IAM

レクチャー	レクチャーで学ぶ内容
IAMの概要	IAMの基本的な機能や仕組みについて理解します。
IAM設計	実際に会社などの組織でIAM設計を行う場合を想定した簡単なケーススタディを実施します。
IAMグループへのポリシー適用（ハンズオン）	IAMポリシーを作ってIAMグループに適用するハンズオンを実施します。
IAMロールへのポリシー適用（ハンズオン）	IAMポリシーを作ってIAMロールに適用するハンズオンを実施します。
AWS Organizationの概要	AWS Organizationの内容と基本的な機能や役割を理解します。

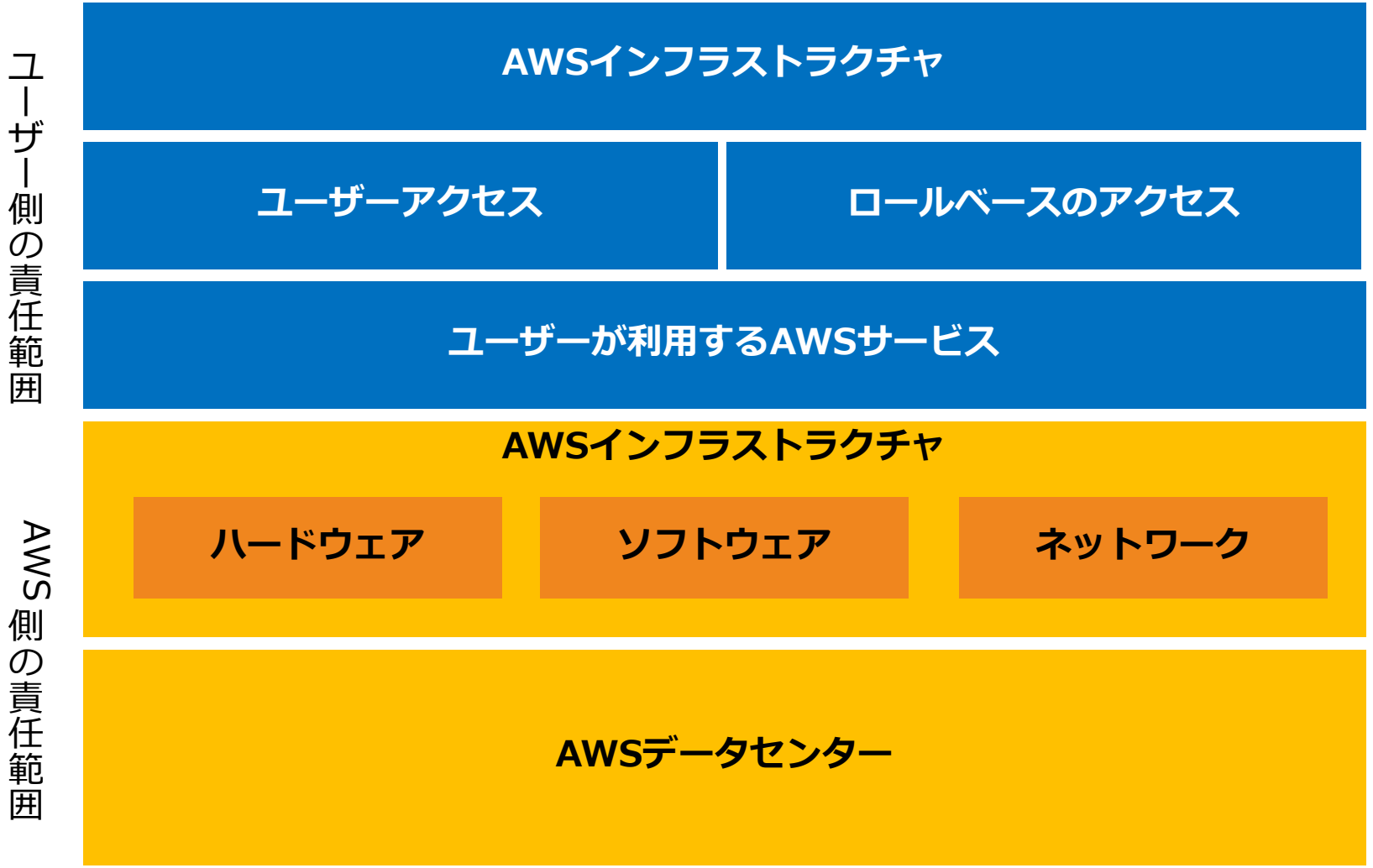
IAM

レクチャー	レクチャーで学ぶ内容
AWS Organization の設定 （ハンズオン）	AWS Organizationの設定のハンズオンを実施します。

IAMの概要

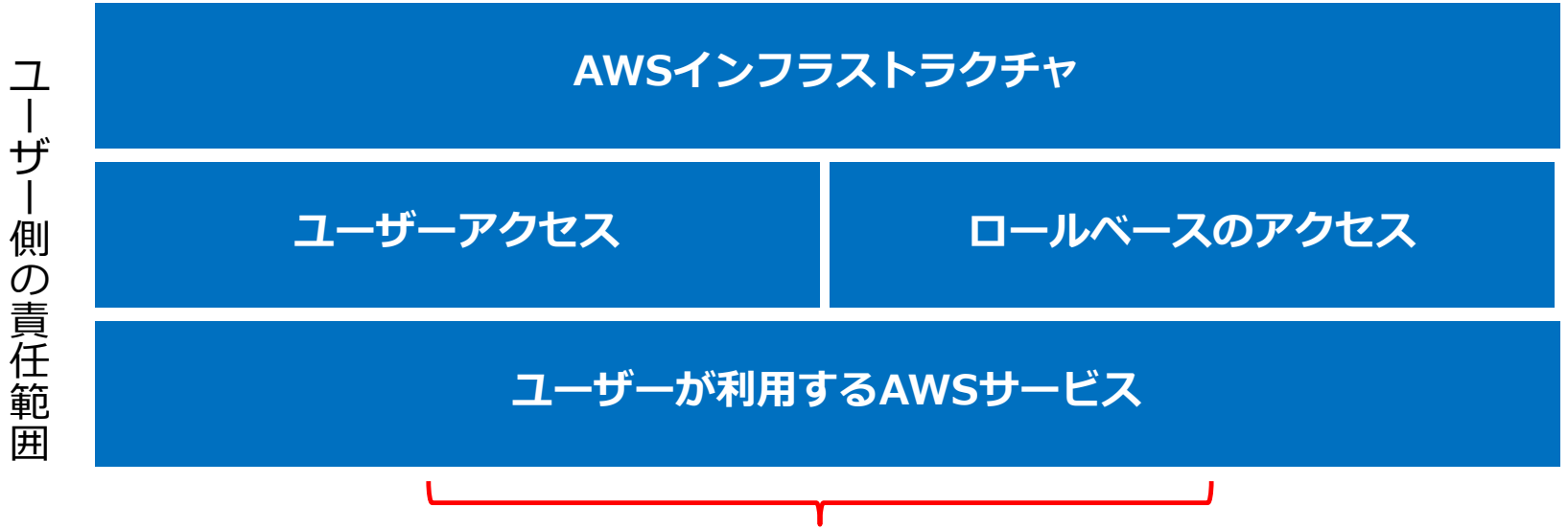
責任共有モデル

セキュリティに対してAWSとユーザーとで責任分解して対応する責任共有モデルとなっている



責任共有モデル

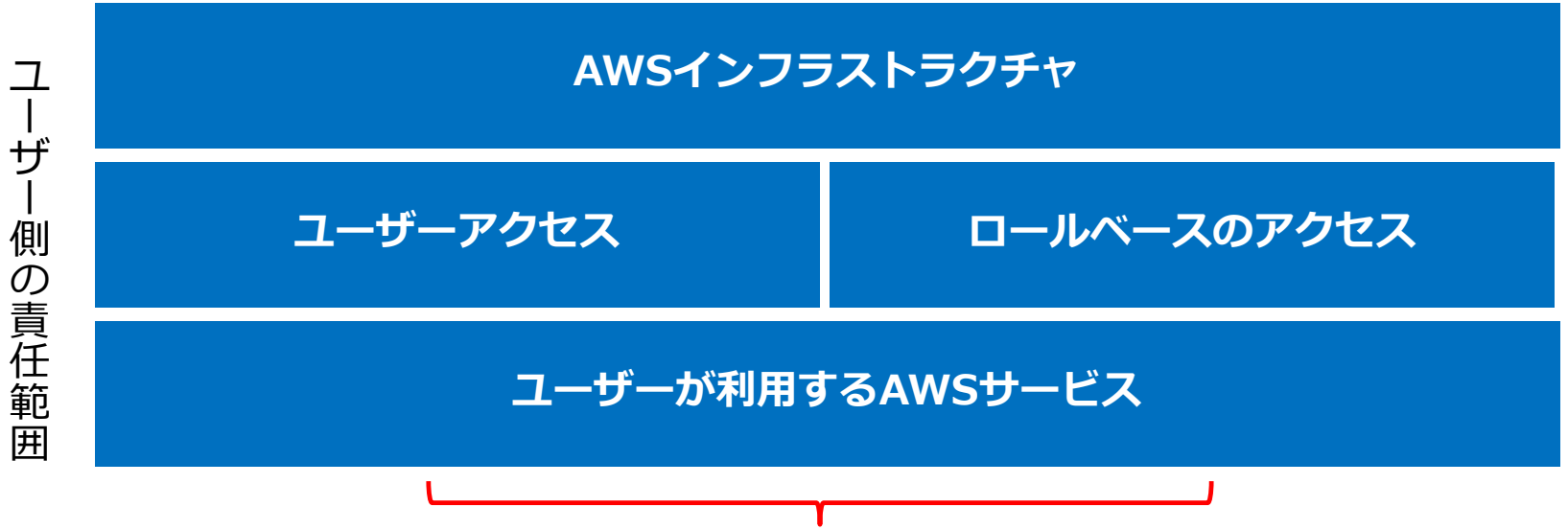
セキュリティに対してAWSとユーザーとで責任分解して対応する責任共有モデルとなっている



- IAMによるアカウント管理
- セキュリティグループの設定
- アプリケーションのロールベースのアクセス設定
- ネットワーク／インスタンスオペレーションシステム（バッチ）などの設定
- OS／ホストベースのファイアーウォール設置

責任共有モデル

セキュリティに対してAWSとユーザーとで責任分解して対応する責任共有モデルとなっている



- **IAMによるアカウント管理**
- **セキュリティグループの設定**
- アプリケーションのロールベースのアクセス設定
- ネットワーク／インスタンスオペレーションシステム（バッチ）などの設定
- OS／ホストベースのファイアーウォール設置

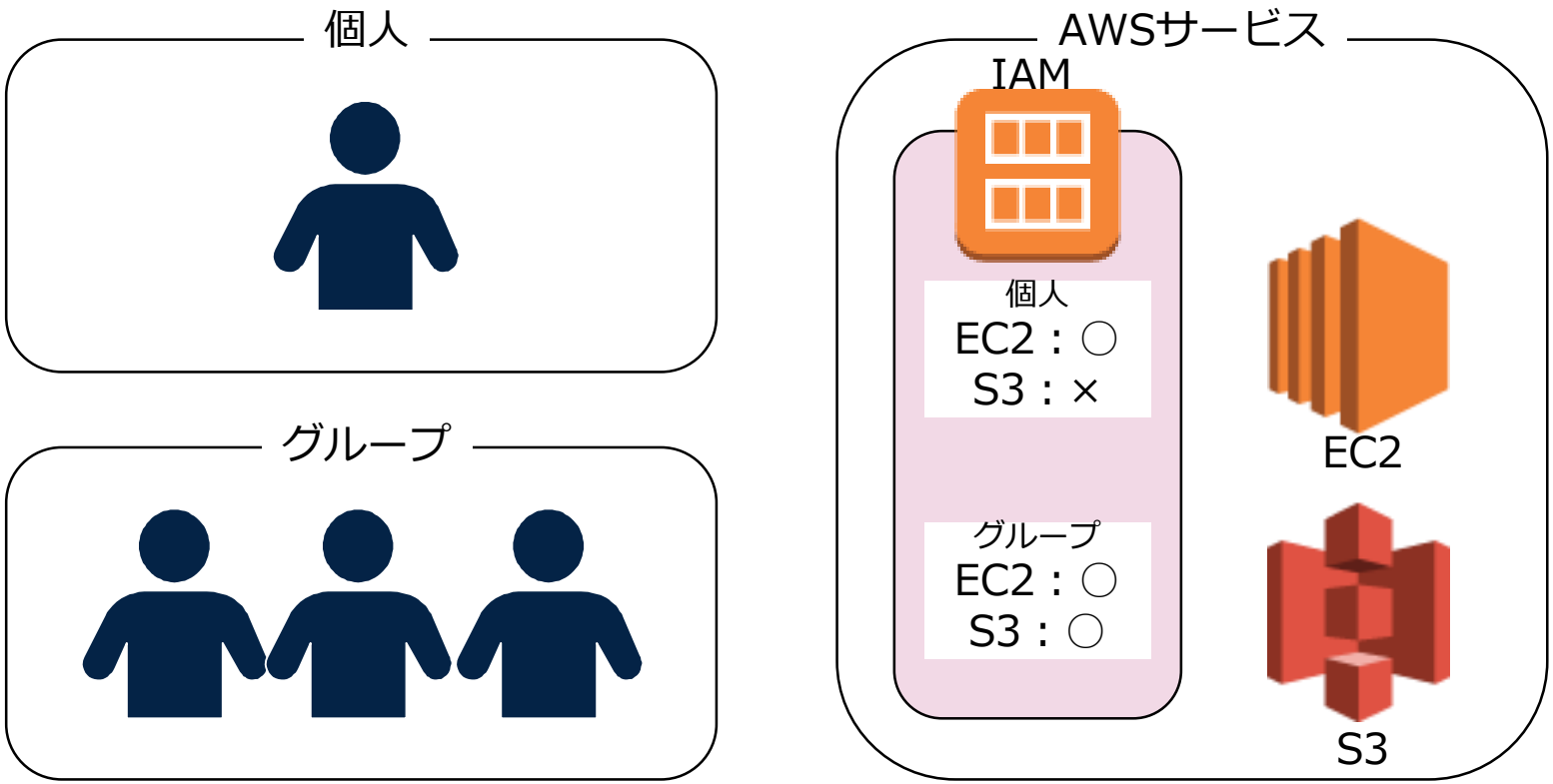
IAMとは

AWS Identity and Access Management (IAM)は安全にAWS操作を実施するための認証・認可の仕組み

- AWS利用者認証の実施
- アクセスポリシーの設定
- ユーザー個人またはグループ毎に設定

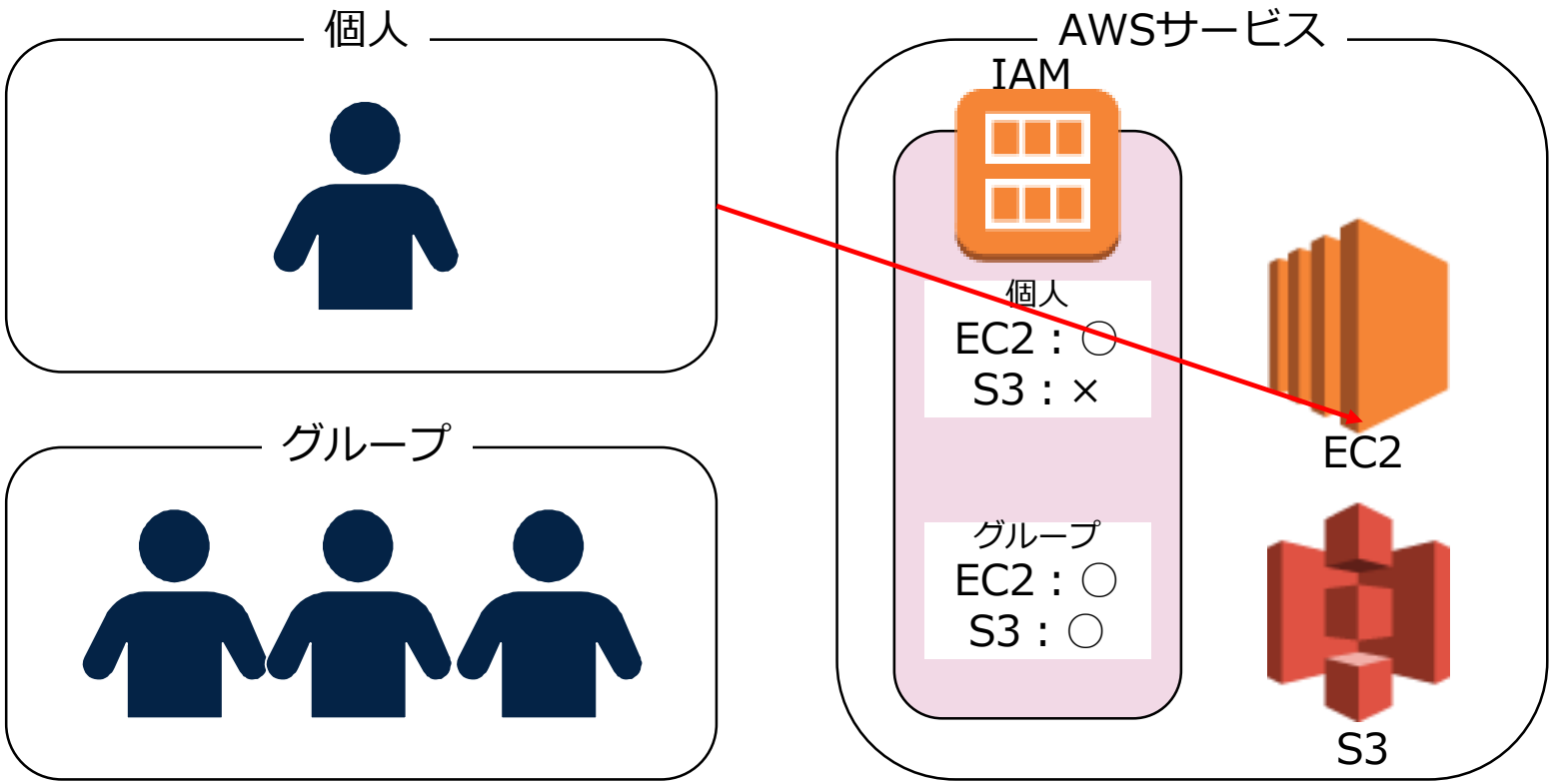
IAMとは

AWS Identity and Access Management (IAM)は安全にAWS操作を実施するための認証・認可の仕組み



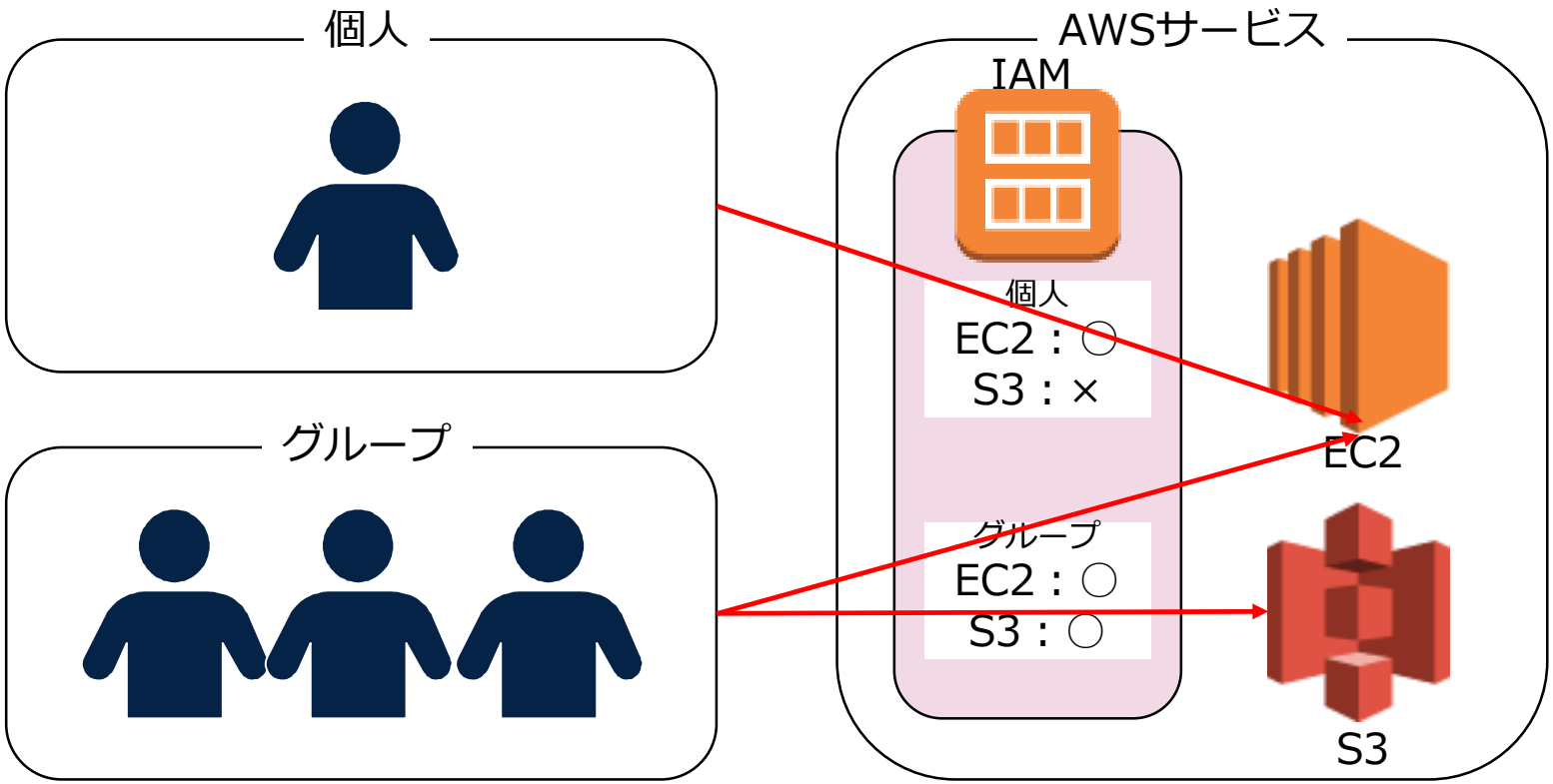
IAMとは

AWS Identity and Access Management (IAM)は安全にAWS操作を実施するための認証・認可の仕組み



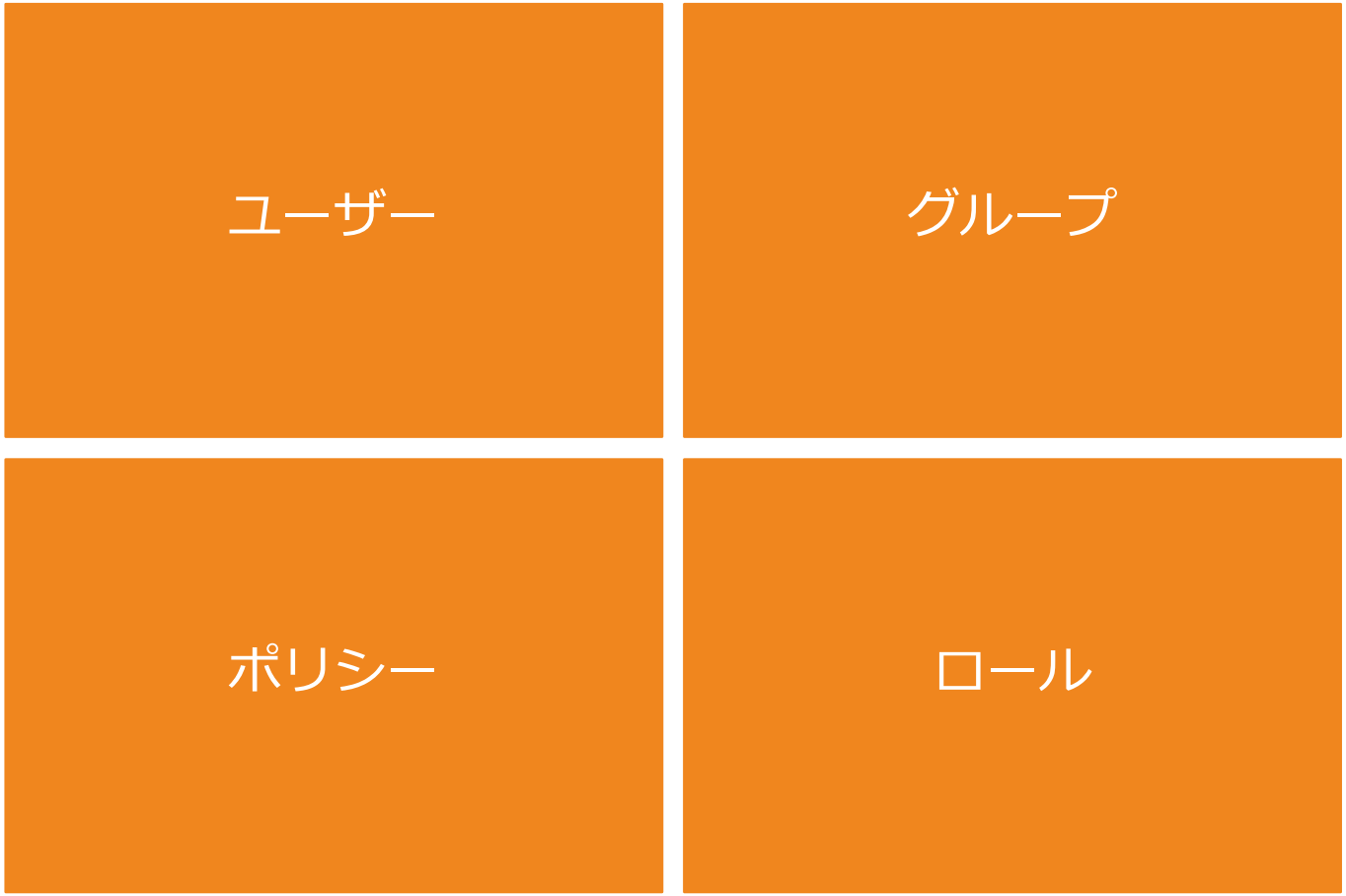
IAMとは

AWS Identity and Access Management (IAM)は安全にAWS操作を実施するための認証・認可の仕組み



主要トピック

IAMの主要トピックは前述のユーザー、グループに加えてポリシーとロールの4つ



ユーザー

- ルートユーザー
- IAMユーザー

ルートユーザー

最初に作成されるのがルートユーザーであり、通常の管理には利用しないアカウント

- AWSアカウント作成時に作られるIDアカウント
- 全てのAWSサービスとリソースを使用できる権限を有するユーザー
- 日常的なタスクはルートユーザーを使用しないことが強く推奨される

※パワーユーザーはIAMユーザーやグループの管理以外の全てのAWSサービスにフルアクセス権限を有するユーザーで別のものです。

ルートユーザー

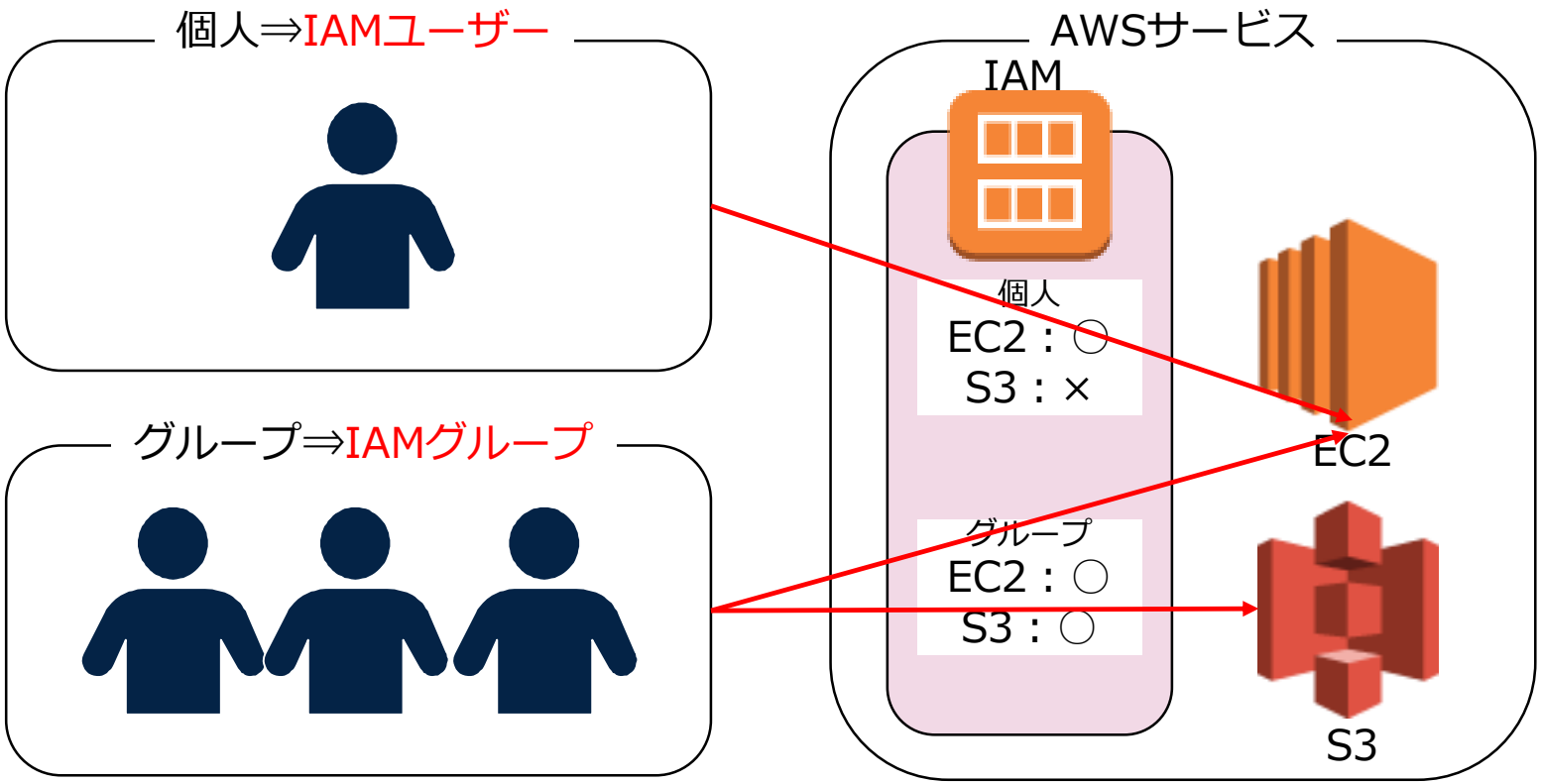
ルートユーザーにしかできない操作権限が存在する

【ルートユーザーのみの実施権限】

- AWSルートアカウントのメールアドレスやパスワードの変更
- IAMユーザーの課金情報へのアクセスに関すactivate/deactivate
- 他のAWSアカウントへのRoute53のドメイン登録の移行
- CloudFrontのキーペアの作成
- AWSサービス（サポート等）のキャンセル
- AWSアカウントの停止
- コンソリデイテッドビリングの設定
- 脆弱性診断フォームの提出
- 逆引きDNS申請

IAMユーザー

IAMポリシー内でAWSサービスを利用できるユーザー。基本操作はIAMユーザーで実施することになる



IAMユーザー

設定上限	1アカウントで5000ユーザーまで作成可能
設計内容	**ユーザー名**
	パス（オプション） ユーザーにオプションとしてセットできる情報 パスを元にユーザーの検索が可能 組織階層やプロジェクトなどをセット （例：/aws/sa/）
	所属グループ 10のグループまで設定可能
	パーミッション AWSサービスへのアクセス権限

IAMグループ

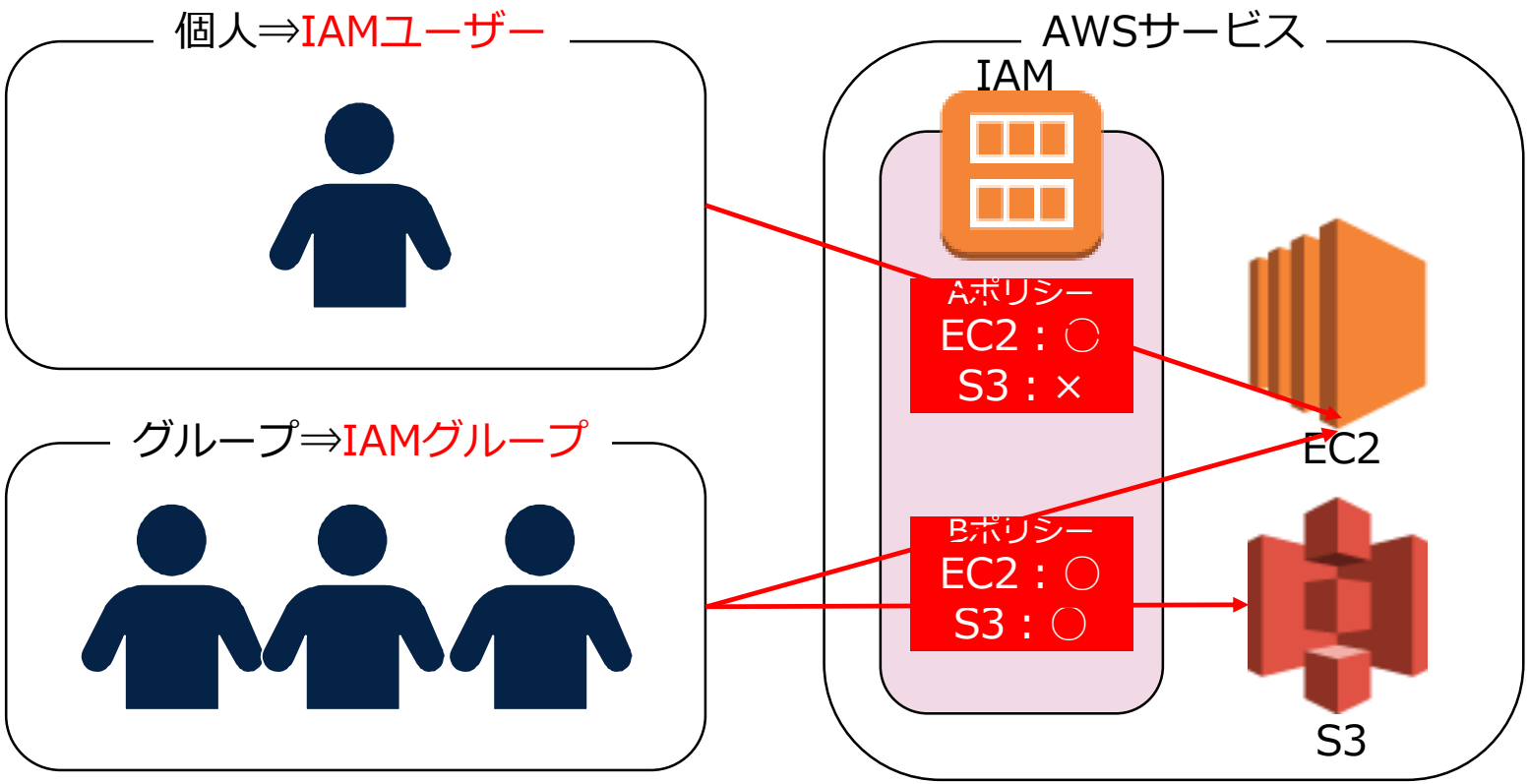
設定上限	1アカウントで100グループまで作成可能
設計内容	グループ名
	パス（オプション） 組織階層などをセット　例）/aws/
	パーミッション グループに設定したパーミッションはIAMユーザーに付与したパーミッションと同時に評価

IAMの認証方式

アクセスキーID／ シークレット アクセスキー	EC2インスタンス接続などREST/Query形式 API利用時の認証に使用する
X.509 Certificate	SOAP形式のAPIリクエスト用の認証方式
AWSマネジメントコンソールへの ログインパスワード	AWSアカウントごとに設定 デフォルトは未設定（ログインできない）
MFA(多要素認証)	その他の物理デバイスなどを利用した認証方式 AWSルートアカウントはMFAで保護して通常利用しない運用にする

IAMポリシー

IAMポリシーを作成してユーザーなどへのアクセス権限を付与（JSON形式の文書）



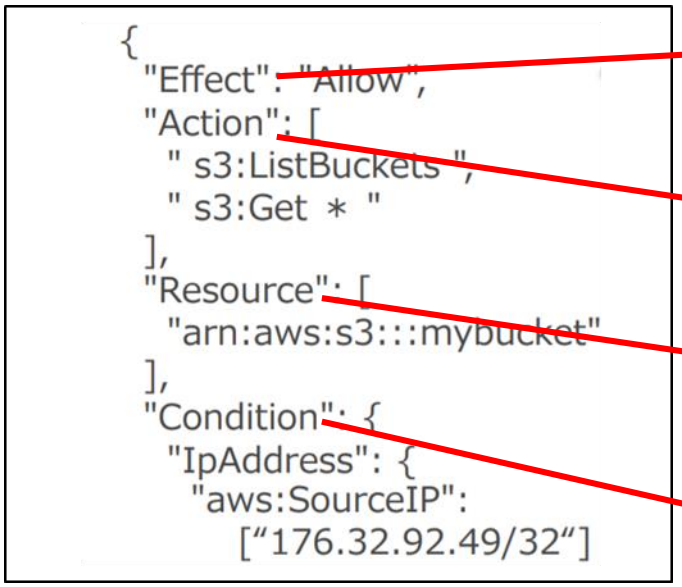
IAMポリシー

IAMポリシーを作成してユーザーなどへのアクセス権限を付与

管理ポリシー	**【AWS管理ポリシー】** AWSが作成および管理する管理ポリシー
	【カスタム管理ポリシー】 AWSアカウントで作成・管理する管理ポリシー 同じポリシーを複数のIAMエンティティにアタッチできる
インラインポリシー	**自身で作成および管理するポリシー** 1つのプリンシパルエンティティ (ユーザー、グループ、またはロール) に埋め込まれたポリシーで、プリンシパルエンティティにアタッチすることができる

IAMポリシー

IAMポリシーはJSON形式で設定される



Effect	“Allow”⇒許可 “Deny”⇒拒否
Action	対象のAWSサービス 例：”s3:Get”
Resource	対象のAWSリソース ARNで記述
Condition	アクセス制御 が有効となる条件

IAMポリシー

ユーザーベースとリソースベースのポリシー適用がある

ユーザーベース
のポリシー適用

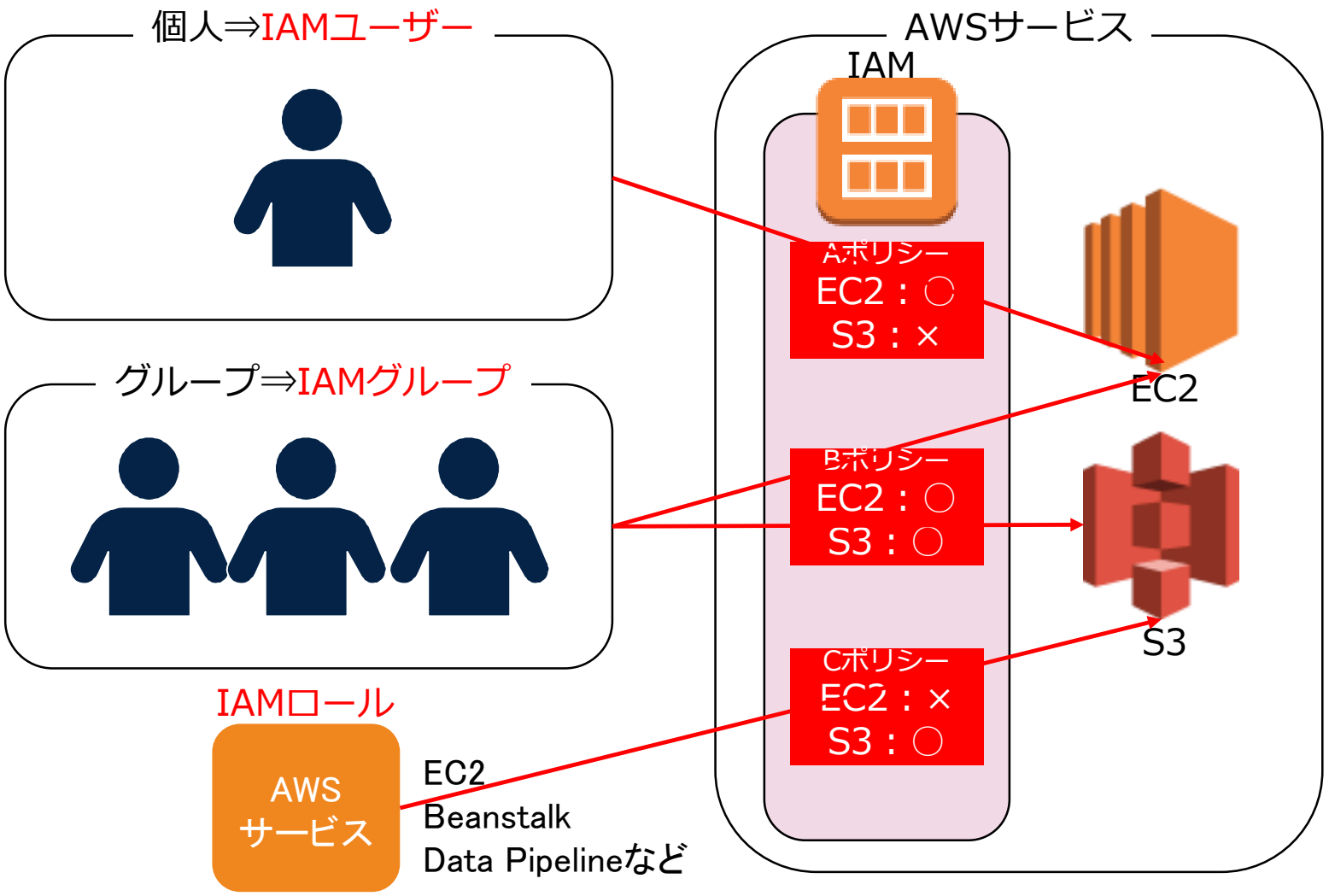
リソースベース
のポリシー適用

- S3バケット
- SNS
- SQS

⇒AWSアカウントを超したアクセス許可が可能

IAMロール

AWSリソースに対してアクセス権限をロールとして付与できる



ユーザーのアクティビティの記録

Access Advisor のService Last Accessed Data	IAMエンティティ(ユーザー、グループ、ロール)が、最後にAWSサービスにアクセスした日付と時刻を表示する機能
Credential Report	利用日時などが記録されたIAM認証情報に係るレポートファイル
AWS Config	IAMのUser、Group、Role、Policyに関して変更履歴、構成変更を管理・確認することができる機能
AWS CloudTrail	AWSインフラストラクチャ全体でアカウントアクティビティをログに記録し、継続的に監視し、保持することができる機能

アクセス権限の一時付与

一時的なアクセス権限を付与を可能にする

AWS Security Token Service(STS)	動的にIAMユーザーを作り、一時的に利用するトークンを発行するサービス
Temporary Security Credentials	AWSに対して一時的な認証情報を作成する仕組み