20th Anniversary

JPCERT CC®

制御システムセキュリティカンファレンス(2017-02-21)資料

制御システムセキュリティの現在と展望 2017

この1年間を振り返って

一般社団法人JPCERTコーディネーションセンター
技術顧問　宮地 利雄

概要： ICSでもサイバー脅威が顕在化

- 国家的な黒幕の下に行われる深刻なサイバー攻撃
  - ICSへのサイバー攻撃によりウクライナで停電 (2015年12月，2016年12月)
- ランサムウェアの大流行
  - ICSでも被害か(?)
- ICS分野におけるセキュリティ認証の動向
- ICS分野における脆弱性の動向

ICSにおける
セキュリティ・インシデント
に関する動向

外部からのサイバー攻撃が重要インフラに打撃

- 2015年12月と2016年12月の2度にわたり
  ウクライナの電力会社にサイバー攻撃があり
  1～数時間にわたる停電が発生

- 重要インフラに対する初めての本格的なサイバー攻撃

- 比較的豊富な情報がもたらされている
  - 米国が現地に調査団を派遣
  - 学びのための絶好の教材

2016年12月のサイバー攻撃で
遮断機を切られた
キエフ近郊の北部変電所

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

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**

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**

2015年12月の
ウクライナの電力会社へのサイバー攻撃の経過

1. 標的型メール攻撃によって，マルウェアBlackEnergy3に感染させ，これを利用して長期間(1年前後か)にわたる偵察活動で情報 (ネットワーク構成や認証子の情報)を収集

2. 遠隔操作機能を利用して，変電所の遮断機を切断

3. 復旧活動を妨害するための補助的攻撃

   - UPS(非常時電源)が動作しないよう設定
   - 遠隔操作用のイーサネット～シリアル変換装置のファームウェアを書き変えて無能化
   - マルウェアKillDiskによりWindows機のディスク消去
   - コールセンターの電話回線を輻輳状態に

攻撃に用いられたマルウェア

マルウェアが直接に停電を引き起こしたわけではない

停電を起こすための情報収集と復旧を遅らせるために利用された

- BlackEnergy 3
  - 情報収集が主な機能と見られる
  - オフィス網のPCに感染
  - 先代のBlackEnergy2には
    米国の電力会社も少なからず感染 (2014～2015年)
    ICS-ALERT-14-281-01E：Ongoing Sophisticated Malware Campaign Compromising ICS (Update E； 2016年12月9日)
    https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B

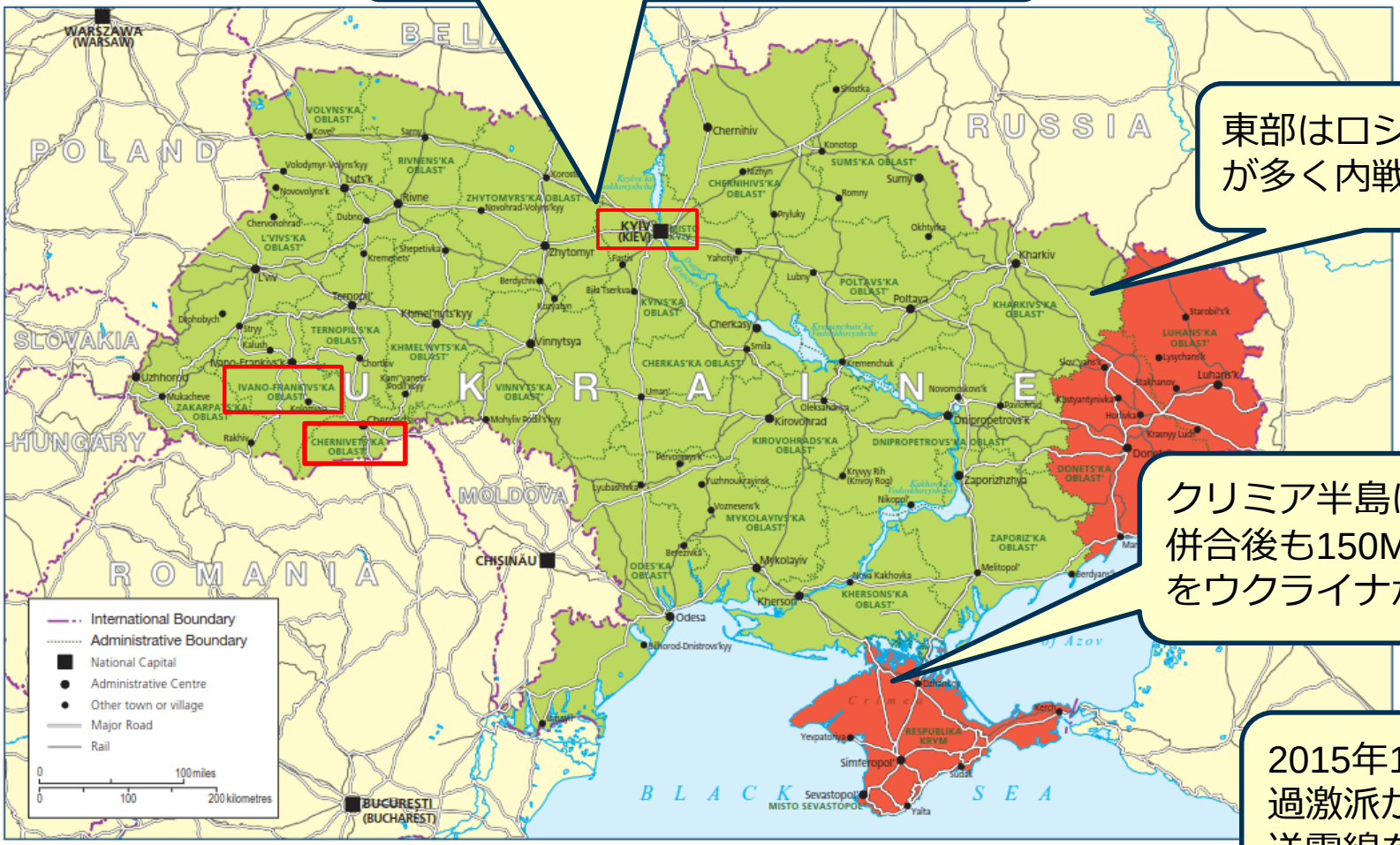
- KillDisk
  - ディスク上のファイルを消去
  - ウクライナでは制御システム内のHMIサーバを破壊
  - その後も改造が進んでいるとされる：
    - ファイルを消去せず暗号化 (ランサムウェア化)
    - Linuxへの移植

ウクライナの地政学

SANDWORM TEAM

FireEye社はロシアのSandWormを嫌疑

ウクライナ政府は欧米やNATOに接近



東部はロシ系の住民が多く内戦状態

クリミア半島はロシア併合後も150MW(約1割)をウクライナから受電

2015年11月には過激派が4系統の送電線を破壊

地図は英国政府の渡航勧告より

JPCERT CC®

[参考資料] サイバー攻撃によるウクライナの停電

- SANS-ICS, E-ISAC: Analysis of the Cyber Attack on the Ukrainian Power Grid
  https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
- US.ICS-CERT: IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure (本来は非公表資料)
  http://www.eenews.net/assets/2016/07/19/document_ew_02.pdf
- E&E News: Inside the Ukrainian hack that put U.S. grid on high alert
  http://www.eenews.net/stories/1060040399
  http://www.eenews.net/stories/1060040460
  http://www.eenews.net/stories/1060040519
  http://www.eenews.net/stories/1060040590

2015年と2016年の停電の双方を紹介

- Archer Security： Hackers struck again in Ukraine, researchers say
  http://www.archersecuritygroup.com/hackers-struck-ukraine-researchers-say/

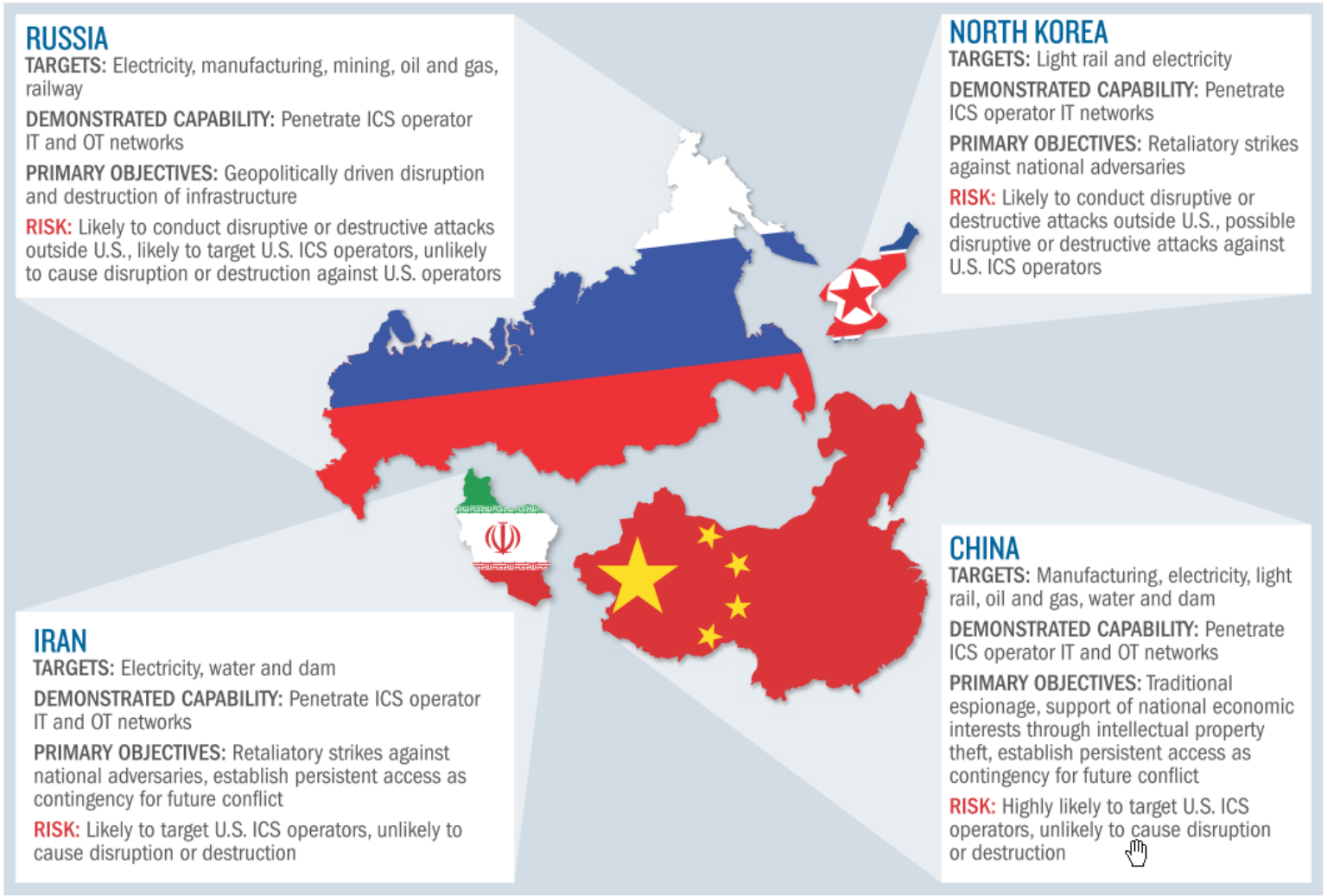
重要インフラに対する外国からのサイバー攻撃

- 米国の電力基幹網へのサイバー攻撃は
  「いつ攻撃されるか」という時間の問題であって
  「攻撃されるかどうか」という可能性の問題ではない
  - 2016年3月のRSAコンファレンスにおける
    Michael Rogers大将 （NSA長官）の講演

- IS(イスラム国)掃討に際して
  米国はサイバー攻撃で敵方の通信を攪乱する計画を公言

- 米国などへのサイバー攻撃でロシアの関与が注目を集めた
  - これまでは「サイバー攻撃」と言えば，中国，イラン，北朝鮮
  - 欧米の選挙に対する干渉
  - ウクライナや米国の電力会社(電力基幹網)

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



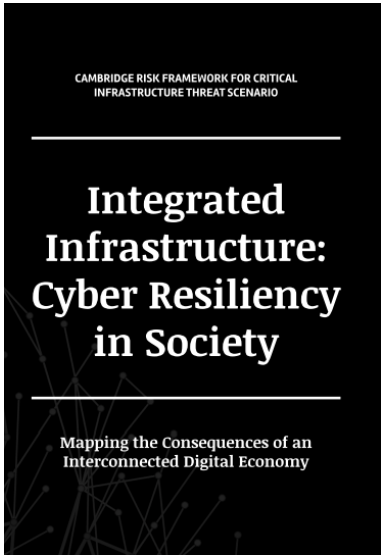
引用：Booz Allen Hamilton社

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

英国で電力網へのサイバー攻撃を想定した社会的被害予測

LockheedMartin: 統合化されたインフラ：社会のサイバー回復性

http://www.lockheedmartin.com/us/news/press-releases/2016/april/collaboration-on-critical-national-infrastructure-cybersecurity.html



- サイバー攻撃による3つのシナリオを想定
  - イングランド南東部の65，95，125ヶ所の変電所が破壊され3，6，12週間にわたって停電
  - 900万～1,300万人が停電の影響を受け
    80万～100万人分の鉄道切符と
    15万～33万人分の航空券がキャンセルされる
  - 影響は様々な業界に及び
    直ちに発生する経済被害だけで120億～850億ポンド
  - その後5年間のGDPの減少は490億～4420億ポンド
    (2.3%相当)

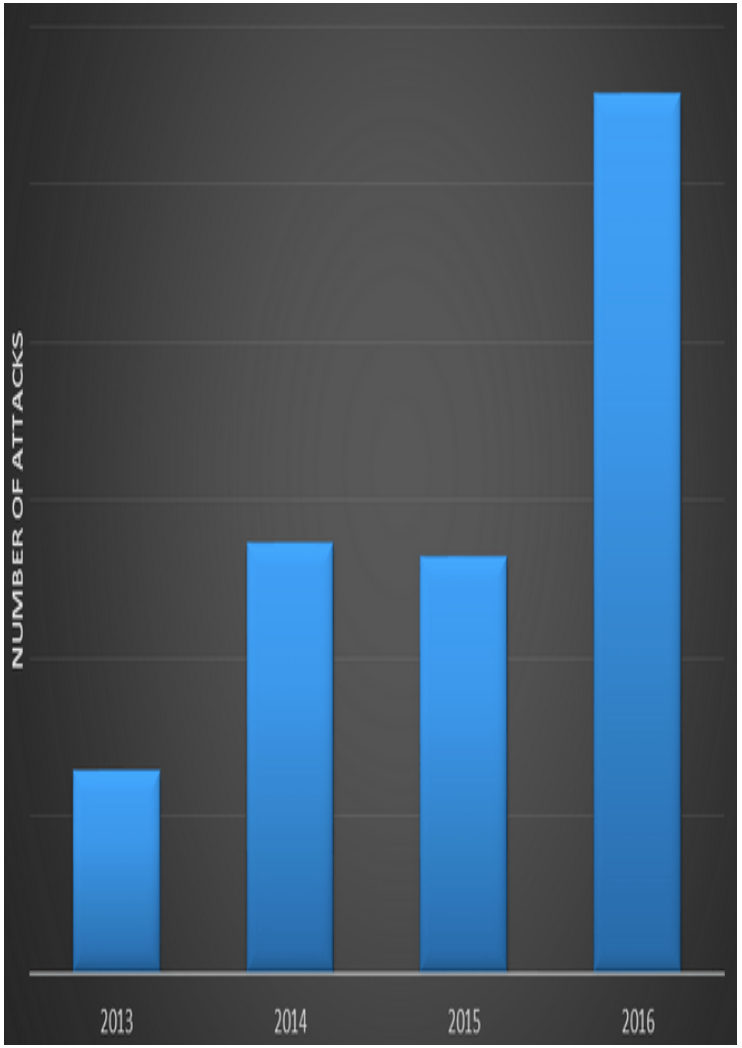
Lockheed Martin社がケンブリッジ大学に委託して調査

ICS網内での攻撃検知数が前年比倍増

IBM Managed Security Services社による報告

https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/

- 2016年はICS網内での悪意ある活動の検知数が前年比110%増
- 多くの攻撃にペネトレーション試験用ツールsmod (Modbus対応)が利用されている
- 攻撃元は，米国(60%)，パキスタン(20%)，中国(12%)など.



ICSに対するサイバー攻撃者の分類 (NIST SP800-82)

攻撃者	説明	動向
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	ランサムウェア大流行
外国諜報機関	スパイ活動	国家からの支援を受けたハッカー集団増加
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	ランサムウェア進化
テロリスト	破壊工作等で社会不安を煽る	

サイバー・セキュリティ・リスクの実態は？

- 制御システムセキュリティに関するアセットオーナー実態調査
  http://www.jpcert.or.jp/ics/asset-owner-survey_2015.pdf
  - JPCERT/CCが2015年度に実施し
    2016年に公表した実名アンケート調査
  - ICSがマルウェアに感染した経験ありとの回答が4.4%

- State of ICS Security Survey
  https://www.sans.org/reading-room/whitepapers/analyst/2016-state-ics-security-survey-37067
  - 米国SANSが2016年前半に実施した匿名アンケート調査
  - ICSのセキュリティ・インシデント経験ありとの回答が27% (前年32%)
    確信をもって経験なしとした回答は13% (前年12%)

あまり自分が運用するICSの
セキュリティ実態が分かっていない

- 実名調査と匿名調査の差？
- 日米の差？

(ブラジルの場合)

ICS環境でのインシデント件数の経年変化

種別	2008	2009	2010	2011	2012	2013	2014	2015
マルウェア	1	1	2	2	3	7	104	667
人為ミス	2	2	3	4	3	3	21	56
機器故障	0	0	1	2	4	4	8	33
破壊行為	0	0	1	0	0	0	1	1
原因不明	0	1	1	0	1	2	6	21

引用：Segurança da Informação社Marcelo Branquiho氏のs4x2017講演資料

- 日本の状況も大同小異と推測される
- マルウェア感染が大多数を占める(86%)
- ランサムウェアの大流行の中でICSの被害事例も
- ICSを攻撃するために作られたランサムウェアも登場か(?)

- 平均請求額： $2,500
- 半数がこの1年に感染事例

出典： The Rise of Ransomware (Ponemon研究所)

ICSを狙うランサムウェア

- E(電力)-ISACからの情報をもとに
  Rockwell社が顧客にメールで警告：
  「Allenbradleyupdate.zip」という悪意あるファイルが出回っている
  —実行するとランサムウェアとして動作

- 被害事例の有無は
  不明

Schneider Downs Information Security Risk Advisory Services

AIR GAPPED SCADA/ICS NETWORKS NOW THREATENED FROM RANSOMWARE

- In July, Rockwell Automation issued an alert that Ransomware malware posing as a Rockwell Automation software update was distributed as "Allenbradleyupdate.zip" posing as a legitimate Rockwell Allen Bradley patch.
- It appears this malware is targeting the electricity energy sector. This is one of the first of its kind specifically targeting commercial utility systems. There are no known victims at this time.

引用： Schneider Downs
2016年8月18日号

参考： http://www.rockwellautomation.com/ja_JP/news/news201604-KB799091-JA.page

ブラジルでのICSのランサムウェア感染事例-1

事業内容：　家具製造

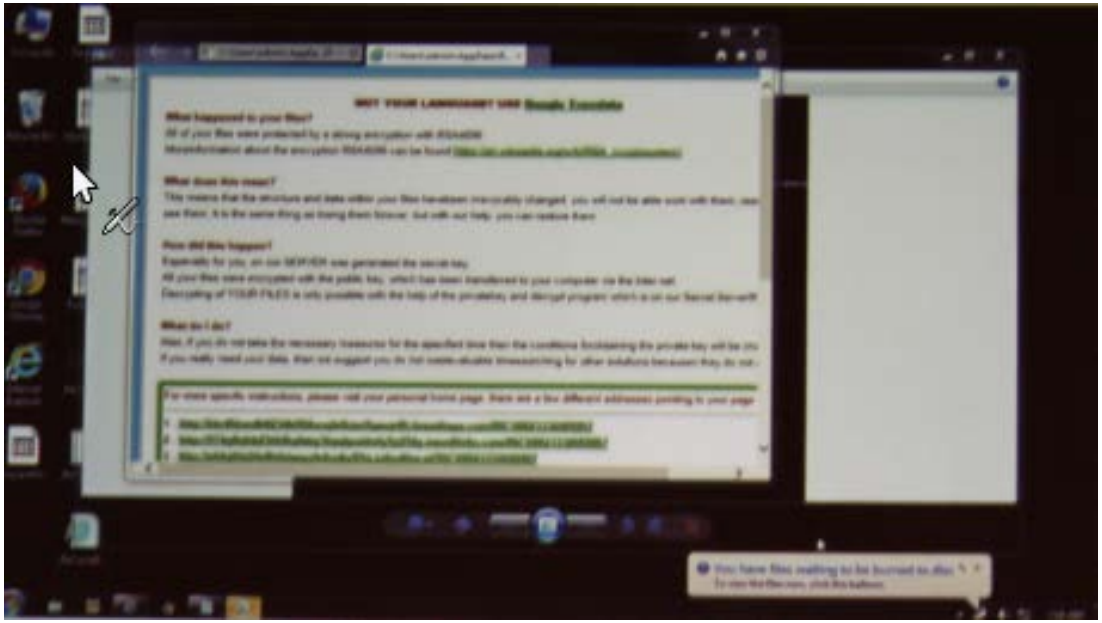
感染したマルウェア：　cryptoRSA4069ランサムウェア

感染したマシン：　工場内のWindows SCADAとHMI

請求金額：　3,061米ドル

影響：　半月間にわたり工場の操業が完全に停止

身代金を支払わないことにしたがバックアップを採取していなかったので完全にシステムを再構築(約10万ドルの損失)



引用：Segurança da Informação社
Marcelo Branquiho氏s4x2017講演資料

ブラジルでのICSのランサムウェア感染事例- 2

事業内容：　電力会社 (南部ブラジル)
感染したマルウェア：　CryptoLockerランサムウェア
感染したマシン：　制御センター内のWindows SCADA(HMI)
請求金額：　300,000米ドル/マシン (4台のマシンが感染)
影響：代替系に自動的に切り替わり正常な稼働を維持

- 最初にHMIがUSBメモリ経由で感染
- ファイル共有機構を経由して同一ネットワーク・セグメント内の他の3台も感染
- 感染したマシンはバックアップから復旧でき，身代金も支払わず

引用：Segurança da Informação社Marcelo Branquiho氏
s4x2017講演資料

サイバー攻撃で原子力発電所の運転が中断

http://www.reuters.com/article/us-nuclear-cyber-idUSKCN12A1OC

- IAEAの天野之弥事務局長が2016年10月10日にReuters紙に語った：
  数年以前にドイツ国内の原子力発電所が
  深刻なサイバー攻撃の標的となった
  - サイバー攻撃により原子力発電所の運用が実際に妨害された
  - 原子力関連施設へのサイバー攻撃を現実的な問題として真剣に対処する必要がある

(詳細については説明せず)

引用： Reuters社
TECHNOLOGY NEWS

インターネットを利用した遠隔制御がDDoS攻撃で使えず

http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter

- フィンランド東部のLappeenranta市で
  インターネット経由で遠隔集中制御されていた
  集中暖房と給湯を制御するシステムがDDoS攻撃で動かせず
  - 少なくとも2棟のビルで暖房が停止


ETELÄ-SAIMAA

ETUSIVU MEDIAMYYNTI ASIAKASPALVELU PALAUTE YHTEYSTIEDOT

Etusivu | Uutiset | Mielipide | Kulttuuri | Saa | Tapahtumakalenteri | Laivat | Lentokoneet | Videot

Hakkerit iskivät lappeenrantalaisen kiinteistön pannuhuoneeseen

6.11.2016 8:14

Kuva: Matti Saarela

Harmaa kaappi toimitusjohtaja Simo Rounelan edessäkätkee sisäänsä lappeenrantalaisen kiinteistön lämmitystä ohjaavan tietokoneen. Rounelan mukaan nykyisin tällaisia, verkkoon kytkettyjä ohjausyksiköitä voidaan asentaa myös jokaiseen asuntoon erikseen. Tällöin asuntojen lämmitystä voidaan säättää automaattisesti tai etäohjauksella kunkin huoneiston sisälämpötilan perusteella.

VIIKON LUETUIMMAT

VIIKKO | KUUKAUSI

- Nainen jäi junan alle Lappeenrannassa
- Fitness-dieetti vie mehut kropasta ja mielestä, lääkäri ja entinen fitness-tähti jarruttelevat kiinnostuneita
- Eekoo avaa kesällä pakohuoneita Lappeenrannan keskustaan
- Kouvolan risumies ja Youtube-videon kuvaaja oikeuteen huhtikuussa – kumpikin syytteeseen rikoksesta
- Kommentti: SaiPa heitti pyykkeen kehään – Mutta miksei sitä voi sanoa suoraan?
- Kolumni: Shishapiiput Marian aukiolla
- Alakanttiin mennyt kausi harmittaa Zugin siirtynyttä Jussi Markkasta – "Yleisöllä täytyy olla oikeus äänestää jalollaan"
- 91-vuotias kotiutettiin omaisen mukaan liian huonossa kunnossa – Kerro kokemuksiasi Eksoten vanhushuollosta
- Savon Mafia pisti töpinäksi – Lappeenrannan Kylpylä sai oman ravintolan ja kuntosalin. Katso kuvat!

引用： ETELA-SAIMAA
http://www.esaimaa.fi/Online/2016/11/06/Hakkerit%20iskiv%C3%A4t%20lappeenrantalaisen%20kiinteist%C3%B6n%20pannuhuoneeseen/2016121454255/4

引用： Metropolitan Fi.

研究者がPLCワームを試作

Ralf Spenneberg他: PLC-Blaster: A Worm Living Solely in the PLC”

https://regmedia.co.uk/2016/04/29/plc_87458745.pdf

http://i.imgur.com/C6KeXBt.gif

- ドイツのセキュリティ研究者が考案し BlackHat Asiaで講演
- PLCのFunction Blockとしてワームの動作を記述
  - 同じネットワーク中の他のPLCを探索しそれを自身(ワーム)に感染させる能力
  - Siemens社製S7コントローラを用いて試作・実証
    (Function Blockに十分な記述能力があれば他のPLCでも実現できる)
  - ネットワーク内で感染したPLCが他のPLCを直接攻撃
    （コンピュータを介さずに感染を拡大）

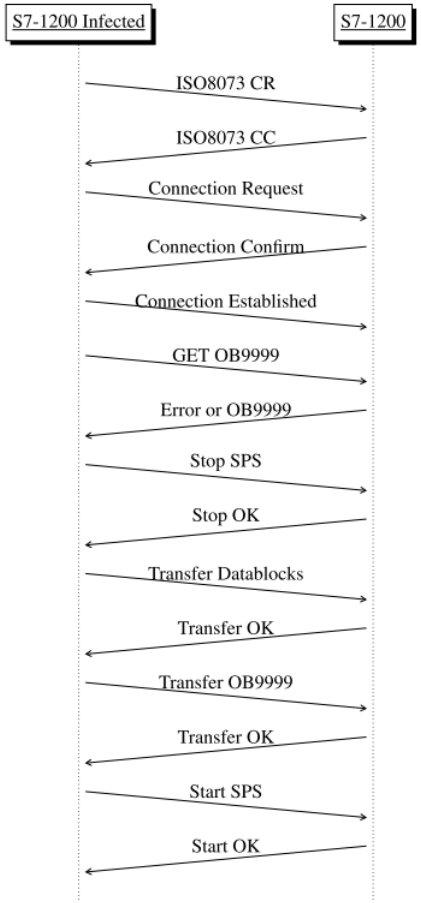


Figure 11. Messages exchanged during infection

ICSを狙って作られた不思議なマルウェアIronGate

FireEye社： IRONGATE ICS Malware: Nothing to See Here...Masking Malicious Activity on SCADA Systems

https://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html

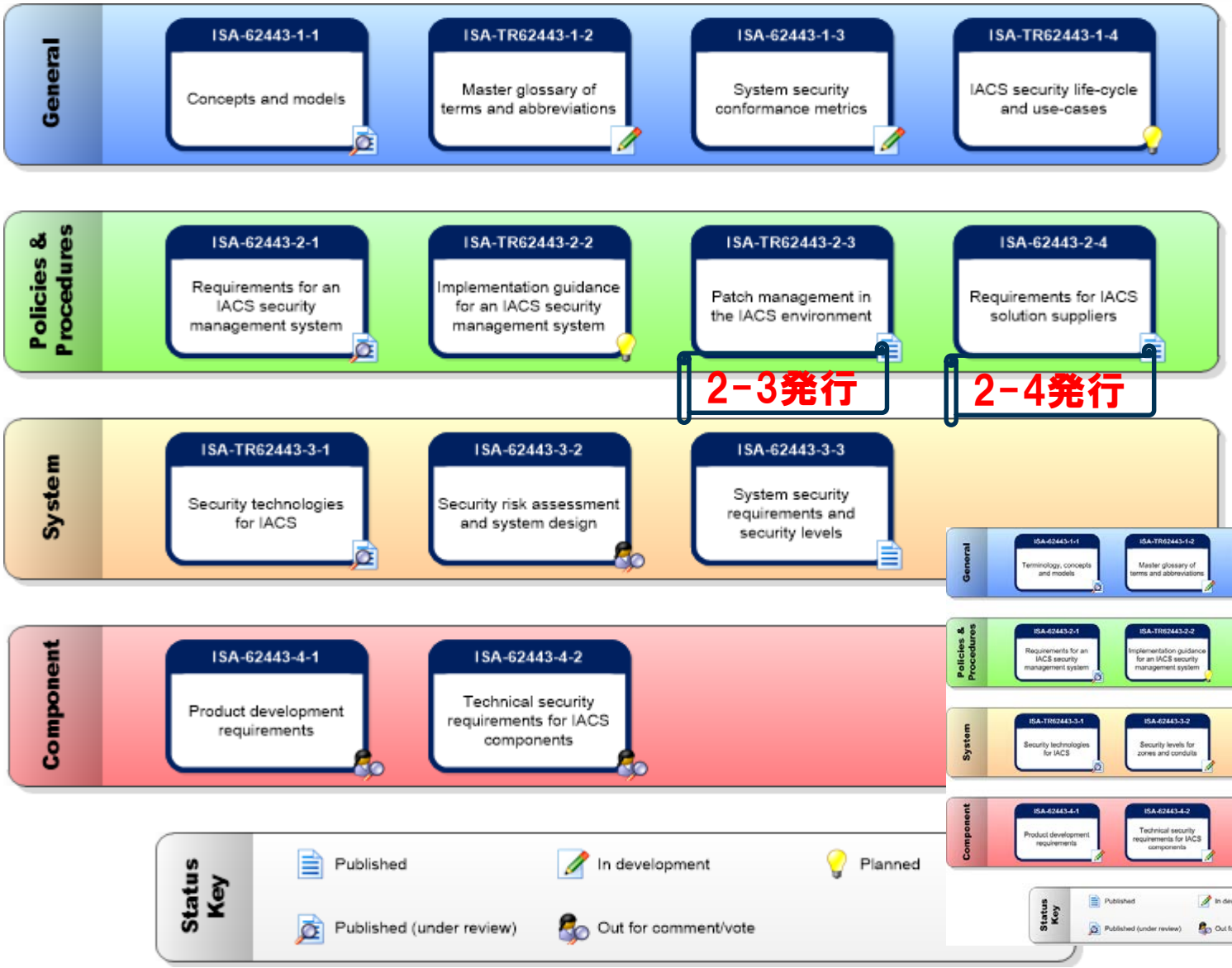
- 2014年に複数の研究者がVirusTotalにアップロード
- 2016年6月になってFireEye社の研究者が動作を解析して報告

- Siemens社のPLCシミュレータ環境で動作
- 本来のDLLを置き換えて中間者攻撃を行う
  (Stuxnetを思い起こさせる動作；
  Stuxnetとコードが類似しているわけではない)
  - 動作環境が実環境か否かを検知して動作を変える
    (分析されることを回避するため)

- 現実の制御システムに及ぼす被害は無さそう
  - ICSを狙った本格的なマルウェアを開発するための試作品か？

ICSセキュリティの標準化に関する動向

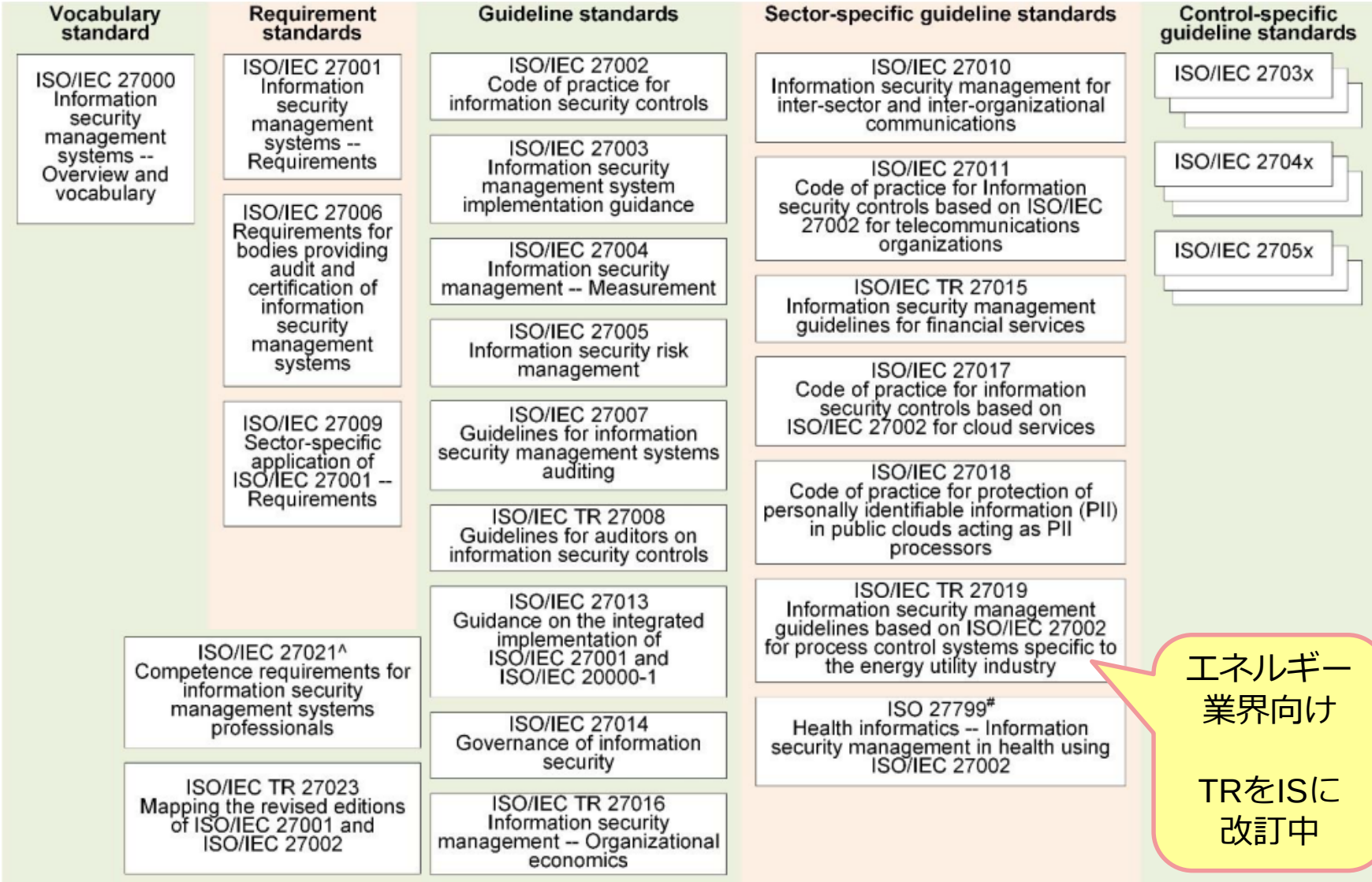
ISA/IEC 62443シリーズ標準化(2016年は動きなし)



2015年

ISO/IEC 27000シリーズ標準化

業界ごとのガイドライン



エネルギー業界向け

TRをISに改訂中

ICSセキュリティに関する認証

	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)	CAP； CCST (ISA)
	UL CAP for ICS (UL)		開発プロセス	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
Achilles Communications Certification	22	135	216 (**GE社が買収**)	**294**	**472**
EDSA (ISA ISCI)	0	5	9	11	13
UL CAP for ICS (UL)					0

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

- 米国ISA Secureと日本のCSSCが認証している
  EDSA (Embedded Device Security Assurance)も少し前進

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

ISASecure® CSSC認証ラボラトリー

UL CAP for ICS

UL Cybersecurity Assurance Program for Industrial Control Systems

- ULは，安全に関する評価試験を事業とする米国の営利企業
  - 2012年まではUnderwriters Laboratories Inc.という非営利企業として100年以上の歴史

- CAP(Cybersecurity Assurance Program)を4月5日に発表
  http://www.ul.com/newsroom/pressreleases/ul-launches-cybersecurity-assurance-program/
- サイバー・セキュリティ標準UL 2900シリーズを策定
  http://www.ul.com/cybersecurity/
  - UL 2900-1： 製品試験
  - UL 2900-2-x： 業界ごと製品試験
  - UL 2900-3： 組織とプロセスの試験
- ICSのサイバー・セキュリティ標準を
  UL 2900-2-2として策定

システムに対する認証をドイツTÜV SÜDが付与

- 2016年11月にドイツTÜV SÜDが
  Siemens社製Simatic PCS7をセキュアなシステムとして
  初めて認証
  http://www.tuev-sued.de/company/press/news/tuev-sued-certifies-siemens-process-control-system-according-to-iec-62443
  - IEC 62443-4-1およびIEC 62443-3-3に基づく認証

- ISA SecureのSSA (System Security Assurance)は
  まだ認証実績がない模様

ICS製品の開発プロセスに対する認証

- IEC 62443-SDLA (Security Development Lifecycle Assurance)としてISA SecureがセキュアなICS製品の開発組織を認証
  http://www.isasecure.org/en-US/Certification/IEC-62443-SDLA-Certification
  - 2016年に新たに3拠点が認証され，合わせて6拠点にSchneider社の5拠点(英米印カ力)，Honeywell社の1拠点(米)
    http://isasecure.org/en-US/End-Users/ISASecure-Certified-Development-Organizations

- ドイツTÜV SÜDも2016年8月に最初の認証を付与
  - IEC 62443-4-1に基づく
  - 2016年8月にSiemens社の1拠点を認証
    https://www.siemens.com/press/PR2016080373DFEN

TÜV SÜDではICSインテグレータの開発プロセスを
IEC 62443-2-4に基づいて認証する計画も

ICSの運用管理に対する認証

- JIPDECがICSを対象としてサイバー・セキュリティ・マネジメント・システム(CSMS)を認証
  http://www.isms.jipdec.or.jp/csms.html
  - IEC 62443-2-1に基づいて
    ICSの運用組織またはインテグレーターを認証
  - 2016年に3組織が新たに認証され，合わせて5組織に
    https://www.isms.jipdec.or.jp/csms/lst/ind/
    - 3月： 東京ガス(株)日立LNG基地
    - 9月： メタウォーター(株)
    - 10月: (株)MHPSコントロールシステムズ(製造部)

Industrial Internet Consortiumから セキュリティ・フレームワーク

- Industrial Internet of Things
  Volume G4: Security Framework
  https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf

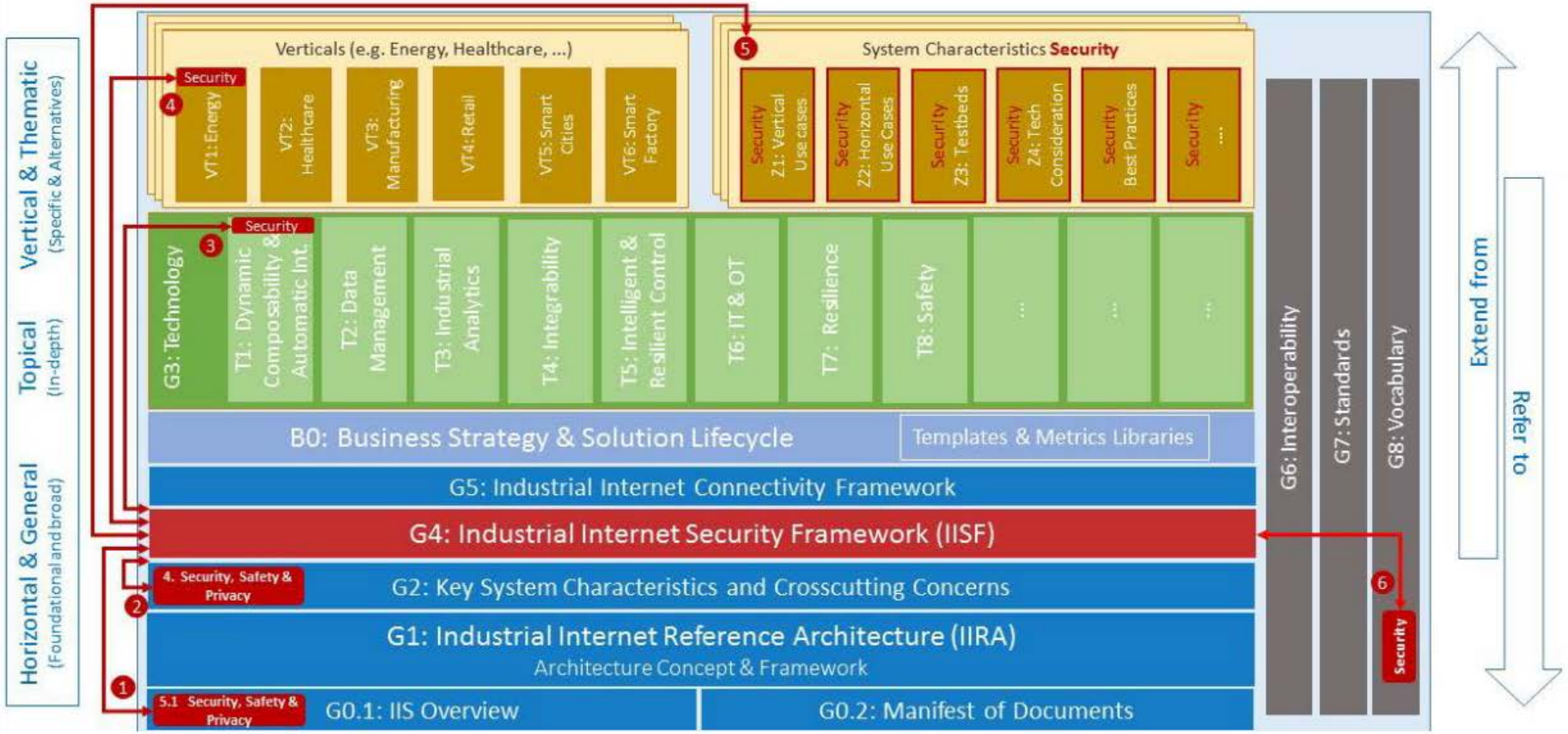
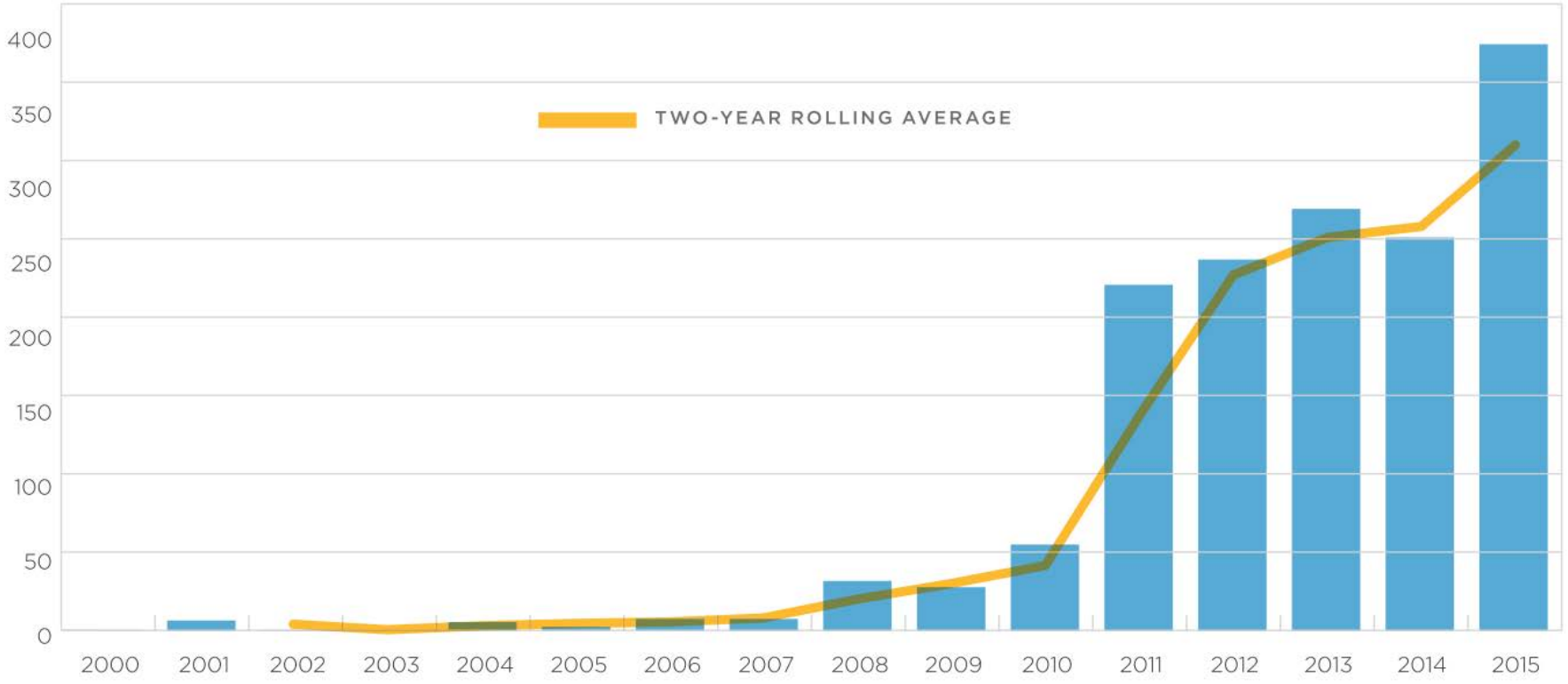


Figure 1-1: IIC Technical Publication Organization

ICS製品の脆弱性に関する動向

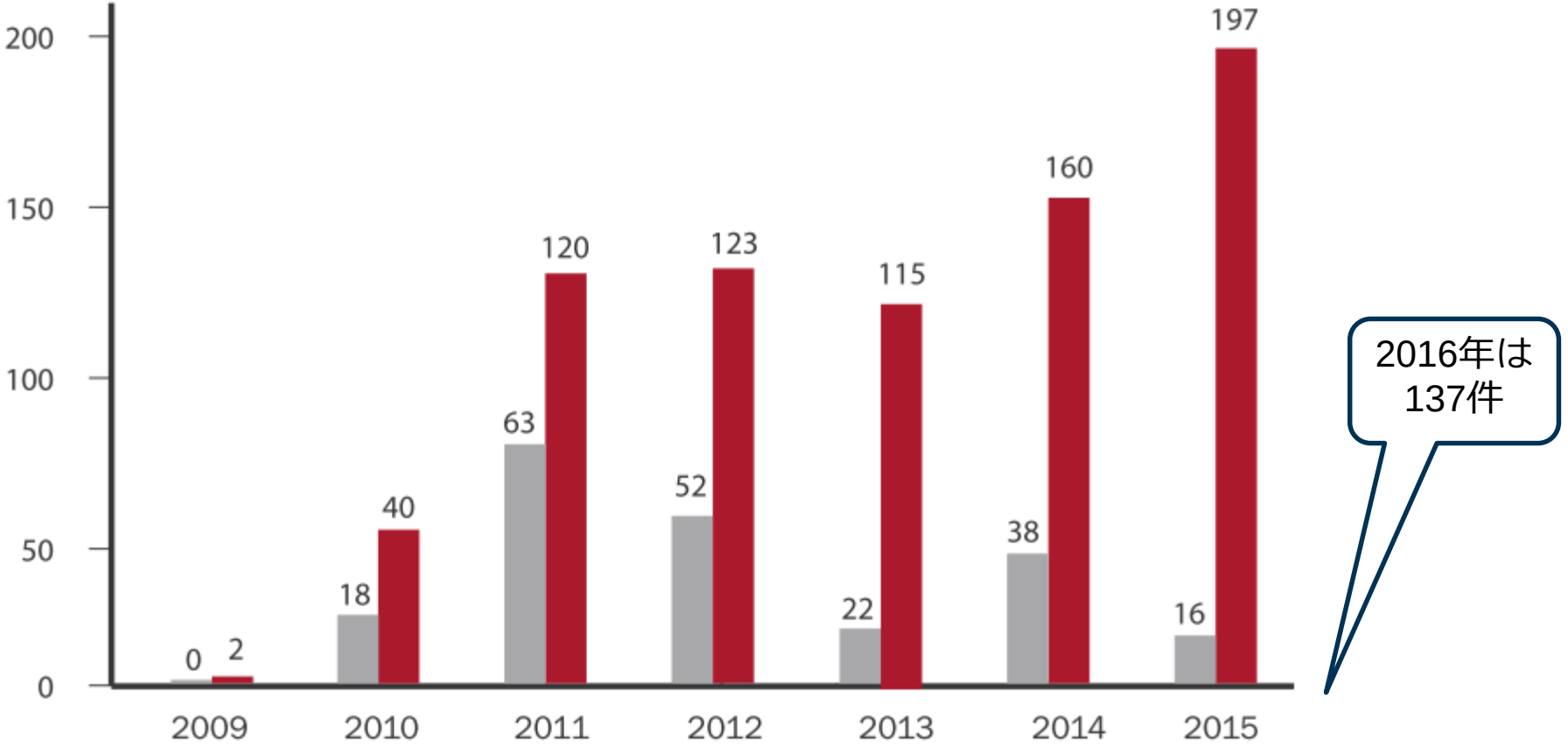
ICS製品の脆弱性報告数の推移

- 2011年以降の脆弱性報告件数は
  毎年200件前後の水準で推移した後さらに増加傾向か



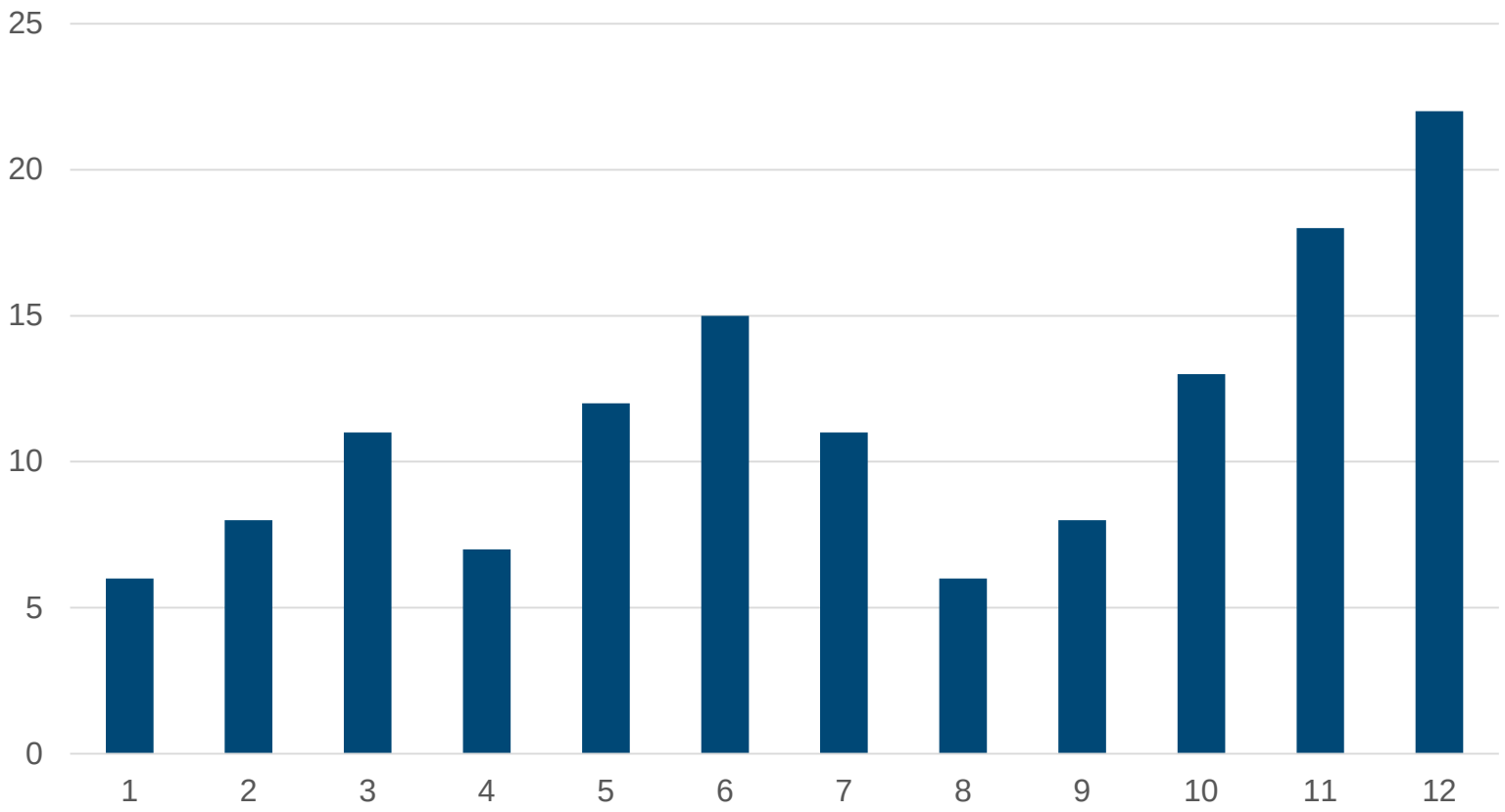
引用： FireEye社： Overload Critical Lessons from 15 Years of ICS Vulnerabilities
https://www2.fireeye.com/rs/848-DID-242/images/ics-vulnerability-trend-report-final.pdf

米国ICS-CERTが公表した脆弱性アドバイザリ数



引用： NCCIC/ICS-CERT FY2015 Annual Vulnerability Coordination Report
https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_FY%202015_Annual_Vulnerability_Coordination_Report_S508C.pdf

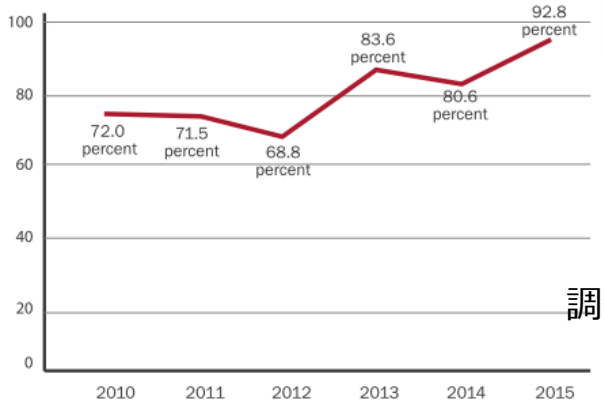
米国ICS-CERTが2016年に公表した脆弱性アドバイザリ数



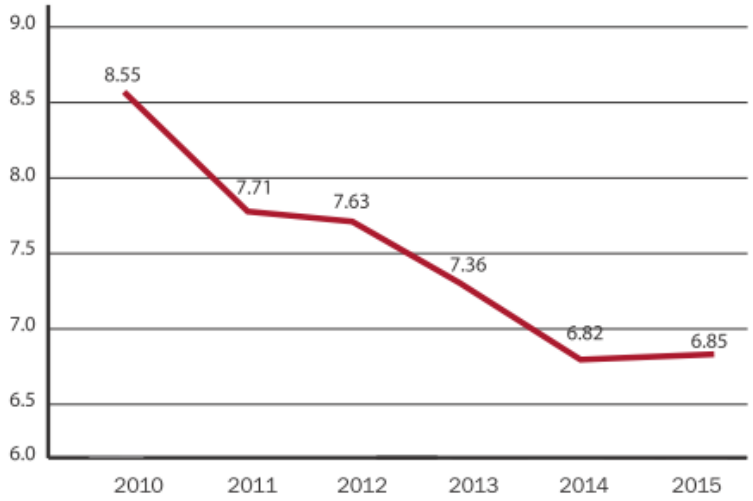
引用：2016年にICS-CERTが公表した脆弱性アドバイザリ数の月ごとの推移をJPCERT/CCが作図

脆弱性の取扱いの成熟度が向上

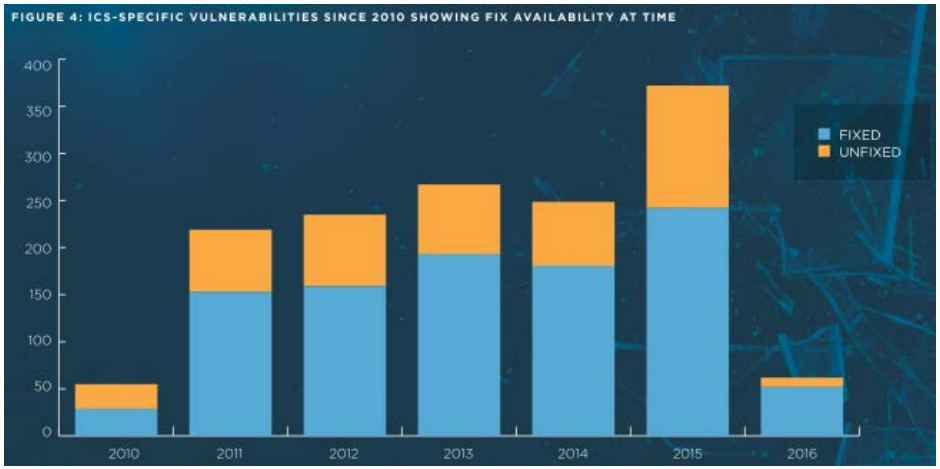
- 調整された開示が大多数に
  - ベンダーの取組みが進展
- 脆弱性の平均深刻度も低下



調整された開示の割合の推移
引用： ICS-CERT



平均CVSS値の推移
出典： ICS-CERT



公表時にパッチの有無の割合の推移
引用： FireEye社

- 単純化Purdueモデルの第3層(HMIやSCADA等)の製品が過半数を占める

ICS製品の脆弱性の種類

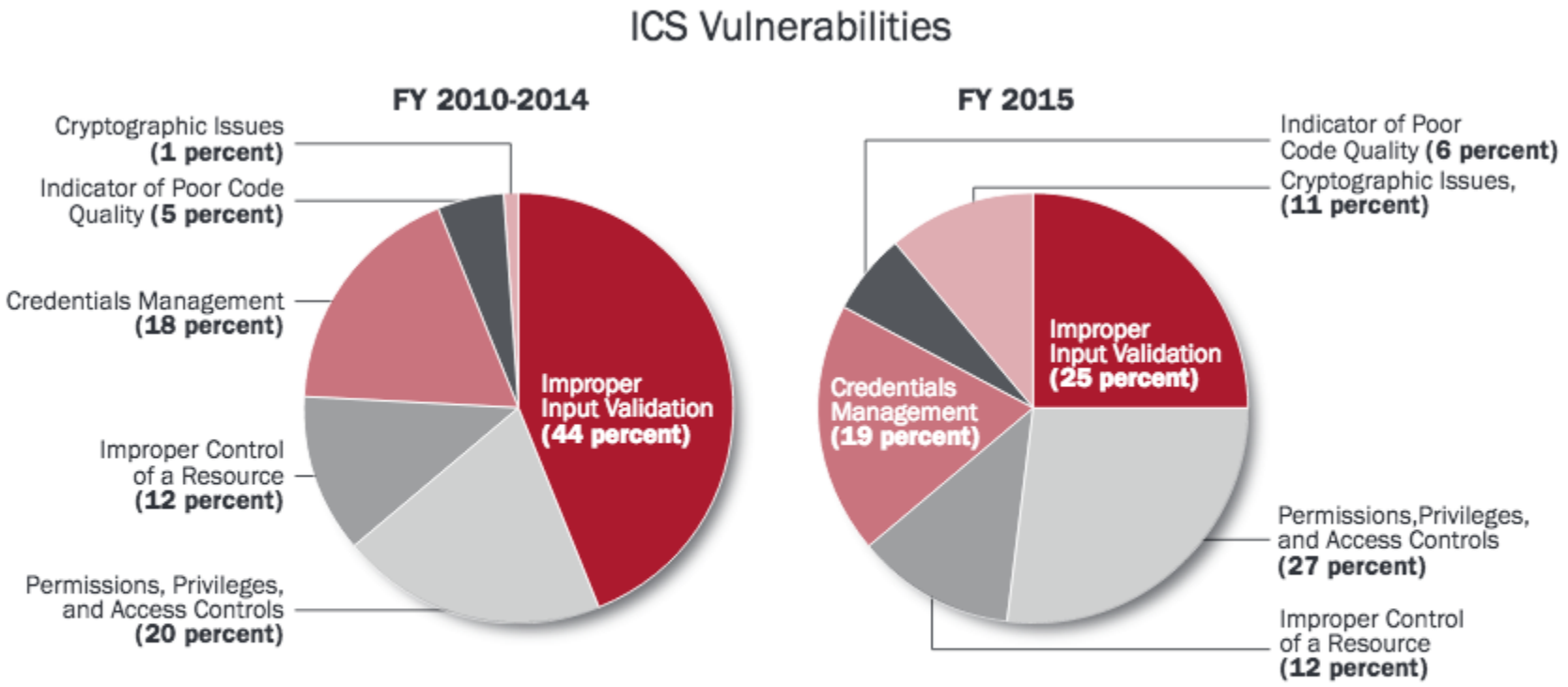


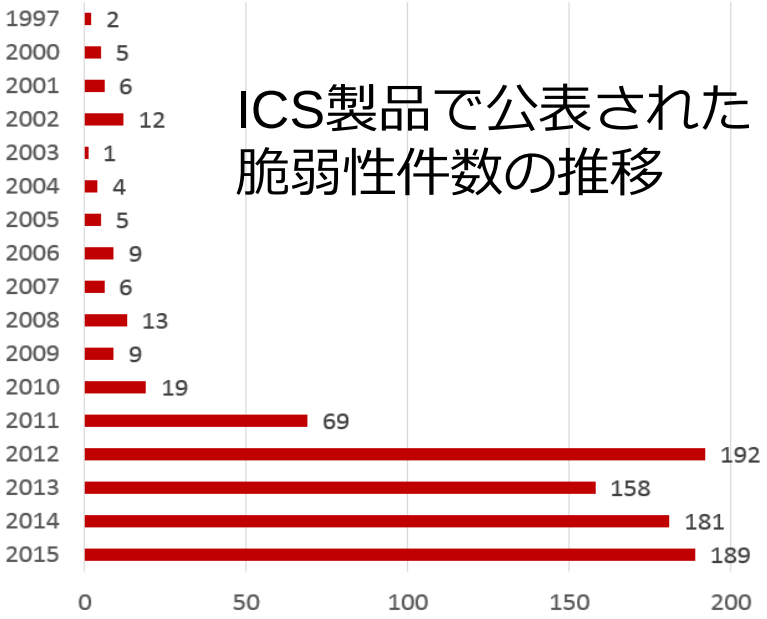
Figure 9. Categories of all vulnerabilities reported to ICS-CERT.

引用： FireEye社

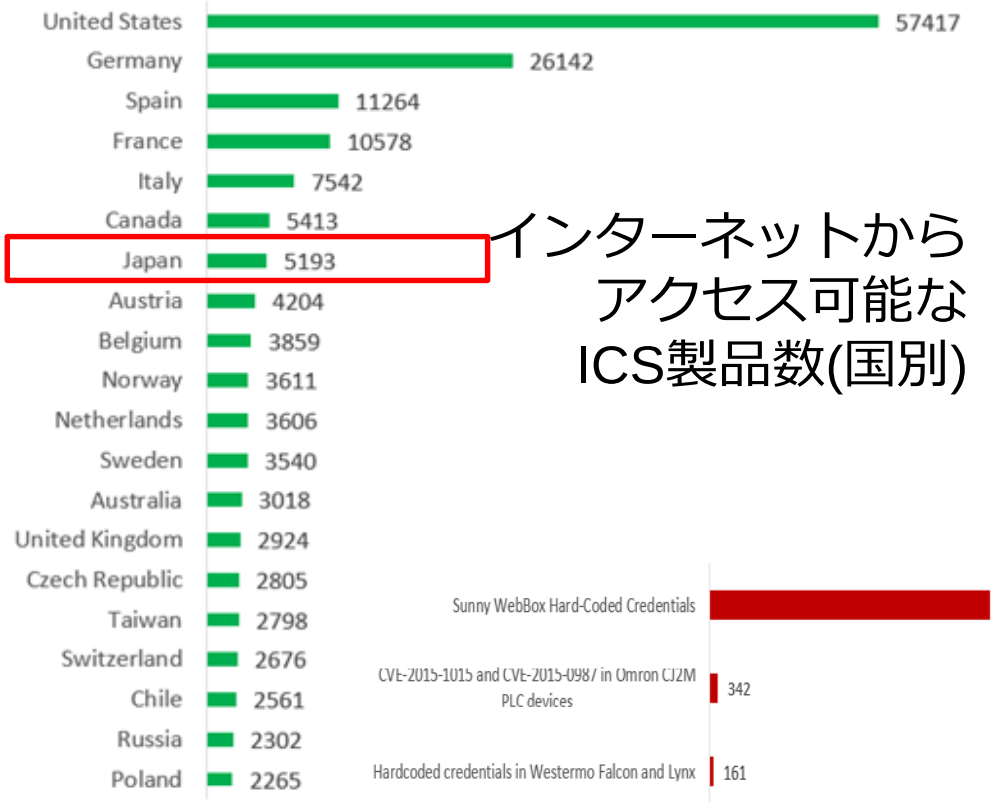
- 入力検証の不備が減少
- 特権の管理やアクセス制御の誤りが増加
- 認証子の管理の問題も減らず

ICS製品の脆弱性に関する調査資料

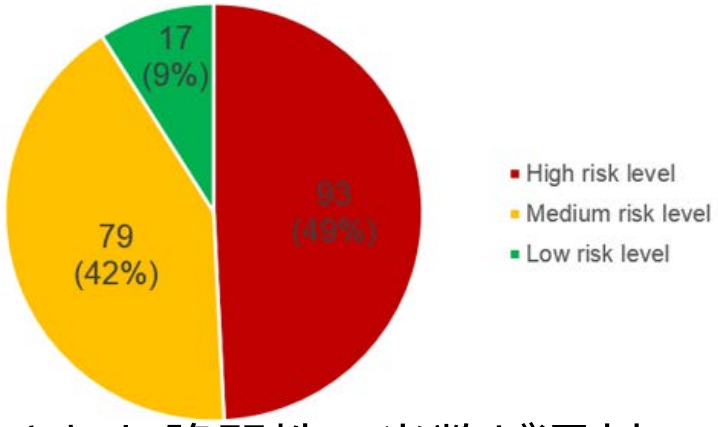
(出典：Kaspersky社)



ICS製品で公表された
脆弱性件数の推移



インターネットから
アクセス可能な
ICS製品数(国別)



公表された脆弱性の半数が深刻

出典：
https://securelist.com/analysis/publications/75343/industrial-cybersecurity-threat-landscape/

脆弱性の今後については明るくない見通しも

- なかなか改まらない製品開発の基本思想
  - 例えば，出荷製品へのデフォルト・パスワードの設定
    SCADAPass：
    研究者がICS製品における100以上の事例を一覧表で公表
    http://www.darkreading.com/endpoint/researchers-out-default-passwords-packaged-with-ics-scada-wares/d/d-id/1323755

- ゼロディ脆弱性は今後も容易に減りそうにない
  Zero Day Report
  http://cybersecurityventures.com/zero-day-vulnerabilities-attacks-exploits-report-2017/
  - 拡がり続ける脆弱性の界面
    - 毎年の新たなコーディング量： 1,100億行
  - オープン・ソース・コードへの依存性の高まり
    - 商用のアプリケーションでもコードの3割がオープン・ソース由来
    - 2017年末時点ではミッション・クリティカルなソフトウェアの99%が
      オープン・ソース由来のコードを含む (Vmware社副社長の予測)

ハードウェアとの境界部分に対する新たな攻撃手法も

- PLCに搭載されているSoCについて
  I/Oピンの設定情報を書き換えることにより
  PLCの動作を無効化するなどが可能
  Ghost in the PLC Designing an Undetectable Programmable Logic Controller Rootkit via Pin Control Attack
  https://www.blackhat.com/docs/eu-16/materials/eu-16-Abbasi-Ghost-In-The-PLC-Designing-An-Undetectable-Programmable-Logic-Controller-Rootkit-wp.pdf

- アナログ・デジタル変換器について
  サンプリング周波数を操作することにより
  不正な値が観測されるようにできる
  How to Fool an ADC Or how to hide the destruction of a turbine with the help of DSP
  https://www.blackhat.com/docs/eu-16/materials/eu-16-Gonzalez-How-To-Fool-An-ADC-Part-II-Or-Hiding-Destruction-Of-Turbine-With-A-Little-Help-Of-Signal-Processing.pdf

参考資料

2016年前後に発行された調査資料

- 米国SANS： ICSセキュリティ現状調査
  SANS 2016 State of ICS Security Survey
  (2016年6月)
  https://www.sans.org/reading-room/whitepapers/analyst/2016-state-ics-security-survey-37067

- JPCERT/CC： 2015年度 制御システムセキュリティに関するアセットオーナー実態調査
  http://www.jpcert.or.jp/ics/asset-owner-survey_2015.pdf

- IPA：重要インフラの制御システムセキュリティとITサービス継続に関する調査報告書
  http://www.ipa.go.jp/security/fy20/reports/ics-sec/index.html

2016年前後に発行された技術的な参考資料

- アプリケーション・ホワイト・リスティング
  - NIST SP800-167： Guide to Application Whitelisting (2015年10月)
    http://csrc.nist.gov/publications/drafts/800-167/sp800_167_draft.pdf
  - DHSから6ページの資料 (2015年12月)
    https://ics-cert.us-cert.gov/sites/default/files/documents/Guidelines for Application Whitelisting in Industrial Control Systems_S508C.pdf

米国ICS-CERTリプリント資料

- Cybersecuring Healthcare Building Control Systems
  https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/QNL_SEP_16/NIBS_0816_Cybersecurity_Chipley_Reprint_S508C.pdf

- Deploying ICS Security in a Right Way
  https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/QNL_SEP_16/ICSJWG_Daniel_Ehrenreich_September_2016_S508C.pdf

- ICS CYBER SECURITY
  https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/QNL_SEP_16/An_Integrated_Approach_to_Protecting_Industrial_Control_Systems_S508C.pdf

- The Perfect Storm Solving critical infrastructure challenges by evolving today's IP networks
  https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/QNL_SEP_16/The_Perfect_Storm_Final_S508C.pdf

JPCERT/CCが提供するICSセキュリティ関連サービス

- インシデントの報告受付と支援依頼
- 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)
- 情報ベースConPaS
  (登録が必要)
- 参考情報
- 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

http://www.jpcert.or.jp/ics/ics-form.html

迅速に脆弱性情報を受け取るため
http://www.jpcert.or.jp/vh/regist.html

http://www.jpcert.or.jp/ics/ics-form.html

http://www.jpcert.or.jp/ics/ics-form.html

今後ともよろしくお願いします

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

ご静聴ありがとうございました