標準から学ぶ ICS セキュリティ #1

# ICS セキュリティ標準 IEC 62443 シリーズの全体概要


2022 年 8 月 4 日

一般社団法人 JPCERT コーディネーションセンター

制御システムセキュリティ対策グループ

## 1. はじめに

IEC 62443 は、十数分冊からなる制御システム（ICS）のセキュリティに関するシリーズ標準です。国際標準の中でも 10 冊以上の分冊を擁する規模のシリーズ標準は珍しい存在と言えると思いますが、さまざまな観点からのセキュリティ対策が包括的にまとまっていますので、ICS セキュリティを学ぶための良い手引きにもなっています。その一方で、現場を担当している方々から、標準の存在は知っているけれど、膨大な文書量に躊躇してしまって活用するに至っていないとの声も漏れ聞きます。JPCERT/CC では、この貴重な情報源を現場の方々に少しでも役立てていただくために、IEC 62443 シリーズの中に書かれている主なセキュリティ概念を順次取り上げて紹介する、気軽に読んでいただける連載記事を企画いたしました。その初めにあたり、今回は IEC 62443 シリーズ標準の全体概要について述べます。このシリーズ標準に親しんでいただき、概要を理解するとともに、必要に応じて的確に原典を入手して活用していただける一助になれば幸いです。

なお、IEC 62443 シリーズ標準では ICS の替わりに IACS （産業用オートメーションと制御システム Industrial Automation and Control Systems）の略号と用語が使われていますが、本稿では ICS の略号で表現することといたします。

## 2. IEC 62443 の開発の経緯

このシリーズ標準は米国の民間標準化組織 ISA[1] 傘下の ISA99 委員会によって 2002 年に開発が始まりました。ISA は 1945 年に「Instrument Society of America（米国計器協会）」として発足しましたが、2008 年に組織名称を「International Society of Automation（国際自動化協会）」に改めて今日に至っています。組織名の変更と同時に、発足時から使ってきた歴史的なロゴも現代風の簡素なものに刷新されました。ISA99 委員会が策定した ICS セキュリティに関するシリーズ標準は、最初は ISA 99-1-1 などと委員会名を冠して採番され、米国の国内標準 ANSI （米国国家標準局；American National Standards Institute）標準として位置づけられていました。


［図 1. ISA の新旧のロゴ］

その後、このシリーズ標準を開発する計画が米国から国際標準化機関の IEC （国際電気標準会議；International Electrotechnical Commission）[2] に提案されて、IEC 62443 の番号を冠したシリーズ標準を策定する活動が始まりました。これまでのところは、標準を策定する検討作業を ISA99 委員会と IEC の対応する作業部会とが合同で一体的に進めていますので、両標準の内容はまったく同じです。ただ、標準の発行にはそれぞれの組織で決められた承認手順を経る必要があり、そのためにタイミングが微妙にずれて前後している場合があります。なお、IEC は電気工学と電子工学およびそれに関連した技術を扱う国際的な標

準化団体で、89 の国が会員となっており、ロンドンに本拠を置いています。また、IEC が発行する標準文書の番号は 60000～79999 の範囲から採番し、ISO が発行するものとの重複を避けています。

国際標準として IEC 62443 シリーズの発行が始まると、この番号が広く認知されるようになったために、2010 年に ISA99 委員会が標準番号を変更し、ISA 62443-1-1 などのように IEC と同じ番号を用いることになりました。こうした経緯から、双方の標準化団体の名称を冠して、この標準を「ISA/IEC 62443」と呼ぶことも便宜的にしばしば行われています。

IEC 62443 シリーズとなるシリーズ標準の開発が始まった 2002 年頃は、まだ ICS のサイバー脅威に関する認識が広く共有されているとは言い難い状況にありました。実際に日本国内では現在の経済産業省の資金を受けて大規模プラントに対するサイバー攻撃の可能性を調査する数年がかりのプロジェクトが実施されましたが、サイバー攻撃の可能性を指摘し、オープン技術の採用が拡大しつつある ICS を考えてさまざまな対策の必要性を指摘しつつも、差し迫ったサイバー攻撃による大事故の可能性には否定的な報告書が 2000 年 3 月に公表されています[3]。このような環境下での標準の策定作業は当初なかなか進みませんでした。

ところが、その後 ICS 技術に大きな変化が生じました。変化の一つは、ICS が Windows などの汎用 OS やインターネット・プロトコルなどの汎用通信プロトコルを利用して実現されるようになったことです。また、以前の ICS は他のシステムから完全に切り離して構築され運用されていましたが、一層の経営の効率化を実現するために、ERP などの IT システムと連携しデータをやり取りしながら運用される ICS が主流になったことがもう一つの変化でした。こうした変化に伴って ICS がマルウェアに感染する事例が散見され始めました。また、2010 年にイランのウラン濃縮プラントの ICS を攻撃して多数の遠心分離機を損壊させた Stuxnet と呼ばれるマルウェアが発見されたことが ICS を提供する業界と ICS を利用している組織に衝撃を与え、ICS のセキュリティ・リスクに関する課題認識が一挙に高まり、IEC 62443 シリーズ標準の開発に拍車がかかるようになりました。

一方で、社会の重要インフラについて、サイバー攻撃に対する耐性を高めることが重要な政策課題となり始めました。例えば、EU で 2016 年に採択されたネットワーク指令（NIS； Network and Information Security directive）[4] がその一例です。そうした動きの中で ICS のセキュリティ対策を多面的な観点から論じた唯一の国際標準として IEC 62443 が参照され注目が高まるようになりました。

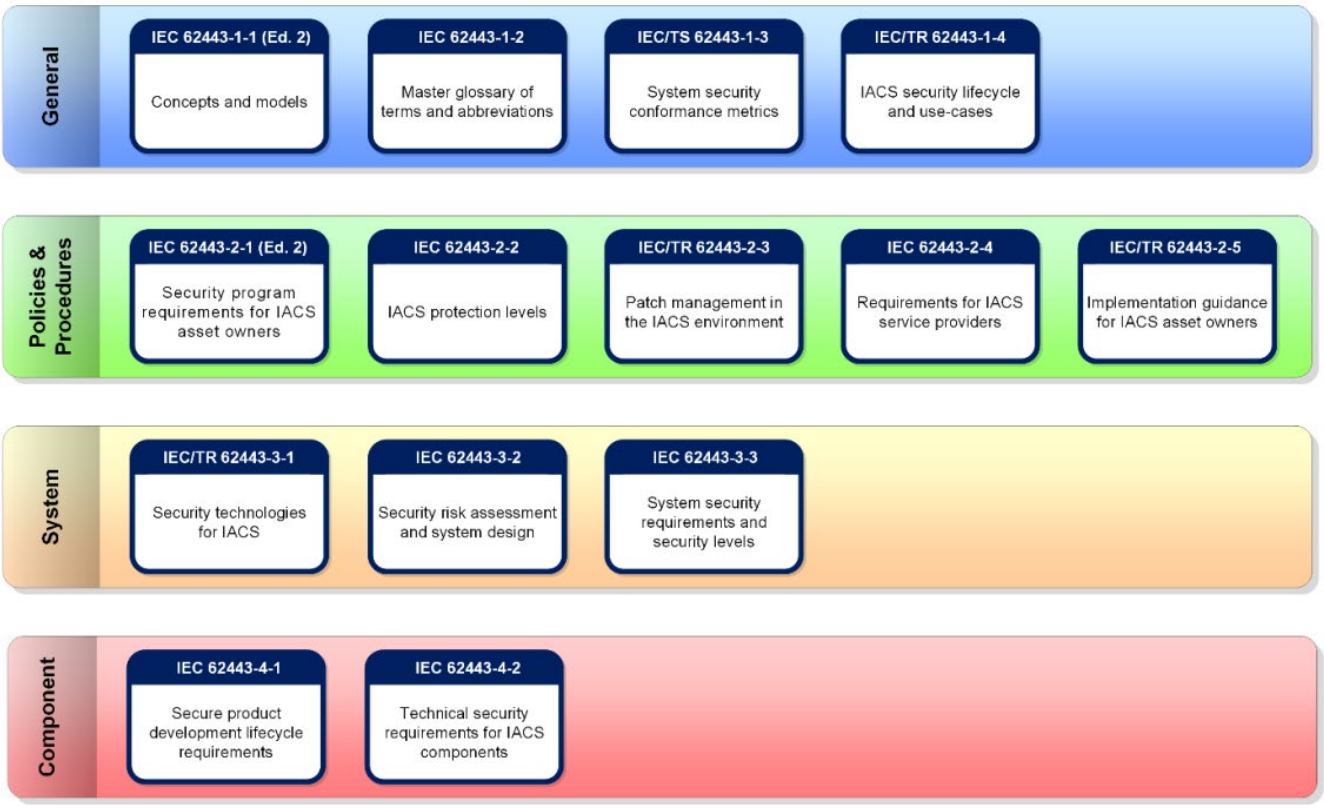
IEC 62443 は製造プラントなど産業分野で自動制御や監視に利用される ICS におけるセキュリティ対策を論じた標準として開発されてきましたが、隣接した分野における制御システムにおいてもサイバー攻撃を受けるリスクが高まり対策が求められるようになりました。医療施設で患者の体調の監視や治療に用いられている医療用機器や医療用ネットワークがその一例です。このような隣接する分野におけるセキュリティ対策においても、IEC 62443 が参照されるケースが見られるようになり、こうした期待に応えて IEC においても IEC 62443 を産業用分野以外の制御システムにも対象範囲を拡大する「水平標準化」（horizontality）[5] と呼ばれる構想が浮上し、その是非を調査して方針を提案するために、IEC 内の OT セキュリティに関連するすべての技術委員会等から代表者を集めた作業部会の設置が決まって今日に至っています。

IEC 62443 シリーズ標準が策定された経緯を紹介してきましたが、実は一つだけ他の分冊とは出自が異なるものが含まれています。IEC 62443-2-4 （ICS サービス提供事業者に対する要件）がそれです。この分冊の原案は、欧州の石油会社などを中核メンバーとして擁する、通称 WIB （Working-party on Instrument Behaviour）と呼ばれるプロセス・オートメーション利用者協会[6] によりインテグレーション・サービス事業者に対するセキュリティ要件としてまとめられた標準が IEC に提案され、それをもとに ISA 99 委員会と IEC による審議を経て国際標準として発行するに至っています。

## 3. IEC 62443 シリーズ標準の全体像

本稿の執筆時点（2022 年 7 月）で公式に IEC 62443 シリーズ標準に含まれるとされているのは［図 2］に掲げた 14 分冊（パート； part）です。これらのうち、9 分冊がすでに発行されており、5 分冊は現在も初版を策定中です。また、すでに発行されているものも発行から時を経て、その間に ICS を構成している技術や ICS に期待される機能、期待されるセキュリティ対策水準などが変化してきていることを受けて、改訂作業が始まっているものが複数あり、シリーズ標準全体としては開発中あるいは進化中と言うべき状況にあります。

分冊は［図 2］に描かれているように、表 1 に示した 4 つの領域に応じたグループに分類されており、それに対応して「分冊 m-n」（IEC 62443-m-n）といったように 2 階層の分冊番号が各分冊に付与されています（m が領域番号）。




［図 2. IEC 62443 シリーズ標準の分冊構成］

［表 1.　現状の IEC 62443 がカバーしている領域］

| 領域番号 | 領域名称 | 備考 |
|---|---|---|
| 1 | 全般的共通事項 | 用語の定義などシリーズ標準の全体に関わる共通事項に関する標準が含まれます |
| 2 | ポリシーと手順 | ICS の導入や運用におけるセキュリティ管理のためのポリシーや手順に関する標準が含まれます |
| 3 | システム | ICS の「システム」としてのセキュリティ水準の設計に関する標準が含まれます |
| 4 | コンポーネント | ICS のコンポーネント製品のセキュリティ保証水準に関する標準と製品開発プロセスに対する要件に関する標準が含まれます |

事務用の情報システムの場合には、利用業界が違っていても、システムの構成や提供される機能の相違が比較的少ないと言えますが、これに対して ICS は、業種や ICS が制御する施設によって、その構成や機能が大きく異なっています。例えば、化学プラントや製油所のような連続プロセスを管理制御するプロセス・オートメーション（PA）と、自動車や電気機械などの組立製造を管理制御するファクトリー・オートメーション（FA）と

では、ICS の構成や運用が大きく異なっています。こうした事情は、業種が違っても似た構成と機能を備えているオフィス業務用の IT システムとは対照的と言えましょう。しかしながら、IEC 62443 では一般的な ICS を想定して、そのセキュリティを担保するための方法論や手順を論じています。それに対して、特定の業種や応用領域においてセキュリティを担保するための標準が欲しいとのニーズが存在し、通常であれば独立した標準を開発することになるところですが、IEC 62443 の策定検討の中では、必要な要件を選び出して「プロファイル」として定義することにより、このニーズに応えることを模索しています。こうしたニーズは、IEC 62443 が産業用以外の分野の制御システムも対象とする水平標準化が進めば、一層強まるものと予想されます。これに備えて、5 番目の領域として「プロファイリング」に関する一連の標準を策定する構想が進み始めているようです。

また、IEC 62443 シリーズ標準に対応した準拠性の検証や認定についても、これまでは ISA 傘下の組織 ISASecure が認証事業として先行して取り組んできていますが、欧州において NIS 指令が改定強化されるなど公的な準拠性の検証認定制度へのニーズが高まる動向を見据えて、6 番目の領域として「準拠性」を設けて標準化する検討が始まっています。

## 4. IEC 62443 シリーズ標準の想定読者

IEC 62443 シリーズ標準のもっとも中心的な想定読者は ICS 利用者です。ICS は、ICS によって監視制御されている装置や施設の付帯物と見なされることが多いので、ICS 利用者は、装置や施設などの資産（アセット）を保有し日々の管理を担当している人という意味で「アセットオーナー」と一般に呼ばれます。情報セキュリティ管理に関する標準 ISO/IEC 27000 シリーズでは、セキュリティ脅威や脆弱性の管理を担当するリスク・オーナーをアセットオーナーとは別の担当者と考え、両者を区別していますが、IEC 62443 の枠組みでは、ICS の運用に関わるセキュリティ管理をアセットオーナーの仕事に含めています。

ICS を簡単な設定だけで稼働させることは稀であり、監視制御対象の装置や施設に対応したさまざまな作り込みや最適化を施した上で設置される ICS が大多数ですので、セキュアな ICS を実現する上で ICS のインテグレーションを担当する事業者も大きな役割を担っています。大規模な施設を監視制御対象とする ICS の場合には、そのシステム設計や設置が EPC（Engineering, Procurement and Construction）事業者の下で進められるケースが多く、EPC 事業者にとって必要なセキュリティ対策を適切に組み込んだ ICS を構築してアセットオーナーに引き渡すことが大きな課題となっています。

ICS が監視制御する施設の中には数十年間にわたる稼働が想定されているものも多く、その安定的な運用のためには定期的および随時の保守作業が不可欠です。ICS 自体の保守についてはもちろんですが、ICS 以外の装置や施設の保守においても、保守用の電子機器を ICS ネットワーク環境に接続して利用する場面が想定されます。そうした際に、持ち込んだ機器が感染していてマルウェアを ICS 内に持ち込んだり、攻撃者が ICS に侵入するための入口となるバックドアを気付かないまま作り込むなどのリスクがありますので、保守サービス事業者も ICS のセキュリティ対策における重要なプレーヤーであると言えます。

ICS を構築するにあたっては、PLC（Programmable Logic Controller）と呼ばれる ICS 固有の機器が用いられることが多く、また近年は、センサーやアクチュエーター等にも CPU を搭載してさまざまな機能を実現した「スマート化」が進んでいます。こうした機器の多くは、いわゆる ICS ベンダーあるいは装置ベンダーから提供される組込み機器です。さらに、IIoT（Industrial Internet of Things）と称してアセットオーナーが自製ないし特注した機器が ICS 内に組み込まれるケースも増えています。こうした機器も、汎用のネットワーク機能を搭載し、汎用 OS を組み込んでいるため、サイバー攻撃を受ける可能性が少なからずあります。しかしながら、その可能性が広く認識されるようになったのは Stuxnet が見つかった 2010 年以降になってからで、それ以前はサイバー攻撃を受ける可能性をほとんど考慮しないまま機器の設計開発製造が行われていました。こうした時代背景の中で策定された IEC 62443 では、ICS を構成するコンポーネントとなる PLC その他のコントローラー製品などのセキュリティを強化するために，「コンポーネント」と呼ばれる領域（領域番号 4）に分類される標準を設け、製品の開発時に留意されるべき要件を定義しています。これらの標準は、ICS 環境に依存することなく書かれていて、また、これほど体系的に論じた適切な文書が他にないために、例えば医療用の機器のセキュリティ規制において参照されるなど、ICS 以外の分野まで利用が拡大しています。

ICS には以上に述べたような多様なプレーヤーが関与しています。シリーズ標準であるとは言え、こうした多様なプレーヤーを念頭にした要件をまとめた一つの標準は先例がないように思います。［表 2］に IEC 62443 の各分冊の主要な想定読者を示しおきます。

［表 2.　IEC 62443 の各分冊と主な想定読者］

| 想定読者 | | | 分冊番号 | 分冊の文書名 |
|---|---|---|---|---|
| ✓ | ✓ | ✓ | 62443-1-1 | 用語と概念とモデル |
| ✓ | ✓ | ✓ | （62443-1-2） | 用語と略号のマスター辞書 |
| ✓ | ✓ | ✓ | （62443-1-3） | システム・セキュリティ準拠性の指標 |
| ✓ | ✓ | ✓ | （62443-1-4） | ICS セキュリティ・ライフサイクルとユースケース |
| ✓ | | | 62443-2-1 | ICS のセキュリティ対策の確立 |
| ✓ | ✓ | | （62443-2-2） | セキュリティ保護の格付 |
| ✓ | ✓ | ✓ | 62443-2-3 | ICS 環境におけるパッチ管理 |
| | ✓ | | 62443-2-4 | ICS サービス提供事業者に対する要件 |
| ✓ | | | （62443-2-5） | ICS アセットオーナーのための実現ガイダンス |
| ✓ | ✓ | ✓ | 62443-3-1 | ICS のためのセキュリティ技法 |
| ✓ | ✓ | | 62443-3-2 | セキュリティ・リスク評価とシステム設計 |
| ✓ | ✓ | | 62443-3-3 | システム・セキュリティ要求とセキュリティ水準 |
| | ✓ | ✓ | 62443-4-1 | セキュリティの製品開発ライフサイクル要件 |
| | ✓ | ✓ | 62443-4-2 | ICS コンポーネントに対する技術的セキュリティ要件 |

| | | |
|---|---|---|
| | | ICS のコンポーネント製品提供事業者 |
| | ICS インテグレーターおよびシステム製品提供事業者 | |
| アセットオーナーおよび彼らを支援する保守サービス事業者 | | |

注）分冊番号が括弧書きされた文書は 2020 年 7 月時点で未発行.

## 5. IEC 62443 シリーズ標準の課題と今後

2 階層の分冊番号が付与された、相互に関連しあった十以上の分冊を含むシリーズ標準は、これまでに類例がなかったかと思います。これだけの規模の標準文書の策定には長い時間がかかり、また、多くの人々が関わってきました。初期に発行されたものの中には、IEC 62443-1-1:2009 （用語と概念とモデル）や IEC 62443-2-1:2010 （ICS のセキュリティ・プログラムの確立）のように 2010 年以前の発行で、すでに策定から 10 年以上が経過しているものがあります。他にも複数の分冊の改訂作業が進められていますが、この十年間余りの ICS 自体および ICS に関するセキュリティ状況の変化を考えるにつけ、新たな対策技術や脅威動向を織り込んだ改訂版の発行が待たれるところです。

また、多面的で相互に関連しあった各分冊の中で使われている基本的な用語と、各分冊が定めている要件の整合性も、課題として認識されており、策定作業グループの中に特別なチームを設置して問題の洗い出しを進めるとともに、相互参照付の用語辞書の整備を含む、今後の IEC 62443 全体の策定計画をロードマップとしてまとめるための作業に取り組んでいるようです。

産業用 IoT いわゆる IIoT （Industrial Internet of Things）の導入が進んでいますが、それに伴うセキュリティ・リスクの変化が懸念されています。この問題も IEC 62443 にとって放置したままにしてはおけない課題と言えるでしょう。

## 6. まとめ

「標準から学ぶ ICS セキュリティ」と題した連載の初回として、IEC 62443 シリーズ標準の策定の経緯と全体概要を紹介しました。次回からは、IEC 62443 シリーズ標準の中で注目される概念を毎回一つずつ取り上げて、紹介していく予定です。

## 参考


[1] International Society of Automation （ISA） History of ISA
https://www.isa.org/about-isa/history-of-isa

[2] International Electrotechnical Commission （IEC）
https://www.iec.ch/who-we-are

[3] 大規模プラント・ネットワーク・セキュリティ対策委員会
大規模プラント・ネットワーク・セキュリティについて ～重要システムのサイバーテロリズム・クラッキング対策のあり方～， 2000 年 3 月

[4] ENISA: The EU Network and Information Security （NIS） directive
https://www.enisa.europa.eu/topics/nis-directive

[5] Eric Cosman: ISA/IEC 62443 as a Horizontal Standard, ARC Advisory Group blog, 2021 年 11 月 3 日
https://www.arcweb.com/blog/isaiec-62443-horizontal-standard

[6] The Process Automation Users' Association
https://www.wib.nl/about-wib/