Analysis Report

SECURITY REPORT

2024

FEB

2024年サイバーセキュリティ脅威及び技術展望 ～後編～

CyberFortress

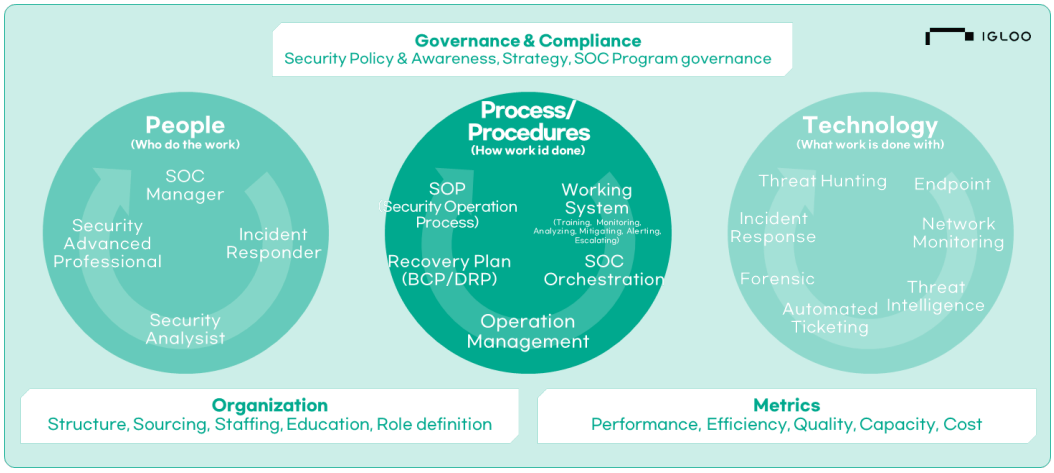
このレポートは、株式会社サイバーフォートレスの独自の調査にて収集されたデータに基づき作成しています。

02. 2024年5大セキュリティ技術展望

1) インテリジェンス基盤のSOC自動化

高度化・知能化されたサイバー攻撃に対応するためには、オンプレミス、クラウド、ネットワーク、アプリケーション、エンドポイントなど、多様な異機種環境全般で発生するログやインベントを人工知能、ビックデータなどの次世代技術を利用して、サイバー攻撃の識別・予防・検知・対応・復旧・管理を実施するために、セキュリティ監視センター(SOC、Security Operation Center)が必要である。

セキュリティ監視を構成するためには、「図 セキュリティ技術 1-1」のように人(People)、手順(Process/Procedures)、技術(Technology) が必要である。すべての要素が均等に成熟度が上がることが一番理想的だが、現実はできない場合が多いため、組織のビジネス目的に基づき、現在のセキュリティ監視の成熟度を考慮して、優先順位の高い順にセキュリティ監視を強化する戦略が必要である。

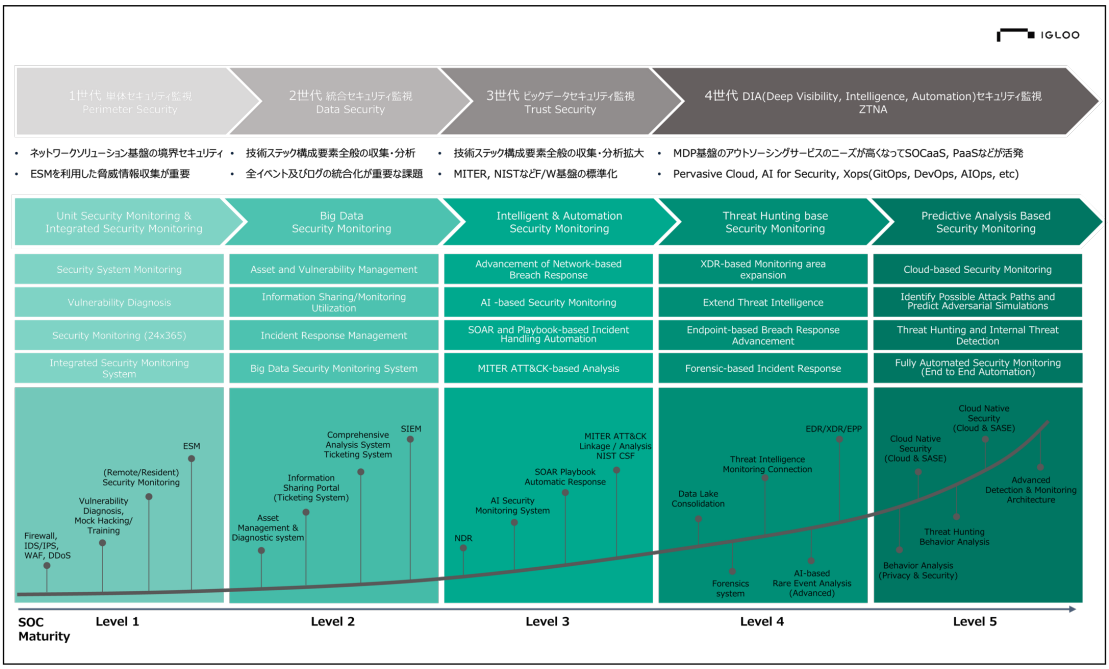


【▲「図 セキュリティ技術 1-1」SOCを構成する基本要素 (参考：Building a World-Class Security Operations Center：A Roadmap(SANS SANS Institute 2015、一部再構成)】

サイバー攻撃も生成型AIやオープンソースを利用した攻撃に多様化されることで、知能型サイバーセキュリティ脅威を分析し、インフラ内に存在するセキュリティ脆弱性や管理などを実施できる自動化・知能化されたセキュリティ監視技術を用いて、セキュリティの可視性を確保し、レジリエンスを高めることが重要である。

2016年セキュリティ専門企業Zerofox社が人工知能を活用して、悪性リンクのアクセスを誘導するスピアフィッシングロボットSNAP_Rを開発してから世界最大ハッキング大会であるDEFCONのサイバーグランドチャレンジ(CGC)では人工知能ハッキング攻撃・防御コンピューターMayhemが優勝した。
この後、2018年IBMは人工知能マルウェアであるDeepLockerを利用した攻撃対象を識別してからランサムウェア攻撃を実施、サイバー攻撃の正確性を向上させ、サイバーアーキテクチャをバイパスするためのセキュリティ体系の無力化する目的で人工知能を活用しようする事例が増加することで、既存のサイバーセキュリティ監視体系にも変化の必要性を引き起こした。

セキュリティ監視センターは、組織や企業でサイバーセキュリティのレベルを維持するために最も基本的な要素で、サイバーセキュリティ生態系のセキュリティマッシュ(Security Mesh)を構成できる重要な役割を行い、多様なセキュリティ技術とプラットフォームの集合体であるため、「図 セキュリティ技術 1-2」のようなセキュリティ監視センターの成熟度によって、徐々に発展する必要がある。セキュリティ監視の成熟度は、セキュリティ監視を構成する要素に影響を受けるため、セキュリティソリューションの構築だけがセキュリティ成熟度を向上させる絶対的な方法にはならない。



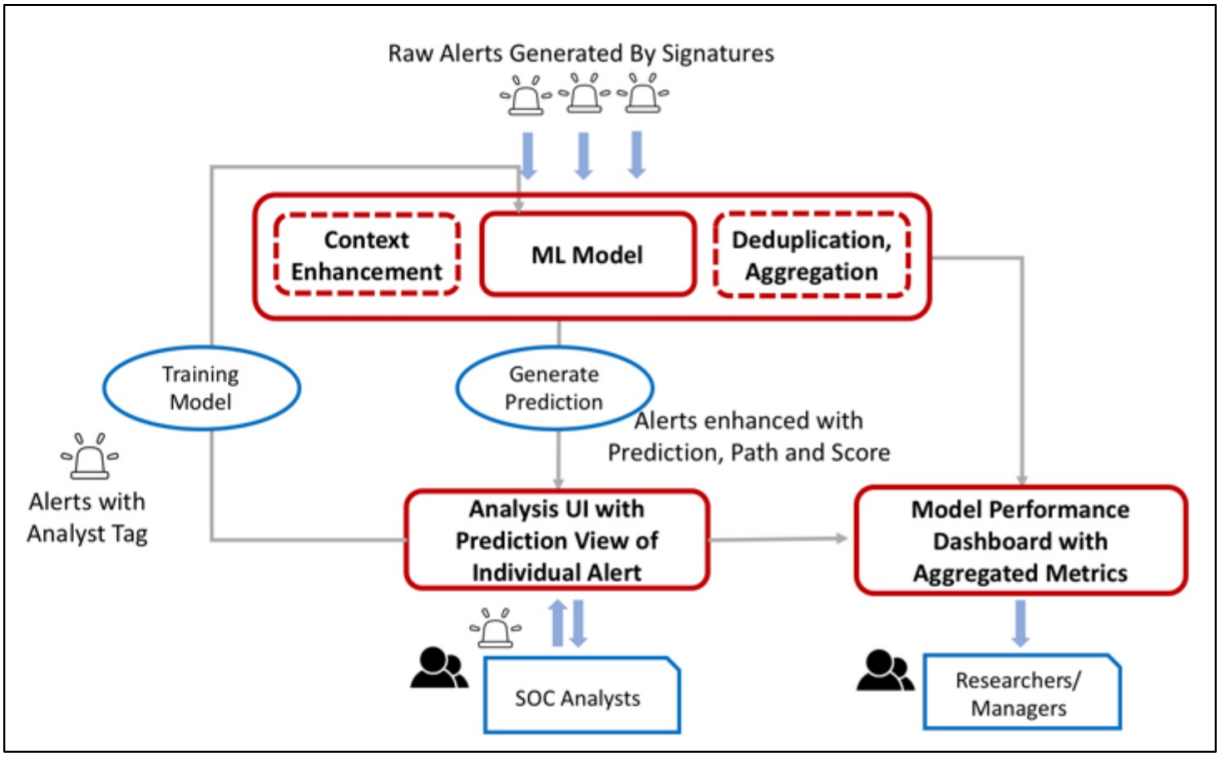
【「図 セキュリティ技術 1-2」サイバーセキュリティ監視センター(SOC)の成熟度モデル発展方向】

単体セキュリティ監視(Perimeter Security) が1世代、 統合セキュリティ監視(Data Security)が2世代、ビックデータセキュリティ監視(Trust Security)が3世代を超え、現在のセキュリティ監視は4世代とも言える。4世代セキュリティ監視は、人工知能セキュリティ監視や次世代セキュリティ監視などと命名される場合があるが、ノンレポートでは深層的な可視性(Deep Visibility)、知能化(Intelligence)、自動化(Automation)の単語から最初のアルファベットだけ取って、DIAで整理してみた。

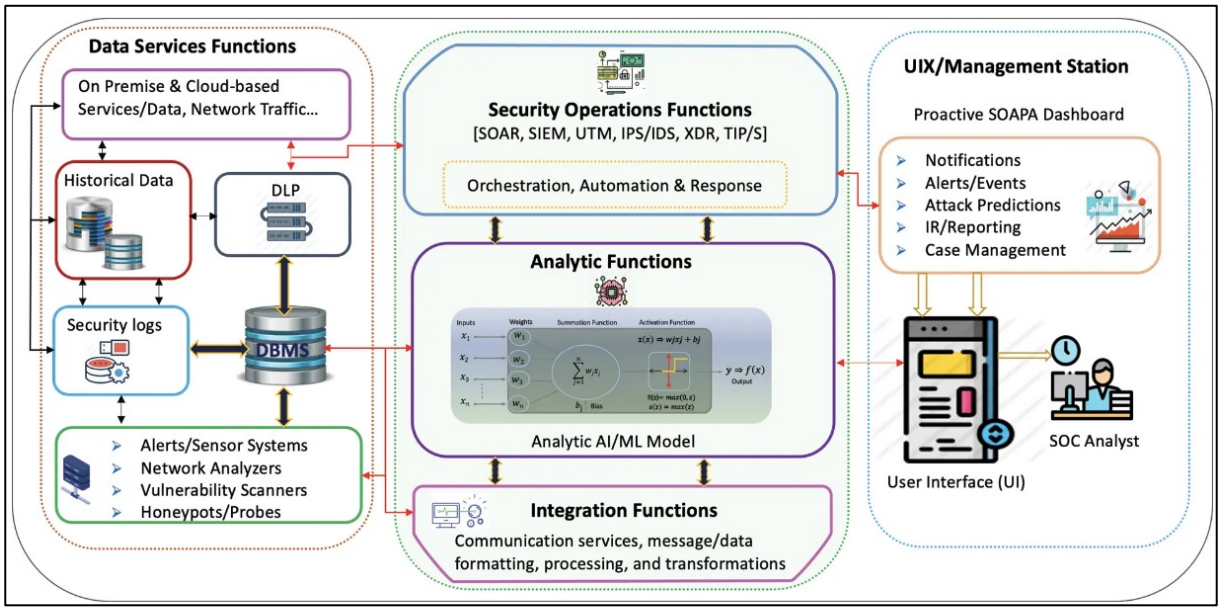
まず、深層的な可視性からみてみると、現在のセキュリティインフラの体系は、組織や企業の資産にもかかわらず、管理されていなかったり、管理対象として識別されていない資産を識別することによって、脅威の可視性を確保することを意味する。「2024年サイバー技術展望」で選ばれた「脅威可視化のための資産識別と危険管理技術、攻撃表面管理」と関連が深い項目とも言える。これで セキュリティ監視センターから管理する組織の資産に対して、識別とモニタリング方法でアプリケーション、ネットワーク、データベース、OSなどの技術ステックを構成している多様な要素のセキュリティ脅威の識別方法の樹立が必要である。

セキュリティ監視の可視性が確保できたら、次に必要なのは知能化(Intelligence)である。ハッキンググループも体系化された組織を基に、サイバー脅威に対応するため、人工知能ーやマシンラーニングなど次世代技術を利用した攻撃事例が報告されることで、セキュリティ監視も次世代技術を利用した対応戦略が必要である。人工知能技術を結合したセキュリティ監視センターを構成した「図 セキュリティ技術 1-3」と「図 セキュリティ技術 1-4」のような自動化されたセキュリティ監視においても、セキュリティ運用・脅威対応自動化(SOAR、Security Orchestration、Automation and Response)分野でも、知能化されたセキュリティ監視を構成するために、人工知能による研究を継続している。

もちろん、このように知能化されたセキュリティ監視を構築するためには、人工知能だけがすべての答えになるわけではい。脅威インテリジェンス(Threat Intelligence)、スレットハンティング(Threat Hunting)、インシデント事例分析による脅威モデリング(Threat Modeling)など、攻撃者の攻撃手順、攻撃方法などTTPsが導出できる要素を識別し、検知できる機能が実施できるのであればなんでも構わない。

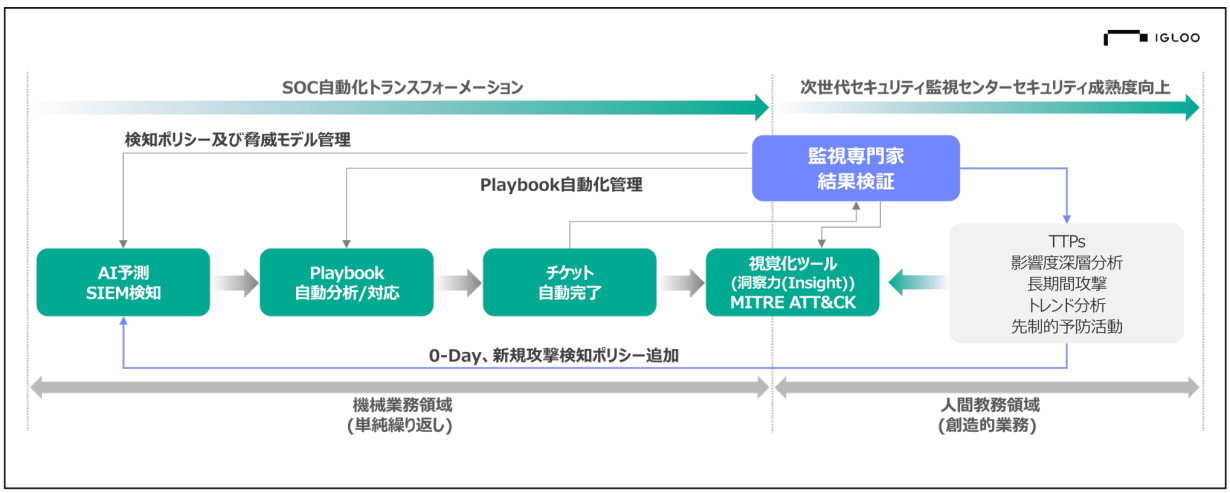


【「図 セキュリティ技術 1-3」人工知能を利用したSOC構成図（参考：Building a Machine Learning Model for the SOC、by the Input from the SOC、and Analyzing it for the SOC)」



【「図 セキュリティ技術 1-4」A High-Level Multi-Functional SOPA System(参考：AI/ML in Security Orchestration、Automation and Response: Future Research Directions)】

セキュリティ脅威を識別、検知、対応する過程で、人工知能基盤のサイバー予測技術を導入し、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以外にも監視の効率性と複雑性を解消するためのSOARの適用が必要である。「図 セキュリティ技術 1-5」のようにSOARを適用して、効率性を導出するために、組織の業務プロセスの標準化及びセキュリティ脅威のタイプ別のプレイブック(Playbook)で、セキュリティ監視の成熟度を向上させるための標準化で、サイバー攻撃のプロファイリングと自動化された体系を構築し、行動化されたセキュリティ監視の構成が必要である。



【「図 セキュリティ技術 1-5」SOARを利用したセキュリティ監視の効率化】

2) 生成型AIが引き起こしたAIセキュリティ

チャットGPT(ChatGPT)のブーム後、大型言語モデル(LLM、Large Language Model)を基にする生成型AIの活用事例と、これによる社会的な問題が発生した。人工知能(AI)モデルを開発する際に意図しない結果が導出され、敵対的攻撃(Adversarial Attack)による中毒攻撃(Poisoning Attack)、回避攻撃(Evasion Attack)、探索的攻撃(Exploratory Attack)など社会的な混乱や間違った意思決定による不利益、個人情報漏洩及び推論、誤作動、人種差別や性差別的な表現などの問題が現れた。

人工知能の悪影響が持続させることで、政府や企業では人工知能生態系内で安全で信頼できる人工知能のための自浄作用ができる人工知能ガバナンスとフレームワークを発表した。AI TRiSM(Trust、Risk、Security Management)は、AIモデルガバナンス、信頼性、公平性、効率性、個人情報保護、データ保護及び信頼性強化のための方法を提示し、セキュアAIフレームワーク(SAIF、Secure AI Framework)は、人工知能ソフトウェア開発サプライチェーン検討、テスト及び制御のようなセキュリティ模範事例を基にAIシステムと関連されたセキュリティメガトレンド及び意見に対するフレームワークを発表した。

その他にも、基礎モデルの生態系の透明性を評価し、今後透明性を向上するためのファンデーションモデルの透明性数値(FMTI、The Foundation Model Transparency Index)、AIやAI研究の公平性、責任、透明性、倫理の定義及び研究を目標にするFATE (Fairness、Accountability、Transparency、and Ethics in AI)がある。アメリカ国立標準技術研究所(NIST)が発表したAI RMF (Artificial Intelligence Risk Management Framework)は、AIシステムと関連する否定的な影響を最小化し、肯定的な影響極大化を目標とし、AI RMFを順守することで、技術に対する信頼度を高めることができると予想する。

MITREから発表した「人工知能セキュリティのための合理的な規制フレームワーク(A Sensible Regulatory Framework for AI Security)」は、広範囲なAIアルゴリズム技術を△AIを構成要素また破壊システムに使用するエンジニアリングシステム、△人の能力の向上のAI、△機関内で自律的に運用されるAIで脅威と危険を緩和する方法の3つのカテゴリに分けて提示している。セキュリティフレームワークは、AIの信頼性及び透明性向上を中心に、言語モデルを根幹とする人工知能生の体系が警戒心を引き起こしている。

フレームワーク	主要事項	主要内容
AI TRiSM	• AI Trust • AI Risk • SI Security Management	▪ 説明可能性 (Explainability)、モデル運用 (ModelOps)、データ異常検知(Data Anomaly Detection)、敵対的攻撃防御(Adversarial Attack Resistance)、データ保護(Data Protection)
SAIF (Secure AI Framework)	• Stealing the model • Data poisoning of the training data • Injecting malicious inputs through prompt injection • Extracting confidential information in the training data	• AI ecosystemで強力なセキュリティ体系構築 • 検知及び対応を拡張して組織内の脅威検知AI導入 • 既存及び新規脅威に対応するための防御自動化 (Automate defenses) • プラットフォームレベルの制御で組織全体に一貫したセキュリティ保障 • AI配布のためにもっと早いフィードバックループ(faster feedback loops)を作成及び制御を調節し、緩和処置を実施 • ビジネスプロセス上、AIシステムの脅威コンタクト化 (Risk Contextualizing)
FMTI (The Foundation Model Transparency Index)	• The upstream / Downstream practices of the foundation model developer、Model-level領域で透明性の概念分析 • 全ての点数に対する異議申し立ての機会提供	• 会社及びFoundation Model Developerを対象にモデル開発及び配布透明性評価 • 関連規制政策を計画時、情報活用及び企業の透明性を向上のための動機づけ
FATE (Fairness、Accountability、Transparency、and Ethics in AI)	• 人工知能(AI)の活用増加によるAIプログラムの道徳性疑問申し立て	• FATE(公平性、責任、透明性、倫理)とAIに対する適宜及び社会的な影響研究
AI RMF 1.0 (Artificial Intelligence Risk Management Framework)	• 有効性及び信頼性、安全性、セキュリティ及びリカバリ性、責任と透明性、説明及び解析可能性、個人情報保護、公平性	• リスク管理による市民の自由と権利脅威などAIシステムの潜在k的な否定的影響を最小化し、肯定的な影響を極大化
A Sensible Regulatory Framework for AI Security	• AI as a Subsystem • AI as Human Augmentation • AI with Agency	• AI記載に対する潜在的な事項とAI開発及び採用のためのガイドライン設定による推奨事項提示

【「表 セキュリティ技術 2−1」人工知能を活用したセキュリティ脅威対応のためのフレームワーク】

「表 セキュリティ 技術2−2」のように、国家及び企業からも人工知能の安全性と信頼性を確保するための人工知能の制裁及び重要事項に対する論議で、人工知能の倫理憲章発表及びセキュリティガイドライン配布、人工知能倫理問題の担当部署の新設などの対応をしている。

国内も含め、EU、アメリカ、カナダ、イタリアなどでも人工知能に関する法律が続々と発議され始めた。AIサービスの領域や危険度ごとに詳細的な規制事項を明示していて、人間に影響を及ぼす領域の製品またはサービス提供者の義務強化と、人工知能の開発過程における透明性及び倫理的なガイドライン順守し、人工知能が技術として人間の生活に役に立つ道具としての目的と意図に合うように、技術の適切な使用と目的達成の順守が必要である。

区分		制裁方向	重要事項
企業	Microsoft	• 重要インフラ施設のAIシステムに「安全ブレーキ」義務装着提案	• 5つの原則提案：政府主導のAI安全フレームワーク実現及び構築、重要インフラを制御するAIシステムに安全ブレーキ(safety brakes)必要、AI技術アーキテクチャ基盤の広範囲な法律及び規制フレームワーク開発、AIに対する学術及び大衆のアクセス確保を目指して、透明性の促進と公民間のパートナーシップの追求
	Google	• 「責任あるAI発展のための政策議題」提案	• AIが持ってくる経済効果の極大化のための機会創出、AI技術の誤用危険を減らすための責任奨励、グローバルセキュリティ強化及び技術悪用防止
	OpenAI	• 国際機関の必要性提案	• AI発展の成長率概念を導入し、開発速度を調整、IAEA(国際原子力機関)のような国際機関の設立で開発管理、人間の価値を従うように「整列(alignment)」技術提案
	Adobe	• 独自AI倫理原則とAIチームで管理	• Adobeが保有しているイメージ、オープンライセンスコンテンツ、著作権が切れたコンテンツ学習で紛争遮断

【「表 セキュリティ技術 2-2」政府と企業のAI制裁方向及び重要事項 (1/2)】

区分		制裁方向	重要事項
정부	韓国	• セキュリティガイドライン及び注意事項案内書配布 • 「人工知能産業育成及び信頼基盤造成関する法律」の定め	• 生成型人工知能技術の代表的なセキュリティ脅威及び安全な技術使用のガイドライン、サービス構築時の考慮事項、セキュリティ脅威及び対応方法に関するセキュリティガイドライン • 人間の生命と安全及び基本権の保護に重大な影響を及ぼす恐れがある領域で活用される部分を「高危険領域人工知能」設定 • 人工知能を利用した製品またはサービスを提供する事業者は利用者に対する高危険人工知能の使用有無通知義務、人工知能の信頼性と安全性確保のための処置義務存在
	EU	• 「人工知能法律(AI Act)」草案ヨロッパ議会の常任委員会の承認	• (Unacceptable risk)EUの価値を違反するサービス(例：潜在意識に害を及ぼしたり改ざんする、人を搾取する、リアルタイムで動作し、人間の制御ができない状態での意思決定)禁止 • (High risk)市場での発売前に厳格な義務適用、このカテゴリに属するAIサービスのリストは毎年検討後、アップデート勧告 • (Limited risk)一般的な意思決定に使用される人工知能システムのアルゴリズム及び意思決定の過程に対する企業の透明性義務適用 • (Minimal risk)ビデオゲーム、スパムフィルターなど危険がないもしくは最小の場合人工知能の法律での規制なし • その他にAIの創作物に「AIで生成する(Made with AI)」表示必須 • 各企業はAIサービスの結果物導出、サービス開発過程内に倫理的ガイドライン順守有無確認
	アメリカ-EU貿易技術協議会 (TTC)	• 「自主行動規範」策定	• チャットGPTのような生成型人工知能の副作用対応及び新技術登場時、規制方法準備及び格差縮小
	アメリカ	• 各「アルゴリズム責任法律(Algorithmic Accountability Act of 2022)」発議	• 適用対象：ADS(Automated Decision System)、ACDP(Augmented Critical Decision Process) • ADSは人間の介入なく、自動化された決定や判断の根拠になる全てのコンピューティングシステムまたはその他データ処理システム、人工知能技術から派生された全てのものを含む • ACDPは重要な意思決定に自動化された意思決定システムを活用する全ての過程が含まれているもの、人間の最終的な意思決定に人工知能・アルゴリズム活用結果を根拠とするとき適用されるように導入された概念
	カナダ	• OpenAIのデータ収集及び使用に関する共同調査スタート	• OpenAIのデータ収集及び使用に関する共同調査スタート • 使用者(residents)の個人情報収集、使用および公開に対する同意有無調査
	イギリス	• 「AI記載に対する革新的なアプローチ」AI白書発表	• AIに対して合わせた法律導入の止揚、既存規制きかんからAI監督実施必要
	イタリア	• イタリア個人情報監督機関(Italian DPA)のチャットGPT使用禁止	• チャットGPTの個人情報収集、処理及び使用者年齢確認の不在による個人情報保護規定(GDPR)違反理由判断後、チャッGPTの禁止措置
	日本	• 「AI戦略チーム」新設	• AIの業務活用に関した課題整理及び部署間のコミュニケーション強化方法論議
	中国	• 「生成型AIに対する管理指針」公表	• 国家インターネット情報弁公室は生成型AIサービス提供対象が一般人である場合、事前にセキュリティ審査評価書を提出するように強制する指針
	ユネスコ	• 「人工知能倫理勧告」発表	• データ保護強化、社会的点数表か及び大量監視(Banning social scoring and mass surveillance)禁止、モニタリング及び評価支援(Helping to monitor and evaluate)、環境保護(Protecting the environment)

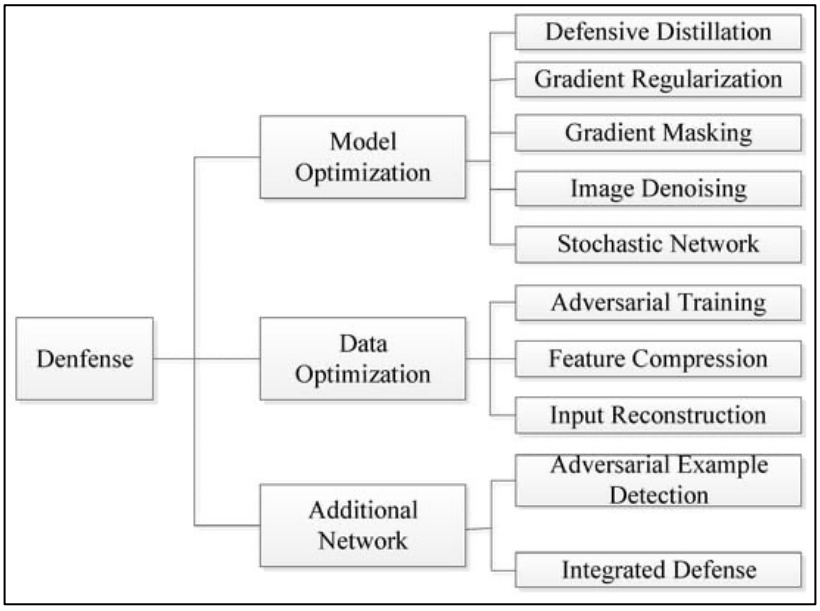
【「表 セキュリティ技術 2-3」政府と企業のAI制裁方向及び重要事項 (2/2)】

人工知能の問題は、制度やセキュリティガイドラインだけで解決できるものではない。生成型AIを含めた人工知能を攻撃する敵対的攻撃に対する敵対的防御(Adversarial Defense)の研究も着実に進行している。

敵対的防御技術を知るためには、敵対的攻撃に対する理解が必要である。敵対的攻撃は、攻撃者が意図的にディープラーニング(Deep learning)システムをごまかすために、ディープラーニングモデルの内部的な脆弱性を利用して作った特定ノイズである摂動(Perturbation)を利用して、誤分類を誘発する入力値を作ることを意味する。敵対的防御技術はこのような敵対的攻撃を防ぐための技術である。
敵対的防御技術は、ディープラーニングを誤魔化しを防ぐためにモデル最適化(Model Optimization)、データ最適化(Data Optimization)、追加的なネットワーク(Additional Network)に分類できる。

敵対的防御技術で最も簡単でよく使用される方法は、敵対的訓練(Adversarial Training)である。ディープラーニングモデルの訓練過程に敵対的な例を生成した後、学習させることで敵対的攻撃に対するエントロピーを最小化するデータ増強(Data augmentation)である。AIリスクの評価チームのリーダーであるAleksander Madryが発表した敵対的攻撃(Projected Gradient Descent)は、クロスエントロピーの損失を最小化する方向で訓練をさせ、敵対的の攻撃に対するロバストネス(Robustness)が確保できるようにする。C&WとPGDなどの攻撃で壊れたDefensive Distillation以外にもGradient Masking、Feature Squeezingなど多様な方法が研究されている。

このようにディープラーニングモデルのロバストネスを確保するための方法で、ディープラーニングモデルの敵対的攻撃を生成してくれるオープンソースプロジェクトであるFoolboxやディープラーニングモデルをホワイトボックスとラベルがなしでテスティングするフレームワークであるDeepXplore、LNPモデルのテストを体系化してチェックリスト基盤のフレームワークを提供するeyond Accuracy：Behavioral Testing of NLP models with CheckListなど人工知能の攻撃と防御以外にも独自の検証方法の研究も必要である。

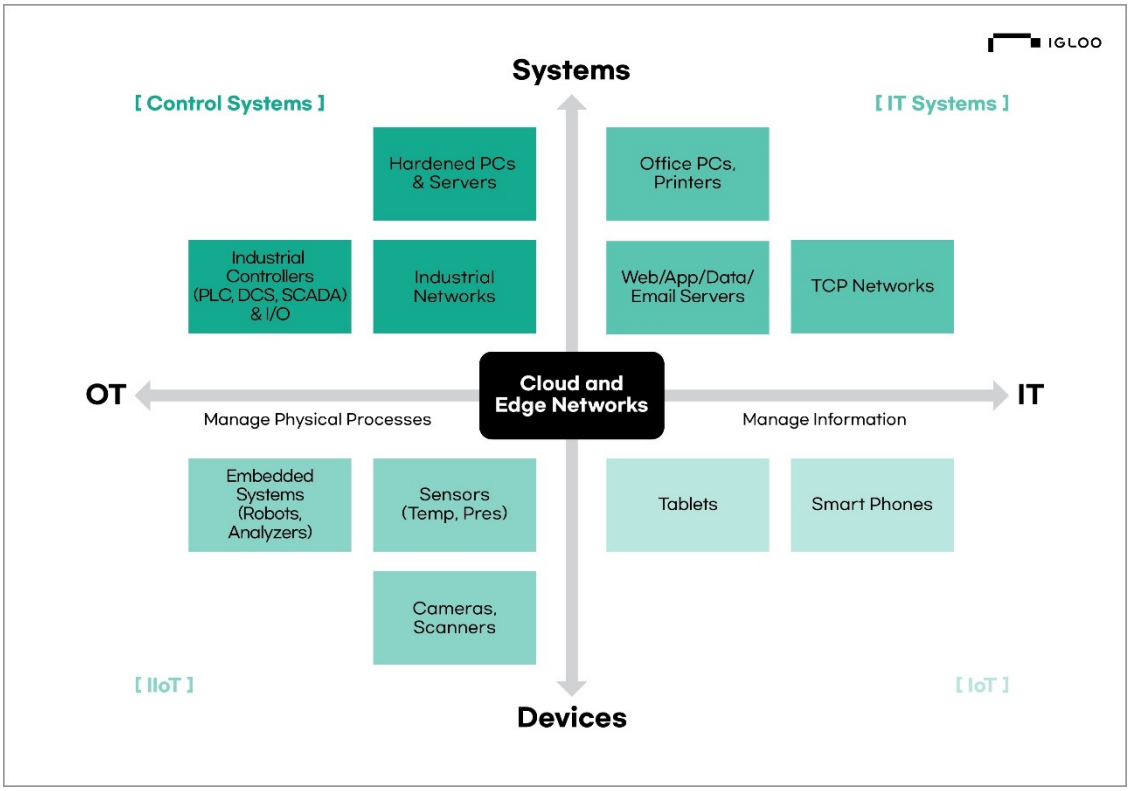


【「図 セキュリティ技術 2-1」Adversarial Attack Defense Methods of Deep Neural Networks (参考：Adversarial Attack and Defense: A Survey)

3) DXによるIT-OT融合生態系拡散及び融合セキュリティ

人工知能(AI)、クラウド、データなど次世代技術を基盤とした産業全般のDXで企業の競争力の強化及び新たな価値の創出は、ビジネスモデルのパラダイムと産業生態系全般に革新を持ってくることで産業間の壁を崩した。融合生態系の確認でサイバー環境と物理的な環境が結合されたサイバー物理システム(CPS、Cyber-physical systems)が登場した。CPSは物理的な実際のシステムとサイバー空間のソフトウェア及び周辺環境を統合するシステムでスマートファクトリ、スマートグリッド、自動運転、自動運航船などグローバル競争力が確保できる革新成長動力である産業分野を意味する。

CPSは「図 セキュリティ技術 3-1」のような情報技術(IT)と運用技術(OT)、システム(System)とデバイス(Devices)4つで分類できる。ITとOTを基準にSystemとDevicesを分離するとそれぞれ制御システム(Control System)とITシステム(IT System)、産業用モノのインターネット(IIoT)とモノのインターネット(IoT)で分類できる。まず、制御システムでは産業用ネットワーク及び制御システムを管理するプログラミング制御装置(PLC、programmable logic controller)、分散制御システム(DCS、distributed control system)、リモート監視制御システム(SCADA、Supervisory Control and Data Acquisition)などが存在し、ITシステムは一般的に使用しているサーバ、ネットワーク、メールサーバなどが含まれる。Devicesを基準でIIoTではセンサー、エンベディッド(Embedded Systems)、スキャナなどが存在し、IoTではスマートフォン、タブレット、ウェアラブル機器(Wearable Device)などが分類できる。



【「図 セキュリティ技術 3-1」ITとOTを利用したCPS相関関係 (参考：Featuring、IT-OT Cybersecurity Convergence、一部再構成)】

CPSで人工知能、ブロックチェーン、マシンラーニング、5G/6Gなど、次世代技術と産業が結合されることで、産業分野ごとに知能化、自動化、効率化が期待できる。CPSを適用した代表的な例では製造分野、医療分野、スマートシティ、運送分野がある。

CPSは、製造分野で複雑な工程による安全事項及び人災を防ぐために、無人化での工程モニタリング及び誤りの追跡を提供する。また制御システムと結合して、物的資源や人的資源の効率化で生産性を向上することもできる。医療分野ではハードウェアであるウェアラブル機器で患者の生理的な特徴をモニタリングし、緊急状況に対応ができ、健康管理アプリによる予防及び治療で個人健康記録(PHR)管理及びカスタマイズサービスが提供できる。
さらに人工知能で治療薬物の開発及びデジタル治療剤など開発期間の短縮及び向上された診療サービスが提供できる。

スマートシティは、都市が提供する交通、安全、生活など便宜性を増大するための目的性を持っているが、スマートグリッド(Smart Grid)を結合させると、知能型電力需要管理、新再生エネルギー
連携、運用効率化、電力網監視・保護の高度化及び電気自動車運転インフラ技術などと結行して、便宜性と効率性の提供ができる。Googleは、AIでデータセンターの全エネルギーの中、15%を節減できそ、BMWやアウディなど自動車メーカーは、自動車から電力網に電気を移動させるV2G(Vehicle to Grid)で電気車の新たな付加価値要素として活用している。

運送分野では、運送手段が無人化できるように自動運転自動車、自動運航船、アーバン・エア・モビリティ(UAM、Urban Air Mobility)などの分野に適用されている。自動運航船の場合、陸上で船をリモート操縦し、船内のシステムを監督・管理及びシステムの問題を制御したり最適の航路を人工知能で分析する方向に技術が活用されている。

区分	期待効果	関連技術
製造分野	• 物理システム及び制御システムと統合、IP割り当て及びモニタリング • 生産性向上、資源(物的、人的)の効果的使用、運用の優秀性達成	• Internet of Service：PLM、SCM、CRM、QMS、ERP • Internet of Things：Sensors、Actuators、Controllers、Mobile Devices • IIoT：Sensors(Temp、Presなど)、Cameras、Scanners、Embedded Systems(Robots、Analyzers)など • Industrial Controllers(PLC、DCS、SCADA)、I/O • Hardened PCs、Servers • Industrial Networks • クラウドコンピューティング • VR·AR • 人工知能
医療分野	• 様々な生理的な特徴を同時にモニタリング及び調節するためのシステム追加 • 予防、治療、緩和及びリハビリ医療サービスに使用されるネットワーキング機能、複雑な物理的な疫学および医療機器制御システム追加 • リモート患者モニタリング、制御、治療薬物開発加速化及び向上された診療可能	• ハードウェア：個人健康管理機器及びウェアラブル機器(ゲートウェイ、血糖、血圧、心電図、活動量測定、医療用センサー挿入スマート機器、現場検査機器(POCT)、バンド/ネックレス型、付着(パッチ)型、人体挿入型)、部品(バイオセンサー、保存及びディスプレイ機器、通信機器) • ソフトウェア：健康情報提供アプリ、カスタマイズ健康管理アプリ、医療整備管理プラットフォーム/DB(医療情報管理プラットフォーム(EMR、EHR))、個人健康情報管理プラットフォーム/DB • サービス：診断サービス(体外診断、遺伝子/ゲノム分析サービス)、健康管理サービス(個人健康健診管理サービス、個人健康記録(PHR)管理及びカスタマイズサービス)、リモート医療サービス(老人健康管理サービス、リモート相談、リモートモニタリングサービス)
スマートシティ	• インフラ、綺麗で持続可能な環境、その他資源準備など • サイバーサービスと年医療サービスを結合してインフラとサービスの強化、雇用創出 • 知能型検知及びリアルタイムモニタリング、制御、データ処理及び意思決定に使用	• 広域モニタリング及び制御：衛星測定器(PMU)、集中リモート監視制御システム(SCADA)、広域モニタリングシステム(WAMS)、広域監視制御システム(WASA) • 情報通信技術統合：通信機器、ルーター交換機、ゲートウェイ、コンピューター、全社的資源管理(ERP)、顧客情報システム(CIS) • 新再生エネルギ、分散発展統合：発展制御機器、保存機器、エネルギ管理システム(EMS)、分散発展管理システム(DERMS)、地理情報システム(GIS) • 送電網高度化：柔軟送電システム(FACTS)、高圧直流送電システム(HVDC)、ネットワーク安定性分析、自動復旧システム • 配電網管理：自動リクローザー(re-closers)、リモート生業分散発展及び保存、変圧器センサー、ケーブルセンサー、停電管理システム(OMS)、人材管理システム(WMS) • AMI(知能型検針インフラ)：スマートメーター、家庭用ディスプレイ、サーバー、計電気、計量データ管理システム(MDMS) • 電気自動車充電インフラ：受電インフラ、バッテリー、インバータ、スマートG2V樹殿及びV2G放電技術
運送分野	• 排気ガスの減少による環境悪化及び交通渋滞解決、道路、航空運送サービス強化など高速交通パラダイムの変化 • 情報通信、知能、検知機能などエッジコンピューティング、データ基盤で次世代共有、自動、連携及びデータ中心交通パラダイム	• 移動手段：自動運航船、UAM(Urban Air Mobility)、無人ロボットタクシー、スマート農機械 • スマート物流：スマート分類·ピッキングシステム、スマート航空貨物

【「表 セキュリティ技術 3-1」CPS使用による多様な分野の発展期待現況】

アメリカでは、サイバー物理システムセキュリティ(CPSSEC、The Cyber Physical Systems Security)プロジェクトで、CPSとIoTのセキュリティ問題を解決しようと論議している。融合生態系は、サイバー環境と物理的環境の考慮が必要になるため、融合生態系の一つであるCPSでセキュリティ強化方法を悩んでいる。CPSセキュリティを脅威する要素は「表 セキュリティ技術 3-2」のように、環境要素、サービス要素、対応技術要素の3つの観点で分類し、物理的環境要素、運用環境要素、社会・経済的環境要素、個人情報、運用階層間総合作用、サイバーセキュリティの6つで再分類できる。

CPSは、サイバー環境と物理的環境ごが結合されているため、サイバー環境のセキュリティ問題と物理的環境のセキュリティ問題が一緒に誘発できる環境である。サイバー環境で発生するネットワークで脆弱なインフラが露出されたり、背セキュリティパッチの未適用、間違ったセキュリティ設定などが攻撃に悪用できるため、周期的な脆弱性診断とセキュリティパッチ管理で安全を維持することが大事である。その他にも物理的な環境から発生する機器欠陥、計画されていないシステム終了、管理者のミスーなど可用性の低下要因に対して予防ができるように教育と管理が必要である。

観点	詳細基準	発生しうる脅威	対応方法
CPSセキュリティを脅威する環境要素	物理的環境要素	• 物理的機器の変造による可用性喪失 • 自然災害：洪水、台風、地震など	• ボタン、ポート、ケーブル、ネットワーク連携、電源など機器の物理的な変造防止が必要 • MIL-STD-810(Military Standard Environmental Engineering Considerations and Laboratory Tests)標準企画(温度、湿気、砂/埃、腐食)に合う機器を考慮
	運用環境要素	• 運用ミス：運用未熟、教育不足、運用手順違反など • 可用性毀損時の対策不備：BCP、DRSなど • 不適切なパッチ管理	• 標準運用手順及び計画樹立、機器に対する運用バックアップ計画、切断計画、攻撃時例外処理機能が必要 • 計画されていない再起動の許可禁止など、電源問題、災難復旧および高可用性に対する考慮が必要 • システムの全ての構成要素に対するサポート可能性 • 物理的機器に対する部品及びソフトウェアアップグレード及びセキュリティパッチに対するポリシー樹立が必要
	社会・経済的環境要素	• 過度な開発費用増加 • 人と相互作用不備(運用の便利性など) • 安全性不備	• 開放型参照アーキテクチャー及び標準、モデル基盤エンジニアリング方法論、シミュレーション、検証及び検証ツールの改善による開発費用の節減 • 人と技術、複雑なインフラと人との相互作用の活用、経済的、社会的、環境的方法で利害関係者の要求、欲求及び熱望充足の観点からのアプローチが必要 • 安全性、信頼性向上及びかち向上で投資受益の証明
CPSセキュリティを脅威するサービス要素	個人情報	• 個人情報管理不備及び漏洩	• 個人情報保護、強化、機密個人情報の適切な使用のためのCPS技術及び方法が必要 • 地理的位置及び当該国の法律に対する暗号化、保存など個人情報保護戦略が必要
	運用階層間相互作用	• 既存セキュリティソリューションとの互換性問題 • 物理システムから使用されるネットワーク暗号化不備	• 個別CPSのシステムを安定的で検証できるように組み立てられるモジュール化及び構成に対するアプローチ方法が必要 • 各運用階層に対する危険評価で潜在的な影響と緩和戦略樹立が必要
CPSセキュリティを脅威する対応技術要素	サイバーセキュリティ	• OSまたは応用プログラムの結合 • マルウェア、ランサムウェア • サプライチェーン攻撃	• ネットワークで繋がっているサイバー物理システムと重要インフラサイバー攻撃に対する弾力性(resilient)が重要 • OSまたは応用プログラムの結合による脅威に対してペネトレーションテスト、脆弱性診断、パッチ管理が必要

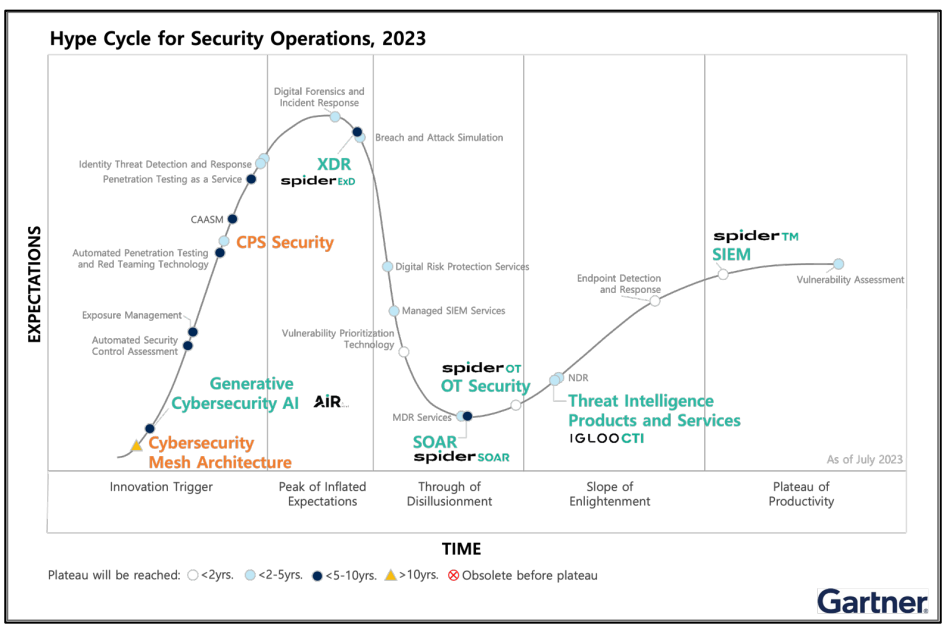
4) 脅威可視化のための資産識別と危険管理技術、攻撃表面管理

ビジネスの柔軟性及び効率性を極大化する目的で、DX及び全てのサービス化(XaaS、Anything as a Service)、マイクロサービスアーキテクチャ(MSA)、応用プログラミングインターフェース(API)など、組織の構成とソフトウェアのモジュール化で組織のインフラ範囲及び曖昧性が増大されている。

問題はこのようなインフラの境界の曖昧性がセキュリティ可視性を低下させそ、新たなセキュリティ脅威になる可能性がある。攻撃表面(Attack Surface)は、既知のセキュリティ脅威(Known Threat)や未知のセキュリティ脅威(Unknown Threat)を識別し、管理するための攻撃者の攻撃接点とも言える。

アメリカ国立標準技術研究所(NIST)とOWASP(Open Worldwide Application Security Project)からも攻撃表面に対して、「システム、システム要素または環境に入ったり、影響を及ぼしたりデータを抽出しようと試みることができるシステム、システム要素または環境の境界にある点の集合」と定義し、攻撃表面管理の必要性を提示している。重要なのは、攻撃表面に内包された「未知のセキュリティ脅威」というのが、必ずしも脆弱性(Vulnerability)だけを意味しているわけではない。公開されているけど、管理されていないセキュアシェル(SSH、Secure Shell)ポート、リモートデスクトッププロトコル(RDP)、不要なWebサービスなどはセキュリティ担当者や使用者に管理(Management)されていない要素である。

攻撃表面管理(ASM、Attack Surface Management)の用語が登場したのは、2018年にクローバルセキュリティリサーチ企業であるガートナー(Gartner)ではサイバーセキュリティ危険管理のために攻撃表面を減らし、モニタリングと管理するための目的で、攻撃表面管理という用語を「セキュリティ運用ハイプ・サイクル(Hype Cycle for Security Operations)」で発表してから始まった。「図 セキュリティ技術 4-1」のセキュリティ運用ハイプ・サイクルからは、2018年に初めて登場した発生期(Innovation Trigger)段階の「外部攻撃表面管理(External Attack Surface Management)」以外にも露出管理(EM、Exposure Management)、サイバー資産攻撃表面管理(CAASM、Cyber Asset Attack Surface Management)などに細分化されていることが確認できる。



【「図 セキュリティ技術 4-1」攻撃表面管理と関連した技術要素の現況
(参考：Hype Cycle for Security Operation 2023、Gartner、一部再構成)】

攻撃表面管理のためには、資産の位置によって外部資産(External Assets)と内部資産(Internal Assets)で分類でき、資産のカテゴリによってクラウド資産(Cloud Assets)、子会社ネットワーク(Subsidiary Networks)、オンプレミス資産(On-premise)で分類できる。攻撃表面は資産のいち、資産のカテゴリ以外にも資産お形によって△デジタル攻撃表面(Digital Attack Surface)、△物理攻撃表面(Physical Attack Surface)、△ソーシャルエンジニアリング攻撃表面(Social Attack Surface)で分類できる。

区分	説明	関連	攻撃ベクター
Digital Attack Surface	• システムアクセスポイント、ウェブサイト、ポート及びサービスに対する外部脆弱性攻撃ポイント	• Server • Database • Cloud instance • Remote system (RDP、SSH、etc) • Shadow IT	• Compromised or Stolen Credentials • Weak Credentials • CVEs • Missing or Poor Encryption • Missing or Poor Authentication • Misconfigurations • Phishing • Malicious Insider • Trust relationships • Denial-of-Service
Physical Attack Surface	• オンプレミス機器と事務室外部で会社ネットワークと繋ぐ機器及び会社のハードウェアに対するアクセスポイントを含めた脆弱性攻撃ポイント	• Desktop • USB • mobile phone	
Social Engineering Attack Surface	• フィッシングメール、フィッシングサイトなどを利用して人を対象にするソーシャルエンジニアリング脆弱性を狙った攻撃ポイント	• E-mail • SMS • SNS • person	

【「表 セキュリティ技術 4-1」攻撃表面ごとの攻撃ベクター】

組織の資産及びインフラの複雑度が高くなるため、潜在的なサイバー攻撃の侵入経路である攻撃表面を識別して管理することに限界が発生する可能性がある。従って、サイバーセキュリティのレベルを維持するためには、組織の資産とインフラ内に存在する脅威と脆弱性になれる攻撃ベクターを持続して識別し、分析して攻撃表面として悪用される要素を最小化することが大事である。これで攻撃表面管理を実施するために攻撃表面管理プロセスの重要要素である△資産の検索と識別、△資産の分類での優先順位指定、△積極的な対応、△n持続的なモニタリング実施が必要である。

区分	説明
資産検索と識別 (Discovery & Mapping)	• 組織とセキュリティチームは資産に対してスキャンを実施し、ログを検討して既知の資産と未知の資産を全て検索 • 組織ネットワーク内のすべての資産、システム、アプリケーション及び進入ポイントを識別 • 資産が自動でマッピングされて既存のSOCツールと統合され、より迅速な所有者の識別及び強化で事故を解決
資産の分類による優先順位指定 (Prioritization& Context)	• 自動化ペネトレーションテスト及びレッドチームの構成が攻撃表面を検証する組織の能力に重要な役割を実施 • 多くの組織が規定遵守要求事項で義務がある場合のみテストを実施 • 組織の特定危険プロフィール、規定遵守要求事項及びビジネス目標の特定状況から資産の脆弱性を分析する作業を含む • 攻撃の潜在的な影響、解決の困難などの要素を含めて危険と潜在的な影響を基準で重要どうによって優先順位を指定
積極的な対応 (Remediation)	• 組織のネットワーク、システムまたはアプリケーションなどに脆弱性が識別されたら修正
持続的なモニタリング (monitoring)	• 外部の攻撃表面と多様な構成環境(ネットワーク、クラウドサービスなど)及び分散攻撃表面を持続的に確認実施

【「表 セキュリティ技術4-2」攻撃表面管理プロセスの重要要素】

攻撃表面管理に対する重要性が強調されることで、多様な攻撃表面管理方法として△露出管理(EM)、△サイバー資産攻撃表面管理(CAASM)、△外部攻撃表面管理(EASM)、△持続脅威露出管理(CTEM)などが適用できる。基本的に攻撃表面管理の一番根本的な概念は、見えない資産に対する限界を乗り越えて全体的なデジタル資産の可視性を確保するために脅威露出管理(CTEM、Continuous Threat Exposure Management)で既存の脅威インテリジェンス基盤の状況認識と自動化されたセキュリティ危険管理の実施が必要である。

区分	説明
Exposure Management (EM)	• 組織が持続的で一貫的に可視性を評価し、組織の手じたる資産のアクセス性と脆弱性が件検証できるようにする一連のプロセス • 素早く拡張される攻撃表面により既存の脆弱性管理で十分ではない組織に存在する脅威露出リスト作成、優先順位指定及び検証などで問題を減少させる
Cyber Asset Attack Surface Management (CAASM)	• セキュリティチームが資産の可視性及び表面の露出問題を乗り越えるためにサポート • エンドポイント(Endpoint)、サーバ及び機器のような資産の配下集合を収集する他の製品から資産可視性を集計 • セキュリティチームはすべてのデジタル資産からセキュリティ制御差、セキュリティ体制及び資産露出などを探してセキュリティ状態改善可能
External Attack Surface Management (EASM)	• インターネットに繋がっている企業資産及びシステムに関する漏洩を検索するために配布されたプロセス、技術、管理サービス • インターネットに繋がっている資産を識別する同時に発見された脆弱性及び関連脅威の優先順位を指定 • 脅威行為者に露出された公開ドメインのデジタル資産に関する危険情報提供
Continuous Threat Exposure Management (CTEM)	• 重要資産に対する危険を識別、測定及び優先順位を指定するプロセス • 企業の物理的資産とデジタル資産の脆弱性を持続的で一貫的に評価されるようにサポートするフレームワーク

【「表 セキュリティ技術 4-3」攻撃表面管理フレームワークごと主要特徴】

持続的な攻撃表面管理で攻撃表面を最小化するためには、外部的には露出されている公開ドメインのデジタル資産と関連された危険情報を識別し、除外が必要であり、内部的には既存のセキュリティ体系との連携などにより、資産識別及び脆弱性除去などの活動を持続的に実施し、セキュリティ制御差の最小化のためにセキュリティ可視性の確保が必要である。これのために△管理的な側面、△技術的な側面によるセキュリティ強化方法を探す必要がある。

管理的な側面では、使用中の資産と管理されない資産に対する資産リスト化作業とレガシーソフトウェア(Legacy Software)、重複資産などを把握し、これに対する資産複雑性を除去する必要がある。ソフトウェアとファームウェア、機器などに対して、周期的に自動化された脆弱性診断、ペネトレーションテスト、インフラセキュリティ診断などを実施し、安全な環境を維持する必要があり、最新セキュリティパッチと最新バージョンの機器導入を実施するなどの対応が必要である。

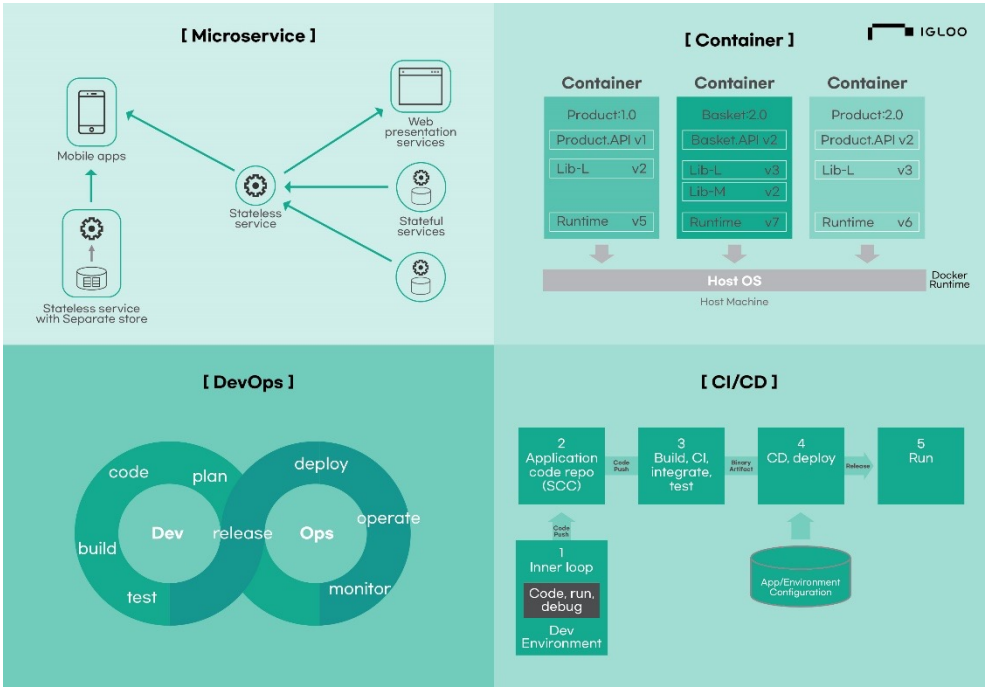
そして不正メール、サイトアクセスによるランサムウェア感染、情報奪取など多様なインシデント事例が発生している。これは企業や機関に所属されている使用者、管理者、開発者のセキュリティ認識が足りないため発生する問題で、内部サイバーセキュリティ規則を導入し、セキュリティ教育と模擬訓練などを実施してセキュリティに対する認識を高める必要がある。

技術的な側面としては、サイバーセキュリティマッシュアーキテクチャー(Cybersecurity Mesh Architecture)の導入、データセキュリティ強化方法の樹立、ソフトウェア開発セキュリティライフサイクル(Secure SDLC、Secure Software Development Life Cycle)の適用、セキュリティソリューションの導入、セキュリティフレームワーク適用など多様な緩和技術を適用して、攻撃表面の拡張による脅威を管理及び対応準備が必要である。

区分	詳細項目	攻撃表面緩和方法
管理的側面	• 資産リスト化作業実施	• ネットワークアクセス制御(NAC)、デスクトップ管理(DSM)、IPアドレス管理(IPAM)などを活用した資産リスト化
	• 可視性確保のための資産複雑性除去	• 重複またはレガシーソフトウェア(Legacy Software)削除 • マイクロセグメンテーション(Micro Segmentation)導入
	• 資産状態最新化作業	• ソフトウェア、ファームウェア及び機器に対する最新セキュリティパッチと最新バージョン適用考慮
	• 周期的なセキュリティ診断実施	• 自動化ペネトレーションテスト(Automated Penetration Test)実施 • Penetration Testing as a Service(PTaaS)モデル導入 • インフラ(Server、Database、など)対象セキュリティ診断実施
	• セキュリティ教育及び訓練実施	• 使用者、管理者、エンジニアなどセキュリティ認識教育 • 基本的なセキュリティ守則順守のためにベネフィットと導入 • 周期的な標的型メール訓練(メール、APT、DDoSなど)実施
技術的側面	• サイバーセキュリティマッシュアーキテクチャー (CSMA)実現	• ゼロトラスト観点からのセキュリティアーキテクチャ(Zero Trust Architecture)実現 • VPN認証システム、FIDOなど認証システム連携及び追加
	• データセキュリティ強化方法樹立	• 同型暗号(EN、Homomorphic Encryption)のようなプライバシー強化技術(PET、Privacy Enhancing Technology)を利用したデータ保護 • 中央集中型ユーザーアクセス管理及びアクセスのための暗号管理
	• Secure SDLC 適用	• セキュアコーディング(Secure Coding)、DevSecOpsを利用した開発
	• セキュリティフレームワーク適用	• NIST Cybersecurity Framework 2.0 • AI RMF 1.0 (Artificial Intelligence Risk Management Framework) • CSPM (Cloud Security Posture Management)などを適用
	• セキュリティソリューション導入	• SOAR(Security Orchestration Automation and Response)、SIEM(Security Information and Event Management)、XDR(Extended Detection and Response)などを導入

【「表 セキュリティ 技術4-4」攻撃表面緩和方法 (参考：韓国情報通信企画評価院、攻撃表面管理概念と最小化方法動向、一部再構成)】

クラウドネイティブを構成するためには、△マイクロサービス(Microservice)、△コンテナー(Container)、△デブオップス(DevOps)、△持続的統合と持続的配布(CI/CD)が必要である。Microserviceは、単独で実行でき、独立できる小さな単位モデルで主要機能を個別サービス化するため、他の機能に影響を及ぼさない。コンテナーは、クラウドサービスを効率的に管理するための技術を意味する。ソフトウェアの開発から運用までのソフトウェア開発周期(SDLC)を管理するためには、DevOpsを基盤としてソフトウェアの開発及びテスト、統合、配布まで一連の活動を自動化して実施できるCI/CDが必要である。



【「図 セキュリティ技術 5-3」クラウドネイティブ構成別、主要特徴】

区分	構成要素	説明	特徴
アーキテクチャ	Microservice	• ソフトウェア開発時、単独で実行できて独立できる小さな単位モジュールに機能を分けてサービスするアーキテクチャ ＊ サービス間プログラミング言語に縛らないAPIで通信、各サービスはそれぞれのDBを所有 • 主要機能を個別サービス化して必要時に当該の機能のみ資源増設、アップデート、障害処理をして他の機能には影響を及ばない	• 安全性：サービス分離で全体障害状況回避 • 拡張性：個別サービス別きのう、性能改善
インフラ	Container	• クラウド環境からサービスを実行し、効率的に管理するたえめの仮想化技術の単位、つまり軽量化された仮想化技術 ＊ OSカーネルなどは共有し、アプリケーション実行に必要なライブラリやプログラム、設定ファイルなどをVMより軽くパッケージングして移植性などを向上 • Micro Serviceの配布及び実行環境で提供	• 効率性：サーバより軽量化で生成、管理便利 • 移植性：どのようなクラウド環境でも配布可能
運営管理	DevOps	• を開発から運用まで持続的に管理するためのプロセス • アプリケーションの開発-運用間協業プロセスを自動化し、アプリケーションの開発と改善の速度を向上させる。	• 自動化「開発-テスト-配布-運用」の業務サイクルを自動化された単一ワークフローに統合 • 生産性：自動化を基にサービスリリース及びアップデート周期を短縮
	CI/CD	• 開発、テスト統合、配布までの一連の過程を自動化して持続実行 • 持続的な統合と配布でアプリケーション開発段階を自動化してより短い周期でサービスを提供し、改善する方法	• 自動化：開発段階を自動化して短い周期で顧客に提供ができるように持続的な統合及び配布

【「表 セキュリティ技術 5-1」クラウドネイティブ構成別、主要特徴 (参考：韓国デジタルフラットフォーム政府委員会)】

クラウド活性化のための生態系造成及びクラウドネイティブでソフトウェアの拡張性と柔軟性を提供するソフトウェアアプローチ方法実現しても、安全なクラウド生態系を造成できるわけではない。クラウド環境をさらに安全に運用するためにはクラウド環境に最適化されたセキュリティ技術が必要である。「表 セキュリティ技術 5-2」のように技術スタックによるクラウドセキュリティのためにはフレームワークは△クラウド側面、△インフラ側面、△アプリケーション側面で分類できる。

クラウド側面のフレームワークはクラウドネイティブアプリケーション保護プラットフォーム(CNAPP)、クラウドアクセスセキュリティ仲介(CASB)、クラウドワークロード保護プラットフォーム(CWPP)、クラウドセキュリティ構成管理(CSPM)、クラウドインフラ権限管理(CIEM)でクラウド基盤セキュリティポリシー及びクラウドサーバワークロード中心のセキュリティ構成およびクラウド構成エラー検知などのポリシーが適用できる。CNAPPはCIEM、CSPM、CWPPの機能を統合してクラウドインフラの脅威検知及び可視性確保、マイクロサービスとコンテナー保護をポイントとしてアプリケーションを保護する。

インフラ側面では、クバネティスセキュリティ構成管理(KSPM)、サービス型ソフトウェアセキュリティ構成管理(SSPM)、セキュリティサービスエッジ(SSE)でクバネティス(Kubernetes)構成要素のセキュリティ及び間違って構成問題解決、SaaS環境のセキュリティ状態管理が可能である。アプリケーション側面としてはウェブアプリケーション及びアプリケーションプログラミングインターフェース保護(WAAP)、セクリティウェブゲートウェイ(SWG)などでアプリケーションやAPIのセキュリティを強化することができる。

側面	フレームワーク	説明	セキュリティポリシー例
クラウド側面	CNAPP (Cloud Native Application Protection Platform)	• 開発及びプロセス全般に渡ってクラウドネイティブアプリケーションを保護し、セキュリティを強化するために設計されたセキュリティ及びコンプライアンス統合のセット定義	• アーティファクトスキャニング(Artifact scanning)、コード型インフラ(IaC：Infrastructure as Code)スキャニング可能 • CIEM、CSPM、CWPP統合
	CASB (Cloud Access Security Broker)	• クラウド基盤のリソースにアクセスする際、エンタプライズセキュリティポリシーを結合して挿入するためにクラウドサービス消費者とクラウドサービス供給者の間に配置されるオンプレミスまたはクラウド基盤セキュリティポリシー適用ポイント • 多様な累計のセキュリティポリシー実施を統合	• 認証、SSO(Single Sign-On)、権限付与、資格証明マッピング、デバイスプロファイリング、暗号化、トークン化、ロギング、パス、マルウェア検知/防止など
	CWPP (Cloud Workload Protection Platforms)	• クラウドサーバワークロード重心のセキュリティのためのソリューション、ワークロードに対する可視性確保及び攻撃防御が目的	• システム整合性保護、マイクロセグメント、メモリ保護、ユーザー行為モニタリング、ホスト型侵入防止及びマルウェア防止
	CSPM (Cloud Security Posture Management)	• 攻撃成功可能性を減らすために持続的なクラウドセキュリティ改善及び適応プロセス	• クラウド構成エラー検知及び自動修正
	CIEM (Cloud Infrastructure Entitlement Management)	• ハイブリッド及びマルチクラウドIaaSの権限ガバナンスのための管理時間制御でクラウドアクセス危険を管理することにポイントを持っている専門ID中心のSaaSソリューション	• リソースプロビジニング/管理機能 • 使用量モニタリング/監査機能
インフラ側面	KSPM (Kubernetes Security Posture Management)	• 自動化ツールを活用して全てのKubernetes構成要素にセキュリティ、間違った構成および規程順守問題識別及び解決	• RBAC(ロールベースアクセス制御)問題識別、ネットワークセキュリティポリシーの偏差検知、HIPAA、SOX、ISO¥IEC 27001のような標準順守、問題発生時自動対応または修正段階の提案
	SSPM (Software-as-a-Service Security Posture Management)	• 組織の可視性確保及びSaaS環境のセキュリティステータス管理ツール	• データモニタリング及び分析、SaaSアプリケーション内に間違った構成及び過度な権限など脆弱性識別、大段階認証及び暗号化のようなセキュリティ制御、危険識別及び優先順位指定、データ保護及び個人情報保護法のような規定及び標準順守確認
	SSE (Security Service Edge)	• クラウド基盤サービスでユーザーにセキュリティ連携提供、クラウド基盤サービスのためにユーザーを企業ネットワークに直接連携は不要	• CASB、ZTNA、SWG、FWaaS(Firewall-as-a-Serice)機能構成
アプリケーション側面	WAAP (Web Application and API Protection)	• クラウドWAAPは主にパブリックウェブアプリケーション及びAPIを保護するクラウド提供サービス	• ランタイム攻撃、ウェブアクリケーション脅威、自動化された脅威、APIの特殊攻撃に対するOWASP TOP 10攻撃緩和
	SWG (Secure Web Gateway)	• ウェブ/インターネットトラフィックで必要ないソフトウェア/マルウェアプログラムをフィルタリングし、企業お及び規定ポリシー順守実施	• URLフィルタリング、マルウェア検知及びフィルタリング、IM(instant messaging)及びSkypeのようなウェブ基盤アプリケーション制御機能
	ZTNA (Zero Trust Network Access)	• アプリケーションまたはアプリケーションセットの周りにID及びコンテキスト基盤の論理的アクセス境界生成	• ID基盤アクセス制限、SASE(Secure Access Service Edge)統合でリモートアクセスセキュリティ、モニタリングによるデータ損失、ユーザー資格証明損傷防止

04. 最後に

2023年に発生したサイバーセキュリティ脅威及び技術発展を振り返り、2024年のサイバーセキュリティ脅威及び技術に対して展望してみた。2022年に発生した国家主導のハッキンググループによる大規模サプライチェーン攻撃の被害が2023年まで続くことで、国家間の武力衝突が長期化すると、サイバー攻撃は攻撃者が状況を打開するために、新たな媒介として活用される可能性が高くなった。さらに2024年は各国の首相が変わる選挙が多いため、今後政治的な方向も迷宮な状況である。

オープンソース生態系が新たなゲームチェーンジャーになり、インフラの複雑度が高くなることで資産の可視性が低くなり、新たな攻撃表面が発生して、危険のチェーン化が加速化されている。攻撃者は、ソフトウェア脆弱性を利用したサプライチェーン攻撃以外にも、生成型AIで武装した従来のセキュリティ体系を無力化し、迂回する方法を探すため、今も絶え間なく新たな脆弱性と弱点を研究している。

融合生態系の拡散により、全てのビジネスと技術は一つに繋がっている。知能化されて自動化される攻撃者は波を耐えるために、従来のセキュリティ体系から跳ねれてDIA(Deep Visibility、Intelligence、Automation)基盤のセキュリティ監視体系を構築し、攻撃表面を最小化できる持続的なセキュリティを構築することが何よりも重要である。

セキュリティは、一つの製品や技術で実現されるものではない。2024年はいつもより不確実性が高いため、この記事でセキュリティを悩んでいる全ての担当者が環境をさらに安全で作れるように期待する。