AWS Black Belt Online Seminar

AWS Control Tower

基礎編

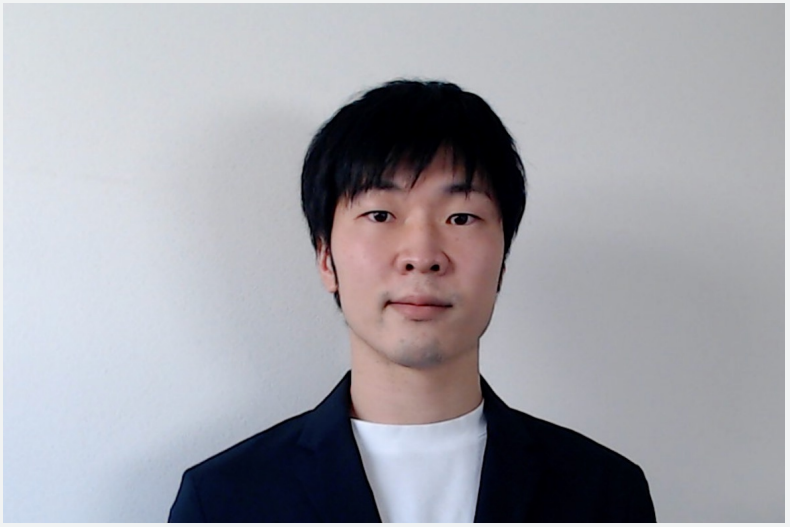
桂井 俊朗

Solutions Architect
2023/08

自己紹介

名前：

桂井俊朗 (かつらい としお)



所属：

アマゾンウェブサービスジャパン合同会社
技術統括本部 ISV/SaaS ソリューション本部
ソリューションアーキテクト

好きなAWSサービス：

AWS Control Tower

本セミナーの対象者

マルチアカウント管理について興味のある方

AWS Control Tower に関心のある方

AWS Control Tower をご利用予定の方

アジェンダ

1. マルチアカウント構成
2. AWS Control Tower とは
3. AWS Control Tower 主要機能
4. まとめ

マルチアカウント構成

ビジネスが求めている環境

Secure & compliant

組織のセキュリティや監査要件に適合する

Scalable & resilient

高可用性でスケーラブルなワークロードに対応できる

Adaptable & flexible

ビジネス要件の変更に対応するよう設定変更が可能

複数の AWS アカウントを利用することの効果

セキュリティ境界

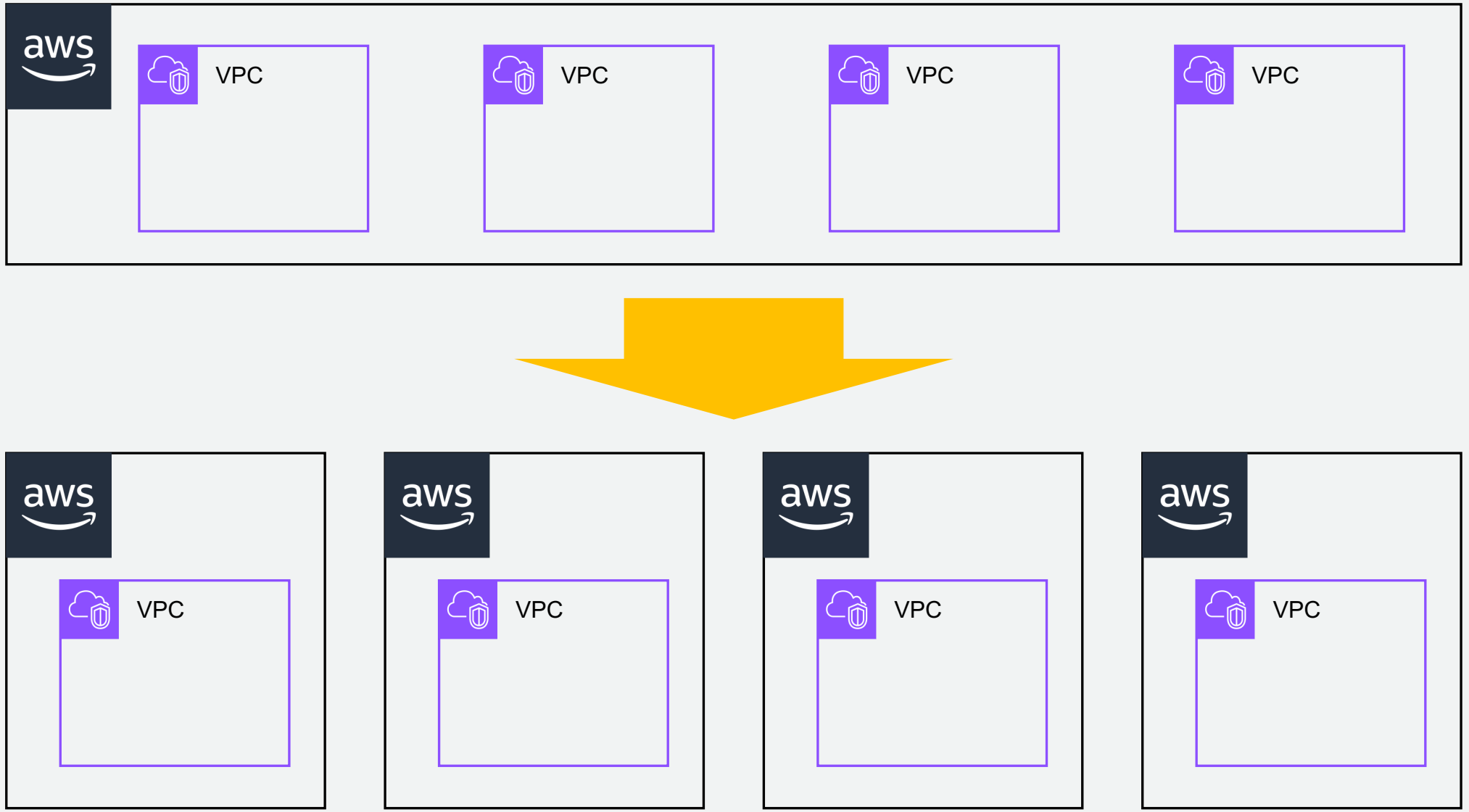
リソースの分離

請求の分離

単一の AWS アカウントだけで全てを構成した場合

- 「グレーな」境界
- 時間経過に伴って複雑で管理が面倒
- リソースのトラッキングが困難
- 責任の範囲が不明確

だから、マルチアカウント構成

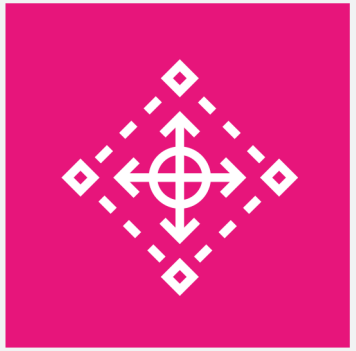


マルチアカウント構成に対するよくある疑問

AWS Control Tower とは

AWS Control Tower

マルチアカウント環境のセットアップを自動化する マネージドサービス



AWS Control Tower

マネージド
サービス

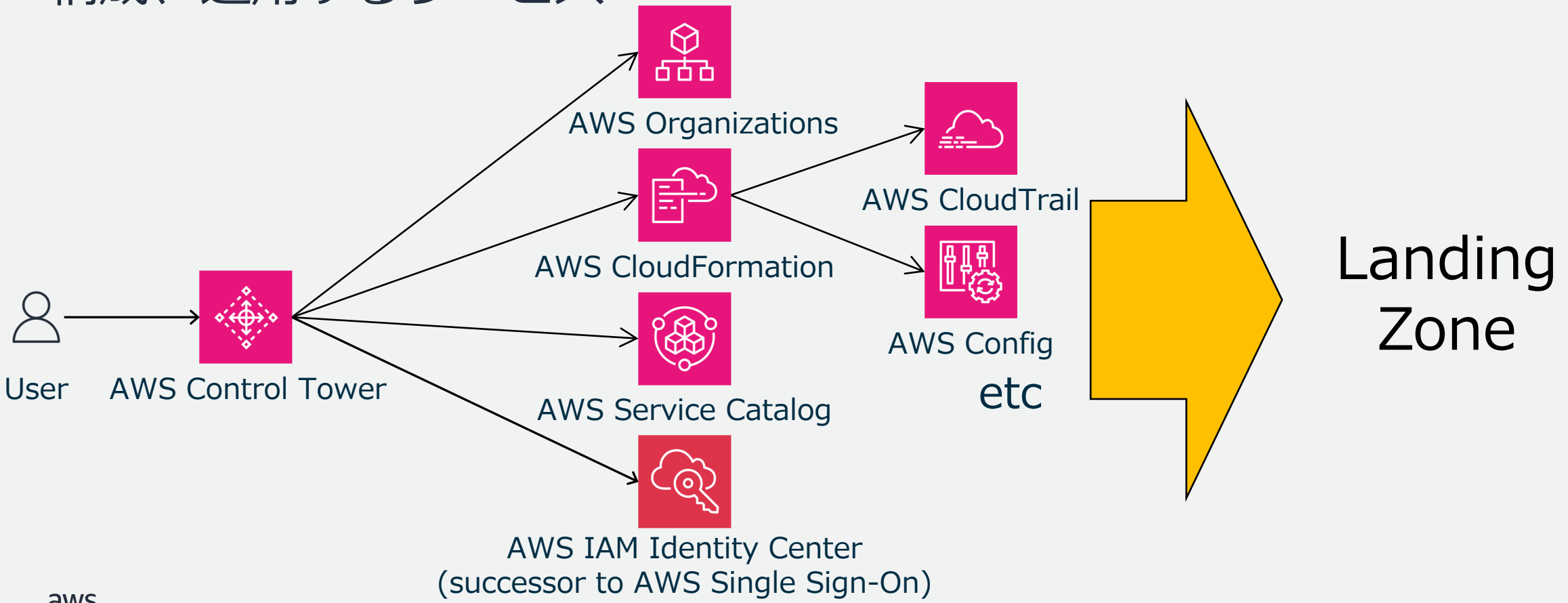
ベストプラクティス
に基づく環境

追加料金なし

注意) AWS Control Tower を通じてセットアップするように設定されたサービスは費用が発生する可能性があります

AWS Control Tower = コンフィグジェネレータ

AWS セキュリティサービス群にベストプラクティスに則った設定を投入し、統制を利かせたマルチアカウント環境 (Landing Zone) を構成、運用するサービス

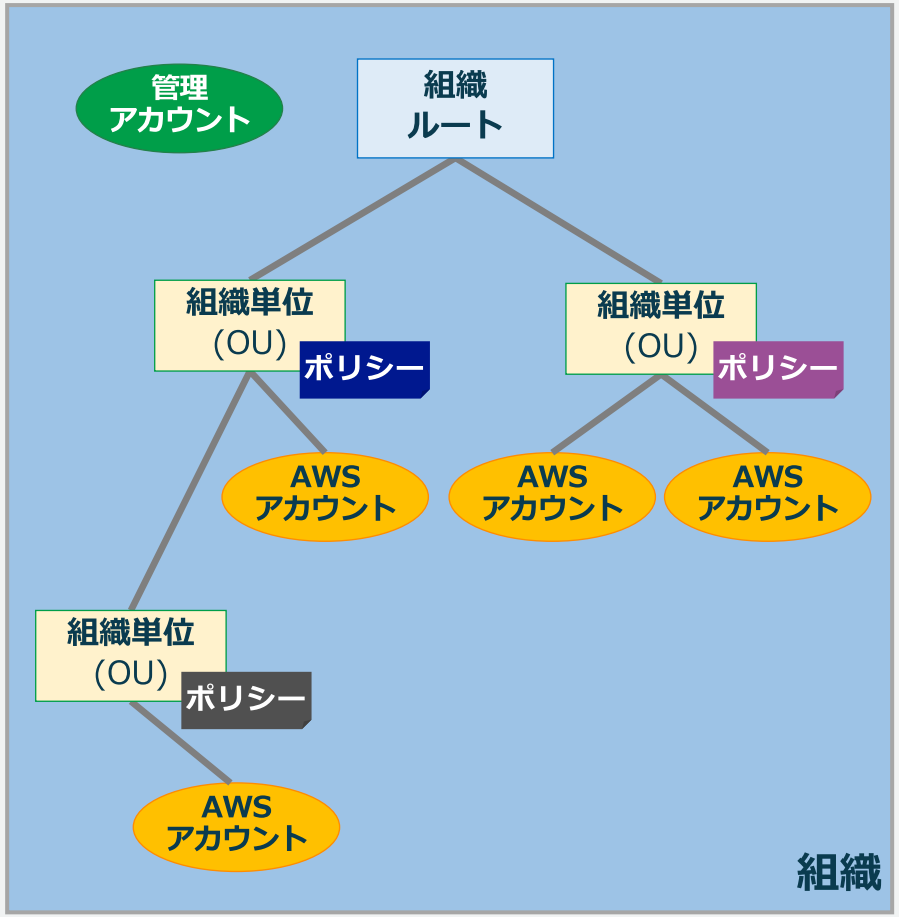


AWS Organizations 概要

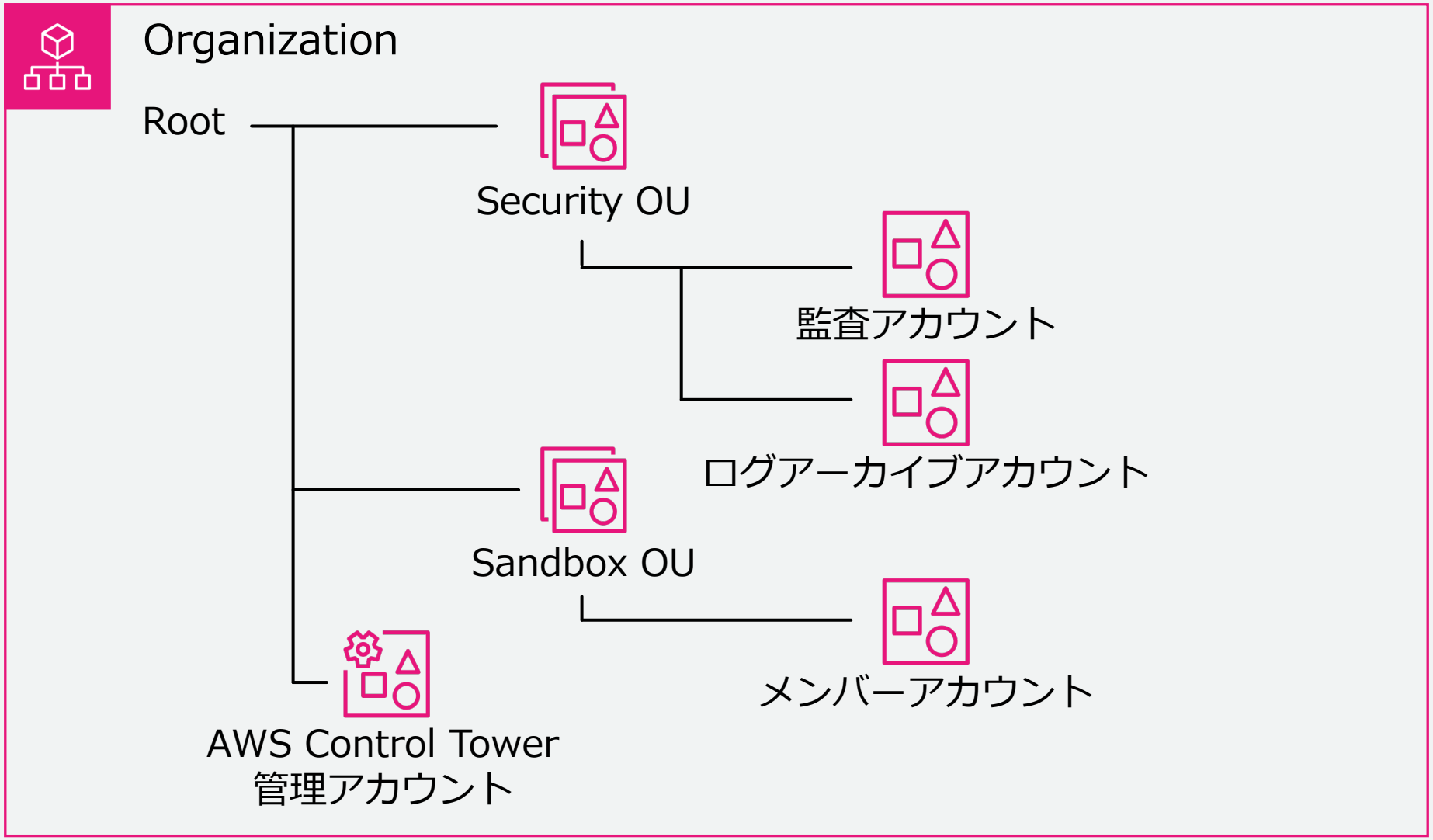
AWS Control Tower も利用する AWS アカウントの一元管理を実現するサービス

用語	説明
組織	•一元管理可能な AWS アカウントの集まり •最低 1 つの管理アカウントから構成される
管理アカウント	アカウントの作成、招待、削除、ポリシーの適用および組織における支払いアカウント
AWS アカウント	AWS Organizations で管理する最小単位
組織単位 (OU)	組織内の AWS アカウントのグループ
組織ルート	組織単位 (OU) の階層全体の開始点
サービスコントロールポリシー (SCP)	アカウントに適用するコントロールを定義したドキュメントで AWS サービスの API へのアクセスを制御 (許可・拒否) する

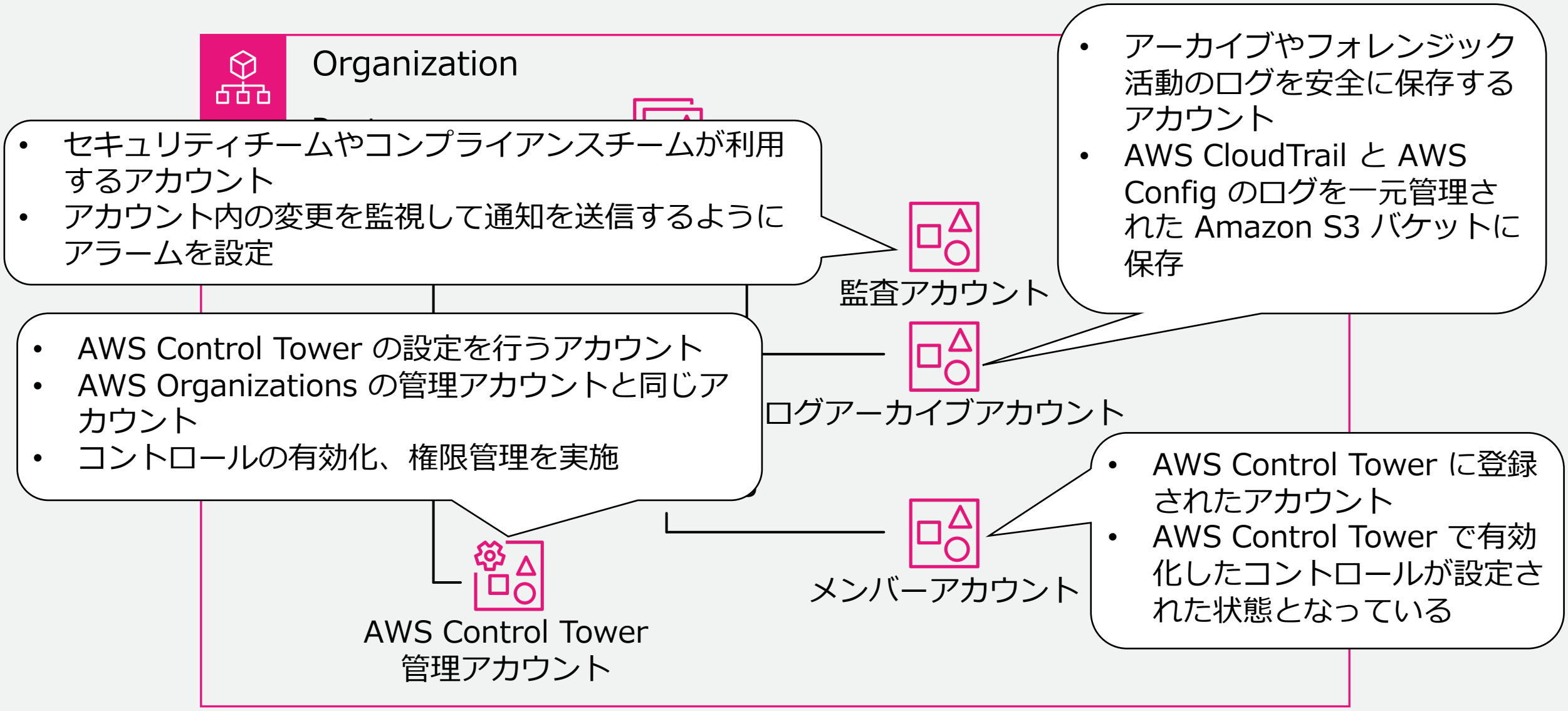
AWS Organizations 概念図



AWS Control Tower のアカウント区分

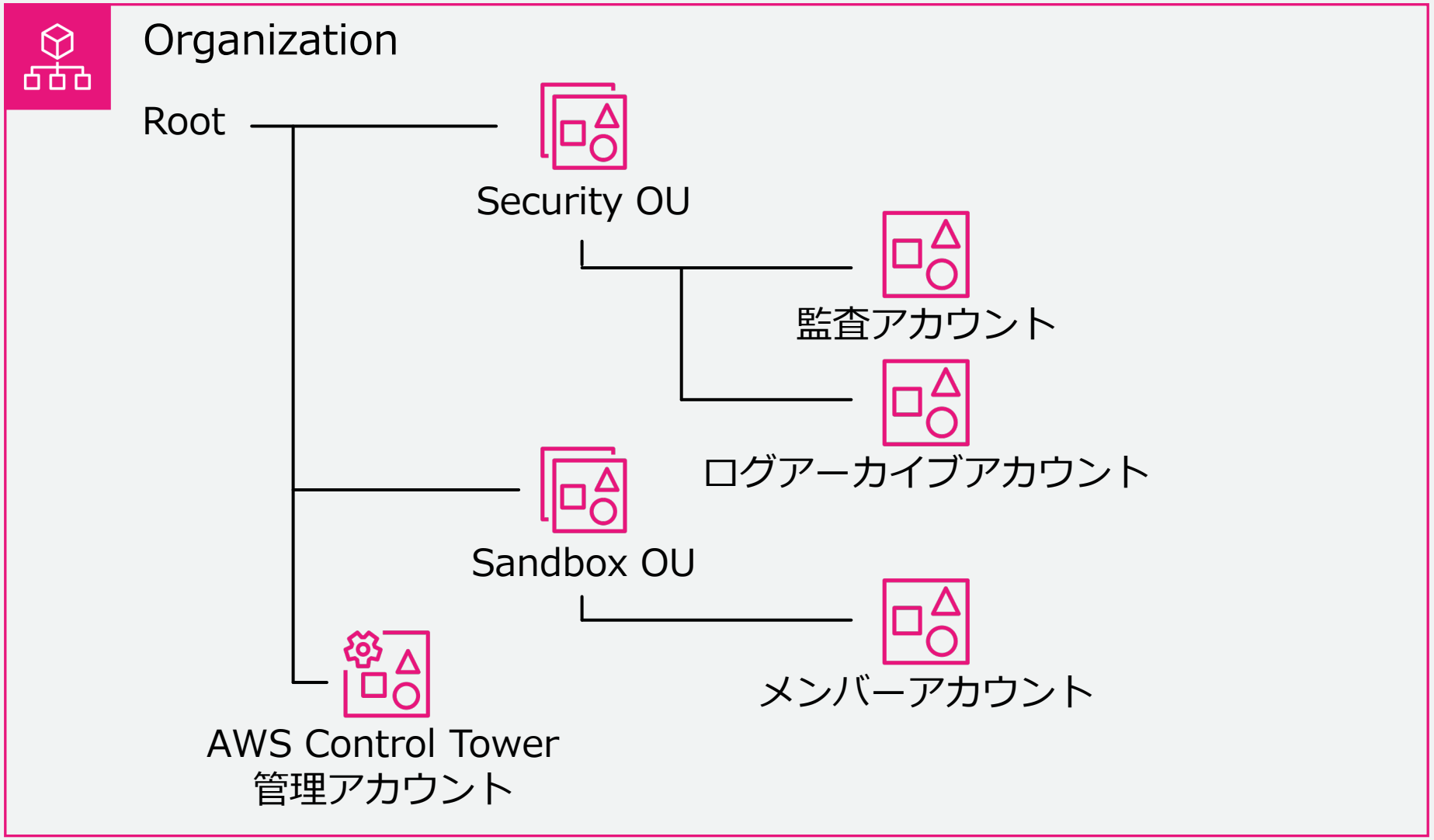


AWS Control Tower のアカウント区分

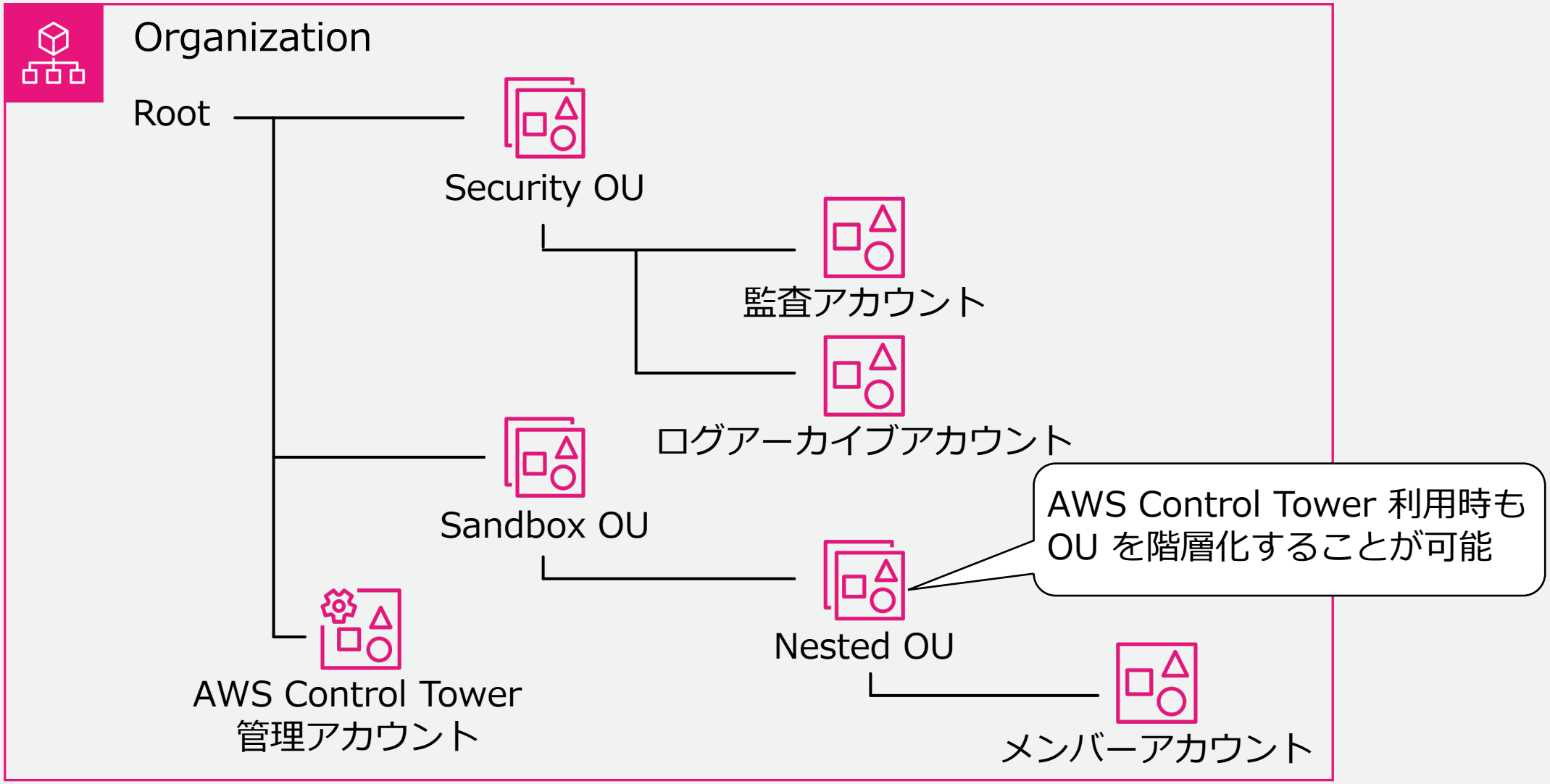


再掲

AWS Control Tower のアカウント区分



AWS Control Tower の OU の階層化



AWS Control Tower 主要機能

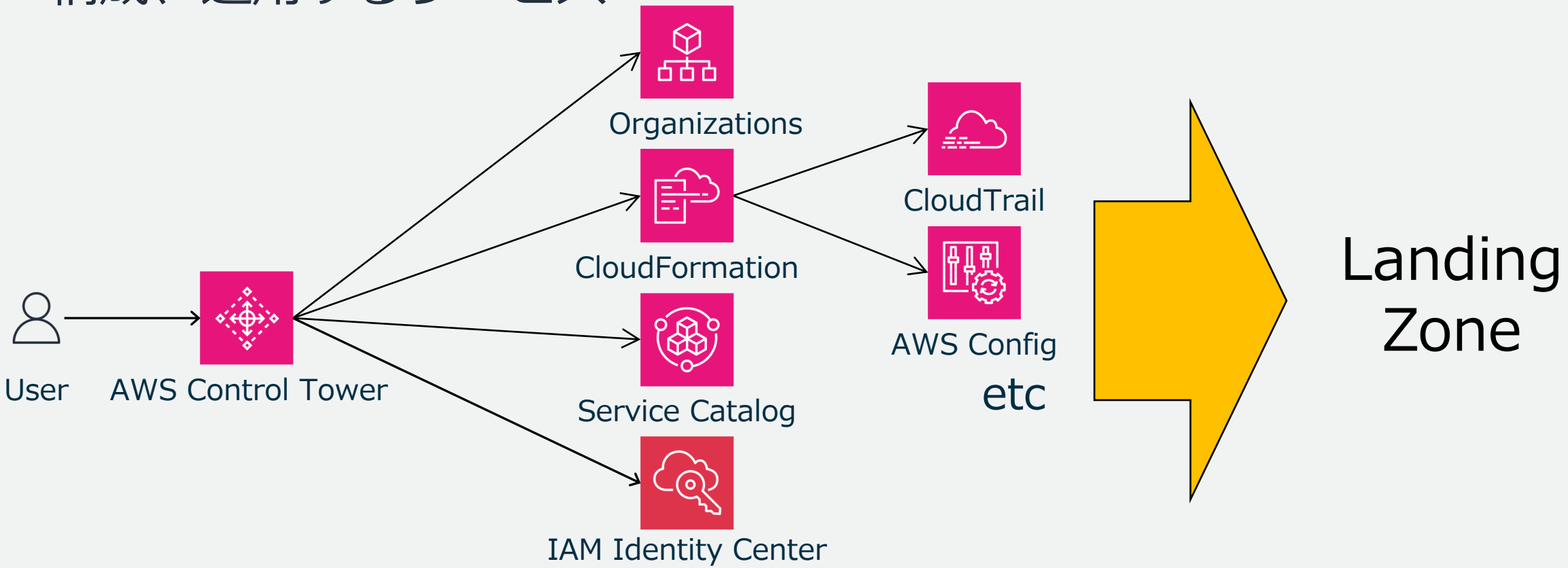
AWS Control Tower 主要機能

1. ログ集約
2. コントロール適用
3. 通知
4. ID 一元管理
5. AWS アカウント作成とプロビジョニング

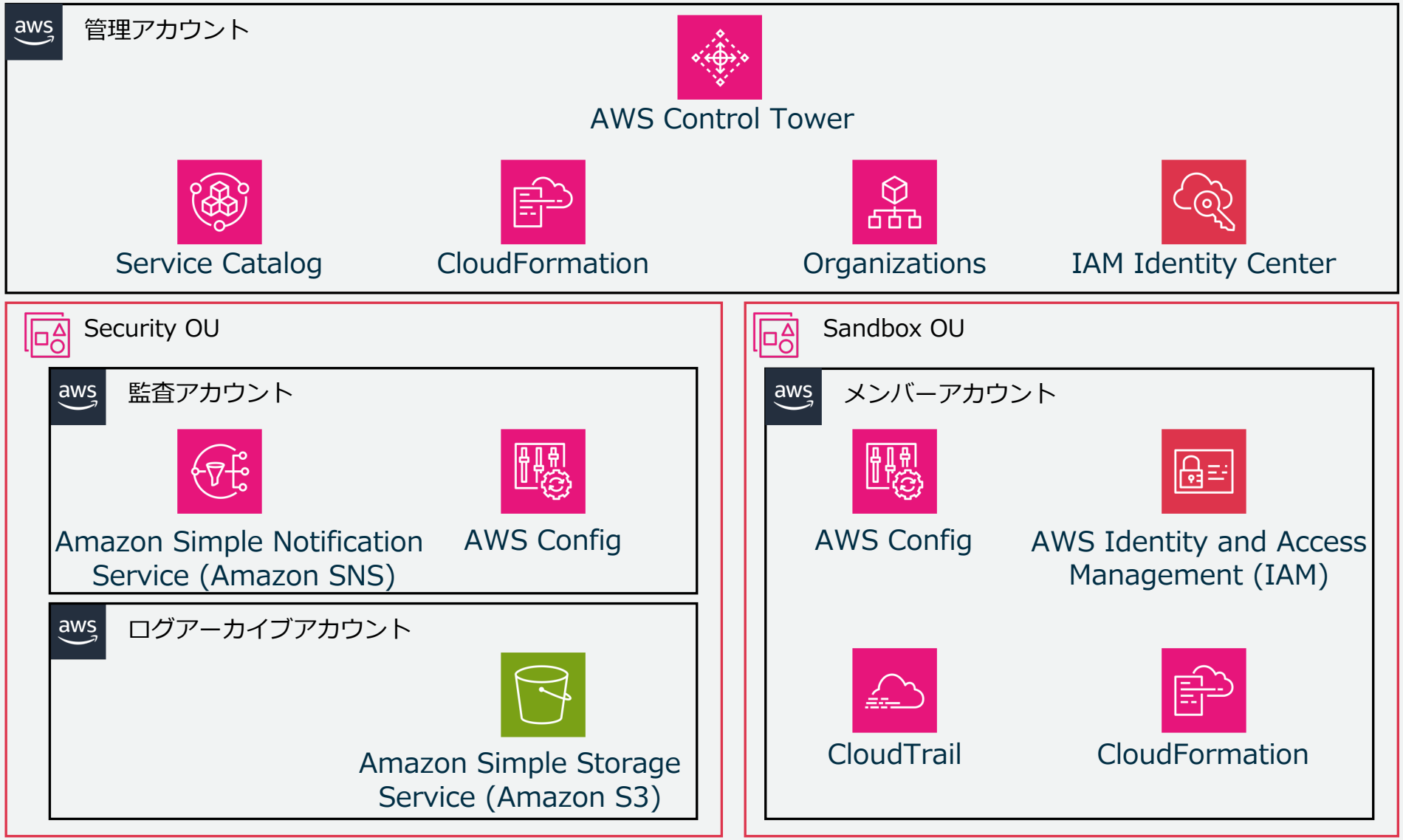
再掲

AWS Control Tower = コンフィグジェネレータ

AWS セキュリティサービス群にベストプラクティスに則った設定を投入し、統制を利かせたマルチアカウント環境 (Landing Zone) を構成、運用するサービス

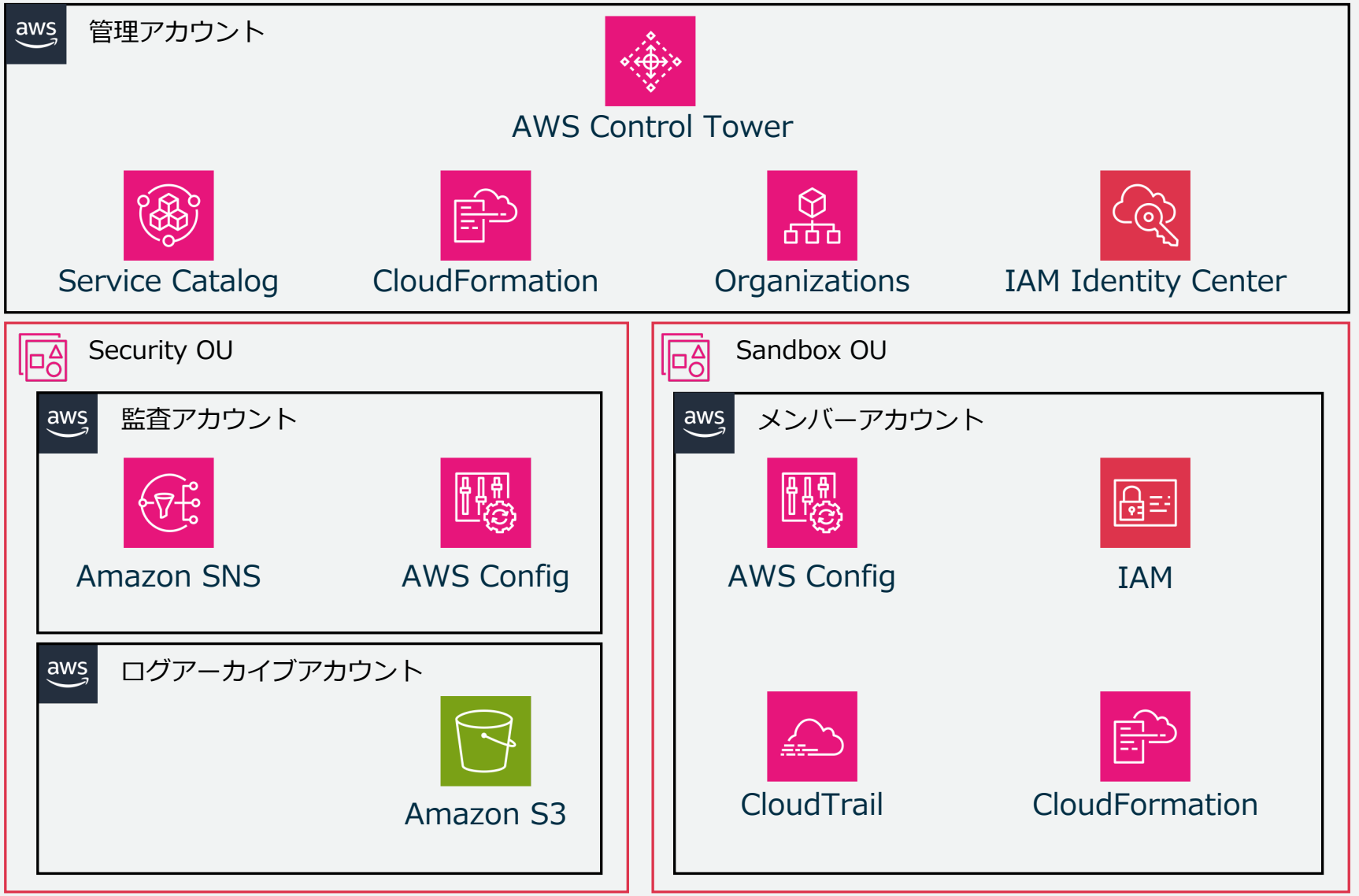


ランディングゾーンの実体



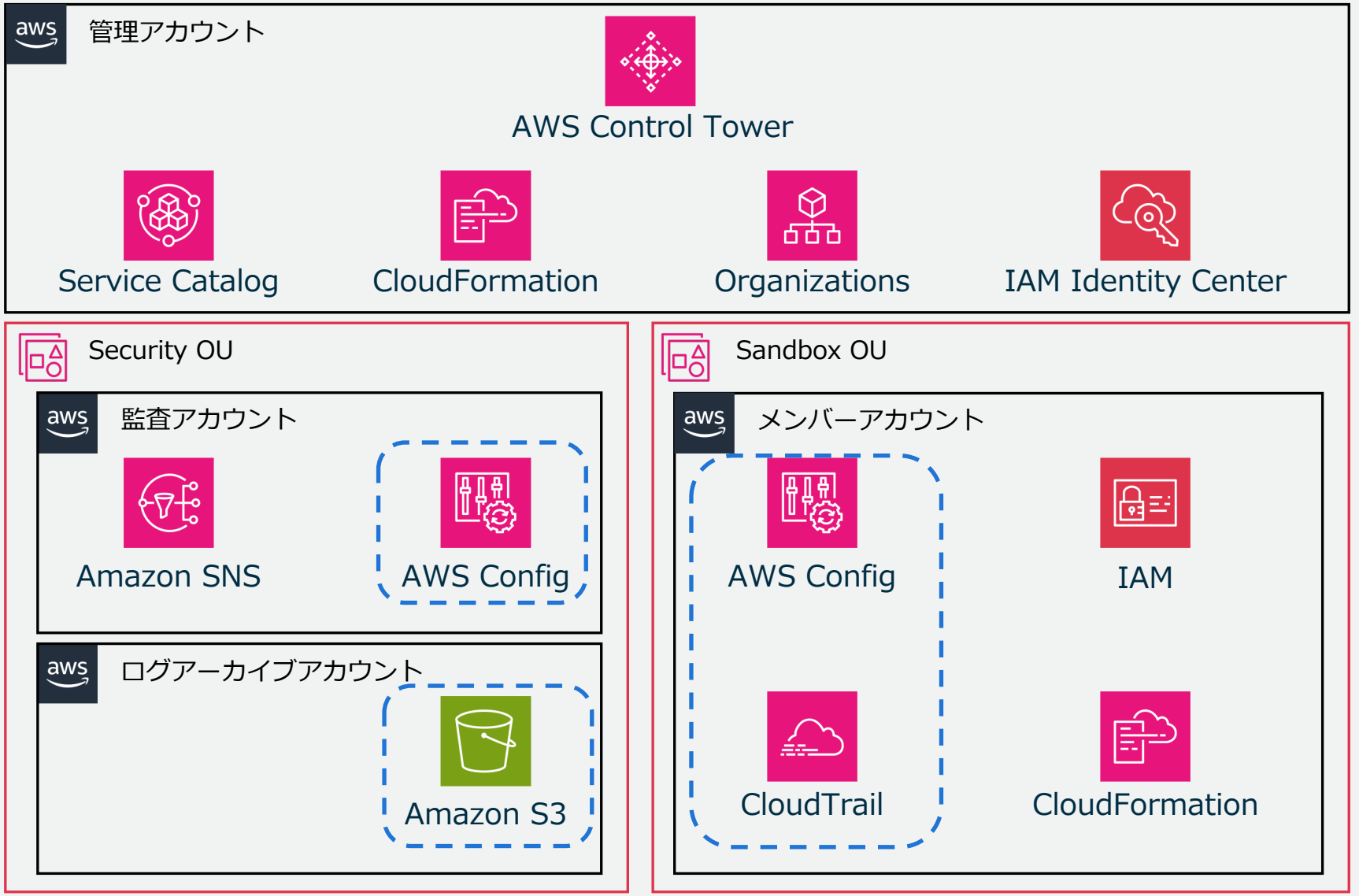
AWS Control Tower で実現できること

- ログ集約
- コントロール適用
- 通知
- ID 一元管理
- AWS アカウント作成とプロビジョニング

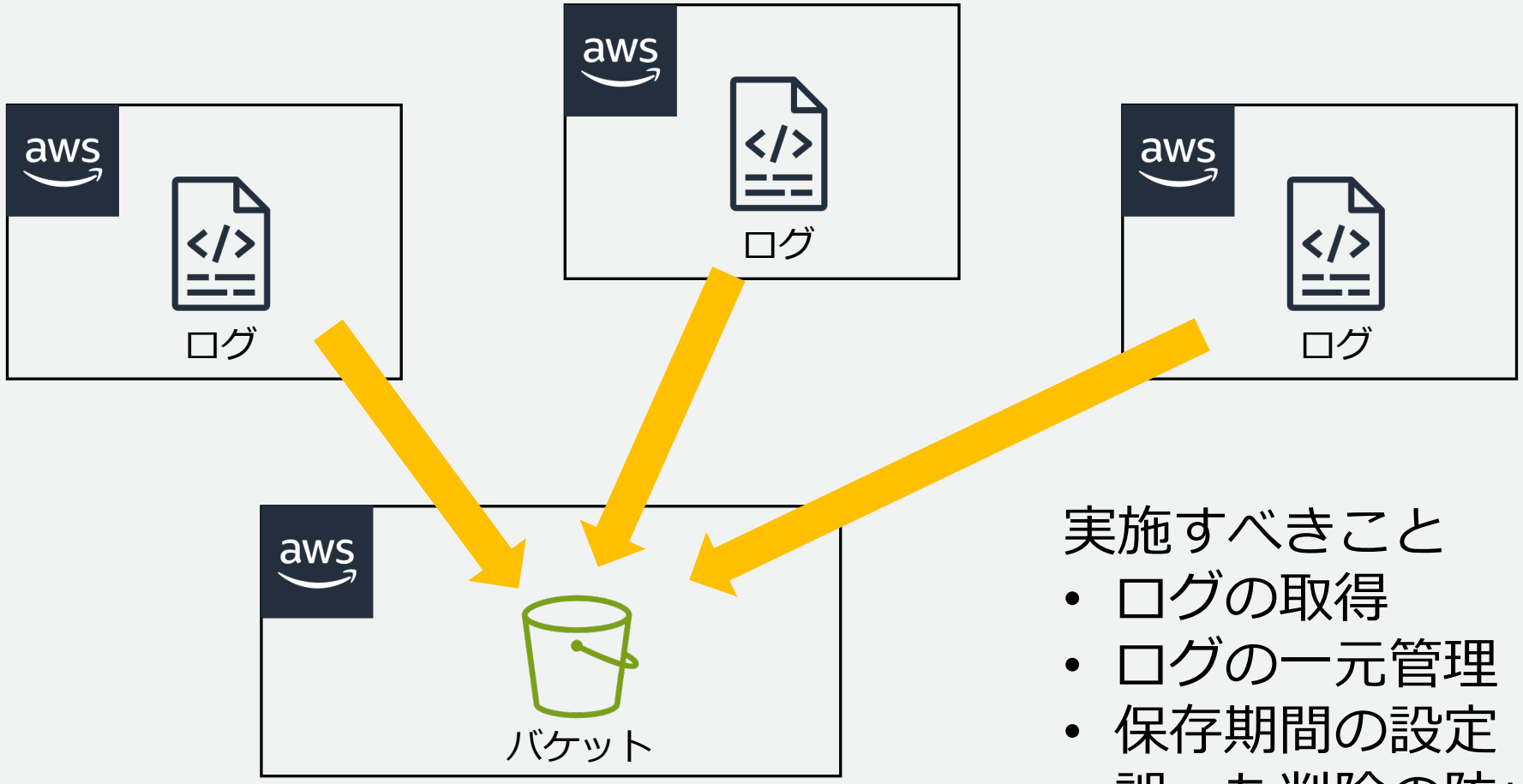


AWS Control Tower で実現できること 1

- ログ集約
- コントロール適用
- 通知
- ID 一元管理
- AWS アカウント作成とプロビジョニング



ログ取得の強制と集約

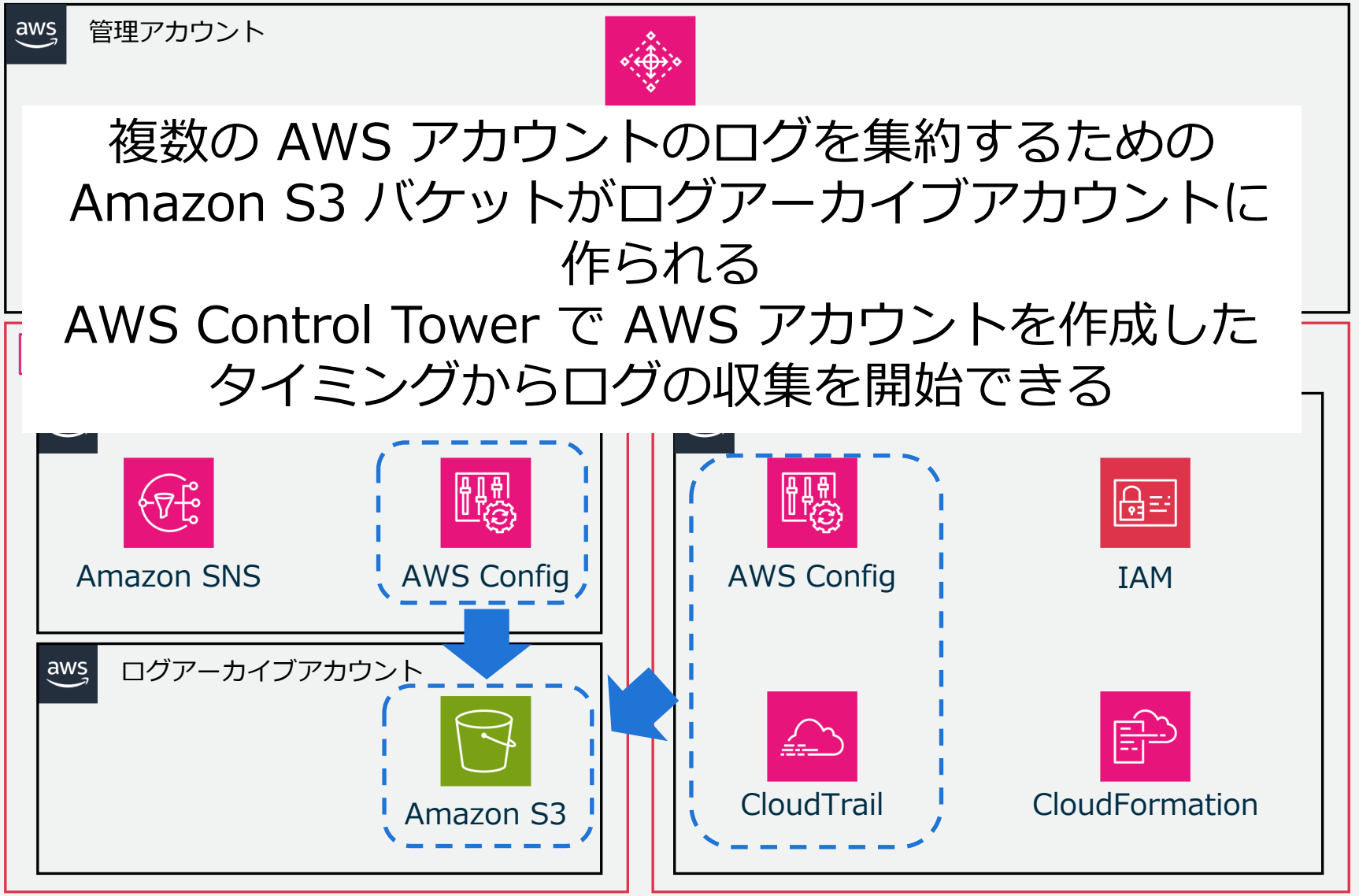


実施すべきこと

- ログの取得
- ログの一元管理
- 保存期間の設定
- 誤った削除の防止

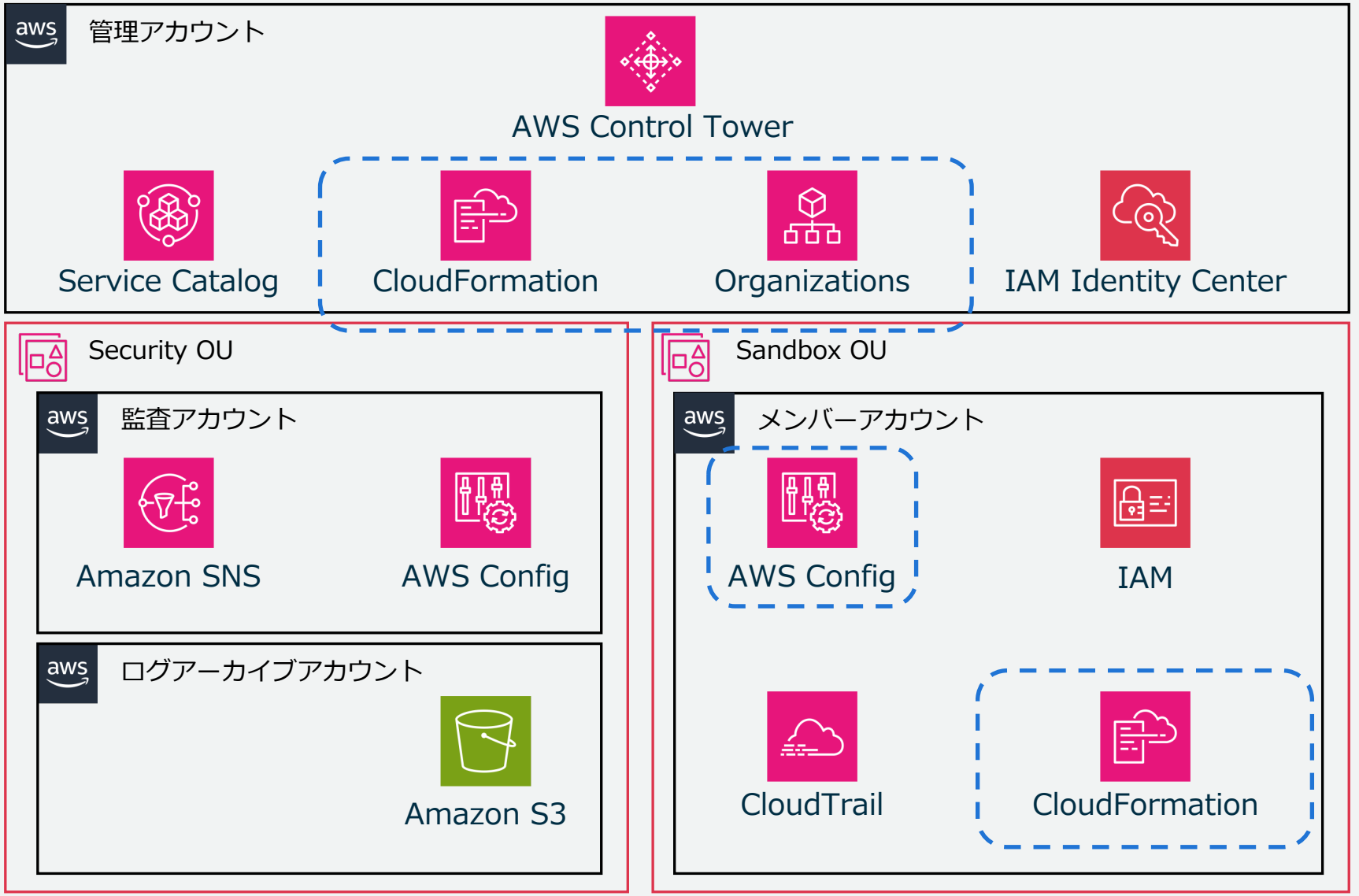
AWS Control Tower で実現できること 1

- ログ集約
- コントロール適用
- 通知
- ID 一元管理
- AWS アカウント作成とプロビジョニング



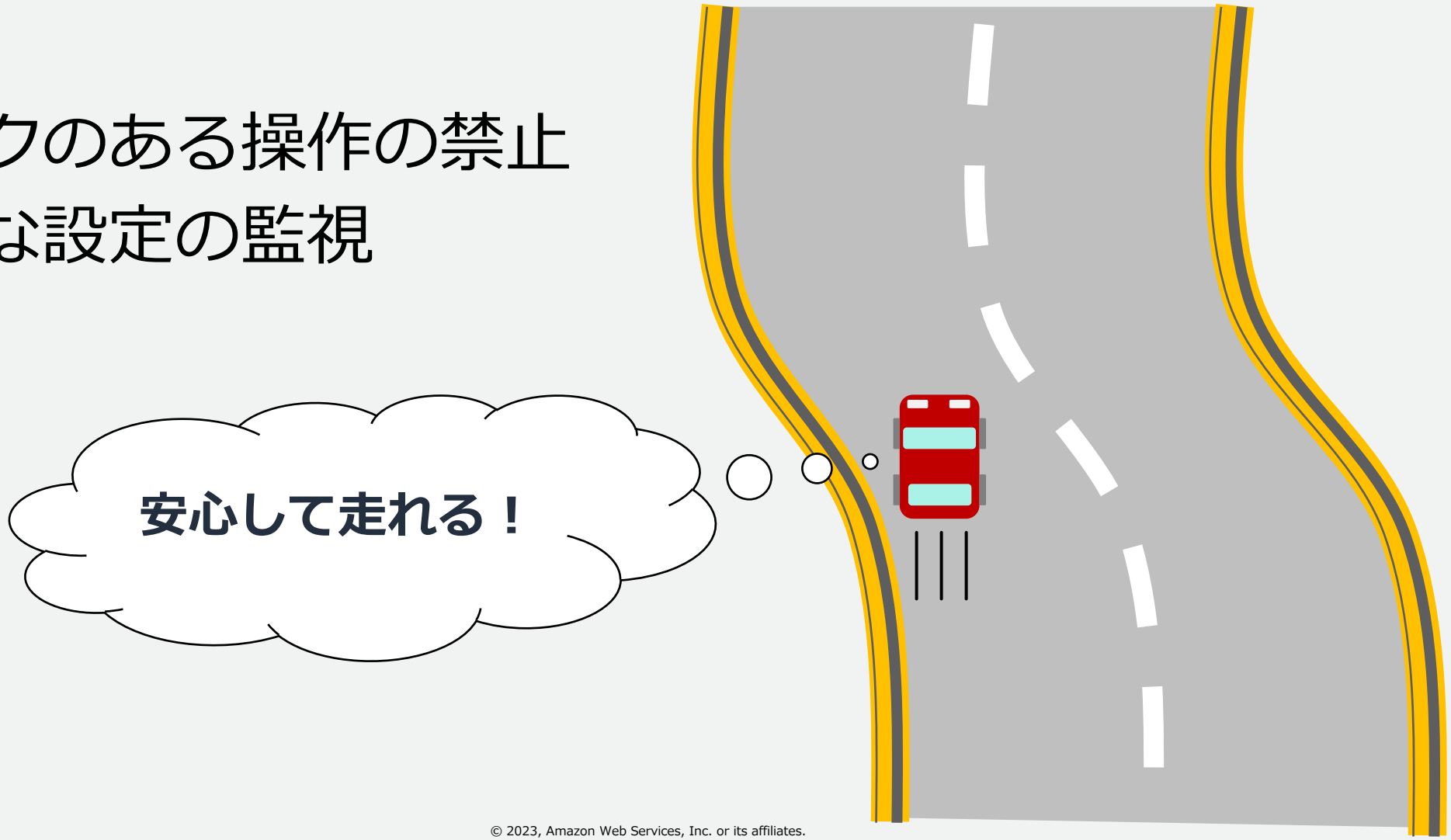
AWS Control Tower で実現できること 2

- ログ集約
- コントロール適用
- 通知
- ID 一元管理
- AWS アカウント作成とプロビジョニング



ガードレールという考え方

- リスクのある操作の禁止
- 危険な設定の監視



コントロールの概要

400 を超えるプリセットから要件に合わせて選択

項目	値
サービス	Amazon Kinesis
名前	[SH.Kinesis.1] Kinesis ストリームは保存時に暗号化する必要があります
統制目標	保管中のデータを暗号化
動作	検出
ガイダンス	選択的

動作の種類

- 予防コントロール
  - 対象の操作を実施できないようにする
    AWS Organizations の SCP で実装
- 検出コントロール
  - 望ましくない操作を行なった場合に発見する
    AWS Config Rules で実装、AWS Security Hub と連携
- プロアクティブコントロール
  - ルールに沿ったリソースのみを作成可能にする
    AWS CloudFormation Hooks で実装

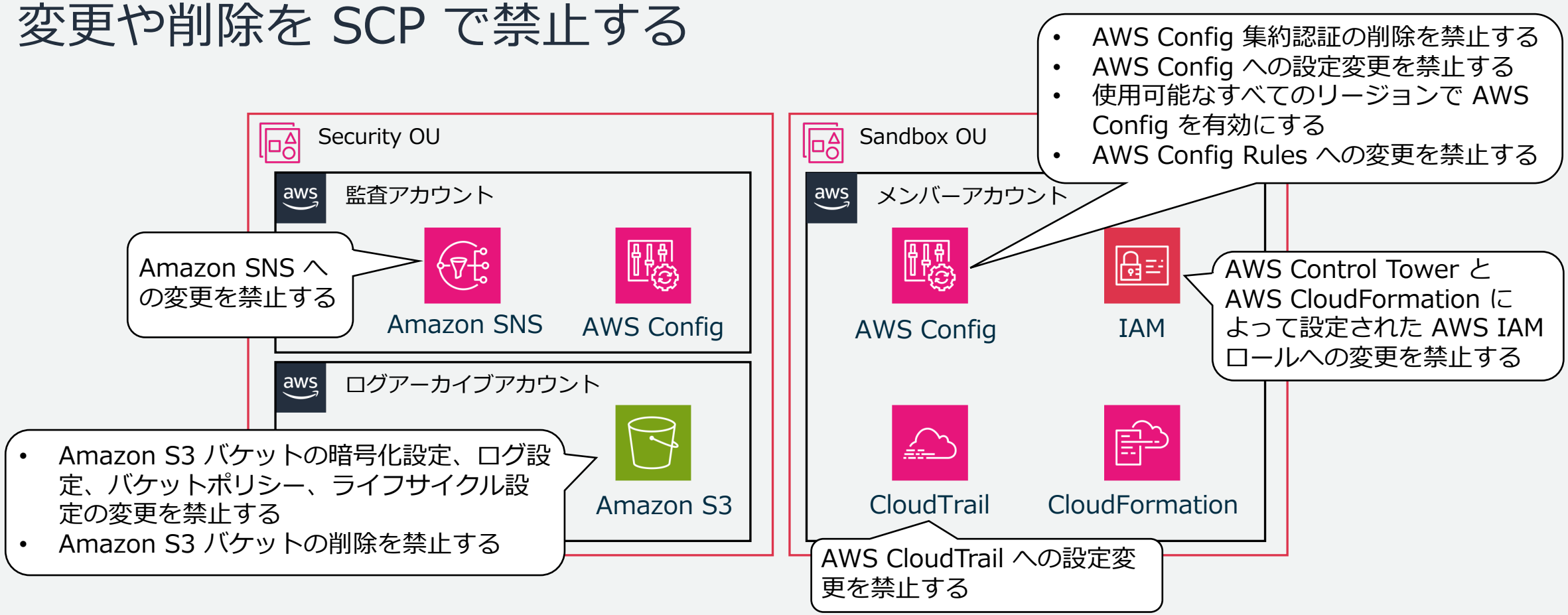
ガイダンスの種類

必須、強く推奨、選択的が存在

必須のコントロールはセットアップ時に必ず適用される

ガイダンスが必須の予防コントロール例

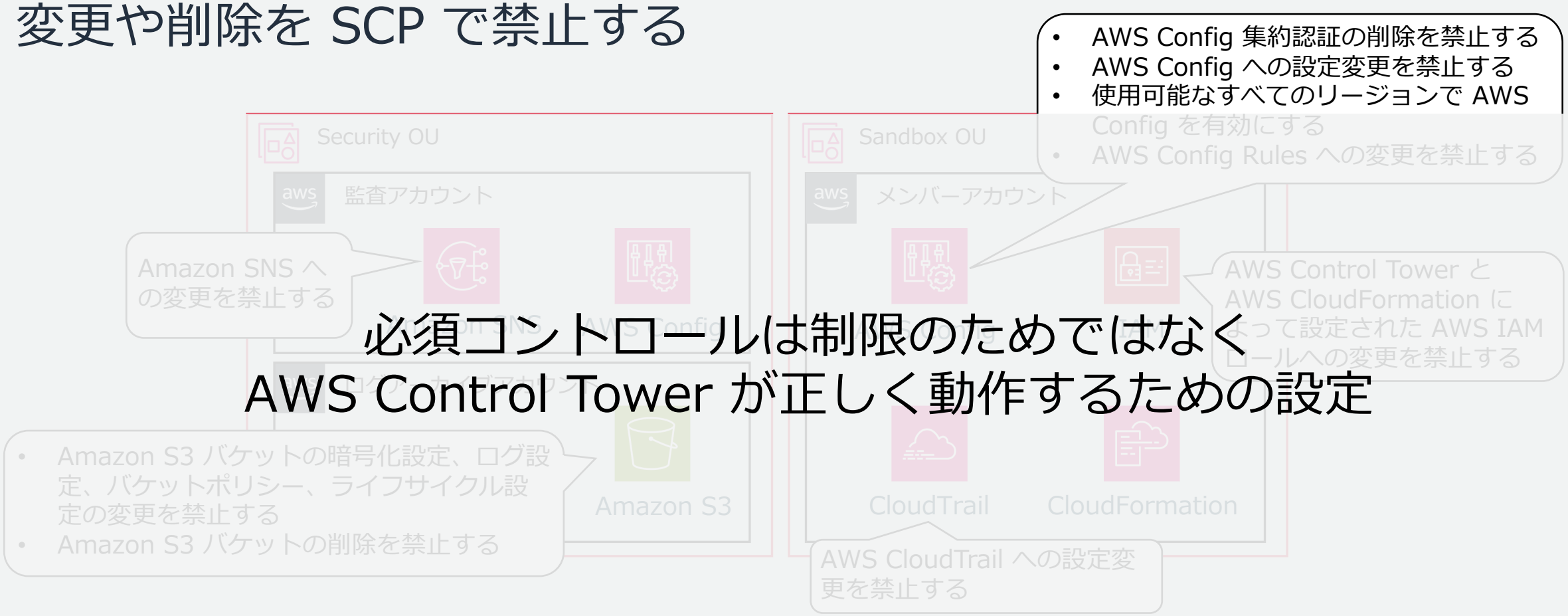
AWS Control Tower で作成、設定したリソースへの変更や削除を SCP で禁止する



https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/mandatory-controls.html

ガイダンスが必須の予防コントロール例

AWS Control Tower で作成、設定したリソースへの変更や削除を SCP で禁止する

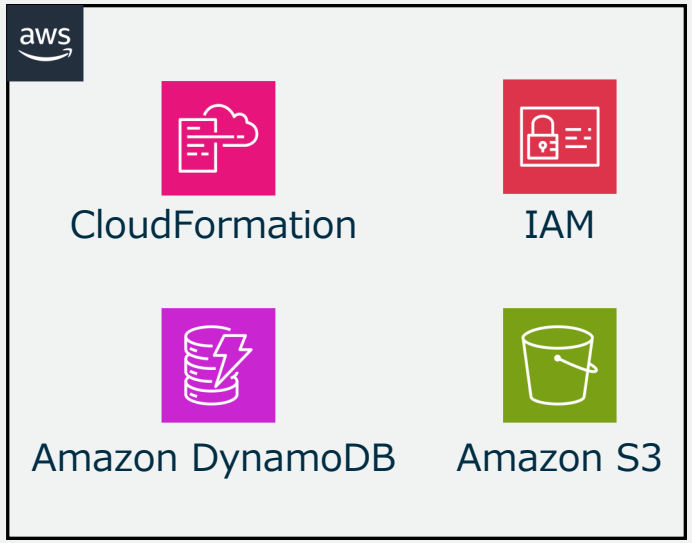


必須コントロールは制限のためではなく
AWS Control Tower が正しく動作するための設定

https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/mandatory-controls.html

コントロール適用例

項目	値
サービス	Amazon DynamoDB
名前	[CT.DYNAMODB.PR.2] Amazon DynamoDB テーブルが AWS KMS キーを使用して保管中に暗号化されることを要求する
統制目標	保管中のデータを暗号化
動作	プロアクティブ
ガイダンス	選択的

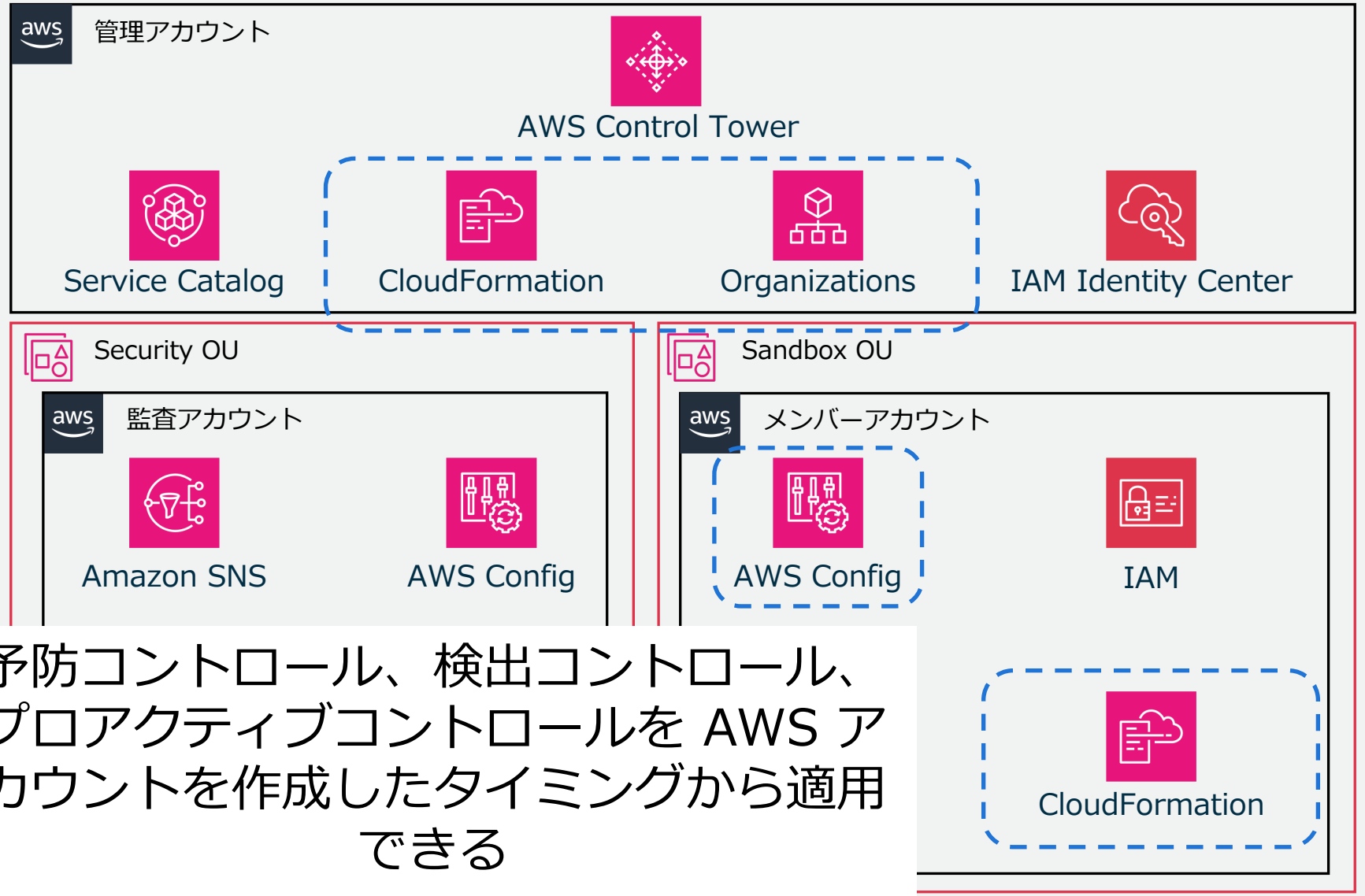


項目	値
サービス	IAM
名前	[AWS-GR_RESTRICT_ROOT_USER] ルートユーザーとしてのアクションを許可しない
統制目標	最小特権を強制
動作	予防
ガイダンス	強く推奨

項目	値
サービス	Amazon S3
名前	[SH.S3.2] S3 バケットはパブリック読み取りアクセスを禁止するべきです
統制目標	最小特権を強制
動作	検出
ガイダンス	選択的

AWS Control Tower で実現できること 2

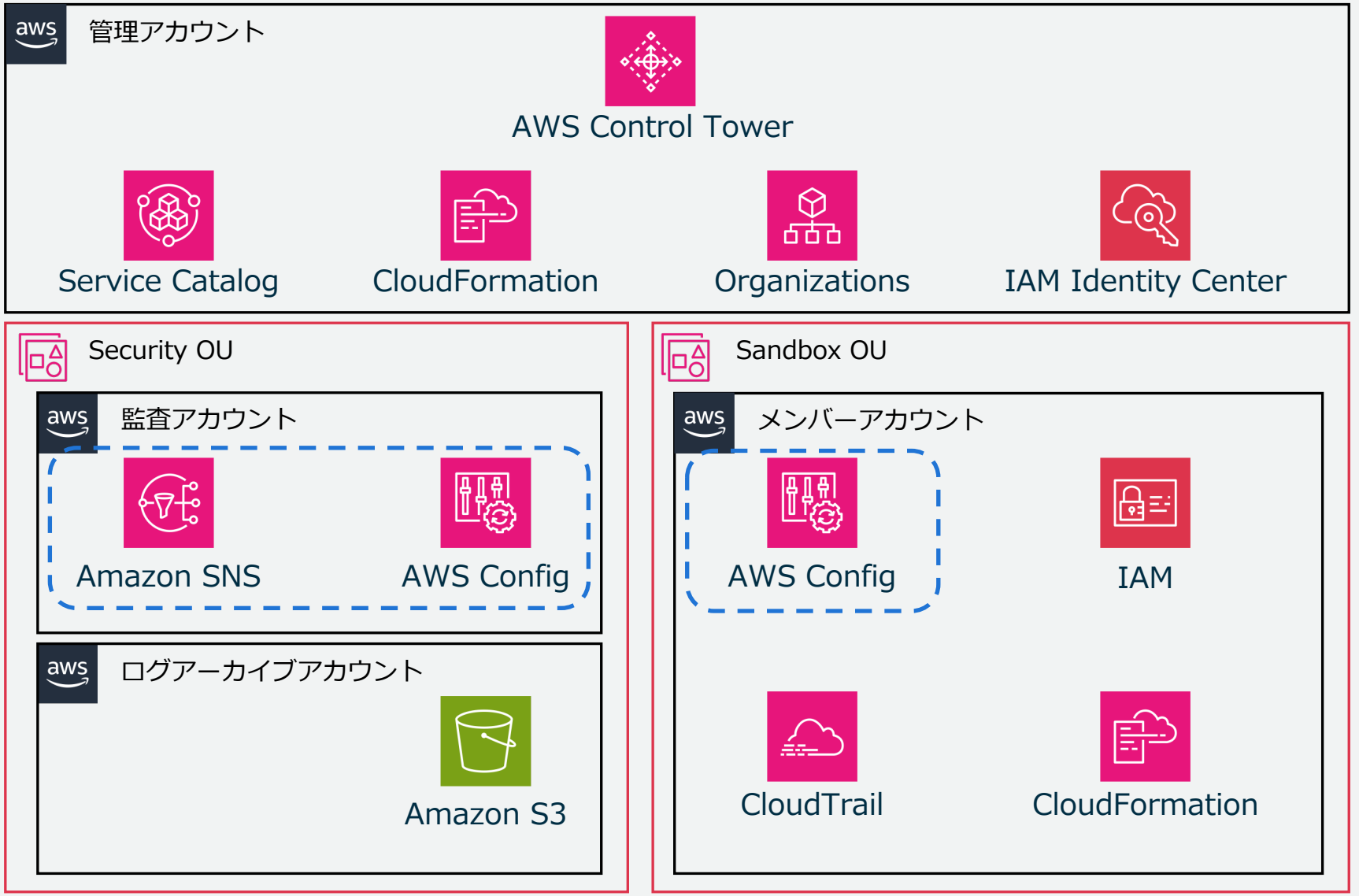
- ログ集約
- コントロール適用
- 通知
- ID 一元管理
- AWS アカウント作成とプロビジョニング



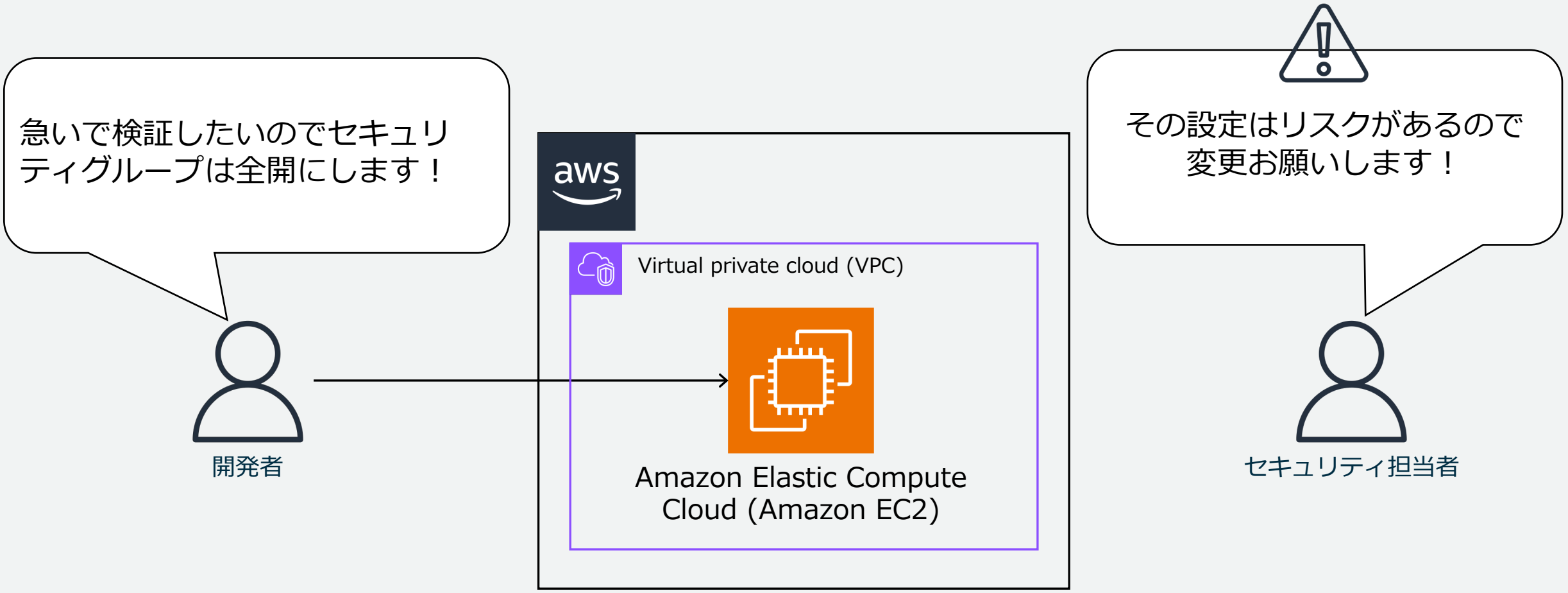
予防コントロール、検出コントロール、プロアクティブコントロールを AWS アカウントを作成したタイミングから適用できる

AWS Control Tower で実現できること 3

- ログ集約
- コントロール適用
- 通知
- ID 一元管理
- AWS アカウント作成とプロビジョニング



リスクある操作に気づく



AWS Control Tower で実現できること 3

ログ集約

コントロール

通知

ID 一元管理

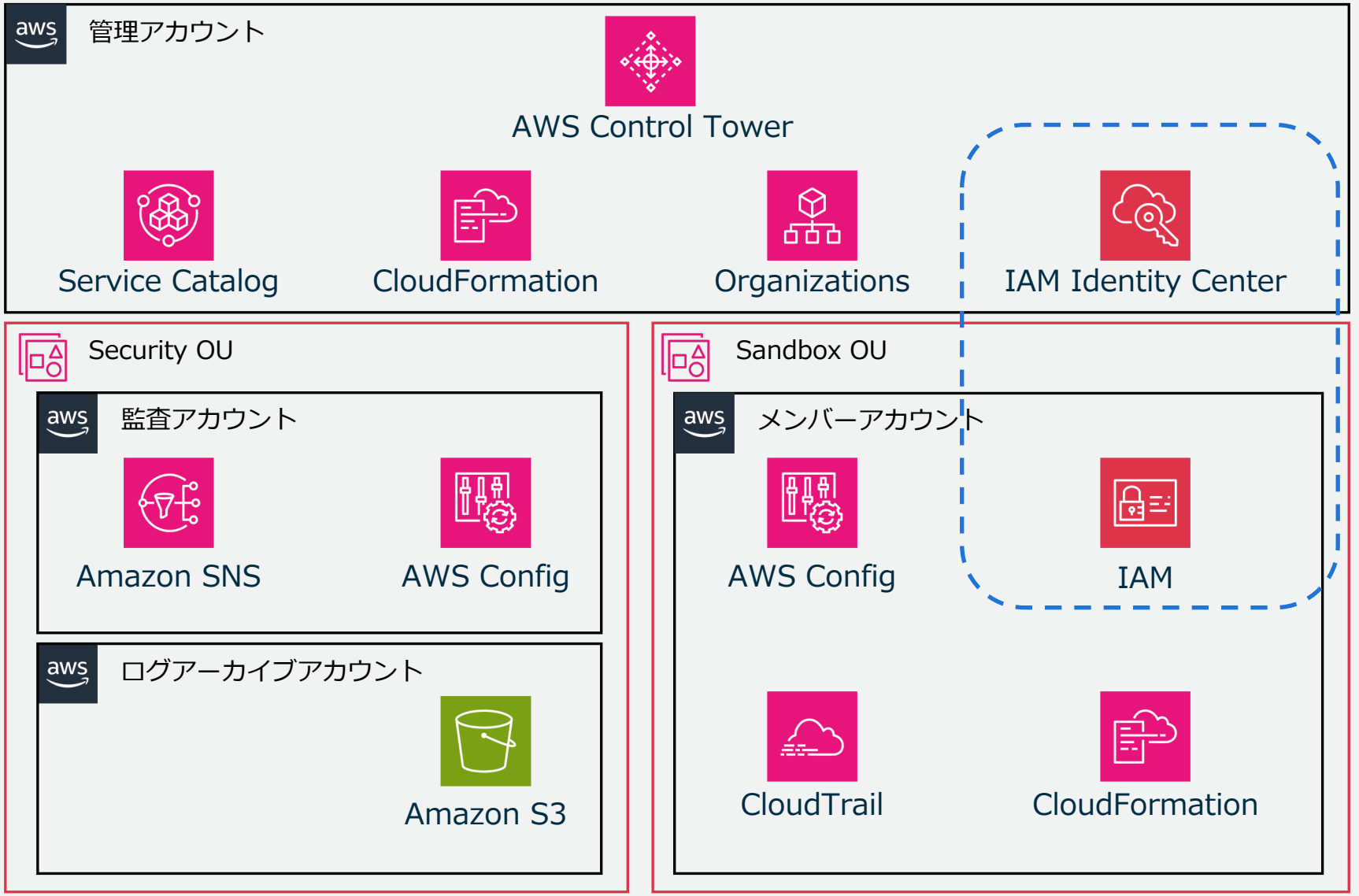
AWS アカウント作成と
プロビジョニング

AWS Config で把握した AWS リソースの変更情報と
AWS Config rules の準拠状況を Amazon SNS を使用して
通知することができる

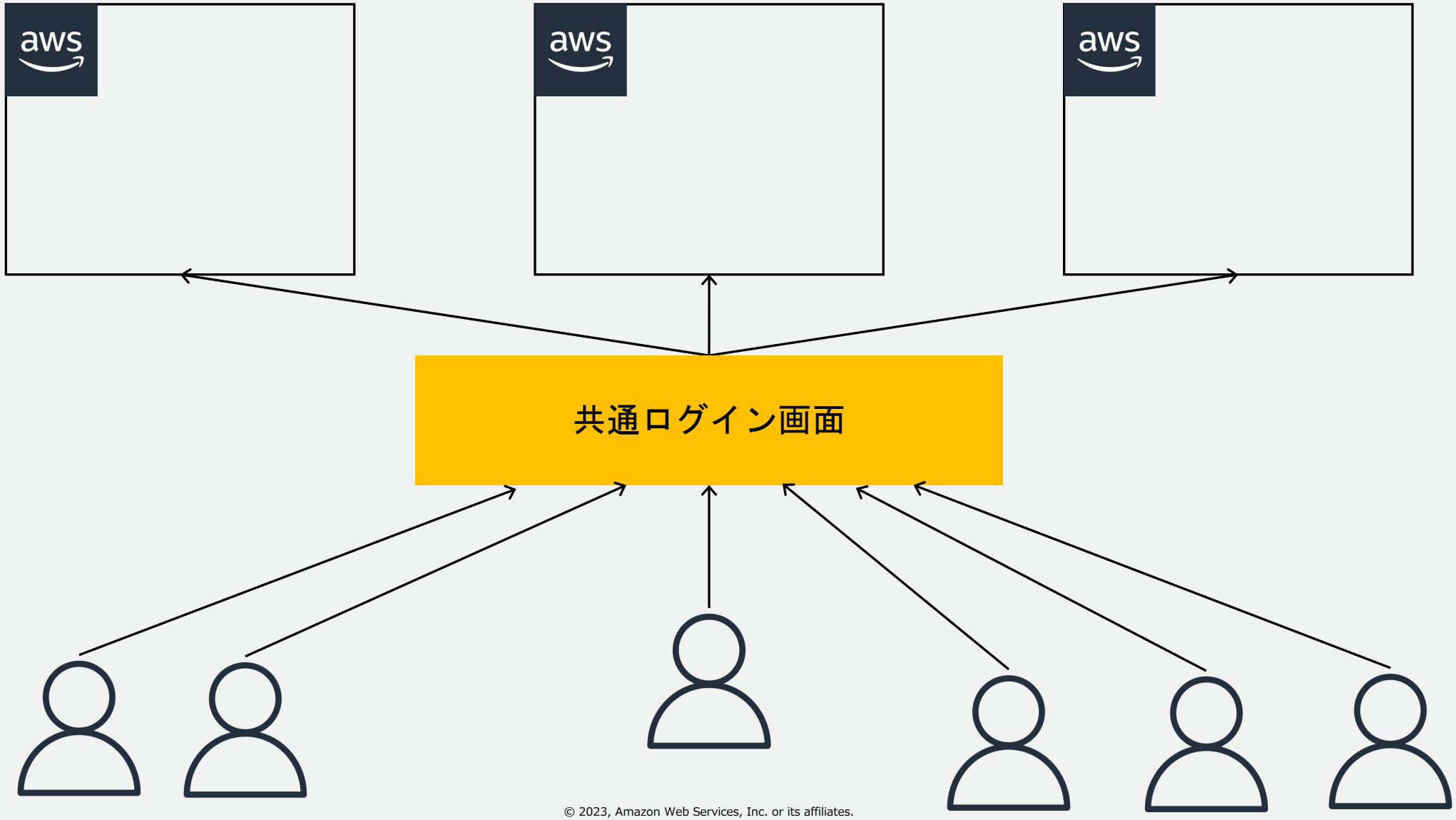
https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/receive-notifications.html

AWS Control Tower で実現できること 4

- ログ集約
- コントロール適用
- 通知
- ID 一元管理
- AWS アカウント作成とプロビジョニング



ログインの導線とユーザ管理を一本化



AWS Control Tower で実現できること 4

ログ集約

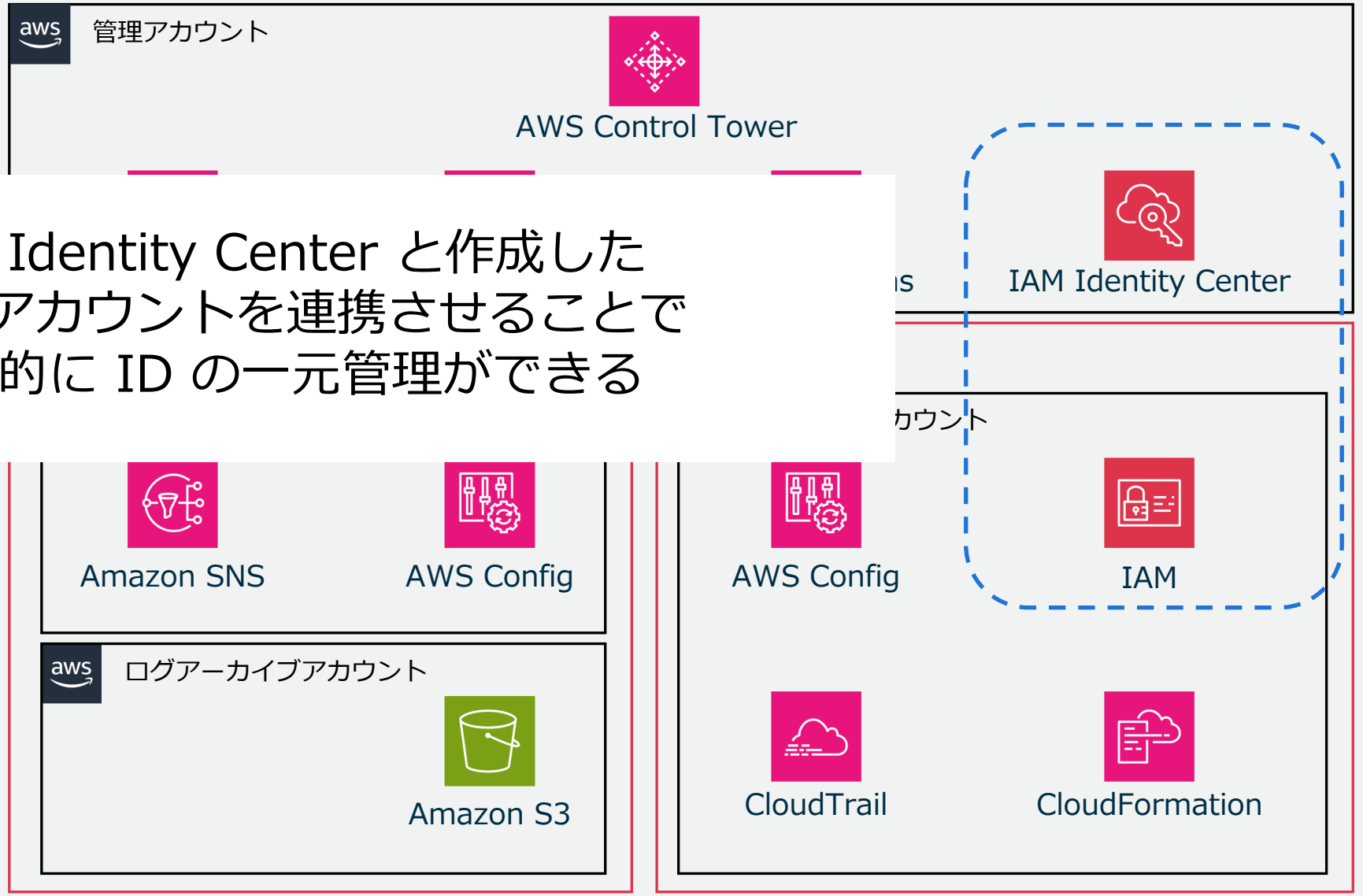
コントロ

通知

ID 一元管理

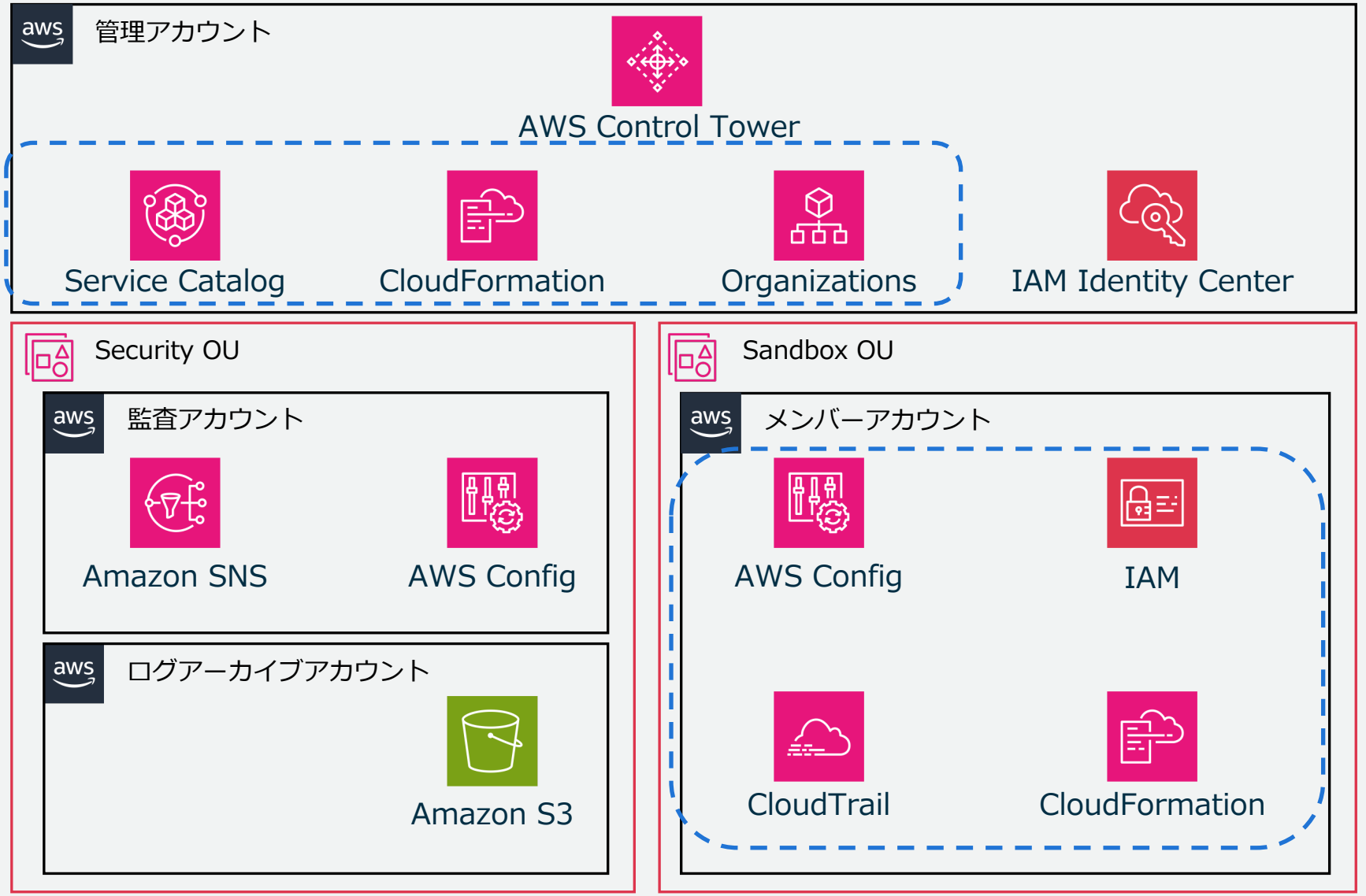
AWS アカウント作成と
プロビジョニング

IAM Identity Center と作成した
AWS アカウントを連携させることで
効率的に ID の一元管理ができる



AWS Control Tower で実現できること 5

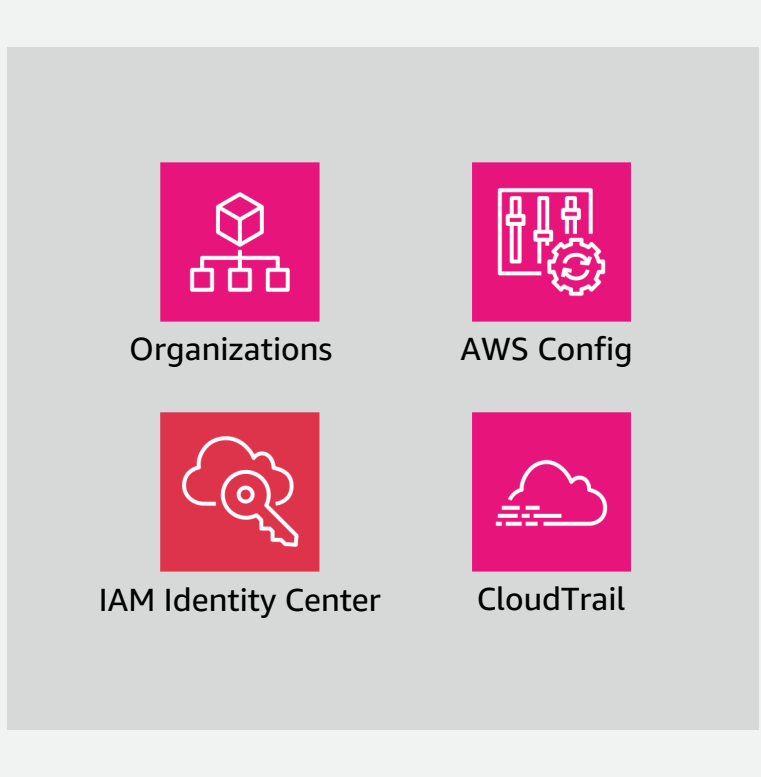
- ログ集約
- コントロール適用
- 通知
- ID 一元管理
- AWS アカウント作成とプロビジョニング



Account Factory で AWS アカウントのプロビジョニング

- 各種機能がはじめから設定

・ログ集約
・コントロール



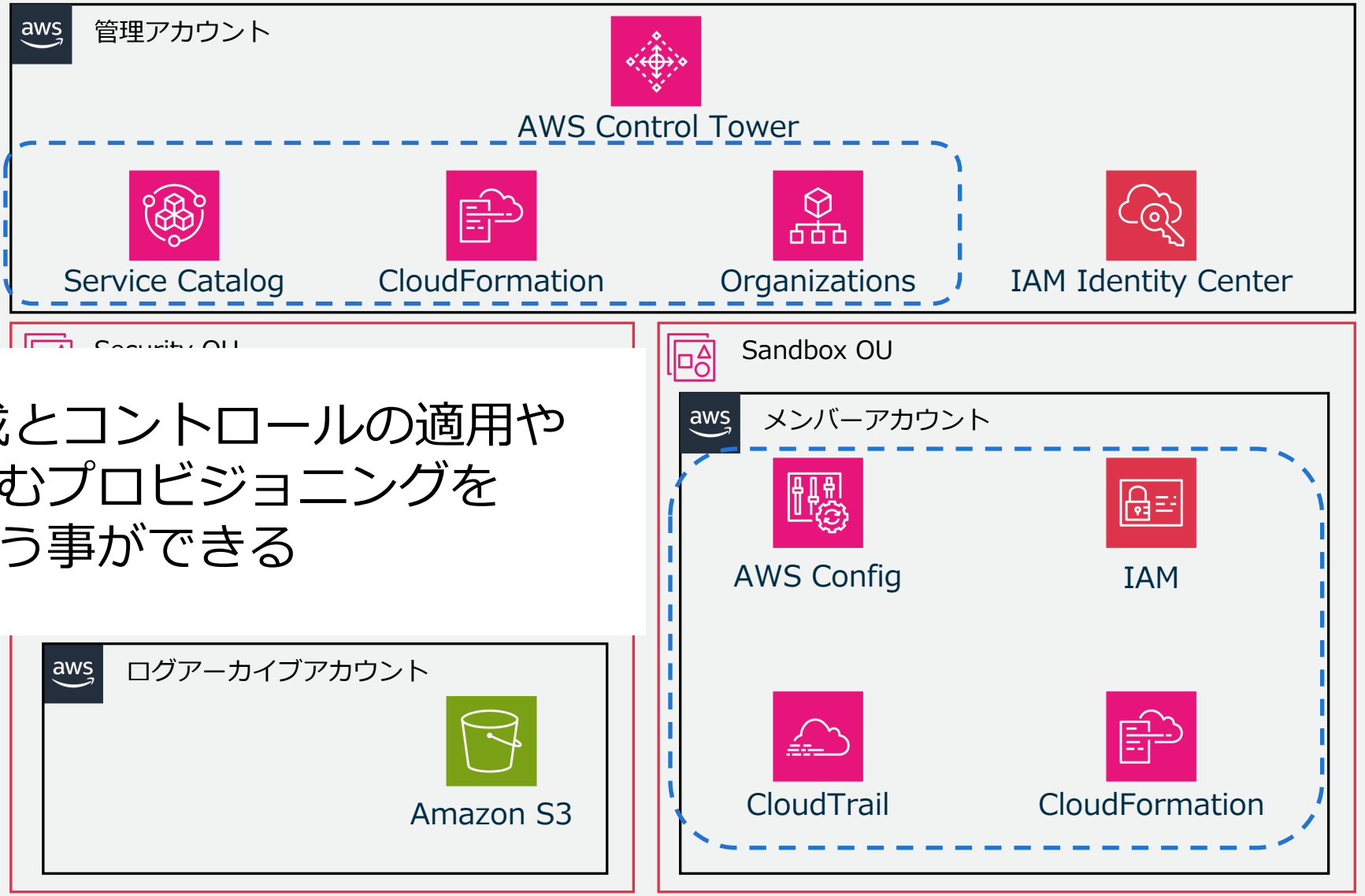
AWS Control Tower で実現できること 5

ログ集約

コントロール適用

AWS アカウントの作成とコントロールの適用や
ログ集約の設定を含むプロビジョニングを
効率的に行う事ができる

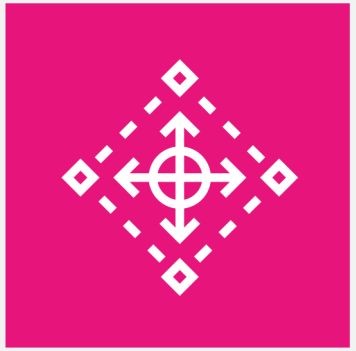
AWS アカウント作成と
プロビジョニング



まとめ

AWS Control Tower

マルチアカウント環境のセットアップを自動化する マネージドサービス



AWS Control Tower

マネージド
サービス

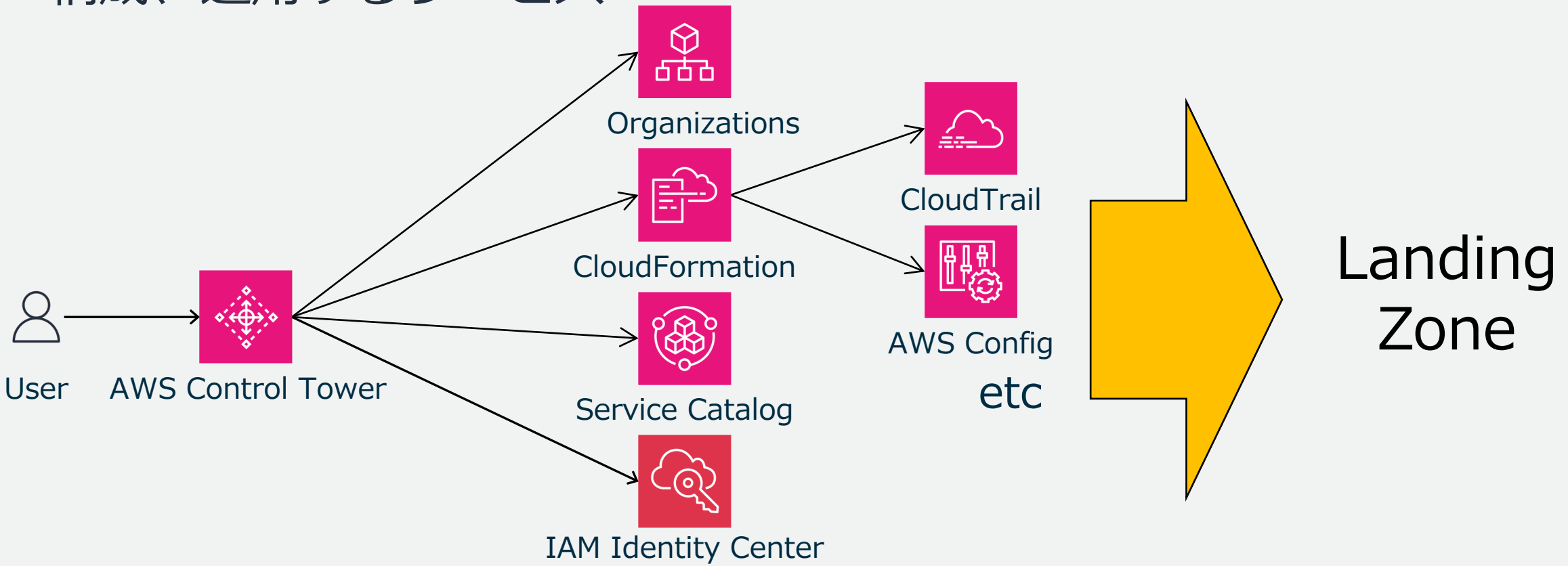
ベストプラクティス
に基づく環境

追加料金なし

注意) AWS Control Tower を通じてセットアップするように設定されたサービスは費用が発生する可能性があります

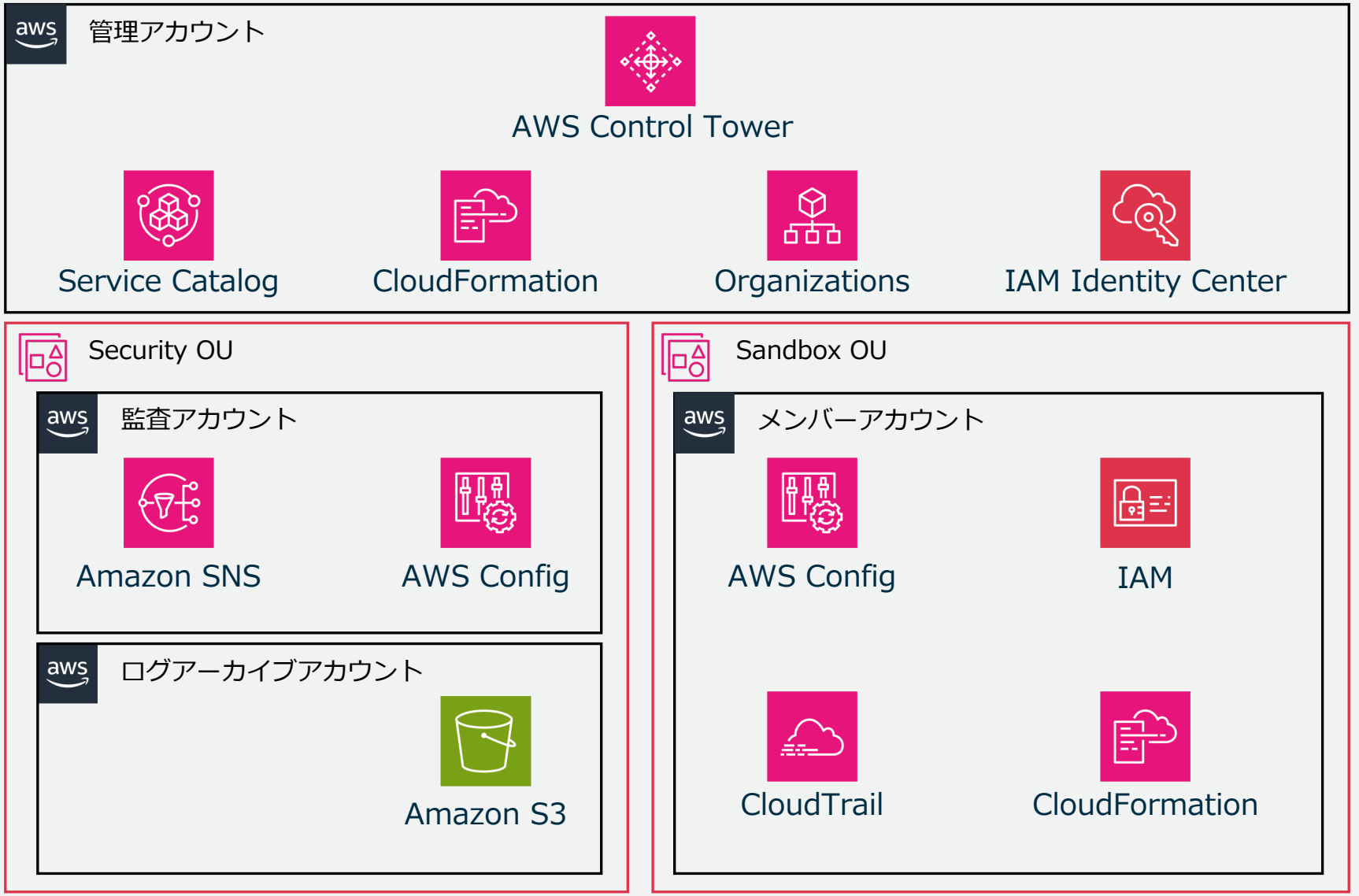
AWS Control Tower = コンフィグジェネレータ

AWS セキュリティサービス群にベストプラクティスに則った設定を投入し、統制を利かせたマルチアカウント環境 (Landing Zone) を構成、運用するサービス



AWS Control Tower で実現できること

- ログ集約
- コントロール適用
- 通知
- ID 一元管理
- AWS アカウント作成とプロビジョニング



AWS Black Belt Online Seminar とは

- 「サービス別」「ソリューション別」「業種別」などのテーマに分け、アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- AWS の技術担当者が、AWS の各サービスやソリューションについてテーマごとに動画を公開します
- 以下の URL より、過去のセミナー含めた資料などをダウンロードすることができます
  - https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/
  - https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY

ご感想は X (Twitter) へ！ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- 本資料では 2023 年 8 月時点のサービス内容および価格についてご説明しています。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (https://aws.amazon.com/) にてご確認ください
- 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます
- 技術的な内容に関しましては、有料の AWS サポート窓口へお問い合わせください
- 料金面でのお問い合わせに関しましては、カスタマーサポート窓口へお問い合わせください (マネジメントコンソールへのログインが必要です)

Thank you!