

制御システムセキュリティセンター ISASecure SSA/SDLA/EDSA認証 説明会

国際的な標準・認証の動向

～制御システムのセキュリティ評価・認証への取り組み～

～IEC/ISA/ISCIとISASecure®の最新動向～

2014年5月14日(東京)、5月22日(大阪)
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
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. 国際的、汎用的な制御システム向け

セキュリティ標準と認証

～IEC/ISA62443、IEC/CAB、ISASecure[®]～

2. EDSA/SSA認証の具体例と

SSA/SDLA/EDSAの認証対象と範囲

3. ISASecure[®] 認証スキームの日本での展開

4. セキュアな日本の重要インフラを実現するためには

多様化する脅威：サイバー攻撃は新しい脅威

サイバー攻撃

重要インフラ・制御システム
も対象に

Stuxnet(破壊、動作異常)、
情報窃取、不正アクセス、
Web改竄、DoS攻撃、ウイルス

社会政治的 災害

9.11テロ、7.7テロ
自爆テロ、大量破壊兵器

コミュニティ
(社会)

自然災害・ 障害

3.11地震、津波、火災、
水害、停電、大型ハリケーン

ハード故障・劣化、 ソフトバグ

動作停止、誤動作、品質不良、
環境汚染

ビジネス (企業)

人為的災害

オペレーションミス
従業員モラル、不法投棄

内部不正

機密情報の持ち出し
不正アクセス、不正操作

ライフ (家庭・個人)

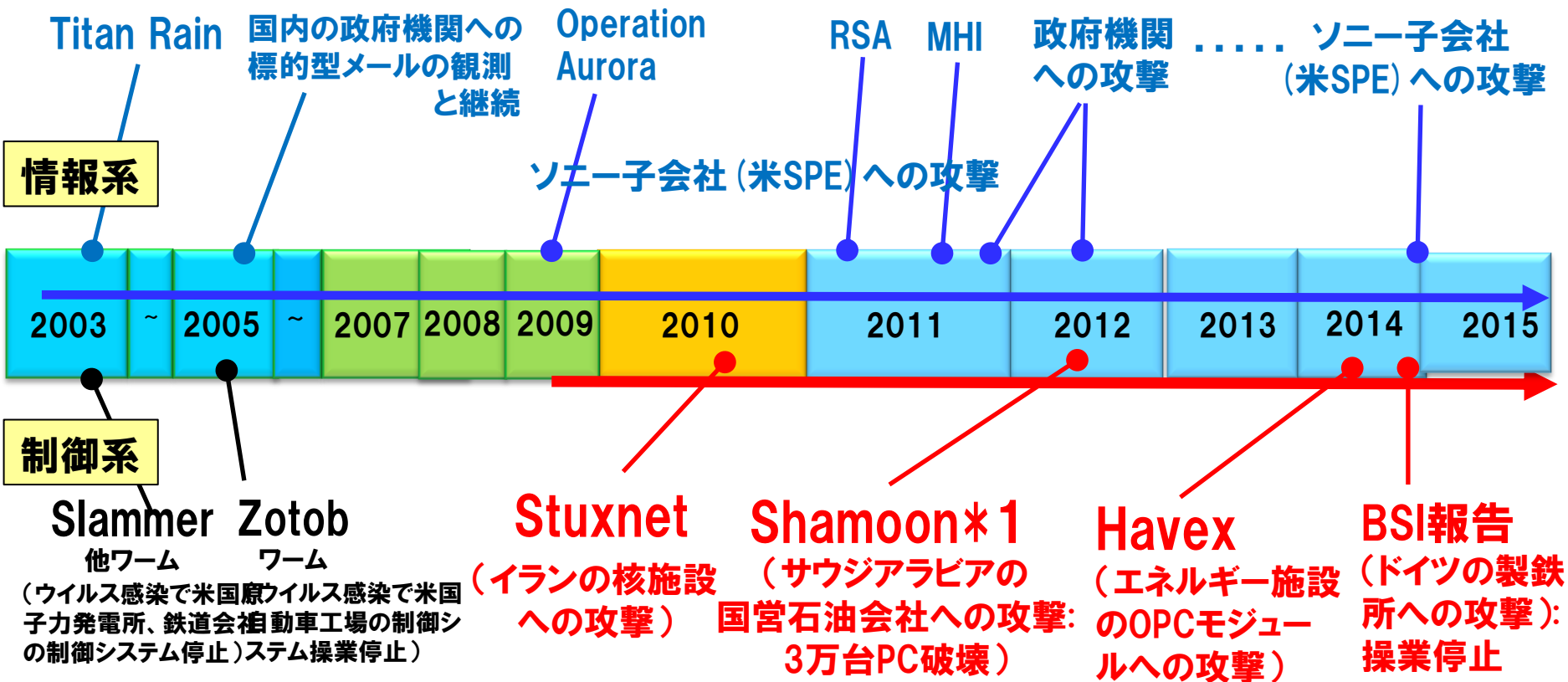
プライバシー 問題

個人情報保護法(05/4施行)
(金融・医療データ等)、
盗聴、盗撮

「サイバー攻撃」の脅威に対する社会的関心増大

参考：重要インフラへの標的型サイバー攻撃の経緯

●標的型攻撃：10年間攻撃が続いており、被害が食止められていない現実



●制御システム：ウイルス感染被害から標的型攻撃の対象になってきている現実

*1:Shamoon: http://www.ipa.go.jp/security/controlsystem/pdf/MonthlyReport_201209.pdf

参考：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/>

参考:ドイツの製鉄所へのサイバー攻撃:操業停止

ドイツ連邦情報技術安全局(BSI)の年次レポート(2014年12月中旬公開。P31):
 ドイツの製鉄所で、サイバー攻撃によって溶鉱炉が正常にシャットダウンできず、
 装置および製鉄システム(操業)に大きな損害を与える事件が発生していた。
 攻撃は、特定の従業員らに対する標的型攻撃を通じて認証情報や機微な情報を
 窃取してOAネットワークに侵入し、その後、生産システムに侵入を拡大。



22 December 2014 Last updated at 13:01



Hack attack causes 'massive damage' at steel works



The hack attack led to failures in plant equipment and forced the fast shut down of a furnace

<http://www.bbc.com/news/technology-30575104>

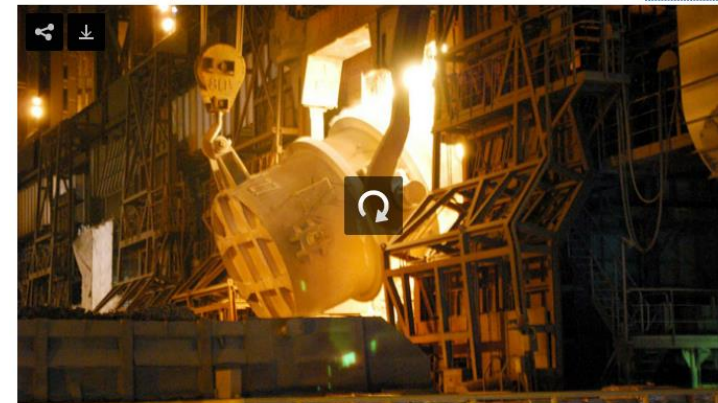
日本ではOAネットワークと
 生産システムは接続されて
 いないと言うが……

Cyberattack on German steel mill inflicts serious damage

Published time: December 21, 2014 02:17

Edited time: December 21, 2014 09:20

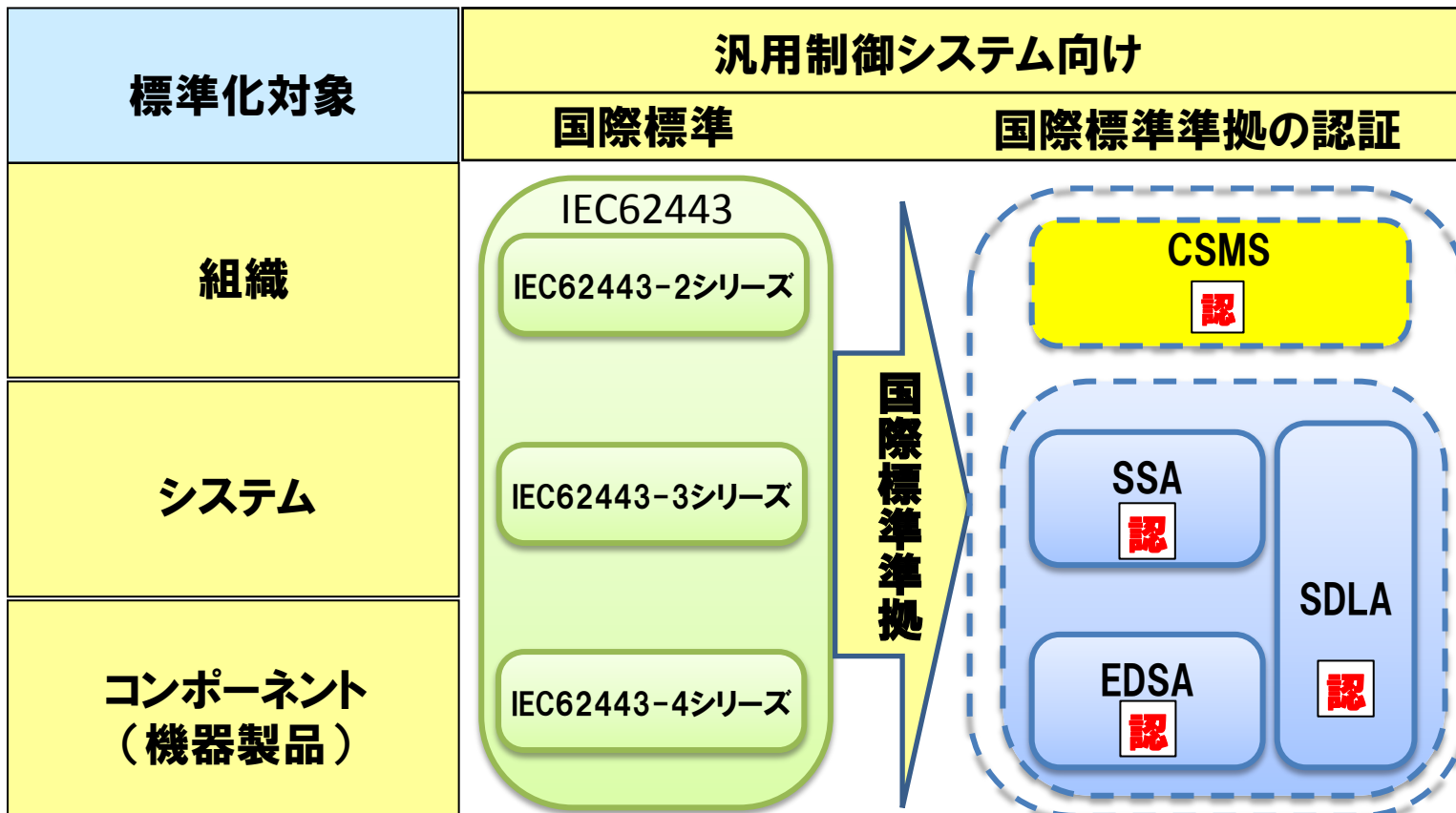
[Get short URL](#)



Download video (9 MB)

<http://rt.com/news/216379-germany-steel-plant-hack/>

国際的、汎用的な制御システム向けセキュリティ標準と認証



■制御システム事業者向けセキュリティマネジメントのCSMS(IEC62443-2-1)認証が日本(JIPDEC)で推進されている。
 ■制御システムや制御機器向けEDSA(IEC62443-4)やSSA(IEC62443-3)認証が世界(ISA/ISCI)で推進されている。

CSMS: Cyber Security Management System EDSA: Embedded Device Security Assurance
 SSA: System Security Assurance SDLA: Security Development Lifecycle Assurance

ISASecure® はIEC62443適合認証 (2015/2 ISCI HP更新)

 **ISASecure®** **IEC 62443 CONFORMANCE CERTIFICATION**
 Certifying Industrial Control System Devices and Systems

HOME ABOUT US CONTACT 



SEE HOW OUR CERTIFICATIONS HELP REDUCE RISKS IN YOUR INDUSTRY 

ISA SECURE CERTIFIED DEVICES
 View Complete List

認証取得製品

SSA ← IEC62443-3-3
 IEC 62443-3-3: Requirements for System Security Assurance (SSA) Certification

EDSA ← IEC62443-4-2
 IEC 62443-4-2: Requirements for Embedded Device Security Assurance (EDSA) Certification

SDLA ← IEC62443-4-1
 IEC 62443-4-1: Requirements for Security Development Lifecycle Assurance (SDLA) Certification

News MORE NEWS  **Certification Specs** **Blogs** MORE BLOGS 

24 MAR Automation Federation releases report commissioned by LOGIIC that studies the us...
 The Automation Federation announced today that it has released a public report—commissioned on behalf of the Linking Oil and Gas Industry to imp...
 Read More

02 FEB WisePlant HQ joins ISA Security Compliance Institute support for the ISASecur...
 WiseSecurity, an independent division of WisePlant HQ, has announced today its support for the ISASecure® Cyber Security Conformance Sc...
 Read More

05 FEB 2014 Year In Review...
 ISA Security Compliance Institute 2014 Year in Review Before charging into the challenge... Read More

ISCI/ISASecure[®] EDSA 認証取得製品 (2015.5現在)

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 Electric Corporation	Safety Control System	ProSafe-RS	R3.02.10	EDSA 2010.1 Level 1
Yokogawa Electric Corporation	DCS Controller	CENTUM VP	R5.03.00	EDSA 2010.1 Level 1
Hitachi, Ltd.	DCS Controller	HISEC 04/R900E	01-08-A1	EDSA 2010.1 Level 1
Azbil Corporation	DCS Controller	Harmonas/Industrial-DEO/ Harmonas-DEO system Process Controller DOPCIV (Redundant type)	R4.1	EDSA 2010.1 Level 1
Schneider Electric	Field Control Processor	Field Control Processor 280 (FCP280)	S91061	EDSA 2010.1 Level 1

6社9製品(内日本3社4製品)

IEC適合性評価評議会CABのWG17：サイバーセキュリティ

2014年、適合性評価評議会CAB配下にサイバーセキュリティの適合性評価を検討するWG17が設置され、IEC62443他を利用したIEC適合性評価の検討が開始された。

市場が国際的な標準・認証を求めてきた

International Electrotechnical Commission
International Standards and Conformity Assessment for all electrical, electronic and related technologies

myIEC | Subscribe | Sitemap | FAQs | Contact us

You & the IEC | About the IEC | News & views | Standards development | Conformity assessment | Members & experts | Developing countries | Webstore | Search... | Advanced search

About the IEC > Who we are > Management Structure > CAB

CAB Conformity Assessment Board

Scope | Structure | Documents | CABPUB Documents | CABPUB Documents open for vote | Working Groups | Meetings

Log in | En | Fr

CAB Working Groups

Committee	Description
WG 10	CAB Policy and Strategy
WG 11	Systems issues
WG 14	Promotion
WG 16	Systems Approach in CA
WG 17	Cyber Security
WG STF	Special Task Force on CB-TF recommendations

Task

The CAB establishes Working Groups (WGs) to accomplish tasks within its responsibilities which require more, or more specialized, preparation and discussion than can be accommodated within the framework of the twice-yearly CAB meetings. Terms of reference and membership are decided in advance for each WG. WGs report regularly to the CAB, and any conclusions or decisions arising from their work are placed on the CABs agenda and decided there. WGs are normally of limited duration and are disbanded by the CAB when no longer needed.

http://www.iec.ch/dyn/www/f?p=103:89:0::::FSP_ORG_ID,FSP_LANG_ID:3250,25

ISASecure® 認証の現状 (2015年5月にISCI公開予定)

3つの認証

制御機器認証

セキュリティ開発ライフサイクル
のプロセス認証

制御システム認証

EDSA

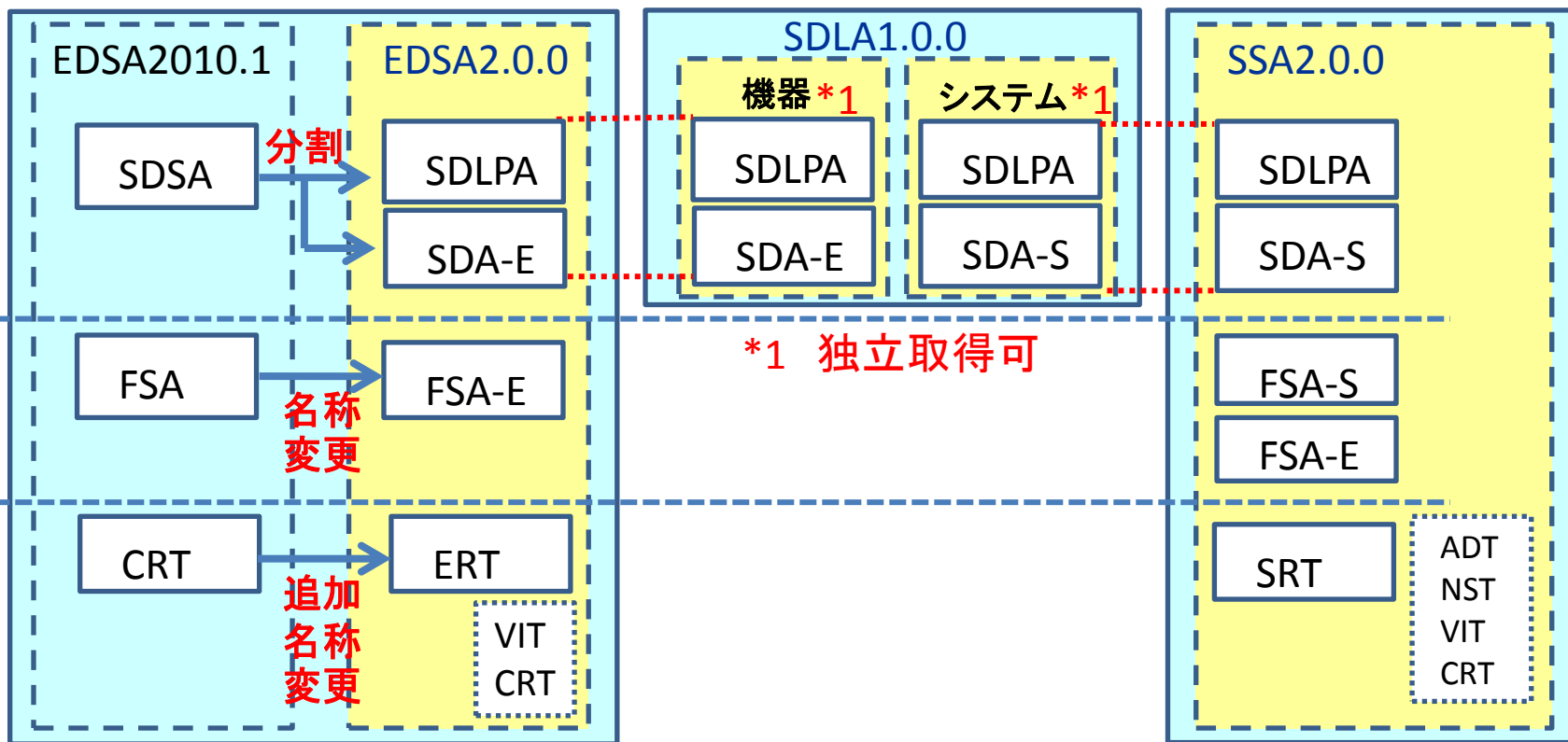
SDLA

SSA

セキュリティ
開発ライフ
サイクル
評価

セキュリティ
機能評価

ロバスト
ネス
試験



EDSA: Embedded Device Security Assurance SSA: System Security Assurance

SDLA: Security Development Lifecycle Assurance

参考: SSAの審査項目

項目		内容
SRT	ADT: Asset Discovery Testing	ポートスキャンによるパッシブな探索
	CRT: Communication Robustness Testing	ツールによるファジングテスト
	NST: Network Stress Testing	ツールによるネットワーク負荷テスト
	VIT: Vulnerability Identification Testing	Nessusによる既知脆弱性探索
FSA-S: Functional Security Assessment for System		システムのセキュリティ機能アセスメント
SDA-S: Security Development Artifacts for System		システムのセキュリティ開発記録評価
SDLPA: Security Development Lifecycle Process Assessment		組織のセキュリティ開発プロセス保証
(FSA-E): Functional Security Assessment for Embedded Device Components		EDSA認証を受けていない機器については、レベル1相当のセキュリティ機能をもつことを確認

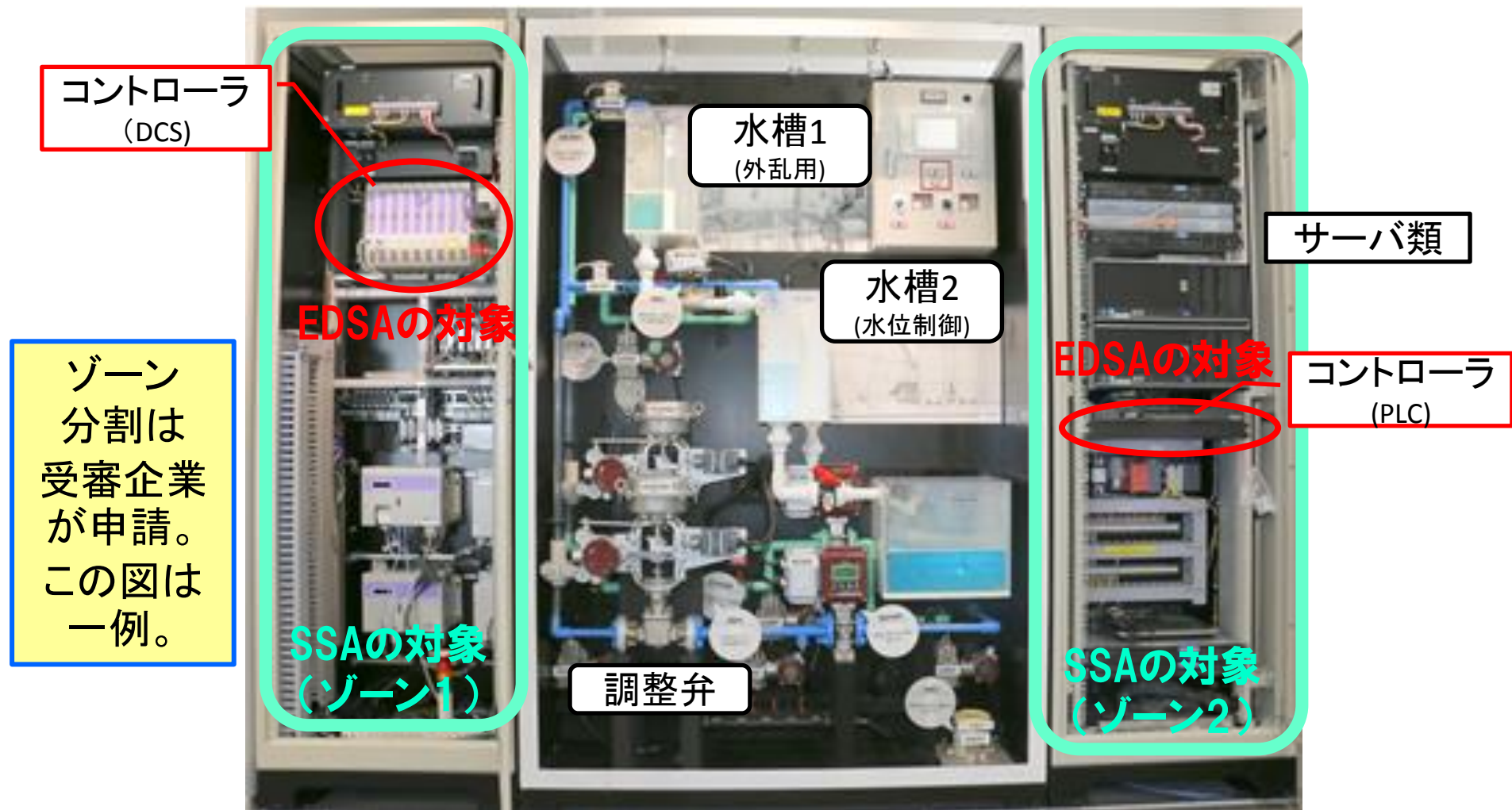
SRT: System Robustness Testing

参考:EDSAの審査項目

項目		内容
ERT	CRT: Communication Robustness Testing	ツールによるファジングテスト
	VIT: Vulnerability Identification Testing	Nessusによる既知脆弱性探索
FSA-E: Functional Security Assessment for Embedded Device Components		セキュリティ機能をもつことを確認
SDA-E: Security Development Artifacts for Embedded Device Components		セキュリティ開発記録評価
SDLPA: Security Development Lifecycle Process Assessment		組織のセキュリティ開発プロセス保証

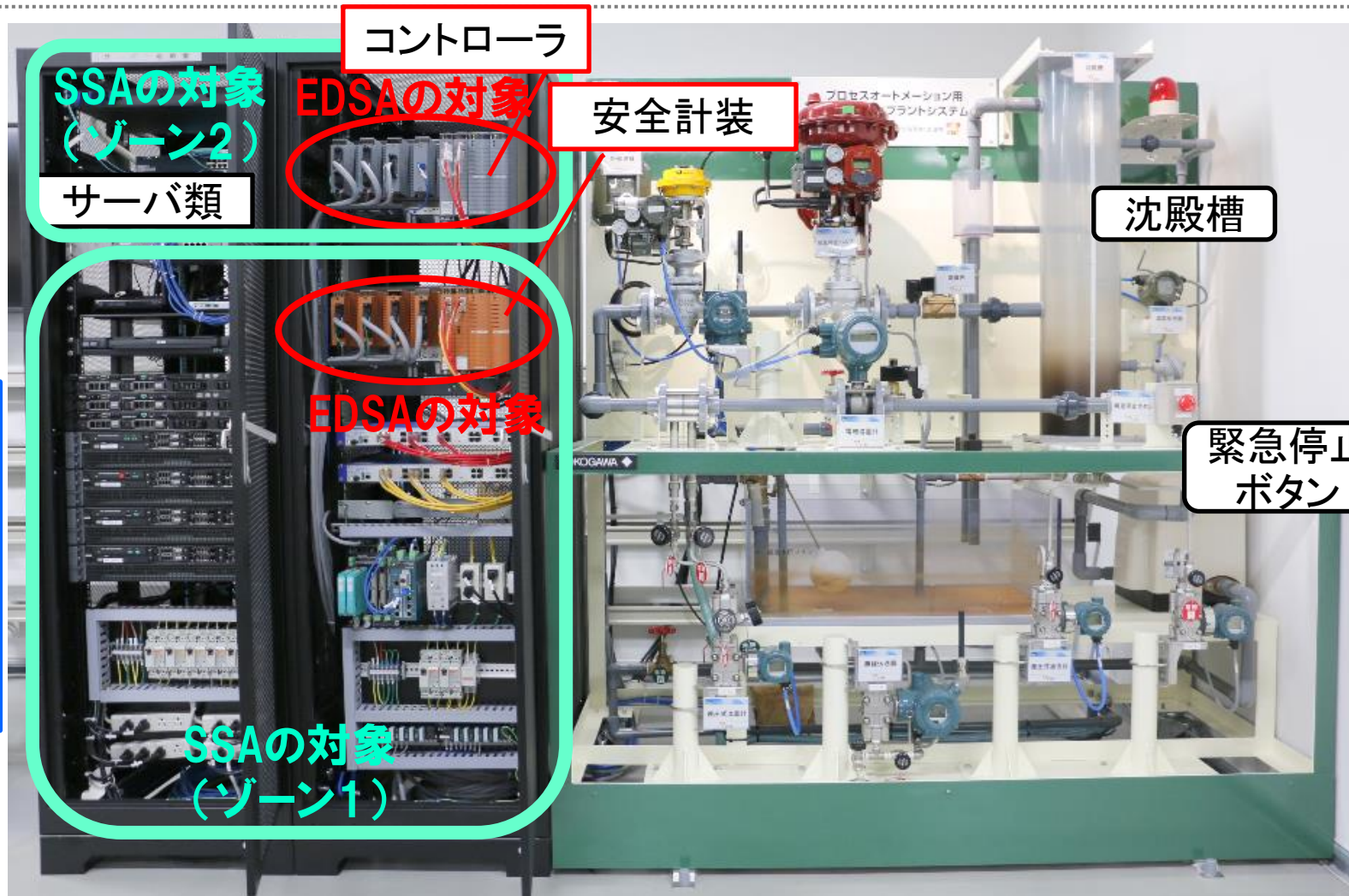
ERT: Embedded device Robustness Testing

EDSA認証とSSA認証の具体例：化学プラント



中央に設置されている水槽2の水位一定制御を行っている
 上段に設置されている水槽1は水槽2の水位を変化させる外乱要素となる

EDSA認証とSSA認証の具体例：排水・下水処理プラント



SSAの対象
(ゾーン2)

サーバ類

コントローラ

EDSAの対象

安全計装

沈殿槽

緊急停止
ボタン

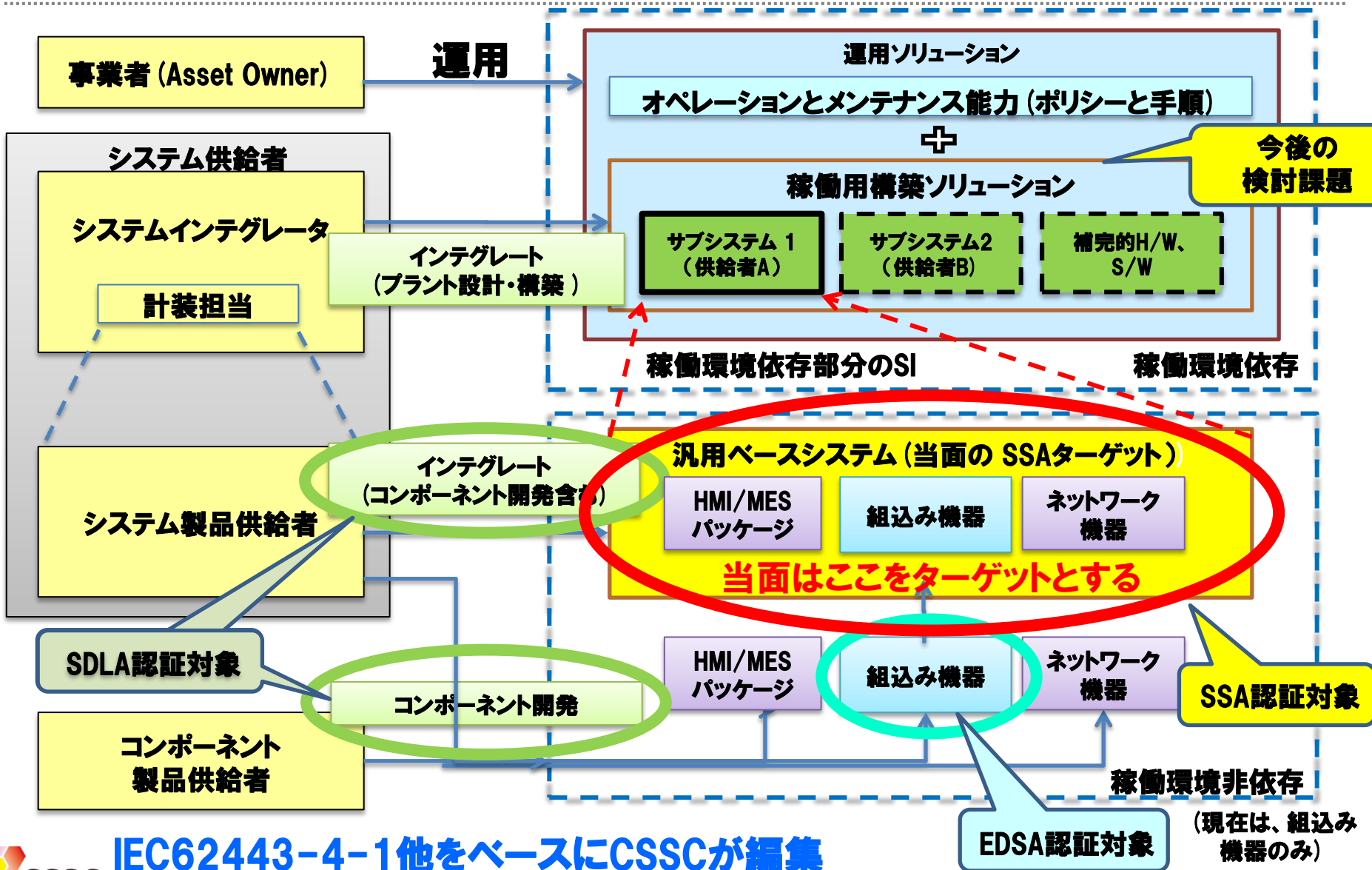
EDSAの対象

SSAの対象
(ゾーン1)

ゾーン
分割は
受審企業
が申請。
この図は
一例。

下水処理で多く用いられている汚泥と水の分離を行う沈殿槽の一部を模擬している
コントローラは流入水量が一定となるように制御している

SSA/SDLA/EDSA認証対象と範囲



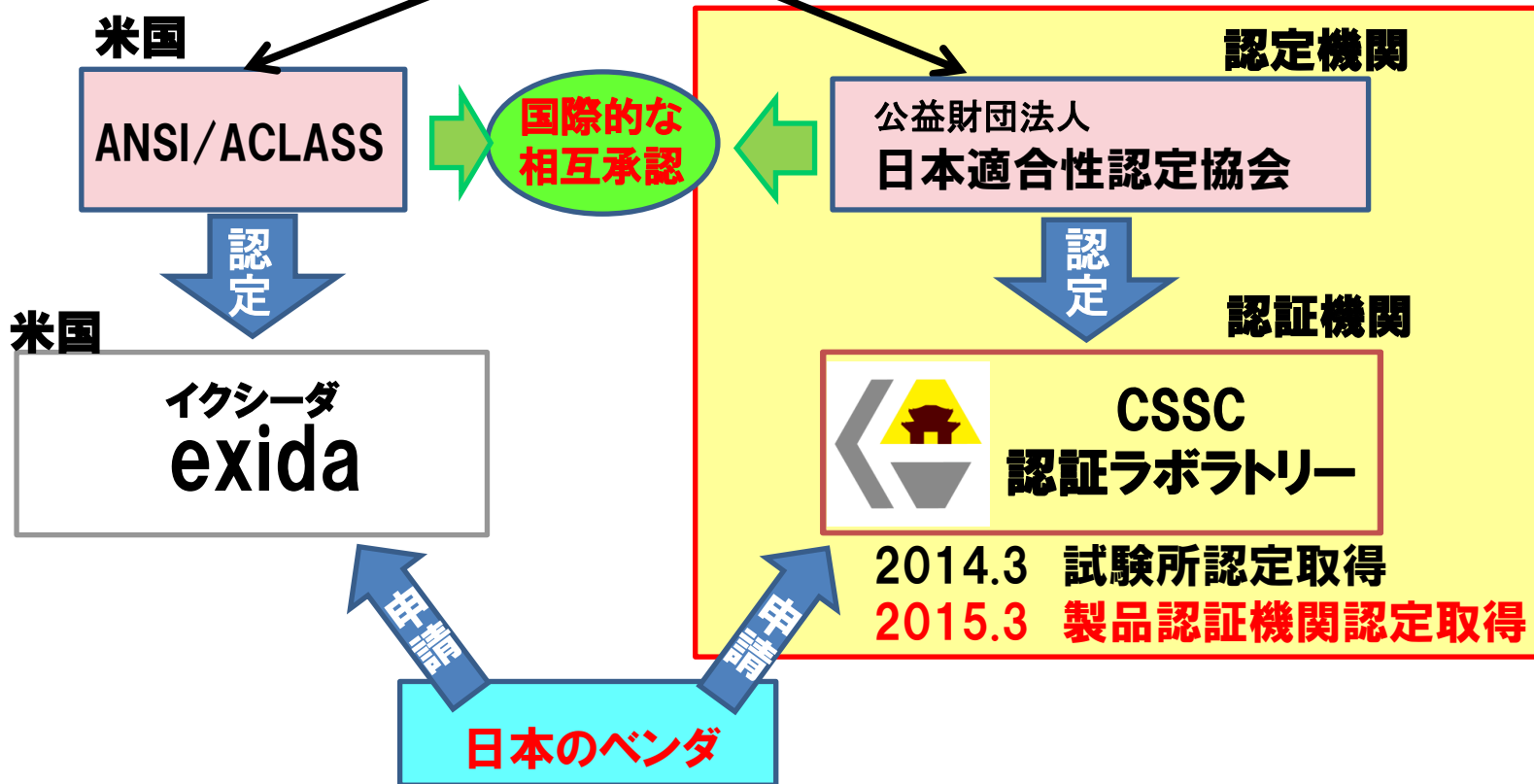
IEC62443-4-1他をベースにCSSCが編集

ISASecure[®] 認証スキームの日本での展開

ISASecure[®]
 スキームオーナー: ISCI

2014.4.1よりEDSA認証実証開始

2016年度初SSA/SDLA認証実証開始目標



日本で日本語による世界共通の認証取得が可能

参考:セキュアな重要インフラを実現するためには

海外では既にIEC62443を活用する活動が進んでいる。IEC62443国際標準の活用状況を示す。

1)オバマ大統領指令による米国の国立標準技術研究所NIST策定の重要インフラ事業者向け**サイバーセキュリティ・フレームワーク**の5つのコア機能(特定、防御、検知、対応、復旧)の参照標準として、ISA62443がポイントされている。

←任意の標準であるが、重要インフラ事業者へのベストプラクティスとなるよう米政府推進

2)制御システムのセキュリティ標準や認証が着実に普及されるためには電力事業者や石油・化学等の事業者が、標準・認証を認識し、調達に指定するのが効果的である。

例えば、**ロイヤル・ダッチ・シェル、シェブロン**など石油関連の国際的大企業の調達要件にIEC62443を指定する動きが出てきている。電力ではNERC CIP標準がある。

←国内ベンダへの調達条件となる。石油・化学分野の国内制御システムベンダが対応中。

3)2014年3月には**アメリカ食品医薬品局FDA**が、ISA/IEC62443をFDAの**認定共通標準リスト**に追加したと発表している。**医療機器分野**でも組み込み機器が多く採用されてきていることからセキュリティ標準への対応が急務となってきている。ISCIでは、さらに**ビル分野**など幅広い分野へのIEC62443準拠の認証の拡大普及を促進する活動をしている。

←業界認定標準への採用推進。2020年オリンピック・パラリンピックに向けて、関係する重要インフラ(通信、電力、ビル/施設、運輸など)業界での認定標準化を官民で推進要。

4) **サイバーセキュリティ基本法第14条**:重要インフラ事業者等におけるサイバーセキュリティの確保の促進<国は、重要社会基盤事業者等におけるサイバーセキュリティに関し、**基準の策定**、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずるものとする。>

5)日本では**METI、IPA、JIPDEC、CSSC**が**制御システムセキュリティの国際標準としてIEC62443を位置づけ**、国際標準IEC62443準拠の認証を立ち上げている。

←日本のセキュアな重要インフラ実現に向け標準及び認証製品の採用・活用を官民で推進要。

参考：制御システムセキュリティ標準・認証のメリット

制御システムセキュリティ標準・認証のメリット		参考情報
利用者	<ul style="list-style-type: none"> 一定レベルの標準を採用している企業や業界に対して信用・信頼感、安心・安全を持てる。企業を選択ができる。 	
重要 インフラ 事業者	<ul style="list-style-type: none"> 標準活用の教育制度確立により従業員の教育、さらに資格化取得での人材育成 自社システムが標準準拠で構築・運用していることで、利用者(国民)への信用・信頼感をアピール、及び規制への対応。 一定レベルのセキュリティレベルを確保していることが、社会的に企業の存続理由となる。CSR他ブランドイメージ向上。 SCM下流へ標準準拠を調達要求に活用することにより、トータルセキュリティ向上、および検収コスト低減 標準準拠・認証品納入を機器・システム調達要求に活用することにより、トータルセキュリティ向上、検収コスト低減、納期短縮等を実現。(自社でペネトレーションテストのような試験を実施しないで済む。) 国際標準準拠の第三者認証による信用・信頼感の確保。国際レベルに標準準拠を客観的に説明できる。 業界標準として設定することにより航空や船舶などグローバルなセキュリティ確保や業界でのセキュリティレベルの向上が実現できる。(インシデントによる事故対応費用が低減できる、) 	<ul style="list-style-type: none"> シェル等のGICSP 米国のCybersecurity FrameworkやNERCのCIP等 サイバーセキュリティ基本法 石油・化学業界 石油・化学業界、ベライゾンなどの通信事業者 トヨタの事例 米国航空宇宙工学協会(AIAA) 米食品医薬品局(FDA)
システム ・機器 供給者	<ul style="list-style-type: none"> 標準活用の教育制度確立により従業員の教育、さらに資格化取得での人材育成 自社が標準準拠で機器やシステムを開発していることで、事業者への信用・信頼感をアピールできる。一定レベルのセキュリティレベルを確保する活動をしていることが、社会的に企業の存続理由となる。CSR他ブランドイメージ向上。 機器やシステムの調達に標準準拠を調達要求に活用することにより、ペネトレーションテストやファジングの実施工数や期間の低減ができる。 標準準拠と記載することで、機器などの調達仕様を明確にすることができる。 要求仕様が明確になるので、不正確さによる追加作業を減らすことができる。 	<ul style="list-style-type: none"> 横河等のGICSP推進 米国のNERCのCIP等 サイバーセキュリティ基本法

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認証ラボラトリー ホームページ

<http://www.cssc-cl.org/>

CSSC説明ビデオ(日本語版)

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