aws INNOVATE
ONLINE CONFERENCE

増加するシステムをマルチアカウントで効率よく管理する

大村 幸敬
アマゾン ウェブ サービス ジャパン
技術統括本部 ソリューションアーキテクト

Twitterハッシュタグ #AWSInnovate

本セッションについて

セッションの対象者

- 複数のシステムが稼働するAWSの環境全体のセキュリティやガバナンスを担当する
  クラウド推進担当者または共通基盤管理担当の方
- （AWSの運用系サービス個別の詳細は BlackBelt オンラインセミナーの資料などをご覧ください）

セッションのゴール

- マルチアカウント環境で何が実現できるかを説明できる
- マルチアカウント環境を管理するための具体的な手法を説明できる

今回扱う課題リスト

- マルチアカウント管理の仕組み（Landing Zone）を独自に実装するにはどうしたらよいのか？

【ご連絡事項】
本セッション内容について確認するためのクイズおよび簡単なアンケートがセッションの最後にあります。
なおクイズの回答はアンケートとあわせて表示されます。

アジェンダ

増え続けるシステムの管理に必要なもの

マルチアカウント管理の概要

マルチアカウント管理の実装例

まとめ

クイズ

増え続けるシステムの管理に必要なもの

aws INNOVATE
ONLINE CONFERENCE

多数のシステムをどのように管理するか

- AWSで稼働するシステムの増加
  - 1　　… そのシステムの管理者がAWS自体の管理も行う
  - 数個　… 共通基盤チームがAWS自体の管理と個別システムの監査を行う
  - 多数　… 仕組みなしにすべてのシステムを管理するのは困難

- 仕組み
  - マルチアカウント化
  - IAMやタグなど権限管理の簡素化、強制化
  - AWS環境提供の自動化
  - ログの集約や保護の実施
  - 共有サービス利用のためのネットワーク構成

AWSアカウントを分割する目的

アカウント分割でVPCだけでなくAPIのレベルで環境を分ける
これによって...

環境

開発、テスト、本番などの環境をセキュリティやガバナンス、規制のために分離できる（PCIなど）

課金

部門単位やシステムの単位でAWSのコストが明確に分離できる

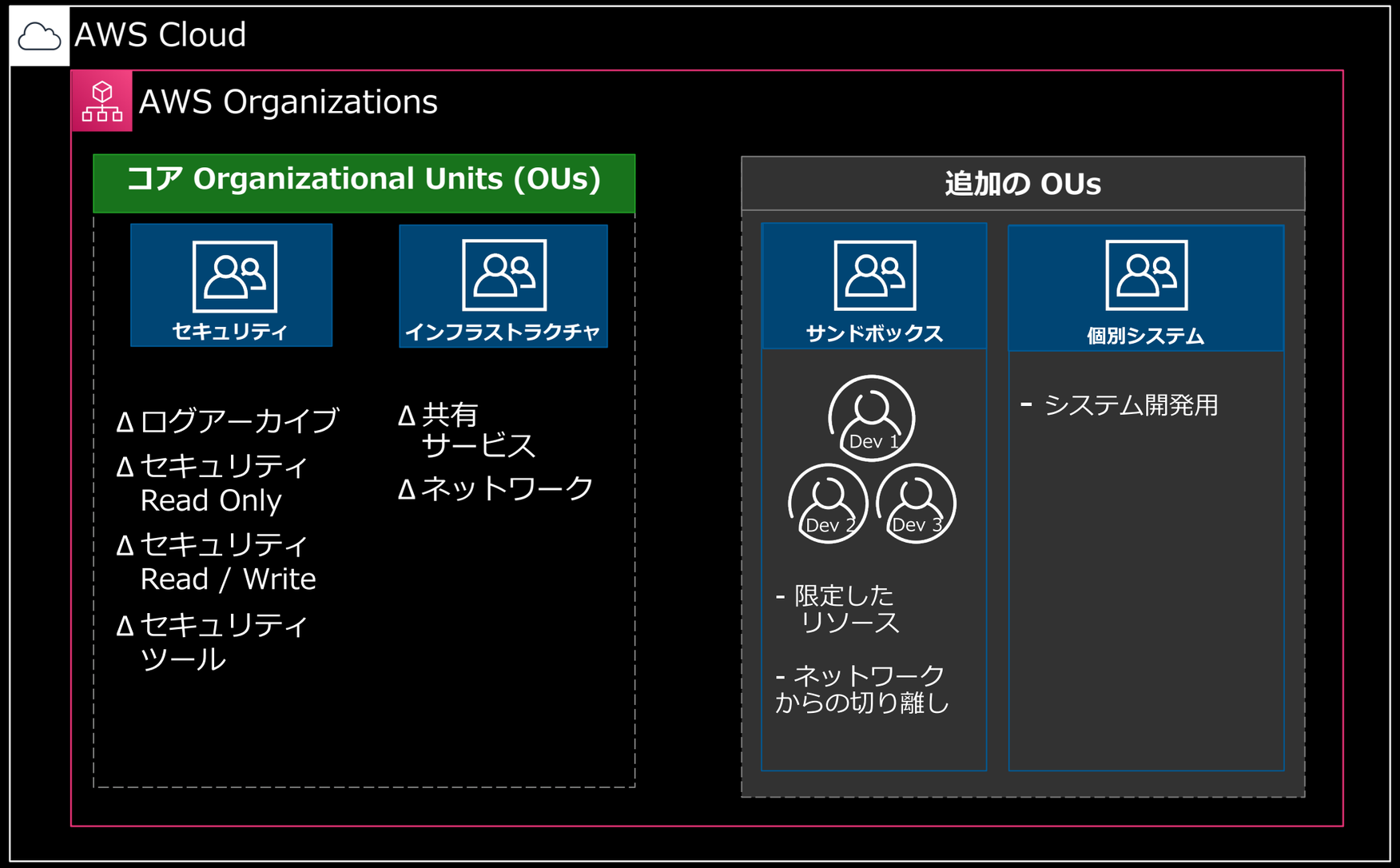
ビジネス推進

事前定義されたガバナンスフレームワークの中で特定のビジネス部門に対する権限の委譲が行える

ワークロード

外部向け/社内向けサービスや、リスクやデータ分類、顧客の違いなどに応じてワークロードを分離できる

マルチアカウント管理のフレームワーク



「Landing Zone」の実装

- Landing Zoneとは
  - セキュアで事前設定済みのAWSアカウントを提供する仕組みの総称
  - ツールを活用してスケーラブルかつ 高い柔軟性を提供
  - ビジネスのアジリティとイノベーションを実現

- 実装1: AWS Control Tower
  - AWSサービスとして提供される Landing Zone （東京リージョンは未対応）
  - 容易に利用開始できるが、既存アカウントへの適用やカスタマイズに制限あり
  - これからAWSを利用する場合に利用

- 実装2: 独自実装の Landing Zone
  - マルチアカウント戦略に基づき独自に実装する Landing Zone
  - 自社の方針にしたがって自由にカスタマイズ可能
  - 既存アカウントに適用する場合に利用

よくご相談いただく課題

- Landing Zone を独自で実装するにはどうしたらよいのか？

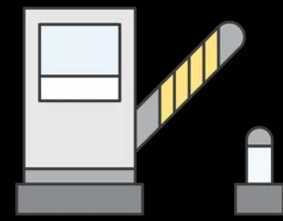
マルチアカウントの管理

aws INNOVATE
ONLINE CONFERENCE

マルチアカウント管理の実際

1. アカウントの発行
   - 必要な初期設定の済んだアカウントを作成
2. 管理用権限の発行
   - 対象アカウントを管理するための権限を作成
3. 共有サービスへのアクセス
   - ADなどの共有サービスやオンプレミスへの接続経路の確保
4. AWSログの集約
   - 監査用ログの集中かつ安全な保存
5. ガードレールの設置
   - 実施してはいけない操作の禁止、危険な設定の監視

ガードレール

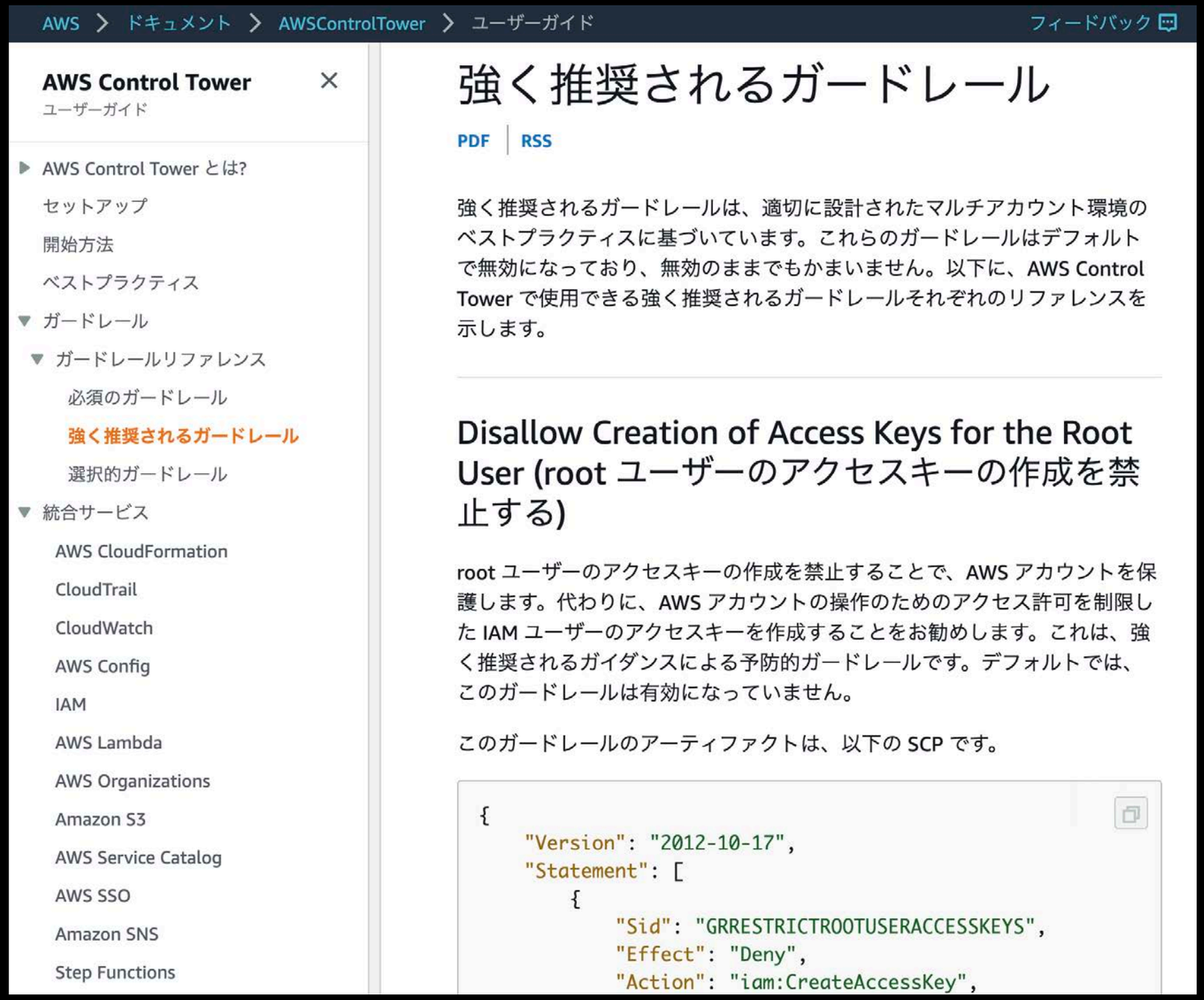


- 予防的ガードレール
  - 対象の操作を実施できないようにするガードレール
  - Organizations Service Control Policy （SCP）で実装する
  - OUやアカウントに対する許可/拒否ポリシーを設定

- 発見的ガードレール
  - 望ましくない操作を行なった場合、それを発見するガードレール
  - 管理しつつ開発のスピードを上げるために効果的
  - AWS Config Rulesで実装する

実装のアプローチ

- Control Tower の実装はAWSサービスの組み合わせ
- 特にガードレールは具体的な実装がControl Tower のドキュメントに記載
- これを参考に自社で必要なLanding Zone を実装



https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/what-is-control-tower.html

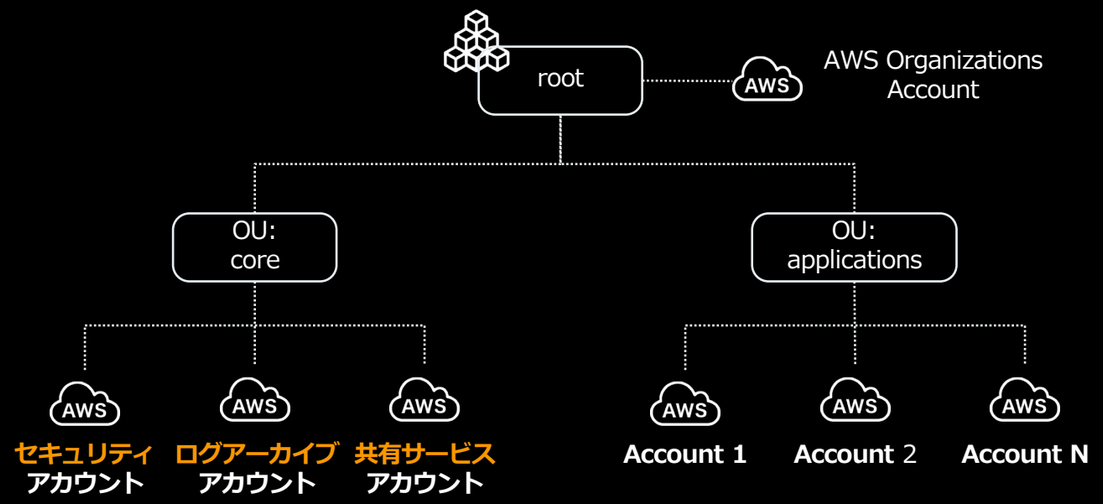
マルチアカウント管理の実装例

aws INNOVATE
ONLINE CONFERENCE

0. アカウント 構成

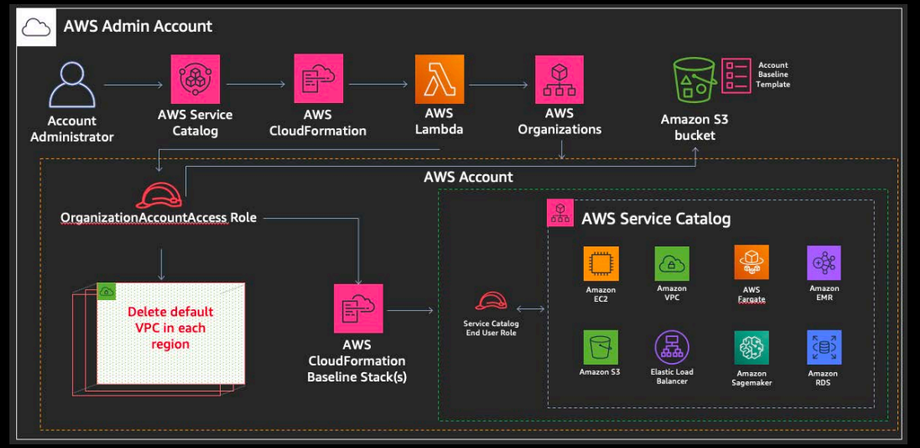
- マルチアカウント管理のフレームワークに準拠する構成を推奨
  - すべてをフレームワークの通りにする必要はない
  - 組織の実情に合わせて実装する

- 実装例
  - マスター (root) アカウント
  - Core OU
    - セキュリティアカウント
    - ログアーカイブアカウント
    - 共有サービスアカウント
  - カスタムOU
    - アプリケーションアカウント



1. アカウント の発行

- スクリプト（AWS CLI）やプログラムで実装
  - Organizations でアカウントを作成
  - Organizations SCP の設定
  - ベースライン（基本設定）用の CloudFormation Stack を作成
    - 管理用権限（IAM Role） の発行
    - AWS Config Rules の設定
    - 標準VPCの作成・設定 など



実装の一例： Account Vending Machine
https://github.com/aws-samples/aws-account-vending-machine

- Service Catalogでアカウントを作成可能
- 作成したアカウント上でもServiceCatalogによる各種環境のデプロイが行えるようになる
- この実装が推奨なのではなく、あくまで実装例

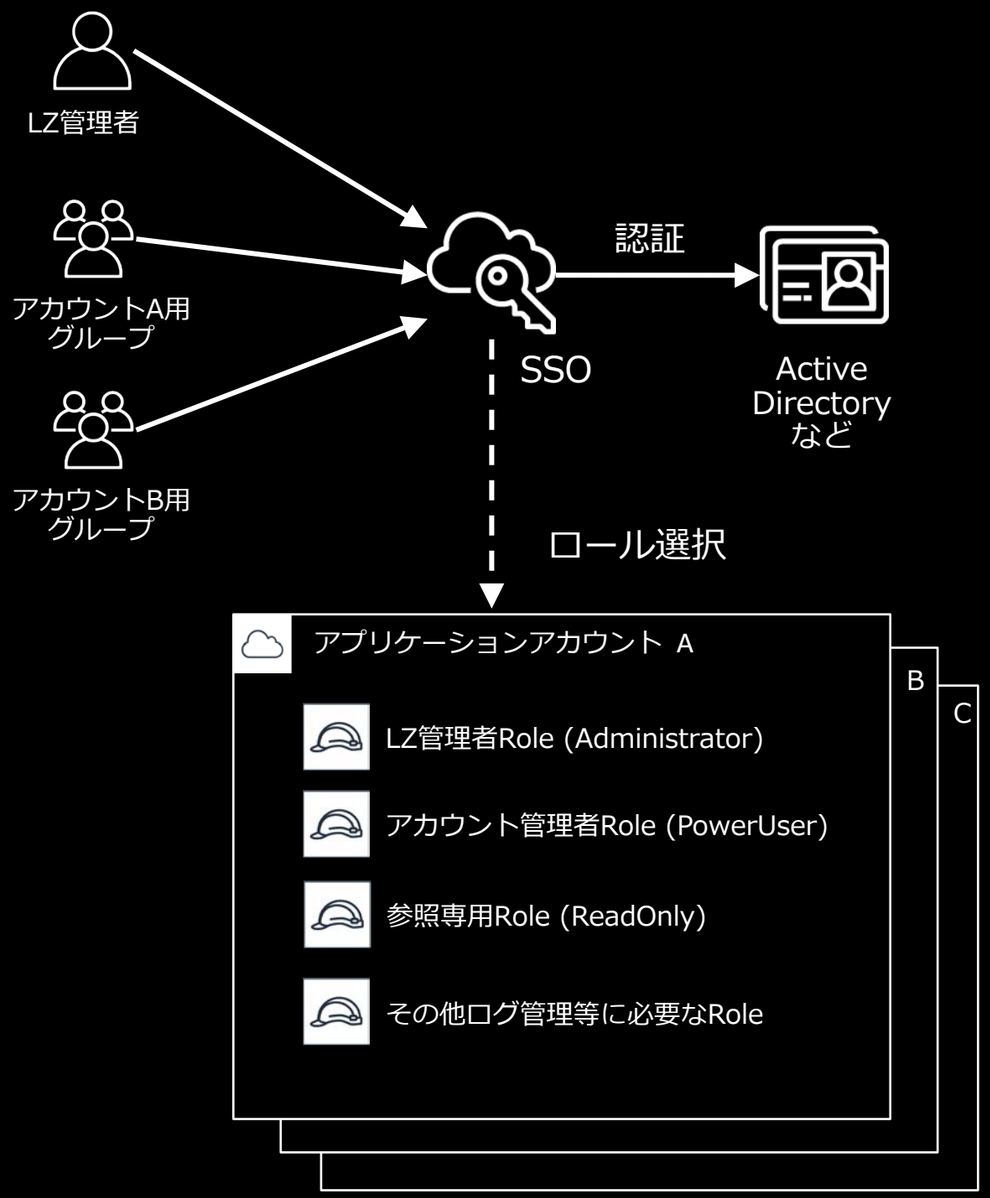
実装の一例：AWS Organizations を利用したアカウント作成の自動化
https://aws.amazon.com/jp/blogs/news/account-management-automation-using-aws-organizations/

2. 管理用権限の発行

- LandingZone管理者あるいは
各アカウントの管理者が
対象アカウントを操作するための権限

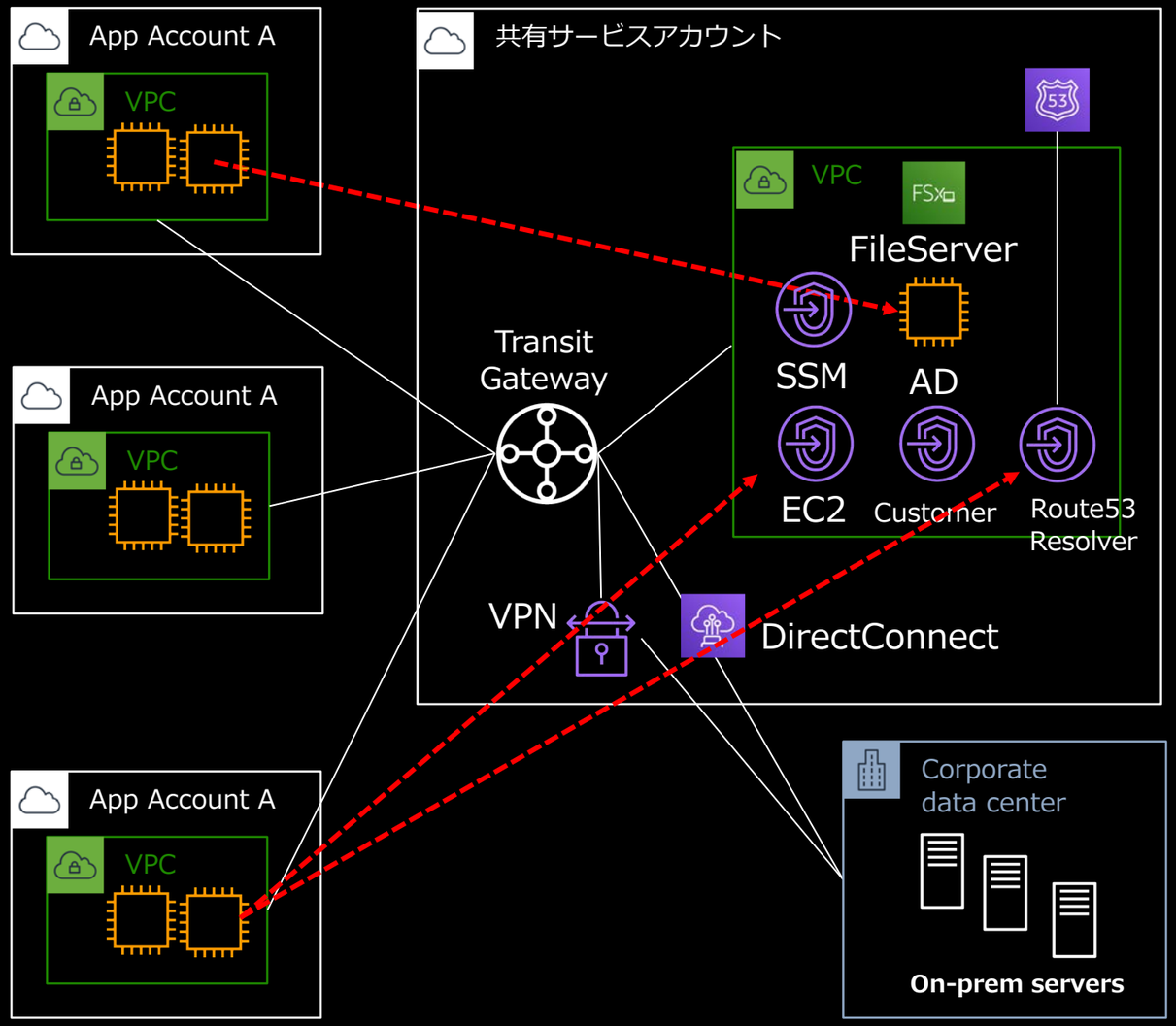
- 認証にはIAM Userではなくシングルサインオン(SSO) の仕組みを使い、各アカウントにロールのみを作成することを推奨

- ユーザの管理を各アカウントに任せる場合は アカウントごとでIAM ユーザを作る方法もある



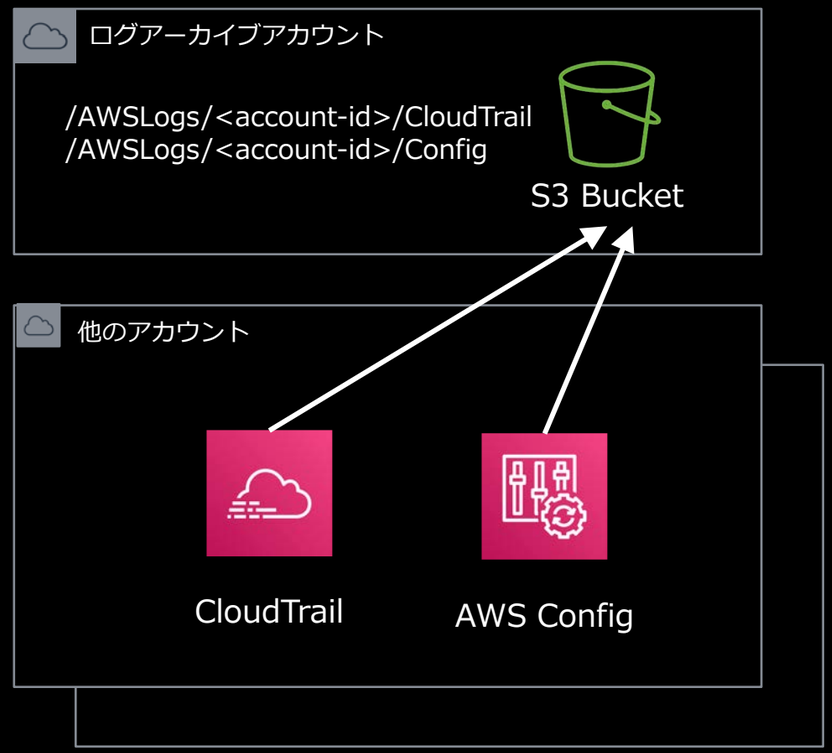
3. 共有サービスへのアクセス

- オンプレミスとの接続経路を提供
- 共有サービスを配置するVPC
- Transit Gatewayを使った マルチアカウントVPC間の通信
- Route53 Private Hosting を使った統一的な名前解決（によるPrivateLinkの共有）
- SharedVPCを使った ネットワークリソースの共有

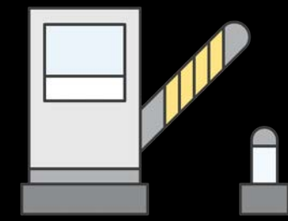


4. AWSログの集約

- CloudTrail のログとAWS Config のログをログアカウントのバケットに集約
- 保存バケットのバケットポリシーと各サービスの送信先設定だけで実現可能
- ログ集約を停止させないSCPも合わせて利用 する



参考：ControlTowerのガードレール



- 必須のガードレール
  - ControlTowerを正常に稼働させるために必要な禁止事項をSCPで定義したもの
  - 独自に実装する場合は必須ではないが、ログ保存を停止させない実装などが参考になる

- 強く推奨されるガードレール
  - マルチアカウントのベストプラクティスに基づく制限事項
  - SCPの例：rootユーザでアクセスキーを作らない、rootユーザで操作しないなど
  - ConfigRulesの例：EBSボリュームが暗号化されていること、S3のパブリック読み書き禁止など

- 選択的ガードレール
  - AWS エンタープライズ環境で一般的に利用されている制限事項
  - SCPの例：MFAなしのS3バケット削除禁止、S3バケットのクロスリージョンレプリカ禁止など
  - ConfigRulesの例：MFAなしのIAMユーザアクセス禁止、バージョニングのないS3の禁止など

5-1. 予防的ガードレール（SCP）の設定

- Organizations SCPによる設定
- 自身で SCP を書くことで
  カスタマイズが可能

[注意]
SCPの権限制御は対象アカウントやOUのすべてのユーザーに影響を与える可能性がある強力な機能です。必要最低限の設定を十分なテストを行なって適用してください。

root ユーザーとしてのアクションを禁止する

AWS アカウントを保護するには、root ユーザー認証情報 (アカウントのすべてのリソースへの無制限のアクセスを許可するアカウント所有者の認証情報) を使用したアカウントアクセスを禁止します。代わりに、AWS アカウントとの日常的なやり取り用に AWS IAM (Identity and Access Management) ユーザーを作成することをお勧めします。これは、強く推奨されるガイダンスによる予防的ガードレールです。デフォルトでは、このガードレールは有効になっていません。

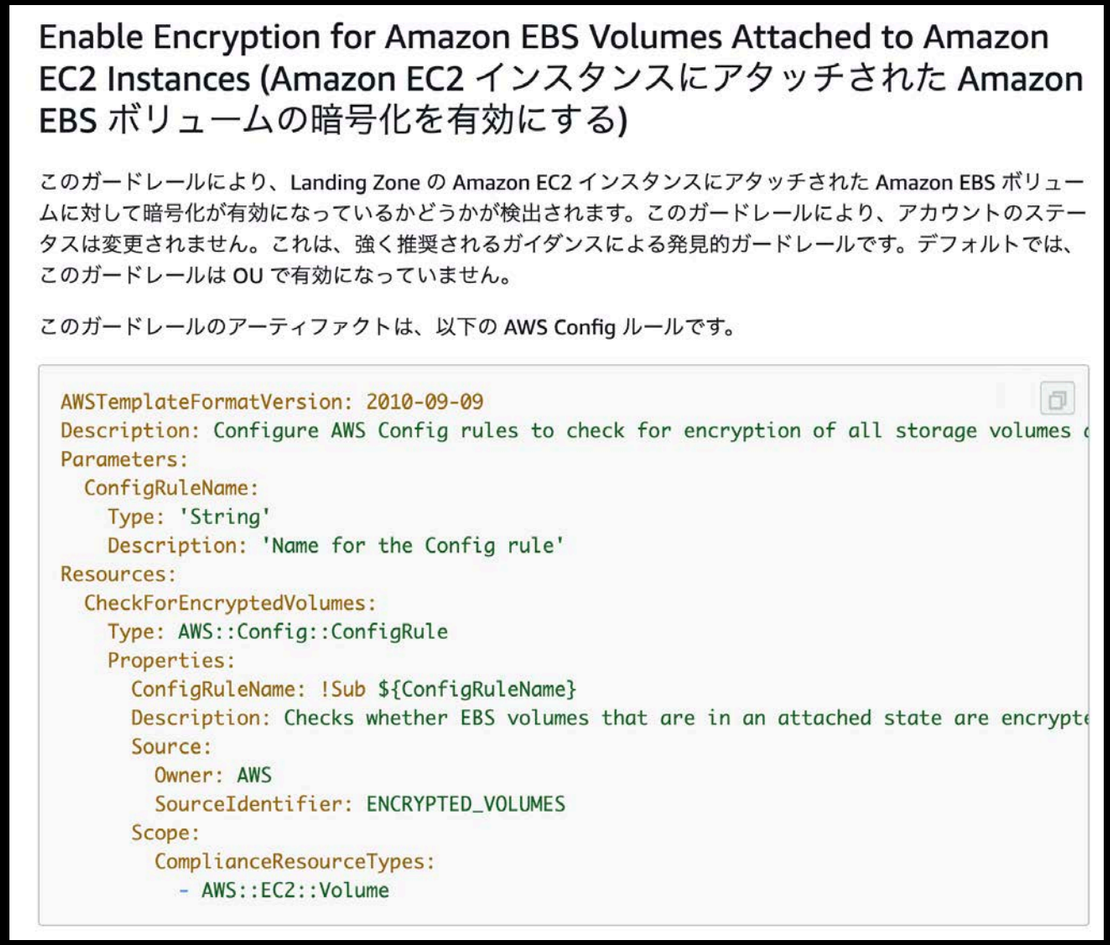
このガードレールのアーティファクトは、以下の SCP です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GRRESTRICTROOTUSER",
      "Effect": "Deny",
      "Action": "*",
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:root"
          ]
        }
      }
    }
  ]
}
```

https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/strongly-recommended-guardrails.html

5-2. 発見的ガードレール（ConfigRules）の設定

- AWS Config Rules の設定をCloudFormationで展開
- StackSetsで複数のアカウント・リージョンに一括展開
- ControlTowerで設定できる推奨項目は CloudFormationテンプレートがドキュメントに記載
- 他の マネージドルールを使用したり AWS Config RDK (Rule Developing Kit) を使ったカスタムルールの作成も可能



Enable Encryption for Amazon EBS Volumes Attached to Amazon EC2 Instances (Amazon EC2 インスタンスにアタッチされた Amazon EBS ボリュームの暗号化を有効にする)

このガードレールにより、Landing Zone の Amazon EC2 インスタンスにアタッチされた Amazon EBS ボリュームに対して暗号化が有効になっているかどうかが検出されます。このガードレールにより、アカウントのステータスは変更されません。これは、強く推奨されるガイダンスによる発見的ガードレールです。デフォルトでは、このガードレールは OU で有効になっていません。

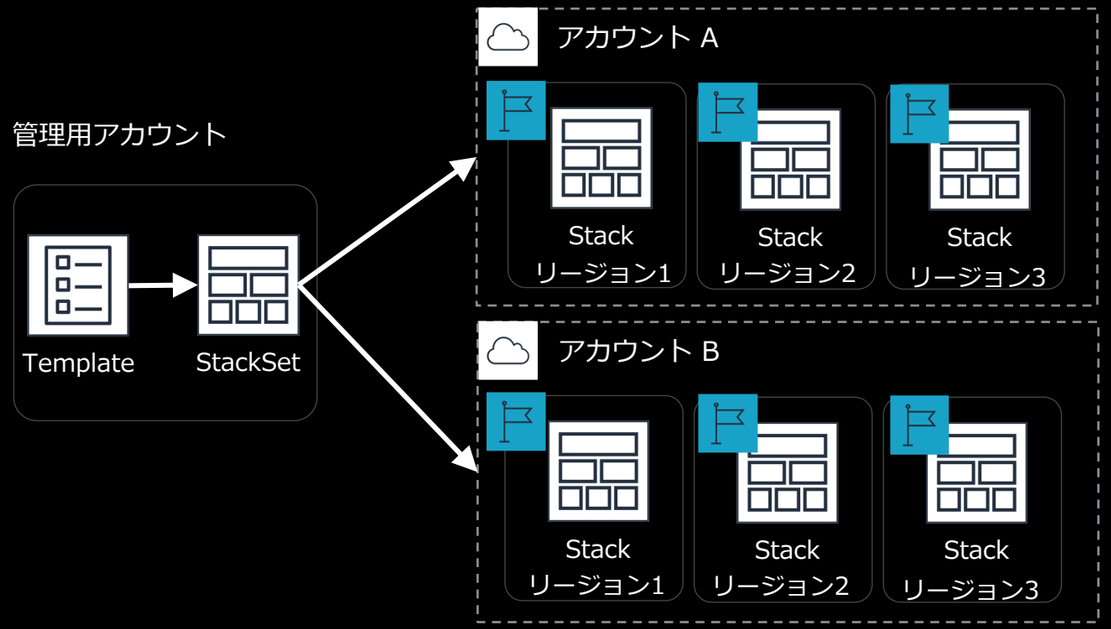
このガードレールのアーティファクトは、以下の AWS Config ルールです。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config rules to check for encryption of all storage volumes
Parameters:
  ConfigRuleName:
    Type: 'String'
    Description: 'Name for the Config rule'
Resources:
  CheckForEncryptedVolumes:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: !Sub ${ConfigRuleName}
      Description: Checks whether EBS volumes that are in an attached state are encrypte
      Source:
        Owner: AWS
        SourceIdentifier: ENCRYPTED_VOLUMES
      Scope:
        ComplianceResourceTypes:
          - AWS::EC2::Volume
```

https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/strongly-recommended-guardrails.html

参考: CloudFormation StackSets

- 1つのCloudFomationテンプレートから、
  複数アカウント、複数リージョンにStackを同時展開する機能
- 各アカウントに用意した管理者権限を有するロールでStackを作成



https://docs.aws.amazon.com/ja_jp/AWSCloudFormation/latest/UserGuide/what-is-cfnstacksets.html

まとめ

aws INNOVATE
ONLINE CONFERENCE

まとめ

- 多数のシステムをシンプルかつスケーラブルに管理するために
  マルチアカウントによる管理と仕組みの活用が効果的

- Landing Zone 実装は状況に合わせて使い分ける
  - ControlTower / 独自の実装

- マルチアカウント管理の実装例
  - アカウントの発行 / 管理用権限の発行 / 共有サービスへのアクセス /
    AWSログの集約 / ガードレールの設置
  - 設定は CloudFormation StackSets を使ってスケーラブルに展開

クイズ

aws INNOVATE
ONLINE CONFERENCE

クイズ

Q1: 特定のタグの付与を強制するにはどのような方法がありますか

Q2: 集約したログを定期的に監査するにはどのような方法がありますか

Q3: 発見的ガードレールで検知された事象を自動的に対応するには
どのような方法がありますか

Thank you!

大村 幸敬
Twitter: @yktko

aws INNOVATE
ONLINE CONFERENCE