制御システム・セキュリティの現在と展望

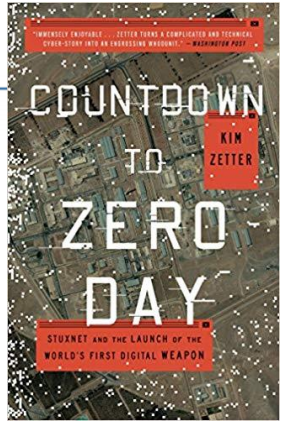
～ この1年間を振り返って ～

JPCERTコーディネーションセンター
ICSR　技術顧問
宮地利雄

- ☞ Stuxnetの発見から10年
- ☞ SHODANのサービス開始から10年
- ☞ 軍事的なサイバー戦略の変化
- IIoT等の新技術普及の中で世界の注目を集める五輪の年

ICSセキュリティにとって節目の2020年

Stuxnetの発見から10年



- ICSを狙って開発された初めてのマルウェア
  - イランの核計画を妨害するために計画されたと言われている
    Kim Zetter: Countdown to Zero Day
  - Stuxnetの構造と動作に関する情報は広く共有されている
    Symantec: W32.Stuxnet Dossier
    https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
  - Siemens社製のPLC上の制御ロジックを改ざんする能力をもつ

オランダの諜報機関が攻撃に関与していたとの新情報も (9月3日)
https://news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html

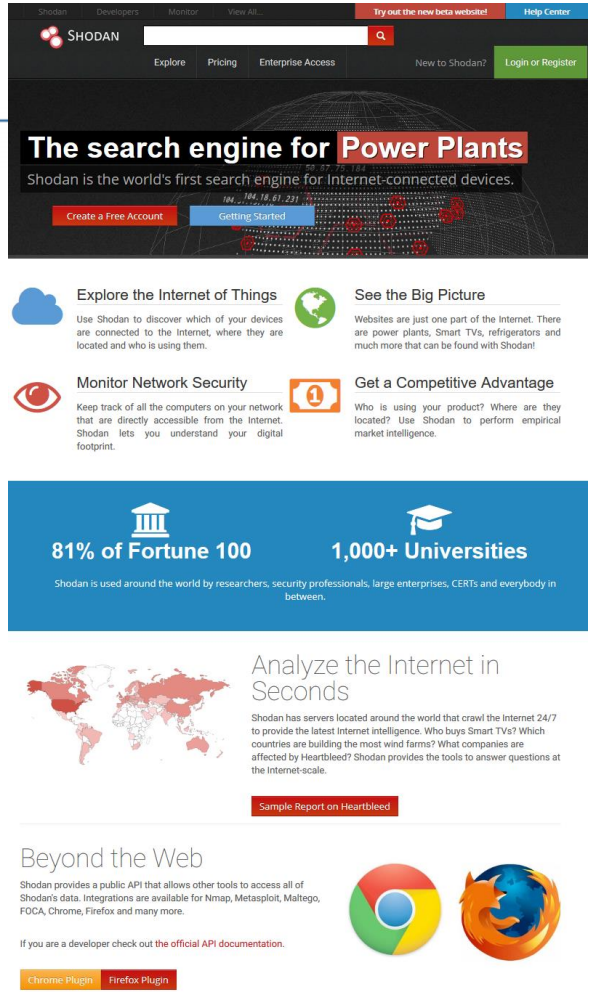
- 研究としてStuxnetの仕組みを他社製PLCに移植する試み (2020年1月)
  Airbus researcher explores 'Stuxnet-type attack' for security training
  https://www.cyberscoop.com/stuxnet-type-attack-airbus-cybersecurity/
  - Schneider社製の古いPLCを使った試作に成功
  - Stuxnetの詳細情報がPLCのセキュリティ強化に生かされてきたのか…

SHODAN (https://www.shodan.io/)

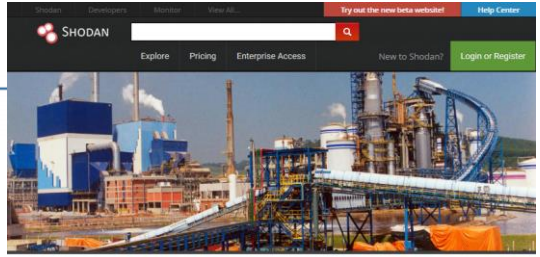
- インターネット上のコンピュータやルータ等を検索できるウェブ・サービス
  - インターネット直結ならICS機器も検索対象
- John Matherly氏が個人的な趣味で開発し2009年後半から公開

  Cyber search engine Shodan exposes industrial control systems to new risks (Washington Post 2012年6月4日)
  http://www.washingtonpost.com/investigations/cyber-search-engine-exposes-vulnerabilities/2012/06/03/gJQAIK9KCV_story.html
- 公開直後から米国ICS-CERTがICSセキュリティへの脅威として警鐘

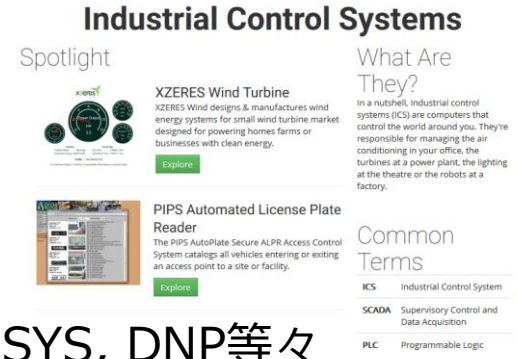
  Analysis of “SHODAN ー Computer Search Engine” (2010年1月25日)
  ICS-ALERT-10-301-01： Control System Internet Accessibility (2010年10月28日)



恐るべし！ SHODAN



- 製造ベンダーや機種を指定しての検索が可能
- 公表されている脆弱性も簡易に参照できる



- ICS向けの拡張機能を整備
  SHODAN Industrial Control Systems
  (https://www.shodan.io/explore/category/industrial-control-systems)
  - ICS固有のプロトコルにも順次拡張されてきている
    Modbus, BACnet, EtherNet/IP, HART/IP, CODESYS, DNP等々
  - 製造ベンダー固有のアクセス保護も回避
    - 特殊なtelnetクライアントにだけ反応する機器の一部も検索可能

- コンピュータ等の検索サービスがSHODAN以外にも登場

SHODAN利用例

ある国内ベンダーの名前を
指定して検索してみると…

インターネット全体で
181台の機器が見つかった

国別には日本が11台等

サービス別には
EtherNet/IPが130台等

ICS機器をインターネット等に接続する場合には…

- ICS機器にアクセスできる範囲(IPアドレス)を最小限に制限する
  - SHODANのクローリングを拒絶する
- ソフトウェア/ファームウェアに対して適切に脆弱性(パッチ)管理
  - 踏み台を介したICS機器への攻撃にも備える
- 遠隔保守を目的としたインターネット接続も定期的に棚卸して見直す

軍事的なサイバー戦略の変化

- 米国国防総省が2018年にサイバー戦略を改定し，
  従来からの「自由で開かれたインターネット」を維持しつつ，
  「Defending Forward」や「Persistence」，
  「重要インフラ防御」の考え方を導入

従来型装備より安上がり；
サイバー攻撃の実効性が上昇

- 「Defending Forward」の定義はないが，次を含むとされている：
  - 実戦に備えた諜報活動
  - 悪意あるサイバー活動を根源(攻撃元?)で阻止する
  - 軍事衝突の水準を低下させる

サイバー空間では
迎撃的な防衛では
有効性が低い

[参考] The 2018 DOD Cyber Strategy: Understanding 'Defense Forward' in Light of the NDAA and PPD-20 Changes
https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes

軍事的な抑止力のためのサイバー作戦

前のめりに傾く
サイバー空間の
防衛

- サイバー的な手段であっても，甚大な被害があれば，戦争行為とみなされる
  - ハッキングも，甚大な被害が無ければ，戦争行為でない(？)
- サイバー攻撃を受けてから防衛することは困難であり，攻撃能力を保有することを通じた「抑止力」に期待せざるを得ない

- 米国がロシアの電力網に対するオンライン攻撃をエスカレート
  U.S. Escalates Online Attacks on Russia's Power Grid (New York Times； 6月15日)
  https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html
- 米国がイランの兵器システムにサイバー攻撃
  US launches cyber-attack on Iranian weapons systems (SC magazine UK； 6月24日)
  https://www.scmagazineuk.com/us-launches-cyber-attack-iranian-weapons-systems/article/1588587

入り乱れる国家のサイバー作戦と犯罪者集団の活動

- サイバー攻撃では行為者特定(attribution)が非常に難しい
- 国家によるサイバー作戦と犯罪者集団によるサイバー攻撃がともに高まっていると見られる

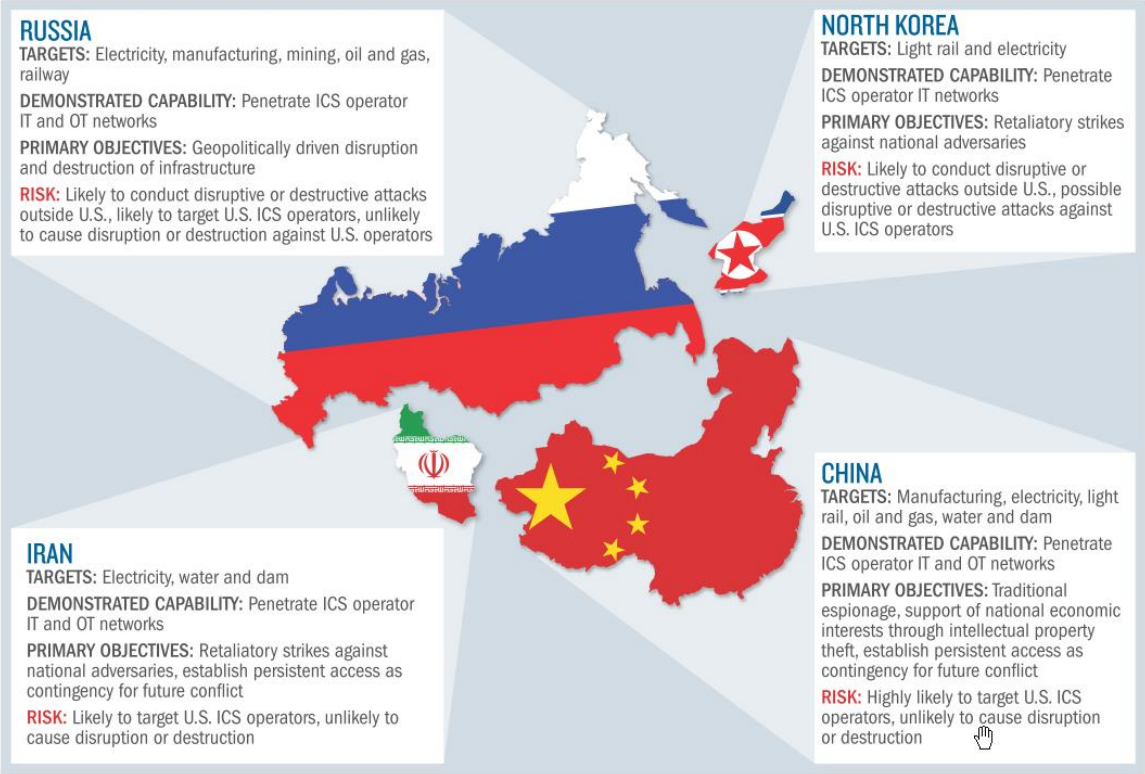
- 世界の企業の27%(米国企業では36%)が2019年に国家によるサイバー攻撃を受けたとの報告書もある
  Radware社： Protecting what you can't see
  https://discover.radware.com/c/ERT-Report_2020

- MITREが公表したATT&CK ICSではICSを狙う10の攻撃集団を記載
  https://collaborate.mitre.org/attackics/index.php/Groups

MITRE社ATT&CK ICSに記載された攻撃集団

ALLANITE
Dragonfly
Dragonfly 2.0
Sandworm
XENOTIME

APT33
HEXANE
OilRig
Leafminer



Lazarus group

他に米国の
Equation

図部分の引用：Booz Allen Hamilton社
https://www.boozallen.com/insights/2016/06/industrial-cybersecurity-threat-briefing

サイバー戦争の時代への心構え

- 物理的な兵器によるミサイル攻撃等とは異なり，
  国が個別のサイバー攻撃から民間組織を守ることはほとんど
  期待できない
  - 民間組織が自身を守る対策をとらなければならない

- 国家によるサイバー攻撃と犯罪集団によるサイバー攻撃との違いは
  事実上ない

- 攻撃集団の動向や手口等に関する情報への感度を高めて
  サイバー攻撃への備えをしておきたい

・ ICSを狙って起こされた重大なインシデントなく経過

☞ ICS上のインシデント件数が世界的には急増か

☞ 米国の電力網の障害報告で初の「サイバー事案」

☞ ランサムウェアが変容；散発的なICSへの影響も

☞ その他のマルウェア感染による生産停止も

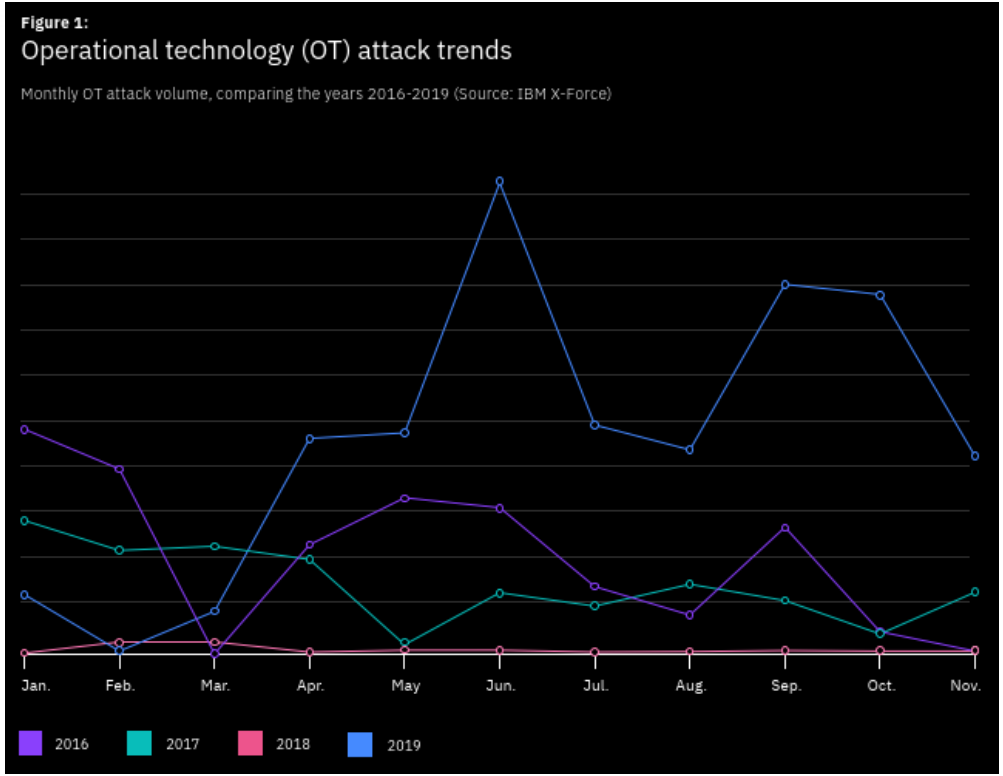
インシデントの動向

ICS上のインシデント件数が世界的には急増か

IBMセキュリティのX-Force Threat Intelligence Index 2020

https://www.ibm.com/security/data-breach/threat-intelligence

- 2018年から2019年にかけてICS上のインシデント件数が20倍に増加
  - ICS製品の既知の脆弱性を狙いパスワード・スプレー攻撃
  - 2020年もこの傾向が続く



出典: X-Force Threat Intelligence Index 2020

米国の電力網の障害報告で初のサイバー事案

- 米国の「電力緊急インシデント障害報告書」に
  初の「サイバー事案」の記載が登場
  https://assets.documentcloud.org/documents/6535023/sPower-FOIA.pdf

- 再エネ発電のsPower社の監視網を構成する多数のVPN機器に
  既知の脆弱性をついたDoS攻撃（2019年3月5日)
  - 個々の機器は5分程度で自動再起動したが，約10時間にわたり次々と停止

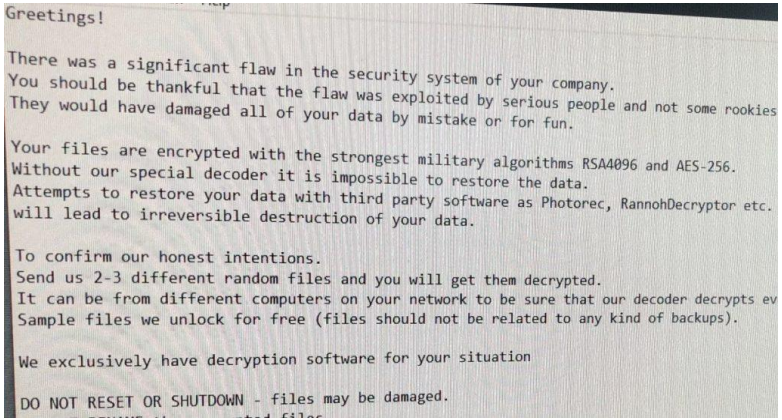
- 送電や配電への影響はなかった

[参考] First-of-a-kind U.S. grid cyberattack hit wind, solar [E&E news； 10月31日]
https://www.eenews.net/stories/1061421301

出典： E&E News

Norsk Hydro社のランサムウェア感染 (1/2)

- Norsk Hydro社はノルウェイの金属エネルギー巨大企業
  - アルミニウム製造では世界最大
- ランサムウェアLockerGogaに感染して操業が停止 (3月19日)
  - 米国拠点が最初に感染し，その後，他の拠点にも感染が拡大
    40ヶ国3.5万人の従業員，数千台のコンピュータに影響
  - まったく自動制御できなくなり，人手による操業だけに追い込まれた
  - 身代金を支払わない方針で対処
  - 概ね約1週間をかけて復旧したが，
    一部の部門ではさらに操業停止が続いた
  - 最終被害額：6,000～7,100万ドル



Hydro社への身代金要求

出典：https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

Norsk Hydro社のランサムウェア感染 (2/2)

- 非常事態として会社幹部が先頭に立って対応
  - すみやかに身代金を支払わない方針を決定
  - 被害と復旧状況を迅速かつオープンに広報
  - 事業部門，財務，広報のそれぞれの担当役員による記者会見も
  - 顧客企業への情報提供

- 保険による補償： 2020万ドル (第4四半期)

- ランサムウェアに関する広報活動に対し
  欧州最優秀広報賞(非常事態広報部門)を受賞
  https://eu-pr.excellence-awards.com/best-of-2019/

出典： Hydro社の復旧状況広報

その他にも相次いだランサムウェア被害 (1/2)

- ベルギーの ASCO industries 社がランサムウエア感染で事業に深刻な影響 (6月23日)
  http://www.asco.be/news
- ドイツに本拠を置く ICS 機器ベンダ Pilz 社がランサムウエアに感染し76か国の拠点で業務に影響 (10月13日)
  https://www.zdnet.com/article/major-german-manufacturer-still-down-a-week-after-getting-hit-by-ransomware/
- メキシコの石油公社 (Pemex) がランサムウエアに感染 (11月10日)
  https://www.bleepingcomputer.com/news/security/mexicos-pemex-oil-suffers-ransomware-attack-49-million-demanded/
- 米国の Southwire 社がランサムウエアに感染し、製造と出荷に支障 (12月9日)
  https://www.bizjournals.com/atlanta/news/2019/12/11/cybersecurity-incident-at-metro-atlantas-4th.html

いずれの場合も操業の深刻な中断や混乱があった事案であるが，ICSまで感染が拡大していたかどうかは明らかでない

その他にも相次いだランサムウェア被害 (2/2)

- 石油ガス業界で2019年11月以降にランサムウェアRyukへの感染事案が5件発生(うち少なくとも2件はICSにも影響)
  https://www.eenews.net/energywire/stories/1062188535
  - 同マルウェアに関する注意喚起を米国沿岸警備隊も12月に発行
    https://assets.documentcloud.org/documents/6594141/MSIB-10-19.pdf
    - 感染の事後対処のために30時間にわたり操業が阻害された

- 制御システムを狙う機能をもつランサムウェアEkans(別名Snake)の登場
  https://dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/
  - 被害事例の報告はまだ無さそう

イーカンズはポケモン「アーボ」の英語名

深刻化するランサムウェア攻撃

- コンピュータやデータを利用できない状態にして復旧のための「身代金」の払込みを要求
  - 身代金を払い込んでも復旧できないケースもある
  - データを持ち出していて「漏洩させるぞ！」との脅迫も

- 狙う対象が個人から法人にシフト
  - 身代金の金額が百万円～数億円になることも
    - 米国内の年間被害総額の見積りが750億ドル
  - 他のマルウェア等と組み合わせた標的型の攻撃に

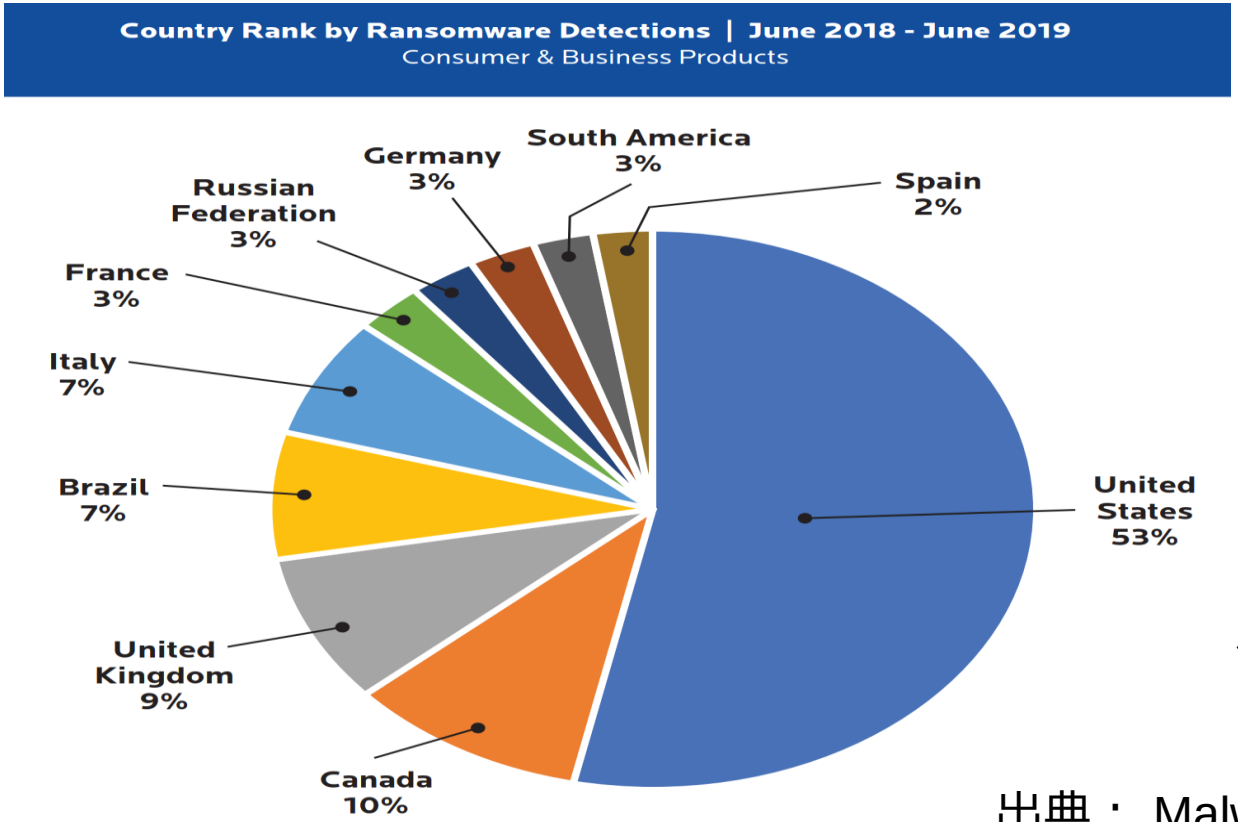
ランサムウェアによる被害

(Coveware社による2019年10～12月期の統計)

- 身代金の平均支払額： 84,116ドル
  (前四半期比104%上昇)
- 平均ダウン時間：16.2日間 (前四半期は12.1日)
- ほとんどがBitcoinによる身代金の支払いを指定
- 身代金を支払った場合：
  - 暗号化の復号ツールが届いた割合： 98%
  - 届いた復号ツールで復旧できた割合： 97%
    (全四半期は94%)

69%とする報告書も
ProofPoint: 2020
State of the Phish

ランサムウェア被害には地域的な偏りも



検知数ベースで
半分以上が米国

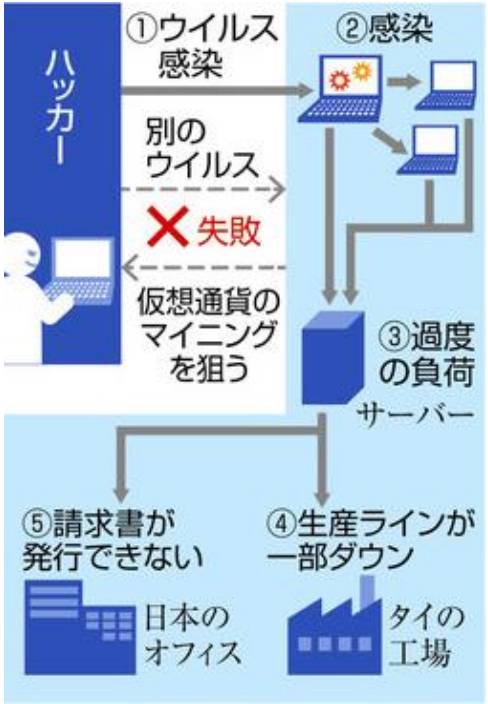
出典： MalwareByte報告書

ランサムウェアの動向に関する参考資料

- MalwareBytes： Cybercrime Tactics and Techniques: Ransomware Retrospective (8月9日)
  https://resources.malwarebytes.com/resource/cybercrime-tactics-and-techniques-ransomware-retrospective/
- Sophos: How Ransomware Attacks (11月14日)
  https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-ransomware-behavior-report.pdf
- EMSISoft: The State of Ransomware in the US: Report and Statistics 2019 (12月12日)
  https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/
- Coveware: Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate (2020年1月23日)
  https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate

日本企業の海外拠点でマルウェア感染

- 日本の眼鏡レンズ・メーカーのタイにある主要工場が仮想通貨をマイニングするマルウェアに感染し2月末に３日間にわたり生産ラインの一部がダウン
  - 仮想通貨マイニング・マルウェアに感染するとCPU負荷が高まり，本来のアプリケーション・ソフトウェアが動かなくなる
  - 当該企業によれば「マルウェア感染活動の段階で異常を検知し復旧」



出典： 中日新聞
https://www.chunichi.co.jp/article/front/list/CK2019040602000308.html

サイバー・インシデントによる損害の主な例

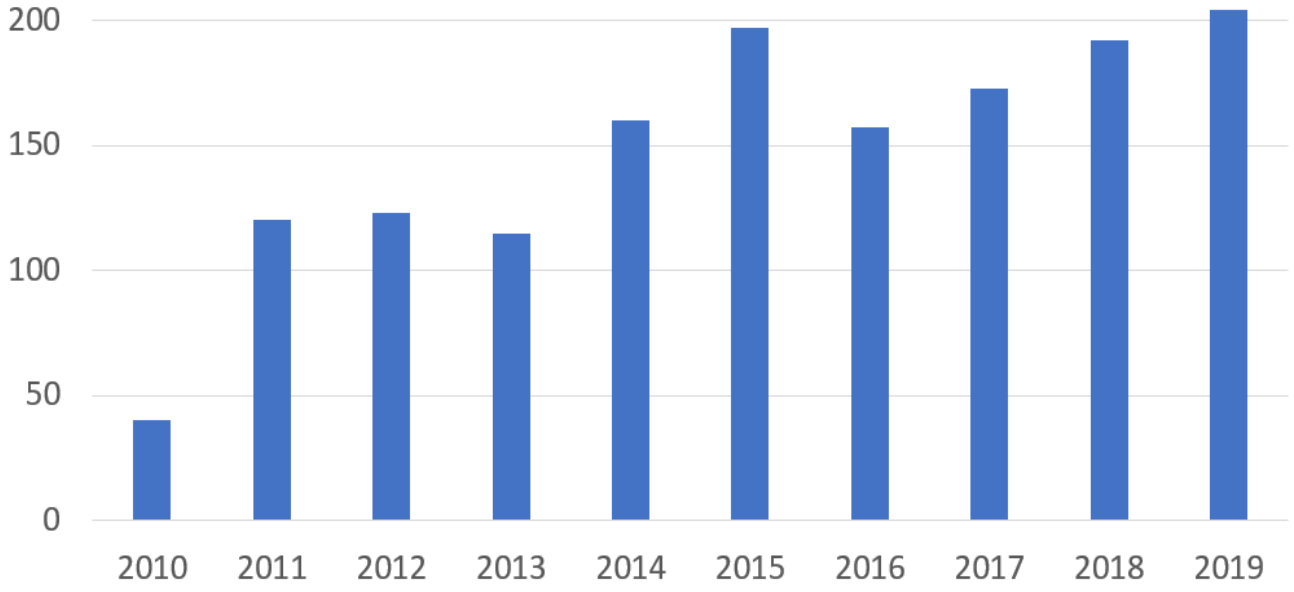
企業名	損害額	年	記事
Duke Energy	1,000万ドル	2016	電力事業者の規制NERC CIPへの違反に対する罰金
A.P. Moller Maersk	3億ドル	2017	破壊型マルウェアNotPetyaに感染；運輸業務の中断
Mondelez	1.9億ドル	2017	破壊型マルウェアNotPetyaに感染；スナック菓子製造業務の中断
FedEx	4億ドル	2017年	破壊型マルウェアNotPetyaに感染；欧州の運送業務の混乱
Merck	8.7億ドル	2017	破壊型マルウェアNotPetyaに感染；医薬品製造業務の混乱
Reckitt Benckiser	1.29億ドル	2017	破壊型マルウェアNotPetyaに感染； 保健用品製造業務の混乱
Norsk Hydro	7100万ドル	2019	ランサムウェアLockerGogaに感染； アルミニウム等製造業務の混乱

- ☞ 毎年に公表される脆弱性の件数は200件前後で安定
- ☞ ICSベンダーにより多様な脆弱性への取組み姿勢
- ☞ N-day脆弱性などICS製品の脆弱性に関する課題あり

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

- 2015年以降のICS関連アドバイザリ件数は年に200件前後
- 他に，医療用機器の脆弱性(17年は16件，18年は31件，19年は25件)



2017年～2019年の件数はJPCERT/CCがカウントして作図
2016年以前の件数は： ICS-CERT Annual Vulnerability Coordination Report 2016
https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_FY%202016_Annual_Vulnerability_Coordination_Report.pdf

Positive Technologies社による動向分析

2019年4月11日公表：ICS vulnerabilities: 2018 in review

https://www.ptsecurity.com/ww-en/analytics/ics-vulnerabilities-2019/

- 企業のITインフラに侵入できれば，82%の場合ICSまで到達し，ICSの動作に影響を与えることが可能

Siemens社は原則として毎月第2火曜日に公表する方針への転換を宣言：
https://new.siemens.com/global/en/company/stories/research-technologies/cybersecurity/rhythm-for-security.html

- 脆弱性の公表件数では，Schneider社とSiemens社が突出
(脆弱性の絶対数というよりも脆弱性の開示に対する企業姿勢の違い)
- 公表された脆弱性の機器カテゴリによる内訳：
ICSネットワーク機器： 23%，HMI/SCADA: 23%，PLC/RTU: 21%
- インターネットに直結されたICS製品： 22.4万台 (前年比27%増し)
うち9.6万台が米国
  - 主にビル管理用か(?)

累積するN-day脆弱性問題

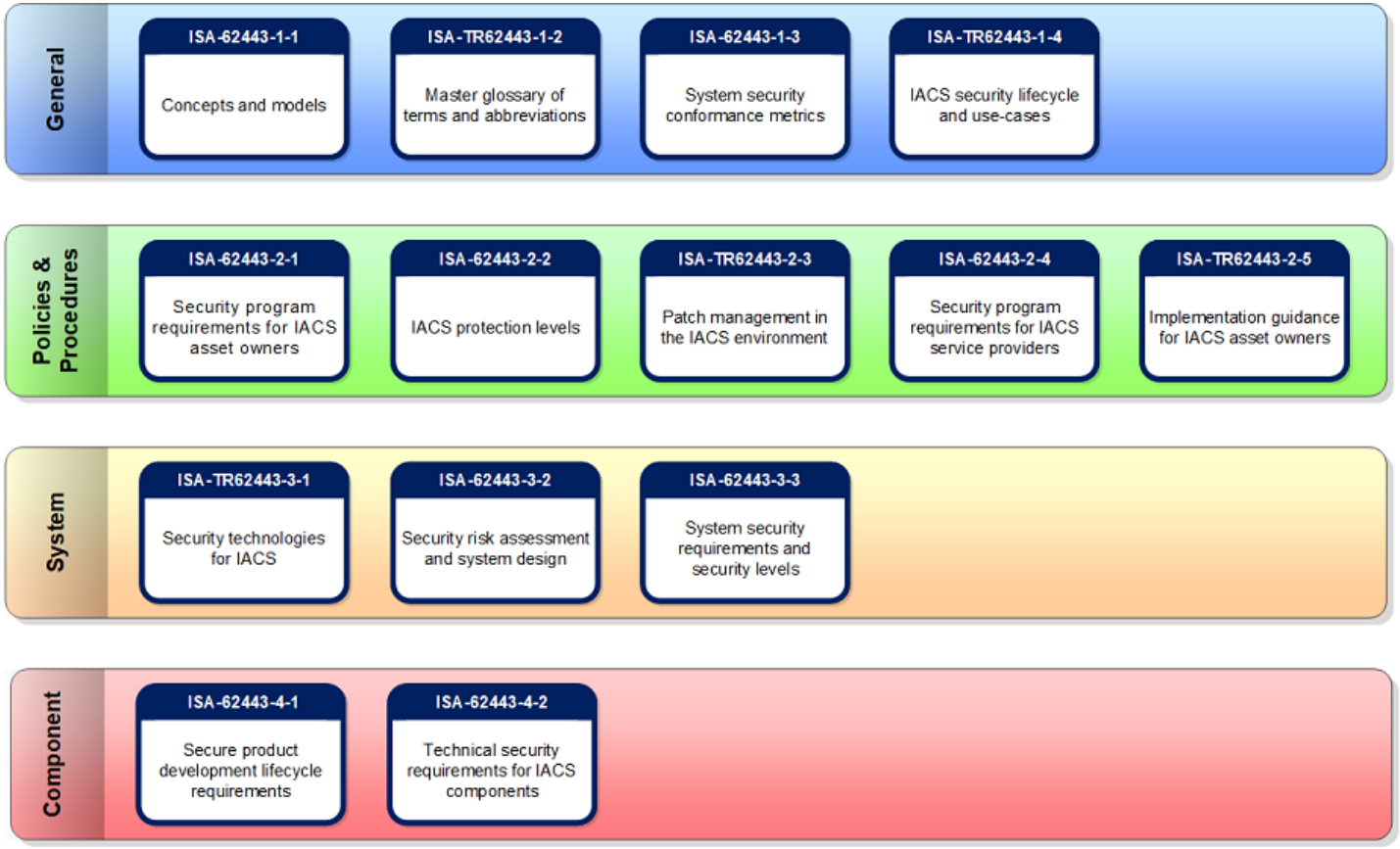
- ICSコンポーネントに組み込まれている多数の他社製ソフトウェア
  - CPU，OS，プロトコル・スタック，PLCの基本機能
- 他社製ソフトウェアに脆弱性が見つかり改修されれば
  ICSコンポーネントも対策が必要(パッチの適用など)だが
  多くのICSベンダーは手が回らず放置しているケースが多い
  - こうした脆弱性を「**N-day脆弱性**」と呼ぶ

- N-day脆弱性は攻撃者にとっては格好の攻撃ポイント
- アセット・オーナーはN-day脆弱性の存在を知ることも難しい
  - 製品のソフトウェア成分表(ソフトウェアBoM)を要求する声もある

☞ 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

標準化や規制に関する動向

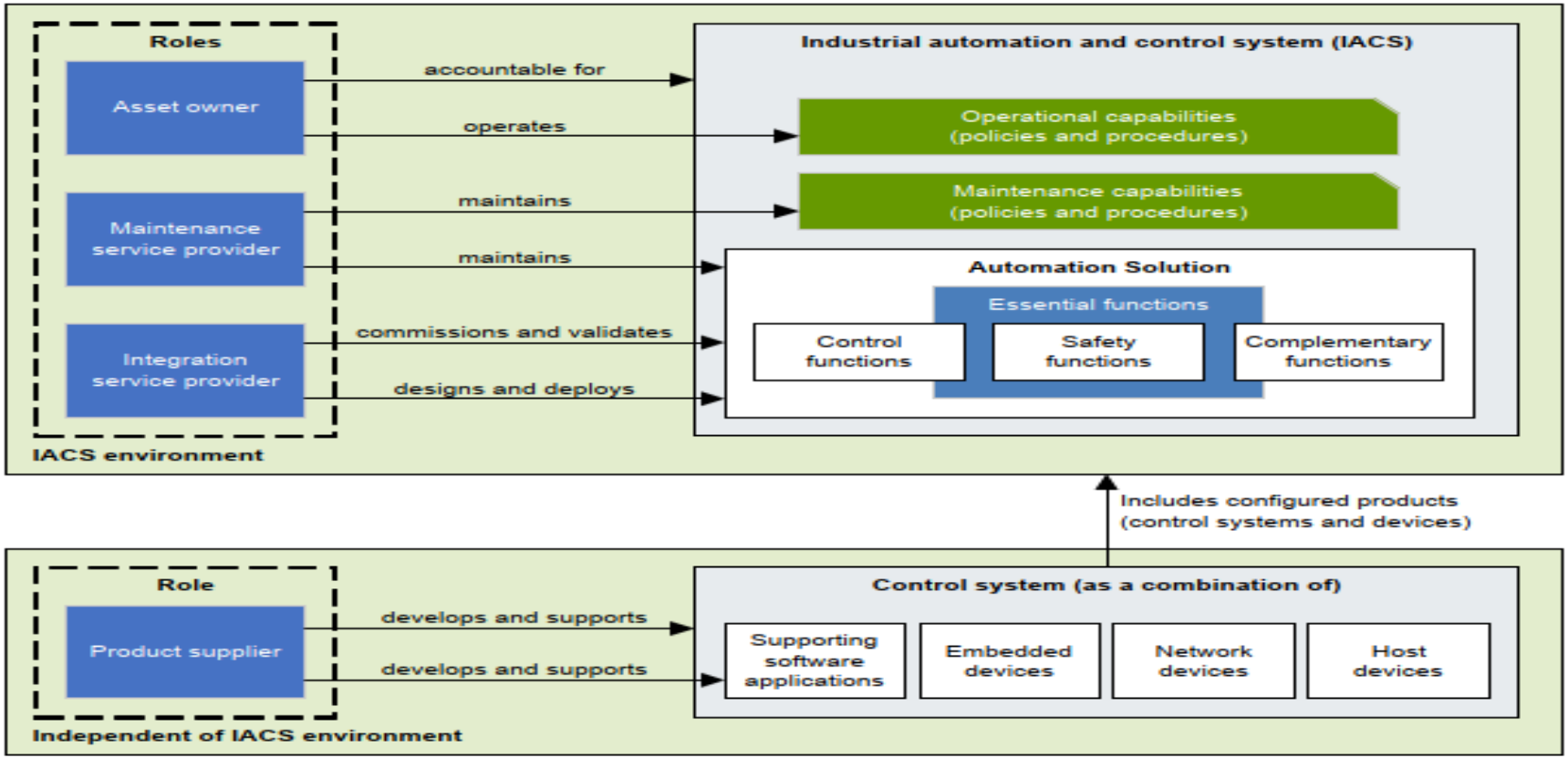
IEC 62443 (ISA 62443) シリーズ



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

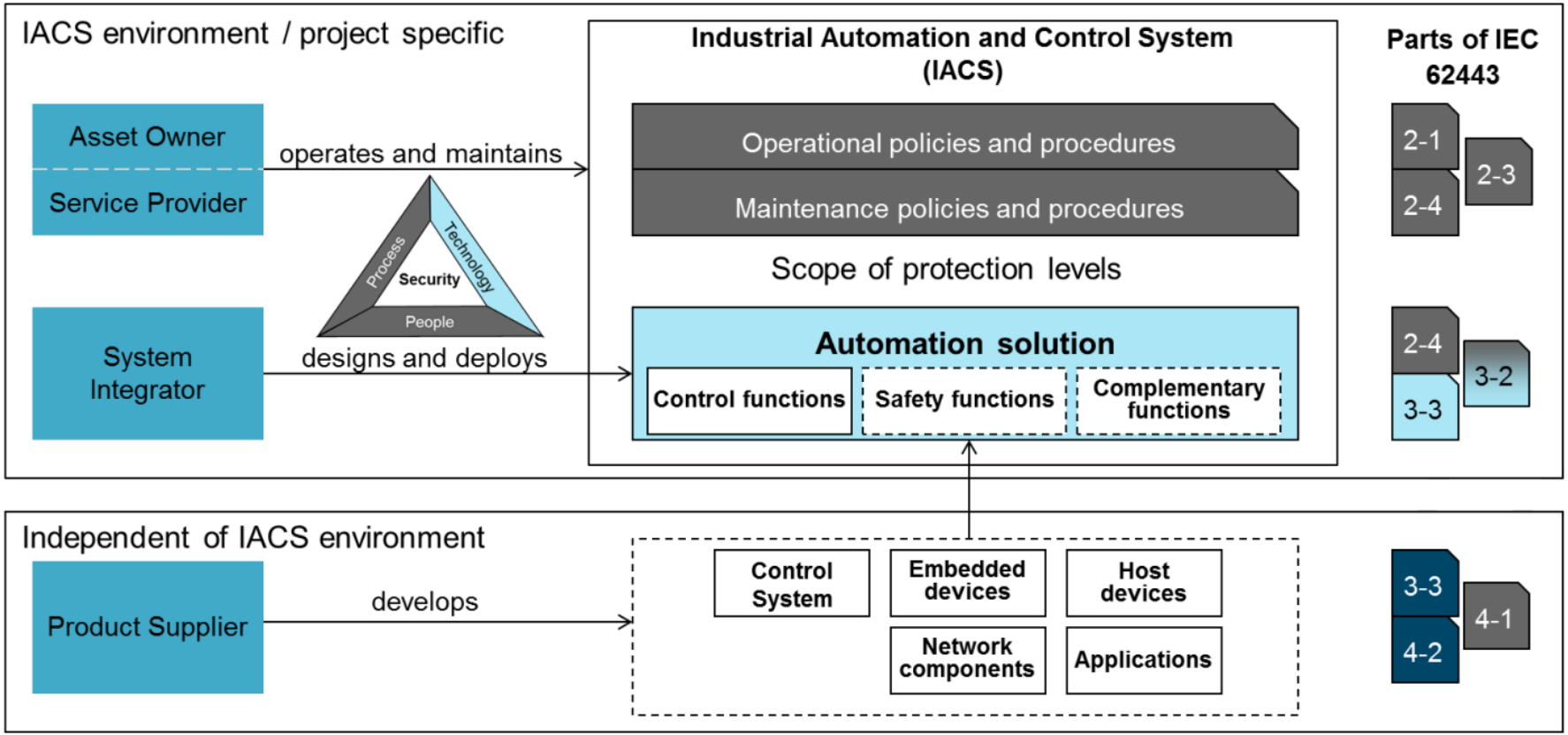
ICSにおける様々なプレイヤーの役割

出典： ISA 62443-2-1草案



IEC / ISA 62443の適用

出典： ISA 62443-2-2草案



ISA/IEC 62443 Part. 1 用語と概念

Security for industrial automation and control systems
初期の名称はIndustrial communication networks - Network and system security

Part	名称	概要
-1-1:2009	(TS) Terminology, concepts and models (改訂を検討中)	用語定義と概念モデル
-1-2	Master glossary of terms and abbreviations (作成中)	用語集
-1-3	System security conformance metrics	
-1-4	IACS security lifecycle and use-cases	

「：年」の表記を伴うものは発行済．年は発行年．

IEC / ISA 62443シリーズ

Part	名称	概要
-2-4:2015	Security program requirements for IACS service providers	サービス提供者要件
-2-5	(以前の-2-2が-2-5に番号変更) Implementation guidance for IACS asset owners	
-3-1:2009	(TR) Security technologies for industrial automation and control systems	セキュリティ用ツールと対策技術
-3-2	Security risk assessment and system design	
-3-3:2013	System security requirements and security levels	SL(セキュリティ水準)
-4-1:2018	Secure product development lifecycle requirements	製品開発要件
-4-2:2018	(ISAのみ) (IECは作成中) Technical security requirements for IACS components	コンポーネント要件

ISA/IEC 62443 Part. 3 システム

Part	名称	概要
-3-1:2009	(TR) Security technologies for industrial automation and control systems	セキュリティ用ツールと対策技術
-3-2	Security risk assessment and system design (作成中)	
-3-3:2013	System security requirements and security levels	SL(セキュリティ水準)

- セキュリティ水準(SL)を定義
- ISA SecureのSystem Security Assurance (SSA)認証のベースとされている
- これをベースにしてドイツが国内標準を整備

ISA/IEC 62443 Part. 4 コンポーネント

Part	名称	概要
-4-1:2018	Secure product development lifecycle requirements	製品開発要件
-4-2:2019	Technical security requirements for IACS components	コンポーネント要件

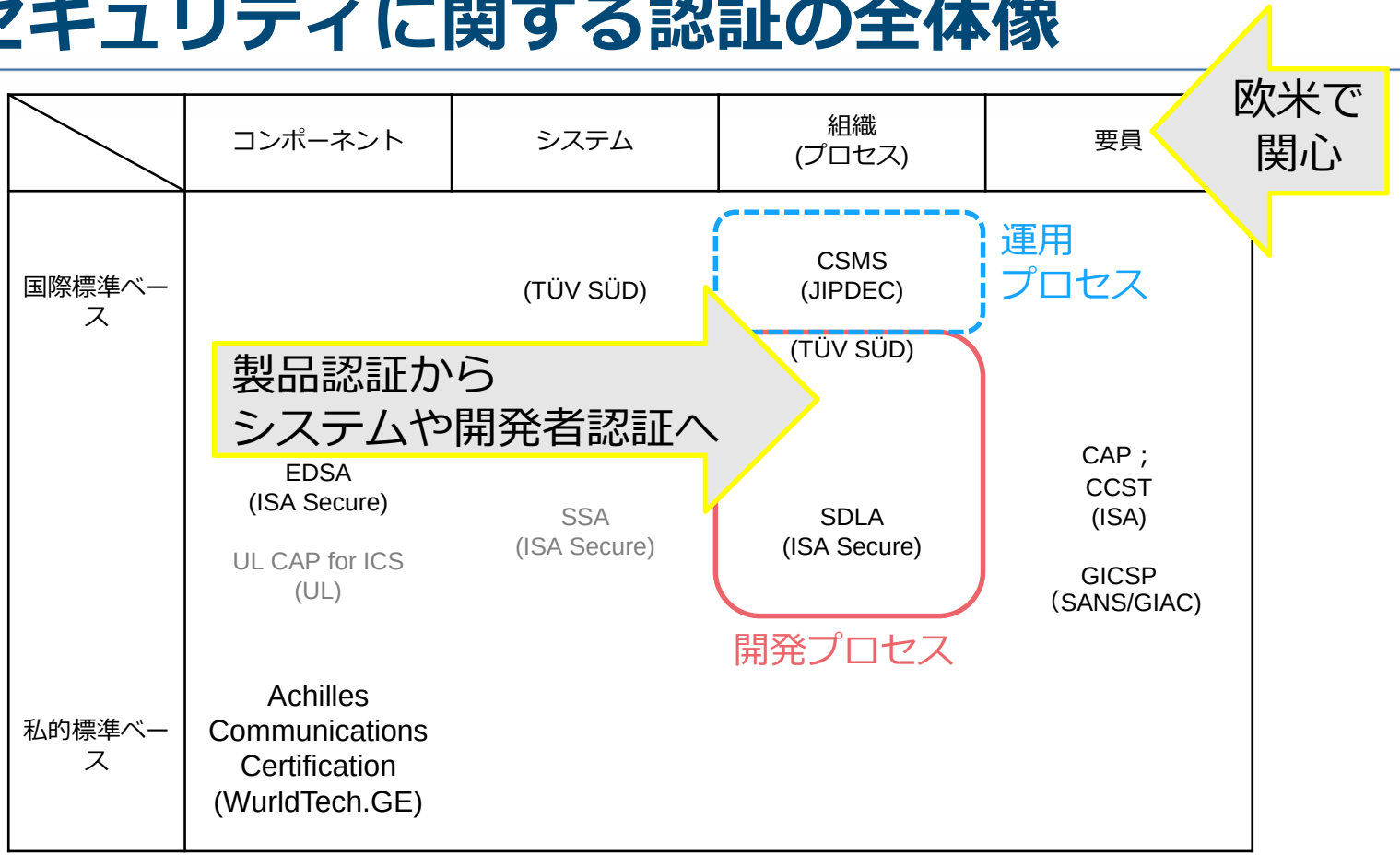
- ISA SecureのEmbedded Device Security Assurance (EDSA)認証のベースとされている

ISA/IEC 62443 Part. 5 要件プロファイリング

Part	名称	概要
-5-1:	Guidelines for drafting profiles (IECが作成中)	62443の要件に対する プロファイルの 概念と作り方

- プロファイルとは要件のサブセット
  - ―たとえば，PLC用，ヒストリアン用など…
- IEC CA (Conformity Assessment) Systemsが62443をベースにした認証制度を創設する準備とも見られている

ICSセキュリティに関する認証の全体像



コンポーネントに対する認証製品数は頭打ち

表示年時点での認証件数の総数

製品認証	2010年	2014年	2015年	2015年 9月末	2017年 1月	2018年 1月	2019年 1月	2020年 1月
Achilles Communications Certification	22	135	216 (GE社が買収)	294	472	581	711	714
EDSA (ISA ISCI)	0	5	9	11	14	20	34	35
UL 2900-2-2					0	2	2	0

2010年時点の認証製品数はRagnar Schierholz氏らによる”Security Certification – A critical review”による

- コンポーネント製品に対するセキュリティ認証への関心が薄がる (?)
  - システム認証や開発者認証に関心がシフト

システム認証で注目されるIEC 62443-3

- システム認証が始まる
  - 米国ISA SecureはSSA
  - ドイツTÜVは独自の認証

ICSベンダーがターンキー・システム製品で取得

最初の認証はEmerson社製品 (3月13日)

- 欧州のNIS指令が2018年5月から発効
  - 加盟国政府には
    重要インフラ(必須サービス)事業者のセキュリティ監査義務

- 国連の欧州経済委員会がISO/IEC 27000シリーズやIEC 62443を認知
  https://www.unece.org/fileadmin/DAM/trade/wp6/documents/2018/ECE_CTCS_WP.6_2018_9E_Cybersecurity.pdf

☞ DARPAのRADICS訓練
☞ サイバー保険

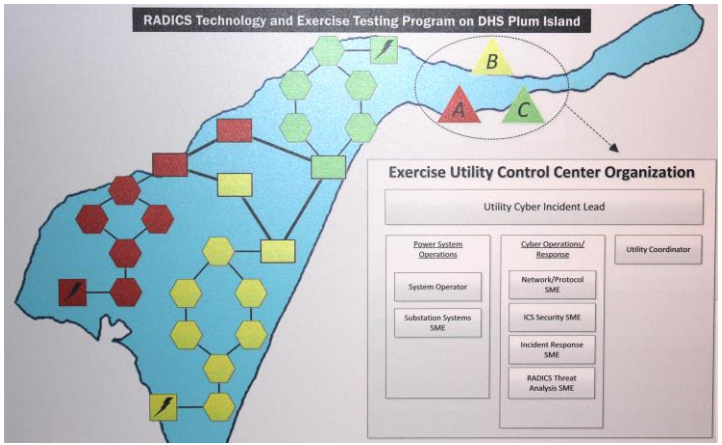
サイバー攻撃からの復旧策

米国DARPAのRADICS

防御対策だけでなく
復旧手順の計画も！

(Rapid Attack Detection, Isolation and Characterization)

- 電力網に対する大規模なサイバー攻撃からの復旧訓練
- 2015年末に提案され
  2018年10月31日～11月6日にPlum島(ニューヨーク州)で実施
  - 200万m²近い面積のほぼ無人島
  - 訓練用に3社の電力事業者の設備
  - 数週間の全電源喪失からの電力復旧
  - 復旧作業へのサイバー攻撃も想定



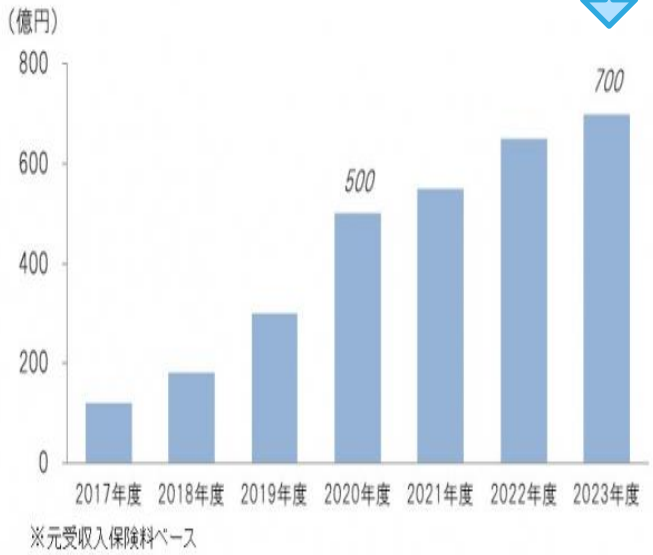
Federal Researchers Simulate Power Grid Cyberattack, Find Holes in Response Plan
https://www.wsj.com/articles/federal-researchers-simulate-power-grid-cyberattack-find-holes-in-response-plan-1541785202

Pentagon Researchers Test 'Worst-Case Scenario' Attack on U.S. Power Grid
https://www.nextgov.com/cybersecurity/2018/11/pentagon-researchers-test-worst-case-scenario-attack-us-power-grid/152803/

サイバー保険の拡大

- ランサムウェア被害の拡大がサイバー保険の普及を後押し
  - 市場規模が急拡大： 国内700億円(2023年；日本能率協会総研予測)
    世界214億ドル(2025年；ResearchAndMarkets社予測)

- 日本損害保険協会からも啓発資料
  - サイバー保険特設サイトなど
    https://www.sonpo.or.jp/cyber-hoken/
    https://www.sonpo.or.jp/news/notice/2019/1907_02.html
  - サイバー保険に関する調査2018
    https://www.sonpo.or.jp/news/release/2018/1903_02.html
  - サイバー攻撃に起因する他人の身体傷害や財物損壊も補償範囲に



模索が続くサイバー保険

第4四半期に支払われた総額は2020万ドル

- Norsk Hydro社にAIG社から360万ドルの損害保険金(初回支払い)
  - 2019年3月にランサムウェアLockerGoraに感染し7100万ドルの損害

- Mondelēz社とZurich American保険とがサイバー保険を巡り係争中
  - 2017年にNotPetyaに感染し1.90億ドルの損害
    1億ドルの保険金を請求
  - 保険会社は「戦争条項」を理由に保険金支払いを拒否

- Merck社には一部の保険会社から4500万ドルの損害保険金
  - 2017年にNotPetyaに感染し8.70億ドルの損害
  - 契約していた30社の保険会社のほとんどが保険金支払いを拒否
  - 1.8億ドルの保険金の支払いを求めて係争中

- ☞ 米国MITREからATT&CK for ICS
- ☞ 米国NISTのNCCoEから破壊的なサイバー攻撃への対策ガイド
- ☞ 英国ENISAからセキュリティ対策と国際標準の規定との対応付けツール

新たに公開された参考文書

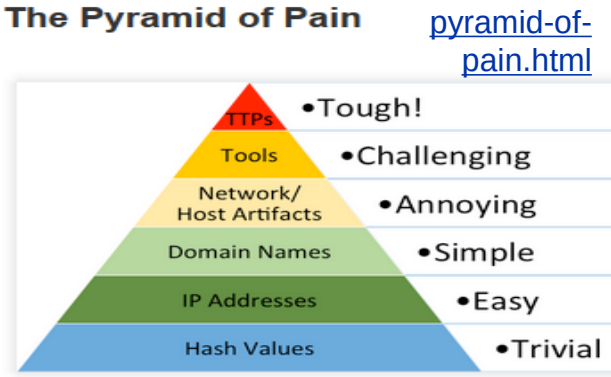
MITREからATT&CK for ICS

TTPs：Tactics, Techniques and Procedures

- MITREは米国連邦政府からの調査研究を請け負うNPO
- ICSに対するサイバー攻撃の手法(TTPs)を論ずるための用語の辞書としてATT&CK for ICSを2020年1月7日に公表
  http://www.mitre.org/news/press-releases/mitre-releases-framework-for-cyber-attacks-on-industrial-control-systems

- 主な内容
  https://collaborate.mitre.org/attackics/index.php/Main_Page
  - 「成りすまし」など，攻撃手法
  - ICSへの攻撃者が利用するソフトウェア
  - ICSを狙っている攻撃集団
  - PLCなど，ICS中に存在し攻撃対象となる資産

出典：https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html



米国NISTのNCCoEから

- ランサムウェアなど破壊的なサイバー攻撃の検知と資産保護に関する実践ガイドの草案 (2020年1月28日公開)
  https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/identify-protect
  - SP 1800-25A： 概要
  - SP 1800-25B： アプローチとアーキテクチャーとセキュリティ属性
  - SP 1800-25C： ガイド方法

欧州のENISAから

- 重要インフラ・サービス事業者がとるべきセキュリティ対策を
  ISO/IEC 27000シリーズやIEC 62443シリーズ等の国際標準中の
  要件や推奨事項に対応付けるツールを公開 (11月28日)
  https://www.enisa.europa.eu/news/enisa-news/enisa-launches-oes-tool-to-map-security-measures

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