CUS-50

ガバメントクラウドで考える 技術的統制と効率性～AWSでの実現策～

山本 教仁
デジタル庁
クラウドチーム/Cloud Architect

佐藤 智樹
デジタル庁
クラウドチーム/Cloud Engineer

目次

発表の目的

発表の内容

- 第1部ではガバメントクラウドで検討しているクラウド利用の考え方
- 第2部ではそのアマゾン ウェブ サービス（AWS）での技術的な設計検討内容

対象者とする視聴者

- ガバメントクラウドを今後使っていく方
- ガバメントクラウドのような大規模な環境管理設計に関心のある方
- AWSでマルチアカウントの統制や運用設計、IaCによるインフラ構成管理を検討している方

本発表の目標

- ガバメントクラウドでのインフラ運用の考え方を知る
- 最新のサービスを使ったAWSマルチアカウント統制や運用の設計、IaCテンプレートを活用したインフラ構成管理方法の例を知る

話さないこと

- デジタル庁やガバメントクラウドの個別の施策
- 固有のAWSサービスに関する詳細な説明
- 自治体や政府など固有の事情による設計内容やその理由

第1部

ガバメントクラウドの概要

自己紹介

デジタル庁クラウドチーム
クラウドアーキテクト
山本教仁

外資系ITベンダーにてインフラ系デリバリーエンジニア、プリセールスアーキテクトを経て、2013年よりクラウドサービスプロバイダーにてコンサルティング組織を立ち上げ

2020年4月に内閣官房政府CIO補佐官に着任
2021年9月のデジタル庁発足と同時にデジタル庁クラウドアーキテクトに就任

デジタル庁について

デジタル庁設置法

第三条　デジタル庁は、次に掲げることを任務とする。
一　デジタル社会形成基本法（令和三年法律第三十五号）第二章に定めるデジタル社会（同法第二条に規定するデジタル社会をいう。以下同じ。）の形成についての基本理念（次号において「基本理念」という。）にのっとり、デジタル社会の形成に関する内閣の事務を内閣官房と共に助けること。
二　基本理念にのっとり、**デジタル社会の形成に関する行政事務の迅速かつ重点的な遂行**を図ること。

デジタル社会の実現に向けた重点計画

https://www.digital.go.jp/policies/priority-policy-program
2021年9月1日、日本のデジタル社会実現の司令塔としてデジタル庁が発足しました。デジタル庁は、この国の人々の幸福を何よりも優先し、**国や地方公共団体、民間事業者などの関係者と連携して社会全体のデジタル化を推進する取組を牽引**していきます。

ガバメントクラウドとは

デジタル庁ホームページより（https://www.digital.go.jp/policies/posts/gov_cloud）

政府共通のクラウドサービスの利用環境です。**クラウドサービスの利点を最大限に活用**することで、**迅速**、**柔軟**、かつ**セキュア**で**コスト効率の高い**システムを構築可能とし、利用者にとって利便性の高いサービスをいち早く提供し改善していくことを目指します。地方公共団体でも同様の利点を享受できるよう検討を進めます。

ユーザー体験を向上させ、世の中の状況の変化に応じて情報システムを柔軟に変更できるような**現代的なアプリケーション開発**にとって、柔軟かつ迅速にITインフラを構築することは必須となります。アプリケーション開発者の要求に応じて自動で柔軟かつ迅速にインフラを用意できる環境を、**最新のクラウド技術を最大限に活用**して政府として共通に提供します。クラウドの最新技術を活用することで、クラウドサービスが提供する高いセキュリティと可用性、スケーラビリティを利用できます。同時に、**ガバナンス機能とテンプレート**を用いることで、政府全体としての管理レベルの向上、ベストプラクティスに基づく品質の底上げと標準化、セキュリティやネットワーク、運用監視などの検討省力化と設定自動化を支援します。テンプレートに基づき適切にマネージドサービスを利用し、構築と運用の自動化を実現することでインフラコストの削減が実現できます。また、ガバメントクラウドを利用することでインフラコストの可視化・透明化を実現し、コストの適切な評価ができるようにします。
最新クラウド技術の活用ができる環境についてテンプレートを使ってベストプラクティスに基づく標準的な環境として提供することにより、政府や地方自治体のアプリケーション開発を現代的なものにしていくことを最大限支援します。

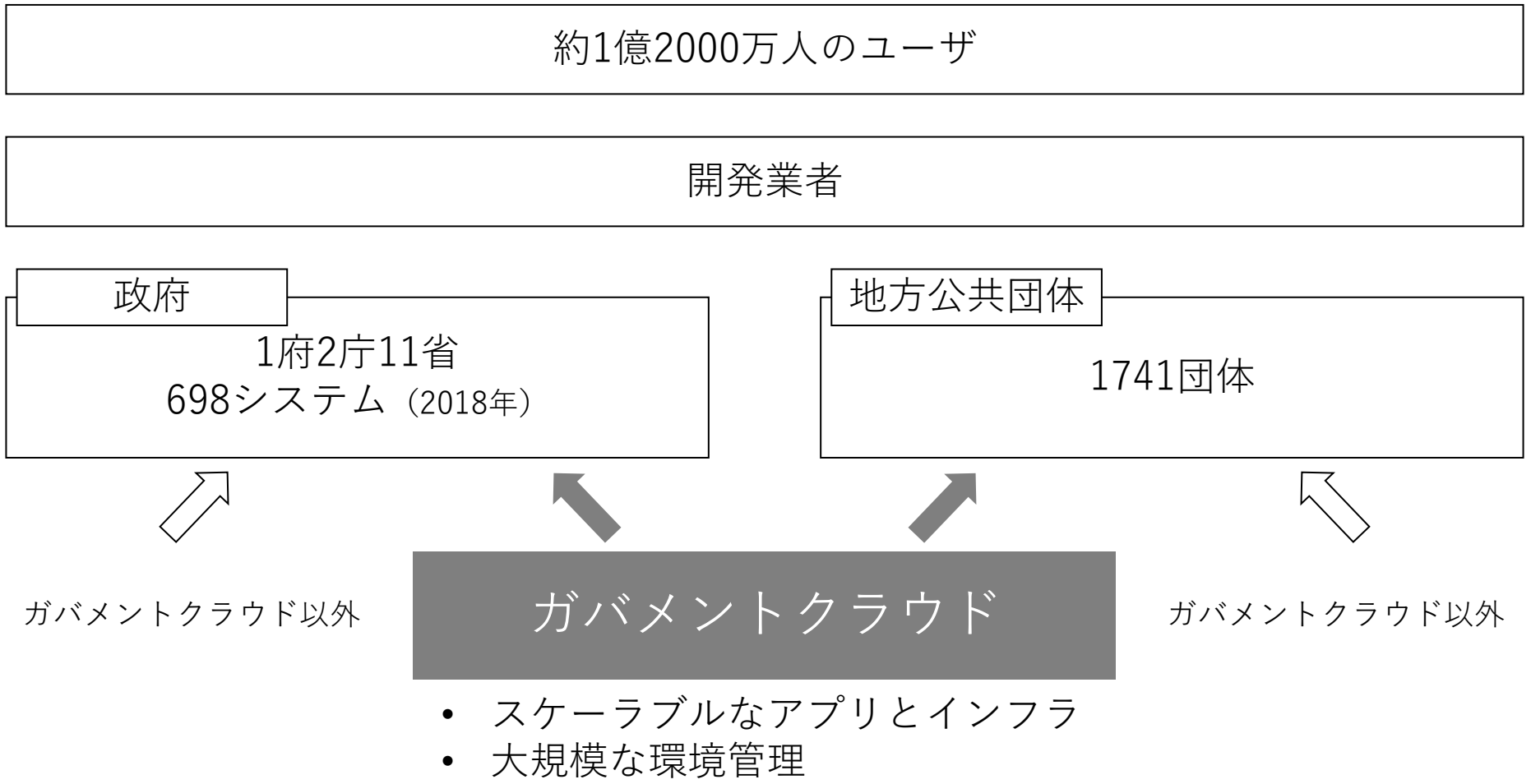
ガバメントクラウドで考える3つの要素

1. IaC(Infrastructure as Code)テンプレート

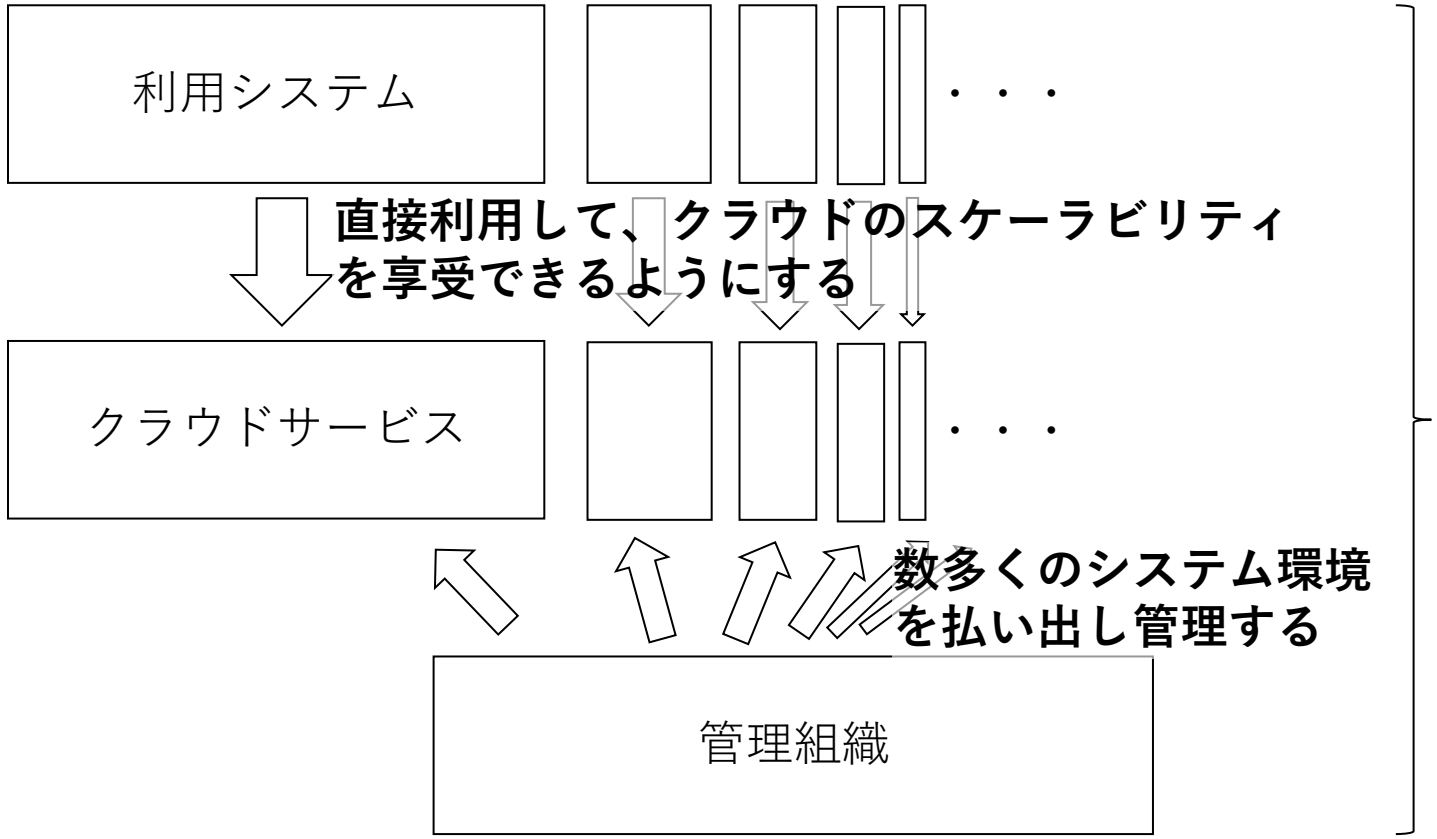
2. 予防的統制・発見的統制

3. 成長するチーム

ガバメントクラウドのユーザ



スケーラビリティと大規模な環境管理を実現するために



- 余計な管理機能を挟まない
- 環境準備を可能なかぎり自動化する
- 複数の環境に共通の設定を行う

AWSでは、

- AWS Control Tower + AWS Organizationsによるマルチアカウント管理
- IaCテンプレート（AWS CDK／AWS CloudFormation）
- ガードレール

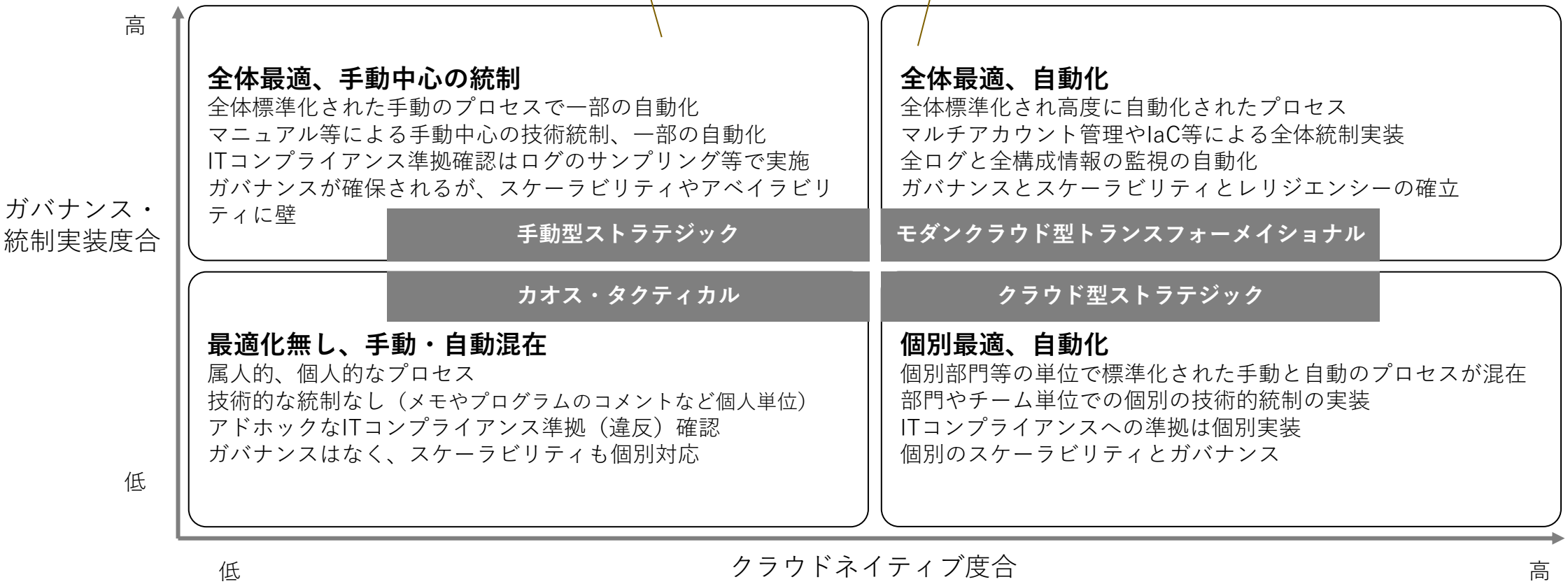
⇨「第2部ガバメントクラウドの設計」で説明

マルチアカウント管理、IaCテンプレート、ガードレールで実現する技術ガバナンス

ガードレール方式による技術ガバナンス

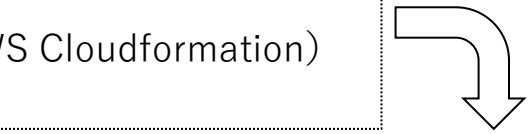
ゲートキーパー方式による技術ガバナンス実現
機能利用の事前承認や境界防御による経路の集約管理はスケーラビリティや柔軟性にとってボトルネックになり、全量チェックできずITコンプライアンス準拠確認も部分的になる

ガードレール方式による技術ガバナンス実現
ITコンプライアンス違反となる操作を未然に防ぐこと（予防的統制）と、違反の疑いや違反の予兆を検知すること（発見的統制）により、スケーラビリティや柔軟性を維持しつつ技術ガバナンスを実現



ガバメントクラウドを構成する要素

- AWS Control Tower + AWS Organizationsによる
  マルチアカウント管理
- IaCテンプレート（AWS CDK／AWS Cloudformation）
- ガードレール



利用者視点で再整理

1. IaC(Infrastructure as Code)テンプレート

IaCテンプレートで環境を自動整備し、利用者もIaCテンプレートでインフラ構築できるようにする

2. 予防的統制・発見的統制

各環境に予防的統制をかけることで、共通にセキュリティ違反を予防し、
発見的統制をかけることで、各環境でのセキュリティ状況を可視化する

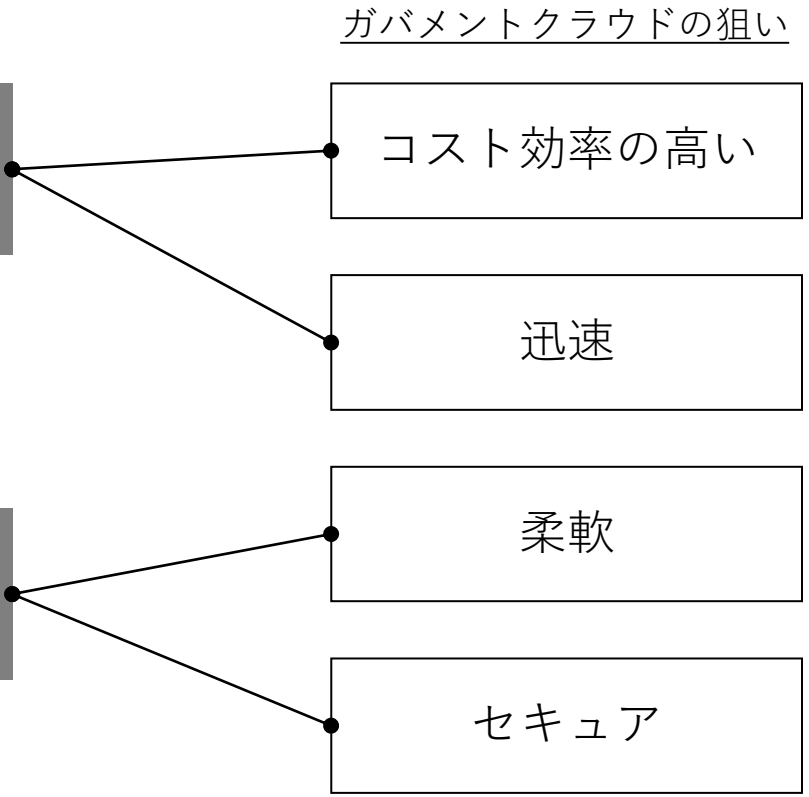
IaCテンプレートと予防的統制・発見的統制はガバメントクラウドの狙いにもつながる

1. IaC(Infrastructure as Code)テンプレート

IaCでインフラ構成を管理し、マネージドサービスやコンテナ、サーバレスを活用し、イミュータブルな運用を行うことでOSのない環境を実現できる
クラウドのスケーラビリティを享受できるとともに、コストの最適化、インフラ構成の透明化が実現できる

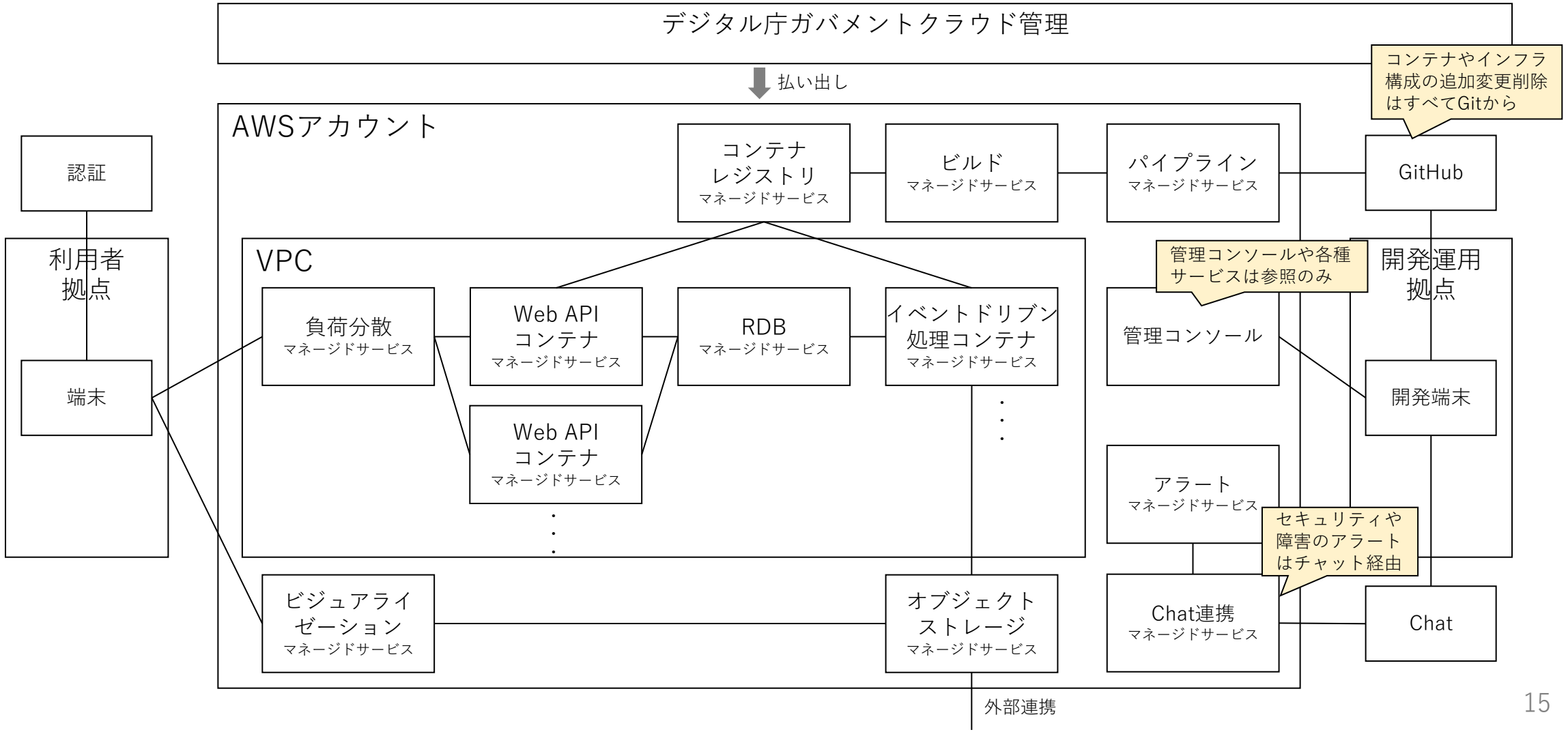
2. 予防的統制・発見的統制

全体ガバナンスを効かせると同時に、各システムに強い権限を与えて構成の柔軟性を実現しつつガバナンス実現を支援する
さらに、統制やルール違反を自動で検知し、継続的なセキュリティ改善を促し、よりセキュアなシステム環境を実現する



OSのない環境の運用イメージ

OSがないことにより、パッチ適用や踏み台の運用がなくなり、インフラコストも最適化される



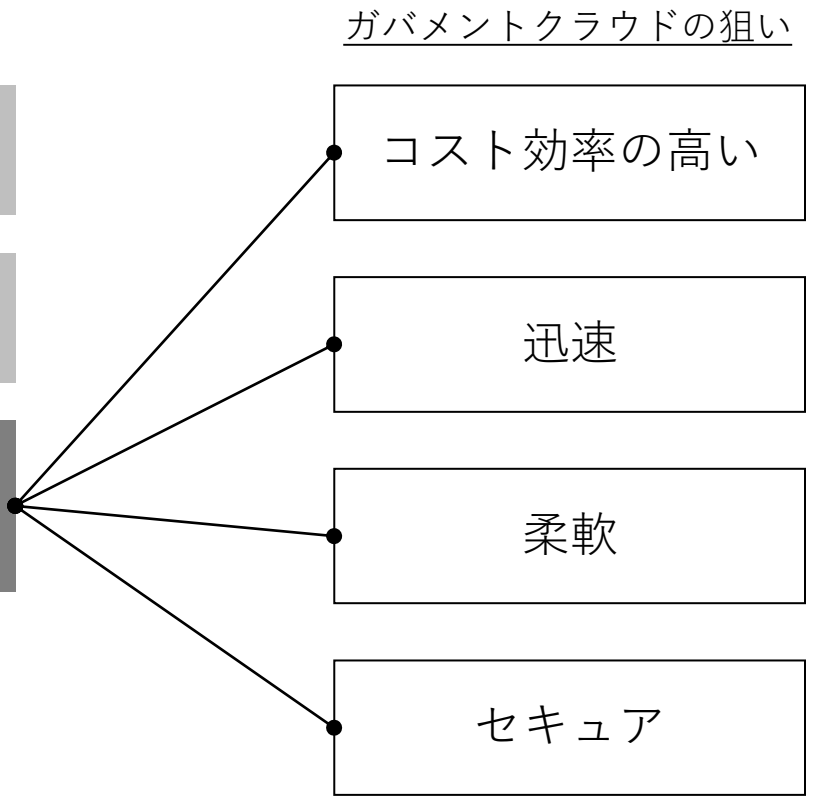
3つ目の（一番大事な）要素

1. IaC(Infrastructure as Code)テンプレート

2. 予防的統制・発見的統制

3. 成長するチーム

こうしたシステム開発と運用を成功させるためには、つねに新しい技術を学習し、新しい取り組みにチャレンジする開発運用チームである必要がある
これまでどうしてきたかに固執せず、システムとしての目標や狙いを実現するためにこれからどうあるべきか、どうしていくべきかにチームとしてチャレンジしていく
これまでの受発注関係ではない、受託事業者やサービス提供者と共に成長するチームをガバメントクラウドでは目指す



ガバメントクラウドで考える3つの要素

1. IaC(Infrastructure as Code)テンプレート

2. 予防的統制・発見的統制

3. 成長するチーム

第2部

ガバメントクラウドの設計

目次

第2部 目次

- マルチアカウントの管理方法
  - AWS Control TowerとAWS Organizations、AWS SSO利用の全体像
  - アカウント払い出し
- IaCテンプレートの活用
  - AWS CDK/AWS CloudFormationの活用
- ガードレールの設定
  - 予防的統制
  - 発見的統制
- 今後の情報展開

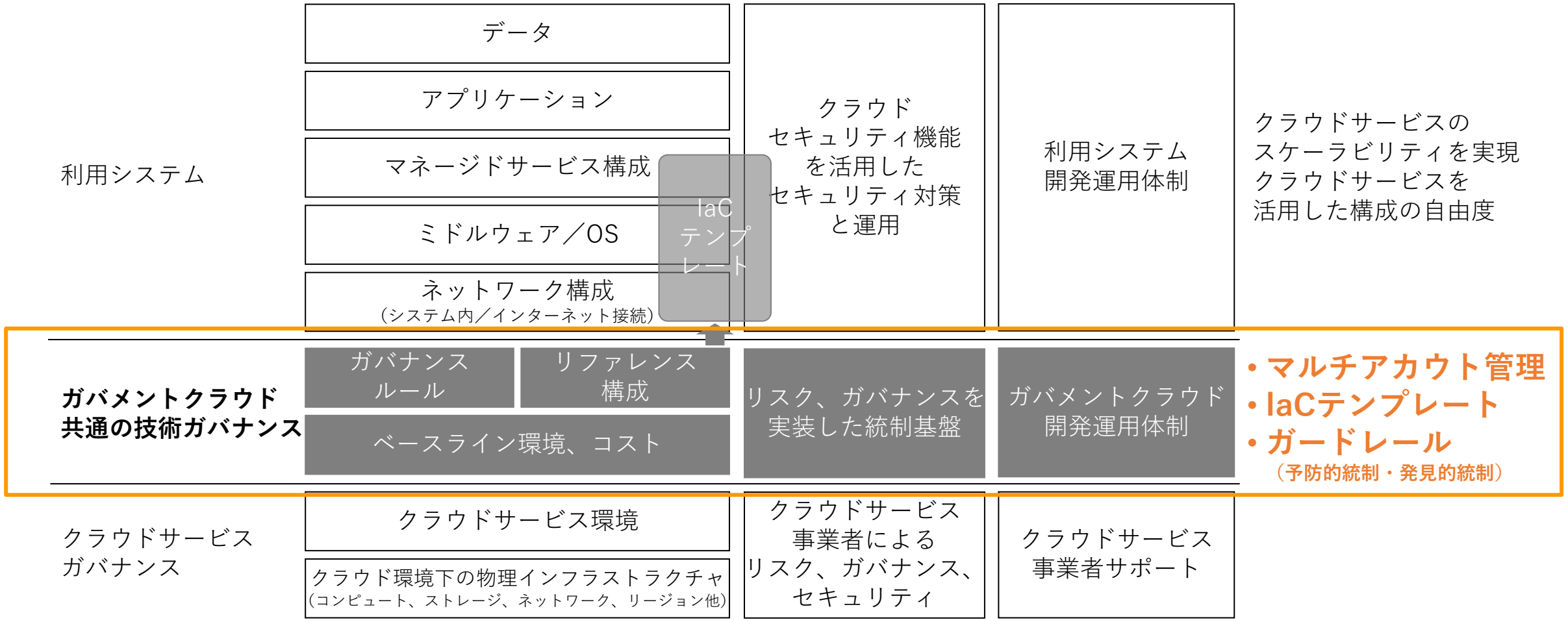
自己紹介

デジタル庁クラウドチーム
クラウドエンジニア
佐藤智樹

日系ITベンダーへ勤務後、開発やクラウドメインの仕事に従事したくクラウドインテグレータに転職。クラウドを利用したシステム開発の案件にバックエンド/インフラエンジニア/アーキテクトとして参画
IaCが好き

2021年4月に内閣官房IT総合戦略室内のデジタル庁の前身となる組織でクラウドエンジニアに就任
2021年9月のデジタル庁発足と同時にデジタル庁へ入庁

マルチアカウント管理、IaCテンプレート、ガードレールで実現する技術ガバナンス



第2部 目次

- マルチアカウントの管理方法
  - AWS ControlTowerとAWS Organizations、AWS SSO利用の全体像
  - アカウント払い出し
- IaCテンプレートの活用
  - AWS CDK/AWS CloudFormationの活用
- ガードレールの設定
  - 予防的統制
  - 発見的統制
- 今後の情報展開

マルチアカウントの利用目的

ガバメントクラウドでは、各府省や地方公共団体はもちろん、府省内のシステムや地方公共団体内のシステム単位でもセキュリティや運用上管理を明確に分離できる必要があります。この管理の分離をAWSではマルチアカウント構成で実現します。
マルチアカウント構成はAWSのWell-Architected Frameworkでも推奨されています。

以下はAWS Well-Architected フレームワーク-セキュリティの柱より引用

個別アカウントごとにワークロードを整理し、機能、コンプライアンス要件、共通のコントロールセットに基づいてアカウントをグループ化することを推奨しています

- アカウントを使用してワークロードを分ける
- AWS アカウントを保護する
- アカウントを一元的に管理する
- 制御を一括設定する
- サービスとリソースを一括設定する

「AWS アカウントの管理と分離」https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/aws-account-management-and-separation.html

第2部 目次

- マルチアカウントの管理方法
  - AWS ControlTowerとAWS Organizations、AWS SSO利用の全体像
  - アカウント払い出し
- IaCテンプレートの活用
  - AWS CDK/AWS CloudFormationの活用
- ガードレールの設定
  - 予防的統制
  - 発見的統制
- 今後の情報展開

ガバメントクラウド(AWS)で利用するサービス

ガバメントクラウドで必要と考えるガバナンスベースを実現するために使用するサービス群の一部を紹介します。

AWS CloudTrail

AWSアカウント内でいつ、誰が、何のリソースを操作したかを記録できるサービス

AWS Config

リソースを操作を継続監視し、設定内容を評価、監査できるサービス

Amazon GuardDuty

悪意のある操作を継続監視し、不正なアクセスの可視化/修復するための調査結果を提供するサービス

AWS Security Hub

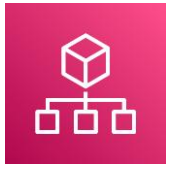
セキュリティのベストプラクティスのチェックを行い、アラートを集約し、自動修復も可能となるサービス

ガバメントクラウド(AWS)で利用するサービス

ガバメントクラウドで必要と考えるガバナンスベースを実現するために使用するサービス群の一部を紹介します。

AWS Control Tower

セキュアなマルチアカウント AWS 環境をセットアップおよび管理できるサービス



AWS Organizations

AWSアカウントの環境を一元管理および統制するためのサービス

AWS Single Sign-On

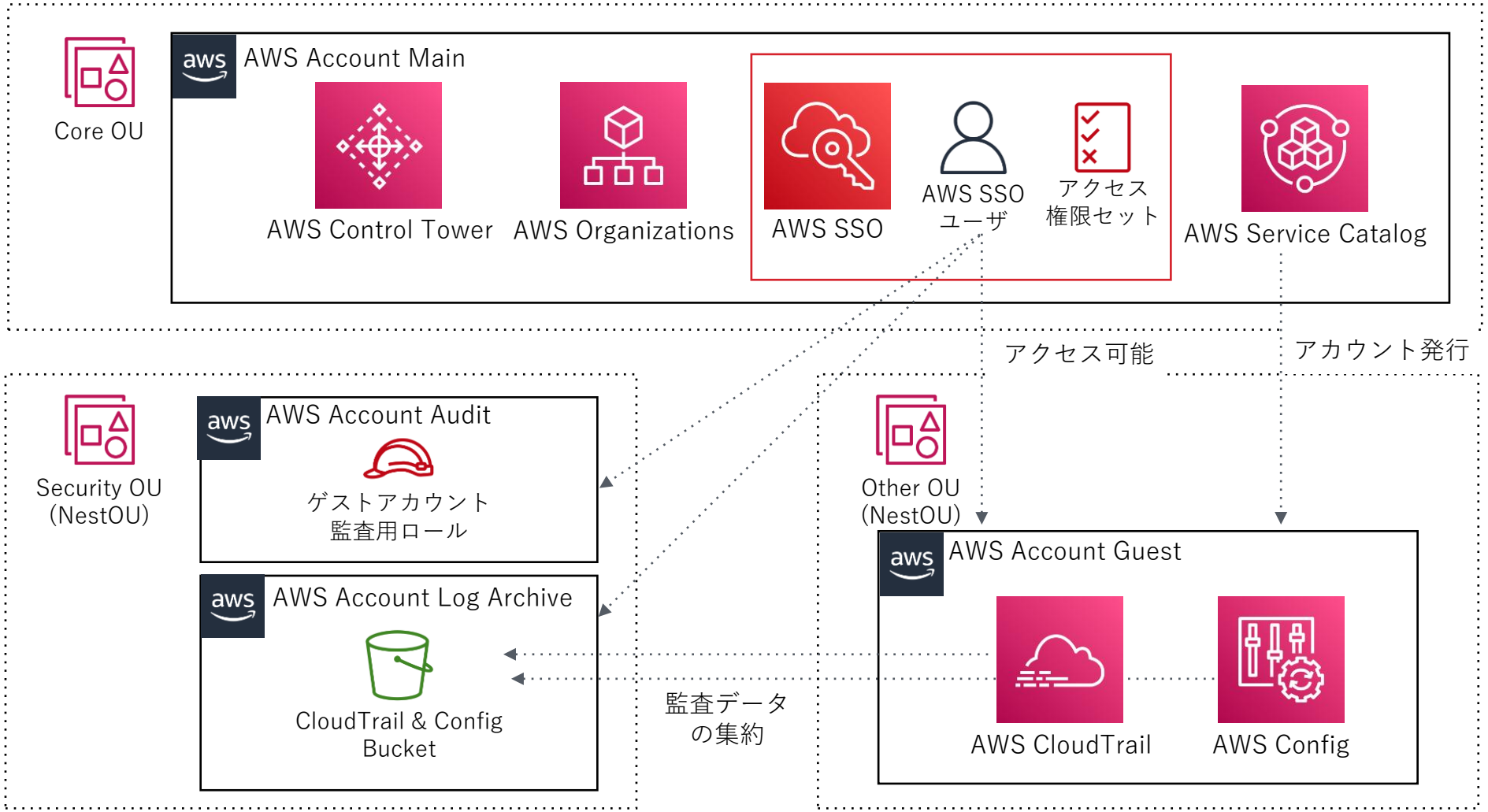
複数の AWS アカウントやアプリケーションへのアクセスを一元管理できるサービス

AWS Service Catalog

AWSが承認したITサービスのカタログを作成/管理できるサービス
(AWSアカウントの作成などで利用)

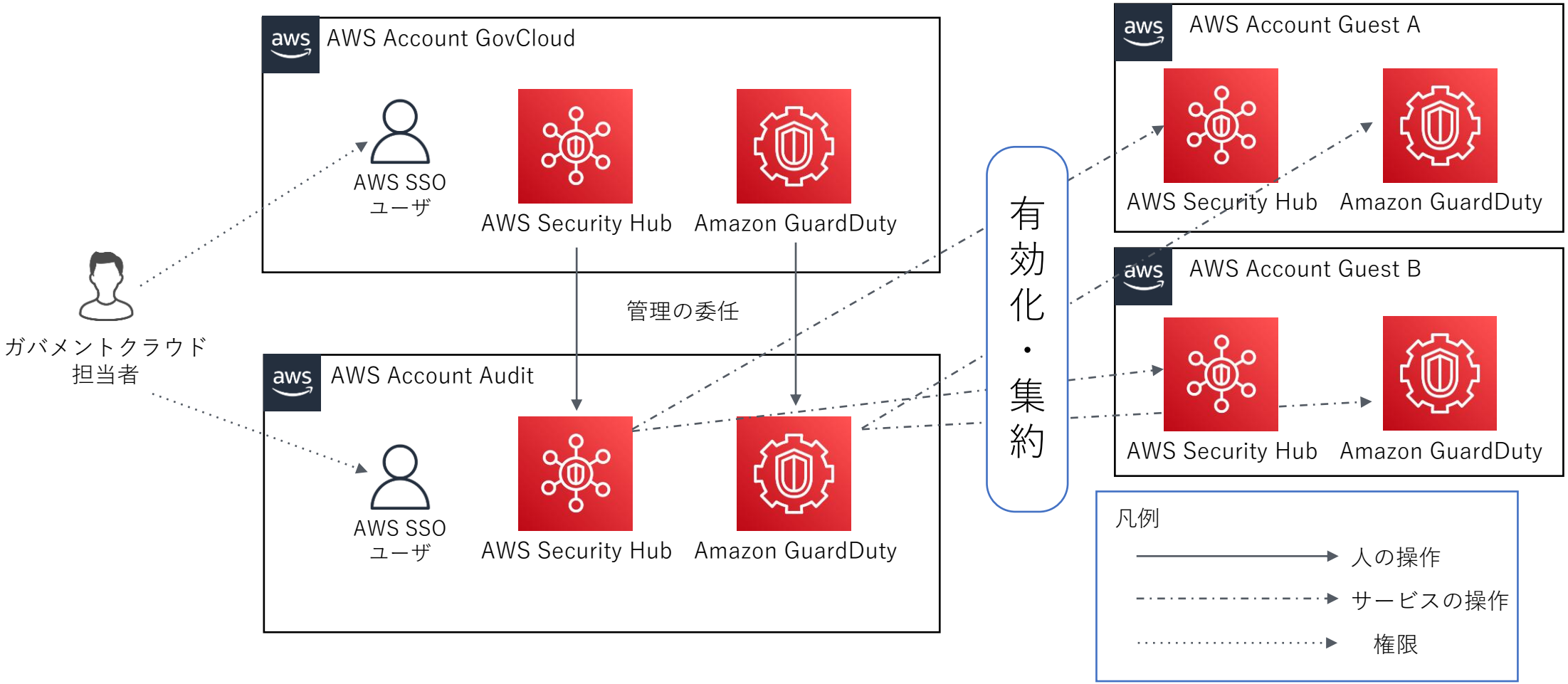
AWS Control Towerが利用するサービスの関係性

AWS Control Towerで使用するサービスと実現イメージ



各アカウントへ統制を展開する例

発見的統制に関連するSecurityHubやGuardDutyをAuditアカウントで一括設定

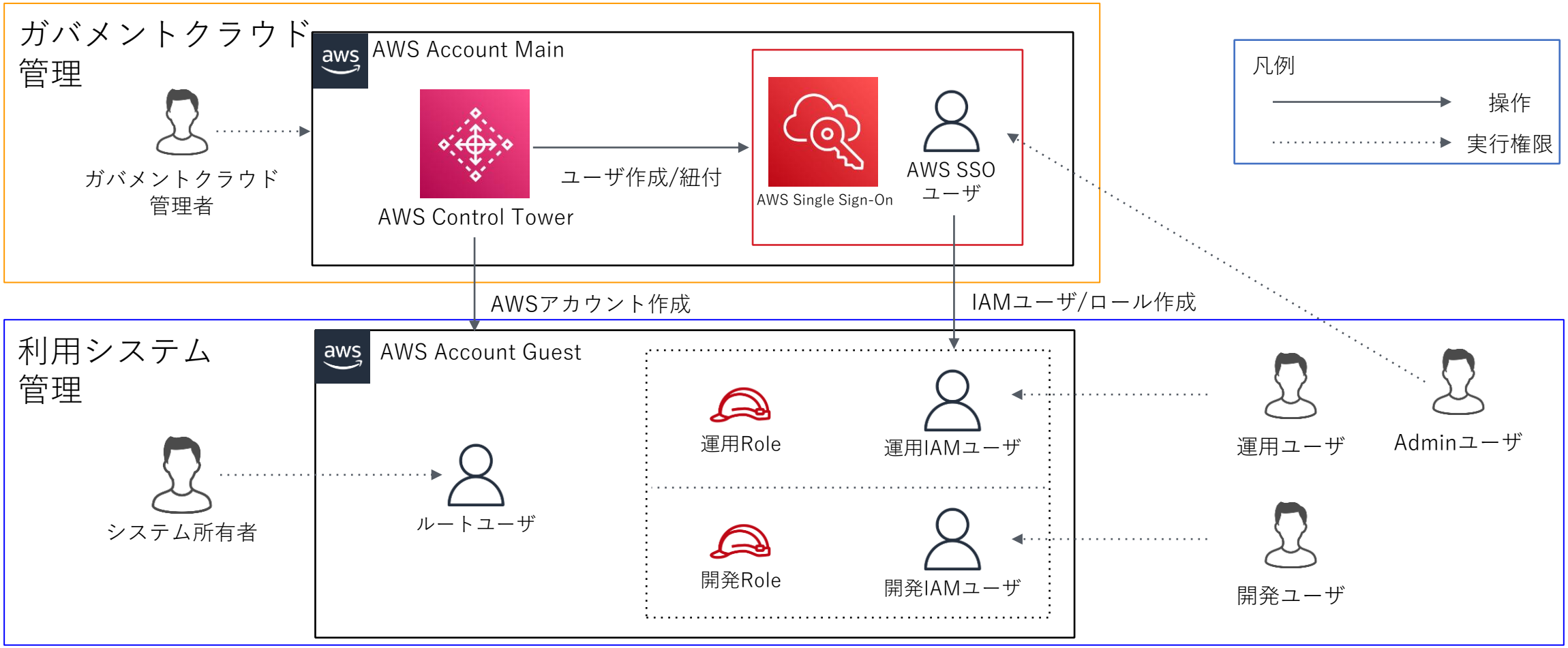


第2部 目次

- マルチアカウントの管理方法
  - AWS ControlTowerとAWS Organizations、AWS SSO利用の全体像
  - アカウント払い出し
- IaCテンプレートの活用
  - AWS CDK/AWS CloudFormationの活用
- ガードレールの設定
  - 予防的統制
  - 発見的統制
- 今後の情報展開

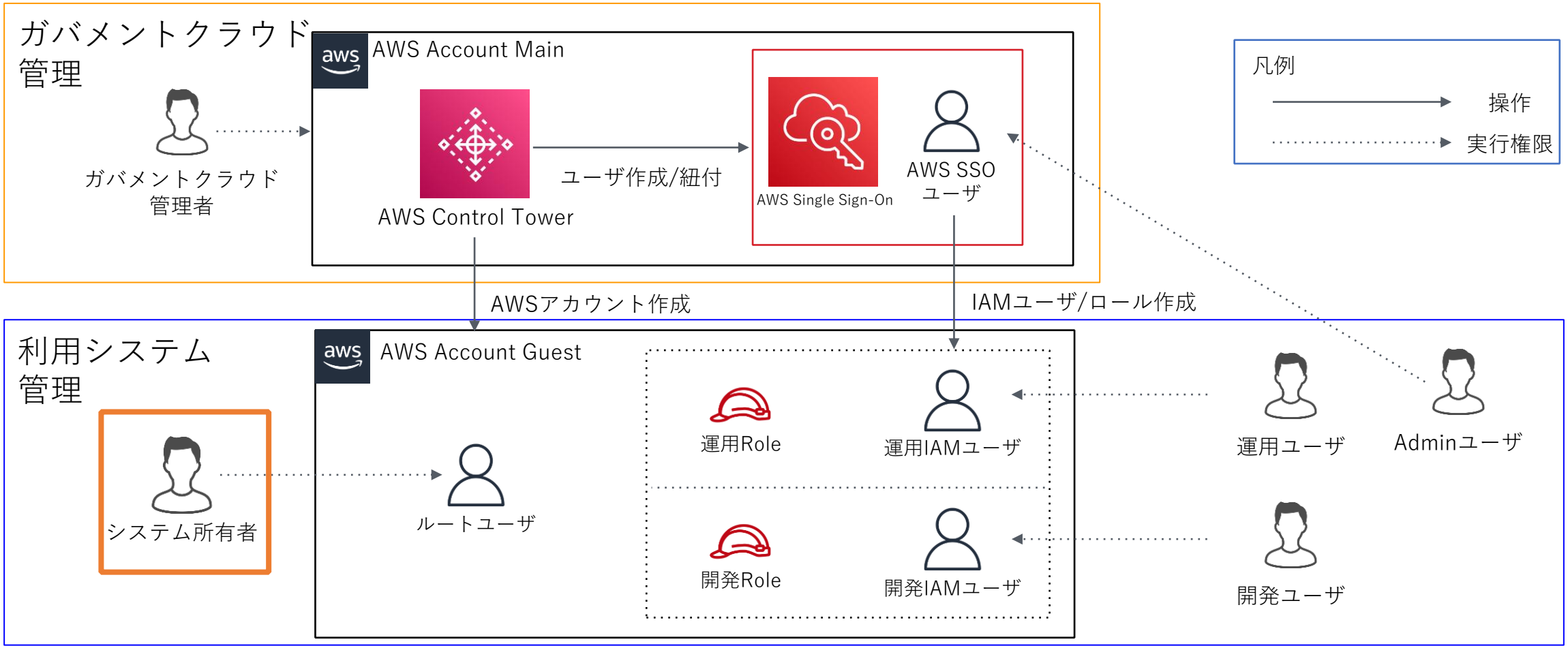
ガバメントクラウド(AWS)のユーザ構成の全体像

AWSアカウントやAWS SSOユーザ、各アカウント内のIAMユーザと実際の担当者との関連を以下のように整理



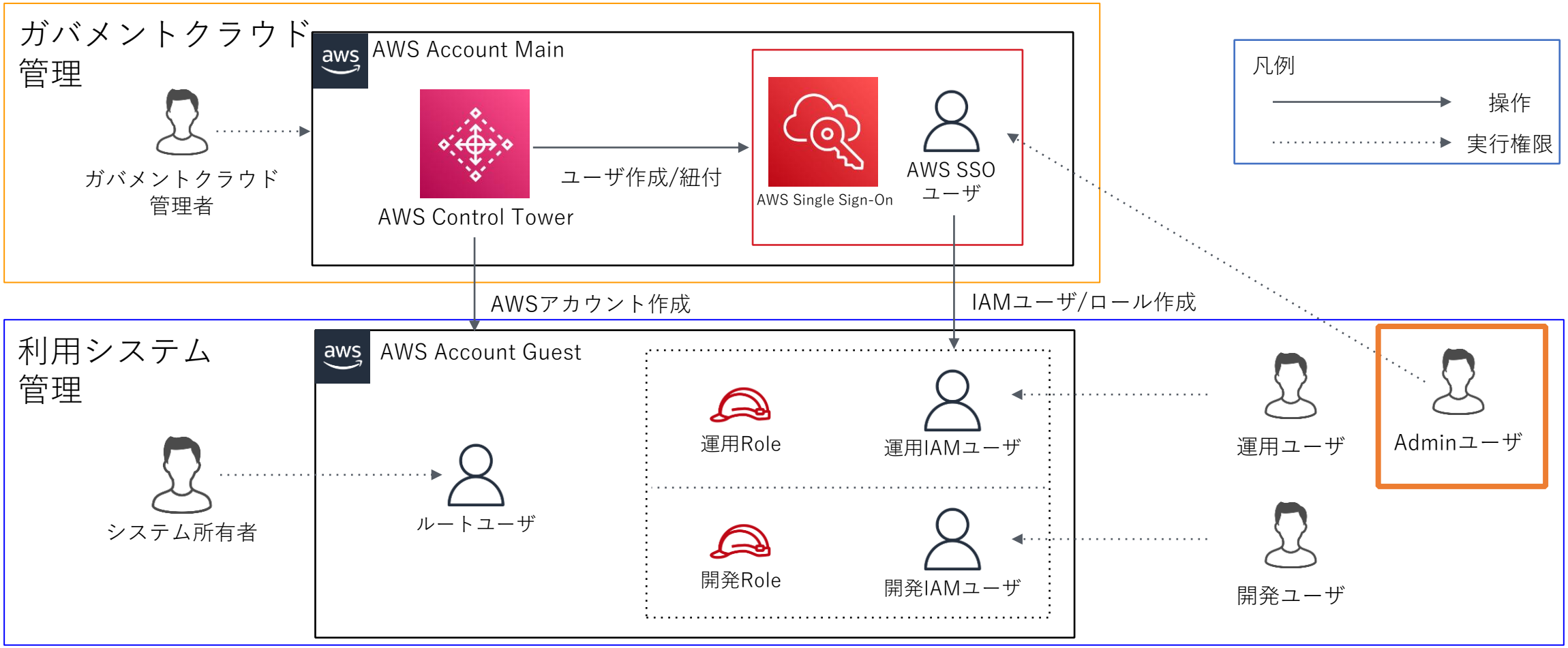
ガバメントクラウド(AWS)のユーザ構成の全体像

システム管理者はルートユーザを管理。基本ハードウェアMFAを使用し厳重管理。ルートユーザの操作が必要な時以外は使用しない



ガバメントクラウド(AWS)のユーザ構成の全体像

Adminユーザは、AWSAdministratorAccessをセットしたAWS SSOユーザを使用し
運用/開発者へIAMユーザ/ロールの払い出しやテンプレートを実行(後述)

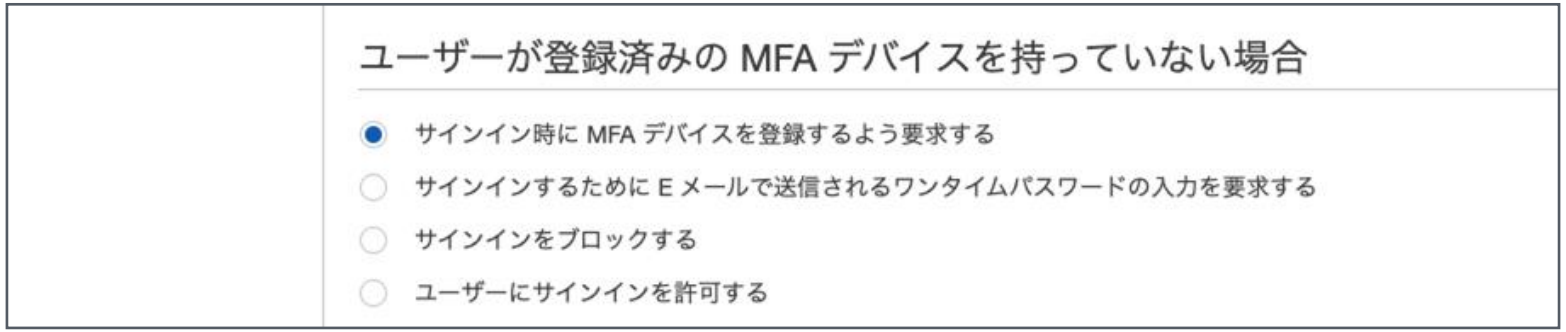


AWS SSOユーザを利用する理由

2つの利点からAWS SSOの利用を選択

- 権限棚卸のためIAMユーザ発行者を制限
  IAMユーザの発行権限があれば、基本どんな操作でも可能になるためユーザ把握が困難になる。
  AWS SSOユーザにIAMユーザ発行権限を絞ることで中央で権限管理を実施できる

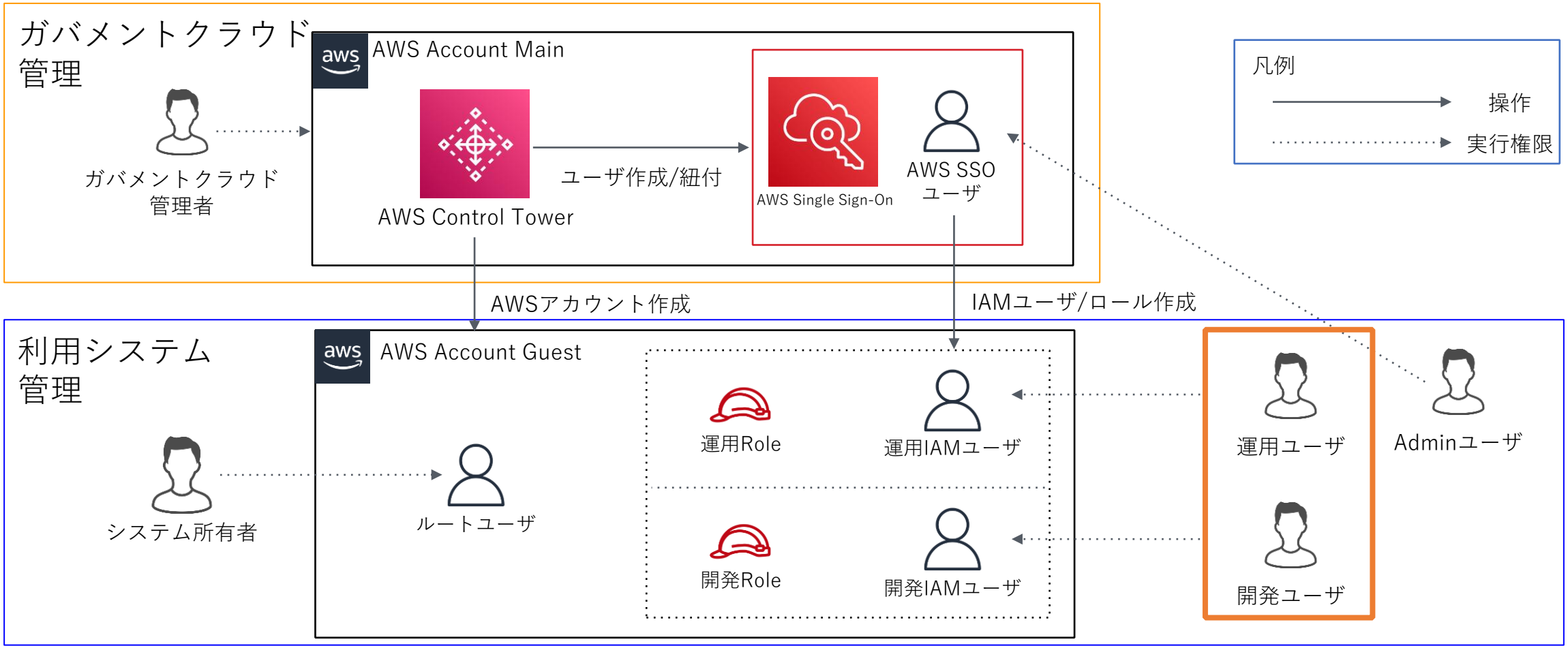
- 最初から安全性の高いユーザを利用
  ルートユーザを配布する場合MFAの設定を強制できない
  AWS SSOユーザなら管理側からMFAの設定を簡単に強制できる



AWS SSOの設定画面

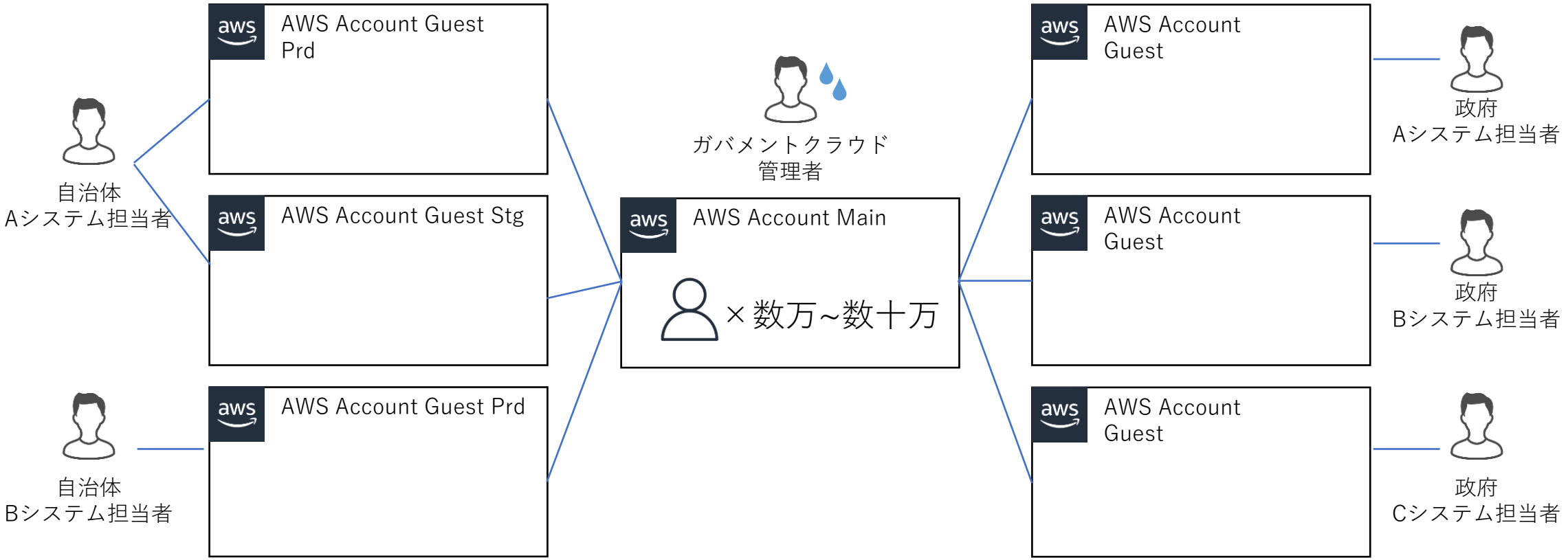
ガバメントクラウド(AWS)のユーザ構成の全体像

運用/開発ユーザは、Adminユーザから払い出されたIAMユーザ/ロールを使用して構築作業や運用保守などを行う



AWS SSOユーザを全体で使わない理由

組織がバラバラでかつ数万~数十万単位のユーザ使用が想定され全てのユーザを1箇所で管理するのは困難なため

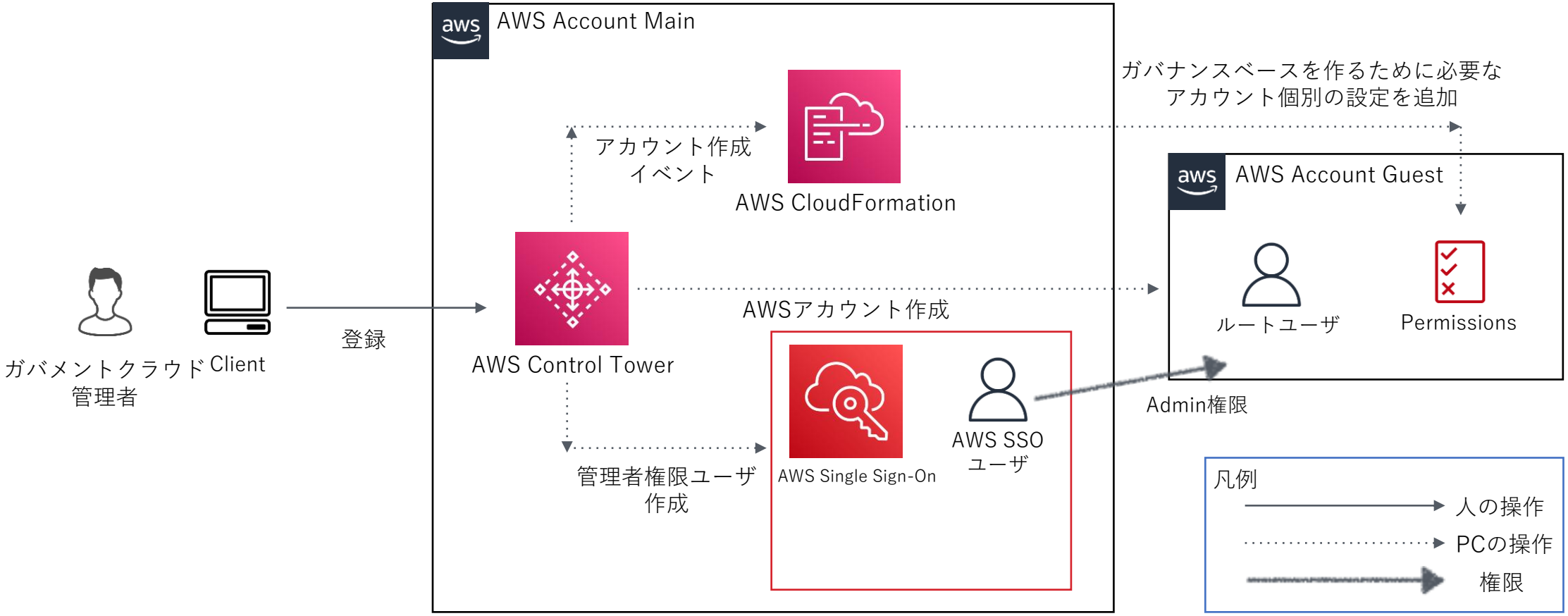


1741アカウント?×2(検証/本番)×IAMユーザ数

698アカウント?×2(検証/本番)×IAMユーザ数

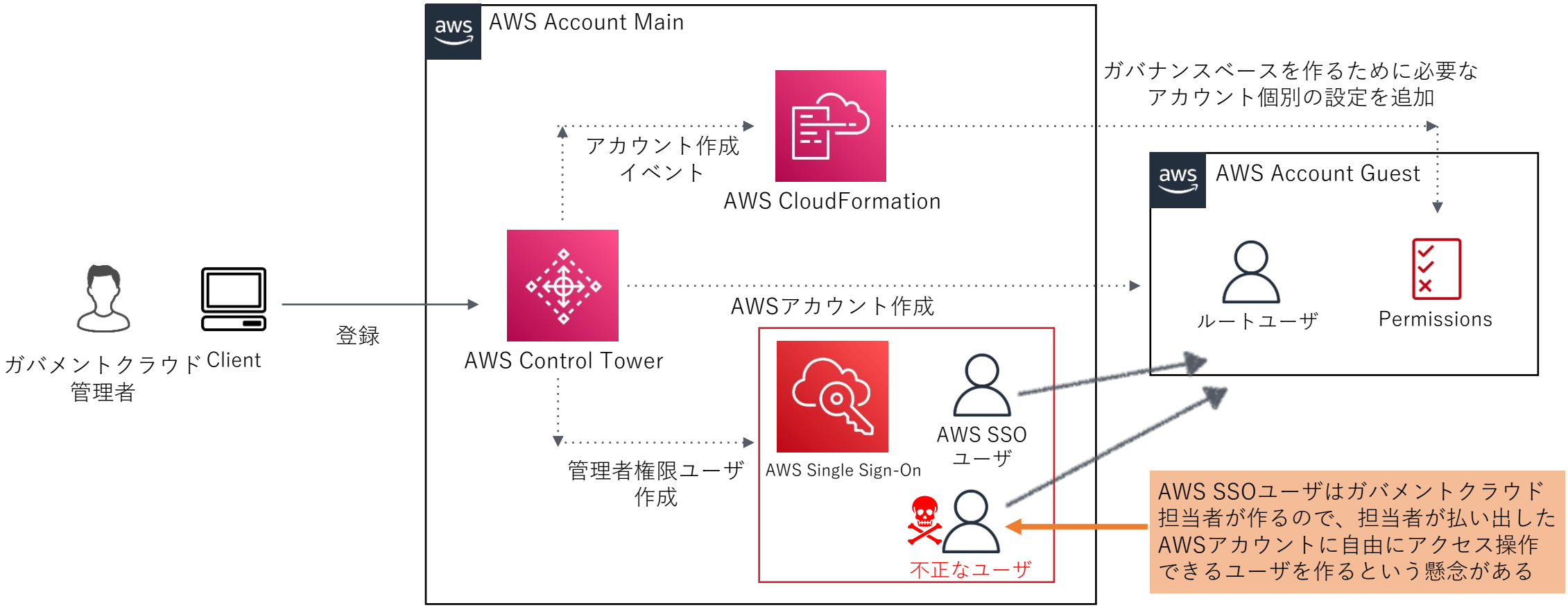
ガバメントクラウド担当者の操作の統制

ガバメントクラウド管理者側からの利用システムアカウントへの操作は、(1)一番最初のそもそものアカウント作成、(2)管理側からのテンプレートによる最初の自動設定、(3)AWS SSOユーザによる操作の3つのみで、それぞれに対する統制は次ページ以降の方法で実施



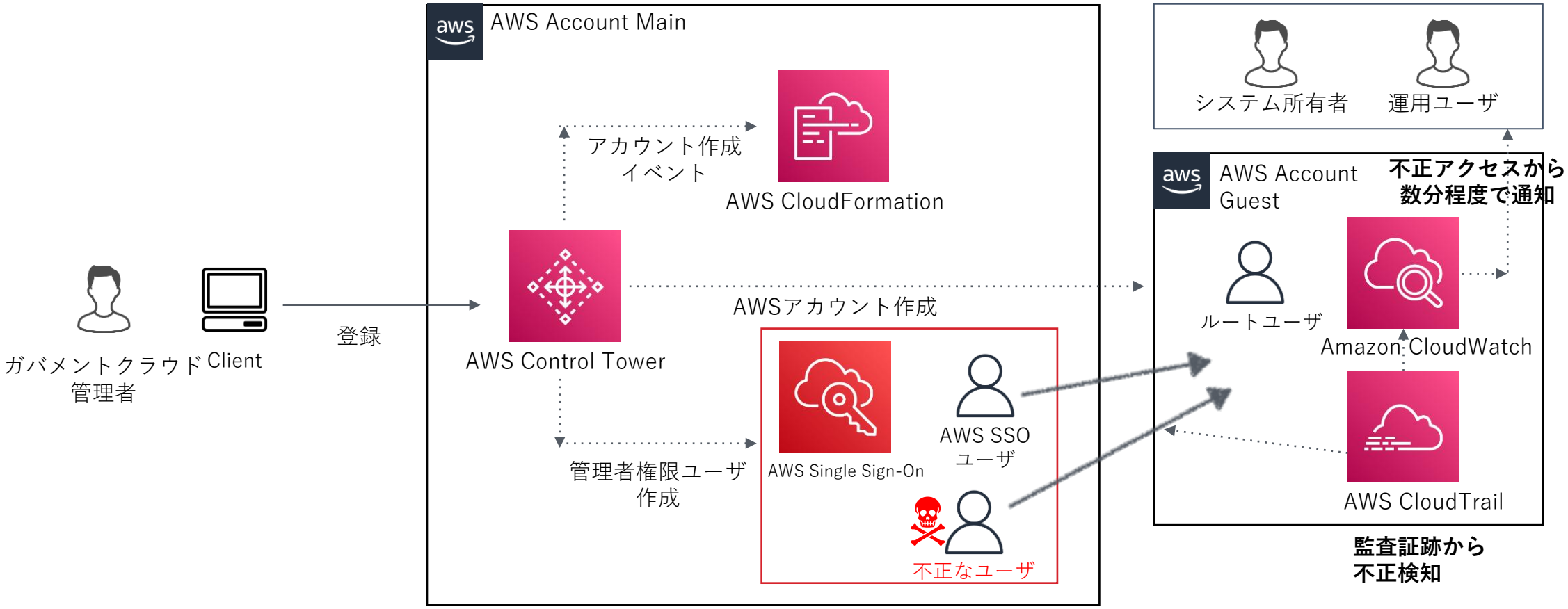
ガバメントクラウド担当者の操作の統制

AWS SSOユーザに関する懸念事項



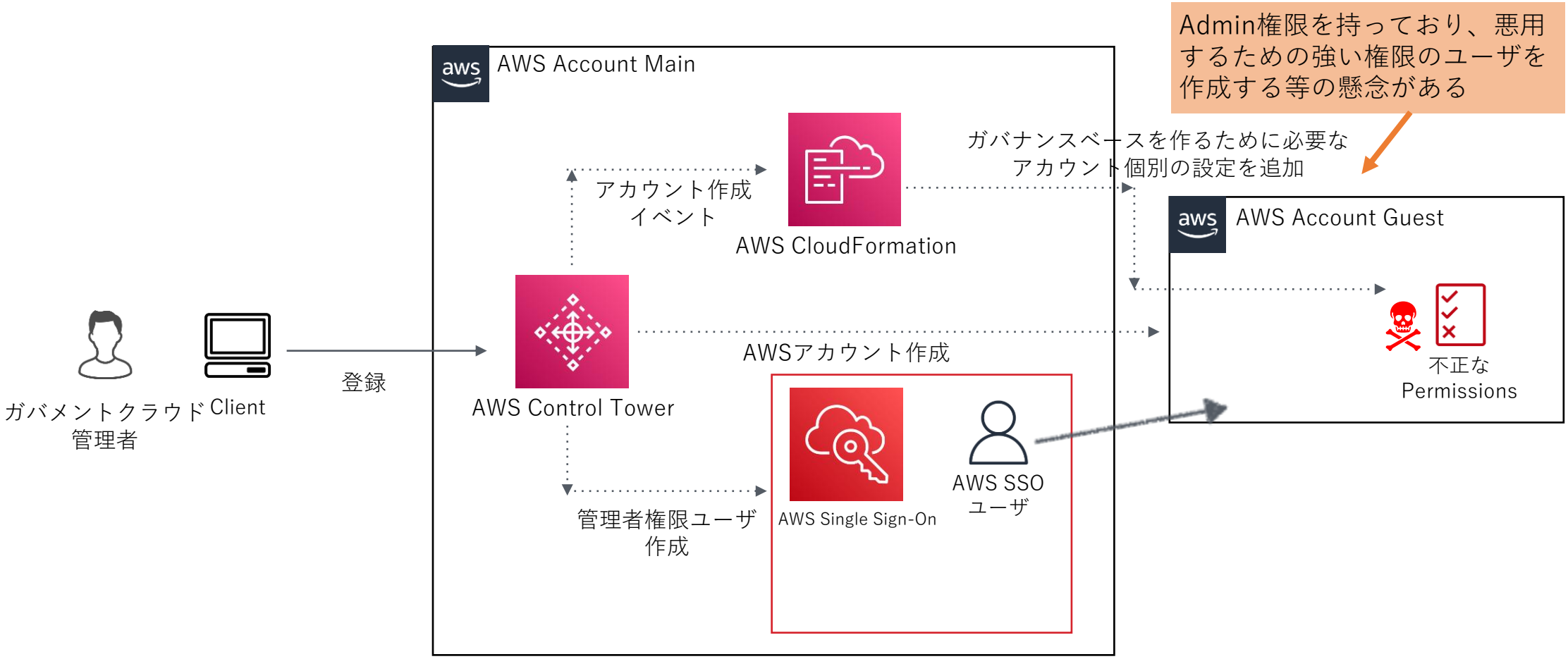
ガバメントクラウド担当者の操作の統制

想定外のユーザによるアクセスが発生した場合、アラートを発行する仕組みをテンプレートとして提供する



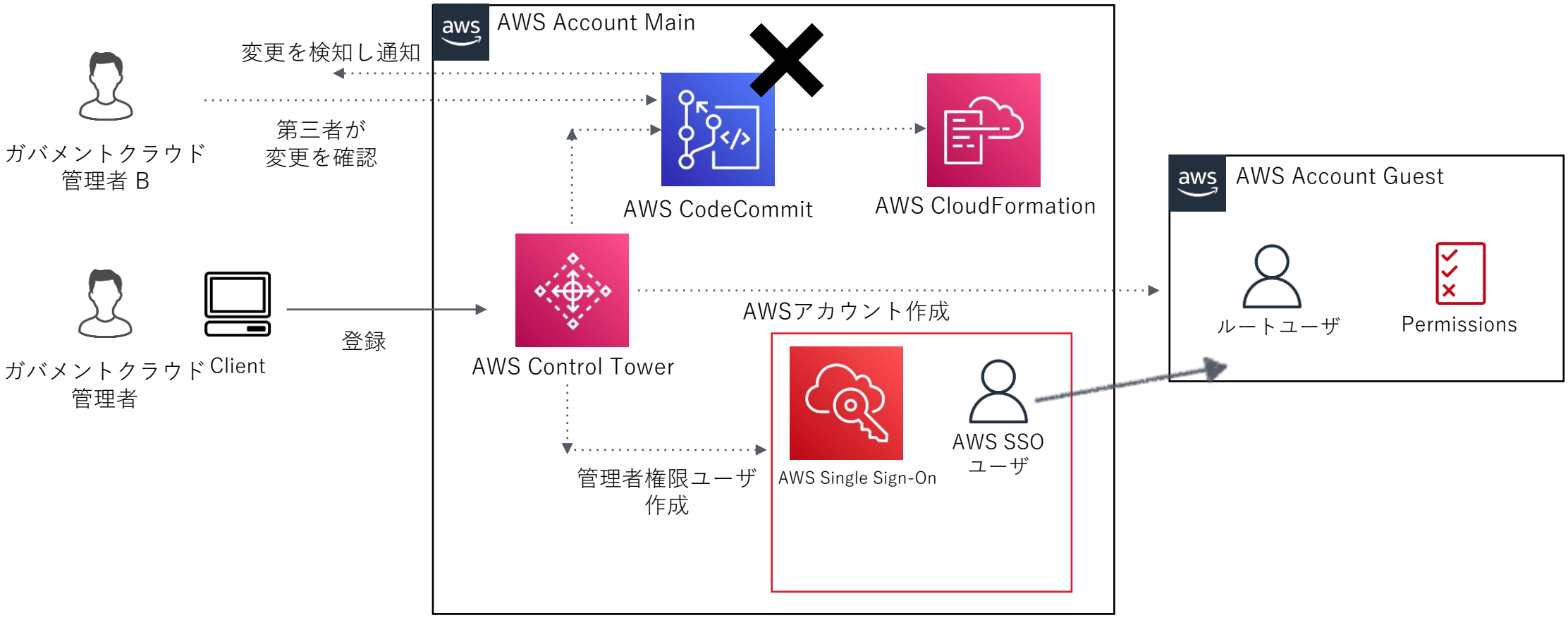
ガバメントクラウド担当者の操作の統制

CloudFormationによるリソース展開での懸念事項



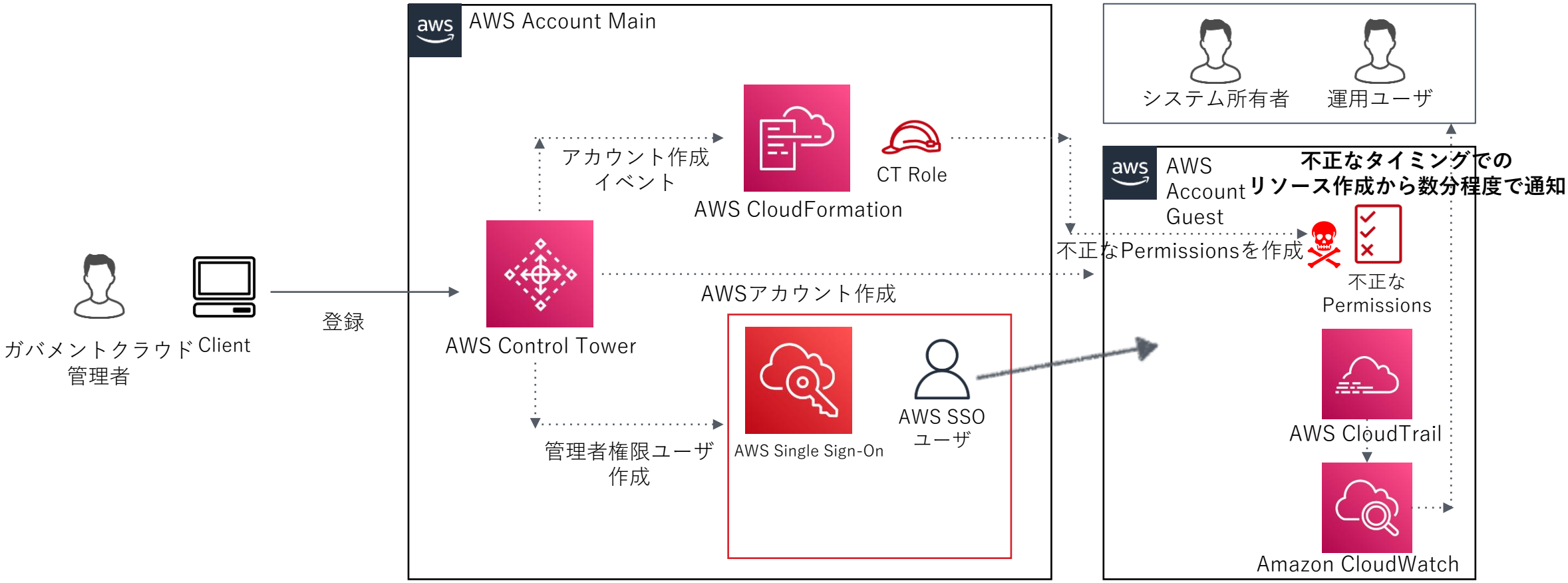
ガバメントクラウド担当者の操作の統制

AWS CodeCommit内のAWS CloudFormationテンプレートがデプロイされるのでテンプレートの変更を検知し不正なリソース作成を防止



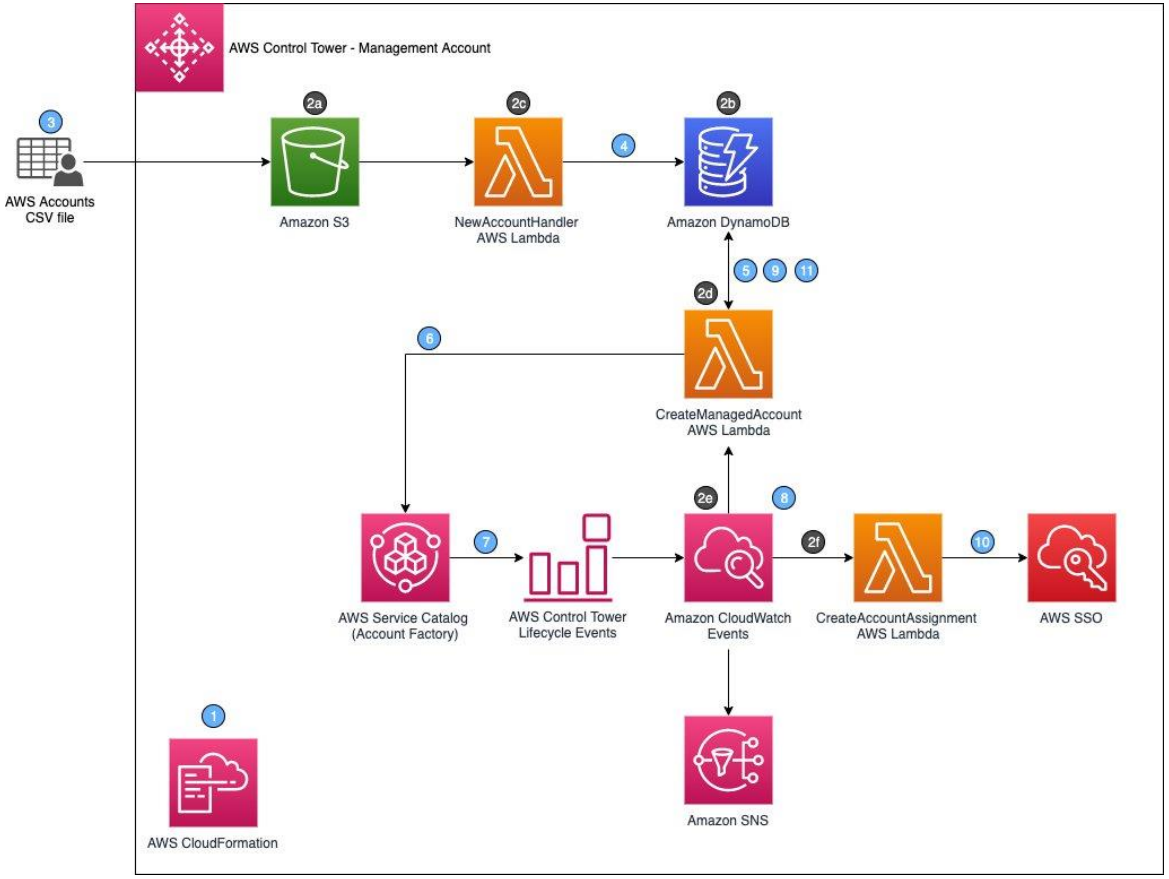
ガバメントクラウド担当者の操作の統制

ガバメントクラウド側が操作した場合アラートを発行するテンプレートを提供し、事前告知なしの通知は不正な操作と判断



アカウント払い出し用ツール

AWSアカウントの作成とAWS SSOユーザの払い出しにAWSサービスを利用



アカウント作成用のCSVをAmazon S3に保存するだけで以下を実施

- AWSアカウントの自動払い出し
  CSVで複数アカウントを一括作成可能
- AWS SSOユーザを作成/グループへ紐付
- アカウント作成完了通知

一部カスタマイズのため改修予定

- 1つのアカウントに紐づく複数のAWS SSOユーザの作成
- SSOグループの指定場所をAmazon DynamoDBに変更
- Amazon DynamoDBのレコード削除でゲストアカウントのOU登録や設定が解除される処理を外す

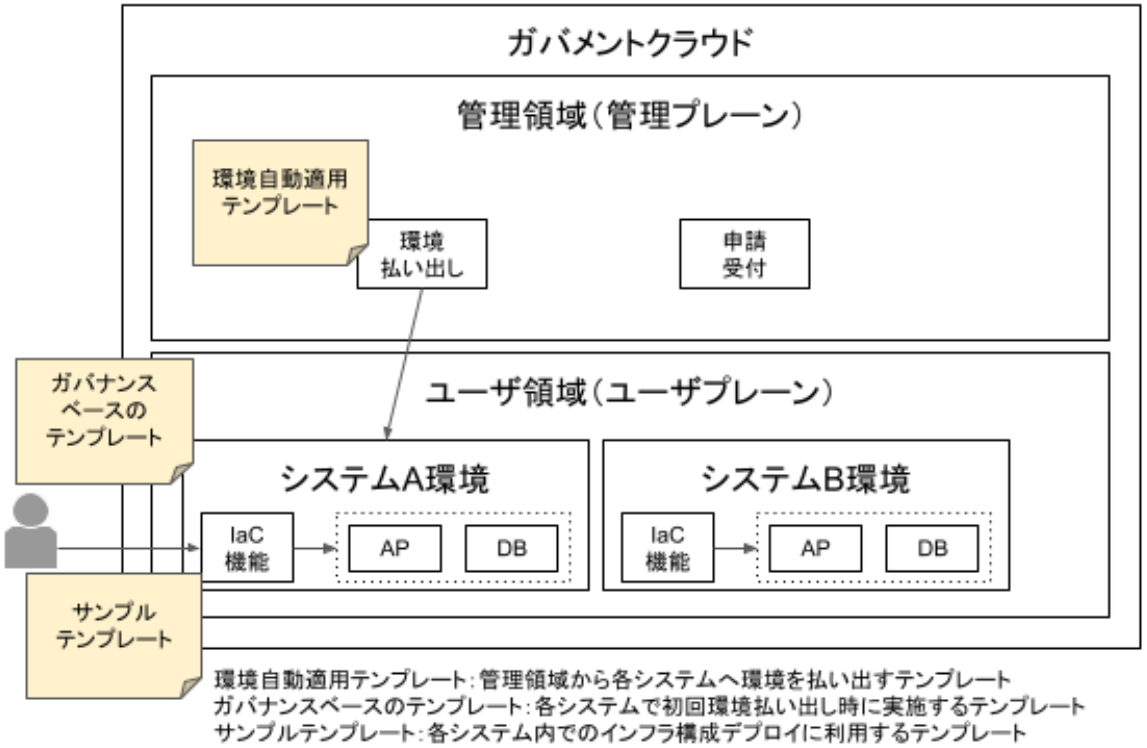
「How to automate AWS account creation with SSO user assignment」
https://aws.amazon.com/jp/blogs/security/how-to-automate-aws-account-creation-with-sso-user-assignment/

第2部 目次

- マルチアカウントの管理方法
  - AWS ControlTowerとAWS Organizations、AWS SSO利用の全体像
  - アカウント払い出し
- IaCテンプレートの活用
  - AWS CDK/AWS CloudFormationの活用
- ガードレールの設定
  - 予防的統制
  - 発見的統制
- 今後の情報展開

IaCテンプレートの活用

ガバメントクラウドとしては、管理領域用の「環境自動適用テンプレート」、利用システムが使うユーザ領域用の「ガバナンスベースのテンプレート」、「サンプルテンプレート」の3つを定義して運用



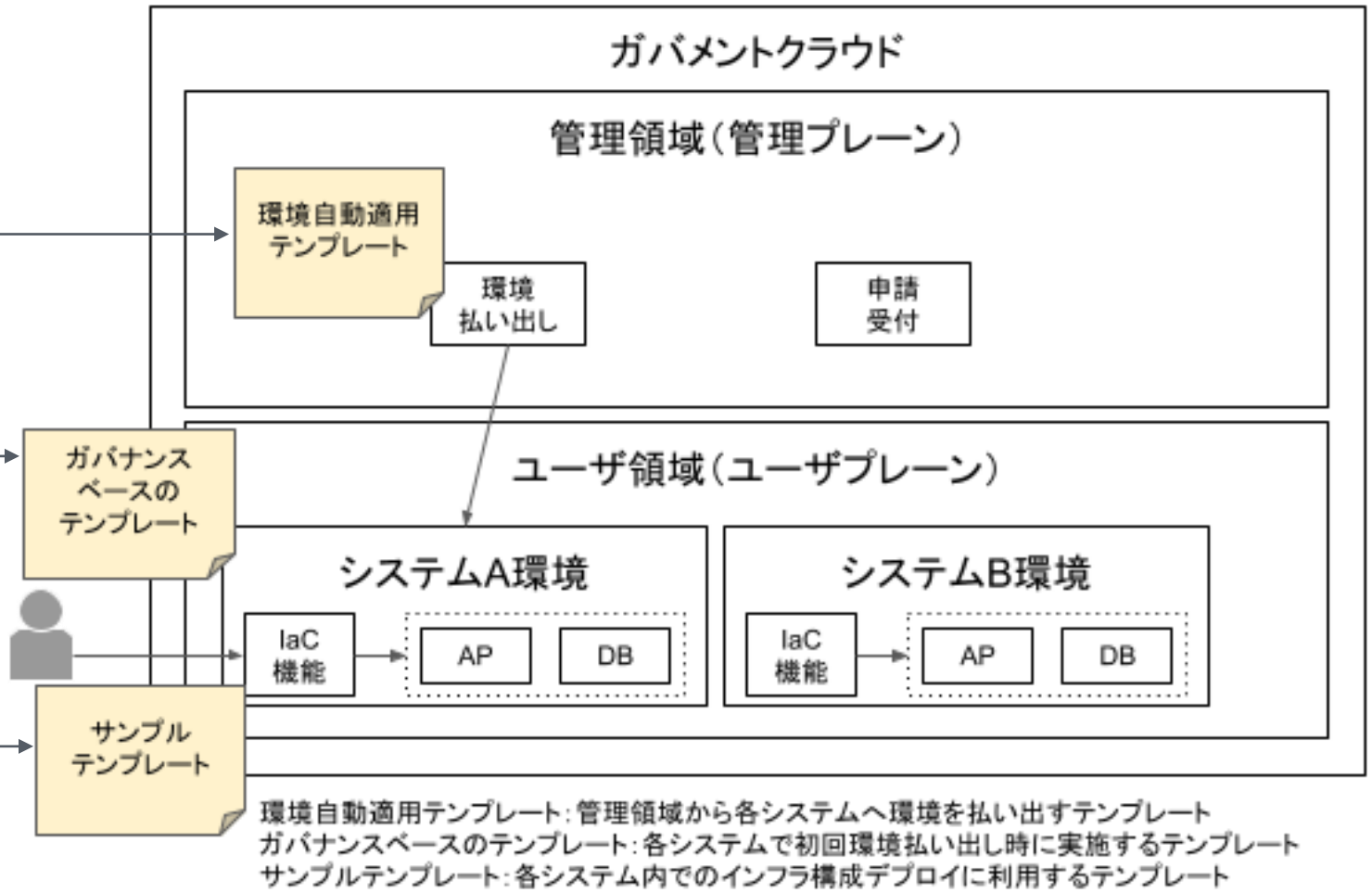
利用方針やなぜ効率的なのかなど、詳しい内容は以下のNoteを参照
「ガバメントクラウドにおけるIaC(Infrastructure as Code)の考え方」
https://cloud-gov.note.jp/n/na2ea9a24e3a1

IaCテンプレートの活用(AWSの場合)

AWS Control Tower、
AWS CDK、
AWS CloudFormarionなど
で実装

AWS CDKの実装を
利用システム側へ提供し、
初回実行してもらう

一般的な構成での実装例を
AWS CDKで提供
自治体先行事業や各種サービスでの結果をヒアリング
しニーズを確認後再実装



「ガバメントクラウドにおけるIaC(Infrastructure as Code)の考え方」https://cloud-gov.note.jp/n/na2ea9a24e3a1

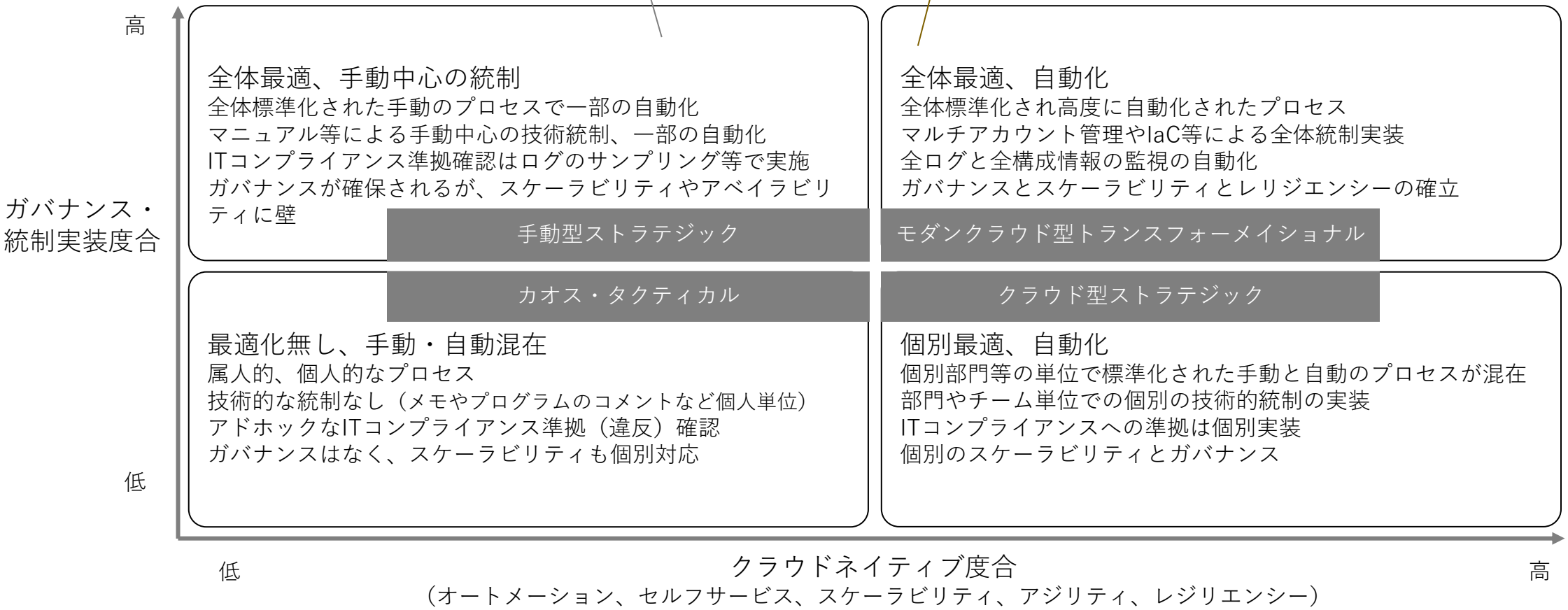
第2部 目次

- マルチアカウントの管理方法
  - AWS ControlTowerとAWS Organizations、AWS SSO利用の全体像
  - アカウント払い出し
- IaCテンプレートの活用
  - AWS CDK/AWS CloudFormationの活用
- ガードレールの設定
  - 予防的統制
  - 発見的統制
- 今後の情報展開

ガードレール方式による技術ガバナンス

ゲートキーパー方式による技術ガバナンス実現
機能利用の事前承認や境界防御による経路の集約管理はスケーラビリティや柔軟性にとってボトルネックになり、全量チェックできずITコンプライアンス準拠確認も部分的になる

ガードレール方式による技術ガバナンス実現
ITコンプライアンス違反となる操作を未然に防ぐこと（予防的統制）と、違反の疑いや違反の予兆を検知すること（発見的統制）により、スケーラビリティや柔軟性を維持しつつ技術ガバナンスを実現



予防的統制と発見的統制

- 予防的統制 … 危険性の高い操作を事前に防止
  - 実装方法
    - AWS OrganizationsのService Control Policy(SCP)
- 発見的統制 … リソースが不正な状態か監視/通知
  - 実装方法
    - AWS Security Hub
    - Amazon GuardDuty
    - Amazon CloudTrail
    - Amazon CloudWatch Logs/Alarm など

- ガバメントクラウドとして実現したい統制が既存のAWSサービスで
  足りない場合はAWS Control Towerカスタマイズソリューションで追加実装

予防的統制

方針：全てのシステムに共通して必要な最低限の統制だけ実施
　　本年度は検証期間のためアグレッシブに変更しつつ運用する

- 設定内容
  - ガバメントクラウドで設定するセキュリティや監査ログの設定/収集に関するサービスの削除防止
  - 東京/大阪リージョン以外の使用禁止、未有効化リージョンの有効化禁止
  - セキュリティ統制が実現しにくいとチームで判断したサービスの禁止
  - IAMユーザにMFAの有効化を強制し必要な権限はIAMロールで管理
  - アクセスキーの作成を禁止
- 各システムAdminユーザ(AWS SSOユーザ)以外は実行不可とする内
  - IAMユーザの作成
  - 一度の誤操作で高額請求となるサービスの購入/実行防止
    (例.RI購入やShield Advanced有効化など)

発見的統制

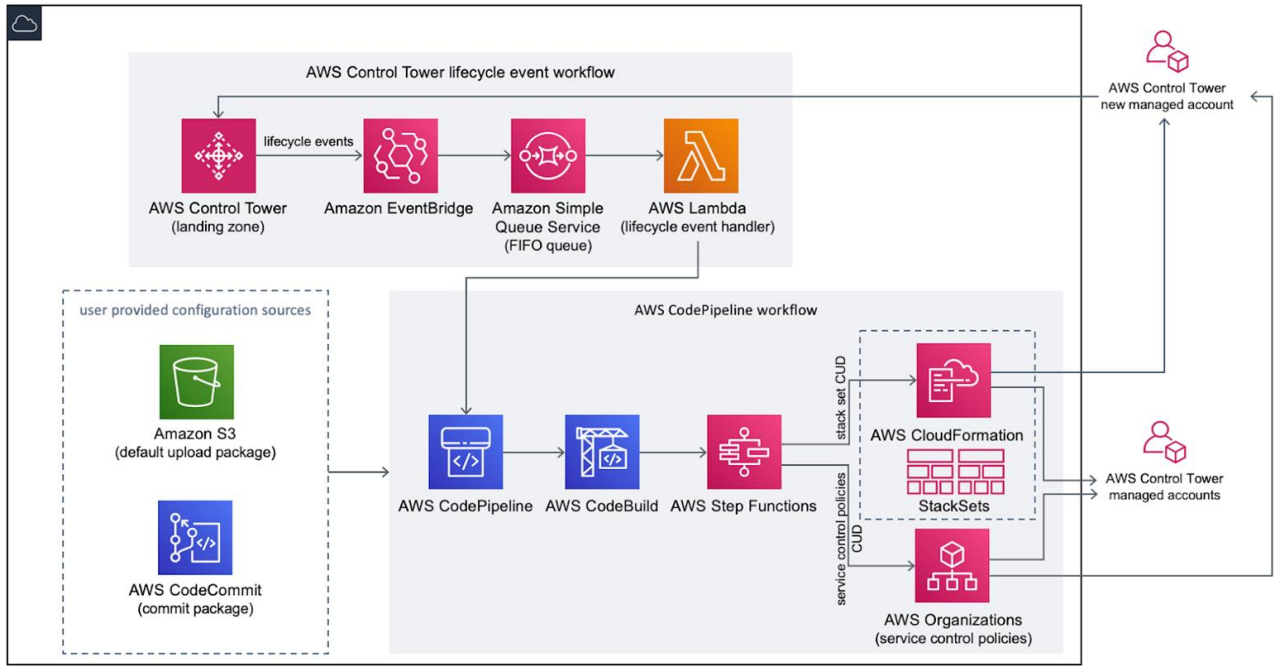
方針：AWS が提供するセキュリティサービスの設定をリスト化し必要な
　　対策は可能な限り既存のサービス(AWS Control Tower, AWS Configなど)で実現する

既存サービスの設定リスト

サービス	項目		設定箇所	統制タイプ	場
Control Tower	ルートユーザーのアクセスキーの作成を許可しない	標準 - 推奨	CT SCP	予防的統制	コ
Control Tower	root ユーザーとしてのアクションを禁止する	標準 - 推奨	CT SCP	予防的統制	コ
Control Tower	Amazon EC2 インスタンスにアタッチされた Amazon EBS ボリュームの暗号化が有効になっているかどうかを検出する	標準 - 推奨	CT Config Rule	発見的統制	コ
Control Tower	無制限の着信 TCP トラフィックが許可されているかどうかを検出する	標準 - 推奨	CT Config Rule	発見的統制	コ
Control Tower	SSH を介した無制限のインターネット接続が許可されているかどうかを検出する	標準 - 推奨	CT Config Rule	発見的統制	コ
Control Tower	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	標準 - 推奨	CT Config Rule	発見的統制	コ
Control Tower	Amazon S3 バケットへのパブリック読み取りアクセスが許可されているかどうかを検出する	標準 - 推奨	CT Config Rule	発見的統制	コ
Control Tower	Amazon S3 バケットへのパブリック書き込みアクセスが許可されているかどうかを検出する	標準 - 推奨	CT Config Rule	発見的統制	コ
Control Tower	Amazon EBS ボリュームが Amazon EC2 インスタンスにアタッチされているかどうかを検出する	標準 - 推奨	CT Config Rule	発見的統制	コ
Control Tower	Amazon EC2 インスタンスの Amazon EBS 最適化が有効になっているかどうかを検出する	標準 - 推奨	CT Config Rule	発見的統制	コ
Control Tower	Amazon RDS データベースインスタンスへのパブリックアクセスが有効になっているかどうかを検出する	標準 - 推奨	CT Config Rule	発見的統制	コ
Control Tower	Amazon RDS データベーススナップショットへのパブリックアクセスが有効になっているかどうかを検出する	標準 - 推奨	CT Config Rule	発見的統制	コ
Control Tower	Amazon RDS データベースインスタンスのストレージ暗号化が有効になっているかどうかを検出する	標準 - 推奨	CT Config Rule	発見的統制	コ
Control Tower	Amazon S3 バケットの暗号化設定の変更を許可しない [以前の: Enable Encryption at Rest at Rest	標準 - 選択	CT SCP	予防的統制	コ
Control Tower	Amazon S3 バケットのロギング設定の変更を許可しない [以前のバージョン: Enable Access Logging for Log Archive	標準 - 選択	CT SCP	予防的統制	コ

予防的/発見的統制を追加実装する方法

各アカウント向けに統制用のリソースをデプロイするためAWS Control Towerカスタマイズソリューション(CfCT)を利用



機能の概要

- AWS CodeCommitかAmazon S3にAWS CloudFormationのテンプレートを配置すると、特定のOUやアカウントに向けてStack Setsが起動しリソースが展開される
- 新規アカウント作成時は、自動的にテンプレートが実行される
- AWS CodeCommitを使うことで承認フローの実装も可能

足りない部分

- 各アカウントでのAWS CloudFormationの実行だけ可能なのでAPI実行がしたい場合は、別途アカウント作成イベントに応じたAWS Step Functionsの実装が必要
- AWS CDKに未対応

https://controltower.aws-management.tools/ja/automation/cfct/

第2部 目次

- マルチアカウントの管理方法
  - AWS ControlTowerとAWS Organizations、AWS SSO利用の全体像
  - アカウント払い出し
- IaCテンプレートの活用
  - AWS CDK/AWS CloudFormationの活用
- ガードレールの設定
  - 予防的統制
  - 発見的統制
- 今後の情報展開

今後の情報展開

クラウドチームの目標や狙い、設計など検討した内容はデジタル庁ガバメントクラウドnoteにて発信

https://cloud-gov.note.jp/

Thank you!

山本 教仁
デジタル庁
クラウドチーム/Cloud Architect

佐藤 智樹
デジタル庁
クラウドチーム/Cloud Engineer