AWS Builders Online Series

AWS Control Tower で始める はじめての AWSアカウント管理

白石 一乃

アマゾン ウェブ サービス ジャパン合同会社
AWS 技術統括本部 西日本ソリューション部
ソリューションアーキテクト

自己紹介

白石 一乃 (しらいし いちの)

ソリューションアーキテクト

- 西日本のお客様をメインで担当
- 国内Sier出身 Webアプリ開発、プロトタイピング、PM

好きなAWSのサービス：

AWS Control Tower

AWS Single Sign-On (SSO)

AWS CloudFront

AWS Elastic Beanstalk

本セッションは…

想定受講者

- AWS をつかい始めたばかりの方
- AWS アカウント管理に興味や疑問を感じている方
- 「AWS Control Tower」という言葉に惹かれた方

ゴール

- AWSのベストプラクティスに則った環境を、AWS Control Tower という 1 つのサービスですぐに構築、始めることができるということを知っていただくこと
- AWSのアカウント管理に自信を持っていただくこと

AWS Control Tower

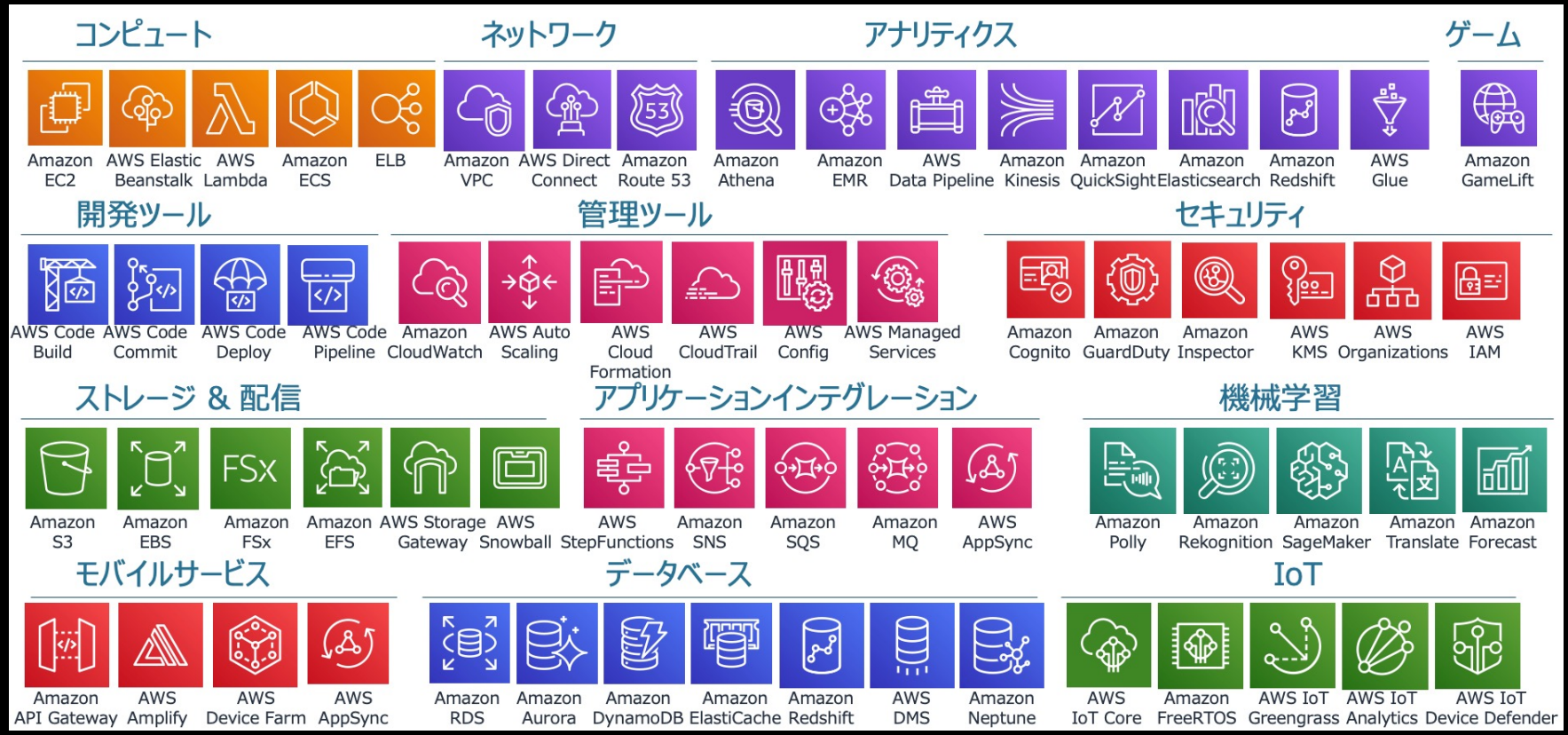
- ベストプラクティスに基づくAWS環境
- 数クリックで利用開始
- マネージド型サービス
- 無償で利用可能

アジェンダ

- AWS アカウント とは
- AWS Control Tower のご紹介
- AWS Control Tower ４つの機能
- まとめ・次の一歩

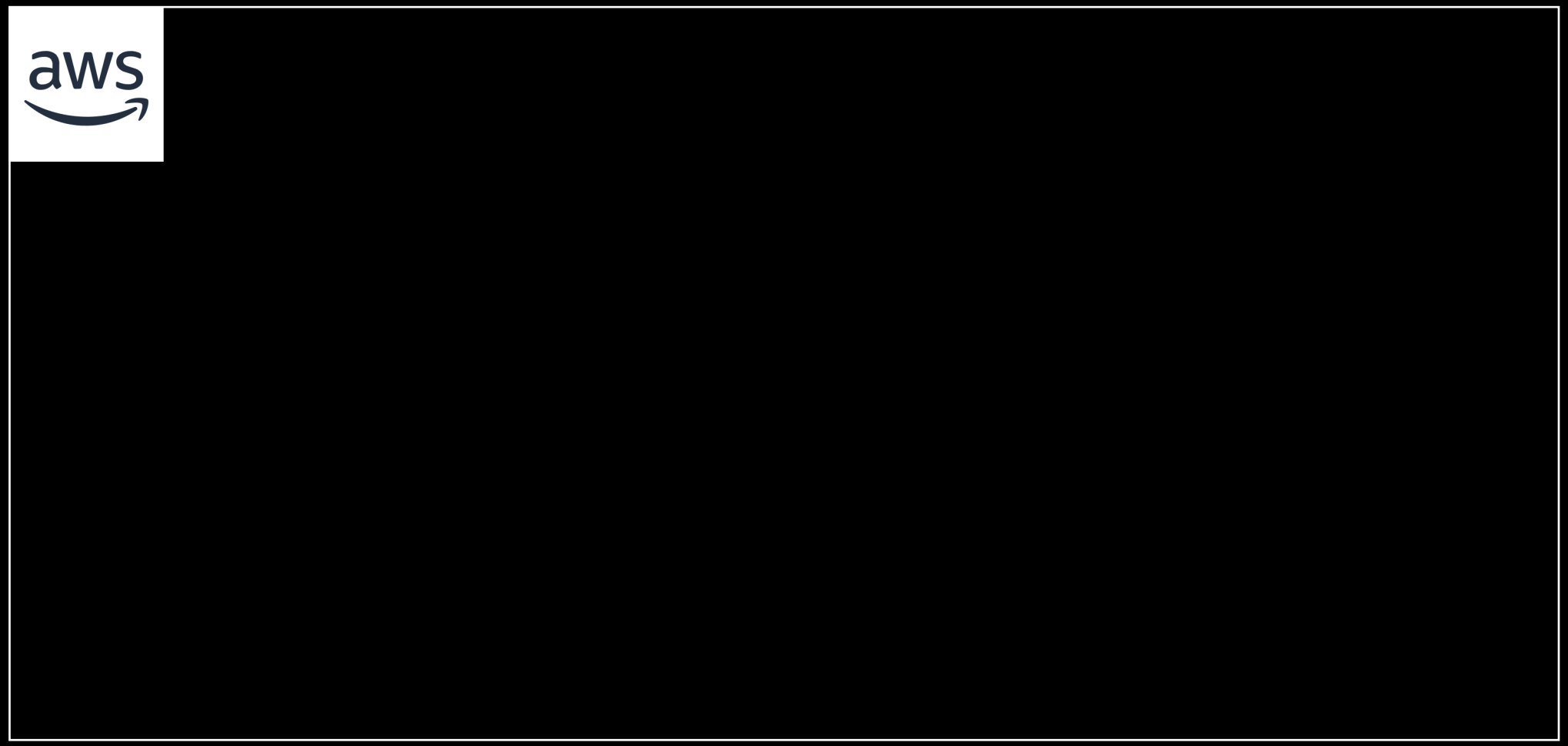
AWSアカウントとは

AWSの200種類以上のサービス、使い始めるには…



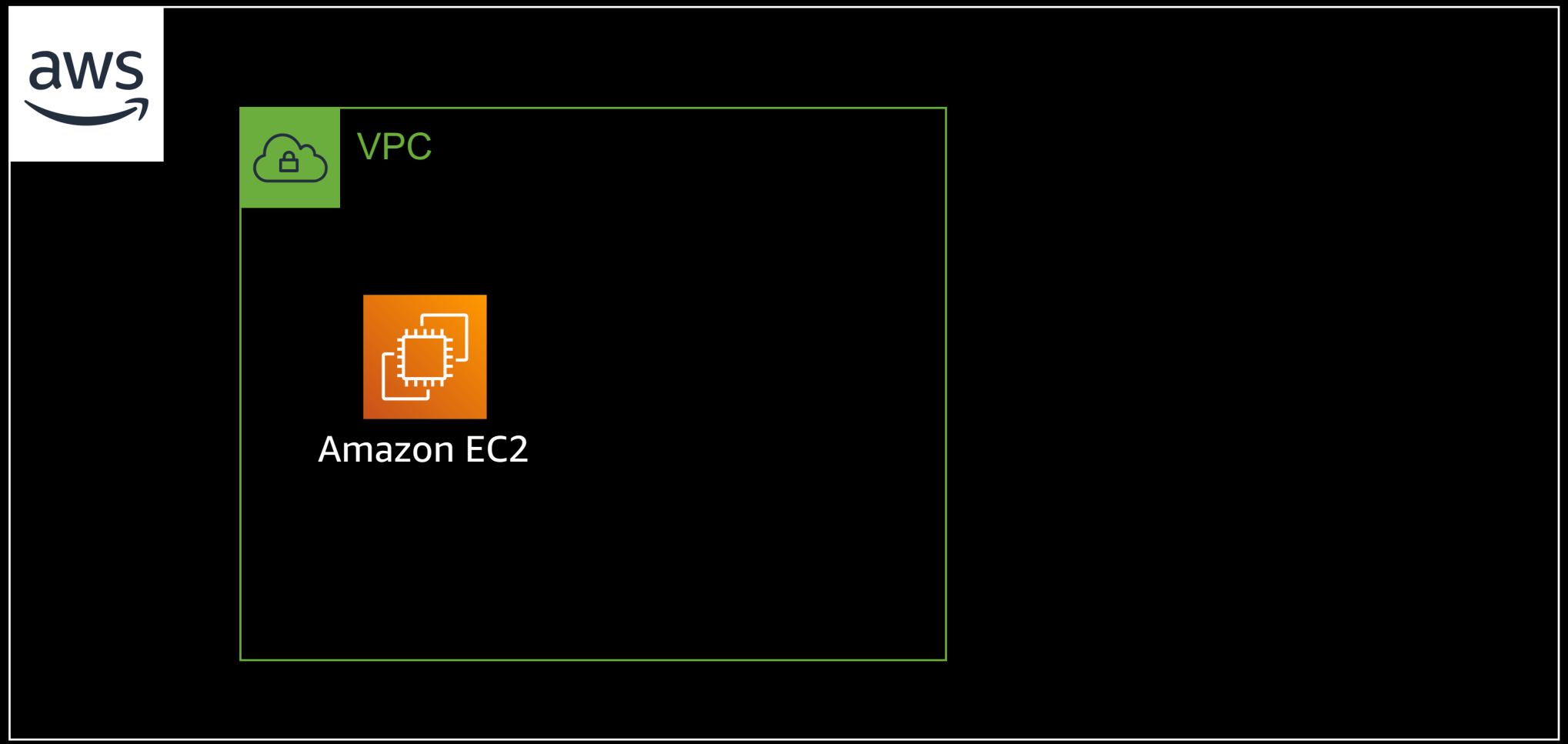
AWSの200種類以上のサービス、使い始めるには…

AWSアカウント ＝ 区画

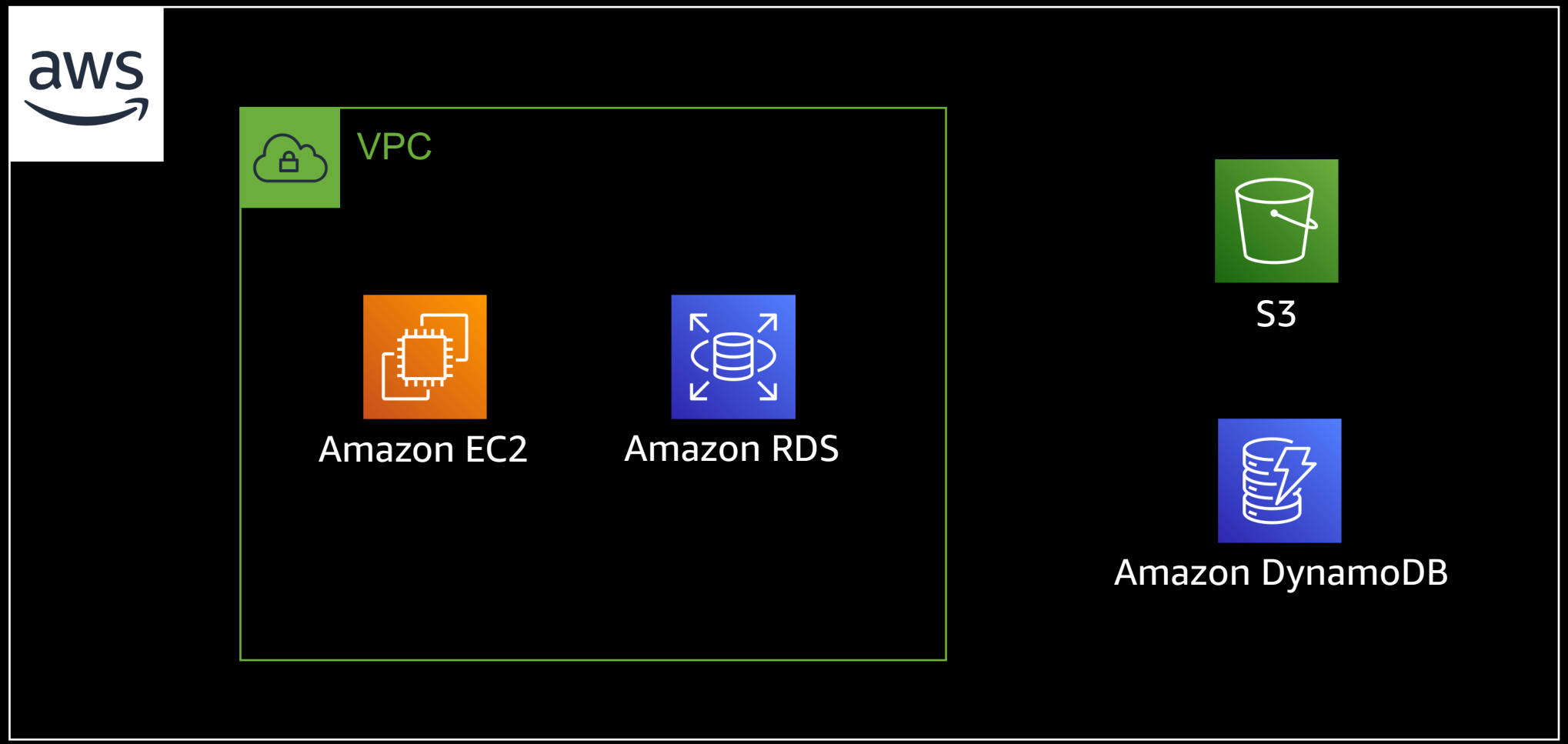


AWSアカウント ＝ 区画

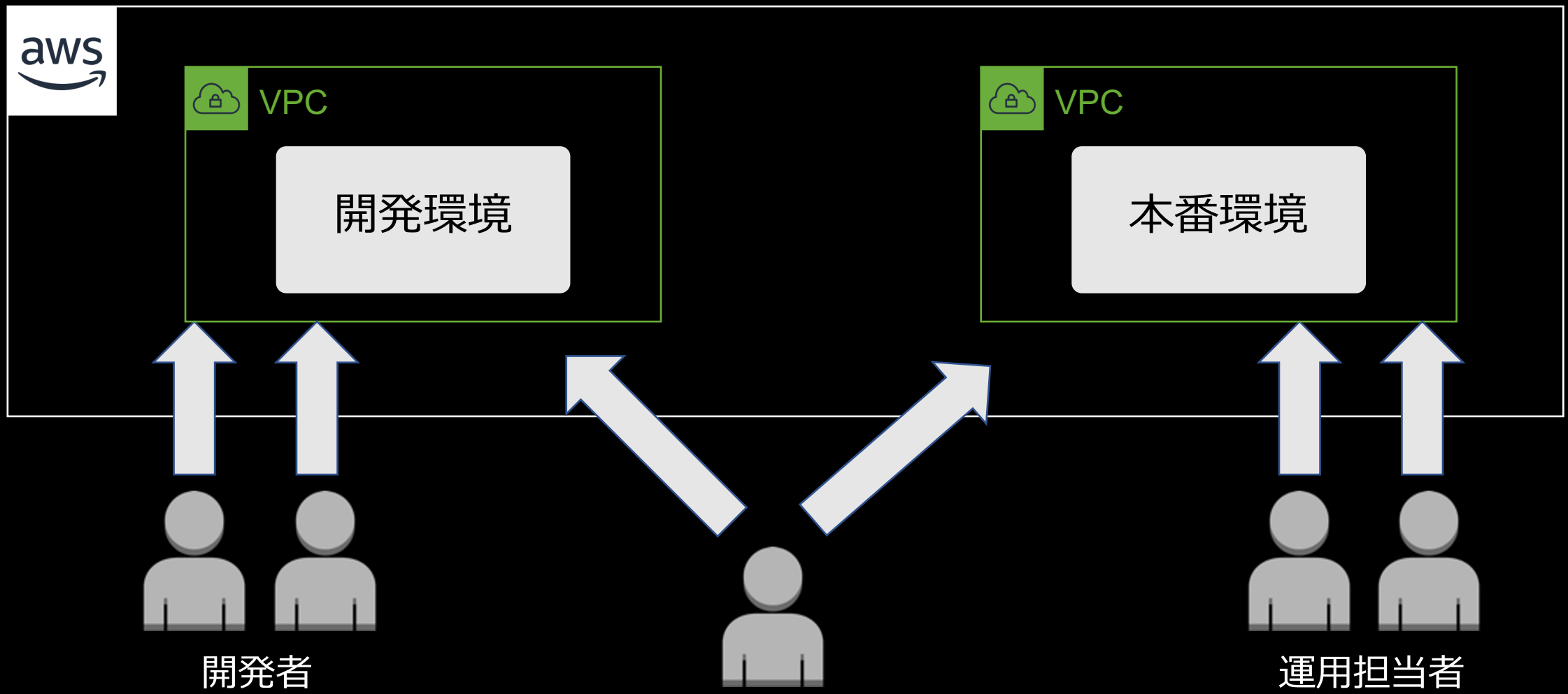
AWSアカウント ＝ 区画



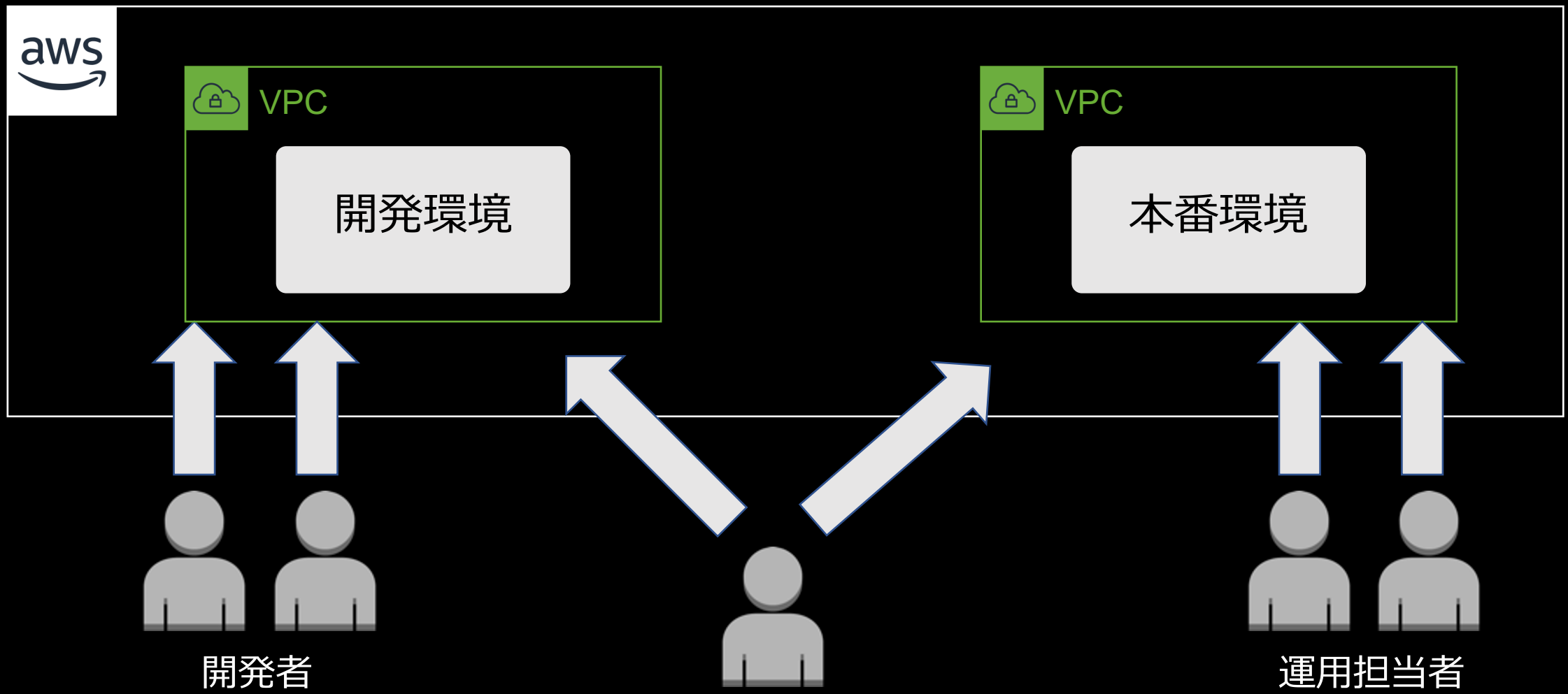
AWSアカウント ＝ 区画



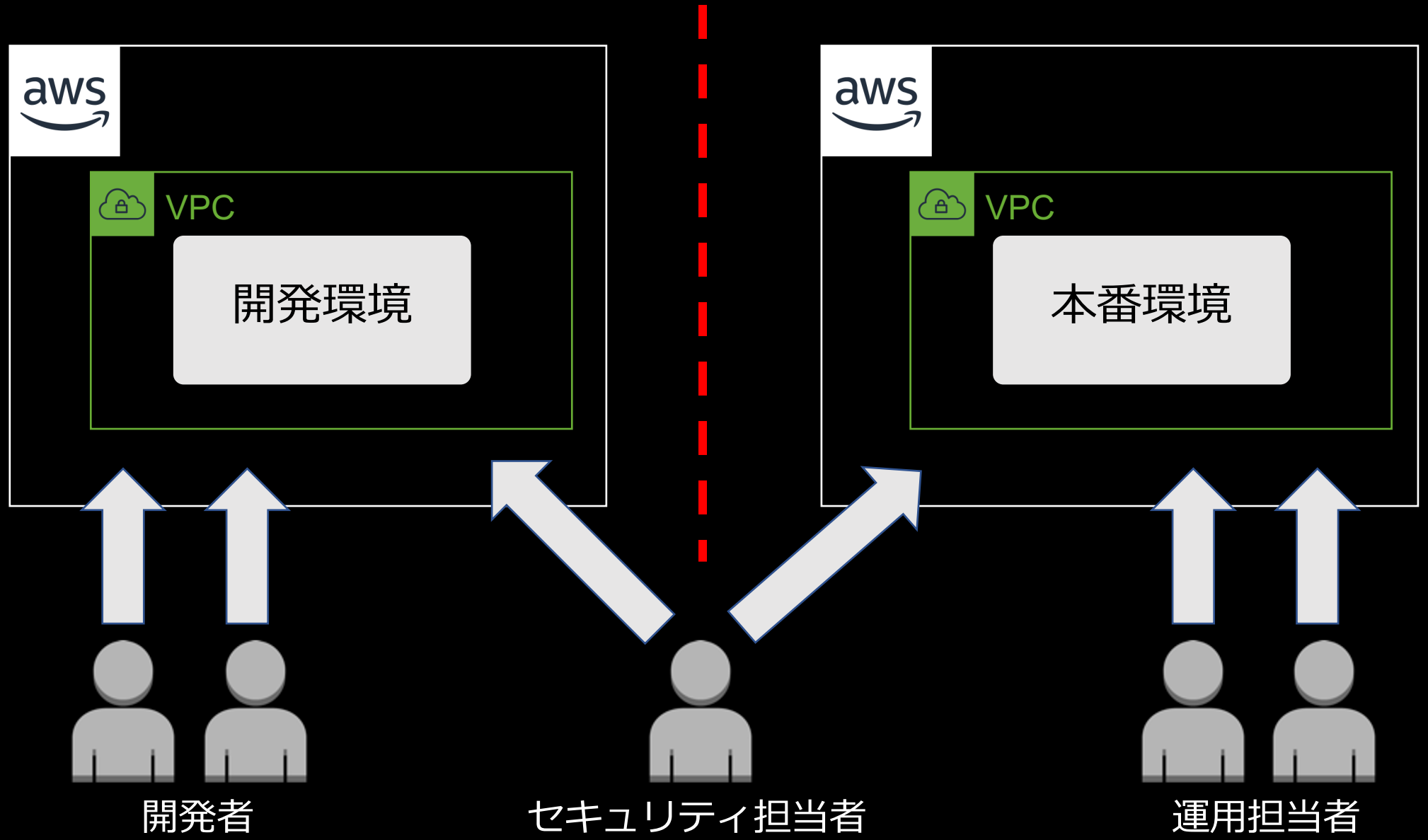
AWSアカウントを**複数人で利用することができる**



AWSアカウントを**複数人で利用することができる**



複数のAWSアカウントをもつことができる



AWSアカウントとは

AWSアカウント

- 様々なサービスを利用するための**区画**。
- **複数のユーザで利用**することができる。
- 単一の人・組織が**AWSアカウントを複数所有して**環境を分離することができる。

AWSアカウントが実現すること

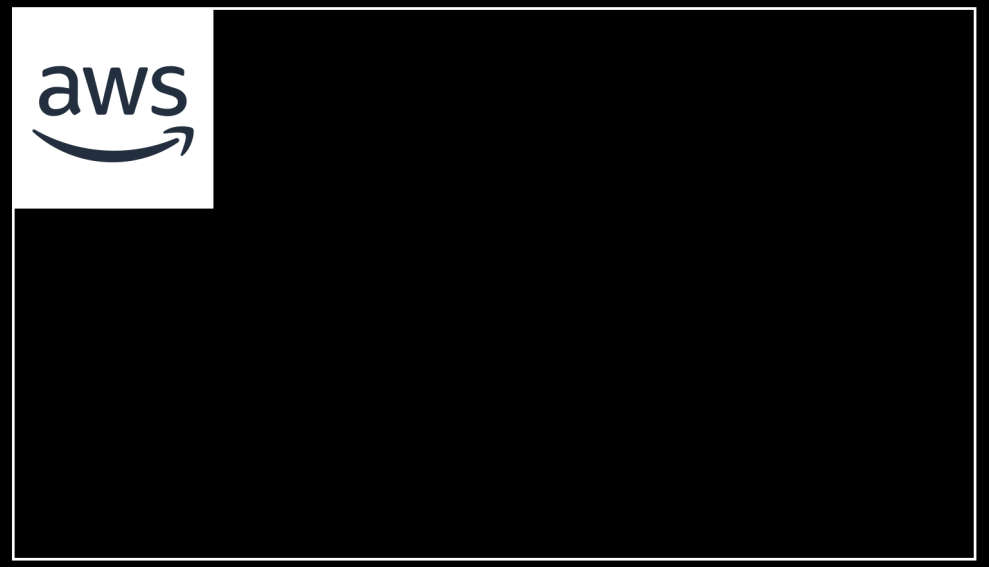
セキュリティ境界

リソースの分離

課金の分離

AWSアカウントをどう展開するか

単一のアカウントで構成

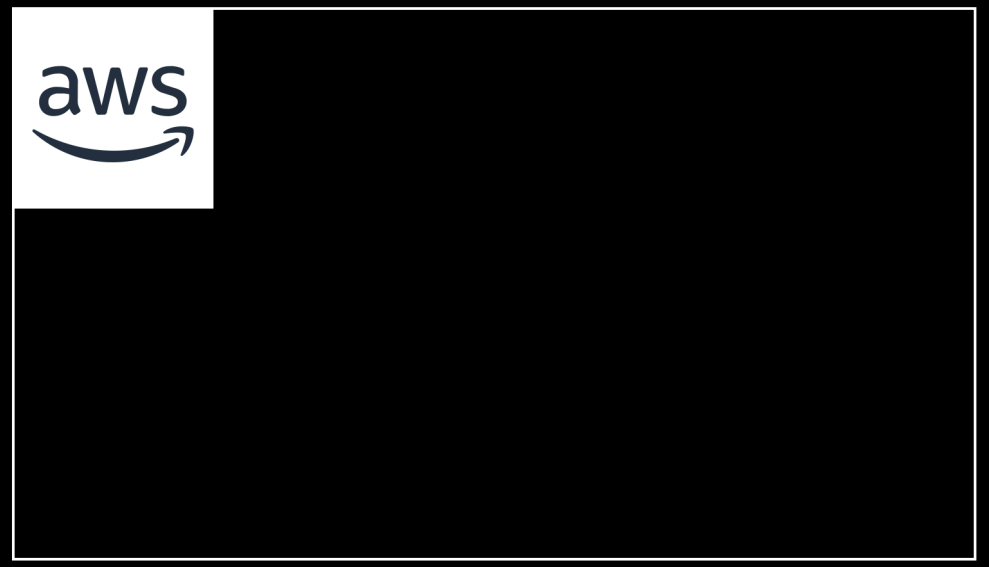


OR

複数のアカウントで構成

AWSアカウントをどう展開するか

単一のアカウントで構成



OR

複数のアカウントで構成

推奨

AWSアカウントをどう展開するか

単一のアカウントで構成

OR

「マルチアカウント構成」と呼ぶ

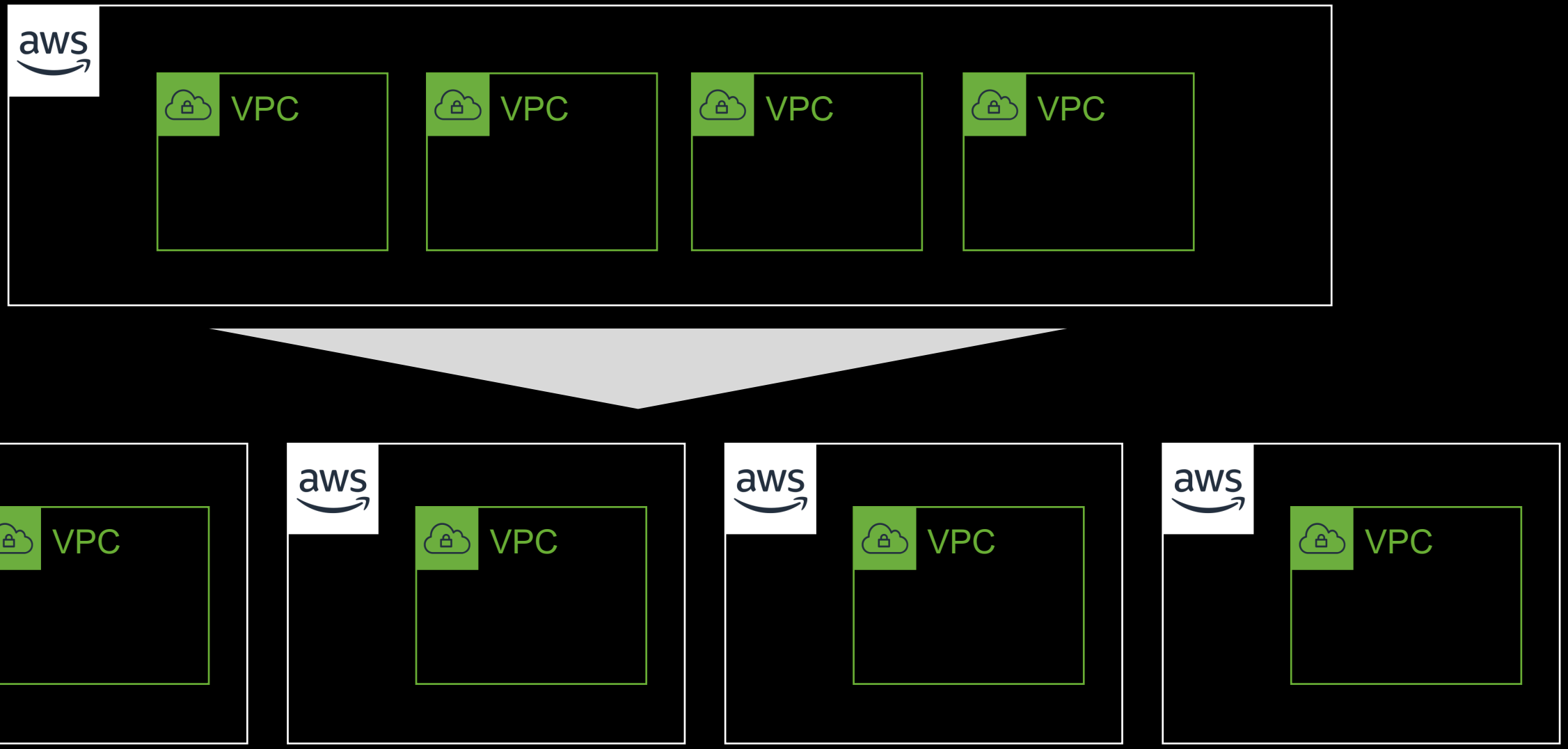
複数のアカウントで構成

推奨

単一のアカウントで構成した場合…

Everything

だから、マルチアカウント構成



マルチアカウント構成に対するよくある疑問

AWS Control Tower のご紹介

AWS Control Tower

再掲

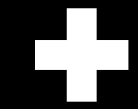
- ベストプラクティスに基づくAWS環境
- 数クリックで利用開始
- マネージド型サービス
- 無償で利用可能

AWS Control Tower の コンセプト

- ベストプラクティスに則った環境やテンプレートがあれば、

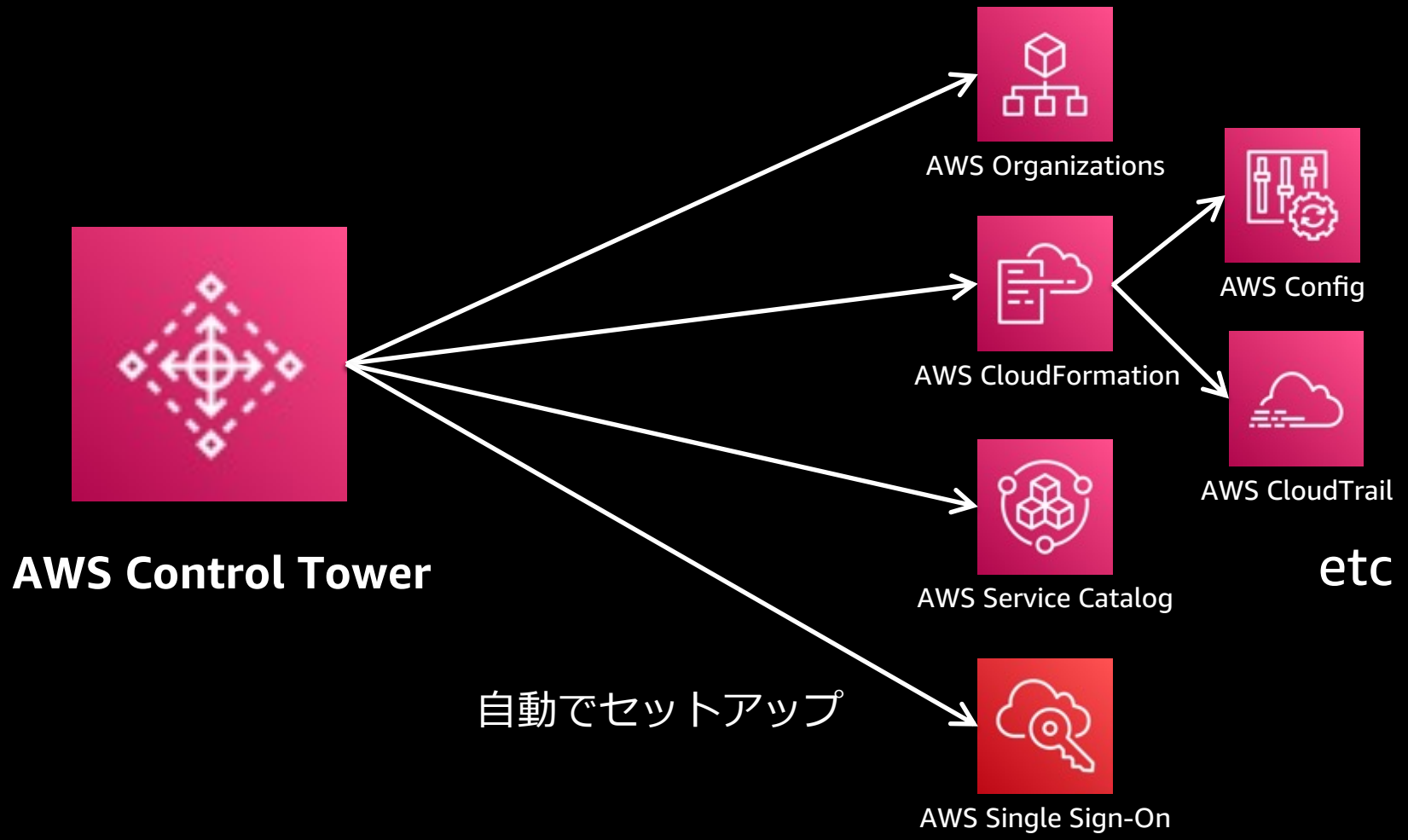
  お客様は車輪の再発明に工数を割かず、ロケットスタートができる

マルチアカウント構成
はじめの一歩

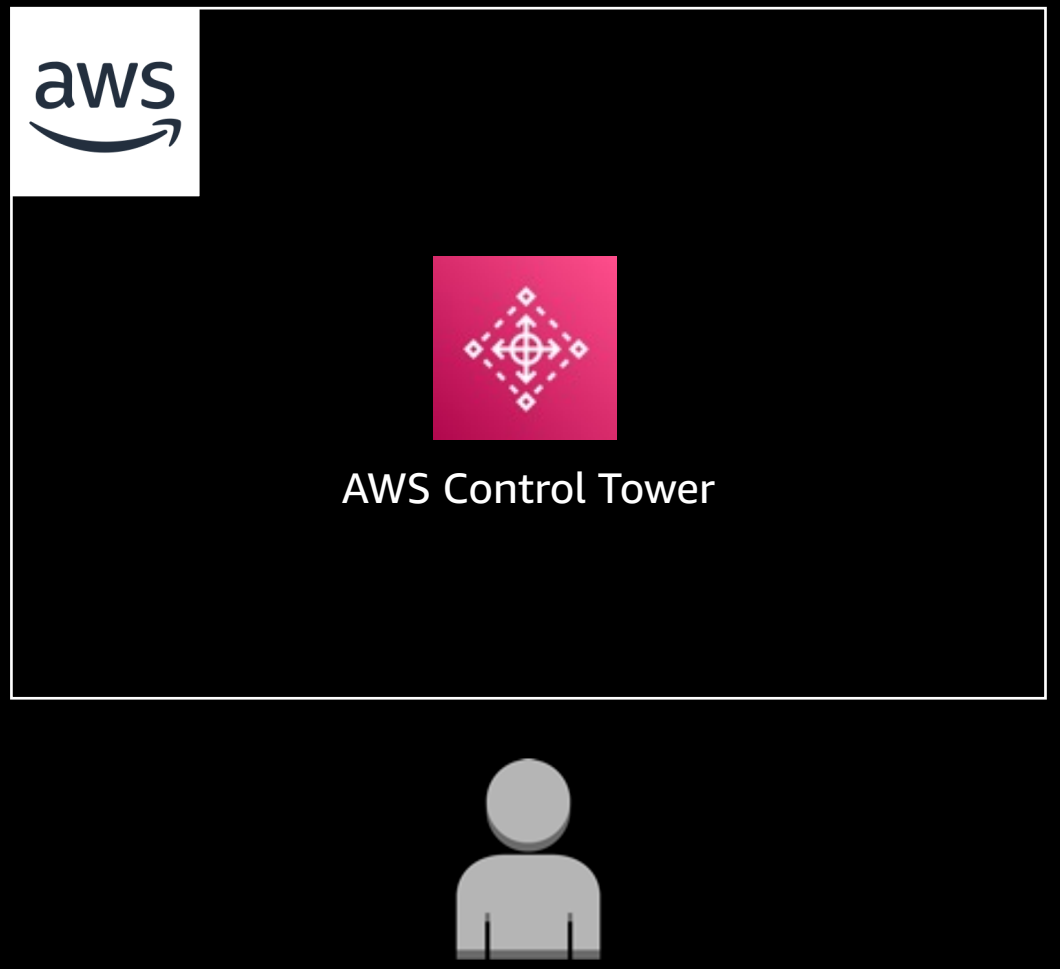


役立つプリセット

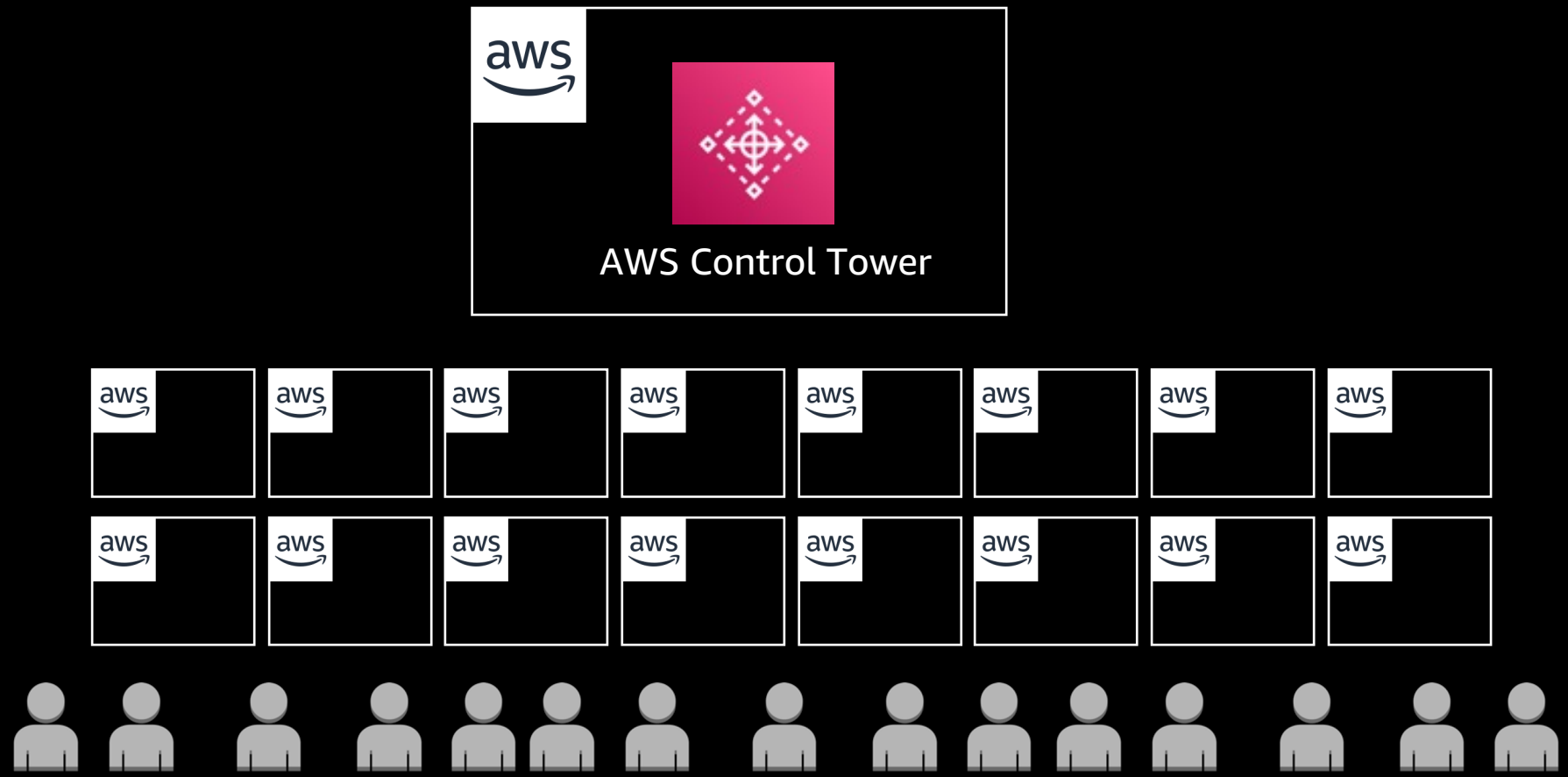
AWS Control Tower の仕組み



ユースケース（１）
これからAWSの利用を始める方



ユースケース（2）
既に複数のAWS環境を運用している方



AWS Control Tower 4つの機能

AWS Control Tower 4 つの機能

① シングルサインオン

複数のAWSアカウントへの
ログインの切り替え

② ログ集約

AWSの操作ログの
自動収集

③ ガードレール

リスクのある操作の
予防・発見

④ アカウント作成

新規AWSアカウントの
自動セットアップ

① シングルサインオン

複数のAWSアカウントへのログインの切り替え

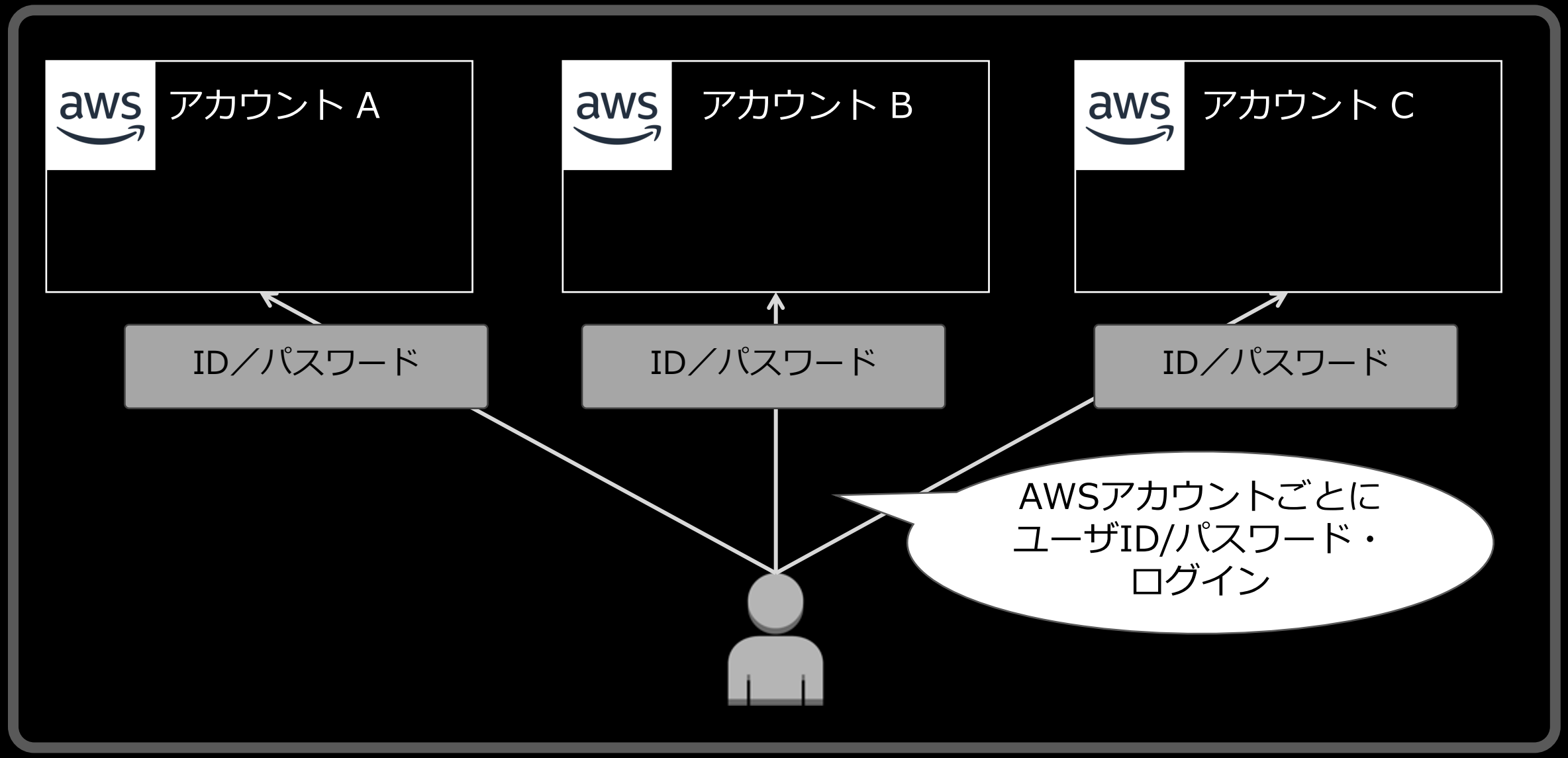
（課題）アカウントの数だけログイン処理

アカウント A

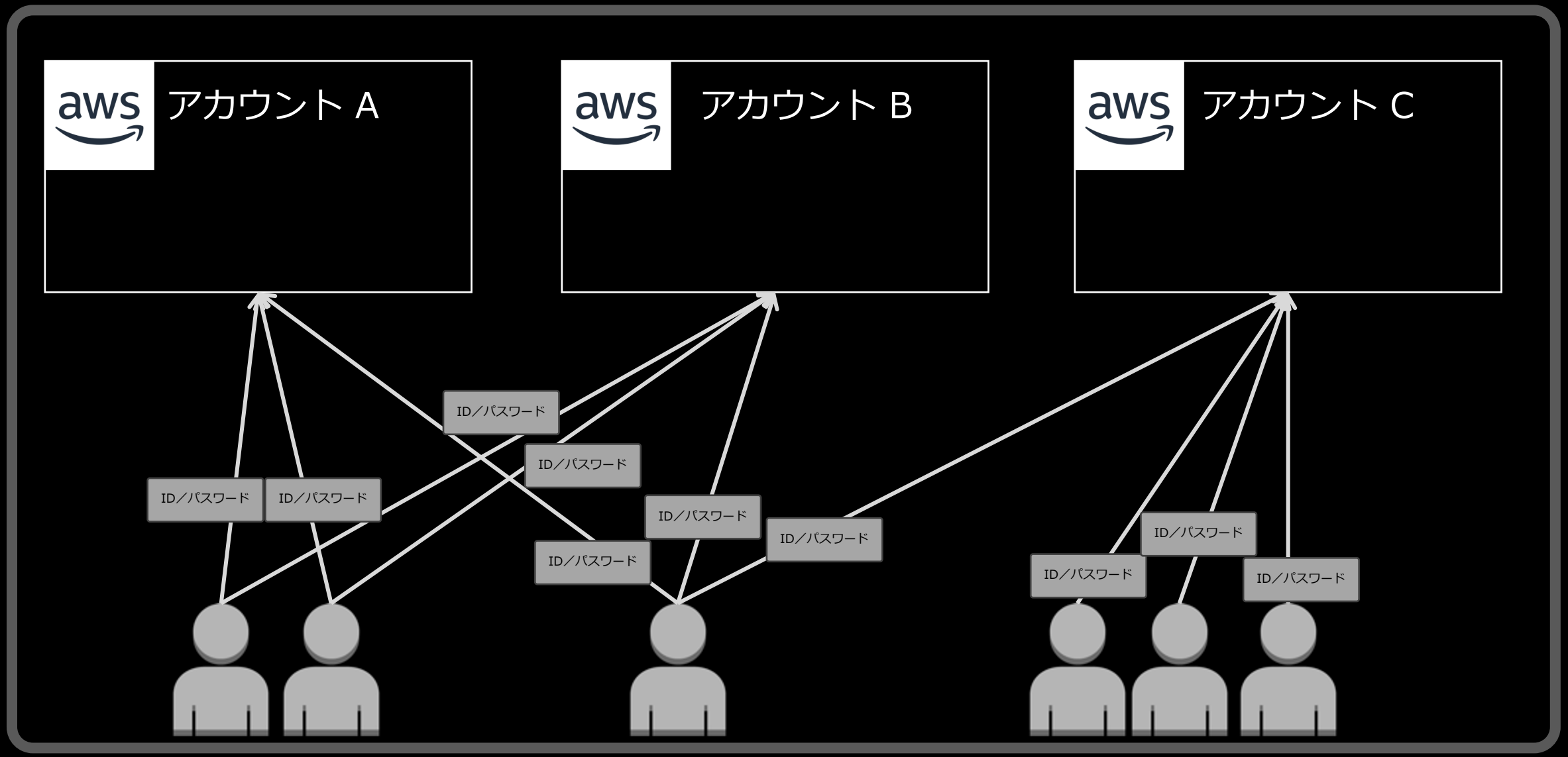
アカウント B

アカウント C

（課題）アカウントの数だけログイン処理

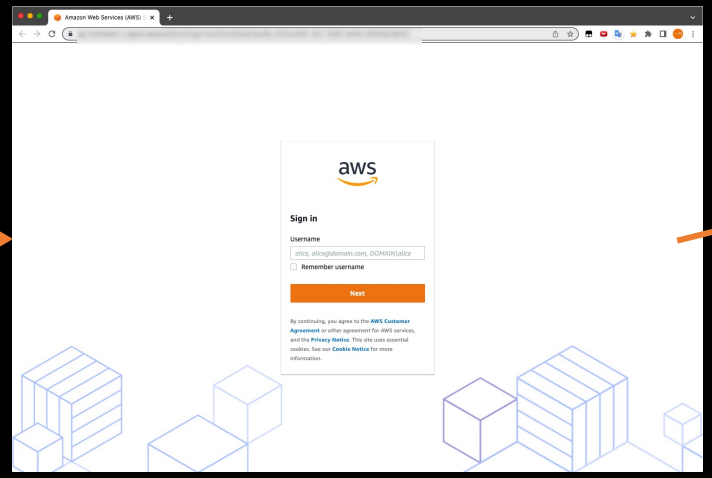


（課題）アカウントの数だけログイン処理

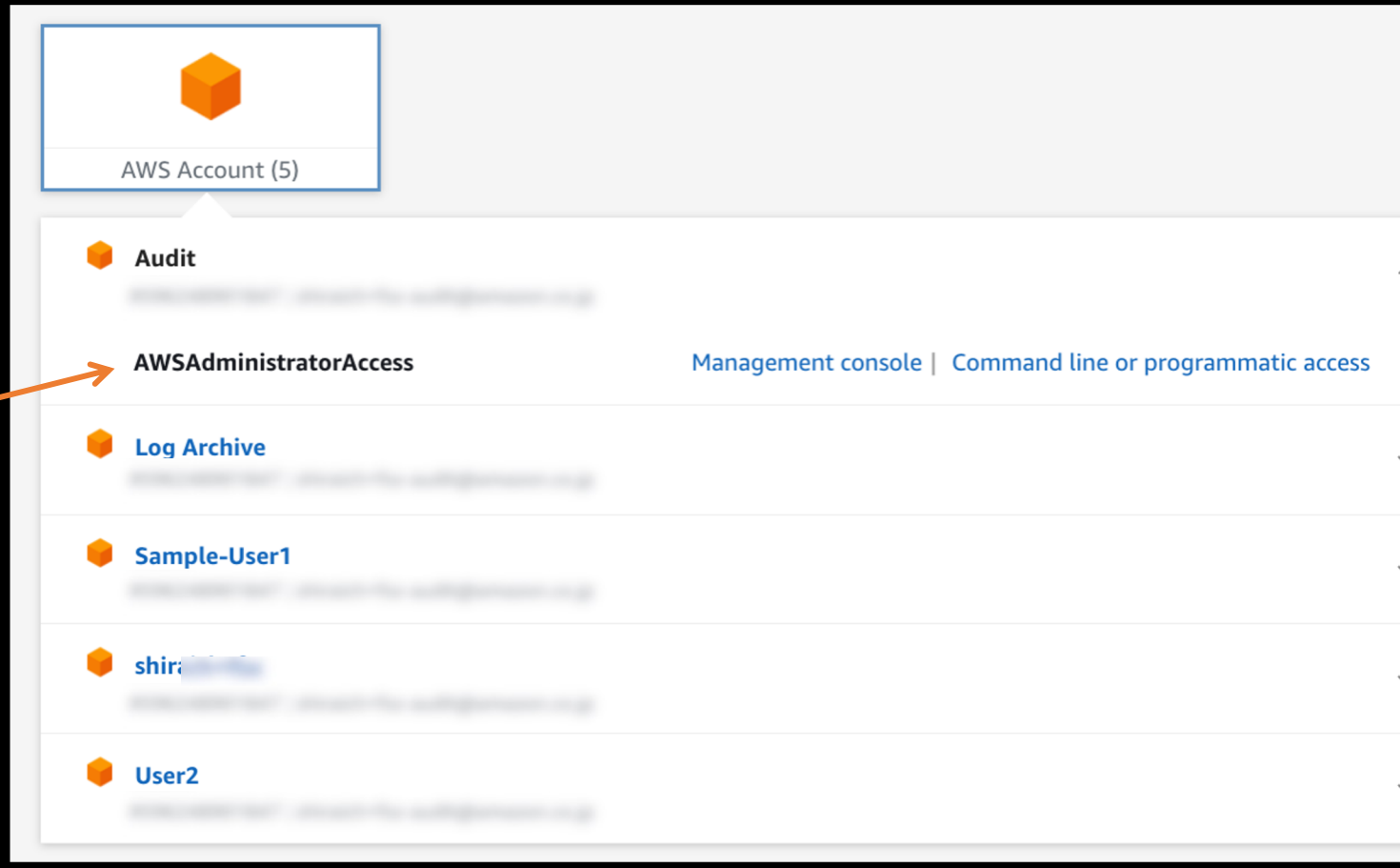


AWS Control Tower の機能
ログイン・ユーザ管理の一本化

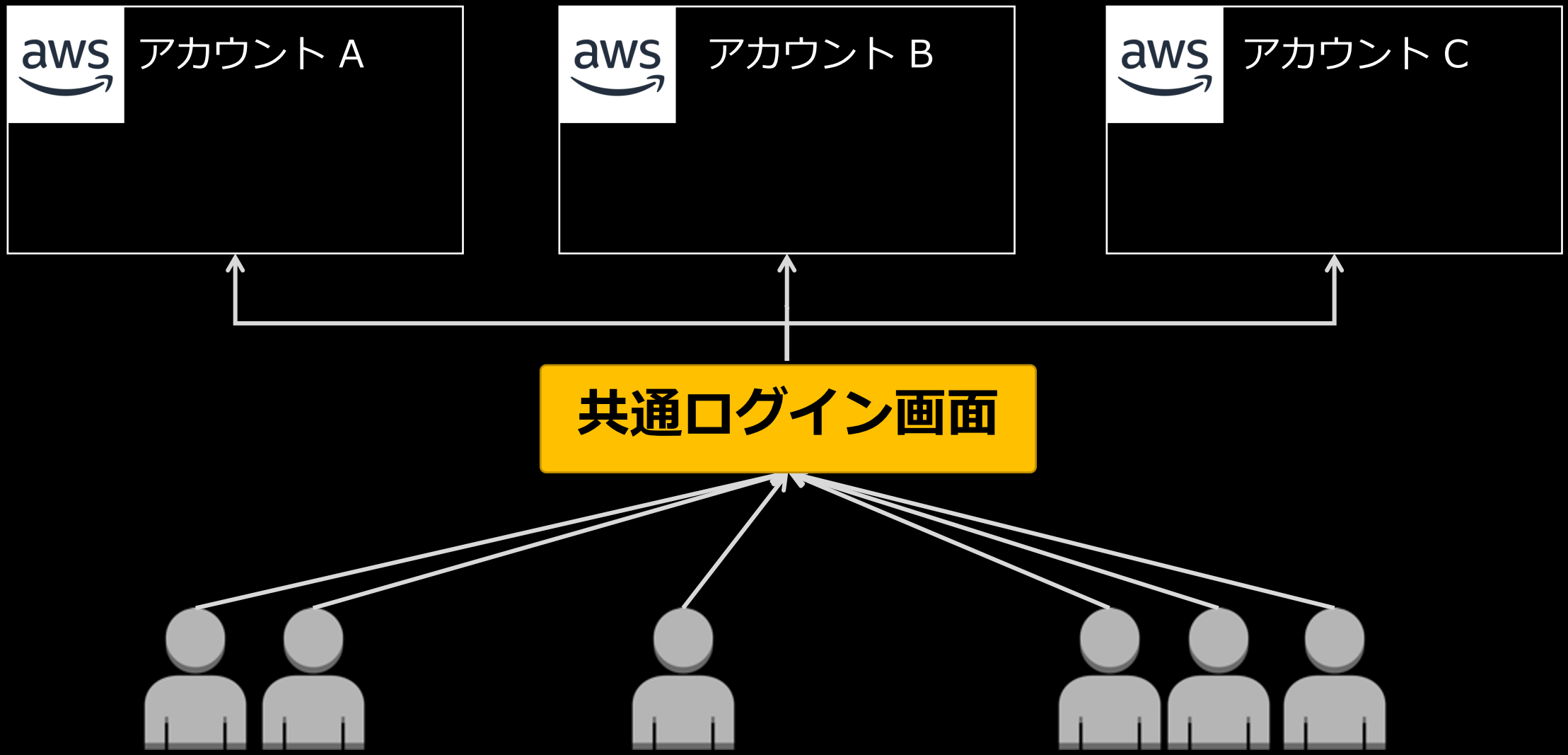
共通ログイン画面



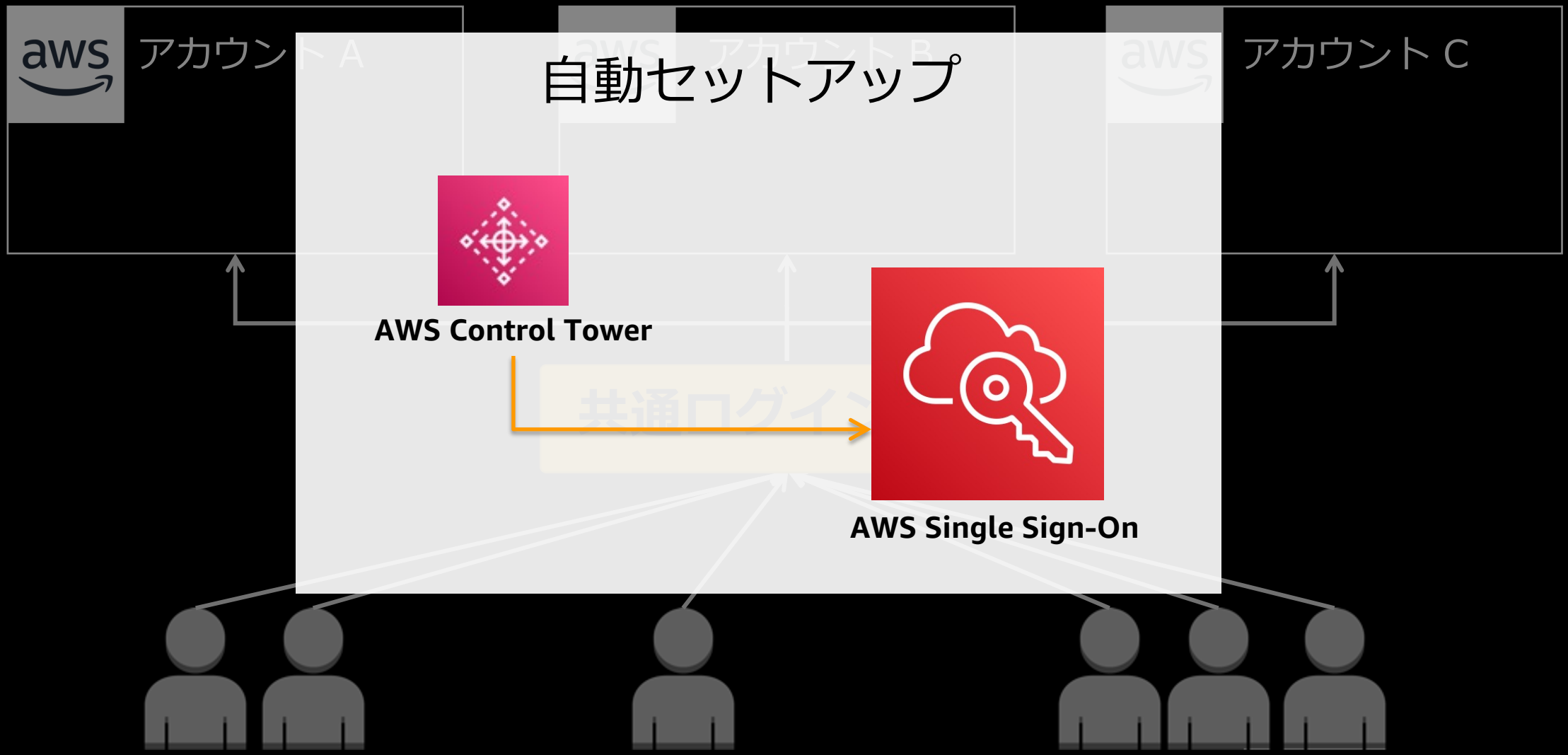
権限のあるアカウント一覧



ログインの導線・ユーザ管理を一本化



ログインの導線・ユーザ管理を一本化



AWS Control Tower 4 つの機能

① シングルサインオン

複数のAWSアカウントへの
ログインの切り替え

② ログ集約

AWSの操作ログの
自動収集

③ ガードレール

リスクのある操作の
予防・発見

④ アカウント作成

新規AWSアカウントの
自動セットアップ

② ログ集約

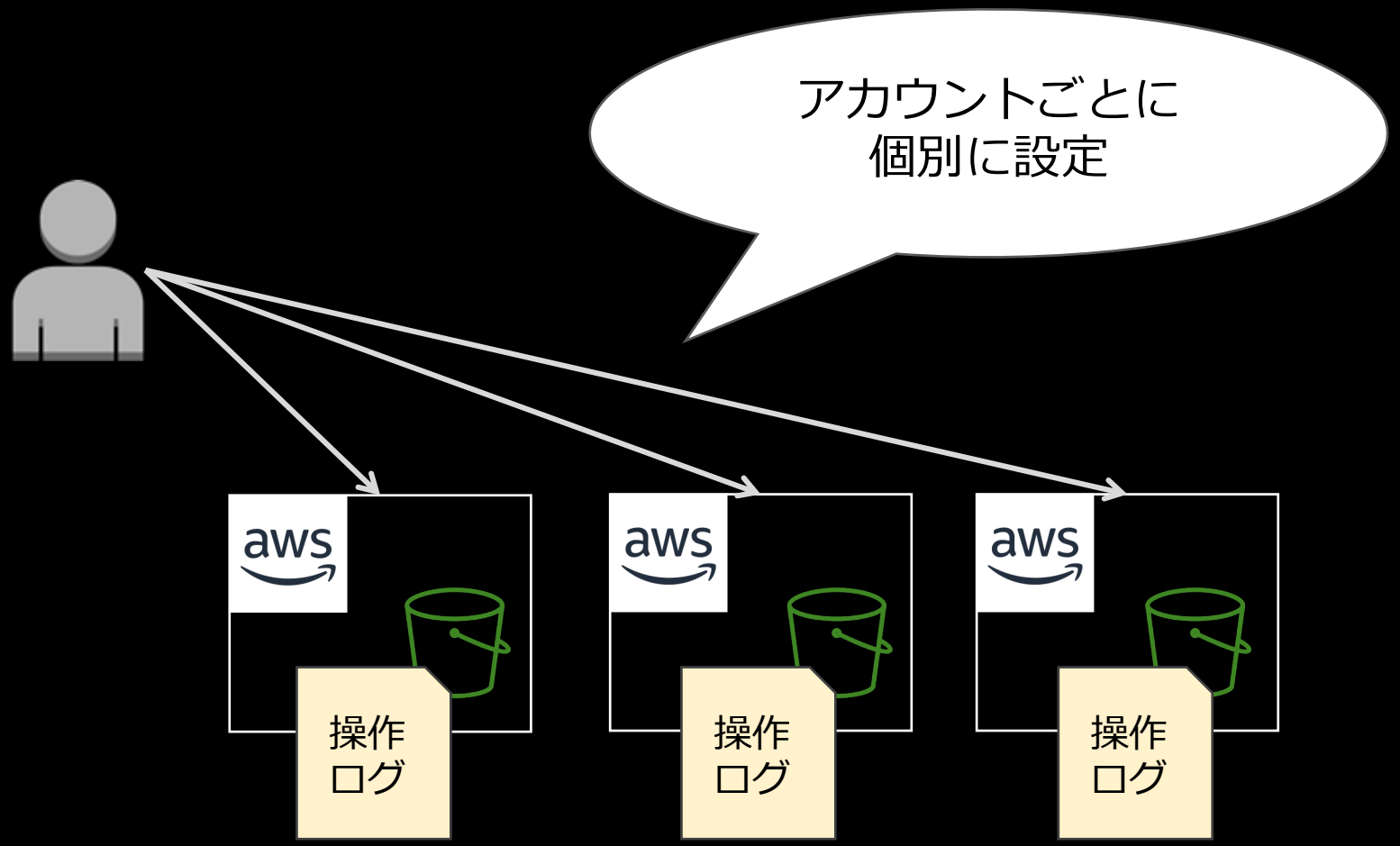
AWSの操作ログの自動収集

（課題）アカウントの数だけ個別に設定

「誰が、いつ、何をしたのか」

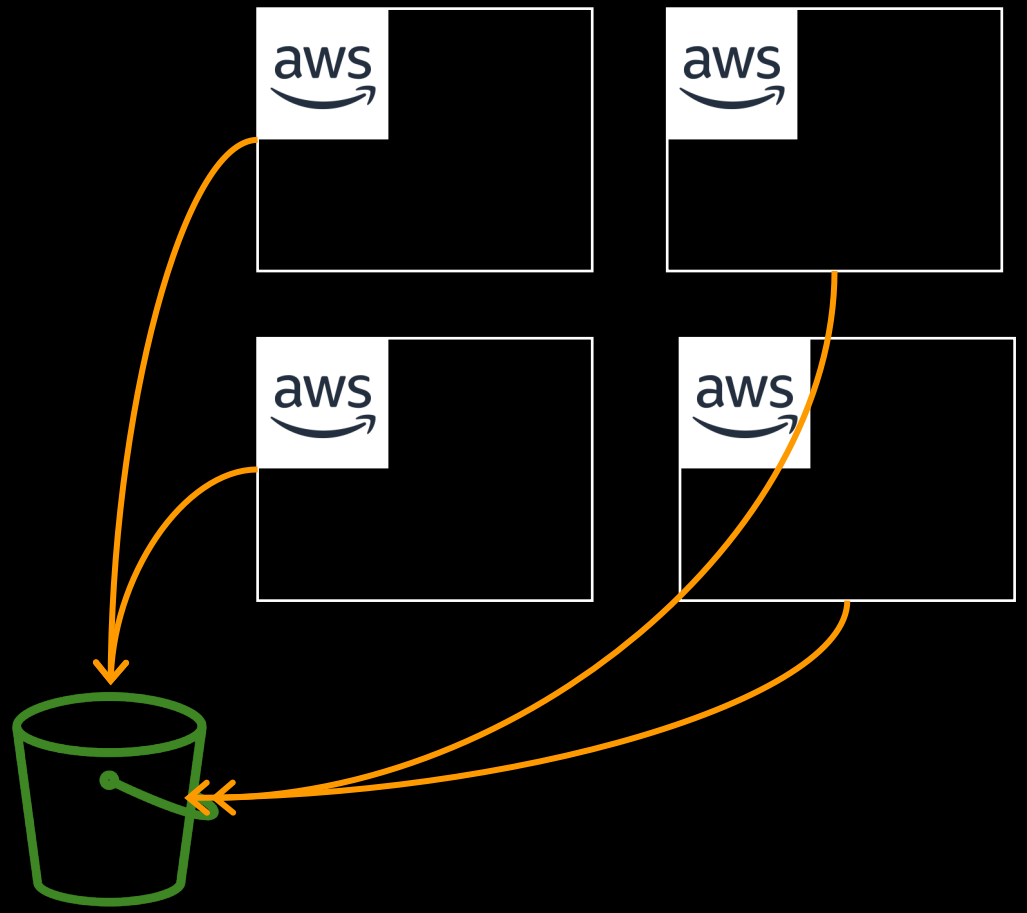
操作
ログ

（課題）アカウントの数だけ個別に設定



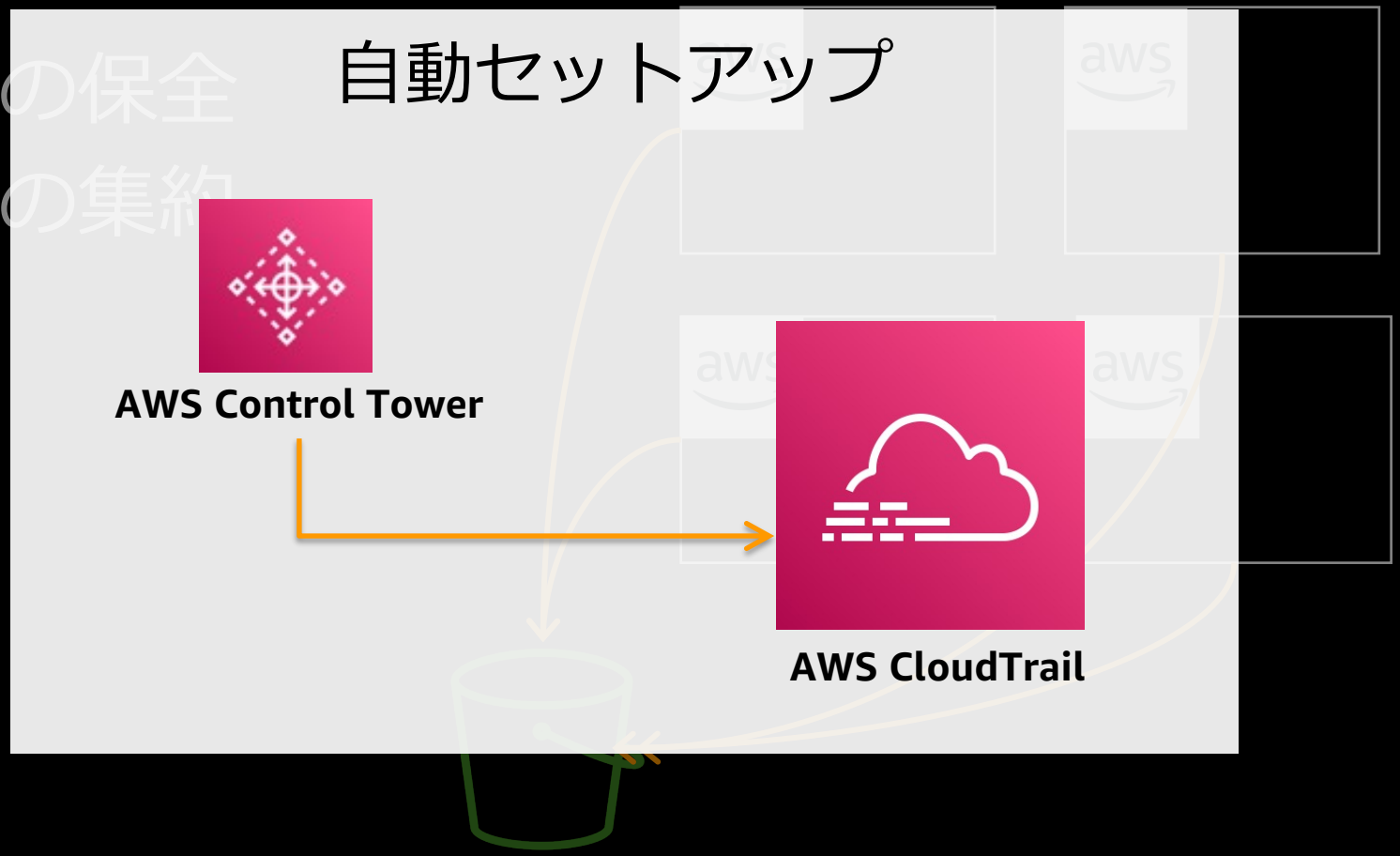
AWS Control Tower の機能
ログの自動収集と集約機能

- ログの保全
- 調査の集約



AWS Control Tower の機能
ログの自動収集と集約機能

- ログの保全
- 調査の集約



AWS Control Tower 4 つの機能

① シングルサインオン

複数のAWSアカウントへの
ログインの切り替え

② ログ集約

AWSの操作ログの
自動収集

③ ガードレール

リスクのある操作の
予防・発見

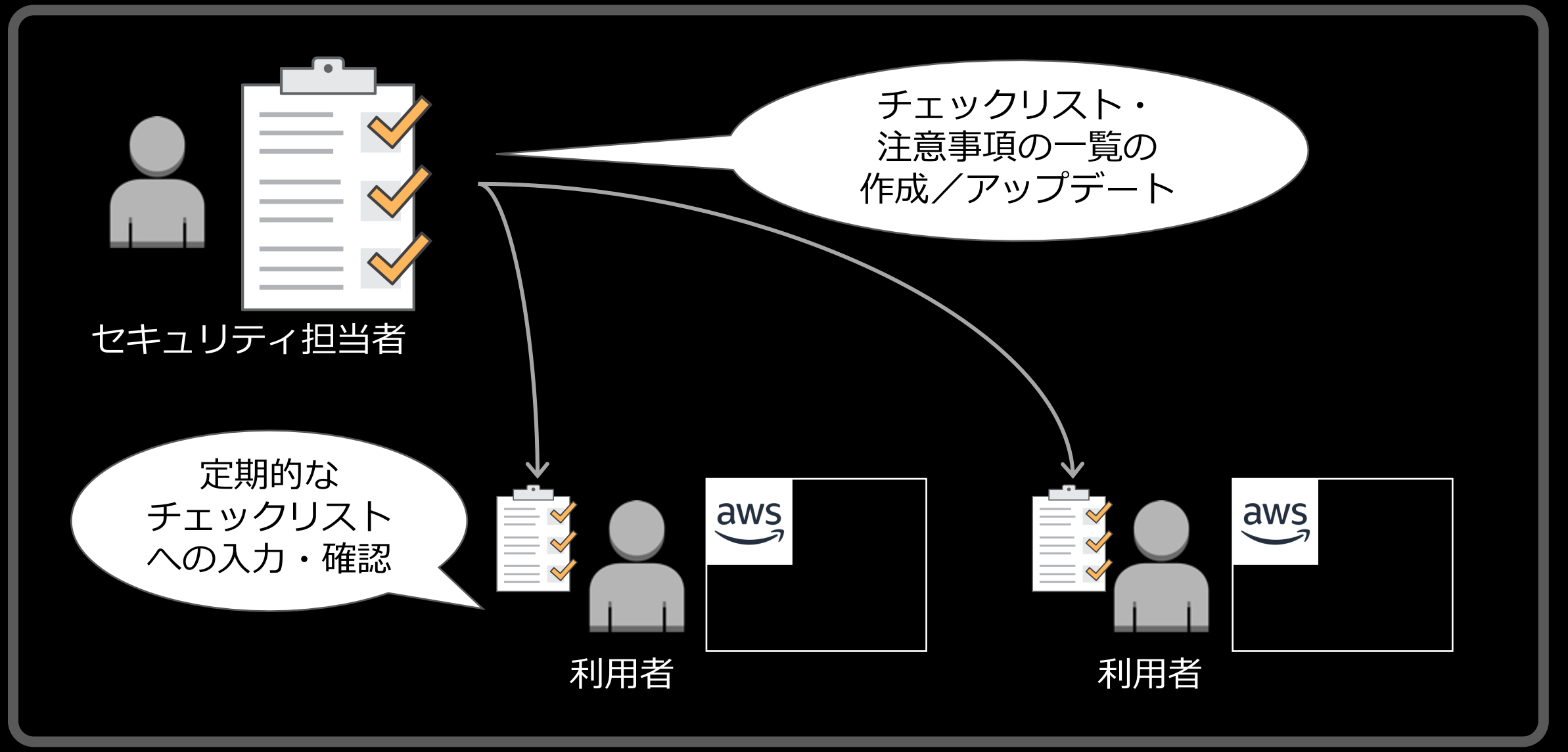
④ アカウント作成

新規AWSアカウントの
自動セットアップ

③ ガードレール

リスクのある操作の予防・発見

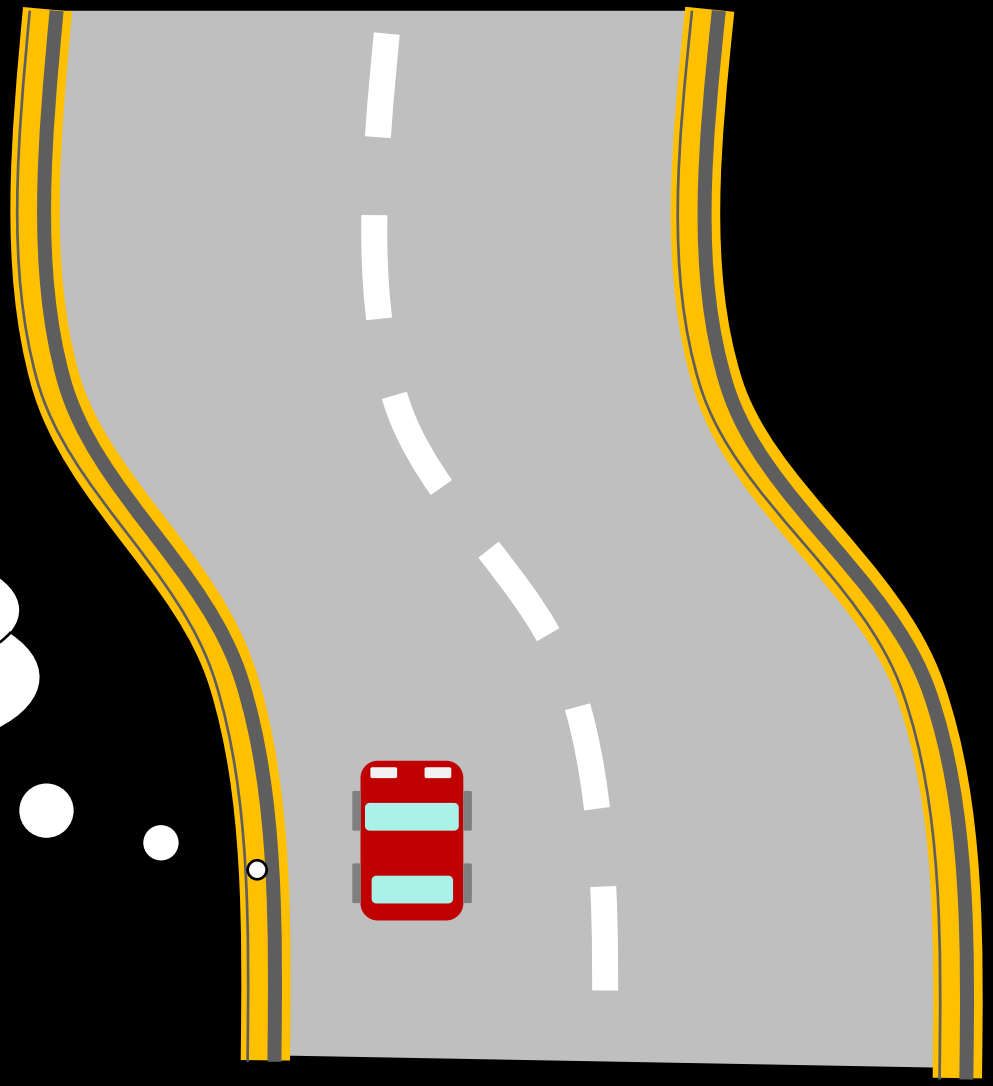
（課題）安全なAWSアカウント利用の実現



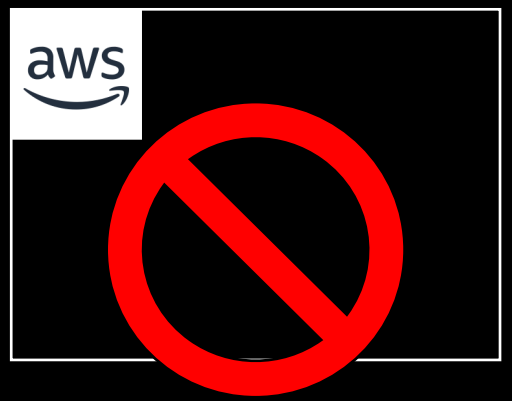
AWS Control Tower の機能
リスクのある操作の予防・発見

- リスクのある操作の禁止
- 危険な設定の監視

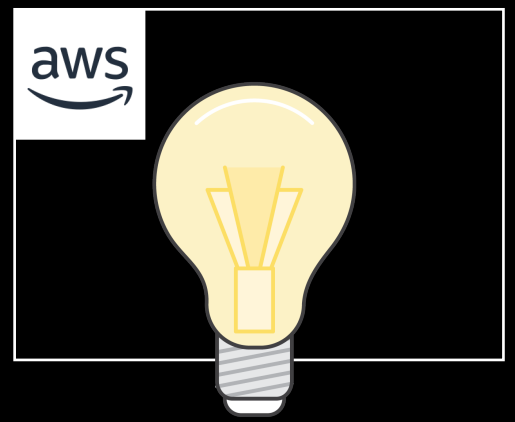
ガードレール機能



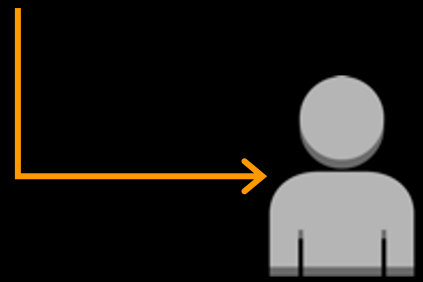
リスクのある操作の禁止、又は監視（通知）



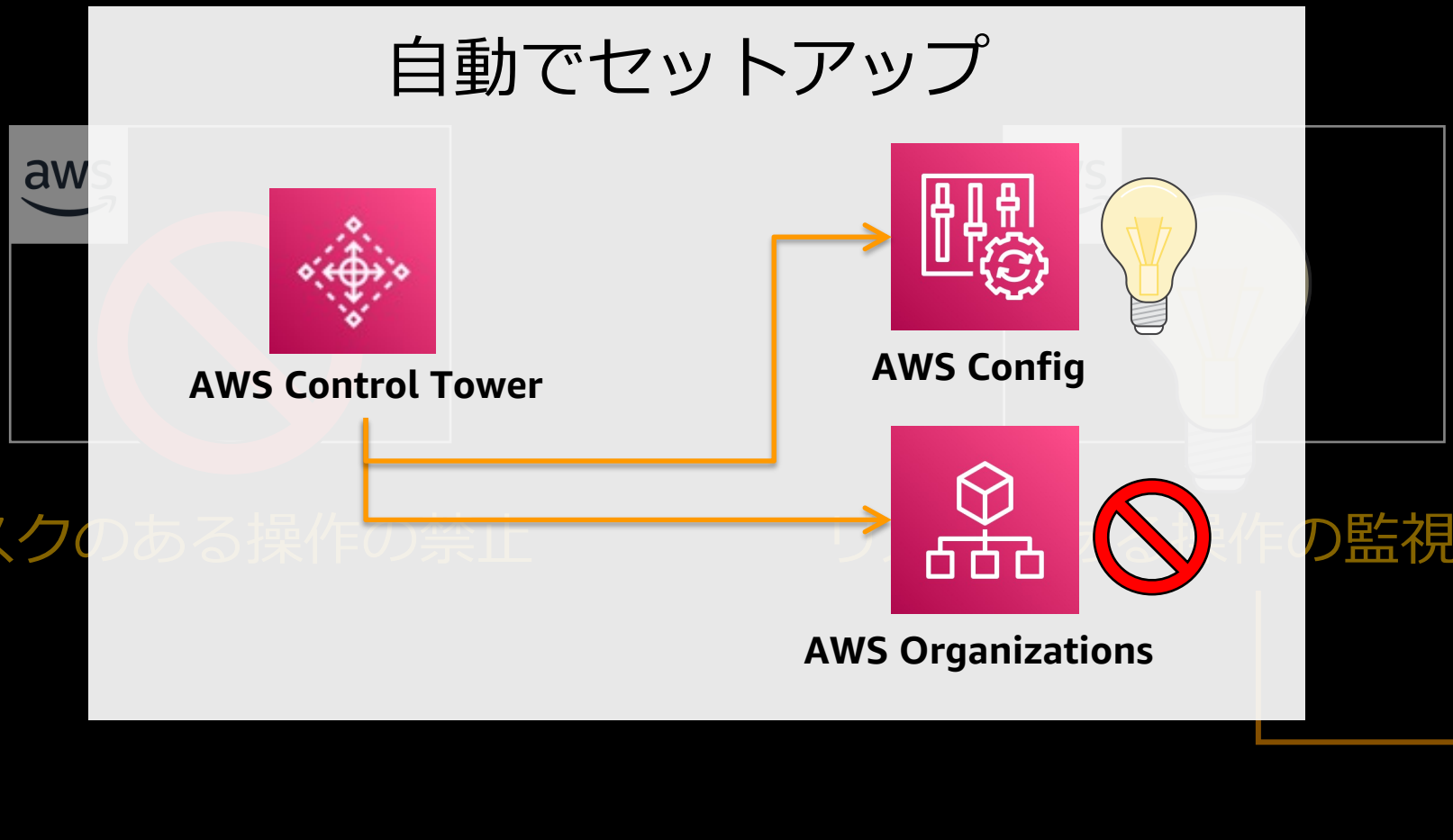
リスクのある操作の禁止



リスクのある操作の監視（通知）



リスクのある操作の禁止、又は監視（通知）



AWS Control Tower 4 つの機能

① シングルサインオン

複数のAWSアカウントへの
ログインの切り替え

② ログ集約

AWSの操作ログの
自動収集

③ ガードレール

リスクのある操作の
予防・発見

④ アカウント作成

新規AWSアカウントの
自動セットアップ

④ アカウント作成

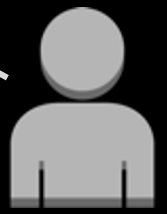
新規AWSアカウントの自動セットアップ

（課題）新規アカウントの手配・環境セットアップ

AWSアカウントの作成
のための各種入力

連絡先、支払情報の設定 etc.

初期セットアップ



利用者向けのログインの設定、
操作ログ設定、ガードレールの設定…

AWS Control Tower の機能
セットアップ済みの新規AWSアカウントの発行

AWS Control Tower コンソール画面

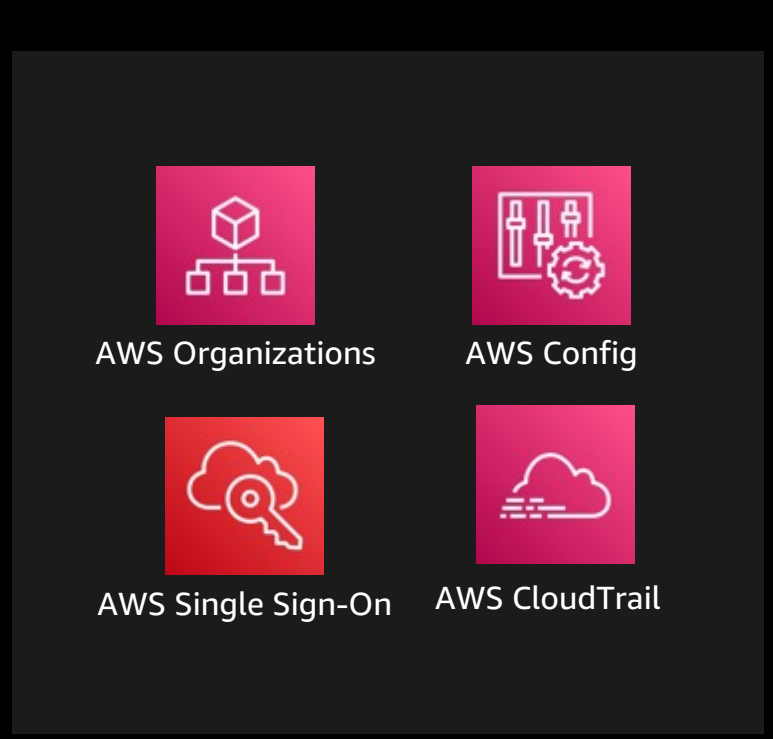
アカウント作成画面

新規AWSアカウントへの自動セットアップ

- 各種機能がはじめから設定

aws

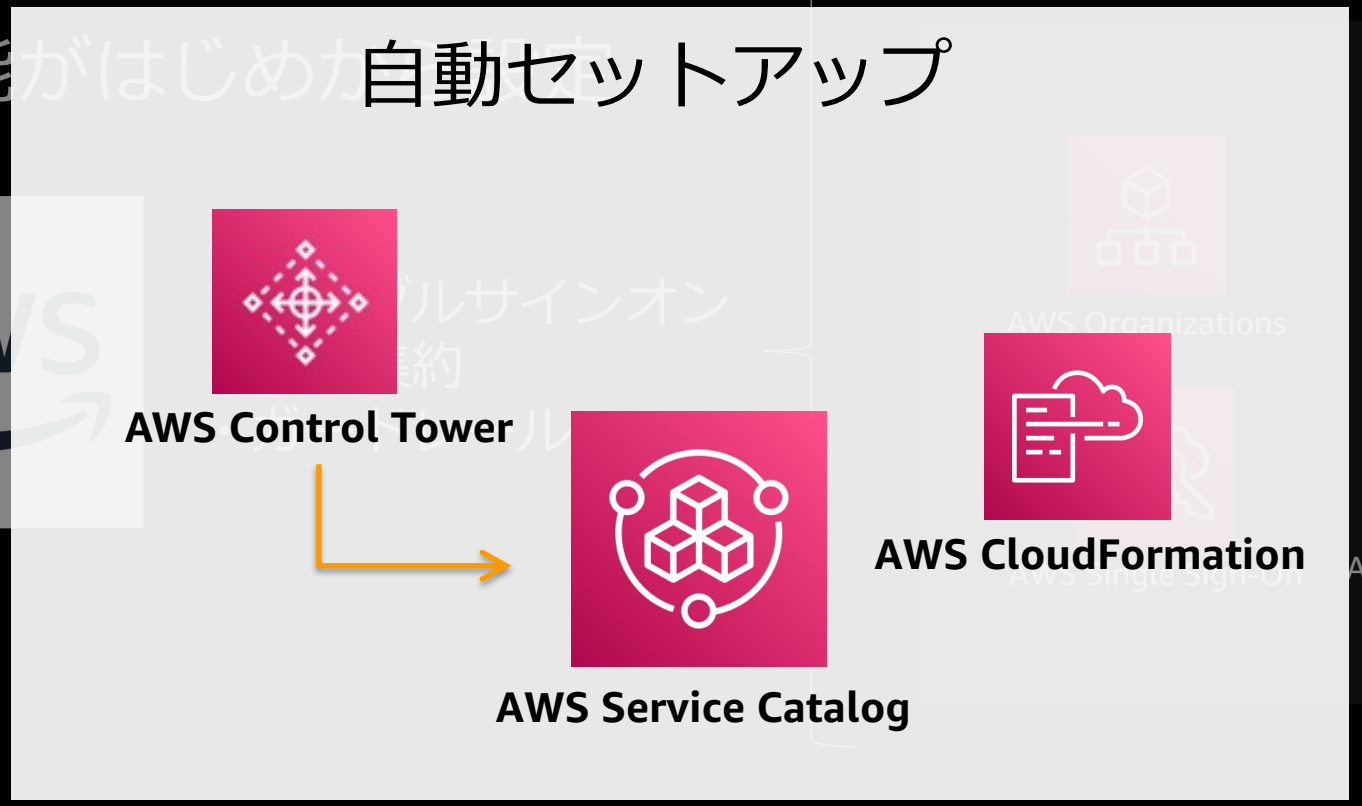
・シングルサインオン
・ログ集約
・ガードレール



aws

新規AWSアカウントへの自動セットアップ

- 各種機能がはじめた状態に



AWS Control Tower 4 つの機能

① シングルサインオン

複数のAWSアカウントへの
ログインの切り替え

② ログ集約

AWSの操作ログの
自動収集

③ ガードレール

リスクのある操作の
予防・発見

④ アカウント作成

新規AWSアカウントの
自動セットアップ

まとめ・次の一歩

AWS Control Tower

再掲

- ベストプラクティスに基づくAWS環境
- 数クリックで利用開始
- マネージド型サービス
- 無償で利用可能

これからAWSを始めるお客様

既に運用を開始されているお客様

AWS Control Tower 4 つの機能

再掲

① シングルサインオン

複数のAWSアカウントへの
ログインの切り替え

② ログ集約

AWSの操作ログの
自動収集

③ ガードレール

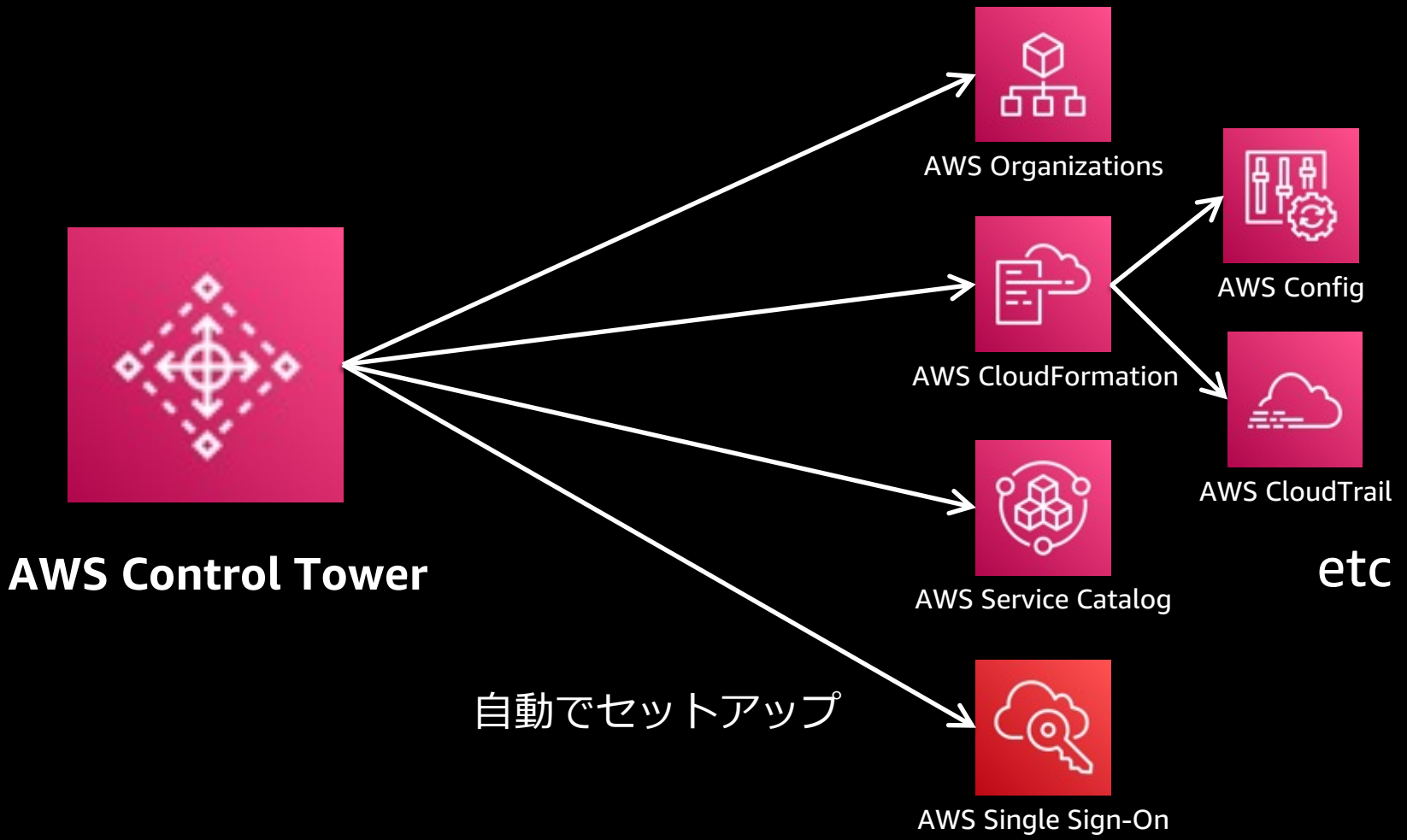
リスクのある操作の
予防・発見

④ アカウント作成

新規AWSアカウントの
自動セットアップ

AWS Control Tower の仕組み

再掲



より詳しい内容については

- [AWS Black Belt Online Seminar] AWS Control Tower

  [AWS Black Belt Online Seminar] オンデマンド動画 コンテンツ

  https://aws.amazon.com/jp/aws-jp-introduction/

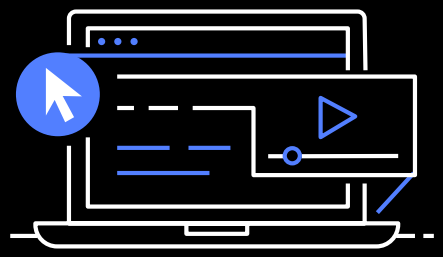
- [AWS Summit Online 2022]
  セキュアでスケーラブルな
  AWS アカウント統制プラクティス最新動向

  上記キーワードで検索

AWS Control Tower の始め方

数クリックで開始

AWS デジタルトレーニング



実力、自信、信頼性を高め、業界で認められた資格で差をつけよう

デジタル学習

- スキルビルダー – AWS のエキスパートが開発した数百のデジタルトレーニングを自分のスケジュールで学習できます
- Cloud Quest - AWS Cloud Quest は、実践的なクラウド経験を積み、AWSクラウドのスキルを身につけることができる、初めてで唯一のロールプレイングゲームです

認定試験準備ためのリソース

- Cloud Practitioner - AWS Certified Cloud Practitioner 取得に役立つリソースをご紹介します
- Developer – Associate – AWS Certified Developer – Associate 取得に役立つリソースをご紹介します

aws

aws.amazon.com/jp/training

AWS Builders Online Series に
ご参加いただきありがとうございます

楽しんでいただけましたか? ぜひアンケートにご協力ください。
本日のイベントに関するご意見/ご感想や今後のイベントについての
ご希望や改善のご提案などがございましたら、ぜひお聞かせください。


aws-apj-marketing@amazon.com


twitter.com/awscloud_jp


facebook.com/600986860012140


https://www.youtube.com/user/AmazonWebServicesJP


https://www.linkedin.com/showcase/aws-careers/


twitch.tv/aws

Thank you!