AWS

SUMMIT

AWSにおけるマルチアカウント管理の手法とベストプラクティス

アマゾン ウェブ サービス ジャパン株式会社
プロフェッショナルサービス本部 プラクティスマネージャー
高田智己

2017年6月2日

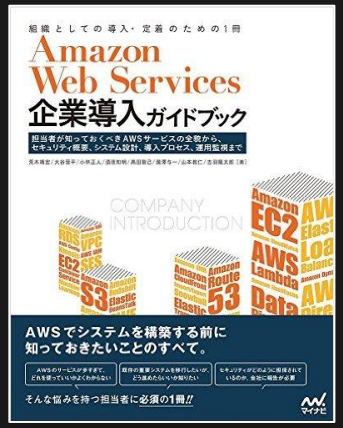
amazon web services

本セッションのスピーカー紹介

名前
高田 智己（Tomomi Takada）

所属
アマゾン ウェブ サービス ジャパン株式会社
プロフェッショナルサービス本部
プラクティス マネージャー

プロフェッショナルサービスにおいて、エンタープライズのお客様の主にセキュリティに関する課題解決に従事



amazon web services Certified
Solutions Architect - Professional

amazon web services Certified
DevOps Engineer - Professional

amazon web services Certified
Developer - Associate

amazon web services Certified
Solutions Architect - Associate

amazon web services Certified
SysOps Administrator - Associate

本セッションの内容

- 本セッションはAWSで複数のアカウントを利用する場合のメリット・デメリットを紹介し、お客様のマルチアカウント方針を考える際の手助けとなることを目的としています。

- マルチアカウントを管理するための機能をご紹介いたしますが、マルチアカウントを検討する際の理解を目的としているため、各機能の詳細な内容は参考資料のご紹介とさせて頂きます。

アジェンダ

- AWSアカウントとマルチアカウント環境
- AWSのマルチアカウント管理機能
    - マルチアカウント環境でのアクセス
    - マルチアカウントの課金管理
    - マルチアカウントのセキュリティ・ログ管理
    - マルチアカウントの統制
- 本日のまとめ

AWSアカウントと
マルチアカウント環境

AWSアカウントとは？

AWSアカウントとは？

- AWS環境の分割単位・リソース管理の枠組み

リソースの管理単位

AWSアカウントとは？

- AWS環境の分割単位・リソース管理の枠組み
- セキュリティ上の境界

リソースの管理単位

セキュリティ上の境界

AWSアカウントとは？

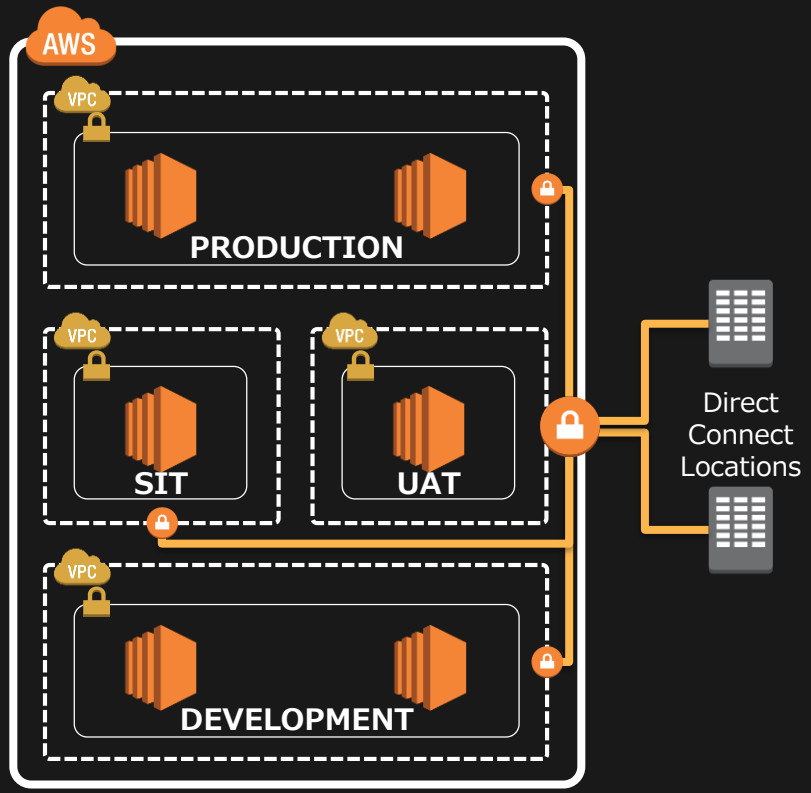
- AWS環境の分割単位・リソース管理の枠組み
- セキュリティ上の境界
- AWS課金の分割

リソースの管理単位

セキュリティ上の境界

課金の分離単位

1つのAWSアカウントによる環境



- 既存DCのコンセプトと類似しているため導入が容易
- シンプルな構成のため素早い導入が可能
- 1つのDX接続でオンプレミスとのハイブリッド環境が導入可能

複数のAWSアカウントを用いる理由は？

AWSアカウントを分割して運用するようになる主な理由：

複数のAWSアカウントを用いる理由は？

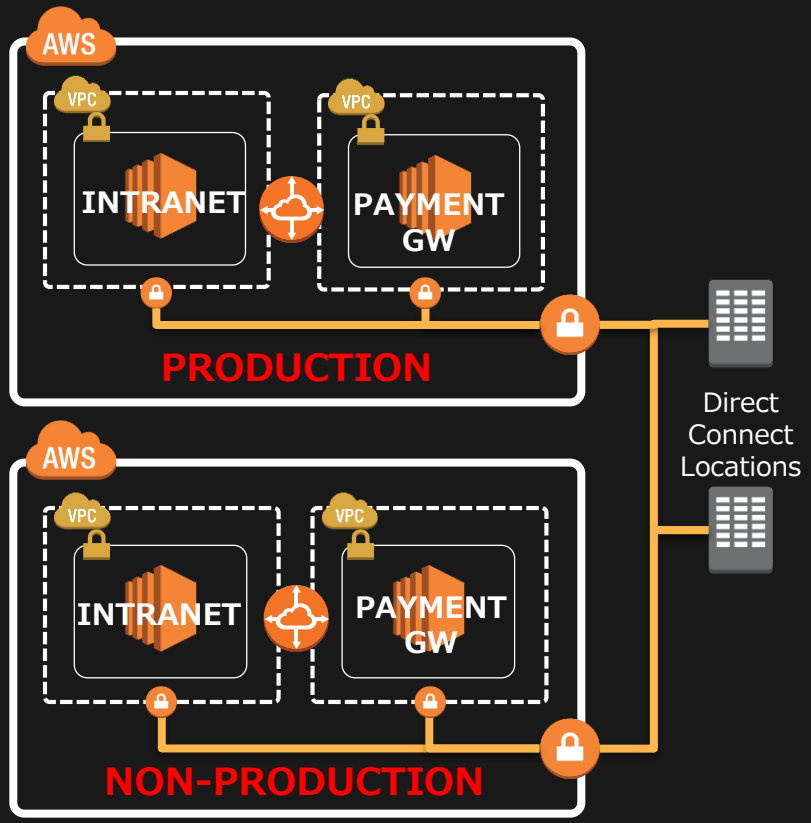
AWSアカウントを分割して運用するようになる主な理由：

ガバナンス

セキュリティ及びガバナンス上の理由から開発環境、テスト環境、本番環境でアカウントを分割したい
例）PCI準拠のワークロードなど

複数のAWSアカウントを用いる理由は？

ガバナンスの観点



メリット

- 本番環境の**管理コンソールを分離**できる
- 本番環境と非本番環境を管理するメンバーとで**明確な権限の分離**
- 環境間における**セキュリティ対策の分離**が可能

デメリット

- ガバナンスのレビューを複数アカウントにまたがり行う必要がでる
- 複数アカウントにまたがる監査情報取得の効率化が必要

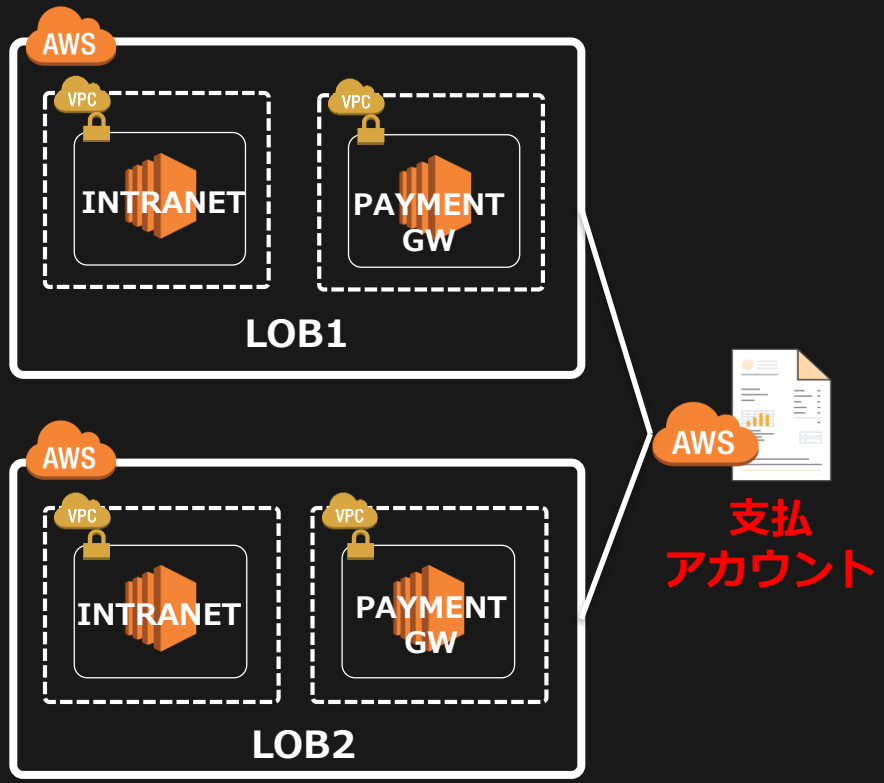
複数のAWSアカウントを用いる理由は？

AWSアカウントを分割して運用するようになる主な理由：

ガバナンス	課金
セキュリティ及びガバナンス上の理由から開発環境、テスト環境、本番環境でアカウントを分割したい 例）PCI準拠のワークロードなど	課金に関する可視性、責任、及びアカウントごとのコントロールを行いたい 例）LOBごとに課金を明確に分けたいなど

複数のAWSアカウントを用いる理由は？

課金の観点



メリット

- 分離した**アカウント毎に明確な課金管理**を行うことができる。
- 複数のコストセンターやLOB等に対し、**シンプルな課金やチャージバックの運用**を行うことができる。

デメリット

- 各アカウントの課金レポートに対するアクセス管理や、レポートを集約する場合にはコンソリデーションを必要とする
- 利用料のボリュームディスカウントのためにはコンソリデーションと社内配賦の合意が必要になる

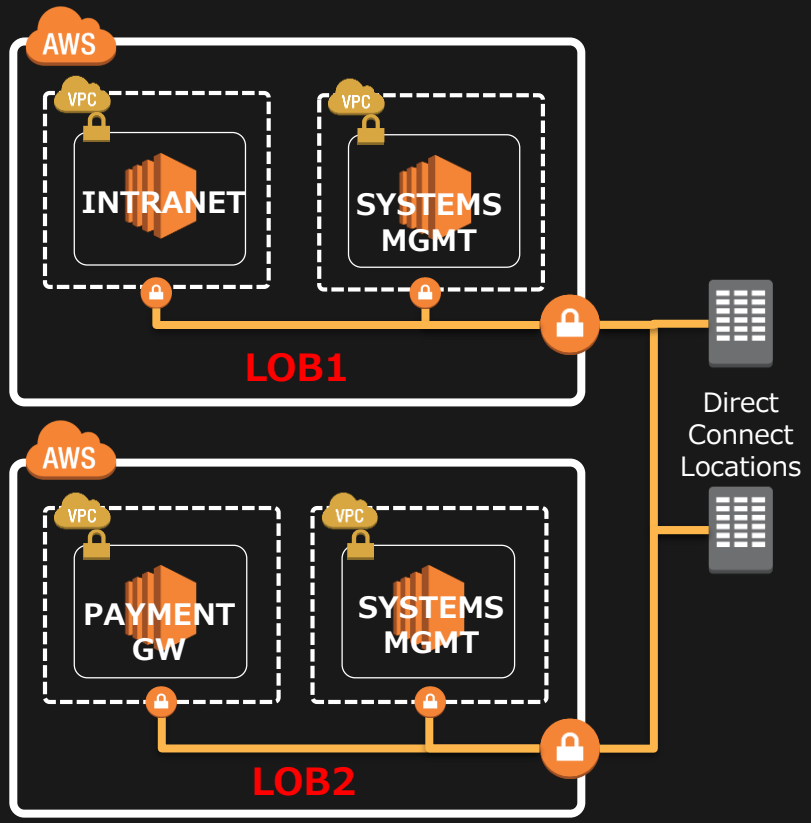
複数のAWSアカウントを用いる理由は？

AWSアカウントを分割して運用するようになる主な理由：

ガバナンス	課金	組織
セキュリティ及びガバナンス上の理由から開発環境、テスト環境、本番環境でアカウントを分割したい 例）PCI準拠のワークロードなど	課金に関する可視性、責任、及びアカウントごとのコントロールを行いたい 例）LOBごとに課金を明確に分けたいなど	リソースの操作権限を特定の業務ユニット（LOB）に委譲し、その中でより自由にAWSプラットフォームを活用したい

複数のAWSアカウントを用いる理由は？

組織の観点



メリット

- 異なるLOBを異なる課金管理と共にサポートすることができ、**LOB単位での管理を容易に行う**ことができる
- 統制や課金が異なる専用アカウントを用いる**個々の顧客に対してサービスプロバイダー型のサービス**を提供しやすい

デメリット

- 共通サービスのような、アカウントをまたいで利用できる機能を重複して持つことへの考慮・対応が必要となる

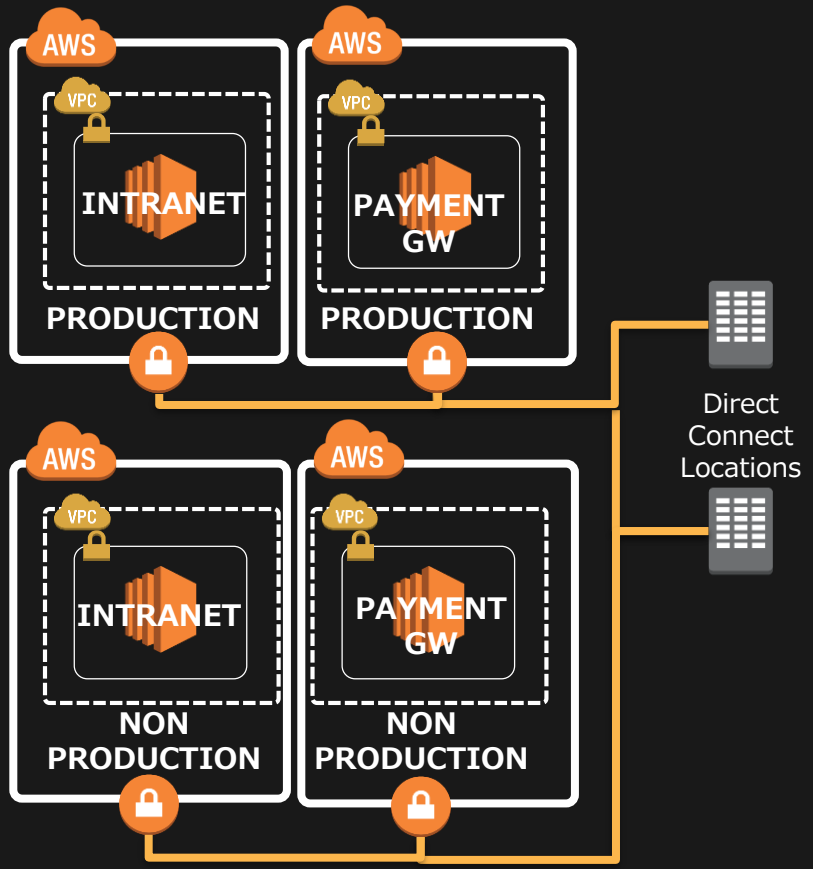
複数のAWSアカウントを用いる理由は？

AWSアカウントを分割して運用するようになる主な理由：

ガバナンス	課金	組織	運用
セキュリティ及びガバナンス上の理由から開発環境、テスト環境、本番環境でアカウントを分割したい 例）PCI準拠のワークロードなど	課金に関する可視性、責任、及びアカウントごとのコントロールを行いたい 例）LOBごとに課金を明確に分けたいなど	リソースの操作権限を特定の業務ユニット（LOB）に委譲し、その中でより自由にAWSプラットフォームを活用したい	構成変更時の影響範囲を小さくし、他の組織を気にすることなく自身固有の環境を利用したい

複数のAWSアカウントを用いる理由は？

運用の観点



メリット

- **変更による影響範囲を縮小**し、リスクアセスメントをシンプルにできる。例）開発環境の変更が本番環境に及ばない
- AWSアカウントの**リソース上限にかかる可能性を緩和**できる

デメリット

- 複数アカウントを管理するため重複設定・操作の増加等、運用ボリュームが増加する
- オンプレミスとAWSおよびAWSアカウント間のネットワーク接続の複雑性・コストが増す

マルチAWSアカウントのメリット・デメリット

メリット

+ 完全なセキュリティとリソースの分離
+ アカウント毎に行える課金管理
+ 問題発生時の影響範囲の縮小化

デメリット

- アカウント間の複雑なセキュリティポリシーの必要性
- アカウント間の課金の取りまとめや配賦管理
- 構築、運用のオーバーヘッド

マルチAWSアカウントのメリット・デメリット

メリット

+ 完全なセキュリティとリソースの分離
+ アカウント毎に行える課金管理
+ 問題発生時の影響範囲の縮小化

デメリット

- アカウント間の複雑なセキュリティポリシーの必要性
- アカウント間の課金の取りまとめや配賦管理
- 構築、運用のオーバーヘッド

AWSのマルチアカウント管理機能

マルチアカウントを管理する機能

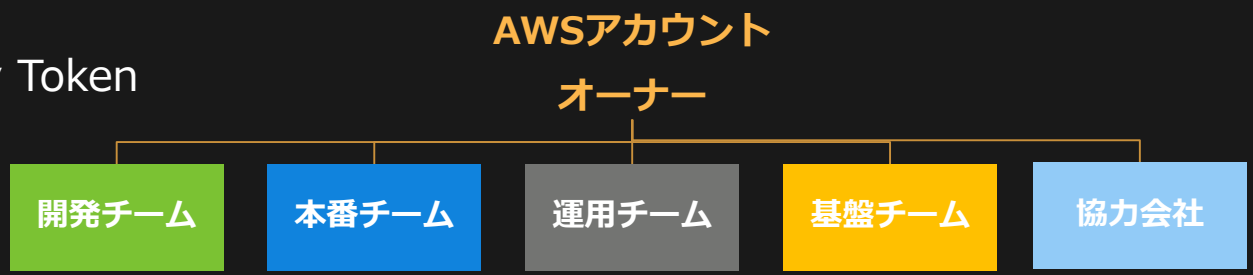
- マルチアカウント環境でのアクセス
- マルチアカウントの課金管理
- マルチアカウントのセキュリティ・ログ管理
- マルチアカウントの統制

マルチアカウントを管理する機能

- マルチアカウント環境でのアクセス
- マルチアカウントの課金管理
- マルチアカウントのセキュリティ・ログ管理
- マルチアカウントの統制

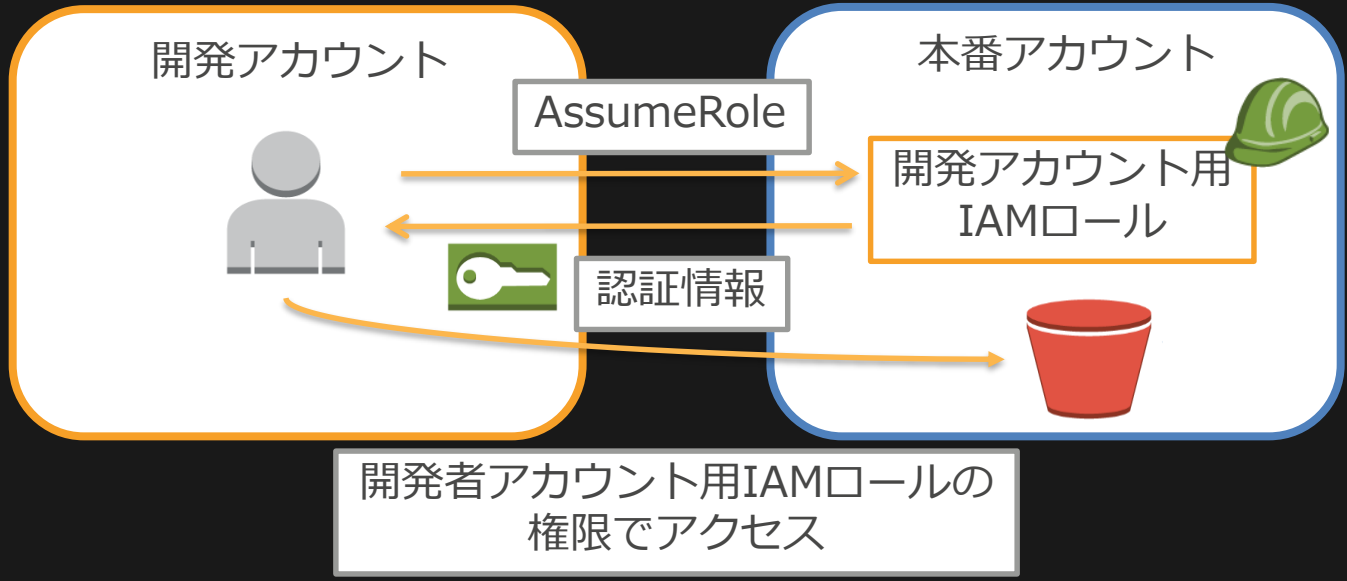
AWS Identity and Access Management (IAM)

- ユーザ/クレデンシャル管理
  - IAMユーザ / パスワード
  - MFA (多要素認証)
  - クレデンシャルのローテーション
- アクセス権限管理
  - IAMグループ
  - IAMポリシー
- 権限の委任
  - IAMロール
  - Security Temporary Token



IAMロールによるクロスアカウントアクセス

あるアカウントのユーザーを別のアカウントのIAMロールに紐づける機能
例えば開発アカウントを使って、本番環境のS3データを更新するようなケースで利用

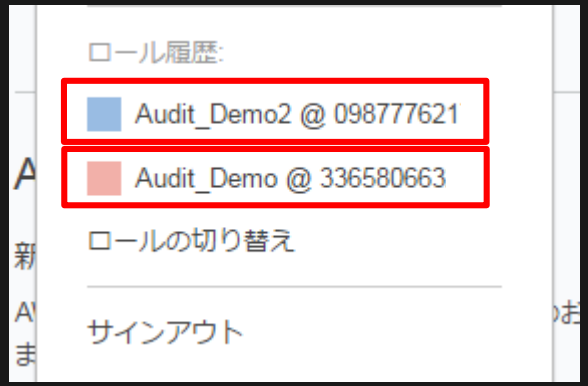


Switch RoleによるAWSアカウントの切り替え

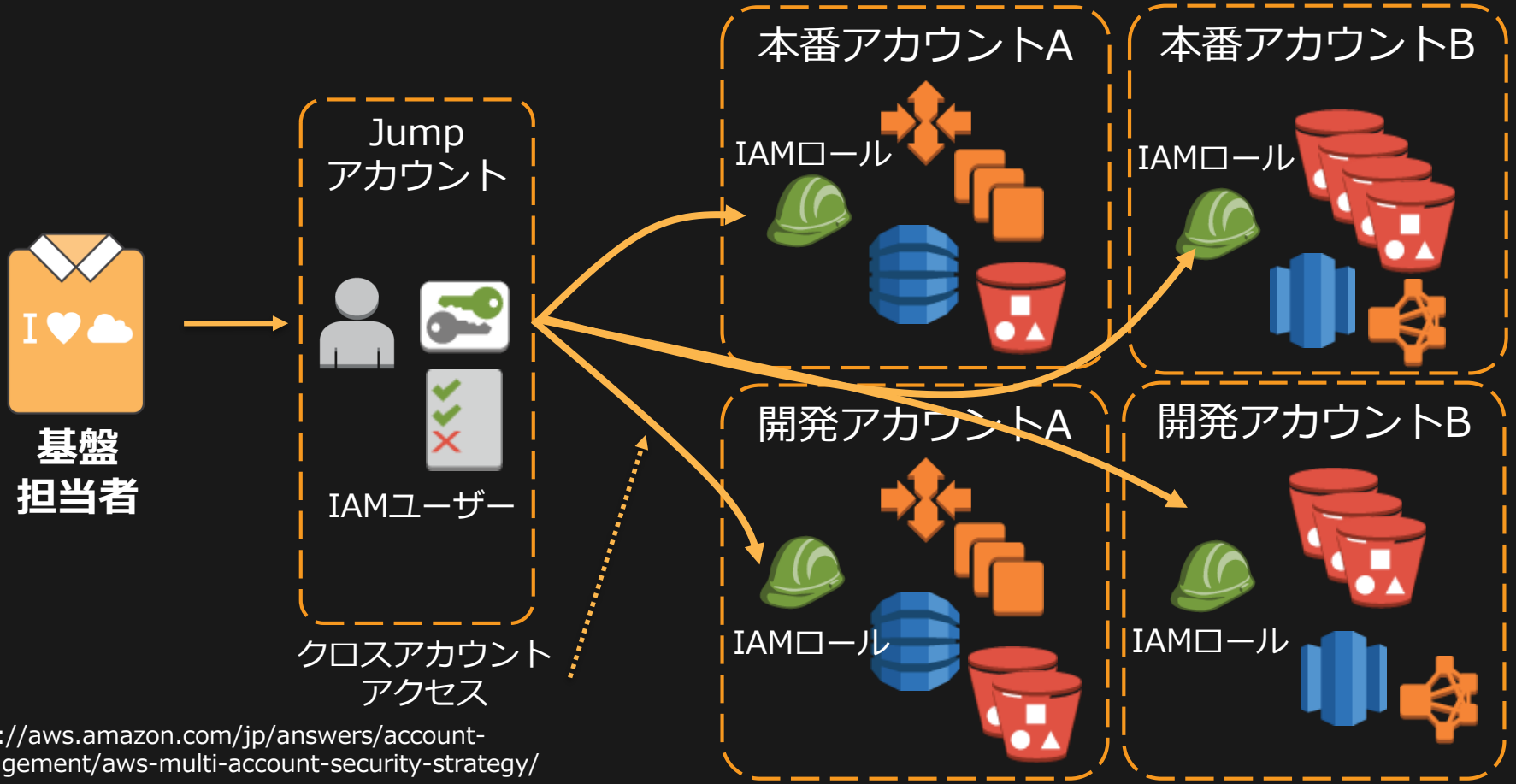
- IAMユーザーからクロスアカウントアクセス用IAMロールに切替

- Switch Roleを活用することにより各アカウントのIAMユーザーとして
  ログインしなおすことなしにセキュアに管理コンソールを切り替え可能

AWS CLI, SDK でも利用可能



クロスアカウントアクセスによる運用効率化



https://aws.amazon.com/jp/answers/account-management/aws-multi-account-security-strategy/

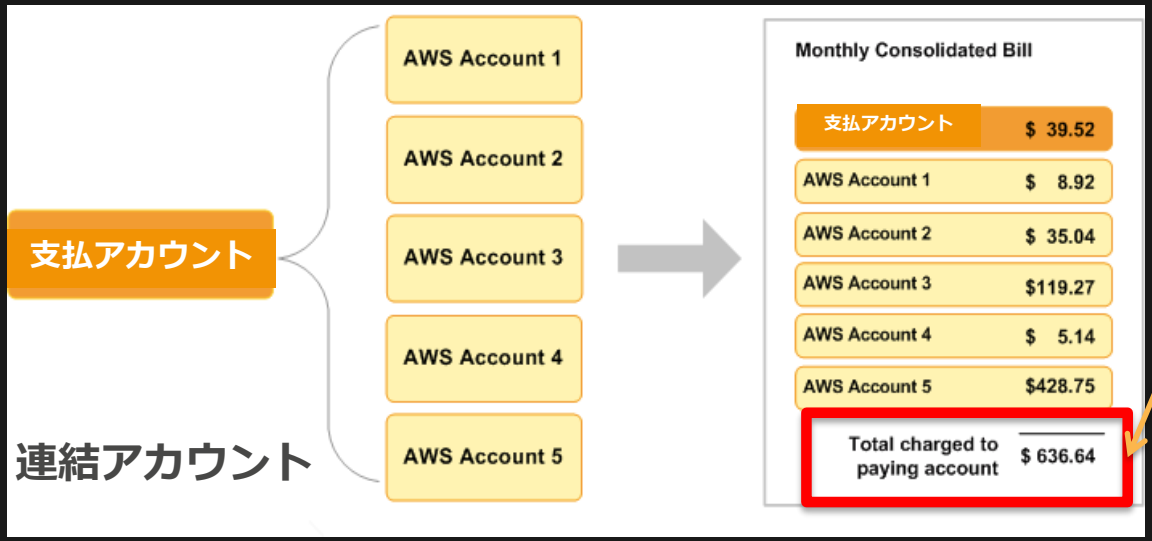
マルチアカウントを管理する機能

- マルチアカウント環境でのアクセス
- マルチアカウントの課金管理
- マルチアカウントのセキュリティ・ログ管理
- マルチアカウントの統制

一括請求（Consolidated Billing）とは

支払おまとめ機能

- 1 つのアカウントを支払いアカウントとして指定し、複数のアカウントに対する支払いを統合可能
- 一括請求対象の全アカウントは請求上、1 つのアカウントとして扱われる



各アカウントごとの
請求金額も確認可能

全アカウントの1 か月間分の費用が請求される

https://aws.amazon.com/jp/answers/account-management/aws-multi-account-billing-strategy/

コスト配分タグを使ったきめ細やかな料金算出

コスト配分タグとは

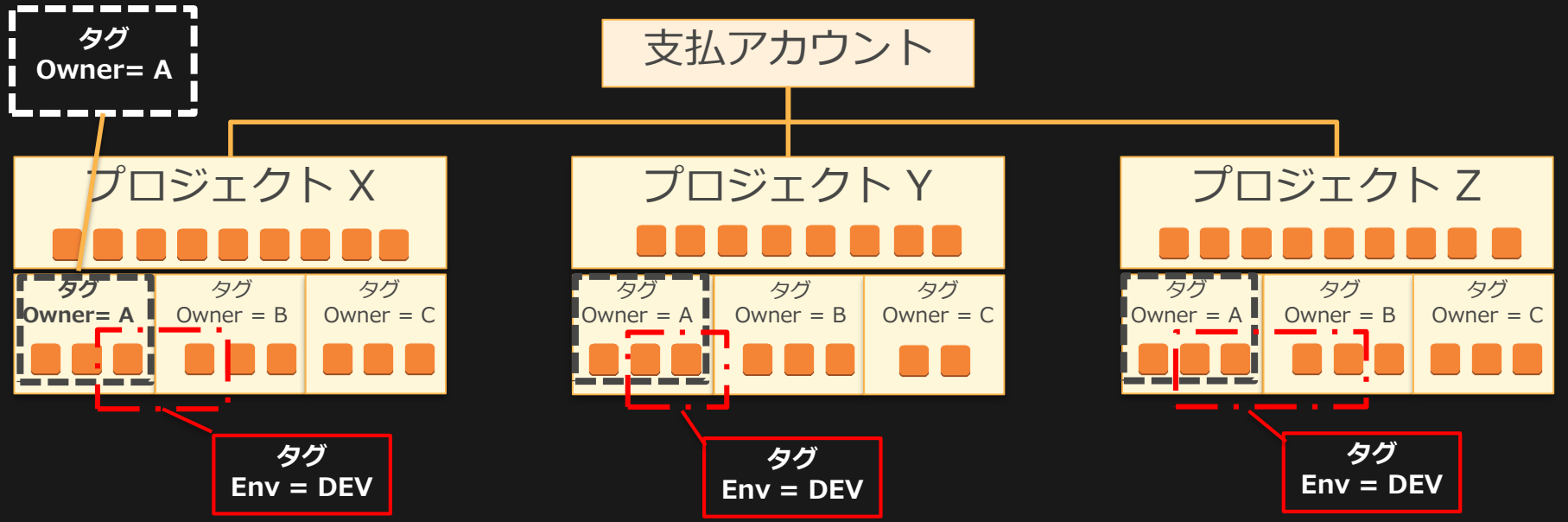
- AWS コストをカテゴライズおよび追跡するためのラベル
- AWS リソース (EC2 インスタンスなど) にカスタムのタグを適用し、そのタグ毎に発生した料金を把握可能
  - 例：部署、プロジェクト etc.

キー	値
ENV	PRD
LOB	IS
Name	WebServer #1
OWNER	YAMADA
RATE	A

タグを用いた複数アカウントでの課金管理

複数アカウントに分けても、共通のタグ運用をすることで、アカウントを跨がる柔軟なコスト管理が可能

- 例) プロジェクトごとにアカウントを分け、コスト配分タグでリソース所有者ごとの金額を算出する。

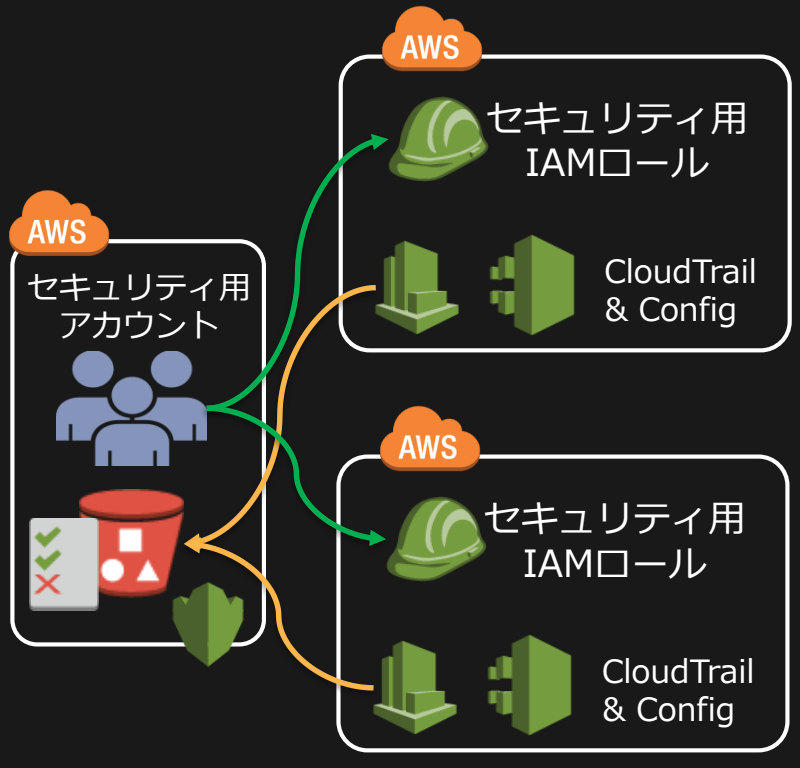


マルチアカウントを管理する機能

- マルチアカウント環境でのアクセス
- マルチアカウントの課金管理
- マルチアカウントのセキュリティ・ログ管理
- マルチアカウントの統制

セキュリティオペレーション用アカウント

- 他のアカウントからの書き込みアクセスのみを許可する、集中管理型のアカウント
- 他のAWSアカウントからのSIEM(Security Information and Event Management)ロギング (例えばCloudTrail、AWS Configなど)
- 他のアカウント全体のログのセキュリティ分析や必要なリスク対応を担う
- ログ暗号化のためのKMSキー管理
- セキュリティ調査、監査業務のためのクロスアカウントアクセス



CloudTrailは
全リージョンで有効化

https://aws.amazon.com/jp/answers/account-management/aws-multi-account-security-strategy/

マルチアカウントを管理する機能

- マルチアカウント環境でのアクセス
- マルチアカウントの課金管理
- マルチアカウントのセキュリティ・ログ管理
- マルチアカウントの統制

AWS Organizations

AWS アカウントのグループを作成して
セキュリティと自動化の設定管理がもっと簡単になります。

AWS Organizations サービス概要

複数アカウントの一元管理

- アプリケーション、環境、チーム毎のグループ化
- グループポリシー適用

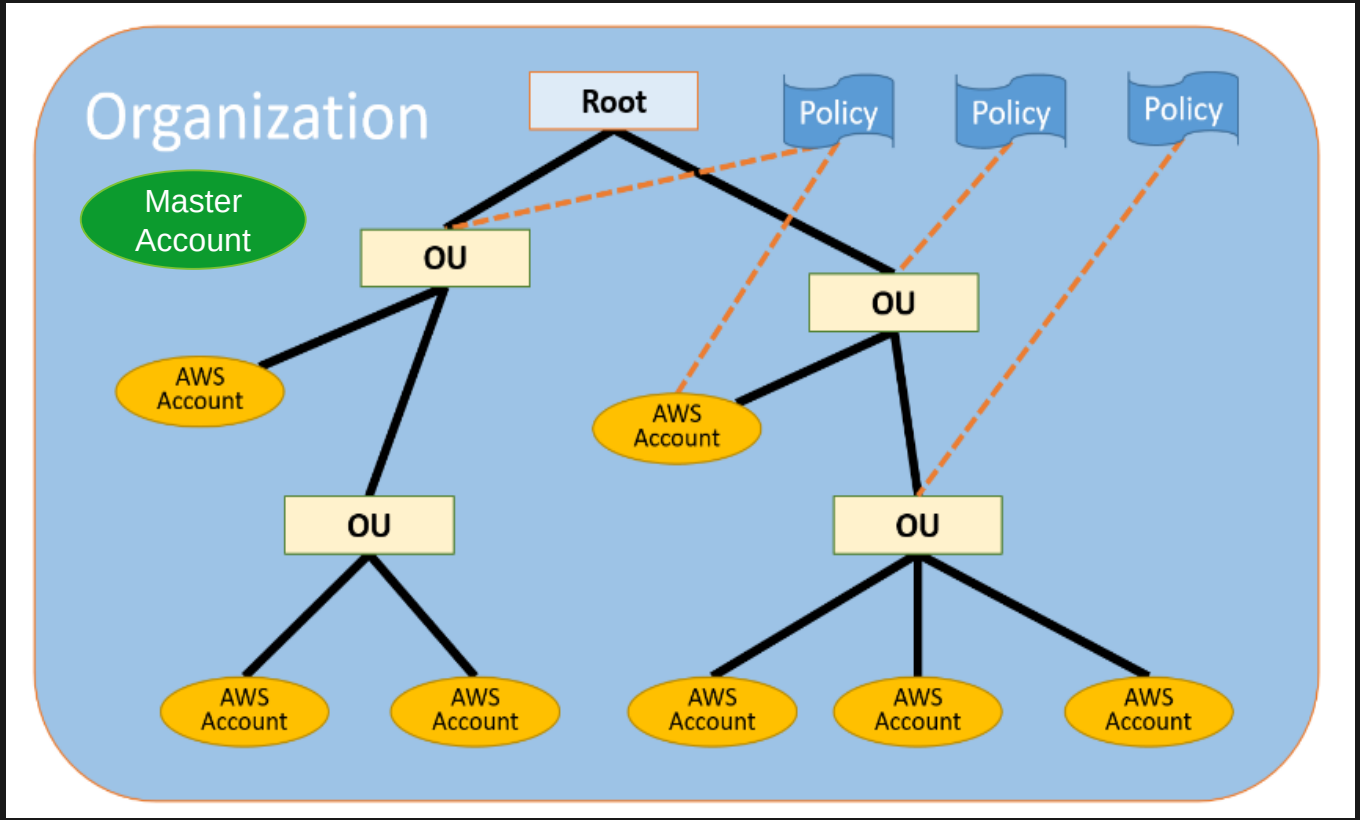
AWSアカウント管理の自動化

- コンソール、SDK、CLIでの管理操作
- 全ての管理操作のロギング(CloudTrail)

請求の簡素化

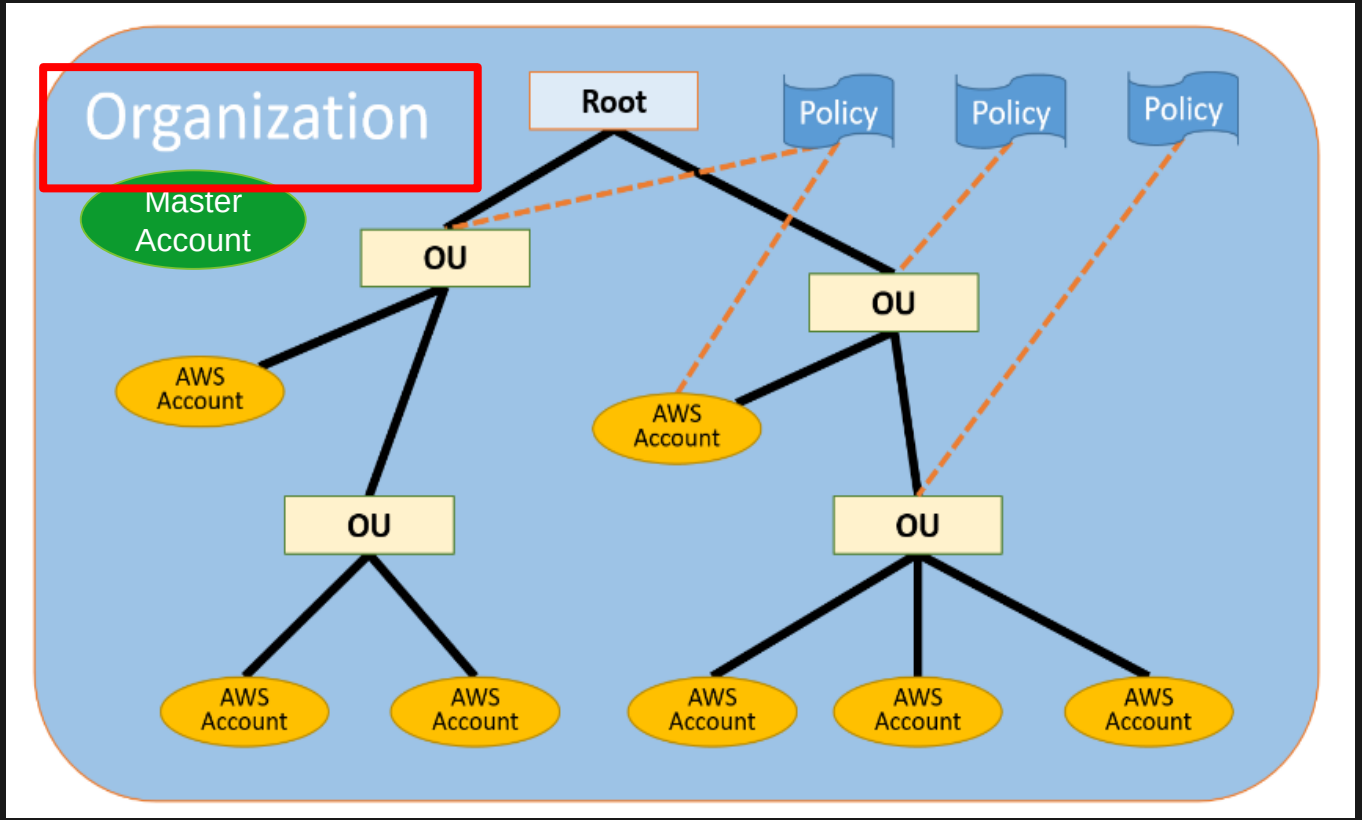
- 複数アカウントの一括請求 (Consolidated Billing)
- CBファミリーの自動移行

AWS Organizationsの主要コンセプト



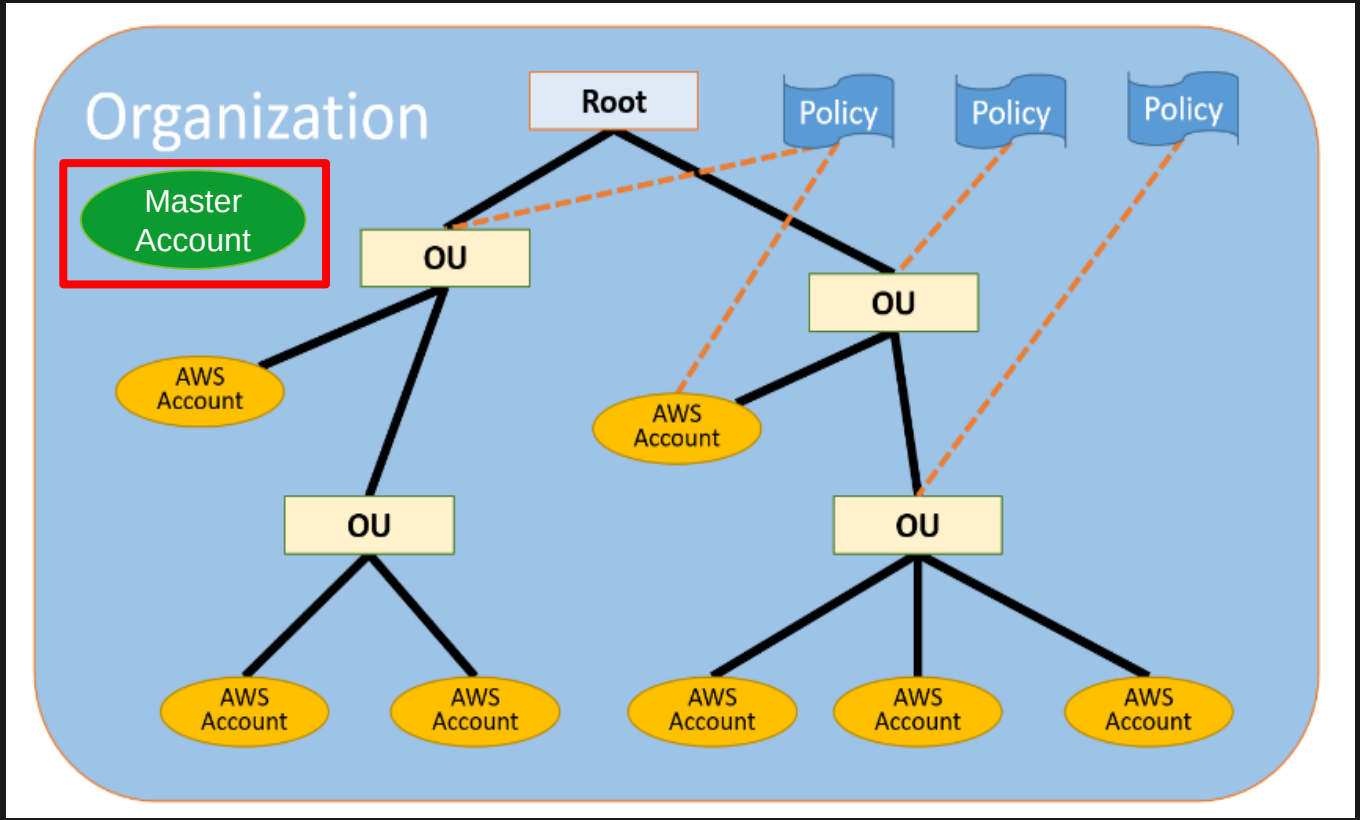
- 組織
- マスターアカウント
- AWSアカウント
- 組織単位 (OU)
- 管理用ルート
- 組織コントロールポリシー (OCP)

AWS Organizationsの主要コンセプト



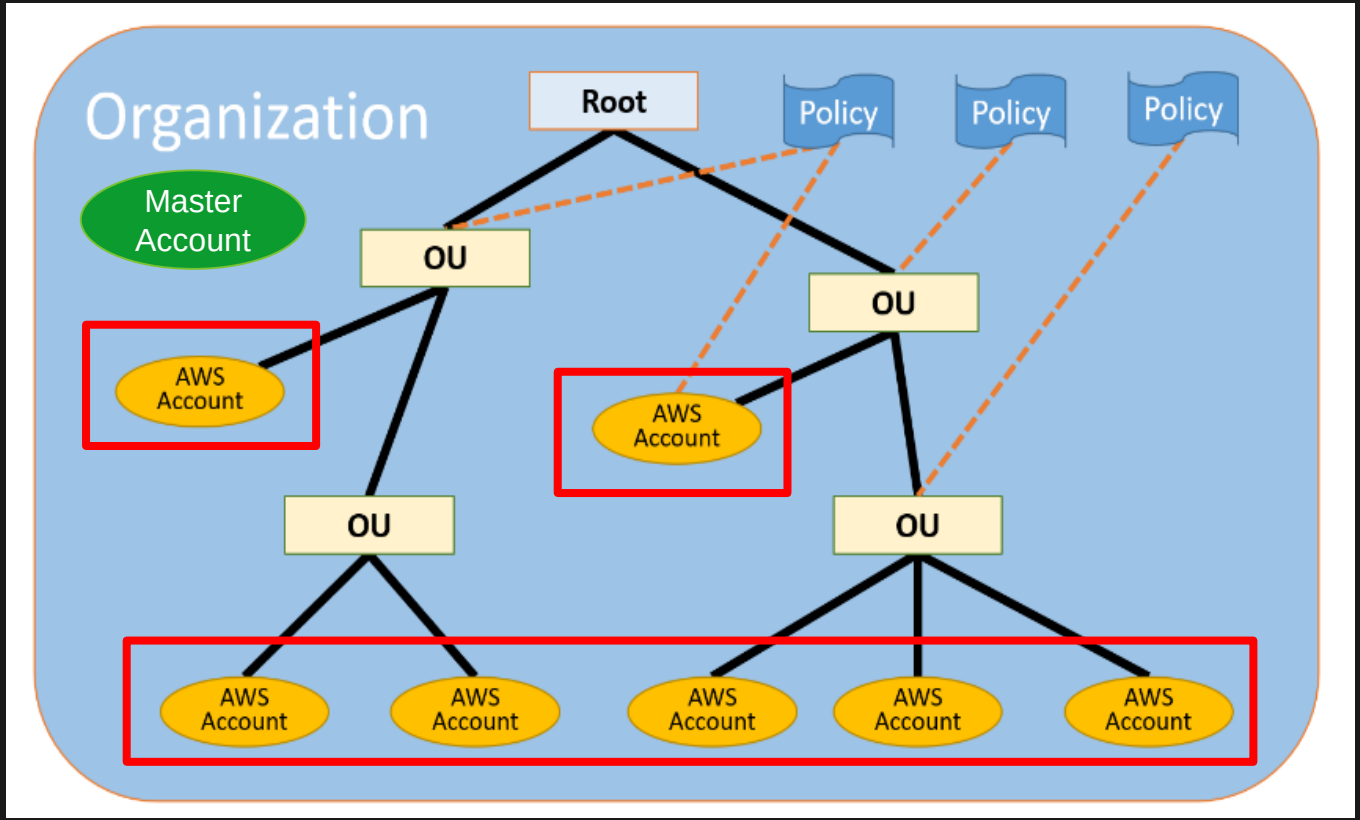
- **組織**
- マスターアカウント
- AWSアカウント
- 組織単位 (OU)
- 管理用ルート
- 組織コントロールポリシー (OCP)

AWS Organizationsの主要コンセプト



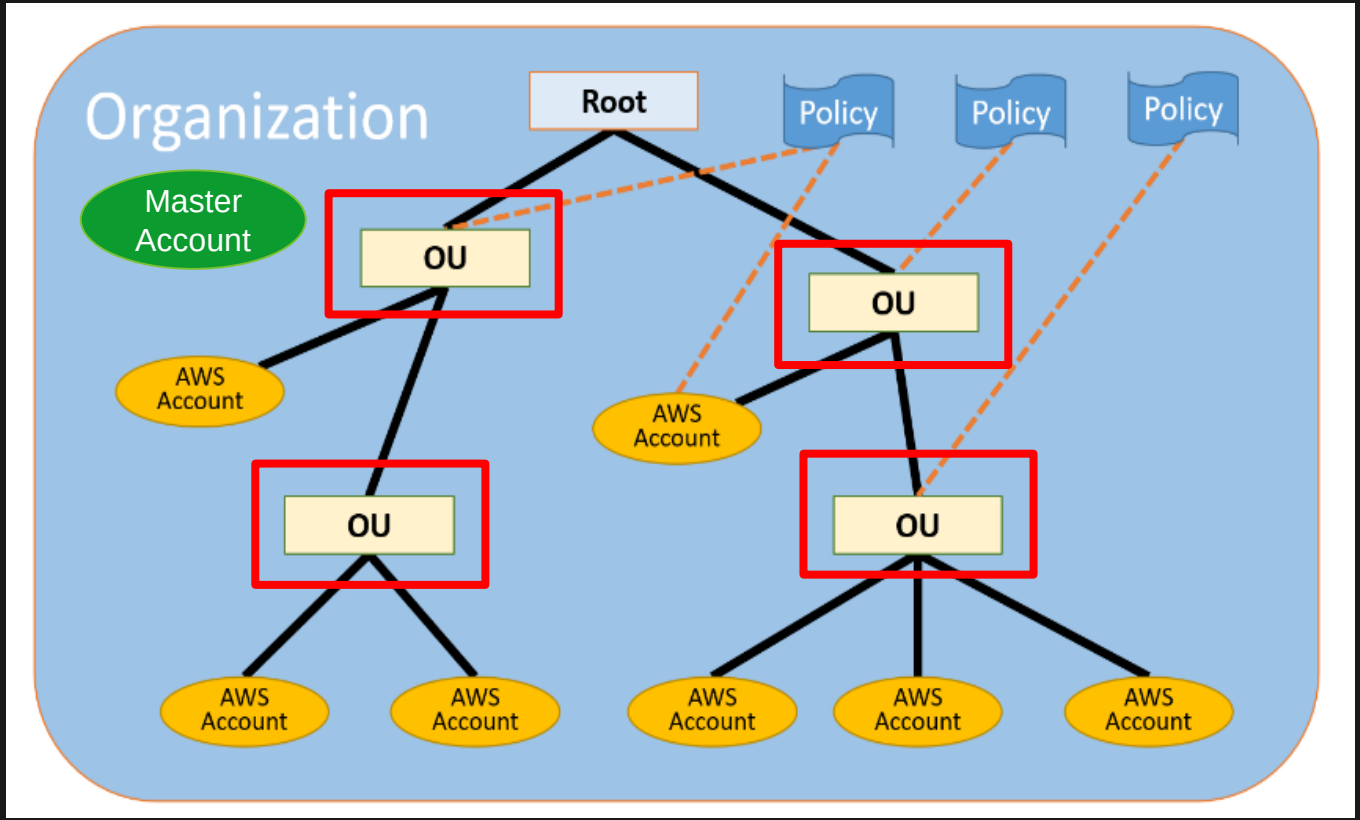
- 組織
- **マスターアカウント**
- AWSアカウント
- 組織単位 (OU)
- 管理用ルート
- 組織コントロールポリシー (OCP)

AWS Organizationsの主要コンセプト



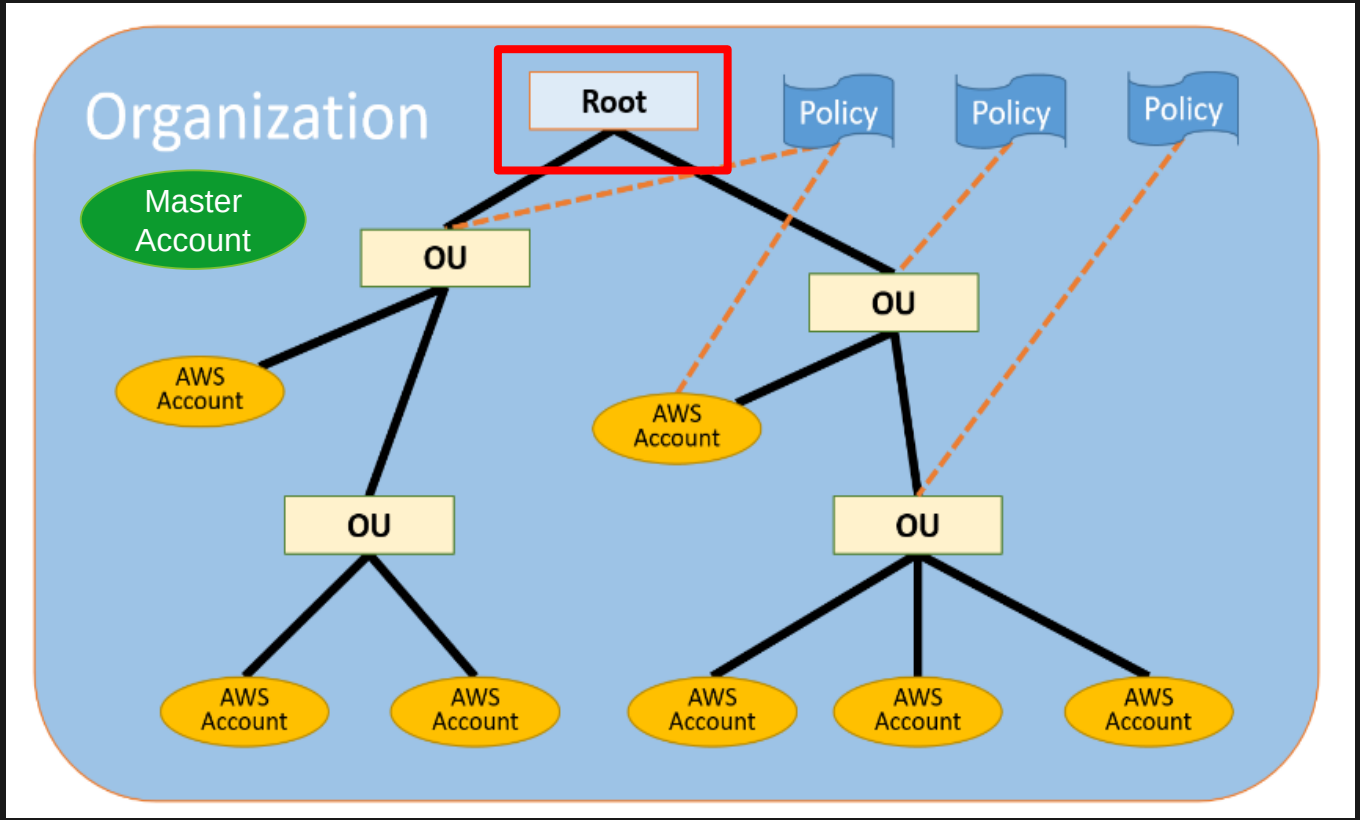
- 組織
- マスターアカウント
- **AWSアカウント**
- 組織単位 (OU)
- 管理用ルート
- 組織コントロールポリシー (OCP)

AWS Organizationsの主要コンセプト



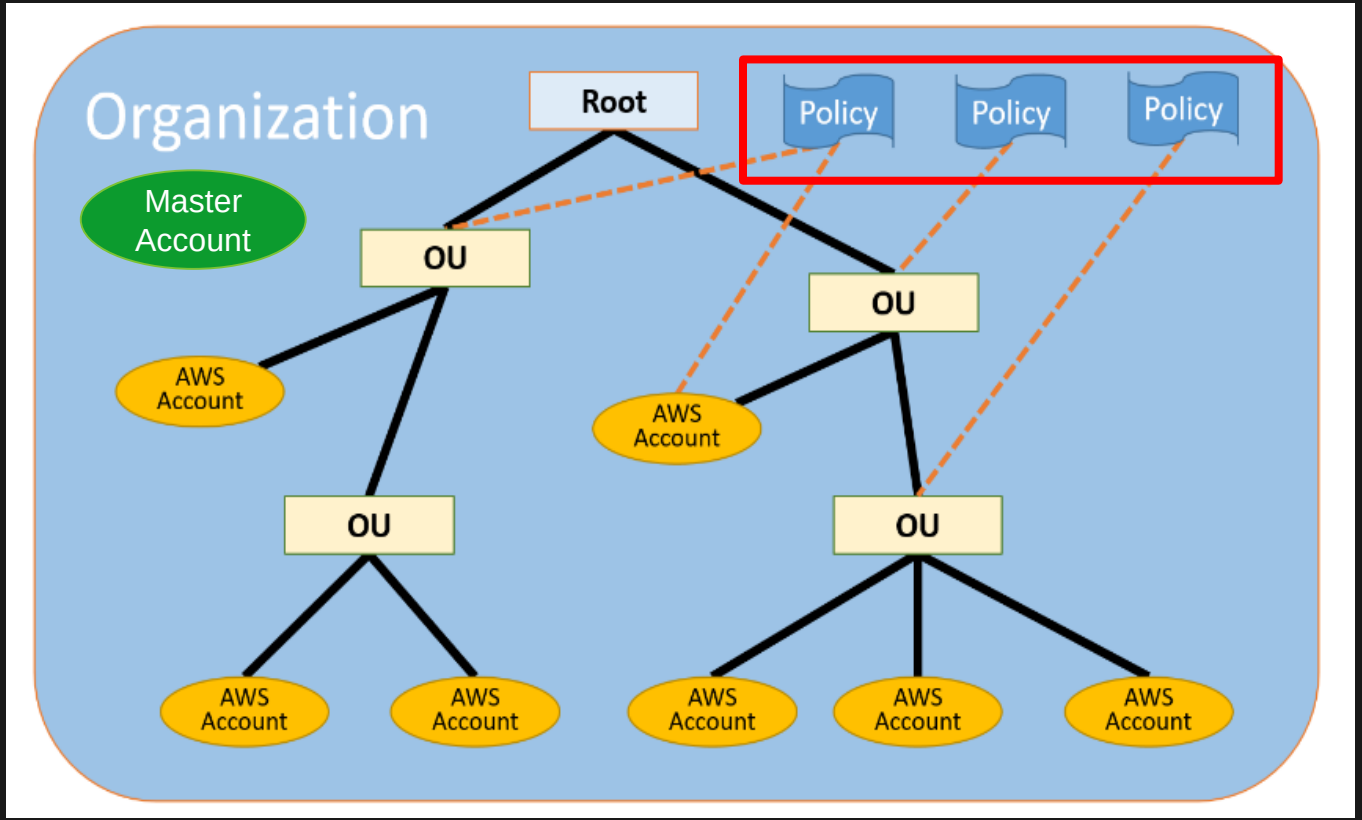
- 組織
- マスターアカウント
- AWSアカウント
- **組織単位 (OU)**
- 管理用ルート
- 組織コントロールポリシー (OCP)

AWS Organizationsの主要コンセプト



- 組織
- マスターアカウント
- AWSアカウント
- 組織単位 (OU)
- **管理用ルート**
- 組織コントロールポリシー (OCP)

AWS Organizationsの主要コンセプト



- 組織
- マスターアカウント
- AWSアカウント
- 組織単位 (OU)
- 管理用ルート
- **組織コントロールポリシー (OCP)**

Organizationsによる新規AWSアカウントの作成

- 新規アカウントはマスターアカウントからのみ作成
- 作成時に必要な情報
    - Eメールアドレス (必須)
    - アカウント名 (必須)
    - IAMロール名 (任意、デフォルト名: OrganizationAccountAccessRole)
        - マスターアカウントからのAssumeRoleが許可される
        - **フルコントロール**権限が付与される
    - billingへのIAMユーザアクセス(任意、IAMユーザには権限が必要)
- 作成された新規アカウントは**自動的に**組織のメンバーアカウントに
- root管理者パスワードは、パスワードを忘れた場合の手順で設定可能
- 既存アカウントも組織に招待可能

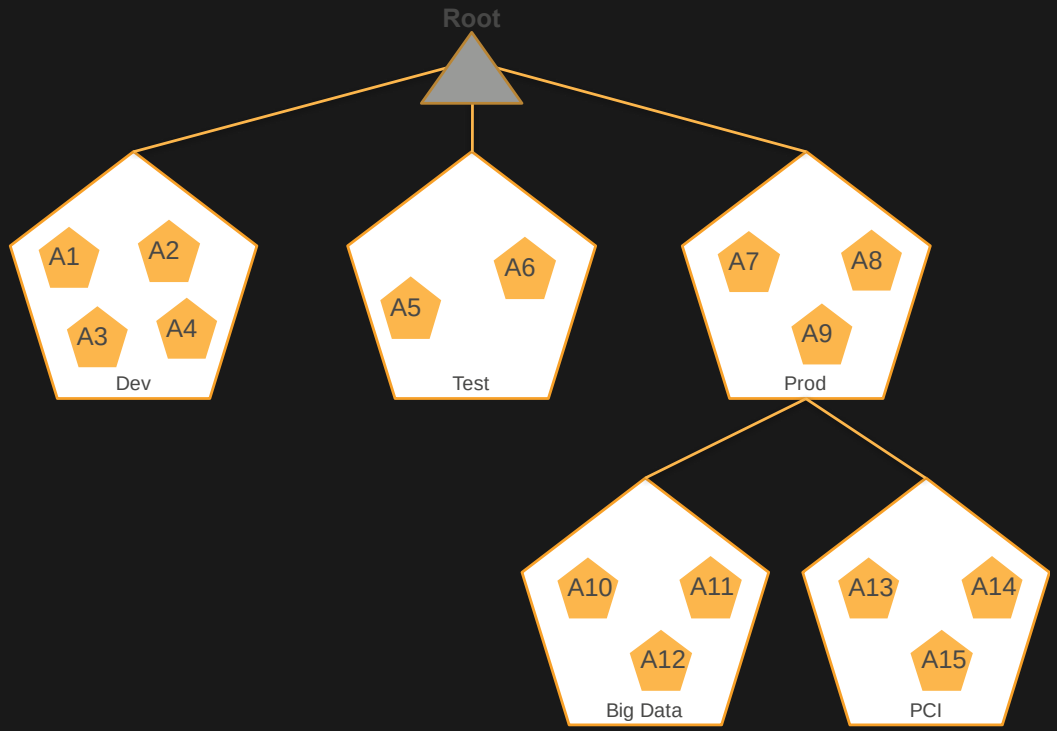
CLIのサンプル – CreateAccount

```
aws organizations create-account
      --email aws.prod@example.com
      --account-name "Production Account”
      --role-name Role-to-access-account
```

- 有効なメールアドレスであることを確認
  - 現状、通知メールは root管理者のメールアドレスへ送付
  - いくつかの操作はroot管理者のみが実行可能
- メールアドレスは絶対に再配布しない
- **Tips:** 多くのメールシステムは、アドレスローカル部の「+」の後の文字列を無視するので、同じメールアドレスで複数アカウントを作成する際に利用可能
  例) aws.prod+acc1@example.com, aws.prod+acc2@example.com

AWSアカウントの論理グループ

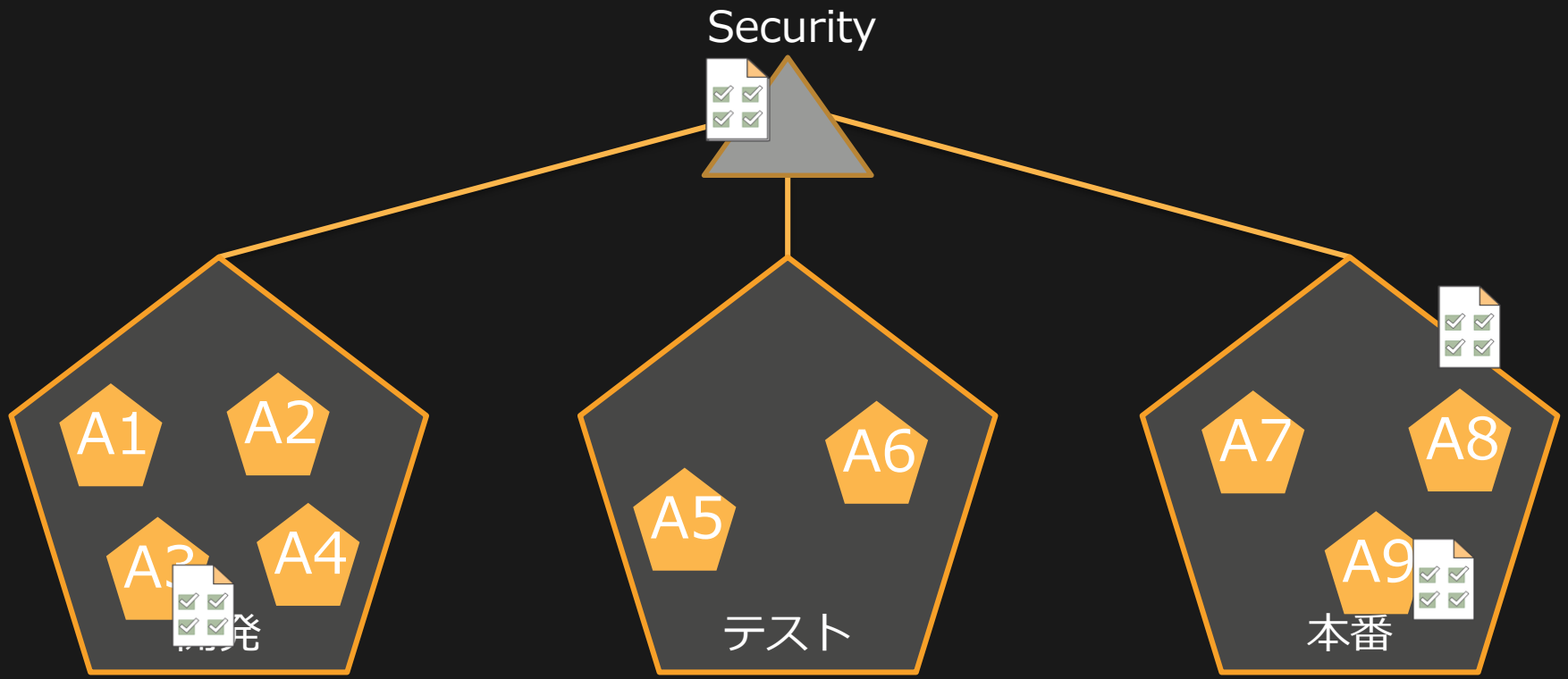
- グループ内のアカウントはOUに追加可能
- アカウント・OUは他のOUのメンバーになることが可能
- アカウントは同時に複数のOUのメンバーになることができない



組織コントロールポリシー (OCP)

- 適用すべきポリシーを記述したもの
- ユースケースごとに異なる種類のOCPが使用される
- OCPが適用される対象:
  - 組織全体
  - 組織単位(OU)
  - AWSアカウント
- 組織の階層構造に基づいて継承される (AWSアカウント、OU、 組織)

AWS Organizationsによる権限管理



組織コントロールポリシー(OCP)は
サービスコントロールポリシー(SCP)をサポート

- OCPの一種で、どのAWSサービスのAPIにアクセス可能かコントロールする
    - 許可されたAPIを定義 – **ホワイトリスト**
    - 拒否されたAPIを定義 – **ブラックリスト**
- ローカルの管理者からは上書きできない
- SCPとIAMポリシーの両方で許可されたAPIが、IAMユーザ/ロールで最終的にアクセス可能
- 通常のポリシールールと同様、明示的な許可(ALLOW)よりも**明示的な拒否(DENY)**が優先される
- **絶対に利用しないサービスを明確にしてブラックリスト化する**
- IAMポリシーシミュレータはSCPにも利用可能
- 要件がより明確・詳細なったらその都度、より複雑なポリシーを適用していく

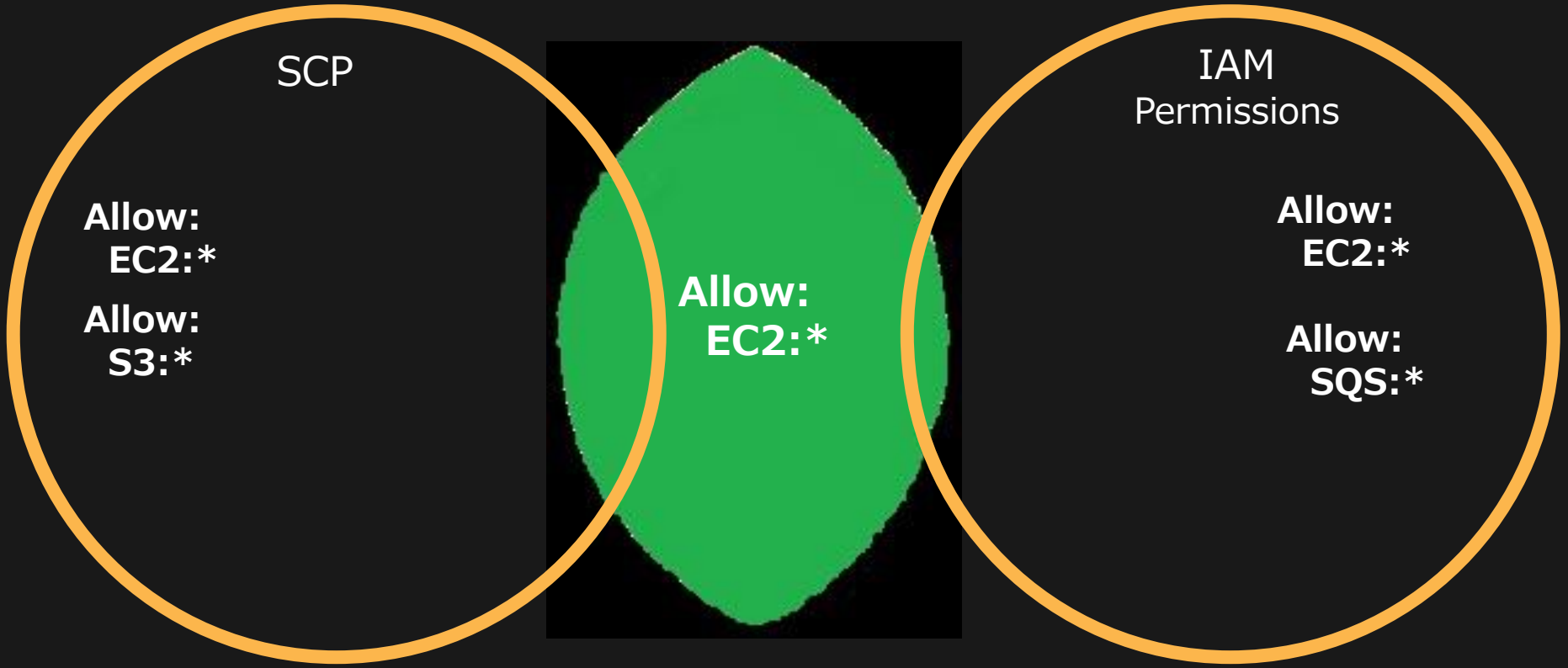
ブラックリストの例

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": ” lambda:*",
      "Resource": "*"
    }
  ]
}
```

ホワイトリストの例

```
{
 "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
                  "ec2:RunInstances",
                  "ec2:DescribeInstances",
                  "ec2:DescribeImages",
                  "ec2:DescribeKeyPairs",
                  "ec2:DescribeVpcs",
                  "ec2:DescribeSubnets",
                  "ec2:DescribeSecurityGroups"
      ],
      "Resource": "*"
    }
 ]
}
```

SCPとIAM権限による権限管理



管理レベルの選択

新しい組織を作成する時は、どちらのモードで作成するかを選択

- Billing モード
  - 現行の一括請求(CB)との互換性あり
  - FinancialコントロールのOCPのみ管理可
  - 一括請求(CB)ファミリーからの組織作成は自動でBillingモード

- Full Control モード
  - Billingモードを包含
  - あらゆる種類のOCPを管理可
  - BillingモードからFull Controlモードへの変更は組織内の全てのAWSアカウントの同意が必要

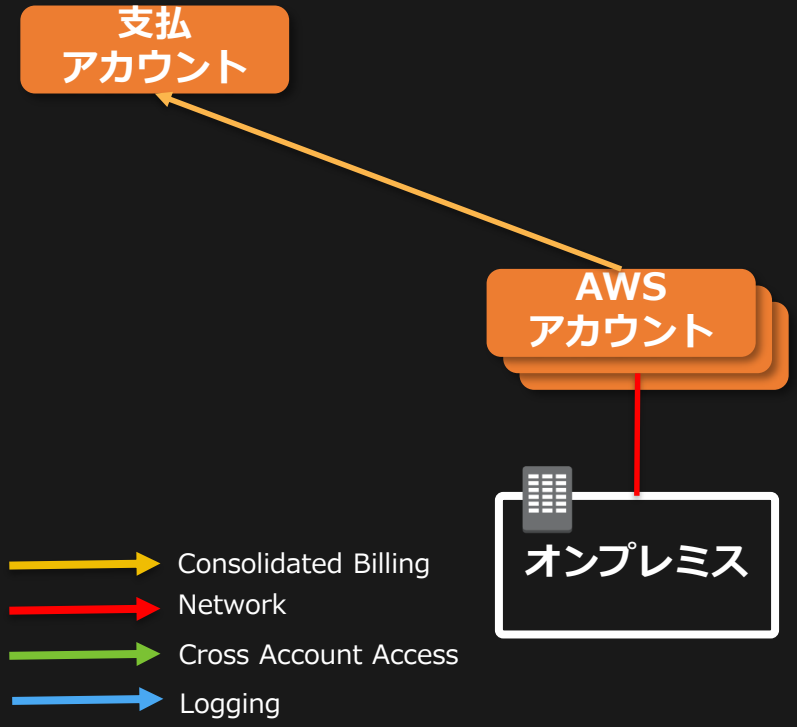
AWS Organizationsのベストプラクティス

1. マスターアカウント内のアクティビティはCloudTrailを利用して監視
2. 組織のマスターアカウントでリソース管理は行わない
3. 「最小権限」の原則に則って組織を管理
4. コントロールポリシーはOUに対してアタッチ
5. まずは単一AWSアカウントでコントロールポリシーをテスト
6. 組織の管理用ルートに対しては必要な時のみコントロールポリシーをアタッチ
7. SCPで“ホワイトリスト”と“ブラックリスト”を混在させないようにする
8. 新規アカウントは必要がある時のみ作成する

本日のまとめ

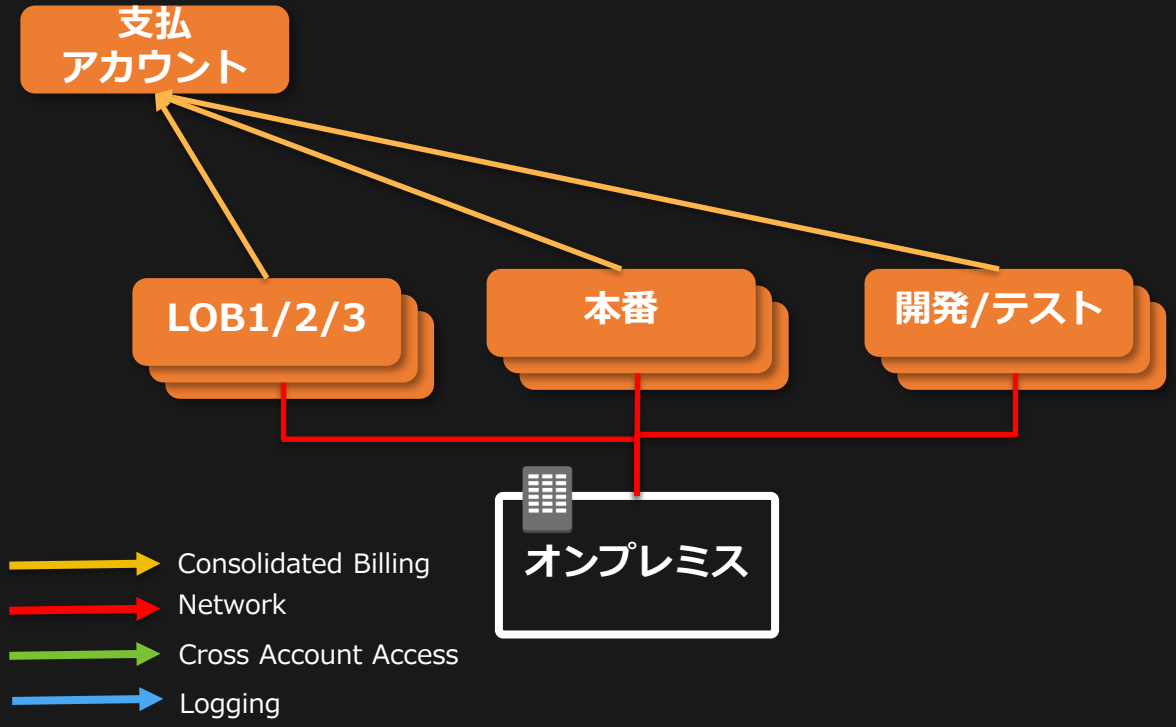
マルチアカウントのベストプラクティス

マルチアカウントのベストプラクティス



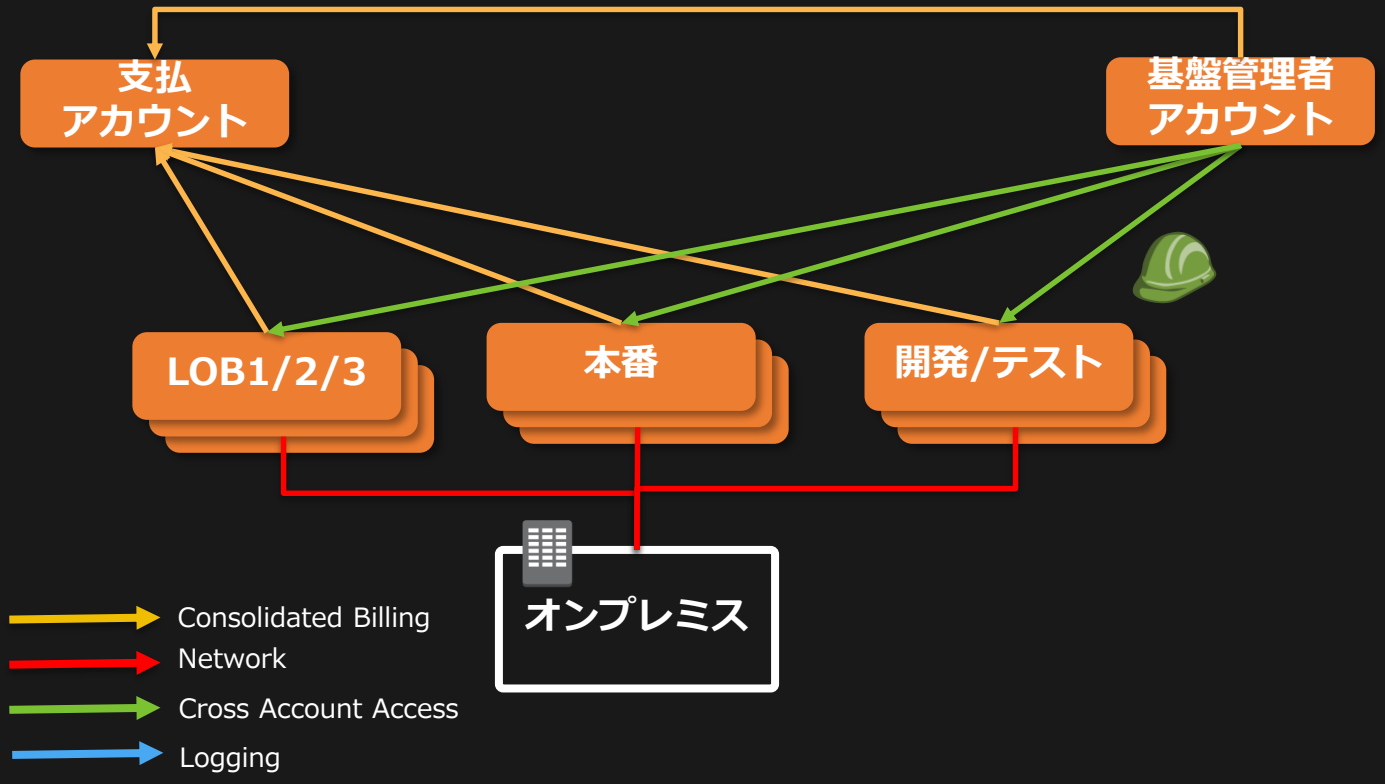
- **請求管理用のアカウント**を作成し、複数アカウントの課金情報をとりまとめる

マルチアカウントのベストプラクティス



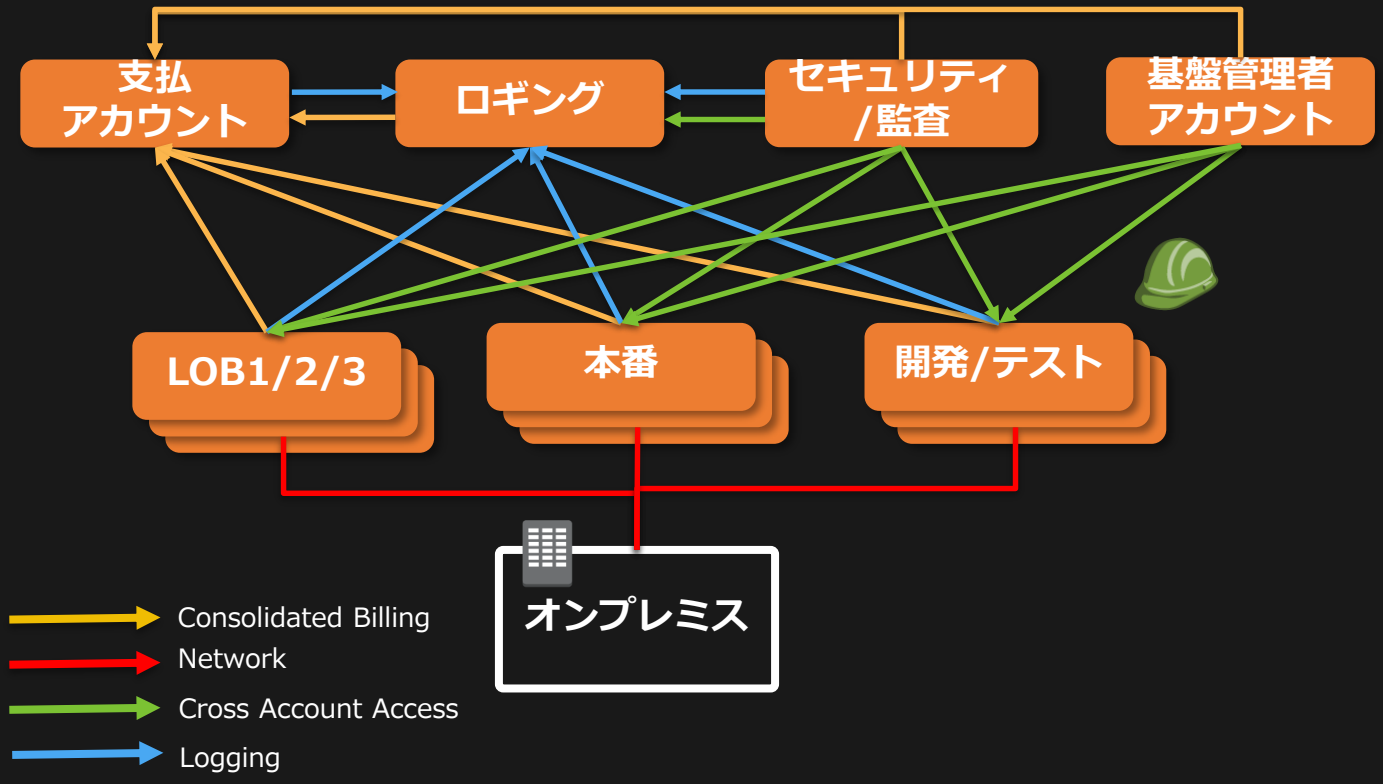
- ワークロードや環境、LOB毎に**アカウントの分割を検討**
- 分割の際には**ガバナンス、課金、組織、運用といった観点**から自社にとってのメリット・デメリットを考慮
- 各アカウントの**請求は支払いアカウント**にまとめる

マルチアカウントのベストプラクティス



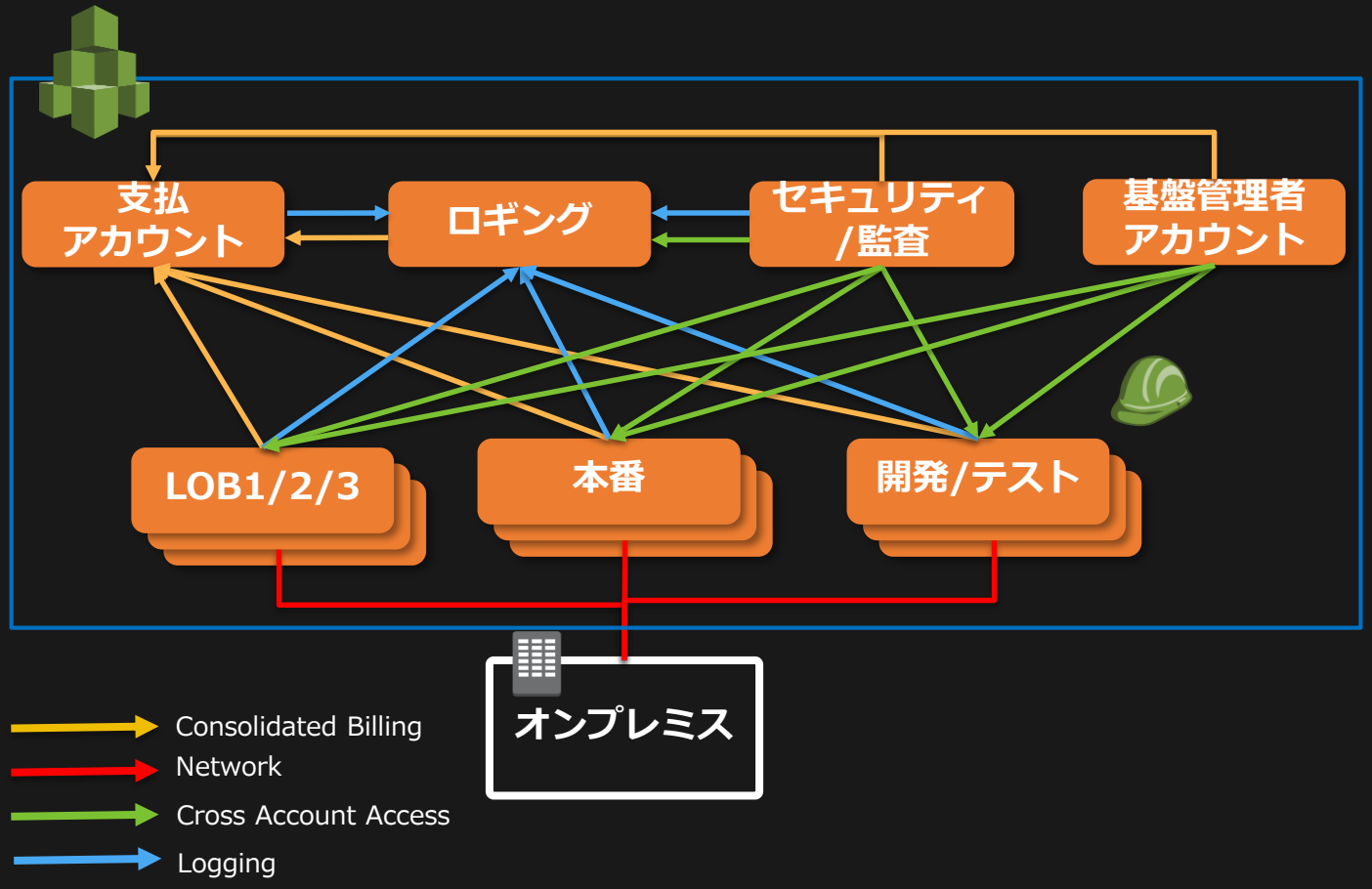
- 複数アカウントの集中管理が必要な場合には、**クロスアカウントアクセス**のできるアカウントによる**運用効率化・自動化**の検討を行う

マルチアカウントのベストプラクティス



- 複数アカウントからの**ログをセキュアに集約**するアカウントを作成
- **セキュリティ調査や監査業務用**にクロスアカウントアクセスにより、情報の収集をできる専用アカウントを作成

マルチアカウントのベストプラクティス



- 多くのアカウントを**集中管理**する必要のある場合はAWS Organizationsの利用
- アカウントの一元管理と運用自動化、課金管理の簡素化に活用

本日のまとめ

- AWSのマルチアカウント方針に単一の答えはありません
- 複数の切り口で、メリット・デメリットを考えつつ、自社にベストな方針を検討する必要があります
- AWSにはアカウント管理を支援する機能が多くあります
- 課金管理やセキュリティ用アカウントの利用、運用管理の効率化を検討してください
- 新機能のリリースを常にウォッチして、実装方法を適宜見直していきましょう

本セッションのFeedbackをお願いします

受付でお配りしたアンケートに本セッションの満足度やご感想などをご記入ください
アンケートをご提出いただきました方には、もれなく素敵なAWSオリジナルグッズを
プレゼントさせていただきます

アンケートは受付、又はパミール3FのEXPO展示会場内にて回収させて頂きます

AWS

SUMMIT

ご清聴ありがとうございました

amazon web services