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 ～

2022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

- ☞ 産業界が大きな変化の時代に
- ☞ ICSが一層のオープン化
- ☞ 米国大統領と日本の首相の交替など政治環境にも変化
- ☞ 抜本的な解決の目途が立たないサイバー・セキュリティ情勢

産業界を洗い始めた変化の大波とサイバー・セキュリティ情勢

Covid-19のパンデミックの中で加速したDX

- Druva社のサーベイ調査によれば，
  76%の回答者がCovid-19によってDXの計画を加速した
  https://www.helpnetsecurity.com/2021/02/02/digital-transformation-plans/

- McKinsey社の報告書によれば，Industry 4.0への取り組みが
  - 以前から進んでいた製造事業者はCovid-19をうまく乗り切った
  - 始まってた製造事業者にはCovid-19が実地試験の機会になった
  - 未着手だった製造事業者は新規投資余裕もなく苦境に陥っている

  https://www.mckinsey.com/business-functions/operations/our-insights/covid-19-an-inflection-point-for-industry-40

産業界が大きな変化の時代に

- 脱炭素(カーボン・ニュートラル)社会への転換
  - 電気化，水素化
- 新しい働き方
  - 遠隔業務，在宅勤務
  - AIやロボット利用による労働力不足の克服
- リスク認識の高まり
  - Covid-19，異常気象，サプライチェーン･リスク
  - サイバー･リスク

今後に新しく配備される
多様なICSの増加

ICSに対する新しい要件

ICSの一層のオープン化

- サイバー攻撃界面の拡大
- ICSの脆弱性の露出が高まる

■ クラウド・サービスの利用の拡大
- ERPやMESがクラウドに移行
- クラウドと連携して稼働するIIoT機器の導入
- ITシステムとOTシステムの融合

■ ICS基盤におけるオープン技術の利用の拡大

■ オープンなICSアーキテクチャーの模索：
OPA (Open Process Automation)
https://www.opengroup.org/forum/open-process-automation-forum

政治環境にも変化

- 米国大統領の交替： Donald Trump ⇒ Joe Biden (1月20日)
  7月12日に：
  - 国土保安省(DHS； Department of Homeland Security)長官にAlejandro N. Mayorkas氏を指名
  - 空席になっていたCISA長官にはJen Easterly氏を指名

- 日本の首相の交替： 菅義偉 ⇒ 岸田文雄 (10月4日)
  - デジタル庁が発足 (9月1日)
  - サイバーセキュリティに関しては引き続き内閣サイバーセキュリティセンター(NISC)が取りまとめ等を担当

社会全体のデジタル化加速

サイバー・セキュリティ情勢

- 国境越しのサイバー攻撃： 司法面の対策に限界
  - 米国がロシアにサイバー攻撃者の取締りを要請
  - 攻撃活動の容認を期待して，ロシア語版Windowsを攻撃対象から除外する機能を組み込むマルウェア開発者も
  - 国際的な連携による取締りの成功事例；懸念されるモグラ叩き状況

- サイバー攻撃のサプライチェーン階層化が進む
  - サービスとしてのランサムウェア(RaaS)
    攻撃基盤の提供者と，それを利用する攻撃者の分離専門化
  - サイバー攻撃の方法を伝授するサービスも登場
    https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-far-reaching-attacks-of-the-void-balaur-cybermercenary-group

- 2021年もICSを狙って起こされた重大なインシデントなく経過
  東京オリンピック・パラリンピック期間もサイバー的には平穏
- 重要インフラを狙うランサムウェア；深刻化した事案も
- 米国で上下水道施設におけるインシデントの発生が続いた

インシデントの動向

米国Colonial Pipeline社のランサムウェア感染

東海岸地域の石油燃料の45%(約3億リットル/日)を供給する石油パイプライン(8,859*km*)が約1週間にわたり停止

- 経過
  - 5月7日早朝： ITシステムで感染を発見；被害の局所化のためにITシステムとパイプラインの運用を停止；
    75Bitocoin(約500万ドル)の身代金を支払い； FBI等に通知
    バックアップからの復旧を決断(復号ソフトウェアが低速)
  - 5月10日： 攻撃集団DarkSideによるものとFBIが発表
  - 5月13日： パイプラインの運用を再開
  - 6月7日： 支払われた身代金のうち63.7Bitcoin(約230万ドル)を回収したと司法省(FBI)が発表

Colonial Pipeline社の石油パイプライン

- ヒューストン(テキサス州)からリンデン(ニュージャジー州)まで14州にまたがり，米国東海岸地域の石油燃料需要の45%を供給
  - ステーションや貯蔵ファーム，様々なポンプなど280施設から構成される

- 2系統からなる**単管式パイプライン**と見られる
  - 異なる宛先の様々な石油燃料(航空機燃料，灯油，ディーゼル燃料，ガソリン等)を時間的に切り替えて送油

- ITシステム内に設置されたERPの停止により送油すべき燃料の情報が得られず，パイプラインの運用が停止に追い込まれた
  - OTシステムはランサムウェアに感染していなかった(?)

Colonial Pipeline社のパイプラインの停止

ガソリン･スタンドに燃料を求めて詰めかけた自家用車

出典： New York Times紙

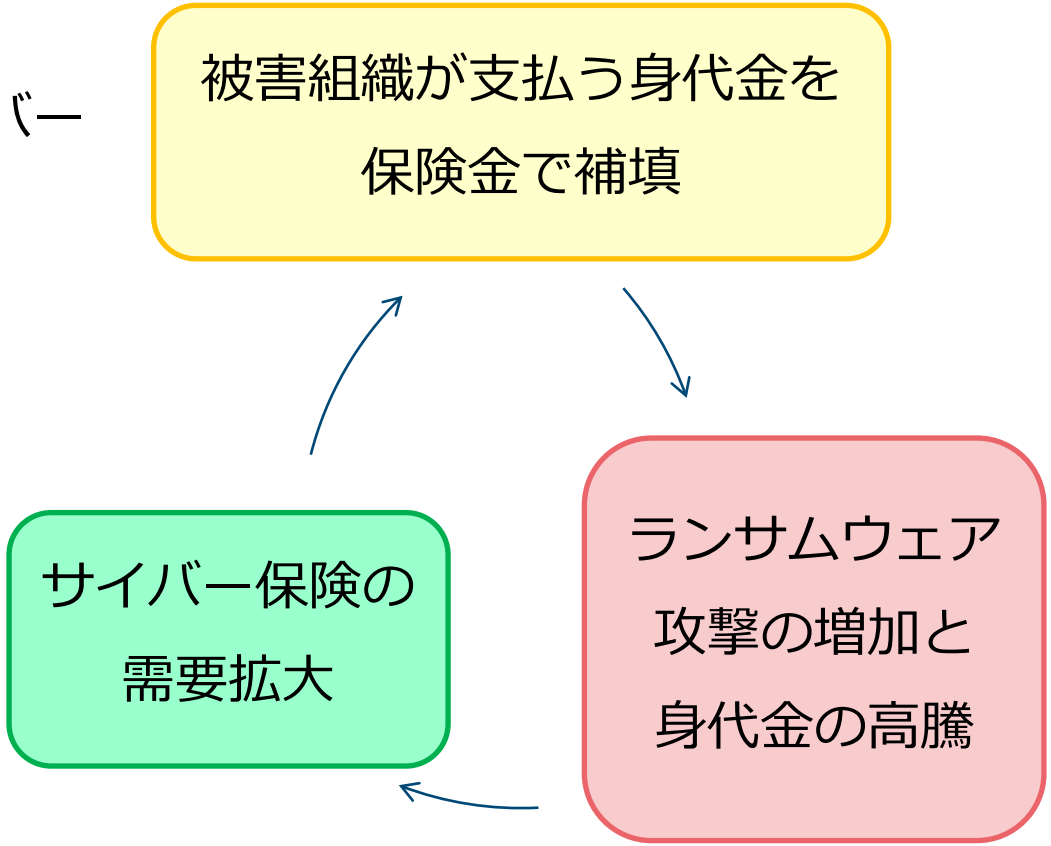
Colonial Pipeline社の感染の経緯と事例からの学び

- VPNのアカウント情報を攻撃者が4月29日に入手
  - 利用されなくなったアカウントが放置されていた
  - 複数のアカウント情報が闇ウェブで売られていた
  - VPNはMFA(多要素認証)を未採用だった

- Colonial Pipeline社に不足していたと考えられる対策
  - 遠隔アクセスに関する基本的なセキュリティ対策
  - サイバーインシデント下での事業継続計画
    特に，ITシステムが長期間使えない事態下でのICSの可用性確保
  - サイバー事案に関する社長(役員)の説明訓練

ランサムウェアが攻撃者にとって「金のなる木」に

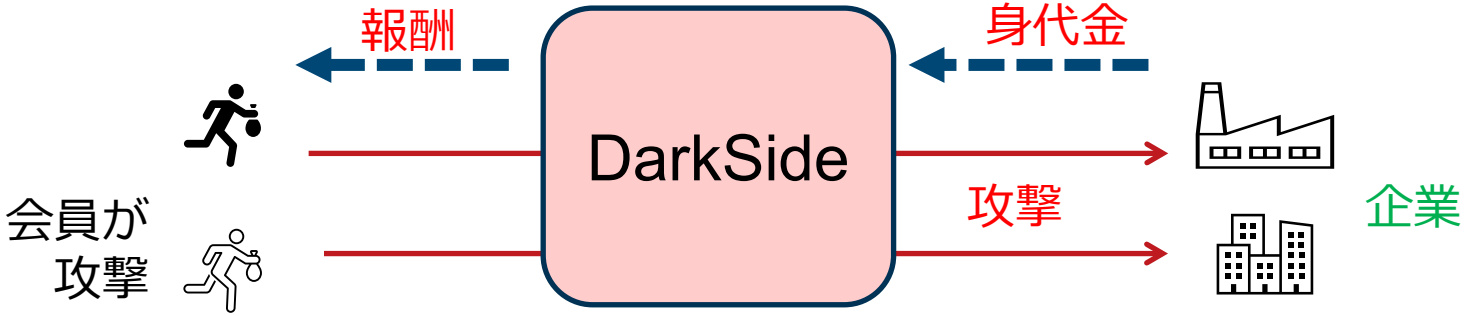
- 特に米国やドイツが深刻
- ランサムウェアが最大のサイバー脅威に；米国では
  - 過去2年間に攻撃が倍増
  - 復旧費用が平均10億ドル(前年比10倍)
- 保険会社の利益悪化
  - サイバー保険料の上昇



なお，日本損害保険協会では身代金をサイバー保険の補償対象としていない

攻撃者DarkSideの概要

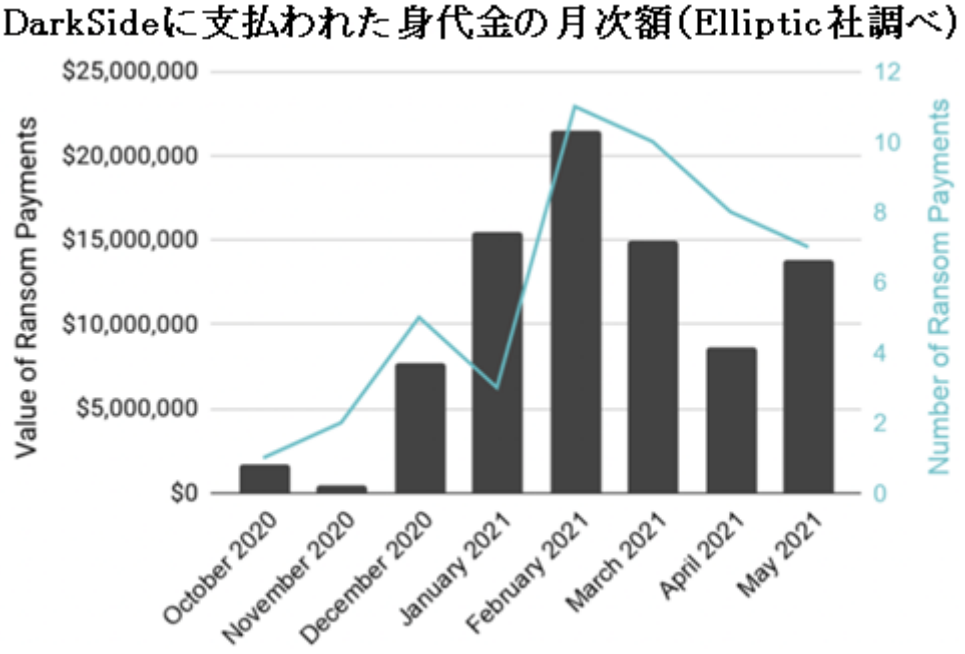
- ロシア国内に本拠を置いていると見られる
- RaaS (ランサムウェア as a サービス)の一つ
  (多くのランサムウェアがRaaS型になっている)
  - DarkSideがランサムウェア攻撃のための基盤を開発運用
  - DarkSideは会員(affiliate)を募集し
    会員が個々の企業に対する攻撃を実行
  - DarkSideは得られた身代金から店賃を差し引いて会員に渡す



攻撃者DarkSideの暗躍

(Elliptic社の調査によれば，2020年10月～2021年5月の調査対象期間中に)

- 99組織がマルウェアDarkSideに感染 (出典： DarkTracer社)
- うち47組織が
  身代金の支払いに応じ
  攻撃者DarkSideは
  総額9千万ドル以上を得た
  - 平均： 約190万ドル/組織
- DarkSideが得る店賃は：
  身代金が5百万ドル以下なら25%
  5百万ドル以上なら10%
  - 店賃の総額： 1550万ドル



RaaSに代表される攻撃基盤提供者と攻撃者の分業

- 技術を持つ者と手間暇を惜しまない者とが補完してサイバー攻撃
  - 高度のソフトウェア開発技術を持つ者が攻撃基盤を開発する
  - 低廉の時給で働ける者を闇市場で募集し，手順書を与えて，与えられた攻撃基盤を使わせて，攻撃を実施させる
  - 得られた利益を分割； 満足できる報酬がない場合もある模様で，闇市場には調停制度がある場合も
- 自律的に動作するタイプのマルウェアによらないインタラクティブに(人手で打鍵して)行われるサイバー攻撃が急増
  - 「2019年からの2年間で4倍に増加」とCrowdStrike社が報告 https://www.crowdstrike.com/resources/reports/global-threat-report/
- 一次的侵入の方法を商品として二次攻撃者に販売することにより売上利益を狙っている者も以前から存在している

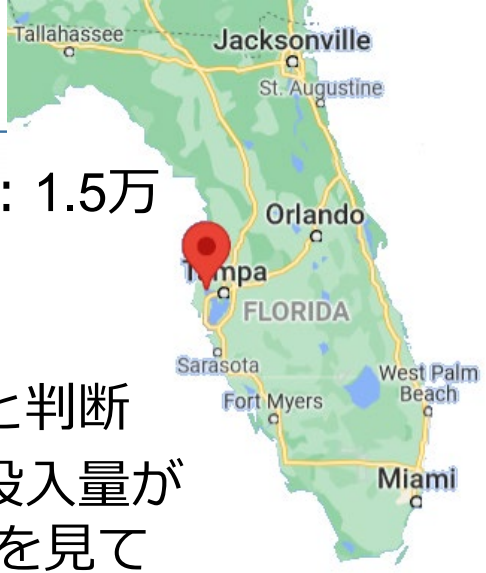
米国の上下水道施設で相次いだインシデント (1/2)

- 2,019年3月27日： Post Rock水道区(カンザス州)で元職員(23歳男性)が遠隔アクセスを通じてシステムを停止 (10月の公判で罪を認めた)
- 2020年12月～2021年2月： フロリダ州の上下水道施設建設業者のウェブ･サイトが改竄され水飲み場攻撃が行われていたことが後日判明
- 1月15日： カリフォルニア州ベイエリアの上水道施設のシステムに不正侵入があり浄水処理プログラムが削除された
- 2月5日：Oldsmar(フロリダ州)の上水道施設が遠隔から操作されて水酸化ナトリウムの投入量が異常な水準に増量された；直後に担当者が気付いて投入量を戻す操作を行えたので健康被害に至らず
- 3月： ネバダ州の水施設がランサムウェア感染； SCADAの監視制御が部分的に使えなくなった

米国の上下水道施設で相次いだインシデント (2/2)

- 4月： Mount Desert島(メイン州)の下水道施設にサイバー攻撃；施設の警報システムを無効化された
- 6月17日： 上下水道ISACが「業界の状況」について調査報告書；主に管理面における基本的なセキュリティ対策の立ち遅れを指摘
- 7月4日： Limestone(メイン州)の下水道施設が遠隔アクセスで侵入されランサムウェア(ZuCaNo)をインストールされる；復旧まで人手で運用
- 8月： カリフォルニア州の水施設でランサムウェア(Ghostの亜種)がSCADA画面にメッセージ表示
- 9月： ニュージャージー州の水施設でランサムウェア感染を発見
- 10月14日： CISAやFBI等が共同で注意喚起(AA21-287A)
  「米国の上下水道システムに対して進行中のサイバー脅威」

Oldsmar市の浄水場で不正な遠隔操作



Oldsmar市：フロリダ州タンパ近郊の小さな街； 人口：1.5万

- 2月5日の午前と午後に遠隔操作されていることを
  プラント操作員が目視で発見
  - 午前8:00の操作については上司による在宅作業と判断
  - 午後1:30に遠隔操作により水酸化ナトリウムの投入量が
    本来の100ppmから11,100ppmに増量されたのを見て
    不正な遠隔操作と判断するとともに，投入量を戻し遠隔操作を遮断
  - 過去には他施設で異常な量の投入による人身被害事例があった

- 2月8日に地元の保安官が記者会見
  https://www.tampabay.com/news/pinellas/2021/02/08/someone-tried-to-poison-oldsmars-water-supply-during-hack-sheriff-says/

Oldsmar市の浄水場で不正な遠隔操作 (続き)

後日，貧弱なサイバー・セキュリティの状況が明るみに

- 古い版のMicrosoft Windows (32bit版Windows 7)を使い続けていた
- すべてのコンピュータで同一の共有パスワードを利用
- 他の製品による遠隔操作に移行したのに，
  不要になったTeam Viewerがそのまま残されていて
  攻撃者に遠隔操作された

- Oldsmar市の浄水場に関連すると見られる11件の認証子が
  窃取された情報を公開しているサイト(COMB: Compilation of Many Breaches)の中にあったことが判明

オーストラリアの上下水道業界でも課題の指摘

監査院の監査報告

https://www.qao.qld.gov.au/sites/default/files/2021-11/Water 2021 (Report 3%E2%80%942021%E2%80%9322).pdf

- 調査した6つの水道当局のうち3つでシステムの管理対策に弱点(ITとOTの双方のシステムを含む)
  - 内部管理を中心に24件の欠陥を指摘
- クィーンズランド州の水道事業者SunWater社(19基のダムを保有)ではサイバー侵害を受けながら9ヶ月間にわたり検知ができず
- 古くなっているシステムがサイバー攻撃者に狙われやい

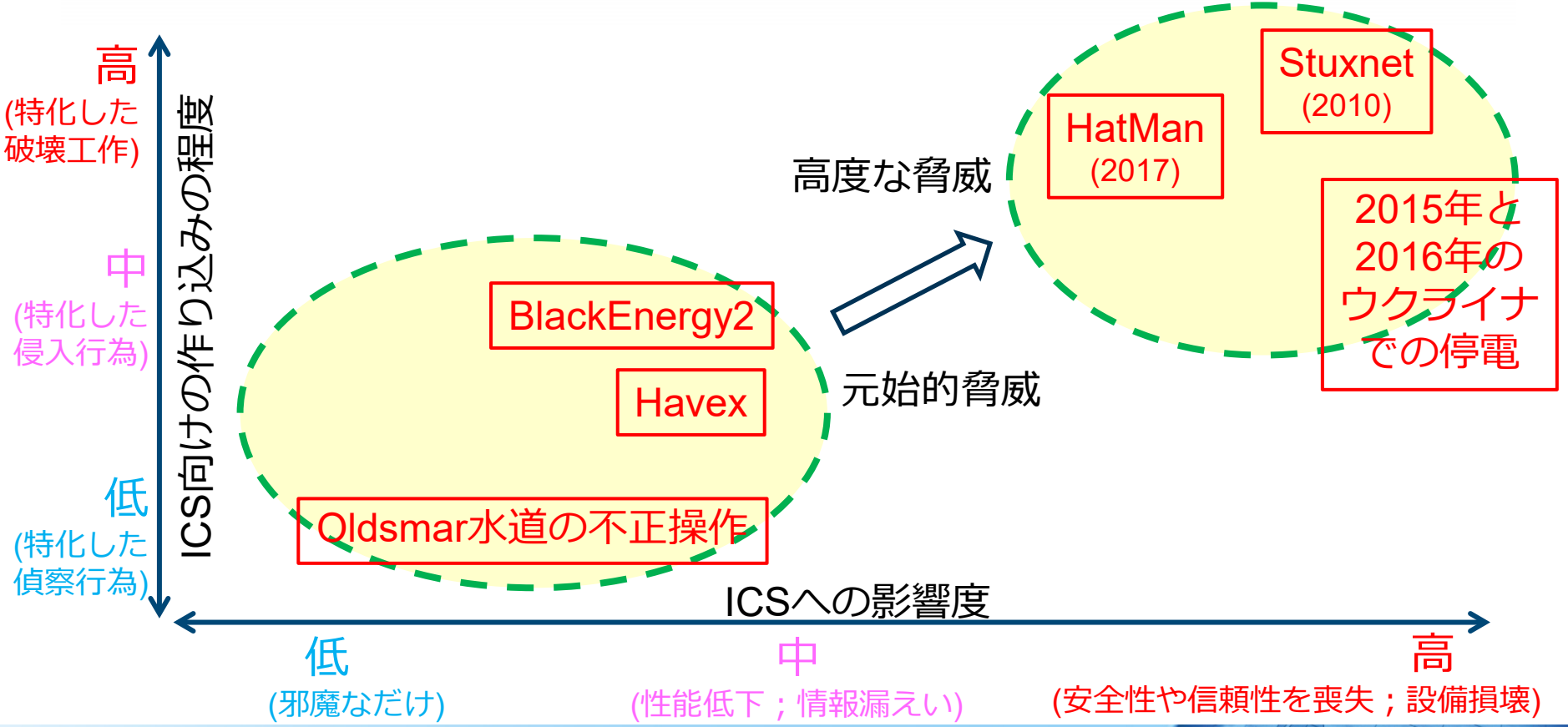
上下水道システムのセキュリティの構造的問題

Foundation for Defense of Democraciesのメモ (11月18日)

https://www.fdd.org/analysis/2021/11/18/poor-cybersecurity-makes-water-a-weak-link-in-critical-infrastructure/

- 多数の中小規模システム(水道：5.2万システム，下水：1.6万システム)
  - ICSやセキュリティに詳しい技術者が不在
  - 地方公共団体の管理下にあり中央政府の管理が及びにくい
- システムと施設が古くなったいるが，再生投資が限られている
- 相互依存性を通じて他の重要インフラにも事故の影響が及ぶ可能性も
- 統一的なサイバーセキュリティに関する標準や規制がなかった

ICSに対するサイバー脅威動向のまとめ



ICSに対するサイバー脅威動向のまとめ (続き)

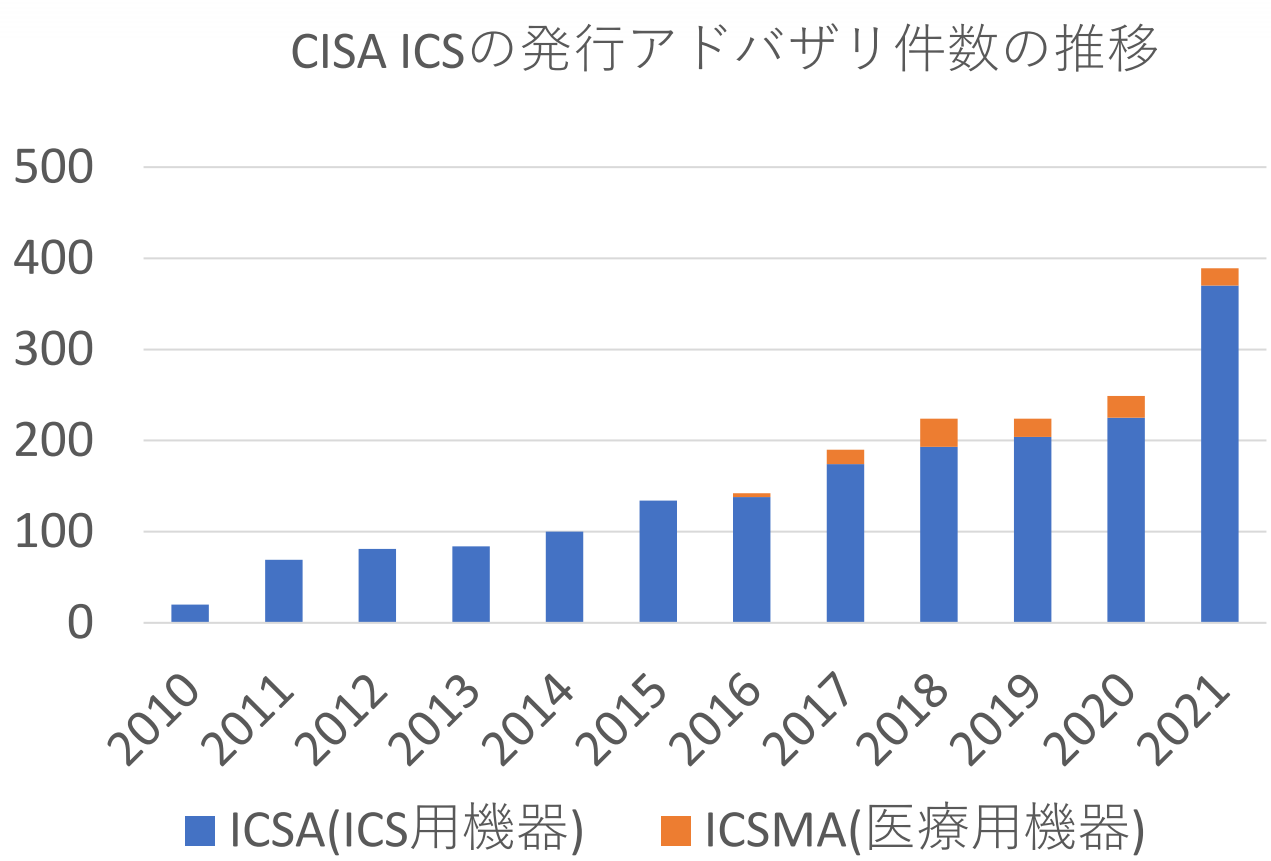
- 2021年を含めて，高度なICSの脅威がこの数年間現れていない
  - 攻撃者が「金のなる木」に手いっぱい？
  - ICSにおけるオープン技術の導入とネットワーク接続性が高まっており攻撃界面が拡大していることは確実と見られる

- 2021年に発生した米国の重要インフラでのインシデントが社会的・政治的に大きく注目を集めた
  - 2022年から重要インフラを中心に規制が強化される予兆あり
    - 米国DHSが陸上輸送事業者に対するサイバーセキュリティ要件を新設
      https://www.tsa.gov/news/press/releases/2021/12/02/dhs-announces-new-cybersecurity-requirements-surface-transportation
    - 重要インフラ、企業にサイバー防衛義務付け 22年度から (日本経済新聞)
      https://www.nikkei.com/article/DGXZQOUA307KB0Q1A131C2000000/

- ☞ 2021年は前年比6割増しの370件(他に19件の医療用機器)
- ☞ ICS製品のセキュリティ試験の最高潮年になったとClaroty社が分析
- ☞ 2021年末に公表されたApache Log4jの脆弱性が不気味

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



2021年に
公表された
脆弱性件数が
前年比６割増しの
370件に

公表されたICS製品の脆弱性のClaroty社による動向分析

公表されたICS製品の脆弱性の動向をClaroty社(イスラエル)が半年ごとに分析

https://claroty.com/wp-content/uploads/2021/08/Claroty_Biannual_ICS_Risk_Vulnerability_Report_1H_2021.pdf

- 2021年上半期の動向 (医療用機器を含む；当該期では7.85%)
  - 76社のベンダー製品に合計637件の脆弱性 (2020年下半期比4割増し)
  - 80.85%の脆弱性が開発者以外の者により発見された
  - Siemens社の製品で発見された脆弱性が146件と最多だが，その多くは同社内で発見されていた
  - 65%の脆弱性は悪用されると可用性が完全に失われそう
  - 25.59%の脆弱性にパッチなどの修復手段が提供されていない うち，61.69%がファームウェアの問題，55.21%で遠隔から任意のコードを実行でき，47.85%で機能停止を起こせる

Log4jソフトウェアの脆弱性に関する問題

CISA Alert(AA21-356A) Mitigating Log4Shell and Other Log4j-Related Vulnerabilities
https://www.cisa.gov/uscert/ncas/alerts/aa21-356a

- Log4jは，エラー等の事象を記録し，診断メッセージをシステム管理者や利用者に通知するための，Apacheソフトウェア財団が提供しているオープンソース・ソフトウェア(Javaライブラリー)
  - Google社の調査によれば少なくとも1.7万種類の製品で利用されている
    ウェブ･サーバー機能をもちウェブ･アプリケーションを利用している
    ICS関連製品もLog4jを利用している可能性がある
- 2021年末にLog4jに複数の脆弱性が報告された
- 脆弱性を悪用すると
  第三者が当該機器を乗っ取り任意のコードを実行できる
  ことが判明した

Log4jソフトウェアの脆弱性に関する問題 (続き)

- 脆弱性の深刻さと脆弱性を継承する製品の種類が多数に及ぶために
  この脆弱性の影響が数年間にわたり長引く可能性がある

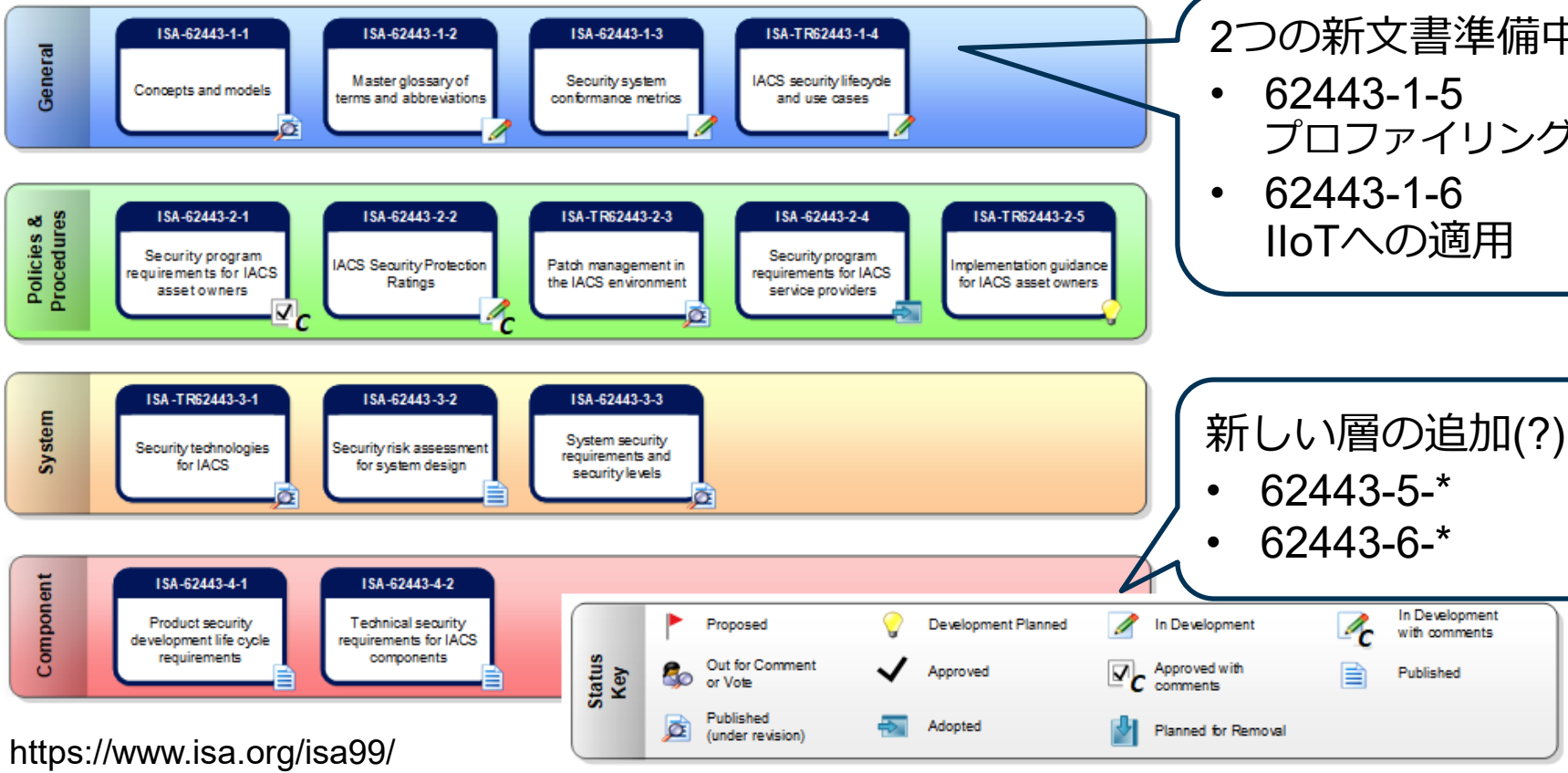
- 良いニュース
  - 一部の製品ベンダー(海外)では自社製品への影響の有無を
    積極的に調査し対処している
  - ICSでの攻撃事例が今のところ報告されていない

- 悪いニュース
  - ベルギーの防衛省で本脆弱性を悪用した侵害が発生
  - 国家支援を受けた攻撃者やランサムウェア集団による悪用事例あり

- ☞ IEC 62443の標準化作業の表立った動きはなかったが…
- ☞ ICS関連の認証件数が微増ないし漸増

標準化や認証に関する動向

IEC 62443 (ISA 62443) シリーズ： 2021年の新公開なし



2つの新文書準備中
- 62443-1-5
  プロファイリング
- 62443-1-6
  IIoTへの適用

新しい層の追加(?)
- 62443-5-*
- 62443-6-*

https://www.isa.org/isa99/

IEC 62443 (ISA 62443) シリーズの整備 (改定)

2021年に新たな発行文書はなかったが，改定作業が進んでいる模様

- シリーズ中の標準文書相互間の整合性を高める

- IEC TS 62443-1-1:2009 Terminology, concepts and models
  ⇒ その後のICSアーキテクチャーやセキュリティ技術の変化を盛り込む
- IEC 62443-2-1:2010 Security program requirements for asset owners
  ⇒ 改訂完了間近
- IEC TR 62443-2-3:2015 Security update (patch) management)
  ⇒ 改定作業中
- IEC 62443-3-3:2013 System security requirements and security levels
  ⇒ 改定作業中

IEC 62443 (ISA 62443) シリーズの整備 (追加)

- IEC 62443-1-3 Performance metrics for IACS security
  - セキュリティ対策状況の定量的な計測指標
- IEC 62443-2-2 IACS security protection
  - 「セキュリティ保護水準」を定義

- IEC 62443シリーズの水平標準化(ICS以外の分野への適用)に向けて
  - IEC 62443-1-5 Scheme for cybersecurity profiles
  - IEC 62443-5-1 個々のプロファイルを定義(?)

- 認証手順を定めたIEC 62443-6-*の検討 (?)
  - EUが62443等の国際標準に基づいた製品認証を期待

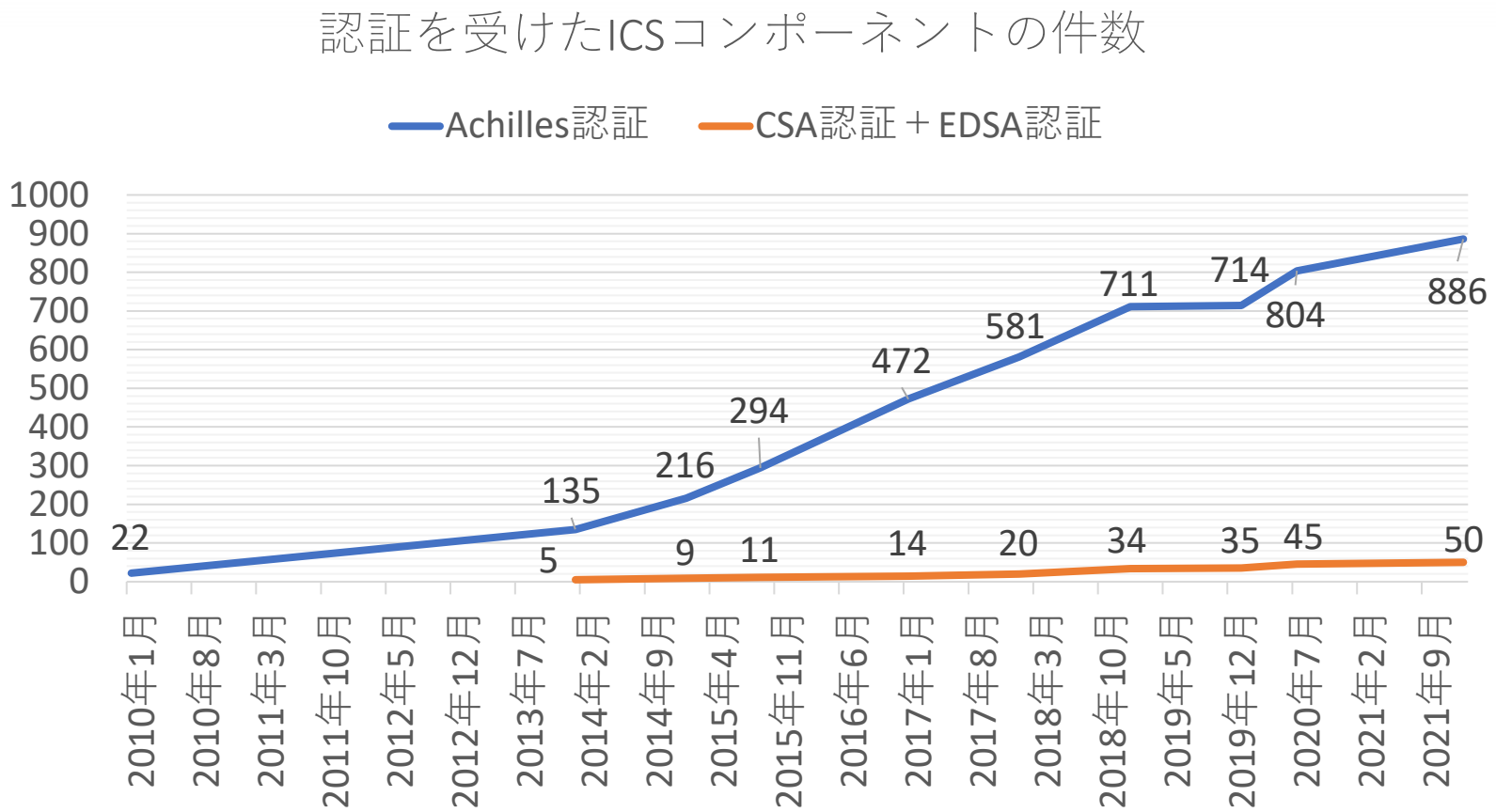
認証を受けたICSコンポーネント製品数の動向

- Achilles認証が，1年で約80製品が増えて，886製品に(前年804製品)
  - GE Digital社が運用している認証制度

- EDSA＋CSA認証は，1年で5製品が認証され，総計50製品に
  - ISA SecureがIEC 62443-4-2に基づいて認証
  - うち1製品は国内ベンダーの製品
  - 2021年に新たに認証された6製品の認証水準は
    すべてCSA 1.0.0 Level 1

EDSA：
Embedded Device Security Assurance
CSA：
Component Security Assurance

認証を受けたICSコンポーネント製品数の推移

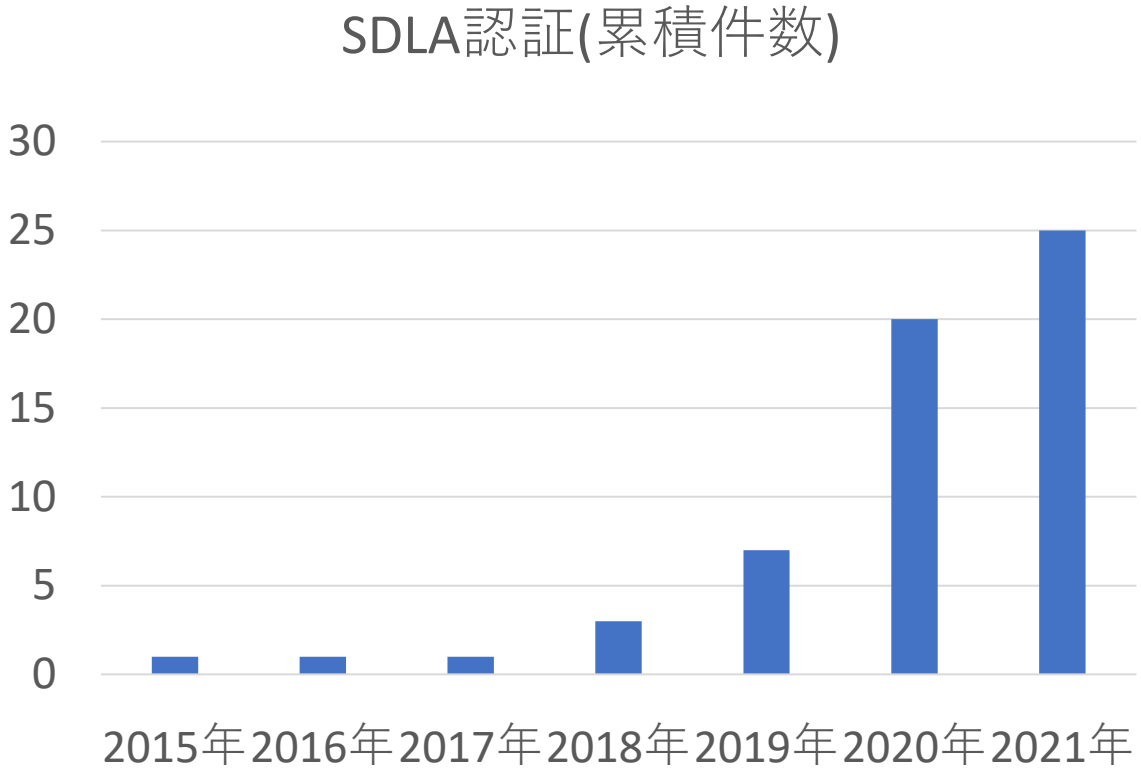


ICS(システム)に対する認証の動向

- SSA (System Security Assurance)認証
  - ISA SecureがICS(システム)を対象としてIEC 62443-3-3 に照らしてセキュリティを認証
  - 実態はDCSやSISのような製品がシステムとして認証されている
  - 2021年には新たに1システムが認証され，累計で4システムに

開発プロセスの認証への関心が高まる

- SDLA (Security Development Lifecycle Assurance) 認証



ISA Secureが，製品/システム開発組織(拠点)を対象として，その開発プロセスにおけるセキュリティ対をIEC 62443-4-1に照らして認証している

米国では電力基幹事業者にインシデント報告義務

- NERC CIPは米国とカナダの電力事業者団体NERCが定めたサイバー・セキュリティ標準集
  https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
- 米国では電力規制委員会(FERC)が
  CIP標準から指定したものを電力基幹網に関連する事業者に義務付け
- CIP 008 (Incident Reporting and Response Planning) に関して
  第6版が2021年1月1日に発効(義務化)
  https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf
- 実害に至らないものついても，インフラや運用に対するサイバー侵害の試みを検知し，報告することが義務付けられた
  (従来は実際に影響があった事案のみ報告義務)
- 重要インフラ事業者のインシデント報告の義務化は米国議会も関心

初版の発行から20年が経過

- ☞ 年初にSolarWinds社製品を介した大規模なサイバー攻撃が判明
- ☞ 一部の外国製品に対する疑念
- ☞ サプライチェーンに沿った脆弱性の継承(Nディ脆弱性)

サプライチェーンと ICSセキュリティ

サプライチェーンを巡るセキュリティ課題

- 「調達>生産>物流>販売>購買」というサプライチェーンに対する内外の脅威に起因するセキュリティ・リスクを管理することが必要
  - SolarWinds社の事案ではソフトウェア製品のオンライン更新の際に不正な機能を組み込んだコードが配付されて，当該製品の利用組織が侵害された
  - Washington Post紙によれば，
    中国政府が要請した監視プログラムを一部の華為社製品が搭載
    https://www.washingtonpost.com/world/2021/12/14/huawei-surveillance-china/

クラウド・サービス利用に関するセキュリティ

米国CISAが1月13日に分析報告書(AR21-013A)

https://us-cert.cisa.gov/ncas/analysis-reports/ar21-013a

- 多数の攻撃者がクラウド･サービスを狙っている
  - フィッシング(なりすましメール)による認証情報の詐取
  - アクセス端末の脆弱性の悪用などによる認証情報の窃取

  多要素認証(MFA)によるVPN等の対策をとっていても
  基本的セキュリティの欠如があると対策を突破される

- クラウドのセキュリティ設定の誤りにも要注意
- 多要素認証のないVPNはセキュリティ･リスクが高い

サプライチェーンに沿って継承される脆弱性

- サプライチェーンに沿って継承される脆弱性

  例　リアルタイムOS ⇒ 各種の組込み機器
  通信プロトコル･ライブラリー製品 ⇒ 通信機能を搭載した機器
  CodeSys社製品 ⇒ 各社のPLC製品

- 修正されるまでに極めて長い時間がかかることがしばしばある

- 継承された脆弱性に製品利用者が気付ける仕組みとして SBOM (ソフトウェア部品表：Software Bill of materials)の開示が求められている
  - 10月にMicrosoft社がSBOMとしてSoftware Package Data Exchange (SPDX)形式への軌道修正を表明
    https://devblogs.microsoft.com/engineering-at-microsoft/generating-software-bills-of-materials-sboms-with-spdx-at-microsoft/

まとめ

1. 変化の時代の中でICSのサイバーリスクが高まっている
   - ICSの中身や使われ方
   - ITシステムとICSとの密結合化
   - 新技術に付随する潜在的な脆弱性
   - 攻撃者の組織化
2. 幸いここ数年間はICSに対する攻撃手法の進化が足踏み状態
3. 懸念される継承されたICS製品の脆弱性の蓄積
4. 新時代の標準化と認証制度に期待
5. 広い戦線に目配りが欠かせないサプライチェーンのセキュリティ

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/

インシデント報告

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

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form.html

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