モジュール6, 7レポート

* AWS共同責任モデル - AWSはユーザー環境の一部を担当し、顧客は他の部分を担当します。 この概念は、共同責任モデルとして知られています。共同責任モデルは顧客責任とAWS責任に分けられます。
* 顧客責任 - お客様はAWSクラウド内で生成し、配置するすべてのセキュリティを担当します。 AWSサービスを使用する際、顧客は独自のコンテンツに対する完全な制御を維持します。 お客様が行うセキュリティステップは、使用するサービス、システムの複雑さ、会社ごとの運用、およびセキュリティ要求事項などの要素によって異なります。
* AWS責任 - AWSはクラウド自体のセキュリティを担当します。 AWSは、インフラストラクチャのすべての階層でコンポーネントを運用、管理、および制御します。 AWSはクラウド自体のセキュリティ、特にリソースをホストする物理的インフラを管理します。 これには次のものが含まれます。
  + データセンターの物理的セキュリティ
  + ハードウェアおよびソフトウェアインフラストラクチャ
  + ネットワーク·インフラ
  + 仮想化インフラ
* AWS Identity and Access Management(IAM) - IAMは会社固有の運営及びセキュリティ要求事項に従ってアクセス権限を構成できる柔軟性を提供します。 この作業を遂行するために、次のようなIAM機能を組み合わせて使用します。
  + IAM ユーザー、グループ、および役割
  + IAM政策
  + 多要素認証 (MFA)
* AWSアカウントルートユーザー - AWSアカウントを最初に作成すると、ルートユーザ資格証明から始まります。 このユーザーは、アカウント内のすべてのAWSサービスとリソースへの完全なアクセス権を持っています。
* IAMユーザー - IAMユーザーは、ユーザーがAWSで生成する資格情報です。 IAMユーザーがAWSでAmazon EC2インスタンスの開始、Amazon S3バケットの生成など、特定の作業を実行できるように許可するには、IAMユーザーに必要な権限を付与する必要があります。
* IAMポリシー - IAMポリシーは、AWSサービスおよびリソースに対する権限を許可または拒否する文書です。 IAM ポリシーを使用すると、ユーザーがリソースにアクセスできるレベルをカスタマイズできます。
* IAMグループ - IAMグループはIAMユーザーの集まりです。 グループにIAMポリシーを割り当てると、そのグループのすべてのユーザーにポリシーに指定された権限が付与されます。
* IAMロール - IAMロールは臨時に権限にアクセスするために受任できる資格証明です。IAMロールを受任するということは、以前の役割に指定されたすべての以前の権限を放棄し、新しい役割に指定された権限を受任することです。
* 多要素認証 (MFA) -  多要素認証 (MFA) はAWSアカウントに追加のセキュリティ層を提供します。
* AWS Organizations - AWS Organizationsでは、サービス制御ポリシー(SCP)を使用して、組織のアカウントに対する権限を中央で制御することができます。 SCPを使用すると、各アカウントのユーザーと役割がアクセスできるAWSサービス、リソース、および個別API作業を制限することができます。
* 組織単位(OU) - AWS Organizationsでは、アカウントを組織単位(OU)にグループ化し、同様のビジネスまたはセキュリティ要件を持つアカウントを簡単に管理できます。 OUにポリシーを適用すると、OUのすべてのアカウントがポリシーに指定された権限を自動的に継承します。
* AWS Artifact - AWS Artifactは、AWSセキュリティおよびコンプライアンスレポート、および一部のオンライン契約に対するオンデマンドアクセスを提供するサービスです。 AWS Artifactは、AWS Artifact Agreements及びAWS Artifact Reportsの二つの基本セクションで構成されます。
  + AWS Artifact Agreements - AWS Artifact契約で個別アカウント及びAWS Organizations内のすべてのアカウントに対する契約を検討、受諾、管理することができます。
  + AWS Artifact Reports - AWS Artifact報告書は、外部監査機関が作成したコンプライアンス報告書を提供します。
* DoS - ユーザーがウェブサイトまたはアプリケーションを利用できないようにする意図的な試みです。
* DDoS - 複数のソースを使用して、ウェブサイトまたはアプリケーションを無効にする攻撃を開始します。
* AWS Shield - AWS ShieldはDDoS攻撃からアプリケーションを保護するサービスです。 AWS ShieldはStandard及びAdvancedの二つの保護レベルを提供します。
  + AWS Shield Standard - ネットワークトラフィックがアプリケーションに入ると、AWS Shield Standardは様々な分析手法を使用してリアルタイムで悪性トラフィックを探知し、自動的に緩和します。
  + AWS Shield Advanced - 詳細な攻撃診断および精巧なDDoS攻撃を探知·緩和できる機能を提供する有料サービスです。
* AWS Key Management Service(AWS KMS) - AWS KMSを使用して、暗号化キーを生成、管理、および使用することができます。 また、幅広いサービスやアプリケーションでキーの使用を制御できます。
* AWS WAF - ウェブ アプリケーションで着信するネットワーク リクエストを監視できるウェブ アプリケーション ファイアウォールです。 Amazon Cloud Front及びApplication Load Balancerと一緒に動作します。
* Amazon Inspector - 自動化されたセキュリティ評価を実行して、アプリケーションのセキュリティとコンプライアンスを改善できるサービスです。
* Amazon GuardDuty - AWSインフラおよびリソースに対する知能型脅威探知機能を提供するサービスです。
* Amazon CloudWatch - Amazon CloudWatchは、様々な指標をモニタリング·管理し、その指標のデータに基づいて警報作業を構成できるウェブサービスです。
* Cloudwatchアラーム - CloudWatchを使用すると、指標の値があらかじめ定義されたしきい値を上回ったり下回ったりする場合、自動的に作業を行うアラートを生成することができます。
* CloudWatchダッシュボード - CloudWatchダッシュボード機能を使用すると、単一の場所でリソースに関するすべての指標にアクセスできます。
* AWS CloudTrail - AWS CloudTrailは、アカウントに対するAPI呼び出しを記録します。 記録される情報には、API呼び出し者ID、API呼び出し時間、API呼び出し者のソースIPアドレスなどが含まれます。
* CloudTrail Insights - CloudTrailでCloudTrail Insightsを有効にすることもできます。 このオプション機能を使用すると、CloudTrailがAWSアカウントで異常なAPI活動を自動的に検出することができます。
* AWS Trusted Advisor - AWS環境を検査し、AWSのベストプラクティスに従ってリアルタイムで推奨事項を提示するウェブサービスです。 Trusted Advisorはコスト最適化、性能、セキュリティ、耐欠陥性、サービス限度という5つのカテゴリーで結果をAWSのベストプラクティスと比較します。 各カテゴリの検査に対して推奨作業リストを提供し、AWSのベストプラクティスを詳細に調べることができる追加資料を提供します。
* AWS Trusted Advisorダッシュボード - AWS管理コンソールでTrusted Advisorダッシュボードにアクセスすると、コスト最適化、性能、セキュリティ、耐欠陥性、サービス限度のカテゴリで完了した検査を検討することができます。
  + 緑のチェックマークは、問題が検出されていないアイテムの数を示します。
  + オレンジ色の三角形は、推奨調査項目の数を示します。
  + 赤い丸は、推奨措置数を示します。