標準から学ぶ ICS セキュリティ #6

# サービス事業者に対するセキュリティ要件


2023 年 12 月 14 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

本分冊の第 2 版が 2023 年 12 月 15 日に公開されました。これに合わせて本稿の一部の記述を見直しました。
2024 年 4 月 3 日

今回は IEC 62443-2-4（以下では本分冊と記します）で定義されている、アセットオーナーがサービス事業者に対して要求するセキュリティ要件について書きます。また、本分冊は IEC 62443 シリーズの他の分冊と大きく異なった文書のスタイルで書かれており、その背景についても紹介したいと思います。

## 2. WIB 標準から IEC 標準へ

本分冊の文書スタイルが他の分冊と大きく異なっているのは、他の分冊が ISA 99 委員会または IEC TC65/WG10 で最初から書き起こされているのに対して、本分冊だけが、WIB と呼ばれる業界団体が作成した標準をベースにして開発されたという生い立ちに由来しています。本章では、業界団体 WIB の概要と本分冊の生い立ちを紹介します。

1963 年にさかのぼりますが、現在の Shell 社の前身企業である Bataafse Petroleum Maatschappij 社や、その後に TATA 製鉄と Unilever 社に分社化された Hoogovens 社を中心とする、当時のオランダの大手プロセス産業企業 5 社が、プロセス計装機器の結合試験を合同で実施して成果を得たことを契機に、競合領域を抱えつつも複数のアセットオーナー企業が ICS 技術の領域で協力して活動する意義を見出し、「Werkgroup voor Instrument Beoordeling」（英語では Working Group for Instrument Assessment；縮めて WIB）と称する協議会を発足させました。その後 WIB[1]は新たな会員企業を迎え、オランダ国外の企業も参加するようになって公用語を英語に切り替えるなど、国際的な組織に衣替えしました。WIB は、21 世紀に入り ICS に対するサイバー攻撃への懸念が高まり始めると、調達先の ICS ベンダーに対して求めるセキュリティ要件を「ベンダーに対するプロセス制御分野のセキュリティ要件」[2]と題した報告書にまとめて公表しました。WIB の会員企業の Shell 社や BP 社などが、ICS の調達時にこの報告書に書かれた要件を ICS ベンダーに要求し始めて、この文書は WIB のセキュリティ標準として ICS のコミュニティーに知られるようになりました。

一方、IEC 62443 シリーズを開発していた作業部会は、WIB のセキュリティ標準を国際標準化する提案を受け、これを ICS サービス提供事業者に関するセキュリティプログラム要件として位置付けた上で分冊 2-4 として採択しました。要件を表の形式で記述して付録 A とし、文書の本文では表の読み方を説明するスタイルが、WIB

のセキュリティ標準から分冊 2-4 に引き継がれました。そのために、本分冊は他の分冊と著しく異なったスタイルになっています。文書のスタイルが継承された一方で、文書のタイトルは「ベンダーに対するセキュリティ要件」から「ICS サービス事業者に対するセキュリティプログラム要件」に置き換えられました。ここで ICS サービスとして注目されているのは、システムインテグレーション（以下では SI と記します）サービスと保守サービスです。アセットオーナーによる ICS あるいはそのコンポーネントの購入は、これらのサービス事業者を介してなされることが多いことを考えると、この文書名の変更は自然なものと言えましょう。

## 3. SI サービス

ICS は、製造装置や生産施設を監視あるいは制御するためのものなので、監視や制御の対象である装置や施設と一体のものとして構築されます。SI 業務は、装置や施設から ICS までを広くカバーして、設計と調達、設置を担当することから、EPC（Engineering, Procurement and Construction）とも呼ばれます。SI 事業に参入している会社の本業は、建設業から装置製造業、ICS ベンダー、エンジニアリング会社までさまざまです。ちなみに、IT システムの SI では、アプリケーション・ソフトウェアの開発が業務の多くを占め、ほぼソフトウェア会社の独壇場となっているのと対照的です。

SI サービス事業者にとって、セキュリティに関する認識のすり合わせは発注者であるアセットオーナーとの間で苦労することが多いようです。予算上はプロジェクト全体のたかだか数パーセント程度しか占めないセキュリティ関連の仕様の合意に手間取って、プロジェクト全体の進捗の遅れを引き起こし、ひいては大きなコスト増を招く要因となることも少なからずあると聞きます。アセットオーナーからのセキュリティに関する要求という側面とともに、SI 事業者側においても、アセットオーナーとセキュリティに関する調整を進める際の基準点として有効に活用されることを期待して、本分冊の開発が進められたものと推測されます。

## 4. セキュリティ要件の全体概要

本分冊で定義されているセキュリティ要件には、基本要件（BR；basic requirement）と要件拡張（RE；requirement enhancement）の 2 種類があります。後で詳しく書きますが、基本要件が一般原則であるのに対して、要件拡張は、対応する基本要件をより具体的で個別的な環境に合わせて、詳細化した要件です。なお、まったく要件拡張を伴わない基本要件もあれば、複数の要件拡張を伴った基本要件

表 1.　要件 ID と機能分野

| 要件 ID | 機能分野 | 備考 |
|---|---|---|
| SP.01.01～07 | ソリューション要員 | 要員の選定や教育訓練 |
| SP.02.01～03 | 保証 | ICS セキュリティ・ポリシーの徹底 |
| SP.03.01～10 | アーキテクチャー | ICS ソリューションの設計 |
| SP.04.01～03 | 無線 | ICS 環境内の無線利用 |
| SP.05.01～09 | 安全計装システム | 安全計装システムの ICS への統合 |
| SP.06.01～03 | 設定管理 | ICS の設定管理 |
| SP.07.01～04 | 遠隔アクセス | ICS への遠隔アクセス |
| SP.08.01～04 | 事故管理 | ICS 環境内の事故の取扱 |
| SP.09.01～09 | アカウント管理 | ICS 環境内の利用者アカウントの管理 |
| SP.10.01～05 | マルウェア防御 | ICS 環境内でのマルウェア対策ソフトウェアの利用 |
| SP.11.01～06x | パッチ管理 | ソフトウェア・パッチの承認と適用のセキュリティ |
| SP.12.01～09 | バックアップ/復元 | バックアップと復元のセキュリティ |

もあります。

基本要件として 72 項目が定義されており、表 1 に示した 12 のカテゴリーに分類されています。なお、本分冊では、セキュリティ要件を「セキュリティ・プログラム要件（security program requirement）」、12 のカテゴリーを「機能分野（functional area）」と呼んでいます。各機能分野には 3 項目から 10 項目のセキュリティ要件が含まれています。

各セキュリティ要件には、例えば「SP.04.02」のように、「SP.*fa.sn*」の形式で要件 ID が割り当てられています。ここで、*fa* は機能分野を示す 2 桁の数字、*sn* は各機能分野で連番になっている 2 桁の数字です。要件拡張には、対応する基本要件と同じ要件 ID が割り当てられています。同じ要件 ID をもつ要件拡張が複数存在する場合もありますので、「RE（*n*）」のように同じ要件 ID を持つものの中で採番して識別されています。

基本要件と要件拡張の例として、無線に関する SP.04.02 の基本要件と要件拡張を表 2 に示します。なお、2023 年 12 月 15 日に公開された第 2 版でセキュリティ要件の記述スタイルが大きく変更されましたので、この改訂の紹介を兼ねて、表 2 では初版である 2017 年版と第 2 版の 2023 版の双方のセキュリティ要件を掲げています。

表 2. 基本要件と要件拡張の例（SP.04.02）

| | 2017 年版 | 2023 年版 |
|---|---|---|
| 基本要件 BR | セキュリティ・コミュニティーと産業用オートメーション・コミュニティーの双方が広く受け入れている認証とアクセス制御の仕組みを使って，無線機器へのアクセスを保護するために，オートメーション・ソリューションを設定する能力をサービス事業者が持たなければならない. | セキュリティ・コミュニティーと産業用オートメーション・コミュニティーの双方が広く受け入れている認証とアクセス制御の仕組みを使うよう，アクセスを保護すべきオートメーション・ソリューションが設定されていることを，アセットオーナーが確かめるために実施できるプロセスをサービス事業者が持たなければならない. |
| 要件拡張 RE（1） | セキュリティ・コミュニティーと産業用オートメーション・コミュニティーの双方が広く受け入れている暗号の仕組みを使って保護された無線通信を使うようオートメーション・ソリューションを設定する能力をサービス事業者が持たなければならない. | 無線通信を保護するようオートメーション・ソリューションが設定されており，かつ，この目的で暗号の仕組みが使わる場合には，その暗号の仕組みがセキュリティ・コミュニティーと産業用オートメーション・コミュニティーの双方が広く受け入れているものであることを，アセットオーナーが確かめるために実施できるプロセスをサービス事業者が持たなければならない. |

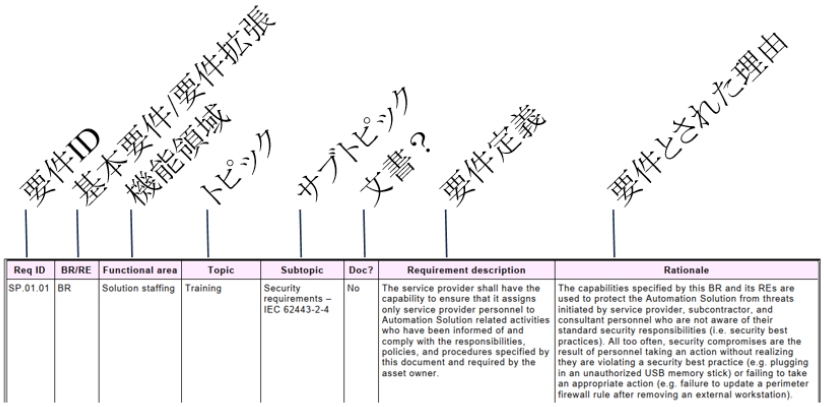
上掲の例において基本要件では「認証とアクセス制御の仕組みを使って」と一般的な状況について要件を述べているのに対して、要件拡張では「暗号の仕組みを使った」と特定された状況に関して要件を述べていることを確認して、基本要件と要件拡張との関係をご理解願います。なお、例示した SP.04.02 では要件拡張は RE（1）の 1 項目のみです。

また、2017 年版と 2023 年版とを比較すると、前者では「サービス事業者が○○しなければならない」とサービス事業者への要求を直接に述べているのに対して、後者では「○○であることをアセットオーナーが確認するために実施できるプロセスをサービス提供事業者が持たなければならない」という見方によっては回りくどい構文で記述されています。この構文は、SP.04.02 だけでなく、すべての要件に共通して採用されています。

発注者から目が届きにくくブラックボックスとなってしまう領域に潜んだサービス事業者による不適切な判断や不手際が原因でセキュリティ事故に至る可能性が決して無視できません。2023 年版では、アセットオーナーによる検証の機会を確保することにより、そうした懸念を解消しようとしています。さらに、それによりアセットオーナーの立ち位置が明確化されました。2017 年版では、サービス事業者に対する要求を定義した本分冊が、アセットオーナーによるセキュリティ管理を論じる IEC 62443-2-x のグループに含められていることに違和感がありましたが、アセットオーナーの立ち位置を示した 2023 年版により、そうした違和感も解消されました。

## 5. セキュリティ要件表の形式

先にも述べたように、本分冊ではセキュリティ要件を表にまとめて付録 A として添付し、本文で表の見方を説明しています。付録 A の冒頭部分を図 1 に示します。個々の要件が表の各行に対応し、そのそれぞれについて、8 つの列に対応する項目が記載されています。




| Req ID | BR/RE | Functional area | Topic | Subtopic | Doc? | Requirement description | Rationale |
|---|---|---|---|---|---|---|---|
| SP.01.01 | BR | Solution staffing | Training | Security requirements – IEC 62443-2-4 | No | The service provider shall have the capability to ensure that it assigns only service provider personnel to Automation Solution related activities who have been informed of and comply with the responsibilities, policies, and procedures specified by this document and required by the asset owner. | The capabilities specified by this BR and its REs are used to protect the Automation Solution from threats initiated by service provider, subcontractor, and consultant personnel who are not aware of their standard security responsibilities (i.e. security best practices). All too often, security compromises are the result of personnel taking an action without realizing they are violating a security best practice (e.g. plugging in an unauthorized USB memory stick) or failing to take an appropriate action (e.g. failure to update a perimeter firewall rule after removing an external workstation). |

**図 1. セキュリティ要件表の形式**
（分冊 2-4 付録 A の冒頭部分）

8 つの列のうち、左側の 3 列の「要件 ID」と「機能要件/要件拡張」、「機能領域」については前章で説明しました。

次の 2 列の「トピック」と「サブトピック」はセキュリティ要件を特徴づけるために付与されたキーワードです。概して、トピックとしては「アカウント－デフォールト」や「脆弱性」など 20 余りの技術を示す語句が、サブトピックとしては「承認」や「無害化」など 40 余りの行動を示す語句が付与されています。トピックとサブトピックは相互に独立していて、階層的な関係になく、また、12 の機能分野とも独立した関係にあるとされています。トピックとサブトピックは、要件をキーワード検索する際に利用することが想定されているようです。

「文書？」の列には、Yes または No が記載されていて、アセットオーナーへの文書提供が必要なセキュリティ要件であるか否かを定めています。

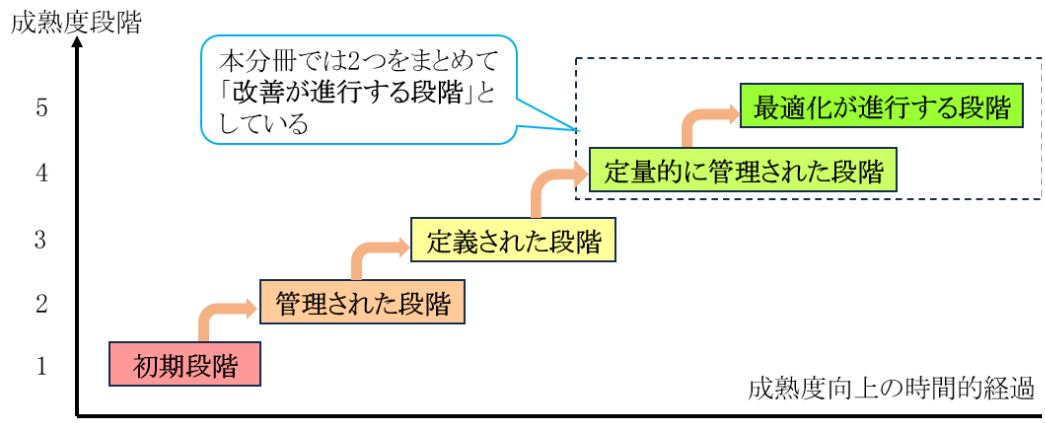
「要件定義」の列にはセキュリティ要件の本体が書かれ、右端の「要件とされた理由」の列には、当該事項をセキュリティ要件に含めている理由が説明されています。

## 6. 成熟度モデルと第三者認証

WIB 標準から本分冊が作られた際に、成熟度モデルを説明した節が新たに追加されました。

「能力成熟度モデル（CMM；Capability Maturity Model）」は、ソフトウェア開発プロセスについて成熟度を測る指標としてカーネギーメロン大学（CMU）で発案されたものです。プロセスの進め方として、「初期段階」（レベル 1）から「管理された段階」（レベル 2）、「定義された段階」（レベル 3）、「定量的に管理された段階」（レベル 4）、「最適化が進行する段階」（レベル 5）の 5 段階を設定し、どの段階にプロジェクト管理能力があるかを評価します（図 2 参照）。この考え方は、その後、ソフトウェア開発だけでなく、組織におけ

るプロジェクト管理一般に対して、管理能力を評価する指標として「能力熟成度モデル統合（CMMI；Capability Maturity Model Integration）」の名称で広く使われるようになりました。




レベル 1「初期段階」：プロセスが定義されておらず場当たり的に実施されていて、成否が個人の力量や運不運に依存する

レベル 2「管理された段階」：コストやスケジュール、機能の充足性を確認する基本的な管理プロセスが確立されている

レベル 3「定義された段階」：組織の標準的なプロセスが文書化され標準化され統合化されていて徹底されている

レベル 4「定量的に管理された段階」：プロセスおよび成果について定量的な計測が収集され理解されている

レベル 5「最適化が進行する段階」：革新的なアイデアや新技術を採用するとともに、定量的なフィードバックに基づくプロセスの改善と最適化がなされている

**図 2. 能力成熟度モデル**

本分冊が定義しているセキュリティ要件をクリアする際のサービス事業者における管理能力を能力成熟度モデル統合によって評価計測しより高い成熟度に誘導することが、本分冊で成熟度モデルについて説明されている理由と言えましょう。本分冊で定義されたセキュリティ要件に場当たり的に対応して何とかクリアする初期段階の管理能力の成熟度で満足することなく、体系的に整備されたプロセス定義をベースとして持ち、そのプロセスを定量的な評価に基づくフィードバックと新たな情報を取り入れて自律的に改善していく活動を伴った、サービス提供のあり方が期待されているのです。なお、本分冊の成熟度モデルでは CMMI のレベル 4 とレベル 5 を一つにまとめ 4 段階で成熟度を定義しています。

現在、本分冊に基づいてサービス事業者の管理能力を評価するための分冊 6-1 の開発が進められています。現時点では、サービス事業者のセキュリティに関する第三者認証は、IT システムについても ICS についても、事業者の組織内におけるセキュリティ管理を ISO/IEC 27000 シリーズに基づいた評価を準用しているケースが多いと思われます。分冊 6-1 が発行されれば、ICS に対応し、本分冊に基づいたサービス事業者に対する第三者認証が始まることが期待されます。

## 7. まとめ

本稿では、ICS に関するシステムインテグレーションや保守のサービス提供事業者に対してアセットオーナーが求めるセキュリティ要件を規定した IEC 62443-2-4 について、標準化の経緯と概要を紹介しました。また、本分冊をベースにしたサービス事業者のプロセスに関する第三者認証の方向性についても概観しました。

## 参考文献

[1] WIB：History of Web, https://www.wib.nl/home

[2] WIB：Process Control Domain - Security Requirements for Vendors, 2010 年, http://osgug.ucaiug.org/conformity/security/Shared%20Documents/WIB%20M2784%20PCS%20VendorSecurity%20v2.pdf