



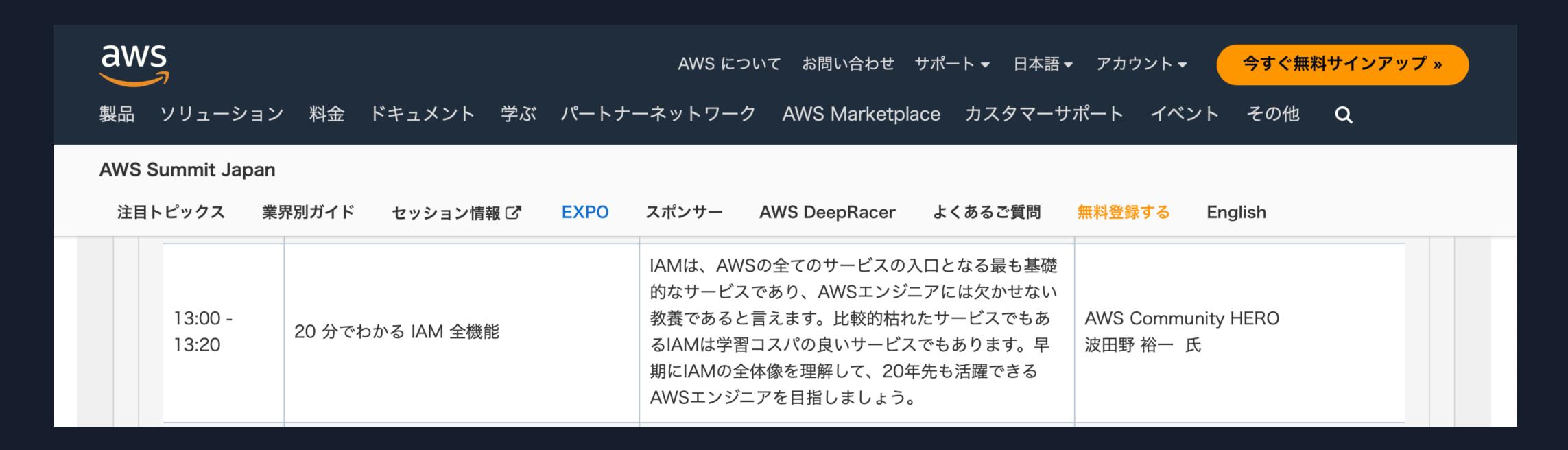


## 20分で分かるIAM全機能

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



「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

### AWS Identity and Access Management

IAM =



誰か?



### AWS Identity and Access Management



何を許可/禁止するか?

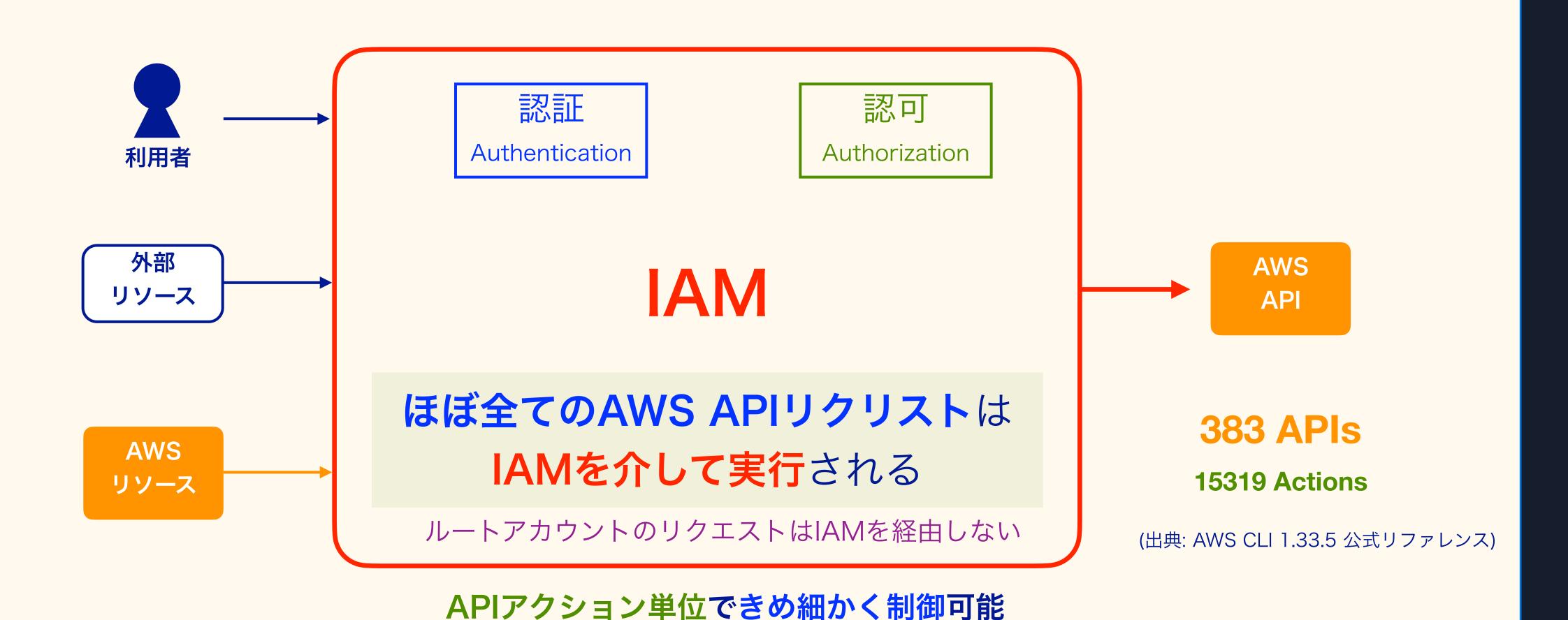
IAMは、AWSの認証・認可の管理という重要な役割を担う。





### 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





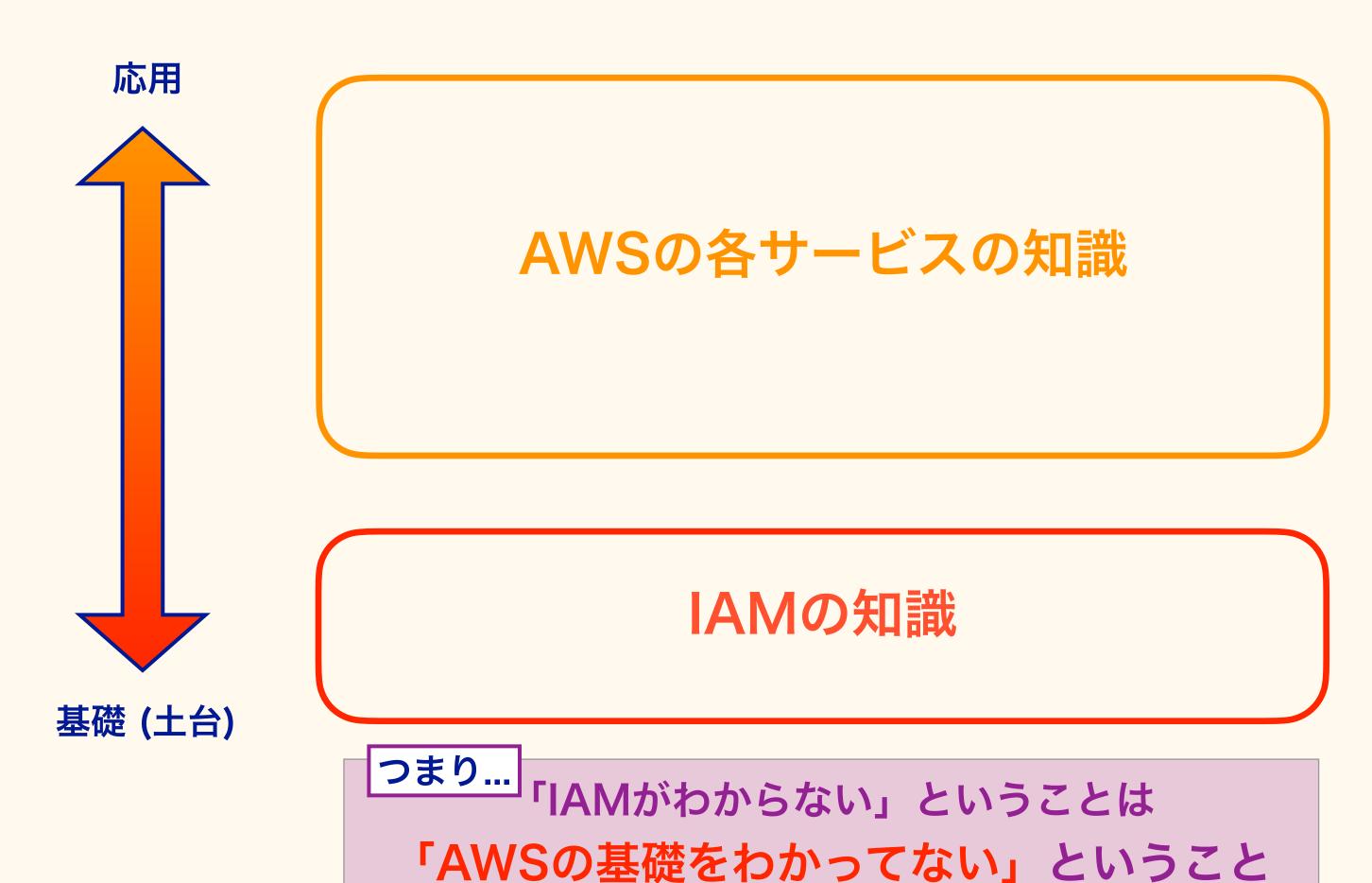






### AWSにおけるIAMの位置付け

IAMは、AWSの学習や実務における、最も重要な土台と言うべきサービス



IAM利用は無料

追加料金なしで利用できる







## 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。 呼び出される側 呼び出す側 利用者 外部 **AWS** リソース API リクエスト AWS リソース プリンシパル



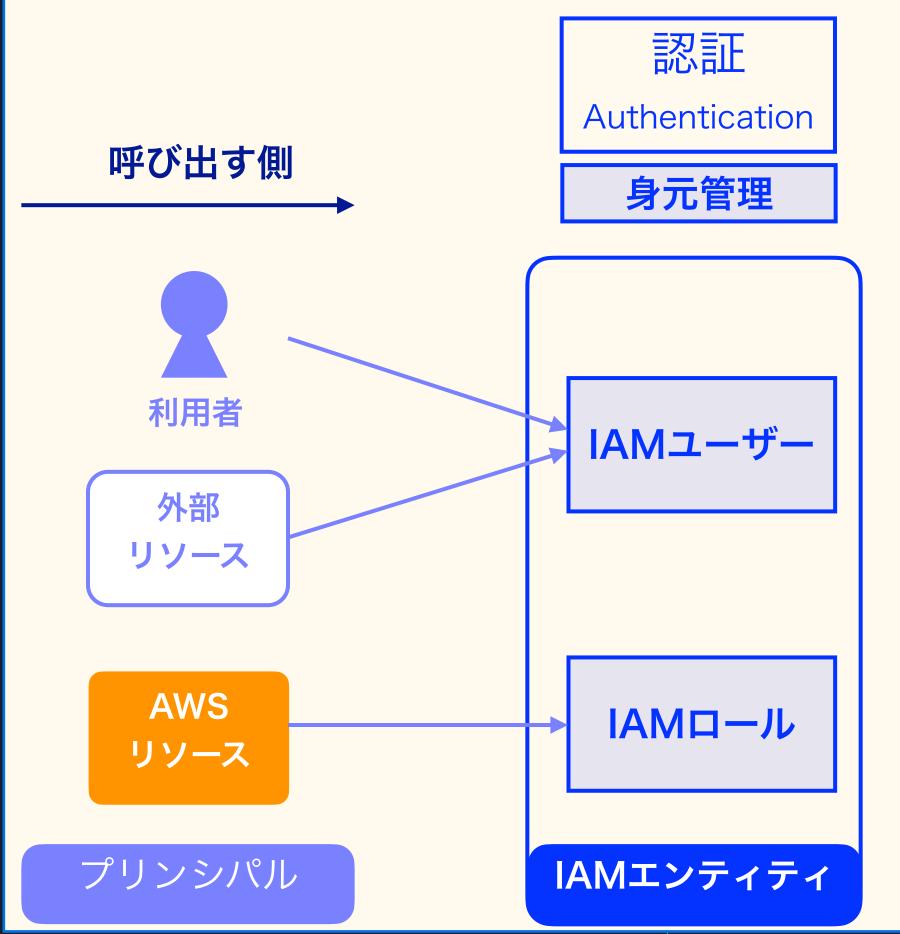






### IAMにおける「エンティティ」

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」と言います。



AWS外部の人やリソースを 管理するためにラベル付けしたもの

AWSリソースへの代理アクセスの提供を 管理するためにラベル付けしたもの 呼び出される側

AWS API



### 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。

認可 認証 Authentication **Authorization** 呼び出す側 呼び出される側 身元管理 アクセス管理 認可されたリクエスト 管理ポリシー 利用者 だけが実行される 外部 AWS インライン リソース API ポリシー アクセス許可 AWS 境界 IAMエンティティ プリンシパル IAMポリシー IAMアイデンティティ









### IAMにおける「アイデンティティ」

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。

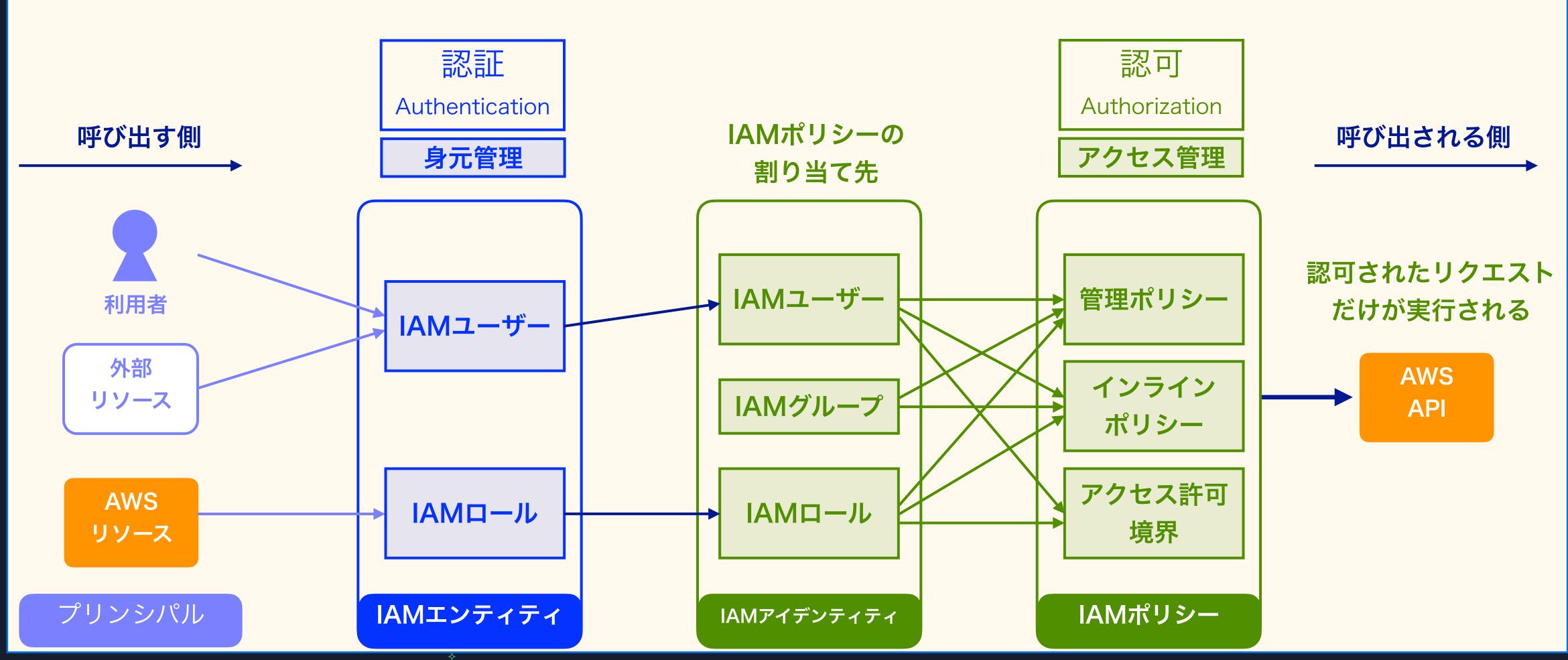
認証 Authentication 呼び出す側 身元管理 利用者 外部 リソース AWS プリンシパル IAMエンティティ

認可 **Authorization** IAMポリシーの 呼び出される側 アクセス管理 割り当て先 IAMユーザー 管理ポリシー AWS インライン IAMグループ API ポリシー アクセス許可 IAMロール 境界 IAMポリシー IAMアイデンティティ



### 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。

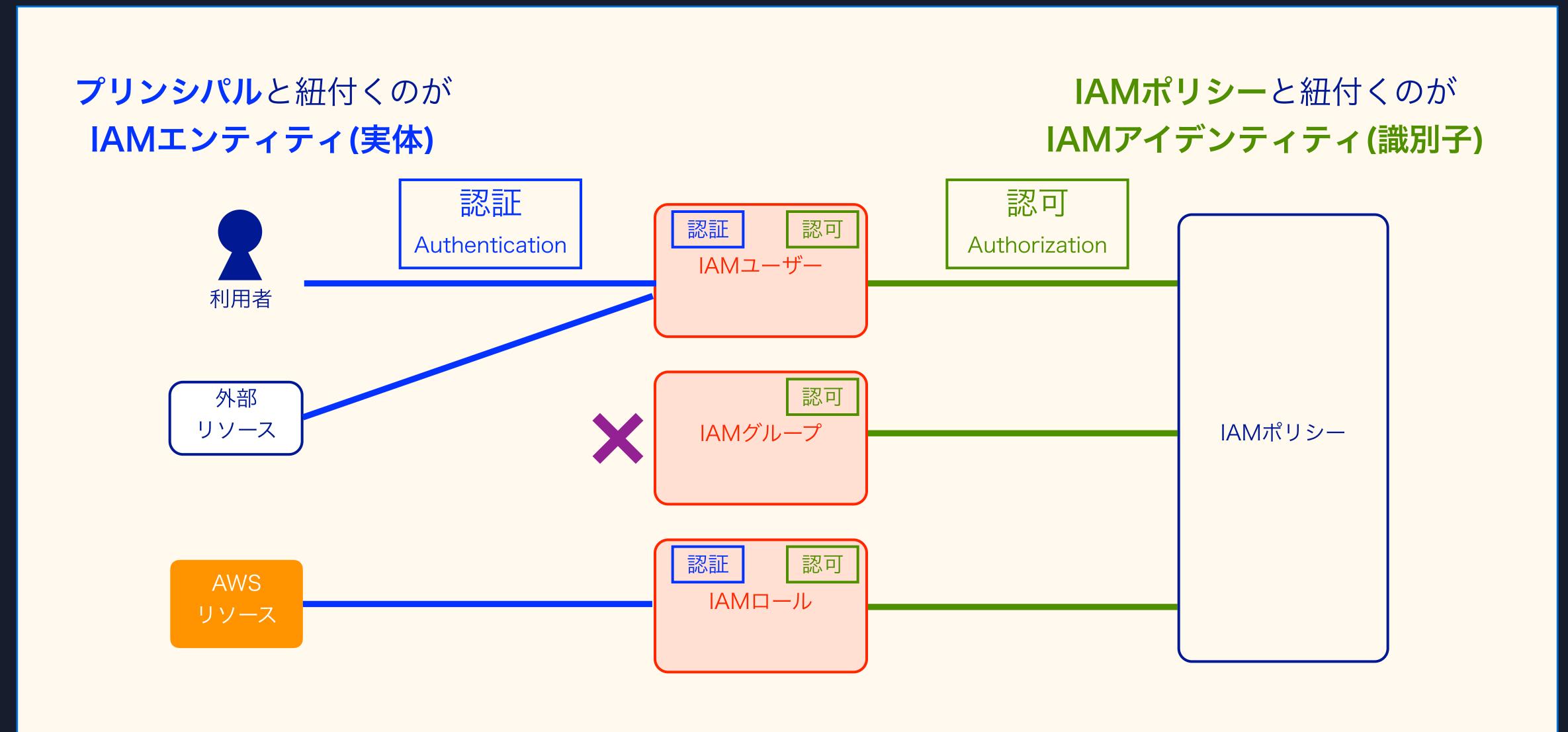








### 参考: IAMエンティティとIAMアイデンティティの区別









### 会談: 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。



#### **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.

グループはIAMエンティティではない Type: String

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



#### PolicyGroups.member.N

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

Type: Array of PolicyGroup objects

#### 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

#### グループはIAMエンティティではない

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







### IAMAPIの全機能マップ

#### 認証

Authentication

身元管理

#### IAMユーザー

#### ユーザー個別

- ・ユーザー
- ・アクセスキー
- ・ログインプロファイル
- MFA
- · SSH鍵
- ・サービス固有の資格情報
- ・署名証明書

#### ユーザー共通

- ・パスワードポリシー
- ・アカウントエイリアス

#### IAMロール

#### ロール個別

- ・ロール
- ・サービスリンクロール
- ・信頼ポリシー
- ・インスタンスプロファイル

#### ロール共通

- ・SAMLプロバイダー
- ・OpenIDコネクタープロバイダー

#### 認可

Authorization

アクセス管理

#

 $\Box$ 

ク

4

ス許可ポ

1

鸎

#### IAMユーザー

- ・ユーザーポリシー
- ・ユーザーアクセス許可境界

#### IAMグループ

- ・グループ
- ・グループポリシー

#### IAMロール

- ・ロールポリシー
- ・ロールアクセス許可境界

#### 管理ポリシー

- ・管理ポリシー
- ・ポリシーバージョン

#### ポリシーシミュレーション

- ・プリンシパルポリシー
- ・カスタムポリシー

#### 管理

#### タグ

#### ユーザー関連

- ・ユーザータグ
- ・MFAタグ

#### 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

#### STS API

#### 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コネクタープロバイダータグ
- ・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

#### サーバー証明書





認証 Authentication

身元管理

IAMユーザー

IAMロール

ユーザー個別

ロール個別

17

ユーザー共通

6

ロール共通

12

37

15

IAMロール

9

認可

Authorization

アクセス管理

4

ス許可ポリ

霓

2

IAMユーザー

9

IAMグループ

管理ポリシー

ポリシーシミュレーション

管理

タグ

ユーザー関連

6

9

レポート

ロール関連

12

STS API

ポリシー関連

サーバー証明者関連

3

サーバー証明書

5







## IAMの全機能









## IAM APIの全機能マップ (14の機能領域 40の機能)

#### 認証

Authentication

身元管理

#### 認可

**Authorization** 

アクセス管理

厂

4

,許可术

#### 管理

タグ

・ユーザータグ

・MFAタグ

ロールタグ

・ポリシータグ

インスタンスプロファイルタグ OpenIDコネクタープロバイダータグ

SAMLプロバイダータグ

・サーバー証明書タグ

#### IAMユーザー

IAMロール

#### ユーザー個別

- ・ユーザー
- ・アクセスキー
- ・ログインプロファイル
- MFA
- · SSH鍵
- ・サービス固有の資格情報

ロール個別

・サービスリンクロール

・インスタンスプロファイル

・署名証明書

・ロール

・信頼ポリシー

#### ユーザー共通

ロール共通

OpenIDコネクタープロバイダー

SAMLプロバイダー

- ・パスワードポリシー
- ・アカウントエイリアス

#### IAMユーザー

- ・ユーザーポリシー
- ・ユーザーアクセス許可境界

#### IAMグループ

- ・グループ
- ・グループポリシー

#### IAMロール

- ・ロールポリシー
- ・ロールアクセス許可境界

#### 管理ポリシー

- ・管理ポリシー
- ・ポリシーバージョン

#### ポリシーシミュレーション

- ・プリンシパルポリシー
- ・カスタムポリシー

#### 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

#### STS API

#### サーバー証明書







\_\_\_\_ aws \_\_\_\_

**HEROES** 

## IAMの全機能 (認証)

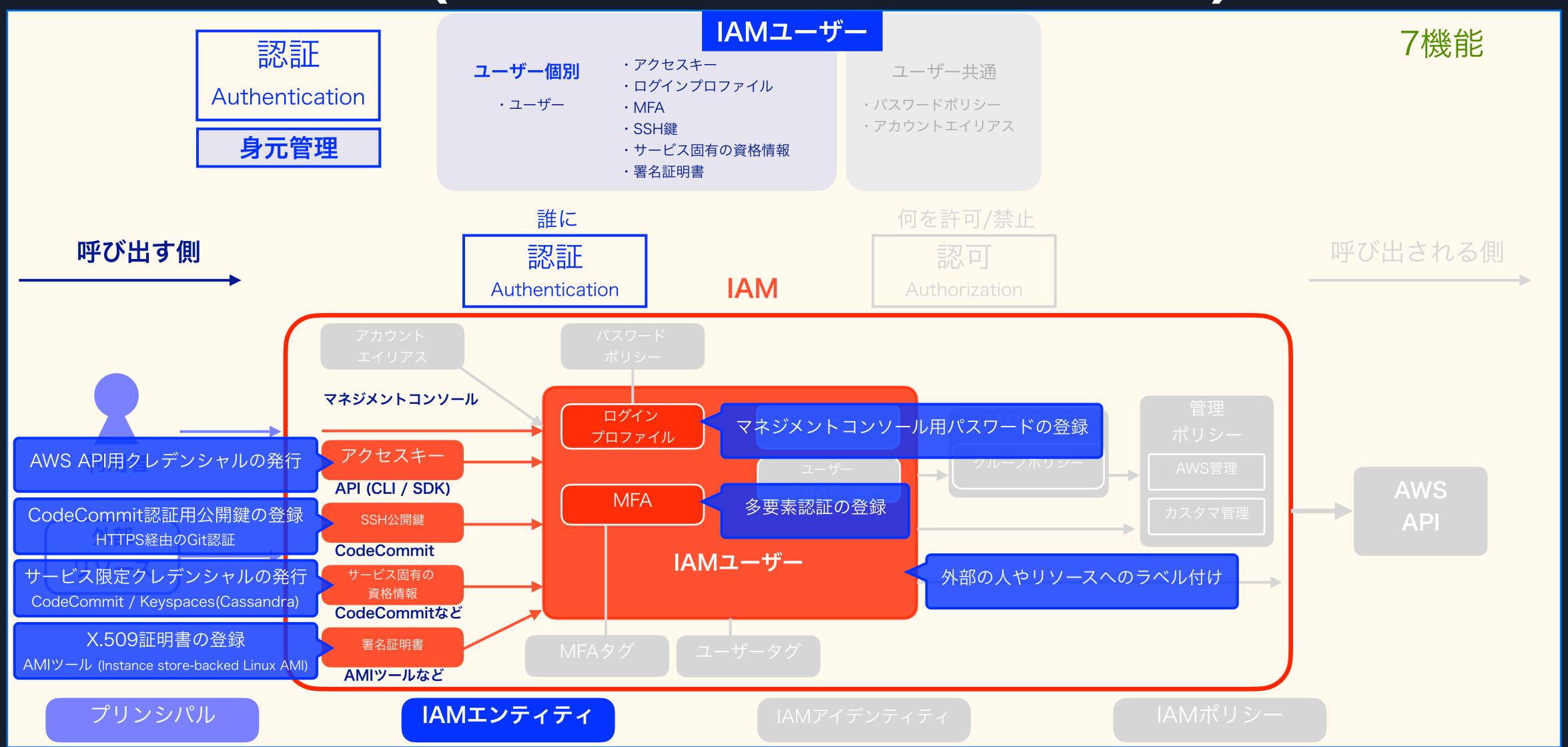




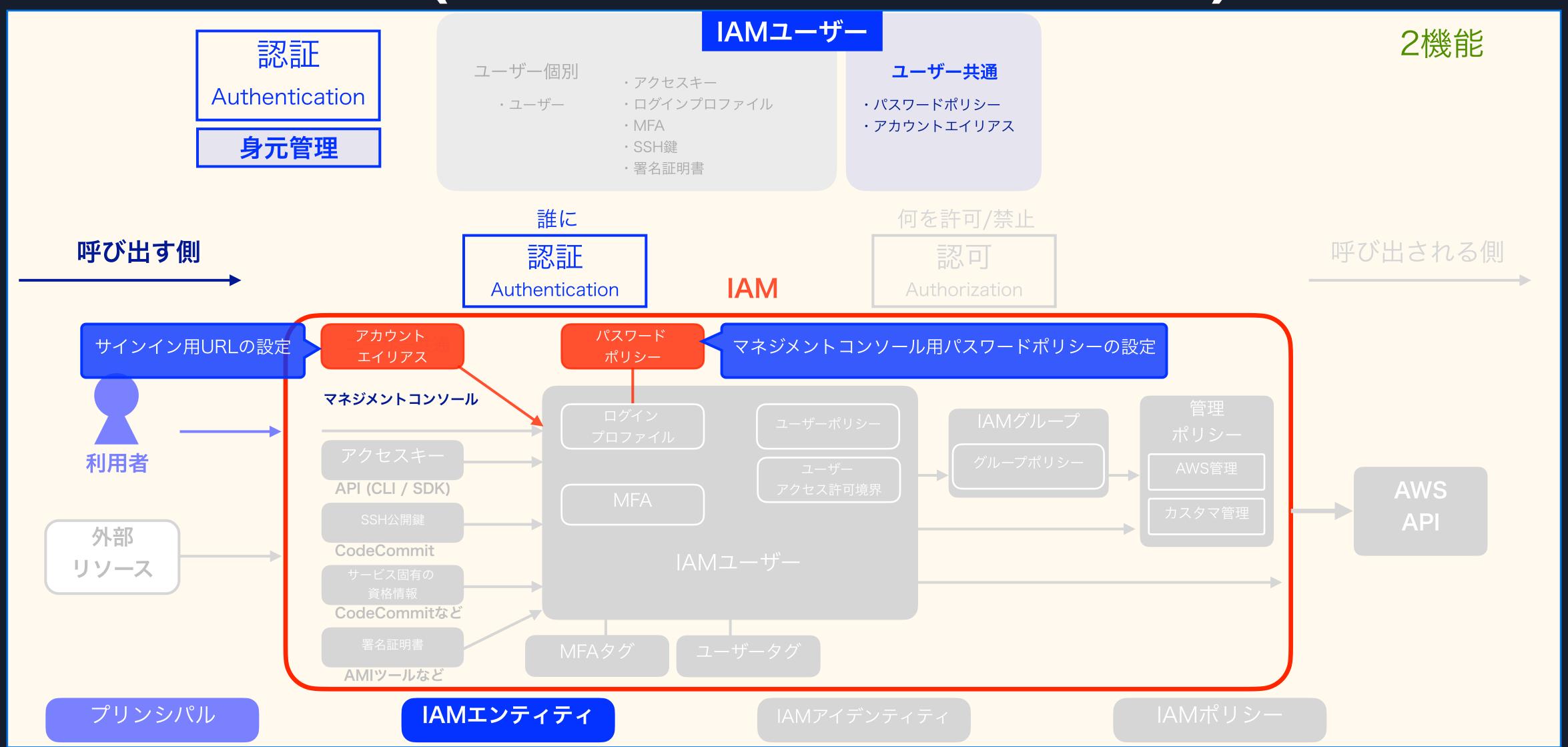




### IAMの全機能 (認証: IAMユーザー 個別)

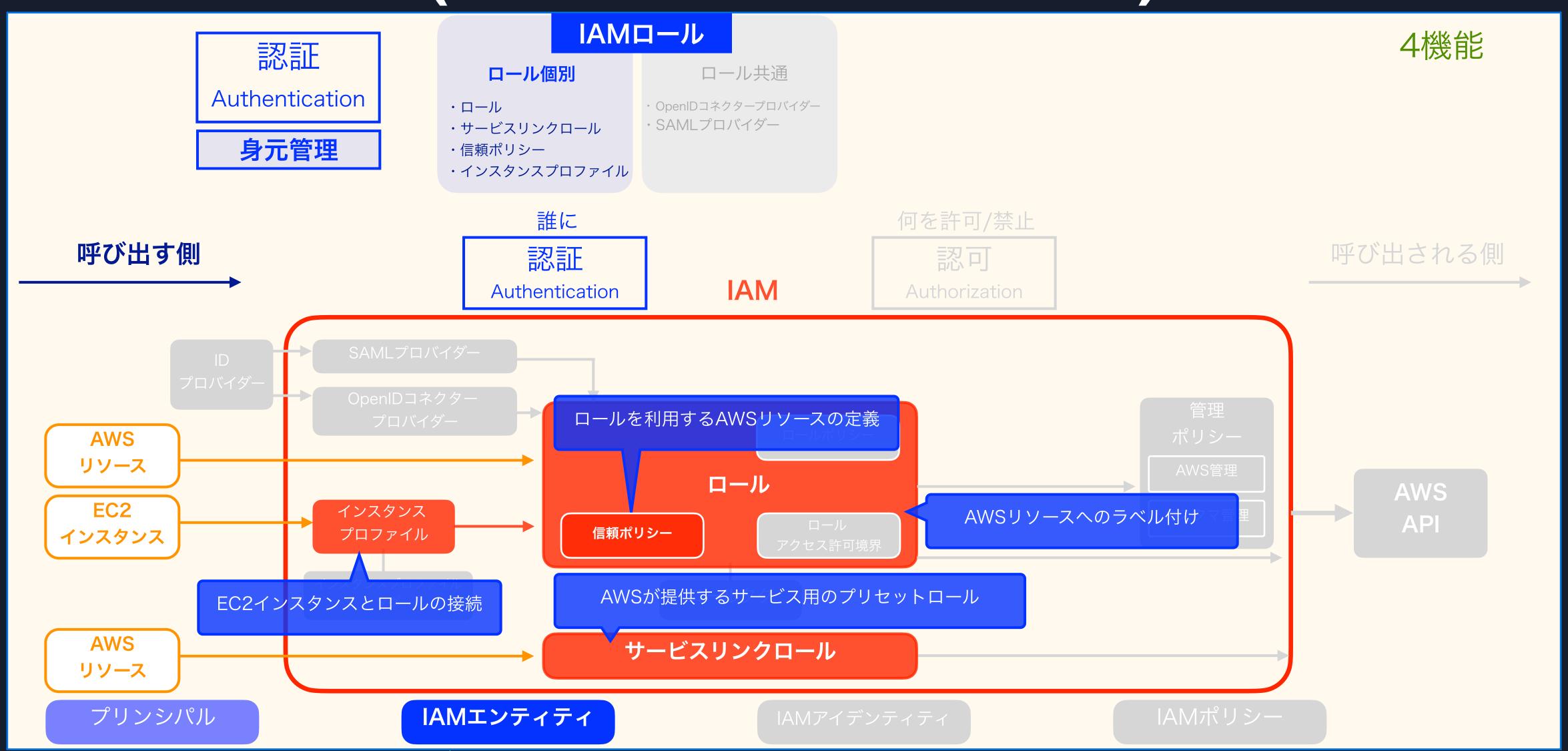


## IAMの全機能 (認証: IAMユーザー 共通)



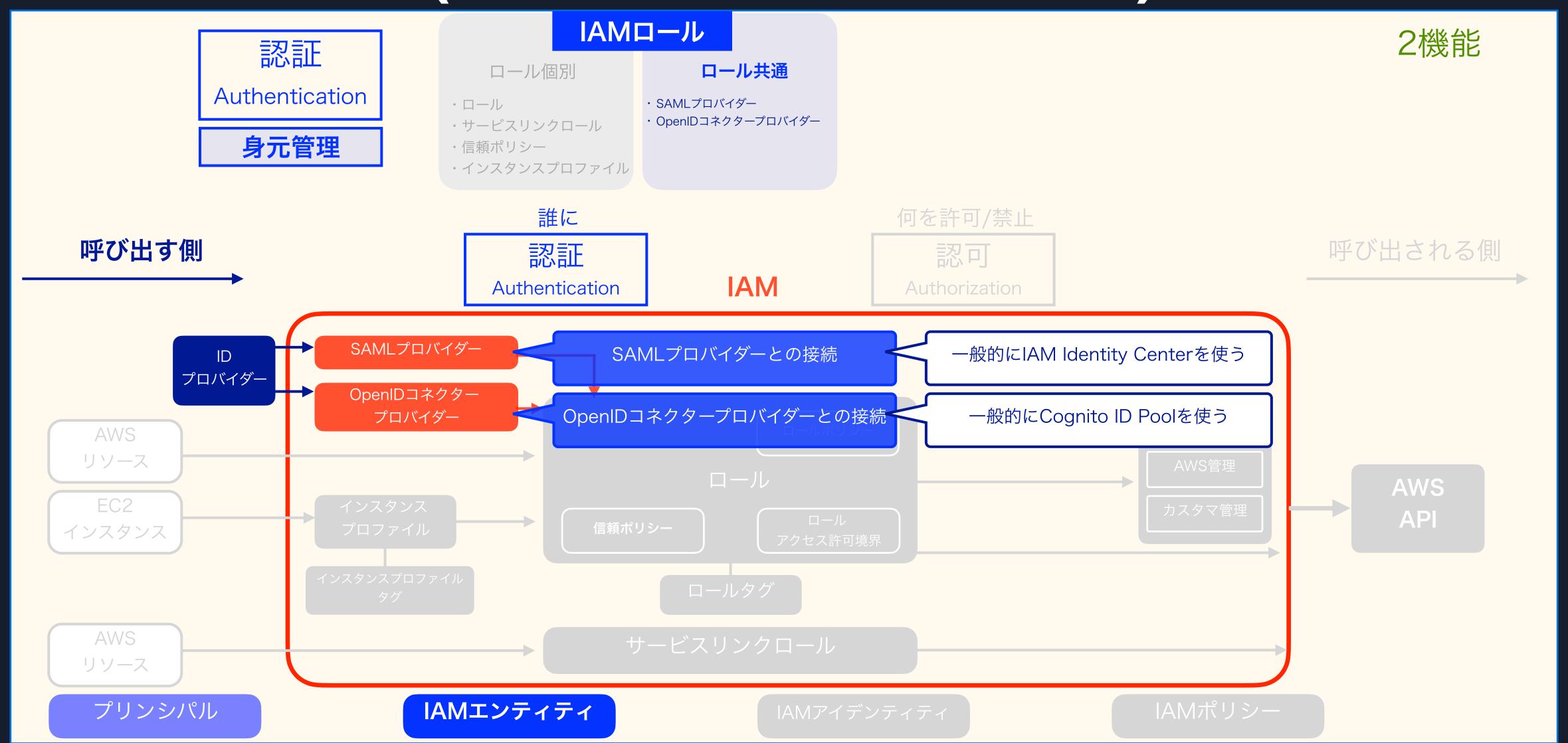


### IAMの全機能 (認証: IAMロール 個別)





### 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)

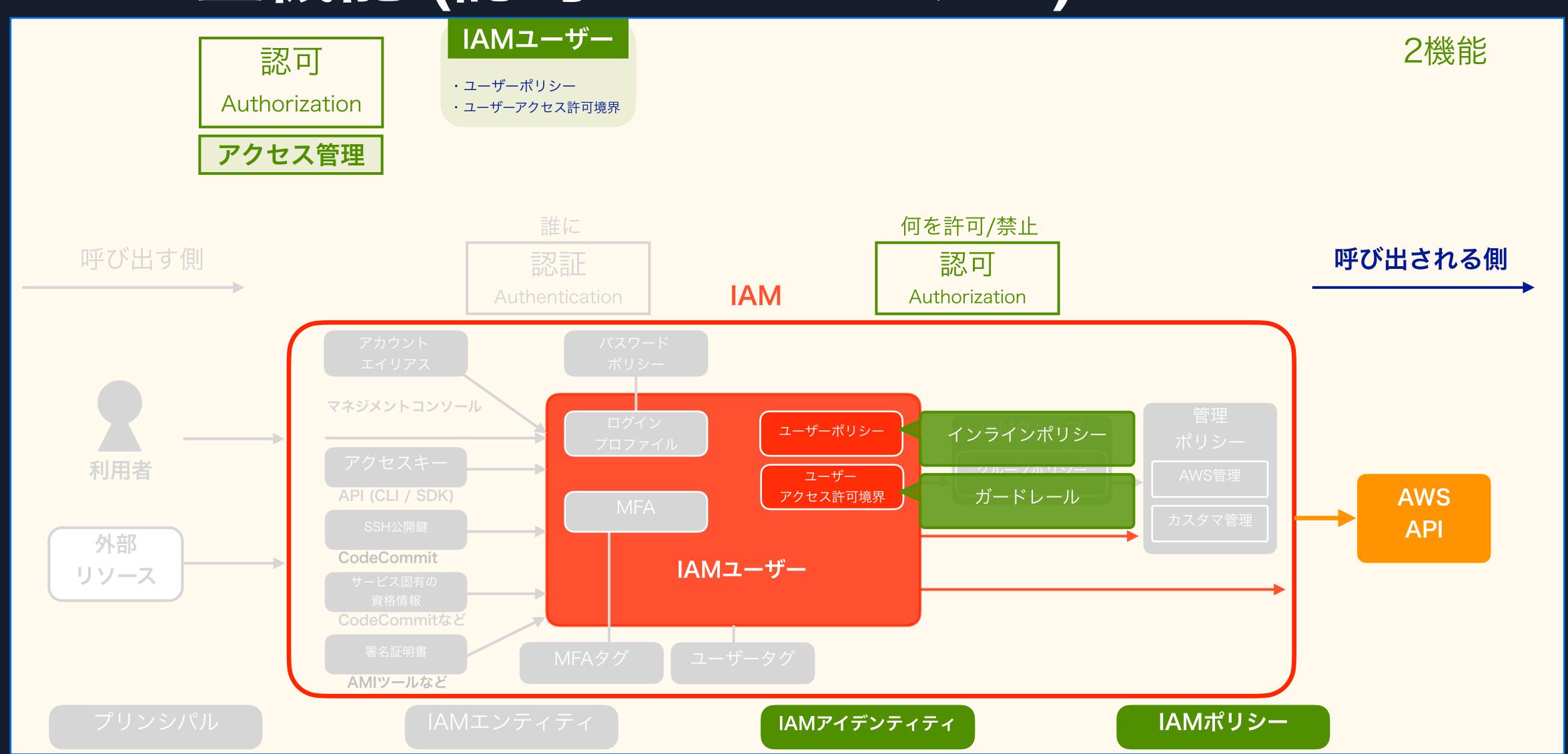






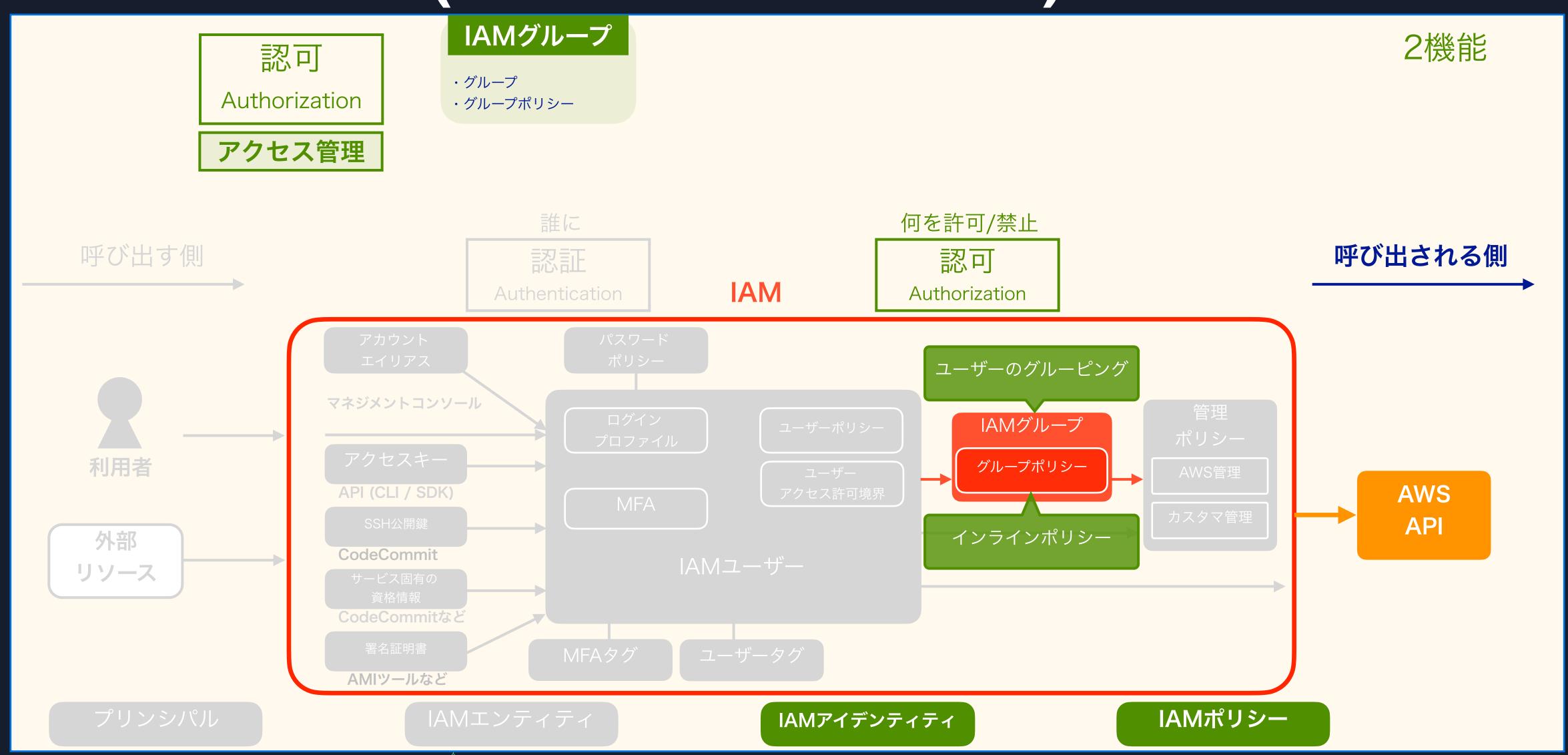


## IAMの全機能 (認可: IAMユーザー)

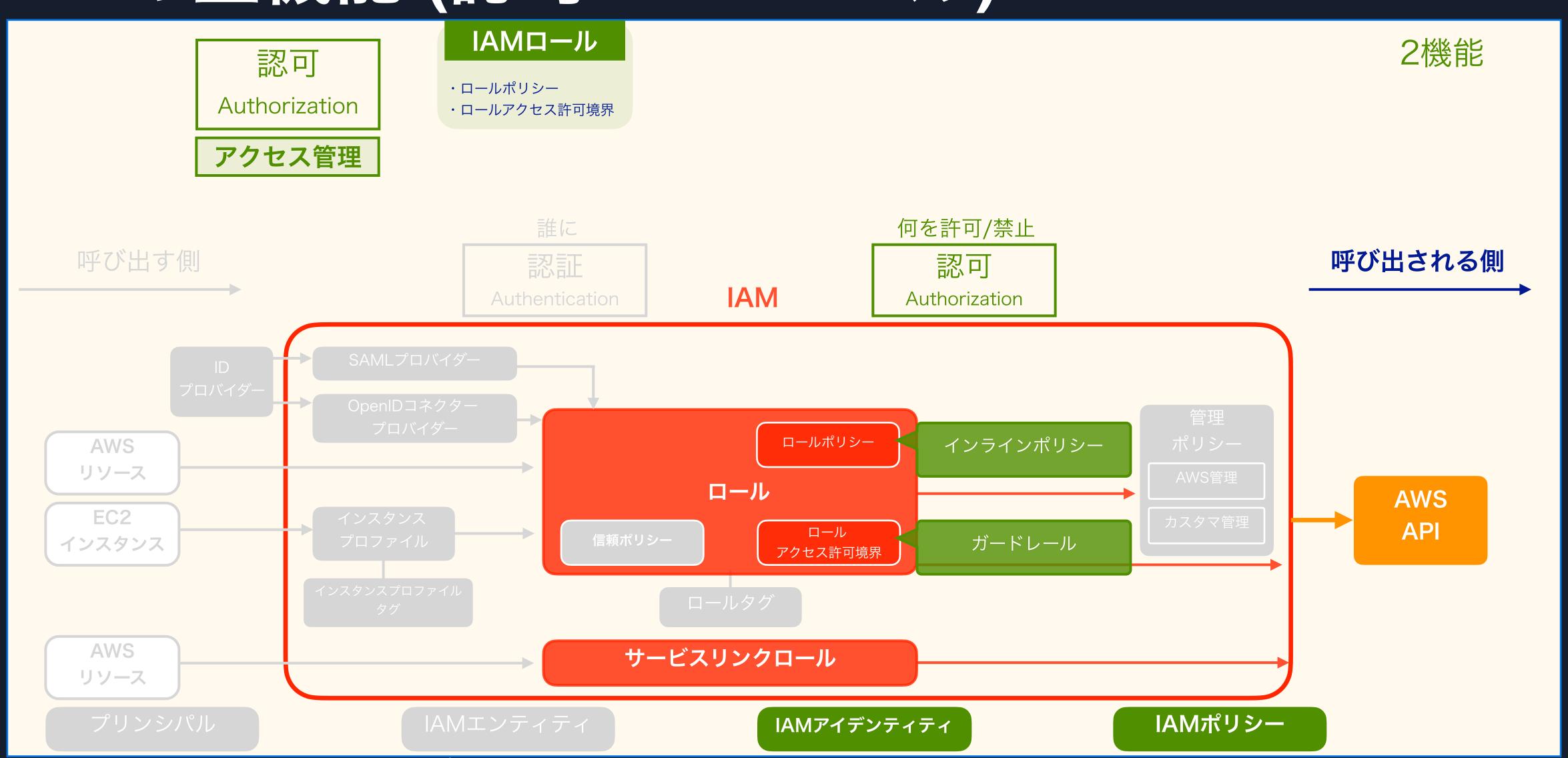




## IAMの全機能 (認可: IAMグループ)

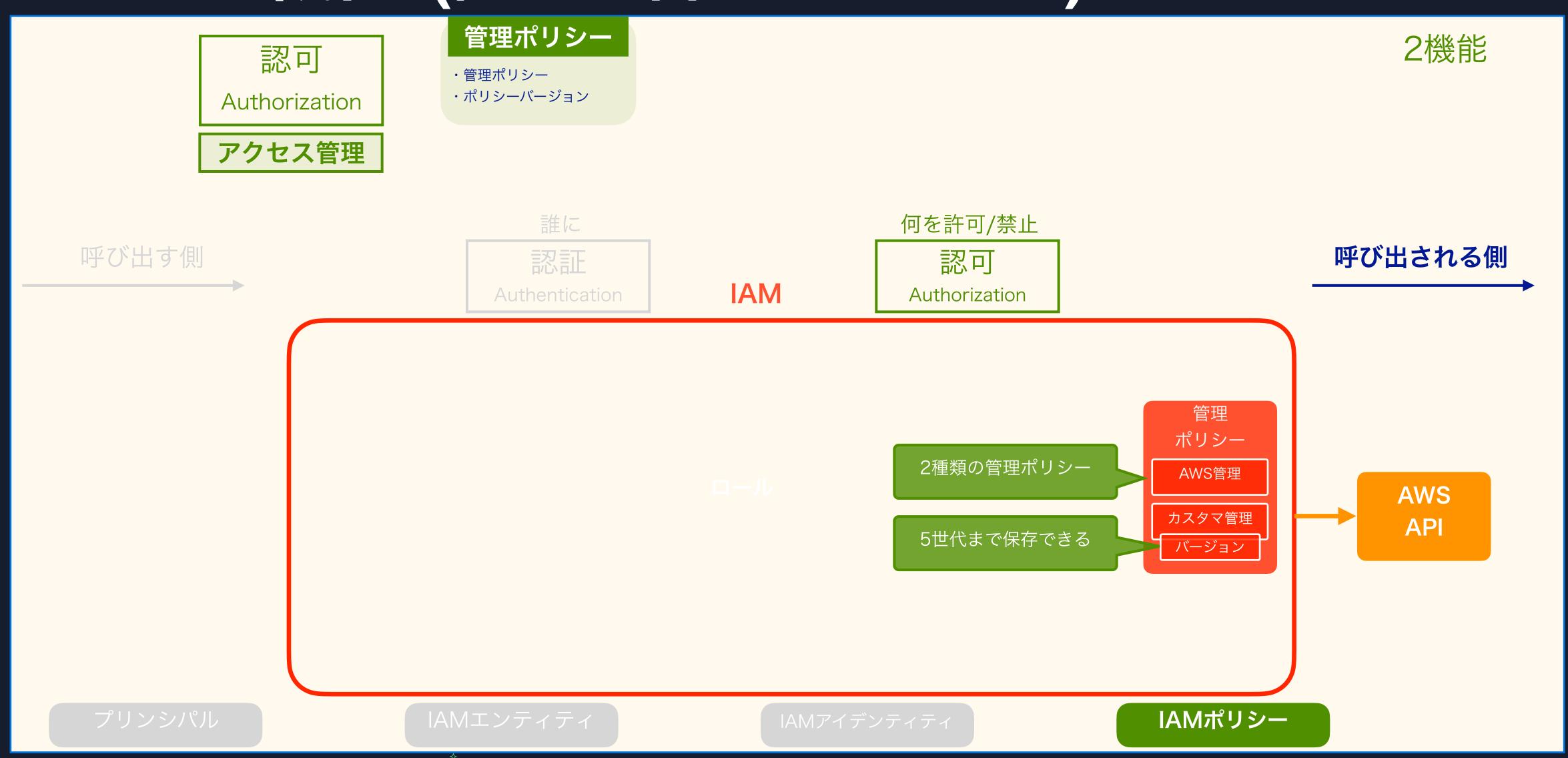


## IAMの全機能(認可: IAMロール)



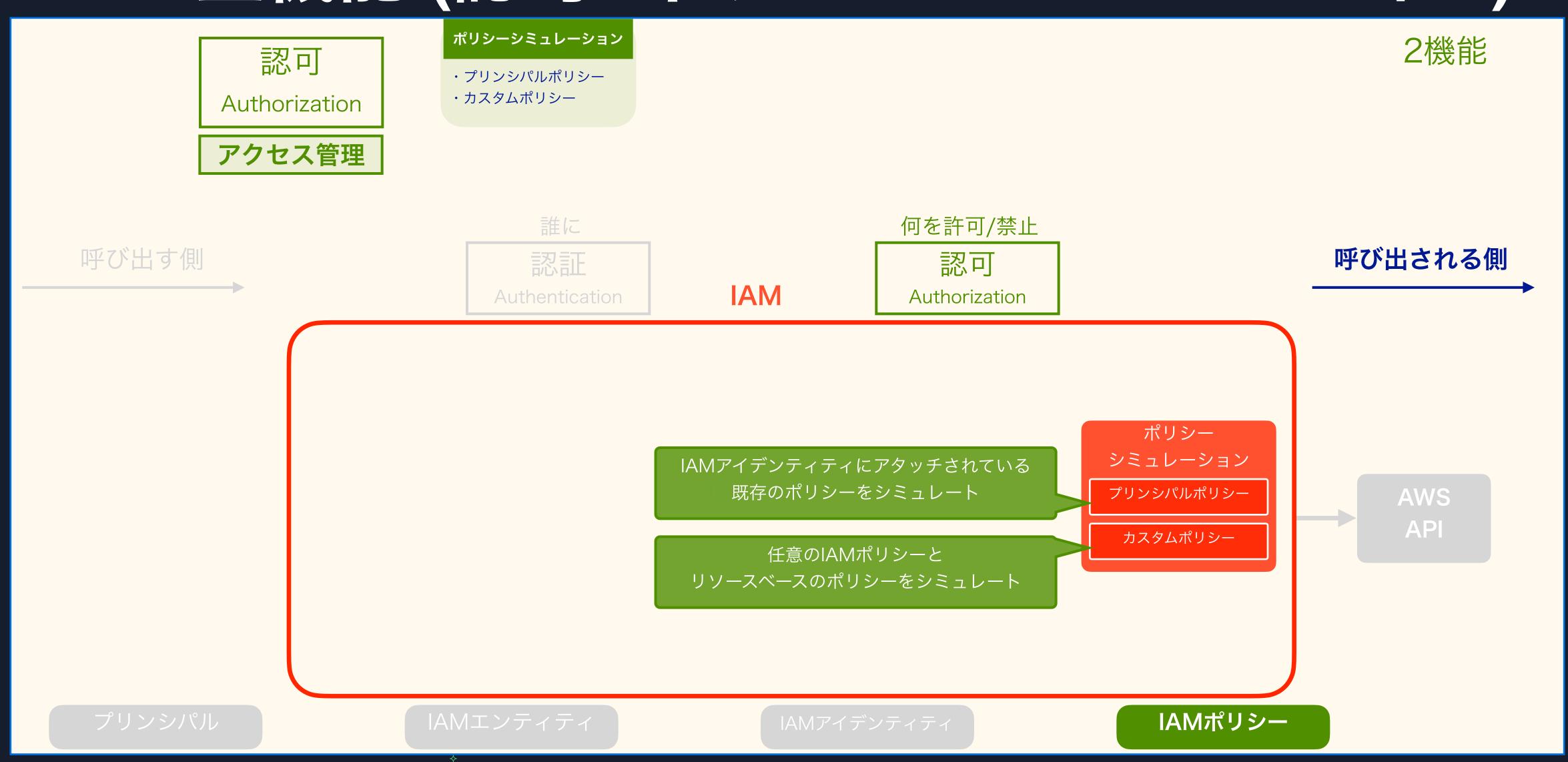


## IAMの全機能 (認可: 管理ポリシー)





## 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)

認可

**Authorization** 

アクセス管理

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 1機能

ービスアクセス許可ポリシー









## IAMの全機能(管理)









## IAMの全機能 (管理: タグ)

管理

マネジメントコンソール

8機能

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コネクタープロバイダータグ
- ・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)

管理

4機能

#### 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

vlToken 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







## 「IAMの重要ポイント」と「まとめ」



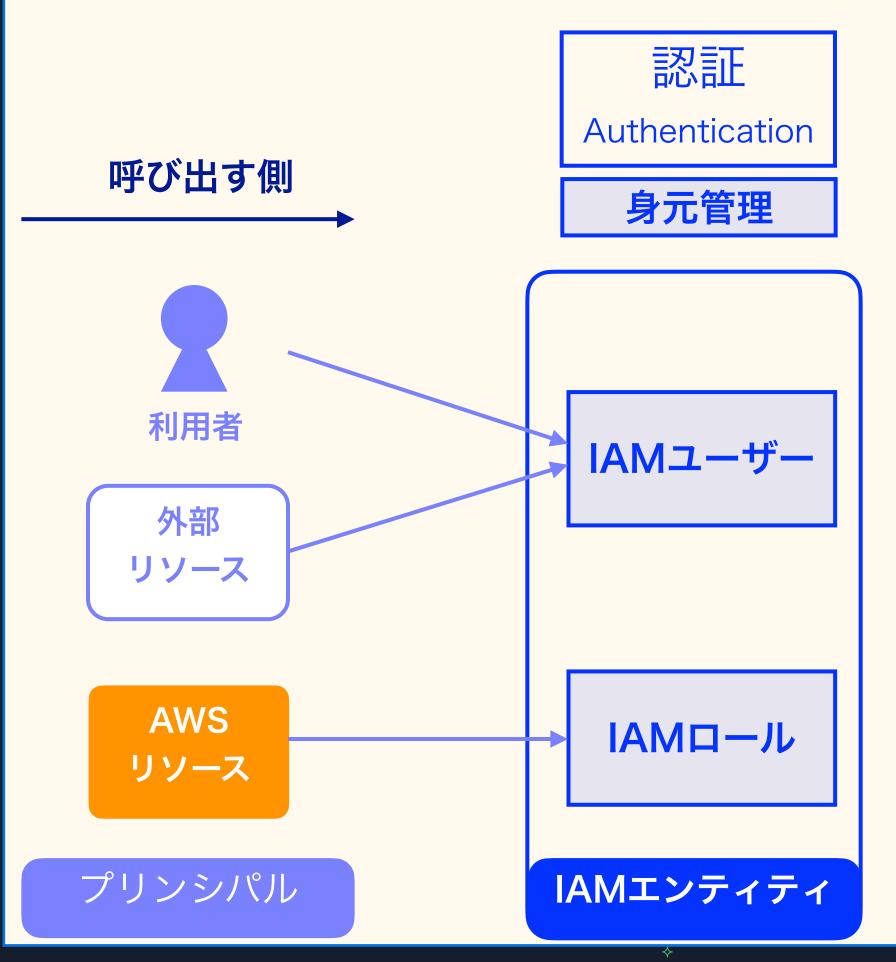






### 「IAMユーザーは原則使わない」のが今風

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



AWS外部の人やリソースを 管理するためにラベル付けしたもの

恒常的なクレデンシャルが常にAWS外にある

AWSリソースへの代理アクセスの提供を 管理するためにラベル付けしたもの

一時的なクレデンシャルを常にAWS内で使う

漏洩リスク高

自動失効なし

漏洩リスク低

自動失効あり





### 今後、IAMユーザーは原則使わない 159-91 = 68アクション

管理 認証 認可 Authentication **Authorization** アクセス管理 身元管理 IAMユーザー IAMユーザー レポート タグ ユーザー共通 ユーザー個別 ユーザー関連 9 37 9 6 6 管理ポリシー 厂 **IAM Identity Center**を使う 7 15 4 ス許可ポリ STS API IAMロール IAMロール ポリシーシミュレーション ロール関連 6 ロール共通 ロール個別 9 17 ポリシー関連 鸎 2 サーバー証明者関連 サーバー証明書 5









68-8 = 60  $\mathbb{Z}$   $\mathbb{Z}$   $\mathbb{Z}$ 

管理 認可 認証 Authentication Authorization アクセス管理 身元管理 IAMユーザー IAMユーザー レポート タグ ユーザー共通 ユーザー関連 ユーザー個別 37 9 6 9 6 管理ポリシー IAMグループ 厂 スアクセ 15 ス許可ポリ STS API IAMロール IAMロール ポリシーシミュレーション ロール関連 6 ロール共通 ロール個別 4 9 17 ポリシー関連 霓 2 サーバー証明者関連 サーバー証明書 Certificate Manager(ACM)を使う 5



認証

Authentication

身元管理

認可

Authorization

アクセス管理

厂

7

4

ス許可ポリ

鸎

2

管理

IAMユーザー

ユーザー個別

37

ユーザー共通

ロール共通

6

IAMユーザー

9

IAMグループ

15

IAMロール

9

管理ポリシー

ポリシーシミュレーション

タグ

ユーザー関連

6

レポート

9

STS API

ロール関連

6

ポリシー関連

サーバー証明者関連

IAMロール

ロール個別

17

サーバー証明書

5





44

## まとめ: 20分で分かるIAM全機能

認証

Authentication

身元管理

認可

**Authorization** 

アクセス管理

厂

アス

4

ス許可ポ

1

管理

### IAMはロールとポリシーが重要

#### IAMロール

#### ロール個別

- ・ロール
- ・サービスリンクロール
- ・信頼ポリシー
- ・インスタンスプロファイル

#### IAMロール

- · OpenIDコネクタープロバイダー
- ・SAMLプロバイダー

ロール共通

- ・ロールポリシー
- ・ロールアクセス許可境界

#### 管理ポリシー

- ・管理ポリシー
- ・ポリシーバージョン

#### ポリシーシミュレーション

- ・プリンシパルポリシー
- ・カスタムポリシー

#### 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コネクタープロバイダータグ
- SAMLプロバイダータグ

#### ポリシー関連

・ポリシータグ

#### 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

STS API

### 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

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 AWS Container HERO す。自分の技術的なアウトプットを多くの人の目に晒 新井 雅也 氏 コミュニティ活動で重要なインプット・ア し、ブラッシュアップし続けていくことが不可欠で 15:30 -ウトプットとアウトプットエンジニアリン す。本セッションでは、アウトプットを継続的に行う 15:50 グ ~ インプット偏重からの脱却 AWS Community HERO ためにはどんな視点や行動が必要なのか、AWS Hero 波田野 裕一 氏 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」





