制御システム・セキュリティの現在と展望

～ この1年間を振り返って ～

2026年版

JPCERTコーディネーションセンター
技術顧問
宮地利雄

全体概要

1. ICSセキュリティ状況の展望
2. ICSインシデントの動向
3. ランサムウェアの動向
4. ICSを狙って作られたマルウェアの動向
5. ICSコンポーネントの脆弱性の動向
6. 標準の整備と規制の強化
7. 米国CISAの混乱と課題

(本資料中の年の表記のない月日は2025年の日付を表しています)

ICSセキュリティ状況の展望

- Stuxnetの発見から15年,
  サイバー攻撃によるウクライナでの広域停電から10年が経過
- ICSとITシステムの連携がさらに高まる
- パワーゲームに傾きつつある国際情勢
- 実務的にはランサムウェア攻撃が最も憂慮すべきリスク
- OTセキュリティに対する新しい見方が形成されつつある

サイバーセキュリティ状況の展望

[参考] World Economic Forum: Global Cybersecurity Outlook 2026 (2026年1月12日)
https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

- AIがリスクを書き換えつつある： 攻撃側と防御側の双方を加速
- 地政学がサイバーセキュリティの様相を再定義
- 変化するサイバー犯罪の情勢：
  AIと詐欺とグローバルな対応
- 経済価値を守るサイバー・レジリエンスへの不安
- リスクの集中と不透明化の中でのサプライチェーンのセキュア化
- サイバーにおける不平等を2026年に後押しするもの(組織規模，地域)
- そっと現れる未来の脅威ベクトル(自律システム，ロボット，量子技術)

SANS報告書「ICS/OTセキュリティの現状 2025年」

State of ICS/OT Security 2025
https://www.sans.org/white-papers/state-of-ics-ot-security-2025

ICSセキュリティ専門家
330人へのアンケート調査

- 21.5%の組織が過去1年間にサイバーセキュリティ・インシデント
  - 4割のインシデントで操業の中断が発生
  - 2割のインシデントが完全復旧までに1ヶ月以上を要した
- 規制に伴う監査がセキュリティ対策の成熟度を押し上げている
- 報告されたインシデントの約半数が不正な外部アクセスから始まった
- セキュリティ投資の弾みが明確に見られるが
  - 新たな脅威への備えに対する充足感は14%にとどまる

☞ インシデント報告の半数前後がランサムウェア攻撃
☞ 戦争など地政学的な緊張下のサイバー攻撃が常態化
(ロシア⇒欧州，イラン⇔イスラエル，中国⇒台湾や米国)

ICSインシデントの動向

産業組織に対するサイバー攻撃の動向

Kaspersky社ICS CERTの報告書によれば…

- 四半期ごとに約118～135件のインシデント報告
- 大多数がランサムウェア攻撃によるもの
- 攻撃を受けた組織の約半数が製造業
- 攻撃を受けた組織の約4割で操業または製品出荷が停止した；
  その多くが製造業だった； 個人情報の流出を伴うことも
- 主なインシデント
  - クアラルンプール空港(3月下旬) ：約10時間搭乗手続きなどできず
  - Jaguar Land Rover社(9月)： 5週間製造が停止

[参考] 産業組織に対するサイバー攻撃の動向

Kaspersky社ICS CERTのA brief overview of the main incidents in industrial cybersecurity.

- Q4 2024 (3月25日)
  https://ics-cert.kaspersky.com/publications/reports/2025/03/25/q4-2024-a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity/
- Q1 2025 (6月26日)
  https://ics-cert.kaspersky.com/publications/reports/2025/06/26/a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity-q1-2025/
- Q2 2025 (10月9日)
  https://ics-cert.kaspersky.com/publications/reports/2025/10/09/a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity-q2-2025/
- Q3 2025 (12月18日)
  https://ics-cert.kaspersky.com/publications/reports/2025/12/18/a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity-q3-2025/

ICS/OTシステムに対するサイバー攻撃の動向

2025年上半期
脅威レビュー

ForeScout社の報告書(8月4日)によれば…
https://www.forescout.com/blog/midyear-threat-report-numbers-grow-in-nearly-all-the-wrong-places/
https://www.forescout.com/resources/2025h1-threat-review/

- OTへの攻撃が増加中 (ハニーポットによる観測)
  - ModbuS(57%)，EtherNet/IP(20%)，BACnet(8%)プロトコルが対象
- ランサムウェア： 89の攻撃集団
  - 攻撃件数が46%増加 (2025年上半期；前年同期比)
- 中国，ロシア，イランを中心に137の脅威集団が活動中
  - イランのAPT IranやCyberAv3ngersなどは
    OTを狙う協調的な攻撃を試みている
- 国家支援を受けた攻撃者とハクティビストの境界が消えつつある

活発化する中国によるサイバー攻撃活動

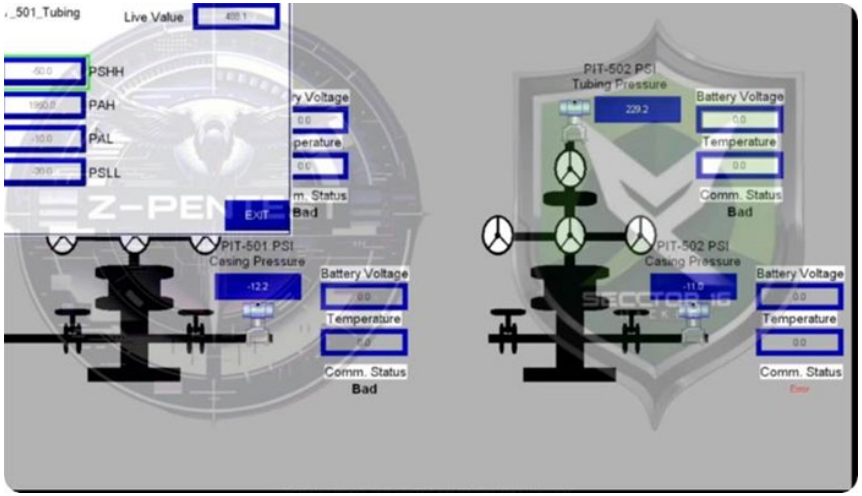
- CISAが国家支援を受けた中国の集団によるサイバー攻撃に注意喚起 (2024年2月7日)
  PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure
  https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
  — Volt Typhoonによる重要インフラなどへの侵害

- 米国の重要インフラへのサイバー攻撃の実施を中国側が2024年末の米中秘密会談で認めたとWall Street Journal紙が報道 (4月10日)
  In Secret Meeting, China Acknowledged Role in U.S. Infrastructure Hacks
  https://www.wsj.com/politics/national-security/in-secret-meeting-china-acknowledged-role-in-u-s-infrastructure-hacks-c5ab37cb

ロシアのハクティビスト集団の動き

[出典] Cyble社： https://cyble.com/blog/dark-web-activity-new-hacktivist-group-emerges/

- 15のハクティビスト集団が見つかった
- 約半数の集団がランサムウェア攻撃の実行を主張
- Sector-16と自称する集団は米国の石油ガス製造施設のICSへの不正アクセス



ICSへのアクセス画面を
Sector-16が公表
[出典] Cyble社

- CISAがアドバイザリー発行
  (12月18日)
  「親ロシア派のハクティビストが米国と重要インフラに日和見的攻撃」
  https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-343a

ノルウェイ南西部のダムのICSが侵害されて放水

https://hackread.com/norwegian-dam-valve-forced-open-hours-in-cyberattack/

- ノルウェイ南西部のSvelgen市近郊のLake RisevatnetダムでICS侵害(4月7日)
  - 遠隔操作インターフェースがインターネットに露出しており，認証子を奪取されたと見られる

- バルブが操作されて5時間にわたり最少流量を毎秒497l上回る放水が行われた
- 特段の被害も危険な状況の発生もなかった(下流の河床は毎秒2万lの放水に耐える強度)

- ロシアのハクティビストが攻撃関連の動画をTelegraphに投稿

ポーランドの水力発電所に2度のサイバー攻撃

https://united24media.com/latest-news/russian-hackers-breach-polish-hydropower-plant-in-major-cyberattack-10882

- ポーランドのGdańsk近郊のTczewにある水力発電所が5月と8月に2度にわたりサイバー攻撃を受けた
- 8月の攻撃では，タービンの運用が侵害され，発電所がオフラインに
- ロシアのハクティビストが攻撃を記録した動画を公表

- 地元紙によれば，複数の上水道処理プラントや下水処理プラント，水泳用プールのICSでも不正なパラメーター操作が報告されている

年末にポーランドの再生可能エネルギー網にサイバー攻撃

- ポーランド首相やエネルギー相が会見で表明 (12/13)
  https://milmag.pl/en/cyberattack-on-polands-renewable-energy-network/
  https://www.gov.pl/web/primeminister/poland-stops-cyberattacks-on-energy-infrastructure

  2025年12月29～30日に攻撃を受けた
  - 多数の再生可能エネルギー源に対して同時かつ協調的に攻撃
    給熱発電施設1ヶ所＋風力または太陽光発電施設(12ヶ所～約30)
  - 停電に至る前に攻撃を遮断

  合計容量： 1.2GW (ポーランド全国の0.5%)

- Eset社が分析結果を公表
  https://www.welivesecurity.com/en/eset-research/eset-research-sandworm-cyberattack-poland-power-grid-late-2025/

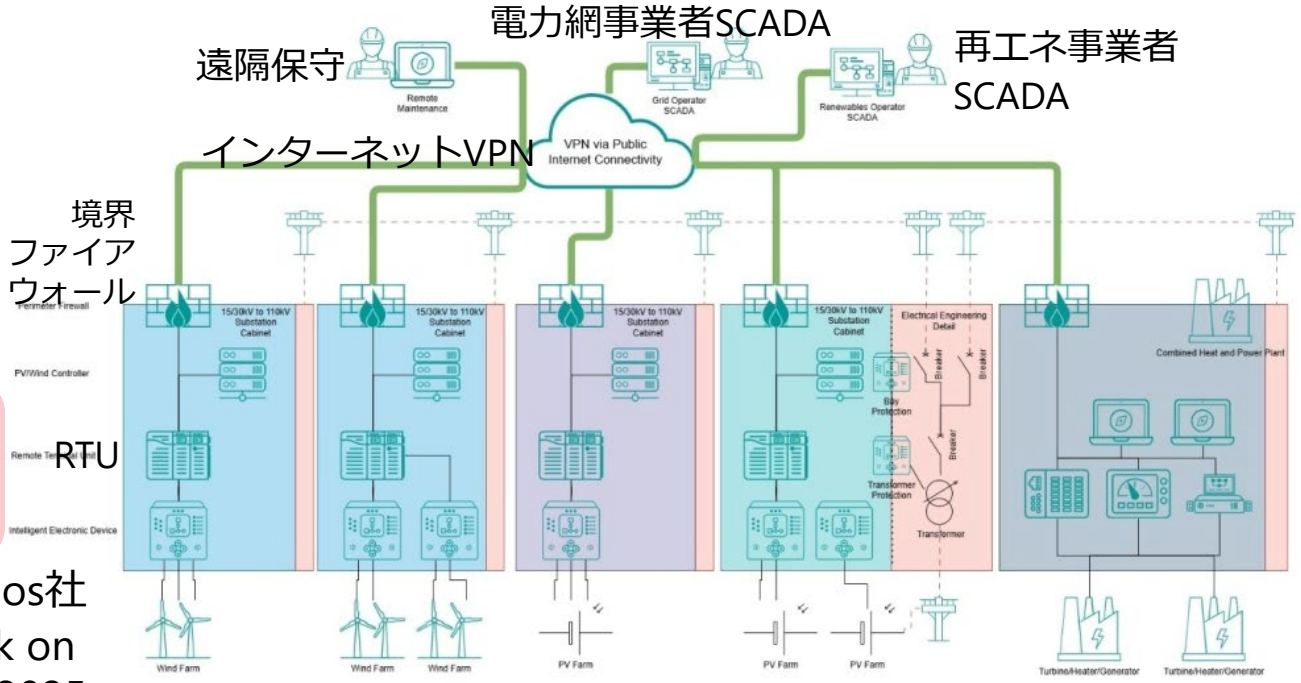
  - データ消去マルウェア(ワイパー)DynoWiperが使われた
    ロシア関連のAPT集団SandWormが使うワイパーとの類似性が高い

ポーランドの再生可能エネルギー網にサイバー攻撃 (つづき)

[インシデント対応に参加したDragos社から報告書](https://www.dragos.com/blog/poland-power-grid-attack-electrum-targets-distributed-energy-2025)
https://www.dragos.com/blog/poland-power-grid-attack-electrum-targets-distributed-energy-2025

- 分散電源施設で可視性や制御性を奪取され物理的に損壊された
- 1月にも再攻撃

10年前のウクライナ停電を引き起こした集団が異なったアプローチで攻撃



[出典] Dragos社
ELECTRUM: Cyber Attack on Poland's Electric System 2025

ポーランドの再生可能エネルギー網へのサイバー攻撃分析

CERT Polskaとデジタル省の報告書「エネルギー業界インシデント報告 – 12月29日」
https://cert.pl/uploads/docs/CERT_Polska_Energy_Sector_Incident_Report_2025.pdf

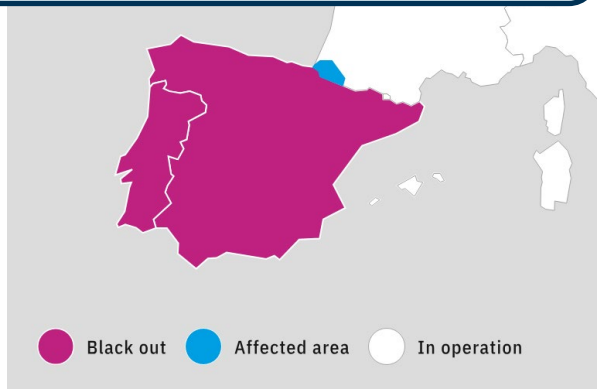
- FortiNet社製のネットワーク境界装置FortiGateが進入口
  — 5～9ヶ月間システム内で潜伏できるよう改変されていた
- 不正操作された日立製やMikronika社製のRTUなどの認証子がデフォールトのままで運用されていた
- 同時に製造業の企業に対する同様のサイバー攻撃があった
  — 攻撃先の選び方は日和見的で戦略性はないと見られる
- オンプレミスで獲得した情報をもとにクラウドを侵害する試み

[参考] イベリア半島(スペイン&ポルトガル)大停電

https://www.entsoe.eu/publications/blackout/28-april-2025-iberian-blackout/

- 2025年4月28日12:33(欧州中央時)にスペインの南西部から停電が始まりイベリア半島全域(フランスの一部を含む)の停電に至った
- 復電までに約半日を要した
- 最初の停電に先立って欧州全域で周波数と電圧の発振現象が生じていた
- 結論には至っていないが，再生可能エネルギー導入に伴う不安定性が原因と見られている

サイバー攻撃ではなかったが，同様の現象をサイバー攻撃で故意に引き起こされる可能性が懸念される



米国がベネズエラの大統領逮捕作戦でサイバー攻撃

Cyberattack in Venezuela Demonstrated Precision of U.S. Capabilities (New York Times)
https://www.nytimes.com/2026/01/15/us/politics/cyberattack-venezuela-military.html

- ベネズエラ大統領を逮捕する2026年1月3日の作戦でサイバー能力を使ったことをTrump大統領がほのめかす
- 匿名の米国当局の関係者がNew York Times紙にサイバー攻撃(Absolute Resolve作戦)が行われたと語った：
  - 米軍のヘリコプターが進入できるように，レーダー妨害と，カラカスの一部地域を停電させた
  - 一般市民の損害を最小化するために，逮捕に関連した地域を除き，数時間以内に復電させた

イランに対するサイバー攻撃

- イランの高官が同国のインフラを狙った広範囲かつ複雑なサイバー攻撃が4月27日になされ，これを撃退したと主張
  https://therecord.media/iran-cyberattack-national-infrastructure

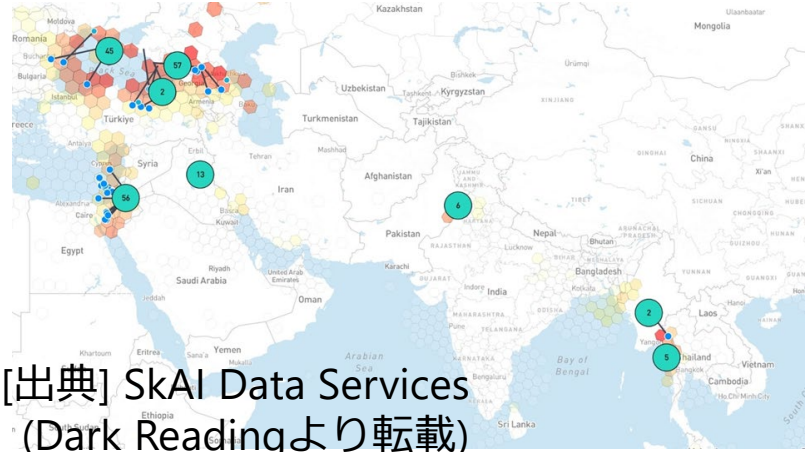
  - 攻撃の詳細情報は不明
  - イラン～米国の核開発計画をめぐる交渉が進行中
  - この攻撃の直前の最大の商業港Shahid Rajaei港での大規模爆発はサイバー攻撃によるものでないと見られている

- イランはPredatory Sparrowからのサイバー攻撃を繰り返し受けてきた
  - 2021年：燃料システム
  - 2022年6月： 製鉄所

偽のGPS信号が黒海と中東，東南アジアで急増

- 紅海をサウジアラビアのJeddah港に向けて航行中のコンテナ船が偽のGPS信号に関連したインシデントが原因で航路を逸脱し座礁
  https://www.worldcargonews.com/shipping-logistics/2025/05/msc-antonia-runs-aground-in-red-sea-amid-gps-spoofing-concerns/
  — イエメンのフーシ派の攻撃を避けて喜望峰をまわる欧州～アジア航路の船舶も多い

- 米国DHSがGNSS強化のための新ツールを公開
  https://www.dhs.gov/science-and-technology/news/2025/05/19/st-releases-new-tool-strengthen-global-navigation-satellite-systems



[出典] SkAI Data Services
(Dark Readingより転載)

- ☞ Silk Typhoon： 偵察活動とデータ収集
- ☞ Salt Typhoon： 電気通信事業者と政府を侵害
- ☞ Volt Typhoon： OTを狙う標的型(APT)攻撃集団

米国への最大の
サイバー脅威は
中国

中国政府の支援を受けているとされる サイバー攻撃活動

重要インフラに対する中国からの脅威

- 「1年間近くVolt Typoonが御社を侵害している」と米国の小規模電力事業者(配電地域の人口：1.5万人)にFBIが通知
  https://go.theregister.com/feed/www.theregister.com/2025/03/12/volt_tyhoon_experience_interview_with_gm/
  https://industrialcyber.co/utilities-energy-power-water-waste/dragos-details-lelwds-fight-against-voltzite-cyberattack-following-300-day-ot-network-breach/

- 中国の高官がVolt Typhoon攻撃の実施を秘密会談で認めたとの報道も
  https://www.securityweek.com/china-admitted-to-us-that-it-conducted-volt-typhoon-attacks-report/

- 関連するとされるAPT攻撃集団UAT-5918は台湾の重要インフラを攻撃
  https://industrialcyber.co/critical-infrastructure/uat-5918-apt-group-targets-taiwan-critical-infrastructure-possible-linkage-to-volt-typhoon/

英国の自動車メーカーJaguar Land Rover社へのサイバー攻撃

- 8月31日に攻撃が始まり，英国内2工場で9月1日から操業を完全に停止
- 10月22日になって徐々に操業を再開
- SNSのTelegram上に「Scattered Lapsus$ Hunters」と名乗る集団が9月3日に犯行声明 (JLR社側による確認はされていない)
- 同社のサプライヤーの株価が一時55%下がるなど英国経済に大きな打撃
- 同社のサプライチェーンと英国経済を守るために英国政府が15億ポンドの債務保証の提供を決定
- 第三者機関の試算によれば，5千社以上が影響を受け，英国経済全体に19億ポンド(約4千億円)の損害

3集団が合同(?)：
・Scattered Spider
・Lapsus$
・Shiny Hunters

https://cybermonitoringcentre.com/2025/10/22/cyber-monitoring-centre-statement-on-the-jaguar-land-rovercyber-incident-october-2025/

英国銀行は第3四半期GDP成長率を03.%⇒0.2%修正

Jaguar Land Rover社の被害

11月14日に同社が発表した7～9月の四半期予測
https://media.jaguarlandrover.com/news/2025/11/jlr-performance-impacted-challenging-quarter

- 売上高： 49億ポンド (7～9月期；24%減)
  115億ポンド(4～9月期；16%減)

親会社のTata Motors社(インド)も18億ポンドの損失を計上

- 税前損と例外項目： 4.85億ポンド(7～9月期)
  13.4億ポンド(4～9月期)
  (計画されていたJaguarの旧モデルの整理とサイバー攻撃による損失)
  それぞれ前年同期の益3.98億ポンド，11億ポンドから悪化

- 例外項目2.38億ポンドにはサイバー関連経費1.96億ポンドを含む

Jaguar Land Rover社へのサイバー攻撃： CyFirma社の分析

https://www.cyfirma.com/research/investigation-report-on-jaguar-land-rover-cyberattack/

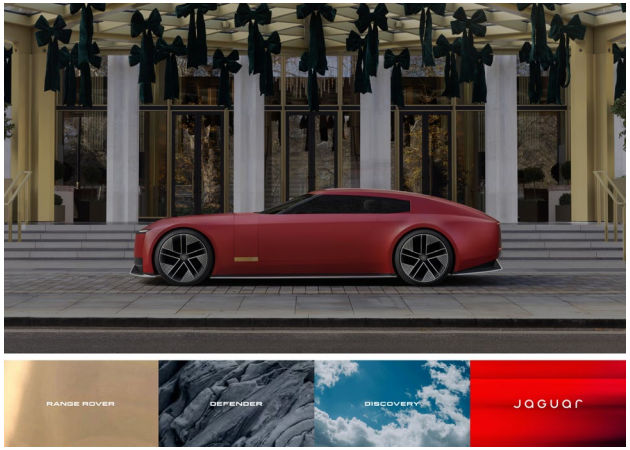
- 3月にランサムウェア集団HellCatが同社を侵害し，
  Reyと名乗るメンバーが約700件の内部文書(秘密文書，ソースコード，従業員データ)が流出
- Reyによる流出の数日後に
  別の攻撃者APTSが(新データを含む)350GBの同社データをさらに流出

- 8月31日にScattered Lapsus$ Hunters(母国語：英語)がサイバー攻撃
  - 狙いは，金銭ではなく，サイバー攻撃コミュニティ内における評価の向上を狙った戦略的なものにありそう
    - 身代金の要求も，窃取データの販売も確認されていない

[参考] Jaguar Land Rover (JLR) 社に関する基礎情報

https://en.wikipedia.org/wiki/Jaguar_Land_Rover

- インドのTata Motors社が所有する英国最大の自動車会社
- 高級車ブランドのJaguarとLand Roverを保有
- 売上高： 289.9ポンド(2024年)，従業員数：3.98万人(2020年)
- 車両組立工場： Halewood, Merseyside； Solihull, West Midlands； Pune, India；常熟(Changshu), 中国； Itatiaia, Brazil； Nitra, Slovakia



[出典] JLR社ホームページ

Halewood

Solihull

☞ 一部の攻撃集団に法執行機関が実施した国際的な粉砕作戦でランサムウェア攻撃コミュニティ内に地殻変動；小規模集団が数多く誕生
☞ 全体的には，身代金支払い総額が激減；攻撃件数は高止まり

ランサムウェアの動向

高止まりしているランサムウェア攻撃

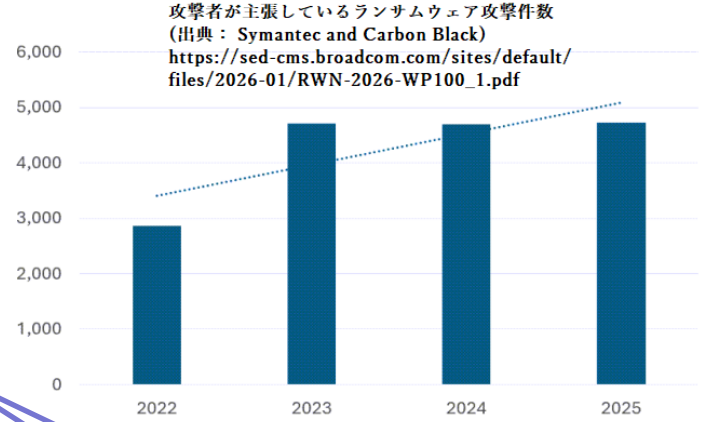
ITとOTの双方を含んだ集計値

[出典] CompariTech社の報告書(2026年1月13日)
https://www.comparitech.com/news/worldwide-ransomware-roundup-2025-end-of-year-report/

- 攻撃件数： 7,419件(攻撃者の主張)，1,204件(被害組織が確認)
  - うち製造業界の事業者が1,466件(攻撃者の主張)
- 身代金の平均金額： 104万ドル以上(要求額)
  - 製造業界だけの平均は120万ドル(要求額)
- 活動が活発だった攻撃集団：
  Qilin(1,034件)，Akira(765件)，Clop(454件)，Play(393件)，SafePay(374件)，INC(359件)，…
- 狙われた国：
  米国(3,810件)，カナダ(392件)，ドイツ(303件)，英国(251件)，フランス(178件)；韓国(64件)

変容するランサムウェア

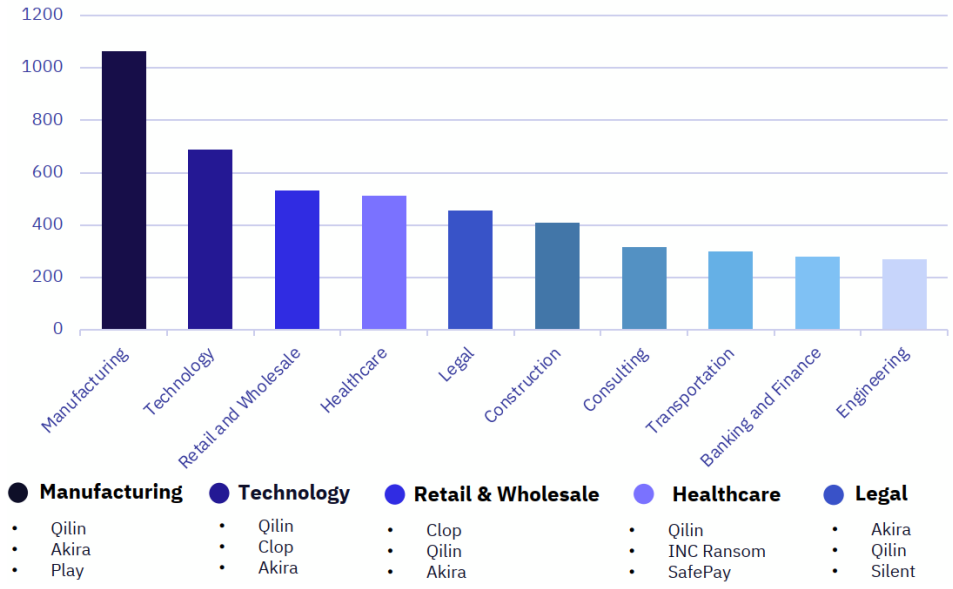
- 全体としては増加傾向が続く
- 第3四半期に身代金の支払い額が急減
  支払い率の減少傾向が続く
- 国際的な法執行機関によるランサムウェア攻撃基盤の粉砕作戦によりランサムエア･コミュニティに地殻変動
  - ランサムウェア族の交替；
    暗号化を伴わない脅迫も
  - アフィリエートの力が増し，攻撃先を多角化
    今後の動きの予想が難しくなっている



CoveWave社の報告
https://www.coveware.com/blog/2025/10/24/insider-threats-loom-while-ransom-payment-rates-plummet

変容するランサムウェア

- 2023年まで猛威をふるったLockBitが
  2024年初頭の法執行機関による粉砕作戦で解体された
  — アフィリエートがRasomHubさらにQilinに移動
- 2025年にはQilinが最も活発に
  活動するランサムウェア集団に
- 引き続いて製造業がもっとも
  狙われている業界



[出典] GuidePoint Security社
2026 Ransomware and Cyber
Threat Report

ランサムウェアに関連するその他の報告

- サイバー攻撃全体の44%がランサムウェア攻撃
  [出典] Verizon社2025 Data Breach Investigations Report (DBIR)

https://www.verizon.com/business/resources/ja/T48/reports/2025-dbir-data-breach-investigations-report.pdf

- ランサムウェア侵害があった組織の58%で業務が中断；
  復旧に平均17.5人で132時間を要した
  [出典] Illumito社

https://www.illumio.com/blog/global-cost-of-ransomware-study-what-the-numbers-tell-us

- ランサムウェア攻撃集団が2極化
  - 容易に攻撃できる中小組織を狙い攻撃件数を稼ぐ
  - 高額の身代金を獲得できそうな大手の組織を狙う

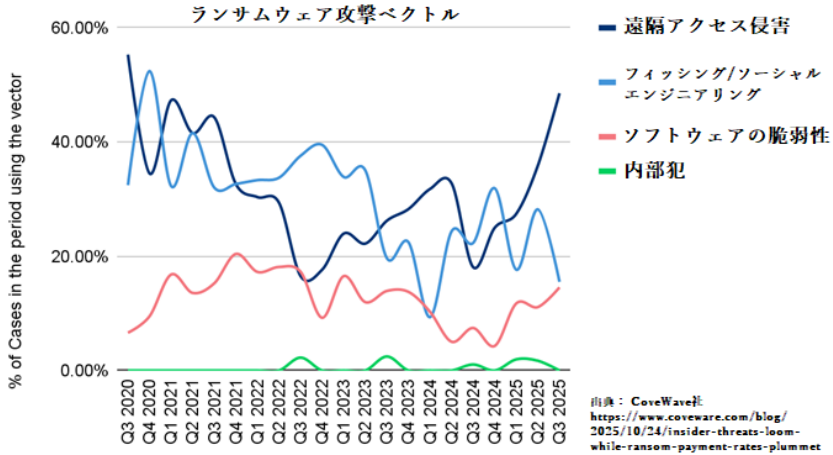
- クラウド上のIT/OTシステムを狙う
  https://www.huntress.com/blog/hypervisor-defenses-against-ransomware-targeting-esxi

ランサムウェアに関連するその他の報告

- 週末と休暇に集中しているランサムウェア攻撃
  Semperis社の報告：
  https://www.semperis.com/resources-semperis-ransomware-holiday-risk-report/

- 2025年になって遠隔アクセスの侵害が多くのランサムウェア攻撃の端緒に

- 重要インフラを狙うハクティビストがランサムウェア攻撃基盤を利用
  Cyble社の報告：
  https://cyble.com/blog/hacktivists-infrastructure-move-into-ransomware/



法執行機関による攻撃集団の粉砕作戦が成功するも…

- 最も活発だったLockBitの基盤を2月に法執行機関が粉砕(Cronos作戦)
  Law enforcement disrupt world's biggest ransomware operation
  https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

- 粉砕作戦によって攻撃コミュニティ内に変動は生じたが
  ランサムウェア全体を抑え込むには至らず
  - RansomHubのような他のRaaSへのアフィリエート移動など
  - 新たに出現するRaaSも多数
  - 初期アクセス・ブローカーへの依存が高まる

[参考] Dragos Industrial Ransomware Analysis: Q3 2024 (12月17日)
https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q3-2024/

アサヒ・グループがランサムウェア攻撃で操業停止

https://www.asahigroup-holdings.com/newsroom/detail/20250929-0102.html

- 9月29日にサイバー攻撃を受けて国内グループ各社の受注出荷業務が停止
- 10月7日にランサムウェア集団(Qilin：麒麟)が，データ流出サイトにアサヒの企業名を表示して，攻撃を実施し27GBのデータを窃取したと主張
- 完全な復旧は2026年2月の予定

調査報告書(11月27日)
https://www.asahigroup-holdings.com/newsroom/detail/20251127-0104.html

[出典] CompariTech社のブログ記事から転載
https://www.comparitech.com/news/ransomware-gang-qilin-says-it-hacked-asahi-group-stole-data/

[考察] JLR社とアサヒ・グループのインシデントについて

- 明確にICS/OTの侵害が報じられているわけではない
  - 一定の地域で，ほぼ完全な操業停止に至っている
  - ICS/OTのID管理・認証基盤が足かせになったとの見方も
- 復旧に数週～数ヶ月の時間を要し，操業の停止が長期化している

[攻撃者の視点]

ITシステムに対する攻撃だけでもICS/OTを攻撃するのと同様の効果が達成できるかも…

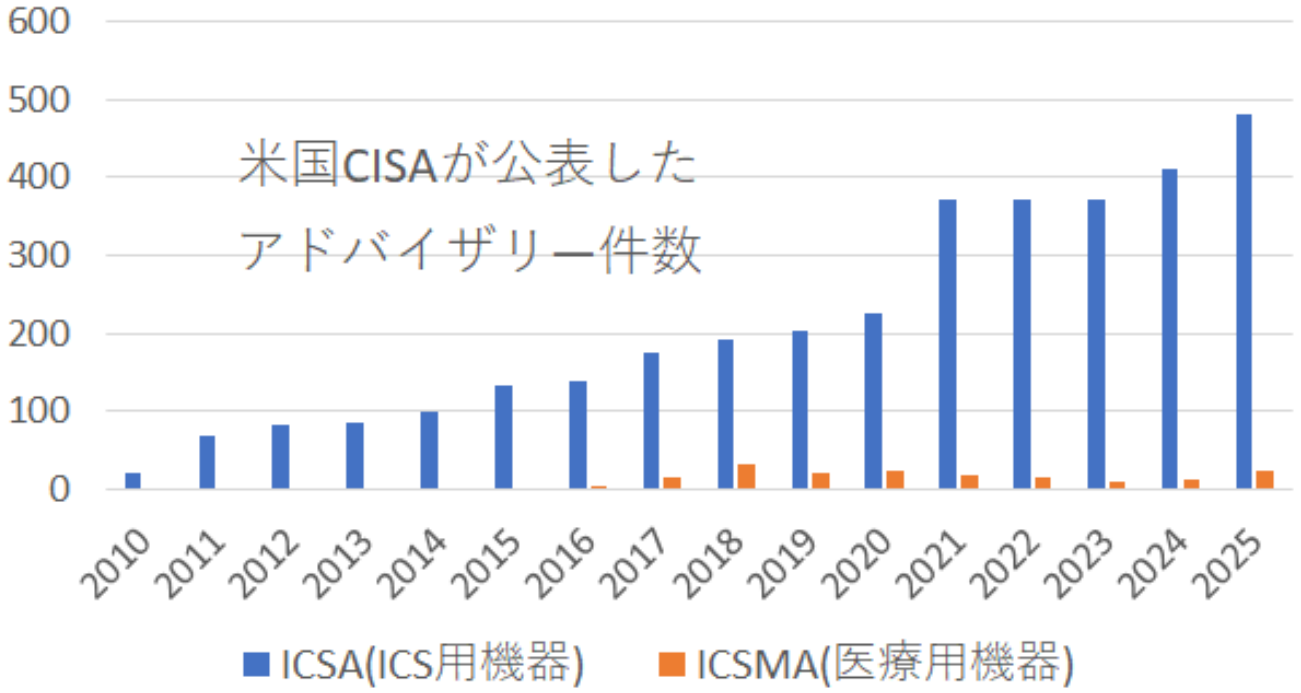
☞ 2025年に広く話題になり注目されたものはなかった

ICSを狙って作られた
マルウェアの動向

☞ CISAが公表したICS関連アドバイザリーの件数は前年の1割増し
☞ インターネットに露出した脆弱なICSコンポーネントが増加中との報告も
☞ 脆弱性情報の管理プログラムに不安

ICSコンポーネントの脆弱性の動向

米国CISA ICSが公表した脆弱性アドバイザリーの件数



・ 前年から2割近く増え481件に

・ うち，Siemens社が132件，Schneider社が54件

・ IT製品を含めた脆弱性の全体はCVEベースで48,177件 (前年比2割増)

ICS関連製品における脆弱性

- インターネットに直結された脆弱性もつICS関連製品が少なくない
  ForeScout社が報告書「The Riskiest Connected Devices of 2025」を公開
  https://www.forescout.com/resources/riskiest-devices-2025-report/

ICSハニーポットが数多くあるとの見方がある一方で，クラウド接続などに伴う，意図せざるインターネット露出も考えられる

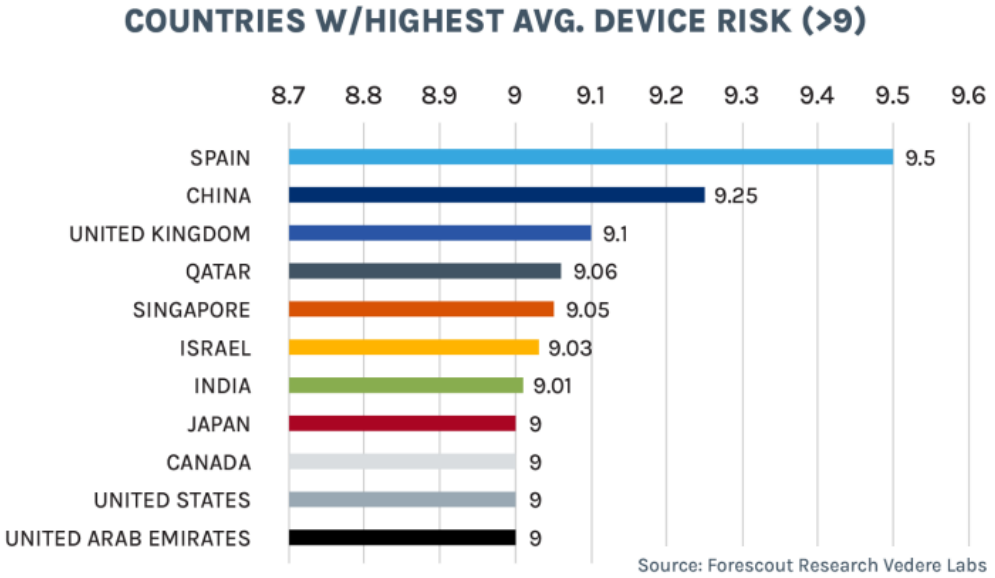


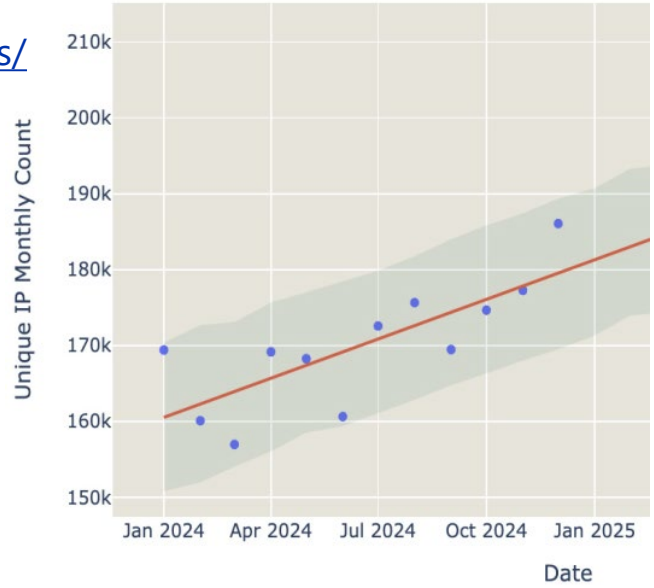
Figure 2 – Countries with the highest average device risk

インターネットに露出したICS/OT用機器が増加傾向

- BitSight社報告書「許し難いICS/OTの露出」
  https://enablement.bitsight.com/sh/5855757368160341l0/assets/

- 毎月16～18万台の機器が新たに露出
- 露出しているICS/OT機器の多くに
  深刻な脆弱性
- プロトコルの内訳：
  — Modbus，Niagara FOX，KNXが多い

- 日本からも約1.5万台が露出しており
  Lantronix社技術の関連が過半数を占める



グローバルな脆弱性情報の採番体制の不安が露呈

https://www.securityweek.com/mitre-cve-program-gets-last-hour-funding-reprieve/

- CVEプログラムにより
  個々の脆弱性にCVE識別子が割り当てられている
  — 米国政府(CISA)の資金でMITRE社が全体統括している

- Trump政権の政府効率化省(DOGE)の混乱の中でMITRE社との契約更改が進まなくなり，CVEプログラムの契約が満了する4月16日以降の運用停止の可能性をMITRE社が警告
  — 大騒動の後に，暫定契約が締結されて混乱を回避

CISA声明文：
https://www.cisa.gov/news-events/news/statement-matt-hartman-cve-program

- 1国の政策に依存しない管理体制を議論するきっかけとなった
  — ユニークな識別子 + 各識別子に対応する信頼できる脆弱性情報

新たなCVE管理プログラムの模索 (1/2)

- 米国で急遽CVE Foundationが発足 (4月16日)
  https://www.thecvefoundation.org/
  - 非営利組織
  - 資金源や活動内容などの詳細不明

- 「標準の脆弱性追跡システムの分裂が始まった」との報道も (4月18日)
  CVE fallout: The splintering of the standard vulnerability tracking system has begun
  https://go.theregister.com/feed/www.theregister.com/2025/04/18/splintering_cve_bug_tracking/

新たなCVE管理プログラムの模索 (2/2)

- ENISAが欧州版の脆弱性データベースEUVD開設を発表 (5月13日)
  https://www.enisa.europa.eu/news/consult-the-european-vulnerability-database-to-enhance-your-digital-security
  - ENISAが開設・運用
  - NIS2指令の要件

- 欧州ではGlobal CVE (GCVE)を開設 (2026年1月7日)
  https://gcve.eu/2026/01/07/gcve-db-announce/
  - EUの資金でルクセンブルグのCSIRT(CIRCL)が構築運用

- 米国NISTはNVDにおけるNISTの役割の見直しを検討
  https://csrc.nist.gov/Events/2026/ispab-january-2026-meeting

NVD (National Vulnerability Database)

NISTによる脆弱性情報の整理補追処理が追い付いていなかった. 脆弱性情報についてはCNAに頼る方向へ

- ☞ 欧州はNIS2指令の国内法整備期限を迎えたが…
- ☞ IEC 62443などOT関連の標準やガイドの整備が進んだ

標準の整備と規制の強化

欧州のNIS-2指令

ネットワークと情報システム(Network and Information Systems Directive)指令(EU) 2022/2555
https://eur-lex.europa.eu/eli/dir/2022/2555

- NIS指令(指令(EU) 2016/1148)の強化版

- 重要基盤のネットワークとシステムの保護に関する規制
  - 重要基盤を運用する事業者に対する規制
  - セキュリティ対策やインシデント報告を義務づけ

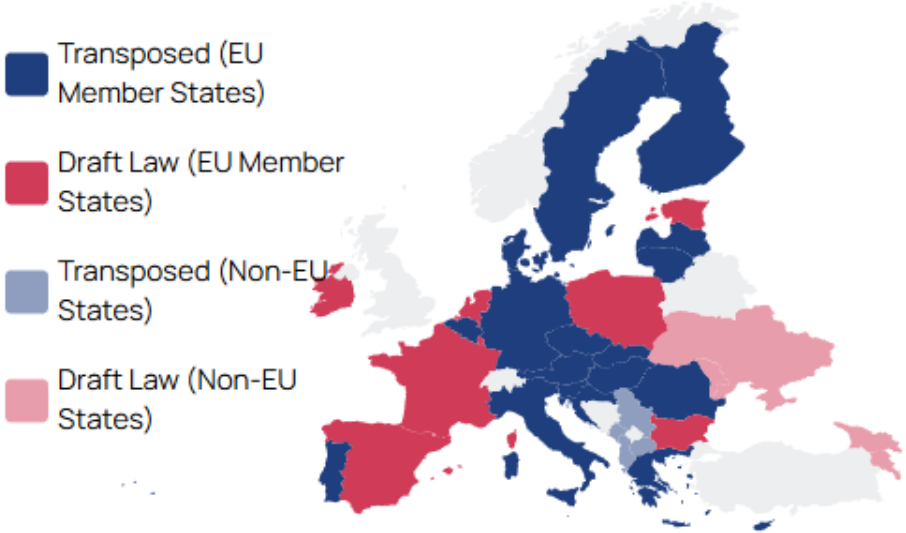
- 2024年10月17日までに対応する国内法を整備することになっていた(加盟各国の義務)

欧州のNIS-2指令の国内法の整備に手間取っている国も

- 期限 (2024年10月17日)内に対応する国内法の整備を終えた国は数ヶ国
  — 2025年末時点でもフランスやスペインなどが草案の段階

[参考] NIS2 in EU Countries
https://www.openkritis.de/eu/eu-nis-2-member-states.html

[加盟各国の現状] State-of-play of the transposition of the NIS Directive
https://digital-strategy.ec.europa.eu/en/policies/nis-transposition



図の出典：Wavestone社
https://www.wavestone.com/en/insight/nis-2-european-countries-transposing-directive/

NIS2対応の国内法を終えた国では対策が進み始めた

- ベルギーでは2024年10月にNIS2対応の国内法を施行 (EU最初)
  - 重要事業者としての登録が2,410組織 (登録期限：3月18日)
  - 登録事業者には各種のセキュリティ・サービスをベルギー・サイバーセキュリティ・センター(CCB)が無料提供
    - ✓ 優先アラートなどの情報サービス
    - ✓ 脆弱なシステムの検知・警告 など
- ENISAが重要インフラ業界の成熟度と機微さに関する報告書「ENISA NIS360 2024」

  https://www.enisa.europa.eu/publications/enisa-nis360-2024

NIS-2： NIS-1からの主な変更点

- 規制対象の事業者を拡大するとともに対象範囲を明確化
  - NIS-1の不可欠なサービスの運用者とデジタルサービス事業者から
    NIS-2では不可欠な組織(大手)と重要な組織(中規模)
- セキュリティ要件をより明示的に定めるとともに拡充
- 3段階のインシデント報告
  - 気付いてから1日以内に速報
  - 重要インシデントに気付いてから3日以内に通知
  - 通知から1ヶ月以内に最終報告
- 違反に対して罰金(最大で1千ユーロと年間売上の2%の高い方)

2025年4月17日までに加盟国が一覧を配布

2027年10月17日までに議会と理事会に状況報告；見直しの可能性

IEC 62443シリーズの動き

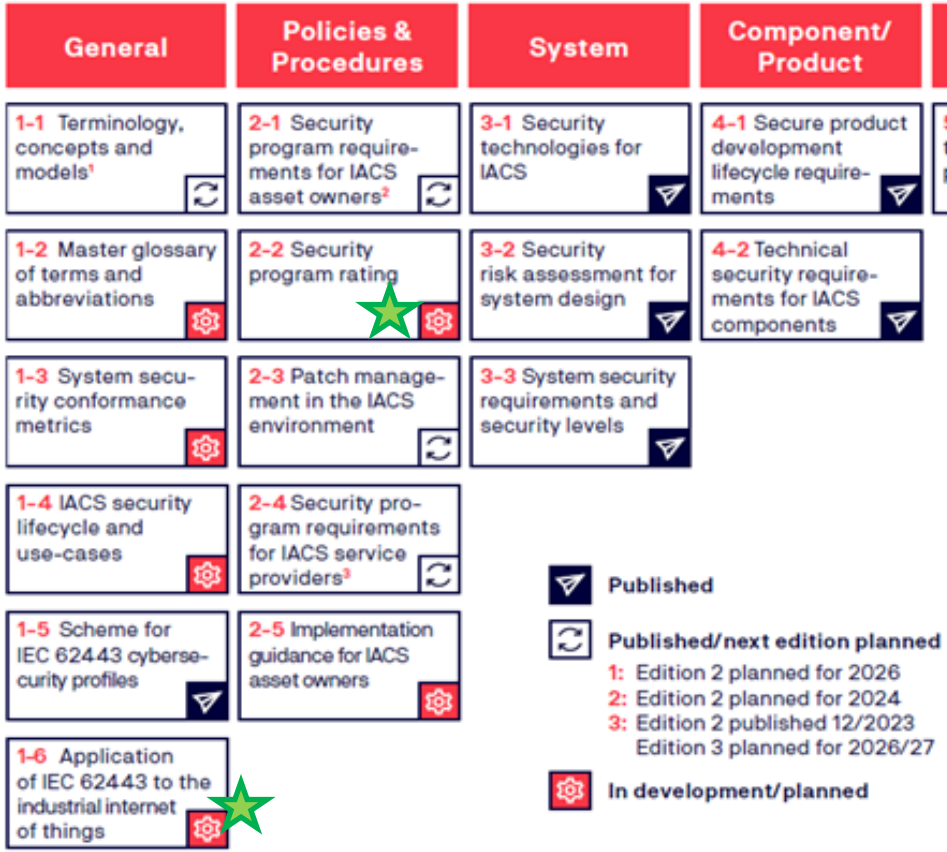
PAS: Publicly Available Specification
TS: Technical Specification

- IEC PAS 62443-1-6:2025
  Security for industrial automation and control systems - Part 1-6: Application of the 62443 series to the Industrial Internet of Things (IIoT)
  62443シリーズ標準のIIoTへの適用

- IEC PAS 62443-2-2:2025
  Security for industrial automation and control systems – Part 2-2: IACS security protection scheme
  セキュリティ管理評価(保護水準)の概念の導入

- IEC TS 62443-6-2:2025
  Security for industrial automation and control systems - Part 6-2: Security evaluation methodology for IEC 62443-4-2
  IEC 62443-4-2のためのセキュリティ評価法

IEC 62443シリーズの体系



★ : 2025年発行文書

Electron Consortium
What is ISO/IEC 62443 standard?
https://www.cybersecurity-lighthouse.com/main-standards/iec-62443/

FERCがCIP-015-1を承認

https://www.ferc.gov/media/e-13-rm24-7-000

- CIP-015-1 (サイバーセキュリティ – 内部ネットワーク監視)を承認(6月26日)
  - CIP(Critical Infrastructure Protection)は北米の電力事業者団体(NERC)が定めているセキュリティ標準
  - 電力基幹網の運用者と直結された設備をもつ事業者が対象
  - 米国ではFERCが指定した項目が事業者に義務づけられる

  - この改訂では，重要設備の制御に関わる部分だけでなく，その部分と接続されたネットワークのセキュリティ監視が追加された

米国政府からの主な公開文書

- (1月17日)湾岸警備隊： Final Rule: Cybersecurity in the Marine Transportation System
  https://www.news.uscg.mil/maritime-commons/Article/4033732/final-rule-cybersecurity-in-the-marine-transportation-system/

MITRE社がATT&CKを第18版に更新

https://attack.mitre.org/resources/updates/

- 半年ごと(春と秋)に定期的に更新されている

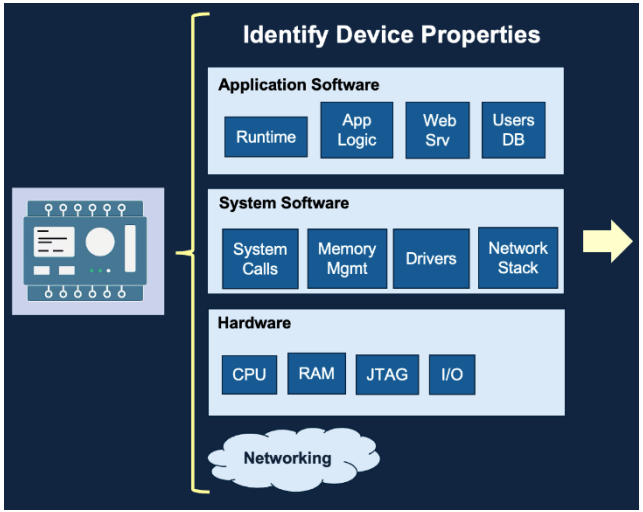
- ICS関連では：
  12の戦術，83の技法，14の攻撃集団，23のソフトウェア，７の攻撃行動，52の攻撃による影響の緩和策，18の資産，83の検知戦略，82の分析，36のデータコンポーネント

MITRE社がEMB3D脅威モデルを更新

https://emb3d.mitre.org/

- EMB3DはICS環境などで見られる組込み機器用の脅威モデル

- 初版公開後のフィードバックに対応した4月22日に2.0版を公開
  https://emb3d.mitre.org/subtabs/version-history.html
  - 機械可読な脅威情報表現
    (STIX) 2.1 JSON形式を導入
  - プロパティーの改訂と追加
  - 脅威の改訂と追加
  - 軽減策の改訂と追加



[関連] Embedded System Threat Matrix (ESTM)
https://estm.mitre.org/

英国政府からICS/OT向けインシデント対応ガイド

- (6月24日) 英国政府の研究機関RITICSが
  ICS/OT向けインシデント対応のためのガイダンスを公表
  GUIDANCE: Considerations for Cyber Incident Response Planning within Industrial Control Systems/Operational Technology.
  https://ritics.org/wp-content/uploads/2024/06/ICS-COI-Considerations-for-Cyber-Incident-Response-Planning-within-ICS-and-OT.pdf

- 英国NCSC(National Cyber Security Centre)がOT関連のガイダンス・ページを開設し文書の整備を進めている：
  [guidance] Operational Technology -- Making sense of cyber security in OT environments.
  https://www.ncsc.gov.uk/collection/operational-technology

- ☞ 約1年間におよぶ長官の不在
- ☞ Trumpによる報復的な組織破壊
- ☞ 強まる敵対的国家によるサイバー攻撃
- ☞ CIRCIA

米国CISAの混乱と課題

国土保安省(DHS)傘下のCISA (Cybersecurity & Infrastructure Security Agency)が，2009年創設のICS CERTを源流とする米国政府におけるICSセキュリティへの取り組みを担ってきたが…

CISAが組織的に弱体化

- 「2019年の大統領選挙に不正無し」とするCISAに対して
  Trumpが5年越しの個人的な怨念
- Trumpの着任と同時にJen EasterlyがCISA長官を辞任

- 3月にTrumpがCISA長官としてSean Plankeyを指名し，
  業界関係者からも好意的に迎え入れられたが，
  上院の同意が得られず(強硬にRon Wyden議員が反対)

- 政府効率化省(DOGE)と政府閉鎖期間中(10月1日～11月12日)に
  大量の職員を解雇し，定員の3割が空席に
  3,387名(Trump就任前) ⇒ 2,389名 (12月中旬； 998名減)

CISAに対する矛盾する要求と内外からの圧力

- TrumpやDHS長官Kristi NoemはCISAのスリム化を主張
  — 選挙セキュリティの要員を真っ先に解雇

- 米国議会は選挙セキュリティを含む体制の拡充と要員の再雇用を要求
  (米国政府の予算は議会の専管事項； 大統領には権限がない)

- 地政学的な野望と攻撃的な中国に起因するサイバー脅威の増大

- 解雇や長官の長期不在によるCISA内の士気の低下

- 議論を招きそうな2022年重要インフラ向けサイバーインシデント報告法の施行準備

2022年重要インフラ向けサイバーインシデント報告法

CIRCIA: Cyber Incident Reporting for Critical Infrastructure Act of 2022

- インシデントの発生(認知後3日以内)とランサムウェアの身代金の支払い(1日以内)について，大手の重要インフラ事業者に対して，CISAへの報告を義務づけ
  https://www.govinfo.gov/link/plaw/117/public/103

- 報告の要件の決定(本来は2025年秋)を2026年5月に延期
  — 最終要件(原案公表から1.5年以内)が決まると発効

重要インフラ事業者に対するインシデント報告義務

- EUではNIS2が報告を義務づけ
- スイスでも4月1日から義務づけ
  https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2025/meldepflicht-2025.html
- 英国政府も義務付けを検討中
  https://therecord.media/uk-sets-out-cyber-reporting-requirements-critical-infrastructure

☞ 急速に進化するAI技術に伴うセキュリティ課題
☞ 量子コンピューター時代に備えた暗号

新技術に伴って浮上するセキュリティ課題

量子コンピューティング時代への備え (1/2)

- 2035年頃に量子コンピューターが実用水準に達する可能性がある
  — 量子コンピュータにより公開鍵暗号アルゴリズムの一部が危殆化

- 製品寿命の長いICSでは暗号を利用しているコンポーネントについて先行的にPQCへの移行対策を検討しておく必要がある

ポスト量子暗号(Post-Quantum Cryptography)

量子コンピューティング時代への備え (2/2)

- PQCA (Post-Quantum Cryptography Alliance)が2024年2月6日に発足
  https://pqca.org/
  - 移行ロードマップを公開 (5月28日)
    https://www.mitre.org/news-insights/news-release/post-quantum-cryptography-coalition-unveils-pqc-migration-roadmap

- ICSやIoT機器でPQCへの移行に立ち遅れ：ForeScout社のブログ記事 (9月30日)
  Q-Day Countdown: New Data on Post-Quantum Cryptography Adoption Across Devices and Industries
  https://www.forescout.com/blog/q-day-countdown-new-data-on-post-quantum-cryptography-adoption-across-devices-and-industries/
  - 暗号モジュールが容易に交換可能な作りが理想

Windows 10の通常のサポートが10月14日に終了した

- Microsoft社「Windows 10 リリース情報」
  https://learn.microsoft.com/ja-jp/windows/release-health/release-information
  - Windows 10の最終バージョンは22H2で10月14日にサービス終了
  - Wwindows 10長期サービス･チャンネル･エディションは別途

- 海運業界では40.36%のシステムでWindows10が稼働中
  Windowsサーバー(5.65%)やWindows7(2.15%)，Windows8.x(0.42%)も
  https://marlink.com/resources/knowledge-hub/end-of-windows-10-support-signals-growing-cyber-threat-to-it-ot-systems/

- 特殊な装置の専用PCなどで使われ続けている可能性も

まとめ

- 表面的には比較的平穏な年だったと言えそう
  一部には新時代への胎動を思われる動きも
- ランサムウェアの猛威は衰えていない； 頂は高まり裾野も拡大
- 地政学的な緊張の高まりの中でサイバー脅威が高止まり
- ICSセキュリティ対策戦略自体が大きく変わり始めていて
  対策の前提から見直す思潮の萌芽も

お問い合わせ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：pr@jpcert.or.jp
- https://www.jpcert.or.jp/reference.html

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

脆弱性に関するお問い合わせ

- Email：vultures@jpcert.or.jp
- https://jvn.jp/

ご清聴ありがとうございました