



[AWS HANDS-ON FOR BEGINNERS - 1ST STEPS]

ハンズオンははじめの一步： アカウントの作り方 & IAM 基本のキ

アマゾン ウェブ サービス ジャパン 株式会社

Solutions Architect

小林 大樹 / Kobayashi Daiki

自己紹介

□ 名前

小林 大樹 Daiki Kobayashi  @kobayasd

□ 所属

アマゾン ウェブ サービス ジャパン合同会社
ソリューションアーキテクト

□ 経歴

- ・ ユーザー企業（金融）のエンジニア → AWS

□ 好きな AWS サービス

- ・ Amazon Codewhisperer



AWS Hands-on for Beginners とは



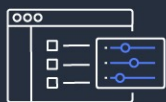
実際に手を動かしながら AWS の各サービスを学んでいただきます



初めてそのサービスをご利用される方がメインターゲットです



好きな時間、好きな場所でご受講いただけるオンデマンド形式です



テーマごとに合計 1 ~ 2 時間の内容 & 細かい動画に分けて公開
スキマ時間の学習や、興味のある部分だけの聴講も可能

内容についての注意点

- 資料では 2023 年 4 月 19 日収録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。最新の情報はAWS公式ウェブサイト(<http://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、資料とAWS公式ウェブサイトとで記載内容に相違があった場合、AWS公式ウェブサイトの記載を優先させていただきます。
- マネージメントコンソールについても、収録時点のものとなります。差異がある場合がございますので、ご注意ください。
- ハンズオンでは AWS の各種サービスの利用、リソースの作成を行います。無料枠を超えるハンズオンもございますが、その場合はご利用料金が発生することをあらかじめご認識ください。
- 学習後のリソースの削除についても、お客様の責任でご実施いただくようお願いいたします。

本シリーズのゴール

- AWS アカウントを作る際に必要なモノ、作成手順について学んでいただき、**ハンズオン用の AWS アカウントを作ってください**
- **IAM の基本** (IAM ポリシー、IAM ユーザー、IAM グループ、IAM ロール) について学んでいただく
- 必要な権限を割り振った **IAM リソースを作成できる** ようになっていただく

本シリーズの前提条件・知識

- なし

※ AWS アカウントを作成する際に必要な情報については、この動画の中で紹介します

本シリーズのアジェンダ

- 1) 今回のハンズオンの説明 + アカウント作成に必要なもの + 作成の流れ
- 2) アカウントを作成してみる 🖐️
- 3) ルートユーザーと IAM ユーザーについて学ぶ
- 4) IAM ユーザーを作成する 🖐️
- 5) IAM (ポリシー、グループ、ロール) について学ぶ
- 6) IAM ポリシーと IAM グループを作ってみる 🖐️
- 7) IAM ロールを試してみる 🖐️
- 8) [Option] マルチアカウント戦略について学ぶ
- 9) [Option] AWS Organizations によるマルチアカウント戦略を試してみる 🖐️
- 10) まとめ + Next Action としてオススメのコンテンツを紹介

本シリーズのアジェンダ

- 1) 今回のハンズオンの説明 + アカウント作成に必要なもの + 作成の流れ
- 2) アカウントを作成してみる 🖐️
- 3) ルートユーザーと IAM ユーザーについて学ぶ
- 4) IAM ユーザーを作成する 🖐️
- 5) IAM (ポリシー、グループ、ロール) について学ぶ
- 6) IAM ポリシーと IAM グループを作ってみる 🖐️
- 7) IAM ロールを試してみる 🖐️
- 8) [Option] マルチアカウント戦略について学ぶ
- 9) [Option] AWS Organizations によるマルチアカウント戦略を試してみる 🖐️
- 10) まとめ + Next Action としてオススメのコンテンツを紹介

アカウント作成に必要なもの + 作成の流れ

- 登録する **メールアドレス**
- アカウント認証に使用する **電話番号**
- お支払いに利用する
クレジットカード or デビットカード

① **基本情報の入力**
メールアドレス・パスワードなど

② **連絡先情報の入力**
氏名・住所など

③ **お支払い情報の入力**
カード情報・請求先住所など

④ **アカウント認証**
SMS or 音声による認証

⑤ **サポートプランの選択**

(参考) AWS アカウントの作成の流れ
<https://aws.amazon.com/jp/register-flow/>

本シリーズのアジェンダ

- 1) 今回のハンズオンの説明 + アカウント作成に必要なもの + 作成の流れ
- 2) アカウントを作成してみる 🖐️
- 3) ルートユーザーと IAM ユーザーについて学ぶ
- 4) IAM ユーザーを作成する 🖐️
- 5) IAM (ポリシー、グループ、ロール) について学ぶ
- 6) IAM ポリシーと IAM グループを作ってみる 🖐️
- 7) IAM ロールを試してみる 🖐️
- 8) [Option] マルチアカウント戦略について学ぶ
- 9) [Option] AWS Organizations によるマルチアカウント戦略を試してみる 🖐️
- 10) まとめ + Next Action としてオススメのコンテンツを紹介

アカウント作成に必要なもの + 作成の流れ

- 登録する **メールアドレス**
- アカウント認証に使用する **電話番号**
- お支払いに利用する
クレジットカード or デビットカード

① **基本情報の入力**
メールアドレス・パスワードなど

② **連絡先情報の入力**
氏名・住所など

③ **お支払い情報の入力**
カード情報・請求先住所など

④ **アカウント認証**
SMS or 音声による認証

⑤ **サポートプランの選択**

本シリーズのアジェンダ

- 1) 今回のハンズオンの説明 + アカウント作成に必要なもの + 作成の流れ
- 2) アカウントを作成してみる 🖐️
- 3) ルートユーザーと IAM ユーザーについて学ぶ**
- 4) IAM ユーザーを作成する 🖐️
- 5) IAM (ポリシー、グループ、ロール) について学ぶ
- 6) IAM ポリシーと IAM グループを作ってみる 🖐️
- 7) IAM ロールを試してみる 🖐️
- 8) [Option] マルチアカウント戦略について学ぶ
- 9) [Option] AWS Organizations によるマルチアカウント戦略を試してみる 🖐️
- 10) まとめ + Next Action としてオススメのコンテンツを紹介

ルートユーザーと IAM ユーザー

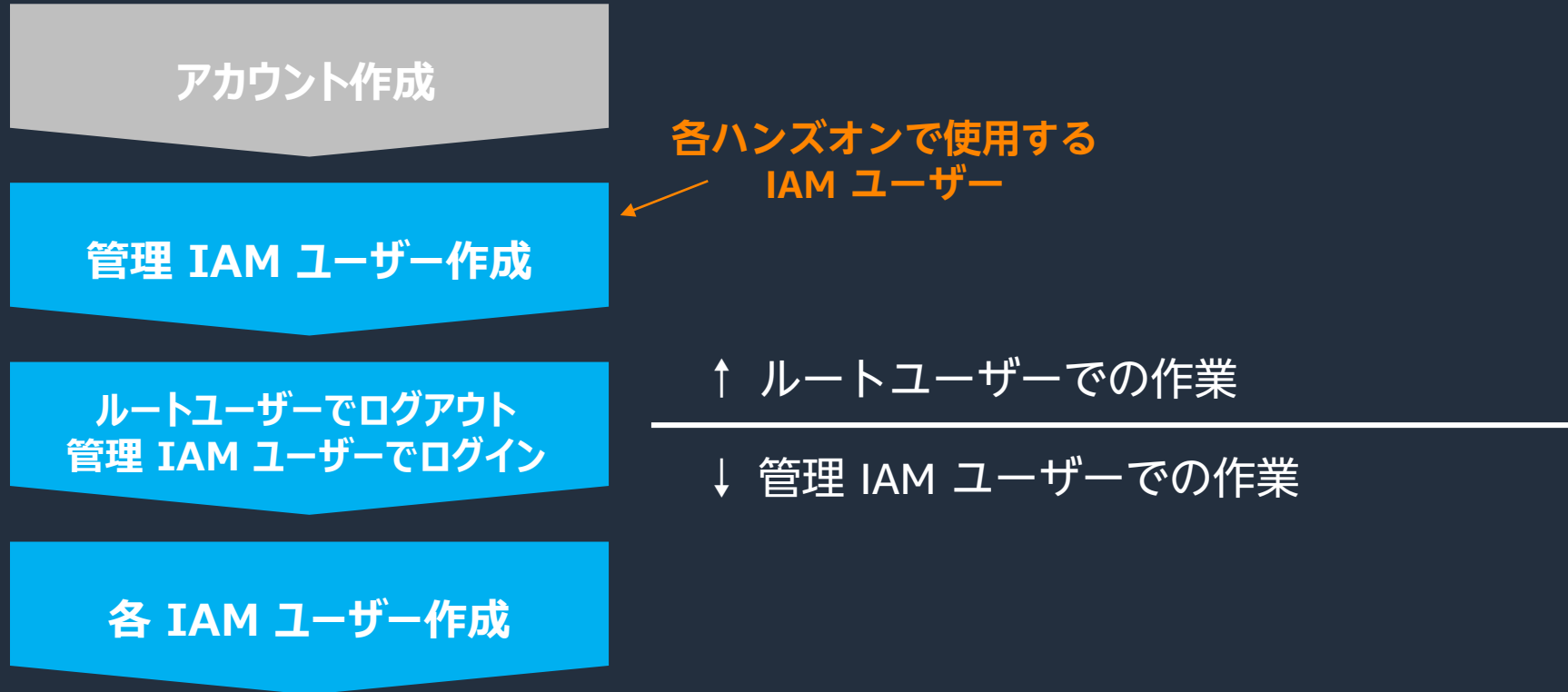
ルートユーザー

- メールアドレス + パスワードでログイン
- 全 AWS サービスとリソースに対して **完全なアクセス権限**
- 日常的なタスクには 使わない

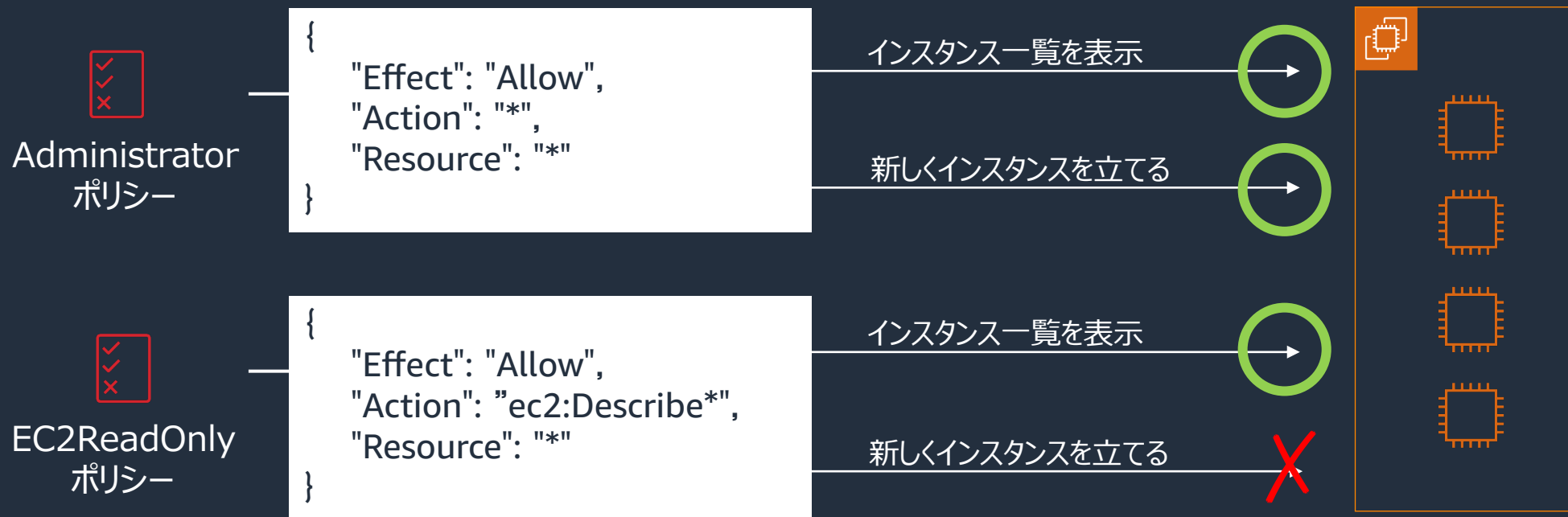
IAM (Identity & Access Management) ユーザー

- アカウントID + IAM ユーザー名 + パスワードでログイン
- 紐付いている **IAM ポリシー権限**で **認められた操作のみ** 可能
- 利用者ごとに IAM ユーザーを作成
利用者は IAM ユーザーでログインし、作業を進めていく

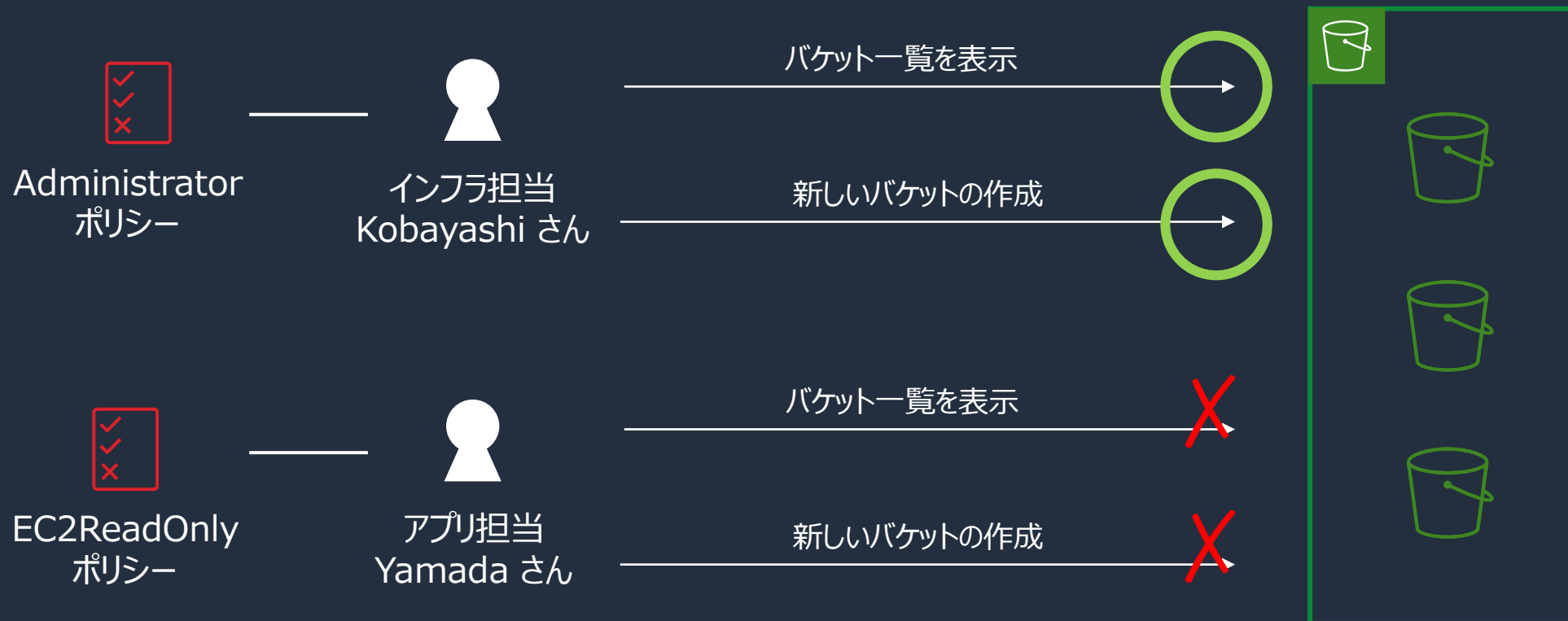
各ユーザー作成までの流れ



IAM ユーザーについて



IAM ユーザーについて



ユーザー作成までの流れ

アカウント作成

管理 IAM ユーザー作成

ルートユーザーでログアウト
管理 IAM ユーザーでログイン

各 IAM ユーザー作成

↑ ルートユーザーでの作業

↓ 管理 IAM ユーザーでの作業

(参考) 本ハンズオンで利用する AWS サービス



Amazon EC2 (Elastic Compute Cloud)

- 数分で起動し、従量課金型の**仮想サーバサービス**
- インスタンスタイプを需要にあわせて選択可能
- 必要なときに必要な分のリソースを起動できる



Amazon S3 (Simple Storage Service)

- 99.999999999% の耐久性を持つ**オブジェクトストレージサービス**
- 容量無制限な安価なストレージ
- 静的 Web ホスティング機能
- 様々な AWS サービスと連携する

本シリーズのアジェンダ

- 1) 今回のハンズオンの説明 + アカウント作成に必要なもの + 作成の流れ
- 2) アカウントを作成してみる 🖐️
- 3) ルートユーザーと IAM ユーザーについて学ぶ
- 4) IAM ユーザーを作成する 🖐️**
- 5) IAM (ポリシー、グループ、ロール) について学ぶ
- 6) IAM ポリシーと IAM グループを作ってみる 🖐️
- 7) IAM ロールを試してみる 🖐️
- 8) [Option] マルチアカウント戦略について学ぶ
- 9) [Option] AWS Organizations によるマルチアカウント戦略を試してみる 🖐️
- 10) まとめ + Next Action としてオススメのコンテンツを紹介

ユーザー作成までの流れ

アカウント作成

管理 IAM ユーザー作成

ルートユーザーでログアウト
管理 IAM ユーザーでログイン

各 IAM ユーザー作成

↑ ルートユーザーでの作業

↓ 管理 IAM ユーザーでの作業

本シリーズのアジェンダ

- 1) 今回のハンズオンの説明 + アカウント作成に必要なもの + 作成の流れ
- 2) アカウントを作成してみる 🖐️
- 3) ルートユーザーと IAM ユーザーについて学ぶ
- 4) IAM ユーザーを作成する 🖐️
- 5) IAM (ポリシー、グループ、ロール) について学ぶ**
- 6) IAM ポリシーと IAM グループを作ってみる 🖐️
- 7) IAM ロールを試してみる 🖐️
- 8) [Option] マルチアカウント戦略について学ぶ
- 9) [Option] AWS Organizations によるマルチアカウント戦略を試してみる 🖐️
- 10) まとめ + Next Action としてオススメのコンテンツを紹介

IAM ポリシー

- **アクセス許可の定義** を行う JSON ドキュメント
- IAM ユーザー、グループ（後述）、ロール（後述）に紐付ける
- AWS で予め準備しているポリシーに加え、独自のポリシーも定義可能
IAM ポリシージェネレーター も有用

```
{  
  "Version": "2012-10-17",  
  "Statement": {  
    "Effect": "Allow",  
    "Action": "dynamodb:*",  
    "Resource": "arn:aws:dynamodb:us-east-2:123456789012:table/Books"  
  }  
}
```

Effect

許可(Allow) or 明示的な拒否(Deny)

Action

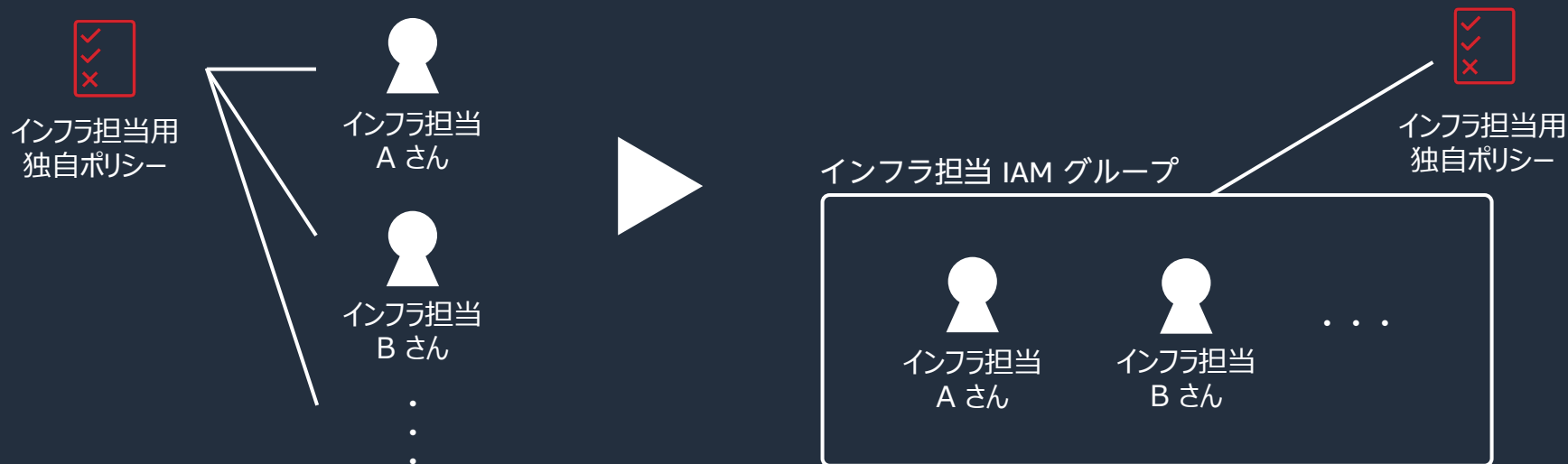
対象のアクションを指定する。
ワイルドカード(*)の指定も可

Resource

対象のリソースを指定する。
ワイルドカード(*)の指定も可

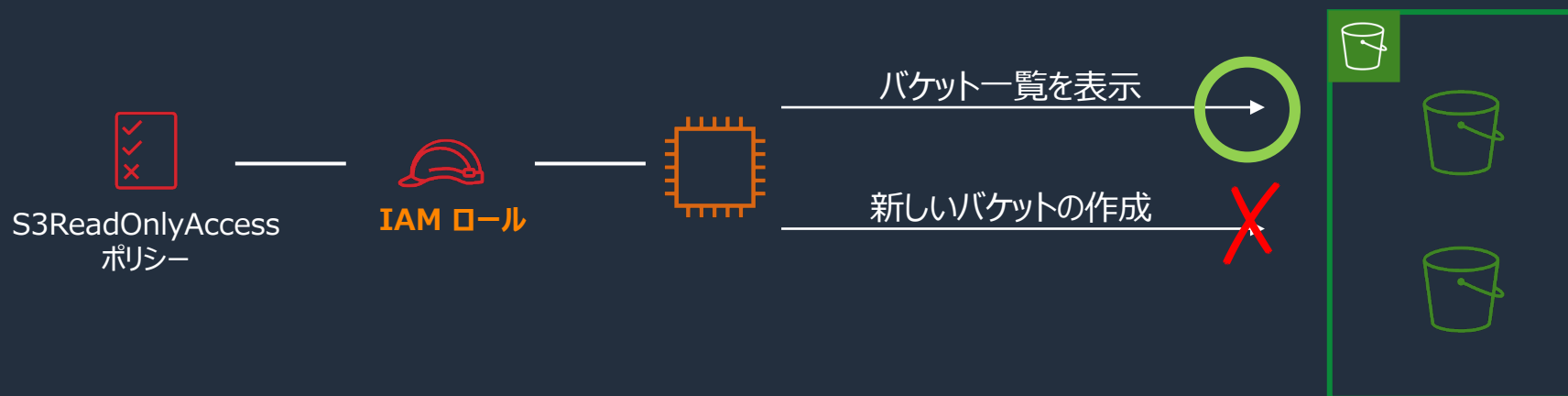
IAM グループ

- IAM ユーザーの集合 を定義
- 複数のユーザーへのアクセス許可を容易に指定できる

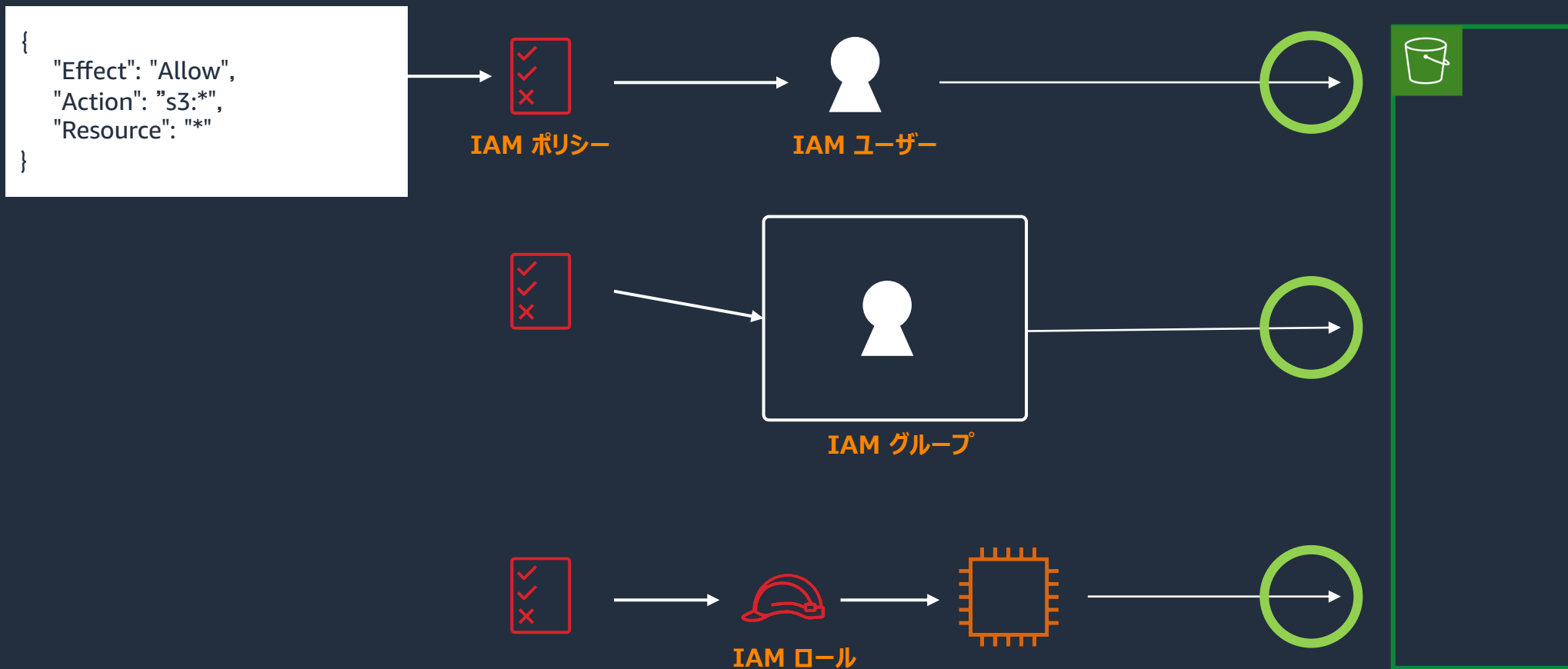


IAM ロール

- **AWS リソースに割り当て**、そのリソースに権限を与える
- 例：S3ReadOnlyAccess ポリシーを IAM ロールにアタッチし、その IAM ロールを EC2 インスタンスに割り当てることで、S3 のバケット一覧を表示可能になる



IAM まとめ1枚もの



本シリーズのアジェンダ

- 1) 今回のハンズオンの説明 + アカウント作成に必要なもの + 作成の流れ
- 2) アカウントを作成してみる 🖐️
- 3) ルートユーザーと IAM ユーザーについて学ぶ
- 4) IAM ユーザーを作成する 🖐️
- 5) IAM (ポリシー、グループ、ロール) について学ぶ
- 6) IAM ポリシーと IAM グループを作ってみる 🖐️
- 7) IAM ロールを試してみる 🖐️
- 8) [Option] マルチアカウント戦略について学ぶ
- 9) [Option] AWS Organizations によるマルチアカウント戦略を試してみる 🖐️
- 10) まとめ + Next Action としてオススメのコンテンツを紹介

ハンズオン - IAM ユーザー


Administrator
ポリシー


インフラ担当
Kobayashi さん

インスタンス一覧を表示



新しくインスタンスを立てる



インスタンス一覧を表示



インスタンスを Stop / Start

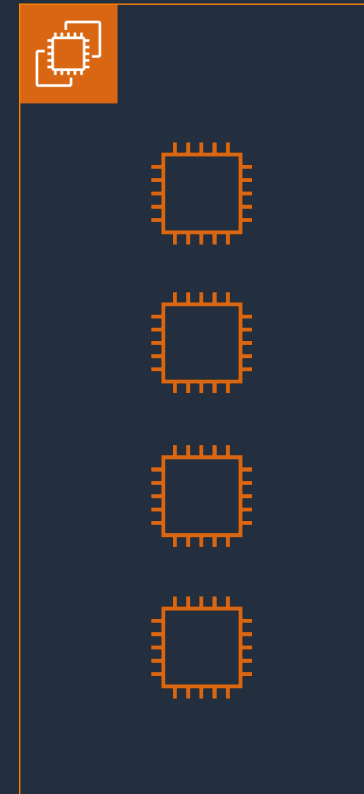


新しくインスタンスを立てる



開発者用
独自ポリシー


アプリ担当
kobayashi-dev



ハンズオン - IAMグループ



本シリーズのアジェンダ

- 1) 今回のハンズオンの説明 + アカウント作成に必要なもの + 作成の流れ
- 2) アカウントを作成してみる 🖐️
- 3) ルートユーザーと IAM ユーザーについて学ぶ
- 4) IAM ユーザーを作成する 🖐️
- 5) IAM (ポリシー、グループ、ロール) について学ぶ
- 6) IAM ポリシーと IAM グループを作ってみる 🖐️
- 7) IAM ロールを試してみる 🖐️**
- 8) [Option] マルチアカウント戦略について学ぶ
- 9) [Option] AWS Organizations によるマルチアカウント戦略を試してみる 🖐️
- 10) まとめ + Next Action としてオススメのコンテンツを紹介

ハンズオン - IAM ロール



本シリーズのアジェンダ

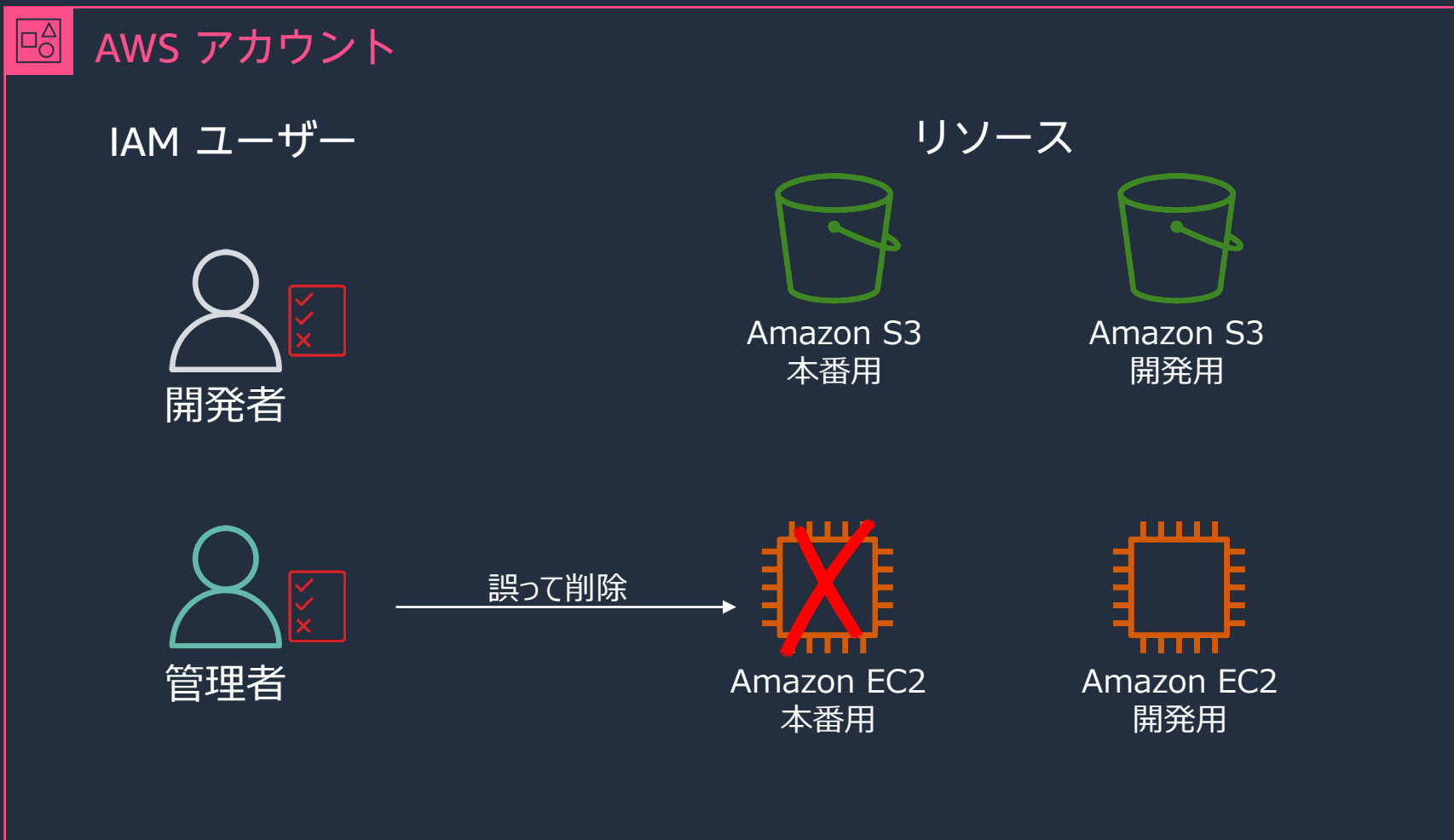
- 1) 今回のハンズオンの説明 + アカウント作成に必要なもの + 作成の流れ
- 2) アカウントを作成してみる 🖐️
- 3) ルートユーザーと IAM ユーザーについて学ぶ
- 4) IAM ユーザーを作成する 🖐️
- 5) IAM (ポリシー、グループ、ロール) について学ぶ
- 6) IAM ポリシーと IAM グループを作ってみる 🖐️
- 7) IAM ロールを試してみる 🖐️
- 8) [Option] マルチアカウント戦略について学ぶ**
- 9) [Option] AWS Organizations によるマルチアカウント戦略を試してみる 🖐️
- 10) まとめ + Next Action としてオススメのコンテンツを紹介

マルチアカウント戦略とは

- 特定の基準によって、AWS アカウント自体を分ける戦略のこと
 - Ex) 環境別、プロジェクト別、部署別、etc



なぜマルチアカウント戦略が必要なのか？



環境の分割と、AWS アカウント

環境

開発、テスト、本番などの環境をセキュリティやガバナンス、規制のために分離できる (PCIなど)

請求

部門単位やシステムの単位でAWSのコストが明確に分離できる

ビジネス推進

事前定義されたガバナンスフレームワークの中で特定のビジネス部門に対する権限の委譲が行える

ワークロード

外部向け/社内向けサービスや、リスクやデータ分類、顧客の違いなどに応じてワークロードを分離できる

マルチアカウント戦略の課題



AWS Organizations

AWS Organizations とは

- **アカウント管理**サービス
- **複数の AWS アカウントを 1つの組織に統合**できるサービス
- **一括請求** (コンソリデーティッドビルギング) およびアカウント管理機能を使用できるサービス

AWS Organizations の機能

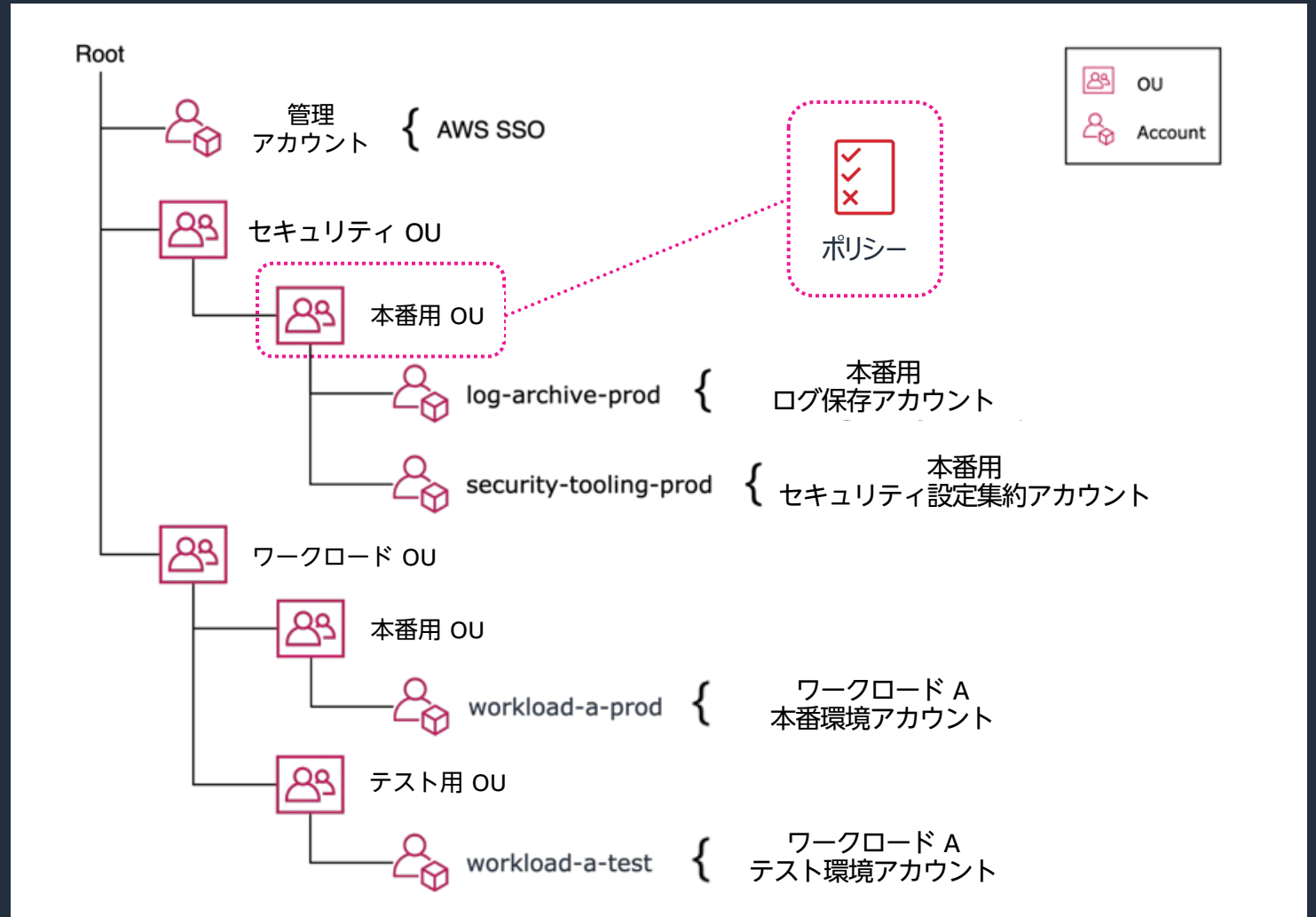
- **メンバーアカウントの階層的なグループ化**
- AWS IAM の統合とサポート
- AWS の各種サービスとの統合
- 結果整合性があるデータレプリケーション



AWS
Organizations

AWS Organizations を利用したアカウント管理

- 管理アカウント/メンバーアカウントの作成
- Organizational Unit (OU) 単位でアカウントをグループ化し、階層を作成
- SCP (サービスコントロールポリシー) によって、OU 単位で共有のポリシーを設定
- 各アカウントへの請求情報は、管理アカウントに一本化

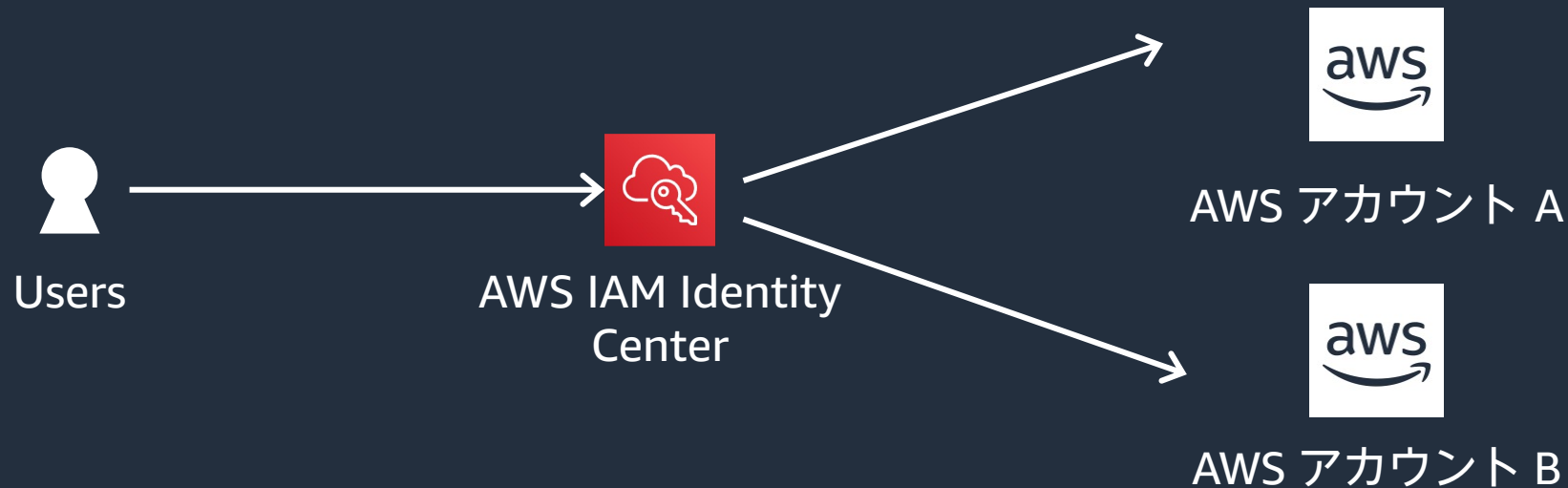


複数環境へのサインイン

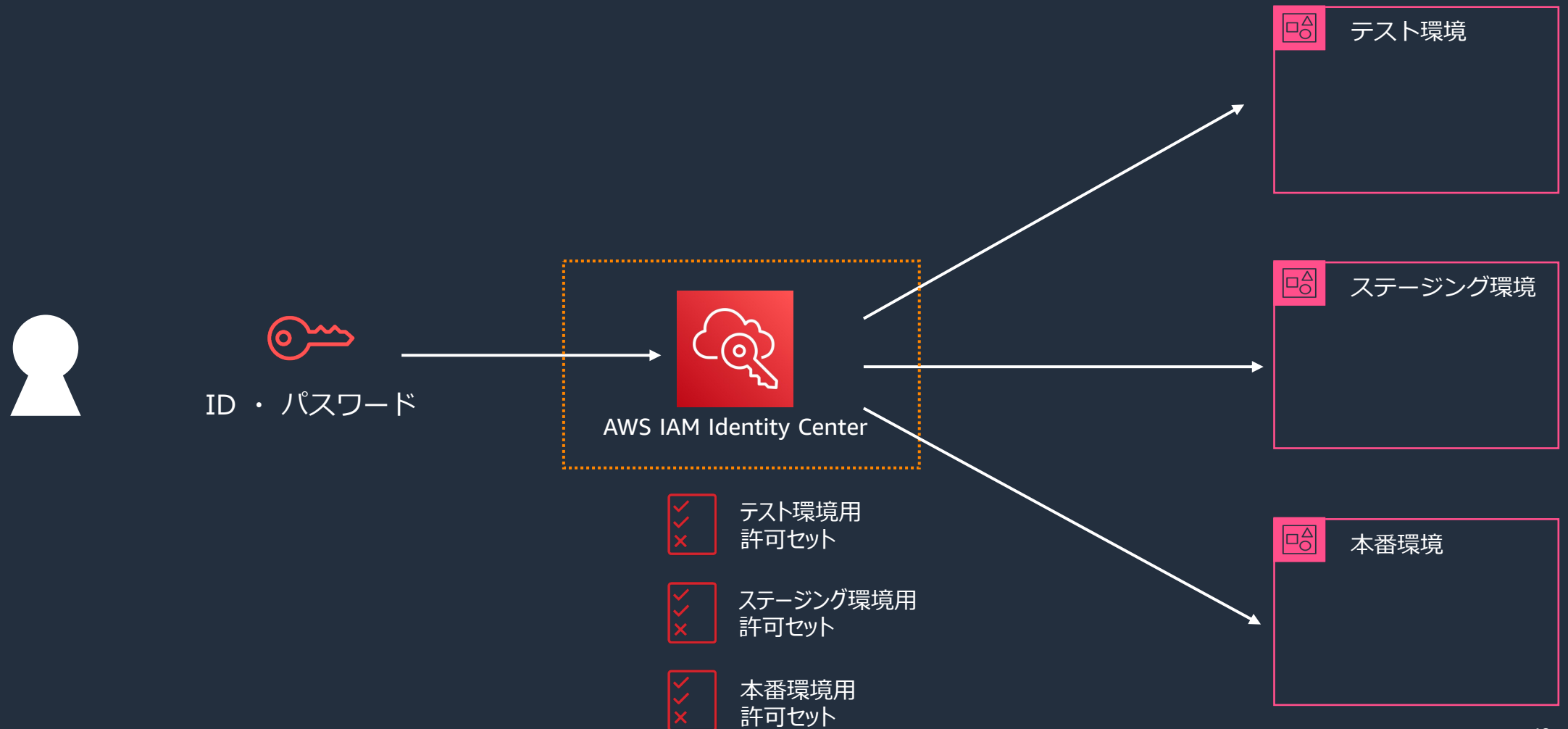


AWS IAM Identity Center

- 複数の AWS アカウントに対するシングルサインオンを実現する仕組み
- マルチアカウント環境におけるID管理/特権管理の悩みを解消する
 - 単一の ID で複数の AWS 環境にログインできる
 - ID と権限の管理が容易になる



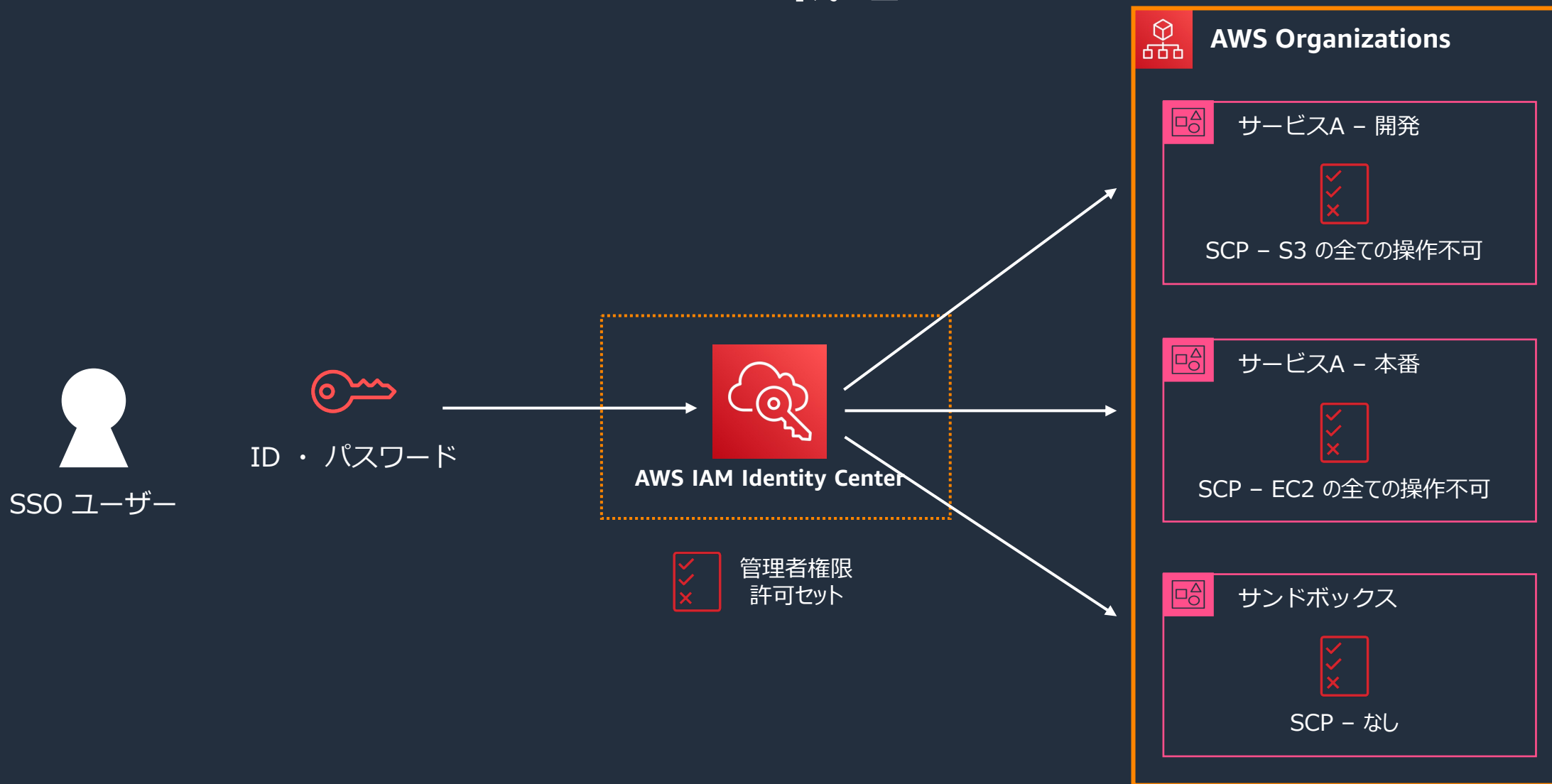
AWS IAM Identity Center を利用したアカウント管理



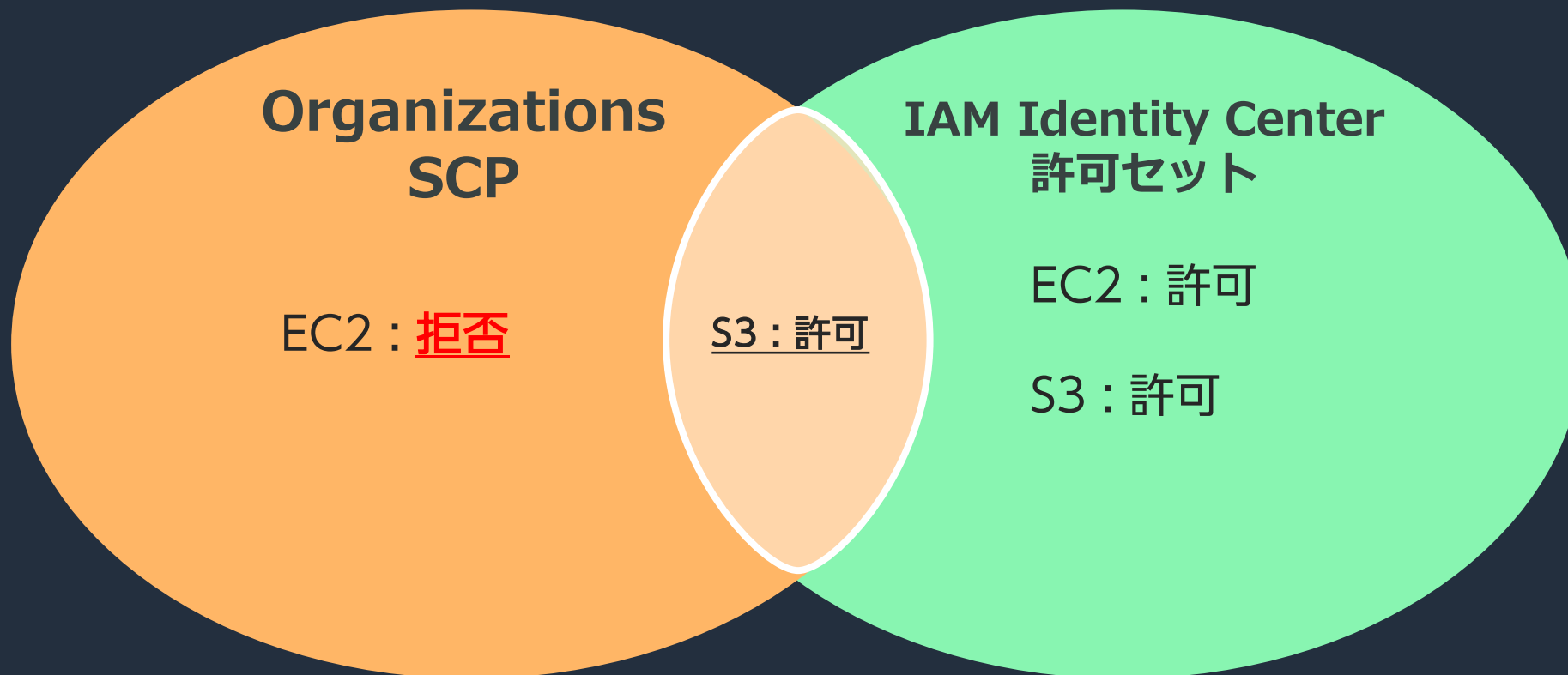
本シリーズのアジェンダ

- 1) 今回のハンズオンの説明 + アカウント作成に必要なもの + 作成の流れ
- 2) アカウントを作成してみる 🖐️
- 3) ルートユーザーと IAM ユーザーについて学ぶ
- 4) IAM ユーザーを作成する 🖐️
- 5) IAM (ポリシー、グループ、ロール) について学ぶ
- 6) IAM ポリシーと IAM グループを作ってみる 🖐️
- 7) IAM ロールを試してみる 🖐️
- 8) [Option] マルチアカウント戦略について学ぶ
- 9) [Option] AWS Organizations によるマルチアカウント戦略を試してみる 🖐️
- 10) まとめ + Next Action としてオススメのコンテンツを紹介

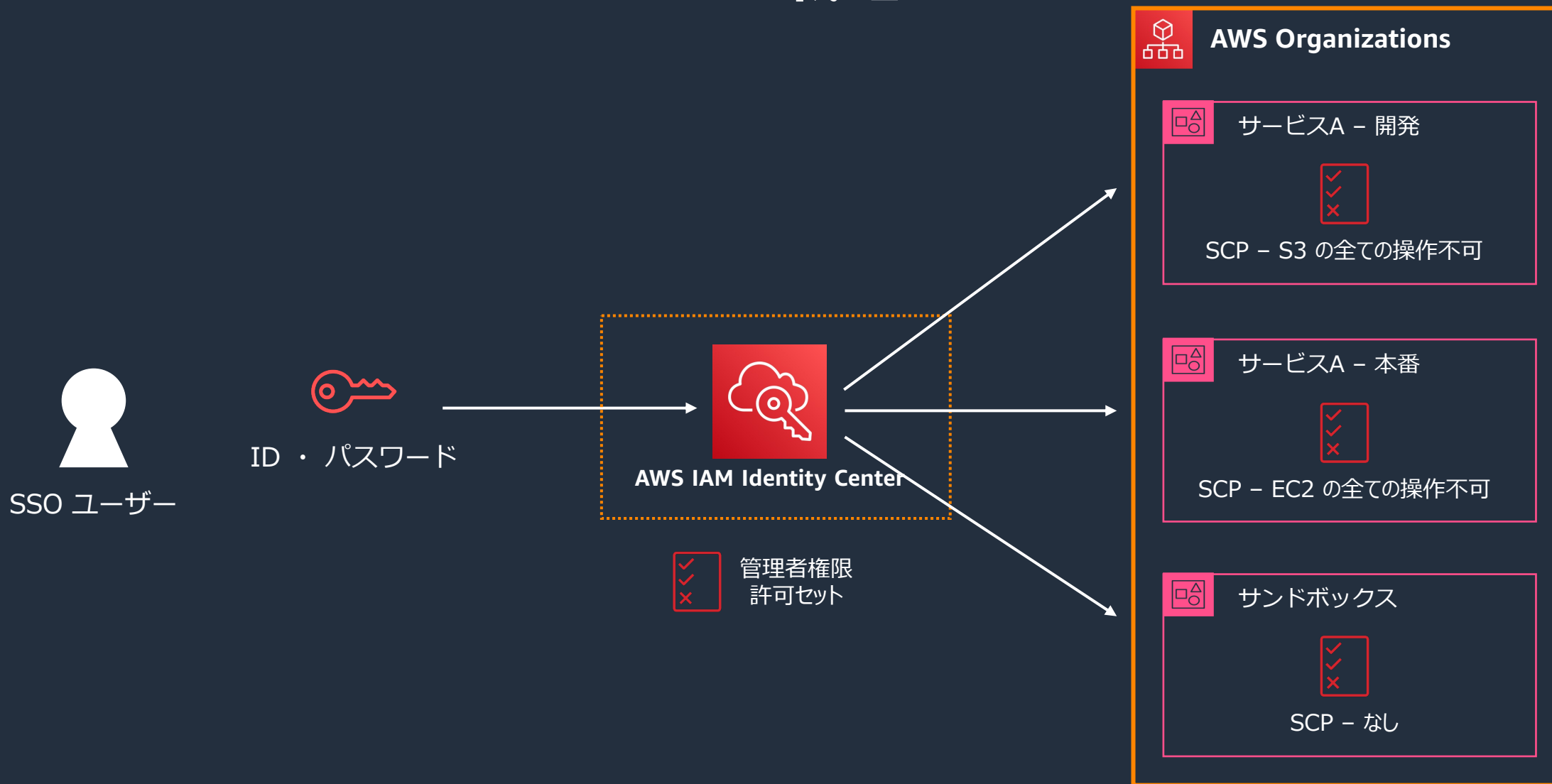
ハンズオン - マルチアカウント戦略



SCP と 許可セットの関係



ハンズオン - マルチアカウント戦略



本シリーズのアジェンダ

- 1) 今回のハンズオンの説明 + アカウント作成に必要なもの + 作成の流れ
- 2) アカウントを作成してみる 🖐️
- 3) ルートユーザーと IAM ユーザーについて学ぶ
- 4) IAM ユーザーを作成する 🖐️
- 5) IAM (ポリシー、グループ、ロール) について学ぶ
- 6) IAM ポリシーと IAM グループを作ってみる 🖐️
- 7) IAM ロールを試してみる 🖐️
- 8) [Option] マルチアカウント戦略について学ぶ
- 9) [Option] AWS Organizations によるマルチアカウント戦略を試してみる 🖐️
- 10) まとめ + Next Action としてオススメのコンテンツを紹介**

AWS アカウントの作成

- 登録する **メールアドレス**
- アカウント認証に使用する **電話番号**
- お支払いに利用する
クレジットカード or デビットカード

① **基本情報の入力**
メールアドレス・パスワードなど

② **連絡先情報の入力**
氏名・住所など

③ **お支払い情報の入力**
カード情報・請求先住所など

④ **アカウント認証**
SMS or 音声による認証

⑤ **サポートプランの選択**

各種 IAM リソースのまとめ

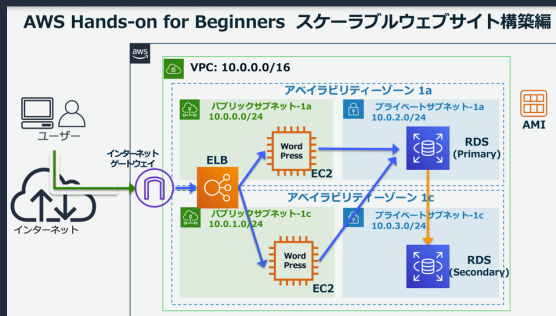


マルチアカウント戦略のまとめ

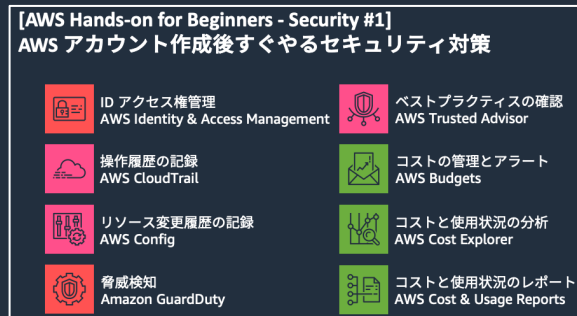


Next Action のオススメ

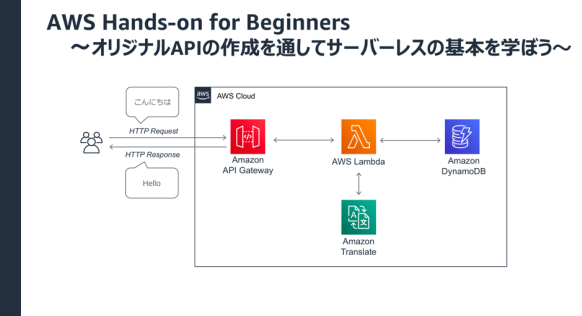
スケーラブルウェブサイト 構築編



AWSアカウント作成後 すぐやるセキュリティ対策



サーバーレスアーキテクチャで 翻訳 Web API を構築する



[AWS 初心者向けハンズオン]

<https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/>

Next Action のオススメ

The screenshot shows the JP Contents Hub website. The header includes the site name, a search bar, and GitHub repository information (127 stars, 8 forks). The left sidebar lists various AWS categories, with 'AWS 日本語ハンズオン' selected. The main content area is titled 'AWS 日本語ハンズオン' and contains the following text:

Amazon Web Services(AWS) の 日本語ハンズオンやワークショップを、カテゴリごとにまとめています。右側の目次や、ヘッダー部分の検索ボックスから、各コンテンツにたどり着けます。また、Ctrl + F や command + F を使ったページ内検索もご利用いただけます。

Two callout boxes provide additional information:

- 料金について**: ハンズオンで作成した AWS リソースは通常の料金が発生します。作成したリソースの削除を忘れずをお願いします。もし忘れてしまうと、想定外の料金が発生する可能性があります。
- 画面の差異について**: ハンズオンで紹介されている手順と、実際の操作方法に差異がある場合があります。AWS は随時アップデートされており、タイミングによってはハンズオンコンテンツが追いついていない事もあります。差異がある場合、AWS Document などを活用しながら進めて頂けると幸いです。

The 'Analytics' section is highlighted with a purple icon and contains the following information:

- [Amazon QuickSight のセルフハンズオンキット日本語版](#)

4 種類の QuickSight ハンズオンを学習いただけます。QuickSight の主要な可視化機能・ML インサイト・Webアプリケーションにダッシュボードを埋め込む方法などを学習いただけます。

tag : Amazon QuickSight, Amazon Athena

[JP Contents Hub 日本語ハンズオン]

<https://aws-samples.github.io/jp-contents-hub/>



アンケートも
よろしくお願いします!

