標準から学ぶ ICS セキュリティ #3

セキュリティ水準 （SL）

2023 年 4 月 20 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 で定義された独特の概念の一つにセキュリティ水準（SL： Security Level）があります。与えられたシステム（ICS）やサブシステムのセキュリティの水準を評価して、1～4 の数字（数字が大きいほど高いセキュリティ）で表現したものです。

一般的な情報システムのセキュリティの議論においても、セキュリティ対策の水準を数値的に表現する試みは「セキュリティ・メトリックス」と呼ばれ、セキュリティ対策投資の効果を説明するための指標として強いニーズがあって、古くからさまざまな試みがなされてきました。しかしながら、今もって一般的に使えて有効であると広く認められた指標化の方法論がなく、多くの実務家にとっては「欲しいけれど入手できる目途がない道具」に位置づけられていると言えそうです。

IEC 62443 のセキュリティ水準は、この難題に切り込もうと、機能安全の評価と認証のための国際標準 IEC 61508 で定義された安全度水準（SIL： Safety Integrity Level）を参考に定義されたものです。本稿では、このセキュリティ水準の考え方について論じることにしたいと思います。

2. 機能安全と安全度水準の概要

セキュリティ水準を編み出す際にお手本とされた安全度水準（SIL： Safety Integrity Level）とは、機能安全に付随する概念で、20 年近くにわたり使われてきました。公式には IEC が制定した基本安全標準 IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems （JIS C 0508 電気・電子・プログラマブル電子安全関連系の機能安全）によって定義されています。機能安全とは、安全な状態を逸脱しようとする兆候を監視し、仮に逸脱しそうになった場合に、それを回避するためのアクションをとる安全機能を付加することにより安全を確保する考え方です。温度や圧力が異常に高まった場合に爆発などの危険を伴うプラントでは、温度や圧力を監視し閾値を超えた場合にプラントを緊急停止させるための安全計装システムが ICS とともに設置されるこ

表 1.連続運転モードにおける安全度水準の定義

安全度水準	機能失敗平均確率
SIL 1	10^{-6} 以上 ～ 10^{-5} 未満
SIL 2	10^{-7} 以上 ～ 10^{-6} 未満
SIL 3	10^{-8} 以上 ～ 10^{-7} 未満
SIL 4	10^{-9} 以上 ～ 10^{-8} 未満

とがあり、機能安全の一例となっています。

機能安全においては、安全機能が必要な時に確実に動作することが期待されますが、実際には故障などにより動作しないことがあり得ます。これを機能失敗と呼びます。安全度水準とは機能失敗の平均確率がどれだけ小さく抑えられているかを SIL 1 から SIL 4 の 4 段階で表現したもので、連続運転モードに適用する場合には各 SIL に対応する機能失敗平均確率が表 1 のように定義されています。

安全度水準とは、安全が脅かされそうになった場合に、安全でなくなることを防ぐために用意した安全機能が働く確からしさの程度を示しています。つまり、例えば SIL 4 であれば、安全が脅かされそうになったとしても、それを食い止めて安全な状態にもどす安全機能において不具合を起こす確率が 1 億回に 1 回以下と極めて低いので、高い確率で安全な状態に復帰することが担保できることになります。

3. セキュリティ水準（SL）の定義

表 2.セキュリティ水準の 4 段階（SL 1～4）の定義

セキュリティ水準	定義
SL 1	ちょっとした、または偶発的な侵害行為に対する保護
SL 2	わずかな資源と通常のスキルと低い動機を持ち、単純な方法を用いた意図的な侵害行為に対する保護
SL 3	並みの資源と ICS 固有のスキルと並みの動機を持ち、高度の方法を用いた意図的な侵害行為に対する保護
SL 4	十分な資源と ICS 固有のスキルと高い動機を持ち、高度の方法を用いた意図的な侵害行為に対する保護

IEC 62443 ではセキュリティ水準をさまざまに定義しています。分冊 1-1 （2009 年版）では「ゾーンまたはコンジットのための、セキュリティ対策と、機器およびシステムの固有のセキュリティ特性の、リスクの評価から必要とされる実効性に対応する水準」としています。システムを対象とした分冊 3-2 と 3-3 や ICS コンポーネントを対象とした分冊 4-2 では「評価対象システムに脆弱性がなく意図したように機能する自信の程度」としています。また、ICS のコンポーネントのセキュリティについて定めた IEC 62443-4-2:2019 では表 2 に示した 4 段階で表現すると定めています。セキュリティ対策の軽重の程度を主観的に表現したものと言えましょう。また、セキュリティ対策がまったく施されていない状態のセキュリティ水準を便宜的に SL 0 と表すこともあります。なお、分冊 3-2 や 3-3 における「システム」は、必ずしも ICS 全体を意味していません。システムは「評価対象システム（SUC： System Under Consideration）」とも呼ばれ、「完全なソリューションを提供するために必要とされる、関連するネットワーク資産を含む、ICS 資産の定義された集まり」と定義されています。分冊 3-3 等に基づいて ISA Security Compliance Institute （ISCI）が SSA （System Security Assurance）認証として認定したシステムの一覧を調べてみると DCS 製品などが含まれており、それから「システム」の具体的なイメージを確認することができます。

ICS にせよ ICS のコンポーネントにせよ、確かに、ICS が制御している対象施設や対象プロセスの社会的な重要性や不正な動作があった場合の危険性に応じて、望まれるセキュリティ対策の手厚さにはピンからキリまでありそうです。しかしながら、表 2 のように定義されても、およそ工学的とは言えず、与えられた ICS のコンポーネントやシステムのセキュリティ水準について、万人のコンセンサスを得た判定もできません。逆に、例えば ICS の調達に際してセキュリティ水準を指定しても、表 2 の定義だけでは、調達者と納入者との間で共有されたイメージを持つことができません。また、例え ICS 固有のスキルが必要で難しい攻撃であっても、その攻撃方法がプログラミングされて攻撃ツールとして出回ることになれば、それを使って大した動機を持たない素人に近い攻撃者が、かつては SL 4 とされた ICS を難なく攻撃するようになることも十分に考えられ、普遍的な

尺度とは言えないことが明らかです。

そこで、ICS コンポーネントを対象とする場合には IEC 62443-4-2 において、ICS のシステムを対象とする場合には IEC 62443-3-3 において、基本的セキュリティ要件（FR： Foundational Requirement）を列挙し、さらに、各基本的セキュリティ要件のそれぞれについて、実施すべき複数のコンポーネント要件（CR： Component Requirement）またはシステム要件（SR： System Requirement）がセキュリティ水準ごとに指定されています。これにより、各セキュリティ水準を実現するために必要なセキュリティ対策を定めています。

表 3. ICS コンポーネントに対する基本的なセキュリティ要件

基本的 セキュリティ要件	要件により規定された機能
FR 1	人間やソフトウェア・プロセス、機器などの識別と認証管理
FR 2	認証された人間やソフトウェア・プロセス、機器への権限付与と権限順守の監視
FR 3	コンポーネントの完全性の保持
FR 4	データの秘密性の保持
FR 5	データの流れを必要な範囲に限定
FR 6	セキュリティ違反事象への迅速な対応
FR 7	アプリケーションや機器の可用性の確保
アプリケーション	ICS やプロセスにアクセスするためのアプリケーション
組込み機器	組込み機器に特有な要件
ホスト機器	ホスト機器に特有な要件
ネットワーク機器	ネットワーク機器に特有な要件

IEC 62443-4-2 が定めている ICS コンポーネントに対する基本的セキュリティ要件の一覧を表 3 に示します。これに関連して、もう少し掘り下げて、セキュリティ水準との対応付けの一例を見ておきましょう。FR 1 に含まれるコンポーネント要件の一つとして「利用者の識別と認証」が掲げられており、さらに次の 2 つの追加要件が定義されています：

> 追加要件1) すべての利用者をユニークに識別し認証できる機能をもつ
> 追加要件2) 当該コンポーネントにアクセスするすべての利用者に対して多要素認証を選べる機能をもつ

その上で、「利用者の識別と認証」の要件に関して、基本機能が実現されていれば SL 1 に、追加要件 1 を満たせば SL 2 または 3 に、追加要件 1 と 2 をともに満たせば SL 4 の対策水準にあると定めています。

セキュリティ水準の本当の定義は、ICS コンポーネントに関しては IEC 62443-4-2 で、システムとしての ICS に関しては IEC62443-3-3 で定められた要件を満足していることであって、表 2 の定義は見せかけに過ぎないように思います。「見せかけ」という意味は、定義されている要件と表 2 との対応関係の妥当性について問われても、この標準文書の作成に関わった人々の間におけるコンセンサスであったという以上の説明ができないからです。逆に言えば、セキュリティ水準とは、4 つのレベルのセキュリティ対策として、標準文書で指定された対策の実施を一律に求める、「ベースライン・アプローチ」と呼ばれるセキュリティ対策の考え方によっていると言えようかと思います。

IEC 62443 の策定が始まった 2010 年頃には、ICS を構成するコンポーネントなどについて、まったくと言ってよいほどサイバーセキュリティに対する配慮がなされていなかったことを考えると、分冊 3-3 や分冊 4-2 でセキュリティ水準ごとに伴って定められたセキュリティ対策のセットが、必要なセキュリティ対策のベースラインを示したことには大きな教育的な効果があったと考えます。ただ、ベースライン・アプローチによるセキュリティ対策は、対策に着手した段階では早期に一定の水準に達することができるなどの点において効果的ですが、ある程度まで対策が進むと、実効性や投資対効果に疑問が生ずるようになる傾向があります。例えば、定められたセキュリティ対策をすべて実施しても、実際には、新たに見つかる脆弱性や攻撃法の進化による「残留リ

スク」と呼ばれるものが存在します。しかしながら、IEC 62443 のセキュリティ水準の考え方は残留リスクの存在を想定していません。個人的な所感になりますが、セキュリティ水準については今後大きく見直される可能性を想定しておいた方が良いように思います。

4. さまざまなセキュリティ水準

セキュリティ水準の概念を、ICS コンポーネントやシステムとしての ICS だけでなく、ゾーンやコンジットなどにも適用するために、IEC 62443 では、セキュリティ水準の表 2 で示した 4 段階と直交する概念として、次の 3 つのタイプのセキュリティ水準があると説明しています。

SL-T （Target Security Level）： 目標としてのセキュリティ水準
SL-A （Achieved Security Level）： 達成できているセキュリティ水準
SL-C （Security Level Capability of Countermeasures, devices or systems）：能力としてのセキュリティ水準

前節で述べたセキュリティ水準は SL-C に当たります。SL-T と SL-A は、ゾーンとコンジットの設計時に用いられます。まず、各ゾーンとコンジットに対して、要求条件のセキュリティ水準として SL-T を割り当てます。詳細設計まで進んだ段階で、各ゾーンとコンジットがセキュリティ対策を具備することによって実現されたセキュリティ水準 SL-A を評価して、SL-A が SL-T と同等以上になっていることを確認することが想定されているようです。

しかしながら、ゾーンやコンジットの SL-T を割り当てる際には、表 2 の定義を物差しとして使わざるを得ません。また、SL-A を評価するためには、ゾーンやコンジットを構成するコンポーネントの SL-C が与えられたとしても、全体としての SL-A を決定する方法論が必要になります。そこで、複数の評価を並べた、いわばベクトル値によるセキュリティ水準の表現についても言及されていますが、それ以上の議論は見当たりません。

このような困った状況は、セキュリティ水準とリスクとの関係の概念的整理が IEC 62443 の中でまだ十分になされていないことに起因しているように思われます。IEC 62443 では「リスク」を「特定の脅威が特定の脆弱性を悪用して特定の結果が生じる確率として表現される損失の見込み」と定義していますが、ISO/IEC 27000 などに見られる定義と大きく異なっており、今後の改訂の中で見直されていく可能性が高いと考えられます。その検討の中でセキュリティ水準とリスクとの関係も整理されていくことが期待されます。

5. 安全度水準とセキュリティ水準

セキュリティ水準は安全度水準から発想を得て作られた概念であるとされています。しかしながら、これまで述べてきたように、1〜4 の 4 段階の水準を設定している点が唯一の共通点で、それ以外については発想がまったく異なっているように思います。

安全度水準は安全機能の信頼性として安全性を定義しています。これをセキュリティにそのまま移し替えれば、セキュリティ水準を「セキュリティ機能の信頼性」として定義することになりますが、実際にはそうなっていません。ちなみに、セキュリティ機能の信頼性の評価に関しては、国際標準 ISO/IEC 15408 （情報技術セキュリティの評価基準；Evaluation criteria for IT security）が存在しています。これは元になった標準の名前により「コモン・クライテリア」とも呼ばれ、米国政府が納入条件としているために、多目的プリンターやスマートカードに組み込まれたセキュリティ機能の信頼性の評価では広く利用されています。

また、安全とセキュリティはともに重要な検討分野だと思いますが、安全のコミュニティとセキュリティのコミュニティとは、これまで接点があまりなく両者が相互に理解しあった議論がなかなかできていないように危

惧されます。さらに、安全機能を実現する際にソフトウェアを使うことが当たり前になっていますので、アナログ時代の色彩を色濃く残した安全の議論だけで安全性を主張することが砂上の楼閣となりつつあります。

標準化活動でも、安全とセキュリティとの概念的な統合を目指した様々な動きが始まっています。例えば、IEC TR 63069 （Framework for functional safety and security）では、機能安全に関する標準 IEC 61508 と ICS のセキュリティに関する標準 IEC 62443 の橋渡しをしようとしています。これは、安全度水準とセキュリティ水準の橋渡しとも言えようかと思いますが、上述のように、安全度水準とセキュリティ水準との議論の土俵が対称的な関係にはないことを理解しておくことが重要だと考えます。

6. アセットオーナーにとってセキュリティ水準とは

前節までを総括すると、アセットオーナーの視点からのセキュリティ水準は 2 つの意味合いをもっています。一つは、ICS のコンポーネントなどを調達する際に、それが装備しているセキュリティ対策水準を知るための指標です。ただ、これまでのところ SSA[1]や CSA[2]のように IEC 62443 に基づいてセキュリティ認証を受けた製品は非常にわずかしかなく、さらにその大多数が SL 1 で認証を取得しています。指標として活用するためには、さまざまなセキュリティ水準で認証された製品が増えて、その中からアセットオーナーが選べるようになる日を待つ必要がありそうです。なお、ICS のコンポーネントのセキュリティ評価の方法については分冊 6-2 を策定する準備も進められているようです。

アセットオーナーにとってのセキュリティ水準のもう一つの意味合いは、ICS のゾーンとコンジットの設計を進める際や妥当性を検証する際における技術的なガイドとしての期待です。ただ本格的にセキュリティ水準を利用して、ゾーンやコンジットの設計や検証をするためには、セキュリティ水準とリスクの考え方がさらに整理された IEC 62443 の改訂版の登場を待たざるを得ません。それまでは独自に工夫したアプローチによらざるを得ません。裏返せば、そうした試みの中で見つかった成功例を形式化し標準として提案することが期待されていると言えましょう。

7. まとめ

IEC 62443 シリーズ標準の全体を通じた重要概念の一つであるセキュリティ水準について述べましたが、筆者自身もすっきりしない後味が残っています。そこで基本に立ち返ろうと、セキュリティ水準を論じる前提となるセキュリティの定義を改めて読み返してみると、次のようになっていました（IEC 62443-1-1:2009 3.2.99 を邦訳）。

a） システムを守るために取られる対策
b） システムを守るための対策の確立および維持による結果として生じるシステムの状態
c） 権限のないアクセスや、権限のない偶発的な変更や破壊あるいは損失がないようなシステム資源の状態
d） 権限のない人やシステムは、ソフトウェアとそのデータを変更することもシステム機能へアクセスすることもできないという十分な確信を与え、かつ、権限のある人やシステムは、ソフトウェアとそのデータの変更もシステム機能へのアクセスも拒絶されることがないことを保証するためのコンピューター・ベースのシステムの能力
e） 本来の意図した ICS の運用のインターフェース、または ICS 自体への違法または意図しない侵入の防止

この定義は次の改定で大きく見直されることになっているようですが、ISO/IEC 27000 （情報セキュリティ管理システム － 概要と語彙）における「情報の機密性と完全性と可用性の保全」という実に簡明な「情報セキュ

リティ」の定義と比べると、長さと分かりにくさが目立つように感じられます。さらに気になるのは、セキュリティ対策をセキュリティと考えている、すなわち、目的と手段との混同であり、この影響が IEC 62443 シリーズのさまざまな所に及んでいるように思います。結局は「『セキュリティ水準』とは、『セキュアさの程度』ではなく、『標準が指定したセキュリティ対策の装備状況』がである」と当面は理解しておくべきかも知れません。なお、策定中の分冊 2-2 では、セキュリティ水準に ICS の運用状況を加味したメトリックスとして「セキュリティ保護水準」の概念を定義しようとしています。今後の議論の推移と分冊の発行に注目したいと思います。

一方で、IEC 62443 シリーズ標準の開発開始後に蓄積された知見をキャッチアップするとともに、ISO/IEC 27000 シリーズとの整合性を高める方針の下に、IEC 62443 シリーズ全体の改訂が衆知を集めて進められています。その中でセキュリティ水準の概念の見直しに向けた議論が始まることを期待し、新しい時代に向けたセキュリティ水準への進化を見守ることにしたいと思います。

参考文献

[1] ISA Secure：System Security Assurance （SSA） Certification
https://isasecure.org/certification/iec-62443-ssa-certification
[2] ISA Secure：Component Security Assurance （CSA）
https://isasecure.org/certification/iec-62443-csa-certification