このコンテンツは公開から3年以上経過しており内容が古い可能性があります
最新情報については[サービス別資料]もしくはサービスのドキュメントをご確認ください

[AWS Black Belt Online Seminar]

AWSアカウント シングルサインオンの設計と運用

ソリューションカットシリーズ

Security Solutions Architect
中島 智広
2020/07/22

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

自己紹介

中島　智広（Tomohiro Nakashima）

AWS Security Solutions Architect

お客様のセキュリティの取り組みを
AWSアーキテクチャの視点からご支援

好きなAWSサービス

AWS Single Sign-On(SSO)

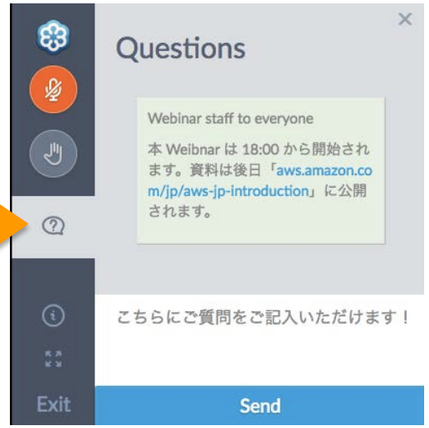
AWS Black Belt Online Seminar とは

「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分かれて、アマゾン ウェブ サービス ジャパン株式会社が主催するオンラインセミナーシリーズです。

質問を投げることができます！

- 書き込んだ質問は、主催者にしか見えません
- 今後のロードマップに関するご質問は
  お答えできませんのでご了承下さい

① 吹き出しをクリック
② 質問を入力
③ Sendをクリック



Twitter 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2020年7月22日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。

- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at http://aws.amazon.com/agreement/. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

本セミナーの概要

AWSアカウントに、IAMユーザーを作成しログインする代わりに、IDプロバイダー(IdP) を使用しシングルサインオンすることができます。

これは、組織に独自のID基盤がある場合や、複数のAWSアカウントを使用している場合に便利です。

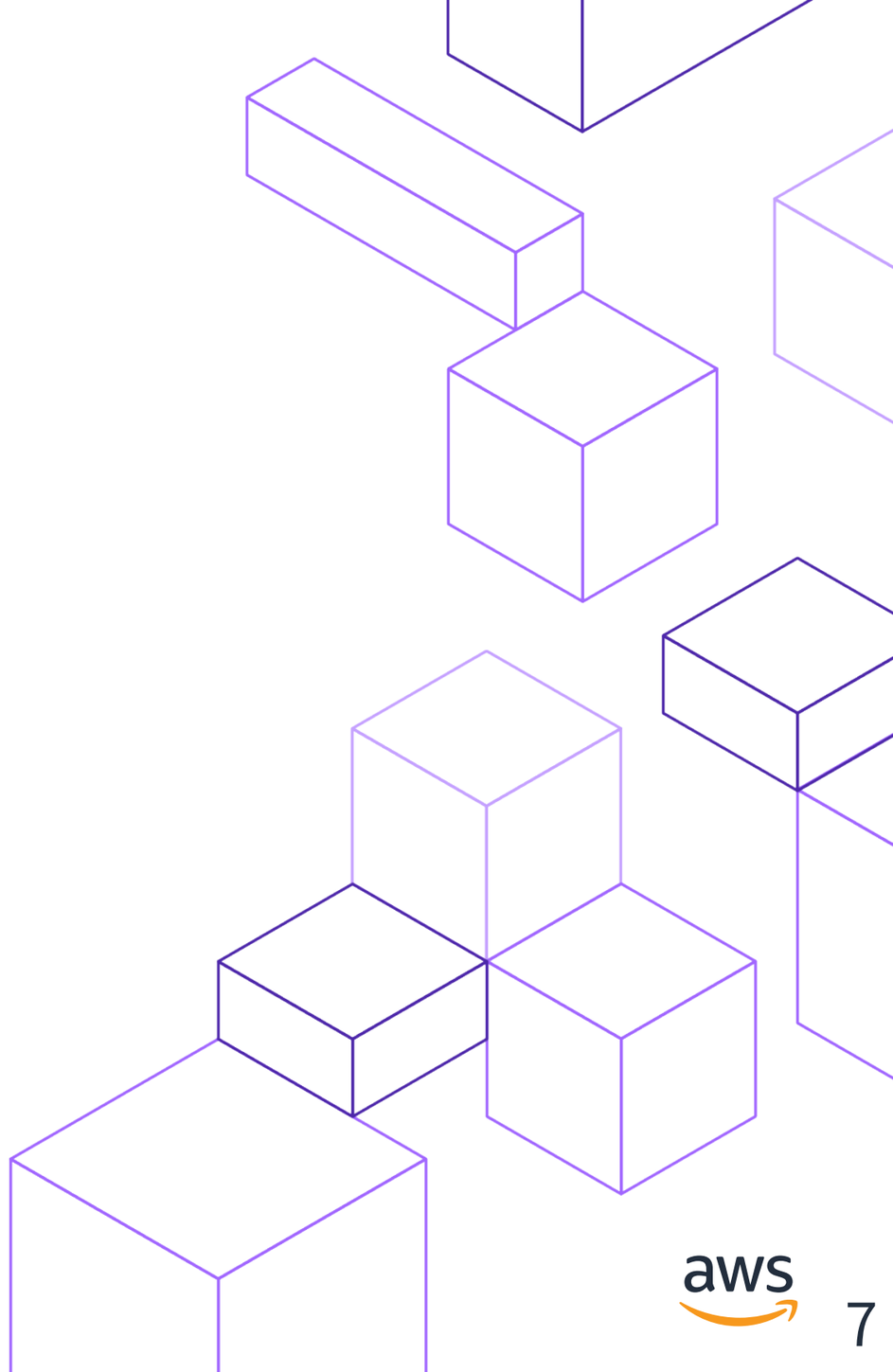
このようなシングルサインオンの構成には、AWS Single Sign-On(SSO)や、Active Directory Federation Services(ADFS)、外部サービスとの連携など、複数のデザインパターンがあります。

運用をふまえながらシングルサインオンを構成する勘所を解説します。

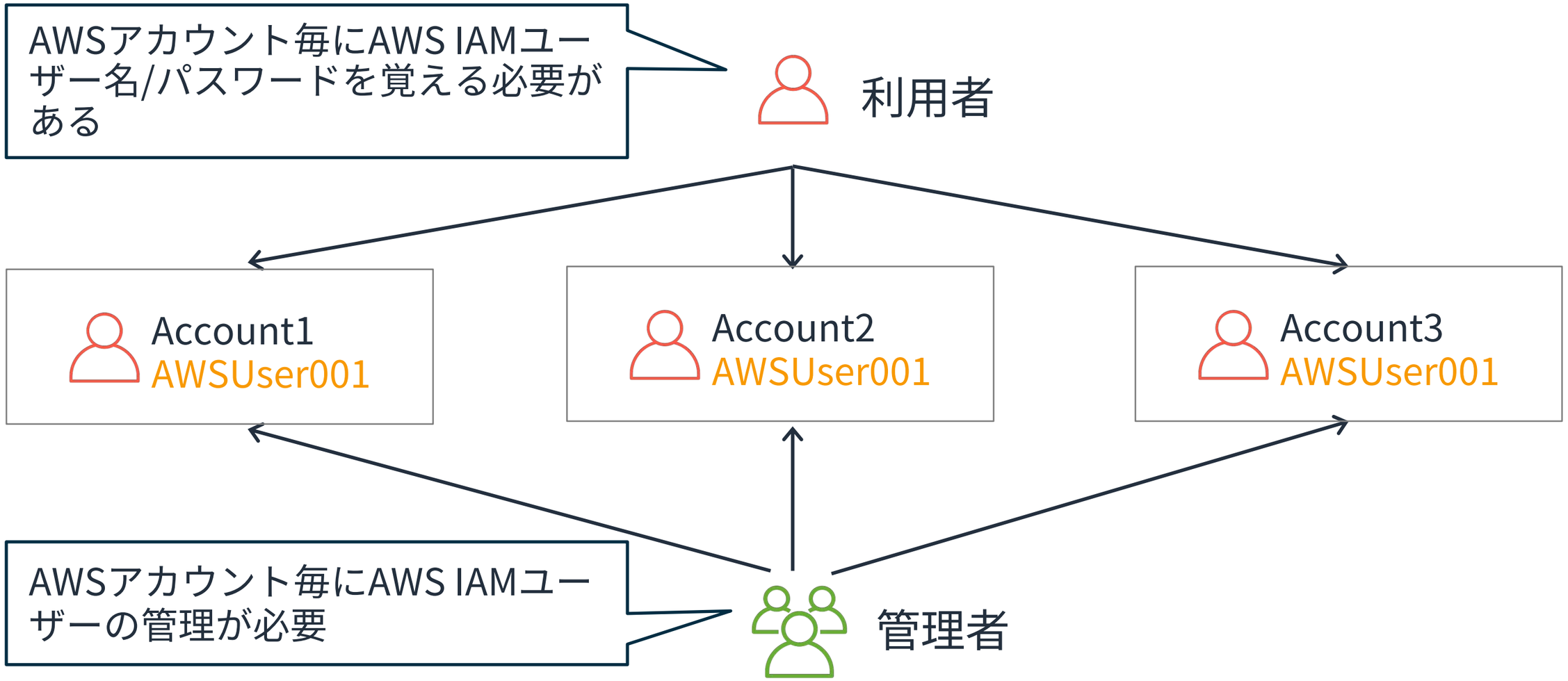
Agenda

1. マルチアカウントのアイデンティティ管理
2. AWSにおけるシングルサインオン
3. AWS Single Sign-On(SSO)
4. シングルサインオン設計のポイント
5. シングルサインオン運用のポイント
6. まとめ

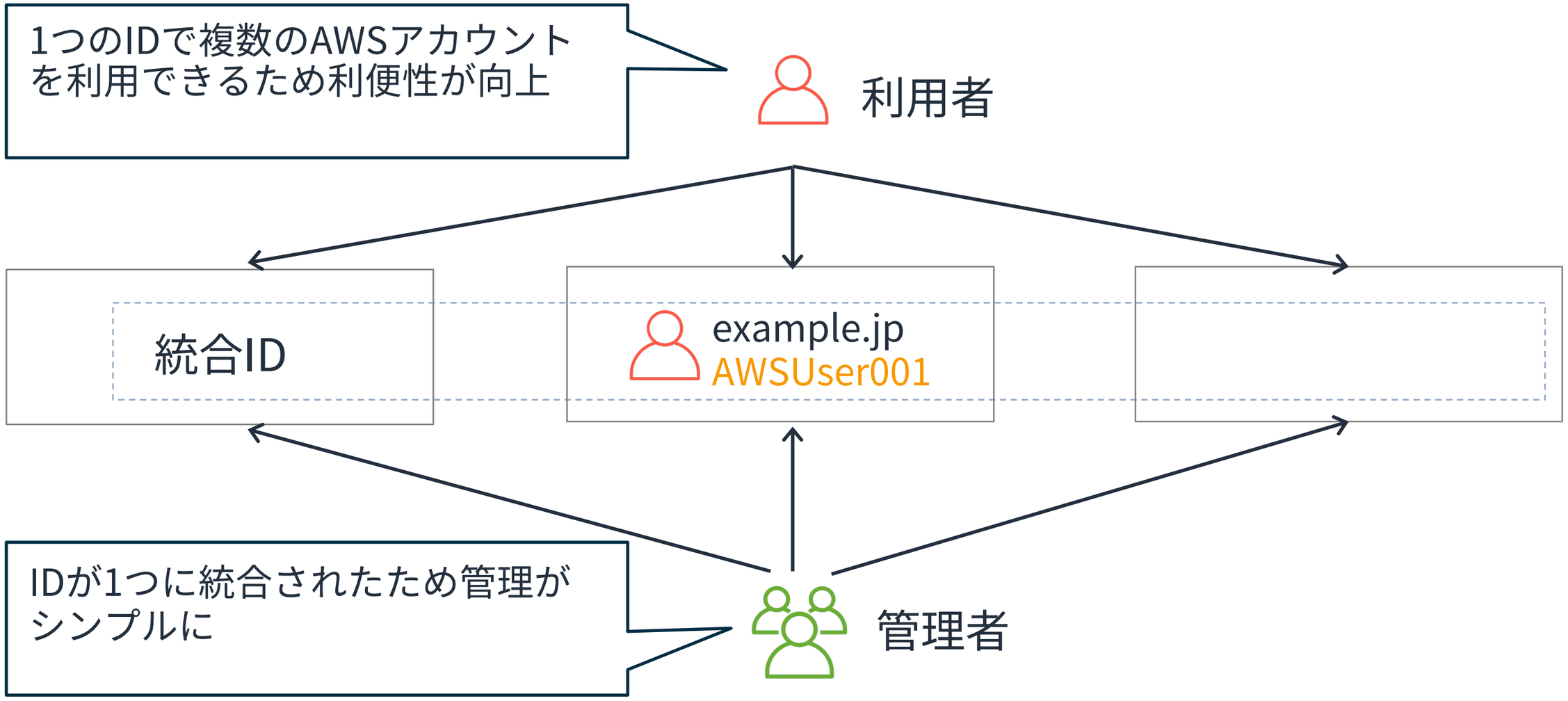
マルチアカウントの
アイデンティティ管理



マルチアカウントではアイデンティティ管理が課題に



統合されたIDを利用することで利用と管理がシンプルに



Terminology

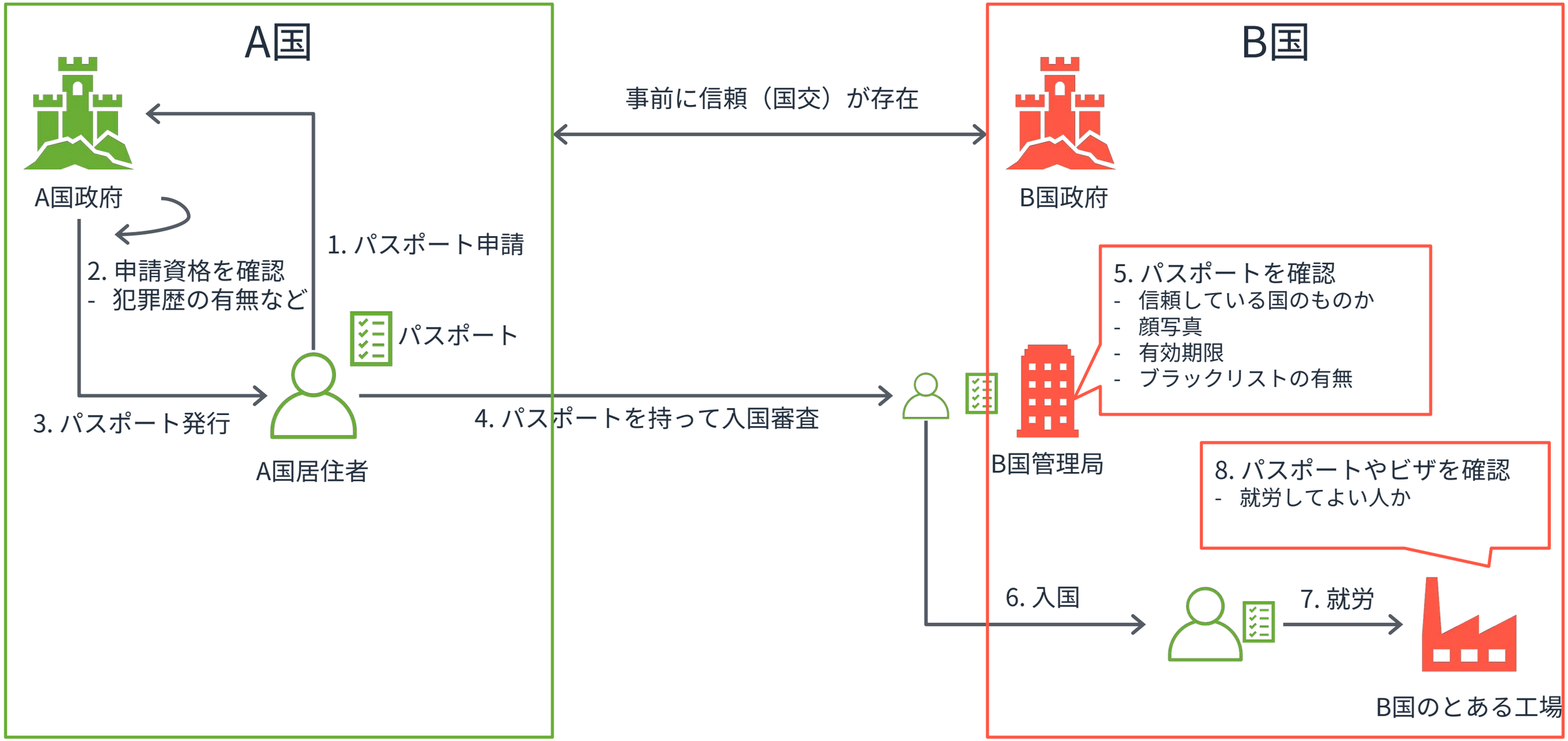
シングルサインオン

一度のユーザ認証処理によって、独立した複数のソフトウェアシステム上のリソースが利用可能になる特性

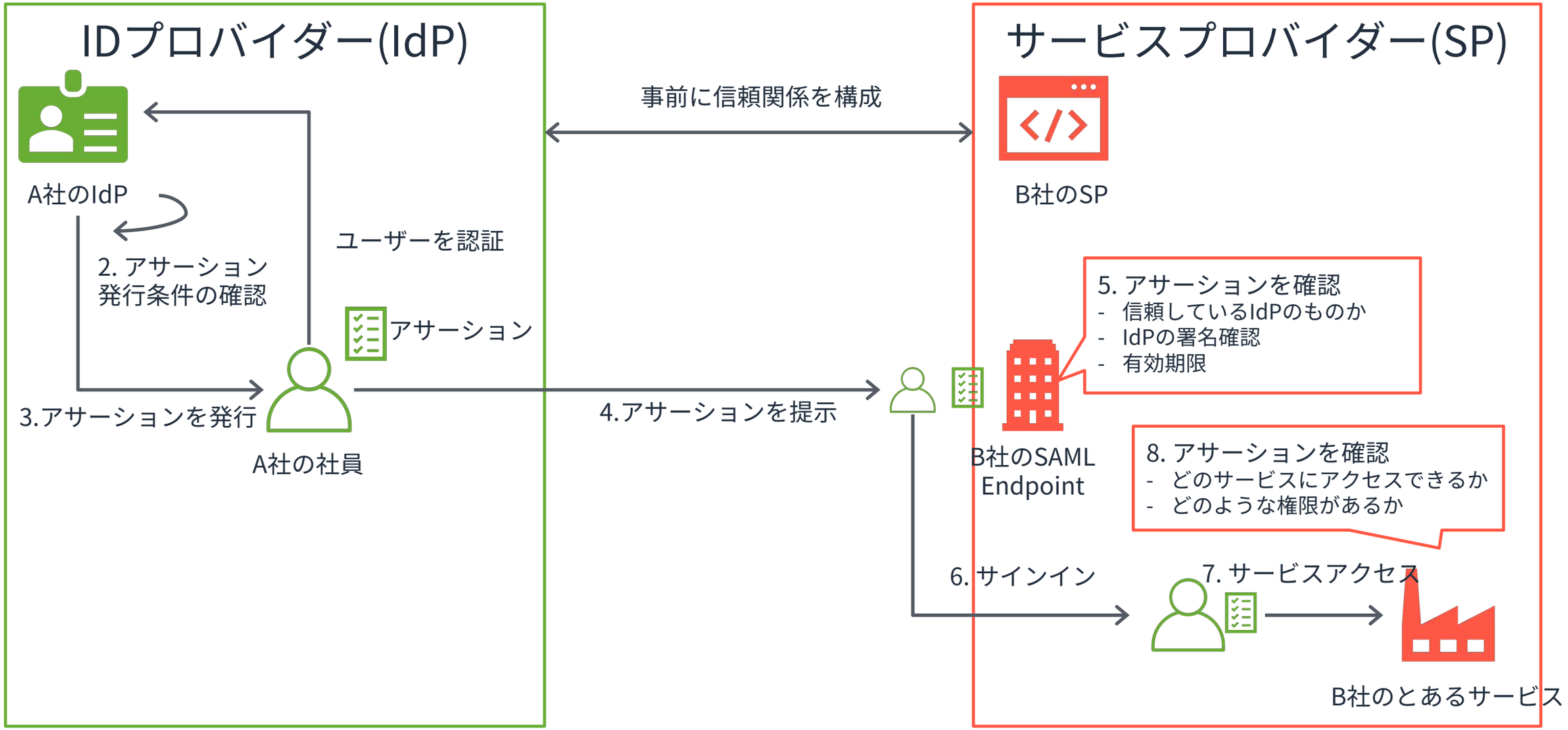
IDフェデレーション

シングルサインオンを実現する方式のひとつ、ひとつの組織（管理ドメイン）を超えて他の管理ドメインのサービスにもログインできるようにする処理のこと、SAMLなどの標準技術を適用して実現することが多い

IDフェデレーションはパスポートのようなもの



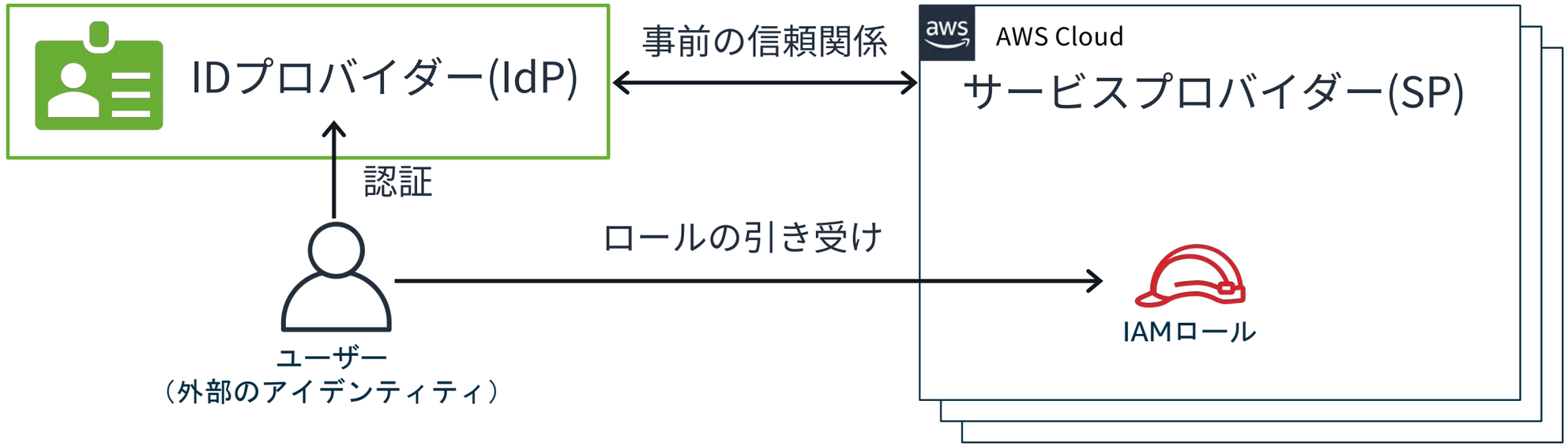
IDフェデレーションはパスポートのようなもの



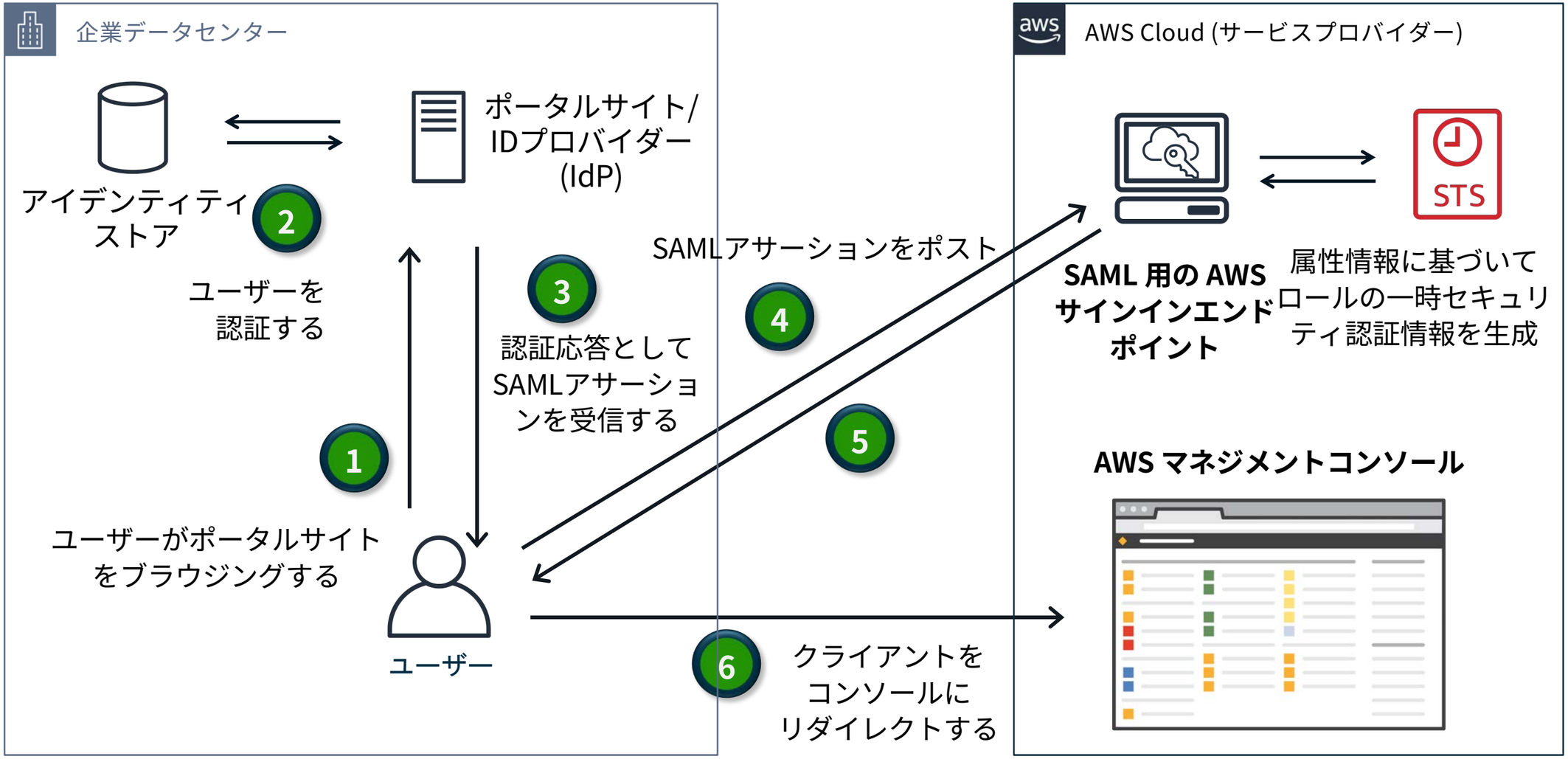
AWSにおけるシングルサインオン

AWSアカウントにおけるシングルサインオン

- SAMLやOIDCを用いたIDフェデレーションをサポート
- 外部のアイデンティティに、IAMロールのセッションを用いてAWSリソースへのアクセスを可能とする



IDフェデレーション with SAML



IDフェデレーションの構成に必要なタスク

アイデンティティストア
- IDプロバイダー（IdP）向け被参照設定（サービスアカウントの作成など）

IDプロバイダー（IdP)
- アイデンティティストアの参照設定
- メタデータドキュメントのエクスポート
- 認証レスポンスの SAML アサーションを設定

AWSアカウント
- IAM IDプロバイダーの設定（ AWS アカウントと IdP の間の「信頼」の確立）
- フェデレーテッドユーザー向けロールの作成

IAM IDプロバイダーの設定

IDプロバイダー（IdP)からエクスポートしたメタデータドキュメントを指定

フェデレーテッドユーザー向けロールの作成

信頼ポリシーのPrincipalには、作成したIAM IDプロバイダーのARNを指定

```
{
   "Version": "2012-10-17",
   "Statement": {
     "Effect": "Allow",
     "Action": "sts:AssumeRoleWithSAML",
     "Principal": {"Federated": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-
provider/PROVIDER-NAME"},
     "Condition": {"StringEquals": {"SAML:aud": "https://signin.aws.amazon.com/saml"}}
   }
}
```

SAML 2.0 フェデレーティッドユーザーが AWS マネジメントコンソールにアクセス可能にする
https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_roles_providers_enable-console-saml.html

認証レスポンスのSAMLアサーションを設定

IDプロバイダー（IdP）からサービスプロバイダー（AWS）に連携する情報(クレーム）を設定

クレーム	必須	概要
Subject and NameID	○	SAMLの仕様で定義されたIdPとSPの間で共有されるユーザー識別子
AudienceRestriction and Audience	○	SAMLの仕様で定義されたセキュリティ上の理由から含める必要のある要素、https://signin.aws.amazon.com/saml または urn:amazon:webservices を指定
SAML Role Attribute	○	マッピングするロールを指定する要素
SAML RoleSessionName Attribute	○	AWS マネジメントコンソールやCloudTrail Logでユーザー情報を表示、記録する際に使用される要素、トレーサビリティの観点で重要（後述）
SAML SessionDuration Attribute		フェデレーテッドユーザーが AWS マネジメントコンソール にアクセスできる時間を指定する 要素、値は900 秒 (15 分) から 43200 秒 (12 時間)
SAML PrincipalTag Attribute		属性ベースのアクセス制御（ABAC）に利用可能な属性をセッションタグとして連携する要素（後述）

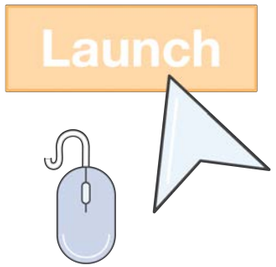
認証レスポンスの SAML アサーションを設定する
https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_roles_providers_create_saml_assertions.html

AWS Single Sign-On(SSO)

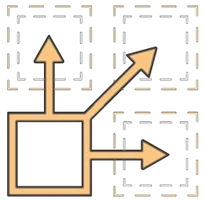
IDフェデレーションをもっと簡単に

AWS Single Sign-On (SSO)

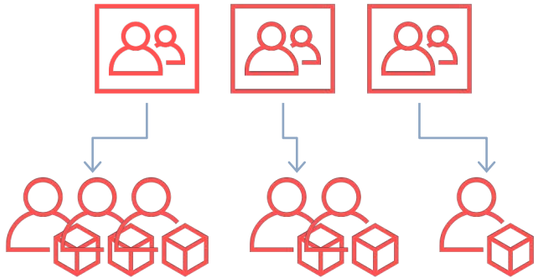
AWS アカウントとビジネスアプリケーションへの シングルサインオン (SSO) を提供するクラウドサービス



簡単に利用を
始められる



複数 AWS アカウント
のコンソールに
SSO アクセス



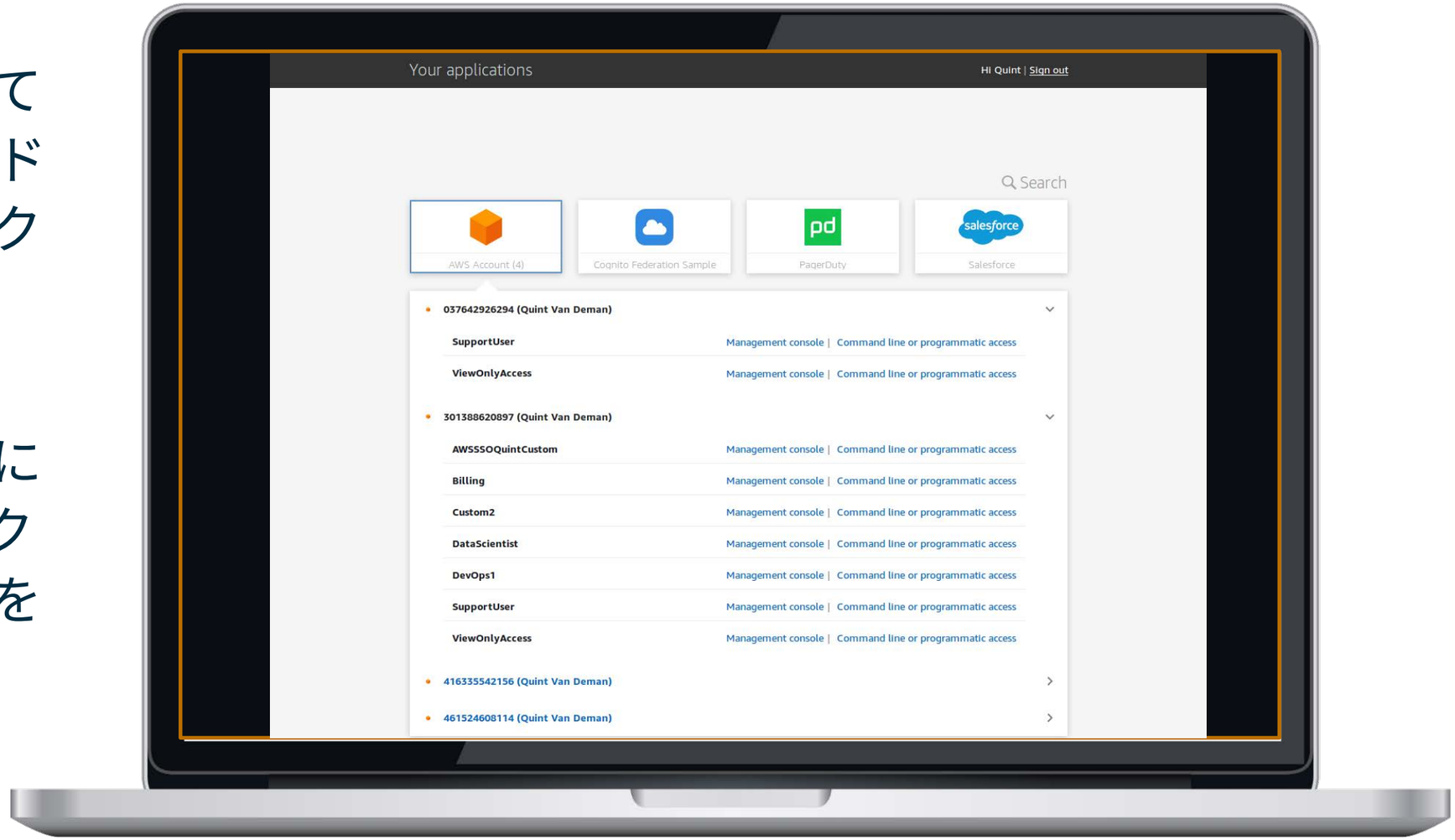
AWS Organizationsと
統合されたアクセス権
限の一元管理

ビジネス
アプリケーションに
SSO アクセス

AWS SSO ユーザーポータル

ユーザーポータルを通じてAWSアカウントとクラウドアプリケーションへのアクセスを提供

マネジメントコンソールに加えて CLI/API によるアクセスのためのオプションを提供



AWS SSO 導入に必要なタスク

アイデンティティストア
- IDプロバイダー（IdP）向け被参照設定（サービスアカウントの作成）

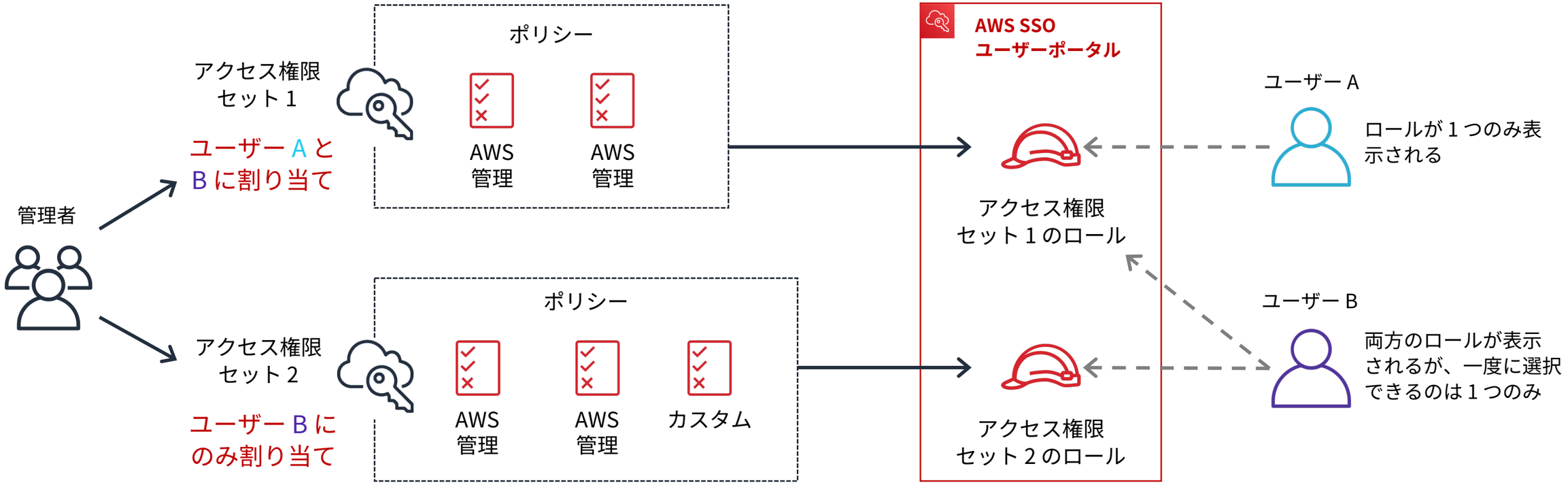
IDプロバイダー（IdP)
- アイデンティティストアの参照設定
- アクセス権限セットの設定

IDフェデレーションの構成に必要な
その他のタスクはAWS SSOが
お客様に代わってプロビジョニング

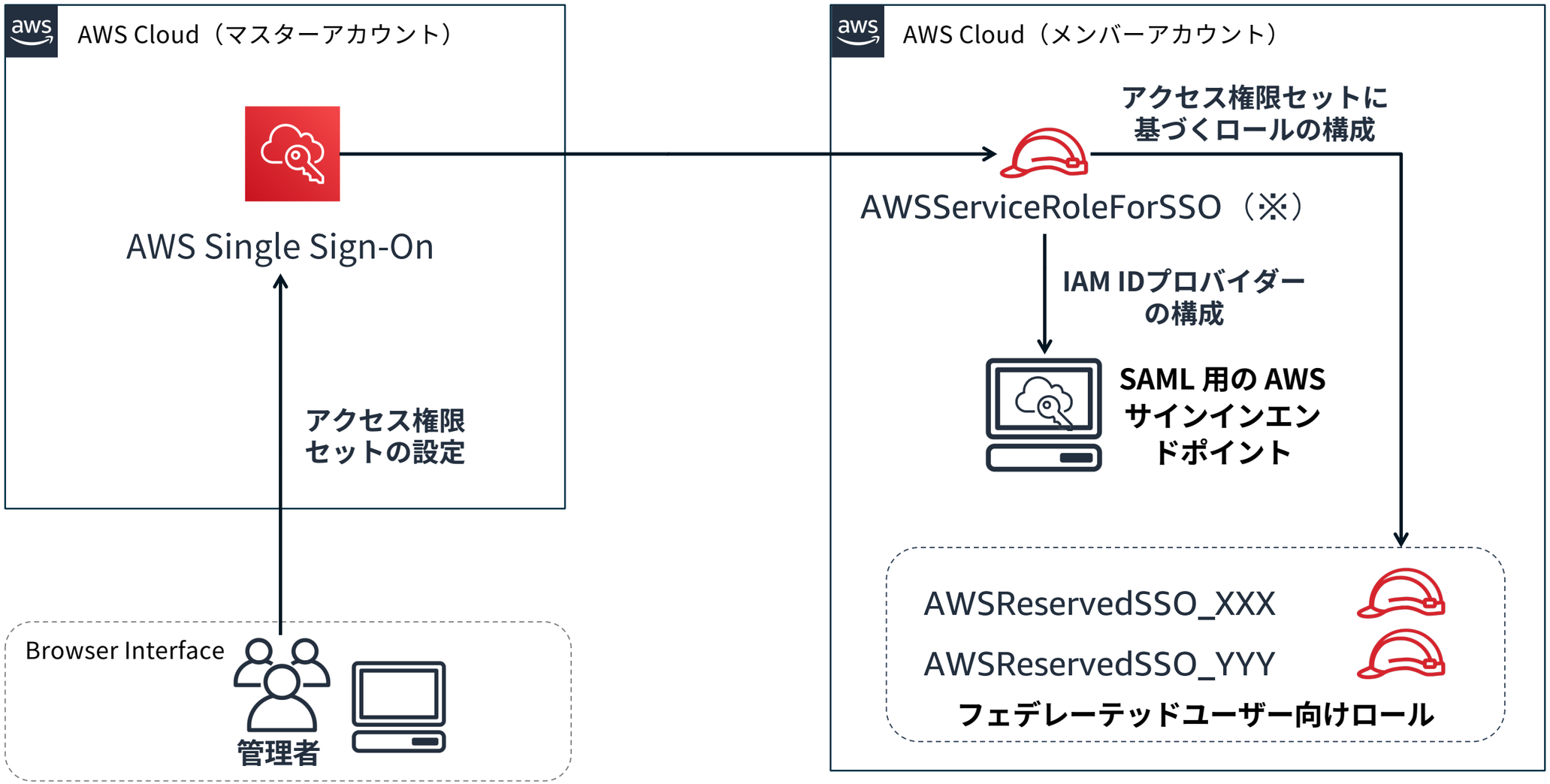
AWSアカウント（AWS Organizations メンバーアカウント）
なし

アクセス権限セット

AWS Organizations マスターアカウントから、ユーザー毎のアクセス権限を一元管理するAWS Single Sign-On(SSO)ならではの仕組み



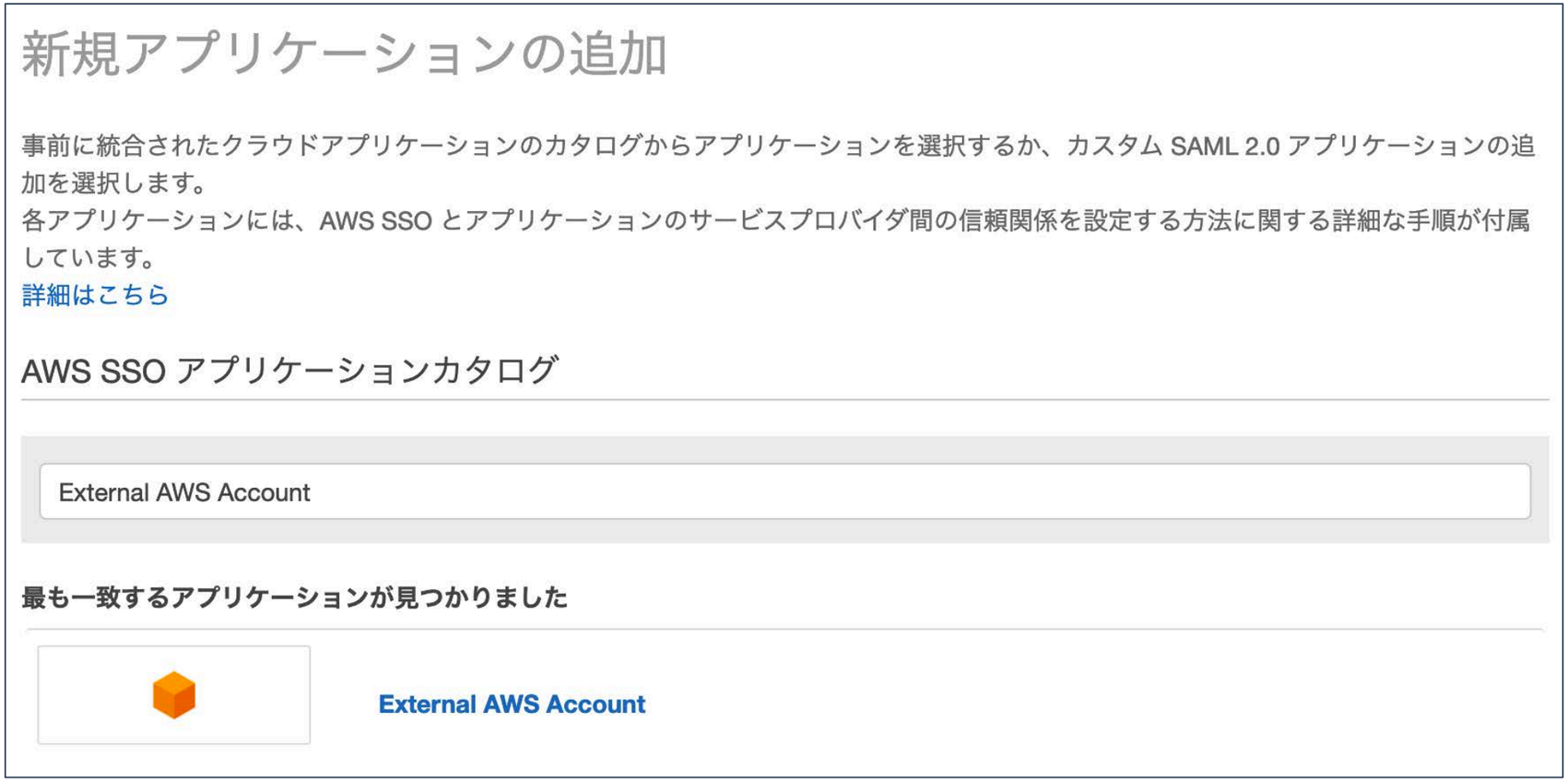
メンバーアカウントへのプロビジョニングの仕組み



※AWS Organizationsマスターアカウントでの AWS Single Sign-On(SSO)利用開始時に自動で作成される

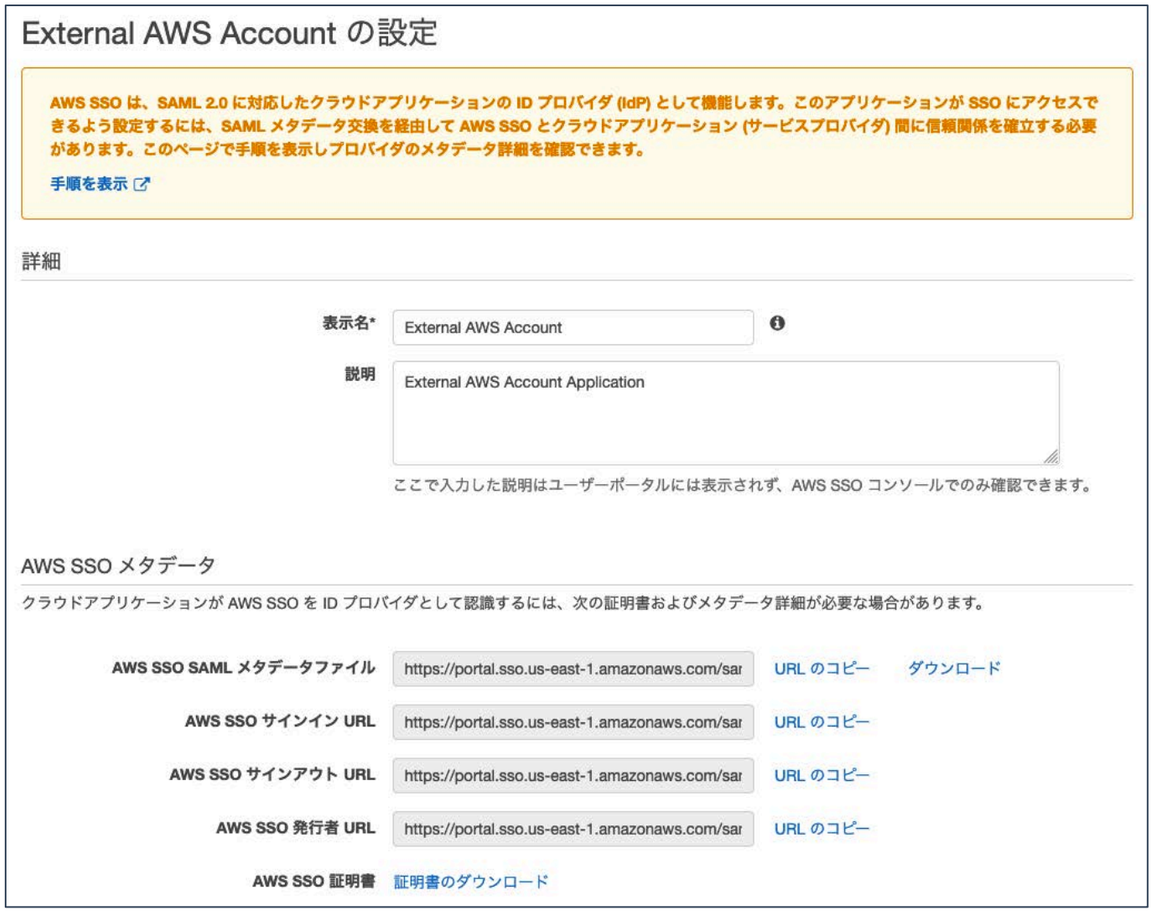
AWS Organizations 組織外のアカウントへの対応

AWS SSO アプリケーションカタログから「External AWS Account」を選択し構成することで、非メンバーのAWSアカウントへのIDフェデレーションを構成可能



AWS Organizations 組織外のアカウントへの対応 続き

非メンバーのAWSアカウントへのプロビジョニングは手動で行う必要がある



AWS CLIv2との統合

```
$ aws sso login  --profile SecurityAudit-123456789012
Attempting to automatically open the SSO authorization page in
your default browser.
If the browser does not open or you wish to use a different
device to authorize this request, open the following URL:


https://device.sso.us-east-1.amazonaws.com/


Then enter the code:

ABCD-EFGH
```

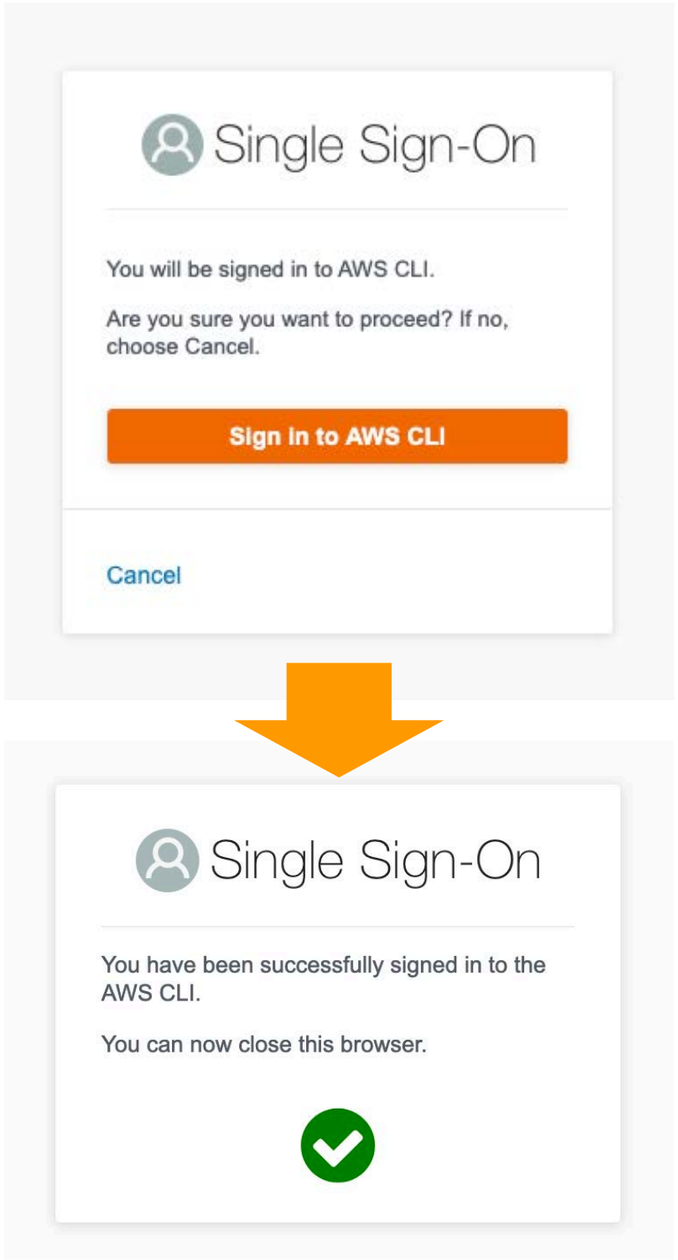
AWS CLIv2との統合

```
$ aws sso login  --profile SecurityAudit-123456789012
Attempting to automatically open the SSO authorization page in
your default browser.
If the browser does not open or you wish to use a different
device to authorize this request, open the following URL:


https://device.sso.us-east-1.amazonaws.com/


Then enter the code:

ABCD-EFGH
```



AWS CLIv2との統合

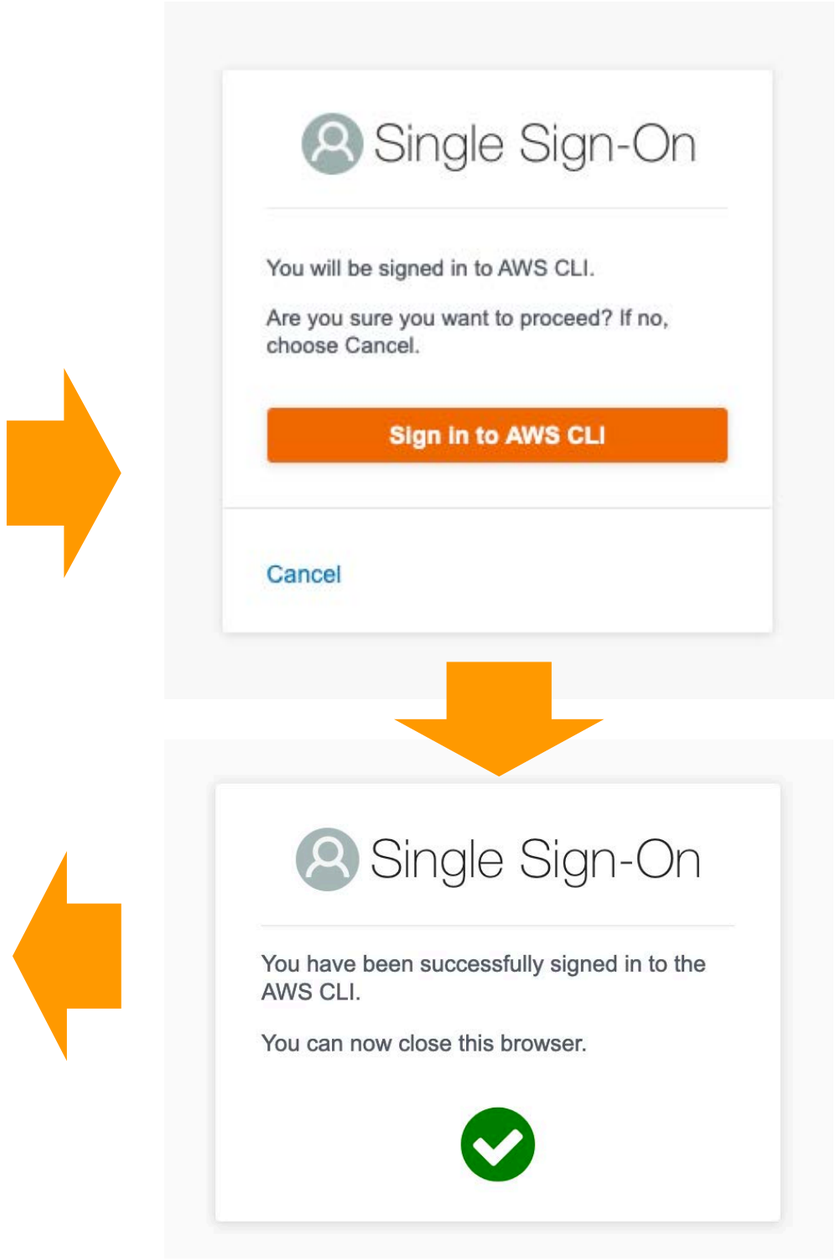
```
$ aws sso login  --profile SecurityAudit-123456789012
Attempting to automatically open the SSO authorization page in
your default browser.
If the browser does not open or you wish to use a different
device to authorize this request, open the following URL:


https://device.sso.us-east-1.amazonaws.com/


Then enter the code:

ABCD-EFGH
Successully logged into Start URL: https://[YOUR APP
URL].awsapps.com/start

$ aws s3 ls --profile SecurityAudit-123456789012
(snip)
$ aws sso logout  --profile SecurityAudit-123456789012
```



シングルサインオン設計のポイント

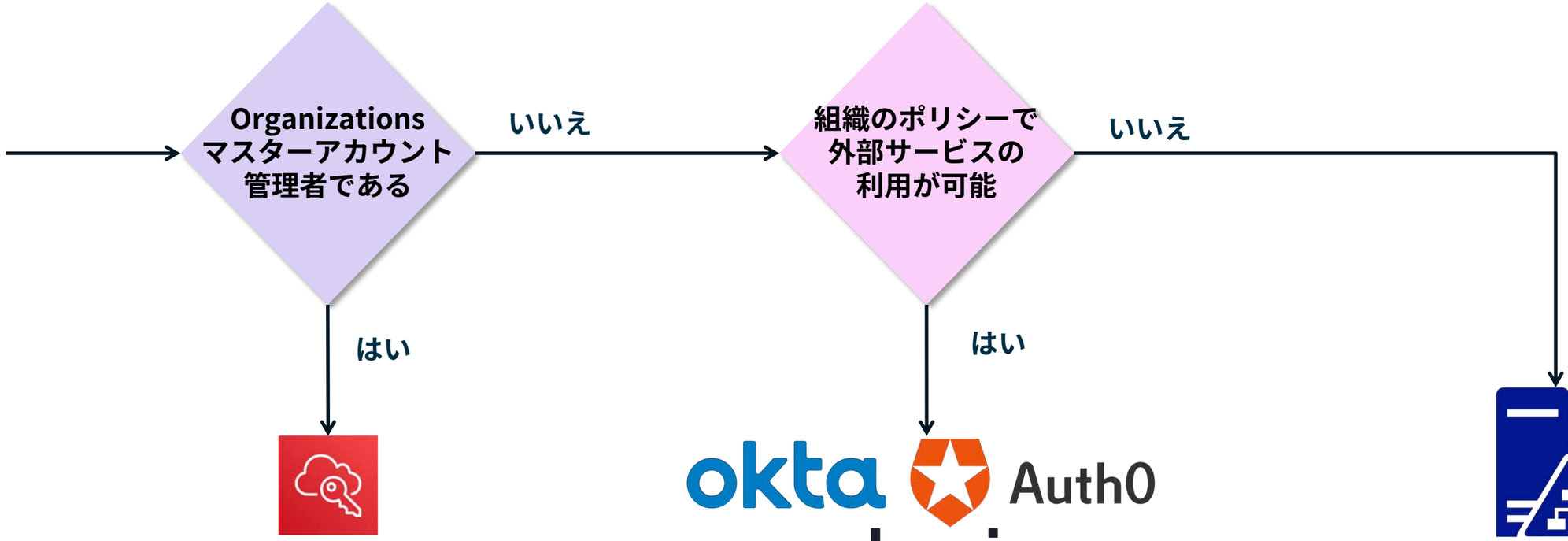
シングルサインオン設計のよくある論点

- IDプロバイダー（IdP）の選択
- アイデンティティストアの選択
- 複雑な要件への対応

IDプロバイダー（IdP）の選択

どのIDプロバイダー（IdP）を選ぶか？

導入や運用のしやすさを軸にした選定ロジックフローの例



AWS Single Sign-On

AWS利用の観点では最も
シンプルなソリューション

マネージドサービスで完結

Active Directory
Federation Service

お客様のAWS環境内で完結

IDプロバイダー（IdP）比較（2020年7月現在）

	AWS Single Sign-On(SSO)	サードパーティ サービス	Active Directory Federation Service （ADFS）
AWS 利用サービス	AWS Single-Sign-On(SSO)	―	Amazon EC2
構成の ポイント	マネージドサービスのみで完結 （AWS提供）	マネージドサービスのみで完結 （サードパーティを含む）	お客様のAWS環境内で完結
管理運用の シンプルさ	AWSアカウントとの連携を前提とした シンプルな設計、非技術者にも管理しやすい	サービス依存	多様な要件に対応可能でパラメータが複雑 管理者にはプロトコルやADFSについて 一定の前提知識を求める
メンバーアカウントへのプロビジョニング	AWS Organizationsマスターアカウントにて IAM IDプロバイダーとロールを一元管理	メンバーアカウントにてIAM IDプロバイダー とロールの手動設定が必要	メンバーアカウントにてIAM IDプロバイダー とロールの手動設定が必要
可用性の考慮	不要 （マネージドサービス）	不要 （マネージドサービス）	要 （お客様自身で冗長化）
AWS CLIv2 との統合	可	不可	不可

次頁につづく

IDプロバイダー（IdP）比較 続き（2020年7月現在）

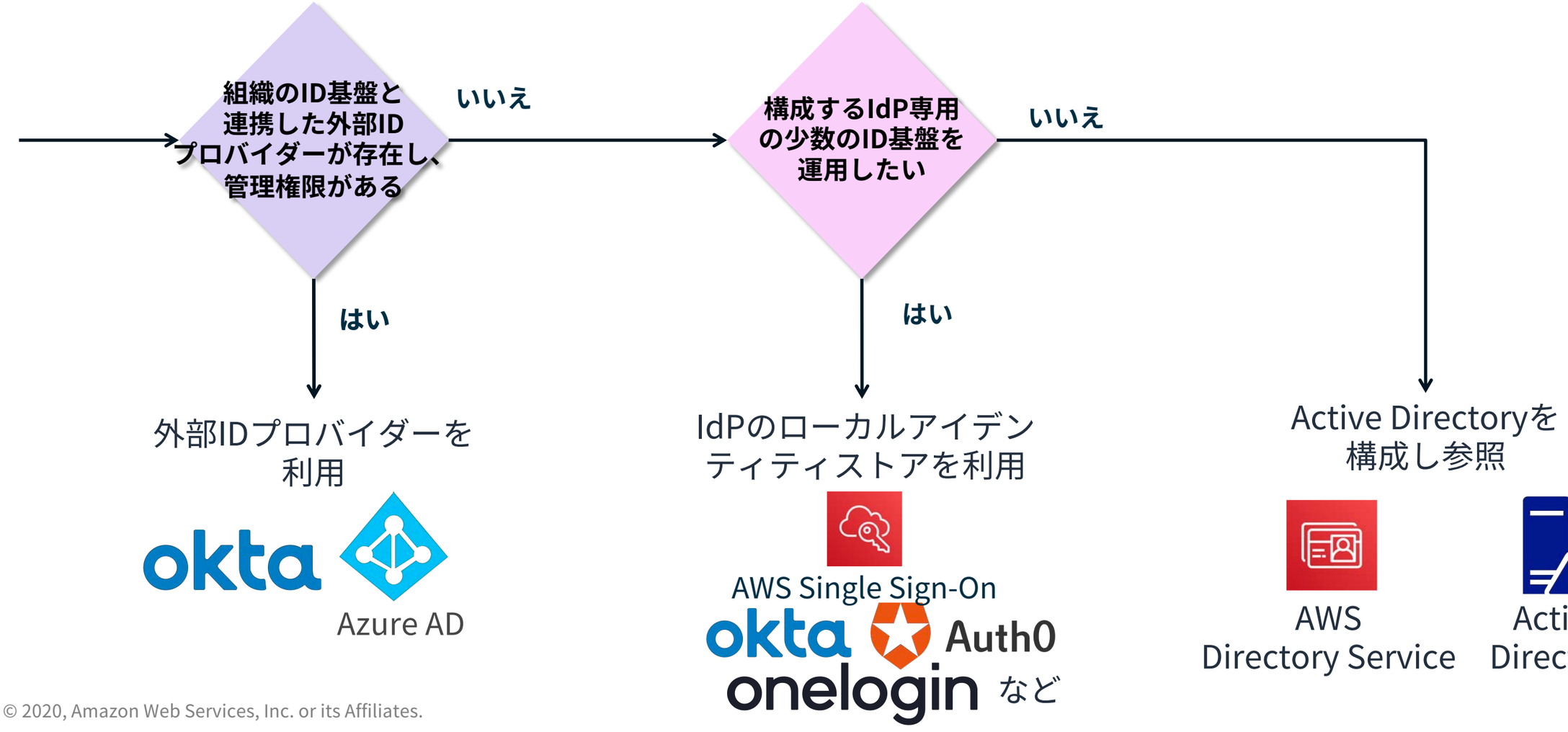
	AWS Single-Sign-On(SSO)	サードパーティ サービス	Active Directory Federation Service （ADFS）
セッションタグ	不可	サービス依存※	可
Windows 統合認証	不可	サービス依存 （基本的にはサードパーティ製コネクタ のクライアントへの導入が必要）	可
ポータルサイト の所在	インターネット	インターネット	Amazon VPC
ポータルサイト への接続元IPア ドレス制限	不可	サービス依存	可
ADからIdPへの 認証情報 取り込み	不要	必要とする場合がある	不要
導入に際しての ADでの作業	サービスアカウントの作成	サービス依存 （モジュールの導入を必要とする場合がある）	サービスアカウントの作成

※セッションタグをサポートするSAML ソリューションプロバイダーは以下を参照
https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_roles_providers_saml_3rd-party.html

アイデンティティストアの選択

どのアイデンティティストアを参照するか？

導入や運用のしやすさを軸にした選定ロジックフローの例



外部 ID プロバイダー

Azure AD
など(※)

SCIM

ユーザー属性
のマッピング

AWS
Single Sign-On
など

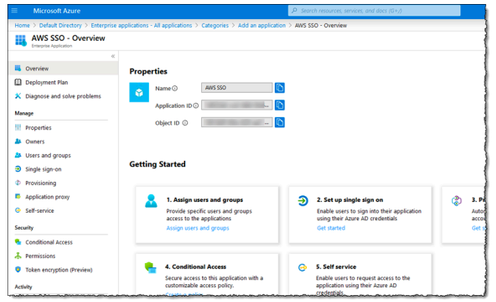
外部IDプロバイダー
/SCIMクライアント

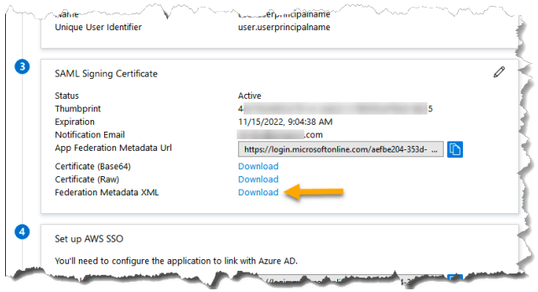
IDプロバイダー
/SCIMサーバー

SCIM
(System for Cross-Domains Identity Management)
異なるドメイン/事業者間のアカウントプロビジョニングを実現する仕組み

たとえば、Azure ADとAWS SSOの場合

1. 外部 ID プロバイダーと IDプロバイダー （IdP） の間でフェデレーションメタデータを交換するための設定を行う





2. AWS SSO の ID ソースで外部 ID プロバイダを指定し、ID プロバイダーメタデータセクションで フェデレーションメタデータとして、ダウンロードした XML ファイルを参照して選択

※AWS Single Sign-On(SSO)がサポートする
テスト済みの外部IDプロバイダーはOktaとAzure ADのみ

IdPのローカルアイデンティティストア

ユーザーやグループ
の登録管理

AWS Single Sign-On

okta Auth0

onelogin

など

注）運用上の利便性が高いものの、組織のアイデンティティを一元管理する観点からは推奨されない点に留意が必要

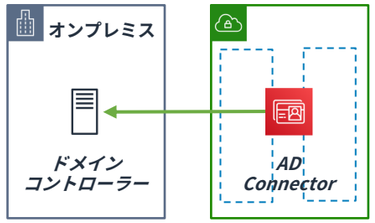
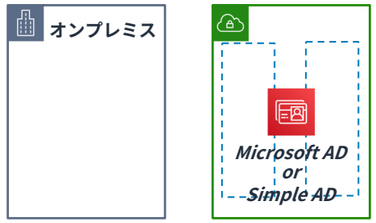
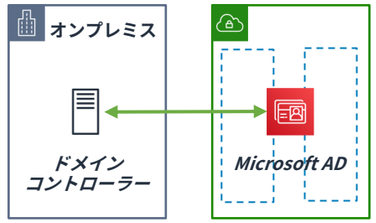
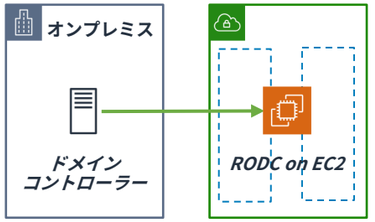
たとえば、AWS SSOの場合

1. IDソースにAWS SSOディレクトリを選択

2. AWS SSOのインターフェイスでユーザーを管理

Active Directoryを構成し参照

適材適所の構成パターンを選択、あるいは組み合わせて構成

	オンプレミス AD を参照	AWS環境に独立した ADを構築	オンプレミス AD との信頼関係	読み取り専用の レプリカ（RODC)
AD 配置				
AWS 利用サービス	AD Connector (ADC)	• Microsoft AD (MSAD) • Simple AD※	Microsoft AD (MSAD)	EC2(Windows Server AMI)
構成の説明	オンプレミスに展開されたドメインコントローラーに対して ADC 経由で接続	MSAD、Simple AD を使用	MSAD とオンプレミス AD ドメインとの双方向の推移的信頼関係	読み取り専用のレプリカドメインコントローラー（RODC)を構築
ポイント	構成はシンプルになるが、オンプレミスへの問い合わせが発生	オンプレミスと独立したドメインとして運用	オンプレミスと独立したドメインとなるが、信頼関係の構築によりオンプレミスドメインを認証に利用することが可能	認証処理がRODCで完結するため、オンプレミスの障害などから影響を分離可能

※AWS Single Sign-On（SSO)は、Samba4 ベースの Simple AD を接続先ディレクトリとしてサポートしていません。

アイデンティティストア比較（2020年7月現在）

	外部IDプロバイダー	IdPのローカル アイデンティティストア	Active Directory
AWS 利用サービス	AWS Single Sign-On(SSO) （IdPとして用いる場合）	AWS Single Sign-On(SSO) （IdPとして用いる場合）	AWS Directory Service あるいはEC2
ポイント	マネージドサービスのみで完結	マネージドサービスのみで完結	お客様のAWS環境内で完結
IdPとの ユーザー属性 マッピング	SCIM	一般にはIdP内でユーザー/グループを管理	Active Directoryの属性
可用性の考慮	不要 （マネージドサービス）	不要 （マネージドサービス）	要 （お客様自身で冗長化）
Sign-in URL	外部IDプロバイダー https://<外部IDプロバイダー Endpoint>	AWS SSOの場合 https://YOUR-DOMAIN.awsapps.com/start/ Third Party Endpointの場合 https://<Third Party Endpoint>	AWS SSOの場合 https://YOUR-DOMAIN.awsapps.com/start/ Third Party Endpointの場合 https://<Third Party Endpoint>
特記事項	AWS Single Sign-On(SSO)がサポートする テスト済みの外部IDプロバイダーは OktaとAzure ADのみ（※）	独立したアイデンティを持つことになり、 一元管理上の課題が生じる	–

※Supported Identity Providers
https://docs.aws.amazon.com/singlesignon/latest/userguide/supported-idps.html

多様な要件への対応

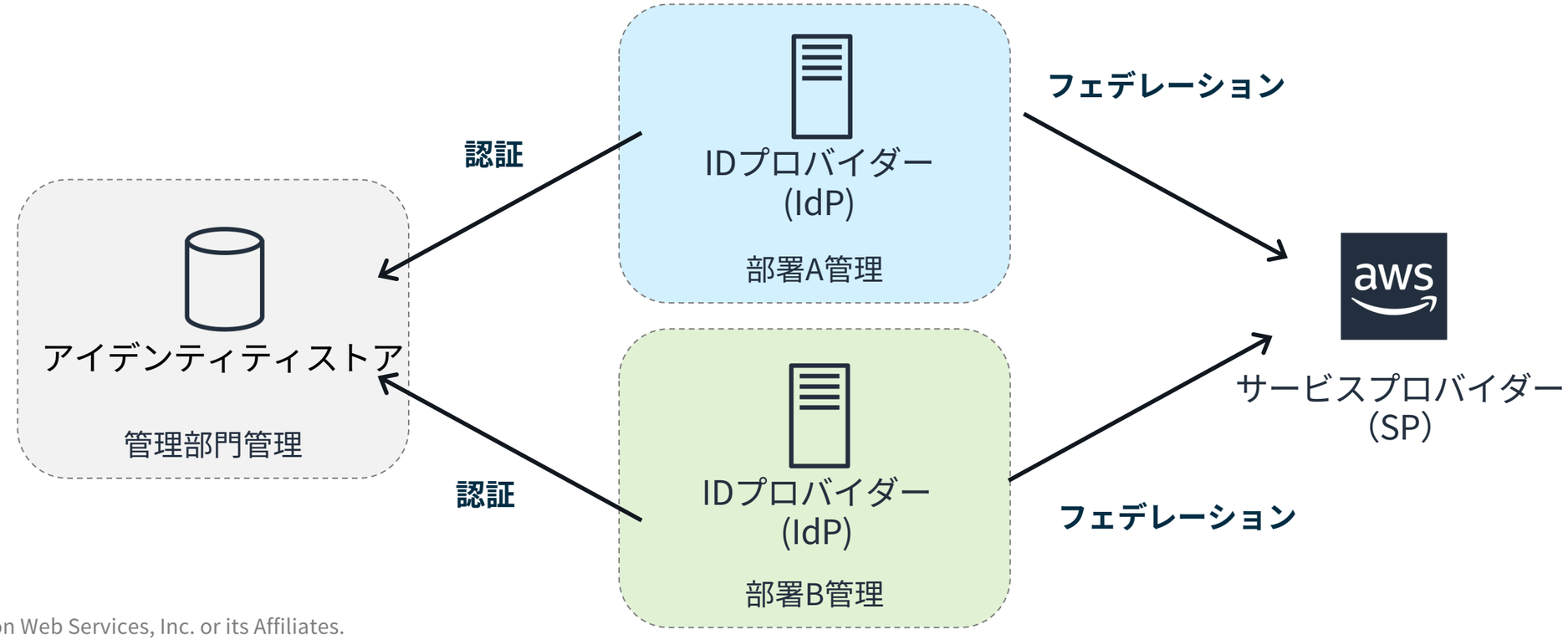
IDフェデレーションは多様な組織の要件に対応可能

- IDフェデレーションのコンポーネントは疎結合
- 各々を組み合わせることで多様な組織の要件に対応可能

たとえば、IDプロバイダー（IdP）の分割

適用シーン例

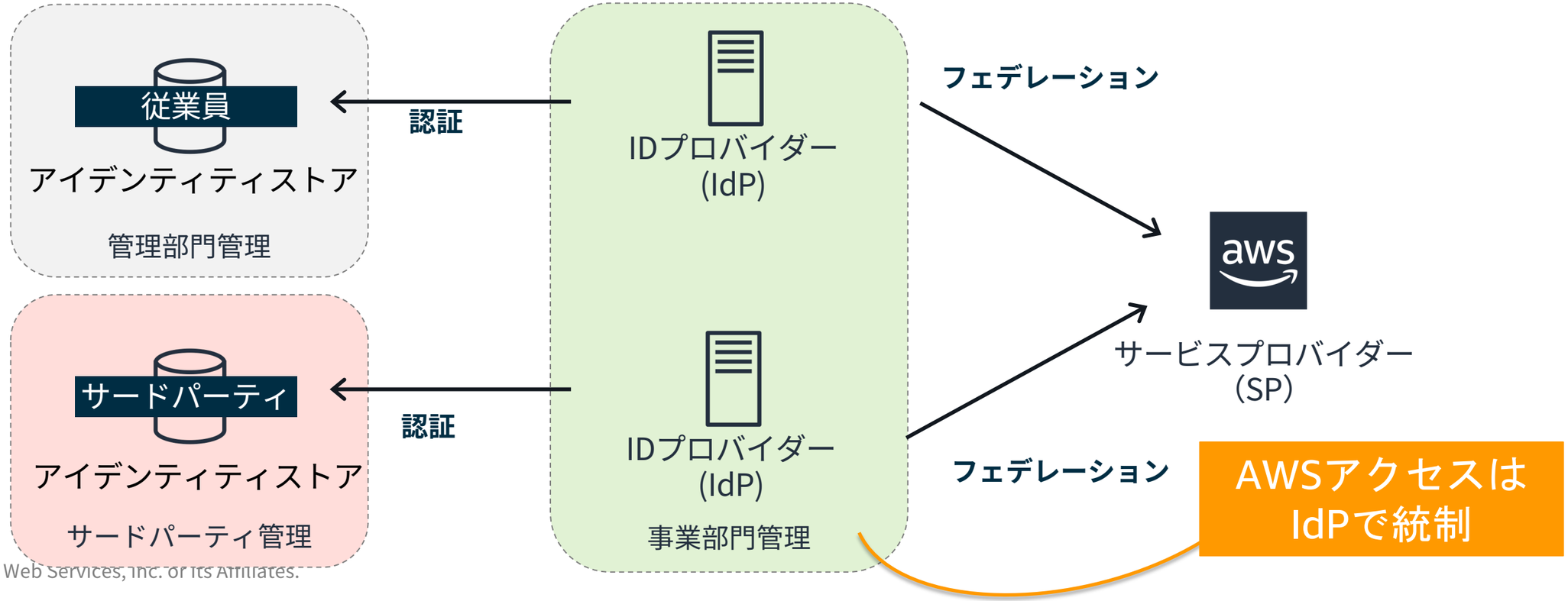
- 部署毎にIdPの管理を分割することで、部署毎の運用の柔軟性を獲得
- アイデンティティは組織で共通のものを利用



たとえば、アイデンティティストアとIDプロバイダーの分割

適用シーン例

- 人事的な職責と離れて権限を付与、たとえば組織のIDを持たないユーザー（パートナーなどのサードパーティ）に事業部門で権限を付与



シングルサインオン運用のポイント

シングルサインオン運用のよくある論点

トレーサビリティ

ロールと権限の管理

操作ログからフェデレーション前の
アイデンティティを一意に識別可能か？

AWSアカウント数とともに増加する
ロールの統制をどうすればよいのか？

操作ログの追跡は
容易かつわかりやすいか？

組織変更や兼務など、
多様なニーズにどう対応するか？

トレーサビリティ

AWS CloudTrailはフェデレーション前のIDを表示

AWS CloudTrail マネジメントコンソールでの確認

フェデレーション前のIDを取得、追跡するメカニズム

AWS CloudTrailログはRoleSessionNameをユーザー名として取り扱う

- IDプロバイダー(IdP)からSAMLアサーションにて連携される属性のひとつ
  ここにフェデレーション前のIDを含めることで追跡が容易になる
- スイッチロールにおいてトレーサビリティを簡単に実現する仕組み (※)と同一

CloudTrailログの例

```
"userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAXXXXXXXEXAMPLE: RoleSessionName ",
        "arn": "arn:aws:sts::123456789012:assumed-role/role-name/RoleSessionName ",
        "accountId": " 123456789012",
        "accessKeyId": "ASIAXXXXXXXEXAMPLE",
        (略)
```

※IAM ロールを使用して実行されたアクションを担当する ID を簡単に特定
https://aws.amazon.com/jp/about-aws/whats-new/2020/04/now-easily-identify-the-identity-responsible-for-the-actions-performed-using-iam-roles/

ロールと権限の管理

IDフェデレーションで変わる運用の論点

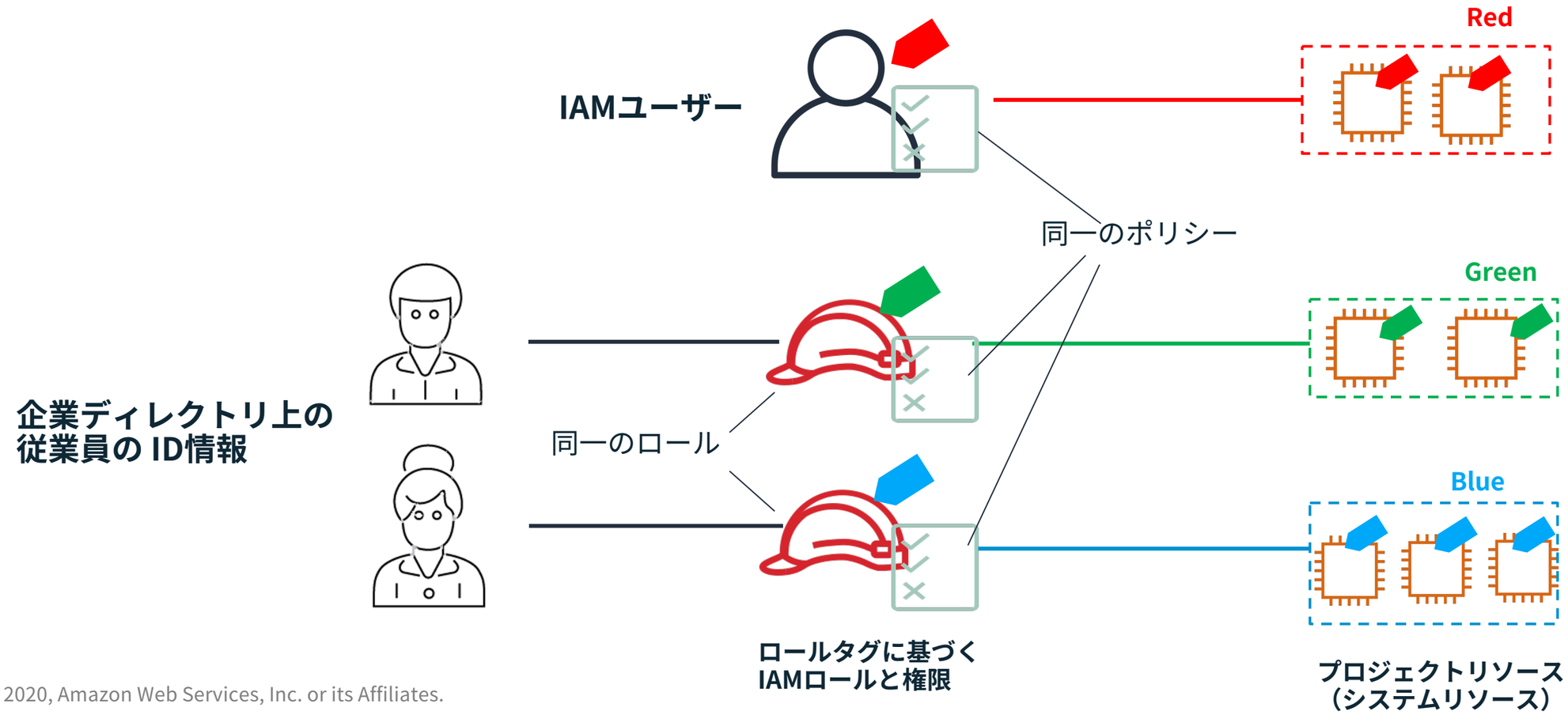
- AWSアカウント毎のアイデンティティ管理は不要となるが、代わりにフェデレーテッドユーザー向けロールの管理が必要（AWS SSOではアクセス権限セット）
- AWSアカウント数とともに管理しなければいけないロール数も増加
- ロールベースのアクセスコントロール（RBAC）では職務毎にポリシーとロールが増加しがち

新しい論点

組織変更や兼務といった多様な権限のニーズに対応しながら、ロールやポリシーの増加という、統制の妨げとなる複雑性をどのように軽減ないし解消していくか？

属性ベースのアクセスコントロール（ABAC）モデル

属性（Attribute）を利用して組織と共にスケールする権限ルールを実現する考え方、
上手く適用することでポリシーやロールの数を削減可能



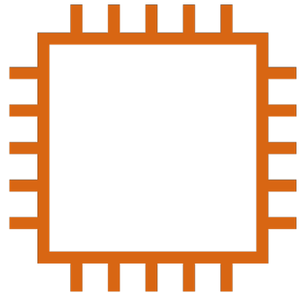
AWS 環境における属性（Attribute）とは

AWSにおける属性は、キーあるいはキーと値のペアから構成されるAWS 上のタグ

- プリンシパルタグ：アクションの主体となるユーザーやロールのタグ
- リソースタグ：アクションの操作対象となるリソースのタグ

属性の例

UserID = Bob
Team = Engineering
Project = Integration



Project = Integration
Env = Development
CreatedBy = Bob

プリンシパルタグ/リソースタグを用いたABACポリシーの例

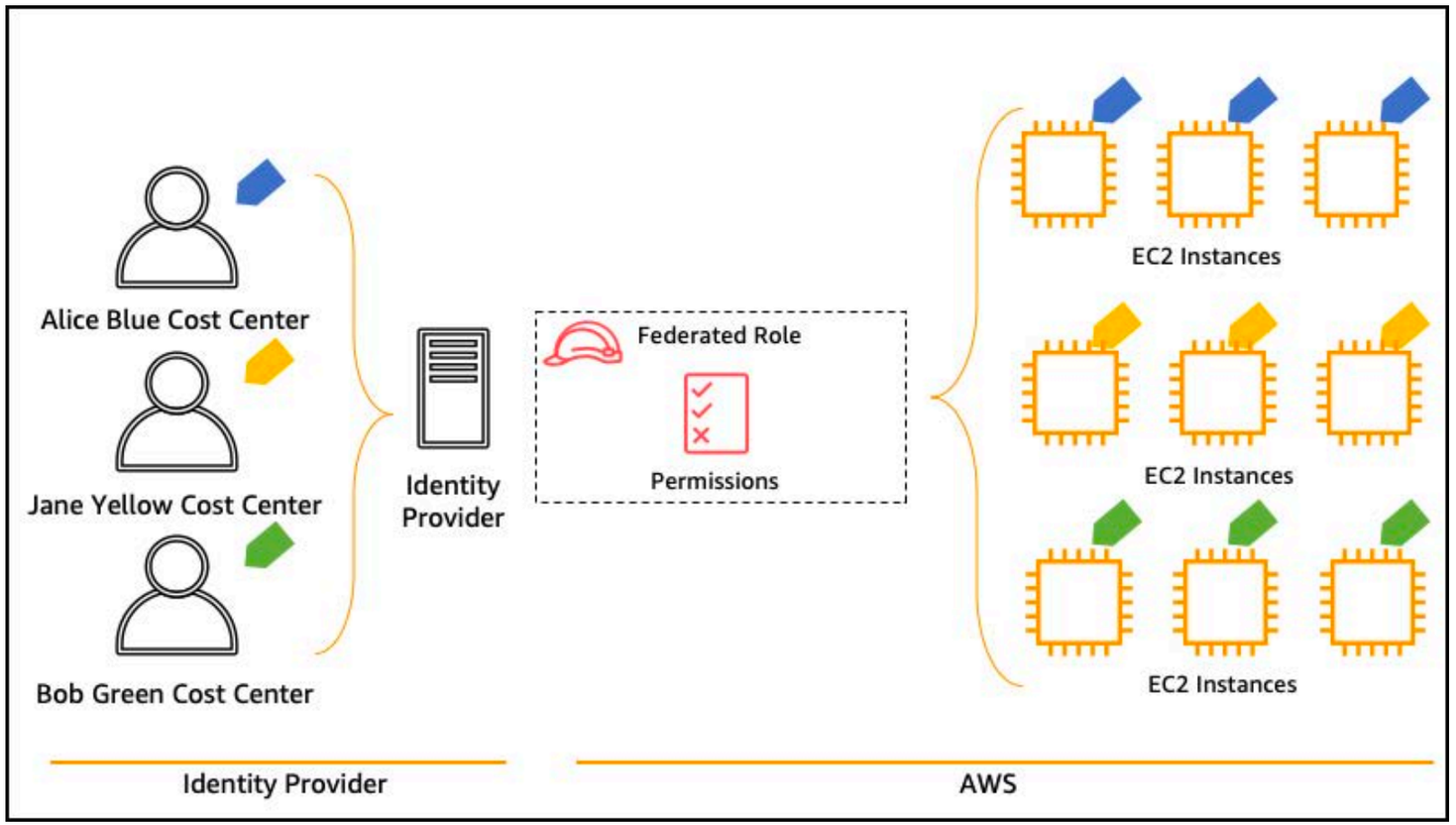
AWS Secrets Manager のポリシーの例

```
{
        "Effect": "Allow",
        "Action": [
          "secretsmanager:GetResourcePolicy",
          (途中省略)
          "secretsmanager:UpdateSecret" ],
        "Resource": "*",
        "Condition": {
          "StringEquals": {
            "secretsmanager:ResourceTag/project": "${aws:PrincipalTag/project}"
        }
 } } ] }
```

プリンシパルタグとリソースタグのProjectの値が等しいリソースのみ操作が可能

セッションタグ：ABACのIDフェデレーションへの拡張

フェデレーテッドユーザー向けロールのセッションにプリンシパルタグを付与する仕組み、 単一のロールに対し、SAMLアサーションを通じてユーザー毎/セッション毎に異なるタグ付けが可能



SAML利用時のセッションタグの受け渡し

IDプロバイダー（IdP） から AWS に送信するSAML アサーションの属性例

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:project">
                < AttributeValue >Automation<AttributeValue>
</ Attribute>
 <Attribute
Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:jobfunction">
                < AttributeValue >SystemsEngineer<AttributeValue>
</ Attribute>
```

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/TransitiveTagKeys
                < AttributeValue >project<AttributeValue>
</ Attribute>
```

属性ベースのアクセスコントロール(ABAC)適用のポイント

- ロールベースのアクセスコントロール（RBAC）との使い分けや併用を整理して適用する（＝ 二者択一ではなく適材適所）

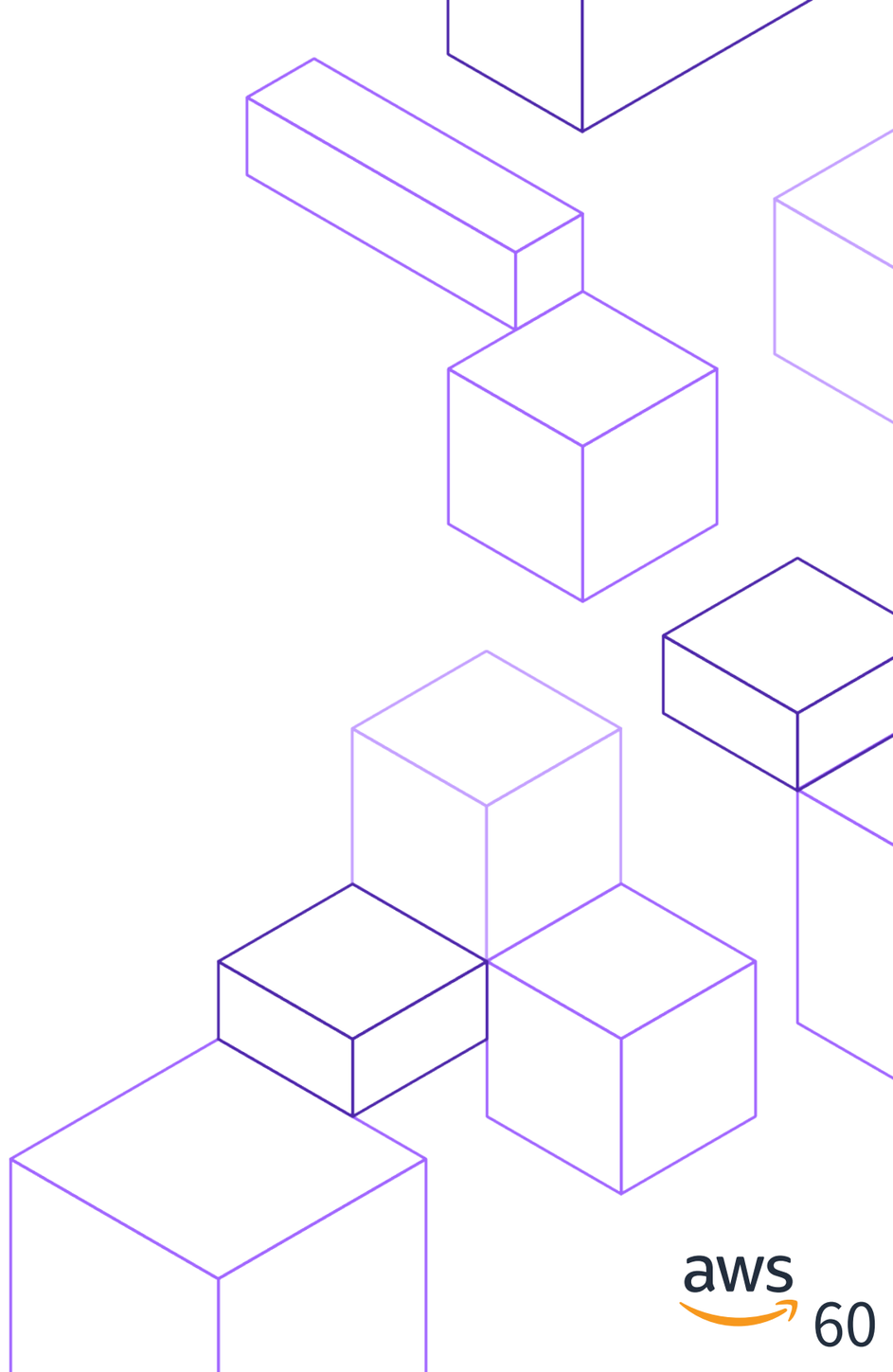
  たとえば、

  - 人事的な職責と離れて短期間で変わる権限：ABAC
  - 人事的な職責と一致する権限：RBAC

- 属性（Attribute）のないプリンシパル/リソースの考慮
  - デフォルトでは権限を付与しないFail Safeのポリシー設計が望ましい
  - IAMポリシーによる強制(※)によってタグ付けの抜けや漏れを防止できる
- タグやポリシーはシンプルさを重視し運用の煩雑化を避ける

※IAM: Create New Users Only With Specific Tags
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_iam-new-user-tag.html

まとめ



ふりかえり

シングルサインオンの構成には、 AWS Single Sign-On(SSO)や、Active Directory Federation Services(ADFS)、 外部サービスとの連携など、複数のデザインパターンがあります。

運用の違いをふまえながらシングルサインオンを構成する勘所を解説しました。

シングルサインオンを上手く適用するとアイデンティティの運用が簡素化されます。導入後の統制のしやすさ、運用のしやすさを大切な指標として設計してください。

まとめ

- シングルサインオンは煩雑なアイデンティティ管理を簡素化
- AWSではIDフェデレーションによってシングルサインオンを実現
- 適材適所の選択＆組み合わせにより、多様な組織の要件に対応可能
- AWS Single Sign-OnやABACはシングルサインオンの運用をよりシンプルにする
- シングルサインオンにおいてもトレーサビリティは維持される
- 導入のしやすさ、運用のしやすさは最も大切な設計上の指標のひとつ

Thank you!

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive