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 ～

2025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. 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. セキュリティ対策としての保険
8. 新技術に伴って浮上するセキュリティ課題

(本資料中の年の表記のない月日は2024年の日付を表しています)

サイバーセキュリティ状況の展望

[参考] World Economic Forum: Global Cybersecurity Outlook 2025 (2025年1月13日)
https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

- 地政学的な緊張の高まり；
  続くウクライナ戦争，米中貿易戦争，イスラエルと中東イスラム諸国との紛争
- サイバー犯罪の高度化；法執行機関とランサムウェア集団との攻防
- サイバー攻撃に狙われるサプライチェーンと相互依存性
- セキュリティ規制が強化され広範囲に適用される
- AIをはじめとする新技術の急速な導入； ITとOTとの融合
- サイバー･スキル不足； OTでは熟練技能者の引退

- ☞ 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
- ☞ 曖昧で形骸化しつつあるインシデント報告

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30～35件のインシデント報告
- 半数前後がランサムウェア攻撃によるもの
- 攻撃を受けた組織の2/3が製造業(自動車，航空宇宙，医薬品，食品飲料，衣料，化粧品など)
- 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
- 米国とドイツの組織からの報告が概して多く，四半期ごとに欧州や南米諸国や豪州が加わる (日本国内からの報告はごく少数と見られる)

産業組織に対するサイバー攻撃の動向

[参考]

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

- Q1 2024 (6月3日)
  https://ics-cert.kaspersky.com/publications/reports/2024/06/03/q1-2024-a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity/

- Q2 2024 (11月8日)
  https://ics-cert.kaspersky.com/publications/reports/2024/11/08/q2-2024-a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity/

Kaspersky社ICS CERTのAPT and financial attacks on industrial organizations

- Q3 2024 (12月26日)
  https://ics-cert.kaspersky.com/publications/reports/2024/12/26/apt-and-financial-attackson-industrial-organizationsin-q3-2024/

分かりにくくなったインシデント報告

- ICSに攻撃が及んでいなくても停止される事例が多い
  - OTとITとの連携が緊密化していることを反映(？)

- 報告の多数を占める米国でのインシデント報告義務
  - 証券取引委員会(SEC)への報告
    - 2023年12月から順次実施
    - 企業のリスクを株主向けに速やかに開示することが狙い
    - 「模範的報告書」をコピペしたような報告が多く技術的な内容が薄い
  - 2022年重要インフラ向けサイバーインシデント報告法(CIRCIA)に基づくCISAへの報告
    - 報告の方法と内容についての詳細をCISAが策定中

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

- 報告の要件案をCISAが公表しコメントを募集 (2024年4月4日)
  https://www.federalregister.gov/documents/2024/05/06/2024-09505/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements-extension-of
  - 集まったコメントへの対応計画を公表(2024年12月16日)
    https://www.cisa.gov/news-events/news/cisa-publishes-draft-national-cyber-incident-response-plan-public-comment
  - 最終要件(原案公表から1.5年以内)が決まると発効

報告書の品質向上が期待される

☞ 一部の攻撃集団に法執行機関が国際的な粉砕作戦実施
☞ 個々の攻撃集団の盛衰があるが相対的には攻撃活動が高止まり

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

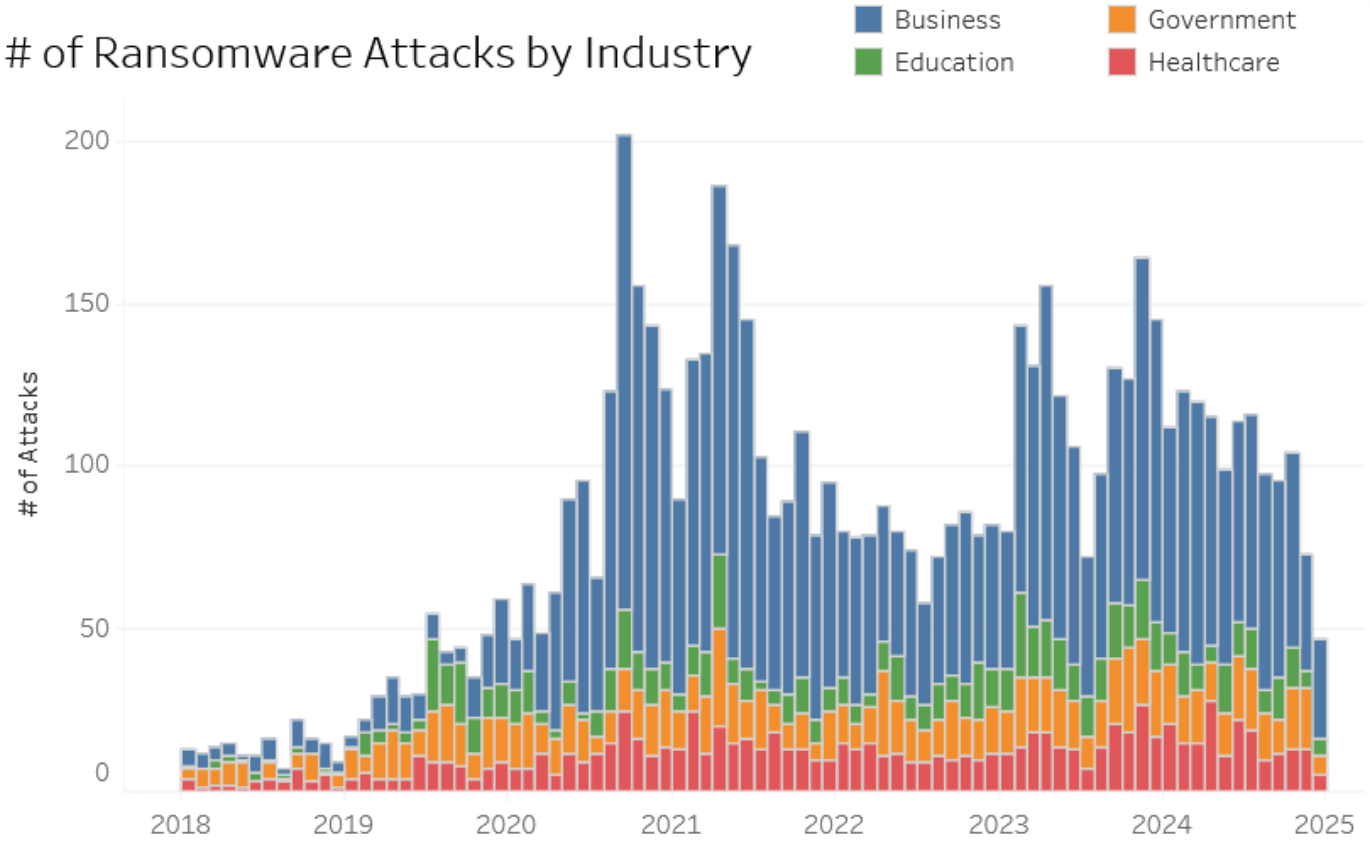
ITとOTの双方を含んだ集計値

[出典] CompariTech社の報告書(2025年1月9日)
https://www.comparitech.com/news/ransomware-roundup-2024-end-of-year-report/

- 攻撃件数： 5,461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142件
  - 前年(2023年)の確認件数は1,474件
    (公表までの時間的な遅れがあり，2024年も最終的には同水準か)

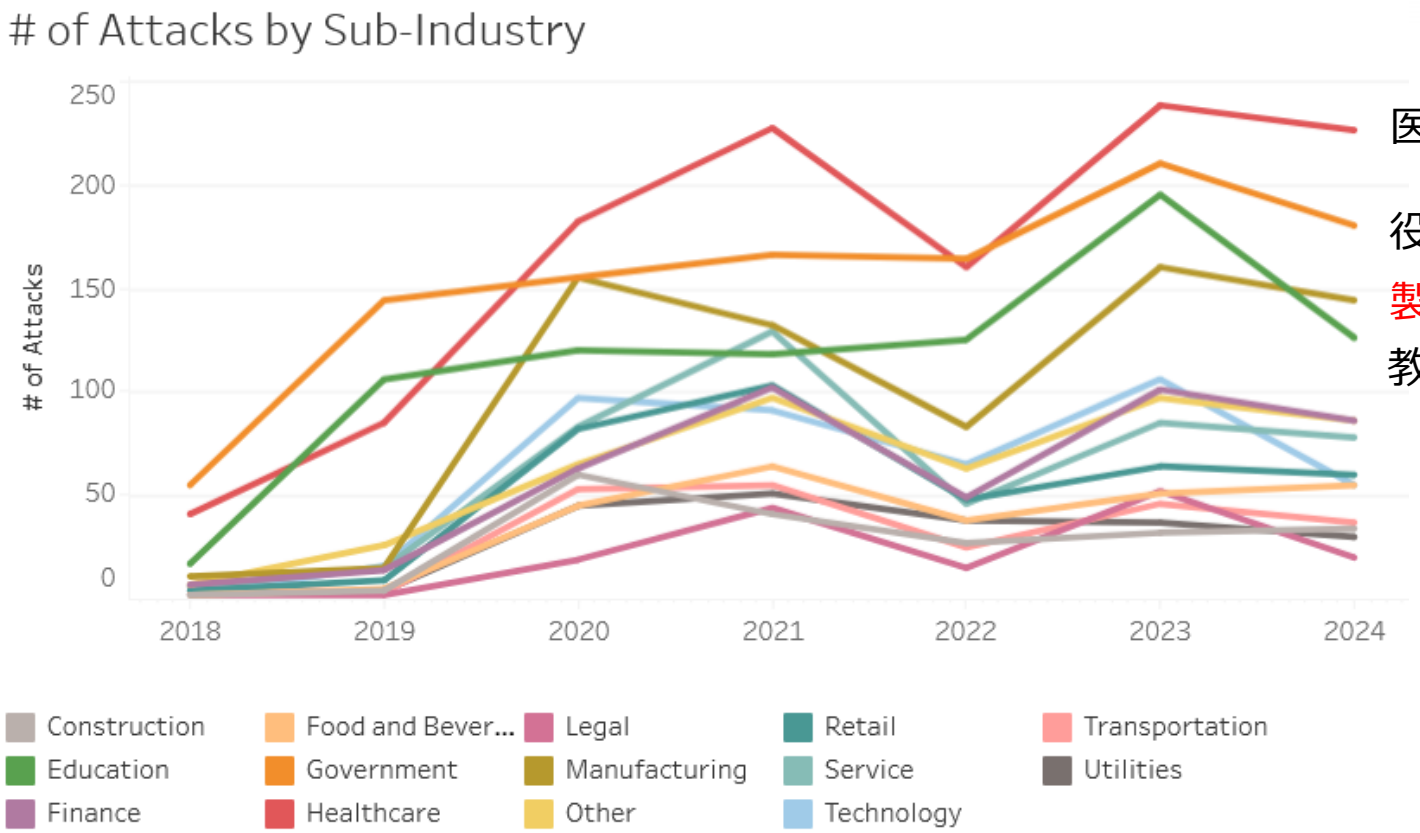
- 身代金の平均金額： 350万ドル以上(要求額)，953万ドル(支払額)
  身代金の支払い総額が1.335億ドル
- 活動が活発だった攻撃集団：
  RansomHub(89件)，LockBit(83件)，Medusa(62件)，Play(57件)，…

ランサムウェア攻撃件数の推移



[出典]
CompariTech社
https://www.comparitech.com/blog/information-security/global-ransomware-attacks/

ランサムウェアの狙い目は医療，役所，製造業，教育機関



医療機関

役所

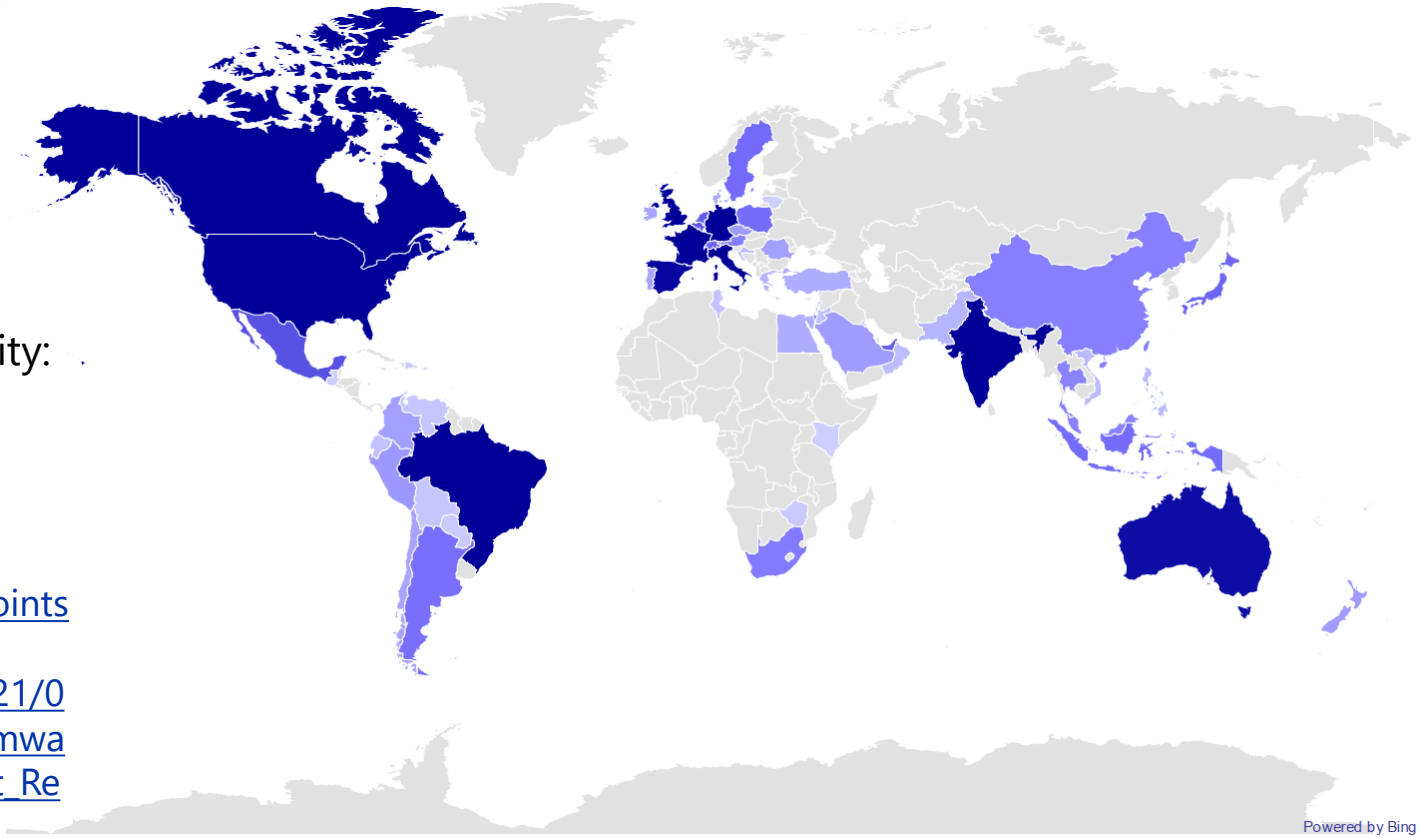
製造業

教育機関

[出典]
CompariTech社
https://www.comparitech.com/blog/information-security/global-ransomware-attacks/

被害は主として欧米だが日本でも

[出典]
Guide Point Security:
GRIT 2025
Ransomware &
Cyber Threat
Report
https://www.guidepointsecurity.com/wp-content/uploads/2021/07/GRIT_2025_Ransomware_and_Cyber_Threat_Report.pdf



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/

ランサムウェアに関連するその他の報告

- Temple大学のランサムウェア攻撃DBの収納事案総数が２千件を超す
  Critical Infrastructure Ransomware Attacks (CIRA)
  https://sites.temple.edu/care/cira/

  2019年9月構築開始

- 攻撃ツール開発にAIを利用するランサムウェア集団も出現
  FunkSec – Alleged Top Ransomware Group Powered by AI (CheckPoint社)
  https://research.checkpoint.com/2025/funksec-alleged-top-ransomware-group-powered-by-ai/

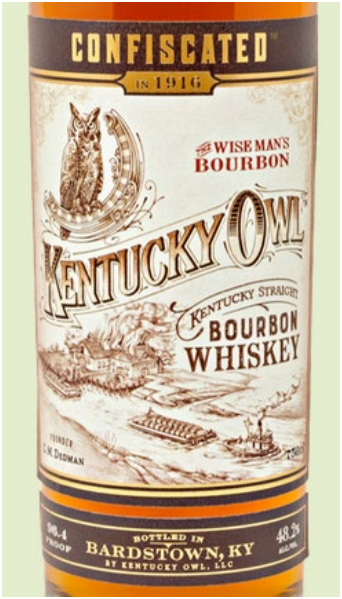
- 被害は金銭だけでなく関係者の心に大きな傷：英国では自殺者も
  The Scourge of Ransomware Victim Insights on Harms to Individuals, Organisations and Society (RoyalUnitedServicesInstitute報告書)
  https://static.rusi.org/ransomware-harms-op-january-2024.pdf

[事例] ランサムウェア攻撃を受けて破産

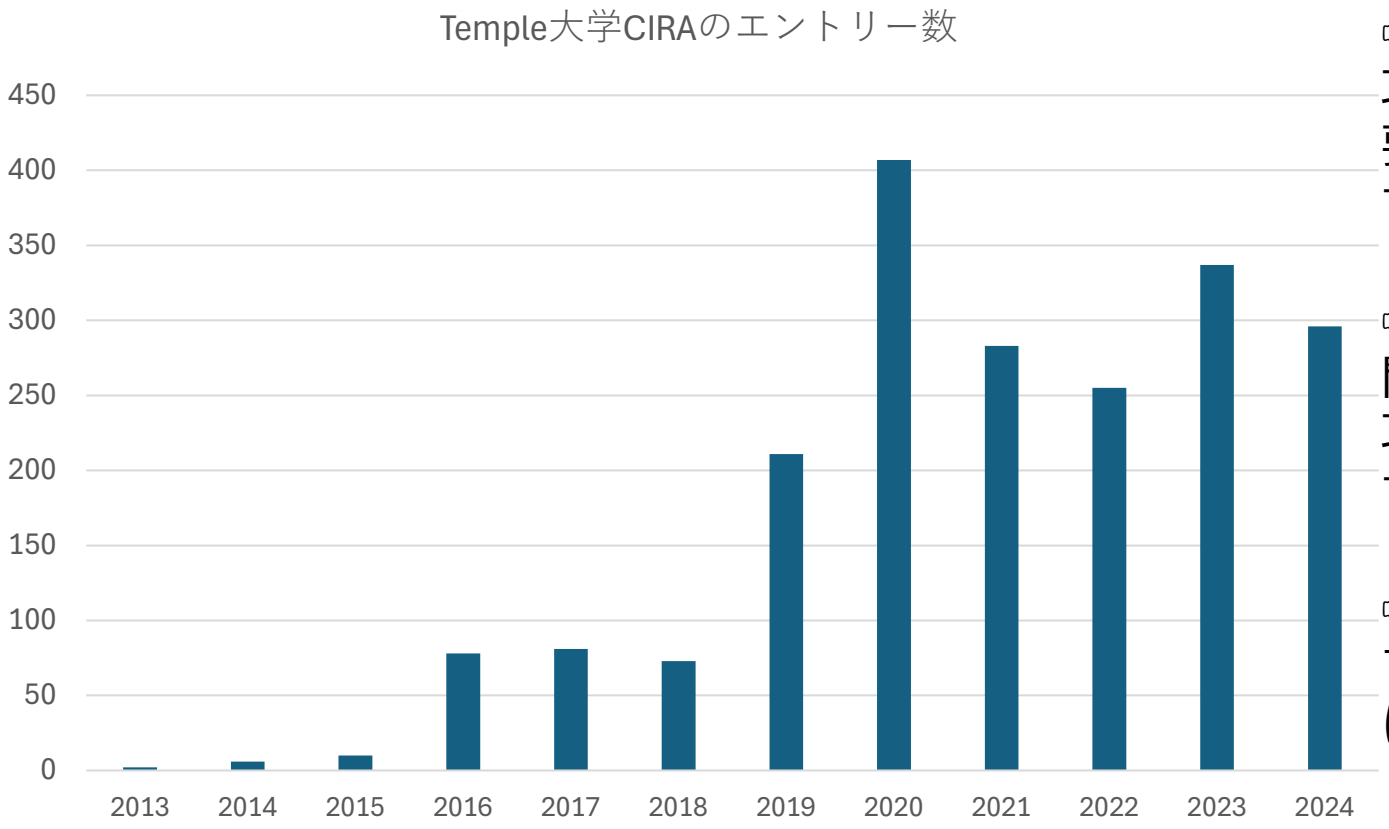
- 多国籍アルコール飲料メーカーのStoliグループの米国子会社が8月にランサムウェア攻撃を受けた (攻撃集団は不明)

- ERPの復旧が2025年第1四半期までかかる
  顧客情報も流出

- 11月29日に破産を申請
  コロナ禍やインフレに伴う需要低迷に加えて
  2022年3月に2つのロシア国内醸造所が没収されて
  財務状況が悪化していた中で
  ランサムウェア被害が決定的な打撃となった



重要インフラに対するランサムウェア攻撃件数の推移



☞ ランサムウェア攻撃の1/4前後が重要インフラを狙っている

☞ 2020年以降は年間に250～400件の攻撃の報告が続いている

☞ 重要インフラのすべてがICS関連とは言えないが…

- ☞ ウクライナの熱供給システムの運用を妨害
- ☞ CyberAv3ngersが燃料管理システムを狙う
- ☞ エンジニアリング・ワークステーションが感染するマルウェア

ICSを狙って作られた マルウェアの動向

マルウェア"FrostyGoop"

https://hub.dragos.com/hubfs/Reports/Dragos-FrostyGoop-ICS-Malware-Intel-Brief-0724_r2.pdf

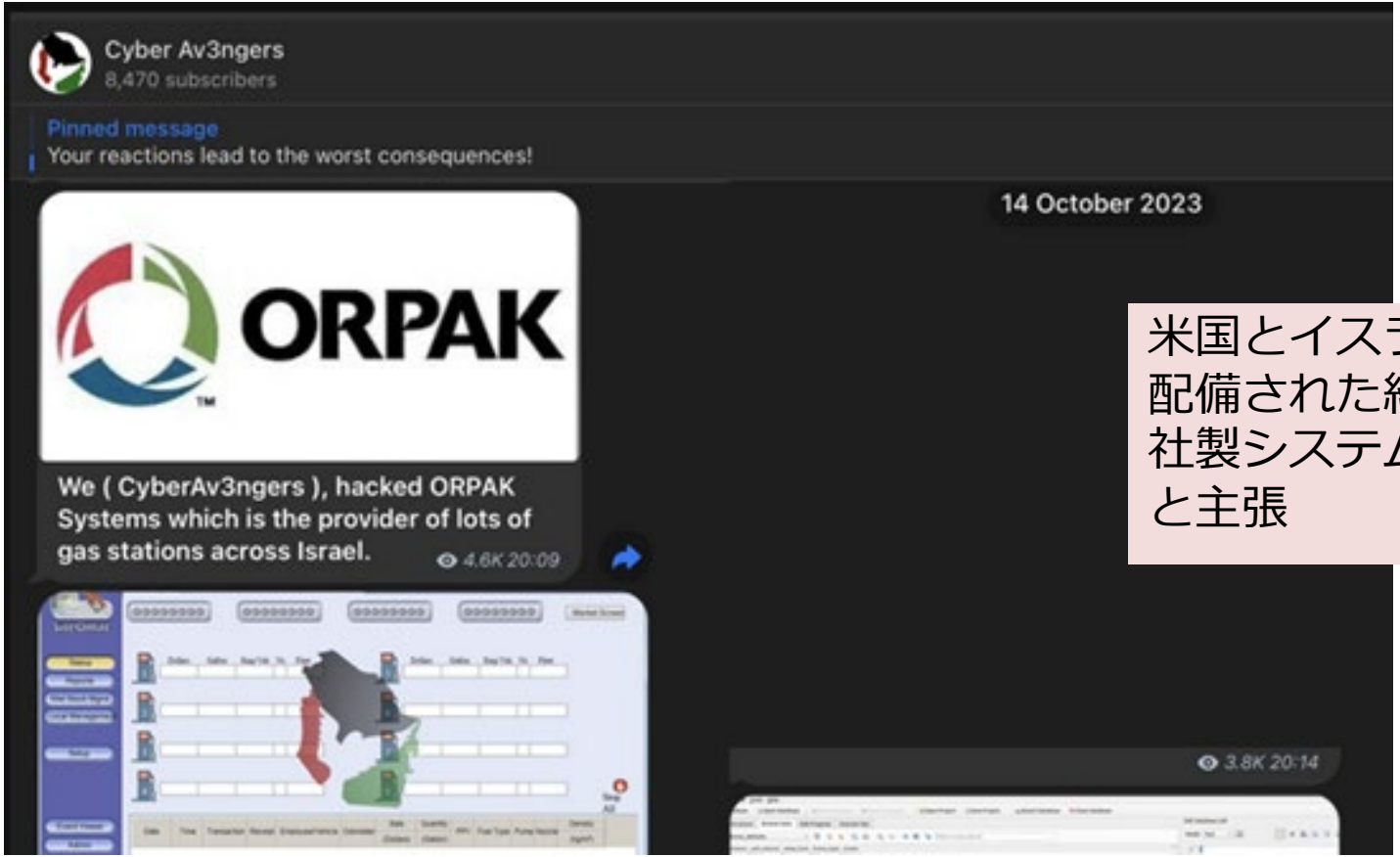
- Dragos社が2024年4月に発見し7月に報告；ICSマルウェアでは9番目
- Modbus TCPプロトコルでICSと直接通信できる
- 2023年にウクライナ西部の地域エネルギー企業の攻撃に使われ
  2日間熱供給が停止
  (Dragos社はウクライナのCSSCからの情報として「500棟のアパートの建物が影響を受けた」と書いているが「アパート建物の500戸」と考える方が合理的だと専門家がコメントしている)

マルウェア"IOcontrol"

https://claroty.com/team82/research/inside-a-new-ot-iot-cyber-weapon-iocontrol

- Claroty社がVirusTotalから検体を入手して分析し12月10日に報告
- 検体は米国内の燃料管理システムから採取された
- 開発者はイラン系の攻撃集団CyberAv3ngersで，
  米国とイスラエルを狙っている，と推測されている
- LinuxベースのIoTやOT機器を攻撃でき，
  カスタマイズが容易なモジュラーな構成をもつ
- MQTTプロトコルを介してC2サーバーと通信

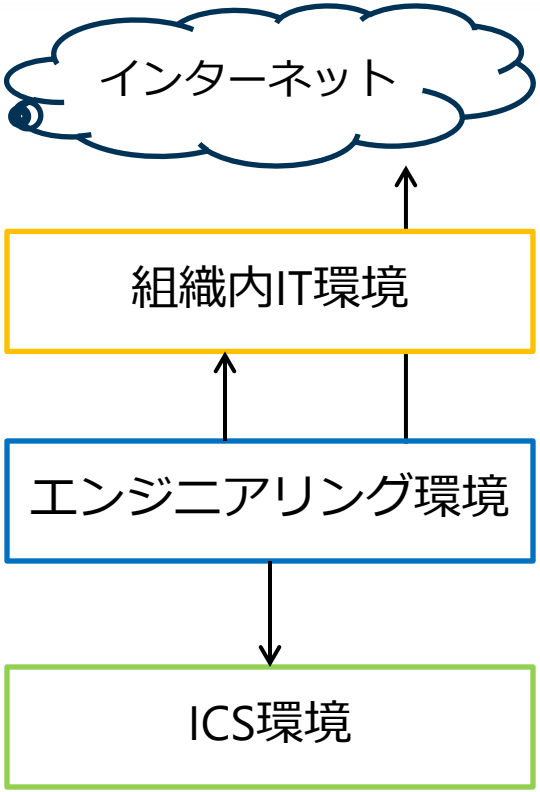
IOcontrolを使ったCyber Av3ngersの攻撃の声明



米国とイスラエル国内に配備された約200のOrpak社製システムを攻撃したと主張

[出典]
Claroty社報告書

ICS攻撃の踏み台となるエンジニアリング環境への注目



- エンジニアリング環境からICS環境にもインターネット環境にもアクセス可能
  - ICSには特権的なアクセスも可能
- ICS環境と比べて豊かなCPU資源がある

☞ ICS攻撃の踏み台としてエンジニアリング環境が利用されることが懸念される

ICS用エンジニアリング・ワークステーションの感染

ForeScout社が12月17日に報告： ICS Threat Analysis: New, Experimental Malware Can Kill Engineering Processes (Fore Scout)
https://www.forescout.com/blog/ics-threat-analysis-new-experimental-malware-can-kill-engineering-processes/

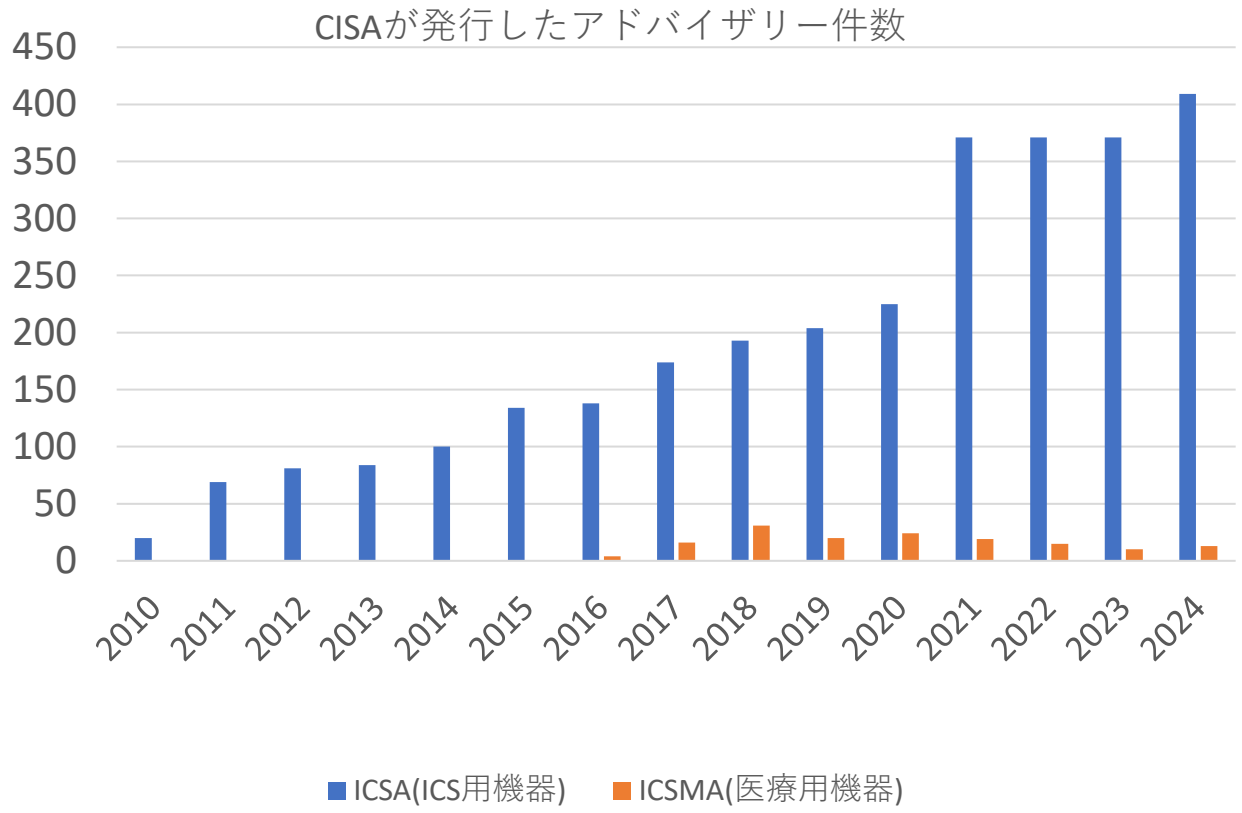
- ICSのエンジニアリング・ワークステーションの感染は珍しくない
  - 多くの場合，インターネットにもICSにもアクセスが可能
  - ICSのインシデントの2割程度がエンジニアリング・ワークステーションで発生
  - 安全計装システムを攻撃したマルウェアHatManの例も

- 三菱電機製GX WorksにRamnit(バンキング・トロイの木馬)への感染事例
  - 偶発的な感染なのか意図的な攻撃なのか不明
- Chaya_003はSiemens TIAポータル・プロセスを終了させるコードを含む

- ☞ 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
- ☞ SBOM関連の活動が続く

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



・ 前年から約1割増加し409件に

・ うち，Siemens社が150件，Rockwell Automations社が55件

・ IT製品を含めた脆弱性の全体はCVEベースで40,704件だった

継承される脆弱性に対する対策としてのSBOMの活用へ

- 経済産業省から「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引ver2.0」 (8月29日)
  https://www.meti.go.jp/press/2024/08/20240829001/20240829001.html

- CISAがSBOMのポータルページを提供
  https://www.cisa.gov/sbom
  — SBOM関係者のコミュニティを醸成

- ☞ 欧州はNIS2指令の国内法整備期限を迎えたが…
- ☞ 欧州でサイバー・レジリエンス法(CRA)が発効
- ☞ 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

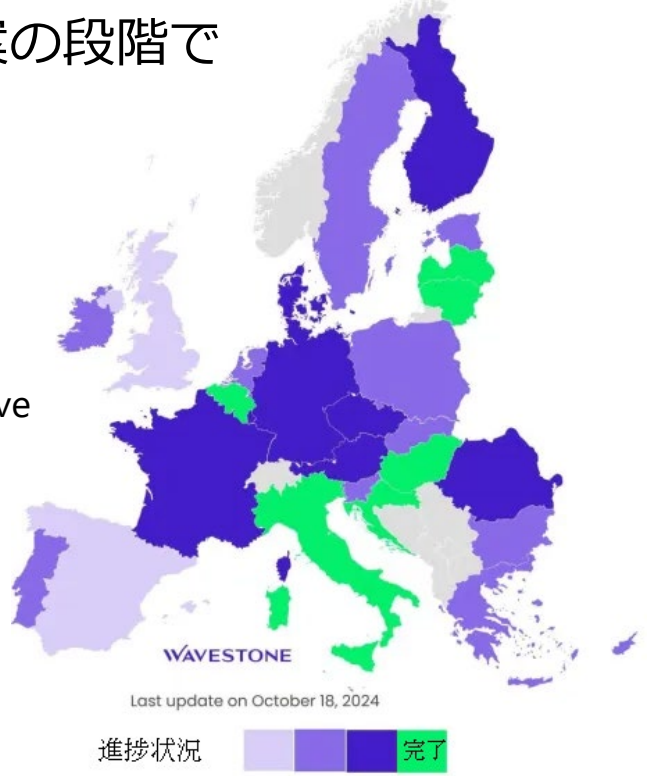
- 2024年10月17日までに対応する国内法を整備することになっていた(加盟各国の義務)

欧州のNIS-2指令の国内法の整備が多くの国で間に合わず

- 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
  - ドイツなど主要国を含む大多数がなお草案の段階で2025年にずれ込んでいる

[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/
JPCERT/CCで一部変更

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

欧州でサイバー・レジリエンス法(CRA： Cyber Resilience Act)

規制(EU) 2024/2847

[法文] https://eur-lex.europa.eu/eli/reg/2024/2847

[広報発表] https://digital-strategy.ec.europa.eu/en/news/cyber-resilience-act-enters-force-make-europes-cyberspace-safer-and-more-secure

- ネットワークに接続して利用される，デジタル要素を搭載した製品のセキュリティ水準を担保する
  - 製造事業者が規制対象
  - 製品が備えるべきセキュリティ要件や製品提供条件を定める
- 2024年12月10日に発効
  - CRAの主な義務規定は2027年12月11日から適用

脆弱性の報告義務は
2026年9月11日から

CRAにおける製品の分類

製品の分類	説明	製品例
重要製品 クラス1	セキュリティ上重要な機能を提供または多数の製品に重大な影響を与える機能を提供する製品 (付録Ⅲ)	ブラウザー OS
重要製品 クラス2	重要なセキュリティ機能を提供し，かつ，本分類に属す他の製品に重大な影響を与える製品 (付録Ⅲ)	ハイパーバイザー ファイアウォール
重大製品	製品が侵害されるサプライチェーンを通じてEU全体に甚大な混乱を招くような製品 (付録Ⅳ)	スマートメーターGW スマートカード
その他	上記の3分類以外の製品	スマートフォン パソコン

ICSコンポーネントはここに分類

欧州で発効する予定のその他の規制

EU AI法

Regulation (EU) 2024/1689 (Artificial Intelligence Act)
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689#enc_1

- AIの運用者や提供者，輸入事業者，小売り事業者を規制
- 2025年8月2日から完全施行； 高リスクAIモデル規制は2027年8月2日

EU製造物責任指令

Directive (2024/2853) on liability for defective products and repealing
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402853#enc_1

- 2026年12月9日までに国内法で実現することを加盟国に義務付け
- ソフトウェアを含むデジタル製品も適用範囲になる

IEC 62443-2-1の改定版 (第2版)が発行された

IEC 62443-2-1 Ed. 2.0:2024 (b)
産業用オートメーション及び制御システムのセキュリティ－第2-1部：IACS アセットオーナーのためのセキュリティプログラム要求事項

Security for industrial automation and control systems - Part 2-1: Security program requirements for IACS asset owners

https://webdesk.jsa.or.jp/books/W11M0090/index/?bunsyo_id=IEC+62443-2-1+Ed.+2.0%3A2024

- 初版(2010年)を改定
- 8月7日に発行； 日本規格協会からは邦訳版も
- ISAからの発表は2025年1月28日

  Update to ISA/IEC 62443 Standards Addresses Organization-Wide Cybersecurity in Industrial and Critical Infrastructure Operations
  https://www.isa.org/news-press-releases/2025/january/update-to-isa-iec-62443-standards-addresses-organi

IEC 62443-2-1の改定 (目次主要部分の比較)

2024年版の目次

1. 適用範囲
2. 標準参照
3. 用語と定義，略語，頭文字，慣行
4. 概念
5. 準拠と評価
6. SPE1 – 組織的セキュリティ対策
7. SPE2 – 設定管理
8. SPE3 – ネットワーク通信セキュリティ
9. SPE4 – コンポーネント･セキュリティ
10. SPE5 – データ保護
11. SPE6 – 利用者アクセス管理
12. SPE7 – イベント･インシデント管理
13. SPE8 – システムの完全性と可用性

2010年版の目次

1. 適用範囲
2. 標準参照
3. 用語と定義，略語，頭文字，慣行
4. サイバーセキュリティ管理システムの要素
   - 4.1 概要
   - 4.2 カテゴリー： リスク分析
   - 4.3 カテゴリー： CSMSによるリスク対処
   - 4.4 カテゴリー： CSMSの監視と改善

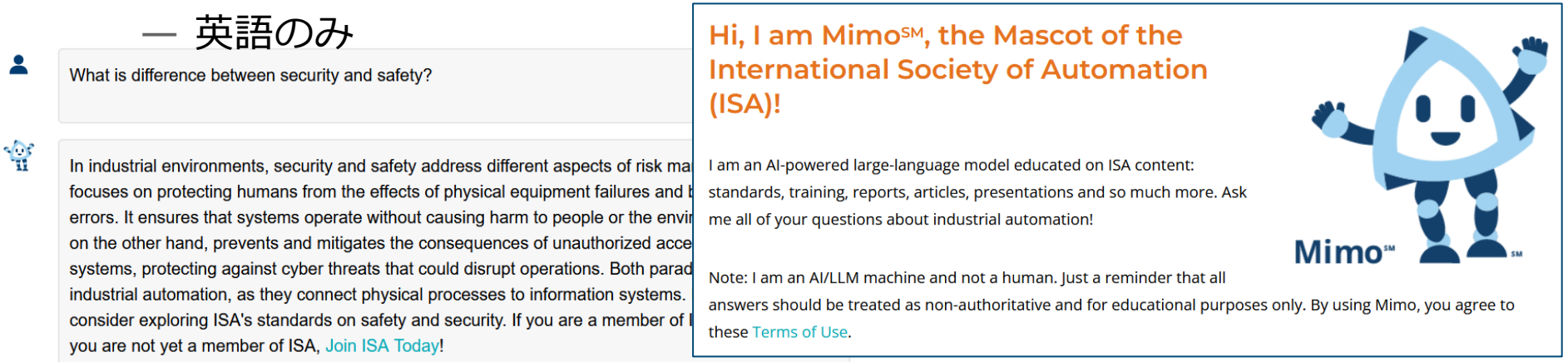
SPE： Security Program Element
CSMS： Cyber Security Management System

[参考] JEMIMA会報2024年10月号
委員会活動報告2
https://www.jemima.or.jp/about/file/jemima_report_202404.pdf

ISAがMIMOを公開

ISA Launches an AI-Powered Large-Language Model Trained on ISA Content (7月11日)
https://www.isa.org/news-press-releases/2024/july/isa-launches-an-ai-powered-large-language-model-tr

- MIMO： ISAの標準や訓練，技術報告書を学習した
  ISAが提供するチャットボット(LLM)
  https://www.isa.org/mimo
  - サインアップしてログイン利用 (ISA会員(会費あり)以外はクエリ数に制限)
  - 英語のみ



米国CISAからの主な公開文書

- (2025年1月13日) 要求によるセキュリティ： OTの保有者と運用者がデジタル製品の選定時に配慮すべき優先事項
  https://www.cisa.gov/sites/default/files/2025-01/joint-guide-secure-by-demand-priority-considerations-for-ot-owners-and-operators-508c_0.pdf

1. 設定管理
2. ベースライン製品のロギング
3. オープンな標準
4. 自律性を担保する製品所有
5. データの保護
6. デフォールトによるセキュリティ
7. セキュアな通信
8. セキュアな管理
9. 強力な利用者認証
10. 脅威モデリング
11. 脆弱性管理
12. アップグレードとパッチ用ツール

調達要件をまとめる際の参考になりそう

米国CISAからの主な公開文書

- (2月23日) 水システムのセキュア化のためのサイバー行動

  Updated: Top Cyber Actions for Securing Water Systems
  https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems

- (9月25日) 誰もができる方法によるOT/ICSへの攻撃が続いている

  Threat Actors Continue to Exploit OT/ICS through Unsophisticated Means
  https://www.cisa.gov/news-events/alerts/2024/09/25/threat-actors-continue-exploit-otics-through-unsophisticated-means

- (12月13日) インターネットに露出したHMIが上下水道システムにサイバーリスクをもたらしている

  Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems
  https://www.cisa.gov/sites/default/files/2024-12/joint-factsheet-epa-cisa-internet-exposed-human-machine-interfaces-508c.pdf

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

MITRE社がD3FEND 1.0を公開

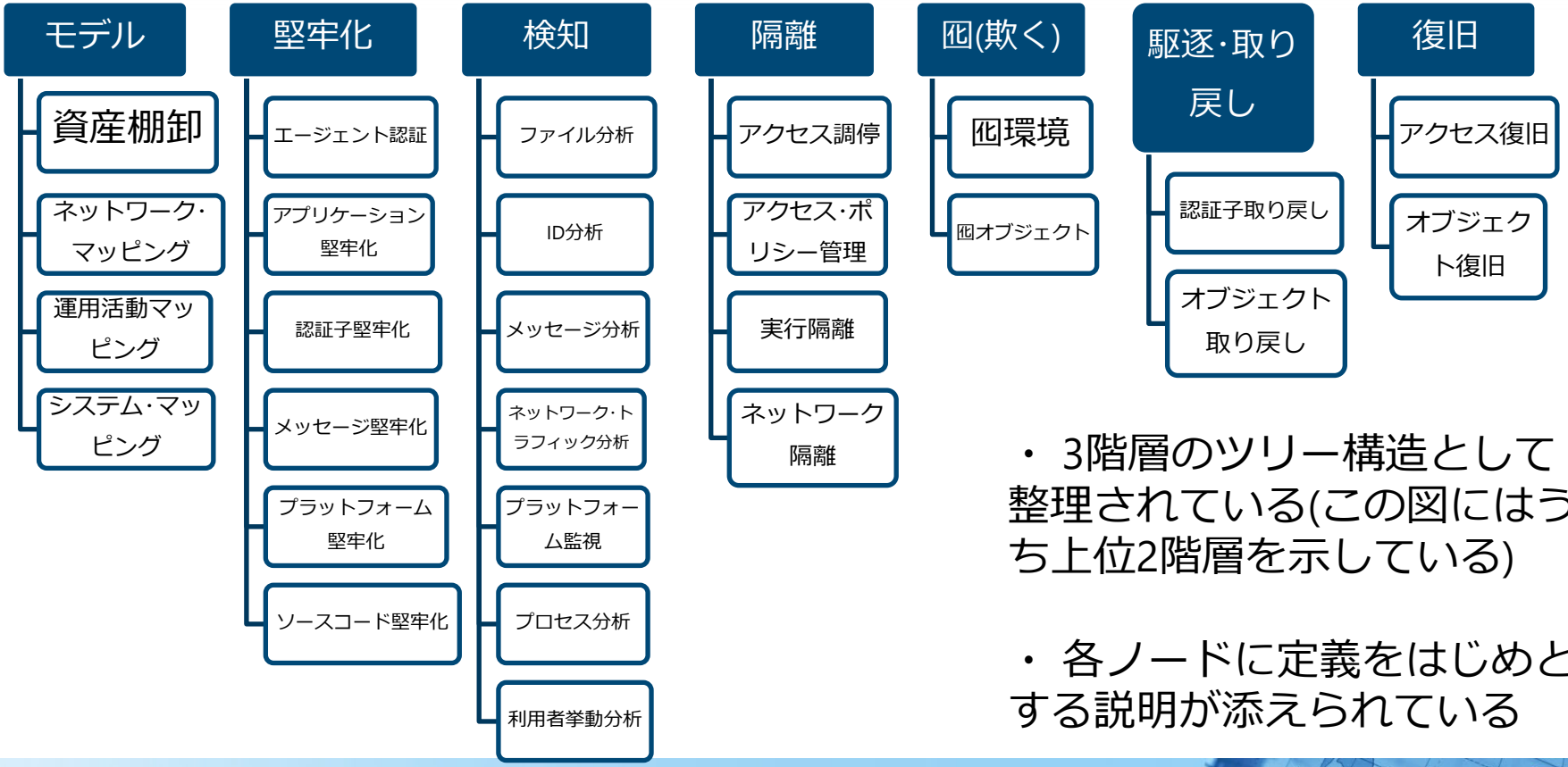
https://d3fend.mitre.org/

- MITRE社がD3FEND 1.0を公開 (2025年1月16日)
  https://www.mitre.org/news-insights/news-release/mitre-launches-d3fend-10-milestone-cybersecurity-ontology
  — 2021年6月に公表したβ版へのフィードバックを反映

- ATT&CKがサイバー攻撃に関する概念と用語のオントロジー
  であるのに対して
  D3FENDはサイバー防御に関する概念と用語のオントロジー

  (オントロジーとはツリー構造状に作られた用語集)

D3FENDの概要



・ 3階層のツリー構造として整理されている(この図にはうち上位2階層を示している)

・ 各ノードに定義をはじめとする説明が添えられている

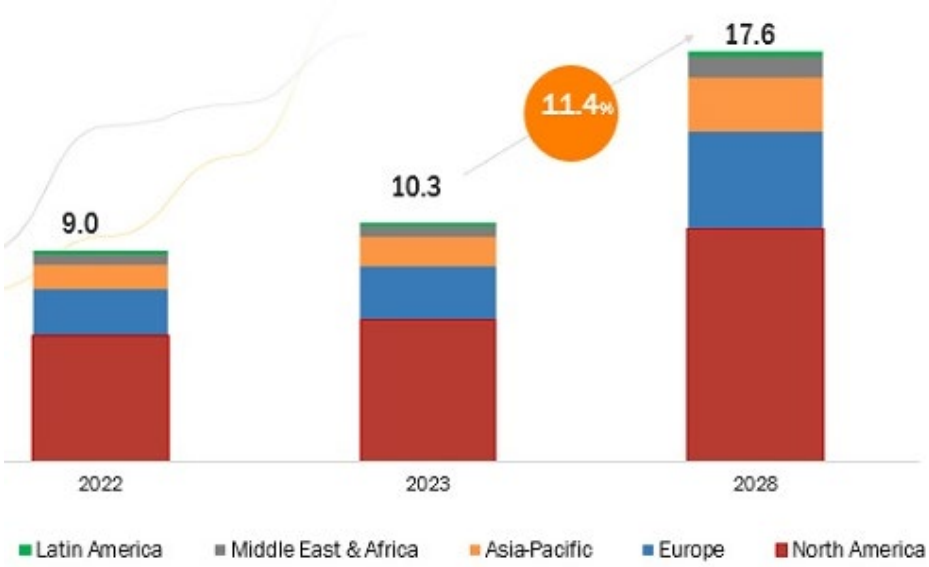
☞ サイバー保険の市場拡大と業界の動き
☞ 戦争条項を巡るMerck社の訴訟が和解；和解条件は不明

セキュリティ対策としての保険

サイバー保険の市場が急速に拡大中

- サイバー保険市場は世界的に平均年率11.4%で拡大しており2028年には1780億ドルに達する (2023年7月のMarketsandMarkets Research社の報告書)
  https://www.marketsandmarkets.com/Market-Reports/cyber-insurance-market-47709373.html

- 系統的なリスク(systemic risk)の扱いが課題
  - 免責にするリスクの定義
  - 国による補償(?)



[出典]
MarketsandMarkets
Rersearch社報告書

サイバー保険の市場拡大への期待と保険モデルの模索

- 保険大手のLloyd's of Londonと情報セキュリティ認証のHITRUST社が中心となってコンソーシアムを立上げた (12月12日)

  Lloyd's of London Launches First-of-its-kind Consortium Built on HITRUST Certification to Shape the Future of Cyber Insurance
  https://hitrustalliance.net/press-releases/lloyds-of-london-consortium-hitrust-certification-cyber-insurance

  - HITRUST社に認証されていれば…
    - 保険契約手続きが簡略になる
    - サイバー保険の保険料率が低く抑えられる
    - 保証範囲が広くなる
  - HITRUST認証を受けた組織で過去2年間に侵害があったのは1%以下

Merck社が1月3日に3社の保険会社と和解

- Merck社は2017年にNotPetyaの攻撃で社内の4万台のコンピュータが動かなくなり長期間業務が混乱；被害額は14億ドルとされている
- Merck社が請求した7億ドルの保険金の支払いは戦争条項を根拠に免責されると損害保険会社が主張して，裁判となった
- 2022年にニュージャージー州の裁判所は，戦争条項に該当するか否かは不明確で，その場合には権利者が有利になるよう解すべきとして，保険会社を敗訴とした
- 保険会社が2023年5月に上訴していたが，口頭弁論開始直前の1月3日に両者が和解した．和解内容は明らかにされていない．

[参考] Merck $1.4 Billion Cyberhack Settlement Ends ‘Warlike’ Act Claim (Bloomberg，1月4日)

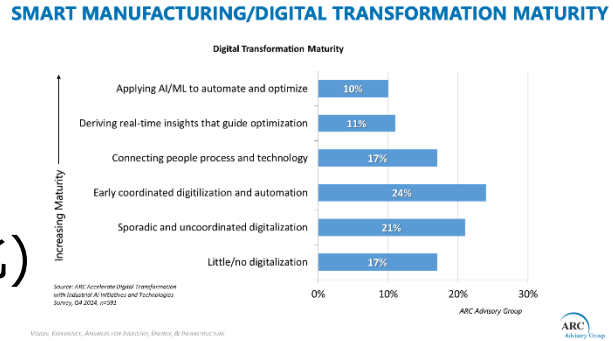
https://news.bloomberglaw.com/litigation/merck-1-4-billion-cyberhack-settlement-ends-warlike-act-claim

☞ 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

OT分野におけるAI利用の拡大

- 先進企業(10%)が成熟段階へ
  - 未着手企業を含め取り組みにバラつき
- 主な応用例
  - 予測保守 (ダウンタイム削減，設備効率化)
  - 製造の品質と管理
  - エネルギー利用の最適化
  - 労働安全
  - 知識ベース検索
- AI推進を主導する部門： OT，IT，事業企画？
  - AI利用に関するセキュリティの責任は？



[出典] ARC Industrial AI's Growing Digital Divide https://www.arcweb.com/blog/industrial-ais-growing-digital-divide

AI技術のセキュリティ課題

AIの利用者	セキュリティ課題	備考・例
正規の利用者	AI固有の脆弱性	AIアルゴリズム自体がもつ脆弱性
	AIシステム実現の脆弱性	AIシステムを実現する際に作り込まれる昔ながらの脆弱性
	AIシステムとの接続部分の脆弱性	AIシステムとの接続部分に作り込まれる昔ながらの脆弱性
攻撃者	攻撃ツールとしてAI利用	• AIを利用して偽情報を生成する • 第三者を攻撃するようAIを誘導する
	攻撃ツール開発のためにAI利用	AIを用いてマルウェアを開発

まだ黎明期にあるAIのセキュリティ対策

[出典] 3 takeaways from red teaming 100 generative AI products (2025年1月13日)
https://www.microsoft.com/en-us/security/blog/2025/01/13/3-takeaways-from-red-teaming-100-generative-ai-products/

- Microsoft社が10月に自社の100の生成AI製品に攻撃を試みて調査

- 教訓-1： 生成AIシステムは既存のセキュリティ・リスクを拡大するとともに新しいセキュリティ・リスクを呼び込んでいる
- 教訓-2： AIの改善とセキュア化の活動の中心は人間である
- 教訓-3： 多層防御がAIシステムを安全に保つための鍵である

AIアルゴリズム自体がもつセキュリティ課題

[出典] MITRE社ATLASプロジェクトによる「AIセキュリティ101」
https://atlas.mitre.org/resources/ai-security-101

- 汚染攻撃
  - AI訓練データを汚染することにより，推論にバックドアを作り込む
- はぐらかし攻撃
  - 入力に細工を加えることにり，誤った推論をさせる
- 機能抽出
  - クエリの反復を通じて，応答から機能的に同等のモデルを獲得
- 反転攻撃
  - クエリの反復を通じて，応答から訓練データ中の秘密データを獲得
- プロンプト注入攻撃
  - プロンプトに細工を加えることで，AIモデルが意図しない応答をさせる

米国CISAから重要インフラ向けAIリスク緩和ガイド

- (4月29日) 重要インフラの保有者と運用者向けの
  AIリスクを緩和する安全性とセキュリティ・ガイドライン

  MITIGATING ARTIFICIAL INTELLIGENCE (AI) RISK: Safety and Security Guidelines for Critical Infrastructure Owners and Operators
  https://www.dhs.gov/sites/default/files/2024-04/24_0426_dhs_ai-ci-safety-security-guidelines-508c.pdf

量子コンピューティング時代への備え

- 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する

- 2月6日にPQCA (Post-Quantum Cryptography Alliance)が発足
  https://pqca.org/

- 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
  先行的に対策を検討しておく必要がある

まとめ

- 比較的平穏な年だったと言えそう
  時代を画するようなICSセキュリティリスクの変化はなかった
- ランサムウェアの猛威は衰えていない
- 地政学的な緊張の高まりの中で
  国の安全保障の観点からセキュリティ規制の拡大が見込まれる
- ICS自体が大きく変わり始めていて
  それに伴うセキュリティリスクの出現が懸念される

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