利用自体には料金はかかりません。無料です。
まず複数アカウントで運用するメリットについて説明します。

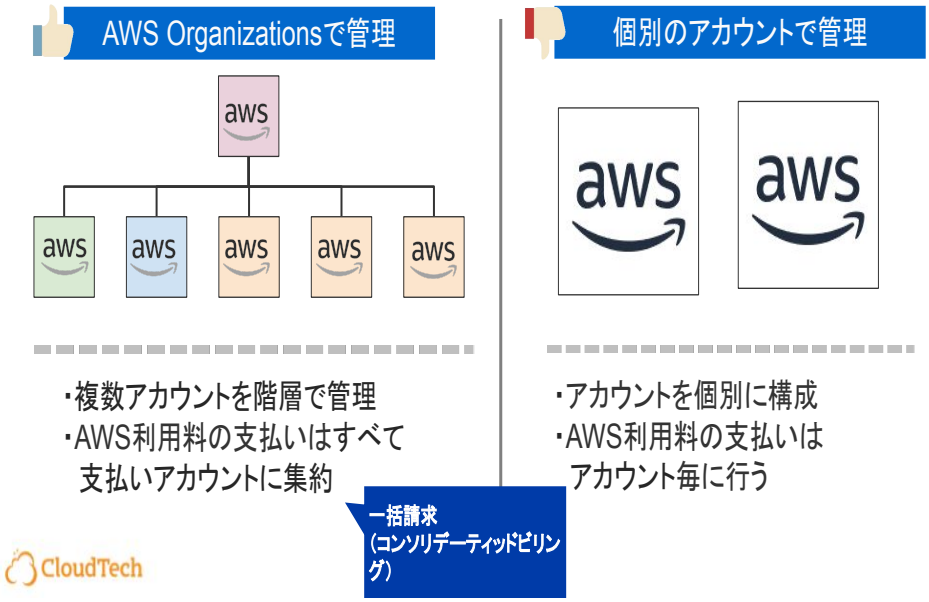
まず、おさらいですが、AWSアカウントの運用については

- 「単一のアカウントの構成」
  - クレジットカード1枚を登録してアカウントを1つというパターン。
  - 簡素で統制を利かせやすい、というメリットがあります。

- しかし、多くの企業では「複数のアカウントの構成」が広く採用されています。
  - 複数アカウントにすると色々とメリットがあります。例えば、
  - セキュリティの境界、アカウント単位でセキュリティの設定をまるっと変えて管理しやすかったり、
  - リソースの管理、ログを集約するだけのアカウントとか、役割に応じてリソースを作成して管理しやすく

    - するなど、
    - 課金の分離、どれだけお金がかかったかアカウント単位で区別しやすいなど
- といった場合には、「複数アカウントの構成」の利用を検討する必要があります。

AWS Organizationsで複数アカウントを運用する



- AWS Organizationsを利用すると、
  - ご覧のように、複数アカウントを階層で管理できます。他のアカウントを、グループに招待することができます。
    - 実際にはOUと呼ばれるグループを用いて管理します。後ほど詳しくみていきます。
  - AWS利用料の支払いは、頂点に位置するアカウントに集約されます。これは一括請求（コンソリデーティッドビリング）と呼ばれるOrganizationsの機能のひとつです。
  - 操作権限を各アカウントにまとめて一括で統制できます。これも詳しくみていきましょう。

- Organizationsを使わずに、個別のアカウントで管理することもできますが
  - セキュリティやリソース管理はアカウント毎に別々に行なう必要があります。

- またAWS利用料の支払いもアカウント毎で行なう必要があります。
  - 会社にとっては、特に請求が別れるという観点から少しつかいにくいですよね

AWS Organizations 概要

CloudTech

AWS Organizations 概要

➤ 複数アカウントの一元管理
- アカウントの招待、作成
- 組織内アカウントを横断した管理
- 一括請求

➤ 2機能のどちらかを選択
- 一括請求機能のみ（Consolidated Billing Only）
- すべての機能（All futures）

➤ 管理アカウント、メンバーアカウント、組織単位（OU）、Root（管理ルート）、SCPなどから構成される

CloudTech

- 複数アカウントの一元管理
  - 既にあるAWSアカウントを自分の組織に招待もできますし、Organizationsの画面から新規アカウントを作成することもできます。
    - 組織内アカウントを横断した管理とは、例えば、複数アカウントに対して一括で CloudTrail の証跡を設定するなど、効率的な管理ができます。
    - また、AWS使用料金の一括請求などで経理などがわかりやすくなります。

- 2つの機能があり、使用開始時にどちらかを選択します。
  - 一括請求機能のみ（Consolidated Billing Only）
    - 複数アカウントの AWS使用料金の請求をまとめることができる機能
  - すべての機能（All futures）
    - デフォルトはこれ

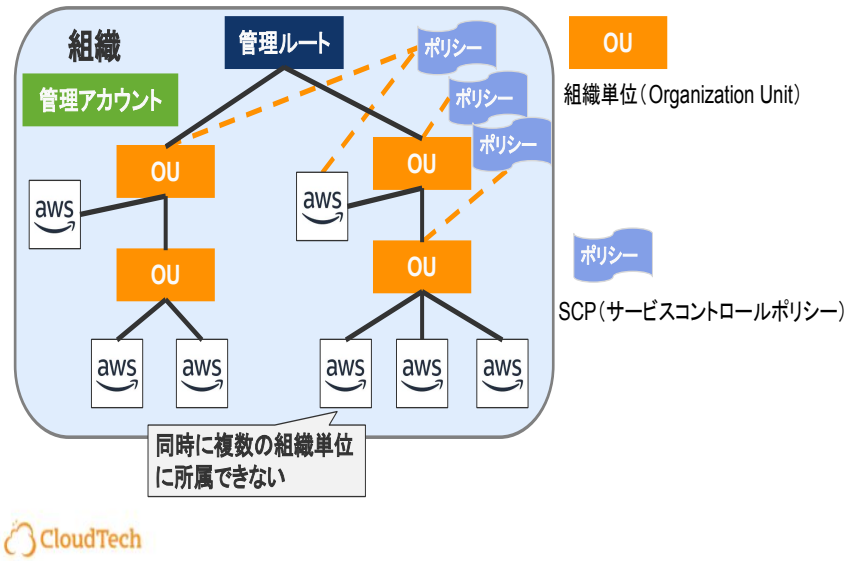
        - 各所属アカウントに対しての操作権限の管理（サービスコントロールポリシー）による一元管理ができる
    - なお、一括請求機能のみを使用して組織を作成する場合、後ですべての機能を有効にできます。

- 構成要素は、管理アカウント、メンバーアカウント、組織単位（OU）、Root（管理ルート）、SCPがあります。
    - これら構成要素を次のスライドから詳しくみていきましょう。

利用自体には料金はかかりません。無料です。個人学習でもやってみてください。

AWS Organizations の構成要素について説明します。

AWS Organizations 構成要素



Organizationsの公式ドキュメントでも登場する各種用語について、スライドをみながら整理していきましょう。

Organizationsでは、
「組織」
「管理ルート」
「組織単位Organization Unit（OU)」
「管理アカウント」
「AWSアカウント」
「サービスコントロールポリシー」
という6つの重要な用語があります。

■組織とは一元管理が可能な複数のアカウントの集まりのことを差し、1つの管理アカウントから構成されます。
大きな枠組みとなり、これから説明していく用語はすべてこの組織の中に存在していることになります。

■管理アカウントは組織全体の AWS利用料金が集約される支払いアカウントになります。
組織に所属するAWSアカウントを作成したり、招待したり、削除したり、後述のサービスコントロールポリシーを適用したり、管理するアカウントです。
管理アカウントは以前「マスターアカウント」と呼ばれていましたが、マスターが差別用語の関係から「管理アカウント」という表現に置き換えが進んでいます。

■組織単位はOrganization Unit（OU）と表記されますが、アカウントのグループのことです。
AWSアカウントはこのOUに所属します。1つのOUに1つのAWSアカウントのみ所属する場合もありますし、複数のアカウントが所属することもあります。

■管理ルートはOUの開始点です。この図のように、組織単体の階層全体の開始点になります。
組織1つあたり、管理ルートは1つだけという制約があります。

■AWSアカウントは、AWS Organizartionsで管理する対象となったアカウントを指します。
Organizations のドキュメントや文脈では、「メンバーアカウント」と呼ぶこともあります。
AWSアカウントは同時に複数の組織単位に所属できない、と言った制約がありますが、とある組織単位から別の組織単位に移行させることが出来ます。

■SCPとは
AWSアカウントレベルでの、AWSのAPIアクセスの許可・拒否の制御を実現する機能です。アカウントに対して適用する IAMポリシーのようなイメージで、IAMポリシーと同様、JSONで記述されています。

つまり、セキュリティ強化のために、このアカウントでは S3の作成を拒否しますよ、このアカウントはインターネットゲートウェイの作成を禁止しますよ、といった特定の操作を拒否するポリシーです。

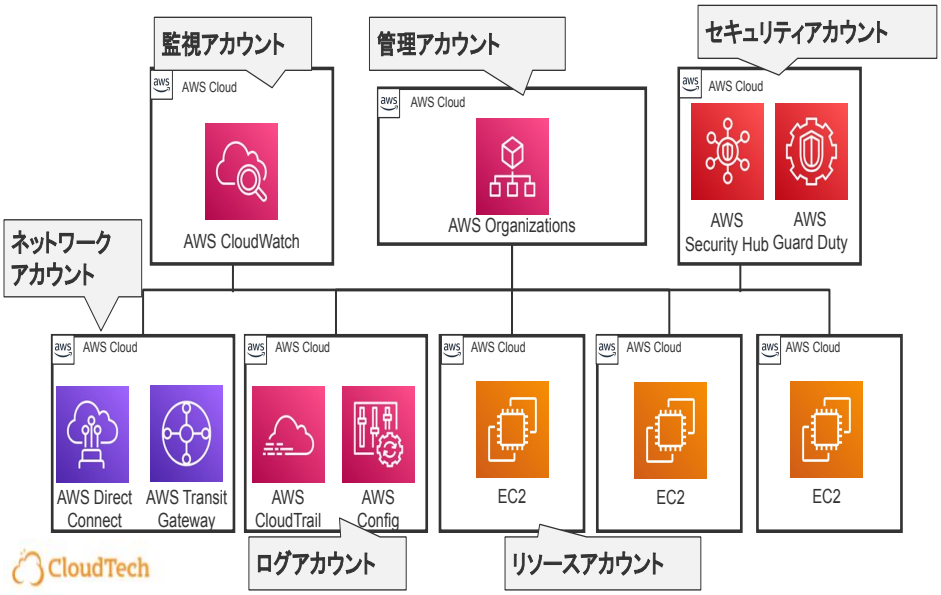
サービスコントロールポリシーは、OUや管理ルートにアタッチして使用します。
OU配下にあるAWSアカウントは、それまでに所属している OU 、または管理ルートにアタッチされた SCP が全て適用されるということです。

なお、AWSアカウント自体にもサービスコントロールポリシーをアタッチすることも出来ます。
ただし、サービスコントロールポリシーの効率的な管理を行なうため、基本的にはOUに対してアタッチしましょう。

AWS Organizations 設計例

CloudTech

AWS Organizations 設計例（アカウントの分離）



まず一般的にアカウントってどんな風に分けるべきか、ついて。
一例を紹介します。

まず、Organizationsの主体となる管理アカウント。
組織に所属する各アカウントの支払いをまとめます。
AWSのベストプラクティスでは、このアカウントで EC2やRDSなどのAWSリソースを作成すべきではない、と提唱されていますが、
ベストプラクティスは絶対ではありません。もちろん例外もあります。スピードやシンプルさを優先することもあるでしょう。

次に、「ネットワークアカウント」
マルチアカウント環境下で Direct ConnectやTransit Gateway を作成、管理する役割を持ったアカウントです。
Transit Gatewayはマルチアカウント間の通信を実現させる機能を有しており、誤った設定変更により通信が出来なくなってしまうとシステム稼働へ大きな影響を与えてしまう恐れがあります。
その理由から「ネットワークアカウント」という役割を持たせたアカウントでこれらのサービスを管理することが好ましいと考えられています。

「ログアカウント」はセキュリティ監査ログを集約するためのアカウントです。
CloudTrailのセキュリティ監査系のログ以外にも、AWS Configの構成管理のログを集約する利用方法が想定されます。
集約された監査系のログは限られた管理者のみがアクセスできるように設定すべきです。

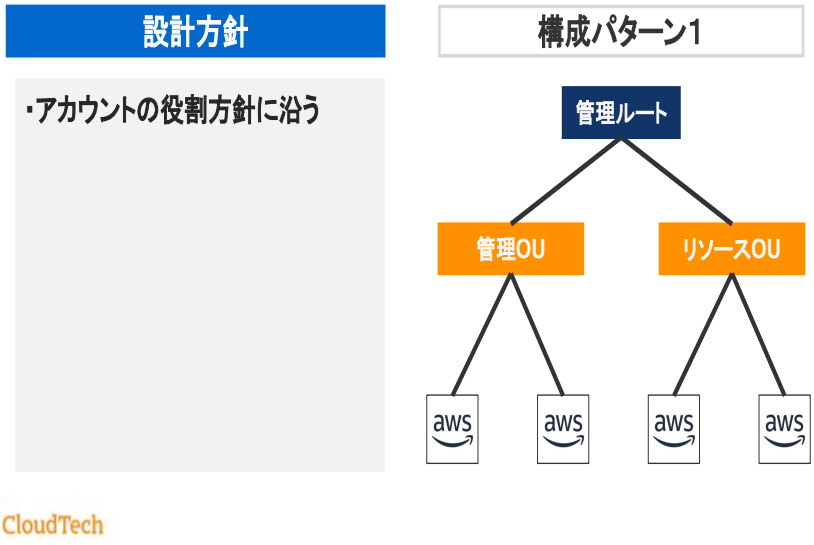
他にも、CloudWatchのダッシュボードを集約して参照するための「監視アカウント」といった役割を持ったアカウントを作成したり、

Security Hub、Amazon GuradDuty といったAWSのセキュリティ関連サービスを集中管理するための「セキュリティアカウント」といった役割を持ったアカウントを作成するのも良いでしょう。

そして、
「リソースアカウント」はシステムを稼動させるための AWSリソースを作成させるアカウントです。
システム単位、環境単位の分割単位を予め検討しておく必要があります。
例えば、開発、仮本番、本番、などといったような分類です。

絶対こうすべきというものはありませんので、組織の実態や計画に合わせて、臨機応変に対応していくことがマルチアカウントの運用において大事なことです。

AWS Organizations 設計例（OUの構成パターン）



CloudTech

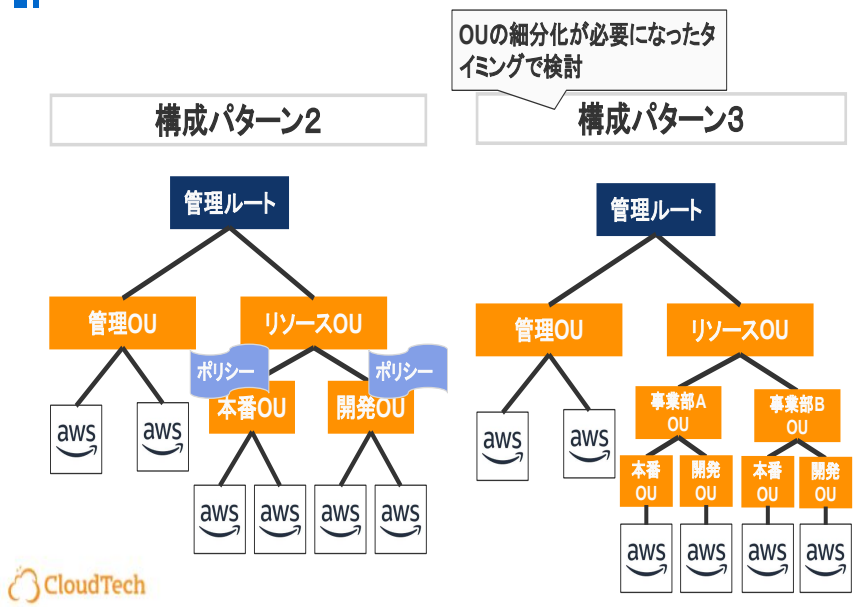
OUについてどのような考えで設計をすればいいか、また構成パターンについて見ていきましょう。

OUの設計方針の１つとして、「アカウントの役割の方針に沿って設計する」という考え方があります。

アカウントの役割、つまり
・管理系アカウント
・リソース系アカウント
この2種の役割がある場合、

・管理OU
・リソースOU
の2つのOUを作成し、それらのOUにアカウントを関連付けをする構成パターンがあります。シンプルですね。

AWS Organizations 設計例（OUの構成パターン）



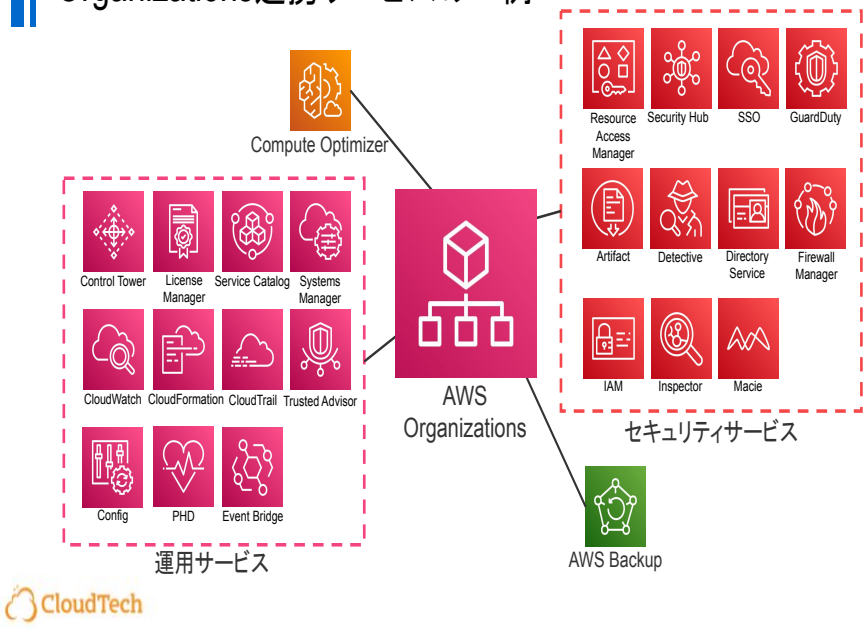
環境別にOUを分けるパターンについてです。

リソースOU配下に
本環境用OUと
開発環境用OUを作成し、アカウントを関連付ける方法もあります。
本番環境だけ特定サービスの操作を制御したい、という要件がある場合、環境別にOUを分けると
SCPの管理効率化に繋がることになります。

全社的にAWSを利用しており、事業部レベルで特定の操作を制御させたい、といった要件がある場合、
リソースOU配下に
更に事業部門のOU、
環境別OUを作成、
アカウントを関連付けを行なう方法があります。
ただしこのパターンになると管理すべき OUが多くなることになり、煩雑になってしまう恐れがあるため慎重な検討が必要になってきます。

OUの構成変更は柔軟に行なえるため、まずは構成パターン1、もしくは構成パターン2で検討を行ない、
利用開始をして更にOUの細分化が必要になったタイミングで検討する進め方をするのが良いでしょう

Organizations連携サービスの一例



最後に、
Organizationsと連携できるサービスの一例です。

OrganizationsはAWSの多くのサービスと統合されています。
特に運用、セキュリティ面で多くの恩恵をもたらします。

CloudWatch, CloudFormation, CloudTrail, Congif
RAM, IAMなどなど、参考にしてみてください。

AWS SSO を連携したアカウント間のシングルサインオンの実装はマルチアカウント環境下ではとても有効なサービスです。
別レッスンで取り上げます。