



ユーザーガイド

AWS アカウント管理



AWS アカウント管理: ユーザーガイド

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 Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

とは AWS アカウント	1
の機能 AWS アカウント	3
初めての AWS ユーザーですか?	3
サポートとフィードバック	4
その他の AWS リソース	4
サインアップオプションを比較する	5
のサインアップ AWS のサービス でサポート AWS (新規)	5
AWS のサービス 新しい AWS エクスペリエンスの無料利用枠に含まれる	6
AWS のサービス 新しい AWS エクスペリエンスの有料プランに含まれる	11
AWS のサービス は新しい AWS エクスペリエンスではサポートされていません	12
へのサインアップ方法の選択に関する考慮事項 AWS	17
サインアップオプションの機能を比較する	17
アクセス管理を比較する	19
の管理 AWS アカウント	21
にサインアップする AWS (新規)	24
にサインアップ (AWS 新規) を使用してサインアップする	26
次の手順	27
AWS 設定を使用する	28
AI コーディングツールを接続する	29
コーディングツールをプロジェクトに接続する際の考慮事項	29
AI コーディングツールをプロジェクトに接続する	30
複数のプロジェクトを操作する	31
AWS プロジェクト所有者の アクション	33
パスワードを更新する	34
多要素認証 (MFA) の管理	35
重要ポイント	35
新しい AWS エクスペリエンスで利用できる MFA タイプ	36
MFA デバイスの登録	38
セキュリティキーを MFA デバイスとして登録する	39
MFA デバイスの名前を変更する	40
MFA デバイスの削除	40
すべてのセッションを削除する	41
名前またはニックネームを管理する	41
E メールアドレスを変更する	42

連絡先情報を編集する	43
サービス改善のためにコンテンツの使用をオプトアウトする	44
AWS Builder ID データをリクエストする	45
プロジェクトの作成	46
プロジェクトの作成に関する考慮事項	46
プロジェクトを作成する	47
AWS リージョン プロジェクトの	47
プロジェクト AWS リージョン 用に選択した を検索する	48
米国東部 (オハイオ) (us-east-2) でリージョンリソースがプロビジョニングされている 国	49
アジアパシフィック (シドニー) (ap-southeast-2) でリージョンリソースがプロビジョニ ングされている国	52
欧州 (ストックホルム) でリージョンリソースがプロビジョニングされている国 (eu- north-1)	55
組織の管理ポリシー	62
プロジェクトのサービスコントロールポリシー	62
プロジェクトの無料利用枠のサービスコントロールポリシー	84
プロジェクトの有料プランのサービスコントロールポリシー	95
プロジェクトのリソースコントロールポリシー	106
プロジェクトを切り替える	109
からアクティブなセッションのプロジェクトを切り替える AWS マネジメントコンソール .	109
AWS 設定でプロジェクトを切り替える	109
からプロジェクトを切り替える AWS マネジメントコンソール	110
チームメンバーを招待する	110
チームメンバーの考慮事項	110
チームメンバーが AWS リソースにアクセスする方法	112
チームメンバーを招待する	112
チームメンバーをプロジェクトに招待する	113
プロジェクトからチームメンバーを削除する	114
チームメンバーを削除する	114
招待を取り消す	115
招待を再送信する	115
アカウントのアップグレード	116
アカウントのアップグレードに関する考慮事項	116
アカウントのアップグレード	117
使用制限を作成する	118

支出制限とは	118
支出制限を設定する	118
通知	119
オプションの早期コストコントロールを使用して支出制限設定をカスタマイズする	119
制限に達したらどうなるか	121
その他の重要な注意事項	121
AWS 設定で使用制限を作成する	121
支出制限を更新する	122
AWS 設定で使用制限を更新する	122
使用制限を削除する	123
AWS 設定で使用制限を削除する	123
無料利用枠	123
無料利用枠の使用状況の追跡	124
追加のクレジットの獲得	126
AWS 設定で請求情報を表示する	126
プロジェクトごとにコストを表示するには	127
AWS 設定で請求履歴を表示する	127
支払い方法を管理する	128
AWS 設定で支払いを行う	128
AWS 設定で希望通貨を変更する	129
AWS 設定で税登録を管理する	130
納税者番号の更新と削除	130
米国の免税を管理する	131
クレジットの表示と引き換え	131
インドでのアカウントの管理	132
India で AWS (新規) AWS にサインアップする	133
顧客検証情報の管理	135
India の請求を設定する	138
Permanent Account Number を追加または編集する	138
複数の Permanent Account Number を編集する	139
複数の Goods and Service Tax 番号を編集する	139
税金請求書を表示する	139
AWS インドとの間で登録販売者を変更する	140
アクセス AWS サポート	142
プロジェクトサポート	142
Technical support (技術サポート)	143

すべてのプロジェクトと組織が閉鎖された場合のサポート	143
Business Support+ トライアルを開始する	143
プロジェクトをモニタリングする	144
AWS CloudTrail を使用してプロジェクトをモニタリングする	144
CloudTrail を使用してプロジェクトを変更したユーザーを確認する	145
プロジェクトを閉じる	148
プロジェクトを閉じる前に知っておくべきこと	148
プロジェクトを閉じるには	149
閉鎖後期間	149
プロジェクトを再開する	149
高度な機能をアクティブ化する	150
高度な機能をアクティブ化するとどうなるか	150
高度な機能をアクティブ化した後のプロジェクトアカウント	152
高度な機能をアクティブ化した後、AWS 設定はどのように変わりますか?	153
高度な機能をアクティブ化した後も、AWS 設定でプロジェクトを作成できますか?	154
高度な機能をアクティブ化するための準備方法	155
高度な機能をアクティブ化する方法	155
高度な機能をアクティブ化した後	156
ルートユーザーのパスワードを設定する	157
ワークフォースメンバーを管理する	158
ID ソースを変更する	160
組織ポリシーを削除する	161
AWS 設定でアカウントを閉じる	162
管理アカウントを閉鎖する前に知っておくべきこと	163
プロジェクトを閉じる	163
管理アカウントを閉じる	164
AWS ビルダー ID を削除する	164
にサインアップする AWS (アドバンスド)	166
ステップ 1: アカウントを作成する	167
ステップ 2: (推奨) をインストールする AWS CLI	169
ステップ 3: (推奨) AWS MCP サーバーを設定する	169
関連 AWS サービス	170
ルートユーザーの使用	171
アカウントへのアクセス	172
ガバナンス構造の計画	173
複数の を使用する利点 AWS アカウント	174

使用するタイミング AWS Organizations	175
使用するタイミング AWS Control Tower	181
API 操作モードについて	182
アカウントの設定	186
アカウントエイリアスの作成または更新	186
アカウント AWS リージョン で を有効または無効にする	187
の請求を更新する AWS アカウント	198
ルートユーザーの E メールと の更新	199
ルートユーザーのパスワードの更新	204
AWS アカウント 名前を更新する	205
の代替連絡先を更新する AWS アカウント	210
のプライマリ連絡先を更新する AWS アカウント	218
アカウント ID の表示	229
アカウントのトラブルシューティング	235
アカウント作成の問題	235
アカウント閉鎖の問題	236
その他の問題	238
インドでのアカウントの管理	239
India AWS アカウント で を作成する AWS	240
顧客検証情報の管理	242
アカウントの閉鎖	247
アカウントを閉鎖する前の確認事項	248
アカウントの閉鎖方法	250
アカウントの閉鎖後に予想されること	253
アカウントを再開する	254
アカウントを再開する前に知っておくべきこと	254
アカウントを再開する方法	255
アカウントを再開した後の予定	256
再開後にアカウントを使用する準備をする	256
リージョンの可用性	256
アカウントの保護	257
データ保護	258
AWS PrivateLink	259
エンドポイントを作成する	259
Amazon VPC エンドポイントポリシー	260
エンドポイントポリシー	260

Identity and Access Management	261
オーディエンス	261
アイデンティティを使用した認証	262
ポリシーを使用したアクセスの管理	263
AWS アカウント管理と IAM	265
アイデンティティベースのポリシーの例	273
アイデンティティベースのポリシーを使用する	277
トラブルシューティング	280
AWS マネージドポリシー	282
AWSAccountManagementReadOnlyAccess	283
AWSAccountManagementFullAccess	284
ポリシーの更新	285
コンプライアンス検証	285
耐障害性	286
インフラストラクチャセキュリティ	287
アカウントのモニタリング	288
CloudTrail ログ	288
CloudTrail でのアカウント管理情報	289
アカウント管理のログエントリについて	290
EventBridge によるアカウント管理イベントのモニタリング	293
アカウント管理イベント	294
クォータ	296
ドキュメント履歴	299
.....	ccci

とは AWS アカウント

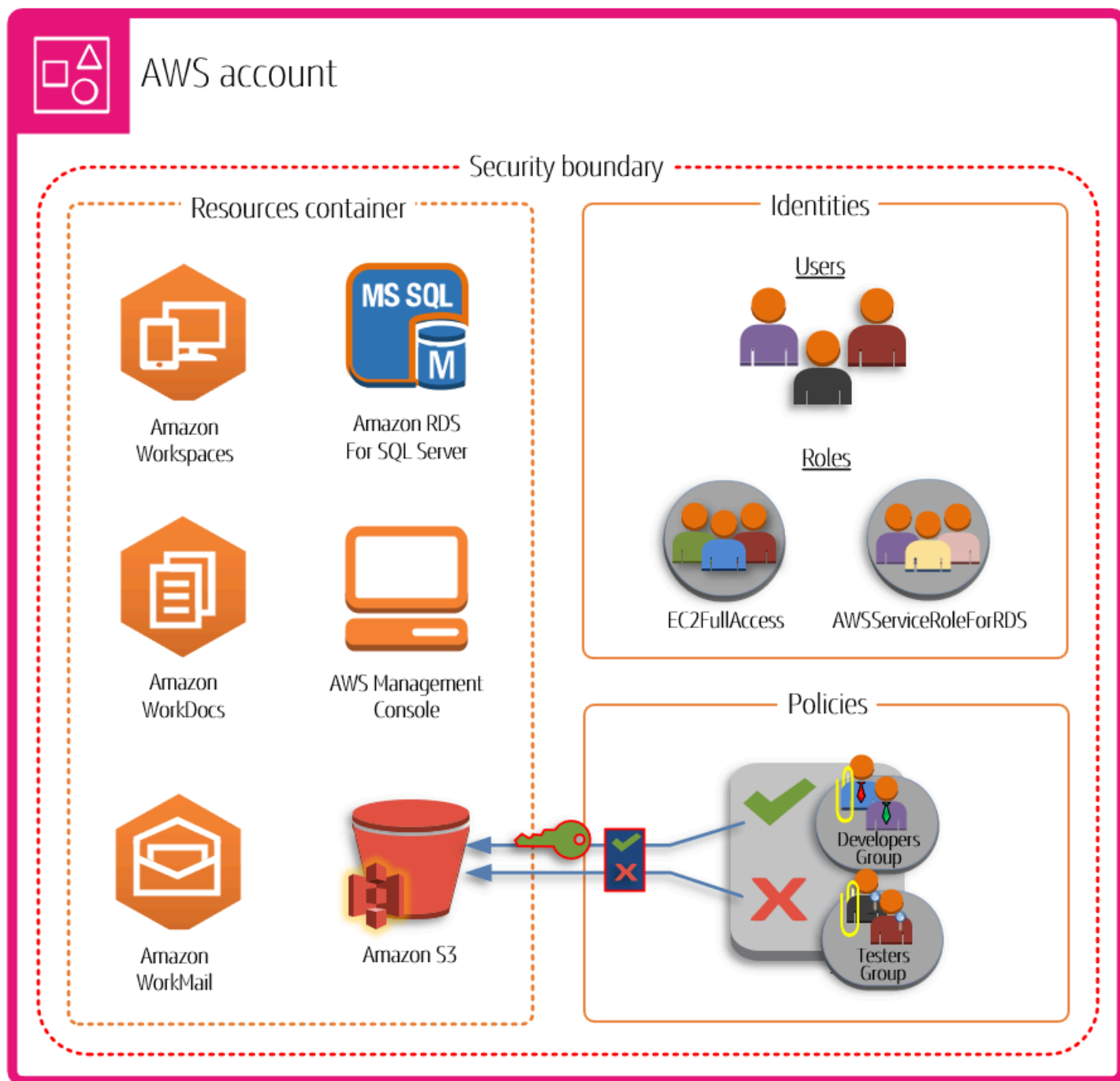
は、お客様が確立した正式なビジネス関係 AWS アカウント を表します AWS。で AWS リソースを作成および管理し AWS アカウント、アカウントはアクセスと請求のための ID 管理機能を提供します。それぞれに一意の ID AWS アカウント があり、他の ID と区別されます AWS アカウント。

にサインアップするときは AWS、サインアップ for AWS (新規) とサインアップ for AWS (詳細) を選択できます。選択した内容に応じて、AWS アカウント または プロジェクトにアクセスできます。プロジェクトには、AWS アカウント と他の共同作業者と共有するための設定が含まれています。詳細については、「[サインアップオプションを比較する](#)」を参照してください。

クラウドリソースとデータは、AWS アカウントに格納されています。アカウントは Identity and access management の分離境界として機能します。2 つのアカウント間でリソースとデータを共有する必要がある場合は、このアクセスを明示的に許可する必要があります。デフォルトでは、アカウント間のアクセスは許可されていません。例えば、本番環境および非本番環境のリソースとデータを格納するために異なるアカウントを指定する場合、デフォルトではこれらの環境間でのアクセスは許可されません。

AWS アカウント は、AWS サービスへのアクセスの基本的な部分でもあります。次の図に示すように、AWS アカウント には 2 つの主要な関数があります。

- リソースコンテナ – AWS アカウント は、AWS 顧客として作成するすべての AWS リソースの基本的なコンテナです。例えば、Amazon Simple Storage Service (Amazon S3) バケット、Amazon Relational Database Service (Amazon RDS) データベース、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスはすべてリソースです。すべてのリソースは、リソースを含む、または所有しているアカウントのアカウント ID を含む Amazon リソースネーム (ARN) によって一意に識別されます。
- セキュリティ境界 – AWS アカウント は、AWS リソースの基本的なセキュリティ境界でもあります。アカウントで作成したリソースは、そのアカウントに対する認証情報を持つユーザーが使用できます。アカウントで作成できる主要なリソースの 1 つに、ユーザーやロールなどの ID があります。ID には、AWS へのサインイン (認証) に使用できる認証情報があります。また、ID には、ユーザーがアカウント内のリソースで何を実行できるか (認可) を指定するアクセス許可ポリシーもあります。



複数の を使用すること AWS アカウント は、環境をスケーリングするためのベストプラクティスです。これは、コストの自然な請求境界を提供し、セキュリティのためにリソースを分離し、新しいビジネスプロセスに適応できるだけでなく、個人やチームに柔軟性を与えるためです。詳細については、「[複数の を使用する利点 AWS アカウント](#)」を参照してください。

の機能 AWS アカウント

AWS アカウント には、次のコア機能が含まれています。

- **コストのモニタリングと制御** – アカウントは、AWS コストを割り当てるデフォルトの手段です。このため、異なるビジネスユニットやワークロードのグループごとに異なるアカウントを使用することで、クラウド支出をより簡単に追跡、制御、予測、予算編成、報告できるようになります。アカウントレベルでのコストレポートに加えて、には、AWS Organizations ある時点で を使用することを選択した場合に、アカウント全体のコストを統合してレポートするためのサポート AWS も組み込まれています。また、AWS Service Quotas を使用して、AWS コストに劇的な影響を与える可能性のある AWS リソースの予期しない過剰なプロビジョニングや悪意のあるアクションから保護することもできます。
- **分離単位** – AWS アカウント は、AWS リソースの自律性と分離を実現するのに役立つリソースのセキュリティ、アクセス、請求の境界を提供します。設計上、アカウント内でプロビジョニングされたすべてのリソースは、独自の AWS 環境内であっても、他のアカウントでプロビジョニングされたリソースから論理的に分離されます。この分離境界により、アプリケーション関連の問題、設定ミス、または悪意のあるアクションのリスクを制限する方法が提供されます。1 つのアカウント内で問題が発生した場合に、他のアカウントに含まれるワークロードへの影響を軽減または排除することができます。
- **ビジネスワークロードのミラーリング** – 複数のアカウントを使用して、共通のビジネス目的を持つワークロードを個別のアカウントにグループ化します。その結果、所有権と意思決定がそれらのアカウントに沿ったものになり、他のアカウントのワークロードをセキュリティ保護および管理する方法との依存関係や競合を回避できます。全体的なビジネスモデルに応じて、異なるアカウントで個別のビジネスユニットや子会社を分離することを選択できます。このアプローチにより、時間の経過に伴ってそれらのユニットを売却することも容易になる可能性があります。

初めての AWS ユーザーですか？

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

を初めて使用する場合 AWS、最初のステップはサインアップすることです AWS。アカウント設定を完全に制御 AWS アカウント できると、HIPAA や FedRAMP などの規制対象のワークロードに

必要なコンテンツが保存されている を作成するか、事前設定されたデフォルトを使用して を作成できます AWS アカウント 。どのサインアップが適切かについては、「」を参照してください [サインアップオプションを比較する](#)。

初期設定を完全に制御できる新しいアカウントを設定する手順については、step-by-step 「」を参照してください [にサインアップする AWS \(アドバンスド\)](#)。

が事前設定されたデフォルトを持つアカウント AWS を作成する新しいアカウントを設定する手順 step-by-step については、「」を参照してください [にサインアップする AWS \(新規\)](#)。

AWS アカウント管理のサポート

[AWS アカウント管理サポートフォーラム](#)を使用して、フィードバックや質問を投稿できます。AWS フォーラムの一般的な情報については、「」を参照してください [AWS re:Post](#)。

探している回答が見つからない場合は AWS re:Post、 を使用してアカウントまたは請求関連のサポートケースを作成できます AWS マネジメントコンソール。詳細については、「[Example: Create a support case for account and billing](#)」を参照してください。

その他の AWS リソース

- [AWS トレーニングとコース](#) – AWS スキルを磨き、実践的な経験を積むのに役立つ、ロールベースのコースや専門コース、セルフペースラボへのリンク。
- [AWS デベロッパーツール](#) – 革新的なアプリケーションの構築に役立つドキュメント、コード例、リリースノート、その他の情報を提供するデベロッパーツールとリソースへのリンク AWS。
- [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、技術上のよくある質問、サービスヘルスステータス、AWS Trusted Advisor などの便利なリソースへのリンクも含まれています。
- [AWS サポート](#) – AWS クラウドでのアプリケーションの構築と実行に役立つ one-on-one の高速応答サポートチャネルである サポート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 請求、アカウント、イベント、不正使用、その他の問題に関するお問い合わせの中心的な連絡先です。
- [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。

サインアップオプションを比較する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

にサインアップすると AWS、世界で最も包括的で広く採用されているクラウドが解放されます。当社では、最も広範なグローバルインフラストラクチャで、業界をリードするセキュリティ、信頼性、パフォーマンスを備えた、革新的なクラウドおよび AI の機能と専門知識を最大限提供しています。

サインアップするには 2 つの方法があります AWS。アカウント設定とコンテンツの保存場所を完全に制御する場合、または HIPAA、FedRAMP などの規制対象のワークロードがある場合は、[を使用しますにサインアップする AWS \(アドバンスド\)](#)。新規ユーザーで、既に所有しているログインを使用して [にサインイン AWS](#) し、[の選択でデフォルトが AWS 事前設定された環境を作成する場合は AWS リージョン](#)、[を使用しますにサインアップする AWS \(新規\)](#)。

のサインアップ AWS のサービス でサポート AWS (新規)

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

にサインアップ AWS (新規) を使用すると、無料利用枠にアクセスできます。無料利用枠は、一部の AWS サービスへのアクセスを提供します。アカウントを有料プランにアップグレードして、追加の AWS サービスや機能にアクセスできます。アカウントをアップグレードする方法については、「[」を参照してくださいAWS 設定でアカウントをアップグレードする。](#)

すべての AWS サービスが AWS (新規) にサインアップできるわけではありません。サービスが次のいずれかのリストにリストされていない場合、またはサポートされていない機能がある場合は、[にサインアップする AWS \(アドバンスド\)](#)または [を使用してアカウントを作成する必要があります高度な AWS 機能をアクティブ化する。](#)

AWS のサービス 新しい AWS エクスペリエンスの無料利用枠に含まれる

以下の AWS サービスは、AWS (新規) のサインアップの無料利用枠に含まれています。マルチリージョンまたはクロスリージョン機能は、どのサービスでもサポートされていません。詳細については、「[AWS リージョン プロジェクトの](#)」を参照してください。

- Amazon API Gateway
- Amazon Athena
- Amazon AppFlow
- AWS App2Container
- Amazon Augmented AI
- Amazon Bedrock
- Amazon Bedrock エージェントコア
- Amazon CloudFront
 - Lambda@Edge はサポートされていません。
- Amazon CloudWatch
- Amazon CloudWatch Logs
- Amazon CodeGuru Profiler
- Amazon Cognito
- Amazon Cognito Sync
- Amazon DynamoDB
- Amazon DataZone
- Amazon Elastic Container Registry (ECR)
- EC2 イメージビルダー
- Amazon EKS Anywhere
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
 - Purchase Capacity Block と Purchase Capacity Block Extension はサポートされていません。
- Amazon Elastic Container Registry Public
- Amazon Elastic Container Service
- Amazon Elastic Kubernetes Service

- Amazon Elastic File System
- Amazon ElastiCache
- Amazon EventBridge
- Amazon Lex
- Amazon Lightsail
- Amazon Location Service
- Amazon Managed Service for Prometheus
- Amazon Managed Workflows for Apache Airflow
- Amazon MQ
- Amazon OpenSearch Service
- Amazon Polly
- Amazon Quick
 - Amazon Quick Free または Quick Plus のみがサポートされています。詳細については、[「Amazon Quick の料金」](#)を参照してください。
- Amazon Rekognition
- Amazon Relational Database Service
- Amazon Route 53
- Amazon SageMaker
- Amazon SageMaker AI
- Amazon SageMaker Unified Studio
- Amazon Simple Email Service
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Simple Storage Service
 - Amazon S3 Access Grants はサポートされていません。
- Amazon Simple Workflow Service
- Amazon Verified Permissions
- Amazon Virtual Private Cloud
- Amazon Aurora
- Amazon Aurora DSQL

- AWS Amplify
- AWS AppConfig
- AWS AppSync
- Application Auto Scaling
- AWS Transform MGN
- AWS Artifact
 - (HIPAA) AWS Business Associate Addendum、(HIPAA) AWS Organizations Business Associate Addendum、AWS SEC Rule 17a-4 Addendum、および AWS SEC Rule 18a-6 Addendum はサポートされていません。
- AWS B2B Data Interchange
- AWS Backint agent
- AWS Backup
- AWS Batch
- AWS Billing and Cost Management
 - AWS 設定を使用して、請求の設定、コストを制御するための支出制限の作成、請求書の取得と支払いを行います。Billing and Cost Management を使用して、予算の作成、分析、コストの最適化を行います。詳細については、[「新しい AWS エクスペリエンスで請求情報とコスト管理コンソールを使用する」](#)を参照してください。
- AWS Budgets
- AWS Certificate Manager
 - [AWS Certificate Manager のエクスポート可能なパブリック証明書](#)はサポートされていません。
- AWS クラウドコントロール API
- AWS Cloud Map
- AWS Cloud9
- AWS CloudFormation
- AWS CloudShell
- AWS CloudTrail
- AWS CodeArtifact
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline

- AWS Compute Optimizer
- AWS Config
- AWS Console Mobile Application
- AWS Cost Explorer
- AWS Data Pipeline
- AWS データ転送
- AWS DataSync
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS End User Messaging Social
- AWS Entity Resolution
- AWS Glue
- AWS Health
- AWS Identity and Access Management
- AWS IoT
 - AWS Greengrass はサポートされていません。
- AWS IoT Device Defender
- AWS IoT デバイス管理
- AWS IoT SiteWise
- AWS IoT TwinMaker
- AWS Key Management Service
- AWS Lake Formation
- AWS Lambda
 - Lambda@Edge はサポートされていません。
- AWS Launch Wizard
- AWS License Manager
- AWS マネジメントコンソール
- AWS Marketplace
 - Bedrock と Free のみ。
- AWS Network Manager

- AWS Payment Cryptography
- AWS PrivateLink
- AWS Resource Access Manager (RAM)
- AWS Resource Explorer
- AWS Resource Groups
- Route 53 Amazon Application Recovery Controller (ARC)
- AWS SDKsとツール
- AWS Secrets Manager
- AWS Security Token Service
- AWS Serverless Application Repository
- サービスクォータ
- AWS Signer
- AWS Step Functions
- AWS サポート
- AWS Systems Manager
- AWS Systems Manager for SAP
- AWS User Notifications
 - ユーザー設定通知およびマネージド通知設定オペレーションはサポートされていません。詳細については、[AWS「ユーザー通知とは」を参照してください。](#)
- AWS WAF
 - AWS Shield はサポートされていません。
- AWS Well-Architected Tool
- AWS X-Ray
- AWS CodeBuild
- Elastic Load Balancing
- AWS SQL Workbench
- Amazon OpenSearch Service Serverless
- Amazon Timestream

無料利用枠サービスへのアクセスを制御するポリシーについては、「」を参照してください[プロジェクトの無料利用枠のサービスコントロールポリシー](#)。

AWS のサービス 新しい AWS エクスペリエンスの有料プランに含まれる

有料プランをお持ちの場合は、次の のサービスを AWS (新規) にサインアップできます。詳細については、「[AWS 設定でアカウントをアップグレードする](#)」を参照してください。マルチリージョンまたはクロスリージョン機能は、どのサービスでもサポートされていません。詳細については、「[AWS リージョン プロジェクトの](#)」を参照してください。

- Amazon DevOps Guru
- Amazon DocumentDB (MongoDB 互換性)
- Amazon EMR
- Amazon Forecast
- Amazon Glacier
- Amazon Kinesis
- Amazon Kinesis Data Streams
- Amazon Data Firehose
- Amazon Kinesis Video Streams
- Amazon Managed Blockchain
- Amazon Managed Streaming for Apache Kafka
- Amazon MemoryDB
- Amazon Neptune
- Amazon Personalize
- Amazon Redshift
- S3 Glacier Deep Archive
- Amazon Textract
- Amazon Transcribe
- Amazon Translate
- AWS AppFabric
- AWS Data Exchange
- AWS End User Messaging SMS
- AWS Fault Injection Service
- AWS Firewall Manager
- AWS Network Firewall

- AWS セキュリティエージェント
- AWS Storage Gateway
- DevOps エージェント

有料プランサービスへのアクセスを制御するポリシーについては、「」を参照してください[プロジェクトの有料プランのサービスコントロールポリシー](#)。

AWS のサービス は新しい AWS エクスペリエンスではサポートされていません

以下の AWS サービスは、お客様が でない限り、新しい AWS エクスペリエンスではサポートされていません[高度な AWS 機能をアクティブ化する](#)。これらの AWS サービスは、新しい開発者や小規模なチームには必要ありません。これらのサービスの一部は、アカウントで自動的に有効になり、によって管理されます AWS。詳細については、「[サインアップオプションの機能を比較する](#)」を参照してください。

- Alexa for Business
- Alexa Top Sites
- Alexa Web Information Service
- Amazon Braket
- Amazon Chime
- Amazon Chime Business AMCS LLC が販売するサービスを呼び出す
- Amazon Chime コールミー
- Amazon Chime Call Me AMCS LLC が販売するサービス
- Amazon Chime Dial AMCS LLC が販売するサービス
- Amazon Chime ダイヤルイン
- Amazon Chime の機能
- Amazon Chime SDK
- Amazon Chime サービス
- Amazon Chime SMS
- Amazon Chime Voice Connector AMCS LLC が販売するサービス
- Amazon Cloud Directory
- Amazon CloudSearch

- Amazon CodeWhisperer
- Amazon Connect Customer
- Amazon Connect Customer Customer Profiles
- Amazon Connect Customer Voice ID
- AWS Deadline Cloud
- Amazon Detective
- Amazon Elastic Inference
- Amazon Elastic Transcoder
- Amazon FinSpace
- Amazon Flexible フリート
- Amazon Fraud Detector
- Amazon FSx
- Amazon GameLift サーバー
- Amazon GameLift Streams
- Amazon GameSparks
- Amazon GuardDuty
- AWS HealthOmics
- Amazon Inspector Classic
- Amazon Interactive Video Service
- Amazon IVS Chat
- Amazon Kendra
- Amazon Keyspaces (Apache Cassandra 向け)
- Kiro
- Amazon Macie
- Amazon Managed Grafana
- Amazon Mechanical Turk
- Amazon Mechanical Turk ワーカー報酬
- Amazon Mobile Analytics
- Amazon Monitron
- Amazon Nimble Studio

- Amazon OpenSearch Service Ingestion Service
- Amazon Q
- Amazon Q Business
- Amazon Q Developer
- Amazon Quantum Ledger Database (Amazon QLDB)
- Amazon S3 on Outposts
- Amazon SageMaker Ground Truth
- Amazon Security Lake
- Amazon Sumerian
- Amazon WorkDocs
- Amazon WorkSpaces
- Amazon WorkSpaces インスタンス
- Amazon WorkSpaces アプリケーション (Amazon WorkSpaces アプリケーション)
- Amazon WorkSpaces Thin Client
- Amazon WorkSpaces Web
- Amazon WorkLink
- Amazon WorkMail
- AWS Application Cost Profiler
- AWS Clean Rooms
- AWS App Studio
- AWS Application Discovery Service
- AWS Audit Manager
- AWS Billing Conductor
- AWS CloudHSM
- AWS Client VPN
- AWS クラウド WAN
- AWS Control Tower
- AWS データベース移行サービス
- AWS DeepRacer
- AWS Device Farm

- AWS Direct Connect
- AWS Elastic Disaster Recovery
- AWS Elemental Live
- AWS Elemental MediaConnect
- AWS Elemental MediaConvert
- AWS Elemental MediaLive
- AWS Elemental MediaPackage
- AWS Elemental MediaStore
- AWS Elemental MediaTailor
- AWS Global Accelerator
- AWS Ground Station
- AWS HealthImaging
- AWS IAM アイデンティティセンター
- AWS Identity and Access Management Access Analyzer
- AWS 相互接続
- AWS IoT イベント
- AWS IoT FleetWise
- AWS IoT RoboRunner
- AWS Mainframe Modernization
- AWS Migration Hub
- AWS Migration Hub Refactor Spaces
- AWS Modular Data Center
- AWS OpsWorks
- AWS Organizations
- AWS Outposts
- AWS Parallel Computing Service
- AWS Partner Network
- AWS 料金見積りツール
- AWS Private Certificate Authority
- AWS Proton

- AWS re:Post Private
- AWS Resilience Hub
- AWS RoboMaker
- AWS RTB ファブリック
- AWS Security Hub
- AWS Security Incident Response
- AWS Service Catalog
- AWS Shield
- AWS SimSpace Weaver
- AWS Snowball
- AWS Supply Chain
- AWS Telco Network Builder
- AWS Transform
- AWS Transfer Family
- AWS Transit Gateway
- AWS Trusted Advisor
- AWS Verified Access
- Site-to-Site VPN
- Amazon VPC Lattice
- AWS Wickr
- Amazon CodeCatalyst
- Amazon Comprehend Medical
- Conferencing Telecommunications (AMCS LLC が販売するサービス)
- コンタクトセンター通信 (AMCS LLC が販売するサービス)
- コンタクトセンターの通信韓国
- コンタクトセンターの通信南アフリカ
- DynamoDB Accelerator
- Amazon Elastic VMware サービス
- Oracle Database@AWS
- Red Hat OpenShift Service on AWS

- AWS App Runner

へのサインアップ方法の選択に関する考慮事項 AWS

サインアップ方法を選択する前に、次の点を考慮してください。必要に応じて、アカウントのすべての AWS 機能をアクティブ化できます。

- HIPAA や FedRAMP を含む規制対象ワークロードなど、特定の製品要件がある場合は、新しい AWS エクスペリエンスを使用しないでください。
- コンテンツは、連絡先情報に基づいて選択された指定されたリージョンに保存されます。
- 新しい AWS エクスペリエンスにより、AWS アクセス許可を作成せずに構築を簡単に開始できます。ユーザーまたはロールベースのアクセス許可をきめ細かく制御する必要がある場合は、にサインアップ AWS (新規) を使用しないでください。
- ネットワーク請求とも呼ばれる AWS、によって設定されたアカウント固有の支払い設定が必要な場合は、にサインアップ AWS (新規) を使用しないでください。
- すべての AWS サービスにアクセスする必要がある場合は、「サインアップ for AWS (new)」を使用しないでください。詳細については、「[のサインアップ AWS のサービス でサポート AWS \(新規\)](#)」を参照してください。

サインアップオプションの機能を比較する

次の表は、Sign up for AWS (new) または Sign up for AWS (advanced) でサポートされている AWS 幅広い要件を比較したものです。特徴がこの表に記載されていない場合、またはで説明されていない場合は[アクセス管理を比較する](#)、その特徴を使用できます。サポートされていない機能が必要な場合は、アカウントの高度な機能をアクティブ化できます。詳細については、「[高度な AWS 機能をアクティブ化する](#)」を参照してください。

機能	にサインアップする AWS (新規)	にサインアップする AWS (アドバンスド)
AWS パートナーネットワークの参加	いいえ	はい
プロフェッショナルサービス契約を作成する	いいえ	はい
でエンタープライズ契約に登録する AWS	いいえ	はい

機能	にサインアップする AWS (新規)	にサインアップする AWS (アドバンスド)
AWS スキルビルダーチームのサブスクリプションを購入する	いいえ	はい
AWS トレーニングパートナーと連携する	いいえ	はい
AWS Activate から追加のクレジットを取得する	いいえ	はい
AWS Marketplace を使用する	いいえ	はい
AWS アカウントを HIPAA または SEC 準拠として指定する	いいえ	はい
特定の AWS リージョン を選択してリージョンリソースを作成する	いいえ。詳細については、「」を参照してください AWS リージョン プロジェクト の。	あり
オプトインリージョンにアクセスする	いいえ	はい
IAM Access Analyzer	いいえ	はい
サインインアクセスポリシー	いいえ	はい
アカウントの支出制限を作成する	あり	いいえ
Savings Plans	いいえ	はい
有料プランの Cost Optimization Hub への自動オプトイン	あり	いいえ
への自動オプトイン AWS Organizations	あり	いいえ
IAM Identity Center への自動オプトイン	あり	いいえ

機能	にサインアップする AWS (新規)	にサインアップする AWS (アドバンスド)
IAM ロールマネージャー に自動的にオプトインする	あり	いいえ
コンソールアカウントの色	いいえ	はい
AWS Console Mobile Application の使用	いいえ	はい
マルチセッションコンソールのサポートを無効にする	いいえ	はい。Builder ID を使用して再度サインインすると、マルチセッションのサポートが自動的に有効になります。

アクセス管理を比較する

新しい AWS エクスペリエンスを使用すると、は構築を開始するのに役立つ事前設定されたデフォルト AWS を作成します。AWS リソースはプロジェクトに整理されています。プロジェクトには AWS アカウント、プロジェクトアカウントと呼ばれる と、他の共同作業者と共有するための設定が含まれています。有料プランを使用する場合、プロジェクトには、使用制限と呼ばれる税引き前の月額コストを設定することもできます。所有しているすべてのプロジェクトが組織を構成し、AWS 設定で管理アカウントを通じて管理します。この組織は AWS Organization と同じですが、AWS はユーザーに代わってこの組織の側面を管理します。

AWS は、AWS 組織の次の要素を管理します。

- 組織の管理ポリシー。新しい AWS エクスペリエンスを使用すると、はリソースコントロールポリシー (RCPs) やサービスコントロールポリシー (SCPs) を含む組織管理ポリシー AWS を管理します。独自の を作成する場合は、「Sign up for AWS (advanced)」を使用します。
- ヒューマンアクセスロール。ヒューマンアクセスロールは、人間固有のアクセス許可を付与する任意のロールです。は、ユーザーとチームメンバーにプロジェクトへの管理者アクセス AWS を提供します。プロジェクト所有者は、チームメンバーを追加および削除できます。詳細については、「[チームメンバーを AWS 設定で共同作業に招待する](#)」を参照してください。ルートユーザーを作成しません。AWS Builder ID は、ルートユーザーの E メールアドレスではなくプロジェクトア

カウントを所有しており、高度な機能をアクティブ化しても変更されません。必要に応じて IAM ロールと IAM ユーザーを作成できますが、コンソールアクセスではなく、プログラムによるアクセスにのみ使用できます。

すべてのプロジェクトには、自信を持って簡単に構築できるマネージドセキュリティ実装があります。デフォルトでは、プロジェクト内のすべてのアプリケーションまたはコードは、同じプロジェクト内のすべての AWS リソースにアクセスできます。追加のアクセス設定を実行する必要はありません。

AWS 異なるプロジェクトのリソースは、特定のリソースのクロスプロジェクトアクセスを有効にしない限り、相互にアクセスできません。たとえば、あるプロジェクトで Lambda 関数を作成し、別のプロジェクトの API を使用して呼び出すことができます。これは、クロスアカウント統合と呼ばれます。詳細については、[「クロスアカウント Lambda 統合」](#)を参照してください。両方のプロジェクトが同じ管理アカウントによって所有されている限り、これはサポートされています。

デフォルトでは、プロジェクトはリソースへの外部アクセスを提供しません。パブリックアクセスを許可するように AWS リソースを設定する必要があります。以下を行うことができます。

- シンプルな静的ウェブサイトまたはファイルをホストするパブリック S3 バケットを作成します。Amazon S3 の詳細については、[Amazon S3 の開始方法](#)を参照してください。
- API Gateway API を作成して、アプリケーションのフロントドアとして機能します。詳細については、[「HTTP API の構築」](#)を参照してください。
- パブリック IP アドレスを使用して EC2 インスタンスを作成し、インスタンスとインターネット間の通信を許可します。詳細については、[「最初の EC2 インスタンスを起動する」](#)を参照してください。
- CloudFront デイストリビューションを作成して、.html、.css、.js、イメージファイルなどの静的および動的なウェブコンテンツをユーザーに配信します。詳細については、[CloudFront の開始方法](#)を参照してください。
- Lambda 関数 URL を作成して、Lambda 関数のシンプルで直接アクセス可能な HTTP エンドポイントを提供します。Lambda 関数に正しいアクセス許可があることを確認します。詳細については、[「関数 URL の作成」](#)および [「Lambda 関数 URLs」](#)を参照してください。
- これらのメカニズムまたは他の AWS メカニズムの組み合わせを使用します。

さらに、高度な機能をアクティブ化すると、リソースへの外部アクセスを提供するさらに多くのメカニズムにアクセスできます。

の管理 AWS アカウント

は、使用している のタイプ AWS アカウント に基づいて管理 AWS します。次の表は、各管理タスクのドキュメントの場所を示しています。

タスク	にサインアップする AWS (新規)	にサインアップする AWS (アドバンスド)
サインアップする	にサインアップする AWS (新規)	にサインアップする AWS (アドバンスド)
アカウントを作成する	AWS 設定でプロジェクトを作成する	にサインアップする AWS (アドバンスド)
アカウントの解約	AWS 設定でプロジェクトを閉じる	を閉じる AWS アカウント
パスワードを更新する	AWS 設定でパスワードを更新する	ルートユーザーのパスワードの更新
MFA デバイスを登録する	AWS 設定で多要素認証 (MFA) を管理する	ステップ 3: (推奨) AWS MCP サーバーを設定する
E メールを変更する	AWS 設定で E メールアドレスを変更する	ルートユーザーの E メールアドレスと の更新
名前を変更する	AWS 設定で名前またはニックネームを管理する	AWS アカウント 名前を更新する
連絡先情報の更新	AWS 設定で連絡先情報を編集する	のプライマリ連絡先を更新する AWS アカウント
代替連絡先の更新	該当しない	の代替連絡先を更新する AWS アカウント

タスク	にサインアップする AWS (新規)	にサインアップする AWS (アドバンスド)
請求の管理	AWS 設定で支払い方 法を管理する	の請求を更新する AWS アカウント
税金情報を管理する	AWS 設定で税登録を 管理する	支払いを管理する
を有効または無効にする AWS リージョン	該当なし。を変更することはできません AWS リージョン。	アカウント AWS リー ジョン で を有効また は無効にする
アカウント識別子を表示する	該当しない	AWS アカウント 識別 子の表示
アカウントエイリアスを作成する	該当しない	AWS アカウント エイ リアスを作成する
アカウントのアップグレード	AWS 設定でアカウン トをアップグレード する	無料利用枠プラン
使用制限を作成する	AWS 設定で使用制限 を作成する	該当しない
支出制限を更新する	AWS 設定で使用制限 を更新する	該当しない
使用制限を削除する	AWS 設定で使用制限 を削除する	該当しない
チームメンバーを招待する	チームメンバーを AWS 設定で共同作業 に招待する	IAM ID
プロジェクトを切り替える	プロジェクトを切り 替える	マルチセッションの サポート

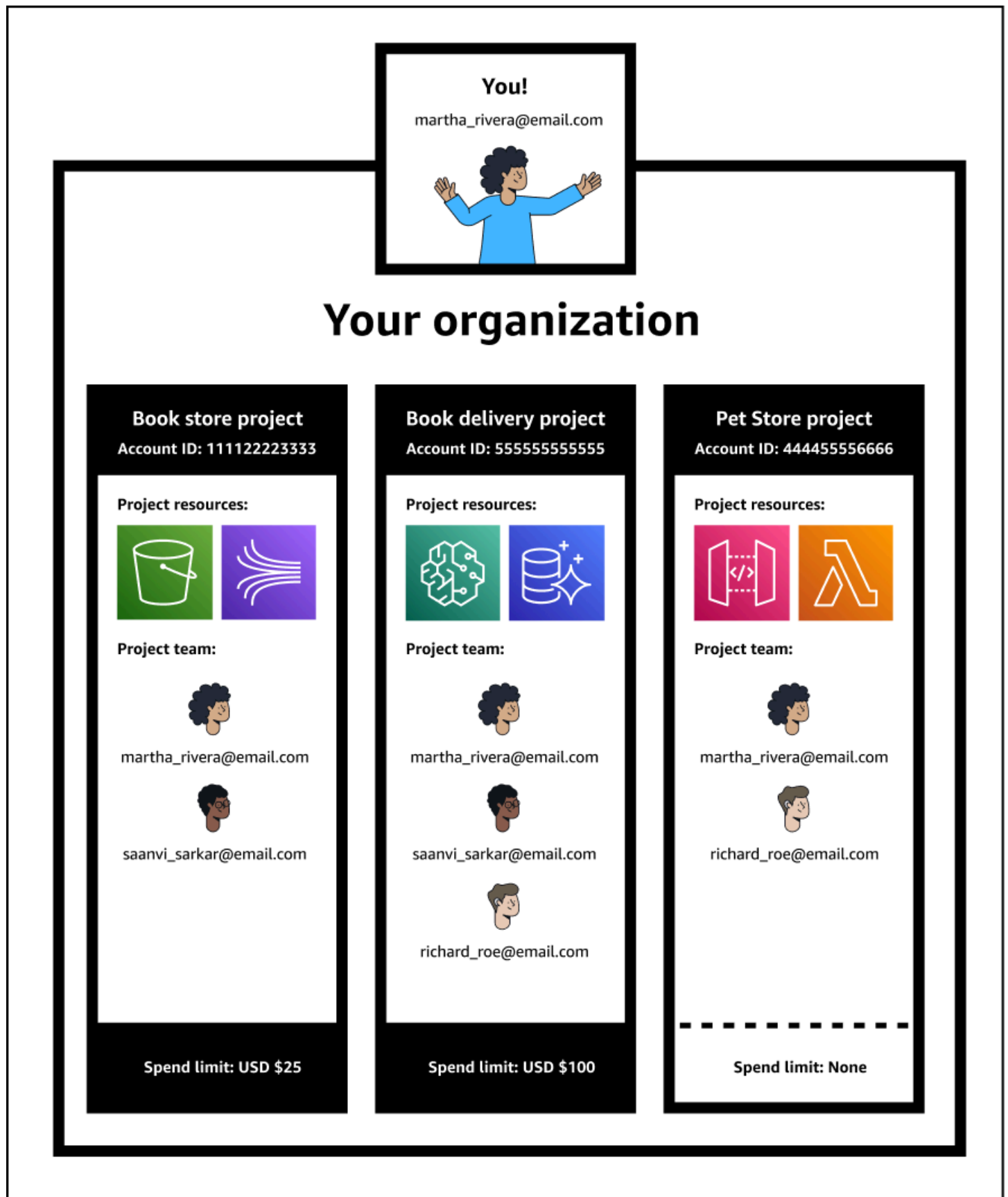
タスク	にサインアップする AWS (新規)	にサインアップする AWS (アドバンスド)
AI コーディングツールを接続する	AI コーディングツールを接続する	該当しない
すべてのセッションを削除する	AWS 設定ですべてのセッションを削除する	該当しない
AI データの使用をオプトアウトする	AWS 設定でサービス改善のためにコンテンツの使用をオプトアウトする	AI サービスのオプトアウトポリシー
データをリクエストする	AWS Builder ID データをリクエストする	データをリクエストする
AWS プロファイルを削除する	AWS 設定でアカウントを閉じる	を閉じる AWS アカウント
インドでのアカウントの管理	AWS 設定でインドのアカウントを管理する	インドでのアカウントの管理
管理者ユーザーの作成	該当しない	にサインアップする AWS (アドバンスド)
アカウントガバナンス構造を計画する	該当しない	AWS アカウント ガバナンス構造を計画する

にサインアップする AWS (新規)

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

Sign up for AWS (new) を使用する場合、Google や GitHub など、既に所有しているログインを使用して AWS リソースにアクセスできる事前設定 AWS 済みの環境を作成します。リソースはプロジェクトに整理されています。プロジェクトには、他の共同作業者と共有するための AWS アカウントと の設定が含まれています。有料プランを使用する場合、プロジェクトには、使用制限と呼ばれる税引き前の月額コストを設定することもできます。所有しているすべてのプロジェクトが組織を構成します。組織を管理し、プロジェクトにアクセスし、AWS 設定でチームメンバーを追加します。



サインアップ for AWS (新規) AWS を使用して にサインアップすると、 は AWS ビルダー ID アカウント AWS も作成します。アカウントは、ユーザーを個人として表す個人プロフィールです。E メールアドレス AWS ビルダー ID ごとに 1 つのみを持つことができます。を作成した AWS ビルダー ID が、 を作成していない場合は AWS アカウント、いくつかの設定が既に作成されている可能性があります。後で変更する必要があります。

へのサインアップ AWS (新規) の詳細については、次のドキュメントを参照してください。

- [サインアップオプションを比較する](#)
- [のサインアップ AWS のサービス でサポート AWS \(新規\)](#)

にサインアップ (AWS 新規) を使用してサインアップする

にサインアップすると AWS、支払い情報をリクエストすることがあります。当社の検証プロセスでは、お客様のアカウントを検証し、不正を防ぐために、1 USD (または同等のもの) を 3~5 日間保持します。有料プランにアップグレードするまで、料金は発生しません。支払い方法は、AWS 設定を使用していつでも管理したり、アカウントを閉鎖したりできます。さらに、 にサインアップすると AWS、 無料利用枠の対象外になる場合があります。その場合は、支払い情報を指定する必要があります。有料プランに配置されます。有料プランでは、予測可能で管理された予算内で運用するように支出制限を設定できます。

にサインアップ AWS する (新規) では、Google、GitHub、Apple、または Amazon をアカウントで使用できます。ブラウザで Google アカウントに既にサインインしている場合、そのアカウントはサインアップ時に使用されます AWS。

にサインアップするには AWS にサインアップする AWS (新規)

1. [AWSのサインアップ](#) ページを開きます。
2. E メールを入力するか、Google、Apple、GitHub、Amazon などのログインを選択します。
3. すでに所有しているログインを使用している場合は、プロバイダーのログインが表示されます。ログインすると、AWS サインアップするようにリダイレクトされます。
4. 名前を入力し、続行を選択します。

この名前は、プロジェクトへのアクセス権をチームメンバーに付与するときに、チームメンバーと共有されます。

5. 検証コードを入力して、ログインに関連付けられた E メールを確認します。E メールを確認したら、続行を選択します。

この E メールは、プロジェクトへのアクセス権をチームメンバーに付与すると、チームメンバーと共有されます。

6. アカウントの強力なパスワードを入力し、続行を選択します。

AWS では、パスワードが次の条件を満たしている必要があります。

- 8～128 文字で構成されていること。
- 英字の大文字、英字の小文字、数字、記号 (! @ # \$ % ^ & * () < > [] { } | _ + =) のうち、少なくとも 3 つの文字タイプを使用する必要があります。
- AWS アカウント 名前や E メールアドレスと同じにすることはできません。

7. 連絡先の詳細を入力し、続行を選択します。

8. AWS は、3 つのうちの 1 つに新しい名前 AWS リージョン で最初のプロジェクトをプロビジョニングします。詳細については、「[AWS リージョン プロジェクトの](#)」を参照してください。名前はいつでも変更できます。

これで、にアクセスできます AWS マネジメントコンソール。AWS 設定にアクセスするには、からプロジェクトを管理するを選択します AWS マネジメントコンソール。AWS 設定では、チームメンバーを招待したり、新しいプロジェクトを作成したり、請求やその他の設定を変更したりできます。

次の手順

にサインアップしたら AWS、AI コーディングツールを接続し、コラボレーションするチームメンバーを追加し、有料プランがある場合は、支出制限を作成できます。

- [AI コーディングツールを接続する](#)
- [チームメンバーを AWS 設定で共同作業に招待する](#)
- [AWS 設定で使用制限を作成する](#)

AWS 設定を使用する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

[AWS 設定](#)は、プロジェクトを管理してアクセスする場所です。AWS 設定は、サインアップ for AWS (新規) を使用してサインアップするときに使用できます。AWS 設定を使用して、以下を実行できます。

- 所有しているプロジェクトを作成してアクセスします。詳細については、「[AWS 設定でプロジェクトを作成する](#)」を参照してください。
- 共有されているプロジェクトにアクセスします。
- チームメンバーを招待してプロジェクトでコラボレーションします。詳細については、「[チームメンバーを AWS 設定で共同作業に招待する](#)」を参照してください。
- プロジェクトを切り替えます。詳細については、「[プロジェクトを切り替える](#)」を参照してください。
- 支払い方法を管理します。詳細については、「[AWS 設定で支払い方法を管理する](#)」を参照してください。
- 無料利用枠から有料プランにアップグレードします。詳細については、「[AWS 設定でアカウントをアップグレードする](#)」を参照してください。
- プロジェクトの支出制限を管理します。詳細については、「[AWS 設定で使用制限を作成する](#)」を参照してください。
- 請求情報を表示します。詳細については、「[AWS 設定で請求情報を表示する](#)」を参照してください。
- プロファイル情報を管理します。詳細については、[AWS 設定で名前またはニックネームを管理する](#)、[AWS 設定で E メールアドレスを変更する](#)、および [AWS 設定で連絡先情報を編集する](#) を参照してください。
- セキュリティ設定とサインイン設定を管理します。詳細については、「[AWS 設定でパスワードを更新する](#)」および「[AWS 設定で多要素認証 \(MFA\) を管理する](#)」を参照してください。

プロファイル情報またはセキュリティ設定を管理すると、AWS ビルダー ID ハブにリダイレクトされます。AWS ビルダー ID は、にサインアップ AWS (新規) を使用するときには作成されます。詳細については、「[とは AWS ビルダー ID](#)」を参照してください。

AI コーディングツールを接続する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

AI コーディングツールにプロジェクトへのアクセスを提供し、AWS MCP サーバー設定と厳選されたエージェントスキルのセットをバンドルする エージェントツールキットをインストールできます。これにより、AI コーディングツールがユーザーに代わって AWS リソースを作成および管理できます。

コーディングツールをプロジェクトに接続する際の考慮事項

- AI コーディングツールを、所有しているプロジェクトまたは共有されているプロジェクトに接続できます。
- AI コーディングツールまたはローカルエージェントが AWS リソースを作成する場合でも、その責任はお客様にあります。これには、[責任共有モデル](#)で定義されているリソースの適切なセキュリティと、無料プランで考慮されているか有料プランで請求されているかにかかわらず、これらのリソースから発生する可能性のある料金が含まれます。
- AI コーディングツールがプロジェクトでユーザーに代わって実行するアクションは、すべてユーザーの責任となります。
- エージェントが作成したリソースを表示するには、そのサービスのサービスコンソールに移動します。
- 生成する認証情報は AWS CLI、AWS Tools for PowerShell、および AWS SDKs で使用するものです。外部ツールはサポートされていない場合があります。リソースへのアクセスは 12 時間有効です。認証情報を更新するには、次のコマンドを使用します。

```
aws login --profile profile-name
```

profile-name を、初期設定時に選択したプロファイル名に置き換えます。コマンドはデフォルトのブラウザを自動的に開きます。ログインプロセスを完了するには、プロジェクト名を選択する必要があります。AWS は 90 日間認証情報を更新できます。90 日後、ブラウザウィンドウで再度アクセスを許可する必要があります。

AI コーディングツールをプロジェクトに接続する

各プロジェクトには、AI コーディングツールがユーザーに代わって AWS リソースを作成および管理するために使用できる独自の認証情報のセットがあります。

AWS マネジメントコンソール

AWS コンソールを使用して AI コーディングツールをプロジェクトに接続するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、アクセスするプロジェクトを選択します。
3. 右上のナビゲーションバーで、クラウドインフラストラクチャの作成と管理を選択します。
4. AI コーディングツールで AWS 認証情報を使用するを選択します。
5. エージェントプロンプトをコピーを選択し、コーディングエージェントに入力します。

これにより、AI コーディングエージェントとステアリングファイルを共有するプロンプトが作成されます。ステアリングファイルは、プロジェクト認証情報と AI コーディングエージェント間の接続 AWS を設定する からスクリプトにアクセスします。

プロジェクトのプロファイル名を入力します。このプロファイル名は、AI コーディングツールがリソースにアクセスする方法です。

Use your terminal

次のコマンドを実行して、セットアップ手順をダウンロードして実行します。

```
curl -fsSL https://github.com/aws/agent-toolkit-for-aws/blob/main/setup-instructions/setup.md
```

新しい AWS エクスペリエンスを使用すると、エージェントは AWS MCP サーバーをインストールし、プロジェクトで利用できるエージェントスキルにアクセスできます。また、このエクスペリエ

ンスに合わせて調整されたガイダンスを含むルールファイルも提供されます。ルールファイルでは、エージェントに提供するヘルプのレベルを定義することもできます。サポートされているヘルプレベルは次のとおりです。

- 低: 構築中、スキルはセキュリティリスクにのみフラグを付けます。アーキテクチャの改善や代替案は提案されません。
- 中: 構築中に潜在的な問題が検出された場合、スキルはいくつかの明確な質問をすることがあります。アーキテクチャの改善や代替案は提案されません。
- 高: 構築中、スキルは高レベルのサポートを提供します。アーキテクチャの改善や代替案を提案します。

複数のプロジェクトを操作する

各プロジェクトには、AI コーディングツールがユーザーに代わって AWS リソースを作成および管理するために使用できる独自の認証情報のセットがあります。プロファイルを使用して各プロジェクトにアクセスします。プロファイルは、によって管理される設定と認証情報ファイルであり AWS CLI、各プロファイルに一意の名前を付けます。

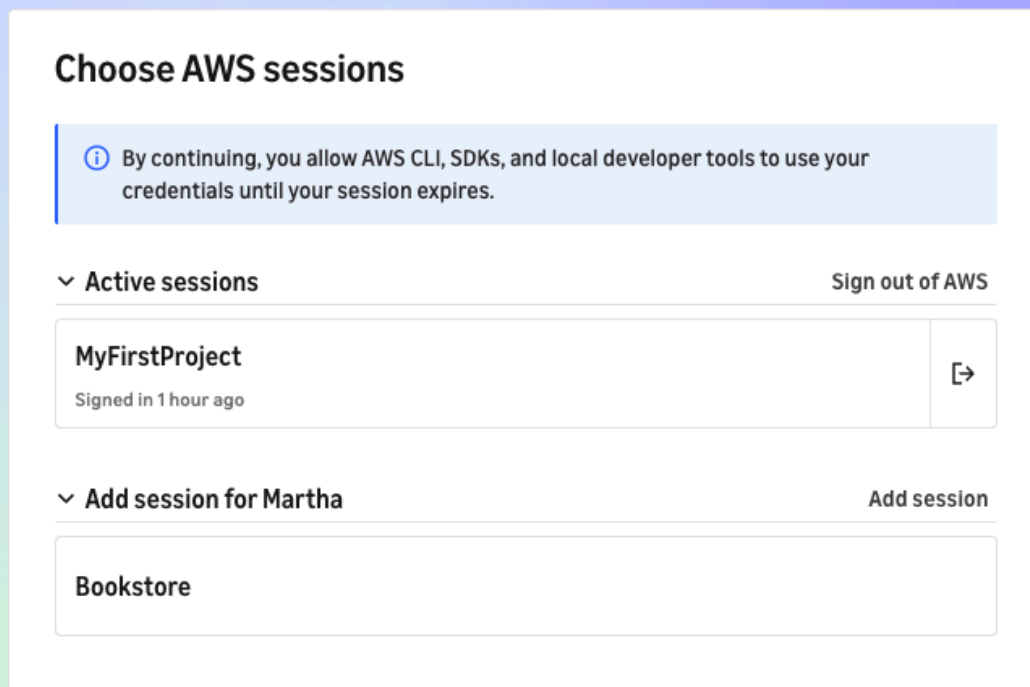
たとえば、最初のプロジェクトが MyFirstProject で、セットアップ MyFirstProjectProfile 時にプロファイル名を選択した場合、次のコマンド AWS CLI を使用して にログインすることで、そのプロジェクトにアクセスできます。

```
aws login --profile MyFirstProjectProfile
```

という名前の別のプロジェクトを作成する場合は Bookstore、セットアップスクリプトを使用してプロファイルを作成することでアクセスできます BookstoreProfile。その後、次のコマンド AWS CLI を使用して にログインできます。

```
aws login --profile BookstoreProfile
```

ただし、これらのコマンドのいずれかを実行する場合は、セッションの選択ページで AWS 認証情報の AWS セッションを選択する必要があります。



このページには、追加できるアクティブなセッションとセッションが表示されます。セッションは認証情報を使用して認証された状態を表し AWS、AI コーディングエージェントがリソースの作成と管理に使用するのと同じ認証情報を提供します。

この例では、既に にログインMyFirstProjectしており、 にログインしていませんBookstore。AWS セッションの選択ページで、以下を実行できます。

- AWS に を引き続き使用するにはMyFirstProject、 を選択しますMyFirstProject。
- にアクセスするにはBookstore、 を選択しますBookstore。
- 現在のセッションを削除するには、終了アイコンを選択します。
- で作成したアカウントなどの IAM ユーザー AWS アカウント を使用して にアクセスするには、セッションの追加 [にサインアップする AWS \(アドバンスド\)](#) を選択します。

選択した認証情報は、AI コーディングエージェントがリソースの作成と管理に使用する認証情報と同じになります。たとえば、次のコマンド AWS CLI を使用して にログインできます。

```
aws login --profile MyFirstProjectProfile
```

次にBookstoreセッションを選択すると、AI コーディングツールによってBookstoreプロジェクトに AWS リソースが作成されます。

プロファイルに関連付けられたプロジェクトに一致するセッションを常を選択します。

AWS プロジェクト所有者の アクション

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

プロジェクトを所有すると、プロジェクトを管理できます。これには、で完了できるタスクが含まれます [AWS 設定を使用する](#)。また、ルートのみアクションを実行することもできます。これらのアクションは、チームメンバーは完了できません。

実行できる現在のルートのみアクションは次のとおりです。

- すべてのプリンシパルを拒否する S3 バケットポリシーを編集または削除します。これを行うと、バケットポリシーの設定ミスで S3 バケットをロック解除できます。
- すべてのプリンシパルを拒否する SQS リソースベースのポリシーを編集または削除します。これを行うと、リソースベースのポリシーの設定ミスで SQS キューをロック解除できます。

ルートのみアクションを実行するには

1. プロジェクトにログインし、<https://console.aws.amazon.com/iam/> で IAM コンソールを開きます。
2. コンソールのナビゲーションペインで、[ルートアクセス管理] を選択します。
3. 特権アクションでは、メンバーアカウントで実行する特権アクションを選択します。

- [Amazon S3 バケットポリシーを削除] を選択して、すべてのプリンシパルが Amazon S3 バケットにアクセスすることを拒否する、誤って設定されているバケットポリシーを削除します。
 - a. S3 URI を入力するか、S3 を参照 を選択して、プロジェクトのバケットから名前を選択します。
 - b. [バケットポリシーを削除] を選択します。
 - c. 誤って設定されたポリシーを削除した後に、Amazon S3 コンソールを使用してバケットポリシーを修正します。詳細については、「Amazon S3 ユーザーガイド」の「[Amazon S3 コンソールを使用したバケットポリシーの追加](#)」を参照してください。
- Amazon SQS ポリシーの削除を選択して、すべてのプリンシパルが Amazon SQS キューにアクセスすることを拒否するリソースベースのポリシーを削除します。
 - a. SQS キュー名にキュー名を入力します。
 - b. SQS ポリシーの削除を選択します。
 - c. 誤って設定されたポリシーを削除した後に、Amazon SQS コンソールを使用してキューポリシーを修正します。詳細については、「Amazon SQS デベロッパーガイド」の「[Configuring an access policy in Amazon SQS](#)」を参照してください。

AWS 設定でパスワードを更新する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

パスワードは AWS 設定で更新できます。

AWS 設定でパスワードを更新するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、セキュリティの管理とサインインを選択します。

Builder ID AWS プロファイルにリダイレクトされます。

3. 認可 で、パスワードの更新 を選択します。

4. [Current password (現在のパスワード)] に現在のパスワードを入力します。
5. 新しいパスワードには、新しいパスワードを入力します。

AWS では、パスワードが次の条件を満たしている必要があります。

- 8～128 文字で構成されていること。
 - 英字の大文字、英字の小文字、数字、記号 (! @ # \$ % ^ & * () < > [] { } | _ + =) のうち、少なくとも 3 つの文字タイプを使用する必要があります。
6. 新しいパスワードの確認 に、新しいパスワードを入力します。
 7. [更新] を選択します。

AWS 設定で多要素認証 (MFA) を管理する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

多要素認証 (MFA) は、セキュリティを強化するためのシンプルで効果的なメカニズムです。1 つ目の要因であるパスワードは、ユーザーが記憶する秘密であり、知識要因とも呼ばれます。その他の要因としては、所有要因 (セキュリティキーなど、ユーザーが持っているもの) や継承要因 (生体認証スキャンなど、ユーザー自身のもの) があります。アカウントにレイヤーを追加するように MFA を設定することを強くお勧めします。

組み込みの認証アプリケーションを登録し、物理的に安全な場所に保管するセキュリティキーも登録することができます。組み込みの認証ソフトを使用できない場合は、登録済みのセキュリティキーを使用できます。認証アプリケーションについては、それらのアプリでクラウドバックアップまたは同期機能を有効にすることもできます。これにより、MFA デバイスを紛失または破損した場合に、プロファイルにアクセスできなくなることを防ぐことができます。

重要ポイント

MFA デバイスを登録および管理するときは、次の重要な点に注意してください。

- 複数の MFA デバイスを登録することをお勧めします。登録されたすべての MFA デバイスにアクセスできなくなった場合、アカウントを復旧することはできません。

- 登録した MFA デバイスを定期的に見直して、最新で機能していることを確認することをお勧めします。また、これらのデバイスは、使用しないときは物理的に安全な場所に保管してください。
- [Google で続行] を使用してアカウントを作成した場合は、Google アカウントを通じて多要素認証を有効にできます。詳細については、「[2 段階認証を有効にする](#)」を参照してください。
- Continue with Apple を使用してアカウントを作成した場合、Apple アカウントで多要素認証が既に有効になっている可能性があります。そうでない場合、有効にする方法の詳細については、「[Apple アカウントの 2 要素認証](#)」を参照してください。
- Continue with GitHub を使用してアカウントを作成した場合は、GitHub アカウントを通じて多要素認証を有効にできます。詳細については、「[\(GitHub\) の 2 要素認証の設定](#)」を参照してください。
- Continue with Amazon を使用してアカウントを作成した場合は、Amazon アカウントを通じて多要素認証を有効にできます。詳細については、「[2 ステップ検証とは](#)」を参照してください。

新しい AWS エクスペリエンスで使用できる MFA タイプ

新しい AWS エクスペリエンスでは、次の多要素認証 (MFA) デバイスタイプがサポートされています。

FIDO2 認証機能

[FIDO2](#) は CTAP2 と [WebAuthn](#) を含む標準であり、パブリックキー暗号に基づいています。FIDO 認証情報は、認証情報が作成された Web サイト (AWS など) 固有のものであるため、フィッシング詐欺に対して強固です。

AWS は、FIDO 認証の最も一般的なフォームファクタとして、組み込み認証とセキュリティキーの 2 つをサポートしています。FIDO 認証機能の最も一般的なタイプの詳細については、以下を参照してください。

組み込みの認証機能

MacBook の TouchID や、Windows Hello 対応のカメラなどの一部デバイスはビルトイン認証システムを装備しています。お使いのデバイスが WebAuthn を含む FIDO プロトコルと互換性がある場合は、指紋や顔を第二の要素として使用できます。詳細については、[FIDO 認証](#) を参照してください。

セキュリティキー

FIDO2 対応の外付け USB、BLE、または NFC 接続のセキュリティキーを購入できます。MFA デバイスの入力を求められたら、キーのセンサーをタップします。YubiKey または Feitian は互換性のあ

るデバイスを製造しています。互換性のあるすべてのセキュリティキーのリストについては、[FIDO 認定製品](#)をご覧ください。

パスワードマネージャー、パスキープロバイダー、その他の FIDO 認証システム

複数のサードパーティプロバイダーが、パスワードマネージャー、FIDO モードのスマートカード、その他のフォームの要素の機能として、モバイルアプリケーションの FIDO 認証をサポートしています。これらの FIDO 互換デバイスは IAM Identity Center で動作しますが、このオプションを MFA で有効にする前に FIDO 認証機能をご自身でテストすることをお勧めします。

Note

FIDO 認証機能の中には、パスキーと呼ばれる検出可能な FIDO 認証情報を作成できるものもあります。パスキーは、パスキーを作成したデバイスにバインドされている場合もあれば、同期可能でクラウドにバックアップされている場合もあります。例えば、サポートされている Macbook で Apple Touch ID を使ってパスキーを登録し、ログイン時に画面に表示される指示に従って iCloud のパスキーで Google Chrome を使って Windows ラップトップからサイトにログインできます。どのデバイスが同期可能なパスキーをサポートしているか、オペレーティングシステムとブラウザ間の現在のパスキーの相互運用性をサポートしているの詳細は、FIDO アライアンスとワールドワイドウェブコンソーシアム (W3C) が管理するリソースである passkeys.dev の「[デバイスサポート](#)」を参照してください。

認証アプリケーション

認証アプリケーションは、ワンタイムパスワード (OTP) ベースのサードパーティー認証機能を備えています。モバイルデバイスやタブレットにインストールされた認証アプリケーションを、許可された MFA デバイスとして使用することができます。サードパーティー認証アプリケーションは、6 桁の認証コードを生成できる標準ベースのタイムベースドワンタイムパスワード (TOTP) アルゴリズムである RFC 6238 に準拠している必要があります。

MFA を求めるプロンプトが表示されたら、認証アプリケーションから有効なコードを入力ボックスに入力する必要があります。ユーザーに割り当てられた各 MFA デバイスは一意であることが必要です。1 人のユーザーに対して 2 つの認証アプリを登録することができます。

以下の有名なサードパーティの認証アプリケーションから選択できます。ただし、TOTP 準拠のアプリケーションは AWS Builder ID MFA で動作します。

オペレーティングシステム	テスト済みの認証アプリ
Android	1Password 、 Authy 、 Duo Mobile 、 Microsoft Authenticator 、 Google Authenticator
iOS	1Password 、 Authy 、 Duo Mobile 、 Microsoft Authenticator 、 Google Authenticator

MFA デバイスの登録

Note

MFA にサインアップし、サインアウトしてから同じデバイスでサインインすると、信頼できるデバイスでは MFA の入力を求められない場合があります。

認証アプリケーションを使用して MFA デバイスを登録するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、セキュリティの管理とサインインを選択します。

Builder ID AWS プロファイルにリダイレクトされます。
3. セキュリティ ページで、デバイスの登録を選択します。
4. MFA デバイスの登録 ページで、認証アプリケーションを選択します。
5. AWS ビルダー ID は、QR コードグラフィックを含む設定情報を操作して表示します。図は、QR コードに対応していない認証アプリケーションでの手動入力に利用できる「シークレット設定キー」を示しています。
6. 認証アプリケーションを開きます。アプリのリストについては、「[認証アプリケーション](#)」を参照してください。

認証アプリケーションが複数の MFA デバイスまたはアカウントをサポートしている場合は、新しい MFA デバイスまたはアカウントを作成するオプションを選択します。

7. MFA アプリケーションが QR コードをサポートしているかどうかを判断し、認証アプリケーションの設定 ページで以下のいずれかの操作を行います。

1. QR コードの表示を選択し、アプリケーションを使用して QR コードをスキャンします。例えば、カメラアイコンまたは スキャンコード に似たオプションを選択します。次に、デバイスのカメラでコードをスキャンします。
2. シークレットキーを表示をクリックし、そのシークレットキーを MFA アプリケーションに入力します。

完了すると、認証アプリケーションがワンタイムパスワードを生成して表示します。

8. 認証システムコードボックスに、現在認証アプリケーションに表示されているワンタイムパスワードを入力します。MFA の割り当てを選択します。

Important

コードを生成したら、即時にリクエストを送信します。コードを生成し、リクエストの送信に時間がかかりすぎると、MFA デバイスは AWS Builder ID に正常に関連付けられますが、MFA デバイスは同期されません。これは、タイムベースドワンタイムパスワード (TOTP) の有効期間が短いために起こります。その場合は、デバイスの再同期ができます。詳細については、#####

9. AWS Builder ID でデバイスにわかりやすい名前を付けるには、名前の変更を選択します。この名前は、このデバイスを登録した他のデバイスと区別するのに役立ちます。

MFA デバイスは、AWS 設定、プロジェクト、AWS ビルダー ID で使用できるようになりました。

セキュリティキーを MFA デバイスとして登録する

セキュリティキーを使用して MFA デバイスを登録するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、セキュリティの管理とサインインを選択します。

Builder ID AWS プロファイルにリダイレクトされます。

3. セキュリティページで、デバイスの登録を選択します。
4. MFA デバイスの登録ページで、セキュリティキーを選択します。
5. セキュリティキーが有効になっていることを確認します。別の物理セキュリティキーを使用する場合は、それをコンピューターに接続します。

6. 画面上の指示に従います。操作性は、オペレーティングシステムとブラウザによって異なります。
7. AWS Builder ID でデバイスにわかりやすい名前を付けるには、名前の変更を選択します。この名前は、このデバイスを登録した他のデバイスと区別するのに役立ちます。

MFA デバイスは、AWS 設定、プロジェクト、AWS ビルダー ID で使用できるようになりました。

MFA デバイスの名前を変更する

MFA デバイスの名前を変更するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、セキュリティの管理とサインインを選択します。

Builder ID AWS プロファイルにリダイレクトされます。

3. セキュリティを選択します。ページに到達すると、名前の変更がグレイアウトされていることがわかります。
4. 変更する MFA デバイスを選択します。これにより、名前の変更を選択できます。そしたら、ダイアログボックスが表示されます。
5. 表示されるプロンプトで、MFA デバイス名に新しい名前を入力し、名前の変更を選択します。名前を変更したデバイスは、多要素認証 (MFA) デバイスに表示されます。

MFA デバイスの削除

2 つ以上の MFA デバイスをアクティブに保つことを推奨します。多要素認証を無効にするには、プロファイルから登録されたすべての MFA デバイスを削除します。

MFA デバイスを削除するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、セキュリティの管理とサインインを選択します。

Builder ID AWS プロファイルにリダイレクトされます。

3. セキュリティページで、変更する MFA デバイスを選択し、削除を選択します。
4. MFA デバイスを削除しますか? モーダルでは、指示に従ってデバイスを削除してください。
5. 削除をクリックします。

削除したデバイスは、[Multi-factor authentication (MFA) devices] (多要素認証 (MFA) デバイス) に表示されなくなります。

AWS 設定ですべてのセッションを削除する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

AWS 設定でデバイス間ですべてのセッションを削除できます。認識できないデバイスがある場合は、パスワードを変更し、すべてのセッションを削除します。

すべてのセッションを削除するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、セキュリティの管理とサインインを選択します。

Builder ID AWS プロファイルにリダイレクトされます。

3. サインインデバイス で、すべてのセッションの削除 を選択します。
4. 選択を確認し、すべてのセッションの削除を選択します。

AWS 設定からログアウトされます。

AWS 設定で名前またはニックネームを管理する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

名前はいつでも変更できます。すべてのチームメンバーは自分の名前を表示できます。有料プランにアップグレードした場合、これは請求情報に表示される名前です。インド AWS でサインアップした場合、お客様の名前は、顧客検証に使用する予定のドキュメントに記載されている名前と完全に一致する必要があります。

名前を変更すると、AWS ビルダー ID の名前が変更されます。これは、AWS 設定、AWS ビルダー ID、および AWS ビルダー ID を介して直接アクセスする AWS リソースの名前に影響します。

名前は、他のユーザーとのやり取り中にツールやサービスで参照される方法です。ニックネームは、密接に協力する人 AWS、友人、その他の人々にどのように知られたいかを示します。

名前またはニックネームを変更するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、プロフィールの管理を選択します。
3. プロファイル情報 で、プロフィールの管理 を選択します。

Builder ID AWS プロファイルにリダイレクトされます。

4. プロファイル情報については、編集 を選択します。
5. (オプション) 名前に新しい名前を入力します。
6. (オプション) ニックネームに新しいニックネームを入力します。
7. [Save changes] (変更の保存) をクリックします。

AWS 設定で E メールアドレスを変更する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

E メールは AWS 設定で変更できます。E メールを変更すると、以前の E メールは AWS プロファイルと AWS Builder ID から分離されます。その E メールを使用して AWS 設定のプロジェクトにアクセスすることはできませんが、その E メールを使用して AWS 再度 にサインアップすることはできます。

プロジェクトへのアクセス権をチームメンバーに付与すると、E メールアドレスがチームメンバーと共有されます。

E メールを変更するには

1. <https://settings.aws.com> で AWS 設定を開きます。

2. メインナビゲーションペインで、プロフィールの管理を選択します。
3. プロファイル情報 で、プロフィールの管理 を選択します。

Builder ID AWS プロファイルにリダイレクトされます。

4. 連絡先情報 で、編集 を選択します。
5. E メールアドレスには、新しい E メールアドレスを入力し、Eメールの確認を選択します。新しい E メールアドレスの検証コードが送信されます。これにより、Eメールの確認ポップアップボックスにと入力されます。
6. 検証コードには、新しい E メールに送信された検証コードを入力します。
7. 確認を選択します。

AWS 設定で連絡先情報を編集する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

AWS 設定に関連付けられた電話番号または住所を編集できます。これらの値を変更すると、納税義務に影響する可能性があります。

連絡先情報を編集するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、プロフィールの管理を選択します。
3. 連絡先情報 で、編集 を選択します。
4. 新しい連絡先情報を入力します。
5. [保存] を選択します。

AWS 設定でサービス改善のためにコンテンツの使用をオプトアウトする

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

AWS AI サービスは、運用上の問題の修正、サービスパフォーマンスの評価、デバッグ、モデルトレーニングなど、サービスの改善のためにお客様のコンテンツを使用および保存する場合があります。この目的のために、このようなコンテンツ AWS リージョン は、サービスを使用している の AWS リージョン 外部に保存される場合があります。AWS 設定を使用して、サービス改善のためのコンテンツの使用をオプトアウトできます。オプトアウトの効果は、AI サービスのオプトアウトポリシーを AWS 組織にア AWS タッチすることです。オプトアウトポリシーの詳細については、[AI サービスのオプトアウトポリシー](#)のドキュメントを参照してください。

すべてのサービスからオプトアウトを選択すると、AI サービスのオプトアウトポリシーでサポートされている現在および将来のサポートされている AI サービスのコンテンツを使用して、すべてのプロジェクトがサービス改善からオプトアウトされます。

Amazon Monitron をオプトアウトするには、追加のステップが必要です。詳細については、「[AWS サービス条件](#)」を参照してください。AWS AI サービスによるデータ使用をオプトアウトできるのは、プロジェクト所有者のみです。

AWS AI サービスによるデータ使用をオプトアウトするには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、プロジェクトを選択します。
3. 概要 で、アクション を選択し、AWS AI サービスによるデータ使用のオプトアウト を選択します。
4. 選択内容を確認し、オプトアウトを選択します。

AWS Builder ID データをリクエストする

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

Builder ID に関連付けられた個人情報、および AWS Builder ID でアクセスした AWS アプリケーションとサービスをリクエストして表示できます AWS。リクエストは 30 日以内に処理され、データの準備ができたなら通知されます。データリクエストが保留中の間は、AWS プロファイルを閉じることはできません。プロジェクトまたはすべてのプロジェクトを所有する組織を閉鎖することはできません。

他の AWS ウェブサイト、アプリケーション、製品、サービス、イベント、エクスペリエンスに関連して提供される個人情報など、データのサブジェクト権の行使の詳細については、[AWS「プライバシー」](#)を参照してください。

個人データをリクエストするには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、プロファイルの管理を選択します。
3. プロファイルの管理を選択します。

Builder ID AWS プロファイルにリダイレクトされます。

4. プライバシーとデータを選択します。
5. ビルダー ID データまたは AWS データをリクエストするには、 を選択します。

リクエストが受領され 30 日以内に処理が完了されることを知らせる緑色の確認メッセージがページ上部に表示されます。

6. リクエストが処理されたという E メールが当社から届いたら、AWS ビルダー ID プロファイルのプライバシーとデータページに戻ります。新しく表示された データを含む ZIP アーカイブをダウンロードボタンを選択します。

データリクエストが保留中の間は、AWS ビルダー ID を削除することはできません。

AWS 設定でプロジェクトを作成する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

プロジェクトには、AWS リソースを作成する 1 つの AWS アカウント が含まれます。プロジェクトには、他の共同作業者と共有するための設定も含まれています。作成する AWS リソースは、アプリケーションまたは一連の関連するユースケースを表す必要があります。1 つのプロジェクトは、アプリケーションの開発環境と本番環境にまたがることができます。たとえば、データベース、コンピューティングリソース、ストレージなど、ブックストアアプリケーションのリソースを保持する Bookstore というプロジェクトを作成できます。

このプロジェクトは他のチームメンバーと共有でき、彼らは書店アプリケーションのリソースを構築および管理できます。

各プロジェクトには、アカウントのリソースに基づいて独自のコスト管理があります。有料プランを使用している場合は、各プロジェクト AWS の設定で支出制限を設定できます。詳細については、「[AWS 設定で使用制限を作成する](#)」を参照してください。プロジェクト所有者は、使用料と定期的な料金の毎月の請求書に責任を負います。

プロジェクトの作成に関する考慮事項

- チームメンバーとして所有していないプロジェクトにアクセスできます。
- 各プロジェクト名はプロジェクトに一意である必要があります。他のチームメンバーが所有するプロジェクトには同じ名前を付けることができます。
- プロジェクト名には、a~z、A~Z、0~9、ピリオド (.) の有効な文字を含めることができます。
- プロジェクトを作成すると、は、連絡先住所の国に基づいて、米国東部 (オハイオ) (us-east-2)、欧州 (ストックホルム) (eu-north-1)、またはアジアパシフィック (シドニー) (ap-southeast-2) のいずれかのリージョンにプロジェクトを AWS 割り当てます。作成したリージョンリソースは、そのリージョンでホストされます。詳細については、「[AWS リージョン プロジェクトの](#)」を参照してください。

プロジェクトを作成する

プロジェクトを作成するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、プロジェクトを選択します。
3. [プロジェクトを作成] を選択します。
4. プロジェクト名に、プロジェクトのわかりやすい名前を入力します。

この名前は、チームメンバーをコラボレーションに招待するときにチームメンバーと共有されます。

5. [作成] を選択します。

プロジェクトの作成には数秒かかります。プロジェクトが利用可能になったら、プロジェクトを選択し、AWS マネジメントコンソール にアクセスして構築を開始できます。

とインターフェイスするように AI コーディングツールを既にセットアップしている場合は AWS アカウント、新しいプロジェクトでリソースを作成するように求めることができます。

AI コーディングツールのプロンプト例を使用して開始します。

What is the Region for my project *test project*?

Create a hello world Lambda function in my project *test project*.

Create an S3 bucket in my project *test project*.

AWS リージョン プロジェクトの

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

プロジェクトを作成すると、は、連絡先住所の国に基づいて、米国東部 (オハイオ) (us-east-2)、欧州 (ストックホルム) (eu-north-1)、またはアジアパシフィック (シドニー) (ap-southeast-2)

のいずれかのリージョンにプロジェクトを AWS 割り当てます。作成したリージョンリソースは、そのリージョンでホストされます。

以下は、アカウント AWS リージョン 用に選択された に関する考慮事項です。

- AWS 設定で連絡先情報を変更しても、選択したリージョンは変更されません。特定のリージョンにアクセスする必要がある場合は、「Sign up for AWS (advanced)」を使用します。アカウントの高度な機能をアクティブ化して、異なるリージョンを選択することもできます。
- AWS は、サポートされているリージョンを追加で導入できますが、新しいサインアップでのみ使用できます。2026 年 8 月 18 日現在の最新のサポートされているリージョンについては、以下の表を参照してください。プロジェクトが既にある場合は、[AWS 「設定」](#) で選択したリージョンを見つけることができます。
- グローバルサービスは、プロジェクトで利用できます。これらのサービスは、ホームリージョンとは異なる 1 つのリージョンを介してアクセスされます。詳細については、「[AWS 障害分離境界](#)」を参照してください。さらに、特定のリージョンで利用できるサービスもあります。では AWS マネジメントコンソール、特定のリージョンでこれらのサービスを表示できますが、別のサービスに移動すると、選択したリージョンに戻ります。
- Amazon Bedrock を使用する場合は、デフォルトで有効になっているすべての商用 でリソースを作成しない APIs AWS リージョン を使用できます。
- CloudFront を使用する場合、選択したリージョンの外部にリソースを作成する特定の機能は利用できません。これには、CloudFront AWS WAF での の使用が含まれます。
- グローバルサービスに関連する一部の CloudTrail イベントは、グローバルサービスが運用されているリージョンに記録されます。これらのイベントにアクセスできます。
- AWS WAF および Amazon CloudWatch Logs は、米国東部 (バージニア北部) () で利用できません us-east-1。

AWS 設定を使用して、アカウント内のすべてのプロジェクトの選択したリージョンを確認できます。では AWS マネジメントコンソール、Bedrock や SageMaker など、ほとんどのサービスコンソールが リージョンでホストされています。グローバルサービスからサービスコンソールを見ると、コンソールはすべての API コールをグローバルサービスの適切なリージョンに自動的にルーティングします。

プロジェクト AWS リージョン 用に選択した を検索する

ベストプラクティスとして、AWS リソースを作成する前に AWS リージョン、プロジェクトの を常に確認することをお勧めします。

プロジェクト AWS リージョン 用に選択された を検索するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、プロジェクトを選択します。
3. 概要セクションで、追加情報を選択します。

このビューでは、プロジェクトに関連付けられた AWS アカウント ID を見つけることもできます。

4. リージョンの場合、AWS リージョン プロジェクトがプロビジョニングされていることが表示されます。

いずれかのプロジェクトでリージョン AWS リソースを作成すると、これらのリソースの Amazon リソースネームにこれが含まれます AWS リージョン。

米国東部 (オハイオ) (**us-east-2**) でリージョンリソースがプロビジョニングされている国

国名	国コード
アンティグアバーブーダ	AG
アルゼンチン	AR
バハマ諸島	BS
バルバドス	BB
ベリーズ	BZ
ボリビア	BO
ブラジル	BR
カナダ	CA
チリ	CL
コロンビア	CO

国名	国コード
コスタリカ	CR
ドミニカ	DM
ドミニカ共和国	DO
エクアドル	EC
エルサルバドル	SV
グレナダ	GD
グアテマラ	GT
ガイアナ	GY
ハイチ	HT
ホンジュラス	HN
ジャマイカ	JM
メキシコ	MX
ニカラグア	NI
パナマ	PA
パラグアイ	PY
ペルー	PE
セントクリストファーネイビス	KN
セントルシア	LC
セントビンセントおよびグレナディーン諸島	VC
スリナム	SR

国名	国コード
トリニダード・トバゴ	TT
アメリカ	米国
ウルグアイ	UY
ベネズエラ	VE
アンギラ	AI
アルバ	AQ
バミューダ	BM
Bonaire、Sint Eustatius、Saba	BQ
英領バージン諸島	VG
ケイマン諸島	KY
キュラソー	CW
フォークランド諸島	FK
フランス領ギアナ	GF
グアドループ	GP
マルチニーク	MQ
Montserrat	MS
プエルトリコ	PR
サン・バルテルミー	BL
サン・マルタン島	MF
サンピエール・ミクロン	PM

国名	国コード
シントマールテン	SX
タークスおよびカイコス諸島	TC
米領バージン諸島	VI

アジアパシフィック (シドニー) (ap-southeast-2) でリージョンリソースがプロビジョニングされている国

国名	国コード
アフガニスタン	AF
オーストラリア	AU
バングラデシュ	BD
ブータン	BT
ブルネイ	BN
カンボジア	KH
中国	CN
東ティモール	TL
フィジー	FJ
Hong Kong	HK
インド	IN
インドネシア	ID
日本	JP

国名	国コード
カザフスタン	KZ
キリバス	KI
キルギスタン	KG
ラオス	LA
マカオ	MO
マレーシア	MY
モルジブ	MV
マーシャル諸島共和国	MH
ミクロネシア	FM
モンゴル	MN
ミャンマー	MM
ナウル	NR
ネパール	NP
ニュージーランド	NZ
パキスタン	PK
パラオ	PW
パプアニューギニア	PG
フィリピン	PH
サモア	WS
シンガポール	SG

国名	国コード
ソロモン諸島	SB
韓国	KR
スリランカ	LK
台湾	TW
タジキスタン	TJ
タイ	TH
トンガ	TO
トルクメニスタン	TM
ツバル	TV
ウズベキスタン	UZ
バヌアツ	VU
ベトナム	VN
アメリカ領サモア	AS
クリスマス島	CX
ココス (キーリング) 諸島	CC
クック諸島	CK
フランス領ポリネシア	PF
グアム	GU
ハード島とマクドナルド諸島	HM
ニューカレドニア	NC

国名	国コード
Niue	NU
ノーフォーク島	NF
北マリアナ諸島	MP
ピトケアン諸島	PN
トケラウ	TK
米国領マイナーアウトリージング諸島	UM
ウォリス・フツナ	WF

欧州 (ストックホルム) でリージョンリソースがプロビジョニングされている国 (**eu-north-1**)

国名	国コード
アルバニア	AL
アルジェリア	DZ
アンドラ	AD
アンゴラ	AO
アルメニア	AM
オーストリア	AT
アゼルバイジャン	AZ
バーレーン	BH
ベラルーシ	BY

国名	国コード
ベルギー	BE
ベニン	BJ
ボスニアヘルツェゴビナ	BA
ボツワナ	BW
ブルガリア	BG
ブルキナファソ	BF
ブルンジ	BI
カーボベルデ	CV
カメルーン	CM
中央アフリカ共和国	CF
チャド	TD
コモロ	KM
コンゴ (ブラザビル)	CG
コンゴ (DRC)	CD
コートジボワール	CI
クロアチア	HR
キプロス	CY
チェコ共和国	CZ
デンマーク	DK
ジブチ	DJ

国名	国コード
エジプト	EG
赤道ギニア	GQ
エリトリア	ER
エストニア	EE
エスワティニ	SZ
エチオピア	ET
フィンランド	FI
フランス	FR
ガボン	GA
ガンビア	GM
ジョージア	GE
ドイツ	DE
ガーナ	GH
ギリシャ	GR
ギニア	GN
ギニアビサウ	GW
ハンガリー	hu
Iceland	IS
イラク	IQ
アイルランド	IE

国名	国コード
イスラエル	IL
イタリア	IT
ヨルダン	JO
ケニア	KE
コソボ共和国	XK
クウェート	KW
ラトビア	LV
レバノン	LB
レソト	LS
リベリア	LR
リビア	LY
リヒテンシュタイン	LI
リトアニア	LT
ルクセンブルグ	LU
マダガスカル	MG
マラウイ	MW
マリ	ML
マルタ	MT
モーリタニア	MR
モーリシャス	MU

国名	国コード
モルドバ	MD
モナコ	MC
モンテネグロ	ME
モロッコ	MA
モザンビーク	MZ
ナミビア	NA
オランダ	NL
ニジェール	NE
ナイジェリア	NG
北マケドニア	MK
ノルウェー	いいえ
オマーン	OM
パレスチナ	PS
ポーランド	PL
ポルトガル	PT
カタール	QA
ルーマニア	RO
ロシア	RU
ルワンダ	RW
サンマリノ	SM

国名	国コード
サントメ・プリンシペ民主共和	ST
サウジアラビア	SA
セネガル	SN
セルビア	RS
セイシェル	SC
シエラレオネ	SL
スロバキア	SK
スロベニア	SI
ソマリア	SO
南アフリカ	ZA
南スーダン	SS
スペイン	ES
スウェーデン	SE
スイス	CH
タンザニア	TZ
トーゴ	TG
チュニジア	TN
トルコ	TR
ウガンダ	UG
ウクライナ	UA

国名	国コード
アラブ首長国連邦	AE
英国	GB
バチカン市国	VA
イエメン	YE
ザンビア	ZM
ジンバブエ	ZW
オーランド諸島	AX
南極大陸	AQ
ブーベ島	BV
英領インド洋地域	IO
フェロー諸島	FO
フランス領南方・南極地域	TF
ジブラルタル	GI
グリーンランド	GL
ガーンジー代官管轄区	GG
マン島	IM
Jersey	JE
マヨット	YT
レユニオン	RE
セントヘレナ	SH

国名	国コード
サウスジョージア・ サウスサンドウィッチ諸島	GS
スバルバル諸島およびヤンマイエン島	SJ
西サハラ	EH

組織の管理ポリシー

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

新しい AWS エクスペリエンスを使用すると、 はリソースコントロールポリシー (RCPs) やサービスコントロールポリシー (SCPs) を含む組織管理ポリシー AWS を管理します。これらの保護コントロールにより、プロジェクト所有者またはチームメンバーが、迅速に構築および開発できるように AWS が定義した事前設定されたデフォルトを妨げるアクションを実行できなくなります。

プロジェクトのサービスコントロールポリシー

以下は、プロジェクト内のすべてのユーザーのサービスコントロールポリシーであり、変更できません。

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BlockOrgEscape",
      "Effect" : "Deny",
      "Action" : [
        "account:CloseAccount",
        "organizations:AcceptHandshake",
        "organizations:LeaveOrganization",
        "sso:CreateInstance"
      ],
      "Resource" : "*"
    }
  ]
}
```

```

    },
    {
      "Sid" : "ProtectManagedRoles",
      "Effect" : "Deny",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam>DeleteRolePermissionsBoundary",
        "iam>DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:TagRole",
        "iam:UntagRole",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole"
      ],
      "Resource" : "arn:*:iam::*:role/managed/*",
      "Condition" : {
        "StringNotLike" : {
          "aws:PrincipalArn" : "arn:*:iam::*:role/managed/
AWSManagedAccountManagementAccessRole"
        }
      }
    }
  ]
}

```

高度な機能をアクティブ化しても、このポリシーは削除されません。詳細については、「[高度な AWS 機能をアクティブ化する](#)」を参照してください。

高度な機能をアクティブ化すると、このポリシーは組織のルートにアタッチされたままになるため、後で作成または招待するアカウントを含むすべてのメンバーアカウントに適用されます。

さらに、プロジェクト内のすべてのユーザーに次のサービスコントロールポリシーを適用して、サポートされていないか、AWS 設定で完了する必要があるプロジェクトへの特定の変更を制限します。

```

{
  "Version" : "2012-10-17",
  "Statement" : [
    {

```

```
"Sid" : "BlockAccountManagementAPIs",
"Effect" : "Deny",
"Action" : [
  "account:AcceptPrimaryEmailUpdate",
  "account:DeleteAlternateContact",
  "account:DisableRegion",
  "account:EnableRegion",
  "account:GetAlternateContact",
  "account:GetContactInformation",
  "account:GetGovCloudAccountInformation",
  "account:GetRegionOptStatus",
  "account:PutAccountName",
  "account:PutAlternateContact",
  "account:PutContactInformation",
  "account:StartPrimaryEmailUpdate"
],
"Resource" : "*"
},
{
  "Sid" : "DenyBillingOperations",
  "Effect" : "Deny",
  "Action" : "billing:*",
  "Resource" : "*"
},
{
  "Sid" : "DenyNotificationContactsOperations",
  "Effect" : "Deny",
  "Action" : "notifications-contacts:*",
  "Resource" : "*"
},
{
  "Sid" : "DenyRestrictedNotificationOperations",
  "Effect" : "Deny",
  "Action" : [
    "notifications:AssociateChannel",
    "notifications:AssociateManagedNotificationAccountContact",
    "notifications:AssociateManagedNotificationAdditionalChannel",
    "notifications:AssociateOrganizationalUnit",
    "notifications>CreateEventRule",
    "notifications>CreateNotificationConfiguration",
    "notifications>DeleteEventRule",
    "notifications>DeleteNotificationConfiguration",
    "notifications:DeregisterNotificationHub",
    "notifications:DisableNotificationsAccessForOrganization",
```



```

        "notifications:DisassociateChannel",
        "notifications:DisassociateManagedNotificationAccountContact",
        "notifications:DisassociateManagedNotificationAdditionalChannel",
        "notifications:DisassociateOrganizationalUnit",
        "notifications:EnableNotificationsAccessForOrganization",
        "notifications:GetEventRule",
        "notifications:GetFeatureOptInStatus",
        "notifications:GetNotificationConfiguration",
        "notifications:GetNotificationEvent",
        "notifications:GetNotificationsAccessForOrganization",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListMemberAccounts",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationEvents",
        "notifications:ListNotificationHubs",
        "notifications:ListOrganizationalUnits",
        "notifications:ListTagsForResource",
        "notifications:PutFeatureOptInStatus",
        "notifications:RegisterNotificationHub",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration"
    ],
    "Resource" : "*"
},
{
    "Sid" : "DenyRoleManagerDisablement",
    "Effect" : "Deny",
    "Action" : "iam:PutAccountProperties",
    "Resource" : "*",
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "iam:AccountPropertyNamespaces" : "RoleManager"
        }
    }
}
]
}

```

このポリシーは、高度な機能をアクティブ化すると削除されます。詳細については、「[高度な AWS 機能をアクティブ化する](#)」を参照してください。

このポリシーを削除しても、プロジェクトアカウントのルートユーザーの E メールアドレスを更新することはできません。詳細については、「[高度な機能をアクティブ化した後のプロジェクトアカウント](#)」を参照してください。

さらに、プロジェクト内のすべてのユーザーに次のサービスコントロールポリシーを適用し、####
#####に応じてパーティションサービスのサポートを許可する AWS リージョン ように を制限します。

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UsEast1Partitional",
      "Effect" : "Deny",
      "NotAction" : [
        "account:*",
        "acm:*",
        "activate:*",
        "artifact:*",
        "aws-marketplace:*",
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles",
        "budgets:*",
        "ce:*",
        "chatbot:*",
        "cloudfront-keyvaluestore:*",
        "cloudfront:*",
        "cloudshell:*
```

```
"cloudtrail:LookupEvents",
"cloudwatch:BatchGet*",
"cloudwatch:Describe*",
"cloudwatch:GenerateQuery",
"cloudwatch:Get*",
"cloudwatch:List*",
"consoleapp:*",
"cost-optimization-hub:*",
"ec2:DescribeRegions",
"ecr-public:*",
"freetier:*",
"health:*",
"iam:*",
"identitystore-auth:*",
"identitystore:*",
"invoicing:*",
"kms:CreateGrant",
"kms:Decrypt",
"kms:DescribeKey",
"kms:ListAliases",
"lightsail:AttachCertificateToDistribution",
"lightsail:CreateCertificate",
"lightsail:CreateContactMethod",
"lightsail:CreateDistribution",
"lightsail:CreateDomain",
"lightsail:CreateDomainEntry",
"lightsail>DeleteAlarm",
"lightsail>DeleteCertificate",
"lightsail>DeleteContactMethod",
"lightsail>DeleteDistribution",
"lightsail>DeleteDomain",
"lightsail>DeleteDomainEntry",
"lightsail:DetachCertificateFromDistribution",
"lightsail:Get*",
"lightsail:IsVpcPeered",
"lightsail:PutAlarm",
"lightsail:ResetDistributionCache",
"lightsail:SendContactMethodVerification",
"lightsail:SetIpAddressType",
"lightsail:TagResource",
"lightsail:TestAlarm",
"lightsail:UntagResource",
"lightsail:UpdateDistribution",
"lightsail:UpdateDistributionBundle",
```

```

    "lightsail:UpdateDomainEntry",
    "logs:*",
    "managedblockchain-query:*",
    "managedblockchain:*",
    "mapcredits:*",
    "notifications:GetManagedNotificationConfiguration",
    "notifications:GetManagedNotificationEvent",
    "notifications:ListManagedNotificationChildEvents",
    "notifications:ListManagedNotificationConfigurations",
    "notifications:ListManagedNotificationEvents",
    "organizations:*",
    "pricing:*",
    "q:*",
    "route53:*",
    "route53domains:*",
    "route53globalresolver:*",
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets",
    "servicequotas:*",
    "signin:*",
    "sso-directory:*",
    "sso-oauth:*",
    "sso:*",
    "sts:*",
    "support:*",
    "tax:*",
    "trustedadvisor:*",
    "uxc:*",
    "waf:*",
    "wafv2:*"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestedRegion" : "us-east-1"
    }
  }
},
{
  "Sid" : "DenyUsEast1WafResourceAssociation",
  "Effect" : "Deny",
  "Action" : [
    "wafv2:AssociateWebACL",
    "wafv2:DisassociateWebACL",

```

```

        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "aws:RequestedRegion" : "us-east-1"
        }
    }
},
{
    "Sid" : "UsWest2Partititional",
    "Effect" : "Deny",
    "NotAction" : [
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles",
        "cloudshell:*",
        "cloudtrail:LookupEvents",
        "health:*",
        "identitystore-auth:*",
        "identitystore:*",
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:ListAliases",
        "networkmanager-chat:*",
        "networkmanager:*",
        "route53-recovery-cluster:*",
        "route53-recovery-control-config:*",
        "route53-recovery-readiness:*",
        "servicequotas:*",
        "sso-directory:*",
        "sso-oauth:*",

```

```

        "sso:*",
        "support:*",
        "trustedadvisor:*",
        "uxc:*"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "aws:RequestedRegion" : "us-west-2"
        }
    }
},
{
    "Sid" : "RegionFloor",
    "Effect" : "Deny",
    "NotAction" : [
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringNotEquals" : {
            "aws:RequestedRegion" : [
                "unspecified",
                "us-east-1",
                "selected-region",
                "us-west-2"
            ]
        }
    }
}
]

```

```
}
```

高度な機能をアクティブ化すると、次のサービスコントロールポリシーがアカウントに適用されます。

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UsEast1Partititional",
      "Effect" : "Deny",
      "NotAction" : [
        "a4b:*",
        "access-analyzer:*",
        "account-access:*",
        "account:*",
        "acm:*",
        "activate:*",
        "artifact:*",
        "aws-marketplace-management:*",
        "aws-marketplace:*",
        "aws-portal:*",
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles",
        "billing:*",
        "billingconductor:*",
        "budgets:*",
        "builderid:*",
        "ce:*",
        "chatbot:*",
        "chime:*
```

```
"cloudfront-keyvaluestore:*",
"cloudfront:*",
"cloudshell:*",
"cloudtrail:LookupEvents",
"cloudwatch:BatchGet*",
"cloudwatch:Describe*",
"cloudwatch:GenerateQuery",
"cloudwatch:Get*",
"cloudwatch:List*",
"compute-optimizer:*",
"config:*",
"consoleapp:*",
"consolidatedbilling:*",
"cost-optimization-hub:*",
"cur:*",
"datapipeline:GetAccountLimits",
"devicefarm:*",
"directconnect:*",
"ec2:DescribeRegions",
"ec2:DescribeTransitGateways",
"ec2:DescribeVpnGateways",
"ecr-public:*",
"fms:*",
"freetier:*",
"globalaccelerator:*",
"health:*",
"iam:*",
"identitystore-auth:*",
"identitystore:*",
"importexport:*",
"invoicing:*",
"iq:*",
"kms:*",
"license-manager:ListReceivedLicenses",
"lightsail:AttachCertificateToDistribution",
"lightsail:CreateCertificate",
"lightsail:CreateContactMethod",
"lightsail:CreateDistribution",
"lightsail:CreateDomain",
"lightsail:CreateDomainEntry",
"lightsail>DeleteAlarm",
"lightsail>DeleteCertificate",
"lightsail>DeleteContactMethod",
"lightsail>DeleteDistribution",
```



```
"lightsail:DeleteDomain",
"lightsail:DeleteDomainEntry",
"lightsail:DetachCertificateFromDistribution",
"lightsail:Get*",
"lightsail:IsVpcPeered",
"lightsail:PutAlarm",
"lightsail:ResetDistributionCache",
"lightsail:SendContactMethodVerification",
"lightsail:SetIpAddressType",
"lightsail:TagResource",
"lightsail:TestAlarm",
"lightsail:UntagResource",
"lightsail:UpdateDistribution",
"lightsail:UpdateDistributionBundle",
"lightsail:UpdateDomainEntry",
"logs:*",
"managedblockchain-query:*",
"managedblockchain:*",
"mapcredits:*",
"mobileanalytics:*",
"networkmanager:*",
"notifications-contacts:*",
"notifications:*",
"organizations:*",
"payments:*",
"pricing:*",
"q:*",
"quicksight:DescribeAccountSubscription",
"resource-explorer-2:*",
"route53-recovery-cluster:*",
"route53-recovery-control-config:*",
"route53-recovery-readiness:*",
"route53:*",
"route53domains:*",
"route53globalresolver:*",
"s3:CreateMultiRegionAccessPoint",
"s3:DeleteMultiRegionAccessPoint",
"s3:DescribeMultiRegionAccessPointOperation",
"s3:GetAccountPublicAccessBlock",
"s3:GetBucketLocation",
"s3:GetBucketPolicyStatus",
"s3:GetBucketPublicAccessBlock",
"s3:GetMultiRegionAccessPoint",
"s3:GetMultiRegionAccessPointPolicy",
```

```

    "s3:GetMultiRegionAccessPointPolicyStatus",
    "s3:GetStorageLensConfiguration",
    "s3:GetStorageLensDashboard",
    "s3:ListAllMyBuckets",
    "s3:ListMultiRegionAccessPoints",
    "s3:ListStorageLensConfigurations",
    "s3:PutAccountPublicAccessBlock",
    "s3:PutMultiRegionAccessPointPolicy",
    "savingsplans:*",
    "servicequotas:*",
    "shield:*",
    "signin:*",
    "sso-directory:*",
    "sso-oauth:*",
    "sso:*",
    "sts:*",
    "support:*",
    "supportapp:*",
    "supportplans:*",
    "sustainability:*",
    "tag:GetResources",
    "tax:*",
    "trustedadvisor:*",
    "uxc:*",
    "vendor-insights:ListEntitledSecurityProfiles",
    "waf-regional:*",
    "waf:*",
    "wafv2:*"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestedRegion" : "us-east-1"
    }
  }
},
{
  "Sid" : "UsWest2Partitional",
  "Effect" : "Deny",
  "NotAction" : [
    "bedrock-mantle:CallWithBearerToken",
    "bedrock-mantle:CreateInference",
    "bedrock-mantle:GetInference",
    "bedrock-mantle:GetModel",

```

```

        "bedrock-mantle:ListModel",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles",
        "cloudshell:*",
        "cloudtrail:LookupEvents",
        "health:*",
        "identitystore-auth:*",
        "identitystore:*",
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:ListAliases",
        "networkmanager-chat:*",
        "networkmanager:*",
        "route53-recovery-cluster:*",
        "route53-recovery-control-config:*",
        "route53-recovery-readiness:*",
        "servicequotas:*",
        "sso-directory:*",
        "sso-oauth:*",
        "sso:*",
        "support:*",
        "trustedadvisor:*",
        "uxc:*"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "aws:RequestedRegion" : "us-west-2"
        }
    }
},
{
    "Sid" : "RegionFloor",
    "Effect" : "Deny",
    "NotAction" : [
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",

```

```

        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringNotEquals" : {
            "aws:RequestedRegion" : [
                "unspecified",
                "us-east-1",
                "selected-region",
                "us-west-2"
            ]
        }
    }
}
]
}

```

使用制限のサービスコントロールポリシー

使用制限を使用する場合、使用制限に近づくと、次のサービスコントロールポリシーがプロジェクトに適用されます。使用制限の詳細については、「」を参照してください[AWS 設定で使用制限を作成する](#)。

```

{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "DenyBedrockUsage",
    "Effect": "Deny",
    "Action": [
      "bedrock:ApplyGuardrail",
      "bedrock:CallWithBearerToken",
      "bedrock:InvokeAgent",

```

```
    "bedrock:InvokeAutomatedReasoningPolicy",
    "bedrock:InvokeDataAutomation",
    "bedrock:InvokeDataAutomationAsync",
    "bedrock:InvokeFlow",
    "bedrock:InvokeInlineAgent",
    "bedrock:InvokeModel",
    "bedrock:InvokeModelWithResponseStream",
    "bedrock:InvokeTool",
    "bedrock:OptimizePrompt",
    "bedrock:Retrieve",
    "bedrock:RetrieveAndGenerate",
    "bedrock:StartFlowExecution",
    "bedrock-mantle:CallWithBearerToken",
    "bedrock-mantle:CreateInference"
  ],
  "Resource": "*"
}
```

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "DenyLambdaUsage",
    "Effect": "Deny",
    "Action": [
      "lambda:DeleteFunctionConcurrency",
      "lambda:InvokeAsync",
      "lambda:InvokeFunction",
      "lambda:InvokeFunctionUrl",
      "lambda:PutFunctionConcurrency"
    ],
    "Resource": "*"
  }
}
```

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "DenySageMakerInference",
    "Effect": "Deny",
    "Action": [
      "sagemaker:InvokeEndpoint",
      "sagemaker:InvokeEndpointAsync",

```

```
    "sagemaker:InvokeEndpointWithResponseStream"
  ],
  "Resource": "*"
}
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCompute",
      "Effect": "Deny",
      "Action": [
        "ec2:CreateNatGateway",
        "ec2:CreateVolume",
        "ec2:CreateVpnConnection",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "elasticloadbalancing:CreateLoadBalancer",
        "autoscaling:CreateAutoScalingGroup",
        "ecs:CreateService",
        "eks:CreateCluster",
        "eks:CreateNodegroup",
        "eks:CreateFargateProfile",
        "elasticbeanstalk:CreateEnvironment",
        "apprunner:CreateService",
        "apprunner:ResumeService",
        "batch:CreateComputeEnvironment",
        "elasticmapreduce:RunJobFlow",
        "appstream:CreateFleet"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyLambda",
      "Effect": "Deny",
      "Action": "lambda:CreateFunction",
      "Resource": "*"
    },
    {
      "Sid": "DenyDatabase",
      "Effect": "Deny",
      "Action": [
```

```

    "rds:CreateDBCluster",
    "rds:CreateDBInstance",
    "rds:RestoreDBClusterFromS3",
    "rds:RestoreDBClusterFromSnapshot",
    "rds:RestoreDBClusterToPointInTime",
    "rds:RestoreDBInstanceFromDBSnapshot",
    "rds:RestoreDBInstanceFromS3",
    "rds:RestoreDBInstanceToPointInTime",
    "rds:StartDBCluster",
    "rds:StartDBInstance",
    "dynamodb:CreateTable",
    "dynamodb:CreateGlobalTable",
    "elasticache:CreateCacheCluster",
    "elasticache:CreateReplicationGroup",
    "timestream:CreateDatabase",
    "timestream:CreateTable",
    "memorydb:CreateCluster",
    "es:CreateDomain",
    "aoss:CreateCollection",
    "redshift:CreateCluster",
    "redshift:ResumeCluster",
    "redshift-serverless:CreateWorkgroup",
    "dsq1:CreateCluster"
  ],
  "Resource": "*"
},
{
  "Sid": "DenyStorage",
  "Effect": "Deny",
  "Action": [
    "elasticfilesystem:CreateFileSystem",
    "datasync:CreateTask",
    "storagegateway:ActivateGateway",
    "glacier:CreateVault"
  ],
  "Resource": "*"
},
{
  "Sid": "DenySageMaker",
  "Effect": "Deny",
  "Action": [
    "sagemaker:CreateApp",
    "sagemaker:CreateEndpoint",
    "sagemaker:CreateNotebookInstance",

```

```

        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:StartNotebookInstance"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyBedrock",
    "Effect": "Deny",
    "Action": [
        "bedrock:CreateCustomModelDeployment",
        "bedrock:CreateDataAutomationProject",
        "bedrock:CreateEvaluationJob",
        "bedrock:CreateMarketplaceModelEndpoint",
        "bedrock:CreateModelCustomizationJob",
        "bedrock:CreateModelImportJob",
        "bedrock:CreateModelInvocationJob",
        "bedrock:CreateProvisionedModelThroughput",
        "bedrock-mantle:CreateCustomizedModel",
        "bedrock-mantle:CreateFineTuningJob",
        "bedrock-mantle:CreateReservation"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyAIML",
    "Effect": "Deny",
    "Action": [
        "kendra:CreateIndex",
        "personalize:CreateSolution",
        "personalize:CreateCampaign",
        "forecast:CreatePredictor",
        "forecast:CreateForecast",
        "rekognition:CreateProject",
        "lex:CreateBot"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyNetworking",
    "Effect": "Deny",
    "Action": [
        "cloudfront:CreateDistribution",

```



```
    "route53:CreateHostedZone",
    "appmesh:CreateMesh"
  ],
  "Resource": "*"
},
{
  "Sid": "DenyApiGatewayCreate",
  "Effect": "Deny",
  "Action": "apigateway:POST",
  "Resource": [
    "arn:aws:apigateway:*::/restapis",
    "arn:aws:apigateway:*::/apis"
  ]
},
{
  "Sid": "DenyMessaging",
  "Effect": "Deny",
  "Action": [
    "mq:CreateBroker",
    "kafka:CreateCluster",
    "kafka:CreateVpcConnection",
    "kinesis:CreateStream",
    "firehose:CreateDeliveryStream",
    "kinesisanalytics:CreateApplication",
    "kinesisvideo:CreateStream",
    "sns:CreateTopic",
    "sqs:CreateQueue",
    "events:CreateEventBus",
    "pipes:CreatePipe",
    "scheduler:CreateSchedule"
  ],
  "Resource": "*"
},
{
  "Sid": "DenyAnalytics",
  "Effect": "Deny",
  "Action": [
    "states:CreateStateMachine",
    "glue:CreateJob",
    "glue:CreateCrawler",
    "athena:CreateWorkGroup",
    "appsync:CreateGraphQLApi",
    "appflow:CreateFlow",
    "datazone:CreateDomain",
```

```

        "datazone:CreateProject",
        "entityresolution:CreateMatchingWorkflow",
        "datapipeline:CreatePipeline",
        "dataexchange:CreateDataSet"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyDevTools",
    "Effect": "Deny",
    "Action": [
        "amplify:CreateApp",
        "amplify:CreateBranch",
        "cloud9:CreateEnvironmentEC2",
        "codebuild:CreateProject",
        "codepipeline:CreatePipeline",
        "codedeploy:CreateApplication",
        "cloudformation:CreateStack",
        "cloudformation:CreateStackSet",
        "codeartifact:CreateRepository",
        "codeartifact:CreateDomain"
    ],
    "Resource": "*"
},
{
    "Sid": "DenySecurity",
    "Effect": "Deny",
    "Action": [
        "kms:CreateKey",
        "wafv2:CreateWebACL",
        "cloudhsm:CreateCluster",
        "network-firewall:CreateFirewall",
        "secretsmanager:CreateSecret",
        "acm-pca:CreateCertificateAuthority",
        "cognito-idp:CreateUserPool",
        "cognito-identity:CreateIdentityPool",
        "ds:CreateDirectory",
        "ds:CreateMicrosoftAD",
        "fms:PutPolicy",
        "payment-cryptography:CreateKey"
    ],
    "Resource": "*"
},
{

```

```
"Sid": "DenyMedia",
"Effect": "Deny",
"Action": [
    "medialive:CreateChannel",
    "mediapackage:CreateChannel",
    "mediaconnect:CreateFlow",
    "mediatailor:CreateChannel"
],
"Resource": "*"
},
{
    "Sid": "DenyIoT",
    "Effect": "Deny",
    "Action": [
        "iot:CreateThing",
        "iot:CreateTopicRule",
        "iotevents:CreateDetectorModel",
        "iottwinmaker:CreateWorkspace",
        "iotsitewise:CreateAssetModel",
        "iotsitewise:CreatePortal",
        "iotfleetwise:CreateCampaign"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyMisc",
    "Effect": "Deny",
    "Action": [
        "ses:CreateConfigurationSet",
        "ecr:CreateRepository",
        "aps:CreateWorkspace",
        "healthlake:CreateFHIRDatastore",
        "transfer:CreateServer",
        "managedblockchain:CreateNetwork",
        "managedblockchain:CreateMember",
        "route53-recovery-control-config:CreateCluster",
        "fis:CreateExperimentTemplate",
        "appfabric:CreateAppBundle",
        "appfabric:CreateIngestion",
        "b2bi:CreateProfile",
        "b2bi:CreateTransformer",
        "geo:CreateMap",
        "geo:CreatePlaceIndex",
        "geo:CreateTracker",
```

```
        "geo:CreateGeofenceCollection",
        "geo:CreateRouteCalculator"
    ],
    "Resource": "*"
}
]
```

プロジェクトの無料利用枠のサービスコントロールポリシー

次のサービスコントロールポリシーは、新しい AWS エクスペリエンスの無料利用枠で利用可能な AWS サービスへのアクセスを制御します。このポリシーは変更できません。追加のサービスにアクセスするには、アカウントをアップグレードします。詳細については、「[AWS 設定でアカウントをアップグレードする](#)」を参照してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowFreeTierServices",
      "Effect": "Deny",
      "NotAction": [
        "a2c:*",
        "access-analyzer:CheckAccessNotGranted",
        "access-analyzer:CheckNoNewAccess",
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:ValidatePolicy",
        "account:*",
        "acm:*",
        "aco-automation:*",
        "action-recommendations:*",
        "activate:*",
        "aiops:*",
        "airflow-serverless:*",
        "amplify:*",
        "amplifybackend:*",
        "amplifyuibuilder:*",
        "aoss:*",
        "apigateway:*",
        "app-integrations:*",
        "appconfig:*",
        "appflow:*",
        "application-autoscaling:*
```

```
"application-signals-mcp:*",
"application-signals:*",
"application-transformation:*",
"applicationinsights:*",
"appmesh:*",
"appsync:*",
"aps:*",
"arc-zonal-shift:*",
"artifact:*",
"athena:*",
"autoscaling-plans:*",
"autoscaling:*",
"aws-external-anthropic:*",
"aws-marketplace:*",
"b2bi:*",
"backup-gateway:*",
"backup-search:*",
"backup-storage:*",
"backup:*",
"batch:*",
"bcm-pricing-calculator:*",
"bedrock-agentcore:*",
"bedrock-mantle:*",
"bedrock-websearch:*",
"bedrock:*",
"budgets:*",
"ce:*",
"chatbot:*",
"cloud9:*",
"cloudformation:*",
"cloudfront-keyvaluestore:*",
"cloudfront:*",
"cloudshell:*",
"cloudtrail-data:*",
"cloudtrail:*",
"cloudwatch:*",
"codeartifact:*",
"codebuild:*",
"codecommit:*",
"codeconnections:*",
"codedeploy-commands-secure:*",
"codedeploy:*",
"codepipeline:*",
"codestar-connections:*
```

```
"codestar-notifications:*",
"cognito-identity:*",
"cognito-idp:*",
"cognito-sync:*",
"compute-optimizer:*",
"config:*",
"consoleapp:*",
"consolidatedbilling:*",
"cost-optimization-hub:*",
"customer-verification:*",
"databrew:*",
"datapipeline:*",
"datasync:*",
"datazone:*",
"dbqms:*",
"dlm:*",
"ds-data:*",
"ds:*",
"dsql:*",
"dynamodb:*",
"ebs:*",
"ec2-instance-connect:*",
"ec2:*",
"ec2messages:*",
"ecr-public:*",
"ecr:*",
"ecs-mcp:*",
"ecs:*",
"eks-auth:*",
"eks-mcp:*",
"eks:*",
"elasticache:*",
"elasticbeanstalk:*",
"elasticfilesystem:*",
"elasticloadbalancing:*",
"entityresolution:*",
"es:*",
"events:*",
"evidently:*",
"execute-api:*",
"finops-agent:*",
"freertos:*",
"freetier:*",
"geo-maps:*
```

```
"geo-places:*",
"geo-routes:*",
"geo:*",
"glue:*",
"groundtruthlabeling:*",
"health:*",
"iam:*",
"identitystore-auth:*",
"identitystore:*",
"imagebuilder:*",
"internetmonitor:*",
"invoicing:*",
"iot-device-tester:*",
"iot:*",
"iotdeviceadvisor:*",
"iotfleethub:*",
"iotjobsdata:*",
"iotmanagedintegrations:*",
"iotsitewise:*",
"iottwinmaker:*",
"iotwireless:*",
"kms:*",
"lakeformation:*",
"lambda:*",
"launchwizard:*",
"lex:*",
"license-manager-linux-subscriptions:*",
"license-manager-user-subscriptions:*",
"license-manager:*",
"logs:*",
"mgn:*",
"migrationhub-orchestrator:*",
"migrationhub-strategy:*",
"mpa:*",
"mq:*",
"networkflowmonitor:*",
"networkmanager-chat:*",
"networkmanager:*",
"networkmonitor:*",
"notifications-contacts:*",
"notifications:*",
"nova-act:*",
"oam:*",
"observabilityadmin:*,
```

```
"opensearch:*",
"organizations:*",
"osis:*",
"payment-cryptography:*",
"pi:*",
"pipes:*",
"polly:*",
"pricing:*",
"q:DeleteConversation",
"q:GenerateCodeFromCommands",
"q:GenerateCodeRecommendations",
"q:GetConversation",
"q:GetIdentityMetadata",
"q:GetTroubleshootingResults",
"q:ListConversations",
"q:PassRequest",
"q:SendEvent",
"q:SendMessage",
"q:StartConversation",
"q:StartTroubleshootingAnalysis",
"q:StartTroubleshootingResolutionExplanation",
"q:UpdateConversation",
"q:UpdateTroubleshootingCommandResult",
"q:UsePlugin",
"ram:*",
"rbin:*",
"rds-data:*",
"rds-db:*",
"rds:*",
"rekognition:*",
"resource-explorer-2:*",
"resource-explorer:*",
"resource-groups:*",
"rhelkb:*",
"route53-recovery-cluster:*",
"route53-recovery-control-config:*",
"route53-recovery-readiness:*",
"route53:*",
"route53domains:*",
"route53globalresolver:*",
"route53profiles:*",
"route53resolver:*",
"rum:*",
"s3-object-lambda:*",
```



```
"s3:*",
"s3express:*",
"s3files:*",
"s3tables:*",
"s3vectors:*",
"sagemaker-data-science-assistant:*",
"sagemaker-geospatial:*",
"sagemaker-mlflow:*",
"sagemaker-unified-studio-mcp:*",
"sagemaker:*",
"scheduler:*",
"schemas:*",
"secretsmanager:*",
"serverlessrepo:*",
"servicecatalog:Describe*",
"servicecatalog:List*",
"servicecatalog:ProvisionProduct",
"servicecatalog:ScanProvisionedProducts",
"servicecatalog:SearchProducts",
"servicecatalog:SearchProvisionedProducts",
"servicecatalog:TerminateProvisionedProduct",
"servicecatalog:UpdateProvisionedProduct",
"servicediscovery:*",
"serviceextract:*",
"servicequotas:*",
"ses:*",
"signer:*",
"signin:*",
"sns:*",
"sqlworkbench:*",
"sqs:*",
"ssm-contacts:*",
"ssm-guiconnect:*",
"ssm-incidents:*",
"ssm-quicksetup:*",
"ssm-sap:*",
"ssm:*",
"ssmmessages:*",
"sso-directory:*",
"sso-oauth:*",
"sso:*",
"states:*",
"sts:*",
"support:*",
```

```

        "swf:*",
        "synthetics:*",
        "tag:*",
        "tax:*",
        "timestream-influxdb:*",
        "ts:*",
        "uxc:*",
        "verifiedpermissions:*",
        "vpce:*",
        "waf-regional:*",
        "waf:*",
        "wafv2:*",
        "wellarchitected:*",
        "xray:*"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyEC2CapacityBlock",
    "Effect": "Deny",
    "Action": ["ec2:PurchaseCapacityBlock", "ec2:PurchaseCapacityBlockExtension"],
    "Resource": "*"
},
{
    "Sid": "DenyRestrictedAgreements",
    "Effect": "Deny",
    "Action": ["artifact:AcceptAgreement", "artifact:AcceptNdaForAgreement"],
    "Resource": [
        "arn:aws:artifact::agreement/agreement-9c1kBcYznTkcpRIm",
        "arn:aws:artifact::agreement/agreement-y03aUwMAEorHtqjv",
        "arn:aws:artifact::agreement/agreement-bexgr7sjvXAW4Gxu",
        "arn:aws:artifact::agreement/agreement-HZTdNwJuq0KLReXC"
    ]
},
{
    "Sid": "DenyDocDB",
    "Effect": "Deny",
    "Action": ["rds:CreateDBCluster", "rds:CreateDBInstance"],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "rds:DatabaseEngine": ["docdb"]
        }
    }
}

```

```
},
{
  "Sid": "DenyCloudWAN",
  "Effect": "Deny",
  "Action": [
    "networkmanager:CreateCoreNetwork",
    "networkmanager:CreateConnectAttachment",
    "networkmanager:CreateConnectPeer",
    "networkmanager:CreateVpcAttachment",
    "networkmanager:CreateSiteToSiteVpnAttachment",
    "networkmanager:CreateTransitGatewayPeering",
    "networkmanager:CreateDirectConnectGatewayAttachment",
    "networkmanager:PutCoreNetworkPolicy",
    "networkmanager:ExecuteCoreNetworkChangeSet"
  ],
  "Resource": "*"
},
{
  "Sid": "DenyTransitGatewayAndVPN",
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTransitGateway",
    "ec2:CreateTransitGatewayVpcAttachment",
    "ec2:CreateTransitGatewayConnect",
    "ec2:CreateTransitGatewayConnectPeer",
    "ec2:CreateTransitGatewayMulticastDomain",
    "ec2:CreateTransitGatewayPeeringAttachment",
    "ec2:CreateTransitGatewayPolicyTable",
    "ec2:CreateTransitGatewayPrefixListReference",
    "ec2:CreateTransitGatewayRoute",
    "ec2:CreateTransitGatewayRouteTable",
    "ec2:CreateTransitGatewayRouteTableAnnouncement",
    "ec2:CreateClientVpnEndpoint",
    "ec2:CreateClientVpnRoute",
    "ec2:AuthorizeClientVpnIngress",
    "ec2:AssociateClientVpnTargetNetwork",
    "ec2:CreateVpnConnection",
    "ec2:CreateVpnConnectionRoute",
    "ec2:CreateVpnGateway",
    "ec2:CreateCustomerGateway"
  ],
  "Resource": "*"
},
{
```

```
"Sid": "DenySageMakerGroundTruth",
"Effect": "Deny",
"Action": [
    "sagemaker:CreateLabelingJob",
    "sagemaker:CreateWorkteam",
    "sagemaker:CreateWorkforce",
    "sagemaker:CreateHumanTaskUi"
],
"Resource": "*"
},
{
    "Sid": "DenyGlacierStorageClasses",
    "Effect": "Deny",
    "Action": ["s3:PutObject"],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "s3:x-amz-storage-class": ["DEEP_ARCHIVE", "GLACIER"]
        }
    }
},
{
    "Sid": "DenyEC2Fleet",
    "Effect": "Deny",
    "Action": ["ec2:CreateFleet"],
    "Resource": "*"
},
{
    "Sid": "DenyEC2BYOLAndLicenseConfigurations",
    "Effect": "Deny",
    "Action": ["ec2:RunInstances", "ec2:StartInstances"],
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
        "StringEquals": {
            "ec2:Tenancy": "host"
        }
    }
},
{
    "Sid": "DenyEC2InstanceStoreRootDevice",
    "Effect": "Deny",
    "Action": ["ec2:RunInstances"],
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
```

```

        "StringEquals": {
            "ec2:RootDeviceType": "instance-store"
        }
    },
    {
        "Sid": "DenyLicenseManagerAssociation",
        "Effect": "Deny",
        "Action": ["license-manager:CreateLicenseConfiguration"],
        "Resource": "*"
    },
    {
        "Sid": "DenyIAMRestrictedActions",
        "Effect": "Deny",
        "Action": [
            "iam:*Alias*",
            "iam:*Organizations*",
            "iam:*Provider*",
            "iam:SetSecurityTokenServicePreferences",
            "iam:*LoginProfile*",
            "iam:CreateGroup",
            "iam:AttachGroupPolicy",
            "iam:AddUserToGroup",
            "iam:PutGroupPolicy",
            "iam:UpdateGroup",
            "iam:UpdateServerCertificate",
            "iam:UpdateSigningCertificate",
            "iam:UploadServerCertificate",
            "iam:UploadSigningCertificate",
            "iam:TagServerCertificate",
            "iam:UntagServerCertificate"
        ],
        "Resource": "*"
    },
    {
        "Sid": "DenySSOCreateInstance",
        "Effect": "Deny",
        "Action": ["sso:CreateInstance"],
        "Resource": "*"
    },
    {
        "Sid": "DenyRequestSpotInstances",
        "Effect": "Deny",
        "Action": ["ec2:RequestSpotInstances"],
    }

```

```
"Resource": "*"
},
{
  "Sid": "DenySpotMarketType",
  "Effect": "Deny",
  "Action": ["ec2:RunInstances"],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "ec2:InstanceMarketType": "spot"
    }
  }
},
{
  "Sid": "DenyReservedInstanceAndCapacityPurchases",
  "Effect": "Deny",
  "Action": [
    "athena:CreateCapacityReservation",
    "cloudfront:CreateSavingsPlan",
    "dynamodb:PurchaseReservedCapacityOfferings",
    "ec2:AllocateHosts",
    "ec2:CreateCapacityReservation",
    "ec2:CreateCapacityReservationBySplitting",
    "ec2:CreateCapacityReservationCancellationQuote",
    "ec2:CreateCapacityReservationFleet",
    "ec2:PurchaseHostReservation",
    "ec2:PurchaseReservedInstancesOffering",
    "ec2:PurchaseScheduledInstances",
    "elasticache:PurchaseReservedCacheNodesOffering",
    "es:PurchaseReservedElasticsearchInstanceOffering",
    "es:PurchaseReservedInstanceOffering",
    "glacier:PurchaseProvisionedCapacity",
    "memorydb:PurchaseReservedNodesOffering",
    "rds:PurchaseReservedDBInstancesOffering",
    "redshift:AcceptReservedNodeExchange",
    "redshift:PurchaseReservedNodeOffering",
    "sagemaker:CreateReservedCapacity",
    "savingsplans:CreateSavingsPlan"
  ],
  "Resource": "*"
},
{
  "Sid": "DenyExportableCertificateRequests",
  "Effect": "Deny",
```

```
    "Action": ["acm:RequestCertificate"],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "acm:AllowExport": "true"
      }
    }
  }
}
```

プロジェクトの有料プランのサービスコントロールポリシー

次のサービスコントロールポリシーは、新しい AWS エクスペリエンスの有料プランで利用可能な AWS サービスへのアクセスを制御します。このポリシーは変更できません。追加のサービスにアクセスするには、高度な機能をアクティブ化します。詳細については、「[高度な AWS 機能をアクティブ化する](#)」を参照してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPaidTierServices",
      "Effect": "Deny",
      "NotAction": [
        "a2c:*",
        "access-analyzer:CheckAccessNotGranted",
        "access-analyzer:CheckNoNewAccess",
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:ValidatePolicy",
        "account:*",
        "acm:*",
        "aco-automation:*",
        "action-recommendations:*",
        "activate:*",
        "aidevops:*",
        "aiops:*",
        "airflow-serverless:*",
        "amplify:*",
        "amplifybackend:*",
        "amplifyuibuilder:*",
        "aoss:*",
        "apigateway:*
```

```
"app-integrations:*",
"appconfig:*",
"appfabric:*",
"appflow:*",
"application-autoscaling:*",
"application-signals-mcp:*",
"application-signals:*",
"application-transformation:*",
"applicationinsights:*",
"appmesh:*",
"appsync:*",
"aps:*",
"arc-zonal-shift:*",
"artifact:*",
"athena:*",
"autoscaling-plans:*",
"autoscaling:*",
"aws-external-anthropic:*",
"aws-marketplace:*",
"b2bi:*",
"backup-gateway:*",
"backup-search:*",
"backup-storage:*",
"backup:*",
"batch:*",
"bcm-pricing-calculator:*",
"bedrock-agentcore:*",
"bedrock-mantle:*",
"bedrock-websearch:*",
"bedrock:*",
"budgets:*",
"ce:*",
"chatbot:*",
"cloud9:*",
"cloudformation:*",
"cloudfront-keyvaluestore:*",
"cloudfront:*",
"cloudshell:*",
"cloudtrail-data:*",
"cloudtrail:*",
"cloudwatch:*",
"codeartifact:*",
"codebuild:*",
"codecommit:*
```



```
"codeconnections:*",
"codedeploy-commands-secure:*",
"codedeploy:*",
"codeguru-profiler:*",
"codeguru-reviewer:*",
"codeguru-security:*",
"codepipeline:*",
"codestar-connections:*",
"codestar-notifications:*",
"cognito-identity:*",
"cognito-idp:*",
"cognito-sync:*",
"compute-optimizer:*",
"config:*",
"consoleapp:*",
"consolidatedbilling:*",
"cost-optimization-hub:*",
"customer-verification:*",
"databrew:*",
"dataexchange:*",
"datapipeline:*",
"datasync:*",
"datazone:*",
"dbqms:*",
"devops-guru:*",
"dlm:*",
"docdb-elastic:*",
"ds-data:*",
"ds:*",
"dsql:*",
"dynamodb:*",
"ebs:*",
"ec2-instance-connect:*",
"ec2:*",
"ec2messages:*",
"ecr-public:*",
"ecr:*",
"ecs-mcp:*",
"ecs:*",
"eks-auth:*",
"eks-mcp:*",
"eks:*",
"elasticache:*",
"elasticbeanstalk:*",
```

```
"elasticfilesystem:*",
"elasticloadbalancing:*",
"elasticmapreduce:*",
"emr-containers:*",
"emr-serverless:*",
"entityresolution:*",
"es:*",
"events:*",
"evidently:*",
"execute-api:*",
"finops-agent:*",
"firehose:*",
"fis:*",
"fms:*",
"forecast:*",
"freertos:*",
"freetier:*",
"geo-maps:*",
"geo-places:*",
"geo-routes:*",
"geo:*",
"glacier:*",
"glue:*",
"groundtruthlabeling:*",
"health:*",
"iam:*",
"identitystore-auth:*",
"identitystore:*",
"imagebuilder:*",
"internetmonitor:*",
"invoicing:*",
"iot-device-tester:*",
"iot:*",
"iotdeviceadvisor:*",
"iotfleethub:*",
"iotjobsdata:*",
"iotmanagedintegrations:*",
"iotsitewise:*",
"iottwinmaker:*",
"iotwireless:*",
"kafka-cluster:*",
"kafka:*",
"kafkaconnect:*",
"kinesis:*,
```

```
"kinesisanalytics:*",
"kinesisvideo:*",
"kms:*",
"lakeformation:*",
"lambda:*",
"launchwizard:*",
"lex:*",
"license-manager-linux-subscriptions:*",
"license-manager-user-subscriptions:*",
"license-manager:*",
"logs:*",
"managedblockchain-query:*",
"managedblockchain:*",
"mapcredits:*",
"memorydb:*",
"mgn:*",
"migrationhub-orchestrator:*",
"migrationhub-strategy:*",
"mpa:*",
"mq:*",
"neptune-db:*",
"neptune-graph:*",
"network-firewall:*",
"networkflowmonitor:*",
"networkmanager-chat:*",
"networkmanager:*",
"networkmonitor:*",
"notifications-contacts:*",
"notifications:*",
"nova-act:*",
"oam:*",
"observabilityadmin:*",
"opensearch:*",
"organizations:*",
"osis:*",
"payment-cryptography:*",
"personalize:*",
"pi:*",
"pipes:*",
"polly:*",
"pricing:*",
"q:DeleteConversation",
"q:GenerateCodeFromCommands",
"q:GenerateCodeRecommendations",
```

```
"q:GetConversation",
"q:GetIdentityMetadata",
"q:GetTroubleshootingResults",
"q:ListConversations",
"q:PassRequest",
"q:SendEvent",
"q:SendMessage",
"q:StartConversation",
"q:StartTroubleshootingAnalysis",
"q:StartTroubleshootingResolutionExplanation",
"q:UpdateConversation",
"q:UpdateTroubleshootingCommandResult",
"q:UsePlugin",
"ram:*",
"rbin:*",
"rds-data:*",
"rds-db:*",
"rds:*",
"redshift-data:*",
"redshift-serverless:*",
"redshift:*",
"rekognition:*",
"resource-explorer-2:*",
"resource-explorer:*",
"resource-groups:*",
"rhelkb:*",
"route53-recovery-cluster:*",
"route53-recovery-control-config:*",
"route53-recovery-readiness:*",
"route53:*",
"route53domains:*",
"route53globalresolver:*",
"route53profiles:*",
"route53resolver:*",
"rum:*",
"s3-object-lambda:*",
"s3:*",
"s3express:*",
"s3files:*",
"s3tables:*",
"s3vectors:*",
"sagemaker-data-science-assistant:*",
"sagemaker-geospatial:*",
"sagemaker-mlflow:*,
```

```
"sagemaker-unified-studio-mcp:*",
"sagemaker:*",
"scheduler:*",
"schemas:*",
"secretsmanager:*",
"securityagent:*",
"serverlessrepo:*",
"servicecatalog:Describe*",
"servicecatalog:List*",
"servicecatalog:ProvisionProduct",
"servicecatalog:ScanProvisionedProducts",
"servicecatalog:SearchProducts",
"servicecatalog:SearchProvisionedProducts",
"servicecatalog:TerminateProvisionedProduct",
"servicecatalog:UpdateProvisionedProduct",
"servicediscovery:*",
"serviceextract:*",
"servicequotas:*",
"ses:*",
"signer:*",
"signin:*",
"sms-voice:*",
"sns:*",
"social-messaging:*",
"sqlworkbench:*",
"sqs:*",
"ssm-contacts:*",
"ssm-guiconnect:*",
"ssm-incidents:*",
"ssm-quicksetup:*",
"ssm-sap:*",
"ssm:*",
"ssmmessages:*",
"sso-directory:*",
"sso-oauth:*",
"sso:*",
"states:*",
"storagegateway:*",
"sts:*",
"support:*",
"swf:*",
"synthetics:*",
>tag:*",
"tax:*
```

```

        "textract:*",
        "timestream-influxdb:*",
        "timestream:*",
        "transcribe:*",
        "translate:*",
        "ts:*",
        "uxc:*",
        "verifiedpermissions:*",
        "vpce:*",
        "waf-regional:*",
        "waf:*",
        "wafv2:*",
        "wellarchitected:*",
        "xray:*"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyEC2CapacityBlock",
    "Effect": "Deny",
    "Action": ["ec2:PurchaseCapacityBlock", "ec2:PurchaseCapacityBlockExtension"],
    "Resource": "*"
},
{
    "Sid": "DenyRestrictedAgreements",
    "Effect": "Deny",
    "Action": ["artifact:AcceptAgreement", "artifact:AcceptNdaForAgreement"],
    "Resource": [
        "arn:aws:artifact::agreement/agreement-9c1kBcYznTkcpRIm",
        "arn:aws:artifact::agreement/agreement-y03aUwMAEorHtqjv",
        "arn:aws:artifact::agreement/agreement-bexgr7sjvXAW4Gxu",
        "arn:aws:artifact::agreement/agreement-HZTdNwJuq0KLReXC"
    ]
},
{
    "Sid": "DenyCloudWAN",
    "Effect": "Deny",
    "Action": [
        "networkmanager:CreateCoreNetwork",
        "networkmanager:CreateConnectAttachment",
        "networkmanager:CreateConnectPeer",
        "networkmanager:CreateVpcAttachment",
        "networkmanager:CreateSiteToSiteVpnAttachment",
        "networkmanager:CreateTransitGatewayPeering",
    ]
}

```

```

        "networkmanager:CreateDirectConnectGatewayAttachment",
        "networkmanager:PutCoreNetworkPolicy",
        "networkmanager:ExecuteCoreNetworkChangeSet"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyTransitGatewayAndVPN",
    "Effect": "Deny",
    "Action": [
        "ec2:CreateTransitGateway",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:CreateTransitGatewayConnect",
        "ec2:CreateTransitGatewayConnectPeer",
        "ec2:CreateTransitGatewayMulticastDomain",
        "ec2:CreateTransitGatewayPeeringAttachment",
        "ec2:CreateTransitGatewayPolicyTable",
        "ec2:CreateTransitGatewayPrefixListReference",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:CreateClientVpnEndpoint",
        "ec2:CreateClientVpnRoute",
        "ec2:AuthorizeClientVpnIngress",
        "ec2:AssociateClientVpnTargetNetwork",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:CreateCustomerGateway"
    ],
    "Resource": "*"
},
{
    "Sid": "DenySageMakerGroundTruth",
    "Effect": "Deny",
    "Action": [
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateWorkteam",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateHumanTaskUi"
    ],
    "Resource": "*"
},
{

```

```
"Sid": "DenyEC2Fleet",
"Effect": "Deny",
"Action": ["ec2:CreateFleet"],
"Resource": "*"
},
{
  "Sid": "DenyEC2BYOLAndLicenseConfigurations",
  "Effect": "Deny",
  "Action": ["ec2:RunInstances", "ec2:StartInstances"],
  "Resource": "arn:aws:ec2:*:*:instance/*",
  "Condition": {
    "StringEquals": {
      "ec2:Tenancy": "host"
    }
  }
},
{
  "Sid": "DenyEC2InstanceStoreRootDevice",
  "Effect": "Deny",
  "Action": ["ec2:RunInstances"],
  "Resource": "arn:aws:ec2:*:*:instance/*",
  "Condition": {
    "StringEquals": {
      "ec2:RootDeviceType": "instance-store"
    }
  }
},
{
  "Sid": "DenyLicenseManagerAssociation",
  "Effect": "Deny",
  "Action": ["license-manager:CreateLicenseConfiguration"],
  "Resource": "*"
},
{
  "Sid": "DenyIAMRestrictedActions",
  "Effect": "Deny",
  "Action": [
    "iam:*Alias*",
    "iam:*Organizations*",
    "iam:*Provider*",
    "iam:SetSecurityTokenServicePreferences",
    "iam:*LoginProfile*",
    "iam:CreateGroup",
    "iam:AttachGroupPolicy",
```



```
    "iam:AddUserToGroup",
    "iam:PutGroupPolicy",
    "iam:UpdateGroup",
    "iam:UpdateServerCertificate",
    "iam:UpdateSigningCertificate",
    "iam:UploadServerCertificate",
    "iam:UploadSigningCertificate",
    "iam:TagServerCertificate",
    "iam:UntagServerCertificate"
  ],
  "Resource": "*"
},
{
  "Sid": "DenySSOCreateInstance",
  "Effect": "Deny",
  "Action": ["sso:CreateInstance"],
  "Resource": "*"
},
{
  "Sid": "DenyRequestSpotInstances",
  "Effect": "Deny",
  "Action": ["ec2:RequestSpotInstances"],
  "Resource": "*"
},
{
  "Sid": "DenySpotMarketType",
  "Effect": "Deny",
  "Action": ["ec2:RunInstances"],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "ec2:InstanceMarketType": "spot"
    }
  }
},
{
  "Sid": "DenyReservedInstanceAndCapacityPurchases",
  "Effect": "Deny",
  "Action": [
    "athena:CreateCapacityReservation",
    "cloudfront:CreateSavingsPlan",
    "dynamodb:PurchaseReservedCapacityOfferings",
    "ec2:AllocateHosts",
    "ec2:CreateCapacityReservation",
```

```

    "ec2:CreateCapacityReservationBySplitting",
    "ec2:CreateCapacityReservationCancellationQuote",
    "ec2:CreateCapacityReservationFleet",
    "ec2:PurchaseHostReservation",
    "ec2:PurchaseReservedInstancesOffering",
    "ec2:PurchaseScheduledInstances",
    "elasticache:PurchaseReservedCacheNodesOffering",
    "es:PurchaseReservedElasticsearchInstanceOffering",
    "es:PurchaseReservedInstanceOffering",
    "glacier:PurchaseProvisionedCapacity",
    "memorydb:PurchaseReservedNodesOffering",
    "rds:PurchaseReservedDBInstancesOffering",
    "redshift:AcceptReservedNodeExchange",
    "redshift:PurchaseReservedNodeOffering",
    "sagemaker:CreateReservedCapacity",
    "savingsplans:CreateSavingsPlan"
  ],
  "Resource": "*"
},
{
  "Sid": "DenyExportableCertificateRequests",
  "Effect": "Deny",
  "Action": ["acm:RequestCertificate"],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "acm:AllowExport": "true"
    }
  }
}
]
}

```

プロジェクトのリソースコントロールポリシー

以下は、[プロジェクト内のリソースのリソース](#)コントロールポリシーです。このポリシーは変更できません。

```

{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DenyAnyoneOutsideMyOrgAndAWS",

```

```
"Effect" : "Deny",
"Principal" : "*",
"Action" : [
  "aoss:*",
  "appconfig:*",
  "appstream:*",
  "autoscaling:*",
  "codebuild:*",
  "codecommit:*",
  "cognito-identity:*",
  "cognito-idp:*",
  "comprehend:*",
  "comprehendmedical:*",
  "dax:*",
  "dynamodb:*",
  "ecr:*",
  "health:*",
  "kinesisvideo:*",
  "kms:*",
  "logs:*",
  "s3:*",
  "secretsmanager:*",
  "sqs:*",
  "sts:*",
  "support:*",
  "textextract:*",
  "transcribe:*",
  "translate:*"
],
"Resource" : "*",
"Condition" : {
  "BoolIfExists" : {
    "aws:PrincipalIsAWSService" : "false"
  },
  "Null" : {
    "aws:PrincipalARN" : "false"
  },
  "StringNotEqualsIfExists" : {
    "aws:PrincipalOrgID" : "${aws:ResourceOrgID}"
  }
}
},
{
  "Sid" : "DenyAWSWhenItsNotMyOrgsSourceAccount",
```

```
"Effect" : "Deny",
"Principal" : "*",
"Action" : [
  "aoss:*",
  "appconfig:*",
  "appstream:*",
  "autoscaling:*",
  "codebuild:*",
  "codecommit:*",
  "cognito-identity:*",
  "cognito-idp:*",
  "comprehend:*",
  "comprehendmedical:*",
  "dax:*",
  "dynamodb:*",
  "ecr:*",
  "health:*",
  "kinesisvideo:*",
  "kms:*",
  "logs:*",
  "s3:*",
  "secretsmanager:*",
  "sqs:*",
  "sts:*",
  "support:*",
  "textract:*",
  "transcribe:*",
  "translate:*"
],
"Resource" : "*",
"Condition" : {
  "Null" : {
    "aws:SourceAccount" : "false"
  },
  "StringNotEquals" : {
    "aws:SourceOrgID" : "${aws:ResourceOrgID}"
  }
}
}
```

プロジェクトを切り替える

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

一度に管理できる AWS リソースは 1 つのプロジェクトのみです。コンソールの AWS 右上にある名前に基づいて、どのプロジェクトにいるかをいつでも確認できます。

からアクティブなセッションのプロジェクトを切り替える AWS マネジメントコンソール

からアクティブなセッションのプロジェクトを切り替えるには AWS マネジメントコンソール

1. [AWS マネジメントコンソール](#) を開きます。
2. の右上にあるプロジェクト名を選択します AWS マネジメントコンソール。
3. Switch project を選択します。
4. アクティブセッションで、アクティブなセッションを選択します。アクティブなセッションは、最大 12 時間サインインされたセッションです。アクティブなセッション時間は変更できません。
5. 新しいプロジェクトの AWS コンソールのホームページにリダイレクトされます。

AWS 設定でプロジェクトを切り替える

AWS 設定でプロジェクトを切り替えるには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、アクセスするプロジェクトを選択します。
3. 右上のナビゲーションバーで、クラウドインフラストラクチャの作成と管理を選択します。

AWS マネジメントコンソール 新しいプロジェクトの にリダイレクトされます。

からプロジェクトを切り替える AWS マネジメントコンソール

からプロジェクトを切り替えるには AWS マネジメントコンソール

1. [AWS マネジメントコンソール](#) を開きます。
2. プロジェクトの管理を選択します。
3. AWS 設定で、アクセスするプロジェクトを選択します。
4. 右上のナビゲーションバーで、クラウドインフラストラクチャの作成と管理を選択します。

AWS マネジメントコンソール 新しいプロジェクトの にリダイレクトされます。

チームメンバーを AWS 設定で共同作業に招待する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

チームメンバーにプロジェクトへのアクセスを許可できます。チームメンバーとプロジェクトを共有する場合、どの AWS サービスにアクセスできるかを制御することはできません。ユーザーとチームメンバーの両方が、プロジェクトへの管理者アクセス権を持ちます。つまり、チームメンバーには、プロジェクトで利用可能なすべての AWS サービスにアクセスするためのアクセス許可があります。これには、サービスとアプリケーションのアクセスコントロールの作成が含まれます。ただし、プロジェクトの削除や使用制限の変更など、管理上または財務上のアクションを実行するアクセス許可はありません。AWS サービスを変更したチームメンバーを確認するには、「」を参照してください [AWS CloudTrail を使用してプロジェクトをモニタリングする](#)。

AWS 「設定」では、ユーザーとチームメンバーのアクセスレベルは異なります。チームメンバーに適用される AWS 管理ポリシーを表示するには、「[AWSManagedSettingsReadOnlyAccess](#)」を参照してください。プロジェクト所有者に適用される AWS 管理ポリシーを表示するには、「[AWSManagedSettingsAdminAccess](#)」を参照してください。

チームメンバーをプロジェクトに追加するときは、次の点を考慮してください。

チームメンバーの考慮事項

チームメンバーは、次のアクションを実行できます。

- プロジェクト内の AWS リソースを表示、作成、編集、削除、および変更します。
- アクセス AWS 設定。
- 支出制限を表示します。
- AWS サービスのクォータの引き上げをリクエストします。

チームメンバーは、次のアクションを実行できません。

- プロジェクトを残します。
- ルートアクションを実行します。詳細については、「[AWS プロジェクト所有者の アクション](#)」を参照してください。
- チームメンバーをプロジェクトに招待します。
- チームメンバーのアクセス許可を管理します。
- プロジェクトからチームメンバーを削除します。
- プロジェクトの名前を変更します。
- 支払い方法をセットアップまたは更新します。
- 住所や電話番号など、請求の詳細を表示または更新します。
- 税金情報を表示または更新します。
- 無料利用枠から有料プランにアップグレードします。
- プロジェクトごとに支出制限を設定または変更します。
- 各プロジェクトのコスト傾向を表示します。
- すべてのプロジェクトの合計 AWS 支出を表示します。
- 無料利用枠以外のプロモーションクレジットを表示して引き換えます。
- すべてのクレジットタイプの残りのクレジットと有効期限を表示します。
- 獲得クレジット、適用クレジット、期限切れクレジットを含むクレジット履歴をすべて表示します。
- プロジェクト間でクレジットがどのように適用されるかをご覧ください。
- 未払い残高を表示します。
- への支払いを実行します AWS。
- 請求書をダウンロードするか、過去のトランザクションを表示します。
- 適用されるクレジットを含め、AWS 料金が正しいことを確認します。

- 管理アカウントレベルの請求通信を受信します。
- 組織レベルでの請求に関する問題に関するヘルプを参照してください。
- アカウントクォータと請求クォータのクォータ引き上げをリクエストします。

チームメンバーが AWS リソースにアクセスする方法

新しい AWS エクスペリエンスでは、変更できないすべてのプロジェクトを含む、組織のサービスにリンクされたロールが作成されます。このロールは、チームメンバーの内部レコードが実際のチームメンバーと同期していることを定期的に検証します。

AWSServiceRoleForAccountAccessManager サービスにリンクされたロールは、次のサービスを信頼してロールを引き受けます。

- `account-access.amazonaws.com`

という名前のロールアクセス許可ポリシー `AccountAccessManagerServiceRolePolicy` により、アカウントアクセスマネージャー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:
`organizations:ListAccounts`、`organizations:ListAWSServiceAccessForOrganization`、
ン `"arn:aws:organizations::*:account/o-*/*"`

詳細については、[AWS「Account Access Manager」](#)を参照してください。

チームメンバーを AWS 設定で共同作業に招待する

チームメンバーを招待するには、AWS 設定のチームページから招待を送信します。チームメンバーは招待を承諾するまでに 14 日間かかります。チームメンバーは、プロジェクトにアクセスするには AWS ビルダー ID を作成する必要があります。これは、[にサインアップ AWS \(新規\)](#) を使用して実行できます。

チームメンバーを AWS 設定で共同作業に招待する

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、チームを選択します。
3. 「新しいチームメンバーを招待する」を選択します。

4. Eメールの場合は、EメールアドレスまたはEメールアドレスのリストを入力します。Eメールアドレスはカンマ (,) またはセミコロン (;) で区切ります。
5. 新しいチームメンバーと共有するプロジェクトを1つ以上選択します。
6. [Send invitation] (招待の送信) を選択します。

チームメンバーに招待が届かない場合は、スパムフォルダとごみ箱フォルダを確認するよう依頼します。

AWS 設定でチームメンバーをプロジェクトに招待する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

チームメンバーを招待してプロジェクトにアクセスできます。プロジェクトでチームメンバーができることについては、「」を参照してください[チームメンバーを AWS 設定で共同作業に招待する](#)。

チームメンバーをプロジェクトに招待するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、アクセスするプロジェクトを選択します。
3. メンバーの場合は、新しいチームメンバーを招待を選択します。
4. Eメールの場合は、EメールアドレスまたはEメールアドレスのリストを入力します。Eメールアドレスはカンマ (,) またはセミコロン (;) で区切ります。
5. 新しいチームメンバーと共有するプロジェクトを選択します。
6. [Send invitation] (招待の送信) を選択します。

チームメンバーに招待が届かない場合は、迷惑メールフォルダとごみ箱フォルダを確認するように依頼します。

AWS 設定でプロジェクトからチームメンバーを削除する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

プロジェクトからチームメンバーはいつでも削除できます。チームメンバーは自分でこれを行うことはできません。チームメンバーを削除すると、そのチームメンバーはそのプロジェクトにアクセスできなくなります。チームメンバーが作成したリソースはプロジェクトに残り、管理する必要があります。

プロジェクトからチームメンバーを削除するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、アクセスするプロジェクトを選択します。
3. メンバータブで、プロジェクトから削除するメンバーを選択し、削除を選択します。
4. 選択を確認し、削除を選択します。

チームメンバーはチームの一部であり、他のプロジェクトに追加できます。AWS 設定からチームメンバーを完全に削除するには、「」を参照してください[AWS 設定でチームメンバーを削除する](#)。

AWS 設定でチームメンバーを削除する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

チームページを使用して、すべてのプロジェクトからチームメンバーを削除できます。プロジェクトへのアクセスは自動的に失われます。チームメンバーが作成したリソースは削除されません。

チームメンバーを削除するには

1. <https://settings.aws.com> で AWS 設定を開きます。

2. メインナビゲーションペインで、チームを選択します。
3. 削除するチームメンバーのチェックボックスをオンにします。
4. [を削除] を選択します。
5. 選択を確認し、削除を選択します。

AWS 設定でチームメンバーへの招待を取り消す

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

保留中の招待を取り消すことができます。招待は AWS 設定に 14 日間残ります。保留中の招待を取り消すと、招待メールのアクセスリンクは無効になります。承認された招待を取り消すことはできません。代わりにチームメンバーを削除してください。詳細については、「[AWS 設定でチームメンバーを削除する](#)」を参照してください。

招待を取り消すには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、チームを選択します。
3. 保留中の招待があるチームメンバーのチェックボックスをオンにします。
4. [取り消す] を選択します。
5. 選択を確認し、招待を取り消すを選択します。

AWS 設定でチームメンバーに招待を再送信する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

チームメンバーに、取り消し、期限切れ、または拒否された招待を再送信できます。招待を再送信すると、チームメンバーは招待を再送信してから 14 日後に有効期限が記載された新しい E メールを受け取ります。

招待を再送信するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、チームを選択します。
3. 招待が取り消された、期限切れになった、または拒否されたチームメンバーのチェックボックスをオンにします。
4. 再送信を選択します。
5. 選択を確認し、招待を再送信を選択します。

AWS 設定でアカウントをアップグレードする

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

Sign up for AWS (new) にサインアップすると、アカウントは無料利用枠に含まれます。無料利用枠では、100 USD のサインアップクレジットを受け取り、最大 100 USD の追加クレジットを獲得できます。クレジットが不足した場合、または 6 か月を超えるアカウントがある場合は、有料プランにアップグレードする必要があります。いつでも有料プランにアップグレードすることもできます。有料プランにアップグレードすると、「」に記載されているサービスにアクセスできます [AWS のサービス 新しい AWS エクスペリエンスの有料プランに含まれる](#)。

アカウントのアップグレードに関する考慮事項

有料プランにアップグレードする場合は、次の点を考慮してください。

- 個々のプロジェクトをアップグレードすることはできません。アカウントをアップグレードすると、すべてのプロジェクトがアップグレードされます。
- アップグレードすると、Always Free サービスと短期トライアルオファーにアクセスできます。
- 他のプロモーションクレジットや割引の対象となります。

- クレジット残高を超える料金を支払う必要があります。
- 支出制限を作成して、プロジェクトの 1 か月あたりの支払い額の上限を設定できます。詳細については、「[AWS 設定で使用制限を作成する](#)」を参照してください。
- プロジェクトを HIPAA または SEC 準拠として指定することはできません。
- クレジットが枯渇しても、アカウントは閉鎖されません。
- これにより、 にアップグレードされません [にサインアップする AWS \(アドバンスド\)](#)。を使用して作成されたアカウントでのみサポートされている機能は [にサインアップする AWS \(アドバンスド\)](#)、アカウントのアップグレード時に使用できなくなります。ただし、 アカウント [高度な AWS 機能をアクティブ化する](#) では 使用できます。
- アップグレードプロセスを元に戻すことはできません。

AWS 設定でアカウントをアップグレードする

アカウントをアップグレードするには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、請求を選択します。
3. [アップグレード] を選択します。
4. [開始する] を選択します。
5. 支払い方法を追加します。

お客様の所在地によっては、税金情報の提供が必要になる場合があります。

6. アカウントのアップグレードを選択します。
7. 「続行」を選択して構築に戻るか、「支出制限の設定」を選択して支出制限を設定します。使用制限の詳細については、「」を参照してください [AWS 設定で使用制限を作成する](#)。
8. コンソールに移動 を選択します。

アップグレードが完了しました。

AWS 設定で使用制限を作成する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

支出制限とは

支出制限により、デベロッパーは予測可能で管理された予算内で運用できるという確信 AWS を持つて使用できます。支出制限を使用して、プロジェクトの 1 か月あたりの支出制限を設定します。支出制限はプロジェクトレベルで設定します。一部のプロジェクトに支出制限を設定し、他のプロジェクトには支出制限を設定しないこともできます。

プロジェクトでの使用量が制限に達すると、はそのプロジェクトを AWS 一時停止してリソースを停止し、コストがその範囲内にとどまります。使用制限は、実験、学習、サンドボックスのワークロード向けに設計されています。これらは、アプリケーションに予期しないコストが発生した場合にリソースを短時間一時停止することが許容される本番環境に使用できます。

支出制限は、プロジェクトにアクセスできるすべてのユーザーに表示されますが、プロジェクト所有者のみが管理できます。支出制限を作成するには、有料プランに参加している必要があります。詳細については、「[AWS 設定でアカウントをアップグレードする](#)」を参照してください。

支出制限は [AWS Budgets](#) の一種です。

支出制限を設定する

使用制限は、プロジェクトの税引き前コストの上限であり、料金ではありません。支出制限を設定する場合、許容される最小値は 20 USD または予想される支出の控えめな見積もりのいずれか大きい方です。

最小が存在する理由: 支出制限に達することは破壊的な経験です。使用量の通常の変動が使用制限に達する可能性が低いように、最小値が存在します。

保守的な見積りの計算方法: 見積りは、これまでのアクティビティに基づいていますが、厳密な線形外挿ではありません。は、これまでの支出と現在実行しているリソース AWS を調べます。AWS また、は前月のアクティビティを使用します。高い場合は、最小値になります。

実行中のリソースが多数ある場合: 予想される支出の控えめな見積もりは高くなります。使用制限を低く設定する場合は、まずこれらのリソースを停止する必要があります。

一時停止したプロジェクトを再アクティブ化する場合: 予想される支出の控えめな見積もりは、その月のこれまでの支出と、課金されなかった使用量です。

Note

使用制限はクレジットを除外し、税引き前の料金に適用されます。

通知

実際のコストが上限の 50%、75%、90% に達した場合、または今後 10 日間に支出上限に達するか超える見込みの場合に通知が送信されます。

オプションの早期コストコントロールを使用して支出制限設定をカスタマイズする

使用制限により、請求額が設定した額を超えて増加することがなくなります。使用量に達すると、はリソースを AWS 一時停止して保護します。これらのオプションのコントロールはより早く、より緻密に動作するため、制限を大幅に下回ることができます。

新しいリソースの作成を停止する

制限に達する約 7 日前に、新しいリソースの起動が停止します。これは、によって管理されるサービスコントロールポリシーの適用によって実現されます AWS。サービスコントロールポリシーは、サービスによって異なります。プロジェクトに適用される可能性のあるすべてのサービスコントロールポリシーを表示するには、「」を参照してください [使用制限のサービスコントロールポリシー](#)。

すでに実行されているすべてのリソースは引き続き実行されます。ほとんどの場合、構築した内容は影響を受けません。ただし、場合によっては、これは破壊的なエクスペリエンスにつながる可能性があります。たとえば、自動スケーリングを有効にしている、このアクションを実行するための条件が満たされた場合、新しいインスタンスは起動しません。

アイドル状態のリソースを一時停止する

制限に達する約 5 日前に、アイドル状態のリソースは一時停止されます。アクティブなアプリケーションは実行し続けます。アイドル状態のリソースは、AWS Compute Optimizer の推奨事項に基づ

いて一時停止されます。詳細については、[「アイドル状態のレコメンデーションを表示する」](#)を参照してください。

プロジェクトにログインし、節約の機会を表示することで、アイドル状態のリソースのレコメンデーションを表示することもできます。詳細については、[「Cost Optimization Hub」](#)を参照してください。現時点では、支出制限エクスペリエンスの一環として、EC2、RDS、SageMaker エンドポイントを自動的に一時停止します。

EC2 インスタンスを一時停止する理由: 過去 14 日間のピーク CPU 使用率が 5% 未満で、ネットワーク I/O が 1 日あたり 5 MB 未満の場合、EC2 インスタンスを一時停止します。

G または P インスタンスタイプがある場合は、別のアイドル条件があります。G または P インスタンスタイプは、過去 14 日間に以下が当てはまる場合、一時停止されます。

- GPU ガルックバック期間の 99% 以上アクティブに動作していない
- GPU エンコーダーがインスタンスのランタイムの 99% 以上に使用されていない
- インスタンスレベルでの GPU メモリ使用量が 5% 未満
- CPU の最大使用率が 5% 未満
- ネットワーク使用率が 5 MB/日未満

RDS データベースを一時停止する理由: データベースインスタンスがリードレプリカではなく、過去 14 日間に次のものがある場合、RDS for MySQL と RDS for PostgreSQL を一時停止します。

- データベース接続なし
- CPU 使用率が低い
- 読み取り/書き込みアクティビティが少ない

アイドル状態の SageMaker エンドポイントを一時停止する理由: 過去 14 日間にエンドポイントの呼び出しがゼロの場合、SageMaker エンドポイントを一時停止します。

上位のコスト要因を一時停止する

制限に達する約 4 日前に、アクティブなリソースが発生する最大コストが一時的に停止されます。これは破壊的な経験になる可能性があります。現時点では、EC2、RDS、Lambda、Bedrock、SageMaker の 5 つのサービスからリソースを選択します。このオプトインコントロールにより、Lambda の暴走や予期しない Bedrock の急増が発生した場合にコストが発生するのを防ぐことができます。

制限に達したらどうなるか

AWS はプロジェクトを一時停止し、すべてのリソースを停止します。データは保持されます。

プロジェクトを再アクティブ化するには、AWS 設定から支出制限を増やします。再アクティブ化後、一部のリソースを手動で再起動する必要がある場合があります。

Important

プロジェクトが一時停止されてから 90 日以内にアクションを実行しない場合、プロジェクトデータ AWS を完全に削除します。

その他の重要な注意事項

- Amazon Route 53 を使用する場合は、24 時間ごとに 1 つのドメインしか購入できません。ドメインのコストが使用制限内であることを確認する必要があります。そうしないと、ドメインの購入は実行されません。このような場合は、購入する前に支出制限を増やす必要があります。
- 最大 10 個のプロジェクトに支出制限を適用できます。

AWS 設定で使用制限を作成する

AWS 設定で使用制限を作成するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、請求を選択します。
3. 「プロジェクト別のコスト」の「使用制限」で、「プロジェクトの制限を設定する」を選択します。
4. 推奨支出制限またはカスタム制限を選択できます。
5. カスタム制限を選択した場合は、カスタム金額を入力します。
6. 支出制限の設定を選択します。
7. 早期のコストコントロールで支出制限をカスタマイズするには、新しいリソースの起動を停止、アイドル状態のリソースを一時停止、またはトップコストドライバーを一時停止を選択します。
8. 「早期コストコントロールの保存」を選択します。

使用制限はすぐに有効になります。

AWS 設定で使用制限を更新する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

プロジェクト所有者は、AWS 設定でいつでも使用制限を更新できます。支出制限を増減したり、オプションの早期コストコントロールを変更したりできます。制限に近づいているために AWS が新しいリソースの起動をブロックしたり、リソースを一時停止したりした場合は、使用制限を増やすことができます。制限に達したためにプロジェクトが一時的に停止した場合は、使用制限を増やしてプロジェクトを再アクティブ化します。支出制限の仕組みの詳細については、「」を参照してください[AWS 設定で使用制限を作成する](#)。

AWS 設定で使用制限を更新する

使用制限を更新するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、請求を選択します。
3. 「プロジェクト別のコスト」の「使用制限」で、鉛筆アイコンを選択します。
4. 月額使用制限 (USD) には、新しい使用制限を入力します。

現在の支出に基づいてレコメンデーションを提供します。

5. プロジェクトで必要な保護を変更するには、新しいリソースの起動を停止、アイドル状態のリソースを一時停止、またはトップコストドライバーを一時停止を選択します。
6. [設定を保存] を選択します。

使用制限の変更はすぐに有効になります。

AWS 設定で使用制限を削除する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

プロジェクト所有者は、AWS 設定でいつでも使用制限を削除できます。支出制限を削除すると、AWS はコストをモニタリングしたり、プロジェクトのコストを早期に制御したりしなくなります。支出制限の仕組みの詳細については、「」を参照してください[AWS 設定で使用制限を作成する](#)。

AWS 設定で使用制限を削除する

使用制限を削除するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、請求を選択します。
3. 「プロジェクト別のコスト」の「使用制限」で、鉛筆アイコンを選択します。
4. 制限の削除を選択します。
5. 選択を確認し、削除を選択します。

使用制限はすぐに削除されます。

新しい AWS エクスペリエンスの無料利用枠

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

AWS 無料利用枠を使用して、コストコミットメントなしで AWS のサービスを調べることができます。を初めて使用する場合は AWS、アカウントプランに関係なく、アカウントの作成後に 100 USD のクレジットを受け取ります。アクティビティを完了することで、すべてのプロジェクトで最大 100

USD の追加のクレジットを獲得することもできます。追加クレジットの獲得に関する詳細については、「[追加のクレジットの獲得](#)」を参照してください。さらに、毎月の無料利用制限を提供する 30 を超える常時無料 AWS サービスにアクセスできます。

無料アカウントプランは、AWS サービスを試し、概念実証を最大 6 か月間無料で構築するお客様に最適です。有料アカウントプランにアップグレードするまでは、この期間中に料金が発生することはありません。無料アカウントプランは、6 か月後、またはクレジットを全額使用したときのいずれか早い時点で終了します。さらに、無料アカウントプランは、AWS 無料利用枠のクレジット額全体、またはハードウェア購入を迅速に消費する特定の AWS サービスにアクセスできません。無料アカウントプランの対象となるサービスのリストについては、「[にサインアップするためのサポート対象 AWS サービス AWS \(新規\)](#)」を参照してください。

[有料アカウントプラン] は、初回クレジット額を超えてスケールする本番環境アプリケーションの構築に最適です。使用量がクレジット残高を超えた場合、またはクレジットが適用されないサービスを使用する場合、pay-as-you-go料金を支払います。

所有しているすべてのプロジェクトは、同じプランタイプになります。有料アカウントプランにアップグレードすると、すべてのプロジェクトが追加の サービスにアクセスでき、すべてのプロジェクトに対してpay-as-you-go標準料金を支払います。詳細については、「[設定](#)」の AWS 「[アカウントのアップグレード](#)」を参照してください。

コスト管理コンソールを使用して、プロジェクトの無料利用枠を提供するすべての AWS サービスの使用状況を追跡できます。

無料利用枠の使用状況の追跡

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

AWS 無料利用枠の使用アラートは、各サービスの無料利用枠の上限の 85% を超えると、E メールで自動的に通知します。追加の追跡のために、支出予算をゼロに設定することで、使用量を無料利用枠の上限の 100% まで追跡するようにを設定できます。予算をフィルタリングして個々のサービスを追跡することも可能です。

AWS 無料利用枠の使用状況は、次の方法で追跡できます。

AWS 設定の使用

AWS 設定で、無料アカウントプランの有効期限、クレジット残高、残り日数をモニタリングできます。詳細については、「[AWS 設定でクレジットを表示して引き換える](#)」を参照してください。また、クレジット残高に関する E メールアラートや、無料アカウントプラン期間の終了が近づいたときの E メールアラートも定期的に送信されます。

有料プランがある場合は、AWS 設定のクレジットページでクレジット残高と有効期限をモニタリングできます。有料プランへのアップグレードの詳細については、「」を参照してください[AWS 設定でアカウントをアップグレードする](#)。

請求情報とコスト管理コンソールの使用

Billing and Cost Management Console を使用して、各プロジェクトの無料利用枠の使用状況を追跡できます。請求情報とコスト管理コンソールには、過去 month-to-date の使用状況と、使用制限以上のサービス提供の概要が表示されます。使用中の無料利用枠オファーごとに、以下を表示できます。

- サービス
- AWS 無料利用枠の使用制限
- 現在の使用状況
- 予測使用量
- month-to-date (MTD) の実際の使用量
- 予測month-to-date (MTD) 使用量

次の手順では、請求情報とコスト管理コンソールを使用して、無料利用枠の使用状況をmonth-to-date使用量でソートする方法を示します。

無料利用枠の使用状況をソートするには

1. <https://console.aws.amazon.com/cost-management/> で Billing and Cost Management コンソールを開きます。
2. 無料利用枠を選択します。
3. month-to-date実際の使用状況でソートするには、MTD の実際の使用状況の割合を選択します。

追加のクレジットの獲得

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

新規の AWS お客様は、アクティビティを完了することで、アカウントプランに関係なく 100 USD のクレジットを追加で獲得できます。これらのアクティビティは、AWS サービスの学習に役立ちます。アクティビティは、AWS コンソールホームダッシュボードの Explore AWS ウィジェットにあります。これらのアクティビティはすべて、AWS 無料利用枠クレジットから差し引かれた AWS サービス料金が発生しますが、各アクティビティを完了すると、20 USD のクレジットを受け取ります。

完了するアクティビティ

- [Amazon EC2 を使用してインスタンスを起動する](#)
- [Amazon Bedrock プレイグラウンドで基盤モデルを使用する](#)
- [予算を作成する](#)
- [Lambda を使用してウェブアプリケーションを作成する](#)
- [Amazon RDS データベースを作成する](#)

AWS 設定で請求情報を表示する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

AWS 設定を使用して、請求情報を表示できます。無料利用枠を使用している場合、このページには無料利用枠の日数と AWS クレジットが表示されます。プロジェクトあたりのコストを表示することもできます。有料プランを使用している場合は、残高、現在の料金、プロジェクトあたりのコストを表示できます。支出制限を使用している場合は、制限に関連する情報を表示できます。[AWS 設定で支払い方法を管理する](#) および [AWS 設定で税登録を管理する](#) も使用できます。

無料プランを使用すると、すべての使用量が AWS 無料利用枠クレジットの対象となります。AWS 無料利用枠クレジットを使い切った場合、または 184 日後のいずれか早い方の時点で、有料プランにアップグレードする必要があります。有料プランへのアップグレードの詳細については、「」を参照してください[AWS 設定でアカウントをアップグレードする](#)。

プロジェクトごとにコストを表示するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、請求を選択します。
3. プロジェクト別のコストには、当月month-to-date料金と当月month-to-date予想料金が表示されます。プロジェクト全体のすべての料金が表示されます。
4. (オプション) Inspect costs でプロジェクトの料金の内訳を表示するには、View を選択します。Billing AWS and Cost Management コンソールにリダイレクトされます。

Billing and Cost Management Console に表示される請求データと Cost Explorer AWS データは、少なくとも 1 日に 1 回更新されます。更新される頻度は異なる場合があります。支出制限を使用すると、AWS Settings and AWS Cost Management Console month-to-date推定請求額が異なる場合があります。

AWS 設定で請求履歴を表示する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

請求履歴は AWS 設定で確認できます。請求履歴は、支払い方法がある場合にのみ使用できます。無料利用枠を使用している場合、請求履歴は表示されません。

請求期間中に取引した各サービスプロバイダーの請求書をダウンロードできます。これには、請求タイプ、請求日、米ドルの合計などの情報が含まれます。請求書が別の通貨で発行された場合、他の通貨での合計も表示されます。請求書は各プロジェクトに分割されません。

請求履歴を表示するには

1. <https://settings.aws.com> で AWS 設定を開きます。

2. メインナビゲーションペインで、請求を選択します。
3. 残高 の横にある請求履歴の表示 を選択します。請求履歴にリダイレクトされます。
4. 請求書をダウンロードするには、請求書 ID を選択します。

AWS 設定で支払い方法を管理する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

支払い方法は AWS 設定で管理できます。支払い方法は、すべてのプロジェクトの AWS リソース使用量の支払いに使用されます。支払い方法は、アカウントの作成時に情報を提供した場合、またはアカウントを有料プランにアップグレードした場合にのみ管理できます。

支払い方法を管理するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、請求を選択します。
3. Balance の下に、支払い情報が表示されます。[Manage] (管理) を選択します。
4. Payment method で、Update を選択します。
5. 新しい支払い方法を入力し、保存を選択します。

AWS 設定で支払いを行う

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

Settings で AWS 請求書を支払うことができます AWS 。 は毎月の初めにデフォルトの支払い方法を自動的に AWS 請求します。その料金が正常に処理されない場合は、コンソールを使用して支払い方法を更新し、支払いを行うことができます。

支払いを行う前に、今後自動的に請求される支払い方法がデフォルトの支払い方法として設定されていることを確認してください。クレジットカードを使用している場合は、カードが有効期限内であることを確認してください。

支払いを行うには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、請求を選択します。
3. Balance の横にある「請求履歴の表示」を選択します。請求履歴にリダイレクトされます。
4. アクション に、未払いの請求書に対する支払い請求書が表示されます。請求書がリストされていない場合は、何もする必要はありません。
5. 請求書の支払いを選択します。
6. 選択内容を確認し、支払いを選択します。

銀行口座への請求や、未払い金の支払いに関してご質問がある場合は、[サポートセンター](#)でケースを作成します。

AWS 設定で希望通貨を変更する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

設定で任意の通貨を変更できます AWS。優先通貨は、所有するプロジェクトにのみ適用されます。特定の請求国では、支払い通貨が制限されています。カード発行者は、他の通貨での移行に対して料金が発生する場合があります。

希望の表示通貨を変更するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、請求を選択します。
3. Balance の下に、支払い情報が表示されます。[Manage] (管理) を選択します。残高が表示されない場合は、通貨を変更することはできません。
4. 通貨の設定 を選択します。

5. デフォルトの支払い通貨で、支払い通貨を選択します。
6. [保存] を選択します。

AWS 設定で税登録を管理する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

税登録番号と免税は AWS 設定で管理します。税金情報は、所有しているプロジェクトにのみ適用されます。

納税者番号の更新と削除

1 つ以上の税登録番号を更新または削除するには、次の手順に従います。

Note

国が [税金設定] ページのドロップダウンに表示されていない場合、AWS は現時点ではその国の税登録を収集しません。

税登録番号を更新するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、請求を選択します。
3. Balance の下に、支払い情報が表示されます。[Manage] (管理) を選択します。
4. 税金設定を選択します。
5. 税登録情報を変更します。
6. [保存] を選択します。

米国の免税を管理する

お客様の州が適格である場合は、AWS 設定のプランと請求ページで米国の免税を管理できます。適用除外のためにアップロードしたドキュメントは、24 時間以内に サポートによってレビューされます。免税は、アカウントがビジネスとして登録されている場合にのみ管理できます。

米国の免税をアップロードまたは追加するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、請求を選択します。
3. Balance の下に、支払い情報が表示されます。[Manage] (管理) を選択します。
4. [免税の管理] を選択し、[免税の追加] を選択します。
5. 免税タイプと税務管轄区を指定します。
6. 証明書ドキュメントをアップロードします。
7. 情報を確認し、[Submit] (送信) を選択します。

24 時間以内に、サポートケースを通じて、追加情報が必要な場合、またはいずれかのドキュメントが有効でなかった場合に通知されます。

免除が承認されると、その免税は、[免税] タブに、[アクティブ] (アクティブ) の有効期間とともに表示できます。

免税が拒否された場合には、サポートケースを通じて通知があります。

AWS 設定でクレジットを表示して引き換える

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

Settings で利用可能なクレジットを表示して引き換えることができます AWS。AWS クレジットは請求書に自動的に適用され、対象となるサービスに関連するコストをカバーできます。対象となるサービスの詳細については、[AWS 「プロモーションクレジットの引き換え」](#)を参照してください。

クレジットは、使い果たされるか期限切れになるまで、所有しているすべてのプロジェクトに適用されます。交換したクレジットを使用するプロジェクトを選択することはできません。クレジットは、所有するすべてのプロジェクトに適用されます。

クレジットを表示するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、請求を選択します。
3. 現在の料金コンテナには、利用可能なクレジットが表示されます。クレジットを選択します。

プランタイプに応じて、アクティブクレジットと期限切れクレジット、またはクレジットと過去 6 か月間の非アクティブなクレジットのビューにリダイレクトされます。

4. クレジットで利用できる AWS サービスを表示するには、「サービスのリストを参照」を選択します。

AWS プロモーションクレジットを引き換えるには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、請求を選択します。
3. 現在の料金コンテナには、利用可能なクレジットが表示されます。クレジットを選択します。

プランタイプに応じて、アクティブクレジットと期限切れクレジット、またはクレジットと過去 6 か月間の非アクティブなクレジットのビューにリダイレクトされます。

4. クレジットを引き換えるを選択してクレジットを引き換えます。
5. プロモーションコードの場合は、表示されたとおりにプロモーションコードを入力します。クレジットを引き換えるときは、[AWS プロモーションクレジットの利用規約](#)を読み、同意することを指定します。
6. クレジットの引き換えを選択します。

AWS 設定でインドのアカウントを管理する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

にサインアップ AWS し、連絡先住所と請求先住所としてインドを選択した場合、ユーザー契約はインドの現地 AWS 販売者である Amazon Web Services India Private Limited (AWS インド) AWS と締結され、請求書の合計は米ドル (USD) ではなくインドルピー (INR) で表示されます。

アカウントが AWS India にある場合は、このトピックの手順に従ってアカウントを管理します。このトピックでは、AWS インドアカウントにサインアップし、AWS インドアカウントに関する情報を編集し、顧客確認を管理し、永続アカウント番号 (PAN) を追加または編集する方法について説明します。

トピック

- [India で AWS \(新規\) AWS にサインアップする](#)
- [顧客検証情報の管理](#)

India で AWS (新規) AWS にサインアップする

AWS India は、インドの の現地販売 AWS 者です。連絡先と請求先住所がインドにある場合は、次の手順を使用してサインアップします。

AWS India で AWS (新規) にサインアップを使用するには

1. aws.amazon.com に移動し、アカウントの作成を選択します。
2. Sign up for AWS (new) と Sign up for AWS (advanced) の違いを説明するバナーで、「Sign up for AWS」を選択します。
3. Google、Apple、GitHub、Amazon などのログインを選択します。
4. プロバイダーのログインが表示されます。ログインすると、AWS サインアップするようにリダイレクトされます。
5. 名前を入力し、続行を選択します。

この名前は、プロジェクトへのアクセス権をチームメンバーに付与すると、チームメンバーと共有されます。

6. 検証コードを入力して、ログインに関連付けられている E メールを確認します。E メールを確認したら、続行を選択します。
7. アカウントの強力なパスワードを入力し、続行を選択します。

AWS では、パスワードが次の条件を満たす必要があります。

- 8～128 文字で構成されていること。

- 大文字、小文字、数字、および ! の文字タイプの少なくとも 3 つの組み合わせを含める必要があります。@ # \$ % ^ 管理ポータル * () < > [] { } | _ + = 記号。
- AWS アカウント 名前や E メールアドレスと同じにすることはできません。

8. 連絡先の詳細を入力し、続行を選択します。

連絡先または請求先住所がインドにある場合、インドのコンピュータ緊急対応チーム (CERT-In) の規制に従い、AWS は、AWS サービスへのアクセスを許可する前にお客様の ID 情報を収集して検証する必要があります。

連絡先情報または請求先情報で選択した名前は、顧客検証に使用する予定のドキュメントに記載されている名前と完全に一致している必要があります。例えば、設立証明証を使用してビジネスアカウントを確認する予定の場合は、そのドキュメントに記載されている事業名を提供する必要があります。受け入れられたドキュメントタイプのリストについては、「[the section called “顧客確認用にインドで受け入れられるドキュメント”](#)」を参照してください。

9. アカウント登録の主な目的を選択してください。

10. アカウントの所有者を最も適切に表す所有権タイプを選択します。所有権タイプとして会社、組織、またはパートナーシップを選択する場合は、主要な管理担当者の名前を入力します。主要な管理担当者には、取締役、業務責任者、または事業の運営責任者を指定できます。
11. 選択した所有権タイプに応じて、検証に使用する承認済みのインドのドキュメントタイプを選択し、ドキュメント情報を入力します。

 Note

個人アカウントを持っており、インド連邦による発行ではない運転免許証を使用する予定の場合は、検証用に別のタイプの個人ドキュメントを使用することをお勧めします。

12. 顧客検証に使用する名前を選択します。

請求情報や連絡先情報にインドの住所が関連付けられている場合、その名前が選択肢として表示されます。選択した名前が、顧客検証に使用する予定のドキュメントタイプに記載された名前と一致していることを確認してください。請求先または連絡先の住所に関連付けられている名前を変更する必要がある場合は、アカウントのサインアップを完了した後に変更できます。

13. 検証のために情報を提出することに同意し、[続行] をクリックします。

アカウントのサインアップが完了すると、顧客検証の結果が E メールで通知されます。マイ AWS 設定のプロファイルページでステータスを確認することもできます。AWS サービスにアクセスするには、顧客検証に合格する必要があります。

14. AWS は最初のプロジェクトをプロビジョニングします。

AWS 設定にアクセスするには、 からプロジェクトの管理を選択します AWS マネジメントコンソール。AWS 設定では、チームメンバーを招待したり、新しいプロジェクトを作成したり、請求やその他の設定を変更したりできます。

顧客検証情報の管理

インドのコンピュータ緊急対応チーム (CERT-In) の規制に従い、AWS は AWS、サービスへの新規または継続的なアクセスを許可する前に、ID 情報を収集して検証する必要があります。入力したインドの請求先住所または連絡先住所に記載されている名前を使用して本人確認を行う必要があります。検証中、AWS はドキュメント番号が有効かどうか、および指定した名前が顧客検証に使用するドキュメントに関連付けられた名前と一致するかどうかを確認します。連絡先情報または請求情報から選択した名前は、ドキュメントに記載されている名前と完全に一致する必要があります。

請求名、住所、その他の連絡先情報を更新するには、「」を参照してください [AWS 設定を使用する](#)。請求先情報や連絡先情報の名前やインドの住所など、以前に顧客検証に使用した情報を編集する場合、顧客検証情報を更新して再提出する必要がある場合があります。

顧客検証ステータスの確認

顧客検証ステータスは、プロフィールの管理ページでいつでも表示できます。検証ステータスが [検証が必要です] または [検証に失敗しました] の場合は、顧客検証情報を作成または更新して、検証のために提出してください。

顧客検証情報の作成

顧客検証を完了するには、承認済みのインドのドキュメントからの情報を提供する必要があります。受け入れられたドキュメントタイプのリストについては、「[the section called “顧客確認用にインドで受け入れられるドキュメント”](#)」を参照してください。

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、プロフィールの管理を選択します。
3. 顧客検証 で、「顧客検証の作成」を選択します。
4. 顧客検証に使用する予定のドキュメントに記載された名前と正確に一致する名前を選択します。例えば、設立証明証を使用してビジネスアカウントを確認する予定の場合は、そのドキュメントに記載されている事業名を提供する必要があります。

5. このページでリクエストされている残りの情報を入力します。選択したドキュメントタイプによっては、ドキュメントの表面と裏面の両方のコピーをアップロードする必要がある場合があります。画像ファイルをアップロードする場合は、ドキュメント内のすべての情報が認識でき、判読可能であることを確認してください。
6. [Submit] を選択してください。

顧客検証の結果と次のステップについては、E メールまたは AWS Health Dashboard で通知されます。

顧客検証情報の編集

アカウント登録の主な目的や組織タイプ、および検証に使用する名前、ドキュメントタイプ、ドキュメントアップロード、またはドキュメント情報など、顧客検証情報を編集できます。

顧客検証に使用する名前やドキュメントタイプを編集する、またはドキュメント情報を更新する場合、変更を保存するには再度本人確認を行う必要があります。

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、プロフィールの管理を選択します。
3. 顧客検証 で、顧客検証 を選択します。
4. [編集] を選択し、変更する情報を更新します。

情報を更新する際には、次のガイダンスに注意してください。

- 別の名前を選択する場合、その名前は顧客検証に使用する予定のドキュメントに記載されている名前と完全に一致する必要があります。例えば、設立証明証を使用してビジネスアカウントを確認する予定の場合は、そのドキュメントに記載されている事業名を提供する必要があります。
- 別のドキュメントタイプを選択する場合は、ドキュメントの表面と裏面 (該当する場合) のコピーをアップロードする必要があります。ドキュメントアップロードに含まれるすべての情報が認識でき、判読可能である必要があります。
- 個人アカウントを持っており、インド連邦による発行ではない運転免許証を使用する予定の場合は、検証用に別のタイプの個人ドキュメントを使用することをお勧めします。
- 受け入れられたドキュメントタイプのリストについては、「[the section called “顧客確認用にインドで受け入れられるドキュメント”](#)」を参照してください。

5. [Submit] を選択してください。

保存した変更のタイプによって再度本人確認を行う必要がある場合は、顧客検証の結果と次の手順が E メールで通知されます。また、顧客検証ページに戻るか、AWS ヘルスダッシュボードで結果を表示することもできます。

顧客確認用にインドで受け入れられるドキュメント

インド政府が発行した以下の種類のドキュメントを顧客確認に使用できます。

Note

以下に示されているリンクは、政府によって変更される可能性があります。

- **PAN カード** - 納税者番号 (PAN) カードは、デジタルと物理の両方の形式で提供されており、個人、企業、および団体に対してインドの所得税局が発行する一意の英数字識別子が含まれています。PAN は、文字と数字を含む 10 文字の形式 (**AAAAA1111A**) で構成されます。このドキュメントを検証に使用する場合は、PAN ドキュメントに記載されている生年月日 (個人の場合) または法人設立日 (ビジネスの場合) も入力し、カードの表面をアップロードする必要があります。PAN の有効性を確認するには、[所得税局の公式ウェブサイト](#)にアクセスしてください。
- **有権者 ID カード/EPIC** - 有権者 ID カードは写真付き選挙人 ID カード (EPIC) と呼ばれ、インド選挙委員会によってインドの適格な有権者に発行される一意の識別番号が含まれています。有権者 ID/EPIC 番号は、文字と数字を含む 10 文字で構成されます。有権者 ID の有効性を確認するには、[インド選挙管理委員会](#)の公式ウェブサイト にアクセスしてください。このドキュメントを検証に使用するには、カードの表面と裏面の両方をアップロードする必要があります。
- **運転免許証** - 運転免許証がインド連邦によって発行されたものではない場合は、検証に別のドキュメントタイプを使用することをお勧めします。運転免許証番号は、文字、数字、スペース、ハイフンを含む 12~16 文字で構成されます。このドキュメントを検証に使用するには、生年月日を入力し、カードの表面と裏面の両方をアップロードする必要があります。運転免許証の有効性を確認するには、道路交通省の [Parivahan Sewa のサイト](#)にアクセスしてください。
- **設立証明証** - 設立証明書は、企業省 (MCA) によって発行されるドキュメントであり、企業が法人として登録された日付を示します。この証明書は、インドで登録されている企業を一意に識別し、追跡するために使用されます。各証明書には企業識別番号 (CIN) が含まれています。これは、文字と数字を含む 21 文字で構成される一意の英数字識別子です。このドキュメントを検証に使用するには、設立証明書ドキュメントをアップロードする必要があります。CIN の有効性を確認するには、[企業省のポータル](#)にアクセスしてください。

個人アカウントとビジネスアカウントでは、インドのさまざまなドキュメントタイプが受け入れられます。

- 個人アカウントの場合 - PAN カード、有権者 ID カード/EPIC、運転免許証。
- ビジネスアカウントの場合 - PAN カードと設立証明書。

AWS 設定で India の請求を設定する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

にサインアップ AWS し、連絡先住所と請求先住所として India を選択した場合、ユーザー契約はインドの現地 AWS 販売者である Amazon Web Services India Private Limited (AWS India) と締結され AWS、請求書の合計はドルではなくルピーで表示されます。すべての税情報は、プロジェクト所有者のみが作成または変更できます。

追加の税金または請求情報については、プロジェクトごとに AWS Billing コンソールを使用できます。

AWS 設定のプロファイル管理ページの計画と請求セクションを使用して、次のタスクを実行します。

- 納税者番号の追加または編集
- 複数の納税者番号の編集
- 複数の Goods and Service Tax 番号を編集する
- 税金請求書を表示する

Permanent Account Number を追加または編集する

Permanent Account Number (PAN) をアカウントに追加して編集できます。

PAN を追加または編集するには

1. <https://settings.aws.com> で AWS 設定を開きます。

2. メインナビゲーションペインで、プロフィールの管理を選択し、計画と請求を選択します。
3. [Tax Settings] ナビゲーションバーで、[Edit] を選択します。
4. [Permanent Account Number (PAN)] に PAN を入力し、[Update] を選択します。

複数の Permanent Account Number を編集する

アカウントで、複数の Permanent Account Number (PAN) を編集することができます。

複数の PAN 番号を編集するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、プロフィールの管理を選択し、計画と請求を選択します。
3. [Manage Tax Registration Numbers (税登録番号の管理)] で、編集する PAN 番号を選択します。
4. [Manage Tax Registration (税登録の管理)] で、[Edit (編集)] を選択します。
5. 変更するフィールドを更新し、[Update (更新)] を選択します。

複数の Goods and Service Tax 番号を編集する

アカウントで、複数の Goods and Service Tax 番号 (GST) を編集することができます。

複数の GST 番号を編集するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、プロフィールの管理を選択し、計画と請求を選択します。
3. [Manage Tax Registration Numbers (税登録番号の管理)] で、編集する GST 番号、または [Edit all (すべて編集)] を選択します。
4. [Manage Tax Registration (税登録の管理)] で、[Edit (編集)] を選択します。
5. 変更するフィールドを更新し、[Update (更新)] を選択します。

税金請求書を表示する

税金請求書は AWS 設定で表示できます。

税金請求書を表示するには

1. <https://settings.aws.com> で AWS 設定を開きます。

2. メインナビゲーションペインで、プロフィールの管理を選択し、計画と請求を選択します。
3. 下にスクロールし、[請求書] タブを選択します。
4. 「税金請求書」セクションで、ドキュメント ID に記載されている請求書リンクを選択します。

 Note

[税金請求書] セクションは、利用可能な税金請求書がある場合にのみ表示されます。

AWS インドとの間で登録販売者を変更する

請求情報または税金情報を更新することで、登録 AWS アカウント 販売者 (SOR) を別の SOR に変更できます。これは、機能が利用できないレガシーモデルで AWS India アカウントが運用されている場合には適用されません。の請求または税金の詳細で国や地域を編集するときに新しい場所のサービスプロバイダーが現在の場所のサービスプロバイダーと異なる場合は、アカウントの SOR が自動的に変更されます。

アカウントを AWS インドとの間で変更する場合、請求書または送金に設定されている場合、デフォルトの支払い方法を更新する必要はありません。デフォルトの支払い方法がクレジットカードまたはデビットカードの場合は、デフォルトの支払いカードの詳細を再確認する必要があります。これは、支払い方法が AWS India 外の取引とは別個に保存されるようにするためです。詳細については、[AWS 「インドの請求書の対象となるクレジットカードまたはデビットカードの表示」](#)を参照してください。

 Note

デフォルトの支払い方法としてクレジットカードまたはデビットカードを使用する AWS インドのアカウントがあり、自動支払い用に e-mandate を設定している場合は、デフォルトの支払い設定を編集する前に e-mandate を無効にする必要があります。

アカウントの SOR を変更するには、次のオプションを使用してこの情報を編集します。

請求情報と税金情報を使用して SOR を変更するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、プロフィールの管理を選択し、計画と請求を選択します。

3. [Default payment preferences] (デフォルトの支払いの詳細設定) セクションで、[Edit] (編集) を選択します。
4. 新しい請求先住所を入力します。
5. [支払い通貨] セクションで、新しい SOR で使用できる通貨のリストからデフォルトの通貨を選択します。
6. (デフォルトの支払い方法がクレジットカードまたはデビットカードの場合) [支払い方法の確認] セクションで、デフォルトの支払いカードの詳細を再入力して、新しいサービスプロバイダーでの使用を確認します。

新しい SOR でデフォルトのカードを変更するには、後ほどカードを追加し、デフォルトの支払い方法設定を変更します。

7. [Save changes] (変更の保存) をクリックします。

数分後、更新された SOR を含めた変更が [お支払いの詳細設定] ページに表示されます。

請求情報と税金情報を使用して SOR を変更するには

アカウントを別の SOR に移動するには、アカウントに関連付けられた納税登録番号 (TRN) を更新し、新しい有効な TRN を入力する必要があります。アカウントに関連付けられている TRN を削除することもできます。アカウントの新しい SOR は、可用性順位と優先順位に従って、新しい課税住所の国と現在の請求先住所に基づいて自動的に解決されます。アカウントの SOR が変更されると、アカウントが AWS インドに出入りしていることが通知されます。

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、プロファイルの管理を選択し、計画と請求を選択します。
3. アカウントを選択し、[納税登録の管理] を選択してから、[編集]、[すべて編集]、または [TRN の削除] を選択します。
4. (デフォルトの支払い方法がクレジットカードまたはデビットカードの場合) メインナビゲーションペインで、プロファイルの管理を選択し、プランと請求を選択します。
5. [支払い方法を追加] を選択して、デフォルトの支払いカードの詳細を再入力するか、新しい支払いカードを追加します。
6. カードを保存したら、[デフォルトとして設定] を選択します。

[デフォルトの支払いの詳細設定] セクションに、新しい SOR では以前のデフォルトの支払い方法を使用できないというアラートが表示されます。支払いカードの追加後にページを更新すると、アラートが非表示になります。

アクセス AWS サポート

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

新しい AWS エクスペリエンスにサインアップすると、AWS サポートと連携できる場所が 2 つあります。

Basic Support または Business Support+ にアクセスできます。デフォルトでは、基本サポートに登録されています。Business Support+ のトライアルを開始して、最大 6 か月間無料で使用できます。

プロジェクトサポート

プロジェクト、チーム管理、または請求に関連する問題が発生した場合は、AWS 「設定」の「基本サポート」または「ビジネスサポート+」にアクセスできます。組織の追加プロジェクトをリクエストしたり、請求に関連するクォータの引き上げをリクエストしたりできます。

サポートケースを作成するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、サポートを選択します。
3. プロジェクトをサポートするには、「ケースの作成」を選択します。
4. 件名には、サポートケースの件名を入力します。
5. 説明 で、問題を記述します。可能な場合は、問題を再現するステップを記述します。
6. [ケースを作成] を選択します。

サポートケースを作成したら、ケース情報を表示してサポートを引き続き使用できます。

ケース情報を表示するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、サポートを選択します。
3. サポートケースを選択します。このビューでは、ケースに関するすべての通信を確認できます。
4. サポートに返信を送信するには、返信で返信を入力し、返信の送信を選択します。

ケースが解決されたら、それを解決して AWS 設定から削除できます。

ケースを解決するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、サポートを選択します。
3. [Resolve case] (ケースを解決) を選択します。

解決後にケースの詳細にアクセスすることはできません。

Technical support (技術サポート)

AWS リソースに問題がある場合は、テクニカルサポートが必要です。テクニカルサポートにアクセスするには、問題のあるプロジェクトの [AWS サポートセンター](#) でケースを開きます。

すべてのプロジェクトと組織が閉鎖された場合のサポート

すべてのプロジェクトと組織が閉鎖された場合は、サポート [フィードバックフォームに記入してサポート](#) にお問い合わせください。

「リクエスト情報」セクションの「How can we help」で、新しい AWS エクスペリエンスを使用していることと、すべてのプロジェクトがクローズされていることを含めます。

Business Support+ トライアルを開始する

Business Support+ は最大 6 か月間無料でご利用いただけます。Business Support+ は、2026 年 10 月 31 日まで無料で提供されます。2026 年 11 月 1 日以降、標準料金が開始され、1 か月あたり最大 6 か月の 29 USD をカバーする 174 USD のビジネスサポート+ クレジットが付与されます。無料期間が終了してクレジットが開始されると、サブスクライブされたままになり、クレジット残高が不足すると、正規料金の請求が開始される前に AWS 通知されます。

Business Support+ の料金は、1 か月あたり 29 USD または AWS 支出の割合のいずれか大きい方です。詳細については、「[料金](#)」を参照してください。プランは、キャンセルするまで毎月更新されます。

Business Support+ トライアルを開始するには

1. <https://settings.aws.com> で AWS 設定を開きます。

2. メインナビゲーションペインで、サポートを選択します。
3. トライアルの開始 を選択します。これは、組織内のすべてのプロジェクトに影響します。
4. 条件を確認し、契約チェックボックスを選択し、トライアルの開始を選択します。

コミットメントやペナルティなしでいつでもキャンセルできます。キャンセルすると、Business Support+ アクセスは直ちに終了し、未使用のクレジットはすべて失効します。いつでも標準料金で再登録できますが、ビジネスサポート+ プロモーションオファーはキャンセルされると再開できません。

Business Support+ をキャンセルするには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、サポートを選択します。
3. プランをキャンセルを選択します。
4. Business Support+ をキャンセルするとすぐに Basic Support に戻ること、リストされている特典にアクセスできなくなること、174 USD のクレジットが削除されて元に戻すことができないことを確認するチェックボックスをオンにします。
5. プランをキャンセルを選択して基本サポートに戻ります。

AWS CloudTrail を使用してプロジェクトをモニタリングする

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

AWS CloudTrail を使用してプロジェクトをモニタリングする

プロジェクトは、チームメンバー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 サービスである AWS CloudTrail と統合されています。CloudTrail は、プロジェクトのすべての API コールをイベントとしてキャプチャします。キャプチャされた呼び出しには、コンソールからの呼び出しと、サポートされているすべての AWS サービスの API オペレーションが含まれます。CloudTrail で収集された情報を使用して、プロジェクトに対して行われたリクエスト、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。

CloudTrail を使用してプロジェクトを変更したユーザーを確認する

このチュートリアルは、に慣れているユーザーを対象としています AWS CLI。プロジェクトを複数のチームメンバーと共有する場合、CloudTrail を使用して、プロジェクト内のリソースを変更したユーザーを表示できます。設定または を使用して AWS プロジェクト AWS マネジメントコンソール にアクセスしたときにユーザーまたはチームメンバーが実行したすべてのアクションは、onBehalfOfパラメータによってログに記録されます。このパラメータは、ユーザー ID と ID ストア ID を示します。これらの値は、プロジェクトにアクセスするために招待したビルダー ID を定義します。

onBehalfOf パラメータを見つけてチームメンバーに接続するには、AWS CLI と にアクセスする必要があります AWS マネジメントコンソール。AWS CLI を設定していない場合は、AWS CloudShell を使用してブラウザベースの事前認証済みシェルにアクセスし、 から直接起動 AWS マネジメントコンソール して AWS CLI コマンドを実行できます。

ステップ 1. AWS CloudTrail イベントを検索するには

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/cloudtrail/> で CloudTrail コンソールを開きます。
2. ナビゲーションペインで [Event history (イベント履歴)] を選択してください。最新のイベントが最初に表示された、フィルタリングされたイベントのリストが表示されます。イベントを選択します。
3. イベントレコードには、次の内容が表示されます。

```
"onBehalfOf": {
  "userId": "000000-e00f-000-000-00000000",
  "identityStoreArn":
    "arn:aws:identitystore::111122223333:identitystore/000000-0000-0000-0000-600000007"
}
```

これは、CloudTrail イベントを作成したチームメンバーを定義する ID です。

ステップ 2. onBehalfOf パラメータをチームメンバーに接続するには

を使用して onBehalfOfパラメータをチームメンバーに接続するには AWS CLI:

ターミナル AWS CLI で 使用するには

1. 次のコマンドを実行して にサインインします AWS CLI。を使用して リージョンを見つけることができます[AWS リージョン プロジェクトの](#)。

```
aws login --region project-region
```

2. 次のコマンドを実行して、ID ストアの ID を取得します。CloudTrail イベントには ID ストア ARN が表示されますが、ID ストア ID は表示されません。ID ストアの ID を検索するときは、AWS リージョン us-east-1常に を使用します。

```
aws sso-admin list-instances --region us-east-1
```

出力は次のようになります。

```
{
  "Instances": [
    {
      "InstanceArn": "arn:aws:sso:::instance/ssoins-0000000000",
      "IdentityStoreId": "d-000000",
      "OwnerAccountId": "111122223333",
      "CreateDate": "2025-10-26T23:10:58.529000+00:00",
      "Status": "ACTIVE",
      "PrimaryRegion": "us-east-1",
      "Regions": [
        {
          "RegionName": "us-east-1",
          "Status": "ACTIVE",
          "AddedDate": "2025-10-26T23:10:58.529000+00:00",
          "IsPrimaryRegion": true
        }
      ]
    }
  ]
}
```

ID ストア ID をコピーします。この場合、ID ストア ID は ですd-000000。

3. 次のコマンドを実行して、 onBehalfOfパラメータに対応するチームメンバーを記述します。

```
aws identitystore describe-user --user-id 00000-e00f-000-000-00000000 --region us-east-1 --identity-store-id d-000000
```

出力は次のようになります。

```
{
  "IdentityStoreId": "d-000000",
  "UserId": "00000-e00f-000-000-00000000",
  "UserName": "carlos_salazar",
  "Name": {
    "FamilyName": "Salazar",
    "GivenName": "Carlos"
  },
  "DisplayName": "Carlos",
  "Emails": [
    {
      "Value": "carlos_salazar@example.com",
      "Type": "work",
      "Primary": true
    }
  ],
  "UserStatus": "ENABLED",
  "CreatedAt": "2025-10-26T23:15:27.213000+00:00",
  "CreatedBy": "000000000000",
  "UpdatedAt": "2025-10-26T23:18:55.432000+00:00",
  "UpdatedBy": "000000000000"
}
```

チームメンバーの表示名と E メールはこの出力で提供されます。

CloudShell を使用して AWS onBehalfOf パラメータをチームメンバーに接続するには、 にログイン AWS マネジメントコンソール し、CloudShell にアクセスします。詳細については、[AWS CloudShell の開始方法](#)」を参照してください。CloudShell にアクセスするための正しい IAM アクセス許可が自動的に付与されます。

AWS 設定でプロジェクトを閉じる

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

プロジェクトが不要になった場合は、プロジェクトを閉じることができます。プロジェクトを閉じた後、閉じた日から 90 日以内にプロジェクトを再開できます。プロジェクトを閉鎖した日から AWS プロジェクトを完全に閉鎖するまでの時間は、閉鎖後期間です。

プロジェクトを閉じる前に知っておくべきこと

プロジェクトを閉じる前に、次の点を考慮してください。

- 使用制限を超えたために一時停止した場合、プロジェクトを閉じることができません。使用制限をオフにしてから、プロジェクトを閉じる必要があります。詳細については、「[AWS 設定で使用制限を更新する](#)」を参照してください。
- すべてのチームメンバーは、このプロジェクトとその中のすべてのリソースに自動的にアクセスできなくなります。
- プロジェクトを解約すると、このプロジェクトのカスタマーアグリーメントの終了 AWS 通知として機能します。
- プロジェクトを閉じる前に、プロジェクト内のリソースを削除する必要はありません。ただし、保持する必要があるリソースやデータをバックアップすることをお勧めします。特定のリソースをバックアップする方法については、そのサービスの適切な AWS ドキュメントを参照してください。
- 閉鎖後期間中にプロジェクトを再開できます。プロジェクトに残っているサービスの料金は、再開すると再開されます。また、未払いの請求書についても引き続き責任を負います。
- プロジェクトの閉鎖前に消費されたサービスの未払いの料金と料金は、引き続きお客様の負担となります。プロジェクトを閉鎖した翌月に AWS 請求書が届きます。例えば、1 月 15 日にアカウントを閉鎖した場合、1 月 1 日から 1 月 15 日までに発生した使用量に対する請求書が 2 月初旬に届きます。
- プロジェクトが終了すると、AWS はドメインを停止するまで最大 5 日間毎日 E メールを送信します。ドメインが停止された後、ドメインのレジストラに応じて、30 日以内にドメインを削除するか、ドメインをレジストラにリリースします。詳細については、「[My AWS アカウント is](#)

[closed or permanently closed](#)」および「[My domain is registered with Route 53](#)」を参照してください。この情報は 用に書かれていますが AWS アカウント、プロジェクトでは情報が正確です。

- AWS CloudTrail は基本的なセキュリティサービスです。つまり、ユーザーがプロジェクトを閉鎖する前にプロジェクト内の証跡を明示的に削除しない限り、ユーザーが作成した証跡は引き続き存在し、プロジェクトを閉鎖した後もイベントを配信できます。が閉じられた後に AWS アカウント 証跡の削除をリクエストする方法の詳細については、CloudTrail ユーザーガイド」の[AWS アカウント「クロージャと証跡」](#)を参照してください。この情報は 用に書かれていますが AWS アカウント、プロジェクトについては情報が正確です。

プロジェクトを閉じるには

プロジェクトを閉じるには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、アクセスするプロジェクトを選択します。
3. プロジェクトを閉じる で、プロジェクトを閉じる を選択します。
4. 選択内容を確認し、プロジェクトを閉じるを選択します。

プロジェクトページには、プロジェクトが完全に削除されるまで 90 日間表示されます。

閉鎖後期間

閉鎖後期間は、アカウントを閉鎖した日から がプロジェクト AWS を完全に閉鎖するまでの時間を指します。閉鎖後期間は 90 日間です。閉鎖後期間中は、プロジェクトを再開することによってのみコンテンツと AWS サービスにアクセスできます。閉鎖後期間が過ぎると、 はプロジェクト AWS を完全に終了し、再開できなくなります。AWS はアカウント内のコンテンツとリソースも削除します (CloudTrail 証跡を除く)。プロジェクトが完全に閉じられた後、そのプロジェクト ID を再利用することはできません。

プロジェクトを再開する

プロジェクトは 90 日後に完全に終了します。その後、プロジェクトを再度開くことができなくなり、プロジェクトに残っているコンテンツ AWS が削除されます。プロジェクトが完全に閉鎖される前にプロジェクトを再開するには、(1) サポート できるだけ早く に連絡する必要があります。また、(2) アカウントの閉鎖日から 60 日以内に、請求書に指定されている必要な情報の提供を含め、未払い残高の全額を受け取る必要があります。

Note

プロジェクトに残っているサービスの料金は、再開すると再開されます。

高度な AWS 機能をアクティブ化する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

高度な機能をアクティブ化すると、作成したプロジェクトと招待したチームメンバーを管理するために使用される AWS 組織、管理アカウント、委任管理者アカウントを完全に制御できます。環境のセキュリティ、ガバナンス、チームメンバーシップを直接管理します AWS。追加の AWS サービス、マルチリージョン機能、強化された管理および請求コントロールにアクセスできます。

高度な機能をアクティブ化する前に、アカウントをアップグレードする必要があります。詳細については、「[AWS 設定でアカウントをアップグレードする](#)」を参照してください。

高度な機能をアクティブ化するとどうなるか

高度な機能をアクティブ化すると、次の変更がすぐに管理アカウントとプロジェクトを含む AWS Organization に適用されます。

- これで、プロジェクトを含む AWS 組織の管理者になります。
- 管理アカウントのルート E メールアドレスを設定します。また、ルートユーザーのパスワードを設定する必要があります。詳細については、「[管理アカウントのルートユーザーパスワードを設定する](#)」を参照してください。
- プロジェクトは、組織のメンバーアカウントとして管理します。この組織の管理者は、組織内にメンバーアカウントを作成できます。Builder ID AWS は引き続きプロジェクトアカウントを所有します。詳細については、「[高度な機能をアクティブ化した後のプロジェクトアカウント](#)」を参照してください。
- 組織に招待するメンバーアカウントに管理者ロールを付与するには、OrganizationAccountAccessRole を作成する必要があります。詳細については、「[招待されたメンバーアカウントでの OrganizationAccountAccessRole の作成](#)」を参照してください。

- チームメンバーはワークフォース ID と呼ばれ、AWS 引き続きアカウントにアクセスできます。IAM Identity Center を使用してワークフォースの ID ソースをカスタマイズすることもできます。AWS Builder ID を ID ソースとして引き続き使用することも、これを外部 ID ソースに変更することもできます。ID ソースを AWS Builder ID から別の ID ソースに変更した場合、元に戻すことはできません。今後、ID ソースとして AWS Builder ID を再度有効にすることはできません。詳細については、「[Builder ID から ID AWS ソースを変更する](#)」を参照してください。
- Account AWS Access Manager を使用して、IAM Identity Center 組織インスタンス内のユーザーとグループのアクセスを制御します。この機能を使用してユーザーアクセスを変更できますが、ユーザーはを使用してサインインaws loginし、ブラウザから IAM ロールセッション認証情報を受け取ることができます。詳細については、[AWS 「Account Access Manager」](#)を参照してください。
- AWS は、委任管理者ロールを持つ組織内に Identity Delegated Admin というメンバーアカウントを作成します。このロールは、IAM アイデンティティセンターとアカウントアクセスマネージャーでほとんどの管理タスクを実行するために使用されます。委任管理者ロールは、米国東部 (バージニア北部) で使用する必要があります。詳細については、「[Delegated admin](#)」を参照してください。

AWS Builder ID は、プロジェクトアカウントと同様に、ID 委任管理者アカウントを所有します。

- リソースコントロールポリシー (RCPs) とサービスコントロールポリシー (SCPs) を設定して、組織にカスタムガードレールを適用できるようになりました。以前は、はユーザーに代わって RCPs と SCPs AWS を管理していました。これらのポリシーは、高度な機能をアクティブ化した後に変更できます。詳細については、「[組織ポリシーを削除する](#)」を参照してください。

高度な機能をアクティブ化すると、次の変更が AWS 組織にも適用されます。

- いずれかの AWS アカウントに支出制限がある場合、その制限は削除されます。現在一時停止しているプロジェクトは再アクティブ化されます。高度な機能をアクティブ化した場合、支出制限を作成することはできません。代わりに、請求情報とコスト管理ツールのスイート全体にアクセスできます。これには、予算の設定、コストエクスプローラーレポートのダウンロード、AWS コスト異常検出による異常な支出の検出が含まれます。これらの高度なツールを使用して、コストの分析、整理、計画、最適化を行うことができます。
- すべての AWS サービスにアクセスできます。利用可能なサービスは、「」に記載されています[the section called “AWS のサービスは新しい AWS エクスペリエンスではサポートされていません”](#)。これらのサービスを有効にする前に、アーキテクチャを計画し、サービスドキュメントを参照してください。さらに、エージェントツールキットは、これらのサービス进行操作するための多くの[スキル](#)を提供します。

- 追加の AWS リージョンオプトインリージョンとマルチリージョン機能にアクセスできます。マルチリージョンアーキテクチャにより、ワークロードの耐障害性が向上します。リージョンのフットプリントを制限して監査する方法を計画することをお勧めします。作成するリソースが、使用する予定のリージョンにのみ存在することを確認することが重要です。
- 組織 AWS アカウント 内の各 の IAM ロールマネージャーをオフにできます。IAM ロールマネージャーは、ロールを自動的にプロビジョニングするオプションのアカウント設定であるため、ユーザーとワークフォースがロールを設定する必要はありません。詳細については、[「ロールマネージャーを有効または無効にする方法 \(コンソール\)」](#)を参照してください。
- [IAM Access Analyzer](#) を使用できます。

高度な機能をアクティブ化すると、以下の変更がユーザーエクスペリエンスにも適用されます。

- 以前は、 は、プロジェクトとアクセス AWS 設定間の変更に使用したメニューを含む簡略化されたビュー AWS マネジメントコンソール を示していました。が AWS マネジメントコンソール 拡張され、リージョンセクタ、追加サービス、それらを視覚的に区別するためにアクセスできるアカウントの色の設定などの追加機能が追加されました。詳細については、[「コンソールの機能」](#)を参照してください。
- 以下を実行できるようになりました。
 - マルチセッションコンソールのサポートを無効にします。
 - AWS アカウントを HIPAA または SEC 準拠として指定します。
 - AWS Marketplace を使用します。
 - AWS Activate から追加のクレジットを取得します。
 - AWS トレーニングパートナーと連携します。
 - AWS スキルビルダーチームのサブスクリプションを購入します。
 - とエンタープライズ契約を結びます AWS。
 - プロフェッショナルサービス契約を作成します。
 - AWS パートナーネットワークに参加します。

高度な機能をアクティブ化した後のプロジェクトアカウント

AWS Settings で作成した各プロジェクトには AWS アカウント、プロジェクトアカウントと呼ばれる が含まれています。AWS Builder ID は、ルートユーザーの E メールアドレスではなく、各プロジェクトアカウントを所有します。高度な機能をアクティブ化すると、後で ID ソースを変更しても、プロジェクトアカウントは組織のメンバーアカウントになり、AWS ビルダー ID は引き続きそ

れらを所有します。AWS Builder ID は、高度な機能をアクティブ化するとき が AWS 作成する Identity 委任管理者アカウントも所有します。

プロジェクトアカウントにはルートユーザーの E メールアドレスがないため、組織内の他のメンバーアカウントとは動作が異なります。

- AWS Organizations コンソールがプロジェクトアカウントに表示する E メールアドレスは、 が AWS 生成するプレースホルダーです。DescribeAccount、ListAccounts、ListDelegatedAdministrators、ListAccountsForProject、および GetPrimaryEmail オペレーションは、同じプレースホルダーを返します。使用または変更できる E メールアドレスではありません。
- プロジェクトアカウントのルートユーザーの E メールアドレスを更新することはできません。プロジェクトアカウントの StartPrimaryEmailUpdate または AcceptPrimaryEmailUpdate への呼び出しは、呼び出し元に必要なアクセス許可がある場合でも AccessDeniedException エラーで失敗します。
- ルートユーザーとしてプロジェクトアカウントにサインインしたり、ルートユーザーパスワードを復元したりすることはできません。
- 組織からプロジェクトアカウントを削除したり、組織を離れたり、別の組織に参加したりすることはできません。RemoveAccountFromOrganization プロジェクトアカウントに を呼び出すと、呼び出しは失敗し、アカウントが Builder ID によって所有されていることを示す ConstraintViolationException エラーが表示されます。

プロジェクトアカウントの使用を停止するには、管理アカウントからプロジェクトアカウントを閉じます。組織からプロジェクトアカウントを削除することはできないため、Identity 委任管理者アカウントを含むすべてのプロジェクトアカウントが完全に閉鎖された後にのみ、組織を削除できます。は、閉鎖後 90 日が経過するとアカウント AWS を完全に閉鎖します。

高度な機能をアクティブ化した後に組織で作成したメンバーアカウントにはルートユーザーの E メールアドレスがあり、これらの違いは適用されません。ルートユーザーの E メールアドレスを変更できるアカウントが必要な場合、または後で組織から削除できるアカウントが必要な場合は、新しいメンバーアカウントを作成してリソースを移動します。

高度な機能をアクティブ化した後、AWS 設定はどのように変わりますか？

高度な機能をアクティブ化すると、ID ソースとして AWS Builder ID を使用する限り AWS、設定を使用できます。AWS 設定には <https://settings.aws.com> からのみアクセスできます。からアクセスすることはできません AWS マネジメントコンソール。AWS 設定は、管理アカウントを使用してア

アカウントを管理するためのリンクを提供します。管理アカウントでは、AWS 設定から次の AWS マネジメントコンソール 場所にアクセスできます。管理アカウントは、次のような管理タスクの実行にのみ使用します。

- Billing and Cost Management Console にアクセスして、請求情報を表示します。
- AWS Organization コンソールにアクセスして、組織を管理する SCPs と RCPs を変更します。
- AWS Account Access Manager コンソールにアクセスして、ワークフォース ID のきめ細かなアクセスを変更します。
- IAM Identity Center にアクセスして、ID ソースを変更します。

管理アカウントを使用して、これらのタスクを実行します。ルートユーザーの E メールとパスワードにもアクセスできますが、アカウントへの緊急アクセスにはルートユーザーの認証情報のみを使用することをお勧めします。

AWS 設定を使用して、組織内の AWS アカウント、および共有されているプロジェクトにアクセスすることもできます。

カスタムロールを作成し、アカウント AWS の設定からアクセスする場合は、セッションの長さを 12 時間に設定する必要があります。

チームメンバーにプロジェクトへのアクセス権がある場合は、高度な機能をアクティブ化する前と同じ方法でプロジェクトを表示してアクセスできます。共有しているプロジェクトは、独自の管理アカウントと AWS 組織の高度な機能をアクティブ化しても影響を受けません。

高度な機能をアクティブ化した後も、AWS 設定でプロジェクトを作成できますか？

高度な機能をアクティブ化した後、現在の AWS Organization でプロジェクトを作成することはできません。組織内にメンバーアカウントを作成する必要があります。

事前設定されたデフォルトを使用して、新しいマネージド AWS Organization を作成できます。これを行うには、AWS 設定で新しいプロジェクトを作成します。その後、追加のプロジェクトを作成し、チームメンバーを共同作業に招待できます。この管理アカウントの高度な機能を有効にすることもできます。

アクセスする新しい事前設定済み環境は、最初にサインアップしたときに作成された以前の AWS 組織に接続されません AWS。

高度な機能をアクティブ化するための準備方法

高度な機能をアクティブ化する前に、以下を実行することをお勧めします。

- すべてのチームメンバーに、高度な機能をアクティブ化することを知らせます。設定を変更しない限り、チームメンバーはプロジェクトに同じアクセス権を持ちますが、簡素化されたビュー AWS マネジメントコンソール からリージョンを表示し、より多くのサービスへのアクセスを提供するビューに変更されます。後で ID ソースを変更したり、新しい SCPs または RCPs を追加したりする場合は、それらの変更がサインイン方法やアクセスできる内容に影響する可能性があるため、ワークフォースに通知してください。
- 現在のすべてのプロジェクトの支出を表示し、コストが大幅に変動するプロジェクトがあるかどうかを書き留めます。使用制限がない場合、リソースによって発生するすべてのコストはお客様の負担となります。高度な機能をアクティブ化する前に、アイドル状態のリソースを削除または一時停止することをお勧めします。
- AWS 組織に加える変更を計画し、ベストプラクティスを調査します。別の でリソースを作成する場合は AWS リージョン、すべてのユーザーに適用されるサービスコントロールポリシーを変更して制限します AWS リージョン。新しいリージョンを含める RegionFloor には、 の statementID を変更する必要があります。詳細については、「[プロジェクトのサービスコントロールポリシー](#)」を参照してください。
- のステップに従った場合 [AI コーディングツールを接続する](#)、AI ツールには新しい AWS エクスペリエンスに関するコンテキストのみが含まれます。これにより、高度な機能を使用して開発する際に問題が発生する可能性があります。次の構成を推奨します。
 - 保存した場所から aws-starter-rules.md ファイルを削除します。エージェントに応じてルールファイルが保存されました。詳細については、「[ルールファイルを配置する場所](#)」を参照してください。

高度な機能をアクティブ化する方法

AWS 設定で高度な機能をアクティブ化できます。アクティベーションを元に戻すことはできません。

高度な機能をアクティブ化するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、プロジェクトを選択します。
3. アクション で、高度な機能の探索 を選択します。

アクティベーションは元に戻すことができないため、アクティベーションプロセスについて調べて学習する時間が長くなります。

4. アクティブ化する準備ができたなら、次の操作を行います。
 - a. チーム名には、チーム名を入力します。これは、ワークフォース ID の保存に使用される IAM Identity Center インスタンスの名前です。ワークフォースにこの名前が表示されます。
 - b. 管理アカウントの E メールアドレスを選択する で、E メールアドレスを選択します。この E メールアドレスは、管理アカウントにアクセスしてタスクを実行するために使用されます。別の E メールアドレスを使用する場合、AWS ID ソースとして Builder ID を使用している限り、AWS Builder ID E メールは AWS 設定から管理アカウントにアクセスできません。
 - c. 管理アカウントの E メールアドレスの検証プロセスを完了します。
 - d. 「確認」を選択し、アクティベーションを完了します。
 - e. 選択を確認し、アクティブ化を選択します。これを行うと、アカウントを元に戻すことはできません。

おめでとうございます。高度な AWS 機能をアクティブ化しました。

高度な機能をアクティブ化した後

高度な機能をアクティブ化したら、以下を実行できます。

- [ワークフォースメンバーを管理する](#)
- [Builder ID から ID AWS ソースを変更する](#)
- [組織ポリシーを削除する](#)
- [組織単位を作成する](#)
- [アカウント AWS リージョン で を有効または無効にする](#)
- [IAM ロールを作成する](#)

管理アカウントのルートユーザーパスワードを設定する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

高度な機能をアクティブ化すると、管理アカウントはアカウントの復旧にルート E メールアドレスを使用するようになりました。[セルフサービスオプション](#)を使用して AWS Builder ID へのアクセスを復旧することはできますが、ルートユーザー認証情報を使用して管理アカウントへのアクセスを復旧できるようになりました。ルートユーザーにアクセスするには、ルートユーザーパスワードを作成する必要があります。さらに、ルートユーザーのセキュリティを強化するために、多要素認証 (MFA) を有効にすることをお勧めします。

ルートユーザーパスワードを設定するには

1. [AWS マネジメントコンソール](#)を開き、ルートユーザーの E メールを使用してサインインを選択します。
2. E メールアドレスには、ルートユーザーの E メールアドレスを入力します。

これは、高度な機能をアクティブ化したときに管理アカウントに設定した E メールアドレスです。

3. [パスワードを忘れた場合] を選択します。

パスワードのリセットプロセスは、高度な機能をアクティブ化した後にルートユーザーのパスワードを設定する方法でもあります。

4. アカウントに関連付けられている E メールアドレスを入力します。
5. CAPTCHA テキストを入力し、ロボットではないを選択します。
6. Amazon Web Services からのメッセージ AWS アカウント については、に関連付けられている E メールを確認してください。メールは @verify.signin.aws で終わるアドレスから届きます。Eメールの指示に従って、ルートユーザーのパスワードを設定します。アカウントに E メールが表示されない場合は、スパムフォルダを確認してください。E メールにアクセスできなかった場合は、AWS「サインインユーザーガイド」の[AWS「アカウントの E メールにアクセスできません」](#)を参照してください。

ルートユーザーのパスワードを設定したら、アカウントへのアクセスを回復できます。次に、[アカウントのルートユーザーの多要素認証 AWS](#)のガイダンスに従って、ルート認証情報の MFA を有効にします。

ルートユーザーを使用してアカウントを復旧するか、[ルートユーザーの認証情報を必要とするタスク](#)を実行するために必要な場合にのみ使用します。日常業務では、AWS Builder ID などの ID ソースでサインインします。

ワークフォースメンバーを管理する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

高度な機能をアクティブ化したら、新しいワークフォースメンバーを招待したり、既存のワークフォースメンバーを削除したりできます。これには、既存のワークフォースを新しい AWS アカウントに追加することが含まれます。以下の情報は、ID ソースとして AWS Builder ID を使用する AWS 組織のみを対象としています。外部 ID プロバイダー (IdP) を使用する場合は、それらの ID プロバイダーでワークフォースを管理します。Identity Center ディレクトリを使用する場合は、[Identity Center ディレクトリの「ユーザーの管理」](#)で説明されているドキュメントを使用します。

新しいワークフォースメンバーを招待するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、プロジェクトを選択します。
3. ID 委任管理者アカウントの AWS コンソールにアクセスします。
4. AWS コンソールホームから、 を検索 **IAM Identity Center**して選択します。
5. IAM アイデンティティセンターコンソールのユーザーページで、新しいチームメンバーを招待を選択します。
6. E メールの場合は、E メールアドレスまたは E メールアドレスのリストを入力します。E メールアドレスはカンマ (,) またはセミコロン (;) で区切ります。
7. [Send invitation] (招待の送信) を選択します。

新しいワークフォースメンバーに AWS アカウントへのアクセス権を付与するには

ワークフォースメンバーが招待を承諾したら、アクセスできる AWS アカウントを設定します。

高度な機能をアクティブ化する前に、作成したアカウントに完全なアクセス許可を付与する

1. アクセスを許可するアカウントのアカウント ID を特定します。アカウント ID を確認するには、[AWS「アカウント識別子の表示」](#)を参照してください。
2. メインナビゲーションペインで、グループを選択します。
3. 識別したアカウント ID で始まるグループ名を選択します。
4. グループへのユーザーの追加を選択します。
5. 追加するユーザーを選択します。
6. ユーザーの追加 を選択します。

新規または既存の AWS アカウントにカスタムアクセス許可を付与する

AWS Account Access Manager でカスタムアクセスを設定します。詳細については、[AWS「アカウントへのアクセスを管理する」](#)を参照してください。

Note

カスタムロールを作成し、AWS 設定からロールへのアクセスを許可する場合は、セッションの長さを 12 時間に設定する必要があります。

ワークフォースメンバーを削除するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、プロジェクトを選択します。
3. アクション で、チームの管理 を選択します。

これにより、IAM アイデンティティセンターが開きます。

4. IAM Identity Center コンソールのユーザーページで、チームメンバーを選択し、削除を選択します。
5. 選択内容を確認し、削除を選択します。

チームメンバーはすぐに AWS 組織へのすべてのアクセスを失います。

これらのステップでは、まず 設定にアクセスして AWS ワークフォースメンバーを管理する方法を示します。ただし、委任管理者アカウント AWS マネジメントコンソール を使用して にサインインし、IAM アイデンティティセンターまたは IAM コンソールにアクセスして、ワークフォースメンバーを管理できます。

Builder ID から ID AWS ソースを変更する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

高度な機能をアクティブ化したら、ID ソースを Builder ID から AWS 変更できます。Builder ID から ID AWS ソースを変更した場合、Builder ID を AWS 組織の ID ソースとして再利用 AWS することはできません。ID ソースを変更すると、ワークフォースのサインイン方法が変わります。Builder ID AWS は引き続きプロジェクトアカウントを所有します。

Builder ID から ID AWS ソースを変更するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、プロジェクトを選択します。
3. この組織の管理で、ID ソースの変更を選択します。

これにより、IAM アイデンティティセンターが開きます。

4. IAM Identity Center コンソールの設定ページで、アクションを選択し、ID ソースを変更します。
5. ID ソースの選択 では、AWS ビルダー ID が選択されます。新しいソースを選択し、次へを選択します。
6. Active Directory に変更する場合は、次のページのメニューから使用可能なディレクトリを選択します。外部 ID プロバイダーに切り替える場合は、[「外部 ID プロバイダーに接続する方法」](#)のステップに従うことをお勧めします。
7. 変更を確認して確認します。組織の変更を理解していることを確認するには、すべてのチェックボックスを選択する必要があります。
8. 選択を確認し、ID ソースの変更を選択します。

これらのステップでは、まず AWS 設定にアクセスして ID ソースを変更する方法を示します。ただし、委任管理者アカウント AWS マネジメントコンソール を使用してサインインし、IAM Identity Center にアクセスして ID ソースを変更できます。

組織ポリシーを削除する

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

高度な機能をアクティブ化したら、リソースコントロールポリシー (RCPs) とサービスコントロールポリシー (SCPs) を変更して、AWS 組織のガバナンスを変更できます。特定の AWS マネージド組織ポリシーは、高度な機能をアクティブ化すると削除されます。詳細については、「[組織の管理ポリシー](#)」を参照してください。以下の情報は、ID ソースとして AWS Builder ID を使用する組織のみを対象とし AWS ています。別のソースを使用する場合は、「[ポリシーの更新](#)」の手順に従ってください。

サービスコントロールポリシー (SCP) を変更するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、プロジェクトを選択します。
3. この組織の管理で、ポリシーの管理を選択します。

これにより、AWS Organizations コンソールが開きます。

4. サービスコントロールポリシーページを選択します。
5. 更新するポリシーの名前を選択します。
6. ポリシーの詳細ページで、[Edit policy] (ポリシーの編集) を選択します。
7. 次の変更のいずれか、またはすべてを行います。

- ポリシーの名前を変更するには、[Policy name] (ポリシー名) に新しい名前を入力します。
- 説明を変更するには、[Policy description] (ポリシーの説明) に新しいテキストを入力します。
- 左側のペインでポリシーを JSON 形式で編集すると、ポリシーテキストを編集できます。または、右側のエディタでステートメントを選択し、コントロールを使用して要素を変更することもできます。各コントロールの詳細については、このトピックで前述した SCP の作成手順を参照してください。

8. 完了したら、[変更の保存] を選択します。

リソースコントロールポリシー (RCP) を変更するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、プロジェクトを選択します。
3. この組織の管理で、ポリシーの管理を選択します。

これにより、AWS Organizations コンソールが開きます。

4. リソースコントロールポリシーページを選択します。
5. 更新するポリシーの名前を選択します。
6. ポリシーの詳細ページで、[Edit policy] (ポリシーの編集) を選択します。
7. 次の変更のいずれか、またはすべてを行います。

- ポリシーの名前を変更するには、[Policy name] (ポリシー名) に新しい名前を入力します。
- 説明を変更するには、[Policy description] (ポリシーの説明) に新しいテキストを入力します。
- 左側のペインでポリシーを JSON 形式で編集すると、ポリシーテキストを編集できます。または、右側のエディタでステートメントを選択し、コントロールを使用して要素を変更することもできます。各コントロールの詳細については、このトピックで前述した「Creating an RCP procedure」を参照してください。

8. 完了したら、[変更の保存] を選択します。

これらのステップでは、AWS 設定で組織ポリシーを変更する方法を示します。ただし、管理アカウント AWS マネジメントコンソール でサインインし、AWS Organizations コンソールにアクセスしてこれらのポリシーを変更できます。

AWS 設定でアカウントを閉じる

Warning

現在、限られた数のお客様に新しいエクスペリエンスをリリースしています。このエクスペリエンスにまだアクセスできない場合があります。

組織とそこに保存されているすべてのプロジェクトが不要になった場合は、プロジェクトを閉じ、管理アカウントを閉じ、AWS ビルダー ID を削除できます。

消費した AWS リソースに対して料金が発生しないようにするには、プロジェクトを閉鎖し、組織の管理アカウントを閉鎖する必要がありますが、AWS プロファイルを閉鎖する必要はありません。関連付けられた AWS Builder ID は無料です。

管理アカウントを閉鎖したら、閉鎖した日から 90 日以内に再開できます。管理アカウントを閉鎖した日から 90 日以内が管理アカウント AWS を完全に閉鎖するまでの時間は、閉鎖後期間です。

管理アカウントを閉鎖する前に知っておくべきこと

管理アカウントを閉鎖する前に、次の点を考慮する必要があります。

- プロジェクトを閉じるときは、「」の考慮事項を考慮してください[プロジェクトを閉じる前に知っておくべきこと](#)。
- 管理アカウントを閉じる前に、すべてのプロジェクトを閉じる必要があります。
- AWS Builder ID を削除する前に、管理アカウントを閉じる必要があります。
- 管理アカウントを閉鎖したら、閉鎖した日から 90 日以内に再開できます。管理アカウントを閉鎖した日から 90 日以内が管理アカウントを完全に閉鎖する AWS までの時間は、閉鎖後期間です。
- 閉鎖後期間中であれば、アカウントを再開できます。
- 閉鎖時に組織に登録されたのと同じ E メールアドレスを、別の組織のプライマリ E メールとして使用することはできません。Sign up for AWS (new) の使用中に別の組織に同じ E メールアドレスを使用する場合は、閉鎖前に更新することをお勧めします。詳細については、「[AWS 設定で E メールアドレスを変更する](#)」を参照してください。
- 管理アカウントで多要素認証 (MFA) を有効にし、MFA デバイスを設定した場合、管理アカウントを閉鎖しても MFA は自動的に削除されません。90 日間の閉鎖後期間中に MFA をオンのままにする場合は、その期間中にアカウントにアクセスする必要がある場合に備えて、閉鎖後期間が終了するまで MFA デバイスをアクティブにしておいてください。ハードウェア TOTP トークンデバイスは、アカウントが完全に閉鎖された後に別のユーザーに関連付けることはできないので注意してください。後で別のユーザーとハードウェア TOTP トークンを使用する場合は、管理アカウントを閉じる前にハードウェア MFA デバイスを無効にするオプションがあります。

プロジェクトを閉じる

プロジェクトを閉じるには、「」を参照してください[AWS 設定でプロジェクトを閉じる](#)。

管理アカウントを閉じる

管理アカウントを閉鎖するには

1. <https://settings.aws.com> で AWS 設定を開きます。
2. メインナビゲーションペインで、プロジェクトを選択します。
3. アクション で、管理アカウントを閉じる を選択します。
4. 選択を確認し、管理アカウントを閉じるを選択します。

AWS ビルダー ID を削除する

AWS ビルダー ID を削除すると、次のようになります。

- アクセスの喪失: プロジェクトと組織に加えて、以前に AWS Builder ID を通じてアクセスした AWS ツールやサービスにアクセスできなくなります。
- コンテンツの削除: AWS Builder ID のみに関連付けられた残りのコンテンツは削除され、AWS Builder ID を使用してアプリケーションからコンテンツにアクセスまたは復元できなくなります。
- 個人情報の削除: AWS Builder ID の作成と管理に関連して提供された個人情報は削除されます。ただし、削除リクエストの記録やお客様を特定できない形式のデータなど、法律で要求または許可されている個人情報は保持 AWS される場合があります。

お客様の情報の処理方法の詳細については、AWS 「プライバシー通知」を参照してください。AWS コミュニケーション設定を更新するか、「コミュニケーション設定センター」にアクセスして AWS サブスクリプションを解除できます。

既存のログインは変更されません – Google や Apple などのログインを使用している場合、AWS ビルダー ID を削除しても、ログインアカウントに関連するものは削除されません。

AWS ビルダー ID を削除するには

1. <https://settings.aws.com> で AWS 設定を開きます。

管理アカウントを削除した場合でも、サインインすることはできます。

2. メインナビゲーションペインで、プロファイルの管理を選択します。
3. プロファイル情報 で、プロファイルの管理 を選択します。

Builder ID AWS プロファイルにリダイレクトされます。

4. メインナビゲーションペインで、プライバシーとデータを選択します。
5. AWS ビルダー ID を削除する で、AWS ビルダー ID を削除する を選択します。
6. 選択を確認して、[削除] をクリックします。

にサインアップする AWS (アドバンスド)

を初めて使用する場合 AWS、最初のステップは にサインアップすることです AWS アカウント。

「Sign up for AWS (advanced)」の情報に従うと、 は、アカウント設定とコンテンツの保存先を完全に制御できるアカウント AWS を作成します。このオプションは、HIPAA、FedRAMP などの規制対象ワークロードがある場合に使用します。

このサインアップを のサインアップ AWS (新規) と比較するには、「」を参照してください[サインアップオプションを比較する](#)。

にサインアップするには AWS アカウント、次の情報を提供する必要があります。

- ルートユーザーの E メールアドレスと – この E メールアドレスは、[ルートユーザー](#)のサインイン名として使用され、アカウントの回復に必要です。このアドレスに送信される電子メールを受信できる必要があります。特定のタスクを実行する前に、このアドレスに送信された電子メールへのアクセス権があることを確認する必要があります。
- AWS アカウント名 – アカウントの名前は、請求書、請求情報とコスト管理ダッシュボード、コンソールなどの AWS Organizations コンソールなど、複数の場所に表示されます。アカウントに名前を付ける際に標準的な方法を使用することで、アカウント名を認識しやすいものにすることをお勧めします。会社のアカウントの場合は、組織-目的-環境 (例えば、AnyCompany-audit-prod) のような命名基準を使用することを検討してください。個人アカウントの場合は、名-姓-目的 (例えば、paulo-santos-testaccount) のような命名基準を使用することを検討してください。
- 住所 – 連絡先と請求先住所がインドにある場合、アカウントのユーザー契約は、インドの現地 AWS 販売者である Amazon Web Services India Private Limited (AWS インド) と締結されます。検証プロセスの一部として CVV を指定する必要があります。銀行によっては、ワンタイムパスワードを入力する必要がある場合もあります。AWS India は、検証プロセスの一環として支払い方法 2 INR を請求します。AWS India は、検証が完了した後に 2 INR を返金します。
- 電話番号 – この番号は、本人確認とアカウントの所有権の確認に使用されます。この電話番号で通話と SMS メッセージを受信できる必要があります。

Important

このアカウントがビジネス用である場合は、従業員が転職したり退職したり AWS アカウントしても、会社が へのアクセスを保持できるように、会社の電話番号を使用してください。

ステップ 1: アカウントを作成する

これらの手順は、インド AWS アカウント 国外で 作成するためのものです。インドでのアカウントの作成については、「[India AWS アカウント で 作成する AWS](#)」を参照してください。が管理する組織の一部であるアカウントを作成するには AWS Organizations、AWS Organizations 「ユーザーガイド」の「[組織内のメンバーアカウントの作成](#)」を参照してください。

AWS マネジメントコンソール

を作成するには AWS アカウント

1. [AWSのサインアップ](#) ページを開きます。
2. ルートユーザーの E メールアドレスと AWS アカウント 名前を入力し、E メールアドレスの確認を選択します。これにより、検証コードが E メールアドレスに送信されます。

Important

このアカウントがビジネス用である場合は、安全な企業ディストリビューションリスト (など `it.admins@example.com`) を使用して、従業員が転職したり退職したり AWS アカウント しても、会社が へのアクセスを保持できるようにします。この E メールアドレスはアカウントのルートユーザー認証情報のリセットに使用できるため、この配信リストやアドレスへのアクセスを保護してください。

3. 検証コードを入力し、[検証] を選択します。
4. ルートユーザーの強力なパスワードを入力し、確認してから、続行を選択します。パスワードが次の条件を満たす AWS 必要があります。
 - 8 ~ 128 文字で構成されていること。
 - 英字の大文字、英字の小文字、数字、記号 (! @ # \$ % ^ & * () < > [] { } | _ + =) のうち、少なくとも 3 つの文字タイプを使用する必要があります。
 - AWS アカウント 名前や E メールアドレスと同じにすることはできません。
5. アカウントプランを選択します。詳細については、「[無料利用枠プラン](#)」を参照してください。
6. 連絡先情報を入力し、[AWS カスタマーアグリーメント](#) を読んで同意します。承諾する前に、必ず用語を理解してください。

⚠ Important

このアカウントがビジネス用である場合は、個人の電話番号ではなく会社の電話番号を入力するのがベストプラクティスです。個人の E メールアドレスや個人の電話番号でアカウントのルートユーザーを設定すると、アカウントが安全でなくなる可能性があります。

7. 請求情報を入力します。請求情報に別の AWS 請求先住所を使用する場合は、新しい住所を使用するを選択します。

有効な支払い方法を追加するまでは、サインアッププロセスを続行できません。

8. ID の確認が必要になる場合があります。
 - a. 国またはリージョンコードには、数分以内に連絡できる電話番号を入力します。
 - b. 電話番号には、数分以内に到達できる電話番号を入力します。
 - c. SMS の送信 を選択します。
 - d. 自動システムから連絡があったら、受け取ったコードを入力し、続行を選択します。
9. 使用可能な AWS サポート プランのいずれかを選択します。利用可能な Support プランとその利点の説明については、「[サポート プランの比較](#)」を参照してください。
10. [登録を完了] を選択します。アカウントがアクティブ化されていることを示す確認ページが表示されます。
11. アカウントが有効化されたことを確認する E メールメッセージが届いているか、E メールフォルダとスパムフォルダを確認します。有効化は、通常は数分で完了しますが、場合によっては最大 24 時間かかることがあります。
12. アクティベーションメッセージを受信したら、にサインイン[AWS マネジメントコンソール](#)して使用を開始できます AWS のサービス。アカウント設定の管理方法に関する一般情報については、「[を設定する AWS アカウント](#)」を参照してください。

複数の AWS アカウント マネージドスルーの場合は AWS Organizations、IAM Identity Center の管理ユーザーに管理アクセスを割り当てます。手順については、[IAM Identity Center ユーザーガイドの「IAM Identity Center 管理ユーザーの AWS アカウント アクセスを設定する」](#)を参照してください。

AWS CLI & SDKs

組織内の管理アカウントにサインインした状態で [CreateAccount](#) 操作を実行すると、AWS Organizations が管理する組織にメンバーアカウントを作成できます。

AWS Command Line Interface (AWS CLI) または AWS API オペレーションを使用して、組織の AWS アカウント 外部でスタンドアロンを作成することはできません。

ステップ 2: (推奨) をインストールする AWS CLI

「のインストール」の AWS CLI 手順に従って、をインストールします。 [AWS CLI](#) バージョン 2.32.0 以降が必要です。

を使用して AWS CLI、エージェントにユーザーに代わって AWS リソースを管理させることができます。

をインストールしたら AWS CLI、次のコマンドを使用してプログラムでサインインします。

```
aws login
```

これにより、認証情報が 15 分ごとに自動的にローテーションされ、手動による介入なしでセッションが最大 12 時間有効になります。

次のコマンドを使用して、認証情報が機能していることを確認します。

```
aws sts get-caller-identity
```

へのアクセスの詳細については AWS アカウント、「」を参照してください [へのアクセス AWS アカウント](#)。

ステップ 3: (推奨) AWS MCP サーバーを設定する

AWS MCP サーバーは、モデルコンテキストプロトコル (MCP) AWS を通じて へのアクセスをエージェントに許可するマネージドサーバーです。エージェントは、認証なしで AWS ドキュメントを検索し、サービス情報を取得できます。AWS API コールを実行する、サンドボックス環境で Python スクリプトを実行する、または厳選されたスキルに従うには、エージェントは既存の IAM 認証情報を使用して認証します。詳細については、[「エージェントツールキットとは AWS」を参照してください](#)。

サインアッププロセスが完了したら、以下のトピックを参照してください。

- [関連 AWS サービス](#)
- [の使用 AWS アカウントのルートユーザー](#)
- [へのアクセス AWS アカウント](#)
- [AWS アカウント ガバナンス構造を計画する](#)
- [を設定する AWS アカウント](#)
- [のトラブルシューティング AWS アカウント](#)
- [インドでのアカウントの管理](#)
- [を閉じる AWS アカウント](#)
- [を再開する AWS アカウント](#)

関連 AWS サービス

サインアップ方法に応じて AWS、AWS アカウント または プロジェクトにアクセスできます。プロジェクトには、AWS アカウント と他の共同作業者と共有するための設定が含まれています。詳細については、「[サインアップオプションを比較する](#)」を参照してください。このセクションでは、「Sign up for AWS (advanced)」を使用して を作成する AWS アカウント 方法が、次のサービスとシームレスに連携する方法について説明します。

- IAM

AWS アカウント は AWS Identity and Access Management (IAM) と緊密に統合されています。アカウントで IAM を使用することで、そのアカウントで作業する他のユーザーに対して、そのユーザーが自分の業務を遂行するために必要なアクセスのみを付与できるようになります。また、IAM を使用して、アカウント固有の情報だけでなく、すべての AWS リソースへのアクセスを制御します。AWS アカウントの構造の設定を大きく進める前に、IAM の主要な概念とベストプラクティスを十分に理解しておくことが重要です。詳細については、「IAM ユーザーガイド」の「[IAM でのセキュリティベストプラクティス](#)」を参照してください。

- AWS Organizations

会社が大きい場合、または成長する可能性がある場合は、会社の特定の構造を反映する複数の AWS アカウントをセットアップできます。は、マルチアカウント環境を構築および管理するための基盤となるインフラストラクチャと機能 AWS Organizations を提供します。既存のアカウントを組織に結合して、アカウントを一元管理することができます。自動的に組織の一部であるアカウントを作成し、他のアカウントを組織に招待することができます。アカウントの一部または全部

に影響するポリシーをアタッチすることもできます。詳細については、「[を使用するタイミング AWS Organizations](#)」を参照してください。

以下のアカウント関連の API アクションは、AWS アカウント管理 AWS Organizations API ではなく、API の一部です。これらのオペレーションは、通常、アカウント管理ドキュメントで検索されますが、AWS Organizations 名前空間で定義されているため、ここに含めます。

- [CreateAccount](#)
- [CreateGovCloudAccount](#)
- [DescribeAccount](#)
- AWS Control Tower

AWS Control Tower は、安全なマルチアカウント AWS 環境をセットアップして管理するための簡単な方法を提供します。は、を使用してマルチアカウント環境の作成 AWS Control Tower を自動化し、初期アカウントのセットをインスタンス化し AWS Organizations、環境のいくつかのデフォルトのガードレールと設定を使用します。AWS Control Tower を使用して、アカウントが組織のポリシーに準拠していることを確認しながら、いくつかのステップ AWS アカウント で新しい をプロビジョニングできます。詳細については、「[を使用するタイミング AWS Control Tower](#)」を参照してください。

の使用 AWS アカウントのルートユーザー

サインアップ方法に応じて AWS、AWS アカウント または プロジェクトにアクセスできます。プロジェクトには、AWS アカウント と他の共同作業者と共有するための設定が含まれています。詳細については、「[サインアップオプションを比較する](#)」を参照してください。このセクションでは、「Sign up for AWS (advanced)」を使用して AWS アカウント 作成した でルートユーザーを使用する方法について説明します。AWS Builder ID は、ルートユーザーの E メールアドレスではなく各プロジェクトアカウントを所有しているため、高度な機能をアクティブ化した後を含め、プロジェクトアカウントでルートユーザーを使用することはできません。

を作成するときは AWS アカウント、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 ルート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。

日常業務にルートユーザーを使用することを回避するために、[AWS IAM アイデンティティセンターで管理ユーザーを設定する](#)方法について説明します。ルートユーザーのセキュリティに関するその他

の推奨事項については、「[AWS アカウントのルートユーザーのベストプラクティス](#)」を参照してください。

Important

のルートユーザー認証情報を持つユーザーは、請求情報を含むアカウント内のすべてのリソースに AWS アカウント 無制限にアクセスできます。

ルートユーザーのパスワードを[変更](#)または[リセット](#)したり、ルートユーザーのアクセスキー (アクセスキー ID とシークレットアクセスキー) を[作成](#)または[削除](#)したりできます。ルートユーザーを使用してサインインする方法については、「[サインインユーザーガイド](#)」の「[ルートユーザー AWS マネジメントコンソールとしてにサインインする](#)」を参照してください。AWS

へのアクセス AWS アカウント

この情報は、サインアップ for AWS (アドバンスド) AWS を使用して にサインアップ AWS アカウントした場合、またはアカウントの高度な機能をアクティブ化した場合の へのアクセスに関するものです。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

には、次のいずれか AWS アカウント の方法でアクセスできます。

AWS マネジメントコンソール

[AWS マネジメントコンソール](#) は、AWS アカウント 設定と AWS リソースの管理に使用できるブラウザベースのインターフェイスです。

AWS コマンドラインツール

AWS コマンドラインツールを使用すると、システムのコマンドラインでコマンドを発行して、AWS アカウント および AWS タスクを実行できます。コマンドラインを使用すると、コンソールよりも高速かつ便利になります。コマンドラインツールは、AWS タスクを実行するスクリプトを構築する場合にも便利です。には、次の 2 セットのコマンドラインツール AWS が用意されています。

- [AWS Command Line Interface](#) (AWS CLI)。 のインストールと使用の詳細については AWS CLI、[AWS Command Line Interface 「ユーザーガイド」](#)を参照してください。
- [AWS Tools for Windows PowerShell](#)。Tools for Windows PowerShell のインストールおよび使用の方法については、[AWS Tools for PowerShell ユーザーガイド](#)を参照してください。

AWS SDK

AWS SDKs は、さまざまなプログラミング言語とプラットフォーム (Java、Python、Ruby、.NET、iOS、Android など) のライブラリとサンプルコードで構成されます。SDK は、暗号署名によるリクエスト、エラーの管理、リクエストの自動再試行などのタスクを処理します。AWS SDKs [「Amazon Web Services のツール」](#) を参照してください。

AWS アカウント管理 HTTPS クエリ API

AWS アカウント管理 HTTPS クエリ API を使用すると、AWS アカウント および へのプログラムによるアクセスが可能になります AWS。HTTPS クエリ API を使用すると、HTTPS リクエストを直接サービスに発行できます。HTTPS API を使用する場合は、認証情報を使用してリクエストにデジタル署名するコードを含める必要があります。詳細については、「[HTTP クエリリクエストを作成して API を呼び出す](#)」を参照してください。

AWS アカウント ガバナンス構造を計画する

この情報は、サインアップ for AWS (アドバンスト) AWS の使用にサインアップした場合、またはアカウントの高度な機能をアクティブ化した場合の AWS アカウント ガバナンス構造の計画に関するものです。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

1 つのアカウントで AWS ジャーニーを開始したかもしれませんが、では、ワークロードのサイズと複雑さが大きくなるにつれて、複数のアカウントを設定する AWS ことをお勧めします。中規模企業であっても大企業であっても、データとワークロードのニーズを確実に満たすガバナンス構造の計画を作成する必要があります。

このセクションでは、マルチアカウントガバナンス構造を実現するために AWS で使用できる利点とガバナンスサービスについて説明します。

トピック

- [複数の を使用する利点 AWS アカウント](#)
- [を使用するタイミング AWS Organizations](#)
- [を使用するタイミング AWS Control Tower](#)
- [API 操作モードについて](#)

複数の を使用する利点 AWS アカウント

この情報は、サインアップ for AWS (アドバンスド) の使用にサインアップ AWS アカウントした場合、またはアカウントの高度な機能をアクティブ化した場合、複数の AWS を使用する利点に関するものです。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

AWS アカウント で基本的なセキュリティ境界を形成します AWS クラウド。これらはリソースのコンテナとして機能し、安全で適切に管理された環境を作成するために不可欠な重要な分離レイヤーを提供します。詳細については、「[とは AWS アカウント](#)」を参照してください。

リソースを分離 AWS アカウント することで、クラウド環境で以下の原則をサポートできます。

- セキュリティコントロール - アプリケーションごとに異なるセキュリティプロファイルがあり、それらの周りに異なるコントロールポリシーとメカニズムが必要になる場合があります。例えば、監査人と話す方がはるかに簡単で、[Payment Card Industry \(PCI\) セキュリティ標準](#)の対象となるワークロードのすべての要素を AWS アカウント ホストする単一の をポイントできます。
- 分離 - AWS アカウント はセキュリティ保護の単位です。潜在的なリスクとセキュリティ上の脅威は、他の に影響を与え AWS アカウント ずに に含める必要があります。チームやセキュリティプロファイルが異なるため、セキュリティニーズが異なる場合があります。
- 多数のチーム - チームごとに異なる責任とリソースニーズがあります。チームを別々の場所に移動することで、チームが互いに干渉するのを防ぐことができます AWS アカウント。
- データの分離 — チームの分離に加えて、データストアをアカウントに分離することが重要です。これにより、そのデータストアにアクセスして管理できるユーザーの数を制限できます。これには、高度にプライベートなデータへの暴露が含まれており、[一般データ保護規則 \(GDPR\)](#) への適合に役立ちます。
- 業務プロセス - 事業単位や製品によって目的やプロセスが異なる場合があります。複数の を使用すると AWS アカウント、ビジネスユニットの特定のニーズをサポートできます。
- 請求 — アカウントは、請求レベルで項目を分ける唯一の真の方法です。複数のアカウントは、ビジネスユニット、機能チーム、または個々のユーザー間で課金レベルでアイテムを分離するのに役立ちます。明細項目を区切りながら、すべての請求書を 1 つの支払者 (AWS Organizations と一括請求を使用) に統合できます AWS アカウント。
- クォータ割り当て - AWS サービスクォータは、それぞれ個別に適用されます AWS アカウント。ワークロードを異なる AWS アカウント に分けることで、互いのクォータを消費し合うのを防止できます。

このドキュメントで説明しているすべての推奨事項と手順は、[AWS Well-Architected フレームワーク](#)に適合するものです。このフレームワークは、柔軟性、耐障害性、スケーラブルなクラウドインフラストラクチャの設計を支援することを目的としています。小規模から始める場合でも、フレームワークにおけるこのガイダンスを守りながら進めることをお勧めします。そうすることで、成長に伴う継続的な運用に影響を与えることなく、環境を安全に拡張できます。

複数の の管理 AWS アカウント

複数のアカウントを追加する前に、アカウントの管理計画を策してください。そのためには、 [を使用することをお勧めします](#)。これは[AWS Organizations](#)、組織内のすべての を管理する AWS アカウント ための無料の AWS サービスです。

AWS は も提供します。これにより AWS Control Tower、Organizations に AWS マネージドオートメーションのレイヤーが追加され AWS CloudTrail AWS Config、Amazon CloudWatch AWS Service Catalogなどの他の AWS サービスと自動的に統合されます。これらのサービスには追加料金が発生する可能性があります。詳細については、「[AWS Control Tower 料金表](#)」を参照してください。

関連情報

- [を使用するタイミング AWS Organizations](#)
- [を使用するタイミング AWS Control Tower](#)

を使用するタイミング AWS Organizations

この情報は、サインアップ for AWS (アドバンスド) AWS の使用にサインアップ AWS Organizations した場合、またはアカウントの高度な機能をアクティブ化した場合に使用するタイミングに関するものです。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

AWS Organizations は、 をグループ AWS アカウント として管理するために使用できる AWS サービスです。このサービスには、アカウントのすべての請求書をグループ化し、単一の支払者によって処理可能にする一括請求 (コンソリデेटッドビルリング) などの機能が備わっています。ポリシーベースのコントロールを使用して、組織のセキュリティを一元的に管理することもできます。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。

信頼されたアクセス

AWS Organizations を使用してアカウントをグループとして管理する場合、組織のほとんどの管理タスクは組織の管理アカウントでのみ実行できます。デフォルトでは、組織自体の管理に関連する操作

のみが含まれます。Organizations とその AWS サービス間の信頼されたアクセスを有効にすることで、この追加機能を他の サービスに拡張できます。信頼されたアクセスは、組織とそれに含まれるアカウントに関する情報にアクセスするためのアクセス許可を指定された AWS サービスに付与します。アカウント管理の信頼されたアクセスを有効にすると、アカウント管理サービスは、組織のすべてのメンバーアカウントのメタデータ (主要連絡先情報や代替連絡先情報など) にアクセスするためのアクセス許可を組織およびその管理アカウントに付与します。

詳細については、「[AWS アカウント管理の信頼されたアクセスを有効にする](#)」を参照してください。

委任管理者

信頼されたアクセスを有効にしたら、いずれかのメンバーアカウントを AWS アカウント管理の委任管理者アカウントとして指定することもできます。これにより、委任管理者アカウントは、これまで管理アカウントのみが行えた、組織内のメンバーアカウントに対するアカウント管理のメタデータ管理タスクを実行できるようになります。委任管理者アカウントは、アカウント管理サービスの管理タスクにのみアクセスできます。委任管理者アカウントは、管理者アカウントが持つ組織に対するすべての管理者アクセス権を持っているわけではありません。

詳細については、「[アカウント管理の委任管理者 AWS アカウントを有効にする](#)」を参照してください。

サービスコントロールポリシー

AWS アカウント が によって管理されている組織の一部である場合 AWS Organizations、組織の管理者は、メンバーアカウントのプリンシパルが実行できる操作を制限できる[サービスコントロールポリシー \(SCPs\)](#) を適用できます。SCP はアクセス許可を付与するものではなく、メンバーアカウントが使用できるアクセス許可を制限するフィルターです。メンバーアカウントのユーザーまたはロール (プリンシパル) は、そのアカウントに適用される SCP とプリンシパルにアタッチされた IAM アクセス許可ポリシーの両方によって許可される操作のみを実行できます。例えば、SCP を使用して、アカウントのプリンシパルが自分のアカウントの代替連絡先を変更できないように設定することもできます。

が適用される SCPs 「」を参照してください[AWS Organizations サービスコントロールポリシーを使用してアクセスを制限する](#)。AWS アカウント

AWS アカウント管理の信頼されたアクセスを有効にする

これらの手順は、サインアップ for AWS (アドバンスド) AWS の使用にサインアップした場合、またはアカウントの高度な機能をアクティブ化した場合に、AWS アカウント管理の信頼されたアクセス

を有効にする方法を示しています。サインアップオプションを比較するには、「」を参照してください [サインアップオプションを比較する](#)。

AWS アカウント管理の信頼されたアクセスを有効にすると、管理アカウントの管理者は、の各メンバーアカウントに固有の情報とメタデータ (プライマリまたは代替の連絡先の詳細など) を変更できます AWS Organizations。詳細については、「AWS Organizations ユーザーガイド」の「[AWS Account Management and AWS Organizations](#)」を参照してください。信頼されたアクセスの仕組みに関する一般的な情報については、「[他の AWS サービス AWS Organizations での の使用](#)」を参照してください。

信頼されたアクセスが有効化されたら、accountID パラメータをサポートする [アカウント管理 API オペレーション](#) で、このパラメータを使用できるようになります。このパラメータを正常に使用できるのは、管理アカウントの認証情報、または組織の委任管理者アカウントの認証情報 (委任管理者アカウントを有効にしている場合) を使用してオペレーションを呼び出した場合のみです。詳細については、「[アカウント管理の委任管理者 AWS アカウントを有効にする](#)」を参照してください。

組織内のアカウント管理用の信頼されたアクセスを有効にするには、次の手順を使用します。

最小アクセス許可

これらのタスクを実行するには、以下の要件を満たす必要があります。

- これは、組織の管理アカウントからのみ実行できます。
- 組織で、[すべての機能が有効になっている](#) 必要があります。

AWS マネジメントコンソール

AWS アカウント管理の信頼されたアクセスを有効にするには

1. [AWS Organizations コンソール](#) にサインインします。組織の管理アカウントで、IAM ユーザーとしてサイン・インするか、IAM ロールを引き受けるか、ルートユーザーとしてサイン・インする (推奨されません) 必要があります。
2. ナビゲーションペインで、[Services] (サービス) を選択します。
3. サービスのリストで [AWS Account Management] (アカウント管理) を選択します。
4. [Enable trusted access (信頼されたアクセスを有効にする)] を選択します。
5. AWS 「アカウント管理の信頼されたアクセスを有効にする」ダイアログボックスで、「有効化して確認します」と入力し、「信頼されたアクセスを有効にする」を選択します。

AWS CLI & SDKs

AWS アカウント管理の信頼されたアクセスを有効にするには

次のコマンドの実行後に、組織の管理アカウントの認証情報を使用して、`--accountId` パラメータを使用するアカウント管理 API オペレーションを呼び出し、組織内のメンバーアカウントを参照することができます。

- AWS CLI: [enable-aws-service-access](#)

次の例では、呼び出し元の AWS アカウントの組織でアカウント管理の信頼されたアクセスを有効にします。

```
$ aws organizations enable-aws-service-access \
    --service-principal account.amazonaws.com
```

このコマンドは成功時に出力を生成しません。

アカウント管理の委任管理者 AWS アカウントを有効にする

これらの手順は、サインアップ for AWS (アドバンスド) AWS の使用にサインアップした場合、またはアカウントの高度な機能をアクティブ化した場合に、AWS アカウント管理の委任管理者アカウントを有効にする方法を示しています。サインアップオプションを比較するには、「」を参照してください [サインアップオプションを比較する](#)。

アカウント管理サービスには、組織ごとに 1 つの委任管理者 AWS アカウントを登録できます。このアカウントを登録すると、そのアカウントのユーザーとロールは、オプションの `AccountId` パラメータをサポートすることで Organizations モードで機能できる `account` 名前空間で AWS CLI および AWS SDK オペレーションを呼び出すことができます。これにより、委任管理者は他のメンバー AWS アカウントのアカウント管理 API オペレーションを呼び出すことができます AWS Organizations。

組織内のメンバーアカウントを委任管理者アカウントとして登録するには、以下の手順を使用します。

AWS CLI & SDKs

アカウント管理サービス用の委任管理者アカウントを登録するには

次のコマンドを使用して、アカウント管理サービス用の委任管理者を有効にすることができます。

最小アクセス許可

これらのタスクを実行するには、以下の要件を満たす必要があります。

- これは、組織の管理アカウントからのみ実行できます。
- 組織で、[すべての機能が有効になっている](#) 必要があります。
- [組織内のアカウント管理で信頼されたアクセスが有効になっている](#) 必要があります。

次のサービスプリンシパルを指定する必要があります。

```
account.amazonaws.com
```

- AWS CLI: [register-delegated-administrator](#)

次の例では、組織のメンバーアカウントをアカウント管理サービスの委任管理者として登録します。

```
$ aws organizations register-delegated-administrator \
  --account-id 123456789012 \
  --service-principal account.amazonaws.com
```

このコマンドは成功時に出力を生成しません。

このコマンドを実行したら、アカウント 123456789012 の認証情報を使用して、`--account-id`パラメータを使用して組織内のメンバーアカウントを参照するアカウント管理 AWS CLI および SDK API オペレーションを呼び出すことができます。

AWS マネジメントコンソール

このタスクは、AWS アカウント管理コンソールではサポートされていません。このタスクは、AWS CLI またはいずれかの AWS SDKs。

AWS Organizations サービスコントロールポリシーを使用してアクセスを制限する

この情報は、サインアップ for AWS (アドバンスド) の使用にサインアップした場合、またはアカウントの高度な機能をアクティブ化した場合に、AWS Organizations サービスコントロールポリシー AWS を使用してアクセスを制限するためのものです。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

このトピックでは、AWS Organizations のサービスコントロールポリシー (SCP) を使用して組織のアカウントのユーザーやロールが実行できる操作を制限する方法を、例を示して説明します。サービスコントロールポリシーの詳細については、AWS Organizations ユーザーガイドの以下のトピックを参照してください。

- [SCP の作成](#)
- [OU およびアカウントに SCP をアタッチする](#)
- [SCP についての戦略](#)
- [SCP ポリシー構文](#)

Example例 1: アカウントが自分の代替連絡先を変更できないようにする

次の例は、[スタンドアロンアカウントモード](#)で PutAlternateContact と DeleteAlternateContact の操作がどのメンバーアカウントからも呼び出されないようにするものです。これにより、影響を受けるアカウントのプリンシパルが自分の代替連絡先を変更できなくなります。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Deny",
      "Action": [
        "account:PutAlternateContact",
        "account>DeleteAlternateContact"
      ],
      "Resource": [ "arn:aws:account::*:account" ]
    }
  ]
}
```

```
}
```

Example例 2: 組織内の他のメンバーアカウントの代替連絡先をメンバーアカウントに変更できないようにする

次の例では、Resource 要素を「*」として一般化しており、これは要素が[スタンドアロンモード](#)と組織モードのリクエストの両方に適用されることを意味します。つまり、アカウント管理についてと委任管理者アカウントでも、SCP が適用されると組織内の任意のアカウントの代替連絡先を変更できなくなります。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Deny",
      "Action": [
        "account:PutAlternateContact",
        "account>DeleteAlternateContact"
      ],
      "Resource": [ "*" ]
    }
  ]
}
```

Example例 3: OU のメンバーアカウントが独自の代替連絡先を変更できないようにする

次の SCP の例には、アカウントの組織パスと 2 つの OU のリストを比較する条件が含まれています。これにより、指定された OU 内の任意のアカウントのプリンシパルが独自の代替連絡先を変更できないようにブロックされます。

を使用するタイミング AWS Control Tower

この情報は、サインアップ for AWS (アドバンスド) AWS の使用にサインアップ AWS Control Tower した場合、またはアカウントの高度な機能をアクティブ化した場合に使用するタイミングに関するものです。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

AWS Organizations は、AWS 環境全体を一元的に管理および保護できる基本的なサービスです。この AWS Organizations 中心的なアプローチの重要な要素は、AWS Control Tower。は Organizations 内のマネジメントコンソール AWS Control Tower として機能し、規範的なベストプラクティスを適用して、安全でマルチアカウント AWS 環境をセットアップおよび管理するための効率的な方法を提供します。

が提供するこのセキュリティのベストプラクティスアプローチは、AWS のコア機能 AWS Control Tower を拡張します AWS Organizations。は、組織とアカウントが推奨されるセキュリティおよびコンプライアンス標準に確実に準拠できるように、一連の予防ガードレールと検出ガードレール AWS Control Tower を適用します。

を使用して適切に設計された AWS Organizations 構造を確立することで AWS Control Tower、スケーラブルで安全で準拠した AWS 環境を迅速にデプロイできます。クラウド管理とガバナンスに対するこの一元化されたアプローチは、最高レベルのセキュリティとコンプライアンス AWS クラウドを維持しながら、AWS の能力を最大限に活用したい企業にとって不可欠です。

詳細については、AWS Control Tower ユーザーガイドの「[AWS Control Tower とは](#)」を参照してください。

API 操作モードについて

この情報は、サインアップ for AWS (アドバンスド) AWS の使用にサインアップした場合、またはアカウントの高度な機能をアクティブ化した場合の API オペレーションモードを理解するためのものです。サインアップオプションを比較するには、「[サインアップオプションを比較する](#)」を参照してください。

AWS アカウントの属性を操作する API オペレーションは、常に 2 つのオペレーションモードのいずれかで動作します。

- **スタンドアロンコンテキスト** — このモードは、アカウント内のユーザーまたはロールが同じアカウント内のアカウント属性にアクセスする、またはそのアカウント属性を変更する場合に使用されます。スタンドアロンコンテキストモードは、アカウント管理 AWS CLI または AWS SDK オペレーションのいずれかを呼び出すときに AccountId パラメータを含めない場合に自動的に使用されます。
- **組織コンテキスト** — このモードは、組織内の 1 つのアカウントのユーザーまたはロールが、同じ組織内の別のメンバーアカウントのアカウント属性にアクセスする、またはそのアカウント属性を変更する場合に使用されます。アカウント管理 AWS CLI または AWS SDK オペレーションのいずれかを呼び出すときに AccountId パラメータを含めると、組織コンテキストモードが自動的に使

用されます。このモードでは、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのみから操作を呼び出すことができます。

AWS CLI および AWS SDK オペレーションは、スタンドアロンまたは組織のコンテキストで機能します。

- AccountId パラメータを含めない場合、操作はスタンドアロンコンテキストで実行され、リクエスト作成に使用したアカウントにリクエストが自動的に適用されます。これは、アカウントが組織のメンバーであるかどうかにはかかりません。
- AccountId パラメータを含めた場合は、操作は組織コンテキストで実行され、指定した組織アカウントで動作します。
 - 操作を呼び出すアカウントが、アカウント管理サービスの管理アカウントまたは委任管理者アカウントである場合、AccountId パラメータにその組織の任意のメンバーアカウントを指定して、指定したアカウントを更新することができます。
 - 代替連絡先に関する操作のいずれかを呼び出して、AccountId パラメータに自身のアカウント番号を指定できる組織内のアカウントは、アカウント管理サービス用の[委任管理者アカウント](#)として指定されたアカウントのみです。管理アカウントを含むその他のアカウントは、AccessDenied 例外を受信します。
- スタンドアロンモードで操作を実行する場合、すべてのリソースを許可する "*"、または[スタンドアロンアカウント用の構文を使う ARN](#) のどちらかの Resource 要素を含む IAM ポリシーで、操作の実行が許可されている必要があります。
- 組織モードで操作を実行する場合、すべてのリソースを許可する Resource のいずれかの "*" 要素を含む IAM ポリシー、または[組織内のメンバーアカウント用の構文に従った ARN](#) で、操作の実行が許可されている必要があります。

アカウント属性を更新するアクセス許可の付与

ほとんどの AWS オペレーションと同様に、IAM アクセス許可ポリシー AWS アカウント を使用して、 のアカウント属性を追加、更新、または削除するためのアクセス許可を付与します。 https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html IAM アクセス許可ポリシーを IAM プリンシパル (ユーザーまたはロール) にアタッチすると、そ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、どのアクションを実行できるかを指定することができます。

以下は、アクセス許可ポリシーを作成する際のアカウント管理特有の考慮事項です。

の Amazon リソースネーム形式 AWS アカウント

- ポリシーステートメントの resource 要素に含める AWS アカウント ことができる の [Amazon リソースネーム \(ARN\)](#) は、参照するアカウントがスタンドアロンアカウントであるか、組織内のアカウントであるかに基づいて構築されます。「[API 操作モードについて](#)」に関する前のセクションを参照してください。

- スタンドアロンアカウントのアカウント ARN:

```
arn:aws:account::{AccountId}:account
```

AccountID パラメータを含めないことによってスタンドアロンモードでアカウント属性のオペレーションを実行する場合は、この形式を使用する必要があります。

- 組織内のメンバーアカウントのアカウント ARN:

```
arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
```

AccountID パラメータを含めることによって組織モードでアカウント属性のオペレーションを実行する場合は、この形式を使用する必要があります。

IAM ポリシーのコンテキストキー

アカウント管理サービスには、付与するアクセス許可をきめ細かく制御するための [アカウント管理サービス固有の条件キー](#) もいくつか用意されています。

account:AccountResourceOrgPaths

コンテキストキー account:AccountResourceOrgPaths を使用すると、組織の階層から特定の組織単位 (OU) へのパスを指定できます。その OU に含まれるメンバーアカウントのみが条件に一致します。次の例のスニペットは、指定された 2 つの OU のいずれかに所属するアカウントにのみポリシーを適用するように制限しています。

account:AccountResourceOrgPaths は複数値を持つ文字列型のため、[ForAnyValue](#) または [ForAllValues](#) 複数値文字列演算子を使用する必要があります。また、組織内の OUs へのパスを参照している場合でも account、条件キーのプレフィックスは であることに注意してください。

```
"Condition": {
  "ForAnyValue:StringLike": {
```



```
    "account:AccountResourceOrgPaths": [  
      "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*",  
      "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/*"  
    ]  
  }  
}
```

account:AccountResourceOrgTags

コンテキストキー `account:AccountResourceOrgTags` を使用すると、組織内のアカウントにアタッチできるタグを参照できます。タグはキーと値の文字列のペアで、アカウント内のリソースを分類し、ラベル付けするために使用できます。詳細については、AWS Resource Groups ユーザーガイドの「[タグエディタの使用](#)」を参照してください。属性ベースのアクセス制御戦略の一環としてタグを使用する方法については、「IAM ユーザーガイド」の「[AWSの ABAC とは](#)」を参照してください。次の例のスニペットは、`project` キー、および `blue` または `red` のいずれかの値を含むタグを持つ組織内のアカウントにのみポリシーを適用するように制限しています。

`account:AccountResourceOrgTags` は複数値を持つ文字列型のため、[ForAnyValue または ForAllValues 複数値文字列演算子](#)を使用する必要があります。また、組織のメンバーアカウントのタグを参照している場合でも`account`、条件キーのプレフィックスは `account:AccountResourceOrgTags` であることに注意してください。

```
"Condition": {  
  "ForAnyValue:StringLike": {  
    "account:AccountResourceOrgTags/project": [  
      "blue",  
      "red"  
    ]  
  }  
}
```

Note

タグは、組織内のアカウントにのみアタッチすることができます。スタンドアロンにタグをアタッチすることはできません AWS アカウント。

を設定する AWS アカウント

これらの手順は、サインアップ for AWS (アドバンスド) AWS を使用して にサインアップ AWS アカウントした場合、またはアカウントの高度な機能をアクティブ化した場合に、 を設定する方法を示しています。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

このセクションでは、 の管理方法について説明します AWS アカウント。

Note

AWS アカウント が Amazon Web Services India Private Limited (AWS インド) を使用してインドで作成された場合は、追加の考慮事項があります。詳細については、「[インドでのアカウントの管理](#)」を参照してください。

トピック

- [AWS アカウント エイリアスを作成する](#)
- [アカウント AWS リージョン で を有効または無効にする](#)
- [の請求を更新する AWS アカウント](#)
- [ルートユーザーの E メールアドレスと の更新](#)
- [ルートユーザーのパスワードの更新](#)
- [AWS アカウント 名前を更新する](#)
- [の代替連絡先を更新する AWS アカウント](#)
- [のプライマリ連絡先を更新する AWS アカウント](#)
- [AWS アカウント 識別子の表示](#)

AWS アカウント エイリアスを作成する

これらの手順は、サインアップ for AWS (アドバンスド) AWS アカウント AWS を使用して にサインアップした場合、またはアカウントの高度な機能をアクティブ化した場合にエイリアスを作成する方法を示しています。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

IAM ユーザーの URL に AWS アカウント ID の代わりに会社名 (またはeasy-to-remember識別子) を含める場合は、アカウントエイリアスを作成できます。

アカウントエイリアスを作成または更新する方法については、IAM ユーザーガイドの[AWS アカウント「ID のエイリアスの使用」](#)を参照してください。

アカウント AWS リージョン で を有効または無効にする

この情報は、サインアップ for AWS (アドバンスト) AWS の使用にサインアップ AWS アカウントした場合、またはアカウントの高度な機能をアクティブ化した場合の AWS リージョン での の有効化または無効化に関するものです。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

AWS リージョン は、 に複数のアベイラビリティゾーン AWS がある世界の物理的な場所です。アベイラビリティゾーンは 1 つ以上の個別の AWS データセンターで構成され、それぞれが冗長な電源、ネットワーク、および接続を備え、別々の施設に収容されています。つまり、それぞれ AWS リージョン が物理的に分離され、他のリージョンから独立しています。リージョンでは耐障害性や安定性が提供され、レイテンシーを低減することもできます。エンドユーザー AWS リージョン に近い でワークロードを実行すると、パフォーマンスが向上し、レイテンシーが短縮されます。利用可能なリージョンと今後予定されているリージョンのマップについては、[リージョンとアベイラビリティゾーン](#)を参照してください。ワークロードの AWS リージョン と回復性アーキテクチャの詳細については、[AWS マルチリージョンの基本](#)を参照してください。

AWS リージョン は、アカウントの可用性の 2 つのカテゴリに分類されます。

- デフォルトリージョン – 2019 年 3 月 20 日より前に設立されたリージョンは、デフォルトで有効になっています。アカウントがアクティブ化された直後に、これらのデフォルトリージョンでリソースを作成および管理できます。デフォルトのリージョンを有効または無効にすることはできません。
- オプトインリージョン – 2019 年 3 月 20 日以降に設立されたリージョンはデフォルトで無効になっており、オプトインリージョンと呼ばれます。無効なオプトインリージョンはコンソールのナビゲーションバーに表示されず、有効にするまでこれらのリージョンを使用してワークロードを作成することはできません。これらのオプトインリージョンを使用するには、まず で有効にする必要があります AWS アカウント。オプトインリージョンを有効にすると、ナビゲーションバーでそのリージョンを選択し、そこでリソースを作成および管理できます。スタンドアロンアカウントのオプトインリージョンを有効にするには、「」を参照[スタンドアロンアカウントのリージョンの有効化または無効化](#)し、メンバーアカウントのオプトインリージョンを有効にするには、「」を参照してください[組織内のリージョンの有効化または無効化](#)。

にサインアップすると AWS アカウント、 は連絡先住所の国に基づいてオプトインリージョン AWS を推奨します。AWS オプトインリージョンがある国の顧客には、その国のオプトインリージョンを

有効にするための推奨事項が連絡先情報ページに表示されます。インド、オーストラリア、カナダなど、オプトインリージョンとデフォルトリージョンの両方を持つ国のお客様には、オプトインリージョンがデフォルトリージョンよりも近い場合、オプトインリージョンを選択することをお勧めします。アカウントがアクティブ化されたら、アカウントの他のオプトインリージョンを有効にするか、サインアップ中に有効にしたオプトインリージョンを無効にするかを選択できます。

を作成すると AWS アカウント、IAM データおよび認証情報がすべてのデフォルトリージョンで動作するように自動的に設定されます。これにより、ルートユーザーおよび IAM アイデンティティは、既存の認証情報を使用してこれらのリージョン AWS のサービスにアクセスするための適切なアクセス許可を持つことができます。AWS オプトインリージョンはデフォルトで無効になり、IAM データおよび認証情報はこれらのリージョンで最初で使用できなくなり、そのリージョン AWS のサービスへのアクセスができなくなります。オプトインリージョンを有効にすると、AWS は IAM データおよび認証情報をそのリージョンに伝播します。伝播が完了し、オプトインリージョンが有効になると、ルートユーザーと IAM ID は、デフォルトリージョンで使用するのと同じ IAM 認証情報を使用して AWS、新しく有効になったオプトインリージョンのサービスにアクセスできます。

オプトインリージョンを無効にすると、IAM 認証情報が非アクティブ化され、そのオプトインリージョンのリソースへの IAM アクセスが失われます。オプトインリージョンを無効にしても、そのリージョンのリソースは削除されず、無効にしたオプトインリージョンのリソース (ある場合) の料金は引き続き標準レートで発生します。

Important

リージョンを無効にすると、リージョン内のリソースへの IAM アクセスが無効になります。これにより、問題のリソースは削除されず、引き続き料金が発生します。リージョンを無効にする前に、残りのリソースを削除します。

AWS はリージョンを[パーティションにグループ化します](#)。各リージョンは 1 つのパーティションに厳密に属し、各パーティションには 1 つ以上のリージョンがあります。パーティションには AWS Identity and Access Management (IAM) の独立したインスタンスがあり、異なるパーティションのリージョン間のハード境界を提供します。AWS 商用リージョンはawsパーティションにあり、中国のリージョンはaws-cnパーティションにあり、AWS GovCloud (US) リージョンはaws-us-govパーティションにあります。を作成したパーティションに応じて AWS アカウント、そのパーティション AWS リージョン 内で 使用できます。

- aws パーティションのアカウントは、要件を満たす場所で AWS リソースを起動できるように、商用パーティション内の複数のリージョンへのアクセスを提供します。例えば、ヨーロッパの顧客に

近づけるため、または法的要件を満たすために、ヨーロッパで Amazon EC2 インスタンスを起動したい場合があります。

- aws-us-gov パーティションのアカウントでは、AWS GovCloud (米国西部) リージョンと AWS GovCloud (米国東部) リージョンにアクセスできます。詳細については、「[AWS GovCloud \(US\)](#)」を参照してください。
- aws-cn パーティションを使用すると、北京および寧夏リージョンにのみアクセスできます。詳細については「[Amazon Web Services in China](#)」(中国でのAmazon ウェブ サービス) を参照してください。

トピック

- [リージョンの可用性リファレンス](#)
- [リージョンを有効化または無効化する前の考慮事項](#)
- [処理時間とリクエスト制限](#)
- [スタンドアロンアカウントのリージョンの有効化または無効化](#)
- [組織内のリージョンの有効化または無効化](#)

リージョンの可用性リファレンス

次の表は、可用性タイプ AWS リージョン 別にリストされています。デフォルトのリージョンは自動的に有効になり、無効にすることはできませんが、オプトインリージョンを使用するには手動で有効にする必要があります。

Opt-in Regions

次のリージョンはオプトインリージョンであり、使用する前に有効にする必要があります。

名前	コード	ステータス
アフリカ (ケープタウン)	af-south-1	GA
アジアパシフィック (香港)	ap-east-1	GA
アジアパシフィック (台北)	ap-east-2	GA
アジアパシフィック (ハイデラバード)	ap-south-2	GA

名前	コード	ステータス
アジアパシフィック (ジャカルタ)	ap-southeast-3	GA
アジアパシフィック (メルボルン)	ap-southeast-4	GA
アジアパシフィック (マレーシア)	ap-southeast-5	GA
アジアパシフィック (ニュージーランド)	ap-southeast-6	GA
アジアパシフィック (タイ)	ap-southeast-7	GA
カナダ西部 (カルガリー)	ca-west-1	GA
欧州 (チューリッヒ)	eu-central-2	GA
欧州 (ミラノ)	eu-south-1	GA
欧州 (スペイン)	eu-south-2	GA
イスラエル (テルアビブ)	il-central-1	GA
中東 (アラブ首長国連邦)	me-central-1	GA
中東 (バーレーン)	me-south-1	GA
メキシコ (中部)	mx-central-1	GA

Default Regions

次のリージョンは、デフォルトで有効になっていて、無効にすることはできません。

名前	コード
アジアパシフィック (東京)	ap-northeast-1
アジアパシフィック (ソウル)	ap-northeast-2
アジアパシフィック (大阪)	ap-northeast-3

名前	コード
アジアパシフィック (ムンバイ)	ap-south-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
カナダ (中部)	ca-central-1
欧州 (フランクフルト)	eu-central-1
欧州 (ストックホルム)	eu-north-1
欧州 (アイルランド)	eu-west-1
欧州 (ロンドン)	eu-west-2
欧州 (パリ)	eu-west-3
南米 (サンパウロ)	sa-east-1
米国東部 (バージニア北部)	us-east-1
米国東部 (オハイオ)	us-east-2
米国西部 (北カリフォルニア)	us-west-1
米国西部 (オレゴン)	us-west-2

リージョン名と対応するコードのリストについては、「AWS 全般のリファレンスガイド」の「[リージョンエンドポイント](#)」を参照してください。各リージョンでサポートされている AWS サービスのリスト (エンドポイントなし) については、[AWS 「リージョンサービスリスト」](#)を参照してください。

 Important

AWS では、レイテンシーを減らすために、グローバルエンドポイントの代わりに Regional AWS Security Token Service (AWS STS) エンドポイントを使用することをお勧めします。リージョン AWS STS エンドポイントからのセッショントークンは、すべての AWS

リージョンで有効です。リージョン AWS STS エンドポイントを使用する場合は、変更を加える必要はありません。ただし、グローバル AWS STS エンドポイント (<https://sts.amazonaws.com>) からのセッショントークンは、AWS リージョン 有効にした またはデフォルトで有効になっている のみ有効です。アカウントの新しいリージョンを有効にする場合は、リージョン AWS STS エンドポイントからセッショントークンを使用するか、グローバル AWS STS エンドポイントをアクティブ化して、すべての で有効なセッショントークンを発行できます AWS リージョン。すべてのリージョンで有効なセッショントークンは大きくなります。セッショントークンを保存すると、これらの大きなトークンがシステムに影響する可能性があります。AWS STS エンドポイントが AWS リージョンと連携する方法の詳細については、[AWS 「リージョン AWS STS での の管理」](#) を参照してください。

リージョンを有効化または無効化する前の考慮事項

リージョンを有効化または無効化する前に、以下の点について考慮することが重要です。

- リージョン最適化のステータスに関係なく、クロスリージョン推論ジオグラフィですべての送信先リージョンを使用できます。Amazon Bedrock ([「クロスリージョン推論によるスループットの向上」](#) を参照) や Amazon Q Developer ([「Amazon Q Developer でのクロスリージョン処理」](#) を参照) などの特定の AWS 生成 AI サービスは、クロスリージョン推論を使用します。これらのサービスを使用すると、選択した地域内で、リソースと IAM データに対して有効にしていないリージョンを含む最適な AWS リージョンが自動的に選択されます。これにより、利用可能なコンピューティングとモデルの可用性を最大化することで、カスタマーエクスペリエンスが向上します。
- IAM アクセス許可を使用してリージョンへのアクセスを制御 – AWS Identity and Access Management (IAM) には、リージョンを有効化、無効化、取得、一覧表示できるユーザーを制御できる 4 つのアクセス許可が含まれています。詳細については、「IAM ユーザーガイド」の「[AWS: AWS リージョンの有効化と無効化を許可する](#)」を参照してください。`aws:RequestedRegion` 条件キーを使用して、AWS のサービス での へのアクセスを制御することもできます AWS リージョン。
- リージョンの有効化/無効化は無料 – リージョンを有効または無効にしても料金はかかりません。新しいリージョンで作成したリソースに対してのみ課金されます。
- Amazon EventBridge 統合 – EventBridge でリージョンオプトステータス更新通知をサブスクライブできます。ステータスに変更されるたびに EventBridge 通知が作成され、お客様はワークフローを自動化できます。
- 詳細なリージョンオプトステータス – オプトインリージョンの有効化/無効化は非同期的に行われるため、リージョンオプトリクエストには次の 4 つのステータスがあります。

- ENABLING
- DISABLING
- ENABLED
- DISABLED

オプトインまたはオプトアウトは、そのステータスが ENABLING または DISABLING である場合はキャンセルできません。それ以外の場合は、`ConflictException` がスローされます。完了した (有効/無効) リージョンオプトリクエストは、基盤となる主要な AWS サービスのプロビジョニングによって異なります。ステータスが `ENABLED` であってもすぐには使用できない AWS サービスもあります `ENABLED`。

処理時間とリクエスト制限

リージョンを有効または無効にする場合は、次のタイミングとリクエストの制限に注意してください。

- リージョンの有効化は、場合によっては数分から数時間かかる - リージョンを有効にすると、AWS はリージョンへの IAM リソースの配信など、そのリージョンでアカウントを準備するためのアクションを実行します。このプロセスは、ほとんどのアカウントでは数分で完了しますが、場合によっては数時間かかることもあります。このプロセスが完了するまでそのリージョンを使用することはできません。
- リージョンの無効化は必ずしも即時に表示されるわけではない - リージョンを無効にした後もサービスやコンソールが一時的に表示される場合があります。リージョンを無効にすると、有効になるまでに数分から数時間かかる場合があります。
- 1 つのアカウントが同時に持つことができる進行中のリージョンオプトリクエストは最大 6 件 - 1 つのリクエストは、1 つのアカウントに対する特定の 1 つのリージョンの有効化または無効化のいずれかに相当します。
- 組織は、AWS 組織全体で一度に 50 件のリージョンオプトリクエストを開くことができます。管理アカウントは、組織の完了保留中のオープンリクエストをいつでも 50 件持つことができます。1 つのリクエストは、1 つのアカウントに対する特定の 1 つのリージョンの有効化または無効化のいずれかに相当します。

スタンドアロンアカウントのリージョンの有効化または無効化

AWS アカウント がアクセスできるリージョンを更新するには、次の手順を実行します。AWS マネジメントコンソール 次の手順は、常にスタンドアロンコンテキストでのみ機能します。を使用し

て AWS マネジメントコンソール、オペレーションの呼び出しに使用したアカウントで使用可能なリージョンのみを表示または更新できます。

AWS マネジメントコンソール

スタンドアロンのリージョンを有効または無効にするには AWS アカウント

最小アクセス許可

以下の手順の手順を実行するには、IAM ユーザーまたはロールに次のアクセス許可が必要です。

- `account:ListRegions` (のリスト AWS リージョン と、現在有効か無効かを表示する必要があります)。
- `account:EnableRegion`
- `account:DisableRegion`

1. に、最小限のアクセス許可を持つ IAM ユーザーまたはロール [AWS マネジメントコンソール](#) AWS アカウントのルートユーザー としてサインインします。
2. ウィンドウの右上にあるアカウント名を選択し、[アカウント] を選択します。
3. [\[アカウント\] ページ](#) で、[AWS リージョン] セクションまでスクロールダウンします。
4. 有効または無効にするリージョンを選択し、目的のアクションの [有効化] または [無効化] を選択します。確認のプロンプトが表示されます。
5. [有効化] オプションを選択した場合は、表示されたテキストを確認してから、[リージョンを有効にする] を選択します。

[無効化] オプションを選択した場合は、表示されたテキストを確認し、確認のために **disable** と入力して、[リージョンを無効にする] を選択します。

オプトインリージョンを有効にすると、リージョンナビゲーションバーからそのリージョンを選択できます。リージョンを選択する手順については、「[AWS マネジメントコンソールのナビゲーションバーからリージョンを選択する](#)」を参照してください。アカウントのリージョン固有のコンソール設定については、「[AWS マネジメントコンソールのデフォルトのリージョンの設定](#)」を参照してください。

AWS CLI & SDKs

リージョンオプトステータスの有効化、無効化、読み取り、一覧表示を行うには、次の AWS CLI コマンドまたは AWS SDK と同等のオペレーションを使用します。

- EnableRegion
- DisableRegion
- GetRegionOptStatus
- ListRegions

最小アクセス許可

次の手順を実行するには、そのオペレーションにマッピングするためのアクセス許可が必要です。

- account:EnableRegion
- account:DisableRegion
- account:GetRegionOptStatus
- account:ListRegions

これらの個別のアクセス許可を使用すると、一部のユーザーにリージョンオプト情報の読み取りのみを許可し、他のユーザーには読み取りと書き込みを許可するということもできます。

次の例では、組織内の指定されたメンバーアカウントのリージョンを有効にします。使用される認証情報は、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのいずれかから取得する必要があります。

同じコマンド (enable-region は disable-region に置き換える) を使用してリージョンを無効にすることもできます。

```
aws account enable-region --region-name af-south-1
```

このコマンドは成功時に出力を生成しません。

このオペレーションは非同期です。次のコマンドを使用すると、リクエストの最新ステータスを確認できます。

```
aws account get-region-opt-status --region-name af-south-1
{
  "RegionName": "af-south-1",
  "RegionOptStatus": "ENABLING"
}
```

組織内のリージョンの有効化または無効化

のメンバーアカウントの有効なリージョンを更新するには AWS Organizations、次の手順を実行します。

Note

AWS Organizations 管理ポリシー `AWSOrganizationsReadOnlyAccess` または `AWSOrganizationsFullAccess` が更新され、AWS Organizations コンソールからアカウントデータにアクセスできるように、AWS アカウント管理 APIs へのアクセス許可が付与されます。更新された管理ポリシーを表示するには、[「Organizations AWS 管理ポリシーの更新」](#)を参照してください。

Note

組織の管理アカウントまたは委任管理者アカウントからメンバーアカウントに対してこれらの操作を実行する前に、以下を行う必要があります。

- メンバーアカウントの設定を管理するために、組織内のすべての機能を有効にします。これにより、管理者がメンバーアカウントを制御できるようになります。これは、組織を作成すると、デフォルトで設定されます。組織が一括決済のみに設定されていて、すべての機能を有効にする場合は、[「組織内のすべての機能の有効化」](#)を参照してください。
- AWS アカウント管理サービスの信頼されたアクセスを有効にします。これを設定するには、[「AWS アカウント管理の信頼されたアクセスを有効にする」](#)を参照してください。

AWS マネジメントコンソール

組織内のリージョンを有効または無効にする手順

1. 組織の管理アカウントの認証情報を使用して AWS Organizations コンソールにサインインします。
2. [AWS アカウント] ページで、更新するアカウントを選択します。
3. [アカウント設定] タブを選択します。
4. [リージョン] で、有効または無効にするリージョンを選択します。
5. [アクション] を選択し、[有効化] または [無効化] オプションのいずれかを選択します。
6. [有効化] オプションを選択した場合は、表示されたテキストを確認してから、[リージョンを有効にする] を選択します。
7. [無効化] オプションを選択した場合は、表示されたテキストを確認し、確認のために `disable` と入力して、[リージョンを無効にする] を選択します。

AWS CLI & SDKs

組織メンバーアカウントのリージョンオプトステータスを有効化、無効化、読み取り、一覧表示するには、次の AWS CLI コマンドまたは AWS SDK と同等のオペレーションを使用します。

- `EnableRegion`
- `DisableRegion`
- `GetRegionOptStatus`
- `ListRegions`

最小アクセス許可

次の手順を実行するには、そのオペレーションにマッピングするためのアクセス許可が必要です。

- `account:EnableRegion`
- `account:DisableRegion`
- `account:GetRegionOptStatus`
- `account:ListRegions`

これらの個別のアクセス許可を使用すると、一部のユーザーにリージョンオプト情報の読み取りのみを許可し、他のユーザーには読み取りと書き込みを許可することもできます。

次の例では、組織内の指定されたメンバーアカウントのリージョンを有効にします。使用される認証情報は、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのいずれかから取得する必要があります。

同じコマンド (enable-region は disable-region に置き換える) を使用してリージョンを無効にすることもできます。

```
aws account enable-region --account-id 123456789012 --region-name af-south-1
```

このコマンドは成功時に出力を生成しません。

Note

組織が同時に持つことができるリージョンリクエストは、最大 20 個のみです。これを超えると、TooManyRequestsException が発生します。

このオペレーションは非同期です。次のコマンドを使用すると、リクエストの最新ステータスを確認できます。

```
aws account get-region-opt-status --account-id 123456789012 --region-name af-south-1
{
  "RegionName": "af-south-1",
  "RegionOptStatus": "ENABLING"
}
```

の請求を更新する AWS アカウント

これらの手順は、サインアップ for AWS (アドバンスド) AWS の使用にサインアップ AWS アカウントした場合、またはアカウントの高度な機能をアクティブ化した場合に、の請求を更新する方法を示しています。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

AWS Billing および コスト管理コンソールを使用して、すべての AWS アカウント 請求設定を更新できます。アカウントの請求関連の設定を更新する方法については、「[AWS Billing and Cost Management ユーザーガイド](#)」を参照してください。

ルートユーザーの E メールアドレスと の更新

これらの手順は、サインアップ for AWS (アドバンスド) AWS の使用にサインアップした場合、またはアカウントの高度な機能をアクティブ化した場合に、ルートユーザーの E メールアドレスを更新する方法を示しています。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

AWS アカウントのルートユーザーの E メールアドレスと を更新する必要があるビジネス上の理由はさまざまです。例えば、セキュリティと管理のレジリエンスなどです。このトピックでは、スタンドアロンアカウントとメンバーアカウントの両方のルートユーザーの E メールアドレスと を更新するプロセスについて説明します。

Note

への変更は、どこでも伝播されるまでに最大 4 時間かかる AWS アカウント 場合があります。

ルートユーザーの E メールとは、アカウントがスタンドアロンであるか、組織の一部であるかに応じて、異なる方法で更新できます。

- スタンドアロンアカウント AWS アカウント または管理アカウント – 組織に関連付けられ AWS アカウント ていない、または組織の管理アカウントの場合は、AWS マネジメントコンソールを使用してルートユーザー E メール メールを更新できます。これを行う方法については、「[スタンドアロンアカウント AWS アカウント または管理アカウントのルートユーザー E メール メールを更新する](#)」を参照してください。
- AWS アカウント 組織内 – AWS 組織の一部であるメンバーアカウントの場合、管理アカウントまたは委任管理者アカウントのユーザーは、AWS Organizations コンソールから、または CLI と SDKs を介してプログラムで、メンバーアカウントの Amazon AWS メールを一元的に更新できます。これを行う方法については、「[組織 AWS アカウント 内の任意の のルートユーザー E メール メールを更新する](#)」を参照してください。

トピック

- [スタンドアロンアカウント AWS アカウント または管理アカウントのルートユーザー E メール メールを更新する](#)
- [組織 AWS アカウント 内の任意の のルートユーザー E メールを更新する](#)

スタンドアロンアカウント AWS アカウント または管理アカウントのルートユーザー E メール メールを更新する

スタンドアロンアカウント AWS アカウント または管理アカウントのルートユーザーの E メールアドレスを編集する、次の手順を実行します。

AWS マネジメントコンソール

Note

としてサインインする必要があります。そのため AWS アカウントのルートユーザー、追加の IAM アクセス許可は必要ありません。IAM ユーザーまたはロールとしてこれらの手順を実行することはできません。

1. AWS アカウントの E メールアドレスとパスワードを使用して、[AWS マネジメントコンソール](#)として にサインインします AWS アカウントのルートユーザー。
2. コンソールの右上隅のアカウント名またはアカウント番号を選択してから [Account] (アカウント) を選択します。
3. [\[アカウント\] ページ](#)で、[アカウントの詳細] の横にある [アクション] を選択し、[E メールアドレスとパスワードの更新] を選択します。
4. [アカウントの詳細] ページで、[E メールアドレス] の横にある [編集] を選択します。
5. [E メールアドレスの編集] ページで、[新しい E メールアドレス] と [新しい E メールアドレスの確認] のフィールドに入力し、現在の [パスワード] を確認します。次に [保存し続行] を選択します。no-reply@verify.signin.aws から新しい E メールアドレスに検証コード送信されます。
6. [アカウント Eメールの編集] ページの [検証コード] で、E メールから受け取ったコードを入力し、[更新の確認] を選択します。

Note

検証コードが到着するまでに最大 5 分かかる場合があります。受信箱で E メールが見つからない場合は、スパムフォルダや迷惑メールフォルダを確認してください。

AWS CLI & SDKs

このタスクは、AWS CLI またはいずれかの AWS SDKs からの API オペレーションではサポートされていません。このタスクは、 を使用してのみ実行できます AWS マネジメントコンソール。

組織 AWS アカウント 内の任意の のルートユーザー E メールを更新する

AWS Organizations コンソールを使用して組織内のメンバーアカウントのルートユーザーの E メールアドレス、次の手順を実行します。

Note

メンバーアカウントのルートユーザーの E メールアドレスと を更新する前に、このオペレーションの影響を理解しておくことをお勧めします。詳細については、「AWS Organizations ユーザーガイド」の「[AWS Organizationsでメンバーアカウントのルートユーザーの E メールアドレスと の更新](#)」を参照してください。

ルートユーザーとしてサインインした後、 のアカウントページから直接、メンバーアカウントのルートユーザーの E メールアドレスを更新することもできます。AWS マネジメントコンソール ステップバイステップの手順については、「[スタンドアロンアカウント AWS アカウント または管理アカウントのルートユーザー E メール メールを更新する](#)」の手順に従います。

Note

AWS 設定でプロジェクトとして作成したメンバーアカウントであるプロジェクトアカウントのルートユーザーの E メールアドレスを更新することはできません。AWS Builder ID は、ルートユーザーの E メールアドレスではなく各プロジェクトアカウントを所有しており、高度な機能をアクティブ化しても変更されません。詳細については、「[高度な機能をアクティブ化した後のプロジェクトアカウント](#)」を参照してください。

AWS Management Console

 注意事項

- 組織内の管理アカウントまたは委任管理者アカウントからメンバーアカウントに対してこの手順を実行するには、[アカウント管理サービス用の信頼されたアクセスを有効](#)にする必要があります。
- この手順を使用して、オペレーションの呼び出しに使用している組織とは異なる組織のアカウントにアクセスすることはできません。

AWS Organizations コンソールを使用してメンバーアカウントのルートユーザーの E メールアドレスを更新するには

1. [AWS Organizations コンソール](#) にサインインします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、ルートユーザーとしてサインインする ([推奨されません](#)) 必要があります。
2. [AWS アカウント] ページで、ルートユーザーの E メールアドレスと を更新するメンバーアカウントを選択します。
3. [アカウントの詳細] セクションで、[アクション] ボタンを選択し、[E メールアドレスの更新] を選択します。
4. [E メール] で、ルートユーザーの新しい E メールアドレスを入力し、[保存] を選択します。これにより、新しい E メールアドレスにワンタイムパスワード (OTP) が送信されます。

 Note

コードを待っている間に Organizations コンソールでこのページを閉じる必要がある場合は、コードの送信から 24 時間以内に OTP プロセスを返して終了できます。これを行うには、[アカウントの詳細] ページで [アクション] ボタンを選択し、[E メール更新の完了] を選択します。

5. [検証コード] で、前のステップで新しい E メールアドレスに送信されたコードを入力し、[確認] を選択します。これにより、アカウントのルートユーザーに更新がコミットされます。

AWS CLI & SDKs

ルートユーザーの E メールアドレス (プライマリ E メールアドレスとも呼ばれます) を取得または更新するには、次の AWS CLI コマンドまたは AWS SDK と同等のオペレーションを使用します。

- [GetPrimaryEmail](#)
- [StartPrimaryEmailUpdate](#)
- [AcceptPrimaryEmailUpdate](#)

注意事項

- 組織内の管理アカウントまたは委任管理者アカウントからメンバーアカウントに対してこれらの操作を実行するには、[アカウント管理サービス用の信頼されたアクセスを有効](#)にする必要があります。
- オペレーションの呼び出しに使用している組織とは異なる組織のアカウントにアクセスすることはできません。
- プロジェクトアカウントの場合、必要なアクセス許可があっても、StartPrimaryEmailUpdate とは AccessDeniedException エラーで AcceptPrimaryEmailUpdate 失敗します。

最小アクセス許可

各操作については、その操作に対応するアクセス許可が必要です。

- `account:GetPrimaryEmail`
- `account:StartPrimaryEmailUpdate`
- `account:AcceptPrimaryEmailUpdate`

これらのアクセス許可を個別に使用すると、一部のユーザーにルートユーザーの E メールアドレスと の情報の読み取りのみを許可し、他のユーザーには読み取りと書き込みの両方の許可を付与するといったことができるようになります。

ルートユーザーの E メールアドレスプロセスを完了するには、プライマリ E メール APIs を次の例に示す順序で一緒に使用する必要があります。

Example `GetPrimaryEmail`

次の例では、組織内の指定されたメンバーアカウントからルートユーザーの E メールアドレスとを取得します。使用される認証情報は、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのいずれかから取得する必要があります。

```
$ aws account get-primary-email --account-id 123456789012
```

Example `StartPrimaryEmailUpdate`

次の例では、ルートユーザーの E メールアドレスと の更新プロセスを開始し、新しい E メールアドレスを識別し、組織内の指定されたメンバーアカウントの新しい E メールアドレスにワンタイムパスワード (OTP) を送信します。使用される認証情報は、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのいずれかから取得する必要があります。

```
$ aws account start-primary-email-update --account-id 123456789012 --primary-email john@examplecorp.com
```

Example `AcceptPrimaryEmailUpdate`

次の例では、OTP コードを受け入れ、新しい E メールアドレスを組織内の指定されたメンバーアカウントに設定します。使用される認証情報は、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのいずれかから取得する必要があります。

```
$ aws account accept-primary-email-update --account-id 123456789012 --otp 12345678 --primary-email john@examplecorp.com
```

ルートユーザーのパスワードの更新

これらの手順は、サインアップ for AWS (アドバンスド) AWS の使用にサインアップした場合、またはアカウントの高度な機能をアクティブ化した場合に、ルートユーザーのパスワードを更新する方法を示しています。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

AWS アカウントルートユーザーのパスワードを編集するには、以下の手順を実行します。

AWS マネジメントコンソール

ルートユーザーパスワードを編成するには

Note

としてサインインする必要があります。そのため AWS アカウントのルートユーザー、追加の IAM アクセス許可は必要ありません。IAM ユーザーまたはロールとしてこれらの手順を実行することはできません。

1. AWS アカウントの E メールアドレスとパスワードを使用して、[AWS マネジメントコンソール](#)としてサインインします AWS アカウントのルートユーザー。
2. コンソールの右上隅のアカウント名またはアカウント番号を選択してから [Account] (アカウント) を選択します。
3. [\[アカウント\] ページ](#)で、[アカウントの詳細] の横にある [アクション] を選択し、[E メールアドレスとパスワードの更新] を選択します。
4. [アカウントの詳細] ページで、[パスワード] の横にある [編集] を選択します。
5. [パスワードの編集] ページで、[現在のパスワード]、[新しいパスワード]、[新しいパスワードの確認] の各フィールドに入力します。その後、[パスワードの更新] を選択します。ルートユーザーのパスワードの設定に関するベストプラクティスを含む追加のガイダンスについては、「IAM ユーザーガイド」の「[AWS アカウントのルートユーザーのパスワードを変更する](#)」を参照してください。

AWS CLI & SDKs

このタスクは、AWS CLI またはいずれかの AWS SDKs からの API オペレーションではサポートされていません。このタスクは、を使用してのみ実行できます AWS マネジメントコンソール。

AWS アカウント 名前を更新する

これらの手順は、サインアップ for AWS (アドバンスド) AWS の使用にサインアップした場合、またはアカウントの高度な機能をアクティブ化した場合に、AWS アカウント 名前を更新する方法を示しています。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

複数の を管理する場合は AWS アカウント、ビジネスユニットやアプリケーションに合わせた明確な命名規則を使用して、識別と整理を行います。再編成、合併、買収、命名規則の更新中に、一貫した識別および管理基準を維持するためにアカウント名を変更する必要がある場合があります。

アカウントの名前は、請求書や請求情報、コスト管理ダッシュボード、コンソールなどの AWS Organizations コンソールなど、複数の場所に表示されます。アカウント名を付ける際に標準的な方法を使用することで、アカウント名を認識しやすいものにするをお勧めします。会社のアカウントの場合は、organization-purpose-environment (例えば、sales-catalog-prod) のような命名基準を使用することを検討してください。プライバシーとセキュリティ上の理由から、個人を特定できる情報 (PII) を反映するアカウント名は使用しないでください。

- スタンドアロンアカウント AWS アカウント または管理アカウント – 組織に関連付けられ AWS アカウント ていないアカウント、または組織の管理アカウントの場合は、AWS マネジメントコンソール、AWS CLI SDKs を使用してアカウント名を更新できます。これを行う方法については、「[スタンドアロンアカウント AWS アカウント または管理アカウントのアカウント名を更新する](#)」を参照してください。
- AWS アカウント 組織内 – の一部であるメンバーアカウントの場合 AWS Organizations、管理アカウントまたは委任管理者アカウントのユーザーは、AWS Organizations コンソールから、またはプログラムで AWS CLI および SDKs を介して、組織内の任意のメンバーアカウントのアカウント名を一元的に更新できます。これを行う方法については、「[組織 AWS アカウント 内の のアカウント名を更新する](#)」を参照してください。

Note

への変更は、どこでも伝播されるまでに最大 4 時間かかる AWS アカウント 場合があります。

トピック

- [スタンドアロンアカウント AWS アカウント または管理アカウントのアカウント名を更新する](#)
- [組織 AWS アカウント 内の のアカウント名を更新する](#)

スタンドアロンアカウント AWS アカウント または管理アカウントのアカウント名を更新する

スタンドアロンアカウント AWS アカウント または管理アカウントのアカウント名を変更するには、次の手順を実行します。

AWS マネジメントコンソール

最小アクセス許可

ルートユーザー、IAM ユーザー、または IAM ロールを使用して、アカウント名を更新できます。ルートユーザーを使用している場合、アカウント名を更新するために追加の IAM アクセス許可は必要ありません。IAM ユーザーまたは IAM ロールを使用する場合は、少なくとも次の IAM アクセス許可が必要です。

- `account:GetAccountInformation`
- `account:PutAccountName`

スタンドアロンアカウントまたは管理アカウントのアカウント名を更新するには

1. AWS アカウントの E メールアドレスとパスワードを使用して、[AWS マネジメントコンソール](#)として にサインインします AWS アカウントのルートユーザー。
2. コンソールの右上隅のアカウント名またはアカウント番号を選択してから [Account] (アカウント) を選択します。
3. [\[アカウント\] ページ](#)で、[アカウントの詳細] の横にある [アクション] を選択し、[アカウント名の更新] を選択します。
4. [名前] で、更新する新しいアカウント名を入力し、[保存] を選択します。

AWS CLI & SDKs

最小アクセス許可

ルートユーザー、IAM ユーザー、または IAM ロールを使用して、アカウント名を更新できます。次の手順を実行するには、IAM ユーザーまたは IAM ロールに少なくとも以下の IAM アクセス許可が必要です。

- `account:GetAccountInformation`

- `account:PutAccountName`

スタンドアロンアカウントまたは管理アカウントのアカウント名を更新するには

以下のいずれかのオペレーションを使用することもできます。

- AWS CLI: [put-account-name](#)

```
$ C:\> aws account put-account-name \  
      --account-name "New-Account-Name"
```

- AWS SDKs: [PutAccountName](#)

組織 AWS アカウント 内の のアカウント名を更新する

では、すべての機能モード AWS Organizations を使用して、管理アカウントと委任管理者アカウントの両方で、承認された IAM ユーザーまたは IAM ロールがアカウント名を一元管理できます。

組織内のメンバーアカウントのアカウント名を変更するには、次の手順を実行します。

要件

AWS Organizations コンソールでアカウント名を更新するには、いくつかの事前設定を行う必要があります。

- メンバーアカウントで設定を管理するには、所属する組織によってすべての機能が有効にされる必要があります。これにより、管理者がメンバーアカウントを制御できるようになります。これは、組織を作成すると、デフォルトで設定されます。組織が一括決済のみに設定されていて、すべての機能を有効にする場合は、「[組織内のすべての機能の有効化](#)」を参照してください。
- AWS アカウント管理サービスの信頼されたアクセスを有効にする必要があります。これを設定するには、「[AWS アカウント管理の信頼されたアクセスを有効にする](#)」を参照してください。

AWS マネジメントコンソール

最小アクセス許可

メンバーアカウントのアカウント名を更新するには、IAM ユーザーまたは IAM ロールに次のアクセス許可が必要です。

- `organizations:DescribeOrganization` (コンソールのみ)
- `account:PutAccountName`

メンバーアカウントのアカウント名を更新するには

1. Organizations コンソール (<https://console.aws.amazon.com/organizations/>) を開きます。
2. メインナビゲーションペインで、[AWS アカウント] を選択します。
3. [AWS アカウント] ページで、更新するメンバーアカウントを選択し、[アクション] ドロップダウンメニューを選択し、[アカウント名の更新] を選択します。
4. [名前] で更新された名前を入力し、[保存] を選択します。

AWS CLI & SDKs

最小アクセス許可

メンバーアカウントのアカウント名を更新するには、IAM ユーザーまたは IAM ロールに次のアクセス許可が必要です。

- `organizations:DescribeOrganization` (コンソールのみ)
- `account:PutAccountName`

メンバーアカウントのアカウント名を更新するには

以下のいずれかのオペレーションを使用することもできます。

- AWS CLI: [put-account-name](#)

```
$ C:\> aws account put-account-name \  
      --account-id 111111111111 \  
      --account-name "New-Account-Name"
```

- AWS SDKs: [PutAccountName](#)

の代替連絡先を更新する AWS アカウント

これらの手順は、サインアップ for AWS (アドバンスド) AWS の使用にサインアップ AWS アカウントした場合、またはアカウントの高度な機能をアクティブ化した場合に、の代替連絡先を更新する方法を示しています。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

代替連絡先を使用すると AWS、アカウントに関連付けられた最大 3 つの代替連絡先に連絡できます。代替連絡先は、特定の人物である必要はありません。請求、運用、およびセキュリティ関連の問題を管理するチームがある場合は、代わりに E メール配布リストを追加できます。これらは、アカウントの[ルートユーザー](#)に関連付けられている E メールアドレスに加えて指定されます。[主要アカウント連絡先](#)は、ルートアカウントの E メールアドレスに送信されたすべての E メール通信を引き続き受信します。

アカウントに関連付けられている次の各連絡先タイプのいずれか 1 つのみを指定できます。

- 請求に関するお問い合わせ先
- 操作お問い合わせ先
- セキュリティお問い合わせ先

アカウントがスタンドアロンであるか、組織の一部であるかに応じて、代替連絡先を異なる方法で追加または編集できます。

- スタンドアロン AWS アカウント – 組織に関連付けられ AWS アカウント していない場合は、AWS マネジメントコンソールまたは CLI & SDKs AWS を使用して、独自の代替連絡先を更新できます。この方法については、「[スタンドアロンの AWS アカウントの代替連絡先を更新する](#)」を参照してください。
- AWS アカウント 組織内 – AWS 組織の一部であるメンバーアカウントの場合、管理アカウントまたは委任管理者アカウントのユーザーは、AWS Organizations コンソールから、または CLI と SDKs AWS を介してプログラムで、組織内の任意のメンバーアカウントを一元的に更新できます。これを行う方法については、「[組織 AWS アカウント 内の任意の の代替連絡先を更新する](#)」を参照してください。

トピック

- [電話番号と E メールアドレスの要件](#)
- [スタンドアロンの代替連絡先を更新する AWS アカウント](#)

- [組織 AWS アカウント 内の任意の の代替連絡先を更新する](#)
- [account:AlternateContactTypes コンテキストキー](#)

電話番号と E メールアドレスの要件

アカウントの代替連絡先情報の更新を進める前に、まず、電話番号と E メールアドレスを入力する際の以下の要件を確認することをお勧めします。

- 電話番号には、数字、空白、および文字「+-()」のみを含めることができます。
- E メールアドレスは最大 254 文字で指定することができ、標準の英数字に加えて、E メールアドレスのローカル部分に特殊文字「+=. # | ! & - _」を含めることができます。

スタンドアロンの代替連絡先を更新する AWS アカウント

スタンドアロンの代替連絡先を追加または編集するには AWS アカウント、次の手順を実行します。AWS マネジメントコンソール 次の手順は、常にスタンドアロンコンテキストでのみ機能します。を使用して AWS マネジメントコンソール、オペレーションの呼び出しに使用したアカウントの代替連絡先のみにアクセスまたは変更できます。

AWS マネジメントコンソール

スタンドアロンの代替連絡先を追加または編集するには AWS アカウント

最小アクセス許可

次の手順を実行するには、少なくとも以下の IAM アクセス許可が必要です。

- `account:GetAlternateContact` (代替連絡先の詳細を表示する場合)
- `account:PutAlternateContact` (代替連絡先を設定または更新する場合)
- `account>DeleteAlternateContact` (代替連絡先を削除する場合)

1. [AWS マネジメントコンソール](#) に最小アクセス許可を持つ、IAM ユーザーまたはロールとしてサインインします。
2. ウィンドウの右上にあるアカウント名を選択し、[アカウント] を選択します。

3. [\[アカウント\] ページ](#)で、[代替連絡先] までスクロールダウンして、タイトルの右側で **[編集]** を選択します。

 Note

編集オプションが表示されない場合は、アカウントのルートユーザーとして、または以前に指定した最小限のアクセス許可を持つユーザーとしてサインインしていない可能性があります。

4. 使用可能なフィールドの値を変更します。

 Important

ビジネスでは AWS アカウント、個人に属する電話番号と E メールアドレスではなく、会社の電話番号と E メールアドレスを入力するのがベストプラクティスです。

5. すべての変更を加え終わったら、[Update] (更新) を選択します。

AWS CLI & SDKs

次の AWS CLI コマンドまたは AWS SDK と同等のオペレーションを使用して、代替連絡先情報を取得、更新、または削除できます。

- [GetAlternateContact](#)
- [PutAlternateContact](#)
- [DeleteAlternateContact](#)

 注意事項

- 組織内の管理アカウントまたは委任管理者アカウントからメンバーアカウントに対してこれらの操作を実行するには、[アカウントサービス用の信頼されたアクセスを有効](#)にする必要があります。

 最小アクセス許可

各操作については、その操作に対応するアクセス許可が必要です。

- `GetAlternateContact` (代替連絡先の詳細を表示する場合)
- `PutAlternateContact` (代替連絡先を設定または更新する場合)
- `DeleteAlternateContact` (代替連絡先を削除する場合)

これらの個別のアクセス許可を使用すると、一部のユーザーに連絡先情報の読み取りのみを許可し、他のユーザーには読み取りと書き込みを許可するということもできます。

Example

次の例では、発信者のアカウントに現在設定されている、請求に関する通知の代替連絡先を取得します。

```
$ aws account get-alternate-contact \
  --alternate-contact-type=BILLING
{
  "AlternateContact": {
    "AlternateContactType": "BILLING",
    "EmailAddress": "saanvi.sarkar@amazon.com",
    "Name": "Saanvi Sarkar",
    "PhoneNumber": "+1(206)555-0123",
    "Title": "CF0"
  }
}
```

Example

次の例では、操作に関する通知の代替連絡先を発信者のアカウントに新規に設定します。

```
$ aws account put-alternate-contact \
  --alternate-contact-type=OPERATIONS \
  --email-address=mateo_jackson@amazon.com \
  --name="Mateo Jackson" \
  --phone-number="+1(206)555-1234" \
  --title="Operations Manager"
```

このコマンドは成功時に出力を生成しません。

Example

Note

同じコンタクトタイプ AWS アカウント と同じコンタクトタイプに対して複数の PutAlternateContact オペレーションを実行する場合、は最初に新しいコンタクトを追加し、同じ AWS アカウント とコンタクトタイプへの連続する呼び出しはすべて既存のコンタクトを更新します。

Example

次の例では、発信者のアカウントに設定されている、セキュリティに関する通知の代替連絡先を削除します。

```
$ aws account delete-alternate-contact \  
    --alternate-contact-type=SECURITY
```

このコマンドは成功時に出力を生成しません。

Note

同じ連絡先を何回も削除しようとする、メッセージは表示されずに 1 回目で成功します。それ以降の試行はすべて ResourceNotFound 例外を生成します。

組織 AWS アカウント 内の任意の の代替連絡先を更新する

組織 AWS アカウント 内の の代替連絡先の詳細を追加または編集するには、次の手順を実行します。

要件

AWS Organizations コンソールで代替連絡先を更新するには、いくつかの事前設定を行う必要があります。

- メンバーアカウントで設定を管理するには、所属する組織によってすべての機能が有効にされる必要があります。これにより、管理者がメンバーアカウントを制御できるようになります。これは、組織を作成すると、デフォルトで設定されます。組織が一括決済のみに設定されていて、すべての機能を有効にする場合は、「[組織内のすべての機能の有効化](#)」を参照してください。

- AWS アカウント管理サービスの信頼されたアクセスを有効にする必要があります。これを設定するには、「[AWS アカウント管理の信頼されたアクセスを有効にする](#)」を参照してください。

Note

AWS Organizations 管理ポリシーAWSOrganizationsReadOnlyAccessまたはAWSOrganizationsFullAccessが更新され、コンソールからアカウントデータにアクセスできるように、AWS アカウント管理 APIsへのアクセス許可が付与されます AWS Organizations。更新された管理ポリシーを表示するには、「[Organizations AWS 管理ポリシーの更新](#)」を参照してください。

AWS マネジメントコンソール

組織 AWS アカウント 内の の代替連絡先を追加または編集するには

1. 組織の管理アカウントの認証情報を使用して、[AWS Organizations コンソール](#)にサインインします。
2. AWS アカウントから、更新するアカウントを選択します。
3. [Contact info] (連絡先情報) を選択して、[Alternate contacts] (代替連絡先) で、連絡先のタイプ ([Billing contact] (請求連絡先)、[Security contact] (セキュリティ問い合わせ先)、または [Operations contact] (操作問い合わせ先)) を指定します。
4. 新しい連絡先を追加するには、[Add] (追加) を選択します。既存の連絡先を更新するには、[Edit] (編集) を選択します。
5. 使用可能なフィールドの値を変更します。

Important

ビジネスでは AWS アカウント、個人に属する電話番号と E メールアドレスではなく、会社の電話番号と E メールアドレスを入力するのがベストプラクティスです。

6. すべての変更を加え終わったら、[Update] (更新) を選択します。

AWS CLI & SDKs

次の AWS CLI コマンドまたは AWS SDK と同等のオペレーションを使用して、代替連絡先情報を取得、更新、または削除できます。

- [GetAlternateContact](#)
- [PutAlternateContact](#)
- [DeleteAlternateContact](#)

注意事項

- 組織内の管理アカウントまたは委任管理者アカウントからメンバーアカウントに対してこれらの操作を実行するには、[アカウントサービス用の信頼されたアクセスを有効](#)にする必要があります。
- オペレーションの呼び出しに使用している組織とは異なる組織のアカウントにアクセスすることはできません。

最小アクセス許可

各操作については、その操作に対応するアクセス許可が必要です。

- GetAlternateContact (代替連絡先の詳細を表示する場合)
- PutAlternateContact (代替連絡先を設定または更新する場合)
- DeleteAlternateContact (代替連絡先を削除する場合)

これらの個別のアクセス許可を使用すると、一部のユーザーに連絡先情報の読み取りのみを許可し、他のユーザーには読み取りと書き込みを許可するということもできます。

Example

次の例では、組織内の発信者のアカウントに現在設定されている、請求に関する通知の代替連絡先を取得します。使用される認証情報は、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのいずれかから取得する必要があります。

```
$ aws account get-alternate-contact \  
    --alternate-contact-type=BILLING \  
    --profile=ADMINISTRATOR
```



```
--account-id 123456789012

{
  "AlternateContact": {
    "AlternateContactType": "BILLING",
    "EmailAddress": "saanvi.sarkar@amazon.com",
    "Name": "Saanvi Sarkar",
    "PhoneNumber": "+1(206)555-0123",
    "Title": "CF0"
  }
}
```

Example

次の例では、組織内の指定されたメンバーアカウントの操作に関する代替連絡先を設定します。使用する認証情報は、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのいずれかである必要があります。

```
$ aws account put-alternate-contact \
  --account-id 123456789012 \
  --alternate-contact-type=OPERATIONS \
  --email-address=mateo_jackson@amazon.com \
  --name="Mateo Jackson" \
  --phone-number="+1(206)555-1234" \
  --title="Operations Manager"
```

このコマンドは成功時に出力を生成しません。

Note

同じコンタクトタイプ AWS アカウント と同じコンタクトタイプに対して複数の PutAlternateContact オペレーションを実行する場合、は最初に新しいコンタクトを追加し、同じ AWS アカウント とコンタクトタイプへの連続する呼び出しはすべて既存のコンタクトを更新します。

Example

次の例では、組織内の指定されたメンバーアカウントのセキュリティに関する代替連絡先を削除します。使用する認証情報は、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのいずれかである必要があります。

```
$ aws account delete-alternate-contact \
  --account-id 123456789012 \
  --alternate-contact-type=SECURITY
```

このコマンドは成功時に出力を生成しません。

Example

Note

同じ連絡先を何回も削除しようとする、メッセージは表示されずに 1 回目で成功します。それ以降の試行はすべて ResourceNotFound 例外を生成します。

account:AlternateContactTypes コンテキストキー

コンテキストキーを使用して account:AlternateContactTypes、IAM ポリシーによって許可 (または拒否) される 3 つの問い合わせタイプを指定できます。例えば、次の例の IAM アクセス許可ポリシーでは、この条件キーを使用して、組織内の特定のアカウントの BILLING 代替連絡先のみを取得し、変更は行わないことを、アタッチされたプリンシパルに許可しています。

account:AlternateContactTypes は複数値を持つ文字列型のため、[ForAnyValue](#) または [ForAllValues](#) [複数値文字列演算子](#)を使用する必要があります。

のプライマリ連絡先を更新する AWS アカウント

これらの手順は、サインアップ for AWS (アドバンスド) AWS の使用にサインアップ AWS アカウントした場合、またはアカウントの高度な機能をアクティブ化した場合に、のプライマリ連絡先を更新する方法を示しています。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

アカウントに関連付けられている主要連絡先情報を更新できます。これには、連絡先の氏名、会社名、郵送先住所、電話番号、ウェブサイトアドレスなどが含まれます。

主な連絡先の電話番号を確認することもできます。詳細については、「[主な連絡先電話番号を確認する](#)」を参照してください。

アカウントがスタンドアロンであるか、組織の一部であるかに応じて、主要アカウント連絡先の編集方法は異なります。

- スタンドアロン AWS アカウント – 組織に関連付けられ AWS アカウント がない場合は、AWS マネジメントコンソールまたは CLI & SDKs AWS を使用して、独自のプライマリアカウントの連絡先を更新できます。これを行う方法については、[「スタンドアロン AWS アカウント の主要連絡先の更新」](#)を参照してください。
- AWS アカウント 組織内 – AWS 組織の一部であるメンバーアカウントの場合、管理アカウントまたは委任管理者アカウントのユーザーは、AWS Organizations コンソールから、または CLI と SDKs AWS を介してプログラムで、組織内の任意のメンバーアカウントを一元的に更新できます。これを行う方法については、[「Update AWS アカウント primary contact in your organization」](#)を参照してください。

トピック

- [電話番号と E メールアドレスの要件](#)
- [スタンドアロンアカウント AWS アカウント または管理アカウントのプライマリ連絡先を更新する](#)
- [組織内の AWS メンバーアカウントの主要連絡先を更新する](#)
- [主な連絡先電話番号を確認する](#)

電話番号と E メールアドレスの要件

アカウントの主要連絡先情報の更新を進める前に、まず、電話番号と E メールアドレスを入力する際の以下の要件を確認することをお勧めします。

- 電話番号には数字のみを含める必要があります。
- 電話番号は + と国コードで始まる必要があり、国コードの後に先行ゼロや追加のスペースがあってはなりません。例えば、+1 (米国/カナダ) や +44 (英国) です。
- 電話番号には、市外局番、交換コード、ローカルコードの間に空白を含めることはできません。例えば、+12025550179 などです。
- セキュリティ上の理由から、電話番号は AWS からの SMS を受信する必要があります。ほとんどの通話料無料番号は SMS をサポートしていないため、受け付けられません。
- ビジネスでは AWS アカウント、個人に属する電話番号と E メールアドレスではなく、会社の電話番号と E メールアドレスを入力するのがベストプラクティスです。アカウントの[ルートユーザー](#)を個人の E メールアドレスまたは電話番号で設定すると、その個人が退職した場合にアカウントの復旧が困難になる可能性があります。

スタンドアロンアカウント AWS アカウント または管理アカウントのプライマリ連絡先を更新する

スタンドアロンアカウント AWS アカウント または管理アカウントの主要連絡先の詳細を編集するには、次の手順を実行します。AWS マネジメントコンソール 次の手順は、常にスタンドアロンコンテキストでのみ機能します。AWS マネジメントコンソール を使用してアクセスまたは変更できるのは、オペレーションの呼び出しに使用したアカウントの主要連絡先情報のみです。

AWS マネジメントコンソール

スタンドアロンアカウント AWS アカウント または管理アカウントのプライマリ連絡先を編集するには

最小アクセス許可

次の手順を実行するには、少なくとも以下のIAM アクセス許可が必要です。

- `account:GetContactInformation` (主要連絡先の詳細を表示する場合)
- `account:PutContactInformation` (主要連絡先の詳細を更新する場合)

1. [AWS マネジメントコンソール](#) に最小アクセス許可を持つ、IAM ユーザーまたはロールとしてサインインします。
2. ウィンドウの右上にあるアカウント名を選択し、[アカウント] を選択します。
3. [Contact information] (連絡先情報) セクションまで下にスクロールし、その隣にある [Edit] (編集) を選択します。
4. 使用可能なフィールドの値を変更します。
5. すべての変更を加え終わったら、[Update] (更新) を選択します。

AWS CLI & SDKs

次の AWS CLI コマンドまたは AWS SDK と同等のオペレーションを使用して、主要な連絡先情報を取得、更新、または削除できます。

- [GetContactInformation](#)
- [PutContactInformation](#)

注意事項

- 組織内の管理アカウントまたは委任管理者アカウントからメンバーアカウントに対してこれらの操作を実行するには、[アカウントサービス用の信頼されたアクセスを有効](#)にする必要があります。

最小アクセス許可

各操作については、その操作に対応するアクセス許可が必要です。

- account:GetContactInformation
- account:PutContactInformation

これらの個別のアクセス許可を使用すると、一部のユーザーに連絡先情報の読み取りのみを許可し、他のユーザーには読み取りと書き込みを許可するということもできます。

Example

次の例では、発信者のアカウントの現在の主要連絡先情報を取得します。

```
$ aws account get-contact-information
{
  "ContactInformation": {
    "AddressLine1": "123 Any Street",
    "City": "Seattle",
    "CompanyName": "Example Corp, Inc.",
    "CountryCode": "US",
    "DistrictOrCounty": "King",
    "FullName": "Saanvi Sarkar",
    "PhoneNumber": "+15555550100",
    "PostalCode": "98101",
    "StateOrRegion": "WA",
    "WebsiteUrl": "https://www.examplecorp.com"
  }
}
```

Example

次の例では、発信者のアカウントに新しい主要連絡先情報を設定します。

```
$ aws account put-contact-information --contact-information \
'{"AddressLine1": "123 Any Street", "City": "Seattle", "CompanyName": "Example Corp,
Inc.", "CountryCode": "US", "DistrictOrCounty": "King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
"StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

このコマンドは成功時に出力を生成しません。

組織内の AWS メンバーアカウントの主要連絡先を更新する

組織内の AWS メンバーアカウントの主要連絡先の詳細を編集するには、次の手順を実行します。

その他の要件

AWS Organizations コンソールでプライマリ連絡先を更新するには、いくつかの事前設定を行う必要があります。

- メンバーアカウントで設定を管理するには、所属する組織によってすべての機能が有効にされる必要があります。これにより、管理者がメンバーアカウントを制御できるようになります。これは、組織を作成すると、デフォルトで設定されます。組織が一括決済のみに設定されていて、すべての機能を有効にする場合は、「[組織内のすべての機能の有効化](#)」を参照してください。
- AWS アカウント管理サービスの信頼されたアクセスを有効にする必要があります。これを設定するには、「[AWS アカウント管理の信頼されたアクセスを有効にする](#)」を参照してください。

AWS マネジメントコンソール

組織 AWS アカウント 内の の の主要連絡先を編集するには

- 組織の管理アカウントの認証情報を使用して、[AWS Organizations コンソール](#)にサインインします。
- AWS アカウントから、更新するアカウントを選択します。
- 連絡先情報を選択し、プライマリ連絡先を見つけます。
- [Edit] (編集) を選択します。
- 使用可能なフィールドの値を変更します。

6. すべての変更を行ったら、保存 を選択します。

電話番号を変更すると、保存を選択すると検証コードが新しい番号に送信されます。番号はすぐに、または後で確認できます。詳細については、「[組織内のメンバーアカウントの電話番号を確認する](#)」を参照してください。

AWS CLI & SDKs

次の AWS CLI コマンドまたは AWS SDK と同等のオペレーションを使用して、主要な連絡先情報を取得、更新、または削除できます。

- [GetContactInformation](#)
- [PutContactInformation](#)

注意事項

- 組織内の管理アカウントまたは委任管理者アカウントからメンバーアカウントに対してこれらの操作を実行するには、[アカウントサービス用の信頼されたアクセスを有効](#)にする必要があります。
- オペレーションの呼び出しに使用している組織とは異なる組織のアカウントにアクセスすることはできません。

最小アクセス許可

各操作については、その操作に対応するアクセス許可が必要です。

- `account:GetContactInformation`
- `account:PutContactInformation`

これらの個別のアクセス許可を使用すると、一部のユーザーに連絡先情報の読み取りのみを許可し、他のユーザーには読み取りと書き込みを許可するということもできます。

Example

次の例では、組織内の指定されたメンバーアカウントの現在の主要連絡先情報を取得します。使用される認証情報は、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのいずれかから取得する必要があります。

```
$ aws account get-contact-information --account-id 123456789012
{
  "ContactInformation": {
    "AddressLine1": "123 Any Street",
    "City": "Seattle",
    "CompanyName": "Example Corp, Inc.",
    "CountryCode": "US",
    "DistrictOrCounty": "King",
    "FullName": "Saanvi Sarkar",
    "PhoneNumber": "+15555550100",
    "PostalCode": "98101",
    "StateOrRegion": "WA",
    "WebsiteUrl": "https://www.examplecorp.com"
  }
}
```

Example

次の例では、組織内の指定されたメンバーアカウントの主要連絡先情報を設定します。使用する認証情報は、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのいずれかである必要があります。

```
$ aws account put-contact-information --account-id 123456789012 \
--contact-information '{"AddressLine1": "123 Any Street", "City": "Seattle",
"CompanyName": "Example Corp, Inc.", "CountryCode": "US", "DistrictOrCounty":
"King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
"StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

このコマンドは成功時に出力を生成しません。

主な連絡先電話番号を確認する

電話番号は、の主要な連絡先情報で確認できます AWS アカウント。の検証により、登録されている電話番号が SMS テキストメッセージを受信できることを確認します。

検証を開始すると、SMS テキストメッセージで 6 桁の検証コードが、アカウントの現在登録されている電話番号に送信されます。検証を開始するために電話番号を入力しません。終了するには、有効期限が切れる前にコードを入力します。

電話番号を検証するときは、次の点に注意してください。

- コードは送信後 5 分で期限切れになります。
- 新しいコードをリクエストすると、以前に送信したコードは機能しなくなります。
- コードが正しくないか、有効期限が切れている場合は、新しいコードをリクエストして、もう一度試してください。
- コードの送信後に電話番号が変更された場合、そのコードは使用できません。現在の番号の新しいコードをリクエストします。
- 検証ステータスは常に、現在登録されている電話番号を記述します。電話番号を変更すると、ステータスは新しい番号を表します。
- 組織内のメンバーアカウントの場合、コードはメンバーアカウントの主要連絡先電話番号に送信され、ユーザーには送信されません。開始する前に、その電話を持っているすべてのユーザーからコードを取得できることを確認してください。

検証ステータスを確認するには、[GetContactInformation](#) オペレーションを使用します。レスポンスの `VerificationStatus` フィールドには、次のいずれかの値があります。

- VERIFIED – ファイルの電話番号が検証されます。
- UNVERIFIED – ファイルの電話番号は検証されません。
- NOT_SUPPORTED – 電話番号の検証はこのアカウントでは使用できません。

スタンドアロンまたは管理の電話番号を確認する AWS アカウント

認証情報を使用するアカウントの電話番号を確認するには、次の AWS CLI コマンドまたは AWS SDK と同等のオペレーションを使用します。

- [SendPhoneNumberVerification](#)
- [VerifyPhoneNumber](#)

最小アクセス許可

各操作については、その操作に対応するアクセス許可が必要です。

- `account:SendPhoneNumberVerification`
- `account:VerifyPhoneNumber`

検証ステータスを確認するには、必要です `account:GetContactInformation`。

Example

次の AWS CLI 例では、発信者のアカウントの主要連絡先電話番号に検証コードを送信します。

```
$ aws account send-phone-number-verification
{
  "Status": "PENDING"
}
```

Example

次の AWS CLI 例では、検証を完了するためにコードを送信します。

```
$ aws account verify-phone-number --otp 123456
{
  "Status": "VERIFIED"
}
```

Example

次の AWS CLI 例では、発信者の主要連絡先電話番号の検証ステータスを取得します。

```
$ aws account get-contact-information --query VerificationStatus
"VERIFIED"
```

組織内のメンバーアカウントの電話番号を確認する

コンソール、AWS CLI または AWS SDK を使用して AWS Organizations、メンバーアカウントの電話番号を確認できます。開始する前に、「」のステップを完了してください [その他の要件](#)。

AWS マネジメントコンソール

メンバーアカウントの主要連絡先電話番号を確認するには

最小アクセス許可

次の手順を実行するには、少なくとも以下のIAM アクセス許可が必要です。

- `account:GetContactInformation` (電話番号と検証済みかどうかを確認するため)
- `account:SendPhoneNumberVerification` (検証コードを送信するため)
- `account:VerifyPhoneNumber` (コードを送信するため)

AWSOrganizationsFullAccess 管理ポリシーには、`account:SendPhoneNumberVerification`または `account:VerifyPhoneNumber` は含まれません。そのポリシーに依存する場合は、これらのアクセス許可を個別に付与します。

1. 組織の管理アカウントの認証情報を使用して、[AWS Organizations コンソール](#)にサインインします。
2. からAWS アカウント、メンバーアカウントを選択します。
3. 連絡先情報を選択し、プライマリ連絡先を見つけます。
4. 電話番号が検証されていない場合は、警告が表示されます。電話番号を選択し、電話番号の確認を選択します。メンバーアカウントの電話番号に 6 桁のコードが送信されます。
5. 検証コードにコードを入力し、検証を選択します。

コードが届かない場合は、そのオプションが利用可能になったときにコードを再送信を選択します。

AWS CLI & SDKs

メンバーアカウントの電話番号を確認するには、次の AWS CLI コマンドまたは AWS SDK と同等のオペレーションを使用して、メンバーアカウント ID を指定します。

- [SendPhoneNumberVerification](#)
- [VerifyPhoneNumber](#)

注意事項

- 使用する認証情報は、組織の管理アカウントまたは AWS アカウント管理の委任管理者アカウントのいずれかからのものである必要があります。
- オペレーションの呼び出しに使用している組織とは異なる組織のアカウントにアクセスすることはできません。

最小アクセス許可

各操作については、その操作に対応するアクセス許可が必要です。

- `account:SendPhoneNumberVerification`
- `account:VerifyPhoneNumber`

検証ステータスを確認するには、必要です `account:GetContactInformation`。

Example

次の AWS CLI 例では、指定されたメンバーアカウントのプライマリ連絡先の電話番号に検証コードを送信します。

```
$ aws account send-phone-number-verification --account-id 123456789012
{
  "Status": "PENDING"
}
```

Example

次の AWS CLI 例では、メンバーアカウントの電話番号に送信されたコードを送信します。

```
$ aws account verify-phone-number --account-id 123456789012 --otp 123456
{
  "Status": "VERIFIED"
}
```

AWS アカウント 識別子の表示

この情報は、サインアップ for AWS (アドバンスド) AWS の使用にサインアップした場合、またはアカウントの高度な機能をアクティブ化した場合の AWS アカウント 識別子の表示に関するものです。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

AWS は、それぞれに次の一意の識別子を割り当てます AWS アカウント。

[AWS アカウント ID](#)

AWS アカウントを一意に識別する 12 桁の数値 (012345678901 など)。多くの AWS リソースには、[Amazon リソースネーム \(ARNs\)](#) のアカウント ID が含まれます。アカウント ID 部分では、あるアカウントのリソースと、別のアカウントのリソースを区別します。AWS Identity and Access Management (IAM) ユーザーの場合は、アカウント ID またはアカウントエイリアス AWS マネジメントコンソール を使用して にサインインできます。アカウント ID は、他の識別情報と同様に、慎重に使用および共有する必要がありますが、秘密情報、センシティブ情報、または機密情報とは見なされません。

[正規ユーザー ID](#)

ID の難読化された形

式79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2beであるなどの英数字識別子 AWS アカウント 。この ID を使用して、Amazon Simple Storage Service (Amazon S3) を使用してバケットとオブジェクトへのクロスアカウントアクセスを許可する AWS アカウント ときに、 を識別できます。Amazon S3 AWS アカウント の正規ユーザー ID は、[ルートユーザー](#)または IAM ユーザーとして取得できます。

これらの識別子を表示するには AWS 、 で認証されている必要があります。

Warning

AWS リソースを共有するために AWS アカウント 識別子を必要とする第三者に AWS 認証情報 (パスワードやアクセスキーを含む) を提供しないでください。そうすることで、ユーザーが持っているのと同じアクセス権がユーザーに付与 AWS アカウント されます。

AWS アカウント ID を検索する

AWS アカウント ID は、AWS マネジメントコンソール または AWS Command Line Interface () を使用して確認できますAWS CLI。コンソールでは、アカウント ID の場所は、ルートユーザーとしてサインインしているか、IAM ユーザーとしてサインインしているかによって異なります。アカウント ID は、ルートユーザーとしてサインインしているか、IAM ユーザーとしてサインインしているかにかかわらず同じです。

ルートユーザーとしてアカウント ID を検索するには

AWS マネジメントコンソール

ルートユーザーとしてサインインしたときに AWS アカウント ID を検索するには

最小アクセス許可

次の手順を実行するには、少なくとも以下の IAM アクセス許可が必要です。

- ルートユーザーとしてサインインすると、IAM アクセス許可は必要ありません。

1. 右上のナビゲーションバーでアカウント名またはアカウント番号を選択し、[セキュリティ認証情報] を選択します。

Tip

[セキュリティ認証情報] オプションが表示されない場合、IAM ユーザーではなく IAM ロールを持つフェデレーションユーザーとしてサインインしている可能性があります。その場合は、[アカウント] エントリとその横にあるアカウント ID 番号を探してください。

2. [アカウントの詳細] セクションの [AWS アカウント ID] の横にアカウント番号が表示されます。

AWS CLI & SDKs

を使用して AWS アカウント ID を検索するには AWS CLI

i 最小アクセス許可

次の手順を実行するには、少なくとも以下の IAM アクセス許可が必要です。

- ルートユーザーとしてコマンドを実行する場合、IAM アクセス許可は必要ありません。

[get-caller-identity](#) コマンドを次のように使用します。

```
$ aws sts get-caller-identity \  
  --query Account \  
  --output text  
123456789012
```

IAM ユーザーとしてアカウント ID を検索する

AWS マネジメントコンソール

IAM ユーザーとしてサインインしたときに AWS アカウント ID を検索するには

i 最小アクセス許可

次の手順を実行するには、少なくとも以下の IAM アクセス許可が必要です。

- `account:GetAccountInformation`

1. 右上のナビゲーションバーでユーザー名を選択し、続いて [認証情報] を選択します。

i Tip

[セキュリティ認証情報] オプションが表示されない場合、IAM ユーザーではなく IAM ロールを持つフェデレーションユーザーとしてサインインしている可能性があります。その場合は、[アカウント] エントリとその横にあるアカウント ID 番号を探してください。

2. ページ上部の [アカウントの詳細] で、[AWS アカウント ID] の横にアカウント番号が表示されます。

AWS CLI & SDKs

を使用して AWS アカウント ID を検索するには AWS CLI

最小アクセス許可

次の手順を実行するには、少なくとも以下の IAM アクセス許可が必要です。

- IAM ユーザーまたはロールとしてコマンドを実行する場合は、次のものがが必要です。
- `sts:GetCallerIdentity`

[get-caller-identity](#) コマンドを次のように使用します。

```
$ aws sts get-caller-identity \  
  --query Account \  
  --output text  
123456789012
```

の正規ユーザー ID を検索する AWS アカウント

AWS マネジメントコンソール または AWS アカウント を使用して、 の正規ユーザー ID を確認できます AWS CLI。 の正規ユーザー ID AWS アカウント は、そのアカウントに固有です。 の正規ユーザー ID は、ルートユーザー、フェデレーティッドユーザー、または IAM ユーザー AWS アカウント として取得できます。

ルートユーザーまたは IAM ユーザーとして正規ユーザー ID を検索する

AWS マネジメントコンソール

ルートユーザーまたは IAM ユーザーとしてコンソールにサインインしたときに、アカウントの正規ユーザー ID を検索するには

最小アクセス許可

次の手順を実行するには、少なくとも以下の IAM アクセス許可が必要です。

- ルートユーザーとしてコマンドを実行する場合、IAM アクセス許可は必要ありません。

- IAM ユーザーとしてサインインすると、次のことが必要です。
- `account:GetAccountInformation`

1. ルートユーザーまたは IAM ユーザー AWS マネジメントコンソール として にサインインします。
2. 右上のナビゲーションバーでアカウント名またはアカウント番号を選択し、[セキュリティ認証情報] を選択します。

 Tip

[セキュリティ認証情報] オプションが表示されない場合、IAM ユーザーではなく IAM ロールを持つフェデレーションユーザーとしてサインインしている可能性があります。その場合は、[アカウント] エントリとその横にあるアカウント ID 番号を探してください。

3. [アカウントの詳細] セクションで、[正規ユーザー ID] の横に、正規ユーザー ID が表示されます。正規ユーザー ID を使用して、Amazon S3 アクセスコントロールリスト (ACL) を設定できます。

AWS CLI & SDKs

を使用して正規ユーザー ID を検索するには AWS CLI

、IAM ユーザー AWS アカウントのルートユーザー、または IAM ロールでも同じ AWS CLI および API コマンドが機能します。

[list-buckets](#) コマンドを次のように使用します。

```
$ aws s3api list-buckets \  
  --max-items 10 \  
  --page-size 10 \  
  --query Owner.ID \  
  --output text  
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

IAM ロールを持つフェデレーションユーザーとして正規 ID を検索する

AWS マネジメントコンソール

IAM ロールを持つフェデレーションユーザーとしてコンソールにサインインしている場合に、アカウントの正規ユーザー ID を検索する手順

最小アクセス許可

- Amazon S3 バケットを一覧表示して表示するには、アクセス許可が必要です。

1. IAM ロールを持つフェデレーテッドユーザー AWS マネジメントコンソール として にサインインします。
2. バケットの詳細を表示するには、Amazon S3 コンソールでバケット名を選択します。
3. [アクセス許可] タブを選択します。
4. [アクセスコントロールリスト] セクションの [バケット所有者] の下に、AWS アカウント の正規 ID が表示されます。

AWS CLI & SDKs

を使用して正規ユーザー ID を検索するには AWS CLI

、IAM ユーザー AWS アカウントのルートユーザー、または IAM ロールでも同じ AWS CLI および API コマンドが機能します。

[list-buckets](#) コマンドを次のように使用します。

```
$ aws s3api list-buckets \
  --max-items 10 \
  --page-size 10 \
  --query Owner.ID \
  --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

のトラブルシューティング AWS アカウント

この情報は、サインアップ for AWS (アドバンスド) AWS の使用にサインアップ AWS アカウントした場合、またはアカウントの高度な機能をアクティブ化した場合の のトラブルシューティングに関するものです。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

以下のトピックの情報は、AWS アカウントに関する問題の診断と解決に役立ちます。ルートユーザーに関するヘルプについては、「IAM ユーザーガイド」の「[ルートユーザーに関する問題をトラブルシューティングする](#)」を参照してください。サインインプロセスに関するヘルプについては、「AWS サインインユーザーガイド」の「[Troubleshooting AWS アカウント sign-in issues](#)」を参照してください。

トラブルシューティングのトピック

- [AWS アカウント 作成に関する問題のトラブルシューティング](#)
- [AWS アカウント 閉鎖に関する問題のトラブルシューティング](#)
- [に関するその他の問題のトラブルシューティング AWS アカウント](#)

AWS アカウント 作成に関する問題のトラブルシューティング

この情報は、サインアップ for AWS (アドバンスド) AWS の使用にサインアップ AWS アカウントした場合、またはアカウントの高度な機能をアクティブ化した場合の作成に関する問題のトラブルシューティングに関するものです。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

次の表のリファレンスリンクを使用して、新しい の作成に関する問題の診断と修正に役立ててください AWS アカウント。

問題	参照リンク	ソース
アカウントのサインアップまたは作成方法がわからない	にサインアップする AWS (アドバンスド)	本ガイド
新しいアカウント AWS を確認するために から電話を受け取らなかった場合、または入	https://repost.aws/knowledge-center/phone-verify-no-call	AWS re:Post

問題	参照リンク	ソース
力した PIN が機能しない場合はどうすればよいですか？		
電話 AWS アカウント による検証を試みたときの「最大試行回数」エラーを解決するにはどうすればよいですか？	https://repost.aws/knowledge-center/maximum-failed-attempts	AWS re:Post
24 時間以上経過しましたが、アカウントが有効になっていません	https://repost.aws/knowledge-center/create-and-activate-aws-account	AWS re:Post
新しいアカウントの作成後にサインインできない	https://docs.aws.amazon.com/signin/latest/userguide/troubleshooting-sign-in-issues.html	AWS サインインユーザーガイド

さらにヘルプが必要な場合は、[AWS re:Post](#) で特定の問題に関連するコンテンツを検索することをお勧めします。さらにサポートが必要な場合は、[AWS サポート](#) にお問い合わせください。

AWS アカウント 閉鎖に関する問題のトラブルシューティング

この情報は、サインアップ for AWS (アドバンスド) AWS の使用にサインアップした場合、またはアカウントの高度な機能をアクティブ化した場合の、AWS アカウント 閉鎖に関する問題のトラブルシューティングに関するものです。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

以下の情報を使用すると、アカウント閉鎖プロセス中に発生する一般的な問題を診断して修正するのに役立ちます。アカウント閉鎖プロセスに関する一般的な情報については、「[を閉じる AWS アカウント](#)」を参照してください。

トピック

- [アカウントを削除またはキャンセルする方法がわからない](#)
- [\[アカウント\] ページに \[アカウントを閉鎖する\] ボタンが表示されない](#)
- [アカウントを閉鎖したが、まだ確認 E メールを受け取っていない](#)
- [アカウントを閉鎖しようとする、「ConstraintViolationException」エラーが表示される](#)

- [メンバーアカウントを閉鎖しようとする](#)と「CLOSE_ACCOUNT_QUOTA_EXCEEDED」エラーが表示される
- [管理アカウントを閉鎖する前に AWS 組織を削除する必要がありますか？](#)

アカウントを削除またはキャンセルする方法がわからない

アカウントを閉鎖するには、「[を閉じる AWS アカウント](#)」の手順に従います。

[アカウント] ページに [アカウントを閉鎖する] ボタンが表示されない

ルートユーザーとしてサインインしていない場合、[アカウント] ページに [アカウントを閉鎖する] ボタンは表示されません。アカウントを閉鎖するには、[ルートユーザー AWS マネジメントコンソールとしてにサインイン](#)する必要があります。サインインできない場合は、「[ルートユーザーに関する問題をトラブルシューティングする](#)」を参照してください。

アカウントを閉鎖したが、まだ確認 E メールを受け取っていない

この確認 E メールは、AWS アカウントのルートユーザーの E メールアドレスとにのみ送信されます。この E メールが数時間以内に届かない場合は、[ルートユーザー AWS マネジメントコンソールとしてにサインイン](#)して、アカウントが閉鎖されていることを確認できます。アカウントが正常に閉鎖されていれば、アカウントが閉鎖されたことを示すメッセージが表示されます。閉鎖したアカウントがメンバーアカウントである場合は、閉鎖したアカウントが AWS Organizations コンソールCLOSEDで とラベル付けされているかどうかを確認することで、閉鎖の成功を確認できます。詳細については、「AWS Organizations ユーザーガイド」の「[組織のメンバーアカウントを閉鎖する](#)」を参照してください。

管理アカウントを閉鎖しようとしており、アカウント閉鎖に関する確認 E メールが届かない場合、最も可能性が高いのは、組織にアクティブなメンバーアカウントが含まれていることです。管理アカウントを閉鎖できるのは、組織にアクティブなメンバーアカウントが含まれていない場合のみです。組織にアクティブなメンバーアカウントが残っていないことを確認するには、AWS Organizations コンソールに移動し、すべてのメンバーアカウントがアカウント名のClosed横に表示されていることを確認します。その後、管理アカウントを閉鎖できます。

アカウントを閉鎖しようとする、「ConstraintViolationException」エラーが表示される

AWS Organizations コンソールを使用して管理アカウントを閉鎖しようとしていますが、これはできません。管理アカウントを閉鎖するには、管理アカウントの[ルートユーザー AWS マネジメントコン](#)

[ソールとしてにサインイン](#)し、アカウントページから閉鎖する必要があります。詳細については、「AWS Organizations ユーザーガイド」の「[組織の管理カウントの閉鎖](#)」を参照してください。

メンバーアカウントを閉鎖しようとする

「CLOSE_ACCOUNT_QUOTA_EXCEEDED」エラーが表示される

メンバーアカウントの 20% は、ローリング 30 日以内にのみ閉鎖できます。このクォータは暦月に縛られず、アカウントを閉鎖した時点で開始されます。最初のアカウント閉鎖から 30 日以内に、20% のアカウント閉鎖制限を超えることはできません。アカウントの 20% が 1000 を超えた場合でも、最小アカウント閉鎖数は 250、最大アカウント閉鎖数は 1000 です。Organizations のクォータの詳細については、「AWS Organizations ユーザーガイド」の「[AWS Organizations のクォータ](#)」を参照してください。

管理アカウントを閉鎖する前に AWS 組織を削除する必要がありますか？

いいえ。管理アカウントを閉鎖する前に AWS 組織を削除する必要はありません。ただし、管理アカウントを閉鎖できるのは、組織にアクティブなメンバーアカウントが含まれていない場合のみです。組織にアクティブなメンバーアカウントが残っていないことを確認するには、AWS Organizations コンソールに移動し、すべてのメンバーアカウントがアカウント名の Closed 横に表示されていることを確認します。その後、管理アカウントを閉鎖できます。

に関するその他の問題のトラブルシューティング AWS アカウント

この情報は、サインアップ for AWS (アドバンスド) AWS の使用にサインアップ AWS アカウントした場合、またはアカウントの高度な機能をアクティブ化した場合の [その他の問題のトラブルシューティング](#)に関するものです。サインアップオプションを比較するには、「[サインアップオプションを比較する](#)」を参照してください。

ここに記載する情報は、AWS アカウントに係る問題のトラブルシューティングに役立ちます。

問題

- [のクレジットカードを変更する必要があります AWS アカウント](#)
- [不正行為を報告する必要がある AWS アカウント](#)
- [を閉じる必要があります AWS アカウント](#)
- [ルートユーザーの E メールアドレス AccessDeniedException を更新すると を取得する](#)

のクレジットカードを変更する必要があります AWS アカウント

のクレジットカードを変更するには AWS アカウント、サインインできる必要があります。AWS には、アカウント所有者であることを証明する必要がある保護があります。手順については、[AWS Billing ユーザーガイド](#)の「クレジットカード支払い方法の管理」を参照してください。

不正行為を報告する必要がある AWS アカウント

を使用した不正行為の疑い AWS アカウント があり、報告を行う場合は、「[AWS リソースの不正使用を報告する方法](#)」を参照してください。

Amazon.com での購入に問題がある場合は、「[Amazon カスタマーサービス](#)」を参照してください。

を閉じる必要があります AWS アカウント

の閉鎖に関する問題のトラブルシューティングについては AWS アカウント、「」を参照してください [を閉じる AWS アカウント](#)。

ルートユーザーの E メールアドレス **AccessDeniedException** を更新すると を取得する

メンバーアカウントがプロジェクトアカウントの場合、ルートユーザーの E メールアドレスを更新することはできません。AWS Builder ID は、ルートユーザーの E メールアドレスではなく、各プロジェクトアカウントを所有します。詳細については、「[高度な機能をアクティブ化した後のプロジェクトアカウント](#)」を参照してください。

インドでのアカウントの管理

この情報は、サインアップ for AWS (アドバンスド) AWS の使用にサインアップした場合、またはアカウントの高度な機能をアクティブ化した場合の、インドでのアカウントの管理に関するものです。サインアップオプションを比較するには、「」を参照してください [サインアップオプションを比較する](#)。

新しい にサインアップ AWS アカウント し、連絡先住所と請求先住所としてインドを選択した場合、ユーザー契約はインドの現地 AWS 販売者である Amazon Web Services India Private Limited (AWS インド) と締結されます。AWS インドは請求を管理し、請求書の合計は米ドル (USD) ではなくインドルピー (INR) で表示されます。の管理の詳細については AWS アカウント、「」を参照してください [を設定する AWS アカウント](#)。

アカウントが AWS India にある場合は、このトピックの手順に従ってアカウントを管理します。このトピックでは、AWS インドアカウントにサインアップし、AWS インドアカウントに関する情報を編集し、顧客確認を管理し、Permanent Account Number (PAN) を追加または編集する方法について説明します。

サインアップ時のクレジットカード検証の一環として、AWS インドはクレジットカードに 2 INR を請求します。AWS インドは、検証が完了した後に 2 INR を返金します。確認プロセス中に、お客様の銀行にリダイレクトされる場合があります。

トピック

- [India AWS アカウント で を作成する AWS](#)
- [顧客検証情報の管理](#)

India AWS アカウント で を作成する AWS

AWS India は、インドの の現地販売 AWS 者です。連絡先と請求先住所がインドにあり、アカウントを作成する場合は、次の手順を使用して AWS India アカウントにサインアップします。

AWS India アカウントにサインアップするには

1. [Amazon Web Services ホームページ](#)を開きます。
2. の作成 AWS アカウント を選択します。

Note

AWS 最近 にサインインした場合、そのオプションは存在しない可能性があります。[Sign in to the Console] (コンソールにサインインする) を選択します。それでも [新しい AWS アカウントの作成] が表示されない場合は、[別のアカウントにサインイン] を選択し、その後に [新しい AWS アカウントの作成] を選択します。

3. アカウント情報を入力し、E メールアドレスを確認し、アカウント用の強力なパスワードを選択します。
4. [ビジネス] または [個人] を選択します。個人アカウントとプロフェッショナルアカウントの機能は同じです。
5. 会社または個人の連絡先情報を入力します。連絡先または請求先住所がインドにある場合、インドのコンピュータ緊急対応チーム (CERT-In) の規制に従って、AWS は、AWS サービスへのアクセスを許可する前に、お客様の ID 情報を収集して検証する必要があります。

連絡先情報または請求情報から選択する名前は、顧客検証に使用する予定のドキュメントに表示される名前と完全に一致する必要があります。例えば、設立証明証を使用してビジネスアカウントを確認する予定の場合は、そのドキュメントに記載されている事業名を提供する必要があります。受け入れられたドキュメントタイプのリストについては、「[the section called “顧客確認用にインドで受け入れられるドキュメント”](#)」を参照してください。

6. カスタマーアグリーメントを読んだら、利用規約のチェックボックスを選択し、[続行] を選択します。
7. [請求情報] ページで、使用する支払い方法を入力します。検証プロセスの一部として CVV を指定する必要があります。
8. [PAN がありますか?] で、税務請求書に表示したい納税者番号 (PAN) がある場合は [はい] を選択して PAN を入力します。PAN がない場合、またはサインアップ後に追加する場合は、[いいえ] を選択します。
9. Verify and continue を選択します。AWS India は、検証プロセスの一環としてカード 2 INR を請求します。AWS India は、検証が完了した後に 2 INR を返金します。
10. [本人確認] ページで、アカウント登録の主な目的を選択します。
11. アカウントの所有者を最も適切に表す所有権タイプを選択します。所有権タイプとして会社、組織、またはパートナーシップを選択する場合は、主要な管理担当者の名前を入力します。主要な管理担当者には、取締役、業務責任者、または事業の運営責任者を指定できます。
12. 選択した所有権タイプに応じて、検証に使用する承認済みのインドのドキュメントタイプを選択し、ドキュメント情報を入力します。

 Note

個人アカウントを持っており、インド連邦による発行ではない運転免許証を使用する予定の場合は、検証用に別のタイプの個人ドキュメントを使用することをお勧めします。

13. 顧客検証に使用する名前を選択します。

請求情報や連絡先情報にインドの住所が関連付けられている場合、その名前が選択肢として表示されます。選択した名前が、顧客検証に使用する予定のドキュメントタイプに記載された名前と一致していることを確認してください。請求先または連絡先の住所に関連付けられている名前を変更する必要がある場合は、アカウントのサインアップを完了した後に変更できます。

14. 検証のために情報を提出することに同意し、[続行] をクリックします。

アカウントのサインアップが完了すると、顧客検証の結果が E メールで通知されます。また、アカウント設定の顧客検証ページまたは後で AWS ヘルスダッシュボードでステータスを確認することもできます。AWS サービスにアクセスするには、顧客検証に合格する必要があります。

15. 携帯電話番号の検証方法として、[テキストメッセージ (SMS)] または [音声通話] のいずれかを選択します。
16. 国とリージョンコードを選択し、携帯電話番号を入力します。
17. セキュリティチェックを完了してください。
18. [SMS を送信] または [今すぐ電話する] を選択します。しばらくすると、携帯電話に SMS または自動通話で 4 桁の PIN が届きます。
19. [本人確認] ページで、受け取った PIN を入力し、[続行] を選択します。
20. [サポートプランの選択] ページでサポートプランを選択し、[サインアップを完了] を選択します。支払い方法と顧客検証が検証されると、アカウントがアクティブ化され、アカウントのアクティブ化を確認する E メールが送信されます。

Note

顧客検証の完了後に、以前に本人確認に使用した名前、住所、またはドキュメントを編集する場合は、再度顧客検証を更新して完了する必要がある場合があります。詳細については、「[the section called “顧客検証情報の編集”](#)」を参照してください。

顧客検証情報の管理

インドのコンピュータ緊急対応チーム (CERT-In) の規制に従い、AWS は AWS、サービスへの新規または継続的なアクセスを許可する前に、ID 情報を収集して検証する必要があります。入力したインドの請求先住所または連絡先住所に記載されている名前を使用して本人確認を行う必要があります。検証中、AWS はドキュメント番号が有効かどうか、および指定した名前が顧客検証に使用するドキュメントに関連付けられた名前と一致するかどうかを確認します。連絡先情報または請求情報から選択した名前は、ドキュメントに記載されている名前と完全に一致する必要があります。

請求名と住所を更新するには、「[お支払いの詳細設定](#)」ページを参照してください。連絡先の名前と住所を更新するには、「[the section called “のプライマリ連絡先を更新する AWS アカウント”](#)」を参照してください。請求先情報や連絡先情報の名前やインドの住所など、以前に顧客検証に使用した情報を編集する場合、顧客検証情報を更新して再提出する必要がある場合があります。

顧客検証ステータスの確認

顧客検証ステータスは、いつでも [顧客検証] ページで確認できます。検証ステータスが [検証が必要です] または [検証に失敗しました] の場合は、顧客検証情報を作成または更新して、検証のために提出してください。

管理アカウントが顧客検証の継承を有効にしている場合、アカウントの検証ステータスはそのアカウントのステータスを反映します。継承がアクティブなときにアクションを実行する必要はありません。

顧客検証情報の作成

顧客検証を完了するには、承認済みのインドのドキュメントからの情報を提供する必要があります。受け入れられたドキュメントタイプのリストについては、「[the section called “顧客確認用にインドで受け入れられるドキュメント”](#)」を参照してください。

1. [AWS マネジメントコンソール](#) にサインインします。
2. 右上隅のナビゲーションバーで、アカウント名 (またはエイリアス) を選択し、[アカウント] を選択します。
3. [その他の設定] で [顧客確認] を選択します。

以前に顧客検証情報を提供していない場合は、[お客様の本人確認情報を作成] ページが表示されます。

4. 顧客検証に使用する予定のドキュメントに記載された名前と正確に一致する名前を選択します。例えば、設立証明証を使用してビジネスアカウントを確認する予定の場合は、そのドキュメントに記載されている事業名を提供する必要があります。
5. このページでリクエストされている残りの情報を入力します。選択したドキュメントタイプによっては、ドキュメントの表面と裏面の両方のコピーをアップロードする必要がある場合があります。画像ファイルをアップロードする場合は、ドキュメント内のすべての情報が認識でき、判読可能であることを確認してください。
6. [Submit] を選択してください。

顧客検証の結果と次のステップについては、E メールまたは AWS Health Dashboard で通知されます。

顧客検証情報の編集

アカウント登録の主な目的や組織タイプ、および検証に使用する名前、ドキュメントタイプ、ドキュメントアップロード、またはドキュメント情報など、顧客検証情報を編集できます。

顧客検証に使用する名前またはドキュメントタイプを編集したり、ドキュメント情報を更新したりする場合は、変更を保存するときに ID を再度確認する必要があります。

検証継承がアクティブ

管理アカウントで顧客検証の継承が有効になっている場合、独自の顧客検証情報を編集または送信することはできません。検証情報が読み取り専用モードで表示されます。

1. [AWS マネジメントコンソール](#) にサインインします。
2. 右上隅のナビゲーションバーで、アカウント名 (またはエイリアス) を選択し、[アカウント] を選択します。
3. [その他の設定] で [顧客確認] を選択します。
4. [編集] を選択し、変更する情報を更新します。

情報を更新する際には、次のガイダンスに注意してください。

- 別の名前を選択する場合、その名前は顧客検証に使用する予定のドキュメントに記載されている名前と完全に一致する必要があります。例えば、設立証明証を使用してビジネスアカウントを確認する予定の場合は、そのドキュメントに記載されている事業名を提供する必要があります。
- 別のドキュメントタイプを選択する場合は、ドキュメントの表面と裏面 (該当する場合) のコピーをアップロードする必要があります。ドキュメントアップロードに含まれるすべての情報が認識でき、判読可能である必要があります。
- 個人アカウントを持っており、インド連邦による発行ではない運転免許証を使用する予定の場合は、検証用に別のタイプの個人ドキュメントを使用することをお勧めします。

受け入れられたドキュメントタイプのリストについては、「[the section called “顧客確認用にインドで受け入れられるドキュメント”](#)」を参照してください。

5. [Submit] を選択してください。

保存した変更のタイプによって再度本人確認を行う必要がある場合は、顧客検証の結果と次の手順が E メールで通知されます。また、顧客検証ページに戻るか、AWS ヘルスダッシュボードで結果を表示することもできます。

AWS Organizations の顧客検証継承を管理する

[AWS Organizations](#) を使用すると、組織の顧客検証継承を有効にできます。継承を有効にすると、組織内のインドベースのメンバーアカウントが管理アカウントの検証ステータスを継承します。顧客検証を個別に完了する必要はありません。

管理アカウントは、継承を有効にする前に、独自の顧客検証を完了する必要があります。継承を有効にした後、検証ドキュメントを再送信する必要はありません。

管理アカウントが顧客検証の継承を有効にすると、検証ステータスは組織内のインドベースのメンバーアカウントに拡張されます。これらのメンバーアカウントでは、法執行機関または規制のリクエストに応じて、お客様の検証情報を使用または開示することがあります。

顧客検証の継承を有効または無効にする

以下の手順に従って、組織のインドベースのメンバーアカウントの顧客検証継承を有効または無効にします。

1. AWS マネジメントコンソール で を開きます[AWS マネジメントコンソール](#)。
2. ナビゲーションバーで、アカウント名 (またはエイリアス) を選択し、アカウントを選択します。
3. [その他の設定] で [顧客確認] を選択します。
4. 顧客検証設定で、継承を有効にするには継承の切り替えをオンにし、無効にするにはオフにします。
5. 確認ダイアログボックスを確認し、選択を確認します。

継承を有効にすると、組織内のすべてのインドベースのメンバーアカウントが検証ステータスを継承します。継承を無効にすると、以前に独自の検証を完了したメンバーアカウントの以前の検証ステータスが復元されます。事前検証のないメンバーアカウントは、顧客検証を個別に完了する必要があります。

AWS Organizations メンバーアカウントの顧客検証

アカウントにインドベースの連絡先または請求先住所がある場合は、管理アカウントの検証ステータスを継承します。これは、管理アカウントが顧客検証の継承を有効にしている場合に適用されます。これを確認するメッセージが顧客検証ページに表示されます。

継承がアクティブな場合、独自の顧客検証情報を送信または編集することはできません。アクションを実行する必要はありません。

管理アカウントで継承が無効になっている場合は、独自の顧客検証ステータスが必要です。アカウントが組織を離れるか、管理アカウントが組織からアカウントを削除する場合も同様です。以前に独自の検証情報を送信した場合は、以前の検証ステータスが復元されます。このプロセスを繰り返す必要はありません。この復元は、以前の検証以降に名前と住所が変更されていない場合にのみ適用されます。

顧客確認用にインドで受け入れられるドキュメント

インド政府が発行した以下の種類のドキュメントを顧客確認に使用できます。

Note

以下のリンクは、政府によって変更される可能性があります。

- **PAN カード** - 納税者番号 (PAN) カードは、デジタルと物理の両方の形式で提供されており、個人、企業、および団体に対してインドの所得税局が発行する一意の英数字識別子が含まれています。PAN は、文字と数字を含む 10 文字の形式 (**AAAAA1111A**) で構成されます。このドキュメントを検証に使用する場合は、PAN ドキュメントに記載されている生年月日 (個人の場合) または法人設立日 (ビジネスの場合) も入力し、カードの表面をアップロードする必要があります。PAN の有効性を確認するには、[所得税局の公式ウェブサイト](#)にアクセスしてください。
- **有権者 ID カード/EPIC** - 有権者 ID カードは写真付き選挙人 ID カード (EPIC) と呼ばれ、インド選挙委員会によってインドの適格な有権者に発行される一意の識別番号が含まれています。有権者 ID/EPIC 番号は、文字と数字を含む 10 文字で構成されます。[インド選挙委員会](#)の公式ウェブサイト にアクセスして、投票者 ID の有効性を確認できます。このドキュメントを検証に使用するには、カードの表面と裏面の両方をアップロードする必要があります。
- **運転免許証** - 運転免許証がインド連邦によって発行されたものではない場合は、検証に別のドキュメントタイプを使用することをお勧めします。運転免許証番号は、文字、数字、スペース、ハイフンを含む 12~16 文字で構成されます。このドキュメントを検証に使用するには、生年月日を入力

し、カードの表面と裏面の両方をアップロードする必要があります。運転免許証の有効性を確認するには、道路交通省の [Parivahan Sewa のサイト](#) にアクセスしてください。

- 設立証明証 - 設立証明書は、企業省 (MCA) によって発行されるドキュメントであり、企業が法人として登録された日付を示します。この証明書は、インドで登録されている企業を一意に識別し、追跡するために使用されます。各証明書には企業識別番号 (CIN) が含まれています。これは、文字と数字を含む 21 文字で構成される一意の英数字識別子です。このドキュメントを検証に使用するには、設立証明書ドキュメントをアップロードする必要があります。CIN の有効性を確認するには、[企業省のポータル](#) にアクセスしてください。

個人アカウントとビジネスアカウントでは、インドのさまざまなドキュメントタイプが受け入れられます。

- 個人アカウントの場合 - PAN カード、有権者 ID カード/EPIC、運転免許証。
- ビジネスアカウントの場合 - PAN カードと設立証明書。

AWS India アカウントを管理する

以下のタスクを除き、アカウントを管理する手順は、インド国外で作成されたアカウントと同じです。アカウントの管理に関する一般情報については、「[the section called “アカウントの設定”](#)」を参照してください。

を使用して、次のタスク AWS マネジメントコンソール を実行します。

- [納税者番号の追加または編集](#)
- [複数の納税者番号の編集](#)
- [the section called “顧客検証情報の管理”](#)
- [複数の物品サービス税 \(GST\) 番号の編集](#)
- [税金請求書の表示](#)

を閉じる AWS アカウント

これらの手順は、サインアップ for AWS (アドバンスド) AWS の使用にサインアップ AWS アカウントした場合、またはアカウントの高度な機能をアクティブ化した場合に、を閉じる方法を示しています。サインアップオプションを比較するには、「」を参照してください [サインアップオプションを比較する](#)。

が不要になった場合は AWS アカウント、このセクションの手順に従っていつでも閉じることができます。アカウントを閉鎖した後は 90 日以内であれば、アカウントを再開できます。アカウントを閉鎖した AWS 日からアカウントを完全に閉鎖するまでの期間は、[閉鎖後期間](#)と呼ばれます。

アカウントを閉鎖する前の確認事項

を閉じる前に AWS アカウント、次の点を考慮する必要があります。

- アカウントの閉鎖は、そのアカウントに関する AWS 顧客契約終了の通知として扱われます。
- を閉じる AWS アカウント 前に リソースを削除する必要はありません。ただし、保持する必要があるリソースやデータをバックアップすることをお勧めします。特定のリソースをバックアップする方法については、そのサービスに該当する [AWS ドキュメント](#)を参照してください。
- [閉鎖後期間](#)中であれば、アカウントを再開できます。アカウントを再開すると、アカウント内に残っているサービスに対する課金も再開されます。また、未払いの請求書や未処理の[リザーブドインスタンス](#)および [Savings Plans](#) についても引き続き責任を負います。
- アカウント閉鎖前に消費されたサービスに対するすべての未処理の料金および請求額については、引き続き責任を負います。アカウントを閉鎖した翌月に AWS 請求書が届きます。例えば、1 月 15 日にアカウントを閉鎖した場合、1 月 1 日から 1 月 15 日までに発生した使用量に対する請求書が 2 月初旬に届きます。[リザーブドインスタンス](#)と [Savings Plans](#) の請求書は、アカウントを閉鎖した後も引き続き有効期限が切れるまで届きます。
- アカウントで以前に利用可能だった AWS サービスにアクセスできなくなります。ただし、解約 AWS アカウント 後期間中にサインインして解約された にアクセスできるのは、過去の請求情報を表示したり、アカウント設定にアクセスしたり、 に連絡したりするためのみです[AWS サポート](#)。 ???
- AWS アカウント の閉鎖時にそのアカウントに登録されていたのと同じ E メールアドレスを、別の AWS アカウントの主要 E メールアドレスとして使用することはできません。同じ E メールアドレスを別の AWS アカウントで使いたい場合は、閉鎖前に更新することをお勧めします。詳細については、「[ルートユーザーの E メールアドレスとの更新](#)」を参照してください。
- 別のアカウントの閉鎖 AWS アカウント 時に に登録したのと同じアカウントエイリアスを使用することはできません AWS アカウント。別の のエイリアスを再利用するには AWS アカウント、アカウントを閉じる前にアカウントエイリアスを削除します。詳細については、IAM [ユーザーガイドの AWS アカウント ID のエイリアス](#)の使用を参照してください。
- AWS アカウント のルートユーザーで[多要素認証 \(MFA\) を有効にしている](#)場合、または [IAM ユーザーに MFA デバイス](#)を設定している場合は、アカウントを閉鎖しても MFA は自動的に削除されません。90 日間の[閉鎖後期間](#)中に MFA をオンのままにする場合は、その期間中にアカウントにアクセスする必要がある場合に備えて、閉鎖後期間が終了するまで MFA デバイスをアクティブに

しておいてください。ハードウェア TOTP トークンデバイスは、アカウントが完全に閉鎖された後に別のユーザーに関連付けることはできないので注意してください。ハードウェア TOTP トークンを後で別のユーザーで使用する場合は、アカウントを閉鎖する前に[ハードウェア MFA デバイスを無効にする](#)オプションがあります。[IAM ユーザー](#)の MFA デバイスは、アカウント管理者が削除する必要があります。

メンバーアカウントに関するその他の考慮事項

- メンバーアカウントを閉鎖しても、そのアカウントは、[閉鎖後期間](#)が終了するまでは組織から削除されません。閉鎖後期間中、閉鎖したメンバーアカウントは、引き続き組織内のアカウントのクォータに対してカウントされます。アカウントがクォータにカウントされないようにするには、そのアカウントを閉鎖する前に「[組織からのメンバーアカウントの削除](#)」を参照してください。
- メンバーアカウントの 20% または 250 件のみを、30 日間のローリング期間中に最大 1,000 件まで解約できます。このクォータは暦月に縛られず、アカウントを閉鎖した時点で開始されます。Organizations のクォータの詳細については、「[AWS Organizations のクォータ](#)」を参照してください。
- AWS Control Tower を使用する場合は、アカウントを閉鎖する前にメンバーアカウントの管理を解除する必要があります。「AWS Control Tower ユーザーガイド」の「[メンバーアカウントの管理を解除する](#)」を参照してください。

サービス固有の考慮事項

- AWS Marketplace サブスクリプションは、アカウント閉鎖時に自動的にキャンセルされません。何らかのサブスクリプションがある場合は、まずサブスクリプション内の[ソフトウェアのすべてのインスタンスを終了します](#)。次に、AWS Marketplace コンソールの[サブスクリプションの管理](#)ページに移動し、サブスクリプションをキャンセルします。
- アカウントが閉鎖されると、AWS はドメインを停止するまで最大 5 日間毎日 E メールを送信します。ドメインが停止されたら、ドメインのレジストラに応じて、30 日以内にドメインを削除するか、そのレジストラにドメインを解放します。詳細については、「[My AWS アカウント is closed or permanently closed](#)」および「[My domain is registered with Route 53](#)」を参照してください。

このアカウントのルートユーザーの E メールアドレスがこの同じアカウントの Route 53 を介して登録されたドメインを使用している場合は、次のいずれかのアクションを完了するまで、このアカウントを閉じないでください。ドメインを別の に移管するか AWS アカウント、このアカウントに登録されていないドメインを使用するようにルートユーザーの E メールアドレスを更新しま

す。それ以外の場合、アカウントを閉じるとドメインが停止され、ルートユーザーアドレスへの E メール配信が中断されます。E メールがない場合、アカウントを復元することはできません。また、アカウントがない場合、ドメインを復元することはできません。30 日後、Route 53 はドメインを完全に削除します。これは、ルートユーザーの E メールアドレスがこのアカウントに登録されたドメインを使用するメンバーアカウントにも適用されます。

- AWS CloudTrail は基本的なセキュリティサービスです。つまり、ユーザーが作成した証跡は、ユーザーが閉じる AWS アカウント 前に の証跡を明示的に削除しない限り、AWS アカウント が閉じられた後も引き続き存在し、イベントを配信できます。AWS アカウント が閉じられた後に証跡の削除をリクエストする方法の詳細については、CloudTrail ユーザーガイド」の[AWS アカウント「クロージャと証跡」](#)を参照してください。

アカウントの閉鎖方法

次の手順 AWS アカウント を使用して を閉じることができます。閉鎖するアカウント [スタンドアロン、メンバー、管理、AWS GovCloud (US)] のタイプに応じて、各タブに異なるガイダンスが提供されることに注意してください。

アカウントの閉鎖プロセス中に問題が発生した場合は、「[AWS アカウント 閉鎖に関する問題のトラブルシューティング](#)」を参照してください。

Standalone account

スタンドアロンアカウントは、 の一部ではない個別に管理されるアカウントです AWS Organizations。

[アカウント] ページからスタンドアロンアカウントを閉鎖する手順

1. 閉じる [のルートユーザー AWS マネジメントコンソール として にサインイン](#) AWS アカウント します。IAM ユーザーまたはロールとしてサインインしている間は、アカウントを閉鎖できません。
2. 右上隅のナビゲーションバーでアカウント名または番号を選択し、[アカウント] を選択します。
3. [\[アカウント\] ページ](#)で、[アカウントを閉鎖] ボタンを選択します。
4. アカウント ID (閉鎖ダイアログボックスの上部に表示される) を入力して、アカウント閉鎖プロセスを読んで理解したことを確認します。
5. [アカウントを閉鎖] ボタンを選択して、アカウント閉鎖プロセスを開始します。
6. 数分以内に、アカウントが閉鎖されたことを確認する E メールが届きます。

Note

このタスクは、AWS CLI またはいずれかの AWS SDKs からの API オペレーションではサポートされていません。このタスクは、を使用してのみ実行できます AWS マネジメントコンソール。

Member account

メンバーアカウントは、の一部 AWS アカウント である です AWS Organizations。

AWS Organizations コンソールからメンバーアカウントを閉じるには

1. [AWS Organizations コンソール](#) にサインインします。
2. [AWS アカウント] ページで、閉鎖するメンバーアカウント名を探し、選択します。OU の階層を移動するか、OU 構造のないアカウントのフラットリストを表示できます。
3. ページ上部のアカウント名の横にあるアカウントを閉じるを選択します。このオプションは、AWS 組織が[すべての機能](#)モードの場合にのみ使用できます。

Note

組織が[一括請求](#)モードを使用している場合、コンソールでアカウントを閉じるボタンを表示することはできません。一括請求モードでアカウントを閉鎖するには、ルートユーザーとして閉鎖するアカウントにサインインします。[アカウント] ページで、[アカウントの閉鎖] ボタンを選択し、アカウント ID を入力し、[アカウントの閉鎖]ボタンを選択します。

4. アカウント閉鎖ガイダンスを読んで、理解していることを確認します。
5. メンバーアカウント ID を入力し、[アカウントを閉鎖] を選択してアカウント閉鎖プロセスを開始します。

Note

閉鎖したメンバーアカウントは、最初の閉鎖日から最大 90 日間、AWS Organizations コンソールでアカウント名の横に CLOSED というラベルが表示されます。90 日後、そのメンバーアカウントは AWS Organizations コンソールに表示されなくなります。

アカウントページからメンバーアカウントを閉じるには

必要に応じて、 のアカウントページから直接 AWS メンバーアカウントを閉鎖できます AWS マネジメントコンソール。ステップバイステップのガイダンスについては、[スタンドアロンアカウント] タブの手順に従ってください。

このオプションは、ルートユーザーを持たないプロジェクトアカウントでは使用できません。コンソールからプロジェクトアカウントを閉じます AWS Organizations 。

AWS CLI および SDKs

AWS CLI および SDKs [「組織内のメンバーアカウントの閉鎖」](#) を参照してください。 AWS Organizations

Management account

管理アカウントは AWS アカウント 、 親アカウントまたはルートアカウントとして機能する です AWS Organizations。

 Note

AWS Organizations コンソールから直接管理アカウントを閉鎖することはできません。

[アカウント] ページから管理アカウントを閉鎖する手順

1. 閉鎖する管理アカウントの [ルートユーザー AWS マネジメントコンソール として にサインイン](#) します。IAM ユーザーまたはロールとしてサインインしている間は、アカウントを閉鎖できません。
2. 組織内にアクティブなメンバーアカウントが残っていないことを確認します。これを行うには、 [AWS Organizations コンソール](#) に移動し、すべてのメンバーアカウントのアカウント名の横に Closed が表示されていることを確認します。まだアクティブなメンバーアカウントがある場合は、[メンバーアカウント] タブに示されるアカウント閉鎖ガイダンスを実行してから、次のステップに進んでください。
3. 右上隅のナビゲーションバーでアカウント名または番号を選択し、[アカウント] を選択します。
4. [\[アカウント\] ページ](#) で、[アカウントを閉鎖] ボタンを選択します。
5. アカウント ID (閉鎖ダイアログボックスの上部に表示される) を入力して、アカウント閉鎖プロセスを読んで理解したことを確認します。

6. [アカウントを閉鎖] ボタンを選択して、アカウント閉鎖プロセスを開始します。
7. 数分以内に、アカウントが閉鎖されたことを確認する E メールが届きます。

 Note

このタスクは、AWS CLI またはいずれかの AWS SDKs からの API オペレーションではサポートされていません。このタスクは、を使用してのみ実行できます AWS マネジメントコンソール。

AWS GovCloud (US) account

AWS GovCloud (US) アカウントは、請求と支払い AWS アカウント の目的で常に 1 つの標準にリンクされます。

AWS GovCloud (US) アカウントを閉鎖するには

AWS GovCloud (US) アカウントにリンク AWS アカウント された がある場合は、アカウントを閉じる前に標準アカウントを閉じる AWS GovCloud (US) 必要があります。データのバックアップ方法や意図しない AWS GovCloud (US) 請求を回避する方法などの詳細については、AWS GovCloud (US) 「ユーザーガイド」の [AWS GovCloud \(US\) 「アカウントの閉鎖」](#) を参照してください。

アカウントの閉鎖後に予想されること

アカウントを閉鎖するとすぐに、次のことが発生します。

- アカウントの閉鎖を確認する E メールが、ルートユーザーの E メールアドレスに届きます。この E メールが数時間以内に届かない場合は、「[AWS アカウント 閉鎖に関する問題のトラブルシューティング](#)」を参照してください。
- 閉鎖したメンバーアカウントは、元の閉鎖日から最大 90 日間、そのアカウント名の横にCLOSEDラベルを AWS Organizations コンソールに表示します。90 日後、メンバーアカウントは AWS Organizations コンソールに表示されなくなります。
- の サービスにアクセスするためのアクセス許可 AWS アカウント を他の アカウントに付与している場合、それらのアカウントから行われたアクセスリクエストは、アカウント閉鎖後に失敗します。を再度開くと AWS アカウント、必要なアクセス許可を付与すると、他の AWS アカウント はアカウントの AWS サービスとリソースに再びアクセスできます。

アカウント閉鎖は、すべてのリージョンとサービスですぐに発生するわけではなく、完了までに数時間かかる場合があります。

閉鎖後期間

閉鎖後期間は、アカウントを閉鎖した日から AWS が完全に閉鎖されるまでの期間を指します AWS アカウント。閉鎖後期間は 90 日間です。閉鎖後期間中は、アカウントを再開することによってのみ、コンテンツや AWS サービスにアクセスできます。閉鎖後期間が過ぎると、AWS は完全に閉じ AWS アカウント、再度開くことはできなくなります。AWS はアカウント内のコンテンツとリソースも削除します (CloudTrail 証跡を除く)。アカウントが完全に閉鎖されると、その [AWS アカウント ID](#) は再使用できなくなります。

の再開 AWS アカウント

アカウントは 90 日後に完全に閉鎖され、その後はアカウントを再度開くことができなくなり、アカウントに残っているコンテンツ AWS が削除されます。アカウントが完全に閉鎖される前にアカウントを再開するには、「」を参照してください [を再開する AWS アカウント](#)。

Note

アカウントを再開すると、アカウント内に残っているサービスに対する課金も再開されます。

を再開する AWS アカウント

を閉鎖 AWS アカウント し、残高がない場合は、[閉鎖後](#)期間中に自分で再開できます。

ルートユーザーとしてサインインし、アカウントページからリクエストを送信して、アカウントを再開します。

アカウントを再開する前に知っておくべきこと

を再開する前に AWS アカウント、次の点に注意してください。

- セルフサービス要件: このセルフサービスプロセスは、アカウントを自分で閉鎖し、アカウント閉鎖時に残高がない場合にのみ使用できます。閉鎖されたアカウントのルートユーザーとしてサインインする必要があります。IAM ユーザーまたはロールとしてサインインしている間は、アカウント

トを再度開くことはできません。アカウントを閉鎖してから 90 日以内に、閉鎖後期間中に再開リクエストを送信する必要があります。

- アカウント閉鎖者 AWS: アカウントを AWS 閉鎖した場合、自分で再開することはできません。アカウントが閉鎖されてから 30 日以内に残高を支払い、[AWS サポート](#)に連絡してアカウントを再開します。
- 支払いと料金: アカウントには有効期限が切れていない有効な支払い方法が必要です。前月の請求書は翌月の初めに確定されるため、アカウントが解約時に残高がない場合でも、解約前の使用量に対して残高がある可能性があります。残高を確認または支払うには、「[支払いを行う](#)」を参照してください。アカウントを再開すると、そのアカウントで実行されているサービスに対して料金が再開されます。アカウントを閉鎖する前にこれらのサービスを停止しなかった場合は、閉鎖後期間にも料金が発生する可能性があります。

アカウントを再開する方法

閉鎖したアカウントを再開するには、次の手順に従います。

Note

このタスクは、AWS CLI またはいずれかの AWS SDKs からの API オペレーションではサポートされていません。このタスクは、[AWS マネジメントコンソール](#)を使用してのみ実行できます。

アカウントページからアカウントを再開するには

1. 再開するクローズ AWS アカウント したの [ルートユーザー AWS マネジメントコンソールとしてサインイン](#)します。IAM ユーザーまたはロールとしてサインインしている間は、アカウントを再度開くことはできません。
2. 次のように、閉鎖されたアカウントのアカウントページを開きます。閉鎖されたアカウントのバナーで、アカウントを再開を選択します。
3. アカウントを再開ダイアログボックスで、ダイアログボックスに表示されるアカウント ID を入力して、アカウントを再開することを確認します。
4. アカウントを再開を選択してリクエストを送信します。アカウントの再開が開始されたことを確認するメッセージが表示されます。
5. 再開が完了するまで待ちます。アカウントが再びアクティブになると、アカウントが正常に再開され、AWS サービスと請求が復元されたことを確認するメッセージが表示されます。

がアカウントを再開 AWS できない場合、解決の理由と方法を説明するコンソール通知が送信されます。

アカウントを再開した後の予定

再開リクエストを送信すると、以下が発生します。

- ステータスを確認するには、アカウントページを更新します。再開が完了すると、アカウントはアクティブと表示され、クローズドアカウントバナーは表示されなくなります。
- アカウントがアクティブになると、 はサービスとリソースへのアクセスを AWS 復元し、請求を再開します。

再開後にアカウントを使用する準備をする

一部のリソースとサブスクリプションは、自動的に実行状態に復元されません。アカウントが再開されたら、通常のオペレーションを再開する前に、次の操作を行う必要がある場合があります。

- アカウントの閉鎖時に停止された Amazon EC2 インスタンスを起動します。詳細については、Amazon EC2 [ユーザーガイド](#)の「[インスタンスの開始](#)」を参照してください。
- アカウント閉鎖時に作成されたスナップショットから Amazon RDS データベースを復元します。
- AWS Marketplace サブスクリプションをキャンセルして再サブスクライブします。サブスクリプションは、アカウントの再開時に自動的に復元されません。

リージョンの可用性

セルフサービスアカウントの再開は、すべての商用リージョンで利用できます。

AWS アカウント管理のセキュリティ

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。

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があります AWS クラウド。AWS また、では、安全に使用できるサービスも提供しています。サードパーティーの監査者は、[AWS コンプライアンスプログラム](#)コンプライアンスプログラムの一環として、当社のセキュリティの有効性を定期的にテストおよび検証。アカウント管理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 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コンプライアンスプログラムによる対象範囲内」](#)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、ユーザーは、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

責任共有モデルはすべてのに適用されます AWS アカウント。これには、新しい AWS エクスペリエンスを使用して AWS アカウント を作成し、高度な AWS エクスペリエンスを使用して作成するアカウントが含まれます。

このドキュメントは、AWS アカウント管理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。セキュリティおよびコンプライアンス上の目的に合わせてアカウント管理を設定する方法について説明します。また、アカウント管理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。このドキュメントの一部は、当社の高度な AWS エクスペリエンスで作成されたアカウントにのみ関連しています。ドキュメントが当社の高度な AWS エクスペリエンスで作成されたアカウントにのみ関係するタイミングを特定します。

トピック

- [AWS アカウント管理でのデータ保護](#)
- [AWS PrivateLink AWS アカウント管理用](#)
- [AWS アカウント管理の Identity and Access Management](#)
- [AWS AWS アカウント管理の 管理ポリシー](#)
- [AWS アカウント管理のコンプライアンス検証](#)
- [AWS アカウント管理の耐障害性](#)

- [のインフラストラクチャセキュリティ AWS アカウント管理](#)

AWS アカウント管理でのデータ保護

以下の情報は、すべてのに関連しています AWS アカウント。

責任 AWS [共有モデル](#)、AWS アカウント管理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、AWS CLI または SDK を使用してアカウント管理または他の 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 PrivateLink AWS アカウント管理用

以下の情報は、すべての [AWS アカウント](#) に関連しています。

Amazon Virtual Private Cloud (Amazon VPC) を使用して AWS リソースをホストする場合、パブリックインターネットを経由することなく、VPC 内から AWS アカウント管理サービスにアクセスできます。

Amazon VPC では、カスタム仮想ネットワークで AWS リソースを起動できます。VPC を使用して、IP アドレス範囲、サブネット、ルートテーブル、ネットワークゲートウェイなどのネットワーク設定を制御できます。VPC の詳細については、[Amazon VPC ユーザーガイド](#)を参照してください。

Amazon VPC をアカウント管理に接続するには、まずインターフェイス VPC エンドポイントを定義する必要があり、そうすることで VPC を他の AWS サービスに接続できます。このエンドポイントを使用すると、インターネットゲートウェイやネットワークアドレス変換 (NAT) インスタンス、または VPN 接続などを必要とせずに、信頼性の高いスケーラブルな方法で接続できるようになります。詳細については、「Amazon VPC ユーザーガイド」の「[インターフェイス VPC エンドポイント \(AWS PrivateLink\)](#)」を参照してください。

エンドポイントを作成する

VPC で AWS アカウント管理エンドポイントを作成するには AWS マネジメントコンソール、AWS Command Line Interface、(AWS CLI)、AWS SDK、AWS アカウント管理 API、または [CloudFormation](#) を使用します。

Amazon VPC コンソールまたは [AWS CLI](#) を使用してエンドポイントを作成および設定する方法については「Amazon VPC ユーザーガイド」の「[インターフェイスエンドポイントの作成](#)」を参照してください。

Note

エンドポイントを作成する際に、VPC の接続先になるサービスとして、以下の形式でアカウント管理を指定します。

```
com.amazonaws.us-east-1.account
```

us-east-1 リージョンを指定する文字列を表示されているとおり正確に使用する必要があります。グローバルサービスとして、アカウント管理は 1 つの AWS リージョンでのみホストされます。

を使用してエンドポイントを作成および設定する方法については CloudFormation、「CloudFormation ユーザーガイド」の[AWS::EC2::VPCEndpoint](#) リソース」を参照してください。

Amazon VPC エンドポイントポリシー

Amazon VPC エンドポイントの作成時にエンドポイントポリシーをアタッチすることで、このサービスエンドポイントで実行できるアクションを制御できます。複数のエンドポイントポリシーをアタッチすることで、複雑な IAM ルールを作成できます。詳細については、「」を参照してください。

- [アカウント管理用の Amazon Virtual Private Cloud エンドポイントポリシー](#)
- AWS PrivateLink ガイドの「[VPC エンドポイントによるサービスへのアクセスのコントロール](#)」

アカウント管理用の Amazon Virtual Private Cloud エンドポイントポリシー

以下の情報は、すべてのに関連しています AWS アカウント。

Amazon SNS の Amazon VPC エンドポイントに対するポリシーを作成して、以下を指定することができます。

- アクションを実行できるプリンシパル。
- プリンシパルが実行できるアクション。
- このアクションを実行できるリソース。

次の例は、アカウント 123456789012 の Alice という名前の 1 人の IAM ユーザーに任意の代替連絡先情報の取得と変更の両方を許可するが AWS アカウント、任意のアカウントの代替連絡先情報を削除するアクセス許可をすべての IAM ユーザーに拒否する Amazon VPC エンドポイントポリシーを示しています。

Organization の一部であるアカウントへのアクセス権を AWS 組織のメンバーアカウントの 1 つにあるプリンシパルに付与する場合、Resource 要素は次の形式を使用する必要があります。

```
arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
```

エンドポイントポリシーの作成方法の詳細については、AWS PrivateLink ガイドの「[VPC エンドポイントによるサービスへのアクセスのコントロール](#)」を参照してください。

AWS アカウント管理の Identity and Access Management

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、誰に請求情報とコスト管理リソースの使用を認可する (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。

以下の情報は、AWS アカウント管理の Identity and Access Management に関する情報です。この情報は、高度な AWS エクスペリエンスを使用するとき、またはアカウントの高度な機能をアクティブ化したときに AWS アカウント 作成する に最も関連します。新しい AWS エクスペリエンスでのアクセスコントロールの仕組みについては、「」を参照してください [アクセス管理を比較する](#)。

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 アカウント管理と IAM の連携方法](#)
- [AWS アカウント管理のアイデンティティベースのポリシーの例](#)
- [AWS アカウント管理にアイデンティティベースのポリシー \(IAM ポリシー\) を使用する](#)
- [AWS アカウント管理の ID とアクセスのトラブルシューティング](#)

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 アカウント管理の 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 (「[AWS アカウント管理と IAM の連携方法](#)」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 (「[AWS アカウント管理のアイデンティティベースのポリシーの例](#)」を参照)

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、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 ルート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、アイデンティティ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。

AWS アカウント管理と IAM の連携方法

この情報は、高度な AWS エクスペリエンスを使用する際に AWS アカウント 作成する に最も関連しています。新しい AWS エクスペリエンスでのアクセスコントロールの仕組みについては、「」を参照してください[アクセス管理を比較する](#)。

IAM を使用してアカウント管理へのアクセスを管理する前に、アカウント管理で利用できる IAM の機能について学習します。

AWS アカウント管理で利用できる IAM 機能

IAM 機能	アカウント管理のサポート
ID 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	あり
ポリシー条件キー	あり
ACL	なし
ABAC (ポリシー内のタグ)	いいえ
一時的な認証情報	あり

IAM 機能	アカウント管理のサポート
プリンシパルアクセス権限	あり
サービスロール	いいえ
サービスリンクロール	いいえ

アカウント管理およびその他の 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。

アカウント管理の 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 ポリシーで使用す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。

アカウント管理 ID ベースのポリシーの例

アカウント管理 ID ベースのポリシーの例は、「[AWS アカウント管理のアイデンティティベースのポリシーの例](#)」でご確認ください。

アカウント管理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。

アカウント管理用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。

アカウント管理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 「アカウント管理で定義されるアクション」](#)を参照してください。

ネットワーク管理 のポリシーアクションは、アクションの前に、プレフィックス を使用します。

```
account
```

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": [  
    "account:action1",  
    "account: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、AWS アカウントの代替連絡先と連携す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": "account:*AlternateContact"
```

アカウント管理 ID ベースのポリシーの例は、「[AWS アカウント管理のアイデンティティベースのポリシーの例](#)」でご確認ください。

アカウント管理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": "*"
```

アカウント管理サービスは、IAM ポリシーの Resource 要素で次の特定のリソースタイプをサポートし、ポリシーをフィルタリングしてこれらのタイプを区別するのに役立ちます AWS アカウント。

- account

この resource タイプは、AWS Organizations サービスによって管理される組織内のメンバーアカウントではないスタンドアロン AWS アカウント のみに一致します。

- accountInOrganization

この resource タイプは、AWS Organizations サービスによって管理 AWS アカウント される組織のメンバーアカウントである のみに一致します。

アカウント管理リソースタイプとその ARNs [AWS 「アカウント管理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 「アカウント管理で定義されるアクション」](#) を参照してください。

アカウント管理 ID ベースのポリシーの例は、「[AWS アカウント管理のアイデンティティベースのポリシーの例](#)」でご確認ください。

アカウント管理用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。

アカウント管理サービスは、IAM ポリシーの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をサポートしています。

- account:TargetRegion

この条件キーは、次のリストで構成される引数を取ります。[AWS リージョンコード](#)。これにより、指定したリージョンに適用されるアクションのみに影響を与えるように、ポリシーをフィルタリングできます。

- account:AlternateContactTypes

この条件キーは、代替連絡先タイプのリストを取ります。

- 請求
- 操作
- SECURITY

このキーを使用すると、指定された代替連絡先タイプをターゲットとするアクションのみにリクエストをフィルタリングできます。

- account:AccountResourceOrgPaths

この条件キーは、組織の階層から特定の組織単位 (OU) へのパスのリストで構成される引数を取ります。これにより、一致する OU 内のターゲットアカウントのみに影響を与えるように、ポリシーをフィルタリングできます。

```
o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*
```

- account:AccountResourceOrgTags

この条件キーは、タグキーと値のリストで構成される引数を取ります。これにより、組織のメンバーであり、指定されたタグのキーと値でタグ付けされたアカウントのみに影響を与えるように、ポリシーをフィルタリングできます。

- `account:EmailTargetDomain`

この条件キーは、E メールドメインで構成される引数を取ります。これにより、指定した E メールドメインに一致するアクションのみに影響を与えるように、ポリシーをフィルタリングできます。この条件キーでは、大文字と小文字が区別されます。ターゲット E メールアドレスドメインに基づいてアクションを制御するには、ポリシーの条件ブロックで `StringEquals` の代わりに `StringEqualsIgnoreCase` を使用する必要があります。E メールドメインに `example.com`、`company.org`、または `EXAMPLE.COM` などの大文字と小文字の任意の組み合わせが含まれている場合に `account:StartPrimaryEmailUpdate` アクションを完了できるようにするポリシーの例を次に示します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowConditionKey",
      "Effect": "Allow",
      "Action": [
        "account:StartPrimaryEmailUpdate"
      ],
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "account:EmailTargetDomain": [
            "example.com",
            "company.org"
          ]
        }
      }
    }
  ]
}
```

アカウント管理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「アカウント管理の条件キー」](#) 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「アカウント管理で定義されるアクション」](#) を参照してください。

アカウント管理 ID ベースのポリシーの例は、「[AWS アカウント管理のアイデンティティベースのポリシーの例](#)」でご確認ください。

Account Management のアクセス制御リスト

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。

アカウント管理を使用した属性ベースのアクセスコントロール

ABAC (ポリシー内のタグ) のサポート: なし

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。では AWS、これらの属性はタグと呼ばれます。IAM エンティティ (ユーザーまたはロール) と多くの AWS リソースにタグをアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合にオペレーションを許可するように ABAC ポリシーをします。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

AWS アカウント管理では、タグベースのアクセスコントロールは `account:AccountResourceOrgTags/key-name` 条件キーを介してのみサポートされます。標準の `aws:ResourceTag/key-name` 条件キーは、アカウント名前空間の API ではサポートされていません。

サポートされている条件キーを使用した JSON ポリシーの例

次のポリシー例では、組織内のキー「CostCenter」と「12345」または「67890」の値でタグ付けされたアカウントの連絡先情報を表示するアクセスを許可します。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "account:GetContactInformation",
```

```
        "account:GetAlternateContact"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "account:AccountResourceOrgTags/CostCenter": [
                "12345",
                "67890"
            ]
        }
    }
}
]
```

ABAC の詳細については、[「IAM ユーザーガイド」の「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」](#)および[「IAM チュートリアル: タグに基づいて AWS リソースにアクセスするアクセス許可を定義する」](#)を参照してください。

アカウント管理で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。

アカウント管理のクロスサービスプリンシパル許可

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、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。

アカウント管理のサービスロール

サービスロールのサポート: なし

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。

アカウント管理用のサービスリンクロール

サービスにリンクされたロールのサポート: なし

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。

AWS アカウント管理のアイデンティティベースのポリシーの例

この情報は、高度な AWS エクスペリエンスを使用する際に AWS アカウント 作成する に最も関連しています。新しい AWS エクスペリエンスでのアクセスコントロールの仕組みについては、「」を参照してください [アクセス管理を比較する](#)。

デフォルトでは、ユーザーおよびロールにはアカウント管理リソースを作成または変更するアクセス許可がありません。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 ARNs [AWS 「アカウント管理のアクション、リソース、および条件キー」](#)を参照してください。

トピック

- [ポリシーに関するベストプラクティス](#)

- [のアカウントページの使用 AWS マネジメントコンソール](#)
- [のアカウントページへの読み取り専用アクセスを提供する AWS マネジメントコンソール](#)
- [のアカウントページへのフルアクセスの提供 AWS マネジメントコンソール](#)

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、アカウント内のアカウント管理リソースを誰かが作成、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。これらはで使えます 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。例えば、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 – 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。

のアカウントページの使用 AWS マネジメントコンソール

の [アカウントページ](#) にアクセスするには AWS マネジメントコンソール、最小限のアクセス許可が必要です。これらのアクセス許可により、 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厳しく制限されたアイデンティティベースポリシーを作成すると、そのポリシーを添付したエンティティ (IAM 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。

ユーザーとロールがアカウント管理コンソールを使用できるようにするには、AWSAccountManagementReadOnlyAccess または AWSAccountManagementFullAccess AWS 管理ポリシーをエンティティにアタッチすることを選択できます。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。

CLI または AWS API AWS 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、多くの場合、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を許可できます。

のアカウントページへの読み取り専用アクセスを提供する AWS マネジメントコンソール

次の例では、AWS アカウントの IAM ユーザーに、AWS マネジメントコンソールの [アカウント] ページへの読み取り専用アクセス権を付与します。このポリシーがアタッチされたユーザーは、変更を加えることはできません。

account:GetAccountInformation アクションは、[アカウント] ページのほとんどの設定を表示するためのアクセス権を付与します。ただし、現在有効になっている AWS リージョンを表示するには、account:ListRegions アクションも含めなければなりません。

JSON

```
{
  "Version": "2012-10-17",
```

```
    "Statement": [
      {
        "Sid": "GrantReadOnlyAccessToAccountSettings",
        "Effect": "Allow",
        "Action": [
          "account:GetAccountInformation",
          "account:ListRegions"
        ],
        "Resource": "*"
      }
    ]
  }
}
```

のアカウントページへのフルアクセスの提供 AWS マネジメントコンソール

次の例では、AWS アカウント の IAM ユーザーに AWS マネジメントコンソールの [アカウント] ページへのフルアクセス権を付与します。このポリシーがアタッチされたユーザーは、アカウントの設定を変更できます。

このポリシーの例は、前述のポリシーの例に、使用可能な書き込みアクセス許可 (CloseAccount を除く) をそれぞれ追加することで作成されており、account:EnableRegion および account:DisableRegion アクセス許可を含むほとんどのアカウント設定をユーザーが変更できるようにします。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GrantFullAccessToAccountSettings",
      "Effect": "Allow",
      "Action": [
        "account:GetAccountInformation",
        "account:ListRegions",
        "account:PutContactInformation",
        "account:PutAlternateContact",
        "account>DeleteAlternateContact",
        "account:EnableRegion",
        "account:DisableRegion"
      ],
    }
  ]
}
```

```
    "Resource": "*"
  }
}
}
```

AWS アカウント管理にアイデンティティベースのポリシー (IAM ポリシー) を使用する

この情報は、高度な AWS エクスペリエンスを使用する際に AWS アカウント 作成する に最も関連しています。新しい AWS エクスペリエンスでのアクセスコントロールの仕組みについては、「」を参照してください [アクセス管理を比較する](#)。

AWS アカウント および IAM ユーザーの詳細については、「[IAM とは](#)」を参照してください。
「IAM ユーザーガイド」の「」を参照してください。

カスタマー管理ポリシーを更新する方法については、「IAM ユーザーガイド」の「[IAM ポリシーの編集](#)」を参照してください。

AWS アカウント管理アクションポリシー

この表は、アカウント設定へのアクセス権を付与するアクセス許可の要約を示しています。これらのアクセス許可を使用するポリシーの例については、[AWS アカウント管理のアイデンティティベースのポリシーの例](#) を参照してください。

Note

のアカウントページで特定のアカウント設定への書き込みアクセスを IAM ユーザーに許可するには AWS マネジメントコンソール、その設定を変更するために使用するアクセス `GetAccountInformation` 許可 (またはアクセス許可) に加えて、アクセス許可を付与する必要があります。

アクセス許可名	アクセスレベル	説明
<code>account:ListRegions</code>	[List] (リスト)	使用可能なリージョンをリストするためのアクセス許可を付与します。

アクセス許可名	アクセスレベル	説明
account:GetAccountInformation	読み取り	アカウントのアカウント情報を取得するためのアクセス許可を付与します。
account:GetAlternateContact	読み取り	アカウントの代替連絡先を取得するためのアクセス許可を付与します。
account:GetContactInformation	読み取り	アカウントの主要連絡先情報を取得するためのアクセス許可を付与します。
account:GetPrimaryEmail	読み取り	アカウントのプライマリ E メールアドレスを取得するためのアクセス許可を付与します。
account:GetRegionOptStatus	読み取り	リージョンのオプトインステータスを取得するためのアクセス許可を付与します。
account:AcceptPrimaryEmailUpdate	書き込み	AWS 組織内のメンバーアカウントのプライマリ E メールアドレスの更新を受け入れるアクセス許可を付与します。

アクセス許可名	アクセスレベル	説明
account:CloseAccount	書き込み	アカウントを閉鎖するためのアクセス許可を付与します。 <div> Note これはコンソール専用のアクセス許可です。このアクセス許可に対しては、API によりアクセスすることはできません。</div>
account>DeleteAlternateContact	書き込み	アカウントの代替連絡先を削除するためのアクセス許可を付与します。
account:DisableRegion	書き込み	リージョンの使用を無効にするためのアクセス許可を付与します。
account:EnableRegion	書き込み	リージョンの使用を有効にするためのアクセス許可を付与します。
account:PutAccountName	書き込み	アカウントの名を更新するためのアクセス許可を付与します。
account:PutAlternateContact	書き込み	アカウントの代替連絡先を変更するためのアクセス許可を付与します。
account:PutContactInformation	書き込み	アカウントの主要連絡先情報を更新するためのアクセス許可を付与します。

アクセス許可名	アクセスレベル	説明
account:SendPhoneNumberVerification	書き込み	アカウントのプライマリ連絡先の電話番号に検証コードを送信するアクセス許可を付与します。
account:StartPrimaryEmailUpdate	書き込み	AWS 組織内のメンバーアカウントのプライマリ E メールアドレスの更新を開始するアクセス許可を付与します。
account:VerifyPhoneNumber	書き込み	検証コードを送信して、アカウントのプライマリ連絡先の電話番号を検証するアクセス許可を付与します。

AWS アカウント管理の ID とアクセスのトラブルシューティング

この情報は、高度な AWS エクスペリエンスを使用する際に AWS アカウント 作成する に最も関連しています。新しい AWS エクスペリエンスでのアクセスコントロールの仕組みについては、「」を参照してください [アクセス管理を比較する](#)。

以下の情報は、アカウント管理と IAM を併用した場合に発生しうる一般的な問題の診断と解決に役立ちます。

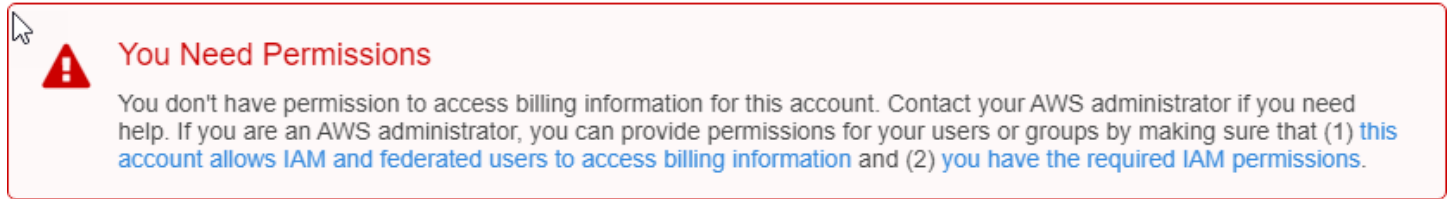
トピック

- [\[アカウント\] ページでのアクションの実行を認可されていない](#)
- [iam:PassRole を実行する権限がない](#)
- [自分の 以外のユーザーに自分のアカウントの詳細 AWS アカウント へのアクセスを許可したい](#)

[アカウント] ページでのアクションの実行を認可されていない

がアクションを実行する権限がないと AWS マネジメントコンソール 通知した場合は、管理者に連絡してサポートを依頼する必要があります。担当の管理者はお客様のユーザー名とパスワードを発行した人です。

次の例のエラーは、IAM mateojackson ユーザーがコンソールを使用しての AWS アカウント アカウントページでの詳細を表示しようとしている AWS マネジメントコンソールが、アクセス `account:GetAccountInformation` 許可がない場合に発生します。



この場合、Mateo は、`account:GetWidget` アクションを使用して `my-example-widget` リソースへのアクセスが許可されるように、管理者にポリシーの更新を依頼します。

iam:PassRole を実行する権限がない

`iam:PassRole` アクションの実行を認可されていないことを示すエラーが表示された場合は、アカウント管理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アカウント管理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 以外のユーザーに自分のアカウントの詳細 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:

- これらの機能をアカウント管理でサポートされるかどうかを確認するには、[AWS アカウント管理と IAM の連携方法](#) 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。

AWS AWS アカウント管理の 管理ポリシー

この情報は、高度な AWS エクスペリエンスを使用するとき、またはアカウントの高度な機能をアクティブ化したときに AWS アカウント 作成する に最も関連します。新しい AWS エクスペリエンスでのアクセスコントロールの仕組みについては、「」を参照してください[アクセス管理を比較する](#)。

AWS アカウント管理では現在、次の 2 つの AWS 管理ポリシーを使用できます。

- [AWS マネージドポリシー: AWSAccountManagementReadOnlyAccess](#)
- [AWS マネージドポリシー: AWSAccountManagementFullAccess](#)
- [AWS 管理ポリシーに対するアカウント管理の更新](#)

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ります。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え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 マネージドポリシー: AWSAccountManagementReadOnlyAccess

AWSAccountManagementReadOnlyAccess ポリシーを IAM アイデンティティにアタッチできます。

以下のポリシーは、読み取り専用の機能へのアクセス許可を提供します。

- に関するメタデータ AWS アカウント
- に対して有効または無効 AWS リージョン になっている AWS アカウント (アカウント内のリージョンのステータスは、AWS コンソールを使用してのみ表示できます)

これは、Get* または List* オペレーションのいずれかを実行するアクセス許可を付与することによって実現されます。アカウントのメタデータを変更したり、アカウントの AWS リージョン を有効または無効にしたりすることはできません。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- account – プリンシパルがメタデータ情報を取得できるようにします AWS アカウント。また、AWS リージョン 内のアカウントで有効になっている AWS マネジメントコンソールを一覧表示できます。

JSON

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "account:Get*",
      "account:List*"
    ],
    "Resource": "*"
  }
]
```

AWS マネージドポリシー: AWSAccountManagementFullAccess

AWSAccountManagementFullAccess ポリシーを IAM アイデンティティにアタッチできます。

このポリシーは、次の項目を表示または変更するための完全な管理者アクセス権を提供します。

- に関するメタデータ AWS アカウント
- に対して有効または無効 AWS リージョン になっている (AWS コンソールを使用してのみ、アカウントのリージョンのステータスを表示または有効または無効に AWS アカウント できます)

これは、あらゆる account オペレーションを実行するアクセス許可を付与することで実現されます。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- account – プリンシパルがメタデータ情報を表示または変更できるようにします AWS アカウント。また、プリンシパルは、アカウントで有効になっている AWS リージョン を一覧表示し、AWS マネジメントコンソール内でそれらの有効と無効を切り替えることができます。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
{
  "Effect": "Allow",
  "Action": "account:*",
  "Resource": "*"
}
```

AWS 管理ポリシーに対するアカウント管理の更新

このサービスがこれらの変更の追跡を開始してからのアカウント管理の 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通知については、アカウント管理ドキュメント履歴ページの RSS フィードをサブスクライブしてください。

変更	説明	日付
AWS アカウント管理が新しい AWS 管理ポリシーで起動され、変更の追跡を開始	<p>アカウント管理は、次の AWS 管理ポリシーで最初に起動されます。</p> <ul style="list-style-type: none">• AWSAccountManagementReadOnlyAccess• AWSAccountManagementFullAccess	2021 年 9 月 30 日

AWS アカウント管理のコンプライアンス検証

当社の新しい AWS エクスペリエンスは、規制対象のワークロードには使用できません。以下の情報は、「Sign up for AWS (advanced)」を使用したときに作成されたアカウントにのみ関連します。

サードパーティーの監査者は、複数のコンプライアンスプログラム AWS アカウントの一環としてで実行できる AWS サービスのセキュリティと AWS コンプライアンスを評価します。これらのプログラムには、SOC、PCI、FedRAMP、HIPAA などがあります。

特定のコンプライアンスプログラムの対象となる AWS サービスのリストについては、[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」を参照してください。一般的な情報については、[AWS「Compliance Programs Assurance」](#)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、「[ユーザーガイド](#)」の [AWS Artifact](#)」を参照してください。AWS Artifact

でサービスを使用する際のお客様のコンプライアンス責任 AWS アカウント 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。は、コンプライアンスに役立つ以下のリソース AWS を提供します。

- [セキュリティとコンプライアンスのクイックスタートガイド](#) – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- [アマゾン ウェブ サービスにおける HIPAA セキュリティとコンプライアンスのためのアーキテクチャ](#) – このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

Note

すべての AWS のサービス が HIPAA の対象となるわけではありません。詳細については、[HIPAA 対応サービスのリファレンス](#)を参照してください。

- [AWS コンプライアンスリソース](#) – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- 「[デベロッパーガイド](#)」の「[ルールによるリソースの評価](#)」 – この AWS Config サービスは、リソース設定が内部プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。AWS Config
- [AWS Security Hub CSPM](#) – これにより AWS のサービス、内のセキュリティ状態を包括的に把握 AWS できるため、セキュリティ業界標準とベストプラクティスへの準拠を確認できます。
- [AWS Audit Manager](#) – これにより AWS のサービス、AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

AWS アカウント管理の耐障害性

以下の情報は、すべてのに関連しています AWS アカウント。新しい AWS エクスペリエンスを使用する場合は、追加のリージョンの考慮事項が適用されます。詳細については、「[AWS リージョンプロジェクトの](#)」を参照してください。

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ゾーンを中心に構築されています。リージョンには、低レイテンシー、高いスループット、そして高度の冗長

ネットワークで接続されている複数の物理的に独立および隔離されたアベイラビリティゾーンがあります。アベイラビリティゾーンでは、ゾーン間で中断することなく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、フォールトトレランス、および拡張性が優れています。

AWS リージョン およびアベイラビリティ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 アカウント管理

以下の情報は、すべてのに関連しています AWS アカウント。

マネージドサービスとして、で実行されている AWS サービスは AWS グローバルネットワークセキュリティによって保護 AWS アカウント されます。AWS セキュリティサービスと がインフラストラクチャを保護する方法については AWS、[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 AWS 環境を設計するには、「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アカウント設定にアクセスします。クライアントは次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、ほとんどの最新システムでサポートされています。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、[AWS Security Token Service](#) (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

をモニタリングする AWS アカウント

これには、新しい AWS エクスペリエンスを使用して AWS アカウント を作成し、高度な AWS エクスペリエンスを使用して作成するアカウントが含まれます。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

モニタリングは、AWS アカウント管理およびその他の 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。には、アカウント管理を監視し、問題が発生したときに報告し、必要に応じて自動アクションを実行するための以下のモニタリングツール AWS が用意されています。

- AWS CloudTrail は、によって、またはに代わって行われた API コールおよび関連イベントをキャプチャ (ログ) AWS アカウント し、指定した Amazon Simple Storage Service (Amazon S3) バケットにログファイルを書き込みます。AWSを呼び出したユーザーとアカウント、呼び出し元の IP アドレス、および呼び出しの発生日時を特定できます。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。
- Amazon EventBridge は、アプリケーションの可用性の問題やリソースの変更などのシステムイベントに自動的に応答することで、AWS サービスに自動化を追加します。AWS サービスからのイベントは、ほぼリアルタイムで EventBridge に配信されます。簡単なルールを記述して、注目するイベントと、イベントがルールに一致した場合に自動的に実行するアクションを指定できます。詳細については、[Amazon EventBridge ユーザーガイド](#)を参照してください。

を使用した AWS アカウント管理 API コールのログ記録 AWS CloudTrail

これには、新しい AWS エクスペリエンスを使用して AWS アカウント を作成し、高度な AWS エクスペリエンスを使用して作成するアカウントが含まれます。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

AWS アカウント管理 APIs は、ユーザー AWS CloudTrail、ロール、またはアカウント管理オペレーションを呼び出す サービスによって実行されたアクションを記録する AWS サービスであると統合されています。CloudTrail は、すべてのアカウント管理 API コールをイベントとしてキャプチャします。キャプチャされたコールには、アカウント管理操作へのすべての呼び出しが含まれます。追跡を作成する場合、アカウント管理のイベントを含む 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。追跡を設定しない場合でも、CloudTrail コンソールの [Event history] (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、請求情報とコスト管理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。

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 でのアカウント管理情報

アカウントを作成する AWS アカウント と、CloudTrail が 有効になります。アカウント管理オペレーションでアクティビティが発生すると、CloudTrail はそのアクティビティを CloudTrail イベントとイベント履歴の他の AWS サービスイベントに記録します。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。

アカウント管理オペレーションのイベントなど AWS アカウント、 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。証跡により、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、 で証跡を作成すると AWS マネジメントコンソール、証跡はすべてのに適用されます AWS リージョン。証跡は、AWS パーティション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。CloudTrail ログで収集されたイベントデータをさらに分析して処理するように、他の AWS サービスを設定できます。詳細については、次を参照してください：

- [追跡を作成するための概要](#)
- [CloudTrail がサポートされているサービスと統合](#)
- 「[CloudTrail の Amazon SNS 通知の設定](#)」
- [CloudTrail ログファイルの複数のリージョンからの受け取り](#)
- [複数のアカウントから CloudTrail ログファイルを受け取る](#)

AWS CloudTrail は、このガイドの API [リファレンスセクションにあるすべてのアカウント管理 API](#) オペレーションを記録します。たとえば CreateAccount、DeleteAlternateContact、および PutAlternateContact の各オペレーションへのコールは、CloudTrail ログファイル内にエントリを生成します。

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または AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか

- リクエストが、IAM ロールまたはフェデレーティッドユーザーの一時的なセキュリティ認証情報によって行われたか
- 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 エlement](#)」を参照してください。

アカウント管理のログエントリについて

「トレイル」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 のログファイルには、単一または複数のログエントリがあります。各イベントは任意の送信元からの単一のリクエストを表し、リクエストされたオペレーション、オペレーションの日時、リクエストパラメータなどに関する情報を含みます。CloudTrail ログファイルは、パブリック 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。

例 1: 次の例は、アカウントの現在の OPERATIONS 代替連絡先を取得する `GetAlternateContact` 操作の呼び出しを記録する CloudTrail ログエントリを示しています。操作によって返される値は、ログに記録される情報に含まれません。

Example例 1

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
```

```

        "creationDate": "2021-04-30T19:25:53Z"
      }
    },
    "eventTime": "2021-04-30T19:26:15Z",
    "eventSource": "account.amazonaws.com",
    "eventName": "GetAlternateContact",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.250",
    "userAgent": "Mozilla/5.0",
    "requestParameters": {
      "alternateContactType": "SECURITY"
    },
    "responseElements": null,
    "requestID": "1a2b3c4d-5e6f-1234-abcd-111111111111",
    "eventID": "1a2b3c4d-5e6f-1234-abcd-222222222222",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "123456789012"
  }
}

```

例 2: 次の例は、アカウントに新しい PutAlternateContact 代替連絡先を追加する BILLING 操作の呼び出しを記録する CloudTrail ログエントリを示しています。

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
    },
  },
}

```

```

    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2021-04-30T18:33:00Z"
    }
  },
  "eventTime": "2021-04-30T18:33:08Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "PutAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "name": "*Alejandro Rosalez*",
    "emailAddress": "alrosalez@example.com",
    "title": "CFO",
    "alternateContactType": "BILLING"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-333333333333",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-444444444444",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}

```

例 3: 次の例は、アカウントの現在の DeleteAlternateContact 代替連絡先を削除する OPERATIONS 操作の呼び出しを記録する CloudTrail ログエントリを示しています。

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI234567890EXAMPLE",

```

```
    "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
    "accountId": "123456789012",
    "userName": "ServiceTestRole"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-04-30T18:33:00Z"
  }
},
"eventTime": "2021-04-30T18:33:16Z",
"eventSource": "account.amazonaws.com",
"eventName": "DeleteAlternateContact",
"awsRegion": "us-east-1",
"sourceIPAddress": "10.24.34.250",
"userAgent": "Mozilla/5.0",
"requestParameters": {
  "alternateContactType": "OPERATIONS"
},
"responseElements": null,
"requestID": "1a2b3c4d-5e6f-1234-abcd-555555555555",
"eventID": "1a2b3c4d-5e6f-1234-abcd-666666666666",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012"
}
```

EventBridge によるアカウント管理イベントのモニタリング

これには、新しい AWS エクスペリエンスを使用して AWS アカウント を作成し、高度な AWS エクスペリエンスを使用して作成するアカウントが含まれます。サインアップオプションを比較するには、「」を参照してください[サインアップオプションを比較する](#)。

Amazon EventBridge (旧称: CloudWatch Events) は、固有のイベントをモニタリングし、他の AWS のサービスを使用するターゲットアクションを開始するのに役立ちます。からのイベント AWS のサービス は、ほぼリアルタイムで EventBridge に配信されます。

EventBridge を使用すると、受信イベントを照合し、処理のためにターゲットにルーティングするルールを作成できます。

詳細については、「Amazon EventBridge ユーザーガイド」の「[Getting started with Amazon EventBridge](#)」を参照してください。

アカウント管理イベント

次の例は、アカウント管理のイベントを示しています。イベントは、ベストエフォートベースで生成されます。

現在、アカウント管理で利用できるのは、リージョンの有効化および無効化と、CloudTrail を介した API 呼び出しに固有のイベントのみです。

イベントタイプ

- [リージョンの有効化および無効化に関するイベント](#)

リージョンの有効化および無効化に関するイベント

コンソールまたは API からアカウントでリージョンを有効または無効にすると、非同期タスクが開始されます。最初のリクエストは、ターゲットアカウントで CloudTrail イベントとして記録されます。さらに、有効化または無効化プロセスが開始されたとき、およびそのプロセスが完了したときに、呼び出し元アカウントに EventBridge イベントが送信されます。

次のイベント例は、2020-09-30 にアカウント 123456789012 の ap-east-1 リージョンが ENABLED にされたことを示すリクエストがどのように送信されるかを示しています。

```
{
  "version": "0",
  "id": "11112222-3333-4444-5555-666677778888",
  "detail-type": "Region Opt-In Status Change",
  "source": "aws.account",
  "account": "123456789012",
  "time": "2020-09-30T06:51:08Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:account::123456789012:account"
  ],
  "detail": {
    "accountId": "123456789012",
    "regionName": "ap-east-1",
    "status": "ENABLED"
  }
}
```

```
}
```

GetRegionOptStatus および ListRegions API が返すステータスは、以下の 4 つのステータスのいずれかと一致します。

- ENABLED – 指定された accountId に対してリージョンの有効化が正常に完了しました
- ENABLING – 指定された accountId に対してリージョンの有効化プロセスが進行中です。
- DISABLED – 指定された accountId に対してリージョンの無効化が正常に完了しました
- DISABLING – 指定された accountId に対してリージョンの無効化プロセスが進行中です。

次のイベントパターンの例は、すべてのリージョンイベントをキャプチャするルールを作成します。

```
{
  "source": [
    "aws.account"
  ],
  "detail-type": [
    "Region Opt-In Status Change"
  ]
}
```

次のイベントパターンの例は、ENABLED および DISABLED リージョンイベントのみをキャプチャするルールを作成します。

```
{
  "source": [
    "aws.account"
  ],
  "detail-type": [
    "Region Opt-In Status Change"
  ],
  "detail": {
    "status": [
      "DISABLED",
      "ENABLED"
    ]
  }
}
```

のクォータ AWS アカウント管理

AWS アカウント には、サービスごとに AWS 、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。

次のクォータ情報は、 を使用する場合に作成するプロジェクト用です [にサインアップする AWS \(新規\)](#)。クォータを調整するには、サポートチケットを作成します。詳細については、「[プロジェクトサポート](#)」を参照してください。

[リソース]	クォータ	引き上げ可能
無料プランで所有しているプロジェクトの数	29	いいえ
有料プランで所有できるプロジェクトの数	299	いいえ
プロジェクトを共有できる人数	500	いいえ
承諾できるプロジェクトの数	100	いいえ

次のクォータ情報は、サインアップ (アドバンスド) を使用してサインアップする場合に AWS アカウント 作成するためのものです。特に明記されていない限り、各クォータは AWS リージョン固有です。

[リソース]	クォータ
ターゲットアカウントあたりの StartPrimaryEmailUpdate リクエストの最大数	30 秒あたり 3
の代替連絡先の数 AWS アカウント	3 - BILLING、SECURITY、および OPERATIONS に 1 つずつ
アカウントあたりの同時リージョンオブジェクトの数	6

[リソース]	クォータ
組織あたりの同時リージョンオプトリクエストの数	50
呼び出し元アカウントごとの AcceptPrimaryEmailUpdate リクエストのレート	毎秒 1 回、バーストは毎秒 1 回まで
アカウントごとの DeleteAlternateContact リクエストのレート	毎秒 1 回、バーストは毎秒 6 回まで
アカウントごとの DisableRegion リクエストのレート	毎秒 1 回、バーストは毎秒 1 回まで
アカウントごとの EnableRegion リクエストのレート	毎秒 1 回、バーストは毎秒 1 回まで
呼び出し元アカウントごとの GetAccountInformation リクエストのレート	毎秒 3 回、バーストは毎秒 3 回まで
アカウントごとの GetAlternateContact リクエストのレート	毎秒 10 回、バーストは毎秒 15 回まで
アカウントごとの GetContactInformation リクエストのレート	毎秒 10 回、バーストは毎秒 15 回まで
アカウントごとの GetGovCloudAccountInformation リクエストのレート	毎秒 3 回、バーストは毎秒 5 回まで
呼び出し元アカウントごとの GetPrimaryEmail リクエストのレート	毎秒 3 回、バーストは毎秒 3 回まで
アカウントごとの GetRegionOptStatus リクエストのレート	毎秒 5 回、バーストは毎秒 5 回まで
アカウントごとの ListRegions リクエストのレート	毎秒 5 回、バーストは毎秒 5 回まで
呼び出し元アカウントごとの PutAccountName リクエストのレート	毎秒 1 回、バーストは毎秒 1 回まで

[リソース]	クォータ
アカウントごとの PutAlternateContact リクエストのレート	毎秒 5 回、バーストは毎秒 8 回まで
アカウントごとの PutContactInformation リクエストのレート	毎秒 5 回、バーストは毎秒 8 回まで
呼び出し元アカウントごとの StartPrimaryEmailUpdate リクエストのレート	毎秒 1 回、バーストは毎秒 1 回まで

アカウント管理ユーザーガイドのドキュメント履歴

次の表に、AWS アカウント管理のドキュメントリリースを示します。

変更	説明	日付
新しい電話番号検証 APIs	新しい SendPhoneNumberVerification API と VerifyPhoneNumber APIs を使用して、主要な連絡先の電話番号を確認できます。GetContactInformation レスポンスには新しいVerificationStatus フィールドも含まれます。	2026 年 10 月 1 日
アカウント閉鎖クォータ値を更新	トラブルシューティングトピックのアカウント閉鎖クォータの割合を 10% から 20% に、最小値を 10 から 250 に修正しました。	2026 年 6 月 23 日
新しいアカウント名 API	アカウント名を表示または変更するための新しい GetAccountInformation および PutAccountName API のサポート。	2025 年 4 月 22 日
秘密の質問の編集のサポート終了	サポートが終了したため、「秘密の質問の編集」トピックをガイドから削除しました。	2025 年 1 月 6 日
新しい主要 E メール API	AWS Organizations内の任意のメンバーアカウントのルートユーザーの E メールアドレスとを一元的に更新する	2024 年 6 月 6 日

ための新しい [GetPrimaryEmail](#)、[StartPrimaryEmailUpdate](#)、および [AcceptPrimaryEmailUpdate](#) API のサポート。詳細については、「AWS Organizations ユーザーガイド」の「[メンバーアカウントのルートユーザーの E メールアドレスとの更新](#)」を参照してください。

[アカウント閉鎖トピックの書き換え](#)

メンバーアカウントと管理アカウントを閉鎖する手順を追加するなど、アカウント閉鎖トピック全体が完全に見直されました。

2024 年 2 月 1 日

[新しい秘密の質問の追加のサポート終了](#)

[アカウント] ページから新しい秘密の質問を追加するオプションが削除されたことを記載した新しいコンテンツが追加されました。

2024 年 1 月 5 日

[aws-portal 名前空間のサポート終了](#)

AWS Identity and Access Management アカウントの管理に以前使用されていた (IAM) アクション (`aws-portal:ModifyAccount` や など `aws-portal:ViewAccount`) は、標準サポートが終了しました。

2024 年 1 月 1 日

[リージョントピックの書き換え](#)

展開コントロールと折りたたみコントロールの追加など、リージョントピック全体が完全に見直されました。

2023 年 10 月 8 日

[「IAM ユーザーガイド」への ルートユーザートピックの移動](#)

ルートユーザーに関する説明を 1 つのトピックに統合し、「IAM ユーザーガイド」に移動されたルートユーザートピックへの相互参照リンクが追加されました。

2023 年 9 月 18 日

[主要アカウント連絡先トピックへの新しいセクションの追加](#)

新たに「Phone number and email address requirements」セクションが追加されました。

2023 年 9 月 12 日

[新しい連絡先情報 API](#)

新しい GetContactInformation API および PutContactInformation API のサポート。

2022 年 7 月 22 日

[AWS アカウント管理では、AWS Organizations コンソールを介した代替連絡先の更新がサポートされるようになりました。](#)

更新された AWS Organizations 管理ポリシーによって提供されるアカウント API アクセス許可を使用して、AWS Organizations コンソールを介して組織の代替連絡先を更新できるようになりました。

2022 年 2 月 8 日

[初回リリース](#)

AWS アカウント管理リファレンスガイドの初回リリース

2021 年 9 月 30 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。