AWSクラウドのセキュリティ

AWSの責任共有モデル➝・お客様(クラウド「における」セキュリティに対する責任)

・

・AWS(クラウド「の」セキュリティに対する責任)

・物理的なセキュリティ、インフラストラクチャ、ネットワークインフラストラクチャ、仮想化インフラストラクチャ

サービスの特性とセキュリティの責任

アプリケーション　　　　アプリケーション アプリケーション

コンポーザ　　　　　　　コンポーザ　　　　　　コンポーザ

ストレージ　　　　　　　ストレージ　　　　　　ストレージ

ネットワーク　　　　　　ネットワーク　　　　　ネットワーク

サーバ　　　　　　　　　サーバ　　　　　　　　サーバ

Iaas Paas　　　　　　　　　Saas

(ただ使うだけ)

IAM(Identity and Access Management)

基本コンポーネント・IAMユーザー、グループ,ポリシー(ずっと),ロール(一時的)

アクセス権のタイプを選択する➝・プログラム

・マネジメントコンソール

MFA➝セキュリティー強化(二段階認証)

アイデンティティ➝認証、アクセス➝認可

ベストプラクティス➝最小権限の原則に従う(一番いい方法)

ポリシー➝許可されたり拒否

ロール➝一時的な

アカウントの保護➝ルートユーザー

1(自分の分身),3(アクセスキーを無効か削除),6(安全な場所に保存)

MFAを有効

AWSアカウントの保護➝CloudTrail(アクセスログ、管理)

Organizations

KMS➝鍵の作成・管理

Cognito➝(別アカウントでログイン可能(Google,Yahoo)

データ保護

Config(リソースの変更履歴を管理)

Artifact➝(AWSのコンプライアンスやセキュリティレポートをダウンロード)