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

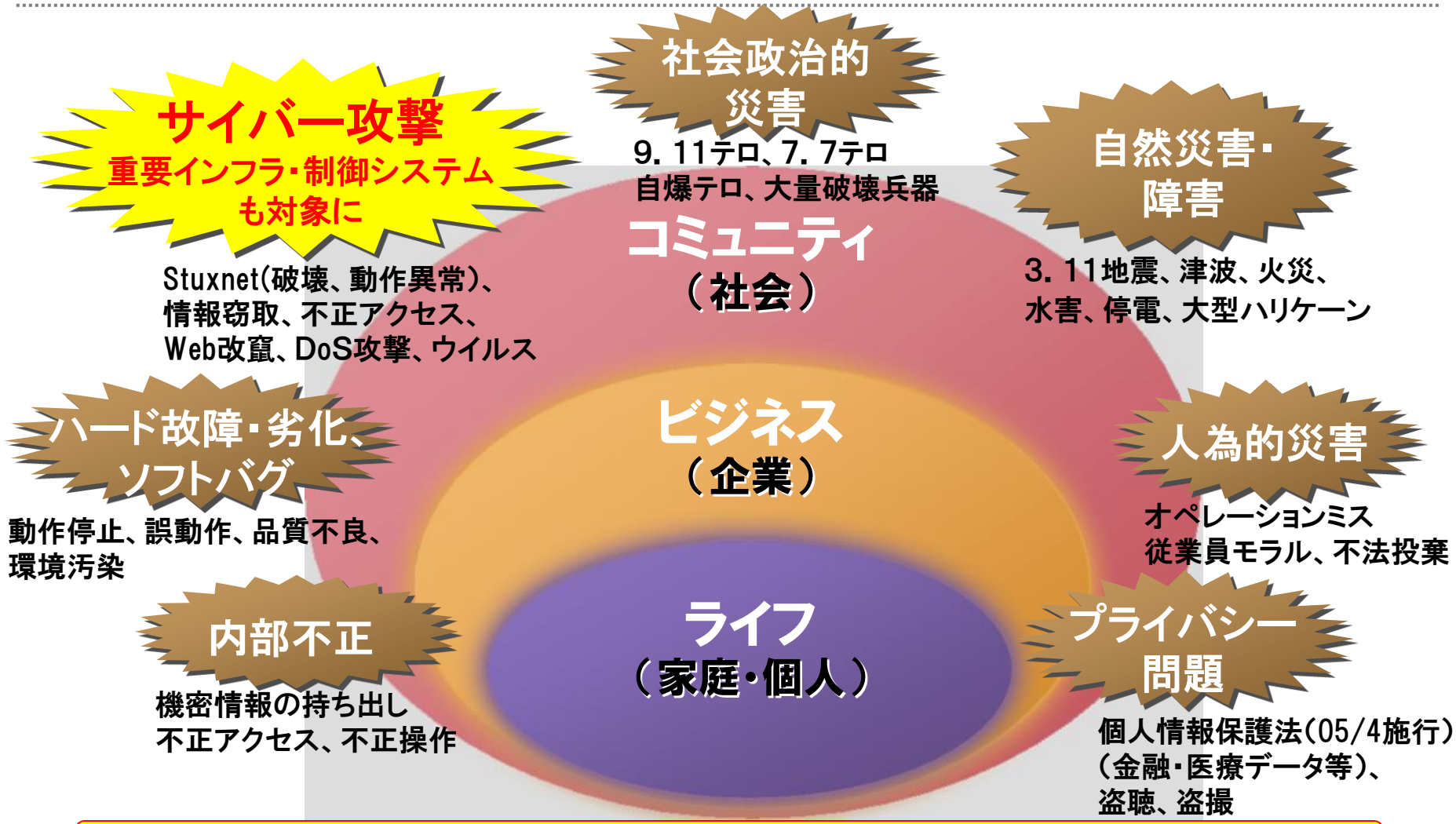
専務理事
CSSC認証ラボラトリー最高責任者

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

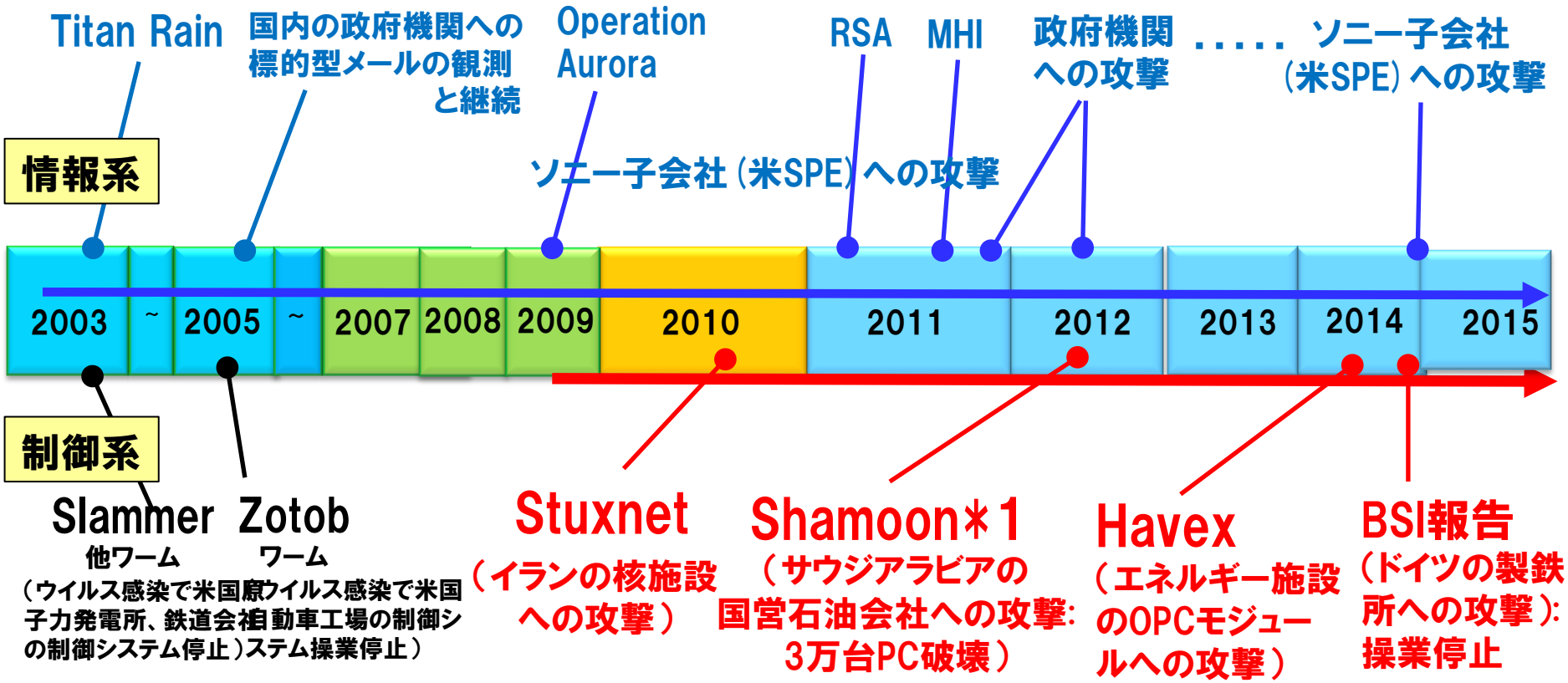
多様化する脅威：サイバー攻撃は新しい脅威



「サイバー攻撃」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。

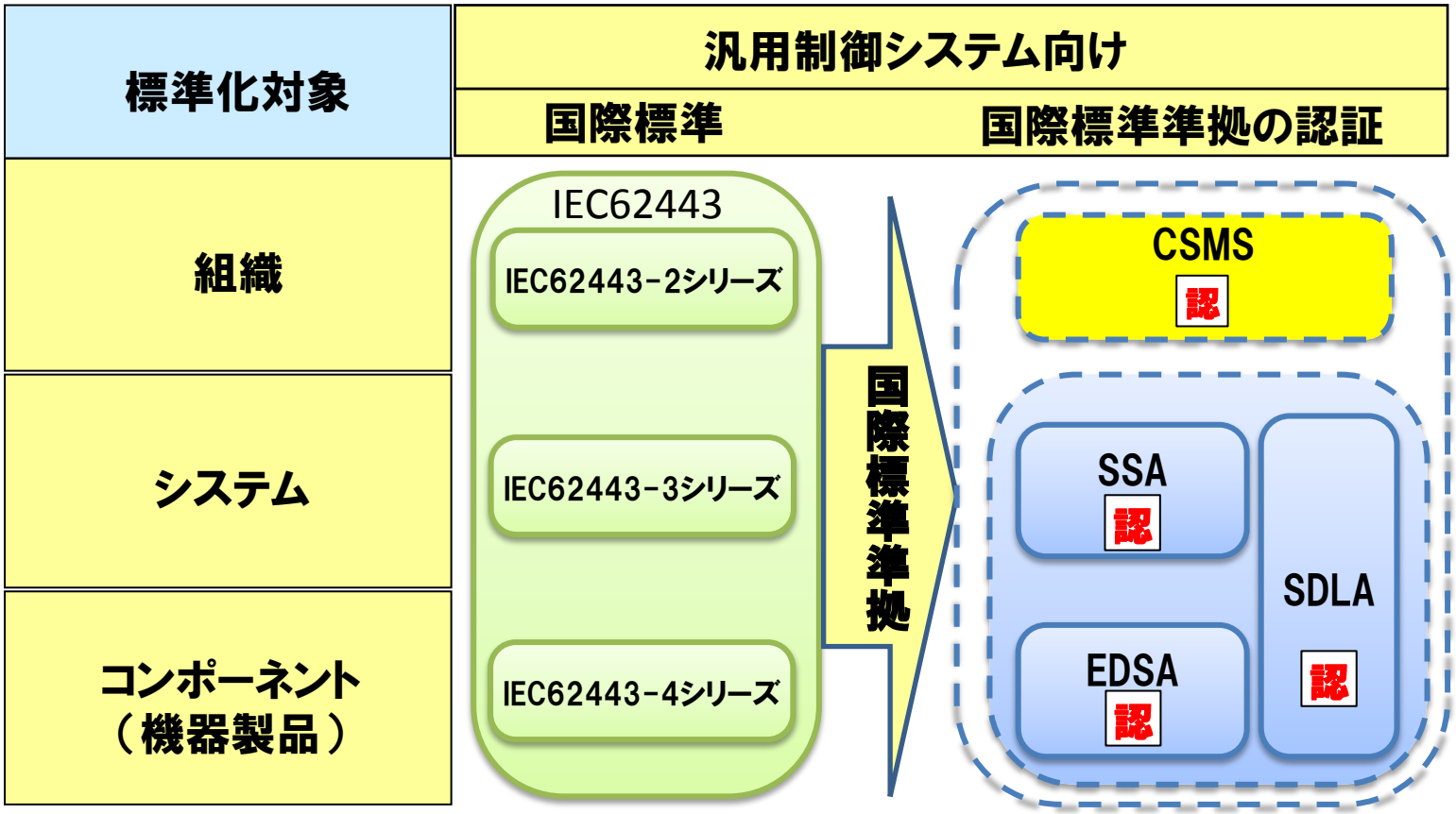
http://www.bbc.com/news/technology-30575104

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・・・・

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

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

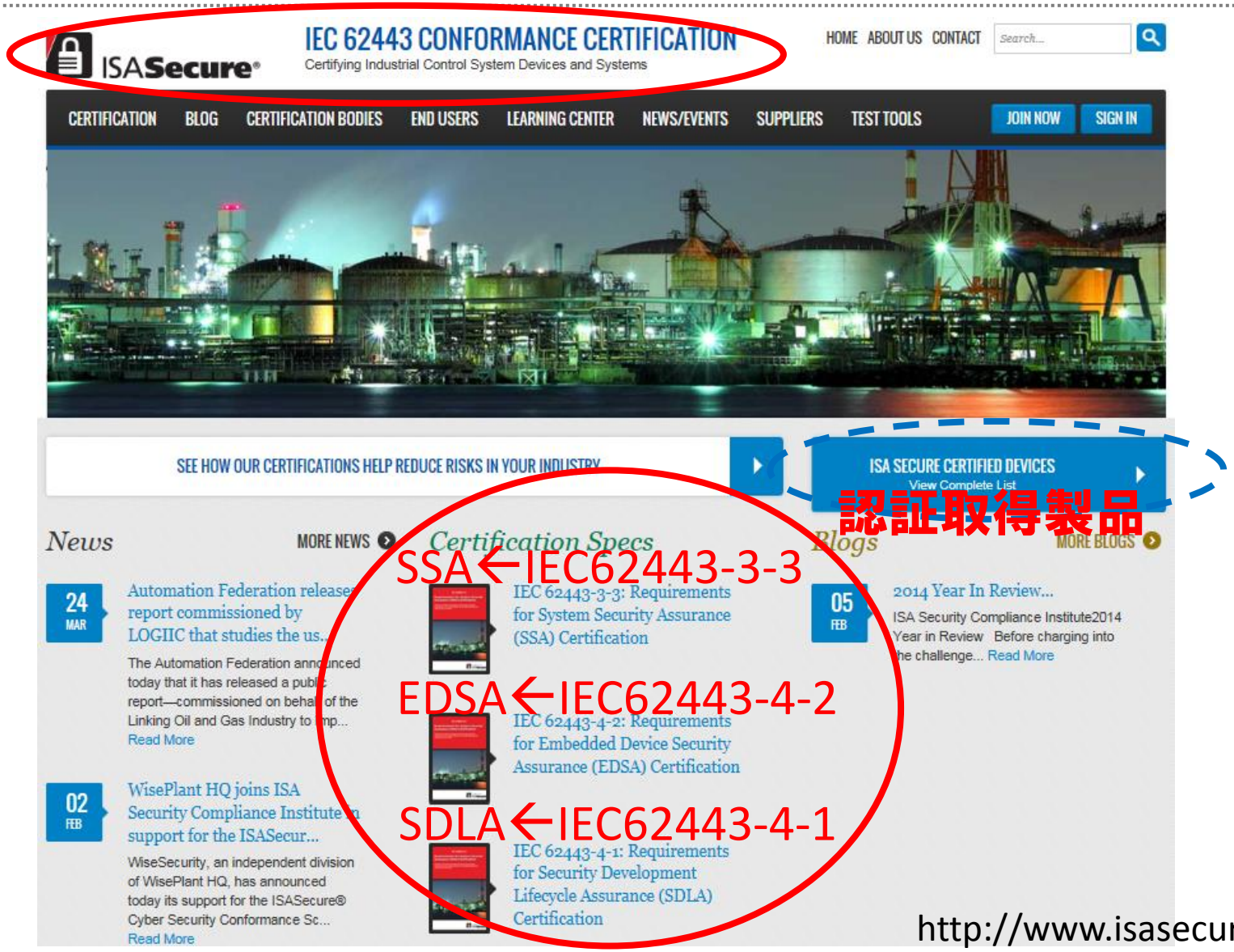
国際的、汎用的な制御システム向けセキュリティ標準と認証



■制御システム事業者向けセキュリィマネージメントの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）



http://www.isasecure.org/

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

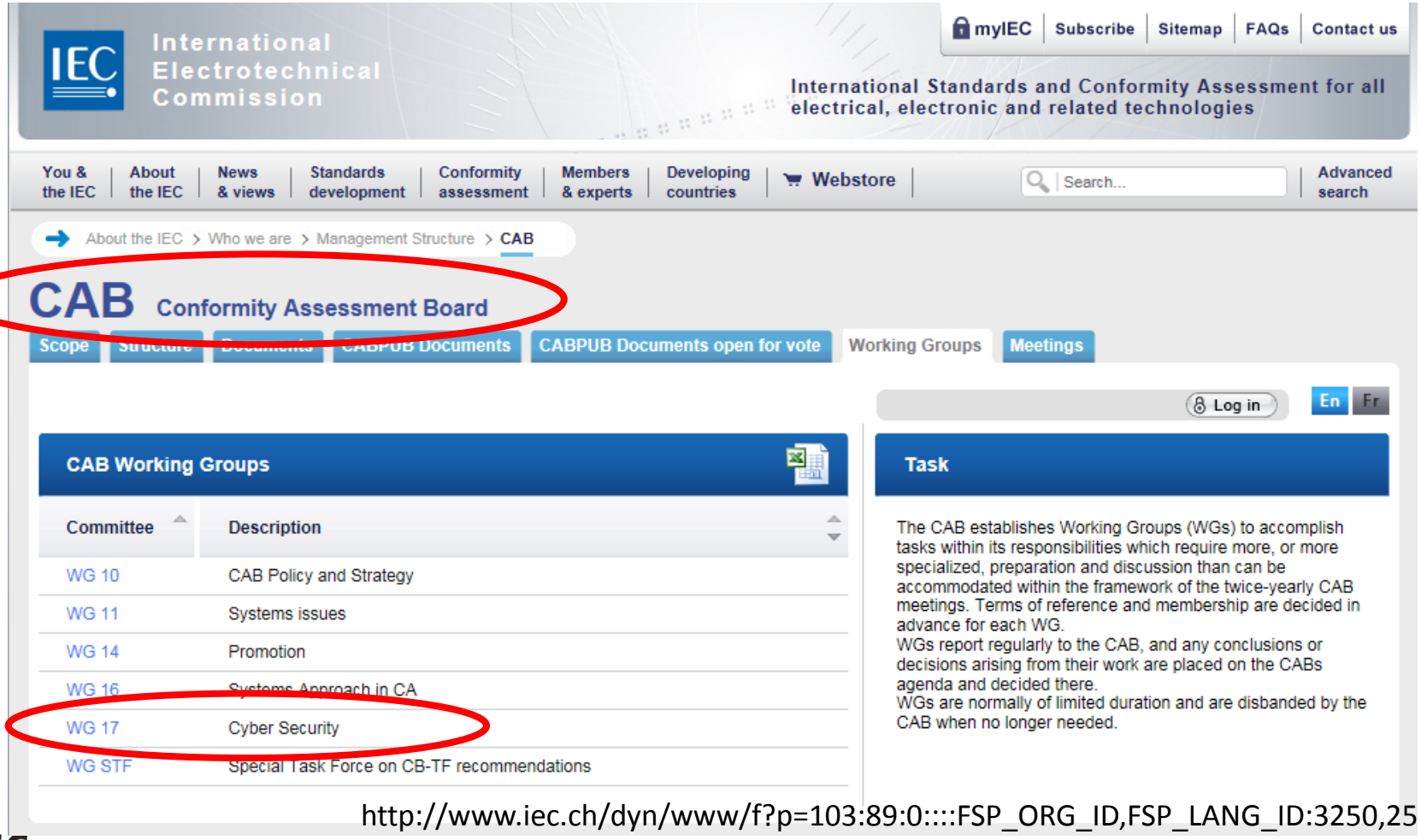
Supplier	Type	Model	Version	Level
Honeywell Process Solutions	Safety Manager	HPS 1009077 C001	R145.1	EDSA 2010.1 Level 1
RTP Corporation	Safety manager	RTP 3000	A4.36	EDSA 2010.1 Level 2
Honeywell Process Solutions	DCS Controller	Experion C300	R400	EDSA 2010.1 Level1
Honeywell Process Solutions	Fieldbus 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

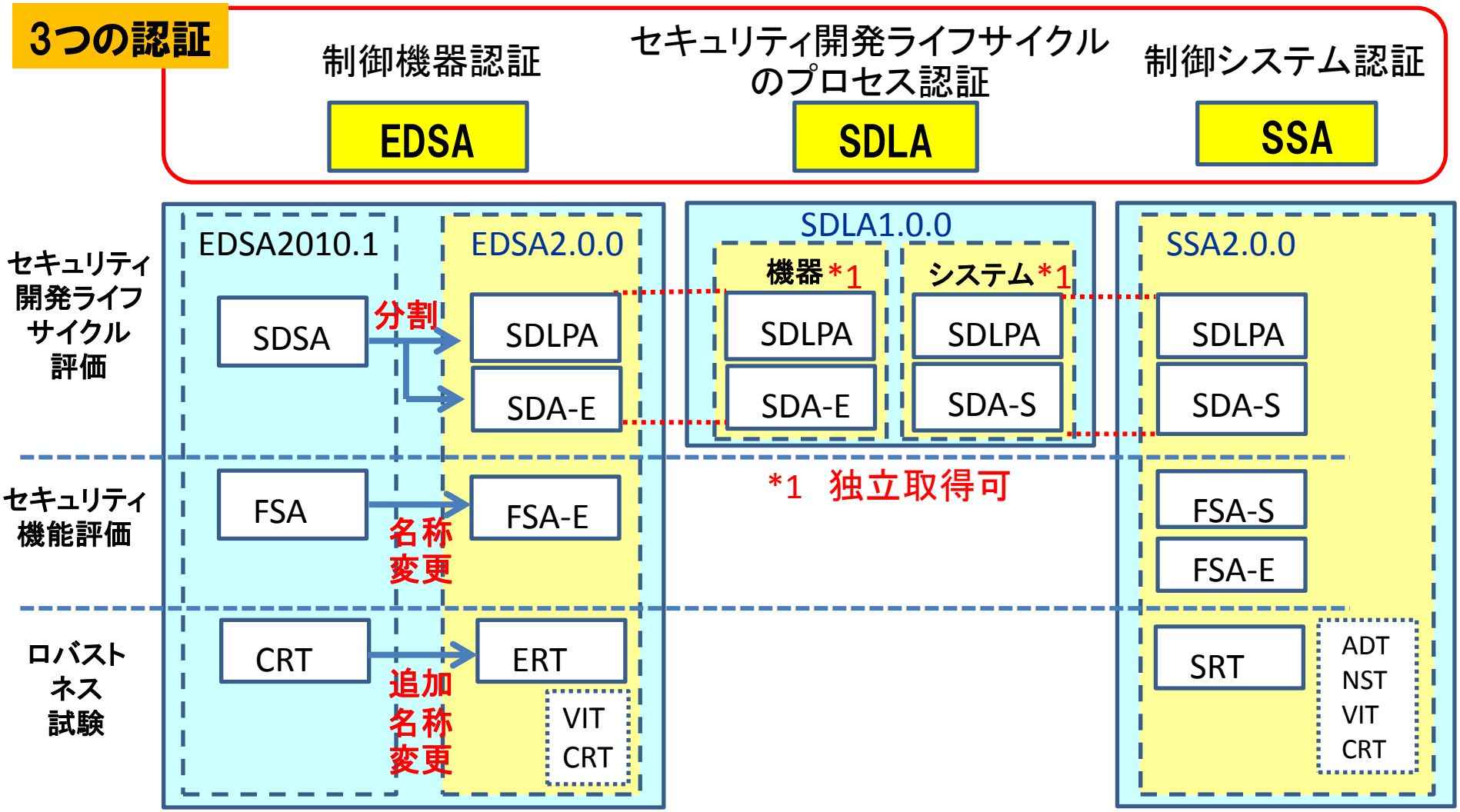
2014年、適合性評価評議会CAB配下にサイバーセキュリティの適合性評価を検討するWG17が設置され、IEC62443他を利用したIEC適合性評価の検討が開始された。

市場が国際的な標準・認証を求めてきた



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）



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

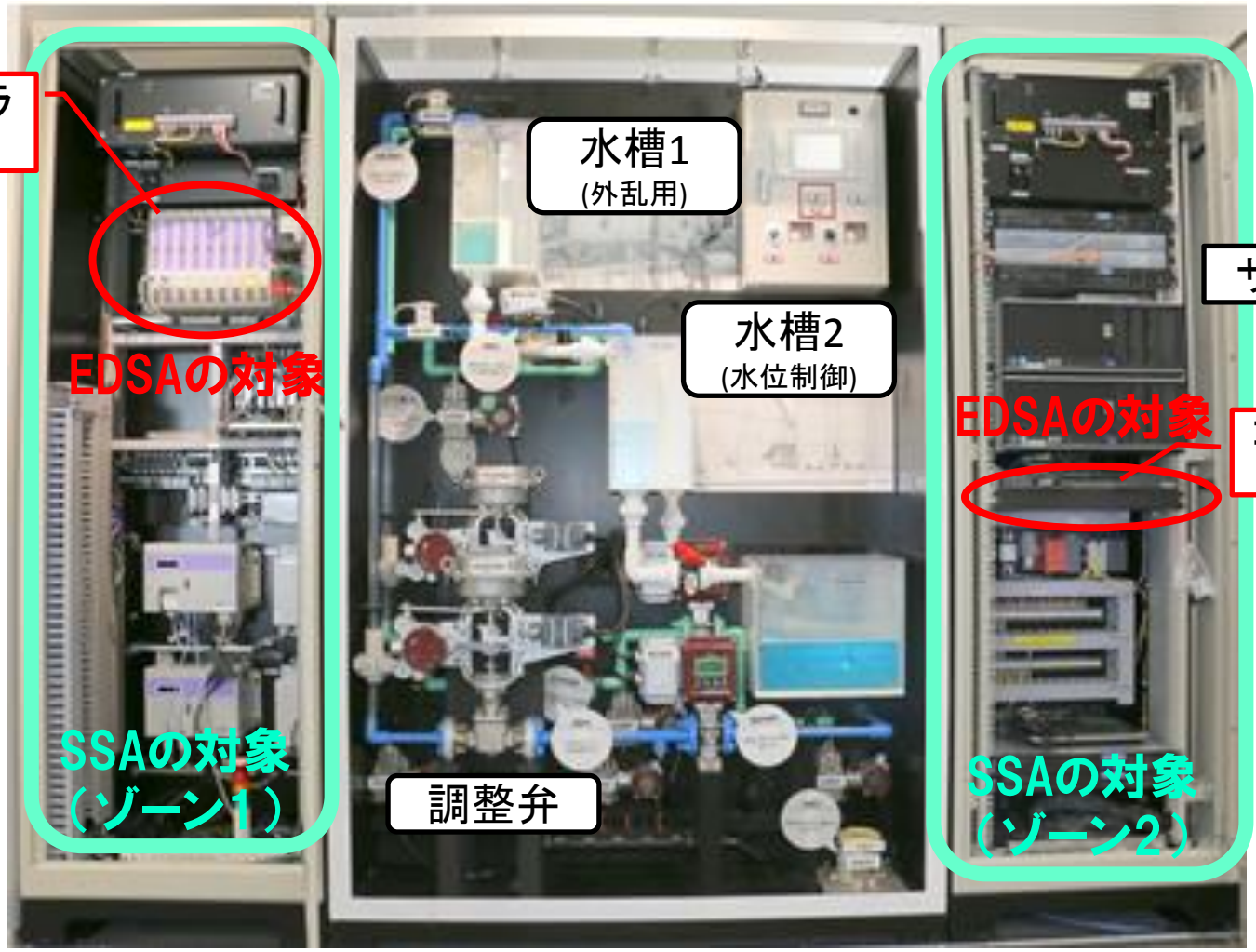
SRT: System Robustness Testing

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

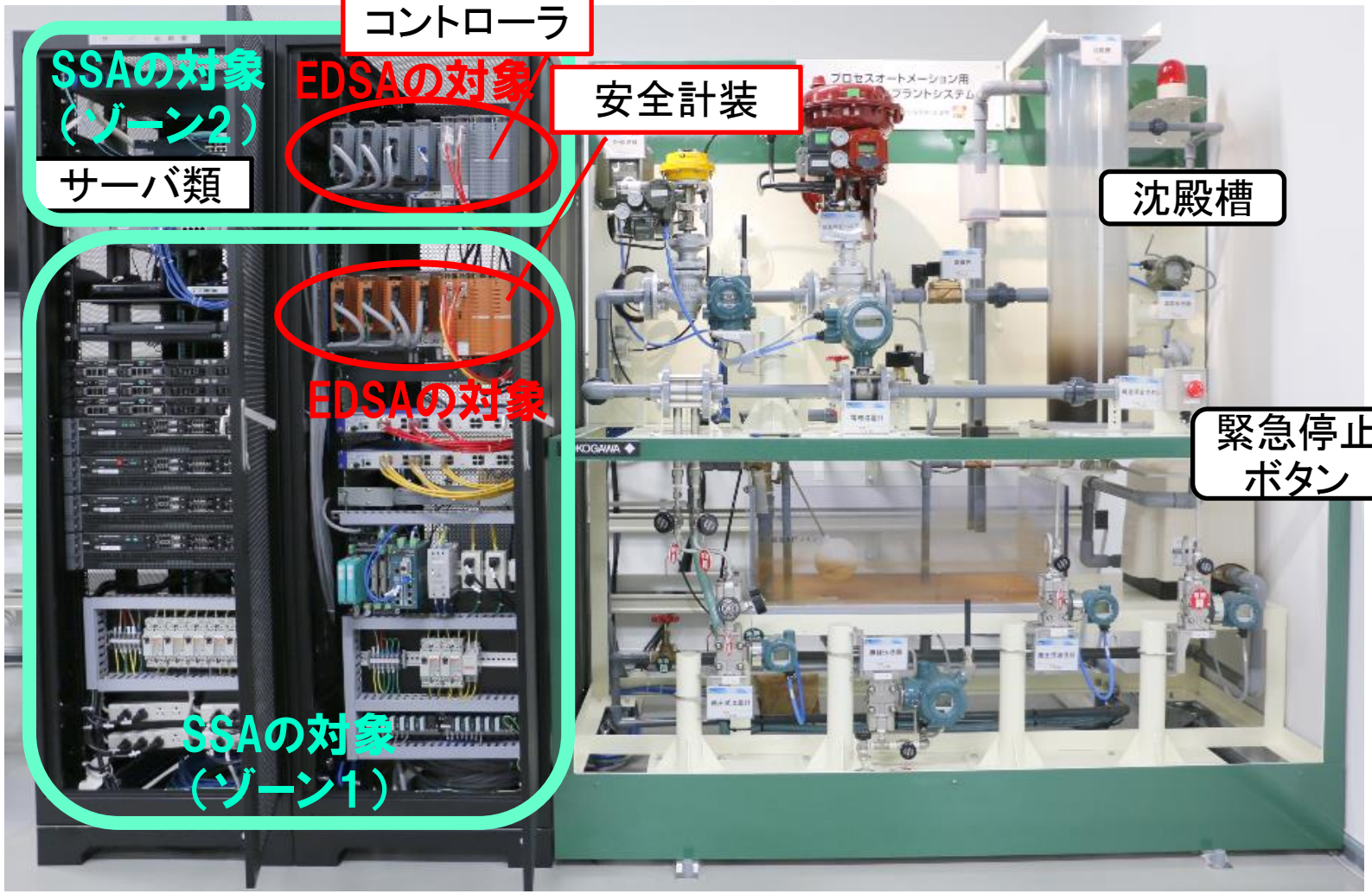
EDSA認証とSSA認証の具体例：化学プラント



ゾーン分割は受審企業が申請。この図は一例。

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

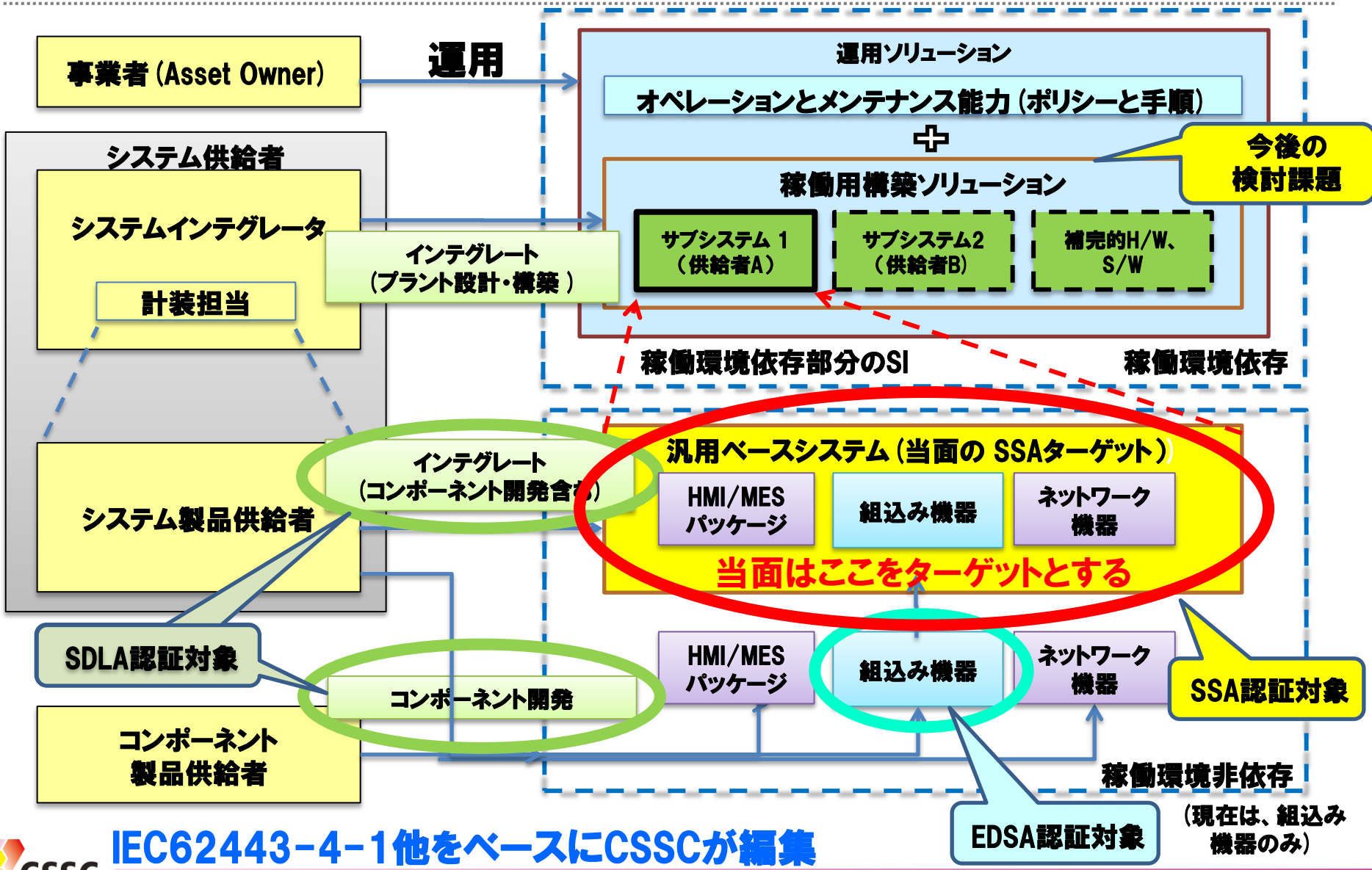
EDSA認証とSSA認証の具体例：排水・下水処理プラント



ゾーン分割は受審企業が申請。この図は一例。

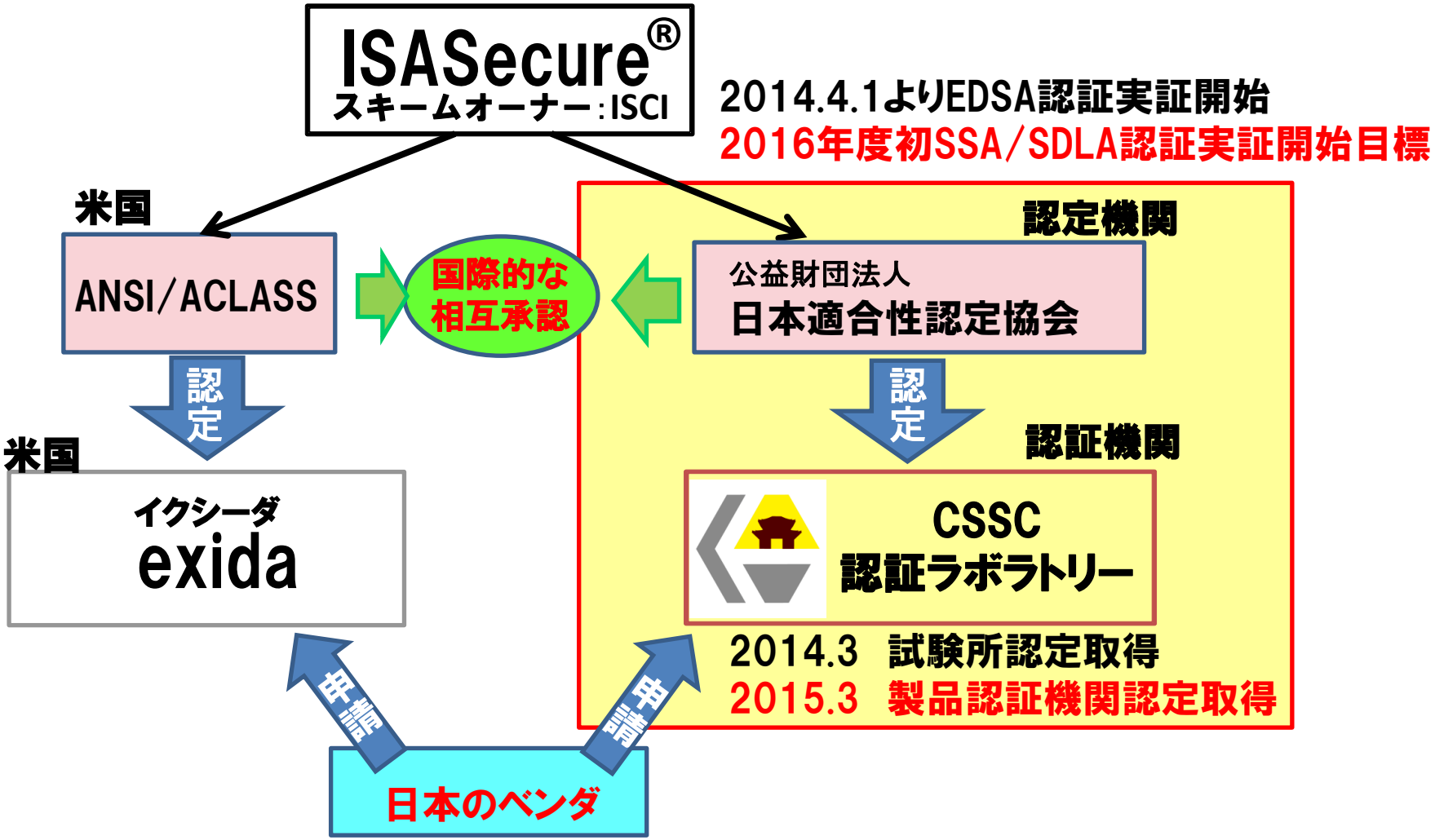
下水処理で多く用いられている汚泥と水の分離を行う沈殿槽の一部を模擬している
コントローラは流入水量が一定となるように制御している

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



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	・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	・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3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、）	・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	・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。	・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