DRAGOS

2025年版
OTサイバーセキュリティレポート

～地政学的緊張の中で進化する脅威と有効な防衛アプローチ～

8TH ANNUAL
YEAR IN REVIEW
2025

OT/ICS
CYBERSECURITY
REPORT

この資料は Dragos 社による OT サイバーセキュリティの 2025 年レビュー (原文: OT Cybersecurity THE 2025 YEAR IN REVIEW) であり、OT サイバーの最新動向を伝えるため極力原文通りに翻訳しています。OT サイバーセキュリティ対策の参考になれば幸いです。

株式会社マクニカ　OT サイバーセキュリティ技術チーム

MACNICA

CONTENTS

イントロダクション

Dragosは1年を通じて、OT（運用技術）およびICS（産業用制御システム）インフラに対する脅威を特定し、防御側のセキュリティ体制を支援するサービスを提供し、安定した運用のための優先対策を明確にしてきました。テレメトリデータや現場経験に基づく実践的知見を活かし、第8回目となる年次報告書「Year in Review」をまとめました。本レポートでは、Dragosが確認した重要な攻撃経路の具体例、それら攻撃の背景にある動機や状況についても詳細に解説しています。

OT/ICS サイバーセキュリティの旅を始めたばかりの方：最初に組織のリスクを体系的に特定し、そのリスクを可能な限り低減することから始めましょう。外部に露出した資産に対する脅威については、22 ページの BAUXITE や 35 ページの KurtLar SCADA に関する詳細をご覧ください。

すでに自社のリスクを把握している、リスクを低減する計画を持っている方：本レポートで取り上げている攻撃シナリオが自社にも当てはまるかどうかを検討してみてください。これらのシナリオを参考に、可視化・監視の戦略を見直したり、インシデント対応計画やネットワークのセグメンテーション（分割）の検討に役立ててください。

すでに有効な脅威対策戦略をお持ちの方：次のステップとして、その戦略が実際に機能するかどうかを検証する段階です。本レポートに登場する攻撃シナリオを参考にしながら、自社システムにおける可視化の抜けや盲点がないかを確認しましょう。たとえば、攻撃者がファームウェアをダウングレードした場合、それに気づくことができるでしょうか？　29ページでは、FrostyGoopマルウェアとその一連の攻撃手法について詳しく解説しています。

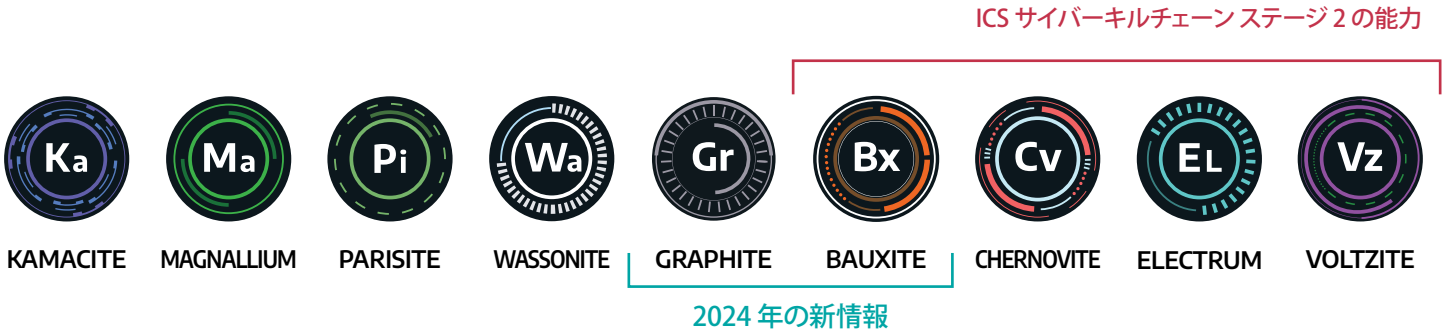
脆弱性管理に不安を感じる方：53ページの「Vulnerability Trends（脆弱性の傾向）」セクションをお読みください。OTの脆弱性管理は、ITとは異なるアプローチが必要です。また、52ページでは「Now, Next, Never（今すぐ・次・やらない）」というフレームワークを通じて、脆弱性への緩和策と修正の優先順位を決定する方法を学べます。

準備を整え脅威の兆候を見つけましょう：ハクティビスト（政治的・社会的主張をもとに攻撃する集団）は自らの存在を主張しますが、私たちはそれ以外にも、ネットワークのノイズにまぎれて行動する攻撃者を継続的に観測しています。13ページの「ELECTRUMによるAcidPour」、14ページの「VOLTZITE」に関する分析をぜひご覧ください。

セキュリティ対策の成熟度にかかわらず、本レポートを読み進めてください：ICSに特化した攻撃グループやハクティビスト、マルウェアを使った攻撃、そして犯罪目的のランサムウェアなど、現実に起きた最新の攻撃事例と、それにどう対応すべきかを学べます。Dragosのインシデント対応チームによる実践知見、脆弱性分析チームからのガイダンスも紹介しており、OT環境や組織が直面する重大なサイバー脅威を包括的に理解できる内容となっています。

主要ハイライト: 数字で見る

Dragos は 23 の脅威グループを追跡しており、そのうち 9 つが 2024 年に活動していました。



主要な脆弱性の発見

70%

脆弱性の 70% は、ネットワークの奥深くに存在しています。

22%

2024 年の勧告の 22% は、ネットワークを介して悪用可能であり、境界に面していました。

39%

Dragos が分析した勧告の 39% は、「可視性の喪失」と「制御の喪失」の両方を引き起こす可能性がありました。これは前年の 53% から低下しました。

22%

2024 年の勧告の 22% に誤ったデータが含まれていました。

47%

Dragos は、対策が示されていなかった勧告の 47% に対し、緩和策を提供しました。

主要なランサムウェアの発見

87%

産業組織に対するランサムウェア攻撃は、前年より 87% 増加しました。

60%

Dragos は、2024 年に OT/ICS に影響を与えたランサムウェアグループを 60% 多く追跡しました。

69%

全ランサムウェア攻撃の 69% が、26 の異なる製造サブセクターに属する 1,171 の製造業組織を標的としていました。

使用される OT プロトコル

Modbus
CIP
FINS
OPC/UA
CODESYS
Meter-bus
S7comm

使用される IT プロトコル

SSH
HTTP
IMAP
RDP
HTTPS
WebDAV (over HTTPS)
VNC
PPTP

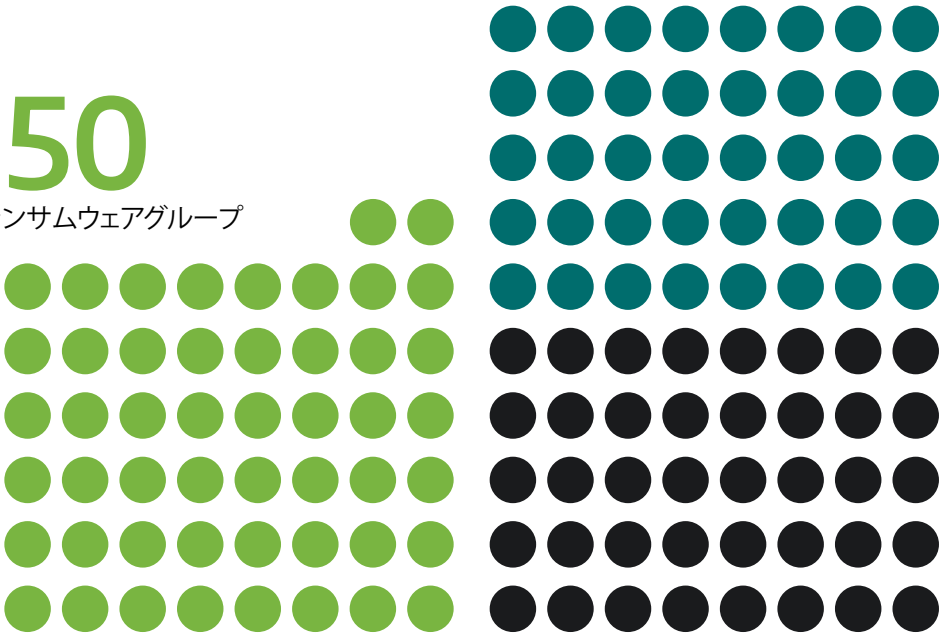
標的とされた産業

電力
石油・ガス
防衛産業基盤
製造業
通信
海運
水道・下水道
食品 & 飲料
化学製造
採掘
交通 & 物流

ランサムウェアグループ

80
2024 年のランサムウェアグループ

50
2023 年のランサムウェアグループ



50%
製造業を標的

現在の脅威情勢に関する防御側のガイド

2024年のサイバーセキュリティの脅威情勢は、激化する地政学的緊張、およびそれが世界中の産業オペレーションと交差することによって形成されました。
成熟した脅威グループによる持続的なキャンペーンから、ハクティビストやランサムウェアオペレーターによる機会的な攻撃まで、攻撃者はOT（運用技術）およびICS（産業用制御システム）環境を目標達成のための攻撃経路として意識するようになっています。
高度化・多様化する脅威の情勢を受けて、防御側に対し、OT/ICSネットワークに対する可視性とレジリエンスの強化への圧力が高まったことが明確になった一年でした。

OTを狙う攻撃者：巧妙さより"把握されている"ことが脅威に

2024年に顕著だった傾向の一つは、OT/ICSを標的とする攻撃者にとっての「参入障壁」が一層低下したことです。これまでOT/ICSに無関心だった、あるいはその存在を知らなかった攻撃者までもが、今やそれを効果的な攻撃ベクトルとして捉え、混乱の発生や注目の獲得に利用しています。
たとえば、2024年4月に明らかになったブラックジャックのマルウェア「Fuxnet」は、ICS専用マルウェア「PIPEDREAM」などと比べると粗削りながら、OTネットワークへの破壊的攻撃がいかに大きな影響を与えるかに対する認識が広がっていることを示しています。
同様に、ハクティビスト「CyberArmyofRussia_Reborn（CARR）」が2024年を通じて展開した、インターネットに公開されたOTデバイスを標的とするキャンペーンでは、たとえ基本的な手法――たとえばインターネット越しに遠隔からHMI（ヒューマン・マシン・インターフェース）の設定を操作するような攻撃――であっても、実際の業務に支障をきたすほどの影響を及ぼすことが可能だということが明らかになりました[1]。

この変化は、OTに対する技術理解の深まりを示すのではなく、むしろOTが攻撃者の目的を達成するための有効手段として広く認識されるようになったことを反映しています。ランサムウェア攻撃者にとって、製造環境を標的にすることでダウンタイムを引き起こし、被害者に身代金を支払わせる圧力を直接的にかける手段になっています。ハクティビストにとっては、OTを標的にすることで自らのメッセージを迅速かつ破壊的に拡散する方法となりました。これらの攻撃は、我々に重要な現実を再確認させます。「影響を与える結果を達成するため、必ずしも高度な手法は必要ない。攻撃者の数が増えることで全体のリスクが拡大する」ということです。

こうした「シンプルさ重視」は、防御側にとって重要な視点を浮き彫りにします。SANS ICS 5 Critical Controlsの効果的な実施、それこそがOTを狙う攻撃者に対し最も有効な防御手段であるということです[2]。
インシデント対応能力が強化され、防御可能なアーキテクチャを持ち、セキュアなリモートアクセスプロトコルを採用し、堅牢なネットワーク監視体制を整えている組織は、たとえこのように複雑化した環境であっても、自社のOTが攻撃を受けるリスクを大幅に低減することが可能なのです。

防御側の進展：段階的に進んでいるがバラつきは大きい

防御側はOTセキュリティの重要性を理解しつつありますが、その進展は業界や地域によって不均一です。北米の電力業界のような規制の厳しい業界は、規制が比較的緩やかな水道事業や製造業などの分野よりも成熟度が高いことを示しています。Dragosのコミュニティ防御プログラム（CDP）のような取り組みは認識の向上に寄与していますが、OT環境に対する可視性は、攻撃者の戦術に遅れをとっている場合が多いのが現状です[3]。

進展の不均一性を示す例として、多くの組織がセキュアなリモートアクセスを導入していますが、サードパーティやレガシー接続を発見するための内部ネットワーク監視や可視性が不足しているため、ネットワークの侵害リスクにさらされています。
一例として、Dragosチームは、ある組織のOTネットワーク内に存在するレガシーなベンダー接続について、ランサムウェアグループが

[1]ロシア軍系ハッカー、米国の水道インフラへの破壊活動を主張 [2]世界水準のOTサイバー対策重要５項目 [3]Dragos集団防衛プログラム

そのベンダーを侵害する数週間前に特定しました。レガシー接続を削除することで、その組織はベンダーの侵害されたネットワークからの被害を防ぐことができました。

更にDragosのサービス支援では、仮想プライベートネットワーク（VPN）からインターネットへの直接接続、セキュリティ設定が不十分な非武装地帯（DMZ）、企業内での即席作業（一時作業）を特定できるような可視性や監視が不足しているケースが頻繁に観察されています。

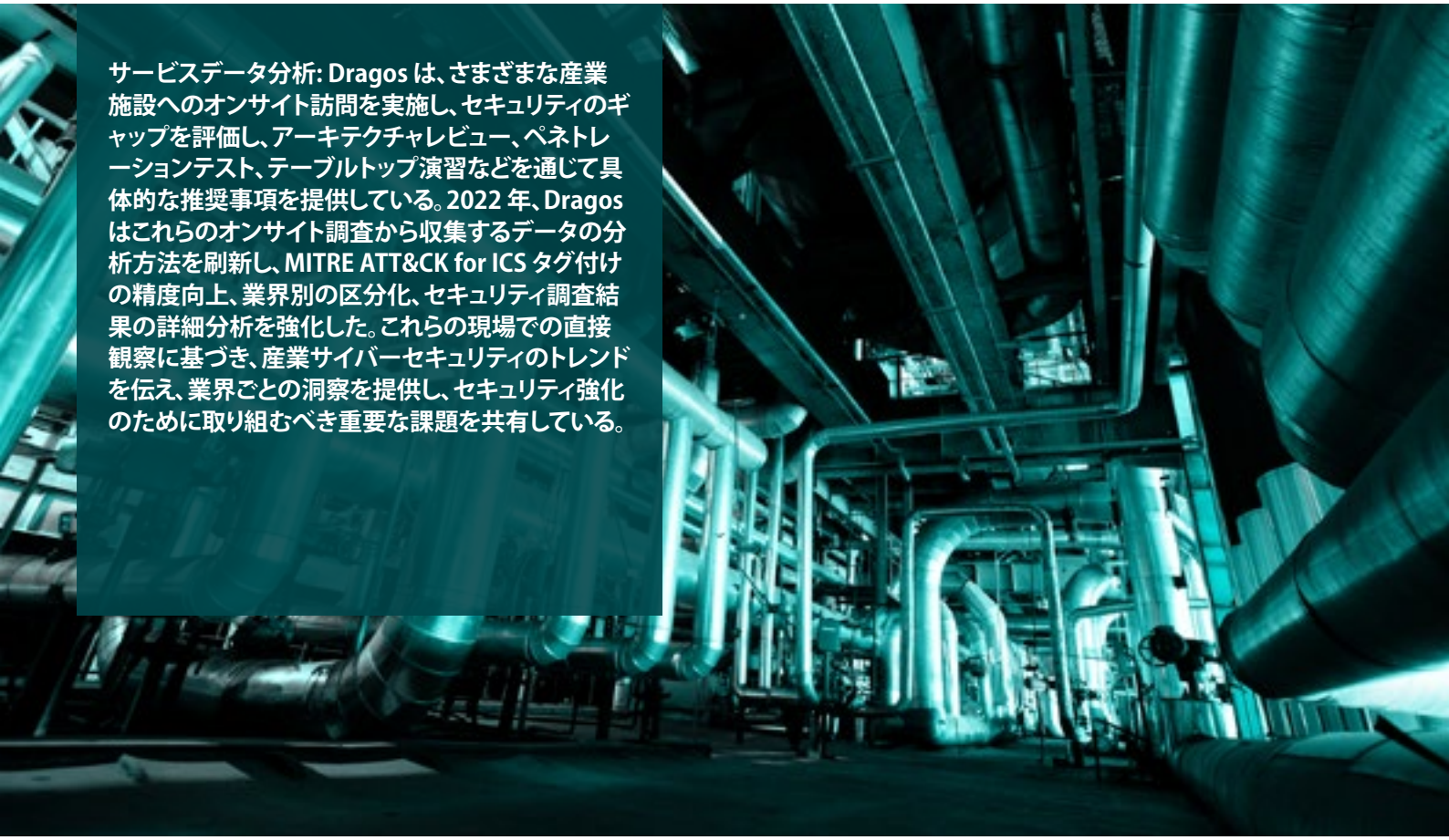
可視性の欠如は、自社ネットワーク内部の攻撃経路を把握できないことに加え、外部から見たアタックサーフェスを理解できない根本的な原因にもなっています。その結果、Shodan や Censys のようなツールを使って、インターネット上に露出しているデバイスを発見しようとする場当たり的な攻撃者に対して無防備な状態をつくります。

2024年において、OTを標的とした攻撃で最も多く悪用された経路のひとつがインターネットに露出したICSデバイスです。「自分たちは標的にならないだろう」という危険な思い込みこそが防御側にとって重大な障害ですが、対策リソースや優先度合いに制約を抱える組織では顕著です。

2024年の状況は、OTがもはやニッチな標的ではないことを示しました。OTに対する認知が広まり、初歩的な攻撃手法さえ通用することから、攻撃者の数は拡大、重要インフラの防御はこれまで以上に難しくなっています。

熟練した攻撃者は、重要インフラの中に潜伏し続け、ハクティビストは露出した脆弱なシステムを悪用します。
こうした状況が生まれる背景には、OTがITとは異なる特有の脅威にさらされているという認識が、まだコミュニティ全体に広く浸透していないことがあります。さらに悪いのは、その事実を知りながらも無視したり、脅威を過小評価しているケースさえあることです。

「基本を着実に実施すること」は、今もなお多くの組織にとって最も重要な指針です。
そして今こそ、隠れた脅威を発見し、それを可視化するために一歩踏み出し、積極的に脅威ハンティングに取り組む防御側の姿勢が求められています。



サービスデータ分析: Dragos は、さまざまな産業施設へのオンサイト訪問を実施し、セキュリティのギャップを評価し、アーキテクチャレビュー、ペネトレーションテスト、テーブルトップ演習などを通じて具体的な推奨事項を提供している。2022 年、Dragos はこれらのオンサイト調査から収集するデータの分析方法を刷新し、MITRE ATT&CK for ICS タグ付けの精度向上、業界別の区分化、セキュリティ調査結果の詳細分析を強化した。これらの現場での直接観察に基づき、産業サイバーセキュリティのトレンドを伝え、業界ごとの洞察を提供し、セキュリティ強化のために取り組むべき重要な課題を共有している。

OT を中心としたサイバー作戦、地政学的緊張と紛争継続に伴い増加

ウクライナでは、市営エネルギー企業に対するサイバー攻撃により、数百棟のアパートビルで暖房が停止しました.[4] 。ウクライナに同調したとされる Blackjack グループによる攻撃では、ロシアの重要インフラの監視装置が損傷しました[5] 。親イラン派の CyberAv3ngers は、イスラエルの燃料管理システムを攻撃しました[6] 。2024 年、Dragos は地政学的な対立に関連した攻撃的なサイバー活動が継続していることを確認しました。ハクティビストを含む脅威グループは、それぞれの陣営の目標に沿ったより露骨なサイバー作戦へと移行し、より成熟したグループは破壊的な影響を与えることを目指しました。

ウクライナ・ロシア間の紛争、脅威グループの活動を加速

KAMACITE と **ELECTRUM** は、ロシアの軍事的目的を支援するために引き続き協調し、ウクライナの重要インフラを標的とした活動を展開しています。KAMACITE は被害者のITネットワークに足がかりを築き、その後、OT（運用技術）領域での作戦を ELECTRUM に引き継ぎます。これは、2016年にキーウ地域の一部で一時的な停電を引き起こした「CRASHOVERRIDE」攻撃のような事例でも見られました [7]。

2024年には、KAMACITE は Kapeka バックドアを使用して、暖房・水道・電力など重要インフラを運営するウクライナ国内組織を狙いました。同時に ELECTRUM は、ハクティビストグループと連携して活動をカモフラージュしながら、ウクライナの通信企業 Kyivstar に対するサイバー攻撃を実行しました。

この新たな KAMACITE と ELECTRUM の活動は、ウクライナ・ロシア紛争が OT 関連のサイバー攻撃技術の発展を加速させていることを示しています。

[4] FrostyGoop ICSマルウェアによるOTシステムへの影響 — Dragos社 [5] Fuxnetマルウェアに関する戦略的な見解 — Dragos社 [6] イラン系グループ、米国の重要インフラ攻撃に独自のサイバー兵器を使用 — The Register [7] CRASHOVERRIDE：電力網を攻撃するマルウェアの解析 — Dragos社

KAMACITE 技術アップデート

KAMACITE を追跡することは重要です。なぜなら、彼らはELECTRUMのようなOT破壊チームにアクセス権を引き渡すからです。ELECTRUMは、他の組織によって追跡されているSandwormと技術的な共通点を持っています[8]

2015 年以降、KAMACITE はウクライナの電力インフラを標的とした少なくとも 3 件の破壊的キャンペーンを実施し、GreyEnergy や BlackEnergy を展開しました。また、VPNFilter や CyclopsBlink などのボットネットを開発・使用しました。2024 年には、新たなカスタム Windows ベースのマルウェアを導入し、欧州の石油・天然ガス (ONG) 事業者への攻撃を拡大しました。
KAMACITE は初期アクセスを提供する役割を担っており、フィッシングを一貫して使用しているため、Dragos は組織に対し、フィッシング試行を特定するための定期的なユーザー教育を実施するよう推奨しています。さらに、エンタープライズ IT と OT/ICS 間の適切なセグメンテーションを行うことは、KAMACITE の侵害が破壊的なイベントに発展するのを防ぐために極めて重要です。その上で、ICS 環境における「南北（north-south）」トラフィックの可視性を確保することも重要です。防御者は、制御センター間の接続が異常に終了したり、変電所のブレーカーステータスを変更する異常なポーリングが発生したりするなどの不審な活動を監視する必要があります。

KAMACITE は、ウクライナおよび東欧・中欧の以下の分野の組織を標的としています。

- **石油・天然ガス**
- **電力**
- **防衛産業基盤**
- **製造業**

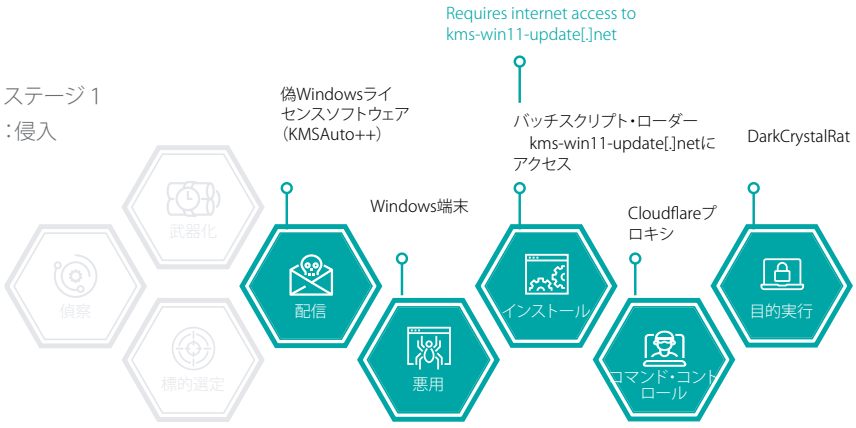
KAMACITE のキャンペーン

Kapeka キャンペーン (2022-2023)

2024 年に発見された KAMACITE の Kapeka は、2023 年 3 月からウクライナの複数の重要インフラ事業者を標的とするキャンペーンで使用されました。[9, 10] 。Kapeka は GreyEnergy と技術的な共通点を持ち、KAMACITE のツールセット内で継続的に開発が進められていることが分析から明らかになっています。発見された Kapeka のサンプル数は少なく、このマルウェアは 2022 年半ば以降、少量かつ特定の標的に対して使用されている可能性が高いと考えられます。

DarkCrystal RAT (2022-2024)

KAMACITE は、ウクライナの組織を標的とするスピアフィッシングキャンペーンで、犯罪者が提供する市販のマルウェアを引き続き使用しています。DarkCrystal RAT（DCRat）は、監視および情報窃取のために使用されました。



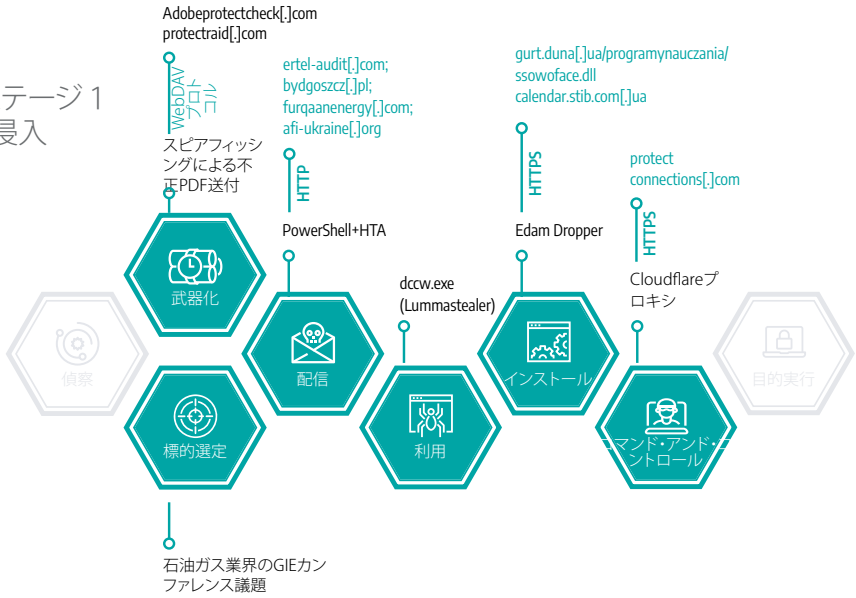
[8]Sandworm Team – MITRE [9]「ロシア国家系脅威グループSandwormと関係のある新たなマルウェア『Kapeka』を発見」— WithSecure [10]「UAC-0133（Sandworm）、ウクライナ国内の約20の重要インフラ施設に対するサイバー破壊工作を計画」— CERT-UA（機械翻訳）

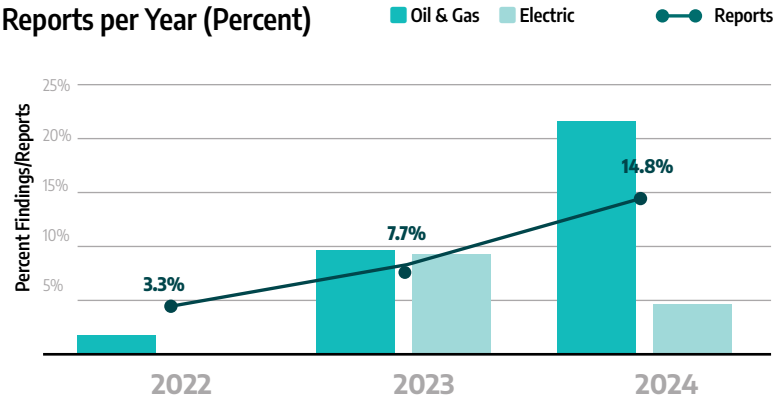
LummaStealer と GIE カンファレンスキャンペーン (2024)

KAMACITE は LummaStealer を使用し、Dragos によって TAT24-97 として追跡されている市販のローダーサービスを利用しました。[11, 12] これらの機能は主にスピアフィッシングによって配信され、著名なテクノロジープロバイダーの名称に似たドメインを使用しています。

KAMACITE は、ドイツで開催された 2024 年の Gas Infrastructure Europe（GIE）カンファレンスをスピアフィッシングのテーマとして利用し、欧州の石油・天然ガス（ONG）事業者を標的としました。このキャンペーンでは、比較的複雑な感染チェーンを利用し、「Edam」と名付けられた別のカスタム開発された Windows バックドアを展開しました。これは、ウクライナのみに焦点を当てていた従来の方針から、欧州全体を標的として拡大したことを示しています。この動きは、ロシア国営企業 Gazprom が東欧および中欧へのガス供給契約の期限切れと一致しました。

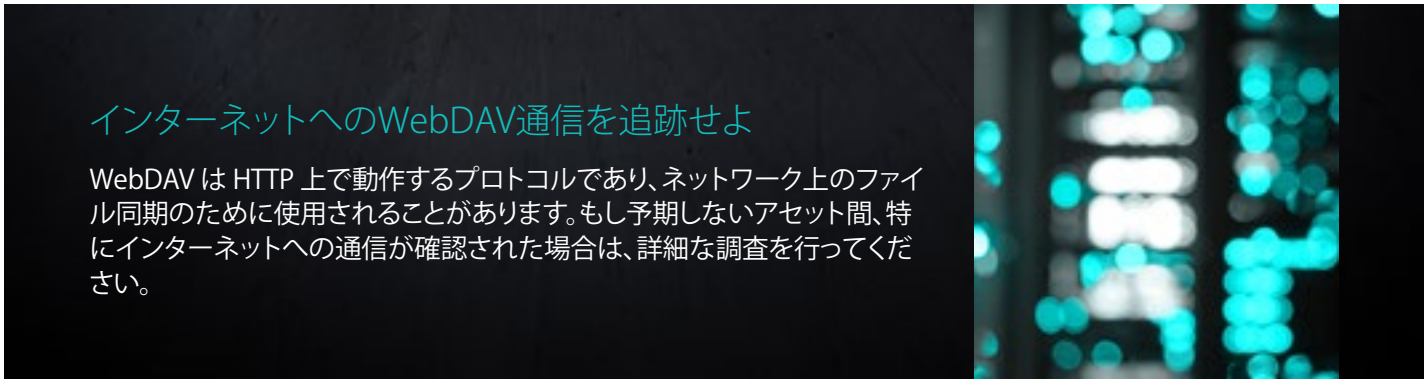
KAMACITE のような追跡対象の脅威グループに関連する PowerShell の戦術、技術、手順（TTP）が増えるにつれ、Dragos は関連するセキュリティ設定の評価をより厳格に行っています。インシデント対応を支援するための PowerShell ログ機能の有効化、悪意のあるスクリプトをブロックする AMSI の有効化は、Dragos のセキュリティ評価において最も一般的な推奨事項となっています。





Dragosのサービス支援において、KAMACITEのEdam攻撃で悪用されたものと同種のPowerShell設定不備が発見された割合を業種別に示したものである。

KAMACITEのような追跡対象の脅威グループに、PowerShellに関連する戦術・技術・手順（TTPs）がますます多く関連付けられる中で、Dragosはこれらに関連するセキュリティ設定について一層厳しい目を向けています。インシデント対応を支援するためにPowerShellのログ記録を有効化し、悪意あるスクリプトをブロックするためにAMSI（Antimalware Scan Interface）を有効化することが、Dragosのセキュリティ評価において最も一般的なPowerShell関連の推奨事項です。



インターネットへのWebDAV通信を追跡せよ

WebDAV は HTTP 上で動作するプロトコルであり、ネットワーク上のファイル同期のために使用されることがあります。もし予期しないアセット間、特にインターネットへの通信が確認された場合は、詳細な調査を行ってください。

[11]「PEAKLIGHT：ステルス性の高いメモリ常駐型マルウェアの解明」— Google [12]「WebDAV-as-a-Service：Emmenthalローダー拡散を支えるインフラの解明」— Sekoia

ELECTRUM 技術アップデート

Dragos が追跡する最も古い脅威グループの 1 つELECTRUMは、複数の ICS 攻撃を実行しており、2016 年の CRASHOVERRIDE 事件では、キエフの一部地域で約 1 時間の停電を引き起こしました。また、2022 年には Industroyer2 攻撃を試みましたが、これは失敗に終わりました。ELECTRUM は Sandworm APT と技術的な共通点を持っています。[13] 2024 年、KAMACITEほどの活動は確認されなかったものの、ELECTRUM はハクティビストのペルソナを利用して他の作戦を隠蔽し、新たなワイパー機能「AcidPour」を開発しました。

ELECTRUM は、ICS サイバーキルチェーンのステージ 2 - ICS 攻撃の実行能力に到達したことを示しました。

ELECTRUM はウクライナを標的としている

が、Dragos はドイツのエネルギー企業も標的にされていることを確認した。

電力

ELECTRUM のワイパーマルウェアの使用履歴を考慮すると、アセットオーナーは、制御システム環境内でのバイナリ実行を防止または監視するための基本的なセキュリティ対策を実施すべきです。また、これらのファイルが ICS ネットワークに転送される際の監視も重要です。エンドユーザーは、新しいサービスのインストールを禁止し、サービスの変更を無効化し、可能であればアプリケーションのホワイトリストを導入することで、許可されたアプリケーションのみがデバイス上で実行されるようにする必要があります。
アセットオーナーおよび運用者は、これらの攻撃を防ぐだけでなく、万が一の際に迅速に復旧できる体制を整えておく必要があります。プロジェクトロジック、IED（インテリジェント電子デバイス）構成ファイル、ICS アプリケーションインストーラーなどのエンジニアリングファイルの堅牢なバックアップを、オフライン環境で保管し、定期的にテストすることが推奨されます。

ELECTRUMワイパーマルウェアの能力

[13]Sandworm Team – MITRE

ELECTRUM のキャンペーン

Kyivstar 攻撃とハクティビストによる隠蔽 (2023 年 12 月)

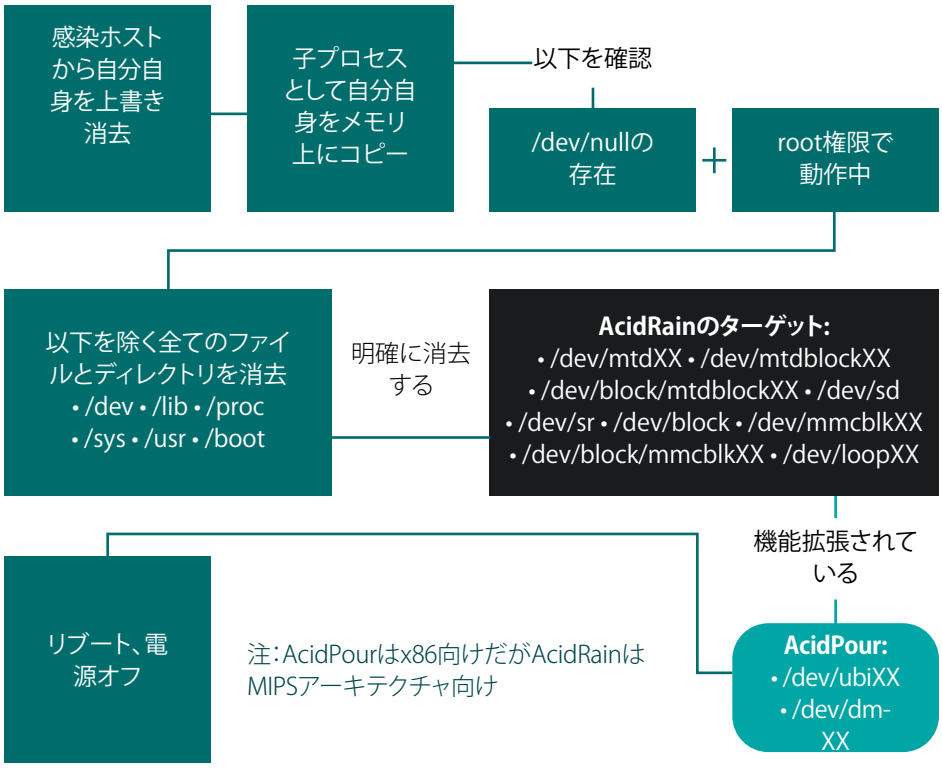
ウクライナの主要な通信事業者である Kyivstar はサイバー攻撃を受け、国内全域で大規模なサービス障害が発生しました。この事件の後、親ロシア派のハクティビスト「KillNet」と「Solnetspek」の 2 つのオンラインペルソナが、それぞれの Telegram チャンネルにほぼ同一のメッセージを投稿し、犯行を主張しました。2024 年初頭、Dragos は Kyivstar 事件を分析し、ELECTRUM がハクティビストペルソナである Solnetspek のリソースと評判を利用して、自らの作戦活動を隠蔽していたことを特定しました。

AcidPour ワイパー (2024 年 3 月)

Dragosは、ELECTRUMによる新たな機能「AcidPour」を分析しました。AcidPourはLinuxオペレーティングシステム向けにコンパイルされたバイナリであり、OT環境を含む組込み機器内のUBI（Unsorted Block Image）ディレクトリを探索し、消去することが可能です。

AAcidPourは、以前使用されたワイパー「AcidRain」の機能を拡張したものであり、2022年2月に確認されました。AcidRainは、ViaSat製モデムに影響を及ぼし、KA-SATの一般消費者向け衛星ブロードバンドサービスに一部中断を引き起こしました。この攻撃は、ドイツ国内の風力タービンにも影響を及ぼしました。[14]

AcidPourワイパーマルウェアの能力



AcidPourの発見とその影響は、ELECTRUMが保有するワイパーマルウェアの脅威が依然として深刻であることを改めて浮き彫りにしています。とくにOT環境において、重大な運用停止や損害を引き起こす可能性がある点で、その脅威は看過できません。

[14]「AcidRain | ヨーロッパに降り注ぐモデムワイパー」 — SentinelOne

アジアの地政学的緊張がVOLTZITEの活動をさらに促進

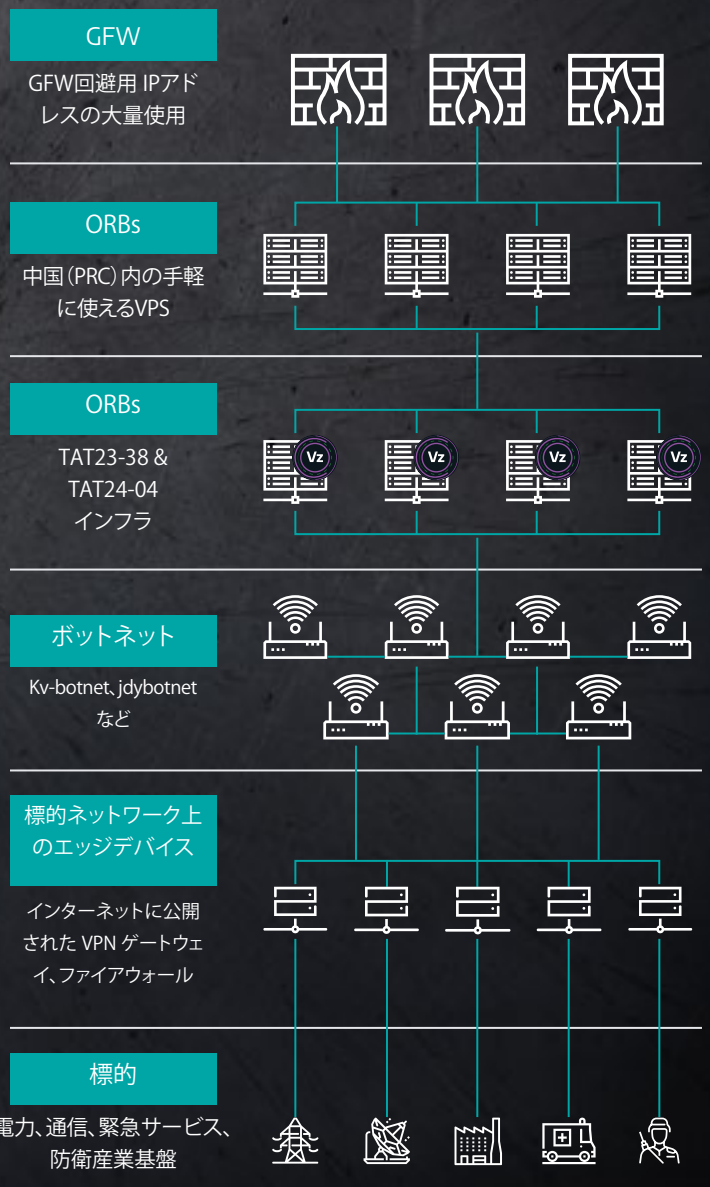
1年を通じて、脅威グループVOLTZITEは活動を継続し、SOHO（小規模オフィス／家庭向け）ルーターの侵害や地理情報システム（GIS）への関与を行っていました。分析によれば、VOLTZITEおよびその関連組織は、侵害された組織のインフラをボットネットの中継ポイントとして利用しており、攻撃者が制御するP2P（ピア・ツー・ピア）型リレーネットワークの構築を可能にしています。こうした行動により、インターネットに公開された重要インフラの特定が可能となり、電力、石油・ガス、水道・下水道、政府機関といった分野に影響を与えています。

VOLTZITE 技術アップデート

VOLTZITEは、重要インフラにおいて最も注視すべき脅威グループの一つと言えるでしょう。OTデータに特化した活動により、ICSアセットオーナーおよび運用者にとって、同グループは現実的かつ重大な脅威となっています。このグループは、他の機関によって追跡されている「Volt Typhoon」脅威グループと多くの技術的共通点があります。VOLTZITEはこれまでもOTネットワークへの侵入を繰り返しており、今年もDragosは、VOLTZITEがさまざまなプロキシネットワークを活用し、被害者からGISデータ、OTネットワーク図、OTの運用手順書などを窃取し続けていることを確認しました。[15] これらのICS関連データによって、VOLTZITEはOTに特化した破壊的なツールを独自に作成できる可能性があります。しかし実際には、このグループは標的システム上にすでに存在するツールを利用する「Living-off-the-Land（LOTL）」手法を用いて攻撃を行っています。

不審なネットワーク通信を丁寧に監視・調査することで、防御側はVOLTZITEの活動を特定し、防御を構築することが可能です。

VOLTZITE は自身の活動を隠すため、ネットワークインフラの複雑な連鎖を構築しています。Dragos は、彼らが引き続き ORB（Operational Relay Box）ネットワークや、電力会社が運用する SOHO ルーター（通信・電力インフラを地域に提供するためのもの）を侵害していることを追跡しています。これらルーターのIPアドレスは防御側から見て通常の通信として見えることから、VOLTZITEはそれらを踏み台にして他の重要インフラを標的とする意図があったと考えられます。



Historical VOLTZITE Infrastructure Usage

（マクニカ注釈）
GFW：The Great Firewall（中国のインターネット検閲システム）
ORB：Operational Relay Box（運用リレーボックス、攻撃者が利用する中継インフラのこと）
PRC：People's Republic of China（中華人民共和国）
VPS：Virtual Private Server（仮想専用サーバー）

[15] Volt Typhoon – MITRE

VOLTZITE は、多層化されたネットワークインフラを用い、時間をかけ継続的な偵察活動を行っており、他の中国国家系とされるグループとインフラを共有していることも確認されています。
Dragos は、VOLTZITE に乗っ取られた既知のボットネット（例：JDYボットネット）から、重要インフラのネットワーク周縁機器（VPNゲートウェイやファイアウォールなど）に対する偵察活動を観測しました。

VOLTZITE は引き続き、標的のネットワークから OT 関連データを持ち出すことに注力しています。多くのケースにおいて、エネルギーシステムの空間配置に関する重要情報を含んだ GIS データが持ち出されていました。

初期侵入の手段としては、インターネットに公開されている VPN アプライアンスやファイアウォールの脆弱性の悪用が中心です。Dragos は、アセットオーナーや運用者に対して、これらの機器に適切なパッチ管理とシステム整合性維持の計画を実施するよう強く推奨しています。

Dragos は、VOLTZITE による米国および西側諸国の重要インフラへの作戦活動が 2025 年にも継続すると予測しています。防御側は、パデューモデル（Purdue Model）のあらゆるレイヤーにおいて VOLTZITE の活動を監視する必要があります。たとえば、インターネットに面した VPN 機器、ビジネスネットワーク、DMZ、OT ネットワーク内部に至るまで、すべての層で監視が必要です。

VOLTZITE を識別する最善の方法は、その行動を監視することです。
彼らは意図的に信頼されたネットワークに溶け込もうとし、既存のツールを悪用（LOTL）するため、異常な横方向の移動（ラテラルムーブメント）を通常の通信と比較して分析し、一般社員のアカウントからの不審なユーザー活動を検証することも重要です。

VOLTZITE の被害者は、北米、グアム、ヨーロッパ、アジア、ニュージーランド、アフリカで確認されており、その攻撃キャンペーンは以下の産業セクターに影響を与えています：

- **電力の発電、送電、配電**
- **緊急管理**
- **通信**
- **衛星通信**
- **防衛産業基盤**

65%

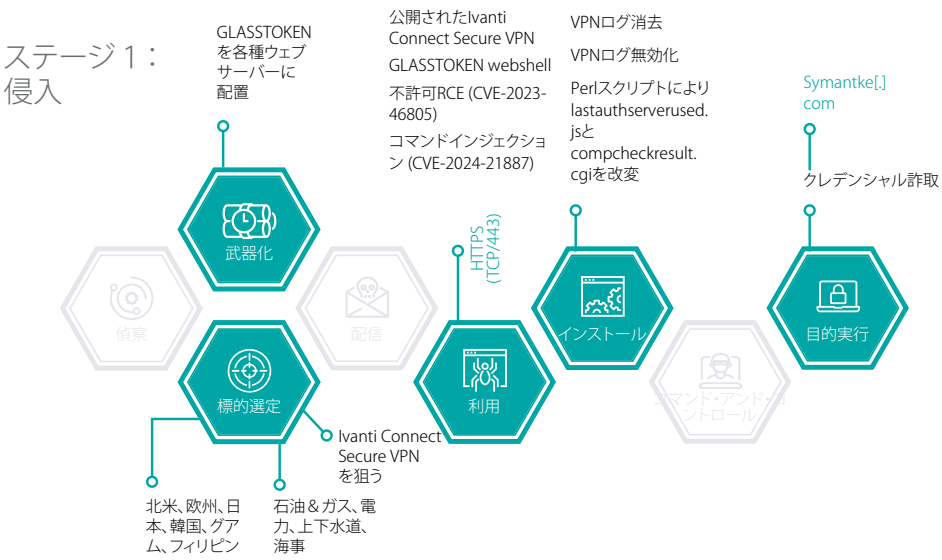
Dragos が評価したサイトの 65% で、安全でないリモート環境が確認されました。これには、セキュリティ設定が不十分な構成、パッチ未適用のシステム、リモートアクセス機器やアプリケーションに関連する不適切なネットワークアーキテクチャが含まれます。

VOLTZITE のキャンペーン

Ivanti VPN ゼロデイキャンペーン (2023 年 12 月)

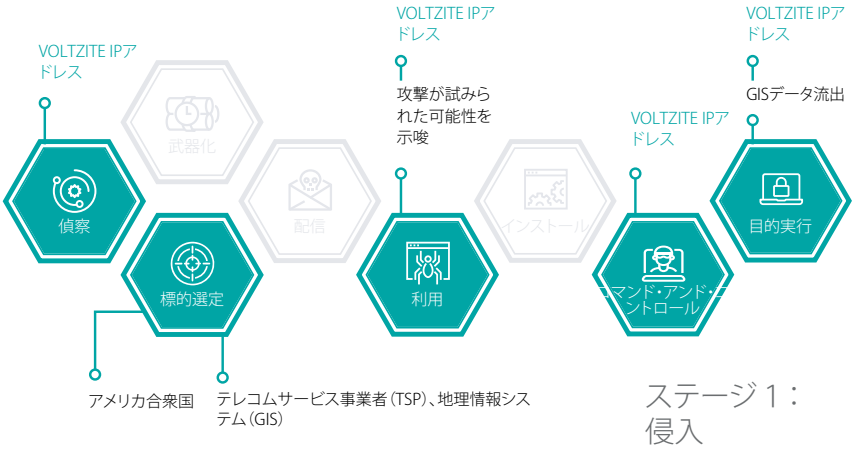
VOLTZITE は複数のエクスプロイトを組み合わせることで、リモートコード実行（RCE）を可能にし、設定データの窃取、ICS VPN アプライアンスからのリバーストンネリング、およびその他の悪意のある動作を実行できます。[16]

SYS32039 および SYS32040 の新規ファイル作成を監視してください



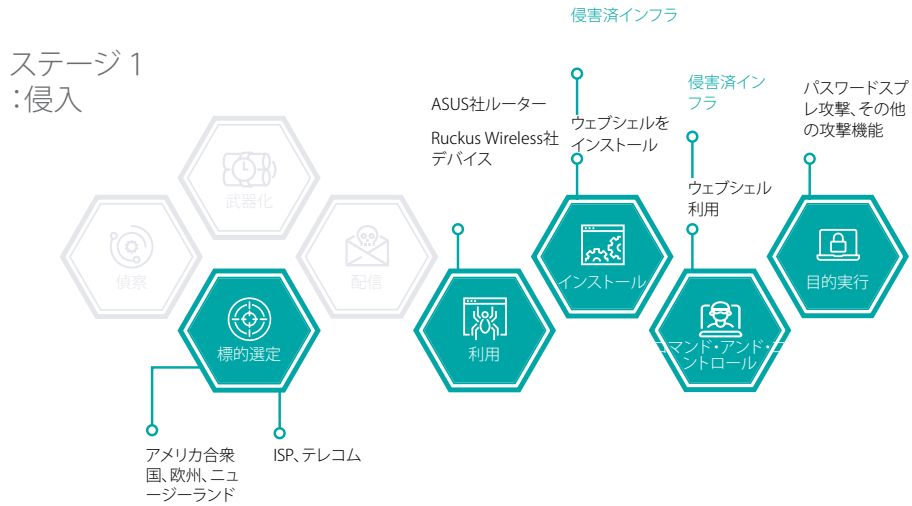
通信および緊急サービス（EMS）キャンペーン (2024 年 1 月)

VOLTZITE は、米国の通信業界への偵察活動を行い、緊急サービスのGISエンドポイントを侵害してコマンド＆コントロール（C2）を実行しました。[17]



ISP および通信キャンペーン (2024 年 8 月)

VOLTZITE は、電力、公益事業、通信協同組合インフラ内の SOHO デバイスを侵害し、今後の作戦を支援するための運用リレーネットワークとして利用しました。



[16]Ivanti Connect Secure VPN における 2 件のゼロデイ脆弱性の積極的な悪用 ― Volexity, [17]米国の重要インフラを標的とする VOLTZITE のスパイ活動 ― Dragos Inc.,

JDY ボットネット（2024 年後半）
VOLTZITE は JDY ボットネットの証明書を使用して標的をスキャンしました。標的となった組織は、電力、石油・天然ガス、製造業、防衛産業基盤の分野に属していました。

ステージ 1：侵入

ハンティングのヒント

自社のネットワーク内に GIS データを収集・流出させている敵対者がいるのか？この疑問に答えるためには、可視性を評価する必要があるかもしれません。「Collection Management Framework」を参照してください。

Collection Management Framework.

Dragos、2024 年に 2 つの新たな脅威グループを特定

既存の脅威グループに加え、Dragosは新たに 2 つの脅威グループを特定し命名しました。この期間、非常に活発に活動し、一連の紛争に関連する攻撃キャンペーンを担いました。

GRAPHITE は、ウクライナ紛争に関連するエネルギー、石油・ガス、物流、政府機関の組織を標的とし、その活動範囲は東ヨーロッパおよび中東に及びます。

一方、中東の紛争に関連する **BAUXITE** は、米国、ヨーロッパ、オーストラリア、中東の石油・ガス、電力、水道・廃水処理、化学製造の分野の組織を標的としています。BAUXITE は、親イラン派のグループ CyberAv3ngers と技術的な共通点を持っています。BAUXITE はその能力を強化し、特にイスラエル・ハマス紛争に関与する OT/ICS 組織に対して、グローバルに破壊的な活動を継続する可能性が高いと考えられます。

GRAPHITE の紹介

Dragos は、水力発電施設を標的とし、認証情報を窃取するキャンペーンを発見した後、GRAPHITE を新たな脅威グループとして指定しました。その後、Dragos は GRAPHITE が東ヨーロッパおよびアジアの産業・エネルギー関連組織を標的にしていることを観察しました。このグループは、APT28 として特定されている集団と強い技術的共通点を持っています。[18] GRAPHITE は、2022 年 2 月のロシアによるウクライナ侵攻以降、ウクライナの軍事的状況に関係する組織を標的としていることが確認されています。

2023 年初頭、Dragos は、GRAPHITE が水力発電施設および東ヨーロッパ・中東の ICS 組織を標的とするスピアフィッシングキャンペーンを実施していることを特定しました。このキャンペーンでは、Microsoft Outlook の「ノークリック脆弱性」を悪用し、Windows 認証データを窃取する手法が用いられました。
[19] 同時に、GRAPHITE はカスタムスクリプトベースのマルウェアを使用したフィッシング攻撃を継続的に実行していました。これらの 2 つのキャンペーンは異なるツールや手法を用いていましたが、同一地域の重要産業組織を標的としていました。

GRAPHITE は、侵害された Ubiquiti Edge ルーター のネットワークを利用してマルウェアを配信し、C2チャネルを維持していました。GRAPHITE は少なくとも 2022 年からこのネットワークを使用しはじめ2024 年 2 月まで稼働していましたが、米国司法省が裁判所の承認を得てこのボットネットを無効化しました。[20] 以降、Dragos は GRAPHITE が API エンドポイントテストサービスや GitHub などの正規のインターネットサービス（LIS）を利用してペイロードの配信や C2 活動を行う傾向が強まっていることを確認しました。

GRAPHITE は少なくとも 2022 年 3 月以降、多数のキャンペーンを実施し、ICS サイバーキルチェーンのステージ 1 への影響を与えました。GRAPHITE の被害者は東ヨーロッパおよび中東全域で確認されており、そのキャンペーンは以下の重要インフラセクターに影響を与えています。

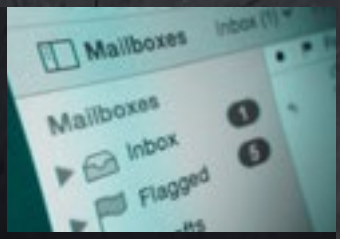
- **電力**
- **石油・天然ガス**
- **鉄道・貨物物流**
- **航空物流**
- **防衛産業基盤**

GRAPHITE は OT/ICS 組織にとって関連性の高い脅威であり、その標的範囲は東ヨーロッパの地政学的な動向に応じて変化する可能性があります。ただし、GRAPHITE は現在のところ、サイバーキルチェーンのステージ2（ICS 攻撃の実行）には達していないことが確認されています。Dragos は、特にウクライナ関連の活動に関与している産業組織の防御者に対し、この敵対者について理解を深めることを推奨しています。

Dragos のペネトレーションテスト担当者も、C2 チャネルのテストのためにインターネットインフラを利用しています。2024 年のペネトレーションテストの 17% で C2 通信に関連する問題が発見され、その主な原因は DNS チャネル でした。もしネットワークが インターネットアドレス（例：www.dragos.com）を解決できる場合、攻撃者はこれを利用してリモートアクセスを確立する可能性があります。

ハンティングのヒント

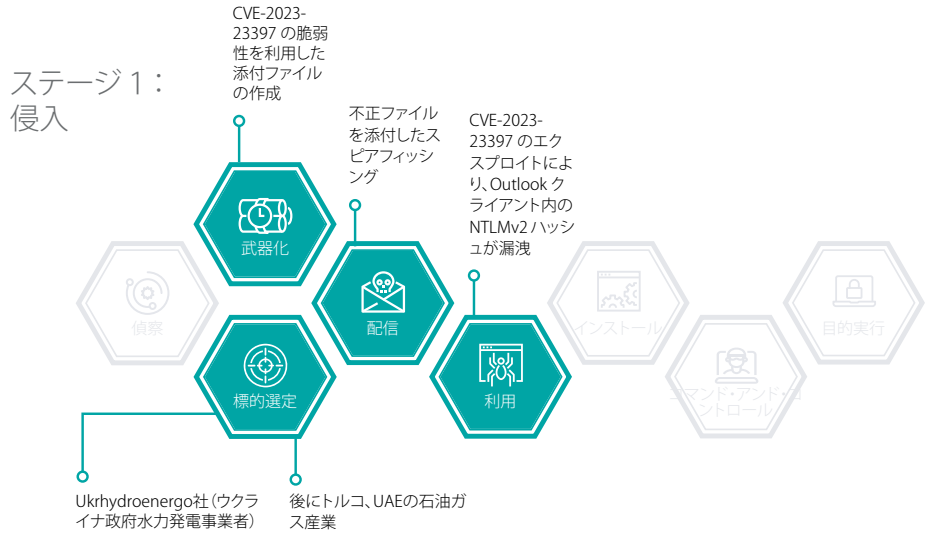
攻撃者が正規のインターネットサービスを通じてスピアフィッシングを行っている可能性はないか？
注: フォーカスすべきは ホスティング元ではなく、スピアフィッシングのフック（誘い込み手法）や行動パターン です。



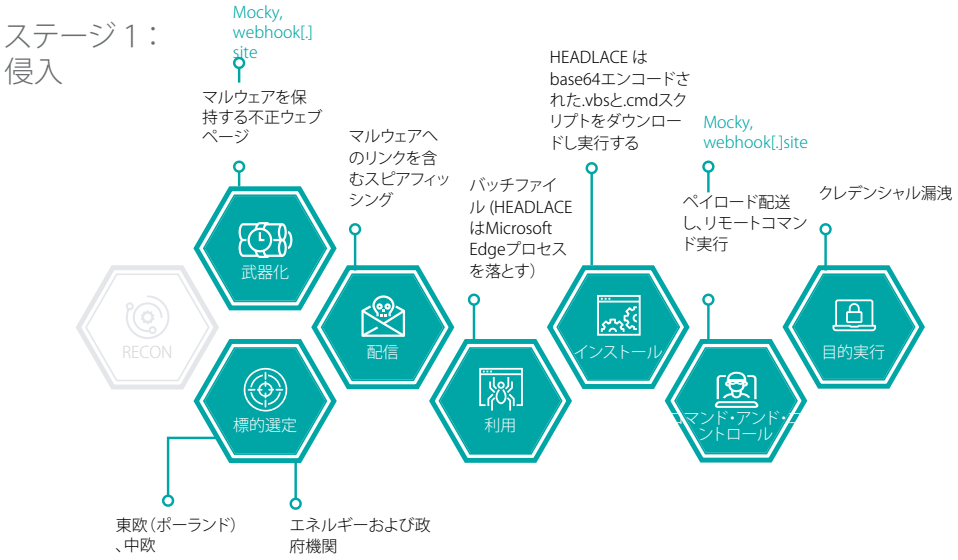
[18]APT28 - MITRE; [19]Microsoft Outlook 権限昇格の脆弱性（CVE-2023-23397） - Microsoft [20]ロシア連邦参謀本部情報総局（GRU）により制御されていたボットネットに対し、米司法省が裁判所の許可のもと撹乱作戦を実施 – 米国司法省

GRAPHITE のキャンペーン

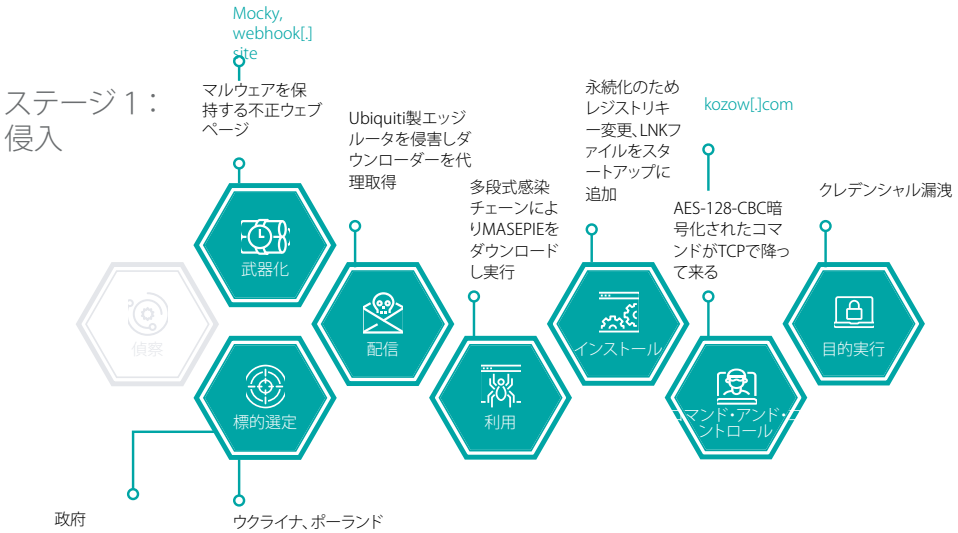
2022 年 3 月から 2023 年 10 月にかけて, スピアフィッシングキャンペーンが 東ヨーロッパおよび西アジアの天然ガスパイプライン事業者および水力発電施設を標的に実施されました。Microsoft Outlook の脆弱性が悪用され、悪意のある添付ファイルを介して認証情報が窃取されました。[21, 22]



2023 年を通じて, スピアフィッシングキャンペーンがポーランドおよび中東のエネルギー・政府機関を標的に実施されました。悪意のあるウェブサイトを通じて、HEADLACE と呼ばれる Windows バッチスクリプト型バックドア が配信され、リモートコマンド実行が可能になりました。[23]

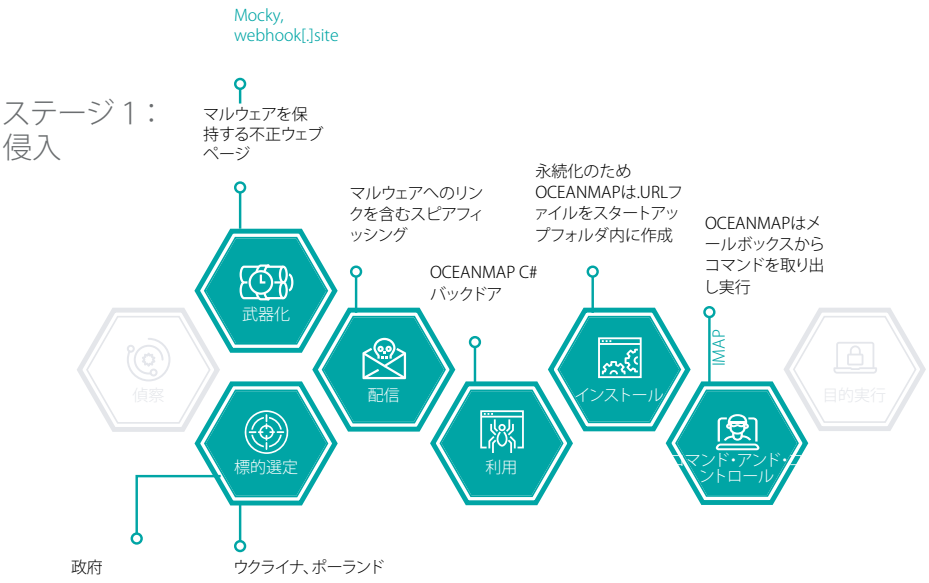


2023 年から 2024 年 2 月にかけて, スピアフィッシングキャンペーンがポーランドおよびウクライナの政府機関を標的として実施されました。侵害された Ubiquiti Edge ルーター を使用して MASEPIE マルウェアが配信されました。この Python ベースのバックドアにより、C2インフラに対し暗号化されたリバースプロキシ接続が確立されました。[24, 25]

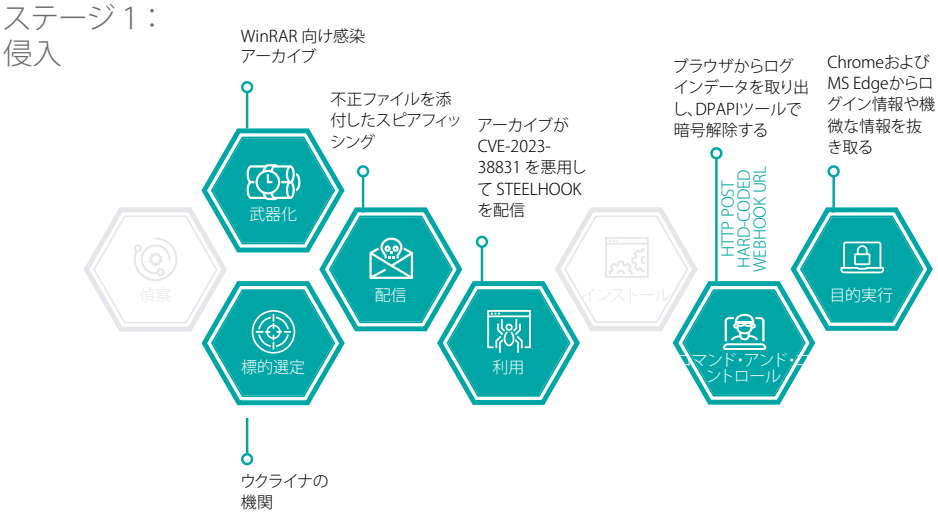


[21]ウルサ（別名APT28）との戦い：隠れたキャンペーンの解明 – Palo Alto [22]CVE-2023-23397脆弱性を利用したAPT28のサイバー攻撃 – ウクライナ国家安全保障・防衛会議 [23]APT28サイバー攻撃：msedgeをブートローダーとして使用、TORおよびmockbin.org/website.hookサービスをコントロールセンターとして使用（CERT-UA#7469） – CERT-UA [24]APT28によるポーランド政府機関を標的にしたキャンペーン – CERT.PL
[25]APT28: 初期攻撃からドメインコントローラーへの脅威の作成まで1時間 – CERT-UA#8399; † CVE-2023-23397を利用した攻撃の調査ガイド

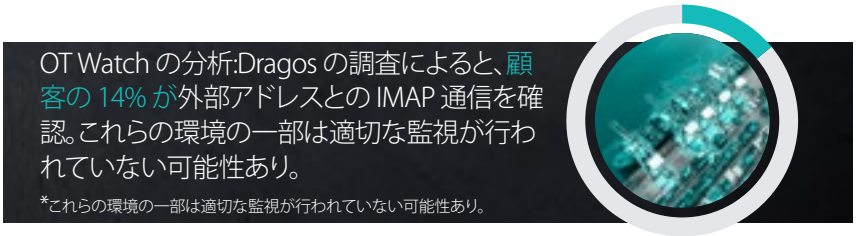
2023 年から現在にかけて, ウクライナおよびポーランドの政府機関を標的としたスピアフィッシングキャンペーンが実行されました。悪意のあるウェブサイトを利用して OCEANMAP マルウェア を配信し、IMAP 経由で被害者デバイスにリモートコマンドを実行可能な C# バックドア を展開しました。[26]



2024 年初頭には, ウクライナの組織を標的としたスピアフィッシングキャンペーンが確認されました。この攻撃では、WinRAR アーカイブツールの脆弱性（CVE-2023-38831）を悪用し、PowerShell ベースの情報窃取マルウェア「STEELHOOK」を展開しました。このマルウェアにより、Google Chrome および Microsoft Edge ブラウザからログインデータを抽出できます。[27, 28]



同時に、2024 年の複数のキャンペーンで GRAPHITE は悪意のあるウェブサイトを運営 し、Outlook on the Web（OWA）や ukr.net（ウクライナの人気オンラインサービス）などの正規のログインページを装ったフィッシングサイト を作成しました。GRAPHITE 独自のフィッシングツールキット を使用し、二要素認証（2FA）および Captcha を回避 して、被害者のブラウザと位置情報 を特定しました。[29]



Dragos プラットフォームでのハンティング方法:

RFC-1918 に該当しないアドレスに対する IMAP 通信を特定するには、以下のクエリを使用:

```
type:Communications AND NOT
ip_dst_network_id:* AND
protocol:IMAP AND dst_port_o2r:*
```

[26]APT28: 初期攻撃から1時間以内にドメインコントローラーに対する脅威の作成 (CERT-UA#8399) - CERT-UA; [27]APT28によるサイバー攻撃：msedgeをブートローダーとして使用し、TORおよび mockbin.org/website.hook サービスをC2（コマンド＆コントロール）に利用 (CERT-UA#7469) - CERT-UA [28]政府支援の攻撃者が WinRAR の脆弱性を悪用 – Google [29]APT28がウクライナ市民社会を標的に複数のフィッシング手法を活用 – Sekoia

BAUXITE の紹介

Dragosが命名した脅威グループ「BAUXITE」は、OT/ICS関連組織や特定のデバイスを標的とした複数のグローバル・キャンペーンに関与していたとされています。このグループは、能力およびネットワークインフラに基づく技術的特徴において、親イラン派ハクティビストのペルソナ「CyberAv3ngers」と大きく重なっており、同ペルソナはイランの「革命防衛隊サイバー・電子司令部（IRGC-CEC）」と明確な関係を有していると、米国政府により報告されています。[30]米国政府は、「CyberAv3ngers」の構成員複数名およびリーダーに対して制裁を科しました。[31]

BAUXITEはCyberAv3ngersとの技術的な共通点や、IRGC-CEC（イラン革命防衛隊・サイバー電子司令部）との関係が報告されていることから、その標的選定や作戦の焦点は、国家の支援を受けた指令や地政学的な圧力の下で進化してきたと考えられます。2025年を通じて、BAUXITEはその能力を強化し、世界中のOT/ICS関連組織に対して破壊的な作戦を試みることが予想されます。

Dragosは、インターネット越しにSSHアクセスが可能な資産を特定し、VPNの背後に隠すことを推奨しています。また、SSHアクセスを持つアカウントに対しデフォルトのパスワードや推測されやすいパスワードが設定されていないか再確認ください。SSHキーを監査し、不要なキーを削除し、公開されていたデバイスについては既存キーを再発行してください。

「Dragos OT-CERT Getting Started Guide: Default Passwords and Internet-Exposed Devices（デフォルトパスワードとインターネット公開機器に関する入門ガイド）」を参照ください。

2023 年後半以降、Dragos は BAUXITE による 4 つのキャンペーンを確認した。その中には、公開されたデバイスの脆弱性を簡単に悪用し、ICS サイバーキルチェーンのステージ 2 へ影響を及ぼすものも含まれていた。BAUXITE の被害は、米国、ヨーロッパ、オーストラリア、西アジア で報告されており、攻撃キャンペーンは、複数の重要インフラ分野に影響を与えた。

- **電力**
- **石油・天然ガス**
- **水道・廃水処理**
- **食品・飲料**
- **化学製造**
- **製造業**

45%

のペネトレーションテスターは、一般的な暗号化通信（C2トンネルやプロキシの実証を含む）に既存のSSH経路を活用している。

*これらの環境の一部には、設定調整が不十分なものも含まれる。

Dragos プラットフォームでのハンティング:

SSH が RFC-1918 以外のアドレスと通信しているかを特定するには、以下のクエリを使用:

type: Communications AND ip_dst_asset_id: * AND NOT ip_dst_network_id: * AND protocol:SSH AND src_port_r2o: *

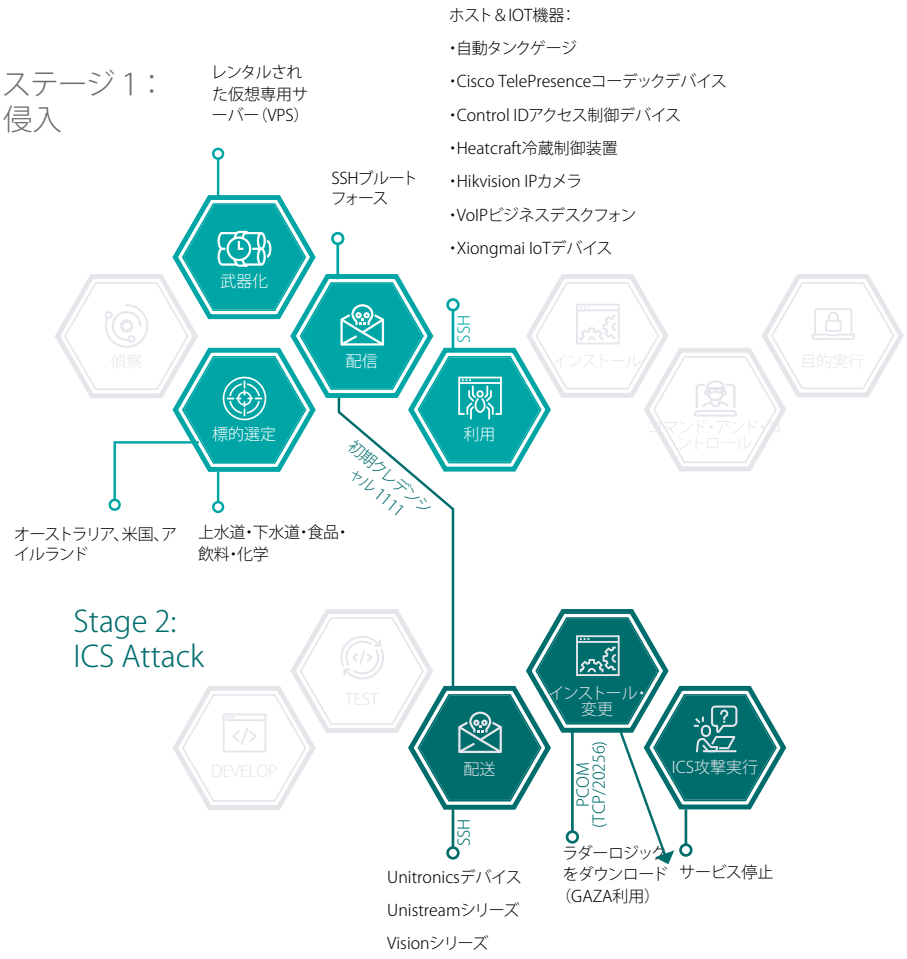
[30]CyberAv3ngers - MITRE; [31]重要インフラへの悪質なサイバー活動に関与した関係者に制裁 — 米財務省

BAUXITE のキャンペーン

Unitronics キャンペーン（2023 年 11 月 - 2024 年 1 月）

このキャンペーンは、世界中のおよそ100のOT/ICS組織に影響を及ぼし、インターネットに露出したUnitronics UnistreamやVisionシリーズのプログラマブルロジックコントローラー（PLC）を侵害することによってICSサイバーキルチェーンのステージ2に到達しました。攻撃者は、これらのコントローラーにロジックをダウンロードし、ICS攻撃を実行するのと同等のサービス障害（DoS）を引き起こします。

2023年後半、Dragosの調査により、Hikvision製IPカメラ、自動タンクゲージ、業務用VoIP電話機、Control IDのアクセス制御システム、Xiongmai製IoTデバイス、Heatcraftの冷蔵制御装置、Cisco TelePresenceのコーデック装置など、多様な脆弱なホストやIoT機器を標的とし、SSHブルートフォース攻撃を含む広範な脆弱性悪用の手口が明らかになりました。[32]



[32]イスラエル製OT機器を標的とするハクティビスト集団「Cyber Av3ngers」— Dragos Inc.

Sophos製ファイアウォール攻撃（2024年4月〜2024年5月）

BAUXITE は脆弱な Sophos製ファイアウォールを標的とし、化学、食品・飲料、水道・下水処理業界に影響を与えました。

Dragos Services は、米国の石油・天然ガス（ONG）企業でインシデント対応を実施し、BAUXITE が油田の Sophosファイアウォールを侵害したことを確認しました。

Dragos のテレメトリデータによると、北米の石油・天然ガス業界および電力事業に Sophos社のデバイスが使用されていることが確認されています。

5%

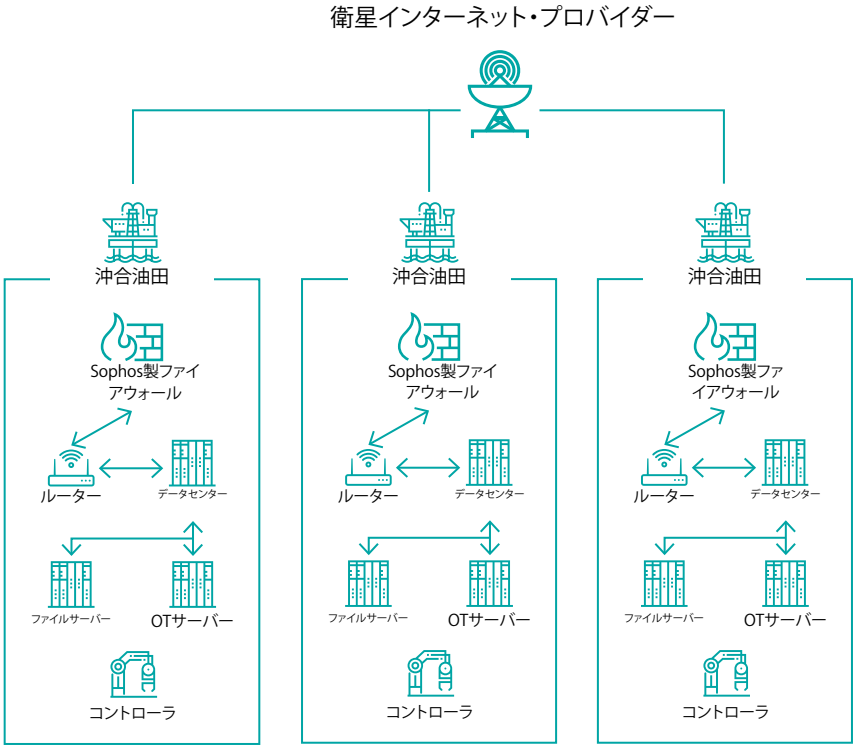
OT Watch の調査によると、**5% の顧客が**外部アドレスとの PPTP 通信を行っていることが確認されました。

*これらの環境の一部は適切に設定されていない可能性があります。

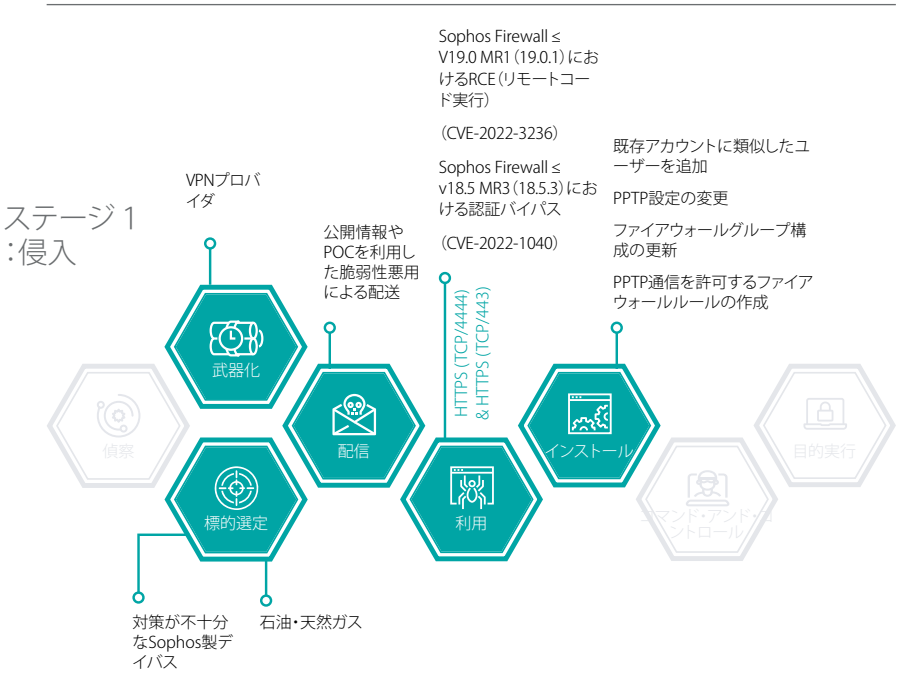
Dragosプラットフォームを使いご自身の環境をハントできます。非RFC-1918アドレスに通信するPPTPを識別するには、次のように検索します：

type:Communications AND NOT ip_dst_network_id:* AND protocol:PPTP AND dst_port_o2r: *

Starlink や Viasat など衛星インターネットプロバイダーを利用している場合、意図せず機器がインターネットに公開されている可能性がある。組織の外部露出を評価する際は、これらのシナリオを考慮する。



Example of Compromised Infrastructure



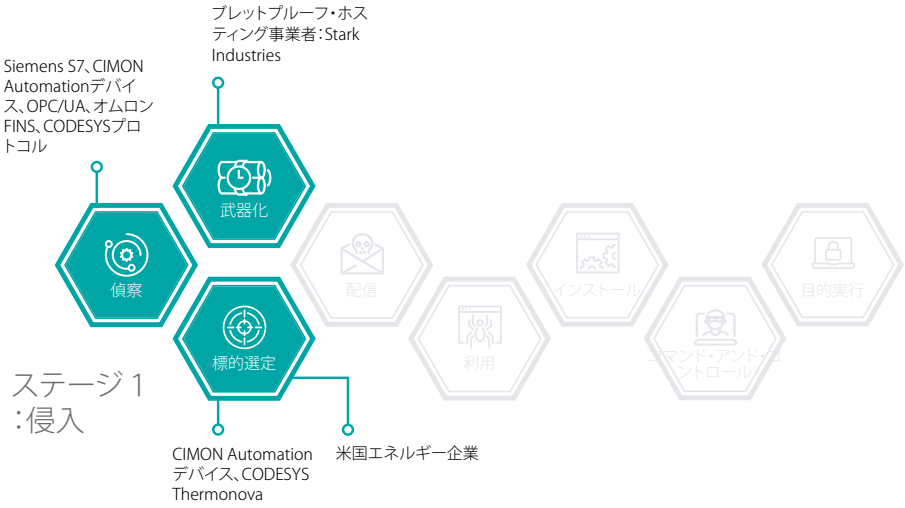
偵察スキャンキャンペーン（2024年6月 - 2024年7月）

BAUXITE は複数の OT/ICS OEM およびユーティリティ関連のウェブページにアクセスしました。この活動は、製品、サービス、その他の重要な情報を収集し、将来の作戦目標を支援するための情報収集を目的としている可能性が高いです。

BAUXITE は、複数のインターネットに公開された OT/ICS デバイスのポートスキャンを実施し、将来の作戦の標的となる可能性のある機器を特定しようとしました。以下のインターネットに公開されたデバイスが標的となりました。

- **Siemens S7デバイス**（s7comm 経由、TCP/102）
- **CIMON Automation デバイス**（CIP 経由、TCP/44818）
- **OPC Unified Architecture（OPC/UA）サーバーを実行するデバイス**（UDP/4840）
- **Omron Factory Interface Network Service**（FINS）（TCP/9600）
- **CODESYS を実行するデバイス**（TCP/11740, TCP/1217, UDP/1740-1743）

これらのプロトコルは、CHERNOVITE が開発した PIPEDREAM と重複しています。.



IOControl キャンペーン（2023年後半 - 2024年）

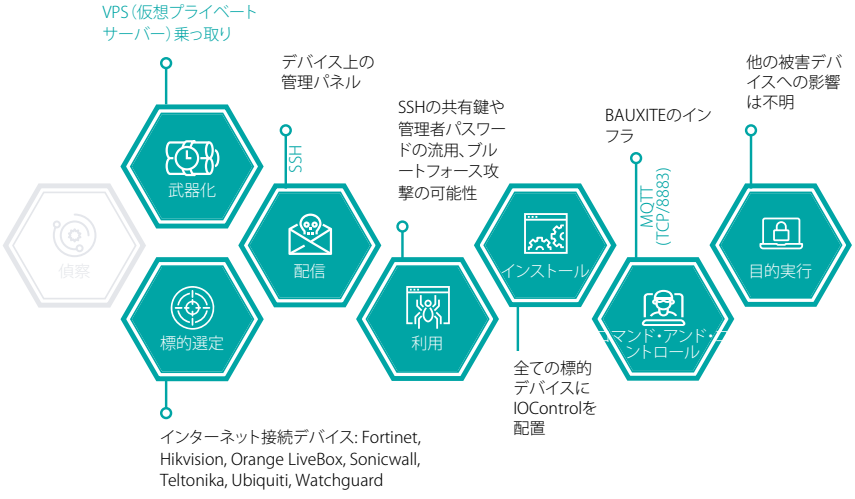
BAUXITEは、カスタム組み込み型Linuxバックドア「IOControl」をインストールすることで、世界中のOT/ICSデバイスおよびファイアウォール400台以上を侵害しました。

IOControlはリモートアクセス型トロイの木馬（RAT）であり、Message Queuing Telemetry Transport（MQTT）プロトコルを使い、TCPポート8883経由でC2サーバと通信します。

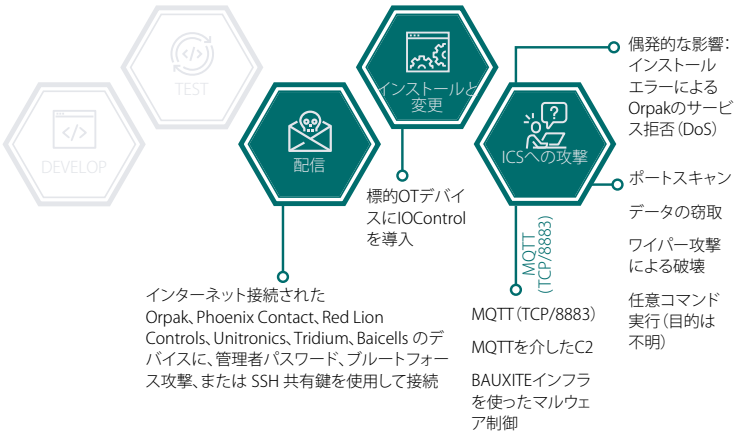
この通信は、DNS over HTTPS（DoH）を介してCloudflare上のハードコードされたドメインに対して確立されます。公開時点ではこのドメインはシンクホール化（sinkhole：無害化）されており、防御側のリスクは軽減されています。

IOControlの各サンプルは対象デバイスに固有であり、最新のサンプルではMTD（Memory Technology Device）操作によるシステムのワイプ（消去）も可能です。

ステージ１：OT以外のデバイスへの広範な侵入攻撃



ステージ２：OTデバイスへの攻撃



Neighborhood Keeper によると、Orpak デバイスはオーストラリアおよびニュージーランドの発電分野で使用されています。

電力

Phoenix Contact デバイスは、北米、アジア、ヨーロッパの以下の業界で使用されています：

運輸・物流

製造業

化学

採掘

紛争を背景とした攻撃キャンペーンでICS特化型マルウェアの使用が増加

2024年4月、新たに２種類のICSマルウェア亜種が確認されました。いずれもウクライナとロシアの紛争に関連して発生したものです。地政学的紛争のツールとしてICSマルウェアが使用されることは以前からもありましたが、今回、ウクライナ・ロシア紛争の両陣営による使用が疑われることから、報復の応酬によるエスカレーションと共にOT/ICSコミュニティ全体に影響を及ぼす可能性があります。

BlackJack、モスクワの産業用センサーを妨害したと主張

2024年4月、自称ハクティビストグループのBlackJackは、モスクワのガス、水道、下水道網の通信システムを管理する自治体組織Moskollektorに侵入したと主張しました。BlackJackは、モスクワ地域の運用維持に関わる数千のセンサーとの通信を妨害したと述べています。

BlackJackが公開ウェブサイト上に流出させたデータによると、彼らはルーターおよびセンサー用ゲートウェイデバイスに対し、デフォルトクレデンシャル（初期設定の認証情報）を利用してアクセスした可能性が高いと考えられます。これらのゲートウェイは、Moskollektorの地下トンネルインフラを監視する産業用センサーにシリアル接続され、物理データの収集および送信を行っています。

BlackJackは、Fuxnetマルウェアを使用して数千のセンサーを無効化および、センサーゲートウェイデバイスを破壊し情報送信機能を停止させたと主張しました。さらに、BlackJackは組織のデータ窃取、SNSアカウントの改ざん、緊急通報番号112へのアクセス、デバイスやワークステーションの工場出荷時設定へのリセットを実施したと主張しています。
また、BlackJackはFuxnetのソースコードのスクリーンショットを公開しましたが、Fuxnetのバイナリサンプルは公開していません。そのため、公開マルウェアリポジトリやDragosのテレメトリデータにも登録されていません。

> 多くの組織は、デフォルトクレデンシャルの存在に気づいていません。Dragosによると、アーキテクチャレビューの中でデフォルトクレデンシャルが指摘されるのはわずか6%ですが、産業環境に対するペネトレーションテストでは約4件に1件の割合でデフォルトクレデンシャルが見つかっています。この問題を特定するには、アクティブな検査（実際にログインを試みる手法など）が最も有効です。

BlackJackによって公開されたすべてのデータを分析した結果、産業用センサーおよびセンサーゲートウェイへの妨害が発生した可能性は高いものの、その影響の範囲はBlackJackの主張ほど大規模ではなかったと考えられます。
公開されたスクリーンショットから判断すると、Fuxnetが使用された場合、センサーゲートウェイの機能停止または破壊につながる可能性が高いと考えられます。ただし、Fuxnetによって、センサー自体に永続的または一時的なサービス障害（DoS）を及ぼしたか否かは解っていません。

The Fuxnet Malware

Fuxnetがコンパイルされた形で確認されるまでは保留扱いではあるものの、産業用センサーのMeter-bus通信を妨害を持つことから、Fuxnetは既知の ICS 専用マルウェアとしては 8 番目の事例となります[33] BlackJack によって公開されたソースコードのスクリーンショットによると、Fuxnet には 2 つの主要コンポーネントが含まれています。

センサーゲートウェイデストラクタ

センサーゲートウェイは、センサーで収集した産業データにインターネット経由でアクセスできるようにします

デストラクターを構成する３要素

1

ファイルシステム
重要なサービスの停止・削除。重要ファイルの削除。

UBI ボリューム
UBIボリューム破壊：約束された量より少ないデータを書き込むことでUBI Volume Update IOCTL操作をハングさせ、デバイスを使用不能に。

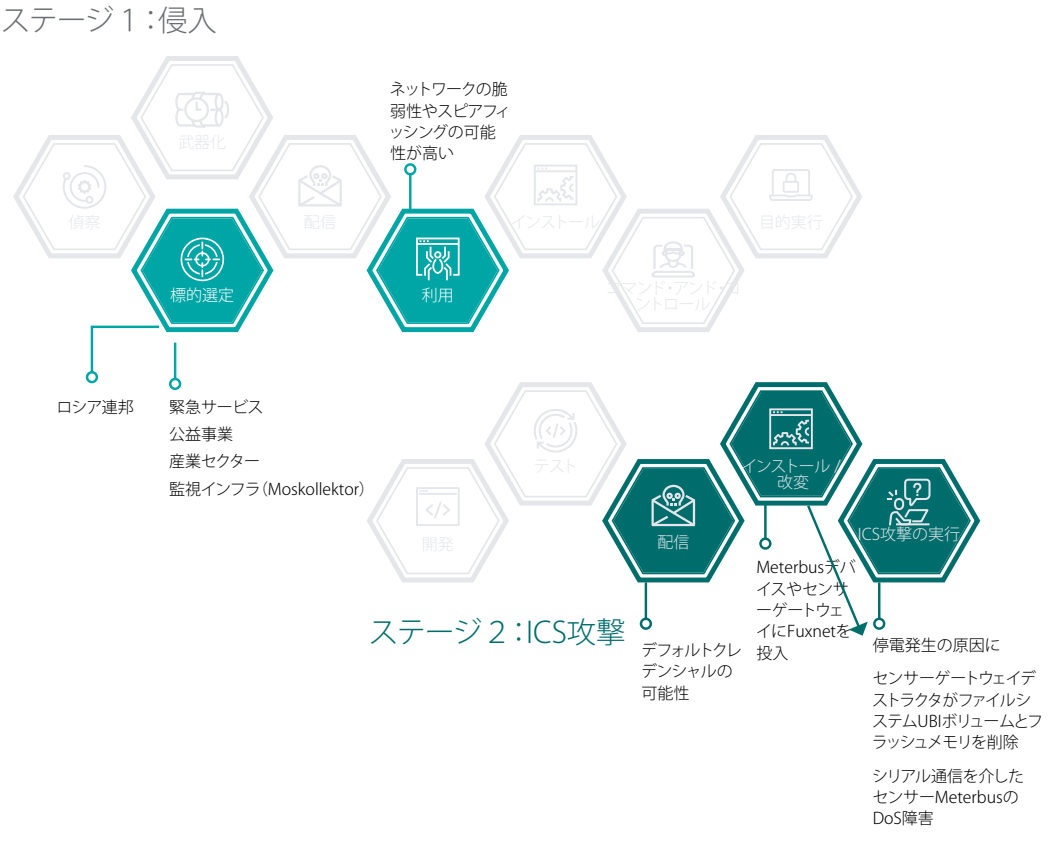
フラッシュメモリ
消去-書き込み法を用いてNANDメモリを摩耗させ、MTDフラッシュメモリを破壊。.

センサー Meter-bus DoS

2

シリアル接続を通じて多数のMeter-Busリクエストを送信し、センサーを過負荷状態にさせる。これらのリクエストは、Meter-Bus規格に準拠した一見正しいが実は異常なデータパケットで構成されており、DoS状態を引き起こす可能性がある。

センサーゲートウェイデストラクタコンポーネントは、汎用的なLinux ワイパーマルウェアである一方、Meter-bus DoS コンポーネントは特有の ICS 向けに作成されています。
Meter-bus は、水道、ガス、電力メーターから特定のセンサーデータを読み取るためのヨーロッパ標準プロトコルです。ランダムに生成されたリクエストをデバイスに送信することで、Fuxnetが産業用センサーの Meter-bus プロトコルスタックにおけるゼロデイ脆弱性を引き起こし、それによってセンサーを使用不能にした可能性があります。
ゲートウェイは物理的な損傷を受けた可能性が高く、通常の運用を再開するにはデバイスの交



[33]Fuxnetマルウェアの戦略的概要 – Dragos

換が必要でした。

Fuxnetからの教訓

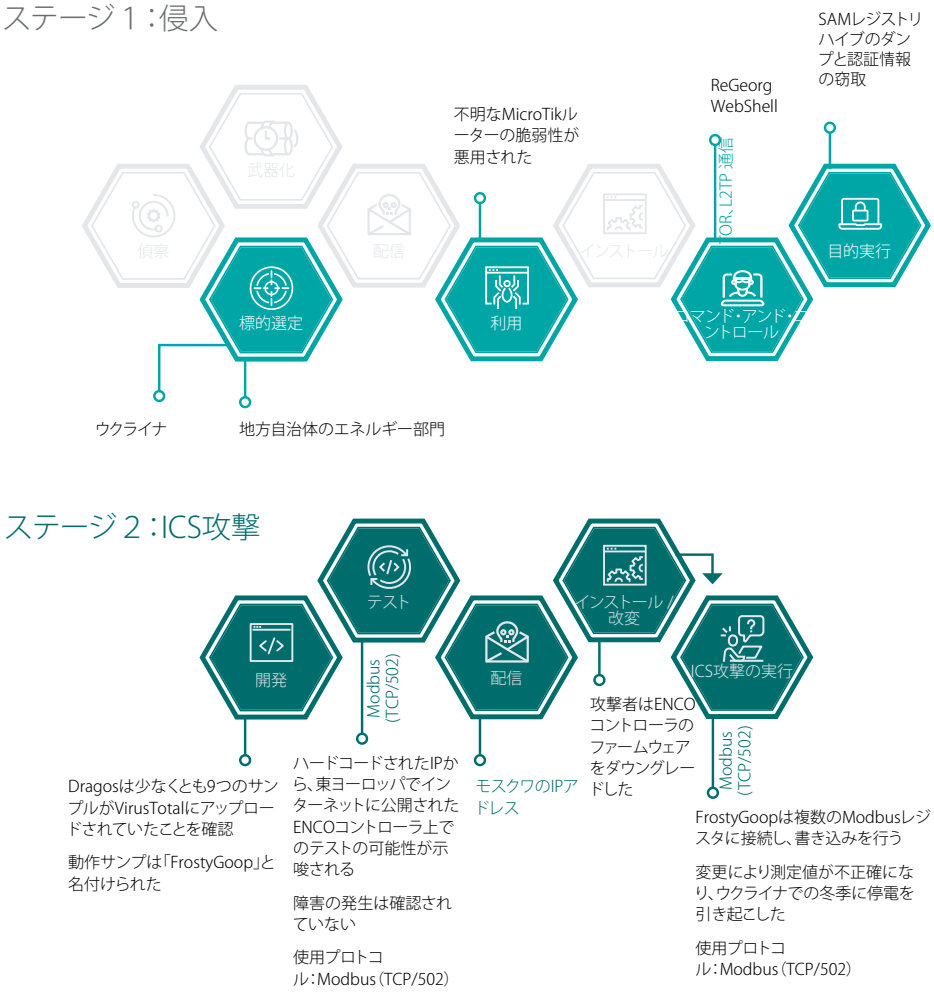
Moskollektor に対する攻撃は、地政学的な対立を背景とした産業用デバイスへのサイバー攻撃が常態化している実態を浮き彫りにしました。
この攻撃に用いられた Fuxnet マルウェアは、Moskollektor に特化して設計されており、大幅なコード変更なしに他の産業環境で再利用される可能性は低いと考えられます。
しかしながら、デフォルトの認証情報を使用したままの運用といった不適切なセキュリティ管理は、攻撃者にとって格好の侵入口となり得ます。こうした設定ミスは、実際の運用現場でも広く見受けられます。Dragos のテレメトリーデータによると、現在でも多くの産業環境でデフォルトの認証情報が使用されていることが確認されています。

こうしたリスクに対抗するために、SANS ICSの「5つの重要管理策（5 Critical Controls）」[34]を実施することで、組織のセキュリティ態勢を強化し、Fuxnet のようなマルウェアへの防御力を高めることが可能です。
特に資産管理者は、リスクベースの脆弱性管理プログラムの一環として、デフォルト認証情報が設定された ICS コンポーネントを特定し、速やかに対策を講じるべきです。さらに、資産の堅牢化（ハードニング）やアクセス制御の厳格化を通じて、防御力の高いセキュリティアーキテクチャを構築していく必要があります。

FrostyGoopマルウェア、冬のウクライナで暖房停止を引き起こす

2024年4月、Dragos社はFrostyGoopを発見しました。これは、既知のICSマルウェアとしては9番目にあたります。[35]
FrostyGoopはENCOコントローラー(暖房や換気等の制御に利用されるコントローラー)の計測値を改ざんし、それにより冬季のウクライナで600棟以上のアパートに暖房の停止が発生しました。
FrostyGoopは、Modbus TCP/502（世界中で使用されているICSの標準プロトコル）を介してICSデバイスと通信します。
このマルウェアは、汎用の公開Modbusライブラリとログ記録機能を組み合わせて、ICSデバイス上のレジスタを読み書きするコマンドを送信することができます。
Dragosはこの一連の活動をTAT24-24として追跡しています。

2024年1月に発生した、ウクライナの地方自治体が運営する地域エネルギー会社に対するFrostyGoopを伴うサイバー攻撃は、ウクライナとロシア間紛争の一環であった可能性が高いとみられています。
ウクライナ保安庁（Ｃｎｙжбａ



[34]The Five ICS Cybersecurity Critical Controls - SANS; [35]FrostyGoop ModbusマルウェアがOTシステムに与える影響

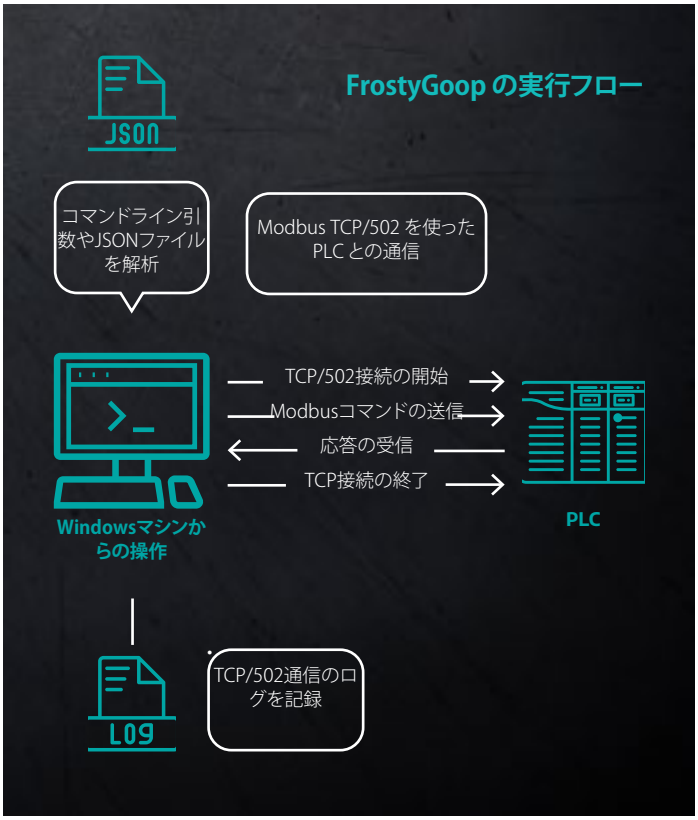
безпеки України）に属するサイバーセキュリティ状況センター（CSSC）は、このインシデントに関する詳細をDragos社と共有しました。
分析によると、FrostyGoopは、インターネット上に公開されていたTCP/502ポートを持つENCOコントローラーを標的として使用されたことが示唆されています。
ENCOコントローラーは東ヨーロッパ全域に広く分布しており、Dragos社のFrostyGoopに関する調査では、Modbusプロトコルを使用して通信するICSデバイスが全世界で46,000台以上インターネットに露出していることが明らかになりました。
FrostyGoopはENCOデバイスを狙うために使用されましたが、その機能はこれらのデバイスに特化したものではなく、PLC、DCS、センサー、アクチュエーター、フィールドデバイスなど、他の一般的なICSデバイスとの通信も可能です。

最も懸念される点は、FrostyGoop が通常の操作と悪意のある活動を巧妙に組み合わせることで、一般的なアンチウイルスソフトウェアでは検出できなかったことです。ICS マルウェアの開発において、広く知られた ICS プロトコルの悪用がますます頻繁に行われるようになっており、OT に対応した高度な検知および対応手法の必要性が浮き彫りになっています。また、TAT24-24 は攻撃前にコントローラーのファームウェアをダウングレードしていたことが分かっています。

この攻撃では、インターネットに公開されたコントローラーとのネットワーク分離が不十分であったことが関係しており、基本的なサイバーセキュリティ対策を実施しないことのリスクと、その実施の重要性が浮き彫りになりました。

FrostyGoop マルウェア

Dragos社は、FrostyGoopおよび類似する8つのマルウェアサンプルを、オープンソースのリポジトリであるVirusTotal上で特定しました。
このマルウェアはGo言語で記述されており、ターゲットのIPアドレスをリスト化したJSONファイルを受け取る仕様です。
FrostyGoopは、TCP/502ポートを通じてModbusレジスタの読み書きが可能であり、ハードコードされたUnitIDとして254を使用しています。
多くのModbusデバイスではデフォルトのUnitIDが254に設定されているため、FrostyGoopはENCO Controlデバイスに限定されず、その他多数のModbus対応デバイスにも影響を与える可能性があります。

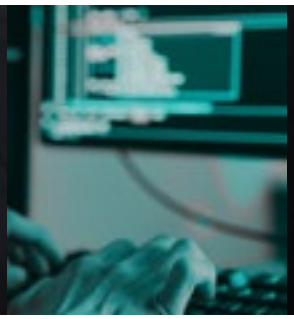


FrostyGoopからの教訓

FrostyGoopは、UnitIDが254に設定されたすべてのModbusデバイスに影響を与える可能性があります。
Dragosは、自組織のネットワーク内に存在する脆弱なデバイスを特定し、それらを継続的に監視することを推奨しています。これには、TCPポート502を介したModbus接続の監視も含まれます。
またDragosは、Modbus TCP/502へのアクセスを制限し、Modbusデバイスがインターネットからアクセス可能な状態になっていないか確認することを強く推奨しています。

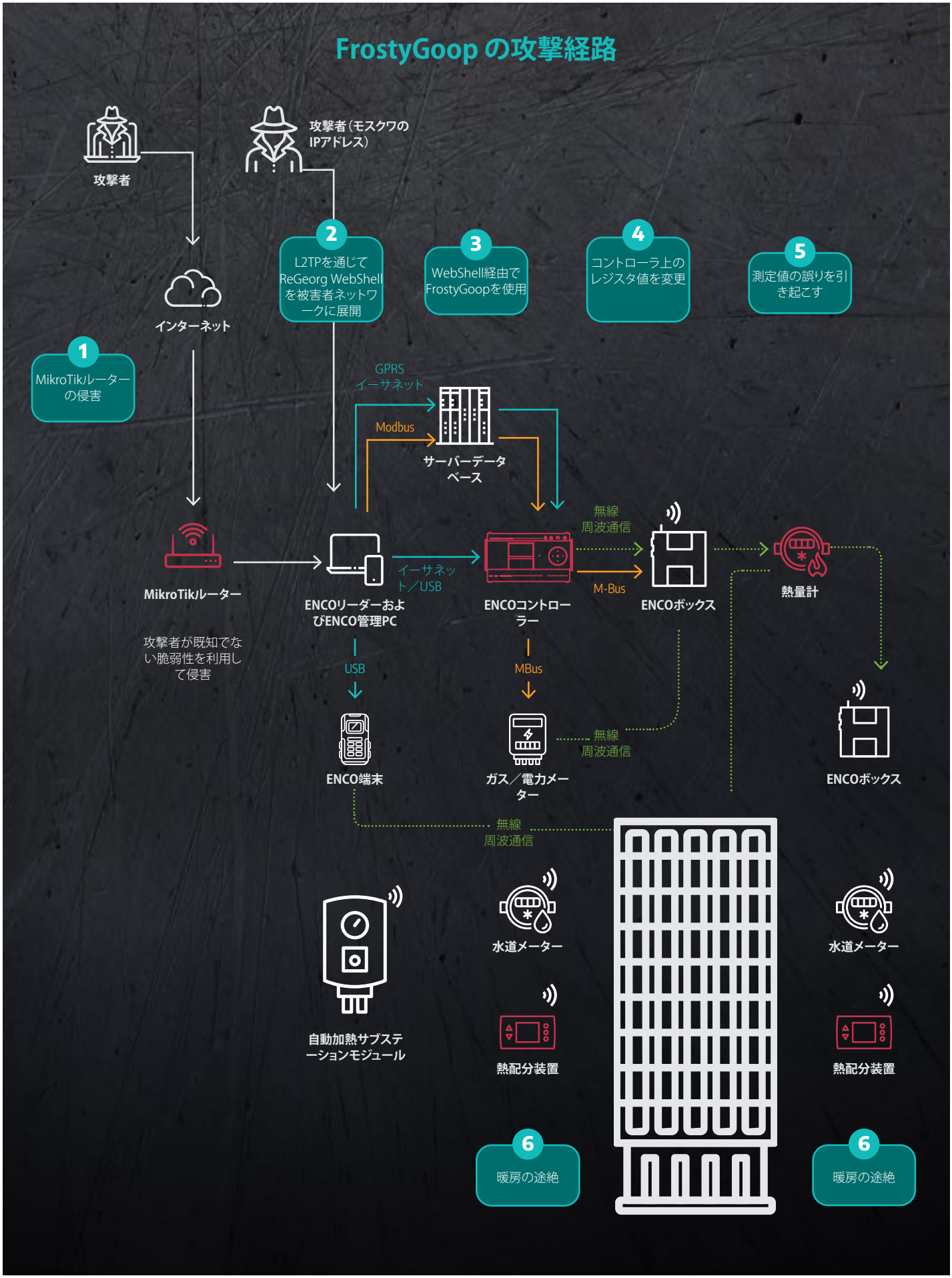
脅威ハンティングのためのヒント

OT Watchは、ファームウェアのダウングレードを監視しています。
環境内で、もし攻撃者がコントローラーのファームウェアを古いバージョンに戻していたとしたら、それに気づくことができますか？



Dragos Platformを使って、自環境内のUnitIDが254であるModbusデバイスを検索するためのクエリ:

```
type:"modbus" AND modbus_unit_id:"254" AND modbus_function_code: (3 OR 6 OR 16)
```


FrostyGoop の攻撃経路
攻撃者
攻撃者（モスクワのIPアドレス）
インターネット
1
MikroTikルーターの侵害
2
L2TPを通じてReGeorg WebShellを被害者ネットワークに展開
3
WebShell経由でFrostyGoopを使用
4
コントローラ上のレジスタ値を変更
5
測定値の誤りを引き起こす
GPRS
イーサネット
Modbus
サーバーデータベース
MikroTikルーター
攻撃者が既知でない脆弱性を利用して侵害
ENCOリーダーおよびENCO管理PC
イーサネット／USB
ENCOコントローラー
無線周波通信
M-Bus
ENCOボックス
熱量計
USB
MBus
ENCO端末
ガス／電力メーター
無線周波通信
ENCOボックス
無線周波通信
水道メーター
水道メーター
自動加熱サブステーションモジュール
熱配分装置
熱配分装置
6
暖房の途絶
6
暖房の途絶

ICS マルウェアの定義

2024年、Dragos社は過去の攻撃事例や自社の経験に基づいて、ICSマルウェアの定義を策定しました。この定義は、防御側にとって、ICSマルウェアが現実的に確度の高い脅威であり、インシデント対応計画、机上演習、脅威ベースライン策定など、シナリオベースの防御対策における前提として考慮すべき対象であることを示しています。

ICS マルウェアの定義

Dragos社ではICSマルウェアを以下のように定義しています：

> ***「OT環境に悪影響を与えることを意図して設計された、ICS対応ソフトウェア」***

この定義を満たす3つの特性：

- ソフトウェアがICS（産業用制御システム）に対して有効であること
- ソフトウェアが悪意を持って設計されていること
- ソフトウェアがOT環境に悪影響(Adverse Effects)を与える能力を有すること

あるサンプルをICSマルウェアと特定するには、これら3つの要件すべてに対する十分な証拠が必要です。すべての要件を裏付ける証拠が確認された場合、そのサンプルにはICSマルウェアの指定が与えられます。

ICSマルウェアの3つの特性

ICS対応（ICS-Capable）

SANSの定義によれば、ICS-Capableとは、OTネットワークやデバイス、ソフトウェアに対して、操作・変更・情報取得を行う機能を備えたソフトウェアを指します。つまり、ICSプロトコルを使用したり、PLCやその他のOTデバイスとやり取りする機能がコードに含まれているということです。
以下は、ICS-Capableなソフトウェアの例です：

- IEC104、OPCUA、HARTなどのICSプロトコルを使用するソフトウェア
- ラダーロジック・プログラムをアップロードまたはダウンロードできるソフトウェア
- PLC上で動作し、ラダー実行環境やOS内部と連携するソフトウェア
- エンジニアリングワークステーション上で動作し、プロジェクトファイルなどを変更するソフトウェア

この「ICS-Capable」という特性は、一般的なWindowsやLinuxのツールとは明確に区別されます。
たとえば、Process Hacker や通常のWindows/Linuxマルウェア、ランサムウェアの多くはICSプロトコルと関係がないため、ICSマルウェアとはみなされません。

悪意を持って設計されている

「悪意のある設計」という特性は、そのソフトウェアが防御目的や正当な用途ではなく、攻撃目的で作られているかどうかを見分けるために重要です。
たとえば、ITの世界でよく使われるPSExecは、攻撃者による横展開にも利用されますが、もともとはシステム管理者向けに設計された正当なツールであるため、マルウェアとは見なしません。[36] 同様に、一見ICSマルウェアのように見えるものであっても、悪意がない場合はICS研究用ツール、レッドチーム用ツール、あるいはベンダー製ソフトウェアのの一部機能が悪用されているだけかもしれません。
Dragosは、ソフトウェアが悪意を持って設計されたかどうかは、コードの機能および挙動、バイナリの類似性、開発者に関する情報、脅威グループとの関連性、インシデント対応時に得られたデータ、被害者や展開手段といった情報をもとに判断します。

OT環境に悪影響(Adverse Effects)を与える能力

この特性は、ソフトウェアが実際にOT環境に悪影響を与えうるかどうかを、分析者が証明する責任を課しています。また、OT環境において「有害」とみなされる行為のカテゴリを明確にし

[36]PsExec – Microsoft Learn

ます。
この特性を特定することで、次の問いに答えることができます：
「ICS-Capableを持つこのソフトウェアは、どのような悪影響を引き起こす可能性があるのか？」
悪影響(Adverse Effects)とは、ICSサイバーキルチェーンのステージ2で説明されている影響に類似しており、拠点や業界によって異なります。[37] 以下に、悪影響(Adverse Effects)の具体例を示します：

- 機密性の高いプロセス情報の収集
- OTデバイスへの不正アクセスを可能にする
- PLCに対するラダーロジックや実行コードのダウンロード
- OTファイアウォール等の回避
- セットポイントや変数、またはその他PLC設定の改ざん

では、もしマルウェアが正しく動作しなかった場合はどうでしょうか？
ツールがICSに対応しており、悪意を持って設計されていたとしても、OT環境に悪影響を及ぼす能力を持っていない場合、それは動作不良のマルウェア、または開発途中のマルウェアである可能性があります。

そのマルウェアが実行可能な状態の近さにより、「潜在的ICSマルウェア（potential ICS Malware）」と分類されることもあります。

[37]The Industrial Control System Kill Chain - SANS

ICSマルウェアの定義はアセットオーナーにとって何を意味するのか？

もし、SANS ICS「5つの重要管理策（5 Critical Controls）」を実施している場合、Dragosが提示するICSマルウェアのリストは、防御の優先順位を定めるための具体的な指針となります。[38]

たとえば、あなたの組織が Modbus/TCP を多用している場合、FrostyGoop型の攻撃にさらされるリスクがあります。
このようなマルウェアに関する情報を活用することで、「5つの重要管理策（5 Critical Controls）」の各項目について、自組織の実装状況を検証することができます。

同様に、アセットオーナーは、報告されている他のICSマルウェアファミリーを参照することで、自社の防御体制を評価するセキュリティ演習を実施することも可能です。
以下の図では、FrostyGoopを例に使ったセキュリティ演習の例を紹介しています。

.

標的型ICSマルウェアによる運用停止は、当社の顧客が共通して懸念している事項であり、Dragosの新しい「Threat Baseline（脅威ベースライン）」サービスで検討されている威イベントの一つです。
このThreat Baselineを通じて、Dragosは各組織が自社ネットワーク内のデバイスに対するFrostyGoopによるModbus TCP攻撃の潜在的な影響を特定し、緩和策の特定および攻撃からの回復を支援してきました。
Threat Baselineは、産業環境が各社固有の構成であることを浮き彫りにしました。
また、さまざまな視点から脅威を検討することで、一般的ではないものを含めたセキュリティ上の弱点を明らかにするのに役立ちました。

ICSインシデント対応計画
（シナリオプランニング）

- 攻撃者が私たちのModbus/TCP コンポーネントを攻撃するには、何をする必要があるか？
- 自社環境では、Modbus/TCPコンポーネントのプログラムや設定はバックアップされているか？（オンライン／オフライン）

防御可能なアーキテクチャ
（資産識別／重要資産）

- Modbus/TCP によって制御されているプロセスには、どのようなものがあるか？
- 自社環境には、Modbus/TCP デバイスが何台存在しているか？

ネットワークの可視性と監視

- 自社ネットワーク内のデバイスが不要なModbus/TCP 通信を発信していないか？
- Modbus/TCPデバイスに対する新規および好ましくない通信を識別できるか？

セキュアなリモートアクセス

- Modbus/TCP デバイスがインターネットに公開されていないか？

リスクベースの脆弱性管理

- FrostyGoop攻撃の調査結果は、攻撃者が外部公開ルーターのアクセスを取得できたことを示唆している。自社内のルーターに存在する脆弱性は何か？それは適切に緩和されているか？

[38]The Five ICS Cybersecurity Critical Controls – SANS

ハクティビストたちは、地政学的な対立に加担する形で、サイバー上での活動を継続している

最近の地政学的な対立（例：イスラエルとハマス、ウクライナとロシアの紛争）は、ハクティビズムと国家の戦略目標との関係をさらに強めています
ハクティビストグループである CyberArmyofRussia_Reborn（CARR） は、引き続きアメリカの重要インフラ分野、特に上下水道および石油・天然ガス部門を標的にしています。
実際に、カリフォルニア州、フロリダ州、ペンシルベニア州では、このグループによる攻撃が確認されています。

親ロシア派のハクティビストグループCyberVolkは、パキスタンの重要インフラに対する攻撃を予告し、新たな「CyberVolkランサムウェア」の開発を進めていると発表しました。
このような動きは、ハクティビストたちが破壊的なマルウェアを利用して、活動の影響力をさらに拡大する可能性を示しており、非常に憂慮すべき傾向です。
2024年7月には、CARR（CyberArmyofRussia_Reborn）、CyberVolkを含む50を超える個人・集団が連携し、「Holy League（ホーリーリーグ）」という親ロシア系ハクティビスト連合体を結成しました。
この連合は、NATO、欧州諸国、ウクライナ、イスラエルに対する重大な脅威となっており、彼らの連携と攻撃能力は、世界中の産業組織に対するリスクをさらに高めています。

ハクティビストが重要インフラへの影響を主張

ハクティビズムは、現代におけるアクティビズムの一つです。DDoS（分散型サービス拒否）攻撃、ウェブサイトの改ざん、インターネット上に公開された機器へのアクセスといった手法を用い、政治的または社会的な主張に注目を集めることを目的としています。
こうしたハクティビストが自称するグループ名、個人名、ブランドは自己宣言によるものであり、確立された組織体ではないことがほとんどです。
2022年以降、ハクティビストたちは、Shodan、Censys、Kali Linuxなどの無料または市販のツールを活用し、脆弱または設定ミスのある標的（OT/ICS OEM製品を含む）を発見・悪用する傾向を強めています。

Dragos OT-CERT は、産業インフラにおけるOT（運用技術）分野のリソース不足に対応することを目的とした、OT専用のサイバー緊急対応チーム（Cyber Emergency Readiness Team）です。
このチームは、産業インフラのアセットオーナーおよび運用管理者を支援するために設計されており、OT/ICSコミュニティに対して無償のサイバーセキュリティリソースを提供しています。

OT-CERTがTAT24-76によるHMI侵害を被害者に通知

2024年9月、Dragos社はPythonベースのマルウェア「kurtlar.exe / kurtlar_scada.exe」を発見しました。
このマルウェアは、インターネットに公開されたVNCサーバに接続し、そのアクセス画面のスクリーンショットを取得します。
このマルウェアに関する証拠をもとに、DragosはTAT24-76が「kurtlar.exe」を使用して、インターネット上に公開されていた複数のVNCサーバ（HMIをホストしているもの）を侵害したと主張しているTelegramチャンネルを特定しました。

Dragos社では、未確認または進行中のサイバー脅威グループや活動に関する情報を追跡・共有するために、「一時的活動スレッド（TAT：Temporary Activity Threads）」を使用しています。
TATは、脅威グループとして正式に分類されるにはまだ十分な分析が行われていないものの、一定の関連性が見られるサイバー脅威活動集合体に対する暫定的な分類を可能にしています。

TAT24-76 は、kurtlar.exe / kurtlar_scada.exe を開発し、Telegramチャンネル内で以下のようなさまざまな提供内容を宣伝していました。：

- Web shellを用いた、公共・民間組織への初期アクセス手

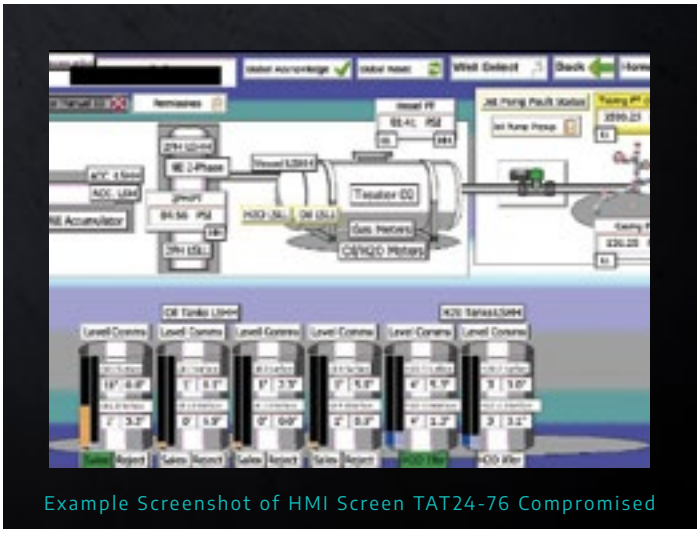
段

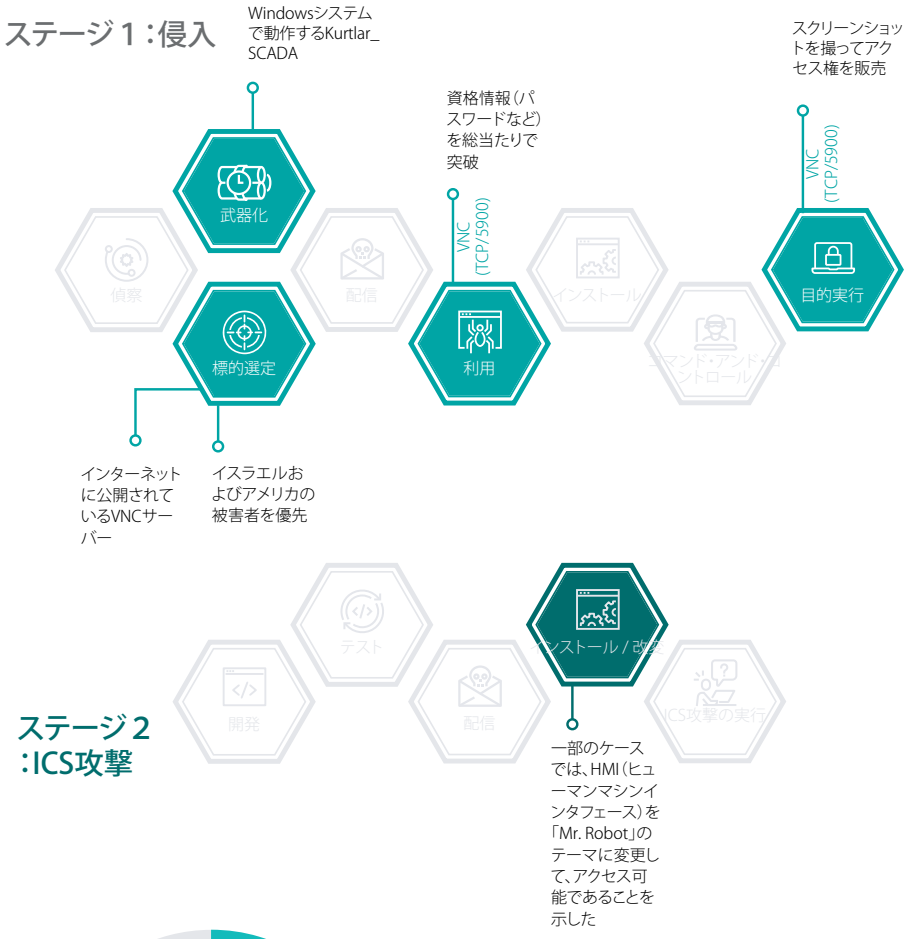
- HMIおよびSCADA機器へのVNCアクセス情報
- エクスプロイト（主にWordPressを対象としたもの）
- Databaseダンプ
- VIPチャンネル
- インターネットに公開された機器の特定方法
- その他のエクスプロイトやマルウェアに関する情報

TAT24-76 は、自身のTelegramチャンネルを使って、マルウェアの販売を行っています。その際、攻撃成功の証拠として、侵害されたHMIのスクリーンショットなどを提示しています（右図参照）。Dragosがこれらのスクリーンショットを調査した結果、被害者の一部が実際に侵害されていたことが判明し、DragosのOT-CERT被害者通知サービスを通じて通知が行われました。
OT-CERTは、侵害された被害者への通知を行い、TAT24-76によるさらなるアクセスや、マルウェア購入者による侵害の継続を制限することができました。

kurtlar.exe および kurtlar_scada.exe は、構造こそ単純ではあるものの、インターネット上に公開され、セキュリティが不十分なVNCサーバを実行している産業機器に対して効果的に機能しています。この脅威に対する対策としては、以下のような手段が有効です：

- すべてのVNCサーバへのアクセス制限を行う。特に TCPポート5800、5900、5901 に注意する。リモートアクセスが必要な場合は、VPNを利用する。
- デフォルトや脆弱な認証情報を確実に変更すること。.





9%

OT Watchは、**顧客全体のうち9%**がVNCを使用して外部アドレスと通信していることを確認しました。

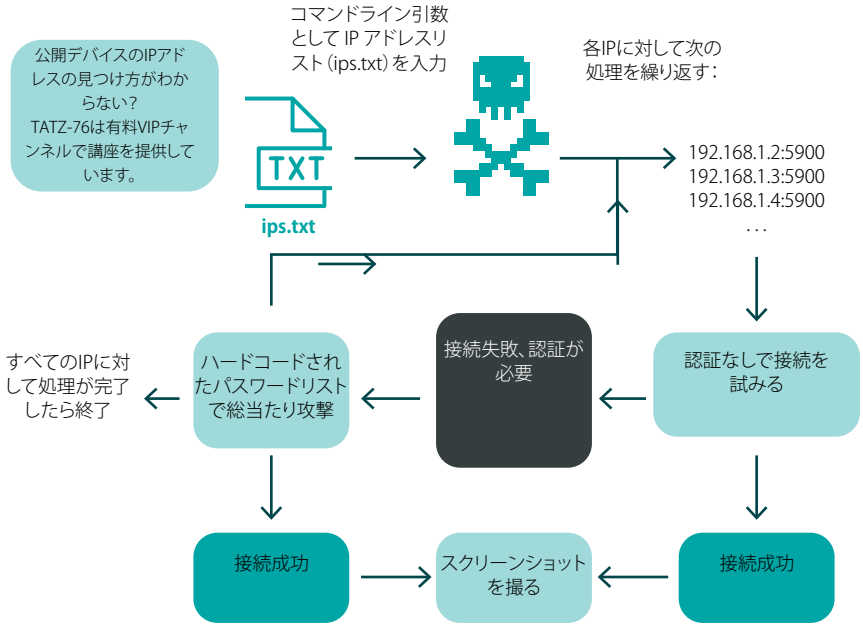
*これらの環境のうち一部は、適切な設定が行われていませんでした。

kurtlar.exe / kurtlar_scada.exe — VNCマルウェア

kurtlar.exe iは、標的のIPアドレス一覧に対して順番に実行されます。

kurtlar_scada.exe は、TCPポート5800、5900、5901 を使用してVNC接続を試み、ハードコードされた認証情報リストを使ってログインを試行します。
ログインに成功すると、接続先のIPアドレスと使用した認証情報を記録した上で、スクリーンショットを取得します。

kurtlar.exe / kurtlar_scada.exe の実行フロー



CyberArmyofRussia_Reborn と Z-Pentest

CyberArmyofRussia_Reborn（CARR）は、Dragosによって TAT24-22 として追跡されている、親ロシア派を自称するハクティビストグループです。
TAT24-22 は、NATO諸国および東欧諸国を標的とし、注目を集めることで、ロシア政府からの正式な支援を得ることを狙っていると見られています。
TAT24-22 は、DDoS攻撃およびインターネットに公開されたOT/ICS機器へのアクセスを行っています。
ただし、取得したOT/ICS機器のインターフェースや、操作による影響をどこまで理解しているかは疑わしく、議論の余地があります。
実際、多くのインシデントにおいて、OT機器へのアクセス後にその機器の場所や業種の分類を誤認していた例が確認されています。
彼らのスキルには疑問が残るものの、米国の上下水道およびエネルギー施設への攻撃が確認されており、さまざまなレベルの障害を引き起こしました。
さらに、以下の国や分野の組織を標的とした攻撃があった可能性が指摘されています：

- ルーマニア、ポーランド、フランスの上下水道分野
- スペインの食品・飲料業界
- アメリカおよびドイツのエネルギー分野

これらの確認された攻撃およびOT/ICS組織を標的とした作戦活動を受け、2024年7月、米国財務省はCARRのメンバーに対して制裁を発動しました。[39]

その後、2024年9月には Z-Pentest（Dragosにより TAT24-56 として追跡）が登場しました。TAT24-56は CyberArmyofRussia（CARR）からインターネット上に公開されたOT/ICS機器を標的とした活動の大部分を引き継いだと見られています。

Hunt3r Kill3rs

Hunt3r Kill3rs は、自らをハクティビストとして名乗るグループであり、Dragosによって TAT24-45 として追跡されています。
同グループは、ヨーロッパ、イスラエル、アメリカのインターネットに公開されたOT/ICS機器を標的とし、特に脆弱な認証設定やデフォルトの認証情報を悪用する形で活動を拡大しています。
高度な技術力を持っていないにもかかわらず、Hunt3r Kill3rs は ICSサイバーキルチェーンのステージ2にまで到達し、機器のデータフィールドの改ざんや、公開されたコントローラーのパスワードリセットを3回にわたって成功させました。

[39]米国財務省、Cyber Army of Russia Reborn のリーダー及び主要メンバーに制裁– U.S. Dept. of the Treasury

Dragosは、これらの攻撃による実際の運用への影響を被害者側から確認することはできなかったものの、このような侵害は「制御の喪失」「可視性の喪失」「運用の混乱」などを引き起こす可能性があります。
Hunt3r Kill3rs のような機会的に標的を選ぶ行動や、Telegram上での活動は、産業環境に対する脅威が拡大していることを示しています。
特に、些細な侵害であっても重大な運用障害につながりかねない環境にとって、そのリスクは深刻です。
Dragosは、Hunt3r Kill3rs がインターネットに公開されたデバイスを利用して知名度を高めようとしている様子を観測しており、この行動は、自己宣言型ハクティビストの間で広がっている傾向とも一致しています。

高度な攻撃者（国家支援型のAPTなど）とハクティビストの融合

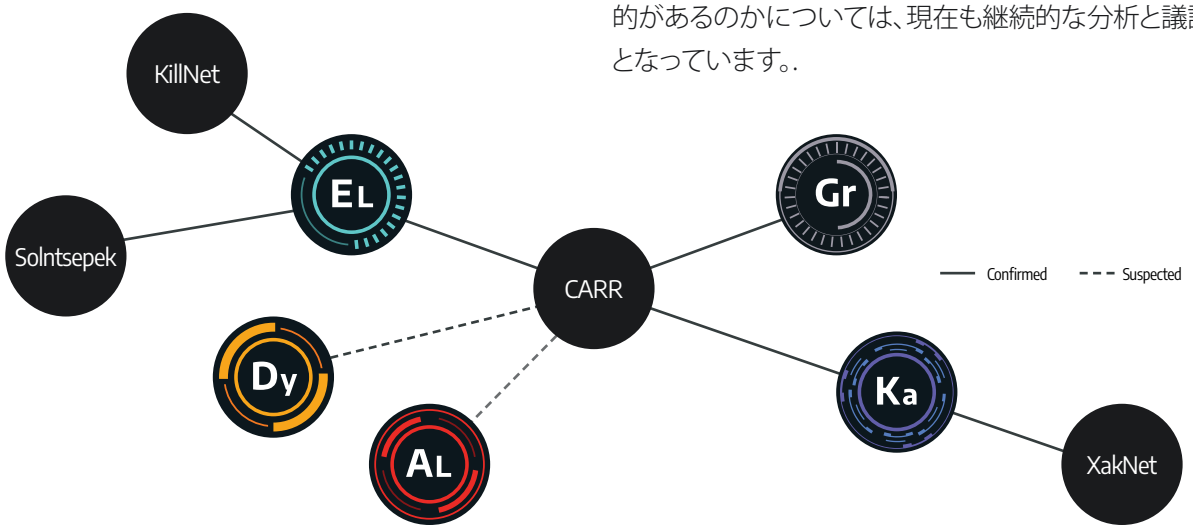
高度な攻撃者（国家支援型のAPTなど）とハクティビストの間で、利害の一致が進んでいます。
Dragosは、両者がOT/ICSを標的とした攻撃において、インフラやインテリジェンス（情報）を共有して使用している事例を確認しています。
2022年以降、以下のグループ間で明確な連携が確認されています：

- GRAPHITEとCARR
- KAMACITE とCARR
- ELECTRUMとCARR
- ELECTRUMとKillNet
- ELECTRUMとSolntsepek
- KAMACITEとXakNet

また、以下のグループ間でも連携が疑われています：

- DYMALLOYとCARR
- ALLANITEとCARR

ICSの防御対策を行う際、この連携の意味合いは非常に大きいものになります。
なぜなら、敵対者はより大きな目的に基づき、スパイ活動を目的とした作戦と、破壊的な攻撃との間を行き来する可能性があるからです。
そしてその過程で、ハクティビストのペルソナを利用して、技術的には高度でない攻撃を実行することもあります。
ハクティビストのペルソナが果たす役割が、主たる攻撃から注意をそらすための意図的な陽動であるのか、それとも別の目的があるのかについては、現在も継続的な分析と議論の対象となっています。.



Confirmed and Suspected Overlaps in Ukraine

ランサムウェアの現状

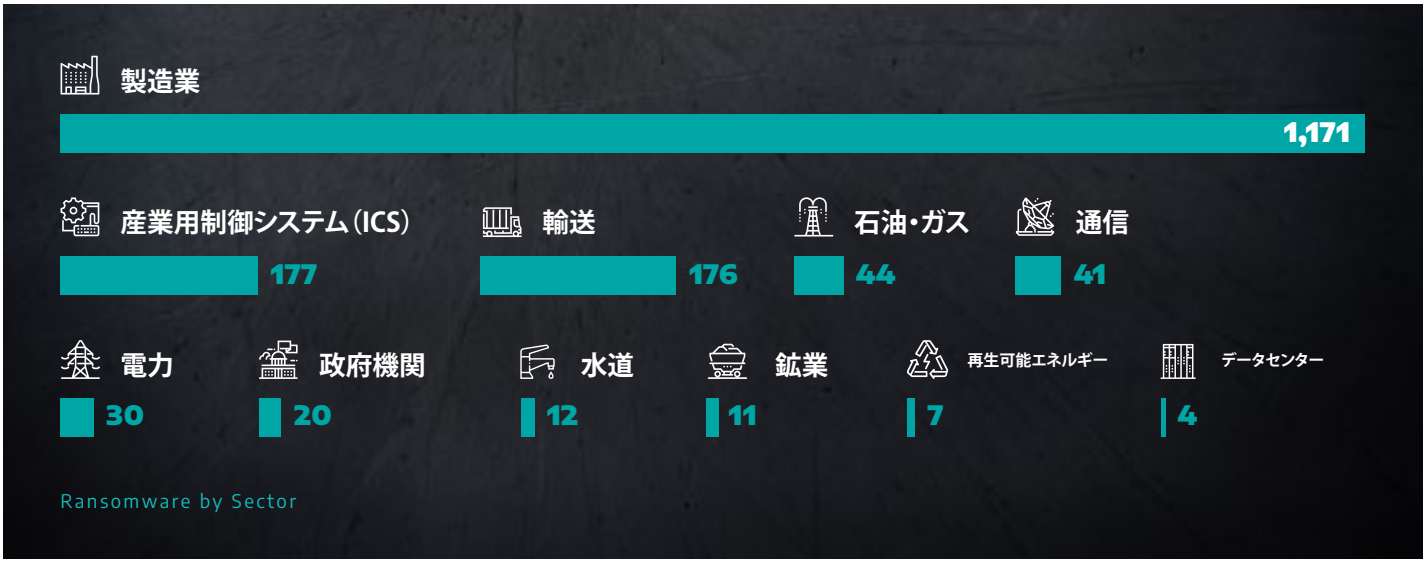
ランサムウェアは、業務妨害性が深刻な為、複数の産業分野にとって大きな脅威となっています。
Dragos社が、2022年に産業組織に対するランサムウェア攻撃の増加を初めて観測して以来、攻撃件数は年々2倍のペースで増加しています。

2024年、Dragosは1,693の産業組織に関する機密データや情報が、複数のランサムウェアグループのリークサイト（DLS）に掲載されていることを確認しました。
DLSへの掲載が必ずしもランサムウェア攻撃の成功を意味するわけではありませんが、掲載件数の多さと増加傾向の明確さは、多くの産業組織が複数のランサムウェアグループから攻撃を受けている現状を浮き彫りにしています。
これらの現状は、すべてのOT/ICSアセットオーナーおよび運用者、産業組織に対し、ランサムウェアの脅威を十分に理解し、自組織のセキュリティ体制および運用への影響を真剣に考えていく必要があることを示しています。

2024年後半の攻撃件数は、前の2四半期と比べて2倍以上に増加しました。
ランサムウェア活動の増加を引き起こした要因は明らかではありません。
考えられる要因としては、2024年初旬に主要なランサムウェアグループに対して法執行機関が措置を行ったこと、侵入経路が増加したこと、そして2024年後半に新たなランサムウェア攻撃者が登場したことなどが挙げられます。

Dragosは、2024年にICS（産業用制御システム）に特化したランサムウェアを特定することはありませんでしたが、ランサムウェア攻撃者は、生産ラインの停止、サプライチェーンの障害、機密データの窃取などを引き起こしており、これらのデータは攻撃活動に容易に利用される可能性があります。
また、2024年のランサムウェアオペレーターは、ダウンタイム（停止時間）への許容度が低い組織を優先する形で、被害者の選定を行っていた可能性が極めて高いと考えられます。

製造業は、産業組織に対するランサムウェア攻撃の最大の標的となっています。
観測された全ランサムウェア被害のうち50%以上が製造業に集中しており、1,171件の攻撃が確認されました。
ランサムウェアグループは、わずかな業務中断であっても重大な財務的・物流的損害を引き起こし、安全性にも影響を与える可能性があることを理解しています。また、これらの要因から、製造業が身代金を支払う可能性が高いことを把握しています。
エネルギー、交通、産業用制御システムのベンダーなど他の産業分野もまた、ランサムウェアグループによる標的リストの上位に位置しており、彼らは圧力と影響力を最大化するために戦術を洗練し続けています。



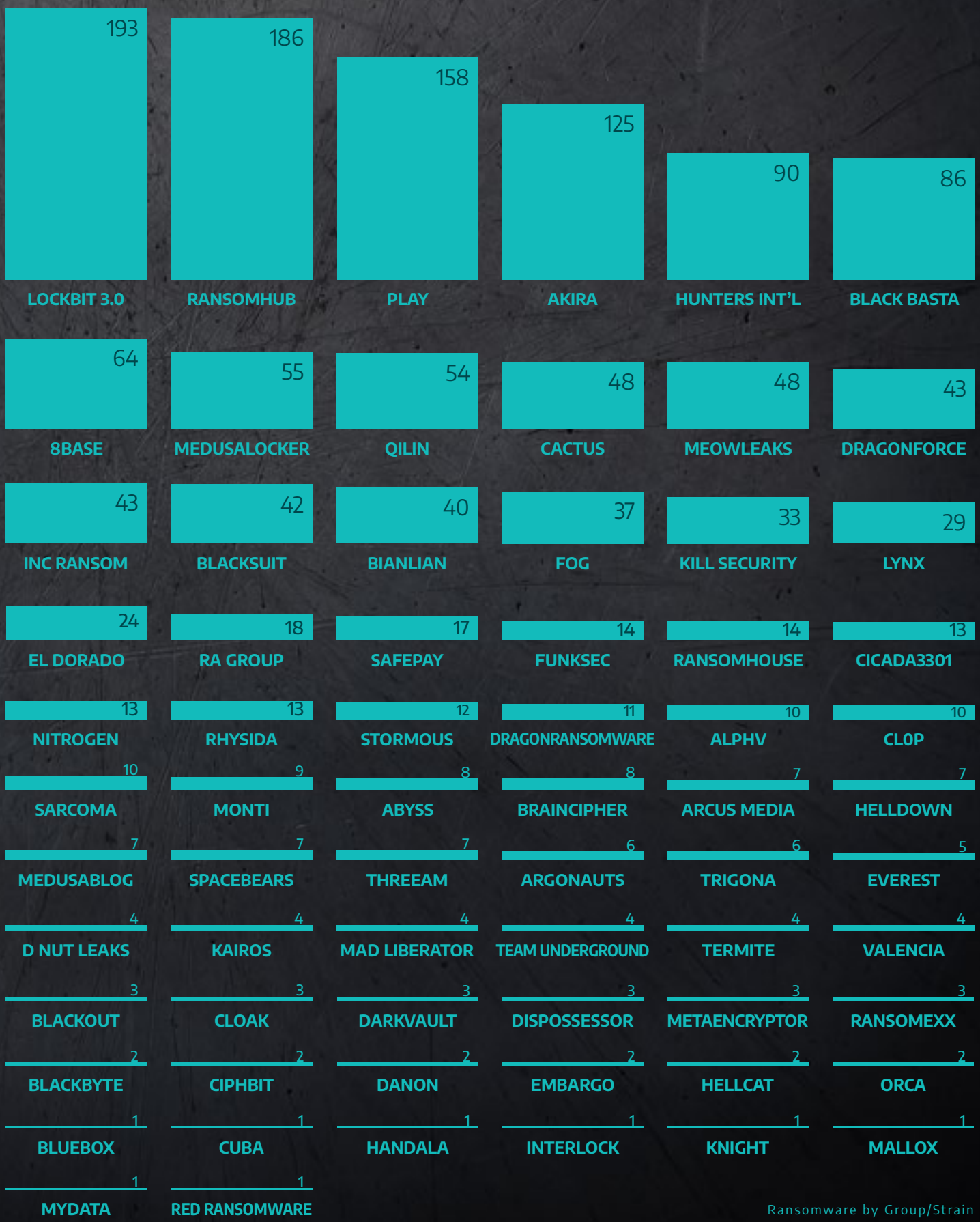
これらの脅威が衰える兆しを見せていない為、各組織はレジリエンス（復元力）、積極的な防御策、そしてインシデント対応体制の整備を最優先に取り組む必要があります。
産業組織に対するランサムウェア攻撃は一様に分布しているわけではなく、
地政学的な緊張、経済的な利害、攻撃者の注目度によって、特定の地域に集中している傾向があります。
北米では984件の攻撃が確認されており、これは全体の58%を占めます。
次いで欧州が419件で、全体の25%を構成しています。
こうした地域ごとの傾向を理解することは、防御力の強化、将来の脅威の予測、そしてリスクに即したセキュリティ戦略の策定を実施する上で極めて重要です。

Dragosは2024年に、約80のランサムウェアグループを追跡しました。
これは、2023年に観測された50グループから60%の増加にあたります。

これらのグループは、2024年前半の時点で、週あたり平均34件の産業組織への攻撃を実行しており、その数は後半には2倍以上に増加しました（次ページの図表を参照）。

産業組織を最も活発に標的としていたランサムウェアグループは、RansomHub、Fog、LockBit3.0 でした。
特に RansomHub は、2024年2月以降に、CyclopsやKnightからのランサムウェアアフィリエイトを引き入れることで勢力を急拡大しました。
彼らは、複数の重要インフラ分野に対する300件以上の侵害を行ったと主張しています。
Fog も同様に、2024年を通じて産業分野への攻撃を拡大し、脆弱なリモートサービスやアプライアンスを標的とする主要なランサムウェアグループの1つです。
LockBit3.0 に関しては、2024年2月に国際的な法執行作戦「Operation Cronos」により活動が妨害されましたが、その後も執拗に活動を継続し、1 年を通して産業組織に対する脅威であり続けました。[40, 41]

[40]英国NCA、「オペレーション・クロノス」によるLockBitに対する活動妨害を発表- NCA [41]明らかになる余波：「オペレーション・クロノス」による歴史的妨害の後、LockBitに及んだ影響– TrendMicro



Ransomware by Group/Strain

2024年におけるランサムウェアの動向

Dragosは、2024年のランサムウェア脅威において、2つの注目すべき傾向を観測しました：

- ランサムウェア攻撃者によるリモートツールやサービスの利用
- 地政学、ハクティビズム、ランサムウェアの融合

リモートツールとリモートサービスを悪用するランサムウェア攻撃者

2023年以降、Dragosは、全体的な傾向としてリモートサービスを標的とした攻撃を行っていることを確認しました。この傾向は、攻撃者が基本的なネットワークセキュリティ防衛策の欠如を悪用している状況を示しています。
またこの傾向は、2024年も継続しています。ランサムウェア攻撃者の多くは、VPNアプライアンスなどのリソースを利用して、被害者ネットワークへの初期侵入を果たし、侵害済みシステム内で横移動を行うことで、ICSサイバーキルチェーンのステージ1を達成しています。
また、ランサムウェア攻撃者はパス・ザ・ハッシュ、ブルートフォース、クレデンシャルスタッフィングといった認証情報ベースの戦術を用いて、多要素認証（MFA）を回避する手法も確認されています。
以下は、その一例です：

- EldoradoおよびPlayランサムウェアグループは、VMware ESXi環境を攻撃し、仮想マシンの暗号化または無効化を試みました。[42, 43]
- Akiraランサムウェアグループは、2024年を通じて脆弱なVPNアプライアンスを悪用し、初期アクセスを獲得し続けました。

ランサムウェアグループは、脆弱なリモートサービスを悪用することに加え、LOTL（Living Off The Land）戦略も活用していました。
LOTL戦略とは、PowerShell、certutil.exe、PsExec などのネイティブな管理ツールを使用し、侵害活動を隠蔽しながら、長期間にわたり検出を回避する手法です。

Dragosが2024年に対応したランサムウェアインシデントのうち、ITシステムとOTシステムの間で厳格なネットワークセグメンテーションを実施し、オフラインバックアップのテストを行っていた被害組織では、復旧時間が大幅に短縮され、身代金の支払いを回避することができました。
一方で、ネットワークセグメンテーションを実施しておらず、リモートアクセス経路のセキュリティも不十分だった組織では、復旧にかかる時間が長引き、対応により多くのリソースを要し、生産停止による影響が深刻化し、修復にかかるコストも増加する結果となりました。

Dragosが実施したランサムウェア被害におけるインシデント対応は、「リモートサービスの標的化」という傾向を強く反映していました。
実際、Dragosが2024年に対応したランサムウェアインシデントの50%以上において、VPNアプライアンスやリモートデスクトッププロトコル（RDP）サーバーなど、何らかのリモートサービスが攻撃者に利用されていました。
さらに、対応したインシデントのうち25%はOT/ICS環境全体の停止を引き起こし、残りの75%でも部分的な障害が発生していました。

この傾向は、ランサムウェアのエコシステム内にも反映されていることがDragosのインシデント対応から観測されました。ランサムウェアのエコシステム内では、初期アクセスブローカー（IABs）が、ハイパーバイザー、VPNアプライアンス、リモートアクセスソリューションに存在する未修正の脆弱性を悪用するケースが一般的となっています。
これらの脆弱性は、公に開示されてから数時間以内に悪用されることも多く、ランサムウェアのアフィリエイトにとって、産業組織を攻撃し、被害者環境内に重要な足がかりを築くため

20%
OT Watch は、顧客環境の20%において VMware ESXi を検出しました。

43%
OT Watch は、顧客の43%が RDP プロトコルを使用して外部アドレスと通信していることを確認しました。
*これらの環境の一部はチューニング（最適化）されていない状態です。

[42]新たなランサムウェア「Eldorado」、WindowsおよびVMware ESXi仮想マシンを標的に – Bleeping Computer [43]Playランサムウェアグループの新しいLinux亜種、ESXiを標的に — 悪名高い「Puma」との関係が示唆される– Trend Micro

の低コストかつ容易な手段となっています。

これらの調査結果は、多くのランサムウェアグループが、産業組織を標的とし、ネットワークやセキュリティの基本的な防衛策の欠如を悪用など参入障壁の低い侵入手法を利用して攻撃を行っている状況を示しています。
これらの要素が適切に対処され、保護されない限り、ランサムウェアグループは今後もそれらを攻撃手段として利用し続けるでしょう。

地政学、ハクティビズム、ランサムウェアの融合

2023年から2024年初頭にかけて、Dragosは、ハクティビストグループまたは自称ハクティビストグループが、産業組織や世界各地の重要インフラ・サービスを標的とし、ICSサイバーキルチェーンのステージ2に到達しているという傾向を観測しました。
そして2024年には、ハクティビズム脅威における新たな進展が見られました。
それは、ハクティビストや自称ハクティビストのグループが、さまざまな対象への攻撃においてランサムウェアを作戦の一部として利用しはじめているというものです。

2024年において、次の3つの著名なハクティビストグループが、作戦の中で積極的にランサムウェアを使用していました：Handala、Kill Security、CyberVolk。

CyberVolkは、2024年6月にランサムウェア・アズ・ア・サービス（RaaS）を開始し、同年7月には独自の「CyberVolk」ランサムウェアの開発を発表しています。[44] CyberVolkは、CyberArmyofRussia_Reborn（CARR）などのハクティビストペルソナをメンバーに含むハクティビスト同盟「Holy League」の自称メンバーであり、主にNATOに同調する国々を標的として、DoS攻撃やランサムウェアを用いた攻撃を展開しています。
彼らの活動内容やSNS上での主張に基づくと、CyberVolkはロシアを支持していると見られます。

経済的・政治的・イデオロギー的な利害の融合が、2025年以降のランサムウェア脅威の状況に影響を与える可能性は高いと考えられます。
特に、公共の安全や経済の安定にとって重要な分野、つまりハクティビストや自称ハクティビストグループにとって戦略的標的と見なされる分野において、その傾向が顕著になると見られます。
そのため、OT/ICSアセットオーナーが、自組織が地政学的緊張の高い地域で事業を展開している場合や、公共向けの重要インフラ・サービスを提供する分野に属している場合は、より地政学的リスクに対する意識を高める必要があります。

[44]ランサムウェアグループの実態解明：CyberVolk ランサムウェア - RAPID7

Dragosによるインシデント対応から得られた知見

2024年を通じて、Dragosのインシデント対応では、主に３種類のインシデントが観測されました：ランサムウェアによる侵害、運用上のエラー、そしてレガシーマルウェアの感染です。
ランサムウェアや運用ミスに関連するインシデントは、OT（運用技術）業務の部分的または全面的な停止を引き起こしました。また、レガシーマルウェアは依然としてOT環境における課題であり、セキュリティ体制の脆弱化を招いています。

ランサムウェアインシデント

Dragosが対応したインシデントの大半は、ランサムウェアによる侵害が占めており、そのうち25%はOTサイト全体の停止につながり、75%は何らかの業務障害を引き起こしました。
また、全インシデントの20%は、リモートアクセスの脆弱性を悪用されたものであり、VPNの脆弱性、リモートアクセスアプリケーション、企業ネットワーク経由のRDPなどが含まれていました。

IT関連のランサムウェアインシデントではデータの持ち出し（情報漏えい）が一般的ですが、DragosはOT環境において、攻撃者がデータを外部に持ち出した形跡を確認していません。攻撃者は、ランサム要求の一環としてデータの持ち出しと公開を組織に対して明示的に脅迫していたものの、実際にはその脅しを実行には移しませんでした。
身代金の支払いは一切行われず、各組織は攻撃者と交渉することなく業務を回復させるための十分な能力を有していました。
とはいえ、Dragosは、バックアップが必ずしも即時に利用できる状態ではなかったことや、実際に報告されたインシデントの多くで拠点が物理的に大きな影響を受けていたことを指摘しています。

運用上のエラーによるインシデント

ランサムウェアを除くと、次に多かったインシデントのタイプはハードウェア設定の誤り、機器の故障、または人的ミスによる運用エラーでした。これらのインシデントはいずれも、何らかの形で業務の中断を引き起こしていました。
こうしたインシデントは当初、攻撃者による活動が原因である可能性があるとしてDragosに報告されましたが、調査の結果、OT関連のサイバーセキュリティインシデントではないと結論づけられました。
Dragosは、攻撃によるものかどうかが明確でない場合であっても、インシデント対応契約（リテイナー）を発動することを組織に推奨しています。
インシデント対応者は、ネットワークおよびホストデータの解析能力を有しており、これは多くの場合、プロセスエンジニアや運用担当者が持ち合わせていない能力です。
これだけでも、根本原因の分析にかかる時間を大幅に短縮でき、平均復旧時間（MTTR）の低減につながります。.

レガシーマルウェア

Dragosのインシデント対応では、レガシーマルウェアによるインシデントも確認されています。これはランサムウェアと似ていますが、「WannaCry」など過去にOTシステム内に存在していたマルウェアが原因であるため、Dragosでは別カテゴリとして追跡しています。
これらのマルウェアは、パッチ未適用、設計上の欠陥、古いオペレーティングシステムの使用などに起因して、レガシー環境内に残存し、既知の脆弱性を突いて感染を広げ続けます。
多くの場合、このようなマルウェアは“ヘッドレス（制御不能）”な状態にあり、感染拡大はしても、現在の攻撃者が操作可能なわけではありません。
ヘッドレスマルウェアの存在は、アクティブな侵入の兆候ではないものの、組織全体のサイバーセキュリティ対応体制の弱体化や、復旧に多くの時間と労力を要する要因となります。
さらに、ヘッドレスマルウェアによって発生するセキュリティ監視アラートは、他のポリシー違反やパッチ管理の不備といった、より広範な問題の兆候である可能性もあります。

ネットワークセキュリティ監視の重要性

ICSプロトコルに対応したネットワークの可視化は、侵害の可能性がある範囲を迅速に特定し、さらに分析すべきシステムを識別するうえで極めて重要です。
ある事例では、インシデント発生前に既にDragos Platform が当該拠点に導入済、かつDragosのOT Watchチームが継続的に監視していたことにより、根本原因の特定、復旧作業、緩和策の実施を約15時間で完了できました。

他のケースでは、インシデント後にセキュリティ監視を導入した場合でも、OTネットワークの隔離解除に向けた判断を迅速に下せ、結果としてダウンタイムを大幅に短縮するうえで重要な役割を果たしました。
一方で、何らかの理由でネットワークベースのセキュリティ監視が実施できなかった場合、影響範囲の特定や原因分析は、ホストベースのフォレンジック調査やログレビューのみに依存することになりました。その結果、現場のOTシステムからフォレンジックデータを収集するために多大な労力を要するだけでなく、分析にかかる時間も大きく延びました。
もしプロセスログにセットポイントの変更や読み取り操作が記録されていなかった場合、アクセスやプロセス操作の有無を検証することは不可能になります。
インシデント発生前にICSプロトコルに対応したネットワーク監視を導入していれば、コントローラーへの読み取り・書き込み通信を検出でき、プロセスの改ざんがあったかどうかを確認するのが容易になります。
また、たとえ根本原因が人的ミスやハードウェア故障であったとしても、監視を行っていれば問題の特定を迅速に行うことができ、分析時間と全体のダウンタイムの双方を削減できます。

基本が重要

繰り返しになりますが、SANS ICSの「5つの重要管理策（5 Critical Controls）」を実施している組織は、侵害が発生した場合でもOTへの影響を大幅に軽減することができ、完全な侵害に至る前に対応するための十分な時間を確保できる可能性が高くなります。
また、分析が必要な際に保護すべき重要なプロセスやシステムを把握し、そこからデータを収集できる体制が整っており、可能性の高いシナリオに焦点を当てたインシデント対応プレイブックを備えていることで、対応者の作業を効率化することが可能になります。
基本を正しく実行することに投資すれば、被害の影響は小さくなり、ダウンタイムも短縮されます。
.

脆弱性について

産業用システムは、もともとサイバーセキュリティを前提に設計されたものではありません。しかし今日では、攻撃者たちがOT機器やプロトコルの弱点を積極的に探し出そうとしています。パッチ適用が不可能な欠陥や設計上の制約など、これらの脆弱性は、攻撃者が運用を妨害したり初期アクセスを得たりするための入り口となります。
脅威が進化するなかで、私たちの対応も進化しなければなりません。単なるパッチ対応にとどまらず、リスクを的確に理解し、それが悪用される前に緩和することに重点を置く必要があります。

フィールドバス：サーボドライブ新たな研究分野を切り拓く

Dragosは2024年もフィールドバスプロトコルに関する調査研究を継続しました。[45] 今年は、サーボドライブに実装されているCANopenプロトコルに焦点を当てた研究が行われました。この調査の主要な発見は、CANopenのような多層プロトコルが組織にもたらすリスクと、それらの攻撃を検知する仕組みが不足しているという点です。このような多層構造を持つプロトコルは「ターダッキン（Turducken）プロトコル」と呼ばれ、今後の新たな研究分野として注目されています。
短期的には、Dragosは、一般的なPLCネットワークプロトコル上でCANopenを利用したさまざまな攻撃に対して、シグネチャベースの検知機能をすでに実装しています。長期的には、フィールドバス機器におけるTurduckenプロトコルへの対応を目的としたツールの導入を計画しており、それにより攻撃の検出や設定ミスの特定における可視性を大幅に向上させることが期待されています。

Turduckenプロトコルとは、複数のアプリケーション層プロトコルが階層的に重ねられたプロトコル構造を指します。
Dragosが2024年に行った調査では、Modbus-RTUがCANopen上に重ねられ、さらにそれがCODESYSの独自プロトコル内部に格納されているというプロトコル階層が確認されました。
また、Modbus-RTUがCANopen上に重ねられ、さらにその下にModbus/TCPが存在するという構造を持つ製品も確認されました。

以前、DragosはLOGIIC Project 12に関連する複数のTurduckenプロトコルについて調査を行いました。このプロジ

[45]Fieldbus - Wikipedia; [46]抜粋：LOGIIC Project 12 安全計装レポート – Global Cybersecurity Alliance

ェクトでは、HARTプロトコルが、独自プロトコルや一般的な産業用プロトコルの上に重ねて使用されている例が多く確認されました。[46]
また別の取り組みとして、DragosはOmron製デバイスを調査し、EtherCATがNXBusという独自プロトコル上に構成され、さらにそれがHTTPリクエスト内に格納されているというプロトコル構造を明らかにしました。[47]

Dragosは、ほとんどのフィールドバス機器を「設計上、安全でない（insecure-by-design）」と見なしています。
これは、下位層のプロトコルによって引き起こされる設計上の問題が、必ずしもCVE（共通脆弱性識別子）として登録されるべきものではないということを意味します。
それでも、このような機器に対して攻撃や誤操作が行われたかどうかを検出できるようにすることは重要です。

これらのプロトコルは、Modbus-RTU／CANopen／X（XにはCIP、CODESYS、Modbus/TCPなどが該当）に見られるように、しばしば組み合わせ可能（コンポーザブル）です。
そして、このようなコンポーザブルなプロトコルの各レイヤーにはそれぞれ特有の特徴があり、たとえば以下のような特徴が見られます：

- 可変長のフィールド
- リクエストのパイプライン化
- 未公開（非公式）の機能

これらの要素が存在することで、ネットワークベースの分析や監視ロジックを作成することが非常に困難になります。

低層レベルの機器に対する攻撃を識別する取り組みが進む中で、エンジニアリング上の対応として期待されるのは、「コンポーザブル・ディセクター（分解解析器）」です。
これは、内包されたペイロードを抽出し、それを適切なディセクター（プロトコル解析器）に順次渡していくことで、すべてのレイヤーを段階的に解析できる仕組みです。
つまり、Turducken（多層構造プロトコル）の内部を、最後の層まで解析することを目的としています。
Dragosが運用するNeighborhood Keeperのデータセットを確認したところ、Turduckenプロトコルをサポートする複数のPLCモデルが特定されました。
Neighborhood Keeperとは、ユーザー参加型のコレクティブディフェンス（集団防御）および業界横断的な可視化ソリューションであり、脅威インテリジェンスを産業・地域を超えて共有することで、より的確な産業防御を可能にするものです。
Turduckenプロトコルをサポートしているモデルの例は以下の通りです：

- Rockwell Automation ControlLogix システム：HART対応のI/Oモジュールを備え、LOGIIC Project 12で示されたような計装機器への直接アクセスや攻撃が可能。
- Schneider Electric製コントローラー（CODESYSランタイムおよびCANopen対応）：CANopenデバイスへの直接SDOアクセスを提供し、プロセス制御ロジックとは別経路での再設定や遠隔操作が可能。

幸いなことに、これらのリスクに対するエンドユーザーのセキュリティ対策は、制御システムのロジック自体で実装可能です。[48] たとえば、コントローラーのロジックで機微な設定値を常時監視し、それらが"プロセス外（out-of-band）"で変更された際には、安全停止を自動で実行するといった方法が有効です。

フィールドバス機器を保護するためには、ICSコミュニティの意識改革が必要です。
一般的に、フィールドデバイス、特に計装機器やアクチュエータは「設計上安全でない（insecure-by-design）」という認識が広く共有されています。
しかし、機器の「アクセス可能性」については、所有者側で十分に考慮されていないケースが多いのが実情です。
たとえば、Ethernetネットワーク経由でフィールドバス機器を管理するためにDTM（デバイスタイプマネージャー）を使用している場合、アクセスに使用される基盤プロトコルが安全でない可能性があります。
このようなプロトコルは、ネスト構造になっていたり、一見すると複雑または意味不明に見えるかもしれませんが、
その見かけ上の複雑さは、研究者や脅威グループによって解析され、突破される可能性があるのです。

たとえDTM（デバイスタイプマネージャー）を使用してフィールドバス機器を管理していない場合でも、機器が外部にさらされている可能性はあります。
そのため、フィールドバス通信機能を持つPLCのエンジニアリングポートや、フィールドバスカプラ、プロトコルトランスレータへのアクセスは必ず制限すべきです。
これらの機器は、フィールドバスプロトコルをModbus/TCP、Ethernet/IP、DNP3など、より一般的なプロセスバスプロトコルへ変換する役割を持つことがあります。
重要なのは、「自分がその機器をどのように使用・管理しているか」だけでなく、
「自分以外の誰かによってどのように使用・管理され得るか」

[47]Omron製NEX PLCのランタイムおよびプロトコルの悪用 – S4, Logan Carpenter [48]安全計装のテスト：プロセス攻撃の検知と阻止 - Dragos [49]Miraiボットネットの亜種、Four-Faith製ルーターの脆弱性を悪用しDDoS攻撃を実行 – The Hacker News

という視点でもリスクを検討することです。

ICS環境におけるIoT機器

2024年11月時点でも、複数のIoT機器の脆弱性が悪用され、Miraiボットネットの拡散に利用されていました。このボットネットは、15,000以上のIPアドレスを維持し、DDoS攻撃を実行するために使用されています。[49] この長期間活動しているボットネットは、IoTおよびOT機器に対して完全自動で感染を行い、悪意のあるプロセスを隠蔽し、脆弱な機器をスキャンし、自己拡散・自己更新を行う機能を備えています。
このボットネットが成功している主な理由は、多くのIoT機器が、十分にハードニングされていないオープンソースのGNU/Linuxを内部で稼働させていることにあります。

多くのIoT機器には、デフォルトで有効化されたTELNETやSSH、認証不要のコマンドインジェクションなど、容易に悪用可能な脆弱性が剥き出しになっています。これら「ロー・ハンギング・フルーツ（低木の果実＝簡単に狙える目標）」型の脆弱性によって、デバイスファームウェアの改ざんに繋がる低レベルのアクセスを許す可能性があります。
また、これらの機器は共通のOSやCPUアーキテクチャを使用しているため、既存の攻撃ツールに対して脆弱でもあります。そのため、HVAC（空調）、照明、物理アクセス制御、物理的セキュリティシステムなどのビル管理システムは、攻撃者にとって格好の標的となり得ます。
これらのシステムは直接的に生産を維持しているわけではないかもしれませんが、いずれか1つが停止するだけで、生産が止まってしまう可能性があります。たとえば、照明制御システムがダウンすれば、作業員が業務を継続できなくなるかもしれません。また、製薬や食品製造のように規制が厳しい業界では、HVACや温湿度制御システムの停止により、生産停止を余儀なくされることもあります。
したがって、産業現場に導入されているIoT機器は「工場におけるプロセスの一部」として捉えるべきです。

2023年、Dragosは「IoT Exploit」と呼ばれるツールを分析しました。これは、「IoT機器の脆弱性スキャン、検証、エクスプロイト（攻撃）を行うツールキット」であり、IPカメラ、NVR、DVR、ルーター、産業機器を対象とした1,000件以上の公開エクスプロイトを含んでいます。
このツールは、RTSP（リアルタイムストリーミングプロトコル）のストリームキャプチャ、複数のプロトコルを使った認証ブルートフォース、DoS攻撃の実行などの機能を備えています。
IoT Exploitは、OTデバイスを標的とした約175件のエクスプロイトを含み、さまざまな産業用プロトコルに対応して通信できるほか、一般的なIoT機器向けのエクスプロイトも数百件含まれています。
このツールキットは一見すると、脆弱性スキャンを目的としたレッドチーミング（擬似攻撃）用ツールとして開発されたように見えますが、その存在が公開されている以上、将来的には自動化された攻撃ツールに組み込まれる可能性が高いと考えられます。
Dragosのテレメトリデータ上では、IoT Exploitツールが悪用された証拠は確認されていません。ただし、研究や防御目的で作成された「デュアルユースツール（Dual-use tools）」が、攻撃者の間で広く悪用されていることから、IoT Exploitもしくはその一部が将来的に悪用される可能性は高いと考えられます。

IoTシステムを保護する最も効果的な方法は、非常にシンプルです：
デフォルトパスワードを特定し、必ず変更すること。
これは、インターネットに公開されているシステムでは特に重要です。[50]加えて、機器の管理インターフェースへのアクセスを制限し、これらのデバイスが悪用されていないかを継続的に監視することも重要です。
そして何よりも大切なのは、これらのシステムが正常に動作しなくなった場合に備えて、事前に対処計画を立てておくことです。たとえば、磁気式ドアロックを手動で解除できる手段を確保しておくことは、すべてのプラントにおける安全対策計画の一部として含めるべきです。

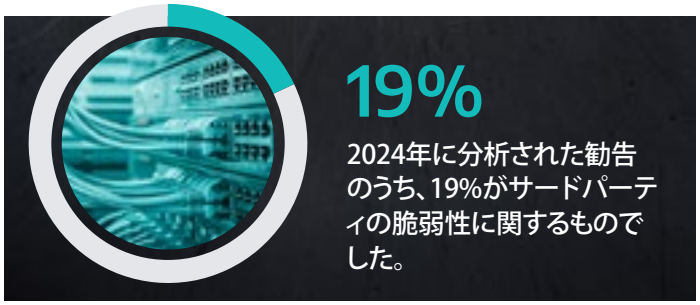
.

[50]中小企業向けOTサイバーセキュリティのベストプラクティス：デフォルトパスワード管理とインターネットに晒されたOT/ICS機器の特定

サプライチェーンとサードパーティ製コンポーネント：見えにくいリスクの認識

サードパーティ製コンポーネントは、OT機器やシステムの機能の拡張や支援する役割を担っています。しかし、これらのコンポーネントはエンドユーザーにとって認知されていないことが多く、その中に脆弱性が存在すると、当該コンポーネントのセキュリティだけでなく、それを組み込んだ製品全体の安全性を損なう可能性があります。
幸いにも、こうしたリスクは、脆弱性管理、ソフトウェア部品表（SBOM）の導入、その他の積極的な戦略によって軽減することが可能です。

サードパーティコンポーネントとは、基盤となるコアソフトウェアの開発元とは異なる外部の組織が作成したソフトウェアまたはハードウェアモジュールのことを指します。これらのサードパーティコンポーネントは、多くの場合、異なるベンダーの製品を統合し、機能を追加することを目的として、企業、個人開発者、あるいは研究機関によって設計されています。
たとえば、産業機器のOEM（相手先ブランド製造業者）は、他社製のソフトウェアモジュールを自社のアプリケーションや機器に組み込むことで、機能を追加したり、他システムとの統合を容易にしたり、互換性を高めたりしています。



2024年に分析されたアドバイザリのうち、19%がサードパーティ製の脆弱性に関連していました。

製品はサードパーティコンポーネントに依存していることが多く、これらのコンポーネントに脆弱性が存在すると、それに依存する製品のセキュリティや機能性にも直接的な影響を及ぼす可能性があります。
たとえば、PLCのようなベンダー製品が、自社で管理している脆弱性に対して最新のセキュリティパッチを適用していたとしても、内部に含まれるサードパーティ製のアドオンコンポーネントに未修正の脆弱性があれば、その影響を受ける可能性があります。
このような場合、ベンダー側は一時的な緩和策（ミティゲーション）を講じてリスクを低減させることはできますが、問題の根本的な解決には、サードパーティの開発元が適切な修正を提供することが不可欠です。

2024年4月、Bianlianランサムウェアグループは、Palo Alto NetworksのPAN-OSに存在する脆弱性（CVE-2024-3400）を利用し、水・廃水処理、製造、鉱業などの複数地域にまたがる組織に対する攻撃を試みました。
注目すべきは、SiemensのRUGGEDCOM APE1808製品が、Palo Alto NetworksのPAN-OSをサードパーティコンポーネントとして統合している点です。そのため、PAN-OSにCVE-2024-3400の脆弱性が存在する限り、Siemens製品も同様の脆弱性に晒されていることになります。
現時点では、Siemens製品がCVE-2024-3400を起因とする標的型攻撃を受けた証拠は確認されていませんが、この事例は、サードパーティコンポーネントがもたらすリスクを浮き彫りにしています。
Siemens製品がPAN-OSに依存していることによって、攻撃者に新たな侵入経路を提供する可能性があり、結果として導入組織が侵害を受けるリスクにもつながります。

サードパーティリスクを管理するための実践的な対策

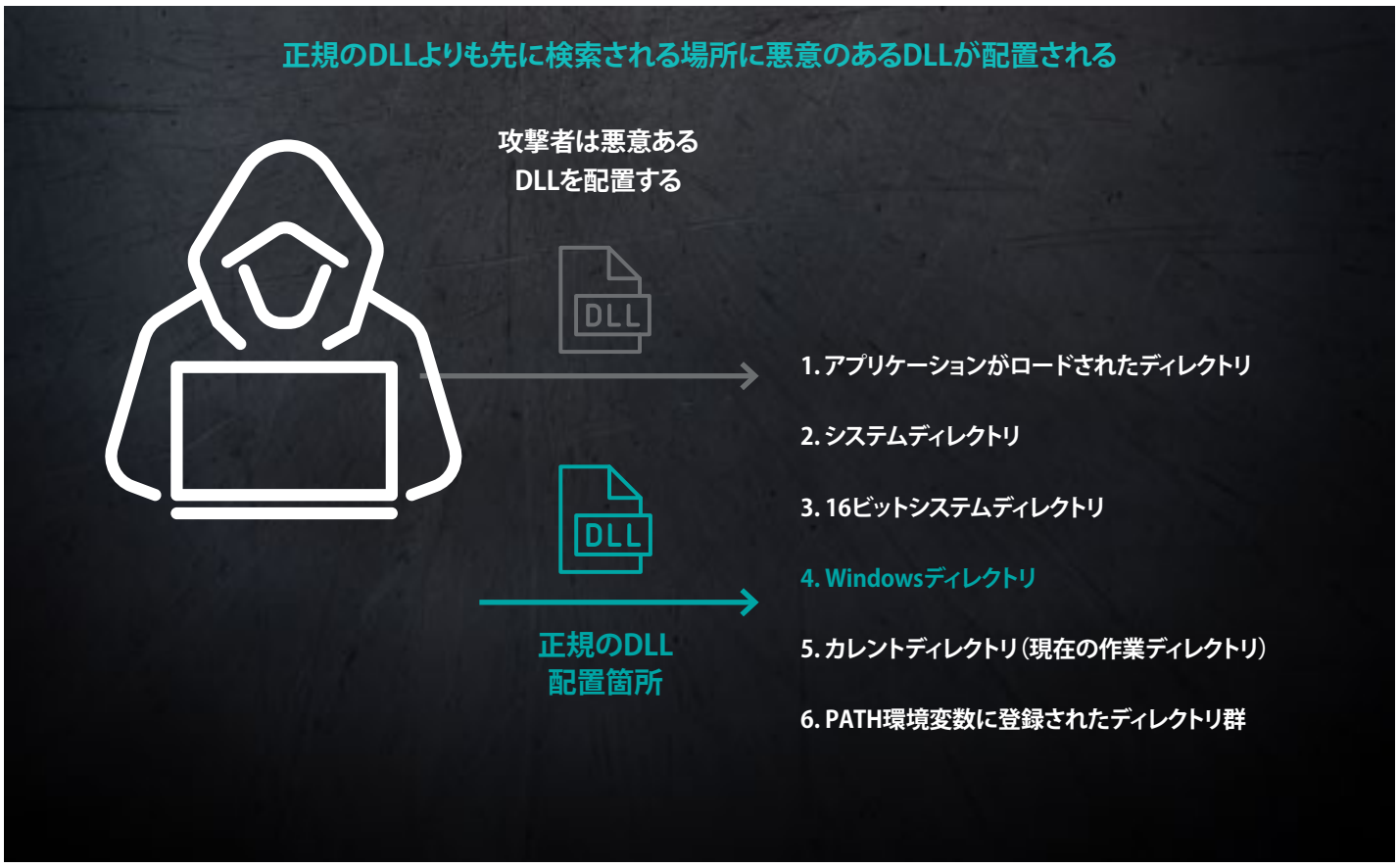
アセットの所有者や運用者は、自身の環境において最も重大な脆弱性を特定し、それに対処することを中心に脆弱性管理へ取り組むべきです。
このアプローチは、脆弱性が攻撃者に悪用される可能性を低減し、重要な運用の保護やシステムの安定稼働に貢献します。つまり、攻撃者に先んじてリスクを処理することで、安全性を維持できるのです。
このプロセスは、リスクベースの脆弱性管理と優先順位付けに対応した Dragos Platform を活用することで、より簡素化できます。
さらに、SANS ICS「5つの重要管理策」フレームワークに従うことで、セキュアな構成や継続的な脆弱性監視といった重要な対策を含む、構造的かつ効果的なリスク管理手法を実現できます。[51]

ベンダーにとって、SBOM（ソフトウェア部品表）の導入は不可欠です。[52] このドキュメントには、製品内に含まれるすべてのソフトウェアバージョンやアドオンコンポーネントが記載されるべきです。
SBOMによって製品構成の可視性が確保されることで、重大な脆弱性への対応がより迅速かつ効率的に行えるようになります。
このような透明性は、運用のレジリエンス（回復力）を高め、サードパーティ統合に特有のリスクに対する能動的なリスク管理を支援します。

DLLハイジャック：OTにおける継続的な課題

Dragosは現在、産業用ソフトウェアに影響を与える104件のDLL（ダイナミックリンクライブラリ）ハイジャックの脆弱性を追跡しています。
Dragosの脆弱性研究者は、これらの脆弱性を「ロー・ハンギング・フルーツ（低木の果実＝簡単に発見・悪用できる標的）」と見なしており、通常、発見も悪用も容易であるとしています。こうしたエクスプロイト（攻撃手法）は非常に汎用性が高く、攻撃者にとっては、初期アクセスの獲得、権限昇格、検知回避、あるいはWindowsホストシステム上への侵害の永続化の確立といった目的で利用可能です。[53]

DLLハイジャックとは、Microsoft Windowsオペレーティングシステムにおける DLLの検索順序アルゴリズムを悪用し、攻撃者が作成した不正なコード（DLL）を読み込ませるタイプの脆弱性です。



[51]The Five ICS Cybersecurity Critical Controls – SANS; [52]SBOM - CISA; [53]DLLハイジャックに対抗するための推奨対策 - Dragos Inc.

歴史的に、DLLハイジャックは産業組織に対して何度も悪用されてきました。

June 2010
StuxnetはCVE-2012-3015を悪用して、Siemens SIMATIC管理ソフトウェアを騙し、悪意あるDLL（S7hkimdbl.dll）を実行させました。
このDLLはStuxnetのペイロードを復号して管理者権限で読み込みました。[54] Stuxnetは、イランのウラン濃縮開発を遅らせるために展開されたとされています。

April 2017
APT10は「Cloud Hopper作戦」で、資格情報窃取ツールを配布するためにDLLハイジャックを利用しました。標的は製造業、エネルギー、鉱業など複数の産業分野に及びました。[55]

February 2022
MuddyWaterは、POWGOOPマルウェアにおいてDLLサイドローディングを活用しました。これはリモートアクセス型トロイの木馬（RAT）であり、政府機関、石油・ガス業界、通信分野などを標的としていました。[56] リモートアクセス型トロイの木馬（RAT）は、攻撃者に対して標的コンピュータの管理者権限の取得や遠隔操作を可能にしますが、公開されている報告によると、この活動の主な目的はスパイ行為であったとされています。

August 2022
Cotx/CotSam/DNSepマルウェアは、東欧およびアフガニスタンの軍事産業組織を標的とし、セキュリティソフトのDLLハイジャックによってバックドアを設置しました。[57] 任意コマンドの実行や情報収集が可能で、スパイ目的の活動と分析されています。

July 2023
MeatballとFourteenHiマルウェアファミリーが、東欧の産業組織やロシア政府機関を標的にDLLハイジャックを用いてリモートアクセス型トロイの木馬をインストールしました。[58]

Sept 2023
MuddyWaterはDLLハイジャックを使って権限昇格を行い、イスラエルの航空会社と空港を標的に攻撃を行いました。[59]

Sept 2023
HEADLACEマルウェアファミリーの亜種であるGRAPHITEによるバッチ型バックドアがDLLサイドローディングを含んでおり、ウクライナの重要インフラ組織に対して使用されました。[60]

July 2024
APT41は、DUSTTRAPマルウェアを実行するためにDLLハイジャックを使用。
標的は自動車業界および物流・海運関連組織でした。[61]

Dragosは、ICSアセットオーナーに対して、自身のシステム内でDLLハイジャックの脆弱性を積極的に調査し、以下のような対策を講じることを推奨しています：

- アプリケーションごとに CWDIllegalInDllSearch レジストリキーを有効化すること。
- アプリケーションの実行時には、「最小権限の原則（Least Privilege）」を遵守すること。
- アプリケーションディレクトリを監査し、「Everyone」や「Standard Users」グループに書き込み権限が付与されていないことを確認すること。

また、OTベンダーに対しては、DLLハイジャック脆弱性の発生を防ぐため、Microsoftの「Dynamic-Link Library Security」ウェブページを参照し、
自社のソフトウェアにおいて安全なプログラミング慣行を採用することを推奨しています。

[54]Stuxnet 0.5: The Missing Link – Symantec (via gwu.edu); [55]Operation Cloud Hopper - PwC, BAE; [56]MAR-10369127, MuddyWater – CISA; [57]産業組織および公共機関を狙った標的型攻撃 –Kaspersky [58]産業組織に対する攻撃の一般的なTTPs（戦術・技術・手順） – Kaspersky [59]イラン国家支援型APTグループ「ブラックボックス」流出 - ClearSky [60]APT28 Cyber attack – CERT-UA; [61]APT41 Has Arisen From the DUST – Mandiant

“Now, Next, Never”脆弱性対応フレームワーク

CVSS（共通脆弱性評価システム）は、ICSにおける脆弱性の優先順位付けには不十分です。[62] CVSSは、技術的属性に基づいて脆弱性を数値で評価するシステムですが、もともと産業システム（ICS）を想定して設計されたものではありません。

そのため、ICS特有のリスク評価に必要な文脈情報が欠けており、たとえば以下のような重要な要素を考慮していません：

• その脆弱性が実際の制御プロセスに影響するかどうか
• 脆弱性に対処することで、その機器が運用不能になるリスクがあるかどうか

こうした課題に対処するために、Dragosは脆弱性を3つのカテゴリに分類する「Now, Next, Never」フレームワークを開発しました。

このフレームワークは、アセットオーナーが自社の運用プロセスにとって最もリスクが高い脆弱性を識別・優先的に対処するのに役立ちます。

Dragosは、新たに出現する脅威、その手法、悪用される脆弱性を継続的に監視しており、

「Now, Next, Never」モデルは、それらの脆弱性がもたらす真の影響を正確に把握するための手段となります。

このモデルにより、組織は新たな脅威に対して的確に対応するためのガイダンスを得ることができます。

本フレームワークで評価される主な脆弱性属性：

- 運用への影響
- 実際の悪用事例や公開されたPoC（概念実証）の有無
- ネットワーク経由での悪用可能性
- 設計上安全でない機能の有無および緩和策の可用性
- 認証やユーザー操作が必要かどうか
- ICSネットワーク全体へのアクセス可能性

Now 特徴

- リモートから悪用可能
- 認証が不要、または認証が簡単に回避される
- ICSプロセスに影響する、またはICSへのアクセスを許す
- 実際にアドバイザリや攻撃者によって悪用されている、またはPOCが公開されている

「Now」の脆弱性には、パッチまたは代替的な緩和策（例：脆弱なポートへのアクセス制限、適切な設計プロセス）があります。**「Now」はICSにおける脆弱性の6%を占めます。**

Next 特徴

- リモートから悪用可能
- 攻撃者に現時点で狙われていない
- 運用に影響を与える可能性あり
- 資格情報の窃取など、攻撃準備が必要

「Next」の脆弱性は、主にネットワーク・ハイジーン（network hygiene）や、ICS 5 Critical Controlsのひとつであるセグメンテーションなどの対策によって緩和されます。**「Next」はICSにおける脆弱性の63%を占めます。**

Never 特徴

- 攻撃の実行が困難
- ICSに本質的に存在する設計上の問題と同じリスク)
- 修正に値するほどの効果がない

補足：「Never」の脆弱性は、ICSにおける脆弱性の31%を占めますが、修正するほどの価値はないと判断されます。

[62]共通脆弱性評価システム(CVSS)SIG – FIRST

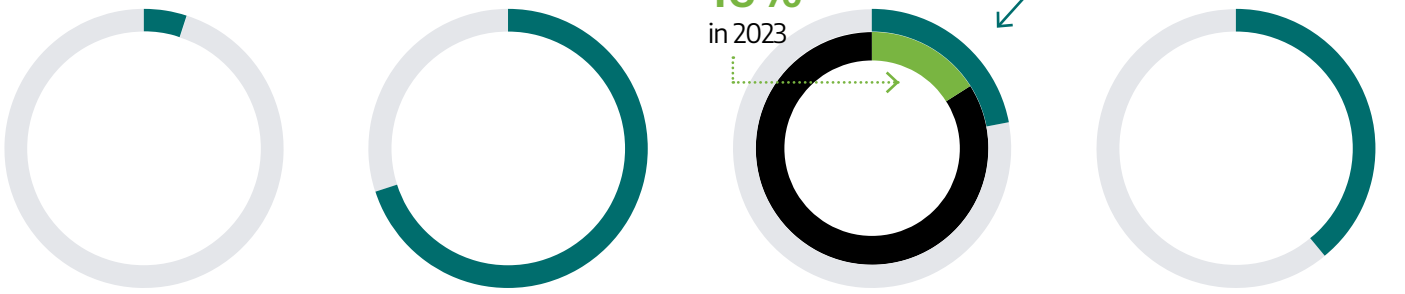
脆弱性トレンド

産業環境では規制遵守や安全・生産の継続が求められるため、IT環境と同じタイムフレームで脆弱性を緩和することはできません。ITでは、脆弱性対応のためのアップデートを柔軟に適用できますが、OTでは日々の運用を中断せずに維持することが重視されるため、脆弱性管理はより複雑で戦略的な計画が必要となります。
Dragosは、OT環境に特有の課題を前提にした脆弱性管理に注力しており、運用の継続性を損なうことなく、重要システムを保護し、リスクを緩和することを目指しています。
Dragosは、悪用された場合に産業プロセスへ深刻な影響を及ぼす脆弱性を優先的に扱っています。

Dragosの脆弱性評価における主な検討項目：

- その脆弱性は現在、実際に悪用されているか？
- その脆弱性はOT／ICSネットワークへの直接アクセスを可能にするか？
- その脆弱性が「視界の喪失（loss of view）」または「制御の喪失（loss of control）」を引き起こす可能性があるか？

私たちの調査が示すように、CVSSスコアだけでは運用環境におけるリスクを正確に反映できないことがよくあります。Dragosは、真の深刻度や緩和策、スコアや正確性の修正、そして防御側にとって有用な文脈情報を提供するために深い分析を行っています。2024年、Dragosは以下のことを明らかにしました：



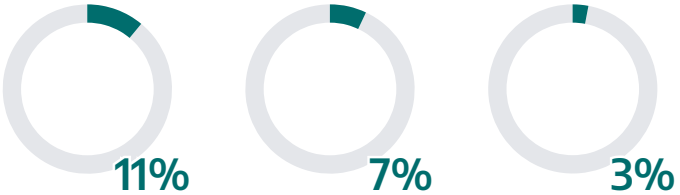
4.5%
の脆弱性に概念実証コード（POC）が存在し、実際に悪用されている。

70%
の脆弱性は、ICSネットワークの深部に存在。これらの脆弱性に関連する機器がPurdueモデルのレベル3.5以下、すなわち、よりプロセスに近い階層に位置していたことを意味する。

22%
の脆弱性はネットワーク経由で悪用可能、且つ、外部（ペリメータ）に面していた。

39%
の脆弱性は「監視の喪失（Loss of View）」と「制御の喪失（Loss of Control）」の両方を引き起こす可能性があった。

2024年、アドバイザリの22%に誤ったデータが含まれ、正確な優先順位付け・パッチ管理・緩和の妨げになった可能性がある



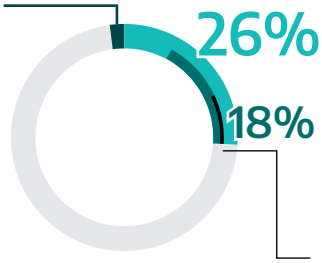
11%
のCVEにエラーが含まれ、的確な優先順位付けが困難

7%
の公開アドバイザリは報告内容以上に深刻度が高い

3%
は逆に報告内容よりも深刻度が低い

一部のアドバイザリは、アセットオーナーに対し解決策なしで問題を提示している

代替緩和策を提供しているアドバイザリは僅か2%だった。

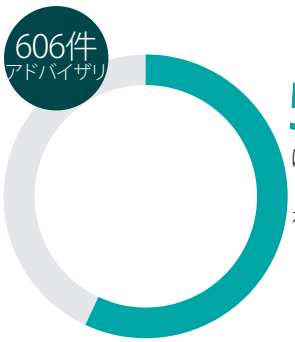


26% の公開アドバイザリがパッチを提供していない

18% の公開アドバイザリは、パッチも緩和策もなかった

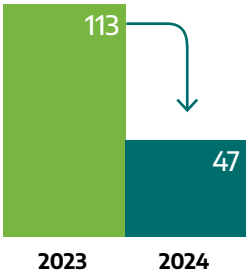
47%
パッチと緩和策を持たないアドバイザリの47%に対し、Dragosは代替緩和策を提供

2024年にDragosが評価した606件の公開アドバイザリについて：



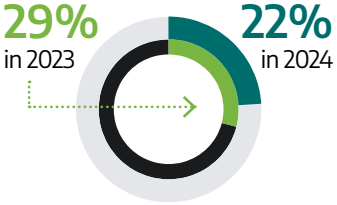
57%
はパッチが存在したものの緩和策がなく、これは2023年から3ポイント増加

ICSプロトコルに関するネットワーク経由で悪用可能な脆弱性のうち、代替緩和策を提示しているアドバイザリーは、2023年の113件から2024年には47件と半分以下に減少。



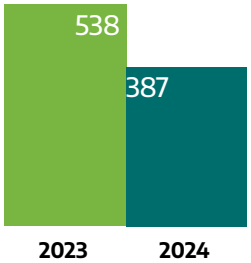
全体として、2023年から2024年にかけて評価対象となったCVEに見られる誤りの数は顕著に減少

CVEエラー



CVEエラーは、2023年の29%から2024年には22%へと減少。脆弱性公開時のベンダーや研究者によるスコアリングがより正確になったことを示している。

概念実証（PoC）付きのCVE



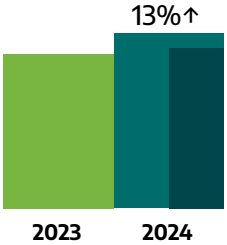
Dragosの研究者は概念実証コード（PoC）が存在するCVE総数が大幅に減少したことを観測した。2023年は538件のCVEにPoCがあったが、2024年は387件に留まった。

更なる調査の結果...

151件のCVEは、より高いスコアとなった

55件のCVEは、より低いスコアとなった

実際に悪用された脆弱性アドバイザリのCVEエラー



110件中101件はPOCを含む

エクスプロイト分析から、2024年には、CVEが付与された脆弱性のうち18%が実際に悪用された。

実施すべき対策

産業オペレーションは今や、国家支援型の脅威グループ、サイバー犯罪者、そしてハクティビストたちの明確な標的となっており、彼らはスパイ活動、業務妨害、破壊を目的に、ICSの脆弱性を悪用しようとしています。

『2025年版OT/ICSサイバーセキュリティレポート』は、ある事実を明確に示しています。それは、「攻撃者の進化は防御側よりも早い」ということです。

攻撃者はOTネットワークを試すだけでなく、実際に重要インフラ内部に入り込み、長期的なアクセス、業務の妨害、そして大規模な影響を狙って拠点を築いています。Living-off-the-land（既存の正規ツールの悪用）手法やICSマルウェア、標的型の偵察活動の使用は、これらの攻撃者が産業システムをこれまで以上に深く理解していることを証明しています。

もはや、受動的な防御戦略や時代遅れのセキュリティ体制では対応できません。「反応型（リアクティブ）セキュリティ」の時代は終わりを迎えました。これからの防御には、OT環境に特化した継続的な監視、プロアクティブな脅威ハンティング、そしてインシデント対応能力の強化が求められています。

SANS ICSの「5つの重要対策（ICS 5 Critical Controls）」のような基本的なセキュリティ実践は、地政学的な対立を背景にしたサイバー事案への備えとして、今なおOT/ICSのアセットオーナーにとって最も有効な手段です。

#1 インシデント対応計画：

OT向けのインシデント対応計画を見直しましょう―または、そもそも計画が存在するかを確認してください。攻撃者はますますOT／ICSへの理解を深めており、その戦術・技術・手順（TTP）は、産業環境の深部を標的とするようになっています。
たとえば、SCADAサーバーがランサムウェアにより暗号化された場合や、BAUXITEによりPLCロジックが改変された場合でも、対応・復旧が可能な計画を整備しておくことが重要です。

#2 防御可能なアーキテクチャ（Defensible Architecture）

自社の攻撃対象領域（アタックサーフェス）を完全に理解しましょう。毎年、アタックサーフェス分析を積極的に実施し、VPN、RDP、SSHなど、BAUXITEが標的にするネットワークゲートウェイやネットワークの境界を優先的に対応することが重要です。
簡単に分析を始める方法として、ShodanやCensysといったツールを活用し、インターネットに公開されている資産を外部から可視化することが有効です。
内部ネットワークに侵入された後を想定し、ファイアウォールルールの監査や、NP-Viewを用いた内部アタックサーフェスの検証を行い、VOLTZITEのような攻撃者によるラテラルムーブメント（水平展開）を防止しましょう。

#3 可視性と監視（Visibility and Monitoring）

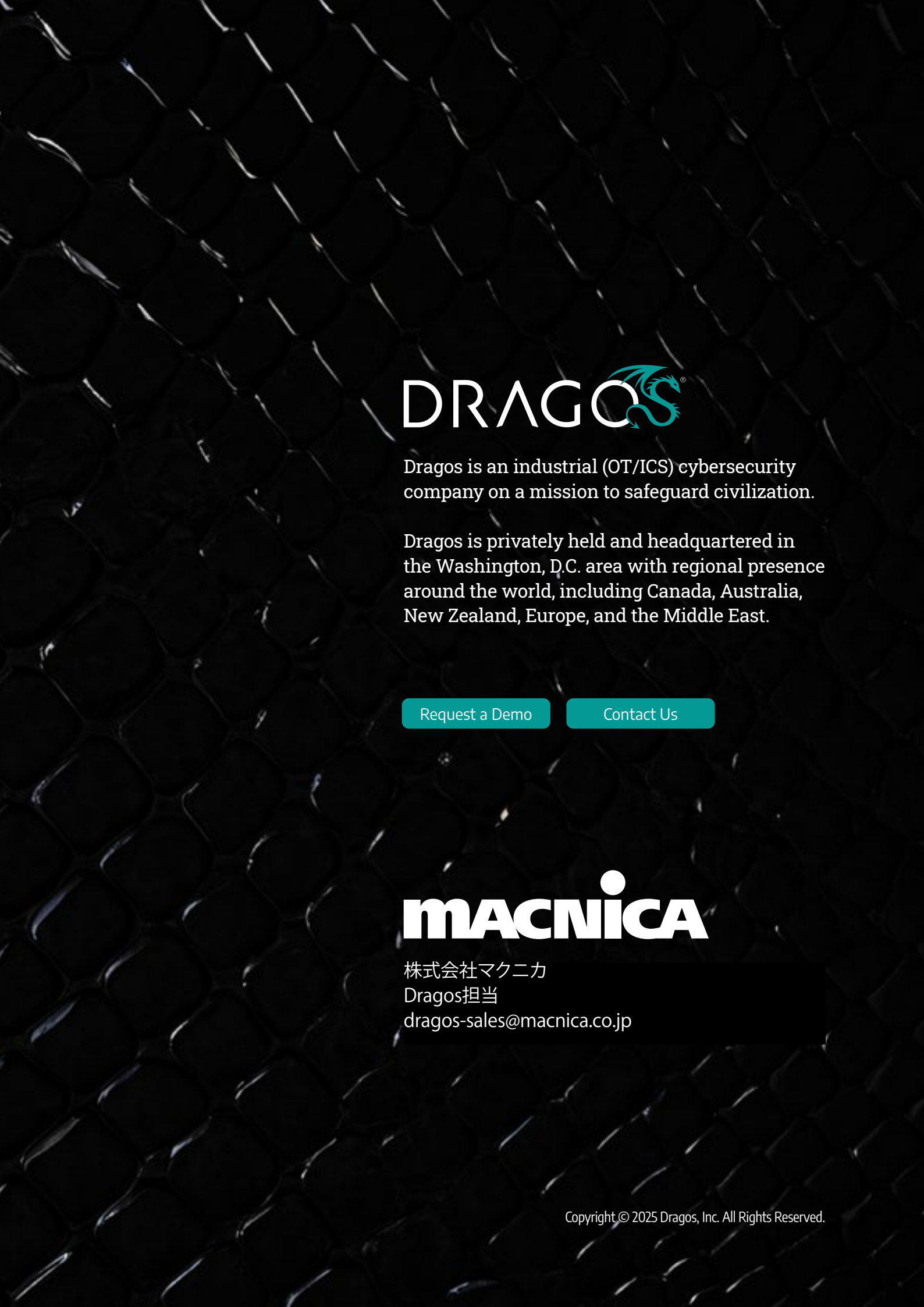
可視性と監視体制を強化しましょう。Dragos Platformのようなotに対応した監視ソリューションは、攻撃者が本格的に動き出す前に、その微細な動きを検知することが可能です。
Dragos Platformは、構成変更やコマンドコードの変更を検知する機能も備えており、セキュリティインシデントとエンジニアリングミスの切り分けにも役立ちます。

#4 安全なリモートアクセス（Secure Remote Access）

リモートアクセスに重点を置きましょう。Dragosのインシデント対応事例でも、ベンダーリモートアクセスは継続的に攻撃経路として利用されています。
臨時のアクセスポイントであっても、本社VPNやファイアウォールと同じレベルのセキュリティ審査を行い、
アクセスログの強化、アラート設定、多要素認証（MFA）の導入を徹底しましょう。

#5 リスクベースの脆弱性管理（Risk-Based Vulnerability Management）

脆弱性対策は、現実的な脅威に焦点を当て、戦略的に取り組みましょう。CVE（共通脆弱性識別子）の内容を精査し、記載情報が正確かどうかを確認したうえで、「制御の喪失」など、プロセスに直接影響を与える可能性のある脆弱性に優先的に対応してください。
そのうえで、たとえ数年かかる計画であっても、明確な対応方針を策定し、着実に実行していくことが重要です。



Dragos is an industrial (OT/ICS) cybersecurity company on a mission to safeguard civilization.

Dragos is privately held and headquartered in the Washington, D.C. area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Request a Demo

Contact Us

株式会社マクニカ
Dragos担当
dragos-sales@macnica.co.jp