AWS Black Belt Online Seminar

AWS Control Tower

手順編 AWS Control Tower の有効化

Hajime Onishi

Cloud Support Engineer
2023/08

自己紹介

名前：大西 朔 (Hajime Onishi)

所属：アマゾン ウェブ サービス ジャパン合同会社
技術支援本部 クラウドサポートエンジニア

好きな AWS サービス：

AWS Control Tower

AWS CodeDeploy

AWS CodePipeline

AWS Distro for OpenTelemetry

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)

本セミナーの対象者

- 複数の AWS アカウントを管理されている方
- AWS Control Tower を導入予定・検討中の方
- AWS Control Tower におけるアカウントの登録手順を整理したい方

本セミナーの Goal

- AWS Control Tower を有効化する手順と留意点を知る

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

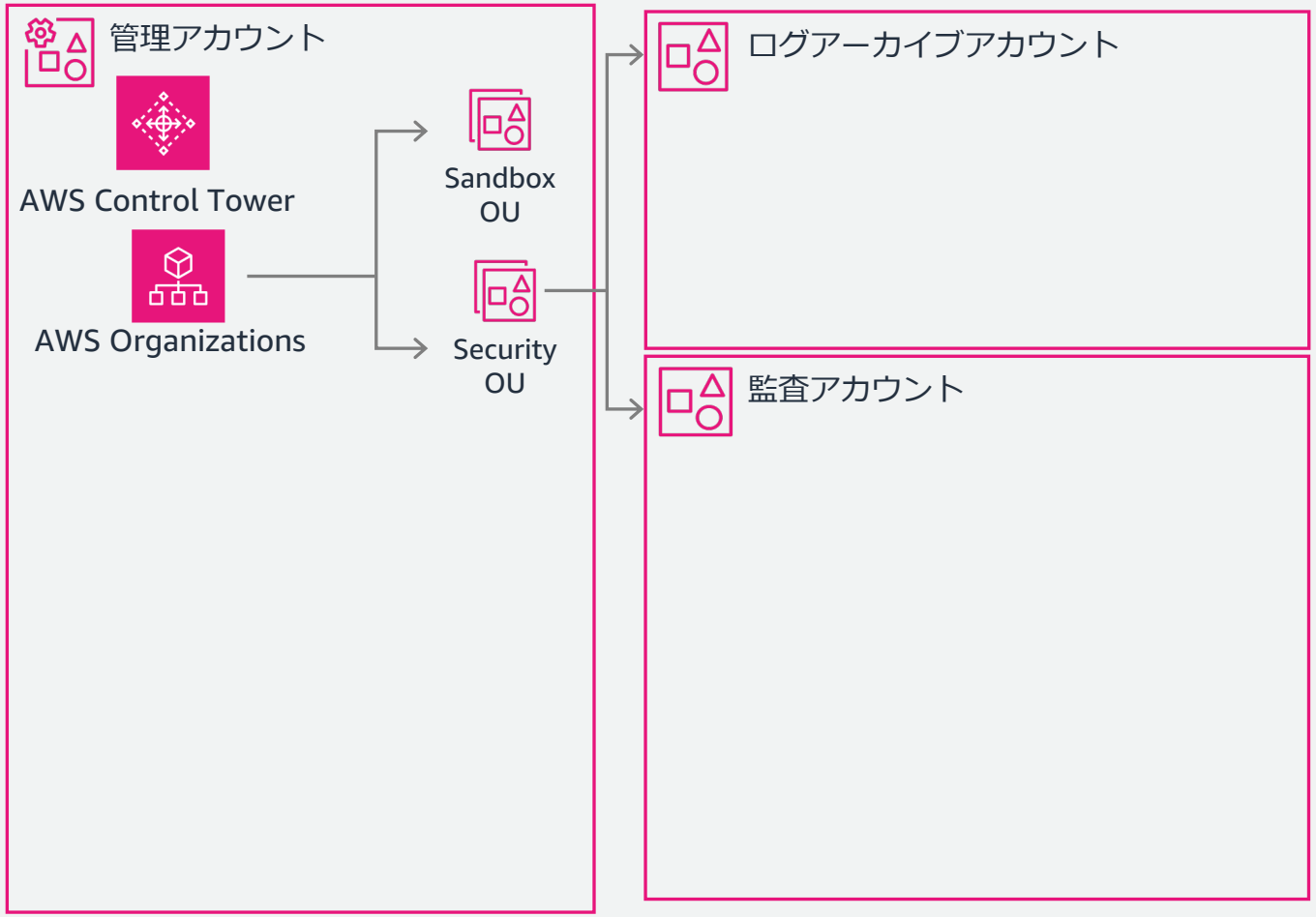
1. ランディングゾーンのセットアップ
    1. AWS Control Tower ランディングゾーンの概要
    2. コンソールでのセットアップ手順
    3. よくあるエラーと修正方法・セットアップ時の留意点

2. メンバーアカウントの登録
    1. 組織単位とその直下のメンバーアカウントの登録手順
    2. Root 直下のメンバーアカウントの登録手順
    3. AWS Config を有効化済みの AWS アカウントの登録申請
    4. 登録手順のまとめ

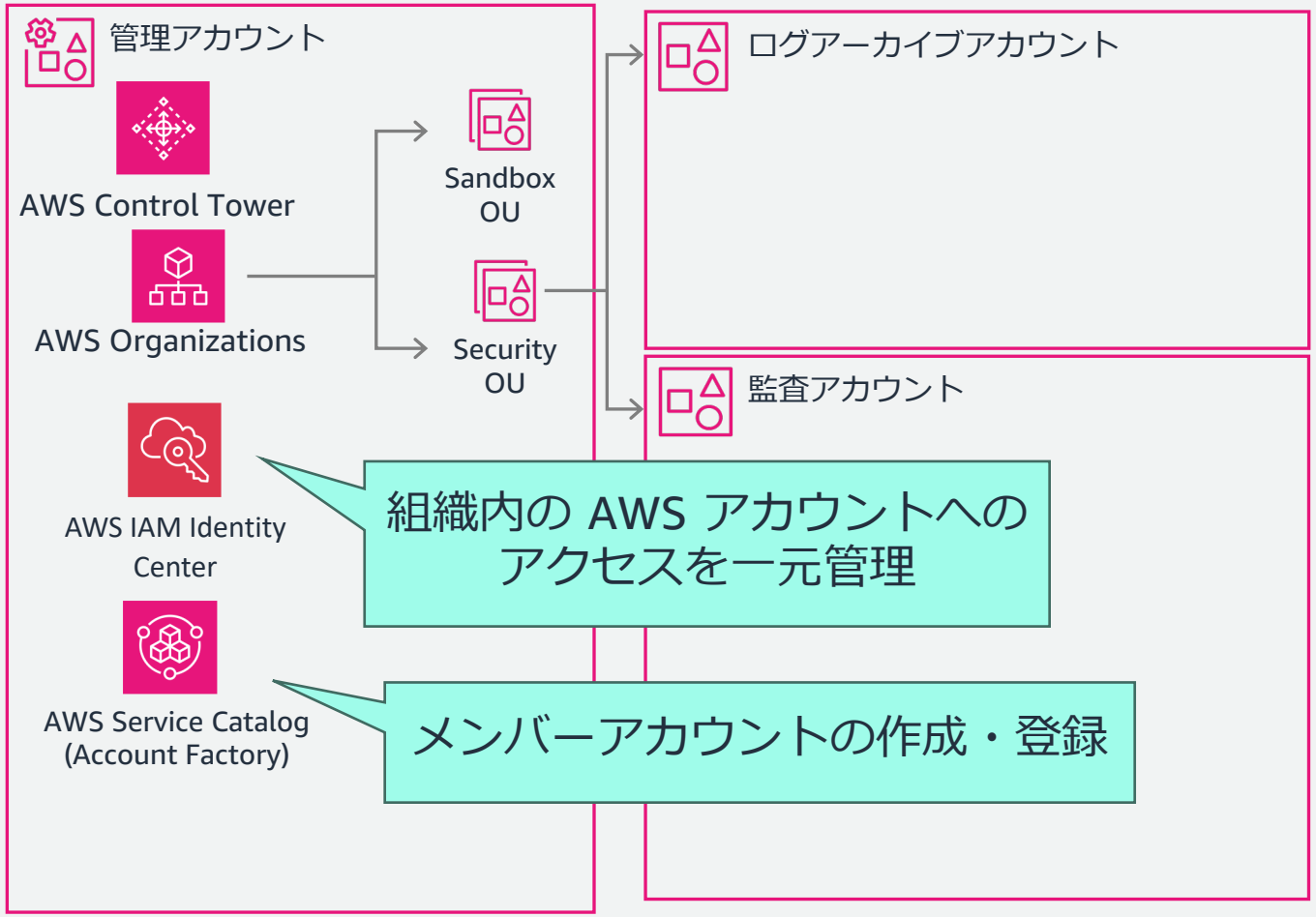
ランディングゾーンのセットアップ

1.1 AWS Control Tower ランディングゾーンの概要

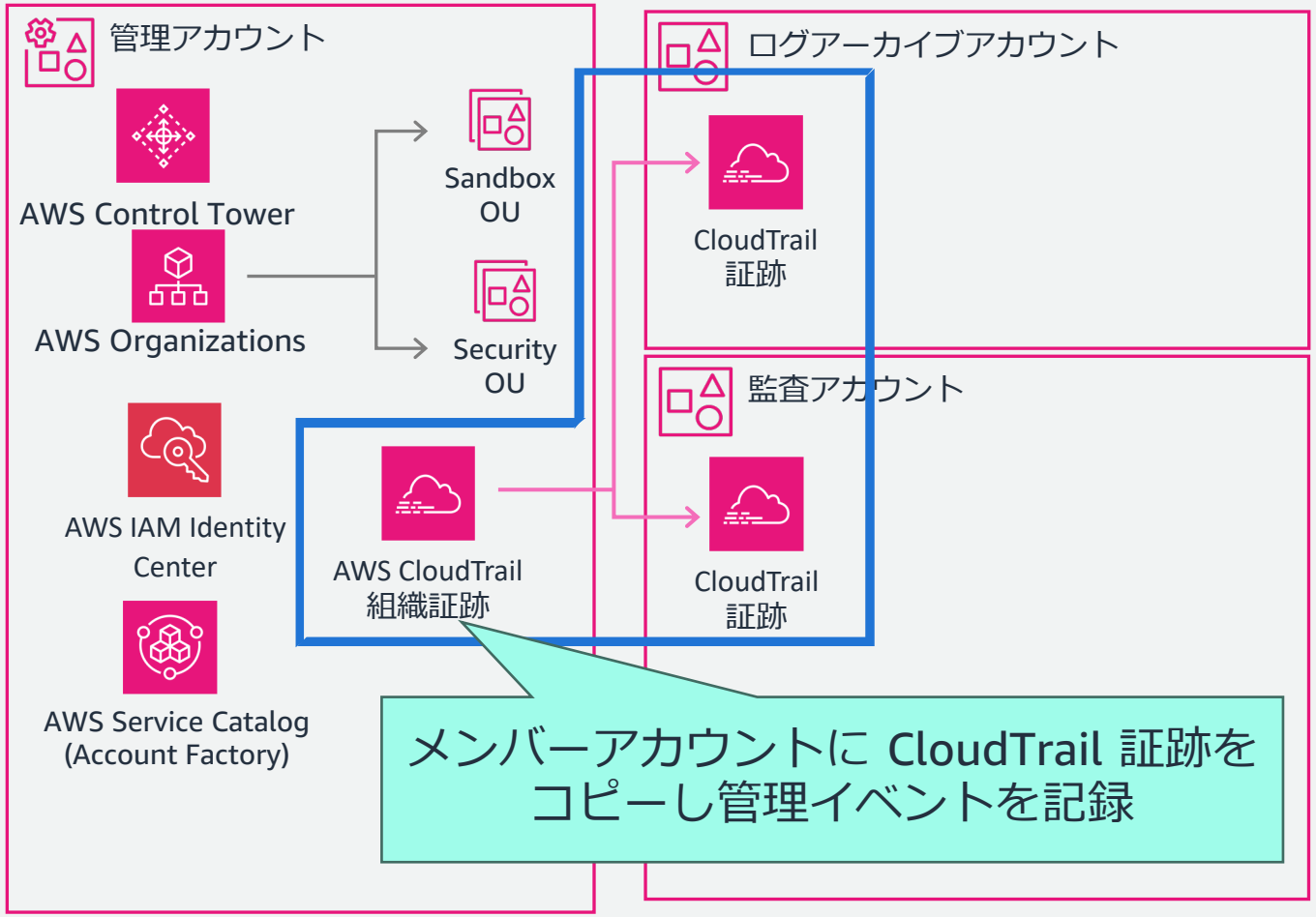
AWS Control Tower が管理アカウントで以下を実行



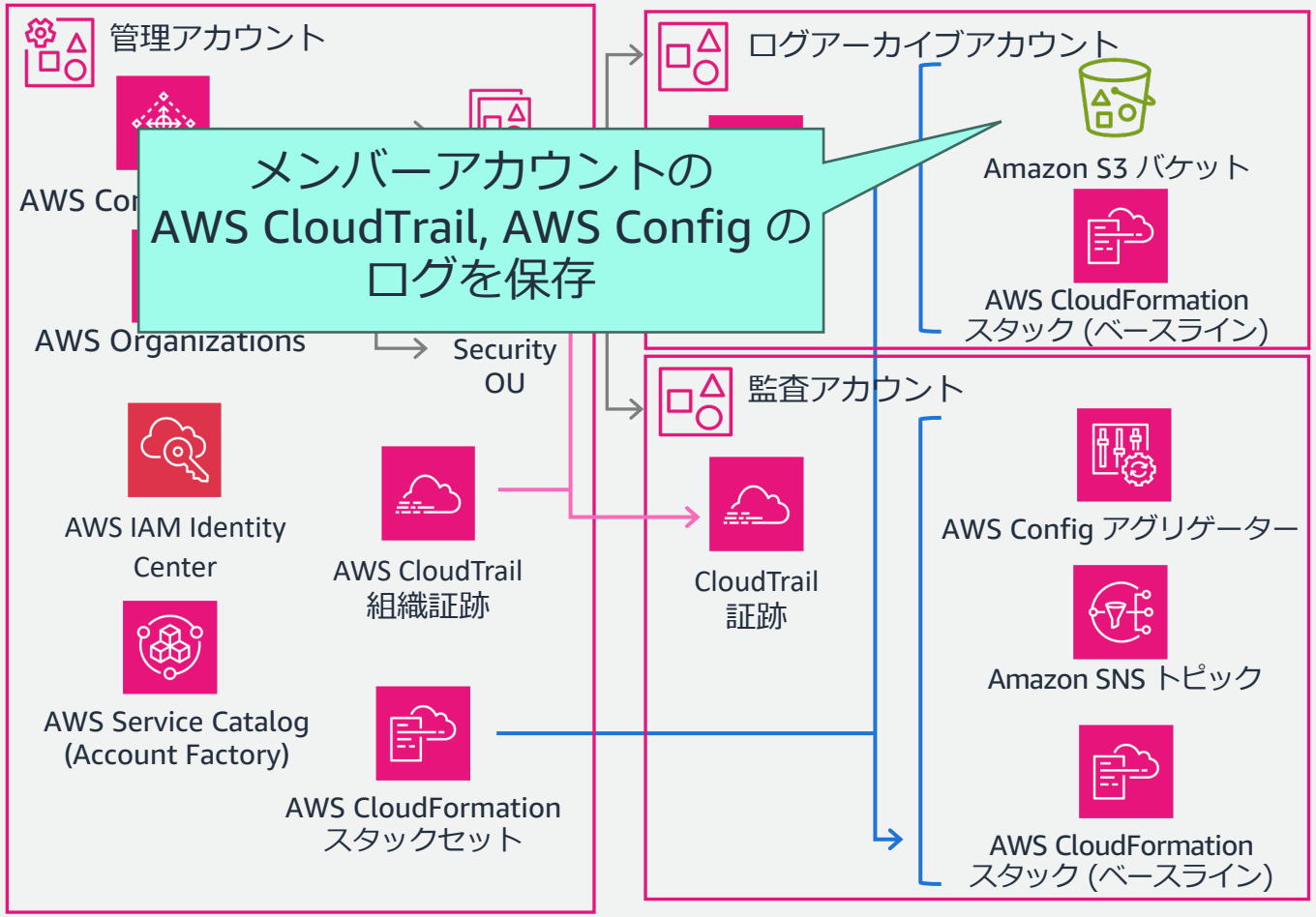
AWS Control Tower が管理アカウントで以下を実行



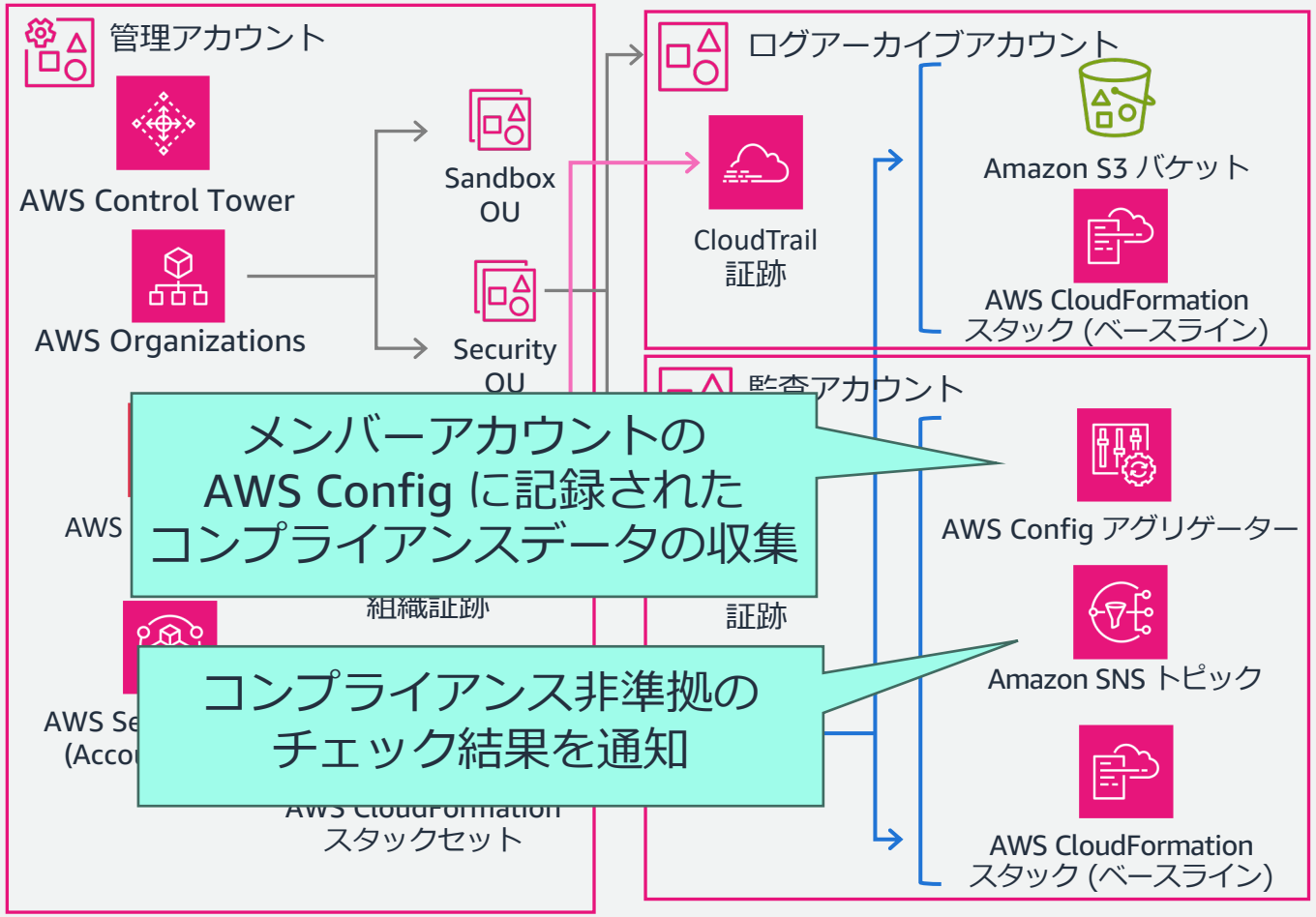
AWS Control Tower が管理アカウントで以下を実行



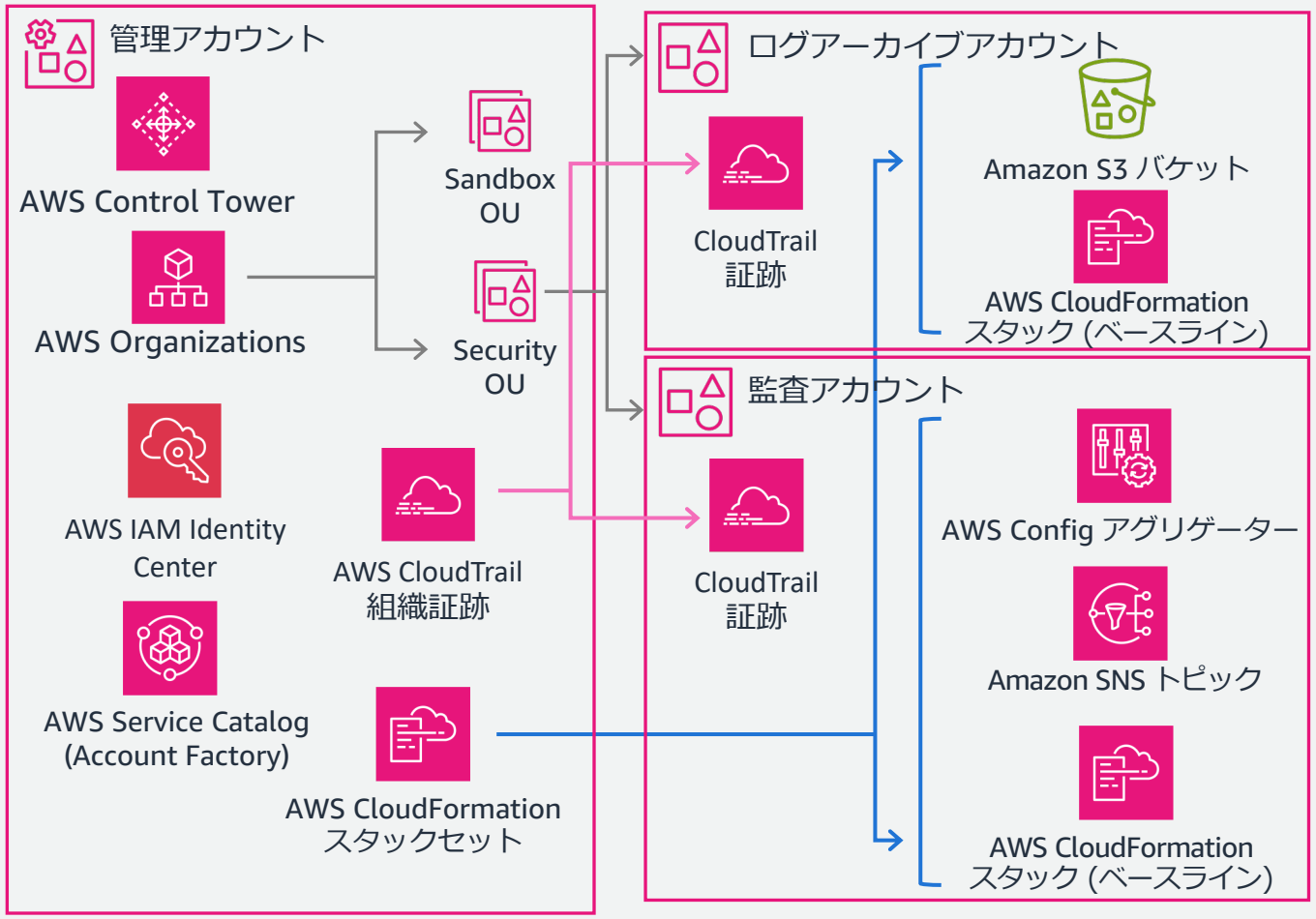
AWS Control Tower が管理アカウントで以下を実行



AWS Control Tower が管理アカウントで以下を実行



まとめ: セットアップ内容の概要



作成されるリソースの詳細は、
下記ドキュメントをご参照ください

https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/how-control-tower-works.html#what-shared

ランディングゾーンのセットアップ

1.2 コンソールでのセットアップ手順

セットアップ手順の概要

- 事前確認
- ステップ 1: リージョンを選択
- ステップ 2: 組織単位 (OU) の設定
- ステップ 3: 共有アカウントの設定
- ステップ 4: その他の設定
- ステップ 5: 確認とセットアップ

事前確認

- 操作する IAM ユーザー・ロールは **管理者権限 (AdministratorAccess)** を持つ

AWS Control Tower コンソールは、管理アカウントの管理者権限を持つユーザーだけが使用できます。それらのユーザーだけが、ランディングゾーン内で管理作業を実行できます。これは、ベストプラクティスに従って、ほとんどのユーザーとメンバーアカウント管理者に AWS Control Tower コンソールが表示されることがないことを意味します。管理アカウントの管理者グループのメンバーは、必要に応じて、ユーザーとメンバーアカウントの管理者に次の情報を説明する必要があります。

https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/best-practices.html

- AWS Control Tower によるリソース作成を妨げる SCP を Root にアタッチしていない
  - **Root には FullAWSAccess ポリシーのみアタッチするのが無難**
  - 登録メンバーアカウントは必ずいずれかの組織単位に所属するので組織単位にアタッチする独自の SCP や予防コントロールでアクセス制御する

AWS マネージドポリシー: FullAWSAccess の内容

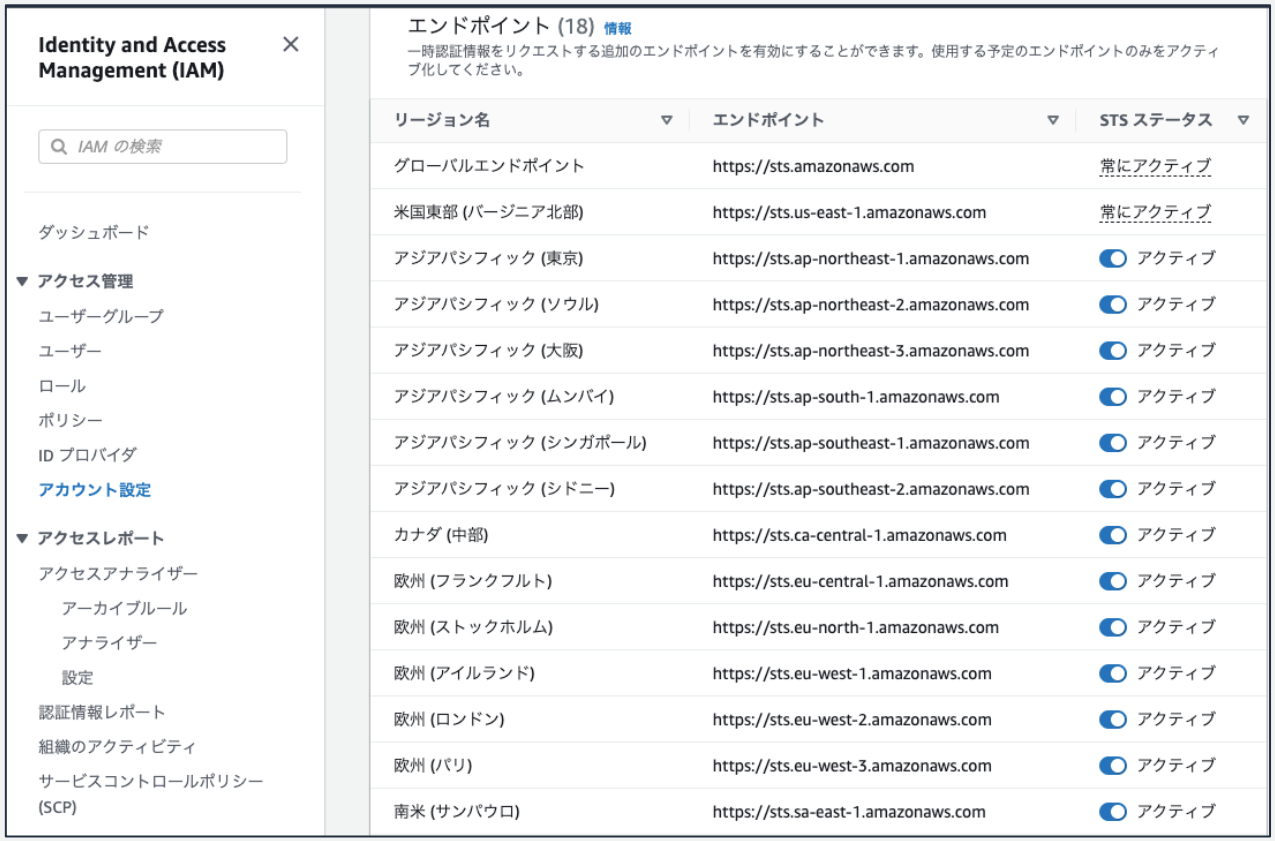
事前確認

- **サポートするすべてのリージョンで AWS STS を有効化している**

> **注記**
> 起動時に、AWS Control Tower が管理するすべてのリージョンの管理アカウントで、AWS Security Token Service (STS) エンドポイントをアクティブにする必要があります。この操作を行わないと、設定プロセスの途中で起動が失敗する可能性があります。

https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/getting-started-prereqs.html

- 確認・修正方法
  - IAM コンソールにアクセス
  - [アクセス管理] -> [アカウント設定]
  - Security Token Service (STS) エンドポイントのステータスを アクティブに変更



IAM コンソールでの AWS STS 設定確認

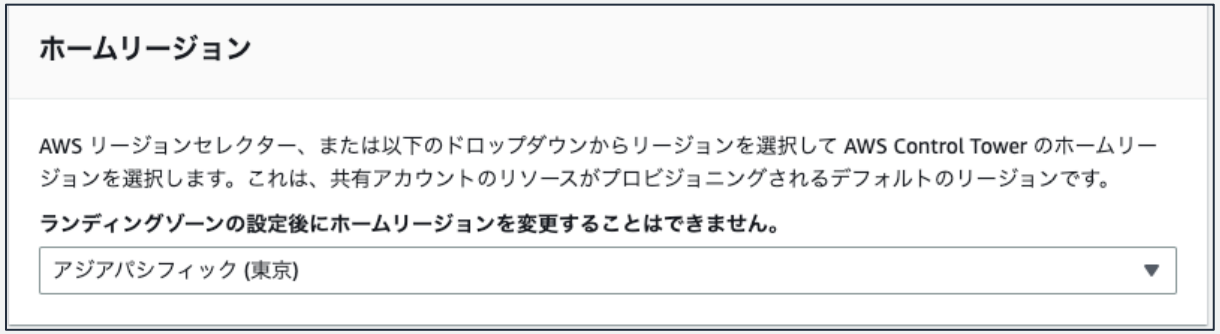
1. リージョンを選択

1. ホームリージョンを選択

- **設定後に変更できない**
- 最も使用頻度の高いリージョンを選択する
- AWS IAM Identity Center を有効化済みの場合
同じリージョンを選択する

https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/region-how.html

事前確認の後、Control Tower コンソールで
ランディングゾーンの設定を開始



Control Tower コンソールでのランディングゾーンのセットアップ
ステップ 1-1: ホームリージョンの選択

1. リージョンを選択

2. 管理対象リージョンを選択

- AWS Control Tower による
  ガバナンスを有効にするリージョン
- AWS Config などのリージョナルな
  AWS サービスをデプロイする
- **設定後にリージョンを**
  変更・追加・削除できる

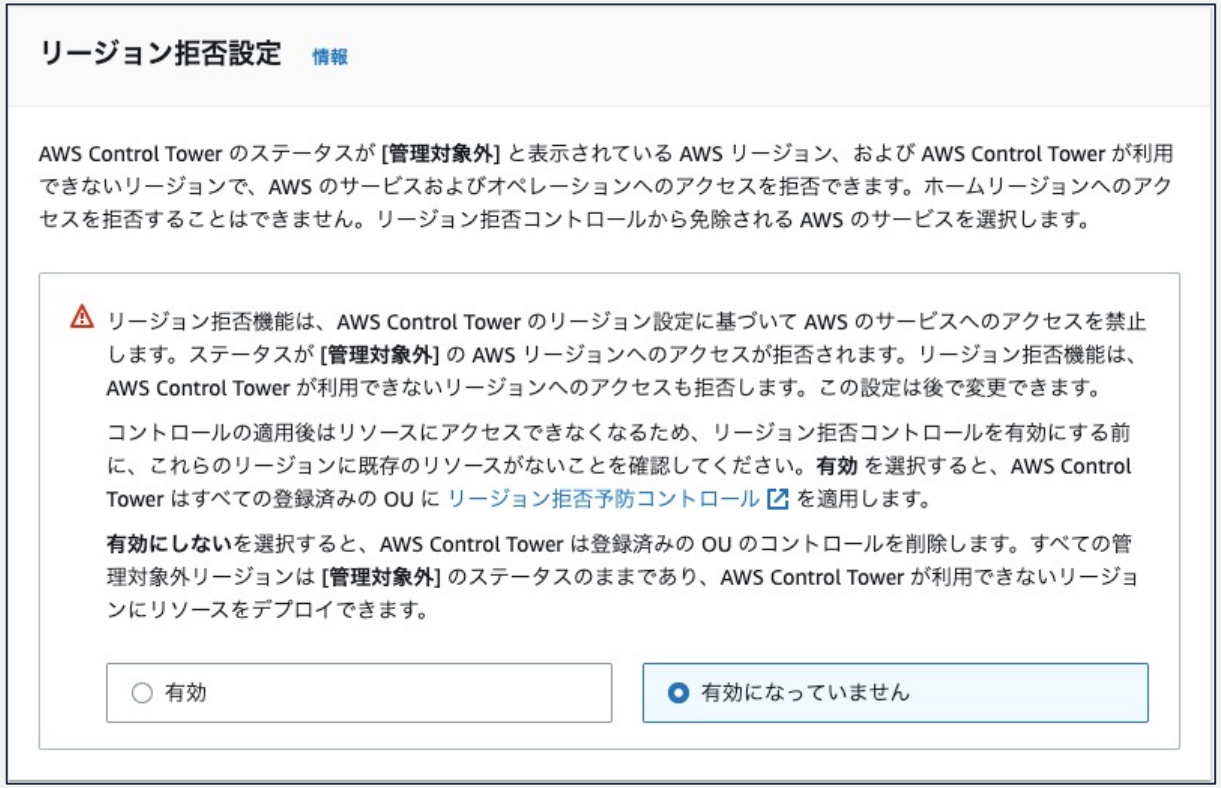
ステップ 1-2: 管理対象リージョンの選択

1. リージョンを選択

3. リージョン拒否設定

- 管理対象リージョン以外では
  AWS サービスのアクセスを拒否する
- **登録済み組織単位に対して**
  リージョン拒否 SCP を設定する
- 一部のグローバルサービスなどは
  例外的にアクセスを許可

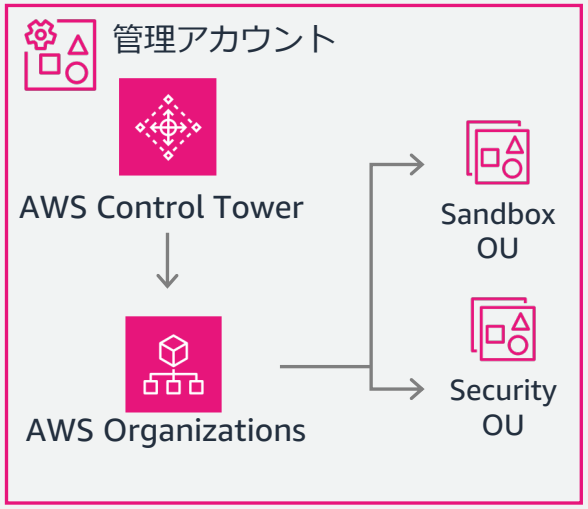
https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/data-residency-controls.html#primary-region-deny-policy



ステップ 1-3: リージョン拒否設定

2. 組織単位 (OU) の設定

- 組織単位 (OU) を作成
  - **基礎となる OU (必須):**
    デフォルト名は Security
  - **追加の OU (任意):**
    デフォルト名は Sandbox

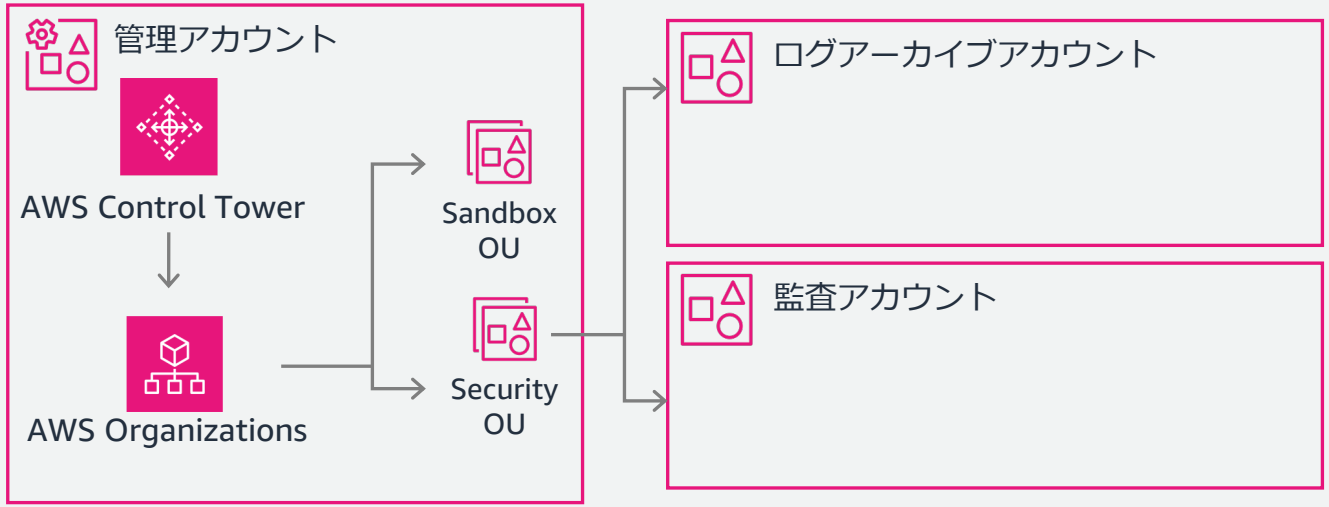


ステップ 2: 組織単位の設定

3. 共有アカウントの設定

- ログアーカイブ・監査アカウント
  - **メールアドレスとアカウント名を指定して新規で作成する**
  - **メンバーアカウントのアカウント ID を指定して使用する**

https://aws.amazon.com/jp/blogs/news/use-existing-logging-and-security-account-with-aws-control-tower/

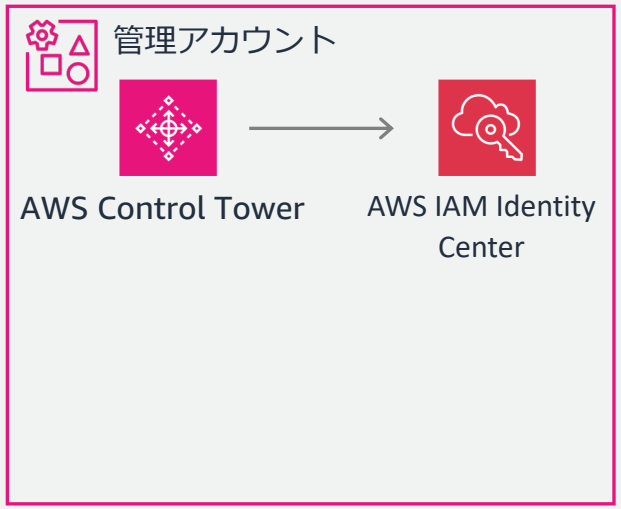


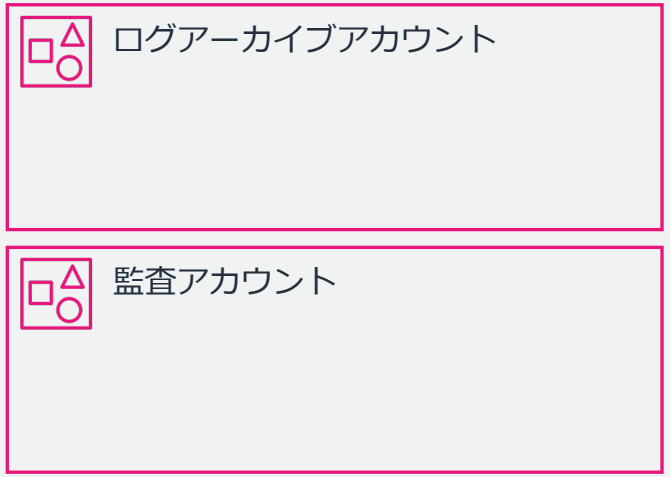
ステップ 3: 共有アカウントの設定

4. その他の設定

- AWS IAM Identity Center による AWS アカウントアクセスの設定
  - ユーザーグループ・許可セットを設定
  - **使用するかしないか選択可能**

https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/sso.html

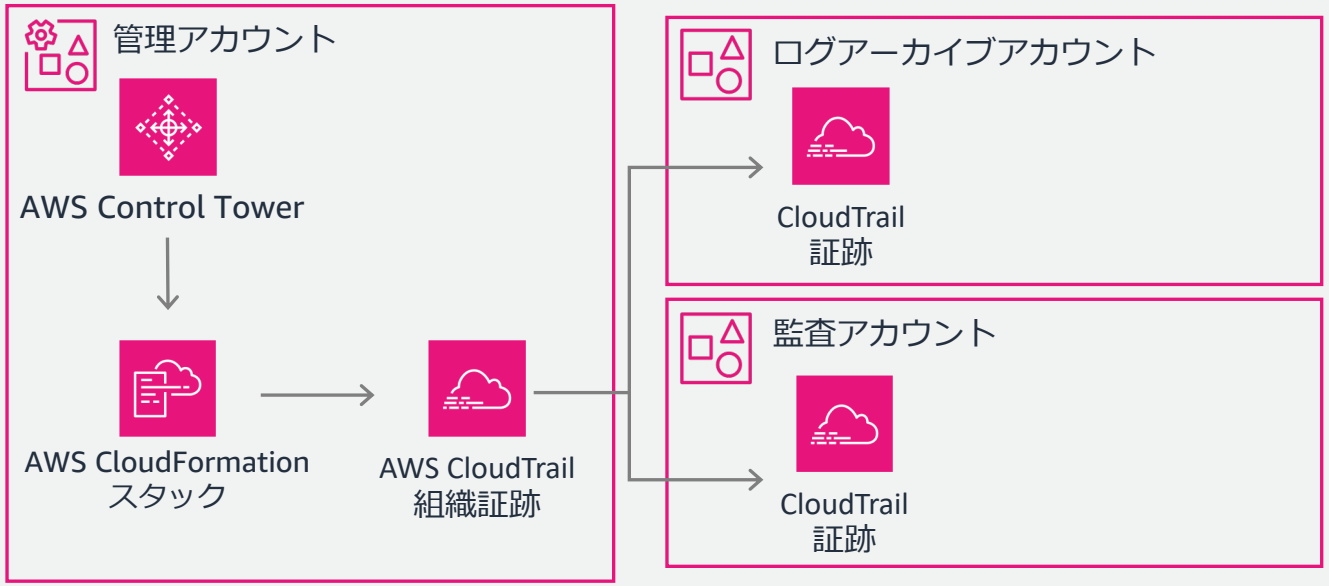




ステップ 4-1: IAM Identity Center による アクセス設定の有効・無効

4. その他の設定

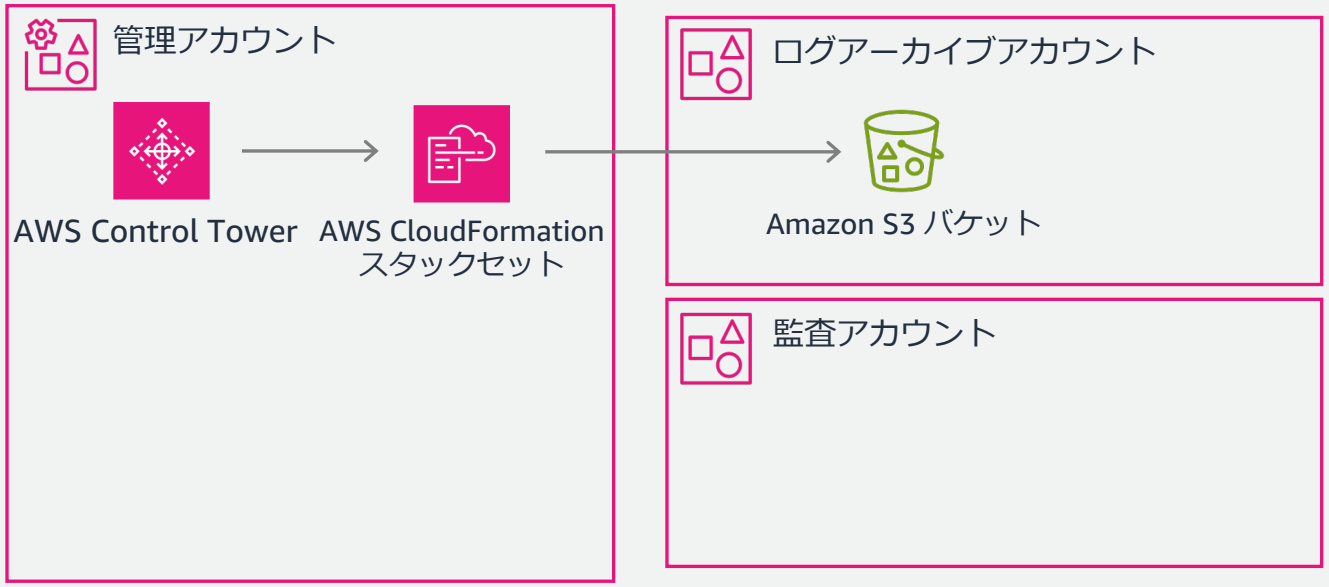
- 管理アカウントのリソース作成
  - AWS CloudTrail 組織証跡を作成
    - **必ず証跡は作成するが**
      有効・無効を選択可能



ステップ 4.2: AWS CloudTrail 組織証跡の有効・無効

4. その他の設定

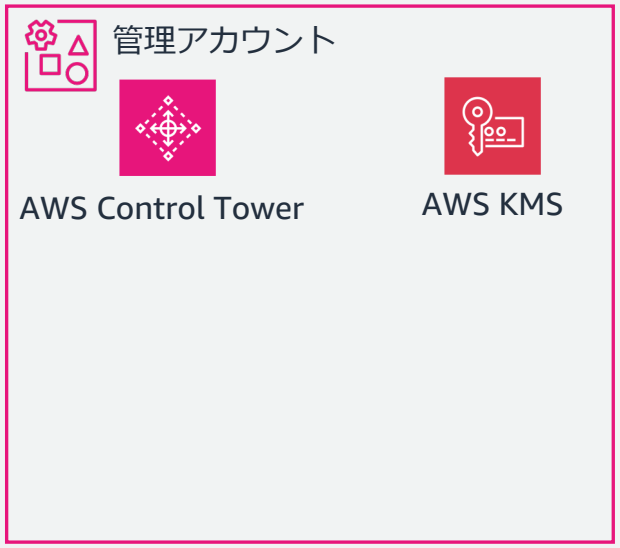
- AWS CloudTrail と AWS Config ログ用の Amazon Simple Storage Service (Amazon S3) バケットの保持期間 (1 日 ~ 15 年)
  - **ログ用のバケットの保持期間: デフォルト 1 年**
  - **アクセスログ用のバケットの保持期間: デフォルト 10 年**

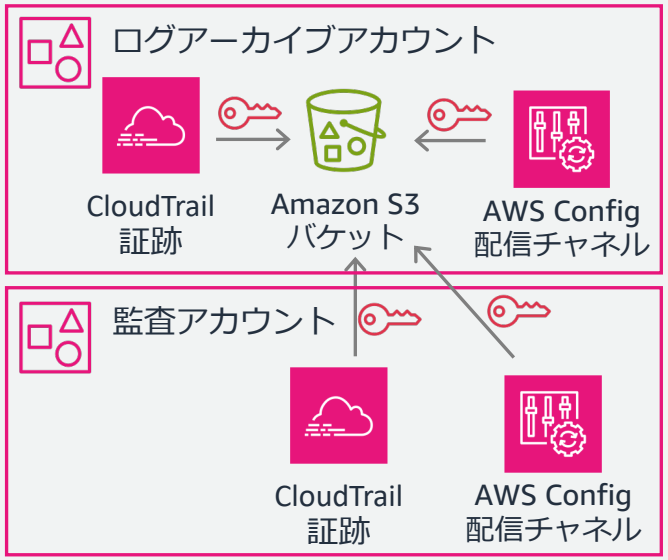


ステップ 4.3: ログバケットの保持期間設定

4. その他の設定

- AWS Key Management Service (AWS KMS) 暗号化
  - AWS CloudTrail, AWS Config のログを管理アカウントの AWS KMS キーで暗号化する
  - **使用するかしないか選択可能**

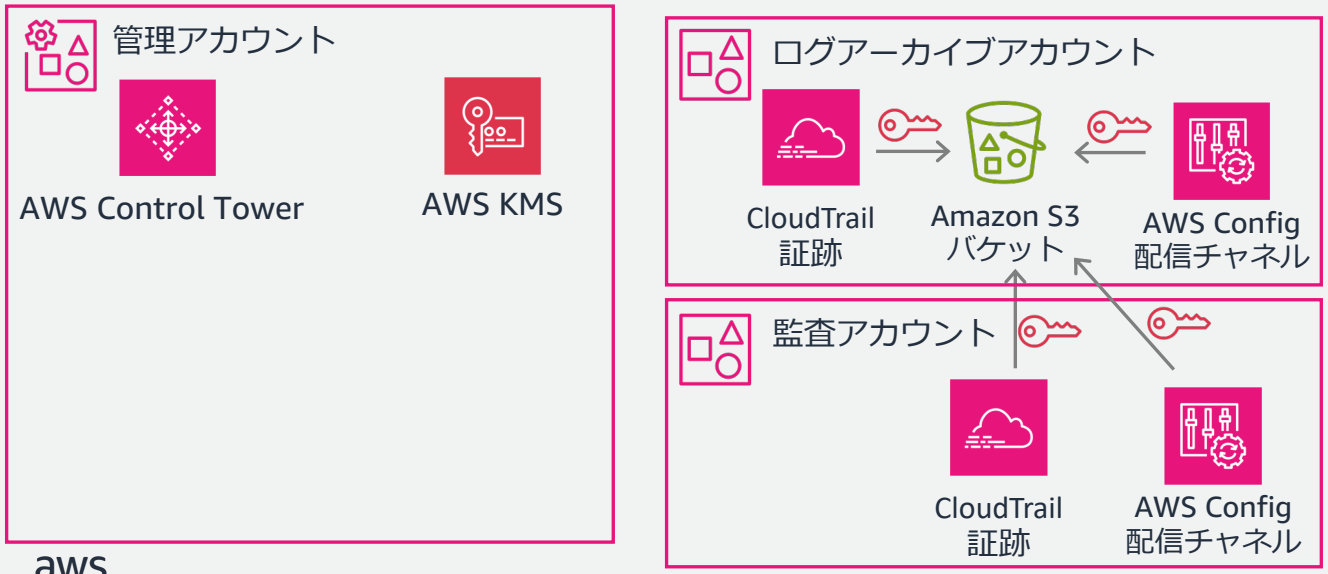




ステップ 4.4: ログの AWS KMS による暗号化

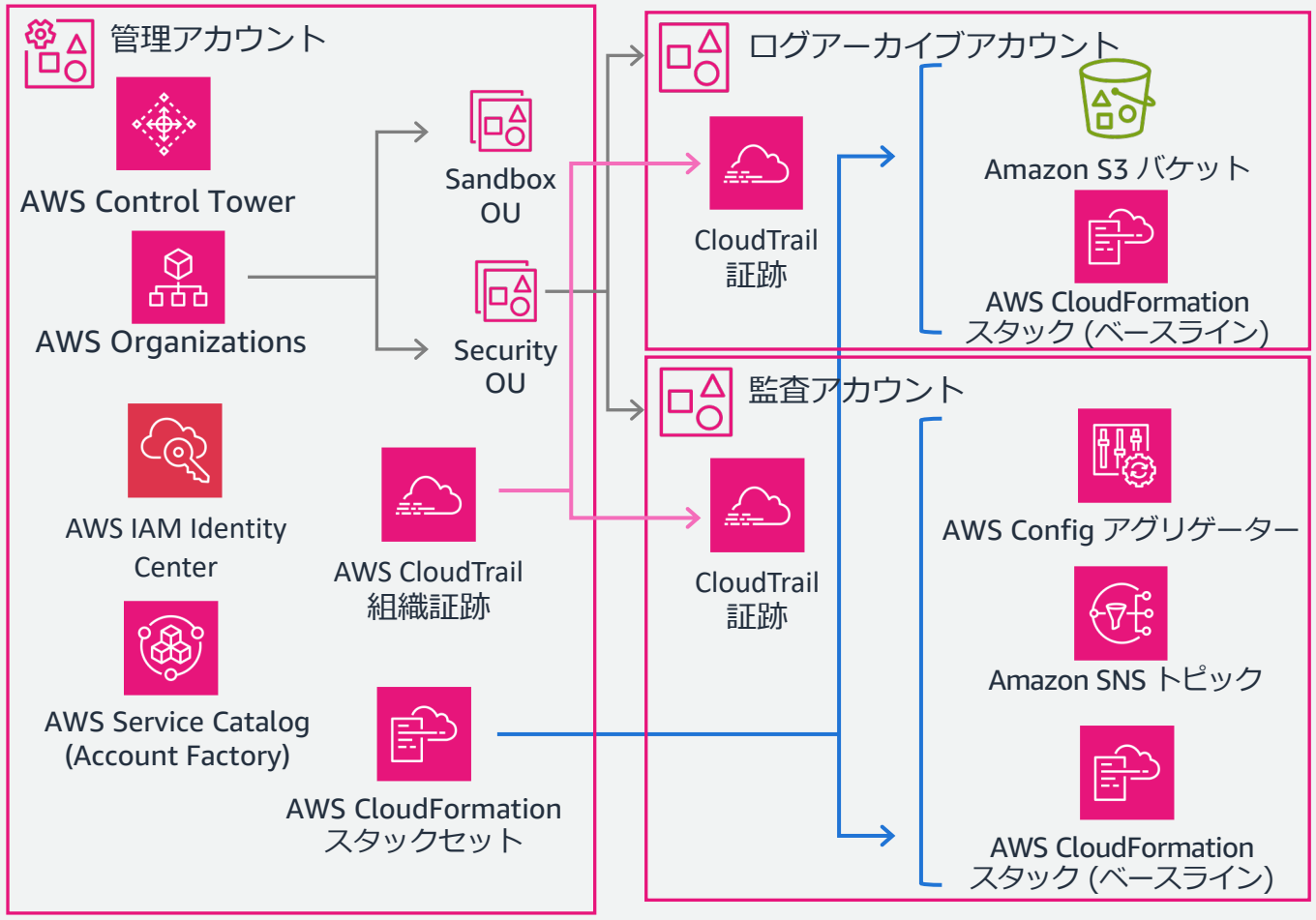
4. その他の設定

- AWS KMS 暗号化の要確認事項
  - **対称な単一リージョンキーか**
  - **キーポリシーにアクセス許可**
    - **AWS CloudTrail, AWS Config のサービスプリンシパルに KMS キーへのアクセス許可を追加**



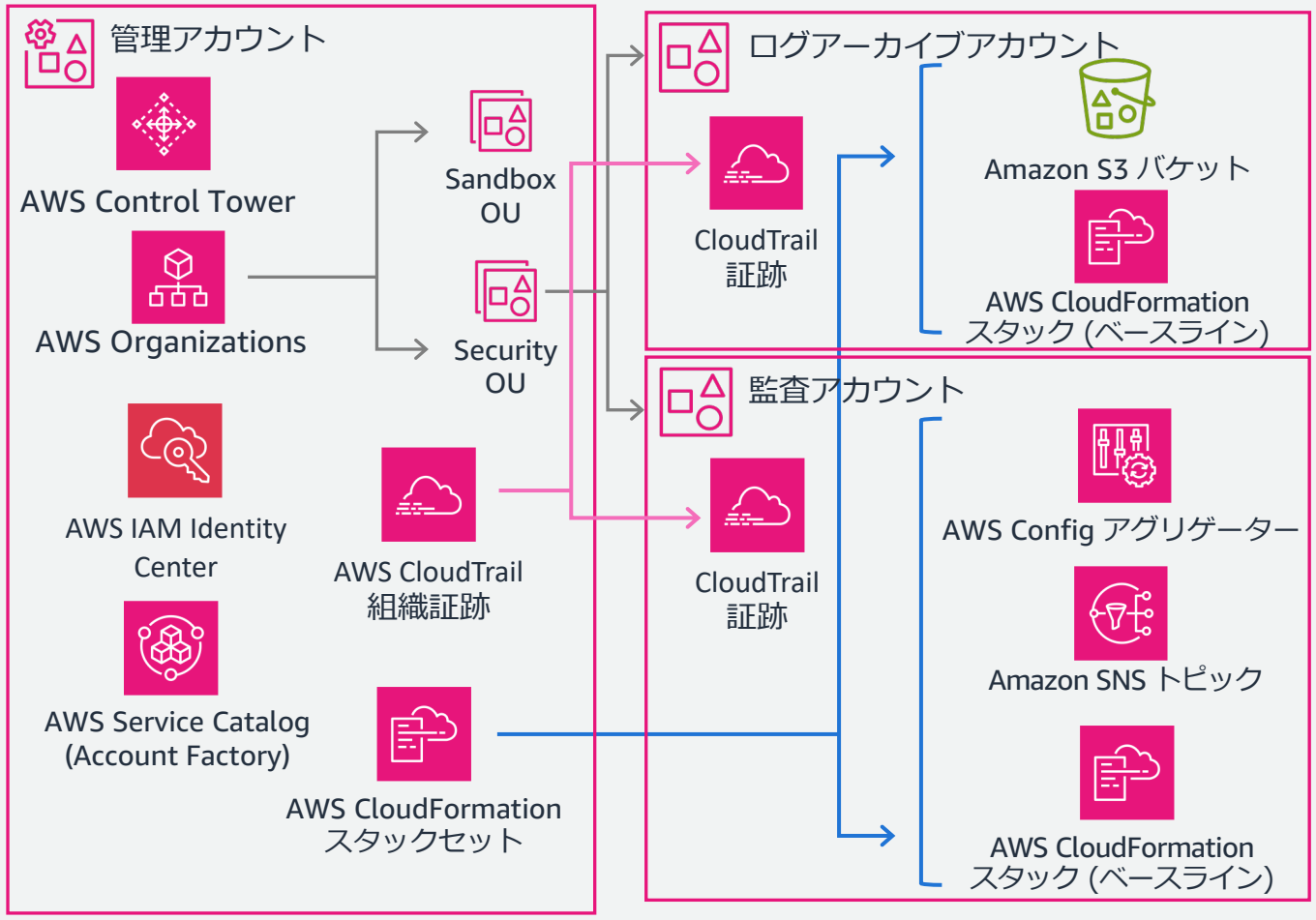
ステップ 4.4: ログの AWS KMS による暗号化

5. 確認とセットアップ

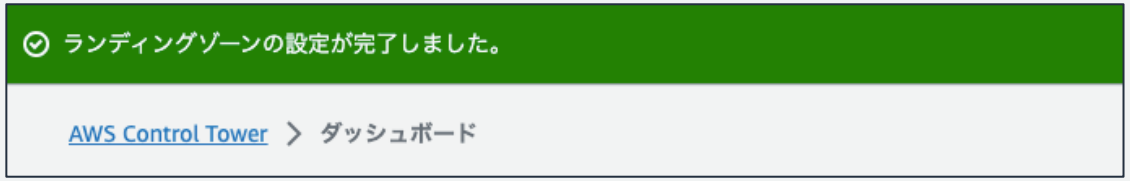


ステップ 5: セットアップの開始

5. 確認とセットアップ



セットアップ中、進捗状況を確認可能



コンソールで上記のように表示されると
セットアップ完了

ランディングゾーンのセットアップ

1.3 よくあるエラーと修正方法
セットアップ時の留意点

セットアップ時の事前エラーと修正

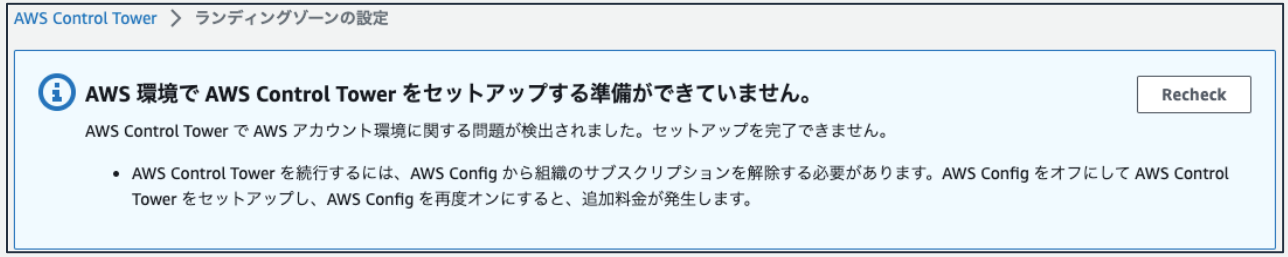
- AWS Control Tower の
セットアップ時には
事前チェックが実行される

https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/getting-started-prereqs.html

- よくある事前エラーの例

1. **AWS Config の信頼された
アクセスが有効**

対処方法:
Organizations コンソールで
信頼されたアクセスを無効化する



セットアップの事前エラー例 1:
AWS Config の信頼されたアクセスが有効

対処方法:
Organizations コンソールで
信頼されたアクセスを無効化

セットアップ時の事前エラーと修正

- よくある事前エラーの例

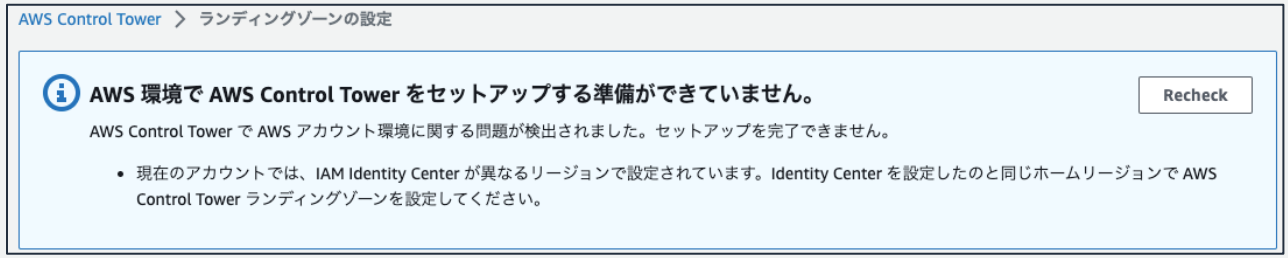
2. IAM Identity Center とホームリージョンが異なる

対処方法:

- ホームリージョンを同じリージョンに変更する
- IAM Identity Center 設定を削除する
  ユーザー・グループ・許可セットなど
  すべてのデータが削除されてしまう

留意点:

- **セルフマネージド IAM Identity Center 設定の場合も、同一リージョンでなければならない**



セットアップの事前エラー例 2:
既存の IAM Identity Center と異なるリージョンがホームリージョン

IAM アイデンティティセンターの設定を削除する

IAM Identity Center 設定を削除すると、その設定のすべてのデータが削除され、復元できなくなります。次の表は、IAM Identity Center で現在設定されているディレクトリタイプに基づいて削除されるデータをまとめたものです。

削除されるデータについて	接続されているディレクトリ (AWS Managed Microsoft AD または AD Connector)	IAM アイデンティティセンター ID ストア
設定したすべての権限セット AWS アカウント	✓	✓
IAM アイデンティティセンターで設定したすべてのアプリケーション	✓	✓
AWS アカウント設定したすべてのユーザー割り当てとアプリケーション	✓	✓
ディレクトリまたはストア内のすべてのユーザーとグループ	**該当なし**	✓

https://docs.aws.amazon.com/ja_jp/singlesignon/latest/userguide/regions.html#delete-config

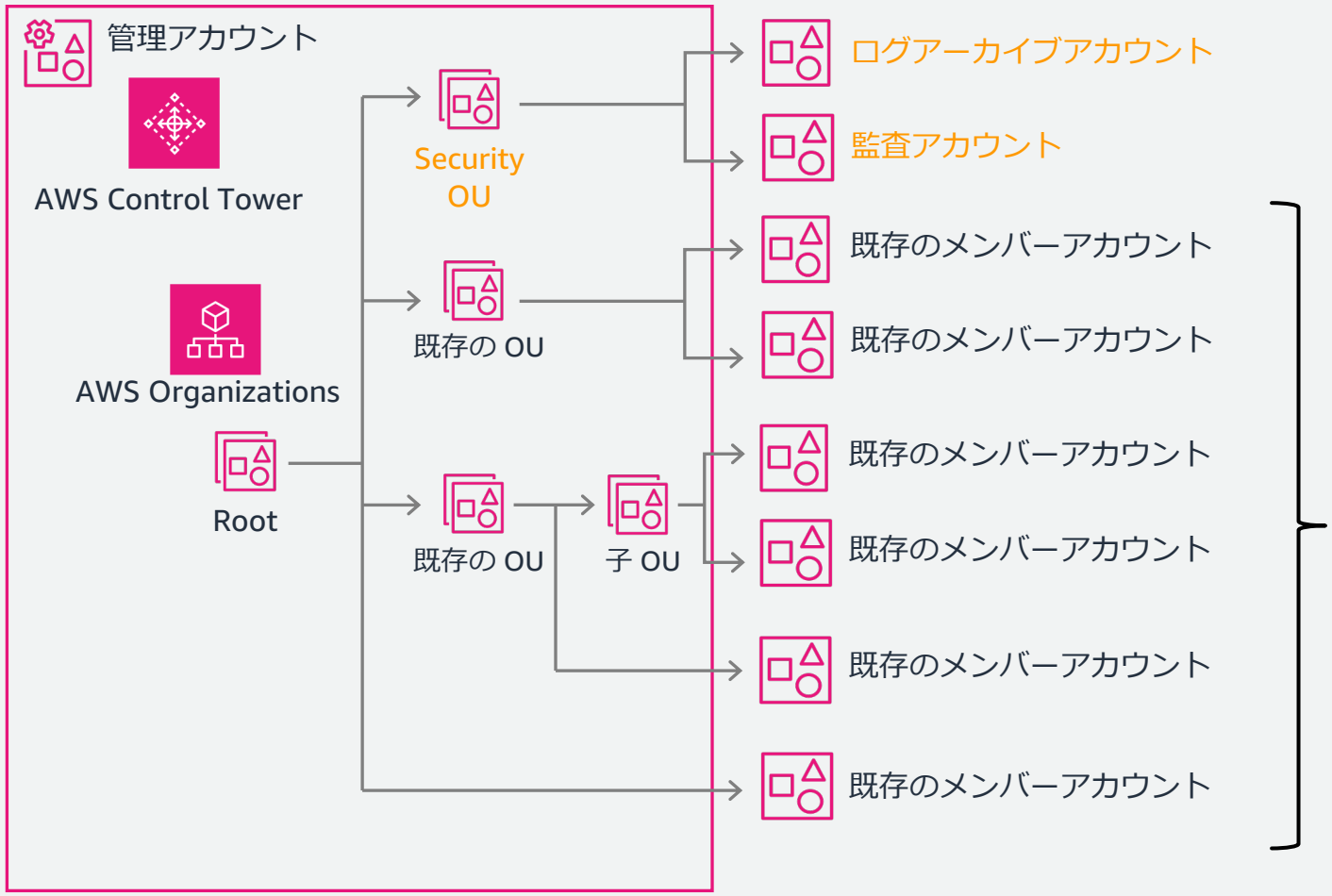
まとめ: ランディングゾーンのセットアップ時の留意点

- 管理アカウント
  - 事前チェックなし: **セットアップ前の確認を推奨**
  1. **管理者権限を持つ IAM ユーザー・ロールでセットアップする**
  2. **Root にリソース作成を妨げる SCP を設定しない**
  3. **サポートするすべてのリージョンの AWS STS を有効化する**
  4. **(AWS KMS 暗号化キーを使用する場合)**
     キーポリシーに正しいアクセス許可があるか・対称な単一リージョンキーか
  - 事前チェックあり: エラー発生後に確認して対応
  1. AWS Config の信頼されたアクセスを無効化する
  2. ホームリージョンと AWS IAM Identity Center のリージョンは一致しているか etc.
- ログアーカイブ・ 監査アカウント (既存アカウントの場合): **セットアップ前の確認を推奨**
  1. **AWS Config 設定レコーダーと配信チャネルは削除する**
  2. **サポートするすべてのリージョンの AWS STS を有効化する**

メンバーアカウントの登録

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



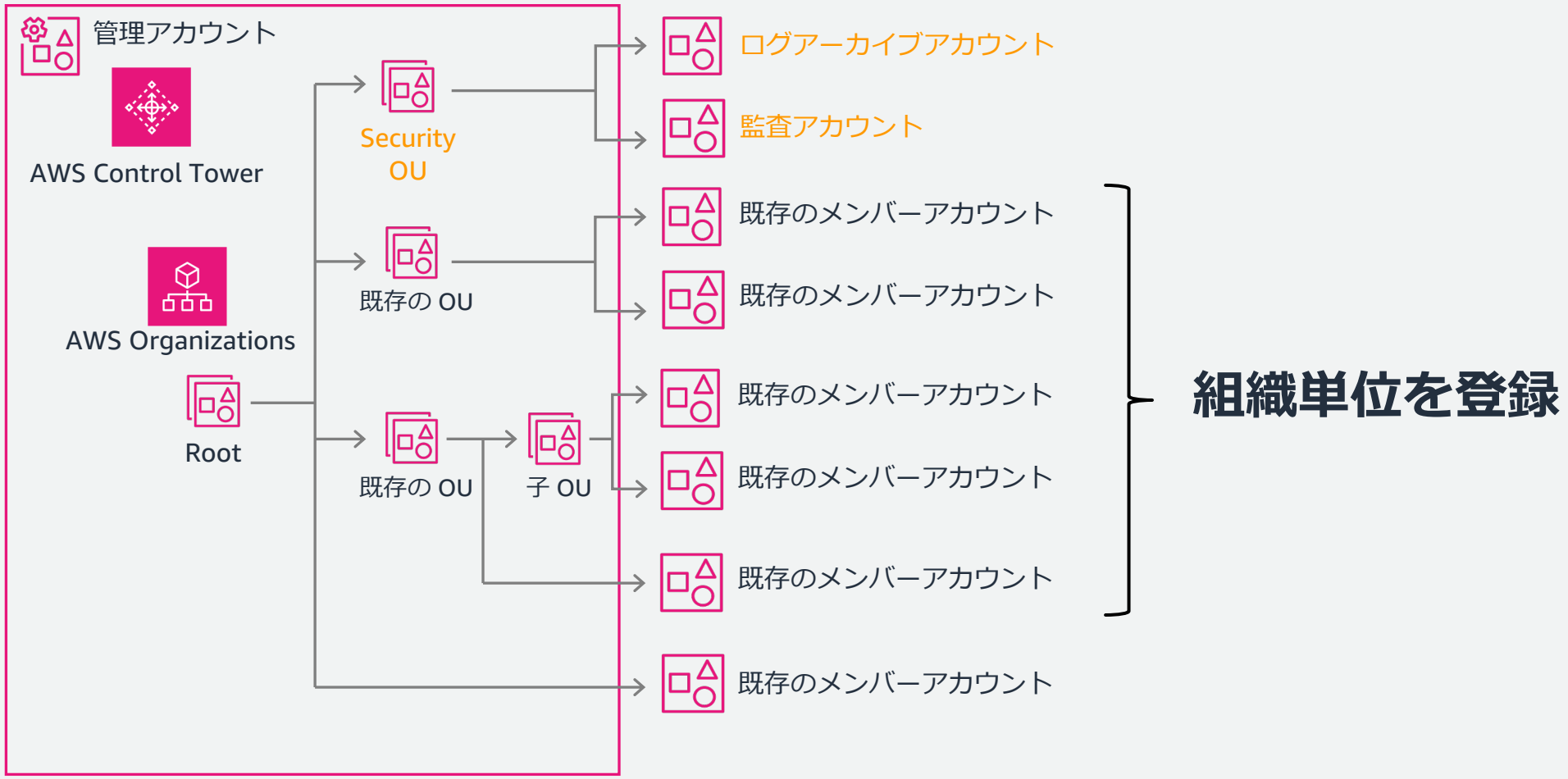
別途 AWS Control Tower への登録作業が必要となる

メンバーアカウントの登録

1.1 組織単位とその直下の メンバーアカウントの登録手順

メンバーアカウントの登録

- 組織単位とその直下のメンバーアカウントの登録



組織単位の登録

組織単位と直下のメンバーアカウントをまとめて登録する

https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/importing-existing.html

- 処理内容

1. **AWSControlTowerExecution ロールをメンバーアカウントにデプロイする**
2. **組織単位と各アカウントが登録前提条件を満たしているか事前チェックする**
3. 1 つでも事前チェックに失敗すると残りのメンバーアカウントの登録も中止する
4. 成功後、メンバーアカウントの登録を開始する (Account Factory をプロビジョニング)
   - ✓ **ネストされた組織単位とそのメンバーアカウントは組織単位の登録後、さらに登録作業を実施する**

Control Tower コンソール -> [組織] での [組織単位を登録]

組織単位への事前チェック

1. **操作する IAM ユーザー・ロールが Account Factory のポートフォリオにあるか**
2. **所属するメンバーアカウント数が 300 を超える組織単位は登録できない**
3. **組織単位にアタッチできる SCP の上限数 (5 個) を超えていると登録できない**
   - SCP を削除・結合するか、SCP の継承を使う
4. 登録を妨げるSCP があるか

など

組織単位への事前チェック

1. **操作する IAM ユーザー・ロールが Account Factory のポートフォリオにあるか**
2. **所属するメンバーアカウント数が 300 を超える組織単位は登録できない**
3. **組織単位にアタッチできる SCP の上限数 (5 個) を超えていると登録できない**
   - SCP を削除・結合するか、SCP の継承を使う
4. 登録を妨げるSCP があるか

など

	レポートでのエラー内容
1.	OU を登録する前に、IAM ユーザーを AWS Service Catalog ポートフォリオに追加します。
2.	AWS Control Tower は、登録時に各 OU のアカウント数を 300 個に制限します。
3.	OU あたりの SCP の制限を超えているか、別のクォータに達した可能性があります。AWS Control Tower のランディングゾーンの OU には、OU あたり 5 SCP の制限が適用されます。それ以上ある場合は、それらを削除する必要があります。
4.	この OU には、AWS Control Tower がアカウントを登録できない既存の SCP があります。AWS Control Tower SCP と競合するポリシーの SCP を確認してください。

メンバーアカウントへの事前チェック

1. **管理対象リージョンの AWS Config を無効化 (設定レコーダー・配信チャネルがない) しているか**
   - 後述のサポートケースでの申請によって有効化していても例外的に登録可能
2. **サポートするすべてのリージョンの AWS STS を有効化しているか**
3. **停止 (Suspended) 状態のメンバーアカウントがあると登録できない**
   - 停止済みアカウント専用の未登録組織単位 (Suspended OU) を用意して移動する
     https://docs.aws.amazon.com/whitepapers/latest/organizing-your-aws-environment/suspended-ou.html

など

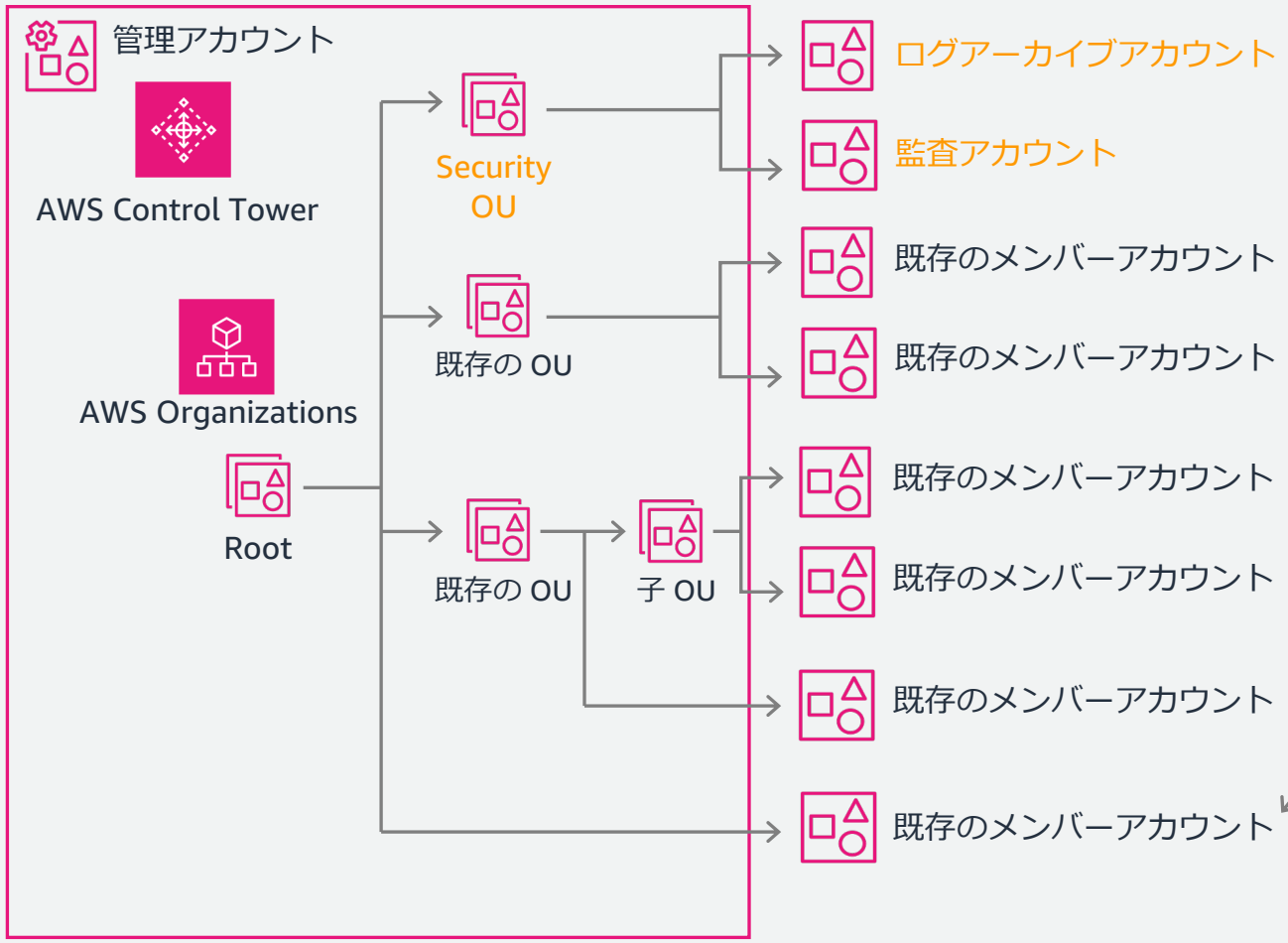
	レポートでのエラー内容
1.	アカウントに既存の AWS Config 設定レコーダーがある場合があります。これらの設定レコーダーは、アカウントを登録する前に、AWS CLI を使用してすべてのリージョンで削除する必要があります。
	アカウントに既存の AWS Config 配信チャネルがある場合があります。これらのチャネルは、アカウントを登録する前に、AWS CLI を使用してすべてのリージョンで削除する必要があります。
2.	AWS STS は、アカウント内で無効にすることができます。AWS STS エンドポイントは、AWS Control Tower でサポートされているすべてのリージョンのアカウントでアクティブ化する必要があります。
3.	このアカウントは停止されており、AWS Control Tower に登録できません。OU からこのアカウントを削除してください。

メンバーアカウントの登録

1.2 Root 直下の メンバーアカウントの登録手順

メンバーアカウントの登録

- Root 直下のメンバーアカウントの登録



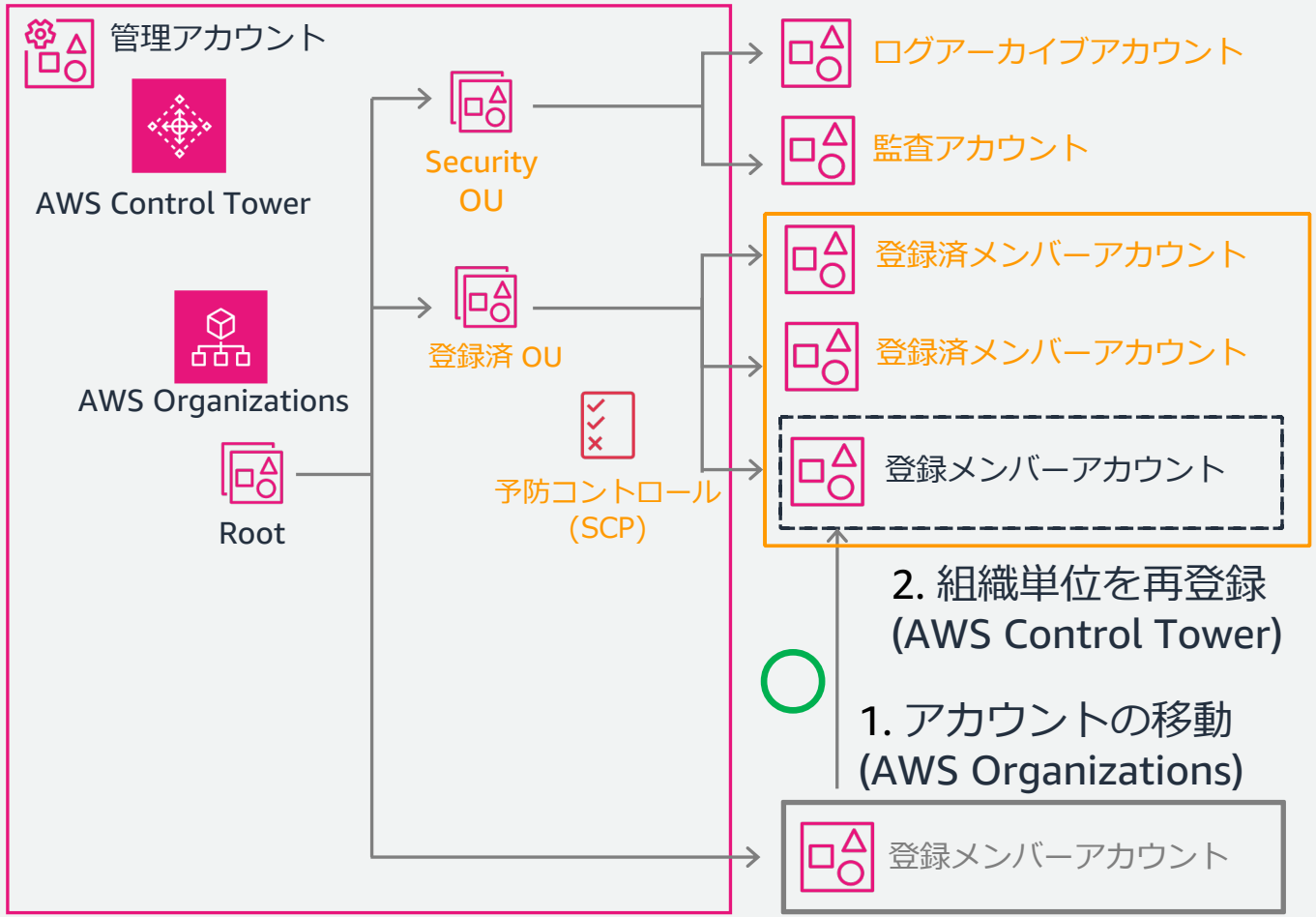
Root 直下のまま AWS Control Tower に登録はできない

1. **先に組織単位を移動して [組織単位を再登録] を実行**
2. [アカウントの登録] を実行し Account Factory によって 組織単位を移動

推奨

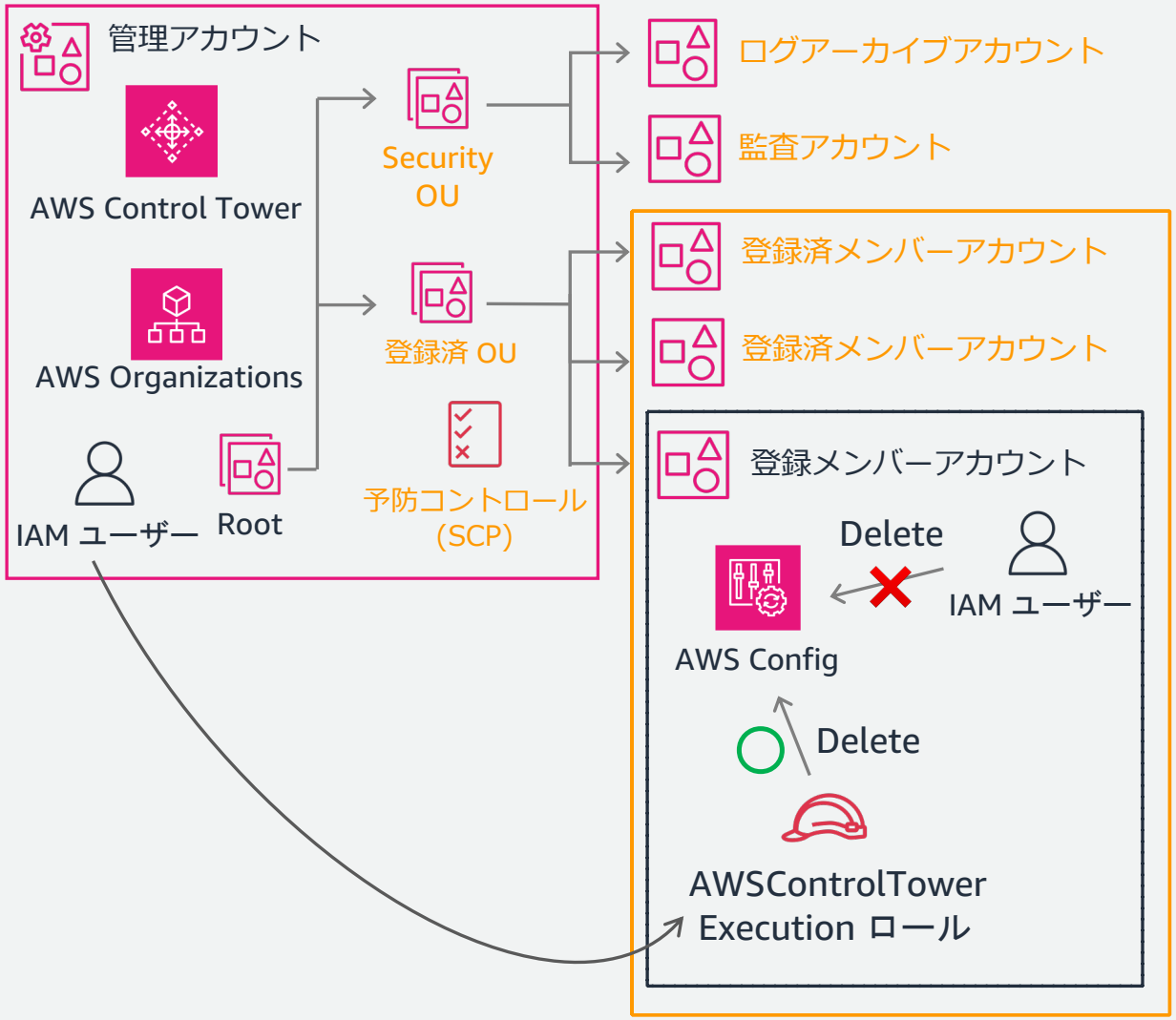
(推奨) 組織単位の再登録

- [組織単位を再登録] の実行で組織単位に追加した未登録のアカウントも登録可能
- 処理内容は組織単位の登録と同様
  - AWSControlTowerExecution ロールのデプロイ
  - 前提条件を満たしているかの事前チェックを実行
- 基本的に登録済のアカウントに影響はない
  - AWS Control Tower がデプロイしたリソースに変更を加えていない前提



(推奨) 組織単位の再登録

- 留意点
  - 事前チェックの失敗を修正時予防コントロールでアクセスが拒否される場合がある
  - 予防コントロールは AWSControlTowerExecution のアクセスを例外的に許可する
  - **管理アカウントからメンバーアカウントの AWSControlTowerExecution に AssumeRole して修正する**



メンバーアカウントの登録

- アカウント単体の登録も可能
  - 登録時に移動する組織単位を選択する

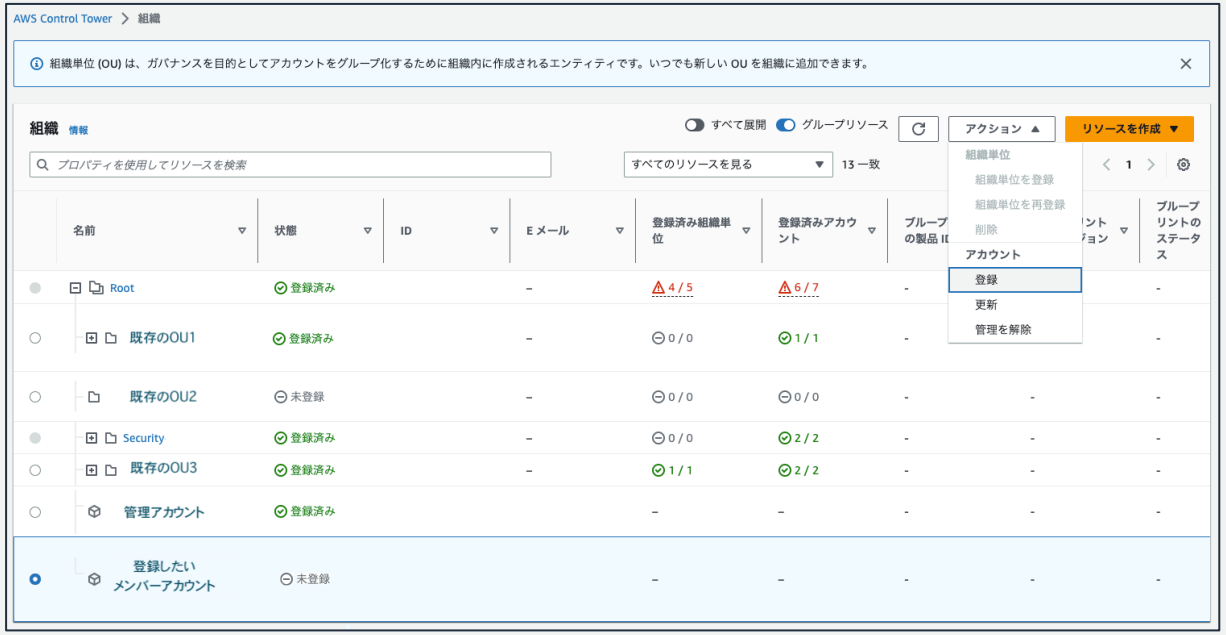
    https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/importing-existing.html

- 制限事項

1. 5 個のアカウントまで同時に登録作業可能

- 事前の実施事項

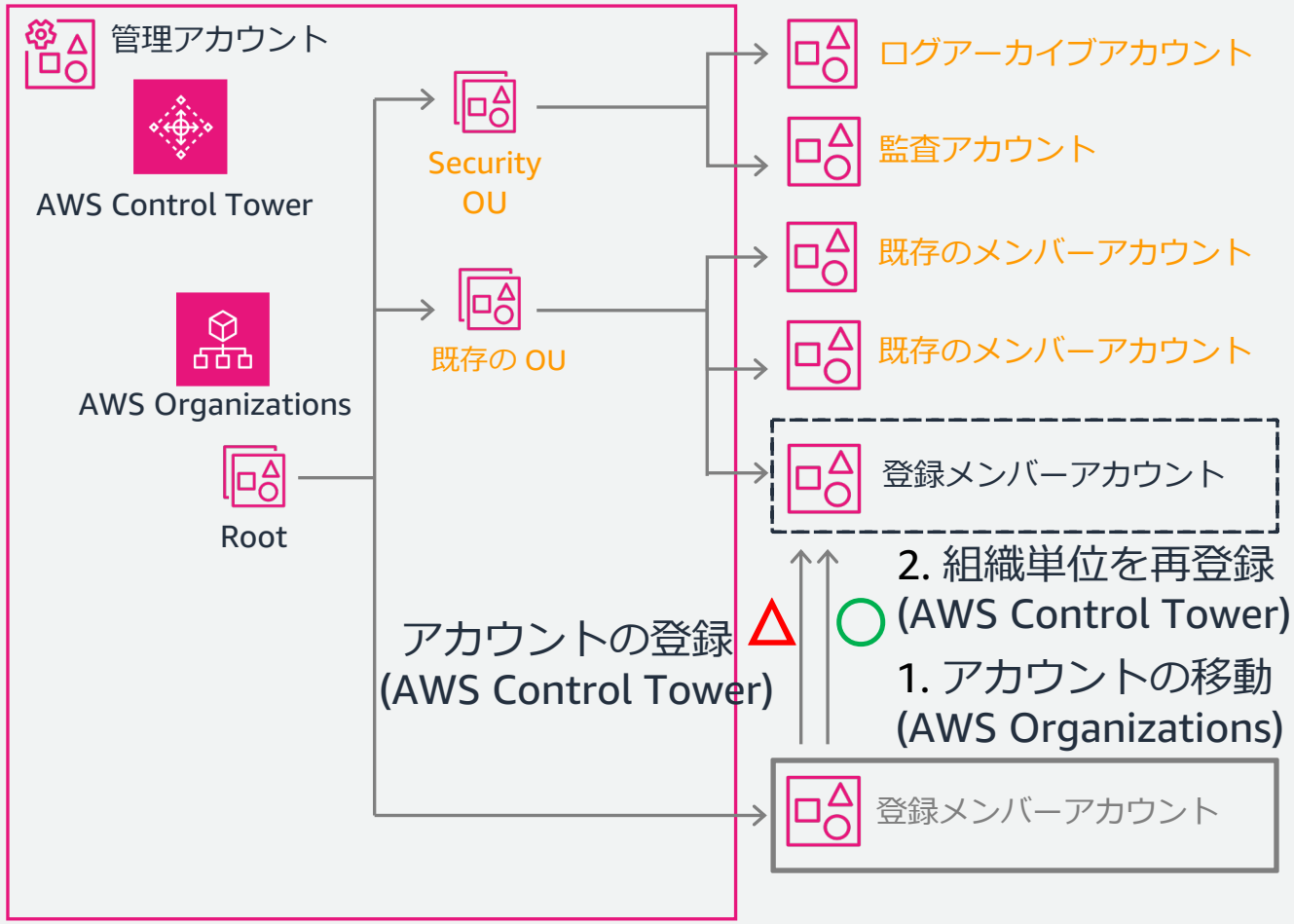
1. メンバーアカウントに AWSControlTowerExecution ロールを手動で作成する
2. 事前チェックを実施しないため、メンバーアカウントが登録前提条件を満たしているか利用者で確認する必要がある



組織単位の再登録を推奨する理由

[組織単位の再登録] の利点

- 複数のメンバーアカウント登録が簡単
  - **5 つを超えるアカウント数でも順次登録可能**
- アカウントの登録に比べて必要手順が簡潔
  - **AWSControlTowerExecution ロールを自動で作成してくれる**
- 登録可能性と必要な修正の確認が容易
  - **登録の前提条件を満たしているかの事前チェックが可能**



メンバーアカウントの登録

1.3 AWS Config を有効化済みの AWS アカウントの登録申請

AWS Config が有効化済みのアカウントの登録申請

- 管理対象リージョンに AWS Config 設定レコーダー・配信チャネルがある
  - 基本的には AWS Control Tower に登録できない
  - **サポートケースでの申請で例外的に登録できるよう許可リストに加えられる**
  - **管理アカウントからの 1 サポートケースで複数のメンバーアカウントについて申請可能**
  - **申請後、本来 AWS Control Tower が作成する AWS Config の設定と一致するよう変更してから組織単位の登録・再登録を行う**

    https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/existing-config-resources.html
  - 申請以外の作業を自動化した blog もご一読ください https://aws.amazon.com/jp/blogs/mt/automate-enrollment-of-accounts-with-existing-aws-config-resources-into-aws-control-tower/
  - **(注意点) AWS Control Tower は AWS Config リソースを管理・更新・修復しない**

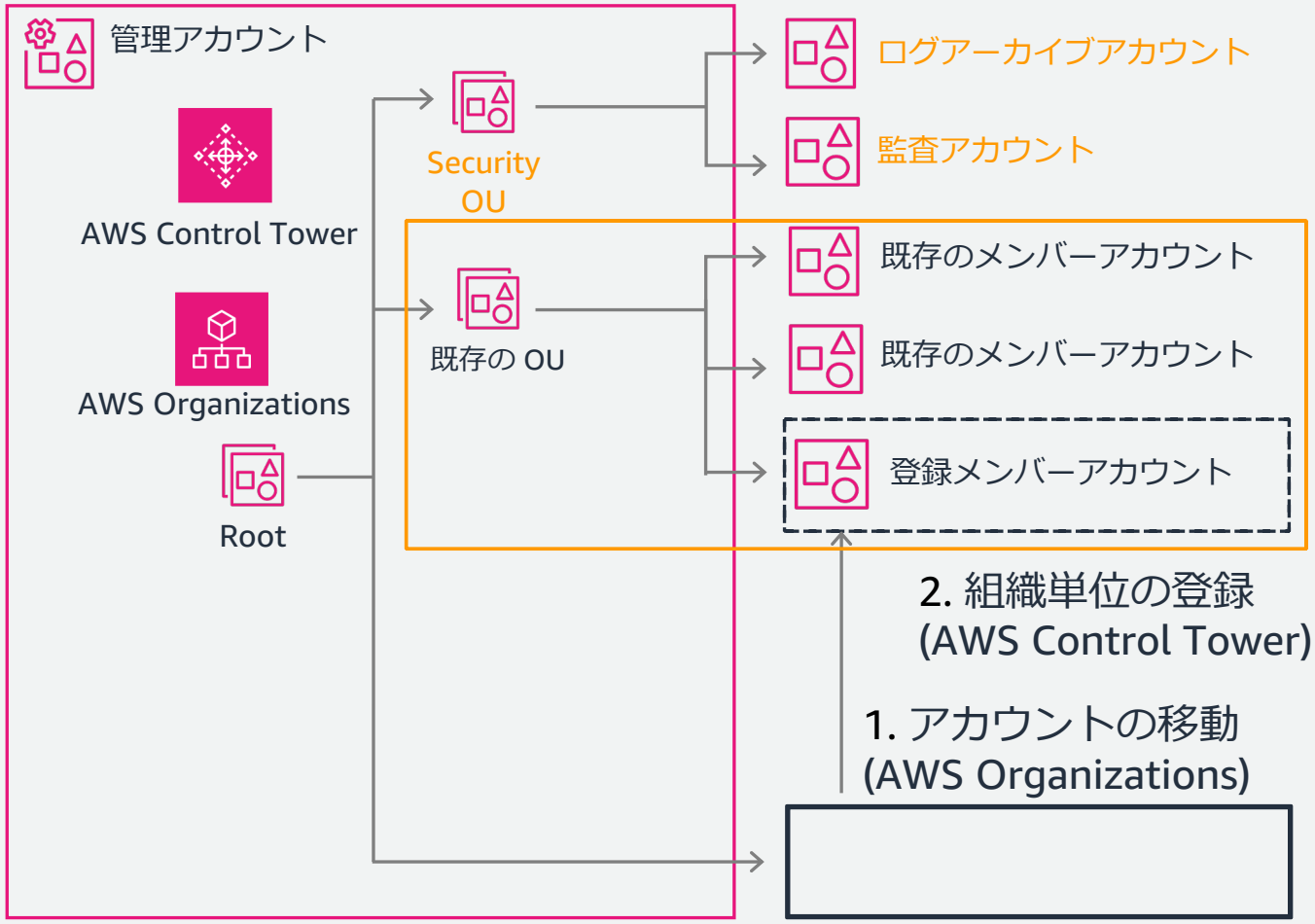
1. ケースの作成時
   技術
   サービス: Control Tower
   カテゴリ: Migration (Account/Organization)
2. ケースの件名
   既存の AWS Config リソースを持つアカウントを AWS Control Tower に登録する
3. ケースの本文に記載する内容
   管理アカウントの ID (12 桁の数字)
   AWS Config リソースを持つメンバーアカウント ID
   AWS Control Tower のホームリージョン

メンバーアカウントの登録

1.4 登録手順のまとめ

まとめ: 既存の組織単位・メンバーアカウントの登録手順

1. **Root 直下のアカウントは登録したい組織単位へ移動する**
2. **組織単位の登録を実行**
3. 事前チェックに失敗した場合:
   1. レポートをダウンロードして対処方法を確認
   2. AWS Config 有効化済みによるエラー:
      - AWS Control Tower で設定レコーダー配信チャネルを作成・管理する場合: **AWSControlTowerExecution ロールで AWS Config リソースを削除**
      - 既存の設定レコーダー・配信チャネルを用いて利用者で管理する場合: **サポートケースで申請**
4. 事前チェックのエラーへの対処後 **組織単位の登録を再度実行**



Thank you!

Appendix

- 参考となる公式ドキュメント
  - Control Tower がサポートするリージョン
    https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/region-how.html
  - ランディングゾーンのセットアップ前の自動チェック
    https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/getting-started-prereqs.html
  - AWS KMS キーに設定するキーポリシー
    https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/configure-kms-keys.html
  - 組織単位の登録・再登録時の事前チェックとよくあるエラー原因
    https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/common-eg-failures.html

Appendix

- AWS Config 設定レコーダー・配信チャネルの削除
  - AWS CLI でのみ削除可能
    https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/using-aws-with-cloudshell.html
    - リソースのステータスを確認 (リソース名をメモしてください)
      $ aws configservice describe-delivery-channels
      $ aws configservice describe-delivery-channel-status
      $ aws configservice describe-configuration-recorders
    - 設定レコーダーを停止
      $ aws configservice stop-configuration-recorder --configuration-recorder-name <NAME-FROM-DESCRIBE-OUTPUT>
    - 配信チャネルと設定レコーダーを削除
      $ aws configservice delete-delivery-channel --delivery-channel-name <NAME-FROM-DESCRIBE-OUTPUT>
      $ aws configservice delete-configuration-recorder --configuration-recorder-name <NAME-FROM-DESCRIBE-OUTPUT>