標準から学ぶ ICS セキュリティ #7

ICS コンポーネントに対するセキュリティ要件

2024 年 6 月 20 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

IEC 62443-4-2（以下、「本分冊」という。）では、ICS コンポーネントが満たすべきセキュリティ要件が 4 段階のセキュリティ水準ごとに定義されています。IEC 62443 シリーズ標準の発行が始まって間もない 2010 年代前半には、マルウェア Stuxnet の報告を契機に ICS セキュリティの問題が注目の的になって脆弱性の探索調査が活発化し、容易に見つかるような多数の脆弱性を ICS コンポーネントが持っていることが明らかにされていました。当時は、悪意を持った攻撃がまったくと言っていいほど配慮されることなく ICS コンポーネントの開発がなされていたためです。そうした状況の改善が喫緊の課題であり、そのための方策の一つとして、ICS コンポーネント製品のセキュリティに関する認証評価制度が整備されました。制度が整備された当時は、認証の取得が調達要件に加えられれば、幅広い製品が認証を取得するようになり、製品のセキュリティ状況が一挙に好転するとの期待もありました。しかしながら、認証を取得するための追加コストが嫌われたことなどから、実際に認証を受けたのは比較的高価格帯の一部の製品に限られる結果となりました。そうであっても、製品のセキュリティ認証の基準が文書として示されたことにより、製品開発事業者がセキュリティ面で配慮すべきことが明確化されたことは大きな意義があったように思います。こうした認証制度の中で整備された文書や知見をベースに策定されたのが本分冊です。その初版が公開されたのは 2019 年で、IEC 62443 シリーズ標準の中でも比較的遅い時期でした。

ICS 関連のセキュリティ認証制度の中で最初に発足したのが、ICS コンポーネント製品を対象とした、ISA 傘下の ISA Security Compliance Institute（ISCI（イスキー））による「ISASecure Embedded Device Security Assurance（EDSA）」でした。2011 年に最初の認証が交付され、その後 2019 年発行の第 3 版まで認証基準の改版が重ねられました。EDSA の後を追って、システムとしての ICS を対象とした認証制度「System Security Assurance（SSA）」も始まり、2013 年には、これに対応した、ICS 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 が発行されました。一方、EDSA の認証基準も IEC 62443-3-3 との整合性を高める方向で改訂が加えられました。こうした経緯を経て 2019 年に発行されたのが本分冊です。

また、EDSA という認証制度の名称からもうかがえるように、初期の製品認証においては、PLC などのコントローラーを中心とする組込み機器だけが対象として想定されていましたが、その後、ネットワーク化の一層の進展に伴って、組込み機器以外の ICS コンポーネントでセキュリティ上の配慮が欠かせないものが誕生しました。本分冊では、そうしたタイプの ICS コンポーネントも想定してセキュリティ要件が定義されました。本分冊の発行と前後して、ISCI の製品認証制度も 2019 年から「Component Security Assurance（CSA）」認証[1]に

移行しています。さらに、ISCI は、本分冊が定義した要件に基づいた、産業用 IoT 機器（いわゆる IIoT 機器）に対する製品認証制度「ICSA（IIoT Component Security Assurance）」[2]も 2022 年に設けています。また、本分冊の発行後は、ISCI とは独立に、本分冊をベースとした ICS コンポーネント製品の認証を行う製品認証団体も現れています。

2. 製品認証とセキュリティ要件

ICS コンポーネント製品に対するセキュリティ認証である ISCI の EDSA や CSA 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を装備していること、3）脆弱性探索試験（ファジング試験など）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。一般に、製品の脆弱性は、a）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たもの、b）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もの、c）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もの、以上の 3 つのカテゴリーのいずれかに分類できます。セキュア開発ライフサイクルによって a タイプの脆弱性の作り込みを避け、本分冊が定義する要件を確認することにより b タイプの脆弱性の作り込みを避け、脆弱性探索試験を通じて c タイプの脆弱性を減らすことを狙っていると考えられます。

ICS コンポーネントに対する技術的なセキュリティ要件をうたっている本分冊では、一般的な原則として、制御のための必須機能のサポートや、権限の付与を必要最小限に抑えること、ハードウェアが提供するセキュリティ機能の活用、分冊 4-1 で定義されたセキュアな開発プロセスによってソフトウェアを開発することなどもごく簡単に言及されてはいますが、コンポーネントが備えるべきセキュリティ機能の定義が中心になっています。必要なセキュリティ機能を本分冊がどのように定義しているのかを以下に述べます。

3. 基礎的要件

本分冊に限らず、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。

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

ICS コンポーネント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ています。

4. ICS コンポーネントの分類

本分冊では、ICS コンポーネントを表 2 に示した 4 つのタイプに分類しています。ICS コンポーネントの製品認証が始まった 2011 年には、組込み機器だけが想定されていましたが、その後に他の 3 つのタイプが追加されて今日に至っています。

表 2. ICS コンポーネントの 4 つのタイプ

記号	タイプ	定義	例
SA	ソフトウェア・アプリケーション	プロセスまたは制御システム自身とインタフェースするために使われる、一つ以上のソフトウェア・プログラムとそれらの依存関係	SCADA やヒストリアンのような ICS 用のアプリケーション・ソフトウェア、エンジニアリング・ツール
ED	組込み機器	産業プロセスを直接に監視、制御、または、作動させるために設計された組込みソフトウェアを稼働させる専用の機器	PLC、コントローラー
HD	ホスト機器	1 社以上の提供事業者からの、一つ以上のソフトウェア・アプリケーションやデータ格納庫、機能を収容することができる OS（Windows OS や Linux など）を稼働させている汎用機器	サーバー、パソコン
ND	ネットワーク機器	機器間のデータの流れを促す、または、制限するが、直接には制御プロセスに影響を及ぼさない機器	ルーター、スイッチ、RTU

これらのタイプごとに ICS コンポーネントに対するセキュリティ要件が定義され、それぞれ「ソフトウェア・アプリケーション要件」「組込み機器要件」「ホスト機器要件」および「ネットワーク機器要件」と呼ばれます。これらの要件は、それぞれ複数の要件項目から構成されます。

要件項目のレベルで見ると、すべてのタイプの ICS コンポーネントに対して共通した項目がある一方で、各タイプに固有な項目もあります。また、前者が多数を占めるであろうことは誰もが容易に推測できるところかと思います。本分冊では、重複した記述を避けるとともに、要件の曖昧さや混乱の可能性を避けるために、次章で述べるように工夫された記述形式でセキュリティ要件を記述しています。

5. セキュリティ要件項目の記述形式

本分冊では、ICS コンポーネントのセキュリティ要件として 86 項目が掲げられており、うち 74 項目に関しては次の 6 項目が、12 項目に関しては最初の 2 項目（要件項目番号と要件項目名称）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＞	::=	＜コンポーネント･タイプ＞ R ＜基礎的要件番号＞ . ＜枝番号＞
＜コンポーネント･タイプ＞	::=	SA または ED または HD または ND または C
＜基礎的要件番号＞	::=	1 ～ 7
＜枝番号＞	::=	1～

ここで、＜コンポーネント･タイプ＞は、表 2 の記号欄にある 2 文字または「C」のいずれかです。「C」以外の場合には、コンポーネント･タイプ固有の要件項目であることを示し、「C」の場合には、コンポーネント･タイプに依らない共通した要件項目であることを示しています。＜基礎的要件番号＞は表 1 の項番欄にある数字です。

「要件項目名称」は、例えば「利用者の識別と権限付与」（CR 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」の割り当てについては、コンポーネント･タイプが異なっていても＜基礎的要件番号＞と＜枝番号＞の組合せが同じならば、該当する要件項目がある限り、同じ「要件項目名称」になるように＜枝番号＞が採番されています。例えば、CR 2.4 と SAR 2.4、EDR 2.4、HDR 2.4、NDR 2.4 の番号を持つ要件項目は共通して「モバイルコード」の名称を持ちます。ちなみに、これらは Web サーバーから Web ブラウザーに送り込まれて実行されるモバイルコード（いわゆるアプレット）に関する要件を規定しています。また、この例のようにコンポーネント・タイプ固有の要件項目が定義されている場合には、「CR ＜基礎的要件番号＞.＜枝番号＞」（この例では CR 2.4）は、実質的に意味のある要件の定義を持たず、項目番号と項目名称だけが定義されています。本節の冒頭部分に書いた、要件番号と要件名称だけが定義された 12 項目の要件項目がこれに該当します。

「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。

「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 コンポーネント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。セキュリティ水準とは、どの程度に高度な攻撃にまで耐えられるかを示す 4 段階の数値ですが、詳しくは本シリーズの第 3 回[3]で紹介していますので、必要に応じてご参照ください。例として「公開鍵ベース認証の強度（CR 1.9）」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。CR 1.9 の要件に関して、セキュリティ水準 1 ならば必要なセキュリティ機能がなく、セキュリティ水準 2 ならば要件の基本部分に適合したセキュリティ機

能を持っている必要があり、さらに、セキュリティ水準 3 または 4 ならば要件の基本部分に加えて要件拡張の（1）に適合したセキュリティ機能をもっている必要があることをこの例は表明しています。ちなみに、CR 1.9 の基本要件は、公開鍵認証が使える場合に、1）署名検証および証明書取消状態の確認によって証明書の有効性を検証する機能と、2）対応する秘密鍵の利用者管理を確立する機能、3）要求された宛先に照らして名前などをチェックすることにより認証対象を利用者に対応付ける機能、4）対称鍵認証のために使われるアルゴリズムと鍵が CR 4.3（暗号を利用する）に準拠していることを担保する機能を、当該コンポーネントが直接的、または他のシステムとの統合によって間接的に備えるよう定めています。また、要件拡張の（1）では、公開鍵認証のための秘密鍵をハードウェアで保護する機能を提供するよう定めています。

5.11.4 セキュリティ水準

4 つのセキュリティ水準に対する CR 1.9 関連の要件は：

- SL-C (IAC, コンポーネント) 1： 非選択
- SL-C (IAC, コンポーネント) 2： CR 1.9
- SL-C (IAC, コンポーネント) 3： CR 1.9 (1)
- SL-C (IAC, コンポーネント) 4： CR 1.9 (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にまとめて表 3 に示します。なお、表 3 の要件項目名称は、備えるべき機能内容を読者が推測しやすいような表現としました。

表 3. セキュリティ要件項目の番号と名称

要件項目番号				要件項目名称
コンポーネント･タイプ	R	基礎的要件番号	枝番号	
C	R	1. (IAC； 識別と認証管理)	1	利用者を認証し権限を制御する
C	R		2	ソフトウェア･プロセスと機器を認証し権限を制御する
C	R		3	アカウントを管理する
C	R		4	認証子（ID）を管理する
C	R		5	認証機構を管理する
ND	R		6	無線アクセスを管理する
C	R		7	パスワード･ベース認証の強度
C	R		8	公開鍵基盤の証明書
C	R		9	公開鍵ベース認証の強度
C	R		10	認証機構からの応答
C	R		11	ログイン試行の失敗
C	R		12	システム利用であることを通知する
ND	R		13	信頼できないネットワークを介したアクセス
C	R		14	対称鍵ベース認証の強度
C	R	2. (UC； 利用管理)	1	権限制御を強制する
C	R		2	無線利用を管理する
C	R		3	携帯機器と移動機器の利用を管理する
SA	R		4	モバイルコード

ED				
HD				
ND				
C	R		5	セッションのロック
C	R		6	遠隔セッションの期限切れ
C	R		7	同時併行セッションを管理する
C	R		8	監査できるようにすべき事象
C	R		9	監査用記録のための記憶容量
C	R		10	監査用記録の不具合への対応
C	R		11	タイムスタンプ
C	R		12	否認を排除する
ED				
HD	R		13	物理的診断の利用と試験インタフェース
ND				
C	R		1	通信の完全性
SA				
ED				
HD	R		2	悪意あるコードから保護する
ND				
C	R		3	セキュリティ機能の作動を検証する
C	R		4	ソフトウェアと情報の完全性
C	R		5	入力を検証する
C	R		6	異常発生時の出力をあらかじめ指定しておける
C	R		7	エラー処理
C	R		8	通信セッションの完全性
C	R		9	監査用情報を保護する
ED		3.		
HD	R	（SI；システムの完全性）	10	更新をサポートする
ND				
ED				
HD	R		11	物理的な攻撃に耐え攻撃を検知する
ND				
ED				
HD	R		12	製品提供者の信頼原点をプロビジョニングする
ND				
ED				
HD	R		13	アセットオーナーの信頼原点をプロビジョニングする
ND				
ED				
HD	R		14	ブート・プロセスの完全性
ND				
C	R	4.	1	情報の秘密性

C	R	（DC； データの秘密性）	2	情報の持続性
C	R		3	暗号を利用する
C	R	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
ND	R		2	ゾーン境界を保護する
ND	R		3	人間から人間への汎用の通信を制限する
C	R	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
C	R		2	連続的に監視する
C	R	7. （RA； 資源の可用性）	1	DoS 攻撃から保護する
C	R		2	資源を管理する
C	R		3	システムのバックアップを採取する
C	R		4	システムを復元し再構成する
C	R		6	ネットワーク設定とセキュリティ設定を構成する
C	R		7	必要な機能だけを持つ（不要な機能を持たない）

凡例： 各行がセキュリティ要件項目に対応しています。例えば最下行は、番号が「CR 7.7」で名称が「必要な機能だけを持つ（不要な機能を持たない）」である項目を表しています。

注： CR 7.5 は欠番です。

6. セキュリティ要件項目の定義例

個々のセキュリティ要件項目がどのように定義されているかを、例として「悪意あるコードから保護する」（SAR 3.2 と EDR 3.2、HDR 3.2、NDR 3.2）を選んで、本節で紹介します。

SAR 3.2 は、コンポーネント･タイプがソフトウェア･アプリケーションである場合に関して、ICS コンポーネントに対するセキュリティ要件のうち「悪意あるコードから保護する」項目として、当該アプリケーションと不整合を起こさないような、悪意あるコードへの対策ソフトウェア等を適格として選んで文書化し、その設定についての要件を提示することを製品提供事業者に求めています。ソフトウェア･アプリケーション自身では悪意あるコードに対する対策がないとしても、その対策を担い、当該アプリケーションと共存可能な仕組みを提示することを要求しているわけです。なお、この要件項目に付随する要件拡張は存在せず、すべてのセキュリティ水準において一様な要件となっています。

EDR 3.2 は、コンポーネント･タイプが組込み機器である場合に関して、ICS コンポーネントに対するセキュリティ要件のうち「悪意あるコードから保護する」項目として、機器自身で、または、補完的な対策の導入により、悪意あるコードまたは不正なコードがインストールされ実行されることを防ぐ機能を提供することを求めています。なお、この要件項目に付随する要件拡張は存在せず、すべてのセキュリティ水準において一様な要件となっています。

HDR 3.2 は、コンポーネント･タイプがハードウェア機器である場合に関して、ICS コンポーネントに対するセキュリティ要件のうち「悪意あるコードから保護する」項目として、当該機器上で動作する、悪意あるコードへの対策ソフトウェア等を適格として選んで文書化し、その設定についての要件を提示することを製品提供事業者に求めています。また、要件拡張として、悪意あるコードへの対策ソフトウェア等の版を自動的に報告する機能を当該コンポーネントが持つことを要求しており、セキュリティ水準が 1 の場合には要件拡張を除き、

セキュリティ水準が 2 以上の場合には要件拡張を含めて、要件としています。

NDR 3.2 は、コンポーネント・タイプがネットワーク機器である場合に関して、ICS コンポーネントに対するセキュリティ要件のうち「悪意あるコードから保護する」項目として、機器自身で、または、補完的な対策の導入により、悪意あるコードに対する保護機能を備えるように求めています。なお、この要件項目に付随する要件拡張は存在せず、すべてのセキュリティ水準において一様な要件となっています。

7. まとめ

本稿では、ICS コンポーネントに対するセキュリティ要件の定義を定義している分冊 4-2 を概観しました。ICS コンポーネントを製品として提供している事業者にとっては、どのようなセキュリティ機能を製品に搭載すべきかを検討する際の参考書として、また、自社製品のセキュリティ機能を顧客に売り込む際の基準として活用できそうです。一方、ICS やそのコンポーネントを調達するアセットオーナーにとっても、システムやコンポーネントを提供する事業者との間の対話における共通基盤として本分冊で定義されたコンポーネントに対するセキュリティ要件を理解しておくことが大切です。

参考文献

[1] ISA：Component Security Assurance（CSA）Certification，https://isasecure.org/certification/iec-62443-csa-certification

[2] ISA：ISASecure Announces ISA/IEC 62443 IIoT Component Security Assurance（ICSA）Certification Launch（広報文：2022年9月1日），https://www.isa.org/news-press-releases/2022/september/isasecure-announces-isa-iec-62443-iiot-component-s

[3] JPCERT/CC：標準から学ぶ ICS セキュリティ #3 セキュリティ水準（SL），https://www.jpcert.or.jp/ics/20230420_ICSsecStandards-03.pdf