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 ～

2024年版

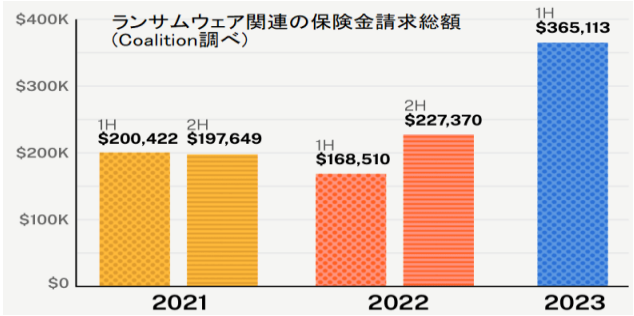
JPCERTコーディネーションセンター
ICSR　技術顧問
宮地利雄

- ☞ 深刻度と頻度において最大のITとOTに共通した脅威に
- ☞ サイバー攻撃が産業化しているとも言える様相
- ☞ 元来は金銭目的だが，一部はサイバー・テロの色合い

ランサムウェアに関連したインシデントの動向

最悪のランサムウェア被害の年になった可能性大

- 身代金として上半期だけで総額4.49億ドルが支払われた
  (Chainalysis社調べ： https://therecord.media/ransomware-gangs-extorted-record-amounts)
  - 最悪だった2021年の年間9.399億ドルとほぼ同水準



- サイバー保険金の請求総額も急増し上半期だけで3.65億ドル
  (Coalition社調べ： https://therecord.media/cyber-insurance-claims-spike-as-ransomware-soars)

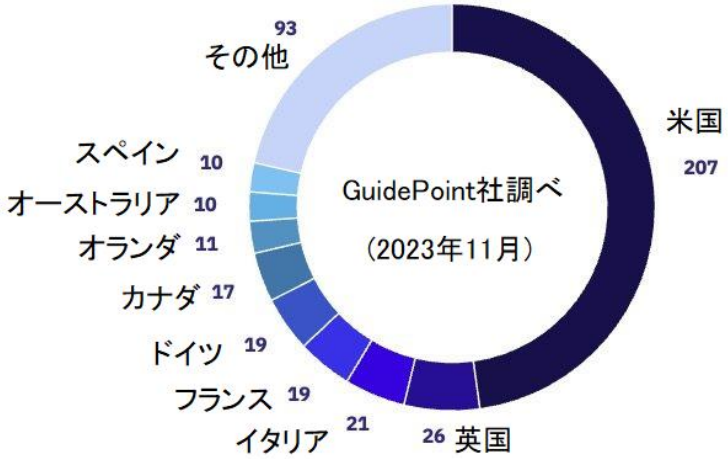
- システム停止による損失の見積総額が7月までで47億ドル
  (CompariTech社調べ： https://www.comparitech.com/blog/information-security/ransomware-manufacturing-companies/)
  - 最悪は2020年の年間142億ドルで，2022年の123億ドルが次ぐ
  - 製造事業者にとっては，身代金もさることながら，システム停止による操業の混乱による損害がはるかに重い負担となる

主なランサムウェアと主な被害者

- 30以上の活動的なランサムウェア攻撃集団の存在が知られている
  - 攻撃成功を宣言するメッセージが日平均十数件投稿されている
  - 被害件数が月平均6%で増加中

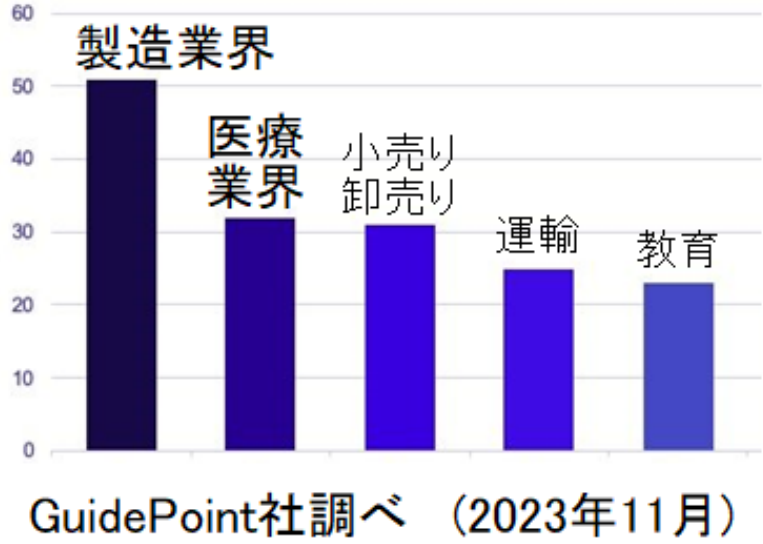
- 半年以上攻撃活動が続く広く知られたランサムウェアによる被害が8割以上を占めている
  LockBit，Alphv/BlackCat，Playなど

- 被害組織の約半数が米国，1/4が欧州
  - 日本企業も海外現法で被害
  - 11月頃から中国企業でも被害



製造業界が最も狙われている

- ランサムウェア攻撃集団が製造業界をもっとも狙っている
  - 操業の混乱による損害が大きく身代金を支払う傾向が高い(?)
  - 最も活動的な攻撃集団LockBitがOTを狙っているとの情報も（Dragos社；3月27日）



GuidePoint社調べ （2023年11月）

https://www.dragos.com/blog/lockbit-ransomware-continued-to-impact-operational-technology-in-2022/

- 大手企業だけでなく中小まで多様な規模の企業が狙われている

ランサムウェアと攻撃技法の変化

- 他の方法で組織内に侵入してから組織内部でランサムウェアを配備する攻撃段階を踏むケースが主流に
  - 組織内への侵入から比較的短期間のうちにランサムウェア攻撃
  - 同時に複数の種類のランサムウェアを配備する手口も

- 身代金の支払いを迫る様々な手口
  - 「持ち出した情報を公表するぞ」と脅迫
  - 被害企業の顧客に対して脅迫
  - 被害企業がインシデント報告義務を果たしていないとSECに提訴
  - 身代金として募金を迫る攻撃者も

SEC: 米国証券取引委員会
https://www.darkreading.com/risk/alphv-ransomware-group-files-sec-complaint-against-own-victim

https://cyberscoop.com/ransomware-charity-malaslocker/

政治的にもランサムウェア対策が課題として浮上

- バイデン政権の主導で国際ランサムウェア対策タスクフォース(ICRTF：Inernational Counter Ransomware Task Force)が1月に発足
  11月には合同声明

  https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/

- 米国CISAがランサムウェア脆弱性警告パイロット(RVWP：Rasomware Vulnerability Warning Pilot)を3月に発表

  https://www.cisa.gov/news-events/alerts/2023/03/13/cisa-announces-ransomware-vulnerability-warning-pilot

  — ランサムウェア攻撃に悪用されがちな脆弱性をもつ機器でインターネットからアクセス可能なものを探索し利用者に警告する

注 CISA: Cybersecurity and Infrastructure Security Agency

RTU機器を狙ったランサムウェアの報告も

Claroty社： https://claroty.com/team82/blog/hacktivist-group-claims-ability-to-encrypt-an-rtu-device

- アノニマスにも関連している親ウクライナ派のハクティビスト集団GhostSecがTeleOfis RTY968 v2を暗号化できると主張
- 当該機器が，インターネットに直結した状態で，ロシアやカザフスタン，ベラルーシュで運用されており，うち117台ではSSHサービスが稼働している
- 実際に稼働中の機器への攻撃の有無は不明

TELEOFIS RTU968 v2（Claroty社ブログより）

船舶管理システムもランサムウェア感染でオフライン運用

DNV船級協会： https://www.dnv.com/news/cyber-attack-on-shipmanager-a-dnv-software-237552

- 70社が保有する約1,000隻の外航船でランサムウェア・インシデントによる影響があったとDNV船級協会(ノルウェイ)が1月に公表
  - 同協会が提供しているソフトウェアShipManager用のサーバーがランサムウェアに感染して運用を停止
  - ShipManagerのオフライン機能(船舶側)は利用できた

2023年の主なランサムウェア・インシデント

- カナダの銅鉱山会社がランサムウェアに感染し予防的にICSを止めて人手作業で対処(2022年12月～1月)
  https://www.isssource.com/copper-miner-hit-in-ransomware-attack/
- 米国Dole社がランサムウェアに感染して北米工場の操業が混乱(2月)
  https://www.isssource.com/dole-hit-in-ransomware-attack/
- 名古屋港がランサムウェアに感染して荷扱いを3日間停止(7月)
  https://www.isssource.com/japanese-port-resumes-ops-after-ransomware-attack/
- 米国Clorox社(洗剤製造)がランサムウェアに感染し1ヶ月以上工場が停止(9月)
  https://therecord.media/clorox-production-issues-after-august-cyberattack
- ラスベガスで著名なMGMとCaesars両ホテルがランサムウェアに感染(9月)
  https://www.darkreading.com/attacks-breaches/-scattered-spider-mgm-cyberattack-casinos

ランサムウェアの動向に関する報告書など

- GuidePoint社によるGRITランサムウェア報告書
  https://www.guidepointsecurity.com/blog/grit-ransomware-report-月-2023/
  (月の部分は「may」のように英語の月名をすべて小文字で表記)

- 重要インフラを狙っているRaaS (Ransomware As A Service)への
  Group-IB社による潜入報告
  https://www.group-ib.com/blog/qilin-ransomware/

- 重要インフラにおけるランサムウェア感染事例データベース
  (米国テンプル大学が管理)
  https://sites.temple.edu/care/cira/

- ☞ ロシアによるウクライナへの進攻(2022年2月24日)から2年に激しいサイバー攻撃の実態が徐々に明らかになってきた
- ☞ イスラエルとハマスが内戦状態に

戦争に関連したインシデントの動向

ウクライナの電力網へのサイバー攻撃

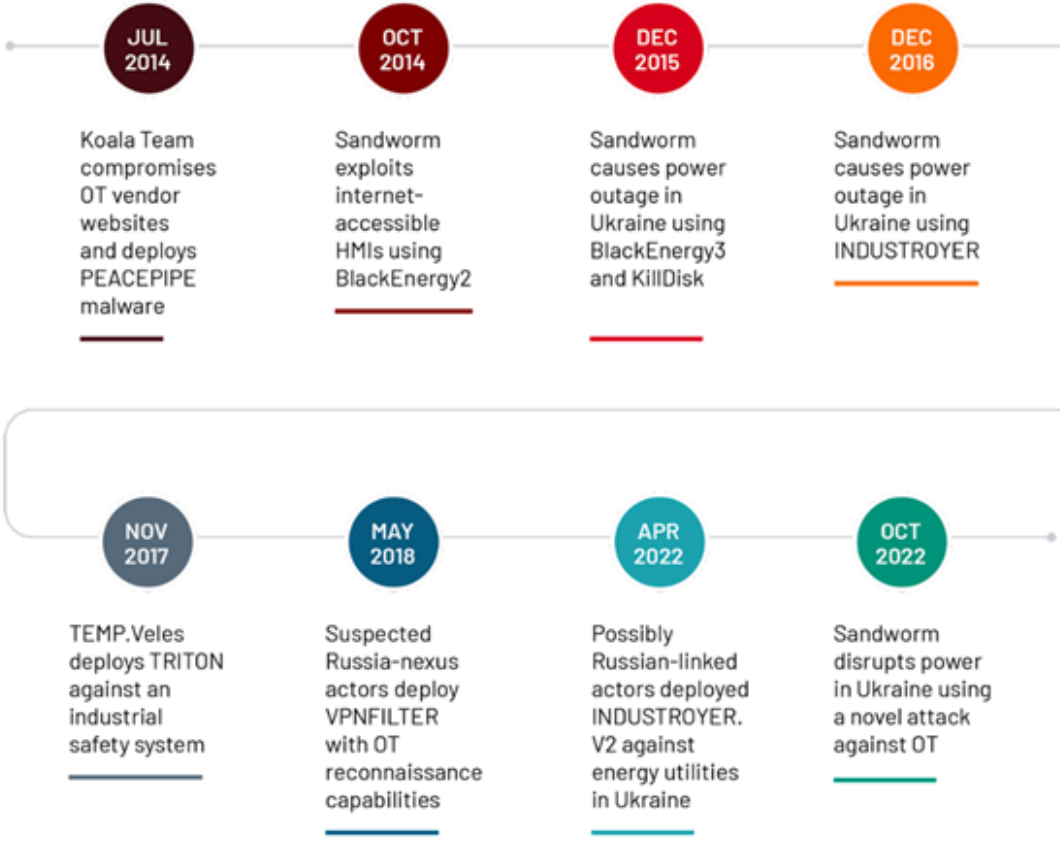
長年のSandworm攻撃集団によるウクライナの電力網に対するサイバー攻撃についてMandiant社が9月にブログ記事：

https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology

- 攻撃は2022年6月以前に始まり
  SCADAをホストしたハイパーバイザーに3ヶ月間潜在し
  2022年10月11日と12日に攻撃の最盛期
  - MicroSCADAサーバーからIEC-104/101プロトコルを介して遮断器のRTUを操作しようとする (未然に攻撃対策がとられて停電なし)

- 被害組織のIT環境にCaddyWiperの亜種を配備

ロシアによるウクライナの電力網へのサイバー攻撃の系譜



(本ページは
Mandiant社の
11月9日のブログ
記事から引用)

ウクライナ戦争下のサイバー攻撃

- ウクライナ特別通信と情報保護庁(SSSCIP： State Service of Special Communications and Information Protection of Ukraine)が
  ロシアによる上期のサイバー攻撃を9月末に報告
  https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/russias-cyber-tactics-h12023.pdf
  - 前期比でインシデント倍増 (4～5件/日；2022年下期は平均1.9件/日)
  - サイバー・スパイ活動の主対象は，民間企業と司法当局
    (特にエネルギー業界と通信業界)
  - 一旦攻撃に遭うと常時攻撃されるようになる
  - 報道機関と緊急対応機関が一定してサイバー攻撃に晒された
  - LOtL (Living Off the Land)戦術が増加傾向

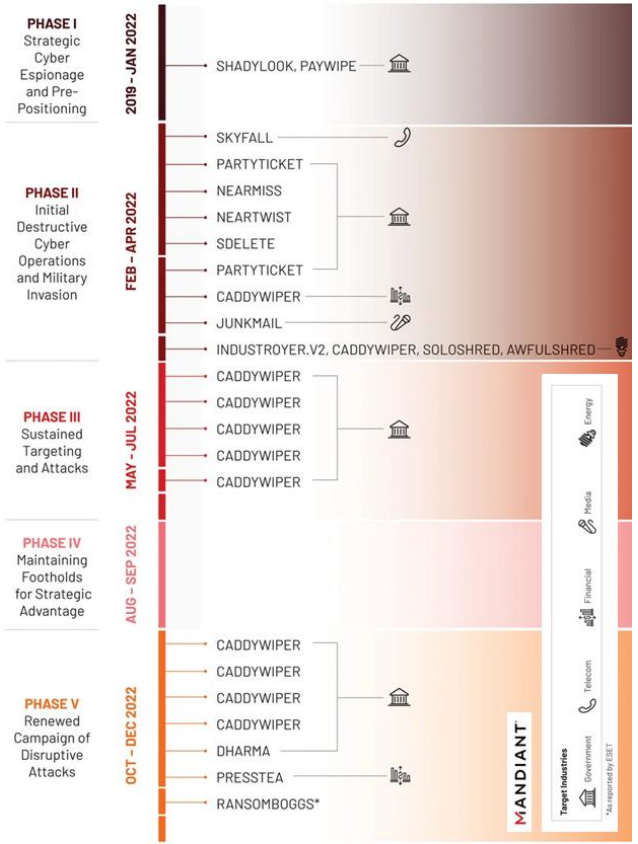
持ち込んだものでなく現地にあるツールを使って攻撃活動を行う

ウクライナ侵攻からの1年間を総括した報告書 (1/2)

- Google社TAGが2月にブログ記事と報告書を公表
  https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/
  https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
  - ロシア政府支援を受けた攻撃者が多面的に活動；多くの成否は半ば
  - 戦争についての世論を誘導するために様々な情報操作活動を展開
  - 東欧のサイバー犯罪エコシステムに地殻変動
    サイバー犯罪集団間に新しい連携と規模拡大

  [その後の見通しとして]
  - ロシア政府支援によるウクライナとNATOへのサイバー攻撃続く
  - 破壊的なサイバー攻撃が増える
  - 効果はともかく，世論操作を狙った偽情報の配付が続く

2022年のロシアのサイバー攻撃は5段階に分けて理解される



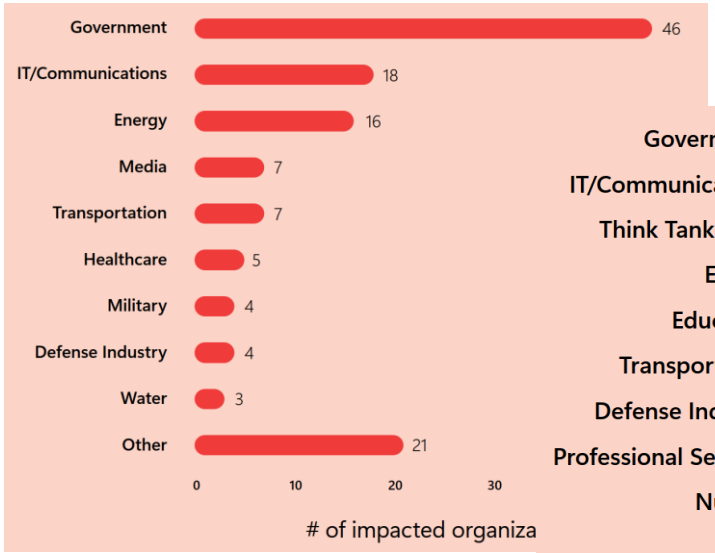
(本ページはGoogle社の報告書15ページから引用)

- 第1段階 (～2022年1月)
  戦略的なサイバー・スパイと事前準備
- 第2段階 (2022年2月～3月)
  軍事侵略と併行する初期の破壊的攻撃
- 第3段階 (2022年5月～7月)
  攻撃と攻撃対象の絞込みを維持
- 第4段階 (2022年8月～9月)
  戦略的優位性を求めた橋頭保の維持
- 第5段階 (2022年10月～12月)
  刷新された破壊的攻撃

ウクライナ侵攻からの1年間を総括した報告書 (2/2)

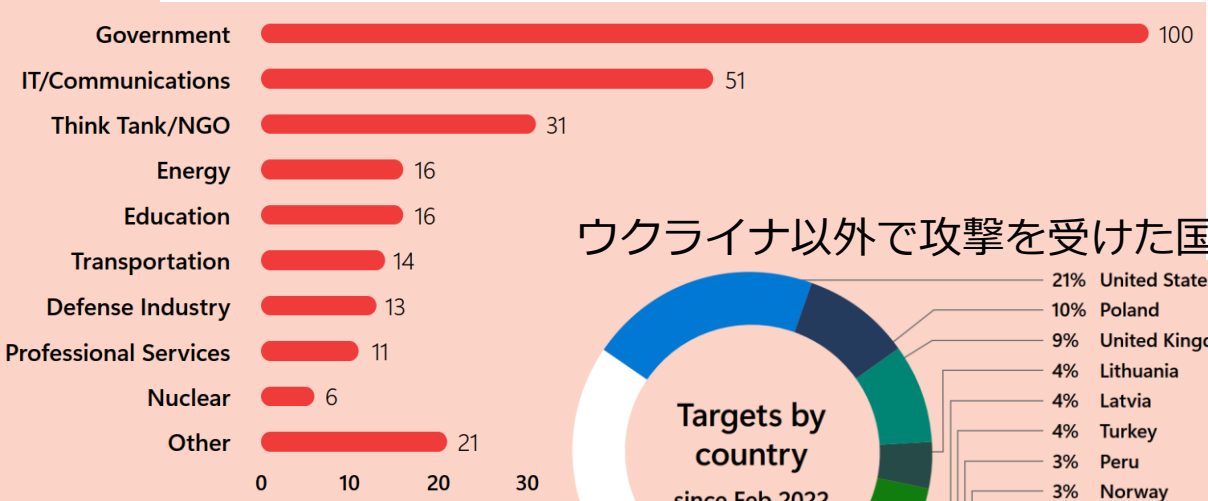
- Microsoft社が3月にブログ記事と報告書を公表
  https://blogs.microsoft.com/on-the-issues/2023/03/15/russia-ukraine-cyberwarfare-threat-intelligence-center/
  https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf
  - 進攻が始まった2022年2月から3月を中心に
    破壊的なサイバー攻撃(ワイパー等)の情報操作活動が活発化
  - ウクライナだけでなく米国やポーランド，英国も狙われている
  - 攻撃がロシアによるものでないと見せかけるために
    ランサムウェアを使って破壊的な攻撃が行われている
  - 攻撃のための初期アクセスの獲得手段が多様化している
  - ハクティビストを煽って攻撃に参加させている

ロシアが戦争の1年間に攻撃した対象

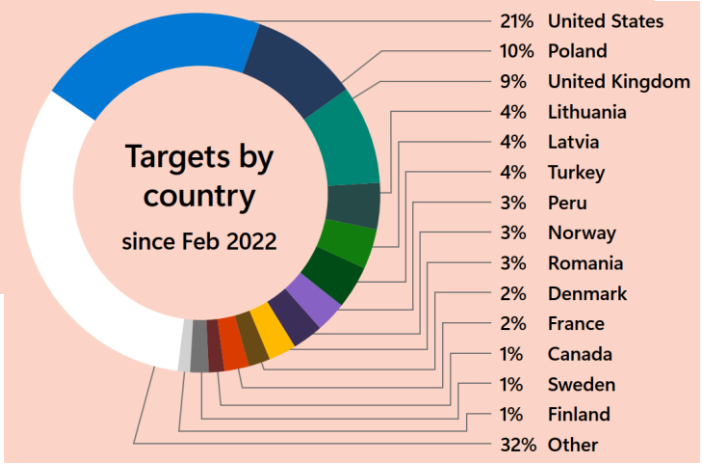


ウクライナ国内で
攻撃を受けた業界

ウクライナ国外で攻撃を受けた業界



ウクライナ以外で攻撃を受けた国



(本ページはMicrosoft社の報告書の
10および11ページから引用)

ロシアによるサイバー攻撃に関してロシア側からも情報

- ロシアの契約企業NTV Vulkan社からサイバー戦争計画の一部が流出(3月)
  https://www.mandiant.com/resources/blog/cyber-operations-russian-vulkan

  - Maniant社と複数の報道機関が
    流出した「Vulkanファイル」を入手して分析
  - 流出した文書の日付は2016年～2020年
  - NTV Vulkan社はロシアの軍事諜報機関GRUなどと契約関係にあり，
    ツール開発や訓練プログラム，侵入基盤を提供
  - ファイルに記載された計画が実施されたか否かなどは不明

ウクライナの事例に基づく将来のサイバー戦争の考察

戦略国際問題研究所(CSIS： Center for Strategic International Studies)から7月に報告書

https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war

- 大局的な勝敗を決するのは機動力を用いた物理的な攻撃
- 曖昧な紛争状態や開戦時において，
  機動力による攻撃を支援する目的でサイバー攻撃

Defence Horizon誌に9月に掲載されたブログ記事「ハイブリッド戦争の観点から見たロシア･ウクライナ紛争」

https://tdhj.org/blog/post/russia-ukraine-hybrid-warfare/

- 2022年2月の侵攻前後はハイブリッド戦争の色合いを帯びていたが，
  その後は，機動力に依存し，なりふり構わぬ残虐性や戦争犯罪を厭わぬ
  昔ながらの軍事戦略に傾斜していった

中東でも，ハマスとイスラエルとが内戦状態に

- ハマスとイスラエルとの間の戦争を理解するには
  次の3つの対立軸の複合体として見る必要がある：
  1. イスラエル国内のユダヤ人とパレスチナ人との戦い
  2. イスラエルと中東地区のパレスチナ勢力との戦い
  3. イランと米国との代理戦争

- これらの関係者に，それぞれの親派のハクティビストが加わって，
  サイバー攻撃や世論操作活動を展開

ハマス・イスラエル間の戦争に伴うサイバー攻撃 (1/2)

- 占領地域で操業しているイスラエルの化学企業に大規模サイバー攻撃 (1月)
  https://www.securitynewspaper.com/2023/01/30/hacker-group-hacks-in-israeli-chemical-factories/
  - 次なる攻撃を示唆しつつ，従業員に離職を促がす
- イスラエル最大の精油事業者BAZANグループを親イラン派のCyber Av3ngerがサイバー攻撃 (7月)
  https://www.darkreading.com/dr-global/israeli-oil-refinery-taken-offline-pro-iranian-attackers
  - 操業への影響がなかったと見られているが，
    多数のOT関連の図面や画像を公表
- 親イラン派攻撃集団SiegedSecがICSを探索中と報じられる
  https://www.darkreading.com/dr-global/pro-iranian-hacktivists-sights-israeli-industrial-control-systems
  - まだ攻撃にまで至った事例は見つかっていない

ハマス・イスラエル間の戦争に伴うサイバー攻撃 (2/2)

- ハマス側のサイバー活動集団とその動向をSentinel Labs社が報告
  https://www.sentinelone.com/labs/the-israel-hamas-war-cyber-domain-state-sponsored-activity-of-interest/
  - ハマスに近い集団
    - Arid Viper (別名： APT-C-23, Grey Karkadann, Desert Falcon, Mantis)
    - Gaza Cybergang (別名： Molerats, TA402, Gaza Hackers Team, Moonlight, Extreme Jackal, Aluminium Saratoga, JEA/Jerusalem Electronic Army(低～中確度))
  - ヒズボラに近い集団
    - Plaid Rain (別名： Aqua Dev 1, Polonium)
    - Lebanese Ceddar (別名： Volatile Cedar, DeftTorero)
  - イランに近い集団
    - ShroudedSnooper (別名： Storm-0861, Scarred Manticore)
    - Cobalt Sapling (別名：Moses Staff, Abraham’s Ax, Marigold Sandstorm)

中国によるサイバー攻撃への警戒感が高まる

- 中国がサイバー能力を急速に高めていることをArmis社が白書で指摘 (4月)
  https://www.armis.com/blog/the-cyberwarfare-capabilities-of-east-vs-west/
- 中国の支援を受けた攻撃集団VoltTyphoonが米国の重要インフラ組織をLotL攻撃で狙っているとMicrosoft社が警鐘 (5月)
  https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/
- 中国のサイバースパイ集団RedFlyがアジアのある国の電力網に侵入しているとSymantec(BroadCom)社が報告 (9月)
  https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/critical-infrastructure-attacks
- 中国のサイバー作戦能力が過去5年間に急速に進化してきているとRecored Future社が報告
  https://www.recordedfuture.com/charting-chinas-climb-leading-global-cyber-power

- ☞ 地政学的な近況が高まる中でGPS信号の攪乱が日常化
- ☞ 中東地域におけるサイバー・インシデント
- ☞ 水道施設に対するサイバー攻撃

その他のサイバー・インシデント

日常化しつつあるGPS信号への攪乱攻撃

- GPS信号は，主に位置情報を得るために使われているが，
  一部のICSは正確な時刻情報を得るためにGPS信号を利用している

- ウクライナの電力網を攻撃するためにGPS信号をロシアが攪乱することに備え，特殊機器をCisco社がウクライナに提供か (CNN報道)
  https://amp-cnn-com.cdn.ampproject.org/c/s/amp.cnn.com/cnn/2023/11/21/politics/ukraine-power-grid-equipment-cisco/index.html

- 偽のGPS信号がイラン周辺でも観測されている
  https://www.avweb.com/aviation-news/gps-spoofing-signals-traced-to-tehran/

中東地域におけるサイバー・インシデント

- パキスタンで2日間にわたる全国的な停電； 当初はサイバー攻撃の可能性も疑われたが，根深いシステム問題が原因と後日に判明 (1月)
  https://asian-power.com/power-utility/exclusive/pakistans-energy-and-economic-woes-intensify-blackouts-reveal-deep-rooted-issues

- イランで革命記念日の大統領演説中にサイバー攻撃で放送中断 (2月)
  https://www.reuters.com/world/middle-east/iran-marks-44th-anniversary-revolution-online-hackers-interrupt-state-tv-2023-02-11/
- 2021年7月のイラン国内の鉄道の広域的な混乱が
  イラン国内の反体制派サイバー攻撃集団によるものだったとの
  分析をCheckPoint社が公表 (8月)
  https://research.checkpoint.com/2021/indra-hackers-behind-recent-attacks-on-iran/

水道施設に対するサイバー攻撃 (1/3)

- サイバー攻撃と報じられた2021年2月のOldsmar浄水場(フロリダ州)でのインシデントは事件性がなく操作誤りだったと判明 (3月)
  https://www.wateronline.com/doc/former-official-claims-oldsmar-drinking-water-hack-was-really-operator-error-0001
  - 当時は保安官が記者会見するなど社会的にも大きなニュースとなった

- 上下水道事業者に対するセキュリティ要件を米国EPA(環境保護庁)が3月に提示したものの，10月に撤回
  https://www.epa.gov/waterresilience/cybersecurity-sanitary-surveys
  - EPAの連邦規制が過剰で州の自律性を侵害しているして知事に共和党が就いている州が提訴したことを受けたもの

水道施設に対するサイバー攻撃 (2/3)

- イスラエルの灌漑および下水処理システムの複数のモニターを監視するコントローラーがサイバー攻撃で機能不全に； 詳細不明 (4月)
  https://www.jpost.com/israel-news/article-738790
- イタリアの公営上下水道事業者Alto Calore Servizi SpA社がランサムウェアMesudaに感染； 詳細不明 (5月)
  https://www.isssource.com/ransomware-attack-at-italian-water-supplier/
- 米国Aliquippa(ペンシルバニア州)と北テキサスの水道事業者にサイバー攻撃 (11月)
  https://arstechnica.com/security/2023/11/2-municipal-water-facilities-report-falling-to-hackers-in-separate-breaches/
- パリの下水処理施設にサイバー攻撃 (11月)
  https://www.isssource.com/paris-wastewater-facility-hit-in-cyberattack/
- 親ウクライナの攻撃集団Blackjackがロシアの水道会社を攻撃 (12月)
  https://www.darkreading.com/ics-ot-security/ukrainian-hackers-strike-russian-water-utility

水道施設に対するサイバー攻撃 (3/3)

(米国Aliquippa(ペンシルバニア州)の公営水道事業者の事例)

- 給水対象が数千人の小規模事業者
- 一部地域で水圧を上げるためのポンプを制御するUnitronics社(イスラエル)製のコントローラーをイランの攻撃集団Cyber Av3ngersが攻撃した
  - 初期パスワードのままで，インターネットに直結されていた
  - 人手によって運用を継続し，断水なし
  - 同様の事案が米国内で数件発生

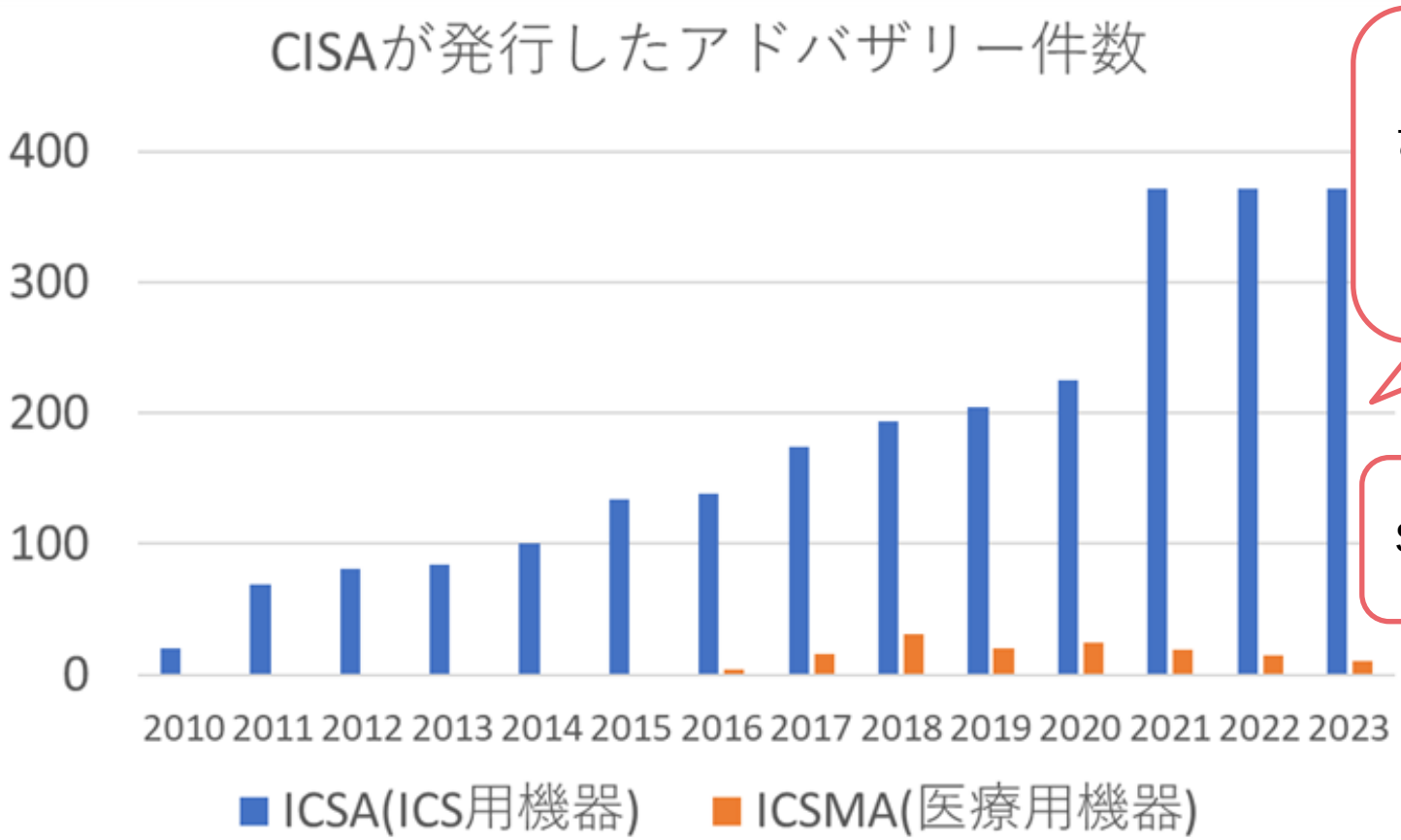
Beaver Countian紙に掲載された
The Municipal Water Authority
of Aliquippaが提供した
スクリーンショット

- アイルランドでも同様の事案；2日間にわたり断水 (12月)
  https://westernpeople.ie/news/hackers-hit-erris-water-in-stance-over-israel_arid-4982.html

- ☞ CISAが公表したICS関連アドバイザリーの件数は前年と同数
- ☞ 継承される脆弱性の課題が残ったまま (SBOMに期待)
- ☞ CVSS第4版公開
- ☞ 機械可読なICS関連アドバイザリーの配布開始

脆弱性の動向

米国ICS-CERTが公表した脆弱性アドバイザリ件数



1年間に公表された脆弱性の件数は2021年以降毎年371件

うち
Siemens社が75件
三菱電機が16件

SynSaber社とICS Advisory Projectによる報告書(上半期)

https://synsaber.com/resources/research-reports/ics-cve-reports/ics-cve-research-first-half-2023/

- CISAが公表したアドバイザリー件数： 185 (前年同期： 205)

- 公表されたCVE件数： 670 (前年同期： 681； 16%減)
- CVEベースで脆弱性の34%に対策なし (前年上期： 13%，下期：35%)
- CVEベースで製造業界には37.3%，エネルギー業界には24.3%の脆弱性の影響が及ぶと見られる
- 脆弱性を数多く発見したのはOEM(56.1%)とセキュリティ企業(28.5%)
- 脆弱性の報告者の居住地は，米国が17人(組織)と最多で，これに日本，イスラエル，中国が次ぐ(いずれも3人(組織))

継承された脆弱性に関する情報

- CODESYS V3 SDKから脆弱性を継承したPLCで遠隔コード実行やDoS攻撃が可能であるとMicrosoft社が報告 (8月)

  https://www.microsoft.com/en-us/security/blog/2023/08/10/multiple-high-severity-vulnerabilities-in-codesys-v3-sdk-could-lead-to-rce-or-dos/
- Log4Jを利用したアプリケーションの約3割が2021年末に公表された脆弱性を今も継承

  https://www.bleepingcomputer.com/news/security/over-30-percent-of-log4j-apps-use-a-vulnerable-version-of-the-library/
- OTとICSにおけるオープンソース利用に関するセキュリティ・ガイダンスをCISA等が公開

  https://www.cisa.gov/news-events/alerts/2023/10/10/cisa-fbi-nsa-and-treasury-release-guidance-oss-itics-environments

継承される脆弱性への対策としてのSBOM関連の動き

- SBOM管理のための推奨事項を米国NSAが公開 (12月)
  https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3617462/nsa-releases-recommendations-to-mitigate-software-supply-chain-risks/
  - 製品提供者と製品利用者の双方に対して
    SBOMを活用するための環境整備に向けた推奨事項を掲げた

- 米国CISAがSBOMのポータルページを開設：
  https://www.cisa.gov/sbom
  - SBOM関連の技術やコミュニティ活動に関する情報など

脆弱性に関連した新技術など

- 脆弱性の深刻度評価指標CVSS (Common Vulnerability Scoring System)の第4.0版をFIRSTが公開 (11月)
  https://www.first.org/newsroom/releases/20231101

- ICS脆弱性に対して，OASIS CSAF (common Security Advisory Framework) 2.0に準拠した機械可読形式のアドバイザリー提供をCISAが追加 (9月)
  https://www.cisa.gov/news-events/news/transforming-vulnerability-management-cisa-adds-oasis-csaf-20-standard-ics-advisories

- ☞ 米国がサイバーセキュリティ戦略を改訂； 製品提供事業者の責任
- ☞ 欧州はNIS2指令の国内法整備を進めサイバー・レジリエンス法策定
- ☞ 経営陣にセキュリティ状況開示を求める米国SECの新規則が発効
- ☞ IEC 62443やNISTのOT関連標準の整備が進んだ
- ☞ MITRE社のATT&CK第14版に
- ☞ 米国FERCが電力業界の規制の追加に向けて動く

標準の整備と規制の強化

欧米の政府の動き

製品提供事業者の責務を強調

- 米国バイデン政権が国家サイバーセキュリティ戦略を公表 (3月)
  https://www.securityweek.com/fda-announces-new-cybersecurity-requirements-for-medical-devices/
- 米国SECがサイバーセキュリティ・リスク管理規則を発行 (9月)
  https://www.sec.gov/files/rules/final/2023/33-11216.pdf
  — サイバーインシデント時に4営業日以内の報告義務等 (12月18日発効)

- 欧州ではNIS 2指令(2021年11月採択)対応の国内法整備へ (期限：2024年10月17日)
  https://www.nis-2-directive.com/
- 欧州のサイバー・レジリエンス法が固まり公式承認手続きを残すのみ
  https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6168
  — IoT機器の脆弱性の情報開示や修正などを義務化(2027年以降)

個人向け機器が対象で
ICSは対象外か(？)

注 SEC： Securities and Exchange Commission
NIS： Network and Information Security

米国SECのサイバーセキュリティ・リスク管理規則

「サイバーセキュリティ・リスク管理・戦略・統治・インシデント管理」

https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214

https://www.federalregister.gov/documents/2023/08/04/2023-16194/cybersecurity-risk-management-strategy-governance-and-incident-disclosure

- 7月に採択され，9月に発行，12月から順次施行
- 投資家がリスクを適切に認識するための情報開示を義務化
  - リスク管理と戦略を定期的に開示
  - 経営陣によるサイバーリスクの管理と経営陣の役割を開示
  - 物的なサイバーセキュリティ・インシデントを4営業日以内に開示
- インシデント情報開示により社会または他社にリスクが生じる場合に開示を延期するためのガイドをFBIが公開 (12月)

  https://www.fbi.gov/investigate/cyber/fbi-guidance-to-victims-of-cyber-incidents-on-sec-reporting-requirements

IEC 62443シリーズ標準の策定の進展

次の2文書が2023年に新たに発行された

- IEC TS 62443-1-5:2023
  Part 1-5: IEC 62443セキュリティ・プロファイルのためのスキーム
  (Scheme for IEC 62443 security profiles)

- IEC 62443-2-4:2023
  Part 2-4: IACSサービス事業者に対するセキュリティ・プログラム要件
  (Security program requirements for IACS service providers)

注 IEC： International Electrotechnical Commission
IACS： Industrial Automation and Control Systems

JPCERT/CCでは，IEC 62443シリーズに書かれているセキュリティに関する鍵となる概念を「標準から学ぶICSセキュリティ」と題して連載の読み物にまとめて公開しています．
https://www.jpcert.or.jp/ics/information07.html

その他のセキュリティ標準

- 米国NIST(標準技術局)が「サイバー・セキュリティ・フレームワーク」第2版の草案を公開 (8月；11月までコメント募集)
  https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd

- 米国NISTがSP800-82「OTセキュリティへのガイド」第3版を公開 (9月)
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

注 NIST： National Institute of Standards and Technology

MITRE社によるATT&CKの改訂

https://attack.mitre.org/

- ATT&CKは，実世界で展開されているサイバー攻撃に関する概念や手法，攻撃集団などを集めたオンライン事典；MITRE社が管理
  - ドメイン(分野)として，「企業」と「ICS」，モバイルが設定さえており各ドメインに沿ってまとめられている

- ほぼ半年ごとに改訂されており，直近では10月に第14版を公開
  https://medium.com/mitre-attack/attack-v14-fa473603f86b
  - 第14版では，PLCやRTUなど14のICS用資産の項目が追加された

米国の電力業界の規制の動向

(FERC(連邦電力規制理事会)によるCIP標準の動き)

- 内部ネットワークのセキュリティ監視(INSM)を義務づけるCIPの追加または改訂を半年以内に行うようNERCに指示 (2月)
  https://www.federalregister.gov/documents/2023/02/09/2023-01453/internal-network-security-monitoring-for-high-and-medium-impact-bulk-electric-system-cyber-systems
  - 高インパクトなBESサイバーシステムと，中インパクトだが外部ルータブルな接続性をもつBESサイバーシステムを監視対象とする

- CIP-003-9(サイバーセキュリティ管理対策)を承認
  https://www.ferc.gov/media/e-1-rd23-3-000
  - サプライチェーン･リスク管理を低インパクトなBESサイバーシステムにも適用することを義務付ける

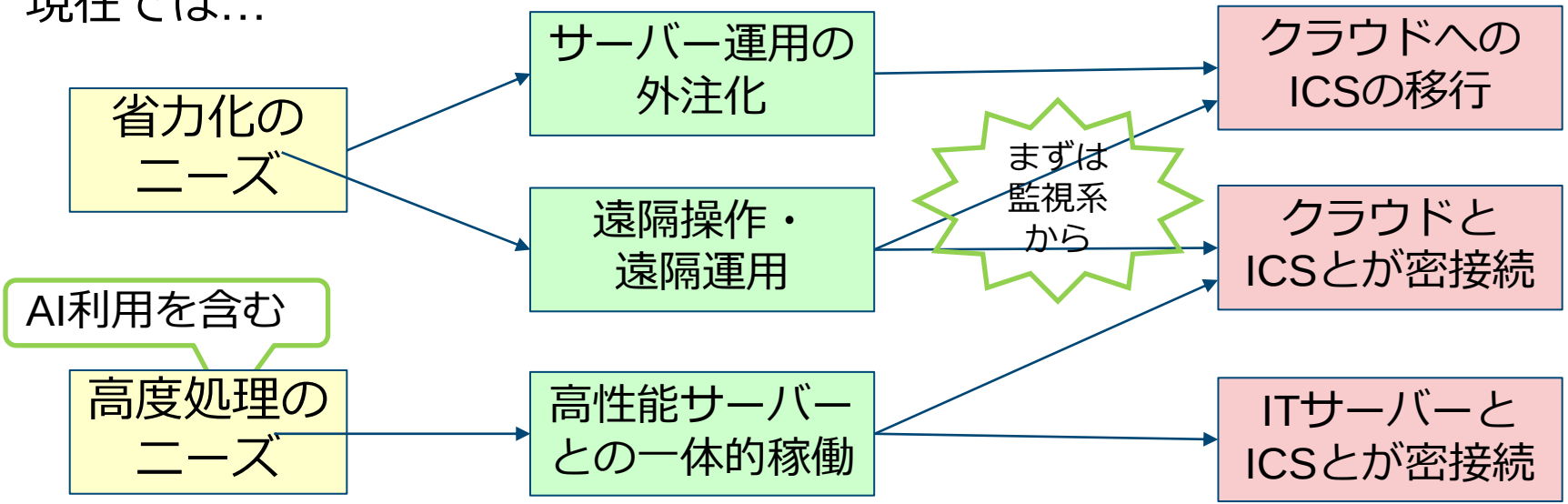
- ☞ ICSのクラウドへの移行とセキュリティ
- ☞ OTの遠隔操作・遠隔運用とセキュリティ
- ☞ OTにおけるAI利用とセキュリティ

新しい技術を採用して変貌するICSのセキュリティ

変貌し始めたICS；そのセキュリティは？

20年前のICSは他のシステムから切り離され単独で動作していた

現在では…



ICS独自のアプリケーションを
ITと共通化されたネットワークやサーバー上で稼働させる形態へ

ICSのクラウドへの移行とセキュリティ

注　BES： Bulk Electric System

- NERC(北米電力事業者協会)が白書「クラウド上でのBES(基幹電力網)運用」を公開 (9月)

注 NERC： North American Electric Reliability Corporation

https://www.nerc.com/comm/RSTC_Reliability_Guidelines/SITES_WhitePaper_BES_Ops_in_Cloud.pdf

  - 技術および運用責任のモデルと概念的セキュリティ課題を整理
- ICS網をクラウド上に移行する方法についてISAがブログ記事 (1月)
  - #1 RTOS
    https://blog.isa.org/how-to-migrate-ics-networks-to-the-cloud-1-rtos
  - #2 エッジ･コンピューティング
    https://blog.isa.org/how-to-migrate-ics-networks-to-the-cloud-2-edge-computing
- クラウド上に移行したICSのセキュリティについてDarkTrace社がブログ記事 (2024年1月)

https://darktrace.com/blog/how-industrial-control-systems-can-be-secure-in-the-cloud

OTの遠隔操作・遠隔運用とセキュリティ

- 産業用遠隔アクセスの現状についてCylo社がTakePointResearch社に委託してまとめた調査報告書を公表 (5月)
  https://info.cyolo.io/the-state-of-industrial-secure-remote-access-research-report
  - 遠隔アクセスに高い需要
    (多くの組織で11人以上の利用者；大企業では50人以上も)
  - APTの攻撃界面として最大
  - 利用組織も強い不安感(可視性，教育訓練，アクセス制御の強度)

- 遠隔アクセスのセキュア化ガイドを米国CISA等が公開 (6月)
  https://www.cisa.gov/news-events/alerts/2023/06/06/cisa-and-partners-release-joint-guide-securing-remote-access-software

AIとセキュリティ

- AI利用がサイバーセキュリティに及ぼす影響をKaspersky社が論じた(12月)
  https://securelist.com/story-of-the-year-2023-ai-impact-on-cybersecurity/111341/
  - AIを利用するための環境に起因する脆弱性
    - クラウドへの接続に伴う脆弱性
    - クラウド自体が持ちうる脆弱性
  - 利用するAI自体がもちうる脆弱性
    - LLM固有の脆弱性など
  - 攻撃者がAIを利用することによる影響
    - なりすましの見分けが難しくなる
    - スキルの低い攻撃者でもマルウェアなどの攻撃ツールを合成

OTにおけるAI利用に
限った問題ではないが

まとめ

- ☞ ランサムウェアの脅威が高止まり；製造業界が狙われている
- ☞ 戦争に伴う地政学的インシデントが頻発
- ☞ 上下水道へのサイバー攻撃が関心を引いた
- ☞ 前年と同数の脆弱性アドバイザリー；残る脆弱性継承の課題
- ☞ セキュリティ標準とセキュリティ規制の整備が続いている
- ☞ 新技術を取り込んで変容するICS；そのセキュリティも要検討

2023年に公開された注目すべきICSセキュリティ動向の報告書

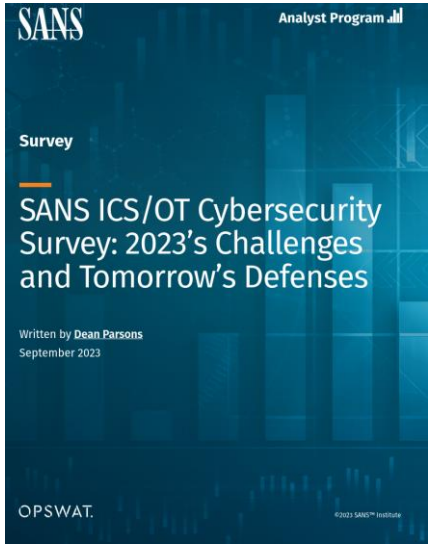
- ☞ SANS ICSのアンケート調査
- ☞ アンケート調査「産業サイバーセキュリティの現状」
- ☞ OT網の最下層における水平移動
- ☞産業セキュリティ・インシデントの分析

SANS ICSのアンケート調査 (OPSWAT社後援)

SANS ICS/OT Cybersecurity Survey: 2023's Challenges and Tomorrow's Defenses (9月)

https://info.opswat.com/sans-predictions-2024

- 世界中のICS関係者約700人へのアンケート調査(毎年実施)
- ICSセキュリティ対策で重要なのは，1) ネットワーク可視性，2) リスク評価，3) ICSに侵入した脅威の検知
- ICSが侵害された契機は，IT網への侵害(38.4%)，エンジニアリングWS侵害(30.2%)，外部遠隔サービス(24.8%)，インターネット･アクセス可能なアプリケーションへの攻撃(23.3%)など



アンケート調査「産業サイバーセキュリティの現状」 (Claroty社)

Survey Report： The Global State of Industrial Cybersecurity 2023:
New Technologies, Persistent Threats, and Maturing Defenses (12月)

https://web-assets.claroty.com/claroty-industrial-survey-report-dec-2023.pdf

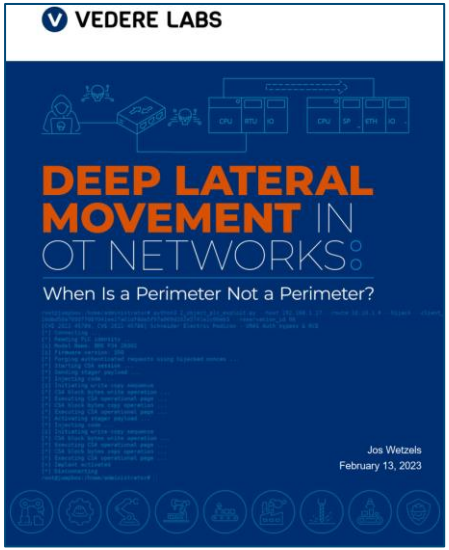
- ランサムェアによるOT環境の侵害が高止まり
  (IT環境だけを侵害： 21%，ITとOTの双方の環境を侵害：37%)
- ランサムウェアの活発化に伴いサイバー保険金請求が急増
  (回答者の67%がランサムウェア攻撃を経験；80%がサイバー保険契約)
- 業界の規制と標準がOTサイバーセキュリティ投資を促している
- 生成AIへの関心が高く，それに伴い
  セキュリティ懸念が高まっている
- 対策の進展で，未対処のセキュリティ・
  リスクが減少

OT網の最下層における水平移動 （ForeScout社VedereLabs)

Deep Lateral Movement in OT Networks: When Is a Perimeter Not a Perimeter? (2月)

https://www.forescout.com/blog/deep-lateral-movement-in-ot-networks-when-is-a-perimeter-not-a-perimeter/

https://www.forescout.com/resources/l1-lateral-movement-report



- OT網の第1層に設置された機器(PLC等)間で攻撃者が水平移動できることを実証
- Schneider社製PLCで構成された網を実験台とし同PLCの脆弱性を利用して水平移動を実現

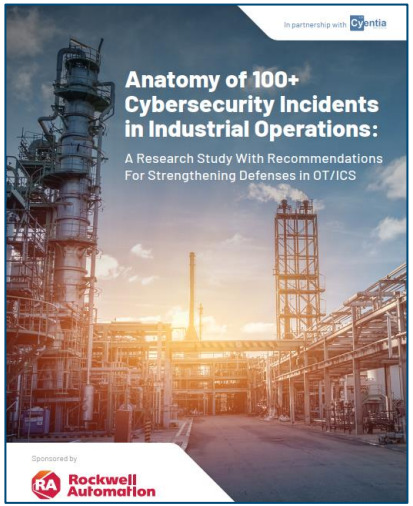
産業セキュリティ・インシデントの分析 (Rockwell社他)

Anatomy of 100+ Cybersecurity Incidents in Industrial Operations (9月)

https://therecord.media/cyber-insurance-claims-spike-as-ransomware-soars

https://www.rockwellautomation.com/en-us/campaigns/cyentiareport.html

- 1982～2022年の122件のOTセキュリティ・インシデントを分析
- エネルギー業界(39%)や重要製造業(11%)，運輸(10%)が狙われた
- 最も多い攻撃法はフィッシング攻撃
- システム内で狙われたのはSCADAシステム(53%)，PLC(22%)
- 脅威活動分子の80%が外部組織員だが，組織内の者が意図せず加担していることも
- 攻撃目的は操業の混乱(60%)，アクセスやデータ流出(40%)；サプライチェーンまで影響が及ぶケースが65%



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