【図解/AWS】初心者にも分かりやすいIAM入門～ロールとグループとポリシーの違い,設計・設定手順について～

2020.08.01　2019.02.19

IAM とは

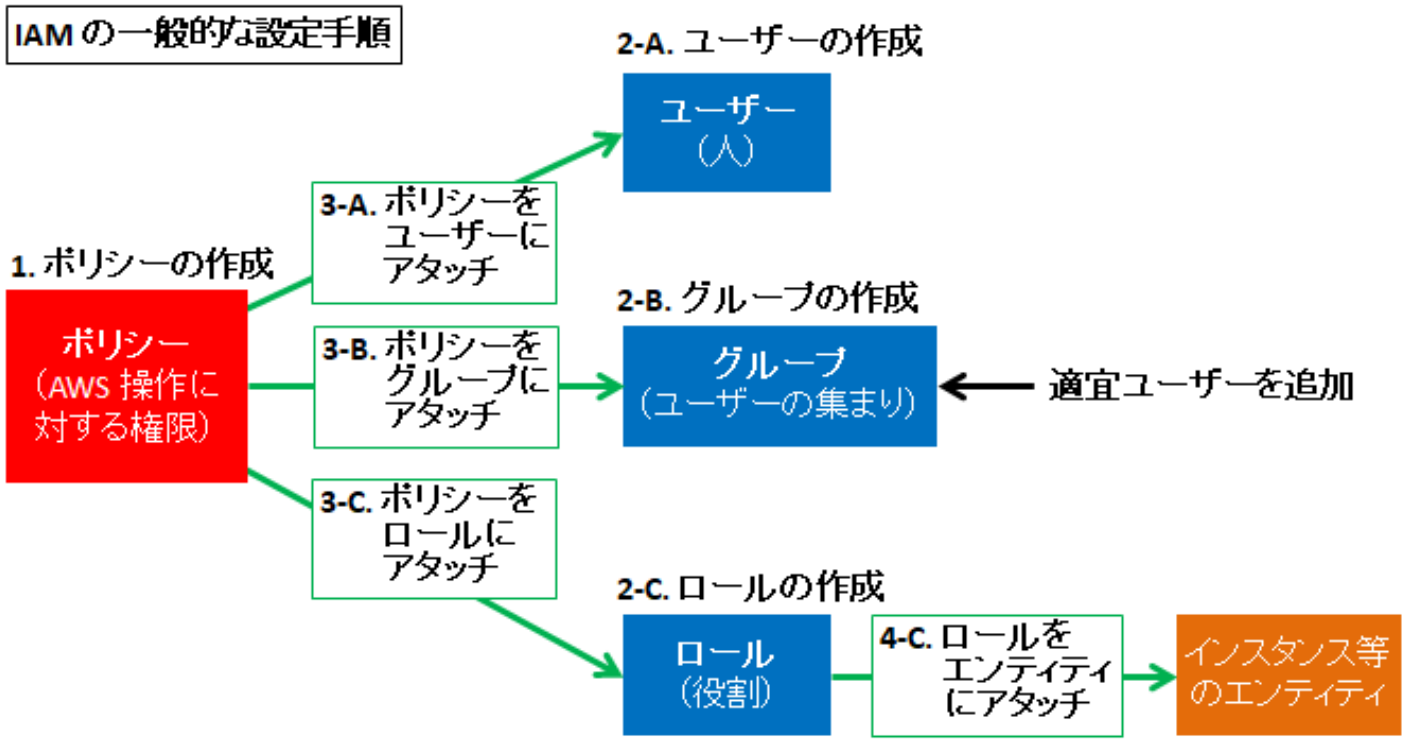
IAM (読み方：あいあむ)とは AWS Identity and Access Management サービスのことです。

IAM は AWS の操作を行うユーザや権限を一元管理する、**ユーザー元管理サービス**です。

最初は「**AWS アカウント**」という (IAM 管理外の) root アカウントにより操作しますが、このアカウントは全ての権限を持っており、**もしアカウントを乗っ取られてしまったら高額請求に繋がるような操作をされたりと危険です**。

なのでまずは IAM でユーザーを作成し、適切な権限を付与した上で「AWSアカウント」をMFA (多要素認証) 等でセキュリティをガチガチに固め、普段の操作は **IAM ユーザーで運用していくのがベストプラクティスです**。

ユーザーやグループ、ロール、ポリシーの一般的な設定手順を以下に示します。



1. ポリシーの作成
   AWS のどのリソースにどのような操作が可能かを定義
   例: S3 に対する読み取り操作
2. ユーザー or グループ or ロールの作成
3. ポリシーをユーザー or グループ or ロールにアタッチ
4. (ロールの場合は) EC2 インスタンス等のエンティティにロールをアタッチ

以降でユーザーやグループ、ロール、ポリシーがそれぞれどのような機能を持つのか、どのように違うのかを説明していきます。

ポリシーとは

ポリシーでは「AWS のどのリソースに対してどのような操作を許可するか」という「権限」を定めます。

「**誰が**」その権限を使うか、という情報は**含まれません**。

ポリシーはユーザーやグループ、ロールにアタッチ (割り当て) されて使うものですので、アタッチしたものに対してその権限が与えられます。

例えば (AWS ストレージサービスの) S3 に対する全ての操作権限を付与した「MyS3FullAccess」というポリシーを作成し、それを IAM ユーザーの Bob にアタッチ (割り当て) すると、Bob は S3 に対して全ての操作をすることができます。

ユーザーとグループ

基本的な考え方として **AWS の操作を行う人間 1 人につき IAM ユーザーを 1 つ**を作成します。

もし**同じ権限を与える人間が複数いるなら、IAM グループを作り、その中に IAM ユーザーを含めていきます**。

例えば開発部の人間に一律同じ権限を与えるのであれば「Dev」グループを作成し、そのグループに開発部の人の IAM ユーザーを含めていきます。

グループ A をグループ B に含めるようなことはできません。グループの入れ子は禁止です。

1 つの IAM ユーザーを複数のグループに含めることは可能です。

ロールとは

ロールはユーザーやグループととても似ていますが、ユーザーやグループが「人」に対して割り当てられるのに対し、**ロールは主に「(EC2 等の) インスタンス」に割り当てられるケースが多いです**。

EC2 (汎用 VM) が S3 との連携でファイルアップロードやファイル削除等の全ての操作を自動で行うためには、例えば「MyEC2Role」というロールを作成し、それに先ほどの例に出た「MyS3FullAccess」というポリシーをアタッチします。

そして EC2 に対してはそのロールをアタッチすることで、EC2 は S3 に対する全ての権限を手に入れます。

「人」が手動で行う操作の権限はユーザーやグループにポリシーをアタッチし、「インスタンス」が自動で行う操作の権限はロールにポリシーをアタッチし、インスタンスにそのロールをアタッチするのです。

ただし、厳密に言うとロールの割り当て先はインスタンスだけではありません。

AWS ではフェデレーション等の SAML 連携でログインすることも可能ですが、SAML ユーザーの ID は別組織の IdP (ID プロバイダー) によって提供されます。

そして**その SAML ユーザーがどのような権限を持つかを「ロール」をアタッチすることによって定めることができます**。

つまり、ロールの割り当てとは IAM ユーザーや IAM グループ以外の「何者か」に対して一時的に権限を与える「魔法のステッキ」を貸与するような行為なのです。

実際、ロールを割り当てられたエンティティ (何者か) は、操作を行おうとする際には都度、KMS という仕組みにより「アクセスキー」と「シークレットキー」が与えられ、その一時キーを使って操作を行います。