\Orchestrating a brighter world NEC

Well-Architected Framework セキュリティの柱で Security By Design

釜山 公徳 (Masanori Kamayama), Well-Architected Lead

NEC (日本電気株式会社)
デジタルビジネス基盤本部金融デジタルシフトグループ
(兼) 金融システム本部
(兼) サイバーセキュリティ戦略本部

2020年3月28日

Orchestrating a brighter world

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ
類のないインテグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。

NECは
ハードウェアメーカー
ソフトウェアベンダー
システムインテグレーター
そして
クラウドインテグレーター

Self-Introduction

略歴

インフラエンジニア、セキュリティコンサルタント、マルウェアアナリスト等を経て、現在セキュリティを専門とするエバンジェリスト、コンサルタント、W-A Lead として従事

その他活動

- ✓ JAWS-UG (Fin-JAWS コアメンバー、JAWS DAYS 2020 実行委員)
- ✓ CompTIA Subject Matter Experts
- ✓ CSAジャパン クラウドセキュリティWG リーダー

コラム等

- ✓ あなたの守りたい「モノ」は何ですか？どうやって守りますか？ (NISC(内閣サイバーセキュリティセンター) ：サイバーセキュリティ ひとこと言いたい！)
  https://www.nisc.go.jp/security-site/month/h29/column/20180314.html

初めにお伝えしたいこと

- ✓ セキュリティは
  単純コストではなく**投資**

- ✓ 最初に**守るべきモノ**を定義

https://www.nisc.go.jp/security-site/month/h29/column/20180314.html

Well-Architected Framework (W-A Framework) の前に知っておきたい話

セキュリティマインド

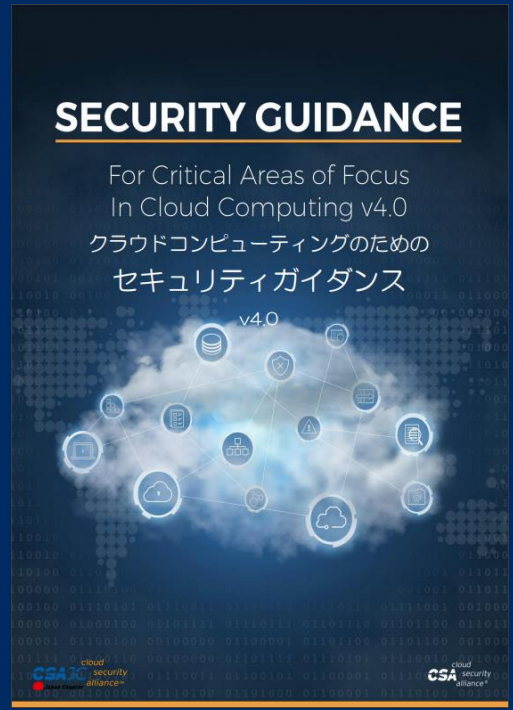
- ✓セキュリティは最優先事項
- ✓守りたい「**モノ**」が何かを定義
- ✓攻撃・侵入されることが前提
- ✓責任範囲を把握
- ✓SecOps
- ✓**Security by Design**

セキュリティリファレンスを有効活用

タイトル	著作者
Security Guidance for the Critical Areas of Focus in Cloud Computing v4.0	CSA: Cloud Security Alliance
NIST Cloud Computing Security Reference Architecture (SP 500-299 (Draft))	NIST: National Institute of Standards and Technology
FISC 安全対策基準	FISC:金融情報システムセンター

CSA セキュリティガイダンスの紹介

No.	Domain name
Domain1	クラウドコンピューティングのコンセプトとアーキテクチャ
Domain2	ガバナンスとエンタープライズリスクマネジメント
Domain3	法的課題、契約および電子証拠開示
Domain4	コンプライアンスと監査マネジメント
Domain5	情報ガバナンス
Domain6	管理画面と事業継続
Domain7	インフラストラクチャ・セキュリティ
Domain8	仮想化とコンテナ技術
Domain9	インシデントレスポンス
Domain10	アプリケーションセキュリティ
Domain11	データセキュリティと暗号化
Domain12	アイデンティティ管理、権限付与管理、アクセス管理(IAM)
Domain13	Security as a Service
Domain14	関連技術



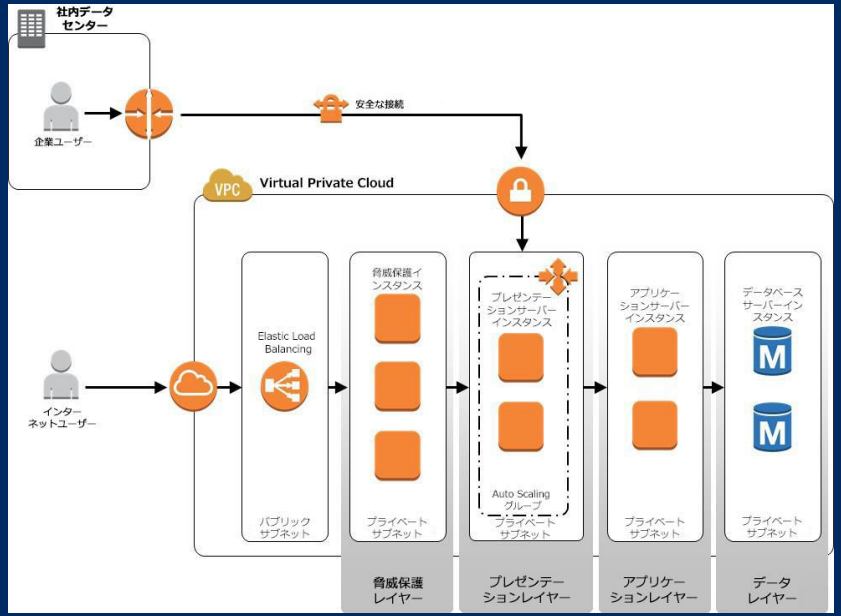
https://cloudsecurityalliance.jp/j-docs/CSA_Guidance_V4.0_J_V1.1_20180724.pdf

参考) AWSセキュリティのベストプラクティス

◆インライン脅威保護テクノロジーの例

1. Third-party firewall devices installed on Amazon EC2 instances (also known as soft blades)
   - Amazon EC2 インスタンスにインストールされたサードパーティー
   - のファイアウォールデバイス (別名ソフトブレード)
2. Unified threat management (UTM) gateways
   - 統合脅威管理 (UTM) ゲートウェイ
3. Intrusion prevention systems
   - 侵入防止システム
4. Data loss management gateways
   - データ損失管理ゲートウェイ
5. Anomaly detection gateways
   - 異常検出ゲートウェイ
6. Advanced persistent threat detection gateways
   - 持続的標的型攻撃検出ゲートウェイ

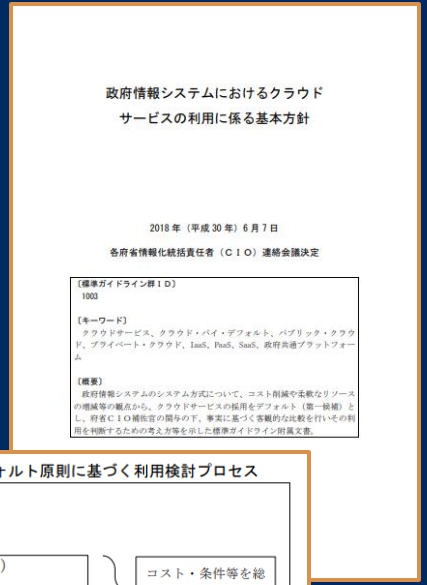
階層型ネットワーク防御



https://d1.awsstatic.com/whitepapers/ja_JP/Security/AWS_Security_Best_Practices.pdf

政府情報システムにおけるクラウドサービスの利用に係る基本方針

- 2018 年 6 月 7 日公開
- 方針を基本方針と具体方針で定義
  - **基本方針**：
    クラウド・バイ・デフォルトの原則をはじめとした選定にあたっての考え方を定義
  - **具体方針**：
    Step毎に検討する事項を定義
    - **Step1: SaaS (パブリック・クラウド)**
    - **Step2: SaaS (プライベート・クラウド)**
    - **Step3: IaaS/PaaS (パブリック・クラウド)**
    - **Step4: IaaS/PaaS (プライベート・クラウド)**
- クラウドのメリットを明記
  - 効率性の向上
  - セキュリティ水準の向上
  - 技術革新対応力の向上
  - 柔軟性の向上
  - 可用性の向上
- サービスモデルをベースにした利用検討プロセス



政府情報システムにおけるクラウド
サービスの利用に係る基本方針

2018 年（平成 30 年）6 月 7 日

各府省情報化統括責任者（ＣＩＯ）連絡会議決定

〔標準ガイドライン群ＩＤ〕
1003

〔キーワード〕
クラウドサービス、クラウド・バイ・デフォルト、パブリック・クラウド、プライベート・クラウド、IaaS、PaaS、SaaS、政府共通プラットフォーム

〔概要〕
政府情報システムのシステム方式について、コスト削減や柔軟なリソースの増減等の観点から、クラウドサービスの採用をデフォルト（第一候補）とし、府省ＣＩＯ補佐官の関与の下、事実に基づく客観的な比較を行いその利用を判断するための考え方等を示した標準ガイドライン附属文書。

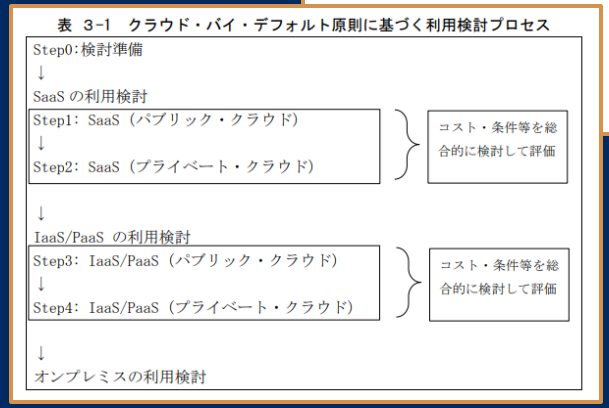
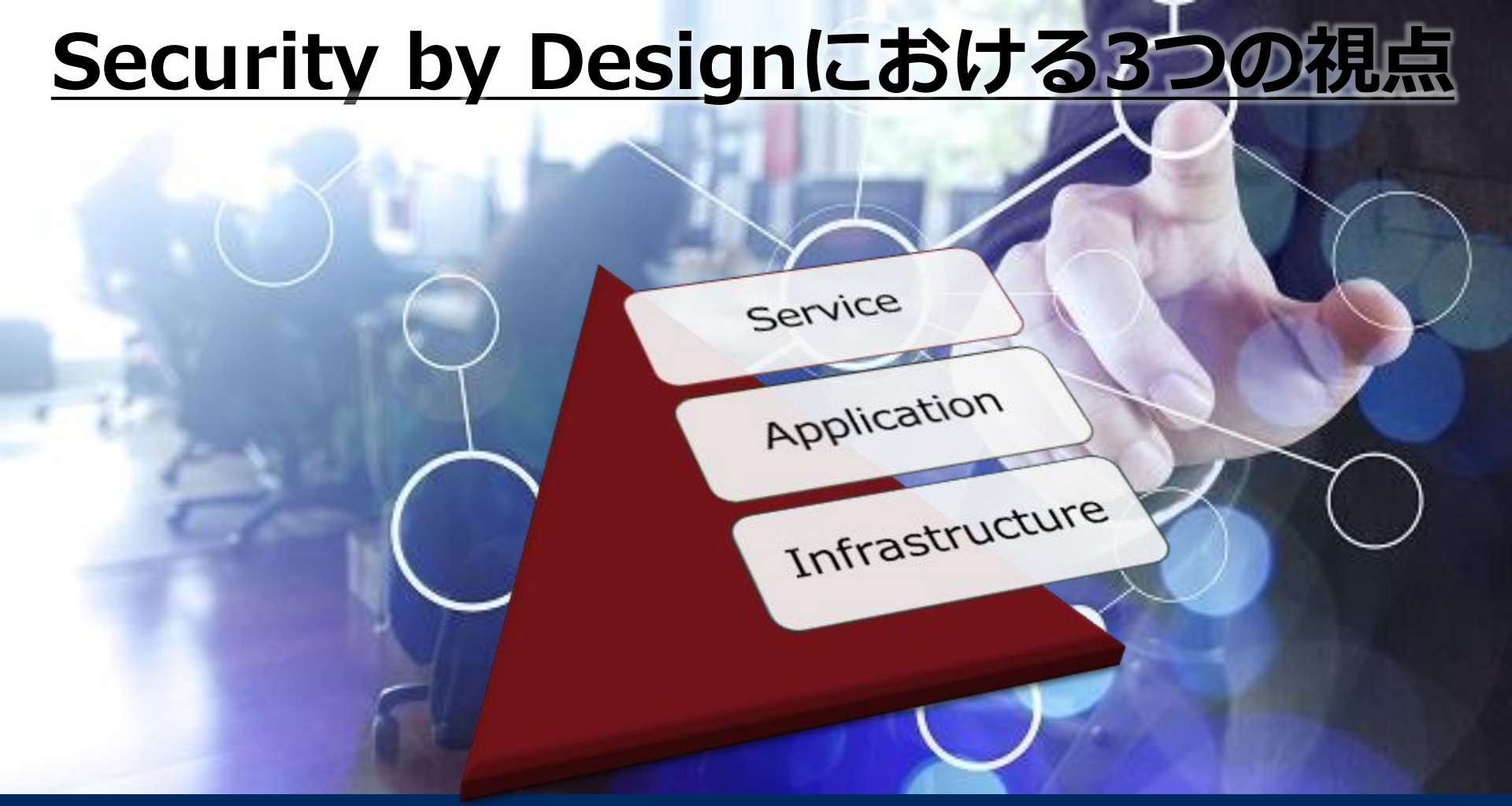


表 3-1　クラウド・バイ・デフォルト原則に基づく利用検討プロセス

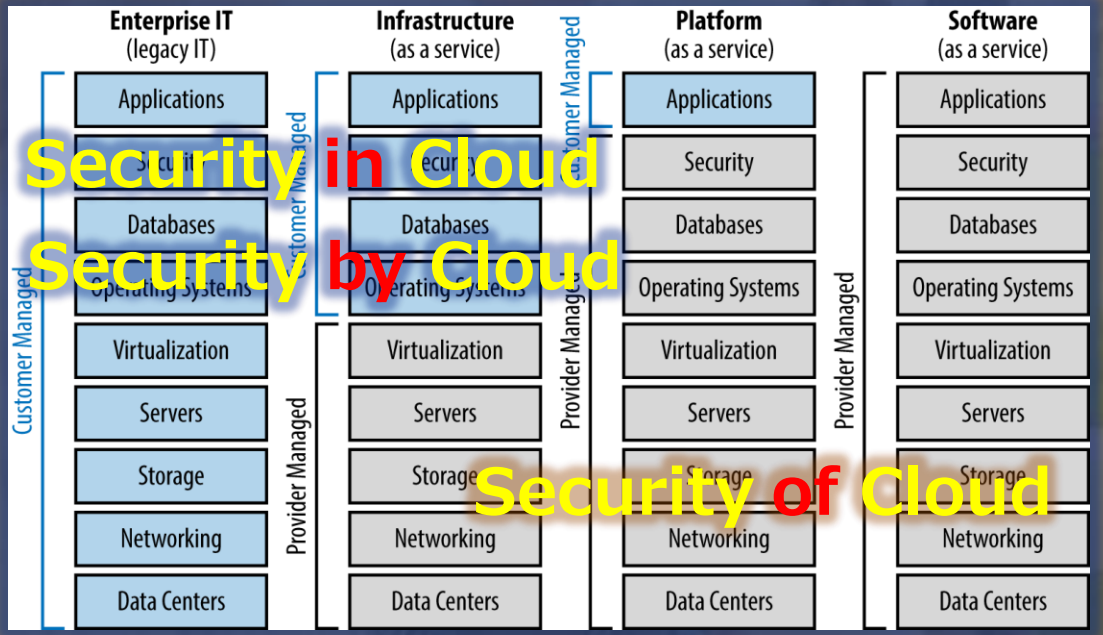
Step0:検討準備
↓
SaaS の利用検討
Step1: SaaS（パブリック・クラウド）
↓
Step2: SaaS（プライベート・クラウド）
} コスト・条件等を総合的に検討して評価
↓
IaaS/PaaS の利用検討
Step3: IaaS/PaaS（パブリック・クラウド）
↓
Step4: IaaS/PaaS（プライベート・クラウド）
} コスト・条件等を総合的に検討して評価
↓
オンプレミスの利用検討

https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf

Security by Designにおける3つの視点



Security X Cloud と責任共有モデル



- ✓サービス毎に異なる責任範囲
- ✓抽象化すればする程、責任はベンダー側に
- ✓利用者側は適切なセキュリティ実装が必要

Figure 1-5. Cloud provider versus customer roles for managing cloud services
<https://www.oreilly.com/library/view/the-enterprise-cloud/9781491907832/ch01.html>

参考) コンプライアンスポートフォリオ (AWS)

グローバル

CSA　ISO 9001 規格　ISO 27001 規格　ISO 27017 規格　ISO 27018 規格　PCI DSS レベル 1　SOC 1　SOC 2　SOC 3

米国

CJIS　DoD SRG　FedRAMP　FERPA　FFIEC　FIPS　FISMA　GxP　HIPAA　ITAR　MPAA　NIST　SEC ルール 17a-4(f)　VPAT / セクション 508

アジア太平洋

FISC [日本]　IRAP [オーストラリア]　K-ISMS [韓国]　MTCS ティア 3 [シンガポール]　FinTech [日本]　日本の医療情報ガイドライン　政府機関等の情報セキュリティ対策のための統一基準群

ヨーロッパ

C5 [ドイツ]　サイバーエッセンシャルズプラス [英国]　ENS 高レベル [スペイン]　G-Cloud [UK]　IT-Grundschutz [ドイツ]

https://aws.amazon.com/jp/compliance/programs/

W-A セキュリティの柱
カテゴリ別レビューポイント

そもそもWell-Architected フレームワークとは

5 つの柱で構成される AWS のベストプラクティス

運用上の優秀性

•変更の管理と自動化、イベントへの対応、日常業務をうまく管理するための定義。

セキュリティ

•データの機密性と整合性、権限管理における権限の特定と管理、システムの保護、セキュリティイベントを検出する制御の確立。

信頼性

•設定、プロジェクト間の要件、復旧計画、変更に対処する方法についての要素。

パフォーマンス効率

•ワークロードの要件に応じた適切なリソースタイプやサイズの選択、パフォーマンスのモニタリング、ビジネスニーズの進展に応じて効率化。

コスト最適化

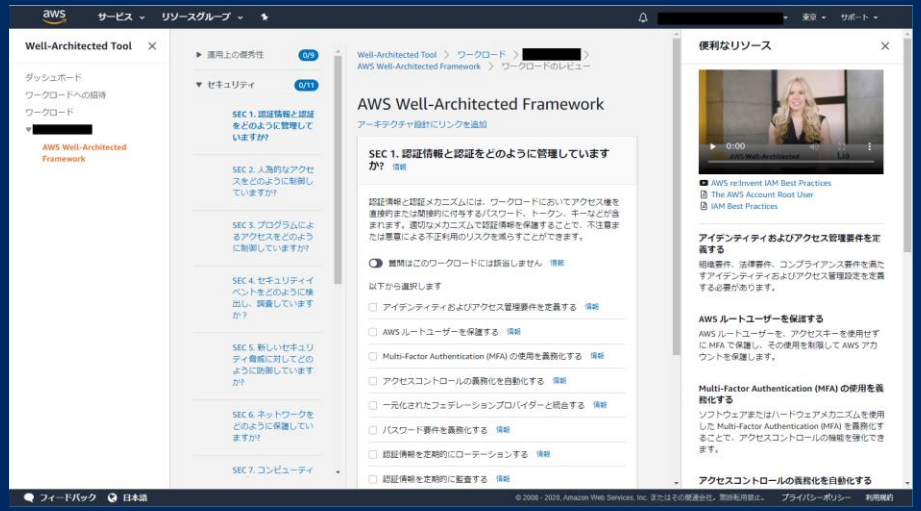
•費用が発生する箇所の把握と管理、最適で正しい数のリソースタイプの選択、時間経過に伴う分析、不要な支出がないビジネスニーズに対応したスケーリング。

レビュー用チェックシート

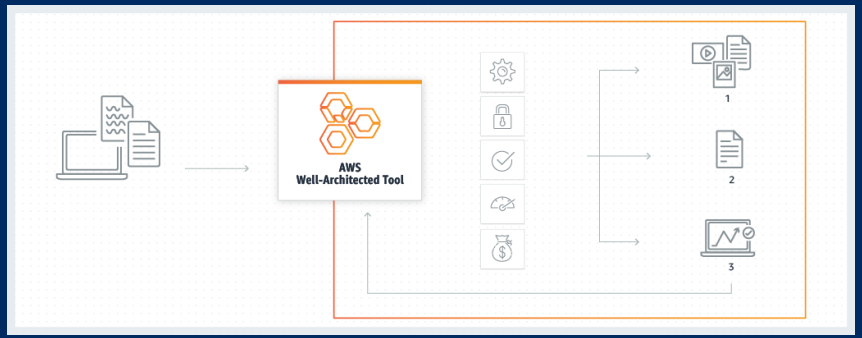
https://aws.amazon.com/jp/architecture/well-architected/

参考) AWS Well-Architected Tool

サービスコンソールでセルフチェックが可能



仕組み



https://aws.amazon.com/jp/well-architected-tool/

SEC 1. 認証情報と認証をどのように管理していますか?

- アイデンティティおよびアクセス管理要件を定義する
- AWS ルートユーザーを保護する
- Multi-Factor Authentication (MFA) の使用を義務化する
- アクセスコントロールの義務化を自動化する
- 一元化されたフェデレーションプロバイダーと統合する
- パスワード要件を義務化する
- 認証情報を定期的にローテーションする
- 認証情報を定期的に監査する

Point：認証部分の不正アクセス防止策

- ✓ **不正アクセス防御策**
  - **パスワード要件、MFA、ユーザー管理、自動化**
- ✓ **インシデント発生時のトレース、現状把握**
  - **定期的な棚卸、監査、不正アクセス確認(CloudTrail等)**
- ✓ **変化への対処**
  - **アクセス要件の変更**

SEC 2. 人為的なアクセスをどのように制御していますか?

- 人為的なアクセス要件を定義する
- 最小限の権限を付与する
- 各個人に一意の認証情報を割り当てる
- ユーザーライフサイクルに基づいて認証情報を管理する
- 認証情報管理を自動化する
- ロールまたはフェデレーションを通じてアクセス権を付与する

Point：人為的なアクセスによる脅威からの防止策

- ✓ **最小権限の原則**
  - **アクセス可能な範囲を把握できるようにする**
- ✓ **休眠情報の削除**
  - **不要なクレデンシャル、ユーザーを削除する**
- ✓ **管理をシンプルにする**
  - **一人一IAMユーザー、IDフェデレーション**

SEC 3. プログラムによるアクセスをどのように制御していますか?

- プログラムによるアクセス要件を定義する
- 最小限の権限を付与する
- 認証情報管理を自動化する
- 各コンポーネントに一意の認証情報を割り当てる
- ロールまたはフェデレーションを通じてアクセス権を付与する
- 動的認証を実装する

Point：プログラムからのアクセスによる脅威からの防止策

- ✓ **最小権限の原則**
  - **アクセス可能な範囲を把握できるようにする**
- ✓ **休眠情報の削除**
  - **不要なクレデンシャル、ユーザー/ロールを削除する**
- ✓ **自動化とトレーサビリティ**

SEC 4. セキュリティイベントをどのように検出し、調査していますか？

- ログの要件を定義する
- メトリクスの要件を定義する
- アラートの要件を定義する
- サービスとアプリケーションのログ記録を設定する
- ログを一元的に分析する
- 主要な指標に関するアラートを自動化する
- 調査プロセスを開発する

Point：セキュリティインシデントを意識したログの定義

- ✓ **漏れの無いアラート要件、ログ要件の定義**
  - **守るべき「モノ」の定義が最優先**
  - **具体的に何をどうやって検知するか**
- ✓ **インシデントレスポンスの最速化**
  - **ログの一元管理、アラートの自動化**

SEC 5. 新しいセキュリティ脅威に対してどのように防御していますか?

- 組織要件、法的要件、コンプライアンス要件に関する最新情報を入手する
- セキュリティのベストプラクティスに関する最新情報を入手する
- セキュリティ脅威に関する最新情報を入手する
- 新しいセキュリティサービスとセキュリティ機能を定期的に評価する
- 脅威モデルを使用してリスクを定義し優先順位付けする
- 新しいセキュリティサービスとセキュリティ機能を実装する

Point：ナレッジの継続的最新化スキームがキー

- ✓ **脅威の前提として、日々進化し新しい手法がでてくることを理解する**
- ✓ **閉域網だから問題無いといった誤った考えを捨てる**
- ✓ **最低でもJPCERTからの情報はキャッチアップする**
- ✓ **インシデント発生時のトリアージを意識する**

SEC 6. ネットワークをどのように保護していますか?

- ネットワーク保護要件を定義する
- 露出を制限する
- 設定管理を自動化する
- ネットワーク保護を自動化する
- 検査および保護を実装する
- すべてのレイヤーでトラフィックをコントロールする

Point：ネットワークのアーキテクチャを意識する

- ✓ **多層多段型ディフェンス・アーキテクチャ**
  - **WAF、ネットワーク型IDS/IPS、ファイアウォール**
- ✓ **設定や異常の検出を自動化**
- ✓ **Attack Surface Reduction**
- ✓ **ネットワークトラフィックの自動遮断**

SEC 7. コンピューティングリソースをどのように保護していますか?

- コンピューティング保護要件を定義する
- 脆弱性をスキャンし、パッチを適用する
- 設定管理を自動化する
- コンピューティング保護を自動化する
- 攻撃領域を削減する
- マネージドサービスを活用する

Point：コンピュートのアーキテクチャを意識する

- ✓ **多層多段型ディフェンス・アーキテクチャ**
  - **WAF、ホスト型IDS/IPS、ファイアウォール**
- ✓ **設定や異常の検出を自動化**
- ✓ **Attack Surface Reduction**
- ✓ **コンピュートを自動隔離**
- ✓ **セキュリティスキャン、パッチの最新化**

SEC 8. データをどのように分類していますか?

- データ分類要件を定義する
- データ保護コントロールを定義する
- データの識別を実行する
- 識別および分類を実装する
- データのタイプを特定する

Point：データ・クラフィシケーション

- ✓ **保護対象のデータの定義**
  - **コンプライアンス、法規制**
  - **個人情報が含まれるか**
- ✓ **リスクベースアプローチ**

SEC 9. 保管中のデータをどのように保護していますか?

- 保管中のデータの管理と保護に関する要件を定義する
- 安全なキー管理を実装する
- 保管中に暗号化を適用する
- アクセスコントロールを適用する
- 人をデータから遠ざけるメカニズムを提供する

Point：データセキュリティ

- ✓ **暗号化**
- ✓ **アクセスコントロール**
- ✓ **管理方法と体制**

SEC 10. 伝送中のデータをどのように保護していますか?

- 伝送中のデータの保護に関する要件を定義する
- 安全な鍵および証明書管理を実装する
- 伝送中に暗号化を適用する
- データ漏洩の検出を自動化する
- ネットワーク通信を認証する

Point：ネットワークトラフィックの保護

- ✓ **トラフィックの区分を明確に**
  - ✓ **インターネット or VPN or Direct Connect**
- ✓ **“専用線 = パーフェクトセキュアソリューション”ではない**
- ✓ **鍵、証明書の管理主体を明確にする**
- ✓ **トレーサビリティを忘れずに**

SEC 11. セキュリティインシデントにどのように対応していますか?

- ☐ 重要な人員と外部リソースを特定する
- ☐ ツールを特定する
- ☐ インシデント対応計画を策定する
- ☐ 封じ込め機能を自動化する
- ☐ フォレンジック機能を確認する
- ☐ アクセスを事前準備する
- ☐ ツールを事前デプロイする
- ☐ ゲームデーを実施する

Point：SecOps を確立させる

- ✓ **セキュリティインシデントは必ず発生することを前提とする**
  - ✓ **ITのみならず、セキュリティに100%はない**
- ✓ **体制と役割を明確にする**
  - **“いつ”、”どこで”、”誰が”、”何を”、”どうするか”**
- ✓ **変化に強い組織**
- ✓ **定期的なシミュレーション(レッドチーム演習等)**

まとめ

- ✓ 様々なリファレンスを活用する
- ✓ ナレッジは常に最新化する
- ✓ W-A レビューで課題を洗い出す

Security by Design で
セキュア・アーキテクチャを実現し
価値ある “モノ” の創造へ


Orchestrating a brighter world
NEC