CloudShift

Stylez

株式会社スタイルズ

2022年6月14日

AWSにおけるマルチアカウント戦略！
Control Tower活用方法
～弊社事例を交えてご紹介～

aws partner network

aws PARTNER Select Tier Services

RANCHER PARTNER NETWORK

ZABBIX CERTIFIED PARTNER

Nextcloud Gold partner

vmware PARTNER PROFESSIONAL SOLUTION PROVIDER

自己紹介

- 江藤 正晃（Masateru Eto）

- 普段やっている業務
  - アプリ開発に関わるご提案から開発・運用
  - 最近はクラウドネイティブなシステム開発の技術支援

- 好きなAWSサービス
  - AWS Lambda、Amazon API Gateway、Amazon S3

本日、お話しする内容

対象

- マルチアカウントでの運用を検討している方
- マルチテナントでのサービスを複数AWSアカウントで検討している方

ゴール

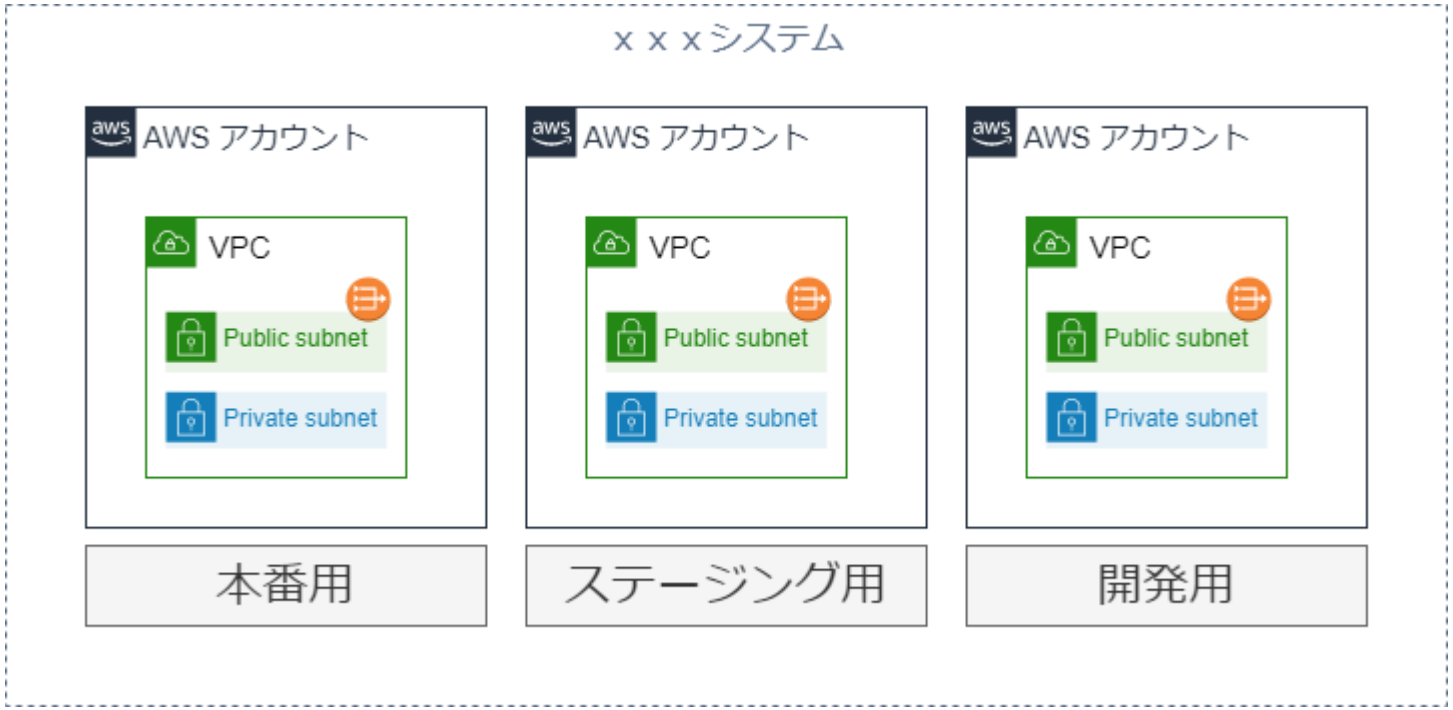
- AWS Control Towerが提供する機能を理解する
- アカウント毎の「環境管理」や「セキュリティ管理」を含めた考え方を理解する

なぜマルチアカウント戦略？

マルチアカウントの利用シーンとは？

➢ シーン１：システム稼働環境を分ける

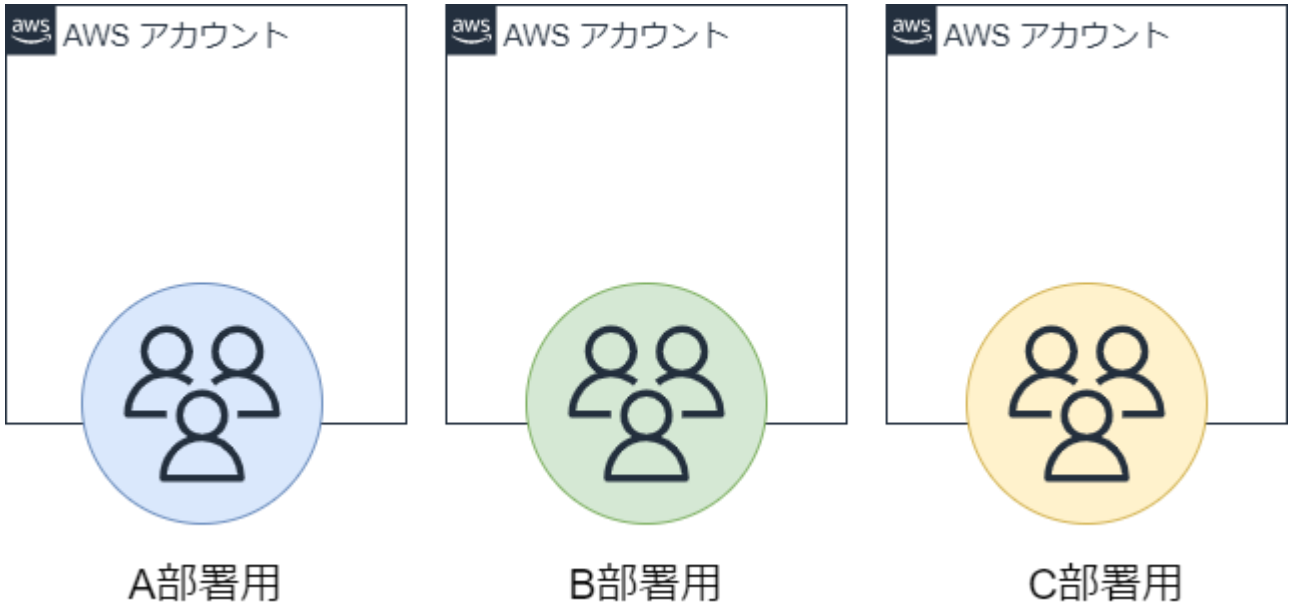
- 本番、ステージング、開発の環境単位でAWSアカウントを分けることで、環境毎に運用方法を決めて利用者や権限などを設定する場合



マルチアカウントの利用シーンとは？

➢ シーン２：部署やチームで分ける

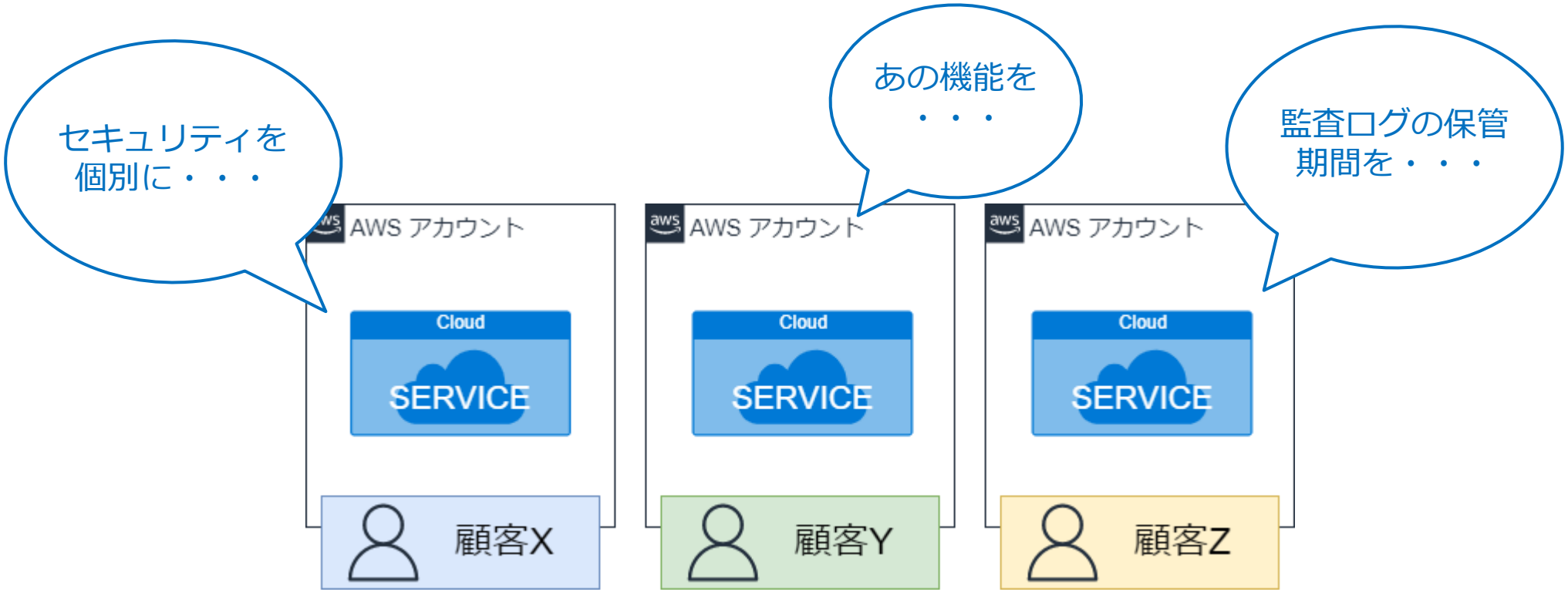
- 組織内の部門やチーム単位でAWSアカウントを分けることで、特定の部門に対する権限移譲や制限を設定する場合



マルチアカウントの利用シーンとは？

➢ シーン３：サービス提供の顧客ごとに分ける

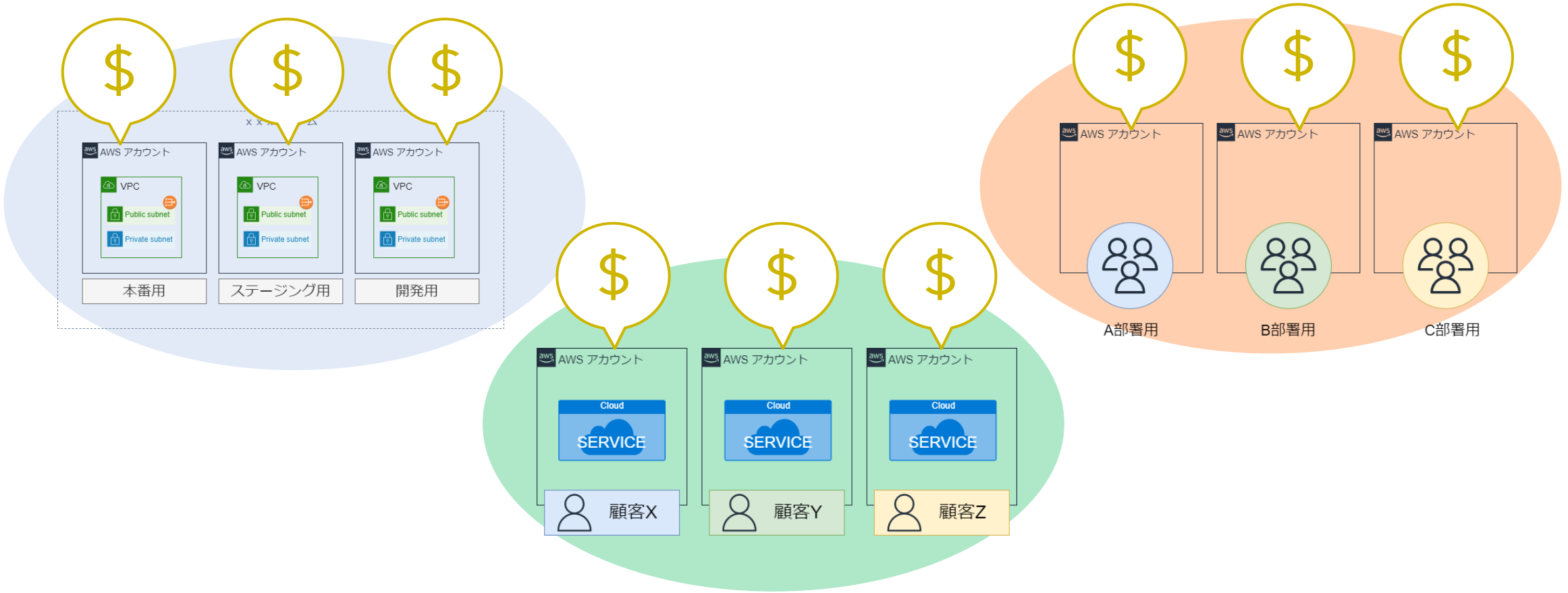
- 提供サービスを1顧客1アカウントにすることで、顧客に応じて柔軟な対応を可能したい



マルチアカウントの利用シーンとは？

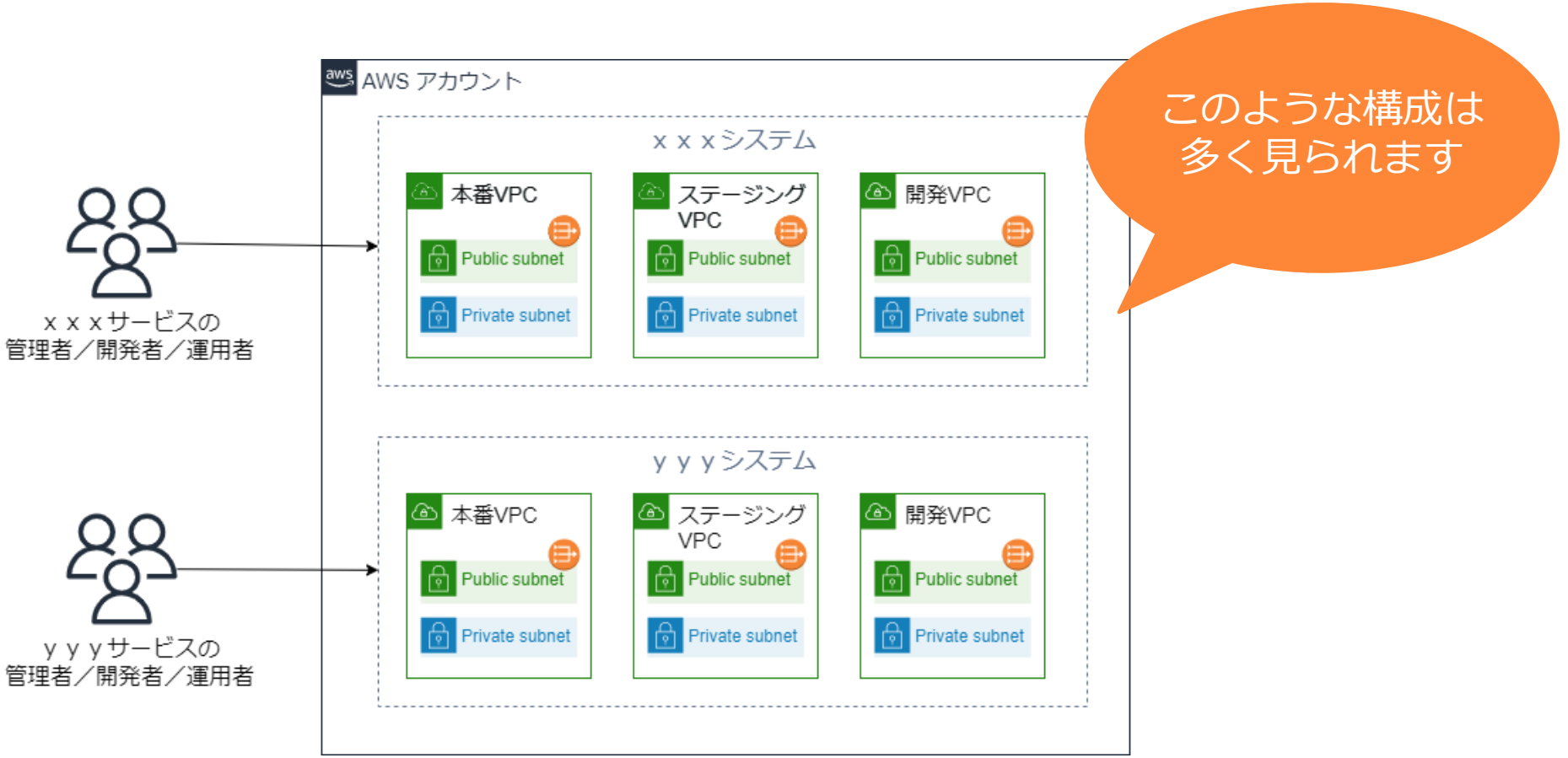
➢ シーン４：コストを明確にした

- アカウントを分けることで、どこにどれだけコストがかかっているか明確にしたい



では、マルチアカウントではない場合は？

例えば、1つのAWSアカウント内に複数のシステムがあり、それらを複数のチームで管理しているような場合に、どのような問題が発生するでしょうか？



マルチアカウントではない場合の問題は？

× 誤操作によるトラブル
- 誤って本番環境のサーバーを停止、もしくは削除するリスクがある

× 権限管理の複雑化
- 利用するユーザー数や、管理するシステムが増えることでIAM管理が困難になる

× アカウントのクォータ制限トラブル
- EC2のvCPU制限・・・開発環境でインスタンス数が増加した結果、本番環境でオートスケールに失敗
- Lambdaの同時実行数・・・ステージング環境で負荷試験した結果、本番環境で起動に失敗

× コスト把握が困難
- システムや部署ごとの利用コストが明確に分離できない

マルチアカウントのメリット・デメリット

➢ メリット

- アカウント単位で必要な権限を設定するため管理がシンプルになる
- 環境・データが分離されるため誤操作発生のリスクを抑えれる
- 顧客の個別要件に応じたセキュリティレベルの設定が調整可能
- アカウント単位のクォータ制限が管理しやすい
- 請求が分かれるためコスト管理が容易

1アカウントでの
問題が解決！

➢ デメリット

- 複数のアカウントを管理する必要がある
- セキュリティや監査ログの統制が必要になる
- アカウント間でのリソース共有など連携の手間が出てくる
- アカウント単位で上限緩和が必要

Control Towerで
管理できます！

AWS Control Towerとは

Control Towerとは？

- マルチアカウント環境を整備できるサービス

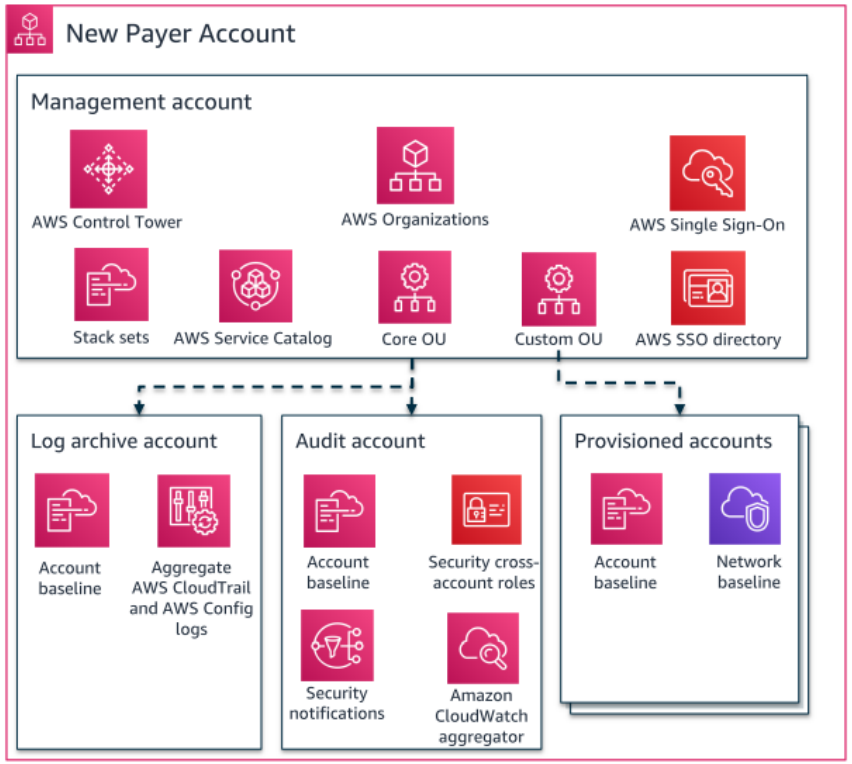
マルチアカウント管理におけるAWSのベストプラクティスに則ったマルチアカウント環境（Landing Zone）を自動で作成できます。

これにより、アカウント作成時にどの利用用途でも必要とされるセキュリティやネットワークのベースライン（基本的な設計）が簡単に適用できます。

Control Towerとは？

➢ Landing Zoneの構成

Control TowerでLanding Zoneを作成すること、このような構成が作成されます。



AWS Control Towerが構成するLanding Zone

Landing Zoneを構成するAWSサービス

- AWS Organizations
- AWS CloudTrail
- AWS Config
- AWS Single Sign-On(SSO)
- AWS Service Catalog

※主要サービスのみ記載

Control Towerの提供機能

➢ Landing Zone

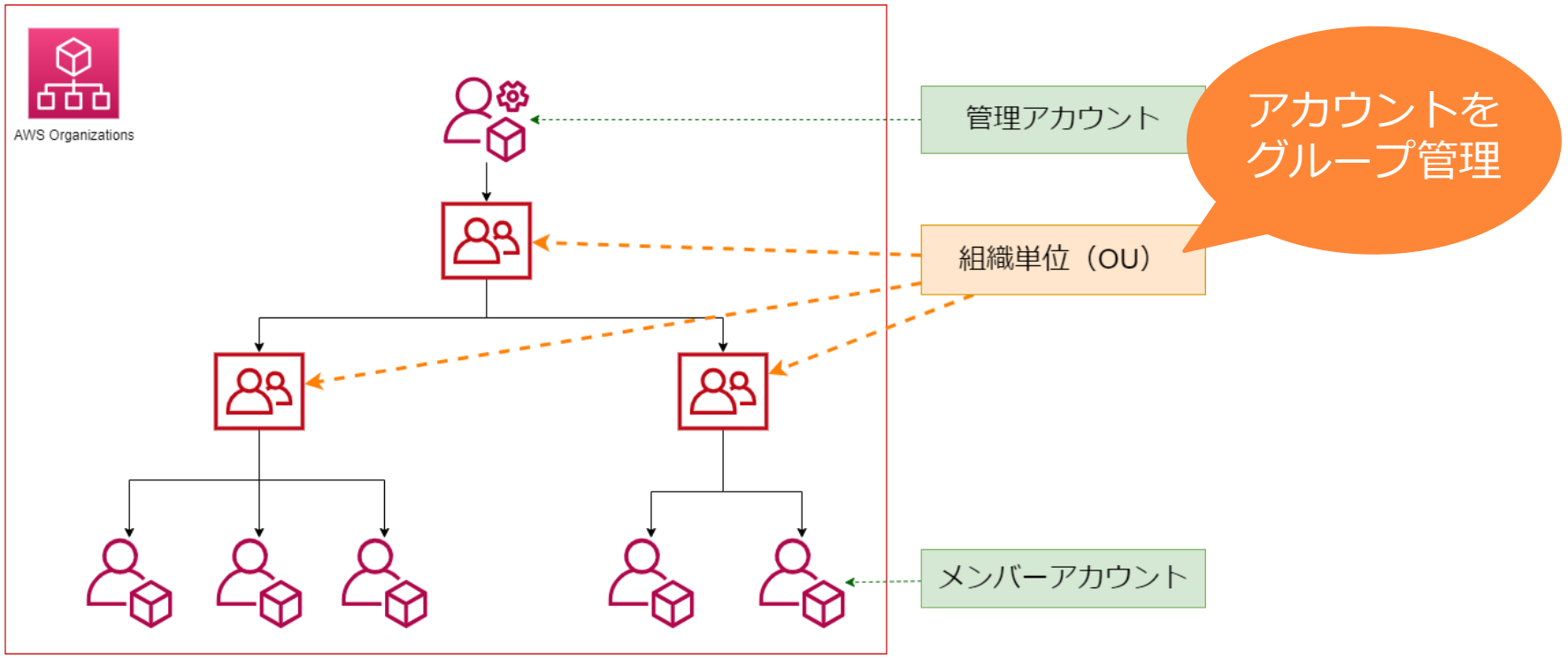
Landing Zoneは、マルチアカウント管理を実現する仕組みとしての総称

- 提供機能
  - 組織単位　・・・　アカウントのグループ管理
  - Account Factory　・・・　アカウント作成・ベースライン構築
  - ガードレール　・・・　リスクある操作の予防・検出
  - セキュリティログ　・・・　ログの一元管理・保護
  - ダッシュボード　・・・　管理状況の視覚化

Control Towerの提供機能

➢ 組織単位

- アカウントをOU（Organization Unit）という論理グループで管理
- 組織やシステムなどで自由にグループおよび階層を作成可能（最大5階層）



Control Towerの提供機能

➢ 組織単位（続き）

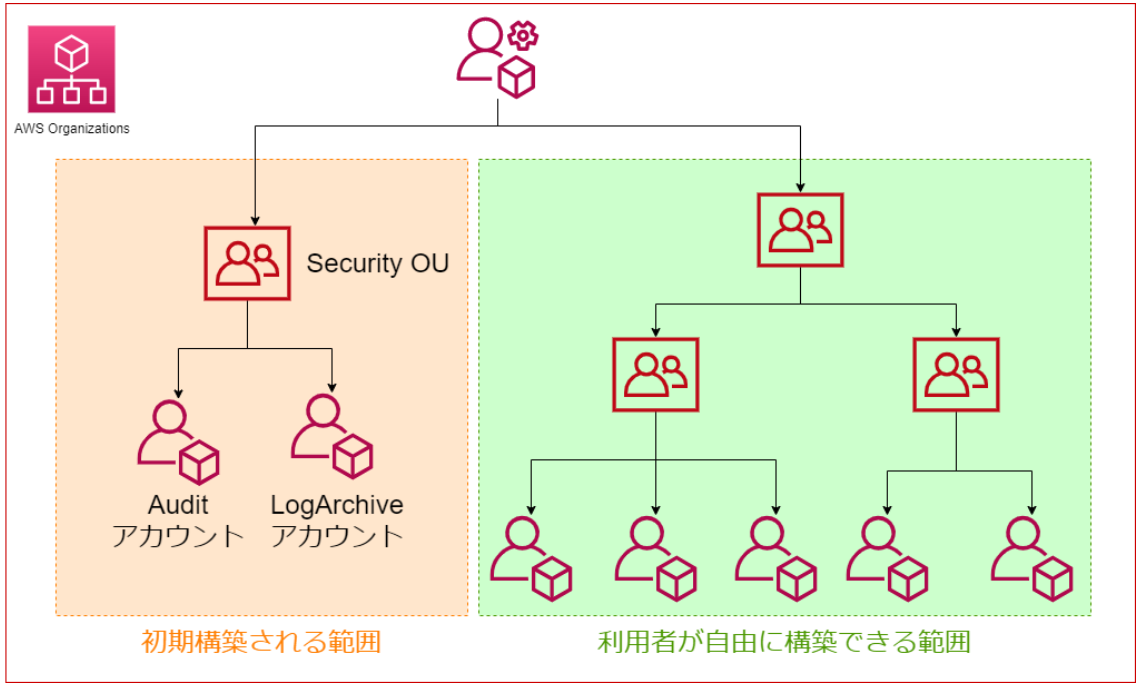
- Landing Zoneの構築時に「Security OU」と「2種類の管理用アカウント」が作成

Audit アカウント

セキュリティチームとコンプライアンスチームに対してランディングゾーンのすべてのアカウントへの読み書きアクセスを許可するように設計された制限付きのアカウント

Log Archive アカウント

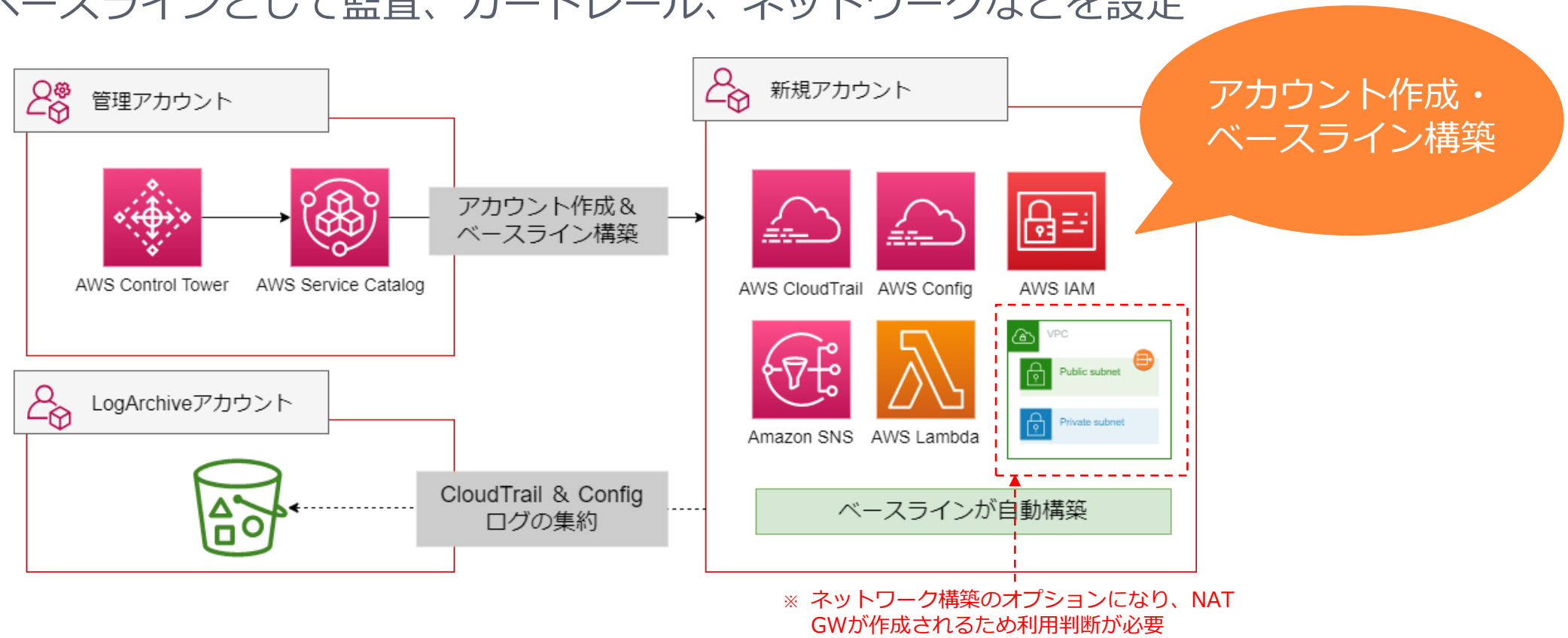
管理対象の全アカウントからAPIアクティビティのログ（CloudTrail）と、AWSリソースの変更に関するログ（Configのログ）を保管するためのアカウント



Control Towerの提供機能

➢ Account Factory

- 新規にAWSアカウントの発行および初期ベースラインを構築
- ベースラインとして監査、ガードレール、ネットワークなどを設定



Control Towerの提供機能

➢ ガードレール

ガードレールは、AWSが提唱する「ブレーキをかけるのではなく、どんなにスピードを出しても安全なセキュリティ」を確保する考え方になります。

セキュリティの考え方

- 従来は、「危険なものをブロックし、ルールを徹底し、リスクの高い行為を禁じるもの」であり、関所を設置して車を止めてから確認するような考え方であった
- これを、車がどんなにスピードを出しても路肩にそれることなく安心して運転できる「ガードレール」のような存在という考えに変える
- これにより、開発者も自由でいて、セキュアにスピード感を維持したサービス開発が可能になる

Control Towerの提供機能

➢ ガードレール（続き）

ガードレールを実現するためには、以下の2種類の動作があります。

予防

- 運用上、実施してはいけない操作を禁止
- AWS Organizations の Service Control Policy （SCP）により実現

検出

- 運用上で発生する可能性のある操作は、一律禁止するのではなく検出・通知して、問題が無いか確認するための仕組み
- AWS Config Rulesにより実現

Control Towerの提供機能

➢ ガードレール（続き）

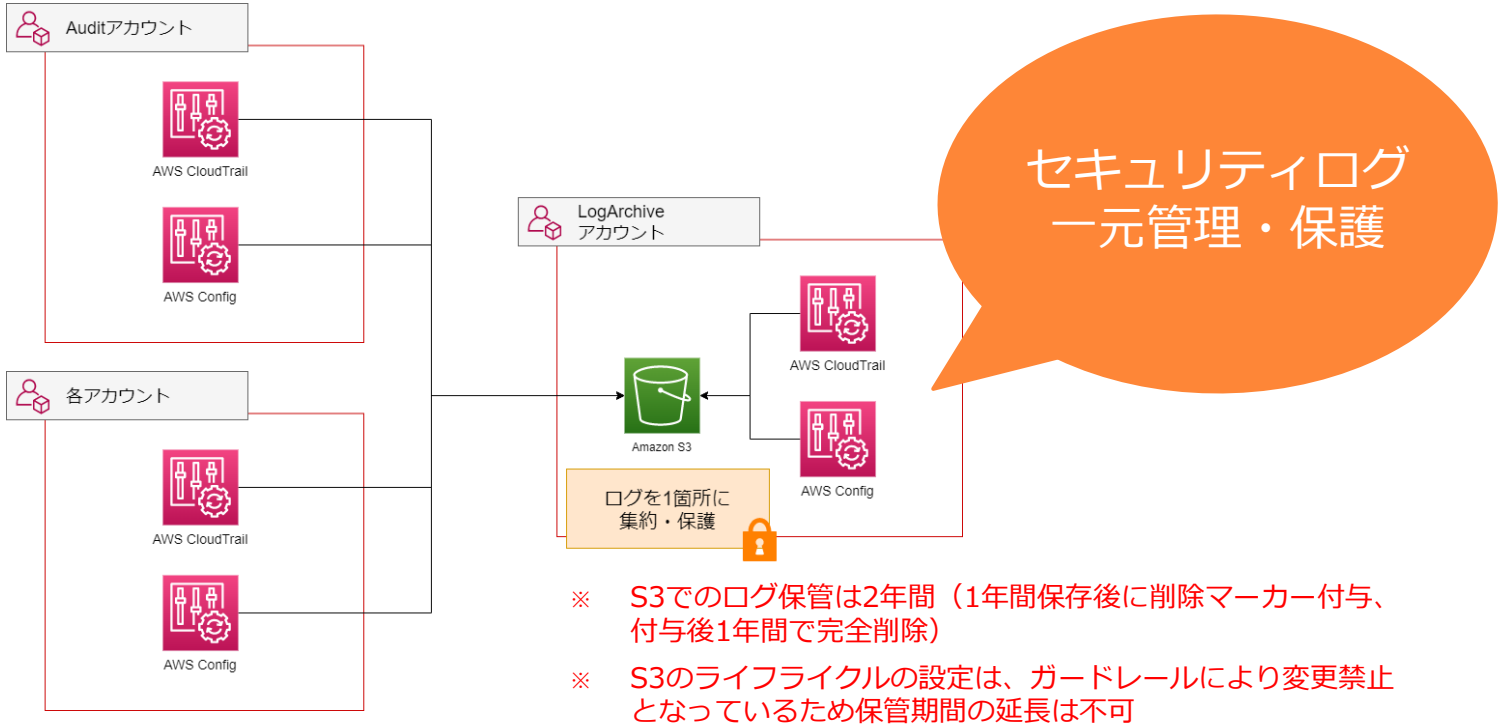
この画面イメージは、マネジメントコンソールで見れるガードレールの一部になります。

名前	ガイダンス	カテゴリ	動作
ログアーカイブの削除を許可しない	必須	監査ログ	予防
Amazon S3 バケットの暗号化設定の変更を許可しない	選択的	監査ログ	予防
Amazon S3 バケットのログ記録設定の変更を許可しない	選択的	監査ログ	予防
Amazon S3 バケットのバケットポリシーの変更を許可しない	選択的	モニタリング	予防
ログアーカイブのパブリック読み取りアクセス設定を検出する	必須	監査ログ	検出
ログアーカイブのパブリック書き込みアクセス設定を検出する	必須	監査ログ	検出
Amazon S3 バケットのライフサイクル設定の変更を許可しない	選択的	監査ログ	予防
Amazon EC2 Auto Scaling のパブリック IP アドレスが起動設定を通じて有効になっているかどうかを検出する	選択的	Data Residency	検出
CloudTrail への設定変更を不許可にします	必須	監査ログ	予防
CloudTrail イベントと CloudWatch logs を統合する	必須	モニタリング	予防
利用可能なすべてのリージョンで CloudTrail を有効にする	必須	監査ログ	予防
CloudTrail ログファイルの整合性検証を有効にする	必須	監査ログ	予防
AWS Control Tower によって設定された Amazon CloudWatch の変更を許可しない	必須	Control Tower のセットアップ	予防
AWS Control Tower によって作成された AWS Config アグリゲーション認可の削除を許可しない	必須	Control Tower のセットアップ	予防
AWS Control Tower で AWS Config リソースに付けたタグの変更を許可しない	必須	Control Tower のセットアップ	予防

Control Towerの提供機能

➢ セキュリティログ

- AWS CloudTrailとAWS Configのログは、Log Archiveアカウントで一元管理
- 予防の必須ガードレールによりログは強力に保護
  - S3バケットの暗号化設定、ライフサイクル設定、ログ記録設定、バケットポリシーの変更禁止



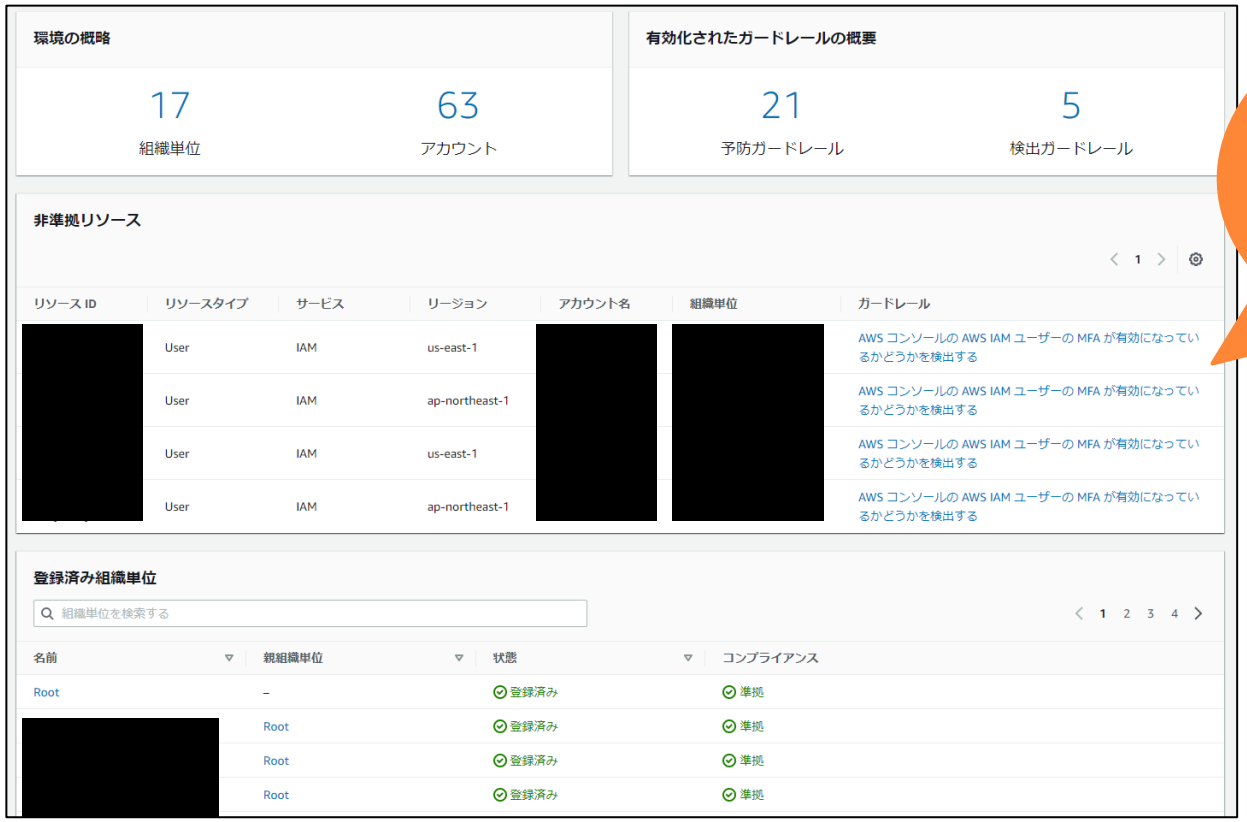
※ S3でのログ保管は2年間（1年間保存後に削除マーカー付与、付与後1年間で完全削除）

※ S3のライフライクルの設定は、ガードレールにより変更禁止となっているため保管期間の延長は不可

Control Towerの提供機能

➢ ダッシュボード

Landing Zoneで管理している情報（組織・アカウント、ガードレール、非準拠など）を確認できます。



管理状況の
可視化を実現

AWSにおけるマルチアカウント戦略（弊社事例）

はじめに

➢ Control Tower導入における考え方

Control Towerで構築するLanding Zoneは、どのような利用であってもアカウント運用に必須とされる内容をベースラインとして構築します。

上記に加えて、組織やサービスなどの個別要件に合わせて、利用者独自のベースラインを構築する必要があります。

2階層目 ・・・ 個別要件に応じて利用者が構築

1階層目 ・・・ Control Towerで構築

弊社事例でのベースラインの構築概要

➢ セキュリティ周りの追加　～　その１

AWSが提供するセキュリティ関連のサービスのうち以下のようなサービスをベースラインとして構築しました。

- AWS Security Hub
- Amazon Guard Duty

AWS Organizationsで全アカウントに自動適用
※Auditアカウントに権限移譲して管理

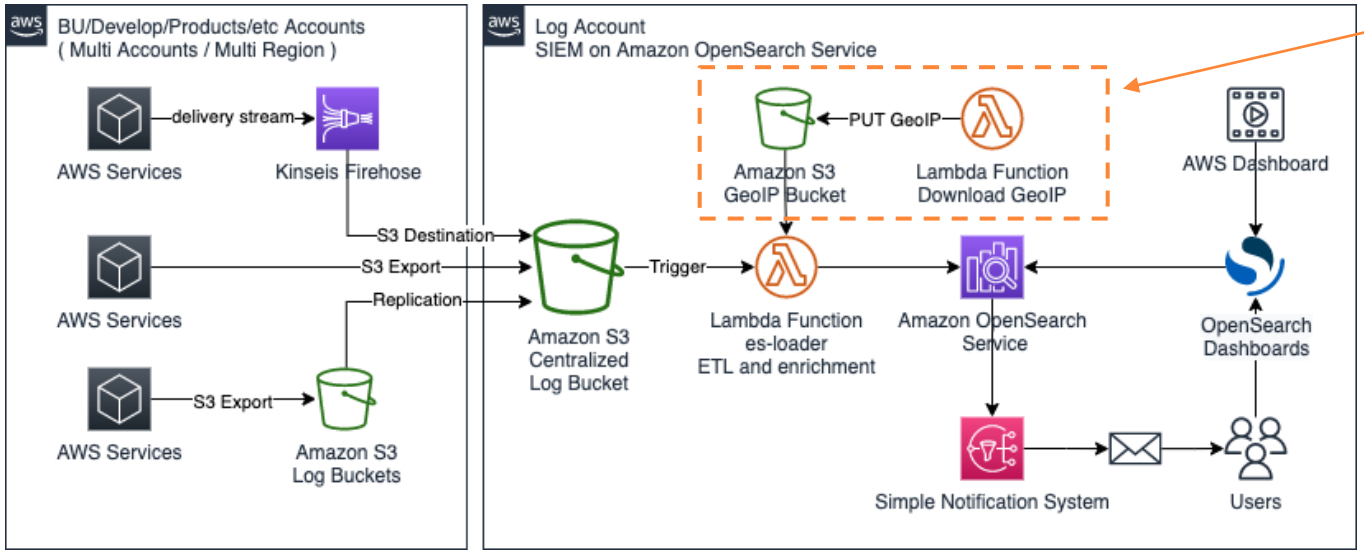
- Amazon Detective

アカウント作成時から48時間経過後に自動適用
※Step Functionsを活用してLambdaで実行

弊社事例でのベースラインの構築概要

➢ セキュリティ周りでの追加　～　その２

セキュリティログの可視化・インシデント調査のため、「SIEM on Amazon OpenSearch Service」を構築



IPアドレスに国情報や緯度・経度のロケーション情報を付与
※MaxMind社のGeoLite2 Freeを利用

SIEM on Amazon OpenSearch Serviceのアーキテクチャ（参考サイトより引用）

参考サイト
https://github.com/aws-samples/siem-on-amazon-opensearch-service/blob/main/README_ja.md

弊社事例でのベースラインの構築内容

➢ セキュリティ周りでの追加　～　その２（補足）

セキュリティログ
可視化！

付与した
ロケーション情報
可視化！

ログ可視化のイメージ（参考サイトより引用）

参考サイト
https://github.com/aws-samples/siem-on-amazon-opensearch-service/blob/main/README_ja.md

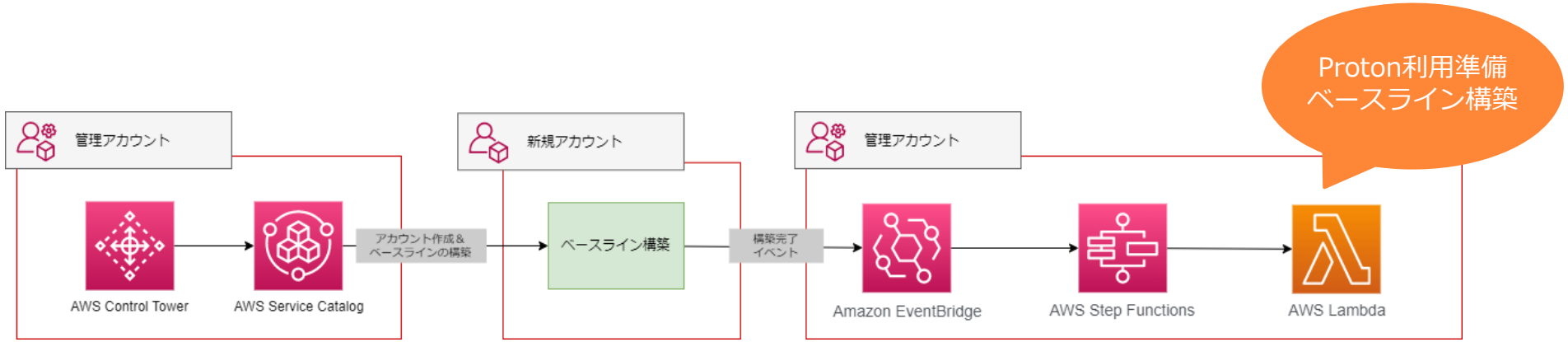
弊社事例でのベースラインの構築内容

➢ サービス個別要件への対応

弊社の事例では、1顧客1アカウントでのサービス提供を行うため、どの顧客でも必要となるような設定をCloudFormationで構築しました。

CloudFormation構築する際、「テンプレートのバージョン管理」や「適用しているテンプレートの状況」を管理するため、AWS Protonを採用しました。

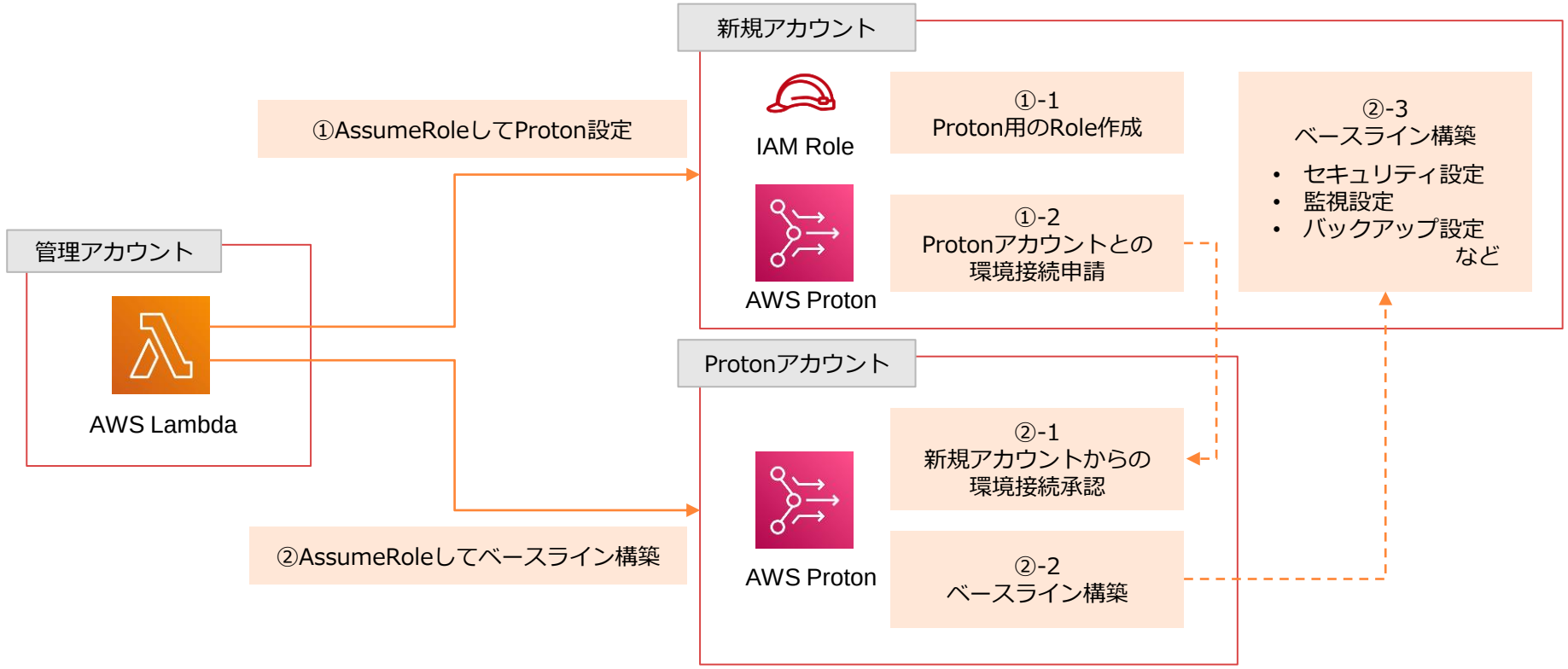
Account FactoryによるアカウントAWS Protonを利用準備とベースライン構築を実施しました。



弊社事例でのベースラインの構築内容

➢ AWS Protonでベースライン構築概要

- AWS Protonの管理用アカウントを事前準備（CloudFormationのテンプレート管理）
- 新規アカウントの作成完了後にProtonの設定を行い自動でベースライン構築



AWSにおける技術支援について

スタイルズにご相談ください

➢ AWSに特化した技術支援サービスを提供

- **AWSに関するよろず相談窓口**
  - 構成の相談、設計構築
  - AWSサービスに対するQA、ノウハウ提供
  - 不明点・懸念点に対する調査・検証（PoC）
- **AWS以外の範囲も含め、可能な範囲で対応可能**
  - アプリ改修、新規開発
  - CI/CD
  - セキュリティ
  - 監視運用保守
- **サービス料金は調整可能**
  - 想定稼働時間に基づいた料金設定（1人日/月～数人月/月　で実績あり）
- **アプリ開発者/インフラ構築者の混成チームで対応**
  - アプリ観点、インフラ観点 両面で的確な意見が出せる

AWSに関するご相談は、
ぜひスタイルズまでお声がけください！

お問合せはHPよりお願いします。
https://www.stylez.co.jp/contacts/

実績豊富なエンジニア集団の技術と開発ツールで「開発期間/コスト削減」「品質向上」を実現

株式会社スタイルズ

https://www.stylez.co.jp

東京都千代田区神田小川町1-2　風雲堂ビル6階

Tel:03-5244-4111

オープンソースソフトウェア推進