SECURITY REPORT

2023

FEB

2023年
サイバーセキュリティ脅威及び
対応技術の展望

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。

2023年サイバーセキュリティ脅威及び対応技術の展望

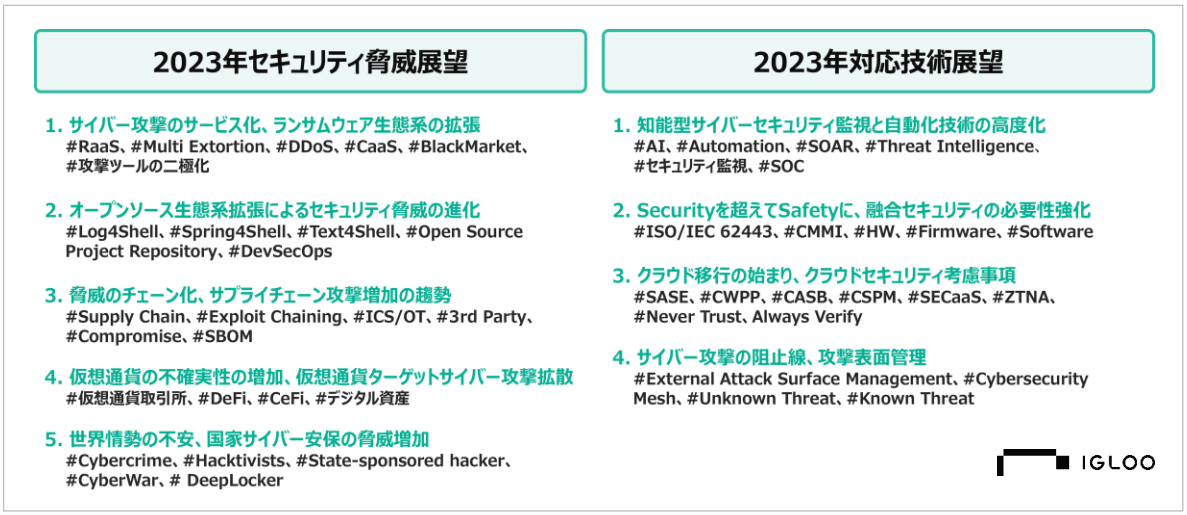
01. 概要

2022年、サイバーセキュリティのキーワードは、ランサムウェア・仮想通貨・国家安保に分類される。
2022年には、LockBit、Conti、Lapsus$、BlackCat、Hive、Deadboltなどのランサムウェアグループが登場した。また、クラウドを利用した犯罪収益の確保が容易になったため、新たなランサムウェア攻撃グループが現れ、組織的な攻撃やサービス型ランサムウェアが増えている。このような進化したランサムウェアによる被害は、個人や企業だけでなく、国家安全保障やグローバル経済市場にも影響を与えるようになり、アメリカを中心に30ヶ国が参加したランサムウェア対策会議が開催された。

ロシアとアメリカ、及び西側諸国間の利害衝突は、世界経済と覇権秩序を揺るがす、サイバーセキュリティの新たなゲームチェンジャー(game changer)として定着している。ロシアのウクライナ侵攻は、物理的な衝突とサイバー攻撃が結合された最初のハイブリッド戦争の事例として記録され、社会の混乱を引き起こし、主要機密情報の奪取、社会基盤施設の破壊、犯罪資金確保などの分野で、サイバー攻撃の効果が出た。ロシアとウクライナの事態は、各国の支持勢力を結集させることとなった。ウクライナ支持勢力は「Operation Ruble」というキャンペーンでロシア政府機関を攻撃した。一方、ロシア支持勢力はアメリカ及び友好国の政府機関及び民間企業への攻撃を行った。この結果、サイバー攻撃が国家間の利害関係を支援する新たな手段として浮き彫りになり、国際安全保障に緊張感が高まっている。

2022年、仮想通貨の人気が低下している。その理由は、世界第3位の仮想通貨取引所であるFTXの破産が影響しており、仮想通貨市場の不確実性が拡散していること、さらにNFT・ステーブルコイン・電子マネー・カストディなど、仮想通貨を含むデジタル資産のセキュリティインシデントが生態系を脅かしていることが原因である。
Flash Loan攻撃、Smart Contract脆弱性、プライベートキー漏洩、電子財布のマネー奪取、仮想通貨の盗難など、仮想通貨とデジタル資産のセキュリティ問題は、2023年にも引き続き話題になるだろう。

デジタル技術を基盤としたビジネスの生態系が広がることで、サイバーセキュリティは選択肢ではなく必須の要素となっている。インフラ選択段階やアーキテクチャ設計段階からセキュリティが考慮され、連鎖的なリスクチェーン化を防ぐために、人工知能や自動化技術を用いたセキュリティの効率性向上やセキュリティホールを最小限に抑える研究が進んでいる。
2023年にはサイバー環境の不確実性を解消するためのセキュリティ脅威が予測され、それに対応する安全な環境を構築する方法が模索されるだろう。



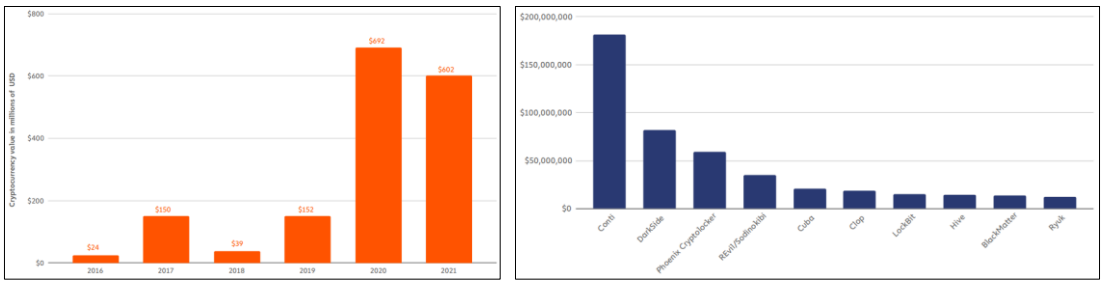
【▲ 2023年サイバーセキュリティ脅威及び対応技術の展望 (参考：イグルーコーポレーション)】

2023年サイバーセキュリティ脅威及び対応技術の展望

02. 2023年5大サイバーセキュリティ脅威展望

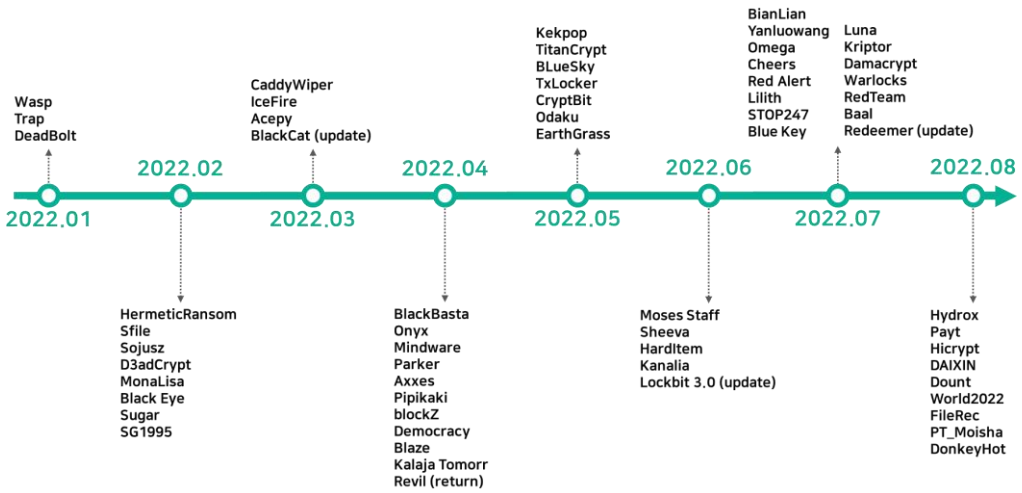
(1) サイバー攻撃のサービス化、ランサムウェア生態系の拡張

サイバー犯罪の専門家や組織は、サービス型ランサムウェア(RaaS)というビジネスモデルを誕生させた。Hive、LockBit、Conti、REVilなど、標的型ランサムウェアを運用している攻撃グループは、Colonial Pipeline、Kaseya、JBS Foodsなどへの大規模攻撃を行い、攻撃範囲はますます拡大している。彼らは体系化された組織運用と被害金額の交渉能力を保有し、公共、金融、製造、教育、国防など、多様な産業に攻撃を仕掛けている。RaaSの生態系では、Discord、Telegram、Wicker、Wireなど、制限されたアプローチ環境を基盤として、サイバー犯罪に使用されるツールや人材を確保しながら、不法データの取引、マネーロンダリング、クレデンシャルの取引、攻撃ツールの取引などが行われ、新しいサイバー攻撃の生態系形成に一役買っている。



【▲ (左) Total cryptocurrency value received by ransomware addresses, 2016–2021、(右) Top 10 ransomware strains by revenue, 2021 (参考： The 2022 Crypto Crime Report, Chainalysis)】

民間ランサムウェア対応から発表した「ランサムウェア動向レポート」によると、2022年にはDeadBolt、Luna、BlueSky、CryptBit、Acepy、BlackCat、Lockbitなど、様々なランサムウェアが登場し、高度化したことが確認された。最近のランサムウェアは、Windows環境に加えてLinuxや組込みシステムなどのクロスプラットフォームにも対応し、サプライチェーン攻撃、セキュリティソリューションの無力化、リストアやバックアップファイルの削除など、攻撃方法を発展させている。



【▲ 2022年発見された新規ランサムウェア攻撃グループの現況 (参考：KARA、ランサムウェア動向レポート)】

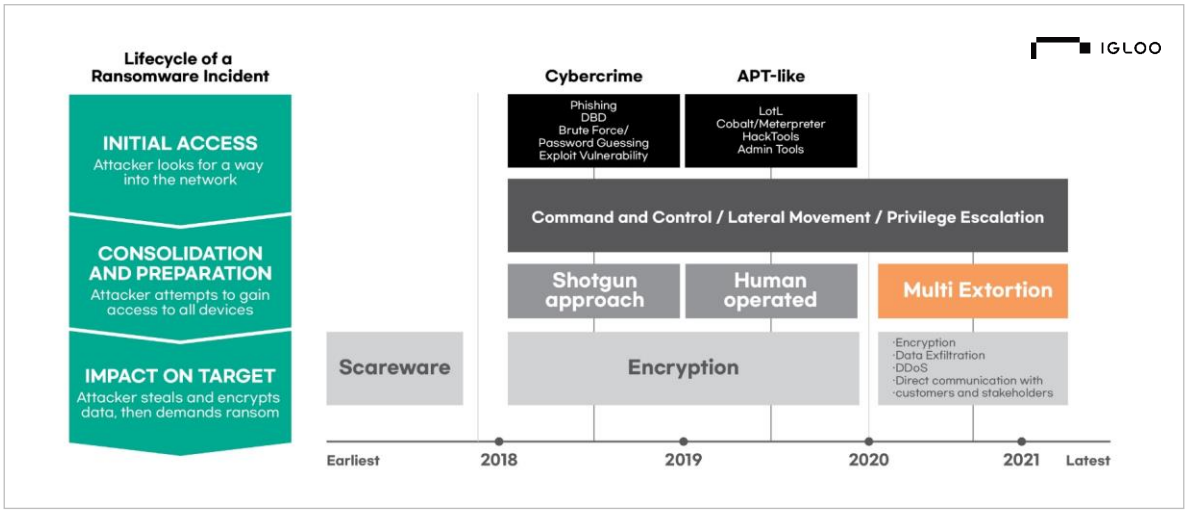
2023年サイバーセキュリティ脅威及び対応技術の展望

攻撃ツールの二極化は、攻撃手法の発展にも影響を与えている。攻撃グループは、APT攻撃に似せるために、自作ツールと共にオープンソースや有料レッドチームツールを混用することがある。
最近では、初期アクセス段階(Initial Access)から内部ネットワークにアクセスするために、FRP(Fast Reverse Proxy)、LCX(aka Htran)、SBD(Shadowinteger's Backdoor)などのツールを使用するケースが増えている。また、クレデンシャルの奪取、Lateral Movement、Privilege Escalationなどのために、Mimikatz、Cobalt Strike、BlueHound、HackTools、Admin Tools、AdFind、Meterpreterなどを使用するケースが目立っている。特に、Cobalt Strikeによる被害が増加しているため、2022年11月には「Making Cobalt Strike harder for threat actors to abuse」という投稿で、Cobalt Strikeクラックまたはマルウェアバージョンを含む34個のYARAルールが配布された。

ランサムウェア攻撃グループは、単純なデータ暗号化だけではなく、データ漏洩・奪取(Infostealer)・データ暗号化・DDoS・データ漏洩脅迫など、多重脅迫(Multi Extortion)形に発展していることがある。また、ランサムウェアの攻撃は、ファイル暗号化だけに限られているわけではない。Windowsから提供するディスク暗号化機能であるBitLockerを使用して、ディスクを暗号化し、パスワードを提供する条件で犯罪被害を誘導したこともある。

ランサムウェア攻撃は、特定の国を攻撃することもあり、GwisnやMasscanなどの攻撃ツールを使用することがあるため、単にお金のためだけでなく、国家基盤のサイバー攻撃ツールとしても利用されていることがわかっている。また、ランサムウェア単独で攻撃することがあるほか、従来の攻撃方法では識別できないような攻撃方法や、ランサムウェア起動トリガーファイルがない場合や、特定の条件に合わせてのみ実行されるなど、対応に混乱を引き起こすことがある。

ランサムウェアは、ファイルの暗号化による直接的な被害を引き起こすだけでなく、個人情報の盗難などの二次的被害が発生するため、持続的なモニタリングと現実的な対応戦略の計画が重要だ。ランサムウェアによる経済的被害を防ぐためには、攻撃に対する国家レベルの情報共有や、情報保護措置をサポートする上で、仮想通貨の不正使用に対する規制強化を行い、モニタリングおよびランサムウェア対応のための国際的な協力体制を維持する活動が必要である。



【▲ ランサムウェア攻撃 様相パラダイム (参考：イグルーコーポレーション)】

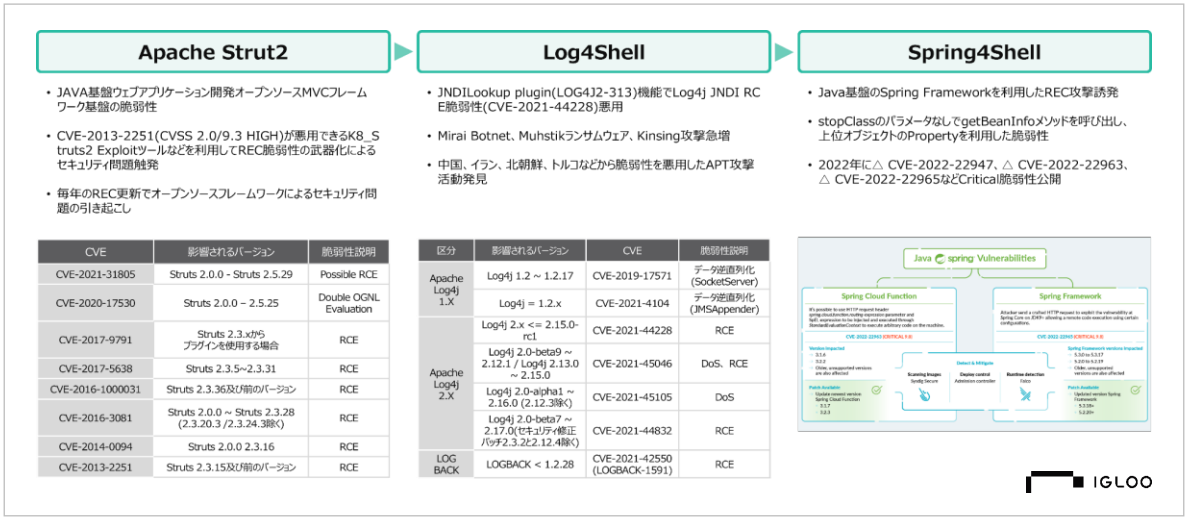
2023年サイバーセキュリティ脅威及び対応技術の展望

(2) オープンソース生態系によるセキュリティ脅威の進化

オープンソースはオープンイノベーションによってソフトウェアの成長を主導し、DXやビッグテック企業が主導するシード技術拡散を基盤として、オープンソース生態系の自立を確保し、市場で優位に立っている。ソフトウェア産業のゲームチェンジャーとして、従来は開発コミュニティーが中心に運用されていた方法は、財団やビッグテック企業が主導し、組織化された運用環境が作られ、ICT事業内のオープンソースの成長を促すようになった。特に人工知能、機械学習、ブロックチェーン、メタバースなど、次世代の新技術は後発のソフトウェア開発の環境でシード技術として活用され、オープンソース生態系の高速成長を促す新たな手法として活用されている。

従来のオープンソース活用による問題の大半はライセンスの問題であったが、Log4Shell、Spring4Shell、Text4Shellなどの権限奪取型リモートコード実行脆弱性の発覚により、オープンソースのセキュリティ脅威に関して脆弱性チェイニング(Vulnerability Chaining)の危険性が認知された。このような脆弱性に対する自浄作用を促進するために、オープンソース生態系から様々な論議や技術が研究されている。

オープンソース生態系の発展は、ソフトウェア産業の新しい成長動力の確保や、技術の一般化に肯定的な影響を与える一方で、Public RepositoryやPrivate Repositoryによるセキュリティインシデントが増加した結果、連続的なサイバーセキュリティ問題に直面することになった。NPM Registryのセキュリティインシデントの事例により、オープンソースレポジトリを利用したサイバー攻撃の拡散方法と危険性を推測できる。



【▲ Framework基盤の高危険度REC脆弱性の変化 (参考：イグルーコーポレーション)】

2023年サイバーセキュリティ脅威及び対応技術の展望

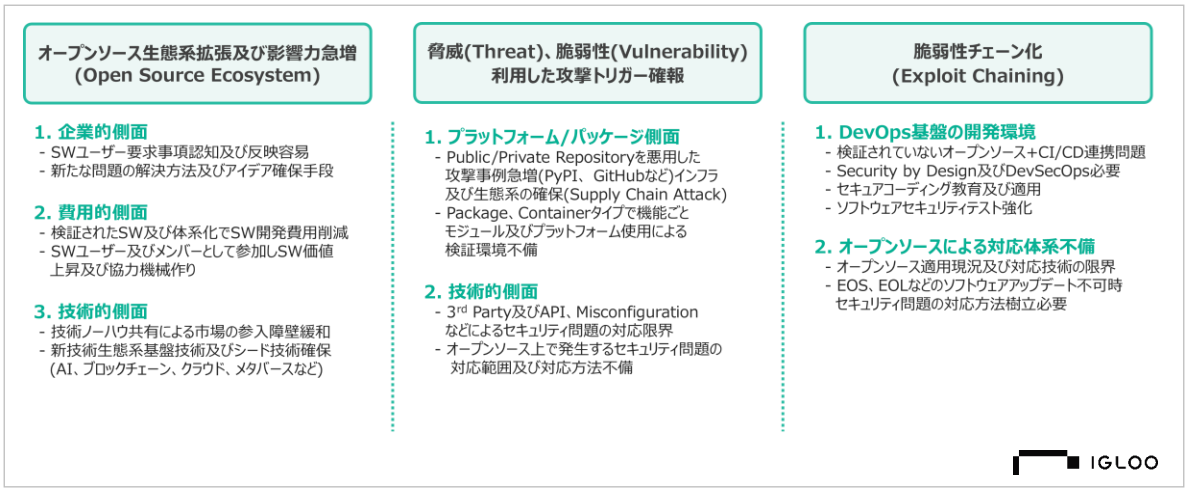
2017年には、cross-envパッケージと類似しているcrossenvパッケージを使用して、マルウェアを配布するTyposquatting攻撃があった。また、2018年には、Streamを簡単に使用できるようにサポートするEvent-Streamパッケージと依存するFlatmap-Streamパッケージに、ビットコインの決済プラットフォーム（Copayウォレット）とのプライベートキーを不正に奪取する不正コードインジェクション事件が発生した。さらに、2022年には、GitHub.com統合業者であるHerokuとTravis CIから発行されたOAuthユーザートークンを不正に奪取して、複数のPrivate NPMレポジトリをダウンロードし、損傷したAWSアクセスキーを使用してアクセス権限を上昇する攻撃などが多発している。

時期	攻撃方法	攻撃タイプ
2017	• cross-envパッケージと類似なcrossenvパッケージ名を使用するTyposquattingを利用して被害システムの環境変数収集不正コード配布	Typosquatting
2018	• Event-Streamパッケージ(Steamを簡単に使用できるようにサポートするパッケージ)と依存関係であるFlatmap-Streamパッケージにビットコイン決済プラットフォーム財布であるCopay財布情報とプライベートキーの奪取ができる不正コード挿入	Dependency Confusion
2021	• UA-Parser-JS NPMライブラリ(ブラウザのUser-Agent情報のパーシング機能を提供するライブラリ)ハイジャックからマイナー(Coinminer、仮想通貨採掘マルウェア)とパスワードスティーラー(Password Stealer、アカウント奪取マルウェア)挿入攻撃	Dependency Confusion
2022	• GitHub.com統合業者であるHeroku及びTravis CIから発行されてから盗まれたOAuthユーザートークンが攻撃キャンペーンに活用 • 攻撃者は盗んだOAうｔｈトークンを使用して複数のPrivate NPMレポジトリをダウンロードした後、獲得した損傷されたAWSアクセスキーを使用してアクセス権限を上昇 • ▲2015年ユーザー情報アーカイブにユーザー名、パスワードハッシュ、メールアドレスなどが含まれている約10万個のアカウントログイン情報、▲2021年4月7日から全てのプライベートパッケージマニフェスト、メタデータ、▲2022年4月10から全てのプライベートパッケージの掲載されたバージョン名とsemVer、▲二社のプライベートパッケージなどが被害	Privilege Leakage

【▲ NPM Registryを利用したオープンソースレポジトリ攻撃 (参考：イグルーコーポレーション)】

2023年サイバーセキュリティ脅威及び対応技術の展望

オープンソースやオープンソースリポジトリのセキュリティ問題は、脆弱性チェーンによる連鎖的なセキュリティインシデントを引き起こす可能性があるため、オープンソースのガバナンスを確立し、オープンソースセキュリティの脆弱性管理を行う方策が必要である。



【▲ オープンソース生態系とセキュリティの相関関係 (参考：イグルーコーポレーション)】

2023年サイバーセキュリティ脅威及び対応技術の展望

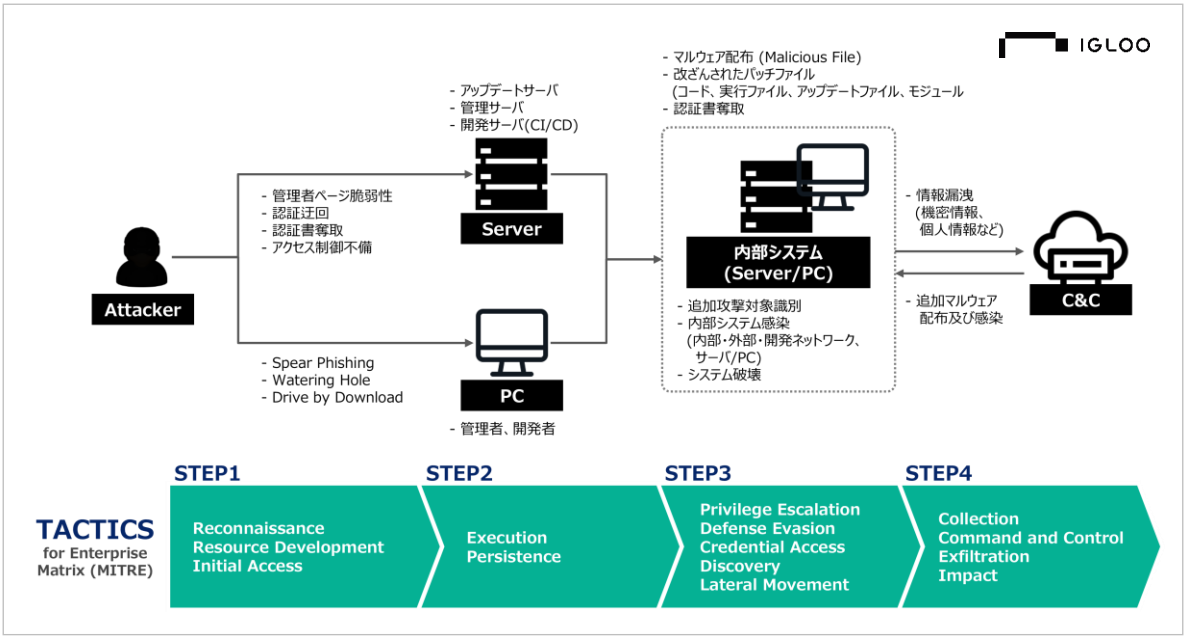
(3) 危険のチェーン化、サプライチェーン攻撃の増加傾向

Microsoft Exchange Serverの脆弱性、SolarWindsハッキング、Kaseyaなどの事例は、サプライチェーンセキュリティの影響範囲を示した。従来のサプライチェーン攻撃は物理的な供給体系に対する攻撃であったため、攻撃者は煩雑なプロセスを必要とした。しかし、デジタル化された供給環境によって、ソフトウェアに対するセキュリティ脅威の比率が高まったため、攻撃の規模や影響が拡大してる。2021年後半から始まったSpring Frameworkの脆弱性は、ソフトウェアの脆弱性によるサプライチェーン全体に影響を与える可能性がある事例である。

アメリカはサプライチェーンのセキュリティ脅威に対処するため、政策的な支援を行っている。コロニアル・パイプラインやJBS Foodsのサイバー攻撃を受けたことを受けて、バイデン政権は行政命令(EO)14028号を発令した。この命令に基づき、ソフトウェアサプライチェーンのセキュリティを強化する指針やガイドが発表され、デジタルインフラの信頼性構築と国家安全の保障が続けられてる。

NIST SP 800-161 Rev. 1（Systems and Organizationsのサイバーセキュリティサプライチェーンリスク管理プラクティス）とSSDF（Secure Software Development Framework）は、ソフトウェア基盤のサプライチェーンセキュリティを強化するための代表的な指針である。
NIST CSFやSP 800-53 Revision 5などは、既存のサイバーセキュリティ体系を基に、不正アクセス制限、ソフトウェア・ビルドマテリアル（SBOM）、ソフトウェアテストの強化などで、ソフトウェア基盤のサプライチェーンから発生する潜在的なセキュリティ脅威を識別し、対応している。
結果的に、ソフトウェアコードの安全性を保証し、脆弱性に対処することで、ソフトウェアの信頼性とセキュリティ性を確保することが必要である。

2023年サイバーセキュリティ脅威及び対応技術の展望



【▲ ソフトウェア基盤のサプライチェーン攻撃シナリオ (参考：イグルーコーポレーション)】

サプライチェーン攻撃は、異なる機器やシステムを組み合わせた攻撃プロセスである。したがって、ソフトウェアサプライチェーン攻撃に対応するためには、サードパーティのライブラリやオープンソースなど、ソフトウェアの可視性を妨げる要素のセキュリティを確保することが必要である。このようなソフトウェアのセキュリティを確保する対策として、SBOMが注目されている。

SBOMは、ソフトウェアの各構成要素のライセンス種類、バージョン情報、パッチ情報など、構成要素間の依存関係を提供することで、ソフトウェア基盤のサプライチェーンセキュリティを確保することができる。SBOMは、単純なセキュリティ要素を超えて、データプライバシーの側面においても重要であるため、注意深く導入する必要がある。

2023年サイバーセキュリティ脅威及び対応技術の展望

時期	攻撃対象	攻撃方法	攻撃タイプ	攻撃ツール
2011	Kernel.org	盗まれたユーザー資格証明を介してアクセス権限獲得し、不正スクリプトを追加	Open Source Project Repository	Source Code compromise
2016	Transmission BitTorrent	MacOS「Transmission BitTorrent」になりすまし、有効な証明書を使用するApple「Gatekeeper」迂回	Single Vendor (Install Program)	KeRanger
2017	NetSarang	Netsarangビルドサーバーに侵入して改ざんされた配布パッケージをユーザーに配信	Single Vendor (Build Server)	Backdoor (ShadowPad)
	Node.js NPM Registry	ハックタスクというアカウントで既存のNPMパッケージ名と類似の不正パッケージ39個を配布	Open Source Repository	Malware (cross-env)
2018	Arch User Repository (AUR)	PDFビュアのAcrobat Readerに不正スクリプトを挿入してシステム情報収集	Open Source Repository	Backdoor
	Ubuntu Snap Store	Ubuntu Snapパッケージソースコードに「systemd」を偽装したコインマイナー挿入	Open Source Repository	Coinminer
2019	PyPI Python Package Repository	dateutilとjellyfishパッケージを成りすました不正Pythonライブラ2種アップロード	Open Source Repository	Backdoor
2020	SolarWinds	ハッカー集団 UNC2452がSolarWinds Orionに挿入されたプログラムソフトウェアアップデート時に配布 （米政府機関含め約18,000機関に被害）	Single Vendor (Monitoring)	SUNSPOT、SUNBURST、TEARDROP
2021	MS Exchange	Microsoft Exchange脆弱性4種を悪用して115ヵ国の約5,000以上のMicrosoft Exchangeサーバーにウェブシェル配布	Single Vendor (Mail Server)	Vulnerability WebShell
	CodeCov	ソフトウェアテスト用のテストコード提供プラットフォームの継続的インテグレーション/継続的デリバリーのパイプラインを操作して不正ソフトウェアを配布	Single Vendor(CI/CD)	Backdoor
	Colonial Pipeline	ダークサイドによるランサムウェア感染で米東南部地域のガソリン供給が一時停止及び500万ドル（約5.7億円相当）の身代金支払い	ICS/SCADA	Ransomware
	Kaseya	Kaseya IT管理用プラットフォームのソフトウェア脆弱性でハッカー集団 REvilからランサムウェア配布	Single Vendor	Ransomware

【▲ サプライチェーン攻撃事例：2011~2021年
(ReversingLabs, How Existing Cybersecurity Frameworks Can Curb Supply Chain Attacks, Agu. 23, 2019. ,Figure 1: Timeline of Historical Supply Chain Attacks、一部再構成)】

2023年サイバーセキュリティ脅威及び対応技術の展望

(4) 仮想通貨の不確実性の増加、仮想通貨をターゲットにしたサイバー攻撃の拡散

近年、異なるブロックチェーンネットワークを相互に接続し、資産の交換やNFTなどのやり取りを可能にするブロックチェーンブリッジ(またはクロスチェーン)攻撃が急増している。ブロックチェーンブリッジは、単独でブロックチェーンの閉鎖性問題を解決できるため、相互運用性をサポートし、ブロックチェーンの生態系の活性化に役立つことができるが、そのために攻撃者から狙われている。

海外のブロックチェーンブリッジプラットフォームであるQubit Finance、Wormhole Bridge、Harmony Horizon Bridgeなどで、ハッキング事故が発生し、莫大な金額の被害が発生している。

オンチェーンとオフチェーンで実現されるブロックチェーンブリッジは、チェーン類型が違っても、Smart Contractやサービスプラットフォームがオープンソースプロジェクトを志向するため、ソースコードが公開されている場合が多く、脆弱性を悪用されることや、Smart Contractの複雑性を利用した攻撃が主に発生する。そのため、ブロックチェーンブリッジの構造的な複雑性による攻撃が発生すると、莫大な金銭被害に遭いやすい。

ブロックチェーンブリッジで奪取された仮想通貨は、国家支援を受けるハッカー集団の場合、マネーロンダリングによる不法資金の流れを作ることがある。ランサムウェアと連携して、仮想通貨による受益が増え続けるため、仮想通貨をターゲットにしたハッキンググループの攻撃は続くだろう。また、仮想通貨の場合、他のサイバー犯罪とは違って、窃取された仮想通貨はミキサーを使うことで追跡が困難であるため、マネーロンダリングがしやすくなる。そのため、攻撃者は要求条件に合わせて、仮想通貨をターゲットにしたサイバー攻撃を行うことが多い。国際的な協力や情報共有が必要であるため、この問題に対しては取り組みが必要である。

2023年サイバーセキュリティ脅威及び対応技術の展望

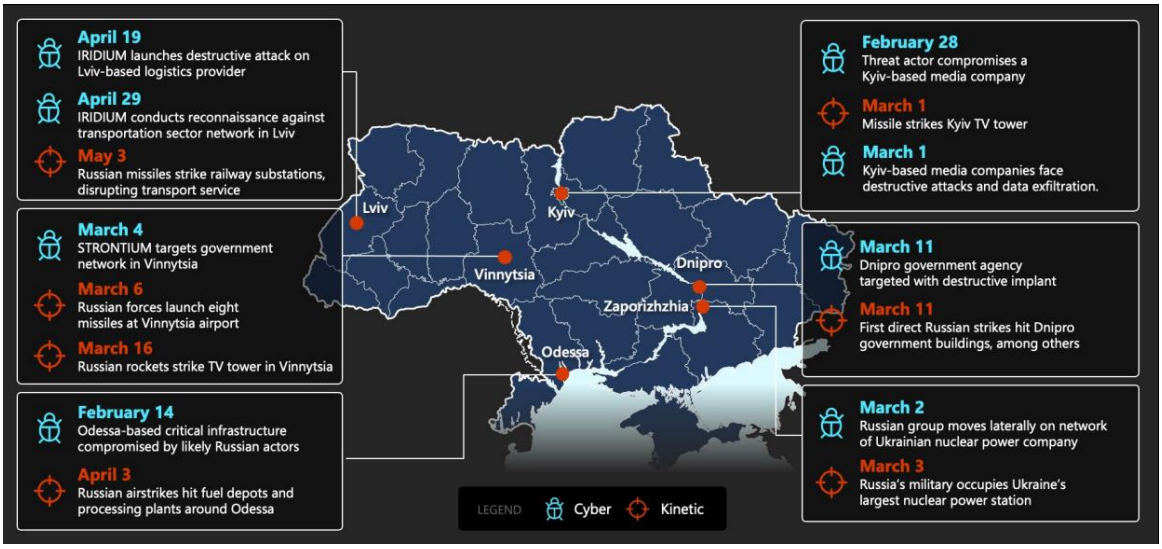
時期	攻撃対象	攻撃内容
2022.02	ブロックチェーン ブリッジサービス 「Wormhole」	- Solana Labsのクロスチェーンブリッジサービスであるwormholeで、3億2,500万ドル相当のイーサリアム（ETH） 120,000 が盗難された。 - Wormholeのプロトコルから保証なしにWeEth（Wormholeが発行するイーサリアム）Mintingし、Solaraブロックチェーンに転送した事件。 - プロトコルの保証を検証するシステムであるGuardianを通って、WeEth取引が可能なSolanaプロトコルが支払不可状態に陥ることもある。
2022.03	仮想通貨プラットフォーム 「Ronin Network」	- P2P ゲーム「アクシーインフィニティ」を起動するブロックチェーンネットワークで、1秒当たり処理可能なトランザクション （TPS）を最大化するために9つの検証者の権限を証明するイーサリウムサイドチェーンでもある。 - イーサリウム 73,600個、ステーブルコイン（USDC） 2,550万個などが盗まれ、これは6億1,600万ドル（約740億円）に相当する。 - 9個の検証ノードの内、「アクシーインフィニティ」と「Ronin Network」の運用会社「Sky Mavis」のノード4個を含め5個のノードがハッキングされる。
2022.08	Solanaブロックチェーン ウォレット資金窃取	- Solanaチェーンに対応しているウォレットPhantom、Slopeなど、ホットウォレット（hot wallet）の脆弱性を突いてウォレット8,000個くらいの資金を窃取する。 - Solanaのネイティブトークンである SOL、スプラッシュ（SPL）、ステーブルコイン（USDC）などが窃取され、7,767個のウォレットから520万ドルの被害が発生した。
2022.11	仮想通貨 デリバティブ取引所「Deribit」 ハッキング	- ハッキングによってホットウォレットにて仮想通貨が盗難された。 - イーサリウム 6,947個（約1,080万ドル）、ビットコイン 691個（約1,410万ドル）、ステーブルコイン（USDC）約 340万ドルなど2,800万ドル規模の資金が窃取された。

【▲ 2022年仮想通貨ターゲット型サイバー攻撃発生現況 (参考：イグルーコーポレーション)】

2023年サイバーセキュリティ脅威及び対応技術の展望

(5) 世界情勢の不安、国家サイバー安保の脅威増加

2022年に始まったロシアのウクライナ侵攻は、物理的な戦闘とサイバー攻撃が組み合わされたハイブリッド戦争の最初の事例と見なされている。この戦争では、物理的な衝突の前後に、国の主要施設、公共機関、民間企業に対して多数のサイバー攻撃が試みられた。これらの攻撃は、システム破壊、心理戦の活用、情報収集など、多岐にわたり、社会の混乱を引き起こし、国家の信頼度を低下させた。1年前の侵攻の前に、イタリアからのサイバー攻撃により、政府の主要な基盤施設のネットワークが乗っ取られ、データ漏洩やシステム破壊などの問題が生じたことで、サイバー戦争が現実味を帯び、新たな覇権競争の舞台が開かれたことが証明された。



【▲ Coordinated Russian cyber and military operations in Ukraine
(参考：Microsoft, Defending Ukraine: Early Lessons from the Cyber War)】

Microsoftの「Microsoft Digital Defense Report」によると、サイバー攻撃の背後には、ロシア、北朝鮮、ベトナム、イラン、中国、トルコなどの国から、ハッキング攻撃をサポートする組織が存在し、多国間の関係が見られる傾向がある。ロシアのEnergetic Bear、UNC2452、APT28ハッキンググループ、北朝鮮のLazarus Group、Kimsukyハッキンググループ、中国のAPT40、UNC2630/UNC2717ハッキンググループ、イランのOilRig、Agriusハッキンググループなど、多数のグループが存在し、外交、安全保障、国防、エネルギー、医療など、多様な産業分野に対して攻撃を行っている。

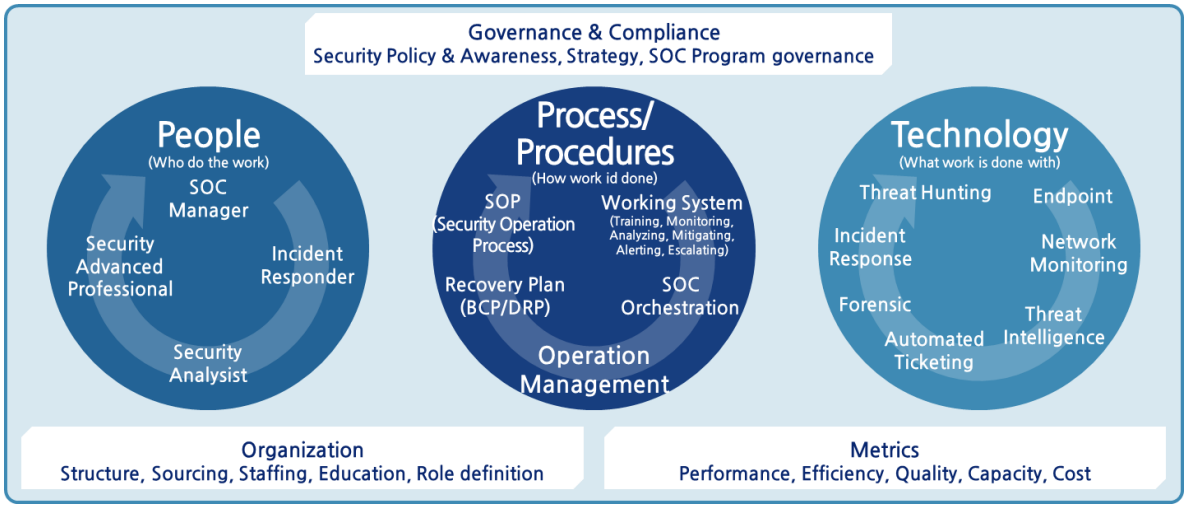
03. 2023年4大サイバー対応技術の展望

(1) 知能型サイバーセキュリティ監視と自動化技術の高度化

ハッキンググループの組織化、体系化、分業化の現象が目立つことにより、サイバー脅威に対応するための人工知能やマシンラーニングなどの次世代技術を適用したリアルタイム検知・対応が高度化されている。人工知能技術が一般化されることで、攻撃者の人工知能活用事例が続々と報告されている。ジョージメイソン大学のSean Palka教授によると、メールセキュリティシステム（SEG）を機械学習を利用して迂回パターンを作成したり、攻撃対象の選好度を調査する過程に人工知能を活用してソーシャルエンジニアリングの成功率を高めることに活用することができる。人工知能基盤のマルウェア（DeepLocker）も、人工知能を利用して攻撃条件が一致した場合、ランサムウェア攻撃を実施することができる。

これに対応するために、セキュリティ監視プロセスの全過程に、人工知能や自動化技術を活用した事例が増えている。セキュリティ脅威を識別・検知・対応する過程に、人工知能基盤のサイバー脅威予測技術を導入し、クラウド及び異機種ドメイン間のサイバー脅威分析のための知能型サイバーセキュリティ監視ソリューションが導入されている。異機種セキュリティソリューション間のセキュリティ監視効率性と複雑性を解消するために、「セキュリティオーケストレーション・自動化及び対応(SOAR, Security Orchestration, Automation and Response)」の適用も着実に増加している。

しかし、次世代技術や自動化プロセスを導入するだけでは、すべてのサイバー脅威に対処できるわけではない。対策としては、標準化されたセキュリティ監視プロセスの導入、サイバー攻撃のプロファイリング、および自動化のための体系の導入が必要である。そして、もし先制的なセキュリティ脅威が識別できる場合は、高度なセキュリティ監視体系を確立することができる。



【▲ Building a World-Class Security Operations Center : A Roadmap
(参考：SANS SANS Institute 2015、一部再構成)】

2023年サイバーセキュリティ脅威及び対応技術の展望

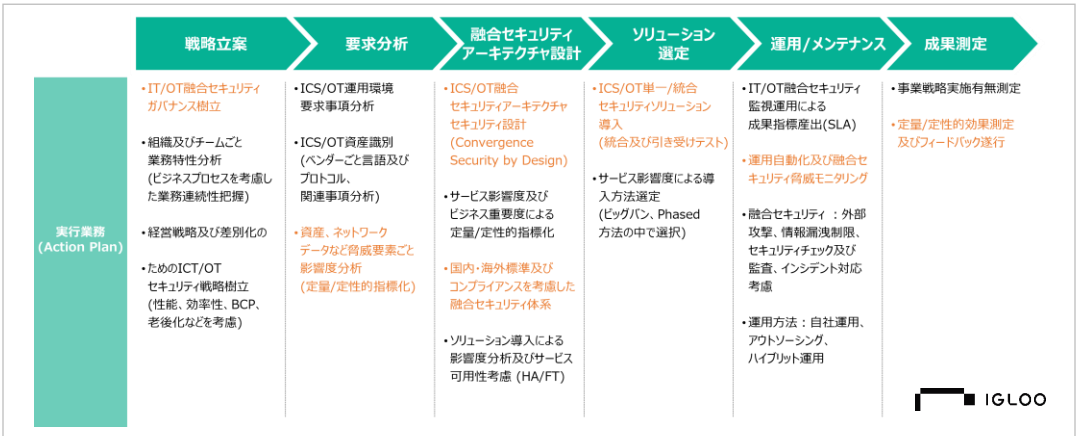
(2) Securityを超えてSafetyに、融合セキュリティの必要性強化

国家主導型サイバー攻撃により、多数の攻撃キャンペーンが同時に発生し、攻撃環境がICT環境に限らずICT/OTにまで拡大している。大規模なサイバー攻撃の頻度が増加することにより、ハードウェア、ファームウェア、ソフトウェアなどのサプライチェーンへの攻撃が活発化し、Active Directory、サードパーティ、VPNなどの信頼関係のある環境にまで攻撃が拡大している。特に、最近ではウクライナ・ロシアの紛争による社会基盤施設を対象としたサイバー攻撃が増加しており、ITとOTのセキュリティを管理する必要性が高まっている。

オープンソースの脆弱性、管理型商用ソフトウェアのセキュリティ問題、大手企業の連鎖的なサイバーインシデントなどによる、サプライチェーンセキュリティ脅威での脆弱性チェーン化が本格化されることで、「情報通信技術及びサービスに対する、脅威に対処するためのICTサプライチェーン保護に関する行政命令(Executive Order on Securing the Information and Communications Technology and Services Supply Chain)及びサイバーセキュリティ人材確保に関する行政命令(Executive Order on America's Cybersecurity Workforce)」の一つである「サプライチェーンセキュリティ強化のための行政命令(Executive Order on Improving the Nation's Cybersecurity)」が発令され、サプライチェーンセキュリティ強化のためのサイバーセキュリティインシデント脆弱性、及びインシデント対応のためのプレイブックの標準化、サイバーセキュリティの現代化、ソフトウェアサプライチェーンセキュリティ強化など、対処指針とガイドによる実現化を始めた。

融合セキュリティモニタリング体系（Converged Security by Design）を構築するためには、まず、SBOMなどを利用してソフトウェアサプライチェーンの完全性対策を行い、また、サイバーインシデントモニタリングなどのセキュリティ機能強化により、オープンソースや連鎖的なセキュリティインシデントを可視化することが必要である。

2023年サイバーセキュリティ脅威及び対応技術の展望



【▲ ICT/OTセキュリティソリューション導入及び融合セキュリティ監視運用 (参考：イグルーコーポレーション)】

(3) クラウド移行の始まり、クラウドセキュリティ考慮事項

パンデミックの影響により、クラウドへの移行が活発化し、その結果、クラウドセキュリティインシデントが増加している。2020年には、「2030年未来社会変化及びICT8大有望技術のサイバーセキュリティ脅威展望」によると、CSP側からは、コンテナーセキュリティ脅威、仮想化環境セキュリティ脅威、データ改ざん及び漏洩などのサイバー脅威が懸念され、ユーザー側からは、クレデンシャル漏洩及びアクセス制限のセキュリティ脅威によるデータ不正アクセスがセキュリティの問題であることが指摘されている。

CSAから発行された「Top Threats to Cloud Computing - Pandemic Eleven」によると、クラウドセキュリティに対する成熟度向上と、クラウド構成や認証の過程から、2つの結果が上げられている。1つ目は、セキュリティを適用したクラウドマイグレーションなどの効果により、不正アクセスによるデータ漏洩及びクラウドセキュリティアーキテクチャが懸念されるようになったことである。2つ目は、戦略不備などにより、セキュリティ脅威の代わりに、安全ではないソフトウェアの開発、システムの脆弱性、サーバーレス及びコンテナーワークロードの間違った構成が悪用されるようになったことである。この結果から、ハッキンググループによるAPT攻撃などのセキュリティ脅威に変化があることが分かり、ユーザーインターフェースやAPIを使用したクラウド攻撃が増加することが予測され、より詳細なクラウドセキュリティポリシーの策定が必要であることが示唆されている。

クラウド移行が金融や公共などICT環境の重要インフラとして位置づけられたため、クラウド管理のセキュリティ強化やリスク管理の重要性が高まっている。クラウドへの移行には、クラウド環境に適合する業務プロセスやデータ管理体系を導入し、クラウドネイティブ認証によるアクセス制限や制限プロセスを導入する必要がある。そのためには、Security by Designの考え方を取り入れ、クラウド移行の設計段階からセキュリティを考慮したクラウド管理戦略を策定する必要がある。

2023年サイバーセキュリティ脅威及び対応技術の展望

#：2021年CSA Top Threats to Cloud Computingセキュリティ脅威番号の意味

NO	セキュリティ脅威	詳細説明
1	不十分なアイデンティティ、クレデンシャルおよびアクセスと鍵の管理、ならびに特権アカウント (Insufficient Identity, Credential, Access and Key Mgt, Privileged Accounts) #4	• ID、クレデンシャル及びアクセス管理不備はデータの損傷及び悪意的な漏洩、サプライチェーンの崩壊などビジネス連続性の阻害
2	セキュアでないインターフェースやAPIS (Insecure Interfaces and APIs) #7	• セキュアでないAPI設計は認証されていないエンドポイントのアクセス、弱い認証手順、過度な権限付与、パッチされていないシステムの悪用、論理的な設計問題、ロギング無効化によるリソース流出、削除及び修正、サービス中断に繋がる可能性がある
3	設定ミスと不適切な変更管理 (Misconfiguration and Inadequate Change Control) #2	• 間違って構成されたデータ格納先及びコンテナー、過度な権限付与、基本資格証明及び構成設定を変更せずに維持、無制限アクセスポート及びサービス、設計ミス及び有効性検証不備などでデータ流出発生
4	クラウドセキュリティのアーキテクチャと戦略の欠如 (Lack of Cloud Security Architecture and Strategy) #3	• クラウド配布モデル、サービスモデル、サービス地域可用性領域などを考慮したクラウドセキュリティ設計が必要 • クラウド移行に対して既存ITスタックとセキュリティ制御機能をクラウド環境にそのまま移行する「lift-and shift」方法と共通責任モデルの低い理解度によるセキュリティ問題の引き起こし
5	セキュアでないソフトウェア開発 (Insecure Software Development)	• ソフトウェアの複雑度の増加によるセキュリティ問題が発生する可能性があるため、安全なキー管理及びCI/CDでアプリケーションの実現が必要
6	セキュアではない3rd Partyのリソース (Unsecure Third-Party Resources)	• オープンソースセキュリティ問題及びAPI問題などでサプライチェーンの危険が高まる可能性があるため、ソフトウェアセキュリティぜいゃく性診断及び資産識別、リソースチェック、SAST/DASTなどを適用
7	システム脆弱性 (System Vulnerabilities) #8	• クラウドサービスプラットフォームの欠陥によるデータの機密性、完全性、可用性を損傷して潜在的なサービス運用に問題になる可能性がある • ゼロデイ脆弱性、セキュリティパッチの漏れ、アーキテクチャの脆弱性、脆弱な資格証明などによる問題発生可能性がある
8	予想外のクラウドデータ公開 (Accidental Cloud Data Disclosure)	• 急速なクラウド移行及び拡張によるセキュリティガバナンスの不備でクラウドインベントリ及びネットワーク漏洩に対するセキュリティ透明性の不備で意図していないデータ漏洩が発生する可能性がある
9	サーバレスやコンテナワークロードの構成ミスやエクスプロイト (Misconfiguration and Exploitation of Serverless and Container Workloads)	• サーバーレス責任モデルはインフラに対する制御不足及びアプリケーションセキュリティ問題に対する緩和方法などを考慮 • サーバーレス及びコンテイナー化されたワークロードで敏捷性と費用削減が図られ、運用単純化とセキュリティ強化が可能
10	組織的な犯罪、ハッカーとAPT (Organized Crime, Hackers & APT) #11	• 国家及び犯罪組織などAPT攻撃グループに対する攻撃でセキュリティ脅威が発生する可能性がある
11	クラウドストレージデータ流出 (Cloud Storage Data Exfiltration)	• 敏感情報、機密情報などアーキテクチャの設計ミス、アプリケーションの脆弱性などで発生する可能性があり、漏洩されたデータによる2次被害が発生する可能性がある

【▲ Top Threats to Cloud Computing Pandemic Eleven (参考：CSA, 06/06/2022)】

2023年サイバーセキュリティ脅威及び対応技術の展望

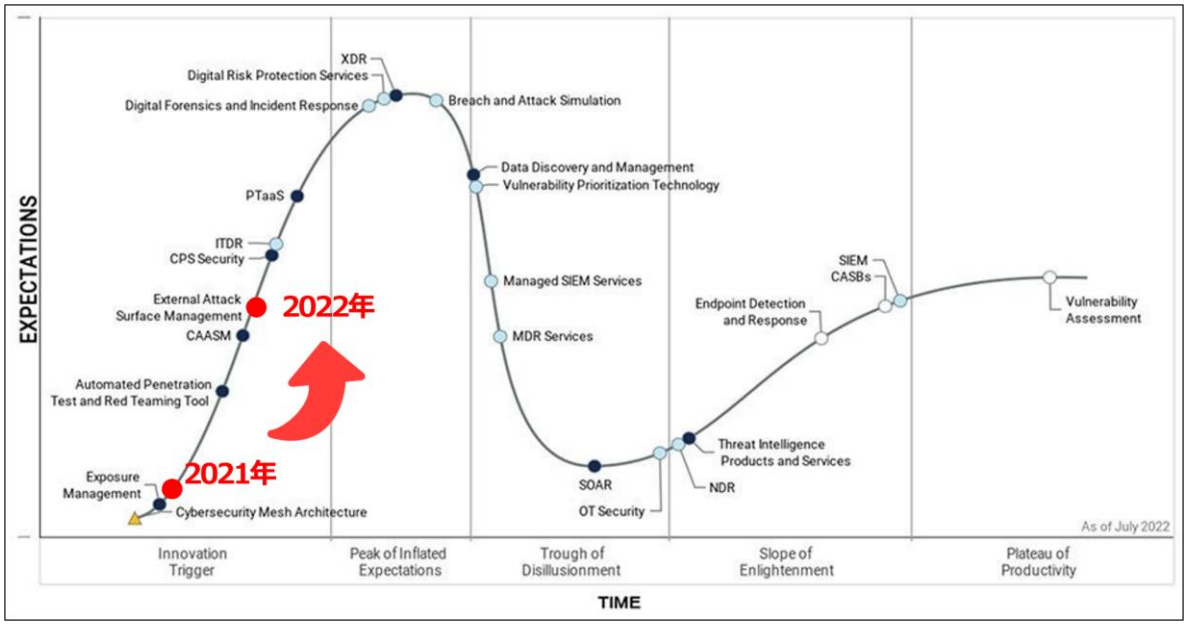
(4) サイバー攻撃の阻止線、攻撃表面管理

Gartnerの2021年版セキュリティオペレーションのハイプサイクルにおいて、Attack Surface Managementは、外部攻撃表面管理（EASM, External Attack Surface Management）から始まり、インフラの複雑性による有機的なサイバーセキュリティ（Cybersecurity Mesh）を実現するための方法として発展している。

資産の複雑性と分散は、インフラ構造の可視性を妨げ、ネットワーク境界の弱体化を引き起こしている。また、勤務の柔軟化や、企業内資産現況の不備などが識別されていない資産やネットワークに影響を与え、新たな攻撃地点として悪用されている。さらに、過去に漏洩したデータやクレデンシャル情報も、新たな攻撃ベクターとして悪用されることがある。

この結果、ダークウェブで情報が販売され、再利用されることにより、大規模なサイバー攻撃の資源が提供されるようになった。クラウド移行に伴い、資金がCloud Firstに集中する中、責任共有モデルに対する理解不足や、クラウドアーキテクチャの不備によるデータやクレデンシャルの漏洩など、多くの問題が発生し、新たな攻撃ベクターとして悪用されることがある。

企業のインフラにアクセス可能な場合や、公開されていないすべてのセキュリティ脅威要素に対して先制的に脅威要因を発見するためには、攻撃表面管理を実施し、内部インフラに対する最小限の権限設定やアクセス制限、セキュリティ設定の承認など、攻撃表面管理に関する対策を適用する必要がある。このような対策によって、攻撃表面管理活動を監視し、持続的な対応体制を強化することが必要である。



【▲ Gartner's Hype Cycle for Security Operations, 2022 (参考：Gartner)】

2023年サイバーセキュリティ脅威及び対応技術の展望

区分	問題事項	対応方法
インフラ側面	• On-premiseからCloud(Multi, Hybrid, Public, Private)にインフラ柔軟性及び拡張性強化 • IoT, IIoTなど連携(Connection)強化で攻撃表面(Attack Point)拡大	• ゼロトラスト(Zero Trust)観点からセキュリティアーキテクチャ設計及び実現(Network Micro-Segmentation, SDP, IAP) • 低電力デバイスセキュリティ強化方法樹立
データ側面	• 定型データ以外に判定形、非定型データでデータ活用拡大による性能及びセキュリティ問題 • データライフサイクルによる収集、保存、分析視覚化などの技術安全性 (△提携：ETL, FTP, OpenAPI、△判定形：Crawling, RSS, OpenAPI、△非定型：Crawling, Streaming) • データ(個人情報、仮名情報、匿名情報)活用によるデータ間セキュリティ及び再識別問題発生	• 無分別なデータスプロール(sprawl)対応のためのデータアクセス対象の業務別権限付与時認証(Authentication)認可(Authorization)強化 • データ暗号化・復号化適用 • プライバシー保存技術(PETs)でテータセキュリティ強化
ソフトウェア側面	• IT技術活用拡大による3rd Partyソフトウェアのセキュリティリスク増加 • 開発インフラ構成及びソフトウェア、中央管理型ソフトウェアなどサプライチェーン攻撃(Supply Chain Attack)を利用したセキュリティ脅威	• DevSecOpsを利用した開発及び運用、自動化されたセキュリティライフサイクル樹立 • セキュアコーディング(Secure Coding)、ソフトウェアテストの高度化
ユーザー側面	• DXなどによる技術依存度増加及び攻撃表面危険指標上昇 • 在宅勤務、分散勤務地、デジタルワークプレースなどによる業務サポートソリューション(ビデオ会議ソリューション、RDP、VPNなど)セキュリティ脆弱性及び情報漏洩問題	• セキュリティ認識を高めて基本セキュリティルールを守るための恵みと制裁の導入 • ペネトレーションテスト及び脆弱性診断でセキュリティ問題発見及び解消

【▲ 攻撃表面管理問題事項及び対応方法 (参考：イグルーコーポレーション)】

04. 最後に

今回は2023年に発生するであろうセキュリティ脅威と対応技術について調査した。パンデミックを超えてエンデミック時代を迎えている今、国や企業のデジタル化はサイバー脅威を伴うようになっている。クラウドやIoTなど、インフラの複雑度が増加することにより、攻撃表面が増え、攻撃の認知が難しくなっている。特にAPIを利用した連携やソフトウェア基盤の仮想環境が増加することにより、断片化されたセキュリティ戦略は、組織のレジリエンスを阻害することになる。

敏捷に変化するビジネス環境の中で、セキュリティを適用するためには、親和性が高いセキュリティ体系の構築が必要である。ビジネス戦略を策定する際、段階ごとにセキュリティ脅威による業務連続性が阻害されていないかを確認し、ビジネス体系が実現された後も持続的な脅威管理を実施し、受容可能なレベルであるかをBIA（Business Impact Analysis）分析によって検証する必要がある。

現在のインフラ環境は複雑で有機的な連携構造を持っている。断片化されたセキュリティ体系は、セキュリティの可視性や運用の効率性を阻害することがある。異なる種類のセキュリティソリューションを統合し分析する中で、最も重要なのは、現在の組織業務プロセスを理解し、ROIを最大化できる組織のセキュリティポリシーを確立することである。