「スタートアップのためのクラウドセキュリティ2024」 解説

一般社団法人　日本クラウドセキュリティアライアンス
理事　諸角昌宏
CSAリサーチフェロー、 CCSP、CCSK、CCAK、CCZT

2025年04月16日

プロフィール

- 一般社団法人日本クラウドセキュリティアライアンス　理事
- Cloud Security Alliance リサーチフェロー
- ISC2 Official Training Instructor
- CSA Authorized Instructor

本日のアジェンダ

1. 「スタートアップのためのクラウドセキュリティ 2024」目的、概要
2. フォーカス・ポイント
3. その他の考察

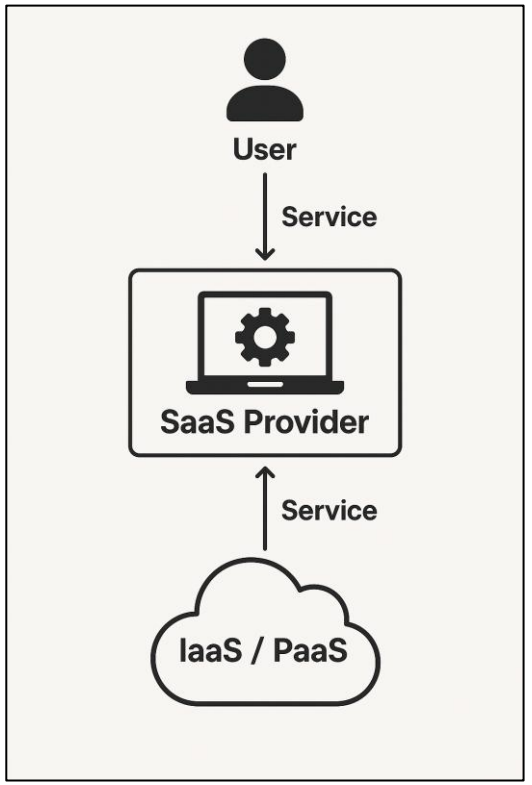
https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2025/02/Cloud-Security-for-Startups-20241218_J.pdf

1. 「スタートアップのためのクラウドセキュリティ 2024」目的、概要

SaaSスタートアップの特徴

- SaaSスタートアップ向けのガイドとしているが、SaaSサービスを提供するプロバイダーすべてに適用可能
  - スタートアップのフェーズとして3段階を定義：
    - 初期段階（フェーズ1）
    - 成熟期（フェーズ2）
    - 成長段階（フェーズ3）

- SaaSサービスのインフラとしてクラウドサービス（IaaS/PaaS）を利用
  - SaaSサービスを提供するプロバイダーであると同時に、IaaS/SaaSからサービスの提供を受ける利用者という位置づけになる
  - 責任共有モデルの2つの視点：
    - SaaSサービスの実装・配備・運用に対する直接的な責任
    - IaaS/PaaSを利用することに対する評価の責任



本セミナーのポイント

1. スタートアップにこだわらず、SaaSプロバイダーとしての考慮点にフォーカス
2. スタートアップの3ステップについては細かく触れない
3. セキュリティガイダンスV5の関連する内容を参照

https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2025/01/Security-Guidance-v5_J1.2.pdf

2. フォーカス・ポイント

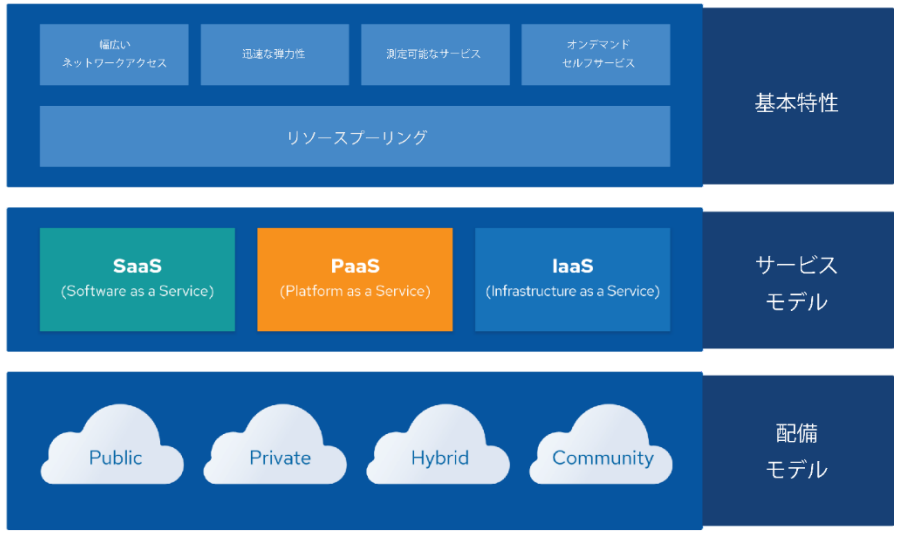
2-1. クラウドプラットフォーム
2-2. アプリケーションセキュリティ
2-3. ガバナンス、リスク、コンプライアンス
2-4. ITセキュリティ
2-5. セキュリティモニタリングとインシデント対応

2-1. クラウドプラットフォーム

プロバイダの選択

SaaSとしてどのプロバイダーを使うかを、セキュリティとコンプライアンスの観点で考慮

- インフラとしてIaaS/PaaSの選択
  - カスタム設定が必要な場合にはIaaS
  - クラウドネイティブは基本的にPaaS
- SaaSの利用
  - セキュリティサービスの利用（DDoS対策、アイデンティティプロバイダなど）
  - 利用時にセキュリティ能力、ポスチャの評価の実施
- デプロイメントモデルの選択
  - 基本パブリッククラウド。要件が厳しい場合にはプライベートクラウド
- その他の考慮点
  - 成熟したプロバイダかどうかの評価（ハイパースケールクラウドプロバイダー）
  - SaaSサービスをマルチクラウドに配備する場合には注意が必要



引用：　セキュリティガイダンスV5

アーキテクチャの考慮点（１）

- デプロイメントの場所
  - コンプライアンス要件に基づくデータレジデンシーを考慮

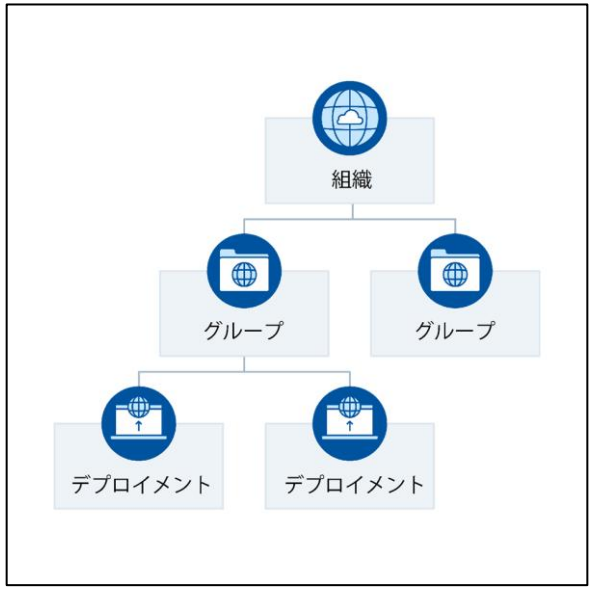
- ネットワークセグメンテーション
  - 隔離されたセグメントにより、ラテラルムーブメントを防ぎ、影響範囲を最小化する
    - VPC/Vnetによる、独立した領域の作成、環境の分離
    - マイクロセグメンテーションによるきめ細かいセキュリティゾーンの作成

- 環境アクセス
  - クラウド環境内のアプリケーションの管理に使うアクセス方法
    - セキュアなリモートアクセス（Bastion等）
    - クラウドベースのアクセス（AWS System Manager, Azure Just In Timeなど）

アーキテクチャの考慮点（２）

- 複数アカウントの論理的分離
  - 組織構造（組織階層モデル）を用いた管理（*ガイダンス第4章*）
    - AWS Organizationなど
  - マルチアカウント機能によるアカウントの分離
  - ポリシーの集中化
  - プロビジョニングの自動化(IaC)

- ランディングゾーン
  - ワークロード、アプリケーションの配備の設定済みの出発点
  - 標準的なセキュリティ構成、自動化ワークフローの確立
    - セキュリティベースラインの確立
    - セキュリティリスクの軽減
  - クラウド全体で一般化したセキュリティポスチャを維持



引用：　セキュリティガイダンスV5

アーキテクチャの考慮点（3）

- 自動化
  - IaC、テンプレート、イミュータブルワークロードによる自動化
    - 一貫したセキュリティポリシー、バージョン管理等
    - テンプレートによる迅速な配備
    - イミュータブルによるセキュリティの強化
      - アタックサーフェスの減少
    - DevSecOpsとの統合

- レジリエンス
  - SaaSサービスとしてのBCP/DR
    - SaaS利用者が管理できる選択肢はほとんどない。SaaSプロバイダーとしての対策が重要
  - マルチゾーン（マルチ・アベイラビリティゾーン）、マルチリージョンの考慮
  - 可用性の判断のパラメータの導入（RTO,RPO等）

データセキュリティの考慮点

- データの保存場所の適切な計画
  - 適用される法律・規制要件
  - 冗長化構成
  - アクセス環境（CDNの分散配置など）

- データ分類
  - データセキュリティの基本
  - 適切なセキュリティコントロールと保護要件の特定

- 暗号化と鍵管理
  - 保存中のデータの暗号化
    - SaaSの利用者に対して、利用者が鍵を管理し、利用者がデータを暗号化できる機能の提供を検討（例：BYOK)

アイデンティティとアクセス制御の考慮点

IAMはセキュリティの要

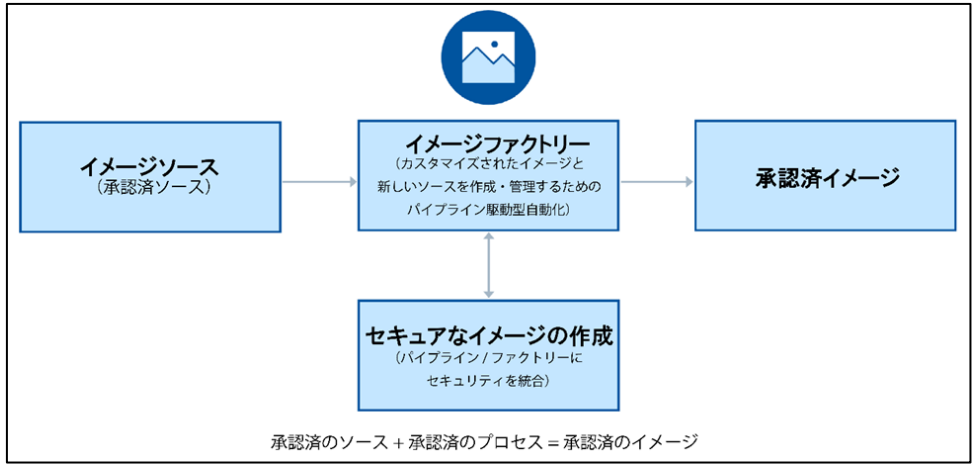
- IAMの対応
  - ユーザ名/パスワード　->　RBAC　->　ABAC/PBAC
  - 最小特権、職務分掌の維持
  - 一元化したIdPの適切な使用（フェデレーション、SSO）
  - あわせて、IAMの監査の実施
  - 進化した環境：　PIM、IGAの導入による自動化

- シークレット管理の実装
  - アプリケーションのシークレットをセキュアにする

ワークロードセキュリティ(1)

VM、コンテナ等、抽象化された処理の単位であるワークロードのセキュリティ考慮点

- イメージのハードニング
  - 責任共有
    - IaaS/PaaSが提供するイメージの責任はIaaS/PaaSプロバイダー
    - イメージ稼働後の責任はSaaSプロバイダー
  - ハードニングを行ったSaaSアプリのゴールデンイメージの作成・管理
    - CI/CDパイプラインの一部としてイメージの作成とハードニングの自動化



- 稼働後の脆弱性とパッチ管理
  - CWPPの利用

- Kubernetesのセキュリティ
  - ランタイムセキュリティを考慮
    - Seccomp, AppArmor, SELinux など
    - IaaS/PaaSプロバイダ提供のKubernetesセキュリティサービスの利用

ワークロードセキュリティ(2)

サーバーレス、FaaSのセキュリティ

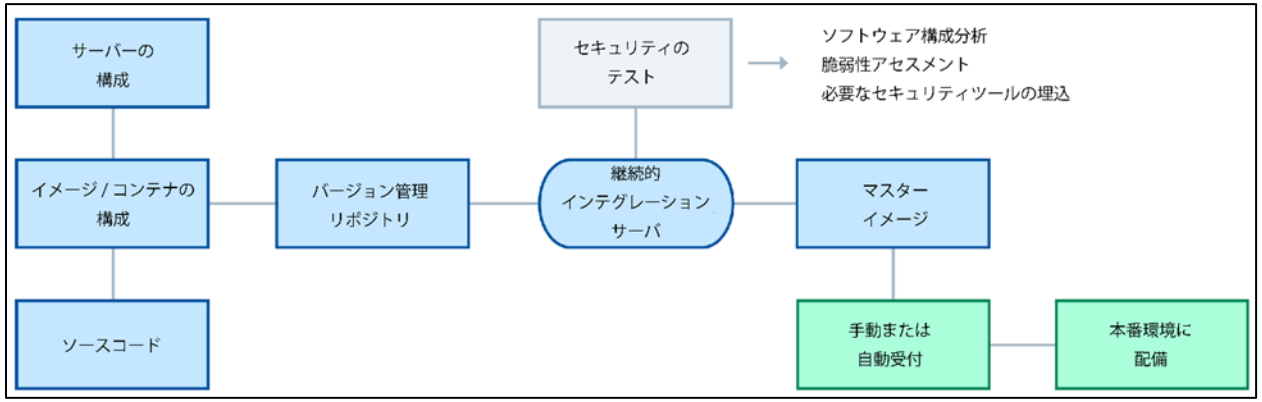
- サーバーレスセキュリティの利点
  - 運用負荷の軽減：　インフラの自動化された管理、セキュアで最新の環境の利用
  - アタックサーフェスの削減：　基盤インフラは抽象化されるので潜在的なアタックサーフェスの減少
  - 組み込みの認証、認可：　きめ細かいIAM
  - 拡張性：　自動スケーリング。ワークロードの効率的な利用

- サーバーレスセキュリティの考慮点（*ガイダンスV5より*）
  - サードパーティサービスおよびそのAPIがアタックサーフェスになる可能性
  - 外部ライブラリへの依存
  - 誤設定、ファンクションへの過剰な権限

ワークロードセキュリティ(3)

CI/CDパイプラインのセキュリティ

- CI/CDパイプラインのセキュリティとは？
  パイプラインの潜在的な脅威を理解
  - 未認可なコード変更
  - セキュアでない依存関係
  - ビルド環境のリスク
  - 不十分なアクセス制御
  - 暗号化されていない通信
  - 脆弱な認証メカニズム
- セキュリティ対策
  - アクセス制御の制限、監査証跡/モニタリング、イミュータブルな監査ログ
  - パイプラインの構成管理の自動化
  - パイプラインの定期的なセキュリティスキャンの実施
  - 機密データの暗号化、など



モニタリング、監査、フォレンジック(1)

クラウド環境の継続的なモニタリングは必須
（*ガイダンスV5では、独立したドメインとして解説*）

- ツールの利用を推奨（必須）
  - CSPM、CNAPP、DSPM、CIEM、ASPMなど
- ログ管理
  - IaaS/PaaSからのログフィード　->　中央ストレージで管理
  - セキュリティログ
    - クラウド構成の変更（AWS CLoudTrailなど）
  - トラフィックログ
    - VPC/Vnetのトラフィック（AWS Flowsなど）
  - クラウドサービスログ
    - パフォーマンス等の運用ログ
  - ワークロードログ
    - VM、コンテナ、サーバーレスのログ（docker log, kubectl logsなど）

モニタリング、監査、フォレンジック(2)

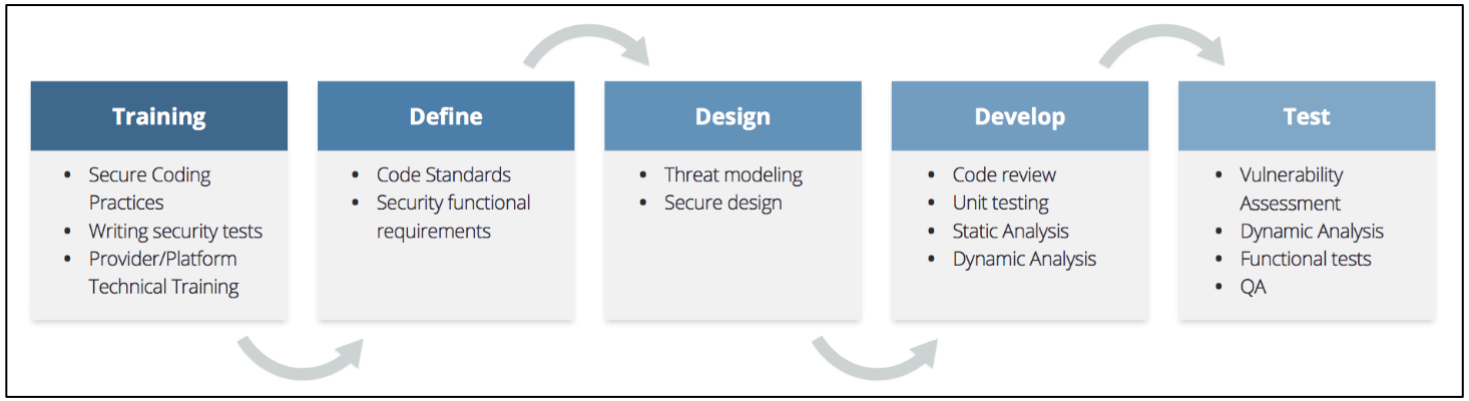
- SIEM、SDL、CDR等による検知・対応
  - SIEM
    - 様々なリソースからのログの集中管理
    - インシデントの特定、分析等、セキュリティの可視性
  - SDL（セキュリティデータレイク）
    - 構造化、非構造化データを生のまま保存、一元管理
    - ビッグデータ分析、機械学習、分析
    - 複数のフォーマットで膨大なデータを柔軟に集約、分析（SIEMを補完）
  - CDR（Cloud Detection and Response）
    - ワークロード、アプリケーション、ユーザのアクティビティをリアルタイムで可視化（SIEMの進化版）
    - 継続的モニタリング、脅威の検出、インシデントレスポンスの自動化等

2-2. アプリケーションセキュリティ

アプリケーションセキュリティの考慮点

SSDLCの各フェーズのセキュリティ対策

- アプリケーション開発者の意識向上、トレーニング
  - アタックサーフェスの理解
  - 脅威モデリングの利用
  - セキュリティ文化の醸成など
- セキュアな開発
  - 入力検証
  - ロギングとモニタリング
  - エラー処理など
- セキュリティ保証とテスト
  - SAST, SCA、セキュリティコードレビュー、静的ぜい弱性スキャン（IaCコードと構成を分析）
  - 動的脆弱性スキャン、DAST、侵入テスト、バグバウンティ
- アプリケーションセキュリティメトリックス
  - セキュリティの評価基準の作成



第三者ソフトの考慮

- サプライチェーンセキュリティの主な考慮点
  - サードパーティ製コンポーネントの脆弱性
  - 互換性
  - サポートリスク、ライセンスリスク

- オープンソースガバナンスの主な考慮点
  - 脆弱性
  - SCA/SBOMの整備

- クローズドソースのサードパーティライブラリ/API
  - SCA/SBOMの整備
  - APIのセキュリティ

その他のアプリケーションセキュリティの考慮点

- 変更管理
  - 変更要求に対する管理された方法での実施
  - 変更管理プロセスの自動化

- CI/CD,　IaC
  - ビルド、テスト、デプロイの自動化
  - 効率性と一貫性の向上。セキュリティの強化。
  - 監査証跡、自動コンプライアンススキャン、コンプライアンス更新の自動化

- API管理とWAF
  - Webアプリケーションとインターネット間のトラフィックを監視
  - Webアプリケーション、APIのセキュリティに重要

2-3. ガバナンス、リスク、コンプライアンス

リスク管理

- リスク管理の考慮点
  - SaaSプロバイダとしてのリスクだけでなく、利用者のリスクも考慮
  - SaaSプロバイダは、第三者に依存するので、サプライチェーンのリスク管理が必要
  - コントロールと防御プロセスの透明性が必要

- リスク管理
  - リスクレジスタの整備
    - すべてのリスクを管理、優先順位付け、監視
    - 外部監査人は、リスクレジスタを調査することで監査を行うことが多い
  - リスク軽減
    - 関連資産の特定、リスクアセスメント、リスク対応

- プライバシーの考慮事項
  - 責任範囲、役割の明確化：　コントローラなのかプロセッサーなのか。
  - 適用される法律の順守：　国ごとに異なる点に注意

サードパーティリスク管理

- ベンダーレジストリの整備
  - 利用しているサードパーティの特定
- デューデリジェンスの実施
  - サードパーティのセキュリティ評価
- ベンダー監査
  - 外部監査人による独立した監査の評価
    - 基準や規制への準拠、セキュリティポリシー、データ保護対策、インシデント対応
    - 標準フレームワークへの準拠
- ベンダー解約時の注意
  - データの削除
  - 終了後のサポートの確認
  - 契約時に明確にしておく

コンプライアンス

- コンプライアンスフレームワークの選択
  - 利用者が必要とするコンプライアンスフレームワークをカバー
    - 必然的に、複数のフレームワークへの対応が必要となる
  - 標準的なフレームワーク
    - ISO/IEC 27001
    - SOC2
  - データ保護規制
    - HIPAA
    - GDPR、CCPA
  - 業界ベースのフレームワーク
    - FedRAMP
  - その他
    - ISO/IEC 27017
    - ISO/IEC 27018
    - CSA STAR Level2

2-4. ITセキュリティ

社内インフラのセキュリティ

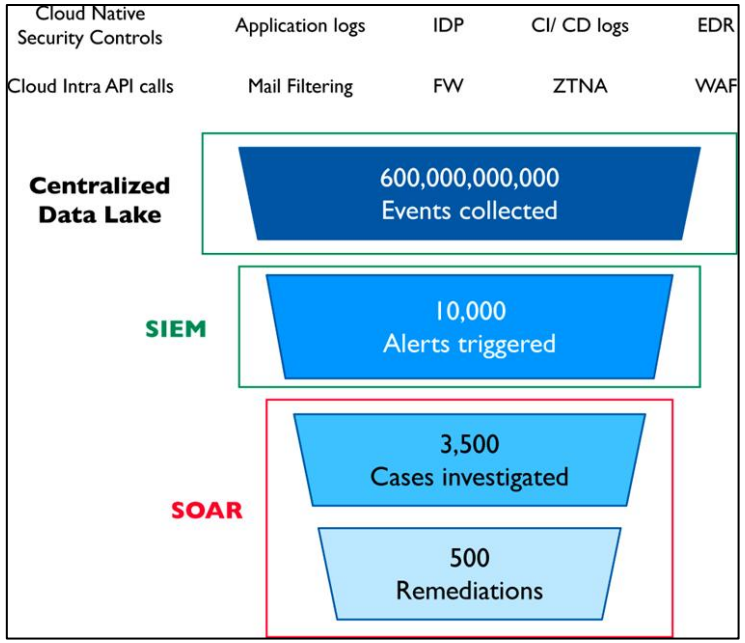
社内システムの重要なコンポーネントをセキュアにするのは利用者責任
（すべてのサービスモデルで、IAM、データガバナンス、クライアントの管理は利用者責任）

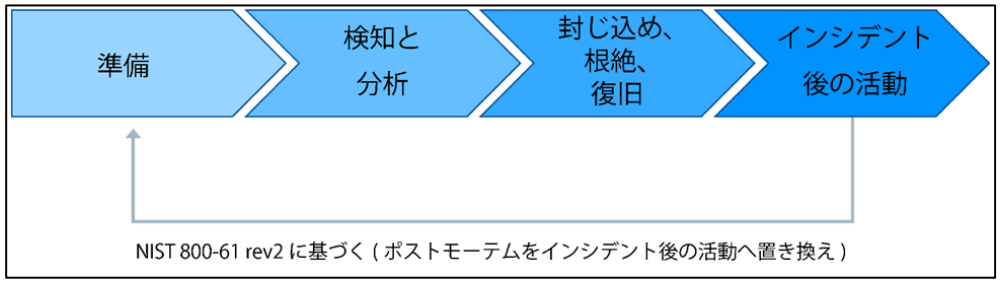
- アイデンティティシステム
  - MFAの強制、管理者への物理的な認証デバイスの導入
- ワークステーション
  - セキュリティアップデートの徹底
  - エンドポイントセキュリティの対策
  - 集中管理（UEM)
- リモートアクセス
  - VPN　->　デバイスセキュリティステータス　->　SASE/ZTA
- コラボレーションツール
  - 認証の強化
  - 共有情報の管理

2-5. セキュリティモニタリングとインシデント対応

セキュリティモニタリング

- スタートアップといえども対応は必須
  - 脅威とトレンドの監視
  - 脆弱性の特定
  - インシデント対応プロセスの確立と組織内の認識
- 方法
  - Data Lake、SIEM、SOARの利用
    - 機械によるインシデントの絞り込み
  - ゴール
    - TTD（Time-to-detect）、TTR(Time-to-respond)、TTM(Time-to-Mitigate)　の短縮
- インシデントレスポンス
  - 対応計画の作成：　被害を最小限に抑える、効果的に復旧





3.　その他の考察

その他の考慮事項

- AI
  - セキュリティの自動化
    - 脅威の検出、脆弱性管理、ユーザ行動分析（UBA)
    - 様々なプロセスの透明化、および、説明責任
- ゼロトラスト
  - 「信用せず、常に検証する」基本原則
  - SaaSスタートアップのニーズに完全に合致
- 量子コンピューティング
  - SaaSにとって、チャンスと課題の両面を持つ
    - 革新的なサービスの開発
    - 耐量子セキュリティ（暗号アルゴリズム）

CSAの活動　==　「場」の提供！

様々なワーキンググループ活動の「場」

自由な情報発信の「場」

https://cloudsecurityalliance.jp

ご意見、ご質問等は、以下にご連絡ください。

mmorozumi@cloudsecurityalliance.jp

（本メールアドレスには、S/MIME電子証明書を付与してお送りしますので、安心して情報交換できます）

ありがとうございました！