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 ～

JPCERTコーディネーションセンター
ICSR　技術顧問
宮地利雄

- ☞ COVID-19対策のための新たな業務形態
- ☞ COVID-19が加速させたシステムの進化
- ☞ COVID-19関連機関へのサイバー攻撃が活発化した一方で
  ICSへのサイバー攻撃は相対的に沈静化か？

COVID-19とICSセキュリティ

COVID-19対策のための新たな業務形態

- 「三密」を避けたICSの運用と保守
  - 操作室や操作卓の分散化
  - 連続運転における操作員の引継ぎの非対面化
  - 遠隔操作の利用の拡大
  - オンライン会議の利用の拡大
  - ☞ ICSや関連ネットワークの設定や構成変更が適切になされていますか？
  - ☞ ICSがインターネットに露出していませんか？
- アウトソーシングの拡大
  - 監視サービスなど
- 大きな需給変動に伴う事業環境の変動
  - 必用なICSセキュリティ対策予算が維持できていますか？

サプライチェーンの
セキュリティに注意！

COVID-19が加速させたシステムの進化

- COVID-19が急加速させたとされる
  - ITとOTとの統合
  - DX (デジタル変革； Digital transformation)

- セキュリティ対策への目配りが伴っていますか？
  - NSAとCISAが共同でICSのセキュリティ対策を推奨 (7月23日)
    AA20-205A： NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems
    https://us-cert.cisa.gov/ncas/alerts/aa20-205a
  - EuroPolがCovid-19流行下の組織犯罪について見通し (4月30日)
    https://www.europol.europa.eu/publications-documents/beyond-pandemic-how-covid-19-will-shape-serious-and-organised-crime-landscape-in-eu

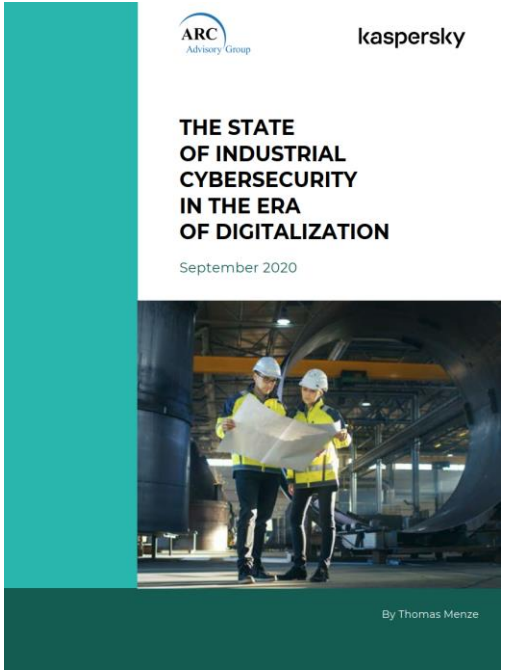
ARCとKaspersky社とが合同報告書

The State of Industrial Cybersecurity 2020

https://ics-cert.kaspersky.com/reports/2020/09/15/the-state-of-industrial-cybersecurity-2020/

2020年のICSセキュリティに影響する要因：

- Covid-19流行
  在宅勤務の増加 (53%)，セキュリティ予算削減(24%)
- 新技術
  IIoT(55%)，クラウド(55%)，
  エッジコンピューティング(36%)，5G(33%)
- DX
  DXに必要なセキュリティ推進(44%)



・ 2020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

☞ 西アジアと南アジアでICSへの攻撃の報道

☞ ランサムウェアの進化が続く

インシデントの動向

イスラエルの水処理施設にサイバー攻撃

- 海水を脱塩処理して飲料水を得るなどイスラエルの水は貴重な資源

- 2020年1月～3月頃にかけて水処理施設がサイバー攻撃を受けているとしてイスラエル政府が注意喚起

  https://securityaffairs.co/wordpress/102361/hacking/israeli-water-facilities-attacked.html

- 4月24～25日に6ヶ所の上下水道施設にサイバー攻撃
  - 未然に防止しされたが，水道の塩素混入量を変えようとしていた

  https://www.timesofisrael.com/6-facilities-said-hit-in-irans-cyberattack-on-israels-water-system-in-april/

- 7月頃にも2ヶ所の水処理施設にサイバー攻撃

  https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/

数百人を毒殺の可能性

イランの港湾施設がサイバー攻撃で麻痺状態に

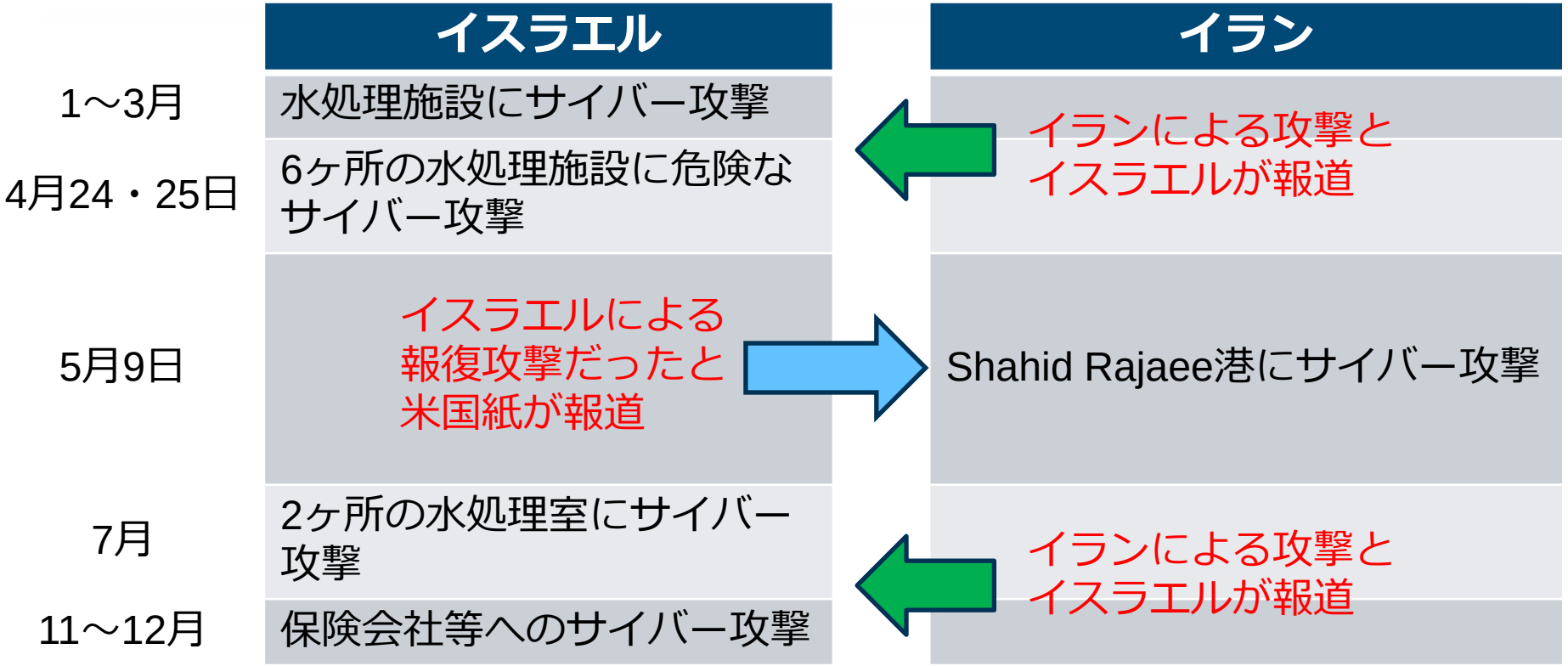
- 5月9日にイランのShahid Rajaee港がサイバー攻撃を受けて港湾施設の機能が麻痺状態に
  - ―港につながる道路と水路で大量の滞留が発生

https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.htm

Shahid Rajaee港

- 年間の貨物取扱量：1億トン
- コンテナ・ターミナルはイラン最大

イスラエル と イラン間のサイバー攻撃



司法長官代理が語るイスラエルの対応方針

https://www.lawfareblog.com/israel-cyberattacks-and-international-law

- Roy Schöndorf氏が12月8日に海軍大学で講演し，
  次の2つを柱とするイスラエルの立場を表明

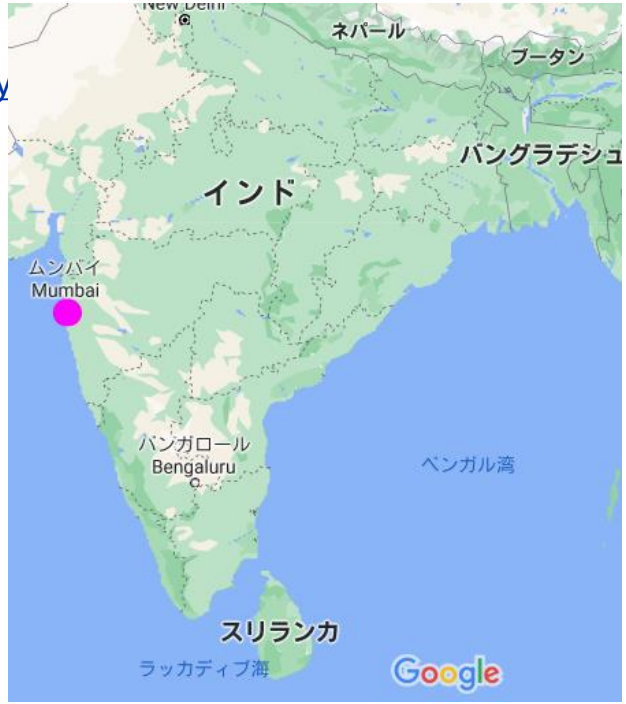
1. 外国に対する脅威や武力の行使を禁止している慣例がサイバー領域にも適用される
2. 武力と同様の効果を伴うサイバー攻撃には国際人道法が適用される
   (有形物に対する損害が予想されるならば国際人道法の義務違反)

- 防衛能力と報復能力による対処から，国際法によるサイバー攻撃への対処を模索しているとも見られている

インドのムンバイ市で10月中旬に大規模停電

https://mumbaimirror.indiatimes.com/mumbai/other/-maharashtra-energy-minister-nitin-raut-on-mumbai-power-outage-incident-possibility-of-foul-play-cant-be-ruled-out/articleshow/78653884.cms

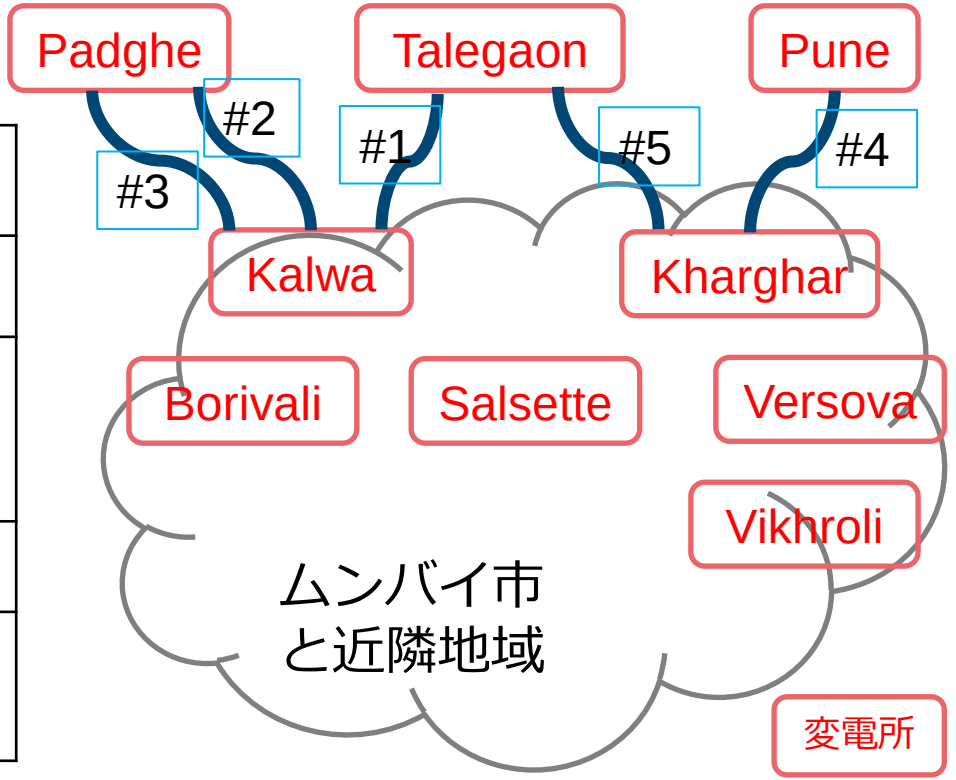
- インド西部の都市ムンバイで10月12日10～12時の約2時間にわたる大規模停電が発生
- 広域停電を防ぐ仕組みも機能せず
- 原因が不明でサイバー攻撃を含む妨害工作の影響が疑われる



インドのムンバイ市で10月中旬に大規模停電

https://mumbaimirror.indiatimes.com/mumbai/other/multiple-power-trips-grid-separation-failure-to-blame/articleshow/78630651.cms

#1	10日	400kV Talegaon－Kalwa線停止
#2	12日 04:33	400kV Padghe－Kalwa線停止
#3	12日09:58	400kV Padghe－Kalwa線停止 周波数低下(50Hz→48Hz)
#4	12日10:00	Pune－Kharghar線停止
#5	12日10:02	Talegaon－Kalwa線停止 域内の火力＆水力発電所にも影響



跋扈するランサムウェア攻撃

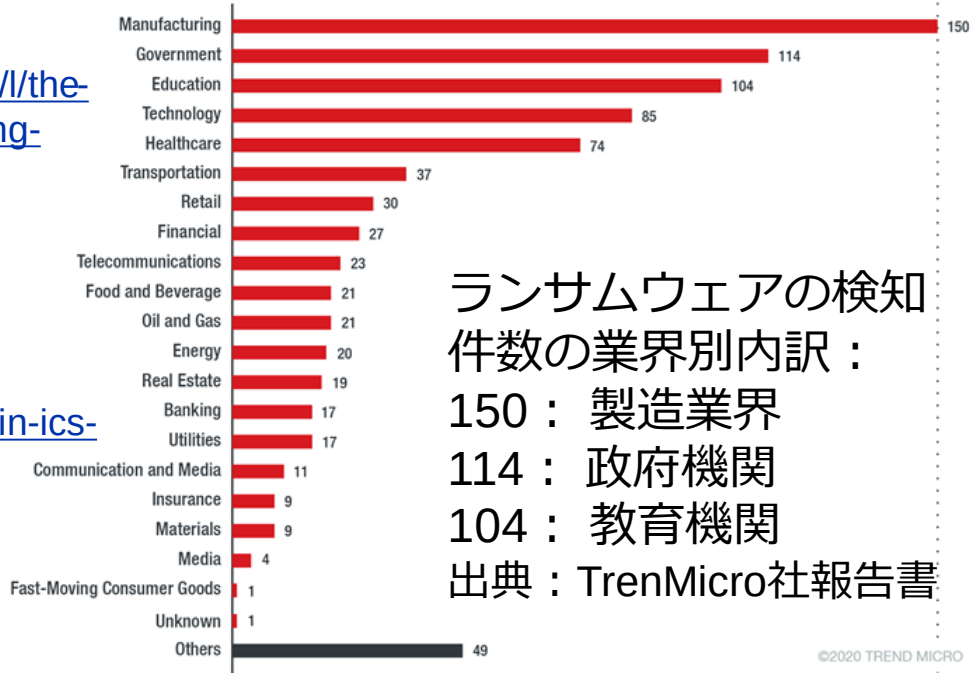
- CrowdStrike社によれば…
  https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeServicesCyberFrontLines.pdf
  同社の顧客が関連した200件のインシデント中：
  - 63%が金銭的な動機によるサイバー攻撃
  - 金銭目的のサイバー攻撃の81%(全体の51%)がランサムウェア攻撃

- Group IB社によれば…
  https://www.group-ib.com/media/gib-report-2020/
  2019年末～2020年において：
  - 45ヶ国以上で500件以上のランサムウェア攻撃が勃発
  - 支払われた身代金総額だけで堅く見積もって10億ドル以上
    (関連する被害総額はそれを遥かに超えるものと見られる)

支払われた身代金の平均額が2億円

製造業界の企業を狙うランサムウェア攻撃

- TrendMicro社が報告書
  https://www.trendmicro.com/en_us/research/20/l/the-impact-of-modern-ransomware-on-manufacturing-networks.html
  - 最も被害を受けているのが製造業界
- Dragos社が報告書
  https://www.dragos.com/resource/ransomware-in-ics-environments/
  - OT網にもランサムウェアで破壊的な被害
- 米国FBIがランサムウェアDoppelPaymerについて注意喚起
  https://www.ic3.gov/Media/News/2020/201215-1.pdf



ランサムウェアの検知件数の業界別内訳：
150： 製造業界
114： 政府機関
104： 教育機関
出典：TrenMicro社報告書

最近のランサムウェアの攻撃プロセス例

■ ネットワーク内に侵害後にランサムウェアを配備

1. フィッシング・メール等を利用して悪意あるサイトに誘導する，
   リモート・デスク・トップ(RDP)を悪用する等の手段で
   最初のコンピュータをマルウェアに感染させる
2. ネットワーク内でマルウェアの感染範囲を拡大しながら，
   ネットワークの情報を収集して狙うべきシステムを特定して，
   又は広範囲にランサムウェアをインストールする
3. データのコピーを外部に送り出す
4. 夜間など気づかれにくい時間帯を狙ってデータを暗号化し，
   その後に身代金要求を表示

ランサムウェアの進化

- 過去の進化
  - 標的を個人から組織に
  - 仮想貨幣を利用して高額の身代金(数百万円～数十億円)
- 近年の進化
  - 開発者と攻撃者の分業 → 攻撃基盤を貸し出すサービス
  - データを暗号化する前に外部にコピーを持出し，
データを開示すると脅して身代金の支払いを迫る
  - ICSも標的に
- 今後もさらに進化すると見込まれる
  - サイバー犯罪者にとってランサムウェアは「金のなる木」

ランサムウェアに関する参考資料

- 重要インフラへのランサムウェア攻撃のデータベース (Temple大学)
  https://sites.temple.edu/care/ci-rw-attacks/

- ランサムウェアの現状
  - Ransomware to blame for nearly half the cyber-insurance claims filed in early 2020
    https://www.cyberscoop.com/ransomware-cyber-insurance-cost-beazley-coalition/

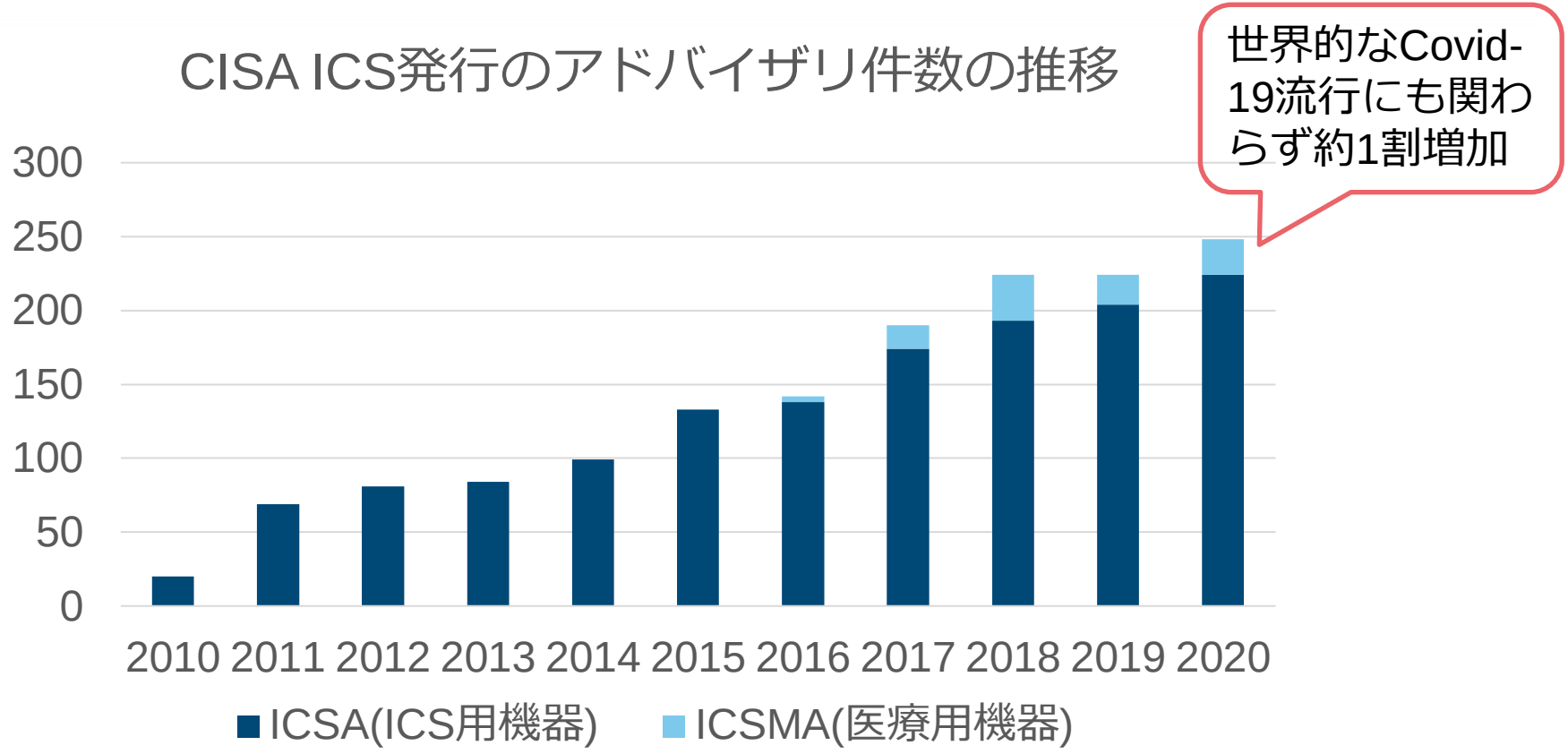
- ランサムウェアとICS
  - Ransomware and ICS
    https://www.cyberscoop.com/ransomware-network-access-accenture/

- ランサムウェアの進化
  - The Emerging Ransomware-As-A-Service Economy
    https://www.forbes.com/sites/robertvamosi/2020/11/27/the-emerging-ransomware-as-a-service-economy/
  - How middlemen are giving ransomware gangs more attack options
    https://www.cyberscoop.com/ransomware-network-access-accenture/
  - Ransomware variants continue to evolve as crooks chase bigger paydays
    https://www.zdnet.com/article/ransomware-variants-continue-to-evolve-as-crooks-chase-bigger-paydays/

- ☞ 毎年に公表される脆弱性の件数は200件前後で増加傾向
- ☞ TCP/IPプロトコル・スタックの脆弱性
- ☞ VEPについて

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



TCP/IPプロトコル・スタックの脆弱性

いずれも，元のライブラリの脆弱性は修正されているが，
ライブラリを組み込んで作られた製品の多くに脆弱性が残留

Nディ
脆弱性

- Ripple20
  https://www.jsof-tech.com/ripple20/
  - Treck社製TCP/IP(アジアでは図研エルミック社が販売)の中にあった19件の脆弱性
- URGENT/11
  https://www.armis.com/urgent11/
  - VxWorksのIPネットワーク部分にあった11件の脆弱性(2019年公表)
- Amnesia:33
  https://www.forescout.com/company/resources/amnesia33-how-tcp-ip-stacks-breed-critical-vulnerabilities-in-iot-ot-and-it-devices/
  - 4つのオープンソースのTCP/IP (uIPとPicoTCP, FNET, Nut/Net)の中にあった33件の脆弱性

蓄積されるNデイ脆弱性

- ICS機器やIIoT機器に
  共通モジュールから継承され
  放置されている脆弱性
  - 例：プロトコル・スタックや
    CODESYS → PLC等
  - 脆弱性情報が公表されている
    ⇒ 攻撃者には情報あり
  - 製品利用者が脆弱性の存在を
    知ることも難しい

- ICS機器やIIoT機器のベンダーは
  S-BOM (ソフトウェア部品表；
  Software Bills of materials)の
  提供に向けた取り組みを！
  - 医療機器を含む重要インフラ
    分野での要求が高まる動き
  - 今から準備を！
    一朝一夕ではできない！

公表される脆弱性情報の識別子の付与について

- 公表される脆弱性にはCVE識別子

例：CVE-2021-12345

- 9月15日に米国CISAが
  ICSと医療用機器に関する
  最上位のルートCNAに指定された
  https://www.cisa.gov/news/2020/09/15/cisa-oversee-cve-numbering-authorities-industrial-control-systems-and-medical

現在のルートCNAは
MITRE,
JPCERT/CC,
CISAの3機関

- CNA (CVE Numbering Authority)
  CVE識別子を付与する機関
  - 多数の脆弱性に円滑にCVE識別子を
    付与する多数のCNAによる分散管理に

https://cve.mitre.org/cve/cna.html

製品ベンダーも
CNAの指定を受ける
ことが可能

脆弱性情報の取扱

- 日本では経済産業省告示「ソフトウエア等脆弱性関連情報取扱基準」による届出が強く推奨されている
  ⇒ 届出機関： IPA,　⇒ 調整機関： JPCERT/CC
  - 原則として製品開発者との調整を経て公表

- 世界的には公表されない脆弱性も
  - 政府機関が発見ないし購入して資産として利用
    - 米国政府にはVEP(脆弱性資産プロセス)
  - 民間企業が発見ないし購入して資産として利用
    - ネットワーク傍受ツールの開発に利用
  - サイバー犯罪集団が発見ないし購入して利用

米国政府の脆弱性資産プロセス(VEP)

(Vulnerabilities Equities Policy and Process)

- オバマ政権が策定；非公開
  - 大統領府のブログ記事「Heartbleed: Understanding When We Disclose Cyber Vulnerabilities」(2014年4月28日)
    https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities
  - 情報公開請求
    https://www.eff.org/document/vulnerabilities-equities-process-january-2016

- トランプ政権が改訂して2017年11月15日に公表
  https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF (政権交代によりURLが変更か？)
  - VEPの運用の透明化が期待されていたが進まないまま政権交代

米国政府の脆弱性資産プロセス(VEP)の概要

- 10の省庁を指定し，それぞれの省庁がVEPに関する代表者(PoC)を指名
- PoCから構成される会議体ERB(資産レビュー会議)を設置
- VEPやERBの事務局をNSAが務める

- 米国政府機関が発見または購入した脆弱性情報で公知になっていない新しいものをVEPに登録する
  - 研究者や製品開発ベンダーが発見した脆弱性はVEPの対象外
- ERBが毎月の会議でVEPに登録された脆弱性を次の3つに振り分ける：1) 公表する， 2) 公開を制限する， 3) 判断を延期する

- VEP事務局(NSA)はPoCに年次報告を行う

脆弱性に関するまとめ

- 公表された脆弱性には…
  - アセットオーナーが影響を評価し必要な対策の実施を！
  - IIoTの導入やクラウドとの接続，遠隔アクセスなどの利用拡大に伴い脆弱性対策が必須に
- 公表されているのに情報を得にくいNディ脆弱性には…
  - 製品開発ベンダーにおける対処に期待
  - ソフトウェア部品表が入手できれば，それに基づいて影響評価を！
- 公表されない脆弱性には…
  - 潜在的な可能性を念頭に多層防御でICSの保護を！

- ☞ IEC 62443の標準化作業が一巡し，改版に向けた検討へ
- ☞ セキュリティ認証は対象がICS製品からICSシステムへ
- ☞ ICSの開発プロセスへの認証への関心が高まる

標準化や認証に関する動向

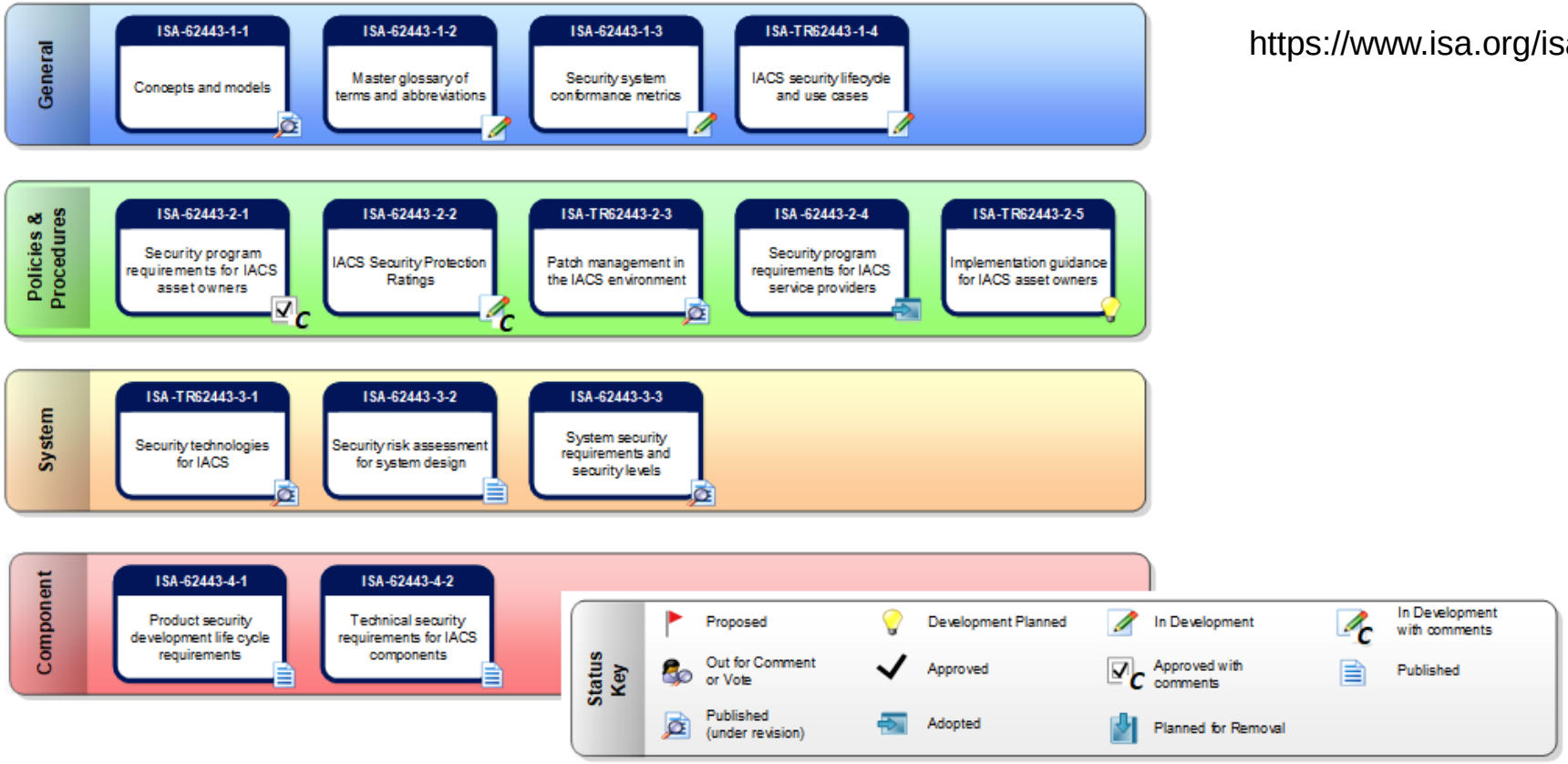
IEC 62443 (ISA 62443) シリーズの整備

2020年に新たな1つの標準

- **IEC 62443-3-2:2020**
  Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design
  1. **対象システムをゾーンとコンジットに分割**
  2. **各ゾーンとコンジットに対するリスクを評価**
  3. **各ゾーンとコンジットに対する目標のセキュリティ水準を設定**
  4. **セキュリティ要件を文書化**

- IEC 62443-2-1:2010 ⇒ 改訂完了間近

IEC 62443 (ISA 62443) シリーズ



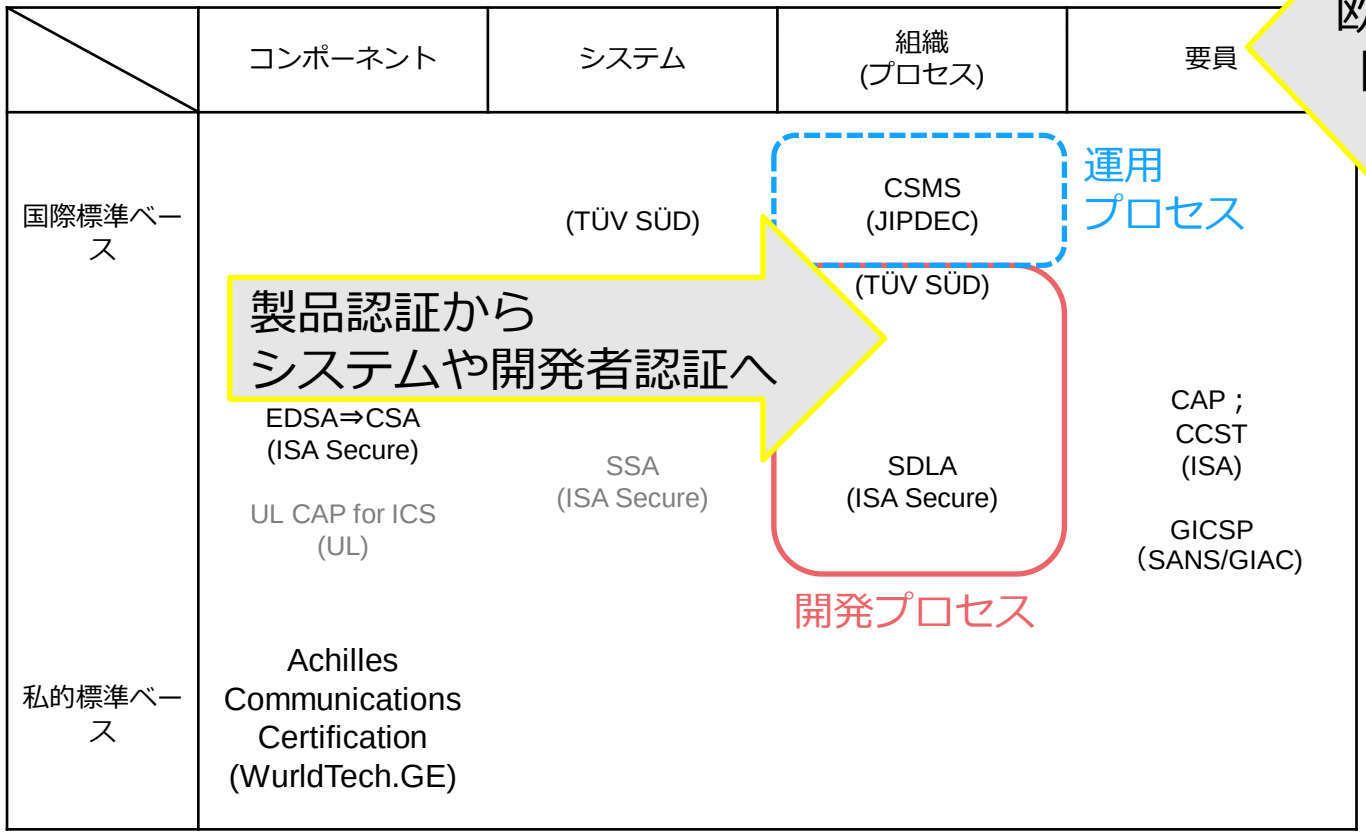
https://www.isa.org/isa99/

IEC 62443 (ISA 62443) シリーズの普及活動

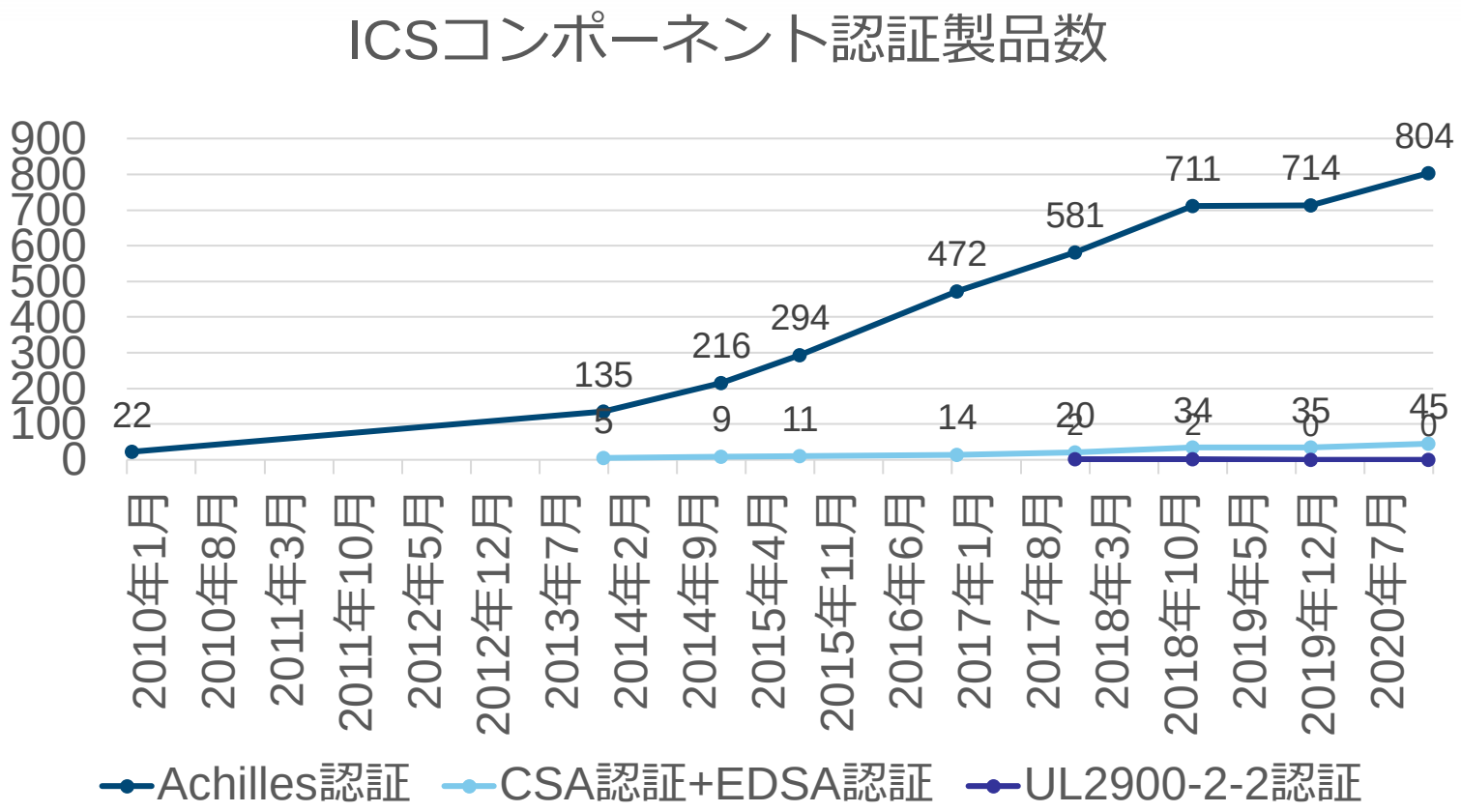
- ISAが2019年に設立したISA Global Cybersecurity Allianceが普及活動
  - Quick Start Guide to ISA/IEC 62443 (要登録)
    https://gca.isa.org/isagca-quick-start-guide-62443-standards
  - Guide to Security Lifecycles in ISA/IEC 62443 (要登録)
    https://gca.isa.org/isagca-security-lifecycles-62443
  - IACS Taxonomy Glossary
    https://gca.isa.org/hubfs/21-29%20-%20ISAGCA/ISAGCA-IACS%20Taxonomy%20Definitions%20of%20Terms.pdf
  - IACS Principal Roles and Responsibilities
    https://gca.isa.org/hubfs/21-29%20-%20ISAGCA/ISAGCA-IACS%20Roles%20and%20Responsibilities.pdf

- 日本におけるJIS化？

ICSセキュリティに関する認証の全体像



認証を受けたICSコンポーネント製品数の推移



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100製品近く増えて，804製品に

- EDSA＋CSA認証は，1年で11製品が認証され，45製品に
  - 11製品はすべてが海外ベンダーの製品
  - 2020年に新たに認証された11製品の認証水準の内訳は：

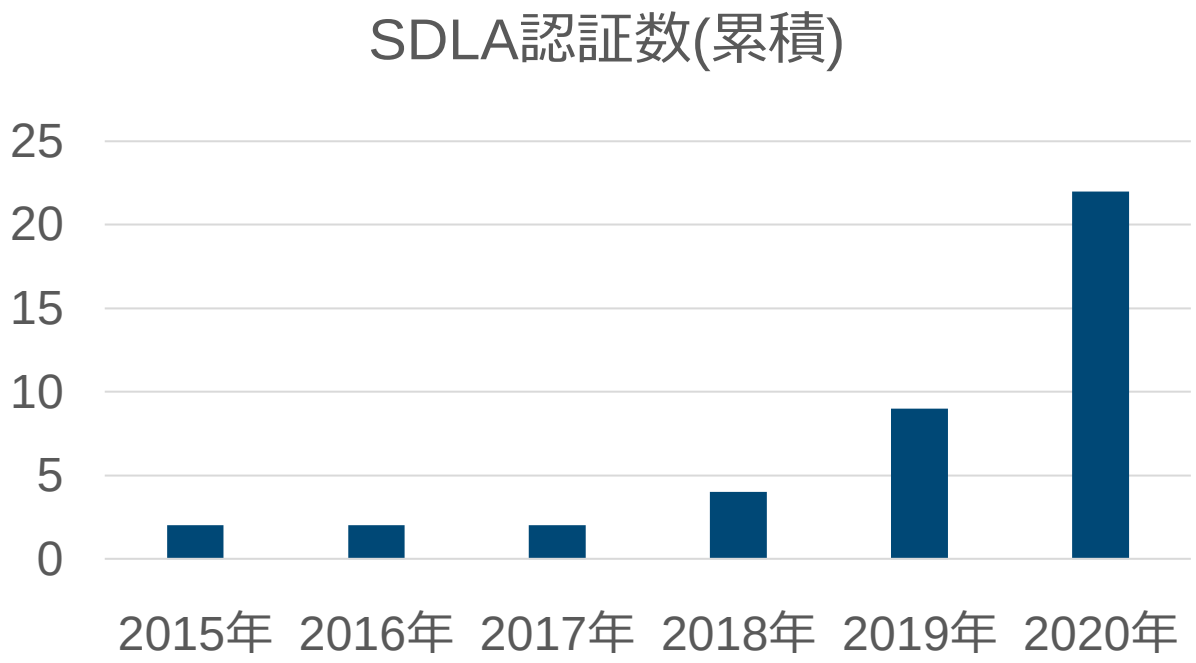
認証水準	製品数
EDSA 2.0.0 Level 2	3
EDSA 2.1.0 Level 1	1
EDSA 3.0.0 Level 1	6
CSA 1.0.0 Level 1	1

EDSA：
Embedded Device Security Assurance

CSA：
Component Security Assurance

開発プロセスの認証への関心が高まる

- SDLA (Security Development Lifecycle Assurance) 認証



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

サプライチェーンと ICSセキュリティ

中国企業が製造した大型変圧器に関する議論

- 5月1日に電力基幹システムのセキュア化に関する大統領令
  - 国防上のリスクが大きい電力業界での海外製品の利用を制限
  - この大統領に関して5月12日にエネルギー省からFAQ
    https://www.energy.gov/sites/prod/files/2020/05/f74/DOE%20BPS%20EO%20FAQ.pdf
- 5月27日にWall Street Journal紙が報道：
  https://www.wsj.com/articles/u-s-seizure-of-chinese-built-transformer-raises-specter-of-closer-scrutiny-11590598710
  - 2019年夏に中国のJSHP社製の大型変圧器がヒューストン港で荷揚げ後に押収されてSandia国立研究所にトラック輸送された
  - その後の追加情報がなく，押収の理由も不明
- 「変圧器にバックドアが組み込まれていた」との憶測が沸騰
  - SANS ICSからは憶測に否定的な分析論文：
    https://ics.sans.org/media/SANS_ICS_DUC_7_supply_chain_attacks_on_US_electric_infrastructure.pdf

SolarWinds社製Orionのアップデート汚染

まだ全容が解明されておらず，現在も調査が進行中

- SolarWinds社製のOrionは，ネットワーク管理用のソフトウェア製品
  米国を中心に広く，ネットワークの設定や監視に利用されている
- SolarWinds社が侵入されて，ソフトウェア製品Orionのアップデートが
  作られるたびに，バックドアをアップデート中に埋め込んで
  汚染するためのマルウェアがインストールされていたと
  FireEye社が12月13日に発表
  https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
  - 汚染したアップデート(コード署名付き)が2020年春頃から提供されていた
  - 米国の主要官庁や大企業を含む世界中のOrion利用組織が攻撃を受けている
    可能性を指摘
  - FBI等の関連官庁やMicrosoft社とも連携して調査中

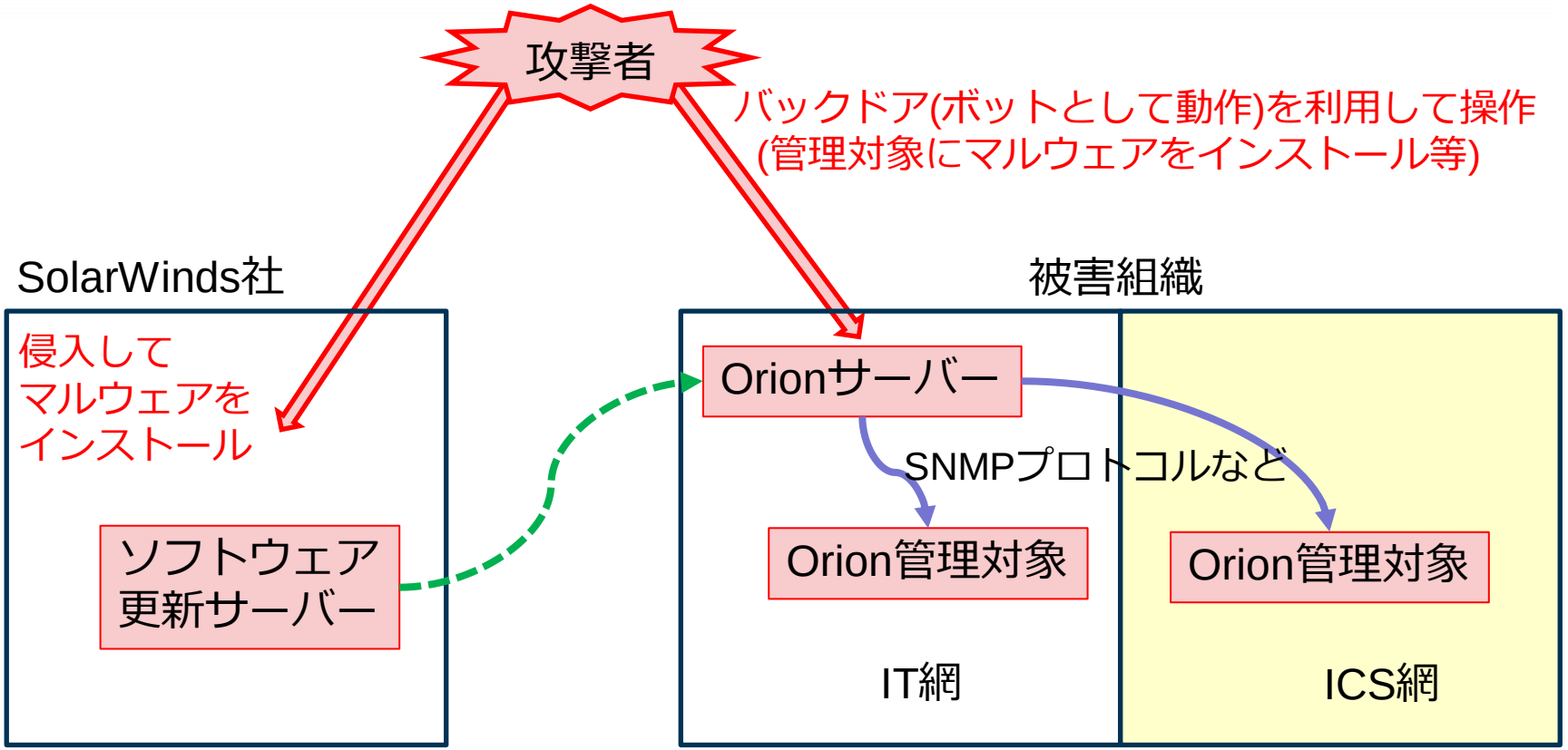
SolarWinds社製Orionのアップデート汚染(つづき)

- 米国CISAが12月13日に緊急指令21-01「SolarWinds社製Orionのコード汚染の対策」を公表し，その後も随時更新ないし追加情報
  https://cyber.dhs.gov/ed/21-01/

- トランプ政権が連邦政府への侵入元がロシア(APT29, CozyBear)だと公表
  https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html
  - Trump大統領は「騒ぎすぎ；中国かも知れない」とツィート
  - 国務長官が改めて「ロシアによる攻撃は明白」と強調

- バイデン大統領が諜報機関に影響の評価調査を指示
  https://www.securityweek.com/biden-orders-intel-agencies-provide-full-assessment-solarwinds-hack

SolarWinds社製Orionのアップデート汚染の影響



サプライチェーンのセキュリティに関する参考資料

- NIST IR 8272 サプライチェーン・リスクの影響分析ツール
  https://csrc.nist.gov/publications/detail/nistir/8272/final
- NIST IR 8276 サプライチェーン・リスク管理の主要プラクティス (草案)
  https://csrc.nist.gov/publications/detail/nistir/8276/draft
- ENISAがIoTのサプライチェーン・セキュリティのガイドライン
  https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things/at_download/fullReport
- NERCがFAQを公表
  https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Supply%20Chain%20Small%20Group%20Advisory%20Sessions%20FAQs%20%E2%80%93%20December%202020.pdf
- FERCとNERCが共同で組み込まれている通信モジュールの製造元を特定する手法
  https://www.nerc.com/pa/comp/CAOneStopShop/Joint%20Staff%20White%20Paper%20on%20Supply%20Chain_07312020.pdf

まとめ

1. Covid-19とICSセキュリティ
2. ICSのセキュリティ・インシデントの動向
3. ICSの脆弱性の動向
4. 標準化と認証制度の動向
5. サプライチェーンとICSセキュリティ

2021年が
Covid-19の克服と
ICSセキュリティの深耕，そして
安全な制御の年となることを祈りつつ…

ご清聴ありがとうございました

お問合せ、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