OT セキュリティに関する
国内外の主要ガイドラインの調査報告書

2026/06/30

NPO 法人 日本ネットワークセキュリティ協会
調査研究部会 OT セキュリティワーキンググループ
サブワーキンググループ 2

目次

1. 概要

本資料は、経済産業省「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」（以下「工場セキュリティガイドライン」を略称として使用する場合がある）を基軸として、国内外の主要な OT セキュリティ関連ガイドライン、標準、手引書等を比較整理したものである。製造業における DX の進展や IT/OT 接続の拡大に伴い、工場システムに求められるセキュリティ対策は高度化・複雑化している。一方で、関連文書は多数存在し、それぞれ対象、記載内容、活用場面が異なるため、実務において参照すべき文書を判断することは容易ではない。そこで本資料では、工場セキュリティガイドラインを基準として、各文書の特徴、適用範囲、相互関係を整理し、組織の状況や目的に応じた文書の選択及び活用に資する基礎資料となることを目指した。主な利用者としては、工場セキュリティに取り組む実務担当者のほか、経営層、業界関係者、ベンダー等を想定している。

2. 調査の背景と目的

2.1. 背景

本資料は、経済産業省「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」を基軸として、国内外の主要な OT セキュリティ関連文書を比較整理したものである。製造業においては、DX の進展、IoT 機器の活用拡大、遠隔保守の普及等により、工場システムと IT システムの接続が進展しており、従来は閉域的に運用されることの多かった制御環境についても、外部接続やデータ連携を前提としたセキュリティ対策が求められている。工場システムにおけるセキュリティ上の問題は、情報資産の漏えいにとどまらず、生産停止、品質低下、設備への影響等を通じて事業継続に影響を及ぼす可能性があるため、IT とは異なる観点を含めた対応が必要である。

一方で、OT セキュリティに関するガイドライン、標準、手引書等は国内外に多数存在し、それぞれ対象業界、想定読者、記載内容、扱う領域等が異なる。そのため、実務担当者が自組織にとってどの文書を基準とし、どの文書を補完的に参照すべきかを判断することは容易ではない。特に、工場セキュリティに取り組む現場では、どのガイドラインを参照すべきか、自社が参照している文書だけで十分か、他の文書とどのような関係にあるのかといった疑問が生じやすい。このような状況を踏まえ、工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインを基軸として、関連する主要文書の特徴、位置付け及び補完関係を整理することを目的として作成したものである。

2.2. 目的

本調査の目的は、工場セキュリティガイドラインを基軸として、国内外の主要な OT セキュリティ関連文書の特徴、適用範囲、位置付け及び活用場面を整理し、利用者が自組織の状況や目的に応じて参照すべき文書を判断しやすくすることにある。
具体的には、第一に、OT セキュリティに関する主要なガイドライン、標準、手引書等を収集し、それぞれの発行主体、対象読者、対象領域及び文書の性格を整理する。第二に、工場セキュリティガイドラインとの比較を通じて、各文書が強みを持つ領域や、補完的に活用し得る場面を明らかにする。第三に、OT セキュリティに取り組む実務担当者、経営層、業界団体、ベンダー等が、目的に応じて参照先を選択しやすくなるよう、文書間の関係性を分かりやすく示す。

本調査は、個々の文書の優劣を単純に示すことを目的とするものではない。各文書の立場や役割の違いを踏まえ、OT セキュリティの実務において、どのように使い分け、どのように組み

合わせて参照すべきかを整理することに主眼がある。これにより、利用者が自組織に適した文書を選定し、不足する観点を必要に応じて他文書で補完するための基礎資料とすることを目指す。

3. 調査方法

3.1. 調査対象

本調査では、工場セキュリティガイドラインを基軸として、OT セキュリティに関する国内外のガイドライン、標準、手引書等を調査対象とした。対象文書の抽出にあたっては、工場セキュリティに関連する文書を幅広く収集した上で、OT との関連性、公開情報としての参照可能性、内容の重複の有無等を踏まえて整理を行い、上記ガイドライン含め以下を対象としている。

1. 工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン
2. 自工会/部工会 サイバーセキュリティ・ガイドライン
3. 制御システムのセキュリティリスク分析ガイド
4. 制御システム セーフティセキュリティ要件検討ガイド
5. 制御システム利用者のための脆弱性対応ガイド
6. 産業用制御システム向け侵入検知製品等の導入手引書
7. ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン
8. 物流分野における情報セキュリティ確保に係る安全ガイドライン（倉庫）
9. 物流分野における情報セキュリティ確保に係る安全ガイドライン（貨物自動車運送）
10. 制御システムにおける資産管理ガイドライン
11. 自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン
12. IEC 62443-2-1
13. IEC 62443-3-2
14. IEC 62443-3-3
15. NIST SP800-82
16. グッド・プラクティス・ガイド プロセス制御と SCADA セキュリティ
17. Principles of operational technology cybersecurity
18. Mitigating the Impacts of Doxing on Critical Infrastructure
19. Design principles and Operational Technology
20. Security Tenets for Life Critical Embedded Systems

3.2. 評価方法

評価にあたって、各文書の特徴や対象等を整理し、工場セキュリティガイドラインを基準として、各文書との関係を整理した。具体的には、各対象文書の対象業界、対象読者、チェックリストの有無等の基礎情報を整理するとともに、工場セキュリティガイドラインを基軸として、特化度、専門度を評価し、文書の性質等の観点から、工場セキュリティガイドラインに記載のチェックリストの各カテゴリへの対応状況を把握した。これにより、各文書の特徴や適用範囲を俯瞰できるよう整理を行った。
この評価は、各文書の優劣を示すことを目的とするものではなく、工場セキュリティガイドラインを基準とした場合に、どの文書がどの領域を補完し得るかを把握するために実施した。

4. 調査結果

本章では、各ガイドラインの比較結果について、主な傾向及び要点を整理して示す。なお、各文書の個別評価結果、対応状況の詳細及びマッピングに用いた整理内容については、別紙に整理しているため、適宜そちらを参照されたい。

4.1. 対象文書の傾向

本調査の対象文書を比較した結果、OT セキュリティ関連のガイドラインは、その特徴(特化度、専門度)に応じて、包括型ガイドライン、特化型ガイドライン、業界特化型ガイドライン及び原則提示型ガイドラインに大別できると整理した。各類型は、対象とする領域、記載の深さ、想定される活用場面が異なっており、OT セキュリティに取り組む組織においては、目的や状況に応じて参照先を使い分けることが重要である。

■ **包括型ガイドライン**

該当する対象文書
• 工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン • IEC 62443-2-1 • NIST SP800-82
主な特徴
• 組織的対策から運用的対策、技術的対策まで広範な領域を扱う • 工場セキュリティの全体像を把握するための基準文書として位置付けやすい
想定される活用先
• 工場セキュリティに初めて体系的に取り組む組織 • 全体方針を整理したい組織

■ 特化型ガイドライン

該当する対象文書
• 制御システムにおける資産管理ガイドライン • 制御システムのセキュリティリスク分析ガイド • 産業用制御システム向け侵入検知製品等の導入手引書 • 制御システム セーフティセキュリティ要件検討ガイド
主な特徴
• 資産管理、リスク分析、監視、要件検討等の特定領域を重点的に扱う • 包括型ガイドラインを補完しつつ、個別テーマを深掘りする際に有効である
想定される活用先
• 基本的な対策方針を整理した上で、個別領域の具体化や高度化を図りたい組織

■ 業界特化型ガイドライン

該当する対象文書
• 自工会/部工会 サイバーセキュリティ・ガイドライン • 自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン • 物流分野における情報セキュリティ確保に係る安全ガイドライン（倉庫） • 物流分野における情報セキュリティ確保に係る安全ガイドライン（貨物自動車運送）
主な特徴
• 各業界に固有の要件やシステム特性、運用実態を踏まえた内容を有する • 対象業界における実務への適用を意識した文書である
想定される活用先
• 業界内での共通理解の形成、業界ガイドラインの参照・見直し、サプライチェーン全体での活用

■ 原則提示型ガイドライン

該当する対象文書
• Principles of operational technology cybersecurity • Design principles and Operational Technology • Security Tenets for Life Critical Embedded Systems
主な特徴
• 個別要件や詳細手順を網羅的に示すというより、基本原則やベストプラクティスを提示する性格が強い
想定される活用先
• 全体方針の策定、設計思想の確認、他文書を参照する際の考え方の補強

以上のとおり、各ガイドラインは同一の役割を持つものではなく、包括型ガイドラインを基軸としつつ、必要に応じて特化型、業界特化型、原則提示型の文書を補完的に参照することが有効であると整理した。

4.2. 工場セキュリティガイドラインとの比較結果

工場セキュリティガイドラインを基準として各対象文書を比較した結果、複数のガイドラインに共通して比較的詳細に記載されている領域が見られた。これらの領域は、組織的対策、運用的対策及び技術的対策の基盤となる項目であり、工場セキュリティに限らず、国内外の文書において共通して重視される傾向が見られた。以下に、対応度の高い主な領域を示す。

表 1 対応度の高い領域（多くのガイドラインで詳細に記載されていた項目）

主な領域	傾向	補足
組織的対策	多くのガイドラインで記載あり	体制構築、ポリシー策定、役割明確化等
ネットワークセグメンテーション	多くのガイドラインで詳細記載	ゾーニング、VLAN 分割等
アクセス制御・認証	多くのガイドラインで詳細記載	多要素認証、アカウント管理等
ログ管理	多くのガイドラインで詳細記載	記録、保管、分析等
脆弱性管理	多くのガイドラインで記載あり	パッチ適用、代替策等
物理セキュリティ	多くのガイドラインで記載あり	入退室管理、監視等

一方で、工場セキュリティガイドラインに記載されている項目の中には、他の対象文書では相対的に記載が少ない領域も確認された。特に、工場特有の運用実態や現場対応に密接に関わる項目、又は実施条件や具体的基準に踏み込む項目については、文書間で記載の有無や粒度に差が見られた。以下に、対応度の低い主な領域を示す。

表 2 対応度の低い領域（多くのガイドラインで詳細に記載されていなかった項目）

主な領域	傾向	補足
工場システム特有の運用ルール	相対的に記載が少ない	メンテナンス期間外の機器接続等の異常検知、安全に関わる緊急対応端末の扱い等

主な領域	傾向	補足
具体的な実施タイミング	相対的に記載が少ない	契約開始時の教育実施、協力会社向け教育の定期実施等
定量的な基準	相対的に記載が少ない	ログ保存期間、パスワード強度要件等
代替策の詳細	相対的に記載が少ない	インストール不可能な端末でのマルウェア対策等

これらの領域は、一般的な管理策や技術対策に比べて、個別の業務運用、設備条件、組織体制又は現場の実態に左右されやすい項目である。そのため、他のガイドラインでは抽象的な原則提示にとどまる場合があり、工場セキュリティガイドラインに示された具体的観点を補完的に参照する意義が大きいと考えられる。

工場セキュリティガイドラインとの比較結果をカテゴリ別に整理すると、領域ごとに記載の具体性や充実度に一定の傾向が見られた。全体としては、運用的対策及び技術的対策では比較的高い対応度が見られた一方、準備、組織的対策及びサプライチェーン管理では、重要性に関する記載は見られるものの、実施方法や運用条件まで踏み込んだ記載は相対的に限定的であった。以下に、カテゴリ別の対応状況を示す。

表 3 工場セキュリティガイドラインのチェックリストのカテゴリへの対応状況

主な領域	対応度	傾向	補足
準備（組織的対策）	中～高	経営層の関与、体制構築は多くの文書で記載	BCP 策定は一部記載に留まる
組織的対策	中～高	ポリシー策定、異常発生時の対応は比較的充実	教育・訓練の実施方法は限定的
運用的対策	高	パスワード管理、バックアップ、マルウェア対策は詳細記載が多い	実施方法に踏み込む記載も多い
技術的対策	高	ネットワーク分割、アクセス制御、ログ管理は詳細記載が多い	共通的に重視される傾向
サプライチェーン管理	中	ベンダー連携や教育の重要性は記載あり	具体策や実施条件は限定的

以上の結果から、工場セキュリティガイドラインとの比較においては、運用的対策及び技術的対策に関する項目では比較的共通した記載が多く確認された一方、準備、組織的対策及びサプライチェーン管理に関する項目では、記載内容の具体性や実務への落とし込みに差が見られた。このことから、工場セキュリティの実務においては、汎用的な管理策については複数の文書を相互参照しやすい一方、工場特有の運用条件や関係者管理に関する項目については、工場セキュリティガイドラインを基準として補完的に参照することが有効であると考えられる。

4.3. 各ガイドラインの関係性の整理（マッピング）

各ガイドラインの特徴を俯瞰的に比較するため、対象領域の絞り込みの程度を示す「特化度」と、記載内容の深さを示す「専門度」をそれぞれ評価し、バブルグラフとしてマッピングした結果を図 1 に示す。なお、各円の大きさは文書のページ数を表している。

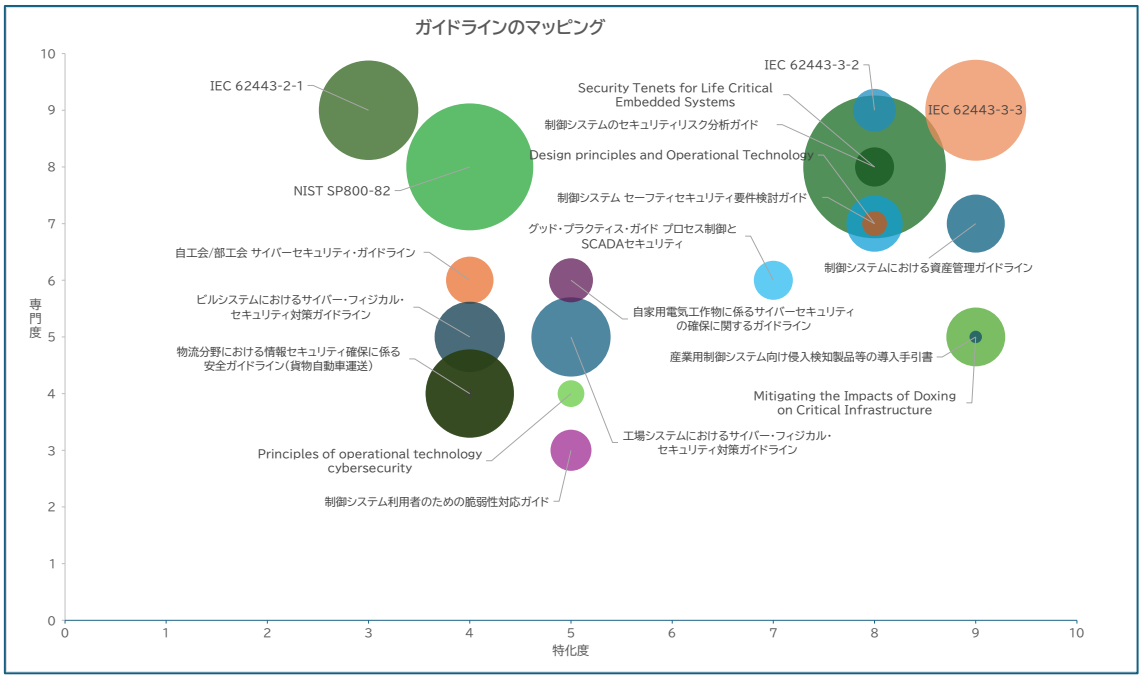

図 1 各ガイドラインのマッピング

本図は、各文書の優劣を示すことを目的とするものではなく、文書ごとの位置付けや性格の違いを視覚的に把握するために整理したものである。これにより、包括的に参照すべき文書、特定領域を深掘りする文書、又は業界やテーマに応じて補完的に参照すべき文書の傾向を俯瞰的に把握できる。

5. ユースケース

本資料は、工場セキュリティに取り組む実務担当者に加え、自社の対応状況を俯瞰したい経営層、顧客提案を行うベンダー担当者、業界ガイドラインの策定又は改定を担当する関係者等が活用することを想定している。以下に、主な利用者ごとの活用場面をユースケースとして示す。

■ ユースケース 1

項目	内容
想定利用者	工場セキュリティを担当する実務担当者
課題	• 関連ガイドラインが多数存在し、どの文書を参照すべきか判断しにくい。 • 自社が属する業界のガイドラインだけで十分かどうか判断しにくい。
活用例	• 本資料を用いて、自社が属する業界のガイドラインと工場セキュリティガイドラインとの関係を整理し、不足し得る観点を確認する。 • 必要に応じて、工場セキュリティガイドラインや他の関連文書を補完的に参照し、自社工場に適した対応基準の整理に活用する。

■ ユースケース 2

項目	内容
想定利用者	自社工場のセキュリティ対応状況を把握したい経営層
課題	• 現場が参照している業界ガイドラインだけで対応として十分かどうか判断しにくい。 • 他社や他文書との比較の中で、自社の対応状況を客観的に把握しにくい。
活用例	• 本資料を参考に、自社が参照しているガイドラインの位置付けや不足し得る観点を確認する。 • 工場セキュリティガイドラインとの比較結果を踏まえ、改善が必要な項目の把握や現場への指示の参考とする。

■ ユースケース 3

項目	内容
想定利用者	工場セキュリティを提案するベンダー担当者
課題	• 業界ごとに参照されるガイドラインが異なり、全体像を把握しにくい。 • 限られた時間の中で、顧客に適した提案観点を整理することが難しい。
活用例	• 本資料を用いて、各業界で参照される主なガイドライン及び重視される観点を把握する。 • 複数のガイドラインに共通する項目や補完が必要な観点を整理し、提案内容の検討に活用する。

■ ユースケース 4

項目	内容
想定利用者	業界ガイドラインの策定又は改定を担当する関係者
課題	• 既存ガイドラインの見直しにあたり、他の主要文書との関係や不足観点を把握する必要がある。 • 自団体のガイドラインが、工場セキュリティに必要な観点を十分に含んでいるか判断しにくい。
活用例	• 本資料を用いて、他の主要ガイドラインとの比較を行い、自団体文書に不足し得る観点を確認する。 • 共通して重視されている項目や補強が必要な項目を整理し、ガイドラインの改定検討に活用する。

以上のとおり、本資料は、工場セキュリティに関わる多様な立場の利用者が、目的に応じて参照すべき文書を判断し、不足する観点を補完するための基礎資料として活用できる。

6. まとめ

本調査では、工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインを基軸として、国内外の主要な OT セキュリティ関連ガイドライン、標準、手引書等を比較整理した。その結果、各文書は同一の役割を持つものではなく、包括的に全体像を示す文書、特定領域を深掘りする文書、業界固有の要件を反映した文書、及び原則や考え方を提示する文書に大別できると整理した。

また、工場セキュリティガイドラインとの比較を通じて、組織的対策、ネットワーク分割、アクセス制御、ログ管理、脆弱性管理、物理セキュリティ等の領域については、多くの文書で比較的共通した記載が見られた。一方で、工場特有の運用ルール、具体的な実施タイミング、定量的な基準、代替策の詳細等については、相対的に記載が少ない傾向が見られた。さらに、カテゴリ別に見ると、運用的対策及び技術的対策は比較的対応度が高い一方、準備、組織的対策及びサプライチェーン管理では、記載の具体性に差が見られた。

以上の結果から、工場セキュリティに関する実務においては、工場セキュリティガイドラインを基準としつつ、目的や状況に応じて他の文書を補完的に参照することが有用であると考えられる。特に、汎用的な管理策及び技術的対策に関する領域については、多くの文書で共通して扱われている一方、工場固有の運用条件や現場実装に関わる項目については、工場セキュリティガイドラインを基準として参照する意義が大きい。

本資料は、各文書の優劣を示すものではなく、それぞれの特徴、位置付け及び補完関係を整理することで、工場セキュリティに取り組む利用者が、自組織の状況や目的に応じて参照先を検討する際の基礎資料となることを目指すものである。

7. 付録

7.1. 調査対象のガイドライン

調査対象とした文書は以下表のとおりである。

表 4 調査対象文書一覧

No.	文書名	発行主体	発行年	URL
1	工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン	経済産業省	2025	https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html
2	自工会/部工会 サイバーセキュリティ・ガイドライン	一般社団法人 日本自動車工業会／一般社団法人 日本自動車部品工業会	2024	https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html
3	制御システムのセキュリティリスク分析ガイド	独立行政法人 情報処理推進機構	2023	https://www.ipa.go.jp/security/controlsystem/riskanalysis.html
4	制御システム セーフティセキュリティ要件検討ガイド	独立行政法人 情報処理推進機構	2018	https://www.ipa.go.jp/archive/digital/iot-en-ci/mieruka/20180319.html
5	制御システム利用者のための脆弱性対応ガイド	独立行政法人 情報処理推進機構	2017	https://www.ipa.go.jp/security/guide/vuln/ug65p90000019by0-att/000058489.pdf
6	産業用制御システム向け侵入検知製品等の導入手引書	独立行政法人 情報処理推進機構	2023	https://www.ipa.go.jp/security/controlsystem/icsidshandbook.html
7	ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン	経済産業省	2023	https://www.meti.go.jp/policy/netsecurity/wg1/building_guideline.html
8	物流分野(倉庫)における情報セキュリティ確保に係る安全ガイドライン	国土交通省	2024	https://www.mlit.go.jp/jidosha/jidosha_tk4_000121.html
9	物流分野(貨物自動車運送)における情報セキュ	国土交通省	2024	https://www.mlit.go.jp/jidosha/jidosha_tk4_000121.html

No.	文書名	発行主体	発行年	URL
	リティ確保に係る安全ガイドライン			
10	制御システムにおける資産管理ガイドライン	独立行政法人 情報処理推進機構	2020	https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2020/assetmanagement.html
11	自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン	経済産業省	2023	https://www.meti.go.jp/policy/safety_security/industrial_safety/law/files/jikayouguideline.pdf
12	IEC 62443-2-1	International Electrotechnical Commission	2024	https://webstore.iec.ch/en/publication/62883
13	IEC 62443-3-2	International Electrotechnical Commission	2020	https://webstore.iec.ch/en/publication/30727
14	IEC 62443-3-3	International Electrotechnical Commission	2014	https://webstore.iec.ch/en/publication/7033
15	NIST SP800-82	National Institute of Standards and Technology	2023	https://csrc.nist.gov/pubs/sp/800/82/r3/final
16	グッド・プラクティス・ガイド プロセス制御と SCADA セキュリティ	Centre for the Protection of National Infrastructure	2005	https://www.jpcert.or.jp/research/2007/GoodPractice-for-ProcessControl-and-SCADA-Security.pdf
17	Principles of operational technology cybersecurity	Australian Cyber Security Centre	2024	https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/critical-infrastructure/principles-operational-technology-cybersecurity
18	Mitigating the Impacts of Doxing on	Cybersecurity and Infrastructur	2021	https://www.cisa.gov/resources-tools/resources/cisa-ins

No.	文書名	発行主体	発行年	URL
	Critical Infrastructure	e Security Agency		ights-mitigating-impacts-doxing-critical-infrastructure
19	Design principles and Operational Technology	National Cyber Security Centre	2020	https://www.ncsc.gov.uk/collection/cyber-security-design-principles/examples/study-operational-tech
20	Security Tenets for Life Critical Embedded Systems	Cybersecurity and Infrastructure Security Agency	2020	https://www.cisa.gov/resources-tools/resources/security-tenets-life-critical-embedded-systems

7.2. 作成メンバー

本資料の作成に参加したメンバーは以下のとおりである。

リーダー

桑田 雅彦（NEC セキュリティ株式会社）
西園 健吾
髙橋 弘宰（フォーティネットジャパン合同会社）
今野 尊之（TXOne Networks Japan 合同会社）
堰根 哲平（株式会社 NTT データ）
石田 晃規（EY 新日本有限責任監査法人）

アドバイザー

江﨑 浩（東京大学）
佐々木 弘志（フォーティネットジャパン合同会社）
藤原 健太（フォーティネットジャパン合同会社）

メンバー

安陪 啓史（三菱電機株式会社）
飯島 安恵（アクセリア株式会社）
上田 高寛（NTT ドコモビジネス株式会社）
大窪 陵介（パーソルクロステクノロジー株式会社）
大林 克成（NEC セキュリティ株式会社）
緒方 日佐男（一般社団法人 重要生活機器連携セキュリティ協議会
／日立チャネルソリューションズ株式会社）
小川 陽平（NEC セキュリティ株式会社）
河島 君知（株式会社 NTT データ先端技術）
岸 和彦
佐藤 良（ニプロファーマ株式会社）
島村 圭（株式会社日立ソリューションズ）
下元 由子
菅野 直樹（株式会社さくらケーシーエス）
芹川 正孝（オムロン デジタル株式会社）
西村 克治（パロアルトネットワークス株式会社）
松田 和博（パーソルクロステクノロジー株式会社）
村田 哲彦（NTT ドコモビジネス株式会社）

7.3. 変更履歴

Version	日付	内容
1.0	2026/06/30	初版公開

