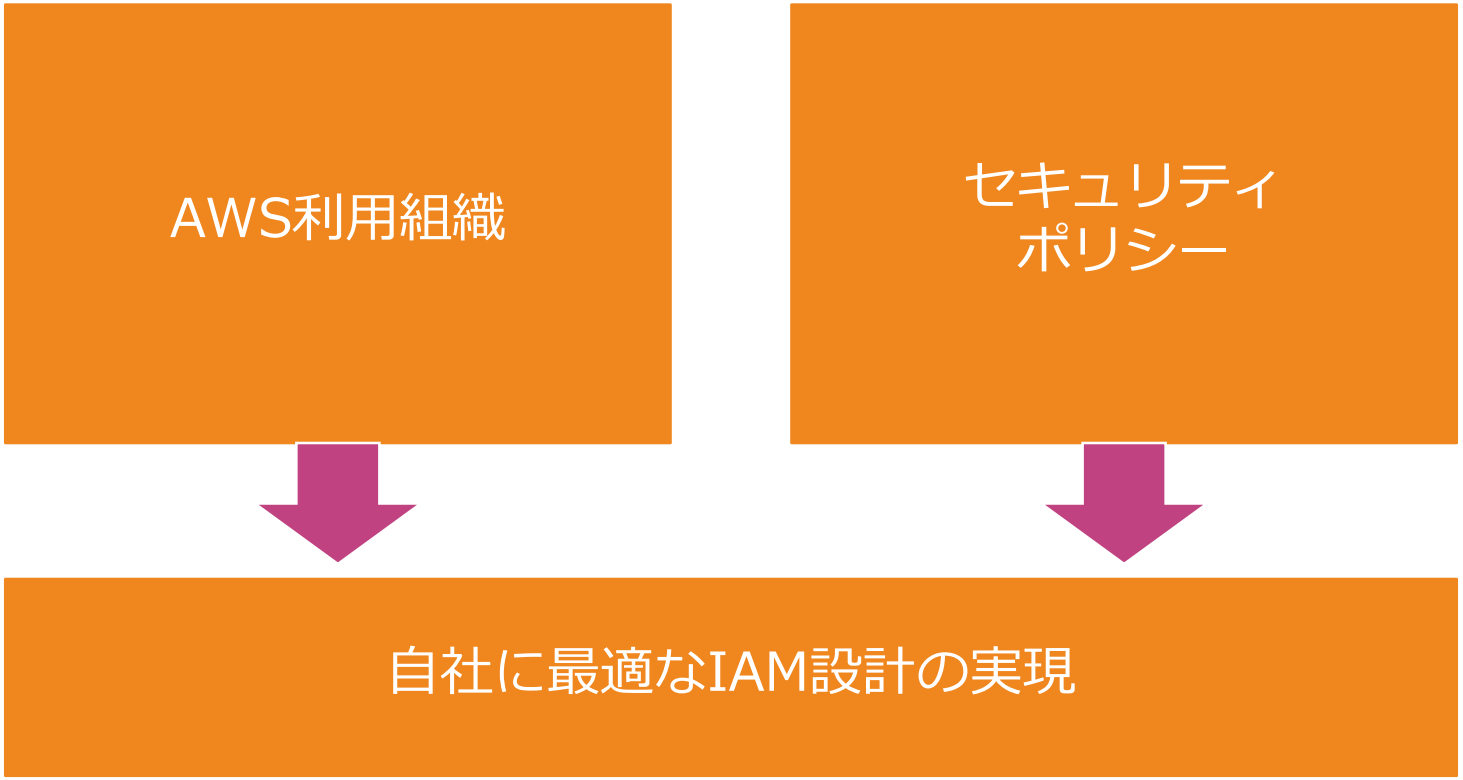
IAM設計

IAM設計

AWSを利用するユーザの役割やアクセス権限を自社の組織構造と合わせて設計することが重要



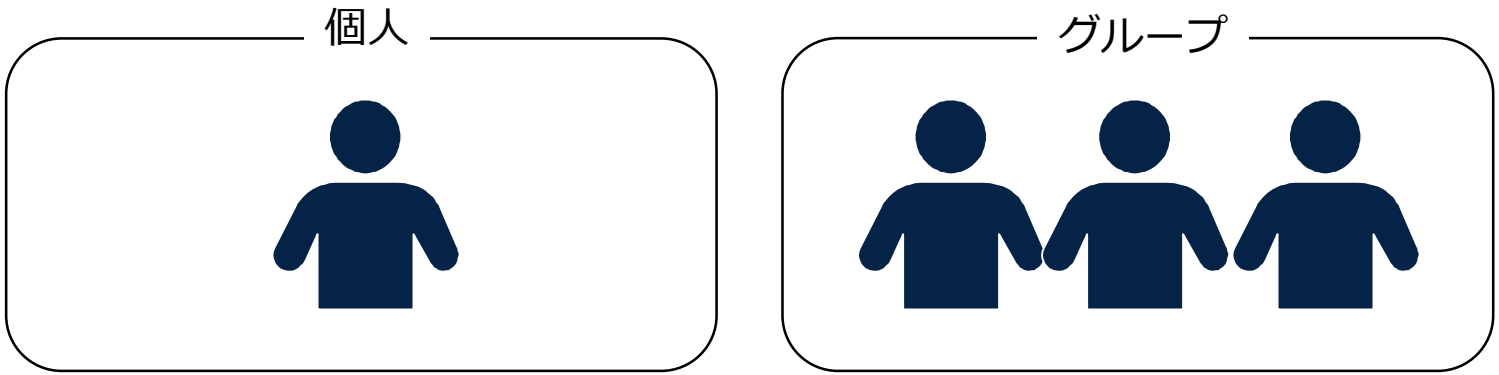
IAM設計のベストプラクティス

ベストプラクティスに沿ったIAM設計をすることが望ましい

1. アカウント設定などの必要な場合の除いて、ルートユーザーを利用しない
2. ルートユーザーなどの特権ユーザーに対して、MFA を有効化する。
3. 利用者ごとにIAMユーザーを作成する
4. 組織利用の場合は、役割ごとのIAMグループを作成してグループで管理するのを基本とする
5. 最小限の権限設定と不要な認証情報は削除を心がける
6. ユーザーのために強度の高いパスワードポリシーを設定する。
7. EC2インスタンスで作動するアプリケーションなどプログラムから利用する場合はなるべくロールを使用する。
8. モバイルやアプリケーションも含め、一時利用にはSTSなどで最小限の利用許可を与える
9. AWSアカウントのアクティビティの常に利用状況を監視する

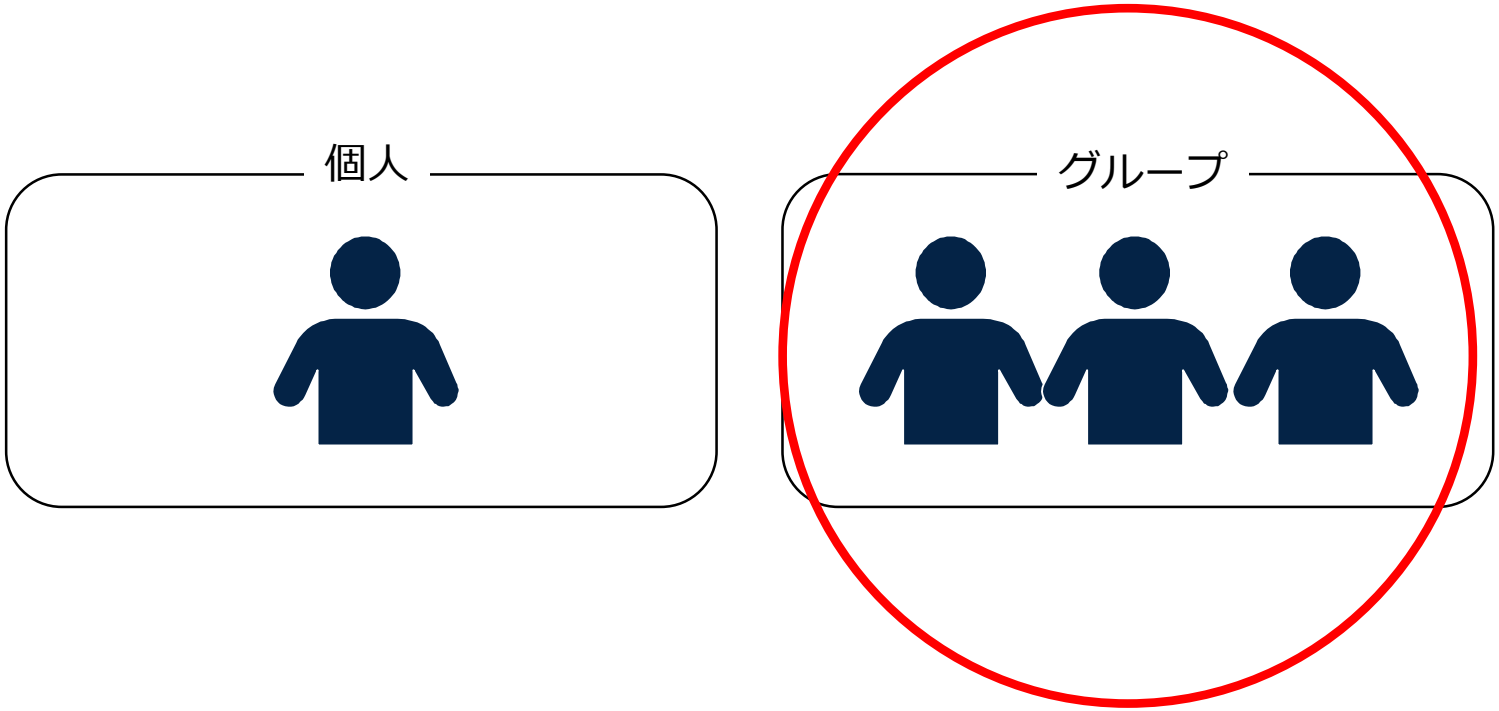
①IAMユーザー or IAMグループ

少数利用はIAMユーザーを組織利用はIAMグループを設定する



①IAMユーザー or IAMグループ

少数利用がずっと継続する場合を除いて、少数利用も含めて最初からIAMグループで設定する方が良い



②グループ設計

組織別または個人単位にAWS利用者とその役割別の利用範囲を整理して、グループ設計を実施する

AWS利用者と役割の洗い出し	利用グループへと集約
AWS利用者の特定	同じ役割や利用範囲を1つのグループとしてまとめる
利用者の役割と利用範囲を整理	グループ別の名称と最小限利用範囲を確定する