JPCERT CC®

制御システムセキュリティ 2011年度動向報告

一般社団法人JPCERTコーディネーションセンター
理事 宮地 利雄

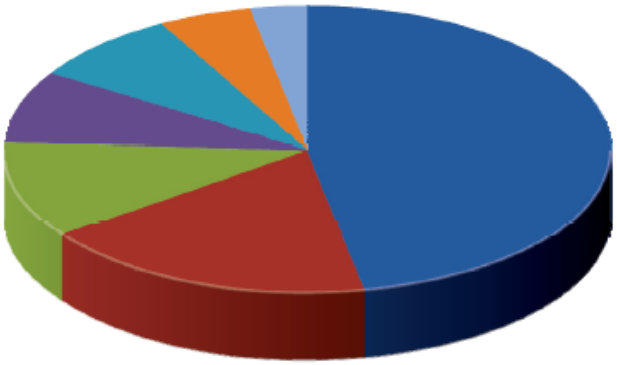
概要

- Stuxnet発見の報告から約1年
  - 露呈した制御システム製品の脆弱さ
  - 高まるマスコミの注目
  - 本格化する各国政府の取組み
  - セキュリティ標準の整備
  - Stuxnet後継マルウェア？
- 拡大する制御システムのオープン化
  - 制御システム分野でのオープン技術の拡大
  - オープン技術への転換が進む制御システム

米国ICS-CERTから一般公表された脆弱性

JPCERT CC®

- 制御システム製品の脆弱性の報告が急増
- 初歩的な脆弱性が大多数を占める



10-GA50251-47

- 47% Improper Input Validation
- 18% Permissions, Privileges, and Access Controls
- 11% Improper Authentication
- 8% Insufficient Verification of Data Authenticity
- 8% Indicator of Poor Code Quality
- 5% Security Configuration and Maintenance
- 3% Credentials Management

Figure 1. Categories of vulnerabilities identified in 2009–2010 CSSP product assessments.

SeonMcBride氏のまとめ

年	ICS-CERT アドバイザリ
2009	活動開始(秋)
2010	20
2011	66

- 設計に由来する脆弱性も少なくない
  - ICS-CERTでは脆弱性とせず
  - 研究者から批判の声

出典：Common Cybersecurity Vulnerabilities in Industrial Control Systems (2011-05)

セキュリティ研究者が制御システムにも注目

JPCERT CC®

- Luigi Auriemma氏（イタリア）
  31歳，ミラノ在住の無神論者
  - 2011年3月の34件以降に次々と多数の脆弱性をブログで公表
  - 開発者への通知をしないままのゼロディ脆弱性の公表も
  - 多くはPoC(実証)コードも公表
  - 脆弱性の探索に使っている複数のツールも公表

参考）http://aluigi.org

Auriemma氏の
実験室の様子
出典：Digitalic

Agora SCADA+ Pack

- ロシアのセキュリティ企業が提供（ライセンス販売）
  http://gleg.net/agora_scada.shtml
- SCADA関連の脆弱性に対する攻撃コード・パッケージ
- 公表されたすべての脆弱性のカバーをめざす
- 制御システムの11件のゼロディ脆弱性を攻撃する22のモジュールも（2011年3月の発表当時）
- ICS-CERTも警告 (ICS−ALERT-11-111-01)

関連記事：http://mobile.eweek.com/c/a/Security/Russian-Firm-Dumps-SCADA-ZeroDay-Exploits-into-the-Wild-685614/

セキュリティ研究者が制御システムにも注目

- Terry McCorkle氏とBilly Rios氏
  - 余暇時間で脆弱性探索
  - 無料でダウンロードできる製品76件を対象に脆弱性探索
  - 探索過程を研究集会(DerbyCon)で講演
  - 665件の脆弱性を発見
    - 360件：ファジングで発見
    - 204件：アクティブXの脆弱性
    - 90件：ウェブ・アプリケーションの脆弱性

参考）

www.irongeek.com/i.php?page=videos/derbycon1/mccorkle-and-rios-100-bugs-in-100-days-an-analysis-of-ics-scada-software

Terry McCorkle氏

Billy Rios氏

セキュリティ研究者が制御システム用PLCに注目

JPCERT CC®

- DigitalBond社のBasecampプロジェクト
  - Reid Wightman氏が率いる6人の専門家チームが脆弱性探索
  - 対象は6種類のPLC
    - 日本のベンダー製品を含む
  - 2012年1月のS4で講演

参考）
http://www.digitalbond.com/2012/01/19/project-basecamp-at-s4/

	A-B QUALITY	Schneider Electric	GE	SEL	Koyo
Firmware	!	✗	!	!	!
Ladder Logic	!	!	✗	!	✗
Backdoors	!	✗	✗	✓	✓
Fuzzing	✗	✗	✗	!	!
Web	!	✗	N/A	N/A	✗
Basic Config	!	!	✗	!	!
Exhaustion	✓	✓	✗	✓	✓
Undoc Features	!	✗	✗	!	!

✗：容易に攻撃できる脆弱性あり
!：容易には攻撃できない脆弱性あり
✓：脆弱性が発見されず

脆弱性だらけの制御システム製品

JPCERT CC®

- 攻撃される可能性を想定せずに設計開発
  - セキュリティ教育を受けないまま設計・開発
  - セキュリティのレビューや試験をしないまま出荷

- 古典的な脆弱性が山積
  特に:
  - HMI
    - ✓パスワードの取扱い
    - ✓ウェブ・アプリケーションの脆弱性(XSSやSQLインジェクション等)
  - PLC等のフィールド機器
    - ✓バッファー・オーバーフローなど

Table 5. Top 10 most critical ICS vulnerabilities.

Rank	Impact/Vulnerability	Generalized CVSS v2 Score
1	Most Likely Access Vector/ Unpatched Published Vulnerabilities	9.8
2	Supervisory Control Access/ Use of Vulnerable Remote Display Protocols	9.8
3	Supervisory Control Access/ Web HMI Vulnerabilities	9.8
4	ICS Host Access/ Buffer Overflows in ICS services	9.3
5	Access to ICS Applications/ Improper Authentication	9.3
6	...o ICS Functionality/ ...ss Control (Authorization)	9.1
7	.../ ...ith Clear-text Authentication	9.0
8	Un... ...lentials	9.0
9	Supervisory ... ICS Data and Comm...	8.8
10	Data Historian Access/ SQL Injection	8.6

ICSの弱点評価報告書 (INL, 2010年)
http://www.fas.org/sgp/eprint/nstb.pdf

Snort (オープンソースのIDS)やMetasploit(侵入試験ツール)のICS対応機能も拡充

インシデント情報を嗅ぎまわるマスコミ

- 停電させようとカナダの電力会社にハッカーが侵入（3月）
  http://www.montrealgazette.com/news/Hackers+worry+power+industry/4439455/story.html
- フロリダの風力タービンの制御システムに匿名ハッカーがアクセス（4月；**アクセス画面自体が偽造だった模様**）
  http://cwonline.computerworld.com/t/7301040/46526483/507346/0/
- 英国Idappcom社は制御システムへの攻撃増大に対応するためにIPS/IDSを強化（4月）
  http://financial.tmcnet.com/news/2011/04/21/5459968.htm
- Q1とPonemon両研究所の報告書が電力業界における対策の立ち遅れを指摘（4月）
  http://q1labs.com/content/press-details/q1-labs-and-ponemon-institute-study-finds-alarming-exposure-to-cyber-attack-in-nations-critical-infrastructure/108.aspx

水道設備にハッカーが侵入してポンプを破壊

- Springfieldの水道事業者の設備にハッカーが遠隔からアクセスしてポンプを破壊（11月上旬）
  http://www.computerworld.com/s/article/9222080/FAQ_What_you_should_know_about_the_Illinois_water_district_SCADA_breach
- ロシアからのサイバー攻撃か？

  - ICS-CERTとFBIが現地調査
  - サービス事業者(モスクワへ家族旅行中)が事業者からの依頼により遠隔アクセスしたもの（事件性なし）
  - ポンプは経年劣化により焼損した

南ヒューストン市の下水道施設

By: a guest | Nov 19th, 2011 | Syntax: None | Size: 5.87 KB | Hits: 27

```
1.  -----BEGIN PGP SIGNED MESSAGE-----
2.  Hash: SHA1
3.
4.                 ___   __
5.                / _ \ / _|
6.    _ __   _ __| | | | |_
7.   | '_ \| '__| | | | |  _|
8.   | |_) | |  | |_| | |
9.   | .__/|_|   \___/|_|
10.  | |       PRESENTS
11.  | |   SCADAPOCALYPSE.
12.  |_|    Or something.
13.      FLUFFYBUNNYMAGEDDON.
14.____ _  _     _  _ ____ ____ ____  /
15.|  | |__|     |\ | |  | |___ [__   /
16.|__| |  |     | \| |__| |___ ___] .
17.
18.
19.___
20. |
21. |
22.
23. ###
    ###
24.
25. Hel
26. It's
27. I've
    SCA
28. It's
    litt
    inst
29. I wo
    bec
    onl
    and
```

- 「pr0f」と名乗るハッカーが，南ヒューストン市の下水道施設の制御システムが，インターネットから侵入可能な状態で運用されていることを暴露（11月）

http://threatpost.com/en_us/blogs/was-three-character-password-used-hack-south-houstons-water-treatment-plant-siemens-default-11

Springfieldのニュースを聞いて，このシステムをたまたま調べてみたら侵入可能だった；注意喚起だけが目的で侵入の意図はない

無防備のシステムだから，私の行為はハックと呼ぶことさえできない；スキルの片鱗もない，こんなシステムの作りなら，Simaticの知識さえあれば，2歳児にだってできる

— pr0f

ハッカーが米国北西部で鉄道の運行を妨害

- 米国の運輸安全管理局(TSA：Transportation Security Administration)の内部メモを入手したとして報道
  http://www.nextgov.com/nextgov/ng_20120123_3491.php

- 米国北西部の鉄道会社(会社名は非開示)のコンピュータをハッカーが攻撃（12月1～2日）
  - 鉄道の信号が混乱
  - 徐行運転を余儀なくされて約15分の遅れを伴うダイヤの乱れ
- これまで鉄道はサイバー攻撃とは無縁と考えられていたが，深刻な影響を受けうるとして注意を喚起

RISI報告書
(Repository of Industrial Security Incidents)

JPCERT CC®

- マルウェア感染に関する報告書（2011年1月14日）
- 石油業界のインシデントに関する報告書（2011年2月1日）
- 上下水道業界のインシデントに関する報告書（2011年2月1日）

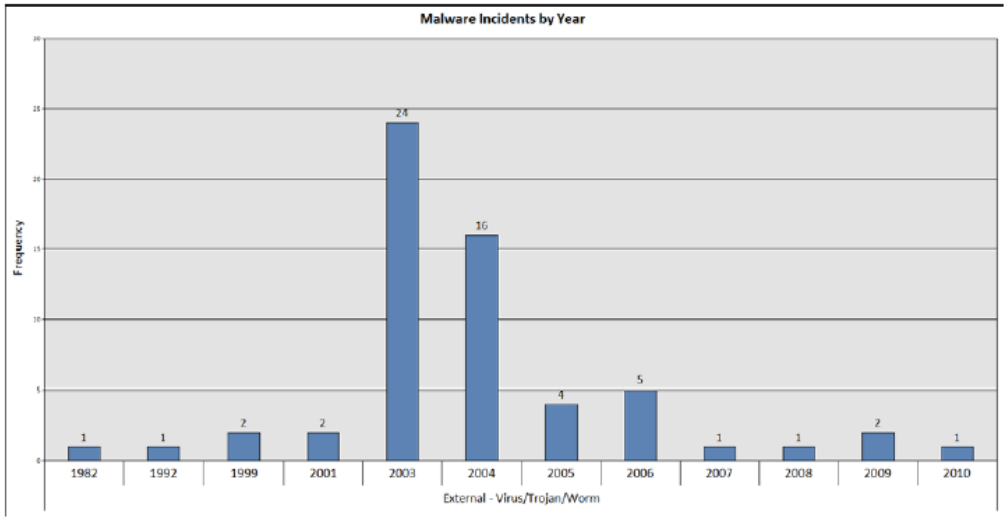


Figure 2-2: Malware Incidents by Year

- 近年のインシデントはマスコミ報道された事案のみ
- RISIの報告に基づいてインシデント情報を収集する事業モデルが破綻

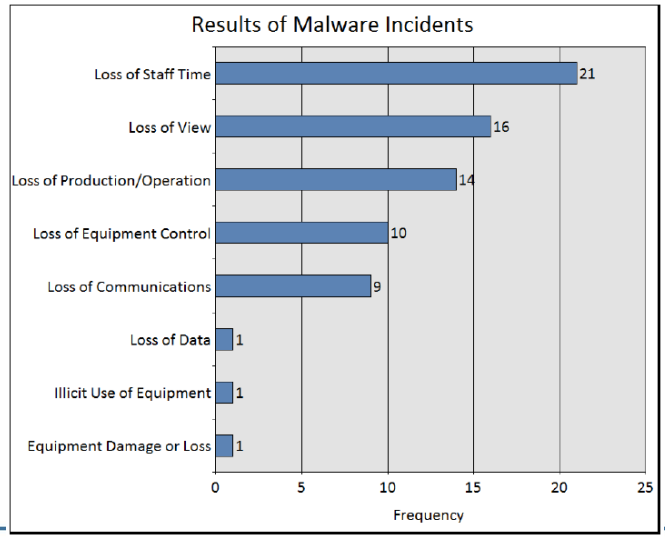


Figure 2-5: Results of Malware Incidents

ICSサイバー・セキュリティに関するロードマップ

- DoE(エネルギー省):
  「エネルギー業界向けサイバー・セキュリティ・ロードマップ」を改訂
  (初版は2006年)(9月)
  http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf

- DHS(国土保安省)のICSJWG:
  「ICSサイバー・セキュリティの業界横断的ロードマップ」を公表(11月)
  http://www.us-cert.gov/control_systems/pdf/Cross-Sector_Roadmap_9-30.pdf
  1. セキュリティ対応体制の評価
  2. 保護ソリューションの開発と配備
  3. 侵入検知とインシデント対応戦略の実現

北米電力業界の規制標準の見直し

- NERCのCIP標準の現状をレビュー
  - FERCから委託を受けたNERCが規定
    FERC：Federal Energy Regulatory Commission（連邦エネルギー規制委員会)
    NERC：North American Electric Reliability Corporation (北米電力信頼性会社)
  - CIP：Critical Infrastructure Protection
    http://www.nerc.com/page.php?cid=2|20
    不適合を報告した場合には，
    不適合の期間中，100万ドル/日の罰金

- 罰金のがれに終始した，本筋から逸脱したセキュリティ対策が横行
- 12月に第5版への改定が投票に付されたが否決された

欧州ではENISAがICS防御に関する報告書と勧告

1. 欧州全域および国ごとのICSセキュリティ戦略を作成する
2. ICSセキュリティのためのグッド・プラクティス・ガイドを作成する
3. ICSセキュリティ計画のテンプレートを作成する
4. アウェアネスの醸成と訓練
5. 共通のテスト・ベッド，または代替として，ICSセキュリティ認証フレームワークを作成する
6. 国のICSコンピュータ緊急対応機能を作成する
7. ICSセキュリティ分野の研究を促進し，既存の研究計画を後押しする

参考： https://www.enisa.europa.eu/act/res/other-areas/ics-scada/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states-1

ドイツは重要インフラ防御のための専門組織を設置

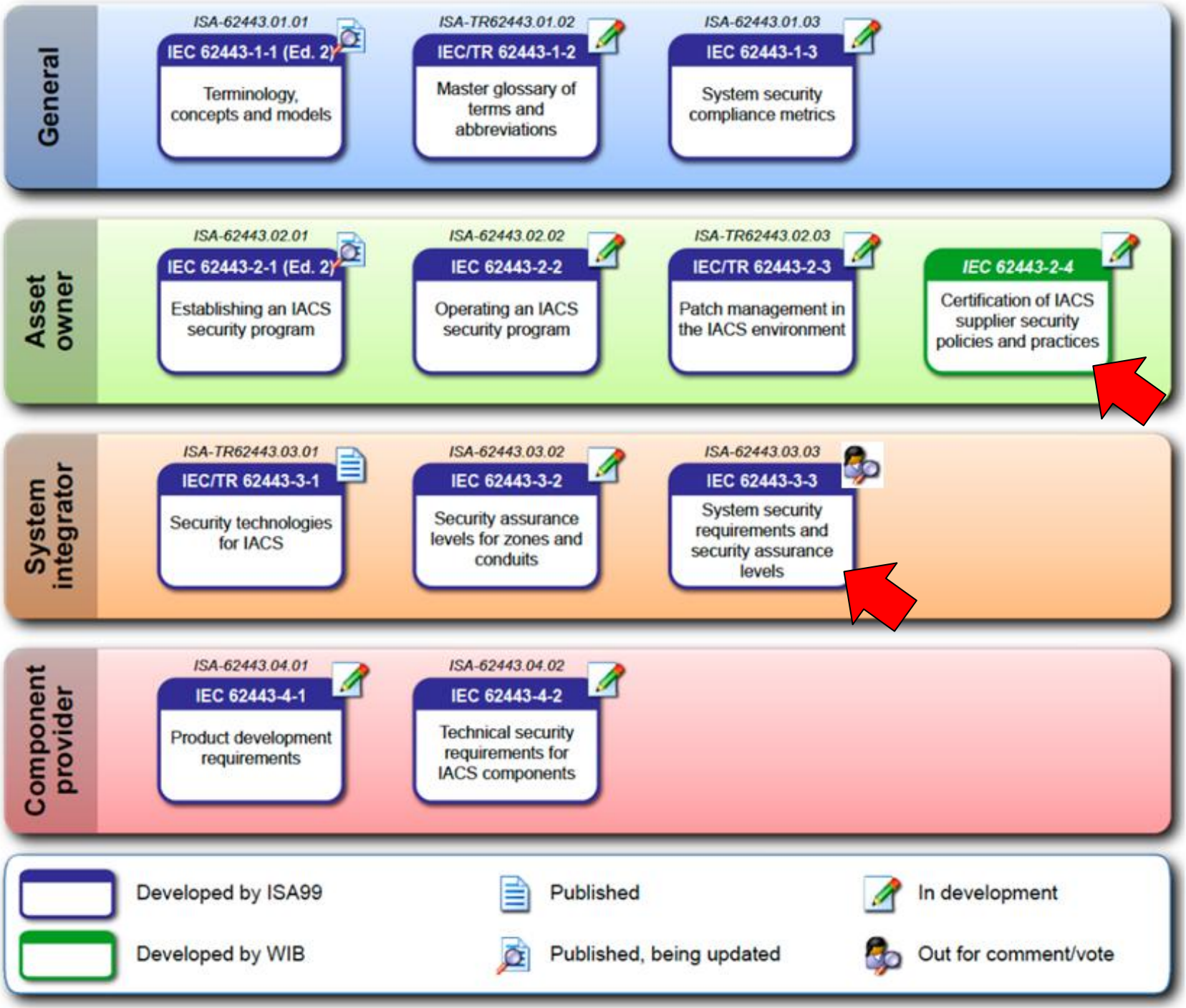
- 重要インフラ防御を専門とするサイバー防衛センター(Cyber-**Abwehrzentrum**)を設置（6月16日）
  http://www.theregister.co.uk/2011/06/16/germany_cyber_defence_to_defend_infrastructure/
- オーストリアはサイバー・セキュリティ要員1,600名からなるサイバー防衛組織を構築中
  http://www.cyber-defense.net/news/%20austria-hires-1600-soldiers-for-cyber-security/

IEC 62443 Industrial Communication Networks — Network and System Security

- 外から見える進捗なし

- IEC TC65/WG10が策定中の標準シリーズ:
  - IEC 62443-1-x: 一般論(概念や用語の定義)
  - IEC 62443-2-x: 制御システム運用者が想定読者
    - 62443-2-4 (ICSサプライヤの認定) 草案を否決;改訂検討中
  - IEC 62443-3-x: 制御システムのシステム・インテグレータが想定読者
    - 62443-3-3 草案を公表しコメント要請中
  - IEC 62443-4-x: 制御システムの要素製品提供ベンダーが想定読者
    - 4本の標準を策定する計画を2本に集約することに変更

- ANSI/ISA 99-xx.yyの名称をANSI/ISA 62443-x-yに変更


General
ISA-62443.01.01
IEC 62443-1-1 (Ed. 2)
Terminology, concepts and models
ISA-TR62443.01.02
IEC/TR 62443-1-2
Master glossary of terms and abbreviations
ISA-62443.01.03
IEC 62443-1-3
System security compliance metrics
Asset owner
ISA-62443.02.01
IEC 62443-2-1 (Ed. 2)
Establishing an IACS security program
ISA-62443.02.02
IEC 62443-2-2
Operating an IACS security program
ISA-TR62443.02.03
IEC/TR 62443-2-3
Patch management in the IACS environment
IEC 62443-2-4
Certification of IACS supplier security policies and practices
System integrator
ISA-TR62443.03.01
IEC/TR 62443-3-1
Security technologies for IACS
ISA-62443.03.02
IEC 62443-3-2
Security assurance levels for zones and conduits
ISA-62443.03.03
IEC 62443-3-3
System security requirements and security assurance levels
Component provider
ISA-62443.04.01
IEC 62443-4-1
Product development requirements
ISA-62443.04.02
IEC 62443-4-2
Technical security requirements for IACS components
Developed by ISA99
Developed by WIB
Published
Published, being updated
In development
Out for comment/vote

Stuxnetの知見を標準規格にフィードバックさせる

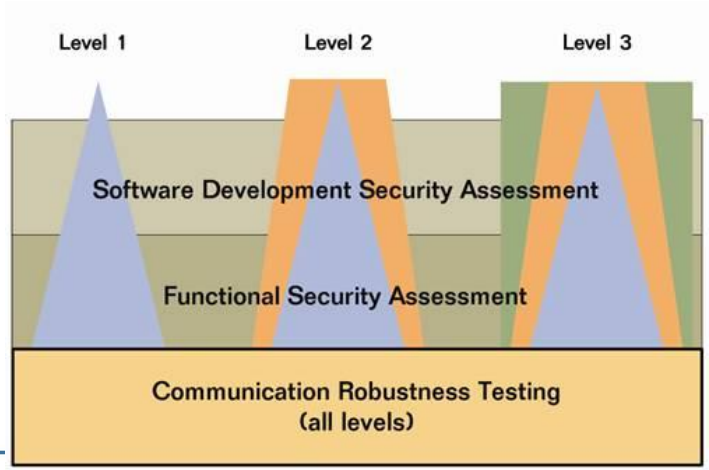
JPCERT CC®

- ISA99タスク・グループがStuxnetの動作に配慮した標準仕様のギャップ分析に2011年半ばの結論を目標に着手 (2011年3月3日)
  http://www.isa.org/Template.cfm?Section=Standards2&template=/ContentManagement/ContentDisplay.cfm&ContentID=85191

  — 評価作業は完了したものの，編集上の作業が残っているとして，まだ結論が公表されていない

ISCIがセキュリティ認定の発行を開始

- ISCI (ISA Security Compliance Institute)がセキュリティ認定の発行を開始 (6月)
  http://www.isasecure.org/Certification-Program/ISASecure-Program-Description.aspx
  1. **機能セキュリティ評価** (FSA: Functional Security Assessment)
  2. **ソフトウェア開発セキュリティ評価** (SDSA: Software Development Security Assessment)
  3. **通信堅牢性試験** (CRT: Communications Robustness Tests)
     WurldTech社のAchilles認定と同じ



- 第1号はHoneywell社製Safety Manager

http://www.isasecure.org/End-User-Resources/Registered-Products.aspx

制御システム用プロトコルの強化

- DNP3のセキュア認証 第5版を公表 (11月)
  http://www.dnp.org/Lists/Announcements/DispForm.aspx?ID=7&Source=http%3A%2F%2Fwww.dnp.org%2Fdefault.aspx
  - 第4版の脆弱性を修正；旧版との互換性はない

- 制御システム用プロトコルの多くに関しては
  なおセキュリティ機能の強化が課題

以外に深刻だったStuxnetの影響

- “In the Dark: Crucial Industries Confront Cyberattacks” (4月)
  http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf
  McAfee社とCSISによる報告書

※ CSIS: Center for Strategic & International Studies

調査対象：世界の14か国200人の重要インフラ運用組織の役員級のセキュリティ専門家

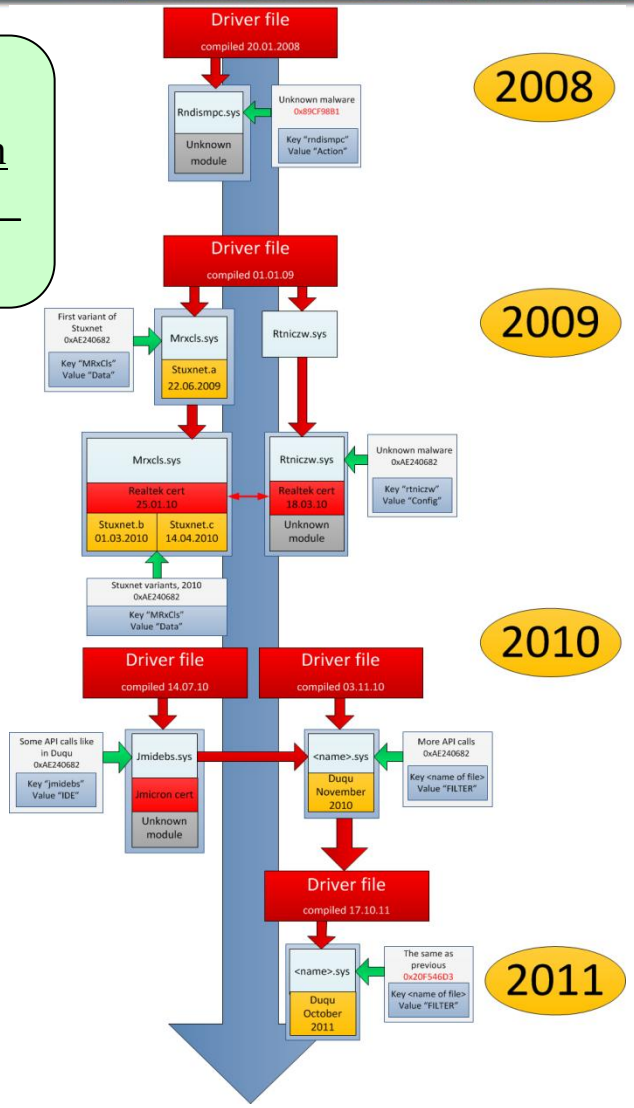
- 以外に深刻だったStuxnetの影響
  - 回答組織の40%で社内での感染事例があった
  - 電力業界の回答組織の46%で社内での感染事例があった
  - 感染事例があった回答組織のうち3/4は自信をもって除去済み
  - 感染率は国によるばらつきが大きい；
    インド，フランス，スペインが比較的高い

マルウェアの系譜: Stuxnet → Duqu → ？

JPCERT CC®

- StuxnetとDuqu
- コードが酷似
  - 同一環境で開発された可能性
  - 同じ環境で，
    2007～2008年にスパイウェアを
    2008～2010年に別のマルウェアを製造

Kaspersky研究所が解析
https://www.securelist.com/en/analysis/204792208/Stuxnet_Duqu_The_Evolution_of_Drivers



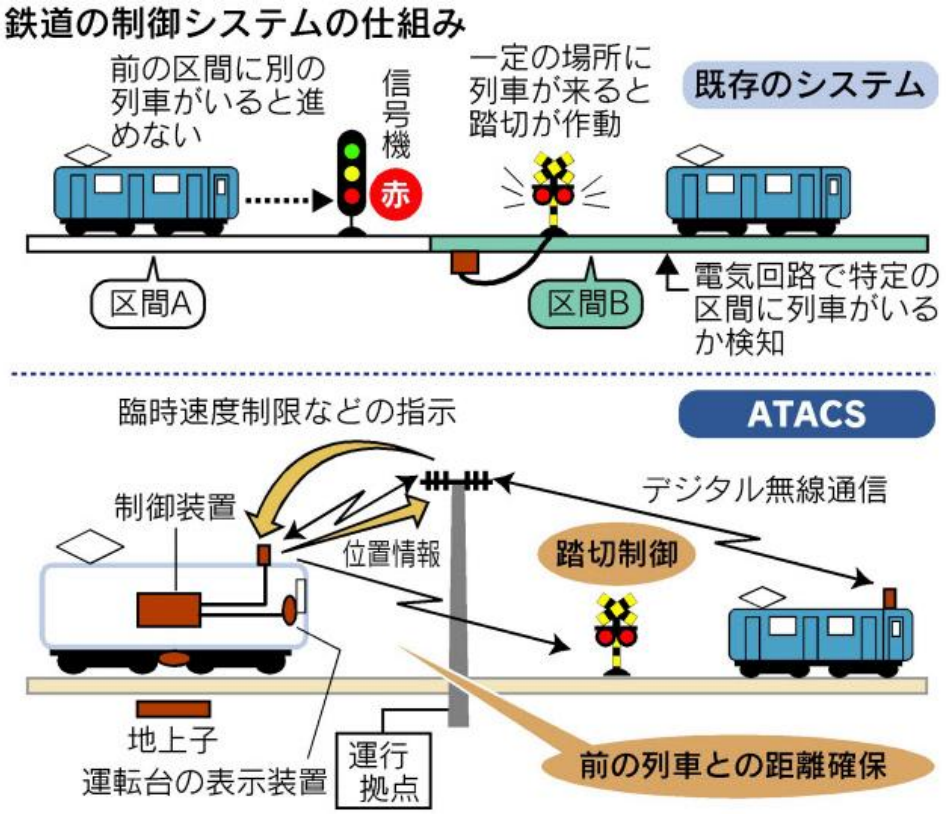
	Stuxnet	Duqu
報告	2010年6月	2011年10月
標的	制御システム	情報システム
狙い	操業妨害	情報窃取

鉄道の運行制御もデジタル化へ

- JR東日本が仙石線でATACSの基本機能の運用開始（10月）
- 列車同士の間隔調整から信号や踏切までがデジタル制御に

ATACS: Advanced Train Administration and Communication System

出典）日本経済新聞



インターネットからログイン可能な制御システムも

JPCERT CC®

- Shodan：サイト自体(≠情報)の検索システム
- ICS-ALERT-11-343-01 Control System Internet Accessibility http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-343-01.pdf

Hungary	14	South Africa	9
Iceland	2	Spain	86
India	14	Sweden	442
Indonesia	2	Switzerland	34
Iran, Islamic Republic of	1	Taiwan	66
Ireland	76	Thailand	7
Israel	10	Trinidad and Tobago	1
Italy	57	Turkey	7
Japan	59	Ukraine	12
Jersey	1	United Kingdom	122
Kazakstan	1	United States	3920
Korea, Republic of	41	Vietnam	1
No Country Information Available	31	Total	7489

Table 2.2: Connections logged per country

出典：Quantitatively Assessing and Visualising Industrial System Attack Surfaces（英国ケンブリッジ大学 Eireann P. Leverett）

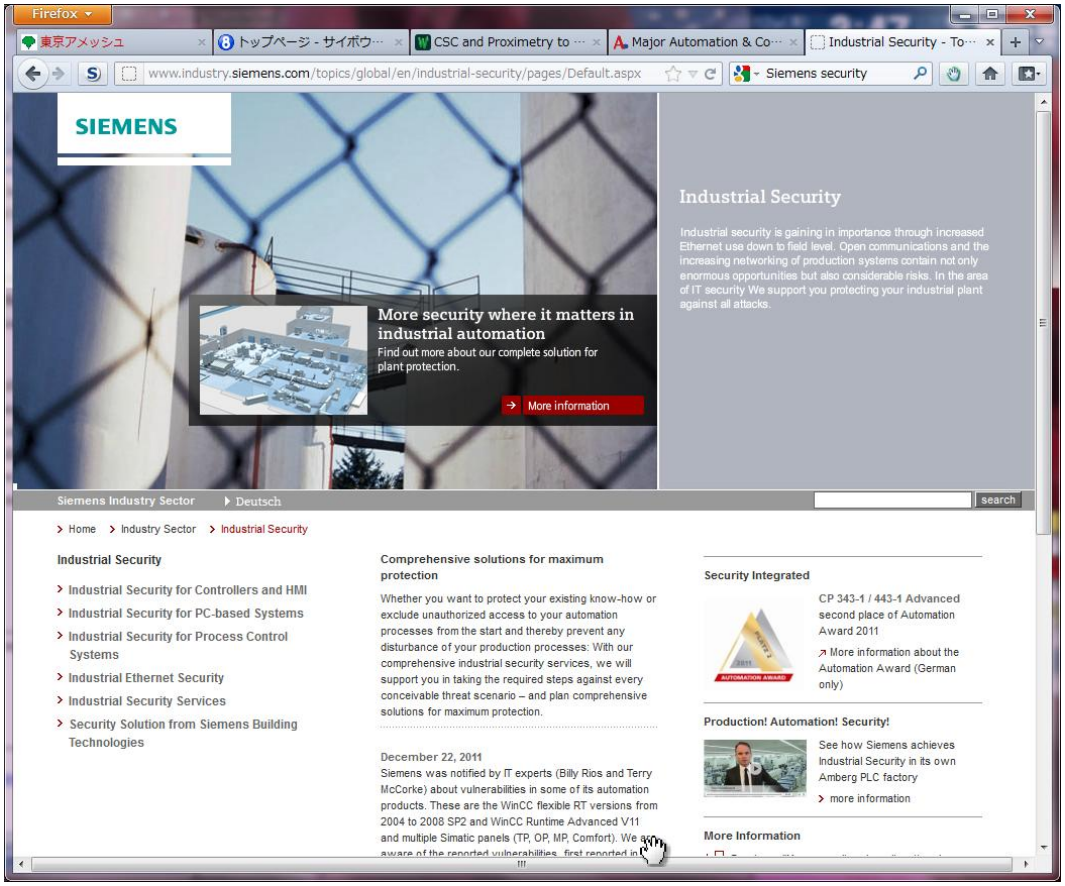
セキュリティに取組み始めた制御システム・ベンダー

JPCERT CC®

- Siemens社がホームページにセキュリティ情報ページを開設

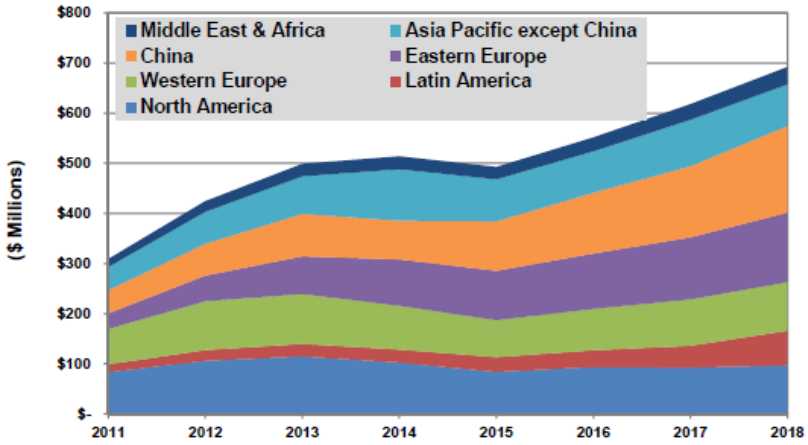
http://www.industry.siemens.com/topics/global/en/industrial-security/pages/Default.aspx

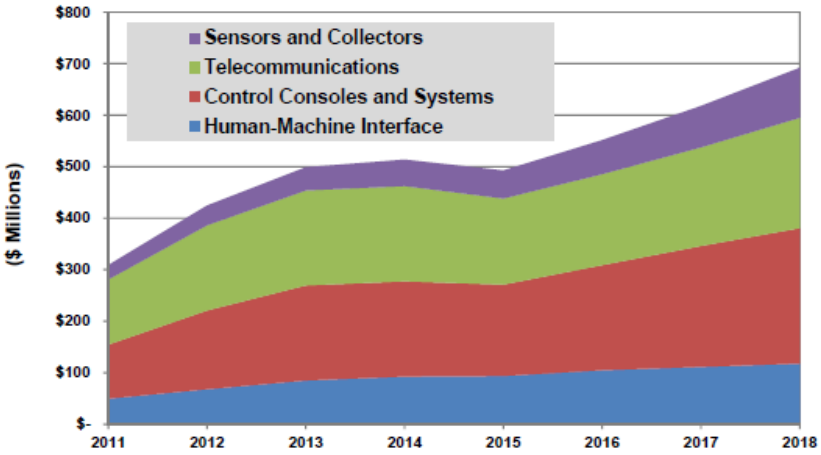
- 提供ソリューションの紹介が中心
- 脆弱性情報への誘導なし

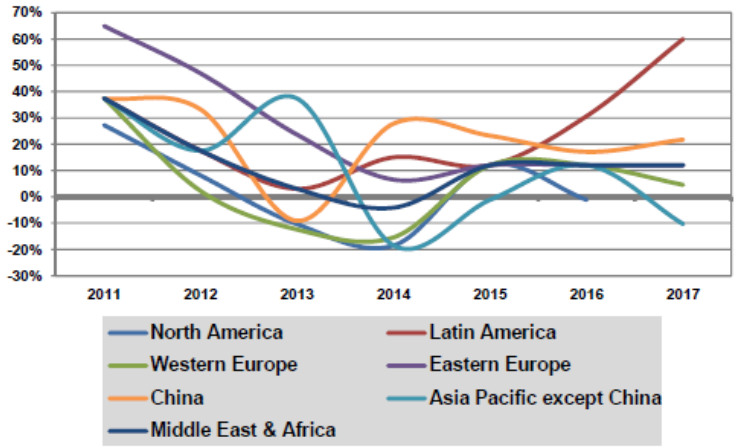


拡大するICSセキュリティ市場

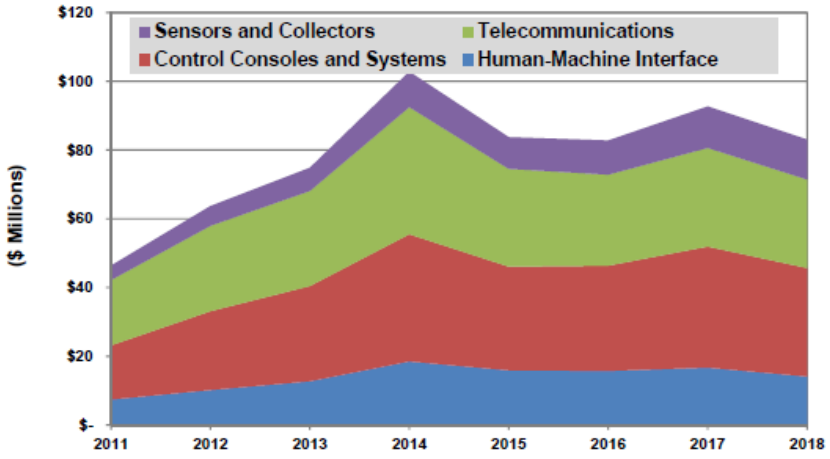
ICSセキュリティ市場
（電力関係のみ）
出典：Pike研究所







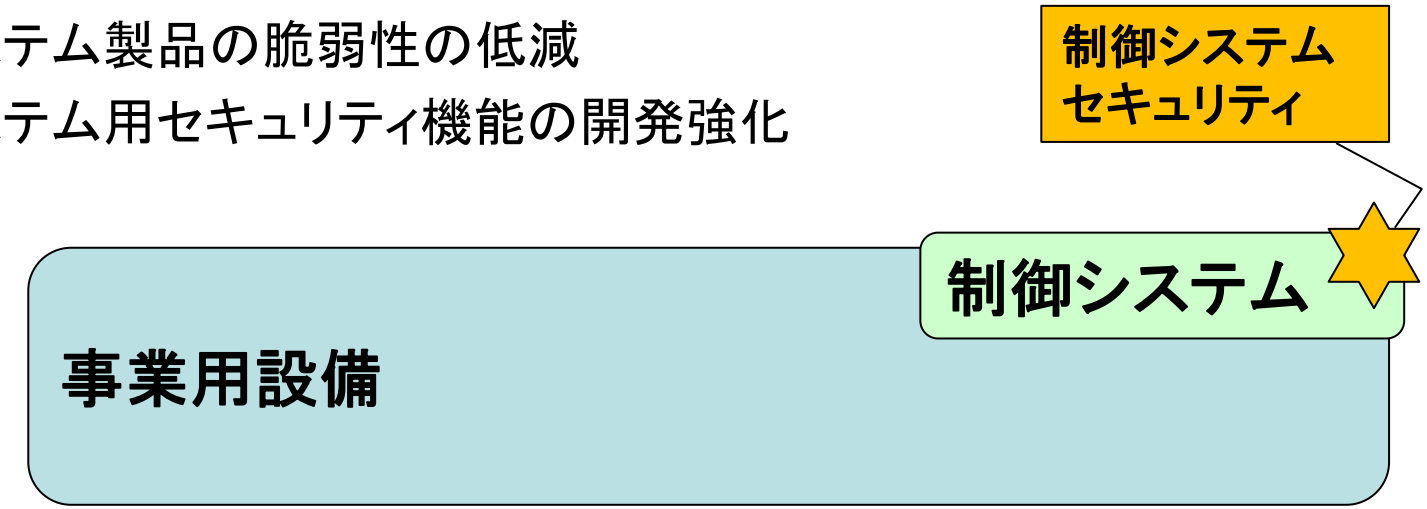
ICS Security Revenue by Technology, Asia Pacific except China: 2011-2018



Security as an Enabler !

まとめ

- 2011年～2012年を制御システムのセキュリティの変曲点の年に！
- 包括的なセキュリティへの取組みが求められている
  - 事業リスクとしてのセキュリティ問題
  - セキュリティに関する社内責任の所在
  - セキュリティに関する提供者vs利用者の責任の所在
  - 制御システム製品の脆弱性の低減
  - 制御システム用セキュリティ機能の開発強化



ご静聴ありがとうございました。

JPCERTコーディネーションセンター

— Email：office@jpcert.or.jp

— Tel：03-3518-4600

— Web: http://www.jpcert.or.jp/