AWS Black Belt Online Seminar

AWS Control Tower

機能紹介編

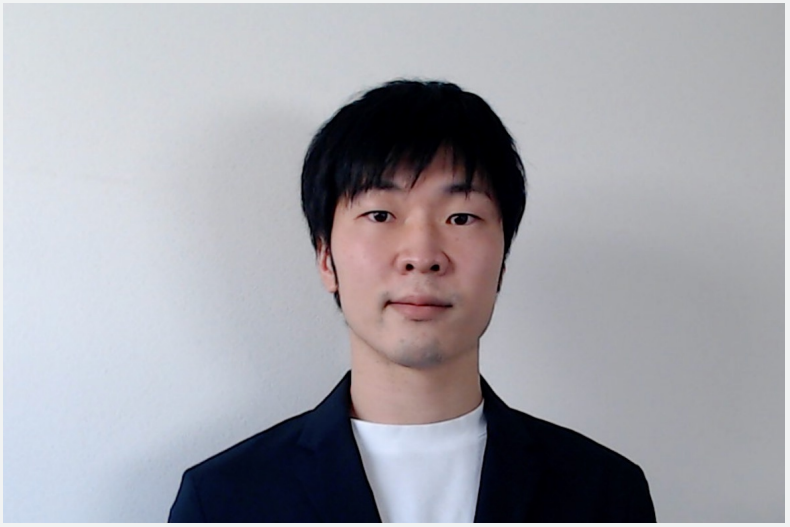
桂井 俊朗

Solutions Architect
2023/09

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

AWS Control Tower に興味のある方

AWS Control Tower について深く学びたい方

本セミナーの前提知識

AWS Black Belt Online Seminar AWS Control Tower 基礎編

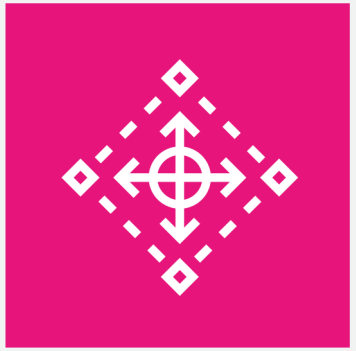
アジェンダ

1. AWS Control Tower とは
2. AWS Control Tower の状態と作成されるリソース
3. AWS Control Tower 機能紹介
4. まとめ

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

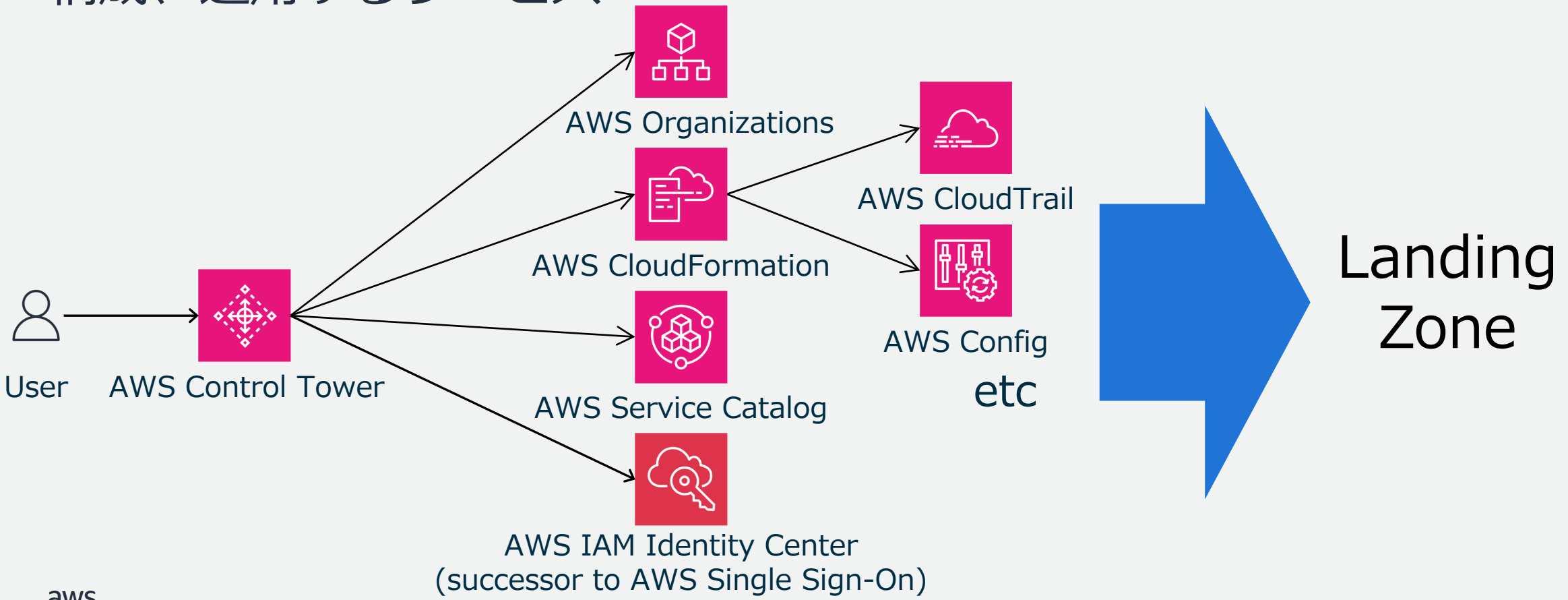
ベストプラクティス
に基づく環境

追加料金なし

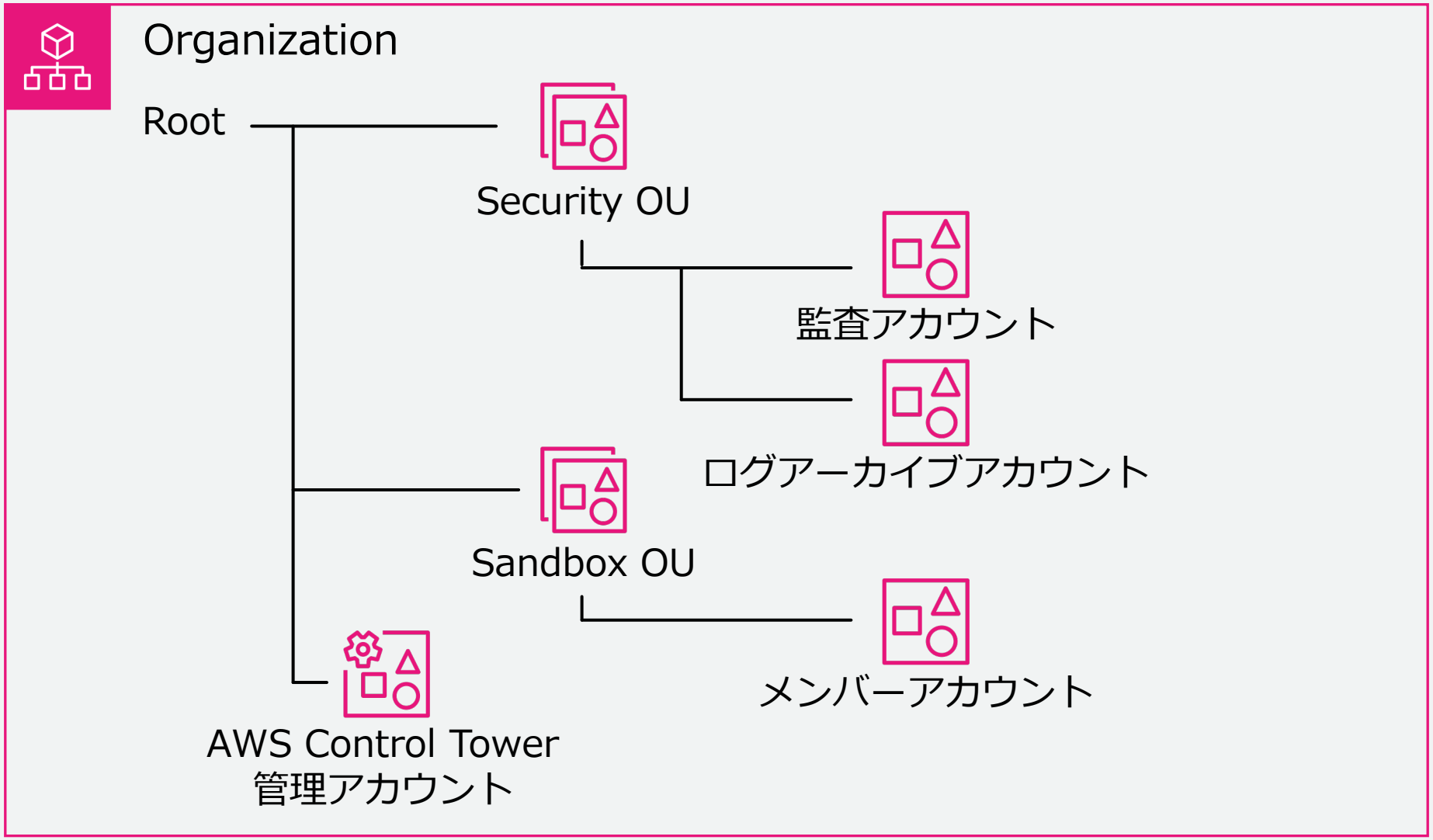
注意) AWS Control Tower を通じてセットアップするように設定されたサービスは費用が発生する可能性があります

AWS Control Tower = コンフィグジェネレータ

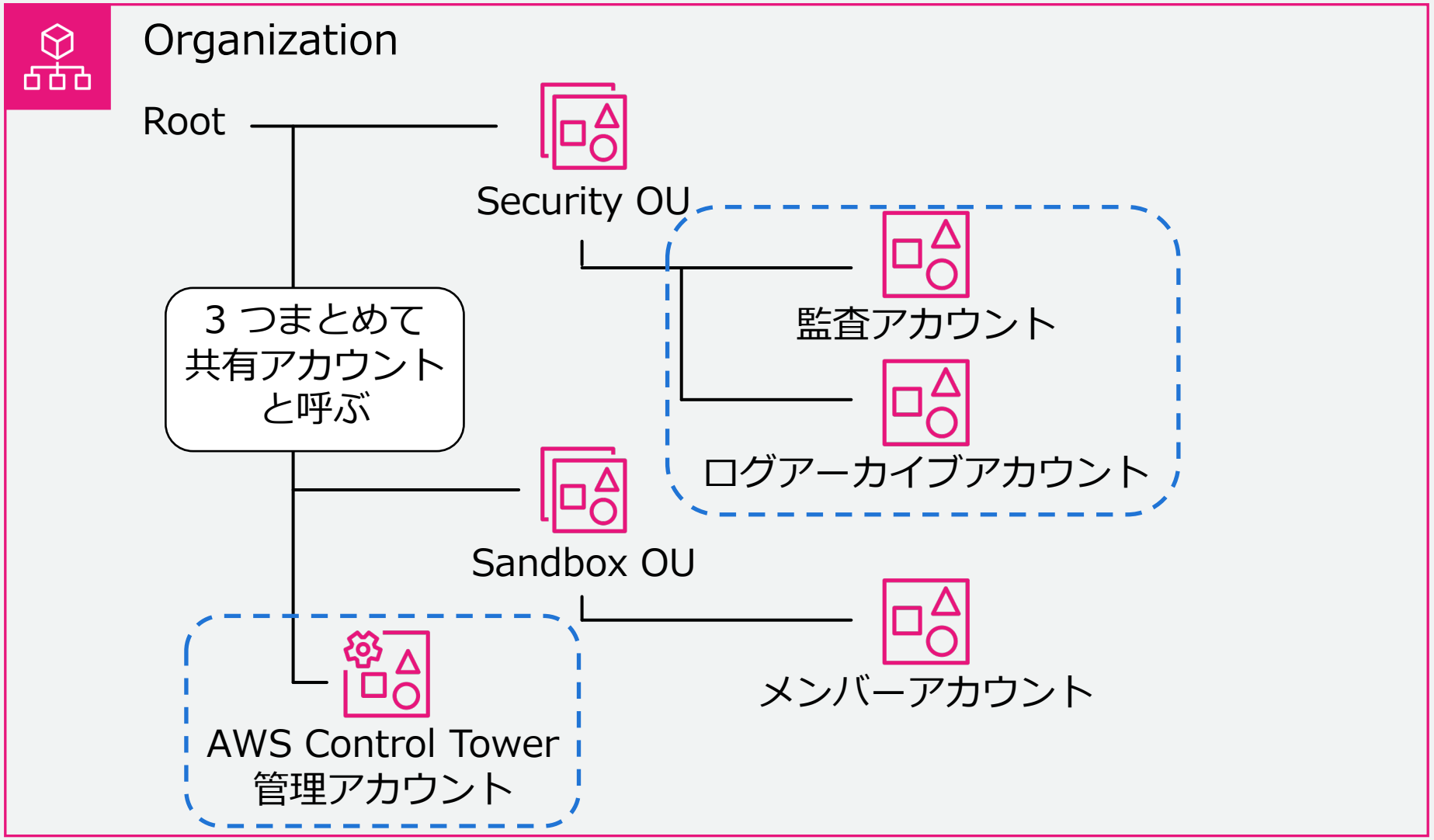
AWS セキュリティサービス群にベストプラクティスに則った設定を投入し、統制を利かせたマルチアカウント環境 (Landing Zone) を構成、運用するサービス



AWS Control Tower のアカウント区分

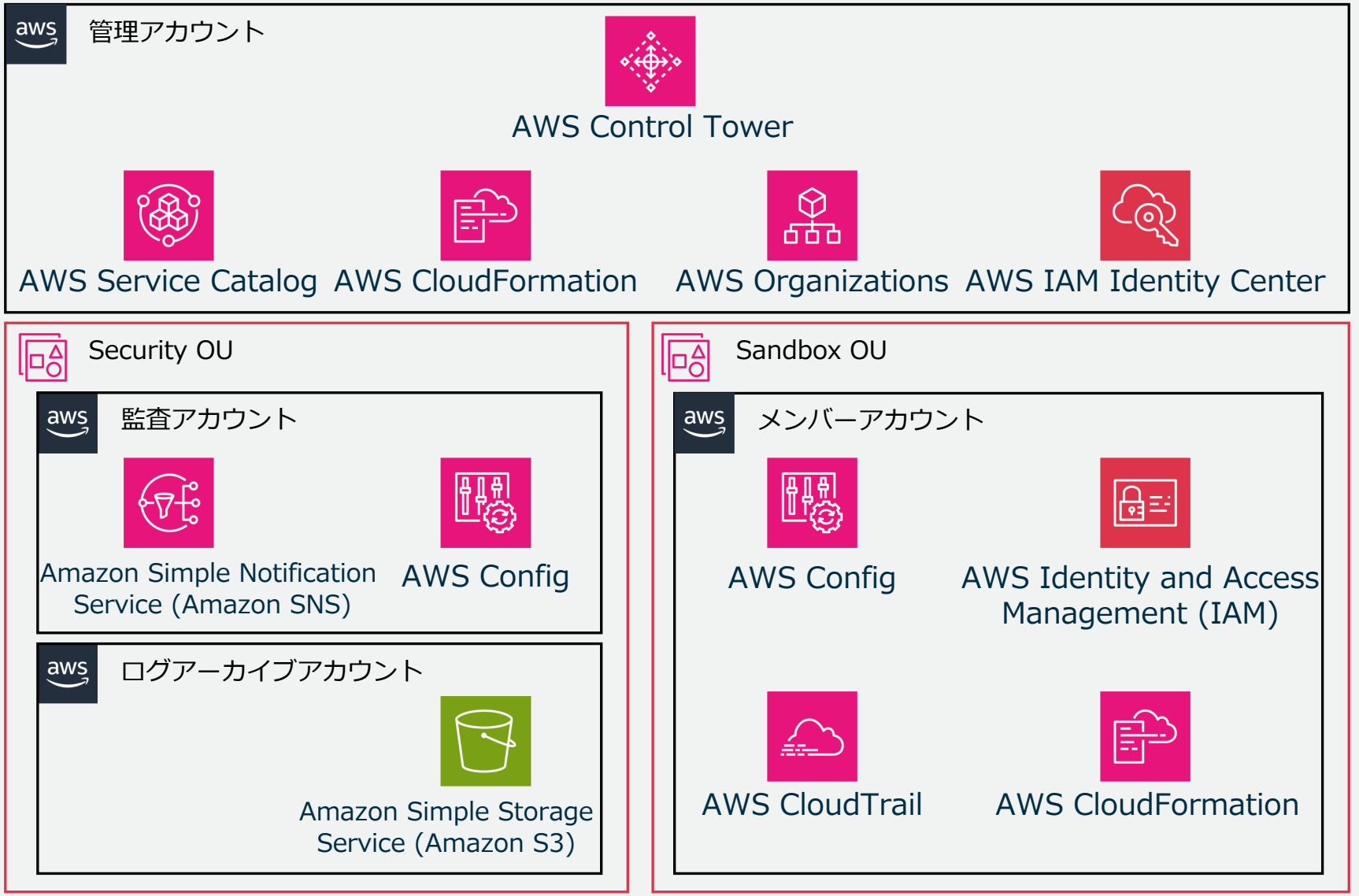


AWS Control Tower のアカウント区分



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 の状態と作成されるリソース

AWS Control Tower の状態

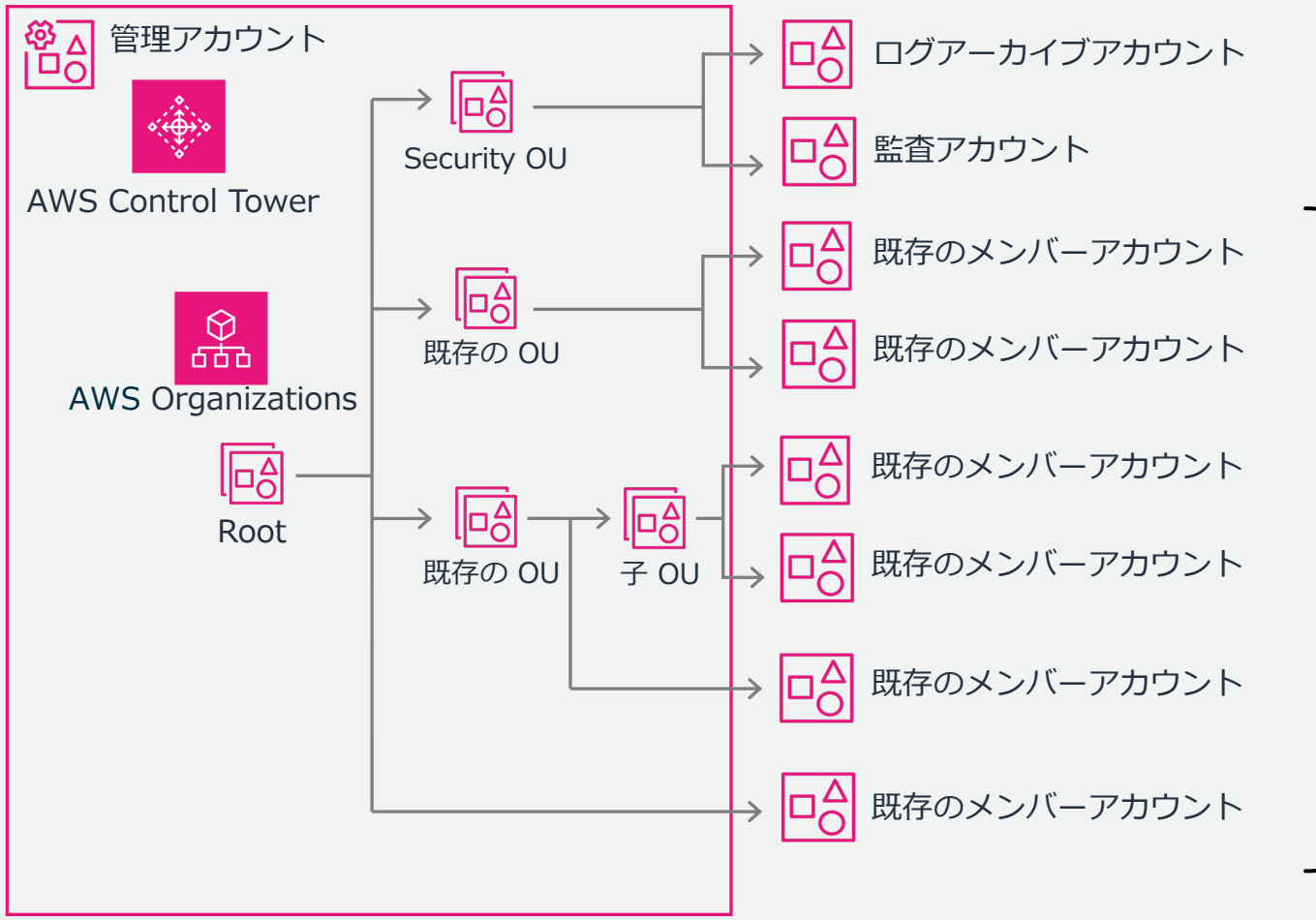
AWS Control Tower で管理対象となるアカウントには状態が存在する

状態	説明
未登録	アカウントは親 OU のメンバーですが、AWS Control Tower によって管理されていません
登録中	AWS Control Tower の管理対象になっています。親 OU のコントロール設定に適合するようにアカウントが調整されてます
登録済み	アカウントは、その親 OU 用に設定されたコントロールによって管理されています。AWS Control Tower によって管理されています
登録に失敗しました	登録を試みましたが、アカウントを AWS Control Tower に登録できていません
更新が利用可能	アカウントは登録済みですが、アカウントには利用可能な更新があります。環境に加えられた最近の変更を反映するには、アカウントを更新する必要があります

初期は「未登録」で登録を実行すると「登録済み」に遷移する

メンバーアカウントの登録

- ランディングゾーンのセットアップだけでは、登録されない



別途 AWS Control Tower への登録作業が必要となる

AWS Control Tower 利用時のリソース作成タイミング

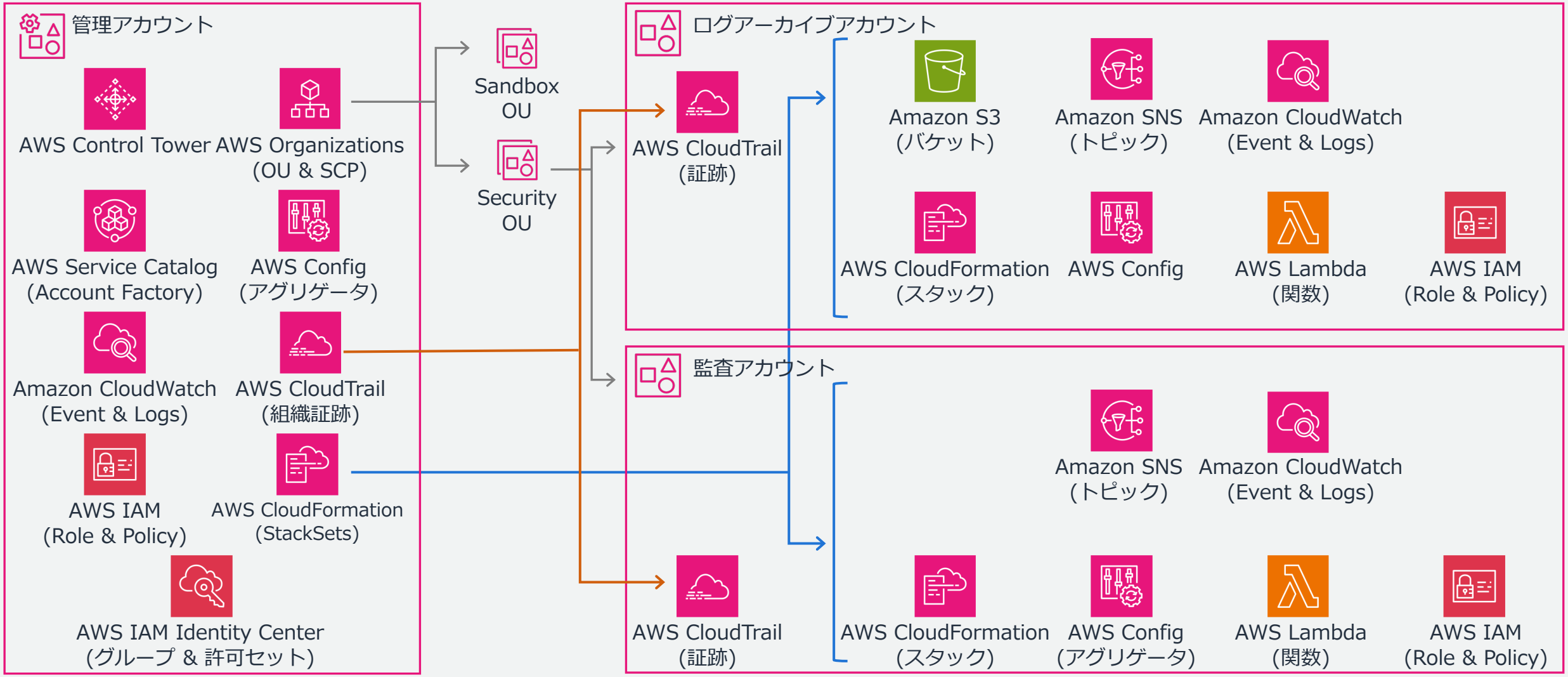
いつ、どのアカウントでリソース作成が行われるか

	管理アカウント	**監査アカウント**	**ログアーカイブアカウント**	**メンバーアカウント**
ランディングゾーンセットアップ	リソース作成あり	リソース作成あり	リソース作成あり	AWS CloudTrail 証跡が作成される
Account Factory でアカウント作成	リソース作成なし	リソース作成なし	リソース作成なし	リソース作成あり
AWS Control Tower への登録	リソース作成なし	リソース作成なし	リソース作成なし	リソース作成あり

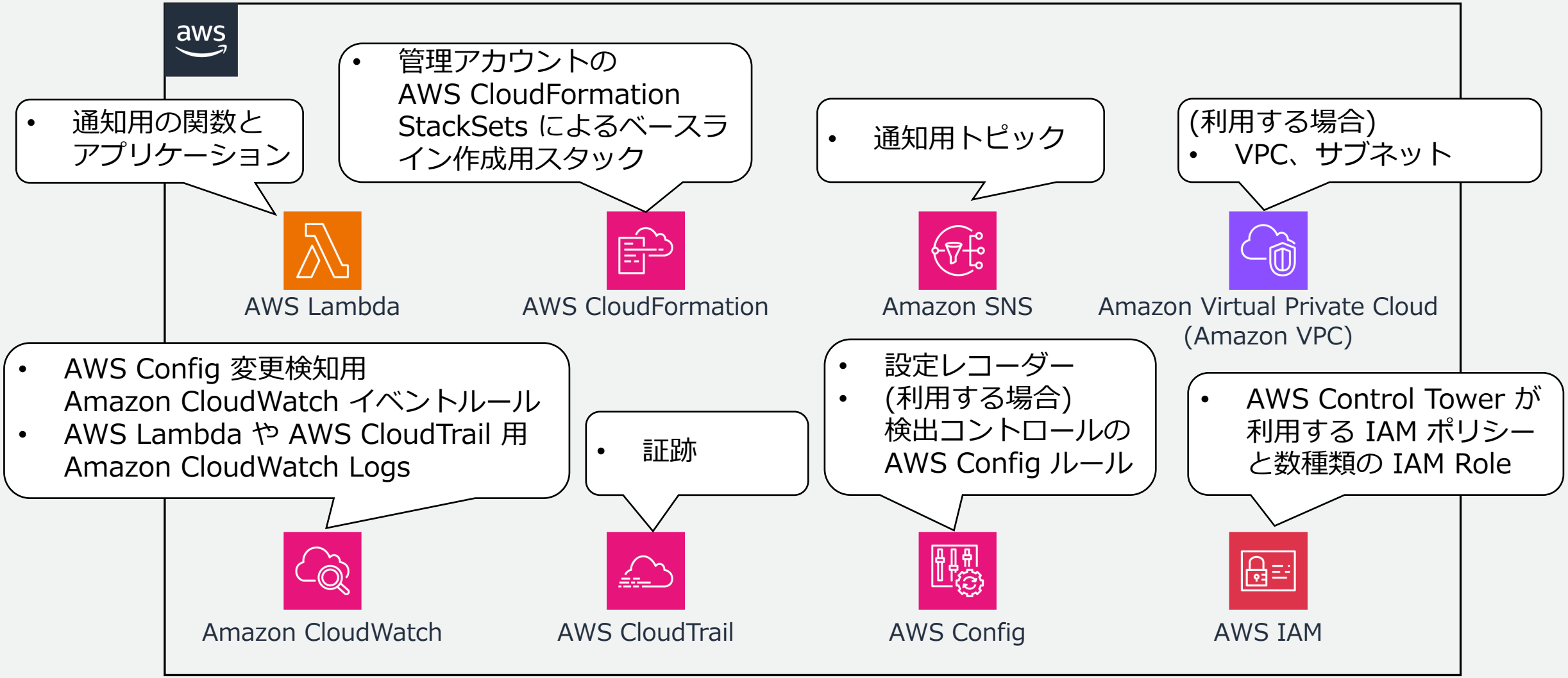
ランディングゾーンセットアップによるメンバーアカウントへの変化は
AWS CloudTrail 証跡が作成されること

Account Factory でアカウント作成もしくは AWS Control Tower への登録によって
AWS Control Tower 管理対象となった時点でメンバーアカウントにリソース作成される

AWS Control Tower の有効化で作成されるリソース



メンバーアカウントで作成される AWS リソース



https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/account-factory-considerations.html

AWS Control Tower 機能紹介

紹介する機能

1. ランディングゾーン
2. コントロール
3. Account Factory
4. 組織
5. ダッシュボード

ランディングゾーン

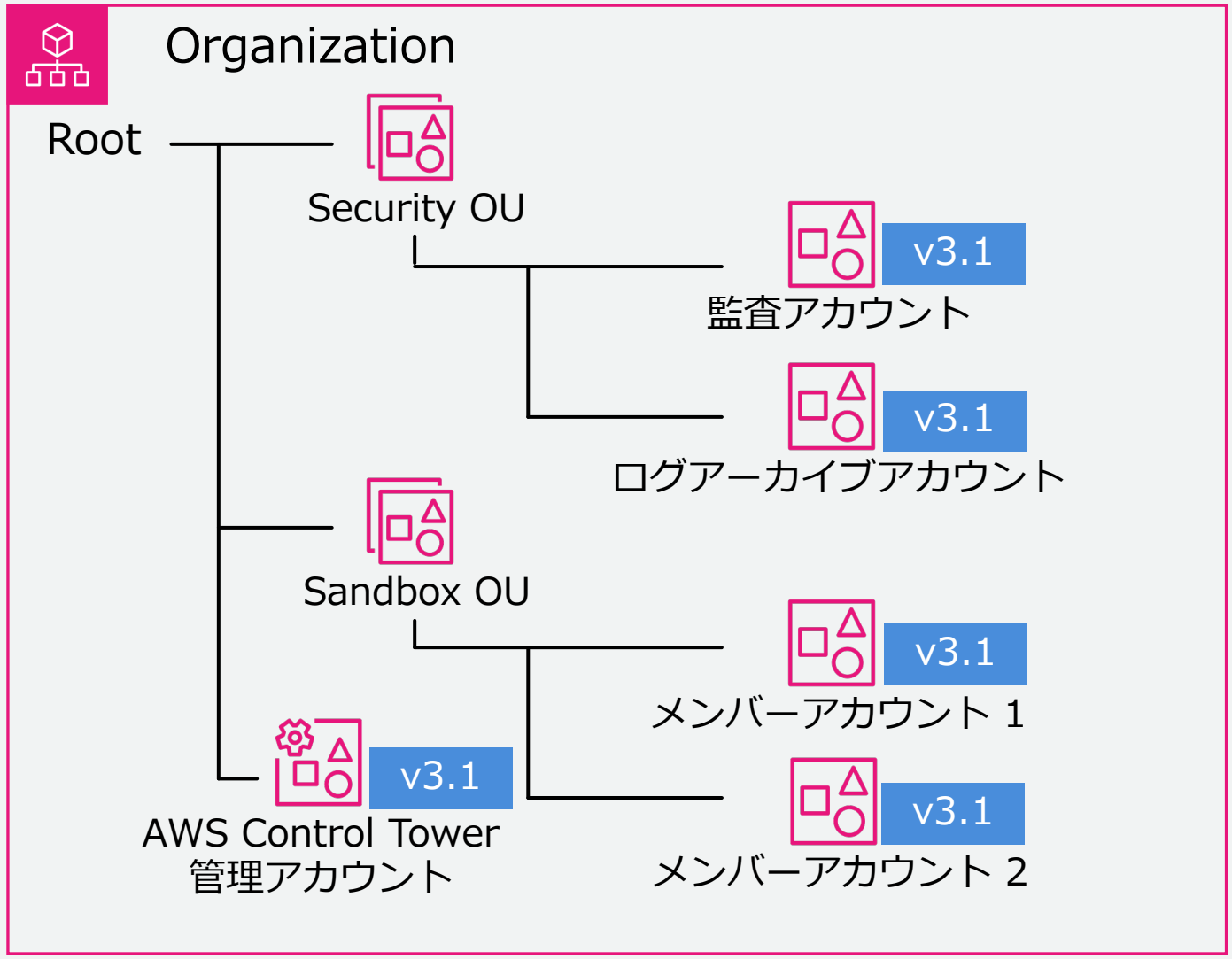
ランディングゾーン設定の項目

- 現在のバージョン
- AWS KMS キーの暗号化
- AWS CloudTrail
- ホームリージョン
- ランディングゾーンリージョン
- AWS IAM Identity Center
- バージョンステータス
- リージョン拒否コントロール

ランディングゾーン設定の項目

- 現在のバージョン
- AWS KMS キーの暗号化
- AWS CloudTrail
- ホームリージョン
- ランディングゾーンリージョン
- AWS IAM Identity Center
- バージョンステータス
- リージョン拒否コントロール

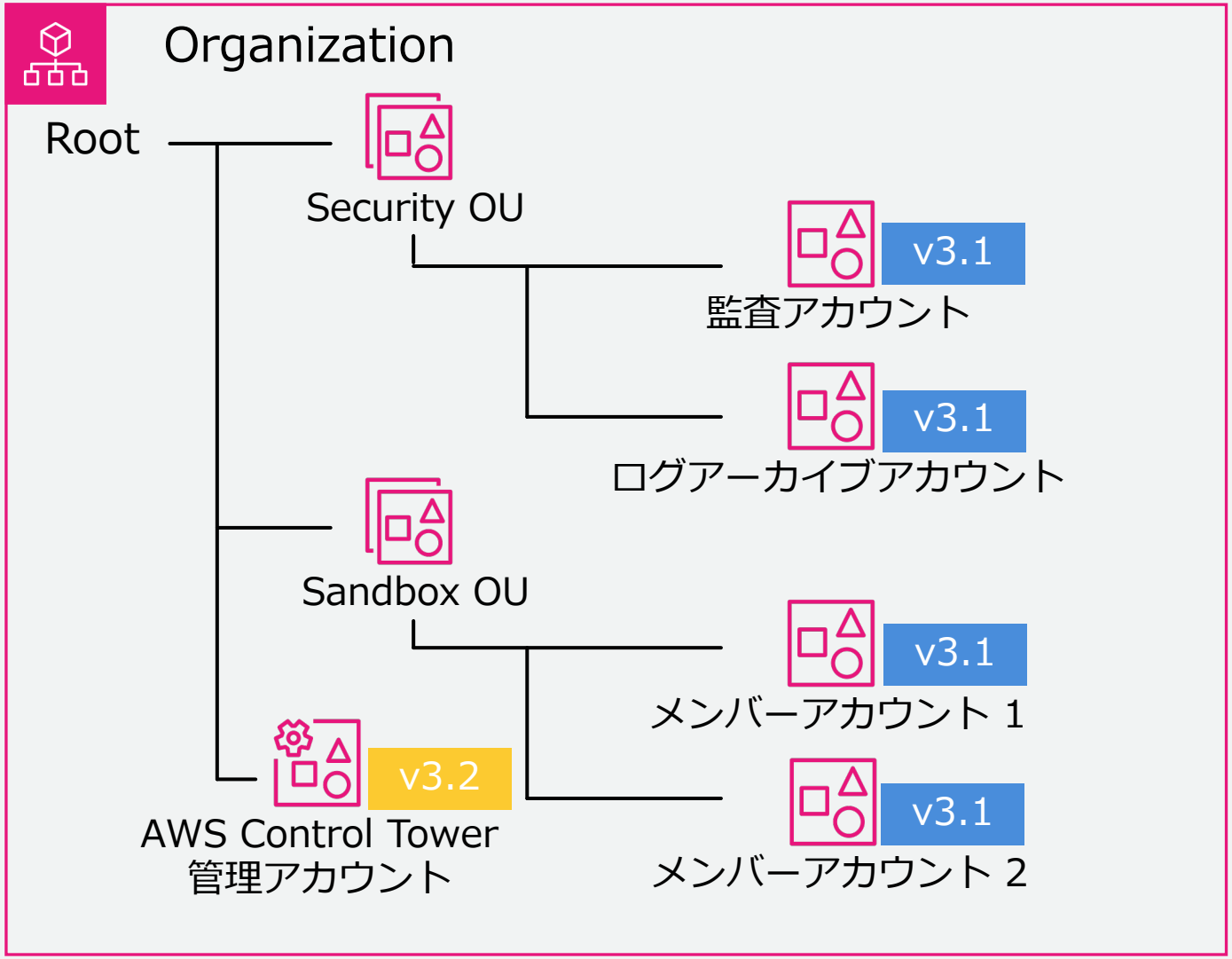
ランディングゾーン バージョン



- ランディングゾーンは
  バージョンがある
  - AWS Control Tower 管理アカウント
  - 各アカウント
- 新しいバージョンが
  リリースされた場合には
  更新を推奨
  - バージョンステータスで状態を把握できる

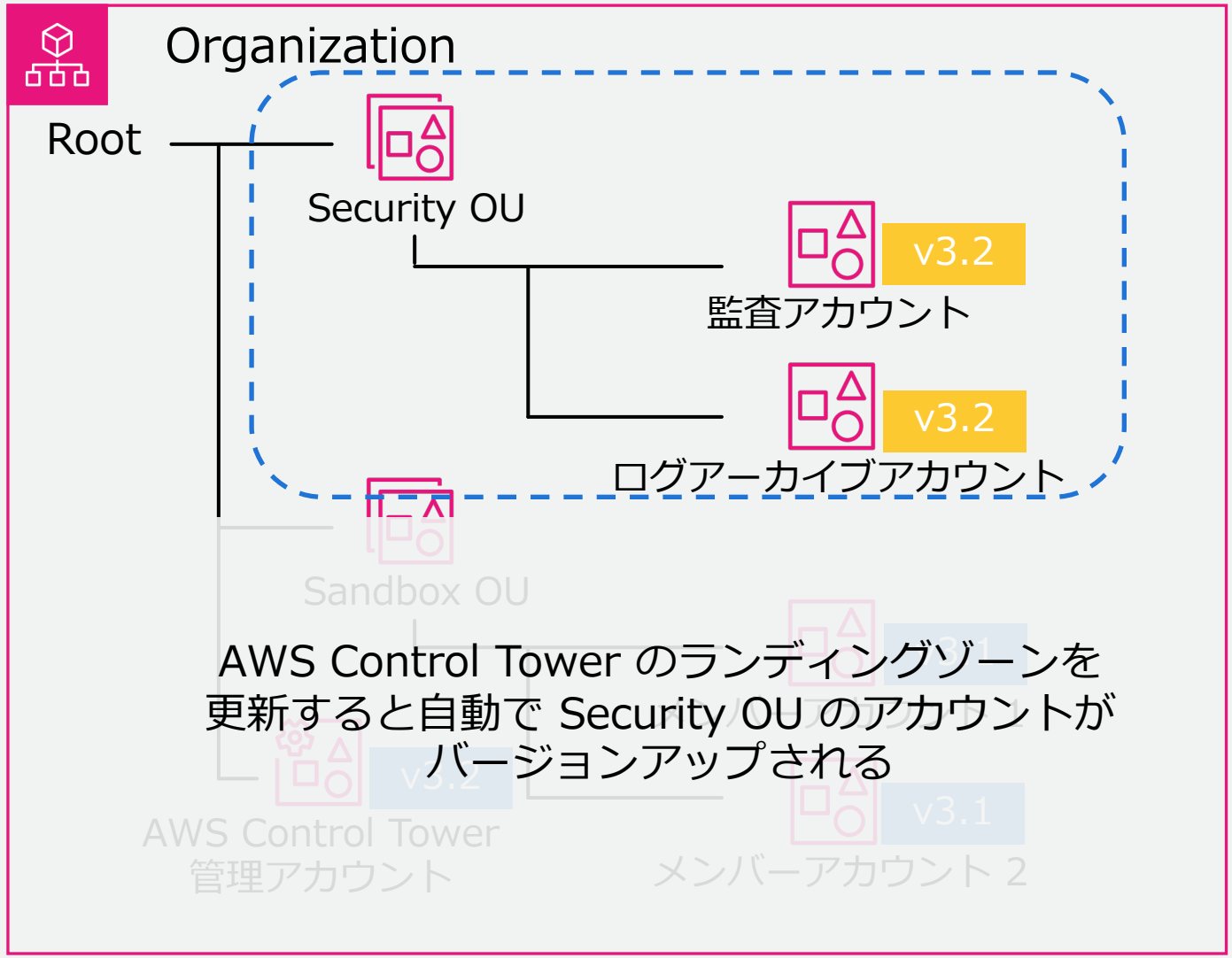
https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/configuration-updates.html

ランディングゾーン バージョン更新



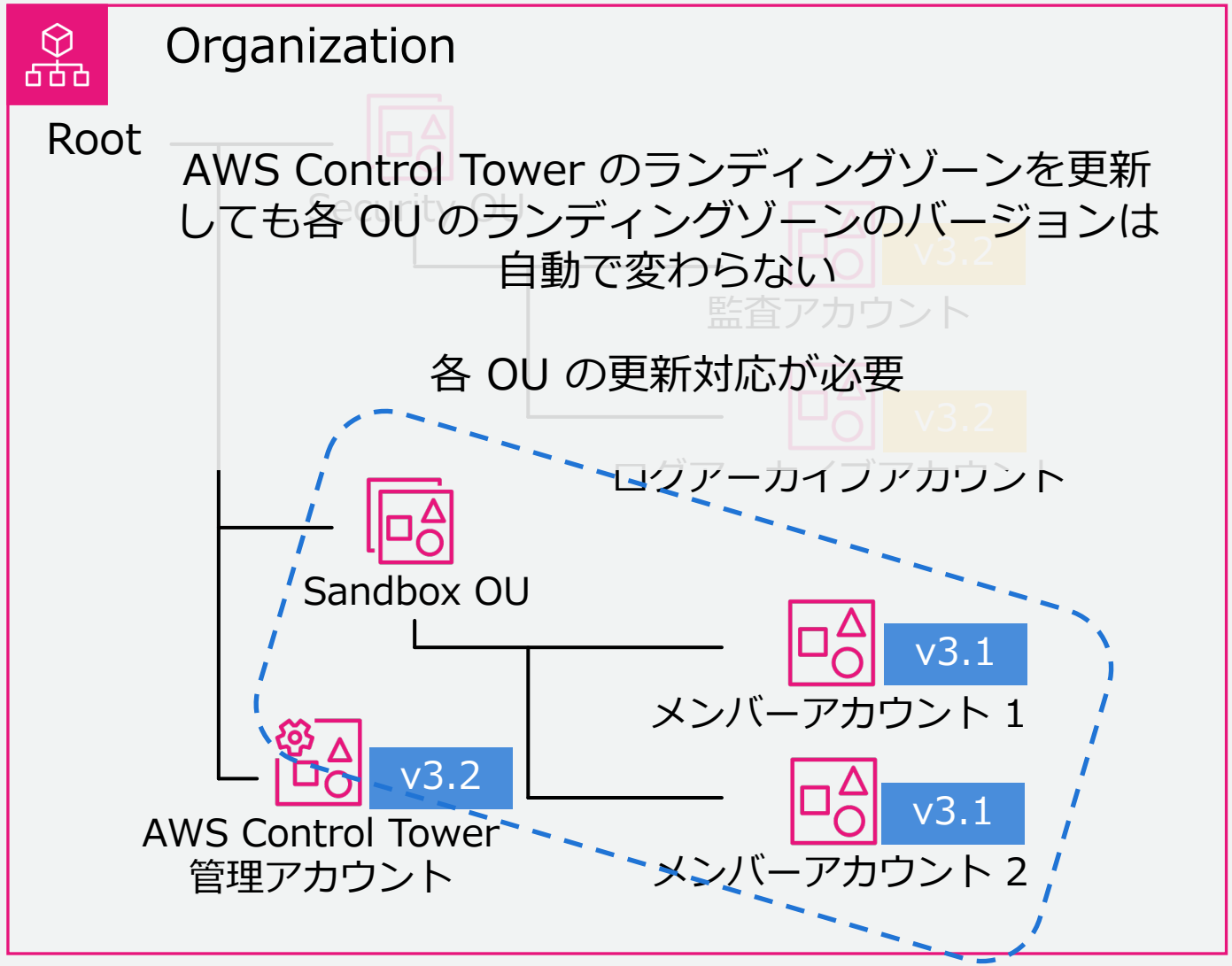
- AWS Control Tower のランディングゾーンを更新後、OU もしくはアカウントのバージョンを更新
- Security OU 配下のアカウントは自動更新

ランディングゾーン バージョン更新



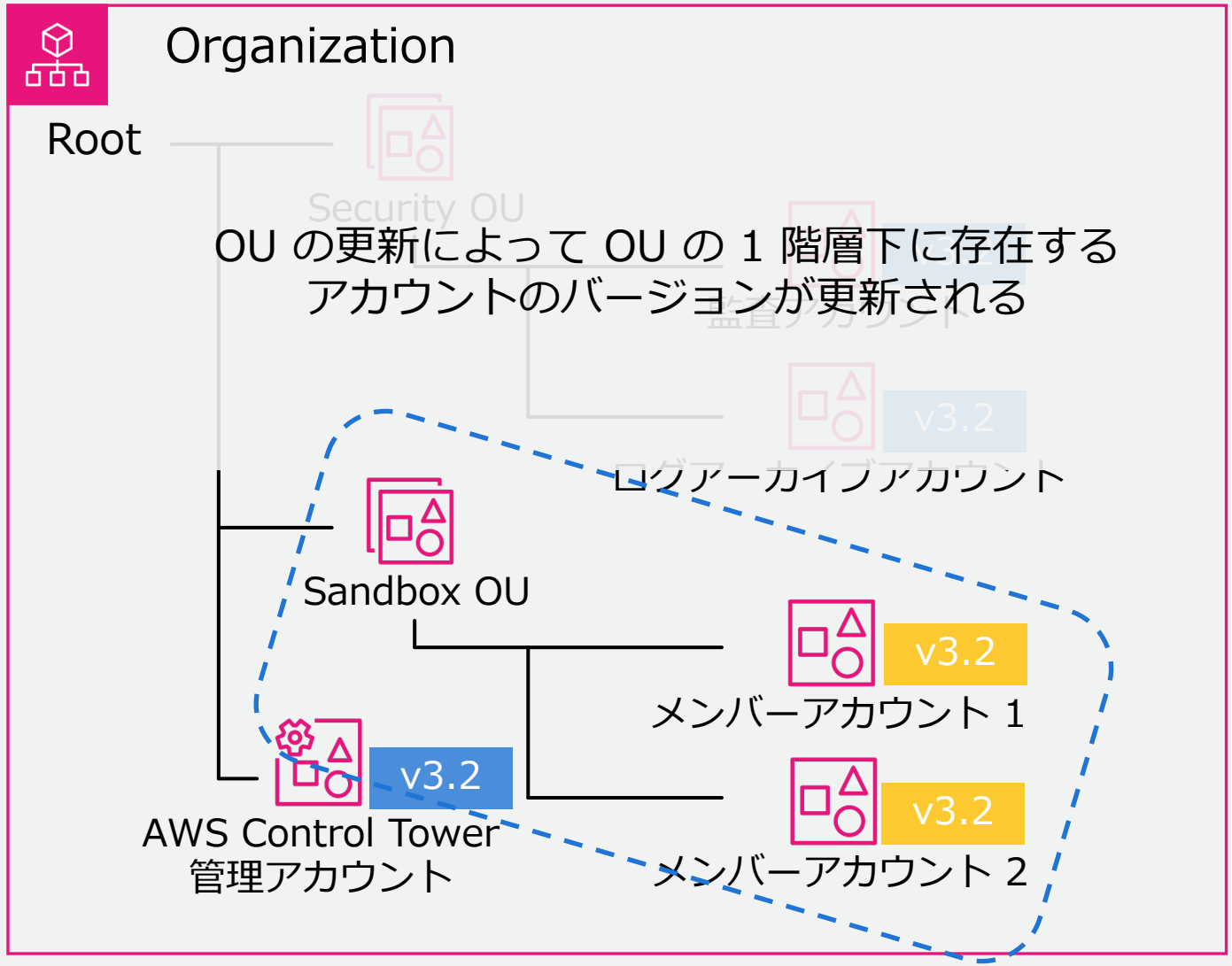
- AWS Control Tower のランディングゾーンを更新後、OU もしくはアカウントのバージョンを更新
- Security OU 配下のアカウントは自動更新

ランディングゾーン バージョン更新



- AWS Control Tower のランディングゾーンを更新後、OU もしくはアカウントのバージョンを更新
- Security OU 配下のアカウントは自動更新

ランディングゾーン バージョン更新



- AWS Control Tower のランディングゾーンを更新後、OU もしくはアカウントのバージョンを更新
- Security OU 配下のアカウントは自動更新

ランディングゾーン設定の項目

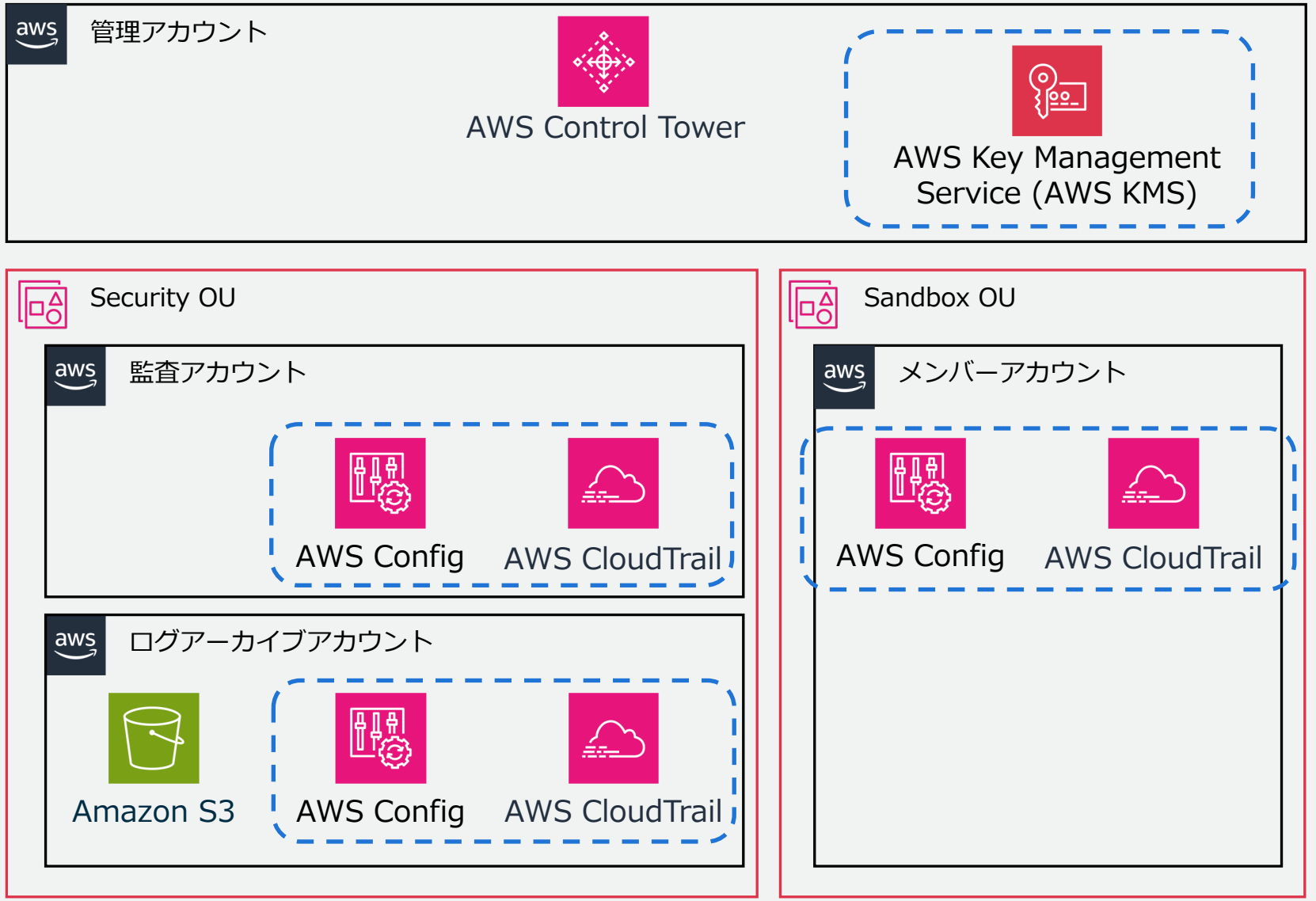
- 現在のバージョン
- AWS KMS キーの暗号化
- AWS CloudTrail
- ホームリージョン
- ランディングゾーンリージョン
- AWS IAM Identity Center
- バージョンステータス
- リージョン拒否コントロール

ランディングゾーン AWS KMS キー

オプション
暗号化設定を有効にして、
カスタマイズする

管理アカウントで
AWS KMS の CMK を作成しランディングゾーンで設定する

AWS CloudTrail と
AWS Config に暗号化を適用してログアーカイブアカウントに保存する



ランディングゾーン設定の項目

- 現在のバージョン
- AWS KMS キーの暗号化
- AWS CloudTrail
- ホームリージョン
- ランディングゾーンリージョン
- AWS IAM Identity Center
- バージョンステータス
- リージョン拒否コントロール

ランディングゾーン AWS CloudTrail

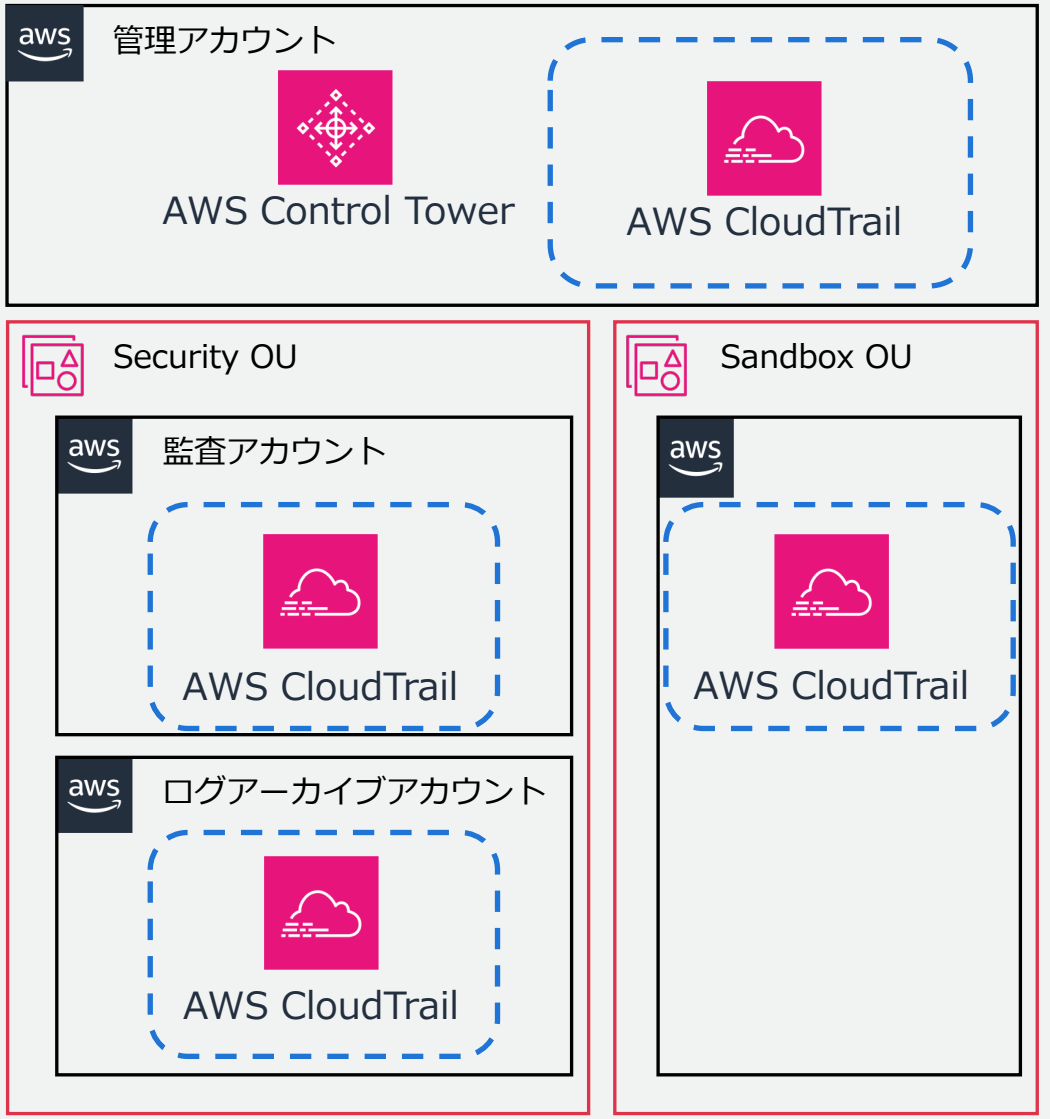
2つの方法から選択

1. AWS CloudTrail の組織証跡を有効化する
2. 有効化しない

1 が推奨

1 は組織証跡が有効化され、ログアーカイブアカウントに保存される

2 は組織証跡が無効なため、別の証跡を作成する必要がある



ランディングゾーン設定の項目

- 現在のバージョン
- AWS KMS キーの暗号化
- AWS CloudTrail
- ホームリージョン
- ランディングゾーンリージョン
- AWS IAM Identity Center
- バージョンステータス
- リージョン拒否コントロール

ランディングゾーン リージョン

- ホームリージョン
  - 1 つのリージョンのみ設定可能
  - AWS Control Tower を有効化するリージョン
  - AWS IAM Identity Center や AWS Organizations を利用するリージョン

- ランディングゾーンリージョン
  - AWS Control Tower の管理対象でランディングゾーンを設定するリージョン
  - AWS Control Tower によって AWS リソースが生成される
  - 追加することも削除することも可能

ランディングゾーン設定の項目

- 現在のバージョン
- AWS KMS キーの暗号化
- AWS CloudTrail
- ホームリージョン
- ランディングゾーンリージョン
- AWS IAM Identity Center
- バージョンステータス
- リージョン拒否コントロール

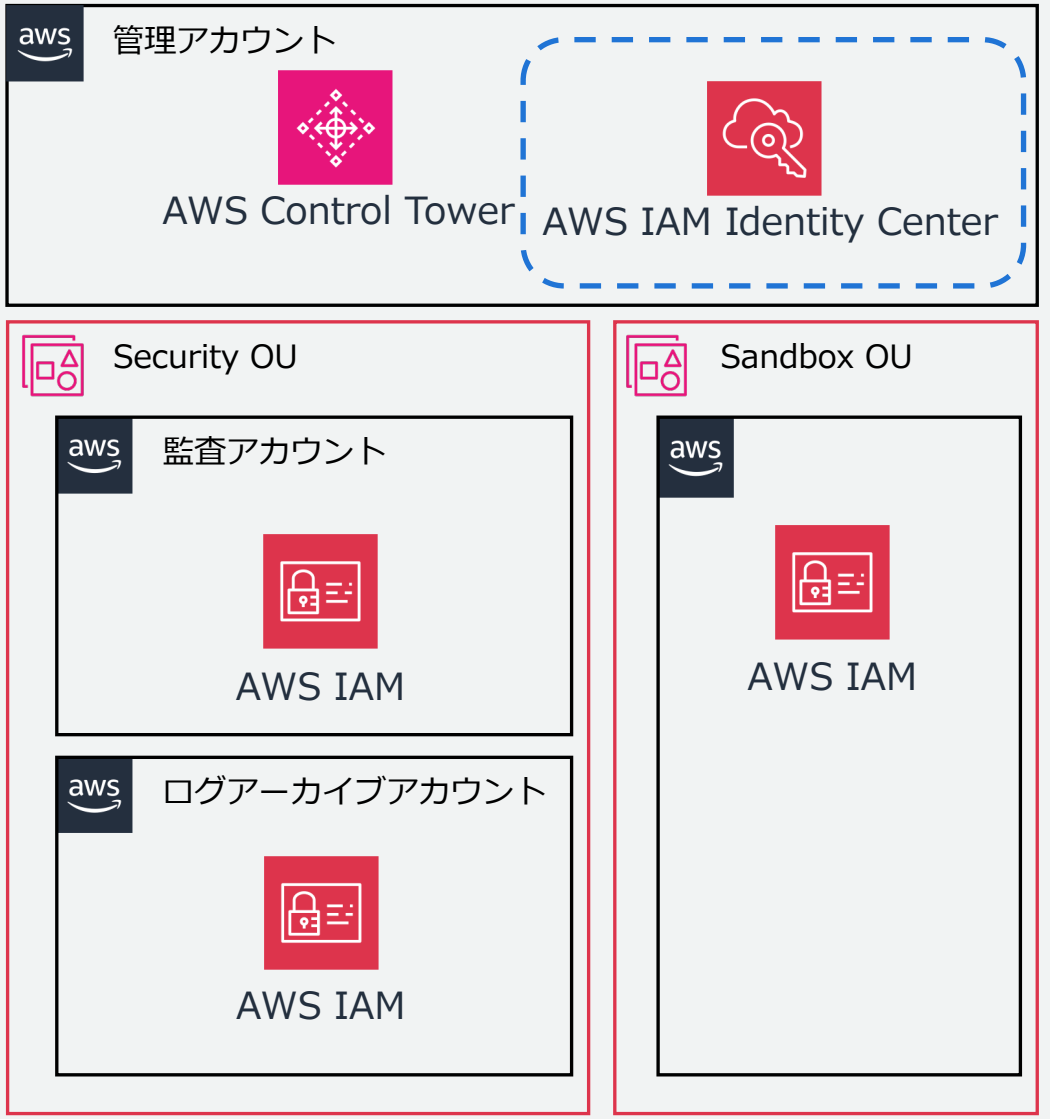
ランディングゾーン AWS IAM Identity Center

2つの方法から選択

1. AWS Control Tower は AWS IAM Identity Center を使用して AWS アカウントアクセスを設定します
2. AWS IAM Identity Center またはその他の方法によるセルフマネージド型 AWS アカウントアクセス

1 は AWS IAM Identity Center のグループと権限セットが作成される

2 は何も作成されない

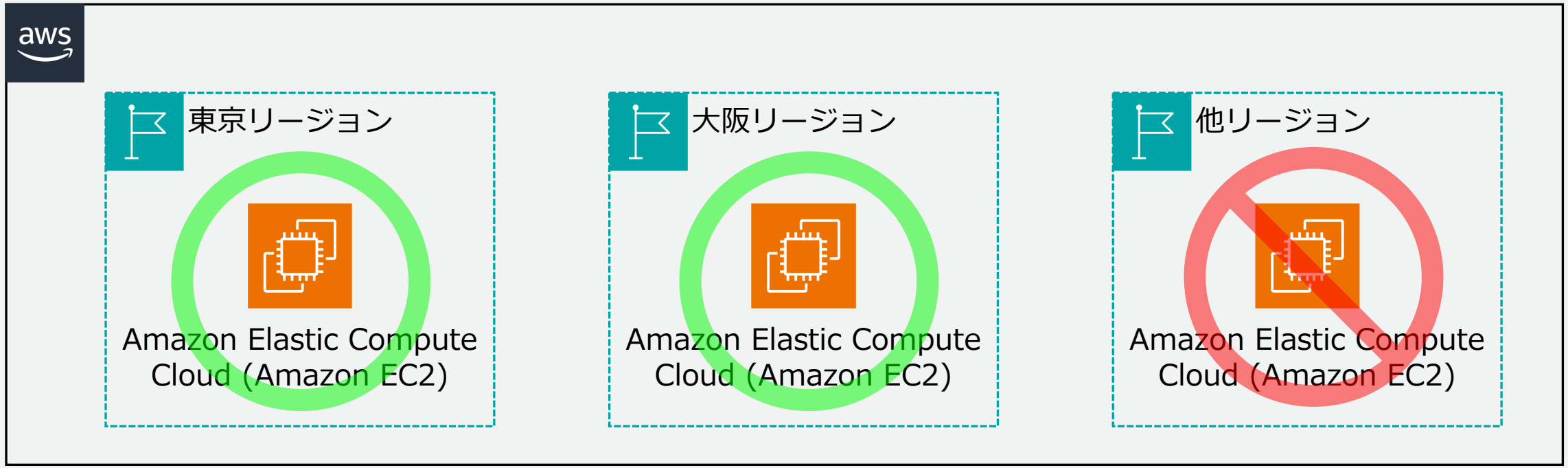


ランディングゾーン設定の項目

- 現在のバージョン
- AWS KMS キーの暗号化
- AWS CloudTrail
- ホームリージョン
- ランディングゾーンリージョン
- AWS IAM Identity Center
- バージョンステータス
- リージョン拒否コントロール

ランディングゾーン リージョン拒否コントロール

- AWS Control Tower のランディングゾーンリージョンに含まれないリージョンの利用を禁止
  - AWS Control Tower で登録されている OU に対して SCP を適用



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

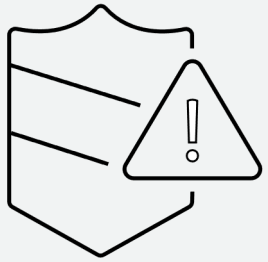
コントロール

コントロール

様々な項目による包括的なガイダンス

サービス	名前	統制目標	動作	フレームワーク	ガイダンス
AWS CloudFormation	[CT.CLOUDFORMATION.PR.1] AWS CloudFormation レジストリ内のリソースタイプ、モジュール、フックの管理を禁止する	設定を保護	予防	NIST 800-53 Rev 5 PCI DSS version 3.2.1	選択的
AWS Identity and Access Management (IAM)	[AWS-GR_ROOT_ACCOUNT_MFA_ENABLED] ルートユーザーの MFA が有効になっているかどうかを検出する	最小特権を強制	検出	CIS AWS Benchmark 1.4 NIST 800-53 Rev 5 PCI DSS version 3.2.1	強く推奨
Amazon S3	[AWS-GR_AUDIT_BUCKET_DELETION_PROHIBITED] ログアーカイブの削除を許可しない	データの完全性を保護	予防	NIST 800-53 Rev 5 PCI DSS version 3.2.1	必須
AWS Lambda	[CT.LAMBDA.PR.3] AWS Lambda 関数がカスタマーマネージド Amazon Virtual Private Cloud (VPC) に配置されていることを要求する	ネットワークアクセスを制限	プロアクティブ	NIST 800-53 Rev 5 PCI DSS version 3.2.1	選択的
Amazon Kinesis	[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	保管中のデータを暗号化	検出	NIST 800-53 Rev 5 PCI DSS version 3.2.1	選択的

コントロールのタイプ

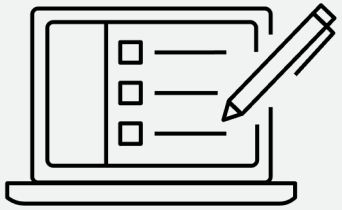


予防

サービスコントロール
ポリシー (SCP)

検出

AWS Config ルール

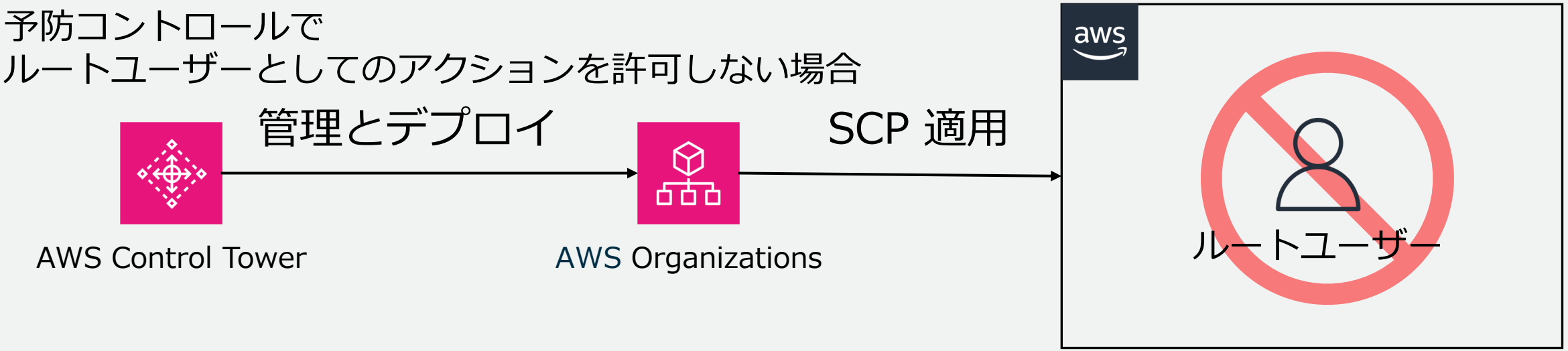


プロアクティブ

AWS CloudFormation
Hooks

予防コントロール

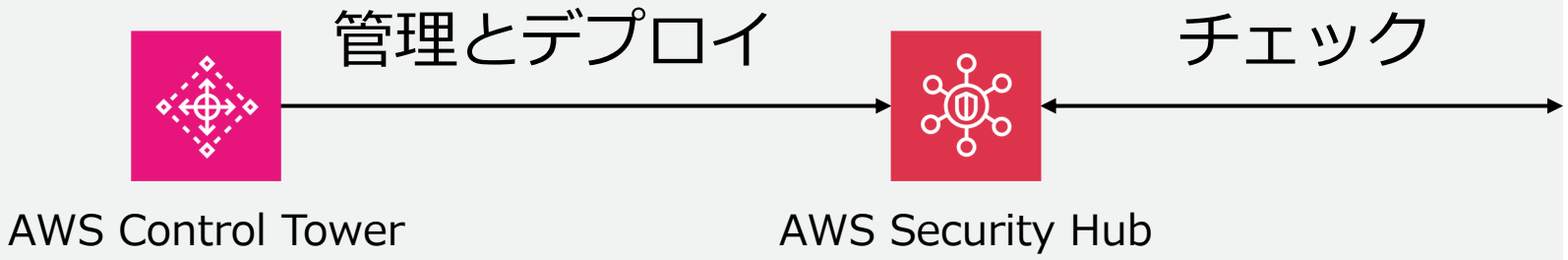
- AWS Organizations の SCP を利用したコントロール
  - ポリシー違反につながるアクションを禁止するため、アカウントはコンプライアンスを維持できる
  - すべての AWS リージョンで適用される

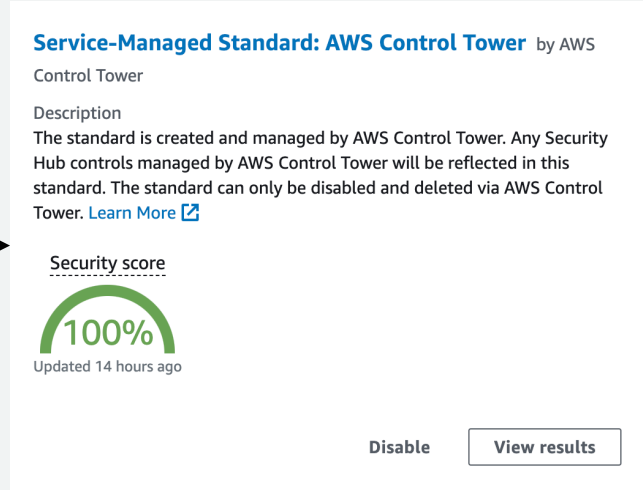


検出コントロール

- AWS Config を利用したコントロール
  - AWS Control Tower 管理下のアカウント内リソースの準拠状態を検出し、非準拠の場合はダッシュボードを通じてアラートを提供する
  - AWS Control Tower ランディングゾーンリージョンに適用される
  - コントロールオーナーは AWS Control Tower と AWS Security Hub の 2 種類

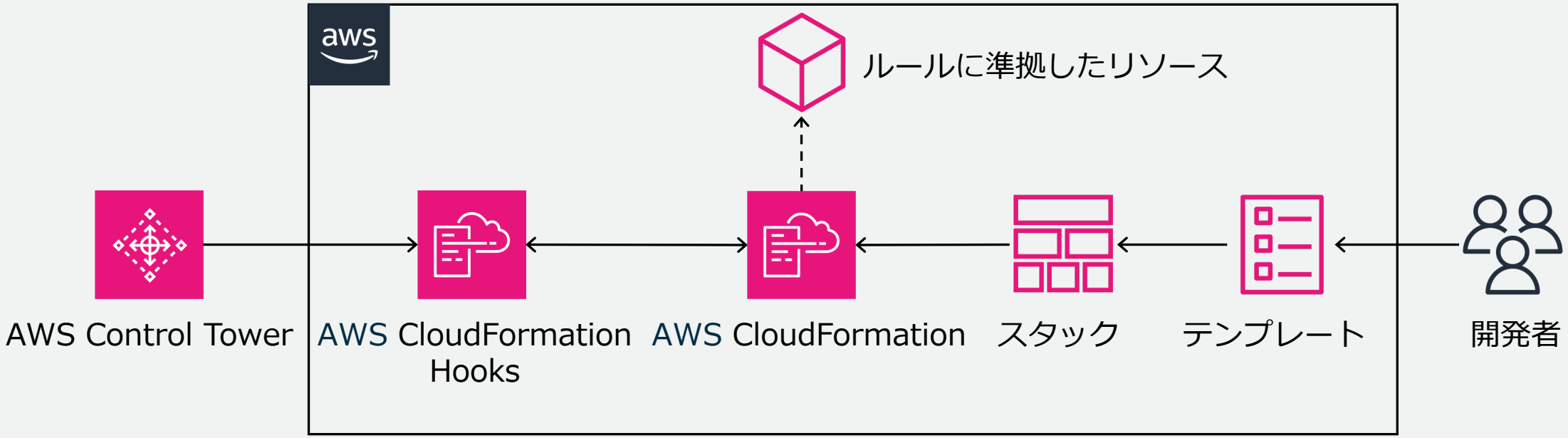
コントロールオーナーが AWS Security Hub の
検出コントロールを有効化した場合



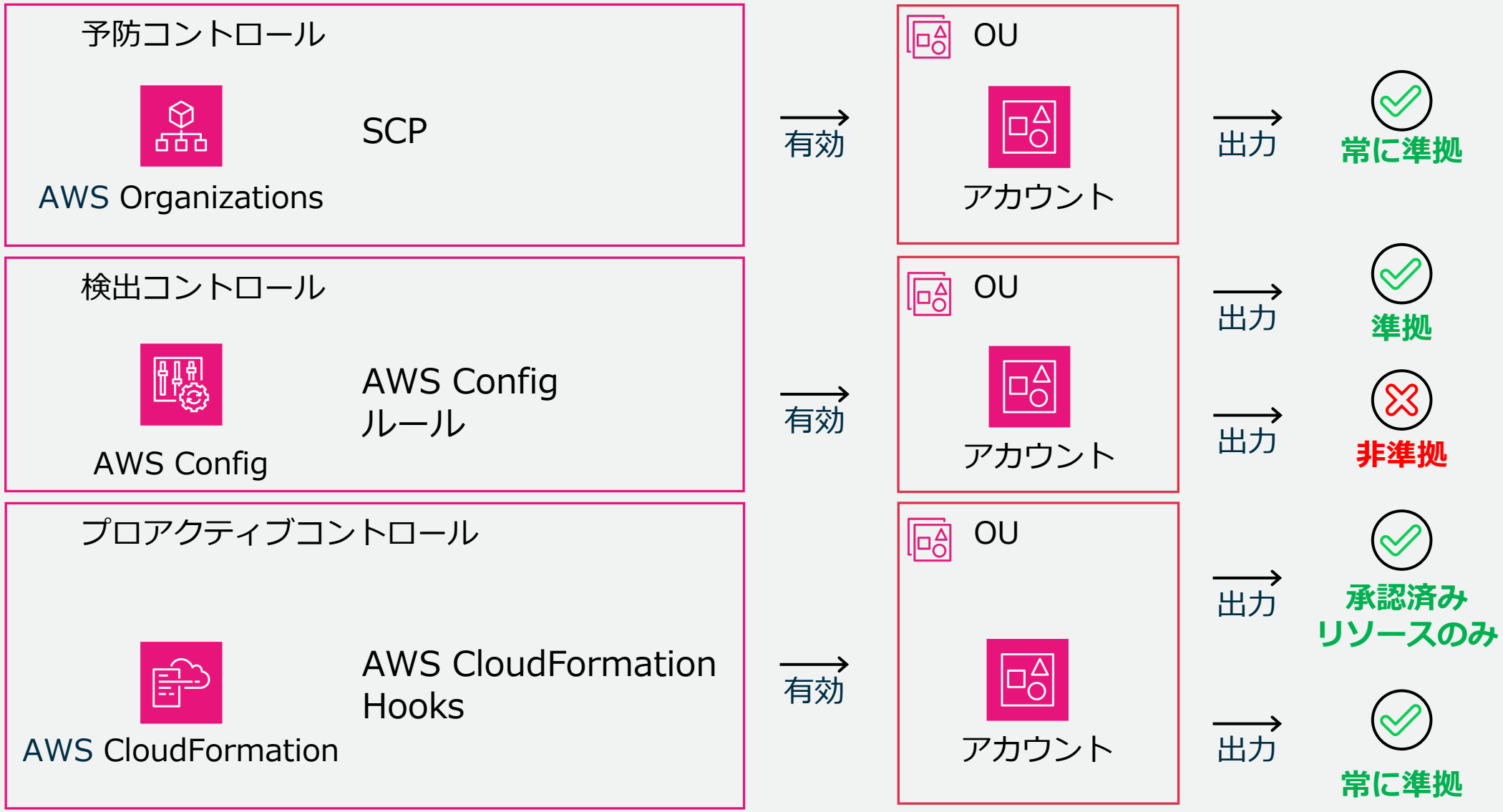


プロアクティブコントロール

- AWS CloudFormation Hooks を利用したコントロール
  - プロビジョニング前にリソースをスキャンし準拠状態を確認し、非準拠の場合はリソースがプロビジョニングされない
  - AWS CloudFormation でプロビジョニングするリソースに適用される



コントロールの制御動作



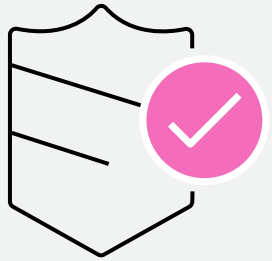
再掲

コントロール

様々な項目による包括的なガイダンス

サービス	名前	統制目標	動作	フレームワーク	ガイダンス
AWS CloudFormation	[CT.CLOUDFORMATION.PR.1] AWS CloudFormation レジストリ内のリソースタイプ、モジュール、フックの管理を禁止する	設定を保護	予防	NIST 800-53 Rev 5 PCI DSS version 3.2.1	選択的
AWS Identity and Access Management (IAM)	[AWS-GR_ROOT_ACCOUNT_MFA_ENABLED] ルートユーザーの MFA が有効になっているかどうかを検出する	最小特権を強制	検出	CIS AWS Benchmark 1.4 NIST 800-53 Rev 5 PCI DSS version 3.2.1	強く推奨
Amazon S3	[AWS-GR_AUDIT_BUCKET_DELETION_PROHIBITED] ログアーカイブの削除を許可しない	データの完全性を保護	予防	NIST 800-53 Rev 5 PCI DSS version 3.2.1	必須
AWS Lambda	[CT.LAMBDA.PR.3] AWS Lambda 関数がカスタマーマネージド Amazon Virtual Private Cloud (VPC) に配置されていることを要求する	ネットワークアクセスを制限	プロアクティブ	NIST 800-53 Rev 5 PCI DSS version 3.2.1	選択的
Amazon Kinesis	[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	保管中のデータを暗号化	検出	NIST 800-53 Rev 5 PCI DSS version 3.2.1	選択的

コントロールのガイダンス

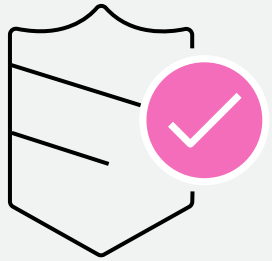


必須

強く推奨

選択的

必須コントロール



必須

- AWS Control Tower の
  ランディングゾーンを保護するための設定
- お客様のワークロードに
  影響を与えるものではない

必須コントロール一覧

名前	動作
AWS Control Tower がログアーカイブに作成した Amazon S3 バケットの暗号化設定の変更を許可しない	予防
AWS Control Tower がログアーカイブに作成した Amazon S3 バケットのログ設定の変更を許可しない	予防
AWS Control Tower がログアーカイブに作成した Amazon S3 バケットのバケットポリシーの変更を許可しない	予防
AWS Control Tower がログアーカイブに作成した 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	予防
AWS Control Tower によって設定された Amazon CloudWatch Logs ロググループへの変更を不許可にする	予防
ログアーカイブの削除を禁止する	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	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	検出
CloudTrail への設定変更を不許可にする	予防
AWS Config への設定変更を許可しない	予防
AWS Control Tower によって設定された AWS Config ルール への変更を許可しない	予防
AWS Control Tower が作成した AWS Config 集約認証の削除を許可しない	予防
AWS Control Tower が作成した リソースのタグの変更を許可しない	予防
AWS Control Tower によって設定された Amazon CloudWatch への変更を不許可にする	予防
AWS Control Tower と AWS CloudFormation によって設定された AWS IAM ロールへの変更を不許可にする	予防
AWS Control Tower によって設定された AWS Lambda 関数の変更を許可しない	予防
AWS Control Tower によって設定された Amazon SNS への変更を不許可にする	予防
AWS Control Tower によって設定された Amazon SNS サブスクリプションへの変更を不許可にする	予防
セキュリティ組織単位の共有アカウントで AWS CloudTrail または CloudTrail Lake が有効になっているかどうかを検出する	検出

必須コントロール一覧

名前		動作
AWS Control Tower がログアーカイブに作成した Amazon S3 バケットの暗号化設定の変更を許可しない		予防
AWS Control Tower がログアーカイブに作成した Amazon S3 バケットのログ設定の変更を許可しない		予防
AWS Control Tower がログアーカイブに作成した Amazon S3 バケットのバケットポリシーの変更を許可しない		予防
AWS Control Tower がログアーカイブに作成した 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		予防
AWS Control Tower によって設定された Amazon CloudWatch Logs ロググループへの変更を不許可にする		予防
ログアーカイブの削除を禁止する	aws-controltower* が対象	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	検出コントロール	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	検出コントロール	検出
CloudTrail への設定変更を不許可にする	aws-controltower-* が対象	予防
AWS Config への設定変更を許可しない	設定レコーダーは各リージョンに1つだけ	予防
AWS Control Tower によって設定された AWS Config ルール への変更を許可しない		予防
AWS Control Tower が作成した AWS Config 集約認証の削除を許可しない		予防
AWS Control Tower が作成した リソースのタグの変更を許可しない		予防
AWS Control Tower によって設定された Amazon CloudWatch への変更を不許可にする		予防
AWS Control Tower と AWS CloudFormation によって設定された AWS IAM ロールへの変更を不許可にする		予防
AWS Control Tower によって設定された AWS Lambda 関数の変更を許可しない		予防
AWS Control Tower によって設定された Amazon SNS への変更を不許可にする		予防
AWS Control Tower によって設定された Amazon SNS サブスク	検出コントロール	予防
セキュリティ組織単位の共有アカウントで AWS CloudTrail または CloudTrail Lake が有効になっているかどうかを検出する		検出

再掲

コントロール

様々な項目による包括的なガイダンス

サービス	名前	統制目標	動作	フレームワーク	ガイダンス
AWS CloudFormation	[CT.CLOUDFORMATION.PR.1] AWS CloudFormation レジストリ内のリソースタイプ、モジュール、フックの管理を禁止する	設定を保護	予防	NIST 800-53 Rev 5 PCI DSS version 3.2.1	選択的
AWS Identity and Access Management (IAM)	[AWS-GR_ROOT_ACCOUNT_MFA_ENABLED] ルートユーザーの MFA が有効になっているかどうかを検出する	最小特権を強制	検出	CIS AWS Benchmark 1.4 NIST 800-53 Rev 5 PCI DSS version 3.2.1	強く推奨
Amazon S3	[AWS-GR_AUDIT_BUCKET_DELETION_PROHIBITED] ログアーカイブの削除を許可しない	データの完全性を保護	予防	NIST 800-53 Rev 5 PCI DSS version 3.2.1	必須
AWS Lambda	[CT.LAMBDA.PR.3] AWS Lambda 関数がカスタマーマネージド Amazon Virtual Private Cloud (VPC) に配置されていることを要求する	ネットワークアクセスを制限	プロアクティブ	NIST 800-53 Rev 5 PCI DSS version 3.2.1	選択的
Amazon Kinesis	[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	保管中のデータを暗号化	検出	NIST 800-53 Rev 5 PCI DSS version 3.2.1	選択的

コントロールのカテゴリー

統制目標、サービス、フレームワークのカテゴリーを利用して適切なコントロールの検討を簡略化

コントロールの画面

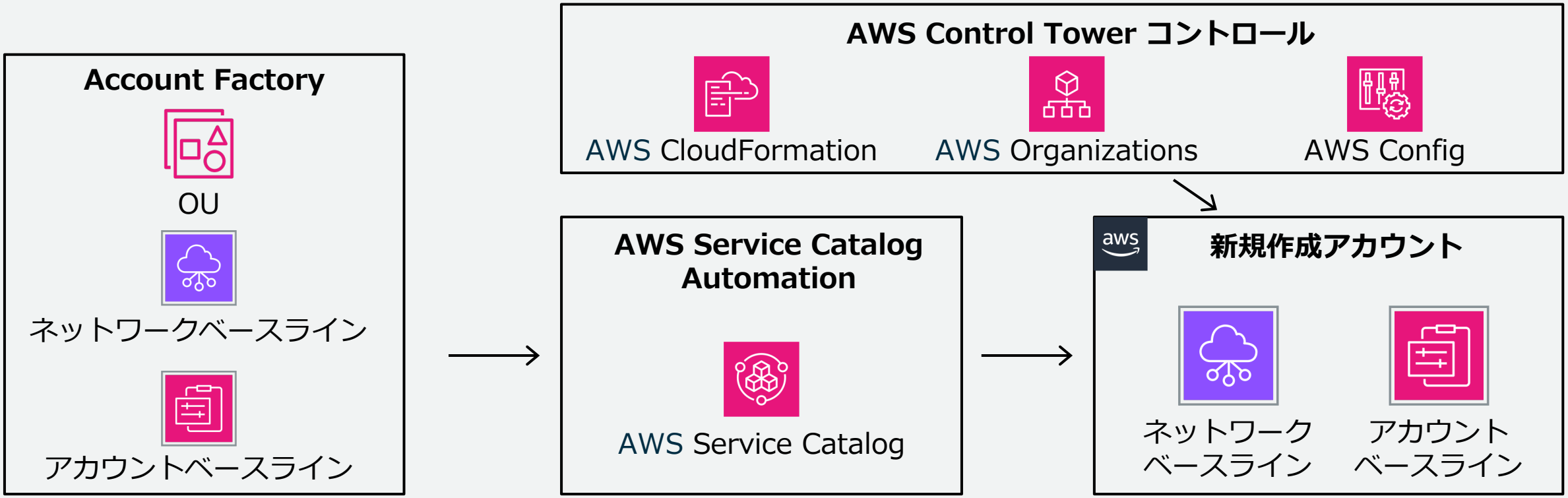
- 統制目標
- サービス
- 動作
- フレームワーク
- ガイダンス
- 関係

適用するコントロールに
依存関係がある場合は事前に適用する

Account Factory

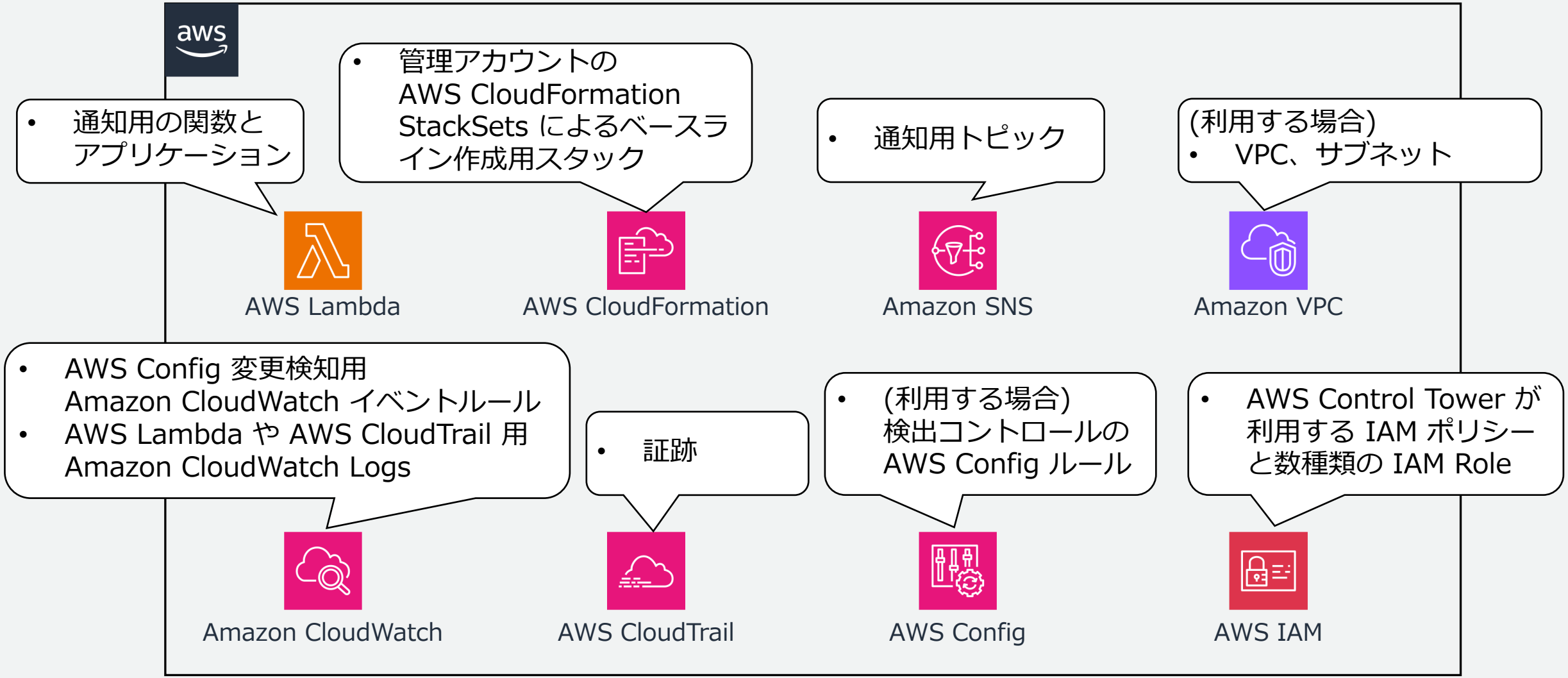
Account Factory

AWS Control Tower のガバナンスの効いた AWS アカウントを作成するための機能
AWS Service Catalog を活用し、Amazon VPC やコントロールが設定されたアカウントをプロビジョニングする



再掲

メンバーアカウントで作成される AWS リソース

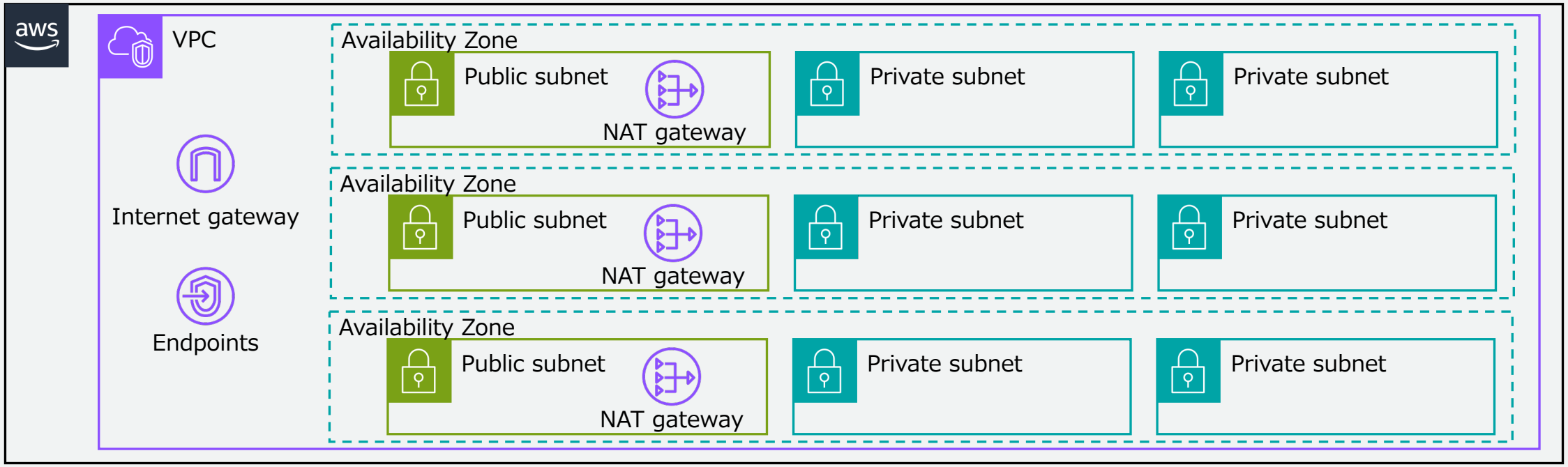


https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/account-factory-considerations.html

VPC 設定により作成されるリソース

インターネットアクセス可能なサブネット、プライベートサブネットの最大数、CIDR、VPC 作成のリージョン
を設定することで新しい VPC が作成される

インターネットアクセス可能なサブネット許可、プライベートサブネットの最大数 2 の場合



https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/vpc-concepts.html

VPC 設定により作成されるリソース 続き

インターネットアクセス可能なサブネット、プライベートサブネットの最大数、CIDR、VPC 作成のリージョン
を設定することで新しい VPC が作成される

インターネットアクセス可能なサブネット不許可、プライベートサブネットの最大数 0 の場合

https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/vpc-concepts.html

AWS Control Tower で作成するアカウントのカスタマイズ

AWS サービス活用

- Account Factory Customization (AFC)
- AWS CloudFormation StackSets (Organizations)

AWS ソリューション活用

- Customizations for AWS Control Tower (CfCT)
- Account Factory for Terraform (AFT)

Account Factory Customization (AFC)

AWS Service Catalog ハブアカウントの作成と IAM Role 作成 (初回のみ実行)

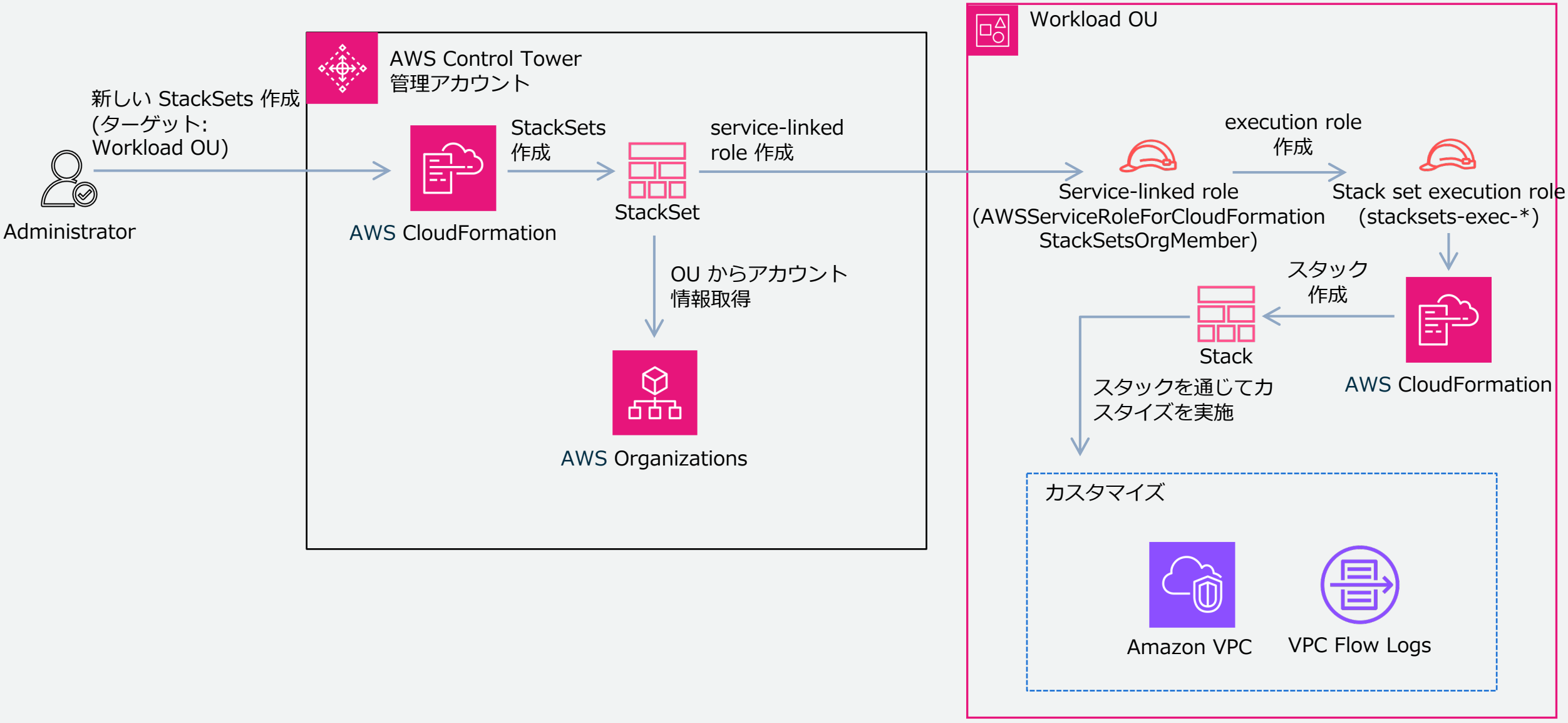
カスタムブループリント作成もしくは AWS パートナーソリューションを利用

AWS Service Catalog のポートフォリオに ブループリントを追加

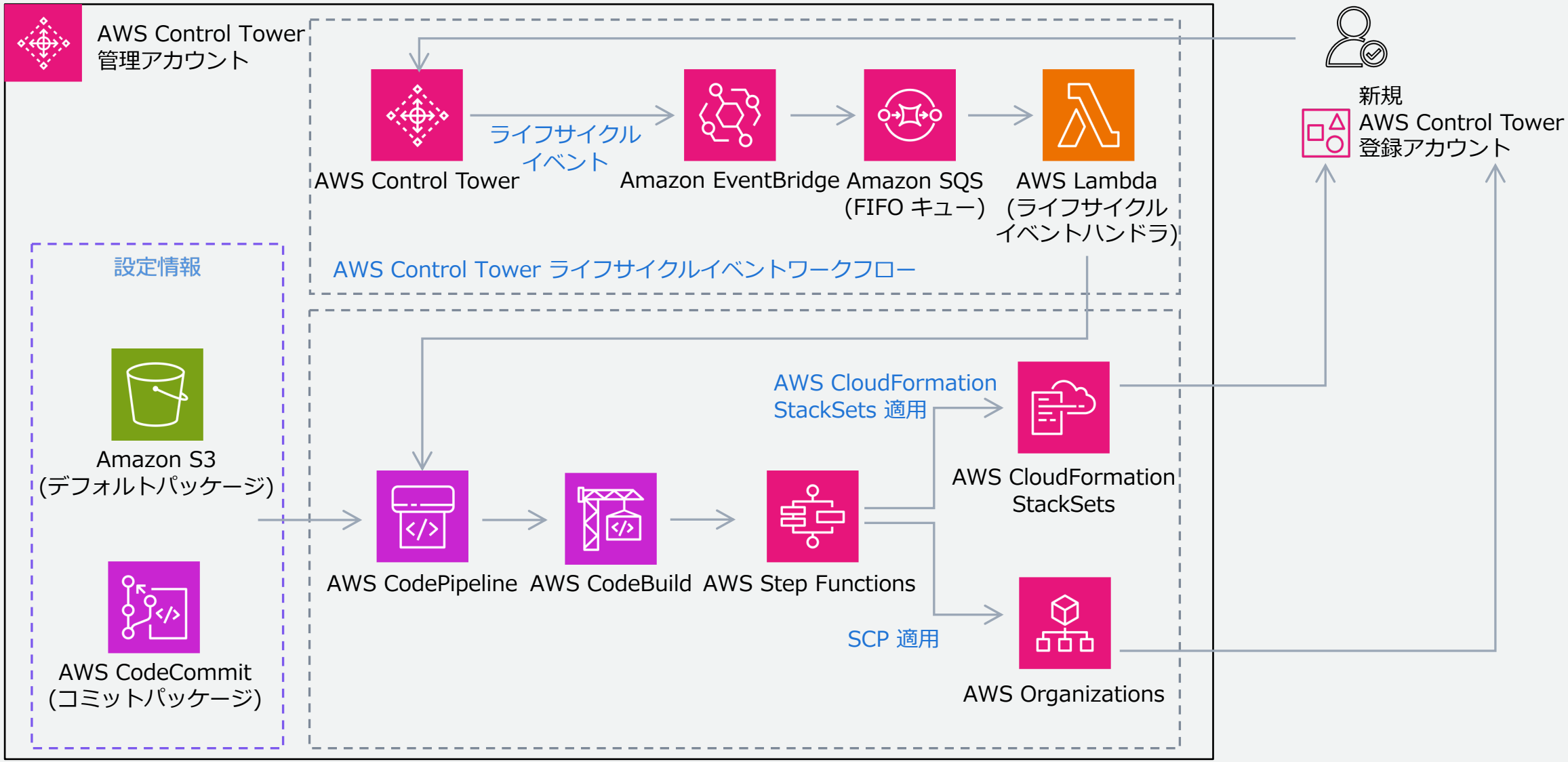
作成時、更新時、登録時にブループリントを選択する

カスタマイズされたアカウント作成

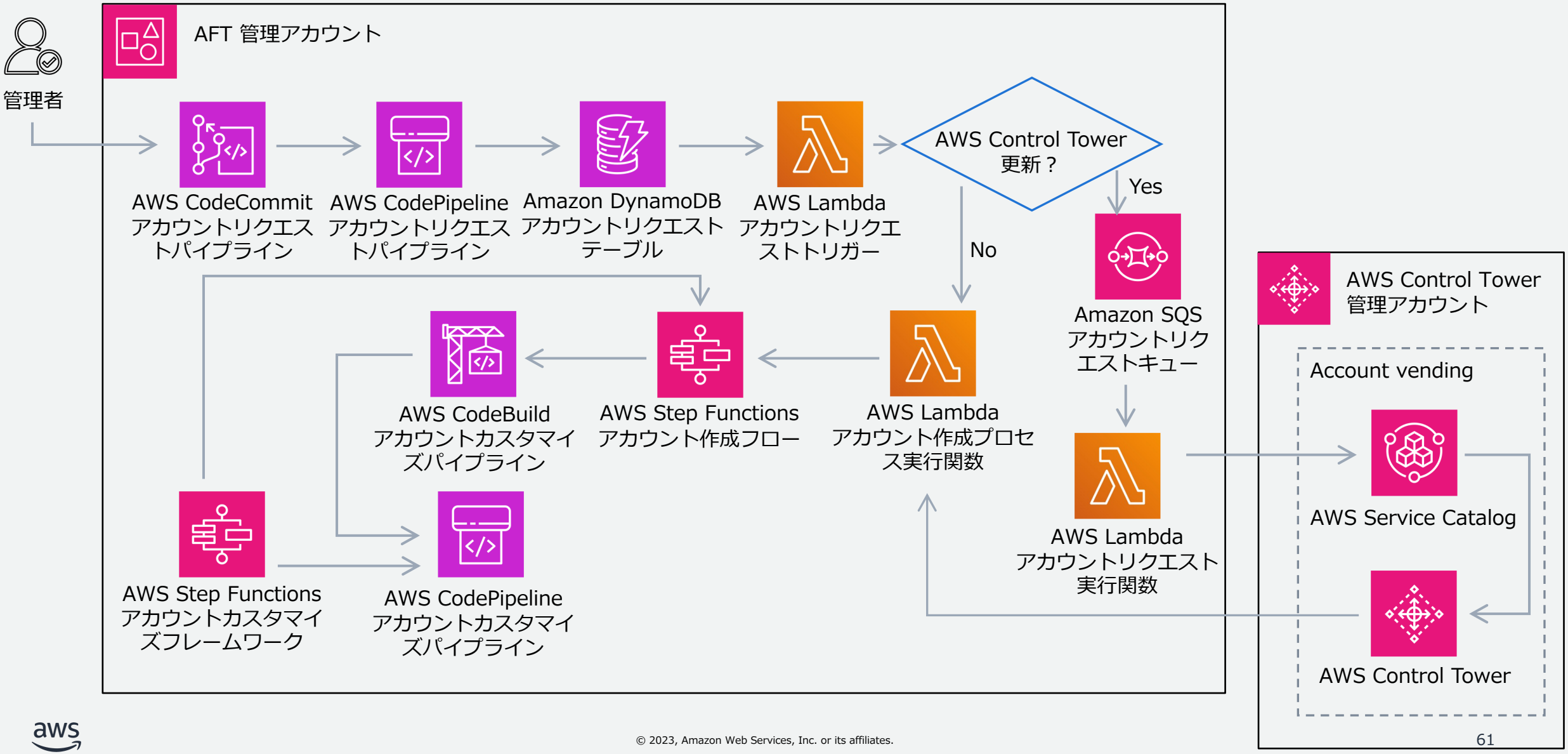
AWS CloudFormation StackSets



Customizations for AWS Control Tower (CfCT)



Account Factory for Terraform (AFT)



カスタマイズ方法の違い

利用する IaC(Infrastructure as Code) やカスタマイズのレベルで選択肢が変わる

名前	マネージドサービス	IaC	SCP設定	複数の設定
Account Factory Customization (AFC)	Yes	AWS CloudFormation Terraform	不可	不可
AWS CloudFormation StackSets	Yes	AWS CloudFormation	不可	可能
Customization for AWS Control Tower (CfCT)	No	AWS CloudFormation	可能	可能
Account Factory for Terraform (AFT)	No	Terraform	可能	可能

組織

再掲

AWS Control Tower の状態

AWS Control Tower で管理対象となるアカウントには状態が存在する

状態	説明
未登録	アカウントは親 OU のメンバーですが、AWS Control Tower によって管理されていません
登録中	AWS Control Tower の管理対象になっています。親 OU のコントロール設定に適合するようにアカウントが調整されてます
登録済み	アカウントは、その親 OU 用に設定されたコントロールによって管理されています。AWS Control Tower によって管理されています
登録に失敗しました	登録を試みましたが、アカウントを AWS Control Tower に登録できていません
更新が利用可能	アカウントは登録済みですが、アカウントには利用可能な更新があります。環境に加えられた最近の変更を反映するには、アカウントを更新する必要があります

初期は「未登録」で登録を実行すると「登録済み」に遷移する

AWS Control Tower の組織

メンバーアカウントの状態を管理し AWS Control Tower の管理下への追加やランディングゾーンの更新を行う

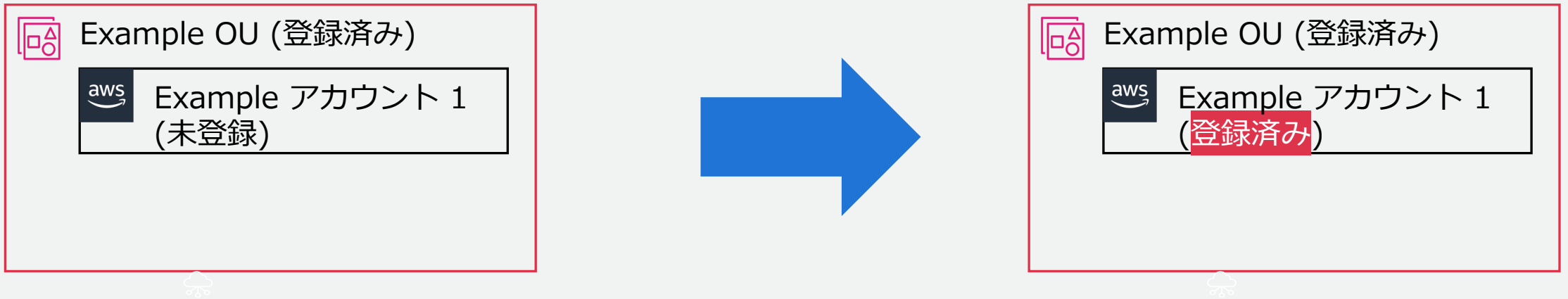
実行可能なアクション

- 組織単位 (OU)
  - 登録、再登録、削除
- アカウント
  - 登録、更新、解除

アカウントの登録

AWS Control Tower のガバナンスを未適用のアカウントに対し
アカウントごとに AWS Control Tower のガバナンスを適用する

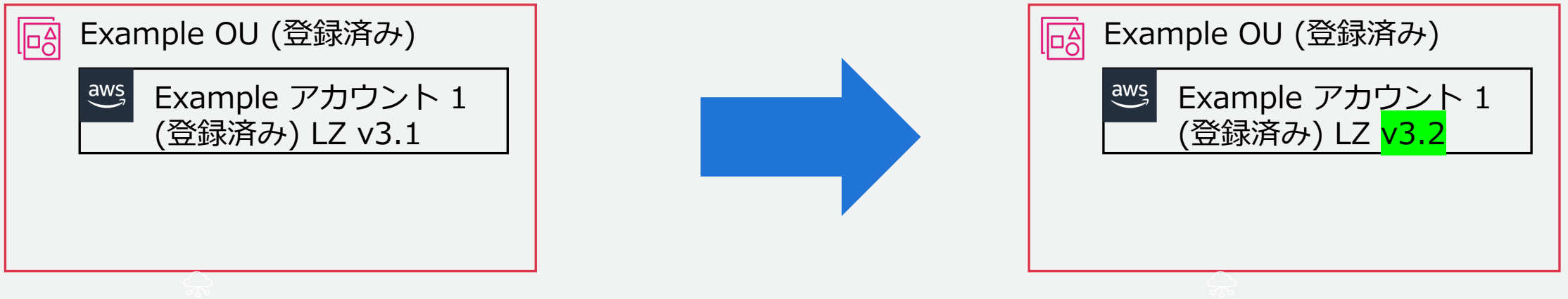
状態は未登録から登録済みとなる



アカウントの更新

AWS Control Tower のガバナンスを適用済みのアカウントに対しランディングゾーン (LZ) の更新を行う

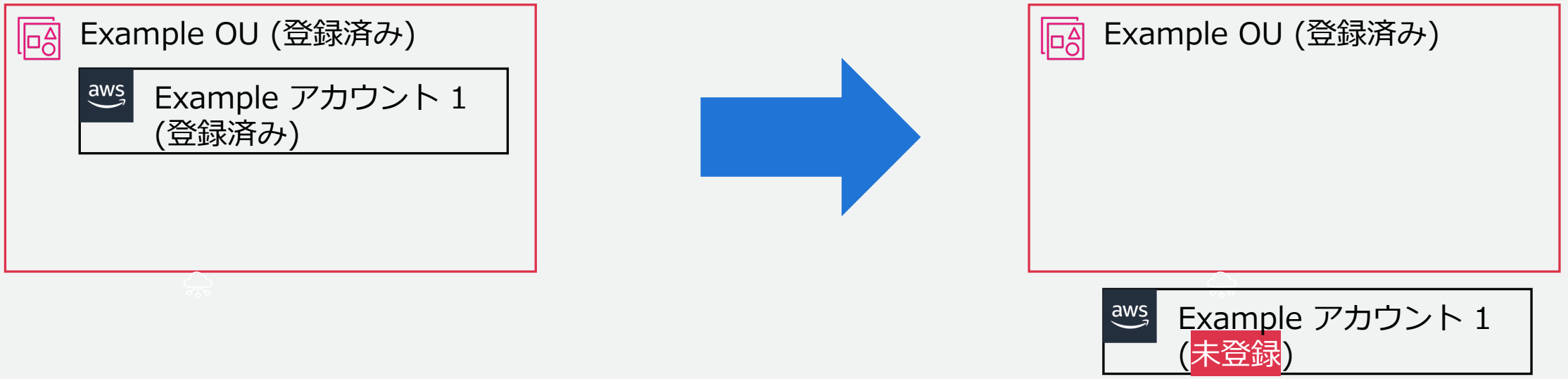
状態は登録済みのままでランディングゾーンのバージョンが更新される



アカウントの解除

AWS Control Tower のガバナンスを適用済みのアカウントに対して AWS Control Tower の管理対象から外す

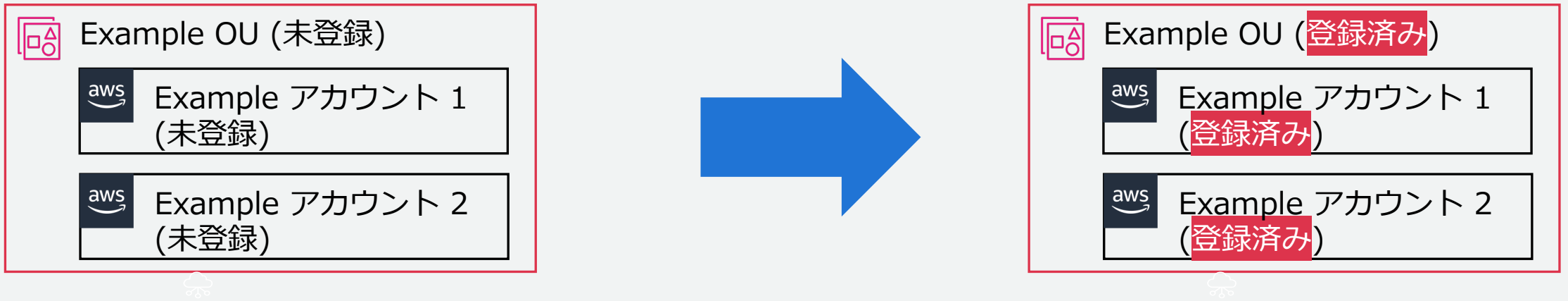
状態は登録済みから未登録となる



OU の登録

AWS Control Tower のガバナンスを未適用のアカウントに対し
OU ごとに AWS Control Tower のガバナンスを適用する

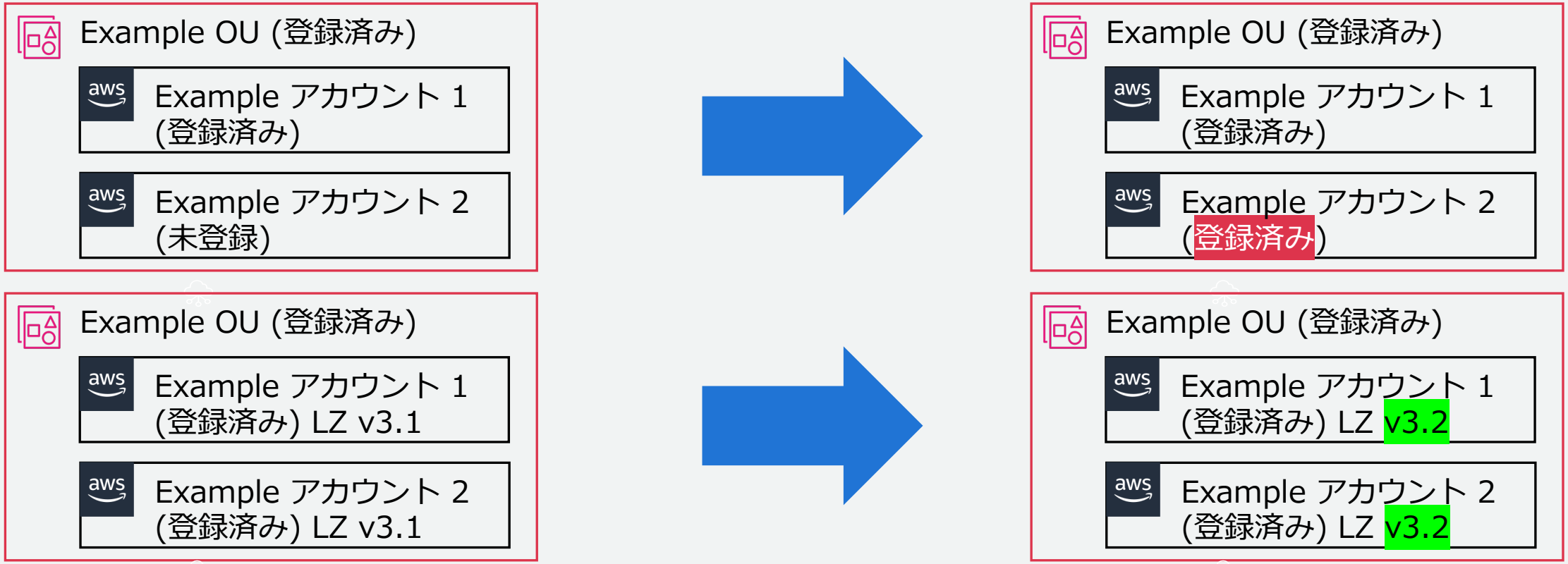
OU 直下のアカウントを未登録から登録済みに変更する



OU の再登録

AWS Control Tower のガバナンスを未適用のアカウントに対し
OU ごとに AWS Control Tower のガバナンスを適用する

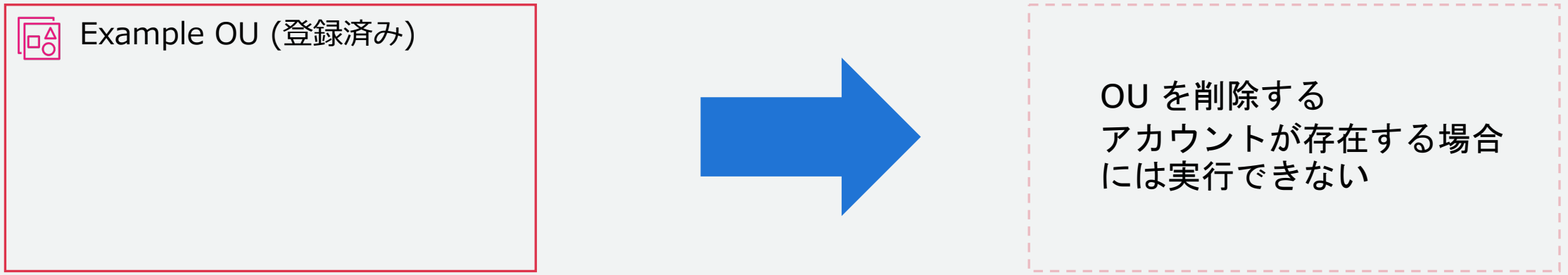
ランディングゾーンのバージョンを更新する



OU の削除

存在する OU を削除する

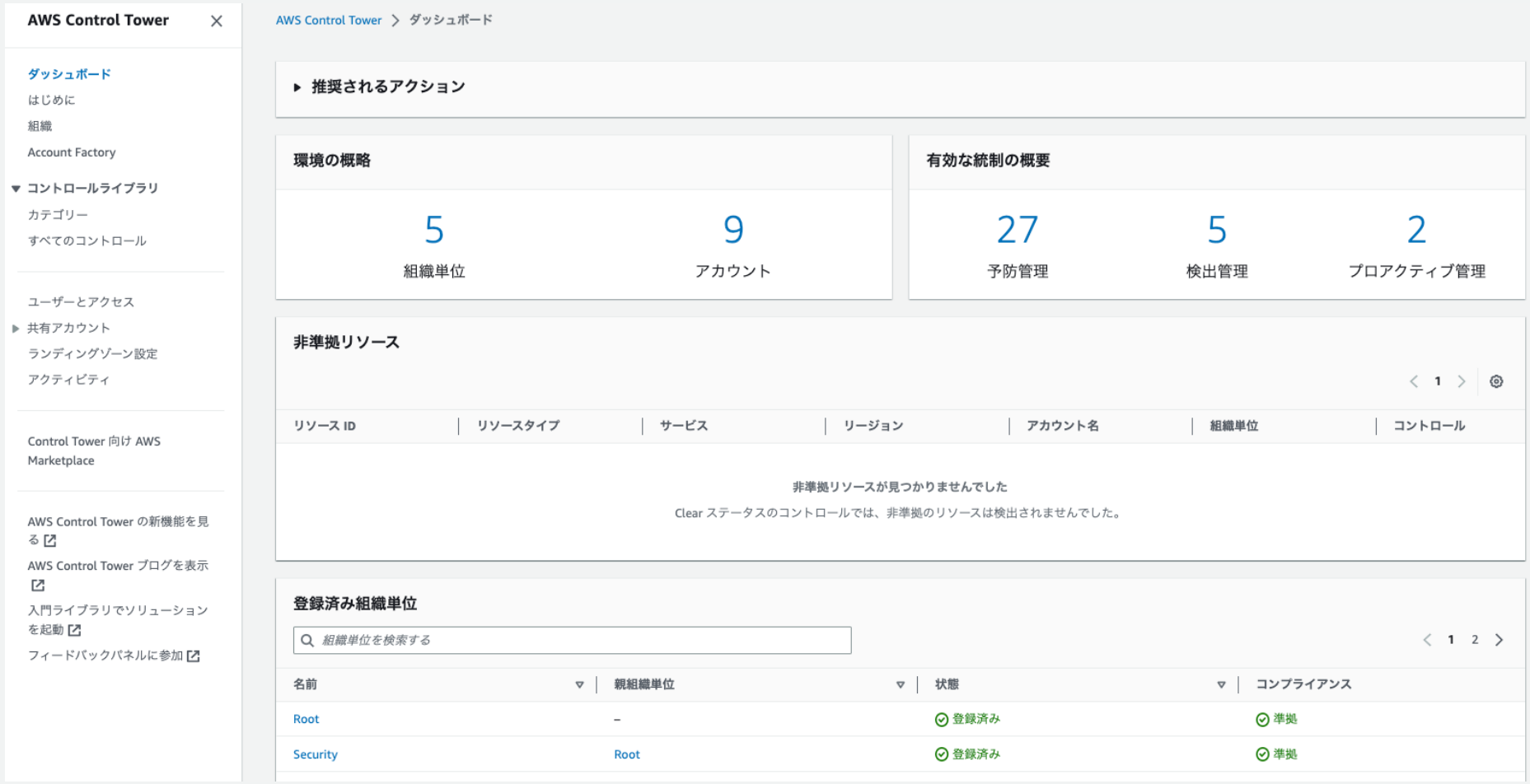
AWS Control Tower の状態を変更するアクションではない



ダッシュボード

情報の一元管理

- アカウント数や非準拠リソースを把握できる



まとめ

紹介した機能

1. ランディングゾーン
   統制の効いた環境を作る
2. コントロール
   ガバナンス強化を実現する
3. Account Factory
   統制の効いたアカウントを作成する
4. 組織
   アカウントや OU の状態を管理する
5. ダッシュボード
   情報を一元管理する

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 9 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!