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

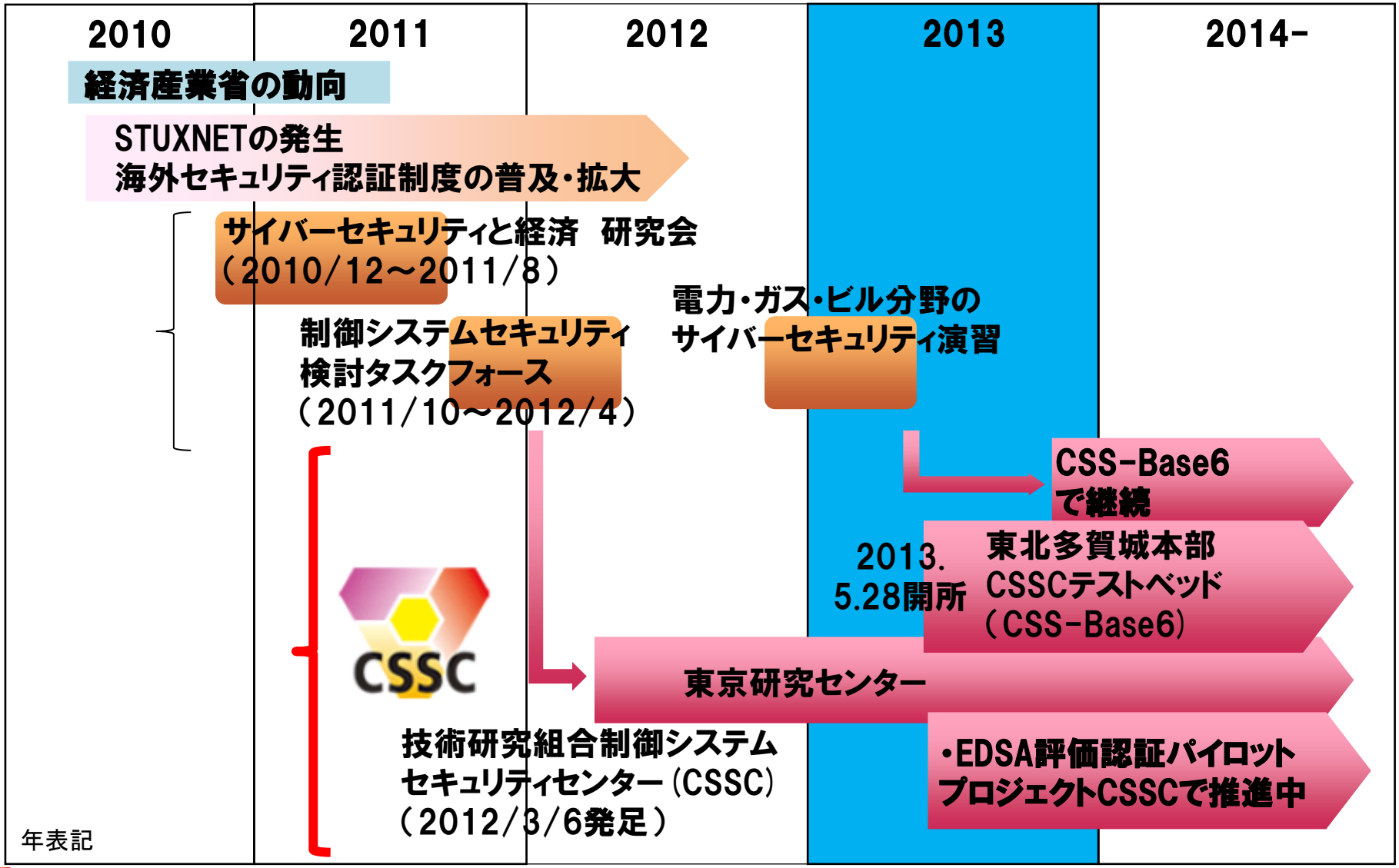
1.制御システムのセキュリティ向上へのCSSCの取り組み

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

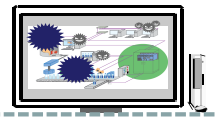
20130801現在

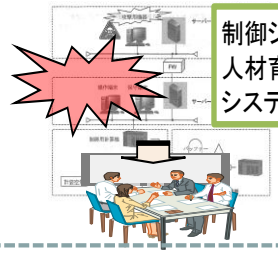
CSSCの研究開発の概要

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

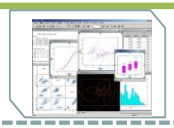
制御システム向け軽量暗号認証技術

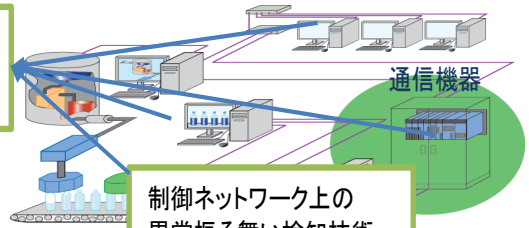
仮想環境における高セキュア制御システム構築技術

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）

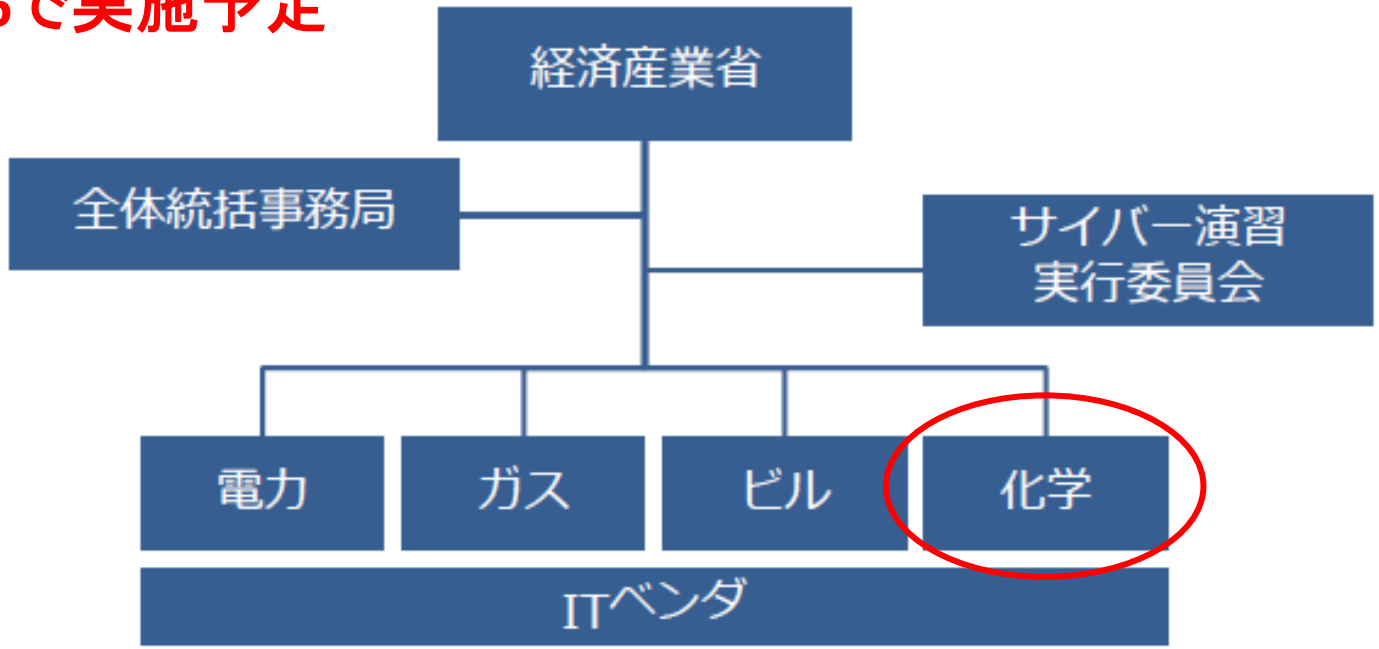
火力発電所訓練シミュレータ

2013年度の制御システムのサイバー演習

[演習の目的]

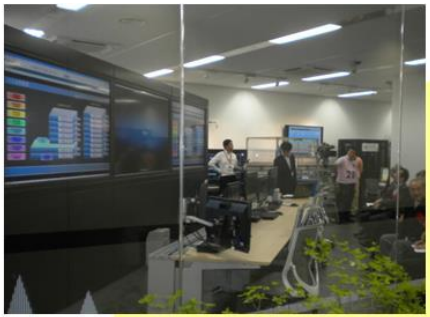
電力分野、ガス分野、ビル分野、化学分野において、現場の担当者、技術者、関係するベンダ等が、制御システムにおけるセキュリティ上の脅威を認識し、セキュリティインシデント発生の検知手順や障害対応手順の妥当性の検証を目的とするサイバーセキュリティ演習を実施し、各分野の参加者における制御システムセキュリティにおける対策を中心とした知見の獲得を促す。

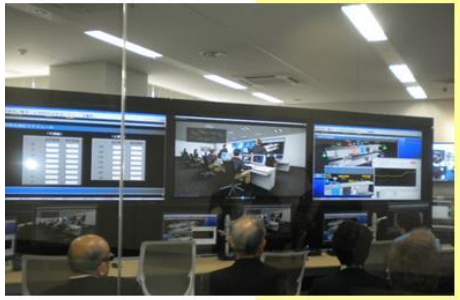
CSS-Base6で実施予定



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）





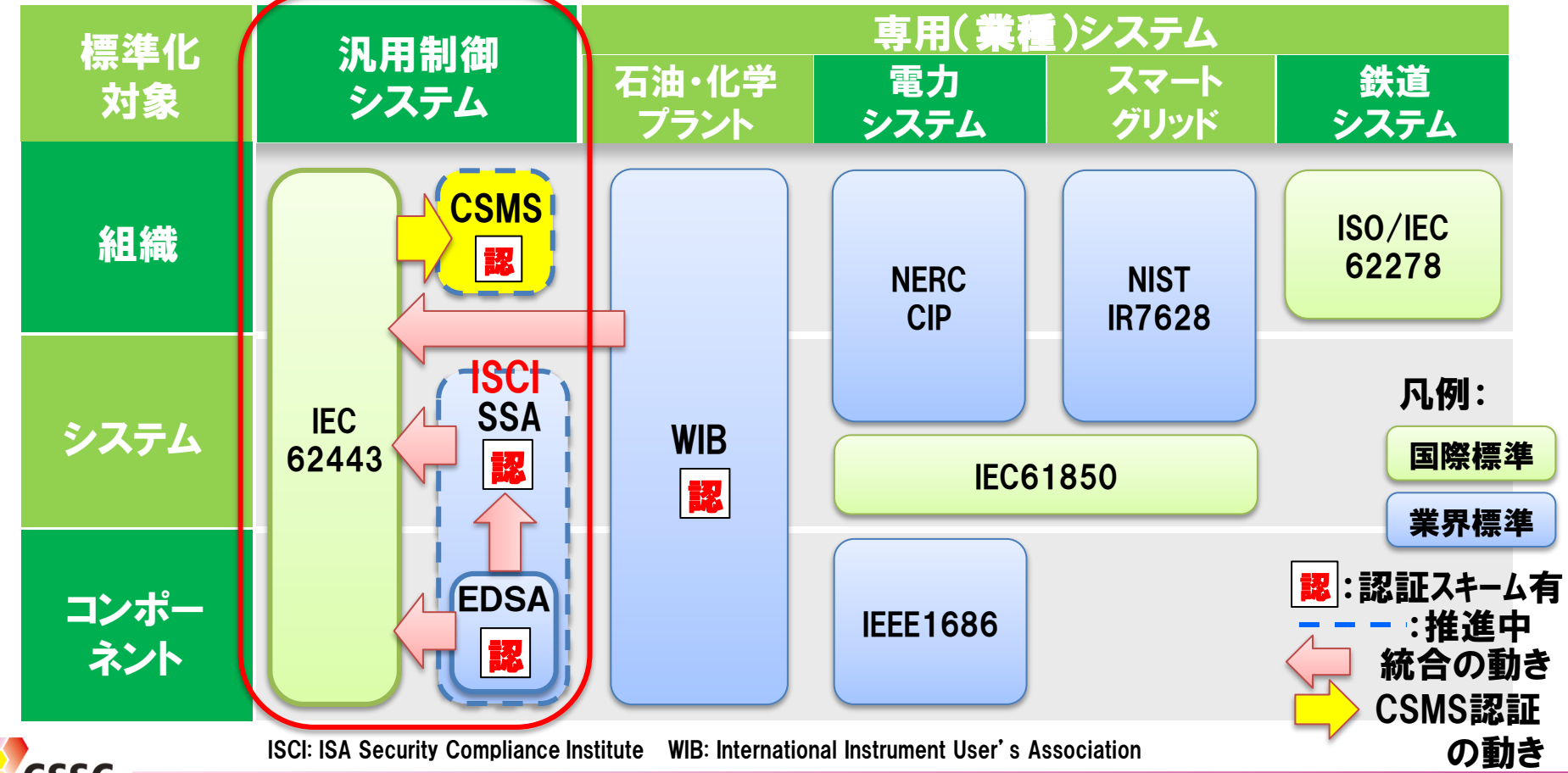
開所式でビル模擬システムのデモ実施。空調、エレベータ制御、照明制御など多種のビル内機器の制御を実施している。本デモは照明制御へのサイバー攻撃。

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)

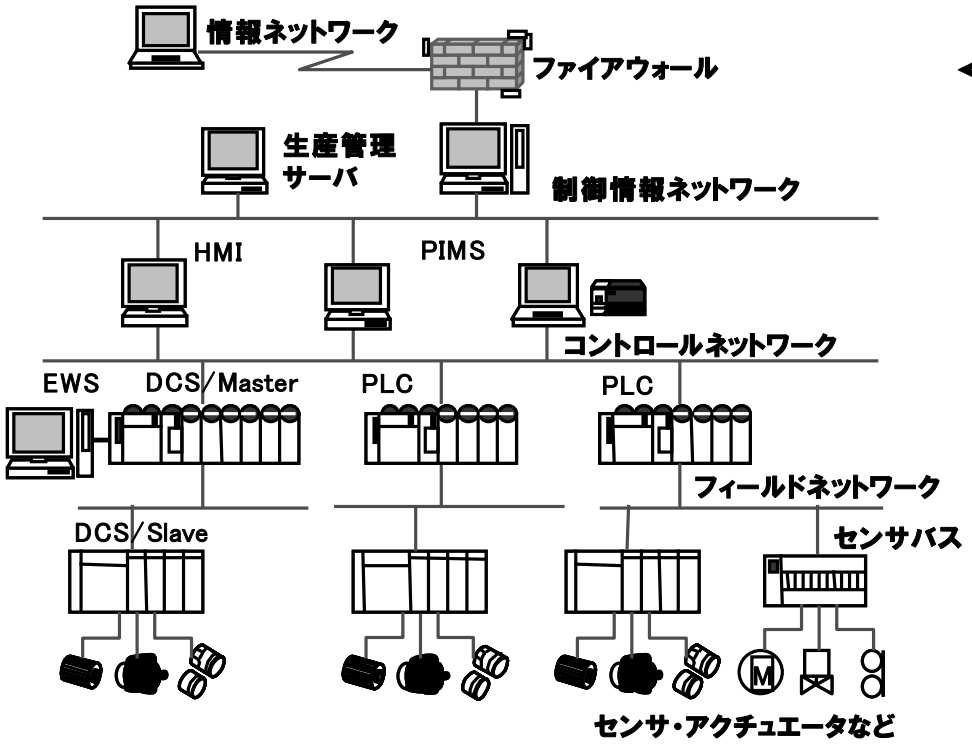
事業者
インテグレータ
装置ベンダ

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）

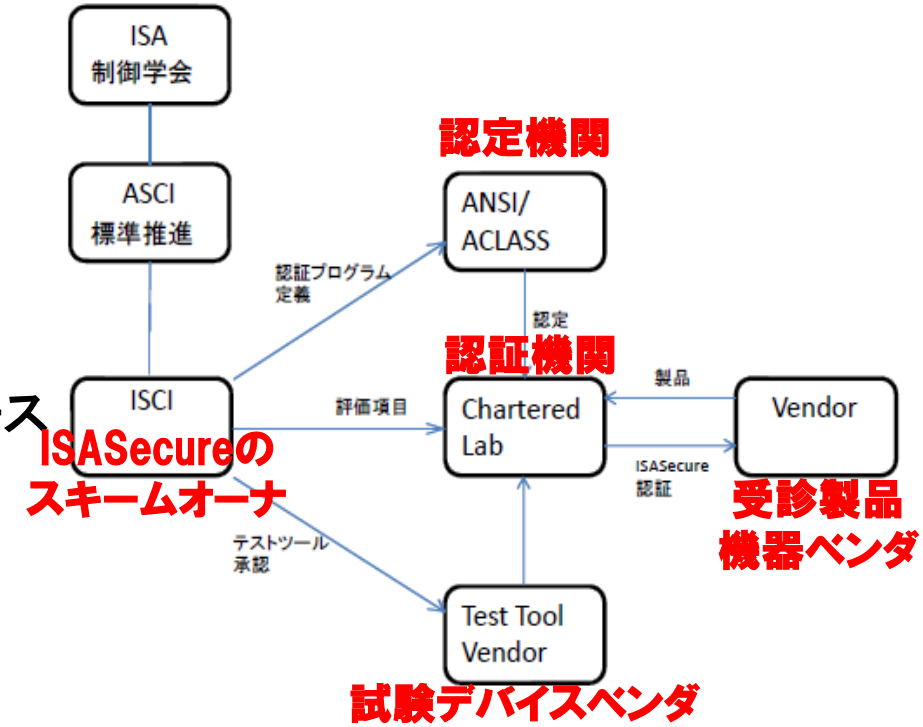
ISA Reference	IEC Reference	Title	Status
ISA-62443-1-1	IEC/TS 62443-1-1	Terminology, concepts and models	Published, Under Revision
ISA-TR62443-1-2	IEC/TR 62443-1-2	Master glossary of terms and abbreviations	Under Development
ISA-62443-1-3	IEC 62443-1-3	System security compliance metrics	Under Development
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。

(参考)ISASecure認証プログラムの評価スキーム



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。

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

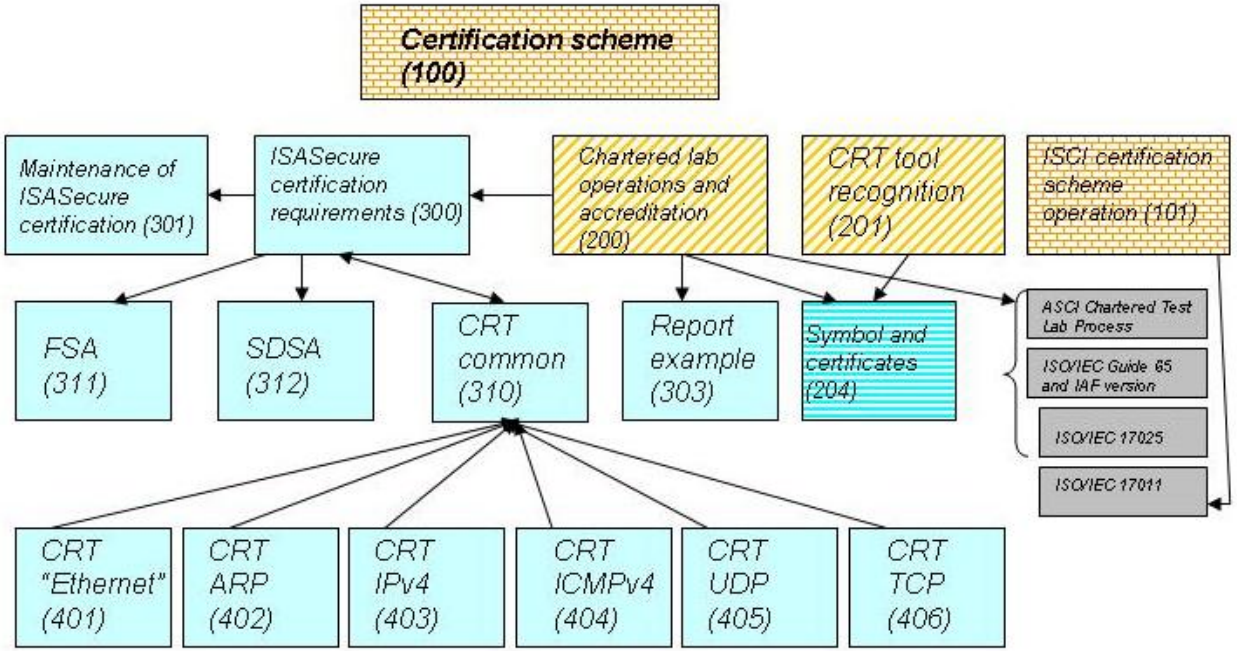
- ISASecure EDSA認証取得済組込み機器：3社5製品

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。

技術仕様

一般的な技術仕様

EDSA-300 ISASecure 認証の要求事項	Pdf ファイルを表示
EDSA-301 ISASecure 認証の維持管理	Pdf ファイルを表示
EDSA-311 機能セキュリティアセスメント(FSA)	Pdf ファイルを表示
EDSA-312 ソフトウェア開発セキュリティアセスメント(SDSA)	Pdf ファイルを表示

CRT 仕様

EDSA-310 IPベースのプロトコル実装に対する通信ロバストネステストの共通要求事項	Pdf ファイルを表示
EDSA-401 2つの一般的な「Ethernet」プロトコルの実装に対するロバストネスのテスト	Pdf ファイルを表示
EDSA-402 IPv4を使用したIETF ARPプロトコルの実装に対するロバストネスのテスト	Pdf ファイルを表示
EDSA-403 IETF IPv4 ネットワークプロトコルの実装に対するロバストネスのテスト	Pdf ファイルを表示

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

EDSA認証の各評価項目概要

ISASecure

EDSA

- ソフトウェア開発セキュリティ評価（SDSA）
- 機能セキュリティ評価（FSA）
- 通信ロバストネス試験（CRT）

◆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

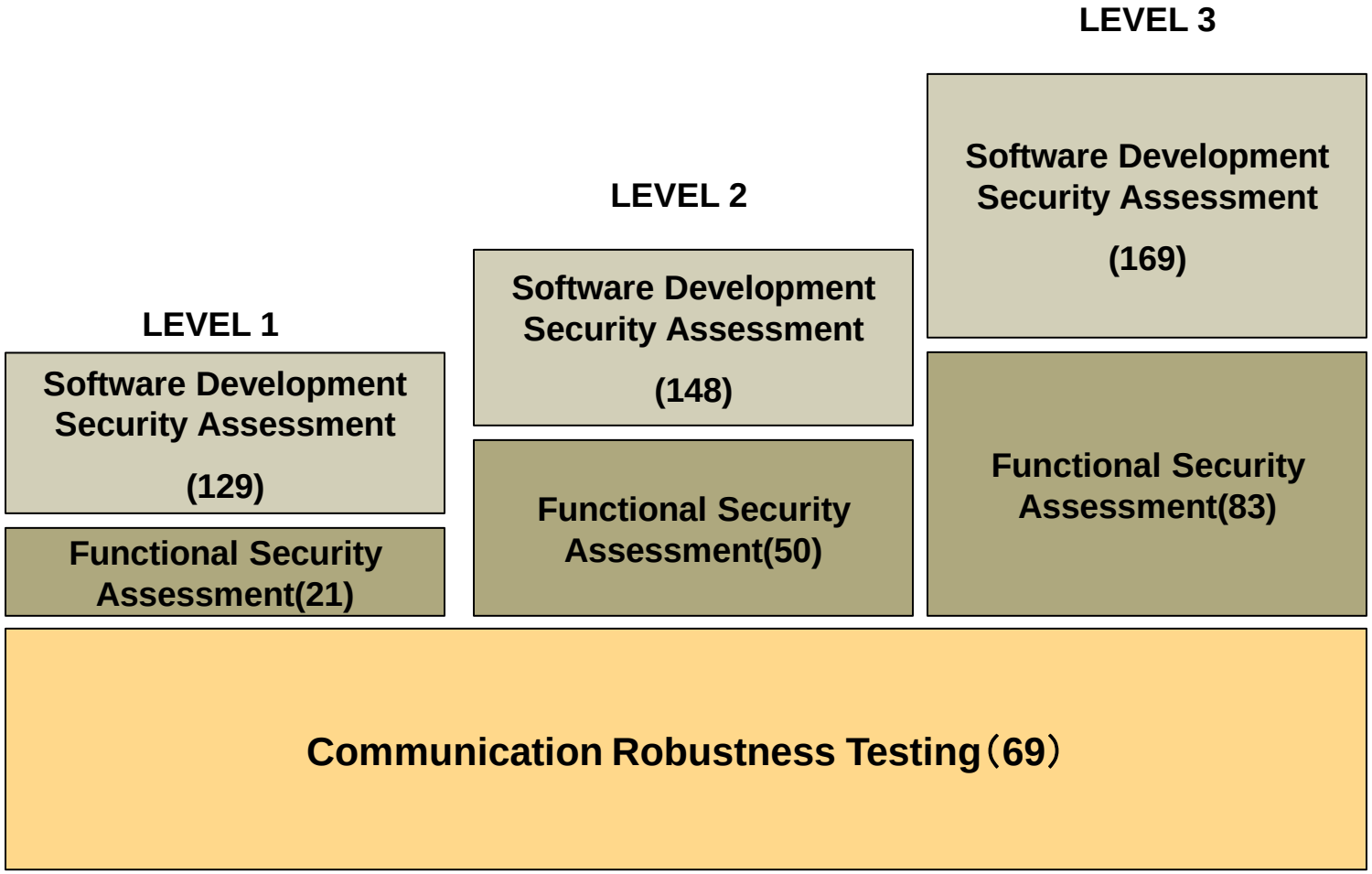
Communication Robustness Testing(CRT), Functional Security Assessment (FSA), Software Development Security Assessment(SDSA)

注：正式には原英文を参照してください。

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

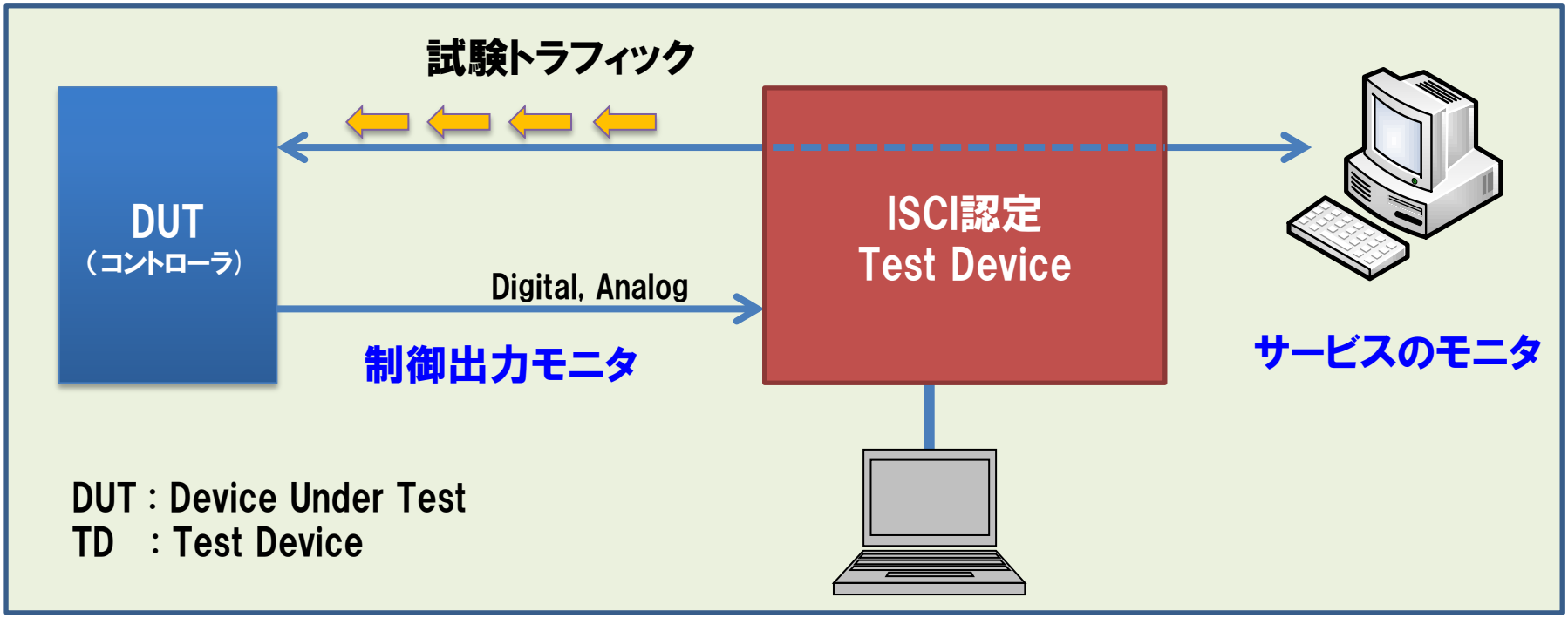
評価項目の数によって3段階の認証レベルを規定



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

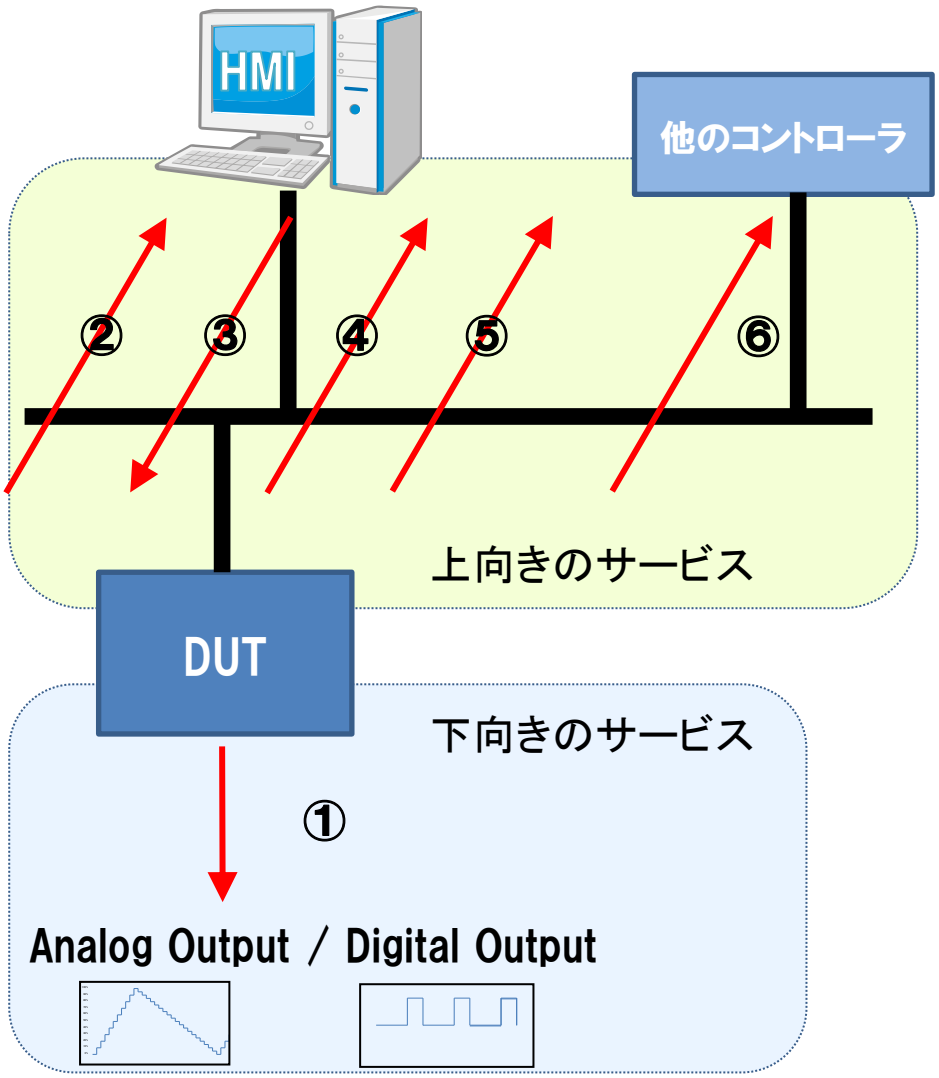
② プロセスのビュー
- プロセスビューを適切なタイミングで提供する機能

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

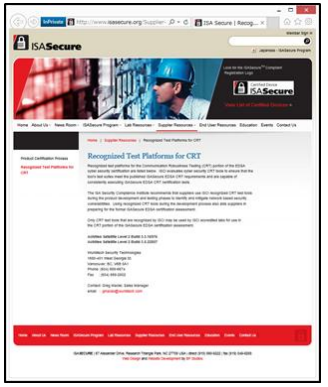
⑥ ピアツーピア制御通信
- ピアツーピア制御通信を送信する機能
- 適用除外可能



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

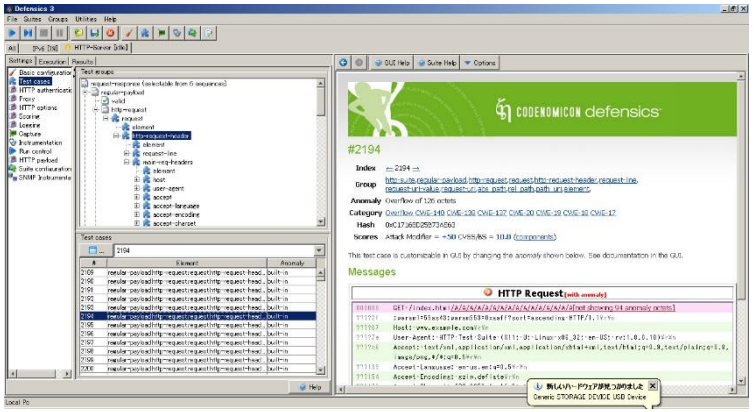


●Wurldtech 社 Achilles Test Platform

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	• 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

コアプロトコル

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

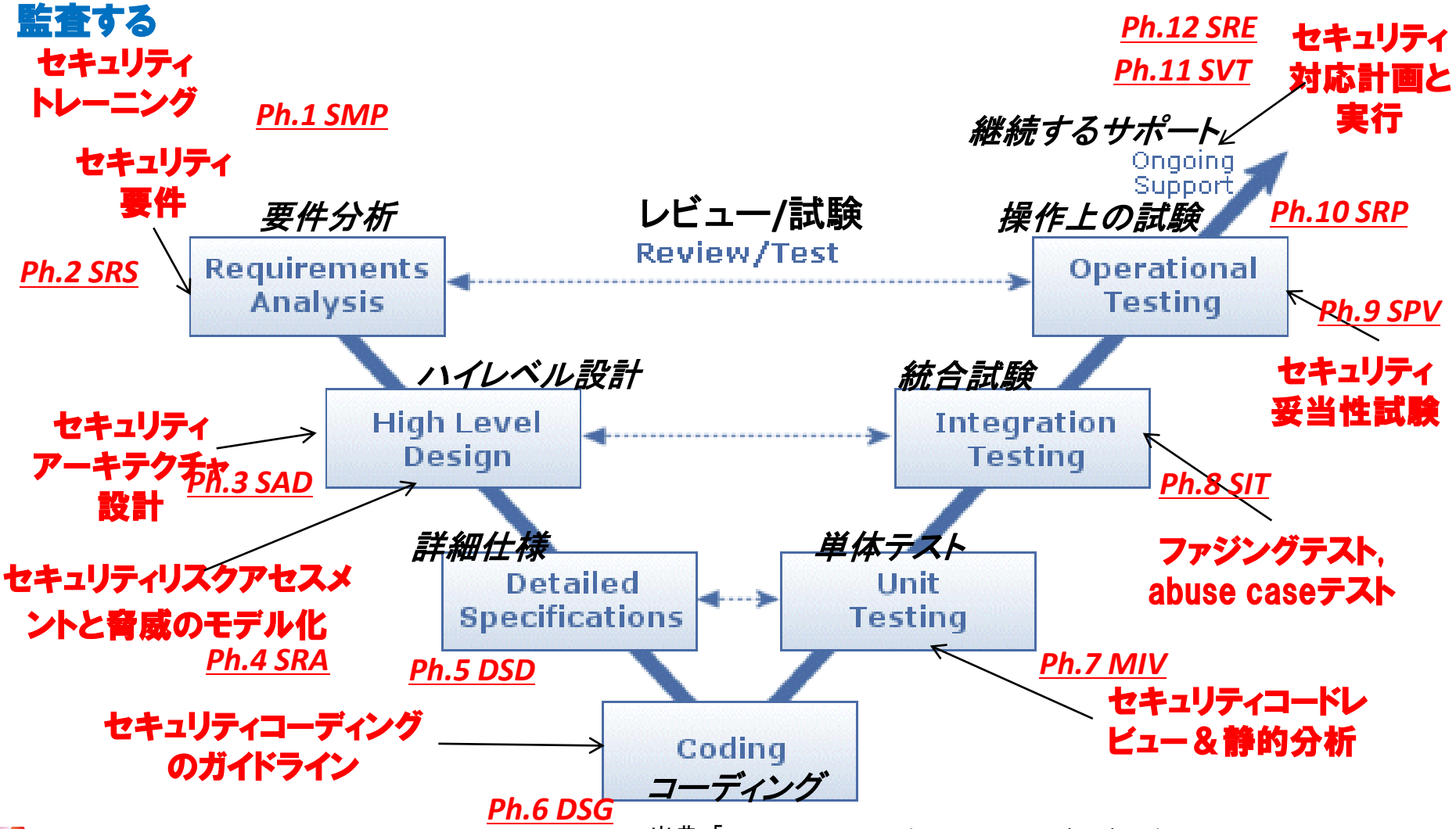
アクセスコントロール (AC: Access Control)	ユーザ承認、ユーザ認証、システム使用通知、セッションロック/終了 User Authorization, User Authentication, System Use Notification, Session Locking/Termination
使用コントロール (UC: Use Control)	デバイス認証、監査証跡 Device Authentication, Audit Trail
データの完全性 (DI: Data Integrity)	転送中のデータ、保管中のデータ Data in Transit, Data at 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

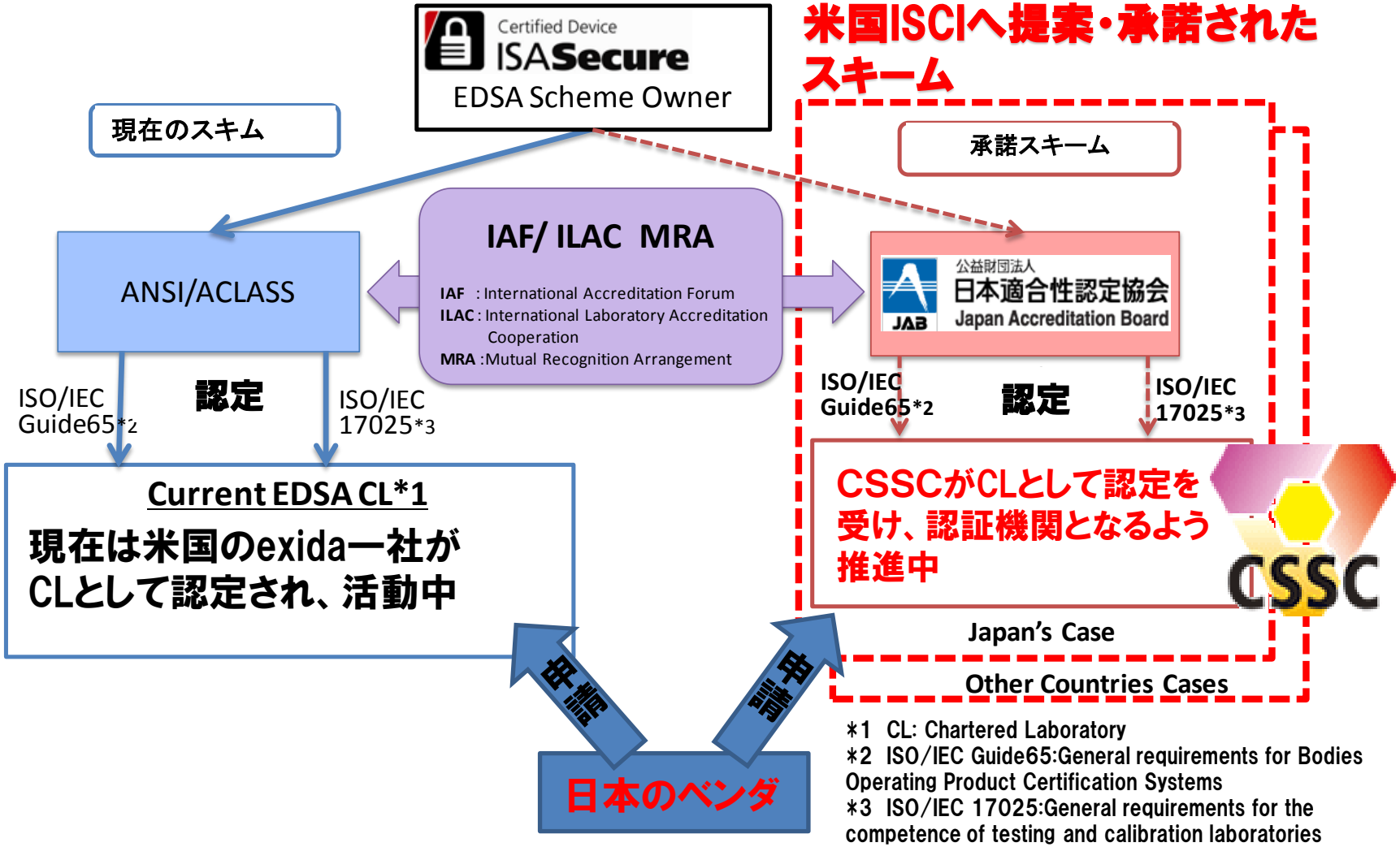
SDSAでは、開発プロセスのV字モデルにセキュリティ活動フェーズが組み込まれていることを監査する



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

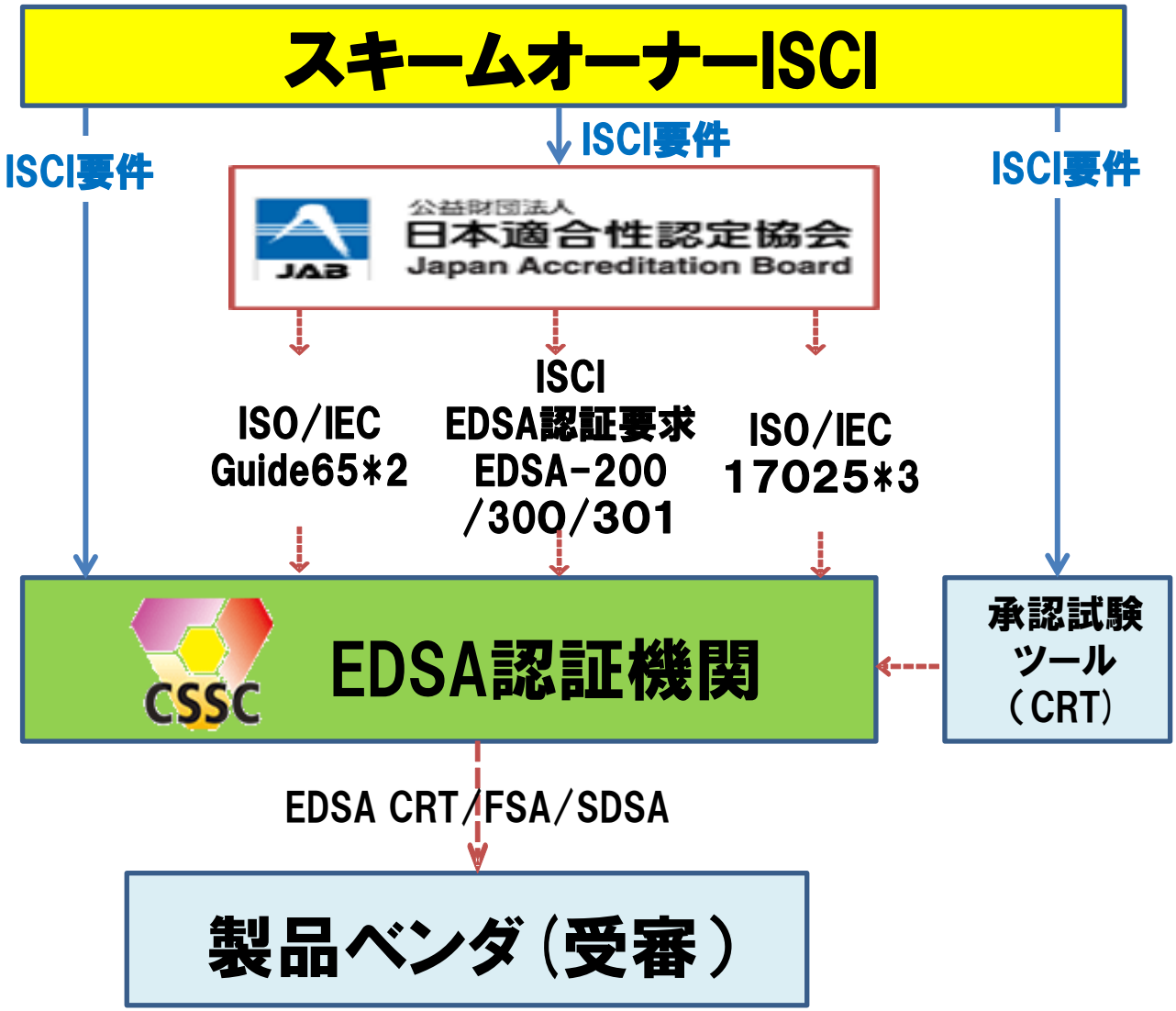
ISASecure EDSA認証の認定取得とは

2013.9JAB へ認定申請

主要な要求事項の標準

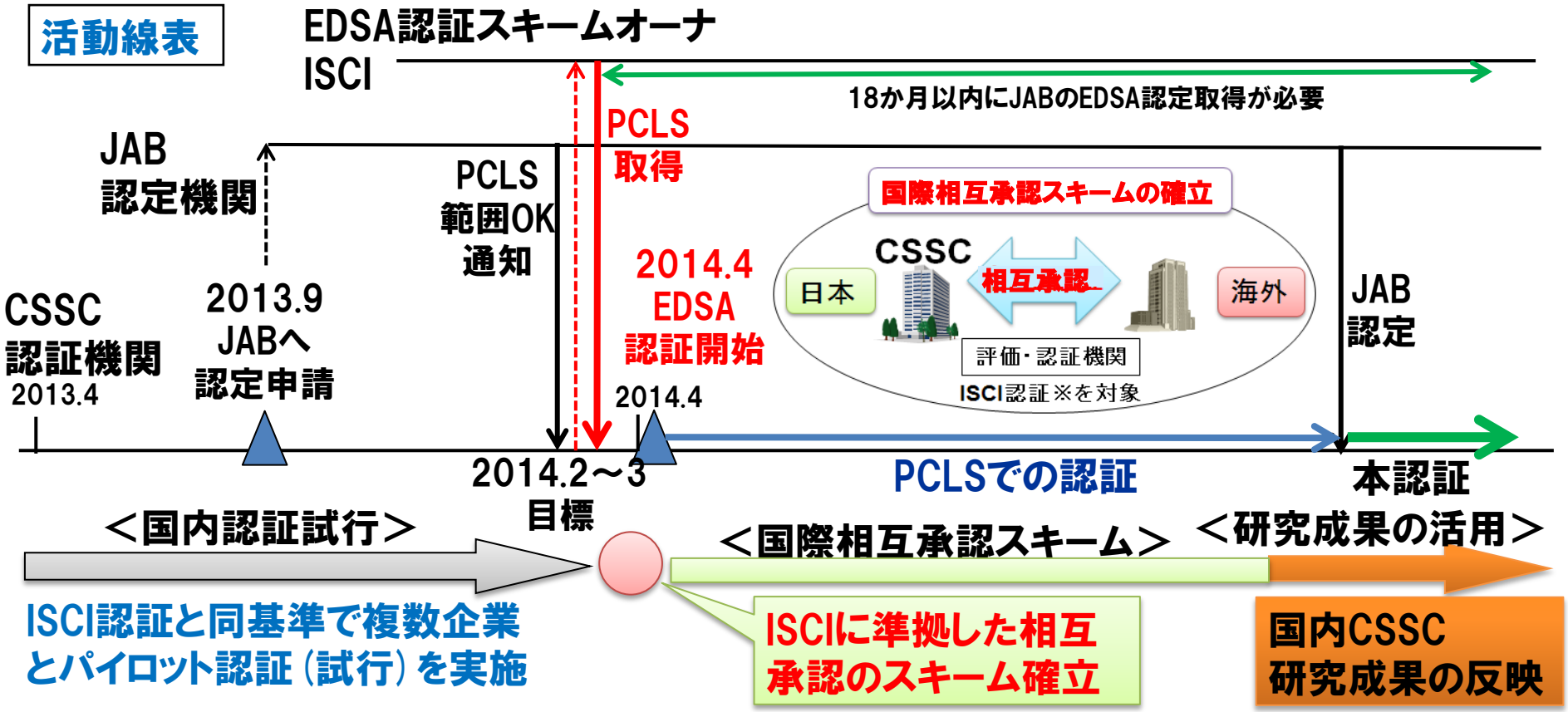
ISO/IEC17025:
試験所及び校正機関の能力に関する一般要求事項

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

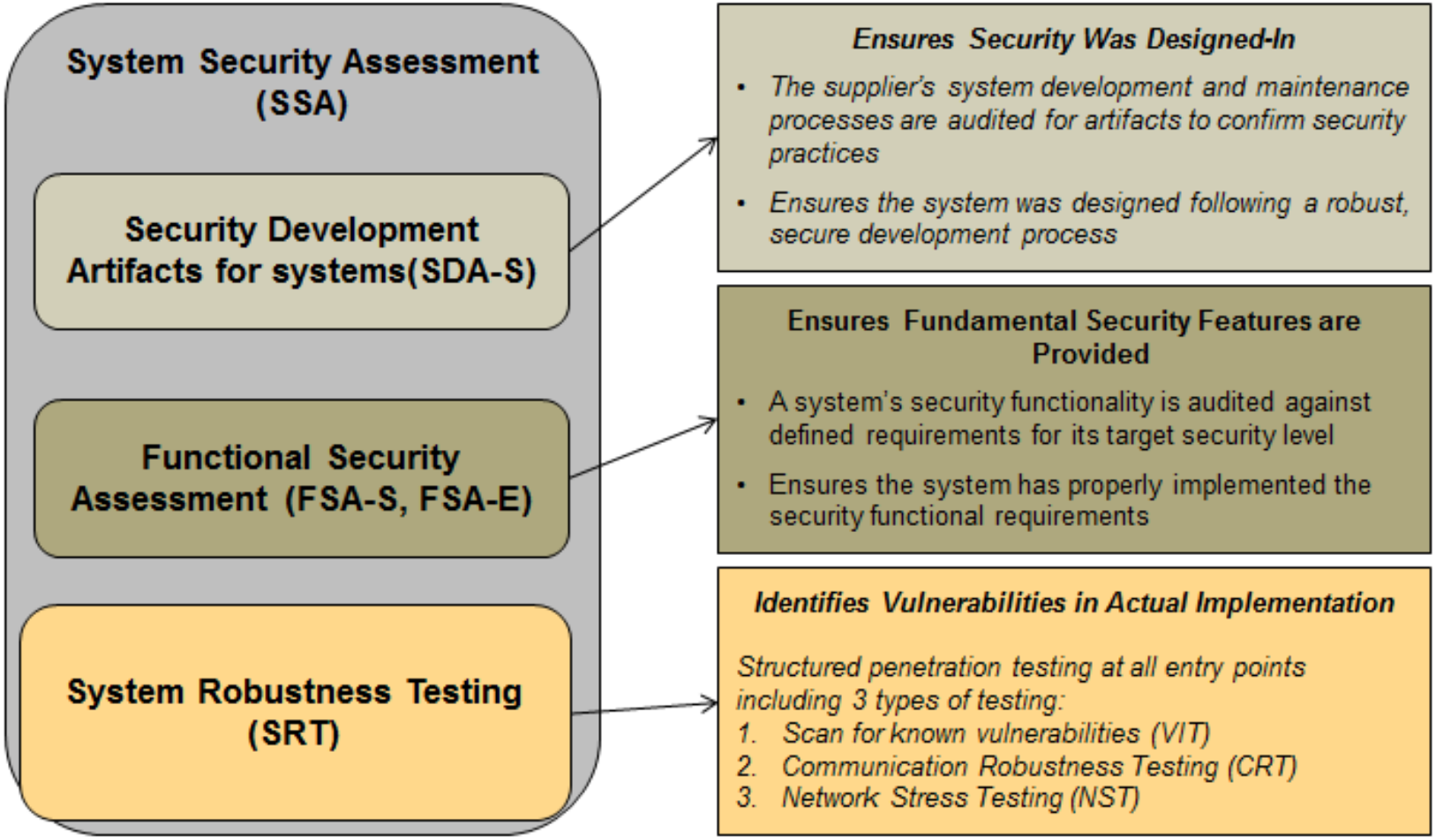
**2014年4月よりPCLS（仮免状態）でのEDSA認証のサービス開始予定。
認証機関の体制・EDSA認証標準への取組み・品質マニュアル等の整備をし、
JABに対し2013.9に認定申請をし、現在審査中の状態。**



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)

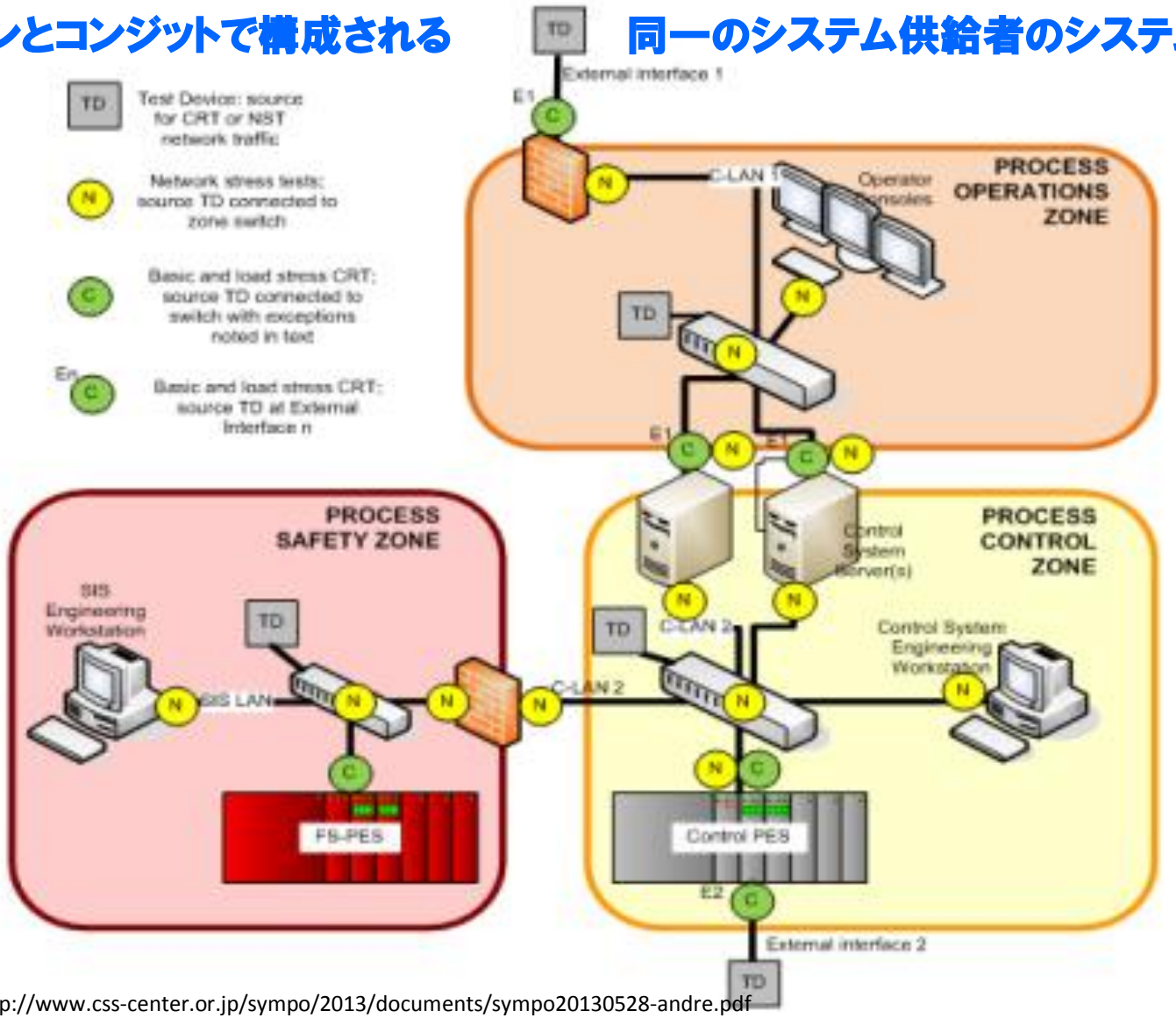


出典：http://www.css-center.or.jp/sympo/2013/documents/sympo20130528-andre.pdf

SSA対象システム

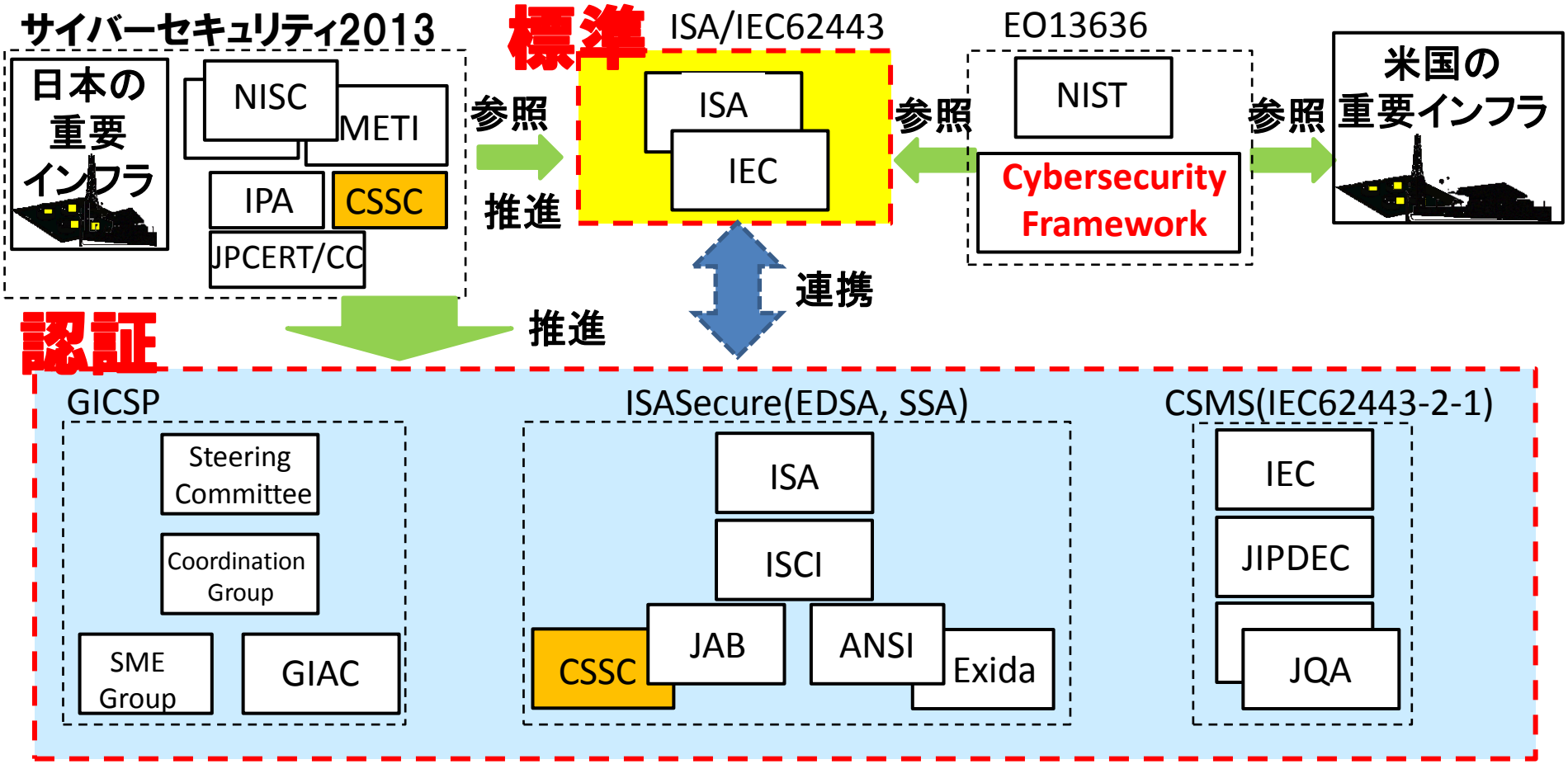
複数のドメインとコンジットで構成される

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



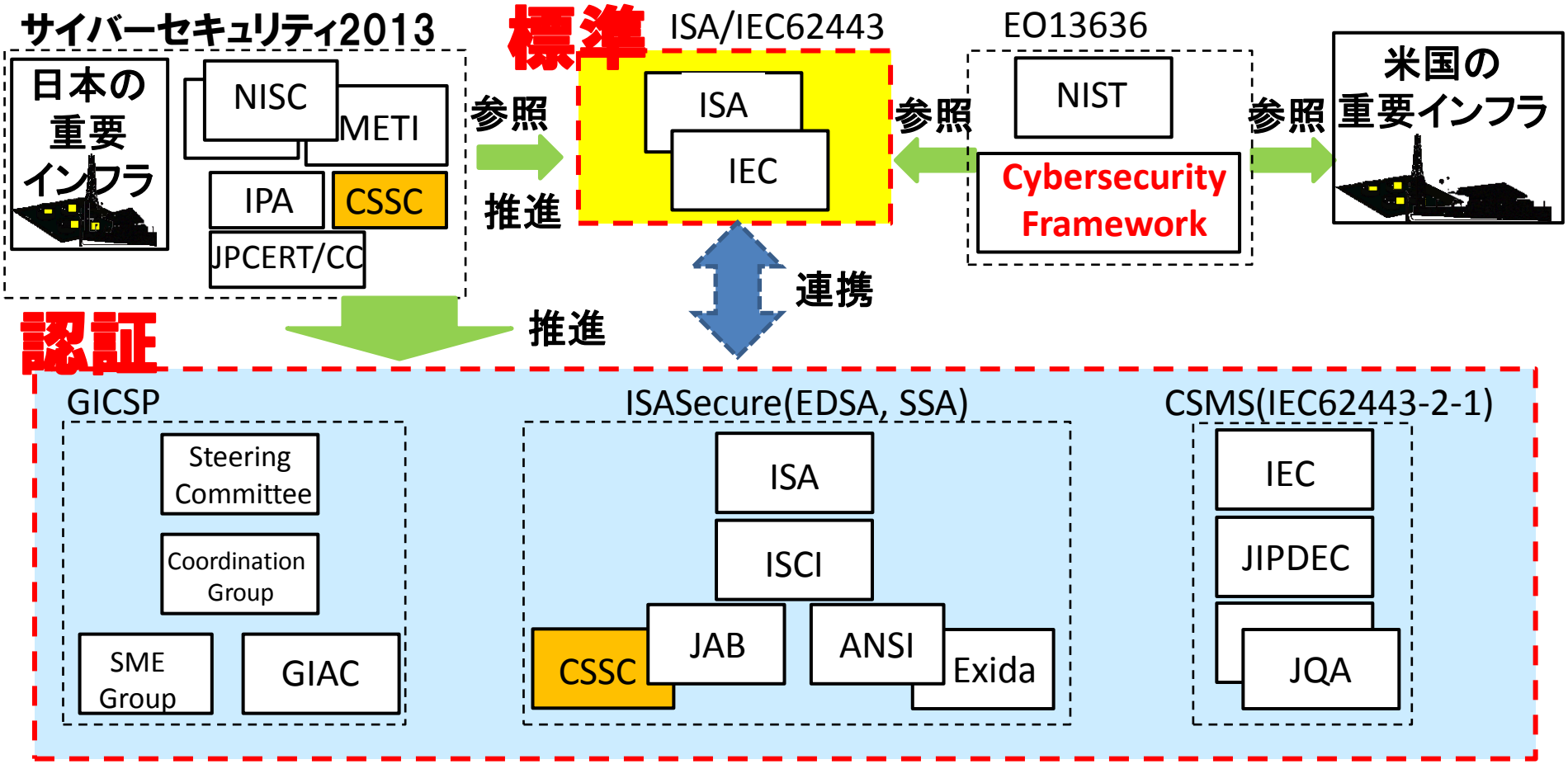
制御システムセキュリティ
プロフェッショナル（人）
認証
(GICSP: Global Industrial Cyber Security Professional
ISA/IEC62663とNERC CIPが参照されている。)

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

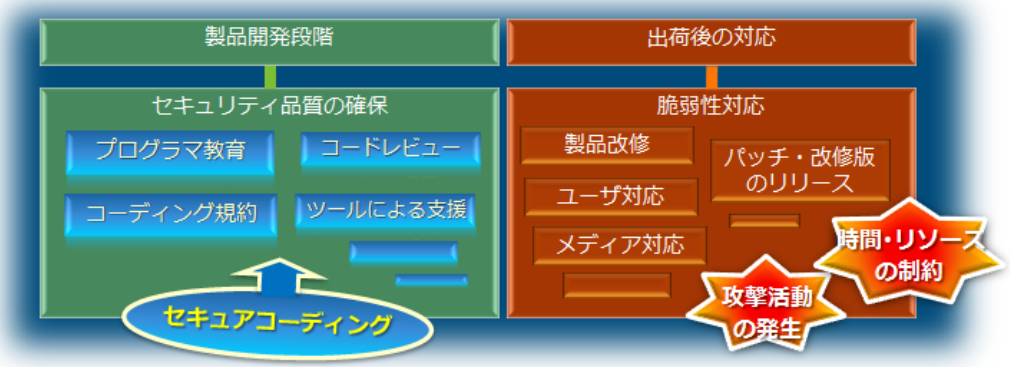


図１：製品へのセキュリティ対策導入タイミングがもたらす効果の違い

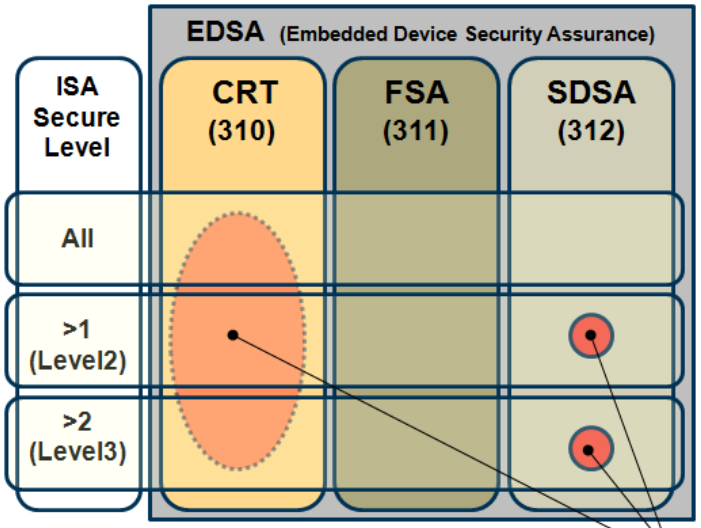


図２：CRTとSDSAの要求事項の一部充足が期待できる

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

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