1. AWS共同責任モデル  
 1) 顧客責任 - クラウド内のセキュリティ  
 顧客データ  
 プラットフォーム、アプリケーション、Identity and Access Management(IAM)  
 オペレーティングシステム、ネットワーク/ファイアウォール構成  
 クライアント側データの暗号化、サーバー側データの暗号化、ネットワーキング トラフィックの保護  
 Amazon EC2 インスタンスで実行するオペレーティング システムを選択、構成、およびパッチを適用する段階、セキュリティ グループを構成する段階、ユーザー アカウントを管理する段階を含む  
  
 2) AWS責任 - クラウド自体のセキュリティ  
 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  
 - ソフトウェア: コンピューティング、ストレージ、データベース、ネットワーキング  
 - ハードウェア:リージョン、可用領域、エッジロケーション  
 ネットワーク·インフラ  
 仮想化インフラ

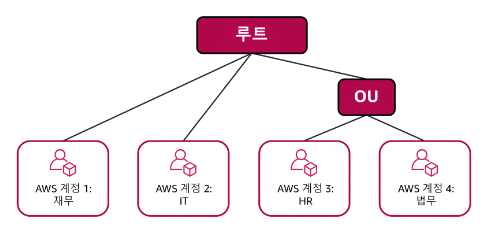
2. AWS Identity and Access Management(IAM)

AWSサービスとリソースへのアクセスを安全に管理できる。  
 次のようなIAM機能を組み合わせて使用  
 - IAM ユーザー、グループ、および役割  
 - IAM政策  
 - 多重認証(MFA)  
  
 1) AWSアカウントルートユーザー  
 AWSアカウントを初めて作ったらルートユーザーという資格証明でスタート  
 アカウントのすべてのAWSサービスおよびリソースに対する全体アクセス権限を持つ  
 ルートユーザ生成 -> ルートユーザがIAMユーザを生成後、他のユーザ生成権限を提供 -> 新しいIAMユーザでログインし、引き続き他のユーザを生成 -> 限られた数の作業に対してのみルートユーザにアクセス  
 ベスト プラクティス: 日常作業にはルート ユーザーを使用しない。 ルートユーザーは、メールアドレスの変更、AWS Support プランの変更などの作業にのみ使用  
  
 2) IAMユーザー  
 ユーザーがAWSで生成する資格情報  
 名前と資格証明で構成される。  
 IAMユーザーに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行えるように許可するには、IAMユーザーに必要な権限を付与しなければならない。  
 ベストプラクティス:AWSにアクセスすべきユーザごとに個別のIAMユーザを生成することが望ましい。  
  
 3) IAM政策  
 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  
 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することができる。  
 ベストプラクティス:権限付与時の最小権限セキュリティ原則に従う。  
 作業を遂行するのに必要なものより多くの権限を持つことを防止することができる。  
  
 4) IAMグループ  
 IAMユーザーのコレクション  
 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る  
 例:コーヒーショップで計算員グループを作成 - 計算員1、計算員2、計算員3  
 計算員1がインベントリ担当者になる場合、計算員グループから削除した後、インベントリグループに追加  
  
 5) IAMロール  
 一時的に権限にアクセスするために受任できる資格情報  
 職員が他の職務に転換しなければならない場合、あるワークステーションへのアクセス権限を放棄し、次のワークステーションにアクセスすることができる。 この職員は複数のワークステーションの間を簡単に切り替えることができるが、特定の時点では単一のワークステーションだけがアクセスできる。  
 ベストプラクティス : IAM 役割は、サービスまたはリソースへのアクセス権限を長期的ではなく、一時的に付与しなければならない状況に理想的である。  
  
 6) 多重認証(MFA)  
 AWSアカウントに追加のセキュリティ層を提供  
 例）暗号入力後、携帯電話に送信された乱数コードのような2番目の認証形式を提供すること  
 - MFA作動方式  
 IAMユーザID、パスワードを入力してログイン->AWS MFAデバイスの認証応答を入力しろというメッセージが表示(デバイス:ハードウェアセキュリティキー、ハードウェアデバイス、またはスマートフォンのようなデバイスのMFAアプリケーション)->ユーザが正常に認証されれば、要請されたAWSサービスまたはリソースにアクセスできる。

3. AWS Organizations

会社に複数のAWSアカウントがあれば、AWS Organizationsを使用して中央位置で複数のAWSアカウントを統合し、管理することができる。  
 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る。

4. 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、似たようなビジネスまたはセキュリティ要求事項があるアカウントを簡単に管理することができる。  
  
 - 企業でAWS Organizationsを使用する方法の例



HR部署と法務部署は同じAWSサービスおよびリソースにアクセスしなければならないため、一つのOUに一緒に配置することができる。 一つのOUに配置した後は、HR部署と法務部署の両方のAWSアカウントに適用されるポリシーを接続することができる。  
  
 AWS Organizationsでサービス制御ポリシー（SCP）を組織ルート、個別メンバーアカウント、またはOUに適用することができる。 SCPはAWSアカウントルートユーザーを含め、アカウント内のすべてのIAMユーザー、グループ、および役割に影響を与える。  
 IAMポリシーは、IAM ユーザー、グループ、または役割に適用することができる。  
 AWSアカウントルートユーザーにはIAMポリシーを適用できない。

5. AWS Artifact

1) AWS Artifact契約  
 - 会社でAWSサービス全体で特定タイプの情報を使用するためにAWSと契約を締結しなければならないと仮定すれば、AWS Artifact契約を通じて遂行することができる。  
 AWS Artifact契約で個別アカウントおよび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る。 特定規定の適用を受ける顧客の要求事項を解決するための多様なタイプの契約が提供される。

2) AWS Artifact レポート  
 - 会社の開発チームのメンバー1人がアプリケーションをビルドする途中、特定の規制標準を遵守することに対する責任に関する追加情報が必要だと仮定すれば、AWS Artifact報告書でこの情報にアクセスするよう助言することができる。

6. 顧客コンプライアンスセンター  
 AWS規定遵守について詳しく調べることができるリソースが含まれている。  
 次のようなテーマに関するコンプライアンス白書および説明書にアクセスできる。  
 ● 主なコンプライアンス質問に対するAWS回答  
 ● AWS危険及びコンプライアンスの概要  
 ● セキュリティ監査チェックリスト

7. サービス拒否攻撃  
 DoS攻撃は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  
 例）攻撃者は、標的としたウェブサイトまたはアプリケーションに過負荷がかかり、これ以上応答できないまで、ウェブサイトまたはアプリケーションを過度なネットワークトラフィックでフラッドすることができる。  
 ウェブサイトまたはアプリケーションが使用できなくなると、合法的なリクエストを試みるユーザーへのサービスを拒否する。

8. 分散サービス拒否攻撃  
 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する。 攻撃者はグループかもしれないし、さらには1人かもしれない。 単一の攻撃者は、感染した複数のコンピュータを使用して、過度のトラフィックをウェブサイトまたはアプリケーションに送信することができる。  
 DoSおよびDDoS攻撃がアプリケーションに及ぼす影響を最小化するために、AWS Shieldを使用することができる。

9. AWS Shield  
 DDoS攻撃からアプリケーションを保護するサービス  
 Standard及びAdvancedの二つの保護レベルを提供  
  
 - AWS Shield Standard  
 : すべてのAWS顧客を自動的に保護する無料サービス  
 AWSリソースを最も頻繁に発生する一般的なDDoS攻撃から保護  
 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  
  
 - AWS Shield Advanced  
 : 詳細な攻撃診断と精巧なDDoS攻撃を探知·緩和できる機能を提供する有料サービス  
 Amazon Cloud Front、Amazon Route 53、Elastic Load Balancingといった他のサービスとも統合される。 また、複雑なDDoS攻撃を緩和するためのユーザ指定規則を作成し、AWS ShieldをAWS WAFと統合することができる。

10. AWS Key Management Service(AWS KMS)

保存状態で（保存時に暗号化）、そして転送される間（転送中に暗号化という）、アプリケーションのデータが安全であることを確認しなければならない。  
 AWS Key Management Service（AWS KMS）を使用すると、暗号化キーを使用して暗号化作業を行うことができる。  
 暗号化キーは、データロック（暗号化）やロック解除（暗号解読）に使用される任意の数字文字列  
 鍵を管理できるIAM ユーザー及び役割を指定することができる。

11. AWS WAF

ウェブアプリケーションに入ってくるネットワークリクエストをモニタリングできるウェブアプリケーションファイアウォール  
 Amazon CloudFront 及び Application Load Balancerと一緒に作動  
  - AWS WAFを使用して特定のリクエストを許可し、ブロックする方法の例  
 アプリケーションが複数のIPアドレスから悪意のあるネットワーク要請を受けていると仮定すると  
 これらの要求がアプリケーションにアクセスし続けるのを防ぐ必要があるが、合法的なユーザーは依然としてアプリケーションにアクセスできるようにする必要がある。 指定したIPアドレスから出た要請を除いたすべての要請を許容するようにウェブACLを構成する。  
 AWS WAFは要請が入ってくると、ウェブACLで構成したルールリストを確認  
 リクエストがブロックされたIPアドレスのいずれかから出てこない場合は、アプリケーションへのアクセスを許可します  
 しかし、要請がウェブACLで指定したブロックIPアドレスのいずれかから出た場合、AWS WAFがアクセスを拒否

12. 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  
 Amazon EC2 インスタンスへのオープンアクセス、脆弱なソフトウェアバージョンのインストールなどのセキュリティベストプラクティス違反およびセキュリティ脆弱性をアプリケーションで検査  
 評価を行った後にセキュリティ検知結果リストを提供  
 このリストは深刻度レベルによって優先順位が決定され、各セキュリティ問題に対する詳しい説明および推奨解決方法が含まれています  
 共同責任モデルによって、顧客はAWSサービスで実行されるアプリケーション、プロセス、およびツールのセキュリティに対する責任がある。

13. 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  
AWS環境内のネットワーク活動及びアカウント動作を継続的にモニタリングし、脅威を識別  
  
 Amazon GuardDuty使用の4つの主要段階  
 - 活性化  
 - 分析  
 - 知能的に探知  
 - 結果を検討して措置  
 AWSアカウントでGuardDutyを有効にすると、GuardDutyがネットワークおよびアカウント活動をモニタリングし始める  
 GuardDutyは、VPC Flow LogsおよびDNSログをはじめとする複数のAWSソースのデータを継続的に分析  
 GuardDutyが脅威を探知した場合、AWS管理コンソールで脅威に対する詳細な探知結果を検討することができる。  
 探知結果には問題解決のための推奨段階が含まれる。  
 また、GuardDutyセキュリティ探知結果に対する応答で自動的に問題解決段階を遂行するようにAWS Lambda関数を構成することもできる。