YOKOGAWA

Co-innovating tomorrow™



# IEC 62443制御システムセキュリティ規格の現状

## ～概要と最新の状況の紹介～

IEC/TC65/WG10 国際エキスパート

横河電機株式会社　星野 浩志 （発表者）

株式会社日立製作所　藤田 淳也

三菱電機株式会社　神余 浩夫

2023年02月09日

# 内容

1. 重要インフラセキュリティをとりまく状況
2. IEC 62443の概要と文書発行・改定状況
3. IEC 62443を取り巻く状況と標準化最新状況
4. 規格適合性評価・認証の状況

# 重要インフラセキュリティをとりまく状況

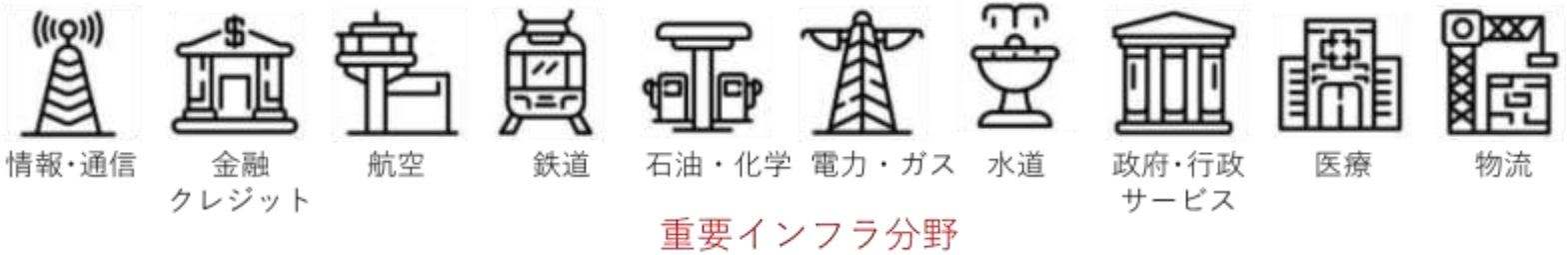
# 重要インフラセキュリティをとりまく状況

## ■ 重要インフラのサイバーセキュリティは「経営問題」から「経営の重要事項」へシフト

- 「サイバーセキュリティは**経営問題**」であり「セキュリティ投資は必要不可欠かつ経営者としての責務」である
  経済産業省/IPA「サイバーセキュリティ経営ガイドライン Ver2.0」(2017年11月16日) ⇒Link

シフト

- 「重要インフラ事業者等においては、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応を一層促進する。特に、**経営の重要事項**としてサイバーセキュリティを取り込む方向で推進する」
  内閣官房サイバーセキュリティ戦略本部「重要インフラのサイバーセキュリティに係る行動計画」(2022年6月17日) ⇒Link




サイバーセキュリティは、システム運用・開発部門だけの問題ではなく
組織統治に組み入れる必要のある、事業リスクに関する問題

# 重要インフラセキュリティをとりまく状況(続き)

- **サイバーセキュリティは、重要インフラ事業者、システムインテグレータ、サービスプロバイダ、産業制御システム・機器サプライヤすべての重要事項**
  - サイバーセキュリティ問題が事業リスクに影響する点では同じ
  - サプライチェーン全体でセキュリティリスクに取り組む必要がある

産業制御システムのサプライチェーン全体に関係する
国際標準規格 IEC 62443の重要性の高まり

# IEC 62443の概要と文書発行・改定状況

注意：IEC62443の標準化状況は、2022年11月時点のものであり今後の審議の進み方によって変更される可能性がある。

# 国際標準 ISA/IEC 62443とは

**産業用オートメーション及び制御システム(IACS)のセキュリティを確保するための国際標準規格**

## ■ だれが国際標準を開発しているか？

- 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

  ISA99発行規格文書　　：ANSI/ISA-62443
  IEC/TC65/WG10発行規格文書：IEC 62443
  } 通称 **ISA/IEC 62443**

## ■ 産業用オートメーション及び制御システム(IACS)とは？

- Industrial Automation and Control System (IACS)
  - 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)
- IACSは、制御プロセスの安全で確実な運用に影響する可能性のある、**人員、ハードウェア、ソフトウェア、手順、プロセス、およびポリシーの集合体**

## ■ IEC 62443が活用されている分野

- 化学、石油、ガス、パイプライン、機器製造、電力分野などでセキュリティ対策の標準規格の一つとして参照
- 鉄道、ビルオートメーション、医療機器分野なども注目

# ISA/IEC 62443 制御システムセキュリティの標準化の経緯

## 2002年 ISAによる取り組み開始

- ISA(International Society of Automation)は米国中心の学会
- 2002年10月、ISA99制御システムセキュリティ標準の開発開始の発表
  - ANSI/ISA 99.00.01:2007 - Security Technologies for Industrial Automation and Control Systems
  - 当初、PLCやフィールドネットワークが直接狙われるとは考えておらず、Windows/UNIXやTCP/IP、Webアプリケーション等のエンタープライズ向けシステムやコンポーネントが攻撃対象と考えられていた

## 2011年 Stuxnetによる制御システムへのサイバー攻撃

- コントローラ(DCS/PLC)や独自ネットワークも直接攻撃される ⇒ 制御システムセキュリティの再検討

## 2013年 ISA/IEC 62443シリーズの開発開始

- ISA99とIEC/TC65/WG10の共同開発(2013～)
  - ISA99メンバの多くがIEC/TC65/WG10に合流
  - ISA99のWGが技術検討し、IEC/TC65/WG10から国際提案・投票を経て国際規格化

TC: Technical Committee, TC65:産業用オートメーション・制御システム(IACS)の標準化活動を担うTC
WG: Working Group

# IEC 62443 標準化の状況

## ■ 標準化の状況

- ISA(S99)、IEC(TC65/WG10)の共同作業により、主要な規格文書が発行済み

- 上記規格文書を元にした第三者評価・認証制度が、ISAおよびIECEEによって推進されている
  - ISA/IEC 62443-4-1, 4-2, 3-3, 2-4 の認証制度

- NIST Cyber Security Frameworkからも、対応する要件が参照されている
  - IEC 62443の元となるISAの
    ISA-62443-2-1(セキュリティマネジメントシステムの構築)
    ISA-62443-3-3(制御システムのセキュリティ機能要件)

- 国内でJIS化の活動開始(2021年から)
  - JIS化により国内法令から参照可能となり、強制力を持つことができる


NIST Cybersecurity Framework Version 1.1

IECEE: IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components
NIST: National Institute of Standards and Technology

# IEC62443シリーズ文書の発行・改定状況 – 概要

| | | | | | |
|---|---|---|---|---|---|
| **Horizontal** | OT Cybersecurity | | | | |
| **Part 1 General** | TS 62443-1-1 Concepts & Models | 62443-1-2 Reserved | 62443-1-3 Performance Metrics | TR 62443-1-4 Security Lifecycle | TS 62443-1-5 Scheme for Security profiles |
| **Part 2 Policies** | 62443-2-1 Security Program requirement | 62443-2-2 Security protection | TR 62443-2-3 Patch management | 62443-2-4 Service providers | TR 62443-2-5 Implementation guide for asset owners |
| **Part 3 System** | TR 62443-3-1 Security Technologies | 62443-3-2 Security Risk Assessment | 62443-3-3 System security Requirements | | |
| **Part 4 Component** | 62443-4-1 Secure product Development Lifecycle | 62443-4-2 Security requirement for Components | PAS 62443-4-3 Application to IIoT | | |
| **Part 6 Conformity** | TS 62443-6-1 Security evaluation for Service Providers (2-4) | TS 62443-6-2 Security evaluation for Components (4-2) | | | 改訂・作成中 |

黒字：IEC文書発行済または審議中
白字：IEC文書未審議

IS:International Standard, TR:Technical Report, TS:Technical Specification,
PAS: Publicly Available Specification

出展：IEC/TC65/WG10審議状況およびISA99 Working Groupの情報を元に作成

# IEC62443シリーズ文書の発行・改定状況 – 詳細

| Category /分類 | IEC No. | Edition /版 | Type /文書タイプ | Title /タイトル | 概要 | 発行日 | ステータス | 発行予定日 |
|---|---|---|---|---|---|---|---|---|
| General | 62443-1-1 | 1.0 | TS | Terminology, concepts and models | 用語、コンセプト、モデルの定義 | 2009-07-30 | 発行済 | |
| | | 2.0 | TS | Terminology, concepts and models | 用語、コンセプト、モデルの定義 | - | IEC審議準備中 | |
| | 62443-1-2 | - | TR | Reserved | 欠番(元は用語・略語集の予定だった) | - | - | |
| | 62443-1-3 | 1.0 | TR | Performance metrics for IACS security | IACSセキュリティパフォーマンス評価基準 | - | IEC審議準備中 | |
| | 62443-1-4 | 1.0 | TR | Security lifecycle and use cases | IACSセキュリティライフサイクルとユースケース | - | ISA99開発中 | |
| | 62443-1-5 | 1.0 | TS | Scheme for IEC 62443 cyber security profiles | IEC 62443のプロファイル(特定分野規格)作成ルール | - | IEC審議中 | 2023-09 |
| Policies and Procedures | 62443-2-1 | 1.0 | IS | Establishing an industrial automation and control system security program | セキュリティマネジメントシステムの構築 | 2010-11-10 | 発行済 | |
| | | 2.0 | IS | Security program requirements for IACS asset owners | IACSアセットオーナーに対するセキュリティプログラム要求事項 | - | IEC審議中 | 2023-06 |
| | 62443-2-2 | 1.0 | IS | IACS Security Protection | IACSセキュリティプロテクション(技術要件+プロセス要件) | - | IEC審議中 | 2023-12 |
| | 62443-2-3 | 1.0 | TR | Patch management in the IACS environment | IACSにおけるパッチ管理方式 | 2015-06-30 | 発行済 | |
| | | 2.0 | IS | Security Update (Patch) management in the IACS environment | IACSにおけるセキュリティ更新（パッチ）管理方式 | | IEC審議準備中 | |
| | 62443-2-4 | 1.1 | IS | Security program requirements for IACS service providers | IACSサービス提供者に対するセキュリティ要求事項 | 2017-08-24 | 発行済 | |
| | | 2.0 | IS | Security program requirements for IACS service providers | IACSサービス提供者に対するセキュリティ要求事項 | - | IEC審議中 | 2023-10 |
| | 62443-2-5 | 1.0 | TR | Implementation guidance for IACS asset owners | アセットオーナ向け実装ガイド | - | ISA99準備中 | |

IS:International Standard, TR:Technical Report, TS:Technical Specification,
PAS: Publicly Available Specification

出展：IEC/TC65/WG10審議状況およびISA99 Working Groupの情報を元に作成

# IEC62443シリーズ文書の発行・改定状況 – 詳細（つづき）

| Category /分類 | IEC No. | Edition /版 | Type /文書タイプ | Title /タイトル | 概要 | 発行日 | ステータス | 発行予定日 |
|---|---|---|---|---|---|---|---|---|
| System | 62443-3-1 | 1.0 | TR | Security technologies for industrial automation and control systems | IACSで利用可能なセキュリティ技術 | 2009-07-30 | 発行済 | |
| | | 2.0 | TR | - | - | - | ISA99準備中 | |
| | 62443-3-2 | 1.0 | IS | Security risk assessment for system design | セキュリティリスク分析とシステム設計 | 2020-06-24 | 発行済 | |
| | 62443-3-3 | 1.0 | IS | System security requirements and security levels | 制御システムのセキュリティ機能要件 | 2013-08-07 | 発行済 | |
| | | 2.0 | IS | - | - | - | ISA99準備中 | |
| Component | 62443-4-1 | 1.0 | IS | Secure product development lifecycle requirements | セキュアな制御機器の開発プロセス | 2018-01-15 | 発行済 | |
| | 62443-4-2 | 1.0 | IS | Technical security requirements for IACS components | 制御機器のセキュリティ機能要件 | 2019-02-27 | 発行済 | |
| | 62443-4-3 | 1.0 | PAS | Application of the IEC 62443 standards to the Industrial Internet of Things | IEC 62443のIIoTへの適用 | - | IEC審議準備中 | - |
| Profiles | 62443-5-X | - | - | - | TC65内の分野向けの規格(Profile)がここに追加される見込み | - | - | - |
| Conformity | 62443-6-1 | 1.0 | TS | Security evaluation methodology for IEC 62443 – Part 2-4: Security program requirements for IACS service providers | IEC 62443-2-4 を用いたセキュリティ評価手法 | - | IEC審議中 | 2023-12 |
| | 62443-6-2 | 1.0 | TS | Security evaluation methodology for IEC 62443 – Part 4-2: Technical security requirements for IACS components | IEC 62443-4-2 を用いたセキュリティ評価手法 | - | IEC審議中 | 2024-02 |

IS:International Standard, TR:Technical Report, TS:Technical Specification,
PAS: Publicly Available Specification

出展：IEC/TC65/WG10審議状況およびISA99 Working Groupの情報を元に作成

# IEC 62443を取り巻く状況と標準化最新状況

# 国際標準 IEC 62443を取り巻く状況

| IEC 62443関係の市場動向 | 関連するIEC/TC65、ISA99等の活動 | 関連する規格 |
|---|---|---|
| **事業環境・体制の変化**<br>• デジタルトランスフォーメーションの進展<br>• クラウドサービス利用の拡大<br>• IT/OTの組織間連携の進展 | • IEC 62443全体コンセプト・モデルの議論<br>• クラウド環境利用時の責任・役割の議論<br>• ISMSとの連携の議論 | IEC 62443-1-1<br>-<br>IEC 62443-2-1 |
| **業界団体でのIEC 62443活用の進展**<br>• システム・機器サプライヤへのセキュリティ関係要求への活用（電力、化学、石油、ビル、鉄道など） | 特定分野用規格(Profile)作成ルールの標準化 | IEC 62443-1-5<br>IEC 62443-5-X |
| **認証・法令・規制によるIEC 62443活用の進展**<br>• 各国で第三者評価・認証に活用(ISASecure、IECEEの62443関係認証)<br>• 法令・規制で参照される可能性(欧州NIS2指令、サイバーセキュリティ法) | 評価認証におけるセキュリティ評価手法の標準化<br>• IEC 62443-2-4: システムインテグレータ、保守サービスプロバイダ<br>• IEC 62443-4-2: 制御機器 | IEC 62443-6-1<br>IEC 62443-6-2 |
| **産業オートメーション以外のOT機器へのIEC 62443活用の動き** | • OTセキュリティの水平規格化の議論<br>• IEC 62443全体のロードマップや、要求項目の整理・見直しの議論 | IEC 62443<br>すべて |

NIS2指令：EU全体のサイバーセキュリティ対策に関する指令

# IEC 62443全体コンセプト・モデルの議論 - (IEC 62443-1-1 改定中)

## IEC TS 62443-1-1 Ed1.0 - Terminology, concepts and models

- 2009年発行の、ISA/IEC 62443シリーズ全体にかかわる共通コンセプト・モデルを定義した技術仕様書
- 用語の定義や要求の分類、モデルの定義などが古いまま

## IEC TS 62443-1-1 Ed2.0

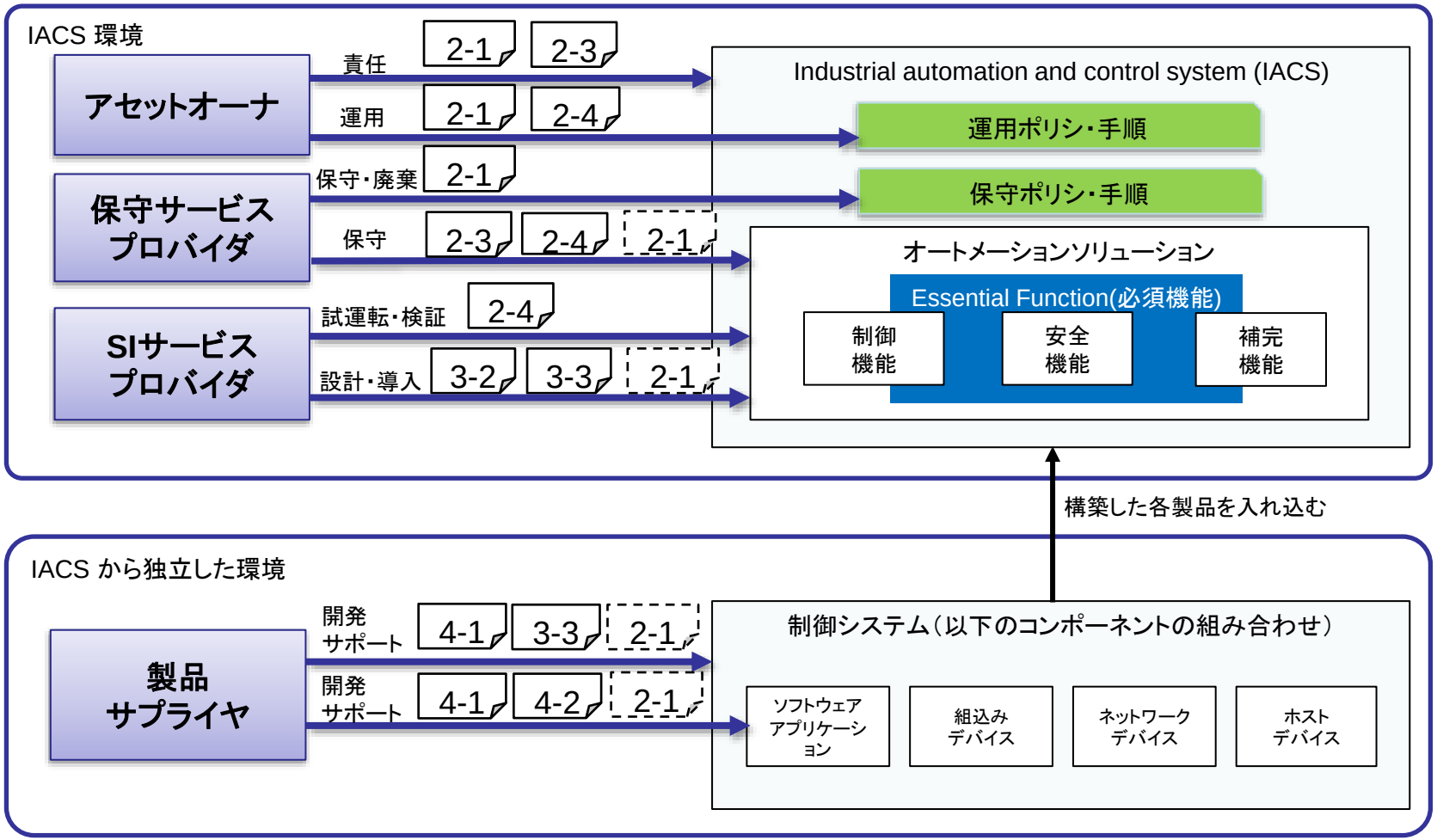
改定のため IEC審議準備中

- これまでに発行されたISA/IEC 62443の各文書で記載された、コンセプト・モデルを集約
  - IACSに関係する役割・責任モデル
  - ライフサイクルモデル
  - IACS構成要素
  - ゾーン・コンジットモデル
  - セキュリティレベル
  - マチュリティレベル（プロセスの成熟度）
  - FR(Foundational Requirements), SPE(Security Program Elements)
  - 等

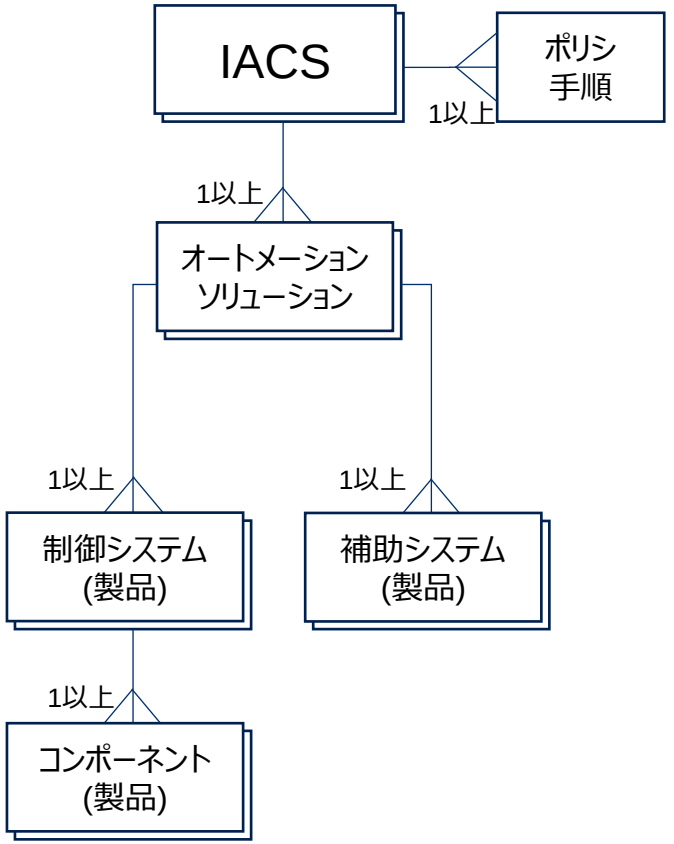
次のスライドで説明

# IACSに関係する役割・責任モデル - (IEC 62443-1-1 改定中)

## IACSに関係する役割・責任




## IACS構成要素の関連図

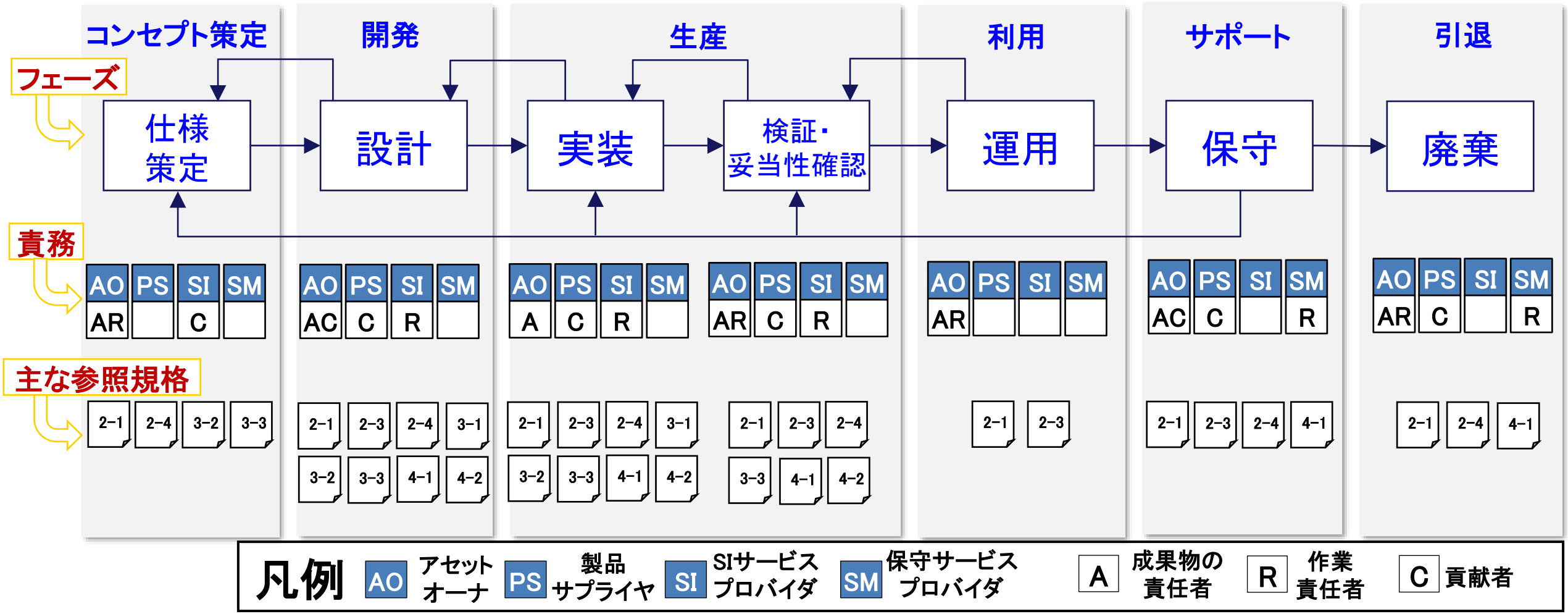



参照する主なIEC 62443文書番号を記載(2-1はEd2.0 draft)
すべての文書を図中に網羅していない。

出展：IEC 62443-1-1 Ed2.0ドラフト版およびISA99 Working Groupの情報を元に作成・一部加筆

# ライフサイクルモデル – (IEC 62443-1-1 改定中)

IACSのライフサイクルの各フェーズにおける役割




出典：IEC 62443-1-1 Edition 2.0 ドラフト版（内容を元に再作図・追記）

# 事業者(アセットオーナー)に求められること - ISMSとの連携 (IEC 62443-2-1 改定中)

## IEC 62443-2-1 Ed1.0 - Establishing an industrial automation and control system security program

- 2010年発行の、事業者(アセットオーナー)におけるIACSのサイバーセキュリティマネジメントシステム(CSMS)の規格
  - システムのセキュリティ上のリスクの明確化と、リスクに対処するための体制(CSMS)の構築
  - 上記体制の監視と改善の継続

## IEC 62443-2-1 Ed2.0 - Security program requirements for IACS asset owners

2023-06発行予定

- Security Program(SP)とは
  - IACSに適用可能なセキュリティサービス(保守・SI)の一覧と、それに関係する管理体制・運用プロセス・製品
- 事業者に求められる「セキュリティ管理体制の構築」は、Ed1.0から変わらず
- ただしEd1.0のCSMSの規定は削除となり、ISMS(ISO 27001,27002)を参照
  - 理由：微妙に異なるマネジメントシステムの乱立を防ぐ目的
- SP要素(SPE)として以下の８つの分類を規定

- ITとOTそれぞれのエリアで個別に適切なセキュリティ対策を実施
- セキュリティ管理体制は共通のフレームワークを活用して構築

| | |
|---|---|
| SPE1 | 組織のセキュリティ対策 |
| SPE2 | 構成管理 |
| SPE3 | ネットワークと通信のセキュリティ |
| SPE4 | コンポーネントセキュリティ |

| | |
|---|---|
| SPE5 | データの保護 |
| SPE6 | ユーザアクセス制御 |
| SPE7 | イベントとインシデントの管理 |
| SPE8 | システムの完全性と可用性 |

SPE: Security Program Element

# システムインテグレータ・サービスプロバイダへの要求 - (IEC 62443-2-4 改定中)

## IEC 62443-2-4 Ed1.1 - Security program requirements for IACS service providers

- 2017年発行の、サービスプロバイダの能力に関する要求をまとめた基本規格

| SP Req. ID | カテゴリ（機能エリア） |
|---|---|
| SP.01.XX | ソリューション人員割り当て |
| SP.02.XX | 保証 |
| SP.03.XX | アーキテクチャ |
| SP.04.XX | 無線 |
| SP.05.XX | SIS(安全計装システム) |
| SP.06.XX | 構成管理 |

| SP Req. ID | カテゴリ（機能エリア） |
|---|---|
| SP.07.XX | リモートアクセス |
| SP.08.XX | イベント管理 |
| SP.09.XX | アカウント管理 |
| SP.10.XX | マルウェア保護 |
| SP.11.XX | パッチ管理 |
| SP.12.XX | バックアップ／復旧 |

## IEC 62443-2-4 Ed2.0

2023-10発行予定

- 新規の要求事項を追加することではなく、サービスプロバイダ(保守・SI)の役割に対する要求として誤解の生じないように、記載を見直すことが中心
- 次のEd3.0改定の準備的位置づけでもある

# 分野用規格(Profile)作成ルール - (IEC 62443-1-5 作成中)

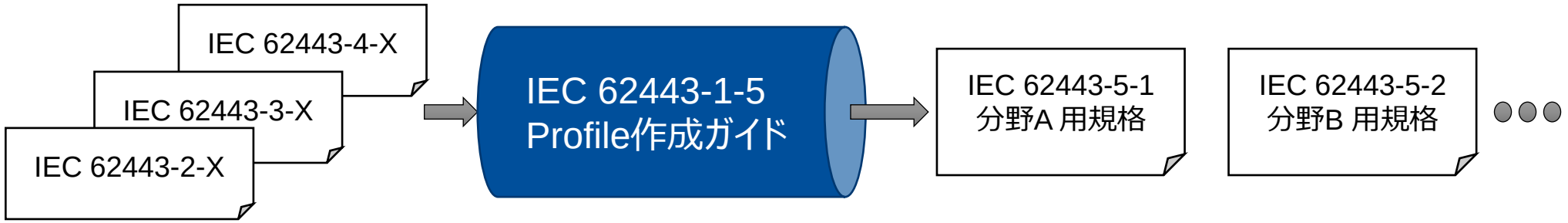
## IEC TS 62443-1-5 – Scheme for IEC 62443 cyber security profiles

2023-09発行予定

- IEC 62443を元に新たに分野向け規格(Profile)を作成する場合のガイド
- IEC 62443-2-X, 3-X, 4-X から既存の要求項目から、特定分野向け規格を作成する
- 要求項目からの抜粋であり、新たな要求項目の追加はしない

## IEC 62443-5-X

- TC65内の分野向けの規格(Profile)がここに追加される見込み
- ISA99でElectric Energy関係Profile作成中



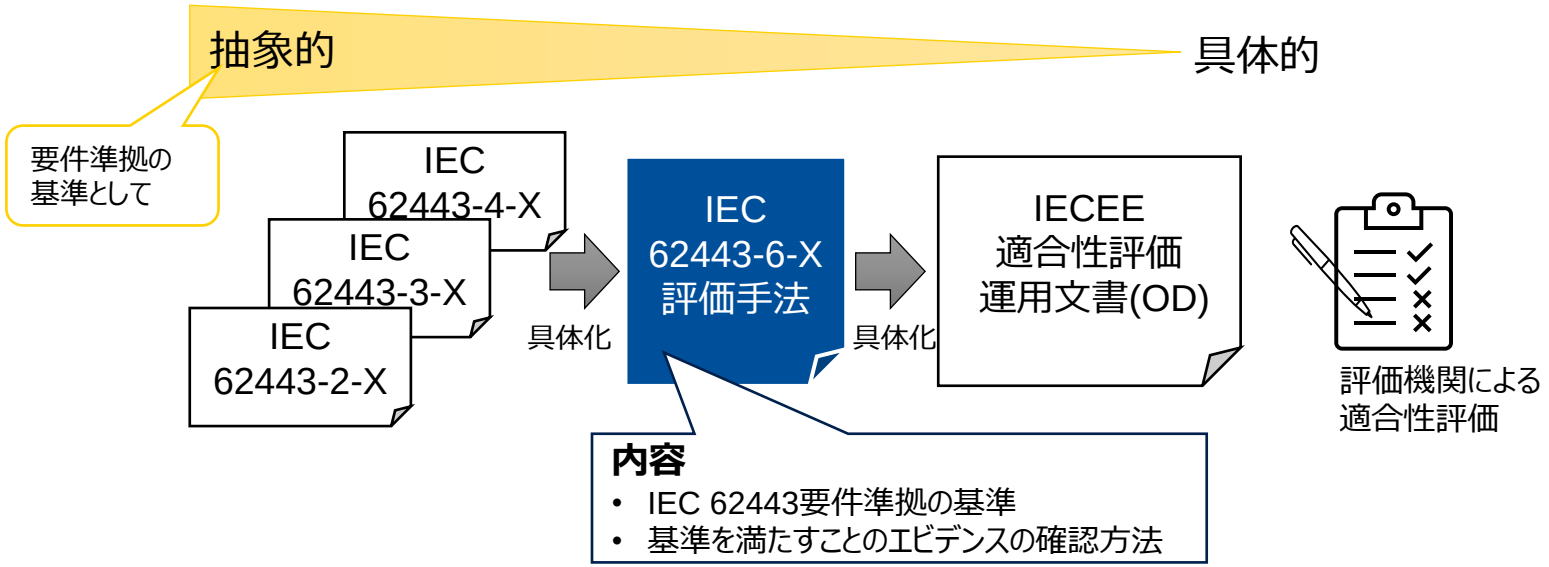
# セキュリティ評価手法の標準化 - (IEC 62443-6-1, 6-2 作成中)

- **IEC TS 62443-6-1 - Security evaluation methodology for IEC 62443 – Part 2-4**
  - IEC 62443-2-4 規格適合性評価のための技術基準
  - SIサービス/保守サービスプロバイダの主に成熟度(Maturity Level: ML1～ML4)の評価基準の明確化

2023-12発行予定

- **IEC TS 62443-6-2 - Security evaluation methodology for IEC 62443 - Part 4-2**
  - IEC 62443-4-2 規格適合性評価のための技術基準
  - 主に機器（コンポーネント）のセキュリティ機能の評価基準の明確化

2024-02発行予定




**背景**

- 取り組みのきっかけは、規格適合性評価の方法を開発するIECEE のワーキンググループからIEC/TC65/WG10への基準作成依頼
- 二つの基準(6-1, 6-2)作成のプロジェクトのリーダは、いずれもドイツの評価機関等で活動

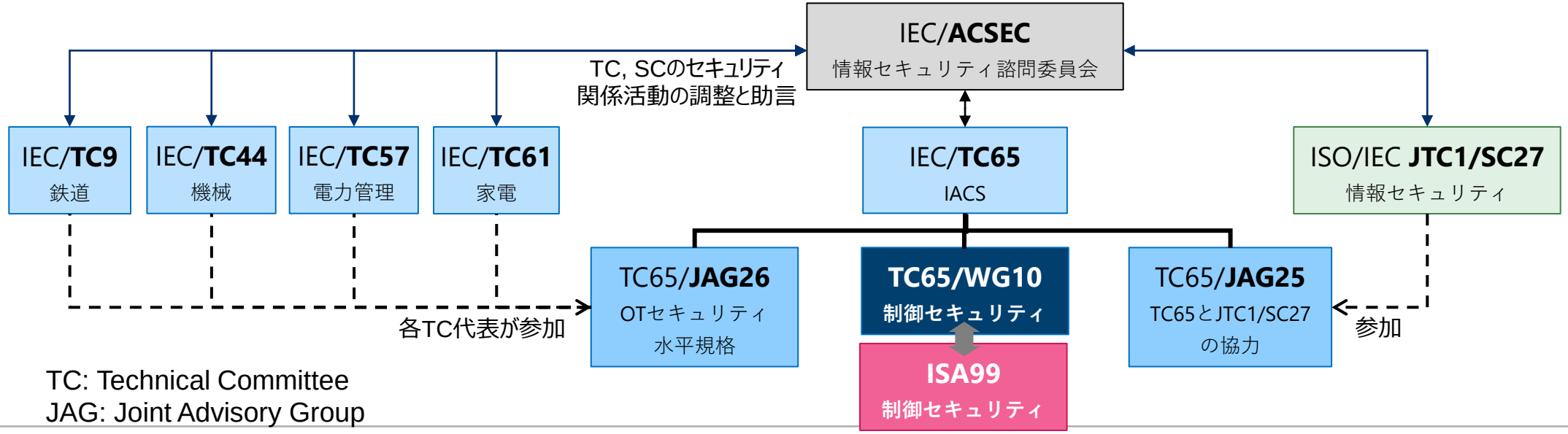
# OTセキュリティの水平規格化

## OTセキュリティの水平規格化とは

- 産業オートメーション以外の分野の、汎用的なOperational Technology (OT) のサイバーセキュリティ標準の開発

## 取り組み状況

- IEC/TC65にOTセキュリティの水平規格化の役割をアサイン
- 現在、関連TC代表が参加する合同諮問委員会(JAG26)を立ち上げ中
  - Horizontal security function for OT linked to TC 9, TC 44, TC 57, TC 61, ISO/IEC JTC 1/SC 27
- 各TCの意見をふまえて、まず『Operational Technology (OT) 』という用語の定義を議論中




TC: Technical Committee
JAG: Joint Advisory Group

# 規格適合性評価・認証の状況

# ISASecure 認証

ISASecureとは
制御システム・機器が ISA/IEC 62443 で規定された
要求を満たすことを評価するスキーム

## 概要

- ISAの下部組織ISCIが開発・運営するセキュリティ認証スキーム
- 提供中の認証プログラム( 3 種類)

| 認証プログラム | 対象 | 対応する IEC 62443規格 |
|---|---|---|
| CSA認証 | 組込み機器、アプリケーションソフトウェア、ネットワークデバイス、ホストデバイス（旧EDSA認証は組込み機器のみ対象） | IEC 62443-4-2 (機能要件)<br>IEC 62443-4-1 (開発プロセス) |
| SSA認証 | システム（例：HMI+コントローラ+ネットワークデバイス） | IEC 62443-3-3 (機能要件)<br>IEC 62443-4-1 (開発プロセス) |
| SDLA認証 | セキュリティ開発プロセス | IEC 62443-4-1 (開発プロセス) |

- 新たな認証プログラムのアナウンス(2022年9月)

| | | |
|---|---|---|
| ICSA認証 | IIoT コンポーネント（IIoTデバイスとIIoTゲートウェイ） | IEC 62443-4-2 (機能要件)<br>IEC 62443-4-1 (開発プロセス)<br>ICSA用の追加基準あり |

認証取得状況
https://www.isasecure.org/en-US/End-Users/IEC-62443-4-2-Certified-Components

ISCI: ISA Security Compliance Institute
https://isasecure.org/
CSA: Component Security Assurance
SSA: System Security Assurance
SDLA: Security Development Lifecycle Assurance
ICSA: IIoT Component Security Assurance

# IECEEセキュリティ認証

IEC/CAB/IECEEとは
IEC規格適合性評価評議会/電気機器安全規格適合試験制度
電気機器の安全関連の認証制度を扱う

## ■ 概要

- IECの規格適合性認証制度として、セキュリティ認証スキームを IECEE/CMC/WG31が開発
- TUV，UL，CSA，JQA，ITEI等の主な審査機関が議論に参加
- IEC 62443規格適合性評価の方法のガイダンス運用文書(Operational Document)を開発・発行
  - OD-2061: Industrial Cyber Security Program
    IEC 62443-2-4, 62443-3-3, 62443-4-1, 62443-4-2 に基づく評価のシナリオを策定
  - OD-2020-F8 Cyber Security TRF Template (TRF: Test Report Form)
- 評価の技術基準等をIECEE/CMC/WG31からTC65/WG10に開発依頼
  - TC65/WG10で IEC TS 62443-6-1, 6-2 を開発中
- 認証取得状況
  - https://certificates.iecee.org/#/search

# 最後に

# 国際標準化活動への参加の意義

## ■ 背景

- 産業制御システム・機器のサイバーセキュリティの国際標準・ガイドライン（あるべき姿）
  法令・規制（市場参入条件）が大きく進展しつつある
  - 欧州NIS2指令、サイバーセキュリティ法、サイバーレジリエンス法
    中国サイバーセキュリティ法など

背景に、国際標準・
ガイドラインあり

## ■ 国際標準化活動参加の意義

- 法令・規制の元となる国際標準の動向と
  市場要求の方向性・重要性の見極め
- 組織に必要な体制・能力の強化と
  必要なセキュリティ対策の実現

「マーケティング」を強化し
これらにいち早く取り組むことで
自社ビジネスの優位性を確保する

# IEC 62443関連の国内の活動

## IEC/TC65/WG10 国内委員会

- IEC 62443の国際標準化活動
- メンバー構成
  - 18企業・団体、約40名が国内委員会に参加
  - 5企業・団体から、国際エキスパートとして標準化活動に参加
    日立製作所、三菱電機、安川電機、横河電機、CSSC

IEC/TC65国内委員会に
関する問い合わせ先
https://www.jemima.or.jp/
⇒お問い合わせ

## IEC/TC65国内委員会 SG201 認証専門グループ

- 主に安全・セキュリティに関する認証・法規制関係の情報収集活動

## 日本規格協会(JSA) 制御システムセキュリティJIS開発研究会および原案作成委員会

- IEC 62443をベースにした、制御システムセキュリティのJIS規格開発

JIS開発に関する
問い合わせ先
https://www.jsa.or.jp/
⇒お問い合わせ

YOKOGAWA

Co-innovating tomorrow™