TXOne Networks

アニュアルレポート

OTサイバーセキュリティレポート 2022

～日・米・独の
OTセキュリティ責任者300名を
対象とした実態調査からの考察～

TXOne Networks

アニュアルレポート

OT サイバーセキュリティレポート 2022

～日・米・独の OT セキュリティ責任者 300 名を対象とした実態調査からの考察～

txOne networks

OT サイバーセキュリティレポート 2022

～日・米・独の OT セキュリティ責任者 300 名を対象とした実態調査からの考察～

目次

エグゼクティブサマリー

2022 年、多くの新しいエコシステム完結型の RaaS（Black Basta、Pandora、LockBit 3.0 など）が出現し、容赦ない多重強奪戦略を採り、重要な製造業、エネルギー、食品・農業、医療公衆衛生業界の重要分野を攻撃しています。つまり、エネルギーや重要な製造業といった産業の重要なサプライヤーに対するサイバー攻撃の頻度が高まっているのです。また、自動車関連製品メーカーへの影響は特に深刻で、製造業の区分では被害者数の約 24% を占めています。自動車メーカーが工場で自動化のトレンドを採用するにつれて、サプライチェーン攻撃を軽減するための対策は、将来的にはこれらの工場にとって死活問題となるでしょう。

企業は、ハッカーの攻撃が実稼働環境を中断させて、生産性に深刻な影響をおよぼし、復旧には数時間から数日も要するということに気づくのがあまりに遅すぎます。攻撃者は、さまざまな恐喝方法を駆使して、機密性の高いビジネス情報を盗み出すため、情報漏洩、財産の損失、顧客の信頼失墜やブランド価値低下を招く可能性があります。インダストリー 4.0 が企業の競争力の重要な局面になっていることを受けて、経営者やサイバーセキュリティのリーダーは、サイバーセキュリティ戦略の最上位に OT ネットワーク保護を優先させる必要があります。サイバーセキュリティが不十分な状態では危険が迫り、企業は極めて不都合な真実に向き合うことになりそうです。まず、ICS/OT には IT とは異なるセキュリティソリューション、スキル、プロセス、および手法が必要であることを学ばなければなりません。将来にわたって重要なインフラと産業を保護するためには、OT/ICS のセキュリティリスクの管理に、具体的なサイバー防御対策を講じる必要があります。

そこで、TXOne Networks では、この状況の深刻さに注目すべく、フロスト＆サリバン社にリサーチを委託し、製造業における OT/ICS サイバーセキュリティの現状に関するグローバル調査を実施しました。理想を言えば、このような認識をすることで、企業は増加する脅威や侵入者に対して自己防衛や反撃する態勢を整えることさえできます。この調査で得られた主な洞察は次のとおりです。

- **IT と OT の統合が進む中、IT セキュリティインシデントの 94% が、OT 環境にも影響をおよぼしている。**
- **OT の複雑さが増し、サードパーティのセキュリティ機能を可視化できないことが、企業にとって深刻なセキュリティ上の課題となっている。**
- **93% の企業が少なくとも 1 つの OT サイバーセキュリティソリューションを導入しており、85% が来年も OT セキュリティ機能の強化を計画している。**
- **OT セキュリティへの投資が増加しているにもかかわらず、70% の企業が依然として OT 環境に IT セキュリティソリューションを導入することを検討している。**
- **エンドポイント・セキュリティ・ソリューションで、Windows デバイスを 100% 保護している企業はわずか 6%。**
- **今後の OT セキュリティは、包括的で、統合されて効率よく、アクセスしやすいものでなければならない。**

TXOne Networks Inc. について

TXOne Networks Inc. は、OT ゼロトラスト手法を通じて産業用制御システムと運用制御技術環境の信頼性と安全性を確保するサイバーセキュリティソリューションを提供しています。TXOne Networks は、大手メーカーや重要インフラ事業者と協力し、サイバー防御に対する実用的で運用しやすいアプローチを開発しています。また、OT ネットワークとミッションクリティカルなデバイスを、リアルタイムかつ多層防御の手法によって安全なものとするために、ネットワークベースとエンドポイントベースの両方の製品を提供しています。

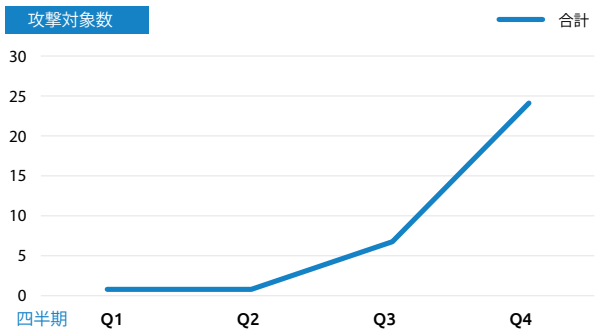
フロスト & サリバンについて

ロスト＆サリバンは、60 年以上にわたり、フォーチュン 1000 社、政府機関、投資家の持続可能な成長戦略の構築に貢献してきました。同社は、経済的な変化への対応、破壊的な技術の特定、新しいビジネスモデルの策定などに実用的な洞察を適用し、将来の成功を導く革新的で持続的、かつ管理可能な成長機会の流れを作り、実施してきました。

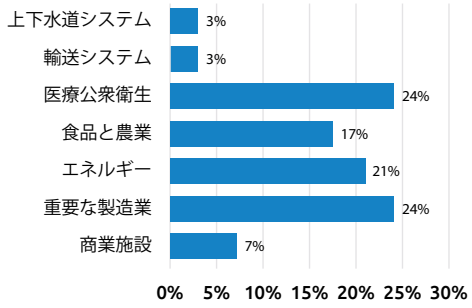
2022 年の ICS/OT サイバーインシデントに関する考察

急増が続く多重脅迫型ランサムウェア

2022 年の LOCKBIT 攻撃の事例



最も影響を受けた産業
（例 : LOCKBIT）



1. 多重脅迫モデルを採用する RaaS（Ransomware-as-a-Service）

2022 年には、完全なエコシステムを備えた多数の RaaS（Black Basta、Pandora、LockBit 3.0 など）が出現し、データの破壊、データを人質にした身代金要求、ダークウェブでのデータの販売、顧客やサプライヤーへの脅迫など、さまざまな脅迫手法を用いて、スマートマニュファクチャリング、エネルギー、食品と農業、医療公衆衛生などの業界を標的にすると予測されていました。全体として、LockBit 3.0 のリリース後、2022 年第 4 四半期に LockBit 3.0 に関連するアクティビティが増加しました。

2. 分析対策機能が付加されるランサムウェア

セキュリティを強化するために、ランサムウェアの中にはメインプログラムの解析にパスパラメータを要求するなど、ランサムウェア解析を妨げるために高度な技術を用いるものがあります（例：Egregor、LockBit 3.0 など）。このため、研究者による分析が困難になり、組織におよぼす攻撃の影響が大きくなります [1]。

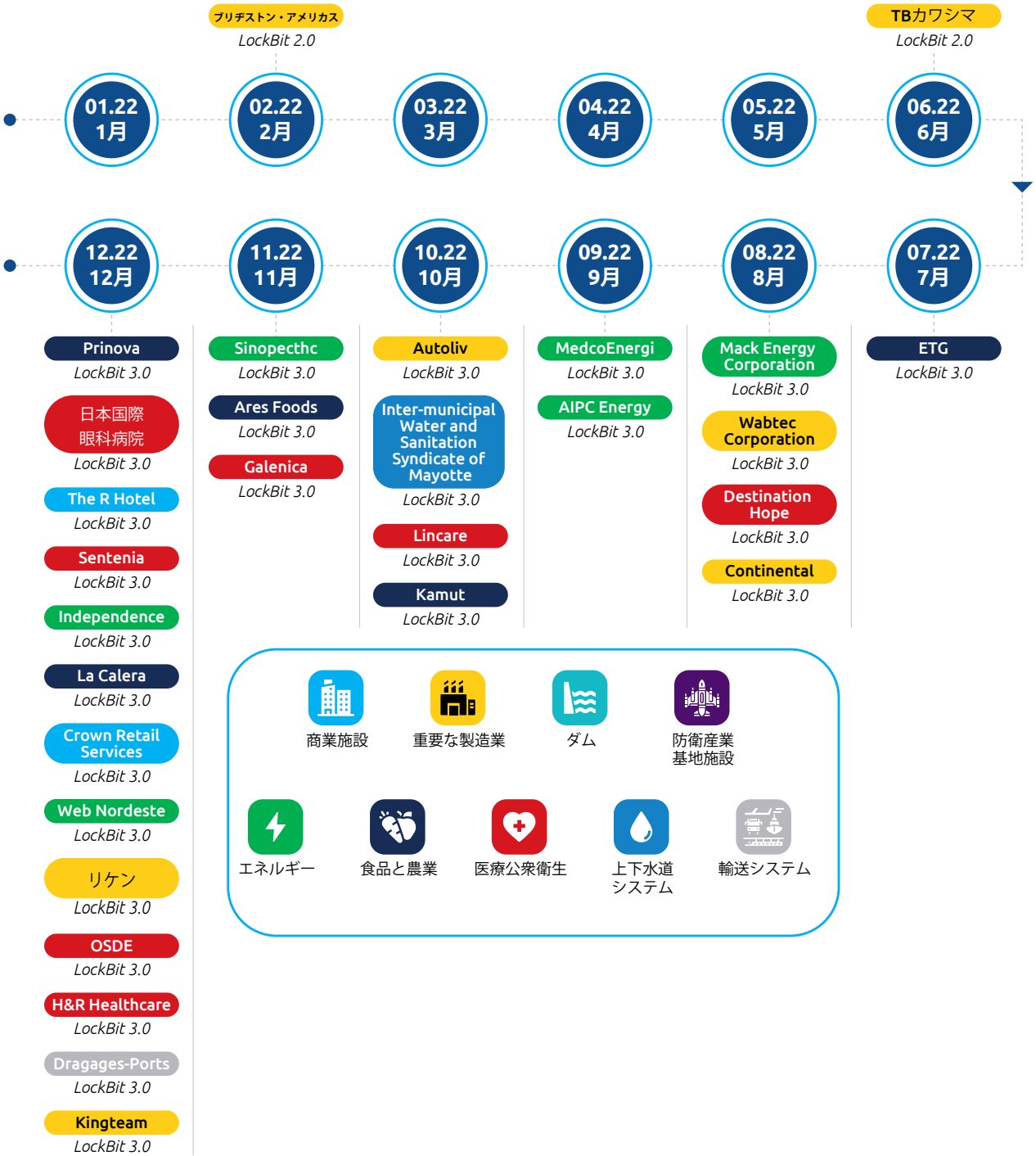
3. 高速暗号化とより優れた方法を採用するランサムウェア

ランサムウェアは、検出を回避して攻撃を防ぐために、高速暗号化方式やハードニング手法を用いています。たとえば、16 バイト単位でファイルを暗号化する断続的な暗号化技術を使用して、ファイル I/O 操作の強度を低下させ、統計分析や検出方法を回避するものもあります。また、ハッカーは、脆弱性（Log4j など）を悪用し、正規の Windows ツールや、Microsoft Defender ツールを使って、悪意のある DLL ファイルや、暗号化された Cobalt Strike ペイロードをダウンロードすることもあります。さらに、特定のサービス (ウイルス対策、バックアップ、ボリューム・シャドー・コピー・サービス、SQL など) を停止させて、ランサムウェアを埋め込むこともできます。

4. 継続的な大規模ランサムウェア攻撃を受け続ける重要なインフラストラクチャ

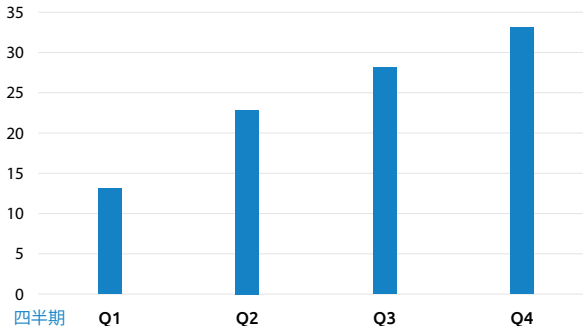
大規模なランサムウェア攻撃は、電力網、石油、ガス、水処理施設にとどまらず、今では医療や公衆衛生機関を標的にするようになっています。医療や公衆衛生業界は、ランサムウェア攻撃からの防御に警戒を怠ってはいけません[2]。

LockBit 攻撃の影響による 2022 年のサイバーセキュリティインシデント

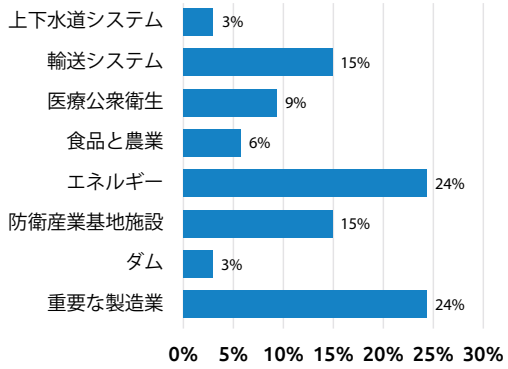


サプライチェーンで求められる徹底したリスク評価

2022 年にサプライチェーン攻撃の影響を受けた サイバーセキュリティインシデントの累積数



サプライチェーン攻撃の影響を 最も受けている産業



1. 主要産業を脅かすサプライチェーン攻撃

SolarWinds や Kaseya への攻撃に見られるように、重要な産業に対するサプライチェーン攻撃が 2022 年に急増しています。たとえば、2022 年上半期には、トヨタ自動車はプラスチック部品や電子部品のサプライヤーに対するサイバー攻撃により、14 カ所の自動車工場での生産停止を余儀なくされました。一方、シェル社（本社：英国）は、物流および貯蔵サプライヤーに対するサイバー攻撃により、石油生産に損失を被りました。これらのインシデントは、サプライチェーン攻撃が主要産業に直接影響をおよぼしていることを示しています [3]。

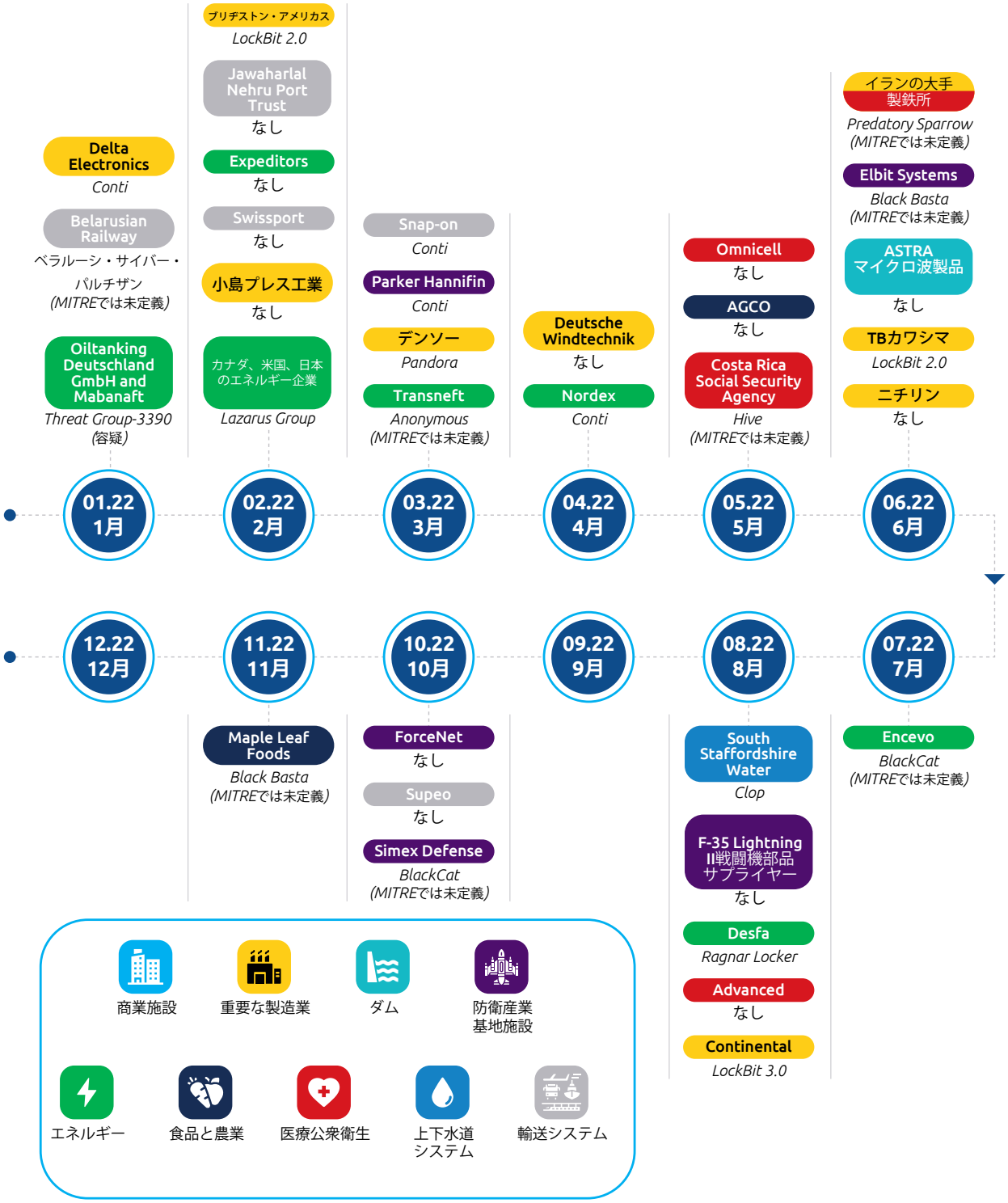
2. サプライチェーンのリスク評価に優先順位を付ける

企業がサプライ・チェーン・リスクを評価できるように、MITRE は System of Trust Framework（セキュリティリスク評価プロセスの仕組み）を開発しました。2022 年の SCS Hot Topics Summit では、サプライチェーンのリスクに対する懸念が高まっていることから、その具体的な問題を取り上げる予定です。サプライチェーン攻撃が主要産業におよぼす影響により、企業が将来的にサプライ・チェーン・リスクの包括的かつ一貫した評価を実施する必要性が浮き彫りになりました [4]。

3. 多数のサプライチェーン攻撃に直面するエネルギー産業および重要な製造業

2022 年の、主要産業のサプライヤーに対するサイバー攻撃が記録されている中で、エネルギー産業と重要な製造業が最も影響を受けていることが判明しました。重要な製造業は全体の 24% を占めています。その中でも、自動車産業が過半数を占めています。自動車産業における自動化生産の台頭に伴い、サプライチェーン攻撃を軽減するための対策が自動車工場にとって重要な焦点になることがわかりました。

2022 年にサプライチェーン攻撃の影響を受けた サイバーセキュリティインシデント



重要なインフラ資産への攻撃は継続

近年、重要なインフラがさまざまな悪意のある犯罪者の標的になっており、サイバーセキュリティは国家安全保障上の問題となっています。重要なインフラの企業（電力会社、水処理プラント、石油ガス輸送会社、病院など）は、インシデントが発生した場合、金目当てや市民不安を意図した集団から容赦なく攻撃されるため、継続的なセキュリティリスクと高いコストに直面しています。最近の例としては、ウクライナの送電網に対する攻撃により、数十万人が停電の被害に遭ったこと、ドイツのデュッセルドルフ大学病院に対する攻撃により、病院が緊急処置室を閉鎖せざるをえなくなり、他の病院への移送の段階で患者が死亡したことなどが挙げられます。ランサムウェア攻撃によってコロニアルパイプライン社のパイプラインシステムが停止したことで、航空会社のジェット燃料不足、商業用燃料不足、ガソリンスタンドの燃料価格高騰が発生しました。2023 年には、エネルギー不足、地政学的緊張、攻撃技術の進歩が相まって、特に米国とその同盟国との間で、重要なインフラへの攻撃が増加すると見られています。そこで各国政府は、次に挙げる現実に立ち向かわなければなりません。

1. 重要インフラに対するサイバー攻撃ではエネルギー産業が主要な標的に

2022 年の世界の重要インフラ攻撃を分析すると、エネルギー産業が全インシデントの 31% を占め、最も標的とされた業界になっています。これは、電力網や風力発電所の運用制御技術（OT）システムと情報技術（IT）システムの接続性が向上して、攻撃者がこれらのシステムにアクセスして制御できるようになっていることが原因です。この業界は新たなセキュリティ上の課題に直面しており、新たな脅威が急速に拡大することに懸念が高まっています。

2022 年後半で見てみると、重要なインフラ産業では ICS/OT 環境に密接に関連する業界の中で、既知のランサムウェア攻撃の件数が最も多くなっています。たとえば、8 月には、ランサムウェアグループ「Clop」が、英国の上水道供給会社に侵入し、産業用制御システムの内部ネットワークにアクセスして水の流れを妨げたことを、水道施設の HMI 画面を公開することにより証拠として示しました。さらに、Sekoia.io[5] は、Conti、LockBit、Hive が公共事業サービスへの攻撃で最も頻繁に目にする RaaS で、Conti と LockBit でそれぞれ攻撃全体の 3 分の 1 を占めていると伝えています。

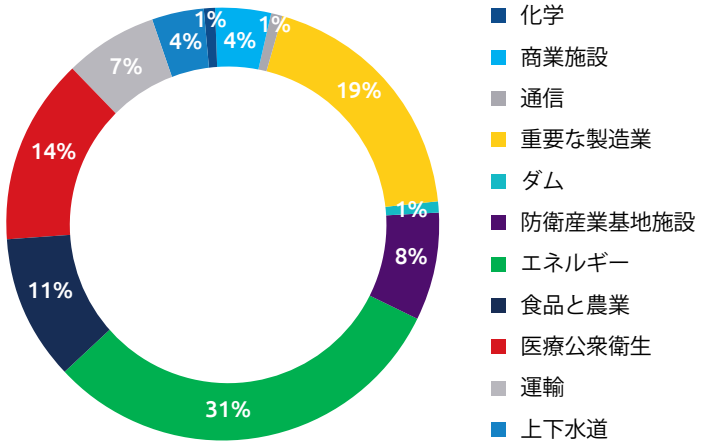
- ***Conti:*** フィッシングメール送信や RDP 認証情報の窃取が、一般的な初期の侵入方法です。2022 年 1 月時点で、Conti は 1,000 社以上の企業体を攻撃して、1 億 5000 万ドル以上の身代金を受け取っており、最も金銭的な損害を与えたランサムウェアファミリーの 1 つとなっています。特に、Conti は標的に対して攻撃的に振る舞うことが観察されており、身代金の支払いを受け取ったとしても、その後データを漏洩する可能性があります [6]。

- ***LockBit:*** 2022 年、LockBit は攻撃件数が大幅に増加し、7 月には被害者のデータ漏洩情報が無料で検索可能になったと発表しました。LockBit 3.0 は、メインプログラ

ムを解析するためにパスパラメータが必要であり分析が困難なことが、セキュリティ研究者にとって悩みの種となっています。分析が困難な環境を構築することで、被害者企業が LockBit への対策に手を焼いている間に、攻撃が与える影響は大きくなってしまいます。

- ***Hive:*** HIVE は主にエネルギー、医療、金融業界を対象としています。Conti と同様に、Hive はフィッシングメール送信や RDP 認証情報の窃取を、初期の攻撃手法として使用することがよくあります。7 月、Hive はコードを GoLang から Rust にアップグレードし、アナリストがリバースエンジニアリングを行うのが比較的困難になりました。2022 年 11 月の時点で、Hive は 1,300 を超える被害者企業からおよそ 1 億ドルの身代金を受け取っています [7]。

2022 年の重要なインフラでのサイバーインシデントの分析



2. 地政学的な対立が重要インフラのセキュリティリスクをエスカレート

まだ全面戦争には至っていませんが、技術戦争の始まりは着実に近づいており、過激なハッカーたちは、すでにそのスキルを駆使して国家の安定と一般市民の日常生活を脅かしています。エネルギー、運輸、通信などの国家インフラは極めて重要であるため、侵害に成功すれば、一国にとって深刻な事態を招くことになりかねません。そのため、重要なインフラは、国家が支援する攻撃者や政治的な動機を持つ攻撃者にとって格好の標的となっています。たとえば、北朝鮮が支援する APT（Advanced Persistent Threat: 持続的標的型攻撃）組織である Lazarus は、カナダ、米国、日本のエネルギー企業を狙い続けています。標的のコンピュータを C&C サーバーに接続するだけでなく、標的のエンドポイントの Active Directory 情報から adfind.exe ツールを取得して、ラテラルムーブメント（横方向の移動）が実行できそうなエンドポイントを特定しようとします。ロシアの APT 組織「Sandworm」は、電力供給システムベースのインフラを標的にしたマルウェア「Industroyer2」を使用し

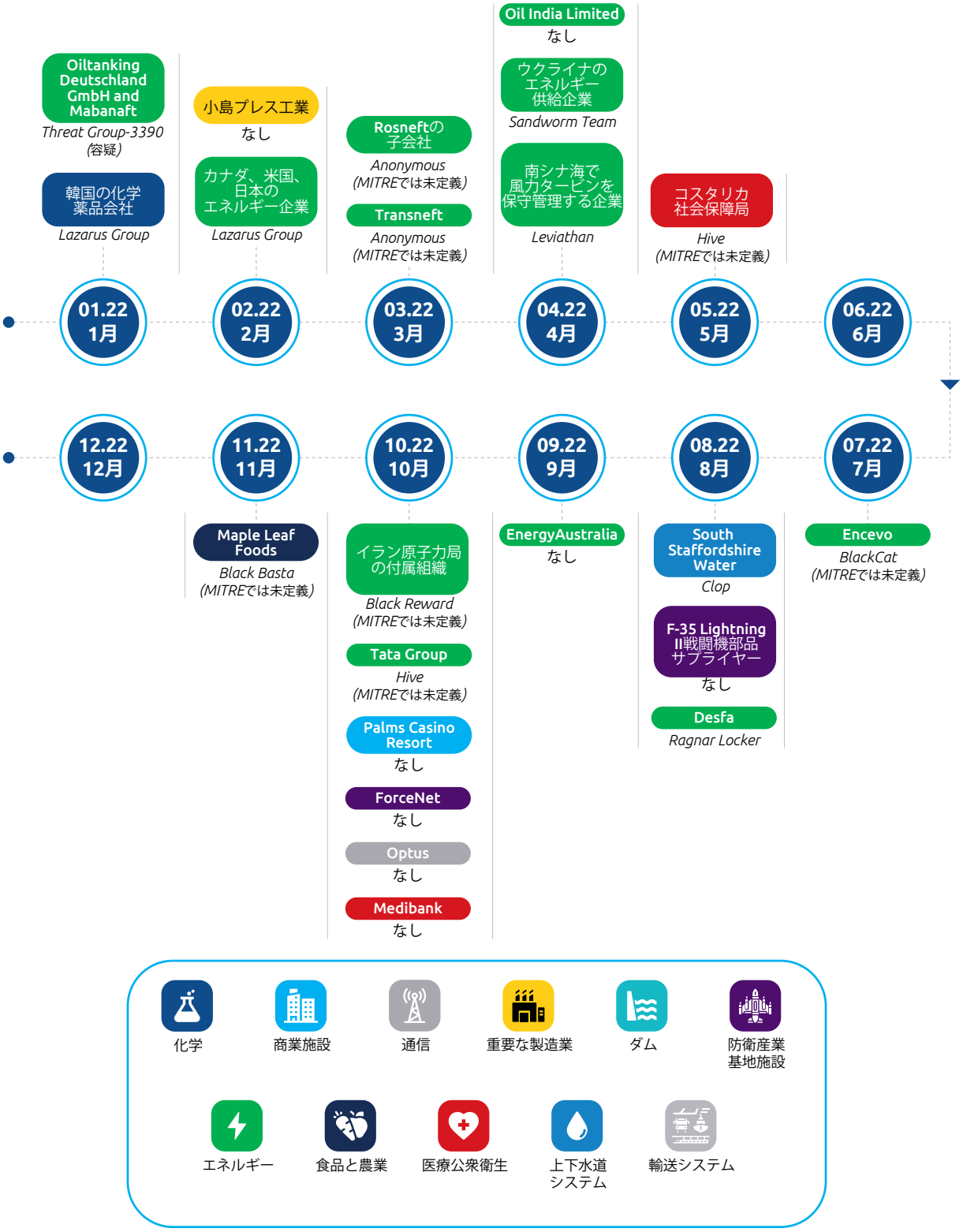
て、ウクライナの複数の変電所を攻撃しようとしました。また、ディスク消去ツールを使用して、エネルギー企業の Windows、Linux、Solaris サーバーにダメージを加え、被害者による電力復旧を困難にしました。さらに、親ロシア派の攻撃グループ「Killnet」は米国の主要空港に対して DDoS 攻撃を仕掛け、アトランタ、シカゴ、ロサンゼルス、ニューヨーク、フェニックス、セントルイスの空港でネットワークをクラッシュさせました。

欧州ネットワーク・情報セキュリティ機関（ENISA）によると、ロシア・ウクライナ紛争により過激なハッキングアクティビティが活発になり、支援国 42 カ国 128 政府行政機関が、国家が支援するハッカーグループの餌食になっています。紛争が始まるとすぐに、ハッカーグループはこの機会に立ち上がり、混乱を招く活動を重ねました。このことから、ハッキングが国家や政府全体に対して、どれほどすばやく武器として使用されるかが理解できます。中国、イラン、北朝鮮などの国々もスパイ活動を増加させており、国家ハッカー集団は東南アジア、日本、オーストラリアなどの国々を標的にしています。アジアで地政学的緊張が続く中、これらの国家ハッカー集団は、チェコ共和国やポーランドなど EU 加盟国を含む台湾と密接な関係を持つ国々を標的にしています。このような攻撃は、ゼロデイ脆弱性を悪用したり、重要なインフラにフォーカスした OT ネットワークを標的にしたりすることがよくあります。ソーシャルエンジニアリング、偽情報、データの脅威も、国家ハッカーが用いる一般的な攻撃手法です。

3. 公共サービス産業の相互依存性とサプライヤーに対する APT やランサムウェア攻撃の脅威

重要なインフラの産業は相互に関連していることが多く、石炭採掘と輸送システムはエネルギー産業と輸送産業の相互依存の例として挙げられます。図中の緑色の記号は、重要なインフラサプライヤーを示しています。サプライヤーがサイバー攻撃を受けた場合、付随する業界は安定した公共インフラサービスを提供できない可能性があります。2022 年 1 月、ドイツの石油貯蔵会社 Oiltanking がサイバー攻撃を受け、トラックへのサービス提供ができなくなり、シェルが本件の被害者となりました。この件では、シェルのような企業の燃料供給が途絶えた場合、国家経済に影響をおよぼす可能性があることが浮き彫りになりました。また同年 10 月には、Supeo 社（本社：デンマーク）がランサムウェアに襲われ、デンマークの鉄道運転手は重要な運行情報にアクセスできなくなり、列車の運行が数時間にわたって中断されました。これらのインシデントで、重要なインフラに対するサプライチェーン攻撃の重大な影響と、包括的なリスク評価の重要性が浮き彫りになりました。

2022 年に標的となった重要なインフラストラクチャ



OT セキュリティ市場の原動力

OT/ICS サイバーセキュリティの脅威が絶えず高まっている中、その根本的原因を理解しておく必要があります。本章では、a) 技術的、法的、経済的な観点から OT セキュリティの重要性を探り、b) 急速に拡大する世界的な OT 脅威に対する政府や企業の対応を見ていきます。

集約される IT システムと OT システム

物理的な機器や、デバイスをデジタル領域に統合することを目的とした IT/OT コンバージェンス（集約）の概念は、新しいものではありません。しかし、業界で大きな支持を得られるようになったのは最近になってからのことです。IoT Analytics による 2019 年のレポートには、工場内の産業資産の約 50% が、2020 年からローカルまたはリモートのデータ収集システムに接続されるだろうと書かれています [8]。 この予測は、COVID-19 パンデミック（新型コロナウイルスの大規模感染）によってさらに加速され、壊滅的な事態に直面した際の企業レジリエンスを高めるインダストリアル IoT（IIoT）の重要性を浮き彫りにしています。製造業においては、「インダストリアル IoT」とも呼ばれる「インダストリー 4.0」が、ダウンタイムの短縮、新たなビジネスモデルの開発、カスタマーエクスペリエンスの向上のための主な原動力と見られています。

IT/OT コンバージェンスのキラーアプリケーション

通常、業界で成功するデジタルトランスフォーメーションは、キーとなる応用事例を見極めて、工場で小規模に実装することから始めます。データが共有され、IT システムのインテリジェンスが OT システムの物理資産に適用されることで、新たな効率性の達成、運用の合理化、イノベーションの促進、新しいサービスの導入が実現します。一般的な OT デバイスには、センサー、プログラマブル・ロジック・コントローラ（PLC）、分散制御システム（DCS）、コンピュータ数値制御（CNC）システム、ビル・オートメーション・システム（BAS）、監視制御とデータ収集（SCADA）システムなどがあります。これらのデバイスは、標準化されたネットワークプロトコルを使用してワイヤレス通信を行い、各物理システムから中央サーバーに関連データを送信して監視や分析を行います。この分析結果は物理システムに戻すことができるため、次のような IT/OT コンバージェンスアプリケーションが実現します [9]。

- **エネルギー業界：**電力、石油、ガスなどの業界において、IT および OT チームが運用データにリモートでアクセスし、産業用制御機器の予防保全の最適化、損害評価の実施、在庫監視、エネルギー配給の最適化などが行えるようになります。
- **製造業：**IT チームと OT チームは、自動化生産のために自動化した資材転送システムやロボットアームを使用し、リアルタイムで生産プロセスを調整し、生産効率を向上させ、製造コストと廃棄材を削減することができます。たとえば、データ分析を用いて、電力コストの削減や、余剰な在庫を削減することが可能です。
- **運輸業界：**IT と OT を統合することで、鉄道、バス、配送などの輸送機関は、資産の調整、状態、使用状況をより深く理解でき、資産のリプレースと安全のための短期メ

ンテナンス、ルートの最適化、長期計画を進めることに役立ちます。

- **製薬業界：**IT と OT の統合により、より多くの医療機器が生理学的パラメータを検出できる製品を評価できるようになり、健康状態や生理学的状態に関する考察が得られます。データ分析システムを使用すると、医薬品製造の強化や製品品質の確保、または医療サービスとの連携により、疾病発生率の予測とともに、より優れた患者分析と効果が見込めます。
- **小売業：**棚センサー、商品ラベル、IP カメラ、POS 機器などの OT デバイスを使用することで、より多くのデータを IT 部門に提供して分析できるようになりました。買い物客の体験を向上させながら、在庫と販売現場の最適化、コストの削減、収益の拡大を実現できます。

新しい IT/OT 集約型企業

プロセスのこのフェーズでは、IT チームと OT チーム間のコミュニケーションとコラボレーションを促進することにフォーカスしており、企業全体の成功には不可欠です。IIoT を成功させる企業を起ち上げるには、企業構造や、コラボレーションの種類、ジョブプロファイル、さらに仕事の役割を変更する必要もあります。その結果、特に IT と OT の融合に伴って、新しい働き方と新しい能力セットが必要になります。これを実現するために、次のフレームワークが必要になります。

- **共通のガバナンスモデル**
- **IT と OT にまたがる整合性のあるプロセス**
- **データとセキュリティの一元管理**

確実に成功するためには、IT と OT はそれぞれのプロセスを改革して相互に順応し、効果的なコミュニケーションチャネルを持つようにしなければなりません。企業には IT データの保存や保護に特定のプロセスがあるかもしれませんが、これらのプロセスは集約型 OT システムに適応または拡張させる必要があるかもしれません。

新たな IIoT 技術が生み出す未曾有の脆弱性

新しいインダストリアル IoT アーキテクチャが勢いを増すにつれて、従来の集中型 SCADA や MES システムの通信方式は変化しています。たとえば、多くのセンサーが今では LoRaWAN、SigFox、NB-IoT などの IoT プロトコルを使用して、産業用センサーを直接クラウドに接続するようになっています。さらに、産業用コンピュータのメーカーは、ソフトウェア・アプリケーション・プラットフォームを介してデバイスをクラウドに接続できるエッジサーバーへの対応を進めています。たとえば、Advantech の ADAM-3600 RTU は、Azure クラウドに接続できます [10]。中小規模の工場では、Linux ベースの HMI やゲートウェイなどのオープンソースの機器や通信プロトコルを積極的に使用し、OPC-UA プロトコルに対応するサーバーを徐々に採用しているところもあります。ただし、このような傾向はハッカーの攻撃対象領域を広げることにもなります。

OT サイバーセキュリティの課題への対応

OT/ICS ネットワークアーキテクチャでは、機密性よりも可用性が最優先事項であり、ほとんどの意思決定プロセスにおいては、生産性第一で検討されます。そのため、OT/ICS のネットワークアーキテクチャはサイバーセキュリティ防御機能を念頭に置いて設計されることはほとんどなく、フラット化される傾向にあります。このため、OT/ICS のサイバーセキュリティには、次のような共通の課題が生じます。

- **不完全なサイバーセキュリティアーキテクチャ：**これまでは、OT/ICS の防御は「完全隔離」(エアギャップ) にもっぱら依存していました。このような前提により、サイバーセキュリティ対策の計画と導入が不完全になりました。たとえば、OT/ICS のネットワークアーキテクチャでは、地域管理のサイバーセキュリティや、詳細な階層的隔離さえ考慮されていません。

- **内部 / サプライチェーンの脅威：**管理ポリシーが緩いエアギャップ環境にモバイルデバイスを持ち込むと、悪意のあるプログラムが OT/ICS 環境に損害を与えたり、機密データを盗み出したりする可能性があります。データ転送用の USB メモリーや修理を待つノートパソコン、あるいはサプライヤーが工場に持ち込んだデバイスさえも、マルウェアを拡散する感染源になる可能性があります。

- **複雑な OT 通信プロトコル：**さまざまな業界で、職場では特別な OT/ICS ネットワークアーキテクチャと通信プロトコルが使用されており、要件が異なるため大きな違いがあります。さらに、多くの産業用制御通信プロトコルは暗号化されていないため、ハッカーが工場のオペレーションを操作して、生産を妨害することが容易に行えます。

- **レガシー・オペレーティング・システム：**一般には、重要な操作を実行したり、生産ラインの決定に基づいて操作したりするレガシーな OT/ICS エンドポイントが環境内に多数存在しています。そのため、OT/ICS のエンドポイントは、OT/ICS サイバーセキュリティの中で Weakest link（最も弱いリンク) となります。同時に、古いシステムを実行している重要な資産のソフトウェアとファームウェアは更新されず、新たに発見された脆弱性にはパッチが適用されません。このため、Windows XP や Windows 7 のシステムはすべて脆弱な標的になります。

- **OT 環境には適さない IT サイバーセキュリティソリューション：**半導体装置業界では、エンドポイントには特別な保証や規制に制約を受けており、追加のアプリケーションをインストールすると保証が無効になったり、規制に違反したりすることになります。さらに、製薬業界にもそのような資産が多数存在します。装置自体のシステム設計に制約があるため、ウイルス対策ソフトウェアをインストールできず、そのようなシステムを維持して保護できる特別なソリューションが必要となります。

サイバーセキュリティに対する政府規制の新たな焦点

今日、世界中の国々では絶えず独自のデジタルインフラと産業が進展しています。情報通信技術の普及により、生活のあらゆる面がかつてないほど相互に結びつき、統合されています。従来のネットワーク境界の多くが消滅し、ネットワークの脅威は政府、重要なインフラ、および民間企業にとって直接的な脅威となっています。近年のサイバーセキュリティインシデントを振り返ってみると、ネットワーク攻撃が人々の生活に直接影響をおよぼすケースが増えていることは明らかです。Stuxnet、WannaCry、SolarWinds、コロニアルパイプライン社、さらにウクライナ戦争の初期段階でのロシアによる米国の衛星企業 Viasat 社へのサイバー攻撃 [11] など、世界的な影響力を持つこれらの有名なネットワーク攻撃が注意喚起となりました。これらの事件が契機となり、ハッカーが都市の電力や水の供給を脅かしたり、機密性の高い企業データや個人データを盗んだりすることを防ぐために、政府はサイバーセキュリティの規制やポリシーを再検討するようになりました。

米国の OT サイバーセキュリティポリシーと規制

米国大統領令 14028 号「国家のサイバーセキュリティの強化」で OT サイバーセキュリティの重要性が明確に

近年、米国では、重要なインフラに対する一連のサイバー攻撃が発生しています。たとえば、コロニアルパイプライン社へのランサムウェア攻撃では、攻撃によって東海岸の燃料供給のほぼ半分が失われ、経済に対するサイバー攻撃の潜在的な影響が一気に取り沙汰されるようになりました。さらに、フロリダ州オールズマーでは、水処理インフラへの危険な攻撃（未遂）がありました。これは身元不明のハッカーが町の水処理システムの水酸化ナトリウム濃度を増加させるという、コミックに出てくるような悪役の手口でしたが、辛うじて事前に回避することができました。事態の深刻さを認識したバイデン大統領は、2021 年 5 月 12 日、大統領令 14028 号「国家のサイバーセキュリティの強化」に署名しました。この大統領令は、国家のサイバーセキュリティを近代化させることで、さらなる攻撃から重要なインフラを保護することを目的としており、保護とセキュリティの範囲には、データを処理するシステム（情報技術（IT））と、私たちの安全を維持するために不可欠なオペレーション（運用制御技術（OT））が含まれなければならないことを初めて明示したものです。2022 年 3 月、バイデン大統領は CIRCIA（重要インフラに関するサイバーインシデント報告法）にも署名し、法制化しました [12]。CIRCIA では、重要なインフラ業界で事業を展開している企業に対して、サイバーインシデント発生から 72 時間以内、および身代金の支払いから 24 時間以内の報告を義務付けるなど、法的保護とガイドが示されています。

重要インフラの ICS/OT がサイバーセキュリティの焦点に

2021 年 7 月 28 日、バイデン大統領は重要インフラ制御システムのサイバーセキュリティの強化に関する国家安全保障の覚書に署名しました [13]。この国家安全保障の覚書（NSM）は、関係者が重要な ICS/OT システムに対するサイバー脅威を理解し、最低限のサイバーセキュリティ基準を採用できるよう、連邦政府と重要インフラコミュニティ間の協力を促進するための自発的な取り組みを策定しています。たとえば、2022 年に運輸保安局（TSA）がパイプラインと鉄道業界のサイバーセキュリティのレジリエンスを強化するために実施した複数のパフォーマンスベースの指令や、2022 年に航空業界のサイバーニーズに対応する措置の導入などが挙げられます。同時に、サイバーセキュリティの達成目標も発表され、主要なサイバーセキュリティの投資結果を理解するのに役立っています。

新たなデジタルインフラに対応したセキュリティを事前に考える

米国政府は、米国のスマートで安全なインフラ確保に向けて、米国のインフラの近代化におけるサイバーセキュリティ投資を強化するために、超党派のインフラストラクチャ法を可決しました。近代化の一例として、全米の電気自動車充電ステーションネットワークを拡張し、耐久性を持たせて、ネットワーク保護の強化など、最新の安全およびセキュリティ基準を満たすことが挙げられます。さらに、この法案は、国内のサービスの行き届いていない地域に高速インターネットを提供して、デジタルデバイドを解消することも定めています。そのために、特に全米の州（State）、地方（Local）、準州（Territorial）（SLT）の政府を対象とした初のサイバーセキュリティ助成プログラムを導入し、州および地方のサイバーセキュリティに 4 年間の助成プログラムを提供し、デジタルセキュリティへの投資を確実に実施するために、SLT パートナーに 10 億ドルの資金を割り当てました [14]。

米国のOTサイバーセキュリティの概要

現在進行中の規制の適用は、大半のメーカーが重要なインフラの基準を満たしているため、全米のメーカーが対象になります

現状

- 北米は最大のOTサイバーセキュリティ市場であり、2019年には市場の39.7%を占めています。米国は、この地域で最大の市場となっており、OTサイバーセキュリティ技術の採用を含み、サイバーセキュリティに対する意識が最も成熟した市場の1つです。
- 米国の製造業界には、包括的で義務的なサイバーセキュリティ規制はありませんが、多くの製造業者は、厳しく規制されている重要なインフラの基準を満たしています。
- 製造業のサイバーセキュリティ全般は**NIST**に準拠しています。米国では、大統領令13636号によって、**重要なインフラのサイバーセキュリティを強化するためのNISTフレームワーク（2018年）**に導かれます。また、インターネットに接続されたスマートデバイスを保護するための上院法案327号（カリフォルニア州）など、州固有の法律も存在します。

展望

- 米国政府は、ITおよびOTセキュリティに関する規制の整備を積極的に行ってきました。極めて公共への影響が大きいセキュリティ攻撃（コロニアルパイプライン攻撃など）では、サイバーセキュリティ保護の必要性が浮き彫りになりました。
- そこで2021年5月、大統領令14028号が発令されました。この中にはホワイトペーパー『消費者向けIoTデバイスのベースラインセキュリティ基準』があり、安全なソフトウェアとIoTデバイスのサプライチェーンを確保するために、NISTを含む複数の機関に義務付けているサイバーセキュリティの強化を目的としています。
- 2022年3月には、「重要インフラに関するサイバーインシデント報告法令(CIRCIA)」が署名され法制化されました。これにより、ITとOTの両方のセキュリティにおいて、規制の整備が進み、いくつかの業界に影響をおよぼすことになると思われます。

EU の OT サイバーセキュリティポリシーと規制

EU NIS 2.0 でサイバー攻撃防御用の対応コマンドセンターを設立

EU のサイバーセキュリティ管理規制の法制化における画期的な瞬間とは、2016 年に「ネットワークおよび情報システムセキュリティ指令」が公式に発表され、実施されたときです。正式名称は「Security of Network and Information Systems（ネットワークおよび情報システムのセキュリティ）」で、略して NIS Directive（NIS 指令）と呼ばれています。2020 年末までに、ますます深刻化するサイバー脅威に対応して、欧州委員会（EC）は、修正案 NIS 2 指令を提案し、現在および将来のニーズに沿うように NIS 指令を更新することを求めました。また、ポストコロナ時代や 5G 時代のサイバーセキュリティの状況にも沿った内容になっています。このアップグレードでカバーされる対象のほとんどは、エネルギーシステム、医療ネットワーク、運輸サービスなどの重要インフラです [15]。

EU のネットワークおよび情報システムセキュリティ指令の新旧バージョンを比較してみると、新バージョン（NIS 2.0）では規制対象範囲が拡大され、地域冷暖房施設、水素エネルギー関連機関、政府行政部門などの 11 の管理機関が追加されていることがわかりました。さらに、NIS 2.0 では、大規模なサイバー攻撃の監視と対応において EU 諸国を支援するために、EU-CyCLONe と呼ばれる対応センターを設置しました。EU 加

盟国は、21 カ月以内に、これらの新しい規則を自国の法律に組み込むことになります。

2022 年 2 月、ベルギーとオランダのいくつかの大規模製油所がサイバー攻撃を受けました[16]。ハッカーは、石油貯蔵所の自動積み下ろしプロセスを麻痺させ、原油製品の積み下ろしを待っている船を操作不能にし、地域全体の石油製品の取引を妨害しました。このように、規制を進化させても、サイバー攻撃の脅威は常に存在しているため、常に警戒が必要となります。

EU サイバーレジリエンス法は設計による製品セキュリティを促進

2022 年 9 月 15 日、欧州委員会（EC）は、EU のデジタル製品のサイバーセキュリティを強化し、既存の規制枠組みを合理化するために、サイバーレジリエンス法（CRA: Cyber Resilience Act）を提案しました[17]。CRA は、ソフトウェアを含むデジタル製品に多くのサイバーセキュリティ上の義務を課しており、NIS 2 指令、人工知能法、一般データ保護規則（GDPR: General Data Protection Regulation）など他の EU 規制と密接に関連しています。これは、EU のサイバーセキュリティ法の中でも最も重要なものの 1 つとなる可能性があります。

CRA は、他のデバイスやネットワークに直接、間接的を問わず接続されているあらゆるデジタル製品に適用されます。デジタル製品とは、「市場に個別に販売されているソフトウェアやハードウェアコンポーネントを含む、ソフトウェアまたはハードウェア製品およびそのリモートデータ処理ソリューション」と定義されています。インターネットに接続された製品は、設計、開発、製造、リスクベースのサイバーセキュリティ、悪用可能な既知の脆弱性がないことなど、基本的なサイバーセキュリティの要件に準拠しなければなりません。CRA の付録 I に記載されている製造業者のサイバーセキュリティ要件および義務に違反した企業は、1,500 万ユーロまたは前年度の全世界の年間売上高の 2.5% のいずれか高い方の罰金を科される可能性があり、無分別または怠慢によるサイバーハイジーンに具体的な責任が示されています。

ドイツのOTサイバーセキュリティの概要

ドイツは、競争力を維持するために高度なOTサイバーセキュリティソリューションが必要となる有数の産業拠点です

現状

- ヨーロッパの企業は、製造プロセスを強化するためにOTとIoTを活用しています。ドイツは産業と製造の有数の拠点であるため、企業は最先端のOTサイバーセキュリティソリューションとサービスを求めています。これには、OTとITの統合も含まれています。
- ドイツ政府は産業界に対するサイバー攻撃のリスクを認識しています。**産業戦略2030（The Industrial Strategy 2030）**では、サイバーセキュリティの向上を柱に掲げています。政府はまた、**サイバーセキュリティ戦略2021-2025（Cybersecurity Strategy 2021-2025）**を採択し、OTを含むサイバーセキュリティ全体を向上させています。
- ベンダーにとって、EUは特にプライバシーとデータ規制に関しては、厳しく規制された市場です。このため、この地域のベンダーには固有の優位性が生まれています。

展望

- 昨年11月、EUはNIS2指令を採択しました。ここではサイバーセキュリティリスク管理対策のベースラインが設定されています。加盟国は、2024年9月までにNIS2を各国国内法に移行しなければなりません。
- OTはNIS2で特段取り上げられていませんが、**CER指令**とともに、OTセキュリティはNIS2の範囲に含まれます。この指令は、サイバー攻撃（NIS2）から物理的な攻撃や自然災害（CER）に至るまで、現在および将来のオンラインおよびオンラインのリスクに対応しています。CERは、重要な事業体に対して、デジタルではなく、物理的なレジリエンス対策に重点を置いています。
- まだ法制化されていませんが、提案されている**EU CRA**は、ハードウェアとソフトウェアの両方にわたりデジタル要素を備えた製品の製造者と開発者に対して、共通のサイバーセキュリティルールの導入を行うものです。このルールは、これらの製品の製造業者、輸入業者、および販売業者のライフサイクル全体に適用されます。また、製造業者に対する脆弱性およびインシデントの処理の要件と事業者に対する義務も規定される予定です。

日本の OT サイバーセキュリティポリシーと規制

日本政府は、世界の他の国々と同様に、国家安全保障戦略において、重要なインフラや産業用制御システムの保護に改めて重点を置いています。2022 年 12 月 14 日、政府はこの戦略の新版を正式に発表しましたが、特に重要インフラにおいて国家サイバー空間の安全かつ安定的な利用を確保するために、サイバーセキュリティ分野における対応能力を向上させる必要性を強調しています。この戦略は、日本のサイバーセキュリティ対応能力を先進国以上に引き上げることを目的としています。戦略に示されている具体的な対策は次のとおりです [18]。

- 政府機関の情報システムのセキュリティを継続的に評価する仕組みの構築、最新のサイバー脅威に基づく対応の強化、政府機関の情報システムの脆弱性の継続的な管理
- 政府の国家安全保障上の懸念や重大な武力攻撃となりうる深刻なサイバー攻撃を回避するための、「積極的サイバー防御」の導入
- サイバーセキュリティ分野における情報収集や分析能力の一層の強化や、官民情報共有の推進、攻撃対象デバイスの検知、ネットワーク対策の開始など、積極的ネットワーク防御システムの構築
- 内閣サイバーセキュリティセンター（NISC）を新たな機関に再編し、サイバーセキュリティの分野でのポリシーをまとめる
- 同盟国などと連携し、情報の収集や分析、帰属、公表を強化し、国際的な枠組みやルールを整備する。このため、日本の経済産業省と米国国土安全保障省（DHS: Department of Homeland Security）はサイバーセキュリティ協力について基本合意契約を締結し、この産業用制御システムのセキュリティが 4 大協力プロジェクトの 1 つになることを示す

このような取り組みに加えて、日本政府は国際協力事業としてスマート・インダストリアル・セーフティの推進にも力を入れています。経済産業省は、2017 年 12 月に「産業サイバーセキュリティ研究会」を設立し、日本の産業界がサイバーセキュリティ分野で直面している課題を特定し、関連する政策を推進しています。また、同省は産業ベースのサイバーセキュリティポリシーを議論するためのワーキンググループも設立し、ビルシステムやプラントシステムのサイバー・フィジカル・セキュリティ対策のガイドラインを発表しました。

さらに経済産業省は、インドネシアやタイなどの諸外国と協力して、スマート・インダストリアル・セーフティ政策を策定しています。2022 年 1 月 25 日、経済産業省とインドネシア共和国工業省は「スマート協力の強化」に関する協力覚書（MOC）に署名 [19] し、同年 9 月 28 日には、経済産業省とタイ工業省（MOI）は、スマート・インダストリアル・セーフティの協力促進に関する協力覚書（MOC）に署名 [20] しました。

日本のOTサイバーセキュリティの概要

日本はアジア太平洋地域におけるOTサイバーセキュリティ市場をリードしており、
規制が進展することでさらに成長すると思われます

現状

- アジア太平洋地域は、最も急速に成長している地域であり、日本と中国がOTサイバーセキュリティ市場をリードしています。
- NICTによると、IoTデバイスに対するサイバー攻撃の数は大幅に増加しています。このため、政府は新しい法律、戦略、施設を作ることになりました。
- **Society5.0**は、サイバー空間と物理空間を高度に統合して実現する国家政策です。**コネクテッドインダストリーズ**は、さまざまなモノ、産業、人をつなぎ、新たな付加価値を創造するもう1つの国家政策です。
- 経済産業省は、**サイバー・フィジカル・セキュリティ対策フレームワーク2019（CPSF）**を通じて、新しいサプライチェーンにおけるセキュリティ確保を目指しています。ここには産業社会におけるセキュリティ対策の概要が示されています。

展望

- 脅威の状況が変化している中、日本はITとOTのセキュリティ環境を絶えず強化しようとしています。
- 日本は、サイバーセキュリティの優先事項を運用する二国間協力を求めています。米国の国土安全保障省との協定は、両政府が直面するサイバー脅威を抑制するための強化と協力が目的です。
- 2021年7月、日本政府は今後3年間の新しいサイバーセキュリティ戦略を発表しました。この抑止力の強化は、サイバー攻撃に中国政府とロシア政府の関与が疑われたことに端を発しています。
- 経済産業省は2022年11月に「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」を発行し、工場システムのセキュリティ対策を実施するための参考となる概念と手順を示しています。

保護貿易主義の台頭で各国は現地生産拠点設立へ

過去数十年にわたり、グローバリゼーションは実質的に不可逆的な傾向と考えられてきました。世界中の多くの製造業は、サプライチェーンの最前線を拡大し、低コストの労働力、土地、サービスが提供できる中国本土やインドに生産拠点を置き、変化し続ける多国籍企業帝国として知られる遠大なモデルを確立してきました。しかし、近年の「インダストリー 4.0」革命の勃発により、ロングチェーンモデルがすべての人にとって本当に有益であるかどうかを思案する企業が増え始めています。

米中貿易摩擦は、新型コロナウイルス感染症拡大と相まって、各国は自動車用チップや医療品の不足など、かつてないサプライチェーンのショックを経験することになりました。各国の政府や企業は、国内での安全な操業を確保するためには、自国内で必要な製品を生産できなければならないということに気付き始めています。このような国民生活や安全保障に基づく配慮が、生産における「グローバリゼーション」ではなく、「ローカリゼーション」や「リージョナライゼーション（地域化）」をさらに定着させています。近年、企業は安い労働力と土地を拠点立地の第一条件とすることをやめて、生産ラインを母国に戻す「回帰」戦略を採り始めています。

近年、米国、ドイツ、日本、韓国、英国などの先進国では、製造業のリショアリング（自国回帰）を積極的に推進しています。新素材、3D プリンティング、スマートマニュファクチャリングなどの技術革新が急速に進み、国内生産チェーンの分業化が進んでいます。新たな工場の建設に伴い、企業は将来のセキュリティのためのより良い基盤を築くために、機器が最初に現場に入る際には ICS/OT サイバーセキュリティを考慮する傾向がより多く見られるようになりました。

OT 環境内での潜在的損失に対する意識向上

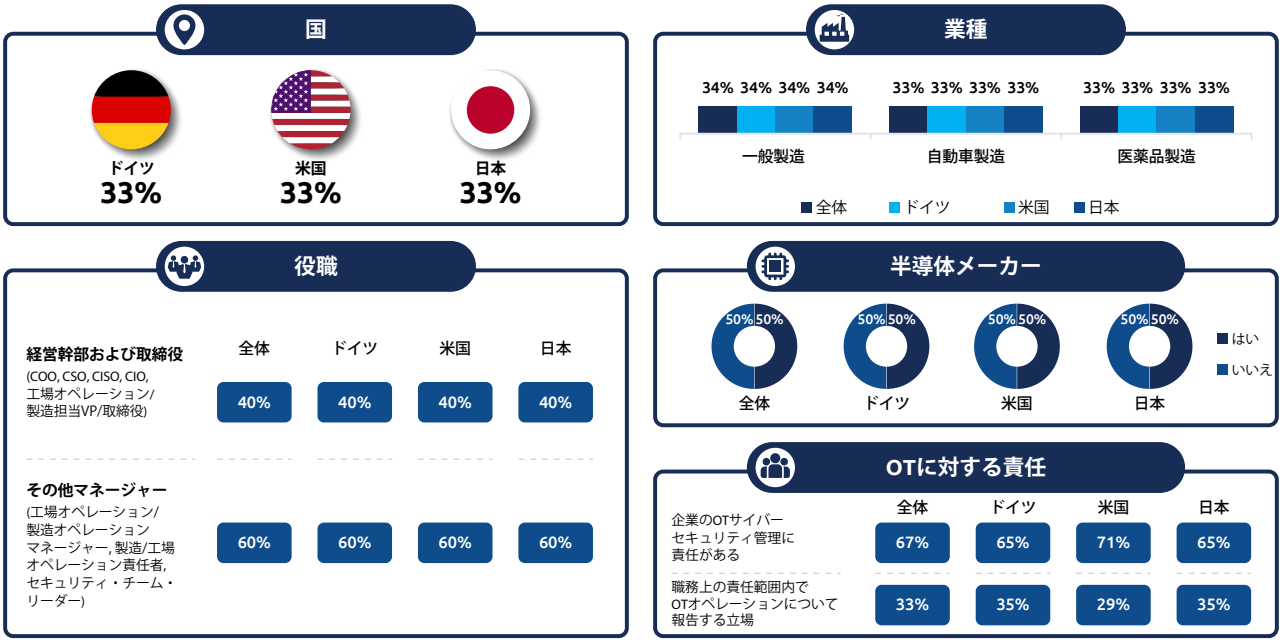
製造業や重要なインフラを標的とした攻撃の増加が、OT（運用制御技術）攻撃の重大性を浮き彫りにし、セキュリティの必要性が明確になっています。企業は、ランサムウェア攻撃によって生産ラインのオペレーションが中断され、生産性が著しく低下し、復旧に数時間以上かかることを理解しています。攻撃者は、さまざまな恐喝方法を駆使して、機密性の高い企業情報を盗み出します。そのため企業は、情報漏洩、財産の損失、さらに違反を招くことになり、顧客の信頼失墜やブランド価値低下を招く可能性があります。「インダストリー 4.0」が企業競争の重要な側面となっているため、企業経営者や情報セキュリティのリーダーは、OT ネットワークの保護を情報セキュリティ戦略の最優先事項にしなければなりません。この新しいサイバーセキュリティアーキテクチャを構築できる基盤を提供するために、2022 年の製造業企業の経験に基づく OT セキュリティについてのエンドユーザー調査を行いました。

OT セキュリティについての エンドユーザー調査

2022 年、TXOne Networks では、フロスト＆サリバン社に委託し、製造業における OT/ICS サイバーセキュリティの現状に関するグローバル調査を実施しました。この調査では、米国、日本、ドイツなどの先進製造国の意思決定者やリーダーにインタビューを行い、300 人の OT/ICS 関係者に参加いただきました。この調査では、企業内の意思決定者が OT セキュリティをどのように認識し、どのような課題に直面しているか調査し、一般的な脆弱性とレジリエンスのレベルを計っています。3 つの主要業種を調査し、ほぼ同等のサンプル規模で調査対象を分けました。34% が一般製造業、33% が自動車製造業、そして 33% が医薬品製造業です。一般製造業の半数は専門性の高い設備を必要とする半導体メーカーであり、そうした工場では、サイバー攻撃による深刻な被害を受ける可能性があります。

調査対象となった方々の役職は経営層で、経営幹部レベルや取締役の階層にまでおよびます。40% が経営幹部であり、60% が工場の運営管理者、製造部門の責任者、セキュリティチームのリーダーです。このような調査対象の選定は意図的なもので、この調査は、セキュリティやサイバーセキュリティに基づく意思決定を行う人たちの考えを知ることを目的としているため、これらのグループのかたがたが最も直接的に関係すると言えます。OT に対する責任に関しては、その大部分（65% 以上）が自分たちに「企業の OT サイバーセキュリティの管理責任がある」と答えています。そのため、調査対象者は、サイバーセキュリティの問題に対処し、日常生活の中でそれらの問題を解決する責任がある人々であると推測できます。残りは、自分自身を「職務上の責任の範囲内で OT オペレーションを報告する」人に分類しています。TXOne Networks では、OT セキュリティの脅威の状況を、その現場にいる人々の視点からより詳しく把握したいと考えました。

OT セキュリティについてのエンドユーザー調査の概要



OT セキュリティの現状

本レポートは、製造業の主要 3 カ国で実施されたインタビューを基にしています。アメリカ、日本、ドイツは、製造業や最先端技術の分野で長らく大国として認識されてきたため、これらの 3 カ国を選びました。回答者からのフィードバックをもとに、最も関係の深い方々の考えを明らかにしています。この分析で、過去 1 年間に各国が直面したセキュリティ上の課題を比較して、世界の製造業の OT サイバーセキュリティの状況について、5 つの重要な考察が得られました。調査の結果、企業は OT インフラのセキュリティに対してますます関心が高まっていますが、まだ盲点があり、OT の脅威を防止するための取り組みを強化する必要があることがわかりました。

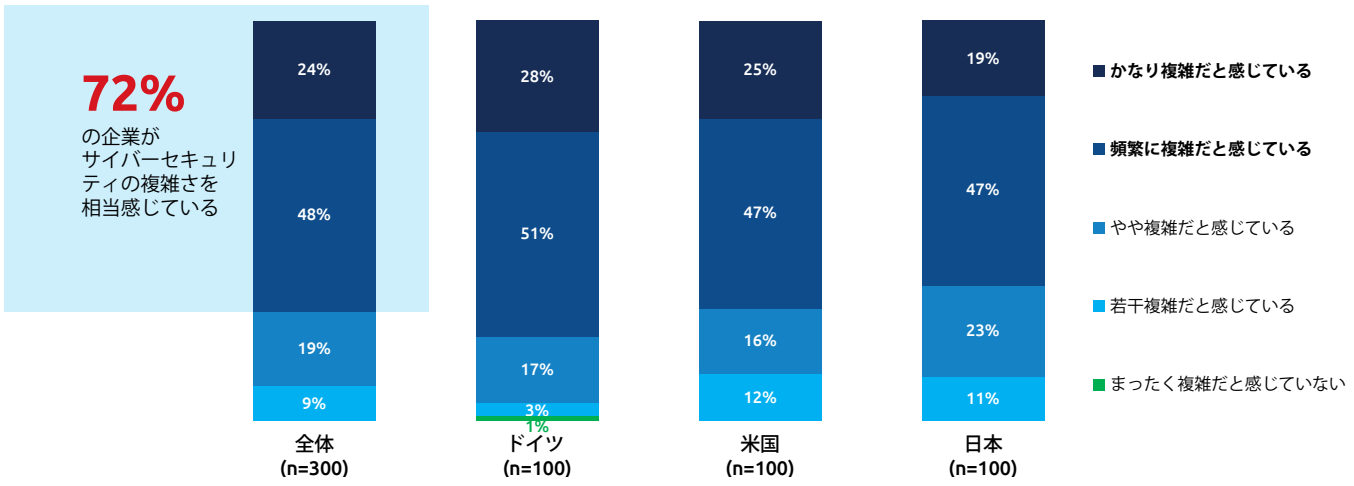
考察 1

サイバーセキュリティの複雑さを生む要因

かつて、情報がコンピュータのハードディスクやフロッピーディスクなどの物理的オブジェクトに閉じ込められていた頃は、情報の所在を追跡して保護することは比較的簡単でした。しかし、インダストリー 4.0 のもと、コネクティビティ（接続性）がトレンドになっている今、このタスクは非常に扱いにくく、予測不可能になっています。情報のセキュリティを維持しようとする際に発生する問題は、「サイバーセキュリティの複雑さ」という一括りの言葉でまとめられてしまいます。今回の調査では、企業の 72% がサイバーセキュリティの複雑さに直面しており、それがどの程度問題になっているのか、さらにサイバー攻撃者が悪用して暴走する前に、企業が自社の防御体制を改善することが急がれる理由が明らかになっています。これらの企業の 24% が（サイバーセキュリティを）「かなり複雑だと感じている」と答え、48% が「頻繁に複雑だと感じている」と回答しています。ここから、サイバーセキュリティを複雑だと感じている企業が大多数で、それを

頻繁に感じていることがわかります。複雑さが増すにつれて、このような複雑さを管理して軽減するためには、セキュリティチームにはより高いレベルの専門知識が必要になります。そのため、セキュリティチームは急速に進展する脅威の状況に大きな影響を受け、人材に関する多くの課題に直面しているのです。

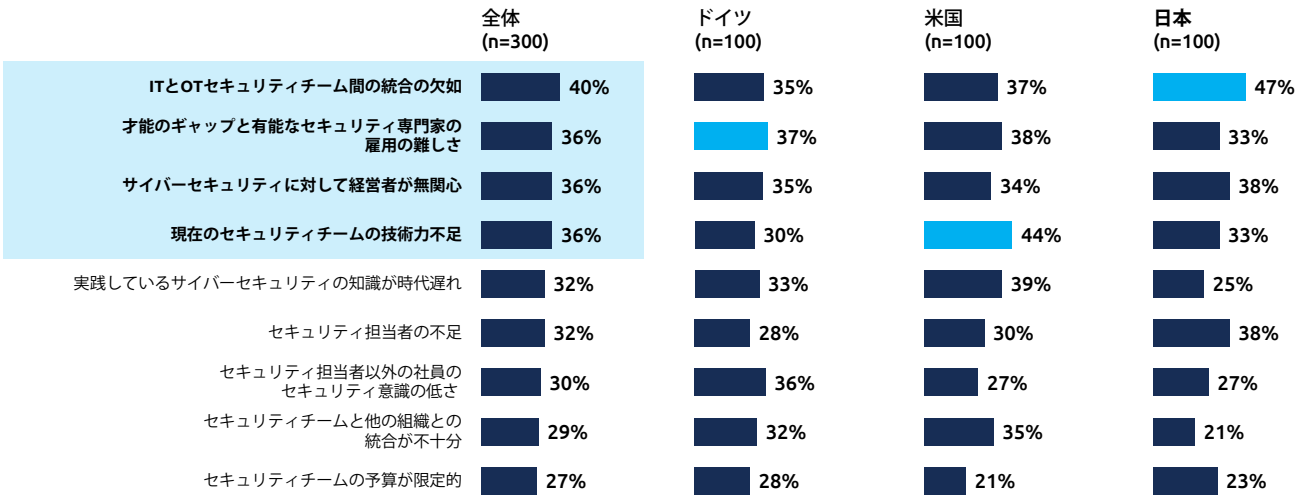
企業でのサイバーセキュリティの複雑さ



Q - あなたの企業ではどの程度サイバーセキュリティが複雑だと感じていますか？
（評価 1- まったく複雑だと感じていない、から 5 - かなり複雑だと感じている、まで）

出典：フロスト & サリバン

セキュリティ人材の主な課題



Q - 過去 12 カ月間に直面してきたセキュリティ人材の主な課題は何ですか？

出典：フロスト & サリバン

IT と OT のセキュリティチームは連携が必要

企業が直面している最大の課題は、IT 部門と OT 部門でのセキュリティチーム間の連携不足です。300 社のうちの 40% は、IT 部門と OT 部門のセキュリティチーム間の連携不足が障害であると回答しています。最近までは、ほとんどのセキュリティは IT を中心に実践しており、ウイルス対策やファイアウォールなどのソフトウェアを使用して対処していました。運用制御技術においては、エアギャプ、つまりセキュアなコンピュータネットワークがセキュアではないネットワークから物理的に切り離すといった単純な対策が講じられていました。ただし、これは、オフライン状態でシステムを更新できず、セキュリティ更新プログラムによるパッチが適用されないままということになります。仮に、セキュリティを更新するために突然ネットワークに接続された場合、かえって更新プログラムやパッチの適用漏れによってシステムが危険にさらされ、セキュリティ更新の試みが不注意によってより多くの危険にさらされることになります。これは、IT システムと OT システムがセキュリティ面で互いに対立する多数の事象のわずか 1 つにすぎません。OT デバイスは、オフラインで他のデバイスから物理的に切り離されている限り安全です。しかし、今の時代にこれらのデバイスを利用可能とするためには、オンラインにして接続する必要があります。テクノロジーの進歩に伴い、IT と OT の双方が対応する戦略を調整して、エンドツーエンドの情報セキュリティを確保するためにより緊密に連携する必要があります。日本では、このようなチーム間の連携不足が最も深刻であり、100 社中 47 社で課題として挙げています。

有能な OT セキュリティ専門家の雇用拡大

次の課題は、限られた人材プールから有能なセキュリティ専門家を採用する難しさです。近年の技術が急速に進歩していることを考えると、（知識や技能など）すべてが最新で十分に訓練された人材の数が限られているのは当然です。サイバーセキュリティは、参入が難しい分野であるだけでなく、技術革新の飛躍によって絶えず進化しているため、常に必要な人材が流動的な状況になっています。ドイツはこの問題に最も苦しんでおり、37% の企業がこの問題に直面しています。ここから、企業内でサイバーセキュリティの専用トレーニングプログラムや専用カリキュラムを設けることが望ましく、将来的にも多くの悪影響を減らすことができると考えられます。優れた OT セキュリティ専門家は、OT ネットワークのセキュリティを管理するために必要なスキルと経験を備えており、事前準備、計画、サポート、トレーニング、インシデント発生時の脅威と対応の特定、影響の軽減、排除、インシデント後の回復などの分野で貢献できます。

OT サイバーセキュリティに対する経営層のコミットメント

多くの企業で広く問題となっているサイバーセキュリティの経験や知識の欠如の他に、サイバーセキュリティに対する姿勢の問題も挙げられます。実際、経営層の 3 分の 1 以上がサイバーセキュリティ全般に無関心であり、それを深刻な脅威と考えていないようだと、調査対象企業の平均 36% が回答しています。これは、サイバーセキュリティの分野がまだかなりニッチで専門的な分野であり、学習曲線が急なカーブを描く、まったく新しいスキルセットを習得する必要があるということを、経営層がなかなか認めようとしないからもしれません。この適応への消極姿勢に加えて、現状に満足してしまっているというのも要因にあります。どうやら、多くの企業は、自社の IT セキュリティで OT セキュリティの基盤をカバーできると考えているようです。調査対象企業の 48% が 2022 年に OT セキュリティインシデントに直面し、47% が 2022 年に IT セキュリティインシデントに直面していることを考えると、経営層の認識と世の中の現実との間に矛盾があることは明らかです。ハッカーは飛躍的に進歩しており、企業が業界内で競争力を維持するために機器を最新化して追いつこうとしている中で露呈する脆弱性に照準を合わせています。さらに、IT インシデントの 94% が、これらの企業内の OT 環境にも影響をおよぼしています。明らかに、IT ソリューションは OT セキュリティの脆弱性をカバーしていませんが、IT の問題は両方の分野にまたがり、OT セキュリティに悪影響をおよぼしています。このような状況は控えめに言っても持続不可能です。IT 環境と OT 環境の両方のセキュリティを保護することの重要性を理解する必要があり、また、OT セキュリティ計画を成功させるためには、経営層によるコミットメント（関与）とサポートが不可欠です。

サイバーセキュリティの複雑さをプロアクティブに軽減することで悪影響を抑制

サイバーセキュリティの複雑さが原因で多くの悪影響が生まれ、企業の多くはこれを運用ルーチンの問題として扱っています。最も悪影響が出ているのが処理時間です。調査対象企業の 47% が、処理時間が大幅に長くなっていると回答しています。この分野ではドイツが 52% と最も被害を被っています。製造業においては、これが企業に与えるダメージは、金銭的にも企業評価的にも極めて壊滅的なものになる可能性があります。それに加えて、メンテナンスコストにも多くを費やす必要があります。これは、企業の 44% が直面している問題です。また、連携とは別の問題ですが、41% がソリューション間の統合が不十分であるという問題に直面しています。さらに、人件費も増加しており、平均で 40% の企業に影響が出ています。脅威の検出と対応の有効性が低いことについては回答幅が最も広く、ドイツの企業では 28% がこの問題に直面しているのに対し、日本の企業では 45% です。ヒューマンエラーの増加は平均 37% が回答しており、調査対象企業の 31% がより広範な脅威の領域に影響を受けています。

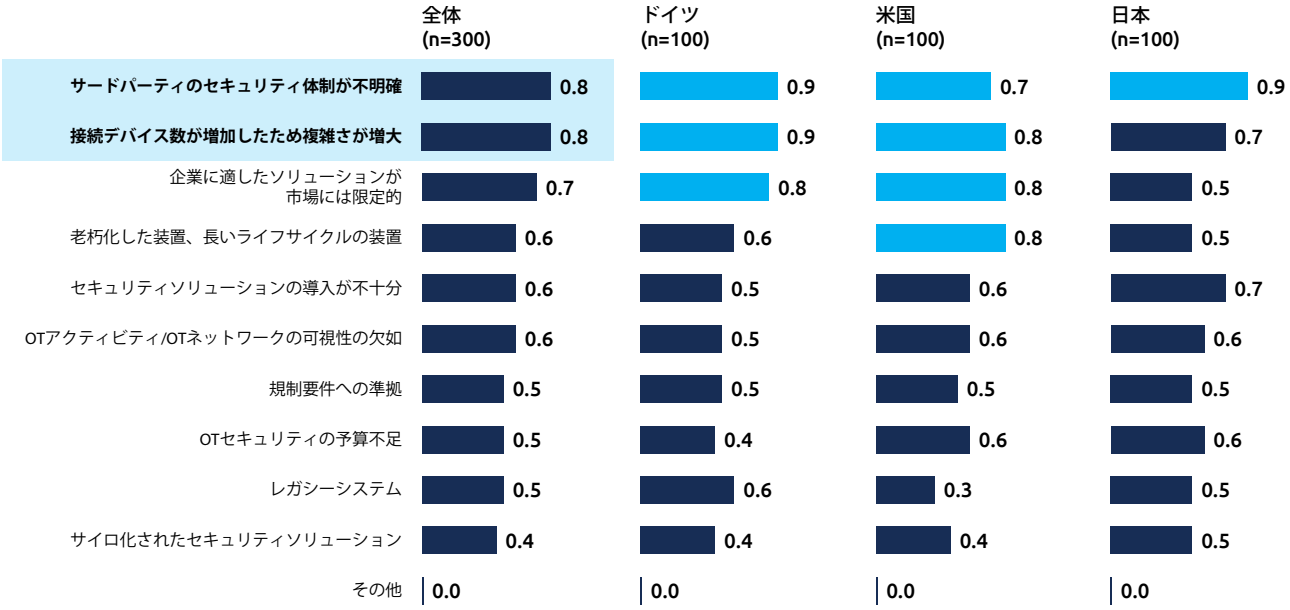
考察 2

特定の課題に対処するための OT サイバーセキュリティの新しい防御要件

サイバーセキュリティの複雑さが増す一方で、企業は新たな攻撃方法、レガシー機器、進化を続ける技術環境、リソースの制約にも直面しています。今回の調査では、これらは ICS/OT の技術とプロセスを保護する上で直面する最大の課題となっています。これらの課題をランク付けすると次のようになります。

1. サードパーティのセキュリティ体制が不明確
2. 接続デバイス数が増加したため複雑さが増大
3. 企業に適したソリューションが市場には限定的
4. 老朽化した装置、長いライフサイクルの装置
5. セキュリティソリューションの導入が不十分

OT サイバーセキュリティの主な課題

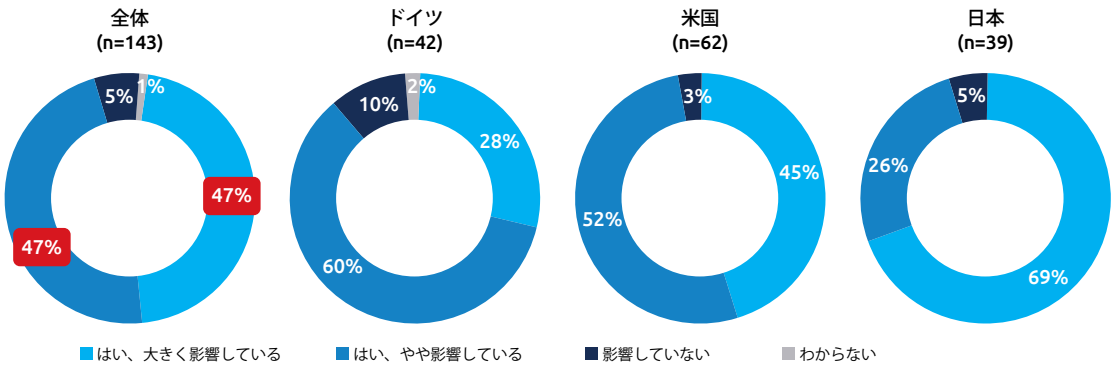


Q - 直面している OT サイバーセキュリティ上の主な課題は何ですか？上位 3 つを選択してください。（平均スコアでランク付け）

出典：フロスト & サリバン

IT セキュリティインシデントの OT 環境への影響度

94%
のITセキュリティインシデントがOT環境にも影響をおよぼしている



Q - これらの IT セキュリティインシデントは、OT 環境にも影響がおよびましたか？

出典：フロスト & サリバン

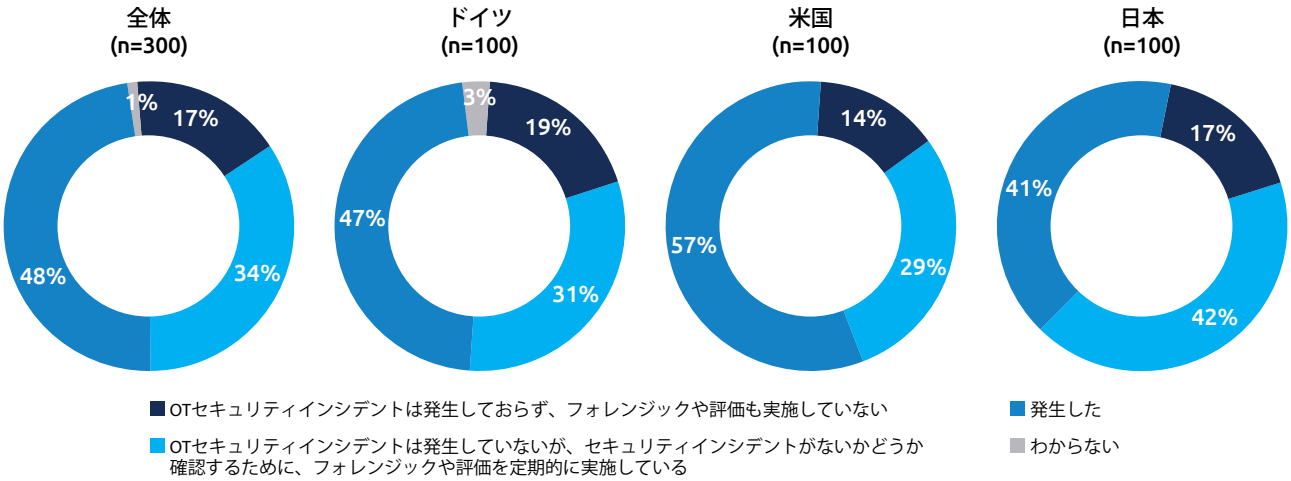
企業は、サードパーティのサプライヤーがサプライチェーンに持ち込む未知の要素こそが最大の課題だと考えています。巧妙なハッカーは、サプライチェーンの最も弱いリンクを探し出し、これらの信頼できる企業を経由したサプライチェーン攻撃を実行します。次に、接続されたデバイスの数が増加し続けていることが、レガシーで老朽化しているICS/OT技術とあいまって、攻撃を受ける可能性をさらに広げています。特に、従来のITセキュリティ技術が制御システム用には設計されておらず、ICS/OT環境に混乱を引き起こす原因となるという事実にOT設備は直面しており、企業は重要資産を保護するため、ICS固有の制御に適合したソリューションを探しています。

IT-OT共同防御対策をセキュリティ計画に組み込むべき

コロニアルパイプライン社やJBS Foods社などの企業に対するランサムウェア攻撃では、IT攻撃がOTシステムにおよぼす危険性に注目が集まりました。これらの攻撃は、当初はOTシステムを標的にしていないかもしれませんが、ITシステムが侵害されると、セキュリティ上の理由からOTチームは手動でオペレーションを停止せざるを得ず、OTに間接的な影響をおよぼすことになります。調査対象企業の94%が、ITセキュリティインシデントがOT環境に影響をおよぼす可能性があることを認識しています。ランサムウェアはラテラルムーブメント（横方向の移動）が可能であるため、OTかITシステムのどちらかの対策に依存するだけでは不十分です。これらのインシデントは、セキュリティ戦略にIT-OTを融合させた防御策をすぐにでも組み込むべきだということを伝えています。

しかし、この調査によると、48%の企業が、2022年にICS/OTセキュリティインシデントを経験したと回答した一方、17%の企業がまったく経験したことがなく、フォレンジックやセキュリティ評価も行っていないと回答しています。逆に、セキュリティインシデントの詳細な調査と評価を完了し、インシデントは発生していないと回答した企業はわずか34%でした。現実を見ると、表面的には安全に見えても、実際はセキュリティ評価やフォレンジックアクティビティを実施していない企業が少なからずあり、ICS/OTセキュリティインシデントを経験している企業の実際の状況は、回答内容よりも深刻である可能性があります。たとえば、米国地域の調査対象企業の57%がICS/OTセキュリティインシデントを経験済みと回答していますが、ICS/OTセキュリティインシデントをまだ検出していない企業もあるかもしれません。このことからも、ICS/OTセキュリティは企業の経営層が今後早急に取り組むべき課題であるとはっきりわかります。

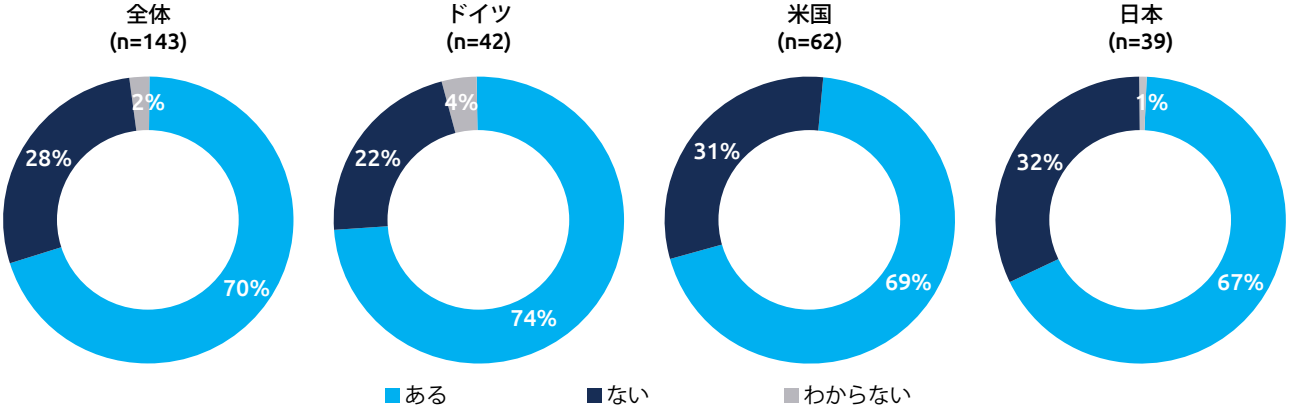
OT セキュリティインシデントを経験した企業



Q - 過去 12 カ月間に OT セキュリティインシデントが発生しましたか？

出典：フロスト & サリバン

データや事業活動を人質に取られた企業



Q - データや事業活動を人質に取られたことがありますか？

出典：フロスト & サリバン

レジリエンス計画強化で影響を軽減

「データや事業活動が人質に取られたことがありますか？」の質問に対して、70% の企業が経験ありと回答しています。何年もの間、ランサムウェアに似た攻撃により大きな損失や金銭的損害が発生しています。最も一般的な手口は、企業のデータや事業活動を人質に取ることです。これは前段で説明したとおり、データは現実の一部しか反映しておらず、未知の危険が潜んでいる氷山の一角ということになります。

企業は、OT へのハッカー攻撃は決して発生しないと決めつけるのではなく、そのような攻撃が発生した場合にどのように対応するか検討する必要があります。そのため、過去の危機から学んだ教訓に基づき、今後の OT の混乱に備えて革新的で適応性のあるソリューションを用意しなければなりません。企業がレジリエントな計画を策定するには、将来を見据えて、経験に基づいた継続的な学習と改訂が求められます。

頻発する攻撃に自動化ツールで対応

サイバーセキュリティの複雑さや、発生した問題の解決に要する時間、人員、コストに加えて、企業はマルウェアやランサムウェア攻撃にもさらされています。実際、企業の 20% が毎週ランサムウェア攻撃に対応し、19% が毎週ウイルスやマルウェアの侵入を経験していると回答しています。過去 1 年を見ると、企業の 70% が悪意のある攻撃者によってデータや事業活動を人質に取られています。サイバーセキュリティ攻撃に頻繁に直面し、人手不足にも向き合う企業は、より自動化されたサイバーセキュリティツールを用いて迅速に対応しなければなりません。

繰り返し OT セキュリティ攻撃を受ける企業

	OTセキュリティインシデントの頻度					
インシデント	毎週	毎月	四半期ごと	半年ごと	毎年	わからない
ウイルスまたはマルウェアの侵入	19%	**38%**	31%	5%	5%	2%
ランサムウェア攻撃	20%	**26%**	**26%**	17%	11%	0%
パッチが未適用のシステムの脆弱性	17%	24%	**41%**	15%	12%	0%
フィッシングメール	15%	**39%**	28%	7%	11%	0%
持続的標的型脅威（APT）攻撃	14%	32%	**34%**	16%	2%	2%
分散型サービス拒否（DDoS）攻撃	18%	**33%**	26%	21%	3%	0%
ヒューマンエラー（意図的ではない）- 従業員の行為	17%	30%	**33%**	17%	0%	2%
悪意ある動機 - 従業員の行為	12%	32%	**38%**	8%	4%	6%
個人情報の窃盗、偽のログイン認証情報	16%	**40%**	20%	16%	7%	2%
サードパーティベンダーやサプライヤーによる侵害	18%	**33%**	31%	11%	4%	2%

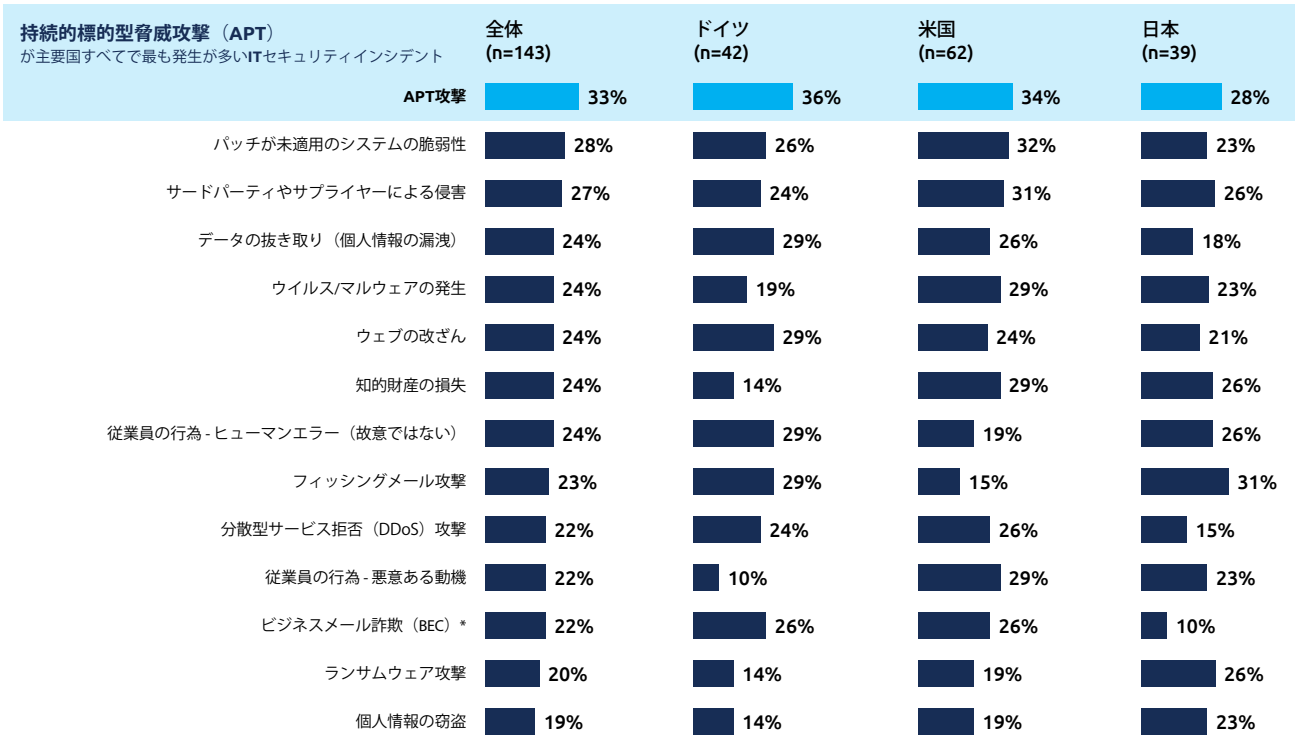
Q - 過去 12 カ月間にどれぐらいの頻度で OT セキュリティインシデントが発生しましたか？（ベースは異なります）

出典：フロスト & サリバン

考察 3 OT 現場に新たな資産を持ち込む際には特段の注意が必要

IT の分野では、持続的標的型（APT：Advanced Persistent Threat）攻撃は、3 カ国すべてで最も高い IT セキュリティインシデントとしてランク付けされています。このタイプの攻撃の問題点は、その目的が長期にわたって攻撃を確立し維持するという点にあります。奇襲攻撃ではなく、企業内に住み着く悪性の毒薬となります。ドイツはこの攻撃で最も被害を受けており、36% の企業が経験ありと回答しています。

被害を受けた IT セキュリティインシデントのタイプ

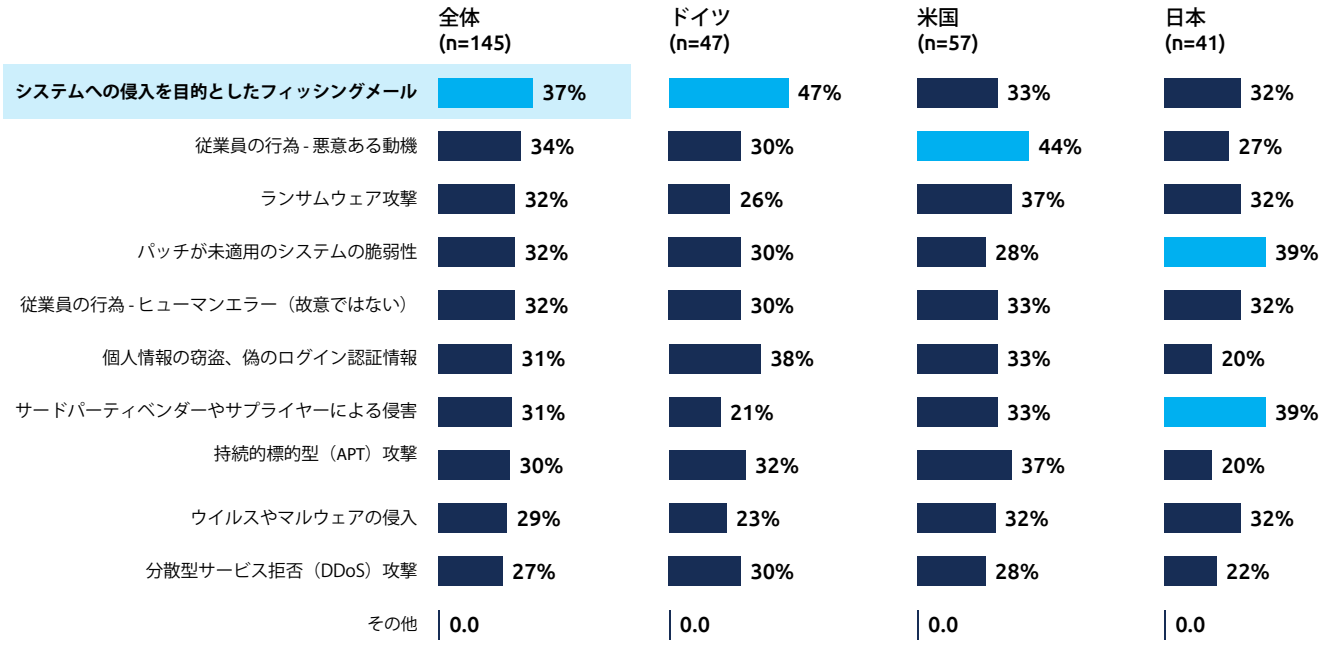


Q - 過去 12 カ月に経験した IT セキュリティインシデントは次のうちどれですか？

出典：フロスト & サリバン

一方、OT 攻撃は主にフィッシングメールを用いて、社内の従業員の騙されやすさや不注意を突いてシステムに侵入することを目的としています。このタイプの攻撃でもドイツが最も被害を受けており、47% の企業が被害を受けています。米国では、「悪意の動機がある従業員の行為」が OT インシデントの 44% を占めています。日本における最大の弱点は、2 つの要素から成り立っており、「パッチ未適用のシステムの脆弱性」と、「サードパーティベンダーやサプライヤーによる侵害」です。レガシーシステムにはネットワークへの接続機能がないことや、セキュリティを維持して装置を動作させ続けるために、意図的にオフラインにしておく場合があります。しかし、このような障壁を作って危険を回避することは、同時に、万一侵入されてしまった場合に自らの助けとなる最新のセキュリティ対策も遮断することになります。「サードパーティベンダーやサプライヤーによる侵害」とは、工場の作業現場に持ち込んだ他社の機器にマルウェアやウイルスが潜んでおり、企業のシステムに損害を与える可能性があるという問題です。これら 2 種類のセキュリティインシデントは、日本で対処しなければならない OT インシデントの 39% を占めています。

被害を受けた OT セキュリティインシデントのタイプ



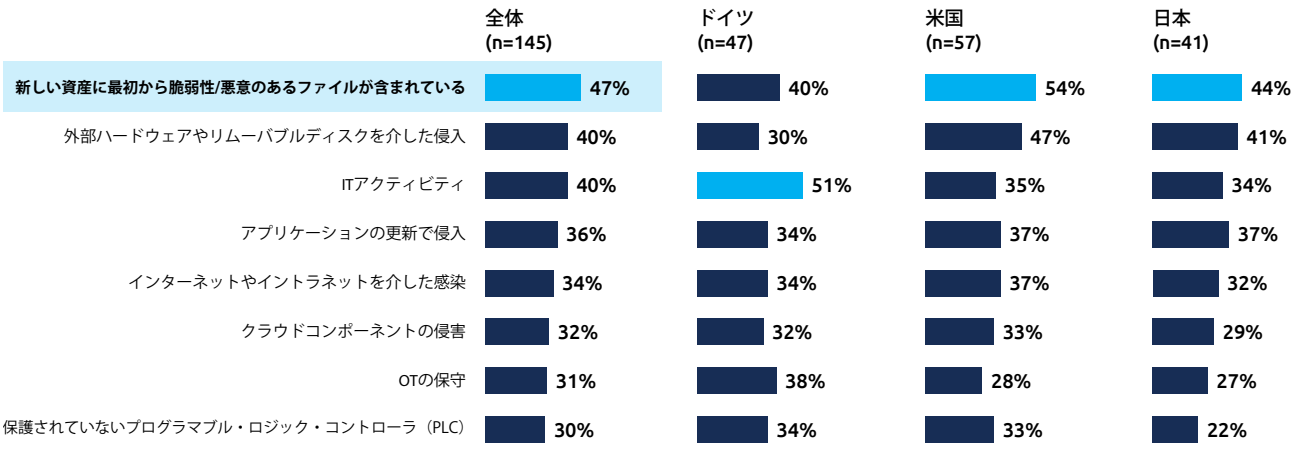
Q - 過去 12 カ月に経験した OT セキュリティインシデントは次のうちどれですか？

出典：フロスト & サリバン

OT セキュリティインシデントの大半は新しい資産から発生

新しい資産は、脆弱性があり、最初から悪意のあるファイルが潜んでいる可能性があるため、OT セキュリティインシデントの大半がこれで発生しています。米国では、54% の企業で問題となっていますが、日本では 44% の企業で発生しています。ここではドイツが例外的で、OT セキュリティインシデントの 51% は新しい資産ではなく IT アクティビティに起因しています。これらの課題は、金銭的損失と生産性の大幅な低下のいずれにもつながります。

OT セキュリティインシデントの原因

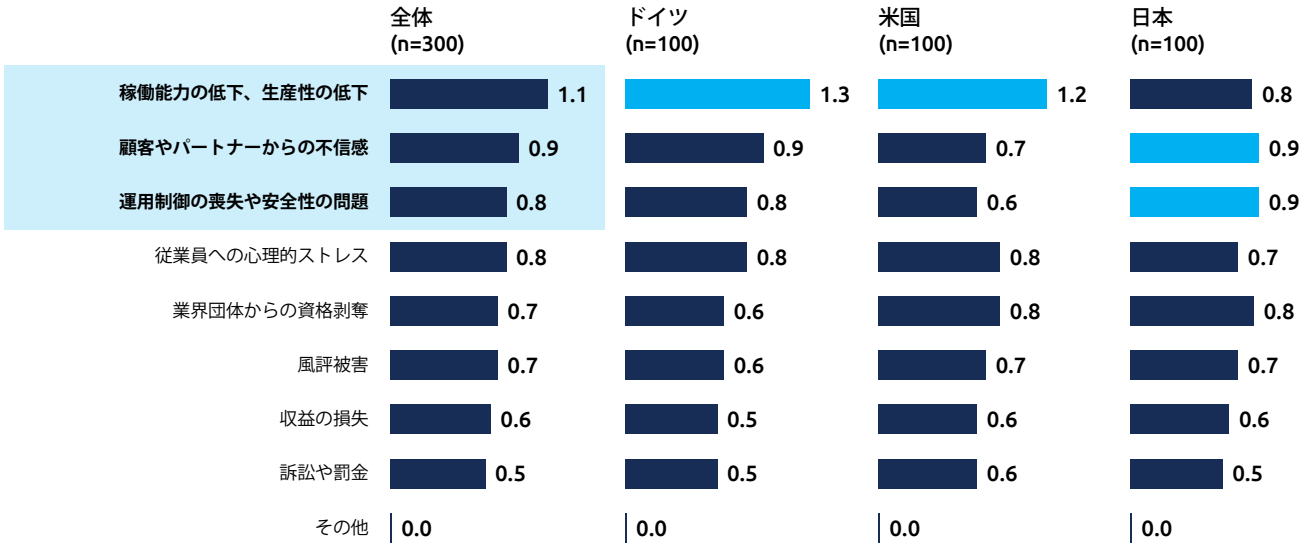


Q - 過去 12 カ月に発生した OT セキュリティインシデントの原因は何ですか？

出典：フロスト & サリバン

このような大きな金銭的損失があるにもかかわらず、企業は生産性の損失を最も懸念しています。セキュリティインシデントが生産性におよぼす影響は、稼働能力の低下や文字通り生産性の低下から、顧客やパートナーからの不信感、運用制御の喪失や安全性の問題に至るまで多岐にわたります。さらに、従業員への心理的ストレス、業界での資格剥奪、風評被害、収益の損失、訴訟や罰金などさまざまです。このようにセキュリティインシデントの影響は多岐にわたる上、回復が極めて困難です。

セキュリティインシデントの影響で最も懸念されるもの



Q - セキュリティインシデントによる影響で、最も懸念しているものは次のうちどれですか？上位 3 つを選択してください。（平均スコアでランク付け）

出典：フロスト & サリバン

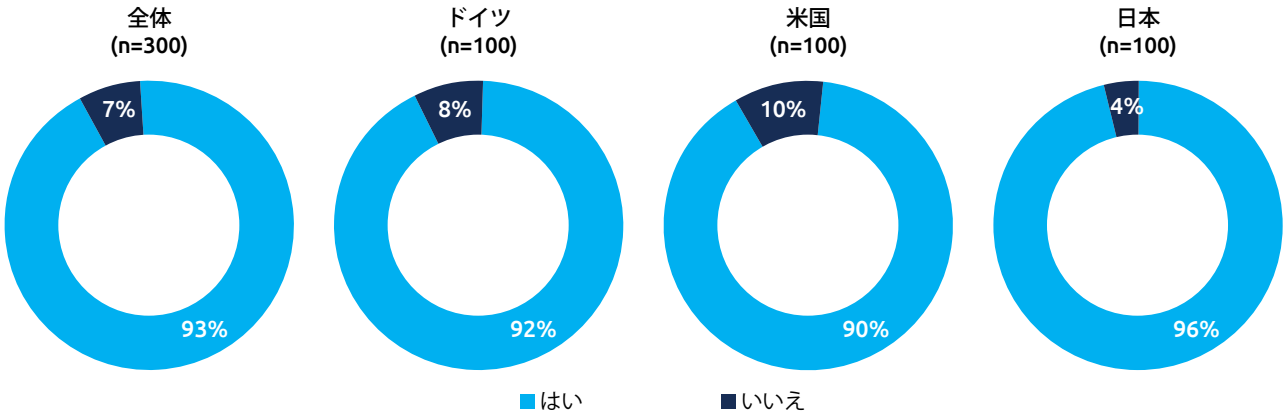
考察 4

OT に特化したサイバーセキュリティソリューションの必要性

今回の調査では、93% の企業がすでにサイバーセキュリティソリューションを使用しており、OT 環境にも適用しています。このことは、第 1 章で述べたように、OT 環境に対するサイバーセキュリティの意識が高まり、潜在的な損失を回避しようとソリューションを導入していることを示しています。それでもなぜサイバーセキュリティインシデントは頻繁に発生するのかという疑問は残ります。当社のこれまでのリサーチに基づき、その考えられる要因は次のとおりです。

1. **OT 環境でもあるのに関わらず、OT サイバーセキュリティソリューションではなく IT ソリューションを使用している。約 70% の企業が、OT 空間で、以前導入した IT ソリューションの再利用を検討している。**
2. **人手不足。日本では、セキュリティに携わる人員が極めて少ない。平均して 101 ～ 200 台のデバイスあたり 1 人のスタッフしかおらず、最も深刻な状況では、301 ～ 400 台のデバイスあたり 1 人の配置。**
3. **ソリューションの導入が不完全。61% の企業で、保護されていない Windows デバイスを使用している。**
4. **ヒューマンエラー。**
5. **レガシーシステムでは、十分なテクニカルサポートが受けられない。**

現在のサイバーセキュリティソリューションの使用状況

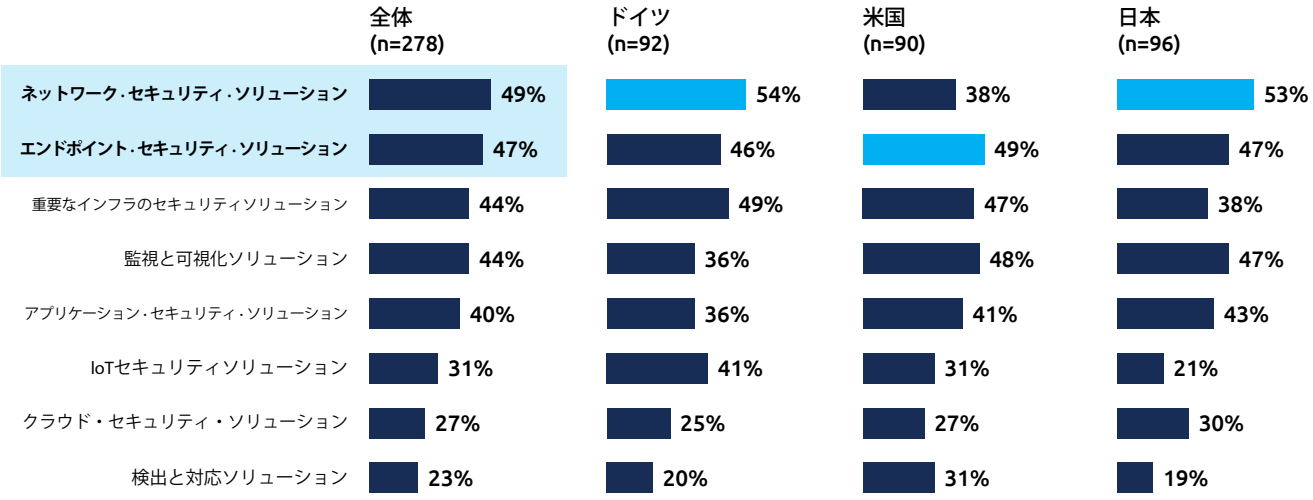


Q - 現在、OT セキュリティ用にサイバーセキュリティソリューションを使用していますか？

出典：フロスト & サリバン

多くの企業がサイバーセキュリティソリューションを導入していることを考えると、どのソリューションが企業にとって最も重要であるかを判断することが必要となります。回答者の 49% が、ネットワーク・セキュリティ・ソリューションを導入しており、47% がエンドポイント・セキュリティ・ソリューションを導入していると回答しています。「重要インフラのセキュリティソリューション」が 44%、「監視と可視化ソリューション」も 44% で並んでいます。一般的に、製造業における、OT 防御の優先順位は、ファイアウォールと侵入検知製品の使用が最も効果的で、次にエンドポイント保護、さらに生産ラインマシンなどの重要インフラの保護、最後にサイバーセキュリティの監視と可視化ソリューションを使用することであると考えられています。

OT セキュリティに使用しているサイバーセキュリティソリューション



Q - 現在、OT セキュリティ用に使用しているサイバーセキュリティソリューションは次のうちどれですか（カテゴリー別）？

出典：フロスト & サリバン

エンドポイント保護ソリューションを導入するには、その仕組みや企業の既存のシステムおよびワークフローへの統合方法を学ぶ必要があるため、ソリューションの検証に通常、3 ～ 6 カ月を要します。たとえば、エンドポイント保護を使用しているとした回答者の 14% が、3 ～ 6 カ月必要であると回答しています。ネットワーク・セキュリティ・ソリューションの回答者も 20% が、3 ～ 6 カ月を要すると回答しています。企業の 20% が毎週ランサムウェア攻撃を受けていることを考えると、保護ソリューションの導入にかかるこの時間は、企業にとって重大な問題と言えます。上記のデータから、企業は大幅な環境の簡素化と、導入や検証に掛かる時間を削減し、より完璧なセキュリティソリューションを求めていることがわかります。

ソリューションの検証に要する時間

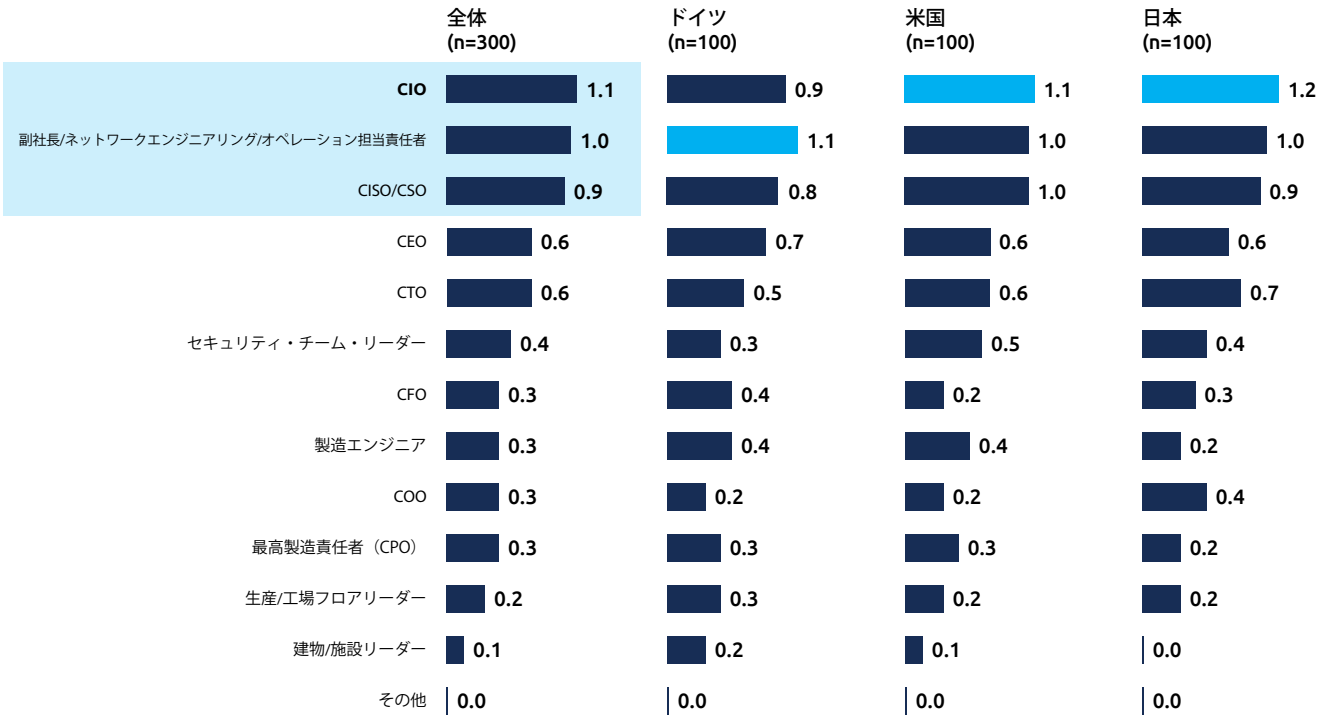
	ソリューションの検証に要する時間					
インシデント	1カ月以下	1～3カ月	3～6カ月	6～9カ月	9～12カ月	12カ月以上
エンドポイント・セキュリティ・ソリューション	13%	12%	**14%**	1%	2%	1%
ネットワーク・セキュリティ・ソリューション	5%	11%	**20%**	6%	3%	0%
重要なインフラのセキュリティソリューション	3%	11%	**17%**	8%	1%	0%
アプリケーション・セキュリティ・ソリューション	7%	8%	**14%**	8%	0%	1%
クラウド・セキュリティ・ソリューション	4%	**9%**	5%	5%	2%	0%
IoTセキュリティソリューション	3%	7%	**12%**	6%	1%	0%
監視と可視化ソリューション	6%	**17%**	12%	3%	2%	1%
検出と対応ソリューション	3%	6%	**8%**	3%	1%	0%

Q - 次の各カテゴリーのソリューションの検証にはどれぐらいの時間がかかりますか？（ベース：合計（n=300）

出典：フロスト & サリバン

企業のサイバーセキュリティへの取り組みに最も影響力を持つのが副社長やネットワーク担当責任者で、CISO、CSO、CIO がそれに続きます。これまでのところ、ほとんどの企業がエンドポイント・セキュリティ・ソリューションを使用しており、88% の企業がこの戦略を採用しています。

OT サイバーセキュリティの意思決定者

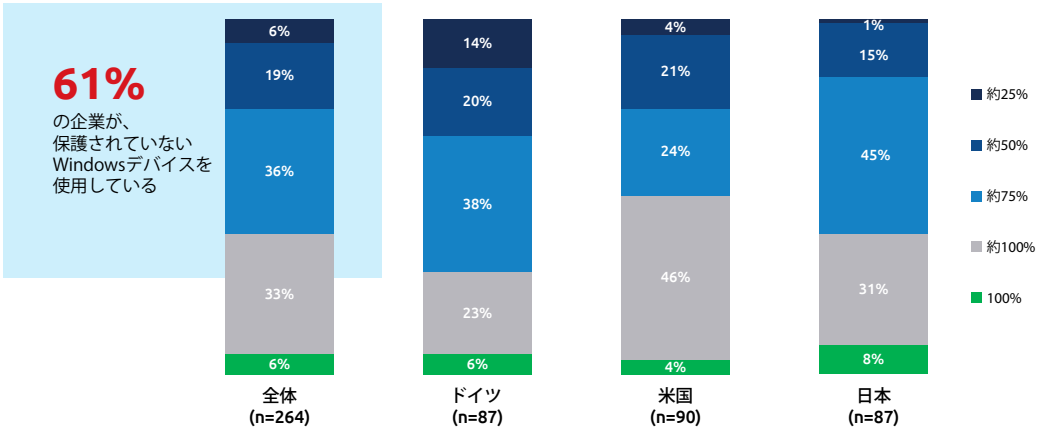


Q - OT サイバーセキュリティの意思決定に最も影響力のある社内リーダーはだれですか？上位 3 人を選択してください。（平均スコアでランク付け）

出典：フロスト & サリバン

すべての企業が、特に Windows デバイスに関して、保護できているわけではありません。多くの企業が保護されていない Windows デバイス（平均 61%）を所有しており、エンドポイント・セキュリティ・ソリューションで Windows デバイスを 100% 保護している企業はわずか 6% です。今後数年間で、より優れたセキュリティソリューションの採用を促進し、拡大できるかどうかは、ベンダーにかかっています。セキュリティインシデントが世界的に多発している状況下にありながら、多くの企業は自社の OT セキュリティに過剰な自信を持っています。だからこそ、サイバーセキュリティへの取り組みの如何によってはこれらの企業が危機的な状況に陥ることを認識してもらうことが重要になります。セキュリティインシデントが発生した場合、ほとんどの企業は外部に支援を求め、外部からのサポートを受けるため、実際の状況においては、その過剰な自信は危険であることを意味します。

エンドポイント・セキュリティ・ソリューションで保護されているデバイスの割合



Q - エンドポイント・セキュリティ・ソリューションで保護されている Windows ベースの PC およびデバイスの割合はどの程度ですか？

出典：フロスト & サリバン

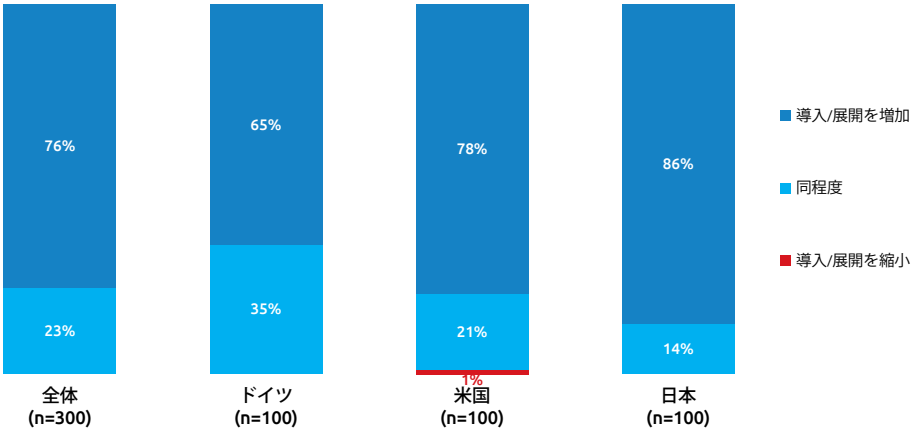
考察 5

OT セキュリティの予算配分は増加傾向

OT セキュリティの今後

今後 12 カ月以内に、世界の主要国が OT セキュリティ管理を強化し、保護アーキテクチャを強化することを計画しています。本調査の参加者の 85% は、OT セキュリティ管理を強化するつもりであると回答しています。そのため、OT セキュリティの予算配分は来年には増加すると予測されます。現時点で、IT と OT のコンバージェンスが避けられなくなっているにもかかわらず、OT セキュリティには IT セキュリティとは別の予算割り当てがなされています。今回の調査結果は、OT サイバーセキュリティ市場の高い成長性を示しており、主要国全体の 76% の企業が、OT サイバーセキュリティ導入を増やす必要性と、支出増を考えていると回答しています。これらの支出は、主にネットワーク・セキュリティ・ソリューション、重要インフラ・セキュリティ・ソリューション、およびエンドポイント・セキュリティ・ソリューションに対して行われます。システムの接続が進むにつれて、悪意のある攻撃が更に猛威を振るうようになる中、これらのソリューションは、企業が自らを守るために適切で基本的な対策となります。また同時に、企業は「監視と可視化ソリューション」、「アプリケーションセキュリティ」、「クラウドセキュリティ」、「IoT セキュリティ」、「検出と対応」にも注目しています。

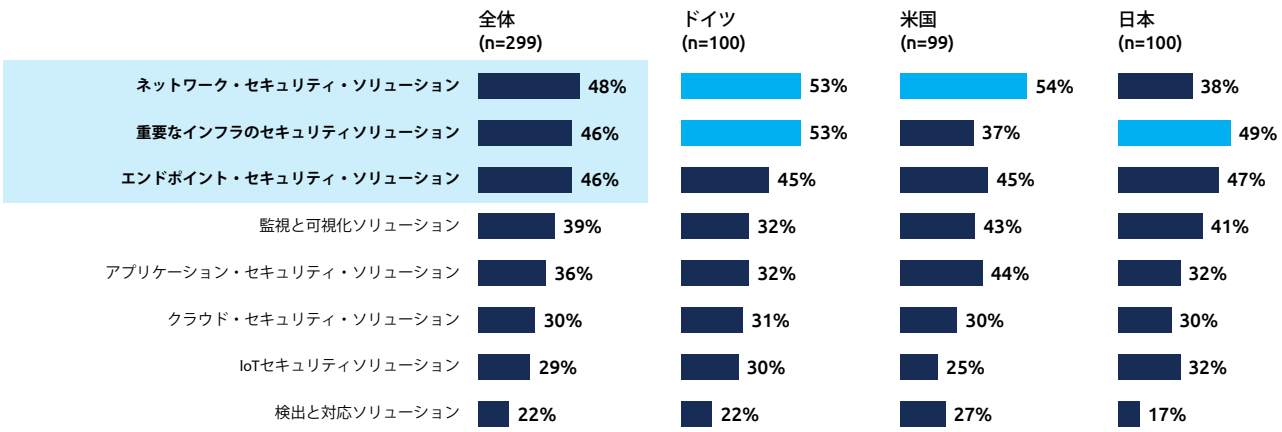
サイバーセキュリティソリューションの導入 / 展開予定



Q - OT セキュリティ用サイバーセキュリティソリューションの導入 / 展開を増やす / 減らす予定はありますか？

出典：フロスト & サリバン

購入する見込みのセキュリティソリューションのカテゴリー



Q - 今後 12 カ月で、OT セキュリティ用として、どのカテゴリーのセキュリティソリューションを購入する可能性がありますか？

出典：フロスト & サリバン

OT セキュリティは IT ソリューションのコピーではない

企業が、過去に IT 分野で効果があると証明されている IT ソリューションを、OT セキュリティ問題の解決策として検討するのは合理的な考えです。これがきちんと機能すれば、一石二鳥（IT ソリューションで IT と OT 両方のセキュリティインシデント対応）となり、素晴らしいことです。上手く適用できれば、新しいセキュリティソリューションを採用する際の学習曲線を短く抑えられ、摩擦もはるかに少なくなるでしょう。しかし一般的に、IT ソリューションの再利用では、OT 環境における穴を完全にカバーしきれないことは明らかです。

今回の調査では、企業は、企業の IT 環境と ICS/OT 環境の違いを認識しつつあります。両者は、システムタイプが異なるだけでなく、直接相互互換性がない技術や、タスクやリスクプロファイルも異なり、初期攻撃ベクトル、与える影響、さらにイベント対応方法さえ異なります。現在、サイバーセキュリティソリューションを選択する際の主な評価ポイントは、次の 3 つの側面に分類できます。

1. **戦略面**：全体としての、総合的な品質が最も重要な戦略的能力と言えます。
2. **運用面**：他のアプリケーションや技術と統合する能力が最も重要な運用能力です。
3. **パフォーマンス面**：全体的を通して、企業はパフォーマンスと可用性に重点を置いて、ビジネス成果を求めます。

まとめ

2023 年のサイバーセキュリティは、2022 年に Black Basta、Pandora、LockBit 3.0 などの新しい RaaS（Ransomware as a Service）が多数登場したことで、ますます複雑化し、困難なものになると予想されます。RaaS ビジネスモデルと収益の流れが確立することで、今後もエネルギー産業や重要な製造業への攻撃は継続する可能性が高く、自動車関連製品のメーカーに大きな影響を及ぼします。

IT と OT の融合に向けた動きに伴い、ますます多くの自動車メーカーが製造プロセスの自動化を採り入れています。これらの工場にとっては、サプライチェーン攻撃を軽減させる事が、今後の対策の重要な鍵となります。例え、個々の企業に強固なセキュリティが備わっていても、サードパーティパートナーの脆弱性が攻撃者に悪用される可能性があります。サードパーティパートナーのセキュリティ能力が把握できていない点は、すべての主要国 / 地域の調査で企業の主要課題となっていました。

米国のバイデン大統領が署名した大統領令 14028 号「国家のサイバーセキュリティ強化」は、OT サイバーセキュリティの重要性を認識する上で重要な規制となりました。これに続く、2021 年 7 月 28 日に署名された「国家安全保障の覚書」で重要インフラ制御システムのセキュリティを強化し、2020 年 12 月に発効した「EU NIS 2.0 指令」により、政府と重要インフラコミュニティの間でサイバーセキュリティに関するコミットメントが確立されました。これらは、重要な ICS/OT システムに対するサイバー脅威にかかわる関係者の意識を高め、最低限のセキュリティ基準の採用を促進するのに役立つと考えられています。たとえば、運輸保安局（TSA）は 2022 年に、パイプラインと鉄道業界のサイバーセキュリティのレジリエンスを強化するパフォーマンスベースの指令を導入し、さらに航空業界のネットワークニーズへの対応策も導入しました。サイバーセキュリティのパフォーマンス目標の開示は、サイバーセキュリティの取り組みの投資収益率を定量化するのにも役立ちます。

幸いなことに、今回の調査では、85% の企業が 2023 年に OT セキュリティ能力を強化させる予定としています。また、70% の企業が OT セキュリティの予算配分を増やそうとしています。これは、重要なインフラやスマートマニュファクチャリングの OT セキュリティの保護対策をさらに後押しするものです。一方で、IT-OT コンバージェンスに伴い、約 70% の企業が OT の領域で、以前導入していた IT ソリューションを転用しようとしているという懸念があります。OT サイバーセキュリティが複雑化する中、企業のセキュリティチームは、IT ソリューションを OT 環境にコピーするのではなく、より高度な専門知識を持つべきです。企業では、潜在的な脅威を防ぐために、サプライ・チェーン・セキュリティ、資産検査、エンドポイント検出と脅威インテリジェンス、ネットワークセグメンテーション、脆弱性管理、パッチ適用、継続的な監視など、OT のプロアクティブ防御戦略を優先させなければなりません。OT ゼロトラストソリューション（ネットワークセグメンテーション、仮想パッチ、許可リスト、資産ハードニング、セキュリティ検査など）に基づき、ネットワークや資産のサイバーセキュリティ基準を根底から高めることで優れた保護基準を満たせられれば、企業は 2023 年に発生しうる OT サイバー脅威への対応をより適切に行うことができるでしょう。

参考文献

[1] *Ivan Nicole Chavez、Byron Gelera、Katherine Casona、Nathaniel Morales、Ieriz Nicolle Gonzalez、 Nathaniel Gregory Ragasa、「ランサムウェアグループ LockBit が BlackMatter 機能で最新亜種 LockBIt3.0 を強化」、トレンドマイクロ、2022 年 7 月 25 日 .*

[2] *SickKids, 「サイバーセキュリティインシデントに対応する SickKids (SickKids responding to cybersecurity incident) 」, SickKids, 2022 年 12 月 19 日 022.*

[3] *Joe Tidy, 「サイバー攻撃がドイツの燃料供給事業者を襲う (Cyber-Attack Strikes German fuel supplies) 」、BBC、2022 年 2 月 01 日 .*

[4] *MITRE, 「System of Trust Framework」、MITER, 2022 年 11 月 3 日 .*

[5] *SEKOIA.IO 脅威検出調査チーム , 「SEKOIAIO 2022 年中盤 ランサムウェア脅威の現状 (SEKOIAIO Mid-2022 Ransomware Threat Landscape) 」 ", SEKOIAIO, 2022 年 7 月 28 日 , アクセス日 2023 年 2 月 7 日 .*

[6] *Flashpoint チーム、「ランサムウェア Conti：世界で最も攻撃的な RaaS グループに隠された歴史 (Conti Ransomware: The History Behind one of the World's Most Aggressive RaaS Groups) 」, Flashpoint 2022 年 10 月 4 日、アクセス日 2023 年 2 月 5 日 .*

[7] *Sumeet Wadhwani,「コスタリカをハッキングしたランサムウェアグループ Hive は何が危険なのか？ (What Makes the Hive Ransomware Gang that Hacked Costa Rica So Dangerous ?)」, Spiceworks, 2022 年 11 月 18 日 , アクセス日 2023 年 2 月 5 日 .*

[8] *Matthew Wopata,「IT-OT コンバージェンスを推進する 5 つの業界コネクティビティトレンド (5 Industrial connectivity trends driving the IT-OT convergence) 」, IoT Analytics, 2019 年 8 月 13 日 .*

[9] *Stephen J. Bigelow, Ben Lutkevich,「IT/OT コンバージェンスとは？知っておくべきこと (What is IT/OT convergence? Everything you need to know) 」、TechTarget、2021 年 8 月 .*

[10] *Advantech,「ADAM-3600 エッジセンシングのデバイス to クラウドソリューションを活用した多地点ステーションデータ転送による下水監視システムの構築 (Utilizing the ADAM-3600 Edge Sensing Device-to-Cloud Solution to Build an Wastewater Monitoring System with Multi-Point Station Data Transmission) 」、Advantech、2018 年 5 月 21 日 .*

[11] *Patrick Howell O'Neill,「ロシアがウクライナ侵攻の 1 時間前にアメリカの衛星会社をハッキング (Russia hacked an American satellite company one hour before the Ukraine invasion) 」, MIT Technology Review, 2022 年 5 月 10 日 .*

[12] *CISA,「重要インフラに関するサイバーインシデント報告法令 2022(CIRCIA)」, CISA, 2022 年 3 月 .*

[13] *プレスブリーフィング,「重要インフラ制御システムのサイバーセキュリティ強化に関する国家安全保障の覚書 (National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems) 」、ホワイトハウス、2021 年 7 月 28 日 .*

[14] *CISA,「州および地方サイバーセキュリティ助成プログラム (State and Local Cybersecurity Grant Program) 」", CISA, 2022 年 9 月 16 日 .*

[15] *プレスリリース、「欧州委員会、ネットワークおよび情報システムのサイバーセキュリティに関する新たな規則への政治的合意を歓迎 (Commission welcomes political agreement on new rules on cybersecurity of network and information systems) 」、欧州委員会、2022 年 5 月 13 日 .*

[16] *Joe Tidy,「欧州石油施設がサイバー攻撃を受ける (European oil facilities hit by cyber-attacks) 」、BBC、2022 年 2 月 3 日 .*

[17] *政策と法律、「サイバーレジリエンス法」、欧州委員会、2022 年 9 月 15 日 .*

[18] *Christopher B. Johnstone,「日本の変革的国家安全保障戦略 (Japan's Transformational National Security Strategy) 」, CSIS, 2022 年 12 月 8 日 .*

[19] *商務情報政策局、「スマート・インダストリアル・セーフティに関する日本・インドネシア政策対話」、経済産業省 2022 年 10 月 4 日 .*

[20] *商務情報政策局「スマート・インダストリアル・セーフティに関する日タイ政策対話」経済産業省、2022 年 12 月 15 日 .*

https://www.txone.com/ja