Deloitte.
デロイト トーマツ

制御システムセキュリティカンファレンス2025講演

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～

注意:本資料に記載されている法律、規制、および標準化の状況と情報は、発表当時のものであり、将来変更される可能性があります。

IEC/TC65/WG10 国際エキスパート

デロイト トーマツ サィバー合同会社	**市川 幸宏（発表者）**
横河電機株式会社	星野 浩志
Hitachi America, Ltd.	藤田 淳也
三菱電機株式会社	神余 浩夫

MAKING AN IMPACT THAT MATTERS since 1845

目次

1. 2024年のサイバーセキュリティ関連市場動向

経済的利益を目的としたランサムウェアの攻撃が製造業を対象に流行しています

2023年から2024年の欧州がまとめたグローバル脅威レポート

1　2023年から2024年までのサイバーセキュリティに関する脅威レポートの公開

サイバーセキュリティの脅威情報についてENISA(欧州ネットワーク情報セキュリティ機関)でレポートを公開している

2　攻撃について

[11,079]のインシデントを観測している
動機としては、政治的な意図の攻撃については多くは[DoS攻撃]で、経済的利益を意図とする攻撃については、[ランサムウェア]を使った攻撃が傾向としてみられる

3　被害について

特にランサムウェアを使った攻撃対象は、様々な対象セクタがある中で[製造業]が[全体の17%]で2位になっている
Lockbitと呼ばれるランサムウェアは、世界情勢の中で[42.65%]の攻撃を占めており、その中でも特に製造業を狙って攻撃している（分野別で[22.64%]の1位）

参照：ENISA THREAT LANDSCAPE 2024

2020-2030年は世界で様々な製品向けのセキュリティの法規制などが施行されます

各国のサイバーセキュリティ関連の法規制・ガイドライン

国・地域	法規制・ガイドライン	対象	時期
欧州	NIS 2 指令	情報システム・重要インフラ事業者向け	2024年10月から適用
	EU CRA (サイバーレジリエンス法)	製品プロバイダ向け	2027年12月から適用
日本	経済安全保障推進法の基幹インフラ事前審査	事業者向け	2024年5月から運用開始
	IoT製品に対するセキュリティ要件適合評価・ラベリング制度(JC-STAR)	IoT製品向け	2025年3月から運用開始
中国	Multi-layered Protection Scheme – MLPS 2.0	事業者向け	2020年から運用開始
	ネットワーク重要機器の強制規格 – GB40050-2021	製品プロバイダ向け	2021年8月から適用
米国	The NIST Cybersecurity Framework (CSF)2.0	全組織向け	2024年2月に改定発行
	Cybersecurity Labeling Program for Smart Devices	IoT機器向け	2024年8月から運用開始

特に欧州で施行される法規制はIEC 62443シリーズに関連していています

欧州におけるサイバーセキュリティ関連法規制の動向

製品プロバイダに関係	情報システム・重要インフラの事業者に関係
RED(無線機器指令) 更新により、サイバーセキュリティ、個人情報、プライバシー要件追加 適用：2025-08-01	**NIS2(ネットワーク・情報システム指令)** NISからNIS2に移行。重要インフラ等の事業者向けセキュリティ要件 適用：2024-10-18
MR(機械規則) 機械指令から規則に変更。サイバーセキュリティ要件追加 適用：2027-01-20	
CRA(サイバーレジリエンス法) 新規法制化進行中。デジタル製品のサイバーセキュリティ要件 施行：2024-12-10、適用：2027-12-11	

製品・コンポーネントの
「セキュリティ・バイ・デザイン」の普及

事業者のアセット・オペレーションの
セキュリティに関する説明責任の高まり

関連する規格

EN 303 645(IoT機器), EN 18031(無線機器),
IEC 62443-4-1(開発プロセス),
4-2(コンポーネント), 等が関連

ISO/IEC 27001,
IEC 62443-2-1(アセットオーナー),
2-4(サービスプロバイダ)等が関連

2. IEC 62443の概要と開発状況

ISA(国際自動制御学会)とIEC(国際電気標準会議)が連携して 62443を開発しています

国際標準 ISA/IEC 62443とは

国際標準の開発

- ISA99が開発
- IEC/TC65/WG10が開発

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

IACSとは

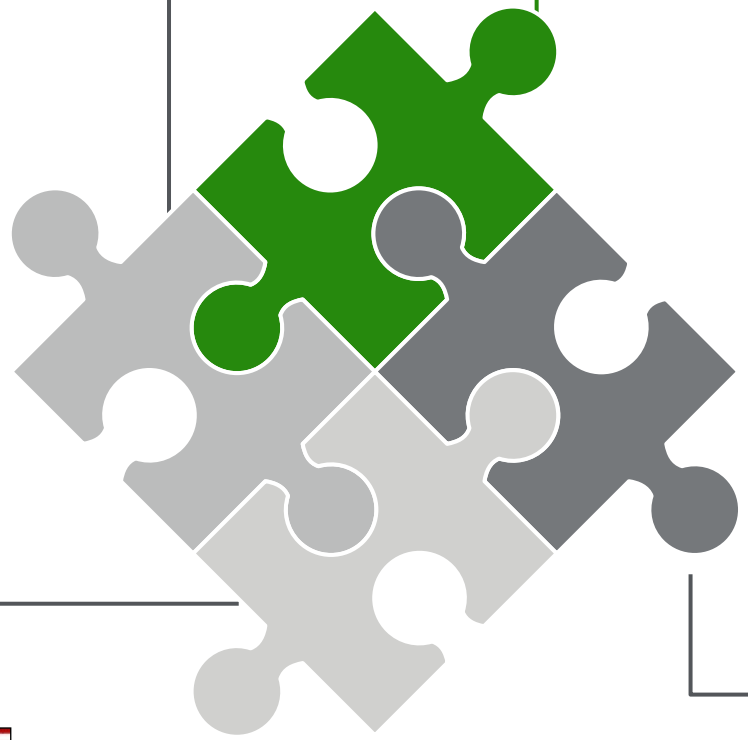
- Industrial Automation and Control System
- IEC 62443-1-1:2009 3.2.57の定義として、制御プロセスの安全、セキュリティ、信頼性(Reliability)のある運用に作用、もしくは影響する人的資産、ハードウェア及びソフトウェアの集合体
- IACSは、制御プロセスの安全で確実な運用に影響する可能性のある、**人員、ハードウェア、ソフトウェア、手順、プロセス、およびポリシーの集合体**

ISAとIECの共同作業であるIEC 62443シリーズは、第三者認証やJIS化を推進されています

ISA/IEC 62443 標準化の状況

主要な規格文書の発行
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

第三者評価・認証
本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

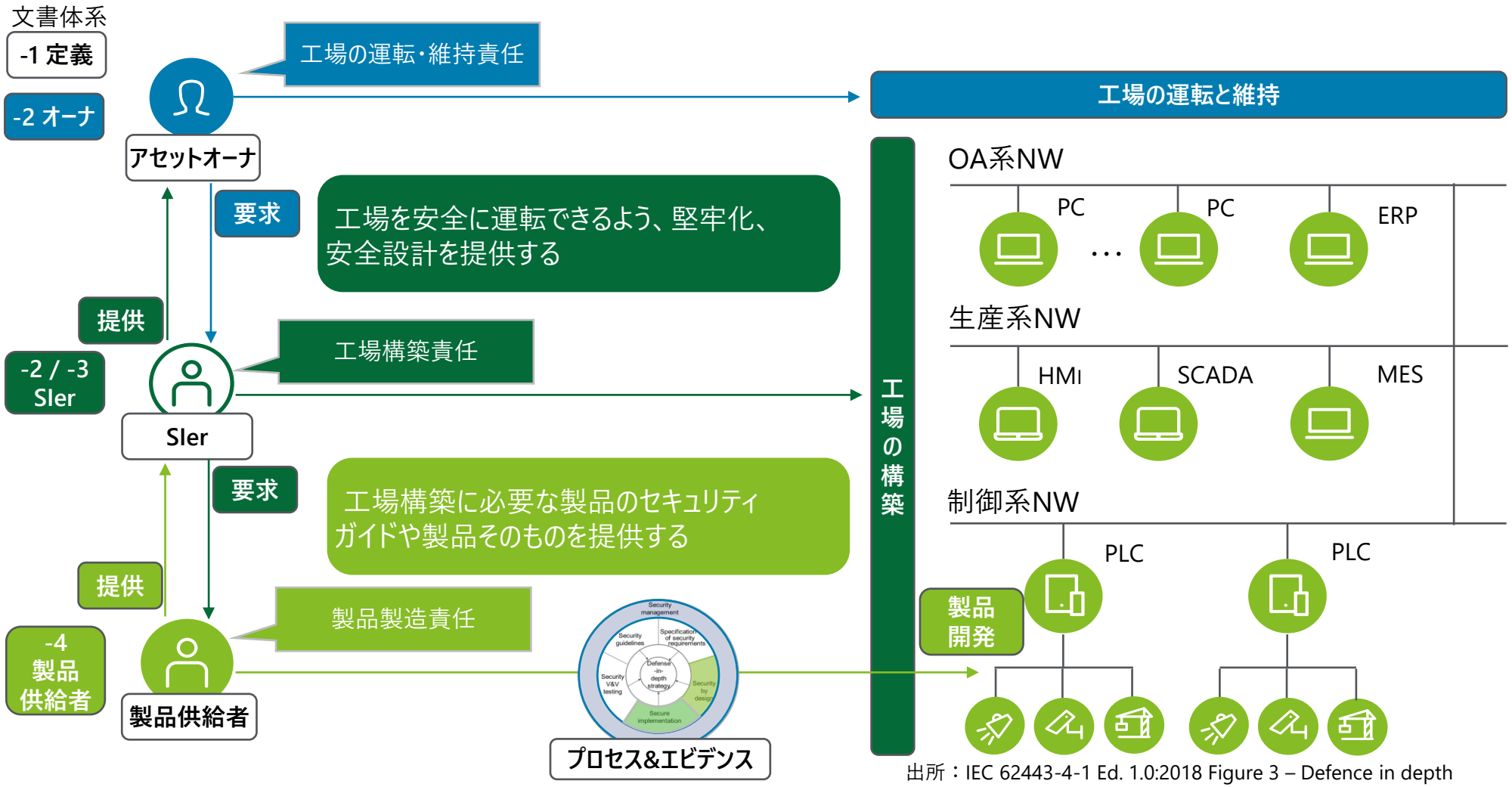


米国標準に参照
NIST Cyber Security Framework からも、対応する要件が参照されている
- ✓ IEC 62443の元となるISAの
  - ➢ ISA-62443-2-1(セキュリティマネジメントシステムの構築)
  - ➢ ISA-62443-3-3(制御システムのセキュリティ機能要件)

JIS化
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

IEC 62443は製品やプロセス単体ではなく、人・運用・システム全体でセキュリティを考えます

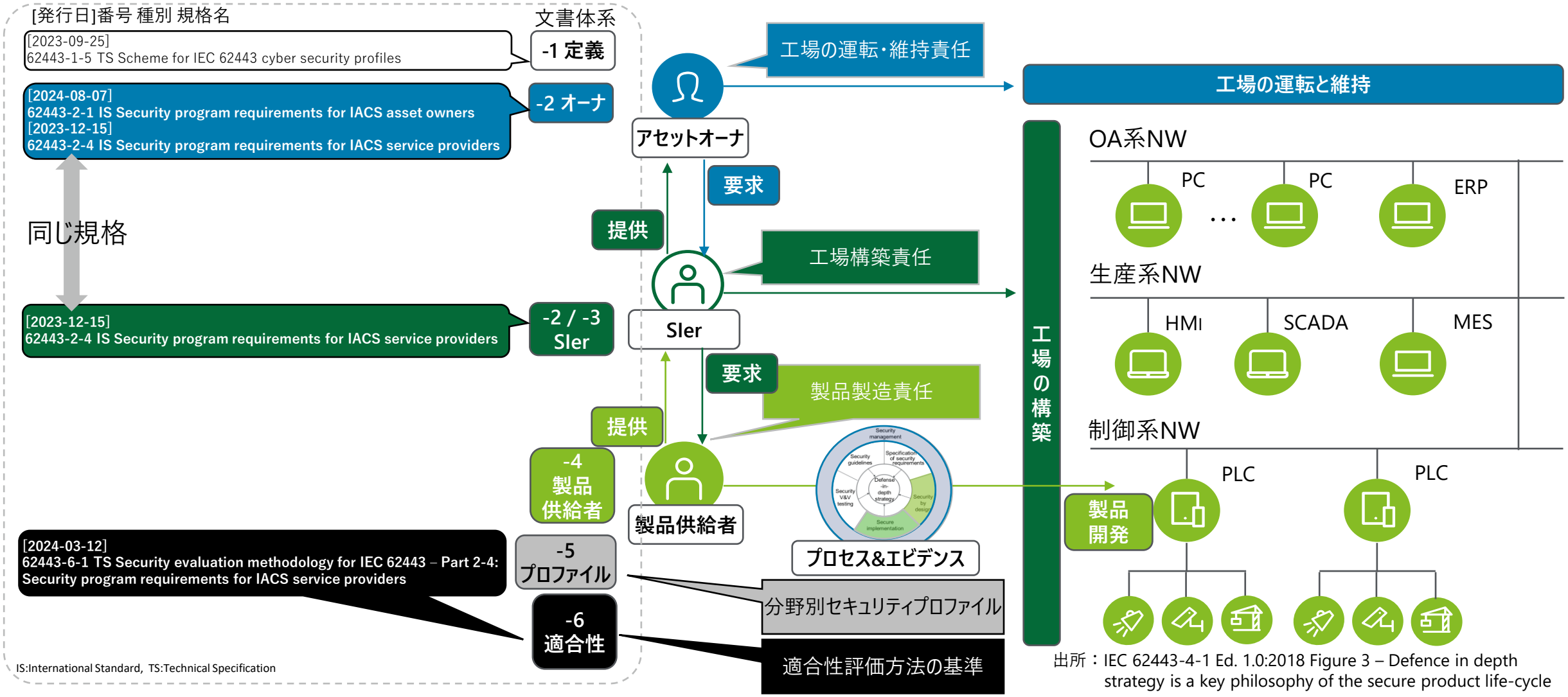
IEC 62443 シリーズの全体像



出所：IEC 62443-4-1 Ed. 1.0:2018 Figure 3 – Defence in depth strategy is a key philosophy of the secure product life-cycle

1年以内で新規発行されたIEC 62443は、1-5、2-1、2-4、6-1の4冊です

1年以内に新規で発行されたIEC 62443一覧



出所：IEC 62443-4-1 Ed. 1.0:2018 Figure 3 – Defence in depth strategy is a key philosophy of the secure product life-cycle

3. IEC 62443-2-1 Edition 2.0の概要

14年ぶりの改訂になった2-1 Ed2.0は主要な標準との整合性を重視し、成熟度を採用しました

IEC 62443-2-1 ED2.0の特徴

IEC 62443-2-1 の概要

- 2024年8月にIEC 62443-2-1 Ed2.0: Security program requirements for IACS asset ownersが発行
- 2010年発行のEd1.0から、約14年ぶりの改訂
- アセットオーナが組織的に実践すべきプロセス要件（Policies and procedures）を規定

Ed1.0からEd2.0の変更点

- Security Program Element(SPE)アセットオーナのセキュリティ対策を分類したもの
  - ✓ 8つのセキュリティ対策の分類と、16つのサブカテゴリで構成されている
- 成熟度モデルとして、シリーズ共通のプロセス成熟度(Maturity Level 1～4)を新規に採用
- IEC 62443シリーズ内やISO27000シリーズなど主要な標準との要求事項のマッピングを新規追加

2-1 Ed2.0 は、8つのSPE(セキュリティ対策の分類)と、16つのサブカテゴリで構成されています

SPEの各章分類の一覧と対策プロセスの例

- SPE (Security Program Element)とは、アセットオーナーのSPを構成するセキュリティ対策の分類
- SPEには、ORG、NET、COMPといったサブカテゴリが定義されており、各サブカテゴリ毎に最大十数個のアセットオーナーにとって推奨セキュリティ対策（組織的・技術的）が規定

SPE		Title	対策プロセスの例
SPE 1	ORG 1	Security related organization and policies	ISMSの構築（ORG 1.1）、セキュリティ役割責任の明確化（ORG 1.3）
	ORG 2	Security assessments and reviews	セキュリティリスク識別と低減（ORG 2.1）、セキュア開発と支援（ORG 2.3）
	ORG 3	Security of physical access	物理アクセス制御（ORG 3.1）
SPE 2	CM1	Inventory management of IACS hardware/software components and network communications	資産一覧表の作成（CM 1.1）、変更管理（CM 1.4）
SPE 3	NET 1	System segmentation	ネットワーク分離（NET 1.1）、ネットワーク切断時の自律性（NET 1.4）
	NET 2	Secure wireless access	セキュアな無線プロトコル（NET 2.1）、攻撃者への情報公開制限（NET 2.3）
	NET 3	Secure remote access	リモートアクセスの保護（NET 3.1）、適切な切断（NET 3.3）
SPE 4	COMP 1	Components and portable media	コンポーネント強靭化（COMP 1.1）、専用メディアの利用（COMP 1.2）
	COMP 2	Malware protection	マルウェアスキャン（COMP 2.1）、マルウェア保護の導入と検証（COMP 2.3）
	COMP 3	Patch management	正当性・完全性検証（COMP 3.1）、未適用時のリスク対処（COMP 3.5）
SPE 5	DATA 1	Protection of data	データの分類（DATA 1.1）強固な暗号アルゴリズムの採用（DATA 1.5）
SPE 6	USER 1	Identification and authentication	ユーザIDの割り当て（USER 1.1）、多要素認証の採用（USER 1. 9 ）
	USER 2	Authorization and access control	アクセス認可（USER 2.1）、職務分離（USER 2.2）
SPE 7	EVENT 1	Event and incident management	セキュリティイベント検知（EVENT 1.1）、脆弱性対応手続き（EVENT 1.9）
SPE 8	AVAIL 1	System availability and intended functionality	継続性管理（AVAIL 1.1）、異常時の縮退処理（AVAIL 1.3）
	AVAIL 2	Backup/restore/archive	バックアップ実行手順（AVAIL 2.1）、メディア選定（AVAIL 2.4）

2-1 Ed2.0 は、IEC 62443-4-1などで採用しているMLを追加しました

Ed2.0の変更点であるプロセス成熟度指標（Maturity Level：ML）の追加

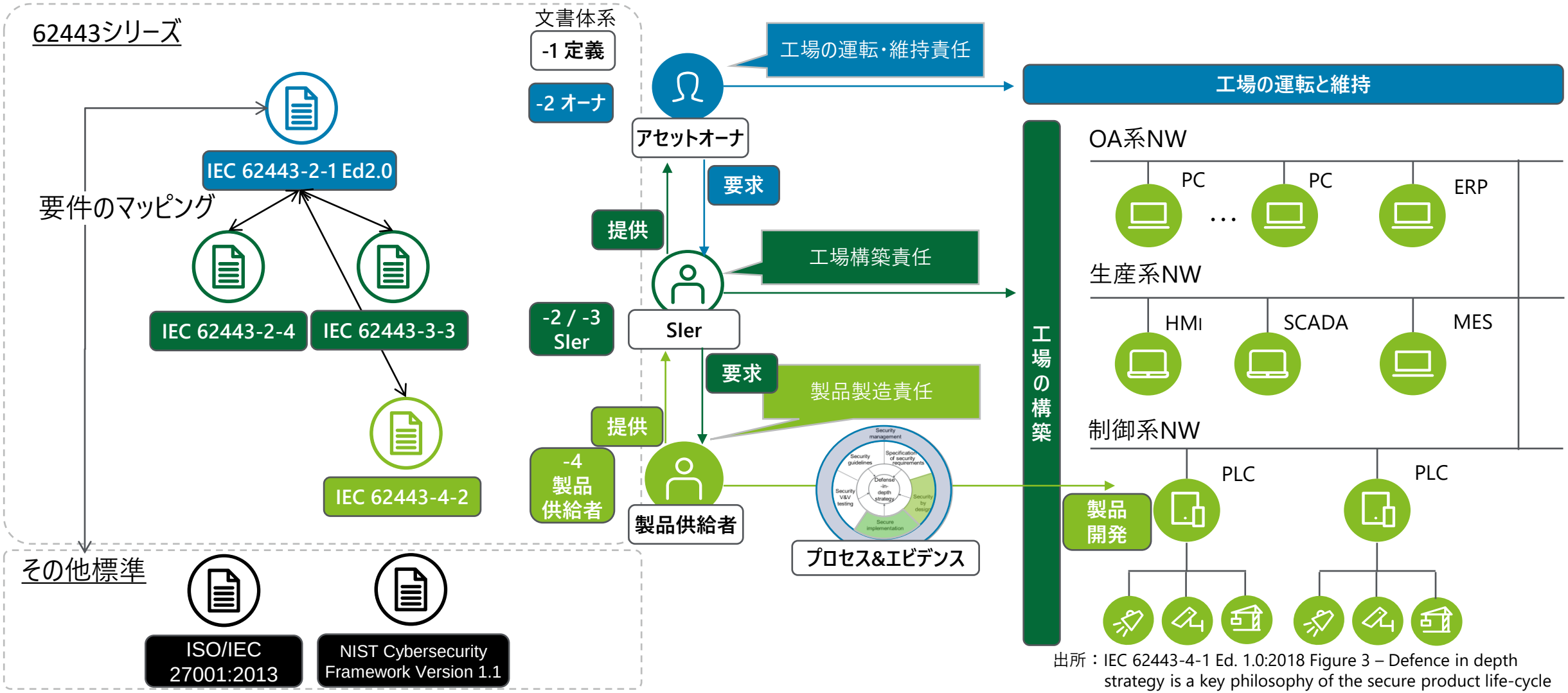
- IEC 62443では、シリーズ共通でCMMIが開発したサービス業務の成熟度モデル(CMMI-SVC)を基礎とする、**Maturity Model (ML)**と呼ばれる4段階の独自プロセス成熟度モデルを規定
- IEC 62443-2-1Ed2.0では、各セキュリティ対策プロセスの成熟度評価指標としてMLを採用し、各プロセス要件の成熟度をMLによって測定することを規定している

プロセス成熟度指標（Maturity Level：ML）の一覧とCMMI-SVCとの関係

Level	CMMI-SVC	IEC 62443の定義	概要
ML 1	Initial	Initial	初期状態のプロセス。完全に文書化されずに実施。
ML 2	Managed	Managed	管理されたプロセス。管理方法の文書が存在するが、詳細の定義は無い。
ML 3	Defined	Defined / Practiced	定義・実践されたプロセス。定義されたプロセスが実践・反復されている。
ML 4	Quantitatively Managed / Optimizing	Improving	改善が続けられているプロセス。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。

2-1 Ed2.0 は、他のIEC 62443分冊や他の標準の関係（各要件・役割）を明確にしました

IEC 62443-2-1 Ed2.0のその他変更点



出所：IEC 62443-4-1 Ed. 1.0:2018 Figure 3 – Defence in depth strategy is a key philosophy of the secure product life-cycle

4. IEC 62443シリーズの今後の動向

今後、シリーズ共通モデル、電力・鉄道などの他分野対応、適合性評価基準の開発、IoTへの適用が検討されています

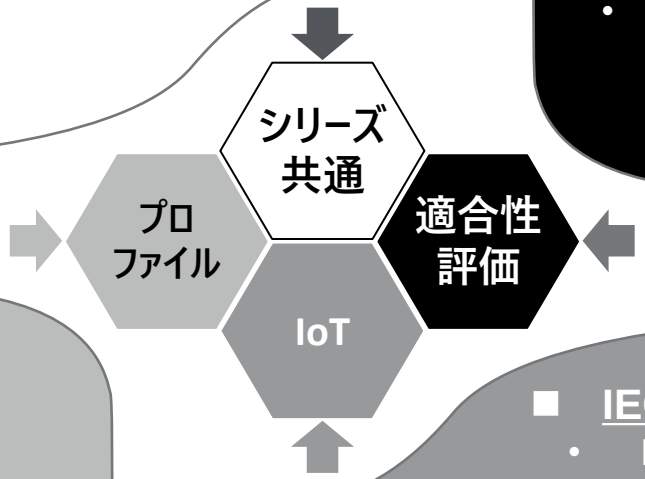
IEC 62443シリーズの今後の動向

■ **IEC 62443 シリーズ共通モデルの開発（IEC 62443-1-1 改訂中）**

- IEC 62443-2-1 Edition 2.0で規定された内容も含めて、シリーズで共通的な概念・モデルの標準開発
- 他のIEC 62443文書も、上記共通概念・モデルをベースに改訂予定
  ⇒2026年目標

■ **適合性評価方法の基準（IEC 62443-6）**

- IEC TS 62443-6-1
  ⇒ IEC 62443-2-4（サービスプロバイダ）に対する適合性評価方法の基準、2024年3月に発行済み
- IEC TS 62443-6-2
  ⇒ IEC 62443-4-2（製品セキュリティ機能）に対する適合性評価方法の基準、2025年に発行予定



■ **分野別セキュリティプロファイルの開発（IEC TS 62443-1-5:2023）**

- ISA99やIECの他TC（専門委員会）において、電力や鉄道等のプロファイル策定の動き

■ **IEC PAS 62443-1-6の開発状況**

- IEC 62443の産業IoTアプリケーションセキュリティへの適用

IECにおける認証の状況と、IEC以外における認証の状況、また日本の認証機関について述べます

IEC 62443適合性評価について

IECの認証状況

- 開発部署
  - IEC/CAB/IECEE/CMC/WG31 Cybersecurity
- 24年に取り組んでいる認証
  - IEC 62443-2-1を認証プログラムに追加
- その他
  - ENISAとの連携、競合について議論（欧州サイバーレジリエンス法との関連）

IEC以外の認証状況

- 開発部署
  - ISA/IEC 62443を開発したISA/S99委員会（ISA-99）
- 24年に取り組んでいる認証
  - Component Security Assurance(CSA)
  - IIoT Component Security Assurance(ICSA)

    IEC 62443-4-1、-4-2ベース
  - Security Development Lifecycle Assurance(SDLA)

    IEC 62443-4-1ベース
  - Automation and Control System Security Assurance (ACSSA)

    IEC 62443-2-1Ed2.0（+2-3, 2-4, 3-2, 3-3）ベース

日本の認証状況

- テストラボ
  - (共同研究組合)制御システムセキュリティセンター(CSSC)
- その他
  - 日本で唯一のIEC 62443テストラボ (ISO 17025取得)
  - ISASecure認証を日本語で取得可能

制御システムに対して攻撃が加速する中、IEC 62443の国際標準化の活動は様々な分野・機器へと活動を広げています

まとめ

- サイバーセキュリティ脅威関連動向と、IEC 62443の概要・開発状況
  - ✓ ランサムウェア攻撃が製造業分野に流行、様々な法規や国際標準が制定されている
  - ✓ これら法規に対して関連しているIEC 62443は新規で1-5、2-1、2-4、6-1の4冊発行されている
- IEC 62443-2-1 Edition 2.0の概要、IEC 62443シリーズの今後の動向
  - ✓ 2-1 Ed2.0 は、他のIEC 62443分冊や他の標準の関係（各要件・役割）を明確にした
  - ✓ IEC 62443シリーズとしては、IoTや認証に関連する適合性評価の適用を検討している

IEC 62443の活動はJEMIMAの国内委員会で、これらのJIS化はJSAの研究会で開催されています

IEC 62443関連の国内委員会 – Japan local committees about IEC 62443

- IEC/TC65/WG10 国内委員会
  - IEC 62443の国際標準化活動
  - メンバー構成
    - 20企業・団体、約40名が国内委員会に参加
    - 6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、デロイト
- 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
  - IEC 62443-2-1 Ed2.0をベースとしたJIS規格化を計画中

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

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

Deloitte.
デロイト トーマツ

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

IS/BCMSそれぞれの認証範囲はこちらをご覧ください
http://www.bsigroup.com/clientDirectory

Member of
Deloitte Touche Tohmatsu Limited