Identity and Access Management

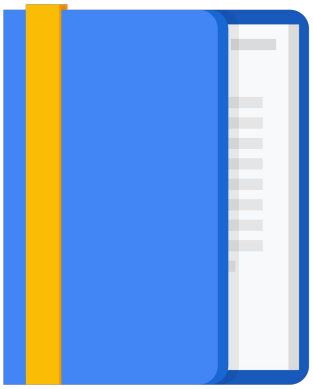
Mylene Biddle

このモジュールでは、Identity and Access Management（IAM）について説明します。

IAM は、メールのようなアドレス名、職種別のロール、きめ細かな権限設定を基盤とする高度なシステムです。他社が実装する IAM に精通している方は、より管理しやすく安全性の高い、Google の実装による IAM との違いをご確認ください。

アジェンダ

- Identity and Access Management（IAM）
- 組織
- ロール
- メンバー
- サービス アカウント
- IAM のベスト プラクティス
- ラボ



まずは IAM の概要を紹介します。次に、IAM のコンポーネントである組織、ロール、メンバー、サービス アカウントについて順に説明します。これらのコンセプトを日常の業務に適用するためのベスト プラクティスも紹介します。

最後に、ラボで IAM を実際に使用してみます。

Identity and Access Management の概要から始めましょう。

Identity and Access Management

ID アクセス管理とは何でしょうか。それは、アクセスの主体、アクション、対象リソースを指定する方法です。

主体というのは、個人、グループ、アプリケーションなどです。アクションは特定の権限または操作を指し、対象リソースは任意の Google Cloud サービスです。

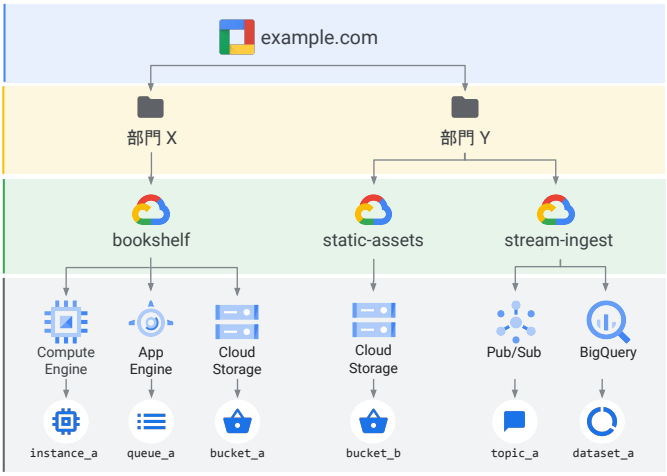
たとえば、「Compute 閲覧者」の権限（ロール）が付与されたとします。この場合、読み取り専用アクセス権が与えられ、Compute Engine リソースを取得して一覧表示することはできますが、そこに格納されているデータを読み取ることはできません。

IAM のオブジェクト

組織　フォルダ　プロジェクト　リソース　ロール　メンバー

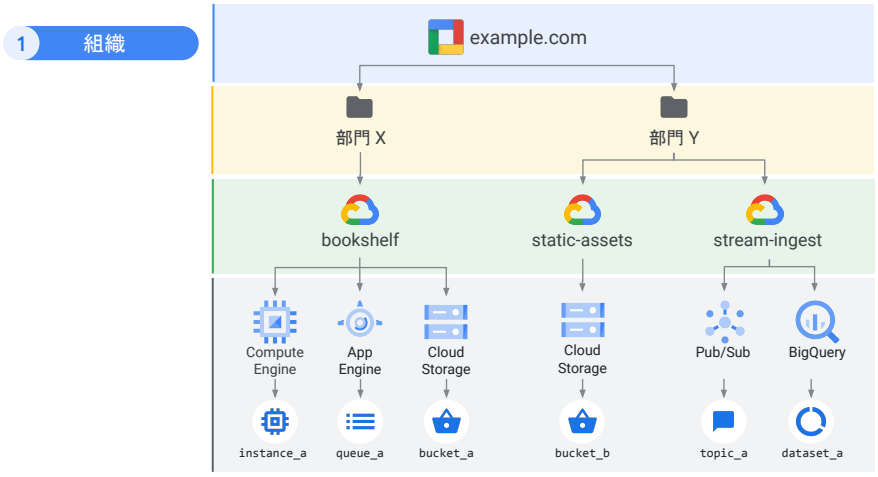
このスライドに示されているように、IAM はさまざまなオブジェクトで構成されています。このモジュールでは、これらについて個別に説明していきます。それぞれのオブジェクトがどこに該当するのかを理解できるよう、IAM のポリシーとリソース階層を確認しましょう。

IAM リソース階層



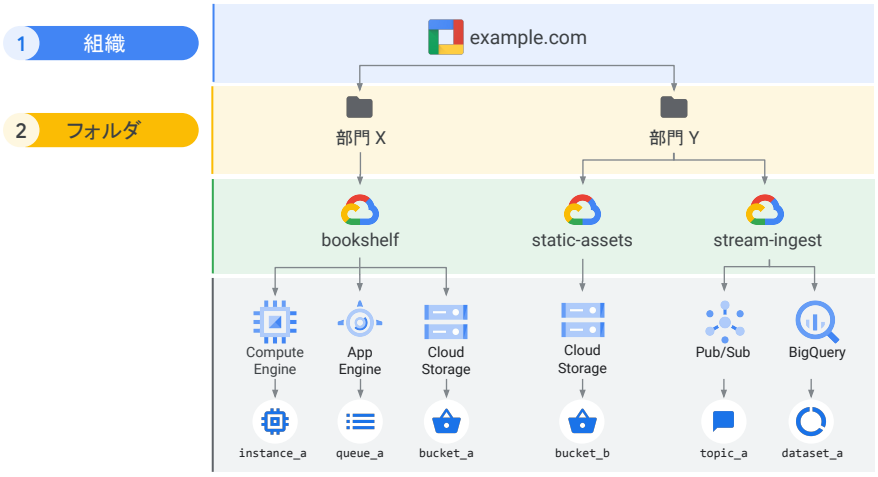
Google Cloud リソースは、このツリー構造に示されているように、階層構造になっています。

IAM リソース階層



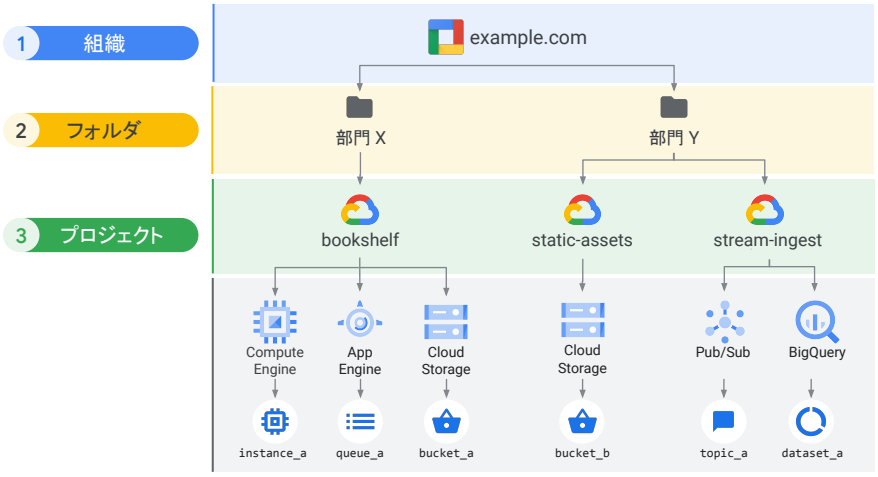
組織ノードは、この階層のルートノードです。

IAM リソース階層



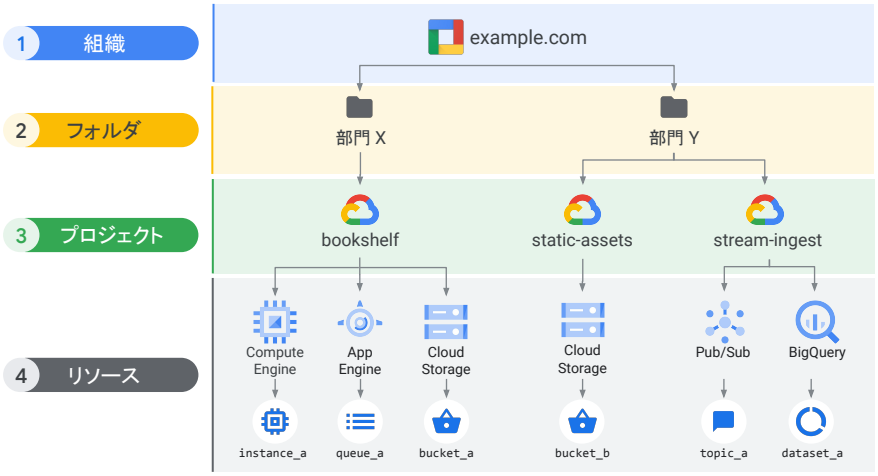
フォルダは組織の子です。

IAM リソース階層



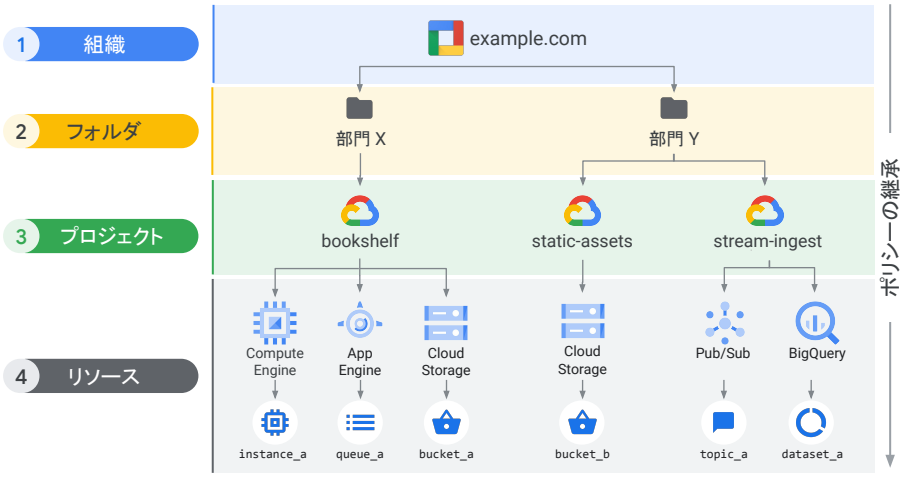
プロジェクトはフォルダの子です。

IAM リソース階層



個々のリソースはプロジェクトの子です。各リソースの親は　1 つだけです。

IAM リソース階層



組織リソースは会社を表します。このレベルで付与された　IAM ロールは、組織内のすべてのリソースに継承されます。

フォルダ リソースでは部門を表すことができます。このレベルで付与された　IAM ロールは、そのフォルダに含まれるすべてのリソースに継承されます。

プロジェクトは社内の信頼境界を表します。同一プロジェクト内のサービスには、同じデフォルトの信頼レベルが設定されます。

アジェンダ

Identity and Access Management（IAM）

組織

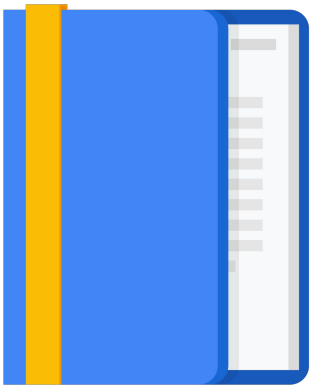
ロール

メンバー

サービス アカウント

IAM のベスト プラクティス

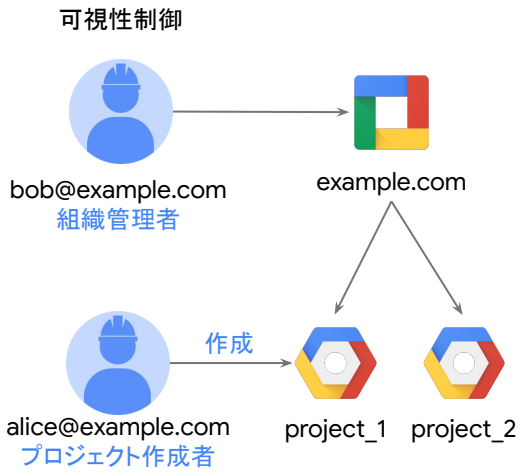
ラボ



組織ノードについて、さらに詳しく学習しましょう。

組織ノード

- 組織ノードは Google Cloud リソースのルートノード
- 組織のロール:
  - 組織管理者: すべてのクラウドリソースを管理、監査に便利
  - プロジェクト作成者: プロジェクトの作成(プロジェクトの作成が可能なユーザー)を管理



前述のとおり、組織リソースは GCP リソース階層のルートノードです。このノードには、組織管理者をなどの多くのロールがあります。

組織管理者は、組織に属するすべてのリソースを管理するためのアクセス権をユーザー(ここでは Bob)に付与します。これは監査を行う場合に便利です。

また、プロジェクト作成者のロールを付与されたユーザー(ここでは Alice)は、組織内にプロジェクトを作成できます。ここでプロジェクト作成者のロールを紹介したのは、組織レベルでも適用できるからです。組織レベルで適用すると、組織内のすべてのプロジェクトに継承されます。

組織の作成と管理

- **Google Workspace** または **Cloud Identity** のアカウントが Google Cloud プロジェクトを作成すると、組織が作成される
- **Workspace** または **Cloud Identity** の特権管理者:
  - 一部のユーザーに**組織管理者**のロールを割り当てる
  - 復旧に関する連絡窓口になる
  - Workspace アカウント、Cloud Identity アカウント、組織リソースのライフサイクルを管理する
- **組織管理者:**
  - IAM ポリシーを定義する
  - リソース階層の構造を決定する
  - IAM ロールを通じてネットワーキング、課金、リソース階層などの重要なコンポーネントに対する責任を委任する

G Suite は Google Workspace となりました

組織リソースは、Google Workspace アカウントや Cloud Identity アカウントと密接に関連しています。

組織の作成と管理

- **Google Workspace** または **Cloud Identity** のアカウントが Google Cloud プロジェクトを作成すると、組織が作成される
- **Workspace** または **Cloud Identity** の特権管理者:
  - 一部のユーザーに**組織管理者**のロールを割り当てる
  - 復旧に関する連絡窓口になる
  - Workspace アカウント、Cloud Identity アカウント、組織リソースのライフサイクルを管理する
- **組織管理者:**
  - IAM ポリシーを定義する
  - リソース階層の構造を決定する
  - IAM ロールを通じてネットワーキング、課金、リソース階層などの重要なコンポーネントに対する責任を委任する

G Suite は Google Workspace となりました

Workspace アカウントや Cloud Identity アカウントを持つユーザーが Google Cloud プロジェクトを作成すると、組織リソースが自動的にプロビジョニングされます。プロビジョニング後、Google Cloud は Workspace または Cloud Identity の特権管理者に、組織リソースが使用可能になったことを通知します。特権管理者アカウントは、組織およびその下のあらゆるリソースに対して広範な制御を行えるため、慎重に使用する必要があります。

Workspace や Cloud Identity の特権管理者と Google Cloud 組織管理者は、設定プロセスと組織リソースのライフサイクル管理における重要なロールです。組織の構造やニーズによっても変わりますが、通常、この 2 つのロールは別々のユーザーまたはグループに割り当てられます。

組織の作成と管理

- **Google Workspace** または **Cloud Identity** のアカウントが Google Cloud プロジェクトを作成すると、組織が作成される
- **Workspace** または **Cloud Identity** の特権管理者:
  - 一部のユーザーに**組織管理者**のロールを割り当てる
  - 復旧に関する連絡窓口になる
  - Workspace アカウント、Cloud Identity アカウント、組織リソースのライフサイクルを管理する
- **組織管理者:**
  - IAM ポリシーを定義する
  - リソース階層の構造を決定する
  - IAM ロールを通じてネットワーキング、課金、リソース階層などの重要なコンポーネントに対する責任を委任する

G Suite は Google Workspace となりました

Google Cloud 組織の設定における Workspace または Cloud Identity の特権管理者の業務は、次のとおりです。

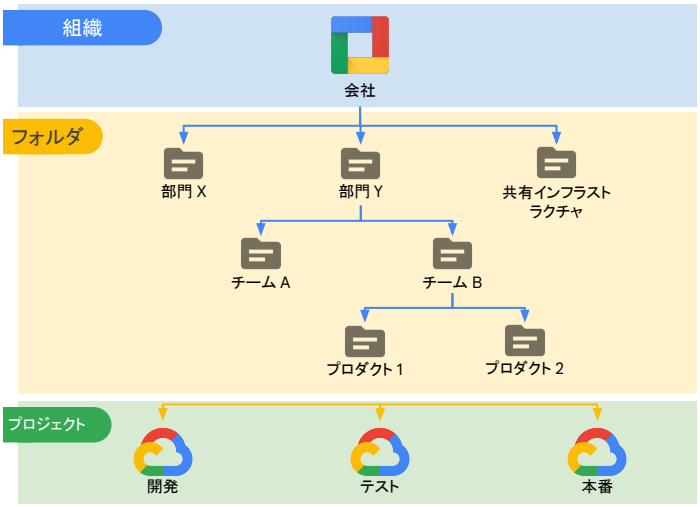
- 一部のユーザーに組織管理者のロールを割り当てます。
- 復旧に関する連絡窓口になります。
- Workspace アカウント、Cloud Identity アカウント、組織リソースのライフサイクルを管理します。

組織管理者の業務は次のとおりです。

- IAM ポリシーを定義します。
- リソース階層の構造を決定します。
- IAM ロールを通じてネットワーキング、課金、リソース階層などの重要なコンポーネントに対する責任を委任します。

最小権限の原則に従い、このロールには、その他のアクション（フォルダの作成など）を実行する権限はありません。これらの権限を取得するには、組織管理者がアカウントに追加のロールを割り当てる必要があります。組織の作成と管理について詳しくは、この動画のリンク セクションに記載されている入門ガイドをご覧ください。
[https://cloud.google.com/resource-manager/docs/creating-managing-organization#adding_an_organization_admin]

フォルダ



追加のグループ化メカニズム、プロジェクト間の分離境界:

- 異なる法人
- 部門
- チーム

フォルダを使用して管理権限を委任可能

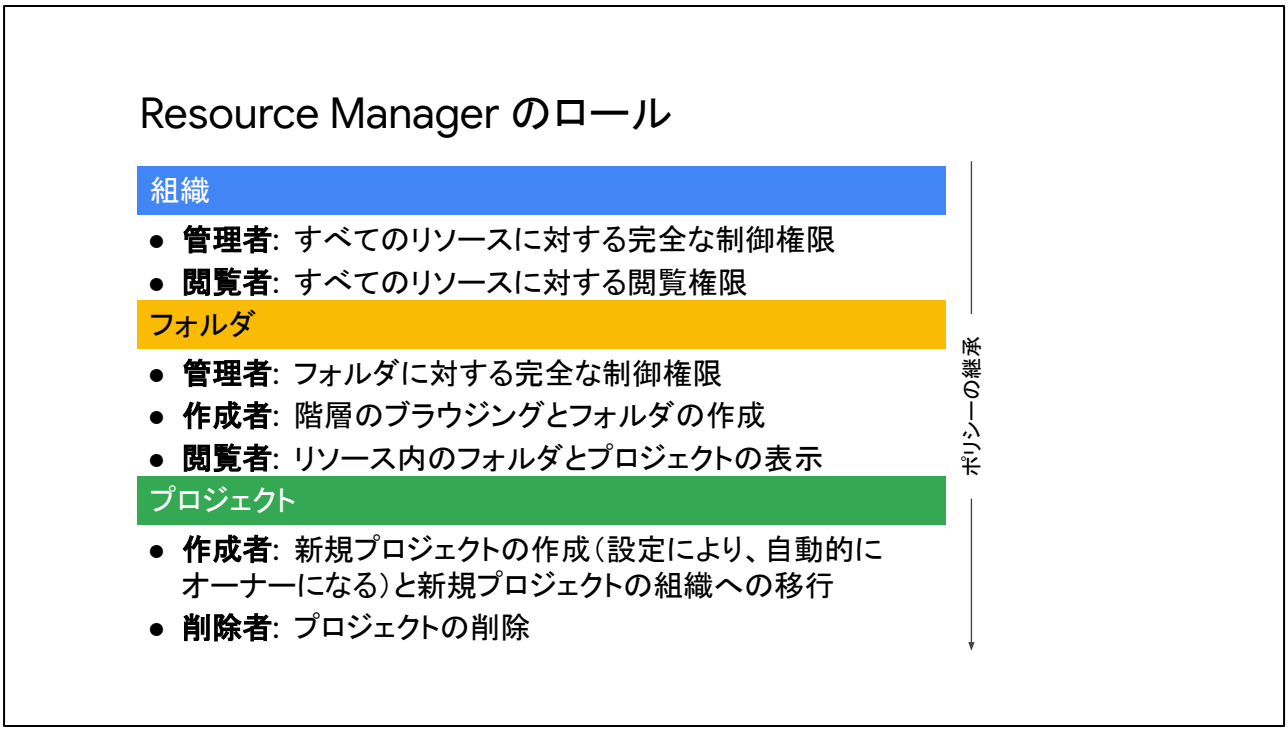
フォルダは組織内のサブ組織を表すこともあるため、フォルダについてもう少し説明します。

フォルダは、追加のグループ化メカニズムや、プロジェクト間の分離境界となります。フォルダを使用して、社内の異なる法人、部門、チームをモデル化できます。たとえば、最初のレベルのフォルダで、組織の主要部門(部門　X、部門 Y など)を表すことができます。

フォルダ内にはプロジェクトや他のフォルダを作成できるので、サブフォルダで他のチーム(チーム A、チーム B など)を表すことができます。

さらに、各チームのフォルダにサブフォルダを追加して、アプリケーション(プロダクト　1、プロダクト 2 など)を表すこともできます。

フォルダを使用すると、管理権限を委任できます。たとえば、部門の各責任者にその部門のすべての GCP リソースに対する完全なオーナー権限を付与できます。同様に、フォルダによってリソースに対するアクセス権を制限できます。これにより、ある部門のユーザーに、その部門のフォルダ内に限り GCP リソースへのアクセスとリソースの作成を許可できます。



他の Resource Manager のロールを見てみましょう。先ほど述べたように、ポリシーは上から下へ継承されます。

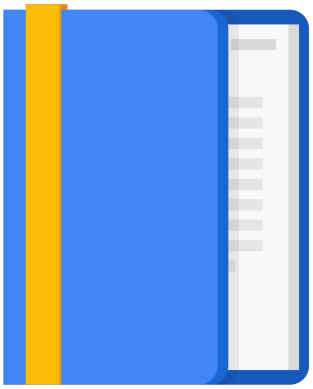
組織ノードには閲覧者のロールもあります。このロールによって、組織内の全リソースへの閲覧権限が付与されます。

フォルダノードにも組織のロールと同様のロールが複数ありますが、これらはフォルダ内のリソースに適用されます。したがって、管理者のロールではフォルダに対する完全な制御、作成者のロールでは階層の参照とフォルダの作成、閲覧者のロールではリソース内のフォルダとプロジェクトの表示が可能です。

同様に、プロジェクトにも、新規プロジェクトを作成できる作成者のロールがあります。プロジェクトを作成したユーザーが自動的にそのプロジェクトのオーナーになります。プロジェクトの削除権限を付与するプロジェクト削除のロールもあります。

アジェンダ

- Identity and Access Management（IAM）
- 組織
- **ロール**
- メンバー
- サービス アカウント
- IAM のベスト プラクティス
- ラボ

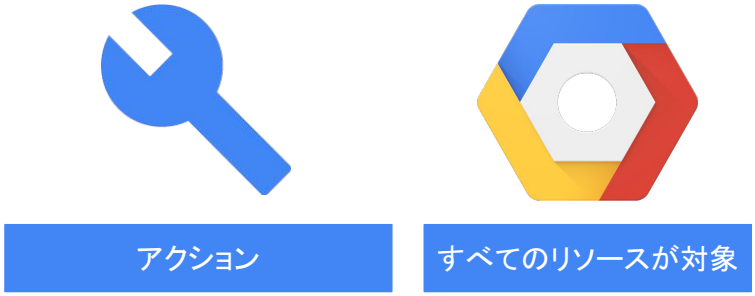


ロールについて、もう少し説明しましょう。ロールは、 IAM の「アクション」と「対象リソース」の部分を定義します。

3 種類の IAM ロール

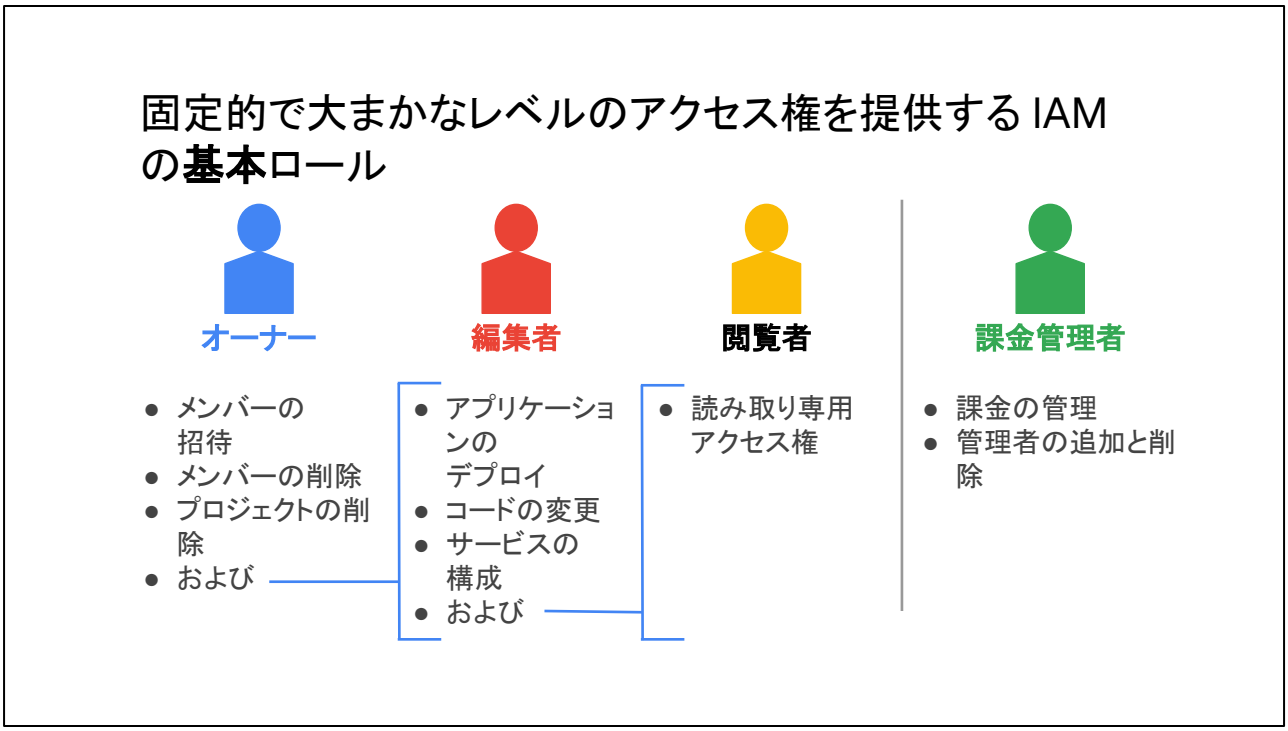
Cloud IAM には、基本ロール、事前定義ロール、カスタムロールという 3 種類のロールがあります。

プロジェクト内のすべての Google Cloud サービスに適用される IAM の**基本**ロール



基本ロールは、Cloud Console に当初からあるロールですが、その範囲は多岐にわたります。

Google Cloud プロジェクトに適用すると、そのプロジェクト内のすべてのリソースに適用されます。



言い換えると、IAM の基本ロールは固定的で大まかなレベルのアクセス権を提供します。

基本ロールには、オーナー、編集者、閲覧者のロールがあります。

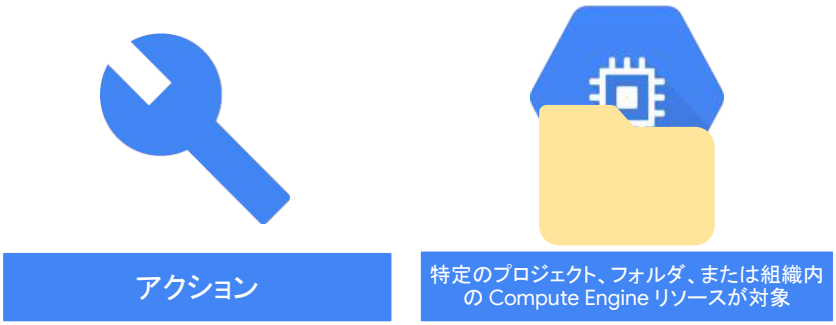
- オーナーには、完全な管理者権限があります。これには、メンバーの追加と削除、プロジェクトの削除などの権限が含まれます。
- 編集者のロールには、変更と削除の権限があります。これにより、デベロッパーはアプリケーションをデプロイして、そのリソースの変更や構成を行えます。
- 閲覧者のロールには、読み取り専用アクセス権があります。

これらのロールは入れ子構造になっています。つまり、オーナーのロールには編集者のロールの権限が含まれ、編集者のロールには閲覧者のロールの権限が含まれます。

そのほかに課金管理者のロールもあります。このロールには、課金を管理する権限、管理者を追加または削除する権限がありますが、プロジェクト内のリソースを変更する権限はありません。

各プロジェクトには、複数のオーナー、編集者、閲覧者、課金管理者を割り当てることができます。

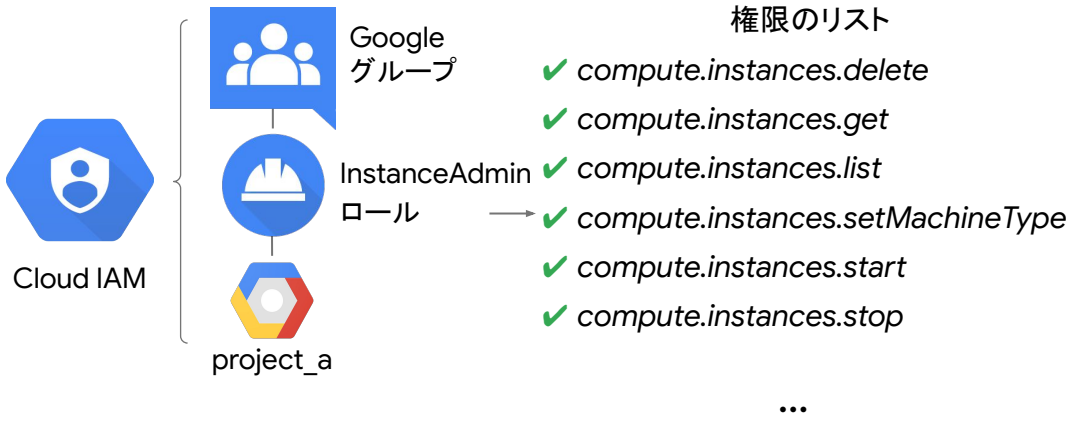
プロジェクト内の特定の GCP サービスに適用される IAM の**事前定義**ロール



GCP サービスには、それぞれ独自の事前定義ロールのセットが用意されており、それらのロールを適用できる対象が定義されています。これにより、特定の　GCP リソースに対するアクセス権を詳細に設定できるため、他のリソースへの不正なアクセスを防ぐことができます。

通常、意味のある操作を行うには複数の権限が必要なので、これらのロールは権限の「コレクション」になっています。

特定のサービスに対してきめ細かな権限を付与できる IAM の**事前定義**ロール



たとえば、ここに示されているように、ユーザーのグループに project_a に対する InstanceAdmin のロールを付与すると、そのグループのユーザーにはスライドの右側に一覧表示されている権限を含むすべての Compute Engine の権限が付与されます。これらの権限をロールにまとめることで、管理しやすくなります。こうした権限自体は API のクラスとメソッドに相当します。

たとえば compute.instances.start は、サービス、リソース、動詞に分けることができ、停止した Compute Engine インスタンスを起動するために使用される権限であることを表しています。

通常、これらの権限はアクションに対応する REST API と連携しています。

Compute Engine の IAM ロール

ロールのタイトル	説明
Compute 管理者	すべての Compute Engine リソース（compute.*）に対する完全な制御権限
ネットワーク管理者	ネットワーキング リソースを作成、変更、削除する権限（ファイアウォール ルールと SSL 証明書を除く）
ストレージ管理者	ディスク、イメージ、スナップショットを作成、変更、削除する権限

Compute Engine には、いくつかの IAM 事前定義ロールがあります。そのうちの 3 つを見ていきましょう。

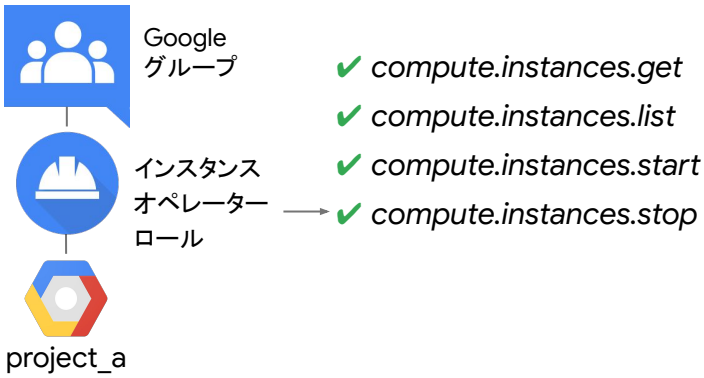
- Compute 管理者のロールでは、すべての Compute Engine リソースを完全に制御できます。このロールには、「compute」で始まるすべての権限が含まれます。したがって、あらゆる種類の Compute Engine リソースに対するすべてのアクションが許可されます。
- ネットワーク管理者のロールには、ネットワーキング リソースの作成、変更、削除を行う権限が含まれます。例外として、ファイアウォール ルールと SSL 証明書にはこれらの権限は適用されませんが、読み取り専用でアクセスすることはできます。エフェメラル IP アドレスを表示するためにインスタンスに読み取り専用でアクセスすることもできます。
- ストレージ管理者のロールには、ディスク、イメージ、スナップショットを作成、変更、削除する権限が含まれます。

たとえば、自社のプロジェクト イメージの管理者にプロジェクトの編集者のロールを付与したくない場合は、そのアカウントにプロジェクトのストレージ管理者のロールを付与します。Compute Engine の事前定義ロールの一覧については、この動画のリンク セクションをご覧ください。[https://cloud.google.com/compute/docs/access/iam#iam_roles]

さて、ロールは職務を抽象的に表現するためのものなので、実際の業務に合わせてカス

タマイズされています。しかし、これらのロールのいずれかで権限が不足している場合や、さらにきめ細かいロールが必要な場合はどうすればよいでしょうか。

詳細な権限セットを定義できる IAM の **カスタム**ロール



そのような場合に使用するのがカスタムロールです。多くの企業は「最小権限」モデルを使用しています。つまり、組織内の各ユーザーには、職務に必要な最小限の権限しか与えられません。

たとえば、「インスタンス オペレーター」のロールを定義して、一部のユーザーに Compute Engine 仮想マシンの起動と停止を行う権限を付与する一方、再構成はできないようにする場合などに、カスタムロールを使用できます。

デモ

カスタムロール

Philipp Maier

GCP でカスタムロールを作成する方法を紹介します。
ここでの目標は、Compute Engine 仮想マシンを起動、停止できるが、再構成はできない インスタンス オペレーター ロールを作成することです。

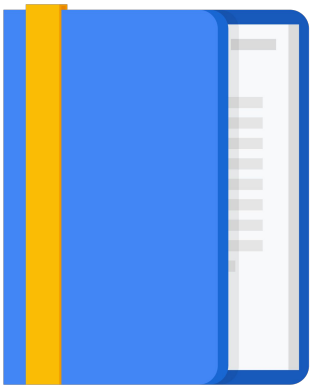
[デモ]

このように、GCP では簡単にカスタムロールを作成できます。別の方法として、インスタンス管理者ロールをベースとして使用し、ロールに付与したくない権限をそこから削除することもできます。

カスタムロールは Google によって管理されないため、新しい権限、機能、サービスが GCP に追加されても、こうしたカスタムロールが自動的に更新されることはありません。

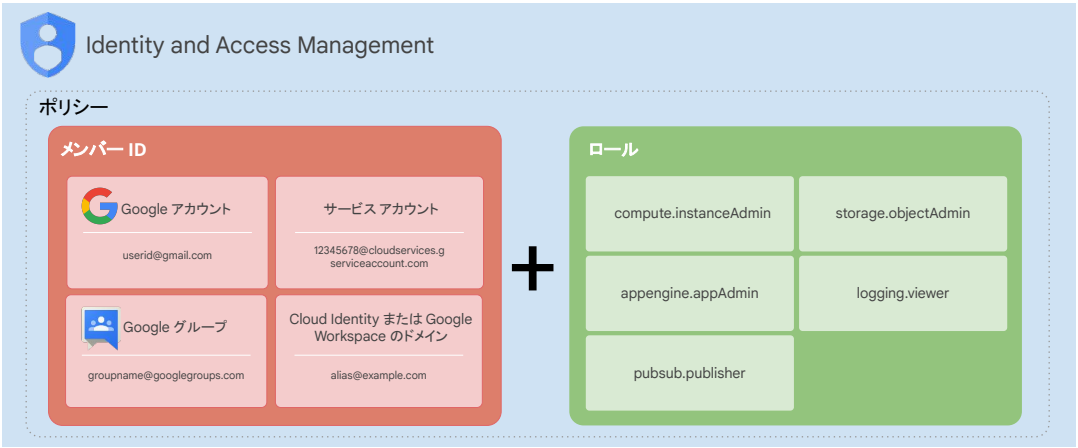
アジェンダ

Identity and Access Management（IAM）
組織
ロール
メンバー
サービス アカウント
IAM のベスト プラクティス
ラボ



メンバーについて、もう少し説明しましょう。メンバーは、対象リソースに対してアクションを起こす「主体」の部分を定義します。

メンバー



注: IAM を使用してユーザーやグループを作成、管理することはできません。

メンバーの種類は 5 つあります。Google アカウント、サービス アカウント、Google グループ、Google Workspace ドメイン、Cloud Identity ドメインです。

Google アカウントは、Google Cloud を操作するデベロッパー、管理者、または他のユーザーを表します。Google アカウントに関連付けられているメールアドレス（ gmail.com や他のドメインのアドレスなど）を、アカウントの ID として使用できます。Gmail でメールを受信しなくても、Google アカウントの登録ページから Google アカウントに新規ユーザーとして登録できます。

サービス アカウントは、個々のエンドユーザーではなく、アプリケーションに属するアカウントです。Google Cloud でホストされているコードを実行する際には、そのコードの実行で使用されるアカウントを指定します。必要な数のサービス アカウントを作成して、アプリケーションのさまざまな論理コンポーネントを表すことができます。

Google グループは、複数の Google アカウントやサービス アカウントを 1 つにまとめて、名前を付けたものです。各グループには、グループ固有のメールアドレスが関連付けられています。Google グループを使用すると、ユーザーの集合に対して簡単にアクセス ポリシーを適用できます。個々のユーザーやサービス アカウントごとにアクセス制御を付与または変更するのではなく、グループ全体に対して一度にアクセス制御を付与および変更できます。

Workspace ドメインは、組織の Workspace アカウントで作成されたすべての Google アカウントの仮想グループを表します。Workspace ドメインは組織のインターネット ドメイン名（example.com など）を表し、Workspace ドメインにユーザーを追加すると、この仮想グループ内のユーザー用に新しい Google アカウント（username@example.com など）が作成されます。

Workspace を利用していない Google Cloud のお客様も、Cloud Identity を介して同じ機能を利用できます。Cloud Identity では Google 管理コンソールを使用してユーザーやグループを管理できますが、Gmail、Google ドキュメント、Google ドライブ、Google カレンダーなどの Workspace のコラボレーション サービスは利用対象とならず、その分の料金を支払うこともありません。

IAM を使用してユーザーやグループを作成、管理することはできないのでご注意ください。ユーザーを作成、管理するには、代わりに Cloud Identity や Workspace を使用します。

[Cloud Identity: https://support.google.com/cloudidentity/answer/7319251?hl=ja]

IAM ポリシー

- ポリシーはバインィングのリストで構成されている

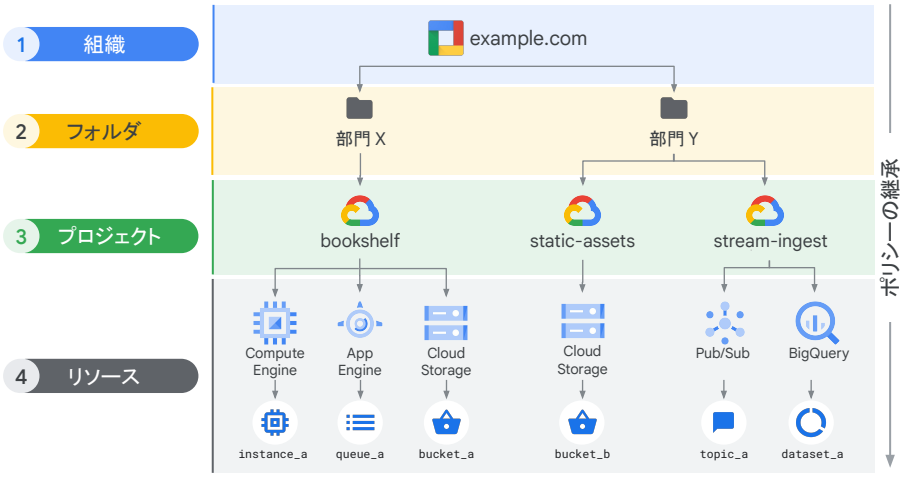
ポリシーはバインィングのリストで構成されています。

IAM ポリシー

- ポリシーはバインィングのリストで構成されている
- バインディングはメンバーのリストをロールにバインドする

バインディングはメンバーのリストをロールにバインドします。メンバーには、ユーザー　アカウント、Google グループ、Google ドメイン、サービス アカウントを指定できます。ロールは IAM で定義された権限の名前付きリストです。ここでもう一度　IAM リソース階層を見てみましょう。

IAM リソース階層



ポリシーは、リソースに関連付けられたアクセス　ステートメントの集合です。

各ポリシーには、ロールとそのメンバーのセットが含まれます。リソースは親リソースからポリシーを継承します。継承については次のように考えてください。リソース　ポリシーは、親とそのリソース自身のポリシーを合わせたもので、親ポリシーの方がリソース　ポリシーより制限が緩い場合は常に親ポリシーが優先されます。

IAM のポリシー階層は、常に Google Cloud リソース階層と同じパスに従います。つまり、リソース階層を変更すると、ポリシー階層も変更されます。たとえば、プロジェクトを別の組織に移動すると、そのプロジェクトの IAM ポリシーは新しい組織の IAM ポリシーを継承するように更新されます。

また、親のレベルで付与されたアクセス権を子のポリシーで制限することはできません。たとえば、部門 X で編集者のロールが付与され、bookshelf プロジェクト レベルで閲覧者のロールが付与された場合、bookshelf プロジェクトでも編集者のロールが付与されることになります。したがって、最小権限の原則に従うことがベスト　プラクティスとなります。この原則は、ID、ロール、リソースに当てはまります。リスクを抑えるためには、常にタスクに必要最小限のスコープを選んでください。

ロールの推奨事項を提供する Recommender を使用すると、過剰な権限を特定してプリンシパルから削除できるので、リソースのセキュリティ構成を改善できます。各ロールの推奨事項によって、プリンシパルに過剰な権限を付与しているロールの削除または置換が提案されます。大規模な環境の場合、これらの推奨事項を使用してプリンシパルが実際に必要な権限のみを持つようにすることで、最小権限の原則を徹底できます。

Recommender は、ポリシーの分析情報を使用して過剰な権限を特定します。ポリシーの分析情報は、プロジェクト、フォルダ、または組織での権限の使用状況に関する　ML ベースの分析結果です。

[Role recommendations: https://cloud.google.com/iam/docs/recommender-overview]

IAM Conditions

Google Cloud リソースに条件付きの属性ベースのアクセス制御を適用

- 構成された条件が満たされる場合にのみ ID（メンバー）に
  リソース アクセス権を付与
- リソースの IAM ポリシーのロール バインディングで条件を指定

IAM Conditions を使用すると、Google Cloud リソースに条件付きの属性ベースのアクセス制御を定義して適用できます。

IAM Conditions では、構成された条件が満たされる場合にのみ、 ID（メンバー）にリソースアクセス権を付与できます。たとえば、本番環境で問題が発生した場合にユーザーに対して一時的なアクセス権を構成したり、リソースへのアクセスを会社のオフィスからリクエストする従業員のみに制限したりできます。

条件は、リソースの IAM ポリシーのロール バインディングで指定します。条件が存在する場合、条件式が `true` に評価されたときに限りアクセス リクエストが許可されます。各条件式は一連の論理ステートメントであり、そこで 1 つまたは複数の属性を指定して検査できます。

組織のポリシー

組織のポリシーとは:

- 制限の構成

組織のポリシーは制限の構成です。

組織のポリシー

組織のポリシーとは:

- 制限の構成
- 必要な制限を含む制約を構成することで定義

組織のポリシーは、組織に必要な制限を含む制約を構成することで定義されます。

組織のポリシー

組織のポリシーとは:

- 制限の構成
- 必要な制限を含む制約を構成することで定義
- 組織ノード、フォルダ、プロジェクトに適用

組織のポリシーは、組織ノードと、そこに含まれるすべてのフォルダやプロジェクトに適用できます。対象のリソース階層ノードの子孫は、親に適用された組織のポリシーを継承します。

これらのポリシーの例外を指定することもできますが、組織ポリシー管理者のロールが必要です。

すでに別の企業ディレクトリがある場合

すでに別の企業ディレクトリがある場合はどうでしょう。どのようにしてユーザーとグループを Google Cloud に取り込むことができるでしょうか。

Google Cloud Directory Sync を使用すると、管理者はすでに使用しているものと同じユーザー名とパスワードで Google Cloud リソースにログインして管理できます。このツールは、既存の Active Directory または LDAP システムのユーザーとグループを Cloud Identity ドメインのユーザーとグループに同期します。

同期は一方向のみです。つまり、Active Directory や LDAP マップの情報は変更されません。Google Cloud Directory Sync は、同期ルールの設定後、スケジュール設定された同期を自動的に実行するように設計されています。

シングル サインオン（SSO）

- Cloud Identity を使用して SAML SSO を構成
- SAML2 がサポートされていない場合はサードパーティ ソリューションを使用（ADFS、Ping、Okta など）

Google Cloud では、シングル サインオン認証も利用できます。

すでに利用している ID システムがある場合は、SSO を構成して、そのシステムとプロセスを使い続けることができます。ユーザー認証が必要になると、そのシステムにリダイレクトされます。そのシステムで認証された場合は Google Cloud にアクセスできますが、そうでない場合はログインを求められます。

これにより、Google Cloud へのアクセス権を取り消すこともできます。

既存の認証システムが SAML2 をサポートしている場合は、このスライドに示されているように、3 つのリンクと証明書だけで簡単に SSO を構成できます。サポートしていない場合は、ADFS、Ping、Okta などのサードパーティ ソリューションを使用できます。

既存の ID 管理システムを使用する方法について詳しくは、この動画のリンク セクションをご覧ください。

[https://cloud.google.com/blog/products/identity-security/using-your-existing-identity-management-system-with-google-cloud-platform]

Gmail を使用しない Google Cloud アクセス

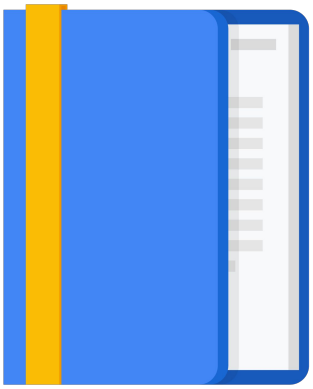
- Gmail を使用せずに Google のパスワードを取得可能
- ドメインを持つことで、グループ権限などのメリットを活用可能

また、Gmail を利用せずに Google アカウントを作成、使用することもできます。詳細については、この動画のリンク セクションをご覧ください。

[https://accounts.google.com/SignUpWithoutGmail?hl=ja]

アジェンダ

Identity and Access Management（IAM）
組織
ロール
メンバー
サービス アカウント
IAM のベスト プラクティス
ラボ



先ほど述べたように、メンバーの種類にはそのほかにサービス　アカウントもあります。

サービス アカウントを ID として使用した サーバー間のやり取り

- Compute Engine インスタンス内で実行されるプログラムは、認証情報付きのアクセス トークンを自動的に取得可能
- トークンを使用して、プロジェクト内の任意のサービス API や、アクセス権が付与されている他のサービスにアクセス
- サービス アカウントは、ユーザーデータにアクセスしない場合に便利

サービス アカウントは、個々のエンドユーザーではなく、アプリケーションに属するアカウントです。サービス アカウントを使用すると、ユーザーの認証情報を入力しなくても、プロジェクトでサーバー間のやり取りを行うことができます。

たとえば、Google Cloud Storage とやり取りするアプリケーションを作成する場合、最初に Google Cloud Storage の XML API または JSON API のいずれかに対して認証を行う必要があります。

そのような場合、サービス アカウントを有効にして、アプリケーションを実行する予定のインスタンス上でアカウントに対して読み取り / 書き込みアクセス権を付与できます。

その後、サービス アカウントから認証情報を取得するようにアプリケーションをプログラムすると、インスタンス、イメージ、アプリケーション コードに秘密鍵や認証情報を埋め込まなくても、アプリケーションは API に対してシームレスに認証されます。

サービス アカウントはメールアドレスで識別

- 123845678986-compute@project.gserviceaccount.com
- 3 種類のサービス アカウント:
  - ユーザー作成（カスタム）
  - 組み込み
    - Compute Engine と App Engine のデフォルトのサービス アカウント
  - Google API サービス アカウント
    - ユーザーに代わって内部の Google プロセスを実行

この例のように、サービス アカウントはメールアドレスで識別されます。

サービス アカウントには、ユーザー作成（つまりカスタム）、組み込み、 Google API の 3 種類があります。

デフォルトでは、すべてのプロジェクトに組み込みの Compute Engine デフォルト サービス アカウントが含まれています。

デフォルトのサービス アカウントのほかに、メールアドレス project-number@cloudservices.gserviceaccount.com で識別される Google Cloud API サービス アカウントがすべてのプロジェクトに含まれます。このサービス アカウントは、ユーザーに代わって内部の Google プロセスを実行するためのものであり、プロジェクトの編集者のロールが自動的に付与されます。

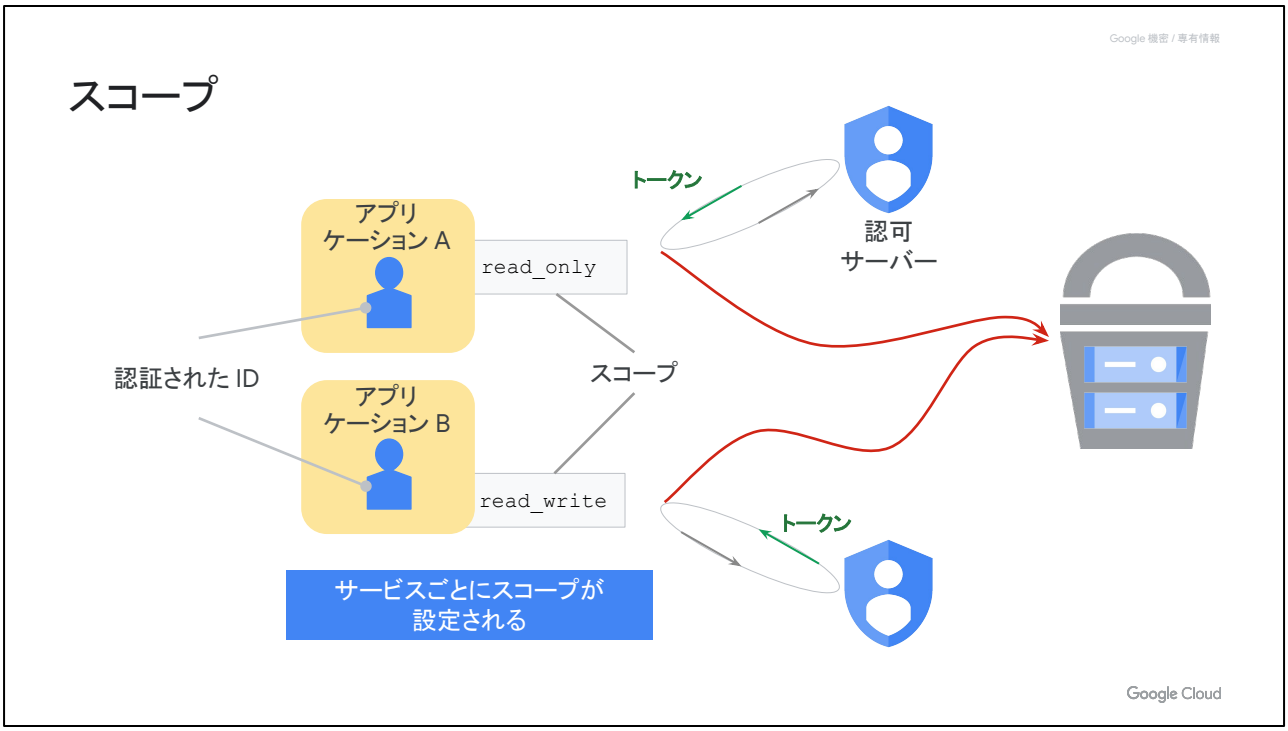
または、カスタムのサービス アカウントでインスタンスを起動することもできます。カスタムのサービス アカウントは、デフォルトのサービス アカウントより柔軟に利用できますが、ユーザーによる管理が必要です。必要な数のカスタム サービス アカウントを作成して、任意のアクセス スコープや IAM ロールを割り当てた後、仮想マシン インスタンスに割り当てることができます。

デフォルトの Compute Engine サービス アカウント

- プロジェクトごとに自動的に作成され、名前とメールアドレスが次のように自動生成される:
  - 名前には -compute というサフィックスが付く（例：`39xxxx0965-compute@developer.gserviceaccount.com`）
- プロジェクト編集者として自動的に追加される
- デフォルトでは、gcloud または Cloud Console を使用して作成されたすべての インスタンスで有効

デフォルトの Compute Engine サービス アカウントについて、もう少し説明します。すでに述べたように、このアカウントはプロジェクトごとに自動的に作成されます。このアカウントは、メールアドレス project-number-compute@developer.gserviceaccount.com で識別され、プロジェクトの編集者のロールが自動的に付与されます。

gcloud を使用して新しいインスタンスを起動すると、そのインスタンスでデフォルトのサービス アカウントが有効になります。この動作をオーバーライドするには、別のサービス　アカウントを指定するか、そのインスタンスのサービス　アカウントを無効にします。



認可とは、指定された一連のリソースに対して、認証された ID がどのような権限を持つかを決めるプロセスのことです。スコープは、認証された ID が認可されるかどうかを決定するために使用されます。

ここに示されている例では、アプリケーション A と B で、認証された ID（すなわちサービス アカウント）が使用されています。両方のアプリケーションが Cloud Storage バケットを使用しようとしていると仮定しましょう。それぞれが Google の認可サーバーにアクセス権をリクエストして、アクセス トークンを受け取ります。アプリケーション A は読み取り専用スコープのアクセス トークンを受け取るため、Cloud Storage バケットからの読み取りしか行えません。それに対して、アプリケーション B は読み取り / 書き込みスコープのアクセス トークンを受け取るため、Cloud Storage バケット内のデータを読み取って変更できます。

VM のスコープのカスタマイズ

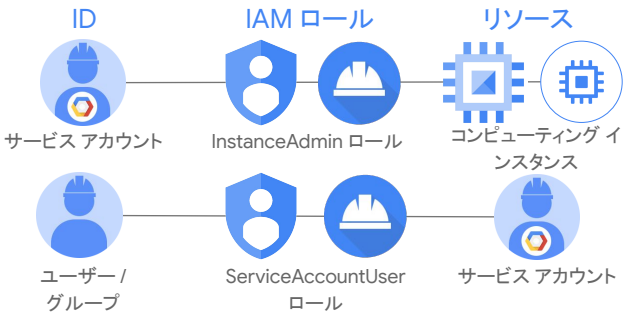
- インスタンスの作成後にスコープを変更可能
- ユーザー作成のサービス アカウントの場合は代わりに IAM ロールを使用する

このスクリーンショットに示されているように、デフォルトのサービス　アカウントを使用してインスタンスを作成するときにスコープをカスタマイズできます。これらのスコープは、インスタンスの作成後でも、インスタンスを停止することで変更できます。実のところ、アクセス スコープは VM の権限を指定する手法としては古いもので、 IAM ロールが登場する前は、アクセス スコープがサービス アカウントに権限を付与する唯一のメカニズムでした。

ユーザー作成のサービス アカウントでは、代わりに IAM ロールを使用して権限を指定してください。

サービス アカウント権限

- デフォルトのサービス アカウント: 基本ロールと事前定義ロール
- ユーザー作成のサービス アカウント: 事前定義ロール
- サービス アカウントのロールはグループやユーザーに割り当て可能

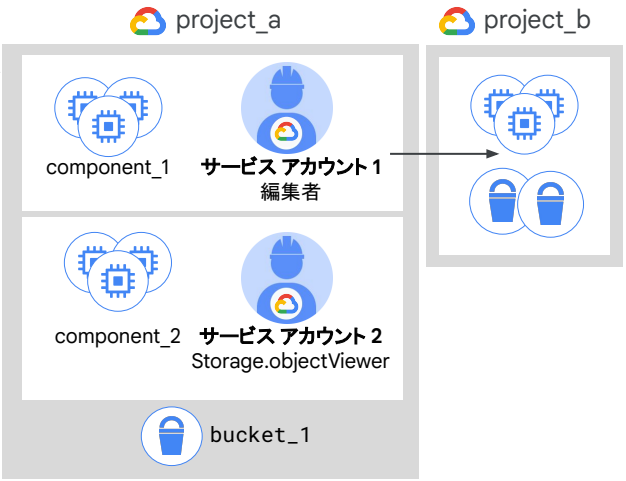


さて、サービス アカウントのロールはグループやユーザーに割り当てることもできます。このスライドの例を見ていきましょう。まず、サービス　アカウントを作成して InstanceAdmin のロールを付与します。このロールには、仮想マシンのインスタンスとディスクを作成、変更、削除する権限が含まれます。次に、このサービス　アカウントをリソースとして扱い、ユーザーやグループにサービス アカウント ユーザーのロールを付与することによって、使用できるユーザーを決定します。それらのユーザーは当該サービス　アカウントとしての役割を果たし、仮想マシンのインスタンスとディスクを作成、変更、削除できます。

サービス アカウント ユーザーは、当該サービス アカウントがアクセス権を持つすべてのリソースにアクセスできます。したがって、サービス　アカウント ユーザーのロールをユーザーやグループに付与するときには注意が必要です。

例: サービス アカウントと IAM

- component_1 を実行している VM には、サービス アカウント 1 を使用して project_b に対する編集者のアクセス権を付与する
- component_2 を実行している VM には、サービス アカウント 2 を使用して bucket_1 に対するオブジェクト閲覧者のアクセス権を付与する
- サービス アカウントの権限は VM を再作成することなく変更可能



別の例を見てみましょう。component_1 を実行している VM には、サービス アカウント 1 を使用して project_b に対する編集者のアクセス権が付与されます。 component_2 を実行している VM には、分離されたサービス アカウント 2 を使用して bucket_1 に対するオブジェクト閲覧者のアクセス権が付与されます。このように、 VM を再作成しなくても、VM の権限のスコープを変更できます。

基本的に、IAM では、プロジェクトを複数のマイクロサービスに分割し、それぞれを表すサービス アカウントを作成することによって、異なるリソースへのアクセス権を持たせることができます。VM を作成するときにサービス アカウントを割り当てると、Google Cloud によってセキュリティが管理されるため、認証情報が正しく管理されていることを確認する必要はありません。

では、サービス アカウントはどのように認証されるのでしょうか。

2 種類の Google サービス アカウント

Google 管理サービス アカウント

- すべてのサービス アカウント キーを Google が管理
- 鍵の公開部分と秘密部分の両方を Google が保管
- 公開鍵はそれぞれ最長 2 週間署名に使用可能
- 秘密鍵に直接アクセスされることはない

ユーザー管理サービス アカウント

- ユーザーが管理する鍵の公開部分のみを Google が保管
- 秘密鍵のセキュリティはユーザーの責任
- ユーザーが管理するサービス アカウント キーをサービスごとに 10 個まで作成可能
- IAM API、`gcloud`、Console で管理可能

Google サービス アカウントには 2 つの種類があります。

デフォルトでは、Google Cloud 内でサービス アカウントを使用すると（Compute Engine や App Engine から使用する場合など）、サービス アカウント キーが自動的に Google で管理されます。ただし、Google Cloud の外部でサービス アカウントを使用する場合や、ローテーション期間を変更したい場合は、独自のサービス アカウント キーを手動で作成して管理することもできます。

2 種類の Google サービス アカウント

Google 管理サービス アカウント

- すべてのサービス アカウント キーを Google が管理
- 鍵の公開部分と秘密部分の両方を Google が保管
- 公開鍵はそれぞれ最長 2 週間署名に使用可能
- 秘密鍵に直接アクセスされることはない

ユーザー管理サービス アカウント

- ユーザーが管理する鍵の公開部分のみを Google が保管
- 秘密鍵のセキュリティはユーザーの責任
- ユーザーが管理するサービス アカウント キーをサービスごとに 10 個まで作成可能
- IAM API、gcloud、Console で管理可能

すべてのサービス アカウントの鍵ペアを Google が管理します。

Google が管理するサービス アカウント キーでは、鍵の公開部分と秘密部分の両方を Google が保管し、定期的にローテーションします。

公開鍵はそれぞれ最長 2 週間署名に使用できます。

秘密鍵は常に信頼できる第三者機関に安全に保管され、直接アクセスされることはありません。

2 種類の Google サービス アカウント

Google 管理サービス アカウント

- すべてのサービス アカウント キーを Google が管理
- 鍵の公開部分と秘密部分の両方を Google が保管
- 公開鍵はそれぞれ最長 2 週間署名に使用可能
- 秘密鍵に直接アクセスされることはない

ユーザー管理サービス アカウント

- ユーザーが管理する鍵の公開部分のみを Google が保管
- 秘密鍵のセキュリティはユーザーの責任
- ユーザーが管理するサービス アカウント キーをサービスごとに 10 個まで作成可能
- IAM API、gcloud、Console で管理可能

Google Cloud の外部から使用できるユーザー管理の鍵ペア（外部鍵）を 1 つ以上作成することもできます。Google では、ユーザーが管理する鍵の公開部分のみを保管します。

秘密鍵のセキュリティと、鍵のローテーションなどの他の管理操作は、手動で行う場合もプログラムを使用する場合も、ユーザーの責任になります。

サービス アカウントごとに最大 10 個のサービス アカウント キーを作成できるので、鍵のローテーションが容易になります。

ユーザーが管理する鍵は、IAM API、gcloud コマンドライン ツール、Cloud Console の [サービス アカウント] ページで管理できます。

ユーザーが管理する鍵のセキュリティは極めて重要 - 作成者の責任

注意事項: Google はユーザー管理の秘密鍵を保存していないため、ユーザーが秘密鍵を紛失した場合に鍵の復元をサポートすることはできない

Google はユーザー管理の秘密鍵を保存していないため、ユーザーが秘密鍵を紛失した場合に鍵の復元をサポートすることはできません。

それらの鍵のセキュリティや定期的なローテーションはユーザーの責任です。

ユーザー管理の鍵を使用するのは最後の手段とし、有効期間が短いサービス　アカウント認証情報（トークン）、サービス　アカウントの権限借用など、その他の方法をまず検討してください。

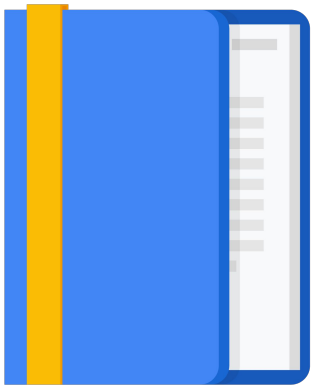
gcloud コマンドライン ツールを使用して、サービス アカウントに関連付けられているすべての鍵のリストをすばやく表示

```
gcloud iam service-accounts keys list --iam-account user@email.com
```


このスライドに示されている gcloud コマンドラインを使用すると、特定のサービス アカウントに関連付けられているすべての鍵のリストをすばやく簡単に表示できます。

アジェンダ

- Identity and Access Management（IAM）
- 組織
- ロール
- メンバー
- サービス アカウント
- **IAM のベスト プラクティス**
- ラボ



これまで学んだコンセプトを日常の業務に適用できるよう、 IAM のベスト プラクティスをいくつか紹介します。

リソース階層の活用と理解

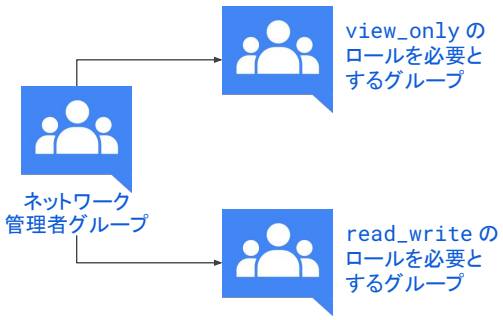
- プロジェクトを使用して、同一の信頼境界を共有するリソースをグループ化する
- 各リソースに付与されたポリシーを確認し、継承について把握する
- 「最小権限の原則」に従ってロールを付与する
- Cloud Audit Logs でポリシーを監査する: setiampolicy
- ポリシーで使用されるグループのメンバーシップを監査する

まず、リソース階層を活用し、理解しましょう。

- 具体的には、プロジェクトを使用して、同一の信頼境界を共有するリソースをグループ化してください。
- 各リソースに付与されたポリシーを確認し、継承について把握します。
- ロールは継承されるため、「最小権限の原則」に従ってロールを付与してください。
- 最後に、Cloud Audit Logs を使用してポリシーを監査し、ポリシーで使用されるグループのメンバーシップを監査します。

個人ではなくGoogle グループへのロールの付与

- IAM ポリシーではなくグループ メンバーシップを更新する
- ポリシーで使用されるグループのメンバーシップを監査する
- IAM ポリシーで使用される Google グループのオーナー権限を制御する



次に、ロールは個人ではなく、グループに付与することをおすすめします。これにより、IAM ポリシーを変更する代わりにグループ　メンバーシップを更新できます。このようにする場合、ポリシーで使用されるグループのメンバーシップを監査し、 IAM ポリシーで使用される Google グループのオーナー権限を制御してください。

複数のグループを使用して、より細かく制御することもできます。このスライドの例では、ネットワーク管理者グループに、Cloud Storage バケットに対する read_write のロールを必要とするメンバーと、read_only のロールを必要とするメンバーが含まれています。これら 3 つのグループすべてで個人を追加、削除することによって、全体的なアクセスを制御できます。したがって、グループは職務に関連付けられるだけでなく、ロールの割り当てにも有効です。

サービス アカウント

- serviceAccountUser のロールの付与は慎重に行う
- サービス アカウントの作成時には、その目的がすぐにわかるような表示名を付ける
- サービス アカウントの命名規則を確立する
- 鍵のローテーションのポリシーとメソッドを確立する
- serviceAccount.keys.list() メソッドで監査を実施する

サービス アカウントの使用に関するベスト プラクティスをいくつか紹介します。

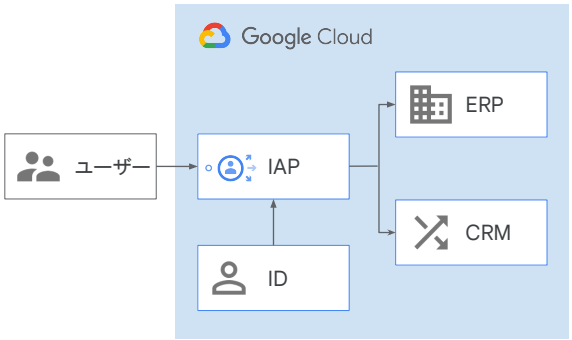
- すでに述べたように、サービス アカウント ユーザーのロールは、そのサービス アカウントがアクセス権を持つすべてのリソースへのアクセスを可能にするため、付与する際は注意が必要です。
- また、サービス アカウントを作成するときには、その目的がすぐにわかるような表示名を付けるようにして、できれば確立された命名規則を使用してください。
- 鍵については、ローテーション ポリシーとメソッドを確立し、serviceAccount.keys.list() メソッドで監査してください。

Identity-Aware Proxy（IAP）

アプリケーションとリソースに対して
アクセス制御ポリシーを適用:

- ID ベースのアクセス制御
- HTTPS 経由でアクセスされるアプリケーションの一元的な認可レイヤ

IAM ポリシーは認証後に適用される



最後に、Identity-Aware Proxy（IAP）を使用することをおすすめします。IAP を使用すると、HTTPS によってアクセスされるアプリケーションの一元的な認可レイヤを確立できるため、ネットワーク レベルのファイアウォールに依存せずにアプリケーション　レベルのアクセス制御モデルを使用できます。

IAP によって保護されたアプリケーションとリソースにアクセスできるのは、適切な　IAM ロールを持つユーザーやグループがこのプロキシを通じてアクセスする場合だけです。IAP によってアプリケーションやリソースへのアクセス権をユーザーに付与すると、使用中のプロダクトによって実装されたきめ細かいアクセス制御が適用されるため、 VPN を使用する必要がなくなります。右に示されているように、ユーザーが　IAP によってセキュリティ保護されているリソースにアクセスしようとすると、 IAP が認証チェックと認可チェックを行います。

IAP の詳細については、この動画のリンク　セクションをご覧ください。

[https://cloud.google.com/iap/docs/concepts-overview]

ラボ

Cloud IAM

このモジュールで学習した内容を実際に試してみましょう。

このラボでは、ロールの付与と取り消しを行って、アクセス権を変更します。具体的には、Cloud IAM を使用してアクセス制御を実装し、特定の機能やリソースへのアクセスを制限して、サービス アカウント ユーザーのロールを使用します。

IAM ロールに変更を加えると、GCP Console は実際のシステムより速く更新されます。したがって、メンバーのロールを変更するときには、短い遅延が発生することを想定してください。

ラボの復習

Cloud IAM

このラボでは、Cloud IAM のロールをユーザーに付与してから取り消す演習を行いました。最初はユーザー Username 2、次にサービス アカウント ユーザーを対象にしました。両方のユーザーを使用することで、行った変更の結果を確認できました。

この後、ラボのチュートリアルを参照できますが、 GCP のユーザー インターフェースは変更されることがあるため、実際の環境は見た目が少し異なる場合があります。

確認

Identity and Access Management

このモジュールでは、Identity and Access Management とそのコンポーネント、そしてベスト プラクティスについて学習しました。IAM は、他の Google Cloud ID サービスに基づいて構築されています。

企業 ID の作成と管理は、Workspace 管理者や Cloud Identity インターフェースを通じて行われ、一般に Google Cloud 管理者とは別のユーザーによって処理されます。

Google グループでは、この 2 つの職務のコラボレーションを実現できます。 Google Cloud 管理者がロールを確立してグループに割り当てた後に、 Workspace 管理者がグループ内のメンバーシップを管理します。

最後に、サービス アカウントは柔軟性に優れており、インフラストラクチャベースのレベルでアプリケーションの制御を行うことができます。