WAF 保護パック (ウェブ ACL) トラフィック」を参照してください。
5. [Policy details] (ポリシーの詳細) タブの [Policy rules] (ポリシールール) セクションで、[Edit] (編集) を選択します。
6. [ログ記録設定] で、[ログ記録を有効にする] を選択してログ記録をオンにします。ログ記録は、ウェブ ACL で分析されるトラフィックに関する詳細情報を提供します。[ログの出力先] を選択し、設定したログ記録の送信先を選択します。名前が `aws-waf-logs-` で始まるログ記録先を選択する必要があります。 AWS WAF ログ記録先の設定については、「」を参照してくださいFirewall Manager での AWS WAF ポリシーの使用。
7. (オプション) 特定のフィールドとその値がログに含まれることを希望しない場合には、このフィールドをマスキングします。マスキングするフィールドを選び、[Add] (追加) を選択します。必要に応じて手順を繰り返し、追加のフィールドをマスキングします。マスキングされたフィールドは、ログに `REDACTED` と表示されます。例えば、[URI] フィールドをマスキングすると、ログの [URI] フィールドは `REDACTED` となります。
8. (オプション) すべてのリクエストをログに送信しない場合は、フィルタリング条件と動作を追加します。[Filter logs] (ログをフィルタリング) で、適用する各フィルターについて [Add filter] (フィルターを追加) を選択し、次にフィルター基準を選択して、基準に一致するリクエストを保持するかドロップするかを指定します。フィルターの追加が完了したら、必要に応じて、[Default logging behavior] (デフォルトのログ記録動作) を変更します。詳細については、「AWS WAF デベロッパーガイド」の 「保護パック (ウェブ ACL) レコードの検索」を参照してください。
9. [次へ] を選択します。
10. 設定を確認し、[Save] (保存) を選択してポリシーに対する変更を保存します。

Firewall Manager での AWS WAF ポリシーのログ記録の無効化

次の手順では、Firewall Manager コンソールで AWS WAF ポリシーのログ記録を無効にする方法について説明します。

AWS WAF ポリシーのログ記録を無効にするには

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

> **Note**
>
> Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Security Policies] (セキュリティポリシー) を選択します。
3. ログ記録を無効にする AWS WAF ポリシーを選択します。
4. [Policy details] (ポリシーの詳細) タブの [Policy rules] (ポリシールール) セクションで、[Edit] (編集) を選択します。
5. [Logging configuration status] (ログ記録設定ステータス) で、[Disabled] (無効) を選択します。
6. [Next] (次へ) を選択します。
7. 設定を確認し、[Save] (保存) を選択してポリシーに対する変更を保存します。

> **Note**
>
> Firewall Manager ポリシーのログ記録は、Firewall Manager インターフェイスを介してのみ変更または無効にします。 AWS WAF を使用して Firewall Manager によって管理されるウェブ ACL のログ記録設定を更新または削除する場合、Firewall Manager は変更を自動的に検出しません。を使用した場合は AWS WAF、 AWS WAF ポリシーのルールを再評価することで、Firewall Manager ポリシーの更新を手動で促すことができます AWS Config。これを行うには、 AWS Config コンソールで Firewall Manager ポリシーの AWS Config ルールを見つけ、再評価アクションを選択します。

Firewall Manager での AWS Shield Advanced ポリシーの使用

このページでは、Firewall Manager で AWS Shield ポリシーを使用する方法について説明します。Firewall Manager AWS Shield ポリシーで、保護するリソースを選択します。自動修復を有効にしてポリシーを適用すると、 AWS WAF ウェブ ACL にまだ関連付けられていないスコープ内のリソースごとに、Firewall Manager は空の AWS WAF ウェブ ACL を関連付けます。空のウェブ ACL は、Shield によるモニタリングの目的のために使用されます。その後、他のウェブ ACL をリソースに関連付けると、Firewall Manager は、空のウェブ ACL の関連付けを削除します。

> **Note**
>
> AWS WAF ポリシーの対象となるリソースが、自動アプリケーションレイヤー DDoS 緩和で設定された Shield Advanced ポリシーのスコープに入ると、Firewall Manager は、 AWS WAF ポリシーによって作成されたウェブ ACL を関連付けた後にのみ Shield Advanced 保護を適用します。

が Shield ポリシーで関連付けられていないウェブ ACLs AWS Firewall Manager を管理する方法

Firewall Manager が関連付けられていないウェブ ACL を、ポリシー内の[関連付けられていないウェブ ACL の管理]設定を使って管理するか、または API のSecurityServicePolicyDataデータタイプにおけるoptimizeUnassociatedWebACLsの設定で管理するかどうかは、設定することができます。[関連付けられていないウェブ ACL の管理]をポリシーで有効にした場合、Firewall Manager は、少なくとも 1 つのリソースがウェブ ACL を使用する場合のみ、ポリシー範囲内のアカウントにウェブ ACL を作成します。アカウントがポリシーの対象になるといつでも、少なくとも 1 つのリソースがウェブ ACL を使用する場合に、Firewall Manager はアカウントにウェブ ACL を自動的に作成します。

関連付けられていないウェブ ACL の管理を有効にすると、Firewall Manager はアカウント内の関連付けられていないウェブ ACL に 1 回だけクリーンアップを実行します。このクリーンアッププロセスには、数時間かかることがあります。Firewall Manager がウェブ ACL を作成した後、リソースがポリシーの範囲から外れても、Firewall Manager はそのリソースとウェブ ACL との関連付けを解除しません。Firewall Manager にウェブ ACL をクリーンアップさせたい場合は、最初にウェブ ACL から手動でリソースの関連付けを解除してから、ポリシーの[関連付けられていないウェブ ACL の管理] オプションを有効にする必要があります。

このオプションを有効にしない場合、Firewall Manager は関連付けられていないウェブ ACL を管理せず、ポリシーの範囲内にある各アカウントにウェブ ACL を自動的に作成します。

が Shield ポリシーでスコープの変更 AWS Firewall Manager を管理する方法

ポリシースコープ設定の変更、リソースのタグの変更、組織からのアカウントの削除など、多くの変更により、アカウントとリソースは AWS Firewall Manager Shield Advanced ポリシーの範囲外になる可能性があります。ポリシーの範囲設定の一般情報については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

AWS Firewall Manager Shield Advanced ポリシーでは、アカウントまたはリソースが範囲外になると、Firewall Manager はアカウントまたはリソースのモニタリングを停止します。

アカウントが組織から削除されて範囲外になった場合でも、そのアカウントは引き続き Shield Advanced にサブスクライブされます。アカウントは一括請求ファミリーのメンバーではなくなるため、アカウントには按分計算での Shield Advanced サブスクリプション料金が発生します。一方、範囲外になったが、組織に残っているアカウントについては、追加料金が発生しません。

Classic WebACL を使用する Shield ポリシーでは、リソースが範囲外になった場合、引き続き Shield Advanced によって保護され、Shield Advanced のデータ転送料金が発生します。

Firewall Manager の Shield Advanced ポリシーでアプリケーションレイヤー DDoS 自動緩和を使用する

このページでは、アプリケーションレイヤー DDoS 自動緩和が Firewall Manager とどのように連携するかについて説明します。

Amazon CloudFront ディストリビューションまたは Application Load Balancer に Shield Advanced ポリシーを適用する際に、ポリシーで Shield Advanced アプリケーションレイヤー DDoS 自動緩和を設定するオプションがあります。

Shield Advanced 自動緩和については、「Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和」を参照してください。

Shield Advanced アプリケーションレイヤー DDoS 自動緩和には、次の要件があります。

- アプリケーションレイヤーの DDoS の自動緩和は、Amazon CloudFront ディストリビューションと Application Load Balancer でのみ機能します。

  Shield Advanced ポリシーを Amazon CloudFront ディストリビューションに適用する場合、グローバルリージョン用に作成する Shield Advanced ポリシーに対してこのオプションを選択できます。Application Load Balancer に保護を適用する場合、Firewall Manager がサポートする任意のリージョンにポリシーを適用できます。
- 自動アプリケーションレイヤー DDoS 緩和は、最新バージョンの (v2) を使用して作成された保護パック AWS WAF (ウェブ ACLs) でのみ機能します。

  このため、 AWS WAF Classic ウェブ ACLs を使用するポリシーがある場合は、ポリシーを の最新バージョンを自動的に使用する新しいポリシーに置き換えるか AWS WAF、Firewall Manager に既存のポリシーの新しいバージョンのウェブ ACLs を作成して使用に切り替える必要があります。

オプションの詳細については、「AWS WAF Classic ウェブ ACLs最新バージョンのウェブ ACLs」を参照してください。

自動緩和設定

Firewall Manager Shield Advanced ポリシーのアプリケーションレイヤー DDoS 自動緩和オプションは、ポリシーの範囲内のアカウントおよびリソースに Shield Advanced 自動緩和機能を適用します。Shield Advanced 機能の詳細については、「Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和」を参照してください。

ポリシーの範囲内の CloudFront ディストリビューションまたは Application Load Balancer について、Firewall Manager で自動緩和を有効または無効にすることを選択でき、あるいはポリシーで Shield Advanced 自動緩和設定を無視することを選択できます。

- [有効化] - 自動緩和を有効にする場合は、一致するウェブリクエストを Shield Advanced 緩和ルールがカウントまたはブロックするかも指定します。Firewall Manager は、自動緩和が有効になっていないか、ポリシーに指定したルールアクションと一致しないルールアクションを使用している場合に、範囲内のリソースを非準拠としてマークします。自動修復のポリシーを設定すると、Firewall Manager は、必要に応じて非準拠のリソースを更新します。
- [無効化] - 自動緩和を無効にすることを選択した場合、Firewall Manager は、自動緩和が有効になっている範囲内のリソースを非準拠としてマークします。自動修復のポリシーを設定すると、Firewall Manager は、必要に応じて非準拠のリソースを更新します。
- [無視] – 自動緩和を無視することを選択した場合、Firewall Manager は、ポリシーの修復アクティビティを実行するときに Shield ポリシーの自動緩和設定を考慮しません。この設定では、Shield Advanced を通じて自動緩和を有効または無効にできます。Firewall Manager によってこれらの設定を上書きされることはありません。この設定は、Shield Advanced を通じて管理される Classic Load Balancers や Elastic IP リソースには適用されません。Shield Advanced は現在、これらのリソースの L7 自動緩和をサポートしていないためです。

AWS WAF Classic ウェブ ACLs最新バージョンのウェブ ACLs

自動アプリケーションレイヤー DDoS 緩和は、最新バージョンの (v2) を使用して作成された保護パック AWS WAF (ウェブ ACLs) でのみ機能します。

Shield Advanced ポリシーのウェブ ACL バージョンを確認するには、「Shield Advanced ポリシー AWS WAF で使用される のバージョンの確認」を参照してください。

Shield Advanced ポリシーで自動緩和を使用し、ポリシーが現在 AWS WAF Classic ウェブ ACLs を使用している場合は、新しい Shield Advanced ポリシーを作成して現在のポリシーを置き換えるか、このセクションで説明されているオプションを使用して、以前のバージョンのウェブ ACLs を現在の Shield Advanced ポリシー内の新しい (v2) ウェブ ACLs に置き換えることができます。新しいポリシーACLs が作成されます AWS WAF。ポリシー全体を置き換えた場合、ポリシーを削除すると、Firewall Manager で以前のバージョンのウェブ ACL もすべて削除できます。このセクションの残りの部分では、既存のポリシー内のウェブ ACL を置き換えるためのオプションについて説明します。

Amazon CloudFront リソースの既存の Shield Advanced ポリシーを変更すると、Firewall Manager は、v2 ウェブ ACL がまだない範囲内のアカウントで、ポリシーの新しい empty AWS WAF (v2) ウェブ ACL を自動的に作成できます。Firewall Manager が新しいウェブ ACL を作成するときに、ポリシーに同じアカウントに AWS WAF Classic ウェブ ACL がすでにある場合、Firewall Manager は既存のウェブ ACL と同じデフォルトのアクション設定で新しいバージョンのウェブ ACL を設定します。既存の AWS WAF Classic ウェブ ACL がない場合、Firewall Manager は新しいウェブ ACL Allowでデフォルトのアクションを に設定します。Firewall Manager が新しいウェブ ACL を作成した後、 AWS WAF コンソールで必要に応じてカスタマイズできます。

次のポリシー設定オプションのいずれかを選択すると、Firewall Manager は、まだそれらを持たない範囲内のアカウント用に新しい (v2)ウェブ ACL を作成します。

- アプリケーションレイヤー DDoS 自動緩和を有効または無効にする場合。この選択のみの場合、Firewall Manager が新しいウェブ ACL を作成するだけであり、ポリシーの範囲内リソース上の既存の AWS WAF Classicウェブ ACL の関連付けを置き換えることはありません。
- 自動修復のポリシーアクションを選択し、 AWS WAF Classic ウェブ ACLs を AWS WAF (v2) ウェブ ACLsオプションを選択します。アプリケーションレイヤー DDoS 自動緩和の設定の選択内容にかかわらず、以前のバージョンのウェブ ACL を置き換えることを選択できます。

  置換オプションを選択すると、Firewall Manager は必要に応じて新しいバージョンのウェブ ACL を作成し、ポリシーの範囲内のリソースについて次の操作を実行します。

  - リソースが他のアクティブな Firewall Manager ポリシーからウェブ ACL に関連付けられている場合、Firewall Manager は関連付けのみを残します。
  - その他の場合、Firewall Manager は AWS WAF Classic ウェブ ACL との関連付けを削除し、リソースをポリシーの AWS WAF (v2) ウェブ ACL に関連付けます。

必要に応じて、Firewall Manager で以前のバージョンのウェブ ACL を新しいバージョンのウェブ ACL に置き換えることを選択できます。以前にポリシーの AWS WAF Classicウェブ ACL をカスタ

マイズしたことがある場合は、Firewall Manager に置換ステップを実行させることを選択する前に、新しいバージョンのウェブ ACL を同等の設定に更新できます。

ポリシーのウェブ ACL のいずれかのバージョンには、 AWS WAF または AWS WAF Classic の同じバージョンコンソールからアクセスできます。

Firewall Manager は、ポリシー自体を削除するまで、置き換えられた AWS WAF Classic ウェブ ACLs を削除しません。 AWS WAF Classic ウェブ ACLs がポリシーで使用されなくなったら、必要に応じて削除できます。

Shield Advanced ポリシー AWS WAF で使用される のバージョンの確認

このページでは、Shield Advanced ポリシーが使用する AWS WAF ウェブ ACL のバージョンを確認する方法について説明します。

AWS WAF Firewall Manager Shield Advanced ポリシーが使用するバージョンを確認するには、ポリシー AWS Config のサービスにリンクされたルールのパラメータキーを確認します。使用中 AWS WAF のバージョンが最新の場合、パラメータキーには `policyId`と が含まれます`webAclArn`。以前のバージョンである AWS WAF Classic の場合、パラメータキーには `webAclId`と が含まれます`resourceTypes`。

この AWS Config ルールは、ポリシーが対象範囲内のリソースで現在使用しているウェブ ACLs のキーのみを一覧表示します。

Firewall Manager Shield Advanced ポリシーのどのバージョンが を使用する AWS WAF かを確認するには

1. Shield Advanced ポリシーのポリシー ID を取得します。

    a. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

    b. ナビゲーションペインで、[Security Policies] (セキュリティポリシー) を選択します。

    c. ポリシーのリージョンを選択します。CloudFront ディストリビューションの場合、これは `Global` です。

    d. 必要なポリシーを見つけて、その [Policy ID] (ポリシー ID) の値をコピーします。

        ポリシー ID の例: `1111111-2222-3333-4444-a55aa5aaa555`。

2. 文字列 にポリシー ID を追加して、ポリシーの AWS Config ルール名を作成しますFMManagedShieldConfigRule。

   AWS Config ルール名の例: FMManagedShieldConfigRule1111111-2222-3333-4444-a55aa5aaa555。

3. 関連付けられた AWS Config ルールのパラメータで、 policyIdおよび という名前のキーを検索しますwebAclArn。

   a. https://console.aws.amazon.com/config/home で AWS Config コンソールを開きます。
   b. ナビゲーションペインで [ルール] を選択します。
   c. リストで Firewall Manager ポリシーの AWS Config ルール名を見つけて選択します。ルールのページが開きます。
   d. [Rule details] (ルールの詳細) の [Parameters] (パラメータ) セクションで、キーを探します。policyId と webAclArn という名前のキーが見つかった場合、ポリシーは最新バージョンの AWS WAFを使用して作成されたウェブ ACL を使用します。webAclId および という名前のキーが見つかった場合resourceTypes、ポリシーは以前のバージョンである AWS WAF Classic を使用して作成されたウェブ ACLs を使用します。

Firewall Manager のセキュリティグループポリシーを使用して Amazon VPC セキュリティグループを管理する

このページでは、 AWS Firewall Manager セキュリティグループポリシーを使用して、 の組織の Amazon Virtual Private Cloud セキュリティグループを管理する方法について説明します AWS Organizations。一元管理されたセキュリティグループポリシーは、組織全体、またはアカウントとリソースの特定のサブセットに適用できます。さらに、監査および使用状況セキュリティグループポリシーを使用して、組織内で使用中のセキュリティグループポリシーをモニタリングおよび管理することもできます。

Firewall Manager は、ポリシーを継続的に維持し、組織全体で追加または更新されるたびにアカウントとリソースに適用します。詳細については AWS Organizations、AWS Organizations 「 ユーザーガイド」を参照してください。

Amazon Virtual Private Cloud セキュリティグループの詳細については、「Amazon VPC ユーザーガイド」の「VPC のセキュリティグループ」を参照してください。

Firewall Manager セキュリティグループポリシーを使用して、 AWS 組織全体で次の操作を実行できます。

- 指定したアカウントとリソースに共通セキュリティグループを適用します。
- セキュリティグループルールを監査し、準拠していないルールを見つけて修復します。
- セキュリティグループの使用状況を監査し、未使用および冗長なセキュリティグループをクリーンアップします。

このセクションでは、Firewall Manager セキュリティグループポリシーの仕組みについて説明し、使用する際のガイダンスを提供します。セキュリティグループポリシーを作成する手順については、「AWS Firewall Manager ポリシーの作成」を参照してください。

セキュリティグループポリシーのベストプラクティス

このセクションでは、 AWS Firewall Managerを使用してセキュリティグループを管理するための推奨事項を示します。

Firewall Manager 管理者アカウントを除外する

ポリシーの範囲を設定する場合は、Firewall Manager 管理者アカウントを除外します。コンソールを使用して使用状況監査セキュリティグループポリシーを作成する場合、これがデフォルトのオプションです。

自動修復を無効にした状態で開始する

コンテンツまたは使用状況監査セキュリティグループポリシーの場合は、自動修復を無効にした状態で始めます。ポリシーの詳細情報を確認し、自動修復による影響を判断します。変更が適切であることを確認したら、ポリシーを編集して自動修復を有効にします。

外部ソースを使用してセキュリティグループを管理する場合は、競合を回避する

Firewall Manager 以外のツールまたはサービスを使用してセキュリティグループを管理する場合は、Firewall Manager の設定と外部ソースの設定との競合を避けるように注意してください。自動修復を使用して、設定が競合する場合は、両側のリソースを消費する、競合する修復のサイクルを作成できます。

例えば、 AWS リソースのセットのセキュリティグループを維持するために別のサービスを設定し、同じリソースの一部またはすべてに対して異なるセキュリティグループを維持するように Firewall Manager ポリシーを設定するとします。他のセキュリティグループを範囲内のリソースに関連付けることを禁止するようにどちらかの側を設定すると、その側ではもう一方の側によって維持されているセキュリティグループの関連付けが削除されます。両側がこのように設定されている場合、競合する関連付けの解除と関連付けのサイクルになる可能性があります。

さらに、Firewall Manager 監査ポリシーを作成して、他のサービスのセキュリティグループ設定と競合するセキュリティグループ設定を強制するとします。Firewall Manager 監査ポリシーによって適用された修復によって、そのセキュリティグループを更新または削除し、他のサービスのコンプライアンスから解除できます。モニタリングして、検出した問題を自動的に修復するように他のサービスが設定されている場合、セキュリティグループを再作成または更新して、また Firewall Manager 監査ポリシーへのコンプライアンスを解除します。Firewall Manager 監査ポリシーに自動修復が設定されている場合、また外部セキュリティグループなどを更新または削除します。

このような競合を回避するには、Firewall Manager と外部ソースの間で相互に排他的な設定を作成します。

タグ付けを使用して、Firewall Manager ポリシーによる自動修復から外部のセキュリティグループを除外できます。これを行うには、外部ソースによって管理されるセキュリティグループまたはその他のリソースに 1 つ以上のタグを追加します。その後、Firewall Manager ポリシーの範囲を定義するときに、リソース仕様で、追加した 1 つまたは複数のタグを持つリソースを除外します。

同様に、外部のツールまたはサービスでは、Firewall Manager が管理するセキュリティグループを管理アクティビティまたは監査アクティビティから除外します。Firewall Manager リソースをインポートしないか、Firewall Manager 固有のタグ付けを使用して外部管理から除外します。

使用状況監査セキュリティグループポリシーのベストプラクティス

使用状況監査セキュリティグループポリシーを使用する場合は、以下のガイドラインに従ってください。

- 15 分以内などの短時間で、セキュリティグループの関連ステータスを何度も変更しないでください。そうする場合、Firewall Manager の対応するイベントの一部またはすべてが紛失する可能性があります。例えば、セキュリティグループを Elastic Network Interface にすばやく関連付けたり関連付けを解除したりしないでください。

セキュリティグループポリシーの規制と制限

このセクションでは、Firewall Manager セキュリティグループポリシーの使用に関する規制と制限事項を一覧表示します。

リソースタイプ: Amazon EC2 インスタンス

このセクションでは、Firewall Manager セキュリティグループポリシーで Amazon EC2 インスタンスを保護するための規制と制限事項を一覧表示します。

- Amazon EC2 Elastic Network Interface (ENI) のセキュリティグループでは、セキュリティグループに対する変更は Firewall Manager にすぐには表示されません。Firewall Manager は通常、数時間以内に変更を検出しますが、検出は最長で 6 時間遅延する可能性があります。
- Firewall Manager は、Amazon Relational Database Service によって作成された Amazon EC2 ENI のセキュリティグループをサポートしていません。
- Firewall Manager は、Fargate サービスタイプを使用して作成された Amazon EC2 ENI のセキュリティグループの更新をサポートしていません。ただし、Amazon EC2 サービスタイプで Amazon ECS ENI のセキュリティグループを更新することはできます。
- Firewall Manager には、リクエスタが管理する Amazon EC2 ENI を変更するアクセス許可がないため、それらのセキュリティグループの更新をサポートしていません。
- 一般的なセキュリティグループポリシーの場合、これらの注意点は、EC2 インスタンスにアタッチされているElastic Network Interface (ENI) の数と、添付ファイルを追加せずに EC2 インスタンスのみを修正するか、すべてのインスタンスを修正するかを指定するポリシーオプション間の相互作用に関係しています。すべての EC2 インスタンスにはデフォルトのプライマリ ENI があり、より多くの ENI をアタッチできます。API では、この選択肢のポリシーオプション設定は `ApplyToAllEC2InstanceENIs` です。

  スコープ内の EC2 インスタンスに追加の ENI がアタッチされており、ポリシーにプライマリ ENI と EC2 インスタンスのみを含めるように設定されている場合、Firewall Manager は EC2 インスタンスの修復を試みません。さらに、インスタンスがポリシーの範囲外になった場合、Firewall Manager はインスタンスに対して確立したセキュリティグループの関連付けの関連付けを解除しようとしません。

  次のエッジケースでは、リソースのクリーンアップ中に、ポリシーのリソースクリーンアップ仕様に関係なく、Firewall Manager はレプリケートされたセキュリティグループの関連付けをそのまま残すことができます。

  - 追加の ENI を持つインスタンスが、以前にすべての EC2 インスタンスを含めるように設定されたポリシーによって修復され、その後、インスタンスがポリシーの対象外になった場合、またはポリシー設定が追加の ENI を持たないインスタンスのみを含むように変更された場合。
  - 追加の ENI がないインスタンスが、追加の ENI がないインスタンスのみを含むように設定されたポリシーによって修復された場合、別の ENI がインスタンスにアタッチされ、インスタンスはポリシーのスコープから外れました。

その他の規制と制限事項

Firewall Manager セキュリティグループポリシーのその他の規制と制限事項を次に示します。

- Firewall Manager セキュリティグループポリシーは、 を通じて共有されるセキュリティグループをサポートしていません AWS RAM。
- を使用して組織全体 AWS RAM でプレフィックスリストを共有することは、Firewall Manager の公式にサポートされている機能ではありません。今日は機能する可能性がありますが、そのユースケースのサポート AWS を提供する義務も、引き続き機能する保証もありません。
- Amazon ECS ENI の更新は、ローリング更新 (Amazon ECS) デプロイコントローラーを使用する Amazon ECS サービスでのみ可能です。CODE_DEPLOY や外部コントローラーなどの他の Amazon ECS デプロイコントローラーでは、Firewall Manager は現在 ENI を更新できません。
- Firewall Manager は、Network Load Balancer の ENI のセキュリティグループの更新をサポートしていません。
- 一般的なセキュリティグループポリシーでは、共有 VPC が後でアカウントとの共有を解除された場合、Firewall Manager はアカウント内のレプリカセキュリティグループを削除しません。
- 使用監査セキュリティグループポリシーを使用する場合、同じスコープを持ち、カスタムの遅延時間設定を持つ複数のポリシーを作成すると、コンプライアンス検出がある最初のポリシーがその検出結果を報告するポリシーとなります。

セキュリティグループポリシーのユースケース

AWS Firewall Manager 一般的なセキュリティグループポリシーを使用して、Amazon VPC インスタンス間の通信のホストファイアウォール設定を自動化できます。このセクションでは、標準 Amazon VPC アーキテクチャを一覧表示し、Firewall Manager 共通セキュリティグループポリシーを使用して各アーキテクチャを保護する方法について説明します。これらのセキュリティグループポリシーを使用すると、統合されたルールセットを適用してさまざまなアカウントのリソースを選択し、Amazon Elastic Compute Cloud および Amazon VPC のアカウント単位の設定を回避できます。

Firewall Manager 共通セキュリティグループポリシーでは、別の Amazon VPC のインスタンスとの通信に必要な EC2 Elastic Network Interface のみにタグ付けできます。同じ Amazon VPC 内の他のインスタンスの方がセキュリティが高く、分離されています。

ユースケース: Application Load Balancer および Classic Load Balancer に対するリクエストのモニタリングと制御

Firewall Manager 共通セキュリティグループポリシーを使用して、範囲内のロードバランサーが処理すべきリクエストを定義できます。これは、Firewall Manager コンソールで設定できます。セキュリティグループのインバウンドルールに準拠したリクエストのみがロードバランサーに到達でき、そのロードバランサーはアウトバウンドルールを満たすリクエストのみを配信します。

ユースケース: インターネットにアクセス可能、パブリック Amazon VPC

Amazon VPC 共通セキュリティグループポリシーを使用して、インバウンドポート 443 のみを許可するなど、パブリック Amazon VPC を保護できます。これは、パブリック VPC のインバウンド HTTPS トラフィックのみを許可することと同じです。VPC 内のパブリックリソースにタグ付けし (「PublicVPC」など)、そのタグを持つリソースのみに Firewall Manager ポリシーの範囲を設定できます。Firewall Manager は、これらのリソースにポリシーを自動的に適用します。

ユースケース: パブリックおよびプライベート Amazon VPC インスタンス

パブリックリソースには、前のインターネットにアクセス可能なパブリック Amazon VPC インスタンスのユースケースで推奨されているのと同じ共通セキュリティグループポリシーを使用できます。2 つ目の共通セキュリティグループポリシーを使用して、パブリックリソースとプライベートリソース間の通信を制限できます。パブリックおよびプライベート Amazon VPC インスタンスのリソースに「PublicPrivate」などのタグを付けて、2 つ目のポリシーを適用します。3 つ目のポリシーを使用して、プライベートリソースと他の企業またはプライベート Amazon VPC インスタンスとの間で許可される通信を定義できます。このポリシーの場合、プライベートリソースで別の識別タグを使用できます。

ユースケース: ハブアンドスポーク Amazon VPC インスタンス

共通セキュリティグループポリシーを使用して、ハブ Amazon VPC インスタンスとスポーク Amazon VPC インスタンス間の通信を定義できます。2 つ目のポリシーを使用して、各スポーク Amazon VPC インスタンスからハブ Amazon VPC インスタンスへの通信を定義できます。

ユースケース: Amazon EC2 インスタンスのデフォルトネットワークインターフェイス

共通セキュリティグループポリシーを使用して、内部 SSH やパッチ/OS 更新サービスなどの標準通信のみを許可し、その他の安全でない通信を禁止することができます。

ユースケース: オープン許可を持つリソースを特定する

監査セキュリティグループポリシーを使用して、パブリック IP アドレスと通信する許可を持つ組織内のすべてのリソース、またはサードパーティベンダーに属する IP アドレスを持つリソースを特定できます。

Firewall Manager の一般的なセキュリティグループポリシーの使用

このページでは、Firewall Manager の一般的なセキュリティグループポリシーの仕組みについて説明します。

Firewall Manager では、共通セキュリティグループポリシーを使用して、組織全体のアカウントおよびリソースに対するセキュリティグループの一元管理された関連付けが提供されます。組織内でポリシーを適用する場所と方法を指定します。

次のリソースタイプに共通セキュリティグループポリシーを適用できます。

- Amazon Elastic Compute Cloud (Amazon EC2) インスタンス
- Elastic Network Interface
- Application Load Balancer
- Classic Load Balancer

コンソールを使用して共通セキュリティグループポリシーを作成する方法については、「共通セキュリティグループポリシーの作成」を参照してください。

共有 VPC

共通セキュリティグループポリシーのポリシーの範囲設定で、共有 VPC を含めるよう選択できます。この選択肢には、別のアカウントによって所有され、範囲内のアカウントと共有される VPC が含まれます。範囲内のアカウントが所有する VPC は、常に含まれます。共有 VPC の詳細については、「Amazon VPC ユーザーガイド」の「共有 VPC の使用」を参照してください。

共有 VPC を含めるには、次の注意事項が適用されます。これらに加えて、セキュリティグループポリシーの規制と制限 のセキュリティグループポリシーに関する一般的な注意事項も適用されます。

- Firewall Manager は、範囲内の各アカウントの VPC にプライマリセキュリティグループをレプリケートします。共有 VPC の場合、Firewall Manager は VPC が共有されている範囲内のアカウントごとに、プライマリセキュリティグループを 1 回 レプリケートします。これにより、単一の共有 VPC に複数のレプリカが作成される可能性があります。
- 新しい共有 VPC を作成する場合、ポリシーの範囲内にある VPC に少なくとも 1 つのリソースを作成するまで、Firewall Manager セキュリティグループポリシーの詳細にその共有VPC は表示されません。
- 共有 VPC を有効にしたポリシーで共有 VPC を無効にすると、共有 VPC において、Firewall Manager は、リソースに関連付けられていないレプリカセキュリティグループを削除します。Firewall Manager は、残りのレプリカセキュリティグループをそのままの状態にしますが、それらの管理を停止します。これらの残りのセキュリティグループを削除するには、各共有 VPC インスタンスで手動で管理する必要があります。

プライマリセキュリティグループ

共通セキュリティグループポリシーごとに、1 つ以上のプライマリセキュリティグループ AWS Firewall Manager を指定します。

- プライマリセキュリティグループは、Firewall Manager 管理者アカウントによって作成される必要があり、アカウント内の任意の Amazon VPC インスタンスに存在できます。
- プライマリセキュリティグループは、Amazon Virtual Private Cloud (Amazon VPC) または Amazon Elastic Compute Cloud (Amazon EC2) を通じて管理します。詳細については、「Amazon VPC ユーザーガイド」の「セキュリティグループの操作」を参照してください。
- Firewall Manager セキュリティグループポリシーのプライマリとして、1 つ以上のセキュリティグループを指定できます。デフォルトでは、ポリシー内で許可されているセキュリティグループの数は 1 つですが、リクエストを送信して増やすことができます。詳細については、「AWS Firewall Manager クォータ」を参照してください。
- プライマリセキュリティグループには、少なくとも 1 つの進入ルールまたは退出ルールが含まれている必要があります。プライマリセキュリティグループからすべてのルールを削除すると、Firewall Manager はルールを持つプライマリセキュリティグループの最新バージョンに基づいてレプリカセキュリティグループを管理し続けます。

ポリシールールの設定

共通セキュリティグループポリシーのセキュリティグループとリソースに対して、次の変更管理動作の 1 つ以上を選択できます。

- ローカルユーザーがレプリカセキュリティグループに対して行った変更を特定し、レポートします。
- ポリシー範囲内の AWS リソースから他のセキュリティグループの関連付けを解除します。
- プライマリグループからレプリカセキュリティグループにタグを配布します。

> **Important**
>
> Firewall Manager は、 AWS サービスによって追加されたシステムタグをレプリカセキュリティグループに配布しません。システムタグは `aws:` プレフィックスで始まります。また、ポリシーに組織のタグポリシーと矛盾するタグがある場合は、Firewall Manager が既存のセキュリティグループでのタグ更新や、新しいセキュリティグループの作成を行うこ

とはありません。タグポリシーの詳細については、「 AWS Organizations ユーザーガイド」の「タグポリシー」を参照してください。

- プライマリグループからレプリカセキュリティグループにセキュリティグループの参照を配布します。

  これにより、指定したセキュリティグループの VPC に関連するインスタンスに対して、スコープ内の全リソースで共通のセキュリティグループの参照ルールを簡単に確立することができます。このオプションを有効にすると、Firewall Manager は、Amazon Virtual Private Cloud 内でセキュリティグループがピアセキュリティグループを参照している場合にのみ、セキュリティグループの参照を適用します。レプリカのセキュリティグループがピアセキュリティグループを正しく参照していない場合、Firewall Manager はこれらのレプリケートされたセキュリティグループを非準拠としてマークします。詳細については、「Amazon VPC ピア機能ガイド」の「セキュリティグループの更新とピアセキュリティグループの参照」を参照してください。

  このオプションを有効にしない場合、Firewall Manager はセキュリティグループの参照をレプリカのセキュリティグループに適用しません。Amazon VPC 内の VPC ピア機能については、「Amazon VPC ピア機能ガイド」を参照してください。

ポリシーの作成と管理

共通セキュリティグループポリシーを作成すると、Firewall Manager はポリシーの範囲内のすべての Amazon VPC インスタンスにプライマリセキュリティグループをレプリケートし、レプリケートされたセキュリティグループをポリシーの範囲内にあるアカウントおよびリソースに関連付けます。プライマリセキュリティグループを変更すると、Firewall Manager はその変更をレプリカに伝達します。

共通セキュリティグループポリシーを削除する場合、ポリシーによって作成されたリソースをクリーンアップするかどうかを選択できます。Firewall Manager の共通セキュリティグループの場合、これらのリソースはレプリカセキュリティグループです。ポリシーの削除後に個々のレプリカを手動で管理する場合を除き、クリーンアップオプションを選択してください。ほとんどの場合、クリーンアップオプションを選択するのが最も簡単な方法です。

レプリカの管理方法

Amazon VPC インスタンス内のレプリカセキュリティグループは、他の Amazon VPC セキュリティグループと同様に管理されます。詳細については、「Amazon VPC ユーザーガイド」の「VPC のセキュリティグループ」を参照してください。

Firewall Manager のコンテンツ監査セキュリティグループポリシーの使用

このページでは、Firewall Manager のコンテンツ監査セキュリティグループポリシーの仕組みについて説明します。

AWS Firewall Manager コンテンツ監査セキュリティグループポリシーを使用して、組織のセキュリティグループで使用されているルールを監査し、ポリシーアクションを適用します。コンテンツ監査セキュリティグループポリシーは、ポリシーで定義した範囲に従って、 AWS 組織で使用されているすべてのお客様が作成したセキュリティグループに適用されます。

コンソールを使用してコンテンツ監査セキュリティグループポリシーを作成する方法については、「コンテンツ監査セキュリティグループポリシーの作成」を参照してください。

ポリシーの範囲リソースタイプ

次のリソースタイプにコンテンツ監査セキュリティグループポリシーを適用できます。

- Amazon Elastic Compute Cloud (Amazon EC2) インスタンス
- Elastic Network Interface
- Amazon VPC セキュリティグループ

セキュリティグループは、明示的に範囲内にある場合、または範囲内のリソースに関連付けられている場合、ポリシーの範囲で考慮されます。

ポリシールールのオプション

コンテンツ監査ポリシーごとに、マネージドポリシールールまたはカスタムポリシールールのいずれかを使用できますが、両方は使用できません。

- マネージドポリシールール - マネージドルールを含むポリシーでは、アプリケーションとプロトコルのリストを使用して、Firewall Manager が監査して準拠または非準拠としてマークされるルールを制御できます。Firewall Manager によって管理されているリストを使用できます。独自のアプリケーションリストとプロトコルリストを作成および使用することもできます。これらのリストタイプおよびカスタムリストの管理オプションの詳細については、「Firewall Manager のマネージドリストの使用」を参照してください。
- カスタムポリシールール - カスタムポリシールールを含むポリシーでは、既存のセキュリティグループをポリシーの監査セキュリティグループとして指定します。監査セキュリティグループルールは、Firewall Manager が監査して準拠または非準拠としてマークされるルールを定義するテンプレートとして使用できます。

監査セキュリティグループ

ポリシーで監査セキュリティグループを使用するには、Firewall Manager 管理者アカウントを使用して監査セキュリティグループを作成する必要があります。セキュリティグループは、Amazon Virtual Private Cloud (Amazon VPC) または Amazon Elastic Compute Cloud (Amazon EC2) を通じて管理できます。詳細については、「Amazon VPC ユーザーガイド」の「セキュリティグループの操作」を参照してください。

コンテンツ監査セキュリティグループポリシーに使用するセキュリティグループは、Firewall Manager によって、ポリシーの範囲内にあるセキュリティグループの比較参照としてのみ使用されます。Firewall Manager は、組織内のどのリソースにも関連付けません。

監査セキュリティグループでルールを定義する方法は、ポリシールール設定での選択によって異なります。

- マネージドポリシールール – マネージドポリシールール設定では、監査セキュリティグループを使用して、ポリシー内の他の設定を上書きし、許可または拒否しなければ別のコンプライアンスに関する結果を発生させ得るルールを明示的に許可または拒否します。
  - 監査セキュリティグループで定義されているルールを常に許可することを選択した場合、監査セキュリティグループで定義されているルールと一致するルールは、他のポリシー設定にかかわらず、ポリシーに準拠しているものとみなされます。
  - 監査セキュリティグループで定義されているルールを常に拒否することを選択した場合、監査セキュリティグループで定義されているルールと一致するルールは、他のポリシー設定にかかわらず、ポリシーに非準拠であるものとみなされます。
- カスタムポリシールール: カスタムポリシールール設定について、監査セキュリティグループは、範囲内のセキュリティグループルールで許容できるものと許容できないものの例を提示します。
  - ルールの使用を許可する場合は、すべての範囲内セキュリティグループに、ポリシーの監査セキュリティグループルールの許可範囲内にあるルールのみを含める必要があります。この場合、ポリシーのセキュリティグループルールは、許容できる操作の例を示します。
  - ルールの使用を拒否する場合は、すべての範囲内セキュリティグループに、ポリシーの監査セキュリティグループルールの許可範囲内にないルールのみを含める必要があります。この場合、ポリシーのセキュリティグループは、許容できない処理の例を示します。

ポリシーの作成と管理

監査セキュリティグループポリシーを作成するときは、自動修復を無効にする必要があります。自動修復を有効にする前に、ポリシー作成の影響を確認することをお勧めします。予想される影響を確認

したら、ポリシーを編集して自動修復を有効にできます。自動修復が有効な場合、Firewall Manager は範囲内セキュリティグループで非準拠のルールを更新または削除します。

監査セキュリティグループポリシーの影響を受けるセキュリティグループ

組織内のすべてのユーザー定義セキュリティグループは、監査セキュリティグループポリシーの範囲に含める資格があります。

レプリカセキュリティグループはユーザー定義ではないため、監査セキュリティグループポリシーの範囲に直接適用することはできません。ただし、ポリシーの自動修復アクティビティの結果として更新できます。共通セキュリティグループポリシーのプライマリセキュリティグループはユーザー定義であり、監査セキュリティグループポリシーの範囲内に含めることができます。監査セキュリティグループポリシーがプライマリセキュリティグループに変更を加えた場合、Firewall Manager はそれらの変更をレプリカに自動的に伝達します。

コンテンツ監査セキュリティグループポリシーの規制と制限事項

コンテンツ監査セキュリティグループポリシーでピアセキュリティグループを参照することはできません。

すべての Firewall Manager セキュリティグループのその他の考慮事項については、「セキュリティグループポリシーの規制と制限」を参照してください。

Firewall Manager の使用状況監査セキュリティグループポリシーの使用

このページでは、Firewall Manager の使用状況監査セキュリティグループポリシーの仕組みについて説明します。

AWS Firewall Manager 使用状況監査セキュリティグループポリシーを使用して、未使用および冗長なセキュリティグループがないか組織をモニタリングし、オプションでクリーンアップを実行します。このポリシーの自動修復を有効にすると、Firewall Manager は次の処理を行います。

1. 冗長なセキュリティグループを統合します (このオプションを選択した場合)。
2. 未使用のセキュリティグループを削除します (このオプションを選択した場合)。

次のリソースタイプに使用状況の監査セキュリティグループポリシーを適用できます。

- Amazon VPC セキュリティグループ

コンソールを使用して使用状況の監査セキュリティグループポリシーを作成する方法については、「使用状況監査セキュリティグループポリシーの作成」を参照してください。

Firewall Manager が冗長セキュリティグループを検知および修復する方法

セキュリティグループを冗長とみなすには、まったく同じルールセットを持ち、同じ Amazon VPC インスタンスに存在している必要があります。

冗長なセキュリティグループのセットを修復するため、Firewall Manager は、保持するセット内のセキュリティグループの 1 つを選択し、セット内の他のセキュリティグループに関連付けられているすべてのリソースに関連付けます。その後、Firewall Manager は、関連付けられたリソースから他のセキュリティグループの関連付けを解除し、使用されていない状態にします。

> **Note**
>
> 未使用のセキュリティグループも削除するように選択した場合、Firewall Manager は次にその処理を実行します。これにより、冗長セットに含まれるセキュリティグループが削除される可能性があります。

Firewall Manager が未使用のセキュリティグループを検知および修復する方法

Firewall Manager は、次の両方が当てはまる場合、セキュリティグループを未使用と見なします。

- セキュリティグループは、Amazon EC2 インスタンスまたは Amazon EC2 Elastic Network Interface では使用されません。
- Firewall Manager は、ポリシールール期間で指定された分間数内にその設定アイテムを受信していません。

ポリシールールの期間はデフォルト設定で 0 分ですが、時間を最大 365 日 (525,600 分) まで延長して、新しいセキュリティグループをリソースに関連付ける時間を確保するのが可能です。

> **Important**
>
> デフォルト値の 0 以外の分間数を指定する場合は、 AWS Configで間接的な関係を有効にする必要があります。それ以外の場合、使用状況監査セキュリティグループポリシーは意図したとおりに機能しません。の間接的な関係については AWS Config、 AWS Config デベロッパーガイドの「 の間接的な関係 AWS Config」を参照してください。

可能な場合、Firewall Manager はルールの設定に従って、アカウントから削除することで未使用のセキュリティグループを修復します。Firewall Manager がセキュリティグループを削除できない場合、ポリシーに準拠していないとしてマークします。Firewall Manager は、別のセキュリティグループによって参照されているセキュリティグループを削除することはできません。

修復の時間は、デフォルトの期間設定とカスタム設定のどちらを使用するかによって異なります:

- 期間を 0 に設定、デフォルト – この設定では、セキュリティグループは Amazon EC2 インスタンスまたは Elastic Network Interface で使用されないと、すぐに未使用と見なされます。

  期間をゼロに設定する場合、Firewall Manager はセキュリティグループを直ちに修復します。
- 0 より大きい期間 – この設定では、Amazon EC2 インスタンスまたはElastic Network Interface で使用されておらず、Firewall Manager が指定された分数内に設定項目を受け取っていない場合、セキュリティグループは未使用と見なされます。

  ゼロ以外の期間を設定する場合、Firewall Manager はセキュリティグループを 24 時間の未使用状態に維持した後に修復します。

デフォルトのアカウント指定

コンソールで使用状況に関する監査セキュリティグループポリシーを作成すると、Firewall Manager は自動的に [Exclude the specified accounts and include all others] (指定されたアカウントを除外し、他のすべてを含める) を選択します。その後、サービスによって、除外するリストに Firewall Manager 管理者アカウントが配置されます。これは推奨されるアプローチであり、Firewall Manager 管理者アカウントに属するセキュリティグループを手動で管理できます。

Firewall Manager での Amazon VPC ネットワークアクセスコントロールリスト (ACL) ポリシーの使用

このセクションでは、 AWS Firewall Manager ネットワーク ACL ポリシーの仕組みと使用に関するガイダンスについて説明します。コンソールを使用してネットワーク ACL ポリシーを作成する方法については、ネットワーク ACL の作成 を参照してください。

Amazon VPC ネットワークのアクセスコントロールリスト (ACL) の詳細については、「Amazon VPC ユーザーガイド」の「ACL を使用して、サブネットのトラフィックを制御する」を参照してください。

Firewall Manager ネットワーク ACL ポリシーを使用して、 AWS Organizationsで組織の Amazon Virtual Private Cloud (Amazon VPC) ネットワークのアクセスコントロールリスト (ACL) を管理

できます。ポリシーのネットワーク ACL ルール設定と、設定を適用するアカウントとサブネットを定義します。Firewall Manager は、組織全体で追加または更新されるたびにポリシー設定をアカウントとサブネットに継続的に適用します。ポリシースコープと の詳細については AWS Organizations、AWS Firewall Manager ポリシースコープの使用「」およびAWS Organizations「 ユーザーガイド」を参照してください。

Firewall Manager ネットワーク ACL ポリシーを定義する場合、名前やスコープなどの標準の Firewall Manager ポリシー設定に加えて、以下を指定します:

- インバウンドおよびアウトバウンドトラフィック処理の最初と最後のルール。Firewall Manager は、ポリシーの範囲内にあるネットワーク ACL でこれらの存在と順序を適用します。または、コンプライアンス違反を報告します。個々のアカウントは、ポリシーの最初と最後のルールの間に実行するカスタムルールを作成できます。
- ネットワーク ACL 内のルール間でトラフィック管理の競合が発生する場合に、修復を強制するかどうか。これは、ポリシーに対して修復が有効になっている場合にのみ適用されます。

Firewall Manager ネットワーク ACL ポリシーを使用するためのベストプラクティス

このセクションでは、Firewall Manager ネットワーク ACL ポリシーとマネージドネットワーク ACL の連携に関する推奨事項を一覧表示します。

FMManaged タグを参照して、Firewall Manager によって管理されるネットワーク ACL を特定します。

Firewall Manager が管理するネットワーク ACL の `FMManaged` タグを `true` に設定します。このタグを使用して、独自のカスタムネットワーク ACL を Firewall Manager を通じて管理している ACL と区別します。

ネットワーク ACL の **FMManaged** タグの値を変更しないでください

Firewall Manager は、このタグを使用して、ネットワーク ACL で管理ステータスを設定および決定します。

Firewall Manager マネージドネットワーク ACL を持つサブネットの関連付けを変更しないでください。

Firewall Manager によって管理されているネットワーク ACL とサブネットの関連付けを手動で変更しないでください。そうする場合、Firewall Manager がこれらのサブネットの保護を管理する機能を無効にできます。Firewall Manager によって管理されるネットワーク ACL は、`true` の `FMManaged` タグ設定を検索することで特定できます。

Firewall Manager ポリシー管理からサブネットを削除するには、Firewall Manager ポリシースコープ設定を使用してサブネットを除外します。例えば、サブネットにタグを付け、そのタグをポリシースコープから除外できます。詳細については、「AWS Firewall Manager ポリシースコープの使用」を参照してください。

マネージドネットワーク ACL を更新するときは、Firewall Manager によって管理されるルールを変更しないでください。

Firewall Manager が管理するネットワーク ACL では、Firewall Manager でのネットワーク ACL ルールの使用とタグ付け で説明されている番号付けスキームに従って、カスタムルールをポリシールールから分離します。5,000 ~ 32,000 の数値を持つルールのみを追加または変更します。

アカウント制限にルールを追加しすぎないようにする

ネットワーク ACL の修正中、Firewall Manager は通常、ネットワーク ACL ルールの数を一時的に増加します。コンプライアンス違反の問題を回避するには、使用しているルールに十分な余裕があることを確認してください。詳細については、「Firewall Manager が非準拠のマネージドネットワーク ACL を修復する方法」を参照してください。

自動修復を無効にした状態で開始する

自動修復を無効にした状態で開始し、その後、自動修復が与える影響を判断するためにポリシーの詳細情報を確認してください。変更が適切であることを確認したら、ポリシーを編集して自動修復を有効にします。

Firewall Manager ネットワーク ACL ポリシーの規制

このセクションでは、Firewall Manager ネットワーク ACL ポリシーの使用に関する規制と制限事項を一覧表示します。

- 他のポリシーに比べて更新時間が遅い – Firewall Manager は、Amazon EC2 ネットワーク ACL API がリクエストを処理できる速度に制限があるため、一般的にネットワーク ACL ポリシーおよびポリシー変更の適用が他の Firewall Manager ポリシーよりも遅くなります。ポリシーの変更は、他の Firewall Manager ポリシーでの同様の変更よりも、特にポリシーを初めて追加するときに時間がかかる場合があります。
- 初期サブネット保護のために、Firewall Manager は古いポリシーを優先する – これは、Firewall Manager ネットワーク ACL ポリシーでまだ保護されていないサブネットにのみ適用されます。サブネットが同時に複数のネットワーク ACL ポリシーの範囲に入る場合、Firewall Manager は最も古いポリシーを使用してサブネットを保護します。

- ポリシーがサブネットの保護を停止する理由 – サブネットのネットワーク ACL を管理するポリシーは、次のいずれかが発生するまで管理を保持します。
  - サブネットはポリシーの範囲外になります。
  - ポリシーが削除されます。
  - サブネットの関連付けは、別の Firewall Manager ポリシーによって管理され、サブネットが範囲内にあるネットワーク ACL に手動で変更します。

トピック

- Firewall Manager でのネットワーク ACL ルールの使用とタグ付け
- Firewall Manager がサブネットのネットワーク ACL 管理を開始する方法
- Firewall Manager が非準拠のマネージドネットワーク ACL を修復する方法
- Firewall Manager ネットワーク ACL ポリシーの削除

Firewall Manager でのネットワーク ACL ルールの使用とタグ付け

このセクションでは、Firewall Manager によって管理されるネットワーク ACL ポリシールールの仕様とネットワーク ACL について説明します。

マネージドネットワーク ACL でのタグ付け

Firewall Manager は、マネージドネットワーク ACL に `true` の値を持つ `FMManaged` タグを付けます。Firewall Manager は、このタグ設定が適用されるネットワーク ACL に対してのみ修復を実行します。

ポリシーで定義するルール

ネットワーク ACL ポリシー仕様では、インバウンドトラフィックに対して最初と最後に実行するルールと、アウトバウンドトラフィックに対して最初と最後に実行するルールを定義します。

デフォルトでは、ポリシー内の最初と最後のルールの任意の組み合わせで使用できるように、最大 5 つのインバウンドルールを定義できます。同様に、最大 5 つのアウトバウンドルールを定義できます。これらの制限の詳細については、ソフトクォータ を参照してください。ネットワーク ACL 一般制限の詳細については、「Amazon VPC ユーザーガイド」の「Amazon VPC quotas on network ACLs」を参照してください。

ポリシールールにルール番号は割り当てません。代わりに、ルールを評価する順序でルールを指定し、Firewall Manager はその順序を使用して、管理するネットワーク ACL にルール番号を割り当てるようにします。

これ以外にも、Amazon VPC を介してネットワーク ACL 内のルールを管理する場合と同様に、ポリシーのネットワーク ACL ルールの仕様を管理します。Amazon VPC でのネットワーク ACL 管理の詳細については、「Amazon VPC ユーザーガイド」の「ACL を使用して、サブネットのトラフィックを制御する」および「ネットワーク ACL の動作」を参照してください。

マネージドネットワーク ACL のルール

Firewall Manager は、個々のアカウントマネージャーが定義するカスタムルールの前後にポリシーの最初と最後のルールを配置することで、管理するネットワーク ACL 内のルールを設定します。Firewall Manager は、カスタムルールの順序を保持します。最も低い番号のルールからルールを評価します。

Firewall Manager がネットワーク ACL を初めて作成するときは、次の番号でルールを定義します。

- 最初のルール: 1、2、… – Firewall Manager ネットワーク ACL ポリシーで定義されています。

  Firewall Manager は、ポリシー仕様で順序を付けたとおりにルールを使用して、1 から始まるルール番号を 1 の増分で割り当てます。
- カスタムルール: 5,000、5,100 … – Amazon VPC を介して個別のアカウントマネージャーによって管理されます。

  Firewall Manager は、5,000 からの後続のルールごとに 100 の増分でこれらのルールに番号を割り当てます。
- 最後のルール: … 32,765、32,766 – Firewall Manager ネットワーク ACL ポリシーで定義されます。

  Firewall Manager は、ポリシー仕様で付けた順序のとおりにルールを使用して、1 の増分で可能な限り高い数である 32766 で終わるルール番号を割り当てます。

ネットワーク ACL の初期化後、Firewall Manager は、個々のアカウントがマネージドネットワーク ACL で行う変更をコントロールしません。個々のアカウントは、ポリシーの最初と最後のルールの間にカスタムルールの番号が付けられたままで、最初と最後のルールが指定された順序を維持することを条件に、コンプライアンスを逸脱することなくネットワーク ACL を変更できます。ベストプラクティスとして、カスタムルールを管理するときは、このセクションで説明されている番号付けに従ってください。

Firewall Manager がサブネットのネットワーク ACL 管理を開始する方法

このセクションでは、Firewall Manager がサブネットのネットワーク ACL 管理を開始する方法について説明します。

Firewall Manager は、Firewall Manager が作成し、`true` に設定された `FMManaged` でタグを付けたネットワーク ACL とサブネットを関連付けると、そのサブネットのネットワーク ACL の管理を開始します。

ネットワーク ACL ポリシーに準拠するには、サブネットのネットワーク ACL が、ポリシーの最初のルールを最初に、ポリシーで指定された順序で、最後のルールを最後に、順番に、および中間に配置された他のカスタムルールを配置する必要があります。これらの要件は、すでにサブネットと関連している非マネージドネットワーク ACL またはマネージドネットワーク ACL によって満たされます。

Firewall Manager が、管理対象外のネットワーク ACL に関連付けられているサブネットにネットワーク ACL ポリシーを適用すると、Firewall Manager は実行可能なオプションを特定したときに停止して、次の順序でチェックします。

1. 関連付けられたネットワーク ACL が既に準拠している – 現在サブネットに関連付けられているネットワーク ACL が準拠している場合、Firewall Manager はその関連付けをそのままにして、サブネットのネットワーク ACL 管理を開始しません。

   Firewall Manager は、所有していないネットワーク ACL を変更したり管理したりしませんが、Firewall Manager が準拠している限り、Firewall Manager はそれをそのままにし、ポリシーに準拠しているかどうかを監視します。
2. 準拠したマネージドネットワーク ACL が利用可能 – Firewall Manager が、必要な設定に準拠するネットワーク ACL を既に管理している場合、これは選択可能になりです。修復が有効になっている場合、Firewall Manager はそれをサブネットと関連します。修復が無効になっている場合、Firewall Manager はサブネット非準拠としてマークし、修復オプションとしてネットワーク ACL 関連付けを置き換えます。
3. 新しい準拠したマネージドネットワーク ACL の作成 – 修復が有効になっている場合、Firewall Manager は新しいネットワーク ACL を作成し、サブネットに関連付けます。それ以外の場合、Firewall Manager はサブネット非準拠としてマークし、新しいネットワーク ACL を作成し、ネットワーク ACL 関連付けを置き換える修復オプションを提供します。

これらのステップが失敗すると、Firewall Manager はサブネットのコンプライアンス違反を報告します。

Firewall Manager は、サブネットが最初に対象範囲内に入り、サブネットのアンマネージド型ネットワーク ACL がコンプライアンス範囲外になった場合に、これらのステップに従います。

Firewall Manager が非準拠のマネージドネットワーク ACL を修復する方法

このセクションでは、マネージドネットワーク ACL がポリシーに準拠していない場合に、Firewall Manager はそれを修復する方法について説明します。Firewall Manager は、`FMManaged` タグが `true` に設定されたマネージドネットワーク ACL のみを修復します。Firewall Manager によって管理されていないネットワーク ACL について、初期ネットワーク ACL 管理 を参照してください。

修復は、最初、カスタム、および最後のルールと関連する場所を復元し、最初と最後のルールの順序を復元します。修復するとき、Firewall Manager は必ずしもルールをネットワーク ACL の初期化で使用するルール番号に移動しません。これらのルールカテゴリの初期番号設定と説明については、初期ネットワーク ACL 管理 を参照してください。

準拠ルールとルールの順序を確立するには、Firewall Manager がネットワーク ACL 内でルールを移動する必要がある場合があります。Firewall Manager は、既存の準拠ルールの順序を可能な限り維持することで、ネットワーク ACL の保護を維持します。例えば、一時的にルールを新しい場所に複製し、その後、元のルールを順序立てて削除することで、処理中に相対的な位置を維持することがあります。

このアプローチは設定を保護しますが、中間ルールにはネットワーク ACL にスペースも必要です。Firewall Manager がネットワーク ACL のルールの制限を超えると、修復が停止します。この場合、ネットワーク ACL はコンプライアンス違反のままになり、Firewall Manager はその理由を報告します。

アカウントが Firewall Manager によって管理されているネットワーク ACL にカスタムルールを追加し、それらのルールが Firewall Manager の修正に干渉する場合、Firewall Manager はネットワーク ACL 上の修復アクティビティを停止し、競合を報告します。

強制修復

ポリシーの自動修復を選択した場合は、最初のルールと最後のルールのどちらを強制的に修復するかも指定します。

Firewall Manager は、カスタムルールとポリシールールの間でトラフィック処理に競合が発生した場合、対応する強制修復設定を参照します。強制修復が有効になっている場合、競合があっても、Firewall Manager は修復を適用します。このオプションが有効になっていない場合、Firewall Manager は修復を中止します。いずれの場合も、Firewall Manager はルールの競合を報告しながら、修復オプションを提供します。

ルール数の要件と制限

修復中、Firewall Manager は、提供する保護を変更せずにルールを移動するために、一時的にルールを複製することがあります。

インバウンドルールまたはアウトバウンドルールのいずれの場合も、Firewall Manager が修復を実行するために必要なルールの最大数は、次のとおりです。

```
2 * (the number of rules defined in the policy for the traffic direction)
+
the number of custom rules defined in the network ACL for the traffic direction
```

ネットワーク ACL とネットワーク ACL ポリシーは、可変ルール制限によって制限されます。Firewall Manager が修復作業で制限に達すると、修復の試行を停止し、コンプライアンス違反を報告します。

Firewall Manager が修復アクティビティを実行するスペースを確保するために、制限の引き上げをリクエストできます。代わりに、ポリシーまたはネットワーク ACL の設定を変更して、使用するルールの数を減らすこともできます。

ネットワーク ACL 制限の詳細については、「Amazon VPC ユーザーガイド」の「Amazon VPC quotas on network ACLs」を参照してください。

修復に失敗した場合

ネットワーク ACL の更新中に、何らかの理由で Firewall Manager を停止する必要がある場合、変更を元に戻せず、代わりにネットワーク ACL を中間状態のままにします。`FMManaged` タグが `true` に設定されているネットワーク ACL に重複ルールが表示された場合、Firewall Manager はおそらくそれを修復しています。変更は一定の期間内に部分的に完了する可能性がありますが、Firewall Manager が修復を行う方法により、トラフィックが中断されたり、関連するサブネットの保護が軽減されたりすることはありません。

Firewall Manager がコンプライアンス以外のネットワーク ACL を完全に修復しない場合、関連するサブネットのコンプライアンス違反を報告し、可能な修復オプションを提案します。

修復に失敗した後の再試行

ほとんどの場合、Firewall Manager がネットワーク ACL の修正変更を完了しなかった場合、最終的には変更を再試行します。

この例外は、修復がネットワーク ACL ルール数制限または VPC ネットワーク ACL 数制限に達した場合です。Firewall Manager は、リソースを制限設定 AWS を超える修復アクティビティを実行できません。このような場合は、続行するには数を減らすか、制限を増やす必要があります。制限の詳細については、「Amazon VPC ユーザーガイド」の「Amazon VPC quotas on network ACLs」を参照してください。

Firewall Manager ネットワーク ACL コンプライアンスの報告

Firewall Manager は、範囲内のサブネットにアタッチされているすべてのネットワーク ACL のコンプライアンスをモニタリングして報告します。

一般的に、ルールの順序が間違っていたり、ポリシールールとカスタムルール間のトラフィック処理動作が競合したりする状況では、コンプライアンス違反が発生します。コンプライアンス違反の報告には、コンプライアンス違反と修復オプションが含まれます。

Firewall Manager は、他のポリシータイプと同様に、ネットワーク ACL ポリシーのコンプライアンス違反を報告します。コンプライアンス報告に関する詳細については、AWS Firewall Manager ポリシーのコンプライアンス情報の表示 を参照してください。

ポリシー更新時のコンプライアンス違反

ネットワーク ACL ポリシーを変更した後、Firewall Manager がポリシーの範囲内にあるネットワーク ACL を更新するまで、Firewall Manager はそれらのネットワーク ACL に非準拠としてマークを付けます。Firewall Manager は、ネットワーク ACL が厳密に言うと、準拠している場合でもこれを行います。

例えば、ポリシー仕様からルールを削除しても、スコープ内ネットワーク ACL にはまだ追加のルールがあるものの、それらのルール定義はポリシーに準拠している可能性があります。ただし、追加のルールは Firewall Manager が管理しているルールの一部であるため、Firewall Manager はそれらを現在のポリシー設定を違反していると見なします。これは、Firewall Manager が Firewall Manager マネージドネットワーク ACL に追加するカスタムルールを扱う方法と違います。

Firewall Manager ネットワーク ACL ポリシーの削除

このセクションでは、Firewall Manager ネットワーク ACL ポリシーを削除すると Firewall Manager で何が起こるかについて説明します。

Firewall Manager ネットワーク ACL ポリシーを削除すると、Firewall Manager はそのポリシーで管理しているすべてのネットワーク ACL の `FMManaged` タグ値を `false` に変更します。

さらに、ポリシーによって作成されたリソースをクリーンアップするかどうかを選択できます。クリーンアップを選択した場合、Firewall Manager は次のステップを順番に試行します。

1. 関連付けを元に戻す – Firewall Manager は、Firewall Manager が管理を開始する前に、関連付けられているネットワーク ACL にサブネットを関連付けようとします。
2. ネットワーク ACL から最初と最後のルールを削除 – 関連付けを変更できない場合、Firewall Manager はポリシーの最初と最後のルールを削除しようとし、サブネットに関連付けられているネットワーク ACL 内のカスタムルールのみを残します。
3. ルールや関連付けには何もしない – 上記のいずれもできない場合、Firewall Manager はネットワーク ACL とその関連付けをそのまま残します。

クリーンアップオプションを選択しない場合は、ポリシーが削除された後、各ネットワーク ACL を手動で管理する必要があります。ほとんどの場合、クリーンアップオプションを選択するのが最も簡単な方法です。

Firewall Manager での AWS Network Firewall ポリシーの使用

このセクションでは、Firewall Manager で AWS Network Firewall ポリシーを使用する方法について説明します。

AWS Firewall Manager Network Firewall ポリシーを使用して、 の組織全体の Amazon Virtual Private Cloud VPCs AWS Network Firewall ファイアウォールを管理できます AWS Organizations。一元管理されたファイアウォールを組織全体に適用することも、アカウントと VPC の選択したサブセットに適用することもできます。

Network Firewall は、VPC 内のパブリックサブネットのために、ネットワークトラフィックフィルタリング保護を提供します。Firewall Manager は、ポリシーで定義されている ファイアウォール管理 タイプに基づいてファイアウォールを作成および管理します。Firewall Manager は以下のファイアウォール管理モデルを提供します。

- 分散型 - ポリシーの範囲内にある各アカウントおよび VPC について、Firewall Manager は Network Firewall ファイアウォールを作成し、ファイアウォールエンドポイントを VPC サブネットにデプロイして、ネットワークトラフィックをフィルタリングします。
- 集約型 - Firewall Manager は、単一の Amazon VPC に単一の Network Firewall のファイアウォールを作成します。
- 既存のファイアウォールのインポート - Firewall Manager は、既存のファイアウォールを、単一の Firewall Manager ポリシーにインポートして管理します。ポリシーで管理されているインポートさ

れたファイアウォールに追加のルールを適用して、ファイアウォールがセキュリティ基準を満たすようにすることが可能です。

> **Note**
>
> Firewall Manager の Network Firewall ポリシーは、組織全体における VPC のための Network Firewall 保護を管理するために使用する Firewall Manager ポリシーです。
> Network Firewall 保護は、ファイアウォールポリシーと呼ばれる Network Firewall サービスのリソースで指定されます。

Network Firewall の使用については、「AWS Network Firewall デベロッパーガイド」を参照してください。

次のセクションでは、Firewall Manager の Network Firewall ポリシーを使用するための要件と、ポリシーの仕組みについて説明します。ポリシーの作成手順については、「の AWS Firewall Manager ポリシーの作成 AWS Network Firewall」を参照してください。

> **Important**
>
> リソース共有を有効にする必要があります。Network Firewall ポリシーは、組織内のアカウント全体で Network Firewall ルールグループを共有します。これを機能させるには、 AWS Organizations用にリソース共有を有効にする必要があります。リソース共有を有効にする方法については、「Network Firewall ポリシーと DNS Firewall ポリシーのリソース共有」を参照してください。

> **Important**
>
> Network Firewall ルールグループを定義する必要があります。新しい Network Firewall ポリシーを指定するときは、 AWS Network Firewall を直接使用する場合と同じようにファイアウォールポリシーを定義します。追加するステートレスルールグループ、デフォルトのステートレスアクション、およびステートフルルールグループを指定します。ルールグループをポリシーに含めるには、そのルールグループが Firewall Manager 管理者アカウントに既に存在している必要があります。Network Firewall ルールグループの作成については、「AWS Network Firewall ルールグループ」を参照してください。

トピック

- Firewall Manager がファイアウォールエンドポイントを作成する方法
- Firewall Manager がファイアウォールサブネットを管理する方法
- Firewall Manager が Network Firewall リソースを管理する方法
- Firewall Manager がポリシーの VPC ルートテーブルを管理およびモニタリングする方法
- AWS Network Firewall ポリシーの口グ記録の設定

Firewall Manager がファイアウォールエンドポイントを作成する方法

このセクションでは、Firewall Manager がファイアウォールエンドポイントを作成する方法について説明します。

ポリシーの Firewall 管理タイプによって、Firewall が Firewall Manager を作成する方法が決まります。ポリシーでは、[Distributed] (分散型) ファイアウォールや [Centralized] (集約型) ファイアウォールを作成することも、[import existing firewalls] (既存のファイアウォールのインポート) を選択することもできます。

- 分散型 - 分散デプロイモデルでは、Firewall Manager は、ポリシー範囲内にある各 VPC のためにエンドポイントを作成します。ファイアウォールエンドポイントを作成するアベイラビリティーゾーンを指定してエンドポイントの場所をカスタマイズすることも、Firewall Manager に、パブリックサブネットを使用してアベイラビリティーゾーンにエンドポイントを自動的に作成させることもできます。アベイラビリティーゾーンを手動で選択する場合は、アベイラビリティーゾーンごとに許可される CIDR のセットを制限するオプションがあります。Firewall Manager でエンドポイントを自動的に作成する場合は、サービスが VPC 内で単一のエンドポイントを作成するか、複数のファイアウォールエンドポイントを作成するかを指定する必要もあります。
  - 複数のファイアウォールエンドポイントの場合、Firewall Manager は、各アベイラビリティーゾーンにファイアウォールエンドポイントをデプロイします。ここには、インターネットゲートウェイ、または Firewall Manager が作成したファイアウォールエンドポイントルートがルートテーブル内に存在するサブネットがあります。これは、Network Firewall ポリシーのデフォルトのオプションです。
  - 単一のファイアウォールエンドポイントの場合、Firewall Manager は、インターネットゲートウェイルートを持つサブネット内の単一のアベイラビリティーゾーンにファイアウォールエンドポイントをデプロイします。このオプションでは、他のゾーンのトラフィックは、ファイアウォールによるフィルタリングの対象となるためにゾーン境界を越える必要があります。

> **Note**
>
> これらのオプションの両方で、IPv4/prefixlist ルートを含むルートテーブルに関連付けられたサブネットが必要です。Firewall Manager は、他のリソースをチェックしません。

- 集約型 - 集約型デプロイモデルを使用すると、Firewall Manager は、検査 VPC 内に 1 つ以上のファイアウォールエンドポイントを作成します。検査 VPC は、Firewall Manager がエンドポイントを起動する中央 VPC です。集約型デプロイモデルを使用する場合は、ファイアウォールエンドポイントを作成するアベイラビリティーゾーンも指定します。ポリシーを作成した後で検査 VPC を変更することはできません。別の検査 VPC を使用するには、新しいポリシーを作成する必要があります。
- 既存のファイアウォールのインポート - 既存のファイアウォールをインポートする場合、ポリシーに 1 つ以上の リソースセット を追加して、ポリシーで管理するファイアウォールを選択します。リソースセットは、組織内のアカウントによって管理されるリソース (この場合は Network Firewall 内の既存のファイアウォール) の集合体です。ポリシーでリソースセットを使用する前に、まずリソースセットを作成する必要があります。Firewall Manager のリソースセットについては、「Firewall Manager でのリソースのグループ化する」を参照してください。

  インポートされたファイアウォールを使用する場合は、以下の点に留意してください。

  - インポートしたファイアウォールが非対応になった場合、Firewall Manager は次の場合を除いて、自動的に違反の解決を試みます。
    - Firewall Manager と Network Firewall ポリシーのステートフルまたはステートレスのデフォルトアクションが一致しない場合。
    - インポートしたファイアウォールのファイアウォールポリシー内のルールグループが、Firewall Manager ポリシーのルールグループと同じ優先度を持つ場合。
    - インポートしたファイアウォールが、ポリシーのリソースセットに含まれていないファイアウォールに関連付けられたファイアウォールポリシーを使用している場合。これは、ファイアウォールに設定できるファイアウォールポリシーは 1 つだけですが、1 つのファイアウォールポリシーを複数のファイアウォールに関連付けることができるため発生する可能性があります。
    - インポートされたファイアウォールのファイアウォールポリシーに属する既存のルールグループのうち、Firewall Manager ポリシーでも指定されているものに、異なる優先順位が割り当てられる場合。

- ポリシーでリソースクリーンアップを有効にすると、Firewall Manager は FMS インポートポリシーに含まれているルールグループを、リソースセットの範囲内のファイアウォールから削除します。
- Firewall Manager の既存のファイアウォールのインポート管理タイプで管理されているファイアウォールは、一度に 1 つのポリシーによってのみ管理できます。同じリソースセットが複数のインポートネットワークファイアウォールポリシーに追加された場合、リソースセット内のファイアウォールは、リソースセットが追加された最初のポリシーによって管理され、2 番目のポリシーでは無視されます。
- 現在、Firewall Manager では、例外ポリシー設定をストリーミングしません。例外ポリシーのストリーミングの詳細については、「AWS Network Firewall デベロッパーガイド」の「例外ポリシーのストリーム」を参照してください。
- 既存のファイアウォールのインポートは、Transit ゲートウェイにアタッチされたファイアウォールのインポートをサポートしていません。

分散型または集約型のファイアウォール管理を使用しているポリシーのアベイラビリティーゾーンのリストを変更すると、Firewall Manager は、過去に作成されたが、現在はポリシーの範囲に含まれていないエンドポイントのクリーンアップを試みます。Firewall Manager は、範囲外のエンドポイントを参照するルートテーブルのルートがない場合にのみ、エンドポイントを削除します。Firewall Manager は、これらのエンドポイントを削除できないことが判明した場合、ファイアウォールサブネットを非準拠としてマークし、安全に削除できるようになるまでエンドポイントの削除を試行し続けます。

Firewall Manager がファイアウォールサブネットを管理する方法

このセクションでは、Firewall Manager がファイアウォールサブネットを管理する方法について説明します。

ファイアウォールサブネットは、ネットワークトラフィックをフィルタリングするファイアウォールエンドポイントのために Firewall Manager が作成する VPC サブネットです。各ファイアウォールエンドポイントは、専用 VPC サブネットでデプロイされる必要があります。Firewall Manager は、ポリシーの範囲内にある各 VPC に少なくとも 1 つのファイアウォールサブネットを作成します。

自動エンドポイント設定で分散型デプロイモデルを使用するポリシーの場合、Firewall Manager は、インターネットゲートウェイルートを持つサブネット、または Firewall Manager がポリシー用に作成したファイアウォールエンドポイントへのルートを持つサブネットを持つアベイラビリティーゾーンにのみ、ファイアウォールサブネットを作成します。詳細については、「Amazon VPC ユーザーガイド」の「VPC とサブネット」を参照してください。

Firewall Manager がファイアウォールエンドポイントを作成するアベイラビリティーゾーンを指定する分散型または集約型モデルのいずれかを使用するポリシーの場合、Firewall Manager は、アベイラビリティーゾーンに他のリソースがあるかどうかにかかわらず、それらの特定のアベイラビリティーゾーンにエンドポイントを作成します。

Network Firewall ポリシーを最初に定義する際に、Firewall Manager が範囲内の各 VPC 内のファイアウォールサブネットを管理する方法を指定します。この選択を後で変更することはできません。

自動エンドポイント設定で分散型デプロイモデルを使用するポリシーの場合、次のオプションから選択できます。

- パブリックサブネットを持つすべてのアベイラビリティーゾーンにファイアウォールサブネットをデプロイします。これがデフォルトの動作です。これにより、トラフィックフィルタリング保護の高可用性を実現できます。
- 1 つのアベイラビリティーゾーンに 1 つのファイアウォールサブネットをデプロイします。この選択により、Firewall Manager は、最もパブリックなサブネットを持つ VPC 内のゾーンを特定し、そこにファイアウォールサブネットを作成します。単一のファイアウォールエンドポイントは、VPC のすべてのネットワークトラフィックをフィルタリングします。これにより、ファイアウォールのコストは削減できますが、可用性は高くなく、他のゾーンからのトラフィックがフィルタリング対象となるためにはゾーン境界を越える必要があります。

カスタムエンドポイント設定または集約型デプロイモデルで分散デプロイモデルを使用するポリシーの場合、Firewall Manager は、ポリシーの範囲内にある指定されたアベイラビリティーゾーンにサブネットを作成します。

Firewall Manager がファイアウォールサブネットに使用する VPC CIDR ブロックを提供することも、ファイアウォールエンドポイントアドレスの選択の決定を Firewall Manager に任せることもできます。

- CIDR ブロックを指定しない場合、Firewall Manager は、使用可能な IP アドレスを VPC にクエリします。
- CIDR ブロックのリストを指定すると、Firewall Manager は、指定した CIDR ブロック内の新しいサブネットのみを検索します。/28 CIDR ブロックを使用する必要があります。Firewall Manager が作成する各ファイアウォールサブネットについて、CIDR ブロックリストをたどり、アベイラビリティーゾーンと VPC に適用可能で、かつ、利用可能なアドレスを持つ最初に見つかったリストを使用します。Firewall Manager が VPC 内のオープンスペースを見つけることができない場合 (制限の有無にかかわらず)、サービスは VPC 内にファイアウォールを作成しません。

Firewall Manager がアベイラビリティーゾーンで必要なファイアウォールサブネットを作成できない場合、そのサブネットをポリシーに非準拠であるものとしてマークします。ゾーンがこの状態にある間、別のゾーンのエンドポイントによるフィルタリングの対象となるためには、ゾーンのトラフィックがゾーン境界を越える必要があります。これは、単一のファイアウォールサブネットのシナリオに似ています。

Firewall Manager が Network Firewall リソースを管理する方法

このセクションでは、Firewall Manager で Network Firewall リソースを管理する方法について説明します。

Firewall Manager でポリシーを定義するときは、標準の AWS Network Firewall ファイアウォールポリシーのネットワークトラフィックフィルタリング動作を指定します。ステートレスおよびステートフル Network Firewall ルールグループを追加し、ステートレスルールと一致しないパケットのデフォルトアクションを指定します。でのファイアウォールポリシーの操作については AWS Network Firewall、AWS Network Firewall 「ファイアウォールポリシー」を参照してください。

分散型および集約型ポリシーの場合、Network Firewall ポリシーを保存すると、Firewall Manager は、ポリシーの範囲内にある各 VPC にファイアウォールとファイアウォールポリシーを作成します。Firewall Manager は、次の値を連結して、これらの Network Firewall リソースの名前を指定します。

- `FMManagedNetworkFirewall` または `FMManagedNetworkFirewallPolicy` のいずれかの固定文字列 (リソースタイプによる)。
- Firewall Manager ポリシー名。これは、ポリシーの作成時に割り当てる名前です。
- Firewall Manager ポリシー ID。これは Firewall Manager ポリシーの AWS リソース ID です。
- Amazon VPC ID。これは、Firewall Manager がファイアウォールとファイアウォールポリシーを作成する VPC の AWS リソース ID です。

Firewall Manager によって管理されるファイアウォールの名前の例を次に示します。

```
FMManagedNetworkFirewallEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

ファイアウォールポリシー名の例を次に示します。

```
FMManagedNetworkFirewallPolicyEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

ポリシーを作成した後、VPC のメンバーアカウントは、ファイアウォールポリシー設定またはルールグループを上書きすることはできませんが、Firewall Manager が作成したファイアウォールポリシーにルールグループを追加することはできます。

Firewall Manager がポリシーの VPC ルートテーブルを管理およびモニタリングする方法

このセクションでは、Firewall Manager がポリシーの VPC ルートテーブルを管理およびモニタリングする方法について説明します。

> **Note**
>
> ルートテーブル管理は、集約型デプロイモデルを使用するポリシーでは現在サポートされていません。

Firewall Manager がファイアウォールエンドポイントを作成すると、それらの VPC ルートテーブルも作成されます。ただし、Firewall Manager は VPC ルートテーブルを管理しません。ネットワークトラフィックを Firewall Manager によって作成されたファイアウォールエンドポイントに送信するように VPC ルートテーブルを設定する必要があります。Amazon VPC イングレスルーティングの拡張機能を使用して、新しいファイアウォールエンドポイントを通じてトラフィックをルーティングするようにルーティングテーブルを変更します。変更によって、保護するサブネットと外部の場所の間にファイアウォールエンドポイントを挿入する必要があります。実行が必要となる正確なルーティングは、アーキテクチャとそのコンポーネントによって異なります。

現在、Firewall Manager では、ファイアウォールをバイパスするインターネットゲートウェイ宛てのトラフィックについて、VPC ルートテーブルのルートをモニタリングできます。Firewall Manager は、NAT ゲートウェイなどの他のターゲットゲートウェイをサポートしていません。

VPC のルートテーブルの管理については、「Amazon Virtual Private Cloud ユーザーガイド」の「Managing route tables for your VPC」(VPC のルートテーブルの管理) を参照してください。Network Firewall のためのルートテーブル管理に関する情報については、「AWS Network Firewall デベロッパーガイド」の「AWS Network Firewallのためのルートテーブル設定」を参照してください。

ポリシーのモニタリングを有効にすると、Firewall Manager は VPC ルート設定を継続的にモニタリングし、その VPC のファイアウォール検査をバイパスするトラフィックについて警告します。サブネットにファイアウォールエンドポイントルートがある場合、Firewall Manager は次のルートを検索します。

- Network Firewall エンドポイントにトラフィックを送信するルート。
- Network Firewall エンドポイントからインターネットゲートウェイにトラフィックを転送するルート。
- インターネットゲートウェイから Network Firewall エンドポイントへのインバウンドルート。
- ファイアウォールサブネットからのルート。

サブネットに Network Firewall ルートがあるが、Network Firewall とインターネットゲートウェイのルートテーブルに非対称ルーティングがある場合、Firewall Manager はサブネットを非準拠としてレポートします。また、Firewall Manager は、Firewall Manager が作成したファイアウォールルートテーブルおよびサブネットのルートテーブルでインターネットゲートウェイへのルートを検出し、それらを非準拠として報告します。Network Firewall サブネットルートテーブルおよびインターネットゲートウェイルートテーブル内の追加ルートも、非準拠として報告されます。Firewall Manager は、違反タイプに応じて、ルート設定を準拠状態にするための修復アクションを提案します。Firewall Manager は、すべてのケースで提案を提供するわけではありません。例えば、お客様のサブネットに、Firewall Manager の外部で作成されたファイアウォールエンドポイントがある場合、Firewall Manager は修復アクションを提案しません。

デフォルトでは、Firewall Manager は、アベイラビリティーゾーンの境界を越えるトラフィックを検査のために非準拠としてマークします。ただし、VPC 内に単一のエンドポイントを自動的に作成するように選択した場合、Firewall Manager は、アベイラビリティーゾーンの境界を越えるトラフィックを非準拠としてマークしません。

カスタムエンドポイント設定で分散デプロイモデルを使用するポリシーの場合、あるアベイラビリティーゾーンからのものであって、アベイラビリティーゾーンの境界を越え、ファイアウォールエンドポイントがないトラフィックを、準拠または非準拠のいずれとしてマークするかを選択できます。

> **Note**
>
> - Firewall Manager は、IPv6 ルートやプレフィックスリストルートなど、IPv4 以外のルートに対する修復アクションを提案しません。
> - `DisassociateRouteTable` API コールを使用して行われた呼び出しは、検出に最大で 12 時間かかる場合があります。
> - Firewall Manager は、ファイアウォールエンドポイントを含むサブネットの Network Firewall ルートテーブルを作成します。Firewall Manager は、このルートテーブルに有効なインターネットゲートウェイと VPC のデフォルトルートだけが含まれていると仮定し

ます。このルートテーブル内の追加ルートまたは無効なルートは、非準拠とみなされます。

Firewall Manager ポリシーを設定するときに、[Monitor] (モニタリング) モードを選択すると、Firewall Manager はリソースの違反とリソースに関する修復の詳細を提供します。これらの推奨される修復アクションを使用して、ルートテーブル内のルートの問題を修正できます。[Off] (オフ) モードを選択した場合、Firewall Manager はルートテーブルのコンテンツをモニタリングしません。このオプションでは、VPC ルートテーブルを自ら管理できます。これらのリソース違反の詳細については、「AWS Firewall Manager ポリシーのコンプライアンス情報の表示」を参照してください。

> **Warning**
>
> ポリシーの作成時に Monitor under AWS Network Firewall route configuration を選択した場合、そのポリシーに対して無効にすることはできません。ただし、[Off] (オフ) を選択すると、後で有効にすることができます。

AWS Network Firewall ポリシーのログ記録の設定

このセクションでは、Network Firewall ポリシーの集中ログ記録を有効にして、組織内のトラフィックに関する詳細情報を取得する方法について説明します。フローログ記録を選択してネットワークトラフィックフローをキャプチャするか、アラートログ記録を選択して `DROP` または `ALERT` に設定されたルールアクションを持つルールに一致するトラフィックをレポートできます。 AWS Network Firewall ログ記録の詳細については、「AWS Network Firewall デベロッパーガイド」の「AWS Network Firewallからのネットワークトラフィックのログ記録」を参照してください。

ポリシーの Network Firewall ファイアウォールから Amazon S3 バケットにログを送信します。ログ記録を有効にすると、 はファイアウォール設定を更新して各設定済み Network Firewall のログを AWS Network Firewall 配信し、予約済み AWS Firewall Manager プレフィックス を使用して選択した Amazon S3 バケットにログを配信します`<policy-name>-<policy-id>`。

> **Note**
>
> このプレフィックスは、Firewall Manager によってログ記録設定が追加されたのか、またはアカウント所有者によって追加されたのかを判断するために、Firewall Manager によって使用されます。アカウント所有者が独自のカスタムログ記録に予約済みプレフィックスを使用しようとすると、Firewall Manager ポリシーのログ記録設定によって上書きされます。

Amazon S3 バケットを作成し、保存されているログを確認する方法の詳細については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 とは」を参照してください。

ログ記録を有効にするには、次の要件を満たす必要があります。

- Firewall Manager ポリシーで指定する Amazon S3 が存在している必要があります。
- アクセス許可を持っている必要があります。
  - `logs:CreateLogDelivery`
  - `s3:GetBucketPolicy`
  - `s3:PutBucketPolicy`
- ログ記録先である Amazon S3 バケットが に保存されているキーによるサーバー側の暗号化を使用している場合は AWS Key Management Service、Firewall Manager が CloudWatch Logs ロググループにログ記録できるように、 AWS KMS カスタマーマネージドキーに次のポリシーを追加する必要があります。

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt*",
        "kms:Decrypt*",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:Describe*"
    ],
    "Resource": "*"
}
```

AWS Network Firewall 一元ログ記録に使用できるのは、Firewall Manager 管理者アカウントのバケットのみであることに注意してください。

Network Firewall ポリシーで集中ログ記録を有効にすると、Firewall Manager はアカウントに対して次のアクションを実行します。

- Firewall Manager は、選択した S3 バケットの許可を更新して、ログ配信を許可します。

- Firewall Manager は、ポリシーの範囲内にある各メンバーアカウントのために、S3 バケットにディレクトリを作成します。各アカウントのログは `<bucket-name>/<policy-name>-<policy-id>/AWSLogs/<account-id>` にあります。

Network Firewall ポリシーのログ記録を有効にするには

1. Firewall Manager 管理者アカウントを使用して Amazon S3 バケットを作成します。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「バケットの作成」を参照してください。
2. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

3. ナビゲーションペインで、[Security Policies] (セキュリティポリシー) を選択します。
4. ログ記録を有効にする Network Firewall ポリシーを選択します。 AWS Network Firewall ログ記録の詳細については、 AWS Network Firewall デベロッパーガイドの「 からのネットワークトラフィックのログ記録 AWS Network Firewall」を参照してください。
5. [Policy details] (ポリシーの詳細) タブの [Policy rules] (ポリシールール) セクションで、[Edit] (編集) を選択します。
6. ログを有効にして集約するには、[Logging configuration] (ログ記録の設定) で 1 つ以上のオプションを選択します。
   - フローログを有効化および集約する
   - アラートログを有効化および集約する
7. ログの配信先とする Amazon S3 バケットを選択します。有効にするログタイプごとにバケットを選択する必要があります。両方のログタイプに同じバケットを使用できます。
8. (オプション) カスタムメンバーアカウントで作成されたログ記録をポリシーのログ記録設定に置き換える場合は、[Override existing logging configuration] (既存のログ設定を上書き) を選択します。
9. [Next] (次へ) を選択します。

10. 設定を確認し、[Save] (保存) を選択してポリシーに対する変更を保存します。

Network Firewall ポリシーのログ記録を無効にするには

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Security Policies] (セキュリティポリシー) を選択します。
3. ログ記録を無効にする Network Firewall ポリシーを選択します。
4. [Policy details] (ポリシーの詳細) タブの [Policy rules] (ポリシールール) セクションで、[Edit] (編集) を選択します。
5. [Logging configuration status] (ログ記録設定のステータス) で、[Enable and aggregate flow logs] (フローログを有効にして集約) および [Enable and aggregate alert logs] (アラートログを有効にして集約) の選択を解除します (選択されている場合)。
6. [Next] (次へ) を選択します。
7. 設定を確認し、[Save] (保存) を選択してポリシーに対する変更を保存します。

Firewall Manager の Amazon Route 53 Resolver DNS Firewall ポリシーを使用する

このページでは、DNS Firewall AWS Firewall Manager ポリシーを使用して、 の組織全体の Amazon Route 53 Resolver DNS Firewall ルールグループと Amazon Virtual Private Cloud VPCs間の関連付けを管理する方法について説明します AWS Organizations。一元管理されたルールグループを組織全体に適用することも、アカウントと VPC の選択したサブセットに適用することもできます。

DNS Firewall は、VPC のアウトバウンド DNS トラフィックのフィルタリングと規制を提供します。DNS Firewall のルールグループで再利用可能なフィルタリングルールのコレクションを作成し、そのルールグループを VPC に関連付けます。Firewall Manager ポリシーを適用すると、ポリシーの範囲内にある各アカウントおよび VPC について、Firewall Manager は、Firewall Manager ポ

リシーで指定した関連付けの優先順位の設定を使用して、ポリシー内の各 DNS Firewall ルールグループと、ポリシーの範囲内にある各 VPC の間の関連付けを作成します。

DNS Firewall の使用方法については、「Amazon Route 53 デベロッパーガイド」の「Amazon Route 53 Resolver DNS Firewall」を参照してください。

次のセクションでは、Firewall Manager の DNS Firewall ポリシーを使用するための要件と、ポリシーの仕組みについて説明します。ポリシーの作成手順については、「Amazon Route 53 Resolver DNS Firewall の AWS Firewall Manager ポリシーの作成」を参照してください。

> **Important**
>
> リソース共有を有効にする必要があります。DNS Firewall ポリシーは、組織内のアカウント全体で DNS Firewall ルールグループを共有します。これを機能させるには、 でリソース共有が有効になっている必要があります AWS Organizations。リソース共有を有効にする方法については、「Network Firewall ポリシーと DNS Firewall ポリシーのリソース共有」を参照してください。

> **Important**
>
> DNS Firewall ルールグループを定義する必要があります。新しい DNS Firewall ポリシーを指定する際に、Amazon Route 53 Resolver DNS Firewall を直接使用する場合と同じようにルールグループを定義します。ルールグループをポリシーに含めるには、そのルールグループが Firewall Manager 管理者アカウントに既に存在している必要があります。DNS Firewall ルールグループの作成については、「DNS Firewall のルールグループとルール」を参照してください。

優先順位が最低のルールグループと最高のルールグループの関連付けを定義します

Firewall Manager の DNS Firewall ポリシーを通じて管理する DNS Firewall ルールグループの関連付けには、VPC について、優先度が最低の関連付けと優先度が最高の関連付けが含まれます。ポリシー設定では、これらは最初と最後のルールグループとして表示されます。

DNS Firewall は、VPC の DNS トラフィックを次の順序でフィルタリングします。

1. Firewall Manager の DNS Firewall ポリシーで定義されている最初のルールグループ。有効な値は 1 ~ 99 です。

2. DNS Firewall を通じて個々のアカウントマネージャーによって関連付けられた DNS Firewall ルールグループ。
3. Firewall Manager の DNS Firewall ポリシーで定義されている最後のルールグループ。有効な値は 9,901 から 10,000 の間です。

Firewall Manager が作成するルールグループの関連付けの名前を付ける方法

DNS Firewall ポリシーを保存するときに自動修復を有効にした場合、Firewall Manager は、ポリシーで指定したルールグループとポリシーの範囲内にある VPC の間に DNS Firewall の関連付けを作成します。Firewall Manager は、次の値を連結することにより、これらの関連付けに名前を付けます。

- 固定文字列、`FMManaged_`。
- Firewall Manager ポリシー ID。これは Firewall Manager ポリシーの AWS リソース ID です。

Firewall Manager によって管理されるファイアウォールの名前の例を次に示します。

```
FMManaged_EXAMPLEDNSFirewallPolicyId
```

ポリシーを作成した後、VPC のアカウント所有者がファイアウォールポリシー設定またはルールグループの関連付けを上書きすると、Firewall Manager は、ポリシーを非準拠としてマークし、是正措置の提案を試みます。アカウント所有者は、DNS Firewall ポリシーの範囲内の VPC に他の DNS Firewall ルールグループを関連付けることができます。個々のアカウント所有者によって作成された関連付けには、最初と最後のルールグループの関連付けの間で優先順位の設定が必要です。

Firewall Manager DNS Firewall ポリシーからルールグループを削除する

ルールグループの削除

Firewall Manager DNS Firewall ポリシーからルールグループを削除するには、次の手順を実行する必要があります。

> **Important**
>
> Firewall Manager DNS Firewall ポリシーからルールグループを削除すると、DNS Firewall ルールグループからルールグループを削除するかどうかにかかわらず、ポリシーが適用され

た VPCs からその効果が削除されます。ルールグループの削除は永続的なアクションであり、元に戻すことはできません。

1. ルールグループを Firewall Manager DNS Firewall ポリシーから削除します。
2. ルールグループの共有を解除します AWS Resource Access Manager。自己所有のルールグループを共有解除するには、リソース共有からルールグループを削除する必要があります。これを行うには、 AWS RAM コンソールまたは CLI AWS を使用します。リソースの共有解除ついては、「AWS RAM ユーザーガイド」の「AWS RAM内のリソース共有を更新する」を参照してください。
3. DNS Firewall コンソールまたは AWS CLI を使用してルールグループを削除します。

Palo Alto Networks Cloud NGFW ポリシーを Firewall Manager で使用する

Palo Alto Networks Cloud Next Generation Firewall (NGFW) は、 AWS Firewall Manager ポリシーに使用できるサードパーティーのファイアウォールサービスです。Palo Alto Networks Cloud NGFW for Firewall Manager を使用すると、すべての AWS アカウントに Palo Alto Networks Cloud NGFW リソースとルールスタックを作成して一元的にデプロイできます。

Firewall Manager で Palo Alto Networks Cloud NGFW を使用するには、まず AWS Marketplace の Palo Alto Networks Cloud NGFW Pay-As-You-Go サービスにサブスクライブします。サブスクライブ後、Palo Alto Networks Cloud NGFW サービスで一連のステップを実行して、アカウントと Cloud NGFW 設定を構成します。次に、Firewall Manager Cloud FMS ポリシーを作成して、 AWS 組織内のすべてのアカウントで Palo Alto Networks Cloud NGFW リソースとルールを一元的にデプロイおよび管理します。

Firewall Manager ポリシーを作成する手順については、「Palo Alto Networks Cloud NGFW の AWS Firewall Manager ポリシーの作成」を参照してください。Firewall Manager 用に Palo Alto Networks Cloud NGFW を設定および管理する方法については、Palo Alto Networks Palo Alto Networks Cloud NGFW on AWS のドキュメントを参照してください。サポートされている AWS リージョンについては、AWS 「サポートされているリージョンとゾーンの Cloud NGFW」を参照してください。

Firewall Manager に Fortigate Cloud Native Firewall (CNF) as a Service ポリシーを使用する

Fortigate Cloud Native Firewall (CNF) as a Service は、 AWS Firewall Manager ポリシーに使用できるサードパーティーのファイアウォールサービスです。Fortigate CNF は、クラウドネットワークの

保護とセキュリティポリシーの管理を容易にする次世代のファイアウォールサービスです。Fortigate CNF for Firewall Manager を使用すると、Fortigate CNF リソースとポリシーセットを作成し、すべての AWS アカウントに一元的にデプロイできます。

Firewall Manager で Fortigate CNF を使用するには、まず AWS Marketplace のサービスとして Fortigate Cloud Native Firewall (CNF) にサブスクライブします。サブスクライブ後、Fortigate CNF サービスで一連の手順を実行し、グローバルポリシーセットやその他の設定を構成します。次に、Firewall Manager ポリシーを作成して、 AWS Organizations 内のすべてのアカウントに Fortigate CNF リソースを一元的にデプロイおよび管理します。

Fortigate CNF Firewall Manager ポリシーを作成する手順については、「サービスとしての Fortigate Cloud Native Firewall (CNF) の AWS Firewall Manager ポリシーの作成」を参照してください。Firewall Manager で使用するために Fortigate CNF を設定および管理する方法については、Fortigate CNF のドキュメントを参照してください。

Network Firewall ポリシーと DNS Firewall ポリシーのリソース共有

Firewall Manager Network Firewall および DNS Firewall ポリシーを管理するには、 AWS Organizations で とのリソース共有を有効にする必要があります AWS Resource Access Manager。これにより、Firewall Manager は、これらのポリシータイプを作成するときに、アカウント全体で保護をデプロイできます。

リソース共有を有効にするには、「AWS Resource Access Manager ユーザーガイド」の「AWS Organizations内でリソース共有を有効にする」の手順に従ってください。

リソース共有に関する問題

AWS RAM を使用してリソース共有を有効にする場合、またはリソース共有を必要とする Firewall Manager ポリシーで作業している場合に、リソース共有で問題が発生することがあります。

これらの問題の例には次が含まれます。

- 共有を有効にする手順に従うと、 AWS RAM コンソールで「 との共有を有効にする AWS Organizations」という選択肢がグレー表示され、選択できなくなります。
- リソース共有を必要とするポリシーで Firewall Manager を使用している場合、ポリシーは非準拠としてマークされ、リソース共有または AWS RAM が有効になっていないことを示すメッセージが表示されます。

リソースの共有で問題が発生した場合は、次の手順を使用してリソース共有の有効化を試みます。

再試行して、リソース共有を有効にする

- 再試行し、次のいずれかのオプションを使用して共有を有効にします。
  - (オプション) AWS RAM コンソールから、AWS Resource Access Manager 「 ユーザーガイド」の「 との共有を有効にする AWS Organizations」の手順に従います。
  - (オプション) AWS RAM API を使用して、 を呼び出しますEnableSharingWithAwsOrganization。「EnableSharingWithAwsOrganization」のドキュメントを参照してください。

Firewall Manager のマネージドリストの使用

このセクションでは、マネージドリストとは何か、またその使用方法について説明します。

マネージドアプリケーションおよびプロトコルリストにより、 AWS Firewall Manager コンテンツ監査セキュリティグループポリシーの設定と管理が合理化されます。ポリシーが許可または禁止するプロトコルとアプリケーションを定義するために、マネージドリストを使用します。コンテンツ監査セキュリティグループポリシーの詳細については、「Firewall Manager のコンテンツ監査セキュリティグループポリシーの使用」を参照してください。

コンテンツ監査セキュリティグループポリシーでは、次のタイプのマネージドリストを使用できます。

- Firewall Manager のアプリケーションリストとプロトコルリスト - Firewall Manager は、これらのリストを管理します。
  - アプリケーションリストには、一般ユーザーに対して許可または拒否される必要がある一般的に使用されるアプリケーションを記述する FMS-Default-Public-Access-Apps-Allowed と FMS-Default-Public-Access-Apps-Denied が含まれます。
  - プロトコルリストには、一般ユーザーに対して許可される必要がある一般的に使用されるプロトコルリストである FMS-Default-Protocols-Allowed が含まれます。Firewall Manager が管理するリストはすべて使用できますが、編集や削除はできません。
- カスタムアプリケーションリストとプロトコルリスト - これらのリストを管理できます。必要な設定を使用して、どちらのタイプのリストも作成できます。独自のカスタムマネージドリストを完全に制御でき、必要に応じて作成、編集、削除できます。

> **Note**
>
> 現在、Firewall Manager は、カスタムマネージドリストが削除されると、そのカスタムマネージドリストへの参照をチェックしません。つまり、アクティブなポリシーによって使用されている場合でも、カスタムマネージドアプリケーションリストまたはプロトコルリストを削除できます。これにより、ポリシーが機能しなくなる可能性があります。アプリケーションリストまたはプロトコルリストは、アクティブなポリシーによって参照されていないことを検証した後にのみ削除します。

マネージドリストは AWS リソースです。カスタムマネージドリストにタグを付けることができます。Firewall Manager のマネージドリストにタグを付けることはできません。

マネージドリストのバージョニング

カスタムマネージドリストにはバージョンがありません。カスタムリストを編集すると、そのリストを参照するポリシーは、更新されたリストを自動的に使用します。

Firewall Manager のマネージドリストはバージョニングされています。Firewall Manager サービスチームは、セキュリティのベストプラクティスをリストに適用するために、必要に応じて新しいバージョンを公開します。

ポリシーで Firewall Manager マネージドリストを使用する場合、次のようにバージョニング戦略を選択します。

- 利用可能な最新バージョン – リスト用に明示的なバージョン設定を指定しない場合、ポリシーは自動的に最新バージョンを使用します。コンソールで使用できる唯一のオプションです。
- 明示的なバージョン - リストのバージョンを指定すると、ポリシーでそのバージョンが使用されます。ポリシーは、バージョン設定を変更するまで、指定したバージョンにロックされたままとなります。バージョンを指定するには、CLI またはいずれかの SDK など、コンソールの外部でポリシーを定義する必要があります。

リストのバージョン設定の選択の詳細については、「コンテンツ監査セキュリティグループポリシーでのマネージドリストの使用」を参照してください。

コンテンツ監査セキュリティグループポリシーでのマネージドリストの使用

コンテンツ監査セキュリティグループポリシーを作成するときに、マネージド監査ポリシールールを使用するように選択できます。このオプションの一部の設定では、マネージドアプリケーションリストまたはプロトコルリストが必要です。これらの設定の例には、セキュリティグループルールで許可されるプロトコルや、アプリケーションがインターネットにアクセスできるプロトコルが含まれます。

マネージドリストを使用する各ポリシー設定には、次の制限が適用されます。

- Firewall Manager のマネージドリストは、任意の設定について最大 1 個指定できます。デフォルトでは、最大 1 個のカスタムリストを指定できます。カスタムリストの上限はソフトクォータなので、その制限の引き上げをリクエストできます。詳細については、「AWS Firewall Manager クォータ」を参照してください。
- コンソールで、Firewall Manager のマネージドリストを選択すると、バージョンを指定できません。ポリシーは、常に最新バージョンのリストを使用します。バージョンを指定するには、CLI またはいずれかの SDK など、コンソールの外部でポリシーを定義する必要があります。Firewall Manager マネージドリストのバージョニングについては、「マネージドリストのバージョニング」を参照してください。

コンソールを通じたコンテンツ監査セキュリティグループポリシーの作成については、「コンテンツ監査セキュリティグループポリシーの作成」を参照してください。

Firewall Managerでのカスタムマネージドリストの作成

カスタムマネージドアプリケーションリストまたはカスタムマネージドプロトコルリストを作成するには、次の手順に従います。

トピック

- カスタムマネージドアプリケーションリストの作成
- カスタムマネージドプロトコルリストの作成

カスタムマネージドアプリケーションリストの作成

カスタムマネージドアプリケーションリストを作成するには

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Application lists] (アプリケーションリスト) を選択します。
3. [Application lists] (アプリケーションリスト) ページで、[Create application list] (アプリケーションリストを作成) を選択します。
4. [Create application list] (アプリケーションリストを作成) ページで、リストに名前を付けます。プレフィックス `fms-` は Firewall Manager 用に予約されているため、使用しないでください。
5. プロトコルとポート番号を指定するか、[Type] (タイプ) ドロップダウンからアプリケーションを選択して、アプリケーションを指定します。アプリケーションの仕様に名前を付けます。
6. 必要に応じて [Add another] (別のものを追加) を選択し、リストが完成するまでアプリケーションに関する情報を入力します。
7. (オプション) リストにタグを適用します。
8. [Save] (保存) を選択してリストを保存し、[Application lists] (アプリケーションリスト) ページに戻ります。

カスタムマネージドプロトコルリストの作成

カスタムマネージドプロトコルリストを作成するには

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

> **Note**
>
> Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Protocol lists] (プロトコルリスト) を選択します。
3. [Protocol lists] (プロトコルリスト) ページで、[Create protocol list] (プロトコルリストを作成) を選択します。
4. プロトコルリスト作成ページで、リストに名前を付けます。プレフィックス `fms-` は Firewall Manager 用に予約されているため、使用しないでください。
5. プロトコルを指定します。
6. 必要に応じて [Add another] (別のものを追加) を選択し、リストが完成するまでプロトコルに関する情報を入力します。
7. (オプション) リストにタグを適用します。
8. [Save] (保存) を選択してリストを保存し、[Protocol lists] (プロトコルリスト) ページに戻ります。

Firewall Manager でのマネージドリストの表示

アプリケーションリストまたはプロトコルリストを表示するには

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Application lists] (アプリケーションリスト) または [Protocol lists] (プロトコルリスト) を選択します。

   ページには、使用可能な、選択したタイプのリストがすべて表示されます。Firewall Manager が管理するリストには、[ManagedList] 列に [Y] があります。

3. リストの詳細を表示するには、その名前を選択します。詳細ページには、リストのコンテンツとタグが表示されます。

   Firewall Manager のマネージドリストの場合、[Version] (バージョン) ドロップダウンを選択して、使用可能なバージョンを確認することもできます。

Firewall Manager でのカスタムマネージドリストの削除

カスタムマネージドリストを削除できます。Firewall Manager が管理するリストを編集または削除することはできません。

> **Note**
>
> 現在、Firewall Manager は、カスタムマネージドリストを削除すると、そのカスタムマネージドリストへの参照をチェックしません。つまり、アクティブなポリシーによって使用されている場合でも、カスタムマネージドアプリケーションリストまたはプロトコルリストを削除できます。これにより、ポリシーが機能しなくなる可能性があります。アプリケーションリストまたはプロトコルリストは、アクティブなポリシーによって参照されていないことを確認した後にのみ削除してください。

カスタムマネージドアプリケーションまたはプロトコルリストを削除するには

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. 次の操作を実行して、削除するリストがいずれの監査セキュリティグループポリシーでも使用中ではないことを確認します。

   a. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。

b. [AWS Firewall Manager policies] (ポリシー) ページで、監査セキュリティグループを選択して編集し、削除するカスタムリストへの参照をすべて削除します。

   監査セキュリティグループポリシーで使用されているカスタムマネージドリストを削除すると、そのリストを使用しているポリシーが機能しなくなる可能性があります。

3. ナビゲーションペインで、削除するリストのタイプに応じて、[Application lists] (アプリケーションリスト) または [Protocol lists] (プロトコルリスト) を選択します。
4. リストページで、削除するカスタムリストを選択し、[Delete] (削除) を選択します。

Firewall Manager でのリソースのグループ化する

このセクションでは、リソースセットとは何かを説明し、また、リソースセットの使用に関する考慮事項を一覧表示します。

AWS Firewall Manager Anresource セットは、Firewall Manager ポリシーでグループ化および管理できるファイアウォールなどのリソースのコレクションです。リソースセットを使用すると、組織内のメンバーは、ポリシーで管理するリソースをきめ細かく制御できます。リソースセットを使用するには、コンソールまたは PutResourceSet API を使用してリソースセットを作成し、Firewall Manager ポリシーに追加します。

次のリソースタイプとセキュリティポリシータイプのリソースセットを作成および管理できます。

リソースタイプ	Firewall Manager のセキュリティポリシータイプ
AWS Network Firewall - ファイアウォール	Network Firewall ポリシー - リソースセットを使用して、Network Firewall から既存のファイアウォールをインポートします。Network Firewall ポリシーでリソースセットを使用する方法については、の AWS Firewall Manager ポリシーの作成 AWS Network Firewall手順の「既存のファイアウォールのインポート」ステップを参照してください。

次のセクションでは、リソースセットの作成と削除の要件について説明します。

トピック

- Firewall Manager でリソースセットを操作するときの考慮事項
- Firewall Manager でのリソースセットの作成
- Firewall Manager でのリソースセットの削除

Firewall Manager でリソースセットを操作するときの考慮事項

リソースセットを使用するときに、次の考慮事項に注意してください。

存在しないリソースへの参照

リソースセットにリソースを追加する際は、Amazon リソースネーム (ARN) を使用してリソースへの参照を作成します。Firewall Manager は Amazon リソースネーム (ARN) が正しい形式であるかどうかを検証するものの、参照先リソースが存在するかどうかは確認しません。リソースが存在しないのに ARN の検証を通過した場合、Firewall Manager はリソースセットにリソース参照を含めます。同じ ARN を持つ新しいリソースが後で作成された場合、Firewall Manager はリソースセットの関連ポリシーのルールグループを新しいリソースに適用します。

削除されたリソース

リソースセット内のリソースが削除されても、リソースへの参照は、Firewall Manager 管理者によって削除されるまでリソースセット内に残ります。

AWS Organizations 組織を離れるメンバーアカウントが所有するリソース

メンバーアカウントが組織を離れると、そのメンバーアカウントが所有するリソースへの参照はすべてリソースセットに残りますが、リソースセットが関連付けられているポリシーでは管理されなくなります。

複数のポリシーへの関連付け

リソースセットは複数のポリシーに関連付けることができますが、すべてのポリシータイプが同じリソースを管理する複数のポリシーをサポートしているわけではありません。サポートされていないシナリオについては、特定のポリシータイプのドキュメントを参照してください。

Firewall Manager でのリソースセットの作成

リソースセットを作成するには (コンソール)

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

   > **Note**
   >
   > Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Resources sets] (リソースセット) を選択します。
3. [Create resource set] (リソースセットの作成) を選択します。

4. [Resource set name] (リソースセット名) には、わかりやすい名前を入力します。
5. (オプション) リソースセットの [Description] (説明) を入力します。
6. [次へ] を選択します。
7. [リソースを選択] で [AWS アカウント ID] を選択し、[リソースを選択] を選択して、このアカウントが所有および管理するリソースをリソースセットに追加します。リソースを選択したら、[Add] (追加) を選択してリソースをリソースセットに追加します。
8. [次へ] を選択します。
9. [Resource set tags] (リソースセットタグ) の場合は、リソースセットに必要な識別タグを追加します。タグの詳細については、「タグエディタの使用」を参照してください。
10. [次へ] を選択します。
11. 新しいリソースセットを確認します。変更するには、変更する部分で [Edit] (編集) を選択します。これにより、作成ウィザードの対応するステップに戻ります。設定が適切であることを確認したら、[Create resource set] (リソースセットの作成) を選択します。

Firewall Manager でのリソースセットの削除

リソースセットを削除する前に、そのリソースセットを使用するすべてのポリシーからリソースセットの関連付けを解除する必要があります。リソースグループの関連付けは、コンソールまたは PutPolicy API からポリシーの詳細ページで解除できます。

リソースセットを削除するには (コンソール)

1. ナビゲーションペインで、[Resources sets] (リソースセット) を選択します。
2. 削除するリソースセットの横にあるオプションを選択します。
3. [Delete] (削除) をクリックします。

AWS Firewall Manager ポリシーのコンプライアンス情報の表示

このセクションでは、 AWS Firewall Manager ポリシーの範囲内にあるアカウントとリソースのコンプライアンスステータスを表示するためのガイダンスを提供します。クラウドのセキュリティとコンプライアンスを維持するために で実施されているコントロールの詳細については、 AWS 「」を参照してくださいFirewall Manager のコンプライアンス検証。

> **Note**
>
> Firewall Manager がポリシーコンプライアンスをモニタリングするには、保護されたリソースの設定変更を継続的に記録 AWS Config する必要があります。 AWS Config 設定では、記録頻度をデフォルト設定である Continuous に設定する必要があります。

> **Note**
>
> 保護されたリソースで適切なコンプライアンス状態を維持するには、Firewall Manager 保護の状態を自動または手動で繰り返し変更しないでください。Firewall Manager は からの情報 AWS Config を使用して、リソース設定の変更を検出します。変更が十分に迅速に適用されると、 AWS Config はそれらの一部の追跡を失い、Firewall Manager のコンプライアンスまたは修復状態に関する情報が失われる可能性があります。
> Firewall Manager で保護するリソースのコンプライアンスまたは修復ステータスが正しくない場合は、まず Firewall Manager の保護を変更またはリセットするプロセスを実行していないことを確認し、関連する設定ルールを再評価してリソース AWS Config の追跡を更新します AWS Config。
> ポリシーまたは対象範囲内のリソースを変更すると、コンプライアンスステータスと詳細の更新が表示されるまでに数分かかる場合があります。

すべての AWS Firewall Manager ポリシーについて、ポリシーの範囲内にあるアカウントとリソースのコンプライアンスステータスを表示できます。ポリシーの設定がアカウントまたはリソースの設定で反映されている場合、そのアカウントまたはリソースは、Firewall Manager ポリシーに準拠しています。各ポリシータイプには独自のコンプライアンス要件があります。これは、ポリシーを定義するときにチューニングできます。一部のポリシーでは、セキュリティリスクをより良く理解および管理するのに役立てるために、範囲内のリソースの詳細な違反情報を表示することもできます。

ポリシーのコンプライアンス情報を表示するには

1. Firewall Manager 管理者アカウント AWS マネジメントコンソール を使用して にサインインし、 で Firewall Manager コンソールを開きますhttps://console.aws.amazon.com/wafv2/fmsv2。Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

> **Note**
>
> Firewall Manager 管理者アカウントの設定については、「AWS Firewall Manager 前提条件」を参照してください。

2. ナビゲーションペインで、[Security policies] (セキュリティポリシー) を選択します。
3. ポリシーを選択します。ポリシーページの [Accounts and resources] (アカウントとリソース) タブで、Firewall Manager は、ポリシーの範囲内にあるアカウントと範囲外にあるアカウントでグループ化された、組織内のアカウントを一覧表示します。

   [Accounts within policy scope] (ポリシーの範囲内のアカウント) ペインには、各アカウントのコンプライアンスステータスが一覧表示されます。[Compliant] (準拠) ステータスは、ポリシーがアカウントのすべての範囲内のリソースに正常に適用されたことを示します。[Noncompliant] (非準拠) ステータスは、ポリシーがアカウントの 1 つ以上の範囲内のリソースに適用されていないことを示します。
4. 非準拠のアカウントを選択します。アカウントページで、Firewall Manager は、準拠していない各リソースの ID と種類、およびリソースがポリシーに違反している理由の一覧を表示します。

> **Note**
>
> リソースタイプ `AWS::EC2::NetworkInterface` (ENI) および `AWS::EC2::Instance` の場合、Firewall Manager は限られた数の非準拠リソースを表示する場合があります。その他の非準拠のリソースを一覧表示するには、対象のアカウントについて最初に表示されるリソースを修正します。

5. Firewall Manager ポリシータイプがコンテンツ監査セキュリティグループポリシーである場合、リソースの詳細な違反情報にアクセスできます。

   違反の詳細を表示するには、リソースを選択します。

> **Note**
>
> 詳細なリソース違反ページが追加される前に、Firewall Manager が非準拠であると判断したリソースには、違反の詳細がない場合があります。

リソースページに、Firewall Manager は、リソースタイプに応じて、違反に関する具体的な詳細を一覧表示します。

- **`AWS::EC2::NetworkInterface`** (ENI) – Firewall Manager は、リソースが準拠していないセキュリティグループに関する情報を表示します。セキュリティグループを選択すると、その詳細が表示されます。
- **`AWS::EC2::Instance`** - Firewall Manager は、非準拠の EC2 インスタンスにアタッチされている ENI を表示します。また、リソースが準拠していないセキュリティグループに関する情報を表示します。セキュリティグループを選択すると、その詳細が表示されます。
- **`AWS::EC2::SecurityGroup`** - Firewall Manager は、次の違反の詳細を表示します。
  - [Noncompliant security group rule] (非準拠のセキュリティグループルール) – 違反しているルール (プロトコル、ポート範囲、IP CIDR 範囲、説明など)。
  - [Referenced rule] (参照されるルール) – 非準拠のセキュリティグループのルールが違反する監査セキュリティグループのルールとその詳細。
  - [Violation reasons] (違反の理由) – 違反の検出結果の説明。
  - [Remediation action] (修復アクション) – 実行する推奨アクション。Firewall Manager が安全な修復アクションを決定できない場合、このフィールドは空白です。
- **`AWS::EC2::Subnet`** – これは、Network Firewall ポリシーに使用されます。

  Firewall Manager は、サブネット ID、VPC ID、アベイラビリティーゾーンを表示します。該当する場合、Firewall Manager には違反に関する追加情報が含まれます。違反の説明のコンポーネントには、リソースの予想される状態の説明、現在の非準拠状態、および使用可能な場合は、不一致の原因の説明が含まれます。

  Network Firewall 違反

  - [management violations] (ルート管理違反) – モニタリングモードを使用する Network Firewall ポリシーの場合、Firewall Manager は、基本的なサブネット情報に加えて、サブネット、インターネットゲートウェイ、および Network Firewall のサブネットルートテーブルの想定ルートと実際のルートを表示します。Firewall Manager は、実際のルートがルートテーブルの想定されるルートと一致しない場合、違反がある旨のアラートを発信します。
  - [Remediation actions for route management violations] (ルート管理違反の修正アクション) – モニタリングモードを使用する Network Firewall ポリシーの場合、Firewall Manager は、違反のあるルート設定に対して可能な修正アクションを提案します。

例えば、サブネットはファイアウォールエンドポイントを介してトラフィックを送信することが想定されていますが、現在のサブネットはインターネットゲートウェイに直接トラフィックを送信しています。これは、ルート管理違反です。この場合の推奨される修復は、順序付けられたアクションのリストである場合があります。1 つ目の推奨事項は、必要なルートを Network Firewall サブネットのルートテーブルに追加して、発信トラフィックをインターネットゲートウェイに転送し、VPC 内の宛先の着信トラフィックを `local` に転送することです。2 つ目の推奨事項は、サブネットのルートテーブル内のインターネットゲートウェイルートまたは無効な Network Firewall ルートを置き換えて、発信トラフィックをファイアウォールエンドポイントに送信することです。3 つ目の推奨事項は、受信トラフィックをファイアウォールエンドポイントに転送するために、インターネットゲートウェイのルートテーブルに必要なルートを追加することです。

- **`AWS::EC2::InternetGateway`** - これは、モニターモードが有効になっている Network Firewall ポリシーに使用されます。
  - [Route management violations] (ルート管理違反) – インターネットゲートウェイがルートテーブルに関連付けられていない場合、またはインターネットゲートウェイのルートテーブルに無効なルートがある場合、インターネットゲートウェイは非準拠です。
  - [Remediation actions for route management violations] (ルート管理違反の修正アクション) – Firewall Manager は、ルート管理違反を修正するための可能な修正アクションを提案します。

  Example 1 — ルート管理違反と修復の提案

  インターネットゲートウェイはルートテーブルに関連付けられていません。推奨される修復アクションは、順序付けられたアクションのリストである場合があります。最初のアクションは、ルートテーブルを作成することです。2 つ目のアクションは、ルートテーブルをインターネットゲートウェイに関連付けることです。3 つ目のアクションは、必要なルートをインターネットゲートウェイルートテーブルに追加することです。

  Example 2 — ルート管理違反と修復の提案

  インターネットゲートウェイは有効なルートテーブルに関連付けられていますが、ルートが正しく設定されていません。推奨される修復は、順序付けられたアクションのリストである場合があります。最初の提案は、無効なルートを削除することです。2 つ目は、必要なルートをインターネットゲートウェイルートテーブルに追加することです。

- **`AWS::NetworkFirewall::FirewallPolicy`** - これは、Network Firewall ポリシーに使用されます。Firewall Manager は、非準拠になるように変更された Network Firewall のファイア

ウォールポリシーに関する情報を表示します。この情報は、予想されるファイアウォールポリシーと、カスタマーアカウントで見つかったポリシーを提供するものであるため、ステートレスルールグループ名とステートフルルールグループ名および優先度の設定、カスタムアクション名、ならびにデフォルトのステートレスアクションの設定を比較できます。違反の説明のコンポーネントには、リソースの予想される状態の説明、現在の非準拠状態、および使用可能な場合は、不一致の原因の説明が含まれます。

- **`AWS::EC2::VPC`** - これは DNS Firewall ポリシーに使用されます。Firewall Manager は、Firewall Manager の DNS Firewall ポリシーの範囲内にあり、ポリシーに準拠していない VPC に関する情報を表示します。提供される情報には、VPC に関連付けられることが予想されるルールグループおよび実際のルールグループが含まれます。違反の説明のコンポーネントには、リソースの予想される状態の説明、現在の非準拠状態、および使用可能な場合は、不一致の原因の説明が含まれます。
- **`AWS::WAFv2::WebACL`** – これは、設定で既存のウェブ ACLs の改良が指定されている AWS WAF ポリシーに使用されます。Firewall Manager は、範囲内のリソースに関連付けられているウェブ ACL に関する情報を表示しますが、Firewall Manager による改良との完全な互換性がありません。例えば、ウェブ ACL がポリシーの範囲外のリソースにも関連付けられている場合、Firewall Manager はそれを改良できません。

AWS Firewall Manager との統合 AWS Security Hub CSPM

このページでは、Firewall Manager と Security Hub CSPM を一緒に使用する方法について説明します。

AWS Firewall Manager は、コンプライアンス違反のリソースと検出した攻撃の検出結果を作成し、送信します AWS Security Hub CSPM。Security Hub CSPM の検出結果の詳細については、「 の検出結果 AWS Security Hub CSPM」を参照してください。

Security Hub CSPM と Firewall Manager を使用すると、Firewall Manager は自動的に検出結果を Security Hub CSPM に送信します。Security Hub CSPM の開始方法については、AWS Security Hub CSPM 「 ユーザーガイド」の「セットアップ AWS Security Hub CSPM」を参照してください。

> **Note**
>
> Firewall Manager は、管理しているポリシーと、モニタリングしているリソースの検出結果のみを更新します。
> Firewall Manager は、以下の検出結果を解決しません:

- 削除されたポリシー。
- 削除されたリソース。
- タグの変更やポリシー定義の変更など、Firewall Manager ポリシーの範囲外になったリソース。

Firewall Manager の検出結果を表示する方法

Security Hub CSPM で Firewall Manager の検出結果を表示するには、「Security Hub CSPM での検出結果の操作」のガイダンスに従い、次の設定を使用してフィルターを作成します。

- [Product Name] (製品名) に設定された属性。
- [EQUALS] に設定された演算子。
- `Firewall Manager` に設定された値。この設定では、大文字と小文字が区別されます。

これを無効にすることはできますか?

Security Hub CSPM コンソールを使用して、検出 AWS Firewall Manager 結果と Security Hub CSPM の統合を無効にすることができます。ナビゲーションバーで [Integrations] (統合) を選択し、Firewall Manager ペインで [Disable Integration] (統合の無効化) を選択します。詳細については、「AWS Security Hub CSPM ユーザーガイド」を参照してください。

AWS Firewall Manager 検出結果タイプ

- AWS WAF ポリシー Firewall Manager の検出結果
- AWS Shield Advanced ポリシー Firewall Manager の検出結果
- 一般的なセキュリティグループポリシーの Firewall Manager 検出結果
- セキュリティグループコンテンツ監査ポリシーの Firewall Manager 検出結果
- 使用状況監査セキュリティグループポリシーの Firewall Manager 検出結果
- Amazon Route 53 Resolver DNS Firewall ポリシーの Firewall Manage 検出結果
- AWS Config Firewall Manager の検出結果

AWS WAF ポリシー Firewall Manager の検出結果

このページでは、 AWS WAF ポリシーの Firewall Manager の検出結果について説明します。

Firewall Manager AWS WAF ポリシーを使用して、 のリソースに AWS WAF ルールグループを適用できます AWS Organizations。詳細については、「AWS Firewall Manager ポリシーの使用」を参照してください。

Firewall Manager マネージドウェブ ACL がリソースにありません。

AWS リソースには、Firewall Manager ポリシーに従って AWS Firewall Manager マネージドウェブ ACL の関連付けがありません。ポリシーの Firewall Manager 修復を有効にして、これを修正できます。

- 重要度 - 80
- ステータスの設定 - PASSED/FAILED
- 更新 - Firewall Manager が修復アクションを実行すると、検出結果が更新され、重要度が `HIGH` から `INFORMATIONAL` に引き下げられます。修復を実行した場合、Firewall Manager は検出結果を更新しません。

Firewall Manager 管理ウェブ ACL に正しく設定されていないルールグループがあります。

これは AWS WAF Classic ポリシーの検出結果です。Firewall Manager によって管理されるウェブ ACL のルールグループが、Firewall Manager ポリシーに従って正しく設定されていません。これは、ウェブ ACL に、ポリシーに必要なルールグループがないことを意味します。ポリシーの Firewall Manager 修復を有効にして、これを修正できます。

- 重要度 - 80
- ステータスの設定 - PASSED/FAILED
- 更新 - Firewall Manager が修復アクションを実行すると、検出結果が更新され、重要度が `HIGH` から `INFORMATIONAL` に引き下げられます。修復を実行した場合、Firewall Manager は検出結果を更新しません。

AWS Shield Advanced ポリシー Firewall Manager の検出結果

このページでは、 AWS Shield Advanced ポリシーの Firewall Manager の検出結果について説明します。

AWS Shield Advanced ポリシーの詳細については、「」を参照してくださいFirewall Manager のセキュリティグループポリシーを使用して Amazon VPC セキュリティグループを管理する。

Shield Advanced 保護がリソースにありません。

Firewall Manager ポリシーに従って、Shield Advanced 保護を持つ必要があるリソースには、その AWS リソースはありません。ポリシーの Firewall Manager 修復を有効にして、リソースの保護を有効にできます。

- 重要度 - 60
- ステータスの設定 - PASSED/FAILED
- 更新 - Firewall Manager が修復アクションを実行すると、検出結果が更新され、重要度が `HIGH` から `INFORMATIONAL` に引き下げられます。修復を実行した場合、Firewall Manager は検出結果を更新しません。

Shield Advanced は、モニタリング対象のリソースに対する攻撃を検出しました。

Shield Advanced は、保護された AWS リソースに対する攻撃を検出しました。ポリシーで Firewall Manager の修復を有効にできます。

- 重要度 - 70
- ステータス設定 - なし
- 更新 — Firewall Manager はこの検出結果を更新しません。

一般的なセキュリティグループポリシーの Firewall Manager 検出結果

このページでは、一般的なセキュリティグループポリシーの Firewall Manager の検出結果について説明します。

セキュリティグループ共通ポリシーの詳細については、「Firewall Manager のセキュリティグループポリシーを使用して Amazon VPC セキュリティグループを管理する」を参照してください。

リソースのセキュリティグループが正しく設定されていません。

Firewall Manager は、Firewall Manager ポリシーに従って、必要な Firewall Manager マネージドセキュリティグループの関連付けがないリソースを特定しました。ポリシーで Firewall Manager 修復を有効にできます。これにより、ポリシー設定に従って関連付けが作成されます。

- 重要度 - 70
- ステータスの設定 - PASSED/FAILED
- 更新 — Firewall Manager はこの検出結果を更新します。

Firewall Manager レプリカセキュリティグループがプライマリセキュリティグループと同期されていません。

Firewall Manager レプリカセキュリティグループが、共通セキュリティグループポリシーに従って、プライマリセキュリティグループと同期されていません。ポリシーで Firewall Manager 修復を有効にして、レプリカセキュリティグループをプライマリと同期させることができます。

- 重要度 - 80
- ステータスの設定 - PASSED/FAILED
- 更新 — Firewall Manager はこの検出結果を更新します。

セキュリティグループコンテンツ監査ポリシーの Firewall Manager 検出結果

このページでは、セキュリティグループコンテンツ監査ポリシーの Firewall Manager の検出結果について説明します。

セキュリティグループコンテンツ監査ポリシーの詳細については、「Firewall Manager のセキュリティグループポリシーを使用して Amazon VPC セキュリティグループを管理する」を参照してください。

セキュリティグループは、コンテンツ監査セキュリティグループに準拠していません。

Firewall Manager セキュリティグループコンテンツ監査ポリシーが、非準拠のセキュリティグループを特定しました。これは、コンテンツ監査ポリシーの範囲内にあり、ポリシーとその監査セキュリティグループで定義された設定に準拠していない、お客様が作成したセキュリティグループです。ポリシーで Firewall Manager 修復を有効にできます。これにより、非準拠のセキュリティグループが変更され、コンプライアンス準拠状態になります。

- 重要度 - 70
- ステータスの設定 - PASSED/FAILED
- 更新 — Firewall Manager はこの検出結果を更新します。

使用状況監査セキュリティグループポリシーの Firewall Manager 検出結果

このページでは、セキュリティグループ使用状況監査ポリシーの Firewall Manager の検出結果について説明します。

セキュリティグループ使用状況監査ポリシーの詳細については、「Firewall Manager のセキュリティグループポリシーを使用して Amazon VPC セキュリティグループを管理する」を参照してください。

Firewall Manager により、冗長セキュリティグループが検出されました。

Firewall Manager セキュリティグループ使用状況監査により、冗長セキュリティグループが特定されました。これは、同じ Amazon Virtual Private Cloud インスタンス内の別のセキュリティグループと同じルールが設定されたセキュリティグループです。使用状況監査ポリシーで Firewall Manager 自動修復を有効にできます。これにより、冗長セキュリティグループが 1 つのセキュリティグループで置き換えられます。

- 重要度 - 30
- ステータス設定 - なし
- 更新 — Firewall Manager はこの検出結果を更新しません。

Firewall Manager により、未使用のセキュリティグループが検出されました。

Firewall Manager セキュリティグループ使用状況監査により、未使用セキュリティグループが特定されました。これは、Firewall Manager の共通セキュリティグループポリシーによって参照されていないセキュリティグループです。使用状況監査ポリシーで Firewall Manager 自動修復を有効にできます。これにより、未使用のセキュリティグループが削除されます。

- 重要度 - 30
- ステータス設定 - なし
- 更新 — Firewall Manager はこの検出結果を更新しません。

Amazon Route 53 Resolver DNS Firewall ポリシーの Firewall Manage 検出結果

このページでは、Amazon Route 53 Resolver DNS Firewall ポリシーの Firewall Manager 検出結果について説明します。

DNS Firewall ポリシーの詳細については、「Firewall Manager の Amazon Route 53 Resolver DNS Firewall ポリシーを使用する」を参照してください。

DNS Firewall 保護がリソースにありません

VPC に、Firewall Manager の DNS Firewall ポリシーで定義されている DNS Firewall ルールグループの関連付けがありません。この検出結果には、ポリシーで指定されたルールグループが一覧表示されます。

- 重要度 - 80

AWS Config Firewall Manager の検出結果

このページでは、 AWS Configの Firewall Manager 検出結果について説明します。

詳細については AWS Config、「」を参照してくださいFirewall Manager の使用 AWS Config の有効化。

アカウントが リージョンで AWS Config を有効にしていません。

Firewall Manager は、アカウントとリージョンで有効に AWS Config する必要があります。この問題を解決するには、Firewall Manager を使用するアカウントとリージョン AWS Config で を有効にします。

- ステータスの設定 - PASSED/FAILED
- 更新 — Firewall Manager はこの検出結果を更新します。

> **Note**
>
> 有効にすると AWS Config、コンプライアンスステータスは PASS に変わりますが、重要度は HIGH のままです。

> **Note**
>
> Firewall Manager がポリシーコンプライアンスをモニタリングするには、保護されたリソースの設定変更を継続的に記録 AWS Config する必要があります。 AWS Config 設定では、記録頻度をデフォルト設定である Continuous に設定する必要があります。

AWS Firewall Manager サービスの使用におけるセキュリティ

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを活用できます。

> **Note**
>
> このセクションでは、Firewall Manager Network Firewall ポリシーや AWS セキュリティグループポリシーなど、 サービスとその AWS リソースの使用 AWS Firewall Manager に関する標準的なセキュリティガイダンスを提供します。
> Firewall Manager を使用して AWS リソースを保護する方法については、Firewall Manager ガイドの残りの部分を参照してください。

セキュリティは、 AWS お客様とお客様の間の責任共有です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ – AWS は、 で AWS サービスを実行するインフラストラクチャを保護する責任を担います AWS クラウド。 は、お客様が安全に使用できるサービス AWS も提供します。セキュリティの有効性は、AWS コンプライアンスプログラムの一環として、サードパーティーの審査機関によって定期的にテストおよび検証されています。Firewall Manager に適用されるコンプライアンスプログラムについては、「コンプライアンスプログラムによる対象範囲内のAWS のサービス」を参照してください。
- クラウドのセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、お客様のデータの機密性、組織の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、Firewall Manager の使用時に責任共有モデルがどのように適用されるかを理解するために役立ちます。次のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために Firewall Manager を設定する方法を示します。また、Firewall Manager リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

- Firewall Manager でのデータ保護
- の Identity and Access Management AWS Firewall Manager
- Firewall Manager での口グ記録とモニタリング

- Firewall Manager のコンプライアンス検証
- Firewall Manager の回復力
- のインフラストラクチャセキュリティ AWS Firewall Manager

Firewall Manager でのデータ保護

AWS 責任共有モデル は、 AWS Firewall Managerでのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「 AWS のサービス 」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「Data Privacy FAQChina」を参照してください。 欧州におけるデータ保護に関する情報については、General Data Protection Regulation (GDPR) Center を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM アイデンティティセンターまたは AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須ですが、TLS 1.3 を推奨します。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール、API、また

は SDK を使用して Firewall Manager AWS CLIまたは他の AWS のサービス を使用する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

Firewall Manager のエンティティ (ポリシーなど) は、中国 (北京) や中国 (寧夏) など、暗号化が利用できない特定のリージョンを除き、保管時に暗号化されます。リージョンごとに一意の暗号化キーが使用されます。

の Identity and Access Management AWS Firewall Manager

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を (サインインについて) 認証し、Firewall Manager リソースの使用について誰を認可 (アクセス許可を付与) するのかを制御します。IAM は、追加料金なしで使用できる AWS のサービス です。

トピック

- オーディエンス
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- が IAM と AWS Firewall Manager 連携する方法
- のアイデンティティベースのポリシーの例 AWS Firewall Manager
- AWS の 管理ポリシー AWS Firewall Manager
- AWS Firewall Manager ID とアクセスのトラブルシューティング
- Firewall Manager のサービスにリンクされたロールの使用
- サービス間の混乱した代理の防止

オーディエンス

AWS Identity and Access Management (IAM) の使用方法は、Firewall Manager で行う作業によって異なります。

サービスユーザー – ジョブを実行するために Firewall Manager サービスを使用するユーザーには、必要な認証情報とアクセス許可を管理者が付与します。さらに多くの Firewall Manager の機能を使

用して作業を行う際には、追加のアクセス許可が必要になる場合があります。アクセスの管理方法を理解すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。アクセスが不可能な Firewall Manager の機能がある場合は、「AWS Shield ID とアクセスのトラブルシューティング」を参照してください。

サービス管理者 – 社内で Firewall Manager のリソースを担当しているユーザーには、通常、Firewall Manager への完全なアクセス権が付与されます。Firewall Manager 機能やリソースに対するアクセス権を、サービスを利用しているユーザーの中の誰に付与するかを決めるのは、管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。社内で Firewall Manager と IAM をどのように使用できるかの詳細については、「が IAM と AWS Shield 連携する方法」を参照してください。

IAM 管理者 – 管理者は、Firewall Manager へのアクセスを管理するポリシーの作成方法について、詳しく理解しておく必要があります。IAM で使用できる、Firewall Manager でのアイデンティティベースのポリシーの例は、「のアイデンティティベースのポリシーの例 AWS Shield」で確認してください。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。、IAM ユーザー AWS アカウントのルートユーザー、または IAM ロールを引き受けることで認証される必要があります。

(AWS IAM アイデンティティセンター IAM Identity Center)、シングルサインオン認証、Google/Facebook 認証情報などの ID ソースからの認証情報を使用して、フェデレーティッド ID としてサインインできます。サインインの詳細については、「AWS サインイン ユーザーガイド」の「AWS アカウントにサインインする方法」を参照してください。

プログラムによるアクセスの場合、 は SDK と CLI AWS を提供してリクエストを暗号化して署名します。詳細については、「IAM ユーザーガイド」の「API リクエストに対するAWS 署名バージョン 4」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、まず、すべての AWS のサービス および リソースへの完全なアクセス権を持つ AWS アカウント root ユーザーと呼ばれる 1 つのサインインアイデンティティから始めます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザー認証情報を必要とするタスクについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーテッドアイデンティティ

ベストプラクティスとして、人間のユーザーが一時的な認証情報 AWS のサービス を使用して にアクセスするには、ID プロバイダーとのフェデレーションを使用する必要があります。

フェデレーティッド ID は、エンタープライズディレクトリ、ウェブ ID プロバイダー、または ID ソースの認証情報 AWS のサービス を使用して Directory Service にアクセスするユーザーです。フェデレーテッドアイデンティティは、一時的な認証情報を提供するロールを引き受けます。

アクセスを一元管理する場合は、 AWS IAM アイデンティティセンターをお勧めします。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「IAM アイデンティティセンターとは」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、特定の個人やアプリケーションに対する特定のアクセス許可を持つアイデンティティです。長期認証情報を持つ IAM ユーザーの代わりに一時的な認証情報を使用することをお勧めします。詳細については、IAM ユーザーガイドの「ID プロバイダーとのフェデレーションを使用して にアクセスすることを人間のユーザーに要求する AWS」を参照してください。

IAM グループは、IAM ユーザーの集合を指定し、大量のユーザーに対するアクセス許可の管理を容易にします。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可を持つアイデンティであり、一時的な認証情報を提供します。ユーザーから IAM ロール (コンソール) に切り替えるか、 または API オペレーションを呼び出すことで、ロールを引き受けることができます。 AWS CLI AWS 詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールは、フェデレーションユーザーアクセス、一時的な IAM ユーザーのアクセス許可、クロスアカウントアクセス、クロスサービスアクセス、および Amazon EC2 で実行するアプリケーションに役立ちます。詳細については、IAM ユーザーガイド の IAM でのクロスアカウントリソースアクセス を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは、ID またはリソースに関連付けられたときにアクセス許可を定義します。 は、プリンシパルがリクエストを行うときにこれらのポリシー AWS を評価します。ほとんどのポリシーは JSON

ドキュメント AWS として に保存されます。JSON ポリシードキュメントの詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は、ポリシーを使用して、どのプリンシパルがどのリソースに対して、どのような条件でアクションを実行できるかを定義することで、誰が何にアクセスできるかを指定します。

デフォルトでは、ユーザーやロールにアクセス許可はありません。IAM 管理者は IAM ポリシーを作成してロールに追加し、このロールをユーザーが引き受けられるようにします。IAM ポリシーは、オペレーションの実行方法を問わず、アクセス許可を定義します。

アイデンティティベースのポリシー

アイデンティティベースのポリシーは、アイデンティティ (ユーザー、グループ、またはロール) にアタッチできる JSON アクセス許可ポリシードキュメントです。これらのポリシーは、アイデンティティがどのリソースに対してどのような条件下でどのようなアクションを実行できるかを制御します。アイデンティティベースポリシーの作成方法については、IAM ユーザーガイド の カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する を参照してください。

アイデンティティベースのポリシーは、インラインポリシー (単一の ID に直接埋め込む) または管理ポリシー (複数の ID にアタッチされたスタンドアロンポリシー) にすることができます。管理ポリシーとインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。例としては、IAM ロール信頼ポリシーや Amazon S3 バケットポリシーなどがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするためのアクセス許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、および Amazon VPC は AWS WAF、ACLs。ACL の詳細については、Amazon Simple Storage Service デベロッパーガイド の アクセスコントロールリスト (ACL) の概要 を参照してください。

その他のポリシータイプ

AWS は、より一般的なポリシータイプによって付与されるアクセス許可の上限を設定できる追加のポリシータイプをサポートしています。

- アクセス許可の境界 – アイデンティティベースのポリシーで IAM エンティティに付与することのできるアクセス許可の数の上限を設定します。詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可境界」を参照してください。
- サービスコントロールポリシー (SCP) - AWS Organizations内の組織または組織単位の最大のアクセス許可を指定します。詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」を参照してください。
- リソースコントロールポリシー (RCP) – は、アカウント内のリソースで利用できる最大数のアクセス許可を定義します。詳細については、「AWS Organizations ユーザーガイド」の「リソースコントロールポリシー (RCP)」を参照してください。
- セッションポリシー – ロールまたはフェデレーションユーザーの一時セッションを作成する際にパラメータとして渡される高度なポリシーです。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成されるアクセス許可を理解するのがさらに難しくなります。が複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、「IAM ユーザーガイド」の「ポリシー評価ロジック」を参照してください。

が IAM と AWS Firewall Manager 連携する方法

IAM を使用して Firewall Manager へのアクセスを管理する前に、Firewall Manager で使用できる IAM の機能を把握してください。

で使用できる IAM 機能 AWS Firewall Manager

IAM 機能	Firewall Manager のサポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	なし

IAM 機能	Firewall Manager のサポート
ポリシーアクション	あり
ポリシーリソース	はい
ポリシー条件キー (サポート固有)	いいえ
ACL	なし
ABAC (ポリシー内のタグ)	あり
一時的な認証情報	あり
転送アクセスセッション (FAS)	あり
サービスロール	部分的
サービスリンクロール	はい

Firewall Manager およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要については、IAM ユーザーガイドのAWS 「IAM と連携する のサービス」を参照してください。

Firewall Manager 用 ID ベースのポリシー

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

Firewall Manager でのアイデンティティベースのポリシーの例については、「のアイデンティティベースのポリシーの例 AWS Firewall Manager」を参照してください。

Firewall Manager のための ID ベースのポリシー例

Firewall Manager でのアイデンティティベースのポリシーの例については、「のアイデンティティベースのポリシーの例 AWS Firewall Manager」を参照してください。

Firewall Manager 内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーで、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、全体のアカウント、または別のアカウントの IAM エンティティを、リソースベースのポリシーのプリンシパルとして指定します。詳細については、IAM ユーザーガイドのIAM でのクロスアカウントリソースアクセスを参照してください。

Firewall Manager のポリシーアクション

ポリシーアクションのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action` 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

Firewall Manager アクションのリストを確認するには、「サービス認可リファレンス」の「AWS Firewall Managerで定義されるアクション」を参照してください。

Firewall Manager のポリシーアクションには、次のプレフィックスを付加します。

```
fms
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "fms:action1",
      "fms:action2"
         ]
```

ワイルドカード (*) を使用して複数アクションを指定できます。例えば、Describe という単語で始まるすべてのアクションを指定するには次のアクションを含めます。

```
"Action": "fms:Describe*"
```

Firewall Manager でのアイデンティティベースのポリシーの例については、「のアイデンティティベースのポリシーの例 AWS Firewall Manager」を参照してください。

Firewall Manager のポリシーリソース

ポリシーリソースのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Resource JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。リソースレベルのアクセス許可をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

Firewall Manager リソースタイプとその ARN のリストを確認するには、「Service Authorization Reference」の「AWS Firewall Managerで定義されるリソースタイプ」を参照してください。どのアクションで各リソースの ARN を指定できるかについては、「AWS Firewall Managerで定義されるアクション」を参照してください。

Firewall Manager でのアイデンティティベースのポリシーの例については、「のアイデンティティベースのポリシーの例 AWS Firewall Manager」を参照してください。

Firewall Manager のポリシー条件キー

サービス固有のポリシー条件キーへのサポート: なし

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Condition 要素は、定義された基準に基づいてステートメントが実行される時期を指定します。イコールや未満などの条件演算子を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「グローバル条件コンテキストキー」を参照してください。

Firewall Manager の条件キーのリストを確認するには、「Service Authorization Reference」の「AWS Firewall Managerの条件キー」を参照してください。条件キーを使用できるアクションとリソースについては、「 で定義されるアクション AWS Firewall Manager」を参照してください。

Firewall Manager でのアイデンティティベースのポリシーの例については、「のアイデンティティベースのポリシーの例 AWS Firewall Manager」を参照してください。

Firewall Manager の ACL

ACL のサポート: なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするためのアクセス許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Firewall Manager を使用する ABAC

ABAC (ポリシー内のタグ) のサポート: あり

属性ベースのアクセス制御 (ABAC) は、タグと呼ばれる属性に基づいてアクセス許可を定義する認可戦略です。IAM エンティティと AWS リソースにタグをアタッチし、プリンシパルのタグがリソースのタグと一致するときにオペレーションを許可するように ABAC ポリシーを設計できます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用する」を参照してください。

Firewall Manager での一時的な認証情報の使用

一時的な認証情報のサポート: あり

一時的な認証情報は、 AWS リソースへの短期的なアクセスを提供し、フェデレーションまたはスイッチロールの使用時に自動的に作成されます。長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成 AWS することをお勧めします。詳細については、「IAM ユーザーガイド」の「IAM の一時的な認証情報」および「AWS のサービス と IAM との連携」を参照してください。

転送アクセスセッション (Firewall Manager)

転送アクセスセッション (FAS) のサポート: あり

転送アクセスセッション (FAS) は、 を呼び出すプリンシパルのアクセス許可と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする を使用します。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

Firewall Manager のサービスロール

サービスロールへのサポート: 一部

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、IAM ユーザーガイドの AWS のサービスに許可を委任するロールを作成するを参照してください。

> **Warning**
>
> サービスロール向けの許可を変更すると、Firewall Manager の機能が破損する可能性があります。Firewall Manager が指示する場合以外は、サービスロールを編集しないでください。

Firewall Manager での IAM ロールの選択

Firewall Manager で *PutNotificationChannel* API アクションを使用するには、Firewall Manager による Amazon SNS へのアクセスを許可するロールを選択する必要があります。これにより、サービスがユーザーに代わって Amazon SNS メッセージを発行できるようになります。詳細については、「AWS Firewall Manager API リファレンス」の「PutNotificationChannel」を参照してください)。

SNS トピックでのアクセス許可設定の例を次に示します。このポリシーを独自のカスタムロールで使用するには、Amazon リソースネーム (ARN) `AWSServiceRoleForFMS` を `SnsRoleName` のARN に置き換えます。

```
{
  "Sid": "AWSFirewallManagerSNSPolicy",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::account ID:role/aws-service-role/
fms.amazonaws.com/AWSServiceRoleForFMS"
  },
  "Action": "sns:Publish",
  "Resource": "SNS topic ARN"
}
```

Firewall Manager のアクションとリソースの詳細については、「 で定義されるアクション AWS Identity and Access Management 」ガイドトピックを参照してください。 AWS Firewall Manager

Firewall Manager のサービスにリンクされたロール

サービスリンクロールのサポート: あり

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

サービスにリンクされたロールの作成または管理の詳細については、「IAM と提携するAWS のサービス」を参照してください。表の「サービスリンクロール」列に `Yes` と記載されたサービスを見つけます。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

のアイデンティティベースのポリシーの例 AWS Firewall Manager

デフォルトでは、ユーザーおよびロールに Firewall Manager のリソースを作成または変更する許可が付与されていません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。

これらのサンプルの JSON ポリシードキュメントを使用して IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーを作成する (コンソール)」を参照してください。

Firewall Manager が定義するアクションとリソースタイプ (リソースタイプごとの ARN の形式を含む) の詳細については、「Service Authorization Reference」の「Actions, resources, and condition keys for AWS Firewall Manager」を参照してください。

トピック

- ポリシーに関するベストプラクティス
- Firewall Manager コンソールの使用
- 自分の権限の表示をユーザーに許可する
- Firewall Manager のセキュリティグループに読み取りアクセス権を付与する

ポリシーに関するベストプラクティス

ID ベースのポリシーは、アカウント内で誰かが Firewall Manager のリソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションでは、 AWS アカウントに費用が発生する場合があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、IAM ユーザーガイド の AWS マネージドポリシー または ジョブ機能のAWS マネージドポリシー を参照してください。
- 最小特権を適用する – IAM ポリシーでアクセス許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、IAM ユーザーガイド の IAM でのポリシーとアクセス許可 を参照してください。

- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。たとえば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用されている場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます CloudFormation。詳細については、IAM ユーザーガイド の IAM JSON ポリシー要素:条件 を参照してください。
- IAM アクセスアナライザー を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM アクセスアナライザー は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイド の IAM Access Analyzer でポリシーを検証する を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイド の MFA を使用した安全な API アクセス を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイド の IAM でのセキュリティのベストプラクティス を参照してください。

Firewall Manager コンソールの使用

AWS Firewall Manager コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 AWS アカウント内の Firewall Manager リソースの詳細をリスト化および表示できます。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

ユーザーとロールが引き続き Firewall Manager コンソールを使用できるようにするには、エンティティに Firewall Manager *ConsoleAccess*または *ReadOnly* AWS 管理ポリシーもアタッチします。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

自分の権限の表示をユーザーに許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Firewall Manager のセキュリティグループに読み取りアクセス権を付与する

Firewall Manager は、ユーザーにクロスアカウントでのリソースアクセスを許可しますが、クロスアカウントでのリソース保護を作成することは許可しません。リソースの保護は、それらのリソースを所有するアカウント内からのみ作成できます。

すべてのリソースの `fms:Get` 、`fms:List`、および `ec2:DescribeSecurityGroups` アクションへの、アクセス許可を付与するポリシーの例を次に示します。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "fms:Get*",
                "fms:List*",
                "ec2:DescribeSecurityGroups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS の 管理ポリシー AWS Firewall Manager

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できるように、多くの一般的なユースケースにアクセス許可を付与するように設計されています。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS マネージドポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) に影響します。 AWS は、新しい が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、 AWS マネージドポリシーを更新する可能性が高くなります。

詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

AWS 管理ポリシー: **AWSFMAdminFullAccess**

AWSFMAdminFullAccess AWS 管理ポリシーを使用して、管理者がすべての Firewall Manager ポリシータイプを含む AWS Firewall Manager リソースにアクセスできるようにします。このポリシーには、 AWS Firewall Managerで Amazon Simple Notification Service 通知を設定するためのアクセス許可は含まれません。Amazon Simple Notification Service のアクセスを設定する方法については、「Setting up access for Amazon Simple Notification Service」(Amazon Simple Notification Service のアクセスをセットアップする) を参照してください。

ポリシーリストの詳細については、IAM コンソールで「AWSFMAdminFullAccess」を参照してください。このセクションの残りの部分では、ポリシー設定の概要を説明します。

アクセス権限のステートメント

このポリシーは、一連のアクセス許可に基づくステートメントにグループ化されます。

- AWS Firewall Manager ポリシーリソース - すべての Firewall Manager ポリシータイプを含む AWS Firewall Manager、 のリソースへの完全な管理アクセス許可を許可します。
- Amazon Simple Storage Service への AWS WAF ログの書き込み - Firewall Manager に Amazon S3 での AWS WAF ログの書き込みと読み取りを許可します。
- サービスにリンクされたロールの作成 – 管理者がサービスにリンクされたロールを作成できるようにします。これにより、Firewall Manager がユーザーに代わって他のサービスのリソースを分析できるようになります。このアクセス許可では、Firewall Manager が使用するサービスリンクロールのみを作成できます。Firewall Manager がサービスリンクロールを使用する方法の詳細については、Firewall Manager のサービスにリンクされたロールの使用 を参照してください。
- AWS Organizations — 管理者による組織への Firewall Manager の使用を許可します。 AWS Organizationsで Firewall Manager の信頼されたアクセスを有効にすると AWS Organizations、管理者アカウントのメンバーは組織全体の結果を表示できます。 AWS Organizations で を使用する方法については AWS Firewall Manager、「 AWS Organizations ユーザーガイド」の「 を他の AWS のサービス AWS Organizations で使用する」を参照してください。

アクセス権限カテゴリ

以下は、ポリシー内のアクセス権限のタイプと、それらが提供するアクセス権限の一覧です。

- `fms` – AWS Firewall Manager リソースを使用します。
- `waf` および `waf-regional` – AWS WAF Classic ポリシーの動作。
- `elasticloadbalancing` – AWS WAF ウェブ ACLsto。
- `firehose` – AWS WAF ログに関する情報を表示します。
- `organizations` – AWS Organizations リソースを使用します。
- `shield` – AWS Shield ポリシーのサブスクリプション状態を表示します。
- `route53resolver` – VPC 用 Route 53 プライベート DNS ポリシー内の VPC 用 Route 53 プライベート DNS ルールグループを使用します。
- `wafv2` – AWS WAFV2 ポリシーを使用します。
- `network-firewall` – AWS Network Firewall ポリシーを使用します。
- `ec2` – ポリシーの利用可能なゾーンとリージョンを表示します。
- `s3` – AWS WAF ログに関する情報を表示します。

AWS 管理ポリシー: **`FMSServiceRolePolicy`**

このポリシーにより AWS Firewall Manager 、 は Firewall Manager および統合サービスでユーザーに代わって AWS リソースを管理できます。このポリシーは、`AWSServiceRoleForFMS` サービスにリンクされたロールにアタッチされます。サービスにリンクされたロールの詳細については、「Firewall Manager のサービスにリンクされたロールの使用」を参照してください。

ポリシーの詳細については、FMSServiceRolePolicy の IAM コンソールを参照してください。

AWS マネージドポリシー: AWSFMAdminReadOnlyAccess

すべての AWS Firewall Manager リソースへの読み取り専用アクセスを許可します。

ポリシーリストとその詳細については、IAM コンソールで「AWSFMAdminReadOnlyAccess」を参照してください。このセクションの残りの部分では、ポリシー設定の概要を説明します。

アクセス権限カテゴリ

以下は、ポリシー内のアクセス許可のタイプと、アクセス許可が読み取り専用アクセスを許可する情報の一覧です。

- `fms` – AWS Firewall Manager リソース。
- `waf` および `waf-regional` — AWS WAF Classic ポリシー。
- `firehose` – AWS WAF ログ。
- `organizations` – AWS リソースを整理します。
- `shield` – AWS Shield ポリシー。
- `route53resolver` – VPC 用 Route 53 プライベート DNS ポリシー内の VPC 用 Route 53 プライベート DNS ルールグループ。
- `wafv2` – で利用可能な AWS WAFV2 ルールグループと AWS マネージドルールのルールグループ AWS WAFV2。
- `network-firewall` – AWS Network Firewall ルールグループとルールグループのメタデータ。
- `ec2` – AWS Network Firewall ポリシーアベイラビリティーゾーンとリージョン 。
- `s3` – AWS WAF ログ。

AWS マネージドポリシー: AWSFMMemberReadOnlyAccess

AWS Firewall Manager メンバーリソースへの読み取り専用アクセスを許可します。ポリシーの詳細については、IAM コンソールで「AWSFMMemberReadOnlyAccess」を参照してください。

AWS 管理ポリシーに対する Firewall Manager の更新

このサービスがこれらの変更の追跡を開始してからの Firewall Manager の AWS マネージドポリシーの更新に関する詳細を表示します。このページへの変更に関する自動アラートについては、Firewall Manager のドキュメント履歴ページ (ドキュメント履歴) で RSS フィードをサブスクライブしてください。

変更	説明	日付
FMSServiceRolePolicy – 更新されたポリシー	Firewall Manager のサービスポリシーにアクセス許可を追加しました。	2025-05-21

変更	説明	日付
	Amazon CloudFront に必要な以下のアクセス許可を追加しました。 • `cloudfront:AssociateDistributionWebACL` – AWS WAF ウェブ ACL を CloudFront ディストリビューションに関連付けるアクセス許可を付与します • `cloudfront:DisassociateDistributionWebACL` – AWS WAF ウェブ ACL と CloudFront ディストリビューションの関連付けを解除するアクセス許可を付与します	
FMSServiceRolePolicy – 更新されたポリシー	Firewall Manager のサービスポリシーにアクセス許可を追加しました。 リソース設定ステータスをバッチで取得する `BatchGetResourceConfig` アクセス許可を追加しました。IAM コンソールで更新されたポリシーを参照してください: FMSServiceRolePolicy。	2025-02-10

変更	説明	日付
FMSServiceRolePolicy – 更新されたポリシー	Firewall Manager のサービスロールポリシーにアクセス権限を追加しました。 Network Firewall TLS 設定情報を読み取る機能を追加しました。IAM コンソールで更新されたポリシーを参照してください: FMSServiceRolePolicy。	2024-07-22
FMSServiceRolePolicy – 更新されたポリシー	ネットワーク ACL を管理するためのアクセス権限を追加しました。 IAM コンソールで更新されたポリシーを参照してください: FMSServiceRolePolicy。	2024-04-22
FMSServiceRolePolicy – 更新されたポリシー	Firewall Manager が、指定された AWS Config ルールが準拠しているかどうかを記述できるようにするアクセス許可を追加しました。 IAM コンソールで更新されたポリシーを参照してください: FMSServiceRolePolicy。	2023-04-21

変更	説明	日付
FMSServiceRolePolicy – 更新されたポリシー	Firewall Manager が Amazon EC2 インスタンスとネットワークインターフェイスの属性を記述できるようにするアクセス許可が追加されました。 IAM コンソールで更新されたポリシーを参照してください: FMSServiceRolePolicy。	2022-11-15
AWSFMAdminReadOnlyAccess – 更新されたポリシー	、Shield AWS WAFV2、Network Firewall、DNS Firewall、Amazon VPC セキュリティグループ、ポリシーをサポートするアクセス許可を追加しました。 IAM コンソールで更新されたポリシーを参照してください: AWSFMAdminReadOnlyAccess。	2022-11-02
AWSFMAdminFullAccess – 更新されたポリシー	、Shield AWS WAFV2、Network Firewall、DNS Firewall、Amazon VPC セキュリティグループ、ポリシーをサポートするアクセス許可を追加しました。Amazon SNS のアクセス許可を削除しました。 IAM コンソールで更新されたポリシー (AWSFMAdminFullAccess) を参照してください。	2022-10-21

変更	説明	日付
FMSServiceRolePolicy – AWS Firewall Manager サードパーティーのファイアウォールポリシーの新しいアクセス許可	この変更により、Firewall Manager は、サードパーティーのファイアウォールポリシーに関連付けられた Amazon EC2 VPC エンドポイントを作成および削除できます。	2022-03-30
FMSServiceRolePolicy – AWS Network Firewall ポリシーの新しいアクセス許可	Network Firewall ポリシーのファイアウォールのデプロイをサポートするための新しい許可を追加しました。新しい許可により、ポリシーの範囲内にあるアカウントのアベイラビリティーゾーンに関する情報を取得できます。	2022-02-16
FMSServiceRolePolicy – AWS Shield ポリシーの新しいアクセス許可	AWS WAF リージョンリソースと AWS WAF グローバルリソースのタグを取得するための新しいアクセス許可を追加しました。リソース ACLs を取得する AWS WAF リージョンアクセス許可を追加しました。Shield アプリケーションレイヤー DDoS 自動緩和をサポートするための許可を追加しました。	2021-11-18

変更	説明	日付
FMSServiceRolePolicy – セキュリティグループと AWS Network Firewall ポリシーの新しいアクセス許可	AWS Network Firewall ポリシーの集中ログ記録を有効にする新しいアクセス許可を追加しました。さらに、セキュリティグループポリシーのリソースを AWS Firewall Manager クエリする方法に影響を与える Config サービスの変更をサポートするために、読み取り専用の Amazon EC2 アクセス許可が追加されました。	2021-09-29
FMSServiceRolePolicy – AWS WAF リソースの ARN 形式	AWS WAF リソースの ARN 形式を標準化するように FMSServiceRolePolicy を更新しました。更新された ARN 形式は arn:aws:waf:*:*:* と arn:aws:waf-regional:*:*:* です。	2021-08-12
FMSServiceRolePolicy - 中国の他のリージョン	AWS Firewall Manager はFMSServiceRolePolicy 、中国の BJS および ZHY リージョンに対して を有効にしました。	2021-08-12

変更	説明	日付
FMSServiceRolePolicy - 既存のポリシーに対する更新	が Amazon Route 53 Resolver DNS Firewall を管理 AWS Firewall Manager できるようにする新しいアクセス許可を追加しました。 この変更により、Firewall Manager は Amazon Route 53 Resolver DNS Firewall の関連付けを設定できるようになります。これにより、Firewall Manager を使用して、 AWS Organizationsの組織全体で VPC のために DNS Firewall 保護を提供できます。	2021-03-17
Firewall Manager が変更の追跡を開始	Firewall Manager は、 AWS 管理ポリシーの変更の追跡を開始しました。	2021-03-02

AWS Firewall Manager ID とアクセスのトラブルシューティング

次の情報は、Firewall Manager と IAM の使用に伴って発生する可能性がある、一般的な問題を診断したり修復したりする際に役立ちます。

トピック

- Firewall Manager でのアクション実行が承認されない
- iam:PassRole を実行する権限がありません
- 自分の 以外のユーザーに Firewall Manager リソース AWS アカウント へのアクセスを許可したい

Firewall Manager でのアクション実行が承認されない

アクションを実行する権限がないというエラーが表示された場合は、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要な fms:*GetWidget* アクセス許可を持っていない場合に発生するものです。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fms:GetWidget on resource: my-example-widget
```

この場合、fms:*GetWidget* アクションを使用して *my-example-widget* リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

iam:PassRole を実行する権限がありません

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Firewall Manager にロールを渡せるようにする必要があります。

一部の AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、既存のロールをそのサービスに渡すことができます。そのためには、サービスにロールを渡すアクセス許可が必要です。

marymajor という IAM ユーザーが、コンソールを使用して Firewall Manager でアクションを実行しようとした際に発生するエラーの例を次に示します。ただし、このアクションをサービスが実行するには、サービスロールから付与されたアクセス許可が必要です。Mary には、ロールをサービスに渡すアクセス許可がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン資格情報を提供した担当者が管理者です。

自分の 以外のユーザーに Firewall Manager リソース AWS アカウント へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまた

はアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- これらの機能を Firewall Manager でサポートしているかどうかを確認するには、「が IAM と AWS Shield 連携する方法」 を参照してください。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイドの外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いの詳細については、IAM ユーザーガイドのIAM ロールとリソースベースのポリシーとの相違点を参照してください。

Firewall Manager のサービスにリンクされたロールの使用

AWS Firewall Manager は AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスにリンクされたロールは、Firewall Manager に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは Firewall Manager によって事前定義されており、サービスがユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用することで、必要な許可を手動で追加する必要がなくなるため、Firewall Manager の設定が簡単になります。Firewall Manager は、サービスにリンクされたロールの許可を定義します。特に定義されている場合を除き、Firewall Manager のみがそのロールを引き受けることができます。定義された許可には、信頼ポリシーと許可ポリシーが含まれます。この許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスにリンクされたロールを削除するには、まずそのロールの関連リソースを削除します。これにより、リソースに対する許可が誤って削除されることがなくなり、Firewall Manager のリソースは保護されます。

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連携するAWS サービス」を参照して、サービスにリンクされたロール列がはいになっているサービスを見つけてください。そのサービスに関するサービスにリンクされたロールのドキュメントを表示するには、リンクが設定されている [Yes] (はい) を選択します。

Firewall Manager でのサービスにリンクされたロールの許可

AWS Firewall Manager は、サービスにリンクされたロール名 AWSServiceRoleForFMS を使用して、Firewall Manager がユーザーに代わって AWS サービスを呼び出し、ファイアウォールポリシーと AWS Organizations アカウントリソースを管理できるようにします。このポリシーは、 AWS マネージドロール にアタッチされますAWSServiceRoleForFMS。マネージドロールの詳細については、「AWS 管理ポリシー: FMSServiceRolePolicy」を参照してください。

AWSServiceRoleForFMS サービスにリンクされたロールは、サービスを信頼し、ロール `fms.amazonaws.com` を引き受けます。

ロールの許可ポリシーは、指定したリソースに対して以下のアクションを完了することを Firewall Manager に許可します。

- `waf` - アカウントの AWS WAF Classic ウェブ ACLs、ルールグループのアクセス許可、およびウェブ ACLs関連付けを管理します。
- `ec2` – Elastic Network Interface と Amazon EC2 インスタンスで、セキュリティグループを管理します。Amazon VPC サブネット上のネットワーク ACL を管理します。
- `vpc` – Amazon VPC 内のサブネット、ルートテーブル、タグ、エンドポイントを管理します。
- `wafv2` - アカウントの AWS WAF ウェブ ACLs、ルールグループのアクセス許可、およびウェブ ACLs関連付けを管理します。
- `cloudfront` – CloudFront ディストリビューションを保護するためのウェブ ACL を作成します。
- `config` - アカウントで Firewall Manager が所有する AWS Config ルールを管理します。
- `iam` - このサービスにリンクされたロールを管理し、 AWS WAF および Shield ポリシーのログ記録を設定する場合は、必要な AWS WAF および Shield サービスにリンクされたロールを作成します。
- `organization` - Firewall Manager が所有するサービスにリンクされたロールを作成して、Firewall Manager が使用する AWS Organizations リソースを管理します。
- `shield` - アカウント内のリソース AWS Shield の保護と L7 緩和設定を管理します。
- `ram` - DNS Firewall ルールグループと Network Firewall ルールグループの AWS RAM リソース共有を管理します。

- `network-firewall` - アカウントの Firewall Manager 所有の AWS Network Firewall リソースと依存する Amazon VPC リソースを管理します。
- `route53resolver` – アカウント内で、Firewall Manager が所有する DNS Firewall の関連付けを管理します。

IAM コンソールの FMSServiceRolePolicy で、すべてのポリシーを確認します。

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するにはアクセス許可を設定する必要があります。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの許可」を参照してください。

Firewall Manager のサービスにリンクされたロールの作成

サービスリンクロールを手動で作成する必要はありません。で Firewall Manager のログ記録を有効にするか AWS マネジメントコンソール、Firewall Manager CLI または Firewall Manager API で`PutLoggingConfiguration`リクエストを行うと、Firewall Manager によってサービスにリンクされたロールが作成されます。

ログ記録を有効化するためには、`iam:CreateServiceLinkedRole` 許可が必要です。

このサービスにリンクされたロールを削除した後で再度作成する必要が生じた場合は、同じ方法でアカウントにロールを再作成できます。Firewall Manager ログ記録を有効にすると、Firewall Manager は、ユーザーのためにサービスにリンクされたロールを再作成します。

Firewall Manager のサービスにリンクされたロールの編集

Firewall Manager では、AWSServiceRoleForFMS のサービスにリンクされたロールを編集することはできません。サービスにリンクされたロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロール記述の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの編集」を参照してください。

Firewall Manager のサービスにリンクされたロールの削除

サービスにリンクされたロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、積極的にモニタリングまたは保守されていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスにリンクされたロールのリソースをクリーンアップする必要があります。

> **Note**
>
> リソースを削除する際に、Firewall Manager のサービスでその口ールが使用されている場合、削除は失敗することがあります。失敗した場合は、数分待ってから操作を再試行してください。

IAM を使用して、サービスにリンクされたロールを削除するには

IAM コンソール、IAM CLI、または IAM API を使用して、AWSServiceRoleForFMS サービスにリンクされたロールを削除します。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの削除」を参照してください。

Firewall Manager サービスにリンクされたロールをサポートするリージョン

Firewall Manager では、このサービスが利用可能なすべてのリージョンで、サービスにリンクされたロールの使用をサポートしています。詳細については、「Firewall Manager エンドポイントとクォータ」を参照してください。

サービス間の混乱した代理の防止

混乱した代理問題は、アクションを実行する許可を持たないエンティティが、より特権のあるエンティティにアクションを実行するように強制できるセキュリティの問題です。では AWS、サービス間のなりすましにより、混乱した代理問題が発生する可能性があります。サービス間でのなりすましは、1 つのサービス (呼び出し元サービス) が、別のサービス (呼び出し対象サービス) を呼び出すときに発生する可能性があります。呼び出し元サービスは、本来ならアクセスすることが許可されるべきではない方法でその許可を使用して、別のお客様のリソースに対する処理を実行するように操作される場合があります。これを防ぐため、 AWS では、アカウントのリソースへのアクセス権が付与されたサービスプリンシパルで、すべてのサービスのデータを保護するために役立つツールを提供しています。

リソースポリシーで `aws:SourceArn`および `aws:SourceAccount` グローバル条件コンテキストキーを使用して、 がリソースに別のサービス AWS Firewall Manager に付与するアクセス許可を制限することをお勧めします。クロスサービスアクセスにリソースを 1 つだけ関連付けたい場合は、`aws:SourceArn` を使用します。そのアカウント内のリソースをクロスサービスの使用に関連付けることを許可する場合は、`aws:SourceAccount` を使用します。

混乱した代理問題から保護するための最も効果的な方法は、リソースの完全な ARN を指定して、`aws:SourceArn` グローバル条件コンテキストキーを使用することです。リソースの完全な

ARN が不明な場合や、複数のリソースを指定する場合には、グローバルコンテキスト条件キー aws:SourceArn で、ARN の未知部分を示すためにワイルドカード文字 (*) を使用します。例えば、arn:aws:fms:*:*account-id*:*。

aws:SourceArn の値に Amazon S3 バケット ARN などのアカウント ID が含まれていない場合は、両方のグローバル条件コンテキストキーを使用して、アクセス許可を制限する必要があります。

の値は、 AWS Firewall Manager 管理者の AWS アカウントaws:SourceArnである必要があります。

次の例では、Firewall Manager で aws:SourceArn グローバル条件コンテキストキーを使用して、混乱した代理問題を防止する方法を示しています。

次の例では、Firewall Manager ロールの信頼ポリシーで aws:SourceArn グローバル条件コンテキストキーを使用して、混乱した代理問題を防止する方法を示しています。*[Region]* (リージョン) および *[Account-ID]* (アカウント ID) をユーザー自身の情報に置き換えます。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
        "Sid": "ConfusedDeputyPreventionExamplePolicy",
        "Effect": "Allow",
        "Principal": {
            "Service": "servicename.amazonaws.com"
        },
        "Action": "sts:AssumeRole",
        "Condition": {
            "ArnLike": {
                "aws:SourceArn": [
                "arn:aws:fms:us-east-1:123456789012:${*}",
    "arn:aws:fms:us-east-1:123456789012:policy/*"
                ]
            },
            "StringEquals": {
                "aws:SourceAccount": "123456789012"
            }
        }
    }
}
```

Firewall Manager でのログ記録とモニタリング

モニタリングは、Firewall Manager と AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、 AWS ソリューションのすべての部分からモニタリングデータを収集する必要があります。 には、Firewall Manager リソースをモニタリングし、潜在的なイベントに対応するための複数のツール AWS が用意されています。

Amazon CloudWatch アラーム

Amazon CloudWatch アラームを使用して、指定した期間にわたって 1 つのメトリクスを確認します。メトリクスが指定されたしきい値を超えると、CloudWatch は Amazon SNS トピックまたは AWS Auto Scaling ポリシーに通知を送信します。詳細については、「Amazon CloudWatch によるモニタリング」を参照してください。

AWS CloudTrail ログ

CloudTrail は、Firewall Manager のユーザー、ロール、または AWS のサービスによって実行されたアクションの記録を提供します。CloudTrail で収集された情報を使用して、Firewall Manager に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。詳細については、「での AWS CloudTrail API コールのログ記録」を参照してください。

Firewall Manager のコンプライアンス検証

新しい AWS サインアップエクスペリエンスは、規制されたワークロード向けには設計されていません。新しい AWS サインアップエクスペリエンスを使用しているが、規制対象のワークロード AWS に を使用する場合は、 AWS (アドバンスド) にサインアップするか、 AWS 環境の高度な機能をアクティブ化できます。

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、「コンプライアンスAWS のサービス プログラムによるスコープ」の「コンプライアンス」を参照して、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「Downloading Reports in AWS Artifact」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。を使用する際のコンプライアンス責任の詳細については AWS のサービス、AWS 「 セキュリティドキュメント」を参照してください。

Firewall Manager の回復力

AWS グローバルインフラストラクチャは、 AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。 は、低レイテンシー、高スループット、高度に冗長なネットワークで接続された、物理的に分離および分離された複数のアベイラビリティーゾーン AWS リージョン を提供します。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断せずに、自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、およびスケーラビリティが優れています。

AWS リージョン およびアベイラビリティーゾーンの詳細については、AWS 「グローバルインフラストラクチャ」を参照してください。

のインフラストラクチャセキュリティ AWS Firewall Manager

マネージドサービスである AWS Firewall Manager は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して環境を AWS 設計するには、「Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

AWS 公開された API コールを使用して、ネットワーク経由で Firewall Manager にアクセスします。クライアントは以下をサポートする必要があります。

- Transport Layer Security (TLS)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

AWS Firewall Manager クォータ

AWS Firewall Manager には、次のクォータが適用されます (以前は制限と呼ばれていました)。

AWS Firewall Manager には、クォータを増やすことができるデフォルトのクォータと固定クォータがあります。

Firewall Manager によって管理されるセキュリティグループポリシーとネットワーク ACL は、標準の Amazon VPC 配分対象となります。詳細については、「Amazon VPC ユーザーガイド」の「Amazon VPC クォータ」を参照してください。

各 Firewall Manager の Network Firewall ポリシーは、関連付けられたファイアウォールポリシーとそのルールグループを使用して Network Firewall ファイアウォールを作成します。これらの Network Firewall リソースは、「Network Firewall デベロッパーガイド」の「AWS Network Firewall クォータ」にリストされているクォータを前提とします。

ソフトクォータ

AWS Firewall Manager には、リージョンあたりのエンティティ数に対するデフォルトのクォータがあります。このクォータの引き上げをリクエストできます。

すべてのポリシータイプ

リソース	リージョンあたりのデフォルトのクォータ
の組織あたりのアカウント AWS Organizations	可変。アカウントに送信された招待はこのクォータに対してカウントされます。

リソース	リージョンあたりのデフォルトのクォータ
	招待されたアカウントが拒否された場合、管理アウントが招待をキャンセルした場合、または招待状の有効期限が切れた場合は、カウントが返されます。
AWS Organizationsの組織ごとの Firewall Manager ポリシー。	50。リージョンの指定 `Global` および `US East (N. Virginia) Region` は同じリージョンを参照しているため、この制限は 2 つのポリシーを組み合わせた合計に適用されます。
Firewall Manager ポリシーあたりの範囲内の組織単位	20
Firewall Manager ポリシーの範囲内にあるアカウント (個々のアカウントを明示的に含めたり除外したりする場合)。	200
Firewall Manager ポリシーの範囲内にあるアカウント (個々のアカウントを明示的に含めたり除外したりしない場合)。	2,500
の組織が Firewall Manager によってオンボーディングされる組織に含める AWS Organizations ことができるアカウント。カウントには Firewall Manager 管理者アカウントが含まれます。	10,000
Firewall Manager ポリシーごとのリソースを含む、または除外するタグ。	8

リソース	リージョンあたりのデフォルトのクォータ
アカウントあたりのリソースセットの数。	20
リソースセットあたりのリソースの数。	100
Firewall Manager ポリシーあたりのリソースセットの数。	5

AWS WAF ポリシー

[リソース]	リージョンあたりのデフォルトのクォータ
AWS WAF Firewall Manager 管理者アカウントあたりの ルールグループ。	100
AWS WAF Firewall Manager 管理者アカウントあたりのクラシックルールグループ。	10
AWS WAF ポリシーあたりのルールグループ。	50
AWS WAF ポリシーあたりのパートナールールグループ。	1

共通セキュリティグループポリシー

[リソース]	リージョンあたりのデフォルトのクォータ。
ポリシーごとのプライマリセキュリティグループ。	3
共有 VPC を含む、アカウントあたりのポリシーごとの範囲内の Amazon VPC インスタンス。	100

コンテンツ監査セキュリティグループポリシー

リソース	リージョンあたりのデフォルトのクォータ
ポリシーごとの監査セキュリティグループ。	1
アプリケーションリストあたりのアプリケーション。	50
すべてのトラフィックを許可するルール用のカスタムマネージドアプリケーションリスト。	1
ポリシールールごとのカスタムマネージドアプリケーションリスト。	1
アカウントあたりのカスタムマネージドアプリケーションリスト。	10
プロトコルリストあたりのプロトコル。	5
ポリシー内における任意の設定のカスタムマネージドプロトコルリスト。	1
アカウントあたりのカスタムマネージドプロトコルリスト。	10

ネットワーク ACL ポリシー

[リソース]	リージョンあたりのデフォルトのクォータ
最初または最後のルールに使用されるネットワーク ACL ポリシーあたりのインバウンドルールの数。例えば、最初のインバウンドルールとして 5 つ、最後のインバウンドルールとして 0 を設定することは可能です。また、最初に 2 つ、最後に 3 つ設定することもできますが、最初に 4 つ、最後に 2 つという設定はできません。	5
ネットワーク ACL ポリシーあたりのアウトバウンドルールの数。最初または最後のルールに使用されます。例えば、最初のアウトバウンドルールとして 5 つ、最後のアウトバウンドルールとして 0 を設定するこ	5

[リソース]	リージョンあたりのデフォルトのクォータ
とは可能です。また、最初に 2 つ、最後に 3 つ設定することもできますが、最初に 4 つ、最後に 2 つという設定はできません。	

Network Firewall ポリシー

[リソース]	リージョンあたりのデフォルトのクォータ
1 つのポリシーに指定できる IPV4 CIDR の数。	50
Network Firewall ポリシーあたりのステートフルルールグループの容量。	30,000

DNS Firewall ポリシー

リソース	リージョンあたりのデフォルトのクォータ
Firewall Manager ポリシーあたりの DNS Firewall ルールグループの数。	2

ハードクォータ

に関連する以下のリージョンごとのクォータは変更 AWS Firewall Manager できません。

すべてのポリシータイプ

[リソース]	リージョンあたりのクォータ
AWS Organizations 組織に含めることができる Firewall Manager 管理者の最大数。1 人の必須デフォルト管理者に加え、最大 9 人の Firewall Manager 管理者を持つことができます。	10

AWS WAF ポリシー

[リソース]	リージョンあたりのクォータ
AWS WAF ポリシー内のルールグループの合計ウェブ ACL キャパシティーユニット (WCU)。	5,000

AWS WAF クラシックポリシー

[リソース]	リージョンあたりのクォータ
AWS WAF ポリシーあたりのクラシックルールグループ。	2: お客様が作成した 1 つのルールグループと 1 つの AWS Marketplace ルールグループ。
AWS WAF Firewall Manager Classic ルールグループあたりの AWS WAF Classic ルール。	10

Network Firewall ポリシー

リソース	リージョンあたりのクォータ
1 つのポリシーについて自動的に修正できる VPC の数。	1,000

リソース	リージョンあたりのクォータ
Network Firewall ポリシーあたりのステートレスルールグループ数。	20
Network Firewall ポリシーあたりのステートフルルールグループ数。	20
Network Firewall ポリシーあたりのステートレスルールグループの容量。	30,000

Firewall Manager での AWS WAF Classic ウェブ ACLs移行

Firewall Manager が AWS WAF Classic WebACLs を使用するシナリオは 2 つあります。

1. AWS WAF Classic ポリシーを使用する
2. 2022 年 1 月より前に作成された Shield Advanced ポリシーを使用する

AWS WAF Classic ポリシーでのウェブ ACLs移行

AWS WAF Classic ポリシーからウェブ ACLs を移行するには、まず AWS WAF Classic ルールグループを AWS WAF (v2) ルールグループに移行する必要があります。その後、移行されたルールグループを使用して新しいポリシーを作成できます。

1. この移行スクリプト: AWS WAF 一括移行スクリプトを使用して AWS WAF Classic 、ルールグループを AWS WAF (v2) ルールグループに移行します。
2. 次の設定で新しい AWS WAF ポリシーを作成します。
   - 新しく移行された AWS WAF (v2) ルールグループを使用する
   - 自動修復を有効にする
3. 移行するアカウントごとに、次の操作を行います。
   a. 古い AWS WAF Classic ポリシーからアカウントを削除する
   b. 約 2～3 分待つ
   c. 新しい AWS WAF ポリシーのスコープにアカウントを追加する
   d. (オプション) リソースタグフィルタリングを使用してポリシーの範囲を特定のリソースに絞り込む

4. 移行を確認します。

    a. 新しい AWS WAF ポリシーで v2 ウェブ ACLs
    b. Firewall Manager が新しいウェブ ACL を適切なリソースに関連付けたことを確認する

Shield アドバンストポリシーでのウェブ ACL の移行

Firewall Manager の自動アプリケーションレイヤー DDoS 緩和は、 AWS WAF (v2) を使用して作成されたウェブ ACLsします。Firewall Manager ポリシーで自動緩和を使用し、ポリシーが現在 AWS WAF Classic ウェブ ACLs、それらを AWS WAF (v2) に移行する必要があります。すべてのウェブ ACL を一度に移行することも、一度に 1 つのアカウントに移行することもできます。

すべてのウェブ ACL を一度に移行する

Shield Advanced ポリシー内のすべてのウェブ ACL を一度に移行するには、ポリシーの自動修復機能を使用できます。

1. Firewall Manager コンソール (https://console.aws.amazon.com/wafv2/fms) を開きます。
2. Shield Advanced ポリシーを選択します。
3. 自動修復を有効にし、 AWS WAF Classic ウェブ ACLs を AWS WAF (v2) ウェブ ACLsオプションを選択します。

Firewall Manager は、必要に応じて新しい AWS WAF (v2) ウェブ ACLs を作成し、 Classic から v2 ウェブ ACLs へのリソース関連付けの移行を管理します。

ウェブ ACL を一度に 1 つのアカウントに移行する

ウェブ ACL を一度に 1 つのアカウントに移行するには、次の手順に従います。

1. 以下の設定で、新しい Shield Advanced ポリシーを作成します。
    - 自動アプリケーションレイヤー DDoS 自動緩和を 無効 に設定する
    - 自動修復を有効にする
2. 移行するアカウントごとに、次の操作を行います。

    a. 古い Shield Advanced ポリシーからアカウントを削除する
    b. 約 2～3 分待つ
    c. 新しい Shield Advanced ポリシーの範囲にアカウントを追加する

d. (オプション) リソースタグフィルタリングを使用してポリシーの範囲を特定のリソースに絞り込む

3. 移行を確認します。

a. 新しい Shield Advanced ポリシーで AWS WAF (v2) ウェブ ACLs

b. Firewall Manager が新しいウェブ ACL を適切なリソースに関連付けたことを確認する

モニタリング AWS WAF、 AWS Firewall Manager、および AWS Shield Advanced

モニタリングは、サービスの信頼性、可用性、パフォーマンスを維持するうえで重要な部分です。

> **Note**
>
> Shield Advanced リソースをモニタリングし、Shield Advanced を使用して発生する可能性のある DDoS イベントを特定する方法については、「AWS Shield」を参照してください。

これらのサービスのモニタリングを開始する前に、次の質問に対する回答を反映したモニタリング計画を作成する必要があります。

- どのような目的でモニタリングしますか?
- どのリソースをモニタリングしますか?
- どのくらいの頻度でこれらのリソースをモニタリングしますか?
- どのモニタリングツールを利用しますか?
- 誰がモニタリングタスクを実行しますか?
- 問題が発生したときに誰が通知を受け取りますか?

次のステップでは、さまざまなタイミングと負荷条件でパフォーマンスを測定することにより、お客様の環境で通常のパフォーマンスのベースラインを確定します。Firewall Manager AWS WAF、Shield Advanced、および関連サービスのモニタリング中に、履歴モニタリングデータを保存して、現在のパフォーマンスデータと比較し、通常のパフォーマンスパターンとパフォーマンス異常を特定し、問題に対処する方法を考案できるようにします。

では AWS WAF、ベースラインを確立するために、少なくとも次の項目をモニタリングする必要があります。

- 許可されたウェブリクエストの数
- ブロックされたウェブリクエストの数

トピック

- モニタリングツール
- Amazon CloudWatch によるモニタリング
- での AWS CloudTrail API コールのログ記録

モニタリングツール

AWS には、 AWS WAF および のモニタリングに使用できるさまざまなツールが用意されています AWS Shield Advanced。これらのツールの中には、自動モニタリングを設定できるものもあれば、手動操作を必要とするものもあります。モニタリングタスクをできるだけ自動化することをお勧めします。

自動モニタリングツール

次の自動モニタリングツールを使用して、問題を監視 AWS WAF AWS Shield Advanced および報告できます。

- 保護パック (ウェブ ACL) トラフィック概要ダッシュボード – AWS WAF コンソールのウェブ ACL のページに移動し、トラフィック概要タブを開いて、保護パック (ウェブ ACL) が評価するウェブトラフィックの概要にアクセスします。

  トラフィック概要ダッシュボードには、アプリケーションウェブトラフィックを評価するときにが AWS WAF 収集する Amazon CloudWatch メトリクスのほぼリアルタイムの概要が表示されます。すべてのウェブトラフィックと、インテリジェントな脅威軽減ルールグループによって評価されたトラフィックの概要を確認できます。これには、AI ボットとエージェントのアクティビティに特化した AI トラフィック分析が含まれます。

  詳細については、「保護パック (ウェブ ACL) のトラフィック概要ダッシュボード」を参照するか、コンソールのダッシュボードに移動してください。

- Amazon CloudWatch アラーム - 指定した期間にわたって単一のメトリクスをモニタリングし、複数の期間にわたる特定のしきい値に対するメトリクスの値に基づいて 1 つ以上のアクションを実行します。アクションは Amazon Simple Notification Service (Amazon SNS) のトピックまたは Amazon EC2 Auto Scaling のポリシーに送信される通知です。アラームは持続している状態変化に対してのみアクションを呼び出します。CloudWatch アラームは、メトリクスが特定の状態になっただけではアクションを呼び出しません。アクションを呼び出すには、状態が変化して、指定した期間継続している必要があります。詳細については、「CloudWatch を使用した CloudFront アクティビティのモニタリング」を参照してください。

> **Note**
>
> CloudWatch メトリクスとアラームは有効になっていません AWS Firewall Manager。

「」で説明されているように、CloudWatch を使用して AWS WAF および Shield Advanced メトリクスをモニタリングできるだけでなくAmazon CloudWatch によるモニタリング、CloudWatch を使用して保護されたリソースのアクティビティをモニタリングすることもできます。詳細については次を参照してください:

- 「Amazon CloudFront デベロッパーガイド」の「Monitoring CloudFront Activity Using CloudWatch」(CloudWatch を使用した CloudFront アクティビティのモニタリング)
- 「API Gateway デベロッパーガイド」の「Logging and monitoring in Amazon API Gateway」(Amazon API Gateway でログ記録とモニタリング)
- 「エラスティックロードバランサーユーザーガイド」の「CloudWatch Metrics for Your Application Load Balancer」(Application Load Balancer 向け CloudWatch メトリクス)
- 「AWS AppSync デベロッパーガイド」の「Monitoring and Logging」(モニタリングとログ記録)
- 「Amazon Cognito デベロッパーガイド」の「Logging and monitoring in Amazon Cognito」(Amazon Cognito でログ記録とモニタリング)
- 「AWS App Runner デベロッパーガイド」の「CloudWatch Log にストリーミングされた App Runner ログの表示」と「CloudWatch に報告された App Runner サービスメトリクスの表示」

- Amazon CloudWatch Logs – AWS CloudTrail またはその他のソースからログファイルをモニタリング、保存、アクセスします。詳細については、「Amazon CloudWatch Logs とは」を参照してください。
- Amazon CloudWatch Events – AWS サービスを自動化し、システムイベントに自動的に応答します。 AWS サービスからのイベントはほぼリアルタイムで CloudWatch Events に配信され、イベントが記述したルールと一致するときに実行する自動アクションを指定できます。詳細については、「Amazon CloudWatch Events とは」を参照してください。
- AWS CloudTrail ログモニタリング – アカウント間でログファイルを共有し、CloudWatch Logs に送信CloudWatch CloudTrail ログファイルをリアルタイムでモニタリングし、Java でログ処理アプリケーションを書き込み、CloudTrail による配信後にログファイルが変更されていないことを確認します。詳細については、「での AWS CloudTrail API コールのログ記録」と、AWS CloudTrail ユーザーガイドの「CloudTrail ログファイルの操作」を参照してください。
- AWS Config – AWS リソースの相互関係や過去の設定など、アカウント AWS 内のリソースの設定を表示して、設定と関係が時間の経過とともにどのように変化するかを確認できます。

手動モニタリングツール

モニタリングのもう 1 つの重要な部分は AWS WAF 、CloudWatch アラームでカバーされていない項目を手動でモニタリング AWS Shield Advanced することです。 AWS WAF、Shield Advanced、CloudWatch、およびその他の AWS マネジメントコンソール ダッシュボードを表示して、環境の状態 AWS を確認できます。ウェブ ACL とルールのログファイルも確認することをお勧めします。

- たとえば、 AWS WAF ダッシュボードを表示するには:
  - AWS WAF ウェブ ACLs ページのリクエストタブで、作成した各ルールに一致するリクエストとリクエストの合計のグラフを表示します。詳細については、「ウェブリクエストのサンプルの表示」を参照してください。
- CloudWatch のホームページで次の情報を確認します。
  - 現在のアラームとステータス
  - アラームとリソースのグラフ
  - サービスのヘルスステータス

  また、CloudWatch を使用して、次のことが可能です。
  - 重視するサービスをモニタリングするためのカスタマイズしたダッシュボードを作成する。
  - メトリクスデータをグラフ化して、問題をトラブルシューティングして、傾向を確認する。
  - すべての AWS リソースメトリクスを検索して参照します。
  - 問題があることを通知するアラームを作成および編集する。

Amazon CloudWatch によるモニタリング

Amazon CloudWatch を使用してウェブリクエスト、ウェブ ACLs、ルールをモニタリングできます。Amazon CloudWatch は、raw データを収集し、読み取り可能なほぼリアルタイムのメトリクス AWS WAF AWS Shield Advanced に加工します。 Amazon CloudWatch Amazon CloudWatch の統計を使用して、ウェブアプリケーションやサービスの動作状況を把握できます。詳細については、「Amazon CloudWatch ユーザーガイド」の「CloudWatch とは」を参照してください。

> **Note**
>
> CloudWatch メトリクスとアラームは、Firewall Manager に対応していません。

アラームの状態が変わったときに Amazon SNS メッセージを送信する Amazon CloudWatch のアラームを作成することができます。アラームは、指定期間にわたって 1 つのメトリクスを監視し、複数期間にわたる指定しきい値との比較結果に基づいて 1 つ以上のアクションを実行します。アクションは、Amazon SNS のトピックまたは Auto Scaling のポリシーに送信される通知です。アラームは、持続している状態変化に対してのみアクションを呼び出します。CloudWatch のアラームは、メトリクスが特定の状態にあるだけではアクションを呼び出しません。アクションを呼び出すには、指定した期間継続している必要があります。

トピック

- メトリクスおよびディメンションの表示
- AWS WAF メトリクスとディメンション
- AWS Shield Advanced メトリクス
- AWS Firewall Manager 通知

メトリクスおよびディメンションの表示

メトリクスは、最初にサービス名前空間によってグループ化され、次に各名前空間内のさまざまなディメンションの組み合わせによってグループ化されます。メトリクスは記録 AWS Firewall Manager されません。

- AWS WAF 名前空間は です。 `AWS/WAFV2`
- Shield Advanced の名前空間は `AWS/DDoSProtection` です

> **Note**
>
> AWS WAF は 1 分に 1 回メトリクスを報告します。
> Shield Advanced は、イベント中 1 分に 1 回メトリクスをレポートし、イベント以外ではその頻度は少なくなります。

および のメトリクスを表示するには、次の手順を使用します AWS WAF AWS Shield Advanced。

CloudWatch コンソールを使用してメトリクスを表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。

2. 必要に応じて、リージョンを AWS リソースがあるリージョンに変更します。CloudFront の場合、米国東部 (バージニア北部) リージョンを選択する必要があります。
3. ナビゲーションペインの [Metrics] (メトリクス) で、[All metrics] (すべてのメトリクス) を選択し、[Browse] (参照) タブでサービスを検索します。

CLI AWS を使用してメトリクスを表示するには

- AWS/WAFV2 の場合、コマンドプロンプトで次のコマンドを使用します。

```
aws cloudwatch list-metrics --namespace "AWS/WAFV2"
```

  Shield Advanced の場合、コマンドプロンプトで次のコマンドを使用します。

```
aws cloudwatch list-metrics --namespace "AWS/DDoSProtection"
```

AWS WAF メトリクスとディメンション

AWS WAF は、メトリクスを 1 分に 1 回レポートします。 はAWS/WAFV2、名前空間にメトリクスとディメンション AWS WAF を提供します。

AWS WAF メトリクスの概要情報は、 AWS WAF コンソールの 保護パック (ウェブ ACL) のトラフィック概要タブで確認できます。詳細については、保護パック (ウェブ ACL) のトラフィック概要ダッシュボード を参照してください。

保護パック (ウェブ ACL)、ルール、ルールグループ、ラベルには、次のメトリクスが表示されます。

> **Note**
>
> Application Load Balancer がルールやその他のアクティブな設定を持たない保護パック (ウェブ ACL) に関連付けられている場合、 AWS WAF はその Application Load Balancer のサンプリングされたリクエストを提供せず、CloudWatch メトリクスを発行しません。この動作とオブザーバビリティ機能を有効にする方法の詳細については、「」を参照してくださいAWS WAF 分散サービス拒否 (DDoS) の防止。

- ルール – メトリクスはルールアクションによってグループ化されます。例えば、Count モードでルールをテストする場合、一致したルールが保護パック (ウェブ ACL) の Count メトリクスとして一覧表示されます。
- ルールグループ – ルールグループのメトリクスは、ルールグループメトリクスの下に一覧表示されます。
- 別のアカウントが所有するルールグループ – ルールグループメトリクスは、通常、ルールグループの所有者にのみ表示されます。ただし、ルールのルールアクションを上書きすると、そのルールのメトリクスが保護パック (ウェブ ACL) メトリクスの下に一覧表示されます。さらに、ルールグループによって追加されたラベルは、保護パック (ウェブ ACL) メトリクスに一覧表示されます。

  ルールグループのカウントアクションルールは、ウェブ ACL ディメンションメトリクスを出力しません - Rule、RuleGroup、およびリージョンディメンションのみ。これは、ルールグループがウェブ ACL で参照されている場合でも適用されます。

  このカテゴリにあるルールグループは AWS の マネージドルール AWS WAF、AWS Marketplace ルールグループ、他のサービスによって提供されるルールグループを識別する、また、他のアカウントから共有されたルールグループも含まれます。Firewall Manager を介して保護パック (ウェブ ACL) がデプロイされると、カウントアクションを持つ WebACL 内のルールはメンバーアカウントにメトリクスを表示しません。
- ラベル – 評価中にウェブリクエストに追加されたラベルは、保護パック (ウェブ ACL) のラベルメトリクスに一覧表示されます。自分のルールやルールグループによって追加されたか、他のアカウントが所有するルールグループのルールによって追加されたかにかかわらず、すべてのラベルのメトリクスにアクセスできます。

トピック

- AWS WAF コアメトリクスとディメンション
- ラベルメトリクスとディメンション
- 無料のボット可視性メトリクスおよびディメンション
- アカウントメトリクスとディメンション
- AWS WAF 使用状況メトリクス

AWS WAF コアメトリクスとディメンション

AWS WAF コアメトリクス

メトリクス	説明
`AllowedRequests`	許可されたウェブリクエストの数。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
`BlockedRequests`	ブロックされたウェブリクエストの数。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
`CountedRequests`	カウントされたウェブリクエストの数。 レポート条件: ゼロ以外の値がある。 カウントされたウェブリクエストは、少なくとも 1 つのルールに一致するリクエストです。リクエストカウントは、通常、テストに使用されます。 有効な統計: Sum
`CaptchaRequests`	CAPTCHA コントロールが適用されたウェブリクエストの数。終了ルールを表し、 は含まれませんRequestsWithValidCaptchaToken 。 レポート条件: ゼロ以外の値がある。 CAPTCHA ウェブリクエストは、CAPTCHA アクション設定を持つルールに一致するリクエストです。このメトリクスは、CAPTCHA トークンが有効期限切れである、無効である、存在しない、または一致していないドメインを持っているかどうかに関係なく、一致するすべてのリクエストを記録します。

メトリクス	説明
	有効な統計: Sum
RequestsWithValidCaptchaToken	CAPTCHA コントロールが適用され、有効な CAPTCHA トークンを持つウェブリクエストの数。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
CaptchasAttempted	CAPTCHA パズルチャレンジに応答してエンドユーザーから送信されたソリューションの数。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
CaptchasSolved	パズルを正解し、送信された CAPTCHA パズルソリューションの数。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
ChallengeRequests	チャレンジコントロールが適用されたウェブリクエストの数。終了ルールを表し、 は含まれませんRequestsWithValidChallengeToken 。 レポート条件: ゼロ以外の値がある。 チャレンジウェブリクエストは、Challenge アクション設定を持つルールに一致するリクエストです。このメトリクスは、チャレンジトークンが有効期限切れである、無効である、存在しない、または一致していないドメインを持っているかどうかに関係なく、一致するすべてのリクエストを記録します。 有効な統計: Sum

メトリクス	説明
ChallengesAttempted	が提供するサイレントチャレンジに応答してエンドユーザーから送信された試行の数 AWS WAF。これには、Challengeルールアクションによって提供されるチャレンジと、トークンが存在しない場合にCAPTCHAアクションの一部として実行されるチャレンジが含まれます。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
ChallengesSolved	が提供するサイレントチャレンジに正常に合格した、送信されたサイレントチャレンジソリューションの数 AWS WAF。これには、Challengeルールアクションによって提供されるチャレンジと、トークンが存在しない場合にCAPTCHAアクションの一部として実行されるチャレンジが含まれます。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
PassedRequests	渡されたリクエストの数。これは、ルールグループのルールのいずれとも一致せず、ルールグループ評価を通過するリクエストについてのみ使用されます。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
RequestsWithValidChallengeToken	チャレンジコントロールが適用され、有効なチャレンジトークンを持つウェブリクエストの数。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum

メトリクス	説明
LowReputationPacketsDropped	既知の悪意のあるソースから削除されたパケットの数。このメトリクスは、リクエストがリソースレベルの DDoS 保護によってブロックされたときに記録されます。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum このメトリクスは、AWS/ApplicationELB 名前空間に公開されます。
LowReputationRequestsDenied	HTTP 403 レスポンスで拒否された HTTP リクエストの数。このメトリクスは、リクエストがリソースレベルの DDoS 保護によってブロックされたときに記録されます。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum このメトリクスは、AWS/ApplicationELB 名前空間に公開されます。
MonetizeRequests	収益化コントロールが適用されたウェブリクエストの数。収益化アクションを持つ終了ルールを表します。 レポート条件: ゼロ以外の値がある。 収益化ウェブリクエストは、収益化アクション設定を持つルールに一致するリクエストです。このメトリクスは、一致するすべてのリクエストを記録します。 有効な統計: Sum

メトリクス	説明
MonetizeRequestsFailedVerification	収益化コントロールが適用され、収益化の検証に失敗したウェブリクエストの数。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum

AWS WAF コアディメンション

ディメンション	説明
Region	Amazon CloudFront ディストリビューションを除くすべての保護されたリソースタイプで必要です。
Rule	次のいずれかです。 • Rule のメトリクス名。 • すべて。これは、WebACL または RuleGroup 内のすべてのルールを表します。 • Default_Action (WebACL ディメンションと組み合わせた場合のみ)。これは、保護パック (ウェブ ACL) のルールのアクションによって評価が終了されなかったリクエストに割り当てられたアクションを表します。
RuleGroup	RuleGroup のメトリクス名。
WebACL	WebACL のメトリクス名。
WebACLArn	Web ACL の Amazon リソースネーム (ARN)。このディメンションは、 AWS WAF が有効になっている場合にのみ使用できます。
ResourceType	CF、APIGW、ALB など、保護されたリソースのタイプ。

ディメンション	説明
Resource	保護されたリソースの Amazon リソースネーム (ARN)。 このディメンションには App Runner リソース ARN は含まれません。
Country	リクエストの送信元の国 これは、国際標準化機構 (ISO) 3166 規格の 2 文字の名称です。たとえば、米国は US、ウクライナは UA です。 リクエストに X-Forwarded-For ヘッダーがある場合、 AWS WAF はそのヘッダーを使用してこの設定を決定します。それ以外の場合は、 AWS WAF はクライアント IP の国を使用します。この決定は、オリジン国を決定するためにルールで使用する口ジックとは無関係です。 は、MaxMind GeoIP データベースを使用して IPs の場所 AWS WAF を決定します。
Attack	ウェブ ACL で使用するルールとルールグループに基づいて、リクエストで が AWS WAF 識別した攻撃のタイプ。 ルールとベースライン AWS マネージドルールグループのルールは、攻撃タイプを識別できます。たとえば、クロスサイトスクリプティング (XSS) ルール一致は XSS 攻撃タイプを識別し、レートベースのルールはボリューム攻撃タイプを識別します。攻撃タイプは、通常、ウェブリクエストの評価を終了したルールのタイプを示します。
Device	ウェブリクエストの user-agent ヘッダーから取得した、リクエストを送信したクライアントのデバイスタイプ。

ディメンション	説明
LoadBalancerArn	ロードバランサーの Amazon リソースネーム (ARN)。
LoadBalancerArnAvailabilityZone	ロードバランサー ARN とアベイラビリティーゾーンの組み合わせ。
ManagedRuleGroup	ManagedRuleGroup のメトリクス名。
ManagedRuleGroupRule	一致した ManagedRuleGroup 内のルール。
VulnerabilityCategory	AWS マネージドルール IP セットに基づいて、リクエストが一致する脆弱性カテゴリ。

ラベルメトリクスとディメンション

ルールおよび保護パック (ウェブ ACL) で使用するマネージドルールグループによる評価中に、リクエストに追加されたラベルのメトリクス。詳細については、「ウェブリクエストのラベル付け」を参照してください。

1 つのウェブリクエストについて、 は最大 100 個のラベルのメトリクス AWS WAF を保存します。保護パック (ウェブ ACL) 評価では、100 個を超えるラベルを適用したり、100 個を超えるラベルと照合したりできますが、メトリクスには最初の 100 個のみが反映されます。

ラベルメトリクス

メトリクス	説明
AllowedRequests	アクション設定 Allow を適用したウェブリクエストのラベルの数。ラベルは、ウェブリクエストの評価中のどの時点でも追加できます。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
BlockedRequests	アクション設定 Block を適用したウェブリクエストのラベルの数。ラベルは、ウェブリクエストの評価中のどの時点でも追加できます。

メトリクス	説明
	レポート条件: ゼロ以外の値がある。 有効な統計: Sum
CountedRequests	Count アクション設定を持つルールグループルールによってウェブリクエストに追加されるラベルの数。 このメトリクスは、ルールグループ内のルールについて、ルールグループの所有者のみが使用できます。その他のケースでは、リクエストに適用された終了アクション (Allow または Block など) にカウントラベルメトリクスがまとめられます。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
CaptchaRequests	終了 CAPTCHA アクションが適用されたウェブリクエストのラベルの数。ラベルは、ウェブリクエストの評価中のどの時点でも追加できます。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
ChallengeRequests	終了 Challenge アクションが適用されたウェブリクエストのラベルの数。ラベルは、ウェブリクエストの評価中のどの時点でも追加できます。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum

メトリクス	説明
AllowRuleMatch	関連付けられたラベルを生成し、Allow アクションを使用してリクエスト評価を終了した一致ルールの数。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
BlockRuleMatch	関連付けられたラベルを生成し、Block アクションを使用してリクエスト評価を終了した一致ルールの数。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
CountRuleMatch	関連付けられたラベルを生成し、Count アクションを適用した一致ルールの数。 複数のルールが同じラベルとアクションで設定されている場合、1 つのリクエストでこのメトリクスの複数のインスタンスが発生する可能性があります。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
CaptchaRuleMatch	関連付けられたラベルを生成し、CAPTCHA アクションを使用してリクエスト評価を終了した一致ルールの数。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum

メトリクス	説明
ChallengeRuleMatch	関連付けられたラベルを生成し、Challenge アクションを使用してリクエスト評価を終了した一致ルールの数。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
CaptchaRuleMatchWithValidToken	関連付けられたラベルを生成し、終了していない CAPTCHA アクションを適用した一致ルールの数。 複数のルールが同じラベルとアクションで設定されている場合、1 つのリクエストでこのメトリクスの複数のインスタンスが発生する可能性があります。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
ChallengeRuleMatchWithValidToken	関連付けられたラベルを生成し、終了していない Challenge アクションを適用した一致ルールの数。 複数のルールが同じラベルとアクションで設定されている場合、1 つのリクエストでこのメトリクスの複数のインスタンスが発生する可能性があります。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum

ラベルディメンション

ディメンション	説明
Region	Amazon CloudFront ディストリビューションを除くすべての保護されたリソースタイプで必要です。

ディメンション	説明
RuleGroup	RuleGroup のメトリクス名。メトリクス CountedRequests に使用されます。
WebACL	WebACL のメトリクス名。
ResourceType	CF、APIGW、ALB など、保護されたリソースのタイプ。
Resource	保護されたリソースの Amazon リソースネーム (ARN)。
LabelNamespace	リクエストに追加されたラベルの名前空間プレフィックス。
Label	リクエストに追加されたラベルの名前。
Context	ラベル追加のコンテキストとして機能するマネージドルールグループ。たとえば、 などのトークン管理ラベルのコンテキストawswaf:managed:token:accepted は、Bot Control や ATP AWS WAF マネージドルールグループなど、リクエストでトークン管理を使用するマネージドルールグループです。このディメンションはすべてのラベルに適用されるわけではありません。

無料のボット可視性メトリクスおよびディメンション

保護パック (ウェブ ACL) で Bot Control を使用しない場合、 は Bot Control マネージドルールグループをウェブリクエストのサンプリングに追加コストなしで AWS WAF 適用します。これにより、保護対象リソースに流入するボットトラフィックを把握できます。Bot Control については、「AWS WAF Bot Control ルールグループ」を参照してください。

無料のボット可視性メトリクス

メトリクス	説明
SampleAllowedRequest	Allow アクションを持つサンプル化したリクエストの割合。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
SampleBlockedRequest	Block アクションを持つサンプル化したリクエストの割合。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
SampleCaptchaRequest	CAPTCHA アクションを持つサンプル化したリクエストの割合。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
SampleChallengeRequest	Challenge アクションを持つサンプル化したリクエストの割合。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
SampleCountRequest	Count アクションを持つサンプル化したリクエストの割合。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum

無料のボット可視性ディメンション

ディメンション	説明
Region	Amazon CloudFront ディストリビューションを除くすべての保護されたリソースタイプで必要です。
WebACL	WebACL のメトリクス名。
BotCategory	ウェブリクエストのラベルに基づく、検出されたボットカテゴリ名。
VerificationStatus	ウェブリクエストのラベルに基づく、検出されたボット検証ステータス名。
Signal	ウェブリクエストのラベルに基づく、検出されたボットシグナル名。

アカウントメトリクスとディメンション

アカウントメトリクスは、JavaScript API を介してサービスが提供された CAPTCHA パズルとサイレント Challenge ルールアクションに関するアカウント全体の情報を提供します。

アカウントメトリクス

メトリクス	説明
CaptchasAttemptedSdk	CAPTCHA JavaScript API を通じて出されたパズルに対して、エンドユーザーが CAPTCHA パズルチャレンジを応答するために提出したソリューションの数。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
CaptchasSolvedSdk	CAPTCHA JavaScript API を通じて提供されたパズルについて、パズルを正常に解決した CAPTCHA パズルソリューションの送信数。

メトリクス	説明
	レポート条件: ゼロ以外の値がある。 有効な統計: Sum
ChallengesAttemptedSdk	Challenge JavaScript API を通じて提供されるサイレントチャレンジに応答してエンドユーザーから送信された試行の数。これには、Challengeアクションによって開始されたチャレンジと、トークンが存在しない場合にCAPTCHAアクションの一部として実行されるチャレンジが含まれます。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum
ChallengesSolvedSdk	Challenge JavaScript API を通じて処理されたサイレントチャレンジに正常に合格した、送信されたサイレントチャレンジソリューションの数。これには、Challengeアクションによって開始されたチャレンジと、トークンが存在しない場合にCAPTCHAアクションの一部として実行されるチャレンジが含まれます。 レポート条件: ゼロ以外の値がある。 有効な統計: Sum

アカウントディメンション

ディメンション	説明
Region	Amazon CloudFront ディストリビューションを除くすべての保護されたリソースタイプで必要です。

AWS WAF 使用状況メトリクス

CloudWatch 使用状況メトリクスを使用して、アカウントのリソースの使用状況を把握できます。これらのメトリクスを使用して、CloudWatch グラフやダッシュボードで現在のサービスの使用状況を可視化できます。

AWS WAF 使用状況メトリクスは、 AWS サービスクォータに対応しています。使用量がサービスクォータに近づいたときに警告するアラームを設定することもできます。CloudWatch とサービスクオータの統合については、「Amazon CloudWatch ユーザーガイド」の「AWS 使用状況メトリクス」を参照してください。

AWS WAF は、 AWS/Usage名前空間に次のメトリクスを発行します。

使用状況メトリクス

メトリクス	説明
ResourceCount	アカウントの指定されたリソースの数。リソースはメトリクスに関連付けられたディメンションによって定義されます。 このメトリクスで最も役に立つ統計は MAXIMUM です。これは1 分間の期間中に使用されるリソースの最大数を表します。

次のディメンションは、 によって発行される使用状況メトリクスを絞り込むために使用されます AWS WAF。

使用状況ディメンション

ディメンション	説明
Resource	使用状況が報告されるリソースのタイプ。

Resource ディメンションでサポートされている値を次に示します。

Resource値

値	説明
WebAclsPerAccountCloudFront	アカウントあたりの CloudFront で顧客が持っている保護パック (ウェブ ACL) の数。このメトリクスは、CloudFront に少なくとも 1 つの保護パック (ウェブ ACL) がある場合にのみ使用可能です。
WebAclsPerAccountRegional	アカウントあたりのリージョンで顧客が持っている保護パック (ウェブ ACL) の数。このメトリクスは、そのリージョンに少なくとも 1 つの保護パック (ウェブ ACL) がある場合にのみ使用使用可能です。
RuleGroupsPerAccountCloudFront	アカウントあたりの CloudFront で顧客が持っているルールグループの数。このメトリクスは、CloudFront に少なくとも 1 つのルールグループがある場合にのみ使用可能です。
RuleGroupsPerAccountRegional	アカウントあたりのリージョンで顧客が持っているルールグループの数。このメトリクスは、そのリージョンに少なくとも 1 つのルールグループがある場合にのみ使用可能です。
IpSetsPerAccountCloudFront	アカウントあたりの CloudFront で顧客が持っている IP セットの数。このメトリクスは、CloudFront に少なくとも 1 つの IP セットがある場合にのみ使用可能です。
IpSetsPerAccountRegional	アカウントあたりのリージョンにで顧客が持っている IP セットの数。このメトリクスは、そのリージョンに少なくとも 1 つの IP セットがある場合にのみ使用可能です。
RegexPatternSetsPerAccountCloudFront	アカウントあたりの CloudFront で顧客が持っている正規表現パターンセットの数。このメトリクスは、CloudFront に少なくとも 1 つの正規表現パターンが設定されている場合にのみ使用可能です。

値	説明
RegexPatternSetsPerAccountRegional	アカウントあたりのリージョンで顧客が持っている正規表現パターンセットの数。このメトリクスは、そのリージョンに少なくとも 1 つの正規表現パターンが設定されている場合にのみ使用可能です。

AWS Shield Advanced メトリクス

Shield Advanced は、保護するすべてのリソースの Amazon CloudWatch 検出、緩和とトップコントリビューターのメトリクスを発行します。これらのメトリクスにより、リソースに関する CloudWatch ダッシュボードとアラームを作成および設定できるようになるため、それらのリソースをより良くモニタリングできます。

Shield Advanced コンソールには、記録する多くのメトリクスの概要が表示されます。詳細については、「Shield Advanced による DDoS イベントの可視性」を参照してください。

アプリケーションレイヤー保護の自動アプリケーションレイヤー DDoS 緩和を有効にすると、Shield Advanced は自動保護の管理に使用するルールグループを保護パック (ウェブ ACL) に追加します。このルールグループは AWS WAF メトリクスを生成しますが、表示することはできません。これは、 AWS マネージドルールルールグループなど、保護パック (ウェブ ACL) で使用する他のルールグループと同じですが、所有していません。 AWS WAF メトリクスの詳細については、「」を参照してくださいAWS WAF メトリクスとディメンション。Shield Advanced 保護オプションの機能については、Shield Advanced によるアプリケーションレイヤー DDoS 自動緩和 を参照してください。

メトリクスレポートの位置

Shield Advanced は、次のように、米国東部 (バージニア北部) (us-east-1) リージョンのメトリクスをレポートします。

- グローバルサービスの Amazon CloudFront と Amazon Route 53。
- 保護グループ 保護グループについては、「AWS Shield Advanced 保護のグループ化」を参照してください。

他のリソースタイプについては、Shield Advanced がリソースのリージョンのメトリクスをレポートします。

メトリクスレポートの時点

Shield Advanced は、DDoS イベント中、進行中のイベントがない場合よりも頻繁に AWS リソースのメトリクスを Amazon CloudWatch に報告します。Shield Advanced は、イベント中は 1 分ごとに、およびイベント終了直後に 1 回、メトリクスをレポートします。

イベントが発生していない間、Shield Advanced は 1 日に 1 回、リソースに割り当てられた時間にメトリクスを報告します。この定期的なレポートにより、メトリクスをアクティブに保ち、カスタム CloudWatch アラームとダッシュボードで使用できるようにします。

アラームの推奨

注意が必要な状況を通知するアラームを作成することをお勧めします。開始点として、`DDoSDetected` 検出メトリクスがゼロ以外の場合にレポートする保護されたリソースごとにアラームを作成できます。このメトリクスのゼロ以外の値は、DDoS 攻撃が進行中であることを必ずしも意味するわけではありませんが、メトリクスがこの状態にある場合は、リソースのステータスを詳しく調べることをお勧めします。

リクエストフラッドについては、アプリケーションのヘルスやウェブリクエストの量などの要素も考慮する複合チェックのアラームを作成することをお勧めします。さまざまな攻撃ベクトルディメンションのトラフィック量を報告する他の 3 つのメトリクスでアラームを発することを選択できます。アプリケーションの容量を考慮し、トラフィックがアプリケーションの制限に近づいたときにアラームを発信することで、望ましくないノイズを過剰に発生させることなく、必要に応じて通知する一連のルールを作成できます。

トピック

- 検出メトリクス
- 緩和のメトリクス
- 上位の寄稿者のメトリクス

検出メトリクス

Shield Advanced は、`AWS/DDoSProtection` ネームスペースで次の検出メトリクスとディメンションを提供します。

検出メトリクス

メトリクス	説明
DDoSDetected	特定の Amazon リソースネーム (ARN) に対して DDoS イベントが進行中かどうかを示します。 このメトリクスは、イベント中はゼロ以外の値を持ちます。
DDoSAttackBitsPerSecond	特定の Amazon リソースネーム (ARN) の DDoS イベント中に認められたビット数。このメトリクスは、ネットワークおよびトランスポートレイヤー (レイヤー 3 およびレイヤー 4) の DDoS イベントにのみ使用できます。 このメトリクスは、イベント中はゼロ以外の値を持ちます。 単位: ビット
DDoSAttackPacketsPerSecond	特定の Amazon リソースネーム (ARN) の DDoS イベント中に認められたパケット数。このメトリクスは、ネットワークおよびトランスポートレイヤー (レイヤー 3 およびレイヤー 4) の DDoS イベントにのみ使用できます。 このメトリクスは、イベント中はゼロ以外の値を持ちます。 単位: パケット
DDoSAttackRequestsPerSecond	特定の Amazon リソースネーム (ARN) の DDoS イベント中に認められたリクエスト数。このメトリクスは、レイヤー 7 の DDoS イベントのみで使用できます。メトリクスは、特に重要なレイヤー 7 イベントのみについて報告されます。

メトリクス	説明
	このメトリクスは、イベント中はゼロ以外の値を持ちます。 単位: リクエスト
DDoSAttackRequests	特定の Amazon リソースネーム (ARN) の DDoS イベント中に認められたリクエスト数。このメトリクスは、DDoS 対策 DDoS マネージドルール (AMR) DDoS イベントでのみ使用できます。 このメティックは AWS/WAFV2 名前空間にあり、イベント中にゼロ以外の値を持ちます。 単位: リクエスト

Shield Advanced は、他のディメンションなしで DDoSDetected メトリクスを投稿します。残りの検出メトリクスには、次のリストから、攻撃のタイプに対応する AttackVector ディメンションが含まれます。

- ACKFlood
- ChargenReflection
- DNSReflection
- AWS/WAFV2
- GenericUDPReflection
- MemcachedReflection
- MSSQLReflection
- NetBIOSReflection
- NTPReflection
- PortMapper
- RequestFlood
- RIPReflection
- SNMPReflection

- SSDPReflection
- SYNFlood
- UDPFragment
- UDPTraffic
- UDPReflection

緩和のメトリクス

Shield Advanced は、AWS/DDoSProtection ネームスペースで次の検出メトリクスとディメンションを提供します。

緩和のメトリクス

メトリクス	説明
VolumePacketsPerSecond	検出されたイベントに対応してデプロイされた緩和策によってドロップされたか、または渡された 1 秒あたりのパケット数。 単位: パケット

緩和のディメンション

ディメンション	説明
ResourceArn	Amazon リソースネーム (ARN)
MitigationAction	適用された緩和策の結果。想定される値は、Pass または Drop です。

上位の寄稿者のメトリクス

Shield Advanced は、AWS/DDoSProtection ネームスペースにメトリクスを提供します。

上位の寄稿者のメトリクス

メトリクス	説明
VolumePacketsPerSecond	上位のコントリビューターの 1 秒あたりのパケット数。 単位: パケット
VolumeBitsPerSecond	上位のコントリビューターの 1 秒あたりのビット数。 単位: ビット

Shield Advanced は、イベントの寄稿者を特徴づけるディメンションの組み合わせによって、上位の寄稿者のメトリクスを投稿します 上位の寄稿者のあらゆるメトリクスについて、次のいずれかのディメンションの組み合わせを使用できます。

- ResourceArn, Protocol
- ResourceArn, Protocol, SourcePort
- ResourceArn, Protocol, DestinationPort
- ResourceArn, Protocol, SourceIp
- ResourceArn, Protocol, SourceAsn
- ResourceArn, TcpFlags

上位の寄稿者のディメンション

ディメンション	説明
ResourceArn	Amazon リソースネーム (ARN)。
Protocol	TCP または UDP のいずれかの IP プロトコル名。
SourcePort	ソース TCP または UDP ポート。
DestinationPort	宛先 TCP または UDP ポート。
SourceIp	送信元 IP アドレス。

ディメンション	説明
SourceAsn	ソース Autonomous System number (ASN)。
TcpFlags	ダッシュ - で区切られた TCP パケットに存在するフラグの組み合わせ。モニタリング対象フラグは、ACK、FIN、RST、SYN です。このディメンション値は、常にアルファベット順にソートされて表示されます。例: ACK-FIN-RST-SYN 、ACK-SYN、FIN-RST。

AWS Firewall Manager 通知

AWS Firewall Manager はメトリクスを記録しないため、Firewall Manager 専用の Amazon CloudWatch アラームを作成することはできません。ただし、可能性のある攻撃のアラートを送信する Amazon SNS 通知を設定することができます。Firewall Manager で Amazon SNS 通知を作成するには、「ステップ 4: Amazon SNS 通知と Amazon CloudWatch アラームを設定する」を参照してください。

での AWS CloudTrail API コールのログ記録

AWS WAF、 AWS Shield Advanced、 AWS Firewall Manager は、ユーザー AWS CloudTrail、ロール、または サービスによって実行されたアクションを記録する AWS サービスと統合されています。CloudTrail は、、Shield Advanced または Firewall Manager コンソールからの呼び出し、および AWS WAF、Shield Advanced、または Firewall Manager API へのコード呼び出しを含む AWS WAF、これらのサービスの API コールのサブセットをイベントとしてキャプチャします。 APIs 証跡を作成する場合は、、Shield Advanced AWS WAF、Firewall Manager のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、CloudTrail コンソールの [イベント履歴] で最新のイベントを表示できます。CloudTrail で収集された情報を使用して、これらのサービスに対するリクエスト、そのリクエストが発信された IP アドレス、リクエストの作成者、リクエスト作成日時、その他の詳細情報などを確認できます。

設定や有効化の方法など、CloudTrail の詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

CloudTrail は、アカウントの作成 AWS アカウント 時に で有効になります。サポートされるイベントアクティビティが AWS WAF、、Shield Advanced、または Firewall Manager で発生すると、その

アクティビティは、イベント履歴の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。で最近のイベントを表示、検索、ダウンロードできます AWS アカウント。詳細については、CloudTrail イベント履歴でのイベントの表示を参照してください。

Shield Advanced、または Firewall Manager のイベント AWS アカウントなど AWS WAF、 のイベントの継続的な記録については、証跡を作成します。追跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成すると、証跡がすべての リージョンに適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集したイベントデータをより詳細に分析し、それに基づいて対応するため、他の AWS サービスを構成できます。詳細については、次を参照してください:

- 証跡の作成のための概要
- CloudTrail がサポートするサービスと統合
- CloudTrail 用 Amazon SNS 通知の構成
- 複数のリージョンから CloudTrail ログファイルを受け取るおよび複数のアカウントから CloudTrail ログファイルを受け取る

AWS WAF の情報 AWS CloudTrail

すべての AWS WAF アクションは によってログに記録 AWS CloudTrail され、 AWS WAF API リファレンスに記載されています。例えば、`ListWebACL`、`UpdateWebACL`、および `DeleteWebACL` を呼び出すと、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストが、ルートユーザーの認証情報で行われたかどうか
- リクエストの送信に使用された一時的なセキュリティ認証情報に、ロールとフェデレーテッドユーザーのどちらが使用されたか
- リクエストが別の AWS サービスによって行われたかどうか

詳細については、「CloudTrail userIdentity 要素」を参照してください。

クロスアカウント CloudTrail イベント

リソースベースのポリシーを介したクロスアカウントアクセスをサポートする特定の AWS WAF API オペレーションの場合、CloudTrail イベントは発信者アカウントとリソース所有者アカウントの両方に記録されます。これは、次の API オペレーションに適用されます。

- `CreateWebACL`
- `UpdateWebACL`
- `GetWebACL`
- `GetRuleGroup`
- `PutFirewallManagerRuleGroups`

これらのオペレーションがアカウント間で実行されると、呼び出し元のアカウントとリソース所有者のアカウントの両方で、成功した API コールとアクセス拒否コールの両方に対して CloudTrail イベントが生成されます。

例: AWS WAF ログファイルエントリ

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 AWS CloudTrail ログファイルには 1 つ以上のログエントリが含まれます。イベントは、任意の出典からの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどに関する情報が含まれます。CloudTrail ログファイルは、公開 API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

以下は、 AWS WAF 保護パック (ウェブ ACL) オペレーションの CloudTrail ログエントリの例です。

例: `CreateWebACL` の CloudTrail ログエントリ

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
```

```
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T03:43:07Z"
      }
    }
  },
  "eventTime": "2019-11-06T03:44:21Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "CreateWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "defaultAction": {
      "block": {}
    },
    "description": "foo",
    "rules": [
      {
        "name": "foo",
        "priority": 1,
        "statement": {
          "geoMatchStatement": {
            "countryCodes": [
              "AF",
              "AF"
            ]
          }
        },
        "action": {
          "block": {}
        },
        "visibilityConfig": {
          "sampledRequestsEnabled": true,
          "cloudWatchMetricsEnabled": true,
          "metricName": "foo"
```

```
        }
      }
    ],
    "visibilityConfig": {
      "sampledRequestsEnabled": true,
      "cloudWatchMetricsEnabled": true,
      "metricName": "foo"
    }
  },
  "responseElements": {
    "summary": {
      "name": "foo",
      "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
      "description": "foo",
      "lockToken": "67551e73-49d8-4363-be48-244deea72ea9",
      "aRN": "arn:aws:wafv2:us-east-1:112233445566:global/webacl/foo/
ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b"
    }
  },
  "requestID": "c51521ba-3911-45ca-ba77-43aba50471ca",
  "eventID": "afd1a60a-7d84-417f-bc9c-7116cf029065",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

例: GetWebACL の CloudTrail ログエントリ

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AssumedRole",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin/admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AssumedRole",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
```

```
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:18:28Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "GetWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "webacl"
  },
  "responseElements": null,
  "requestID": "f2db4884-4eeb-490c-afe7-67cbb494ce3b",
  "eventID": "7d563cd6-4123-4082-8880-c2d1fda4d90b",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

例: UpdateWebACL の CloudTrail ログエントリ

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
```

```
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:20:56Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "UpdateWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "defaultAction": {
      "block": {}
    },
    "description": "foo",
    "rules": [
      {
        "name": "foo",
        "priority": 1,
        "statement": {
          "geoMatchStatement": {
            "countryCodes": [
              "AF"
            ]
          }
        },
        "action": {
          "block": {}
        },
        "visibilityConfig": {
          "sampledRequestsEnabled": true,
          "cloudWatchMetricsEnabled": true,
          "metricName": "foo"
```

```
        }
      }
    ],
    "visibilityConfig": {
      "sampledRequestsEnabled": true,
      "cloudWatchMetricsEnabled": true,
      "metricName": "foo"
    },
    "lockToken": "67551e73-49d8-4363-be48-244deea72ea9"
  },
  "responseElements": {
    "nextLockToken": "a6b54c01-7975-4e6d-b7d0-2653cb6e231d"
  },
  "requestID": "41c96e12-9790-46ab-b145-a230f358f2c2",
  "eventID": "517a10e6-4ca9-4828-af90-a5cff9756594",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

例: DeleteWebACL の CloudTrail ログエントリ

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin/session-name",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
```

```
    }
  },
  "eventTime": "2019-11-06T19:25:17Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "DeleteWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "lockToken": "a6b54c01-7975-4e6d-b7d0-2653cb6e231d"
  },
  "responseElements": null,
  "requestID": "71703f89-e139-440c-96d4-9c77f4cd7565",
  "eventID": "2f976624-b6a5-4a09-a8d0-aa3e9f4e5187",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

例: AWS WAF 従来のログファイルエントリ

AWS WAF Classic は の以前のバージョンです AWS WAF。詳細については、「AWS WAF クラシック」を参照してください。

ログエントリは、CreateRule、GetRule、UpdateRule、および DeleteRule の各オペレーションを示しています。

```
{
  "Records": [
   {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
```

```
      "eventTime": "2016-04-25T21:35:14Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "CreateRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "name": "0923ab32-7229-49f0-a0e3-66c81example",
        "changeToken": "l9434322-8685-4ed2-9c5b-9410bexample",
        "metricName": "0923ab32722949f0a0e366c81example"
      },
      "responseElements": {
        "rule": {
          "metricName": "0923ab32722949f0a0e366c81example",
          "ruleId": "12132e64-6750-4725-b714-e7544example",
          "predicates": [

          ],
          "name": "0923ab32-7229-49f0-a0e3-66c81example"
        },
        "changeToken": "l9434322-8685-4ed2-9c5b-9410bexample"
      },
      "requestID": "4e6b66f9-d548-11e3-a8a9-73e33example",
      "eventID": "923f4321-d378-4619-9b72-4605bexample",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:22Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "GetRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
```

```
      "requestParameters": {
        "ruleId": "723c2943-82dc-4bc1-a29b-c7d73example"
      },
      "responseElements": null,
      "requestID": "8e4f3211-d548-11e3-a8a9-73e33example",
      "eventID": "an236542-d1f9-4639-bb3d-8d2bbexample",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:13Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "UpdateRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "ruleId": "7237b123-7903-4d9e-8176-9d71dexample",
        "changeToken": "32343a11-35e2-4dab-81d8-6d408example",
        "updates": [
          {
            "predicate": {
              "type": "SizeConstraint",
              "dataId": "9239c032-bbbe-4b80-909b-782c0example",
              "negated": false
            },
            "action": "INSERT"
          }
        ]
      },
      "responseElements": {
        "changeToken": "32343a11-35e2-4dab-81d8-6d408example"
      },
      "requestID": "11918283-0b2d-11e6-9ccc-f9921example",
```

```
      "eventID": "00032abc-5bce-4237-a8ee-5f1a9example",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:28Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "DeleteRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "changeToken": "fd232003-62de-4ea3-853d-52932example",
        "ruleId": "3e3e2d11-fd8b-4333-8b03-1da95example"
      },
      "responseElements": {
        "changeToken": "fd232003-62de-4ea3-853d-52932example"
      },
      "requestID": "b23458a1-0b2d-11e6-9ccc-f9928example",
      "eventID": "a3236565-1a1a-4475-978e-81c12example",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    }
  ]
}
```


AWS Shield Advanced CloudTrail の情報

AWS Shield Advanced は、CloudTrail ログファイルのイベントとして次のアクションのログ記録をサポートします。

- ListAttacks

- DescribeAttack
- CreateProtection
- DescribeProtection
- DeleteProtection
- ListProtections
- CreateSubscription
- DescribeSubscription
- GetSubscriptionState

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストが、ルートユーザーの認証情報で行われたかどうか
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、「CloudTrail userIdentity 要素」を参照してください。

例: Shield Advanced ログファイルエントリ

追跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントはあらゆるソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメータなどの情報が含まれます。CloudTrail ログファイルは、公開 API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

`DeleteProtection` と `ListProtections` のアクションを示す CloudTrail ログ入力の例を次に示します。

```
[
 {
   "eventVersion": "1.05",
   "userIdentity": {
     "type": "IAMUser",
```

```
      "principalId": "123456789098765432123l",
      "arn": "arn:aws:iam::123456789012:user/SampleUser",
      "accountId": "123456789012",
      "accessKeyId": "1AFGDT647FHU83JHFI81H",
      "userName": "SampleUser"
    },
    "eventTime": "2018-01-10T21:31:14Z",
    "eventSource": "shield.amazonaws.com",
    "eventName": "DeleteProtection",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "aws-cli/1.14.10 Python/3.6.4 Darwin/16.7.0 botocore/1.8.14",
    "requestParameters": {
      "protectionId": "12345678-5104-46eb-bd03-agh4j8rh3b6n"
    },
    "responseElements": null,
    "requestID": "95bc0042-f64d-11e7-abd1-1babdc7aa857",
    "eventID": "85263bf4-17h4-43bb-b405-fh84jhd8urhg",
    "eventType": "AwsApiCall",
    "apiVersion": "AWSShield_20160616",
    "recipientAccountId": "123456789012"
  },
  {
    "eventVersion": "1.05",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "123456789098765432123",
      "arn": "arn:aws:iam::123456789012:user/SampleUser",
      "accountId": "123456789012",
      "accessKeyId": "1AFGDT647FHU83JHFI81H",
      "userName": "SampleUser"
    },
    "eventTime": "2018-01-10T21:30:03Z",
    "eventSource": "shield.amazonaws.com",
    "eventName": "ListProtections",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "aws-cli/1.14.10 Python/3.6.4 Darwin/16.7.0 botocore/1.8.14",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "6accca40-f64d-11e7-abd1-1bjfi8urhj47",
    "eventID": "ac0570bd-8dbc-41ac-a2c2-987j90j3h78f",
    "eventType": "AwsApiCall",
    "apiVersion": "AWSShield_20160616",
```

```
    "recipientAccountId": "123456789012"
  }
]
```

AWS Firewall Manager CloudTrail の情報

AWS Firewall Manager は、CloudTrail ログファイルのイベントとして次のアクションのログ記録をサポートします。

- AssociateAdminAccount
- DeleteNotificationChannel
- DeletePolicy
- DisassociateAdminAccount
- PutNotificationChannel
- PutPolicy
- GetAdminAccount
- GetComplianceDetail
- GetNotificationChannel
- GetPolicy
- ListComplianceStatus
- ListPolicies

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストが、ルートユーザーの認証情報で行われたかどうか
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、「CloudTrail userIdentity 要素」を参照してください。

例: Firewall Manager のログファイルエントリ

追跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントはあらゆるソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメータなどの情報が含まれます。CloudTrail ログファイルは、公開 API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

`GetAdminAccount-->` アクションを示す CloudTrail ログエントリの例を次に示します。

```
 {
                "eventVersion": "1.05",
                "userIdentity": {
                                "type": "AssumedRole",
                                "principalId": "123456789098765432123",
                                "arn": "arn:aws:sts::123456789012:assumed-role/Admin/
SampleUser",
                                "accountId": "123456789012",
                                "accessKeyId": "1AFGDT647FHU83JHFI81H",
                                "sessionContext": {
                                                "attributes": {
                                                                "mfaAuthenticated":
 "false",
                                                                "creationDate":
 "2018-04-14T02:51:50Z"
                                                               },
                                                "sessionIssuer": {
                                                                "type": "Role",
                                                                "principalId":
 "123456789098765432123",
                                                                "arn":
 "arn:aws:iam::123456789012:role/Admin",
                                                                "accountId":
 "123456789012",
                                                                "userName": "Admin"
                                                                 }
                                                  }
                                },
                "eventTime": "2018-04-14T03:12:35Z",
                "eventSource": "fms.amazonaws.com",
                "eventName": "GetAdminAccount",
                "awsRegion": "us-east-1",
```

```
            "sourceIPAddress": "72.21.198.65",
            "userAgent": "console.amazonaws.com",
            "requestParameters": null,
            "responseElements": null,
            "requestID": "ae244f41-3f91-11e8-787b-dfaafef95fc1",
            "eventID": "5769af1e-14b1-4bd1-ba75-f023981d0a4a",
            "eventType": "AwsApiCall",
            "apiVersion": "2018-01-01",
            "recipientAccountId": "123456789012"
    }
```

AWS WAF および AWS Shield Advanced API の使用

このセクションでは、 AWS WAF でマッチセット、ルール、保護パック (ウェブ ACLs) を作成および管理するためのリクエストを および Shield Advanced API に行う方法 AWS WAF と、Shield Advanced のサブスクリプションと保護を行う方法について説明します。さらに、リクエストの構成要素、レスポンスの内容、リクエストの認証方法について説明します。

トピック

- AWS SDKsの使用
- AWS WAF または Shield Advanced への HTTPS リクエストの実行
- HTTP レスポンス
- リクエストの認証

AWS SDKsの使用

に SDK AWS を提供する言語を使用する場合は、 APIs を使用して作業するのではなく、SDK を使用します。SDKs、認証が簡単になり、開発環境と簡単に統合され、 AWS WAF および Shield Advanced コマンドに簡単にアクセスできます。 AWS SDKs「」を参照してくださいアカウントを設定してサービスを使用する。 ツールをダウンロード

AWS WAF または Shield Advanced への HTTPS リクエストの実行

AWS WAF および Shield Advanced リクエストは、RFC 2616 で定義されている HTTPS リクエストです。HTTP リクエストと同様に、 AWS WAF または Shield Advanced へのリクエストには、リクエストメソッド、URI、リクエストヘッダー、リクエスト本文が含まれます。レスポンスには HTTP ステータスコードとレスポンスヘッダーが含まれており、レスポンス本文が含まれている場合もあります。

リクエストの URI

リクエスト URI は常に 1 つのスラッシュ / です。

HTTP ヘッダー

AWS WAF および Shield Advanced では、HTTP リクエストの ヘッダーに次の情報が必要です。

Host (必須)

リソースが作成される場所を指定するエンドポイント。エンドポイントの詳細については、「AWS サービスエンドポイント」を参照してください。例えば、CloudFront ディストリビューションHostの AWS WAF ヘッダーの値は ですwaf.amazonaws.com:443。

x-amz-date または Date (必須)

Authorization ヘッダーに含める署名を作成するときに使用できる日付。ISO 8601 の標準形式に基づいて UTC 時間で日付を指定します (次の例を参照)。

```
x-amz-date: 20151007T174952Z
```

x-amz-date または Date のどちらかを含める必要があります。(一部の HTTP クライアントライブラリでは、Date ヘッダーを設定することができません)。x-amz-date ヘッダーが存在する場合、 はリクエストを認証するときにDateヘッダー AWS WAF を無視します。

タイムスタンプは、リクエストが受信された AWS システム時刻から 15 分以内にする必要があります。このようにしないと、リクエストは RequestExpired エラーコードで失敗し、任意のユーザーがリクエストを再現できなくなります。

Authorization (必須)

リクエスト認証に必要な情報。このヘッダーの作成方法の詳細については、「リクエストの認証」を参照してください。

X-Amz-Target (必須)

AWSWAF_ または AWSShield_、API バージョン (ピリオドなし)、ピリオド (.)、オペレーション名を連結したもの。例えば、以下のようになります。

AWSWAF_20150824.CreateWebACL

Content-Type (条件付き)

コンテンツタイプとして JSON をそのバージョンと共に指定します。例えば、次のようになります。

```
Content-Type: application/x-amz-json-1.1
```

条件: POST リクエストに必要です。

Content-Length (条件付き)

RFC 2616 に基づくメッセージの長さ (ヘッダーなし)。

条件: リクエストボディ自体に情報が含まれる場合、必須です (このヘッダーは、ほとんどのツールキットで自動的に追加されます)。

次に示しているのは、 AWS WAFで保護パック (ウェブ ACL) を作成するための HTTP リクエストのヘッダーの例です。

```
POST / HTTP/1.1
Host: waf.amazonaws.com:443
X-Amz-Date: 20151007T174952Z
Authorization: AWS4-HMAC-SHA256
               Credential=AccessKeyID/20151007/us-east-2/waf/aws4_request,
               SignedHeaders=host;x-amz-date;x-amz-target,

 Signature=145b1567ab3c50d929412f28f52c45dbf1e63ec5c66023d232a539a4afd11fd9
X-Amz-Target: AWSWAF_20150824.CreateWebACL
Accept: */*
Content-Type: application/x-amz-json-1.1; charset=UTF-8
Content-Length: 231
Connection: Keep-Alive
```

HTTP リクエストボディ

多くの AWS WAF および Shield Advanced API アクションでは、リクエストの本文に JSON 形式のデータを含める必要があります。

次に示しているリクエストの例では、シンプルな JSON ステートメントを使用して、IP アドレス 192.0.2.44 (CIDR 表記では 192.0.2.44/32) を含めるように、`IPSet` を更新しています。

```
POST / HTTP/1.1
Host: waf.amazonaws.com:443
X-Amz-Date: 20151007T174952Z
Authorization: AWS4-HMAC-SHA256
               Credential=AccessKeyID/20151007/us-east-2/waf/aws4_request,
               SignedHeaders=host;x-amz-date;x-amz-target,

 Signature=145b1567ab3c50d929412f28f52c45dbf1e63ec5c66023d232a539a4afd11fd9
X-Amz-Target: AWSWAF_20150824.UpdateIPSet
Accept: */*
Content-Type: application/x-amz-json-1.1; charset=UTF-8
Content-Length: 283
Connection: Keep-Alive
```

```
{
   "ChangeToken": "d4c4f53b-9c7e-47ce-9140-0ee5ffffffff",
   "IPSetId": "69d4d072-170c-463d-ab82-0643ffffffff",
   "Updates": [
      {
         "Action": "INSERT",
         "IPSetDescriptor": {
            "Type": "IPV4",
            "Value": "192.0.2.44/32"
         }
      }
   ]
}
```

HTTP レスポンス

すべての AWS WAF および Shield Advanced API アクションには、レスポンスに JSON 形式のデータが含まれます。

HTTP レスポンスの重要なヘッダーと、それらをアプリケーション内で扱う方法 (該当する場合) を示します。

HTTP/1.1

このヘッダーにはステータスコードが続きます。ステータスコード 200 はオペレーションの成功を示します。

型: 文字列

x-amzn-RequestId

リクエストを一意に識別する AWS WAF または Shield Advanced によって作成された値。例: K2QH8DN0U907N97FNA2GDLL8OBVV4KQNS05AEMVJF66Q9ASUAAJG。で問題が発生した場合は AWS WAF、この値を使用して問題のトラブルシューティング AWS を行うことができます。

タイプ: 文字列

Content-Length

レスポンス本文の長さ (バイト単位)。

型: 文字列

日付

AWS WAF または Shield Advanced が応答した日時。例: Wed, 07 Oct 2015 12:00:00 GMT。

タイプ: 文字列

エラーレスポンス

リクエストの結果がエラーの場合、HTTP レスポンスには次の値が含まれます。

- レスポンス本文としての JSON エラードキュメント
- Content-Type
- 該当する HTTP ステータスコード (3xx、4xx、または 5xx)

次に示しているのは、JSON エラードキュメントの例です。

```
HTTP/1.1 400 Bad Request
x-amzn-RequestId: b0e91dc8-3807-11e2-83c6-5912bf8ad066
x-amzn-ErrorType: ValidationException
Content-Type: application/json
Content-Length: 125
Date: Mon, 26 Nov 2012 20:27:25 GMT

{"message":"1 validation error detected: Value null at 'TargetString' failed to satisfy
 constraint: Member must not be null"}
```

リクエストの認証

SDK AWS を提供する言語を使用する場合は、SDK を使用することをお勧めします。すべての AWS SDKs は、 AWS WAF または Shield Advanced API を使用する場合と比較して、リクエストの署名プロセスを大幅に簡素化し、時間を大幅に節約します。また、SDK は開発環境と容易に統合されるため、関連するコマンドへのアクセスが簡単です。

AWS WAF および Shield Advanced では、リクエストに署名して送信するすべてのリクエストを認証する必要があります。リクエストに署名するには、暗号化ハッシュ関数を使用してデジタル署名を計算します。この関数は入力に基づいてハッシュ値を返します。入力には、リクエストのテキスト、およびシークレットアクセスキーが含まれます。ハッシュ関数から返されるハッシュ値をリクエストに署名として含めます。署名は、リクエストの Authorization ヘッダーの一部です。

リクエストを受け取ると、 AWS WAF Shield Advanced はリクエストの署名に使用したのと同じハッシュ関数と入力を使用して署名を再計算します。結果の署名がリクエストの署名と一致する場合、 AWS WAF または Shield Advanced がリクエストを処理します。一致しない場合、リクエストは拒否されます。

AWS WAF および Shield Advanced は、AWS 署名バージョン 4 を使用した認証をサポートしています。署名の計算プロセスは 3 つのタスクに分けることができます。

タスク 1: 正規リクエストを作成する

『https://docs.aws.amazon.com/general/latest/gr/sigv4-create-canonical-request.html』の「Amazon Web Services 全般のリファレンスタスク 1: 署名バージョン 4 の正規リクエストを作成する」で説明されているように、正規形式で HTTP リクエストを作成します。

タスク 2: 署名対象の文字列を作成する

暗号化ハッシュ関数への入力値の 1 つとして使用する文字列を作成します。署名対象の文字列と呼ばれる文字列は、次の値を連結したものです。

- ハッシュアルゴリズムの名前
- リクエスト日
- 認証情報スコープ文字列
- 前のタスクからの正規形式のリクエスト

認証情報スコープの文字列自体は、日付、リージョン、およびサービス情報を結合したものです。

`X-Amz-Credential` パラメータでは、次の内容を指定します。

- リクエストの送信先であるエンドポイントのコード (`us-east-2`)
- サービスの省略形としての `waf`

例:

```
X-Amz-Credential=AKIAIOSFODNN7EXAMPLE/20130501/us-east-2/waf/
aws4_request
```

タスク 3: 署名を作成する

2 つの入力文字列を受け取る暗号化ハッシュ関数を使用して、リクエストの署名を作成します。

- タスク 2 からの署名対象の文字列。

- 派生キー。シークレットアクセスキーから開始し、認証情報スコープの文字列を使用して一連のハッシュベースのメッセージ認証コード (HMAC) を作成することで、派生キーが計算されます。

関連情報

このサービスを利用する際に役立つ関連リソースは次のとおりです。

AWS WAF、、および では AWS Shield Advanced、次のリソースを使用できます AWS Firewall Manager。

- 実装のガイドライン — AWS WAF既存および新規のウェブアプリケーションを保護するため AWS WAF の実装に関する最新の推奨事項を含む技術刊行物。
- AWS ディスカッションフォーラム – このサービスやその他の AWS サービスに関連する技術的な質問について話し合うためのコミュニティベースのフォーラム。
- AWS WAF ディスカッションフォーラム – 開発者が関連する技術的な質問について話し合うためのコミュニティベースのフォーラム AWS WAF。
- Shield Advanced ディスカッションフォーラム – デベロッパーが Shield Advanced に関連する技術的な質問について話し合うためのコミュニティベースのフォーラム。
- AWS WAF 製品情報 – 機能 AWS WAF、料金など、 に関する情報のプライマリウェブページ。
- Shield Advanced の製品情報 – 機能、料金など、Shield Advanced に関する情報の主要なウェブページ。

次のリソースは Amazon Web Services で利用可能です。

- クラスとワークショップ – AWS スキルを磨き、実践的な経験を積むために、セルフペースラボに加えて、ロールベースおよび専門コースへのリンク。
- AWS デベロッパーセンター – チュートリアルを詳しく調べ、ツールをダウンロードし、デ AWS ベロッパーイベントについて学習します。
- AWS デベロッパーツール – AWS アプリケーションを開発および管理するためのデベロッパーツール、SDKs、IDE ツールキット、コマンドラインツールへのリンク。
- 入門リソースセンター – をセットアップし AWS アカウント、 AWS コミュニティに参加して、最初のアプリケーションを起動する方法について説明します。
- ハンズオンチュートリアル - ステップ バイ ステップのチュートリアルに従って、最初のアプリケーションを AWSで起動します。
- AWS ホワイトペーパー – ソリューションアーキテクトや他の技術専門家によって AWS 作成されたアーキテクチャ、セキュリティ、経済学などのトピックを網羅した、技術 AWS ホワイトペーパーの包括的なリストへのリンク。

- AWS サポート センター – AWS サポート ケースを作成および管理するためのハブ。フォーラム、技術的なFAQs、サービスのヘルスステータスなど、その他の役立つリソースへのリンクも含まれています AWS Trusted Advisor。
- サポート – クラウドでのアプリケーションの構築と実行に役立つ サポート one-on-one の高速応答サポートチャネルである に関する情報のプライマリウェブページ。
- お問い合わせ – AWS の請求、アカウント、イベント、不正使用、その他の問題などに関するお問い合わせの受付窓口です。
- AWS サイト規約 – 当社の著作権と商標、お客様のアカウント、ライセンス、サイトアクセス、およびその他のトピックに関する詳細情報。

ドキュメント履歴

このページでは、このドキュメントの大きな変更点をまとめています。

サービス機能は、サービスが利用可能な AWS リージョンに段階的にロールアウトされることがあります。このドキュメントは、最初のリリースのためにのみ更新されています。リージョンの可用性に関する情報を提供したり、その後のリージョンのロールアウトを発表したりすることはありません。サービス機能のリージョンの可用性と更新に関する通知のサブスクライブについては、「 の最新情報 AWS」を参照してください。

変更	説明	日付
の AWS マネージドルールを更新しました AWS WAF	SQL データベースマネージドルールグループの静的バージョン 2.4 をリリースしました。	2026 年 8 月 12 日
AWS WAF テキスト変換の事前解析	が個々のクエリ引数に解析する前に raw AWS WAF クエリ文字列を正規化する事前解析テキスト変換を追加しました。	2026 年 7 月 29 日
AWS WAF 新しいテキスト変換と事前解析テキスト変換	10 個の新しいテキスト変換と、解析前に未加工のクエリ文字列を正規化する新しい事前解析テキスト変換機能を追加しました。	2026 年 7 月 29 日
の AWS マネージドルールを更新しました AWS WAF	Bot Control ルールグループの静的バージョン 6.1 をリリースし、追加のボットカテゴリにわたってボット検出を拡張しました。	2026 年 7 月 24 日
の AWS マネージドルールを更新しました AWS WAF	コアルールセット (CRS) マネージドルールグループの静	2026 年 7 月 20 日

	的バージョン 1.22 をリリースしました。	
の AWS マネージドルールを更新しました AWS WAF	既知の不正な入力マネージドルールグループの静的バージョン 1.26 をリリースしました。	2026 年 7 月 15 日
AI トラフィック収益化	AI トラフィック収益化の仕組み、AI トラフィック収益化の開始方法、料金設定、支払いネットワークと決済、収益分析、AI エージェントへのライセンス条項の伝達など、AI トラフィック収益化に関するドキュメントを追加しました。データ保護と口グ記録の軽微な更新。	2026 年 6 月 15 日
の AWS マネージドルールを更新しました AWS WAF	Windows オペレーティングシステムマネージドルールグループの静的バージョン 2.5 をリリースしました。	2026 年 6 月 1 日
Application Load Balancer の HTTP/2 本文検査コントロール	が HTTP/2 ターゲットにルーティングするときに Application Load Balancer で HTTP/2 リクエストボディを AWS WAF 検査する方法を設定できるようになりました。	2026 年 6 月 1 日

の AWS マネージドルールを更新しました AWS WAF	Web Bot Auth をサポートする Bot Control ルールグループの静的バージョン 6.0 を商用パーティションのリージョン AWS WAF 統合にリリースし、追加のボットカテゴリにわたってボット検出を拡張しました。	2026 年 5 月 22 日
ウェブ ACL あたりのリソースの関連付け	Amazon API Gateway REST API、Amazon Cognito ユーザープール、 AWS AppSync GraphQL API、 AWS App Runner service、 AWS Verified Access インスタンス、およびウェブ ACL あたりの AWS Amplify 関連付けの新しいクォータを追加します。ウェブ ACL あたりのデフォルトのクォータは、それぞれ 100 です。	2026 年 5 月 1 日
の AWS マネージドルールを更新しました AWS WAF	SQL データベースマネージドルールグループの静的バージョン 2.3 をリリースしました。	2026 年 4 月 29 日
の AWS マネージドルールを更新しました AWS WAF	Windows オペレーティングシステムマネージドルールグループの静的バージョン 2.4 をリリースしました。	2026 年 4 月 28 日

AWS WAF Application Load Balancer と AppSync の API アクセス許可の更新	IAM ベストプラクティスに沿ってガイドを更新しました。詳細については、「IAM でのセキュリティのベストプラクティス」を参照してください。	2026 年 4 月 8 日
の AWS マネージドルールを更新しました AWS WAF	コアルールセット (CRS) マネージドルールグループの静的バージョン 1.21 をリリースしました。	2026 年 4 月 6 日
動的ラベル補間	`${namespace:}` 構文を使用して、カスタムリクエストヘッダー、カスタムレスポンスヘッダー、カスタムレスポンス本文のラベル値を動的に解決できるようになりました。	2026 年 4 月 1 日
の AWS マネージドルールを更新しました AWS WAF	PHP アプリケーションルールグループの静的バージョン 2.2 をリリースしました。	2026 年 3 月 24 日
の AWS マネージドルールを更新しました AWS WAF	ボット検出機能を拡張した Bot Control ルールグループの静的バージョン 5.0 をリリースしました。	2026 年 2 月 25 日
AWS WAF コンソールに新しい AI トラフィック分析ダッシュボードがある	AWS WAF コンソールのウェブ ACL ページには、新しい AI トラフィック分析ダッシュボードがあります。	2026 年 2 月 25 日

AWS Shield ネットワークセキュリティディレクターのネットワークトポロジウィジェットドキュメントを更新	AWS Shield ネットワークセキュリティディレクターのネットワークトポロジウィジェットのドキュメントを更新し、その生成方法と表示方法を反映しました。	2026 年 2 月 9 日
の AWS マネージドルールを更新しました AWS WAF	POSIX オペレーティングシステムルールグループの 3.2 の静的バージョンをリリースしました。	2026 年 1 月 15 日
AWS Shield ネットワークセキュリティディレクターのパブリックプレビューを更新しました	AWS Shield ネットワークセキュリティディレクターのパブリックプレビューを更新し、マルチアカウント機能と AWS Organizations との統合を追加しました。	2025 年 12 月 12 日
の AWS マネージドルールを更新しました AWS WAF	既知の不正な入力ルールグループの静的バージョン 1.25 をリリースしました。	2025 年 12 月 8 日
の AWS マネージドルールを更新しました AWS WAF	POSIX オペレーティングシステムルールグループの 3.1 の静的バージョンをリリースしました。	2025 年 12 月 8 日
の AWS マネージドルールを更新しました AWS WAF	既知の不正な入力ルールグループの静的バージョン 1.24 をリリースしました。	2025 年 12 月 4 日
の AWS マネージドルールを更新しました AWS WAF	広告、AI、コンテンツフェッチャー、ソーシャルメディアなどの複数のカテゴリにまたがるボット検出の拡張をサポートする Bot Control ルールグループを更新しました。	2025 年 11 月 20 日

AWS WAF マネージドポリシーの変更	Amazon CloudFront Flat rate 料金設定のアクセス許可を AWSWAFConsoleFullAccess 、 AWSWAFConsoleReadOnlyAccess 管理ポリシーに追加しました。	2025 年 11 月 18 日
AWS WAF CloudFront の定額料金プランとの統合	に関連付けられた CloudFront ディストリビューションを定額料金プラン AWS WAF にサブスクライブできるようになりました。この新しい料金プランは、従pay-as-you-goとは異なり、料金プランには使用量とリソースの事前設定されたサービスクォータがあります。料金プランのディストリビューションをサブスクライブすると、そのディストリビューションの予期しない使用料金は発生しません。料金プランに含まれるすべてのリソースと機能に対して 1 つの料金が適用されます。	2025 年 11 月 18 日
の AWS マネージドルールを更新しました AWS WAF	Bot Control ルールグループに AI エージェントのウェブボット認証のサポートが追加されました。	2025 年 11 月 17 日

AWS WAF マネージドポリシーの変更	Amazon API Gateway のアクセス許可を、AWSWAFConsoleFullAccess および AWSWAFConsoleReadOnlyAccess マネージドポリシーに更新しました。Amazon CloudWatch、 AWS AppSync、Amazon Data Firehose AWS の料金表、および AWS Marketplace を AWSWAFConsoleFullAccess および AWSWAFConsoleReadOnlyAccess 管理ポリシーに追加しました。	2025 年 11 月 3 日
ウェブ ACL あたりの ALB 関連付け	ウェブ ACL ごとに ALB 関連付けの新しいクォータを追加します。ウェブ ACL あたりのデフォルトのクォータは 100 です。	2025 年 10 月 22 日
の AWS マネージドルールを更新しました AWS WAF	コアルールセットまたは共通ルールセット (CRS) を更新しました。	2025 年 10 月 2 日
AWS WAF Bot Control のしきい値を更新しました	TGT_TokenReuseIpLow および TGT_TokenReuseIpMedium のしきい値を更新しました。	2025 年 8 月 29 日
ルールごとに地域一致国のクォータを追加する	ルールの地域一致国の最大数は 50 です。	2025 年 8 月 29 日
の AWS マネージドルールを更新しました AWS WAF	コアルールセットまたは共通ルールセット (CRS) を更新しました。	2025 年 8 月 14 日

の AWS マネージドルールを更新しました AWS WAF	コアルールセットまたは共通ルールセット (CRS) を更新しました。	2025 年 6 月 18 日
ネットワークセキュリティディレクターの最初のプレビューリリース	AWS Shield Network Security Director がプレビューで利用可能になりました。これにより、 AWS セキュリティ設定に関するインサイトが得られます。	2025 年 6 月 17 日
AWS Shield ネットワークセキュリティディレクターにアイデンティティベースのカスタマー管理ポリシーを追加	独自のアイデンティティベースのポリシーを作成および管理して、 AWS Shield ネットワークセキュリティディレクターに AWS リソースへの適切なアクセスを許可できます。	2025 年 6 月 17 日
AWS WAF に新しいコンソールユーザーエクスペリエンスが追加されました	AWS WAF コンソールのオンボーディングワークフローが簡素化され、保護パック (ウェブ ACLs) を使用してウェブ ACLs。	2025 年 6 月 17 日
AWS WAF メトリクスとディメンションの更新	2 つの新しい分散型サービス拒否 (DDoS) 防止メトリクスが、`LowReputationRequestsDenied` および `LowReputationPacketsDropped` という `AWS/ApplicationELB` 名前空間に公開されるようになりました。	2025 年 6 月 11 日

の新しい DDoS 対策マネージドルールグループ AWS WAF	AWSManagedRulesAntiDDoSRuleSet は、DDoS 攻撃に関与している疑いのあるリクエストを検出、ラベル付け、チャレンジすることで、 リソースを保護します。	2025 年 6 月 11 日
AWS WAF でリソースレベルの DDoS 保護を追加	DDoS 対策機能を使用して、Application Load Balancer での DDoS 攻撃を検出および防止できるようになりました。	2025 年 6 月 11 日
AWS WAF ASN 一致ステートメントを追加する	発信元 IP アドレスの AS 番号 (ASN) に基づいてウェブリクエストを照合できるようになりました。	2025 年 6 月 5 日
AWS WAF カスタムキー集約オプションとして ASN を追加する	カスタムキー集約を使用して、特定の AS 番号 (ASN) からのリクエストを制限できるようになりました。	2025 年 6 月 5 日
の AWS マネージドルールを更新しました AWS WAF	AWS WAF Bot Control ルールセットを更新しました。	2025 年 5 月 29 日
AWS Firewall Manager セキュリティポリシーの更新	Amazon CloudFront に必要なアクセス許可を追加するために FMSServiceRolePolicy を更新。	2025 年 5 月 21 日

サイレントの AWS WAF メトリクスとディメンションを更新しました Challenge	AWS AWS WAF メトリクスとディメンションセクションChallengesSolvedSdk に ChallengesAttempted ChallengesSolved 、ChallengesAttemptedSdk 、、 を追加しました。	2025 年 5 月 16 日
AWS WAF マネージドポリシーの変更	AWSWAFFullAccess 、、AWSWAFReadOnlyAccess 、AWSWAFConsoleReadOnlyAccess 管理ポリシーに対する AWS Amplify アクセス許可とAWSWAFConsoleFullAccess 、AWSWAFConsoleFullAccess AWSWAFConsoleReadOnlyAccess 管理ポリシーに対する Amazon CloudFront アクセス許可を追加しました。	2025 年 5 月 5 日
AWS WAF が新しい CloudFront ディストリビューションのサポートを追加	AWS WAF ウェブ ACLs CloudFront マルチテナントディストリビューションとディストリビューションテナントに関連付けることができるようになりました。	2025 年 4 月 28 日
ログ一致の詳細の URI フラグメント	ログのルール一致の詳細に、ウェブリクエストからの URI フラグメントが含まれるようになりました。ログからこのフィールドを編集するようにログを設定できます。	2025 年 3 月 17 日

新しい AWS WAF リクエストコンポーネント	これで、URI fragment を検査できるようになりました。	2025 年 3 月 17 日
にクライアント側の保護を追加 AWS WAF	からのクライアント側の保護 AWS Marketplace が利用可能になりました。 AWS Marketplace コンソールを使用して、クライアント側の保護をサブスクライブおよびサブスクライブ解除できます。	2025 年 3 月 10 日
AWS WAF が新しい JA4 フィールドマッチングをサポート	高度な JavaScript フィンガープリント (JA4) の特性に基づいてトラフィックを検出してブロックし、WAF レートベースのルール内のサポートされているリクエストキーの 1 つとして JA4 フィンガープリントを使用できます。	2025 年 3 月 4 日
の AWS マネージドルールを更新しました AWS WAF	コアルールセットまたは共通ルールセット (CRS) を更新しました。	2025 年 3 月 3 日
AWS WAF メトリクスとディメンションの更新	使用状況メトリクスに関する情報を AWS WAF メトリクスとディメンションセクションに追加しました。	2025 年 2 月 21 日
AWS WAF でデータ保護オプションを追加	AWS WAF では、保護パック (ウェブ ACL) レベルまたはログ記録のみレベルでデータ保護を設定できるようになりました。	2025 年 2 月 14 日

AWS Firewall Manager セキュリティポリシーの更新	FMSServiceRolePolicy を更新して、リソース設定ステータスをバッチで取得するためのアクセス許可を追加。	2025 年 2 月 10 日
AWS Firewall Manager のクォータの更新	Firewall Manager のクォータセクションを更新して、新しい AWS WAF および Network Firewall ポリシーを反映しました。	2025 年 2 月 10 日
の AWS マネージドルールを更新しました AWS WAF	SQLi データベースルールグループを更新しました。	2025 年 1 月 24 日
の AWS マネージドルールを更新しました AWS WAF	Linux オペレーティングシステムのルールグループを更新しました。	2025 年 1 月 24 日
の AWS マネージドルールを更新しました AWS WAF	SQLi データベースルールグループを更新しました。	2025 年 1 月 24 日
AWS Firewall Manager リソースタグの更新	Firewall Manager では、論理 AND 演算子または論理 OR 演算子を使って複数のリソースタグを組み合わせることができるようになりました。リソースタグで新しいワイルドカード演算子を使用して、任意のキーまたは値に一致させることもできます。	2025 年 1 月 9 日
AWS WAF ウェブ ACL ダッシュボードがトップのセキュリティインサイトを追加	AWS WAF コンソールウェブ ACL トラフィック概要ダッシュボードには、新しいトップインサイトタブがあります。	2025 年 1 月 2 日

JA3 および JA4 フィンガープリントでのレートベースのルール集約	レートベースのルールのカスタム集約キーに JA3 フィンガープリントと JA4 フィンガープリントを指定できるようになりました。	2024 年 12 月 20 日
AWS WAF に JA4 フィンガープリントの検査が追加されました	Amazon CloudFront ディストリビューションと Application Load Balancer に対して、ウェブリクエストの JA4 フィンガープリントと完全に一致できるようになりました。	2024 年 12 月 20 日
AWS WAF モバイル SDK 仕様の更新	`loadTokenIntoProvider` 操作を `WAFTokenProvider` に追加しました。	2024 年 11 月 19 日
アプリケーション統合 SDK が TV アプリを追加	Android と iOS の統合 SDK は、TV アプリやモバイルアプリに使用できます。	2024 年 11 月 19 日
AWS WAF トークンのラベル付けでブラウザのフィンガープリントを追加	トークン管理がブラウザフィンガープリントのラベルを追加しました。	2024 年 11 月 13 日
の AWS マネージドルールを更新しました AWS WAF	Bot Control ルールグループを更新しました。	2024 年 11 月 7 日
Firewall Manager AWS WAF ポリシーは既存のウェブ ACLs を使用できます	Firewall Manager AWS WAF ポリシーは、既存のアカウント所有ACLs を改良し、必要な場合にのみ新しいウェブ ACLs を作成できるようになりました。	2024 年 10 月 22 日
の AWS マネージドルールを更新しました AWS WAF	コアルールセット (CRS) ルールグループを更新しました。	2024 年 10 月 16 日

の AWS マネージドルールを更新しました AWS WAF	Bot Control、ATP および ACFP マネージドルールグループを更新しました。	2024 年 9 月 13 日
の AWS マネージドルールを更新しました AWS WAF	Linux オペレーティングシステムのルールグループを更新しました。	2024 年 9 月 2 日
の AWS マネージドルールを更新しました AWS WAF	コアルールセット (CRS) ルールグループを更新しました。	2024 年 8 月 30 日
レートベースのルールのしきい値を低くする	今のレートベースのルール最小リクエストレートが 10 になりました。以前、それは 100 でした。	2024 年 8 月 30 日
の AWS マネージドルールを更新しました AWS WAF	Windows オペレーティングシステムのルールグループを更新しました。	2024 年 8 月 28 日
AWS WAF メトリクスに CAPTCHA JavaScript API の新しいメトリクスが追加されました	AWS WAF は、CAPTCHA JavaScript API を使用してアカウント全体の CAPTCHA パズルの試行を表示するためにCaptchasSolvedSdk 、2 つの新しいメトリクス CaptchasAttemptedSdk と を追加しました。	2024 年 8 月 28 日
ListResourcesForWebACL の組織ごとの呼び出しに配分を追加する	AWS WAF は、任意の 1 つのリージョンについて、組織内のアカウントListResourcesForWebACL による への呼び出し数を制限するようになりました。	2024 年 7 月 26 日

AWS Firewall Manager セキュリティポリシーの更新	Network Firewall の TLS 構成情報を読み取るための権限を追加するための FMSServiceRolePolicy の更新。	2024 年 7 月 22 日
の AWS マネージドルールを更新しました AWS WAF	WordPress アプリケーションルールグループを更新しました。	2024 年 7 月 15 日
の AWS マネージドルールを更新しました AWS WAF	Linux オペレーティングシステムのルールグループを更新しました。	2024 年 7 月 12 日
の AWS マネージドルールを更新しました AWS WAF	コアルールセット (CRS) ルールグループを更新しました。	2024 年 7 月 9 日
の AWS マネージドルールを更新しました AWS WAF	PHP アプリケーションと Windows オペレーティングシステムのルールグループを更新しました。	2024 年 7 月 3 日
JSON ボディ解析の仕組みを明確にする	が解析をどのように AWS WAF 処理するか、および本文解析のフォールバック動作を明確にするために、JSON 本文検査のカバレッジを更新しました。	2024 年 6 月 25 日
の AWS マネージドルールを更新しました AWS WAF	Linux オペレーティングシステムのルールグループを更新しました。	2024 年 6 月 6 日

AWS WAF マネージドポリシーの変更	アクセス権限設定にステートメント ID (Sid) を追加するため、WAFV2LoggingServiceRolePolicy および AWSServiceRoleForWAFV2Logging を更新しました。	2024 年 6 月 3 日
AWS WAF マネージドポリシーの変更の追跡	AWS WAF は、管理ポリシー WAFV2LoggingServiceRolePolicy とサービスにリンクされたロール の変更の追跡を開始しましたAWSServiceRoleForWAFV2Logging 。	2024 年 6 月 3 日
の AWS マネージドルールを更新しました AWS WAF	Bot Control、ATP、ACFP マネージドルールグループがバージョン管理され、他のバージョン AWS 管理ルールと同じバージョン更新の SNS 通知が提供されるようになりました。	2024 年 5 月 29 日
の AWS マネージドルールを更新しました AWS WAF	POSIX オペレーティングシステムのルールグループを更新しました。AWSManagedRulesUnixRuleSet	2024 年 5 月 28 日
CAPTCHA および Challenge アクション	ブラウザクライアントが CAPTCHA パズルおよびサイレントチャレンジを実行するために HTTPS を必要とすることを明確にしました。	2024 年 5 月 20 日

Amazon Security Lake との統合	Security Lake を使用して保護パック (ウェブ ACL) トラフィックデータを収集できるようになりました。詳細については、「Amazon Security Lake ユーザーガイド」の AWS 「サービスからのデータ収集」を参照してください。	2024 年 5 月 22 日
Amazon Security Lake との統合	Security Lake を使用して保護パック (ウェブ ACL) トラフィックデータを収集できるようになりました。詳細については、「Amazon Security Lake ユーザーガイド」の AWS 「サービスからのデータ収集」を参照してください。	2024 年 5 月 22 日
の AWS マネージドルールを更新しました AWS WAF	コアルールセット (CRS) ルールグループを更新しました。	2024 年 5 月 21 日
の AWS マネージドルールを更新しました AWS WAF	SQLi データベースルールグループを更新しました。	2024 年 5 月 14 日
の AWS マネージドルールを更新しました AWS WAF	既知の不正な入力と POSIX オペレーティングシステムルールグループを更新しました。	2024 年 5 月 8 日
の AWS マネージドルールを更新しました AWS WAF	Windows オペレーティングシステムのルールグループを更新しました。	2024 年 5 月 3 日
AWS WAF モバイル SDK Android Kotlin コードサンプル	Kotlin ベースの Android 統合のサンプルコードを追加しました。	2024 年 5 月 2 日

AWS WAF メトリクスがディメンションと新しいメトリクスを追加	AWS WAF は、ルールメトリクス`ManagedRuleSetRule` に の新しいディメンションを追加し、ラベルメトリクスの一致ルールアクションに新しいメトリクスを追加しました。	2024 年 5 月 2 日
AWS Firewall Manager がネットワーク ACL ポリシーをサポート	Firewall Manager は、Firewall Manager ネットワーク ACL ポリシーを介した Amazon VPC ネットワークアクセスコントロールリスト (ACL) の管理をサポートするようになりました。	2024 年 4 月 25 日
AWS Firewall Manager セキュリティポリシーの更新	`FMSServiceRolePolicy` に更新して、ネットワーク ACL を管理するためのアクセス権限を追加します。	2024 年 4 月 22 日
更新されたヘルスチェックメトリクスリスト	ヘルスチェックで一般的に使用されるメトリクスのリストからいくつかのメトリクスを削除しました。	2024 年 4 月 16 日
Firewall Manager セキュリティグループポリシーの更新	使用状況監査セキュリティグループポリシーを更新し、ドキュメントを改善しました。使用監査ポリシーのセクションと、ベストプラクティスと制限に関するセクションを参照してください。	2024 年 4 月 2 日

Bot Control の例を更新しました	ターゲットとなる検査レベルを示す例を追加し、ベストプラクティスを反映するように既存の例を更新しました。	2024 年 3 月 27 日
更新された ATP の例	レスポンス検査設定を示す例を追加し、ベストプラクティスを反映するように既存の例を更新しました。	2024 年 3 月 27 日
ACFP の例の更新	レスポンス検査設定を示す例を追加しました。	2024 年 3 月 27 日
Amazon CloudWatch Logs ロググストリームの制限を更新する	AWS WAF CloudWatch Logs ロググストリームへのログの発行には、保護パック (ウェブ ACL) ごとの制限がなくなりました。	2024 年 3 月 27 日
AWS Shield Advanced アプリケーションレイヤー (レイヤー 7) の保護	アプリケーションレイヤーの検出と緩和、ウェブ ACL の使用、レートベースのルール、アプリケーションレイヤー DDoS の自動緩和に関する一般的なガイダンスとベストプラクティスガイダンスを更新しました。	2024 年 3 月 14 日
の AWS マネージドルールを更新しました AWS WAF	IP 評価ルールグループを更新しました。	2024 年 3 月 13 日
ボディ検査サイズ制限の変更	AWS WAF では、一部のリージョンリソースのボディ検査サイズ制限が大きくなりました。	2024 年 3 月 7 日

AWS WAF レートベースのルールの設定可能な評価ウィンドウ	レートベースのルールがリクエストのカウントに使用する時間枠を 1、2、5、または 10 分に設定できるようになりました。デフォルトは 5 で、このリリース前の唯一のオプションでした。	2024 年 2 月 28 日
CAPTCHAおよびChallenge のログ記録情報の拡大	トップレベル `captchaResponse` と `challengeResponse` フィールドには、終了の有無にかかわらず、リクエストに適用されるこれらのアクションの最後の値が入力されるようになりました。それ以前は、これらのフィールドはアクションの終了にのみ入力されていました。	2024 年 2 月 22 日
JavaScript CAPTCHA API キーの管理	API を使用して CAPTCHA JS API キーを削除できるようになりました AWS WAF APIs 。	2024 年 2 月 6 日
AWS WAF CAPTCHA パズルオーディオ	CAPTCHA パズルの音声バージョンは、複数の言語をサポートするようになりました。	2024 年 2 月 6 日
AWS WAF チャレンジと CAPTCHA トークンのラベル付け	トークン管理で CAPTCHA トークンのラベルが追加され、チャレンジトークンのトークンラベル付けが強化されました。	2023 年 12 月 20 日
の AWS マネージドルールを更新しました AWS WAF	既知の不正入力ルールグループを更新しました。	2023 年 12 月 16 日

の AWS マネージドルールを更新しました AWS WAF	既知の不正入力ルールグループを更新しました。	2023 年 12 月 14 日
の AWS マネージドルールを更新しました AWS WAF	コアルールセット (CRS) ルールグループを更新しました。	2023 年 12 月 6 日
の AWS マネージドルールを更新しました AWS WAF	次のルールグループを更新しました。 AWS WAF Bot Control。	2023 年 12 月 5 日
AI エージェント Bot Control マネージドルールグループの新しいウェブ認証ラベル。	Bot Control マネージドルールグループは、CloudFront ディストリビューションにアクセスするボットと AI エージェントの暗号化検証方法として Web Bot Authentication (WBA) をサポートするようになりました。この機能により、正当な AI クローラとエージェントは、従来のチャレンジレスポンスメカニズムを必要とせずにアイデンティティを証明できます。	2023 年 11 月 20 日
Firewall Manager の AWS Config 前提条件を更新	Firewall Manager マネージドロールの代わりにカスタム IAM ロールを使用する場合は AWS Config、アクセス許可ポリシーで AWS Config レコーダーが Firewall Manager リソースを記録できるようにする必要があります。	2023 年 11 月 17 日

AWS WAF コンソールダッシュボード	AWS WAF コンソールで保護パック (ウェブ ACL) のすべてのルールとサンプルリクエストを表示するためのガイダンスを修正しました。	2023 年 11 月 17 日
の AWS マネージドルールを更新しました AWS WAF	Bot Control ルールグループを更新しました。	2023 年 11 月 14 日
AWS WAF コンソールに新しいウェブ ACL ダッシュボードがある	AWS WAF コンソールのウェブ ACL ページには、新しいウェブトラフィック概要ダッシュボードがあります。	2023 年 11 月 14 日
ATP マネージドルールグループを更新しました	ルール `VolumetricIpFailedLoginResponseHigh` および `VolumetricSessionFailedLoginResponseHigh` のラベル情報を修正しました。	2023 年 11 月 13 日
更新された ACFP マネージドルールグループ	ルール `VolumetricIPSuccessfulResponse` および `VolumetricSessionSuccessfulResponse` のラベル情報を修正しました。	2023 年 11 月 13 日
の AWS マネージドルールを更新しました AWS WAF	コアルールセット (CRS) ルールグループを更新しました。	2023 年 11 月 2 日

Shield Advanced アプリケーションレイヤー DDoS 自動緩和	Shield Advanced は、DDoS 攻撃のソースであることが判明している IP アドレスからのリクエストの量を制限するレートベースのルールを自動緩和ルールグループに保持するようになりました。	2023 年 10 月 31 日
の AWS マネージドルールを更新しました AWS WAF	コアルールセット (CRS) ルールグループを更新しました。	2023 年 10 月 30 日
Bot Control マネージドルールグループがリクエスト CSP のシグナルラベルを削除しました	Bot Control マネージドルールグループから、クラウドサービスプロバイダー (CSP) を示すシグナルラベルが削除されました。	2023 年 10 月 28 日
リクエスト CSP の Bot Control マネージドルールグループのシグナルラベル	Bot Control マネージドルールグループのシグナルラベルには、クラウドサービスプロバイダー (CSP) を示すラベルが含まれています。	2023 年 10 月 27 日
IAM AWS WAF アクセス許可情報の更新	保護パック (ウェブ ACL) の関連付けを管理する AWS WAF アクションについて、ポリシーアクションセクションに各ウェブアプリケーションリソースタイプのアクセス許可要件が一覧表示されるようになりました。	2023 年 10 月 25 日

Firewall Manager による変更されたウェブ ACL の管理	関連付けられていないウェブ ACL の管理を有効にすると、Firewall Manager は変更されたウェブ ACL を未使用リソースの 1 回限りのクリーンアップに含めません。	2023 年 10 月 19 日
の AWS マネージドルールを更新しました AWS WAF	POSIX オペレーティングシステムのルールグループを更新しました。`AWSManagedRulesUnixRuleSet`	2023 年 10 月 12 日
AWS WAF メトリクスにディメンションが追加されました	AWS WAF は、ウェブ ACL メトリクスを表示するための新しいディメンションを追加しました。	2023 年 10 月 12 日
の AWS マネージドルールを更新しました AWS WAF	コアルールセット (CRS) ルールグループを更新しました。	2023 年 10 月 11 日
AWS WAF モバイル SDK 仕様の更新	`storeTokenInCookieStorage` 操作を `WAFTokenProvider` に追加しました。	2023 年 10 月 11 日
の例外デプロイ AWS マネージドルール AWS WAF	マネージドルールが、既知の不正入力ルールグループの 2 つの静的バージョンを更新しました。また、最新の静的バージョンに指すデフォルトバージョンを更新しました。	2023 年 10 月 4 日
AWS WAF HTML エンティティデコードテキスト変換	HTML エンティティデコードのテキスト変換機能を拡張しました。	2023 年 10 月 4 日

Firewall Manager のセキュリティグループ共通ポリシーに新しいオプションを追加しました	Firewall Manager は、セキュリティグループの参照をレプリカのセキュリティグループに配布できるようになりました。	2023 年 10 月 3 日
AWS WAF に JA3 フィンガープリントの検査が追加されました	Amazon CloudFront ディストリビューションと Application Load Balancer で、ウェブリクエストの JA3 フィンガープリントと完全に一致できるようになりました。	2023 年 9 月 26 日
Firewall Manager セキュリティグループのポリシールール設定の更新	Firewall Manager は、プライマリセキュリティグループからレプリカセキュリティグループへのセキュリティグループの参照をサポートするようになりました。	2023 年 9 月 25 日
Shield Advanced アプリケーションレイヤー DDoS 自動緩和を更新しました	Firewall Manager は、アプリケーションレイヤー DDoS 自動緩和が設定された Shield Advanced ポリシーの Application Load Balancer リソースをサポートするようになりました。	2023 年 9 月 14 日
の AWS マネージドルールを更新しました AWS WAF	次のルールグループを更新しました。 AWS WAF Bot Control。	2023 年 9 月 6 日

AWS WAF ボットコントロール	Bot Control マネージドルールグループのターゲットを絞った保護レベルで、IP アドレス間のトークンの再利用を検出できるようになりました。また、オプションでトラフィック統計の機械学習分析が可能になり、ボット関連のアクティビティも検出できるようになりました。	2023 年 9 月 6 日
AWS WAF モバイル SDK 仕様の更新	`tokenRefreshDelaySec` の最小値、最大値、デフォルト値をそれぞれ 300、600、300 から、88、300、88 に引き下げました。	2023 年 9 月 5 日
の AWS マネージドルールを更新しました AWS WAF	AWS WAF Bot Control ルールグループを更新しました。	2023 年 8 月 30 日
Shield Advanced アプリケーションレイヤー DDoS 自動緩和	を使用して CloudFormation 、アプリケーションレイヤー DDoS 自動緩和で使用するウェブ ACLs を管理するためのガイダンスを追加しました。	2023 年 8 月 30 日
セキュリティグループ監査ポリシーの Firewall Manager の新しいオプション	過度に許容されるルールグループを監査するための新しいオプションが追加され、コンソール手順の説明が改善されました。	2023 年 8 月 29 日

新しい Firewall Manager Shield および AWS WAF ポリシーオプション	AWS WAF および Shield で関連付けられていないウェブ ACLs の管理を有効にすると、Firewall Manager は、少なくとも 1 つのリソースがウェブ ACLs を使用する場合にのみ、ポリシー範囲内のアカウントにウェブ ACLs を作成します。	2023 年 8 月 9 日
の AWS マネージドルールを更新しました AWS WAF	コアルールセット (CRS) ルールグループを更新しました。	2023 年 7 月 26 日
URI パスにおけるレートベースのルールの集約	レートベースのルールのカスタム集約キーに URI パスを指定できるようになりました。	2023 年 7 月 19 日
の AWS WAF Newpolicy ルールオプション AWS Firewall Manager	AWS Firewall Manager では、AWS WAF ウェブリクエスト本文の検査サイズ制限の設定のサポートが追加されました。	2023 年 7 月 18 日
AWS WAF マネージドポリシーの変更	`AWSWAFFullAccessPolicy` 、、`AWSWAFConsoleFullAccess` 、および を更新`AWSWAFConsoleReadOnlyAccess` して`AWSWAFReadOnlyAccess` 、保護できるリソースタイプに AWS Verified Access を追加しました AWS WAF。	2023 年 6 月 17 日
の AWS マネージドルールを更新しました AWS WAF	ルールグループ `AWSManagedRulesACFPRuleSet` を更新します。	2023 年 6 月 13 日

AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) の更新	正規表現を使用して、ATP マネージドルールグループのログインエンドポイントを指定できるようになりました。	2023 年 6 月 13 日
CAPTCHA JavaScript API に関する新しい情報	新しいセクションでは、 が CAPTCHA でリクエストに AWS WAF 応答したときにカスタム CAPTCHA パズルを提供する方法について説明します。	2023 年 6 月 13 日
新しい ACFP マネージドルールグループ	新しいルールグループ `AWSManagedRulesACFPRuleSet` を使用して、アカウント作成の不正な試みを検出およびブロックします。	2023 年 6 月 13 日
新しい AWS WAF Fraud Control アカウント作成不正防止 (ACFP)	新しい AWS WAF Fraud Control Account Creation Fraud Prevention (ACFP) マネージドルールグループ を使用して、不正なアカウント作成の試みを検出してブロックできます`AWSManagedRulesACFPRuleSet` 。保護された CloudFront ディストリビューションでは、ACFP を使用して、最近送信したアカウント作成の試みの失敗回数が過度に多いクライアントからの新しいアカウント作成の試みをブロックすることもできます。	2023 年 6 月 13 日

AWS WAF マネージドポリシーの変更	AWSWAFFullAccessPolicy 、、AWSWAFReadOnlyAccess 、および AWSWAFConsoleFullAccess を更新AWSWAFConsoleReadOnlyAccess して、 AWS App Runner サービスのアクセス設定を修正しました。	2023 年 6 月 6 日
Firewall Manager のセキュリティグループポリシーの制限を追加	共有 VPC が後で共有を解除された場合、Firewall Manager は関連するアカウントのレプリカセキュリティグループを削除しません。	2023 年 6 月 2 日
新しい AWS WAF リクエストコンポーネント: Header order	リクエスト内のヘッダー名の順序付けされたリストと照合できるようになりました。	2023 年 5 月 30 日
の AWS マネージドルールを更新しました AWS WAF	Linux オペレーティングシステムのルールセットを更新しました。	2023 年 5 月 22 日
AWS WAF ルールセクションの組織を更新しました	ルールステートメントのリストがステートメントタイプ別にグループ化されるようになりました。	2023 年 5 月 16 日
トピックの移動: レート制限されている IP アドレスの一覧表示	レートベースのルールによってレート制限されている IP アドレスを一覧表示するトピックが、レートベースのルールのトピックに追加されました。	2023 年 5 月 16 日

レートベースのルールの拡張オプション	IP アドレス以外の集約キーに基づくウェブリクエストのレート制限や、キーの組み合わせを使用した集約が可能になりました。また、スコープダウンステートメントに一致するすべてのリクエストをさらに集約せずにレート制限することもできます。	2023 年 5 月 16 日
Firewall Manager のクォータの引き上げ	の組織あたりの Firewall Manager ポリシーの数を 20 AWS Organizations から 50 に増やしました。ポリシーごとのプライマリセキュリティグループの最大数を 1 から 3 に増やしました。WCU の最大数をソフトクォータからハードクォータに変更しました。	2023 年 5 月 5 日
ルールグループあたりの最大 WCU が引き上げられました	サポートに引き上げをリクエストしなくても、ルールグループあたり最大 5,000 保護パック (ウェブ ACL) キャパシティユニット (WCU) を使用できるようになりました。この新しい制限を引き上げることはできません。	2023 年 5 月 1 日
AWS WAF プレフィックス付きの Amazon S3 ログバケットの場所	AWS WAF で Amazon S3 ログバケット名のプレフィックスが許可されるようになりました。	2023 年 5 月 1 日
の AWS マネージドルールを更新しました AWS WAF	コアルールセット (CRS) ルールグループを更新しました。	2023 年 4 月 28 日

に AWS Verified Access インスタンスのサポートを追加 AWS WAF	AWS WAF ウェブ ACL を Verified Access インスタンスに関連付けることができるようになりました。この変更は、 の最新バージョンでのみ使用でき AWS WAF 、 AWS WAF Classic では利用できません。	2023 年 4 月 28 日
複数の Firewall Manager 管理者との連携に関する章を改訂しました	組織のファイアウォールリソースを作成および管理する Firewall Manager 管理者を、複数指定できるようになりました。	2023 年 4 月 24 日
AWS Firewall Manager マネージドポリシーの更新	`FMSServiceRolePolicy` を更新しました。	2023 年 4 月 21 日
CAPTCHA 用の新しい JavaScript クライアントアプリケーション統合	JavaScript クライアントアプリケーションでの CAPTCHA パズルの配置と特性をカスタマイズできるようになりました。	2023 年 4 月 20 日
アプリケーションインテグレーションの名前をインテリジェントスレット統合に変更	クライアントアプリケーション統合の既存の機能が、「インテリジェントな脅威に対応した統合」に名称変更され、JavaScript 用の新しい CAPTCHA アプリケーション統合と区別しやすくなりました。	2023 年 4 月 20 日

1,500 WCU を超えるウェブ ACL に適用される変動料金	ウェブ ACL で 1,500 WCU を使用すると追加コストが発生しますが、このコストは、ウェブ ACL WCU の使用量の増減に応じて自動的に調整されます。ウェブ ACL の最大容量は 5,000 WCU です。	2023 年 4 月 11 日
保護パック (ウェブ ACL) あたりの WCU の最大数が引き上げられました	サポートに引き上げをリクエストしなくても、保護パック (ウェブ ACL) あたり最大 5,000 保護パック (ウェブ ACL) キャパシティユニット (WCU) を使用できるようになりました。この新しい制限を引き上げることはできません。	2023 年 4 月 11 日
CloudFront 保護パック (ウェブ ACL) の本文検査のサイズ制限	Amazon CloudFront ディストリビューションを保護する保護パック (ウェブ ACL) の場合、保護パック (ウェブ ACL) 設定で本文検査サイズの制限を最大 64 KB まで引き上げることができます。	2023 年 4 月 11 日
CloudFront の本文検査サイズの引き上げ	Amazon CloudFront ディストリビューションの最大 AWS WAF ボディ検査サイズ制限が 8 KB から 64 KB に引き上げられました。CloudFront のデフォルトの検査サイズの制限は 16 KB です。	2023 年 4 月 11 日

のニュー AWS WAFポリシールールオプション AWS Firewall Manager	AWS Firewall Manager は、AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) と AWS WAF Bot Control AWS マネージドルールのルールグループ、Amazon S3 ログ記録先、ルールアクションの上書き、CAPTCHAChallenge ルールアクション、トークンドメインリストのサポートを追加します。	2023 年 4 月 7 日
AWS WAF マネージドポリシーの変更	AWSWAFFullAccessPolicy 、AWSWAFConsoleFullAccess 、、および を更新AWSWAFConsoleReadOnlyAccess してAWSWAFReadOnlyAccess 、保護できるリソースタイプに AWS App Runner サービスを追加しました AWS WAF。	2023 年 3 月 30 日
セキュリティグループポリシー内でのタグの使用に関する警告を追加しました	ポリシーに、組織のタグポリシーと矛盾するタグが存在する場合に、Firewall Manager が既存のセキュリティグループでのタグ更新や、新しいセキュリティグループの作成を行うことはありません。	2023 年 3 月 28 日
サービスロール情報の更新	Firewall Manager でのサービスロールの使用方法を更新しました。	2023 年 3 月 8 日

レートベースのルールによるレート制限処理の方法についての情報を修正しました	スコープダウンステートメントを含むレートベースのルールは、ルールのスコープダウンステートメントと一致するリクエストのみをレート制限します。以前は、レート制限された IP アドレスのすべてのリクエストに対して、この制限が適用される旨を表記していました。	2023 年 3 月 1 日
の AWS マネージドルールを更新しました AWS WAF	PHP アプリケーションルールグループを更新しました。	2023 年 2 月 27 日
AWS App Runner への のサポートを追加 AWS WAF	AWS WAF ウェブ ACL を AWS App Runner サービスに関連付けることができるようになりました。この変更は、の最新バージョンでのみ使用でき AWS WAF 、 AWS WAF Classic では利用できません。	2023 年 2 月 23 日
の IAM ガイダンスを更新しました AWS Firewall Manager	IAM ベストプラクティスに沿ってガイドを更新しました。詳細については、「IAM でのセキュリティのベストプラクティス」を参照してください。	2023 年 2 月 16 日
の AWS マネージドルールを更新しました AWS WAF	Amazon CloudFront ディストリビューションを保護するウェブ ACL の、ログインレスポンスインスペクションを追加するルールグループ `AWSManagedRulesATPRuleSet` を更新しました。	2023 年 2 月 15 日

AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ログインレスポンス検査	保護された CloudFront ディストリビューションでは、ATP を使用して、最近送信したログイン試行の失敗回数が過度に多いクライアントからの新しいログイン試行をブロックできるようになりました。	2023 年 2 月 15 日
の AWS マネージドルールを更新しました AWS WAF	コアルールセットを更新しました。	2023 年 1 月 25 日
インテリジェントな脅威軽減のベストプラクティス	Bot Control、ATP、およびその他のインテリジェントな脅威の軽減機能を実装するためのベストプラクティスを記載したセクションを追加しました。	2023 年 1 月 22 日
HTTP/2 擬似ヘッダーを検査する方法	HTTP/2 疑似ヘッダーを対応するウェブリクエストコンポーネントにマップするセクションを追加しました。	2023 年 1 月 20 日
AWS WAF Classic の IAM ガイダンスを更新しました	IAM ベストプラクティスに沿ってガイドを更新しました。詳細については、「IAM のセキュリティのベストプラクティス」を参照してください。	2023 年 1 月 3 日
の IAM ガイダンスを更新しました AWS Shield	IAM ベストプラクティスに沿ってガイドを更新しました。詳細については、「IAM のセキュリティのベストプラクティス」を参照してください。	2023 年 1 月 3 日

Amazon Route 53 Resolver DNS Firewall ポリシーの更新	Amazon Route 53 Resolver の DNS Firewall ルールグループの削除に関する情報を追加しました。	2022 年 12 月 29 日
の AWS マネージドルールを更新しました AWS WAF	Linux オペレーティングシステムのルールセットを更新しました。	2022 年 12 月 15 日
の AWS マネージドルールを更新しました AWS WAF	コアルールセットを更新しました。	2022 年 12 月 5 日
Firewall Manager は、Fortigate Cloud Native Firewall (CNF) as a Service ポリシーのサポートを追加します	Firewall Manager が Fortigate CNF ポリシーをサポートするようになりました。	2022 年 12 月 2 日
DNS Firewall ポリシー AWS Config の要件を削除	DNS Firewall ポリシーでは、リソースタイプ EC2 VPC の Config を有効にするだけでよくなりました。	2022 年 11 月 17 日
AWS Firewall Manager マネージドポリシーの更新	`FMSServiceRolePolicy` を更新しました。	2022 年 11 月 15 日
AWS WAF CAPTCHA パズルの言語オプションの拡張	CAPTCHA パズルは、複数の言語で書かれた説明を提供するようになりました。各オーディオパズル内の説明は、現在も英語でのみ提供されています。	2022 年 11 月 11 日
Firewall Manager のリソースセットの新しいクォータ	リソースセットの新しいクォータを追加しました。	2022 年 11 月 8 日

リソースセットのサポートを追加する	リソースセットを作成して、Firewall Manager ポリシーで管理するリソースをグループ化できます。	2022 年 11 月 8 日
Network Firewall からのファイアウォールのインポートのサポートを追加する	リソースセットを使用して、Network Firewall ポリシーの既存のファイアウォールをインポートして管理できるようになりました。	2022 年 11 月 8 日
AWS Firewall Manager マネージドポリシーの更新	`AWSFMAdminReadOnly Access` を更新しました。	2022 年 11 月 2 日
地理一致ステートメントは、国と地域のリクエストにラベルが追加されるようになりました	地理マッチングとラベルマッチングを組み合わせることで、リージョンレベルで地理的なリクエスト元を管理できるようになりました。	2022 年 10 月 31 日
上位レベルのセクションの名前を「マネージド保護」に変更しました	このセクションには、マーケティングページに沿った AWS WAF インテリジェントな脅威軽減策という名前が付けられました。	2022 年 10 月 27 日
Bot Control マネージドルールグループのターゲットを絞った新しい保護レベル	Bot Control マネージドルールグループには、高度なボットを検出および軽減するためのターゲットを絞ったルールが追加されました。この保護レベルは追加料金でご利用いただけます。	2022 年 10 月 27 日
AWS WAF トークンに関する新しいセクション	がトークン AWS WAF を使用してインテリジェントな脅威の軽減を行う方法を理解します。	2022 年 10 月 27 日

Firewall Manager Network Firewall ポリシーの更新に関する重要な注意事項を追加しました	Firewall Manager ポリシーを更新すると、そのポリシーによって作成されたすべての Network Firewall ポリシーが、Firewall Manager ポリシーの Network Firewall ポリシー構成で更新されます。	2022 年 10 月 27 日
ルールグループ内のアクションオーバーライド	ルールグループ内のルールアクションを任意のルールアクション設定にオーバーライドできるようになりました。前の Count アクションオーバーライドと同様に、オーバーライドをルールグループ内のすべてのルールと個々のルールに適用できます。	2022 年 10 月 27 日
AWS WAF 新しいChallenge ルールアクションオプション	リクエストがブラウザから送信されていることを確認するために、Challenge を使用するようにルールを設定できます。	2022 年 10 月 27 日
AWS WAF では、複数の保護されたアプリケーション間でトークンを共有できます。	保護パック (ウェブ ACL) のトークンドメインリストを設定することで、保護されている複数のアプリケーション間でトークンの使用を有効にできます。	2022 年 10 月 27 日
すべてのヘッダーの仕様は大文字と小文字を区別しない	すべてのヘッダーの仕様を大文字と小文字を区別しないように変更しました。これは単一ヘッダーの動作と一致します。	2022 年 10 月 26 日

AWS Firewall Manager マネージドポリシーの変更	`AWSFMAdminFullAccess` の修正。	2022 年 10 月 21 日
の AWS マネージドルールを更新しました AWS WAF	既知の不正入力ルールグループを更新しました。	2022 年 10 月 20 日
の AWS マネージドルールを更新しました AWS WAF	既知の不正入力ルールグループを更新しました。	2022 年 10 月 5 日
AWS WAF モバイル SDK 仕様の更新	`tokenRefreshDelaySec` のデフォルト値を 600 (10 分) から 300 (5 分) に引き下げました。	2022 年 9 月 30 日
の AWS マネージドルールを更新しました AWS WAF	このドキュメントに記載されている POSIX オペレーティングシステム、PHP アプリケーション、WordPress アプリケーションのルールグループのラベル名を修正しました。	2022 年 9 月 19 日
の AWS WAF Newpolicy ルールオプション AWS Firewall Manager	AWS Firewall Manager は、AWS WAF ポリシーのデフォルトのウェブアクションに対してカスタマイズされたウェブリクエストとレスポンスをサポートするようになりました。	2022 年 9 月 9 日
の AWS マネージドルールを更新しました AWS WAF	次のルールグループを更新しました: IP の評価。	2022 年 8 月 30 日

AWS WAF マネージドポリシーの変更	AWSWAFFullAccessPolicy 、AWSWAFConsoleFullAccess 、、および を更新AWSWAFConsoleReadOnlyAccess してAWSWAFReadOnlyAccess 、保護できるリソースタイプに Amazon Cognito ユーザープールを追加しました AWS WAF。	2022 年 8 月 25 日
AWS WAF Fraud Control アカウント乗っ取り防止 (ATP)	Amazon CloudFront ディストリビューションで AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) 機能を使用できるようになりました。	2022 年 8 月 24 日
の AWS マネージドルールを更新しました AWS WAF	次のルールグループを更新しました: 既知の不正入力。	2022 年 8 月 22 日
の AWS マネージドルールを更新しました AWS WAF	次のルールグループを更新しました: AWSManagedRulesATPRuleSet 。	2022 年 8 月 11 日
に Amazon Cognito ユーザープールのサポートを追加 AWS WAF	AWS WAF ウェブ ACL を Amazon Cognito ユーザープールに関連付けることができるようになりました。この変更は、 の最新バージョンでのみ使用でき AWS WAF 、 AWS WAF Classic では利用できません。	2022 年 8 月 11 日

バージョン管理された AWS マネージドルールルールグループのデプロイに関するセクションを追加しました	バージョン管理された AWS マネージドルールルールグループのデプロイを文書化した新しいセクションを追加しました。このセクションには、リリース候補のデプロイ中におけるデフォルトバージョンの命名方法に関する情報が含まれています。	2022 年 7 月 29 日
Network Firewall ポリシーのログ記録を設定するための要件を更新	暗号化された Amazon S3 バケットをログの送信先として使用する Network Firewall ポリシーの要件を追加しました。	2022 年 7 月 26 日
SQLi ルールステートメントの感度レベルオプション	これで、SQL インジェクションルールステートメントの感度を上げることができます。ただし、デフォルトの感度レベルが LOW の既存のステートメントの動作は変更されません。	2022 年 7 月 15 日
Network Firewall ポリシー設定オプションを追加	Firewall Manager は、Network Firewall のファイアウォールポリシー設定で、ステートフルな評価順序とデフォルトアクションをサポートするようになりました。	2022 年 7 月 14 日
Firewall Manager セキュリティグループのポリシールール設定の更新	Firewall Manager は、プライマリセキュリティグループからレプリカセキュリティグループへのタグ配布をサポートするようになりました。	2022 年 7 月 7 日

AWS Shield ガイドの更新	Shield ガイドの情報を拡充して、Shield がイベントの軽減をどのように実行するかを説明します。	2022 年 6 月 24 日
テストとチューニング AWS WAF の保護に関するガイダンスを更新	テストとチューニングの一般的なガイダンス AWS WAF が更新され、最上位のトピックになりました。	2022 年 6 月 20 日
の AWS マネージドルールを更新しました AWS WAF	次のルールグループを更新しました: コアルールセット (CRS)。	2022 年 6 月 9 日
新しい Firewall Manager における混乱した代理に関するガイダンス	Firewall Manager における混乱した代理問題の防止方法に関するガイダンスを追加しました。	2022 年 6 月 1 日
の AWS マネージドルールを更新しました AWS WAF	次のルールグループを更新しました: コアルールセット (CRS)。	2022 年 5 月 24 日
新しい AWS WAF リクエストコンポーネント: Headersおよび Cookies	これで、Cookie を検査できるようになり、単一のヘッダーだけでなく、ウェブリクエスト内のすべてのヘッダーを検査できます。	2022 年 4 月 29 日
新しい AWS WAF リクエストコンポーネント: Headersおよび Cookies	これで、ウェブリクエストで cookie を検査でき、単一のヘッダーだけでなく、ウェブリクエスト内のすべてのヘッダーを検査できるようになりました。	2022 年 4 月 29 日

AWS WAF オーバーサイズの本文、ヘッダー、Cookie リクエストコンポーネントの処理	これらのコンポーネントを検査するルール内で、 AWS WAF がオーバーサイズのリクエスト本文、ヘッダー、Cookie を処理する方法を指定できるようになりました。これらのコンポーネントを検査する、すでに作成済みのルールは、オーバーサイズ処理の新しい Continue オプションに一致する動作をします。	2022 年 4 月 29 日
AWS WAF Amazon S3 ログポリシーの変更	Amazon S3 ログ許可ポリシーと例を更新しました。	2022 年 4 月 12 日
Application Load Balancer AWS Shield Advanced の でアプリケーションレイヤー DDoS 自動緩和オプションが利用可能に	Shield Advanced は、Application Load Balancer 向けにアプリケーションレイヤー DDoS 自動緩和をサポートするようになりました。これにより、すべてのアプリケーションレイヤー保護のために使用できます。保護されたリソースに対するアプリケーションレイヤー DDoS 攻撃の一部であるウェブリクエストを自動的にカウントまたはブロックするように Shield Advanced を設定できます。	2022 年 4 月 8 日
マネージドルールグループの現在のデフォルトバージョン設定のインジケーターを追加しました	マネージドルールグループのバージョンリストに、現在のデフォルトバージョンが示されるようになりました。	2022 年 4 月 8 日

の AWS マネージドルールを更新しました AWS WAF	次のルールグループを更新しました。 AWS WAF Bot Control。	2022 年 4 月 6 日
の AWS マネージドルールを更新しました AWS WAF	次のルールグループを更新しました: 既知の不正入力。	2022 年 3 月 31 日
の AWS マネージドルールを更新しました AWS WAF	次のルールグループを更新しました: 既知の不正入力。	2022 年 3 月 30 日
Firewall Manager が Palo Alto Networks Cloud Next Generation Firewall (NGFW) のサポートを追加	Firewall Manager が Palo Alto Networks Cloud Next Generation Firewall (NGFW) をサポートするようになりました。	2022 年 3 月 30 日
Palo Alto Networks Cloud NGFW のサポートを に追加する AWS Firewall Manager	AWS Firewall Manager が Palo Alto Networks Cloud Next Generation Firewall (NGFW) ポリシーをサポートするようになりました。	2022 年 3 月 30 日
AWS Shield ガイドの更新	Shield ガイドの情報を拡充して、Shield がイベント検出をどのように実行するかを説明し、DDoS に対する耐性が高いアーキテクチャの例を記載しました。	2022 年 3 月 16 日
AWS Shield ガイドの更新	Shield ガイドの情報を拡充し、さまざまなセクションの編成を改善しました。主な変更点は、Shield Response Team (SRT) サポート、 でのリソース保護 AWS Shield Advanced、DDoS イベントの可視性の Shield ガイドセクションです。	2022 年 2 月 28 日

Firewall Manager が Network Firewall の集約型デプロイモデルのサポートを開始	分散型および集約型デプロイモデルを使用するポリシーを設定する方法を説明する新しい手順を追加しました。	2022 年 2 月 24 日
Firewall Manager が AWS Network Firewall 一元化されたデプロイモデルのサポートを追加	分散デプロイモデルまたは集中デプロイモデルを使用するように AWS Network Firewall ポリシーを設定できるようになりました。分散デプロイモデルでは、Firewall Manager は、ポリシー範囲内の各 VPC にファイアウォールエンドポイントを作成および維持します。集約型デプロイモデルでは、Firewall Manager は、単一の検査 VPC でファイアウォールエンドポイントを作成および維持します。	2022 年 2 月 24 日
AWS WAF マネージドルールグループのバージョニングのサポートを に追加する AWS Firewall Manager	AWS Firewall Manager は、Firewall Manager AWS WAF ポリシーで AWS WAF マネージドルールグループのバージョニングをサポートするようになりました。	2022 年 2 月 18 日
AWS Firewall Manager マネージドポリシーの変更	`FMSServiceRolePolicy` に更新します。	2022 年 2 月 16 日
の AWS マネージドルールを更新しました AWS WAF	次のルールグループを更新しました: IP 評価リスト。	2022 年 2 月 15 日

の AWS マネージドルールを更新しました AWS WAF	AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループ を更新しましたAWSManagedRulesATPRuleSet 。	2022 年 2 月 11 日
AWS WAF ガイドの組織の変更	マネージド保護の新しい上位のセクションを追加しました。CAPTCHA セクションをルールから新しいマネージド保護セクションに移動しました。ラベルセクションをルールから独自の上位のセクションに移動しました。	2022 年 2 月 11 日
AWS WAF クライアントアプリケーション統合	AWS WAF JavaScript およびモバイルクライアント APIs を使用して、クライアントアプリケーションをインテリジェントな脅威軽減 AWS マネージドルールルールグループと統合し、検出を強化します。	2022 年 2 月 11 日
AWS WAF Fraud Control アカウント乗っ取り防止 (ATP)	新しい AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) マネージドルールグループ を使用して、アカウント乗っ取りの試行を検出してブロックできますAWSManagedRulesATPRuleSet 。	2022 年 2 月 11 日
の AWS マネージドルールを更新しました AWS WAF	次のルールグループを更新しました: 既知の不正入力。	2022 年 1 月 28 日

AWS WAF マネージドポリシーの変更	AWSWAFFullAccessPolicy および AWSWAFConsoleFullAccess が更新され、ログ記録の許可が修正されました。	2022 年 1 月 11 日
の AWS マネージドルールを更新しました AWS WAF	次のルールグループを更新しました: コアルールセット (CRS)、SQLi データベース。	2022 年 1 月 10 日
Firewall Manager が Shield Advanced アプリケーションレイヤー DDoS 自動緩和をサポート	Amazon CloudFront リソース向けの Firewall Manager Shield Advanced のポリシーに、アプリケーションレイヤー DDoS 自動緩和のサポートが含まれるようになりました。	2022 年 1 月 7 日
AWS Firewall Manager マネージドポリシーの変更	FMSServiceRolePolicy に更新します。	2022 年 1 月 7 日
の AWS マネージドルールを更新しました AWS WAF	次のルールグループを更新しました: 既知の不正入力。	2021 年 12 月 17 日
の AWS マネージドルールを更新しました AWS WAF	次のルールグループを更新しました: 既知の不正入力。	2021 年 12 月 11 日
の AWS マネージドルールを更新しました AWS WAF	次のルールグループを更新しました: 既知の不正入力。	2021 年 12 月 10 日
新しい AWS Shield Advanced サービスにリンクされたロール	アプリケーションレイヤー DDoS 自動緩和機能をサポートするために AWSServiceRoleForAWSShield を追加しました。	2021 年 12 月 1 日

新しい AWS Shield 管理ポリシー	アプリケーションレイヤー DDoS 自動緩和機能をサポートするために `AWSShieldServiceRolePolicy` を追加しました。	2021 年 12 月 1 日
CloudFront AWS Shield Advanced の でアプリケーションレイヤー DDoS 自動緩和オプションが利用可能に	Shield Advanced は、Amazon CloudFront ディストリビューション向けにアプリケーションレイヤー DDoS 自動緩和をサポートするようになりました。CloudFront ディストリビューションに対するアプリケーションレイヤー DDoS 攻撃の一部であるウェブリクエストを自動的にカウントまたはブロックするように Shield Advanced を設定できます。	2021 年 12 月 1 日
の AWS マネージドルールを更新しました AWS WAF	次のルールグループを更新しました: コアルールセット (CRS)、Windows オペレーティングシステム、Linux オペレーティングシステム、および IP 評価リスト。	2021 年 11 月 23 日
AWS Firewall Manager マネージドポリシーの変更	`FMSServiceRolePolicy` に更新します。	2021 年 11 月 18 日

の拡張ログ記録オプション AWS WAF	保護パック (ウェブ ACL) トラフィックのログを Amazon CloudWatch Logs ロググループまたは Amazon Simple Storage Service (Amazon S3) バケットに記録できるようになりました。これらのオプションは、Amazon Data Firehose 配信ストリームへのログ記録の既存のオプションに追加されています。	2021 年 11 月 15 日
AWS WAF マネージドポリシーの変更	`AWSWAFFullAccessPolicy` および `AWSWAFConsoleFullAccess` が更新され、追加のログ記録の宛先をサポートするようになりました。	2021 年 11 月 15 日
AWS WAF 新しいCAPTCHA ルールアクションオプション	ウェブリクエストに対して CAPTCHA を実行し、必要に応じてクライアントに CAPTCHA 問題を送信するようにルールを設定できます。	2021 年 11 月 8 日
の AWS マネージドルールを更新しました AWS WAF	コアルールセット (CRS) ルールグループを更新しました。	2021 年 10 月 27 日
の AWS マネージドルールを更新しました AWS WAF	すべての AWS マネージドルールルールグループでラベル付けがサポートされるようになりました。ルールの説明には、ラベルの指定が含まれます。	2021 年 10 月 25 日

Firewall Manager が Network Firewall ログフィルタリングをサポート	AWS Firewall Manager で Network Firewall ポリシーのログフィルタリングがサポートされるようになりました。	2021 年 10 月 4 日
AWS Firewall Manager マネージドポリシーの変更	`FMSServiceRolePolicy` に更新します。	2021 年 9 月 29 日
正規表現一致ステートメントを追加しました	ウェブリクエストを 1 つの正規表現と照合できるようになりました。	2021 年 9 月 22 日
ルールグループ内のレートベースの AWS WAF ルール	ルールグループ内でレートベースの AWS WAF ルールを定義できるようになりました。では AWS Firewall Manager、この機能は ポリシーで AWS WAF 完全にサポートされています。	2021 年 9 月 13 日
でout-of-scopeのリソース保護を自動的に削除する AWS Firewall Manager	AWS Firewall Manager では、ポリシーの範囲を離れるリソースから保護を自動的に削除できます。	2021 年 8 月 25 日
AWS Firewall Manager マネージドポリシーの変更	`FMSServiceRolePolicy` に更新します。	2021 年 8 月 12 日
マネージドルールグループにバージョニングを追加しました	マネージドルールグループのプロバイダーは、ルールグループをバージョニングできるようになりました。	2021 年 8 月 9 日
AWS Firewall Manager 管理者要件の変更	Firewall Manager 管理者アカウントとして、組織の管理アカウントを使用できます。これは禁止されていました。	2021 年 8 月 2 日

Firewall Manager のクォータの引き上げ	Firewall Manager ポリシーの範囲内に存在できる Amazon VPC インスタンスの数を 10 から 100 に引き上げました。	2021 年 7 月 28 日
AWS Firewall ManagerAWS Network Firewall ルートテーブルモニタリングのサポート	AWS Firewall Manager は、ルートテーブルのモニタリングをサポートするようになりました。また、ルートの設定ミスがある AWS Network Firewall ポリシーについて、セキュリティ管理者に修復アクションの推奨事項を提供します。	2021 年 7 月 8 日
AWS WAF 追加のテキスト変換オプション	テキスト変換のオプションが拡張され、リクエストを検査する前にウェブリクエストコンポーネントを適用できるようになりました。	2021 年 6 月 24 日
Firewall Manager AWS WAF ポリシーリソースの命名を変更	Firewall Manager が AWS WAF ポリシーに対して管理するウェブ ACLs、ルールグループ、ログ記録の命名が変更されました。	2021 年 5 月 26 日
の AWS マネージドルールを更新しました AWS WAF	IP 評価リストへのラベル付けのサポートを更新し、Amazon IP 評価リストのルール名のサフィックスを削除しました。	2021 年 5 月 4 日

AWS Organizations 委任管理者のサポートを追加する	AWS Firewall Manager 管理者アカウントを設定すると、Firewall Manager はアカウントを Firewall Manager の AWS Organizations 委任管理者として指定するようになりました。この変更により、Firewall Manager 管理者アカウントを設定するときに、組織の管理アカウント以外のメンバーアカウントを指定する必要があります。この変更は、既存の設定には影響しません。	2021 年 4 月 30 日
の AWS マネージドルールを更新しました AWS WAF	AWS WAF Bot Control ルールグループを更新しました。	2021 年 4 月 1 日
ルールグループ内で個別のルールアクションを Count に設定	ルールグループ内の個々のルールアクションを Count に設定できるようになりました。ルールグループレベルにある既存の上書きの情報が修正されました。	2021 年 4 月 1 日
マネージドルールグループのスコープダウンステートメント	レートベースのステートメントと同じ方法で、マネージドルールグループでスコープダウンステートメントを使用できるようになりました。	2021 年 4 月 1 日
ログのフィルタリング	ルールのアクションとラベルに基づいて、ログに記録する保護パック (ウェブ ACL) トラフィックをフィルタリングできるようになりました。	2021 年 4 月 1 日

AWS WAF ウェブリクエストのラベル	一致するウェブリクエストにラベルを追加し、他のルールによって追加されたラベルと照合するルールを設定できます。	2021 年 4 月 1 日
AWS WAF ボットコントロール	Bot AWS WAF Control マネージドルールグループとウェブリクエストのラベル付け、スコープダウンステートメント、ログフィルタリングを組み合わせた新しい Bot Control 機能を使用して、ボットトラフィックをモニタリングおよび制御できます。	2021 年 4 月 1 日
Firewall Manager が Amazon Route 53 Resolver DNS Firewall ポリシーをサポート	AWS Firewall Manager は VPCs の Amazon Route 53 Resolver DNS Firewall アウトバウンド DNS トラフィックフィルタリングの一元管理をサポートします。	2021 年 3 月 31 日
カスタムリクエストとレスポンスの処理	AWS WAF がブロックしないウェブリクエストのカスタムヘッダーを含めることができ、 AWS WAF がブロックするウェブリクエストについてはカスタムレスポンスを送信できます。これは、保護パック (ウェブ ACL) のデフォルトアクションおよびルールアクションの設定で使用できます。	2021 年 3 月 29 日
AWS Firewall Manager マネージドポリシーの変更	`FMSServiceRolePolicy` に更新します。	2021 年 3 月 17 日

の AWS マネージドルールを更新しました AWS WAF	次のルールグループを更新しました: コアルールセット (CRS)、管理者保護、既知の不正入力、および Linux オペレーティングシステム。	2021 年 3 月 3 日
AWS Shield マネージドポリシーの変更の追跡	Shield は、 AWS 管理ポリシーの変更の追跡を開始しました。	2021 年 3 月 3 日
AWS Firewall Manager マネージドポリシーの変更の追跡	Firewall Manager は、 AWS 管理ポリシーの変更の追跡を開始しました。	2021 年 3 月 2 日
AWS WAF マネージドポリシーの変更の追跡	AWS WAF は、 AWS 管理ポリシーの変更の追跡を開始しました。	2021 年 3 月 1 日
ウェブリクエストボディを解析された JSON として検査する	ウェブリクエストボディを解析およびフィルタリングされた JSON として検査するオプションを追加しました。これは、ウェブリクエストボディをプレーンテキストとして検査する既存のオプションに追加されるものです。	2021 年 2 月 12 日
Firewall Manager が AWS Network Firewall ポリシーをサポート	AWS Firewall Manager は VPCs の AWS Network Firewall ネットワークトラフィックフィルタリングの一元管理をサポートします。	2020 年 11 月 17 日
AWS Shield Advanced 保護グループのサポートを追加する	保護されたリソースを論理グループにグループ化し、それらの保護をまとめて管理できるようになりました。	2020 年 11 月 13 日

AWS AppSync に のサポートを追加 AWS WAF	AWS WAF ウェブ ACL を AWS AppSync GraphQL API に関連付けることができるようになりました。この変更は、 の最新バージョンでのみ使用でき AWS WAF 、 AWS WAF Classic では利用できません。	2020 年 10 月 1 日
の AWS マネージドルールを更新しました AWS WAF	Windows オペレーティングシステムのルールグループを更新しました。	2020 年 9 月 23 日
の AWS マネージドルールを更新しました AWS WAF	PHP アプリケーションと POSIX オペレーティングシステムのルールセットを更新しました。	2020 年 9 月 16 日
更新された AWS Shield コンソール	AWS Shield は、ユーザーエクスペリエンスを向上させた新しいコンソールオプションを提供します。このドキュメントのコンソールに関するガイダンスは、新しいコンソールに関するものです。	2020 年 9 月 1 日
Firewall Manager が共通セキュリティグループポリシーを更新	AWS Firewall Manager 共通セキュリティグループポリシーは、コンソール実装を通じて Application Load Balancer と Classic Load Balancer のリソースタイプをサポートするようになりました。新しいオプションは、共通ポリシーの [Policy scope] (ポリシーの範囲) 設定で使用できます。	2020 年 8 月 11 日

の AWS マネージドルールを更新しました AWS WAF	コアルールセットを更新しました。	2020 年 8 月 7 日
ウェブリクエストで IP アドレスの場所を指定する	ウェブリクエストの発信元を使用する代わりに、指定した HTTP ヘッダーからの IP アドレスを使用するオプションを追加しました。代替ヘッダーは通常 `X-Forwarded-For` (XFF) ですが、任意のヘッダー名を指定できます。このオプションは、IP セット一致、geo 一致、およびレートベースのルールカウント集約に使用できます。	2020 年 7 月 9 日
Firewall Manager がコンテンツ監査セキュリティグループポリシーを更新	AWS Firewall Manager では、マネージドルールオプション、マネージドアプリケーションとプロトコルリストを使用する マネージドルールオプション、リソース違反の詳細など、コンテンツ監査セキュリティグループポリシーの機能を拡張しました。	2020 年 7 月 7 日
Firewall Manager マネージドリスト	AWS Firewall Manager でマネージドアプリケーションおよびプロトコルリストがサポートされるようになりました。Firewall Manager はいくつかのリストを管理します。また、独自のリストを作成して管理できます。	2020 年 7 月 7 日

Firewall Manager は、共通セキュリティグループポリシーで共有 VPC をサポートします	AWS Firewall Manager は、共有 VPCsでの一般的なセキュリティグループポリシーの使用をサポートするようになりました。これは、範囲内のアカウントが所有する VPC での使用に加えて、行うことができます。	2020 年 5 月 26 日
の AWS マネージドルールを更新しました AWS WAF	の AWS マネージドルールに各ルールのドキュメントを追加しました AWS WAF。	2020 年 5 月 20 日
の AWS マネージドルールを更新しました AWS WAF	Linux オペレーティングシステムのルールグループを更新しました。	2020 年 5 月 19 日
AWS WAF Classic リソースを AWS WAF (v2) に移行するためのサポートを追加	コンソールまたは API を使用して、最新バージョンの に移行するために AWS WAF Classic リソースをエクスポートできるようになりました AWS WAF。	2020 年 4 月 27 日

ポリシー範囲内の AWS Organizations 組織単位のサポートを追加する	AWS Firewall Manager では、AWS Organizations 組織単位 (OUsを使用してポリシーの範囲を指定できるようになりました。OU を使用して、特定のアカウントを含めたり除外したりするほかに、範囲にアカウントを含めたり、スコープからアカウントを除外したりできます。OU を指定する方法は、OU およびその子である OU のすべてのアカウント (後から追加される子の OU およびアカウントを含む) を指定する方法と同じです。	2020 年 4 月 6 日
AWS WAF (v2) のサポートを に追加する AWS Firewall Manager	AWS Firewall Manager は AWS WAF、以前のバージョンである AWS WAF Classic に加えて、 の最新バージョンをサポートするようになりました。	2020 年 3 月 31 日
AWS Firewall Manager 一般的なセキュリティグループポリシーの更新	AWS Firewall Manager 共通セキュリティグループポリシーに、範囲内の Amazon EC2 インスタンス内のすべての Elastic Network Interface にポリシーを適用するオプションが追加されました。ただし、引き続きデフォルトの Elastic Network Interface にのみポリシーを適用することも選択できます。	2020 年 3 月 11 日

の AWS マネージドルールを更新しました AWS WAF	AWS のマネージドルールにAWSManagedRulesAnonymousIpList ルールグループ AWS WAF が追加されました。	2020 年 3 月 6 日
の AWS マネージドルールを更新しました AWS WAF	AWS のマネージドルールが WordPress アプリケーションとAWSManagedRulesCommonRuleSet ルールグループ AWS WAF を更新しました。	2020 年 3 月 3 日
AWS Shield Advanced 保護オプションに Amazon Route 53 ヘルスチェックを追加	Shield Advanced では、Amazon Route 53 ヘルスチェックの関連付けの使用をサポートして、脅威の検出と緩和機能の精度を向上させます。	2020 年 2 月 14 日
の AWS マネージドルールを更新しました AWS WAF	AWS のマネージドルール AWS WAF が SQL Database ルールグループを更新し、メッセージ URI のチェックを追加しました。	2020 年 1 月 23 日
セキュリティグループ使用状況監査ポリシーの Firewall Manager の新しいオプション	Firewall Manager には、セキュリティグループ使用状況監査ポリシーの新しいオプションがあります。セキュリティグループの未使用状態が最低何分続いたら非準拠とみなすかを設定できるようになりました。デフォルトでは、この時間設定はゼロです。	2020 年 1 月 14 日

AWS WAF ポリシーの Firewall Manager の新しいオプション	Firewall Manager には、 AWS WAF ポリシーの新しいオプションがあります。ポリシーの新しいウェブ ACL を関連付ける前に、範囲内のリソースから既存のウェブ ACL の関連付けをすべて削除することを選択できるようになりました。	2020 年 1 月 14 日
の AWS マネージドルールを更新しました AWS WAF	AWS のマネージドルール AWS WAF は、コアルールセットと SQL データベースルールグループのルールのテキスト変換を更新しました。	2019 年 12 月 20 日
AWS Firewall Manager と統合 AWS Security Hub CSPM	AWS Firewall Manager は、コンプライアンス違反のリソースと攻撃の検出結果を作成し、送信するようになりました AWS Security Hub CSPM。	2019 年 12 月 18 日

AWS WAF バージョン 2 のリリース	デ AWS WAF ベロッパーガイドの新しいバージョン。JSON 形式でウェブ ACL またはルールグループを管理できます。拡張された機能には、論理ルールステートメント、ルールステートメントのネスト、IP アドレスおよびアドレス範囲の完全な CIDR サポートが含まれます。ルールは AWS リソースではなくなりましたが、ウェブ ACL またはルールグループのコンテキストにのみ存在します。既存のお客様の場合、以前のバージョンの サービスが AWS WAF Classic と呼ばれるようになりました。APIs、SDKs、および CLIs、 AWS WAF Classic は命名スキームを保持し、この最新バージョンの AWS WAF は、context に応じて「V2」または「v2」を追加して参照されます。 AWS WAF は AWS WAF Classic で作成された AWS リソースにアクセスできません。これらのリソースを で使用するには AWS WAF、移行する必要があります。	2019 年 11 月 25 日
AWS のマネージドルールルールグループ AWS WAF	AWS マネージドルールのルールグループを追加しました。これらは AWS WAF お客様に対しては無料です。	2019 年 11 月 25 日

AWS Firewall Manager Amazon Virtual Private Cloud セキュリティグループの サポート	Firewall Manager に Amazon VPC セキュリティグループのサポートを追加しました。	2019 年 10 月 10 日
AWS Firewall Manager のサポート AWS Shield Advanced	Firewall Manager に Shield Advanced のサポートを追加しました。	2019 年 3 月 15 日
チュートリアル: 階層型ポリシーの作成	チュートリアル : AWS Firewall Managerでの階層型ポリシーの作成に関するチュートリアルを追加しました。	2019 年 2 月 11 日
ルールグループのルールレベルの制御	ルール AWS Marketplace グループと独自のルールグループから個々のルールを除外できるようになりました。	2018 年 12 月 12 日
AWS Shield AdvancedAWS Global Accelerator 標準アクセラレーターのサポート	Shield Advanced で AWS Global Accelerator 標準アクセラレーターを保護できるようになりました。	2018 年 11 月 26 日
AWS WAF Amazon API Gateway のサポート	AWS WAF は、Amazon API Gateway APIsを保護するようになりました。	2018 年 10 月 25 日
拡張 AWS シールドアドバンスト入門ウィザード	新しいウィザードは、レートベースのルールと Amazon CloudWatch Events を作成する機会を提供します。	2018 年 8 月 31 日
AWS WAF logging	ログ記録を有効にして、ウェブ ACL で分析されるトラフィックに関する詳細情報を取得します。	2018 年 8 月 31 日

条件内のパラメータのクエリをサポート	条件を作成するときに、特定のパラメータに対するリクエストを検索できるようになりました。	2018 年 6 月 5 日
Shield Advanced 使用開始ウィザード	Shield Advanced AWS にサブスクライブするための新しい合理化されたプロセスを紹介します。	2018 年 6 月 5 日
許可される CIDR 範囲が拡張されました	IP 一致条件を作成するときに、 は IPv4 アドレス範囲 /8 および /16 から /32 までの任意の範囲をサポートする AWS WAF ようになりました。	2018 年 6 月 5 日

2018 年よりも前の更新

次の表は、「AWS WAF デベロッパーガイド」の各リリースでの 2018 年より前の重要な変更を示しています。

変更	API バージョン	説明	リリース日
更新	2016-08-24	AWS Marketplace ルールグループ	2017 年 11 月
更新	2016-08-24	Elastic IP 向けの Shield Advanced サポート	2017 年 11 月
更新	2016-08-24	グローバル脅威ダッシュボード	2017 年 11 月
更新	2016-08-24	DDoS 対応ウェブサイトのチュートリアル	2017 年 10 月

変更	API バージョン	説明	リリース日
更新	2016-08-24	Geo 条件と正規表現条件	2017 年 10 月
更新	2016-08-24	レートベースのルール	2017 年 6 月
更新	2016-08-24	再編成	2017 年 4 月
更新	2016-08-24	DDOS 保護とアプリケーションロードバランサーのサポートに関する情報を追加しました。	2016 年 11 月
新機能	2015-08-24	アカウントの API コールを記録し AWS CloudTrail、ログファイルを S3 バケットに配信するサービスである AWS WAF AWS を通じて、 へのすべての API コールを記録できるようになりました。CloudTrail ログを使用すると、セキュリティを分析したり、 AWS リソースの変更を追跡したりできます。また、このログは準拠に関する監査に役立ちます。 AWS WAF と CloudTrail を統合することで、 AWS WAF API に対してどのようなリクエストが行われたか、各リクエストが行われた送信元 IP アドレス、リクエストの実行者、リクエストの実行日時などを判断できます。 すでに を使用している場合は AWS CloudTrail、CloudTrail ログに AWS WAF API コールが表示されます。アカウントのために CloudTrail を有効にしていない場合は、AWS マネジメントコンソール から CloudTrail で有効にできます。CloudTrail を有効にしても追加料金はかかりませんが、Amazon S3 と Amazon SNS の標準の使用料金がかかります。	2016 年 4 月 28 日

変更	API バージョン	説明	リリース日
新機能	2015-08-24	AWS WAF を使用して、クロスサイトスクリプティングまたは XSS と呼ばれる悪意のあるスクリプトが含まれているように見えるウェブリクエストを許可、ブロック、またはカウントできるようになりました。攻撃者は、ウェブアプリケーションの脆弱性を悪用するために、悪意のあるスクリプトをウェブリクエストに挿入することがあります。詳細については、「クロスサイトスクリプティング攻撃ルールステートメント」を参照してください。	2016 年 3 月 29 日
新機能	2015-08-24	このリリースでは、 に次の機能 AWS WAF が追加されました。 • クエリ文字列や URIs など、リクエストの指定された部分の長さに基づいてウェブリクエストを許可、ブロック、またはカウント AWS WAF するように を設定できます。詳細については、「サイズ制約ルールステートメント」を参照してください。 • リクエスト本文の内容に基づいてウェブリクエストを許可、ブロック、またはカウント AWS WAF するように を設定できます。これは、HTTP リクエストボディとしてウェブサーバーに送信する追加のデータ (フォームからのデータなど) を含むリクエストの部分です。この機能は、文字列一致条件、SQL インジェクション一致条件、上記の新しいサイズ制約条件に適用されます。詳細については、「でのルールステートメント設定の調整 AWS WAF」を参照してください。	2016 年 1 月 27 日
新機能	2015-08-24	AWS WAF コンソールを使用して、ウェブ ACL を関連付ける CloudFront ディストリビューションを選択できるようになりました。詳細については、「ウェブ ACL と CloudFront ディストリビューションの関連付けまたは関連付け解除」を参照してください。	2015 年 11 月 16 日

変更	API バージョン	説明	リリース日
初回リリース	2015-08-24	これは「AWS WAF デベロッパーガイド」の初回リリースです。	2015 年 10 月 6 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。