CSSC認証ラボラトリー　ISASecure EDSA認証 説明会

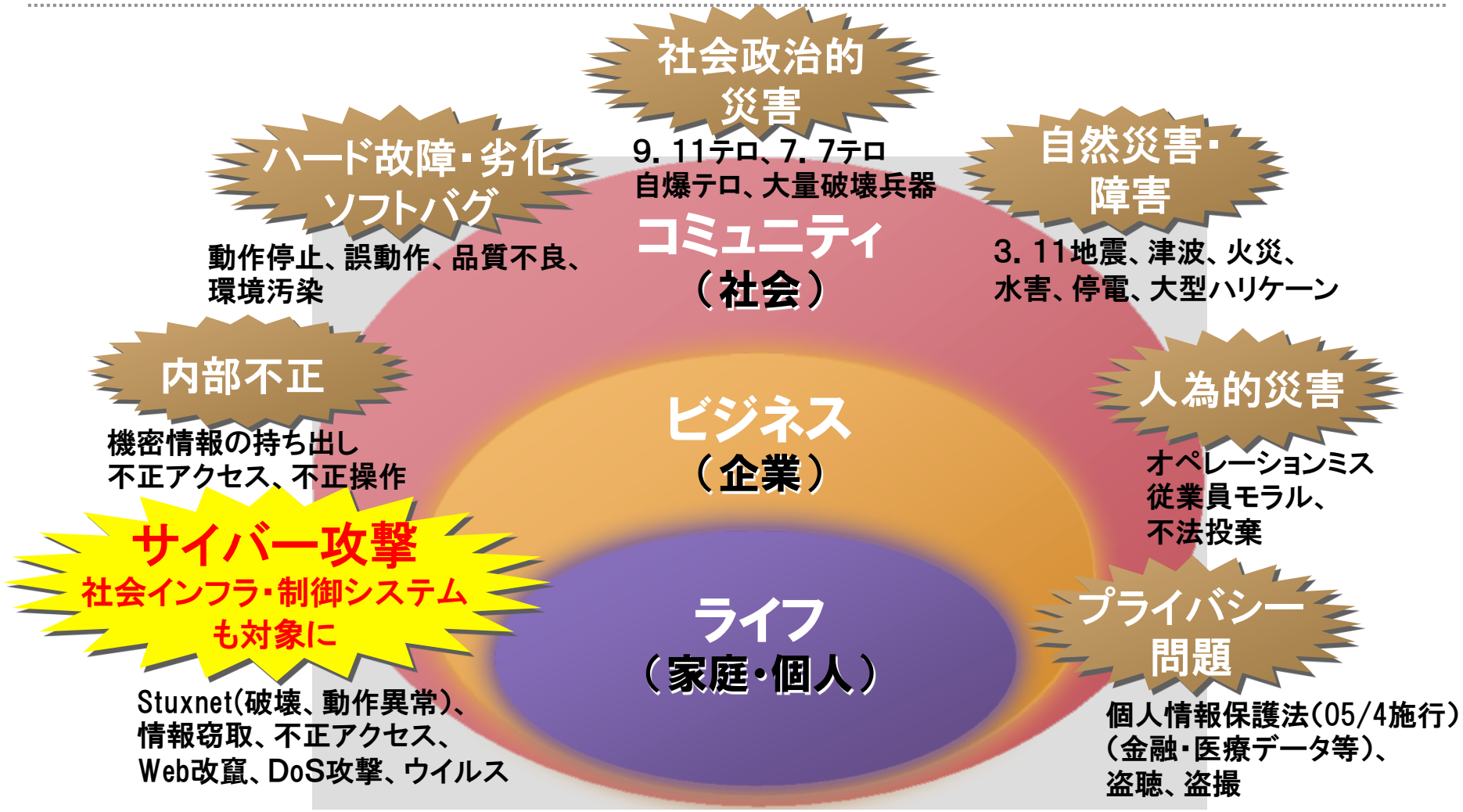
ISASecure EDSA認証と日本の取組み

2014年1月15日
公益財団法人 日本適合性認定協会（JAB）
堀江　隆
CSSC認証ラボラトリー
吉松　健三 ・ 小林　偉昭

全体概要

- 標準化動向
- ISA/ASCI/ISCIについて
- EDSAについて
- 日本の取組み

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

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
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

既知の脆弱性を利用した攻撃が75％

製品ベンダ

脆弱性を作りこまない
セキュアコーディング、ファジング、ストレステスト

既知の脆弱性対策の徹底
定期的なスキャニング、ペネトレーションテスト

政府・業界、普及啓発組織等

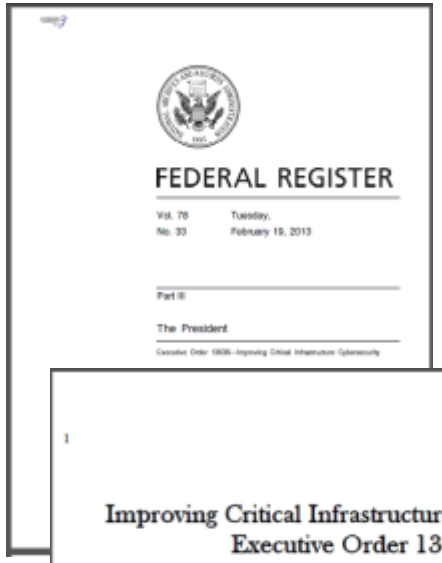
サイバー空間の脅威の周知
ex）NISC「サイバーセキュリティ2013」（6/27）
NIST「重要インフラ向けCybersecurity Frameworkドラフト」（推進中）

業界等でのセキュリティ対策推進
ex）米国航空宇宙工学協会（AIAA）（8/13）
FDAガイド（8/13）やVerizon社の調達条件

FDA: Food and Drug Administration

NIST CybersecurityフレームワークとISA/IEC62443

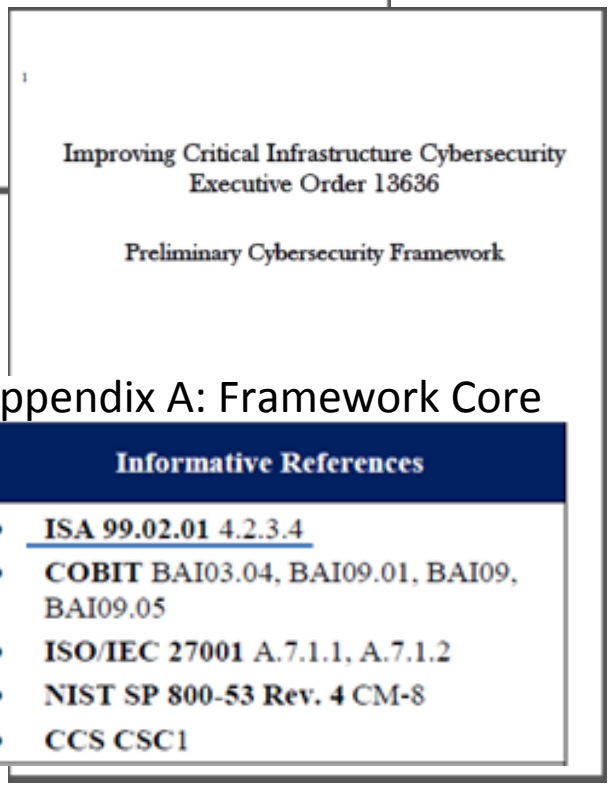
- US government Cybersecurity Framework workshop 2013/11/15開催。産学官から400名が出席
- Cybersecurity Frameworkのdraftの内容、必要な変更、実現の戦略に関して議論された
  - Cybersecurity Frameworkは
    2013年2月のオバマ大統領の行政命令
    （ Executive Order 13636—
    Improving Critical Infrastructure Cybersecurity ）
    によりNISTが作成
    （DraftはNISTからダウンロード可能）
  - Framework CoreにおいてISA/IEC 62443 (ISA99)等がクロスセクタの標準として参照されている


FEDERAL REGISTER

Vol. 78 Tuesday,
No. 33 February 19, 2013

Part II

The President


Improving Critical Infrastructure Cybersecurity
Executive Order 13636

Preliminary Cybersecurity Framework

Appendix A: Framework Core

Informative References
• **ISA 99.02.01** 4.2.3.4
• **COBIT** BAI03.04, BAI09.01, BAI09, BAI09.05
• **ISO/IEC 27001** A.7.1.1, A.7.1.2
• **NIST SP 800-53 Rev. 4** CM-8
• **CCS CSC1**

NIST Cybersecurity FrameworkとISA/IEC62443

Cybersecurity Framework:

任意の標準であるが、
デファクトになるだろう。

現在パブリックコメント
募集中で、
２月に公開予定。

InformationWeek Government CONNECTING THE GOVERNMENT TECHNOLOGY COMMUNITY

Home News & Commentary Authors Slideshows Video Reports White Papers Events Inte

STRATEGIC CIO | SOFTWARE | SECURITY | CLOUD | MOBILE | BIG DATA | INFRASTRUCT

GOVERNMENT // CYBERSECURITY

COMMENTARY
12/9/2013
02:45 PM

NIST Cybersecurity Framework: Don't Underestimate It

A cybersecurity framework for critical infrastructure owners is voluntary but will become the de facto standard for litigators and regulators. Here's how to prepare.

Gerald Ferguson
Commentary

Connect Directly

6
COMMENT NOW

Login

50% 50%

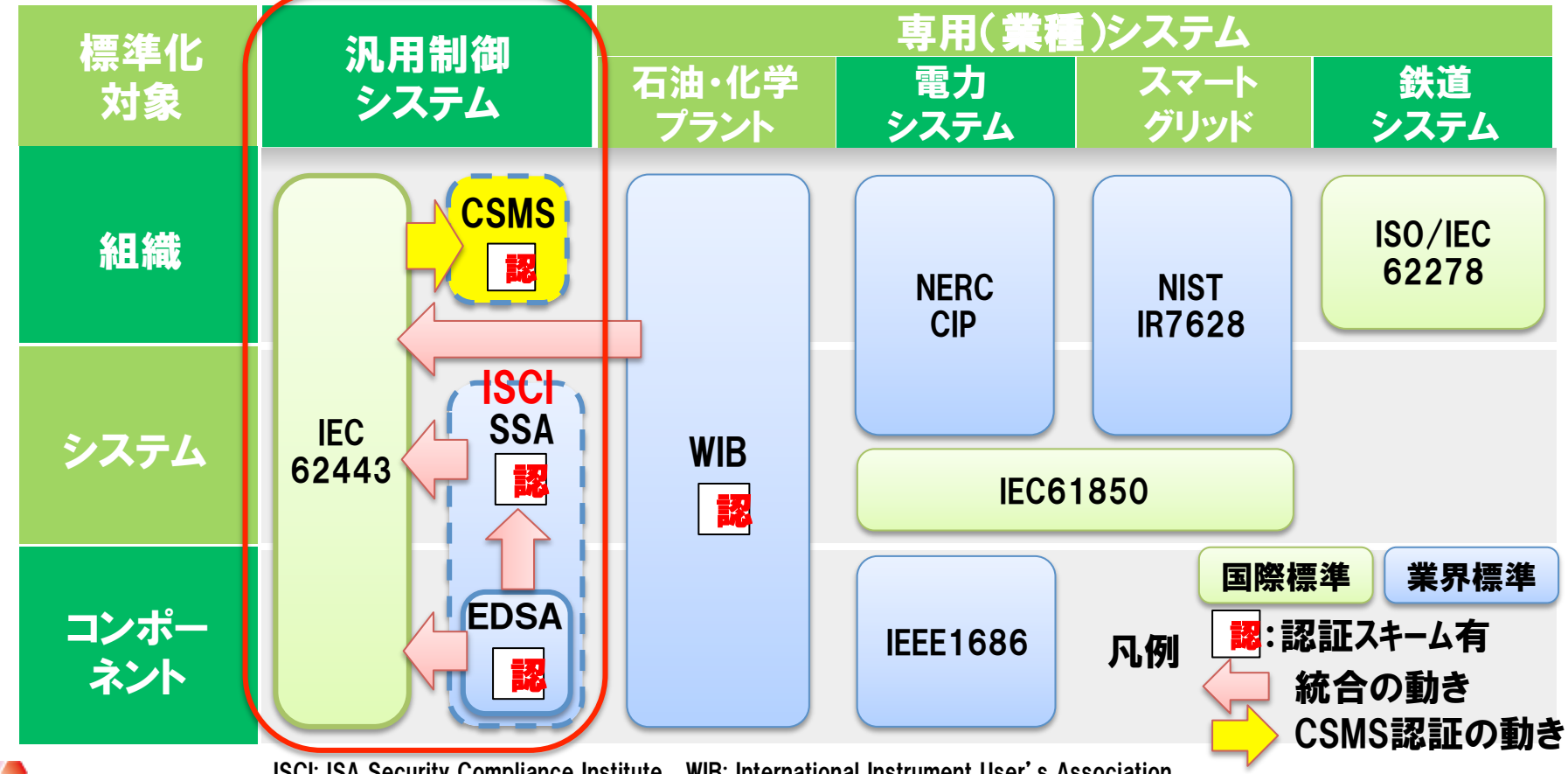
Any company that is managing critical infrastructure in the US and disregards the Preliminary Cybersecurity Framework, issued by the National Institute of Standards and Technology (NIST) in late October, does so at its own peril. The framework, which is now in its final comment stage and due to be released in mid-February, lays out a set of comprehensive but voluntary cybersecurity practices.

However, critical infrastructure owners need to recognize that, if a company's cybersecurity practices are ever questioned during a regulatory investigation and litigation, the baseline for what's considered commercially reasonable is likely to become the NIST Cybersecurity Framework.

The Department of Homeland Security defines critical infrastructure companies broadly to include banking and finance, communications, critical

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テ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

ISA Security Compliance Institute （ISCI）とは

組織

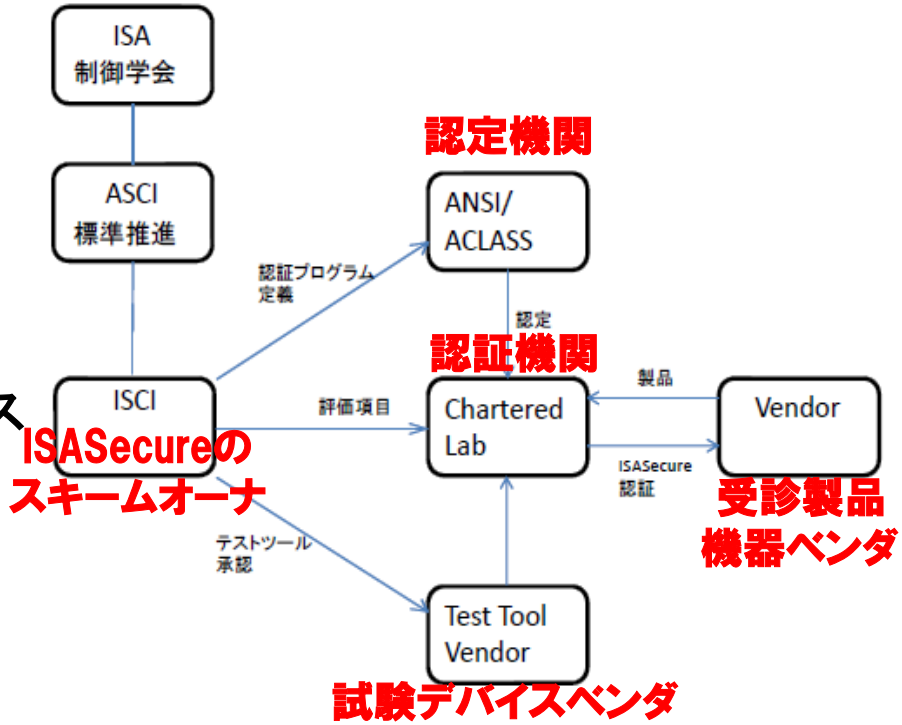
●アセットオーナー（制御システム事業者）、サプライヤ、及び業界組織からなるコンソーシアムで、ISA のAutomation Standards Compliance Institute(ASCI)内に2007年に構築された。

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

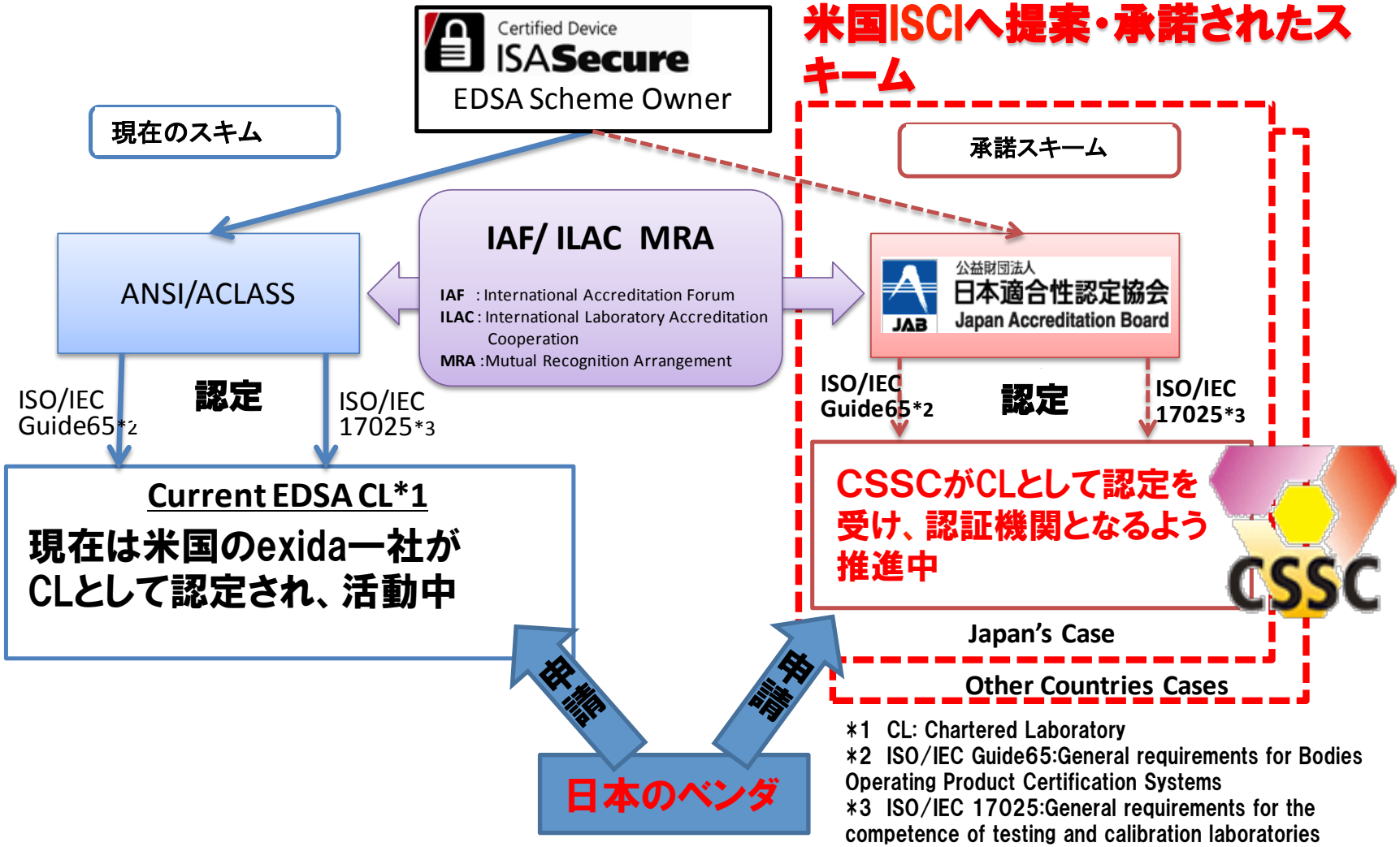
CSSCは、ISCIにアソシエートメンバとして加入（2013.11.26公表）。

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

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

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

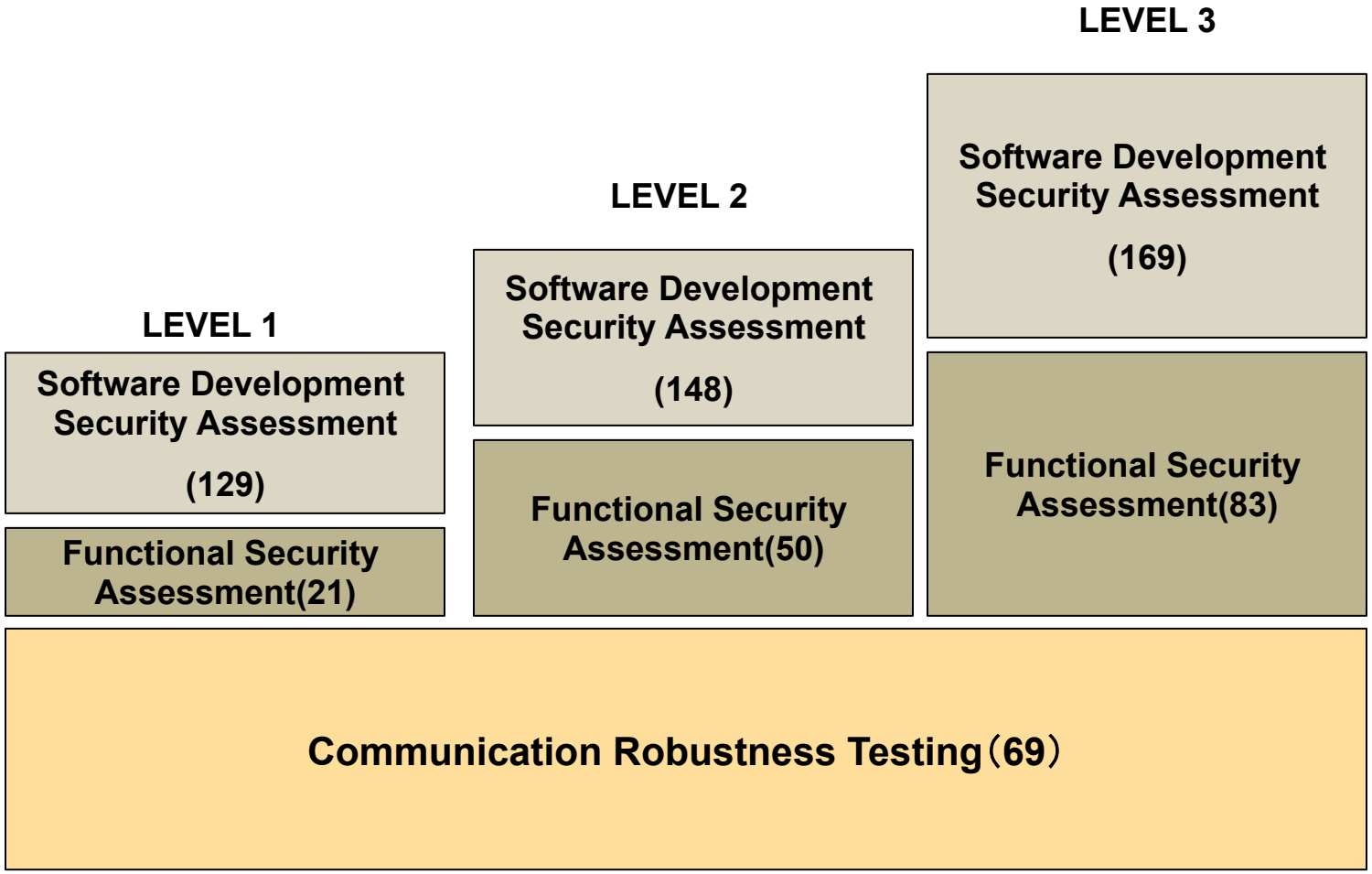
Communication Robustness Testing(CRT), Functional Security Assessment (FSA), Software Development Security Assessment(SDSA)

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-article.pdf

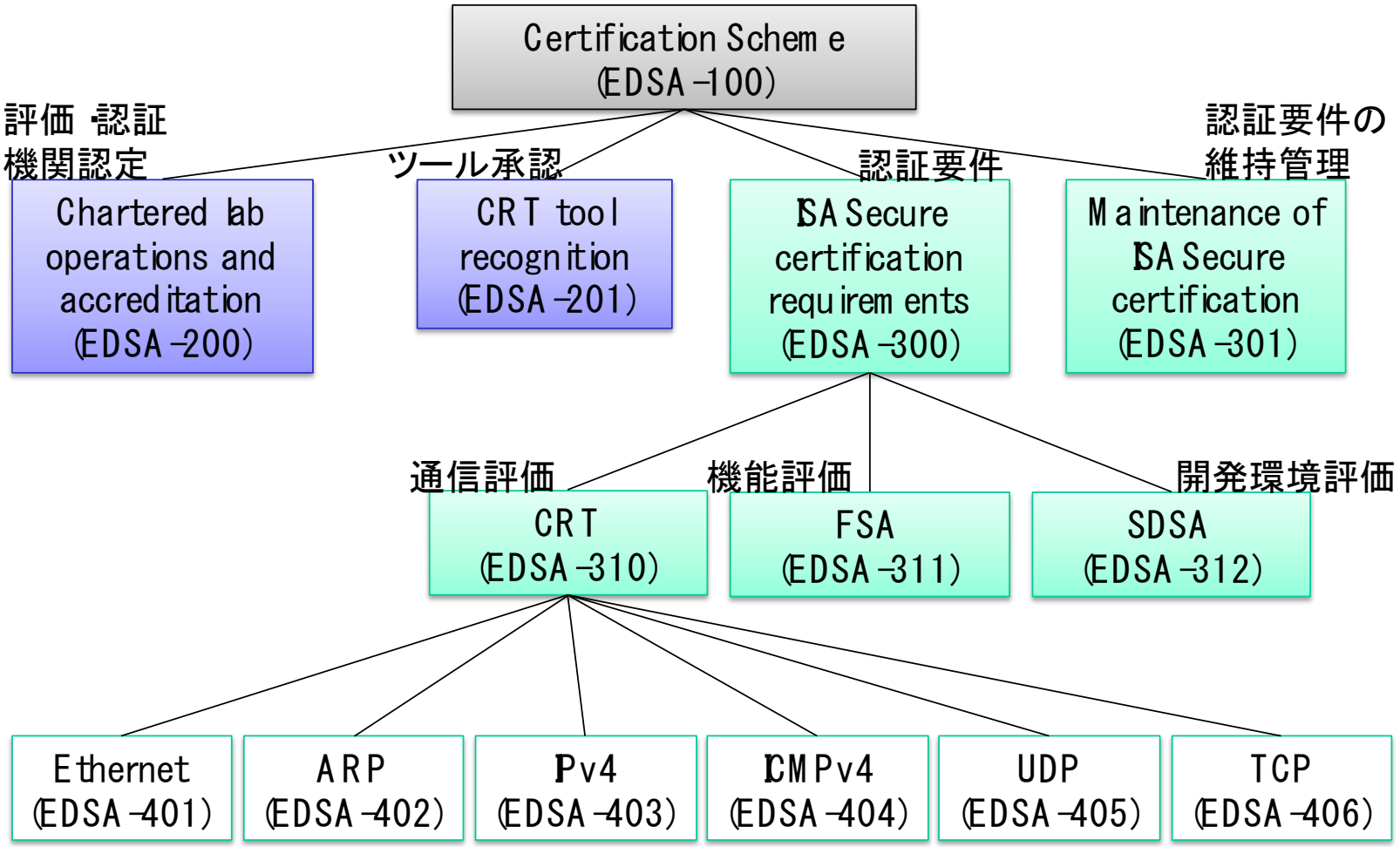
ISASecure 3段階のセキュリティレベル

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

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:

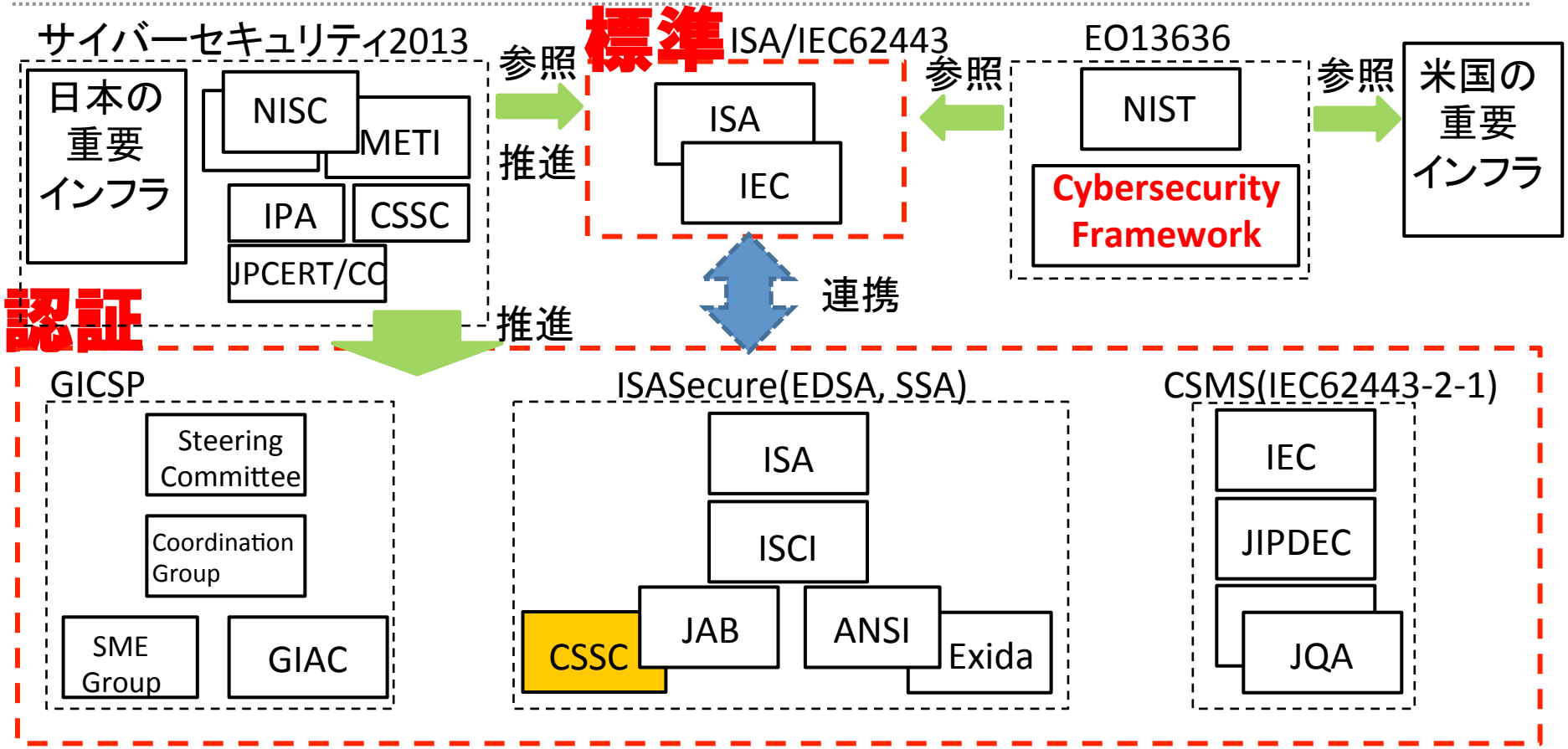
Programmable Logic Controller (PLC), Distributed Control System (DCS) controller
Safety Logic Solver, Programmable Automation Controller (PAC)
Intelligent Electronic Device (IED), Digital Protective Relay
Smart Motor Starter/Controller, SCADA Controller, Remote Terminal Unit (RTU)
Turbine controller,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

- ISASecure EDSA認証取得済組込み機器：

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

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

まとめ　標準と認証 Standard & Certification



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