ユーザーガイド

AWS 設定

AWS 設定: ユーザーガイド

Table of Contents

概要

このガイドでは、最新のセキュリティベストプラクティスに従った AWS IAM Identity Center で、新しい AWS アカウント を作成し、最初の管理ユーザーを設定する方法について説明します。

AWS アカウント は AWS サービス へのアクセスに必要で、次の 2 つの基本機能として機能します。

- コンテナ — AWS アカウント は AWS カスタマーとして作成されるすべての AWS リソースのためのコンテナです。Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Relational Database Service (Amazon RDS) データベースを作成する場合、またはデータを処理するために Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを作成すると、アカウントにリソースが作成されます。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す。アカウントで作成したリソースは、同じアカウントの認証情報を持つユーザーのみが使用できます。

  アカウントで作成できる主なリソースには、IAM ユーザーやロールなどの ID と、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、IAM Identity Center ディレクトリのユーザー、または ID ソースから提供された認証情報を使用して AWS サービス にアクセスするユーザーなど、フェデレーティッド ID があります。これらのアイデンティティには認証情報があり、ユーザーはそれを使用して AWS にサインインまたは認証できます。アイデンティティには、サインインしたユーザーがアカウント内のリソースで何をする権限があるかを指定するアクセス許可ポリシーも含まれます。

用語

Amazon Web Services (AWS) では、一般的な用語を使用してサインインプロセスを説明しています。これらの用語を読んで理解することをお勧めします。

管理者

AWS アカウント 管理者または IAM 管理者とも呼ばれます。管理者 (通常は情報技術 (IT) 担当者) は、AWS アカウント を監督するユーザーです。管理者は、組織の他のメンバーよりも高いレベルの AWS アカウント 権限を持っています。管理者は AWS アカウント の設定と実装を行います。IAM Identity Center ユーザーも作成されます。管理者はこれらのユーザーにアクセス認証情報と AWS サインイン用のサインイン URL を提供します。

アカウント

標準の AWS アカウント で、AWS リソースと、それらのリソースにアクセスできる ID の両方を含みます。アカウントは、アカウント所有者の E メールアドレスとパスワードに関連付けられます。

認証情報

アクセス認証情報またはセキュリティ認証情報として参照されます。認証情報は、ユーザーがサインインして AWS リソースにアクセスするために AWS に提供する情報です。認証情報には、E メールアドレス、ユーザー名、ユーザー定義パスワード、アカウント ID またはエイリアス、検証コード、および 1 回限り使用できる多要素認証 (MFA) コードが含まれます。認証および認可を実行する際にシステムは、誰が呼び出しをしているかを特定し、リクエストされたアクセスを許可するかどうかを決定するために認証情報を使用します。AWS では、これらの認証情報は通常、アクセスキー ID とシークレットアクセスキーです。

認証情報の設定の詳細については、「AWS 認証情報の理解と取得」を参照してください。

> **Note**
>
> ユーザーが送信する必要のある認証情報の種類は、そのユーザーの種類によって異なります。

企業認証情報

ユーザーが企業ネットワークやリソースにアクセスする際に提供する認証情報。社内管理者は、社内ネットワークやリソースへのアクセスに使用するのと同じ認証情報で AWS アカウント にアクセスできるように設定できます。これらの認証情報は、管理者またはヘルプデスクの従業員から提供されます。

プロファイル

AWS Builder ID にサインアップすると、プロファイルが作成されます。プロファイルには、入力した連絡先情報と、多要素認証 (MFA) デバイスとアクティブなセッションを管理する機能が含まれます。また、プライバシーやプロフィールのデータの取り扱い方法について説明しています。プロファイルとそれがどのように AWS アカウント に関連しているかについて詳しくは、「AWS Builder ID とその他の AWS 認証情報」を参照してください。

ユーザー

ユーザーは、AWS 製品に対して API 呼び出しを実行するユーザーまたはアプリケーションです。各ユーザーには、AWS アカウント 内での一意の名前と、他のユーザーと共有されない一連の認証情報があります。これらの認証情報は、AWS アカウント のセキュリティ認証情報とは異なります 各ユーザーが関連付けられる AWS アカウント は 1 つだけです。

ルートユーザーの認証情報

ルートユーザーの認証情報は、ルートユーザーとして AWS Management Console にサインインするときに使用する認証情報と同じです。ルートユーザーの詳細については、「ルートユーザー」を参照してください。

検証コード

認証コードは、サインインプロセス中に多要素認証 (MFA) を使用して、ユーザー ID を確認します。認証コードの配信方法はさまざまです。テキストメッセージまたは E メールで送信できます。詳細については、管理者に確認してください。

AWS ユーザーと認証情報

AWS の操作時に、自身が誰であるか、そしてリクエストしているリソースに対してアクセス許可を持つかどうかを確認するための AWS セキュリティ認証情報を指定します。AWS は、このセキュリティ認証情報を使用してリクエストを認証、承認します。

たとえば、Amazon Simple Storage Service (Amazon S3) バケットから保護されたファイルをダウンロードする場合、認証情報はそのアクセスを許可する必要があります。認証情報にファイルをダウンロードする権限がないことが示される場合、AWS はリクエストを拒否します。ただし、公開されている Amazon S3 バケット内のファイルのダウンロードにセキュリティ認証情報は必要ありません。

ルートユーザー

アカウント所有者またはアカウントルートユーザーとも呼ばれます。ルートユーザーは、AWS アカウント のすべての AWS サービスとリソースへの完全なアクセス権を持ちます。AWS アカウント を初めて作成する場合は、このアカウントのすべての AWS サービスとリソースに対して完全なアクセス権を持つシングルサインインアイデンティティで始めます。このアイデンティティは、AWS アカウントのルートユーザーです。アカウントの作成に使用した E メールアドレスとパスワードを使用して、AWS Management Console にルートユーザーとしてサインインできます。サインインの手順については、「ルートユーザーとして AWS Management Console にサインインする」を参照してください。

> **Important**
>
> AWS アカウント を作成する場合は、このアカウントのすべての AWS サービス とリソースに対して完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることによってアクセスできます。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。ルートユーザーの認証情報を保護し、それらを使用してルートユーザーのみが実行できるタスクを実行します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「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。

ルートユーザーを含む IAM ID の詳細については、「IAM ID (ユーザー、ユーザーグループ、ロール)」を参照してください。

IAM Identity Center ユーザー

IAM Identity Center ユーザーは、AWS アクセスポータルからサインインします。AWS アクセスポータルまたは特定のサインイン URL は、管理者またはヘルプデスクの従業員によって提供されます。AWS アカウント 用に IAM Identity Center ユーザーを作成した場合、IAM Identity Center ユーザーへの参加招待が AWS アカウント の E メールアドレスに送信されました。特定のサインイン URL は招待メールに含まれています。IAM Identity Center ユーザーは、AWS Management Console からサインインすることはできません。サインインの手順については、「AWS アクセスポータルへのサインイン」を参照してください。

> **Note**
>
> 後ですぐにアクセスできるように、AWS アクセスポータルの特定のサインイン URL をブックマークしておくことをお勧めします。

IAM Identity Center の詳細については、「IAM アイデンティティセンターとは」を参照してください。

フェデレーティッド ID

フェデレーティッド ID は、よく知られている外部 ID プロバイダー (IdP) (例: Login with Amazon、Facebook、Google などの OpenID Connect (OIDC) 互換の IdP) を使用してサインインすることができるユーザーです。ウェブ ID フェデレーションで認証トークンを受け取ったら、そのトークンを AWS アカウント のリソースを使用するためのアクセス許可を持つ IAM ロールにマッピングし、AWS の一時的セキュリティ認証情報に変換することができます。AWS Management Console または AWS アクセスポータルでサインインする必要はありません。代わりに、使用する外部 ID によって、サインイン方法が決まります。

詳細については、「フェデレーティッド ID へのサインイン」を参照してください。

IAM ユーザー

IAM ユーザーは、AWS で作成したエンティティです。このユーザーは、特定のカスタム許可を持つ AWS アカウント 内の ID です。IAM ユーザー認証情報は、AWS Management Console へのサインインに使用される名前とパスワードで構成されます。サインインの手順については、「IAM ユーザーとして AWS Management Console にサインインする」を参照してください。

IAM ユーザーを含む IAM ID の詳細については、「IAM ID (ユーザー、ユーザーグループ、ロール)」を参照してください。

AWS Builder ID ユーザー

AWS Builder ID ユーザーは、アクセスしたい AWS サービスまたはツールに特別にサインインします。AWS Builder ID は、すでに所有している、または作成したい AWS アカウント を補完するものです。AWS Builder ID はユーザーを個人として表し、AWS アカウント を使用しなくても AWS サービスやツールにアクセスできます。また、自分の情報を確認したり更新したりできるプロフィールもあります。詳細については、「AWS Builder ID でサインインするには」を参照してください。

前提条件と考慮事項

セットアッププロセスを開始する前に、アカウントの要件を確認し、AWS アカウント が複数必要かどうかを検討し、IAM Identity Center の管理者アクセス用にアカウントを設定するための要件を理解してください。

AWS アカウント の要件

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

- アカウント名 — アカウントの名前は、請求書、コンソール内の請求情報とコスト管理ダッシュボード、および AWS Organizations コンソールなど複数の場所に表示されます。

  認識しやすいアカウント名を付けて、所有している他のアカウントと区別できるように、アカウント命名基準に従うことをお勧めします。会社のアカウントの場合、会社-目的-環境 (例えば、AnyCompany-audit-prod) のような命名基準に従うことを検討してください。個人アカウントの場合、名-姓-目的 (例えば、paulo-santos-testaccount) のような命名基準に従うことを検討してください。

- E メールアドレス — この E メールアドレスは、アカウントのルートユーザーのサインイン名として使用され、パスワードを忘れた場合など、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 E 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、E メールアカウントへのアクセス権があることを確認する必要があります。

  > **Important**
  >
  > このアカウントがビジネス向けである場合、企業の配布リスト (`it.admins@example.com`など) を使用することをお勧めします。個人用の会社 E メールアドレス (`paulo.santos@example.com` など) を使用することは避けてください。これにより、従業員が職位を変更したり、会社を辞めたりしても、企業が AWS アカウントにアクセスできることを保証するのに役立ちます。E メールアドレスは、アカウントのルートユーザーの認証情報をリセットするために使用できます。この同報リストまたはアドレスへのアクセスを保護してください。

- 電話番号 — アカウント所有権の確認が必要な場合にこの番号を使用できます。この電話番号で通話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向けである場合は、個人の電話番号ではなく、会社の電話番号を使用することをお勧めします。これにより、従業員が職位を変更したり、会社を辞めたりしても、企業が AWS アカウント にアクセスできることを保証するのに役立ちます。

- 多要素認証 (MFA) デバイス — AWS リソースを保護するには、ルートユーザーアカウントで多要素認証 (MFA) を有効にします。通常のサインイン認証情報に加えて、MFA を有効にする際には二次認証が必要になり、セキュリティがさらに強化されます。詳細については、「IAM ユーザーガイド」の「MFA とは」を参照してください。
- AWS Support プラン — アカウントの作成プロセスで、利用可能なプランのいずれかを選択するよう求められます。使用可能なプランの説明については、「AWS Support 予定を比較する」を参照してください。

IAM Identity Center に関する考慮事項

以下のトピックには、特定の環境用に IAM Identity Center を設定するためのガイダンスが記載されています。パート 2: IAM Identity Center での管理ユーザーの作成 に進む前に、ご使用の環境に適用されるガイダンスを理解してください。

トピック

- Active Directory または外部 IdP
- AWS Organizations
- IAM ロール
- 次世代ファイアウォールとセキュアウェブゲートウェイ

Active Directory または外部 IdP

Active Directory または外部 IdP ですでにユーザーとグループを管理している場合は、IAM Identity Center を有効にして ID ソースを選択する際に、この ID ソースの接続を検討することをお勧めします。デフォルトの Identity Center ディレクトリでユーザーやグループを作成する前に接続しておくと、後から ID ソースを変更する場合に必要となる追加の設定を回避できます。

Active Directory を ID ソースとして使用する場合、設定は次の前提条件を満たす必要があります。

- AWS Managed Microsoft AD を使用している場合は、AWS Managed Microsoft AD ディレクトリが設定されている場所と同じ AWS リージョン で IAM Identity Center を有効にする必要があります。IAM Identity Center では、割り当てデータに関するディレクトリと同じリージョンに保存されます。IAM Identity Center を管理するには、Identity Center が設定されているリージョンに切り替える必要がある場合があります。また、AWS アクセスポータルでは、ディレクトリと同じアクセス URL が使用されます。
- 管理アカウントにある Active Directory を使用してください。

  AWS Directory Service に既存の AD Connector および AWS Managed Microsoft AD ディレクトリを設定し、それを AWS Organizations 管理アカウント内に配置する必要があります。一度に接続できる AD Connector あるいは AWS Managed Microsoft AD は、1 つのみです。複数のドメインやフォレストをサポートする必要がある場合は、AWS Managed Microsoft AD を使用してください。詳細については、以下を参照してください。

  - 「AWS IAM Identity Center ユーザーガイド」にある IAM Identity Center に、AWS Managed Microsoft AD のディレクトリを接続します。
  - 「AWS IAM Identity Center ユーザーガイド」の IAM Identity Center に Active Directory にあるセルフマネージドディレクトリを接続します。
- 委任された管理者アカウントにある Active Directory を使用してください。

  IAM Identity Center の委任管理を有効にし、IAM ID ソースとして Active Directory を使用する予定の場合は、委任された管理者アカウントにある AWS ディレクトリに設定された既存の AD Connector または AWS Managed Microsoft AD ディレクトリを使用できます。

  IAM Identity Center ソースを他のソースから Active Directory に変更するか、Active Directory から他のソースに変更する場合、そのディレクトリは IAM Identity Center 委任管理者メンバーアカウント (存在する場合) に配置する (所有されている) 必要があります。それ以外の場合は、管理アカウントに含まれている必要があります。

AWS Organizations

AWS アカウント は AWS Organizations によって管理されている必要があります。まだ組織を設定していない場合は、必要な操作はありません。IAM Identity Center を有効にするときに、AWS で組織を作成するかどうかを選択できます。

すでに AWS Organizations を設定している場合は、すべての機能が有効になっていることを確認してください。詳細については、「AWS Organizations ユーザーガイド」の「組織内のすべての機能の有効化」を参照してください。

IAM Identity Center を有効にするには、AWS Organizations 管理アカウントの認証情報を使用して AWS Management Console にサインインする必要があります。AWS Organizations メンバーアカウントの認証情報を使用してサインインしている場合は、IAM Identity Center を有効にできません。詳細については、「AWS Organizations ユーザーガイド」の「AWS 組織の作成と管理」を参照してください。

IAM ロール

AWS アカウント で IAM ロールをすでに設定している場合は、アカウントが IAM ロールのクォータに近づいているかどうかを確認することをお勧めします。詳細については、「IAM オブジェクトクォータ」を参照してください。

クォータに近づいている場合は、クォータ引き上げをリクエストすることを検討してください。これを行わない場合、IAM ロールのクォータを超えたアカウントにアクセス許可設定をプロビジョニングする際に、IAM Identity Center で問題が発生する可能性があります。クォータ引き上げのリクエストの詳細情報については、「Service Quotas ユーザーガイド」の「クォータ引き上げリクエスト」を参照してください。

次世代ファイアウォールとセキュアウェブゲートウェイ

NGFW や SWG などのウェブコンテンツフィルタリングソリューションを使用して、特定の AWS ドメインや URL エンドポイントへのアクセスをフィルタリングする場合は、以下のドメインや URL エンドポイントをウェブコンテンツフィルタリングソリューションの許可リストに追加する必要があります。

特定の DNS ドメイン

- *.awsapps.com (http://awsapps.com/)
- *.signin.aws

特定の URL エンドポイント

- https://*[yourdirectory]*.awsapps.com/start
- https://*[yourdirectory]*.awsapps.com/login
- https://*[yourregion]*.signin.aws/platform/login

複数の AWS アカウント の使用

AWS アカウント は AWS において基本的なセキュリティ境界として機能します。これらは、有用な分離レベルを提供するリソースコンテナとして機能します。リソースとユーザーを隔離する能力は、安全で適切に管理された環境を確立するための重要な要件です。

リソースを個別の AWS アカウント に分離することは、クラウド環境で以下の原則をサポートするのに役立ちます。

- 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、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、PCI セキュリティ基準の対象となるワークロードのすべての要素のホストが単一の AWS アカウント であることを示せれば、監査担当者と話がしやすくなります。
- 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の脅威は、他のユーザーに影響を与えずに、AWS アカウント 内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。チームを個別の AWS アカウント に移動することで、チーム同士の干渉を防ぐことができます。
- 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 AWS アカウント を用意すると、事業単位固有のニーズに対応できます。
- 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 AWS アカウント で分けながら、(AWS Organizations と一括請求を使用して) すべての請求を単一の支払者に集約することができます。
- クォータ割り当て – AWS サービスクォータは AWS アカウント ごとに個別に適用されます。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。

このガイド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、組織内の AWS アカウント のすべてを管理する無料の AWS サービスである AWS Organizations を使用することをお勧めします。

AWS は AWS Control Tower も提供し、これは AWS マネージドオートメーションのレイヤーを組織に追加し、それを 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します。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」を参照してください。

パート 1: 新しい AWS アカウント のセットアップ

これらの手順は、AWS アカウント の作成とルートユーザー認証情報の保護に役立ちます。パート 2: IAM Identity Center での管理ユーザーの作成 に進む前に、すべての手順を完了してください。

トピック

ステップ 1: AWS アカウントにサインアップする

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. [AWS アカウント を作成する] を選択します。

   > **Note**
   >
   > 最近 AWS にサインインしていれば、[コンソールにサインインする] を選択します。[新しい AWS アカウント を作成する] オプションが表示されない場合、まず [別のアカウントにサインインする] を選択してから、[AWS アカウント を作成する] を選択します。

3. アカウント情報を入力してから [続行] を選択します。

   アカウント情報、特に E メールアドレスを正しく入力してください。E メールアドレスを間違って入力すると、アカウントにアクセスできなくなります。

4. [個人] または [プロフェッショナル] を選択します。

   これらのオプションの違いは、お客様にお尋ねする情報のみにあります。どちらのアカウントタイプも同じ機能と機能を備えています。

5. AWS アカウント の要件 に記載されている手順に従って、企業情報または個人情報を入力します。
6. AWS カスタマーアグリーメントを読み、同意します。
7. [アカウントを作成してサインインする] を選択します。

   この時点で、AWS アカウント を使用する準備が完了したことを確認する E メールメッセージが届きます。サインアップ時に指定した E メールアドレスとパスワードを使用して、新しいア

カウントにサインインできます。ただし、アカウントのアクティベーションが完了するまでいずれの AWS サービスを使用することはできません。

8. [支払い情報] ページで、支払い方法に関する情報を入力します。アカウントの作成に使用した住所と異なる住所を使用する場合は、[新しい住所を使用] を選択し、請求に使用したい住所を入力します。
9. [確認して追加] を選択します。

> **Note**
>
> 連絡先住所がインドにある場合、AWS のローカル販売者である AISPL との利用規約が適用されます。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。確認プロセスの一環として、AISPL からカードに 2 インドルピー (INR) が請求されます。確認が完了すると、2 INR が AISPL より返金されます。

10. 電話番号を確認するには、リストから国または地域コードを選択し、数分以内に電話できる電話番号を入力します。CAPTCHA コードを入力し、送信してください。
11. AWS 自動検証システムから電話がかかり、PIN が提供されます。電話を使用して PIN を入力し、[続行] を選択します。
12. AWS Support プランを選択してください。

    使用可能なプランの説明については、「AWS Support 予定を比較する」を参照してください。

    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。通常、これには数分かかりますが、最大で 24 時間かかる場合があります。アクティベーション中に、新しい AWS アカウント にサインインできます。アクティベーションが完了するまで、[サインアップを完了する] ボタンが表示される場合があります。それは無視できます。

    AWS アカウントのアクティベーションが完了すると、確認メールを送信します。メールとスパムフォルダで確認メールメッセージを確認します。このメッセージを受信すると、すべての AWS のサービスにフルアクセスできるようになります。

ステップ 2: ルートユーザーとしてサインインする

AWS アカウント を最初に作成する場合は、アカウントのすべての AWS サービス とリソースに対して完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカ

ウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることによってアクセスできます。

> **Important**
>
> 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。ルートユーザーの認証情報を保護し、それらを使用してルートユーザーのみが実行できるタスクを実行します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「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。

ルートユーザーとしてサインインするには

1. https://console.aws.amazon.com/ で AWS Management Console を開きます。

   > **Note**
   >
   > 以前にこのブラウザでルートユーザーとしてサインインしたことがある場合は、お使いのブラウザに AWS アカウント の E メールアドレスが記憶されている可能性があります。
   > 以前にこのブラウザを使用して IAM ユーザーとしてサインインしたことがある場合は、代わりに IAM ユーザーのサインインページが表示される場合があります。メインのサインインページに戻るには、[ルートユーザーの E メールでサインイン] を選択します。

2. このブラウザを使用して以前にサインインしたことがない場合は、メインのサインインページが表示されます。アカウント所有者の場合は、[ルートユーザー] を選択します。アカウントに関連付けられている AWS アカウント の E メールアドレスを入力し、[次へ] を選択します。
3. セキュリティチェックの完了が求められる場合があります。これを完了して、次のステップに進みます。セキュリティチェックを完了できない場合は、音声を聞くか、セキュリティチェックを更新して新しい文字セットがないか試してください。
4. パスワードを入力して、[サインイン] を選択します。

ステップ 3: AWS アカウント ルートユーザーの MFA を有効にする

ルートユーザーの認証情報を引き続き使用する場合、セキュリティ上のベストプラクティスに従って AWS アカウント 用の多要素認証 (MFA) をアクティブにすることをお勧めします。ルートユーザー

はアカウント内で機密性の高い操作を実行できるまで、さらに認証レイヤーを追加することで、アカウントのセキュリティを強化できます。MFA には複数のタイプがあります。

ルートユーザーの MFA を有効にする手順については、「IAM ユーザーガイド」の「AWS でのユーザーの MFA デバイスの有効化」を参照してください。

パート 2: IAM Identity Center での管理ユーザーの作成

パート 1: 新しい AWS アカウント のセットアップ を完了したら、以下の手順を参考に管理ユーザーの AWS アカウント アクセスを設定し、日常的なタスクを実行します。

> **Note**
>
> このトピックでは、IAM Identity Center で AWS アカウント 管理者アクセスを正常に設定し、管理者ユーザーを作成するために最低限必要な手順について説明します。詳細については、「AWS IAM Identity Center ユーザーガイド」の「使用開始」を参照してください。

トピック

ステップ 1: IAM Identity Center を有効にする

> **Note**
>
> ルートユーザーの多要素認証 (MFA) を有効にしていない場合は、ステップ 3: AWS アカウント ルートユーザーの MFA を有効にする を完了してから次に進んでください。

IAM Identity Center を有効にするには

1. [ルートユーザー] を選択し、AWS アカウント の E メールアドレスを入力して、アカウント所有者として AWS Management Console にサインインします。次のページでパスワードを入力します。
2. IAM Identity Center コンソールを開きます。
3. IAM Identity Center を有効にするで、[有効化] を選択します。

4. IAM Identity Center には AWS Organizations が必要です。組織をまだ設定していない場合は、AWS で組織を作成するかどうかを選択する必要があります。このプロセスを完了するには、[AWS 組織の作成] を選択します。

   AWS Organizations により、管理アカウントに関連付けられたアドレスに検証 E メールが自動的に送信されます。検証 E メールの受信には時間がかかる場合があります。24 時間以内に E メールアドレスを検証します。

> **Note**
>
> マルチアカウント環境を使用している場合は、委任された管理を設定することをお勧めします。委任された管理では、AWS Organizations の管理アカウントへのアクセスを必要とするユーザーの数を制限できます。詳細については、「AWS IAM Identity Center ユーザーガイド」の「委任された管理」を参照してください。

ステップ 2: ID ソースを選択する

IAM Identity Center の ID ソースは、ユーザーやグループがどこで管理されているかを定義します。ID ソースとして以下のいずれかを選択できます。

- IAM Identity Center ディレクトリ — IAM Identity Center を初めて有効にすると、デフォルトの ID ソースとして IAM Identity Center ディレクトリで自動的に設定されます。ここでは、ユーザーとグループを作成し、AWS アカウントやアプリケーションへのアクセスレベルを割り当てることができます。
- Active Directory — AWS Directory Service または Active Directory (AD) のセルフマネージドディレクトリを使用した AWS Managed Microsoft AD ディレクトリのいずれかでユーザー管理を継続する場合は、このオプションを選択します。
- 外部 ID プロバイダー — Okta や Azure アクティブディレクトリなどの外部 ID プロバイダー (IdP) でユーザーを管理したい場合は、このオプションを選択します。

IAM Identity Center を有効にしたら、ID ソースを選択する必要があります。選択する ID ソースによって、シングルサインオンアクセスを必要とするユーザーとグループを IAM Identity Center が検索する場所が決まります。ID ソースを選択したら、ユーザーを作成または指定し、そのユーザーに AWS アカウント の管理アクセス許可を割り当てます。

> **Important**
>
> Active Directory または外部 ID プロバイダー (IdP) ですでにユーザーとグループを管理している場合は、IAM Identity Center を有効にして ID ソースを選択する際に、この ID ソースの接続を検討することをお勧めします。これは、ユーザーやグループをデフォルトの Identity Center ディレクトリに作成して割り当てを行う前に実行する必要があります。すでに 1 つの ID ソースでユーザーとグループを管理している場合、別の ID ソースに変更すると、IAM Identity Center で設定したユーザーとグループの割り当てがすべて削除される可能性があります。この場合、IAM Identity Center の管理ユーザーを含むすべてのユーザーが、AWS アカウント とアプリケーションへのシングルサインオンアクセスを失います。

トピック

Active Directory または別の IdP に接続してユーザーを指定する

すでに Active Directory または外部 ID プロバイダー (IdP) を使用している場合は、以下のトピックがディレクトリを IAM Identity Center に接続するのに役立ちます。

AWS Managed Microsoft AD ディレクトリ、Active Directory のセルフマネージドディレクトリ、または外部 IdP を IAM Identity Center に接続できます。Active Directory 内の AWS Managed Microsoft AD ディレクトリまたはセルフマネージドディレクトリを接続する予定がある場合は、Active Directory の設定が Active Directory または外部 IdP に示されている前提条件を満たしていることを確認してください。

> **Note**
>
> セキュリティのベストプラクティスとして、多要素認証を有効にすることを強くお勧めします。Active Directory 内の AWS Managed Microsoft AD ディレクトリまたはセルフマネージドディレクトリを接続する予定で、AWS Directory Service で RADIUS MFA を使用していない場合は、IAM Identity Center で MFA を有効にします。外部 ID プロバイダーを使用する予定の場合は、IAM Identity Center ではなく外部 IdP が MFA 設定を管理することに注意してください。IAM Identity Center の MFA では、外部 IdPs による使用はサポートされていませ

ん。詳細については、「AWS IAM Identity Center ユーザーガイド」の「MFA の有効化」を参照してください。

AWS Managed Microsoft AD

1. 「Microsoft Active Directory への接続」のガイダンスを確認してください。
2. 「AWS Managed Microsoft AD のディレクトリを IAM Identity Center に接続する」の手順を実行します。
3. 管理アクセス許可を付与したいユーザーを IAM Identity Center と同期するように Active Directory を設定します。詳細については、「管理ユーザーを IAM Identity Center に同期する」を参照してください。

Active Directory のセルフマネージドディレクトリ

1. 「Microsoft Active Directory への接続」のガイダンスを確認してください。
2. 「Active Directory のセルフマネージドディレクトリを IAM Identity Center に接続する 」の手順を実行します。
3. 管理アクセス許可を付与したいユーザーを IAM Identity Center と同期するように Active Directory を設定します。詳細については、「IAM Identity Center の管理ユーザーを同期する」を参照してください。

外部 IdP

1. 「外部 ID プロバイダーに接続する」のガイダンスを確認してください。
2. 「外部 ID プロバイダーに接続する方法」の手順を実行します。
3. IAM Identity Center にユーザーをプロビジョニングするように IdP を設定します。

> **Note**
>
> IdP から IAM Identity Center へのすべてのワークフォース ID のグループベースの自動プロビジョニングを設定する前に、管理アクセス許可を付与したい 1 人のユーザーを IAM Identity Center に同期させることをお勧めします。

管理ユーザーを IAM Identity Center と同期します。

ディレクトリを IAM Identity Center に接続したら、管理アクセス許可を付与するユーザーを指定し、そのユーザーをディレクトリから IAM Identity Center に同期できます。

1. IAM Identity Center コンソールを開きます。
2. [設定] を選択します。
3. [設定] ページで、[ID ソース] タブを選択し、[アクション] を選択し、[同期を管理] を選択します。
4. [同期を管理] ページで、[ユーザー] タブを選択し、次に [ユーザーとグループを追加] を選択します。
5. [ユーザー] タブで、[ユーザー] に正確なユーザー名を入力した上で、[追加] を選択します。
6. [追加したユーザーとグループ] で、次の操作を行います。
   a. 管理アクセス許可を付与するユーザーが指定されていることを確認します。
   b. ユーザー名の左にあるチェックボックスをオンにします。
   c. [送信] を選択します。
7. [同期の管理] ページで、指定したユーザーが同期対象のユーザーリストに表示されます。
8. ナビゲーションペインで [ユーザー] を選択します。
9. [ユーザー] ページでは、指定したユーザーがリストに表示されるまでに時間がかかる場合があります。ユーザーリストを更新するには、[更新] アイコンをクリックします。

この時点では、ユーザーは管理アカウントにアクセスできません。このアカウントへの管理アクセス許可を設定するには、管理アクセス許可セットを作成し、その許可セットにユーザを割り当てます。

次のステップ: ステップ 3: 管理アクセス許可セットを作成する

デフォルトディレクトリを使用して IAM Identity Center でユーザーを作成します。

IAM Identity Center を初めて有効にすると、デフォルトの ID ソースとして IAM Identity Center ディレクトリが自動的に設定されます。IAM Identity Center でユーザーを作成するには、以下のステップを完了します。

1. [ルートユーザー] を選択し、AWS アカウント の E メールアドレスを入力して、アカウント所有者として AWS Management Console にサインインします。次のページでパスワードを入力します。
2. IAM Identity Center コンソールを開きます。
3. 「ユーザーの追加」の手順に従ってユーザーを作成します。

   ユーザーの詳細を指定すると、パスワード設定手順を記載した E メールを送信するか (これはデフォルトのオプションです)、ワンタイムパスワードを生成できます。メールを送信する場合、アクセス可能な E メールアドレスを必ず指定します。
4. ユーザーを追加したら、この手順に戻ります。パスワード設定手順を記載した E メールを送信するというデフォルトのオプションをそのまま使用した場合は、次の操作を行います。

   a. 「AWS シングルサインオンへの招待」という件名の E メールが届きます。招待メールを開き、[招待を承諾] を選択します。
   b. [新規ユーザー登録] ページで、パスワードを入力して確認し、[新しいパスワードを設定] を選択します。

   > **Note**
   > 必ずパスワードを保存してください。後で ステップ 5: 管理者の認証情報を使用して AWS アクセスポータルにサインインする に必要になります。

この時点で、ユーザーには管理アカウントへのアクセス権がありません。このアカウントへの管理アクセス許可を設定するには、管理アクセス許可セットを作成し、その許可セットにユーザを割り当てます。

次のステップ: ステップ 3: 管理アクセス許可セットを作成する

ステップ 3: 管理アクセス許可セットを作成する

IAM Identity Center に保存されているアクセス権限セットは、ユーザーおよびグループが持つ AWS アカウント へのアクセスのレベルを定義します。以下の手順を実行して、管理アクセス許可を付与する許可セットを作成します。

1. [ルートユーザー] を選択し、AWS アカウント の E メールアドレスを入力して、アカウント所有者として AWS Management Console にサインインします。次のページでパスワードを入力します。

2. IAM Identity Center コンソールを開きます。
3. IAM Identity Center のナビゲーションペインの [マルチアカウントのアクセス許可] で、[許可セット] を選択します。
4. [アクセス許可セットの作成] を選択します。
5. ステップ 1: 許可セットの種類の選択 では、[許可セットの種類の選択] ページで、デフォルト設定のまま [次へ] を選択します。デフォルト設定では、管理者アクセスの事前定義済み許可セットを使用して、AWS サービスとリソースへのフルアクセスを付与します。

   > **Note**
   >
   > 定義済みの管理者アクセス許可セットは、管理者アクセス AWS 管理ポリシーを使用します。

6. ステップ 2: 許可セットの詳細を指定するでは、[許可セットの詳細の指定] ページで、デフォルト設定のまま [次へ] を選択します。デフォルト設定では、セッションは 1 時間に制限されています。
7. ステップ 3: レビューと作成では、[レビューと作成] ページで次の操作を行います。
   1. 許可セットタイプを確認し、管理者アクセスであることを確認します。
   2. AWS マネージドポリシーを確認し、管理者アクセスであることを確認します。
   3. [作成] を選択します。

ステップ 4: 管理ユーザーの AWS アカウント アクセスを設定する

IAM Identity Center で管理ユーザーの AWS アカウント アクセスを設定するには、そのユーザーを管理者アクセス許可セットに割り当てる必要があります。

1. [ルートユーザー] を選択し、AWS アカウント の E メールアドレスを入力して、アカウント所有者として AWS Management Console にサインインします。次のページでパスワードを入力します。
2. IAM Identity Center コンソールを開きます。
3. ナビゲーションペインの [マルチアカウントのアクセス許可] で、[AWS アカウント] を選択します。

4. [AWS アカウント] ページには、組織のツリービューリストが表示されます。管理者アクセスを割り当てる AWS アカウント の横にあるチェックボックスをオンにします。組織内に複数のアカウントがある場合は、管理アカウントの横にあるチェックボックスをオンにします。
5. [ユーザーまたはグループの割り当て] を選択します。
6. ステップ 1: ユーザーとグループの選択では、[ユーザーとグループを「*AWS-account-name*」に割り当てる] ページで、次の操作を行います。

   1. ユーザータブで、管理アクセス許可を付与するユーザーを選択します。

      結果をフィルタリングする場合は、検索ボックスに目的のユーザーの名前を入力します。

   2. 正しいユーザーが選択されていることを確認したら、[次へ] を選択します。
7. ステップ 2: 許可セットの選択では、[*#AWS-account-name############*] ページの [許可セット] で、[管理者アクセス] 許可セットを選択します。
8. [次へ] をクリックします。
9. ステップ 3: 確認して送信では、[「*AWS-account-name*」への割り当ての確認と送信] ページで、次の操作を行います。

   1. 選択したユーザーと許可セットを確認します。
   2. 管理者アクセス許可セットに正しいユーザーが割り当てられていることを確認したら、[送信] を選択します。

   > **Important**
   >
   > ユーザーへの割り当てプロセスが完了するまでに数分かかることがあります。プロセスが正常に完了するまでこのページを開いたままにします。

10. 以下のいずれかに当てはまる場合は、「MFA を有効にする」の手順に従って IAM Identity Center の MFA を有効にします。

    - ID ソースとしてデフォルトの Identity Center ディレクトリを使用しています。
    - Active Directory 内の AWS Managed Microsoft AD ディレクトリまたはセルフマネージドディレクトリを ID ソースとして使用していますが、AWS Directory Service では RADIUS MFA を使用していません。

> **Note**
>
> 外部 ID プロバイダーを使用している場合は、IAM Identity Center ではなく外部 IdP が MFA 設定を管理することに注意してください。IAM Identity Center の MFA では、外部 IdPs による使用はサポートされていません。

管理ユーザーのアカウントへのアクセス権をセットアップすると、対応する IAM ロールが IAM Identity Center により作成されます。この IAM Identity Center が制御するロールは、関連する AWS アカウント に作成され、アクセス許可セットで指定されたポリシーがアタッチされています。

ステップ 5: 管理者の認証情報を使用して AWS アクセスポータルにサインインする

次の手順を実行して、管理ユーザーの認証情報を使用して AWS アクセスポータルにサインインできること、および AWS アカウント にアクセスできることを確認します。

1. [ルートユーザー] を選択し、AWS アカウント の E メールアドレスを入力して、アカウント所有者として AWS Management Console にサインインします。次のページでパスワードを入力します。
2. https://console.aws.amazon.com/singlesignon/ で AWS IAM Identity Center コンソールを開きます。
3. ナビゲーションペインで、[ダッシュボード] を選択します。
4. [ダッシュボード] ページの [設定概要] で、AWS アクセスポータル URL をコピーします。
5. 別のブラウザを開き、コピーした AWS アクセスポータル URL を貼り付け、Enter キーを押します。
6. 次のいずれかの方法でサインインします。
   - Active Directory または外部 ID プロバイダー (IdP) を ID ソースとして使用している場合は、IAM アイデンティティセンターの [管理者アクセス] 許可セットに割り当てた Active Directory または IdP ユーザーの認証情報を使用してサインインします。
   - ID ソースとしてデフォルトの IAM Identity Center ディレクトリを使用している場合は、ユーザーを作成したときに指定したユーザー名と、そのユーザーに指定した新しいパスワードを使用してサインインします。

7. サインインすると、ポータルに [AWS アカウント] アイコンが表示されます。
8. [AWS アカウント] アイコンを選択すると、そのアカウントに関連付けられているアカウント名、アカウント ID、および E メールアドレスが表示されます。
9. [管理者アクセス] 許可セットを表示するアカウントの名前を選択し、[管理者アクセス] の右側にある [マネージメントコンソール] リンクを選択します。

   サインインすると、ユーザに割り当てられている許可セットの名前が使用可能なロールとして AWS アクセスポータルに表示されます。このユーザーを `AdministratorAccess` 許可セットに割り当てたため、ロールは AWS アクセスポータル に「`AdministratorAccess/`*`username`*」と表示されます。
10. AWS マネージメントコンソールにリダイレクトされれば、AWS アカウント への管理者アクセスの設定は正常に完了しています。ステップ 10 に進みます。
11. AWS Management Console へのサインインと IAM Identity Center の設定に使用したブラウザに切り替え、AWS アカウント ルートユーザーからサインアウトします。

> **Important**
>
> AWS アクセスポータルにサインインするときは、管理ユーザーの認証情報の使用に関するベストプラクティスに従って、日常の作業にはルートユーザーの認証情報は使用しないことを強くお勧めします。

他のユーザーがアカウントやアプリケーションにアクセスできるようにし、IAM Identity Center を管理できるようにするには、IAM Identity Center を通じてのみ許可セットを作成して割り当ててください。

AWS アカウント の作成に関する問題のトラブルシューティング

ここに記載する情報は、AWS アカウント の作成に関係する問題のトラブルシューティングに役立ちます。

問題点

- 新しいアカウントを検証するための電話が AWS からかかってきません。
- 電話による AWS アカウント の検証をしようとすると、「最大失敗回数」が表示されます。
- 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

新しいアカウントを検証するための電話が AWS からかかってきません。

AWS アカウント を作成する際には、SMS テキストメッセージまたは音声通話を受信できる電話番号を指定する必要があります。番号の検証に使用する方法を指定します。

メッセージや通話が届かない場合、以下の点を確認します。

- サインアッププロセスで正しい電話番号を入力し、正しい国番号を選択しました。
- 携帯電話を使用している場合、SMS テキストメッセージまたは通話を受信するための電波があることを確認します。
- 支払い方法として正しい方法を入力してあります。

本人確認プロセスを完了するのための SMS テキストメッセージまたは電話が届かない場合、手動で AWS Support をアクティブにするには AWS アカウント が役立ちます。以下のステップを使用します。

1. AWS アカウント に提供した電話番号に出られることを確認します。
2. AWS Support コンソールを開いて [ケースの作成] を選択します。
   a. [アカウントおよび請求サポート] を選択します。
   b. [タイプ] で [アカウント] を選択します。
   c. [カテゴリー] で [アクティベーション] を選択します。

d. [ケースの説明] セクションで、連絡可能な日時を指定します。
e. [連絡先オプション] セクションで [連絡先方法] に [チャット] を選択します。
f. [送信] を選択します。

> **Note**
> AWS アカウント がまだアクティブになっていなくても AWS Support でケースを作成できます。

電話による AWS アカウント の検証をしようとすると、「最大失敗回数」が表示されます。

AWS Support は、アカウントを手動でアクティブにしようとする際に役立ちます。以下の手順に従います。

1. アカウントの作成時に指定した E メールアドレスとパスワードを使用して AWS アカウント にサインインします。
2. AWS Support コンソールを開いて [ケースの作成] を選択します。
3. [アカウントおよび請求サポート] を選択します。
4. [タイプ] で [アカウント] を選択します。
5. [カテゴリー] で [アクティベーション] を選択します。
6. [ケースの説明] セクションで、連絡可能な日時を指定します。
7. [連絡先オプション] セクションで [連絡先方法] に [チャット] を選択します。
8. [送信] を選択します。

AWS Support はユーザーに連絡し、手動で AWS アカウント をアクティブにしようと試みます。

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

アカウントのアクティベーションが遅れる場合があります。処理に 24 時間以上かかる場合は、次の点を確認してください。

- アカウントのアクティベーションプロセスを完了します。

必要な情報をすべて追加する前に、サインアッププロセスのウィンドウを閉じている場合は、[登録] ページを開きます。[既存の AWS アカウント にサインイン] を選択して、アカウント用に選択した E メールアドレスとパスワードを使用してサインインします。

- お支払い方法に関連する情報を確認してください。

  AWS Billing and Cost Management コンソールで、エラーの支払い方法をチェックします。

- 金融機関に問い合わせます。

  金融機関は、AWS からの承認リクエストを拒否することがあります。支払い方法に関連付けられた機関に連絡し、AWS からの承認リクエストを承認するよう依頼してください。金融機関によって承認されると、AWS はすぐに承認リクエストをキャンセルします。そのため、承認リクエストに対して請求されることはありません。承認リクエストは、金融機関からの明細書に小額料金 (通常 1 USD) として表示される場合があります。

- メールおよびスパムフォルダで追加情報のリクエストを確認します。
- 別のブラウザを試します。
- AWS Support に連絡します。

  AWS Support にお問い合わせください。既に試したトラブルシューティング手順について言及してください。

> **Note**
>
> AWS との通信において、クレジットカード番号などの機密情報を提供しないでください。