Analysis Report

SECURITY REPORT

2023

JUN

クラウド環境の
セキュリティインシデント事例からみる
対応方法

CyberFortress

このレポートは、株式会社サイバーフォートレスの独自の調査にて収集されたデータに基づき作成しています。

Analysis Report.

クラウド環境の セキュリティインシデント事例からみる 対応方法

01. クラウドコンピューティングの発展現況及びセキュリティ脅威要素

1) クラウドコンピューティングの発展現況

DX及びアジャイルビジネス戦略でクラウドへの移行が本格化された。分散構造とオートスケーリングによる効率的なストレージ管理で費用節減など運用の効率とブロックチェーン、人工知能など次世代新技術のテストベッドで活用されて2017年から急速な成長を行い、インフラ生態系の「パーフェクトストーム」になった。クラウド移行が拡散されてクラウドの攻撃表面を活用した攻撃が増加した。従って今回はクラウドセキュリティ協会(Cloud Security Alliance, CSA)から発表したクラウドセキュリティ脅威を基にクラウド環境のセキュリティインシデント事例の分析によるセキュリティ強化方法について調べてみよう。

クラウドインフラのセキュリティ脅威を確認する前にフレーム環境からクラウドまでのITインフラの発展現況は以下の【表①】になる。初期インフラ環境はIBMのように製造業者が独自的な通信プロトコルと単一ハードウェア及びソフトウェアを提供するメインフレーム構造だった。中央管理が本格的になってサーバとクライアント構造から物理的なリソースを効率的に使用できる仮想化に発展された。その後、分散処理技術及びロードバランシング、コンテナー仮想化、サーバレスなどの技術の成熟度が向上されて物理的なリソースの制約なく、ストレージを使用できるクラウドへ拡大された。

区分		メインフレーム	サーバ/クライアント	仮想化	クラウド
時期	登場背景	汎用メインフレーム及びミニコンピューター(1960年代)	パーソナルコンピューターの登場(1980年代半ば)	汎用小規模サーバの拡大(2000年代年代初め)	大容量のデータ処理限界(2000年~現在)
	特徴	• 対話式処理環境	• 中央集中型環境 • ネットワーク依存性	• 物理的リソース確保 • 仮想ネットワーク分離	• ネットワーク地域制 • ITリソース要求即時提供(on-demand availability)
変化動因	技術環境	大量のデータ処理	分散システム	サーバの非効率性	仮想化及びIT技術の発展
	市場環境	企業、金融及び政府機関の成長	ネットワーク発展及びインターネット普及	CPUの価格下落	モバイル及び人工知能の成長

【表①　インフラ発展過程の主要特徴】

2) クラウドサービスモデル別、セキュリティ強化方法

クラウドサービスモデルによってセキュリティにアクセス方法が既存オンプレミスとは違う。クラウドサービス提供者(CSP)とクラウド使用者が領域別にセキュリティに対する責任を分担する責任共有モデル(Shared Responsibility Model, SRM)を使用しているためサービスモデル別に発生しうるセキュリティ脅威要素及び対応方法について考慮が必要である。【表②】はクラウドサービスモデル別、発生しうるセキュリティ脅威要素と対応方法をマッピングした資料である。

区分		IaaS	PaaS	SaaS	FaaS	CaaS	BaaS
機能説明		サーバ、ストレージ、ネットワークなどと同じITインフラを提供	アプリケーション開発及び配布に必要なプラットフォーム提供	ウェブブラウザーまたはモバイルアプリでアクセスできるソフトウェアアプリケーションを提供	サーバレスアーキテクチャから実行されるコード欠片(関数)を提供	コンテナー作成及び配布に必要な管理を提供	モバイルアプリケーション開発に必要なバックアンドインフラを提供
実現技術		仮想化及びストレージ	データベース管理	ウェブアプリケーション	サーバレスコンピューティングフレームワーク	コンテナーオーケストレーション	クラウドデータベース
セキュリティ観点	脅威要素	• 仮想マシンイメージセキュリティ脆弱性 • ネットワーク構成及びアクセス制御	• アプリケーションコードセキュリティ脆弱性 • 認証及びアクセス制御	• データ漏洩 • 脆弱なアカウント及びパスワードの漏洩	• コードインジェクション • 認証及びアクセス制御	• コンテナーイメージ脆弱性	• データ漏洩 • 認証及びアクセス制御
	対応方法	• 仮想マシン及びネットワークセキュリティ • サーバハードニング、ストレージセキュリティ	• アプリケーションセキュリティ • ランタイム環境 • データベースセキュリティ	• ウェブアプリケーションセキュリティ • 認証及び権限管理 • ソフトウェアアップデートセキュリティ	• 関数コードセキュリティ • 実行環境セキュリティ • イベント及びメッセージセキュリティ	• クライアントアプリケーションセキュリティ • API及びデータ格納先セキュリティ	• コンテナーイメージセキュリティ • ホスト及びネットワークセキュリティ • サービス及びアプリケーションセキュリティ
		• データ暗号化 / セキュリティ認証及びアクセス制御 / 監査追跡 / HSM(Hardware Security Module)					

【表②　クラウドサービスモデル別セキュリティ脅威及び対応方法 (参考：イグルーコーポレーション)】

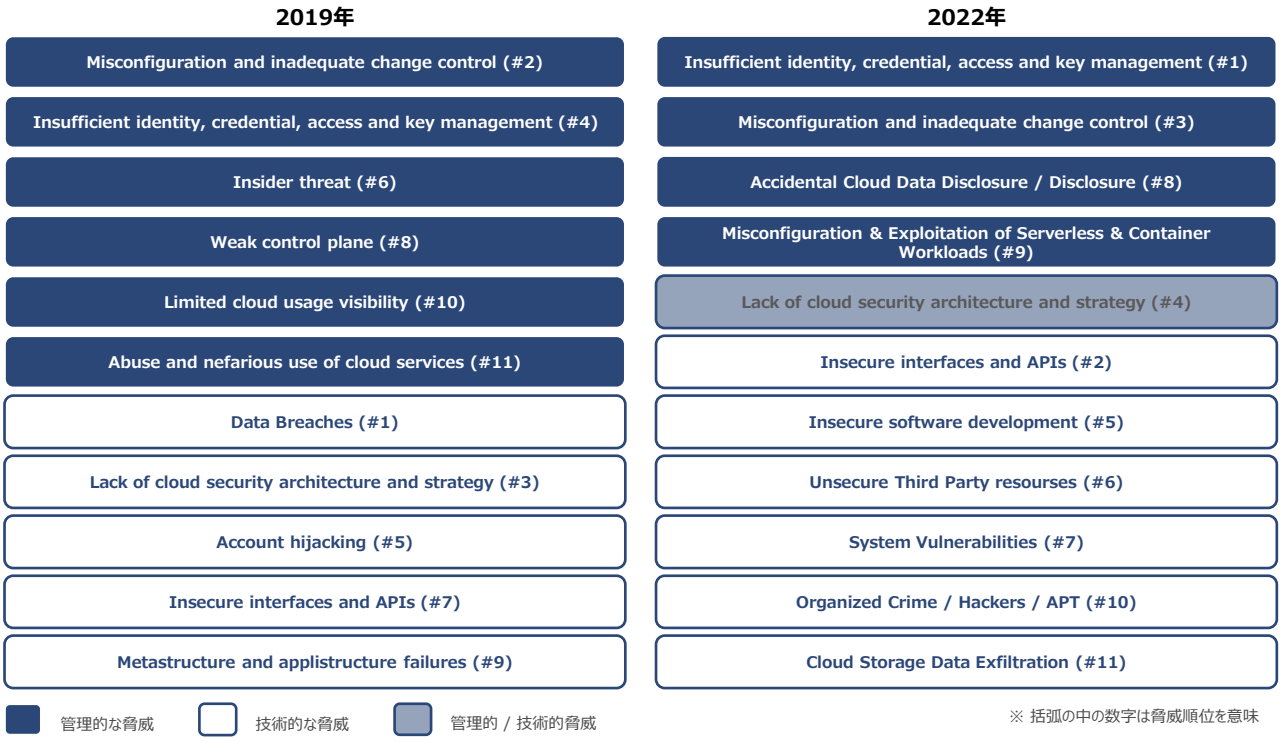
IaaS, PaaS, SaaS, FaaS, BaaS, CaaSなどクラウドサービスモデルは提供機能及び実現技術が違うため、クラウドサービスモデル別、脅威要素を識別することはセキュリティを強化する一番簡単な方法でもいえる。責任共有モデルで重要なのはクラウドサービスモデル別に脅威が発生しうる要素に対するセキュリティ強化方法に対する対策とR&R(Role & Responsibilities)を分類することである。

クラウドサービス提供者が提供すべきのセキュリティ強化方法についてはSLA(Service Level Agreement)や提供サービスの明細による正確に認識されるのが必要である。クラウドサービ提供者は最小のセキュリティサービスを提供するため、追加的にセキュリティを強化するためにはセキュリティソリューションの導入、モニタリング方法などクラウド使用者が工夫する必要があるため、サービス目的とクラウドアーキテクチャ環境から発生しうる脅威要素が識別できるように努力する必要である。

02. クラウドコンピューティングのセキュリティ脅威要素

1) CSA基盤のクラウドコンピューティングセキュリティ脅威要素

CSAから発表したクラウドコンピューティングの主な脅威(Top Threats to Cloud Computing: Egregious Eleven)の2019年と2022年のリストをみるとクラウド環境のセキュリティ脅威を大きく管理的な観点と技術的な観点で分類できる。CSAから発表した2019年と2022年のクラウドセキュリティ脅威を確認してみると、コロナによる勤務環境の変化及びウクライナ・ロシア戦争のような国際情勢の不安によるクラウド環境のセキュリティ脅威も増加した。結局国内・海外の環境要因の変化によってサイバー環境の攻撃パラダイムも影響を受ける。



【図①　クラウドセキュリティ脅威要素 (参考：CSA, Top Threats to Cloud Computing: Egregious Eleven一部再構成)】

【図①】から分類した管理的なセキュリティ脅威と技術的なセキュリティ脅威で攻撃パラダイムの変化が理解できる。管理的な脅威ではクラウド環境に最適化されたクラウドセキュリティ管理体系の不在とヒューマンエラーによる問題が目立っている。2019年には内部脅威(Inside Threat)がセキュリティインシデントを起こす要因だったが2022年には内部脅威より管理不備や間違った構成の設定及びアクセス制御によるインシデント影響度が高くなっていることが確認できる。技術的な脅威でも攻撃の変化は目立っている。クラウドへの移行が増加してクラウドに最適化された(Cloud Driven)ソフトウェアが増加し、APIやサプライチェーンからシステム脆弱性やAPT攻撃による連鎖的なセキュリティ脅威が増加した。

【図①】から重要なのは管理的な脅威と技術的な脅威に影響を及ぼす「クラウドセキュリティアーキテクチャ及び戦略不足(Lack of Cloud Security Architecture and Strategy)」である。管理的な脅威からはクラウドセキュリティアーキテクチャ及び戦略不在によるセキュリティ脅威が問題になるが、技術的な脅威では管理的な脅威の影響によるクラウドの攻撃表面(AttackSurface)が増加し、クラウドの外部と内部のセキュリティ脅威に影響を及ぼしている。

クラウド環境のセキュリティ脅威及び対応方法を樹立するためにCSAから2022年に発表したクラウドセキュリティ脅威11個を基準で【表③】のように4つの項目を再グループ化して脅威を識別した。

NO	区分	脅威要素	脅威発生原因	対応方法	観点	主体	サービスモデル
1	セキュリティ体系及び戦略管理不備	不適切なID、資格証明、アクセス及びキー管理、特権アカウント (1) Insufficient ID, Credential, Access and Key Mgt, Privileged Accounts	認証及びアクセス制御に対する管理不在	アクセス権限及びアクセス制御	管理的	御客	IaaS, PaaS, SaaS
		間違った構成及び不適切な変更制御 (3) Misconfiguration and Inadequate Change Control	構成ミス及び間違った構成設定	モニタリング及び構成プロセス構築	管理的	共有責任	IaaS, PaaS, SaaS
		クラウドセキュリティアーキテクチャ及び戦略不足 (4) Lack of Cloud Security Architecture and Strategy	クラウドセキュリティ戦略及びアーキテクチャの不在	クラウドセキュリティ規定遵守及びアーキテクチャ戦略設計	管理的 / 技術的	御客	IaaS, PaaS, SaaS
		間違った構成 & サーバレスの脆弱性 & コンテナーワークロード (9) Misconfiguration & Exploitation of Serverless & Container Workloads	サーバレス及びコンテナーに対する管理不備	クラウドガバナンス及びセキュリティプロセス教育	管理的	共有責任	IaaS, PaaS
2	クラウドデータ情報漏洩	安全ではないインターフェース及びAPI (2) Insecure Interfaces and APIs	インターフェース及びAPI管理不備	ソリューションパッチ及びAPIトラフィックモニタリング	技術的	御客/CSP	IaaS, PaaS, SaaS
		偶然なクラウドデータ漏洩 / 公開 (8) Accidental Cloud Data Disclosure / Disclosure	クラウドセキュリティガバナンス及び制御不足	クラウドセキュリティ教育及びソリューション導入	管理的	共有責任	IaaS, PaaS, SaaS
		クラウド格納先データ漏洩 (11) Cloud Storage Data Exfiltration	クラウドの間違った構成及びアプリケーション脆弱性	クラウドセキュリティモデル設計	技術的	共有責任	IaaS, PaaS, SaaS
3	インフラの拡大及びソフトウェア共有増加	安全ではないソフトウェア開発 (5) Insecure Software Development	オープンソース脆弱性	セキュリティ脅威モニタリング及びペネトレーションテスト	技術的	共有責任	IaaS, PaaS, SaaS
		サードパーティリソースセキュリティ解除 (6) Unsecure Third Party Resources	サプライチェーン脆弱性		技術的	共有責任	IaaS, PaaS, SaaS
		システム脆弱性 (7) System Vulnerabilities	ゼロデー脆弱性		技術的	共有責任	IaaS, PaaS, SaaS
4	サイバー犯罪増加	犯罪組織 / ハッカー / APT (10) Organized Crime / Hackers / APT	ハッキング団体及びAPT脅威増加	サイバーセキュリティ専門企業支援	技術的	共有	IaaS, PaaS, SaaS

【表③　CSAのクラウドコンピューティングの主なセキュリティ脅威及び対応方法一部再構成（参考：イグルーコーポレーション)】

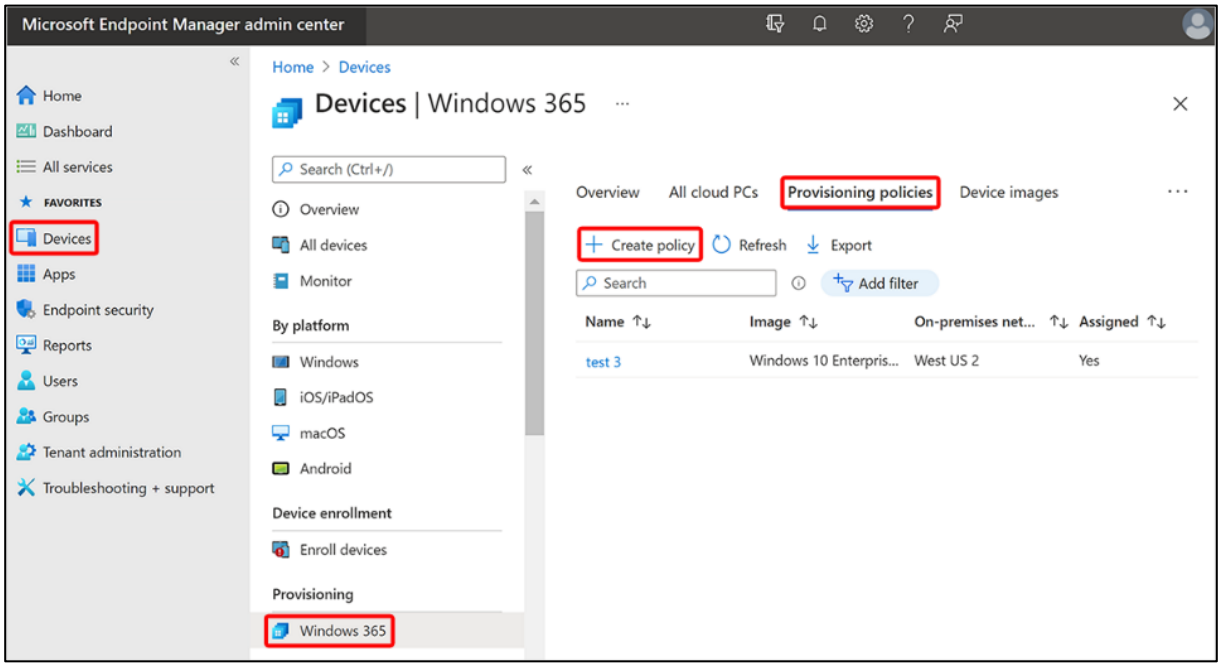
【表③】のようにクラウドセキュリティ脅威は大きく4つの項目に分類できる。「セキュリティ体系及び戦略と管理の不備」はクラウド体系に合うセキュリティ体系や戦略の不在及び管理方法の不備にようる問題である。アーキテクチャの設計、セキュリティソリューション、データの流れ、アクセス体系などクラウド環境に最適化されたセキュリティガバナンス及びアーキテクチャががない場合、セキュリティインシデントに繋がる可能性がある。「クラウドデータ情報漏洩」は恣意的や他意的な問題でクラウドに保存されているデータが公開される問題である。特にクラウドに保存されているクレデンシャルAPIや機密情報が漏洩された場合、2次被害が発生する可能性があるため影響度が高い。

「インフラの拡大及びソフトウェアの共有増加」はクラウド環境のソフトウェアライフサイクルを考慮しないセキュリティ脅威といえる。クラウド内で運用されているソフトウェアはオンプレミスと同じく静的分析と動的分析による脅威要素の除去活動が必要だが、ソフトウェア開発パラダイムと相まってAPIやパッケージなどサードパーティ(3rd Party)使用が増加されることによってクラウド環境にも影響を及ぼすことになる。「サイバー犯罪増加」は前の危険要素の悪用可能性が高くなり、攻撃者のターゲットが変化されていることを意味する。

2) クラウドセキュリティ脅威：① セキュリティ体系及び戦略と管理不備

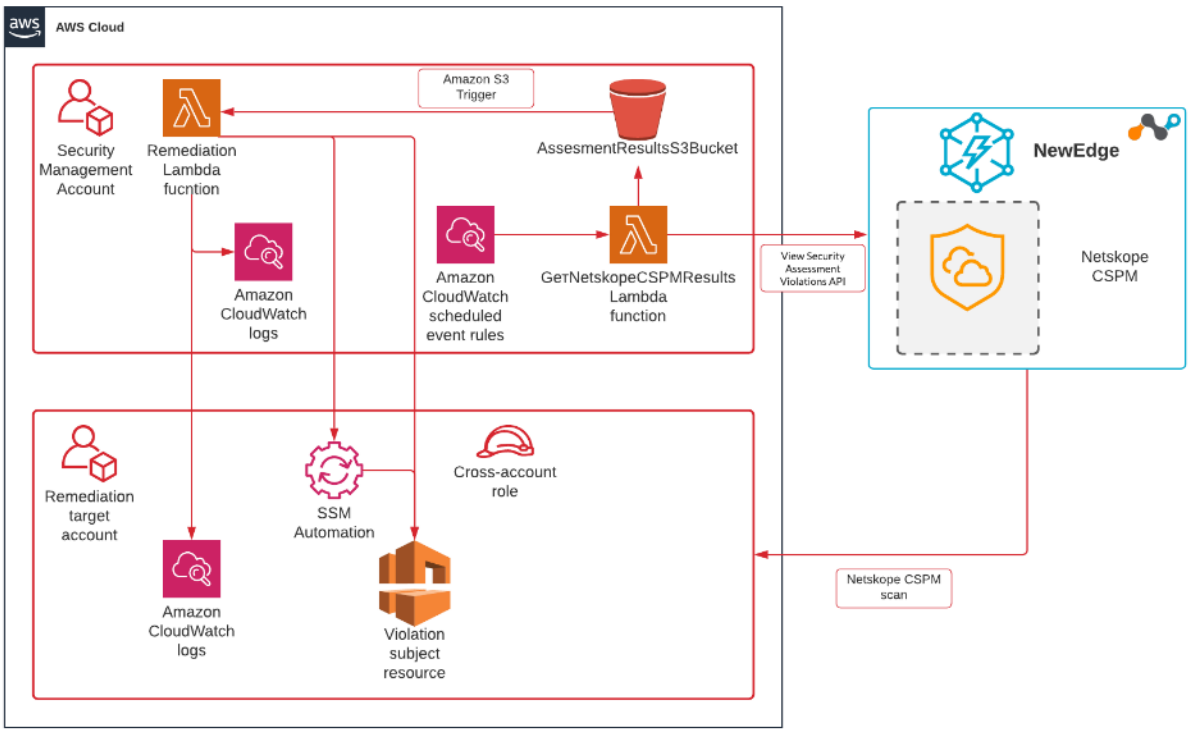
クラウドセキュリティ脅威が発生する11個の要素を4つのグループに分けて一つずつ調べてみよう。まず「セキュリティ体系及び戦略と管理不備」で発生するセキュリティ脅威には4つがある。「不適切なID、資格証明、アクセス及びキー管理、特権階層(Insufficient ID, Credential, Access and Key Mgt, Privileged Accounts)」はアクセス権限付与時、ユーザーの不注意によって発生する問題である。アクセス制御に影響を及ぼすID、資格証明、キー管理、アカウント管理の不在及び不備によるデータ漏洩が発生する可能性があり、権限上昇でアクセスが制限されたデータにアクセスすることができるようになる。

クラウドのアクセス制御を強化するためにはクラウドのリソースにアクセスするまえにクラウドサービス認証レベルぐらいの構築モデルを生成し、【図②】のようなProvisioningやDeprovisioning過程でリソースの権限とアクセス範囲を確認し、持続的なモニタリングが必要である。



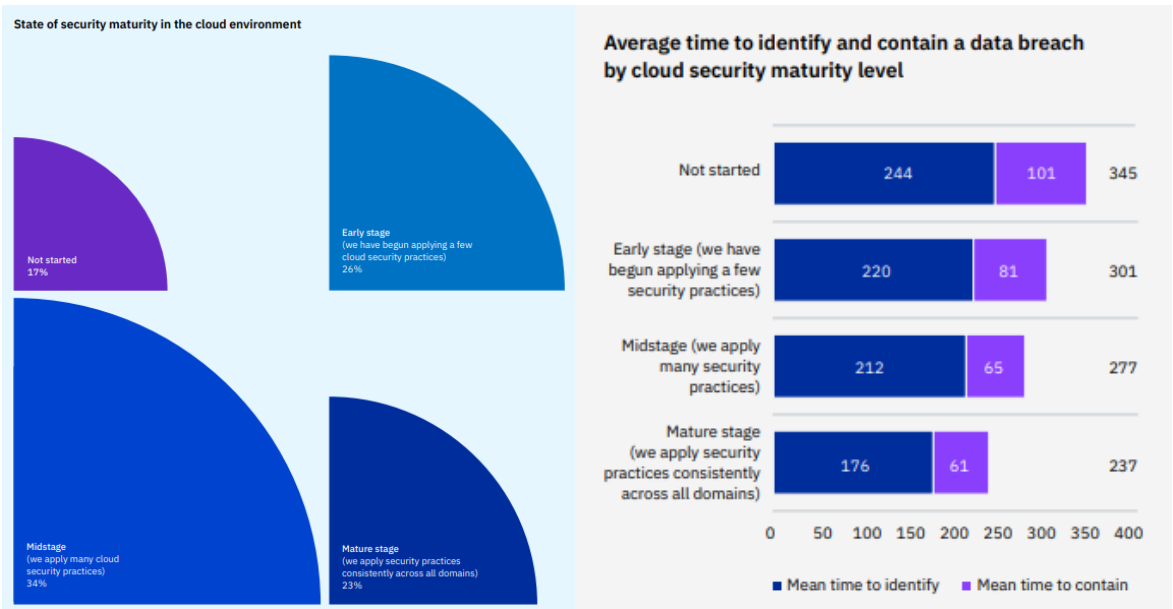
【図②　Microsoft 365のProvisioning過程中ポリシー設定画面 (参考：Microsoft) 】

「間違った構成及び不適切な変更制御(Misconfiguration and Inadequate Change Control)」はデータの保存先や間違ったコンテナー構成で資格証明漏洩及び不正アクセスが許可される問題である。セキュリティを強化するためには【図 ③】のようにCSPMソリューションを適用して持続的な変更制御を行う必要がある。不適切なクラウド構成はクラウドアーキテクチャの低い理解及び技術成熟度の低下によって発生しうる問題であるため、クラウド内サービス変化にたするモニタリングとサービス配布の前後にペネトレーションテストなどを実施し不適切な設定を確認する必要がある。



【図③ AWSのCSPM AutoRemediation (参考：Github, CSPM-AWS-AutoRemediation – CSPM security violation findings Auto-Remediation framework for AWS】

「クラウドセキュリティアーキテクチャ及び戦略不足(Lack of Cloud Security Architecture and Strategy)」と「間違った構成&サーバレス脆弱性&コンテナーワークロード(Misconfiguration & Exploitation of Serverless & Container Workloads)」はクラウドセキュリティ戦略と管理規定の現実化が重要である。2つのセキュリティ脅威要素はクラウドの復元力と抵抗性に影響を及ぼすため、クラウドサービスとインフラ設計時にガバナンス及びコンプライアンスなど多様な要素の考慮が必要である。クラウドセキュリティアーキテクチャの設計及び脅威モデリングプロセスはCSAから提示するセキュリティインフラ戦略を参考できる。

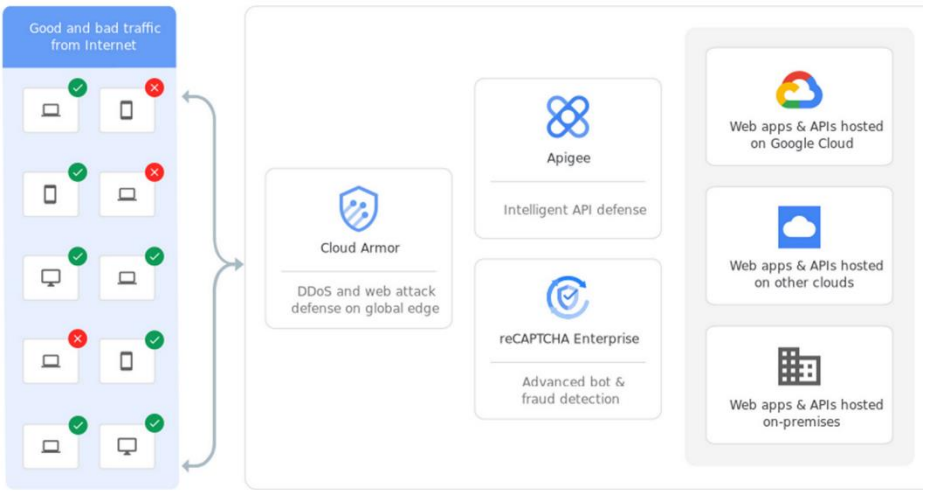


【図④ クラウド環境のセキュリティ成熟度(左)、クラウドセキュリティ成熟度レベルごにデータ漏洩期別及び抑制に所要される平均時間(右) (参考：IBM, 2022年データ漏洩費用レポート)】

クラウドセキュリティ成熟度によってデータ漏洩及び識別に所要される時間が違うが、【図 ④】はIBMデータ漏洩レポートのクラウドセキュリティ成熟度に関する内容である。セキュリティ成熟度が高い場合、平均176日が所要されるが、セキュリティ成熟度が低い場合平均244日が所要される。結局、セキュリティ成熟度はデータ漏洩インシデントを識別して対応するのに平均68日を減少する効果があるため、クラウドのセキュリティレベルの強化は必須的な要素とも言える。

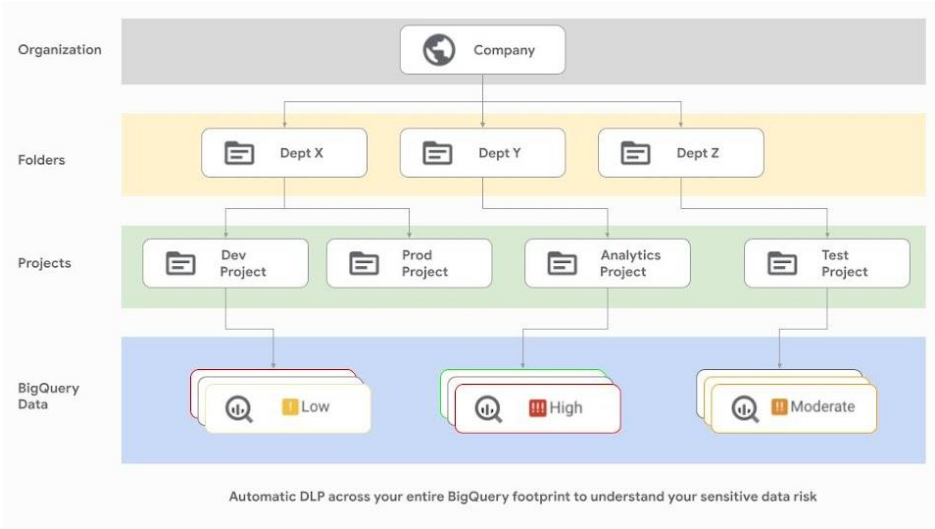
2) クラウドセキュリティ脅威：② クラウドデータ情報漏洩

「安全ではないインターフェース及びAPI(Insecure Interfaces and APIs)」はAPI使用量の増加と関係ある。Akamai 2021レポートによると300兆個以上のAPIリクエストが発生していてこの数値は前年と比べて53%増加した数値だと発表した。API使用量の増加は「安全ではないインタフェース及びAPI(Insecure Interfaces and APIs)」のセキュリティ脅威に繋がるしかない。インタフェースやAPIは機能明細意外に機能やセキュリティ脅威を識別することが難しいため、ソフトウェアを開発時、セキュアコーディングの適用及びSAST, DASTなどを実施したり【図 ⑤】のようにWAAPソリューションに適用が必要である。



【図⑤ Google Cloud WAAPソリューションアーキテクチャ (参考：Google Cloud, Better protect your web apps and APIs against threats and fraud with Google Cloud)】

「偶然なクラウドデータの漏洩/公開(Accidental Cloud Data Disclosure / Disclosure)」はクラウド環境の可視性の不在とデータ管理不備によって発生する。マルチクラウドやハイブリッドクラウドで構成されているサービスの場合クラウド間のセキュリティ可視性が低下してネットワークセキュリティ不備及び間違った設定にデータの漏洩が引き起こされる。従って、クラウドサービス運用のためには組織構成員にクラウドセキュリティ教育及び政策を提示し、データ漏洩による問題を最少化して【図 ⑥】のようなCloud DLPなどでデータの流れを分析し、漏洩有無の確認が必要である。



【図⑥　Cloud DLP使用事例 (参考：Google Cloud, Cloud Data Loss Prevention)】

「クラウド保存先データ漏洩(Cloud Storage Data Exfiltration)」は内部役職員を対象にする「フィッシング(Phishing)」やセキュリティアーキテクチャを対象にする「サプライチェーン攻撃(Supply Chain Attack)」から発生する。クラウドセキュリティアーキテクチャ及ガバナンスを樹立したとしてもデータ漏洩インシデントはいつでも発生する可能性があるためクラウド環境に最適化されたデータ漏洩脅威及びインシデント対応計画を樹立する必要がある。

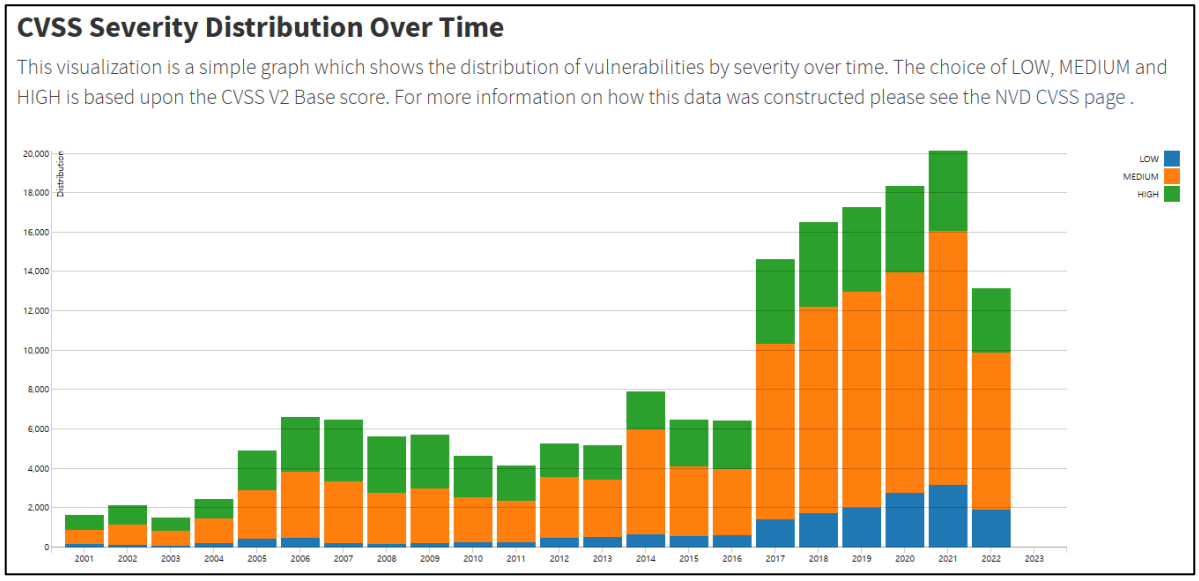
【図⑦　データ漏洩による平均費用増加 (参考：IBM, 2022年データ漏洩費用レポート)】

【図⑦】のIBMのレポートによると2020年から2021年にデータ漏洩費用が386万ドルから424万ドルに増加し、2022年には435万ドルに増加した。2年間平均費用が12.7%増加することであるが、コロナの影響でリモートワークが続くことで管理不備及び外部攻撃によるデータ漏洩セキュリティインシデントが発生したためである。従って社会的にリモートワークとデータ漏洩間の密接な相関関係があると分析できる。更に管理不備とも相関関係があると解析できる。追加にコロナ以外にもデジタル社会が発展してクラウド移行が加速化されることでデータ情報漏洩による問題は2022年以降にも持続的に増加すると専門家たちは予測する。

2) クラウドセキュリティ脅威：③ インフラの拡大及びソフトウェアの供給増加

「安全ではないソフトウェア開発(Insecure Software Development)」と「システム脆弱性(System Vulnerabilities)」はSDLCと関連している。ソフトウェア上に発生する弱点(Weakness)と脆弱性(Vulnerabilities)を管理しないと連鎖的なセキュリティ脅威を引き起こす。従って、ソフトウェアサプライチェーンの強化のためにはソフトウェアセキュリティ強化及びセキュリティアップデートの政策を作る必要がある。

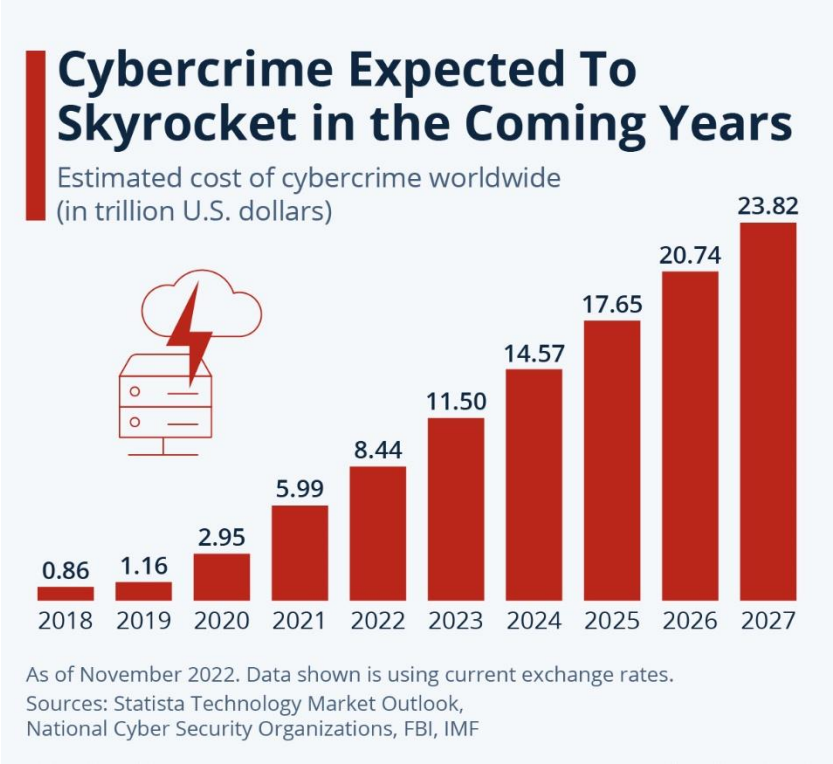
「サードパーティリソースセキュリティ解除(Unsecure Third Party Resources)」は全てのソフトウェアサプライチェーンに影響を及ぼす。オープンソースソフトウェアやAPI、インターフェース、フレームワークなどでソフトウェアが有機的な繋がりを持つため、脆弱性が発生すると新たな攻撃のトリガーとして悪用できる。そのため、ソフトウェアサプライチェーンのセキュリティ強化のためにSBOM(Software Bill of Material)などでソフトウェア構成要素の透明性の確保が必要である。



【図⑧　セキュリティ脆弱性増加統計 (参考： NIST, CVSS Severity Distribution Over Time)】

【図 ⑧】はアメリカNIST(National Institute of Standards and Technology)から発表したセキュリティ脆弱性推移を整理した資料である。ソフトウェア数値が増加することでソフトウェア脆弱性も増加していることが確認できる。クラウドへの移行でインフラのオープンソース活用が増加してる。サービスを構成している一部ソフトウェアに活用されていたオープンソースはOS、データベース、WEB/WAS、フレームワークなど多様な領域に拡大することでオープンソースによるセキュリティ脅威も増加している。

ソフトウェアセキュリティ強化のためにはソフトウェア開発組織の業務プロセス及びツール、人、構成要素などを識別することから始まる。SSDLC(Secure Software Development Life Cycle)を実現するためにはソフトウェアの要求事項、分析、設計、実現の流がれで段階別の検証とテストが必要である。



【図⑨　サイバー犯罪増加展望 (参考： statista, Cybercrime Expected To Skyrocket in Coming Years)】

【図⑨】のようにStatistaから発表した資料によると組織の勤務体系及び国際情勢変化によるサイバー攻撃の比率が増加されている。勤務体系の多変化によるリモートワークの拡散はVPN、RDPなどリモートアクセス環境の増加で内部システムにアクセスできる攻撃接点として悪用される可能性が高くなった。また、国家支援型サイバー攻撃が増加することで北朝鮮、ロシアなどサイバー攻撃の活動増加でクラウドの被害規模が大きくなり、「犯罪組織 / ハッカー / APT(Organized Crime / Hackers / APT」によるクラウドセキュリティ脅威影響度が増加された。

組織化されて高度化されたサイバー攻撃に対応するためには体系的なセキュリティ体系を樹立することが必要である。持続的な脅威ハンティング(Threat Hunting)でクラウドインフラの可視性を確保し、OSINTやIntelligenceなどを分析して先制的なセキュリティ対応体系の構築が必要である。

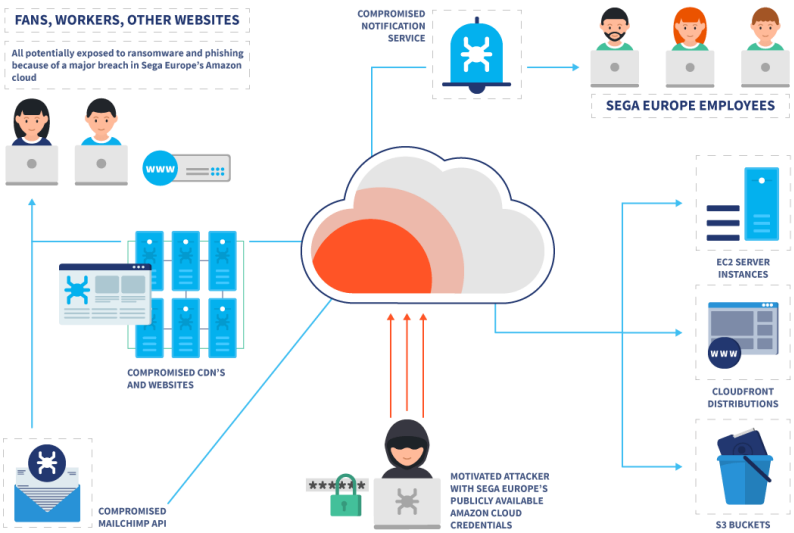
今までCSA基盤のクラウドコンピューティングのセキュリティ脅威と攻撃ベクターなどを分析した。次はクラウドのセキュリティインシデントを基にクラウドセキュリティ脅威に対応する方法について調べてみよう。

03. 事項事例分析からみるクラウドセキュリティ対応時の考慮事項

1) クラウドセキュリティ体系及び戦略と管理不備を対応するための考慮事項

クラウド環境のセキュリティインシデント事例から導出した4つのセキュリティ脅威ベクターでクラウド環境のセキュリティ考慮事項を調べてみよう。クラウドセキュリティに対する理解度と成熟度が増加し、一部緩和されたようにみえるがいまだにクラウドセキュリティ体系及び戦略と管理不備の問題はクラウド環境から持続的発生している。

2022年7月アマゾンのS3バケットの設定間違いでコロンビアとペルー空港4か所を含めて空港に関するデータ3TBが外部に漏洩され、航空会社職員の写真及び社会保障番号情報などの職員個人識別情報も含まれていた。同じ2022年10月マイクロソフトもクラウドストレージ設定間違いでAzure Blobストレージバケットが漏洩されて6万5千個の企業に関するデータが漏洩された。



【図⑩ SEGA Europeクラウドセキュリティ脆弱性 (参考： VPNoverview.com, SEGA Europe Thoroughly Scrutinizes its Cloud Security)】

SEGAのクラウドセキュリティ事例分析からクラウドセキュリティ体系及び戦略と管理不備による問題点、そしてセキュリティ強化のための考慮事項について詳細に調べてみよう。SEGAクラウドセキュリティインシデントは公開的にアクセスできるAWS S3バケットに間違って機密ファイルが保存されて第3者がアクセスできる問題だった。当該のバケットはデータアクセス及び修正ができる色々なキーと資格証明が含まれていて追加的な被害を予想したが迅速な対処で追加被害が発生しなかったため、セキュリティインシデント対応プロセスの模範事例ともいえる。

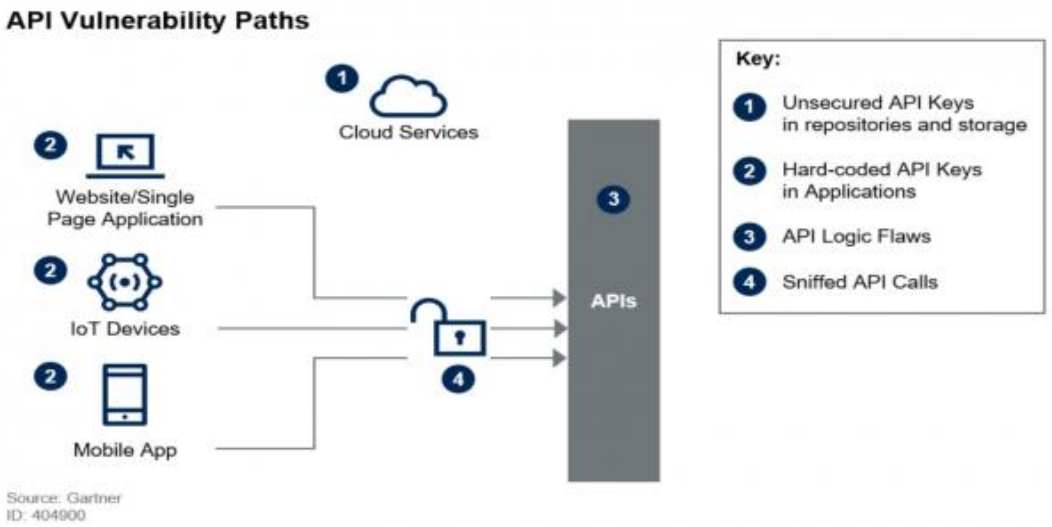
【図⑩】の攻撃シナリオを見ると第3者はバケットに保存されているキーと資格証明でアクセスが可能な問題がある。バケット情報を利用してCDN(Content Delivery Network)と結合するとマルウェアやランサムウェアの流布が可能になる。また、漏洩された資格証明を使用すると悪的なアラートの生成やMailChimp損傷を利用したAPI攻撃が可能になる。

AWS S3のバケット構成ミスによるセキュリティインシデントは最近も続けて発生している。従って実行発生時、管理者のミスや間違った構成で問題が引き起こされるためバケット設定時には非公開設定前提として保存されたデータによって公開有無を決定する方法の適用が必要である。また、インシデント対応及び分析のためにバケットロギング設定で正常の動作有無や以上アクセスのモニタリングが必要である。

他の方法としてはS3バケットに保存されたデータを暗号化することである。AWS S3暗号化機能はデフォルト的には無効になっているため、保存されたデータによって暗号化適用の考慮が必要である。暗号化はデータ保存以外にも送信・受信間の暗号化まで考慮する必要があるため、技術ステックを考慮してネットワーク及びエンドポイントの送信・受信のセキュリティを講ずる必要がある。

2) クラウドデータ情報漏洩対応のための考慮事項

クラウドデータ情報漏洩によるインシデント事例はAPI攻撃やセキュリティガバナンス及び制御不足にようる問題などが関連されていてデータ情報漏洩に繋がる。海外セキュリティ業者であるCloudSEKの発表にようると3,207個のアプリの中で230個が認証関連クレデンシャル4つを全部公開していて、ツイッターアカウントの奪取ができる問題につながる可能性があると発表した。これはツイッターAPIが漏洩されるモバイルアプリが悪用される問題であるため、API管理不備や悪用が発生する場合、データ情報漏洩に繋がる可能性がある体表的な事例だといえる。



【図⑪　API脆弱性経路 (参考：Gartner)】

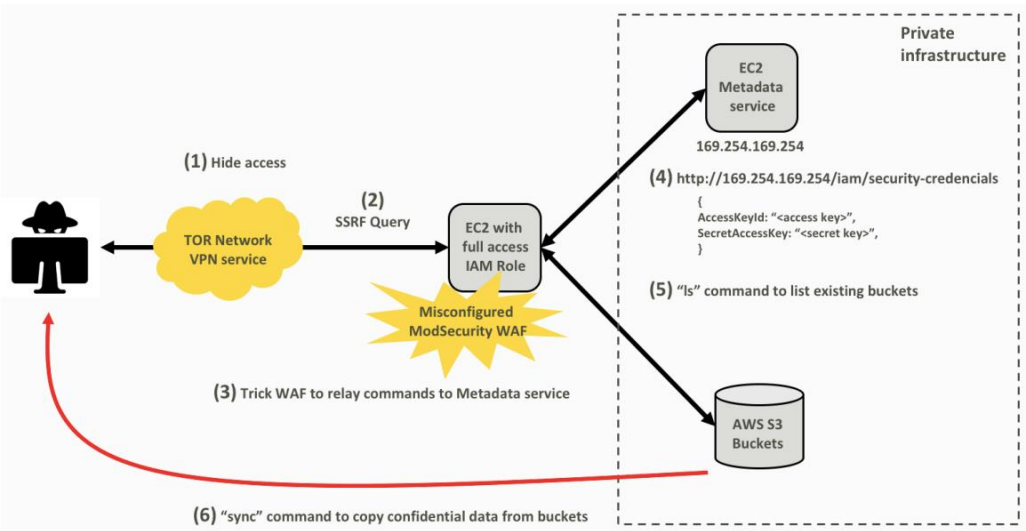
Gartnerから発表した【図⑪】のようにAPIで発生する脆弱性や攻撃ベクターは多様であるため、対応方法を講ずる際に多様な観点の考慮が必要である。GartnerはAPI脆弱性パスと共に企業のAPI管理不備で今後2025年まで攻撃者の攻撃ベクターとして悪用されると警告した。また、API攻撃を対応するためにはAPI保護機能が実現されたソリューションの導入及びセキュリティチェックの必要性を語った。

Elasticsearchもサーバの設定ミスによる問題で「意図しないデータの漏洩」の危険性を警告している。Elasticsearchの使用率が増加することで間違って構成されたサーバの設定がデータ漏洩に繋がることが頻繁になり、クラウドセキュリティガバナンス樹立及び制御の必要性を強調した。

アメリカの大手金融持株会社であるCapital Oneの事例は脆弱性によるデータ漏洩の危険性を語っている。退職した職員がSSRF(Server Side Request Forgery)の脆弱性を悪用してAWSサーバを攻撃し、約14万名の社会保障番号と約8万この銀行口座情報が奪取された。

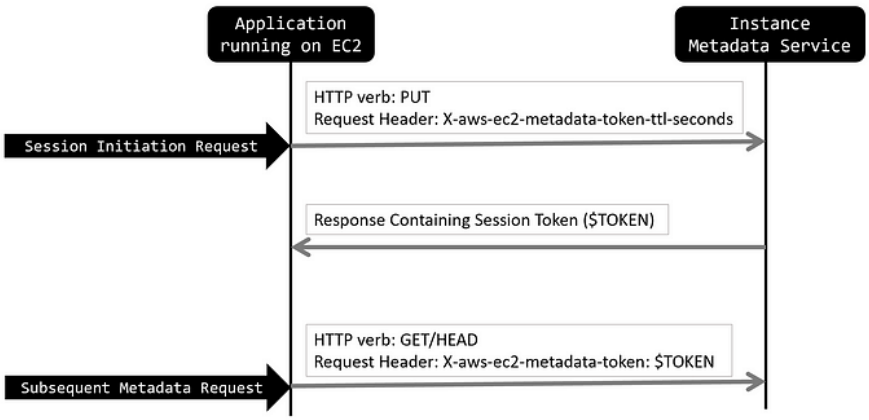
SSRF攻撃は一般的に外部から内部にアクセスができない対象に行う攻撃で脆弱なサーバにサーバ内部のリースに対するリクエストを改ざんして行う攻撃である。SSRF脆弱性は現在様々な企業がクラウドへ移行している今の時期に巨大な脅威として増加している。クラウドではサーバリソースに対するアクセス権限を制限してセキュリティを強化するために多様な方法が存在するが、クラウド内部のサービスはお互いネットワークで繋がっているためSSRF攻撃にとても脆弱である。

【図⑫】はMIT Sloanから分析したCapital Oneの攻撃流れ図である。まず攻撃者は匿名化のためにTorネットワークサービスを使用して複数アクセスを試みる。既存Capital OneはSSRF攻撃を防ぐためにWAF(Web Application Firwall)セキュリティポリシーを設定したが、間違った構成設定で攻撃が防げなかった。攻撃者AWS EC2インスタンスメタデータに対する要請を改ざんし、その結果S3バケットでデータのアクセスができた。



【図⑫ Capital Oneの攻撃流れ図 (参考： Cybersecurity at MIT Sloan, A Case Study of the Capital One Data Breach)】

Capital Oneインシデント事例は内部者の脅威と間違って構成されたWAFによるインシデントである。しかしSSRF脆弱性は今のクラウド時代に引き続き増加してる脅威であるため、適切な分析と対応が必要である。攻撃者がCapital Oneを対象にSSRF攻撃ができた原因はCapital OneのAWSは脆弱なインスタンスメタデータアクセス方法であるIMDSv1を使用しているためである。IMDSv1はメタデータURLに対してGETリクエストし、メタデータの情報漏洩が簡単で、これを利用して変更または改ざんができる。従って対応できる方法としてIMDSv2を使用した方が良い。【図⑬】のようにIMDSv2はGETリクエストをする前にPUTリクエストでTokenを発行して、Tokenを利用してGETリクエストをメタデータのURLで送信するため、SSRF攻撃に対応できる。

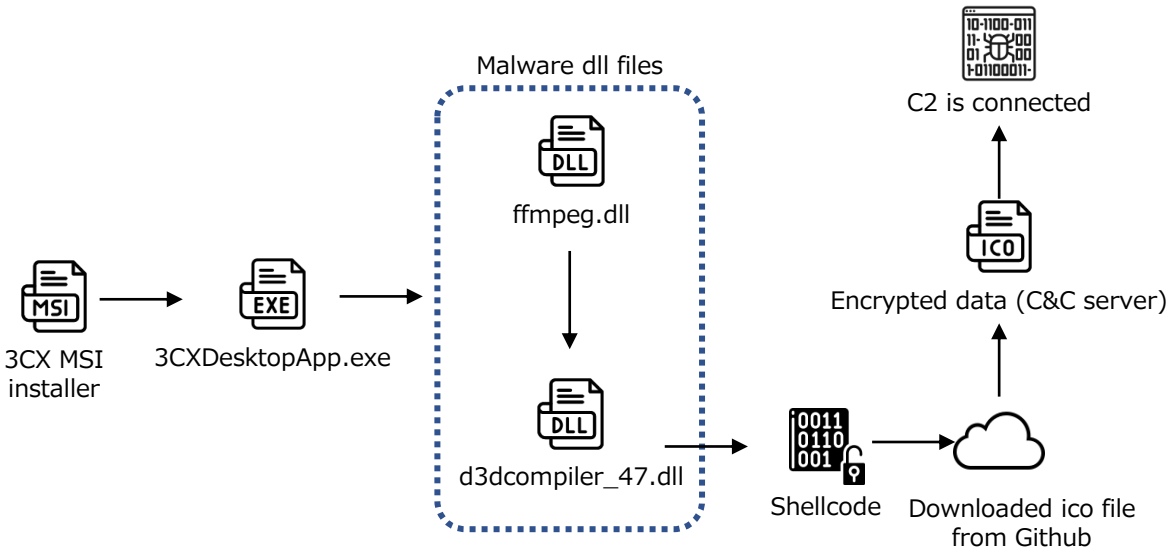


【図⑬　IMDSc2セッション流れ図 (参考：　medium.com, AWS Enhances Metadata Service Security with IMDSv2)】

また、入力値に対する検証を徹底に実施し、外部から送信されるリクエストをフィルタリングすることも一つの対応方法になる。URLに対しては許可リストを設定し、必要なURLのみ許可する方法がある。追加にユーザーが入力したURLを検証し、有効なURLであるか確認して間違ったURLを修正したりユーザーが入力したURLを中継サーバから変換して安全に送信する方法を使用することを推奨する。

3) インフラ拡大及びソフトウェア供給増加対応のための考慮事項

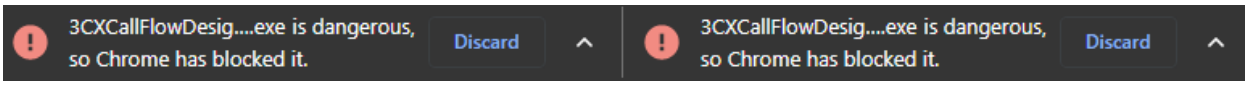
コロナによる非対面及びリモートワーク環境の拡散と企業のクラウド移行などデジタル社会が加速化されてソフトウェアの供給と開発も同じく加速化された。これの事例がLog4jオープンソースとSolarWindsのサプライチェーン攻撃である。二つの事例は大きく問題になってSBOMと呼ばれるソフトウェアの構成要素に関するメタ情報が注目されることになり、サプライチェーン管理とよばれるSCM(Supply Chain Management)のセキュリティの重要性が話題になった。



【図⑭　3CXサプライチェーンWindows環境攻撃流れ図】

最近にはクラウド基盤のIP PBXシステムを提供する統合コミュニケーションソリューションである3CXがサプライチェーン攻撃を受けた。【図⑭】のWindows環境の攻撃流れをみるとMSIファイルで関連ファイルをインストールした後、「3CXDesktopApp.exe」ファイルを実行して悪性DLLファイルをロードする。「ffmpeg.dll」は「d3dcompiler_47.dll」ファイルの中にインコードされたデータを読み取る機能を実行する。インコードデータをデコードすると、シェルコードが存在し、メモリに存在するマルウェアを実行させる。当該のマルウェアはダウンローダー機能を実施してGithubからicoファイルをダウンロードするが、icoファイルには実際C&Cサーバのアドレスがインコードされて存在する。

当該の脆弱性の解決方法として現在3CX業者に新たな証明書を発行するまでに他のソフトウェアであるPWAアプリケーションを代わりに使用するように対処した。追加に脆弱性パッチが必要だが、3CX Hosted/StartUP御客は別途の対応は要らなく、ホスティングサービスを実施及びオンプレミス環境の御客は最新バージョンにアップデートが必要である。また、【図⑮】のようにGoogle Chromeからはソフトウェアセキュリティ証明書を無効にして3CX MSIインストールファイルからダウンロードできないように対応した。

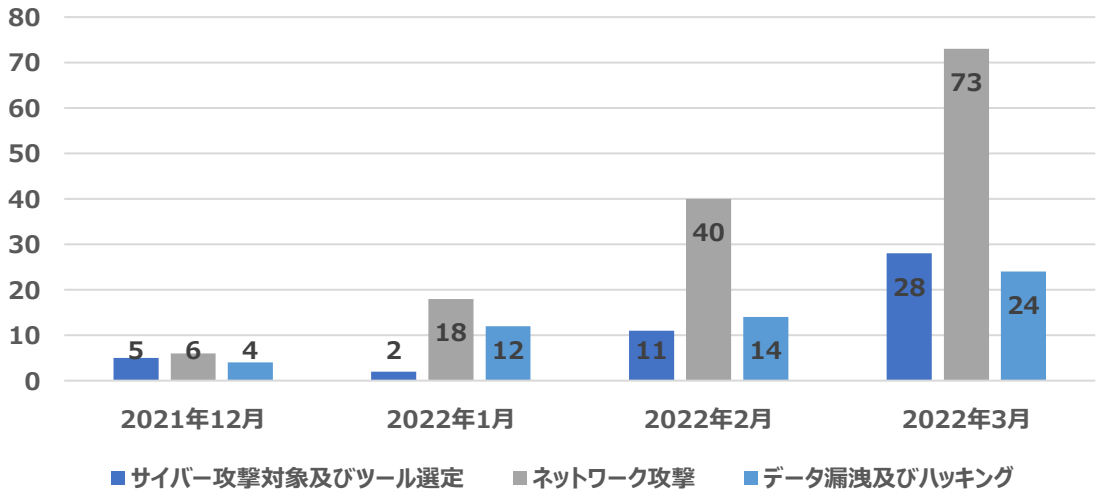


【図⑮ Chromeの3CX MSIインストールプログラムの遮断 (参考： 3CX, Chrome blocks latest 3CX MSI installer)】

SolarWinds及び3CXのようなサプライチェーン攻撃が二度と発生しないようには持続的なセキュリティ強化体制を構築することが大事である。現在の資産は何があるのか調査して記録することも一つの対策になる。また、不要もしくは不法的にダウンロードされて認証なく使用されるソフトウェア及びサービスはセキュリティに脆弱な状態になる可能性がある。このようにクラウドを介した攻撃は見落とせない脅威であり、オープンソース及びサプライチェーンのセキュリティ脆弱性分析と積極的な対応が要求される。

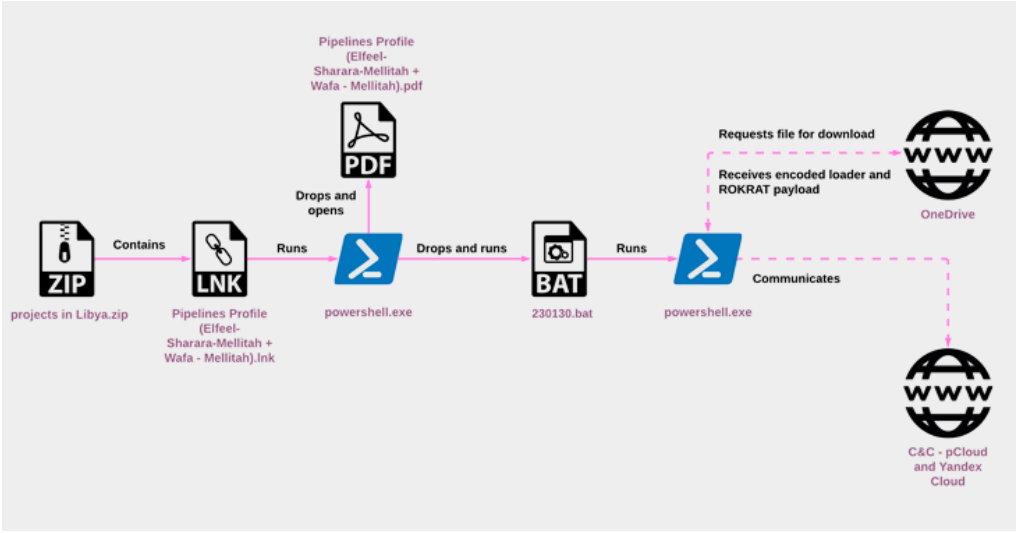
4) サイバー犯罪増加対応のための考慮事項

サイバー犯罪とハッキング団体の攻撃試みは引き続き増加していて最近ウクライナ・ロシア事態とも関係深い。また、受益創出のための仮想資産及びランサムウェア攻撃も活発であるが、北朝鮮はクラウドサービスを悪用して仮想通貨のマイニング及びフィッシング攻撃など多様な攻撃ほうほうで国家及び企業を脅威させている。



【図⑯　2021年12月以降のロシアサイバー活動 (参考： Microsoft, An overview of Russia's cyberattack activity in Ukraine)】

【図⑯】はウクライナとロシアの戦争以降のサイバー活動に対するイベントを表すものである。ロシア戦争は2022年2月に始まって以前ロシアのサイバー攻撃が段々進行されて2月に急速に増えたことが確認できる。調査されたサイバー攻撃段階によると「サイバー攻撃対象及びツール選定(Tooling and Reconnaissance)」でアクセスを確保して目標対象と侵入先を広げて追加的にネットワークアクセスで「ネットワーク攻撃(Actions on Network)」を行い、持続性を高めた。結果的に主要基盤施設と多数の企業が「データ漏洩及びハッキング(Data Exfil/Destruction)」の被害が発生した。



【図⑰　LNKファイを利用したRokRATマルウェア (参考： TheHackerNews, North Korea's ScarCruft Deploys RokRAT Malware via LNK File Infection Chains)】

最近北朝鮮は【図⑰】のようにLNKファイルでRokRATマルウェアを配布していると知られている。LNKファイルはPDFアイコンのように偽装していて悪性パワーシェル(powershell)コマンドが含まれている。攻撃者は正常PDFファイルでユーザーをごまかし、スクリプトファイルで不正行為を実施する。最終的にパワーシェルにインコードされたデータをダウンロードし、当該のデータをプロセスにインジェクションした後、収集した情報をクラウドサービスを利用して攻撃者のサーバに送信する。このような持続的なAPT(Advanced Persistent Threat)攻撃はクラウドサービスに影響を及ぼすため、ユーザーの注意が必要である。

このようなハッキング団体とAPT攻撃に対応するためには、システムのセキュリティアップデートを定期的に実施し、脆弱性管理を徹底的に行う必要がある。システムセキュリティ脆弱性が持続的に増加していてハッキング団体とAPT攻撃者はこのような点を利用して攻撃するためである。また、強力なパスワード及びアクセス制御でシステムを保護することも重要である。これを利用すると機密データを非承認者から保護できる。

【図⑱ ソーシャルエンジニアリング技術の種類 (参考： seon.io, What Are Social Engineering Attacks? Techniques & Protection)】

APT攻撃者は【図⑱】のように多様な方法のソーシャルエンジニアリング技術を利用するため戦略的に対応することが重要である。対応するためには企業のセキュリティ教育が最も重要で職員のセキュリティ認識を高めて悪性メールやウェブページに注意するようにする。また、多段階認証(Multi-factor Authentication, MFA)を使用して攻撃者のアカウント奪取からの脅威を減らすことができる。その他にも様々な方法はあるが、APT攻撃はセキュリティ認識を強化することが最も大事である。

最近ハッキング団体の攻撃はとても巧妙に行われるため、企業は多様な対応方法を利用して攻撃を防止し、対応しなければならない。セキュリティ戦略を持続的に検討し、アップデートすることも重要でこれのために企業はセキュリティ担当者とペネトレーションテストなどのセキュリティテストを行い、脆弱性を洗い出して対応する必要がある。また最近のセキュリティ動向を把握して最新の脆弱性と攻撃ツールを探してセキュリティソリューションを利用し、迅速な検知と遮断をすることが重要である。

04. 最後に

今までクラウドセキュリティインシデントからクラウド環境のセキュリティ脅威と対応方法について調べてみた。クラウドへの移行が本格化されてクラウドセキュリティインシデントに対する認知と分析及び対応方法が必須になった。サイバー攻撃は知能的に発展し、ハッキングツールは上位標準化になってもっと脅威的になっている。従って、流動的なクラウド環境からは全てのユーザーを信頼しない環境構成を前提にする「ゼロトラストアーキテクチャ(Zero Trust Architecture)」モデルが必要がある。

オープンソースとサプライチェーンそして多様なアーティファクトに対する脅威が増加している社会で具体的な対応方法の準備と能動的な体系が重要である。クラウド環境は流動的ネットワーク環境とリソースを提供するために脅威にさらされやすい。既存のネットワーク境界中心のセキュリティクラウド環境にとても脆弱なであるため、高度化されるサイバー攻撃に対応するためには追加的な戦略が必要である。このようにCSAのクラウドの脅威とセキュリティインシデント事例分析でクラウド環境のセキュリティ脅威を最少化させることが重要である。

05. 参考資料

1) https://cloudsecurityalliance.org/press-releases/2022/06/07/cloud-security-alliance-s-top-threats-to-cloud-computing-pandemic-11-report-finds-traditional-cloud-security-issues-becoming-less-concerning/
2) https://www.ibm.com/kr-ko/reports/data-breach
3) https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time
4) https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/
5) https://vpnoverview.com/news/sega-europe-security-report/
6) https://web.mit.edu/smadnick/www/wp/2020-16.pdf
7) https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-service.html
8) https://asec.ahnlab.com/ko/50965/
9) https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
10) https://thehackernews.com/2023/05/north-koreas-scarcruft-deploys-rokrat.html
11) https://www.imperva.com/learn/application-security/social-engineering-attack/