認証と認可

- ルートユーザ:AWSアカウント自体のユーザ。Emailアドレスとパスワードで認証。全権限をもつ。
  - Power User:IAM管理以外の全権限をもつユーザ設定。
- IAM:認証と認可(権限)のサービス。
  - IAMポリシー：AWSサービスへの権限設定を記述したファイル。
    - AWS 管理ポリシー:デフォルトで用意されているポリシー。
    - カスタマー管理ポリシー:ユーザが自分で作成したポリシー。
    - インラインポリシー:IAMユーザなどに直接記述するポリシー。使いまわしができない。非推奨。

- IAMユーザー：AWSアカウント内で作成可能なユーザアカウント。IAMポリシーをアタッチして、権限設定可能。
  - ユーザ名とパスワード、またはアクセスキーによってAWSサービスを使用する。
- IAMグループ：IAMユーザのグループ。複数ユーザに対してアクセス許可を一括指定可能。
- IAMロール：AWSリソースなどに対してアクセス許可を与えるもの。EC2インスタンスなどにアタッチしてい使用する。
  - STSによって一時的認証情報を発行してAWSサービスを使用する。

- Organizations:AWSアカウントの統合管理機能。「ルートユーザ」の管理。
  - OU:Organizations Unit。組織単位。ユーザーのグループ。
  - SCP:Security Control Policy。権限「範囲」設定ファイル。OUやユーザに付与する。
    - 「拒否」されたアクションはそのアカウント内の設定にかかわらず拒否される。
    - 「許可」されたアクションは、そのアカウント内で「許可」されれば許可される。
  - 一括請求(コンソリデーティッドビリング)：複数アカウントの請求を一括して行うことができる。RIの共有、S3の割引が可能。

- Cognito: アプリケーションの認証と認可機能を作成するサービス。AWSアカウントなどの認証・認可設定ではない。
- ADS:Active Directory Service。AWSとADの連携などのサービス。
- MFA:多要素認証。ルートユーザ・IAMユーザなどに設定し、セキュリティを高めることができる。
- 最小権限の原則：アクセス許可は最小範囲で許可するべきという原則。
- S3バケットポリシー：S3バケットに対する権限設定ファイル。
- STS:Security token Service。一時的認証情報発行サービス。CognitoやIAMロールで使用されている。

IAMのベストプラクティス(一部)

- AWS アカウントルートユーザーのアクセスキーをロックする
- インラインポリシーではなくカスタマー管理ポリシーを使用する
- MFA の有効化
- Amazon EC2 インスタンスで実行するアプリケーションに対し、ロールを使用する
- 認証情報を定期的にローテーションする。

類題

問題19： 不正解
B社には1000人の従業員がいます。 各部門や担当グループ別にAWSアクセスを設定したいと考えています。IAMのどのような設定を利用するべきですか？

問題28： 不正解
1000人以上いる会社において各部門のユーザーにAWSのアクセス権限を付与して、管理したいと考えています。その際に、利用するべきサービスと設定方法を選択してください。

問題20： 正解
AWSコンソールにログインするときに、ユーザー名とパスワードに加えて、高いセキュリティを提供するために使用できる機能はどれでしょうか？

問題32： 不正解
会社の新規に作成するAWSアカウントをコントロールして、アカウント内のエンティティに必要なAWSサービスへのアクセスのみに許可を与える必要があります。どのサービスを利用するべきですか？

問題40： 不正解
A社では多数の開発者がAWSリソースを使用しています。 次のサービスのうち、開発者によるAWSリソース利用を直接的に制御するためのサービスはどれでしょうか？

セキュリティ

- WAF:Web Application Firewall。L7ファイアウォール。SQLインジェクションやDDoS攻撃などを防げるほか、URLベースのアクセス制御が可能。CloudFront、ALB、API Gateway、AppSyncにデプロイ可能。
- Shield Standard：DDoS攻撃をL4で防御するためのサービス。基本デフォルトで動作している(らしい)。CloudFront、Route53とともに使用。
- Shield Advanced:より高度な機能が追加されたShield。WAFと統合されており、24時間365日専門家チームに相談可能。

- Inspector:EC2インスタンスを分析・脆弱性のチェックをするサービス。インスタンス「内部」の設定やアプリをチェックする。
- GuardDuty:不正アクティビティのモニタリングサービス(脅威検知サービス)。AIを利用して、あやしい攻撃を検知。
- Macie:機密データ検出サービス。個人情報 (PII) などの重要情報がS3のオブジェクトに含まれている場合、自動検知。
- KMS:Key Management Service。暗号鍵の発行・管理サービス。
- CloudHSM:Hardware Security Module。FIPS 140-2 のレベル 3 認証済みのハードウェアに暗号鍵を保存。コンプライアンスなどが厳しい場合、KSMではなくこちらを使用する。

- Network Firewall:VPCのマネージドファイアウォール。簡単にトラフィック制御やフィルタリングが可能。らしい。
  - 「侵入防止システム (IPS) 」を提供。
- Firewall Manager:Organizationsにおける複数アカウントのWAFを一括管理。
- SecurityHub:AWSのセキュリティ関連サービスを集約して確認・管理可能なサービス。
- Detective:GuardDutyなどによるインシデント(問題)検知時に、根本原因は複数リソースから「調査」するサービス。
- Fault Injection Simulator:わざと障害を発生させる実験サービス。

そのほか

- CodeGuru:自動コードレビューサービス。コードのセキュリティの脆弱性やバグなどを特定し、推奨事項を提供する。
- X-Ray:分散アプリケーションの分析とデバッグサービス。Lambdaなどを複数組み合わせたサービスにおいて、アクセス速度などを計測し可視化。ボトルネックなどを特定可能。
- ACM:AWS Certifcate Manager。SSL/TLS証明書の作成・管理などをするサービス。https接続などのために使用。
- Secrets Manager:秘密情報の管理・ローテーションサービス。パスワードなどをサービスに直接記述せずに管理できる。

類題

問題39： 正解
SQLインジェクションやアプリケーションコードの脆弱性からWebアプリケーションを保護するのに役立つサービスはどれですか？

問題45： 正解
事前に定義されたテンプレートに基づいてEC2インスタンスを分析し、脆弱性をチェックするサービスはどれでしょうか？

問題27： 不正解
VPC経由のネットワークトラフィックに対してファイアーウォールや侵入防止システムを提供するサービスはどれでしょうか？

問題30： 正解
次のAWSサービスの中で、欧米などで求められる業界標準の暗号化対応実施を保証するために利用されるサービスはどれでしょうか？

問題54： 不正解

コスト最適化

- Pricing Calculator：サービスの使用量などを入力して、請求額を「見積もる」ツール。https://calculator.aws/
- TCO計算ツール：AWS利用時の総コスト算出ツール。オンプレや他のクラウドから移行する際に使用。
- 請求ダッシュボード:AWSマネジメントコンソールのページ。Cost Exporerなどの請求系サービスやリンクがそろっている。
- Cost Explorer:コスト予測分析・可視化ツール。現在の使用量から、月額のコスト予想や使用データの傾向分析・異常特定などを行う。

- Budgets:予算設定管理サービス。コストと使用状況が予算の設定値を超える、あるいはRIおよびSavings Plansの使用率やカバレッジが設定値を下回る場合に、Eメールなどで通知。
- 請求アラート(Billing alarm):請求額が設定値に達した場合に通知する機能。
- コストと使用状況レポート:AWSリソース使用状況・コストのレポートをS3に保存するサービス。詳細情報の一覧で、SQLなどで分析して使用。

- コスト配分タグ:リソースに付与して、請求レポートなどで請求金額を分類するためのタグ。Billingのページから有効化して使用する。
- Compute Optimizer:機械学習を用いたコスト削減・パフォーマンス最適化提案サービス。EC2、AutoScalingグループ、EBS、Lambdaに対応。

類題

問題3： 正解
AWSの毎月の請求額を見積もる際に使用できるツールは次のうちどれですか？

問題64： 正解
コストを可視化して確認するための分析用のブラウザとして利用できるサービスはどれでしょうか？

問題29： 正解
リザーブドインスタンス（RI）または Savings Plans の集計使用率とカバレッジメトリクスを管理するAWSサービスを選択してください。

問題47： 正解
EC2インスタンスの最適な利用を機械学習によって検証するために利用するべきサービスはどれでしょうか？