SECURITY REPORT

2022 JAN

2022年セキュリティ脅威・技術予測

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。

2022年セキュリティ脅威・技術予測

Introduction

2022年に発生する主要なサイバーセキュリティ脅威と、その脅威に柔軟に対応するためのセキュリティ技術と方法論を独自の観点でまとめてみました。

Highlights

サイバーフォートレスは、2022年に攻撃者が狙う「攻撃対象領域(Attack Surface)」がさらに広がると見込んでいる。 まず、コロナ19および選挙・国際行事などの社会的問題を悪用したサイバー攻撃が持続し、柔軟化された勤務環境の弱点を狙う攻撃もさらに増加すると予想。 また、国家支援を受けるハッキンググループによるサプライチェーン攻撃が増え、ダークウェブ(Dark Web)による情報取引や流通がより活発に行われると予測している。 さらに、デジタル化されたユーザー情報が幅広く活用される「メタバス(Metaverse)」プラットフォームをめぐるセキュリティ脅威も発生すると予想している。

このようなセキュリティ脅威に対抗して、すべての企業・組織インフラと資産に対する可視性を確保し、脅威対応速度を高めることができるセキュリティ技術と方法論の重要性が高まる見通しだ。サイバーフォートレスは、ITとOT環境を合わせる「融合セキュリティ監視体系」とセキュリティ管理の効率性を高めることができる「セキュリティオーケストレーション・自動化および対応(SOAR)」、インフラ・データ・ソフトウェア・ユーザー側で脅威要因を検知する「攻撃対象領域管理(ASM)」の重要性が高まると見込んでいる。 また、人工知能(AI)の逆機能（マイナス的側面）を最小化し、データ活用の安全性を高める技術導入の重要性も高まると予測している。

2022年5大セキュリティ脅威

1. 社会的問題を悪用したサイバー攻撃急増
2. 勤務環境の柔軟化によるセキュリティ脅威の増加
3. 国家支援ハッキンググループによるサプライチェーン攻撃の増加
4. DarkWebでの情報取引と流通の増加
5. ハイパーコネクティビティ新技術の拡散によるセキュリティ問題の増加

2022年5大技術・方法論

1. ITとOT環境を合わせるセキュリティ可視性の確保、融合セキュリティ(Convergence Security)
2. SOARによる4世代セキュリティ監視(Playbook with SOC)
3. 攻撃対象領域の管理による攻撃可能性の最小化
4. データ経済の活性化、個人情報保護と活用のトレードオフ
5. セキュリティの「ひとつの指輪」人工知能(AI for Security)

1 社会的問題を悪用したサイバー攻撃急増

#WithCorona #ワクチン追加接種 #IE11支援終了 #第20代大統領選挙 #第8回全国同時地方選挙 #2022年FIFAワールドカップカタール #2022年北京冬季オリンピック #ソーシャルエンジニアリング手法 #フィッシング #スピアフィッシング

コロナ19ワクチン接種と検査キット等の普及拡大に支えられ、日常回復水準として「ウィズコロナ(With Corona)」に転換されいる。しかし、サイバー環境は「ウィズサイバー脅威(With Cyber Threats)」の状態にとどまっている。コロナ19および最新の社会的問題を利用した攻撃が着実に発生しているからだ。昨年、攻撃者たちは防疫マスク、手消毒剤、ソーシャルディスタンス、コロナワクチン、コロナ感染現況などのコロナ関連キーワードを利用してきた。彼らは今後も「ワクチン追加接種」、「飲むコロナ治療薬など」の最新コロナ19関連問題を使用して攻撃を続けると予想される。

2022年には、選挙や大規模な国際イベントを攻撃キーワードとするスピアフィッシング(spear phishing)およびウォーターリングホール(watering holes)攻撃がピークに達すると見込まれる。2022年北京冬季オリンピック、2022年FIFAカタールワールドカップと関連した攻撃が増加する見通しだ。各イベントに密接に関連する組織または一般ユーザーを狙う攻撃が増えると予想されるため、これに対する万全の備えが必要と思われる。

2022年5大セキュリティ脅威予測

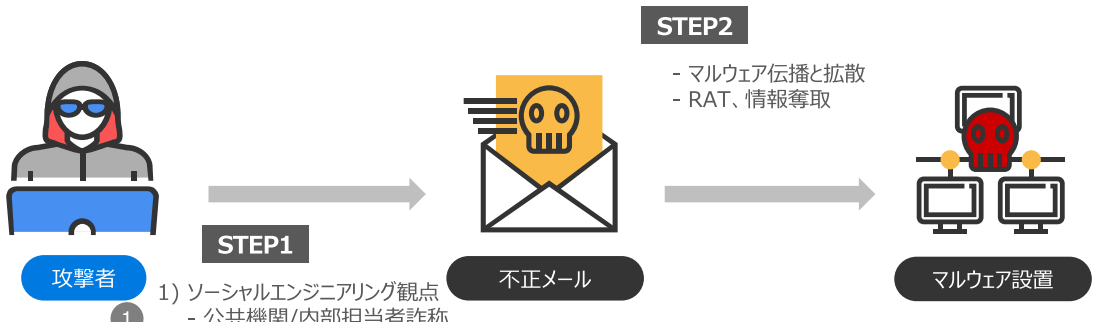
1 社会的問題を悪用したサイバー攻撃急増

#WithCorona #ワクチン追加接種 #IE11支援終了 #第20代大統領選挙 #第8回全国同時地方選挙 #2022年FIFAワールドカップカタール #2022年北京冬季オリンピック #ソーシャルエンジニアリング手法 #フィッシング #スピアフィッシング

2022年主要政治的・社会的問題分析

区分	Key Point	主な内容
政治的問題	国際メガーイベント開催	2022年北京冬季オリンピック(2月)、UEFA女子ユーロ2022(7月)、2022年杭州アジアゲーム(9月)、2022年FIFAワールドカップカタール(11月)
社会的問題	コロナ19問題活用継続	コロナ19防疫品(マスク・外用消毒剤)、With Corona、ソーシャルディスタンス緩和、ワクチン追加接種、飲むコロナ治療薬

ソーシャルエンジニアリング手法を活用した攻撃シナリオ



1) ソーシャルエンジニアリング観点
- 公共機関/内部担当者詐称
- 社会問題悪用(Credential窃取)

2) 技術的観点
- 圧縮/パスワード/大容量メール付き (Spear Phishing)
- HTTP Authentication、PHProxy

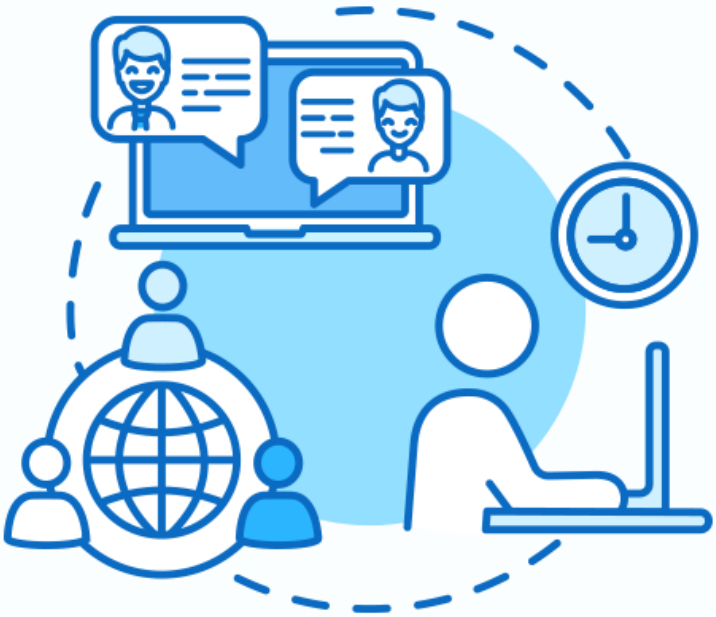
<2022年の主要サイバー攻撃キーワードベースの攻撃戦略及び攻撃技法>

2 勤務環境の柔軟化によるセキュリティ脅威の増加

#テレワーク #ビデオ会議 #VPN #リモートアクセス #セキュリティ可視性の低下 #データ脅威

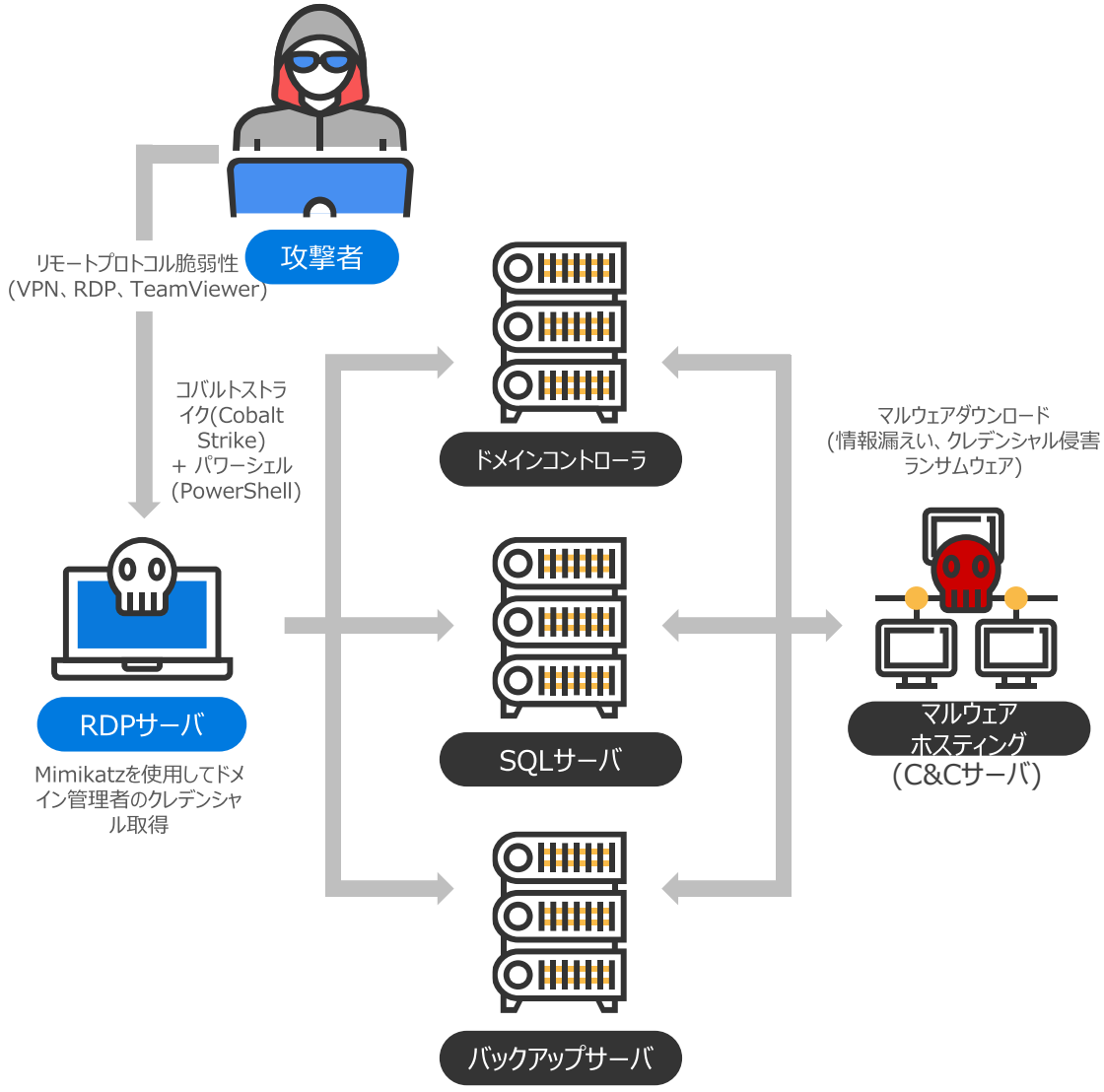
コロナ19により、リモートデスクトッププロトコル(RDP)と仮想プライベートネットワーク(VPN)などに基づく非対面・テレワークが急速に広がるにつれ、変化した勤務環境を狙うセキュリティ脅威も増加する見通しだ。コロナ19発生初期には、自宅や共有オフィスなどで勤務し、勤務場所を分散する断片的な形が主になった。しかし、クラウドを利用することで地理的・技術的な制約が解消され、時間と空間の制約なしに業務をすることができる勤務体制の柔軟化が急速に行われている。 最近では、拡張現実(XR)、ホログラム、メタバス(Metaverse)などの多様なICT融合技術が集約されたデジタル勤務環境(Digital Workspace)まで発展する傾向にある。

これに合わせて柔軟化された勤務環境の新たな攻撃要因とし、組織と組織インフラ、組織メンバーを狙う攻撃も増加すると予測される。2021年にはPulse Secure、Fortinet、Palo Alto Networksなど、複数のグローバル企業のVPNで攻撃者が利用できる多数の脆弱性が報告され、韓国では原子力研究院や韓国航空宇宙産業などの主要研究機関に浸透しようとするVPNの脆弱性を悪用した攻撃が発生したことがある。今後もリモートアクセスを支援するソフトウェアやVPNを悪用した攻撃が増えると予想されるため、企業インフラを脅かす可能性のあるアクセス経路に対するセキュリティチェックと、これらの攻撃に対する対応戦略の準備が必須となるものと見られる。



2 勤務環境の柔軟化によるセキュリティ脅威の増加

#テレワーク #ビデオ会議 #VPN #リモートアクセス #セキュリティ可視性の低下 #データ脅威



<リモートデスクトッププロトコル(RDP)を利用した内部ネットワーク侵入攻撃構成図>

2022年5大セキュリティ脅威予測

3 国家支援ハッキンググループによるサプライチェーン攻撃の増加

#IT #OT #Industrial IoT #SCADA #Cloud #Supply Chain #OT/ICS #Cyber War #APT

上水道施設、製造工場など運用技術/産業制御システム(OT/ICS)環境を狙ったサイバー攻撃も持続する見通しだ。 2010年イランの遠心分離機100台を破壊したStuxnet攻撃後、台湾の半導体メーカーTSMCやノルウェーのアルミメーカーであるノルスク・ハイドロ(Norsk Hydro)など世界有数の生産施設を狙ったインシデントが継続的に発生してきた。今年2月には、米国フロリダ州でリモートデスクトッププロトコル(RDP)を利用して水道インフラにアクセスし、飲料水の水酸化ナトリウム濃度を異常なレベルに高めようとする攻撃が発生し、警戒心をさらに高めた。

OT/ICS環境で発生したセキュリティインシデントを分析すると、一般的に△攻撃範囲の多様化、△攻撃ツールの普遍化、△攻撃波及力拡大、△融合セキュリティ認識不在などの特徴が把握される。従来は、閉鎖ネットワーク環境で運用されていたOT/ICS環境が運用効率向上や自動化の目的でクラウド、アクティブディレクトリなどのIT技術との連携によって、攻撃者が攻撃可能な範囲が拡大した。 また、過去には攻撃者がスタックスネット、トリトン(Triton)などの特定ソフトウェア・機器を標的とする専用のマルウェアを作って攻撃を試みたのとは異なり、最近は高度な技術がなくてもランサムウェア、RDPをはじめとする公開されたソフトウェア、オープンソースを活用して攻撃する事例が急増しているという点もやはり目立っている。

OT/ICSを取り巻くセキュリティ脅威とインシデント発生による影響はさらに拡大するものと見られる。昨年発生した米国送油パイプのハッキングは、ロシアのハッキング組織である「ダークサイド(DarkSide)」によって行われたと推定される。北朝鮮のハッカー組織も国家インフラを狙ったサイバー攻撃を実行していることが明らかになった。OT/ICS環境で発生したサイバー攻撃のかなりの数が国家支援を受けるハッキンググループによって行われたと分析されており、今後もOT/ICS環境に最適化されたサイバー対応策づくりの重要性がさらに高まると予想される。

2022年5大セキュリティ脅威予測

3 国家支援ハッキンググループによるサプライチェーン攻撃の増加

#IT #OT #Industrial IoT #SCADA #Cloud #Supply Chain #OT/ICS #Cyber War #APT

- IT環境を超えてOT/ICS環境まで攻撃範囲を拡大
- コロナ19の影響でデジタルへの転換が加速し、クラウド、アクティブディレクトリなどへの攻撃対象領域が増加

- OT/ICS専用のマルウェア(スタックスネット、トリトンなど)とともに、ランサムウェアおよびリモート接続プログラムの活用拡大
- オープンソースソフトウェアを活用した攻撃ツールの作成・配布の容易性拡大

- 社会基盤施設などにセキュリティインシデント発生時、システム麻痺・破壊を超える人的被害発生可能
- 可用性中心の産業特性上、セキュリティパッチの適用に困難がある

- IT中心のセキュリティガバナンスの確立によるOT環境特性に適合するガイドラインの不在
- ユーザーセキュリティ認識の欠如

<OT/ICS環境のセキュリティインシデント分析結果>

4 DarkWebでの情報取引と流通の増加

#DarkWeb #DeepWeb #CaaS(Cybercrime-as-a-Service)
#RaaS(Ransomware-as-a-service) #個人情報 #Information Leak

2022年には「ダークウェブ(Dark Web)」を通じた情報取引及び流通がより活発に行われると予想される。「ダークウェブ」は暗号化されたネットワークに基づいており、一般的な検索エンジンやブラウザによるアクセスが制限される。当初はハッカーの技術共有目的として使われたが、数年前からは強力な匿名性に基づいて麻薬、銃器などはもちろん、個人情報や企業の主要情報などを取引するサイバー犯罪の目的として使用されている。実際、ダークウェブ上の違法取引規模は継続的な増加傾向である。韓国では、2019年基準韓国内のダークウェブアクセス者数は1日平均15,000人に達したとのこと。これは2016年と比較して3倍以上増えた数値だ。

ダークウェブ市場は特有の匿名性に基づいて不法行為に関連する取引の場の役割をし、急速に拡大すると見られる。ダークウェブによる企業機密情報および個人情報販売の問題は着実に提起されているが、企業インフラにアクセス可能なリモートアクセスアカウントなどが取引されていて、現在ではその被害規模を算定することさえ難しい状況だ。また、ダークウェブでは違法な情報取引に加え、ウォーターリングホール(watering holes)、ウェブスキマー(web skimmers)、分散サービス拒否(DDoS)、ランサムウェアなどをサービスの形で提供する「請負ハッキング」取引も行われており、 より強力な対応戦略づくりが求められる。

5 ハイパーコネクティビティ新技術の拡散によるセキュリティ問題の増加

#メタバス #XR #生体情報 #個人情報 #ブロックチェーン #人工知能 #6G

コロナ19以降、デジタル非対面技術が広く普及し、「メタバス(Metaverse)」をめぐるセキュリティ脅威も発生する見通しだ。メタバスは、仮想現実(VR)や拡張現実(AR)をはじめとする各種実感メディア技術をデータ通信技術と組み合わせた概念で、ユーザーがオフラインと同様に経済、社会、文化活動を営み、現実世界と相互作用できるようにする。実際に発生する可能性のある状況を仮想現実でシミュレーション・モデリングする「デジタルツイン(Digital Twin)」と似ているが、現実世界の自我とつながった多重自我である「マルチペルソナ(Multi Persona)」を通じてプラットフォーム内で商品を購入・流通できるという違いがある。

このようなメタバスの特性を考慮すると、メタバスプラットフォームのユーザーは機密な個人情報の漏洩やデータの改ざんなどのセキュリティ脅威にさらされる可能性がある。メタバスプラットフォームでユーザーは、マウス・キーボードなどの入力装置を通じて生成されるデータとともに、脳波・血圧・呼吸などの生体信号、行動および感情情報データ、そして接続時間と位置、消費性向、財保有状況など、デジタル化された多様な情報を一緒に活用することになる。

このような情報が漏洩したり改ざんされたりすると、深刻なプライバシー侵害や資産価値の低下などの被害が発生する可能性がある。したがって、メタバス産業が活性化するためには、これに対する先制的なセキュリティ規制と対応策の確立が必要であると見られる。特に、収集されるユーザーデータの保存形態、保存場所、適用コンプライアンスによって、その規制範囲と処理方式が異なる可能性があるため、メタバスプラットフォーム上の個人情報保護のための制度的支援とサイバーセキュリティ強化努力を伴わなければならない。

1 ITとOT環境を合わせるセキュリティ可視性の確保、融合セキュリティ (Convergence Security)

#Convergence Security by Design #ISO/IEC 62443 #CMMI #Monitoring #Consulting

異種の機器の連携が強化され、ITとOT領域間の連携性が増加することによって、ITとOT環境のセキュリティ要素を識別しセキュリティ状況を把握するためのセキュリティ可視性確保の重要性が高まることが見込まれる。最近のリサーチによると、OT/ICS環境から発生したセキュリティインシデントによる被害金額は9倍以上で、予想値より上回ることが分かった。OT/ICS環境で見つかるセキュリティ脆弱性の数は増える一方で、インシデントが発生すると予想を超える莫大な被害が引き起こされると見られる。

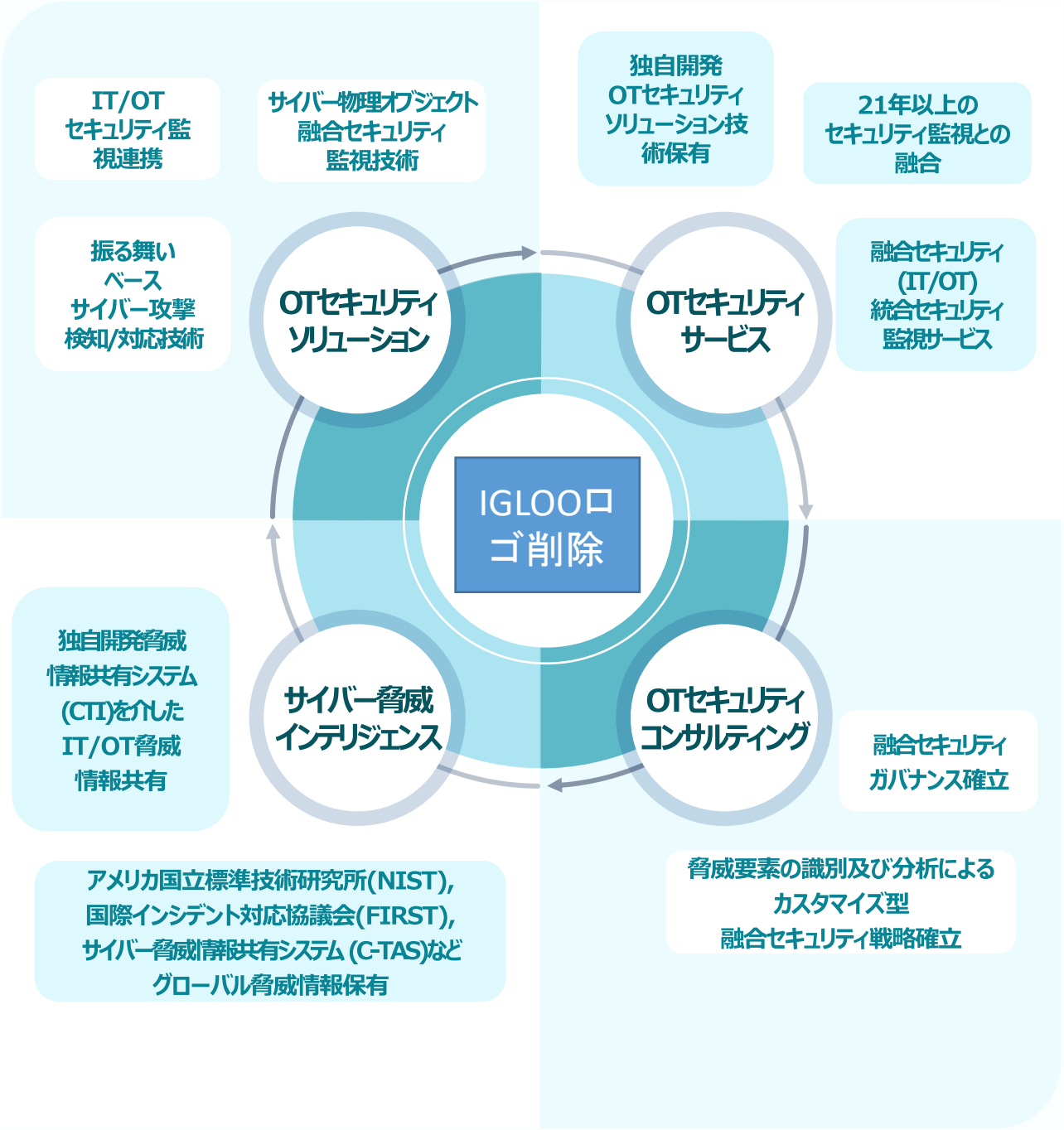
しかし、このような攻撃試行に立ち向かうための融合セキュリティ管理体系を整えるには少なからぬ困難が生じる。OT環境は、ネットワーク、OS、交換周期、運用観点などでITシステムとは異なる特徴を持っている。 OTシステムはメーカー別の異なるプロトコルや専用のOS、開発言語などを使用するため、複数の機器を統合管理して資産を最新化するには難しいところがある。 また「機密性」が重要なITとは違ってOTは「可用性」確保に優先順位をつけるため、製品の交換やセキュリティパッチなどを実施するためのセキュリティを担当する組織がない場合が多いのだ。言い換えれば、OT/ICS脆弱性を含めた脅威情報共有プラットフォームがないことよってセキュリティインシデントに対する対応能力に問題が発生する可能性が高いのだ。

OT/ICS環境を狙うセキュリティ脅威に備えるためにはIT･OT環境の特性と優先順位を考慮した融合セキュリティガバナンスの確立をもとに企業IT･OT資産を狙ったセキュリティ脅威に対する可視性の確保ができる「融合セキュリティモニタリング体系(Convergence Security by Design)」が構築される必要がある。セキュリティ組織はOTセキュリティコンサルティング、OTセキュリティ管理ソリューション、OTセキュリティサービス、OT/ICSサイバー脅威情報共有などによってモニタリング、定期的にセキュリティ検討及びペンテストを実施し、ITとOT領域を包括する識別-検知-分析-対応機能を確保する必要がある。

2022年5大技術･方法論

1 ITとOT環境を合わせるセキュリティ可視性の確保、融合セキュリティ (Convergence Security)

#Convergence Security by Design #ISO/IEC 62443 #CMMI #Monitoring #Consulting



2 SOARによる4世代セキュリティ監視 (Playbook with SOC)

#SOAR #Playbook #セキュリティ監視 #SOC(Security Operation Center) #SIRP #SOA #TIP

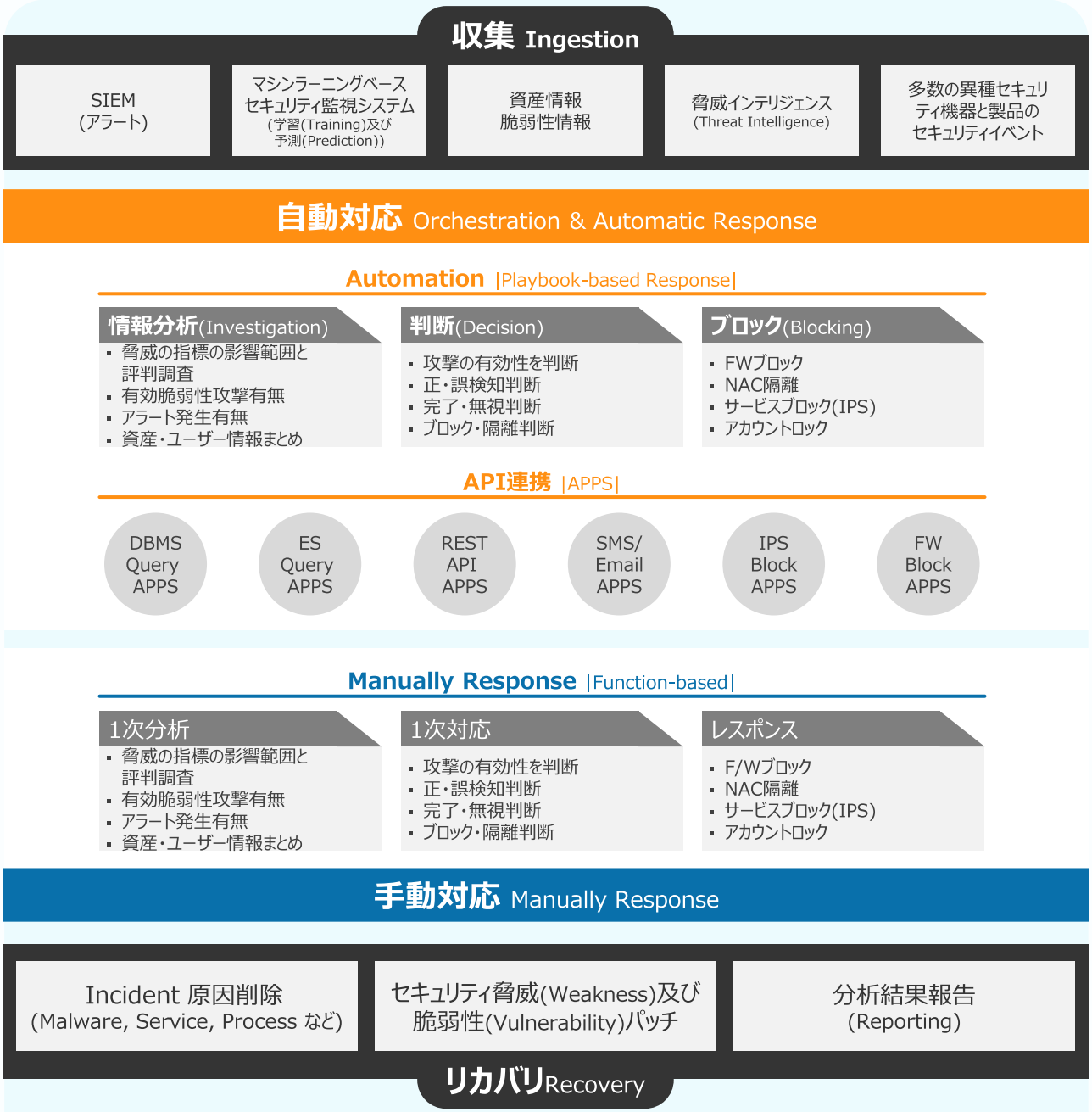
日々組織化かつ高度化されていくサイバー犯罪に対応しようと現在のセキュリティ組織は異種のセキュリティソリューションを運用できるセキュリティ監視 (SOC, Security Operation Center)プラットフォームをもとに脅威要素を識別、対応している。しかし、知能化したサイバー攻撃は日々増加している中、セキュリティの人手不足やスキルの格差による難しさも生じ、すべてのセキュリティ脅威を識別、対応するのは現実的に不可能な状況である。これに対してセキュリティ監視の効率性を高めてSOCの複雑性を解消するための策として「セキュリティのオーケストレーション・自動化及びレスポンス(SOAR, Security Orchestration, Automation and Response)」技術の必要性がさらに増大される見込みだ。

SOAR技術を効果的に導入するためには △レスポンスプロセスの標準化、要員間のスキル格差の縮小、専門人材不足解決に重点をおいた「セキュリティインシデントレスポンスプラットフォーム(SIRP, Security Incident Response Platforms)」、△複数の異種セキュリティソリューション運用による連携複雑性と管理負担の解消にフォーカスを合わした「セキュリティオーケストレーション及び自動化 (SOA, Security Orchestration and Automation)」、△脅威データ収集及び収集データ分析で先制的なレスポンス体系を整う「脅威インテリジェンスプラットフォーム(TIP, Threat Intelligence Platforms)」が適切に構成され、緊密に結合されなければならない。

すべてのセキュリティ技術がそうであるように、SOARの導入によってすべてのセキュリティ脅威を検知、対応するわけではない。 しかしながら、標準化したセキュリティ監視プロセスをもとに攻撃タイプ別のレスポンス要素をひとつの過程にまとめた「プレイブック(Playbook)」利用することで、セキュリティ組織は数多くのセキュリティ業務に発生する「サイロ(silo)現象」を防止し、潜んだ脅威要因をより早く探り出すことができる。これによって脅威検知からレスポンスまで至る過程を短縮することで、より高度化したセキュリティ監視体系を確立することができる。

2 SOARによる4世代セキュリティ監視 (Playbook with SOC)

#SOAR #Playbook #セキュリティ監視 #SOC(Security Operation Center) #SIRP #SOA #TIP



3 攻撃対象領域の管理による攻撃可能性の最小化

#インフラ柔軟性 #データライフサイクル #サードパーティソフトウェアのセキュリティ強化
#デジタル転換 #ゼロトラスト #デブセックオプス #セキュアコーディング

2022年には企業、組織で保有しているすべてのインフラと資産に対するセキュリティ管理案である「攻撃対象領域の管理(ASM, Attack Surface Management)」の重要性がさらに高まる見込みだ。デジタル転換が加速化することにつれ、数多くの組織のデータとインフラがオンプレミス環境からエラスティックにリソースの活用ができるクラウド環境に移動され、データ収集・保存・加工・分析及び再活用などの過程に含まれたデータ活用プロセスの効率性が一層高まってきた。

しかしこのような変化によって△インフラサイド、△データサイド、△ソフトウェアサイド、△ユーザーサイドの攻撃対象領域がさらに広がり、データ漏えい及びサプライチェーン攻撃などの攻撃も急速に増加する傾向だ。サイバー攻撃者たちは企業情報の窃取とシステム破壊を目的とする攻撃を効率的に実行しようと新規脆弱性や脅威要因について研究を持続的にし続けている。韓国~~インターネット振興院(KISA)の資料によると~~では、2021年の上半期に公開された約8,950件の脆弱性の相当がリモート接続のためのバーチャルプライベートネットワーク(VPN)とリモートデスクトップ(RDP)と関連されているなど、テレワーク環境の穴を狙う攻撃が急増している~~が分かっ~~た。また、ディープウェブ、ダークウェブを通じて取引される不法~~の~~な情報を悪用したサイバー攻撃も増える一方である状況だ。

ゆえに組織では、組織内・外部資産に基づいて脅威要因を見つけ出して、アクセスコントロール、ネットワーク分離、セキュリティ適用などの適切な対応を実施するための「攻撃対象領域の管理(ASM)」に力を入れる必要がある。

3 攻撃対象領域の管理による攻撃可能性の最小化

#インフラ柔軟性 #データライフサイクル #サードパーティソフトウェアのセキュリティ強化
#デジタル転換 #ゼロトラスト #デブセックオプス #セキュアコーディング

項目	ポイント	対策案
インフラサイド	• オンプレからマルチ/ハイブリッド、パブリック、プライベートクラウドに切り替えし、環境の柔軟性及び拡張性の強化 • モノのインターネット(IoT)及びインダストリアルIoT(IIoT)連携強化による「攻撃接点(Attack points)」の拡大	• 「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装 (マイクロセグメンテーション、ソフトウェア定義の境界(SDP)、ID認証型プロキシ(IAP) など) • 低電力機器セキュリティ強化案の確立
データサイド	• 定型データと合わせ半定型データ･非定型データ活用拡大による性能及びセキュリティ事象発生 • データライフサイクルによる収集/分析/見える化などの技術安定性の必要 • データ(個人情報･偽名情報･匿名情報)活用によるデータセキュリティ及び再識別問題発生	• 敏感な企業情報が無分別に分散される「データスプロール (Data sprawl)」現象を防止するためにデータアクセス対象者の業務権限によって認証(Authentication)及び認可(Authorization)ポリシーの強化 • データの暗･複合化適用 • プライバシー強化技術(PETs, Privacy Enhancing Technologies)適用によるデータセキュリティの強化
ソフトウェアサイド	• サードパーティソフトウェアに対するセキュリティリスクの増加 • 開発インフラ･ソフトウェア、中央管理型ソフトウェアを狙ったサプライチェーン攻撃の増加	• DevSecOpsによる開発及び運用、自動化されたセキュリティライフサイクルの確立 • セキュアコーディング、ソフトウェアテストの高度化
ユーザーサイド	• デジタル転換による技術依存度の増加、攻撃対象領域の拡大 • 自宅･分散業務及び「デジタルワークプレイス」拡散による業務支援ソリューション(テレビ会議ソリューション、リモート接続プログラム、VPNなど)のセキュリティ脆弱性をついたセキュリティ脅威の増加	• 基本セキュリティ規則遵守及びセキュリティ認識を高めるためのベネフィット/制限案を整える • ペンテスト及び脆弱性診断によるセキュリティ事象の発見や解決

<攻撃対象領域の管理(ASM)のためのポイント分析及び対策案>

4 データ経済の活性化、個人情報保護と活用のトレードオフ

#データ経済 #マイデータ #PETs #暗号化 #データライフサイクル #データ3法

データが知能化基盤産業革新の必須要素となり、データ活用規制の改善でデータ活用を極大化しようとする動きが早まっている。情報主体が自身の個人情報を自身または第三者に転送要求できる「マイデータ」事業を通じて情報主体のニーズに合した多様なカスタマイズ型マイデータサービスも発展する見込み。

このようにデータ経済時代の開化に合して、多くの組織が「データ・マネタイゼーション(Data Monetization)」力量を確保してから、データ誤用・乱用や情報流出問題に備え、安全にデータを活用できるようにする技術の重要性もさらに高まるとみられる。現在プライバシー保護モデル (K-Anonymity)、連合学習(Federated Learning)、合成データ(Synthetic Data)、プライバシー保護データマイニング(PPDM)、準同型暗号(Homomorphic Encryption)など個人を識別できる要素を非識別処理するか暗号化する技術がプライバシー保護のために主に使われている。これらの技術的要素に加え、データ活用の逆機能を最小化できる制度革新や技術投資がより積極的に行われる必要があると考えられる。

4 データ経済の活性化、個人情報保護と活用のトレードオフ

#データ経済 #マイデータ #PETs #暗号化 #データライフサイクル #データ3法

項目	プライバシー保護モデル (K-Anonymity)	連合学習 (Federated Learning)	合成データ (Synthetic Data)	プライバシー保護データマイニング (PPDM)	準同型暗号 (Homomorphic Encryption)
概念	プライバシー侵害に対する定量的な危険性を規定する方法	複数のクライアント・ひとつの中央サーバがデータでなくデータをもとに統合した(Federated)研究開発モデルを共有する方式	元のデータと似た統計的・確率的特徴を持つ任意のデータを作成する技術	個人情報が含まれたビックデータから個人情報を保護しながらデータを分析する技術	暗号化された状態でもデータ演算が可能な暗号技術
特徴	連結攻撃(Linking Attack)対応	データ分析結果だけ外部へ転送するためデータが直接に流出される可能性はない	敵対的生成ネットワーク(GAN)の理論を活用	統計処理及びマシンランニング使用	暗号化状態ですべて計算可能(チューリング安定性), 量子コンピューターを利用した攻撃にも安全(量子耐性暗号)
長所	直観的で単純	学習結果をまとめより高い正確度のモデルを導出できる	無限大にサンプル数を増やすことができる	ランダム手法で実用化可能	データを暗号化して外部へ転送可能
短所	同質性、背景知識、片寄り、類似性による再識別の可能性が存在する	モデル確立時に評価が必要	不一致によって予測正確度が落ちる可能性がある	コンピューティング環境によって多者間計算方法(SMC)技術適用時実効性が落ちる可能性がある	処理速度に限界がある

<主要プライバシー保護技術タイプ別特徴の比較>

5 セキュリティの「ひとつの指輪」人工知能 (AI for Security)

#ディープフェイク #インフォデミック(情報感染症) #サイバーテロ #データセット
#ブロックチェーン #AI倫理ガイド #XAI #AI対応セキュリティ技術

映画「ロード・オブ・ザ・リング」にでる「一つの指輪」のように両面性を内在する人工知能(AI)に対する期待と懸念は持続的に共存する見込みだ。AIは、サイバーセキュリティをはじめ、いろんな分野で幅広く活用されている。しかし悪意のある目的でAIを利用したり偏見的なデータ・アルゴリズムによる片寄った結果が出たりするなどの副作用もでている。「ディープフェイク(Deepfake)」技術を悪用したフェイクニュースを流出しAIプロセスに介入する「中毒攻撃(Poisoning)」及び「回避攻撃(Evasion)」を介して自動運転車の事故を引き起こし、人間の偏見が反映された学習データを学習したAIが人種差別的な意味を含めた結果を出す形だ。

AIの逆機能によって引き起こされる問題を解決するためには制度的、技術的、社会的の側面の支援が支えられる必要がある。このような背景から経済協力開発機構(OECD)、主要20か国(G20)首脳会議、国際電気電子学会(IEEE)、世界経済フォーラム(WEF)などを中心に「倫理的なAI開発ガイドライン」と実質的な適用基準を整える動きが加速している。人間中心価値をもとにした透明性、堅固性、安全性、責任性などAI技術の基本価値を保障できるようにするのが骨子である。

また、AI技術安全性を高めて、悪意のある誤用及びプライバシー侵害の可能性を下げるためのいろんな研究も盛んに行われている。AIベースのハッキング防止技術はもちろんAI技術を活用したセキュリティ脅威を検知する技術、自己学習及び複合認知技術に基づいたセキュリティ脅威の自律対応、暗号化された状態のデータを処理できる準同型暗号技術など複数の技術開発が行われている。さらにAIシステム開発ライフサイクルを考慮したガイドラインと標準の重要性ももっと高まる見込みである。

5 セキュリティの「ひとつの指輪」人工知能 (AI for Security)

#ディープフェイク #インフォデミック(情報感染症) #サイバーテロ #データセット
#ブロックチェーン #AI倫理ガイド #XAI #AI対応セキュリティ技術

人工知能の純機能	人工知能の逆機能
ビジネス効率性･連携性の強化 (自動化：ロボティックスプロセス自動化(RPA), デジタル転換, セキュリティオーケストレーション･自動化及びレスポンス (SOAR)など)	**ディープフェイク(Deepfake)** **インフォデミック(Infodemic)**
新成長動力による **未来の付加価値を創出**	**サイバーテロ** **(社会的･政治的に混乱を招く)**
	社会の二極化

人工知能の逆機能（マイナス側面）を補うことによる人工知能活性化策

人工知能の逆機能補完策

- 良質の人工知能データセット共有 (偏向性除去及び多様性確保)
- リアルデータ(Real Data)とフェイクデータ(Fake Data) 仕分けるための ブロックチェーン技術と融合
- 倫理的AI開発ガイドライン (韓国内･海外AI倫理基準反映)
- 説明可能な人工知能(XAI)による 人工知能ブラックボックス解消 データ暗号化技術
- AI対応セキュリティ技術の強化 (ペンテスト･防御シミュレーション、AIアンチウイルス)

＜人工知能の純機能活用と逆機能補完による人工知能活性化策＞