Presented by

Trellix ADVANCED RESEARCH CENTER

OPERATIONAL TECHNOLOGY THREAT REPORT

日本語翻訳版

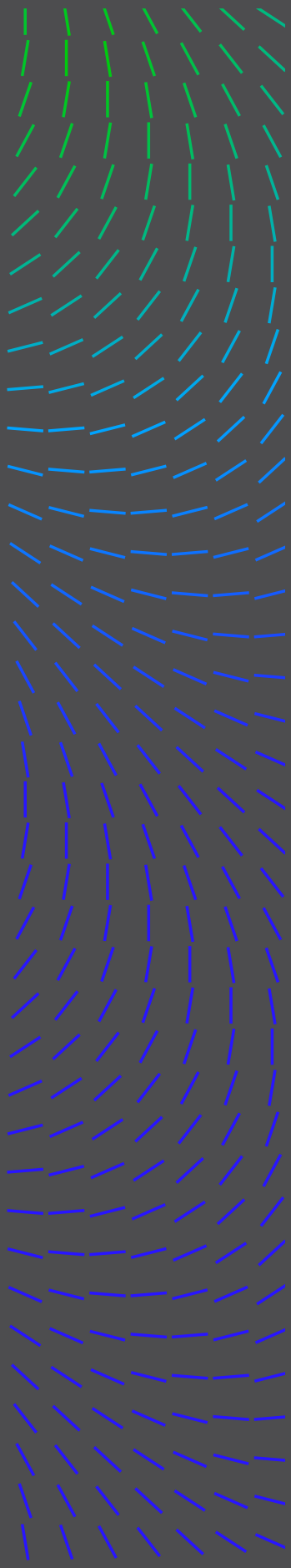
November 2025

エグゼクティブサマリー

2025年4月1日から9月30日にかけて、オペレーショナルテクノロジー（OT）および産業用制御システム（ICS）は、高度な攻撃者による前例のない脅威に直面しました。Trellixのテレメトリ（観測データ）は、572のユニークカスタマー（顧客）にわたり272,512件のOT/ICS関連の脅威を検出しました。

さらに、333件のランサムウェア攻撃が特に重要インフラセクターを標的としました。

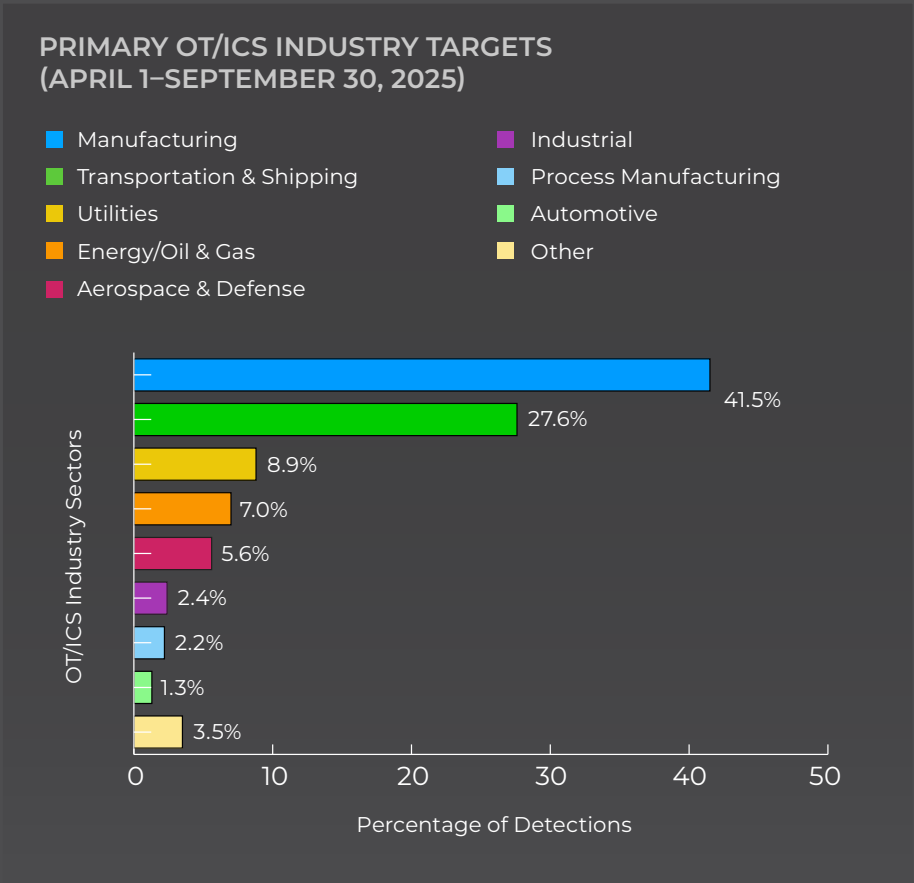
この脅威の状況は、国家が支援する攻撃者やランサムウェアグループによる協調的な攻撃活動（キャンペーン）を明らかにしており、製造、運輸・海運、公共事業、およびエネルギー・石油・ガスセクターが最も高いリスクを負っています。注目すべき脅威アクター（攻撃者）には、Sandworm Team、Qilinランサムウェア、および安全システムを標的とするTEMP.Velesのような専門グループが含まれます。



OT THREAT LANDSCAPE OVERVIEW

世界のOT（オペレーショナルテクノロジー）の脅威環境は、地政学的な緊張と産業システムのデジタル化の促進によって、著しく深刻化しています。ロシア、イラン、北朝鮮の国家が支援する攻撃者は、重要インフラへの標的を拡大しており、一方でランサムウェアグループはOT環境に特化した能力を開発しています。

製造業は主要な標的として浮上し、全検出件数の41.5%を占めました。この集中は、グローバルサプライチェーンにおける同セクターの重要な役割と、しばしば不十分なOTセキュリティ対策を反映しています。運輸・海運は検出件数で2番目に多く27.6%を占め、公共事業、エネルギー・石油・ガス、そして航空宇宙・防衛産業は合わせて21.5%を占めました。.



この内訳は、OT/ICS産業の組織において、OT環境自体から検出されたものではなく、主としてITインフラストラクチャ内で検出された脅威を表しています。メール（55.6%）、ネットワーク境界（25.4%）、およびエンドポイント（18.5%）の各環境にわたるこれらの検出は、産業セクターを標的とする脅威に対する極めて重要な可視性を提供します。というのも、ITシステムの侵害が、接続されたOTシステムに影響を与えうる攻撃の主要な侵入経路としてしばしば機能するためです。

地政学的要因が、標的選定のパターンに著しい影響を与えました。ロシア関連のグループはウクライナのエネルギーインフラに焦点を当て、一方でイランの攻撃者は地域の石油化学施設に集中しました。ウクライナで進行中の紛争は、産業システムに対するサイバー能力の兵器化を加速させています。

THREAT ACTOR ACTIVITY

Sandworm Team (Russia, GRU Unit 74455)

プロフィール
Sandworm Team（別名: BlackEnergy, Voodoo Bear, Iron Viking）は、OT環境を標的とする、最も攻撃的かつ有能な国家支援の脅威アクター（攻撃者）の一つであり続けています。ロシアのGRU（ロシア連邦軍参謀本部情報総局）の特別技術メインセンター（GTsST、部隊番号74455）によって運営されるSandwormは、ロシアのハイブリッド戦争戦略の一環として、サイバーフィジカル（サイバーと物理空間の連携）妨害活動を専門としてきました。

活動と戦術
2022年から2025年にかけて、Sandwormは産業分野の脅威テレメトリ（観測データ）を席巻し、観測されたOT関連侵入のほぼ3分の1を占めました。彼らはウクライナのエネルギー、電気通信、政府のネットワークに対する組織的な攻撃活動（キャンペーン）を継続し、変電所を停止させるためにIndustroyer2を展開したほか、システムデータを消去して復旧作業を妨害するために、CaddyWiper、NikoWiper、ORCSHREDといった複数の破壊的なワイパー（データ消去マルウェア）を使用しました。彼らの作戦はしばしば物理的な軍事行動と同時に行われており、サイバー戦争と通常戦争の連携が示唆されます。

影響と見通し
Sandwormの攻撃活動は、ICS（産業用制御システム）を標的とするための反復可能でモジュール化された攻撃モデルを実証しており、国家レベルのOT脅威における基準（ベンチマーク）として位置づけられています。このグループによるワイパーファミリーの持続的な進化と、ITおよびOTプロトコルの両方の悪用は、継続的な研究開発（R&D）投資を示しています。彼らの活動は、紛争が起こりやすい地域において、レジリエンス（回復力）を重視した防御、迅速なシステム復旧、オフラインバックアップ、およびアウトオブバンド（帯域外）通信の必要性を改めて浮き彫りにしています。

TEMP.Veles / XENOTIME (Russia-linked, Safety Systems Focus)

プロフィール
TEMP.Veles（XENOTIMEとしても追跡されている）は、TRITON（別名 TRISIS または HatMan）マルウェアの背後にいる、ロシア関連の可能性があるエリート級のアクター（攻撃者）です。彼らは、安全計装システム（SIS）、具体的には産業プラントにおける壊滅的な障害を防ぐために使用される Triconex 製コントローラーを侵害することを専門としています。

活動と戦術
彼らの代表的な侵入事例である2017年のサウジアラビアの石油化学施設に対する攻撃は、物理的な損害や人命の損失を引き起こすために、安全コントローラーを再プログラムすることを目的としていました。それ以来、TEMP.Velesは、世界中のエネルギーおよび化学施設において、偵察および持続化（潜伏）活動を行っているところが観測されています。彼らは、OT環境へ横展開（ラテラルムーブメント）するために、エンジニアリングワークステーションやシステムインテグレーターの認証情報を悪用します。彼らの作戦には、ITの悪用とOTプロトコルの操作を組み合わせた多段階の侵入が含まれており、プロセスに関する深い理解を実証しています。

影響と見通し

TEMP.Veles/XENOTIMEは、安全システムを直接的に破壊しようと試みた唯一のアクター（攻撃者）であり、既知のOT（オペレーショナルテクノロジー）の敵対者の中で最も技術的に高度な存在であり続けています。彼らが継続している偵察活動は、将来起こりうる妨害工作（サボタージュ）のために、不測の事態に備えたアクセス（コンティンジェンシー・アクセス）を維持する意図を示唆しています。防御側にとって、このグループの存在は、安全ネットワークを個別に監視し、SIS（安全計装システム）のファームウェアの完全性を監査し、エンジニアリングワークステーションを厳格な変更管理のもとで隔離することの重要性を浮き彫りにしています。

Qilin Ransomware Group (Cybercriminal, OT-targeting Affiliate Network)

プロフィール

Qilin（Agendaとしても知られる）は、産業環境に明確に進出してきている新世代のRaaS（サービスとしてのランサムウェア）オペレーションを代表する存在です。金銭的な動機によるものですが、彼らのオペレーションは、特にエネルギー配給や水処理セクターにおいて、産業の依存関係に関する知識をますます顕著に示しています。

活動と戦術

2024年半ばから2025年にかけて、Qilinは産業組織に対するすべてのランサムウェア活動を主導し、ウガンダ送電公社（Uganda Electricity Transmission Company）やヨーロッパ・アジア各地の複数の水道事業者に対する攻撃を含む、63件の攻撃が確認されています。彼らはしばしば、共有されたエンジニアリングリソース、設定サーバー、ヒストリアンシステム（履歴データ管理システム）を暗号化することにより、ITとOT両方のネットワークを混乱させることが可能なデュアルユース（両用）のペイロード（攻撃コード）を展開します。QilinがWindowsおよびLinuxペイロードを持つAgendaランサムウェアの亜種を使用することで、混在環境内でのクロスプラットフォーム実行が可能になっています。最近、Qilinは日本のアサヒビールに対する攻撃の犯行声明を出しています。

影響と見通し

Qilinは、ランサムウェアを恐喝と業務妨害の両方のツールとして利用し、犯罪的脅威とOT（オペレーショナルテクノロジー）に焦点を当てた脅威との境界が曖昧になっていることを実証しています。彼らの成功は、ランサムウェアオペレーターが、影響力を最大化するために可用性（稼働率）に敏感な環境をいかに悪用するかを学習しているかを浮き彫りにしています。彼らの拡大する活動範囲に対抗するためには、IT SOC（セキュリティオペレーションセンター）とOT防御担当者の間での、セクターを越えた継続的な連携とテレメトリ（観測データ）の共有が不可欠です。

APT33 and APT34 (Iran, Oil and Gas Espionage and Sabotage)

プロフィール

APT33（Elfin）およびAPT34（OilRig）は、2010年代半ばから活動しているイラン国家関連のグループであり、両者ともエネルギーセクターおよび湾岸地域の（イランにとっての）ライバル国に重点を置いています。当初はサイバースパイ活動や認証情報の窃取（クレデンシャル・ハーベスティング）で知られていましたが、両グループとも、その作戦（活動）において徐々に破壊的な要素（コンポーネント）を取り入れるようになってきました。

活動と戦術

APT33は、航空、石油化学、製造業のネットワークを標的とし、後続のアクセス（フォローオン・アクセス）のために知的財産や認証情報を盗み出してきました。APT34は、フィッシングや外部公開インフラ（Web-facing infrastructure）の悪用を通じて、エネルギーおよび政府機関の環境において持続的な足がかり（潜伏拠点）を維持しています。その後の攻撃活動（キャンペーン）では、両グループはデータ損失とダウンタイム（システム停止）を引き起こすために、ShamoonおよびZeroCleareワイパー（データ消去マルウェア）を展開しました。彼らの使用するツール群は、インフラの共有や目的の重複を伴いながら、その成熟度が高まっていること、また活動の手口（トレードクラフト）が部分的に収束していることを示唆しています。イランのサイバー能力に関するさらなる詳細は、我々が公開している調査レポートでご覧いただけます。

影響と見通し

イランの作戦（活動）は、日和見的なスパイ活動から、しばしば地政学的な緊張と時期を合わせた戦略的なサイバー威圧へと進化してきました。彼らの攻撃活動（キャンペーン）が持つ、スパイ活動の後に破壊活動が続くという二重性（デュアルユース）は、防御を特に困難なものにしています。エネルギーセクターの組織にとって、OT DMZ（非武装地帯）における強化されたID管理、ネットワークのセグメント化（分割）、およびエンドポイントのテレメトリ（観測データ）は、引き続き不可欠な緩和策（ミティゲーションレイヤー）です。

Recent Campaigns (2025 Focus)

- **PathWiper (Ukraine, June 2025):** ウクライナのエネルギー事業者を標的とした破壊的な攻撃活動（キャンペーン）であり、Sandwormに関連する可能性があります。ランサムウェアを装いながらデータを永久に消去するように設計されています。これは、ロシアが政治的動機に基づく妨害工作（サボタージュ）を隠蔽するために、「偽装ランサムウェア（pseudo-ransomware）」の使用を継続していることを裏付けるものです。
- **Blue Locker (Pakistan, 2025):** パキスタンの石油・ガス会社に影響を与えたランサムウェアインシデント。攻撃者は、犯罪的動機と地政学的動機を織り交ぜ、現地のベンダー（取引業者）経由でアクセスを悪用し、サードパーティのOT（オペレーショナルテクノロジー）サービスエコシステムの脆弱性を露呈させました。
- **Static Tundra (Global, 2025):** 未パッチのCisco IOSの脆弱性を悪用し、電気通信および製造業のネットワークへのアクセスを獲得する攻撃活動（キャンペーン）。これは、侵害したネットワーク機器をOT（オペレーショナルテクノロジー）セグメントへの横展開（ラテラルムーブメント）の踏み台（ステージング・ポイント）として利用する、高度な持続的攻撃者（APT）によるものとみられる。

Strategic Context

2020年から2025年にかけて、OT（オペレーショナルテクノロジー）の脅威の状況（脅威ランドスケープ）は、国家が関連する散発的な妨害活動から、国家（支援）のアクター（攻撃者）と犯罪アクターの手法や標的が重複し、融合したエコシステム（生態系）へと変化しました。Sandworm TeamやTEMP.Velesのような国家（支援）グループが戦略的な妨害活動を追求する一方で、Qilinのようなハイブリッド（型）グループやランサムウェアグループは、利益のために同じ（侵入）経路を悪用しています。

「侵害されたリモートアクセス」「サプライチェーンの悪用」「ランサムウェアに偽装した破壊的マルウェア」といった繰り返し見られる手口は、スレットインテリジェンス（脅威インテリジェンス）、OTネットワークの可視性、そしてサプライヤーの説明責任を、重要インフラの防御モデルに統合することの緊急性を浮き彫りにしています。

TACTICS, TECHNIQUES, PROCEDURES (TTPS)

最も蔓延している攻撃テクニックは、IT（情報技術）とOT（制御技術）の境界を標的にし、不十分なネットワークセグメンテーション（分離）を悪用するものです。PowerShellが主要な攻撃ベクトル（攻撃経路）として浮上し（96,061件の検出）、次いで、侵害後の活動（ポストエクスプロイテーション）のためにCobalt Strike（85,986件の検出）が続きました。

MITRE ATT&CK for ICS Mapping

- T1046 – ネットワークサービススキャン: 産業用プロトコルの発見
- T1021.002 – SMB/Windows管理共有: エンジニアリングワークステーションへのラテラルムーブメント（横展開）
- T1078 – 有効なアカウント: 侵害されたエンジニアリング用認証情報
- T1485 – データ破壊: プロセスデータと安全システムの標的化
- T1489 – サービス停止: 安全システムの不正操作

ITからOTへの（侵入の）足がかりの移動は、侵害されたエンジニアリングワークステーション、共有された認証情報、およびリモートアクセスソリューションの悪用を通じて発生します。攻撃者は、正規の産業プロトコル（Modbus、DNP3、IEC 61850）を悪用して、悪意のあるコマンドを通常の操作に紛れ込ませ、検出を困難にします。

高度な（技術を持つ）グループは、電力変電所のスイッチを直接制御するためのIndustroyerや、安全システムを操作するためのTRITONのような専門的なツールを配備します。これらの能力は、従来のITに焦点を当てた攻撃から、物理的な損害を引き起こすことが可能なオペレーション（活動）へと、（脅威が）著しくエスカレート（深刻化）していることを表しています。

VULNERABILITY AND EXPOSURE INSIGHTS

レガシーな（旧来の）産業用プロトコルが依然として主要な攻撃対象領域（アタックサーフェス）であり、Modbus、DNP3、および独自のSCADAプロトコルには固有のセキュリティ機能が欠けています。ヒューマン・マシン・インターフェース（HMI）とエンジニアリングワークステーションは、ITとOTのデュアルネットワーク接続（両方に接続されていること）により、しばしば（攻撃の）足がかり（ピボットポイント）として機能します。

オペレーショナル（運用）な階層構造を枠組みとして示すため、このレポートではISA-95/Purdueモデル（パデューモデル）を参照します。このモデルでは、レベル4/3がエンタープライズ（企業システム）および製造オペレーション管理（MES）システムを含み、レベル2が監視制御（HMIおよびSCADA）、レベル1/0が物理的なコントローラーとセンサー（PLC）を対象としています。

プログラマブル・ロジック・コントローラー（PLC）は、ますます標的とされており、特にシュナイダーエレクトリック社のTriconexシステム（TRITON攻撃）やシーメンス社のコントローラーが狙われています。VPNやリモートデスクトッププロトコルを含むリモートアクセスソリューションは、不適切に保護されている場合、初期侵入ベクトル（経路）となります。

ベンダーの対応時間は著しく異なり、OTの重大な脆弱性は、運用上の制約により、パッチ適用サイクルが長期化することがしばしばあります。OT環境において脆弱性が公開されてからパッチが適用されるまでの平均時間は180日を超えており、これは従来のITシステムの30日と比較されます。

現在のOT（オペレーショナルテクノロジー）の脅威の状況（脅威ランドスケープ）を決定づける最も重要な傾向は、ITとOTの境界（接点）に戦略的な焦点が当てられていることです。脅威アクター（攻撃者）は、低レベルのコントローラーを直接標的にすることに伴う固有の困難さと検知されるリスクの高さを認識し、その代わりに、ネットワーク間の橋渡しをするレベル3およびレベル4のシステムを侵害することを優先しています。

これらの境界デバイスや産業用ソフトウェアプラットフォームは、（リモートアクセスツールやエンタープライズアプリケーションにおけるRCE＝リモートコード実行のような）ITによくある脆弱性を介して、より容易でスケーラブルな侵入経路を提供する一方で、非常に「キネティック（物理的）」なOT上の結果をもたらします。すなわち、生産データの操作、安全制御の無効化、あるいは制御プレーン（制御層）全体にわたる広範な機能停止を引き起こす能力です。このような動向は、運用の完全性（オペレーショナル・インテグリティ）を維持するために、境界防御（ペリメータディフェンス）が今やこれまで以上に重要になっていることを意味します。

以下に詳述する特定のCVE（共通脆弱性識別子）の例は、網羅的なリストとして意図されたものではなく、むしろ2025年の第2四半期（Q2）および第3四半期（Q3）の期間中に公開され、活発に悪用された影響の大きな脆弱性の代表的なケースとして挙げるものです。これらの事例は、現代の脅威アクターの焦点が、産業エコシステム内の戦略的な（攻撃の）足がかり（ピボットポイント）へと移行していることを、総じて示しています。

1. Exploitation in Perimeter and Remote-access Devices

OT（オペレーショナルテクノロジー）ネットワークのセグメント化（分離）や、そこへのリモートアクセスを提供するために頻繁に使用される主要なネットワークインフラ機器が、絶え間ない攻撃にさらされていました。これらの欠陥（脆弱性）を悪用されると、認証なしで内部ネットワークへのルートレベル（管理者権限）のアクセスが可能になってしまいます。

- Cisco ASA/FTD ゼロデイキャンペーン (CVE-2025-20333 & CVE-2025-20362): 「ArcaneDoor」活動に関連するとされる国家支援の脅威アクター（攻撃者）が、2025年第3四半期にCisco ASAおよびFirepower Threat Defense (FTD) デバイスにおける一連のゼロデイ脆弱性を活発に悪用しました。この攻撃活動（キャンペーン）により、ファイアウォール自体への認証なしのアクセスとリモートコード実行（RCE）が可能となり、攻撃者は再起動後も持続性（永続性）を確保するためにデバイスのファームウェア（ROMMON）さえも改ざんしていました。

  OTリスクとの関連: これらのデバイスはネットワーク境界を形成しています。これらが侵害されることは、主要なセグメンテーション（分離）防御が完全に無効化されることを意味し、攻撃者は（横展開や偵察のために）OTネットワークセグメントへの制限のないアクセスを得ることになります。これは、ネットワーク防御の直接的な喪失に直結します。

- Erlang/OTP SSH RCE (CVE-2025-32433): 多くのネットワーキングコンポーネントやOTアプライアンスに見られるErlang SSHライブラリのこの欠陥（CVSS 10.0）は、認証されていないリモートの攻撃者によるコード実行を可能にしました。2025年第2四半期には、公開されているポートを標的とした悪用の試みが観測されました。

  OTリスクとの関連: OT環境における多くの堅牢化された（hardened）Linuxベースの制御サーバー、データヒストリアン、通信ゲートウェイは、管理インターフェースとしてErlang/OTPに依存しています。これらのシステムに対する認証なしのリモートコード実行（RCE）は、制御ネットワーク内部への特権的な足がかりを提供することになり、（ヒストリアンデータの改ざんによる）「視界の喪失（loss of view）」や、即時の（侵入拡大の）足がかり（ピボットポイント）となる可能性につながります。

2. Compromise of IT-integrated Industrial Software

ビジネスシステム（ERP）と製造プロセス（MES）を連携させるソフトウェアの脆弱性は、中核となるOT（オペレーショナルテクノロジー）環境への（侵入のための）特権的な足がかり（ピボットポイント）として機能します。

- SAP NetWeaver RCEチェーン (CVE-2025-31324 & CVE-2025-42999): SAP NetWeaverのVisual Composerにおけるこれら一対の重大な脆弱性は、2025年第2四半期を通じて、複数のランサムウェアおよびスパイ活動グループ（QilinやBianLianを含む）によって活発に悪用されました。OTリスクとの関連: SAP NetWeaverは、生産スケジューリング、部品表（BOM）、および品質管理データの主要な供給源であり、それらのデータは製造実行システム（MES）に直接送られます。このプラットフォームが侵害されると、攻撃者は中核となる生産データを巧妙に汚染（poison）または妨害（disrupt）することが可能になり、バッチエラー、品質不良、または予期せぬ運用停止（完全性および制御の喪失）を引き起こす潜在的な可能性があります。

- Dassault DELMIA Apriso RCE (CVE-2025-5086): DELMIA Apriso Manufacturing Operations Management (MOM) ソフトウェアにおけるこの重大なRCE（リモートコード実行）の欠陥は、実際の環境（in the wild）での悪用が確認されたため、2025年第3四半期にCISA KEV（既知の悪用された脆弱性）カタログに追加されました。OTリスクとの関連: MES/MOMプラットフォームとして、Aprisoは資産、労働力、プロセスフローを追跡し、工場フロア全体を統括（オーケストレート）しています。このサーバーでのRCEは、攻撃者が産業ワークフローを駆動するシステム（＝Apriso）の制御権を握ることを意味し、それにより（生産レポートの偽装による）可視性の喪失、および制御システムへ悪意のあるコマンドを発行する可能性（制御の喪失）につながります。

3. High-risk Direct OT Device Disclosures

これらの重大な欠陥（脆弱性）はコントローラー自体を標的とするものであり、ベンダー製品ラインに内在するリスクと、パッチ適用が不可能なOT（オペレーショナルテクノロジー）インフラがもたらす長期的な脅威を表しています。

- Rockwell ControlLogix RCE (CVE-2025-7353): ControlLogixイーサネットモジュールにおける重大な脆弱性。これにより、認証されていない攻撃者が、意図せず（公開されている）Webベースのデバッガエンドポイントを悪用することで、RCE（リモートコード実行）を達成できます。OTリスクとの関連: イーサネットモジュールは、PLC（プログラマブル・ロジック・コントローラー）シャーシの通信の「背骨（スパイン）」です。ここでRCEを達成すると、攻撃者はプロセッサへの通信を改ざん、または停止させることが可能になります。これにより、エンジニアリング用の認証情報を必要とせずに、悪意のあるロジック（制御プログラム）の注入や安全機能の無効化が容易になります。

- Rockwell DoS 脆弱性 (CVE-2025-24478 & CVE-2025-9166): GuardLogixおよびControlLogix PLCにおいて、認証されていないリモートの攻撃者が、重大な回復不能障害（MNRF）またはサービス拒否（DoS）状態を引き起こすことを可能にする、複数の深刻度の高い欠陥（脆弱性）。OTリスクとの関連: これは可用性を直接的に侵害し、コントローラーを（解決に物理的な電源の再投入が必要となる）フェイル状態（障害停止状態）に強制します。連続プロセス環境（連続生産プロセス）においては、これは即時の、計画外の生産シャットダウン、原材料の廃棄（仕損）、および重大な経済的影響につながります。

- ABB ASPECT 認証バイパス (CVE-2025-53187): ABB ASPECTシステムにおける重大な（CVSS 9.8）欠陥（脆弱性）であり、認証されていない攻撃者がセキュリティをバイパスし、管理者制御（権）を獲得することを可能にする。OTリスクとの関連: ASPECTはビル管理システム（BMS）または制御管理システム（CMS）である。（システムが）侵害されると、物理的な施設インフラ（HVAC＝空調、換気、電力管理）に対する制御権が（攻撃者に）与えられる。この制御（権）は、安全上のリスク（例：クリーンルームの気圧操作）のために悪用されたり、あるいはアクセス制御（入退室管理）を解錠して物理的な侵入を容易にするために悪用されたりする可能性がある。

Key Takeaways

- ゼロトラスト・ベンダー・アクセス: 長期的なインテグレーターやOEM（相手先ブランド製造メーカー）からの接続を含め、すべての外部接続を「信頼できないもの」として扱ってください。すべてのリモートメンテナンスに対し、粒度の細かい（きめ細かな）、時間制限付きの認証情報（の利用）とセッション監視を徹底してください。

- ソフトウェア保証とSBOM（ソフトウェア部品表）の可視性: ベンダーに対し、ソフトウェア部品表（SBOM）の提供、デジタル署名の検証、およびアップデートに含まれる改ざんされた、あるいは古いコンポーネントの監視を要求する。

- ベンダーの説明責任: サプライヤーとの契約にサイバーセキュリティ条項を盛り込み、安全なアップデート慣行、脆弱性の開示、およびOT環境に影響を与えうるインシデントの即時報告を義務付ける。

- ネットワークのセグメント化（分離）と継続的監視: サプライヤー向けのゲートウェイを本番（生産）ネットワークから確実に隔離し、不正なデータ交換やコマンド活動を示唆する可能性のあるアウトバウンド（外部行き）トラフィックに対する可視性を維持する。

- 脅威インテリジェンスの共有: （ISACやISAOなどの）セクター（分野）別の情報共有に参加し、業界内の同業他社や上流プロバイダーに影響を与えるサプライチェーンの侵害を迅速に特定する。

HISTORICAL CASE STUDIES

1) 2024 – Cyber Av3ngers Target Unitronics PLCs (Water and Other Sectors, U.S.)

2023年後半から2024年にかけて、Cyber Av3ngersとして知られるイラン関連のグループが、水道・廃水セクターやその他の小規模な産業環境において、インターネットに公開されていたUnitronics社製PLCを悪用しました。攻撃者はHMI（ヒューマン・マシン・インターフェース）の画面を政治的なメッセージで改ざんし、場合によってはPLCのロジック（制御プログラム）を変更しました。これは、デフォルトの認証情報（パスワード）とインターネットへの直接公開がもたらすリスクを浮き彫りにしました。米国のいくつかの公益事業者が影響を受け、CISA（サイバーセキュリティ・インフラストラクチャセキュリティ庁）およびWaterISAC（水関連情報共有分析センター）による全国的な勧告が発令される事態となりました。

得られた教訓: 制御デバイスのインターネットへの直接アクセスを排除すること、ベンダーのデフォルトパスワードを変更すること、メンテナンスアクセスにはネットワークのセグメント化（分離）とVPNゲートウェイ（の使用）を徹底すること、そして不正なロジックや設定の変更がないか継続的に監視すること。

2) 2022 – Industroyer2 Attempt on Energy Infrastructure (Ukraine)

2022年4月、ロシアのSandworm Teamは、2016年に送電網を攻撃したマルウェアの後継であるIndustroyer2を、ウクライナの高圧変電所に対して展開しました。CERT-UA（ウクライナのCERT）とESET社による迅速な防御活動により、停電は阻止されました。このマルウェアのモジュール設計と（IEC-104といった）ネイティブなOTプロトコルの使用は、国家（支援）アクターが物理プロセスを直接操作するための攻撃能力を保持していることを実証しました。

得られた教訓：エネルギー事業者は、厳格なアローリスト（許可リスト）、シリアルインターフェースの保護、およびアクティブなプロトコル検査によって、変電所ネットワークを堅牢化しなければなりません。迅速な封じ込めと復旧のためには、OEM（機器メーカー）や国のCSIRT（シーサート）との合同インシデント対応演習が引き続き不可欠です。

3) 2021 – Colonial Pipeline Ransomware Incident (U.S.)

2021年5月、DarkSideランサムウェア（グループ）の活動がColonial Pipeline社の企業のITシステムを攻撃し、（OT側への）横展開を防ぐために、OTオペレーション（操業）の予防的なシャットダウンを余儀なくされました。5日間にわたる（操業）停止は、東海岸の燃料供給の45%を停止させ、連邦政府の緊急事態宣言の発令に至りました。OTネットワークが直接暗号化されたわけではありませんでしたが、ビジネス（IT）機能と操業（OT）機能間の相互依存性が、復旧を複雑にしました。

得られた教訓：ITとOTの間にレジリエントな（障害耐性のある）インターフェースを構築すること、手動操作や再起動計画の訓練を行うこと、そして安全なプラント機能を停止させることなくITシステムを隔離できるインシデント対応（体制）を確保すること。

4) 2021 – Oldsmar Water Utility Intrusion (Florida, U.S.)

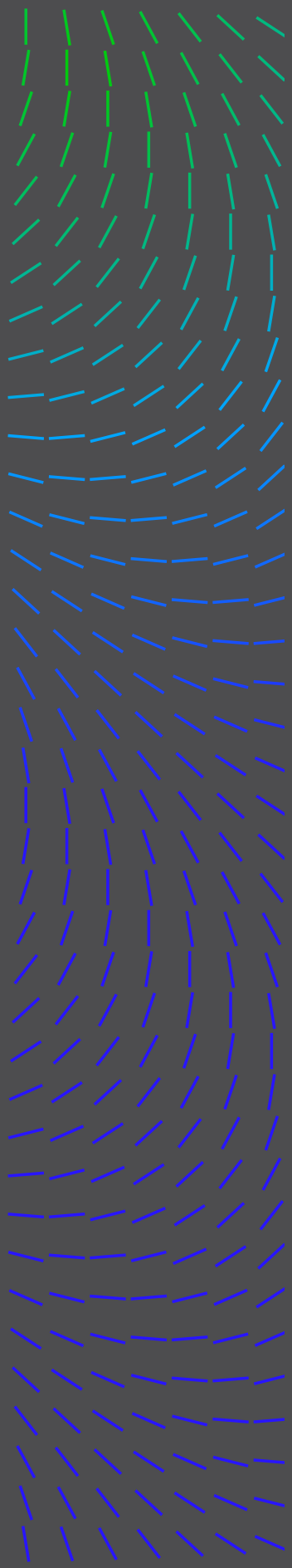
2021年2月、未知の攻撃者がTeamViewer経由でOldsmar浄水場のSCADA HMIにアクセスし、化学薬品の注入設定を一時的に危険なレベルに変更しました。オペレーターがそれに気づき、変更を元に戻したため、被害は防がれました。被害は発生しなかったものの、このインシデントは、小規模な公益事業者に共通するリモートアクセスの脆弱な管理体制を露呈させました。

得られた教訓：リモートコントロールソフトウェア（の使用）を制限すること、多要素認証を要求すること、HMIの活動（ログ）を記録すること、そして（通常とは異なる）プロファイル外の設定値（が入力された場合）に対するプロセスアラームを設定すること。

5) 2020 – Natural Gas Compression Facility Ransomware (U.S.)

2020年初頭、ランサムウェアが米国の天然ガス圧縮施設の制御・通信資産を妨害し、2日間のシャットダウンとサプライチェーンの遅延を引き起こしました。この攻撃は、不十分なネットワークセグメンテーション（分離）と認証情報の共有が原因で、ITからOTへと拡散しました。

得られた教訓：堅牢なIT/OTセグメンテーション（分離）を実装すること、エンジニアリングワークステーションとコントローラー設定の定期的なバックアップを行うこと、そして包括的なOTインシデント対応訓練を実施すること。



Sector context and takeaways (2020–2025)

ここ5年間で、オペレーショナルテクノロジー（OT）への攻撃は、偶発的なIT（システム）からの波及から、犯罪者と国家支援のアクター（攻撃者）両方による重要インフラへの意図的な標的化へと進化しました。エネルギーセクターと水（インフラ）セクターがその矢面に立たされており、ランサムウェアによる業務妨害、リモートアクセスの悪用、サプライチェーンの弱点といった（攻撃）テーマが（共通して）見られます。

ウクライナやCyber Av3ngersの事例は、サイバーフィジカルな影響（効果）を通じて（行われる）ハイブリッド戦争や地政学的なメッセージ発信への傾向を浮き彫りにしています。防御側にとって、取るべき必須の対策は明確です。それは、攻撃対象領域（アタックサーフェス）を最小限に抑えた防御可能なOTアーキテクチャを構築すること、オフラインの復旧経路を維持すること、そして物理的な影響が発生する前に検知・対応するために官民の連携を促進することです。

DEFENSIVE POSTURE AND BEST PRACTICES

- ISA/IEC-62443標準に従い、OTネットワーク専用のセキュリティゾーンを設け、IT環境とOT環境の間に制御されたアクセスポイントを設置するなど、堅牢なネットワークセグメンテーション（分離）を実装する。不正なラテラルムーブメント（横展開）を防ぐために、産業用ファイアウォールやデータダイオードを導入する。

- 産業用プロトコルアナライザーや行動分析を用い、OTネットワーク内の異常な通信を検知するための包括的な監視体制を確立する。資産インベントリ（台帳）、脆弱性管理、およびインシデント対応手順に重点を置いた、OT固有の制御（対策）を取り入れたNISTサイバーセキュリティフレームワークを導入する。

- 多要素認証、特権アクセス管理、およびセッション監視を通じて、リモートアクセスを保護する。計画されたメンテナンス期間中にOTシステムのアップデートとパッチ適用を定期的に行い、本番環境への導入前に隔離された環境で徹底的なテストを実施する。

- 安全性の考慮事項と運用継続性の要件を考慮に入れた、OT固有のインシデント対応手順を策定する。産業用制御システムに関連する特有のリスクとサイバーフィジカル攻撃の可能性を強調し、運用スタッフに対してサイバーセキュリティ意識向上トレーニングを実施する。

CONCLUSION

2025年4月から9月の期間は、OT/ICS（オペレーショナルテクノロジー/産業用制御システム）を標的とする攻撃の増加を示し、高度な脅威アクター（攻撃者）が産業環境向けの（攻撃）能力を開発していることが明らかになりました。製造業およびエネルギーセクターへの攻撃の集中は、安全システムを標的とする（攻撃の）出現と相まって、世界のインフラに対する重大な脅威となっています。

組織は、OTセキュリティへの投資を優先し、産業システム特有の運用要件を考慮に入れた多層防御戦略を実行しなければなりません。日和見的な攻撃から安全システムに対する標的型攻撃活動（キャンペーン）へと（脅威が）進化したことで、人命の損失や広範な経済的混乱につながりかねない潜在的な壊滅的インシデントを防ぐため、即時の対応が求められています。

See more threat reports from Trellix Advanced Research Center.