



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

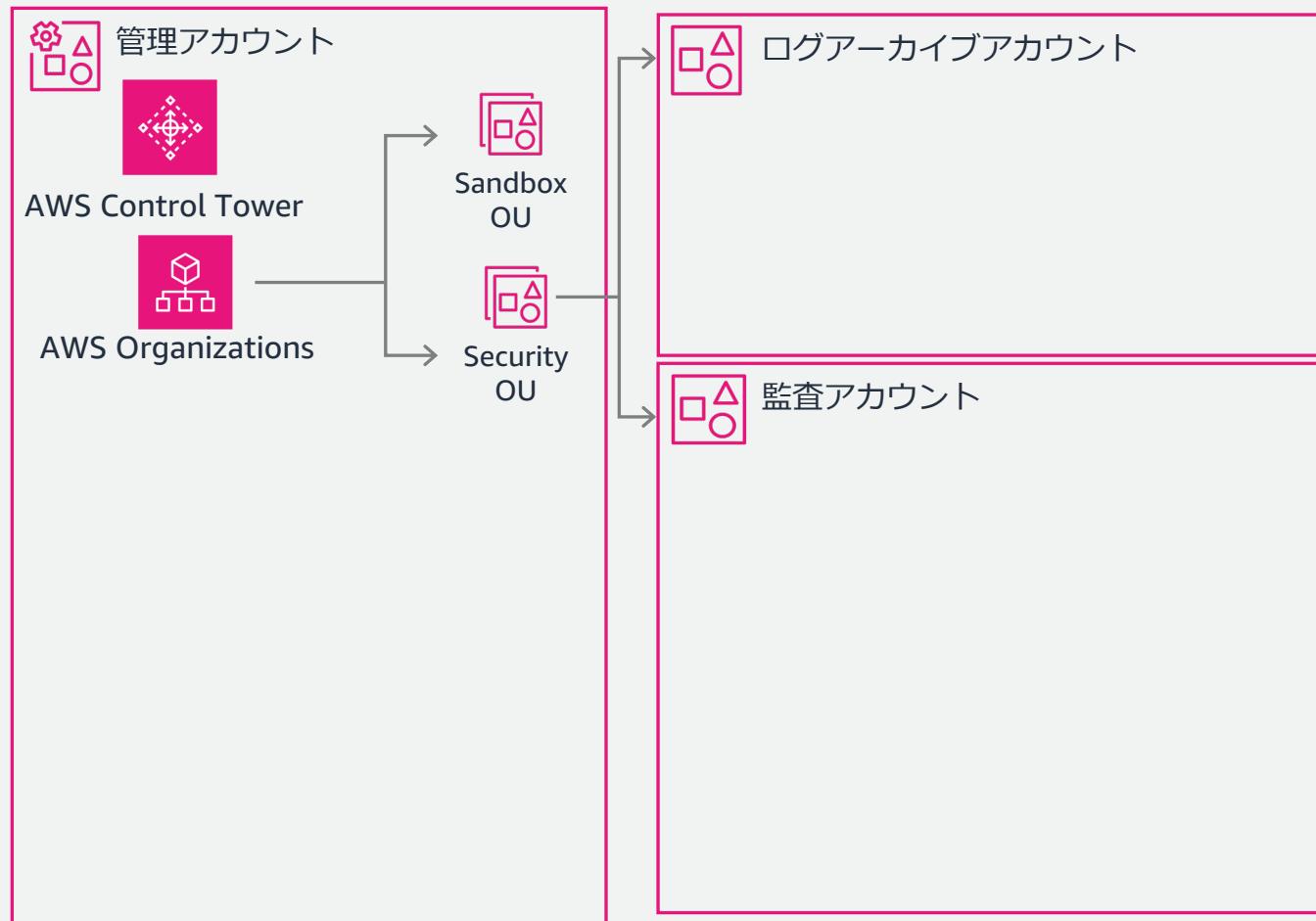
アジェンダ

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

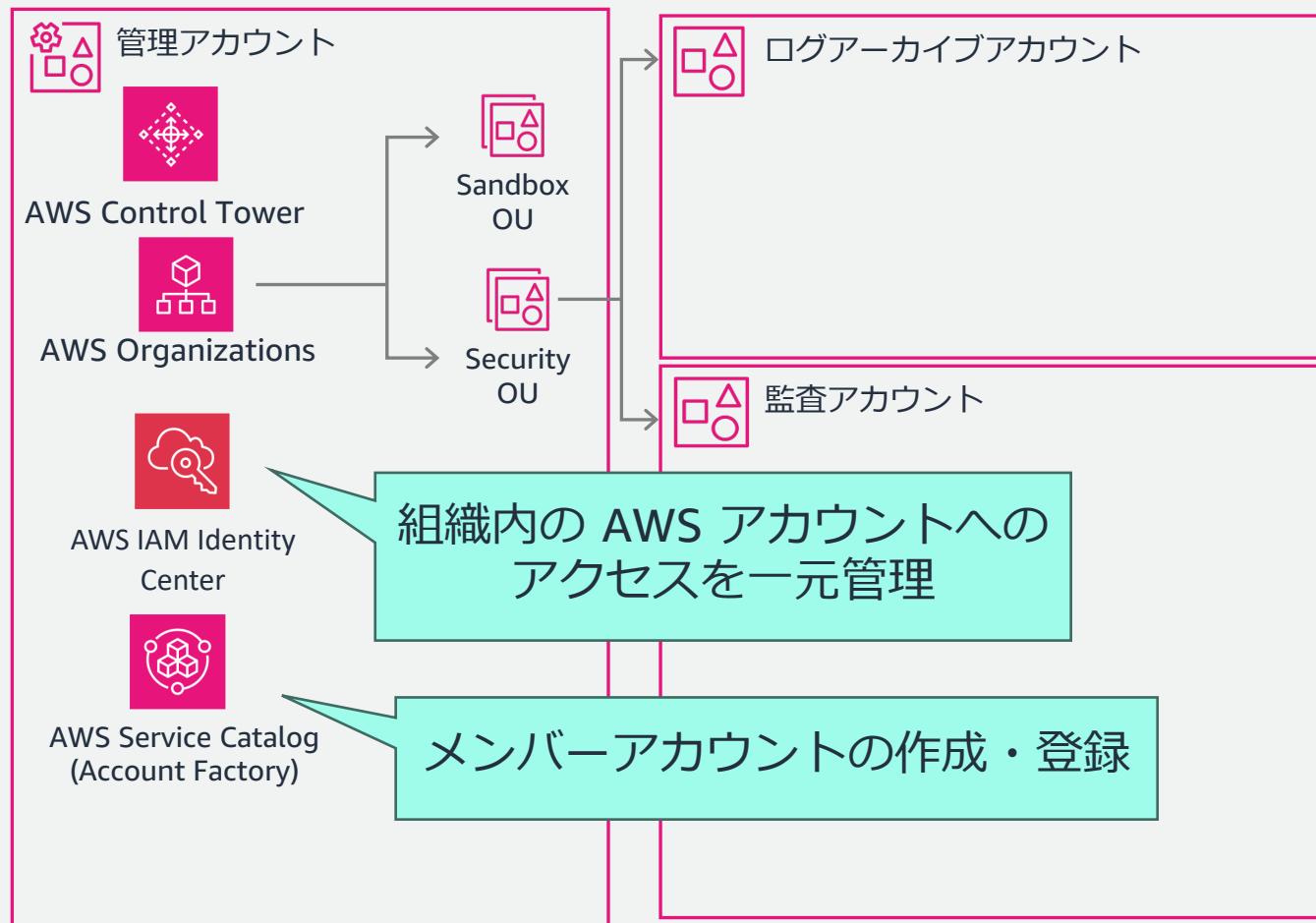
ランディングゾーンの セットアップ

1.1 AWS Control Tower ランディングゾーンの概要

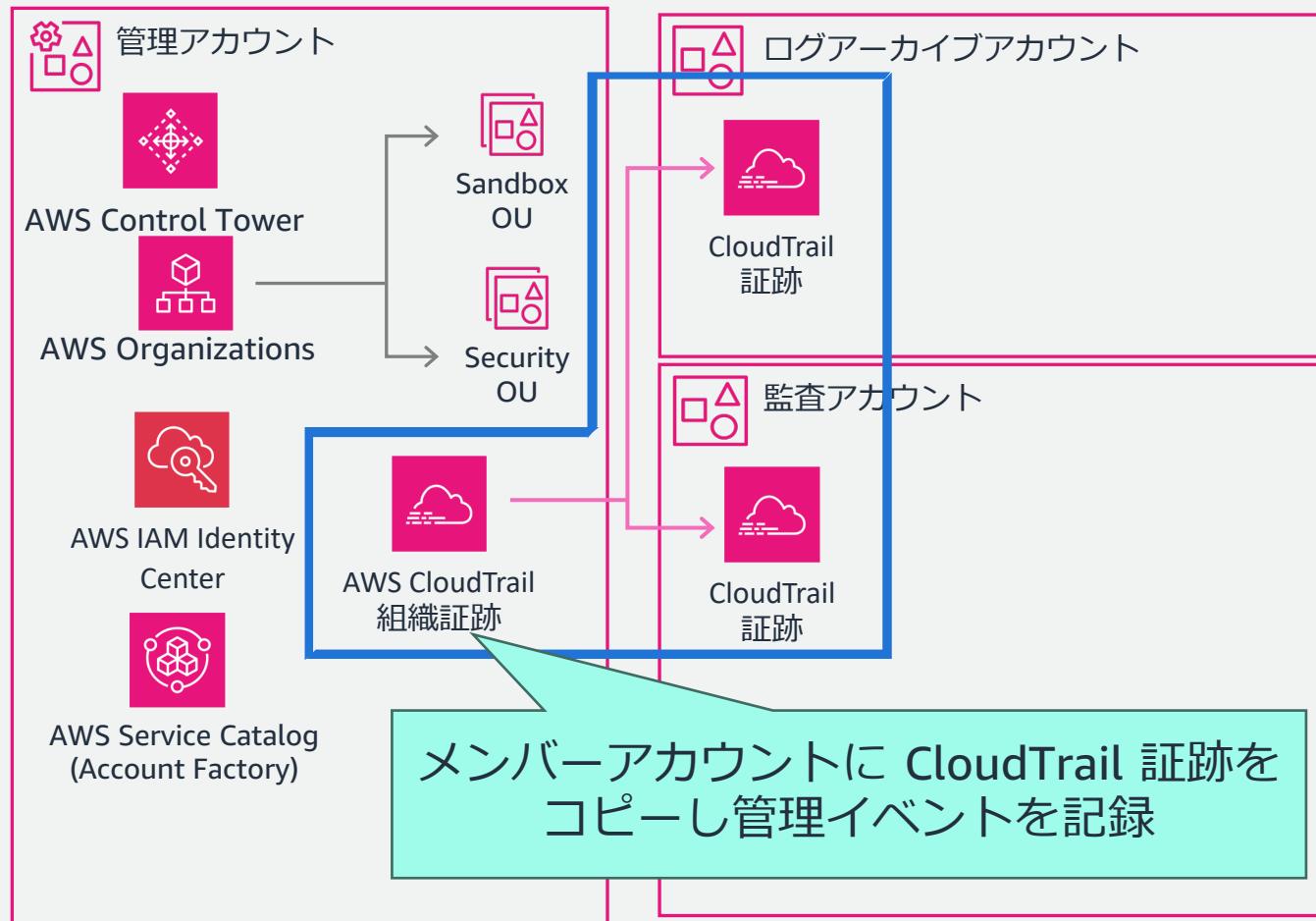
AWS Control Tower が管理アカウントで以下を実行



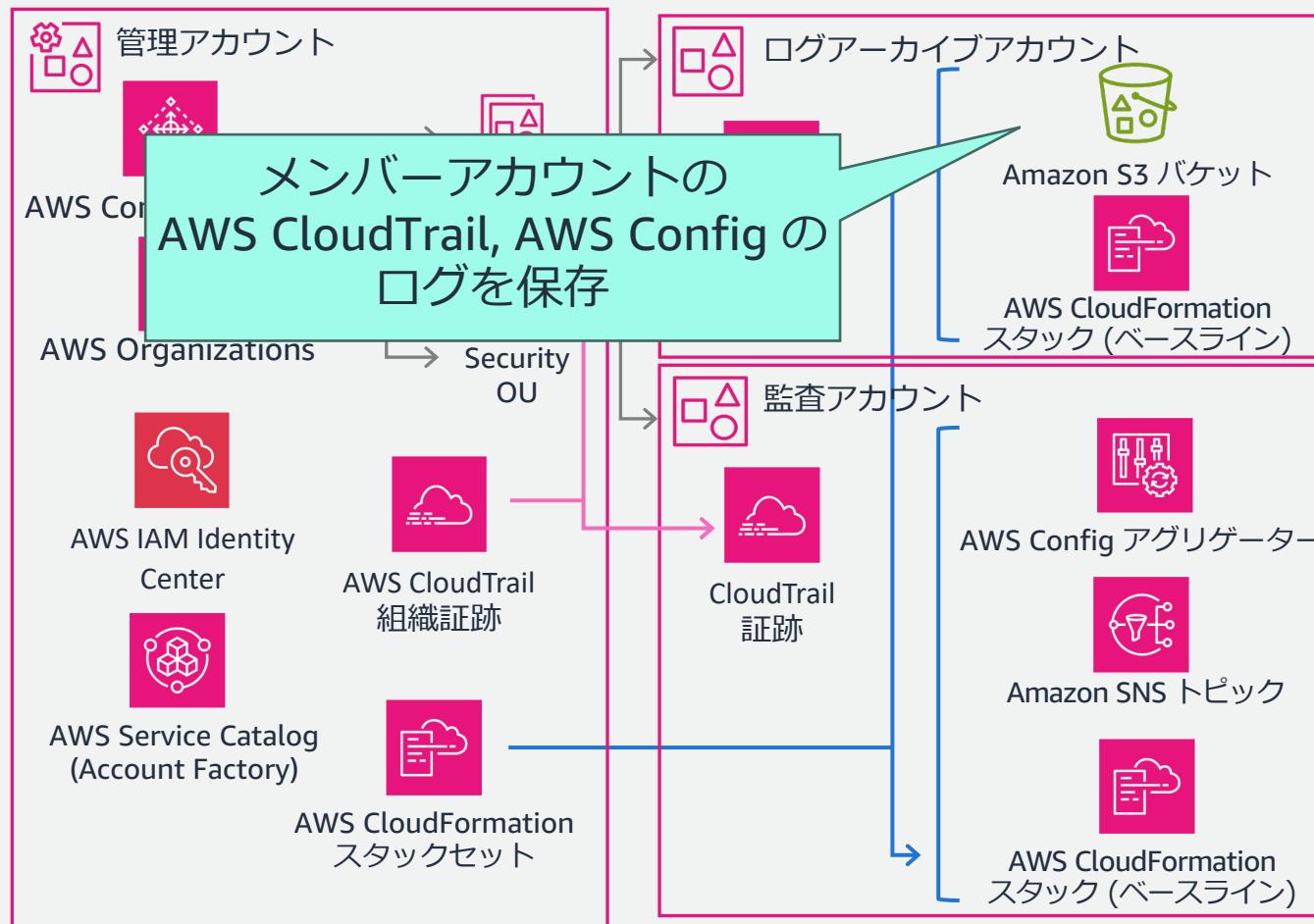
AWS Control Tower が管理アカウントで以下を実行



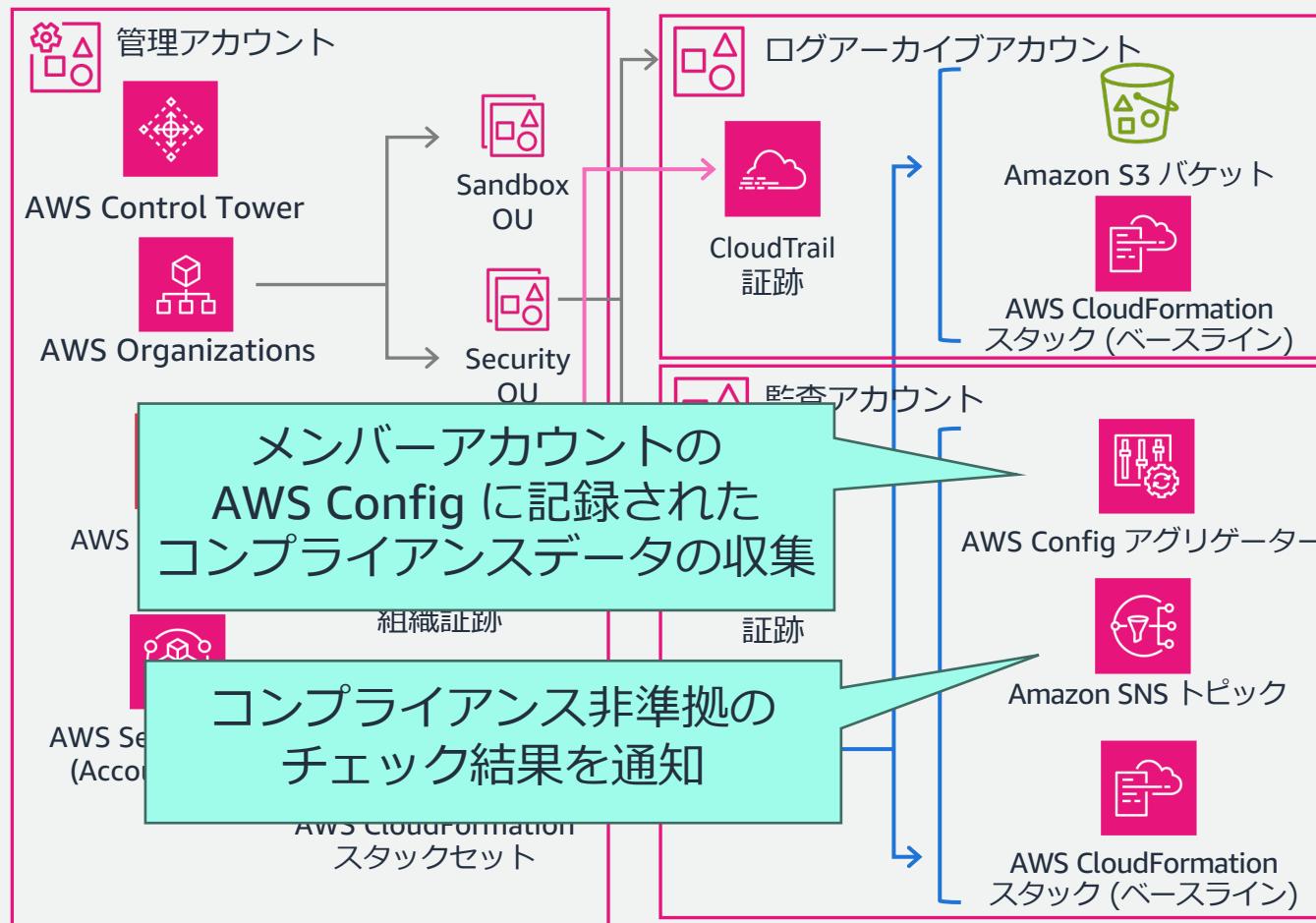
AWS Control Tower が管理アカウントで以下を実行



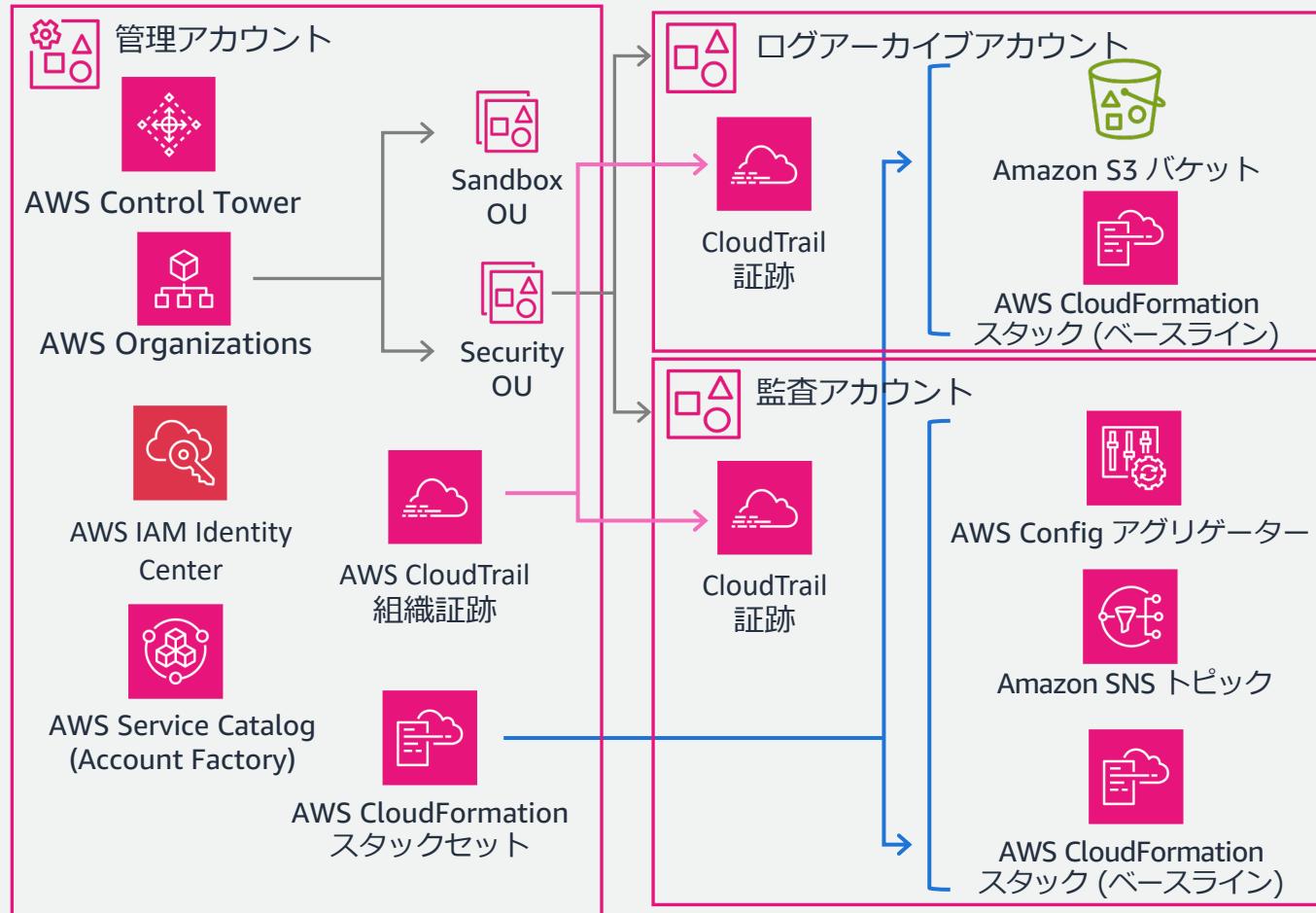
AWS Control Tower が管理アカウントで以下を実行



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 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 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/controlltower/latest/userguide/best-practices.html

ポリシーの詳細	
名前	FullAWSAccess
ARN	arn:aws:organizations::aws:policy/service_control_policy/p-FullAWSAccess
ポリシータイプ	サービスコントロールポリシー (AWS マネージド)
説明	Allows access to every operation

コンテンツ	ターゲット
<pre>{\n "Version": "2012-10-17",\n "Statement": [\n {\n "Effect": "Allow",\n "Action": "*",\n "Resource": "*"\n }\n]\n}</pre>	

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

① 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/controlltower/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

リージョン名	エンドポイント	STS ステータス
グローバルエンドポイント	https://sts.amazonaws.com	常にアクティブ
米国東部 (バージニア北部)	https://sts.us-east-1.amazonaws.com	常にアクティブ
アジアパシフィック (東京)	https://sts.ap-northeast-1.amazonaws.com	● アクティブ
アジアパシフィック (ソウル)	https://sts.ap-northeast-2.amazonaws.com	● アクティブ
アジアパシフィック (大阪)	https://sts.ap-northeast-3.amazonaws.com	● アクティブ
アジアパシフィック (ムンバイ)	https://sts.ap-south-1.amazonaws.com	● アクティブ
アジアパシフィック (シンガポール)	https://sts.ap-southeast-1.amazonaws.com	● アクティブ
アジアパシフィック (シドニー)	https://sts.ap-southeast-2.amazonaws.com	● アクティブ
カナダ (中部)	https://sts.ca-central-1.amazonaws.com	● アクティブ
欧州 (フランクフルト)	https://sts.eu-central-1.amazonaws.com	● アクティブ
欧州 (ストックホルム)	https://sts.eu-north-1.amazonaws.com	● アクティブ
欧州 (アイルランド)	https://sts.eu-west-1.amazonaws.com	● アクティブ
欧州 (ロンドン)	https://sts.eu-west-2.amazonaws.com	● アクティブ
欧州 (パリ)	https://sts.eu-west-3.amazonaws.com	● アクティブ
南米 (サンパウロ)	https://sts.sa-east-1.amazonaws.com	● アクティブ

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

ホームリージョン

AWS リージョンセレクター、または以下のドロップダウンからリージョンを選択して AWS Control Tower のホームリージョンを選択します。これは、共有アカウントのリソースがプロビジョニングされるデフォルトのリージョンです。

ランディングゾーンの設定後にホームリージョンを変更することはできません。

アジアパシフィック (東京)

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

ガバナンスのための追加リージョンを選択 (1/22) [情報](#) [C](#)

AWS Control Tower によるガバナンスのための追加リージョンを選択します。ホームリージョンは自動的に選択され、選択を解除することはできません。ステータスが「非アクティブ」のリージョンを選択すると、AWS Control Tower はセットアップ中に自動的にリージョンをアクティビ化します。

① AWS Control Tower のランディングゾーンは、ワークフローを実行する必要がある AWS リージョンにのみ拡張することをお勧めします。

AWS Control Tower の一部のコントロールは、すべての AWS リージョンで利用できるわけではありません。詳細については、次をご覧ください: [コントロールの制限](#). [\[リンク\]](#)

- AWS Security Hub コントロールは、バーレーン (me-south-1)、ジャカルタ (ap-southeast-3)、ケープタウン (af-south-1)、香港 (ap-east-1)、大阪 (ap-northeast-3)、ミラノ (eu-south-1) ではご利用いただけません。
- ジャカルタ (ap-southeast-3)、ケープタウン (af-south-1)、大阪 (ap-northeast-3)、ミラノ (eu-south-1)、および北カリフォルニア (us-west-1) では 16 件の検出コントロールがご利用いただけません。

リージョン名	リージョンコード	AWS Control Tower ステータス	AWS リージョンのステータス
アジアパシフィック (東京) [ホームリージョン]	ap-northeast-1	管理対象外	デフォルトでアクティブ
米国東部 (バージニア北部)	us-east-1	管理対象外	デフォルトでアクティブ
米国東部 (オハイオ)	us-east-2	管理対象外	デフォルトでアクティブ

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/controlltower/latest/userguide/data-residency-controls.html#primary-region-deny-policy

リージョン拒否設定 [情報](#)

AWS Control Tower のステータスが [管理対象外] と表示されている AWS リージョン、および AWS Control Tower が利用できないリージョンで、AWS のサービスおよびオペレーションへのアクセスを拒否できます。ホームリージョンへのアクセスを拒否することはできません。リージョン拒否コントロールから免除される AWS のサービスを選択します。

⚠️ リージョン拒否機能は、AWS Control Tower のリージョン設定に基づいて AWS のサービスへのアクセスを禁止します。ステータスが [管理対象外] の AWS リージョンへのアクセスが拒否されます。リージョン拒否機能は、AWS Control Tower が利用できないリージョンへのアクセスも拒否します。この設定は後で変更できます。

コントロールの適用後はリソースにアクセスできなくなるため、リージョン拒否コントロールを有効にする前に、これらのリージョンに既存のリソースがないことを確認してください。**有効** を選択すると、AWS Control Tower はすべての登録済みの OU に [リージョン拒否予防コントロール](#) を適用します。

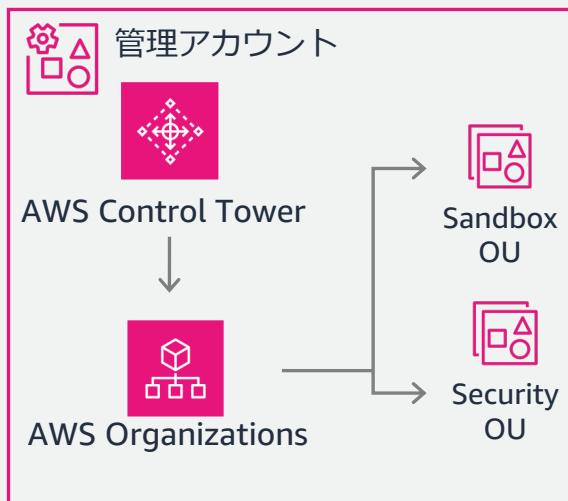
有効 を選択すると、AWS Control Tower は登録済みの OU のコントロールを削除します。すべての管理対象外リージョンは [管理対象外] のステータスのままであり、AWS Control Tower が利用できないリージョンにリソースをデプロイできます。

有効 有効になっていません

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



基礎となる OU

AWS Control Tower は、ランディングゾーンで適切に計画された OU 構造を開始するために、ユーザー用のセキュリティ OU をセットアップします。この OU には、ログアーカイブアカウントとセキュリティ監査アカウント (監査アカウントとも呼ばれます) の 2 つの共有アカウントが含まれています。

OU 名を変更 - オプション

「Security」は、共有アカウントについてのデフォルト OU 名です。OU 名は一意である必要があります、ランディングゾーンのセットアップ後に編集できます。

Security

追加の OU

マルチアカウントシステムのセットアップをサポートするために、AWS Control Tower はランディングゾーンのセットアップ時にセカンダリ OU を作成することを推奨します。この OU は、任意のプロダクションアカウントまたは開発アカウントを保存するために使用できます。追加の OU は、ランディングゾーンのセットアップ後に作成することができます。

新しい OU を作成 - 推奨

OU の作成をオプトアウト

新しい OU を作成 - 推奨

OU 名を変更 - オプション

「Sandbox」は、追加 OU についてのデフォルト OU 名です。OU 名は一意である必要があります、ランディングゾーンのセットアップ後に編集できます。

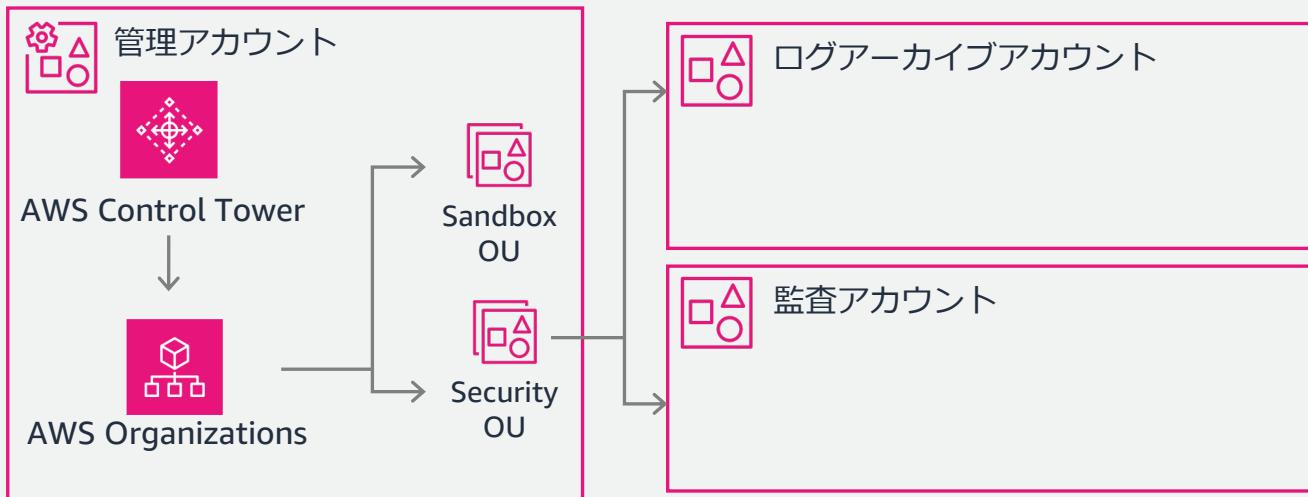
Sandbox

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/>



ログアーカイブアカウント

ログアーカイブアカウントは、すべてのアカウントの API アクティビティとリソース設定の immutable ログのリポジトリです。

新規アカウントの作成
ログアーカイブアカウント用の新しいメールアドレスを作成します。この E メールアドレスを既存の AWS アカウントで使用することはできません。

既存のアカウントの使用
組織に存在する ログアーカイブアカウント のアカウント ID を入力します。

AWS Organizations に存在するアカウント ID を入力します
xxxxxxxxxxxxxx
12 行の数字である必要があります。アカウントの桁数が 12 行未満の場合は、先頭にゼロを追加します。

既存の AWS アカウントの詳細

アカウント E メール
-

アカウント名
-

アカウントの監査

監査アカウントは制限付きアカウントです。これにより、セキュリティおよびコンプライアンスチームは、組織内のすべてのアカウントへのアクセスを取得できます。

新規アカウントの作成
アカウントの監査用の新しいメールアドレスを作成します。この E メールアドレスを既存の AWS アカウントで使用することはできません。

既存のアカウントの使用
組織に存在する アカウントの監査 のアカウント ID を入力します。

アカウントの作成
audit@example.com
監査アカウント E メールアドレスを既存の AWS アカウントで使用することはできません。さらに、6~64 文字である必要があります。
アカウント名を変更 - オプション
監査アカウント名は、他のアカウント名と重複しないようにしてください。ランディングゾーンをセットアップした後で名前を編集することはできません。

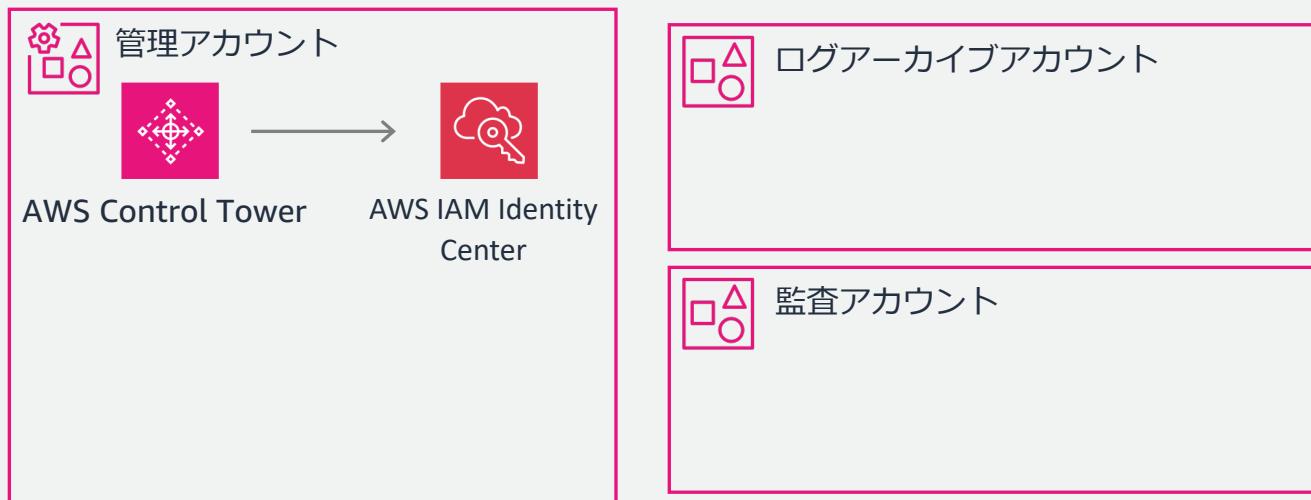
Audit

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/controlltower/latest/userguide/sso.html



AWS アカウントアクセス設定 情報
AWS Control Tower に登録されている AWS アカウントへのアクセスを管理する方法を選択します。これは後で変更できます。

AWS Control Tower は IAM Identity Center を使用して AWS アカウントアクセスを設定します。
AWS を使い始めたばかりの場合や、アクセス管理構造が AWS Control Tower のグループとアクセス許可セット  と連携している場合に最適です。後で IAM Identity Center で外部 ID プロバイダー (IdP) に接続できます。

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。
AWS アカウントアクセス管理に関するカスタム要件がある場合に最適です。AWS Control Tower はアカウントアクセスを管理しません。IAM Identity Center または別のアクセス方法を設定する必要があります。

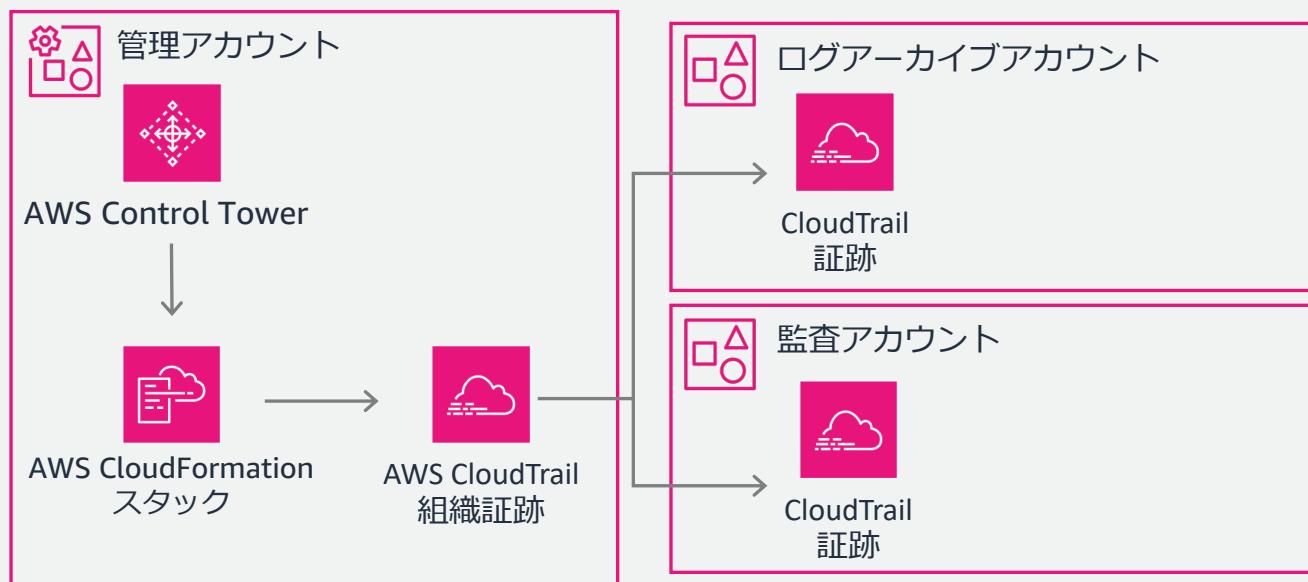
ステップ 4-1: IAM Identity Center による
アクセス設定の有効・無効

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**



AWS CloudTrail の設定 情報

AWS CloudTrail は、AWS Control Tower のアクションをイベントとしてキャプチャします。証跡を作成すると、Amazon S3 バケットへの CloudTrail イベントの継続的デリバリーを有効にできます。

組織レベルの CloudTrail では、AWS Control Tower はすべてのアカウントの情報を組織の証跡に集約し、ログ情報を指定された Amazon S3 バケットに配信します。ファイルパスには、組織 ID がプレフィックスとして含まれています。

⚠️ 組織レベルの CloudTrails を有効にしない場合、AWS Control Tower は AWS CloudTrail ログを管理しません。この設定は、ランディングゾーンを更新するときに変更できます。

AWS Control Tower では、すべての組織またはアカウントが AWS CloudTrail のログ記録を確立することを強く推奨します。AWS Control Tower で管理されないカスタム証跡を作成するか、[有効] を選択できます。必須の検出コントロールは、登録されたアカウントが CloudTrail のログ記録が有効かどうかを検出します。詳細は[こちら](#)

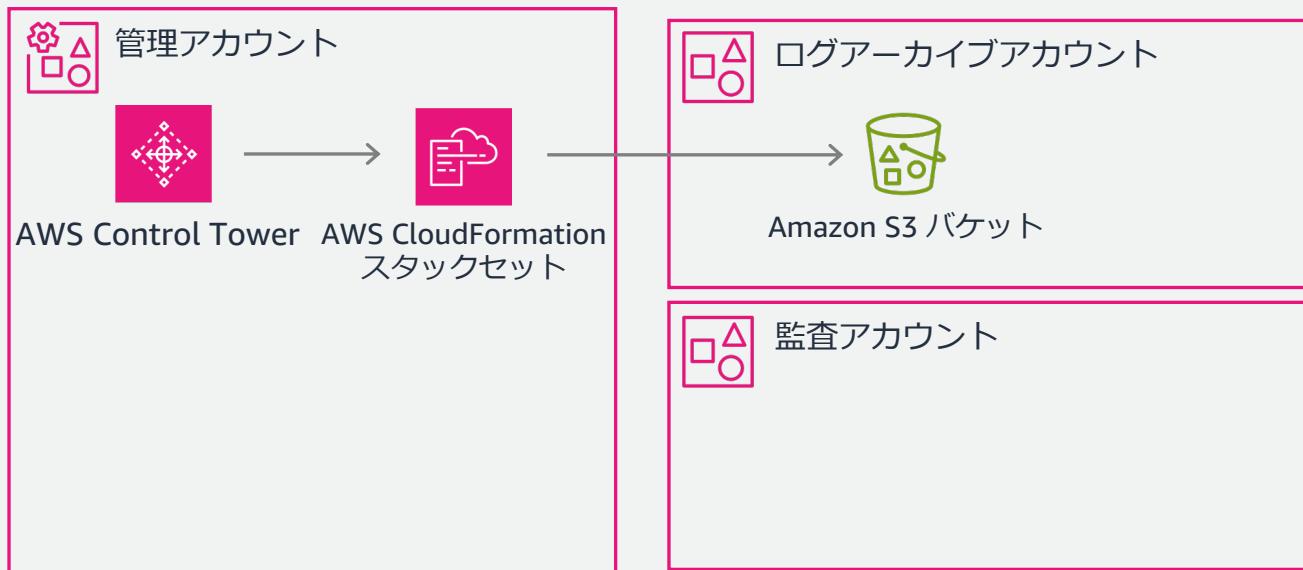
有効

有効になっていません

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



Amazon S3 のログ設定 - オプション 情報

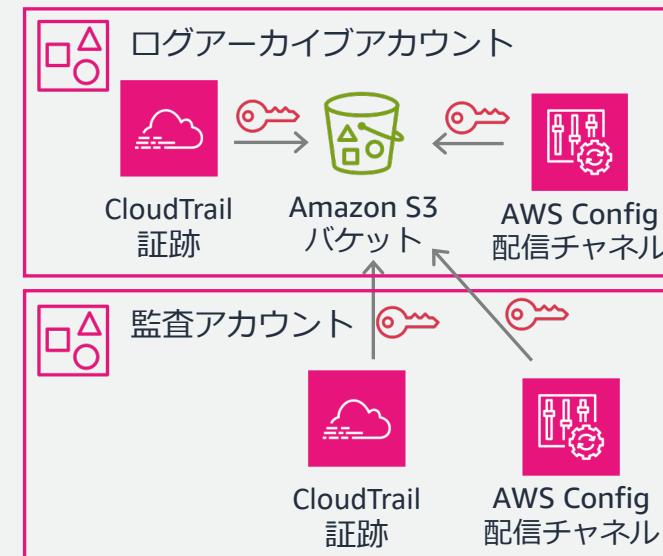
これらの 2 つのフィールドに、Amazon S3 ロギングバケットとアクセスロギングバケットのライフサイクル保持時間を表す数値を入力します。どちらのバケットでも指定できる最小保持時間は 1 日です。年の場合は、小数点以下 2 衆まで表すことができます。日の場合は整数を指定する必要があります。例えば、5 日や 1.02 年を指定できますが、1.34 日は指定できません。1.34 日間を指定する場合は、数値を切り上げるか切り下げるかで整数値にします。1 年未満 (0.02 年など) の期間の場合は、日数に変換してください。

ログ用の Amazon S3 バケットの保持	Format for logging
Default: 1	years
1 ~ 15 の整数と小数点以下 2 衆まで含める必要があります。	
アクセスログ用の Amazon S3 バケットの保持	Format for access logging
Default: 10	years
1 ~ 15 の整数と小数点以下 2 衆まで含める必要があります。	

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



KMS 暗号化 - オプション [情報](#)

AWS Key Management Service (KMS) は、暗号化キーを作成および管理し、AWS Control Tower でリソースをコントロールするのに役立ちます。キーを選択するには、チェックボックスをオンにします。KMS キーには、AWS CloudTrail および AWS Config のアクセス許可が必要です。マルチリージョンキーはサポートされていません。詳細は[こちら](#)

暗号化設定を有効にして、カスタマイズする
暗号化設定を無効にするには、このチェックボックスをオフにします。

AWS KMS カスタマーキーを選択する
このキーは、リソースの暗号化と復号化に使用されます。

AWS KMS キーを選択するか、ARN を入力します。

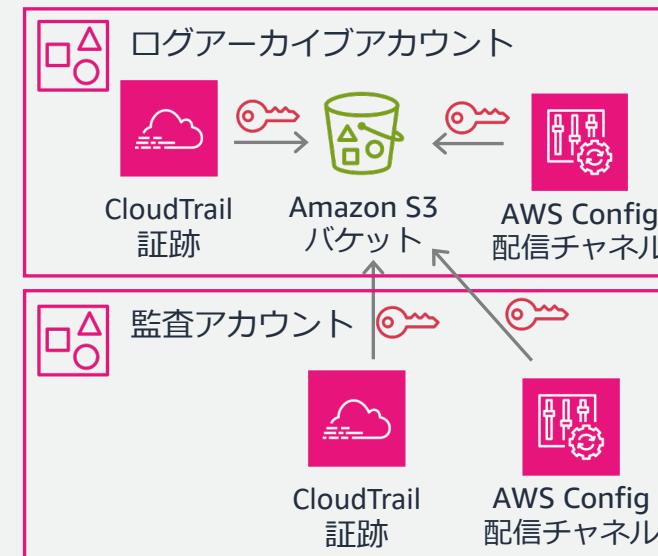
対称キーのみが表示されます。非対称キーはサポートされていません。

[KMS キーを作成する](#)

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
 - 対称な單一リージョンキーか
 - キーにアクセス許可
 - 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



KMS 暗号化 - オプション [情報](#)

AWS Key Management Service (KMS) は、暗号化キーを作成および管理し、AWS Control Tower でリソースをコントロールするのに役立ちます。キーを選択するには、チェックボックスをオンにします。KMS キーには、AWS CloudTrail および AWS Config のアクセス許可が必要です。マルチリージョンキーはサポートされていません。詳細は[こちら](#)。

暗号化設定を有効にして、カスタマイズする
暗号化設定を無効にするには、このチェックボックスをオフにします。

AWS KMS カスタマーキーを選択する
このキーは、リソースの暗号化と復号化に使用されます。

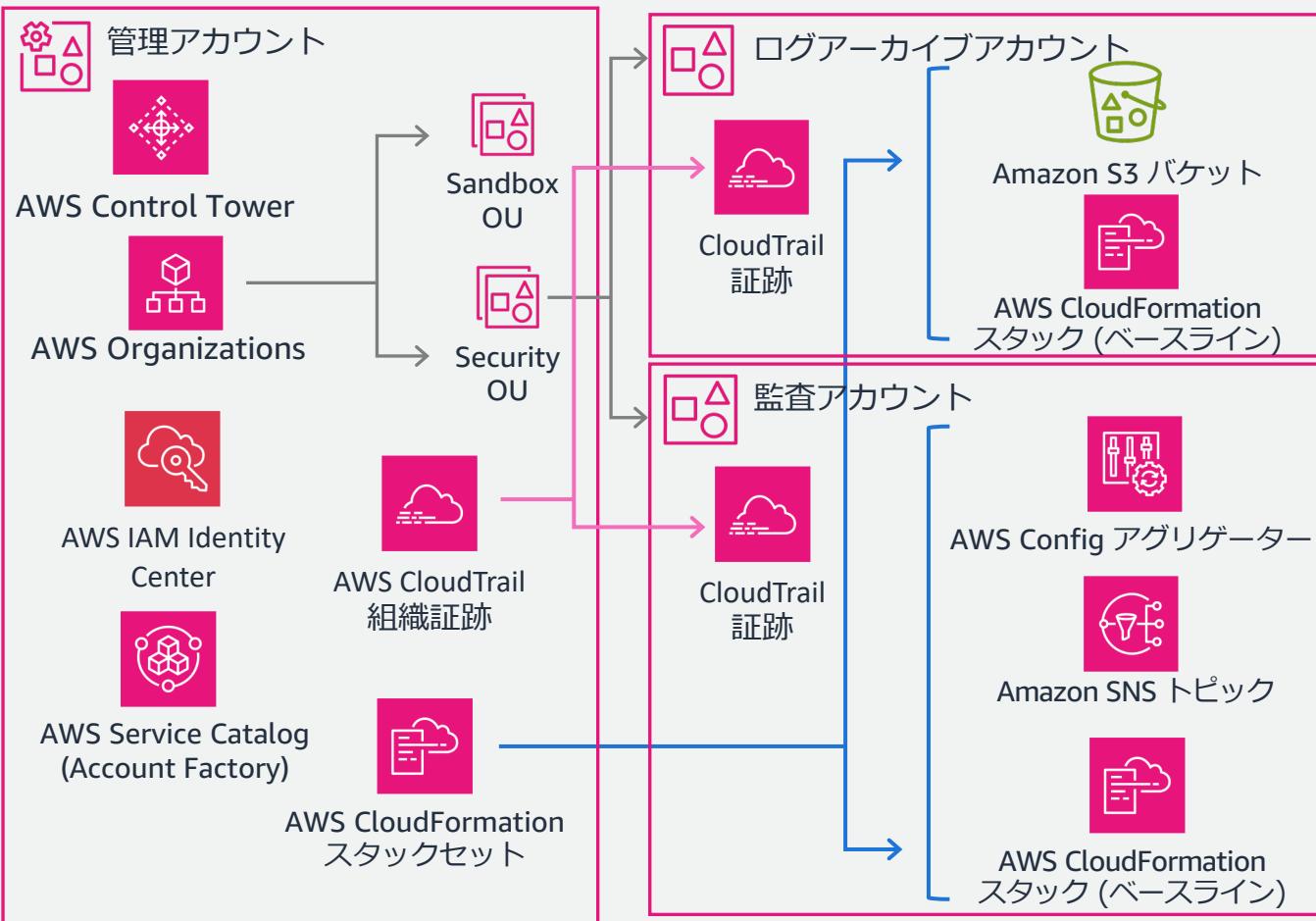
AWS KMS キーを選択するか、ARN を入力します。

対称キーのみが表示されます。非対称キーはサポートされていません。

KMS キーを作成する

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



サービスのアクセス許可

AWS Control Tower には、AWS リソースを管理し、お客様に代わってルールを適用するためのアクセス許可が必要です。

▶ アクセス許可の詳細

▶ ガイダンスの詳細

私は、AWS リソースを管理する目的で、および私に代わってルールを適用する目的で、AWS Control Tower がアクセス許可を使用することを了承しています。また、AWS Control Tower の使用に関するガイダンス、およびその基盤となる AWS リソースについても了承しています。

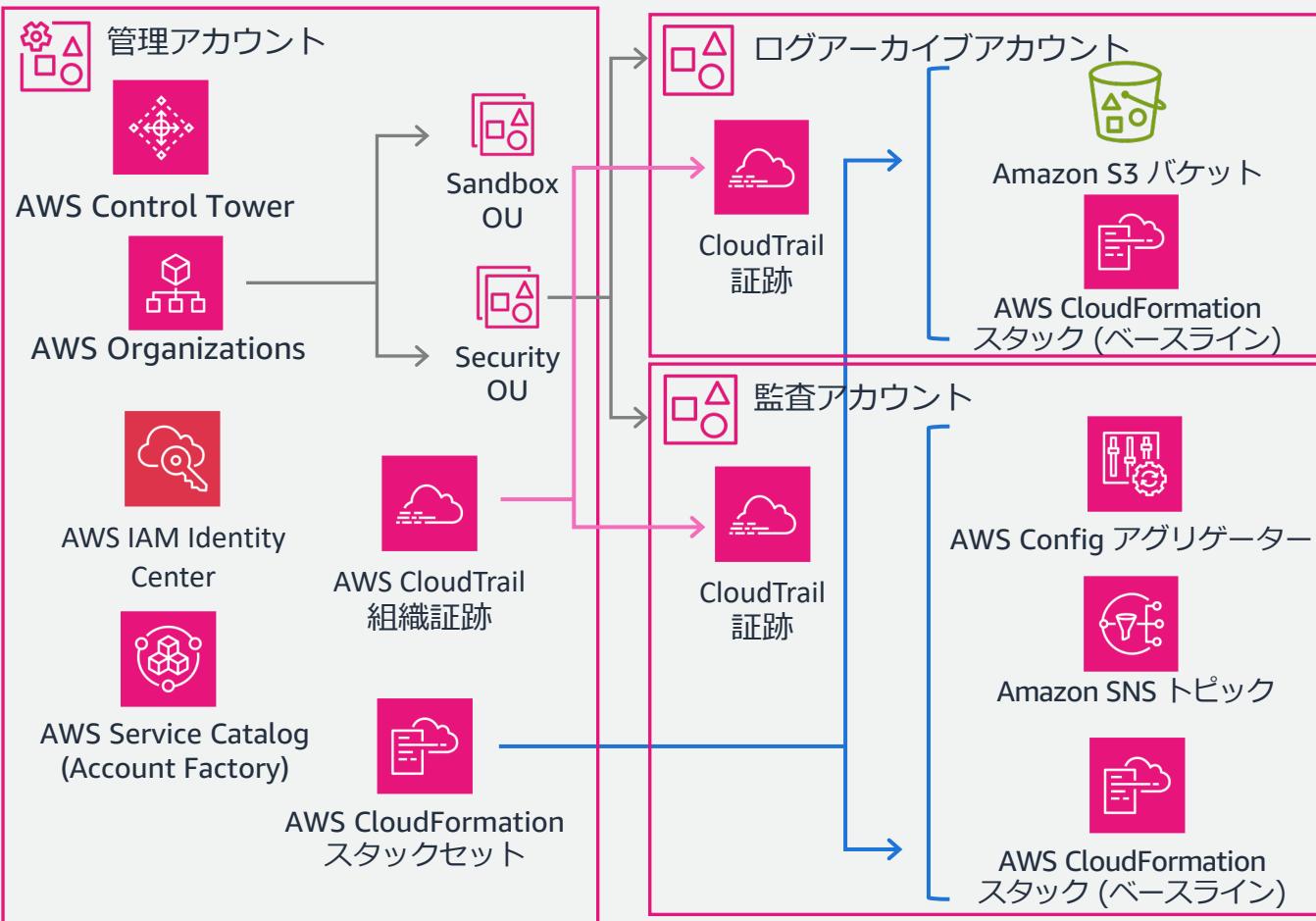
キャンセル

戻る

ランディングゾーンの設定

ステップ 5: セットアップの開始

5. 確認とセットアップ



ランディングゾーンのステータス

詳細	ステータス
セキュリティ OU で、監査とログ記録のための共有アカウントを作成または登録しています	成功
管理アカウント、監査アカウント、およびログ記録アカウントのすべてのユーザー権限を設定しています	成功
AWS Control Tower メンバーアカウントをプロビジョニングするため Account Factory を設定しています	成功
監査アカウントを設定しています	成功
ログアーカイブアカウントを設定しています	成功
組織ユニットで必須のコントロールを有効にする	進行中

セットアップ中、進捗状況を確認可能

⌚ ランディングゾーンの設定が完了しました。

[AWS Control Tower > ダッシュボード](#)

**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

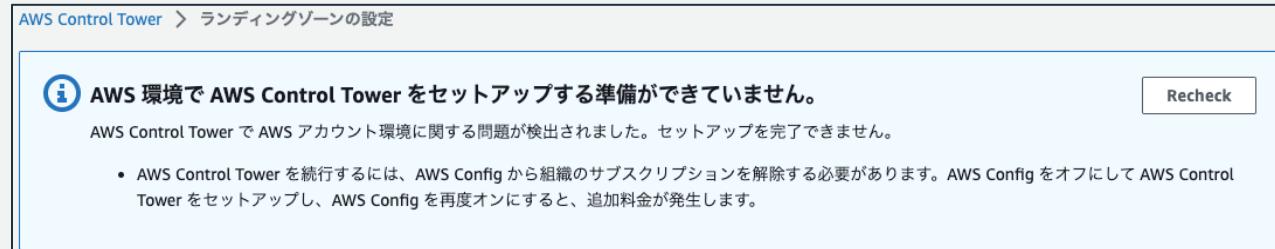
- AWS Control Tower のセットアップ時には事前チェックが実行される

https://docs.aws.amazon.com/ja_jp/controlltower/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

AWS Control Tower > ランディングゾーンの設定

AWS 環境で AWS Control Tower をセットアップする準備ができていません。

AWS Control Tower で AWS アカウント環境に関する問題が検出されました。セットアップを完了できません。

- 現在のアカウントでは、IAM Identity Center が異なるリージョンで設定されています。Identity Center を設定したのと同じホームリージョンで AWS Control Tower ランディングゾーンを設定してください。

Recheck

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

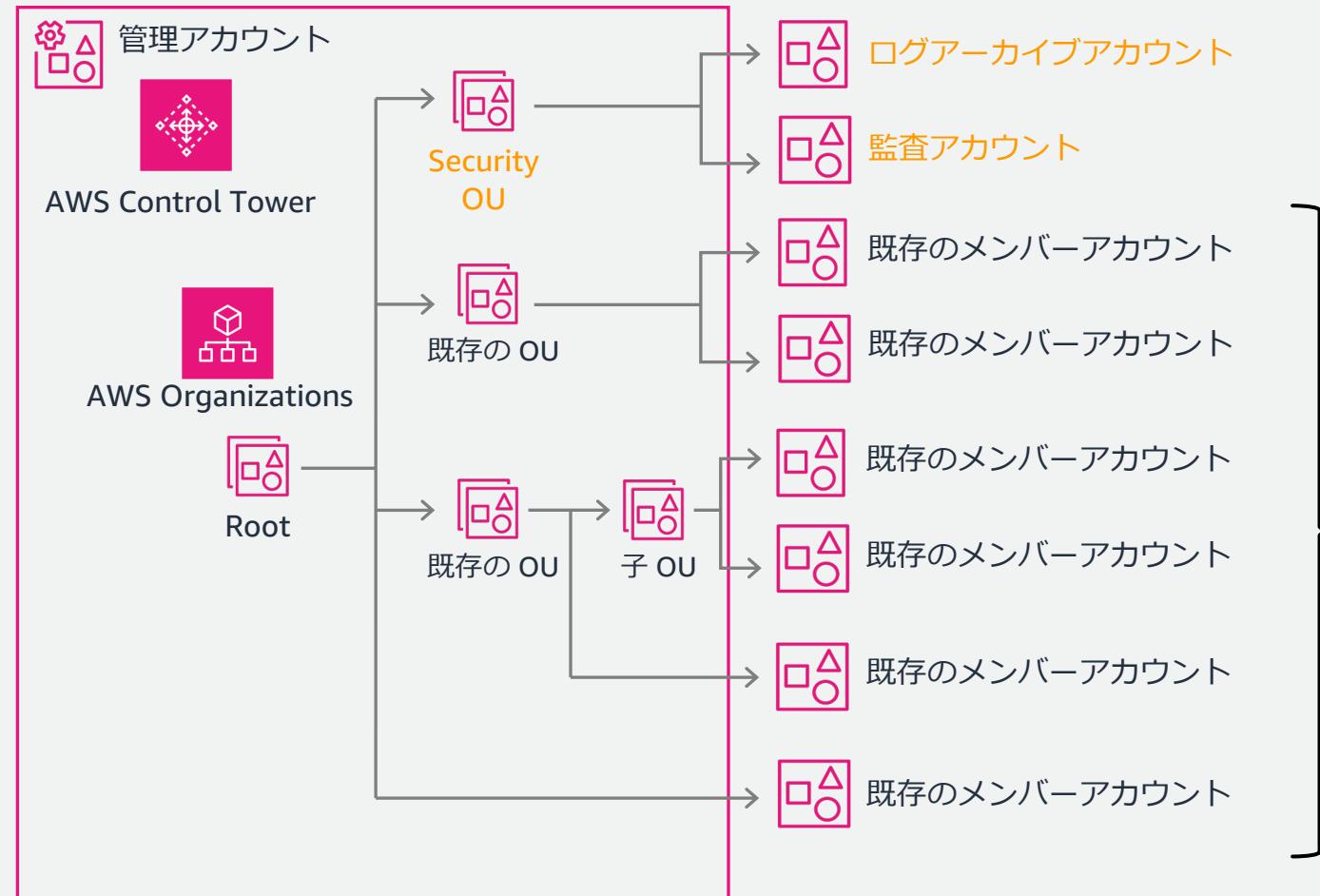
- 管理アカウント
 - 事前チェックなし: **セットアップ前の確認を推奨**
 1. 管理者権限を持つ IAM ユーザー・ロールでセットアップする
 2. Root にリソース作成を妨げる SCP を設定しない
 3. サポートするすべてのリージョンの AWS STS を有効化する
 4. (AWS KMS 暗号化キーを使用する場合)
キーポリシーに正しいアクセス許可があるか・対称な単一リージョンキーか
 - 事前チェックあり: エラー発生後に確認して対応
 1. AWS Config の信頼されたアクセスを無効化する
 2. ホームリージョンと AWS IAM Identity Center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



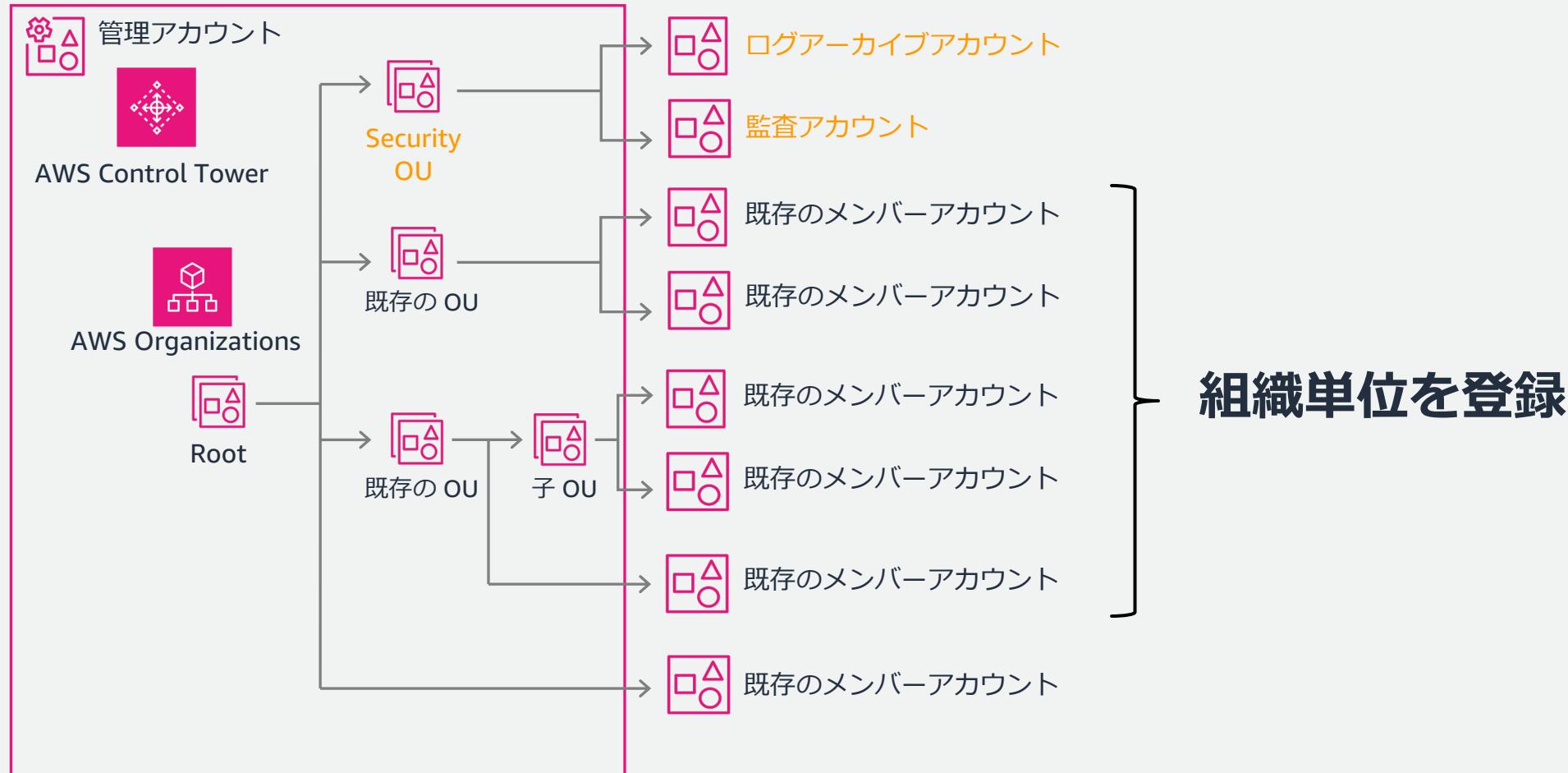
**別途 AWS Control Tower への
登録作業が必要となる**

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/controlltower/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

名前	状態	ID	Eメール	登組	アカウント	登録	更新	管理を解除
Root	登録済み	Root の ID	-					
登録したい既存OU 1	未登録	OU の ID	-					
既存 OU 2	未登録	OU の ID	-	0/0	0/0			
Security	登録済み	OU の ID	-	0/0	2/2			
既存 OU 3	未登録	OU の ID	-	0/1	0/2			
管理アカウント	登録済み	アカウント ID	アカウントのメールアドレス	-	-	-	-	-

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

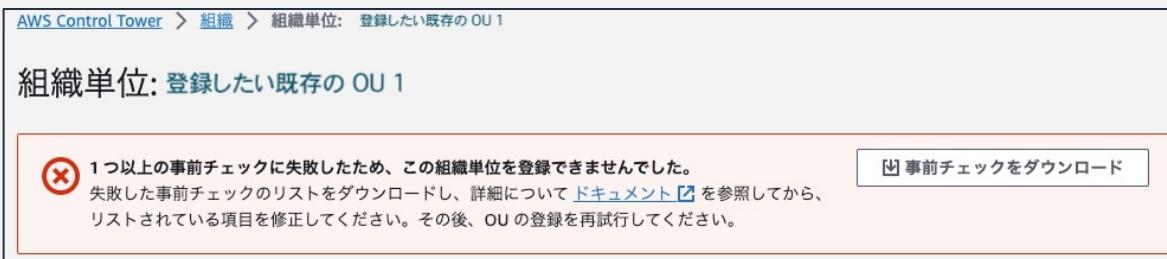
組織単位への事前チェック

- 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
- 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
- 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
- 登録を妨げるSCP があるか

など

組織 情報		すべて展開	グループリソース	G	アクション ▾	リソースを作成 ▾
名前		状態	ID	E メール	登録済み組織単位	登録済みアカウント
●	□ Root	登録済み	Root の ID	-	△ 3 / 4	△ 6 / 7
○	□ 登録したい既存 OU 1	未登録、事前チェックに失敗しました	OU の ID	-	⊖ 0 / 0	⚠ 0 / 1
○	登録したい直下のメンバーアカウント	未登録	アカウント ID	アカウントのメールアドレス	-	-

事前チェック失敗時のエラー



コンソールから、事前チェックの失敗原因レポートを取得可能

組織単位への事前チェック

- 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
- 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
- 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
- 登録を妨げるSCP があるか

など

レポートでのエラー内容

- 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。
- 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。
- 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。
- 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

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。

1. 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。

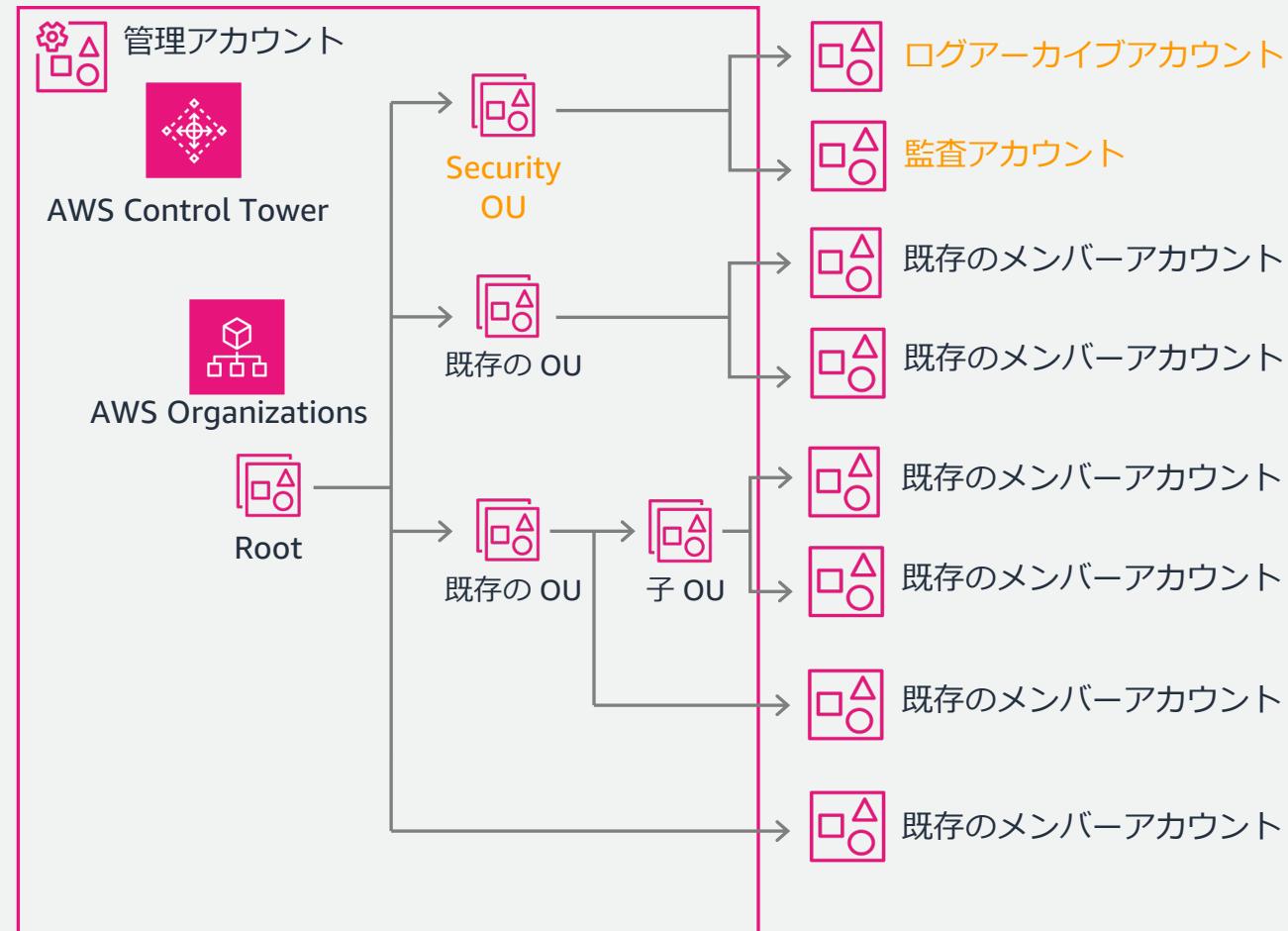


メンバーアカウントの登録

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

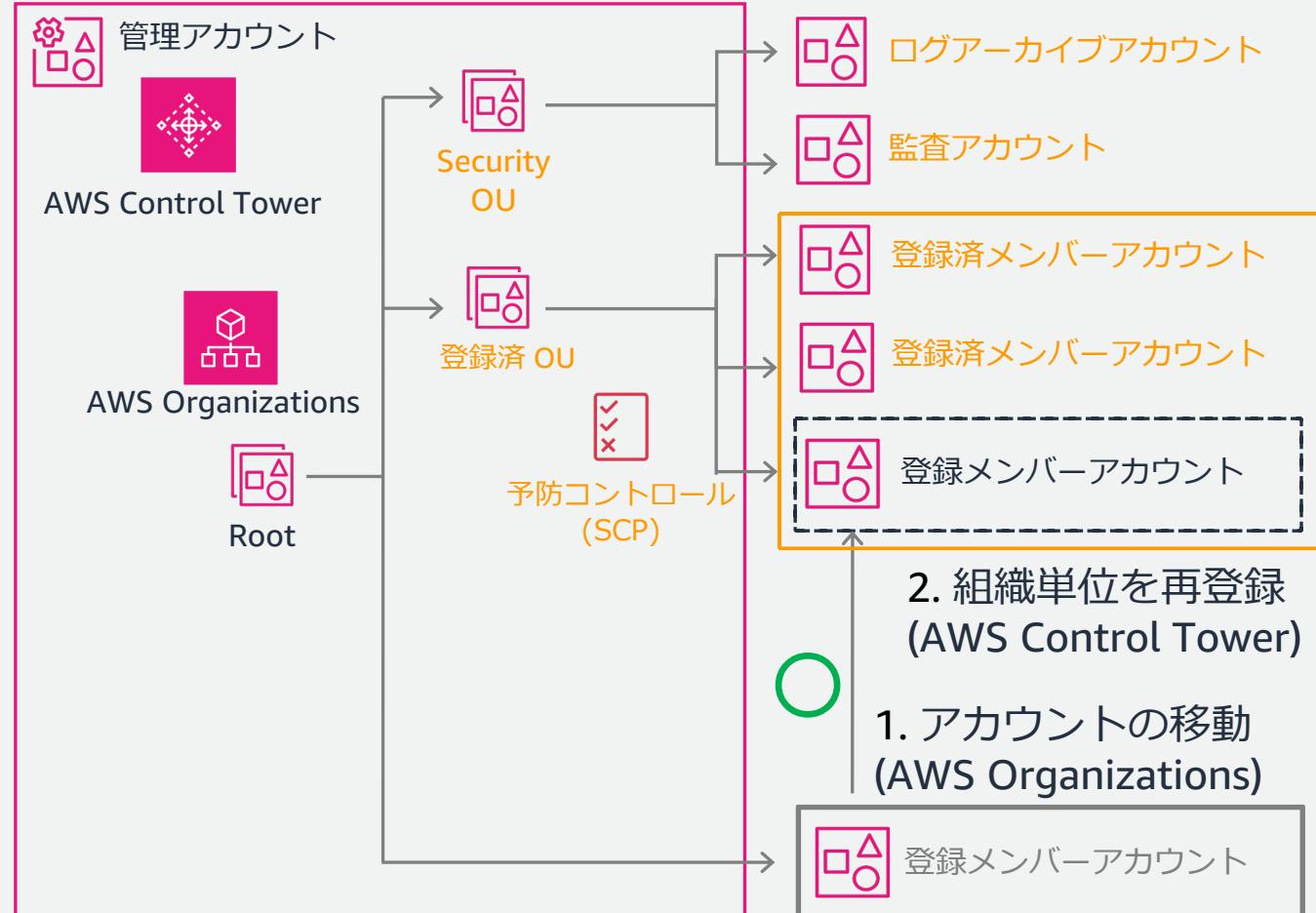


Root 直下のまま AWS Control Tower に登録はできない

1. 先に組織単位を移動して [組織単位を再登録] を実行 推奨
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) 組織単位の再登録

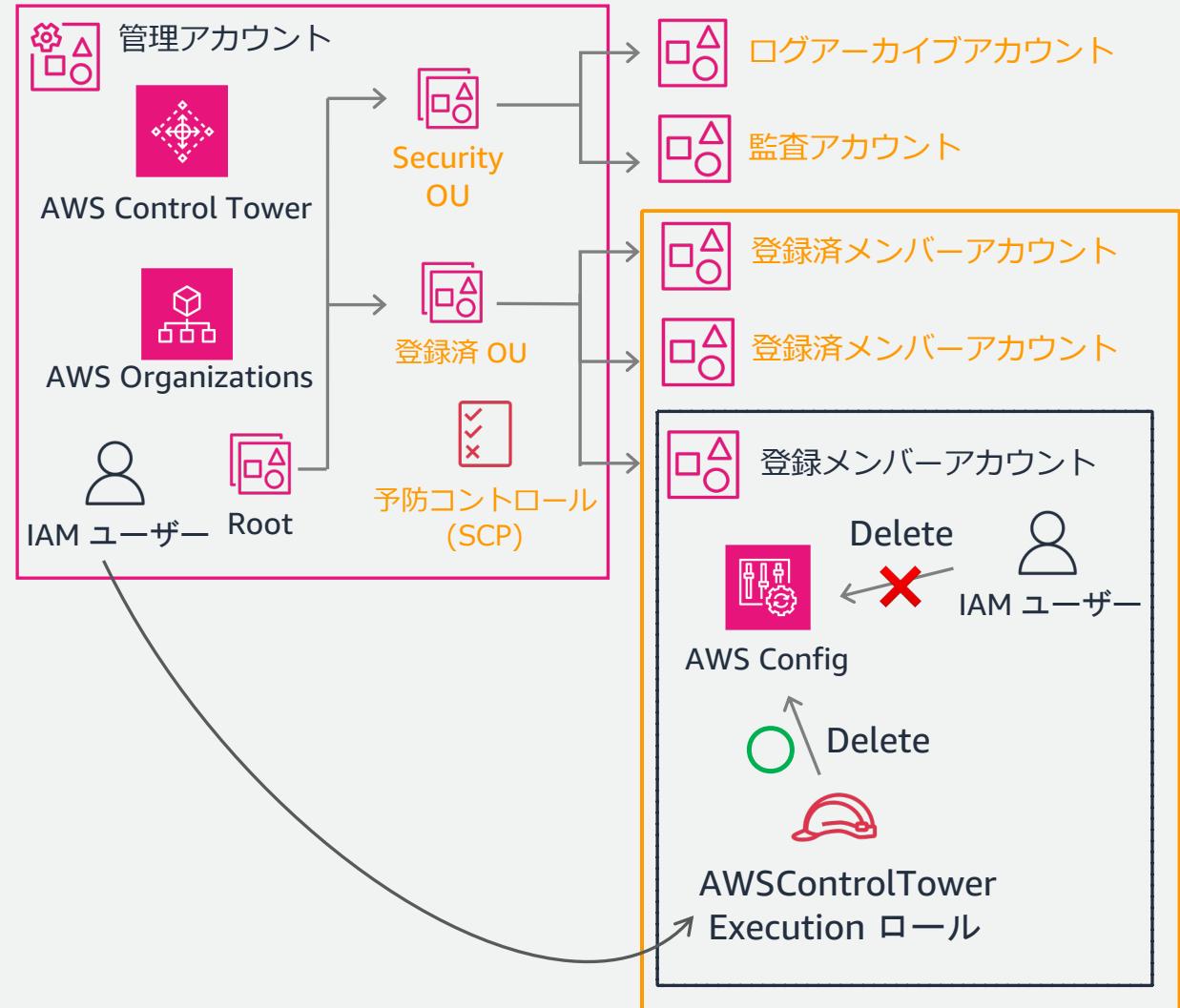
- ・ [組織単位を再登録] の実行で組織単位に追加した未登録のアカウントも登録可能
- ・ 処理内容は組織単位の登録と同様
 - AWSControlTowerExecution ロールのデプロイ
 - 前提条件を満たしているかの事前チェックを実行
- ・ 基本的に登録済のアカウントに影響はない
 - AWS Control Tower がデプロイしたリソースに変更を加えていない前提



(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/controlltower/latest/userguide/importing-existing.html

制限事項

- 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

- メンバーアカウントに AWSControlTowerExecution ロールを手動で作成する
- 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

The screenshot shows the AWS Control Tower Organization console. It lists several accounts under the '既存のアカウント' section. The columns include Name, Status, ID, Email, Registered Organization Units (OU), Registered Accounts, and Group Products. The 'Root' account is registered with 4 OUs and 6 accounts. Other accounts like '既存のOU1' and '既存のOU3' are also listed. A new account entry for '登録したい メンバーアカウント' is shown at the bottom.

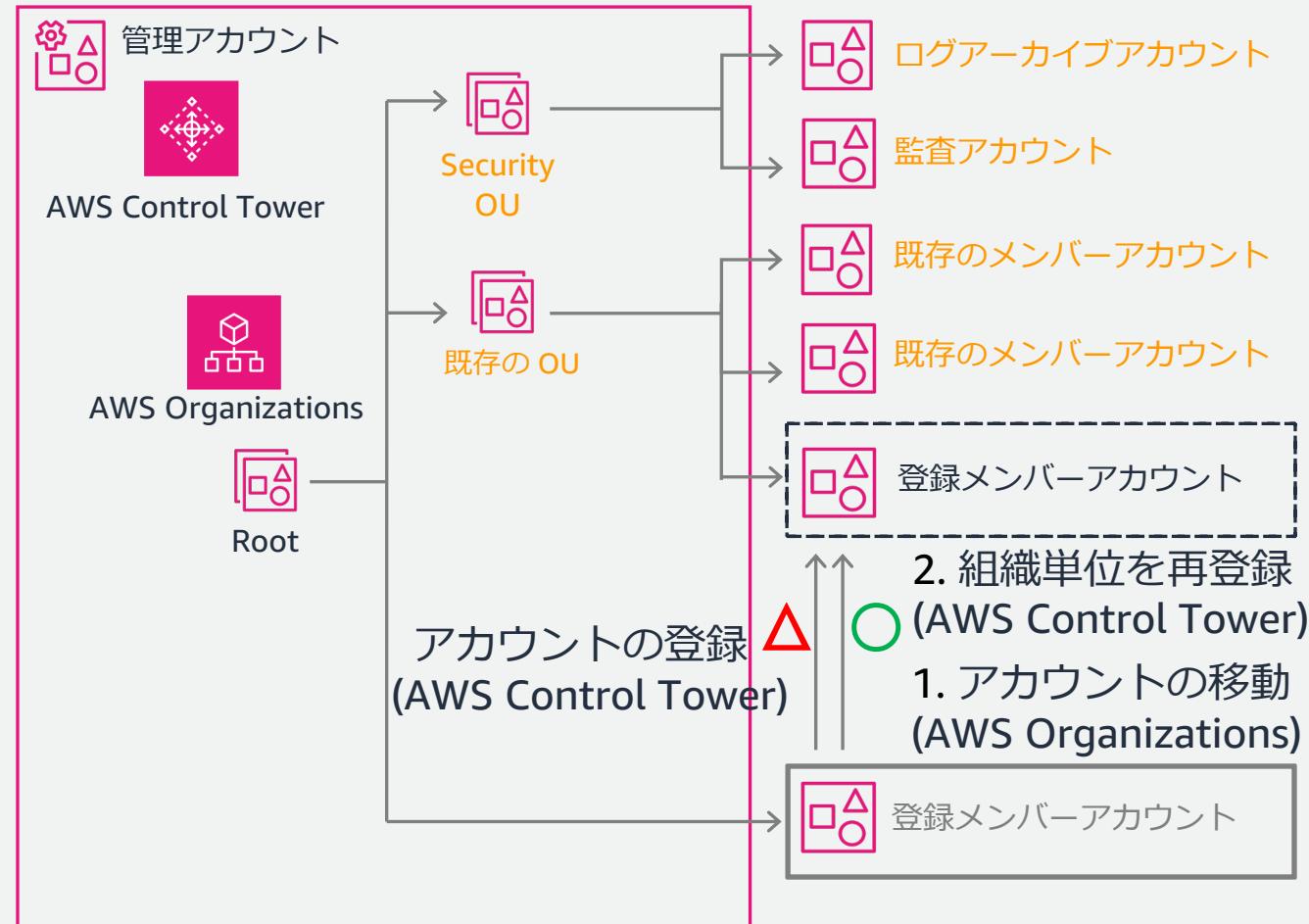
The screenshot shows the 'Account Registration' step in the AWS Control Tower wizard. It displays the 'Account Registration Settings' section with a note about projecting the account into AWS Control Tower. It also shows the 'Organization Unit' selection dropdown, which lists 'Registered Organization Units 1 (Level 1)', 'Registered Organization Units 2 (Level 1)', 'Nested Registered Organization Units (Level 2)', and 'Registered Organization Units 3 (Level 1)'. The 'Account Registration' button is at the bottom right.



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

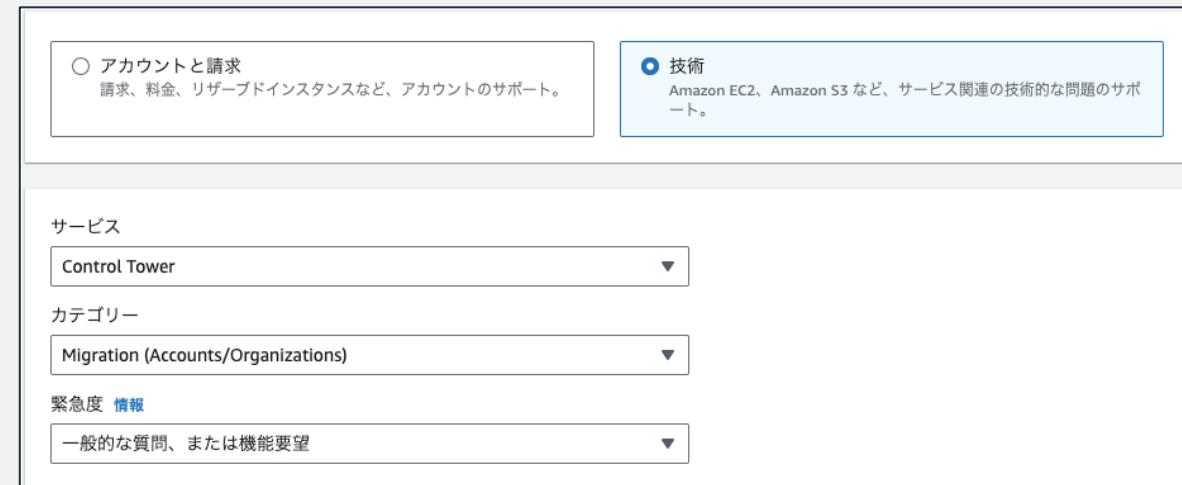
AWS Config が有効化済みのアカウントの登録申請

- 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/controlltower/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



The screenshot shows the AWS Support case creation interface. It includes sections for 'Account and Billing' (selected), 'Technical' (selected), 'Service' (Control Tower), 'Category' (Migration (Accounts/Organizations)), and 'Priority' (Information). A note at the bottom says '一般的な質問、または機能要望' (General questions or feature requests).

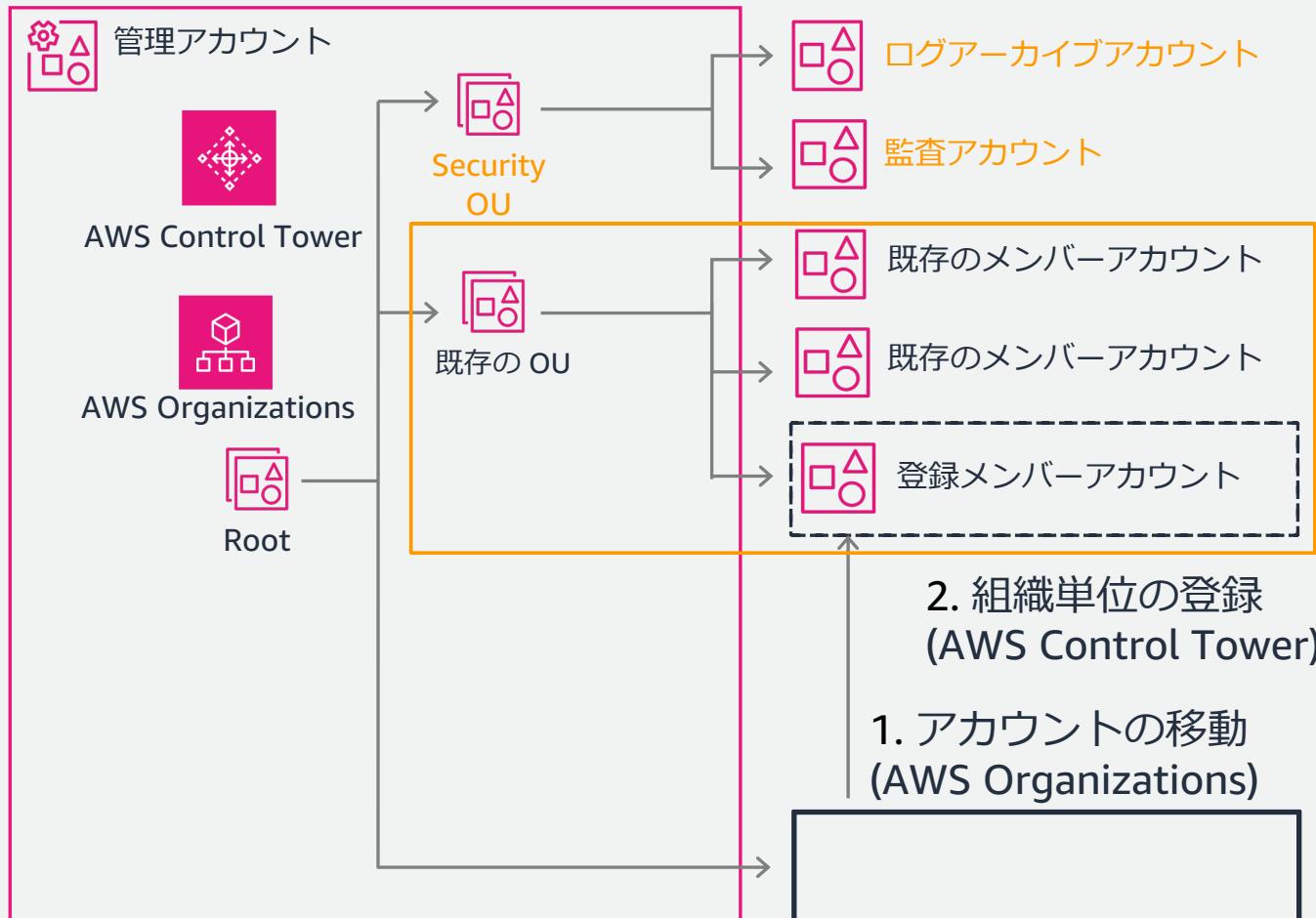
- ケースの作成時
技術
サービス: Control Tower
カテゴリ: Migration (Account/Organization)
- ケースの件名
既存の AWS Config リソースを持つアカウントを AWS Control Tower に登録する
- ケースの本文に記載する内容
管理アカウントの ID (12 桁の数字)
AWS Config リソースを持つメンバーアカウント ID
AWS Control Tower のホームリージョン

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/controlltower/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/controlltower/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/controlltower/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/controlltower/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/controlltower/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>
```