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

Copyright 2026 NPO 日本ネットワークセキュリティ協会

目次

1. 概要 1
2. 調査の背景と目的 2
2.1. 背景 2
2.2. 目的 2
3. 調査方法 3
3.1. 調査対象 3
3.2. 評価方法 4
4. 調査結果 4
4.1. 対象文書の傾向 4
4.2. 工場セキュリティガイドラインとの比較結果 6
4.3. 各ガイドラインの関係性の整理（マッピング） 8
5. ユースケース 9
6. まとめ 11
7. 付録 12
7.1. 調査対象のガイドライン 12
7.2. 作成メンバー 15
7.3. 変更履歴 16

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。

Copyright 2026 NPO 日本ネットワークセキュリティ協会

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

Copyright 2026 NPO 日本ネットワークセキュリティ協会

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

Copyright 2026 NPO 日本ネットワークセキュリティ協会

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

Copyright 2026 NPO 日本ネットワークセキュリティ協会

■ 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

Copyright 2026 NPO 日本ネットワークセキュリティ協会

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

Copyright 2026 NPO 日本ネットワークセキュリティ協会

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

Copyright 2026 NPO 日本ネットワークセキュリティ協会

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。

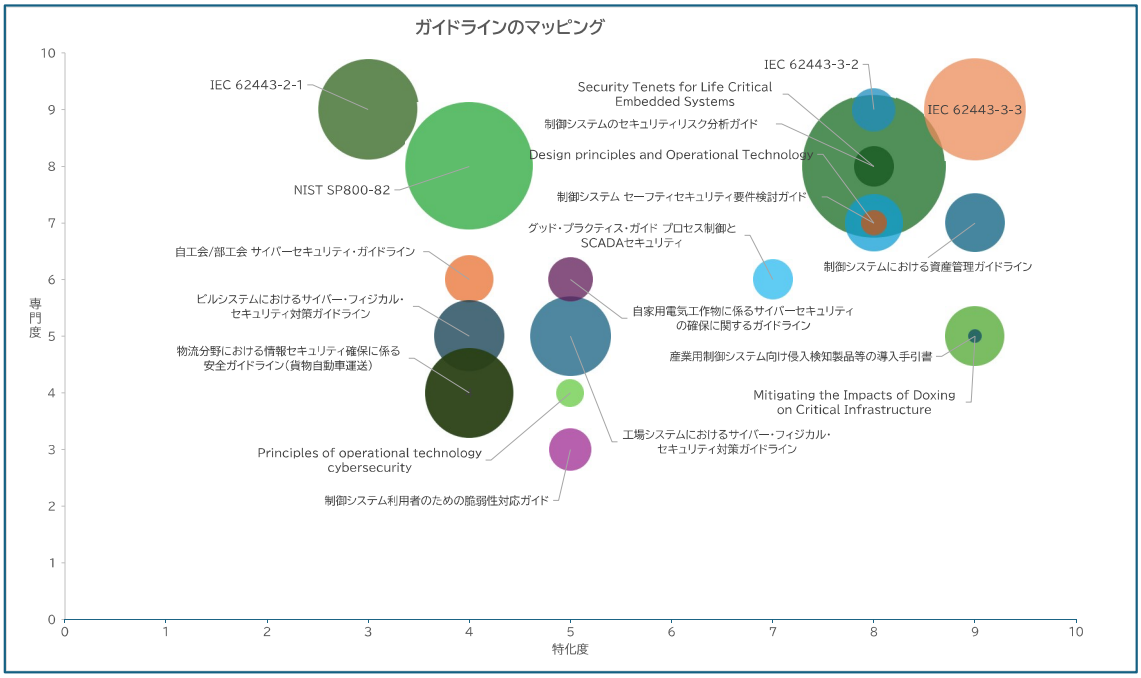


図 1 各ガイドラインのマッピング

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。

Copyright 2026 NPO 日本ネットワークセキュリティ協会

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。

Copyright 2026 NPO 日本ネットワークセキュリティ協会

■ 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。

Copyright 2026 NPO 日本ネットワークセキュリティ協会

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。

Copyright 2026 NPO 日本ネットワークセキュリティ協会

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

Copyright 2026 NPO 日本ネットワークセキュリティ協会

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

Copyright 2026 NPO 日本ネットワークセキュリティ協会

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

Copyright 2026 NPO 日本ネットワークセキュリティ協会

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）

Copyright 2026 NPO 日本ネットワークセキュリティ協会

7.3. 変更履歴

Version	日付	内容
1.0	2026/06/30	初版公開

Copyright 2026 NPO 日本ネットワークセキュリティ協会

別紙1 対象ガイドラインの整理

No.	文書名	概要	発行年月	国内/国際区分	発行者・組織	対象業界	対象業種	対象読者	技術系/管理系分野	チェックリスト有無	ガイドラインURL	工場セキュリティGLとの関連性	備考
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	工場システムのセキュリティ対策を実施する上で、業界団体や企業が自ら対策を企画・実行するに当たり、参照すべき考え方やステップを「手引き」として示している。 また、必要最小限と考えられる対策事項として、脅威に対する技術的な対策から運用・管理面の対策までを明記している。 構成は、1章にてガイドラインの目的や適用範囲を示し、2章にて保護対象として想定する工場を例示し、3章にてセキュリティ対策の企画・導入の進め方を3ステップに分け説明している。 付録にて、関連する基準や工場セキュリティ対策のチェックリスト等、読者の参考になると考えられる情報を掲載している。 別冊として、工場のスマート化を進める上でのセキュリティ対策のポイントや、中小企業向けに工場セキュリティの重要性と始め方を説く文書も提供している。	初版(Ver 1.0):2022年11月、 第二版(Ver 1.1):2025年4月	国内	経済産業省 産業サイバーセキュリティ研究会 ワーキンググループ1 (制度・技術・標準化) 工場サブワーキンググループ	製造業全般	製造業	・IT関係部門(情報システム部門、セキュリティ部門 等)、 ・生産関係部門(生産技術部門、生産管理部門、工作部門 等)、 ・戦略マネジメント部門(経営企画等)、 ・監査部門、 ・リスク管理部門、 ・機器システム提供ベンダ、機器メーカ(サプライチェーンを構成する調達先を含む)	技術系/管理系	有	https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html	工場セキュリティGL自体	
2	自工会/部工会 サイバーセキュリティ・ガイドライン	日本自動車工業会(JAMA)と日本自動車部品工業会(JAPIA)が共同で策定したものであり、自動車産業全体のサイバーセキュリティ強化を目的としている。サプライチェーン全体を対象とし、中小企業も活用可能な内容である。 CASEなどの技術革新により IT 活用が進む自動車産業では、サプライチェーンを狙ったサイバー攻撃が深刻化している。固文省や経産省の制度対応を踏まえ、業界共通の対策・自己評価基準を示し、セキュリティレベル向上を図ることを目的とする。 本ガイドラインは、対象範囲・構成・活用方法・要求事項・用語集で構成されている。OA環境を中心に、Lv1～Lv3の達成条件を設定した対策項目を整理し、付録のチェックシートにより自己評価が可能。教育や社内のセキュリティ評価にも活用できる。	初版:2020年3月 第2.2版:2024年8月	国内	一般社団法人 日本自動車工業会(JAMA) 一般社団法人 日本自動車部品工業会(JAPIA)	自動車産業	・完成車メーカー(OEM) ・自動車部品メーカー ・電装品・電子機器メーカー ・ソフトウエア・システム開発会社(車載系・製造系) ・物流・倉庫業(自動車部品の輸送・保管) ・設備・装置メーカー(工場向け) ・ITサービス・クラウド事業者(自動車関連企業向け) ・その他、自動車産業のサプライチェーンに関わる企業	・CISO(最高情報セキュリティ責任者) ・リスク管理部門 ・監査部門 ・セキュリティ対応部門 ・情報システムの開発・運用部門 ・データマネジメント部門 ・購買・調達部門(サプライチェーン管理) ・人事・法務・総務などのセキュリティ関連部門	技術系と管理系の両方の要素を含むハイブリッド型	有	https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html	自工会/部工会 サイバーセキュリティ・ガイドラインは、企業全体の情報セキュリティ体制やサプライチェーン管理を対象とし、「エンタープライズIT」に重点を置いた内容である。 一方、工場セキュリティGLは工場の制御系システムや生産設備に特化した内容である。 これら両者を組み合わせることにより、企業全体(IT)と現場(OT)のセキュリティを統合的に管理する「サイバー・フィジカル・セキュリティ」の実現が可能となる。	■ベンチマークにした外部基準 ・経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク」 ・NIST Cybersecurity Framework v1.1 ・ISO/IEC 27001 ・AIAG Cyber Security 3rd Party Information Security ・IPA「中小企業の情報セキュリティ対策ガイドライン」
3	制御システムのセキュリティリスク分析ガイド	独立行政法人情報処理推進機構(IPA)は、2023年3月に「制御システムのセキュリティリスク分析ガイド 第2版」を公開しました。このガイドは、制御システムのセキュリティリスクを事業者自身が体系的に分析できるよう支援することを目的としています。 本ガイドでは、「資産ベースのリスク分析」と「事業被害ベースのリスク分析」の2手法を提示しており、いずれも独立して使用可能ですが、併用により補完的な分析が可能です。分析工数への配慮として、資産のグループ化や攻撃経路の絞り込み方法も示されています。 支援ツールとしてExcel形式の分析シート、脅威・対策項目の対応関係表、各種チェックリスト(脆弱性、内部不正対策等)が提供されており、分析結果はIEC 62443に準拠した認証制度や適合性評価制度と連携可能です。企業のセキュリティ整備強化に技術的根拠として活用できます。	初版:2017年10月 第二版:2023年3月	国内	独立行政法人 情報処理推進機構(IPA) セキュリティセンター	重要インフラ分野全般	電力 交通 石油 化学など	・設備所有者・運営者(工場などのオーナ企業) ・エンジニアリング企業(プラント建設など) ・設計事務所・コンサルタント(制御系設計など) ・制御機器メーカー・ベンダ ・制御システムの運用・保守会社 ・情報セキュリティ部門 ・テナント・ユーザー部門 ・サービス・クラウドプロバイダ ・セキュリティ・ネットワークベンダ ・行政機関・業界団体	管理系 (但し、一部技術的な評価基準はあり)	有	https://www.ipa.go.jp/security/controlsystem/riskanalysis.html	補完関係 本ガイドにてリスク分析手法を提供	
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	制御システムの設計・開発・運用に携わる開発者が、検討すべき「安全性を確保しつつ、セキュリティ対策を講じるための検討ポイント」を整理し、その検討手順を具体的に示している。 制御システムに関わる事業者やインテグレータが、システムのライフサイクルを通じて、セーフティを確保しながら制御システムのセキュリティ検討を行う際に参考となる「セキュリティ検討の基本的な考え方・手順」を確認できる。 本編に加え、脅威分析を実施する際の分析シートのテンプレートおよびケーススタディも発行されている。	2018年3月19日発行	国内	独立行政法人情報処理推進機構 技術本部 ソフトウェア高信頼化センター	制御システムを運用する分野全般	・電力、鉄道など、重要インフラ設備を持つ事業者 ・ビル管理等、施設監視用で制御システムを持つ事業者 ・医療情報システムを運用するヘルスケア領域の事業者 ・産業ロボットを運用する製造業	・中堅レベルのセーフティ開発の経験・スキルを持つインテグレータ ・セーフティシステムを含む重要インフラを保有する事業者 ・工場並びに生産設備システムの構築・運用の関係者として、事業者、 システムインテグレータ、機器メーカを想定	技術系	無し	https://www.ipa.go.jp/archive/digital/iot-enci/mieruka/20180319.html	工場だけではなく、ビル、ヘルスケア領域など 制御システムを運用する事業者全般を対象としている。	電力、鉄道など各システムの概要を示している点が各業種の一般的なシステムを理解するために有用と考えられる。
5	制御システム利用者のための脆弱性対応ガイド	このガイドは、工場やプラントなどで使用される制御システムに対するセキュリティリスクへの対応を目的として作成された もので、企業の経営層や管理者が取るべき対策や留意点を解説しています。制御システムの脆弱性が企業活動に与える影響を踏まえ、実際の被害事例や対策方法を紹介しています。	初版:2015年3月 第2版:2016年3月 第3版:2017年3月	国内	独立行政法人 情報処理推進機構(IPA)	製造業、社会インフラ	工場・プラント:石油、化学、鉄鋼、自動車、輸送機器、精密機械、食品、製薬、ビル管理など 社会インフラ:電力、ガス、水道、鉄道など	・経営者・役員 ・経営企画・リスク管理部門の担当者 ・制御システムの導入・調達担当者 ・制御システムの運用・管理者	管理系／技術系	無し (ただし、簡易なチェック項目の記載あり)	https://www.ipa.go.jp/security/guide/vuln/ug65p900000019by0-att/000058489.pdf	制御システムを扱う企業向けのエントリー向けのセキュリティ対策啓蒙資料の位置づけ。	
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	本手引きは、これから産業用制御システム向け侵入検知製品等を導入しようと考えている企業における導入の支援、産業用制御システム向け侵入検知製品等に対する認知度の向上、普及促進を狙いとしており、手引き書作成の背景と目的、侵入検知製品等の基本情報や検討ポイントの比較、製品選定のポイント、具体的な導入の進め方、導入後の運用における留意点などがまとめられています。	2023年6月19日 発行	国内	独立行政法人 情報処理推進機構(IPA)	重要インフラ、製造業	産業用制御システムを有する業種で、特定の対象業種の指定などはなし	産業用制御システム向け侵入検知製品等を導入しようと考えている組織/事業体の導入・運用担当者、関係者	管理系／技術系	無し	https://www.ipa.go.jp/security/controlsystem/icsidshandbook.html	工場セキュリティGLで必要な対策として挙げられている侵入検知にフォーカスし導入方法や進め方の詳細資料の位置づけ	侵入検知製品を導入しようとする企業の目線で、製品・ベンダー選定から始まり、導入方法や運用方法などが詳しくまとめられているため、大変参考になると考えられる。
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	経済産業省は平成29年7月に「産業サイバーセキュリティ研究会」を設立し、平成30年2月に「WG1」の下で「サイバー・フィジカル・セキュリティ・フレームワーク(CPSF)」の検討を開始した。その一環として「ビルサブワーキンググループ」を設置し、ビルシステムのサイバーセキュリティ対策について議論を行った。 この結果、平成31年6月に「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(共通編)」第1版が策定された。しかし、第1版策定から約4年が経過し、スマートビルの進展によりサイバー攻撃のリスクが高まっているにもかかわらず、システムの制約やコストの問題から十分な対策が取られていない状況がある。 そこで、事前対策とインシデントレスポンスについて議論を重ね、第2版ではインシデントレスポンスの記述が追加されることになった。これにより、日本国内のビルシステム全体のサイバーセキュリティ確保に向けた取組がさらに進展することが期待されている。	初版:2018年6月 第二版:2023年4月	国内	経済産業省 産業サイバーセキュリティ研究会 ワーキンググループ1 (制度・技術・標準化) ビルサブワーキンググループ	建設業	・不動産業 ・総合建設業等	・ビルオーナー ・ゼネコン、サブコン ・設計事務所 ・個別システム事業者(ビル管理システム、空調、エレベータ、ビデオ監視、電力・熱供給 等) ・ビル管理会社 ・テナント ・サービスプロバイダ ・セキュリティベンダ、ネットワークシステムベンダ ・自治体、関係省庁 等	管理系	有	https://www.meti.go.jp/policy/netsecurity/wg1/building_guideline.html	業界特化	空調・照明等工場でも設置されるファシリティインフラであり、汎用的に活用できるガイドラインとなり得る。チェックリストもあるため、工場の新設、改修時に大変参考になると考えられる。
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	このガイドラインは、物流分野(特に倉庫業)における情報セキュリティ確保のための指針です。重要インフラ事業者がサイバー攻撃や災害などのリスクに備え、経営層の関与、リスクマネジメント、BCP(事業継続計画)、サプライチェーン管理、人的・物理的・技術的対策など、組織全体で継続的にセキュリティレベルを向上させることを目的としています。実際のインシデント事例や最新の脅威動向も踏まえ、現場で実践しやすい具体策を網羅しています 。	第1版(令和6年4月18日制定)	国内	国土交通省	物流分野(特に倉庫業)	倉庫業(WMS:倉庫管理システムを利用する事業者) 輸配送管理(TMS:輸配送計画・実行管理) 倉庫内機器・設備制御(WCS:倉庫内の機器や設備の制御) 倉庫内管理(WES:倉庫内の作業全体の管理) 特殊な寄託物管理(医薬品・化学物質等の特殊な保管・管理が必要な業種)	重要インフラ事業者の経営層、情報セキュリティ責任者(CISO等)、システム管理者、現場担当者など、組織全体で情報セキュリティに関与するすべての関係者	管理系	無	https://www.mlit.go.jp/jidosha/jidosha_tk4_000121.html	相互補完	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は、倉庫と貨物自動車運送の2つに分かれている。大枠の内容は共通しているが詳細が異なる。

9	物流分野(貨物自動車運送)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	貨物自動車運送事業を支えるシステムを重要システムとし、「安全ガイドライン」の対象範囲とする。重要インフラサービスを支える重要システムは各貨物自動車運送事業で異なり、以下に例示する情報資産が重要システムとなりうる。 (例) 集配管理システム 貨物追跡システム	第1版(令和6年4月18日制定)	国内	国土交通省	物流分野(貨物自動車運送)	物流分野(貨物自動車運送、集配管理システムや貨物追跡システムなどを保有)する企業	重要インフラ事業者の経営層、情報セキュリティ責任者(CISO等)、システム管理者、現場担当者など、組織全体で情報セキュリティに関与するすべての関係者	管理系	無	https://www.mlit.go.jp/jidosha/jidosha_tk4_000121.html	相互補完	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は、倉庫と貨物自動車運送の2つに分かれている。大枠の内容は共通しているが詳細が異なる。
10	制御システムにおける資産管理ガイドライン	工場のDX化促進やIoT機器の導入にあたり、工場をクラウドサービスやインターネットに接続する機会が増加した結果、サイバーセキュリティリスクも増加しています。インターネット接続によるコスト削減や利便性向上と引き換えに、制御システムのセキュリティ対策が課題となっています。サイバー攻撃の影響を最小化するには、ISO31000で定義される資産管理を含むリスクマネジメントやリスクアセスメントが不可欠ですが、効果的な資産管理の具体的な方法に言及しているガイドラインはほとんどありません。 また、本ガイドラインで指摘されている資産管理の課題として、現状多くの組織が手作業による資産管理を実施していること、セキュリティ視点での資産管理を実施できていないこと等がアンケート結果により浮き彫りとなり、多くの組織が資産管理に困難を抱えていることが示されています。 このような課題に対し、本ガイドラインは多角的なアプローチによる解決策を提示しています。 ・収集すべき資産情報の具体的な定義: 資産情報を具体的にリストアップ(何を収集すべきかの基準を提示) 資産情報とサイバーセキュリティ脅威の紐付け ・実践的な情報収集方法: 資産情報を収集するための具体的な手法(既存の収集方法や開発した自動化ツール)の解説および検証結果の提示 ・資産管理の成熟度モデル: 組織が自らの資産管理レベルを客観的に評価し、	初版:2020年6月29日	国内	独立行政法人 情報処理推進機構 産業サイバーセキュリティセンター 中核人材育成プログラム 3 期生 資産管理プロジェクト	産業界全体 ※GL作成メンバーの業界:電力、ガス、化学、自動車、機械、原子力、情報通信	産業界におけるアセットオーナー、およびシステム供給者(ベンダー) ※GL作成メンバーの業種: ・電力供給業 ・ガス供給業 ・化学工業 ・自動車製造業 ・産業用機械、自動車部品製造業 ・電機、電子機器製造業 ・制御システム開発、販売業 ・ITサービス、インテグレーション業 ・原子力関連サービス業	制御システム関係者 以下に限定される訳ではないが、主な対象読者は以下の各担当者としている ・リスクマネジメント ・リスクアセスメント ・資産管理	管理系 OT環境に特化した、実践的かつ段階的な資産管理手法を提示している	有	https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2020/assetmanagement.html	「産業制御システムにおける資産管理ガイドライン」(本GL)と「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」(工場セキュリティGL)は、一連のセキュリティ対策活動の中で連携・活用する事ができると考えます。 工場セキュリティGLでは、対策の最初のステップ(ステップ1-4)として「保護対象の整理」が挙げられています。これは、自社の工場にどのような機器やシステムがあり、それらが自社の事業にとってどの程度重要かを把握するプロセスです。 この「保護対象の整理」を具体的にどう進めるのか、どのような情報を収集・管理すべきかという詳細な手法を紹介しているのが本GLです。本GLに沿って資産の一覧(資産台帳)を作成することで、工場セキュリティGLが要求する「保護対象の整理」を効率的に実施できると考えます。	
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	自家用電気工作物(発電事業の用に供するもの及び小規模事業用電気工作物は除外)の遠隔監視システム等、制御システム等のサイバーセキュリティの確保を目的とし、設置者が実施すべきセキュリティ対策を記載したガイドライン。 本ガイドラインの対象には、各システムに付随するネットワークも対象として含まれる。 組織体制、文書管理、セキュリティ管理、機器・通信・システム運用・物理的なセキュリティ、そして事故対応まで幅広く網羅しており、設置者等が自家用電気工作物のサイバーセキュリティを確保するための行動指針が記載されている。 系統連系する発電設備(蓄電設備を含む)の制御システム場合、区分Aに分類され、設置者等が実施すべき「動的的事項」が存在する。 残りの区分B と区分Cには、設置者等が実施の要否及び実施方法を判断すべき「推奨的事項」のみが存在する。 遠隔監視システムと制御システムの両方が無い場合、本ガイドラインは適用されない。 ※この概要は、2023年3月に改正されたガイドラインをベースにまとめ直した。	制定:2022年6月 改正:2023年3月	国内	経済産業省大臣官房技術総括・保安審議官	●設置者 バイオマス:林業、 太陽光:農業、漁業、製造業、運輸業、小売業、 風力:漁業、 石炭火力:鉱業、コージェネレーション:鉱業、製造業、倉庫業 ●保守点検者、遠隔サービス提供事業者:専門・技術サービス業	●設置者 バイオマス:林業、 太陽光:農業、漁業、製造業、運輸業、小売業、 風力:漁業、 石炭火力:鉱業、 コージェネレーション:鉱業、製造業、倉庫業 ●保守点検者、遠隔サービス提供事業者:専門・技術サービス業 ●遠隔監視・制御システムがある場合は需要設備の設置者も区分Cの対象	自家用電気工作物の設置者、保守点検者、遠隔サービス提供事業者	管理系	有 https://www.meti.go.jp/policy/safety_security/industrial_safety/law/files/cybersecurity_checklist.xlsx	https://www.meti.go.jp/policy/safety_security/industrial_safety/law/files/jikayoguideline.pdf	業界特化	組織体制からシステムやネットワークのセキュリティ、物理セキュリティやインシデント対応体制にまで言及されており、自家用電気工作物のサイバーセキュリティ対策に取り組む際にまず最初に読むべきガイドラインであると考える。
12	IEC 62443-2-1	IEC 62443-2-1は、産業オートメーションおよび制御システム(IACS)の資産所有者(アセットオーナー)向けに、運用中のシステムを保護するためのセキュリティプログラムに関するポリシーおよび手順要件を定めた国際規格。 2024年版では、従来のISMS(情報セキュリティマネジメントシステム)要件との重複を排除し、「セキュリティプログラム要素(SPEs)」という新たな構造を導入することで、資産所有者が自組織のリスクに即した管理体制を構築しやすくしている。また、IACSのライフサイクルが20年以上に及ぶことを踏まえ、レガシーシステムへの補償的セキュリティ対策の適用を正式に許容するなど、実運用に即した柔軟性も確保。 IEC 62443シリーズは、IACSの設計・開発から運用・保守までを包括的に扱う枠組みであり、そのうちPart 2-1は「資産所有者のセキュリティプログラム」に特化した位置づけである。シリーズ全体としては、ISO/IEC 27000系の情報セキュリティマネジメントと連携的に、産業制御システム特有のリスクを管理するための共通用語、プロセス、技術要件を提供。	Edition1: 2010年11月 Edition2: 2024年8月	国際	ISA 99、IEC TC65 WG10	産業オートメーション制御システム(IACS)全般(製造、エネルギー、水道、交通インフラ等)	プロセス製造、ディスクリート製造、公益事業(電力・水処理)、輸送制御等	IACSアセットオーナー(資産所有者)、エンドユーザー組織の運用管理者・セキュリティ責任者	管理系	無(標準本文で要件が体系化されているものの、独立したチェックリスト形式の付録は付属しません)	https://webstore.iec.ch/en/publication/62883	付録の「B-1.2 セキュリティに関わる標準規格・ガイドライン準拠の要求」にて、国際標準規格として共通的で代表的な企画としてIEC 62443規格群が挙げられている	
13	IEC 62443-3-2	この規格は、IEC 62443シリーズの中でもIEC 62443-3-2は「設計と統合」フェーズに位置づけられて、その中でもシステムのリスク評価に焦点を当てており、セキュリティレベル(SL)を決定するための基盤を提供。 IEC 62443-3-2で決定されたSLに基づいて、密接に関連しているIEC 62443-3-3(システムセキュリティ要件)で、システム全体に必要なセキュリティ機能を定義。 IEC 62443-3-2には、以下のポイントが挙げられる。 1. リスク評価の枠組みの提供 IEC 62443-3-2では、IACSに対するセキュリティリスクを体系的に評価するためのプロセスを定義。これにより、組織は自社の制御システムに対する脅威や脆弱性を明確にし、適切な対策を講じることができる。 2. ゾーンとコンジットの概念 この規格では、システムを「ゾーン(Zone)」と「コンジット(Conduit)」に分割することで、セキュリティ境界を明確にし、リスクを管理しやすくします。ゾーンは同じセキュリティ要件を持つ資産の集合体、コンジットはゾーン間の通信経路。 3. セキュリティレベル(SL)の導入 「リスク評価の結果に基づき、各ゾーンやコンジットに対して必要なセキュリティレベル(SL)を設定。SLは0~4まであり、数字が大きいほど高いセキュリティ対策が求められる。 4. 資産の識別と分類	Ediiton1: 2020年6月	国際	ISA 99、IEC TC65 WG10	産業オートメーション制御システム(IACS)全般(製造、エネルギー、水道、交通インフラ等)	プロセス製造、ディスクリート製造、公益事業(電力・水処理)、輸送制御等	・資産所有者(OT/工場経営層) ・システムインテグレータ/DCS・SCADA ベンダ ・OT/IT セキュリティ運用者・アーキテクト	管理+技術	無(標準本文で要件が体系化されているものの、独立したチェックリスト形式の付録は付属しません)	https://webstore.iec.ch/en/publication/30727	付録の「B-1.2 セキュリティに関わる標準規格・ガイドライン準拠の要求」にて、国際標準規格として共通的で代表的な企画として IEC 62443規格群が挙げられている	IT-OT 分離の判断材料を提供する。

14	IEC 62443-3-3	産業オートメーション制御システム(IACS)に求められる技術的防御策を定めた国際規格。 利用者が共通して満たすべき7つのFR(基本要件:識別・認証制御、使用制御、システム完全性、データ機密性、データフロー制限、イベント適時対応、リソース可用性)を軸に、44件のSR(システム要件)とRE(強化要件)を提示。 また、想定する攻撃者像からSL0～SL4の各セキュリティレベルを定義し、SL-C(セキュリティレベルケーパビリティ)としてSLごとに実装が必要なSRおよびREを紐づけることで、IACS設計者やベンダは必要な対策を特定できる。規格はゾーン／コンジットモデルも示し、3-2や4-2などIEC 62443の他パートと連動してライフサイクル全体のセキュリティ確保を支援。 2013年に発行され、2027年まで有効とされる現行版は、ISASecure SSA認証や各国ガイドラインの技術チェックリストの根拠文書にもなっている。	Edition1: 2013年8月 COR1(訂正版): 2014年4月	国際	ISA 99、IEC TC65 WG10	産業オートメーション制御システム(IACS)全般(製造、エネルギー、水道、交通インフラ等)	プロセス製造、ディスクリート製造、公益事業(電力・水処理)、輸送制御等	・資産所有者(OT/工場経営層) ・システムインテグレータ/DCS・SCADA ベンダ ・OT/IT セキュリティ運用者・アーキテクト	技術系	無(標準本文で要件が体系化されているもの、独立したチェックリスト形式の付録は付属しません)	https://webstore.iec.ch/en/publication/7033	付録のIB-1.2 セキュリティに関わる標準規格・ガイドライン準拠の要求」にて、国際標準規格として共通的で代表的な企画として IEC 62443規格群が挙げられている	
15	NIST SP800-82	物理環境を制御する運用技術(OT)システムを、その安全性と運用要件を維持しながらサイバー脅威から守るための包括的な指針を提供する文書。 主なポイントは以下の通り。 ・OTとは：物理的なプロセスやデバイス (例：産業用制御システム(ICS)、ビル管理システム、交通システムなど)を監視・制御し、直接的な物理的変化を引き起こすシステム。 ・なぜセキュリティが必要か： 以前は隔離されていたOTシステムが、ITシステム(インターネット、IPなど)と接続性向上により、外部からの脅威にさらされるため。 ・提供する内容：OTの概要、一般的な脅威と脆弱性を特定し、それらを軽減するための推奨されるセキュリティ対策を提示。	Rev.1: 2013年5月 Rev.2: 2015年6月 Rev.3: 2023年9月	国際	米国商務省 米国国立標準技術研究所	米国の重要なインフラストラクチャの運用に不可欠なセクター	化学セクター 商業施設セクター 通信セクター 重要製造業セクター ダム エネルギー (電力網、石油・ ガスパイプライン などを含む) 食品・農業 医療・公衆衛生 原子力炉、資材、廃棄物 交通システム (鉄道、公共交通機関、 航空交通管制、 パイプライン輸送システム などを含む) 水・廃水 (水道配給、 廃水収集システムなどを含む)	OTシステムを設計または実装する制御エンジニア、インテグレーター、アーキテクト OTシステムを管理、パッチ適用、または保護するシステム管理者、エンジニア、その他の情報技術(IT)専門家 OTシステムのセキュリティ評価やペネトレーションテストを実施するセキュリティコンサルタント OTシステムを担当するマネージャー OTシステムのサイバーセキュリティプログラムを正当化し適用する際に、OTシステムへのリスクをより深く理解する必要がある上級管理職 OTシステムの固有のセキュリティニーズを理解しようとしている研究者およびアナリスト OTシステムの一部として展開さ	技術系と管理系の両方の側面を持つ文書	無し	https://csrc.nist.gov/pubs/sp/800/82/r3/final	工場セキュリティガイドラインは、工場システムにおけるセキュリティ対策の策定や実行において、ICS/OT(産業用制御システム/オペレーショナルテクノロジー)のセキュリティに関する国際的な参照規格の一つとしてNIST SP 800-82の利用を推奨している	
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	重要インフラにおけるプロセス制御システム(PCS)やSCADA(監視制御およびデータ収集)システムのセキュリティ向上に向けたベストプラクティスとして以下の7つのセキュリティ強化フレームワークを示している。 1. 事業リスクの理解: プロセス制御システムが侵害された場合の事業へのリスクを評価し、継続的に再評価するプロセスを確立 。 2. セキュア・アーキテクチャの実装: 事業リスクに基づいて、適切なセキュリティ対策を選択、実施 。これには、ネットワーク・アーキテクチャ、ファイアウォール、リモート・アクセス、ウイルス対策、システムの強化、バックアップと回復、物理的セキュリティなどが含まれる。 3. 対応能力の確立: セキュリティインシデントの発生を監視し、評価し、対応するための手順を確。 4. 意識とスキルの改善: 組織全体のプロセス制御セキュリティ意識を高め、必要な知識とスキルを要員に持たせることを目指す。 5. サード・パーティ・リスクの管理: ベンダ、サポート組織、サプライ・チェーン内の関係者など、サード・パーティからもたらされるセキュリティ・リスクを管理。 6. プロジェクトへの参画: プロジェクト開発プロセスの早い段階でセキュリティ・リスクに対する保護対策を組み込むことで、効果的かつ費用対効果の高いセキュリティを実現。 7. 継続した統制の確立: プロセス制御システム・セキュリティの管理を公式に監視することにより、組	原典: 2005年2月 翻訳版: 2010年7月	国際(UK CPNI)	CPNI / PA Consulting	製造業	プロセス制御、SCADA	プラント運用・保全部門、経営層	管理+技術	無し	https://www.jpcert.or.jp/research/2007/GoodPractice-for-ProcessControl-and-SCADA-Security.pdf	工場セキュリティガイドラインに沿ってセキュリティが提唱するPDCAサイクルのうち、実行(Do)時に本ガイドを利用可能	JPCERT/CCが公開している邦訳を参照した。
17	Principles of operational technology cybersecurity	重要インフラにおけるOT環境の設計・運用・管理に関するセキュリティガイドラインです。 重要インフラの安全性と事業継続を守るための6つの基本原則を記載しています。 【6つの基本原則】 1.Safety is paramount(安全が第一) 2.Knowledge of the business is crucial(ビジネスの知識が重要) 3.OT data is extremely valuable and needs to be protected(OTデータは極めて貴重であり、保護する必要あり) 4.Segment and segregate OT from all other networks(OTを他のネットワークから分離・隔離する) 5.The supply chain must be secure(サプライチェーンは安全でなければならない) 6.People are essential for OT cybersecurity(OTのサイバーセキュリティには人材が不可欠)	初版:2024年10月 ※以降更改なし。	国際	ASD's ACSC (オーストラリア通信情報局オーストラリアサイバーセキュリティセンター) ※以下、共同署名組織 ・米国土安全保障省サイバーセキュリティ・インフラ庁(CISA) ・米国国家安全保障局 (NSA) ・米国連邦捜査局 (FBI) ・州横断情報共有分析センター(MS-ISAC) ・英国国家サイバーセキュリティセンター(NCSC-UK) ・カナダサイバーセキュリティセンター (Cyber Centre) ・ニュージーランド国家サイバーセキュリティセンター (NCSC-NZ) ・ドイツ連邦情報セキュリティ庁(BSI Germany) ・オランダ国家サイバーセキュリティセンター (NCSC NL) ・内閣サイバーセキュリティセンター (NISC) ・警察庁 (NPA) ・韓国国家情報院(NIS)のサイバーセキュリティセンター	全般	全般	・IT 関係部門(情報システム部門、セキュリティ部門 等) ・生産関係部門(生産技術部門、生産管理部門、工作部門 等) ・戦略マネジメント部門(経営企画等) ・監査部門 ・リスク管理部門 ・機器システム提供ベンダ、機器メーカ(サプライチェーンを構成する調達先を含む) ・経営層(CTO、CIO、CISO 等) ・重要インフラ事業者	管理系	無	■原本 https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/critical-infrastructure/principles-operational-technology-cybersecurity ■和訳(内閣 国家サイバー統括室) https://www.nisc.go.jp/pdf/policy/kokusai/Provisional_Translation_JP_ASD_OT_Guidance.pdf	・ステップ1 内外要件(経営層の取組や法令等)や 業務、保護対象等の整理 ・ステップ2 セキュリティ対策の 立案 ・ステップ3 セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し ※原則1、原則6については、工場セキュリティGLで詳細に言及されていない。	-
18	Mitigating the Impacts of Doxing on Critical Infrastructure	米国CISA(サイバーセキュリティ・インフラセキュリティ庁)は、重要インフラや人員を保護するため、すべての関係者に対し積極的なサイバーセキュリティ対策の実施を奨励しています。特に仮想環境が高度化する中、組織は利用可能なリソースを活用し、脅威の変化に応じた継続的な評価と対策の強化が求められます。この文脈でCISAは「ドクシング(個人情報の悪意ある公開)」の脅威に対応するためのガイド「CISA Insights: Mitigating the Impacts of Doxing on Critical Infrastructure」を発行しました。これは、重要インフラの運用者やセキュリティ専門家に向けて、情報・対策・リソースを提供するもので、現場での実践的なセキュリティ強化に役立つ内容となっています	初版:2021年5月21日	国際	CISA: Cybersecurity and Infrastructure Security Agency (米国サイバーセキュリティ・インフラセキュリティ庁) 米国国土安全保障省(DHS: Department of Homeland Security)の外局(sub-agency)として設立	重要インフラ	医療機関 官公庁等	・セキュリティ担当者 ・自治体、関係省庁 等 ・サービスプロバイダ ・セキュリティベンダ、ネットワークシステムベンダ ・自治体、関係省庁 等	管理系	無	https://www.cisa.gov/resources-tools/resources/cisa-insights-mitigating-impacts-doxing-critical-infrastructure	工場セキュリティガイドラインのインシデント対応章に、CISAのドキシング対策を補完的に統合することで、標的型攻撃や情報漏洩に晒される人的情報への保護を強化できる。個人情報の悪意ある公開は、従業員や経営層への脅威となり得るため、具体的な対処策の導入は、工場システムの安全性向上に有効ではないか。	

19	Design principles and Operational Technology	本ガイドラインでは、まずIT/OT共通のセキュアなシステム設計原則として下記の5つを提示しています。システムには、仮想化システムも含みます。 1, 前提を整理する事(コンテキストの確立) 補足:システムの設計にあたり構成要素、運用環境および関係性の全てを把握する 2, システムへの候害を困難にさせる事 3, システムを高負荷に陥らせない事 4, システムへの侵害検知を用意にする事 5, システムへの侵害後の影響を最小限にする事 そのうえで、本該当ページ(2ページ分)では、OT環境に対し、実際にどうすれば上記原則に沿って、安全性と可用性も確保したセキュアな設計が実施できるか明白になるよう、丁寧に例も用いて説明されています。 ・OTシステム設計においての、上記5原則ごとのOTに特化した観点、留意点が記載される 補足:主に下記のフェーズが対象 ・基本設計 ・検証 ・運用設計 ・OTシステムへとくに仮想化を適用する際の、上記5原則ごとの観点、留意点が記載される	初版:2020年5月 ※以降更改なし。	国際	NCSC(英国のサイバーセキュリティのための国家技術局)	全般	全般	OTシステム設計者 (工場セキュリティGLでの、下記に該当/関連すると考えられる) ・IT 関係部門(情報システム部門、セキュリティ部門 等) ・監査部門 ・機器システム提供ベンダ、機器メーカ(サプライチェーンを構成する調達先を含む)	技術系	無	https://www.ncsc.gov.uk/collection/cyber-security-design-principles/examples/study-operational-tech	本ガイドラインはより技術的な解説を扱うため、関連項目は下記程度 (以下工場セキュリティGLの項目から) ・STEP1 のうち1-4 保護対象の整理 ・STEP2 セキュリティ対策の立案(システム面) ※粒度比較のイメージとしては、工場セキュリティGLが、一般的な実装手段を名称で挙げて紹介するに留まっているのに対し、本ガイドラインは実装手段の具体的な適用方法まで解説している	
20	Security Tenets for Life Critical Embedded Systems	現代社会では、医療機器や自動車、SCADA、ICSなどのライフクリティカルな組込みシステムが重要な役割を担っており、これらがIoTを通じて相互接続されることで、サイバー攻撃への対策が急務となっています。米国CISA(サイバーセキュリティ・インフラセキュリティ庁)は、 「ライフクリティカルな工ンベデッドシステムのセキュリティ原則」にて、人命や環境を守るための基本的なセキュリティガイドラインを提示し、業界や組織を問わず適用可能な中核的技術原則を示しています。これにより、現行の標準よりも高い安全性を実現し、標準策定やシステム開発の出発点として活用されることを目的としています。	初版:2020年12月17日	国際	CISA: Cybersecurity and Infrastructure Security Agency (米国サイバーセキュリティ・インフラセキュリティ庁) Defense Industrial Base and Information Technology Sector members (防衛産業基盤および情報技術部門のメンバーによるクロスセクター作業部会)	ライフクリティカルな組込みシステムを有するすべての業界・組織	製造業 医療機器製造業 自動車産業等	・医療機器メーカー ・病院のIT部門 ・遠隔医療システム開発者 ・コネクテッドカーや自動運転車の開発者 ・製造業のシステム運用管理者 ・電力・水道・ガス 事業者 ・IoTデバイス開発企業 ・通信インフラ提供企業 ・自治体、関係省庁 等	技術系	無	https://www.cisa.gov/resources-tools/resources/security-tenets-life-critical-embedded-systems	国際的な原則集としてセキュリティ要件や原則を提唱している。開発技術者向けに、暗号・認証・コード署名・最小権限などのセキュリティ原則を詳細に記述している。	

別紙２：下書きセキュリティガイドラインチェックリストとの対応

凡例：
P1　：下書きセキュリティガイドライン（1.0）原則1（P1.1～P1.3）
P2　：下書きセキュリティガイドライン（1.0）原則2（P2.1～P2.3）
P3　：下書きセキュリティガイドライン（1.0）原則3（P3.1～P3.3）
○　：上記項目がガイドラインチェックリストの内容と対応している（Yes/Applicable）
－　：上記項目がガイドラインチェックリストの内容と対応していない（No/Not Applicable）

カテゴリ	カテゴリID	番号	概要説明	対応策：関連する下書きセキュリティガイドライン（P1/P2/P3）の記載	組織レベルのためのセキュリティガイドライン（P1）	業務有効性システム向け考え方のためのセキュリティガイドライン（P2）	組織レベルのためのセキュリティ運用管理ガイド	組織レベルの有効性のための継続的改善ガイド	開発者（システムインテグレーター）向けセキュアバイデザインフレームワーク	製品開発（調達）者向けセキュアバイデザイン・セキュアバイデフォルト	製品開発（調達）者向けセキュアバイデザイン・セキュアバイデフォルト（P3）	SAL 組織レベルにおける脆弱性管理ガイドライン	組織有効性（SAL）向けセキュリティガイドライン（P2/P3）	IEC 62443-3-1	IEC 62443-3-2	IEC 62443-3-3	NIST SP800-82	クールプラクティス ガイド（2024年版） IC4DA	Principles of operational technology cybersecurity	Mitigating the Impacts of Doxing on Critical Infrastructure	Device orientation and Operational Technology Containers	Secure Design for Life-Critical Medical Device Software
物理	AM	1.1	組織システムにおける資産・組織全体の管理方針策定（資産の定義と分類、資産の管理責任者の明確化、資産の適切な利用ルールの策定、資産の廃棄・返却手順の整備）	○ ■対応している内容 第1章 はじめに（P1.1 Step 1） 「本ガイドラインの適用対象は、組織システムにおいて、情報処理・通信機能を有する資産（ハードウェア、ソフトウェア、ネットワーク機器、IoT機器、クラウドサービス等）を対象とする。」 ■適用している理由 「組織システムにおいて、情報処理・通信機能を有する資産（ハードウェア、ソフトウェア、ネットワーク機器、IoT機器、クラウドサービス等）を対象とする。」 ■実施する具体策 ・資産の定義と分類 ・資産管理責任者の明確化 ・資産の適切な利用ルールの策定 ・資産の廃棄・返却手順の整備 ■実施する理由 ・資産の定義と分類 ・資産管理責任者の明確化 ・資産の適切な利用ルールの策定 ・資産の廃棄・返却手順の整備	○ ■対応している内容 第1章 はじめに（P1.1 Step 1） 「本ガイドラインの適用対象は、組織システムにおいて、情報処理・通信機能を有する資産（ハードウェア、ソフトウェア、ネットワーク機器、IoT機器、クラウドサービス等）を対象とする。」 ■適用している理由 「組織システムにおいて、情報処理・通信機能を有する資産（ハードウェア、ソフトウェア、ネットワーク機器、IoT機器、クラウドサービス等）を対象とする。」 ■実施する具体策 ・資産の定義と分類 ・資産管理責任者の明確化 ・資産の適切な利用ルールの策定 ・資産の廃棄・返却手順の整備 ■実施する理由 ・資産の定義と分類 ・資産管理責任者の明確化 ・資産の適切な利用ルールの策定 ・資産の廃棄・返却手順の整備	第1章 はじめに（P1.1 Step 1） 「本ガイドラインの適用対象は、組織システムにおいて、情報処理・通信機能を有する資産（ハードウェア、ソフトウェア、ネットワーク機器、IoT機器、クラウドサービス等）を対象とする。」 ■適用している理由 組織システムの適用対象の明確化	第1章 はじめに（P1.1 Step 1） 「本ガイドラインの適用対象は、組織システムにおいて、情報処理・通信機能を有する資産（ハードウェア、ソフトウェア、ネットワーク機器、IoT機器、クラウドサービス等）を対象とする。」 ■適用している理由 「組織システムにおいて、情報処理・通信機能を有する資産（ハードウェア、ソフトウェア、ネットワーク機器、IoT機器、クラウドサービス等）を対象とする。」 ■実施する具体策 ・資産の定義と分類 ・資産管理責任者の明確化 ・資産の適切な利用ルールの策定 ・資産の廃棄・返却手順の整備 ■実施する理由 ・資産の定義と分類 ・資産管理責任者の明確化 ・資産の適切な利用ルールの策定 ・資産の廃棄・返却手順の整備

別紙3 ガイドラインのマッピング

特化度と専門度は以下の特性について「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5とし、定性的に0から10の11段階で表したものである。
特化度　対象領域の絞り込みの程度。数字が大きくなるほど特定領域に特化した内容となる
専門度　記載内容の深さの程度。数字が大きくなるほど専門家向けとなる

No.	ガイドライン名	特化度	専門度	ページ数	発行元	発行年	対象業界	チェックリスト	URL	備考
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	5	5	123	経済産業省	2025	製造業全般	有	https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html	基準文書・包括的
2	自工会/部工会 サイバーセキュリティ・ガイドライン	4	6	44	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	自動車産業	有	https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html	IT寄り・サプライチェーン
3	制御システムのセキュリティリスク分析ガイド	8	8	399	独立行政法人 情報処理推進機構	2023	重要インフラ全般	有	https://www.ipa.go.jp/security/controlsystem/riskanalysis.html	リスク分析特化
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	8	7	62	独立行政法人 情報処理推進機構	2018	制御システム全般	無	https://www.ipa.go.jp/archive/digital/iot-en-ci/mieruka/20180319.html	セーフティ特化
5	制御システム利用者のための脆弱性対応ガイド	5	3	33	独立行政法人 情報処理推進機構	2017	製造業・社会インフラ	無	https://www.ipa.go.jp/security/guide/vuln/ug65p90000019bv0-att/000058489.pdf	入門向け
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	9	5	68	独立行政法人 情報処理推進機構	2023	産業用制御システム	無	https://www.ipa.go.jp/security/controlsystem/icsidshandbook.html	侵入検知特化
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	4	5	97	経済産業省	2023	建設業・不動産業	有	https://www.meti.go.jp/policy/netsecurity/wg1/building_guideline.html	ビル業界特化
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	4	4	151	国土交通省	2024	物流業(倉庫)	無	https://www.mlit.go.jp/jidosha/jidosha_tk4_000121.html	物流業界特化
9	物流分野(貨物自動車運送)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	4	4	153	国土交通省	2024	物流業(運送)	無	https://www.mlit.go.jp/jidosha/jidosha_tk4_000121.html	物流業界特化
10	制御システムにおける資産管理ガイドライン	9	7	66	独立行政法人 情報処理推進機構	2020	産業界全般	有	https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2020/assetmanagement.html	資産管理特化
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	5	6	38	経済産業省	2023	電力・発電設備	有	https://www.meti.go.jp/policy/safety_security/industrial_safety/law/files/jikayouguideline.pdf	電力業界特化
12	IEC 62443-2-1	3	9	194	International Electrotechnical Commission	2024	産業オートメーション全般	無	https://webstore.iec.ch/en/publication/62883	セキュリティプログラム
13	IEC 62443-3-2	8	9	36	International Electrotechnical Commission	2020	産業オートメーション全般	無	https://webstore.iec.ch/en/publication/30727	リスクアセスメント
14	IEC 62443-3-3	9	9	200	International Electrotechnical Commission	2014	産業オートメーション全般	無	https://webstore.iec.ch/en/publication/7033	システム要件
15	NIST SP800-82	4	8	316	National Institute of Standards and Technology	2023	重要インフラ全般	無	https://csrc.nist.gov/pubs/sp/800/82/r3/final	包括的・国際標準
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	7	6	30	Centre for the Protection of National Infrastructure	2005	プロセス制御・SCADA	無	https://www.jpcert.or.jp/research/2007/GoodPractice-for-ProcessControl-and-SCADA-Security.pdf	SCADA特化
17	Principles of operational technology cybersecurity	5	4	14	Australian Cyber Security Centre	2024	重要インフラ全般	無	https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/critical-infrastructure/principles-operational-technology-cybersecurity	6原則・入門的
18	Mitigating the Impacts of Doxing on Critical Infrastructure	9	5	3	Cybersecurity and Infrastructure Security Agency	2021	重要インフラ	無	https://www.cisa.gov/resources-tools/resources/cisa-insights-mitigating-impacts-doxing-critical-infrastructure	ドキシング特化
19	Design principles and Operational Technology	8	7	12	National Cyber Security Centre	2020	OT環境全般	無	https://www.ncsc.gov.uk/collection/cyber-security-design-principles/examples/study-operational-tech	設計原則特化
20	Security Tenets for Life Critical Embedded Systems	8	8	30	Cybersecurity and Infrastructure Security Agency	2020	組込みシステム	無	https://www.cisa.gov/resources-tools/resources/security-tenets-life-critical-embedded-systems	組込み特化

下記チャートの円の大きさはページ数を表す。

