JPCERT CC®

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

本日ご紹介する1年間の主な話題

- 注目されたマルウェア
- 世界的なサイバー攻撃の深刻化
- インシデントの実態
- ICS製品の脆弱性に関する動向
- 標準化に関する動向
- 技術開発動向
- 人材開発

ICSに関連したマルウェアの動向

ICSを狙って作られたマルウェア

ランサムウェアの大流行とICS

ICSを狙って作られたマルウェア：新たに２つ

マルウェア名	報告年	概要
Stuxnet	2010	イランのウラン濃縮工場の遠心分離機に異常な回転をさせて破壊
Havex (DragonFly, EnergeticBear, CrouchingYeti)	2014	オフィス網上のPCが感染；OPC関連情報を収集
BlackEnergy2	2014	複数のベンダーのHMI製品が感染；米国ICS-CERTからアラート
BlackEnergy3	2015	電力およびその関連業界が感染 (情報収集に利用された?) 2015年末と2016年末のウクライナでの停電の前段階で多数の感染 KillDiskを用いてICSのディスク装置の内容を破壊
Industroyer (CrashOverRide)	2017	2016年末にウクライナで遮断機を開き停電を引き起こした
HatMan (Triton, Trisis)	2017	Schneider社製安全計装コントローラのプログラムを改竄

サイバー攻撃によるウクライナの停電の概要

発生月日	被害電力会社	操業地域	被害
2015年 12月23日	PrykarpattyaOblEnergo	Ivano-Frankivsk	変電所のブレーカの切断で最大約6時間にわたり停電 ICS用機器の機能を破壊
	AES KyivOblEnergo	Kiev	
	ChernivtsiOblEnergo	Chernivtsi	
2016年 12月17日	Ukrenergo	Kiev	変電所のブレーカの切断で1時間15分の停電

「マルウェアが直接に停電を引き起こしたわけではない」との昨年の説明は訂正します

2015年の停電は：

- **サイバー攻撃により
エネルギー供給が停止した初の事例**
- **オフィス網に標的型攻撃をかけて
情報収集した後にICSを攻撃**
- **同時に電話網を過負荷状態で利用不能に**

BlackEnergy3
KillDisk
Industroyer

2016年の停電は：

- **官庁や鉄道への攻撃の数日後**
- **前年と似た手口ながら高度化**

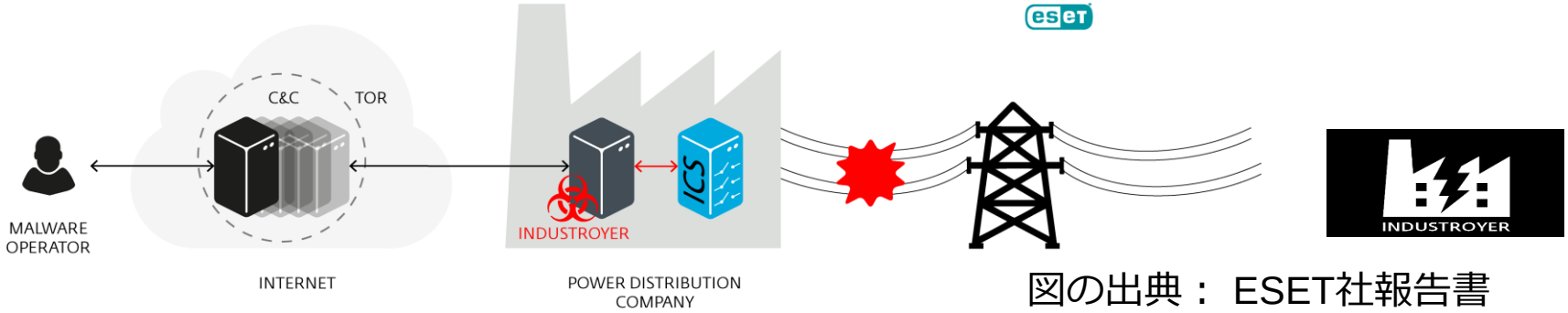
(前回(2017年2月)の講演資料から再掲)

Industroyerの概要

ESETが独自に分析して報告書をまとめ
公表直前にDragos社に査読を依頼

- 報告者
  - スロバキアのセキュリティ企業ESET社(6月12日)：
    Win32/Industroyer
    https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/
  - 米国のセキュリティ企業Dragos社(6月12日)： CrashOverRide
    https://dragos.com/blog/crashoverride/

- 2016年末のウクライナでの停電でICSに遮断機を開くよう指令

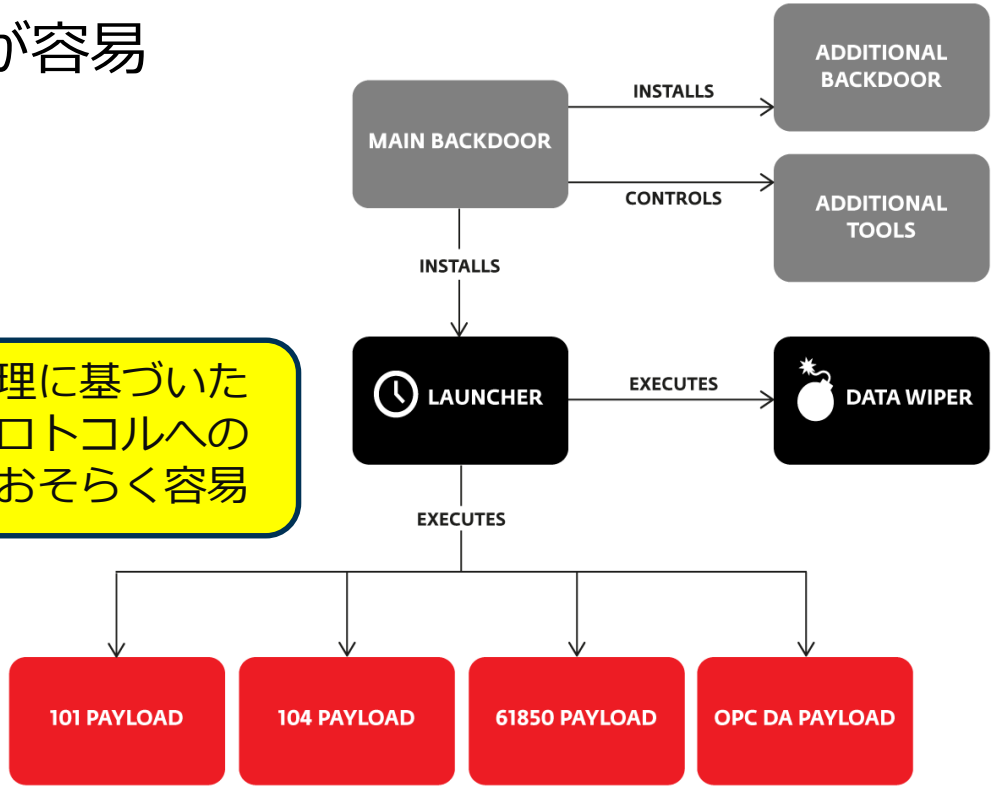


図の出典： ESET社報告書

Industroyerの構造と機能

- モジュラー構造で機能追加が容易
- ツール
  - ポート・スキャナー
  - DOSツール
- ランチャーで起動
  - データ消去
  - 遮断機の操作
    101用，104用，
    61850用, OPC DA用の
    ペイロードがある

同じ原理に基づいた
他のプロトコルへの
拡張はおそらく容易



図の出典： ESET社報告書

HatMan(別名： Triton, Trisis)の概要

- Schneider社製の安全計装システムTriconexを狙ったマルウェア
  - ICSを狙って作られたマルウェアとして史上6つめ
  - ICSの制御を乗っ取ることを狙って作られたマルウェアとして史上３つめ
  - 安全計装システムを狙って作られたマルウェアとしては史上初

Saudi Aramco社？ http://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/

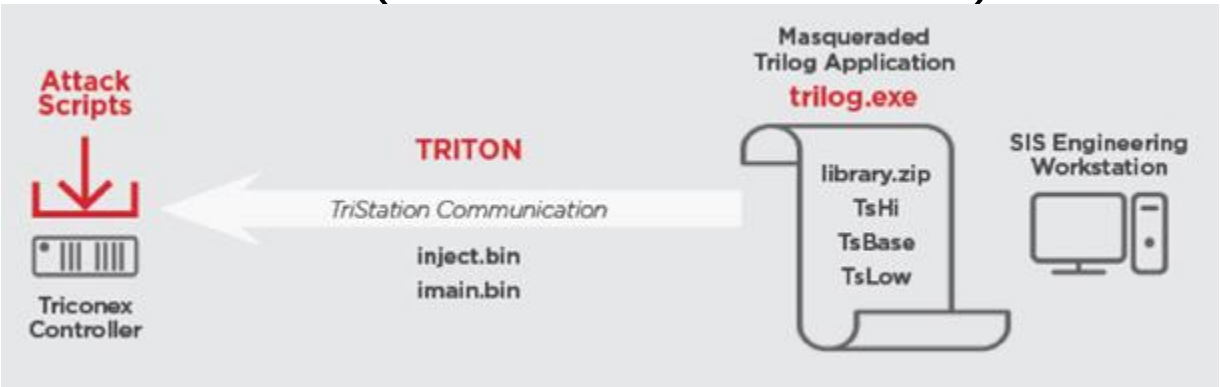
- 2017年8月4日に中東の企業でTriconexの自己検証機能が異常を検知し，監視していた設備を緊急停止した
- その後の調査でマルウェアHatManが見つかり12月中旬に公表

https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%E2%80%94Safety%20System%20Targeted%20Malware_S508C.pdf

HatManの動作概要

- エンジニアリング・ワークステーション等から
  設定用アプリケーションになりすまして
  コントローラに攻撃用スクリプトを注入し，それを起動する

- コントローラに注入されたスクリプトにより
  コントローラの状態の偵察など (潜在的には改竄も可能)

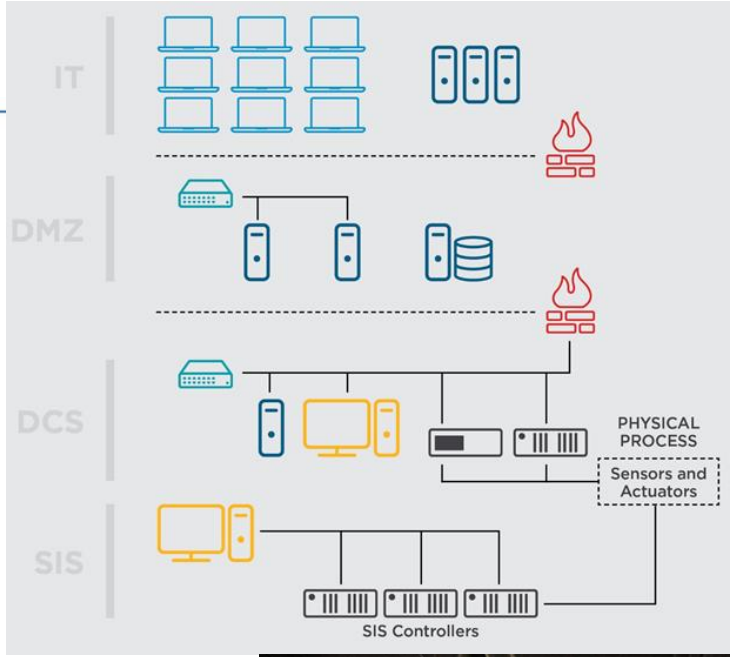


右図の出典：
FireEye社報告書

HatManまとめ

- 安全計装システムが改竄されても甚大な災害には直結しないが…
  - 異常がないのに緊急停止
  - 異常があっても見過ごされる
  - …といった事態が懸念される

- コントローラの設定変更を禁ずる「キー」が備わっているが…
  - 切替て厳格運用しているか？
  - 侵害され無効化される可能性



出典：
図と写真は
FireEye社の
報告書より

ランサムウェアの大流行とICS

- ICSを狙って開発されたわけではない
  - 「システムを復旧させて欲しければ身代金を支払え！」
  - 身代金を払っても，システムを復旧できるとは限らない
    - ランサムウェアにもバグがある
    - 破壊型のマルウェアが「ランサムウェア」に見せかけ

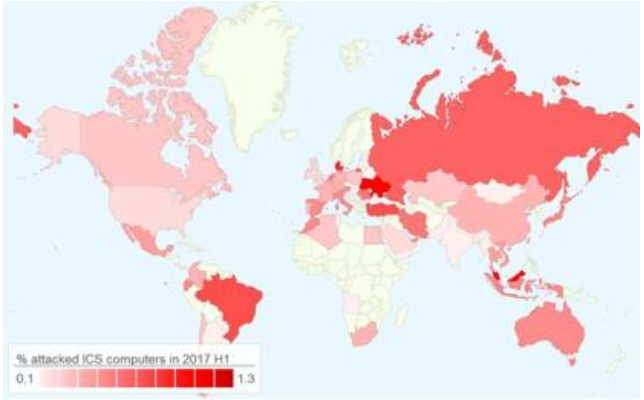
- ICSが感染すれば，操業の停止や復旧コスト等，企業業績に響くような被害にも
- バックアップが無くて普及に手間取るケースもある

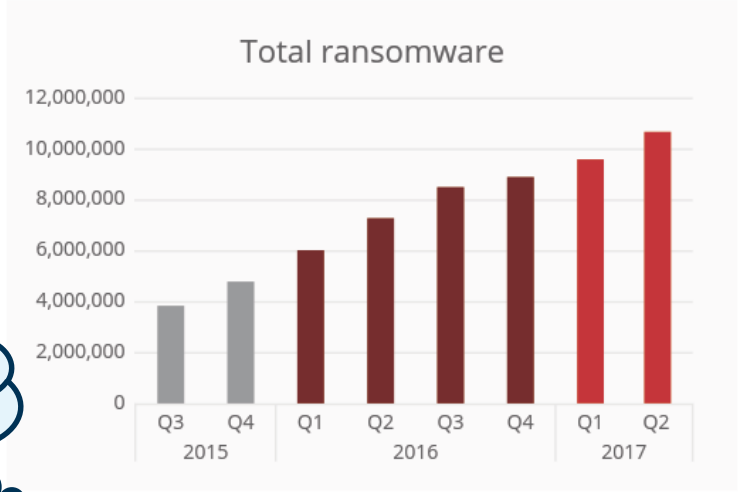
ここ数年はランサムウェア攻撃が増加傾向

■ 続々と新種のランサムウェアが出現

出典： Kaspersky社

https://ics-cert.kaspersky.com/wp-content/uploads/sites/6/2017/09/KL-ICS-CERT_H1-2017_report_FINAL_EN.pdf



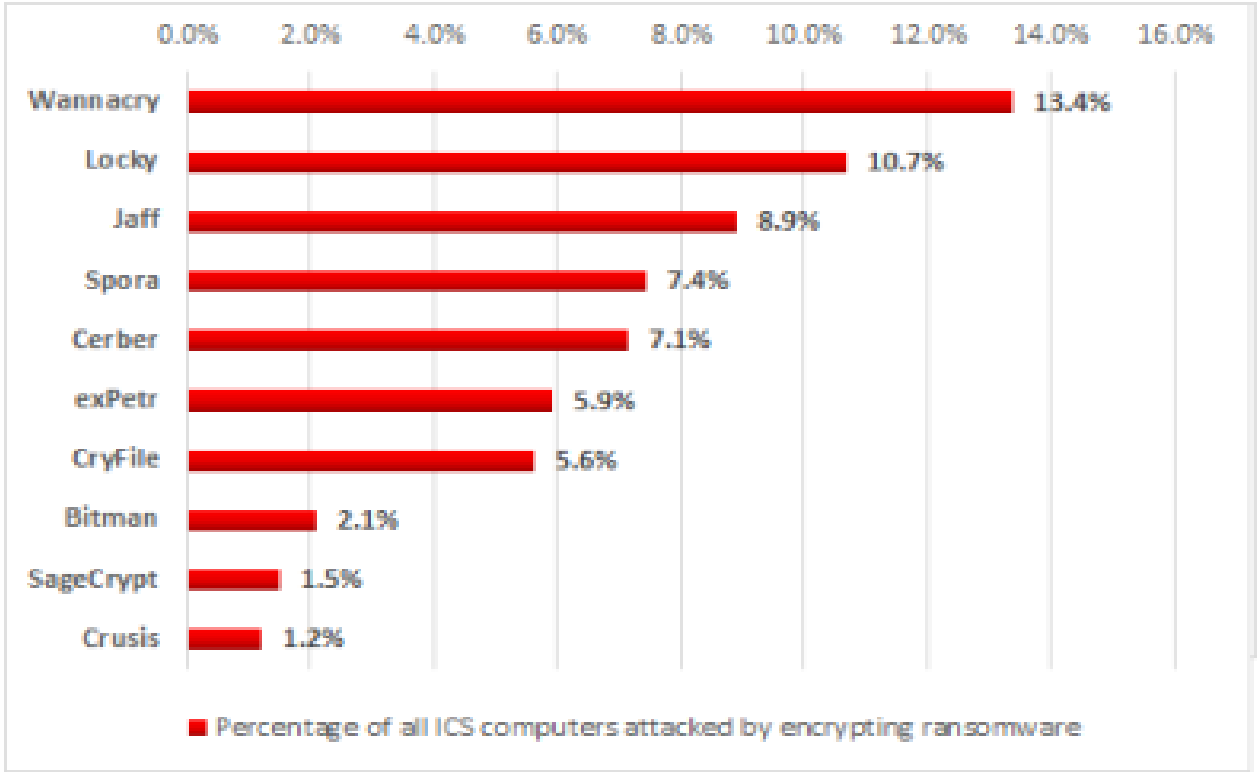


Source: McAfee Labs, 2017.

仮想通貨の普及で身代金を集めやすくなった？

	Country*	% of systems attacked
1	Ukraine	1.33%
2	Malaysia	1.31%
3	Denmark	1.12%
4	Republic of Korea	1.06%
5	Turkey	0.88%
6	Brazil	0.85%
7	Russia	0.80%
8	Romania	0.67%
9	Iran	0.65%
10	Austria	0.65%

2017年前半に流行したランサムウェア： 次々に新種登場



TOP 10 most widespread encryption Trojan families, H1 2017

ランサムウェアの大流行とICSへの影響

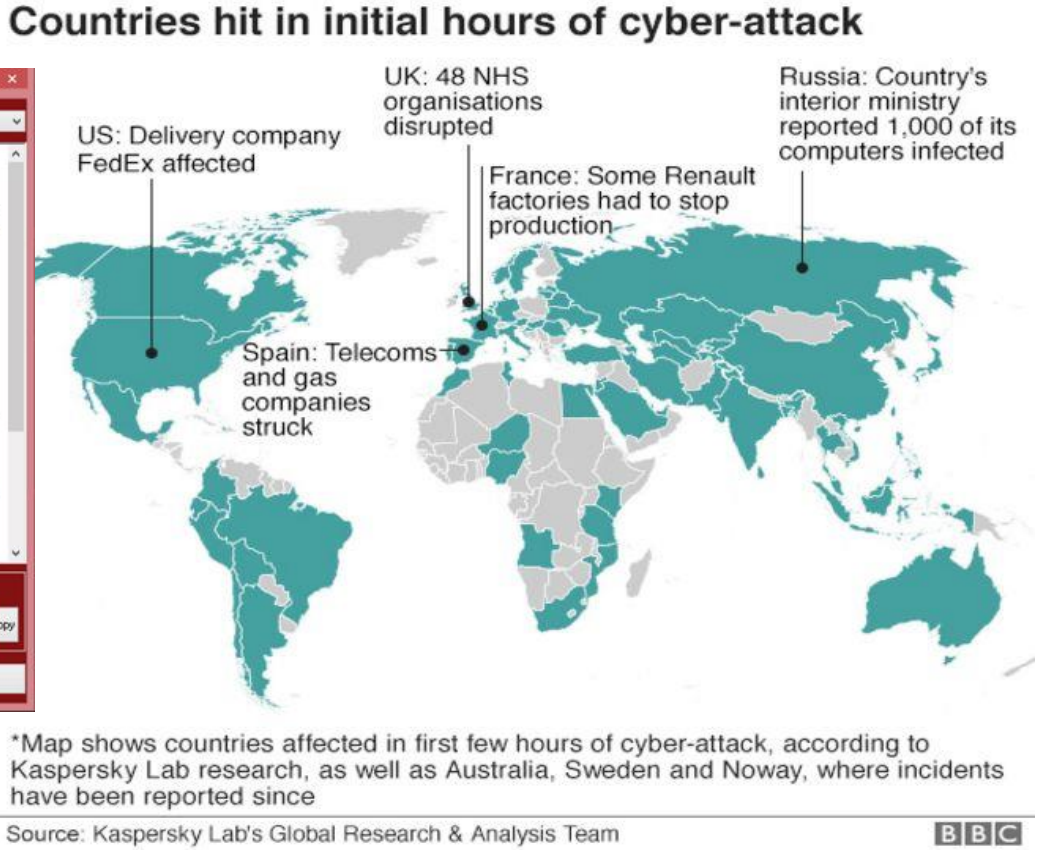
米国NSAから流出したとされるServer Message Blockの脆弱性を突く攻撃コードが組み込まれたことにより，強い感染力を獲得したWannaCryとNotPetya

時期	記事
2016年	ランサムウェア攻撃が増加(前年比5割増)
2017年3月	Server Message Blockの脆弱性情報の公表
2017年5月	ランサムウェアWannaCry攻撃 1日で150ヶ国の23万台に感染
2017年5月	Marcus Hutchins氏がkill switchを発見
2017年6月	破壊型マルウェアNotPetya攻撃 ウクライナ国内の1.25万台を攻撃 その後に少なくとも64ヶ国に感染拡大

北朝鮮による攻撃？

ロシアによる
対ウクライナ攻撃？

ランサムウェアWannaCry



WannaCry感染被害事例

月日	被害企業	状況
5月12日	英国NHS	英国内の40病院が感染；入院患者も転院
5月12日		英国の研究者が「kill switch」を発見
5月13日	日産	英国Sunderland工場が感染
5月13日		74ヶ国で感染被害；米国 FedEx, 英国Scottish Power, フランスのルノー, ドイツの鉄道(券売機), スペインの通信会社やガス会社など
5月19日		研究者がWindows XP用復号ツールを公開
6月21日	ホンダ	狭山工場の感染で19日は生産できず(1000台)
6月22日	豪州 ビクトリア州	速度違反監視カメラ280台のうち97台が感染

- 5月末時点で，150ヶ国にわたり30万台が感染
- 米国ではICSにおける感染事例も

破壊型マルウェアNotPetya

「復号鍵を買え」とあるが実際には復号できない

別名： PetrWrap, exPetr, GoldenEye, Diskcoder.C

6月27日のNotPetya感染の急拡大

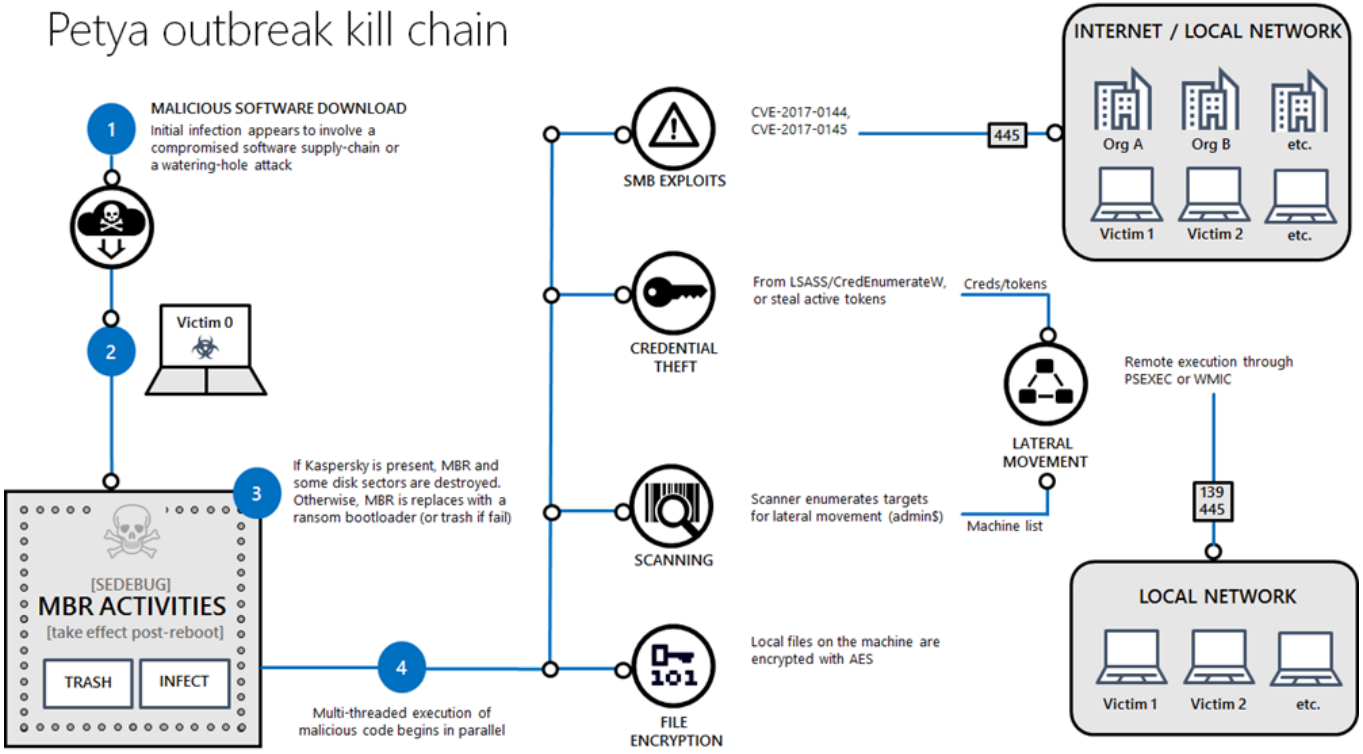
- M.E.Docはウクライナ国内で広く利用されている会計用ソフトウェア
  - Intellect Service社製
  - 税務署や他の企業とのデータ交換機能を含む

(攻撃者の手口)

- 2017年4月以降の版にバックドアを埋め込んだ
- 2017年6月27日に更新用ウェブ・サーバがNotPetyaをダウンロードさせるように改竄

- ウクライナのサイバー警察が家宅捜索して押収

ランサムウェアNotPetyaの挙動



出典： Microsoft社

NotPetya被害： Merck社

- 米国に本拠を置く製薬会社
  売上： 395億ドル，従業員数： 7万人

- 6月27日にサイバー攻撃を被った
  - 製造，R&D, 販売の各部門で操業に影響
  - 1ヶ月で梱包は復旧できたが，調剤は復旧途上
  - 一部の原薬製造は復旧までに半年以上の見通し
  - 売れ筋商品の出荷を確保して売上への影響を回避

四半期決算報告書：
http://www.mrknewsroom.com/news-release/corporate-news/merck-announces-second-quarter-2017-financial-results

NotPetya被害： FedEx社

- 米国に本拠を置く物流企業
  売上： 503億ドル，従業員数： 40万人

- 2016年5月に買収した欧州のTNT Expressで6月27日にランサムウェア攻撃を被った
  - ウクライナの拠点から始まりTNT全域が感染
  - 7月中旬時点で：
    - 非常事態計画を発動しなんとかサービスを復旧
    - システムの完全復旧の見通し立たず

売上：
69.1億ユーロ

被害： 3億ドル
(復旧費用を含む)

年次報告書

http://investors.fedex.com/news-and-events/investor-news/news-release-details/2017/FedEx-Files-10-K-with-Additional-Disclosure-on-Cyber-Attack-Affecting-TNT-Express-Systems/default.aspx

NotPetya被害： Reckitt Benckiser社

- 英国に本拠を置く衛生用品製造企業
  売上： 99億ポンド，従業員数： 3.5万人

- 6月27日にNotPetyaに感染
  - 7月上旬時点で：
    - 期末の出荷やインボイスの発行ができず
    - まだ一部の製造工場では完全稼働できず
  - NotPetyaだけが原因ではないが売上目標未達
    (目標に対して1億ポンド前後の売上減？)

サイバー攻撃に関してお客様へ
https://www.rb.com/media/news/2017/june/cyber-attack-statement-to-customers/

NotPetya被害：A.P. Moller-Maersk社

- デンマークに本拠を置く海上運送会社
  売上： 355億ドル， 従業員数： 8.8万人

- 27日午後から感染
  - 当初は予防措置の停止解除後にすぐ回復と楽観視
  - 港湾管理のAPMターミナル部門が深刻な感染
    - 世界中の72の港湾ターミナルの一部(香港，ムンバイ，ニューヨーク，バルセロナ，ロッテルダム等)で7月4日頃まで操業が止まった
    - EDIによる発注書の処理が滞留

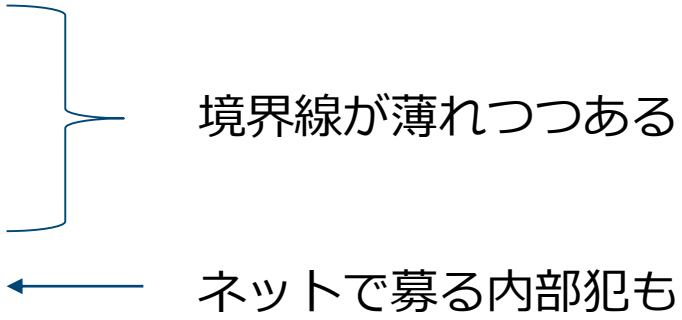
サイバー攻撃の深刻化

国家の支援が疑われるサイバー攻撃

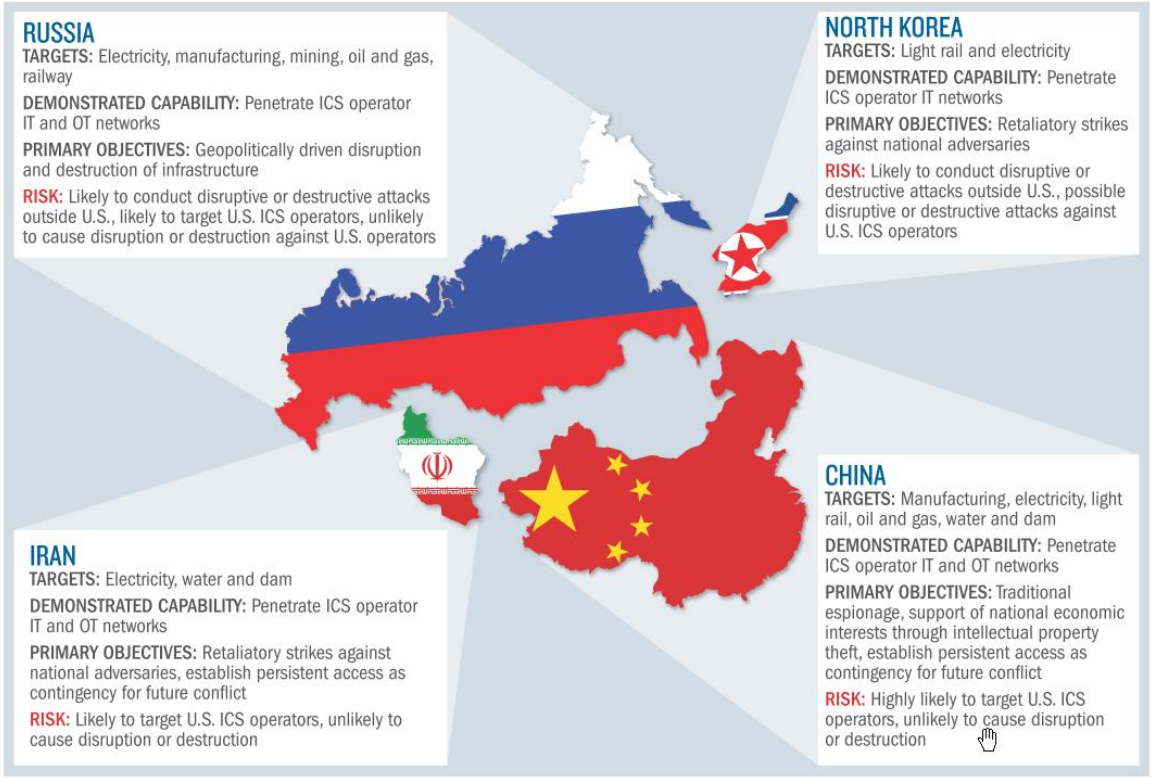
サイバー攻撃元としての犯罪集団と国家との見分けが困難に

ICSに対するサイバー攻撃者の分類 (NIST SP800-82)

攻撃者	説明
ボットネット運用者	ボットを使って金儲け
犯罪集団	金品の詐取や強請り
外国諜報機関	スパイ活動
ハッカー	ネットワークへ侵入
内部犯	ルール違反；雇用主への報復
フィッシャー	認証情報の詐取
スパマー	迷惑メールを発信
マルウェア開発者	マルウェアの作成
テロリスト	破壊工作等で社会不安を煽る



ICSへのサイバー脅威 (Booz Allen Hamilton報告書より)



引用：Booz Allen Hamilton社

https://www.boozallen.com/insights/2016/06/industrial-cybersecurity-threat-briefing

サイバー戦争が議論の俎上に

- 2018年の世界ワールド・フォーラムが挙げた
  将来の潜在的なショック10項目の一つ：
  合意されたサイバー戦争のルールがない中での国際紛争
  http://reports.weforum.org/global-risks-2018/press-release/

- Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 公開 (初版の公開は2013年)

- ジュネーブ条約のデジタル版を求める声明も
  https://techcrunch.com/2017/02/14/microsoft-calls-for-establishment-of-a-digital-geneva-convention/

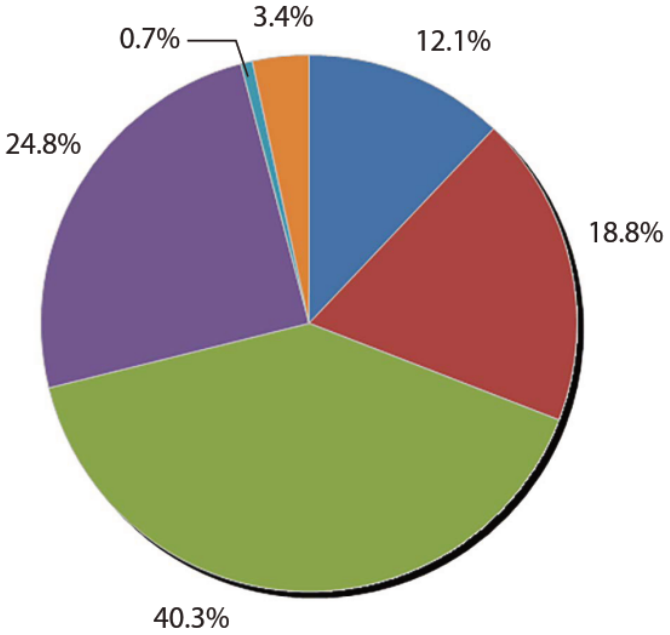
ICSセキュリティ・インシデントの実態

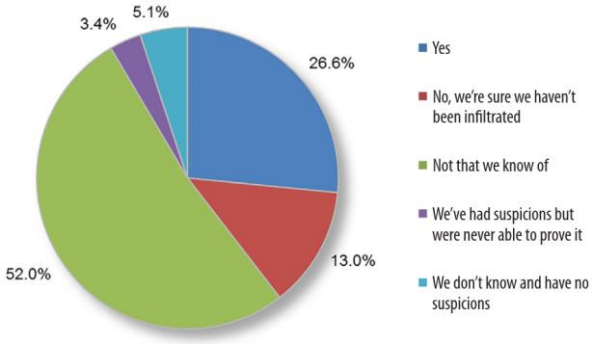
SANSの年次報告書(2017年6月公表)より

HTTPS://WWW.SANS.ORG/READING-ROOM/WHITEPAPERS/ANALYST/SECURING-INDUSTRIAL-CONTROL-SYSTEMS-2017-37860

過去1年間のICSセキュリティ・インシデントの有無

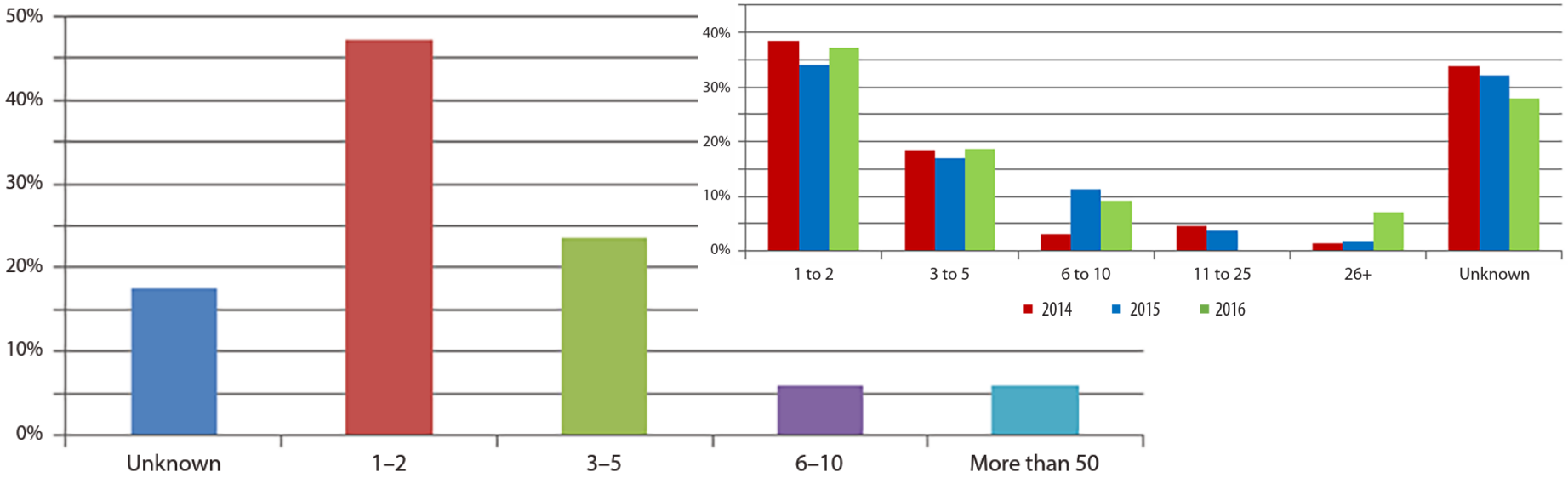
- 「あった」の回答が前年に対して半減
- 断定的に「ない」との回答が前年に対して5割増し





過去1年間のICSセキュリティ・インシデントの頻度

- 数回以下が大多数だが
  「毎月ないし毎週インシデントが起きている」との回答も



調査結果 (Securing Industrial Control Systems-2017)

- ICSセキュリティ予算： 2016年度から増額(46%)
- 脅威ベクトル：
  - 自衛能力の欠けた機器の接続 (44%)
  - ランサムウェアを含む脅迫 (36%)
- 予算付け優先度： セキュリティ評価・監査 (36%)
- コントローラが最大のリスク： 24%
- 社内ポリシー等をNISTのサイバー・セキュリティ・フレームワークに対応付け： 48%
- ICSへの脅威水準： 高い～深刻 (69%)

ICSセキュリティに対する2017年度予算額

- 10万～250万米ドルの企業が多い
- 規模(従業員数)に応じて予算額が増える

Organization's Control System Security Budget for FY 2017 by Size

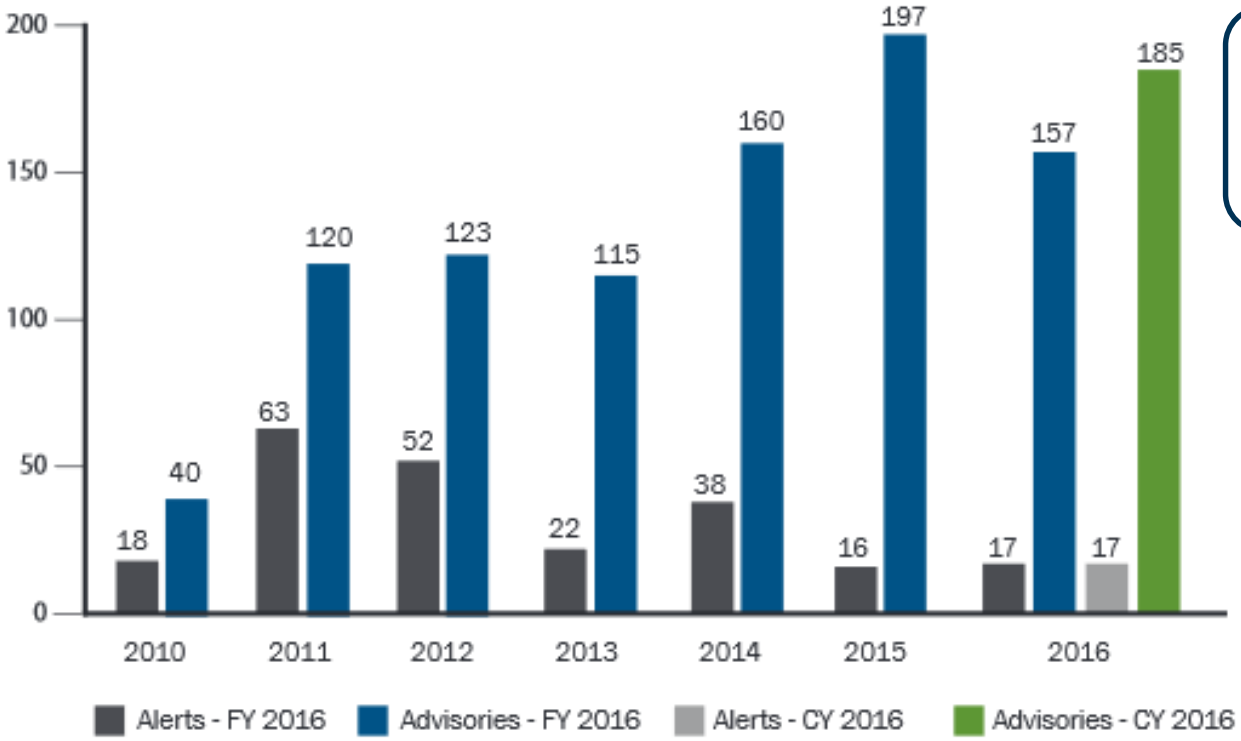
	<1K	1K to 10K	>10K
We don't have one	9.4%	3.4%	2.6%
Less than $100,000	3.4%	2.6%	0.0%
$100,000–$499,999	6.0%	3.4%	3.4%
$500,000–$999,999	0.0%	1.7%	4.3%
$1 million–$2.49 million	0.9%	6.8%	4.3%
$2.5 million–$9.99 million	0.0%	4.3%	1.7%
Greater than $10 million	0.0%	0.9%	2.6%

ICS製品の脆弱性に関する動向

統計的な動向

懸念事項

米国ICS-CERTが公表した脆弱性アドバイザリ数

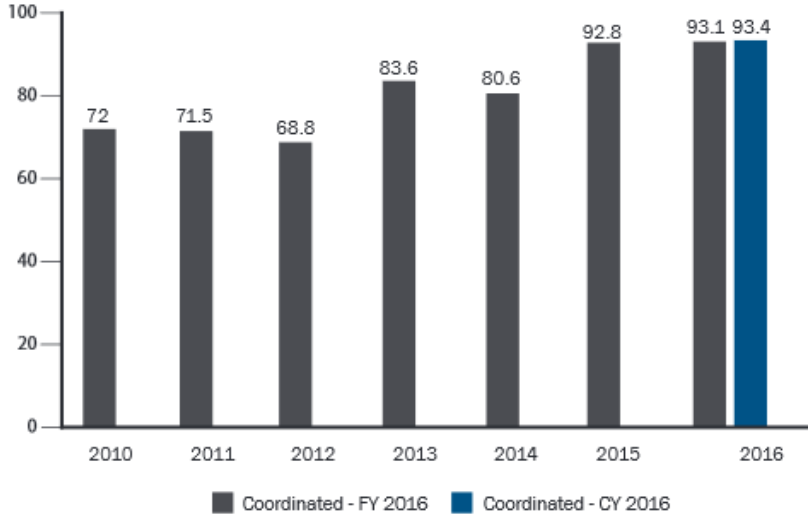


2017年(CY)は
アドバイザリ： 189件
(うち16件は医療用機器)
アラート： 9件

引用： 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

ICS関連の脆弱性の動向

- 公表された脆弱性の9割は公表前調整されている



- 脆弱性のカテゴリ別内訳で筆頭に位置する
  - バッファ・オバーフロー(34%)
  - 入力検証の不備(7%)
  - クロスサイト・スクリプティング(5%)

- ベンダーが自らICS-CERTに報告する事案の割合が増加

懸念されるICS関連の脆弱性：継承される脆弱性

ICSベンダー自身が作り込んだわけではないが上流から継承される脆弱性がある

- SpectreとMeltdown：プロセッサの脆弱性
  ICS-ALERT-18-011-01B （https://ics-cert.us-cert.gov/alerts/ICS-ALERT-18-011-01B）
  — 読めないように管理されているはずのメモリ領域が見える
- WiFiに対するKrack攻撃
  https://www.krackattacks.com/
- OPC-UAプロトコル・スタックの脆弱性
  ICSA-17-243-01B (https://ics-cert.us-cert.gov/advisories/ICSA-17-243-01B)
  — Siemens社は脆弱性を報告しているが他のベンダーは？
- ソフトウェア・ライセンス管理用USB(SafeNetセンチネル)の脆弱性
  Kaspersky社報告 (https://securelist.com/a-silver-bullet-for-the-attacker/83661/)
  — 14件の脆弱性；挿入されたPCが脆弱な状態になる

懸念されるICS関連の脆弱性：産業用ロボット

- これまでのICS用機器と同様に多数の潜在した脆弱性をもつと推測される
- 機能的な複雑さに対応して，サプライ・チェーンの上流から，多数の脆弱性を継承していると推測される

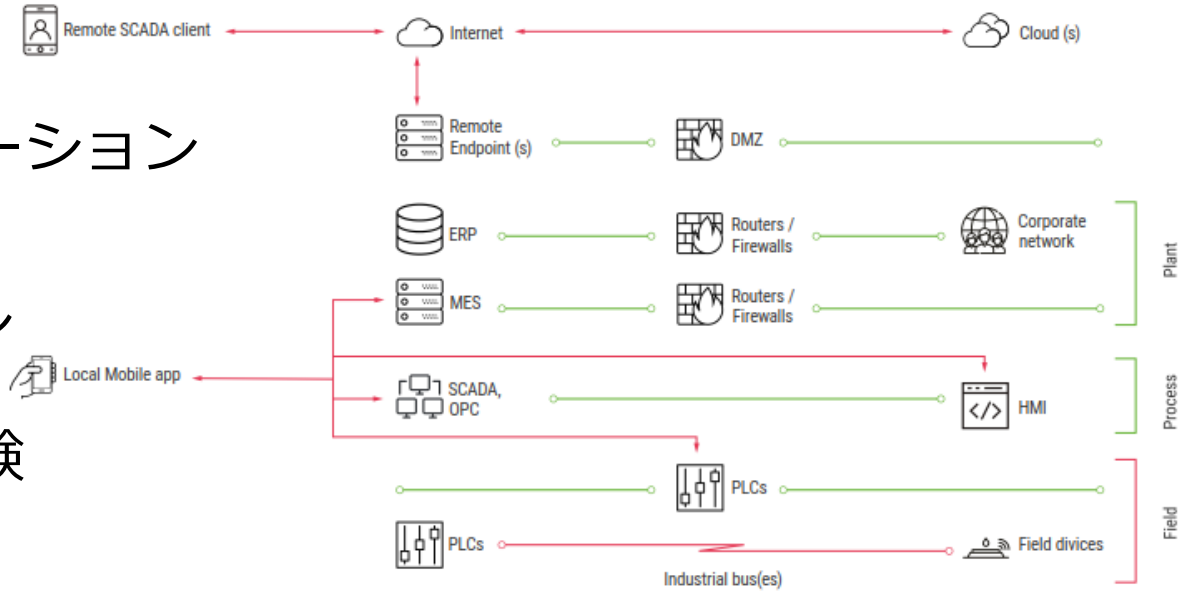
- 注意を喚起する報告書
  - IOActive： Hacking Robots Before Skynet
    https://ioactive.com/pdfs/Hacking-Robots-Before-Skynet.pdf
  - TripWire: More than 90% of IT Pros Expect More Attacks, Risk, and Vulnerability with IIoT in 2017
    https://www.tripwire.com/state-of-security/featured/90-pros-expect-attacks-risk-vulnerability-iiot-2017/

懸念されるICS関連の脆弱性：モバイル・アプリケーション

- ICS用モバイル・アプリケーションの脆弱性について
  IOActive社とEmbedi社による共同報告書
  https://ioactive.com/pdfs/SCADA-and-Mobile-Security-in-the-IoT-Era-Embedi-FINALab%20(1).pdf

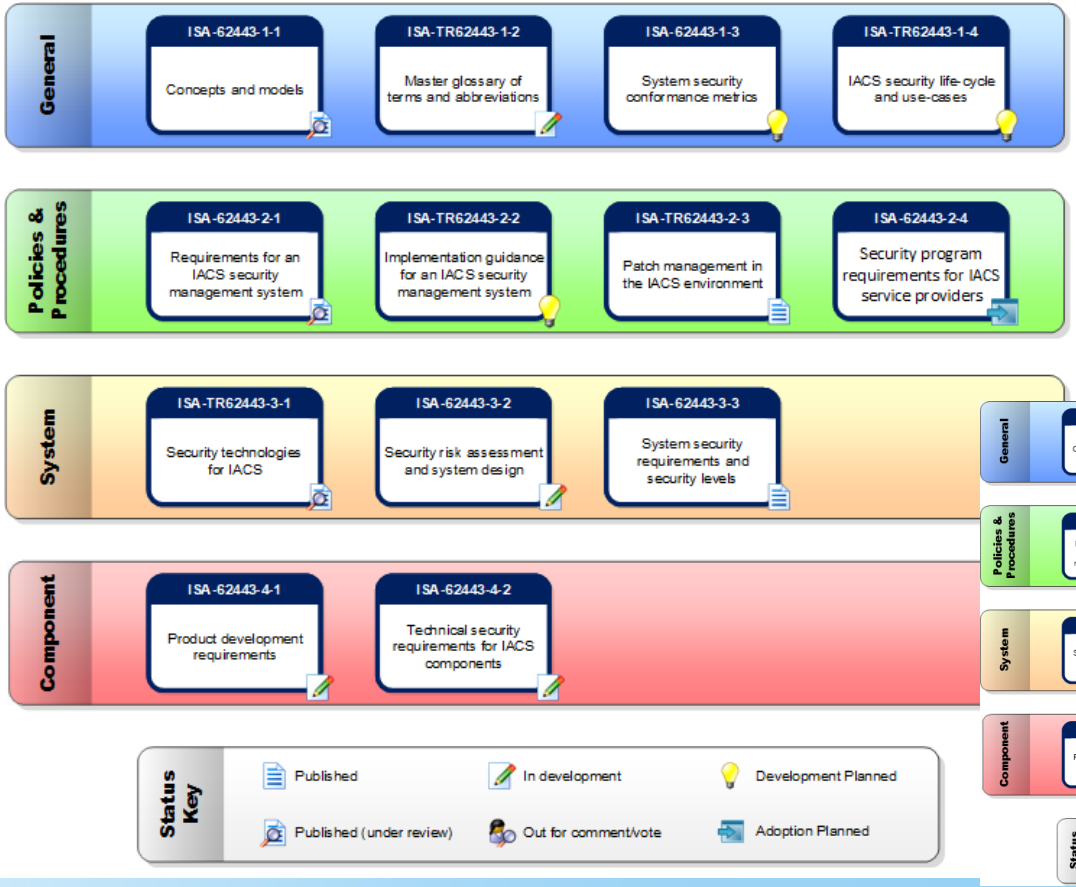
- 普及するICS用
  モバイル・アプリケーション

- 34社のICS用モバイル
  アプリケーションを
  ランダムに選んで試験
  ― 147件の脆弱性



ICSセキュリティの標準化に関する動向

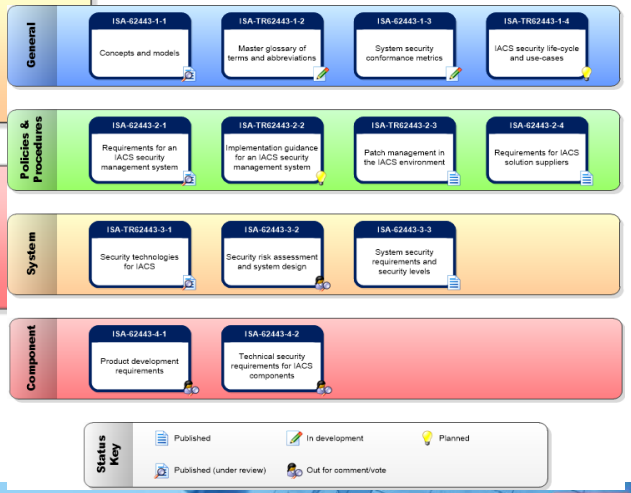
ISA/IEC 62443シリーズ標準化



ISA-62443-1-5

Protection levels

2016年



ISO/IEC 27000シリーズ標準化

- ISO/IEC 27019:2017
  Information technology -- Security techniques -- Information security controls for the energy utility industry
  https://www.iso.org/standard/68091.html
  - エネルギー業界向けのISMS(情報セキュリティ管理システム)管理策
  - ICSについても言及
  - 2013年版TRを改定し，IS(国際標準)として2017年に発行

ICSセキュリティに関する認証の全体像

	コンポーネント	システム	組織 (プロセス)	要員
国際標準ベース		(TÜV SÜD)	CSMS (JIPDEC) 運用プロセス	
	EDSA (ISA Secure)	SSA (ISA Secure)	(TÜV SÜD) SDLA (ISA Secure) 開発プロセス	CAP； CCST (ISA)
	UL CAP for ICS (UL)			GICSP （SANS/GIAC)
私的標準ベース	Achilles Communications Certification (WurldTech.GE)			

コンポーネントに対する認証に関してはAchilles認証が独走

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
Achilles Communications Certification	22	135	216 (GE社が買収)	294	472	581
EDSA (ISA ISCI)	0	5	9	11	14	20
UL CAP for ICS (UL)					0	2

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

- 米国ISA Secureと日本のCSSCが認証しているEDSA (Embedded Device Security Assurance)も健闘； 約5割増しに(東芝製DCSコントローラ等)

http://www.isasecure.org/en-US/End-Users/ISASecure-Certified-Devices

ISASecure® CSSC認証ラボラトリー

UL認証(UL 2900)が始まる

- 5月に初のUL 2900-2-2に基づく製品認証を発行

  (Standard for Software Cybersecurity for Network-Connectable Devices, Part 2-2: Particular Requirements for Industrial Control Systems)
  https://www.businesswire.com/news/home/20170516005575/en/Electric-Imp-World%e2%80%99s-IoT-Platform-Earn-UL

- 7月にANSIがUL 2900-1を米国/カナダ標準として承認

  (General Requirements for Software Cybersecurity for Network-Connectable Products)
  https://industries.ul.com/cybersecurity/ul-2900-standards-process

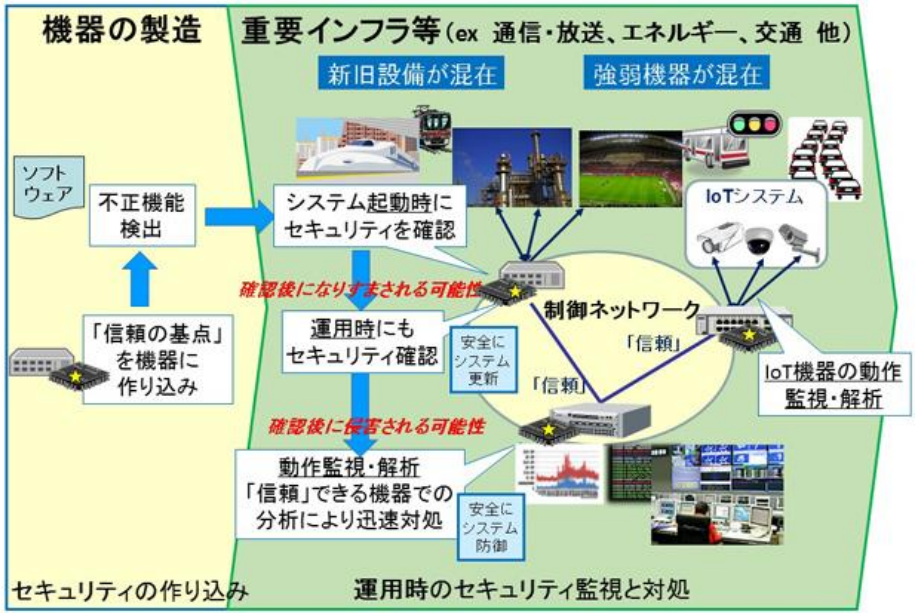
UL 2900	UL 2900-1	ネットワークに接続可能な製品の要件
	UL 2900-2-1	医療用機器に固有な要件
	UL 2900-2-2	ICSに固有な要件

ICSセキュリティの技術開発動向

SIP/重要インフラ等におけるサイバーセキュリティの確保

http://www.nedo.go.jp/activities/ZZJP_100109.html

- 重要インフラサービスの安定運用を担う制御ネットワークおよび制御ネットワークを構成する制御・通信機器のサイバー攻撃対策として研究開発
  - 制御・通信機器のセキュリティ確認技術
  - 制御・通信機器
  - 制御ネットワークの動作監視・解析技術と防御技術



ICSにおける異常検知・分析技術

- 名古屋工業大学「つるまいプロジェクト」
  https://iotnews.jp/archives/54238

- 日立製作所から制御システム向けセキュリティ監視システム
  https://it.impressbm.co.jp/articles/-/15126

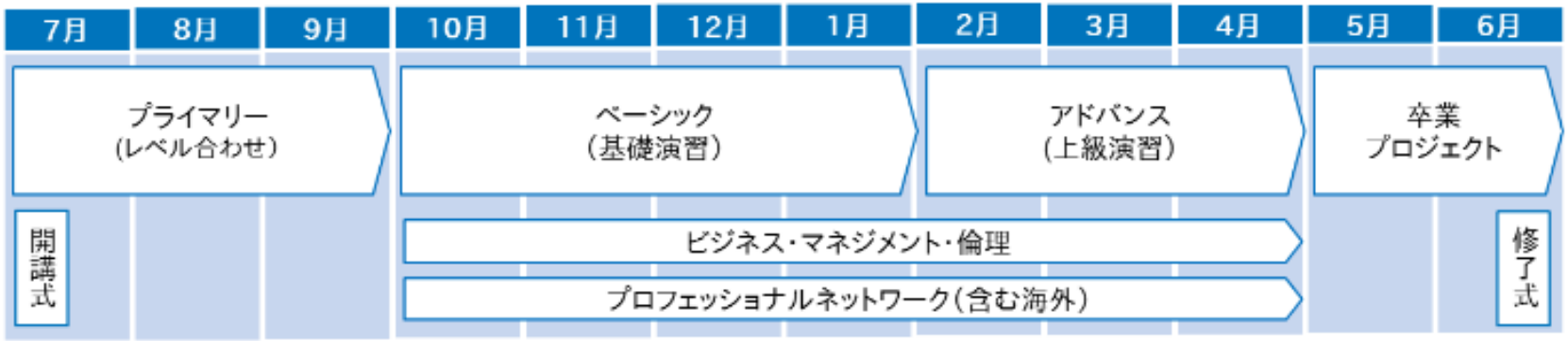
- 米国で開催されたS4x2018でも
  ICSネットワークの異常検知分析用製品の競技会を実施
  https://s4x18.com/the-ics-detection-challenge/

ICSセキュリティの人材開発

IPA産業サイバーセキュリティセンター

- 2017年4月にセンター発足
  http://www.ipa.go.jp/icscoe/index.html

- 2017年7月から人材育成事業として教育プログラム始動



ISAが終身教育プログラムを新設

- ISA/IEC 62443に基づいた教育コース

- ICSサイバー・セキュリティの設計と実現
  IACS Cybersecurity Design & Implementation (IC34)
  https://www.isa.org/training-certifications/isa-training/instructor-led/course-descriptions/ic34/
  ―3日コース

- ICSサイバー・セキュリティの運用と維持
  IACS Cybersecurity Operations & Maintenance (IC37)
  https://www.isa.org/training-certifications/isa-training/instructor-led/course-descriptions/ic37/
  ―3日コース

ご静聴ありがとうございました

JPCERT/CCが提供するICSセキュリティ関連サービス

今後ともよろしくお願いします

- インシデントの報告受付と支援依頼
  - http://www.jpcert.or.jp/ics/ics-form.html
- 脆弱性情報の調整
  (製品開発者登録が望ましい)
- 月刊ニュース・レター配布
  (登録が必要)
  - **迅速に脆弱性情報を受け取るため**
    http://www.jpcert.or.jp/vh/regist.html
- 情報ベースConPaS
  (登録が必要)
  - http://www.jpcert.or.jp/ics/ics-form.html
- 参考情報
  - http://www.jpcert.or.jp/ics/ics-form.html
- 制御システム・セキュリティ・コンファレンス
- 制御システム・セキュリティ・アセスメント・サービス
- 情報共有会・報告会

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
- Tel：03-3518-4600
- 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