Embedded Technology 2013

制御セキュリティセッション

IEC62443の概要と認証について

EDSA：Embedded Device Security Assuranceを中心に

2013年11月20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　部長
CSSC認証ラボラトリー長
評価認証・標準化委員会 副委員長

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

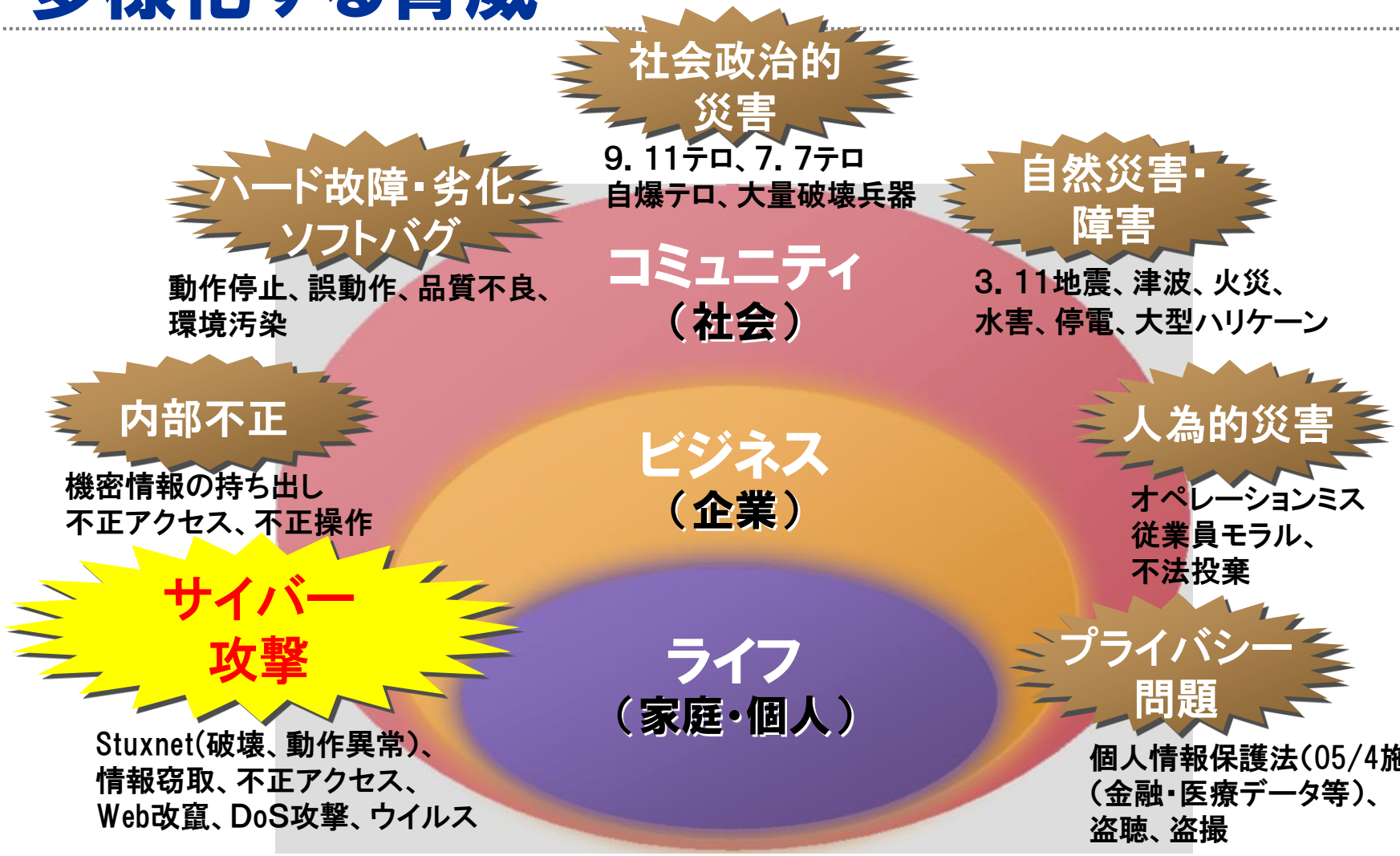
目次

1. 制御システムへのサイバー攻撃の脅威増大
2. 制御システムセキュリティセンターの紹介
3. IEC62443の概要と認証について
   ～制御システムの認証への取り組み～

奈良時代後半の多賀城外郭南門（推定復元図）

1． 制御システムへのサイバー攻撃の脅威増大

多様化する脅威



「サイバー攻撃」の脅威に対する社会的関心増大

重要インフラの制御システムへの攻撃例

➢Stuxnet(スタックスネット)による制御システム停止攻撃

- Stuxnet攻撃の特長

◇入念に準備されたマルウェア
（事前に制御システムの構成や数を把握）

◇複数のゼロデイ脆弱性を狙う

◇オペレータの監視を欺く

- 制御システムを停止させた目的は？

◇イランの核開発を遅らせるために使われたと言われている

2009年の終わりから2010年の初頭にかけて、イランにある遠心分離器9000台のうち、約1000台がStuxnetによって破壊されたとしている。

http://japan.zdnet.com/security/analysis/35005709/

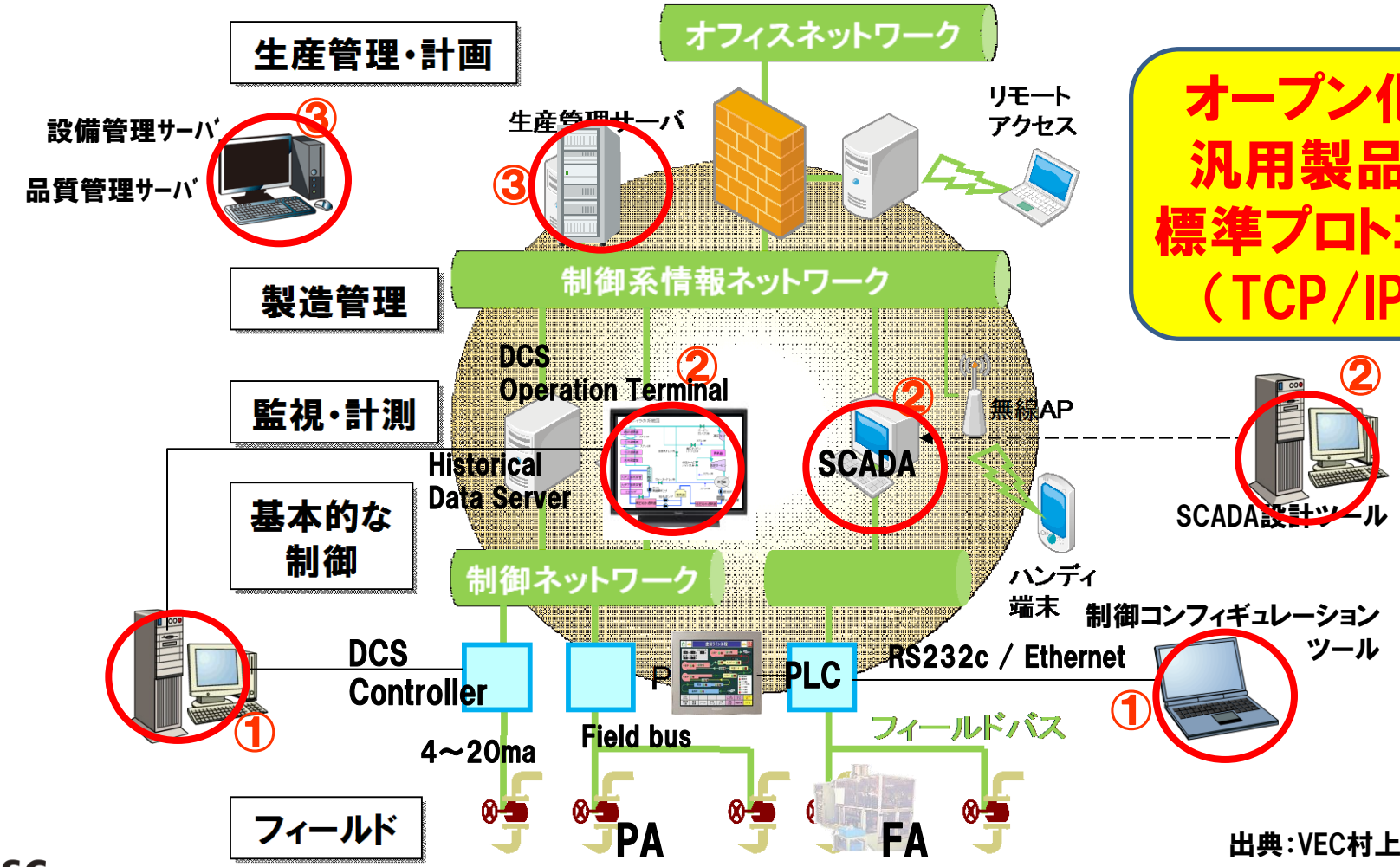
このウイルスの目的は、イランの核施設における遠心分離機を破壊することであり、そのため、遠心分離機の回転速度に関わる制御システムに特定のコマンドを出したという。

http://wired.jp/2012/06/04/confirmed-us-israel-created-stuxnet-lost-control-of-it/

制御システムへのサイバー攻撃の対象例

攻撃目的：装置や設備の破壊、悪品質製品生産や生産の暴走、装置ベンダの信頼失墜等

攻撃ターゲット⇒



オープン化：汎用製品と標準プロトコル（TCP/IP）

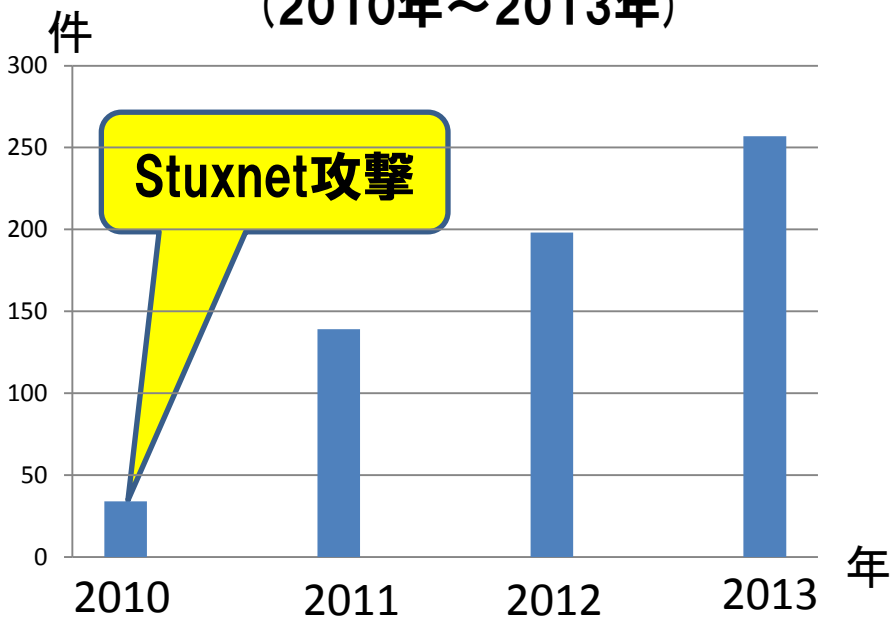
出典：VEC村上氏

制御システム「セキュリティインシデント」増加

- 米国ICS-CERT：2009年に設置以降、インシデント届出件数が飛躍的に増大
- エネルギー、水道、原子力、化学、政府関連設備など、届出が多い

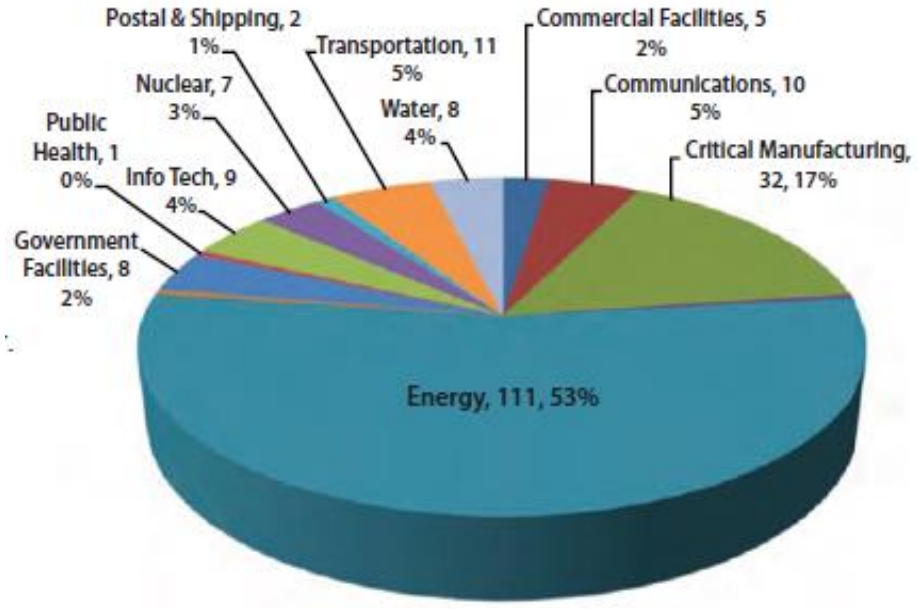
ICS－CERT：Industrial Control Systems － Cyber Emergency Response Team

ICS-CERTのインシデント報告傾向（2010年～2013年）



2013.11@ICSJWG

分野別インシデント報告割合（2013年）



ICS-CERT Monitor Newsletters April-June 2013
http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Apr-Jun2013.pdf

ICS-CERTウェブサイト、ICSJWG2013Fall情報をもとに作成

サイバー攻撃者に対する防護ハードルを高くしよう！

社会インフラ事業者やシステムを提供・運用する事業者

DSD: Defense Signals Directorate

1．サイバー攻撃のリスクを低減する4つの対策実施（オーストラリアDSD, NIST）

①アプリケーションに対するホワイトリスティング（Whitelisting）適用
②アプリケーションの脆弱性対策パッチ適用　pdfやwordなど
③基本ソフトOSの脆弱性対策パッチ適用　ネットワーク機器も
④特権ユーザの数を最小にする

既知の脆弱性を利用した攻撃が75％

上記の対策で85％以上のリスク低減が実現できた。

2．継続的な監視（Continuous Monitoring）によるリスク低減

①ネットワーク状態やシステムログの継続的監視：デジタルに加えアナログ情報
②正常・通常状態との差分の継続的監視：SIEM技術の拡張

3．標準準拠・認証された製品やシステムの利用

守るカギが多いと攻撃者は時間がかかる。
ただしコストとの関係も。

2. 制御システムセキュリティセンターの紹介

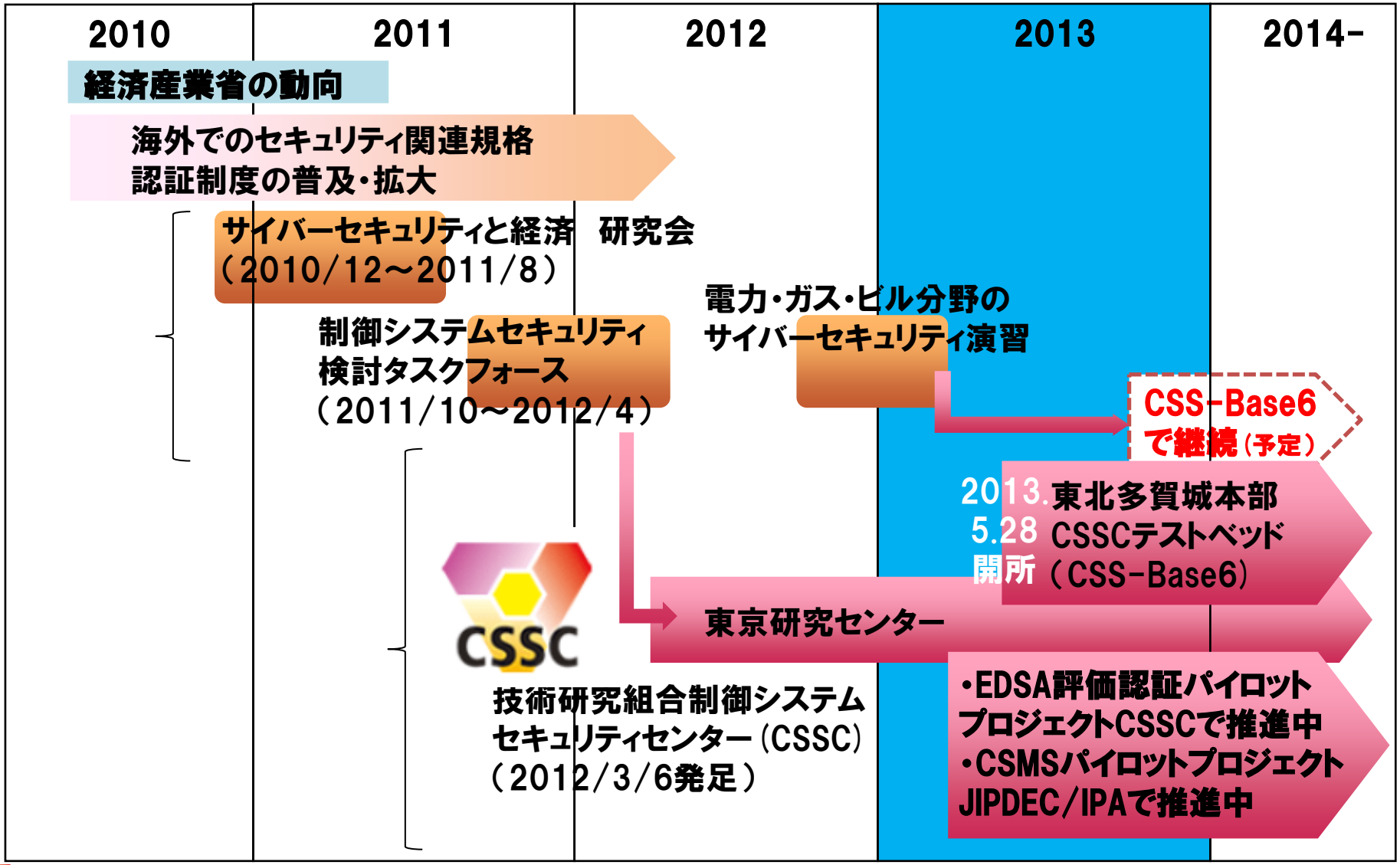
CSSC: Control System Security Center

＜ビデオ＞約10分

東京都心で大規模な停電が発生したら・・・

CSSCの紹介

制御システムセキュリティへの日本の取組み状況とCSSC



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）

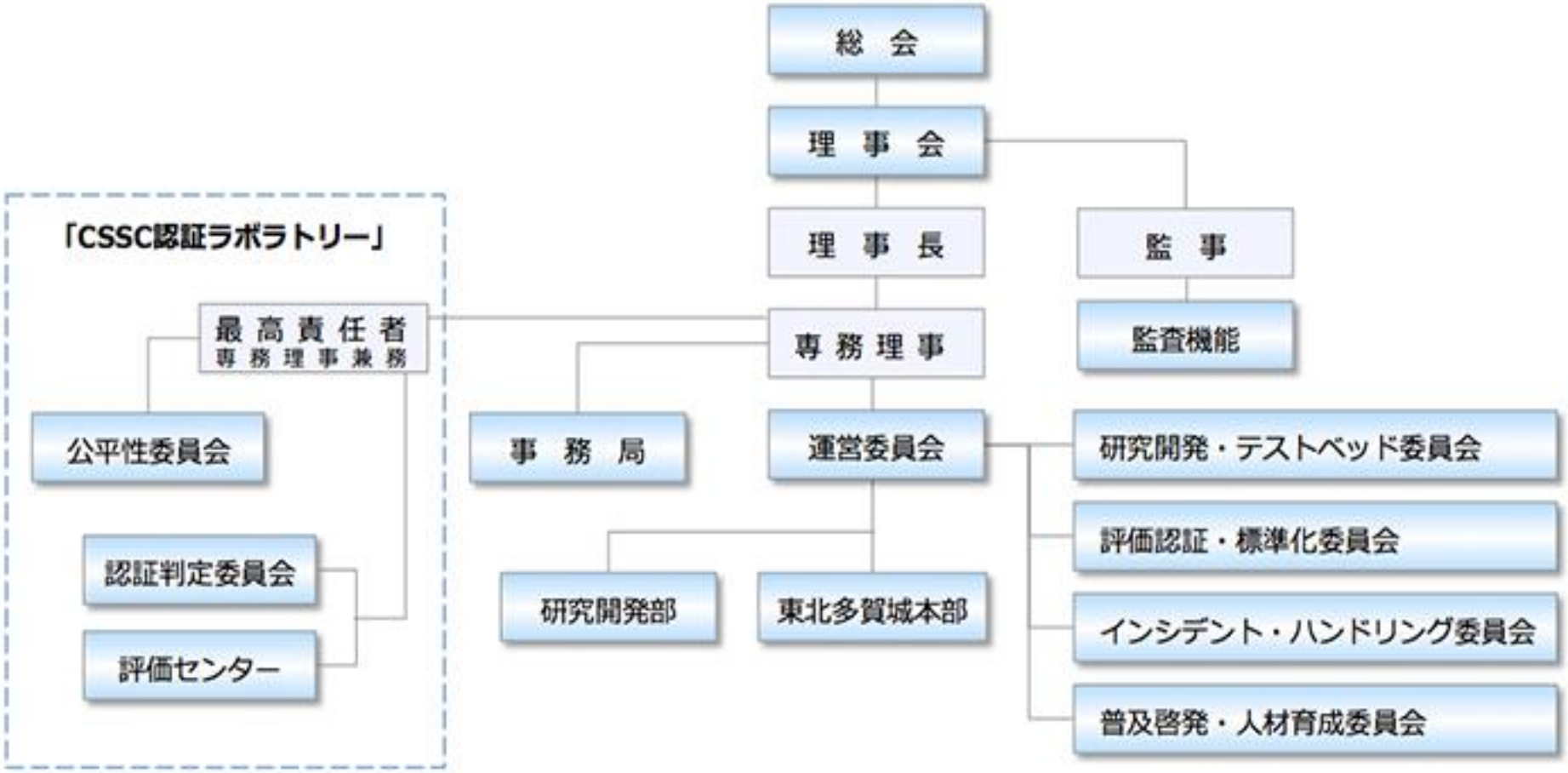
独立行政法人
産業技術総合研究所
情報処理推進機構

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21社（2013年11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、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*
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



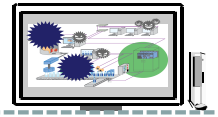
20130801現在

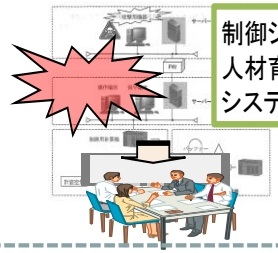
CSSCの研究開発の概要

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

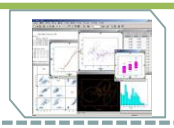
制御システム向け軽量暗号認証技術

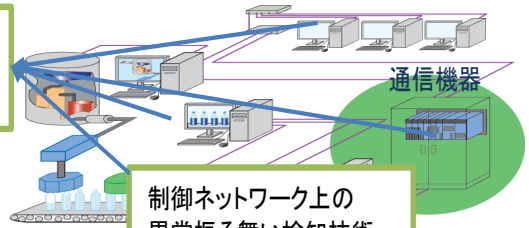
仮想環境における高セキュア制御システム構築技術

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





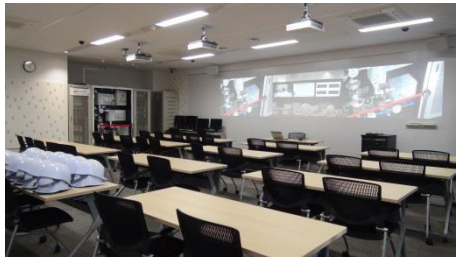
制御ネットワーク上の異常振る舞い検知技術

テストベッド（CSS-Base6）の7つの模擬プラントシステム

■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。

■2013年5月時点では、下記の7種類の模擬システムが稼働中。

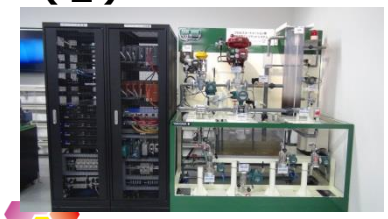
（7）



（１）排水・下水プラント
（２）ビル制御システム
（３）組立プラント
（４）火力発電所訓練シミュレータ
（５）ガスプラント
（６）広域制御（スマートシティ）
（７）化学プラント

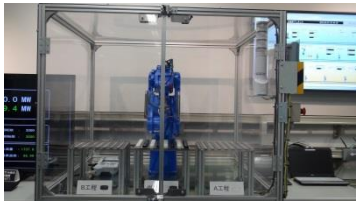
（４）

（１）



（２）

（３）



（５）

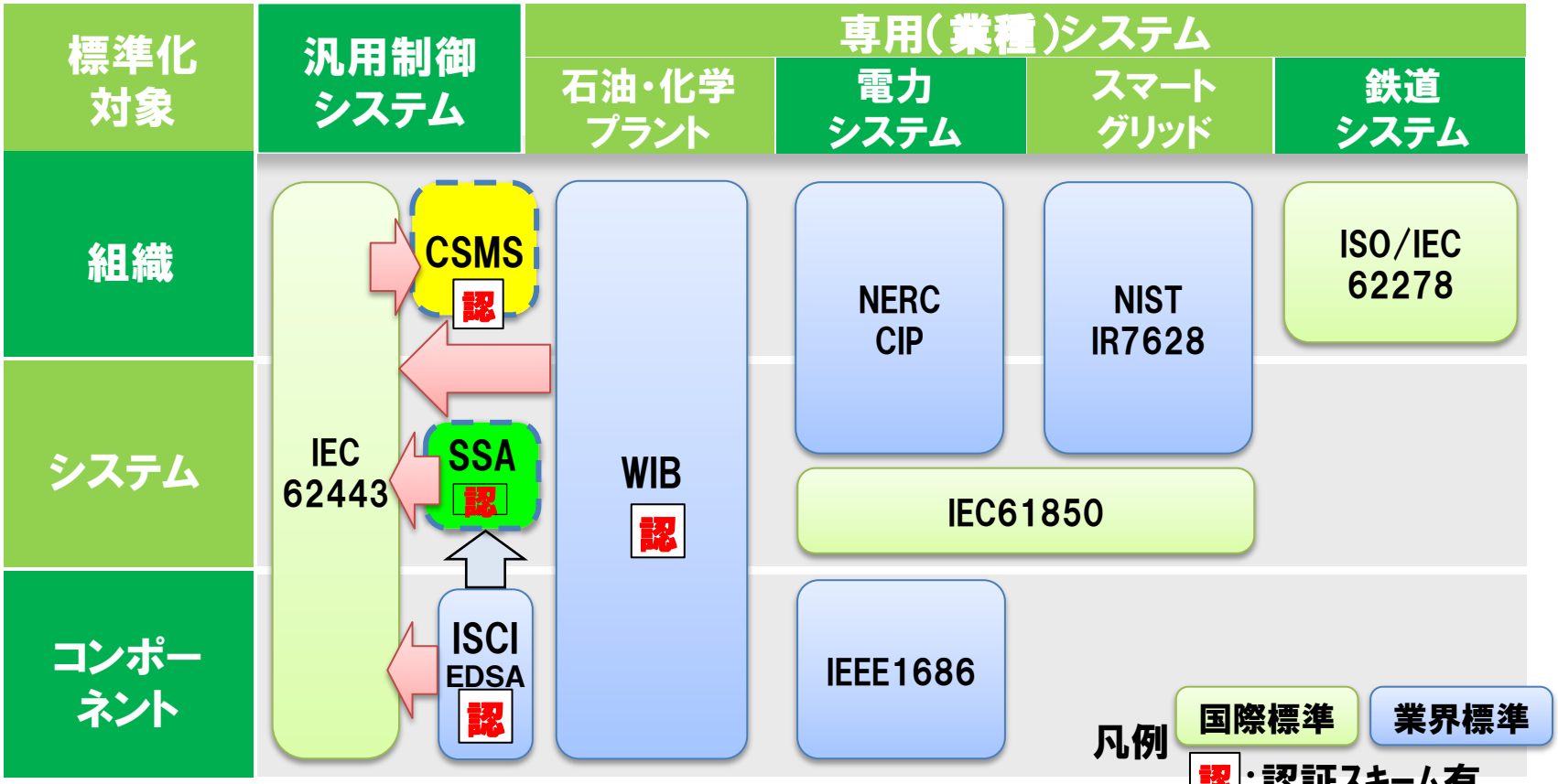
（６）

3. IEC62443の概要と認証について
～制御システムの認証への取り組み～

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技術動向

■制御システムのセキュリティの標準・基準には、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・基準が提案されている。
■こうした中で、汎用的な標準・基準として、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の基準が、IEC62443のシリーズに統合される動きとなっている。



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標準(EDSA認証等)がIEC62443に採用される方向

標準化 *1)

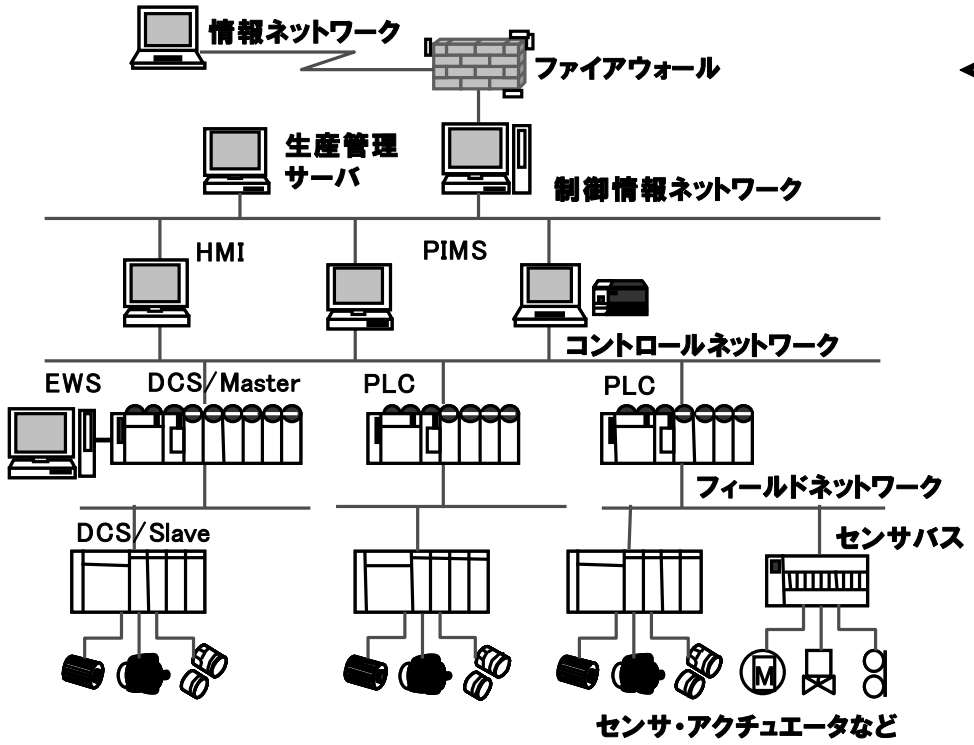
事業者
インテグレータ
装置ベンダ

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

IEC62443標準化状況と評価・認証の状況

■12の標準中、3つが標準化済みだが、他の標準については、国内意見の反映を推進

■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

区分	主対象者	IEC	原本名	現状のステータス ドキュメントの状況，ドラフトの現状	リリース・予定 （2012.3時点）	頁数	概要
共通	全体	62443-1-1	Terminology, concepts and models	発行済み，アップデート中	2009.07	81	用語
		62443-1-2	Master glossary of terms and abbreviations	テクニカルレポートとしてレビュー			
		62443-1-3	System security compliance metrics	ドラフト執筆中	DTR:2013.02		
セキュリティプログラム	事業・運用者	62443-2-1	Establishing an IACS security program	発行済み，アップデート中	2010.10 Ed.2:CDVは2012Q4	159	＜事業者自体のセキュリティマネージメントシステム構築＞ ISMS（ISO27001）の制御システム版
		62443-2-2	Operating an IACS security program	ドラフト執筆中	CDV:2013Q1		
		62443-2-3	Patch management in the IACS environment	ドラフト執筆中	DTR:2012Q3		
		62443-2-4	Certification of IACS supplier security policies and practices	レビュー中	CDV:2011.10	42	＜要達
システム	構築事業者	62443-3-1	Security technologies for IACS	発行済み	2009.07		
		62443-3-2	Security assurance levels for zones and conduits	ドラフト執筆	2013.02		
		62443-3-3	System security requirements security assurance levels	ドラフトが75%完成済み	CDV:2012Q1		システムに対するセキュリティ要件。保証レベル（3段階）での要件集。
部品	装置ベンダ	62443-4-1	Product development requirements	ドラフト執筆中	CDV:2013Q1		セキュアなコンポーネントを開発するための方法を規定。 ISASecureのEDSA（SDSA）をベースにしている。
		62443-4-2	Technical security requirements for IACS components	ドラフト執筆中	CDV:2013Q1		デバイス、システムに搭載されるセキュリティ機能を規定。 ISASecureのEDSA（FSA）をベースにしている。

②CSMS認証
（Cyber Security Management System）

①EDSA認証
（Embedded Device Security Assurance）

IEC: International Electrotechnical Commision
IACS: Industrial Automation and Control
CD：Committee Draft 、CDV：Committee Draft for Vote、DC：Document for Comments
DTR: Draft Technical Report 、NP：New Work Item Proposal 、RR:Review Report
ISA: International Society of Automation
WIB: International Instrument User's Associations

制御システムセキュリティの評価・認証の動向

- 民間組織が主体の認証スキーム
  - ◆ドイツTUViT社
    - Trusted Site Security SCADA Infrastructure
  - ◆オランダWIB(International Instrument Users' Association)
  - ◆カナダWurldtech社
    - Achilles

- 国際制御学会ISAとその下部の認証フレームワーク推進組織ISCIが主体の制御機器認証スキームが拡大
  - –ISCI(ISA Security Compliance Institute)
    - ◆ISASecure認証：**EDSA**

（ **E**mbedded **D**evice **S**ecurity **A**ssurance ）

国際標準(IEC62443)への組込みが見込まれており、
認証のスキームも綿密に組み立てられているため、
今後拡大してゆく可能性大

ISA Security Compliance Institute （ISCI）とは

組織

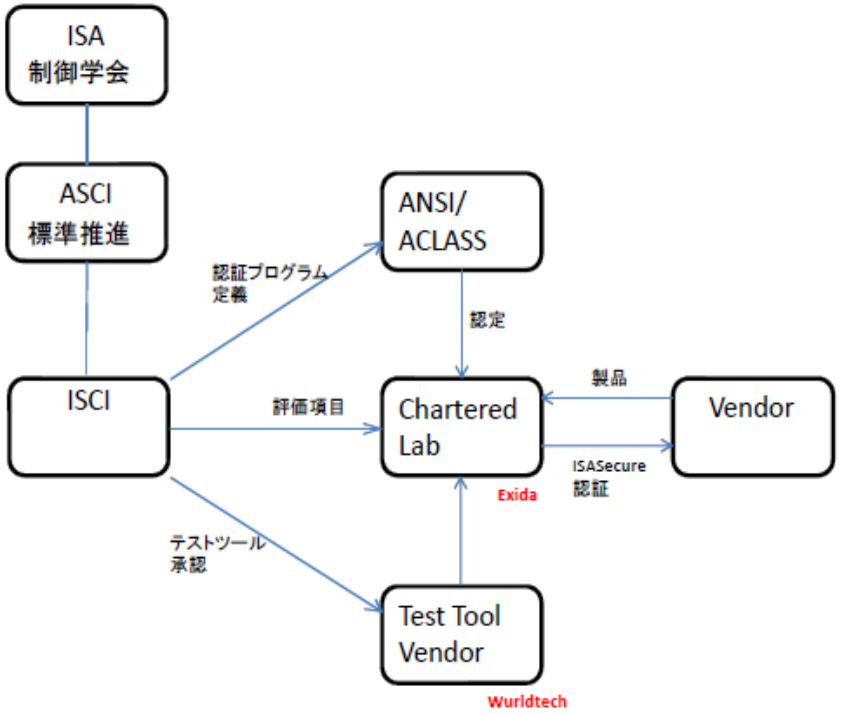
●アセットオーナー（制御システム事業者）、サプライヤ、及び業界組織からなるコンソーシアムでISA Automation Standards Compliance Institute(ASCI)内に2007年に構築された。

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

①Strategic Member： Chevron、ExxonMobil、Honeywell、Invensys、Siemens、Yokogawa
Voting有 年会費50000ドル
②Technical Member： Exida、RTP Corporation
Voting有 年会費5000ドルから25000ドル
③Associate Member： 現在加入組織無（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
Voting 無 年会費1500ドル

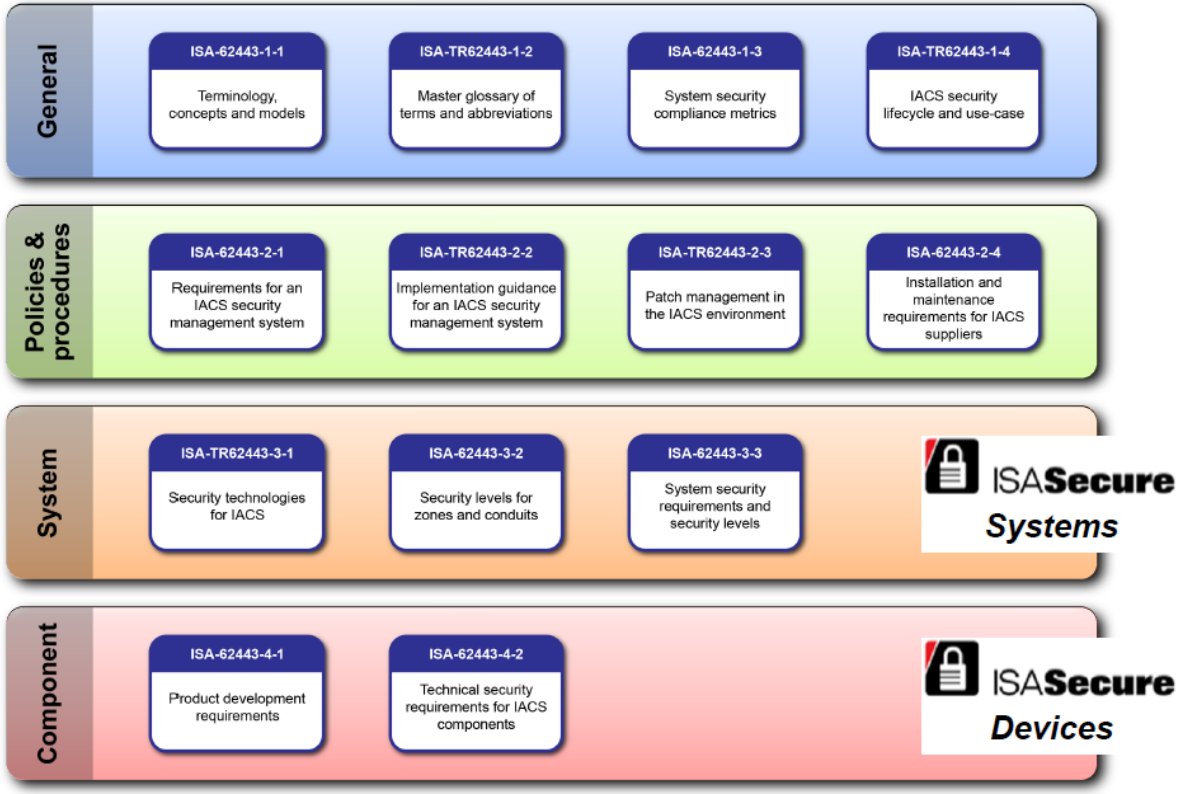
CSSCは、ISCIに加入予定。

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
等がある。特にSSAの早期仕様入手が来年度以降の活動の検討に必要となってきている。

ISCIのISASecure認証標準進捗状況

ISCIは、ISASecureの認証標準を制定している組織である。現在ISASecure の第1弾としてEDSA認証の標準を提供している。制御システム事業者、サプライヤ(制御システム構築事業者、装置ベンダ) 等からなるコンソーシアム。

ISA99　62443 (=IEC62443) 標準化状況とISASecureの関係



SSA とSDLAは現在開発中

ISASecureは3つの認証標準
（現在EDSA認証が標準済）

ISASecure™ System Security Assurance (SSA)
ISASecure™ Embedded Device Security Assurance (EDSA)
ISASecure™ Security Development Lifecycle Assurance (SDLA)

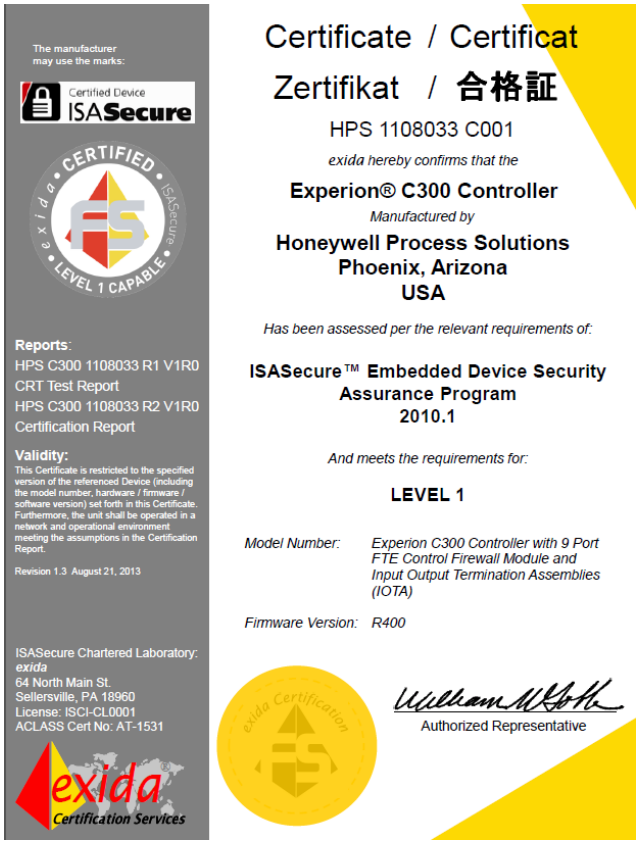
ISCI ： ISA Security Compliance Institute
ISA ： International Society of Automation国際計測制御学会
PCLS: Provisional Chartered Laboratory Status 仮免状態

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

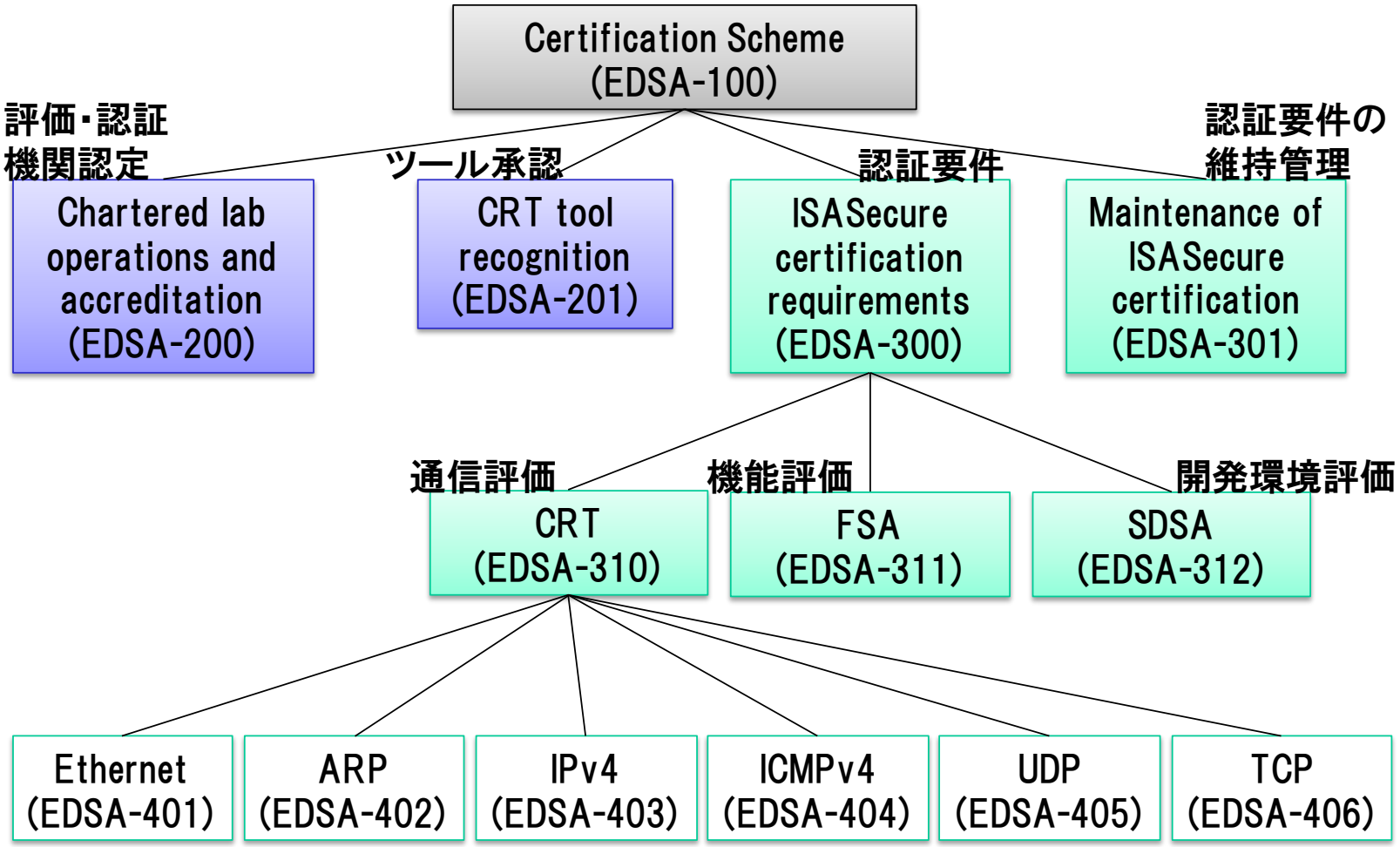
EDSA製品認証の最新動向

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

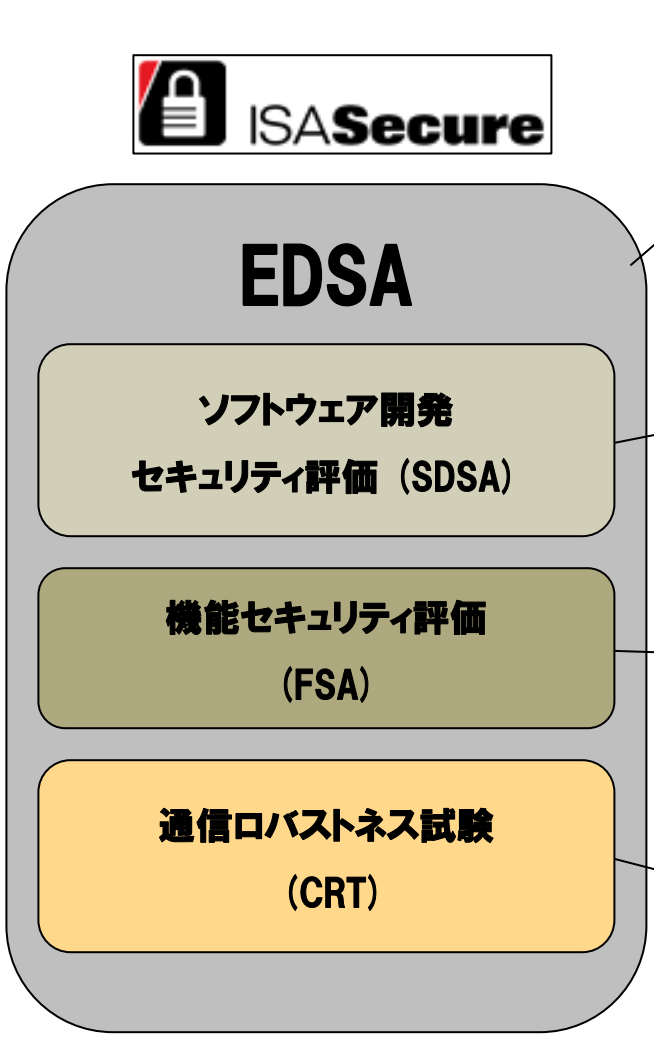


EDSA標準のドキュメント体系



◇ 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



◆SDSA、FSA、CRTの3つを評価することで、想定脅威に対する対策のカバー範囲が十分であることを認証

体系的な設計不良の検出と回避

- ベンダのソフトウェア開発とメンテナンスのプロセス監査
- 堅牢（robust）で,セキュアなソフトウェア開発プロセスを当該組織が守っていることを評価する。

※3段階のセキュリティレベルにより評価項目数が決まる

実装エラー / 実装漏れの検出

- セキュリティ機能要件について、目標とするセキュリティレベルに対応する全要件が実装済みであるかどうかを評価

※3段階のセキュリティレベルにより評価項目数が決まる

デバイスの堅牢性を評価する試験

- コンポーネントのロバストネス（堅牢性）について試験
- 奇形や無効な形式のメッセージを送り、脆弱性等を分析

※セキュリティレベルによらず、評価項目数は同一

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

ソフトウェア開発セキュリティ評価（SDSA）

目的: ソフトウェア開発プロセスがセキュア（脆弱性を作り込まないよう）に行われていることを監査する

構成

- Set of requirements, derived from existing reference standards and traceable to source standard (IEC 61508, ISO/IEC 15408)

SDSAの主な参照標準

ISO/IEC 15408-1 ～ I5408-3	情報技術 - セキュリティ技術 - ITセキュリティ評価基準 Part1～Part3
IEC 61508 Part 3	電気/電子/プログラマブル電子的安全関連システムの機能安全：ソフトウェア開発

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

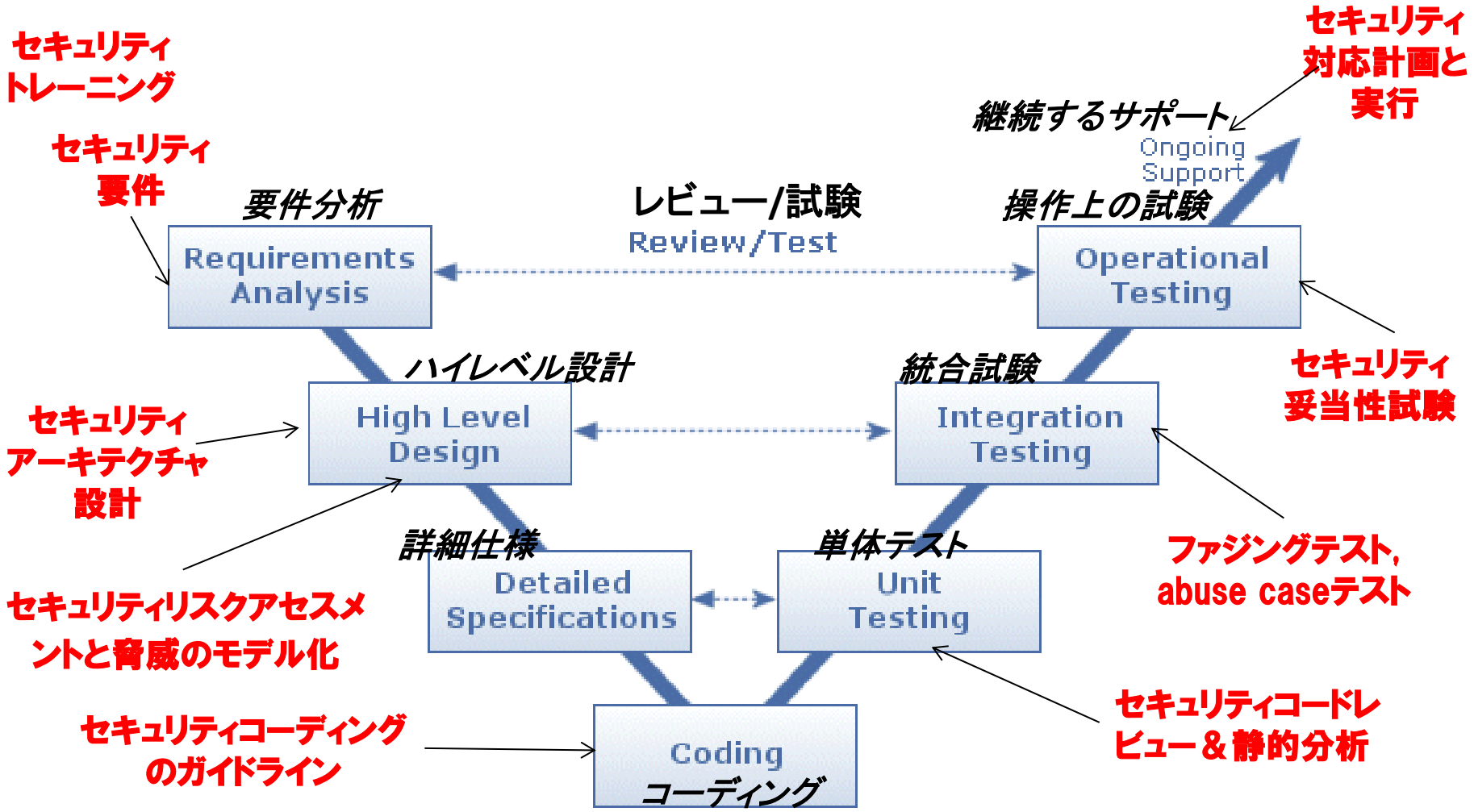
SDSAの主な要求事項

セキュリティマネジメントプロセス	This phase specifies a process for planning and managing security development activities to ensure that security is designed into a product. For example, this phase incorporates requirements that the development team have a security management plan and that the developers assigned to the project are competent and have been provided basic training in good security engineering practices and processes. Also includes requirements that the project team creates and follows a configuration management plan.
セキュリティ要件仕様	Most vulnerabilities and weaknesses in software intensive information systems can be traced to inadequate or incomplete requirements. This phase requires that the project team document customer driven security requirements, security features and the potential threats that drive the need for these features.
ソフトウェアアーキテクチャ設計	Software architecture facilitates communication between stakeholders, documents early decisions about high-level design, and allows reuse of design components and patterns between projects. This phase requires the project team develop a top-level software design and ensures that security is included in the design.
セキュリティリスクアセスメントと脅威モデリング	This phase requires the project team determine which components can affect security and plan which components will require security code reviews and security testing. Also requires that a threat model be created and documented for the product.
詳細ソフトウェア設計	This phase requires the project team design the software down to the module level following security design best practices.
セキュリティ指針の文書化	This phase requires the project team create guidelines that users of the product must follow to ensure security requirements are met.
ソフトウェアモジュール実装と検証	This phase requires the project team implement design by writing code following security coding guidelines. It ensures that software modules are implemented correctly by conducting security code reviews, static analysis and module testing.
セキュリティ統合試験	This phase requires that the project team perform security specific tests such as fuzz testing and penetration testing.
セキュリティプロセス実証	This phase requires an independent assessment that all required software development processes have been followed
セキュリティレスポンス計画	This phase requires the project team establish a process to be able to quickly respond to security issues found in the field if and when they happen.
セキュリティ実証試験	This phase requires that the project team confirm that all security requirements have been met preferably by test or by analysis.
セキュリティレスポンス実行	This phase requires the project team respond to security problems in the field by taking action to both preventative and corrective action.

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

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モデルにセキュリティを組み込まれていることを監査する



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

機能セキュリティ評価（FSA）

目的:

- **製品の機能が一定の要求事項を満たしているかを監査する**

構成:

- **既存の参照規格で、且つ出典元の規格にトレース可能な要件**
- **各要件に対して識別された1個以上の容認可能な解決策(対抗策)**
- **適用可能なときは,要件検証手順が満たされている。**
  - ＊適用可能とは、要求事項でアロケータブルとなっている(allocation が Yesとなっている）場合、その機能をデバイス以外のもので実現してもよい、ということを示す

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

FSAの主な参照標準

[N1]	ISA-99.01.03D2-20090527	産業自動制御システム向けセキュリティ：システムセキュリティ要件とセキュリティ保証レベルISA-99.01.03
[N2]	NERC 規格 CIP-001-1 ～ CIP-001-9	North American Electric Reliability Council Cyber Security Standards
[N3]	NIST 800-53	連邦情報システムのための推奨されたセキュリティ制御 Recommended Security Controls for Federal Information Systems
[N4]	ISO/IEC 15408-1 ～ I5408-3	情報技術 - セキュリティ技術 - ITセキュリティ評価基準 - Part1～Part3
[N5]		国土安全保障省：制御システムセキュリティのカタログ：標準策定者のための推奨事項 Department of Homeland Security: Catalog of Control Systems Security: Recommendations for Standards Developers

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

FSAの主な要求事項

アクセス制御	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
使用制御	デバイス認証、監査証跡 Device authentication, audit trail
データ完全性	転送中のデータ、保管中のデータ Data in transit, data at rest
データ機密性	転送中のデータ,保管中のデータ,暗号化 Data in transit, data at rest, crypto
データのフロー制限	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
イベントへの迅速な応答	インシデント応答 Incident response
ネットワークリソース有用性	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

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

通信ロバストネス試験（CRT）

- 組込み機器へのネットワークプロトコル実装が,ネットワークから受信した異常な又は意図的な悪意のトラフィックに対して,自分自身及び他のデバイス機能を防御する程度を測定する。

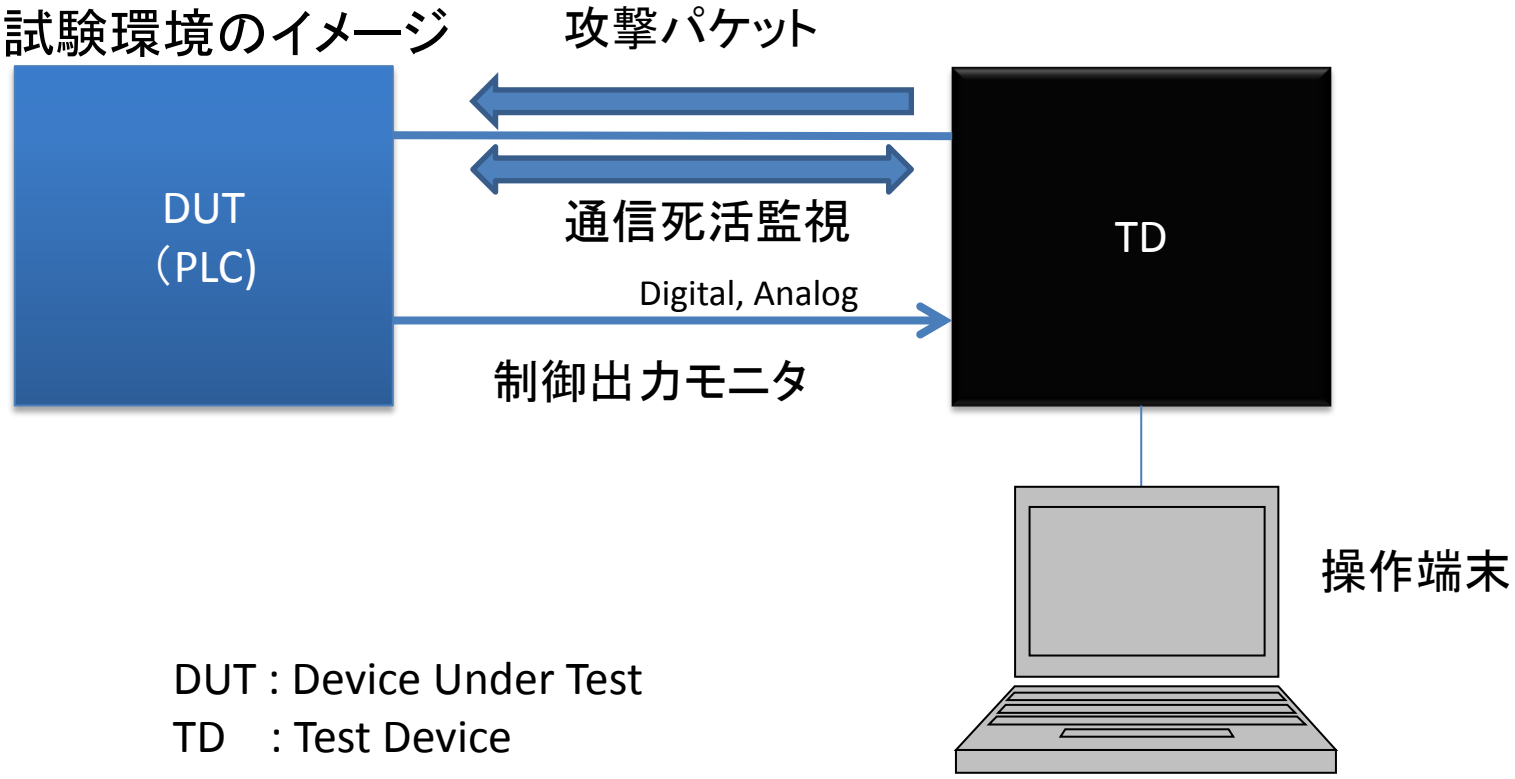
- 不適切なメッセージ応答,又はデバイスが重要サービスを適切に実行継続できないと,デバイス内部の潜在的なセキュリティ脆弱性の存在を示している。

- **共通 CRT 要件** (EDSA-310)
  - ●Ethernet (EDSA-401)
  - ●IPv4 (EDSA-403)
  - ●ICMP (EDSA-404)
  - ●ARP (EDSA-402)
  - ●TCP (EDSA-406)
  - ●UDP (EDSA-405)

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

CRT試験の実施方法

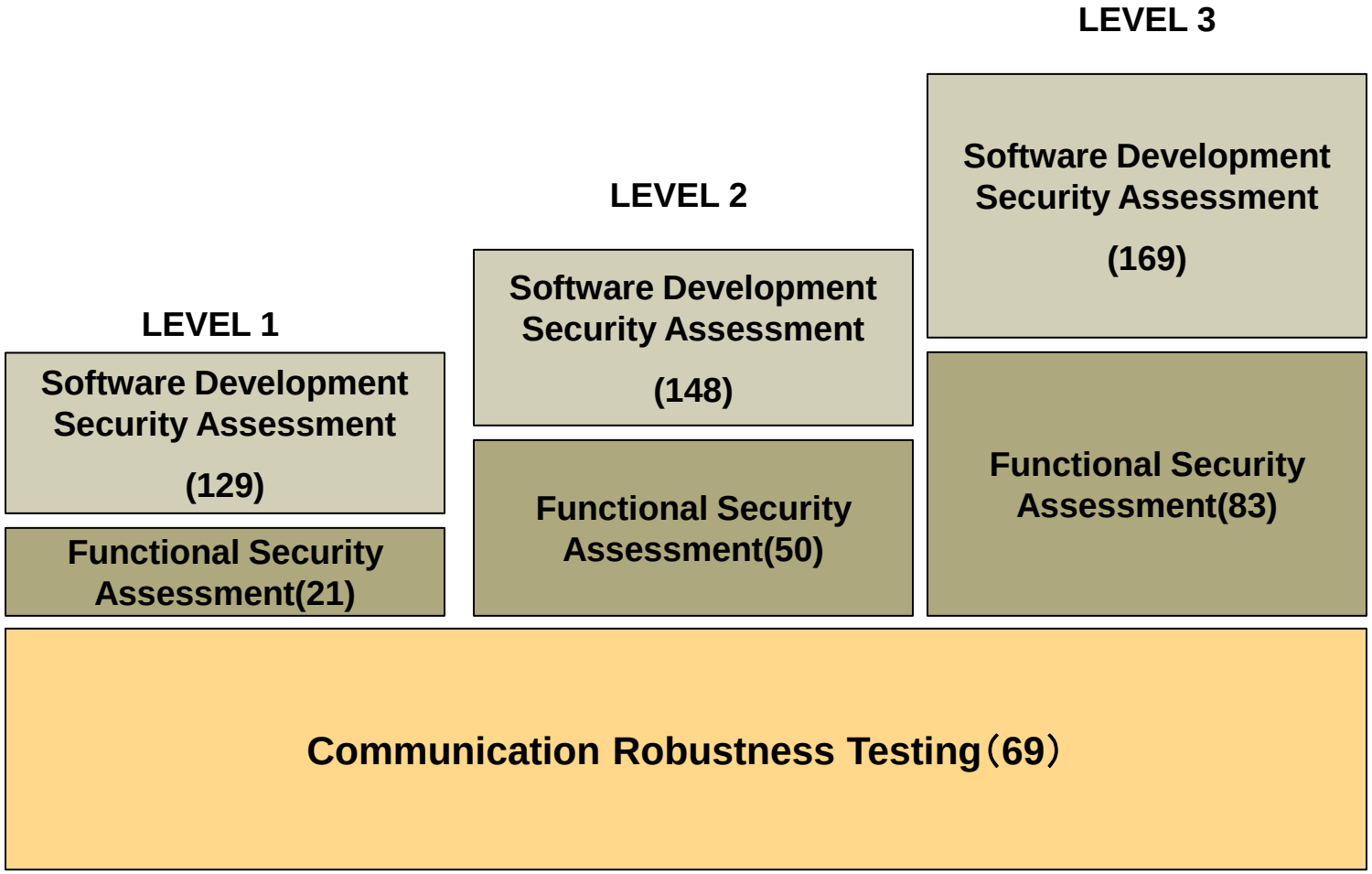
- ISCIの認定(承認)ツールを使う
  （現在はAchillesとdefensicsが認定ツール。現在、他のツールも認定中。）
- コントローラだけではなく、事実上HMI側の用意も必要
  （Achilles認証とは違う）
- 試験環境のイメージ



DUT : Device Under Test
TD　: Test Device

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

EDSA Certification Process

Typical Chartered Lab Level of Effort in Man Weeks

	Level 1	Level 2	Level 3
1. CRT test all accessible TCP/IP interfaces	1 - 2 weeks	1 - 2 weeks	1 - 2 weeks
2. Perform FSA on device and all interfaces	< 1 week	1 week	1 – 2 weeks
3. Audit supplier's software development process	1 week	1 – 2 weeks	1 – 2 weeks
4. Perform ITA and issue report	1 week	1 week	1 week
	3 – 5 weeks	4 – 6 weeks	4 – 10 weeks

ITA : Integrated Threat Analysis (統合脅威分析)

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

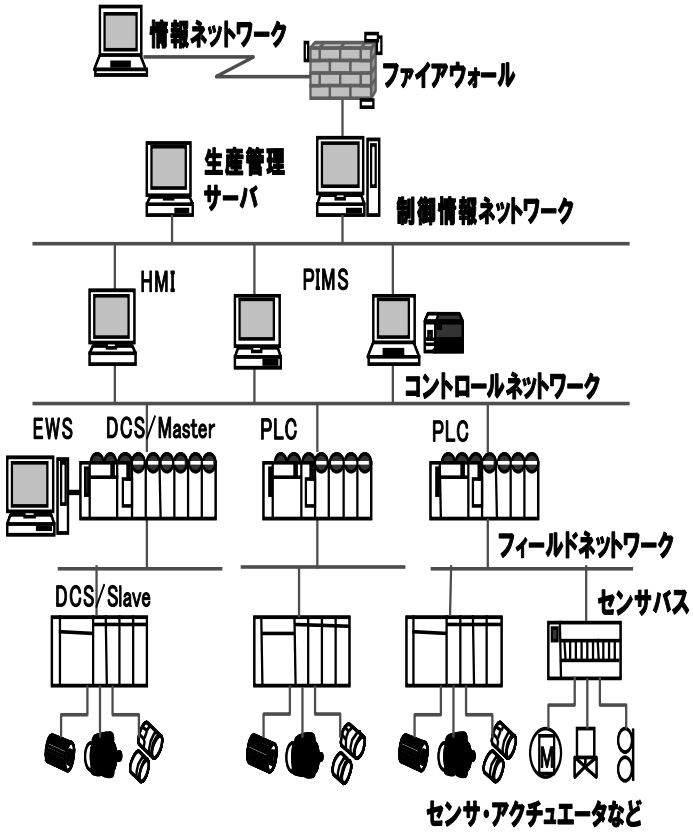
EDSA規格とIEC62443の対応関係

EDSAの「SDSA」、「FSA」
の要求事項がほぼ同内容で
IEC62443-4-1、
IEC62443-4-2
へそれぞれ提案されている

EDSA認証

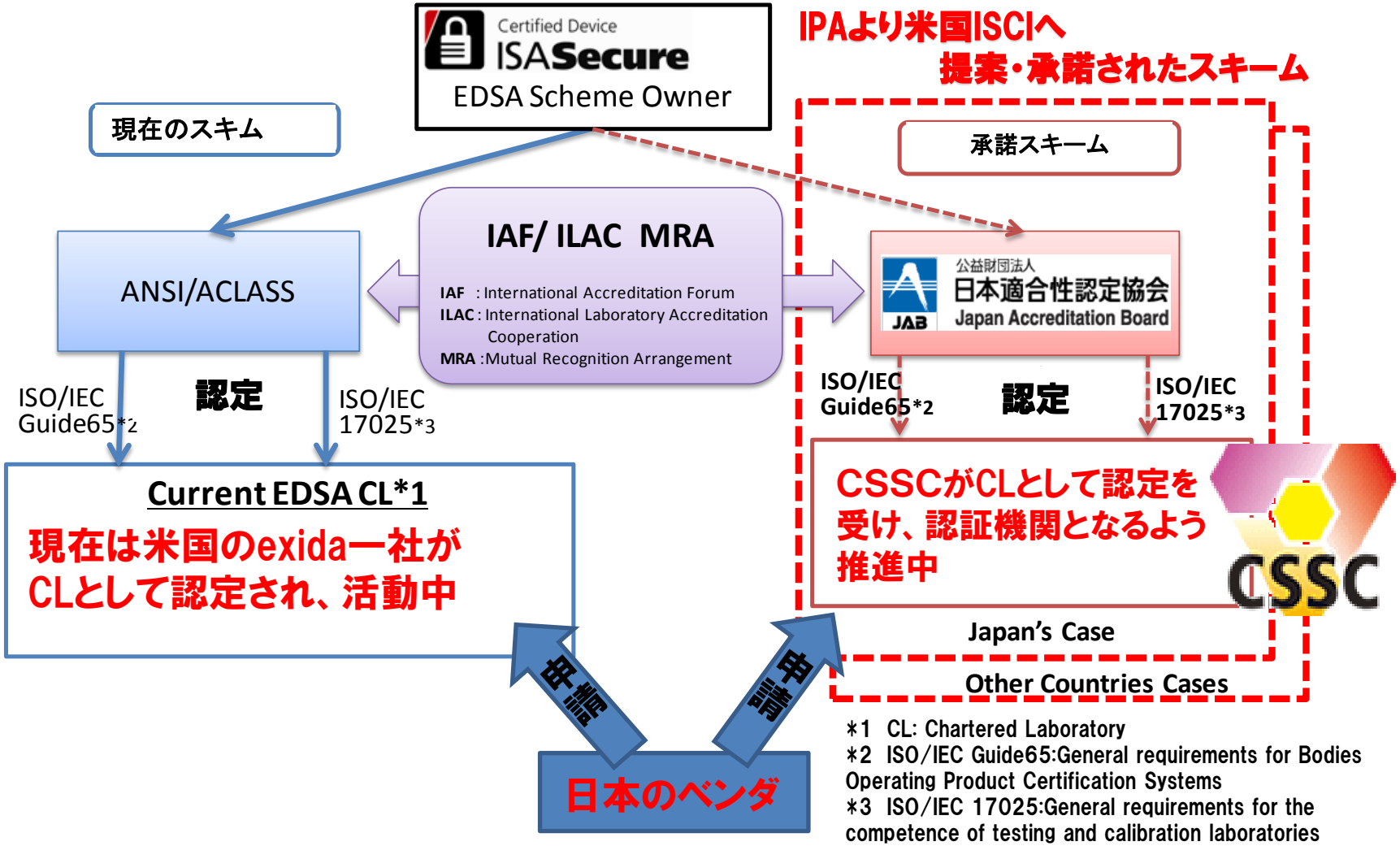
- Software Development Security Assessment(SDSA)
- Functional Security Assessment(FSA)
- Communications Robustness Testing(CRT)

IEC	主対象者	区分
62443-2-1	事業・運用者	セキュリティプログラム
62443-2-2		
62443-2-3		
62443-2-4		
62443-3-1	構築事業者・SIer	システム
62443-3-2		
62443-3-3		
62443-4-1	装置ベンダ	部品
62443-4-2		



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

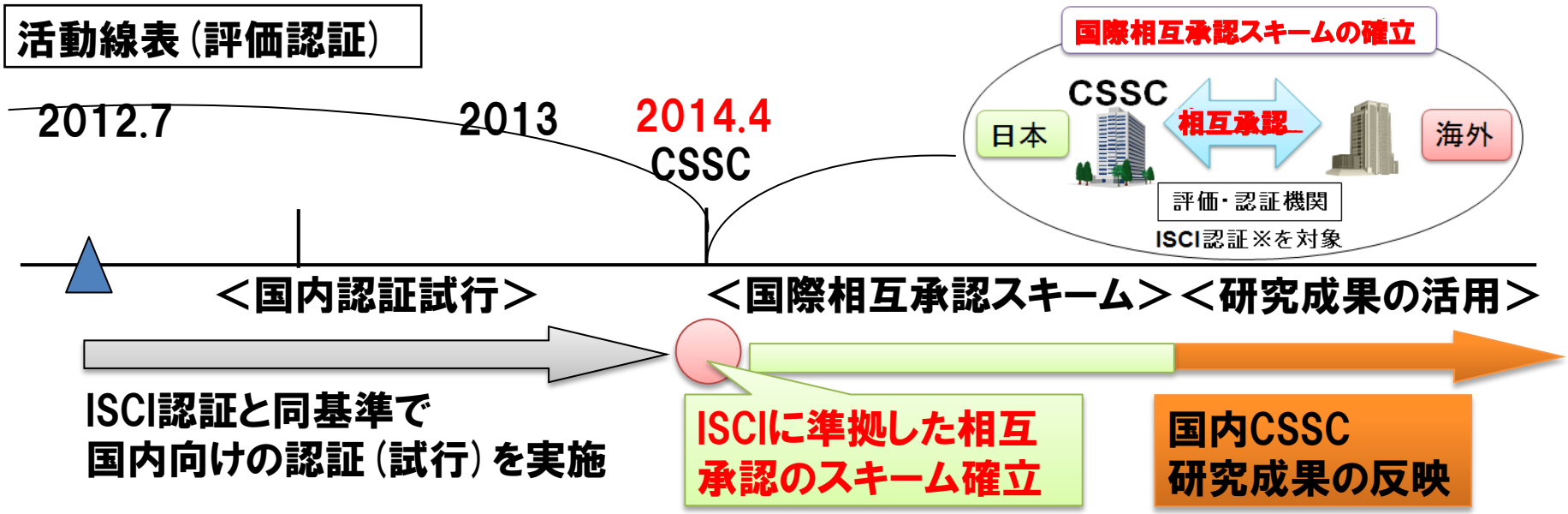


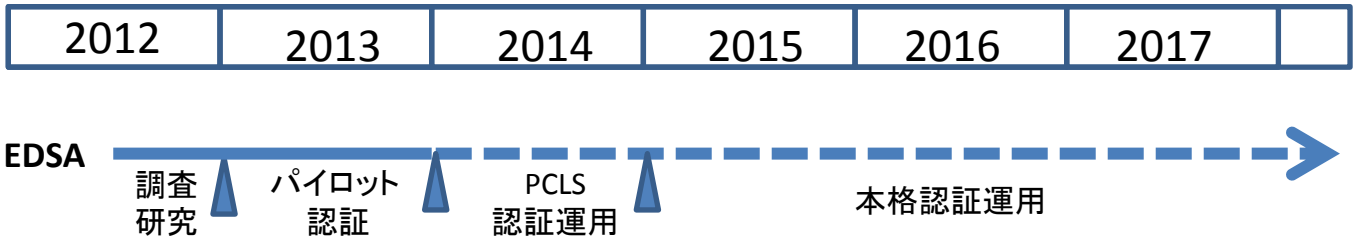
*1 CL: Chartered Laboratory
*2 ISO/IEC Guide65:General requirements for Bodies Operating Product Certification Systems
*3 ISO/IEC 17025:General requirements for the competence of testing and calibration laboratories
*4 CSSC:Control System Security Center

CSSCのISASecure認証制度への取り組み（EDSAから）

**制御システムのセキュリティに関する評価認証の国際相互承認のスキーム確立。
今後の取組みについては下記の線表を予定。**

活動線表（評価認証）



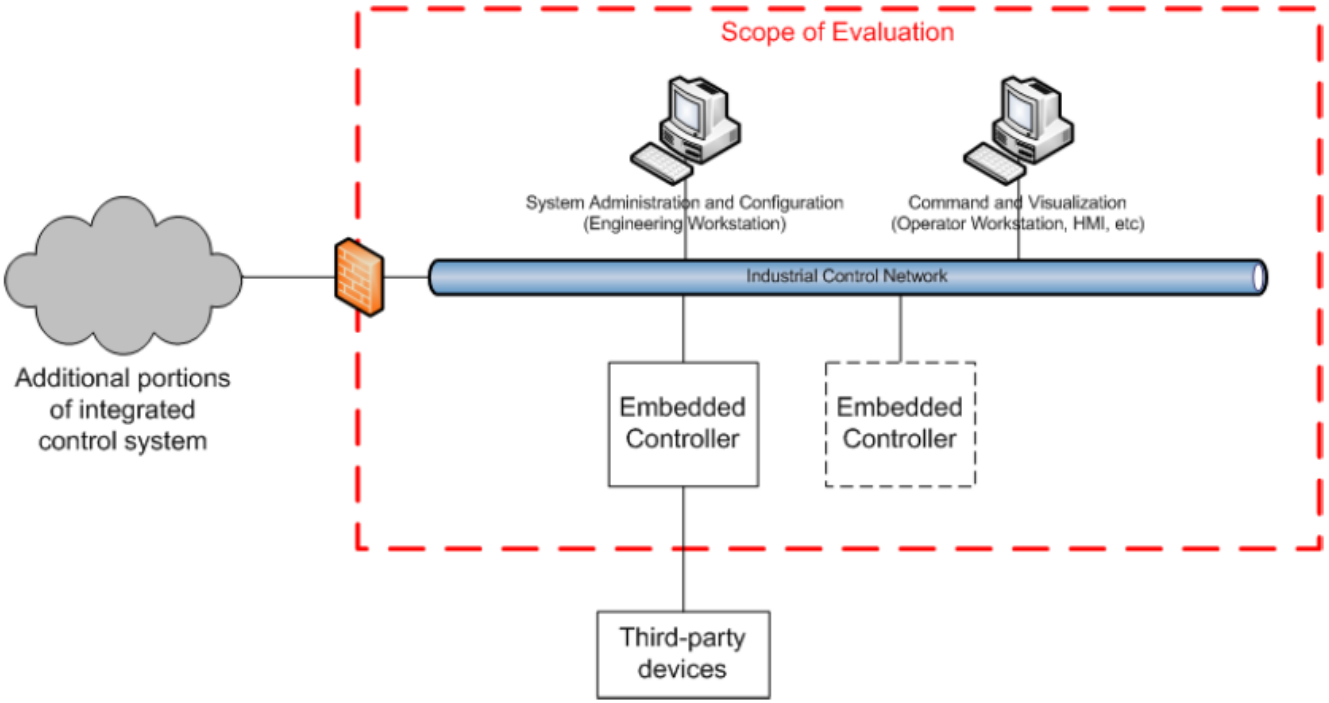


ISCIの規格化状況に基づき、CSSCの対応計画案を示す。実線は計画済で、実施中のもの。年度表記。

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システム認証の最新動向

システムとは？

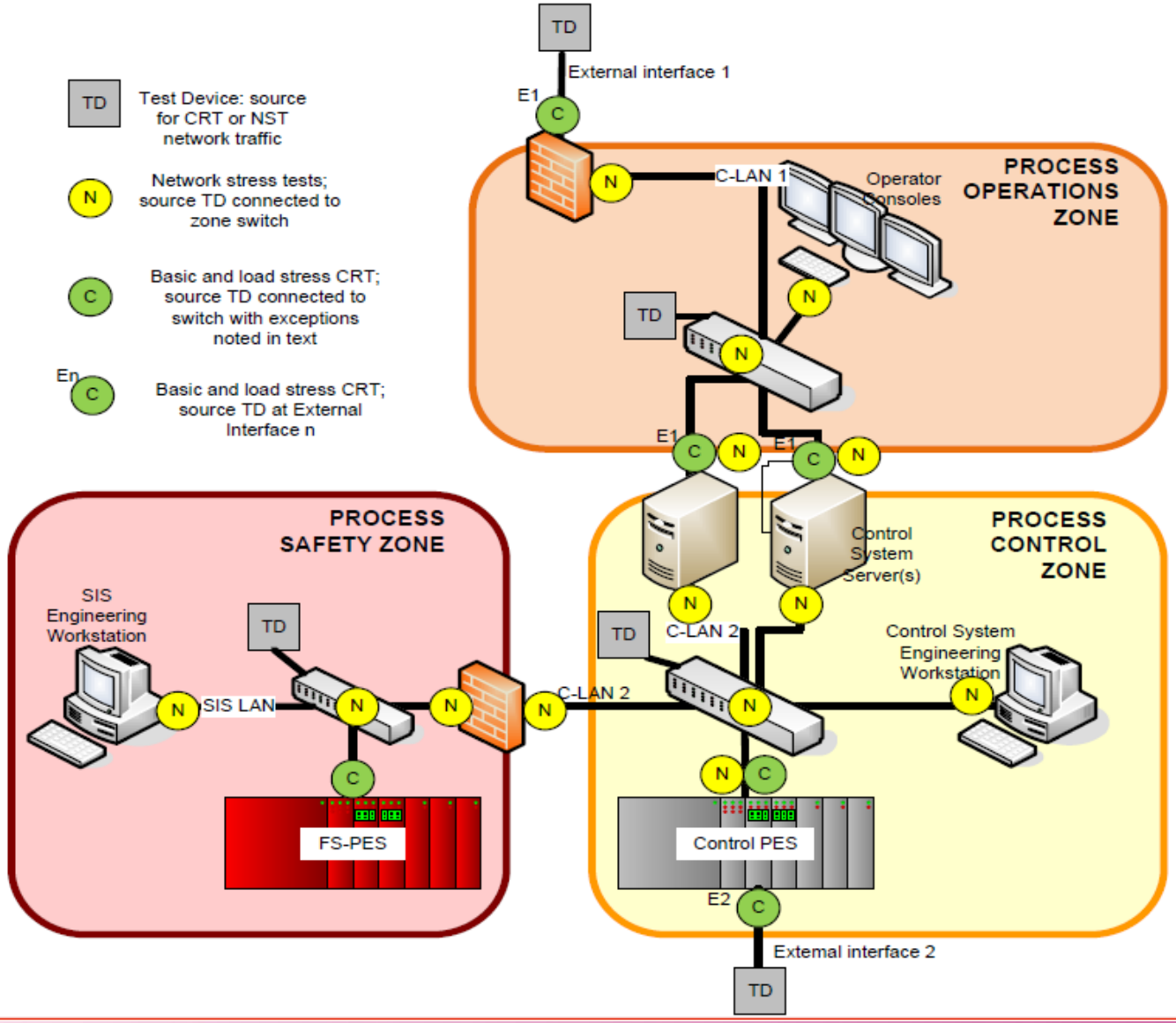


- An Industrial Control System (ICS) or SCADA system
  that is available from a single system supplier
- It may be comprised of hardware and software components from several manufacturers
  but must be integrated into a single system and supported, as a whole, by a single supplier

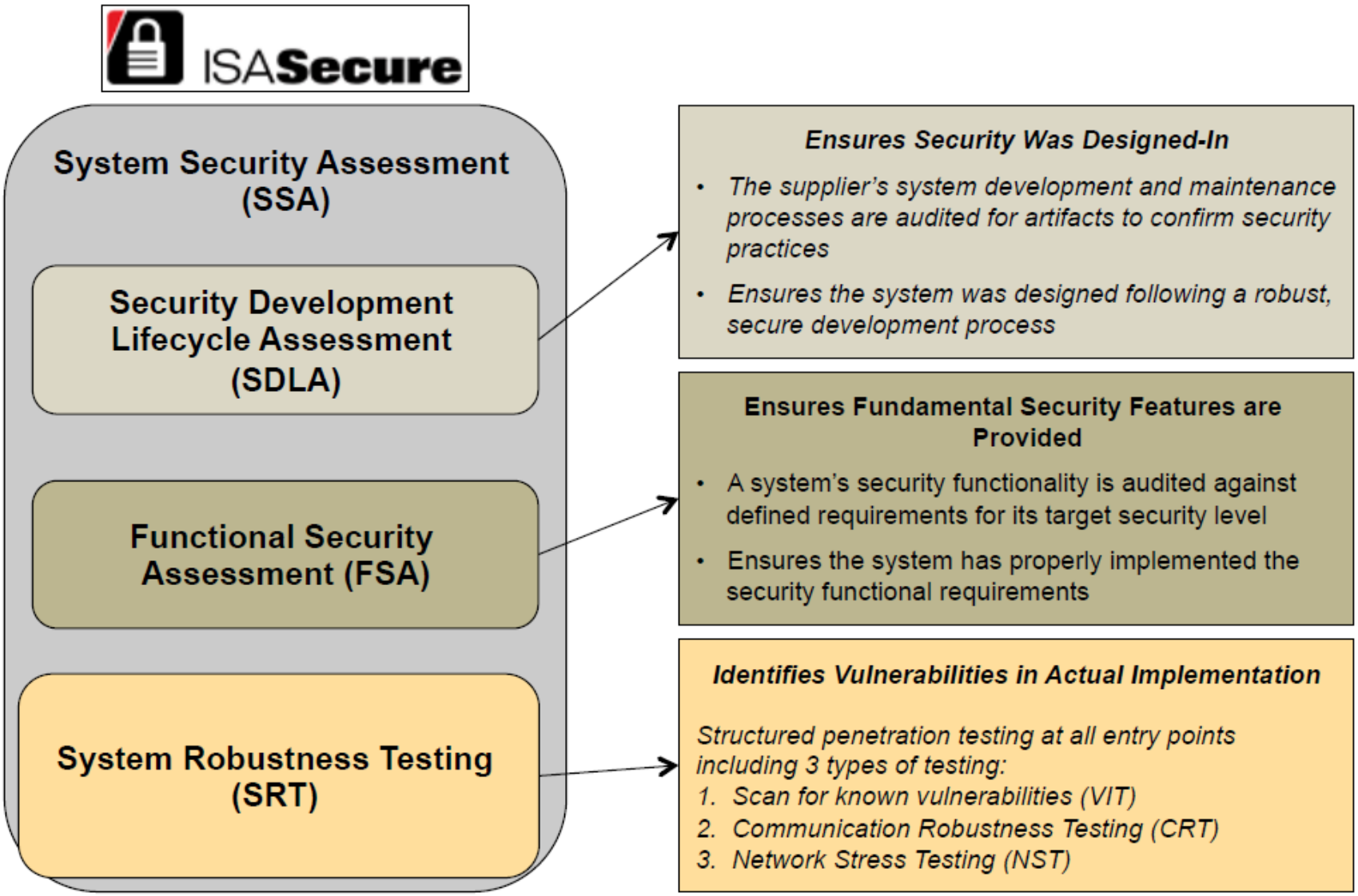
＜出典＞

制御システムセキュリティセンター
東北多賀城本部（CSS-Base6）開所記念シンポジウム
パネルディスカッション
テーマ：「制御システム セキュリティと国際連携」
・Automation Standards Compliance Institute (ASCI)
Managing Director of ISCI　Andre Ristaino 氏
http://www.css-center.or.jp/sympo/2013/documents/sympo20130528-andre.pdf

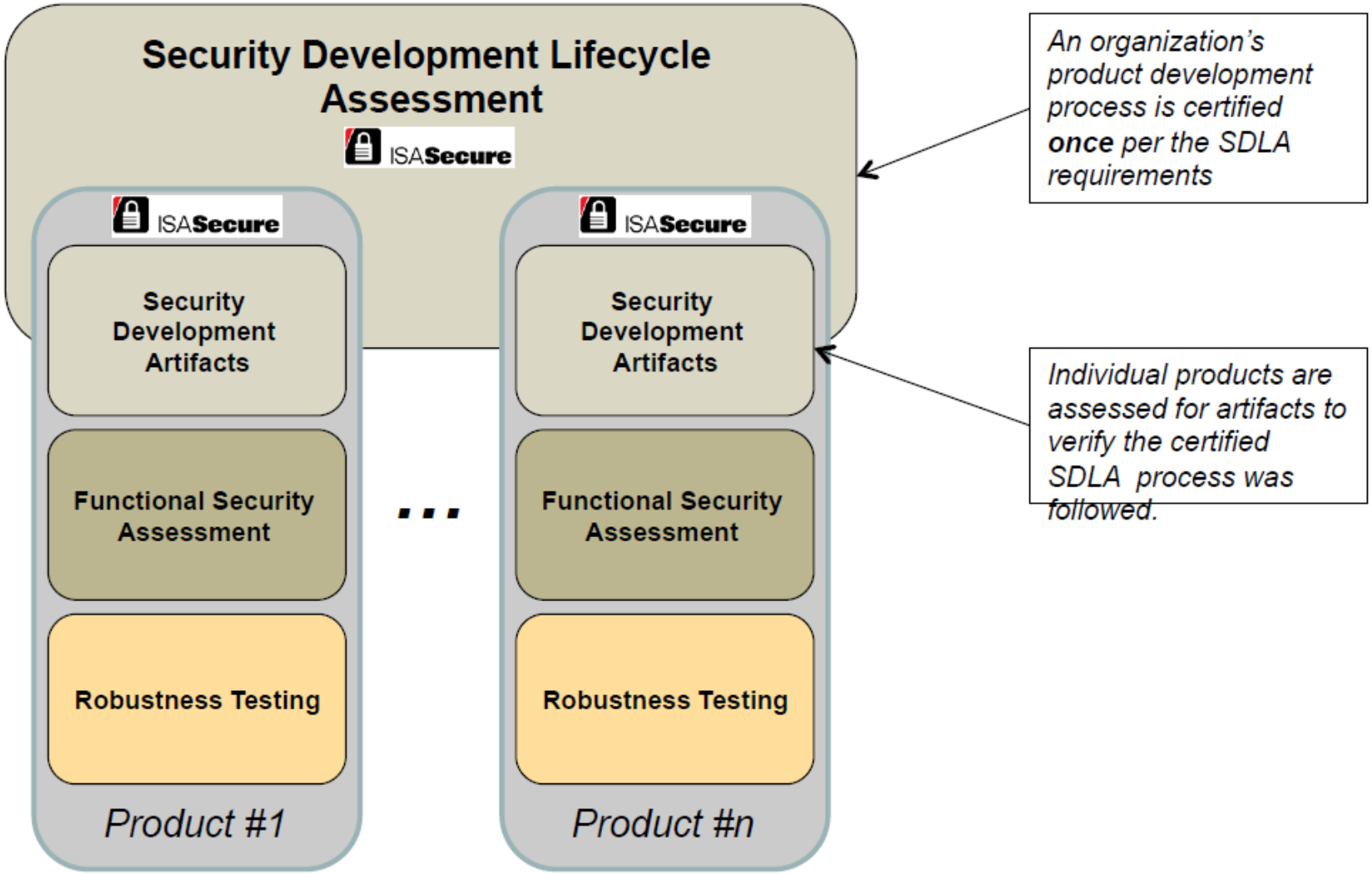
Zones and Accessible Network Interfaces



ISASecure SSA Certification Program



SDLA : Multiple Product Certification



CSMS認証制度の推進

IPA Information-technology Promotion Agency, Japan

ISMS(ISO27001)のIACS版と考えられ、ほぼ同様の要求事項。
*IACS: Industrial Automation and Control Systems
・制御システムのトータルなセキュリティ向上を目指して、CSMS認証を導入する
・ISMS適合性評価制度のスキームに沿って、CSMS認証を実現する

2013 年 → 2014 年 → 2015 年

認証取得の試行

・先行的な評価・認証による
ノウハウの蓄積
・効果的な試行者の選定
三菱化学エンジニアリング(株)
横河ソリューションサービス(株)
・パイロットプロジェクト
国家施策による立上げ
(METI, IPA, JIPDEC)

評価認証の拡大

・一般認証事業開始
・業界固有の特徴分析、
ノウハウの蓄積
(CSSC会員企業を中心に
各業界1件程度)
・国家施策による
評価認証施策の拡大

認証の本格的普及

・蓄積されたノウハウに
基づくガイドの策定
(各業界向けガイド公開)
・ガイドを活用した
評価・認証の実施
・認証取得の事業メリット
の明確化、活用

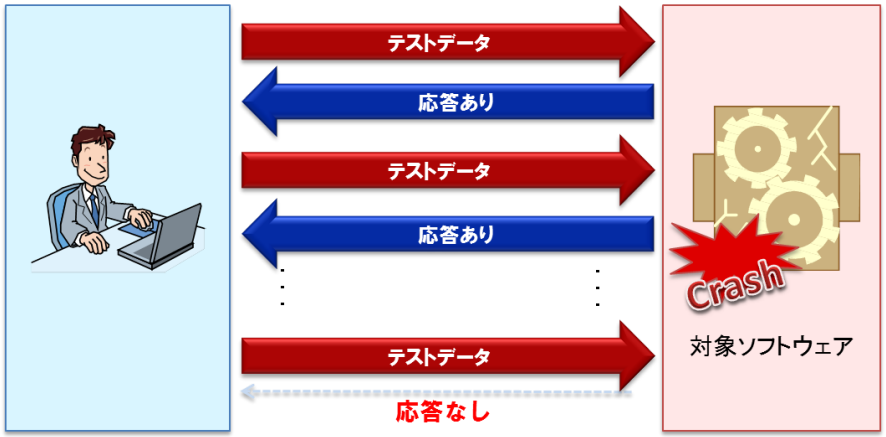
・2013年度:パイロットプロジェクトにより、認証基準、スキームを立ち上げ
・2014年度:認証事業の開始。先行事業者によるノウハウの蓄積
・2015年度:業界別のガイド策定。事業メリット明確化、認証取得拡大

※最新のドラフトでは「CSMS」 →「IACS-SMS」と名称変更が予定されている。

参考：
ソフトウェア製品の開発ライフサイクルにファジングの導入を（1/2）

IPA Information-technology Promotion Agency, Japan

ファジングとは



ファジングとは、ソフトウェア製品に、問題を引き起こしそうなテストデータを大量に送り込み、その応答や挙動を監視することで脆弱性を検出する検査手法です。

- バグや脆弱性の低減

- テストの自動化・効率化による労力削減

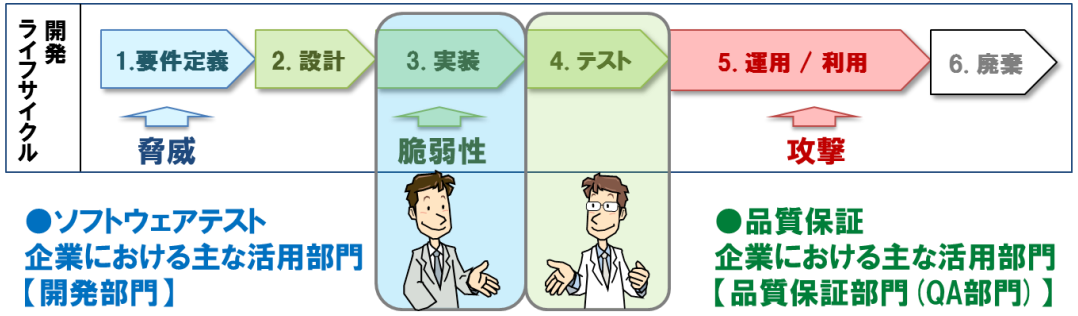
ソフトウェア製品の開発ライフサイクルにファジングの導入を(2/2)

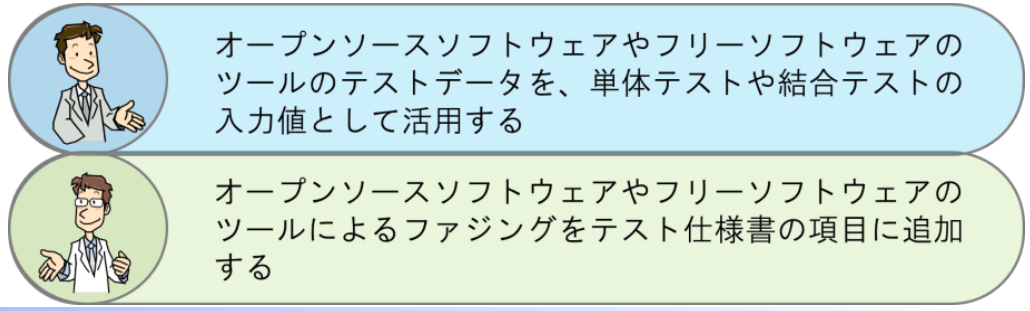
IPA Information-technology Promotion Agency, Japan

ファジングの活用

製品開発企業でまだファジングを導入していない場合、まずは開発部門、品質保証部門でのファジングを活用を推奨します。

製品開発における品質保証部門だけではなく、開発部門でもファジングを活用することで、製品出荷後に脆弱性が発見される可能性を低減させることができます





活用の手引き・ファジング実践資料

http://www.ipa.go.jp/security/vuln/fuzzing.html

管理部門・開発部門向け

ファジングの概要から実践方法、および製品開発組織におけるファジングの活用方法などをまとめた手引書です。

開発部門・品質部門向け

オープンソースソフトウェアなどを活用してすぐにファジングを実践できるよう、ツールの使い方などをまとめた解説書です。

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

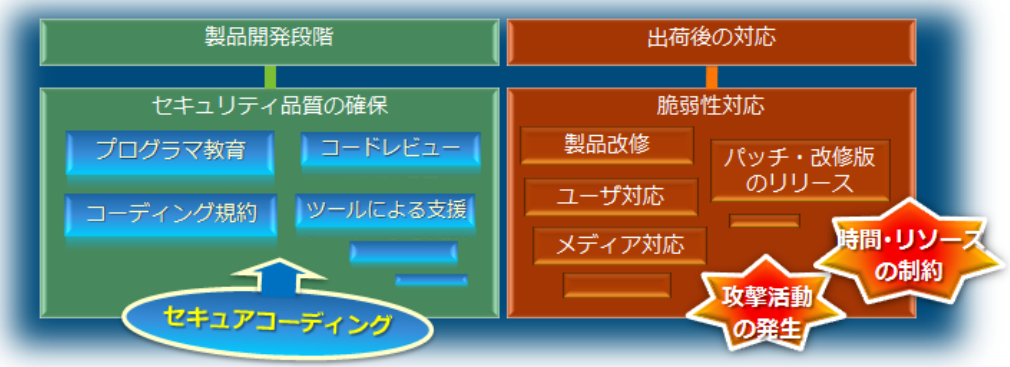


図１：製品へのセキュリティ対策導入タイミングがもたらす効果の違い

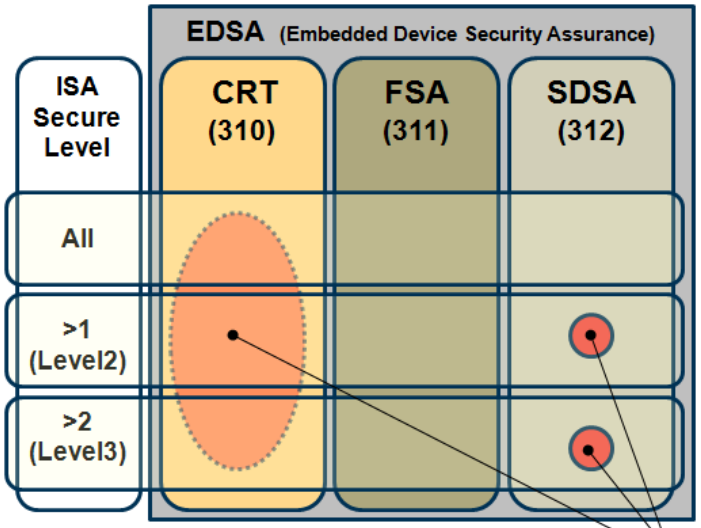


図２：CRTとSDSAの要求事項の一部充足が期待できる

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