
**制御システムセキュリティの標準化動向
～IEC 62443の最新状況と認証制度の紹介～**

**2020年 2月14日
(株)日立製作所 研究開発グループ**

藤田 淳也

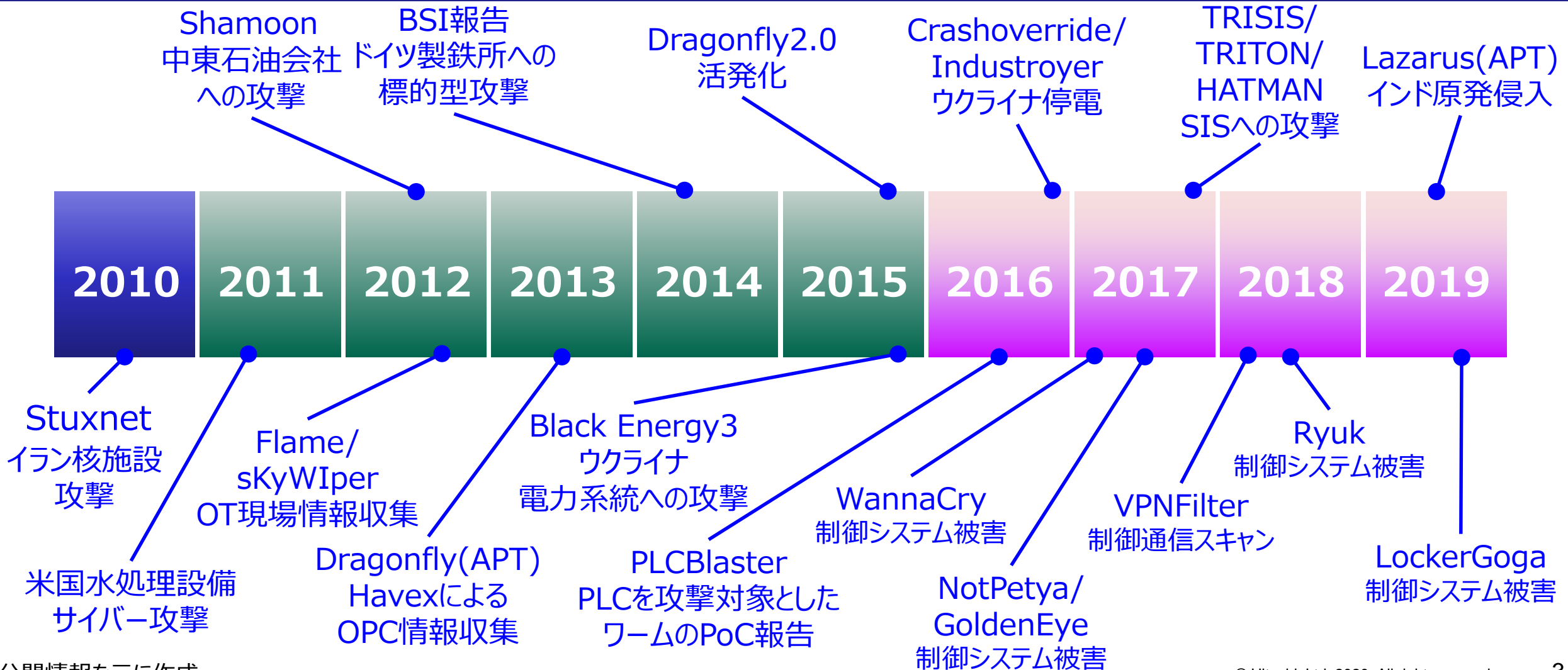
Content

1. 制御システムセキュリティと標準規格
2. IEC 62443シリーズの概要と最新動向
3. IEC 62443シリーズに関連する認証制度

本日お話する内容は、2020年1月時点の
規格書ドラフト版やワーキンググループ会議での
議論を元にした内容です

本日紹介した概念や項目は
最終版に反映されない可能性があります

制御システムに関連するサイバー攻撃の報告は増加傾向 多くは組織化された攻撃グループによって行われ、攻撃手法も日々巧妙化



*公開情報を元に作成

攻撃グループが大規模組織化しており、 サイバー攻撃のビジネス化・プラットフォーム化が顕著

	過去	近年
主な目的	<ul style="list-style-type: none"> • 技術力の誇示 • 興味本位 	<ul style="list-style-type: none"> • 金銭 • 事業損失, 信用失墜 • 思想表明(ハクティビズム) • 軍事利用
対象	<ul style="list-style-type: none"> • 汎用システム • 無差別 	<ul style="list-style-type: none"> • 特定組織, 特定設備
手段 (マルウェア・ 攻撃ツール)	<ul style="list-style-type: none"> • スクラッチで開発 • ネットで入手したものそのまま 	<ul style="list-style-type: none"> • 闇市場で流通 (未公表の脆弱性も売買) • マルウェア開発支援プラットフォーム

制御システムのセキュリティ脅威は攻撃経路，手法，攻撃成立条件は多種多様
それら脅威への対策も技術・管理・運用を含めた様々な面でのアプローチが求められる

順位	制御システムのセキュリティ10大脅威（2019年）	対策の一例
1	リムーバブルメディアや外部機器経由のマルウェア感染	外部機器／メディア管理ポリシー・接続前スキャン
2	インターネットおよびイントラネット経由のマルウェア感染	ネットワークゾーニング・異常通信監視
3	ヒューマンエラーと妨害行為	安全設計・教育・従業員管理ポリシー
4	外部ネットワークやクラウドコンポーネントへの攻撃	サービスプロバイダ管理・ネットワーク堅牢化
5	ソーシャルエンジニアリングとフィッシング	教育・重要情報管理・データ復旧ポリシー
6	DoS/DDoS攻撃	ネットワーク堅牢化・冗長化・専用線の採用
7	インターネットに接続された制御機器	機器の管理・監視・ネットワーク接続ポリシー
8	リモートアクセスからの侵入	ネットワーク堅牢化・アクセス認証
9	技術的な不具合と不可抗力	システムベンダ・IRTとの連携体制構築
10	スマートデバイスへの攻撃	スマートデバイスの堅牢化・管理ポリシー

制御システムは保護対象や特徴が従来の情報システムと異なるため、従来の情報セキュリティとは異なるアプローチが必要

内容	従来の情報システム	工場・プラントの制御システム
システムの特徴	トランザクション中心 情報管理が重要	周期処理中心 常時安定稼働が必要不可欠
データ保護の優先順位	C→I→A <ul style="list-style-type: none"> ・機密性(Confidentiality) ・完全性(Integrity) ・可用性(Availability) 	A→I→C <ul style="list-style-type: none"> ・可用性(Availability) ・完全性(Integrity) ・機密性(Confidentiality)
耐用年数	3～5年	10～20年以上
管理・運用組織	情報システム部門	工場・プラント現場の生産技術部門
パッチ適用	頻繁・定期的 配信システムによる自動適用	レガシーOSを利用 稼働優先のため、リプレースなどの タイミングで実施
リアルタイム性	遅延は許容	リアルタイム性が不可欠
利用技術の標準化	標準化された技術がほとんど	少しずつ標準化は進んでいるものの 独自仕様技術を採用する現場が大半
主な攻撃の目的・被害	情報搾取、金銭搾取	システム・設備破壊、業務停止、社会の混乱 (HSE : Health, Safety and Environmentへの影響)

制御システムのセキュリティ確保のために推奨セキュリティ対策の標準の策定・活用が進んでいる

標準規格 = 専門家の間で開発・合意が取れた推奨事項

- 要求事項や推奨事項を満足することで一定水準の効果が得られる
- 規格文書が想定するスコープ(適用範囲, 前提条件)において有効
- 多くは幅広く・汎用的に利用することを想定して記載 (参照モデル)
現場では内容を解釈し, 個々ケースに適用する方法の検討が必要

業界標準・ローカル基準から国際標準へと進展 特にIEC 62443が多くの規格から参照される位置づけ

	情報システム	一般制御システム	石油化学	電力・原子力	鉄道
組織	ISO 27000シリーズ				
	ISO 22320 (emergency management)				
	ISO 22301 (BCP)				
	ISO 31000 (risk management)				
	NIST Cybersecurity framework				
システム	ISO/IEC 15408	DCID	NIST SP 800-82	IEC 62443 (ISA-62443)	WIB (IEC 62443)
装置			UL 2900	API 1164	NERC CIP
				NISTIR 7628	IEC 62645
				IEEE 1686	IAEA Nuclear Security Recommendation Rev.5
					NEI 08-09
					IEC 62278 (RAMS)
					政府系団体ガイド (米・英・豪等)
個別技術	凡例 <input type="checkbox"/> : 国際標準 <input type="checkbox"/> : 業界標準・ローカル基準		ISO/IEC 29192	IEEE 2030	IEC 62280
				IEC 62351	

Content

1. 制御システムセキュリティと標準規格
- 2. IEC 62443シリーズの概要と最新動向**
3. IEC 62443シリーズに関連する認証制度

産業用自動制御システム(IACS)セキュリティを確保するための推奨セキュリティ対策を規定

IEC 62443シリーズ (ISA/IEC-62443)

IACS(Industrial Automation Control System)のセキュリティ技術仕様を提供する文書群。
ISA(国際自動制御学会), およびIEC(国際電気標準会議)にて開発。

*ISA: International Society of Automation IEC: International Electrotechnical Commission

IACSとは？

制御プロセスの安全, セキュリティ, 信頼性(Reliability)のある運用に作用,
もしくは影響する人的資産, ハードウェア及びソフトウェアの集合体
(IEC 62443-1-1:2009 3.2.57)

➡ セキュリティ確保の対象はソフトウェア・ハードウェアを含む制御関連のデータ処理基盤
であるシステムだけでなく, システムの運用にかかわる「人」と, 「業務」も対象

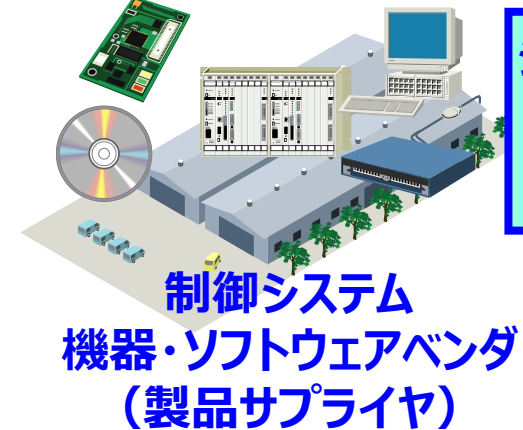
『IACS』は制御処理を実行・管理するコンピュータシステムと
人・組織・運用・規則（ポリシ・手順）すべてを含む

制御システム・サービス
ソリューションベンダ
(サービスプロバイダ)

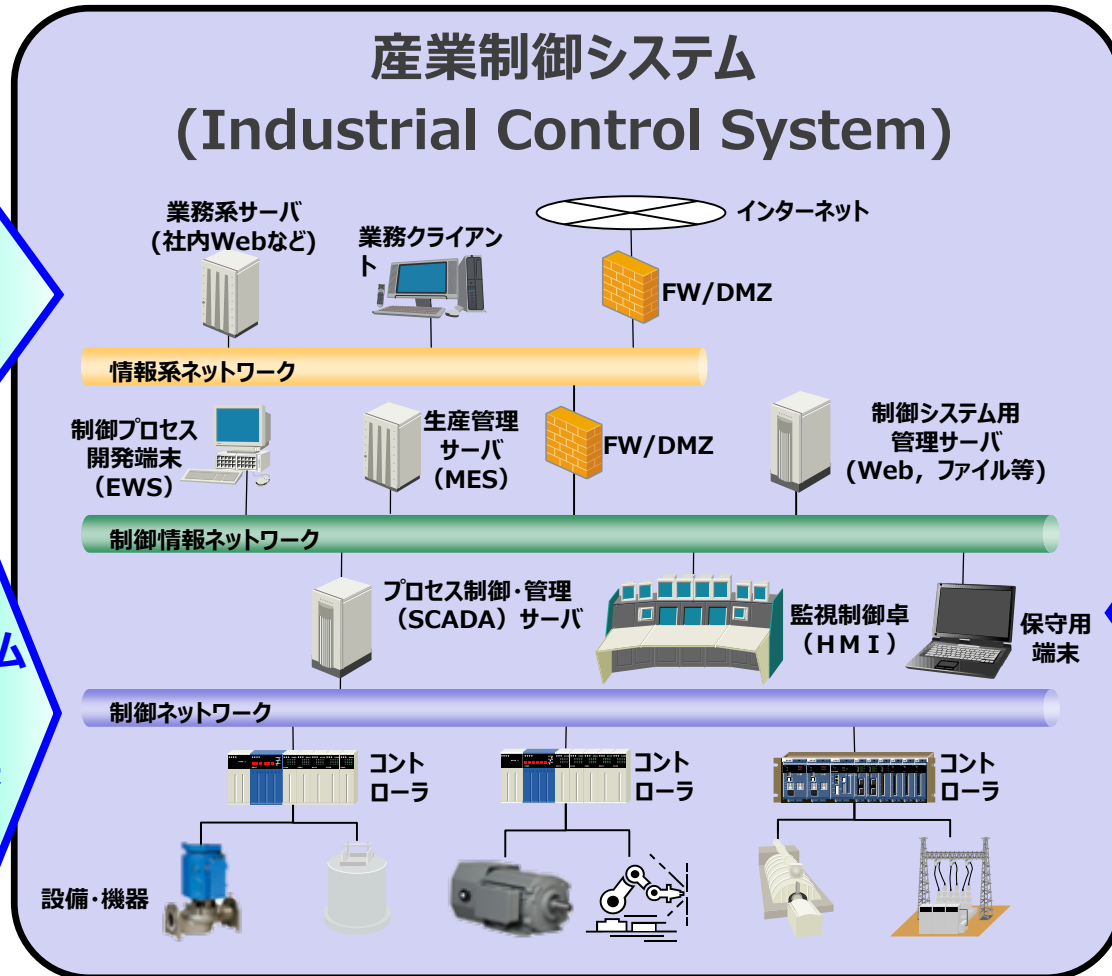


システム・
サービス
提供

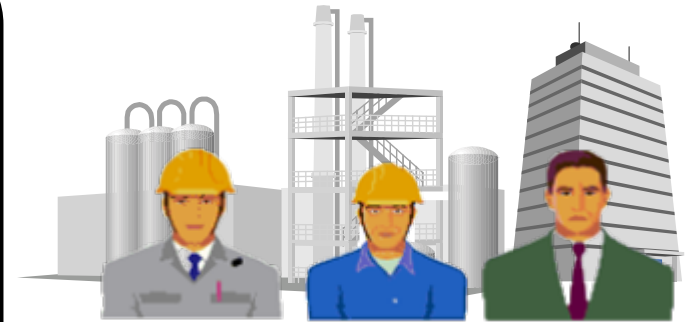
システム部品
提供



システム
部品
提供



制御システム運用・管理組織
(アセットオーナ)



運転員・保守員・管理者・経営者等

システム
運用・管理



運用管理ポリシ・手順書群

- ・ユーザ/サードパーティ管理
- ・システム管理
- ・システム運用手順 等

ISA/IEC 62443シリーズは2つのワーキンググループによって開発

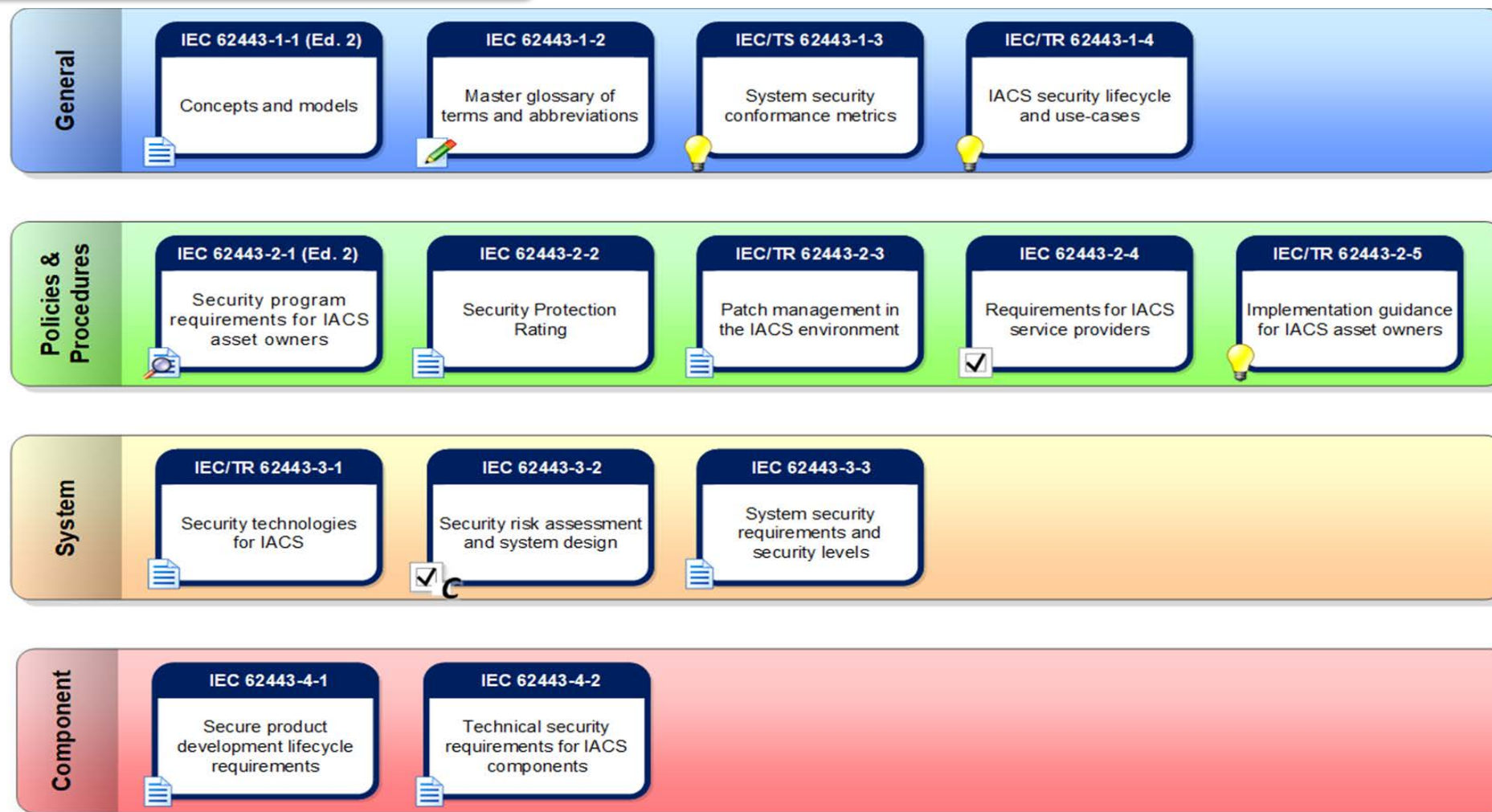
ISA/IEC 62443シリーズの開発は以下の2グループによって開発

- ・ ISA99 WGによって開発される標準：**ANSI/ISA-62443**
- ・ IEC/TC65/WG10によって開発される標準：**IEC 62443**
- ・ 厳密には異なる標準であるが、大きな内容の違いはない
※本発表では『ISA/IEC 62443』を『IEC 62443』で表現を統一
- ・ 規格の内容は、ISA99内の分冊毎に設けられたサブWGで開発
ドラフトがある程度完成すると、IECに提案・IEC側で個別に内容の照査・修正・承認







開発に当たって、ISO/IEC 27000シリーズの策定WGと議論

- ・ 標準の策定に当たり、ISO/IEC JTC1/SC27と連携

IEC 62443シリーズの一覧










ステータス アイコンの説明

-  開発提案
-  開発中
-  コメント付き承認
-  コメント募集中
-  発行済み
-  発行済み (レビュー中)

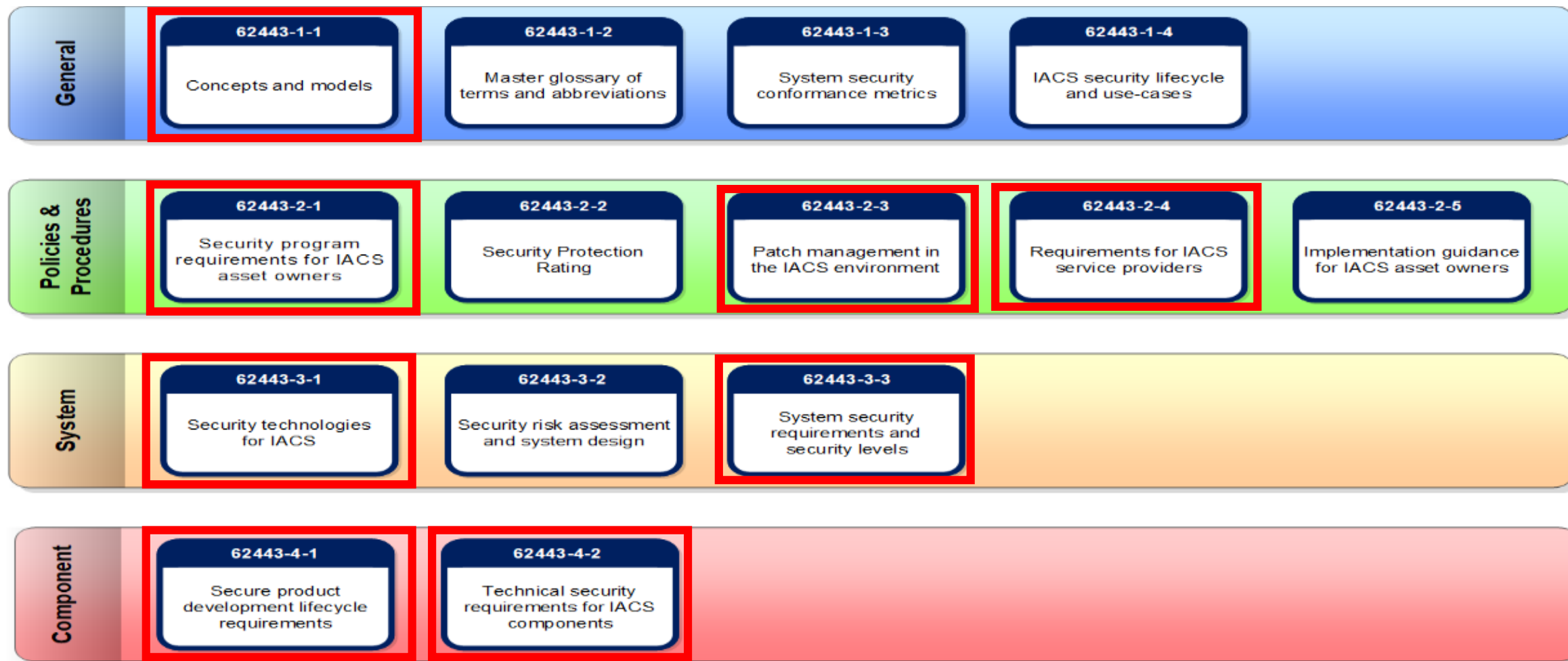
ISA-62443シリーズの一覧

Category	Standard ID	Title	Status
General	ISA-62443-1-1	Concepts and models	開発中
	ISA-62443-1-2	Master glossary of terms and abbreviations	開発中
	ISA-62443-1-3	System security conformance metrics	開発中
	ISA-TR62443-1-4	IACS security lifecycle and use-cases	開発中
Policies & Procedures	ISA-62443-2-1	Security program requirements for IACS asset owners	コメント付き承認
	ISA-62443-2-2	Security Protection Rating	開発中
	ISA-TR62443-2-3	Patch management in the IACS environment	開発中
	ISA-62443-2-4	Requirements for IACS service providers	開発中
	ISA-TR62443-2-5	Implementation guidance for IACS asset owners	開発中
System	ISA-TR62443-3-1	Security technologies for IACS	開発中
	ISA-62443-3-2	Security risk assessment and system design	コメント付き承認
	ISA-62443-3-3	System security requirements and security levels	開発中
Component	ISA-62443-4-1	Secure product development lifecycle requirements	発行済み
	ISA-62443-4-2	Technical security requirements for IACS components	発行済み

ステータス アイコンの説明

-  開発提案
-  開発中
-  コメント付き承認
-  コメント募集中
-  発行済み
-  発行済み (レビュー中)
-  IECから採用

ISA/IEC 62443シリーズの一覧



2020年1月最新のステータス（全14冊中 8冊発行済）

出典：ISA99 Working Group

ISA/IEC 62443シリーズの一覧

General

全般・全文書共通事項

Policies &
Procedures

システム開発・運用組織の
セキュリティ運用ポリシ・手順

System

システムのセキュリティ機能

Component

コンポーネントのセキュリティ(開発プロセス・機能)

制御システムセキュリティ標準：ISA/IEC 62443シリーズの一覧

規格名	対象	説明	状態
62443-1-1	全般	(Ed1.0) 用語, コンセプト, モデル (TS) (Ed2.0) コンセプト, モデル	Ed1.0発行済み (2009) Ed2.0に向けて議論開始
62443-1-2	全般	マスター用語・略語集 (TR)	ドラフト開発中
62443-1-3	全般	システムセキュリティ評価基準	提案あり
62443-1-4	全般	IACSセキュリティライフサイクルとユースケース (TR)	ドラフト開発中
62443-2-1	オーナ	(Ed1.0)産業自動制御システムのセキュリティマネジメントシステム構築 (Ed2.0) IACSアセットオーナ向けセキュリティプログラムの要求事項	Ed1.0発行済み(2010) Ed2.0ドラフト開発中
62443-2-2	オーナ	セキュリティプロテクション (プログラム) 格付け (TR)	ドラフト開発中
62443-2-3	オーナ	IACS環境におけるパッチ管理 (TR)	Ed1.0発行済み(2015) Ed2.0ドラフト開発中
62443-2-4	オーナ	IACSサービス提供者向けセキュリティプログラムの要求事項	Ed1.0発行済み(2015) Ed2.0に向けて議論開始
62443-2-5	オーナ	IACSアセットオーナ向け実践ガイドライン	提案あり
62443-3-1	システム	IACSで利用可能なセキュリティ技術 (TR)	Ed1.0発行済み(2009) Ed2.0に向けて議論開始
62443-3-2	システム	リスク分析とゾーンやコンジット設計	ドラフト開発中
62443-3-3	システム	システムセキュリティ要件とセキュリティレベル	Ed1.0発行済み(2013) Ed2.0に向けて議論開始
62443-4-1	コンポーネント	セキュアプロダクト開発ライフサイクルの要件	Ed1.0 発行済み (2018)
62443-4-2	コンポーネント	IACSコンポーネントの技術的セキュリティ要件	Ed1.0 発行済み (2019)

IEC 62443-1グループはシリーズ全体で共通するトピックについて規定

IEC 62443-1-1：Concepts and models

- ・ 62443シリーズで共通的に参照されるコンセプトやモデルについて説明。
62443全体の概念や参照モデルを理解したい読者向け。
- ・ 基本モデルはPurdue Enterprise Reference Architecture (PERA)を採用
- ・ Ed1.0のタイトルは“**Terminology, concepts and models**”。TSとして発行。
一方で、Ed2.0はISとして策定予定。用語の説明は62443-1-2に委譲。

TS: Technical Specifications (技術仕様)
IS: International Standard (国際標準)

IEC 62443-1-2：Master glossary of terms and abbreviations

- ・ シリーズ全体で使用されている用語と略語のマスター用語集。
- ・ 未発行。Ed1.0に向けて開発中。

IEC 62443-1グループはシリーズ全体で共通するトピックについて規定

IEC 62443-1-3 : System security conformance metrics

- ・ システムセキュリティ対策の定量的な指標（パフォーマンス指標）についての標準.
- ・ 未発行. Ed1.0に向けて開発中（位置づけ・方向性議論中）

IEC TR62443-1-4 : IACS security lifecycle and use-cases

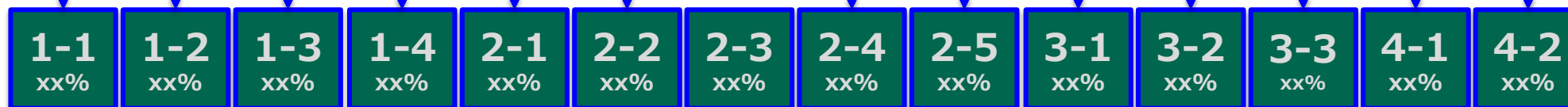
- ・ IACSライフサイクル全体モデル, セキュリティの取り組み方法, および実アプリケーションを想定したユースケースについて紹介（予定）.
- ・ IEC 24748（システム・ソフトウェア開発のライフサイクル管理の標準）のライフサイクルモデルを元に, IACSに関係するステークホルダのセキュリティ上の役割について定義.
- ・ 未発行. Ed1.0に向けて開発中.

ライフサイクル全体に渡って利用可能なセキュリティプログラム評価の 定量指標（KPI）の標準について議論中

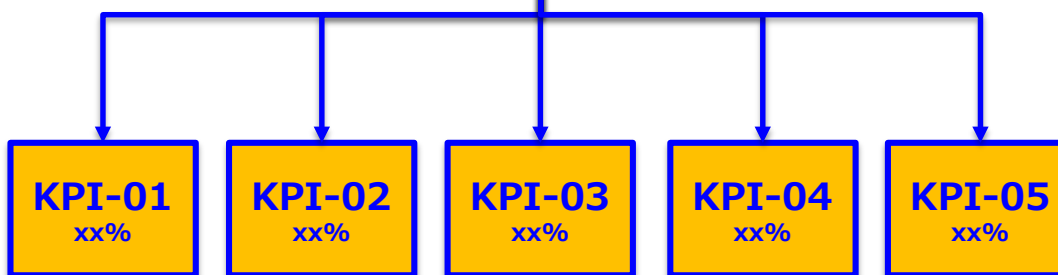
プラント

○×プラントの
セキュリティプログラム
83%

標準
(62443シリーズ)



KPI

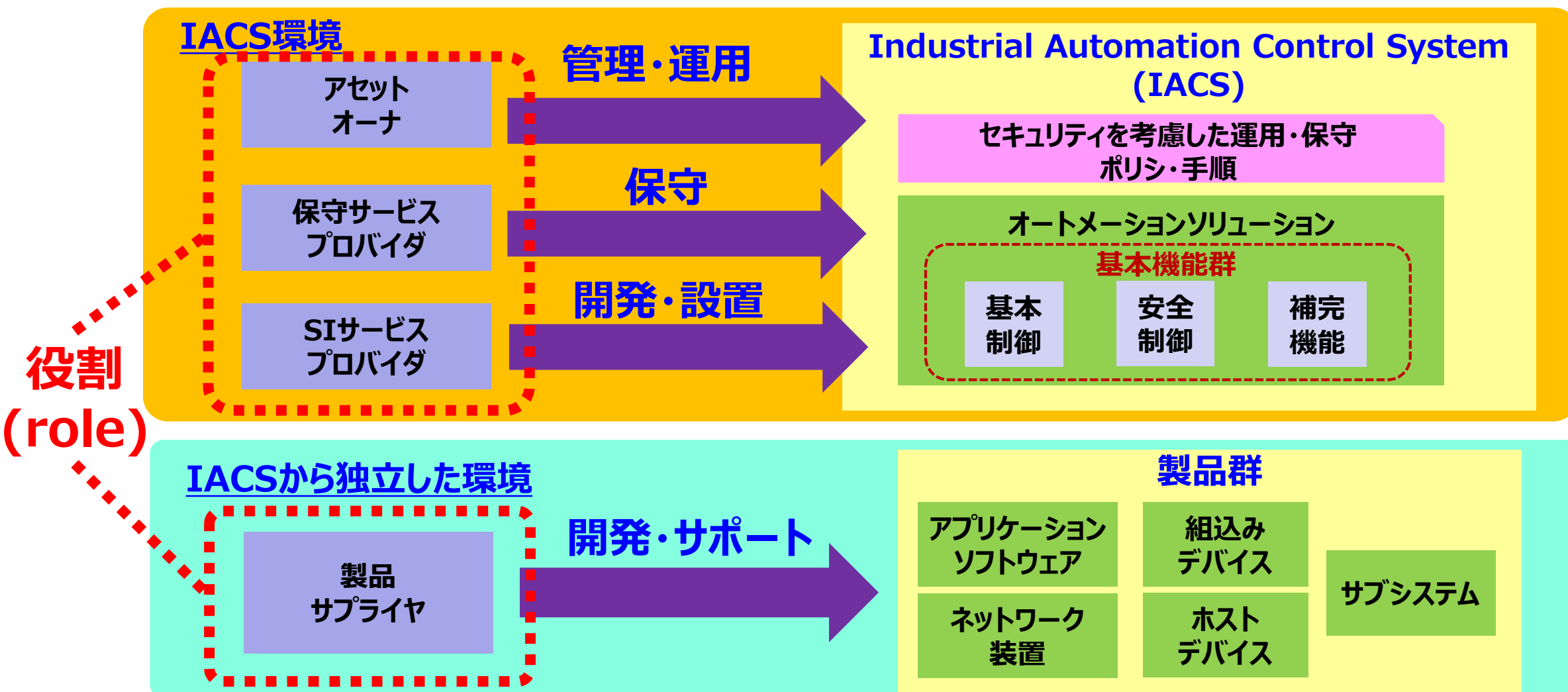


KPI達成状況

KPI-01

項目	○/×	重み	項目の達成情報	KPI達成状況
1-xxxxxx	○	14%	100%	14%
2-xxxxxx	60%	14%	60%	9%
3-xxxxxx	×	14%	0%	0%
4-xxxxxx	○	14%	100%	14%
5-xxxxxx	50%	14%	50%	7%
...

IACSにおける主要役割(Principal role)モデルとIACSとの関係・各エンティティのIACSライフサイクル上の位置づけについて規定



IEC 62443-2グループは、IACSに関する組織のマネジメント・運用に関するポリシーや手順に関する要件・ガイドラインを規定

IEC 62443-2-1：Security Program requirements for IACS asset owners

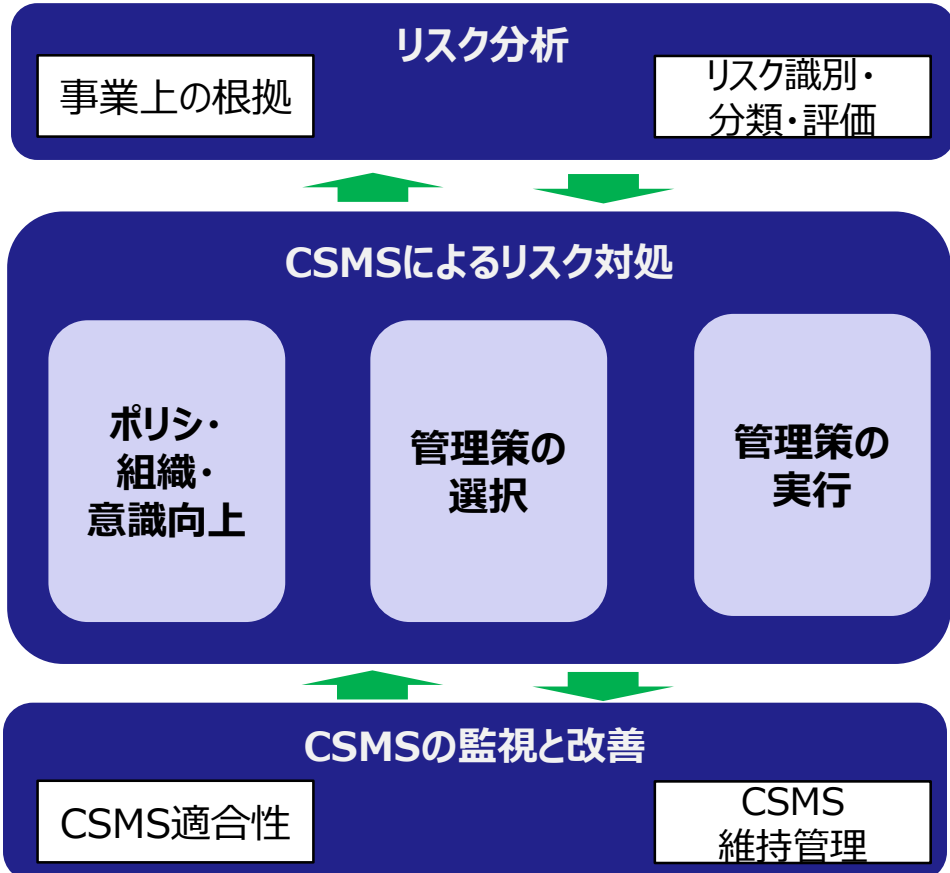
- IACSのアセットオーナー向けのセキュリティプログラム（管理・運用の枠組み）の要件を規定
- 2010年にEd1.0発行済。
- Ed1.0のタイトルは“Establishing an Industrial Automation and Cyber Security Management System (CSMS)”，制御システム向けマネジメントシステムの枠組みである『CSMS』に関する要件を規定。
- 現在はEd2.0開発中。次バージョンでは大きく変更予定（2020年中に発行予定）。

IEC 62443-2-2：Security Protection Rating (Security Program Rating)

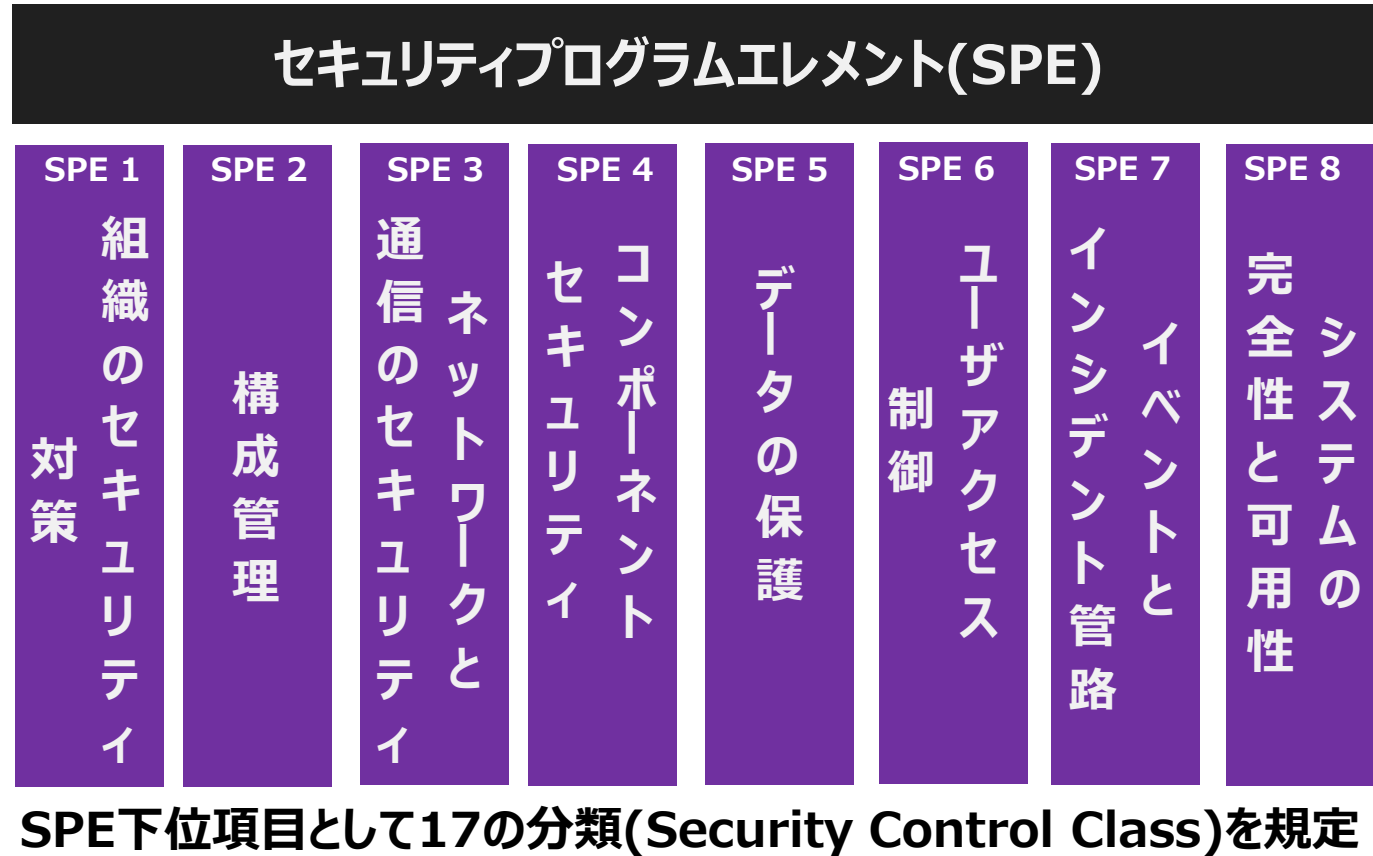
- 技術対策と運用対策とを合わせたセキュリティ保護レベルの評価方法について規定（予定）。
- 当初の名称は“IACS Protection Level”であったが、最新は“Security Program Rating”。技術対策と運用・保守のプロセス成熟度を用いた対策効果の指標化に関して規定。
- 未発行。Ed1.0に向けて開発中（位置づけ・方向性議論中）。

IACSアセットオーナーの「セキュリティマネジメントシステム」を対象としたものから「セキュリティプログラム」となり、更に広い観点で管理策を規定

IEC 62443-2-1 Ed1.0 (CSMS)



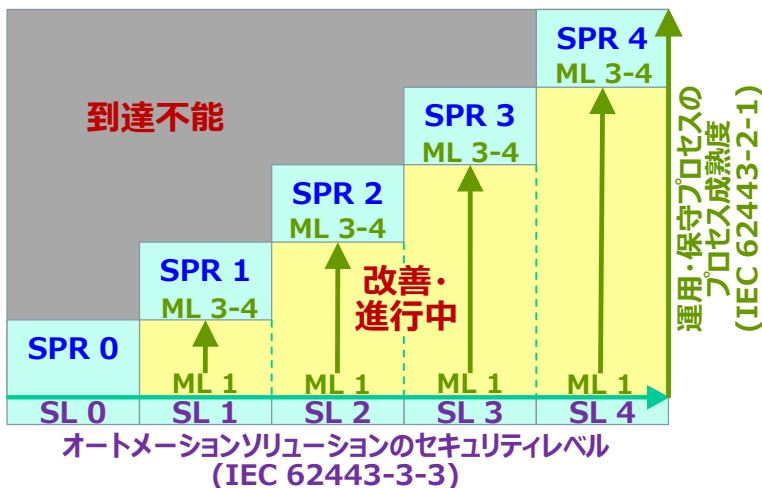
IEC 62443-2-1 Ed2.0 (Security program for IACS asset owner)



オートメーションソリューションの技術的対策の評価指標 (SL: Security Level)	
SL 4	巧妙な手法, 拡張リソース, IACSに特化したスキルを有し, かつ高い動機を持つ攻撃者による意図的なセキュリティ違反から保護
SL 3	巧妙な手法, 中程度のリソース, IACSに特化したスキルを有し, かつ中程度の動機を持つ攻撃者による意図的なセキュリティ違反から保護
SL 2	単純な手法, 限られたリソース, 一般的なスキルを有し, かつ低い動機を持つ攻撃者による意図的なセキュリティ違反から保護
SL 1	偶発的, または偶然のセキュリティ違反からの保護
SL 0	特定のセキュリティ保護がない

運用・保守時の組織的対策の評価指標 (ML: Maturity Level)	
ML 4	適切なプロセス定量評価指標を用い, プロセスの有効性, またはパフォーマンスの改善, もしくはその両方を実証できる.
ML 3	Level 2で定義されたプロセスが実践されている
ML 2	機能の提供とパフォーマンスを管理する方法を説明したドキュメントが存在する. プロセスの定義と実行・実践に大きな遅延を生じる可能性がある.
ML 1	行き当たりばったりで文書化されていないか, 完全に文書化されずに実施されているプロセス

SPR: Security Program Rating



SPR 4	巧妙な手法, 拡張リソース, IACSに特化したスキルを有し, かつ高い動機を持つ攻撃者による意図的なセキュリティ違反から保護
SPR 3	巧妙な手法, 中程度のリソース, IACSに特化したスキルを有し, かつ中程度の動機を持つ攻撃者による意図的なセキュリティ違反から保護
SPR 2	単純な手法, 限られたリソース, 一般的なスキルを有し, かつ低い動機を持つ攻撃者による意図的なセキュリティ違反から保護
SPR 1	偶発的, または偶然のセキュリティ違反からの保護
SPR 0	特定のセキュリティ保護がない

IEC 62443-2グループは、IACSに関する組織のマネジメント・運用に関するポリシーや手順に関する要件・ガイドラインを規定

IEC TR62443-2-3： Patch management in the IACS environment

- ・ IACS環境におけるパッチ管理の要求事項を提供。
- ・ 2015年にTRとしてEd1.0発行済み。 Ed2.0はISを目指して開発中。

TR: Technical Report (技術報告書)

IEC 62443-2-4： Requirements for IACS service providers

- ・ システムベンダやネットワークサービス等， IACSオーナーに対してサービスを提供するに提供者のセキュリティプログラムの要件が規定（調達仕様作成時に参照可能）
- ・ WIB（欧州の製造業ユーザ団体）が開発したセキュリティ要件(Report M 2784-X)がベース
- ・ 2015年にEd1.0発行済み。 Ed2.0に向けて議論開始。

IEC 62443-2-5： Implementation guidance for IACS asset owners

- ・ IACSアセットオーナー向けセキュリティプログラムの実装ガイダンスを提供（予定）。
- ・ 未発行。 IEC 62443-2-1 Ed 2.0発行後に本格検討開始予定。

IEC 62443-3グループは、IACSの「システムとして」の セキュリティ機能要件・セキュリティ機能設計・技術に関して規定

IEC TR62443-3-1： Security technologies for IACS

- ・ IACS環境に利用可能なセキュリティ技術のカタログを提供。
- ・ 2009年にEd1.0発行済。Ed2.0に向けて議論中。

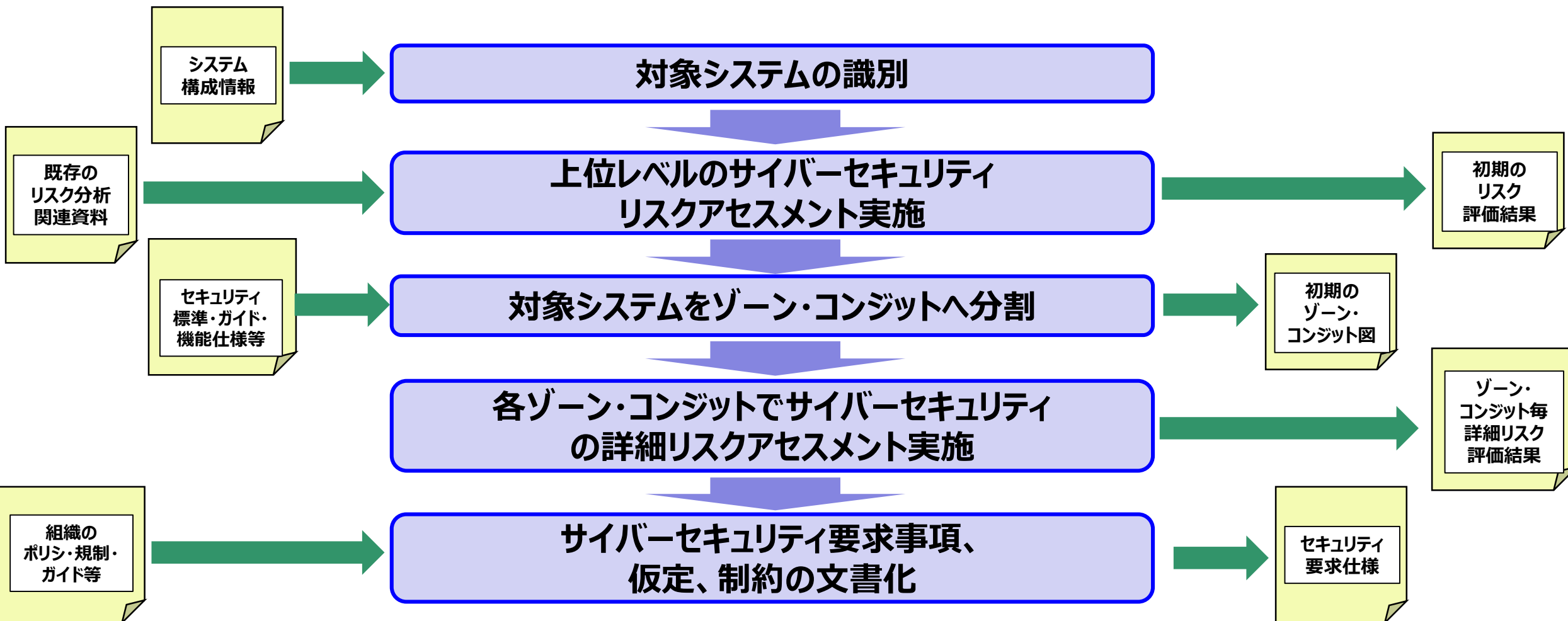
IEC 62443-3-2： Security risk assessment and system design

- ・ システムのセキュリティ設計手順。特にリスク評価とセキュリティゾーン設計の流れを規定。
- ・ 未発行。Edition 1.0に向けて開発中（ISA/IECからのコメント反映中）。

IEC 62443-3-3： System security requirements and security levels

- ・ セキュリティレベル(Security Level)の基準とシステムのセキュリティ機能要件
(FR：Foundational Requirement, SR：System Requirement) を規定。
- ・ 2013年にEd1.0発行済。Ed2.0に向けて議論開始。

IEC 62443-3-2はシステムのセキュリティ設計のための リスク分析やセキュリティゾーン分割の手順について規定



IEC 62443-4グループは、IACSの「コンポーネントとして」のセキュリティ機能要件・セキュリティ開発プロセスに関して規定

IEC 62443-4-1 : Security product development lifecycle requirements

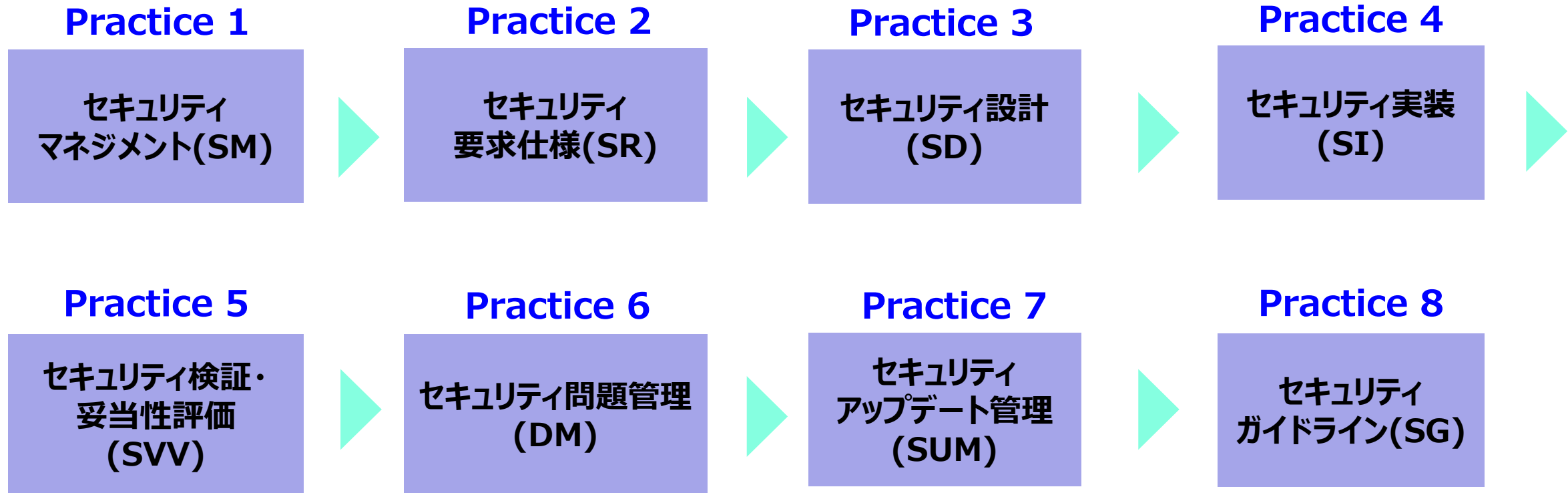
- ・ IACSコンポーネントベンダのセキュリティ開発プロセスの要件について規定.
- ・ 2018年にEd1.0発行済.

IEC 62443-4-2 : Technical security requirements for IACS components

- ・ IACSを構成するソフトウェア・ハードウェア・ネットワーク装置などコンポーネントのセキュリティ機能要件を規定.
- ・ 2019年にEd1.0発行済み.

IEC 62443-4-1はIACSコンポーネント製品のセキュリティ開発プロセスの要件を規定

- 8つの実践分野(Practice)に関して要件を規定



IEC 62443-4-2はIACSコンポーネントのセキュリティ機能要件を規定

- IEC 62443-3-3の要件 (FR, SR) をベースに各種コンポーネントに合わせて最適化

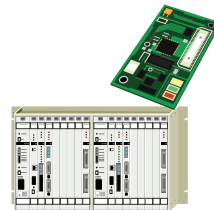
ソフトウェアアプリケーション要件(SAR)

ソフトウェアアプリケーション要求 (SAR: Software Application Requirements)
SAR x.x xxxxxxxx
SAR x.x xxxxxxxx



組み込みデバイス要件(EDR)

組み込みデバイス要求 (EDR: Embedded Device Requirements)
EDR x.x xxxxxxxx
EDR x.x xxxxxxxx
...



ホストデバイス要件(HDR)

ホストデバイス要求 (HDR: Host Device Requirements)
HDR x.x xxxxxxxx
HDR x.x xxxxxxxx
...



ネットワークデバイス要件(NDR)

ネットワークデバイス要求 (NDR: Network Device Requirements)
NDR x.x xxxxxxxx
NDR x.x xxxxxxxx
...



システム要件(SR)

システム要求(SR: System Requirements)
SR 1.1 xxxxxxxx
SR 1.2 xxxxxxxx
SR 1.3 xxxxxxxx
...

コンポーネント要件(CR)

コンポーネント要求 (CR: Component Requirements)
CR 1.1 xxxxxxxx
CR 1.2 xxxxxxxx
CR 1.3 xxxxxxxx
...

基本要件

(FR: Foundational Requirements)

FR 1: 識別と認証制御(IAC)

FR 2: 利用制御(UC)

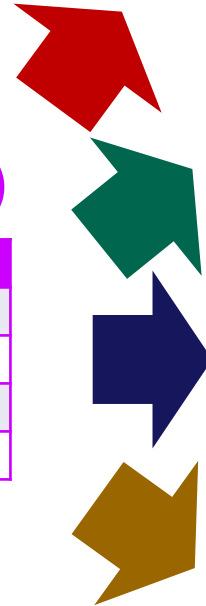
FR 3: システム完全性(SI)

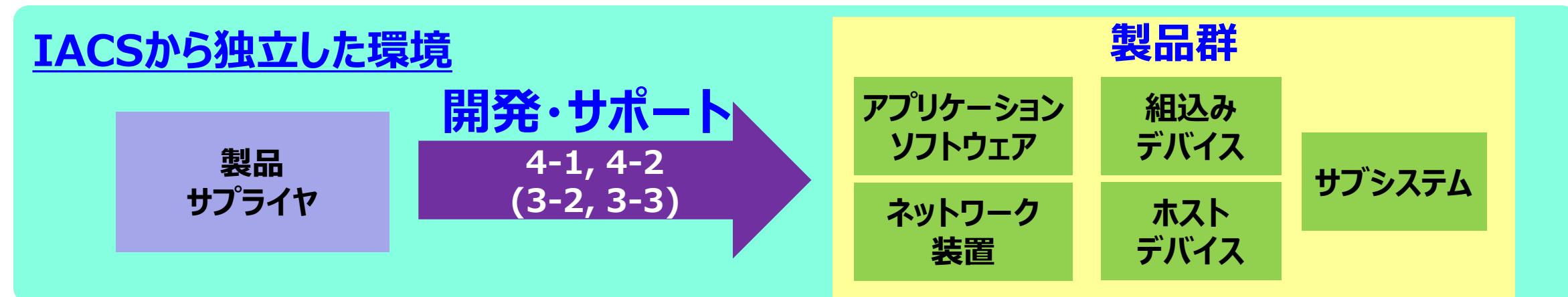
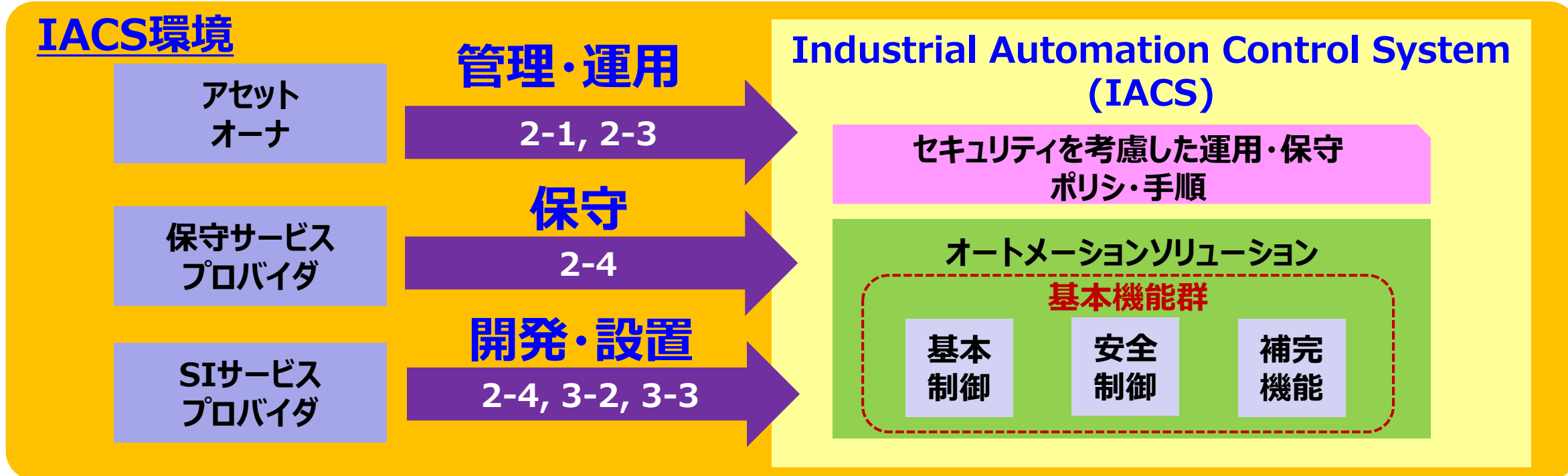
FR 4: データ機密性(DC)

FR 5: 制限されたデータフロー (RDF)

FR 6: イベントへのタイムリーな対応 (TRE)

FR 7: リソース可用性(TA)





**62443シリーズ全体の一貫性が保たれていない点が課題
今後はIEC 62443シリーズ全体で統一化されたモデル・要件の整合性の確保がトピック**

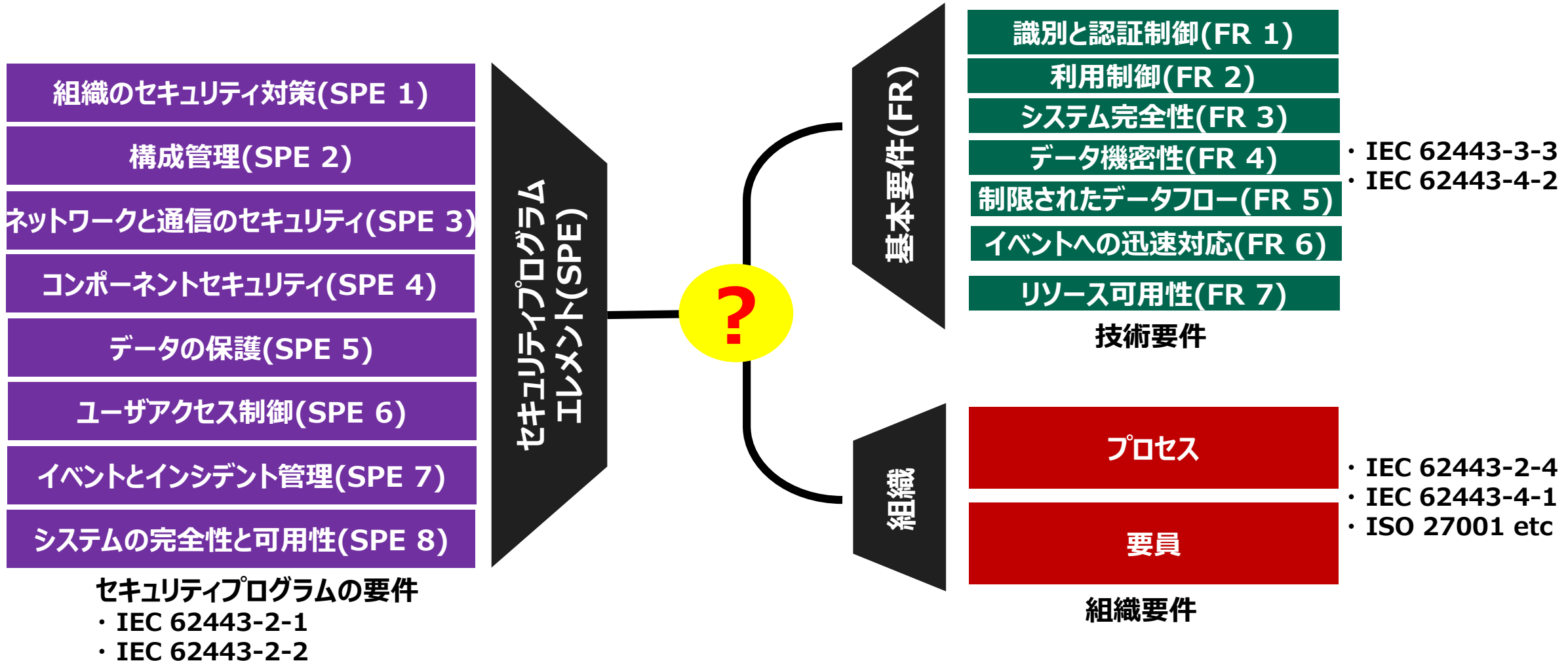
シリーズ共通の基本コンセプト（Fundamental Concepts）の確立

- ・ IACSの主要役割のモデル (Principal Roles)
- ・ ライフサイクルのモデル (Life Cycles)
- ・ セキュリティ定量化指標
 - －セキュリティレベル(Security Levels)
 - －プロセス成熟度 (Maturity Levels)
 - －管理策実践状況・保護レベル (Security Program Rating)
 - －セキュリティ観点のKPI(Key Performance Indicator)

要件の整合

- ・ 62443シリーズの各分冊，およびISO 2700xの要求事項間の整合性

62443シリーズ全体の参照モデル間の関連付けが今後の大きな議題の一つ



システムの安全性とセキュリティを両立するための標準が策定され始めている

機能安全

IEC 62879
ヒューマンファクタ
(Human factors and functional safety)

IEC 61511
プロセス機能安全
(Safety instrumented systems for the process industry sector)

IEC 61131-6
安全PLC
(PLC- Part 6: Functional safety)

IEC 62061
機械機能安全
(Safety of machinery)

IEC 61784-3
安全ネットワーク
(Functional safety fieldbuses)

IEC 61508
機能安全
(Functional safety)

IEC TR63074
安全制御システムのセキュリティ
(Functional safety of safety-related control systems)

IEC TR63069
安全セキュリティ連携
(Framework for functional safety and security)

制御セキュリティ

情報セキュリティ

ISO/IEC 15408
コモンクライテリア
(Common Criteria)

ISO 2700X
情報セキュリティ
(Information security)

IEC 62443
制御セキュリティ
(Security for IACS)

IEC 62443と深く関連する安全とセキュリティに関するIEC標準

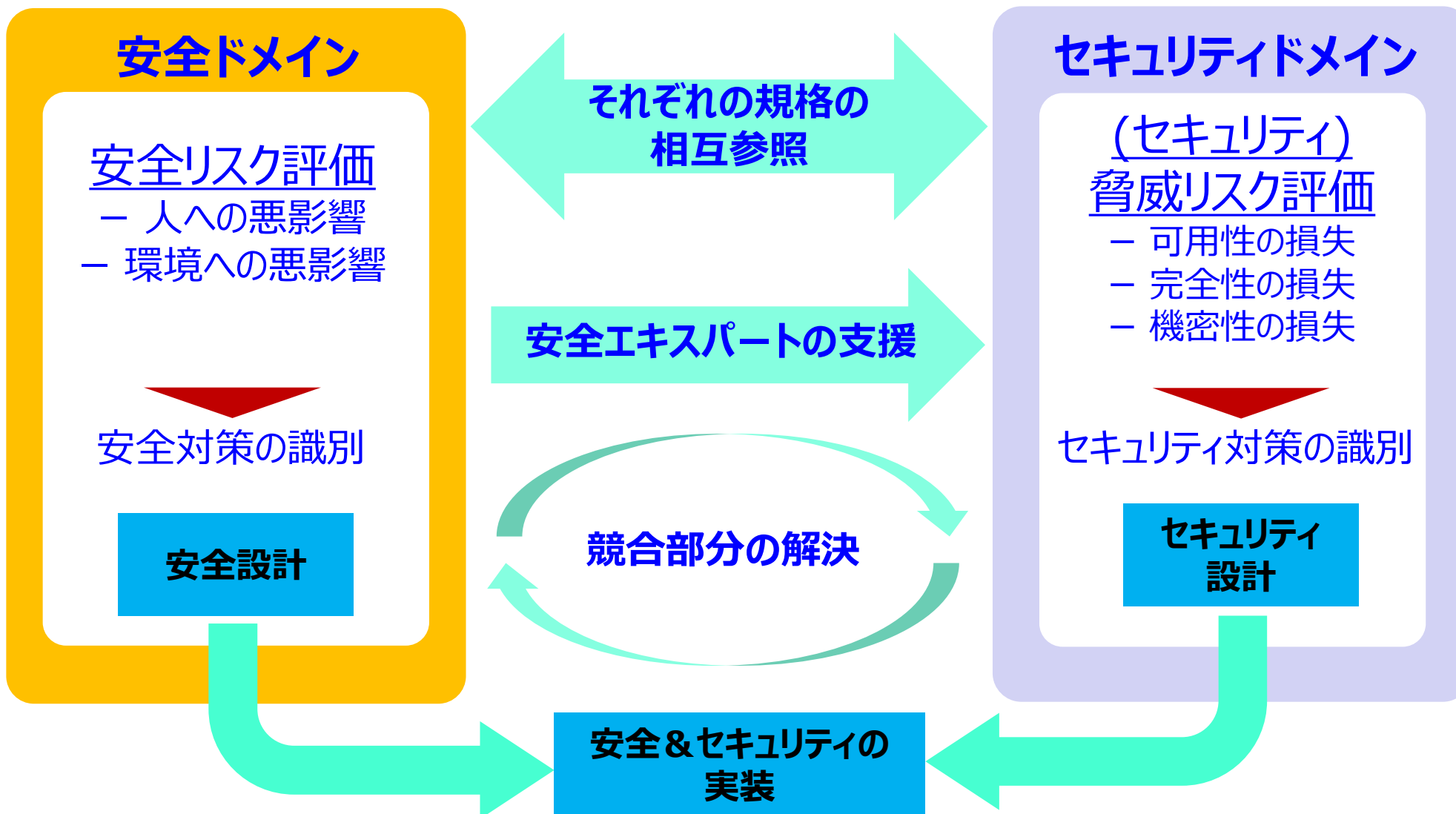
IEC TR63069:2019 Framework for functional safety and security

- 機能安全(IEC 61508)とセキュリティ(IEC 62443)の両立を目指した規格
- 制御システムにおいて、安全機能(機能安全)を考慮せずにセキュリティ機能を導入した場合、セキュリティ機能が安全機能に悪影響を及ぼす可能性がある
e.g. セキュリティ修正パッチ適用した結果、安全機能が損失する
- 機能安全とセキュリティの両方を同時に考慮したシステム設計プロセスのガイダンスを提供

IEC TR63074:2019 Security aspects related to functional safety of safety related control systems

- 機械向け機能安全制御システム(IEC 62061)でのセキュリティ脅威や対策面で考慮すべき事項を記載
- 本書が取り上げるセキュリティ対策はIEC 62443ベース

IEC TR63069が規定する安全・セキュリティを両立させた設計プロセス



IEC 62443の活用を促進・教育・情報連携推進に向けた ISA（国際自動制御学会）が主催するコミュニティ



The ISA Global Cybersecurity Alliance
will work together to develop solutions that
address our biggest challenges



COLLABORATION

When end-users, asset owners, vendor companies, government agencies, and other stakeholders join together in an open and transparent way, we can move industry forward faster and more effectively



STANDARDIZATION

Standards exist, but aren't well understood. Our companies need easy-to-follow guides for implementing best practices, and industry needs to increase the adoption of standards globally



EDUCATION

Human error is the biggest factor in safety and security incidents around the world. Providing accessible, consistent training and education for professionals at all levels gives our companies a first line of defense



PROTECTION

Ensuring the inherent security of vendor devices and systems, and exploring ways to increase compliance with best practices, offers real risk reduction in your operations

Content

1. 制御システムセキュリティと標準規格
2. IEC 62443シリーズの概要と最新動向
- 3. IEC 62443シリーズに関連する認証制度**

IEC 62443シリーズへの適合性を第三者の観点で評価・認証する制度

システム・装置・開発プロセスの認証

- ・ ISASecure認証制度 (ISCI)
- ・ IEC EE認証制度 (IEC)
- ・ 認証団体独自の認証制度 (TÜV, UL 等)

組織の認証

- ・ CSMS認証制度 (JIPDEC)

個人の認証

- ・ ISA/IEC 62443 Cybersecurity Certificate Programs (ISA)

ISA配下のISCI(The ISA Security Compliance Institute)が提供する IEC 62443準拠の機器・システム・開発プロセスの認証プログラム

CSA (Component Security Assurance)

- ・ コンポーネント※のセキュリティを認証 (IEC 62443-4-2準拠)
※ソフトウェアアプリケーション・組み込みデバイス・ホストデバイス・ネットワークデバイス
- ・ 脆弱性有無やセキュリティ機能だけでなく、製品開発プロセスも対象 (IEC 62443-4-1準拠)
- ・ EDSA認証の後継。最新はVersion 1.0.0 (2019/8/28～)

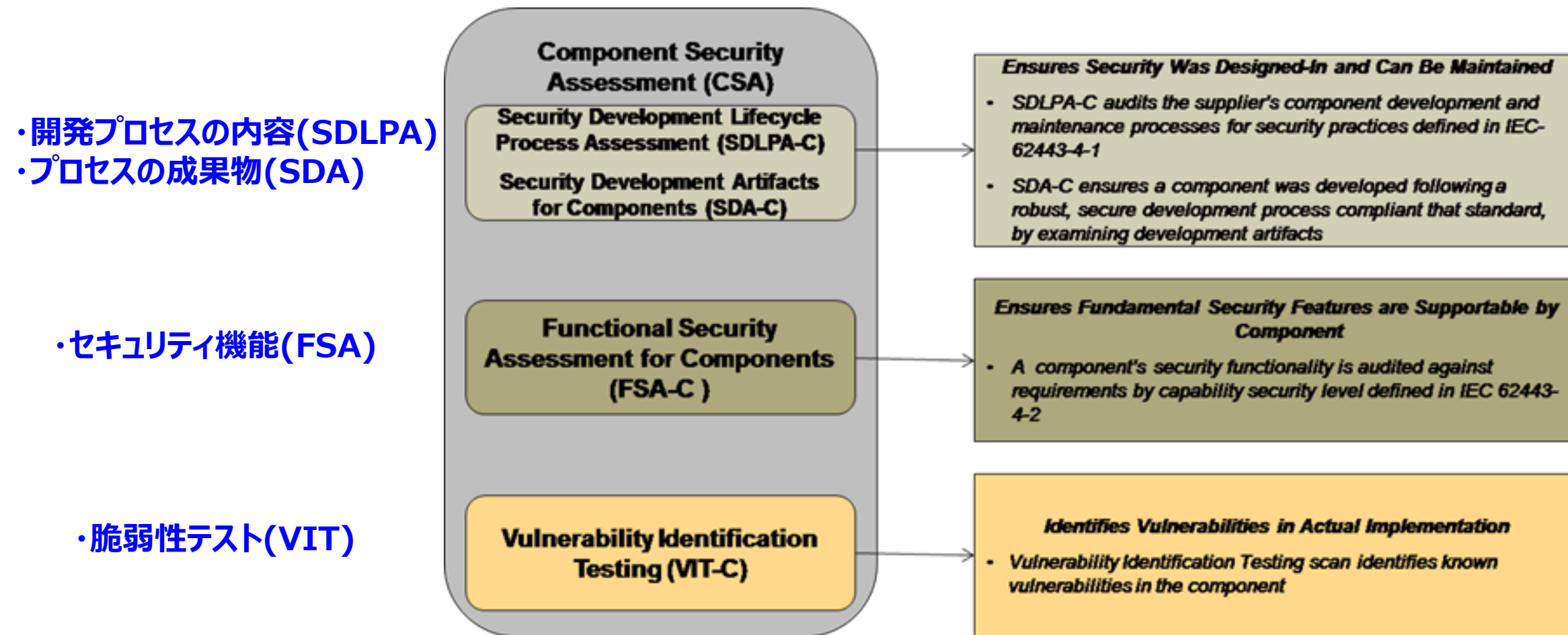
SSA (System Security Assurance)

- ・ 制御システムのサブセットを認証 (IEC 62443-3-3準拠)
- ・ 脆弱性有無やセキュリティ機能だけでなく、システム開発プロセスも対象 (IEC 62443-4-1準拠)
- ・ 最新はVersion 4.0.0 (2019/8/28～)

SDLA (Security Development Lifecycle Assurance)

- ・ コンポーネントサプライヤのセキュリティライフサイクルプロセスを認証 (IEC 62443-4-1準拠)
- ・ 最新はVersion 2.0.0 (2018/2/13～)

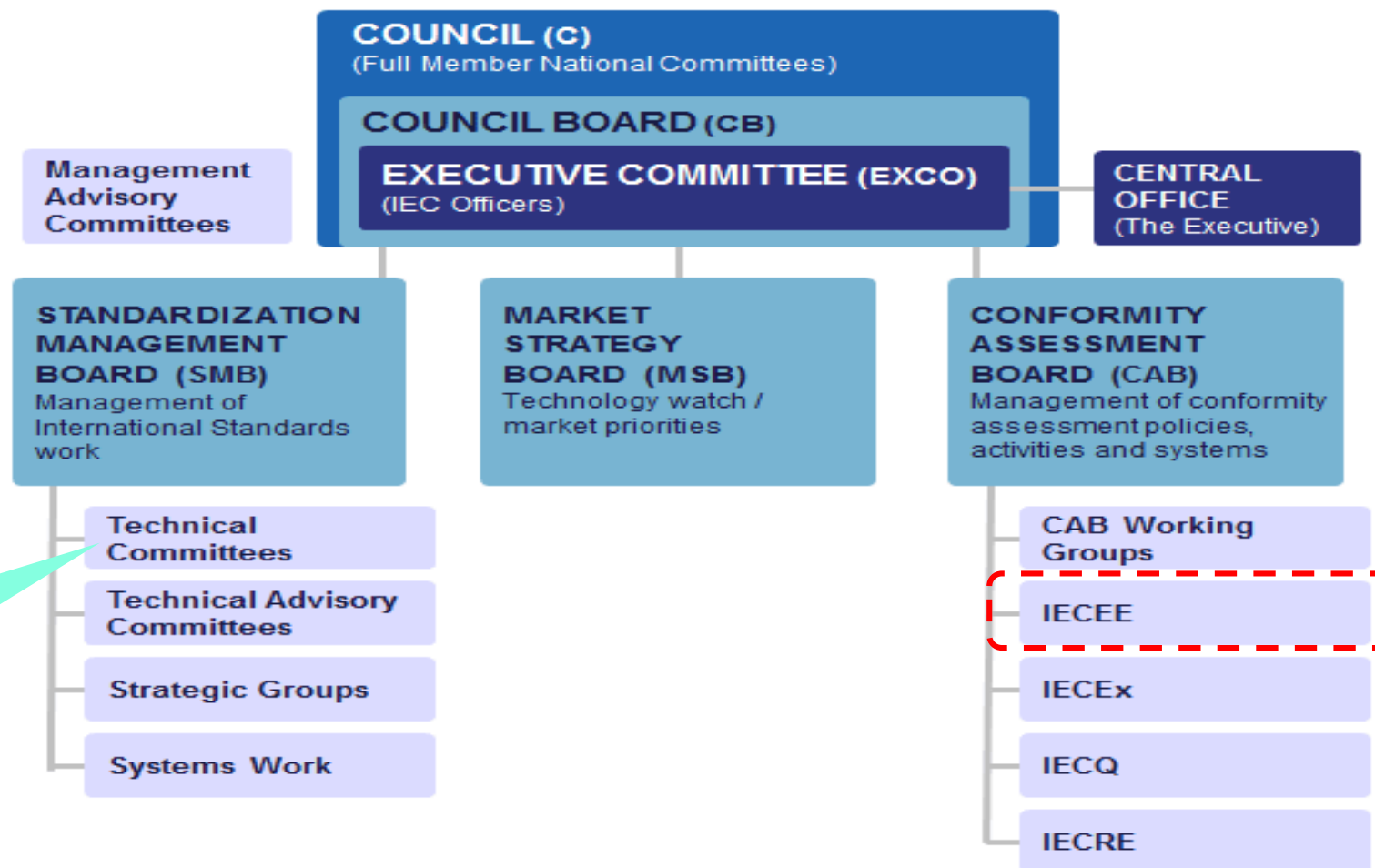
IEC 62443-4-2:2019の発行に合わせて一新。特定製品の開発プロセス・セキュリティ機能・脆弱性評価を実施する点はEDSA認証から大きく変化はない



IEC配下組織のIECEEが開発する認証制度。IECEEでは「CBスキーム」と呼ばれる世界共通の製品やシステムの安全性・セキュリティを評価・相互承認の仕組みを提供

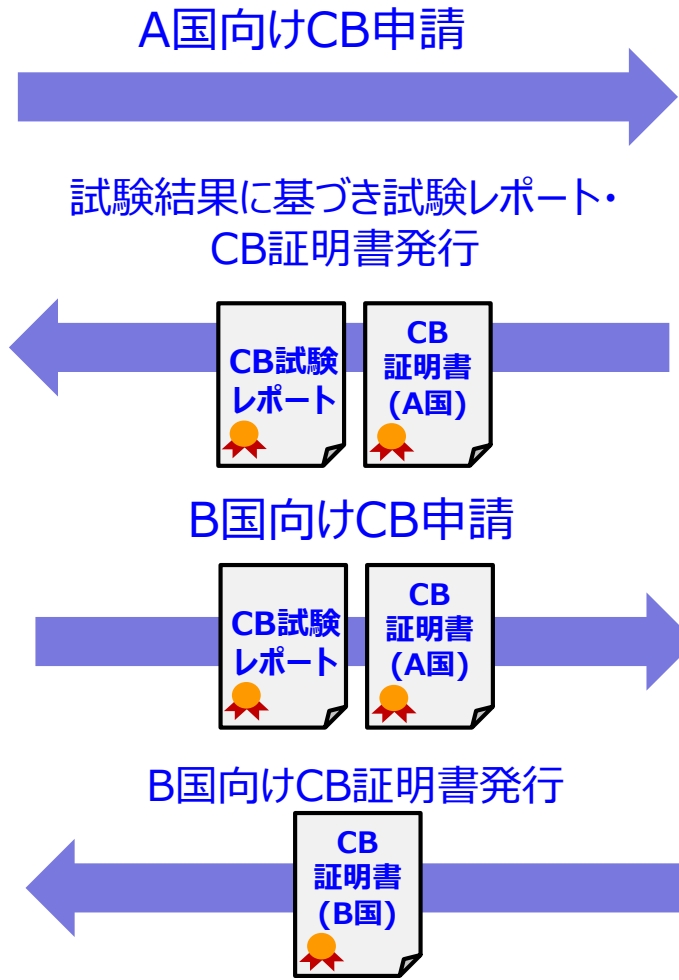
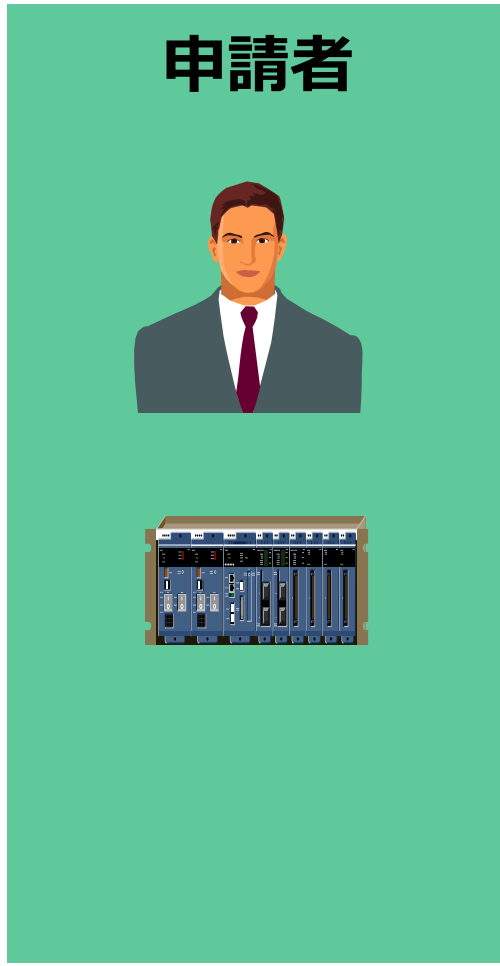
*IECEE: IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components

*CB: Certification Body



Technical Committee(TC)
規格を策定するGr

CB(Certification Body)スキーム



A国(CBスキーム加盟国)

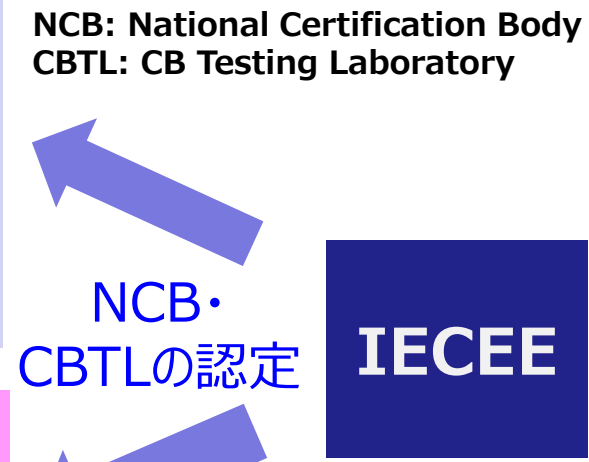
A国の認証機関
(NCB) CB試験場
(CBTL)

NCB: National Certification Body
CBTL: CB Testing Laboratory

B国(CBスキーム加盟国)

B国の認証機関
(NCB)

NCB: National Certification Body



- CBスキームにおけるセキュリティ試験・評価のシナリオはIECEEが策定する「OD 2061 (Industrial Cyber Security Program)」に基づき実施。

シナリオ 1：能力(Capability)評価（技術：3-3/4-2 プロセス：2-4/4-1）

シナリオ 2：特定の製品・ソリューションに対する能力の応用評価(Application of Capabilities)

各シナリオと参照規格との対応関係

	IEC 62443-2-4	IEC 62443-3-3	IEC 62443-4-1	IEC 62443-4-2
プロセス	シナリオ 1	—	シナリオ 1	—
製品	シナリオ 1	シナリオ 1 ※必要時に4-1のシナリオ 2 評価結果を参照	シナリオ 2 ※3-3と4-2のシナリオ 1 評価結果と共に評価	シナリオ 1 ※4-1のシナリオ 2 評価結果と共に評価
ソリューション	シナリオ 2	—	—	—

出典：www.iecee.org（内容を元に作図）

- 規格に対応するCB試験レポートの標準フォーマット(Test Report Form：TRF)が利用可

— IEC62443_2_4B (2018.6)

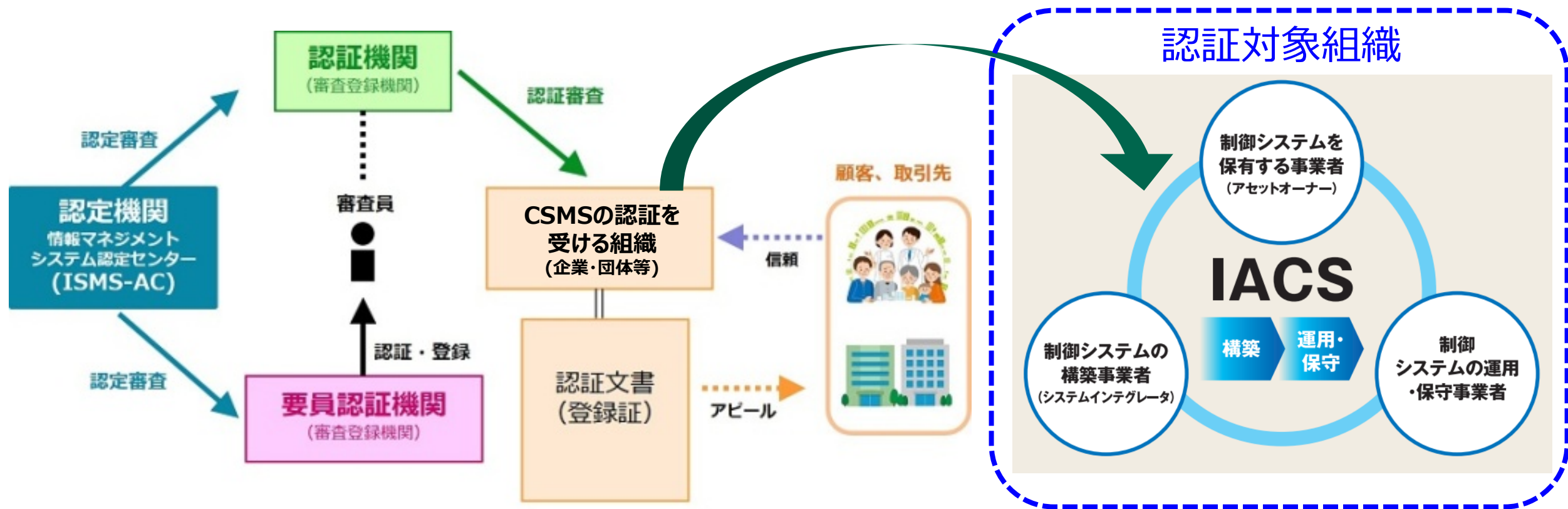
— IEC62443_4_1A (2018.6)

— IEC62443_3_3A (2018.6)

— IEC62443_4_2A (2019.6)

制御システム(IACS)を運用・開発する組織のセキュリティマネジメントシステム(CSMS)を評価

IEC 62443-2-1 Ed1.0の要求事項に準拠するセキュリティマネジメントシステム (Cyber Security Management System: CSMS) への適合性を評価



ISAが提供するIEC 62443に精通し、IEC 62443に準拠する
コントロールの実践能力を評価する要員認証プログラム

ISA/IEC 62443 Cybersecurity Certificate Programs



- **Certificate 1:** ISA/IEC 62443 Cybersecurity Fundamentals Specialist
- **Certificate 2:** ISA/IEC 62443 Cybersecurity Risk Assessment Specialist
- **Certificate 3:** ISA/IEC 62443 Cybersecurity Design Specialist
- **Certificate 4:** ISA/IEC 62443 Cybersecurity Maintenance Specialist
- **ISA/IEC 62443 Cybersecurity Expert:** Individuals who achieve Certificates 1, 2, 3, and 4 are designated as ISA/IEC 62443 Cybersecurity Experts.

- 制御システムのセキュリティ対策の必要性は認知されつつあり、セキュリティ対策の取りかかりとしてIEC 62443シリーズを中心とした標準が活用され始めている。
- IEC 62443シリーズは様々な分野や業界で参照されており、制御システムセキュリティ分野で特に注目すべき標準の一つである。
- IEC 62443シリーズは日々アップデートされている。シリーズ全体の一貫性の確保が今後の課題。
- IEC 62443シリーズの要求事項への準拠性を認証する制度が始まっており、システム・製品だけでなく、開発プロセス、組織のセキュリティマネジメント、要員を対象とした認証制度も展開されている。

HITACHI
Inspire the Next