出國報告（出國類別：開會、考察）

參加2014年工控系統安全年會

服務機關：台電電力調度處

姓名職稱：　張木軍副處長

派赴國家：　日本

出國期間：103年2月4日至6日

報告日期：103年3月19日

目　　次

一、 出國緣由

行政院「國家資通安全會報」積極推動我國資通安全基礎建設工作，幕僚作業由資通安全辦公室辦理。本(電力調度)處肩負全國電力系統調度作業，屬 A 級資安重要核心單位，須積極配合國家資安政策，做好資通安全防護工作及健全資安防護能力。

本處近年來多次配合資通安全辦公室辦理資安演練，在雙方共同努力之下，本處資安應變能力逐步提昇。

去(102)年 10 月 23 日行政院資通安全辦公室王道弘專員致電本處表示日本 JPCERT/CC (Japan Computer Emergency Response Team/ Coordination Center)擬邀請本國之工控系統使用者企業參加 2014 年「工控系統安全年會」並發表演講，王專員希望本處能派員參加，對提昇本公司工控系統網路安全水準及降低網路安全風險應有助益。

JPCERT/CC 是一個獨立的法人組織，受日本政府委託執行資訊安全的相關計劃，類似台灣電腦網路危機處理暨協調中心(TWCERT/CC)。

經本處與 JPCERT/CC 分析員林永熙先生聯繫後，知悉 JPCERT/CC 已舉辦過數次工控系統安全年會，2014 年年會預定在日本東京舉辦，對日本工控系統業界推廣安全意識。過去年會多以工控系統的系統/元件製造商、工控標準化/認證、以及工控系統相關漏洞檢查及處理機制為主。JPCERT/CC 希望本次年會由使用工控系統之企業如電力公司等參與，尤其希望分享國外的案例經驗，JPCERT/CC 因此透過行政院資通安全辦公室推薦本公司派員參加。

本處因此選派張副處長木軍參加該 2014 年工控系統安全年會，除分享本公司中央調度中心電能管理系統等工控系統安全經驗與遭遇問題時之對策並學習國外資安案例，對於資安技術之交流及與國際同業間友好關係之促進頗有助益。

二、 參加年會紀要

本次開會行程如下表：

日　期	開會地點	活動內容
103.2.4	台北-日本東京	往　程
103.2.5	日本東京	參加2014年工控系統安全年會
103.2.6	日本東京-台北	返　程

日本2014年度之工控系統安全年會於2014年2月5日（三）假東京都港区港南 kokuyo hall 舉行，主辦單位為經濟產業省下之社團法人 JPCERT 協調中心(Coordination center)，協辦單位有資訊安全政策會議、獨立行政法人資訊處理推進機構(IPA)、技術研究組合 控制系統安全中心、公益社團法人 計測自動控制學會（SICE）產業應用部門、一般財團法人 日本資訊經濟社會推進協會（JIPDEC)、一般財團法人 電子資訊技術產業協會（JEITA)、一般財團法人 日本電力計測器工業會（JEMIMA)、一般財團法人 日本電機工業會（JEMA）以及一般財團法人 日本電力控制機器工業會（NECA）等。參加年會之對象為工控系統用戶企業、工控系統廠商、工控機器廠商、工控系統整合之研究人員，據主辦單位告知，日本各大電力公司皆有派員出席年會。

今年年會由JPCERT協調中心理事宮地 利雄先生致詞後即陸續展開8場工控系統資安議題演講，政府機關代表經濟產業省之商務資訊政策局資訊安全政策室室長上村昌博先生則於中午時才上台致詞，年會8場演講講題如次(演講內容及演講者資料詳如附件)：

講題一：回顧這1年間工控制系統、安全的現況與展望

演講者：宮地 利雄先生

JPCERT 協調中心理事/顧問

講題二：CSSC 推行的測試床(test bed)CSS-Base6 及 EDSA 認證～具備世界性與未來性的安全控制系統～

演講者：小林 偉昭先生

控制系統安全中心 技術研究組合專務理事

講題三： CSMS 認證制度

演講者：高取 敏夫先生
日本資訊經濟社會推進協會 資訊管理推進中心副中心長

講題四：企業組織陷入安全威脅的準備與對策

演講者：真鍋 敬士先生
JPCERT 協調中心理事/分析中心長

講題五：ICS Security Enhancement in the National Control Centers of Taiwan Power Company（臺灣電力公司中央調度室控制系統安全的強化）

演講者：張木軍先生
臺灣電力公司電力調度處副處長

講題六：The Kaizen of ICS Security（ICS 安全的改善）

演講者：Ralph Langner 先生
Langner 集團 Co-Founder and managing Principal

講題七：ICS Security Enhancement in Australia（澳大利亞工控制系統安全的強化）

演講者：Simeon Simes 先生
CERT Australia 資深技術顧問

講題八：**國內控制系統安全的實態**

演講者：山田 秀和先生
JPCERT 協調中心控制系統安全集團負責人(group Leader)

日本政府近年來發現智財及生命線等相關設施之資安持續被攻擊事件，於 2010 年開始領導業界針對控制系統安全事宜積極討論。經由政府機關經濟產業省的推動，一些與控制系統相關產商學界人士紛紛投入資安標準、認證程序等工作。

本次年會中，日本經濟產業省的 JPCERT 協調中心依往例邀請工控系統專家們對控制系統資安發展及展望提出報告。工控系統(ICS)專家如宮地先生報告近年來工控系統設施發現脆弱性事件高達 1 百 8、90 件，並且報告在 DNP3 通訊協定產品發現脆弱性之衝擊；宮地先生引用日本 Trend Micro 公司的 ICS「Honeypot 蜜罐」系統所補捉到的資料，說明主要攻擊來源為中國大陸、寮國及美國。小林先生介紹 CSSC(Control System Security Center)成立緣由、目的及該中心研發之

CSS-Base6 系統；CSSC 將受委託辦理控制設備廠商之 EDSA(Embedded Device Security Assurance)認證及企業等之 CSMS(Cyber Security Management System) 認證。高取先生介紹日本資訊經濟社會推進協會（JIPDEC）組織及 CSMS(Cyber Security Management System)之認證。本公司則向與會者介紹台北高雄雙主控中央調度中心架構、有關資安規劃、資安演練及遭遇問題時對策等。Simeon Simes 先生則介紹澳洲的國家電腦網路危機應變中心（CERT）在控制系統安全所做的努力與經驗。

三、 心得與建議

本次出國參加日本 2014 年工控系統安全年會，本公司讓國外如日本、澳洲等國家的人了解我們先進的南北雙主控中央調度中心架構以及本公司在強化工控系統資安工作上的經驗與努力如配合政府資安要求，每年都要參與 CIIP(Critical Information Infrastructure Protection)演練，明顯獲得良好交流的效果，因為，對於本公司參與政府 CIIP 演練的報告，引發與會者中有一位人員當場詢問 CIIP 演練除了電力系統外是否還納入其他基礎設施，會後還就 CIIP 問題交換意見。另外，本次年會，我駐日經濟文化代表處徐副組長亦與會，對於本公司的報告，徐副組長在會後對本公司的努力表示肯定。

經聆聽與會專家幾場演講後，對本公司辦理工控系統有關業務之單位建議如下：

(一) 建議本公司各單位辦理重要工控系統及設備計畫時，自採購建置開始至日後維護必須要求廠商提供符合國際資安標準認證之產品。

(二) 本公司工控系統或設備如受資安攻擊，後果極為嚴重，建議本公司各單位辦理工控系統或設備維護工作時，應提高警覺、特別注意國內外資安訊息。

(三) 建議本公司各單位針對重大資安事故加強演練，檢視事件處置能力及通報作業流程，藉以強化在資安事件發生時之應變處置、系統復原、協調管控等能力，作為日後處置參考經驗。

(四) 建議本公司能定期派員參加類似日本工控系統安全年會之國際會議，藉以與國際交流工控系統之資安經驗與心得。

四、 附件

JPCERT CC®
Japan Computer Emergency Response Team Coordination Center
JPCERTコーディネーションセンター

制御システムセキュリティカンファレンス 2014

2014年2月5日（水）　コクヨホール（品川）

主　催

経済産業省
一般社団法人 JPCERT コーディネーションセンター

後　援

情報セキュリティ政策会議
独立行政法人情報処理推進機構(IPA)
技術研究組合 制御システムセキュリティセンター(CSSC)
公益社団法人 計測自動制御学会（SICE）産業応用部門
一般財団法人 日本情報経済社会推進協会（JIPDEC）
一般社団法人 電子情報技術産業協会（JEITA）
一般社団法人 日本電気計測器工業会(JEMIMA)
一般社団法人 日本電機工業会(JEMA)
一般社団法人 日本電気制御機器工業会(NECA)
(順不同)

目　次

開催概要

名　　称　制御システムセキュリティカンファレンス 2014

日　　時　2014 年 2 月 5 日（水）10 時より（受付開始 9 時 30 分）

会　　場　コクヨホール
東京都港区港南 1-8-35
http://www.kokuyo.co.jp/showroom/hall/access/

主　　催　経済産業省
一般社団法人 JPCERT コーディネーションセンター

後　　援　情報セキュリティ政策会議
独立行政法人情報処理推進機構(IPA)
技術研究組合 制御システムセキュリティセンター(CSSC)
公益社団法人 計測自動制御学会（SICE）産業応用部門
一般財団法人 日本情報経済社会推進協会（JIPDEC）
一般社団法人 電子情報技術産業協会（JEITA）
一般社団法人 日本電気計測器工業会(JEMIMA)
一般社団法人 日本電機工業会(JEMA)
一般社団法人 日本電気制御機器工業会(NECA)　(順不同)

対 象 者　制御システム関係者（ユーザ企業・事業者、システムインテグレータ・エンジニアリング会社、製品開発者、研究者）

参加費用　無料

定　　員　300 名

お問合せ先　「制御システムセキュリティカンファレンス 2014」事務局
E-mail：csc-regist@e-side.co.jp

プログラム

10:00 - 10:10 **開会挨拶**
経済産業省 商務情報政策局 情報セキュリティ政策室 室長 上村 昌博

10:10 - 10:40 **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**
一般社団法人 JPCERT コーディネーションセンター 理事/顧問　宮地 利雄

10:40 - 11:10 **CSSC の進めるテストベッド CSS-Base6 と EDSA 認証について**
～セキュアな制御システムを世界へ未来へ～
技術研究組合 制御システムセキュリティセンター　専務理事　小林 偉昭

11:10 - 11:30 **CSMS 認証制度について**
一般財団法人 日本情報経済社会推進協会　情報マネジメント推進センター
副センター長 高取敏夫

11:30 - 12:00 **企業組織に迫りくるセキュリティ脅威への備えと対策**
一般社団法人 JPCERT コーディネーションセンター 理事
分析センター長 真鍋 敬士

12:00 - 13:00 <昼休憩>

13:00 - 13:40 **ICS Security Enhancement in the National Control Centers of Taiwan Power Company**
(台湾電力公司の中央給電指令所における制御システムセキュリティ強化)
Mu-Chun Chang, Deputy Director System Operation Department,
台湾電力公司 (Taiwan Power Company)

13:40 - 14:20 **The Kaizen of ICS Security (ICS セキュリティの改善)**
Ralph Langner, Co-Founder and Managing Principal, The Langner Group

14:20 - 14:35 <休憩>

14:35 - 15:15 **ICS Security Enhancement in Australia**
(オーストラリアにおける制御システムセキュリティの強化)
Simeon Simes, Senior Technical Adviser, CERT Australia

15:15 - 15:55 **国内における制御システムセキュリティの実態**
一般社団法人 JPCERT コーディネーションセンター
制御システムセキュリティグループリーダ 山田 秀和

15:55 - 16:00 **閉会挨拶**
一般社団法人 JPCERT コーディネーションセンター 理事/顧問　宮地 利雄

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

一般社団法人 JPCERT コーディネーションセンター
理事/顧問
宮地 利雄

制御システム・セキュリティの現在と展望

Status and Prospects on ICS Security

この1年間を振り返って

Looking back over this one year

2014年2月5日
JPCERTコーディネーションセンター
理事・顧問　宮地　利雄

概要

Summary of Look-backs

1. ICS製品の脆弱性
   - 発見された脆弱性
   - 脆弱性の取扱
2. ICS上のサイバー・インシデント
   - ニュースになったICSインシデント
   - 重要インフラ事業者を狙う標的型攻撃
   - マルウェア感染
   - インターネットに直結されたICS
3. ICSセキュリティ関連の標準
   - 標準規格
   - 認証制度
4. ICSセキュリティ関連の研究開発活動

1. Vulnerabilities on ICS products
   - Reported vulnerabilities
   - Processes and framework for handling vulnerabilities
2. Cyber incidents on ICS
   - Incidents reported on news media
   - Targeted attacks against critical infrastructure providers
   - Malware infection on ICS
   - Internet reachable ICS
3. Standards on ICS security
   - Standards
   - Certifications
4. Research and development on ICS security

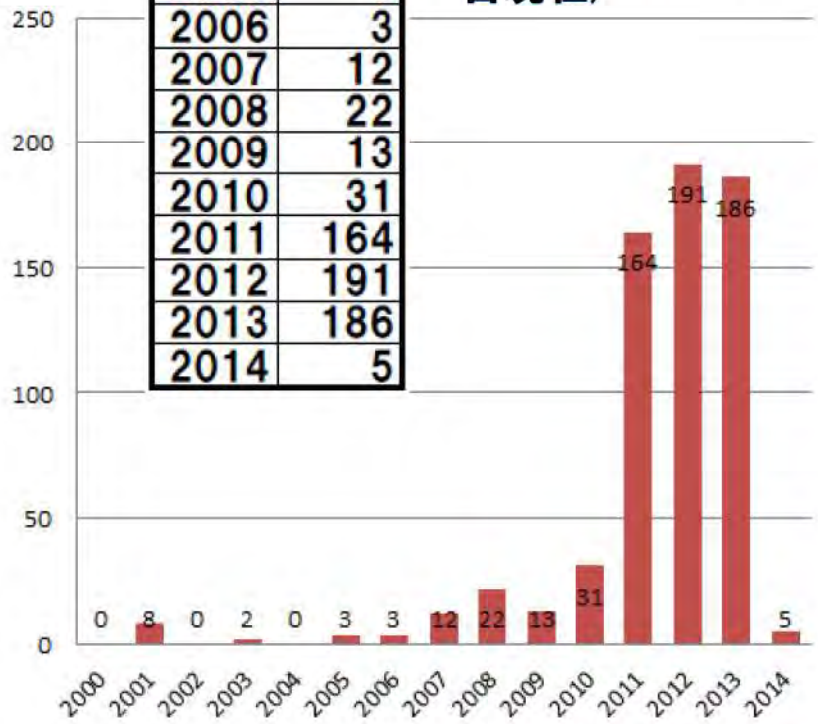
制御システム製品の脆弱性

Vulnerabilities in ICS products

- **脆弱性の報告数の高止まり**
  Number of vulnerability reports remains high.
  - **伸びは一服**
    No more rocket upsurge, but at a high altitude
- **DNP3に関連する脆弱性の衝撃**
  Shockwave of vulnerabilities found in DNP3 products
  - **脆弱性探索技術の高度化**
    Sophistication of fuzzing techniques
- **脆弱性の取扱制度の動向**
  Trends on vulnerability handling
  - **国際標準**
    International standard
  - **国内制度の検討**
    Framework in Japan
  - **ベンダーによる報奨金**
    Bounty program by vendors

OSVDBに登録された制御システム製品の脆弱性件数（2014年1月19日現在）

年	件数
2000	0
2001	8
2002	0
2003	2
2004	0
2005	3
2006	3
2007	12
2008	22
2009	13
2010	31
2011	164
2012	191
2013	186
2014	5



DNP3製品の脆弱性の余波

Shockwave of vulnerabilities in DNP3 products

- Adam Crain氏が9月13日に公表
  Mr. Adam Crain disclosed them on September 13

Aegis Platform

—開発中のDNP3ファザーを2014年3月に公表予定
He said that he was developing a fuzzing tool for DNP3 and that he would release it in March, 2014

- Modbus, IEC 61850, ICCP/TASE.2も計画中 (in their future plan)

—DNP3製品の脆弱性を多数発見しICS-CERTに報告中
He had found a number of vulnerabilities on various DNP3 implementations and reported them to ICS-CERT

CORPORATE SPONSORS

AUTOMATAK

RESEARCH LEADS

Adam Crain (Automatak)

Chris Sistrunk (independent)

RESEARCH CONTRIBUTORS

Adam Todorski (independent)

STATUS

15 of 28

ADVISORIES

#	Link	Vendor	Notes
1	ICSA-13-161-01	IOServer	
2	ICSA-13-213-03	IOServer	
3	ICSA-13-219-01	SEL	
4	ICSA-13-226-01	Kepware	
5	ICSA-13-234-02	TOP Server	

http://www.automatak.com/robus/

Project *Robus*

An ongoing search for 0-day vulnerabilities in SCADA/ICS protocols. 'Robus' is Latin for bulwark, source of strength, or solidity.

Why?

We believe that robust software is required to secure the ICS space. Research will create awareness. If not us, who? If not now, when?

How?

We're using a custom smart fuzzer. The tool used in this research is going open source in March.

Disclosure Policy

Relax, we're the good guys. We disclose vulnerabilities to the vendor and ICS-CERT. We work with affected vendors to validate patches and improve testing practices.

DNP3とは？

What is DNP3?

Distributed Network Protocol

- HMI/SCADA～RTU間で利用される通信プロトコル

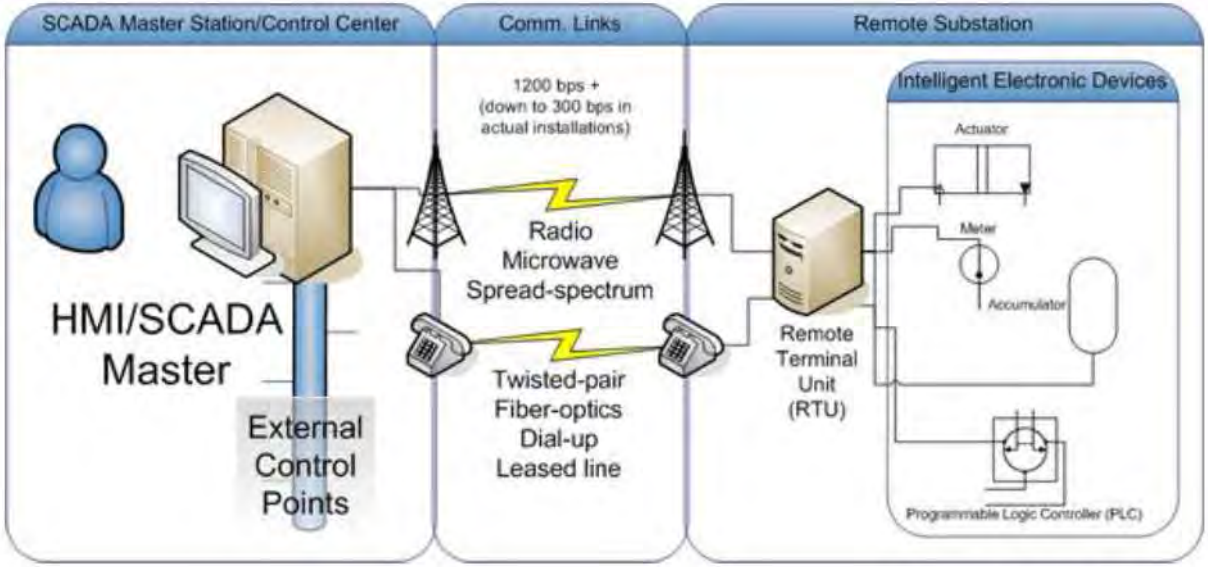
  Communication protocol used between HMI/SCADA and RTU

- 電力と水道業界でもっぱら利用

  Mainly used in electric companies and water companies

- 日本では馴染みが薄いが，米国等で広く利用されている

  Widely used in the U.S. and other countries although not so popular in Japan



出典: WikiPedia

DNP3の脆弱性で注目される点

What is unique about the DNP3 vulnerabilities?

- ICSプロトコルに対する初の体系的なファジング
  First systematic fuzzing on an ICS protocol
  - —EDSAのファジング試験(通信耐性試験)では
    イーサネットやTCP/IPだけが対象
    Current fuzzing test of EDSA certification (CRT: Communication Robustness Test) covers only Ethernet and basic TCP/IP protocols
  - —DNP3以外のICSプロトコルの実現も同程度に脆弱か
    Implementation of other ICS protocols seems to be as vulnerable as DNP3's
- シリアル回線からも攻撃が可能
  The vulnerabilities can also be exploited through serial communication lines.
- PLC/RTU側だけでなくHMI/SCADA側の脆弱性も探索
  Fuzzing not only on the PLC/RTU side but also on the HMI/SCADA side

DNP3の脆弱性が意味するもの

What DNP3 vulnerabilities mean

- ICSプロトコルは堅牢だとの神話も崩壊

  Some Japanese ICS experts said that ICS protocols are implemented robustly but it is only a dream

  —従来はICSプロトコル用の試験ツールが未整備なために発見される脆弱性が少なかったに過ぎない

  The number of vulnerability reports on ICS protocols was low so far, just because fuzzing test has been applied to them rarely.

  —ICSプロトコル・スタックに潜在する脆弱性がツールが整備されるにつれて発見されそう

  Vulnerabilities on ICS protocols will be often reported as test tools become widely used in the future.

- センター側の方が末端側よりも攻撃の打撃が広域に及ぶ

  Exploitation against the center side equipment is more attractive than the terminal side for attackers.

  —末端が広域に分散しているシステムにおいては物理的な防御が困難

  —遠隔の端末の位置からセンター側が攻撃される可能性

HARTプロトコルの脆弱性

(Highway Addressable Remote Transducer)

- 多くの先進的フィールド機器に，監視システムとの情報交換のために実装されたプロトコル

  HART protocol is the standard for sending and receiving digital information between smart devices and control or monitoring system.
  http://www.hartcomm.org/protocol/about/aboutprotocol_what.html

- Ralph Langner氏他のICSセキュリティ専門家が深刻な被害につながる可能性がある脆弱性がHARTプロトコルに存在することを報告

  Ralph Langner and other ICS cyber security experts have warned that the critical ICS vulnerabilities that can cause significant damage and/or personal injuries lie in the functional design of the instrumentation and control systems.
  http://www.controlglobal.com/blogs/unfettered/an-ics-cyber-vulnerability-beyond-stuxnet/

脆弱性取扱の手順のガイドライン制定

Guidelines on vulnerability handling processes

- 脆弱性のベンダーによる取扱に関する国際標準の制定

  International standardization on how vendors should handle vulnerability reports

  —ISO/IEC 30111 (脆弱性取扱手順)：
  国際標準として11月1日発行

  "Vulnerability handling processes" was published as an international standard.

  —ISO/IEC 29147 (脆弱性開示)：
  国際標準として承認

  "Vulnerability disclosure" was approved as an international standard.

- 2004年から運用されてきた国内の脆弱性届出制度を
  ICS分野に拡大することを検討中

  — The vulnerability handling program coordinated by IPA and JPCERT/CC has been operated in Japan since 2004.

  — Its extension to ICS products has been studied in the vulnerability research committee convened by IPA.

脆弱性報告の報奨制度と闇市場

Bounty programs and black markets for bugs and vulnerabilities

- バグ報奨金制度はベンダーにとってうまみ (CMU研究者)
  CMU researchers said that bug bounty program may be beneficial for vendors.
  http://www.networkworld.com/news/2013/071013-study-bug-bounty-programs-provide-271650.html
  —Microsoft, Google, Mozilla

- 制御システム・ベンダー(Integraxor社)も
  Integraxor became the first ICS vendor who started bug bounty program.
  http://www.integraxor.com/blog/integraxor-hmi-scada-bug-bounty-program/
  —製品の利用権を報奨として提供

- ロシアのサイバー犯罪市場が2012年に19億ドル規模に (グループIB社の見積り)
  Group IB estimated that Russian cyber crime market had expanded to 1.9 billion dollar size in 2012.
  http://www.securityweek.com/russia-cybercrime-market-reached-19-billion-2012-group-ib-estimates

セキュリティ・インシデントの動向

Trends on cyber security incidents

- 深刻なサイバー攻撃の報告は無かった
  No ICS security incident affecting widely and severely has been reported.
- 研究発表としてのICS攻撃デモ
  A lot of attack techniques against ICS have been demonstrated and reported in various technical conferences.
- 重要インフラ事業者へのAPTが深刻化ないし高水準維持
  APT continues to be in a severe level or worsens at critical infrastructure service providers.
- CSのマルウェア感染がかなり広範囲に散発
  Malware infection of ICS seems to have occurred more often than expected.
- インターネットに直結された制御システムも減らず
  Many ICSs or ICS products have been found on the Internet.

深刻なサイバー攻撃の報告は無い

No critical cyber security incident on ICS is reported

- ハッカー団「シリア電子軍」がイスラエルのICSを攻撃

  A attacker group called “Syrian Electric Army” breached an ICS in Israel.
  http://abna.ir/data.asp?lang=3&Id=417250
  http://news.softpedia.com/news/Syrian-Electronic-Army-Claims-to-Have-Hacked-Israeli-Critical-Infrastructure-Systems-351779.shtml

  - 「イスラエルの重要インフラに侵入」との犯行声明だった

    They declared that they have breach a critical infrastructure of Israel.
  - 侵入したICSは農業灌漑ポンプだった模様

    The ICS is for an irrigation system of a small farm.

- イスラエルの道路トンネル管理システムにサイバー攻撃

  A cyber attack on a tunnel in Israel was reported.
  http://phys.org/news/2013-10-israeli-tunnel-cyber.html

  - 保安用カメラを狙ったトロイの木馬による攻撃

    Trojan horse attack targeted the security camera system
  - 9月8日に20分間，9月9日に8時間にわたり通行止め

    The roadway was shut down for 20 minutes on September 8 and for 8 hours on September 9

標的型サイバー攻撃とICS

Targeted cyber attack and ISC

- 重要インフラ事業者への標的型サイバー攻撃の深刻化に米国DHSが懸念

  U.S. DHS alerted that critical targeted cyber attacks on critical infrastructure providers operating their ICSs had been often observed.
  http://www.securityweek.com/dhs-spear-phishing-campaign-targeted-11-energy-sector-firms

  —サイバー攻撃がICSに及んだ事例は極めて少ないが，社内情報システム内でICS関連情報を探し回った形跡

  —標的になっているのはエネルギー業界

  Especially, providers of the energy industry.

- 中小を含む製造事業者にも多数(24%)の標的型サイバー攻撃(Symantec社が報告)

  Symantec reported that manufacturers including MSB was most common targets of cyber attacks.
  http://www.symantec.com/security_response/publications/threatreport.jsp?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2013Apr_worldwide_ISTR18

緊張する朝鮮半島

International tension mounted in the Korean Peninsula

- 北朝鮮からのサイバー攻撃を韓国政府が発表
  South Korean government alerted about cyber attacks by North Korea.
- 韓国が原子力発電所のICS網でセキュリティ対策
  S. Korea divides nuclear plant controls from Internet (4月14日)
  http://english.yonhapnews.co.kr/business/2013/04/14/65/0503000000AEN20130414000500320F.HTML
  - —ICS網をイントラネットおよびインターネットから完全に分離
    ICS networks on nuclear plants were separated completely from intranets and the Internet.

ICSに対する攻撃に関する研究発表

Research reports on attack against ICSs

- ビル制御システム (2月6日)

  Researchers Demo Building Control System Hack
  http://www.darkreading.com/security/vulnerabilities/240147983/researchers-demo-building-control-system-hack.html

- ビル暖房システムに脆弱性

  Security hole can damage heating systems
  http://www2.majorgeeks.com/story.php?id=38552

- 頻発していると見られるICS内でのマルウェア感染
  公式の統計情報がないが…

  Malware infection in ICS is often reported though there is no formal statistics.

  —あるウィルス対策製品ベンダーによれば
  ICSを利用している顧客企業の3割でマルウェア感染
  うち4割は操業の継続に影響

  According to an anti-virus vendor's notice, 30% of their Japanese customers operating ICS have had their ICS infected by malware, 40% of which have been forced to discontinue their normal business operation.

インターネットに直結された制御システム

ICS reachable from the Internet

- コンピュータ(インターネット・サーバ)検索サービスの Shodan

  “Shodan” is a service for searching computers on the Internet.

  http://www.shodanhq.com/

- 見えてきた検索キーワード

  Keywords for searching ICS have been shared in the researchers’ community.

  —SHINEプロジェクト等で数十万台規模の製品を発見

  About a million ICS products have been identified by several projects such as SHINE

- 減らない

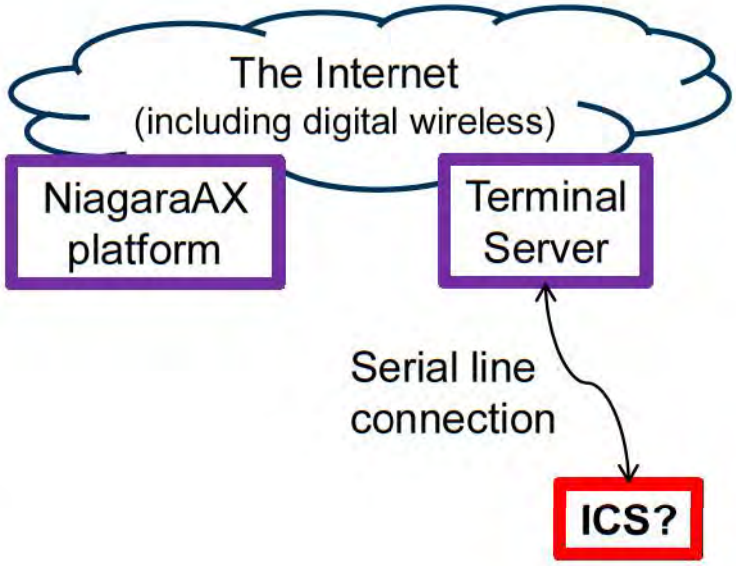
  Japanese cases is not so many but still remain.

  —日本の事例はそれほど多くはない

インターネット直結の制御システム事例

Cases of Internet reachable ICS

- 特定のビル制御用ICS製品
  (Cylance社が報告)
  http://www.computerworld.com/s/article/9239040/Researchers_find_hundreds_of_insecure_building_control_systems
- インターネットに接続された多数(11.4万台)のターミナル(シリアル回線)サーバー (Rapid7社が報告)
  Rapid7 reported 114 thousand terminal servers were reachable via the Internet.
  https://community.rapid7.com/servlet/JiveServlet/downloadBody/2271-102-1-4509/Serial%20Offenders%20FAQ.pdf
  https://community.rapid7.com/community/metasploit/blog/2013/04/23/serial-offenders-widespread-flaws-in-serial-port-servers
  —シリアル回線で接続されている機器の多数がレガシーICS？



Terminal servers

ICSハニーポットによる調査

Research with ICS honeypot

- TrendMicro社がICSに見せかけたハニーポットを設置し攻撃活動を調査報告

  TrendMicro installed multiple ICS honeypots and investigated activities attacking them.

  - Who's Really Attacking Your ICS Equipment?
    http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf
  - The SCADA That Didn't Cry Wolf
    https://media.blackhat.com/us-13/US-13-Wilhoit-The-SCADA-That-Didnt-Cry-Wolf-Whos-Really-Attacking-Your-ICS-Devices-Slides.pdf
- HoneyNetプロジェクトがConPot (Control Honeypot)を公表

  HoneyNet Project released Control Honeypot or ConPot for short, which simulated ICSs including Siemens SIMATIC S7-200 PLC.
  http://www.honeynet.org/node/1047

  - Siemens SIMATIC S7-200 PLC等をソフトウェアで模擬
- 油井施設に見せかけたハニーポットに侵入

  Cyber attacks were observed on a honeypot simulating a oil rig.
  http://www.theregister.co.uk/2013/08/01/scada_plc_vulnerability/

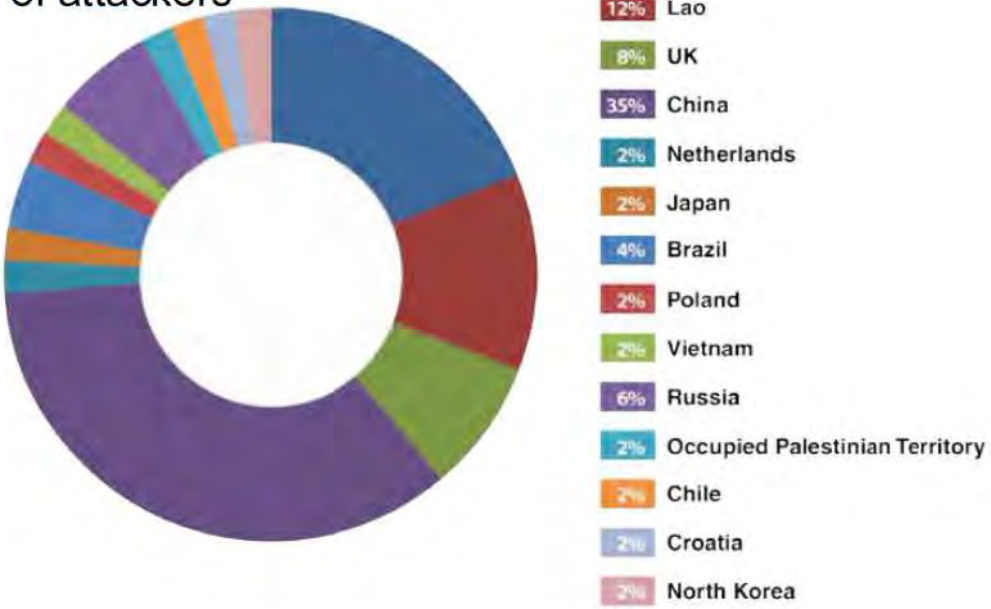
TrendMicro社のICSハニーポット

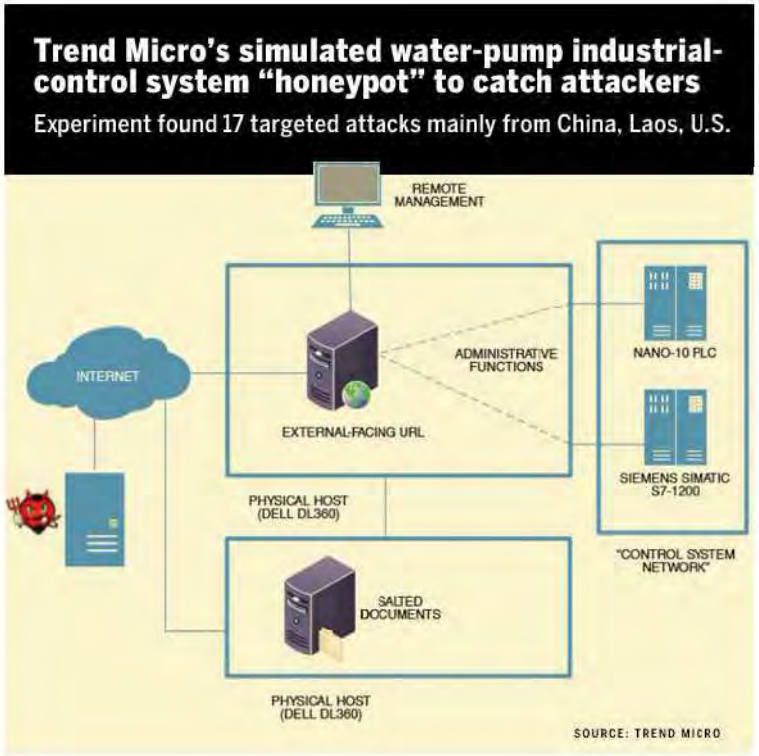
ICS honeypot operated by TrendMicro

- TrendMicro社の研究者がICSハニーポットを
  インターネット上に構築して攻撃の様子を観測

  http://blog.trendmicro.com/trendlabs-security-intelligence/whos-really-attacking-your-ics-devices/
  http://blog.trendmicro.co.jp/archives/7740

Network location of attackers





サイバー・セキュリティ・インシデント訓練

Cyber Security Incident Drills

- 国内初の電力・ガス・ビル分野のサイバー・セキュリティ演習実施 (経済産業省；2013年2月4日)

  ICS cyber Security Incident Response Drills were carried out in electric, gas and building automation industries.

  http://www.meti.go.jp/press/2012/02/20130204002/20130204002.html

  http://www.arcweb.com/industry-news/2013-03-22/first-cyber-security-drills-conducted-in-electricity-gas-and-buildings-areas-in-japan.aspx

- 米国DoEの資金でNESCORがサイバー・セキュリティ事故シナリオと影響を分析

  The National Electric Sector Cybersecurity Organization Resource has published three cyber security failure scenario and impact analyses documents for the electric sector.

  http://www.smartgridnews.com/artman/publish/Technologies_Security/Here-s-exactly-how-a-cyberattack-will-bring-down-your-utility-6108.html

- 米国NERCが電力基幹網に模擬サイバー攻撃 (11月13日)

  The North American Electric Reliability Council (NERC) launched a simulated attack on the U.S. power grid.

  GridEx II

  http://www.nytimes.com/2013/11/15/us/coast-to-coast-simulating-onslaught-against-power-grid.html

Stuxnetその後

Sequel of Stuxnet

- Symantec社の研究者がStuxnet 0.5版を報告

  Revealed: Stuxnet “beta’s” devious alternate attack on Iran nuke program
  http://arstechnica.com/security/2013/02/new-version-of-stuxnet-sheds-light-on-iran-targeting-cyberweapon/
  http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf

- 総括報告

  —Ralf Langner氏の最終Stuxnet分析報告書

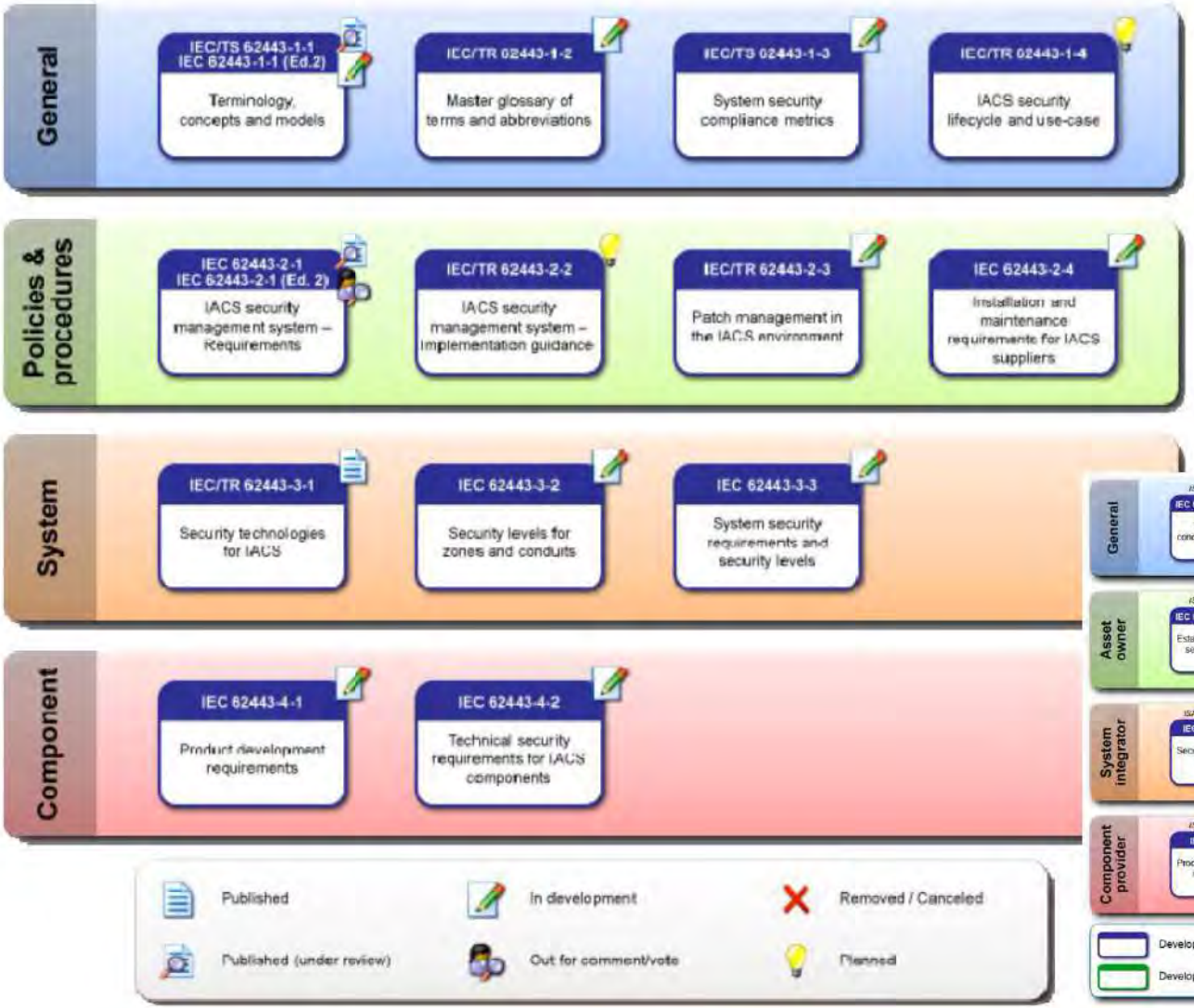
  Final Stuxnet analysis by Mr. Ralf Langer
  http://www.langner.com/en/2013/11/20/langner%E2%80%99s-final-stuxnet-analysis-comes-with-surprises/

  —Stuxnetの本当の話 (The Real Story of Stuxnet)

  http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

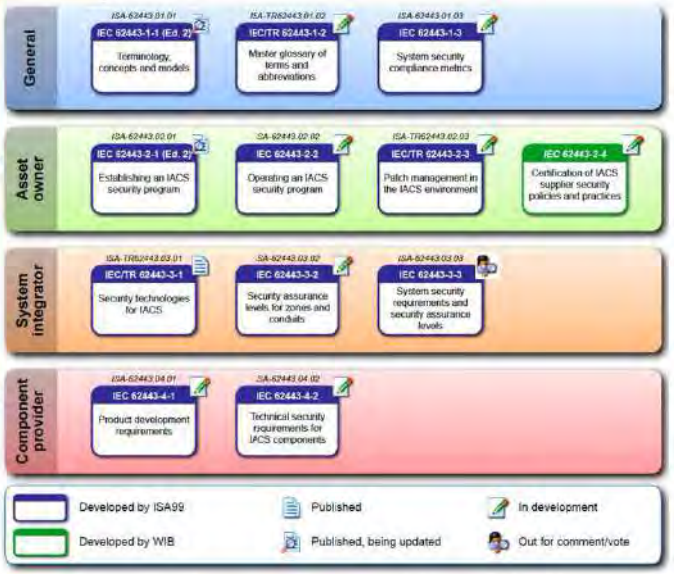
IEC 62443 (ISA-62443)シリーズ

http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx



複数の草案が公表されたが，新たに発行された標準はない

No new standard but a few drafts were released.



IEC 62443 (ISA-62443)シリーズ関連の動き

- ISO/IEC 27000シリーズの見直し
  - —中核部分を再構成中
  - —業界ごとISMSの拡充
    - ISO/IEC TR 27019 (エネルギー業界のためのISMS)
    - IEC 62443もISO/IEC 270xxと二重採番標準をめざす

- ISAが62443-3-3を承認(8月)；62443-3-2の草案も公表

Part 3-3: System Security Requirements and Security Levels
http://www.isa.org/Template.cfm?Section=press_releases5&template=/ContentManagement/ContentDisplay.cfm&ContentID=94074
Part 3-2: Security risk assessment and system design
http://isa99.isa.org/Documents/Drafts/ISA-62443-3-2-WD.pdf

セキュリティ認証

Security certification

製品 Products	運用管理 Operation practice	人員 Staff's skill
• EDSA (by ISASecure) • Achilles Communication Certification (by WurldTech)	• Achilles Practices Certification (by WurldTech) • CSMS (Control System Security Management System or AICSMS)	• GICSP (by SANSとICSベンダー) • ISASecure

EDSA (Embedded Device Security Assurance)

- ISASecureが認定
  Planned by ISASecure
- 製品の認証
  Product certification
  —新しい認証：1
  まだ5製品のみ
  Only 5 products have been certified; One new certified product in a recent year

ベンダー名	製品タイプ	モデル名
Honeywell Process Solutions	Safety Manager	HPS 1009077 C001
RTP Corporation	Safety manager	RTP 3000
Honeywell Process Solutions	DCS Controller	Experion C300
Honeywell Process Solutions	Fieldbus Controller	Experion FIM
横河電機 (Yokogawa)	Safety Manager	SCP451/461-11：Vnet/IP

- CSSCとIPAがISASecureと連携してEDSA認証の準備中
  CSSC and IPA are collaborating with ISASecure to kick off EDSA certification program in Japan

認証を受けたICS製品の数

製品認証	2010年	2014年
Achilles Communications Certification	22	135
MuDynamics	3	(Spirent社が買収) (acquired by Spirent)
ISA ISCI (EDSA)	0	5
Exida	1	

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

The number of certified products are based on a paper “Security Certification – A critical review” by Ragnar Schierholz et al.

ICSセキュリティ専門家の認定制度

- Global Industrial Cyber Security Professional (GICSP)
  http://www.prnewswire.com/news-releases/new-industrial-control-systems-cyber-security-certification-in-development-223462451.html
  - —SANSの配下のGIAC(Global Information Assurance Certification)が主導
  - —ABBやRockwell, Schneider, 横河などのICSベンダーや RedTiger, Wurldtechなどのセキュリテイ会社や BP, Shellなど利用組織も参加

- ISAの専門家認定制度
  - —Certified Control Systems Technician (CCST)
  - —Certified Automation Professional (CAP)
  - —新たにCertified Mission-Critical Professional (CMCP)をノース・カロライナ州の5大学と開発
    http://www.automation.com/automation-news/industry/isa-to-develop-mission-critical-professional-certification-program

ICSセキュリティ研究施設(海外)

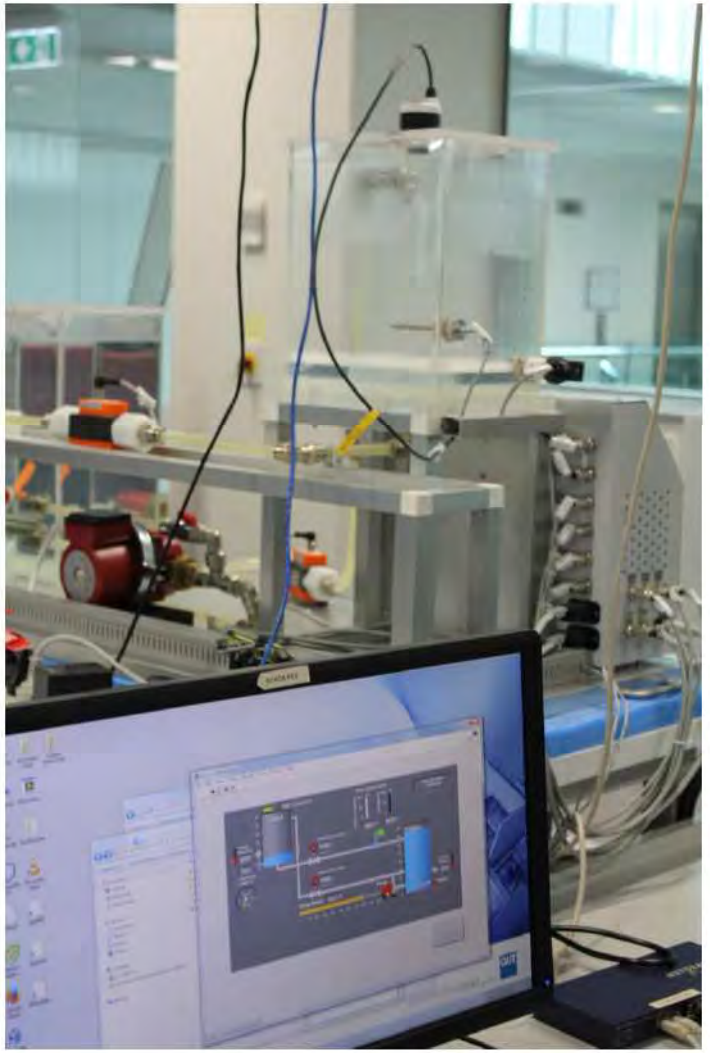
Research laboratories for ICS security

- European Network for Cyber Security (ENSC)
  https://www.encs.eu/

- モントリオールにSCADAサンドボックス
  SCADA 'Sandbox' Tests Real-World Impact Of Cyberattacks On Critical Infrastructure in Montreal
  http://www.darkreading.com/taxonomy/index/printarticle/id/240149728

- スペインに産業用サイバー・セキュリティ・センター
  Spain to welcome the new Industrial Cybersecurity Center
  http://www.infosecurity-magazine.com/view/31095/spain-to-welcome-the-new-industrial-cybersecurity-center/

- 豪クイーンズランド工科大学 →
  Queensland University of Technology



ICSセキュリティ研究施設(日本)

Research laboratories for ICS security in Japan

- 制御システムセキュリティセンター(CSSC)が東北多賀城本部を開設

  Control System Security Center or CSSC opened its Tohoku Tagajo head

  http://www.css-center.or.jp/sympo/2013/documents/press20130513.pd

- 名古屋工業大学の越島・橋本研究室
  - —セキュリティ・デモ用のICS

- JPCERT/CCも技術的な検証環境を整備

御静聴ありがとうございました

Thank you for
your attention

ICSセキュリティは
世界規模の課題；
一朝一夕の解決は望めない；
10年単位の時間枠での取組を！

ICS security is a problem to be resolved globally;
There seems to be no simple solution;
Let's resolve the problem in time range of a decade.

CSSCの進めるテストベッドCSS-Base6とEDSA認証について
～セキュアな制御システムを世界へ未来へ～

技術研究組合 制御システムセキュリティセンター
専務理事
小林 偉昭

JPCERT CC®
Japan Computer Emergency Response Team Coordination Center
JPCERTコーディネーションセンター

制御システムセキュリティカンファレンス 2014

CSSCの進めるテストベッドCSS-Base6とEDSA認証について
～セキュアな制御システムを世界へ未来へ～

2014年2月5日

技術研究組合制御システムセキュリティセンター
Control System Security Center　CSSC
専務理事　　研究開発部長
CSSC認証ラボラトリー最高責任者

小林　偉昭（ひであき）
hideaki.kobayashi@css-center.or.jp

目次

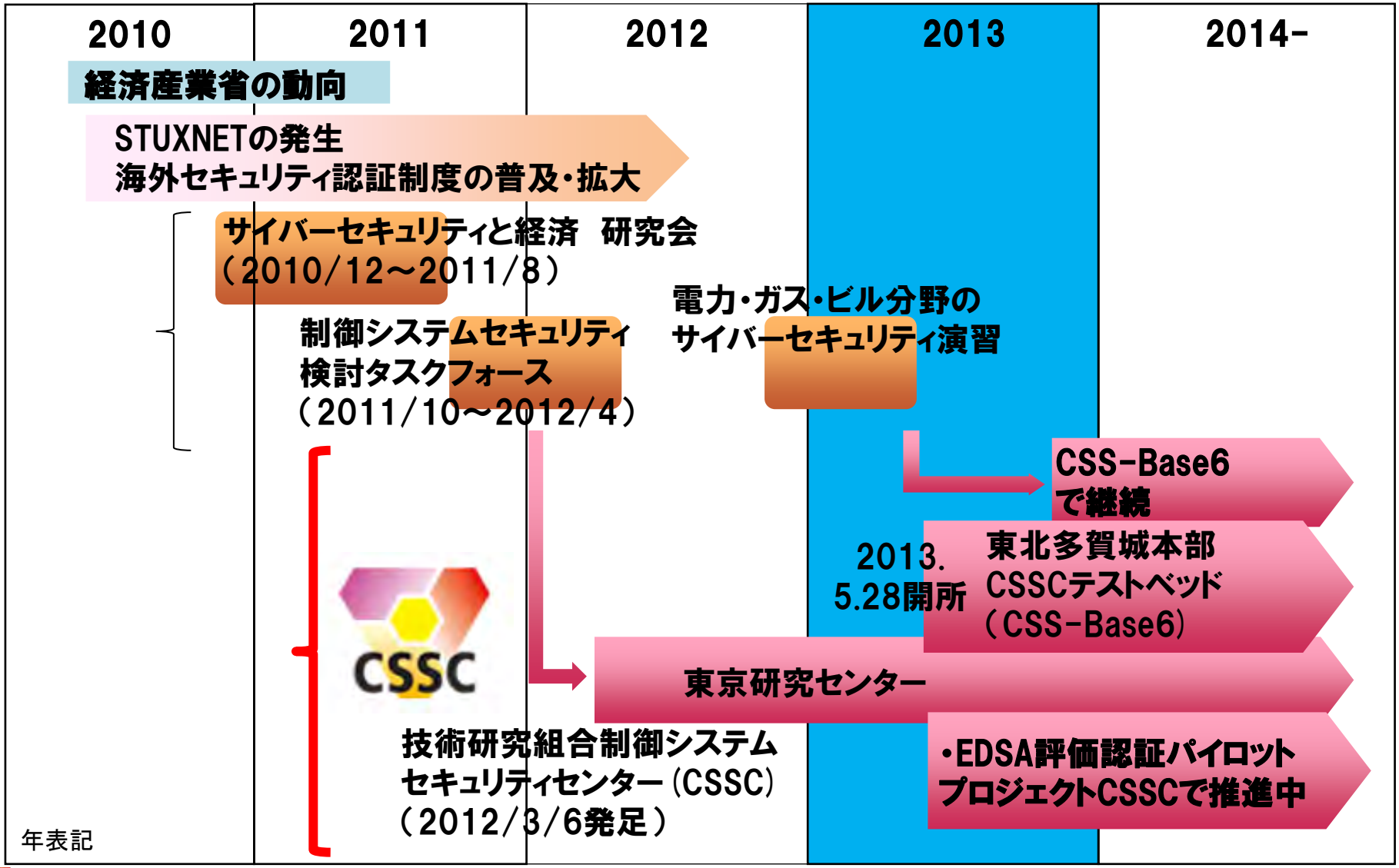
1.制御システムのセキュリティ向上へのCSSCの取り組み

2.制御システムセキュリティ認証への取り組み
～ISA/IEC62443の概要とEDSA認証について～

奈良時代後半の多賀城外郭南門（推定復元図）

1．制御システムのセキュリティ向上へのCSSCの取り組み
～セキュアな制御システムを世界へ未来へ～

制御システムセキュリティへの日本の取組み状況とCSSC



CSSC紹介ビデオ（約10分）

http://www.css-center.or.jp/en/index.html

東京都心で大規模な停電が発生したら・・・

http://www.youtube.com/watch?v=wbEiDQZU5sI&feature=youtu.be

2012年3月、CSSCを設立

1. 重要インフラをサイバー攻撃から守るための技術開発をしよう！
2. 日本の制御システムは、サイバー攻撃に強いことを実証しよう！
3. サイバーセキュリティ事業を震災復興、減災に役立てよう！
   → 「多賀城市減災リサーチパーク構想」への貢献

経済産業省
震災復興補助金

宮城県、多賀城市
みやぎ復興パーク

技術研究組合
制御システムセキュリティセンター
理事長： 新誠一
活動拠点： 東北多賀城本部と東京研究センター

制御システム製造・ユーザー企業
ユーザ企業、制御ベンダ、セキュリティベンダ、その他

大学
電気通信大、（東北大、倉敷芸術科学大学、名古屋工業大学）

独立行政法人
産業技術総合研究所
情報処理推進機構

CSSCの概要

名称	**技術研究組合 制御システムセキュリティセンター** （英文名）Control System Security Center （略称）　CSSC ※経済産業大臣認可法人	**組合員** （50音順）	**全23社（2014年1月現在）** ＊：創設時メンバー8社 アズビル株式会社*、エヌ・アール・アイ・セキュアテクノロジーズ株式会社、エヌ・ティ・ティ・コミュニケーションズ株式会社、オムロン株式会社、独立行政法人産業技術総合研究所*、独立行政法人情報処理推進機構、国立大学法人電気通信大学、株式会社東芝*、東北インフォメーション・システムズ株式会社、株式会社トヨタIT開発センター、トレンドマイクロ株式会社、日本電気株式会社、一般財団法人 日本品質保証機構、株式会社日立製作所*、富士通株式会社、富士電機株式会社、マカフィー株式会社、三菱重工業株式会社*、株式会社三菱総合研究所*、三菱電機株式会社、森ビル株式会社*、横河電機株式会社*、株式会社ラック
設立日	**2012年3月6日**（登録完了日）		
所在地	【東北多賀城本部(TTHQ)】 宮城県多賀城市桜木3-4-1 （みやぎ復興パーク F-21棟 6階） 【東京研究センター(TRC)】 東京都江東区青海2-4-7 （独立行政法人産業技術総合研究所 臨海副都心センター別館8階）	**連携団体** (予定含む)	一般社団法人JPCERTコーディネーションセンター、一般社団法人日本電機工業会、公益社団法人計測自動制御学会、一般社団法人電子技術情報産業協会、一般社団法人日本電気計測器工業会、一般財団法人製造科学技術センター、電気事業連合会、一般社団法人日本ガス協会、一般社団法人日本化学工業協会

賛助会員の新設　：　研究成果などの普及活動

CSSCの組織体制

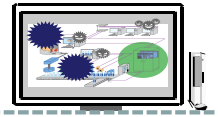
20130801現在

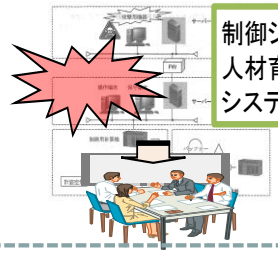
CSSCの研究開発の概要

人材育成プログラムの開発

制御システムにインシデントが発生した場合の対策に関する普及啓発システムについての技術を開発する。

制御システムにおけるマルウェア感染の影響および対策のための人材育成プログラム構築技術





制御システムセキュリティ人材育成のための模擬システム構築技術

評価・認証手法の開発

制御機器が実環境と同等の環境で稼働することを保証し、制御機器の接続性・脆弱性を検証し、それらの結果を視覚化する技術を開発する。

制御機器

制御機器間の接続性検証技術

制御システムにおける脆弱性検証技術

実環境エミュレーションソフトウェア技術

セキュリティ検証結果の視覚化技術

高セキュア化技術の開発

マルウェアの侵入防止や感染後の不正な動作の防止を図ることによるマルウェア対策技術、通信路での暗号化を図るための暗号化技術、構造自体をセキュアにする技術などを開発する。

制御機器

制御システムへのマルウェア侵入対策技術

高セキュアデバイス保護技術

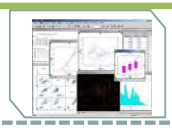
制御システム向け軽量暗号認証技術

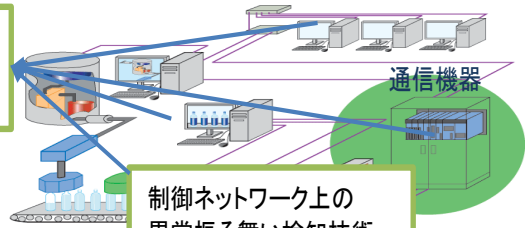
仮想環境における高セキュア制御システム構築技術

インシデント分析技術の開発

インシデントを検知するために、ネットワーク上の振る舞いや制御機器の異常を検知できる技術を開発する。

仮想環境化におけるサーバや制御機器の異常検知技術





制御ネットワーク上の異常振る舞い検知技術

テストベッド（CSS-Base6）の7つの模擬プラントシステム

ガスプラント

排水・下水プラント

■ 制御システムの特徴的な機能を切り出し、デモンストレーションとサイバー演習が実施可能な模擬システムを構築した。

組立プラント

化学プラント

ビル制御システム

広域制御（スマートシティ）

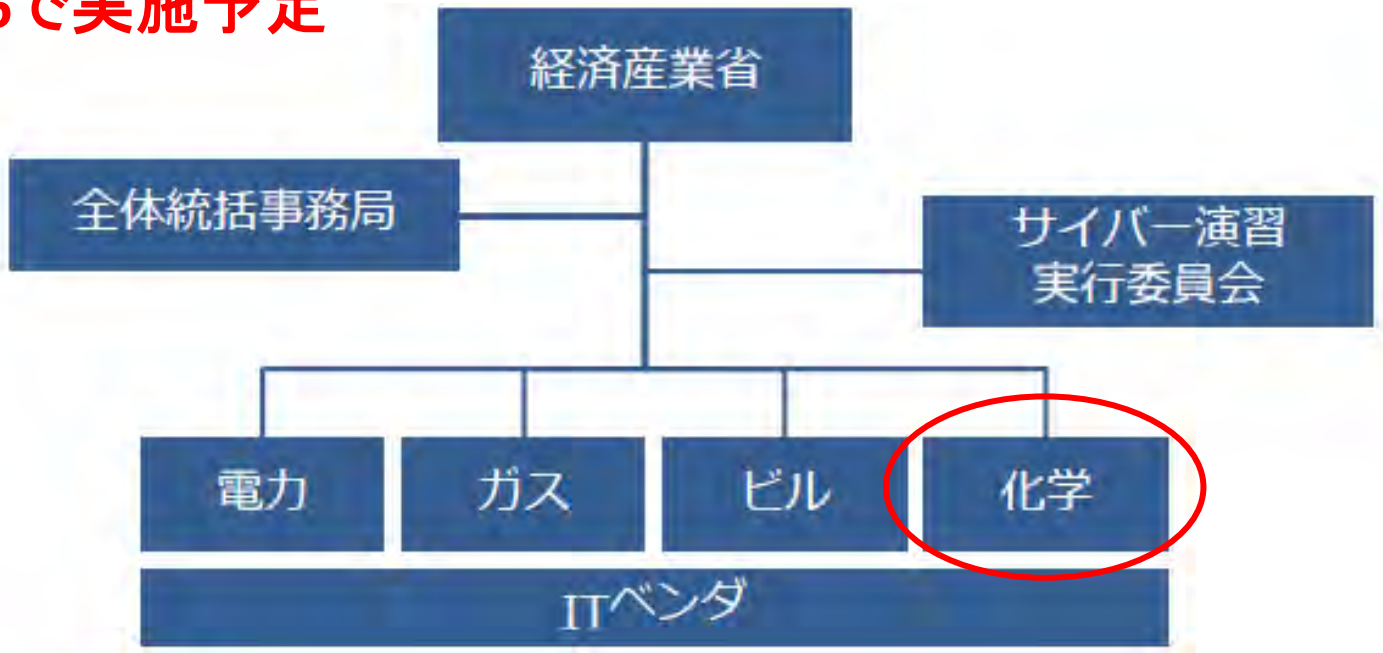
火力発電所訓練シミュレータ

2013年度の制御システムのサイバー演習

[演習の目的]

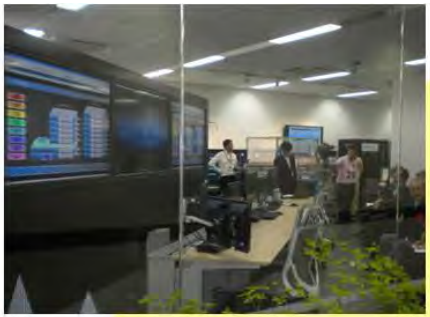
電力分野、ガス分野、ビル分野、化学分野において、現場の担当者、技術者、関係するベンダ等が、制御システムにおけるセキュリティ上の脅威を認識し、セキュリティインシデント発生の検知手順や障害対応手順の妥当性の検証を目的とするサイバーセキュリティ演習を実施し、各分野の参加者における制御システムセキュリティにおける対策を中心とした知見の獲得を促す。

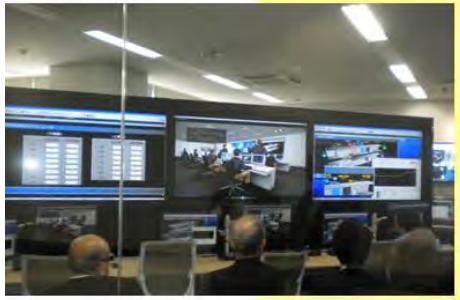
CSS-Base6で実施予定



CSS-Base6多賀城センターへの訪問状況

2013年5月開所式後、海外組織19を含む155の組織から704名の訪問者を受け入れている。CSSCでは、模擬プラントシステムを使用して認識向上、トレーニングやセミナーなどの普及啓発を進めている。（2013.12末現在）





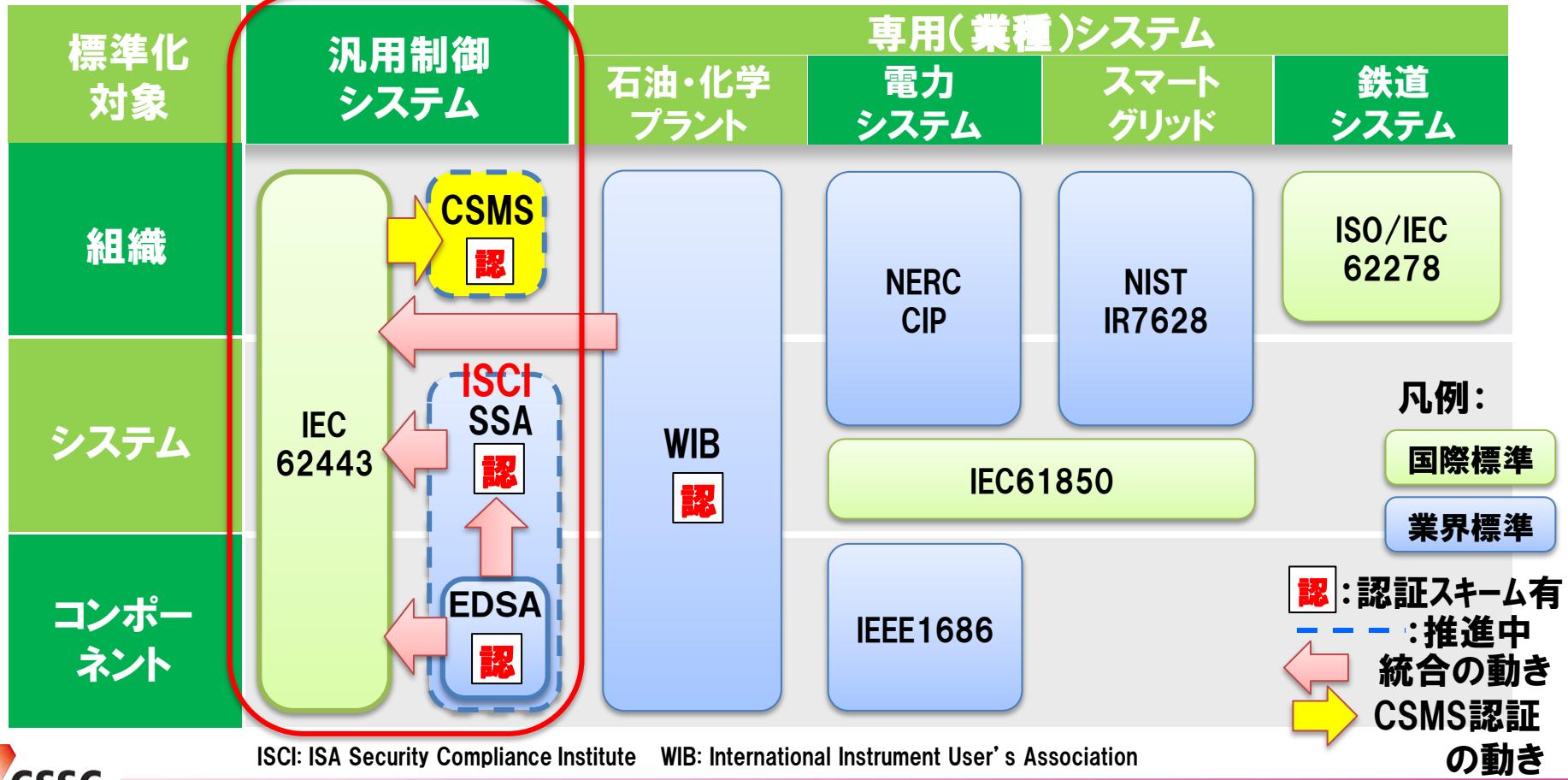
開所式でビル模擬システムのデモ実施。空調、エレベータ制御、照明制御など多種のビル内機器の制御を実施している。本デモは照明制御へのサイバー攻撃。

2. 制御システムセキュリティ認証への取り組み
～ISA/IEC62443の概要とEDSA認証について～

ISA ：International Society of Automation 国際計測制御学会
ISASecure : ISCI（ ISA Security Compliance Institute ）の認証プログラム
EDSA : Embedded Device Security Assurance

制御システム分野での標準化に関する動向

■制御システムのセキュリティの標準には、組織やシステムのレイヤに対応したもの、業種や業界に対応したものなど、様々な標準が提案されている。
■こうした中で、汎用的な標準として、IEC62443が注目されてきており、一部事業者の調達要件に挙がってきている。
■業界で評価認証が先行しているISCIやWIBの標準が、IEC62443のシリーズに統合される動きとなっている。
■制御システム事業者向けセキュリィマネージメントであるCSMS(IEC62443-2-1)認証が日本で推進されている。



ISCI: ISA Security Compliance Institute WIB: International Instrument User's Association

制御システムセキュリティ基準　IEC62443の全体像

■IEC62443は制御システムセキュリティの全レイヤ/プレイヤーをカバーした規格
■先行する評価認証の規格(EDSA認証等)がIEC62443に採用される方向

標準化 *1)

事業者

インテグレータ

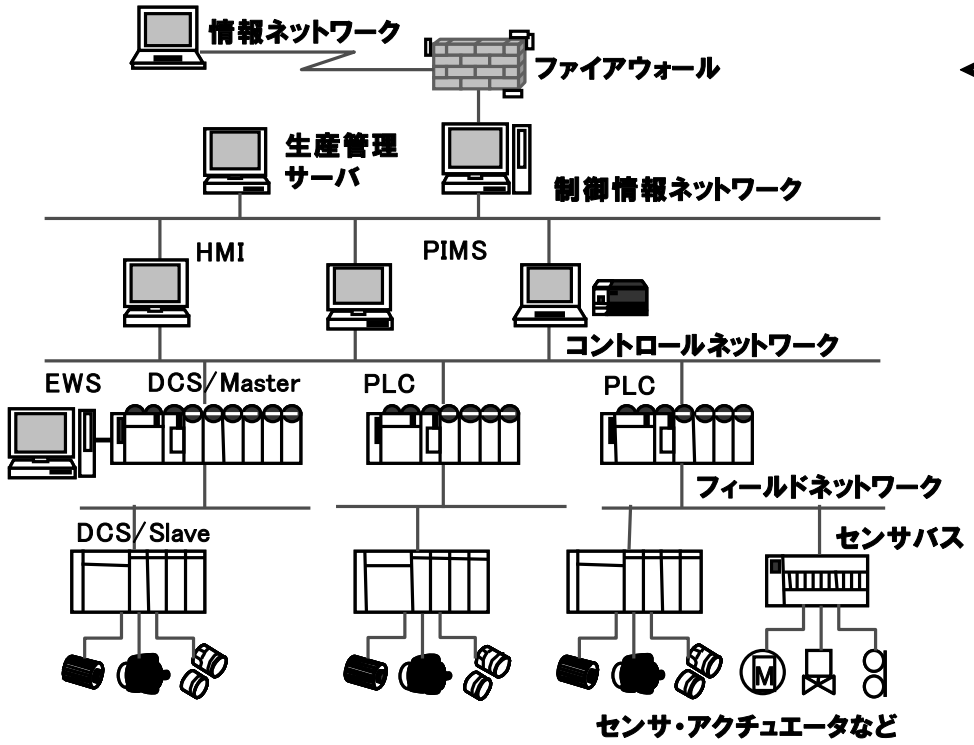
装置ベンダ

IEC62443-1

IEC62443-2
管理・運用・ﾌﾟﾛｾｽ

IEC62443-3
技術・システム

IEC62443-4
ｺﾝﾎﾟｰﾈﾝﾄ・ﾃﾞﾊﾞｲｽ



評価・認証

＜評価事業者＞

・WIB*3)

・ISCI : ISASeure
EDSA 認証*2)

*1) IEC62443のCyber securityの標準化作業は、IEC/TC65/WG10が担当(日本国内事務局はJEMIMAが対応)
*2) EDSA:Embedded Device Security Assurance:制御機器(コンポーネント)の認証プログラム→IEC62443-4に提案されている
*3) WIB: International Instrument User's Association →IEC62443-2-4に提案されている

DCS: Distributed Control System PLC: Programmable Logic Controller PIMS: Process Information Management System

ISA/IEC62443標準化状況と認証の状況

■13標準中、4つが標準化済み

■装置ベンダ向けEDSA認証は米国で先行、事業・運用者向けCSMS認証は国内で先行

CSMS認証

（Cyber Security Management System）

EDSA認証

（Embedded Device Security Assurance）

ISA Reference	IEC Reference	Title	Status
ISA-62443-1-1	IEC/TS 62443-1-1	Terminology, concepts and models	Published, Under Revision
ISA-TR62443-1-2	IEC/TR 62443-1-2	Master glossary of terms and abbreviations	Under Development
ISA-62443-1-3	IEC 62443-1-3	System security compliance metrics	Under Development
ISA-62443-1-4	IEC/TR 62443-1-4	IACS security life cycle and use case	Proposed
ISA-62443-2-1	IEC 62443-2-1	IACS security management system – Requirements	Published, Under Revision
ISA-62443-2-2	IEC 62443-2-2	IACS security management system - Implementation guidance	Proposed
ISA-TR62443-2-3	IEC/TR 62443-2-3	Patch management in the IACS environment	Under Development
ISA-62443-2-4	IEC 62443-2-4	Requirements for IACS solution suppliers	Under development within IEC TC65 WG10
ISA-TR62443-3-1	IEC/TR 62443-3-1	Security technologies for IACS	Published
ISA-62443-3-2	IEC 62443-3-2	Security assurance levels for zones and conduits	Under Development
ISA-62443-3-3	IEC 62443-3-3	System security requirements and security assurance levels	Published
ISA-62443-4-1	IEC 62443-4-1	Product Development Requirements	Under Development
ISA-62443-4-2	IEC 62443-4-2	Technical security requirements for IACS components	Under Development

ISA Security Compliance Institute (ISCI)とは

組織

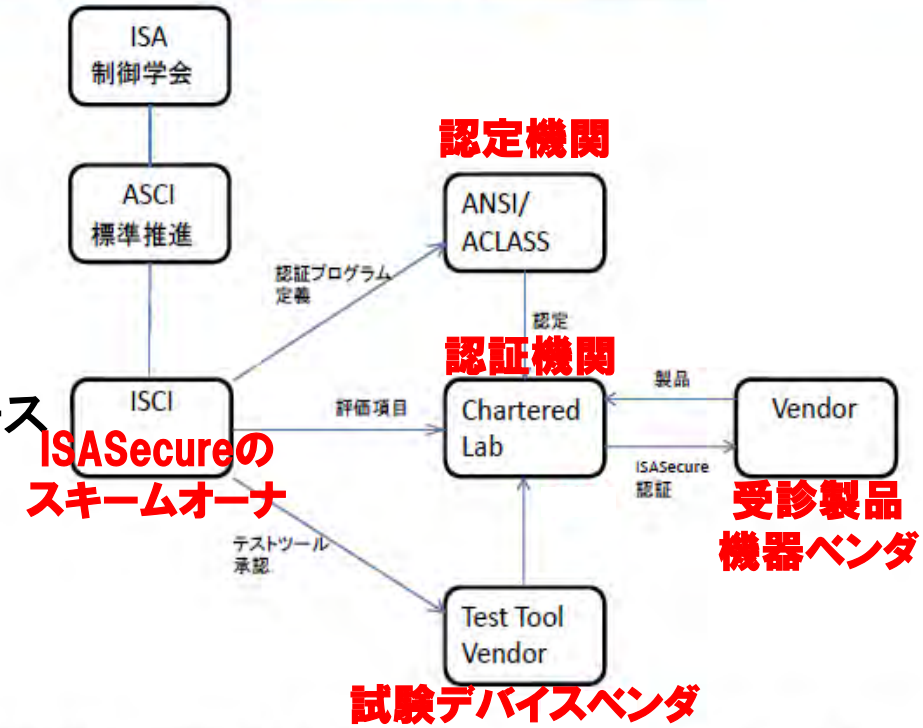
●アセットオーナー(制御システム事業者)、サプライヤ、及び業界組織からなるコンソーシアムで、ISA のAutomation Standards Compliance Institute(ASCI)内に2007年に構築された。

目的

● 制御システム製品向け
試験及び認証のための仕様とプロセスの確立

● アセットオーナー、サプライヤ、及び利害関係者の間の業界ベースのプログラム確立により、制御システムの開発、購入及び構築のための時間、コスト及びリスクの低減。

(参考)ISASecure認証プログラムの評価スキーム



出典:「ISA Security Compliance Institute (ISCI) and ISASecure™

ISA(International Society of Automation):世界各国に会員を持つ計測・計装・制御に関する学会
ASCI(Automation Standards Compliance Institute):ISAのもとに設置された制御システムの標準推進組織
ISCI (ISA Security Compliance Institute):ASCIのもとに設置されたコンポーネント・システムの規格策定・運用組織

ISCIのメンバタイプと加入組織

CSSCは、ISCIにアソシエートメンバとして加入（2013.11.26公表）。

①Strategic Member： Chevron、ExxonMobil、Honeywell、Invensys、Siemens、Yokogawa
　Voting有 年会費50000ドル
②Technical Member： Aramco Services、Codenomicon、Exida、RTP Corporation
　Voting有 年会費5000ドルから25000ドル
③Associate Member： CSSC（コンソーシアム組織が対象）
　Voting 無 年会費5000ドル
④Government Member ： IPA
　Voting 無 年会費5000ドル
⑤Information Member： Egemin、Globecomm
　Voting 無 年会費1500ドル

加入の目的：
1）SSA（ System Security Assurance ）の検討状況把握及び最終仕様の早期入手
2）EDSAのエンハンス検討状況の早期把握
3）適宜CSSCからの評価・認証実績に基づくコメント提案
　等

EDSA製品認証の動向

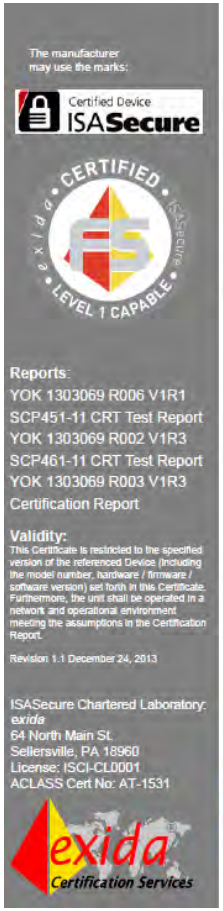
EDSA認証対象：制御システム向けの組込み機器

- 組込み機器とは、産業プロセスを直接、監視、制御及び駆動するよう設計された組込みソフトウェアを実行する特定目的を持ったデバイス
- 例:

  Programmable Logic Controller (PLC), Distributed Control System (DCS) controller
  Safety Logic Solver, Programmable Automation Controller (PAC)
  Intelligent Electronic Device (IED), Digital Protective Relay
  Smart Motor Starter/Controller, SCADA Controller, Remote Terminal Unit (RTU)
  Turbine controller, Vibration monitoring controller, Compressor controller

- ISASecure EDSA認証取得済組込み機器：3社5製品

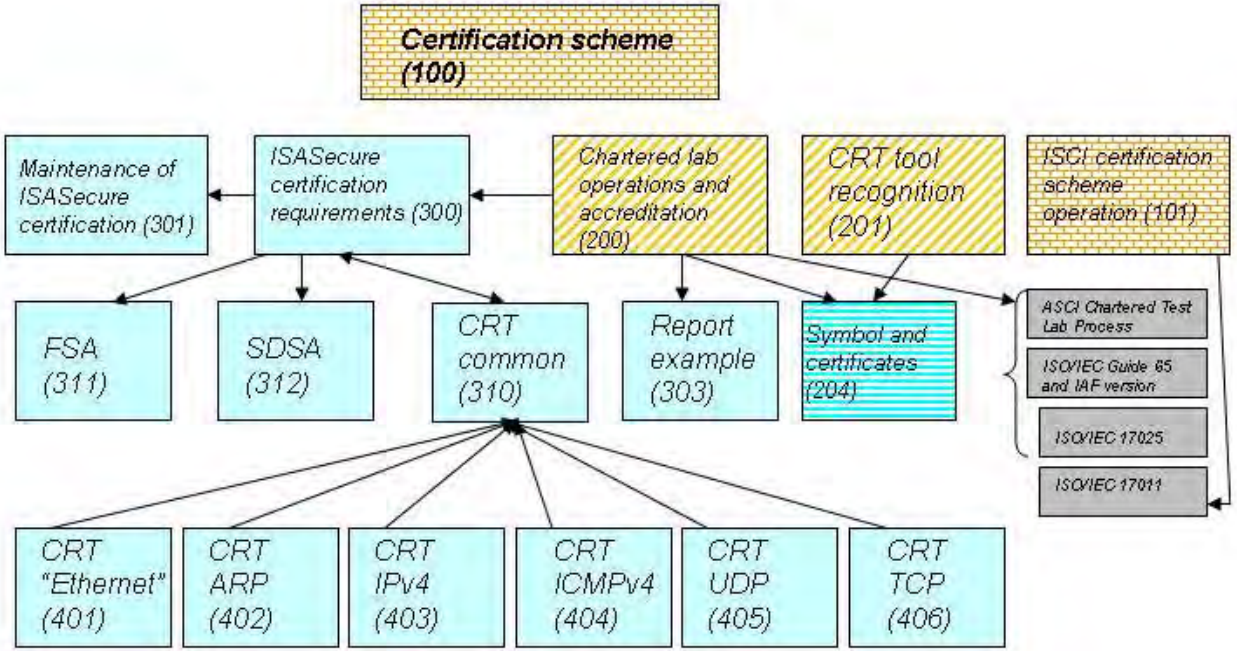
Supplier	Type	Model	Version	Level
Honeywell Process Solutions	Safety Manager	HPS 1009077 C001	R145.1	EDSA 2010.1 Level 1
RTP Corporation	Safety manager	RTP 3000	A4.36	EDSA 2010.1 Level 2
Honeywell Process Solutions	DCS Controller	Experion C300	R400	EDSA 2010.1 Level1
Honeywell Process Solutions	Fieldbus Controller	Experion FIM	R400	EDSA 2010.1 Level 1
Yokogawa	Safety Manager	SCP451-11 : Vnet/IP Firmware R19 SCP461-11 : Vnet/IP Firmware R18	R3.02.10	EDSA2010.1 Level 1



http://exida.com/YOK_1303069_ProSafe-RS_ISASecure_Level_1_Cert_C001_V1R3.pdf

出典：「ISA Security Compliance Institute (ISCI) and ISASecure™

ISASecure EDSA 適合スキーム定義ドキュメント



ISASecure EDSA 適合スキーム定義ドキュメント

ISASecure EDSAプログラムドキュメントには5つの主要なカテゴリーがあります。

- **技術仕様**：薄い水色で表示。デバイスが認証されるか否かを決定するために適用される技術評価基準を記しています。
- **認定/認可**：ゴールドの斜線で表示。どのようにすればある組織が公認試験所になれるか、又はツールサプライヤがCRTツールの認可を得られるかについて、記載しています。
- **シンボルと認証**：水色の横線で表示。ISASecureシンボルや証書の適切な使用についてカバーしています。
- **構成**：オレンジの煉瓦模様で表示。プログラム全体及び運営について記載しています。
- **外部参照**：濃い灰色で表示。ISASecure EDSAプログラムドキュメントで参照されるこの特定プログラムの外部に存在するドキュメントです。

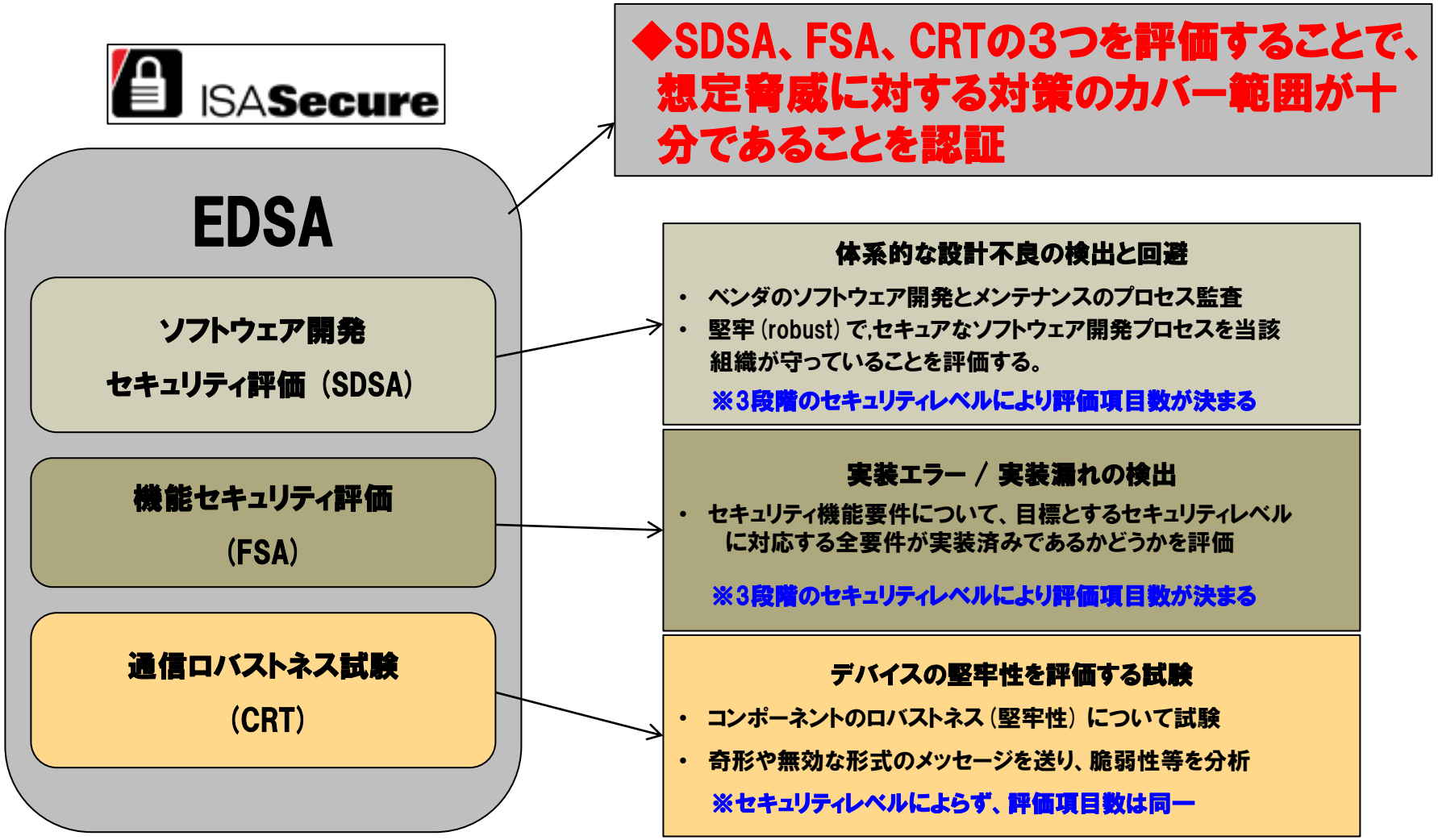
http://isasecure.org/ISASecure-Program/Japanese-ISASecure-Program.aspxからダウンロードできます。

EDSA標準の対訳版

IPAにより翻訳されたEDSA標準の対訳版はISCIウェブサイトにて公開。

http://isasecure.org/ISASecure-Program/Japanese-ISASecure-Program.aspx

EDSA認証の各評価項目概要



EDSA：Embedded Device Security Assurance

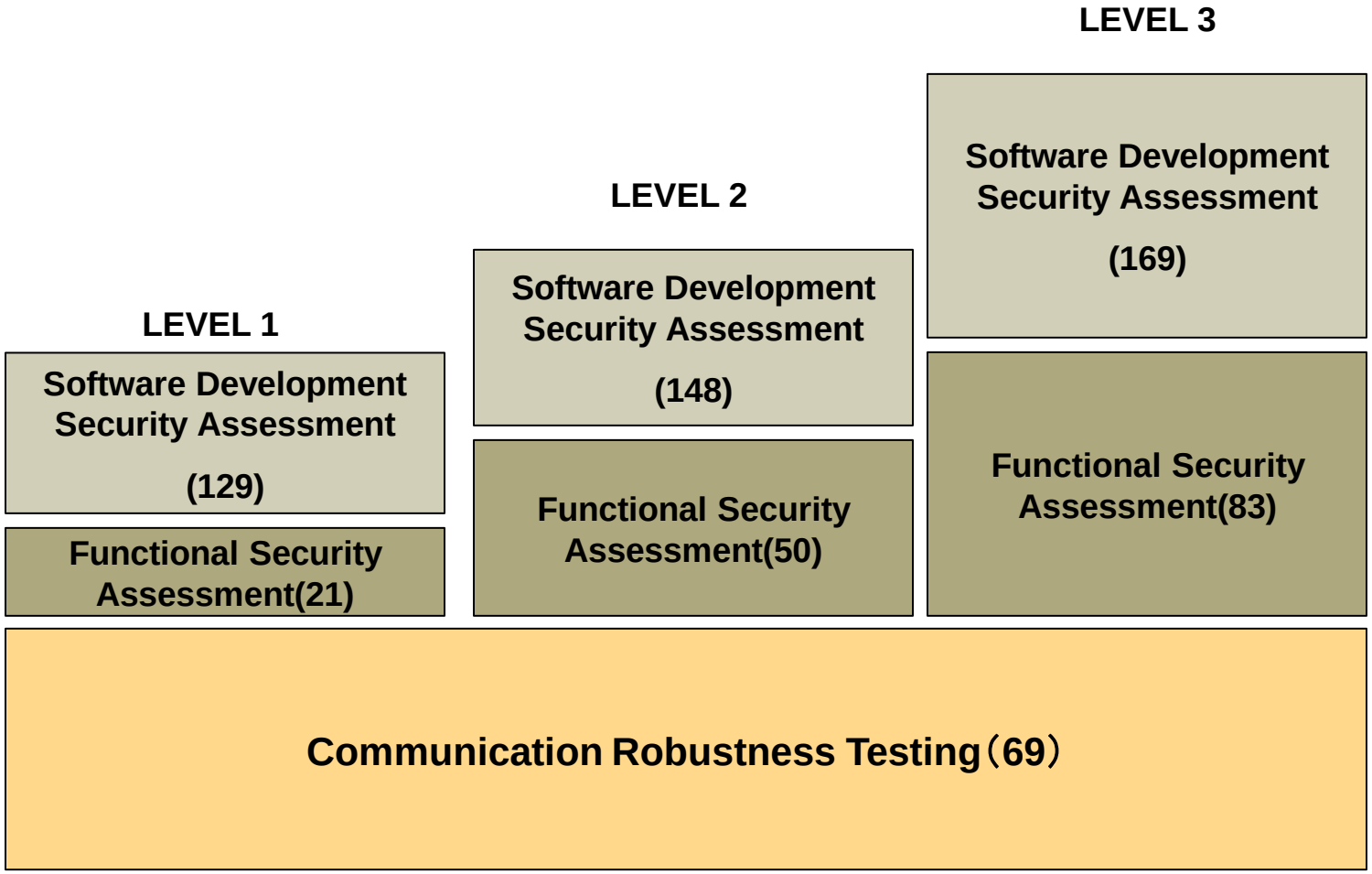
注：正式には原英文を参照してください。

Communication Robustness Testing(CRT), Functional Security Assessment (FSA), Software Development Security Assessment(SDSA)

出典：「ISA Security Compliance Institute （ISCI） and ISASecure™及びhttp://www.css-center.or.jp/sympo/2013/documents/sympo20130528-andre.pdf

ISASecure 3段階のセキュリティレベル

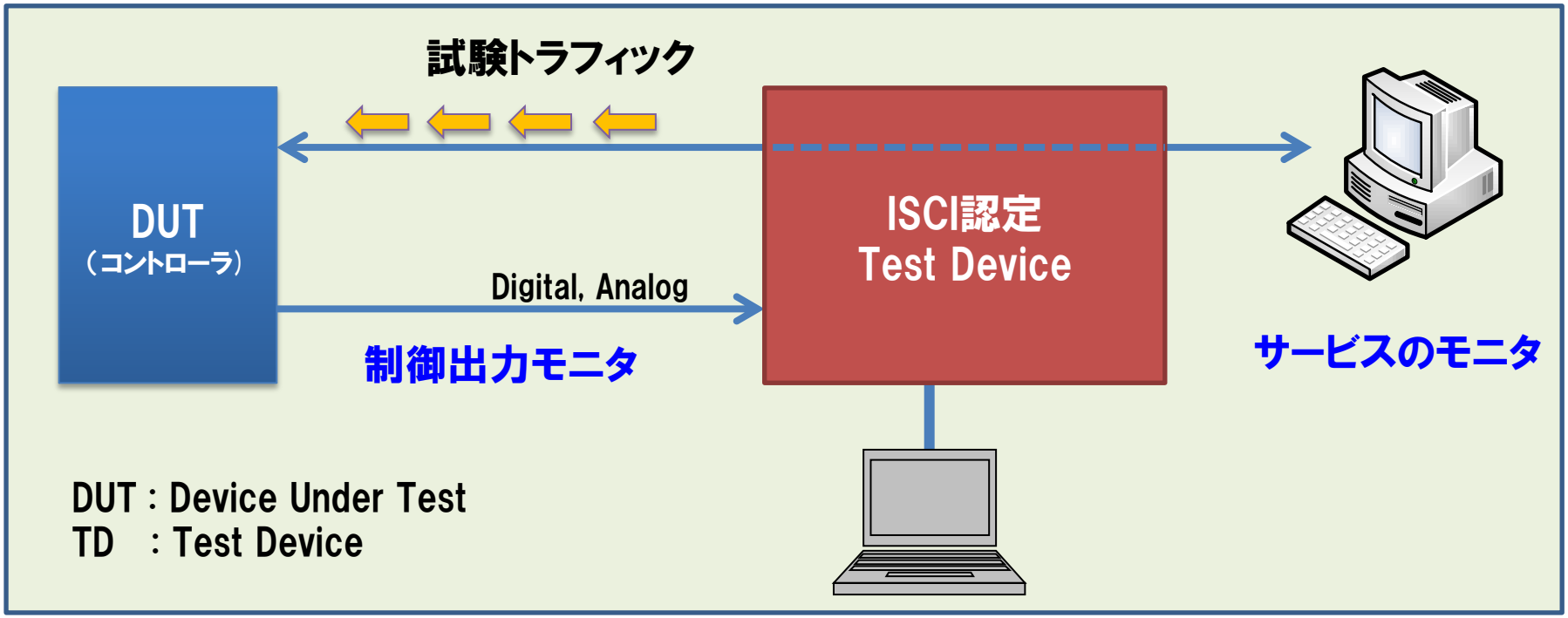
評価項目の数によって3段階の認証レベルを規定



出典：ICSJWG Spring 2011, (ASCI)
「Validating the Security Assurance of Industrial Automation Products

CRT試験の内容 ・・・ CRT試験機器構成

- ISCI認定の試験デバイスにより試験パケットをDUTに対して送信し、サービスの維持を確認
- 6つの必須サービスの維持が合否判定基準
  ⇒コントローラだけではなく、事実上HMI側の用意も必要



図：CRT試験環境のイメージ

CRT試験の内容 ・・・ 6つの必須サービス

■ 6つの必須サービス

次の機能を用いたサービスが適切に維持されていることを確認する

① 制御ループ
- 規定の信号を出力する機能

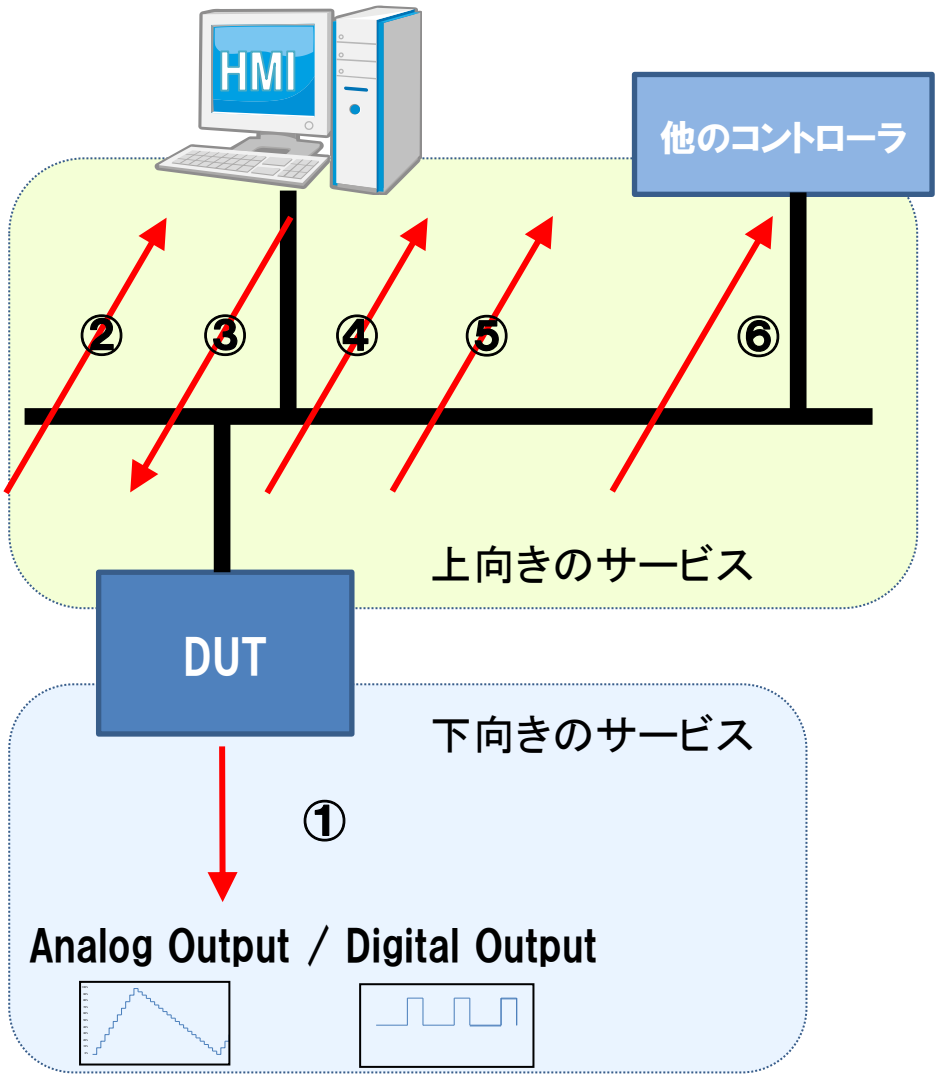
② プロセスのビュー
- プロセスビューを適切なタイミングで提供する機能

③ コマンド
- 上位システムからの命令に適切なタイミングで応答する機能

④ プロセスアラーム
- プロセスアラームを適切なタイミングで送信する機能

⑤ 必須履歴データ
- 必須履歴データを適切なタイミングで送信する機能
  例：製薬事業におけるFDA対応
- 適用除外可能

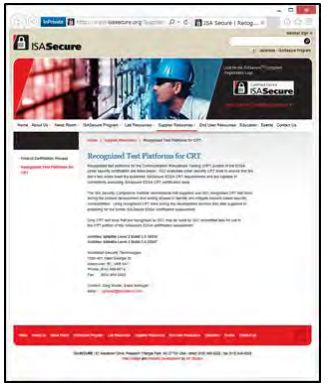
⑥ ピアツーピア制御通信
- ピアツーピア制御通信を送信する機能
- 適用除外可能



CRT試験の内容 ・・・ ISCI認定 試験デバイス

CRT試験には、ISCI の認定した試験デバイスを用いる。

ISASecure : Recognized Test Platforms for CRT
http://www.isasecure.org/Supplier-Resources/Recognized-Test-Platforms-for-CRT.aspx

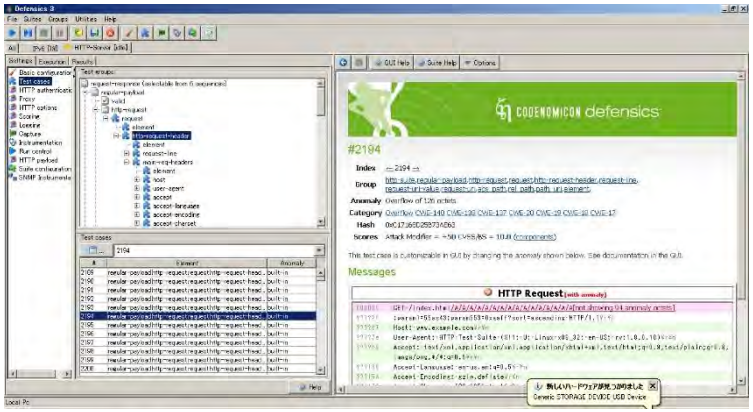


●Wurldtech 社 Achilles Test Platform

http://www.wurldtech.com/product_services/discover_analyze/achilles_test_platform/

●Codenomicon社 DEFENSICS

http://www.codenomicon.com/defensics/



CRT試験とは ・・・ 試験対象プロトコル

- Group 1 に該当するプロトコルに対する要件は、EDSA 401～406で規定
- Group 2～Group 5 については、ISASecure EDSA認証プログラムで用意されていく予定

Group 1	Group 2	Group 3	Group 4	Group 5
• IEEE 802.3 (Ethernet) • ARP • IPv4 • ICMPv4 • TCP • UDP コアプロトコル	• BOOTP • DHCP • DNS • NTP, SNTP • FTP, TFTP • HTTP • SNMPv1-2 • Telnet	• HTTPS • TLS • Modbus/TCP	• IPv6 • OPC • Ethernet/IP/CIP • PROFINET • FFHSE • Selected wireless protocols/stacks with elements such as: - IEEE 802.11 - ISA100.11a - WirelessHART	• SNMPv3 • SSH • Server • OPC-UA • MMS • IEC 61850 • SMTP

Protocols for ISASecure Communications Robustness Testing

FSA/SDSA概要

- FSA: Functional Security Assessment (EDSA-311)
  - 対象機器のセキュリティ機能のアセスメント
  - EDSA-311の要求事項に沿って、対象機器の機能や初期設定等の確認を行い、適合/不適合を評価する
  - 実機テスト
    - 一部要求事項については、実機を用いて実際に動作を確認する
- SDSA: Software Development Security Assessment (EDSA-312)
  - 対象機器のソフトウェア開発プロセスのアセスメント
  - 開発ドキュメント(計画/成果物)とレビュー記録(PDCAプロセスの妥当性と記録確認)
- EDSA情報
  - ISASecure Webサイト

    http://www.isasecure.org/ISASecure-Program.aspx

FSAの主な要求事項

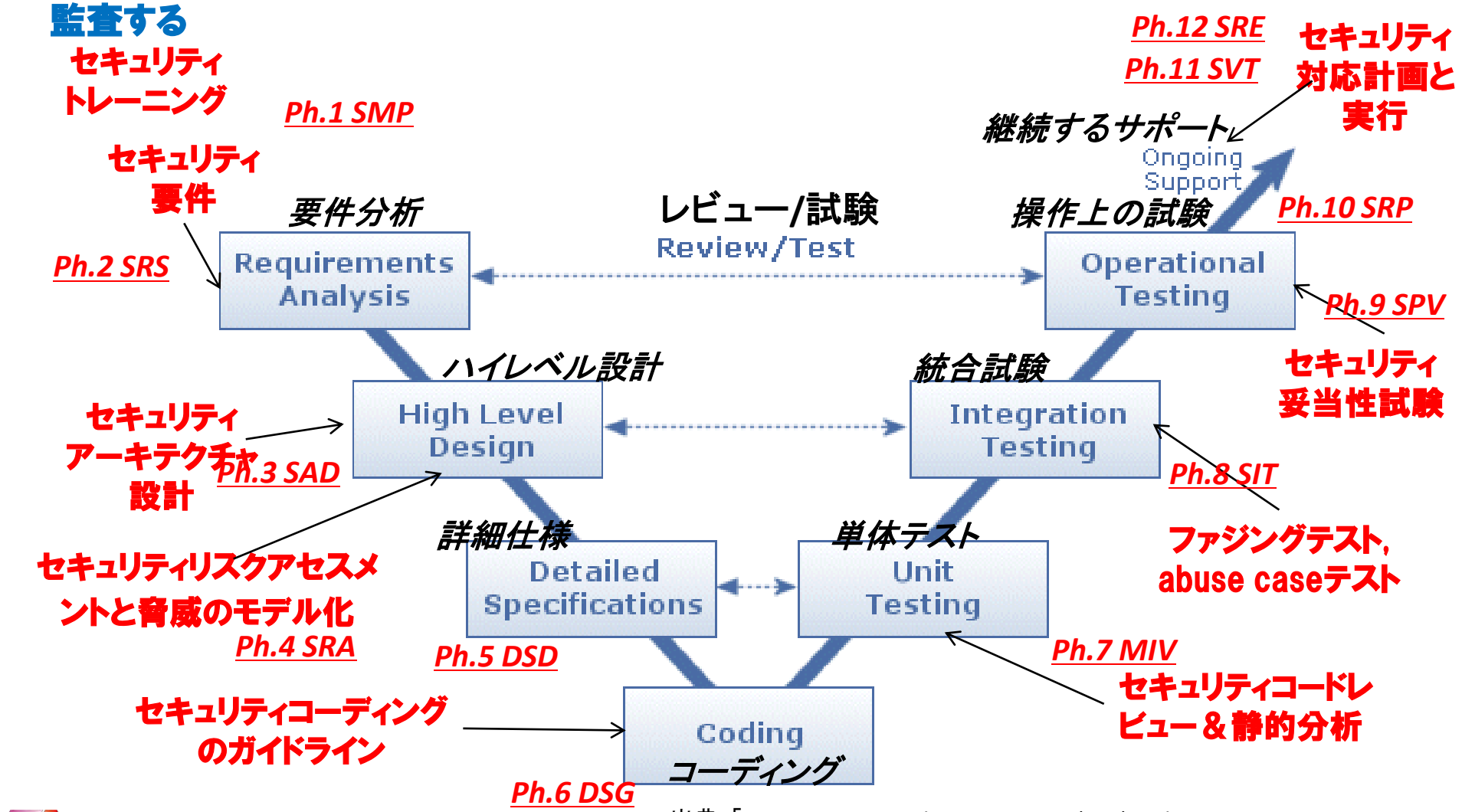
アクセスコントロール (AC: Access Control)	ユーザ承認、ユーザ認証、システム使用通知、セッションロック/終了 User Authorization, User Authentication, System Use Notification, Session Locking/Termination
使用コントロール (UC: Use Control)	デバイス認証、監査証跡 Device Authentication, Audit Trail
データの完全性 (DI: Data Integrity)	転送中のデータ、保管中のデータ Data in Transit, Data at Rest
データの機密性 (DC: Data Confidentiality)	転送中のデータ、保管中のデータ、暗号化 Data in Transit, Data at Rest, Crypto
データフロー制限 (RDF: Restrict Data Flow)	情報フロー実施、適用パーティッショニング、機能分離 Information Flow Enforcement, Application Partitioning, Function Isolation
イベントへのタイムリーなレスポンス (TRE: Timely Response to Event)	インシデント応答 Incident Response
ネットワークリソースの可用性 (NRA: Network Resource Availability)	サービス不能攻撃防御、バックアップと回復 Denial of Service Protection, Backup & Recovery

SDSA ： 活動フェーズ一覧

番号	活動フェーズ
PH1	セキュリティ管理プロセス（SMP）
PH2	セキュリティ要求事項仕様（SRS）
PH3	ソフトウェアアーキテクチャ設計（SAD）
PH4	セキュリティリスクアセスメントと脅威のモデル化（SRA）
PH5	詳細ソフトウェア設計（DSD）
PH6	セキュリティ指針文書（DSG）
PH7	モジュールの実装と検証（MIV）
PH8	セキュリティ統合テスト（SIT）
PH9	セキュリティプロセス検証（SPV）
PH10	セキュリティ対応計画（SRP）
PH11	セキュリティ検証テスト（SVT）
PH12	セキュリティ対応実行（SRE）

ソフトウェア開発ライフサイクルへのセキュリティ導入

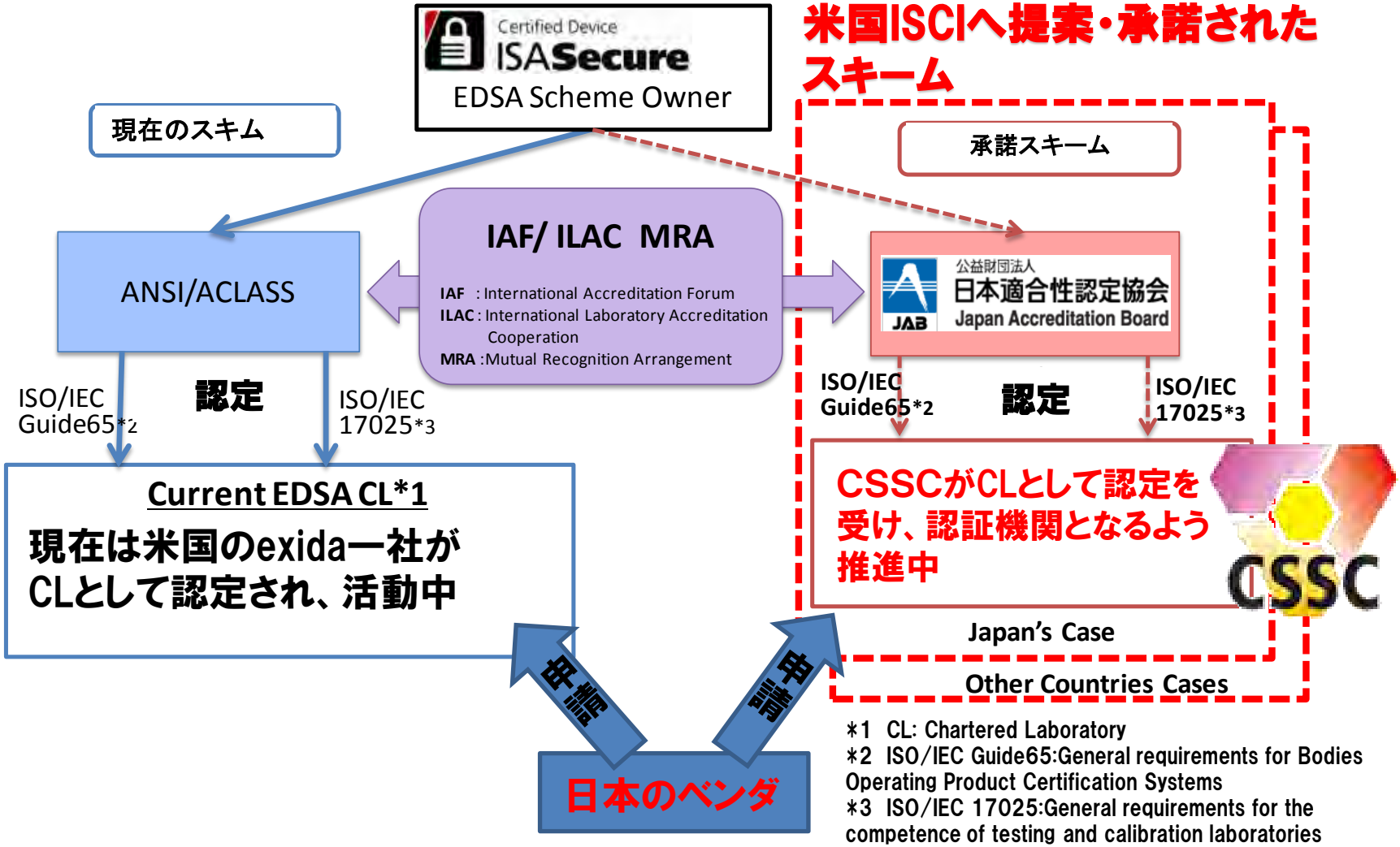
SDSAでは、開発プロセスのV字モデルにセキュリティ活動フェーズが組み込まれていることを監査する



出典：「ISA Security Compliance Institute (ISCI) and ISASecure™

ISASecure (EDSA) 認証スキームの日本での展開

日本で日本語による世界共通の認証取得を可能に



*1 CL: Chartered Laboratory
*2 ISO/IEC Guide65:General requirements for Bodies Operating Product Certification Systems
*3 ISO/IEC 17025:General requirements for the competence of testing and calibration laboratories
*4 CSSC:Control System Security Center

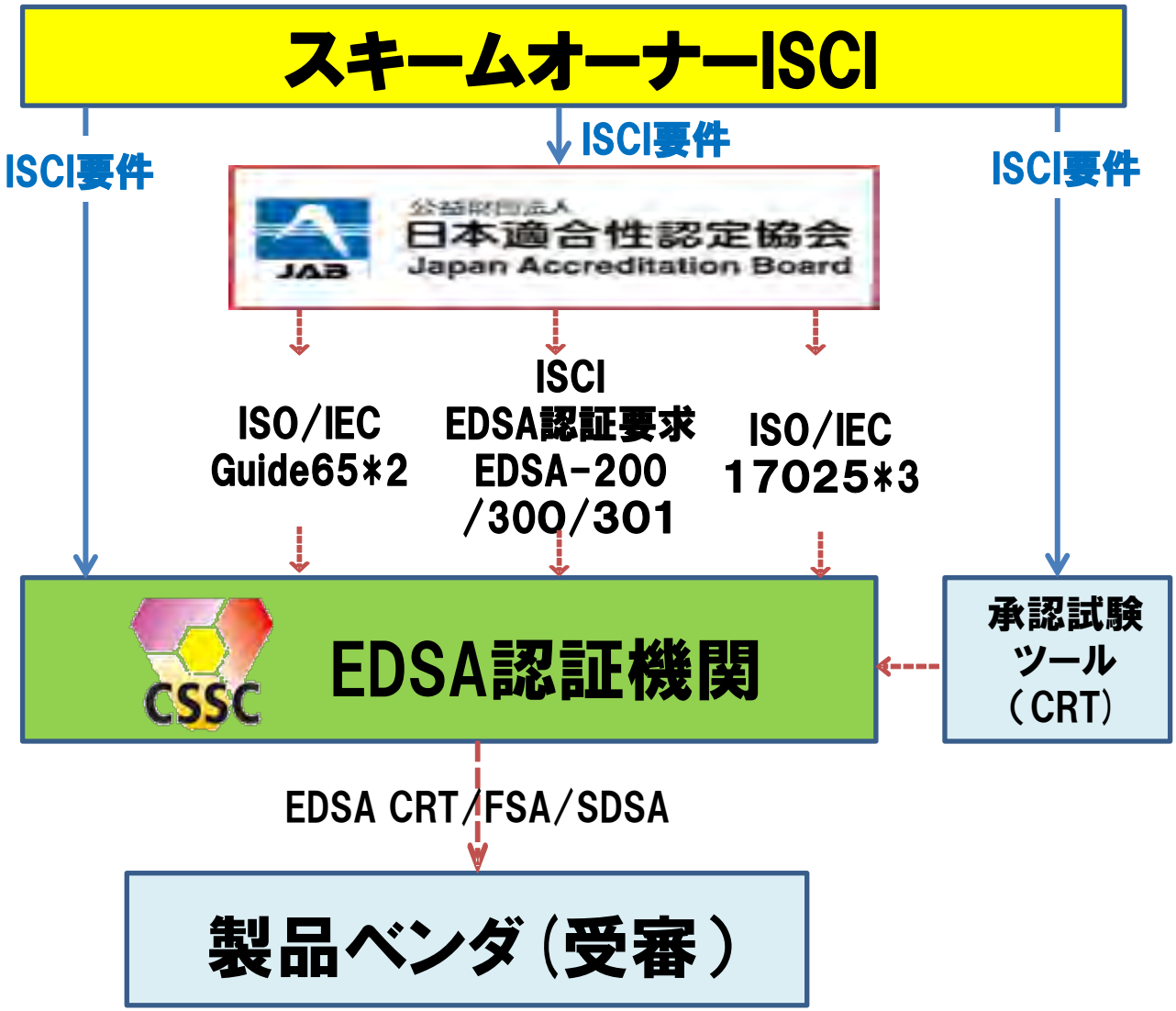
ISASecure EDSA認証の認定取得とは

2013.9JAB へ認定申請

主要な要求事項の標準

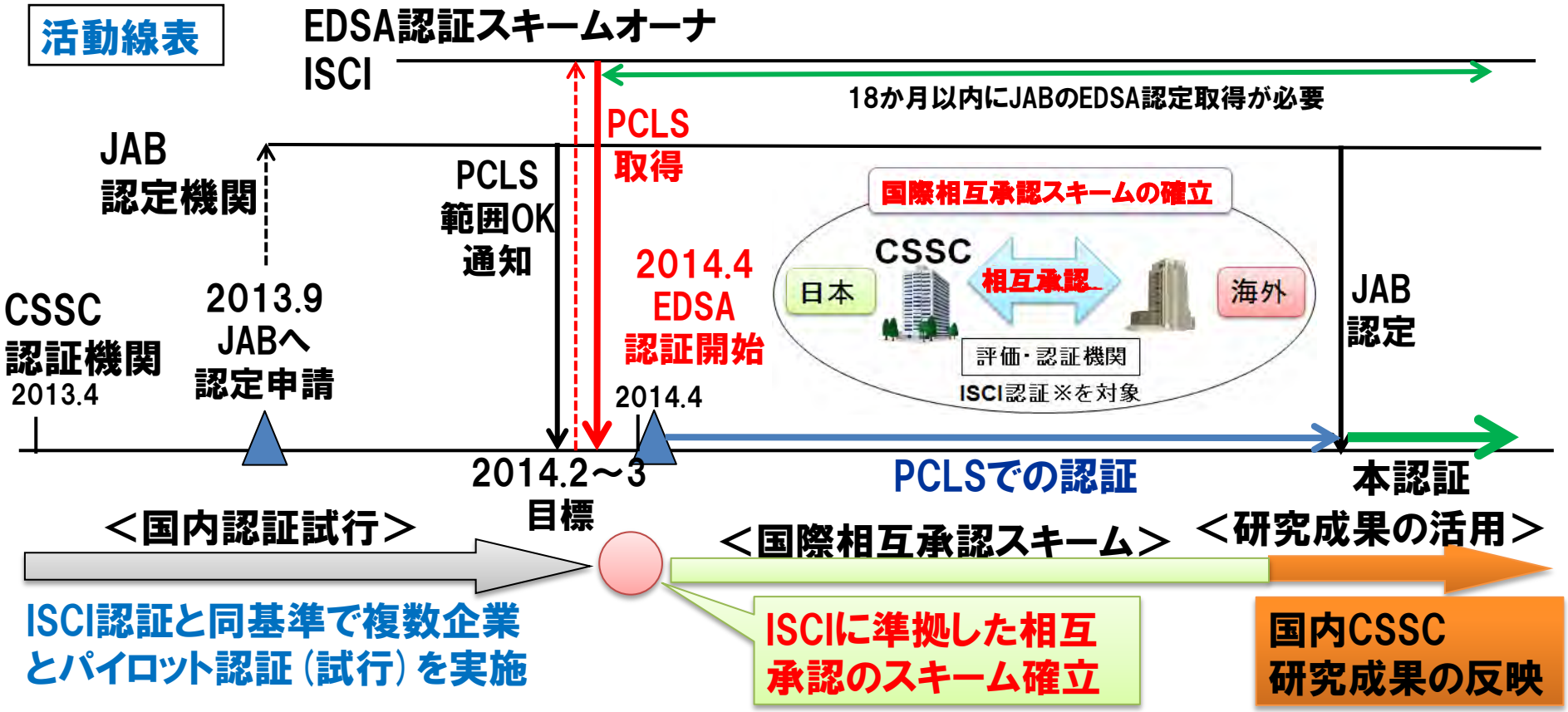
ISO/IEC17025:
試験所及び校正機関の能力に関する一般要求事項

ISO/IECGuide65:
製品認証機関に対する一般要求事項



EDSA認証機関に向けての具体的取組み

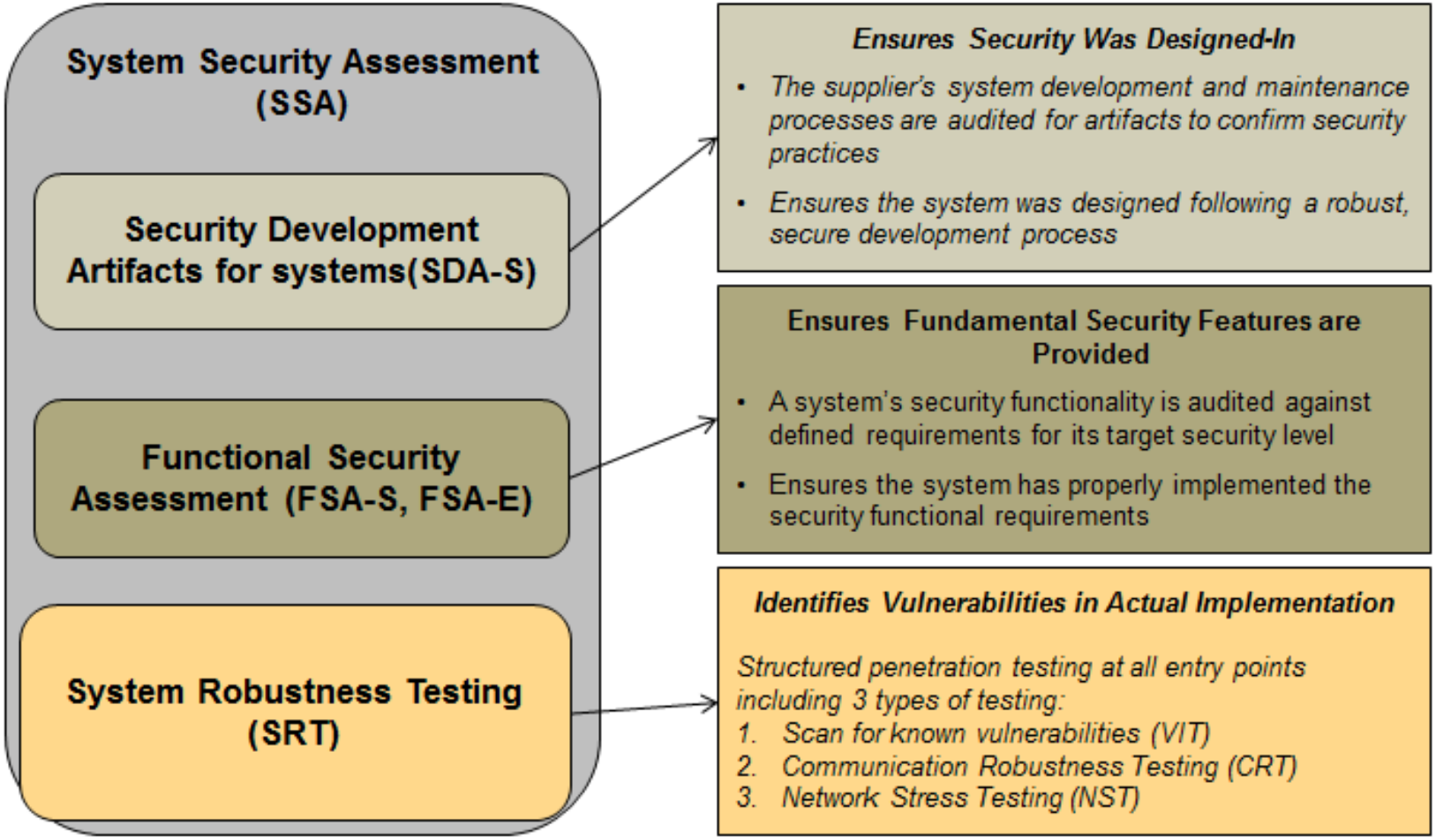
**2014年4月よりPCLS（仮免状態）でのEDSA認証のサービス開始予定。
認証機関の体制・EDSA認証標準への取組み・品質マニュアル等の整備をし、
JABに対し2013.9に認定申請をし、現在審査中の状態。**



ISCI：ISA Security Compliance Institute　ISA ：International Society of Automation国際計測制御学会 PCLS: Provisional Chartered Laboratory Status 仮免状態

SSA認証の各評価項目概要

SSA ： ドメインにコンジット対する3つの評価
（SDA-S, FSA-S, FSA-E, SRT (VIT, CRT, NST)

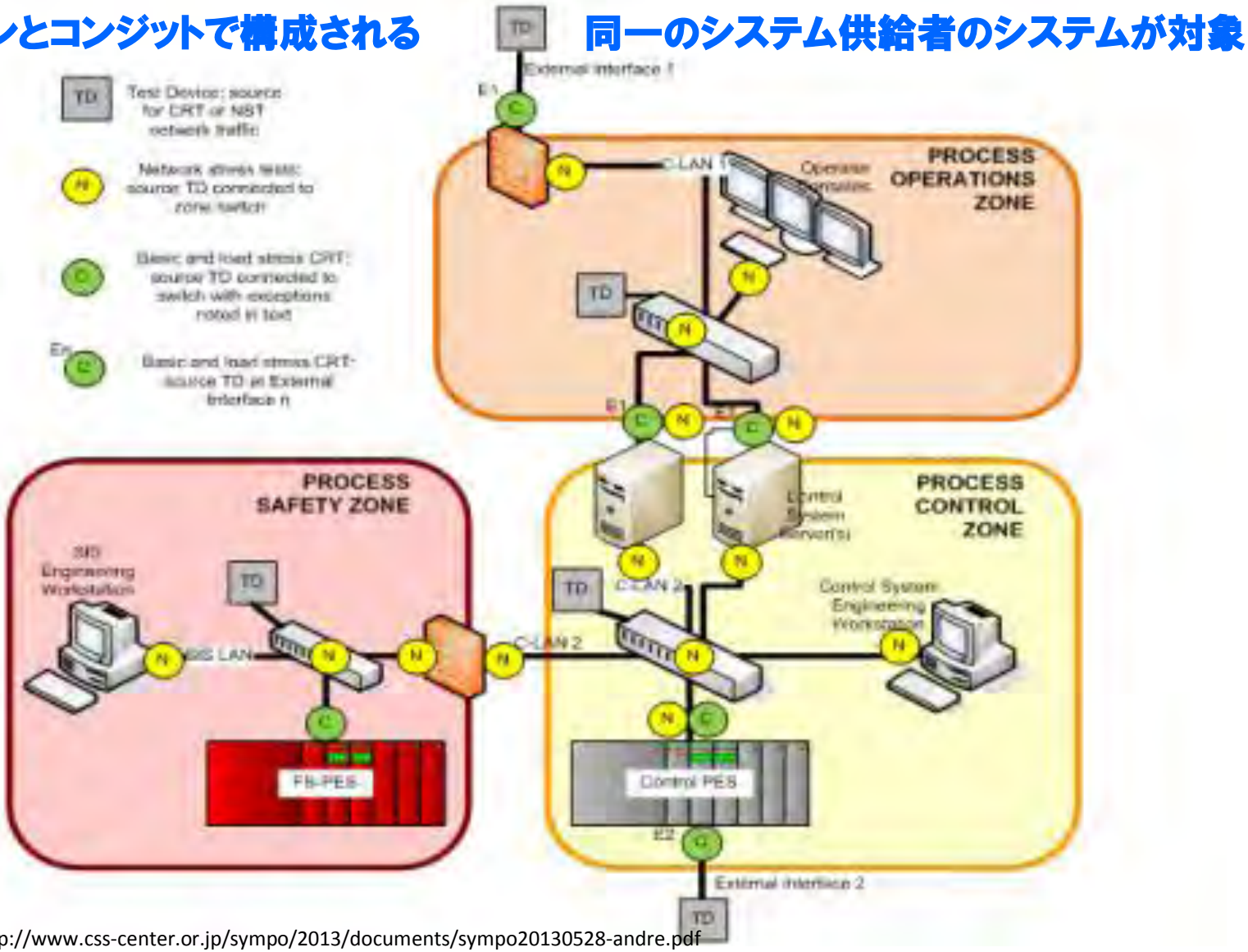


出典：http://www.css-center.or.jp/sympo/2013/documents/sympo20130528-andre.pdf

SSA対象システム

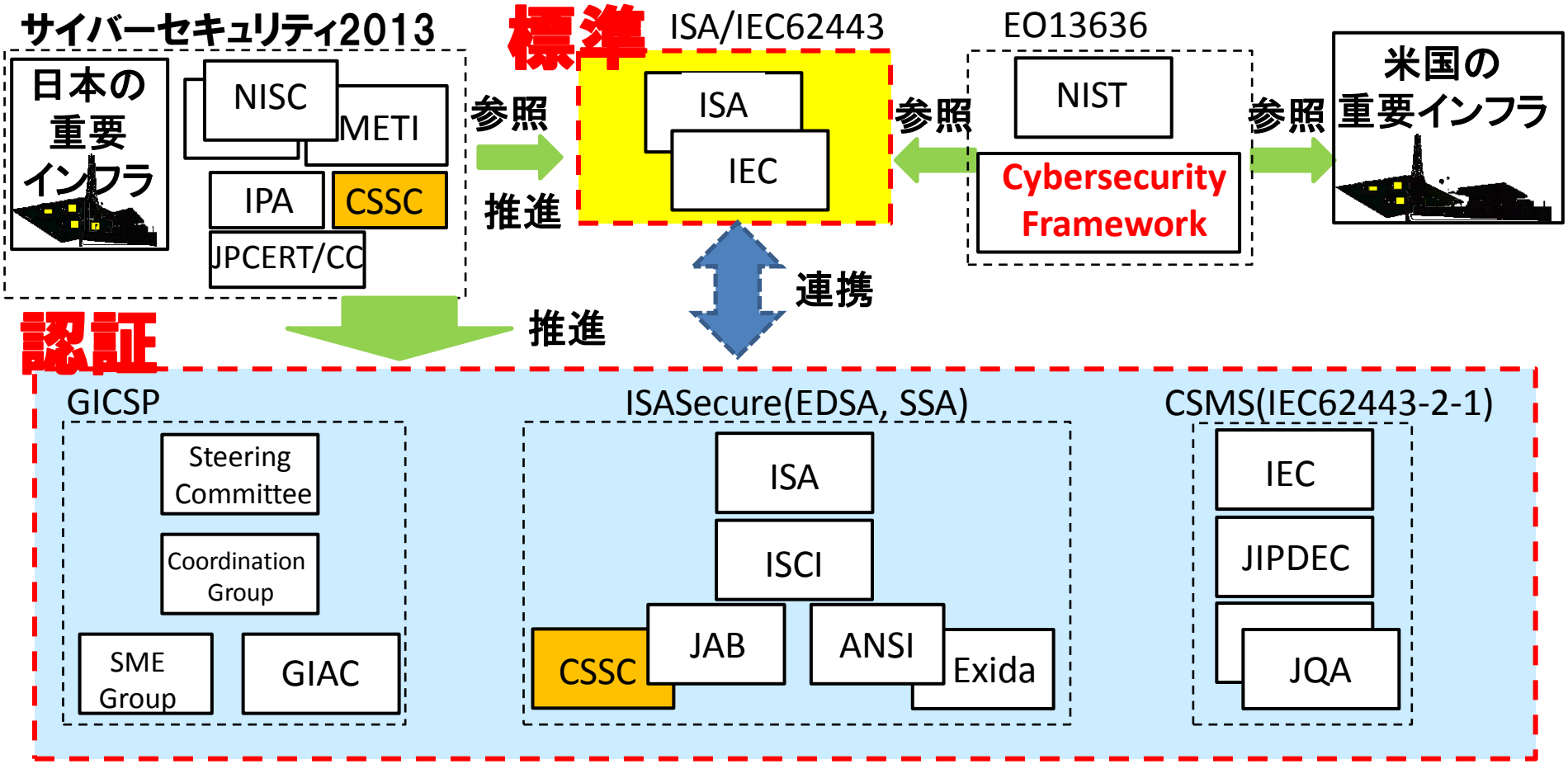
複数のドメインとコンジットで構成される

同一のシステム供給者のシステムが対象



出典：http://www.css-center.or.jp/sympo/2013/documents/sympo20130528-andre.pdf

参考：ISA/IEC62443を中心とした標準と認証



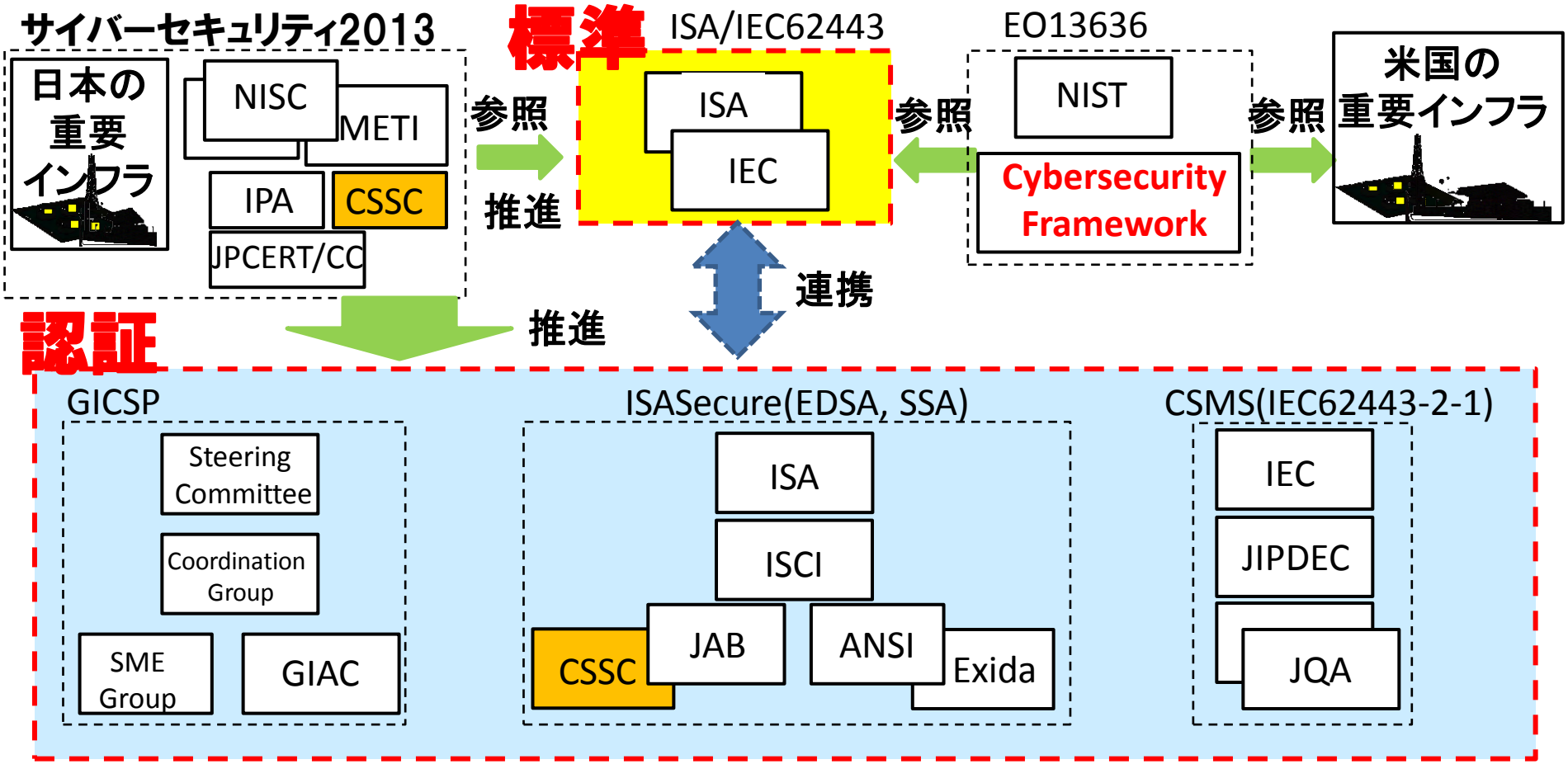
制御システムセキュリティ
プロフェッショナル（人）
認証
(GICSP: Global Industrial Cyber Security Professional
ISA/IEC62663とNERC CIPが参照されている。)

制御システム
システムや機器
認証

制御システム
運用・供給組織
認証

ICS : Industrial Control Systems

参考：ISA/IEC62443を中心とした標準と認証



制御システムセキュリティ
プロフェッショナル（人）
認証
(GICSP: Global Industrial Cyber Security Professional
ISA/IEC62663とNERC CIPが参照されている。)

制御システム
システムや機器
認証

制御システム
運用・供給組織
認証

ICS : Industrial Control Systems

参考：CERT C/C++セキュアコーディングスタンダード

JPCERT CC® Japan Computer Emergency Response Team Coordination Center
JPCERTコーディネーションセンター

- セキュアコーディングとは、プログラムの実装(コーディング)段階で、脆弱性を作り込まない、あるいは作り込まれた脆弱性を検出し修正する取組みや手法である。CERT C / C++ セキュアコーディングスタンダードは、脆弱性に直接つながる製品の弱点となるコードや、セキュリティ品質に関わるコーディングを特定し、セキュアで品質の高いコードを作成するためのコーディング規約としてまとめられている。
- 全てのルールに準拠する必要はなく、各ルールに設定された優先度に基づき、組織や開発プロジェクトに合わせてカスタマイズして利用することが可能である。このCERT C / C++ セキュアコーディングスタンダードを導入することで、以下の実現が期待できる。
  - より高品質でセキュアな製品開発
  - 発生しうる攻撃リスクの把握
  - コードのセキュリティ品質を評価する指標のひとつとして活用
  - 2014年度より開始が予定されているEDSA認証の要求事項の一部への対応

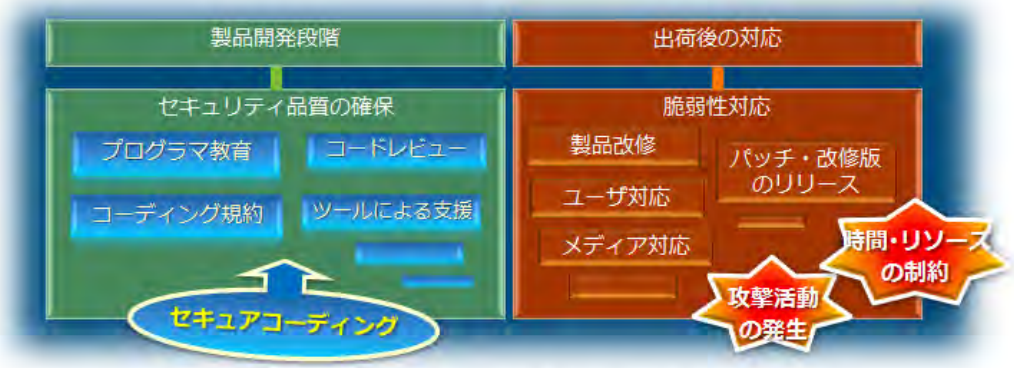


図１：製品へのセキュリティ対策導入タイミングがもたらす効果の違い

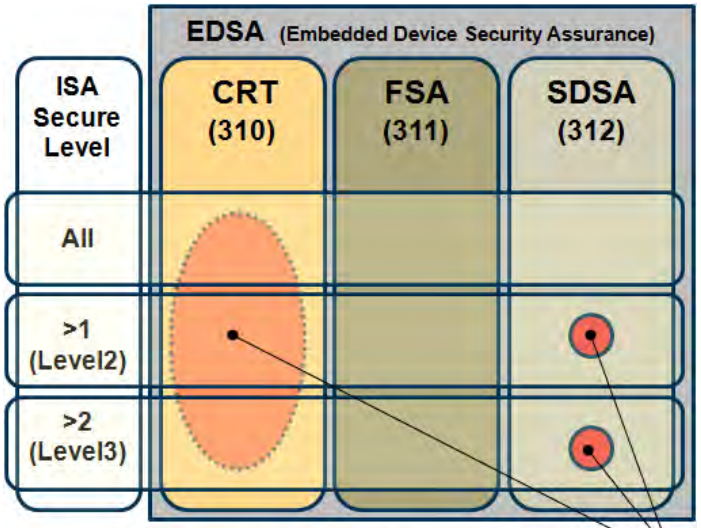


図２：CRTとSDSAの要求事項の一部充足が期待できる

CERT セキュアコーディングスタンダードは、C / C++ / Java の3種類を提供中
詳細情報: https://www.jpcert.or.jp/securecoding.html
本件に関する連絡先：secure-coding@jpcert.or.jp

セキュアな制御システムを世界へ未来へ

CSSCホームページ
http://www.css-center.or.jp/

CSSC説明ビデオ（日本語版）
http://www.youtube.com/watch?v=wbEiDQZU5sI&feature=youtu.be