



AWS
User Groups

AWS
community
builders




20分で分かるIAM全機能

波田野 裕一

シニアアーキテクト
運用設計ラボ合同会社

Abstract



[AWS について](#) [お問い合わせ](#) [サポート](#) [日本語](#) [アカウント](#) [今すぐ無料サインアップ »](#)

[製品](#) [ソリューション](#) [料金](#) [ドキュメント](#) [学ぶ](#) [パートナーネットワーク](#) [AWS Marketplace](#) [カスタマーサポート](#) [イベント](#) [その他](#) [🔍](#)

AWS Summit Japan

[注目トピックス](#) [業界別ガイド](#) [セッション情報](#) [EXPO](#) [スポンサー](#) [AWS DeepRacer](#) [よくあるご質問](#) [無料登録する](#) [English](#)

13:00 - 13:20	20 分でわかる IAM 全機能	IAMは、AWSの全てのサービスの入口となる最も基礎的なサービスであり、AWSエンジニアには欠かせない教養であると言えます。比較的枯れたサービスでもあるIAMは学習コスパの良いサービスでもあります。早期にIAMの全体像を理解して、20年先も活躍できるAWSエンジニアを目指しましょう。	AWS Community HERO 波田野 裕一 氏
---------------	------------------	--	--------------------------------

「20分で分かる」は、セッションが20分だからです。
この資料を読めば誰でも20分で理解できる、という意味ではないです。

おことわり

本資料は、Amazon Web Servicesのテクニカルレビューを経っていますが
発表者独自の観点および分類により作成しています。

一次情報として、必ずAWS公式ドキュメントをご参照ください。

<https://aws.amazon.com/jp/iam/>

Agenda

- ・ IAMの概要
- ・ IAMの基本構造
- ・ IAMの全機能
- ・ IAMの重要ポイントと「まとめ」



この発表の見方

今回の発表を聞いて、AWS IAMについて
「どんなことができるか」「どんなことができないか」
を把握してください。

サービスの限界を把握したら、
あとは公式ドキュメントを読みながら実践するのみです。

IAMの概要

IAMの概要

AWS IAM (Identity and Access Management)



IDとAWSのサービス・リソースへのアクセスを安全に管理

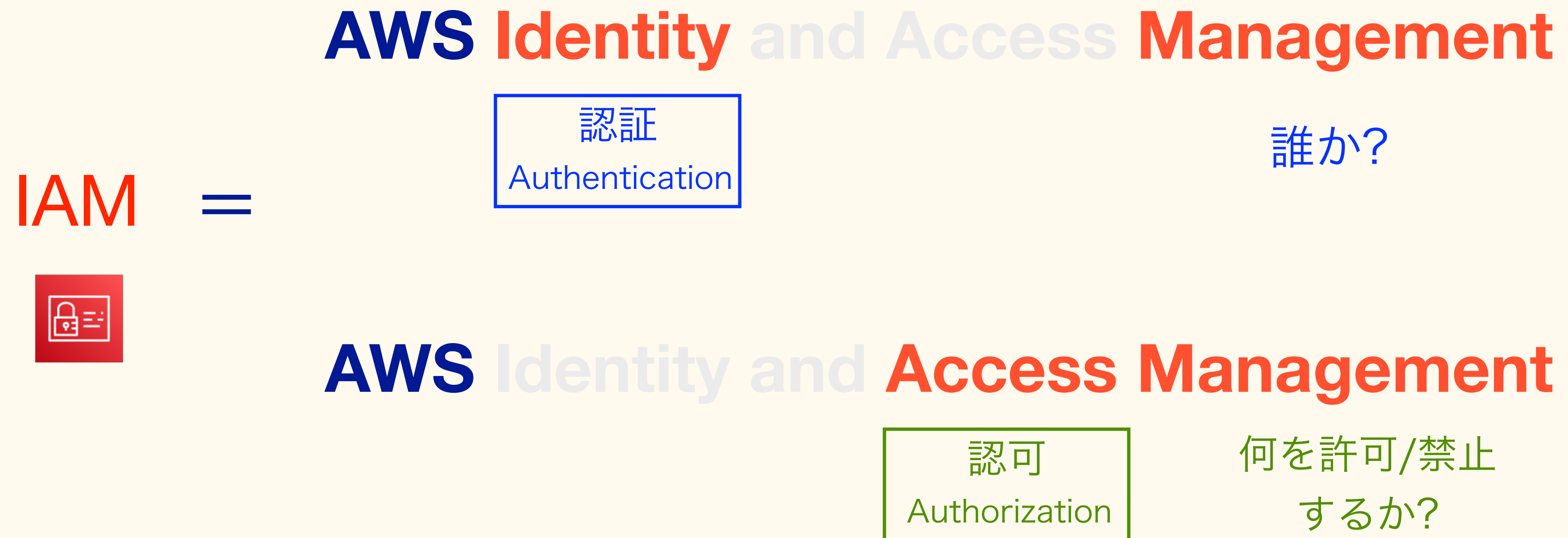
きめ細かいアクセス制御を
設定・管理

AWSアカウントのID管理

一時的なセキュリティ認証情報の付与

継続的にアクセスを分析

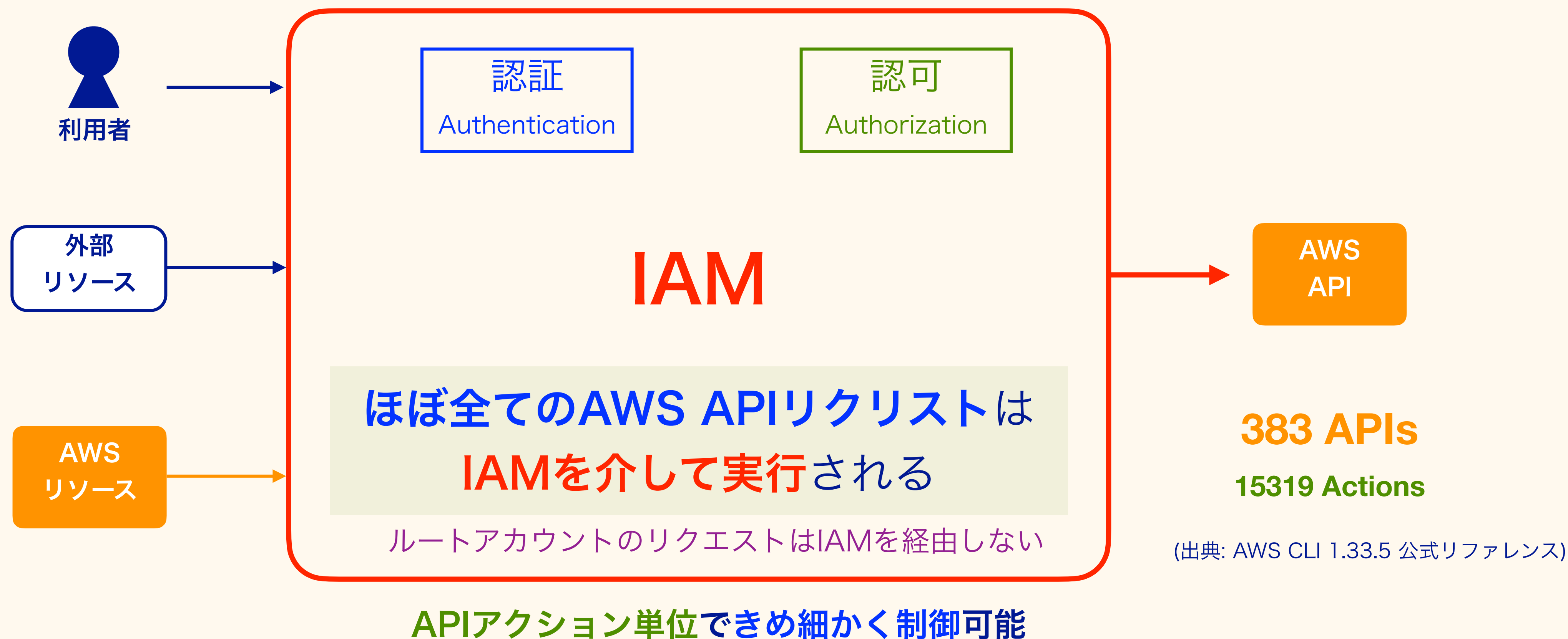
IAMの役割



IAMは、AWSの認証・認可の管理という重要な役割を担う。

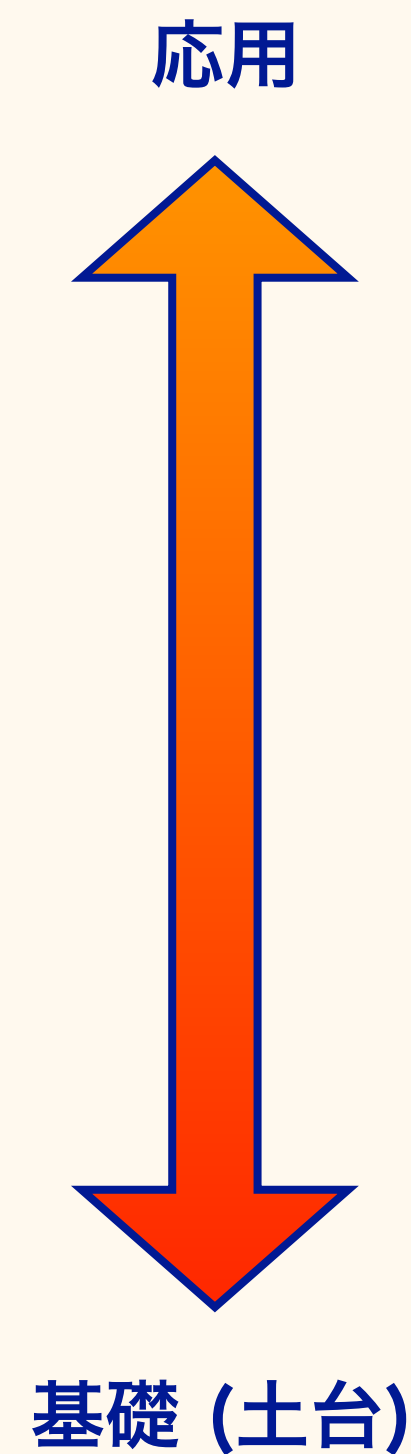
IAMはAWS APIのアクセス制御基盤

IAMはAWS APIへのアクセス制御基盤



AWSにおけるIAMの位置付け

IAMは、AWSの学習や実務における、最も重要な土台というべきサービス



AWSの各サービスの知識

IAMの知識

IAM利用は無料
追加料金なしで利用できる

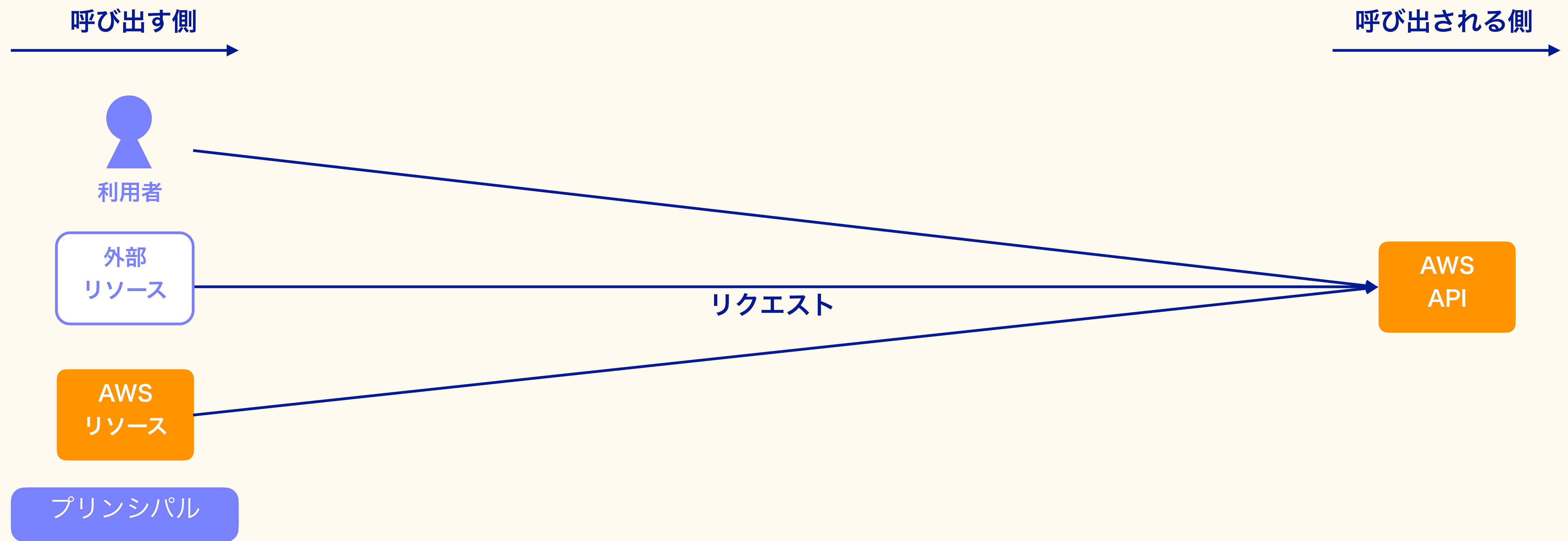
つまり...

「IAMがわからない」ということは
「AWSの基礎をわかってない」ということ

IAMの基本構造

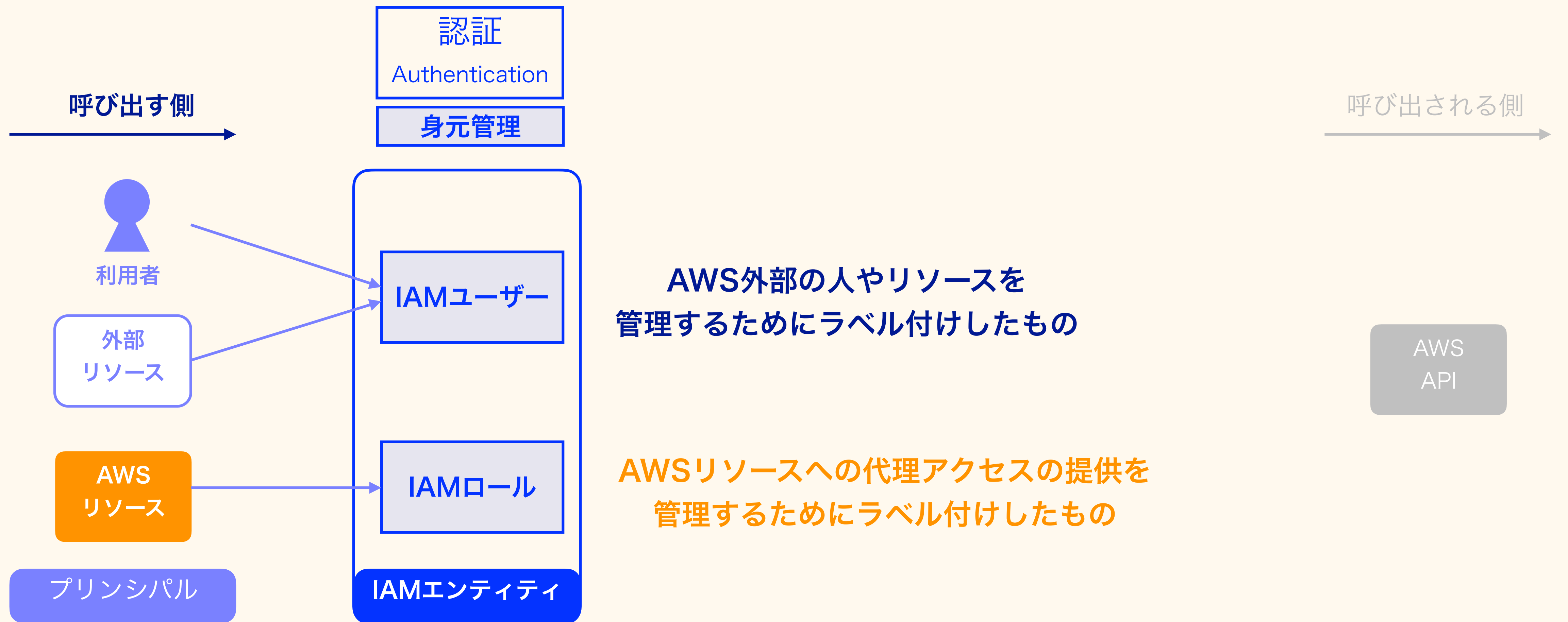
IAMにおける「プリンシパル」

AWSサービスにリクエストを行う、呼び出し側のことを「プリンシパル」と言います。



IAMにおける「エンティティ」

IAM管理のためにプリンシパルにラベル付けしたものを「IAMエンティティ^{実体}」と言います。



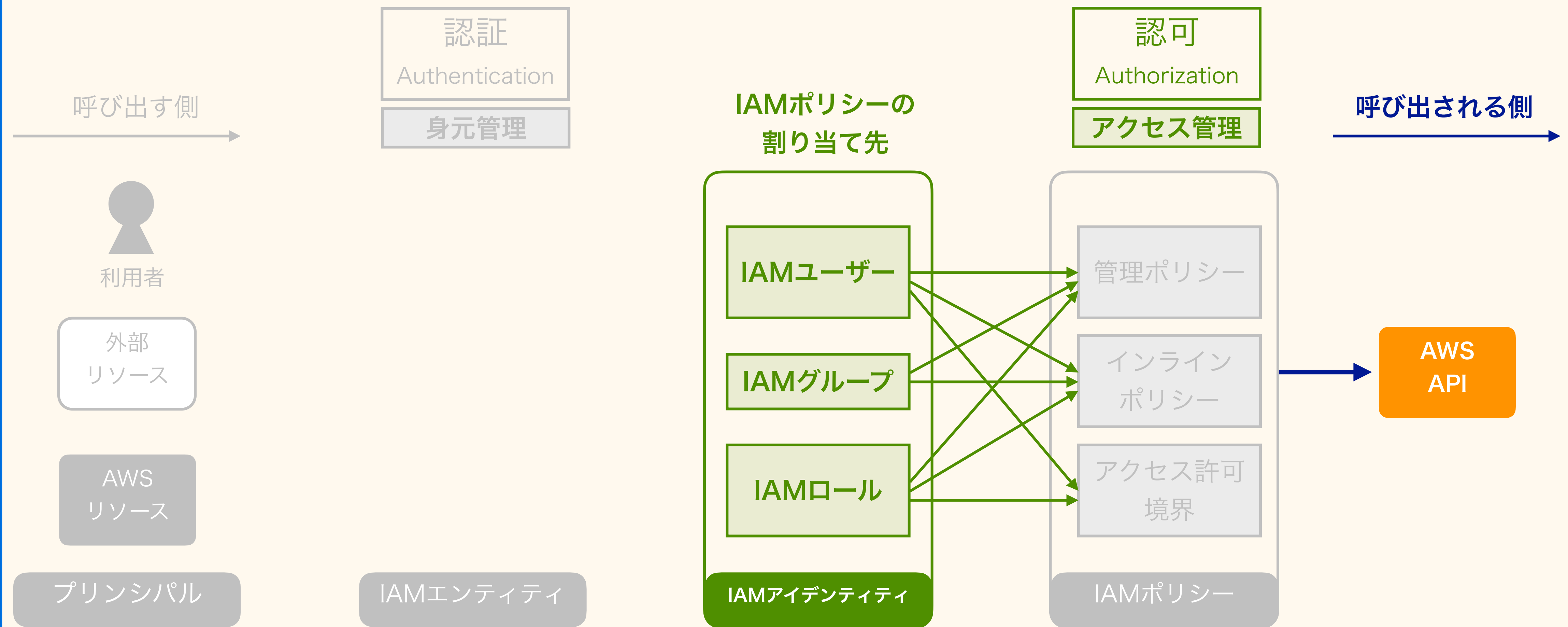
IAMにおける「ポリシー」

リクエストをIAMで許可/拒否するルールのことを「IAMポリシー」と言います。



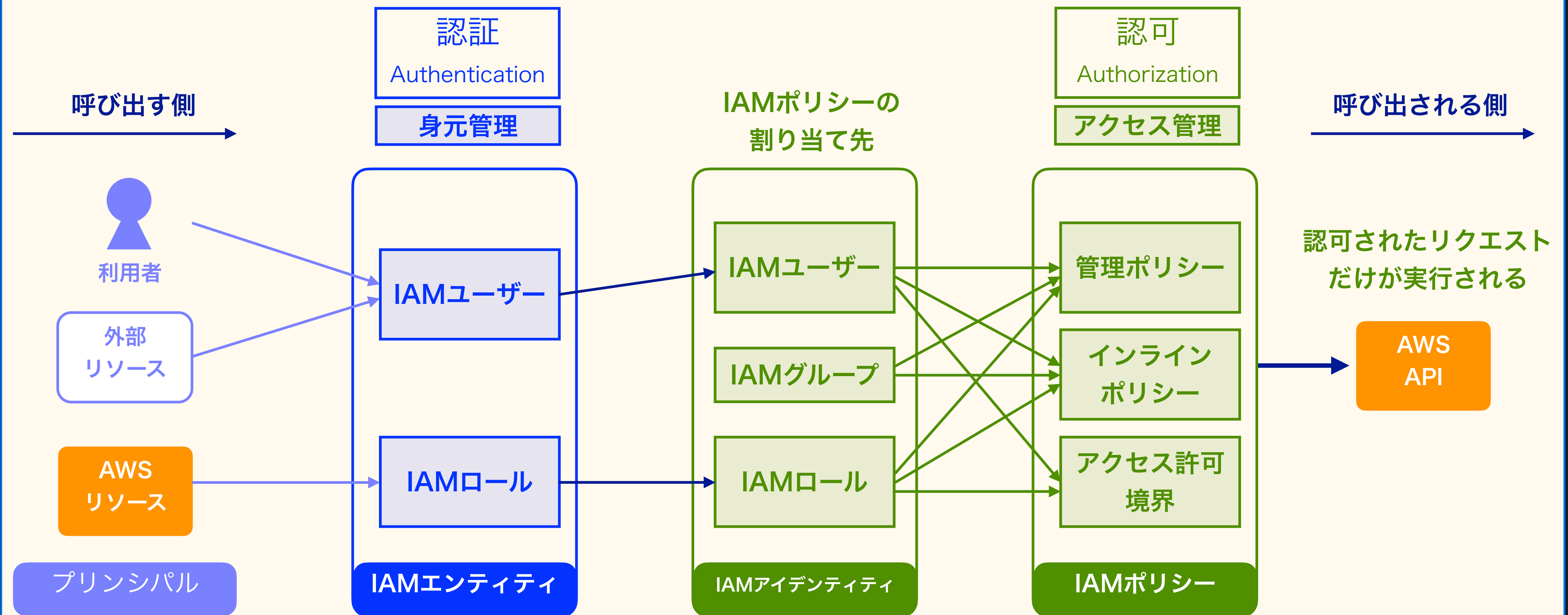
IAMにおける「アイデンティティ」

識別子
IAMポリシーの割り当て先のことを「IAMアイデンティティ」と言います。



IAMの基本構造

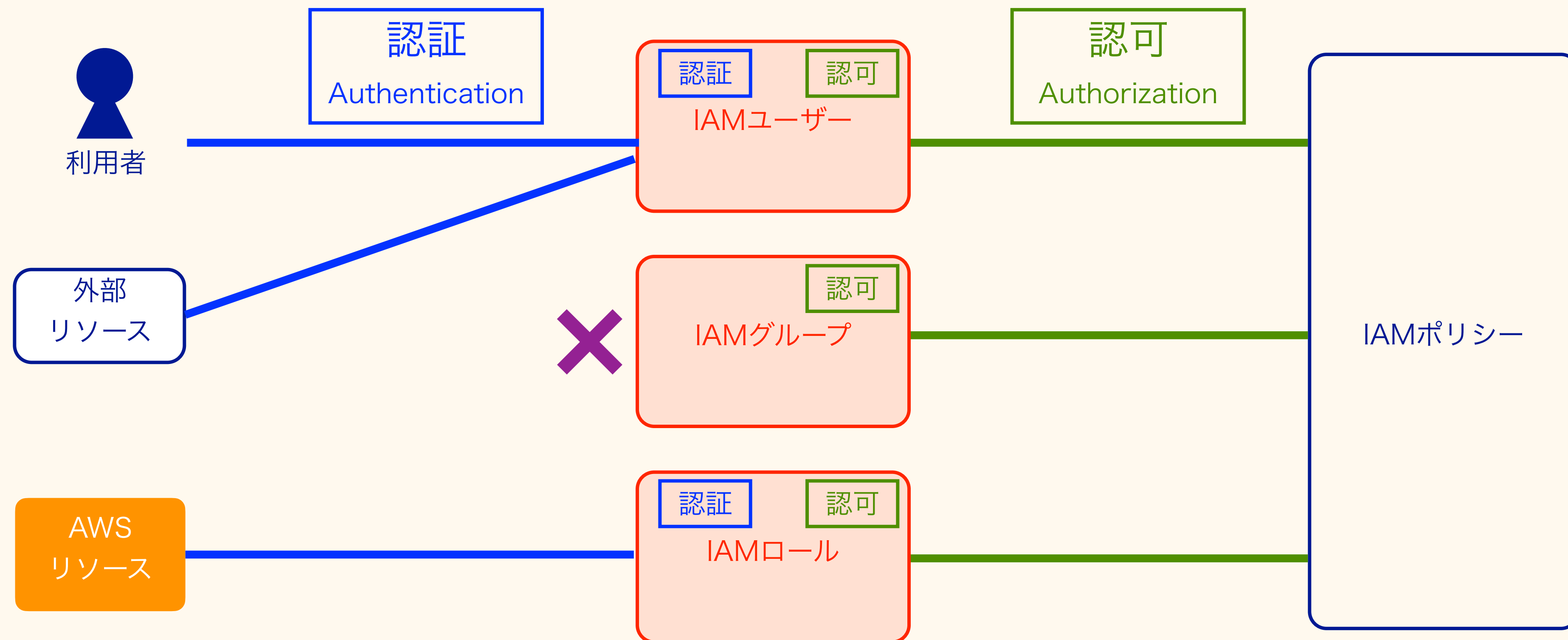
公式ドキュメントを正確に読み取るために、正しく理解しておきましょう。



参考: IAMエンティティとIAMアイデンティティの区別

プリンシパルと紐付くのが
IAMエンティティ(実体)

IAMポリシーと紐付くのが
IAMアイデンティティ(識別子)



余談: APIにも混乱がある

ListEntitiesForPolicyアクションでは、IAMアイデンティティが扱われる。

Parameter

EntityFilter

The entity type to use for filtering the results.

For example, when `EntityFilter` is `Role`, only the roles that are attached to the specified policy are returned. This parameter is optional. If it is not included, all attached entities (users, groups, and roles) are returned. The argument for this parameter must be one of the valid values listed below.

Type: String グループはIAMエンティティではない

Valid Values: `User` | `Role` | `Group` | `LocalManagedPolicy` | `AWSManagedPolicy`

Required: No

仕様バグなのか、特に意味をなさないパラメータ

Response

PolicyGroups.member.N

A list of IAM groups that the policy is attached to.

Type: Array of `PolicyGroup` objects

グループはIAMエンティティではない

PolicyRoles.member.N

A list of IAM roles that the policy is attached to.

Type: Array of `PolicyRole` objects

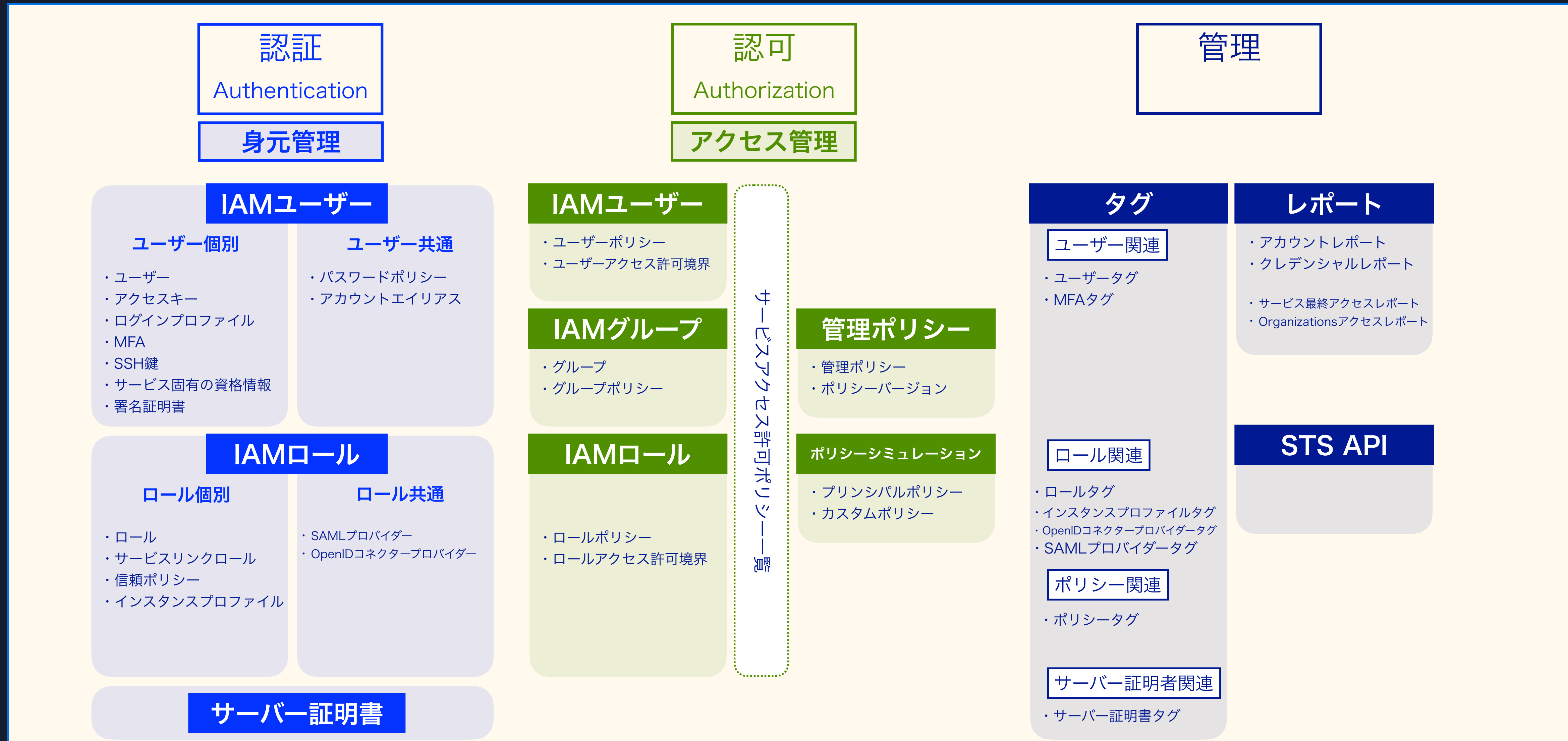
PolicyUsers.member.N

A list of IAM users that the policy is attached to.

Type: Array of `PolicyUser` objects

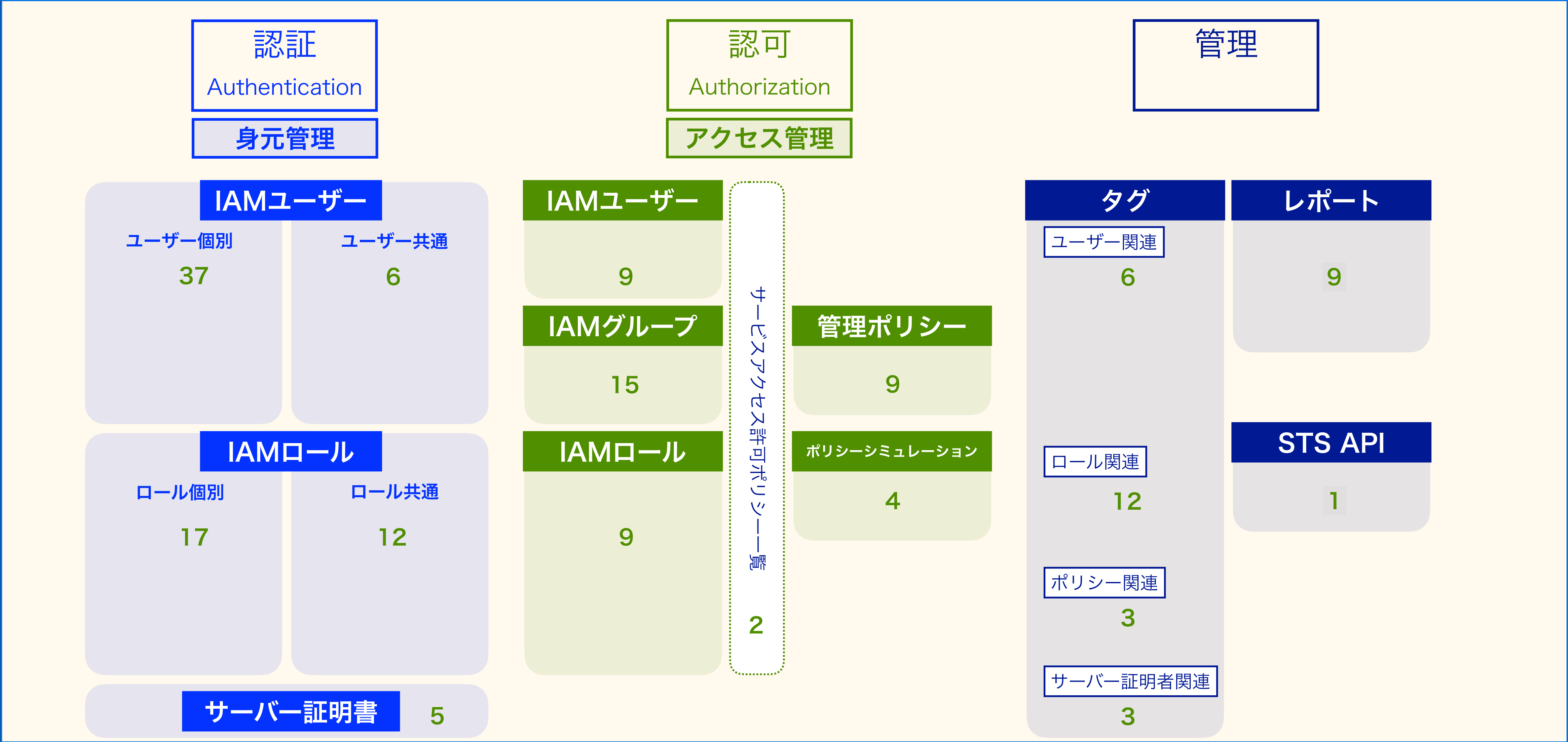
正確には、ListIdentitiesForPolicyアクションなのでは？

IAM APIの全機能マップ



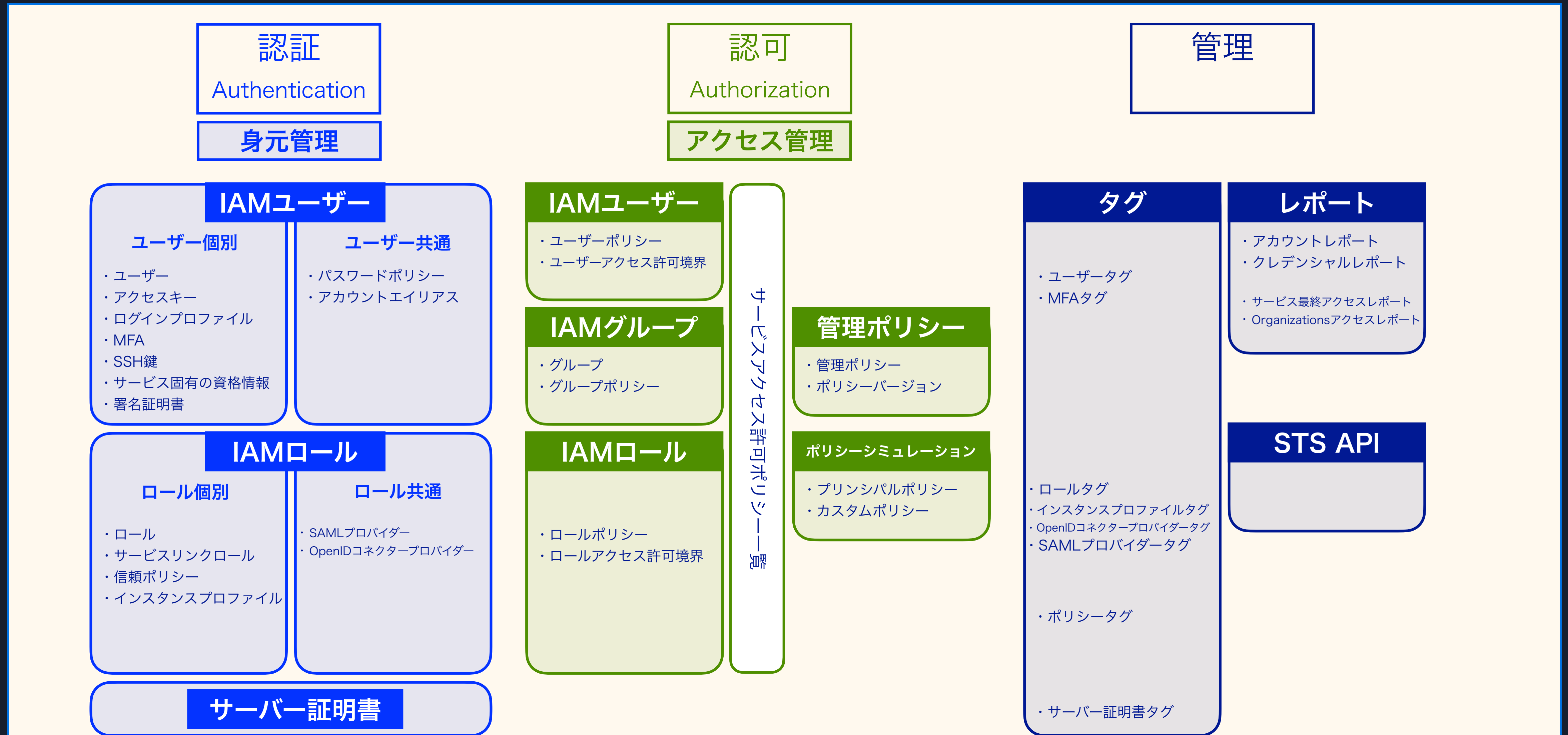
IAM APIアクション数マップ

159アクション



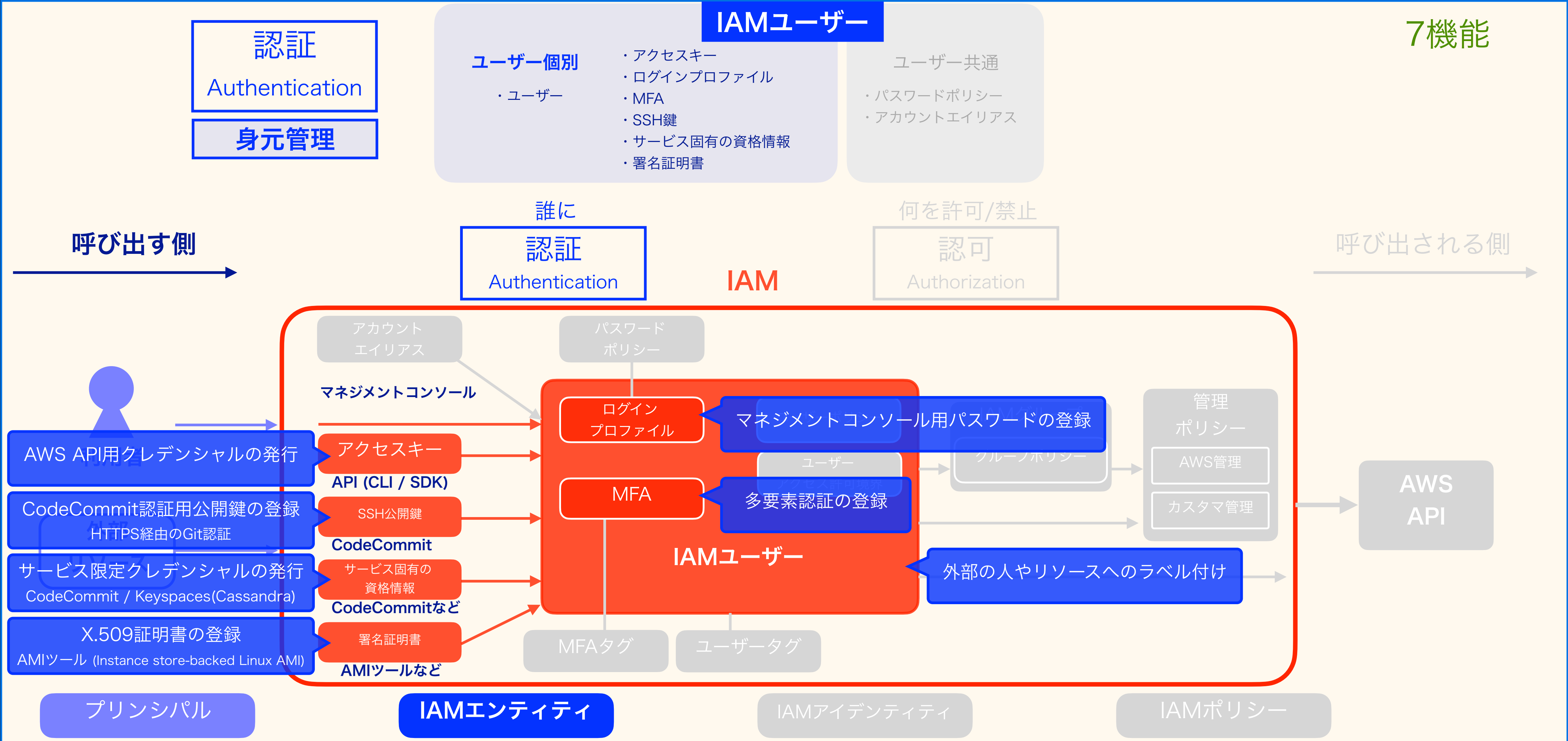
IAMの全機能

IAM APIの全機能マップ (14の機能領域 40の機能)

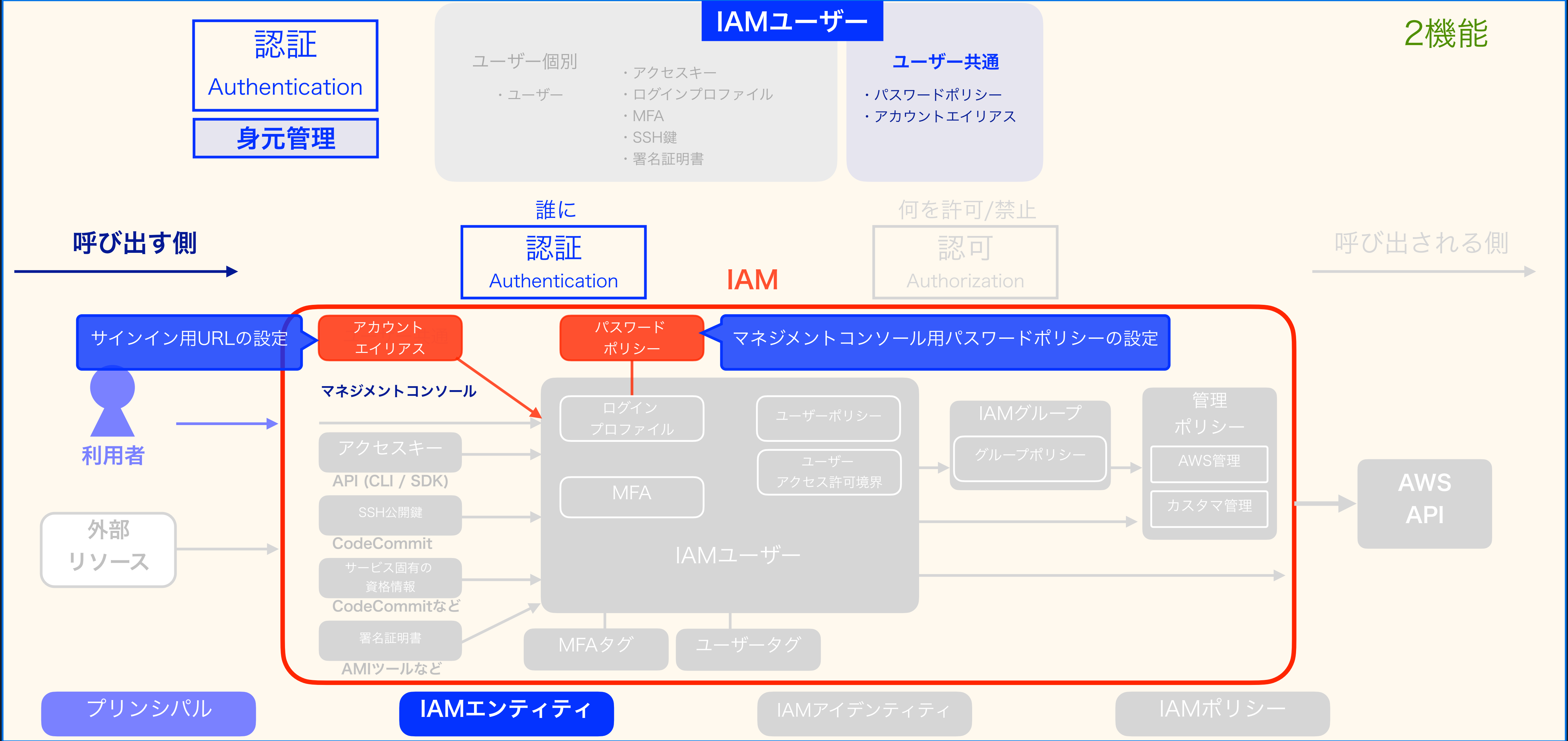


IAMの全機能 (認証)

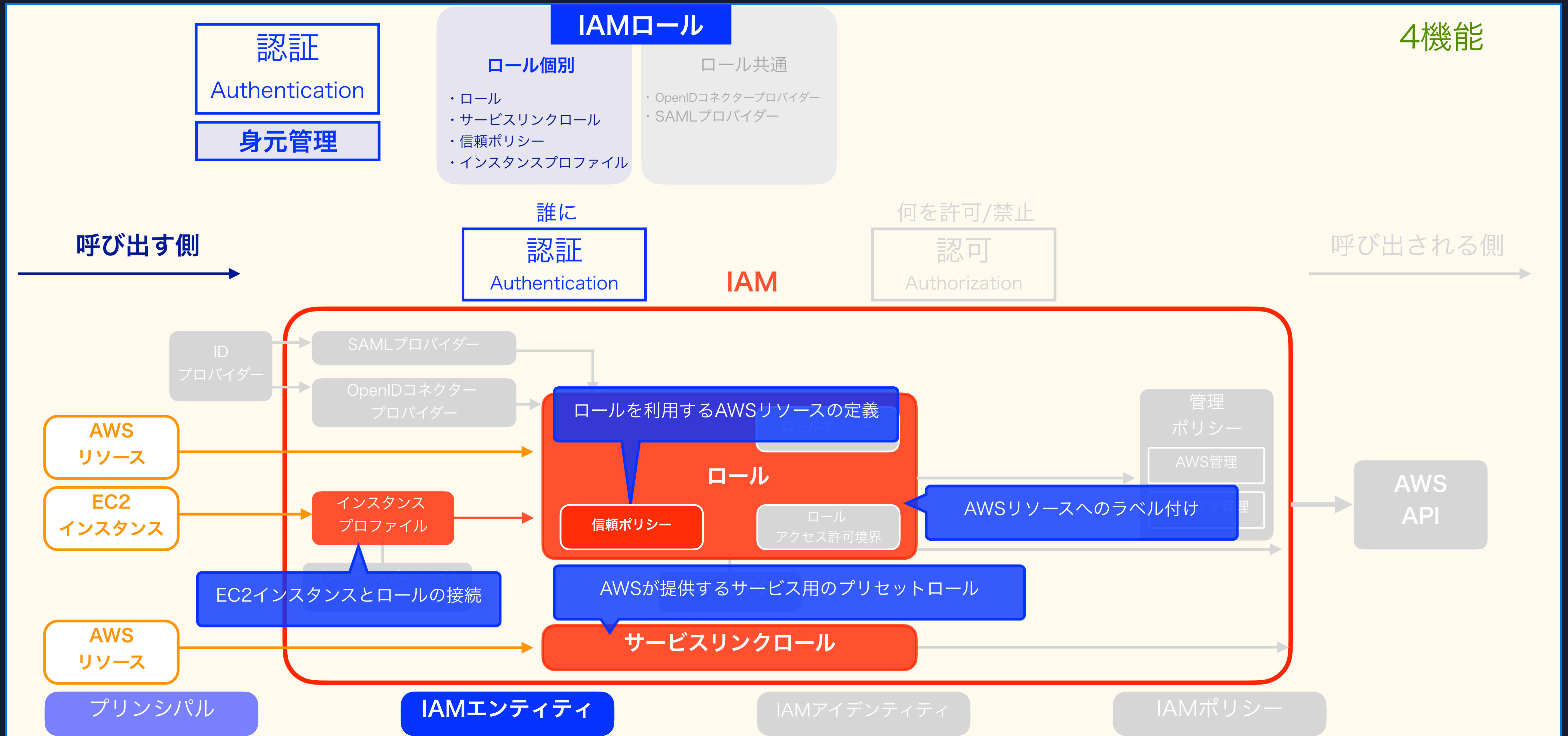
IAMの全機能 (認証: IAMユーザー 個別)



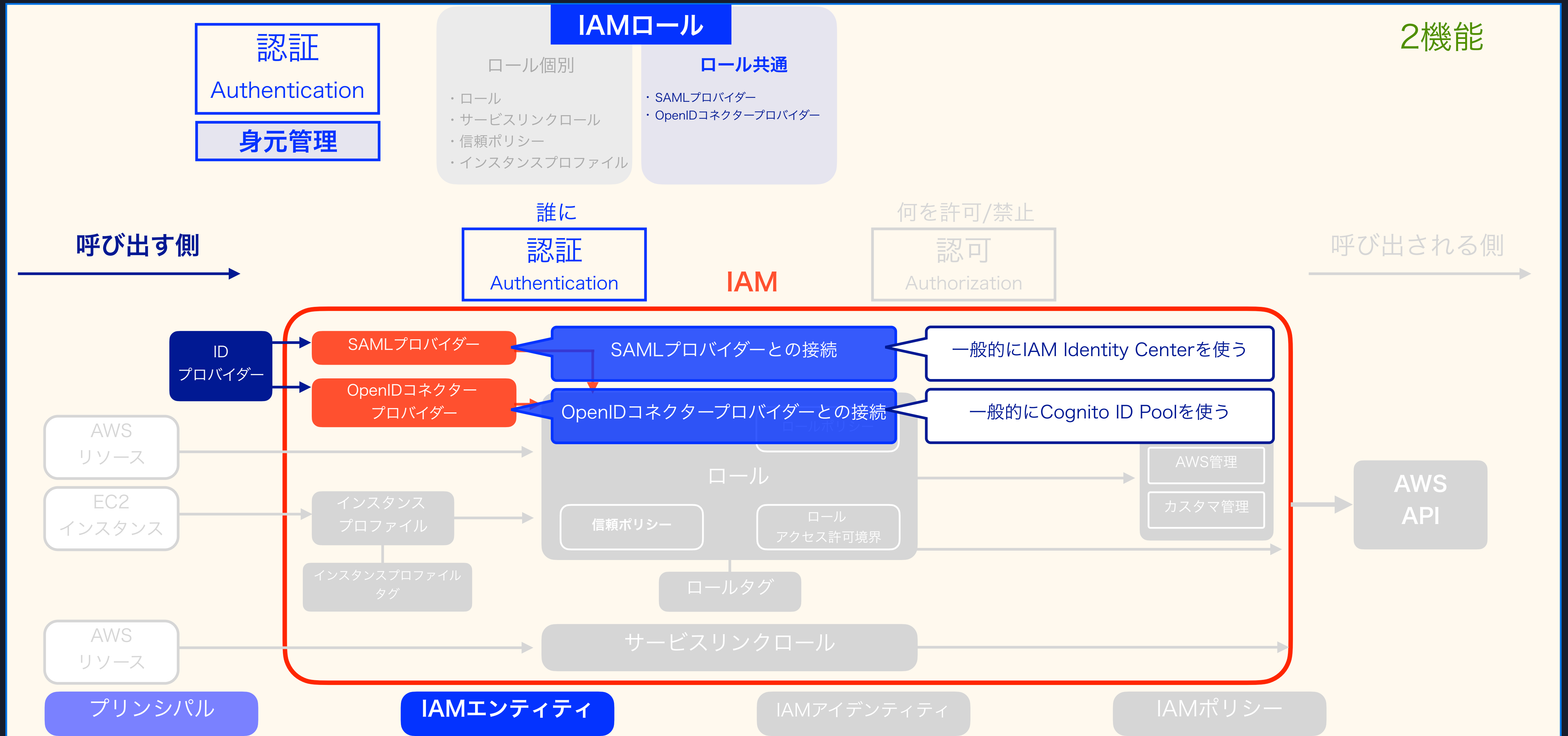
IAMの全機能 (認証: IAMユーザー 共通)



IAMの全機能 (認証: IAMロール 個別)



IAMの全機能 (認証: IAMロール 共通)



IAMの全機能 (認証: サーバー証明書)

認証

Authentication

身元管理

1 機能

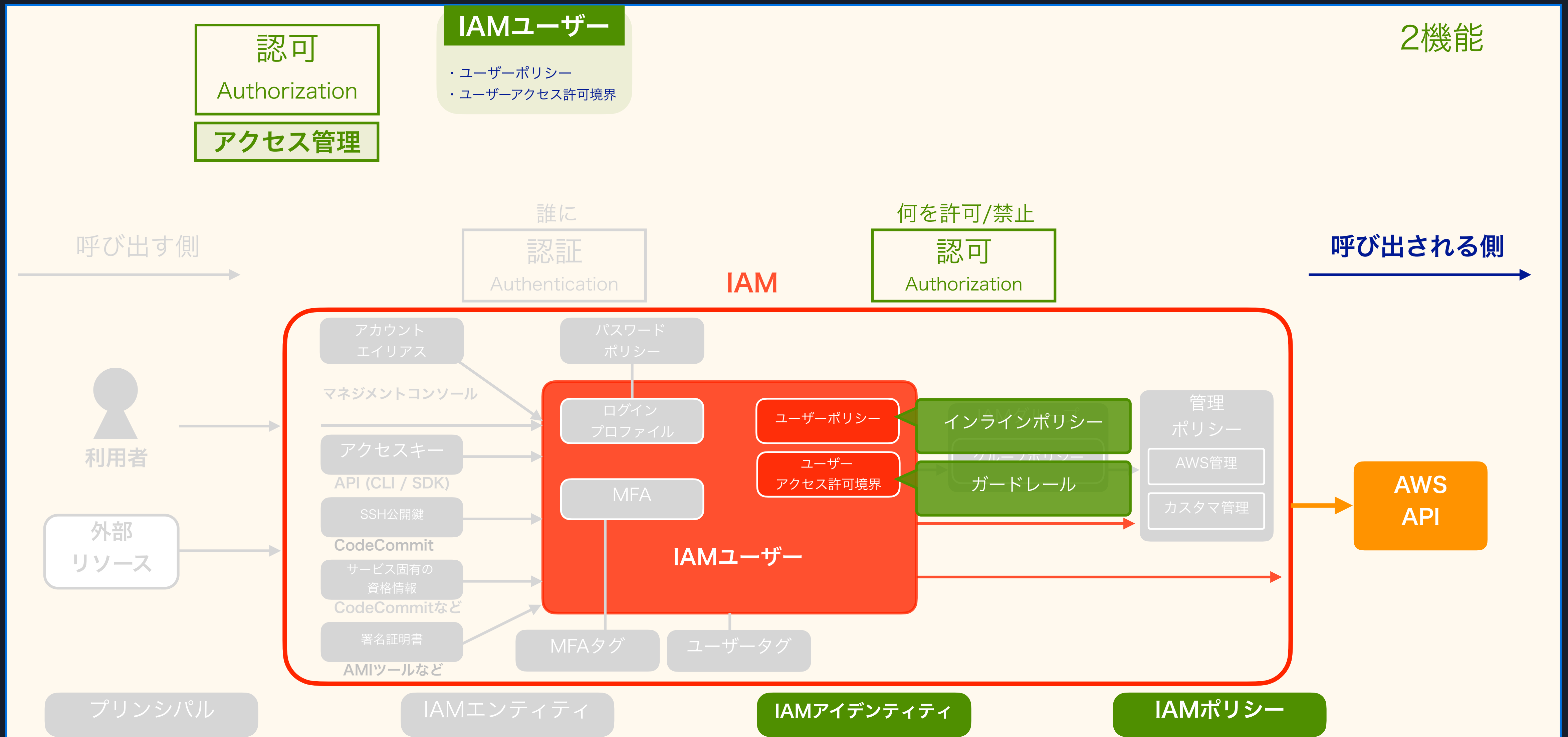
サーバー証明書

- ・ X.509証明書をアップロードできる。
- ・ CloudFrontやELBでSSL証明書として利用できる。

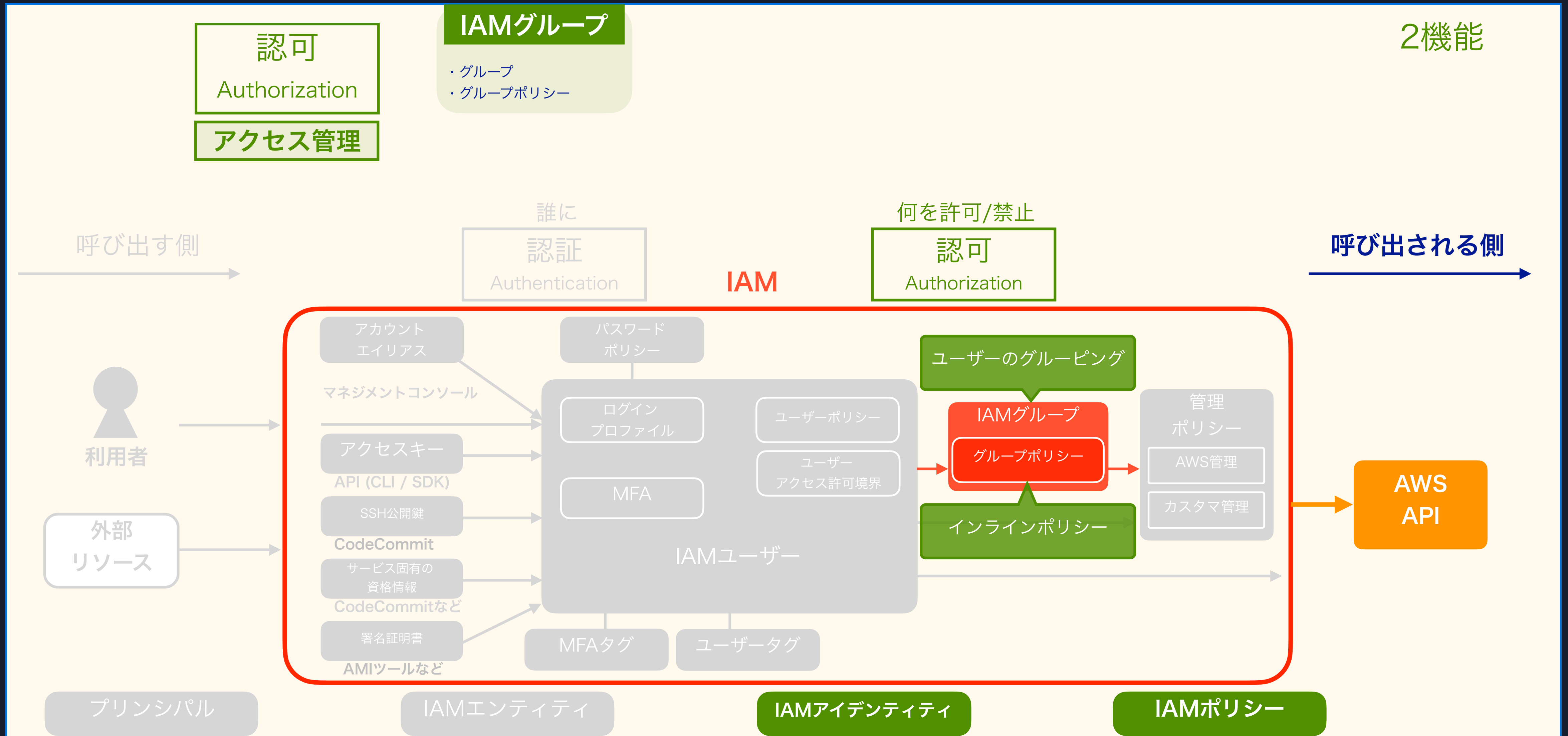
Certificate Manager(ACM)が提供されているリージョンでは
ACMの利用を推奨

IAMの全機能 (認可)

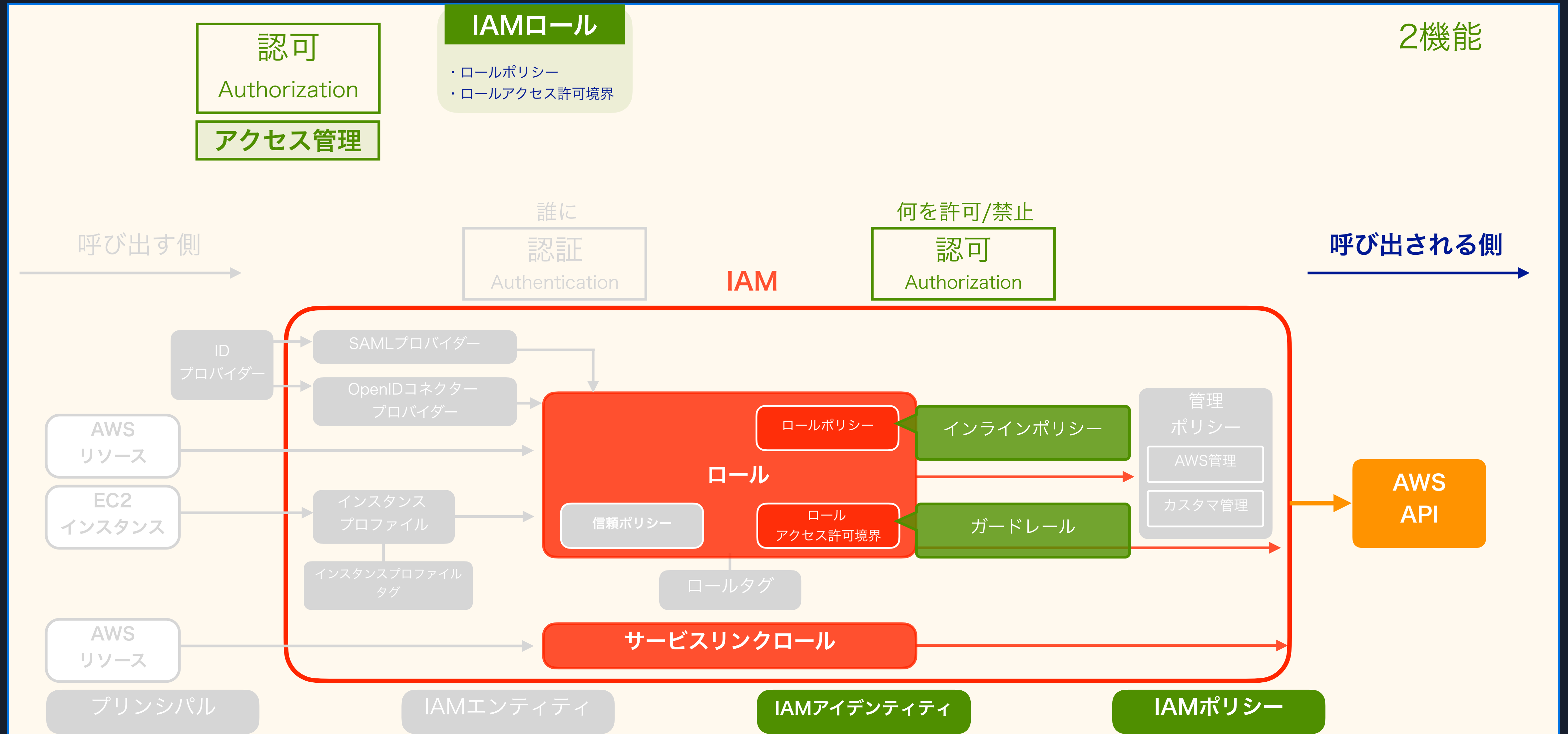
IAMの全機能 (認可: IAMユーザー)



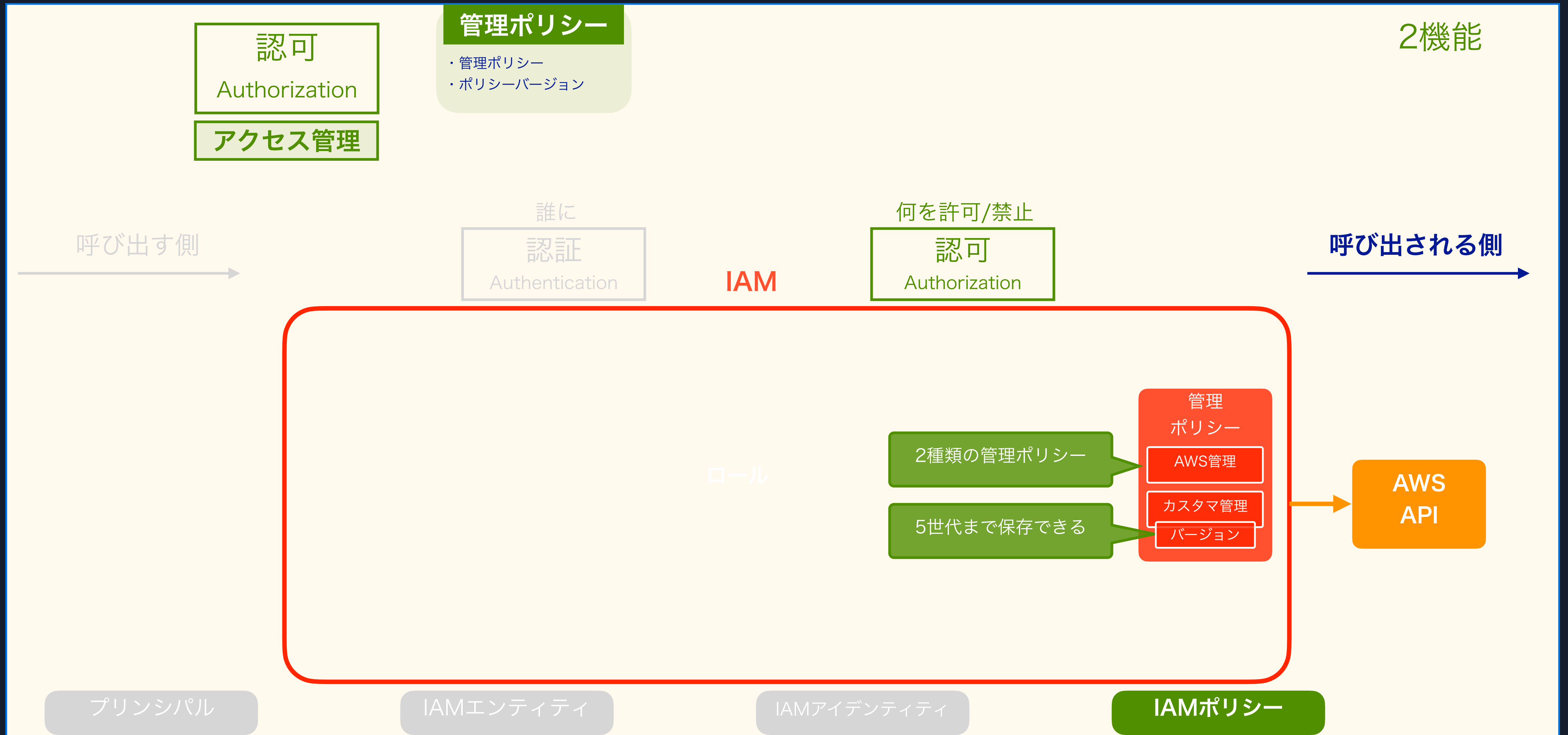
IAMの全機能 (認可: IAMグループ)



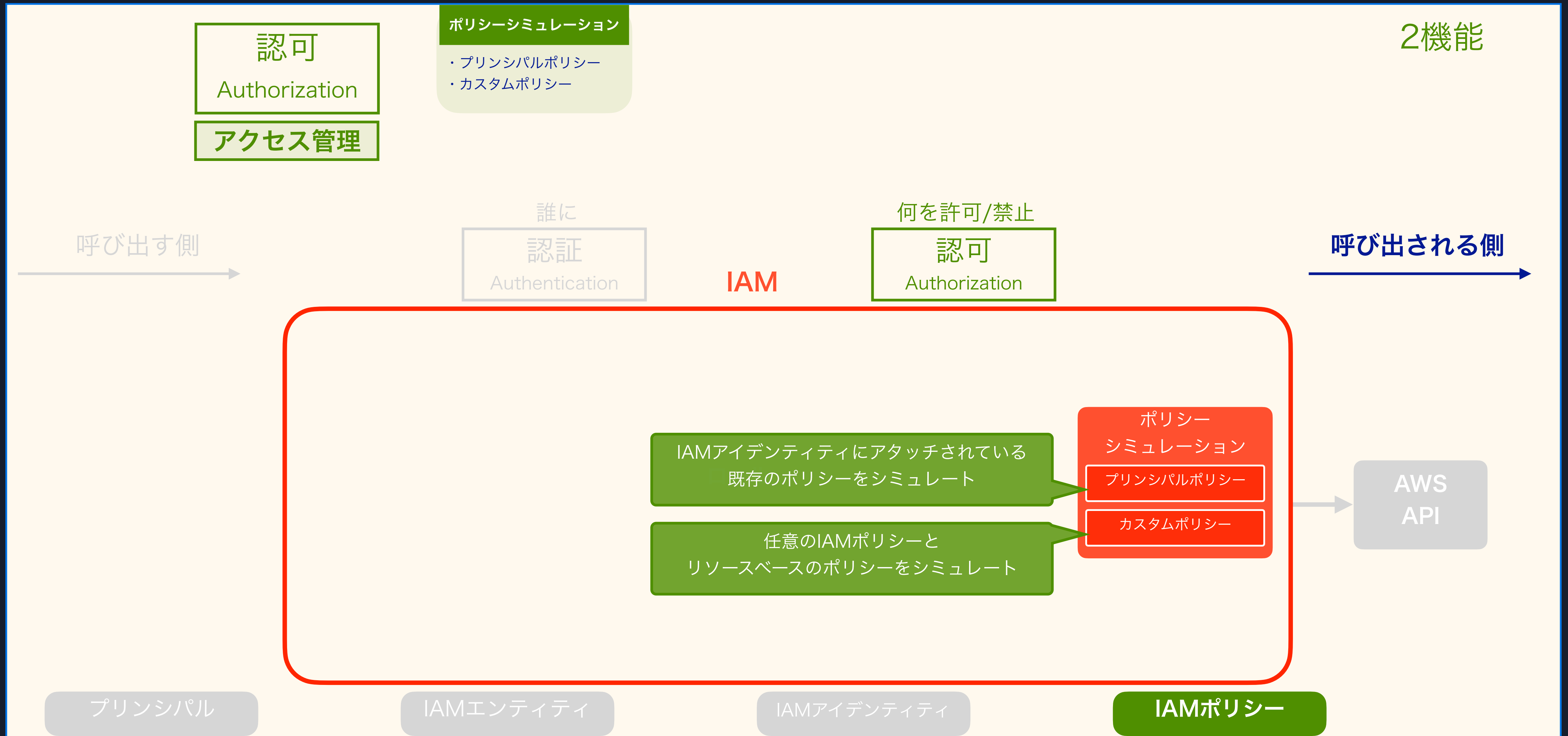
IAMの全機能 (認可: IAMロール)



IAMの全機能 (認可: 管理ポリシー)



IAMの全機能 (認可: ポリシーシミュレーション)



IAMの全機能 (認可: サービスアクセス許可ポリシー一覧)

1 機能

認可

Authorization

アクセス管理

サービスアクセス許可ポリシー一覧

指定されたサービスにアクセスするために
IAMアイデンティティが使用できるポリシーのリスト取得

IAMの全機能 (管理)

IAMの全機能 (管理: タグ)

8機能

管理

マネジメントコンソール

タグは表示されず、フィルターに使えない。

AWS CLI

一覧表示にタグが表示されないものが多い。

ユーザーとロールは、仕様上は一覧に表示されることになっているが、(一時的?)に表示されない。
ポリシーとインスタンスプロファイルは、一覧に表示される仕様。
他の4種類のタグは、一覧に表示されない仕様。

注意点

ユーザーとロールのタグはキーも値も、大文字小文字を区別しない。

他の6種類のタグは、キーも値も、大文字小文字を区別する。(混乱を避けるためのルールが必要)

IAMのタグはリソース管理には、使い勝手が悪いが...

ABAC (属性ベースアクセス制御)

重要

ポリシーの条件句で、特定のタグと値を条件にすることができる。

(例) Env=Devのタグが付いている場合は、アクションを許可する、など。

タグ

ユーザー関連

- ・ユーザータグ
- ・MFAタグ

ロール関連

- ・ロールタグ
- ・インスタンスプロファイルタグ
- ・OpenIDコネクタプロバイダータグ
- ・SAMLプロバイダータグ

ポリシー関連

- ・ポリシータグ

サーバー証明者関連

- ・サーバー証明書タグ

IAMの全機能 (管理: レポート)

4機能

管理

レポート

- ・ アカウントレポート
- ・ クレデンシャルレポート
- ・ サービス最終アクセスレポート
- ・ Organizationsアクセスレポート

IAMエンティティの使用状況、IAMのクォータに関する情報、すべてのIAMアイデンティティ、ポリシーに関する情報などの取得

AWSアカウントの認証情報レポートの生成・取得

AWSサービスへのアクセス試行でIAMリソースが最後に使われたときの詳細を含むレポートの生成・取得

Organizationsのサービスの最終アクセスデータのレポートの生成・取得

IAMの全機能 (管理: STS API)

管理

1 機能

STS APIグローバルエンドポイントのトークンバージョンの設定

STS API

グローバルエンドポイント

<https://sts.amazonaws.com>

v1Token 非オプトインリージョンのみで利用可能

v2Token 全リージョンで利用可能。(トークンが長い)

STS API

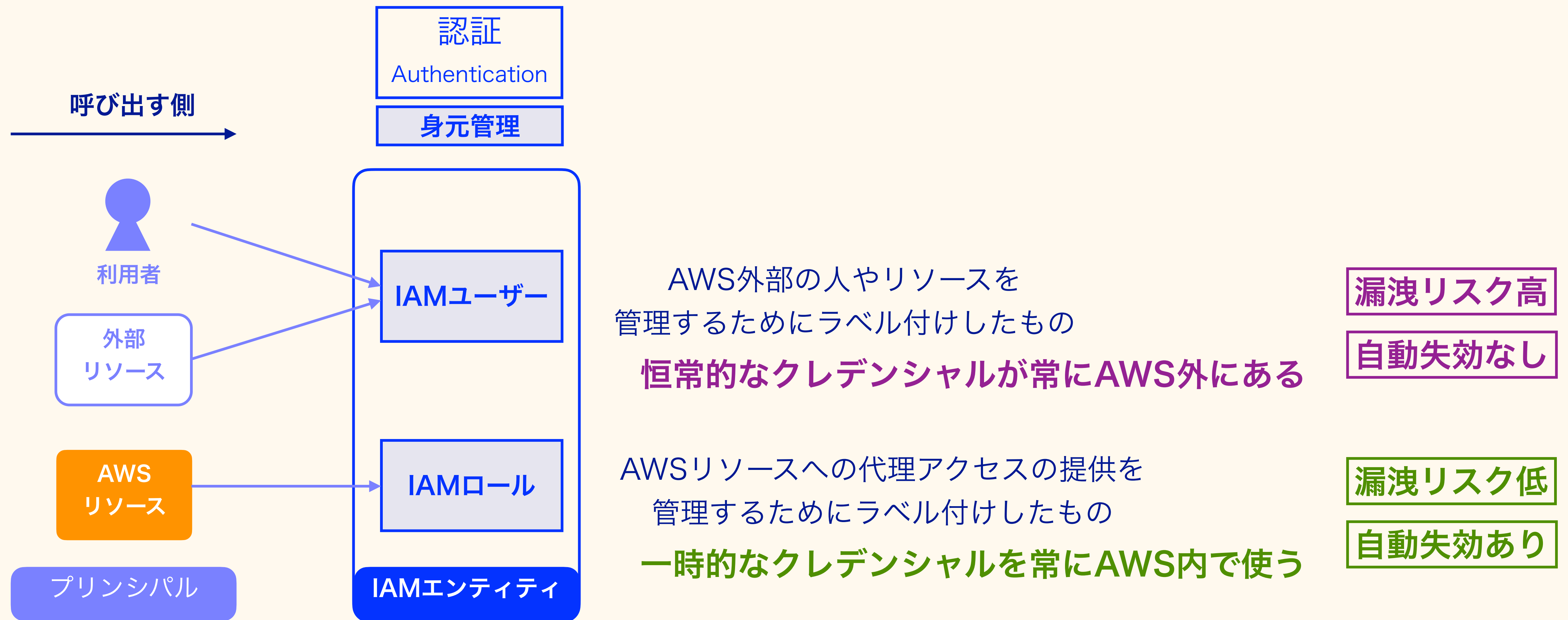
リージョンエンドポイント

[https://sts.\\${リージョン}.amazonaws.com](https://sts.${リージョン}.amazonaws.com)

「IAMの重要ポイント」と「まとめ」

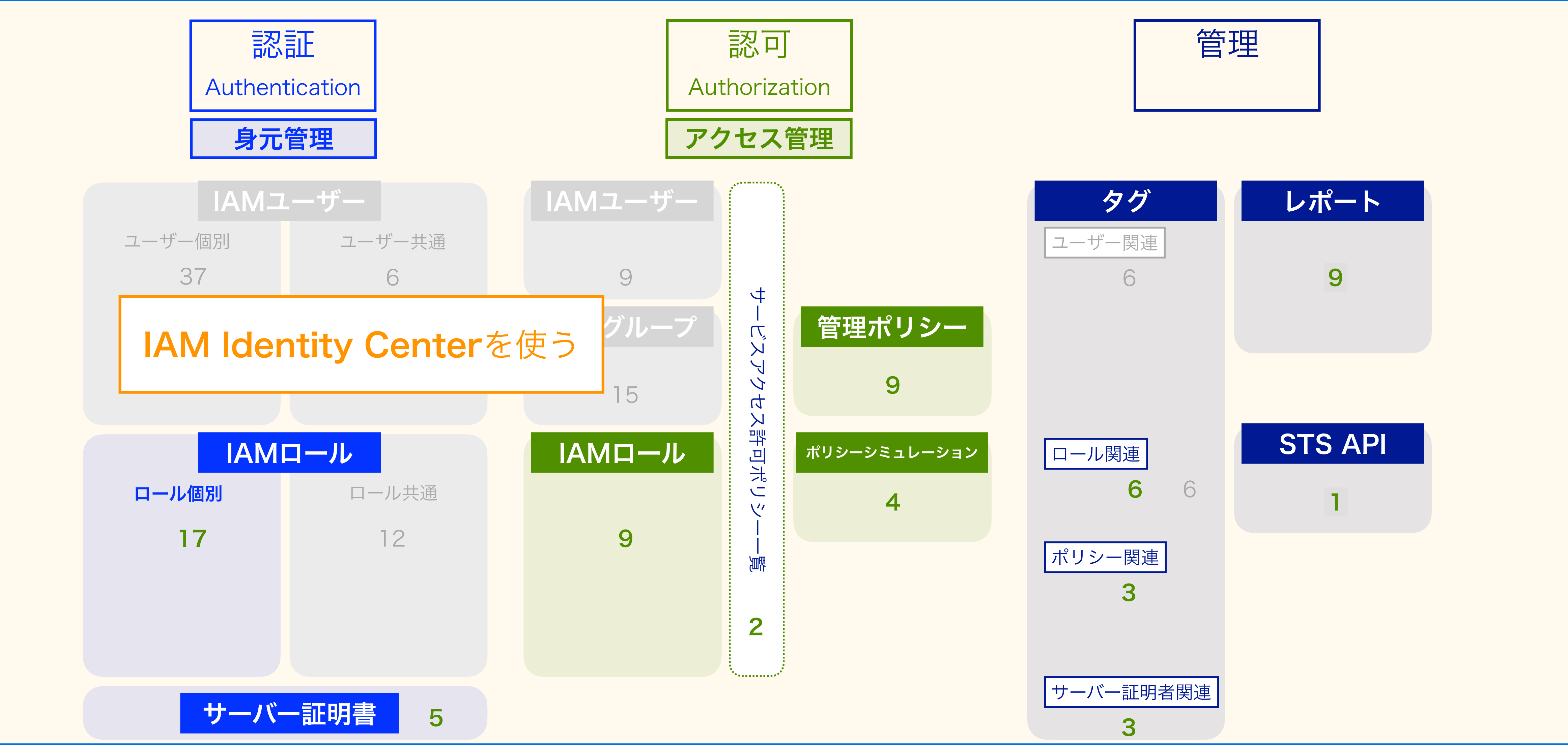
「IAMユーザーは原則使わない」のが今風

IAM公式ガイドで、繰り返し「IAMユーザー利用は非推奨」と表明されている



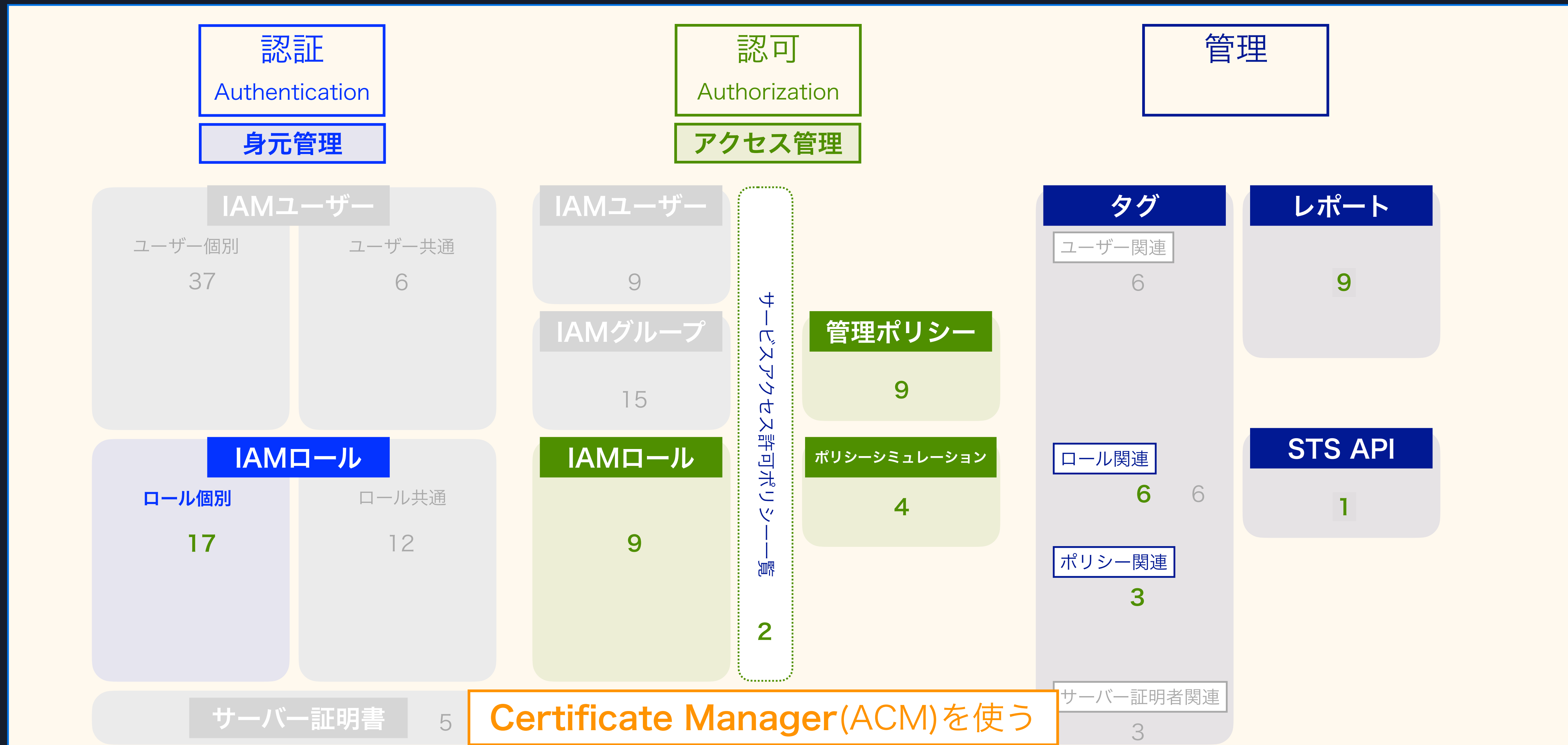
今後、IAMユーザーは原則使わない

159-91 = 68アクション



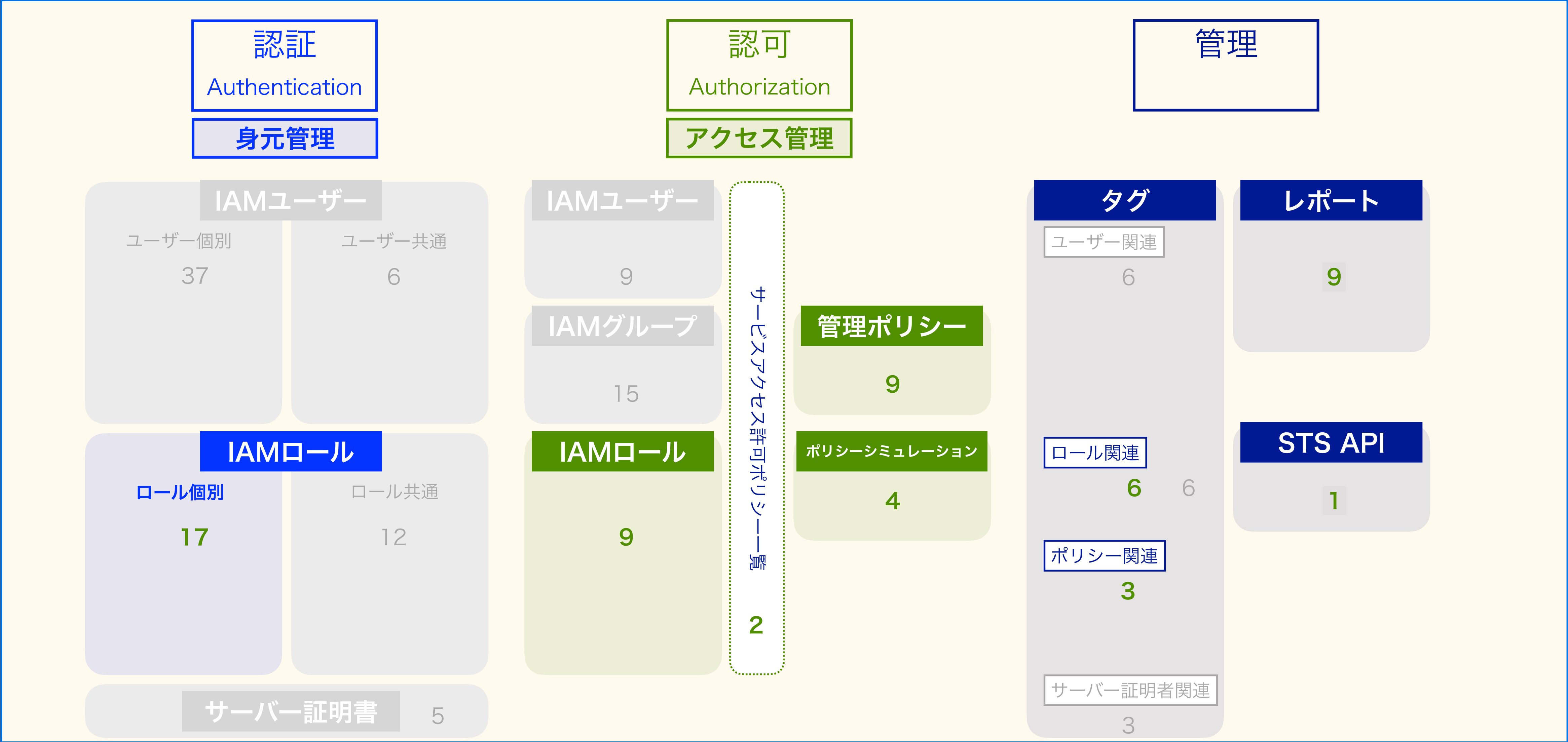
サーバー証明書は原則使わない

68-8 = 60アクション



結論: IAMはロールとポリシーが重要

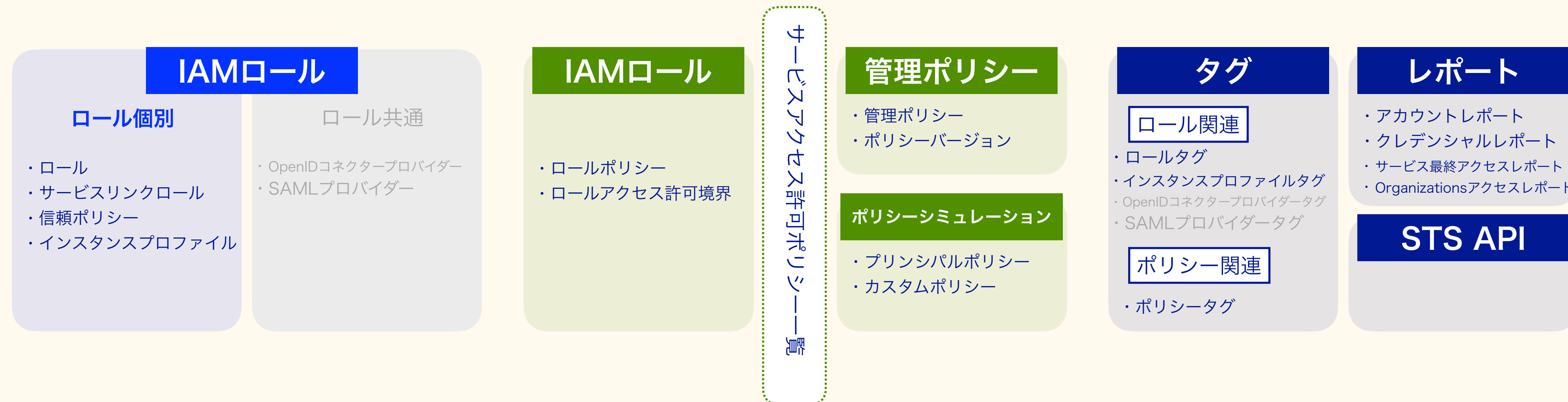
60アクション/159



まとめ: 20分で分かるIAM全機能



IAMはロールとポリシーが重要



IAMユーザーを作ったら負け

IAM Identity Center(SSO)を使う

こんな解説やハンズオンをやっています



JAWS-UG CLI
CLI専門支部

<https://jawsug-cli.connpass.com/>

JAWS-UG 最初の専門支部 (ハンズオン **411**回開催: 2014.7～)

Thank you!

波田野 裕一
@tcsH

15:30～ Hero2人で継続的なアウトプットのやり方の話をします

15:30 - 15:50	コミュニティ活動で重要なインプット・アウトプットとアウトプットエンジニアリング ～ インプット偏重からの脱却	情報収集や学習のためにセミナーなどに参加することは大変有意義なことです。しかし、参加するだけ、聞くだけでは、エンジニアとしての成長に限界があります。自分の技術的なアウトプットを多くの人の目に晒し、ブラッシュアップし続けていくことが不可欠です。本セッションでは、アウトプットを継続的に行うためにはどんな視点や行動が必要なのか、AWS Heroたちがエンジニアリング(知的生産工学)的な視点で議論します。 キーワードは「アウトプットしないのは知的な便秘」	AWS Container HERO 新井 雅也 氏 AWS Community HERO 波田野 裕一 氏
------------------	--	--	---