委員会活動報告

計測制御システムのセキュリティ標準IEC 62443の最新動向およびIEC 62443-2-1 Edition 2.0の概要

IEC TC65国内委員会

1．はじめに

IEC TC65/WG10では、産業プロセスの計測制御システムのセキュリティ（Security for industrial process measurement and control - Network and system security）の標準化を推進している。この標準はIACS（Industrial Automation and Control System）に関するセキュリティの概念、各役割における要求事項、要求事項の実践に関するガイドラインからなる規格群である。IACSとは、ソフトウェア・ハードウェアからなる計測制御に関する情報処理システム（Automation Solution）に加えて、そのシステムの運用にかかわる人、業務（Policies and Procedures）も含む概念であり、システム、コンポーネントの技術的セキュリティ対策に加えて、管理・運用といった非技術的セキュリティ対策も含まれる。2009年7月にIEC 62443-1-1 Edition 1.0が発行されてから今日まで15年に渡り開発、改定が続く標準である。これまでに発行されたJEMIMA会報にてIEC 62443の開発状況を紹介してきたが、本稿では、現時点でのIEC 62443規格群の開発状況、および2024年8月7日にIS（国際規格）発行となったIEC 62443-2-1 Edition 2.0の主な改定内容、そして今後の展望を解説する。

2．IEC 62443の概要と開発状況

IEC 62443は2024年8月時点で18分冊が提案、開発、または発行されている。規格の内容はISA（International Society of Automation）内の規格開発グループであるWorkgroup 99（ISA99）と共同で開発されており、それぞれで共通する分冊コード（62443-x-y）として、IEC、ISA各団体から各分冊が発行される。各分冊の概要と発行状況の一覧を表1に示す。

表１　IEC 62443 シリーズの概要と開発状況

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	（同上）	（同上）	-	WD	未定
	62443-1-2	-	-	Reserved	欠番	-	-	
	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	-	WD	未定
	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で開発中	未定
	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	2023-09-15	発行済	
	62443-1-6	1.0	PAS	Application of the IEC 62443 standards to the Industrial IoT	IEC 62443の産業IoTへの適用	-	WD	未定
Policies and Procedures	62443-2-1	1.0	IS	Establishing an industrial automation and control system security program	サイバーセキュリティマネジメントシステム(CSMS)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	2024-08-07	発行済	
	62443-2-2	1.0	PAS	IACS Security Protection	IACSセキュリティプロテクション(技術要件・プロセス要件の決定スキーム)	-	DPAS	2024年
	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		WD	2024年
	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	（同上）	（同上）	2023-12-15	発行済	
		3.0	IS	（未定）	（未定）	-	Joint Teamにて改定に着手	未定
	62443-2-5	1.0	TR	Implementation guidance for IACS asset owners	IACSアセットオーナー向け実装ガイド	-	ISA99で提案有	未定
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	Use of security technologies in the IACS environment	IACS環境におけるセキュリティ技術の使用	-	ISA99で開発中	未定
	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	
		2.0	IS	（同上）	（同上）		Joint Teamにて改定に着手	2025年
	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	
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	
Profiles	62443-5-X	-	TR	（未定）	（分野向けのProfileが追加される見込み）	-	ISA99で電力分野向けProfileを開発中	未定
Conformity	62443-6-1	1.0	TS	Security evaluation methodology for IEC 62443-2-4	IEC 62443-2-4のためのセキュリティ評価手法	2024-03-12	発行済	
	62443-6-2	1.0	TS	Security evaluation methodology for IEC 62443-4-2	IEC 62443-4-2のためのセキュリティ評価手法	-	CD	2025年

（文書タイプ・進捗ステータス略号の説明）
IS：国際規格、TS：技術仕様書、TR：技術報告書、PAS：公開仕様書
WD：作業原案、CD：委員会原案、DPAS:公開仕様書原案、FDIS:最終国際規格案

IEC 62443では、図1に示すシリーズで共通するIACSにおける役割と責任（Roles and responsibilities）のモデルが定義されており、当モデルに基づき各役割において遵守すべきセキュリティ対策要件が規定されている。すなわち、各分冊のスコープも当モデルをベースとしており、例えば、アセットオーナー（Asset owner）はIEC 62443-2-1を参照してIACSセキュリティの全体方針を立て、各サービスプロバイダ（Maintenance service provider、Integration service provider）はIEC 62443-2-4、IEC 62443-3-3を参照してシステム開発、保守時のセキュリティを確保する。アセットオーナーのIACSから独立した環境にあるIACSコンポーネントプロバイダは、IEC 62443-4-1、IEC 62443-4-2を参照してセキュアなコンポーネントを開発、保守するといった形である。

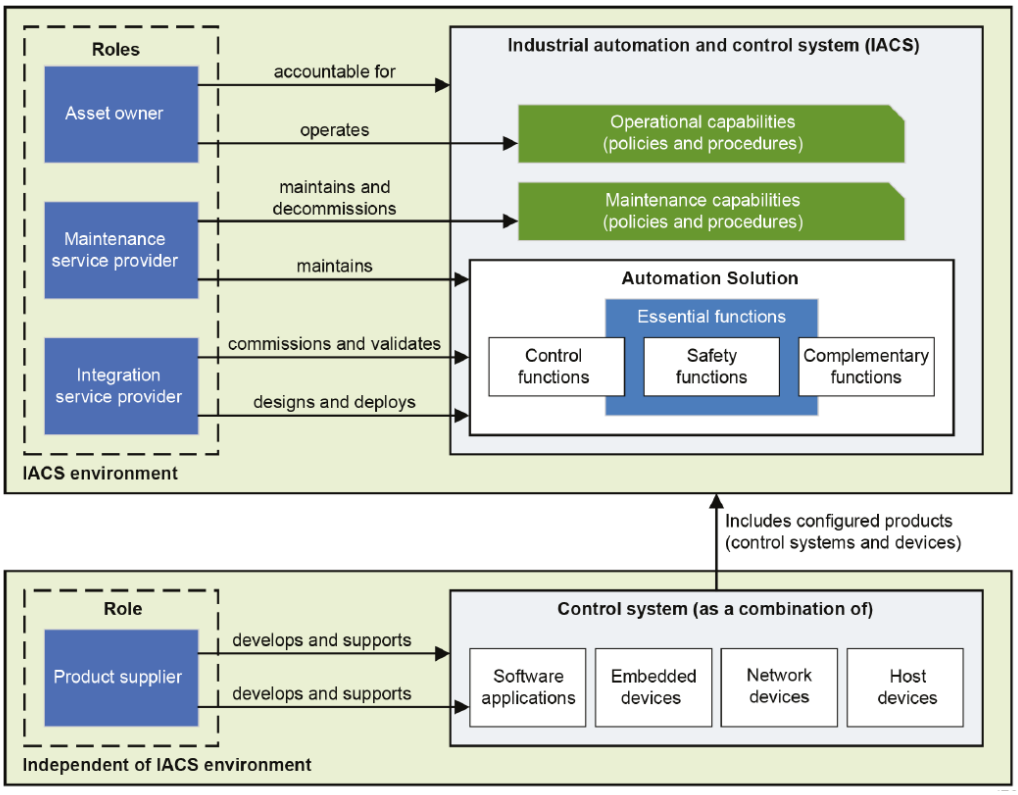

図１　IEC 62443 における役割責任モデル（引用元：IEC TC65/WG10）

IEC 62443は、IEC TC65/WG10、ISA99のいずれかのワーキンググループ（WG）で個々に開発したドラフトを双方で審議、承認し、発行する形式で進めていたが、分冊毎のIEC TC65/WG10、ISA 99共同のJoint Team （JT-62443-x-y）が2023年から立ち上がり始め、一部の分冊はJoint Teamを通じてドラフト開発段階から共同開発する体制に移行している。このJoint Teamは、IEC TC65/WG10のコンビナとISA99の議長間の合意により立ち上がった取り組みであり、当面の間は各WG共通のメーリングリストの運用、WG間の会議オープン化、会議資料のWG間での共有といった取り組みが進められている。Joint Teamの現状の会議体は、62443-1-5、2-4、6-1、6-2の開発はIEC TC65/WG10が主体、それ以外の分冊の開発はISA99が主体で進められているが、将来的には、共通化する方向で検討されている。

３．IEC 62443-2-1 Edition 2.0の概要

IEC 62443-2-1 Edition 2.0は、アセットオーナーに対するセキュリティプログラム（Security program: SP）の要求事項を規定する標準であり、アセットオーナーが組織的に実践すべきプロセス要件（Policies and procedures）を規定する。2010年に発行されたEdition 1.0では、CSMS（Cyber Security Management System）と呼ばれ、IACSにおけるセキュリティマネジメントシステムの要求事項を規定するものであったが、Edition 2.0では、ISMS（Information Security Management System）を実践するアセットオーナーも存在する現状も鑑み、ISMSと共存することを前提とした構成に変更された。その結果、Edition 2.0では、

CSMSという用語を廃止し、ISMSまたは他の適切なセキュリティマネジメントプロセスの構築をSPの一要素とし、その実施を要件化している。特にIEC 62443-2-1 Edition 2.0では、アセットオーナーが安全に生産活動を行うためのセキュリティ対策活動という位置付けを明確化しており、広範囲な情報セキュリティ確保のための活動としてのISMSだけではカバーできない、IACSに特化した要求事項を定義することで、ISMSとの差別化を図っている。例えば、安全システムとのネットワーク分離や、セキュリティインシデントに起因するシステム異常時に安定なシステム状態に復元する手順などが要件化されている。

SPの構成を表2に示す。SPはSPE（Security Program Element）と呼ばれる8つの大分類に基づき、個々のプロセス要件を規定する。

表２　SPE の一覧と概要

SPE ID	Title	略号コード	概要
SPE 1	Organizational security measures	ORG	組織のセキュリティ対策
SPE 2	Configuration management	CM	構成管理
SPE 3	Network and communications security	NET	ネットワークと通信のセキュリティ
SPE 4	Component security	COMP	コンポーネントセキュリティ
SPE 5	Protection of data	DATA	データの保護
SPE 6	User access control	USER	ユーザアクセス制御
SPE 7	Event and incident management	EVENT	イベントとインシデントの管理
SPE 8	System integrity and availability	AVAIL	システムの完全性と可用性

各SPEは個々のプロセス要件をまとめる小分類を規定している。その小分類と、各小分類が規定する対策例を表3に示す。IEC 62443-2-1 Edition 2.0に準拠するSPは、これら対策プロセスに対応したポリシーと手順書の整備、それらの実践を要求している。

表３　SPE の各章分類の一覧と対策プロセスの例

SPE ID	Code	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）、サプライチェーンセキュリティ（ORG 1.6）など
	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）など
	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	ベースとなる資産一覧表の作成（CM 1.1）、変更管理（CM 1.4）など
SPE 3	NET 1	System segmentation	非IACSとのネットワーク分離（NET 1.1）、ネットワーク切断時の自律性（NET 1.4）など
	NET 2	Secure wireless access	セキュアな無線プロトコルの利用（NET 2.1）、無線ネットワークの情報公開制限（NET 2.3）など
	NET 3	Secure remote access	リモートアクセスアプリケーションの保護（NET 3.1）、リモートアクセスの適切な切断（NET 3.3）など
SPE 4	COMP 1	Components and portable media	コンポーネントの強靭化（COMP 1.1）、専用ポータブルメディアの利用（COMP 1.2）
	COMP 2	Malware protection	マルウェアスキャン（COMP 2.1）、マルウェア保護ソフトウェアの導入と検証（COMP 2.3）など
	COMP 3	Patch management	セキュリティパッチの正当性・完全性検証（COMP 3.1）、セキュリティパッチ未適用時のリスク対処（COMP 3.5）など
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）など
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 1.2）など
	USER 2	Authorization and access control	アクセス認可（USER 2.1）、職務分離（USER 2.2）など
SPE 7	EVENT 1	Event and incident management	セキュリティイベント検知（EVENT 1.1）、ログアクセス管理（EVENT 1.6）、脆弱性対応手続き（EVENT 1.9）など
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）など
	AVAIL 2	Backup/restore/archive	バックアップ実行手順（AVAIL 2.1）、適切なバックアップメディアの選定（AVAIL 2.4）など

IEC 62443-2-1 Edition 2.0は、2-4や4-1等の他のIEC 62443シリーズ分冊で既に採用済みであるMaturity level（ML)と呼ばれるプロセス成熟度モデルを新たに採用している。MLはCMMI Instituteが管理するCMMI®-SVC（Capability Maturity Model Integration - Service）を基に開発されたモデルであり、表4に示す対応関係でプロセス成熟度のモデルを規定している。

表４　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における定義	概要
ML 1	Initial	Initial	初期状態のプロセス。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。
ML 2	Managed	Managed	管理されたプロセス。プロセスの管理方法を説明する文書が存在するが、プロセス詳細の定義は無く、プロセスを円滑に実践できない場合がある。
ML 3	Defined	Defined / Practiced	定義・実践されたプロセス。ML 2で定義されたプロセスが実践され、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。

IEC 62443-2-1 Edition 2.0は、前述の役割責任モデルを基に他分冊との重複を排除し、アセットオーナー以外の役割が責任を持って実施すべき事項との差別化を図っている。また、アセットオーナーの責任で実施すべきセキュリティ対策事項であっても、その実装はサービスプロバイダやコンポーネントプロバイダで担う場合もある。そのような要件については、IEC 62443-2-1 Edition 2.0の各要件のクロスリファレンスがAnnex Aに提供されており、各要求事項の実装において参照することができる。クロスリファレンスの例としては、同じIEC 62443シリーズのIEC 62443-2-4:2023、IEC 62443-3-3:2013、IEC 62443-4-2:2019に加えて、ISMSの要求事項を規定するISO/IEC 27001:2013、組織全体のセキュリティ対策のフレームワークであるNIST Cybersecurity Framework Version 1.1の各要求事項とのマッピングも含まれている。

以上で説明した通り、IEC 62443-2-1 Edition 2.0では、Edition 1.0と比較してIACSセキュリティ対策の現状の反映とIEC 62443シリーズ全体の位置づけを明確にしたうえで、アセットオーナーが遵守すべき要求事項の最適化が図られている。

４．IEC 62443シリーズの今後の動向

現在、IEC 62443シリーズ共通モデルを規定するIEC 62443-1-1の改定が進められており、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、モデルの標準開発が進んでいる。それに合わせて、IEC 62443-2-4、IEC 62443-3-3などの発行済みの分冊についても、シリーズ共通の概念、モデルに合わせて改定される計画であり、各分冊の内容はシリーズ全体で最適化されていく予定である。

また、2023年9月にIEC 62443の分野別セキュリティプロファイルを開発するためのスキーム（IEC TS 62443-1-5:2023）も発行された。更にISA99やIECの他TC（専門委員会）において、電力や鉄道を始めとする各ドメイン共通のIEC 62443プロファイルを策定する動きもある。関連して、TC65配下に設立されたJAG 26（Joint Advisory Group 26）において、IEC 62443シリーズを、TC 65が対象とするプロセス産業の枠を超えた、様々なOT（Operational Technology）を含めた様々な産業分野から参照できるように水平規格化（Horizontal Standard）する動きがある。現時点ではIECではOTという用語の定義が定まっておらず、審議されている状況である。

IEC 62443の各分冊が規定する要求事項の適合性評価の方法論に関する標準（IEC 62443-6シリーズ）において、2024年3月にIEC 62443-2-4に対する適合性評価方法の基準であるIEC TS 62443-6-1:2024（TS：Technical Specification技術仕様書）が発行された。更にIEC 62443-4-2を対象としたIEC TS 62443-6-2も、現時点での計画では、2025年に発行予定である。また、IEC 62443の産業IoTアプリケーションセキュリティに関して、IEC TR 62443-1-6（TR：Technical Report技術報告書）として開発を進めていたものが、IEC PAS 62443-1-6（PAS：Publicly Available Specification公開仕様書）として開発を進める提案がされていたが、2024年7月に、その提案が承認された状況である。

セキュリティ対策の状況を定量化、可視化する動きとして、アセットオーナーのSP達成状況を可視化するKPI（Key Performance Indicator）モデルの標準（IEC TR 62443-1-3）、およびサイバー攻撃に対する防御能力に関する指標（Security Protection）の標準（IEC PAS 62443-2-2）が提案されている。Security Protectionは、技術的セキュリティ対策の指標であるSecurity Level（SL）と、上述のプロセス成熟度の指標であるMLとを合わせた、セキュリティ保護レベル（Security Protection Level）と呼ばれるサイバー攻撃に対する防御能力に関する指標と、セキュリティ保護レベルを決定するスキーム（Security Protection

Scheme）であり、IEC PAS 62443-2-2では、これら概念の詳細仕様が文書化される予定である。

５．まとめ

サイバーセキュリティの脅威が日々深刻化していく中、IACSのセキュリティ確保は今後も一層重要となり、多くのアセットオーナーにおいて経営課題の一つとして認識されつつある。上述の通り、各分冊で固有の概念、モデルを前提に開発を進められていたものを、シリーズ共通の概念、モデルに合わせて再構築する動きがあり、ユーザが使いやすい形にアップデートされている状況である。また、産業IoTやKPI、セキュリティ保護といった、新しいトピックの標準についても議論中である。

IEC TC 65内外においてもIEC 62443に基づき個々のドメイン、ユースケースに応じたセキュリティ標準を開発する動きもあり、IEC 62443は、産業分野のサイバーセキュリティ標準として、より重要な位置づけになる可能性がある。今後もIEC TC65/WG10国内委員会では、IEC 62443に関連する規格開発の動向を発信していきたい。

執筆
IEC TC65/WG10 国際エキスパート
藤田　淳也（株式会社日立製作所・研究開発グループ）