標準から学ぶ ICS セキュリティ #8

ICS のシステムに対するセキュリティ要件

2025 年 8 月 21 日

一般社団法人 JPCERT コーディネーションセンター

1. はじめに

ICS 分野でのセキュリティ認証制度は、まずコンポーネント製品に対するものから始まりました。これに次いで、コンポーネントよりも複雑なコントローラー製品等を対象とした ICS のシステムに対するセキュリティ認証制度が開始されました。いずれもセキュリティ水準（SL）のそれぞれに対して定められた機能セキュリティが装備されているかどうかを第三者が確認した上で認証が付与されることになっています。ICS 自体が「産業用制御システム」（Industrial Control System）ですので、「ICS のシステム」の表現は冗語のように見えるかもしれませんが、今回は、ICS のシステムに対するセキュリティ認証基準をベースに、ICS のシステムが満たすべきセキュリティ要件を定義した IEC 62443-3-3 「システムのセキュリティ要件とセキュリティ水準」（以下、「本分冊」という。）について紹介します。必要に応じて本シリーズの第 7 回「ICS コンポーネントに対するセキュリティ要件」と比較対照していただければ幸いです。

本分冊でセキュリティ要件が定義される対象の「システム」は、「考察対象システム」（SuC：System under Consideration）と呼ばれるものです。その定義は本分冊中に見当たりませんが、他の分冊の中、例えば分冊 3-2 では「セキュリティリスク分析を実施する目的のための ICS と関連資産の定義された集まり」とされ、「一つ以上のゾーンと関連するコンジットから構成され、システム内の資産はすべてゾーンまたはコンジットに属する」と説明されています。厳密さを犠牲にして平たく表現すれば、DCS などのコントローラー製品が相当し、アセットオーナーが導入構築し運用する ICS 全体とは異なります。

一方で、ICS のコンポーネント（特に組込み機器タイプのコンポーネント）と ICS のシステムの境界線は曖昧であり、コントローラーなどは両者のいずれでもあるといえそうです。なお、IEC 62443 シリーズにおける「システム」の用語については第 5 章で論ずることにします。

本シリーズ「標準から学ぶ ICS セキュリティ」の第 7 回で紹介した ICS コンポーネントのセキュリティ要件を定めている分冊 4-2 は本分冊をベースに策定されており、対象が ICS のシステムであるのか ICS のコンポーネントであるのかに由来する相違点があるのみで、分冊 3-3 と分冊 4-2 とは基本的に共通した考え方に基づいた内容となっています。

また、本分冊に記述された考え方に基づいた、ICS のシステムを対象とした認証制度「System Security Assessment（SSA）」[1] が、ISA 傘下の ISA Security Compliance Institute（ISCI（イスキー））によって 2013 年から運用されています。これまでに SSA の認証を受けている製品[2] の多くが安全計装システムです。この背

景には、顧客からの要求と、高価格製品でなければ認証を取得するためのコストを吸収することが難しいことがあるとみられます。

2. 製品認証とセキュリティ要件

ICS システム製品に対するセキュリティ認証である ISCI の SSA では、1）分冊 4-1 で定義されているセキュア開発ライフサイクルに即して製品が開発されていること、2）本分冊で定義された機能セキュリティ（functional security capability）を装備していること、3）脆弱性探索試験（ファジング試験）をパスしていることを第三者機関が評価確認して、認証が付与されることになっています。コンポーネント製品に対するセキュリティ認証である EDSA や CSA では装備すべき機能セキュリティが分冊 4-2 であったのに対して、SSA では分冊 3-3 になっていることだけが両者の間の違いです。すなわち、SSA では、分冊 4-1 で定められているセキュア開発ライフサイクルによって潜在的に可能な攻撃シナリオを設計時に洗い出せていなかったために作り込まれる脆弱性を回避し、本分冊が定義する要件を確認することによって当然に装備されるべき基本的なセキュリティ機能が設計から抜け落ちていたことによる脆弱性を回避し、脆弱性探索試験によってコーディングなど実現段階における不注意から作り込まれる脆弱性を減らすことを狙っています。

3. 基礎的要件

IEC 62443 シリーズ全体を通して、各分冊の中で必須であると定められているセキュリティ要件は、技術的要件または組織的要件にさかのぼることができなければならないとされています。このうち、技術的要件の基礎となっているのが、表 1 に示した 7 つの特性を備えていることを求めた「基礎的要件」（Foundational Requirement）と呼ばれるものです。ICS のシステムやコンポーネントが技術的にセキュアであると主張するためには、これら 7 つの特性を備えている必要があります。

ICS システムのセキュリティ要件は、基礎的要件をさらに詳細化し具体化したものとして定義されます。

表 1. 7 つの基礎的要件

項番	セキュリティ対策	説明
1	識別と認証管理 （IAC） Identification and Authentication Control	ICS にアクセスしようとする利用者（人、ソフトウェア・プロセス、または機器）を正しく特定し、利用者に応じた権限を許諾する
2	利用管理 （UC） Use Control	許諾された行為だけを利用者が行うよう強制し、それを監視する
3	システムの完全性 （SI） System Integrity	ICS の状態を設計時に想定された範囲内に保ち、想定外の状態への遷移を防ぐ
4	データの秘密性 （DC） Data Confidentiality	通信中または格納中のデータの秘密性を守り、許されるべきでない開示を防ぐ
5	データの流れの制限 （RDF） Restricted Data Flow	不必要なデータの流れを防ぐために、ゾーンとコンジットによってシステムをセグメント化する
6	事象に対するタイムリーな応答 （TRE） Timely Response to Events	セキュリティ違反事象（インシデント）が見つかった際に、適切に通知し、必要な証拠を提示し、タイムリーな訂正行為を取ることによって、当該事象に対処する
7	資源の可用性 （RA） Resource Availability	必須サービスが停止したり縮退したりすることのないよう ICS の可用性を担保する

基礎的要件のうち、**識別と認証管理**（1）と**利用管理**（2）は、ICS システムを操作しようとする利用者に対して、本人であることを確認し、確認結果に基づいて許されるべき操作だけに操作を制限するセキュリティ機能を ICS システムが備えることを求めています。IEC 62443 の策定が始まった 2010 年ごろの、いわば ICS セキュリティの創成期以前には ICS に悪意の利用者が存在する可能性を想定していませんでした。利用者を識別することを求め、その結果に基づいて許される操作を制限する、これらの要件は今では当然のものとして受け入れられていますが、本分冊が発行された 2013 年当時においては厳しい要件と見られていたように思います。ICS へのサイバー攻撃の可能性を懸念していなかった時代の名残として、認証情報のメモ書きが操作卓に貼ってあったり、デフォルトの認証情報のままで運用されていたりするケースが今でも一部に見られることは大変に残念なことです。

基礎的要件のシステムの完全性（3）とデータの秘密性（4）と資源の可用性（7）は、「セキュリティの CIA」とも呼ばれるセキュリティの 3 つの基本概念に対応しています。「セキュリティの CIA」とは秘密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の三者の頭文字を並べたものです。**秘密性**とは、情報へのアクセスや情報の開示に関する許諾制限が適切に維持されていて、不適切な情報流出の可能性がない状態を維持する性質です。また**完全性**とは、資産の正確さと、欠落の無い完全さが守られた状態を維持する性質です。さらに**可用性**とは、遅滞なく信頼性をもって、制御システムの情報と機能にアクセスでき利用することができる状態を維持する性質です。セキュリティの CIA は、IT を対象とした情報セキュリティにも ICS などを対象とした OT セキュリティにも共通する概念ですが、前者では秘密性が損なわれた場合の損失が大きくなりがちであるのに対して、後者では可用性が損なわれた場合の損失が問題になりやすいといった色合いの相違がしばしば指摘されています。

基礎要件の**事象に対するタイムリーな応答**（6）では、文字どおり、セキュリティ違反を検知した場合に遅滞なくアラームを発し違反を示す証拠を提示することを求めています。成功した ICS に対する攻撃の多くに意図的でない場合を含めて組織内部の者が関与しているとされており、セキュリティ違反に対する迅速な対処には内部犯や不注意を防ぐための牽制効果も期待されます。

4. セキュリティ要件

本分冊では、ICS のシステムに対するセキュリティ要件として 49 項目が掲げられており、それぞれに次の 6 項目が定義されています。

1） 要件項目番号
2） 要件項目名称
3） 要件項目の基本部分の定義
4） この項目が要件とされている理由や付加的なガイダンス
5） 要件拡張
6） セキュリティ水準ごとの要件の指定

「要件項目番号」は次のような形式で付与されています。

＜要件項目番号＞	::=	SR ＜基礎的要件番号＞ . ＜枝番号＞
＜基礎的要件番号＞	::=	1 ～ 7
＜枝番号＞	::=	1～

要件項目番号は、先頭の文字が「S」に固定されていることを除き、ICS コンポーネントに対するセキュリティ要件におけるそれと共通した形式になっています。ちなみに ICS コンポーネントに対するセキュリティ要件の先頭の文字はコンポーネントを示すCまたはコンポーネントの種別を示すSAか、ED、HD、NDのいずれかでした。＜基礎的要件番号＞は表1の項番欄にある数字を意味しています。

「要件項目名称」は、例えば「利用者の識別と権限付与」（SR 1.1）のように、要件項目の概要を表現した語句です。

「要件項目番号」と「要件項目名称」との組み合わせは、本分冊で定義されている ICS システムに対するセキュリティ要件と、分冊 4-2 で定義されている ICS コンポーネントに対するセキュリティ要件との間で共通しているものも多くありますが、一部に相違や枝番号のズレが少なからずありますのでご注意ください。

「要件拡張」は、要件の基本部分に追加される要件で、「(1)」「(2)」のように連番で定義されます。なお、要件項目によって「要件拡張」がまったくない場合もあります。この記法も ICS コンポーネントに対するセキュリティ要件を定義した分冊 4-2 と同様です。

「セキュリティ水準ごとの要件の指定」は、1～4 のセキュリティ水準のそれぞれに対して ICS システムに要求される要件を、要件番号とそれに付随する要件拡張の番号により指定するものです。セキュリティ水準については本シリーズの第 3 回で紹介していますので、必要に応じて参照ください。例として「公開鍵ベース認証の強度（SR 1.8）」を選び、「セキュリティ水準ごとの要件の指定」の記述を図 1 に示します。この例は、SR 1.8 の要件に関して、無条件にセキュリティ水準 1 のセキュリティ機能を持っているといえますが、セキュリティ水準 2 のセキュリティ機能を持っているというためには要件の基本部分に適合している必要があり、さらに、セキュリティ水準 3 または 4 のセキュリティ機能を持っているというためには、要件の基本部分に加えて要件拡張の(1)に適合している必要があることを意味しています。

4.10.4 セキュリティ水準

4 つのセキュリティ水準に対する SR 1.8 関連の要件は：

- SL-C（IAC、ICS システム）1：非選択
- SL-C（IAC、ICS システム）2：SR 1.8
- SL-C（IAC、ICS システム）3：SR 1.8 (1)
- SL-C（IAC、ICS システム）4：SR 1.8 (1)

図 1.　セキュリティ水準ごとの要件の指定の例

ICS コンポーネントに対するセキュリティ要件として本分冊で定義されている要件項目について、要件項目番号と要件項目名称を一覧表にまとめて表 2 に示しています。

表 2.　ICS のシステムに対するセキュリティ要件の項目番号と名称

要件項目番号		要件項目名称	
SR	基礎的要件番号	枝番号	
SR	1. （IAC；識別と認証管理）	1	利用者を識別し権限を制御する
		2	ソフトウェア・プロセスと機器を識別し権限を制御する
		3	アカウントを管理する
		4	認証子（ID）を管理する
		5	権限制御機構を管理する
		6	パスワード・ベース認証の強度
		7	公開鍵基盤の証明書

		8	公開鍵ベース認証の強度
		9	認証機構からの応答
		10	ログイン試行の失敗
		11	システム利用であることを通知する
		12	信頼できないネットワークを介したアクセス
		13	対称鍵ベース認証の強度
	2. （UC；利用管理）	1	権限制御を強制する
		2	無線利用を管理する
		3	携帯機器と移動機器の利用を管理する
		4	モバイルコード
		5	セッションのロック
		6	遠隔セッションの期限切れ
		7	同時併行セッションを管理する
		8	監査できるようにすべき事象
		9	監査用記録のための記憶容量
		10	監査用記録の不具合への対応
		11	監査情報を保護する
		12	否認を排除する
	3. （SI；システムの完全性）	1	通信の完全性
		2	悪意あるコードから保護する
		3	セキュリティ機能（security functionality）の作動を検証する
		4	ソフトウェアと情報の完全性
		5	入力を検証する
		6	エラー処理
	4. （DC；データの秘密性）	1	情報の持続性
		2	情報の秘密性
		3	暗号を利用する
	5. （RDF；データの流れの制限）	1	ネットワークをセグメント化する
		2	ゾーン境界を保護する
		3	人間から人間への汎用の通信を制限する
		4	ゾーン化を助けるために、データやアプリケーション、サービスを分離できる機能を持つ
	6. （TRE；事象に対するタイムリーな応答）	1	監査用ログを読み出せる
		2	連続的に監視する
	7. （RA；資源の可用性）	1	DoS 攻撃から保護する
		2	資源を管理する
		3	ICS システムのバックアップを採取する機能を持つ
		4	ICS システムを復元し再構成する機能を持つ
		5	非常時電源への切り替え機能を持つ
		6	ネットワーク設定とセキュリティ設定の設定機能を持つ
		7	必要な機能だけを持つ（不要な機能を持たない）
		8	ICS システムのコンポーネントの棚卸しを報告する機能を持つ
		9	監査記録を格納するために十分な容量を割り当てている

ICS のシステムに対するセキュリティ要件（表 2）を、ICS のコンポーネントに対するセキュリティ要件と対比して、相違点を次にまとめておきます。

基礎的要件 1（IAC；識別と認証管理）に関連しては、ネットワーク機器タイプのコンポーネントに要求されている無線アクセス管理（CR1.6）がありません。それ以外の 13 項目はおおむね同じです。

基礎的要件 2（UC；利用管理）に関連しては、ICS のコンポーネントに要求されている、監査用データを格納しておくための記憶領域の容量（CR2.9）と、物理的診断の利用と試験インタフェース（CR2.13）の 2 項目がありません。それ以外の 12 項目はおおむね同じです。なお、監査用データを格納しておくための記憶領域の容量（CR2.9）の要件については、類似したもの（SR7.9）が ICS のシステムに対する基礎的要件 7 の中に含まれています。

基礎的要件 3（SI；システムの完全性）に関連しては、ICS のコンポーネントに要求されている、監査情報の保護（CR3.9）、アップデートのサポート（CR3.10）、物理的なタンパー（いたずら細工）に対する耐性（CR3.11）、製品提供事業者の信頼の根底の提供（CR3.12）、アセットオーナーの信頼の根底の提供（CR3.13）、ブート・プロセスの完全性（CR3.14）の 6 項目がありません。それ以外の 7 項目はおおむね同じです。

基礎的要件 4（DC；データの秘密性）に関連する 3 項目、基礎的要件 5（RDF；データの流れの制限）に関連する 4 項目、基礎的要件 6（TRE；事象に対するタイムリーな応答）に関連する 2 項目には大きな相違がありません。

基礎的要件 7（RA；資源の可用性）に関連しては、ICS のコンポーネントに対しては要求されていない緊急電源（SR7.5）と監査用データを格納しておくための記憶領域の容量（SR7.9）が加わっています。それ以外の 8 項目はおおむね同じです。なお、ICS のコンポーネントに対するセキュリティ要件の一覧中で「CR7.5」の項目番号は欠番になっています。

5. IEC 62443 シリーズにおける「システム」

2009 年版の分冊 1-1（用語と概念とモデル）は、システムを「複雑な全体を形成している、相互作用し、相互に関連し、相互に依存している要素」と定義し、IACS（Industrial Automation and Control System）を「産業プロセスの安全でセキュアで信頼できる運用に影響し得る人々とハードウェアとソフトウェアの集まり」と定義しています。いずれも厳密な定義とは言い難いように思います。また、分冊 3-3 には先にも書いたように「システム」の定義が見当たりません。なお、分冊 1-1 の改訂案では、産業用以外の制御システムもスコープに含める水平標準化を見据えて「産業用（Industrial）」を削除した「ACS（Automation and Control System）」で置き換えるとともに、人的側面を取り去ったものとして定義する方向で検討されているようです。

一方、ICS のコンポーネントの製品認証の後を追って、システムの認証が検討される中で分冊 3-3 が作られた経緯を思い起こすと、ICS 全体をイメージして「システム」と呼んでいた可能性があります。しかしながら、製品認証において参照される要件であることから、制御システム製品ベンダーが提供するターンキー・システムなどを中心とした製品と理解される方向に変化していったのかもしれません。

また、現在改訂中の分冊 1-1 の草案では、各分冊の主な役割を、分冊 4-2 については製品提供事業者向けとしていますが、分冊 3-3 は製品提供事業者だけでなくアセットオーナーやサービス提供事業者にも向けたものと位置付けています。さらに、ライフサイクルにおける適用期間を、分冊 4-2 については製造段階までとしています

が、分冊 3-3 については廃棄までの全期間としています。2013 年版の分冊 3-3 にはシステムの利用や廃棄に関する記述は見当たらないように思いますので、今後に規模の大きな改定が計画されているのかとも推測されます。

なお、ISA ではアセットオーナーによる ICS の構築運用が IEC 62443 シリーズが規定したセキュリティ基準に合致していることを認証する新しい認証制度「IACS Security Assurance（ACSSA）プログラム」[3] [4] を 2025 年 1 月に発表しています。

6. まとめ

本稿では、ICS システムに対するセキュリティ要件の定義について概観しました。これを定義している本分冊は、ICS のコンポーネントに対するセキュリティ要件を定義した分冊 4-2 と非常に似通った構成を持ち、要件番号も双方の間で整合させようとしたかに見えて、一部にズレが生じています。本分冊が 2013 年に発行され、分冊 4-2 が 2019 年に発行されていて、6 年間の時間的な隔たりによるやむを得ない事情があったのかもしれません。分冊間の整合性を高める取り組みが現在進められているとも聞いていますので、次の改訂ではそうしたズレが一掃されることも期待されます。加えて、第 5 章で言及したような大改訂の可能性もありそうです。

参考文献

[1] ISA： System Security Assurance (SSA) Certification, https://isasecure.org/certification/iec-62443-ssa-certification

[2] ISA： ISA/IEC 62443-3-3 Certified Systems, https://isasecure.org/end-users/iec-62443-3-3-certified-systems

[3] ISA： Update to ISA/IEC 62443 Standards Addresses Organization-Wide Cybersecurity in Industrial and Critical Infrastructure Operations, 2025 年 1 月 28 日, https://www.isa.org/news-press-releases/2025/january/update-to-isa-iec-62443-standards-addresses-organi

[4] ISA： Partner with Us: ISA/IEC 62443 IACS Security Assurance (ACSSA) Program, https://isasecure.org/isasecure-site-assessment