

IAMグループへの ポリシー適用



このハンズオンで実施する内容

1. 自社組織に必要な権限を設計する
2. 自分で独自のポリシーを作成する
3. グループを作成しポリシーを適用する



ケーススタディ：自社組織に必要な権限設計

今回のIAM設計を行う組織は以下の通りです。どのような権限を設定すべきか考えてみましょう

IT管理者

IT管理者としてルートユーザーも保持し、権限設定などの責任を負っている

運用管理者

運用管理全般を担っているスタッフで、様々なモニタリングと障害対応などで直接アプリに触れることもある

アプリ開発者

主だったAWSサービスを利用してサービス開発を行っている。



ケーススタディ：自社組織に必要な権限設計

今回のIAM設計を行う組織は以下の通りです。どのような権限を設定すべきか考えてみましょう

IT管理者

フルアクセスの管理者
権限の付与（MFAが必須）

運用管理者

運用ツール全般と開発
環境へのアクセスも付
与して、DevOpsに参
加できるようにする

アプリ開発者

担当しているアプリの
開発範囲でのみアクセ
ス権限を付与する



ケーススタディ：自社組織に必要な権限設計

今回のIAM設計を行う組織は以下の通りです。どのような権限を設定すべきか考えてみましょう

IT管理者

フルアクセスの管理者
権限の付与（MFAが必須）

管理ポリシー
Administrator

運用管理者

運用ツール全般と開発
環境へのアクセスも付
与して、DevOpsに参
加できるようにする

- ELB／EC2／RDB／
S3／Auto-Scaling／
VPC
- Config／Trail／
CloudWatch

アプリ開発者

担当しているアプリの
開発範囲でのみアクセ
ス権限を付与する

- ELB／EC2／RDB／
S3／Auto-Scaling／
VPC

