経済産業省　御中

令和4年度サプライチェーン・サイバーセキュリティ対策促進事業（産業分野別のセキュリティガイドライン等の整備）

報告書

三菱総合研究所

デジタル・イノベーション本部

2023年3月31日

目次

図 目次

表 目次

1. はじめに

1.1 調査背景・目的

我が国では、AIやＩｏT、ビッグデータなど、サイバー空間とフィジカル空間を高度に融合させるシステムによって、経済発展と社会的課題の解決を両立する人間中心の社会である「Society5．0」の実現を目指している。「Society5．0」を実現するためには、サイバー空間とフィジカル空間を高度に融合させたシステムの社会実装を進めることが必要である一方、「つながる」ことによるネットワーク化の進展は、悪意のある者にとって新たな攻撃の機会ともなっていくおそれがある。このような背景の下、経済産業省では、平成30年2月7日に「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（WG1）（制度・技術・標準化）」を設置し、「Society5．0」における新たなサプライチェーン全体のセキュリティ確保を目的としたサイバー・フィジカル・セキュリティ対策についての議論を進め、『サイバー・フィジカル・セキュリティ対策フレームワーク』（以下、「CPSF」という。）を平成31年4月18日に取りまとめた。さらに、CPSFの実装に向け、令和元年8月2日より『第2層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースを開催し、IoT機器等のフィジカル空間とサイバー空間をつなぐ機器・システムに対するセキュリティの検討を行っている。加えて、CPSFの考え方を産業活動に実装するために、産業活動の実態に応じて、必要な対策要件や対策水準について検討を行う産業分野別のサブワーキンググループ（ビルサブワーキンググループ、工場サブワーキンググループ、宇宙産業サブワーキンググループ等。以下、まとめて「産業分野別SWG」という。）を立ち上げ、それぞれの課題に応じた検討を並行して進めている。

本事業では、以下の3つの産業分野別SWGについて、調査や検討会の運営、資料作成等を行った。

なお、それぞれのSWG等の産業サイバーセキュリティ研究会における位置づけについては仕様書参考資料「研究会構成図」を参照した。

- 工場等の製造現場でのサイバーセキュリティ対策を検討するため、国内外の工場セキュリティ対策の動向について調査を行うとともに、産業分野別SWGとして令和4年1月に設置した「工場SWG」の開催や資料の取りまとめ等を行った。
- ビルシステムのサイバーセキュリティ対策の更なる高度化、広範化、個別化に向けた調査を実施するとともに、その推進に資する体制構築に向けた調査を実施し、その成果を取りまとめ、ビルシステムにおけるサイバーセキュリティの一層の確保を目指した。
- 産業分野別SWGとして令和3年1月に新たに立ち上げた「宇宙産業SWG」及び当該SWGの下に設置をした「宇宙産業SWG作業部会」の事務局として会議開催や資料案作成を行った。

1.2 調査実施概要

調査目的を達成するために、以下の項目に関して調査・検討・支援等を行った。

1. 工場分野関係
   （1） 工場等の製造現場におけるサイバーセキュリティ対策の検討
   （2） 検討会の運営
2. ビル分野関係

（1）ビルガイドラインの高度化のための調査
（2）ビルシステムのサイバーセキュリティ推進体制の調査
（3）検討会の運営

3. 宇宙分野関係
（1）宇宙分野における海外のサイバーセキュリティ対策等についての調査
（2）検討会の運営
（3）民間宇宙システムにおけるサイバーセキュリティ対策ガイドラインの開発・更新
（4）ガイドラインの英訳
（5）情報共有・教育訓練のあり方などの検討

2. 工場分野に係る調査

工場等の製造現場でのサイバーセキュリティ対策を検討するため、国内外の工場セキュリティ対策の動向について調査を行うとともに、産業分野別SWGとして令和4年1月に設置した「工場SWG」の開催や資料の取りまとめ等を実施した。

2.1 工場等の製造現場におけるサイバーセキュリティ対策の検討

工場等の製造現場でのサイバーセキュリティ対策を検討にあたって、工場SWGで検討が進められている工場セキュリティガイドライン案を基に公開案を策定するための一連の作業を実施した。また、その策定後の普及啓発及び残存する課題の解決に向けた調査・検討を実施した。

工場には各産業分野の特性に応じて、セル生産・組立やライン生産・組立といったディスクリート製造、プラントのようなプロセス製造等の様々なタイプがあり、工場セキュリティにおける課題やリスク、関連制度等も異なっている。また、スマート工場の普及によって、今までとは全く異なるリスクにさらされる可能性も出てくる。このため、各産業分野の特性に応じた工場のサイバーセキュリティ関連動向等について調査を行うとともに、工場現場におけるデータ利活用の段階に応じたセキュリティ導入に係る課題やリスクの整理等も実施した。

これらの検討に当たっては、「2.2 検討会の運営」に示した工場 SWG を活用し、有識者や工場関係者の意見も反映しながら実施をした。

2.1.1 工場セキュリティガイドラインの策定に関する調査

(1) 工場セキュリティガイドラインの策定作業

1) パブリックコメントに基づくガイドライン修正作業

前年度に開催された第3回工場 SWG(令和4年3月 23 日開催)における「工場セキュリティガイドライン(案)」についての議論やコメントを踏まえ、「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(案)第1版」として修正、整理を行い、パブリックコメントを実施した。また、ガイドライン(案)の英訳を行い、「The Cyber/Physical Security Framework for Factory Systems (draft) Version 1.0」として、英語でのパブリックコメントも実施している。

表 2.1-1 パブリックコメントの実施概要

	「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(案) 第1版」	「 The Cyber/Physical Security Framework for Factory Systems (draft) Version 1.0」
期間	2022 年 4 月 27 日(水) ～2022 年 6 月 30 日(木)	2022 年 6 月 1 日(水) ～2022 年 6 月 30 日(木)
意見数	205 件(30 者)	11 件(2 者)

パブリックコメントの結果、日本語版・英語版合わせ、216 件のコメントを受領した。各コメントは以下に示す 12 種類の観点で分類し、それぞれ対応方針を整理した。

① ガイドラインの必要性
② 経営層とのコミュニケーション
③ 想定工場におけるインターネット接続やクラウド利用の考慮
④ 想定工場のモデル化
⑤ ゾーンの設定目的／定義
⑥ 各ステップの実施事項
⑦ 脅威と影響
⑧ 残存リスクへの対応
⑨ システム構成面でのセキュリティ対策
⑩ 運用面でのセキュリティ対策
⑪ 情報共有
⑫ チェックリストの記載項目

分類、整理したコメントに対するガイドライン（案）の対応方針を以下に報告する。

a. ガイドラインの必要性

表 2.1-2 ガイドラインの必要性へのコメントに対する対応方針

主なコメント	• インターネットに接続していなければセキュリティ対策は不要との誤認識を与えないような表現にすべき。【No.34】 • 自社は攻撃を受けないという人に、等しく攻撃を受ける注意喚起をした方がよい。【No.67】 • 攻撃者の動機を理解したうえでガイドラインを読んだ方がインパクトがある。【No.97】 • 工場 DX が推進されることによるクラウドやサプライチェーンに関するセキュリティ対策が必要になる点を追記してはどうか。【No.184】 • 生産システムが攻撃し易い点を、ガイドラインの動機付けにすると良いのではないか。【No.200】
コメントへの対応方針	• 工場システムは、インターネットに限らず、ネットワークに接続することでセキュリティリスクが高まる点を記載する。 • 工場 DX の推進によりクラウドやサプライチェーンの接続が進展している点を追記する。 • 重要な情報や金銭を目的とした標的型攻撃として特定の工場が狙われる場合もあれば、たまたま攻撃した先が工場である場合もあり、いかなる工場においても、サイバー攻撃を受ける可能性があることを記載する。

※主なコメントの【No.】表記は、コメントに一意に附番した番号（以下同じ）

b. 経営層とのコミュニケーション

表 2.1-3 経営層とのコミュニケーションへのコメントに対する対応方針

主なコメント	• リスクは投資対効果が見えないため、意思決定機関が率先して進めることが前提である。【No.73】

	• 経営層及び部門間のコミュニケーションの重要性を強く明記したほうが良い。【No.185】
コメントへの対応方針	• 主な想定読者である実務層が、経営層を始めとした意思決定を行う者と適切なコミュニケーションを行うことが重要である点を本文に記載する。

c. 想定工場におけるインターネット接続やクラウド利用の考慮

表 2.1-4 想定工場におけるインターネット接続やクラウド利用の考慮へのコメントに対する対応方針

主なコメント	• 制御ゾーンや生産管理ゾーンから直接インターネットへ接続する経路を記載してはどうか。【No. 17】 • 制御ゾーンの機器をリモートでメンテナンスしたり、生産性分析業務を外部クラウドで行うことも増えている。外部ネットワークとの接続も想定すべきではないか。【No.35】 • 想定工場のシステムでクラウドに関する指針を示してほしい。【No.62】 • 自動倉庫の遠隔保守以外は拠点内に閉じているため、インターネット接続やクラウド技術の使用も想定に加える必要はないか。【No.76】
コメントへの対応方針	• 設備系/生産情報系から直接インターネットに接続し、クラウドを利用する場合でも、本ガイドラインに示したステップに応じて対策を進めることが可能である点を追記する。

d. 想定工場のモデル化

表 2.1-5 想定工場のモデル化へのコメントに対する対応方針

主なコメント	• 工場システムの例は、ISA95 等のリファレンスに沿った図に変更するのが望ましい。【No.187】 • 具体的な想定工場の設定と同時に、抽象的な論理モデルとして Purdue Model を導入したほうが良いのではないか。【No.201】
コメントへの対応方針	• 本ガイドラインでは、工場システムをモデル化して現場の業務や保護対象に当てはめリスク分析・対策を行うというアプローチではなく、現場の業務や保護対象の重要性からゾーンを設定しリスク分析・対策を行うというアプローチを提示している旨を記載する。

e. ゾーンの設定目的／定義

表 2.1-6 ゾーンの設定目的／定義へのコメントに対する対応方針

主なコメント	• ゾーンを設定する意図目的を補足したほうが良い。個社・業界の性質を踏まえ、作業の粒度を調節すればよいことが伝わることが望ましい。【No.1】 • ゾーンは論理的な区画だけなのか、物理的な区画も含まれるのか説明すべき。【No.125】
コメントへの対応方針	• ゾーンを設定することにより、工場の機器やシステムを俯瞰的に見ることが可能となるなどの考え方を追記する。 • ゾーンの定義を明確化し、同じゾーンの保護資産に対しては、同等の水準のセキュリティ対策が求められる点を記載する。

f. 各ステップの実施事項

表 2.1-7 各ステップの実施事項へのコメントに対する対応方針

主なコメント	• 「計画・対策・運用体制の不断の見直し」は、「ステップ 2：セキュリティ対策の立案」で実施すべき。【No.15】 • 「ステップ 3：セキュリティ対策の実行」ではステップ 2 の中で決められたことを実施

	することを記載し、実施内容をいかに従業員等に周知徹底させるか記載してはどうか。【No.15】 • 「ステップ 4：セキュリティ対策実施の監査と評価」を追加してはどうか。【No.16】 • 「3.2.2 体制や運用面での対策」では「(1)システム構成面での対策」、「(2)物理面での対策」しかないが、「体制面での対策」「運用面での対策」「教育面での対策」等もあるのではないか。【No.14】
コメントへの対応方針	• ステップ 3 では、周知徹底も含め運用や不断の見直しについて求めていることから、ステップ 3 の名称を「(PDCA サイクルの実施)」に修正し、実施・運用状況の確認と評価について明示する。 • 体制面、運用面、教育面での対策は、ステップ 1-1 (1)経営目標等の整理や(3)内部要件／状況の整理において自社の状況を確認する際に、内部要件として体制や運用面等で対策が十分でない点があれば、この段階で実施することを明記する。

g. 脅威と影響

表 2.1-8 脅威と影響へのコメントに対する対応方針

主なコメント	• 工場の脅威をグルーピングして記述した方がよい。(1. 管理上の脅威(ISO27001)、2. 設備への脅威(IEC62443)、3. サイバー攻撃の脅威、4. 誤検知、誤動作による動作停止の脅威、5. 災害の脅威。)【No.60】 • 自然環境の脅威とシステム／機器の障害・故障と、セキュリティとの関連性、意図を示した方が良い。【No.93】 • 「自然環境の脅威」に「火災」がない。その他「施設や作業環境の脅威」をまとめてはどうか。【No.13】 • 従業員の過失に加え、保守要員(設備ベンダ)のリスクも記載するのが望ましい。【No.189】 • 「ゾーン外からのネットワークを介した不正アクセス」については、外→内に限らず、内→外を想定した記述にすることが望ましい。【No.190】
コメントへの対応方針	• 脅威の種別を再整理する。 • セキュリティ脅威への対策としてパッチの適用等を行うことにより、システム・機器の障害という別の脅威につながる場合もある点について記載する。

h. 残存リスクへの対応

表 2.1-9 残存リスクへの対応へのコメントに対する対応方針

主なコメント	• ステップ 2-3 に、対策後の残存リスクに対する対策方針の策定(サイバー保険への加入等)を追加してはどうか。【No.81】
コメントへの対応方針	• システム構成面や物理面でのセキュリティ対策後、残存するリスクに対しては、対策方針の策定(例：サイバー保険への加入、事業継続計画におけるセキュリティリスク対応の考慮 等)を行うことを記載する。

i. システム構成面でのセキュリティ対策

表 2.1-10 システム構成面でのセキュリティ対策へのコメントに対する対応方針

主なコメント	• 出口対策(インターネット出口の URL フィルタリングや通信ログ監視)に関しても記述すべき。【No.30】 • 境界防御だけでは、ゾーン内の拡散を防げないのではないか。NDR などの対策を例示すべき。【No.64】 • 脆弱性対策の高「＋ソフトウェア更新」は、OS は古いままでも良いとの誤解を生むため、最低限又は中であるべき。【No.40】 • 「パスワード(定期)変更」に加えて「複雑なパスワードの設定」を追記した方が良

	い。【No.6】
コメントへの対応方針	• ネットワークにおけるシステム構成面でのセキュリティ対策、機器におけるシステム構成面でのセキュリティ対策について、工場の実態を踏まえて見直しする。

j. 運用面でのセキュリティ対策

表 2.1-11 運用面でのセキュリティ対策へのコメントに対する対応方針

主なコメント	• ステップ 2-2 に、ヒューマンエラーに関する対策を追記してはどうか。【No.E-1】 • パッチ管理と BCP は多層防御の重要な部分であるため、実用的な方法を追加する必要がある。【No.E-8】 • 社員教育への注力について記載があっても良い。【No.53】
コメントへの対応方針	• 運用面でのセキュリティ対策として、ヒューマンエラー対策、パッチ管理について追記する。 • 人材育成については、工場システムに関わる従業員、セキュリティ確保を職務とする従業員、機器やサービスの提供者、それぞれの立場に応じたセキュリティスキルの向上が必要である点を記載する。

k. 情報共有

表 2.1-12 情報共有へのコメントに対する対応方針

主なコメント	• OT 環境に適した情報収集は困難であり、業種により差がある等の課題を明記してはどうか。【No.196】
コメントへの対応方針	• 産業機械等に関する脅威情報は、業種や対象によって入手可能な情報に差がある点を記載する。 • 業界やコミュニティ等を通じて情報共有を行うことが望ましい点を記載する。

l. チェックリストの記載項目

表 2.1-13 チェックリストの記載項目へのコメントに対する対応方針

主なコメント	• 3.1 節～3.2 節の項目がチェックリストにあると良い。【No.173】 • [2-8] 攻撃方法や脆弱性を特定するだけでなく、脆弱性へ対応している、緩和策を講じている等、特定後の対処を明文化すべき。【No.46】 • [2-9] 「工場内に外部記録媒体やポータルメディアの利用・持ち込みを制限している。」は困難なので、利用可能な条件を示してはどうか。【No.176】 • [2-10] 「工場内のシステムのパスワードの強度と有効期限を含むパスワードルールがある。」について、パスワードの有効期限設定は推奨される内容か。【No.177】 • [2-11] 「使用していない古いアカウントの削除」は「速やかに」など時間軸を入れるべき。【No.47】 • [2-13] バックアップしたデータは、可用性の観点からシステム侵害の影響が及ばない保護された場所に格納するべき。【No.178】 • [3-6] 外部からのインターネットアクセスが可能な場合、認証(2 要素認証等)や接続対象機器の制限、接続可能時間の制限、ネットワーク侵入防護などの保護対策を追記すべき。 他
コメントへの対応方針	• ステップ 1～2 の内容を、チェックリストに反映する。 • チェックリスト記載のセキュリティ対策について、工場の実態を踏まえて見直しする。

これらの対応方針及び方針に基づくガイドライン修正版(案)については、第4回工場 SWG(令和4年11月1日開催)において報告し、承認を得た。

2）ガイドラインの概要

工場セキュリティガイドラインは、令和4年 11 月 16 日、「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 Ver1.0」として経済産業省ホームページにおいて公表された。以下ではその概要を報告する。

a. ガイドラインの背景・目的

工場の IoT 化や自動化に伴い工場をインターネット等のネットワークに接続する機会が増加する結果、サイバーセキュリティ上のリスクが増大している。また、インターネット接続の機会に乏しい工場であっても、不正侵入者等による攻撃を受ける場合もある。

サイバー攻撃は、意図的に狙われる場合もあれば、たまたま攻撃される場合もあることから、いかなる工場においてもサイバー攻撃を受ける可能性あるということができる。

特に、一般的に製造業／工場では、安全確保（S：Safety）、事業／生産継続（BC：Business Continuity）、品質確保（Q：Quality）、納期遵守・遅延防止（D：Delivery）、コスト低減（C：Cost）という価値が重視されているが、サイバー攻撃はこれらを脅かすおそれがある。

このため、喫緊に取り組むべきこととして、工場にサイバーセキュリティ対策が求められており、セキュリティの推進は経営層等の意思決定を行う者による体制の構築や適切な指示が重要である。

工場ガイドラインは、対策を行う実務層向けのものであり、工場のセキュリティ対策を行うにあたり参照すべき考え方や対策のステップを「手引き」として示している。そして各業界・業種が自ら工場のセキュリティ対策を立案・実行することで、産業界全体、とりわけ工場システムのセキュリティの底上げを図ることを目的としている。

b. 想定読者

工場ガイドラインの想定読者は以下の通りである。

- IT システム部門
- 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
- 機器システム提供ベンダ、機器メーカー（サプライチェーンを構成する調達先を含む）

なお、上記想定読者が経営層（CTO、CIO、CISO）をはじめとした意思決定層と適切なコミュニケーションを行うことが重要である。

c. ガイドラインの想定工場

工場ガイドラインでは、工場システムのセキュリティ対策のステップを提示するにあたり、わかりやすさの観点から、想定工場を設定している。なお、読者の置かれた環境と想定工場とが必ずしも一致しない部分もあると考えられるため、読者の置かれた環境に応じて適宜読み替えることを前提としている。

工場ガイドラインにおける想定工場は以下のようなものとなる。

想定企業

- 経営者によってDX(デジタルトランスフォーメーション)が求められている
- 電子機器メーカ
- 複数の拠点に工場が存在し、それぞれの拠点で製品を生産
- 本社が管理する拠点間ネットワークで拠点同士は接続されるが、拠点内ネットワークは拠点ごとに管理
- 工場における有益な情報を見極めて収集、状態を見える化し、得られた気付きを知見・ノウハウとして蓄積

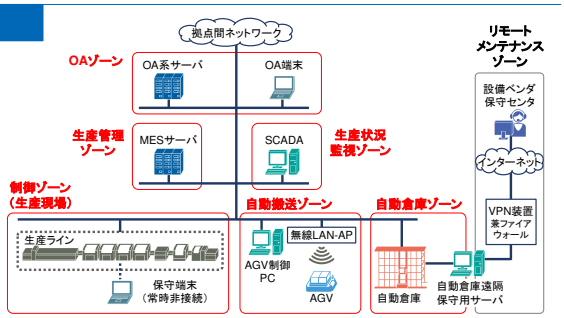
想定組織構成

- 生産技術・管理部門
- 工作部門
- 営業部門
- 資材部門
- 品質管理部門
- 情報システム部門

想定生産ライン

- 生産ラインでは電子機器に組み込まれるプリント基板を生産
- 生産自体は自動化されており、生産指示に基づいて複数機種を生産可能
- 段取り掛け、部品の補充などは工場の従業員が実施
- 工場内には複数の生産ラインが存在し、それぞれ独立して異なる機種を生産可能
- 生産設備(装置・機器)は設備メーカから導入し、生産技術・管理部門が生産ラインを構築・管理
- 設備の保守は設備ベンダが実施
- 自動倉庫は、設備ベンダが保守に備えてリモートで状態監視、及び現地での保守を実施

想定システム、ゾーン



工場システム例における構成要素

- ネットワーク
  - 設備系ネットワーク※
  - 生産管理系ネットワーク※
  - 情報系ネットワーク
- 装置・機器（機能・プログラム）
  - VPN装置兼ファイアウォール
  - 無線LAN-AP
  - MESサーバ
  - 生産ライン
  - SCADA
  - 保守端末（常時非接続）
  - AGV制御PC
  - AGV
  - 自動倉庫
  - 自動倉庫遠隔保守用サーバ
  - OA系サーバ
  - OA端末

※近年、設備系ネットワークや生産情報系ネットワークから情報系ネットワークを経由することなく、直接インターネットに接続できる経路も増えているが、そのような場合でも、本ガイドラインに示したステップや対策は活用可能。

想定業務

- 生産計画設定
- 生産(＋検査)
- 生産状況監視(現場)
- 部材補充(現場へ)
- 部材購入(倉庫へ)
- 生産性分析
- トレーサビリティデータ参照
- メンテナンス
- リモートメンテナンス

想定データ

- 生産計画
- 生産指示(生産機種・量)
- 生産レシピ
- 生産実績(トレサビデータ)
- 設備状態
- 設備プログラム・パラメタ・図面
- 部材在庫量(現場)
- 部材在庫量(倉庫)

図 2.1-1 工場ガイドラインにおける想定工場の設定内容

d. 工場システムのセキュリティ対策企画・導入ステップ

工場ガイドラインでは、工場システムのセキュリティ対策の企画・導入を3つのステップで実施する方法を提示している。以下に各ステップや対策の概略を示す。なお、このステップや対策の概略は想定工場を前提に例示したものであり、各ステップにおいて、個社や業界ごとに適した整理や考え方の定義を行うことが必要である。

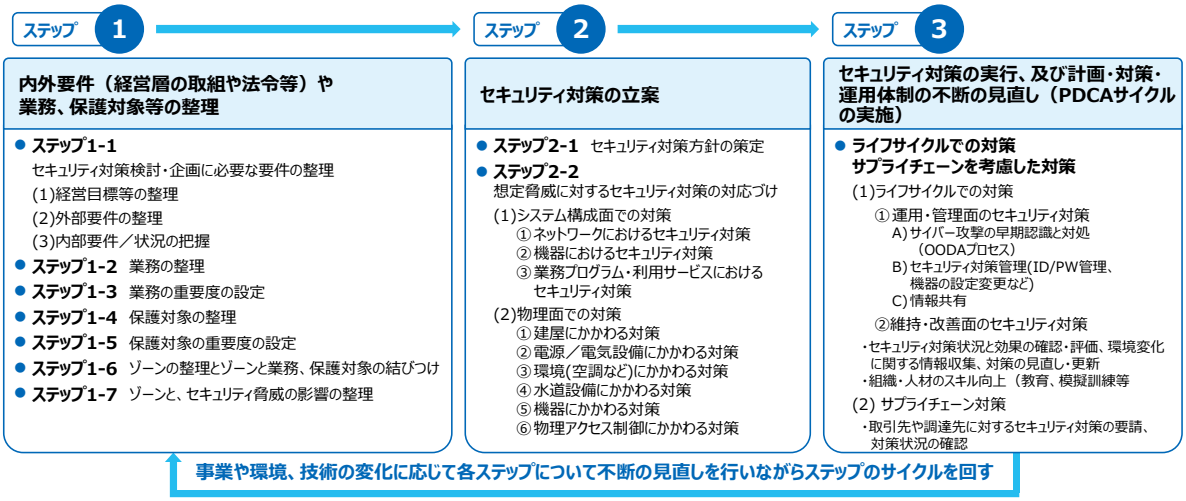


図 2.1-2 セキュリティ対策企画・導入の3ステップ

e. ステップ 1 内外要件や業務、保護対象等の整理

ステップ1では、工場システムのセキュリティを検討する上で、実施する内容を妥当なものとするために必要な情報を収集、整理する。

表 2.1-14 ステップ1を構成するサブステップとその概要

ステップ1-1	**セキュリティ対策検討・企画に必要な要件の整理**【3.1.1】	**（1）経営目標等の整理** 工場のセキュリティ対策に関わる経営目標（事業伸張、事業継続等）を整理する。特に、事業継続の観点では、事業継続計画（BCP）が策定されているかが重要であるため、その内容を確認する。BCPが整備されていなければ、必要に応じて担当部署とともに策定の検討を実施する 。 **（2）外部要件の整理** 工場のセキュリティ対策に関わる外部要件（セキュリティ法規制・標準規格・ガイドライン準拠、国・自治体／業界／市場・顧客／取引先／出資者からの要求等）を整理する。 **（3）内部要件／状況の整理** 自社の工場セキュリティに関わる内部要件（システム面、運用・管理面、維持・改善面、等）や体制を整理する。体制等が不明確である場合は、セキュリティ対策を推進するための体制やルール・手順等を整備し実施計画を立案し周知・教育等を実施する 。
ステップ1-2	**業務の整理**【3.1.2】	工場システムが使われている日々の業務の洗い出しを行う。
ステップ1-3	**業務の重要度の設定**【3.1.3】	洗い出した業務について、それぞれの業務の重要度を定める。
ステップ1-4	**保護対象の整理**【3.1.4】	セキュリティ対策を強化すべき業務を支援／実施する工場システムの構成要素(ネットワーク、装置・機器（機能・プログラム）・データ)を洗い出し、システム構成図の模式図を整理する 。
ステップ1-5	**保護対象の重要度の設定**【3.1.5】	事業伸張・継続(BC)、安全確保(S)、品質確保(Q)、納期遵守・遅延防止(D)、コスト低減(C)、それによる業務の重要性の視点から、洗い出した保護対象それぞれの重要度を明確にする。
ステップ1-6	**ゾーンの整理と、ゾーンと業務、保護対象の結びつけ**【3.1.6】	業務の重要度が同等であり、同等の水準のセキュリティ対策が求められる領域として、ゾーンを設定する。 ゾーンごとに、これまでに整理した業務、保護対象を結びつける。 ※ゾーンを設定することにより、工場の機器やシステムを大きな括りの概念として俯瞰的に見ることが可能となり、あるゾーン内の保護対象がサイバー攻撃を受けた際、別のゾーンへ影響が及ぶことを抑止し、被害を極小化することを検討することが可能となる。
ステップ1-7	**ゾーンと、セキュリティ脅威の影響の整理**【3.1.7】	最新の脅威について認識した上で、こうした脅威と生産・事業への影響を勘案し、それぞれのゾーンに対するセキュリティ脅威と影響を整理する。

f. ステップ 2 セキュリティ対策の立案

ステップ2では、ステップ1で収集・整理した情報に基づき、工場システムのセキュリティ対策方針を策定する。

表 2.1-15 ステップ2を構成するサブステップとその概要

ステップ2-1	**セキュリティ対策方針の策定**【3.2.1】	ステップ１で整理したゾーンとこれに紐づく業務、保護対象、想定脅威に対して、業界や個社の置かれた環境に応じ、重要度・優先度を設定する。
ステップ2-2	**想定脅威に対するセキュリティ対策の対応づけ**【3.2.2】	どのようなセキュリティ対策が対応づけられるのか整理する。脅威に対応するためには物理面、システム構成面どちらか一方でなく双方の対策が重要となるため、参照されたい。

g. 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(PDCA サイクルの実施)

ステップ 3 ではライフサイクルでの対策、及びサプライチェーンを考慮した対策を実施する。

(1)ライフサイクルでの対策

① 運用・管理面のセキュリティ対策

A)サイバー攻撃の早期認識と対処(OODA プロセス)

サイバー攻撃に起因するシステムの異常を早期に検知・把握するために、機器からのアラート、計測値、指示値の挙動などから、通常と異なる兆候に気付き対処する一連の運用業務にサイバー攻撃の視点での監視を加えることが考えられる。また、迅速な対処を実現するために、異常の兆候や問題・被害の発生を想定し、あらかじめ役割・体制や手順を整備しておくことが考えられる。

B)セキュリティ管理(ID/PW 管理、機器の設定変更など)

セキュリティ対策を運用する上で必要な管理作業として、下記に挙げるような運用ルールやそれに基づく標準的な手順の作成・実施と、関係者への徹底を行うことが考えられる。

これらの管理を実施していくため、利用者等に対して、機器や媒体の利用や入退室等に関わる運用ルールに関して、周知・教育を定期的に行うことが望ましい 。

なお、ヒューマンエラーへの対策として、セキュリティに関する業務に対する過失や疲労への対策、及びセキュリティに関するルールや意識付け・教育の不備等への対策についても考慮することが望ましい。

C)情報共有

サイバー攻撃に関する情報の入手を適時に行うことは、個社の適切な備えや効果的なセキュリティ対応につながり、個社が入手したサイバー攻撃に関する情報を業界や政府に提供することは、業界や社会全体でサイバー攻撃から防御することにつながる。

※業種や対象によって入手可能な情報に差があることに留意。こうした状況にあって可能な限り情報を入手・共有するためには、脅威情報や効果的な対策等、各社の対策に資する情報について、業界やコミュニティ等を通じて情報共有を行うことが望ましい。

② 維持・改善面のセキュリティ対策

セキュリティ対策の実施・運用状況とその効果を確認した上で、工場システムを取り巻く環境の変化に関わる情報を収集し、BC/SQDC 確保の観点も踏まえて、セキュリティ対策を評価し、必要に応じて物理面、システム面、運用・管理面のセキュリティ対策を見直し、更新する。

(2)サプライチェーン対策

- サプライチェーンの広がりとともに、大企業から中小企業までが関わるサプライチェーンの中でも、セキュリティ対策が進んでいない企業がサイバー攻撃によって狙われる事例が増加。
- 対策予算や人材に限りがある中小企業においても、自分たちの事業を守るために工場におけるセキュリティ対策を進める必要。
- グローバル化の進展の中で、サプライチェーンもグローバル化しているため、グローバルなビジネスを行っている企業は、世界情勢の考慮や、各国の法制度あるいは標準規格やガイドライン等に準拠した対策を進める必要。

サプライチェーンにおけるセキュリティリスクは、一つの工場内に閉じずに、エンジニアリングチェーン、サプライチェーンバリューチェーンの連携先まで影響を及ぼし得ることから、サプライチェーン全体でのセキュリティ対策を検討することが重要。

図 2.1-3 ステップ3の概要

h. チェックリスト

工場ガイドラインでは、特に実施して欲しい対策について、具体的な実施内容をイメージし、対策ができているか確認するためのチェックリストを付録として用意し、5 カテゴリ、5 段階の達成度で提示している。

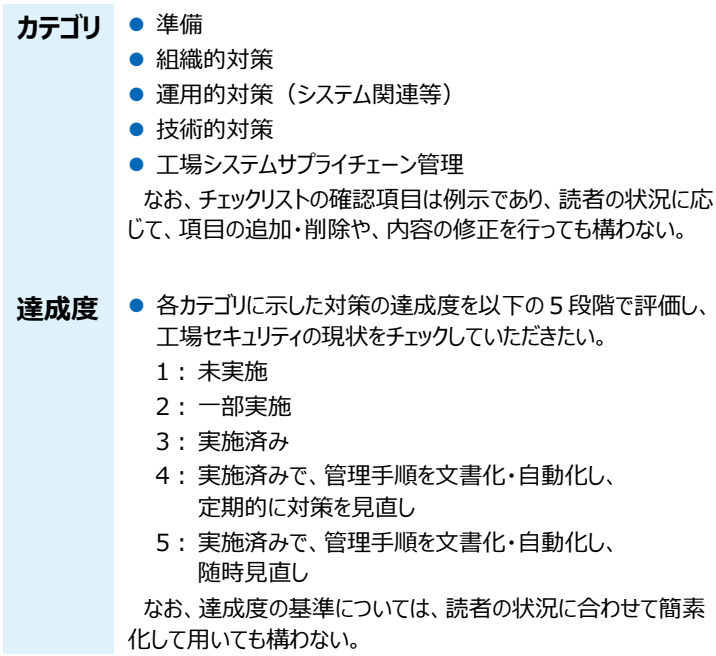


図 2.1-4 対策についてチェックするための 5 つのカテゴリと5段階の達成度

表 2.1-16 付録 E チェックリスト

カテゴリ	番号	確認項目	達成度	参照
準備	0-1	工場システムにおけるセキュリティ対策の検討・企画に必要な経営目標、外部要件、内部要件/状況を整理する。		3.1.1 ステップ 1-1
	0-2	工場システムにおける業務・保護対象の整理及び重要度の設定を行う。この結果を踏まえてゾーンを設定し、業務・保護対象を結びつけ、セキュリティ脅威との影響の整理を行う。		3.1.1 ステップ 1-2 ～ステップ 1-7
	0-3	工場システムに関する内外の要件や、業務・保護対象・ゾーン等の情報の収集・整理結果に基づき、工場システムのセキュリティ対策方針を策定し、想定脅威に対する対策の対応づけを行う。		3.2 ステップ 2-1 ステップ 2-2
組織的対策	1-1	工場システムのセキュリティの必要性について、決裁者（工場長、カンパニー長等）又は経営層が認識を持っており、十分な予算・人員配置などの協力を得られる状態にある。		3.1.1(3) 内部要件／状況の整理

	1-2	工場システムのセキュリティ対応について情報システム部門や生産関係部門等の関係する部署・部門との間で協力・連係態勢が取られている。		3.1.1(3) 内部要件／状況の整理
	1-3	工場システムのセキュリティ検討組織や、担当者が準備されており、責任と業務内容が明確化されている。		3.1.1(3) 内部要件／状況の整理
	1-4	事業継続計画（BCP）が策定されており、工場のセキュリティ事故発生時の担当者が準備されていて、責任と業務内容が明確化されている。		3.1.1(1) 経営目標等の整理 3.1.1(3) 内部要件／状況の整理
	1-5	工場セキュリティに関する脅威の動向などについて、定期的に情報提供を受けたり、勉強会を開いたりするなどの現場教育を行っている。		3.3(1) ライフサイクルでの対策
運用的対策（システム関連等）	2-1	システムが侵害・停止した場合の事業に対するリスクを検討している		3.1.1(1) 経営目標等の整理
	2-2	工場システムにおける専用のセキュリティポリシーが規定されていて、認知されている。		3.1.1(3) 内部要件／状況の整理
	2-3	工場内のシステムからの電子メールやインターネットアクセスはポリシーによって禁止している。		3.1.1(3) 内部要件／状況の整理
	2-4	工場システムにおけるセキュリティの異常発生時の責任者の対応が明確化されている。		3.1.1(3) 内部要件／状況の整理
	2-5	工場システムにおけるセキュリティの異常発生時の対応方法を現場作業者が理解し、訓練を実施している。		3.3(1) ライフサイクルでの対策
	2-6	情報資産の検出ツールを利用するなど、工場ネットワークに接続している機器（サーバ、クライアント端末、ネットワーク機器、設備等）の台帳を作成し、システム構成図を作成している。		3.1.4 保護対象の整理
	2-7	工場内に無線 LAN を導入している場合、ネットワークへの接続を許可された機器の台帳を作成し、無許可の機器を拒否する仕組みがある。		3.1.4 保護対象の整理 3.2.2(1) システム構成面での対策
	2-8	システムへの侵入を可能とする攻撃手法や脆弱性を特定し、脆弱性へ対応している、又は緩和策を講じてい		3.2.2(1) システム構成面での対策

		る。(脆弱性を特定する手法の例:定期的な脆弱性診断やペネトレーションテスト(侵入可否検査)、組込機器(PLC や IoT 機器など)のモデル情報やファームウェア情報の把握及び脆弱性情報の定期的な確認等(※1))		
	2-9	工場内に外部記録媒体(USB メモリ、フラッシュデバイス)やポータルメディアの利用・持込みに関するルールを定め、運用している。		3.3(1) ライフサイクルでの対策
	2-10	工場内のシステムのパスワードの強度や有効期限等のパスワード設定の考え方を定めたルールがある。(安全に関わる緊急対応を必要とする表示器などの端末は除く)		3.2.2(1) システム構成面での対策
	2-11	工場内のシステムへのアクセス権で使用していない古いアカウント(退職者・異動者など)を速やかに削除している。		3.2.2(1) システム構成面での対策
	2-12	工場ネットワーク内の接続機器について、事前にそれらがウィルスに感染していないことを確認する手順がある。		3.2.2(1) システム構成面での対策
	2-13	システム機能の完全な復旧を想定したバックアップを行い、バックアップデータは保護された場所に格納するとともに、定期的にバックアップデータからの復旧テストを行っている。また、その手順が明確化されている。		3.2.2(1) システム構成面での対策
技術的対策	3-1	インストールできる端末にはアンチウィルスソフト又はアプリケーションホワイトリスト(許可リスト)を導入し、インストール不可能な端末では何らかの代替策(USB 型のアンチウィルスなど)を導入している。		3.2.2(1) システム構成面での対策
	3-2	アプリケーション/オペレーティングシステム(OS)の重大な脆弱性については可能な限り速やかにセキュリティパッチを適用している。もしくは代替策を講じている。		3.2.2(1) システム構成面での対策
	3-3	端末のオペレーティングシステム(OS)の使用サービスやアプリケーションは必要最小限とし、未使用のサービスやポートは停止・無効化している。		3.2.2(1) システム構成面での対策

	3-4	工場の重要設備への物理的なアクセスについてレベル分けなどの十分な対策を行っている（例：監視カメラ、警報装置）。又は、入退室管理、外部の入室者への関係者の付添いなど運用面での代替策を講じている。		3.2.2(2) 物理面での対策
	3-5	工場ネットワーク内において、セキュリティレベルに応じたネットワークセグメント管理を行っている（VLAN 等）。		3.2.2(1) システム構成面での対策
	3-6	工場システムのリモートメンテナンスなどを目的とした外部からのインターネットアクセスが可能な場合、認証（2要素認証等）やリモートユーザ毎の接続対象機器(※2)の制限、接続可能時間の制限、メンテナンス期間外の機器接続等の異常検知、ネットワーク侵入防護などの保護対策を行っている。		3.2.2(1) システム構成面での対策
	3-7	工場内のネットワーク（情報システムとの境界やリモートアクセスを含む）の不審な通信を特定するためのネットワーク検知／防護システムを導入している。		3.2.2(1) システム構成面での対策
	3-8	工場内のシステムのログイン、操作履歴などのイベントログを取得している。それらのログは定期的に分析し、必要日数保存している。		3.2.2(1) システム構成面での対策
工場システムサプライチェーン管理	4-1	工場システムのセキュリティ事故発生時に対応ができるよう、制御システムベンダ・構築事業者と連絡・連携体制を構築している。		3.3(2) サプライチェーン対策
	4-2	工場システムのメンテナンス等に関わる協力会社向けのセキュリティ教育を契約開始時及び定期的に実施している。		3.3(2) サプライチェーン対策
	4-3	納品された工場システムに関するセキュリティの脆弱性が発見された場合、その情報が速やかに共有されるように、制御システムベンダ・構築業者との連絡・連携体制を構築している。		3.3(2) サプライチェーン対策
	4-4	サプライチェーン（協力会社、生産子会社など）における工場システムの脅威、影響度、対応状況（内部及び/または外部監査実施など）を把握できている。		3.3(2) サプライチェーン対策

	4-5	納入する工場システム機器に対して、一定のセキュリティ基準を満たしているかを判定するプロセスや受入検査がある。		3.3(2) サプライチェーン対策
	4-6	新規システム導入時の設計仕様要件にセキュリティに関する要求仕様が明確化されている。		3.3(2) サプライチェーン対策

i. 調達仕様テンプレート

工場ガイドラインでは、セキュアな工場を構築するためには、工場で使用する製品・サービスを調達する際に、あらかじめセキュリティに関する要件をサプライヤーに提示し、その上で調達契約を締結することが重要であるとして、製品・サービスの調達時に考慮すべきセキュリティ要件についての調達仕様書の記載例も提示している。

例１：制御機器サプライヤへのセキュリティ要件指定の例

X.X　サプライヤが備えるべきセキュリティ要件
　「中小企業の情報セキュリティ対策ガイドライン第3版（IPA）」を自己評価し、
　SECURITY ACTION の二つ星を宣言していること。

　また、(2)、(3)については、サプライヤから調達する製品・サービスの個別のセキュリティ要件である。(2)は、製品・サービスが備えるべきセキュリティ要件である。例えば、工場内で用いられる機器であれば、権限に応じたアクセス管理、ログイン認証等、達成したいセキュリティ強度に応じて、機器に必要なセキュリティ機能を列挙することになる。

例２：PLCの調達仕様書のセキュリティ要件指定の例

X.X　ペネトレーションテストの実施
　公開されている脆弱性や攻撃手法を用いたペネトレーションテストを実施し、
　セキュリティリスクを低減するための対策を行うこと。

　PLCのような制御機器は、セキュリティ機能を実装するだけの物理的なリソースがない場合がある。その場合、サプライヤから情報を取得して、調達する機器が満たしている要件と、追加対策が必要な要件と実装方法を明確にすることが重要である。そうすることで、リスクを把握した上で、一時的にリスク受容するなど、柔軟な選択を行うことができる。

　次に、(3)は、製品・サービスのライフサイクル関するセキュリティ要件である。これらの要件は、製品・サービスの開発、製造、流通、運用、廃棄といったライフサイクル上で発生するセキュリティリスクを低減するための要件である。調達する機器によっては、ここまでの要件を求めない場合もあるため、必要に応じて取捨選択していただきたい。

例３：PLCの製品ライフサイクルに関するセキュリティ要件指定の例

X.X　開発時のセキュリティ要件
　X.X.1　開発環境
　　X.X.1.1　開発人員の管理
　　X.X.1.2　開発環境の物理的なセキュリティ
　　X.X.1.3　開発環境のセキュリティ対策
　　X.X.1.4　開発ソフトウェア管理
X.X　使用するOSSに関するセキュリティ要件
　X.X.1　ライセンス管理の実施
　X.X.2　脆弱性管理の実施
X.X　製造・流通時のセキュリティ要件
　X.X.1　流通時のセキュリティ
　製造拠点からどのような流通経路で納品されたかの記録を保持すること。
　開封シールなど機器の改ざん防止の措置をとること。
X.X　保守・メンテナンス・廃棄時のセキュリティ要件
　X.X.1　バージョン変更時のファームウェア更新
　X.X.2　脆弱性発見時の対応
　　X.X.2.1　報告
　　X.X.2.2　対処

図 2.1-5 調達仕様書の記載例

3）ガイドラインの英訳

「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」については英訳を行い、「The Cyber/Physical Security Framework for Factory Systems」としてとりまとめた。

（2） 工場セキュリティガイドラインの普及啓発及び残存課題の解決に向けた調査

1） 工場セキュリティガイドラインの普及啓発に関する調査

a. アンケート調査概要

工場に関連する 25 の経済産業省所管の業界団体を中心に、工場システムのセキュリティに関する対策・課題・要望の把握と工場セキュリティガイドラインの普及策の検討を目的にアンケート調査を実施した。調査対象・依頼数・有効回答数・調査項目数・調査項目・調査手法・調査期間を表 2.1-17 にまとめた。依頼した業界団体が複数の業界団体から構成される団体等については、1 件の依頼に対して複数の業界団体の回答が得られた場合があり、依頼数と比較して有効回答数が多くなった。

表 2.1-17 業界団体向けアンケート調査概要

調査対象	経済産業省所管の業界団体 配布対象業種： パルプ・紙・紙加工品製造業 生産用機械器具製造業、印刷・同関連業、業務用機械器具製造業、電子部品・デバイス・電子回路製造業、化学工業、石油製品・石炭製品製造業、電気機械器具製造業、プラスチック製品製造業、情報通信機械器具製造業、窯業・土石製品製造業、輸送用機械器具製造業、鉄鋼業
依頼数	25 件
有効回答数	31 件
調査項目数	26 項目
調査項目	A） 団体の属性情報 B） セキュリティ活動状況 C） セキュリティ課題 D） ガイドライン作成 E） ガイドライン認知状況
調査手法	Web アンケート調査（任意回答）
調査期間	2022 年 9 月～2022 年 10 月

b. アンケート結果概要

アンケート結果の一部を概要として以下で紹介する。

ア） 業界団体の属性情報

会員数は、「100 社～500 社未満」が 17 団体と最も多かった。企業規模割合（大企業）は「1～10%」が 7 団体と最も多かった。製造業の割合は、「91%～100%」が 11 団体と最も多かった。

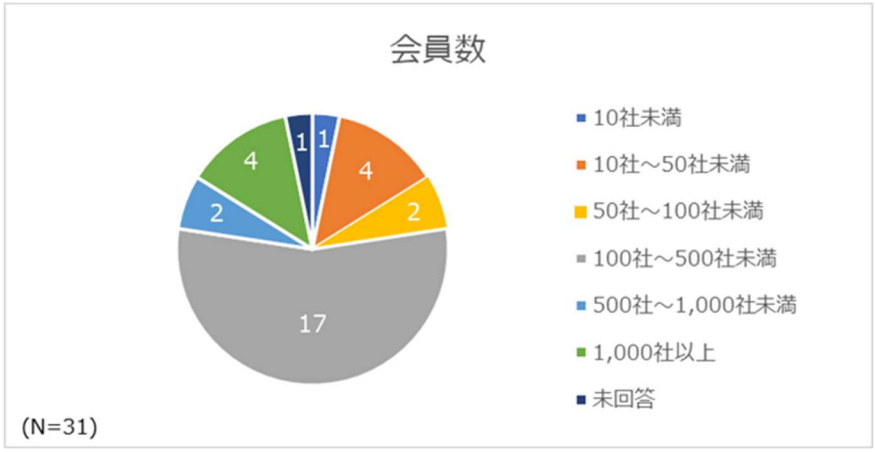


図 2.1-6 業界団体の会員数

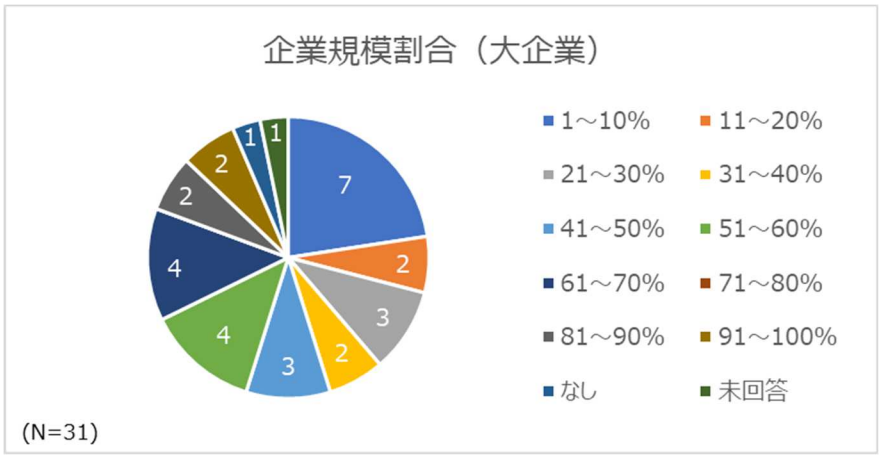


図 2.1-7 業界団体の会員における大企業の割合

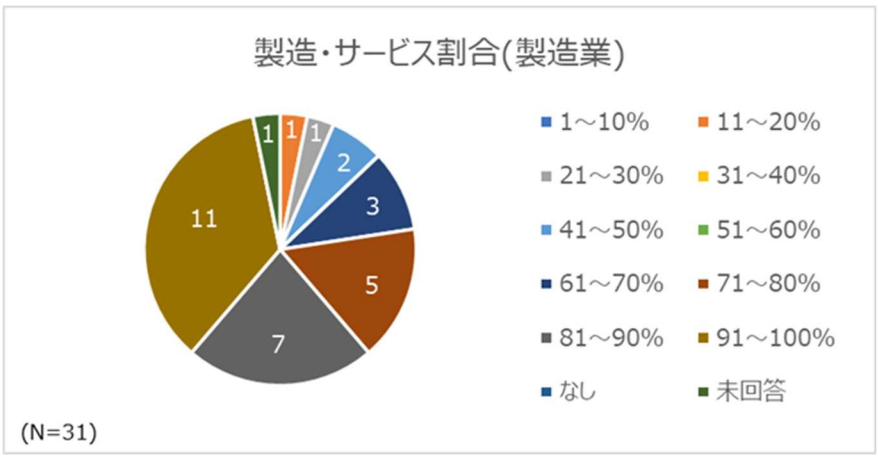


図 2.1-8 業界団体の会員における製造業の割合

イ） 業界団体におけるセキュリティ活動状況

「①国や関係機関等組織からの脅威・インシデント情報等の会員への提供」と「②業界団体が収集した脅威・インシデント情報等の会員への提供」は、半数以上の業界団体が実施している。一方で、「③会員間の情報共有の仕組みの構築・運営」と「④会員のインシデントに関する情報を元にした注意喚起や関

連情報の提供」は、半数未満の業界団体の実施にとどまる。

すなわち、業界団体は、外部組織から収集した情報の提供といった「単一方向の情報共有活動」の実施率は比較的高い一方で、会員間の情報共有といった「双方向の情報共有活動」の実施率は低い傾向にある。また、「会員企業の 58.2%が業界団体に対して情報共有活動を期待している」との調査結果に表れているとおり、会員企業からの業界団体に対する情報共有活動の期待は高い。以上から、「単一方向の情報共有活動」は比較的実施されていることを鑑みると、業界団体は特に「双方向の情報共有活動」に特に力を入れていくことが望ましいと考えられる。

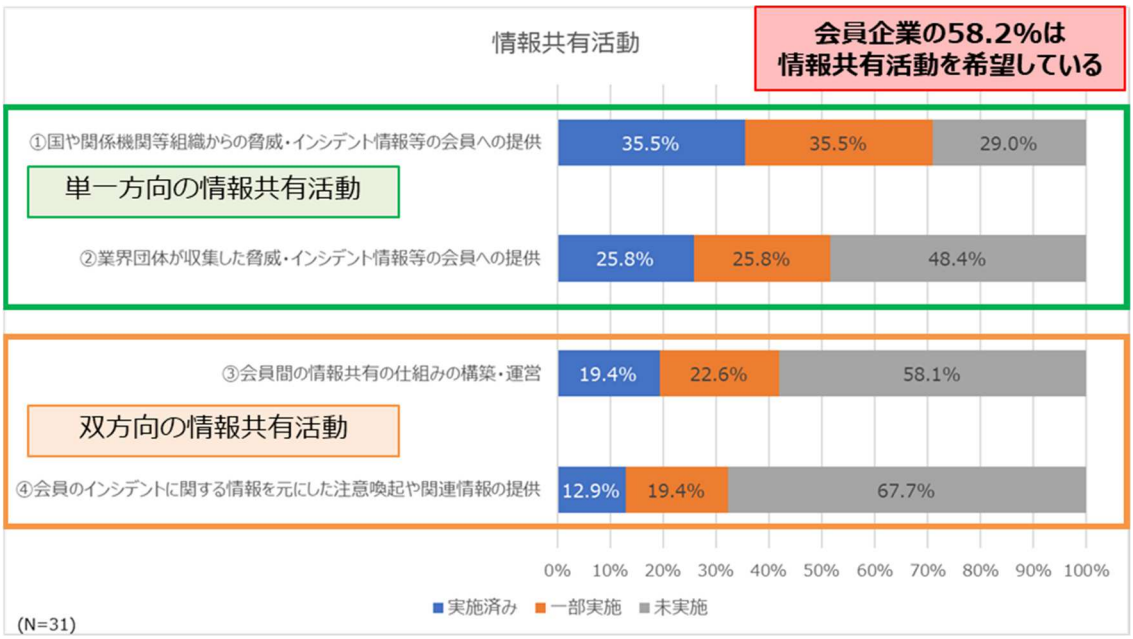


図 2.1-9 業界団体における情報共有活動の状況

「①会員のサイバーセキュリティ対策事例に関する情報共有」を実施している団体は約3割であった、「②サイバーセキュリティ関連製品・ソリューション等の情報提供」を実施している団体は約 2 割、「③インシデント対応に関するマニュアル等作成・提供」を実施している業界団体は約 1 割程度であった。また、「会員企業の 55.9%は業界団体に対して対策事例共有を期待している」との調査結果に表れているとおり、会員企業からの業界団体に対する対策事例共有の期待は高いが、「①他社の対策事例」、「②ソリューション情報」、「③インシデント対応情報」のいずれも業界団体の実施状況は低い。以上から、業界団体は、対策事例共有活動全般について、特に力を入れていくことが望ましいと考えられる。

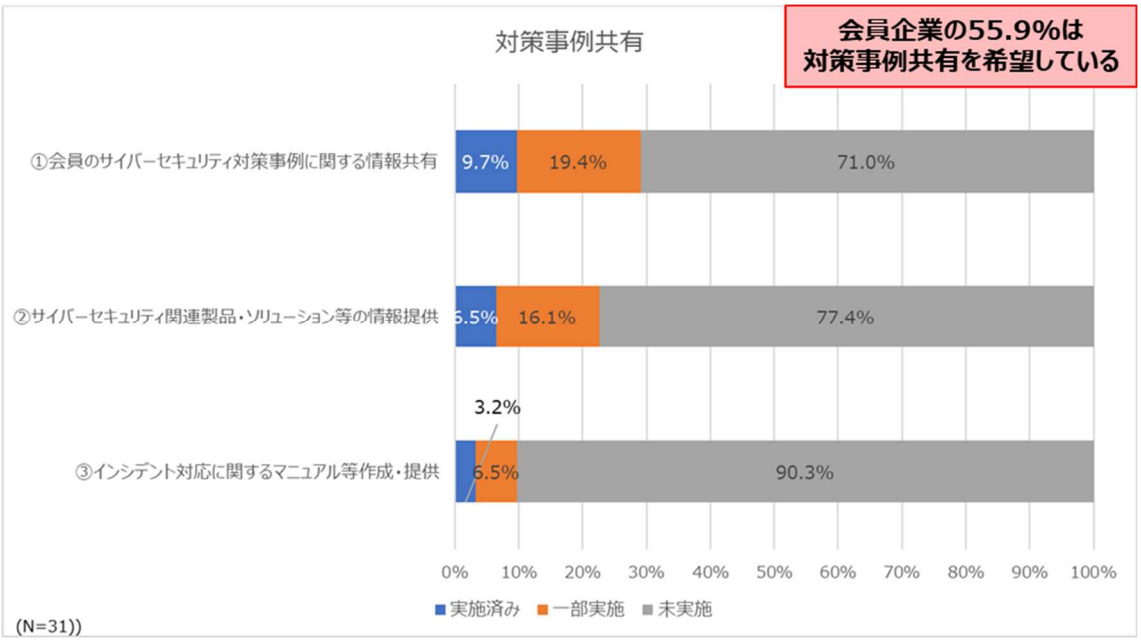


図 2.1-10 業界団体における対策事例共有の状況

「①セキュリティに関する教育・研修、セミナー等の実施」を実施している業界団体が約 4 割、「②サイバーセキュリティ教育コンテンツの作成・提供」を実施している業界団体が約 2 割であった。一方で、「③外部事業者のサイバーセキュリティ演習の提供」、「④業界独自のサイバーセキュリティ演習の企画・実施」、「⑤各社サイバーセキュリティ演習実施方法に関するマニュアル等作成・提供」実施している業界団体は約 1 割程度であった。

したがって、①②のような基本的な人材育成活動が実施されているとは言い難く、とりわけ③④⑤⑥のような実践的なサイバーセキュリティ演習関連の活動はさらに実施されていない傾向にある。ただし、「会員企業の 32.2%は業界団体に対して人材育成を期待している」との調査結果に表れているとおり、他のセキュリティ活動と比較し業界団体に対する期待は低い傾向にある。しかしながら、ニーズが存在する会員企業も存在することから、業界団体と会員企業の間で丁寧かつ詳細なニーズのすり合わせを行っていくことが望ましいと考えられる。

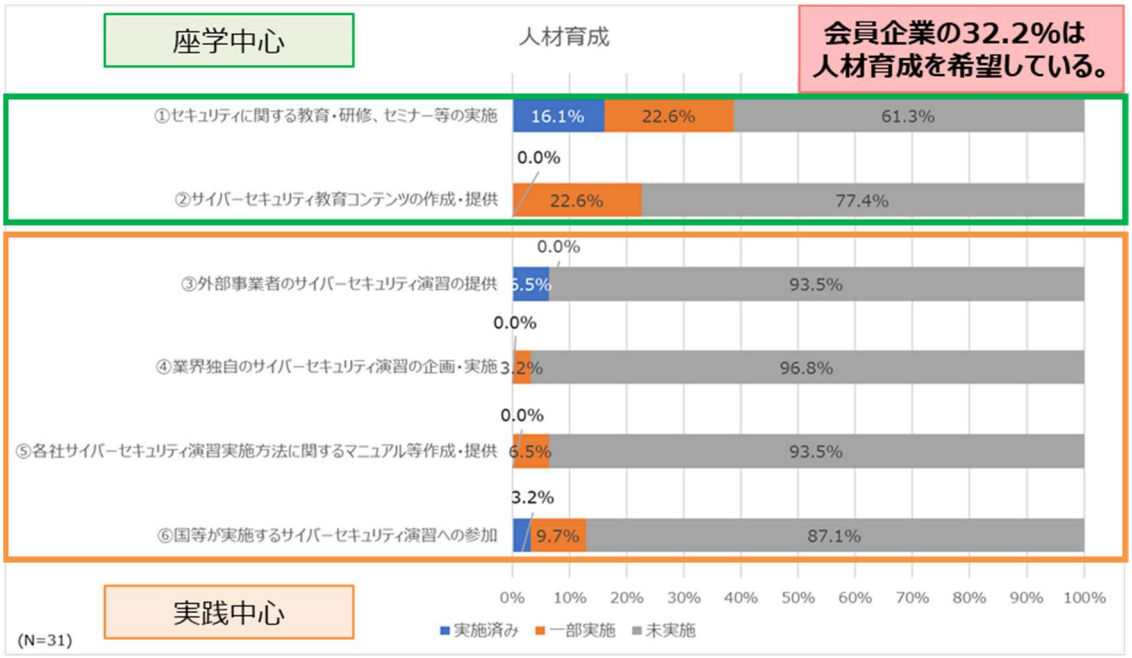


図 2.1-11 業界団体における人材育成活動の状況

「①会員が情報共有を行うための会議体の設置・運用」、「②業界としてのセキュリティ方針・対策を検討する会議体の設置・運用」、「⑤他の業界団体や ISAC 等とのサイバーセキュリティに関する連携」を実施している業界団体は約 4 割であった。一方で、「③インシデント発生時のサポート」「④会員のサイバーセキュリティに関する意識や対策状況等の把握・実態調査」を実施している業界団体は約 1 割であった。

したがって、①②⑤のような業界団体内での基本的な組織設計が実施されているとは言い難く、また特に③④のような会員企業の調査やサポートはさらに実施されていない傾向にある。ただし、「会員企業の 34.8%は業界団体に対してセキュリティ向上活動を期待している」との調査結果に表れているとおり、他のセキュリティ活動と比較し業界団体に対する期待は低い傾向にある。しかしながら、企業のアンケートの自由回答より、特に業界としてのセキュリティ指針やセキュリティ対策の提供が期待されていることから、「②業界としてのセキュリティ方針・対策を検討する会議体の設置・運用」に力を入れることが望ましいと考えられる。

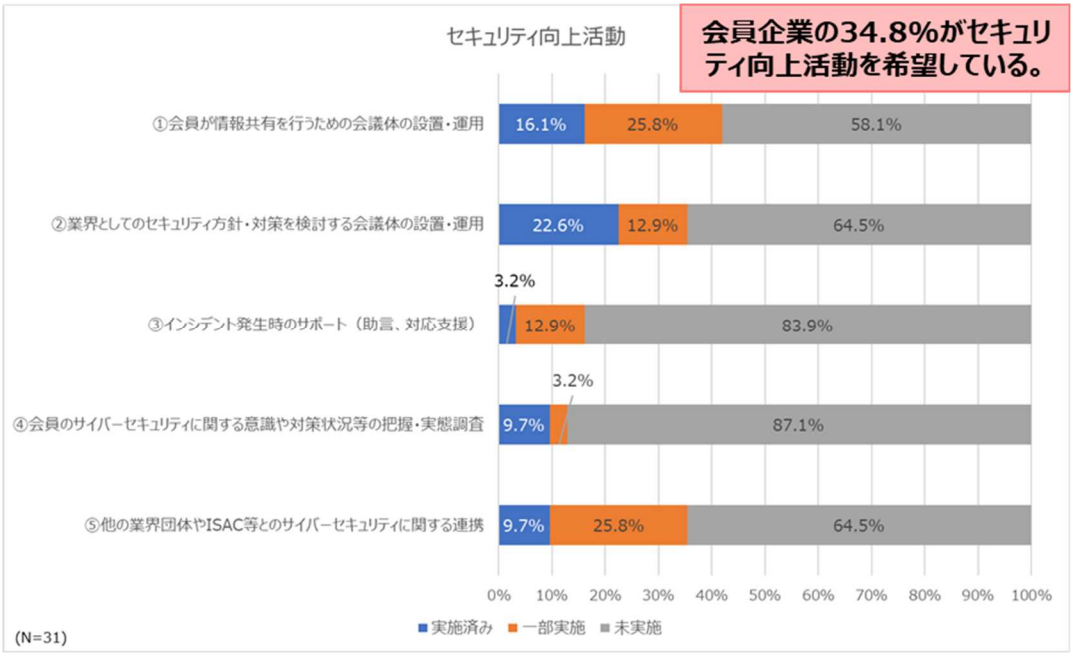


図 2.1-12 業界団体におけるセキュリティ向上活動の状況

ウ）業界団体におけるセキュリティに関するガイドラインの作成状況

「①組織」に関するセキュリティガイドラインについて、「作成・一般公開」、「作成・限定公開」、「作成中」と回答した業界団体は約３割であった。一方で、「②工場」、「③製品」、「④サプライチェーン」に関するセキュリティガイドラインについて、「作成・一般公開」、「作成・限定公開」、「作成中」と回答した業界団体は約 1 割であった。「②工場」は特に作成率が低かった。したがって、①のような基本的な組織設計を会員企業に示すためのガイドの整備が業界団体で実施されているとは言い難い。さらに②③④といった昨今の製造業のサイバーセキュリティを取り巻く脅威に対応するために必要と考えられるガイドの整備については、より一段と実施されているとは言い難い。

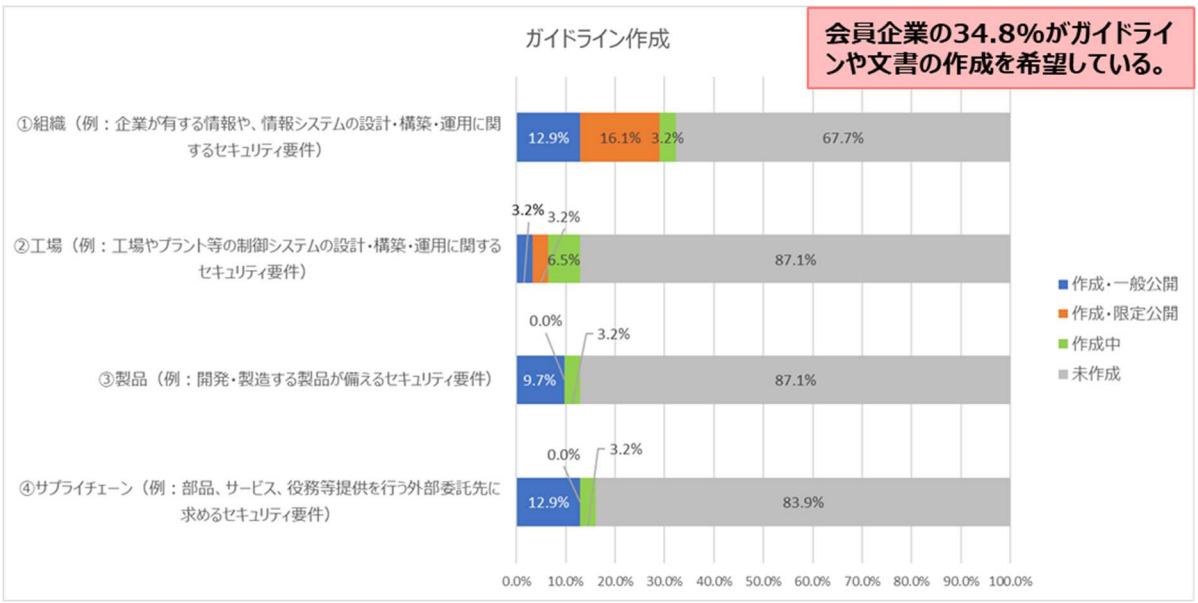


図 2.1-13 業界団体におけるセキュリティに関するガイドラインの作成状況

エ） 工場セキュリティガイドラインの活用状況

工場セキュリティガイドラインの認知状況について、「本アンケートで初めて知った」が 20 団体と最も多かった。工場セキュリティガイドラインの会員周知について、「未実施」が 26 団体であった。工場セキュリティガイドラインの業界ガイドライン作成時の参考情報としての利用や、業界におけるサイバーセキュリティ施策検討への活用については、「未実施」と全ての団体が回答した。

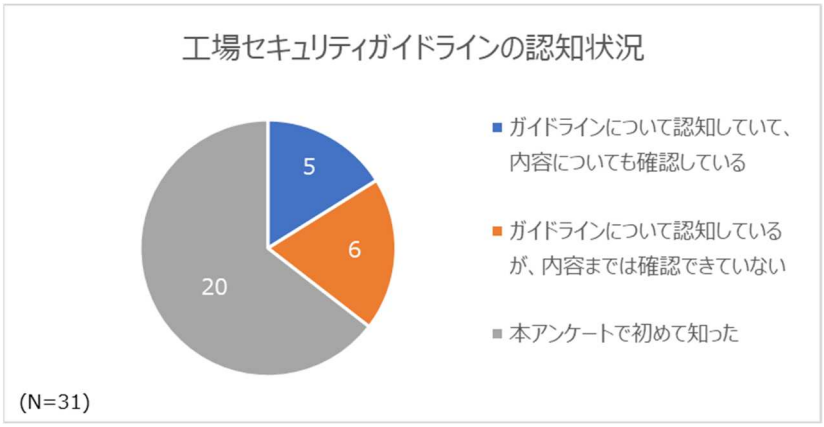


図 2.1-14 業界団体における工場セキュリティガイドラインの認知状況

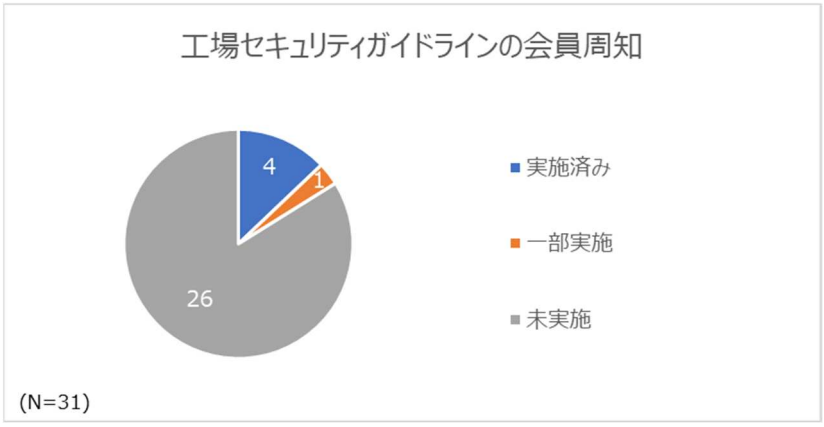


図 2.1-15 業界団体における工場セキュリティガイドラインの会員周知

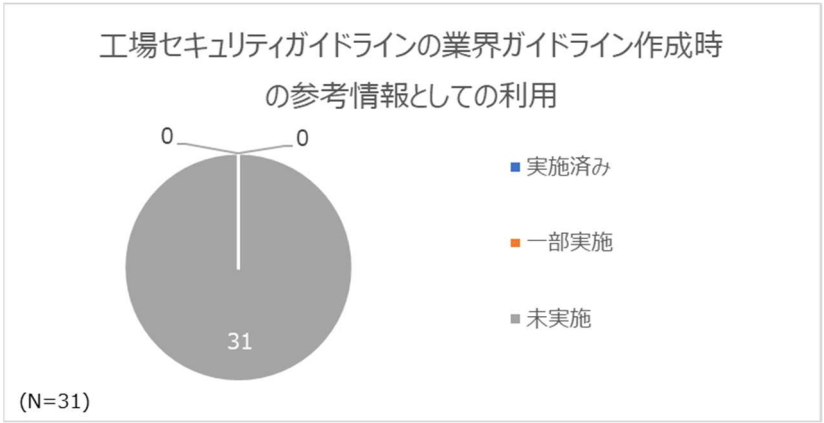


図 2.1-16 業界団体における工場セキュリティガイドラインの業界ガイドライン作成時の参考情報としての利用

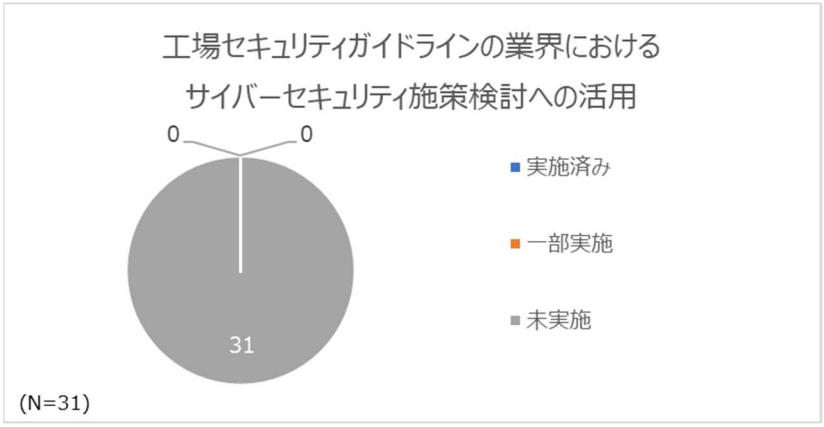


図 2.1-17 工場セキュリティガイドラインの業界における
サイバーセキュリティ施策検討への活用

c. ヒアリング調査概要

アンケートに回答いただいた業界団体のうち、セキュリティ活動状況や会員企業のセキュリティ対策状況を考慮し、10 団体に対してヒアリングを実施した。業界団体のセキュリティ活動状況、会員企業のセキュリティ対策状況、工場ガイドラインに対する意見、工場ガイドラインの普及活動等について、より具体的な内容を調査した。調査対象・ヒアリング件数・調査項目数・調査項目・調査期間を表 2.1-18 にまとめた。

表 2.1-18 業界団体向けヒアリング調査概要

調査対象	経済産業省所管の業界団体
ヒアリング件数	10 件
調査項目数	13 項目
調査項目	A） 業界団体のサイバーセキュリティ活動状況・展望 （サイバーセキュリティ活動内容・活動経緯・課題・影響など） B） 会員企業におけるサイバーセキュリティ対策状況・展望 （サイバーセキュリティ対策状況・対策の実施理由など） C） 工場セキュリティガイドラインについて （工場セキュリティガイドラインの難易度・活用可能性など） D） 工場セキュリティガイドラインの普及に向けた活動について （工場セキュリティガイドラインの周知や支援策への協力など）
調査期間	2022 年 12 月～2023 年 2 月

d. ヒアリング結果

ヒアリング対象の業界団体では、セキュリティ対策が進んでいる会員企業から構成される会議体を設立し、セキュリティに関する検討を行うケースが複数確認できた。業界団体がセキュリティ活動を推進する一方、セキュリティ活動による効果や影響を確認できていない業界団体が半数以上であった。セキュリティ活動の効果や影響を確認するために有効な会員企業のセキュリティ実態の把握ができていないことも影響していると考えられる。

セキュリティ課題として OT セキュリティに関する課題が挙げられた。OT セキュリティ対策の必要性を

経営層が認識できていない点や IT・OT の部署の連携が実施できていない点などが具体的な課題として挙げられた。業界の統一的な基準を作成する上での課題も複数確認できた。特に規模が異なる企業が含まれるサプライチェーン全体において、業界の統一的なセキュリティ基準を策定することが難しいという課題が挙げられた。

表 2.1-19 ヒアリング結果概要

設問	カテゴリ	意見
業界団体における サイバーセキュリティ 活動状況	会議体の設置	● インシデント報告を受け、業界全体としての対策が必要という認識が生まれ、特定製品のセキュリティに関する委員会を設立している。 ● 業界内のインシデントや昨今のニュースを受け、セキュリティに関する分科会や工場セキュリティタスクフォースを設立し、セキュリティ活動を推進している。 ● 業界の主要企業と会議体を立ち上げ、業界基準に則った業界専用の規則を整備している。 ● 技術課題の検討と育成の取り組みを会員企業を募集した会議体を立ち上げて実施している。 ● 喫緊の課題として認識し、特定製品のセキュリティに関する分科会を設立している。
	ガイドラインの構築	● 重要インフラ業界として、サイバーセキュリティ活動を行うのは重要であると認識し情報セキュリティに関する安全ガイドラインを策定している。 ● 業界専用のガイドラインを作成し、サプライチェーンでのセキュリティ対策状況を確認するために活用している。
業界団体のセキュリティ活動が与えている 効果や影響		● 具体的な効果や影響については把握できていない。 ● 情報共有の会合にて、CSIRT 構築含めて近年セキュリティ報告が増えていると感じている ● 自社のセキュリティ対策状況を業界ガイドラインをベースに自己採点してもらい、その結果を収集し分析している。ガイドラインの浸透具合を実感している。
業界が抱える セキュリティ課題	IT・OT の連携不足	● セキュリティ対策への意識は向上しているが、IT セキュリティと OT セキュリティを実施する部署の連携が取れていない。
	OT セキュリティの検討	● IT のセキュリティ対策は世の潮流に沿って実

	不足	施できている企業が多い一方、OT セキュリティ対策の必要性を経営層が認識できていない。 ● IT 以外のセキュリティについて、検討を進めきれていない。
	業界統一基準策定の困難さ	● セキュリティ対策について、基準が乱立しないよう業界としての統一的な基準作成が求められている。 ● 様々な規模の企業が所属する中、サプライチェーンを個社の取組ではなく、業界全体の取組として取り上げる必要がある。 ● サプライチェーン全体で利用できる統一的な基準を整理するのが難しい。
	その他	● 自社のセキュリティの取組が他業界や他社と比較してどのレベルにあるかについて関心が高いが、認識できていない。 ● 会員企業からの情報共有について概要以上について紹介いただけない。 ● 中小企業におけるセキュリティ対策の推進が難しい。

e. 普及啓発の方向性

業界団体のアンケート調査の結果、工場セキュリティガイドラインの認知率・普及率が業界団体で低く、普及の底上げを図ることが必要であることを確認した。普及の底上げに向けて、以下の普及策を検討していくことが望まれる。

- SC3の活動と連携し工場ガイドを業界団体に対して周知
- セキュリティベンダや IPA など各者が実施するセミナー等を活用した周知
- 関係省庁（デジ庁デジタル臨調等）や業所管部局との連携、継続的なフォローアップ

また、業界団体のセキュリティ活動と会員企業が業界団体に期待するセキュリティ活動を比較したところ、以下のセキュリティ活動を優先的に実施することが効果的だと考えられる。下記のセキュリティ活動を実施するとともに工場セキュリティのテーマを取り上げることで工場セキュリティの底上げに繋がると考えられる。

- 会員企業間における業界独自の情報を中心とした情報共有活動
- 会員のサイバーセキュリティ対策事例の共有
- 具体なテーマに関するガイドラインの作成

ヒアリング結果より、業界独自の情報や会員の対策事例に関する情報共有の会合に関する事例を確認できた。また、ガイドラインの作成に向けた活動に関しても複数確認できた。

2）工場セキュリティに関する残存課題の解決に向けた調査

a. スマートファクトリーにおけるセキュリティ検討の必要性

現行の「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」については、各業界・業種が自ら工場のセキュリティ対策を立案・実行することで、産業界全体、とりわけ工場システムのセキュリティの底上げを図ることを目的として作成した。

しかし、工場のスマート化が進むにつれて、制御システムにおけるシステムアーキテクチャが変化していくことや、外部との連携が深まることでサプライチェーンの脅威が増すことから、工場がクラウドやデジタルツインといったサイバー空間に密接に繋がっていく世界におけるセキュリティのあり方を検討することが必要である。

スマートファクトリーは、新たなニーズへ対応した商品やサービスの迅速な提供を実現できるなど、製造業のビジネス競争力を強化する源泉である。工場のスマート化を進めていくためには、付随するリスクを管理するための考え方や対応のあり方を検討する必要性が生じていると考えられる。

具体的には、汎用品活用への対応、外部連携対応、新たな制御モデルへの対応について検討が必要であるとともに、スマートファクトリーに対応できる人材のあり方について、検討を進めていくことが必要と考えられる。また、汎用品の活用や連携の増加に伴い、サプライチェーンで考慮しなければいけない事項も変化・増加し得ることから、スマートファクトリー特有のサプライチェーン対応についても、検討を進めていくことが必要と考えられる。

加えて、戦略的イノベーション創造プログラム（SIP）においてもスマート工場のセキュリティに資する技術開発がなされていることから、こうした技術との連携も模索していくことが効果的と考えられる。

これらに対応したガイドを通じ、先進的な事業者が臆することなく工場のスマート化を進め、「稼げる工場化」を促進することを後押ししていくことが必要である。

b. スマートファクトリーを考慮したセキュリティガイドに期待する効果

工場セキュリティガイドラインのパブコメにおいては、インターネット接続やクラウド利用、サプライチェーンにおけるセキュリティ確保に関する御意見が複数者から挙げられたことからも、関心は一定数存在することが想定される。

パブコメでの意見は以下の通り。

＜インターネット接続やクラウド利用、工場間の接続に関する御意見＞

- 制御ゾーンや生産管理ゾーンから直接インターネットへ接続する経路を記載してはどうか。【セキュリティ会社】
- 制御ゾーンの機器をリモートでメンテナンスしたり、生産性分析業務を外部クラウドで行ったりすることも増えている。外部ネットワークとの接続も想定すべきではないか。【印刷】
- 想定工場のシステムでクラウドに関する指針を示してほしい。【個人】
- 自動倉庫の遠隔保守以外は拠点内に閉じているため、インターネット接続やクラウド技術の使用も想定に加える必要はないか。【工作機器】
- 拠点間の脅威や被害拡大・対策の意識を強めてもよい。【製造】

＜サプライチェーンに関する御意見＞

- Society5.0 では、柔軟で動的なサプライチェーンの構成が可能だが、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という新たなリスクへの対応が必要となっている。【セキュリティ会社】
- 工場 DX の推進により、ソフトウェアやクラウドが導入されていく製造環境、サプライラーと連携した製造環境に必要なセキュリティ対策の必要性を追加することが望ましい。【セキュリティ会社】

また、国内のスマートファクトリー市場は主要 10 カ国で見ても大きく、様々な分野の製造業においてスマート化や DX 化の事例も見られる。

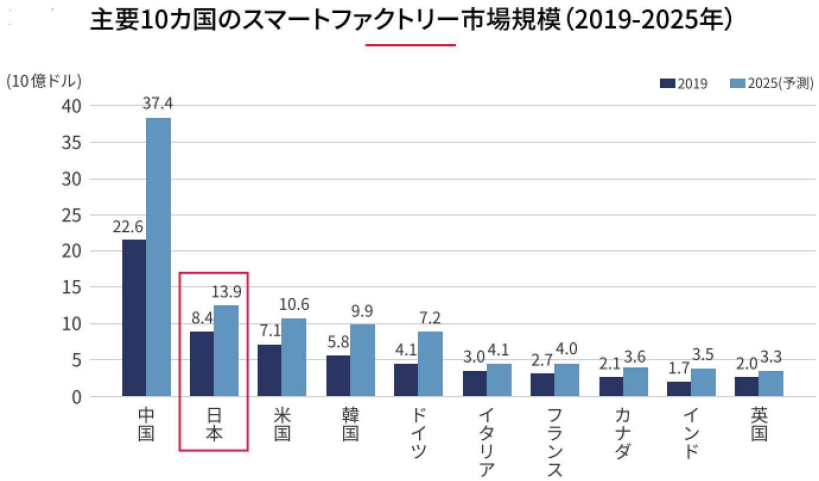


図 2.1-18 主要 10 カ国のスマートファクトリー市場規模（2019-2025 年）
「INVEST JAPAN 製造業」（JETRO）において BIS Research のデータを元に作成

表 2.1-20 製造業 DX 取組事例

株式会社今野製作所（油圧機器）	株式会社ダイセル（化学）
沖電気工業株式会社（通信機器）	三菱電機株式会社（総合電機）
富士通株式会社（総合 IT ベンダー）	ヤマハ発動機株式会社（輸送用機器）
オークマ株式会社（工作機器）	ビジネスエンジニアリング株式会社（システムベンダー）
トヨタ自動車株式会社（自動車）	川崎重工業株式会社（重工業）
三和工機株式会社（工作機器）	オムロン株式会社（産業機器）
株式会社アイデン（制御盤）	ダイキン工業株式会社 （空調機）
株式会社 IHI（重工業）	

「製造業 DX 取組事例集」（経済産業省）を元に作成

2.1.2 工場等におけるサイバーセキュリティ対策関連調査

（1） 各産業分野の特性に応じた工場のサイバーセキュリティ関連動向等の調査

1） アンケート調査概要

アンケート調査対象とした業界団体（25 団体）に依頼を行い、会員企業を対象に、工場システムのセキュリティに関する対策・課題・要望等を把握することを目的に任意のアンケート調査を実施した。調査対象・有効回答数・調査項目数・調査項目・調査手法・調査期間を表 2.1-21 にまとめた。また、業界団体経由のため、企業への正確な依頼数は把握できないが、回答のあった企業が所属する業界団体の会員企業数を合計すると約 2,700 件であり、これが概ねの依頼数と想定される。

表 2.1-21 会員企業へのアンケート調査概要

調査対象	経済産業省所管の業界団体の会員企業
有効回答数	397 件
調査項目数	71 項目
調査項目	A） 回答者の属性情報 B） 基本セキュリティ対策 C） セキュリティインシデント D） 工場におけるデータ分析 E） 工場におけるリスク分析 F） 工場におけるセキュリティ体制 G） 工場における外部委託状況 H） 工場における具体のサイバーセキュリティ対策 I） サイバーセキュリティ全般における課題や要望について J） 工場セキュリティにおける課題や要望について K） OSS の対策
調査手法	Web アンケート調査（任意回答）
調査期間	2022 年 9 月～2022 年 10 月

2） アンケート結果概要

アンケート結果の一部を概要として以下で紹介する。

a. 企業回答者の属性情報

業種について、「その他」（60 社）が最も多いが、それ以外では「輸送用機械器具製造業」（59 社）、「生産用機械器具製造業」（56 社）、「非鉄金蔵製造業」（50 社）が多い。

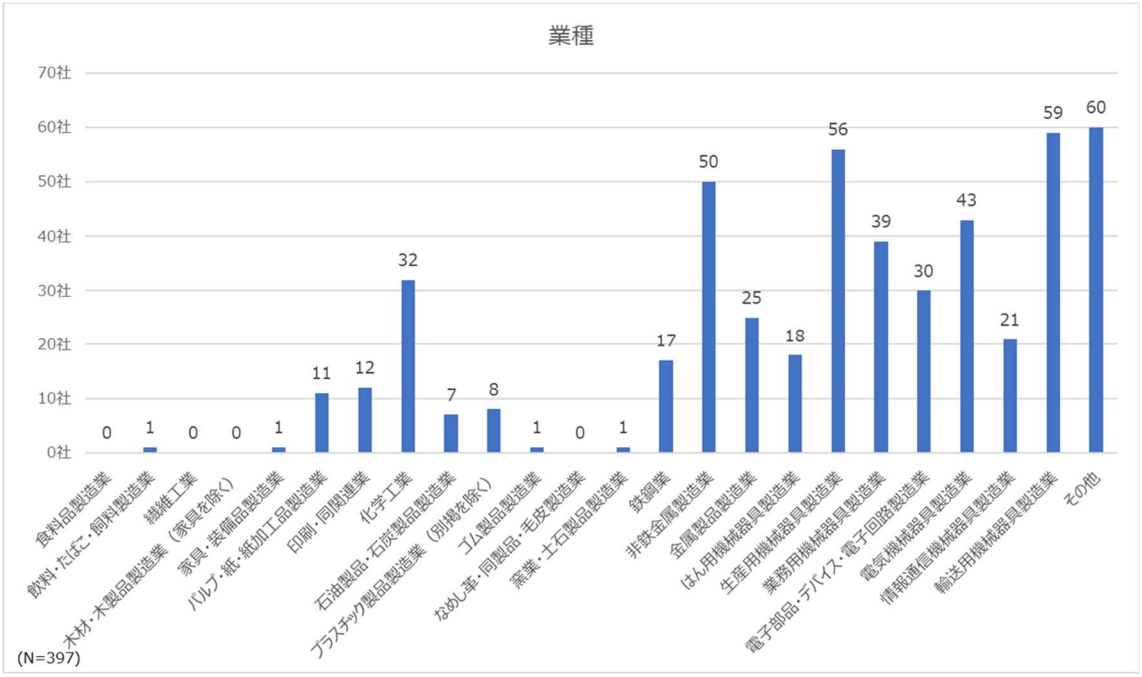


図 2.1-19 回答企業の業種

総従業員数が 300 名未満と回答した企業は 38.6%であった。取り扱っている製品種類数は、100 種未満が 37.4%であった。国内工場数について、「5 ヶ所未満」が 66.5%と最も多かった。国外工場数について、「所持していない」が 51.1%と最も多かった。

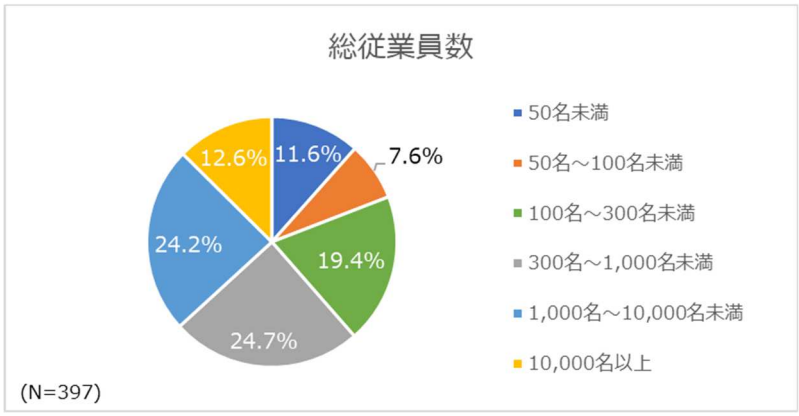


図 2.1-20 回答企業の総従業員数

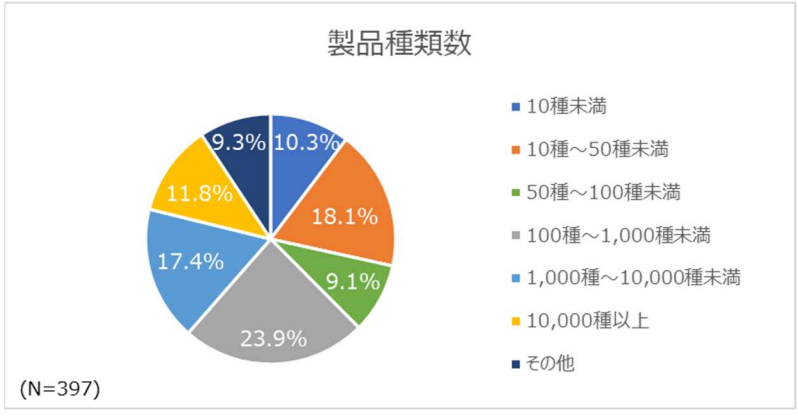


図 2.1-21 回答企業の製品種類数

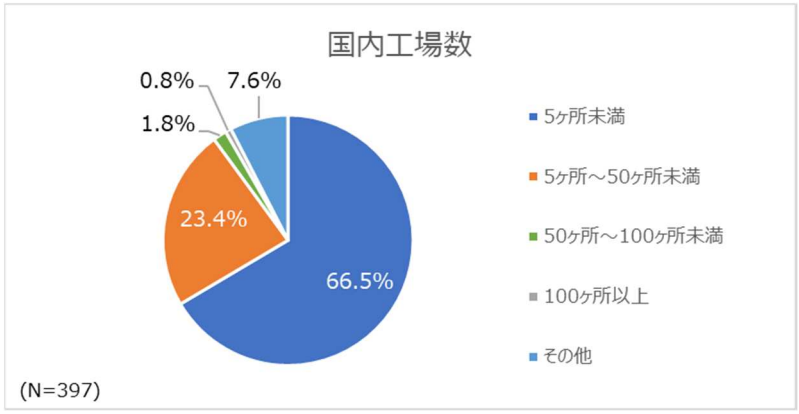


図 2.1-22 回答企業の国内工場数

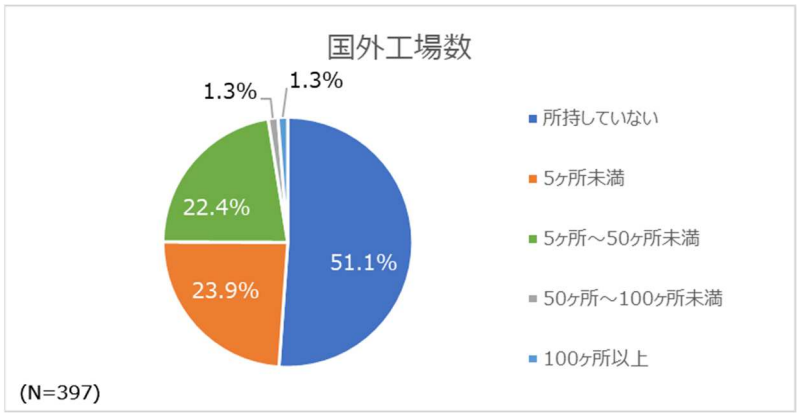


図 2.1-23 回答企業の国外工場数

b. 売上規模及び各 IT・セキュリティ関連の予算額

年間総売上規模が 10 億円未満と回答した企業は 13.2%であった。IT 予算額は、「1 億円～10 億円未満」が 25.4%と最も多かった。セキュリティ予算額は、「1,000 万円～1億円未満」が 23.9%と最も多く、次いで 100 万円未満が 20.4%であった。工場のセキュリティ予算額は、100 万円未満が 23.7%と最も多かった。また、不明が 27.5%であった。

工場セキュリティ予算額が「～100 万円未満」の企業のうち、47.9%の企業が、「工場システムのサイバーセキュリティ予算額が少ない」ことを工場セキュリティの課題に挙げていた。これらの企業が具体的にどのような課題認識を持っているかの設問は、本アンケートに含まれていない。「不明」と回答した理由の可能性としては、工場におけるセキュリティ予算額が切り出されていない、本社側で工場側の予算を把握していない、アンケート調査の回答者が企業の IT を中心に担当する者であったため把握できていない、等が推察される。

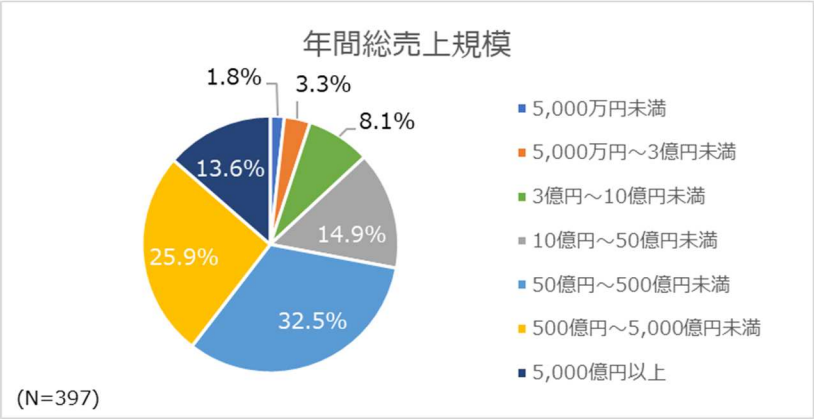


図 2.1-24 回答企業の年間総売上規模

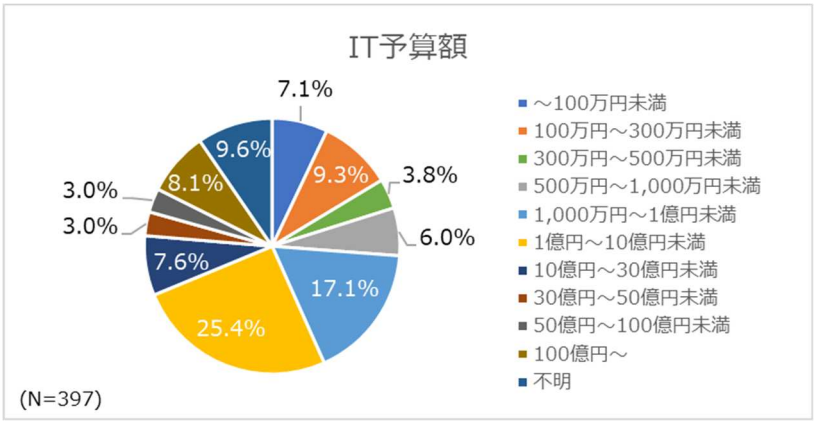


図 2.1-25 回答企業の IT 予算額

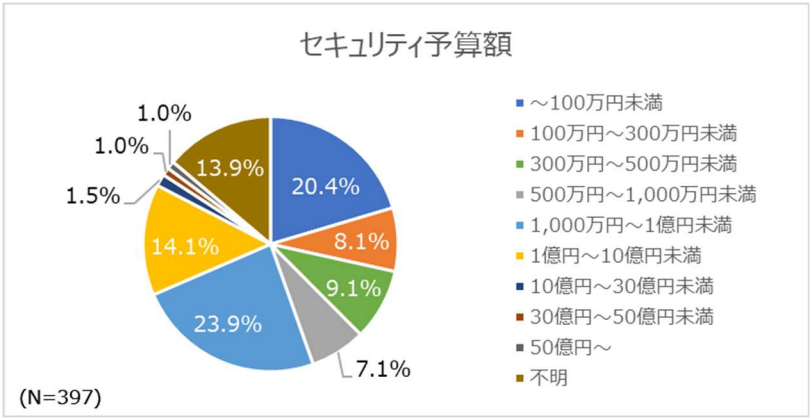


図 2.1-26 回答企業のセキュリティ予算額

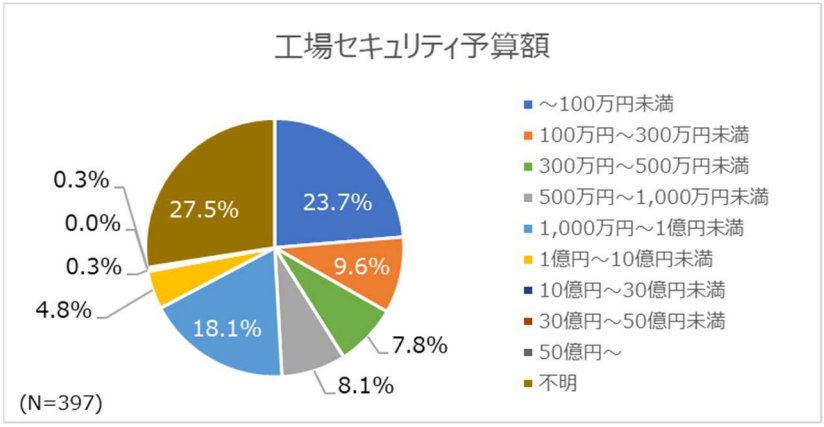


図 2.1-27 回答企業の工場セキュリティ予算額

c. 工場におけるデータ分析

工場データの利活用状況について、「工場全体のデータの収集・蓄積を実施している」と答えた企業46.3%と最も多かった。一方で、「データを利活用していない」と答えた企業は 18.0%であった。工場データの利活用の意向について、「データ利活用を促進する予定である」が 48.8%と最も多かった。

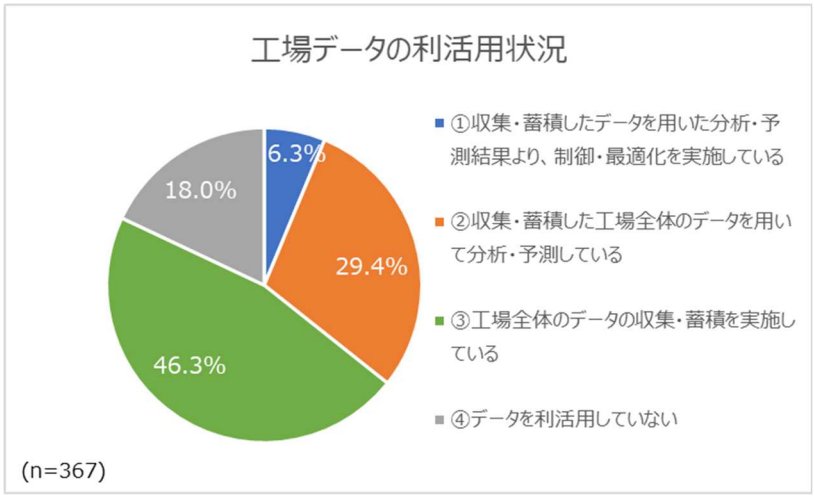


図 2.1-28 回答企業の工場データの利活用状況

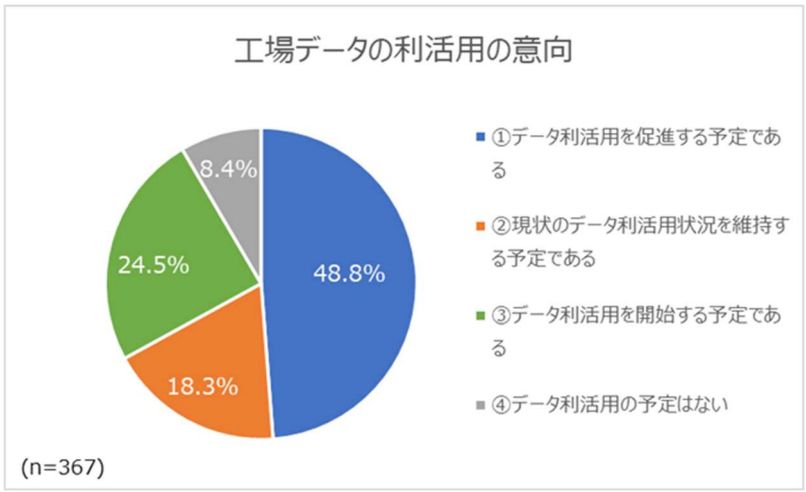


図 2.1-29 回答企業の工場データの利活用の意向

d. 工場におけるリスク分析

認識している工場のサイバーセキュリティのリスクについて、「工場システムへの不正侵入」が 77.4%と最も多く、「データ盗難・漏えい」(76.8%)、「データ改ざん・破壊」(69.8%)「システム/機器の障害・故障」(68.7%)と続いた。リスク分析の頻度について、「実施していない」が 47.4%と最も多かった。

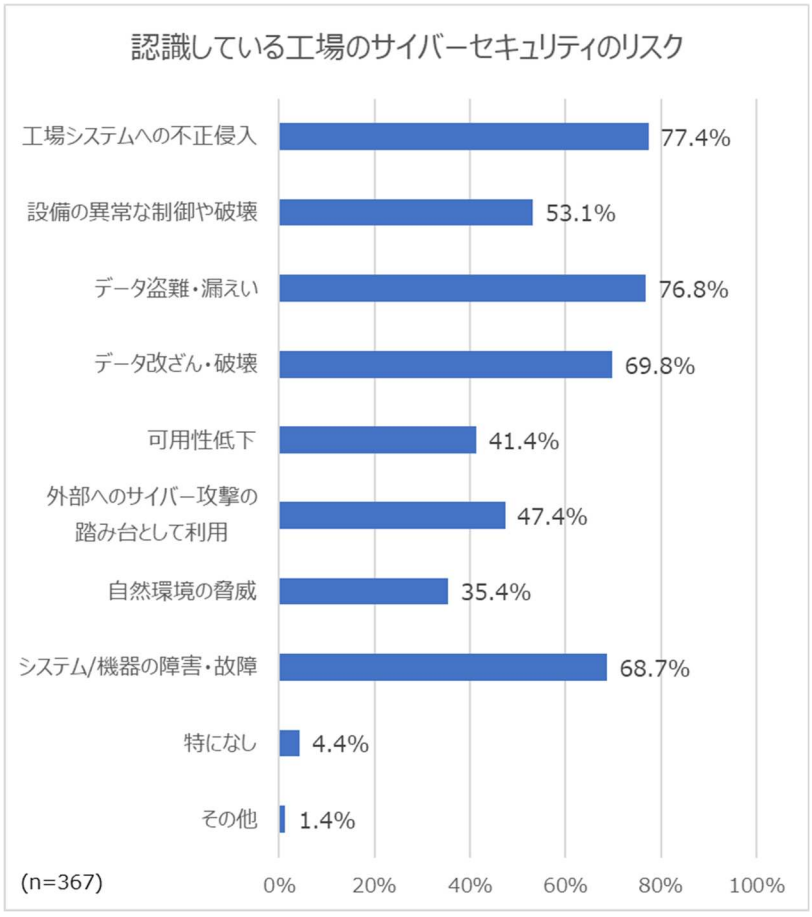


図 2.1-30 回答企業が認識している工場のサイバーセキュリティのリスク

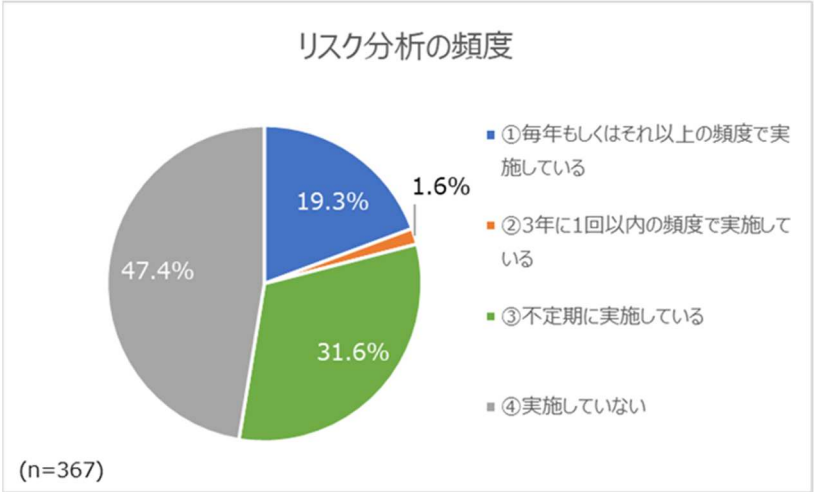


図 2.1-31 リスク分析の頻度

e. 工場におけるセキュリティ体制

CISO の設置について、「設置している」が 51.8%と半数程度だが、工場セキュリティ責任者の設置については、「設置している」が 41.7%と CISO 設置率より低かった。情報セキュリティ委員会の設置について、「設置している」が 52.6%と半数程度であった。

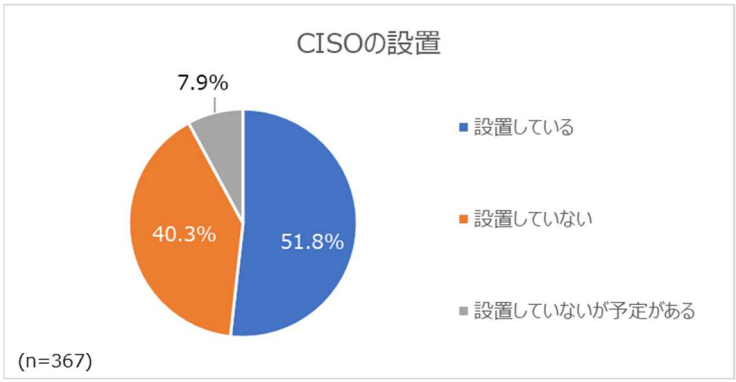


図 2.1-32 回答企業における CISO の設置状況

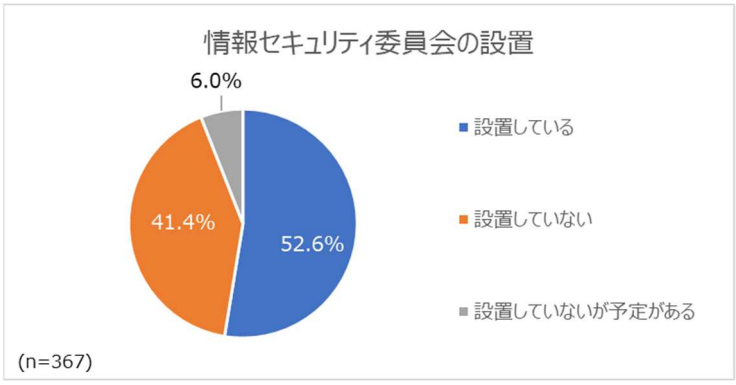


図 2.1-33 回答企業における情報セキュリティ委員会の設置状況

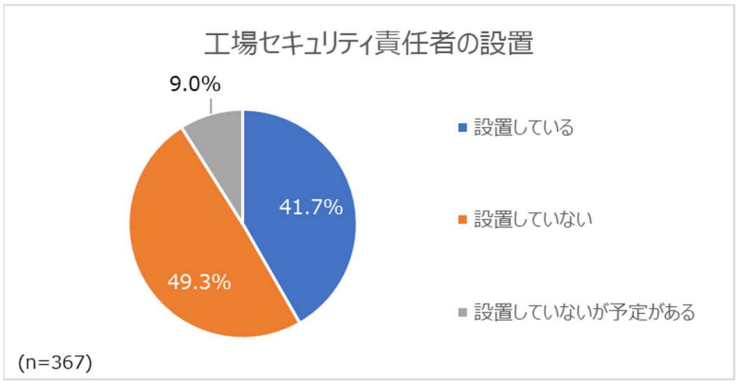


図 2.1-34 回答企業における工場セキュリティ責任者の設置状況

f. 工場における外部委託状況

工場システムの構築・保守の外部委託状況について、「工場システムの構築・保守を外部委託している」が 59.7%と約 6 割は外部委託があった。外部委託のある企業における契約書等へのセキュリティ

要件の取り込み状況について、「契約書・仕様書等にセキュリティ要件を取り込んでいる」が 72.6%であり、7 割以上でセキュリティが考慮されていた。

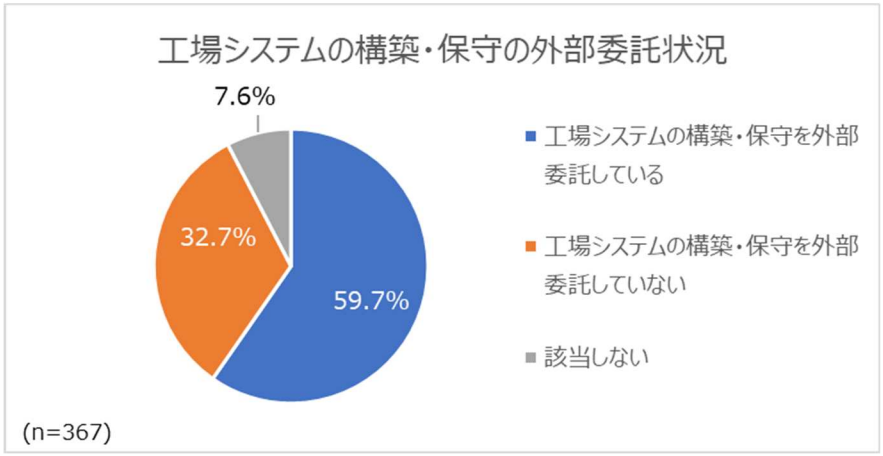


図 2.1-35 回答企業の工場システムの構築・保守の外部委託状況

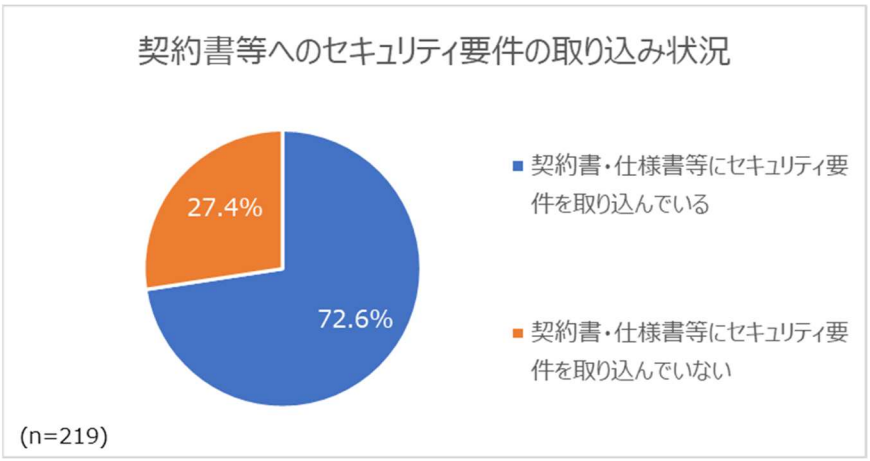


図 2.1-36 外部委託のある回答企業における契約書などへのセキュリティ要件の取り込み状況

g. 工場ガイドチェックリストの実施状況

工場システムの組織的対策のうち、「情報収集」について「未実施」または「該当しない・わからない」が 41.0%と他の対策と比較して、最も多かった。

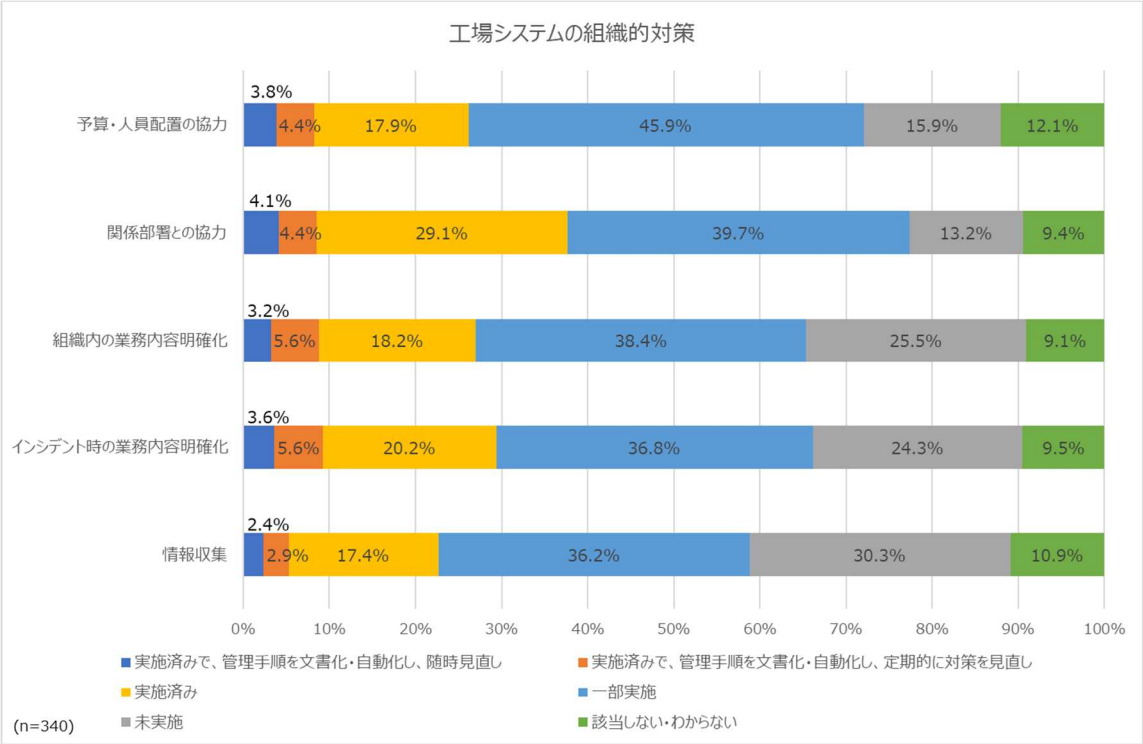


図 2.1-37 回答企業における工場システムの組織的対策状況

工場システムの運用的対策のうち、「脆弱性判断・脆弱性の特定」について「未実施」または「該当しない・わからない」が 65.0%と他の対策と比較して、最も多かった。

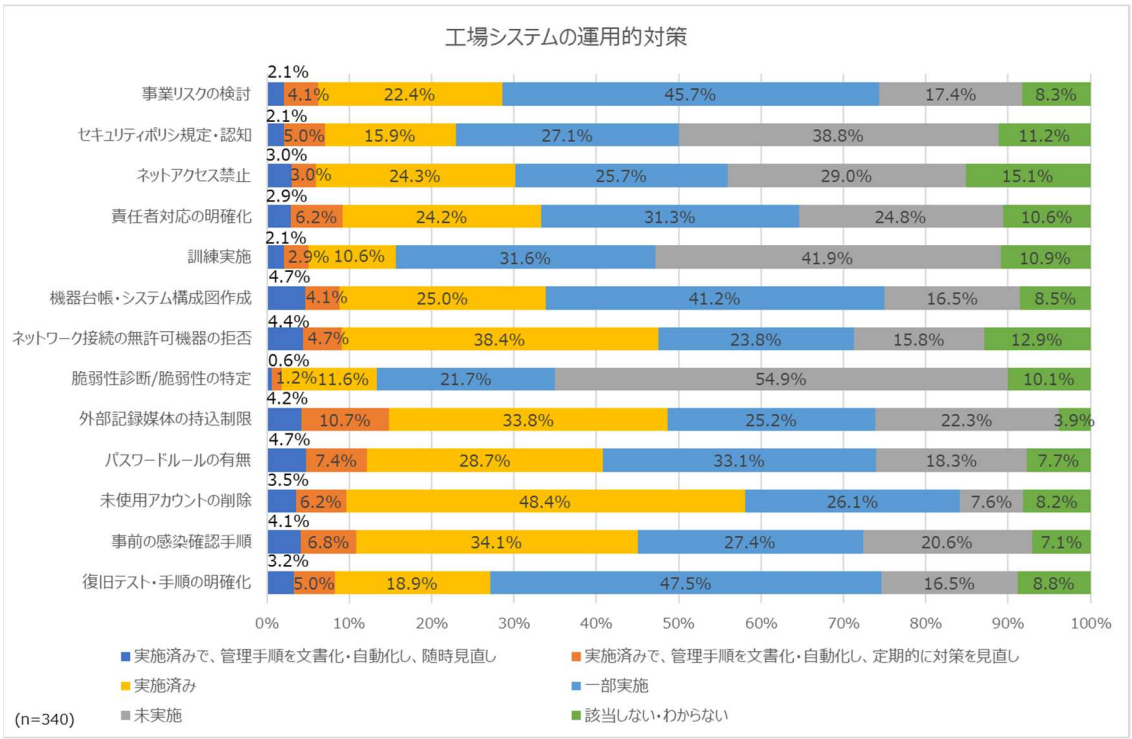


図 2.1-38 回答企業における工場システムの運用的対策状況

工場システムの物理的対策のうち、「ウィルス対策の導入」「セキュリティパッチの適用/代替策」について実施済み(「実施済みで、管理手順を文書化・自動化し、随時見直し」「実施済で、管理手順を文書化・

自動化し、定期的に対策を見直し」「実施済み」の合計）であるのがそれぞれ 63.7%、55.3%と他の対策と比較して多かった。

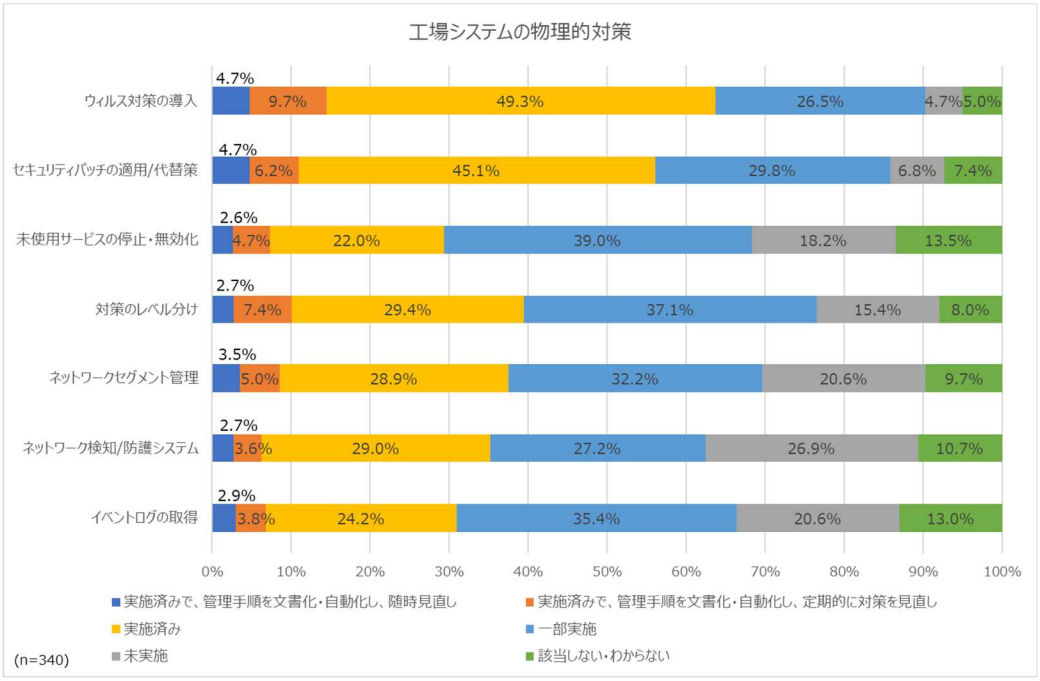


図 2.1-39 回答企業における工場システムの物理的対策状況

工場システムのサプライチェーン対策のうち、「セキュリティ教育の実施」について「未実施」または「該当しない・わからない」が 68.3%と他の対策と比較して、最も多かった。

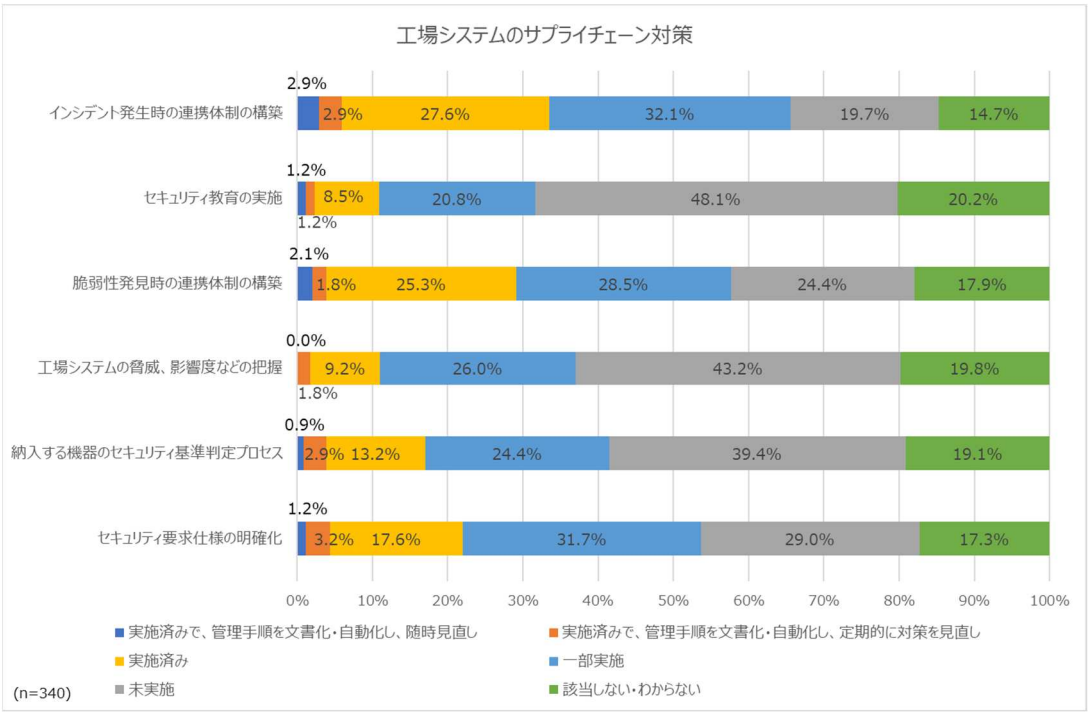


図 2.1-40 回答企業における工場システムのサプライチェーン対策状況

h. 工場セキュリティにおける課題や要望について

工場システムのセキュリティ対策における組織的な課題について、「工場システムのサイバーセキュリティを確保するための人材がいない」が 76.0%と最も多かった。工場システムのサイバーセキュリティ対策を進める際の課題について、統一的な基準構築やリスク分析、対策状況の管理の難しさ等、いずれの項目についても 3～4 割の企業が課題としていた。

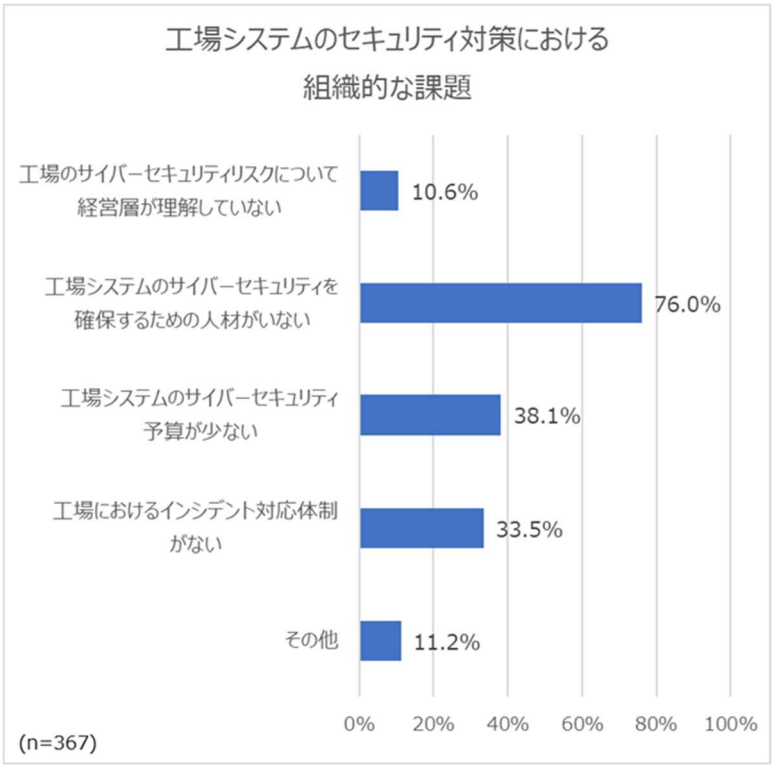


図 2.1-41 回答企業の工場システムのセキュリティ対策における組織的な課題

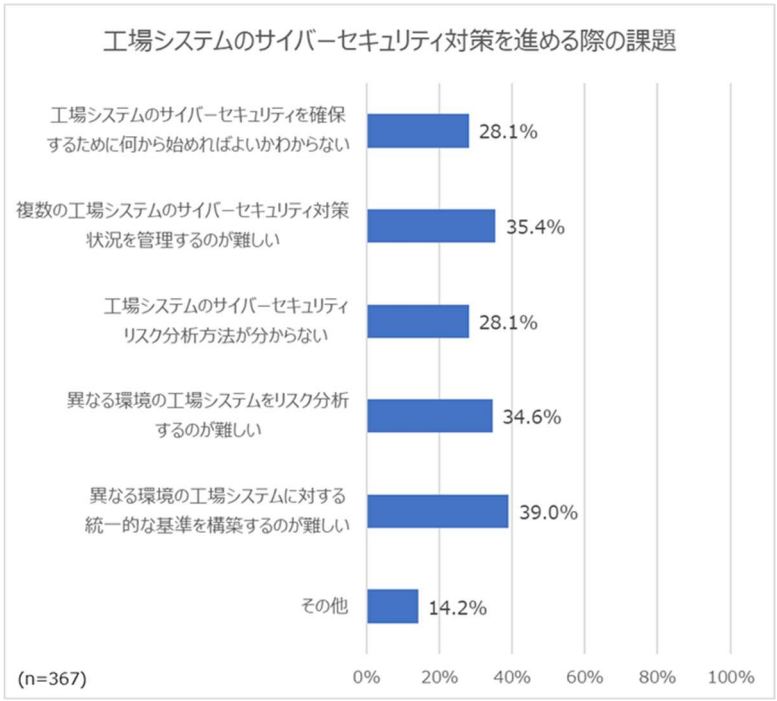


図 2.1-42 回答企業の工場システムのサイバーセキュリティ対策を進める際の課題

工場セキュリティガイドラインの認知状況について、「本アンケートで初めて知った」が 68.4%と最も多く、「ガイドラインについて認知していて、内容についても確認している」のは 9.8%であった。工場セキュリティガイドラインを認知した経緯について、「業界団体からの案内」が 44.8%と最も多く、「経済産業省の HP」(37.9%)、「セキュリティ関連セミナー等での案内」(35.3%)が続いた。ガイドラインの活用可能性について、「活用できると考える」が 63.9%と最も多かった。

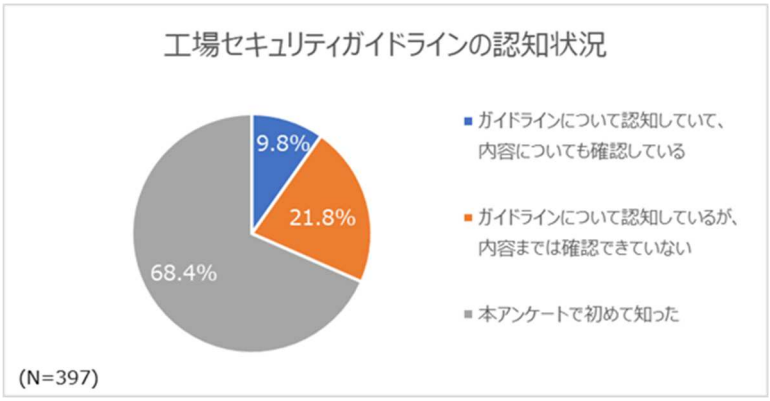


図 2.1-43 回答企業における工場セキュリティガイドラインの認知状況

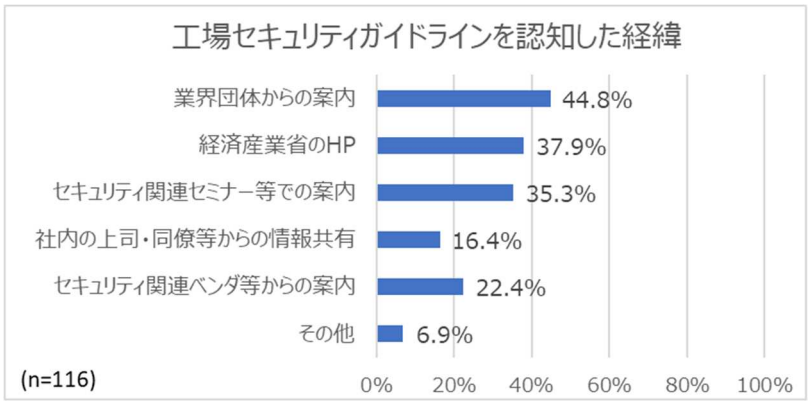


図 2.1-44 工場セキュリティガイドラインを認知している回答企業における認知した経緯

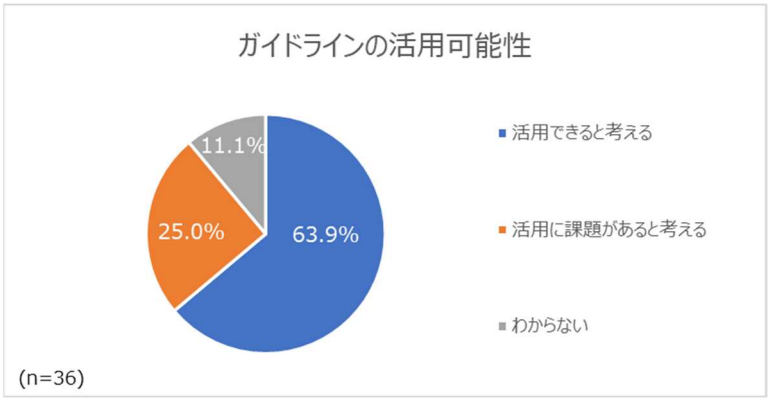


図 2.1-45 工場セキュリティガイドラインを認知していて内容も確認している回答企業における
ガイドラインの活用可能性

ガイドラインを活用する上で国に期待する支援策について、「具体的な対策を示してほしい」が

55.2%と最も多く、「対策毎の具体的な実施方法の例がほしい」が 47.6%と続いた。業界団体に期待する支援策について、業界における構成事例やチェックリスト、ガイドラインの利用方法、統一的な対策内容等、いずれの支援策についても 3～4 割強の企業が期待していた。

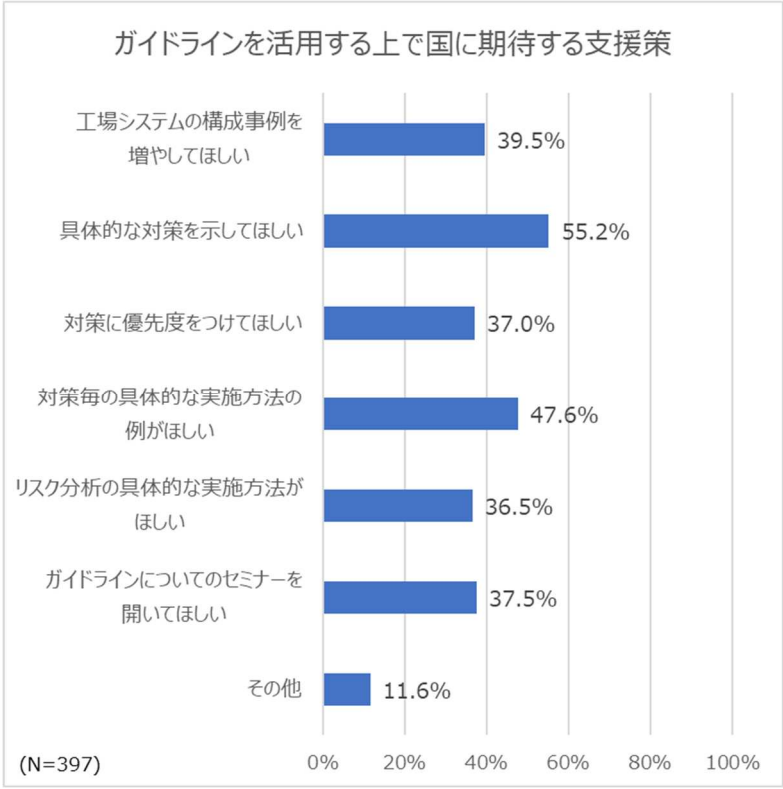


図 2.1-46 回答企業のガイドラインを活用する上で国に期待する支援策

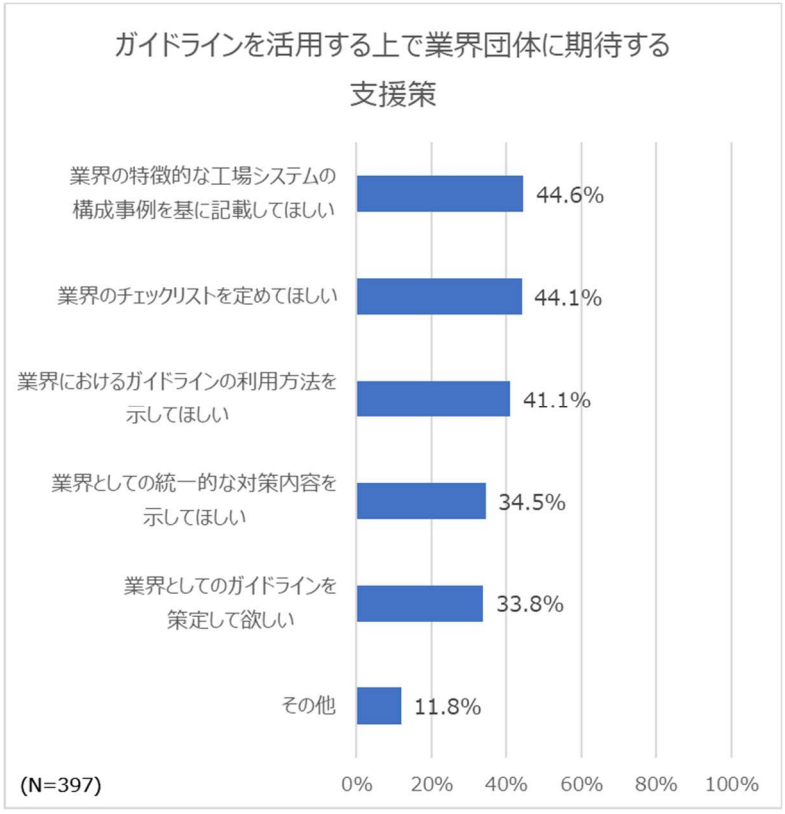


図 2.1-47 回答企業のガイドラインを活用する上で業界団体に期待する支援策

3）各企業への工場セキュリティの普及の方針

工場セキュリティにおける企業の課題としては人材不足が最も多かった。また、企業は工場現場のデータの利活用を行う意向がある割に、リスク分析はできていない。さらに、国に対しては、工場ガイドの具体的な対策や事例を示してほしいという声が多い。上記のような声が多い中、以下のような取り組みの方向性が検討されうる。

- 情報処理安全確保支援士等の更なる活用といった支援層の拡大
  情報処理安全確保支援士や ICSCoE 卒業生等の人材に対して、OT セキュリティに関する教育を実施したうえで、各企業へ派遣するなどが検討される。
- 関係機関（IPA 等）とも連携した工場ガイドの深掘り・具体化した文書（詳細ガイド、実施例）の作成・ブラッシュアップ
  IPA においても、「スマート工場のセキュリティリスク分析調査」や「制御システムのセキュリティリスク分析ガイド」などが発行され、今後具体的なセキュリティ対策事例や侵入検知製品の導入手引書が公開される予定である。その他、JNSA も工場セキュリティの簡易リスク分析のハンドブックを公開されていることから、このような関係機関との連携を行うことが望まれる。
- 業界団体、セキュリティベンダ等によるサポート
  SC3 で工場セキュリティガイドラインを業界団体に紹介することで、会員企業へのサポートを行うことが検討される。また、このようなサポート状況を SC3 等で共有することも望まれる。

（2）工場におけるデータ利活用の段階に応じたセキュリティ導入に係る課題等の調査

1）工作機器市場の動向

工作機械は我が国で強みを有する産業領域であり 、主要プレイヤーに DMG 森精機、アマダ、ジェイテクト、オークマ、牧野フライス製作所、ヤマザキマザック等多くの日本企業が含まれる。日本企業のシェアは 1 割を超えるとみられる。

世界の工作機械市場は、2027 年に約 1,000 億米ドル規模で、4%以上で成長すると見込まれる。

REPORTOCEAN(2021/10/21)によると、世界の工作機械市場は、2021 年から 2027 年において、4%以上の成長率が見込まれ、2020 年には約 803 億米ドル、2027 年までに 1,056 億 7,000 万米ドルの市場規模に達する見込みである。

Astute Analytica(2021/9/24)によると、世界の工作機械市場は、2027 年には 95,169.1 百万米ドルに達し、予測期間中に 4.7%の CAGR を記録すると予想されている。

日本の工作機械市場は、2021年(受注実績)で、前年比70・9%増の1兆5414億1900万円で3年ぶりの増加。過去4番目の受注額を記録。中国が先行して回復し、年後半は欧米や国内でも回復傾向にある(日工会)。自動運転技術、5G や AI、IoT 等の新たな技術に伴う設備投資の推進により、今後工作機械の需要は増加見込である。

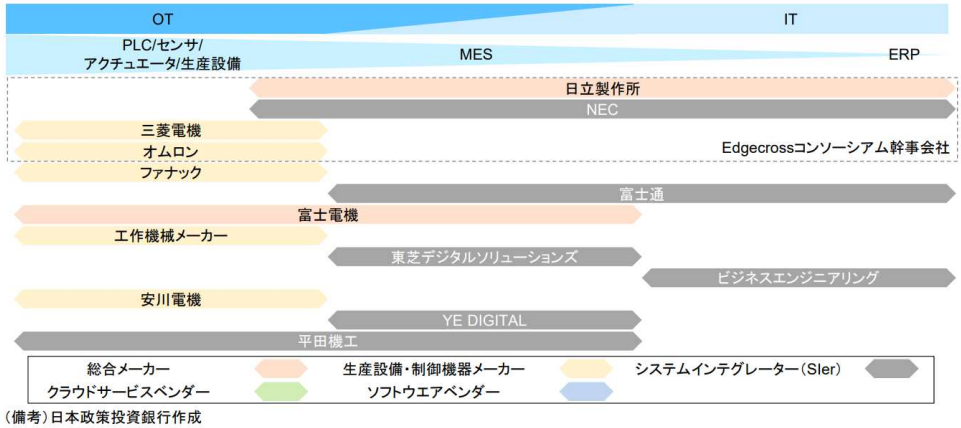
2）参入事業者の状況

一方、工作機器市場では、近年参入企業が多く、低コスト製品を供給する海外企業が台頭している。

工場データの利活用のためには、製造現場(工場システム:OT)のデータと企業経営に関わる(情報システム:IT)データを連携する必要がある。しかし、OT と IT が接続されたシステムは日本においてはまだ少ないと考えられる。

提供側を見ても、国内市場におけるプレイヤーは OT もしくは IT の一方に得意分野があり、OT～IT まで一気通貫した取組は一部にとどまる(例:エッジクロス、フィールドシステム等)。一方、海外市場では、シーメンス、ロックウェル等が買収・連携等により、OT・IT の統合を進めている。

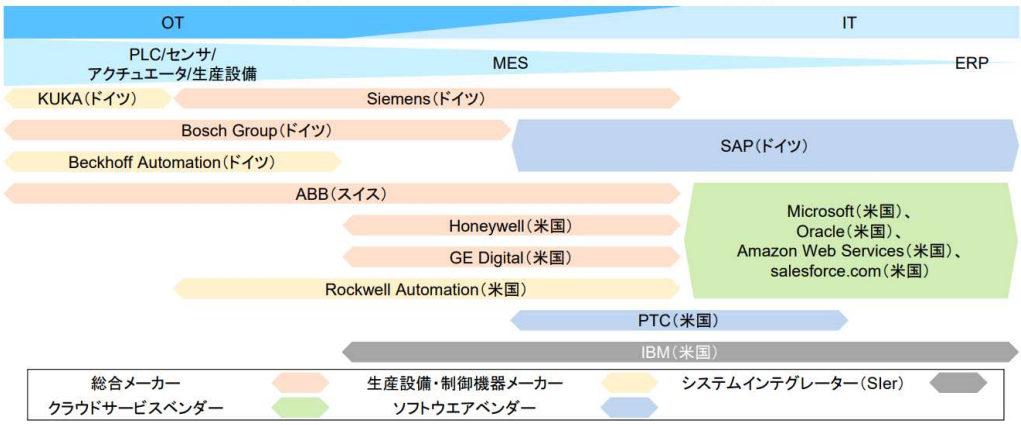
スマートファクトリー化の進展に伴い、製造現場の OT からのインテグレーションを実施可能なプレイヤーが台頭する可能性があり、国内の工作機器メーカーもこのような動きに追従する必要がある。



(備考)日本政策投資銀行作成

図 2.1-48 製造業におけるデジタル化の主要事業者(日系企業、順不同)[1]

[1] https://www.dbj.jp/upload/docs/229e0d17f17e02eaeff65f40f8e3535f.pdf



（備考）日本政策投資銀行作成

図 2.1-49 製造業におけるデジタル化の主要事業者（海外企業、順不同）[2]

（3）国内外の工場セキュリティについての対策等についての調査

1）国内

a. 工場セキュリティに関する関連組織の取組

ア）スマート工場のセキュリティリスク分析調査

2022 年 7 月 1 日に、IPA がスマート工場化によって生じるセキュリティリスクを正しく認識するための情報を提供することを目的に実施された調査の報告書を公表した。9 社 22 類型のシステムに対するヒアリングを行い、CPSF の第 2 層・第 3 層に注目して 7 つの実装モデルが整理されている。本報告書では、類型された 7 つの実装モデル毎に被害・脅威・対策がまとめられている。スマート工場の対策は、各実装モデルでの整理に加えて、全てのモデルに共通する対策も、物理的・運用的に分けて記載されている。各実装モデルにおいて、システム図・データフロー・業務運用の想定が詳細に記載されている。これらの情報を用いて、想定される被害、被害に繋がる脅威、脅威に対する対策の 3 点が表形式にまとめられている。

[2] https://www.dbj.jp/upload/docs/229e0d17f17e02eaeff65f40f8e3535f.pdf

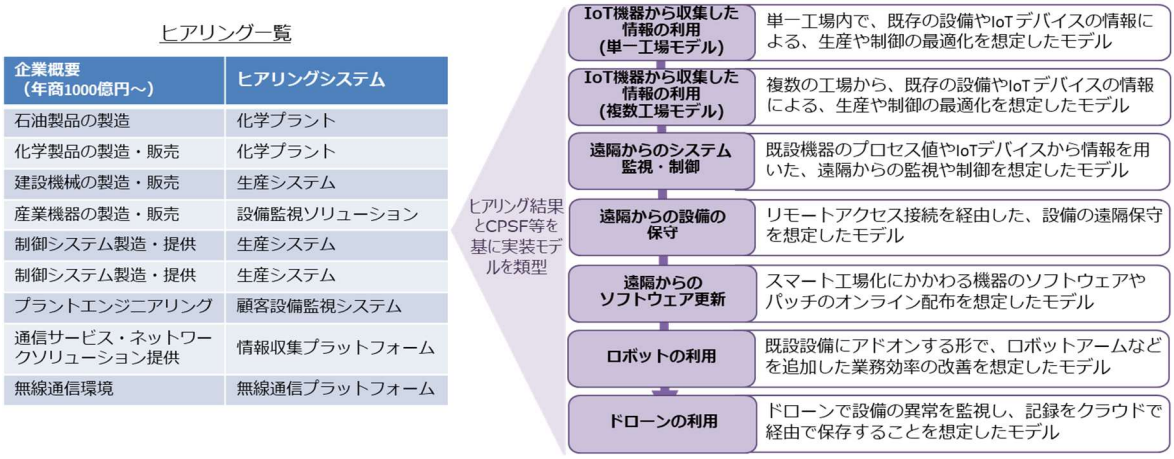


図 2.1-50 スマート工場のセキュリティリスク分析調査の概要[3]

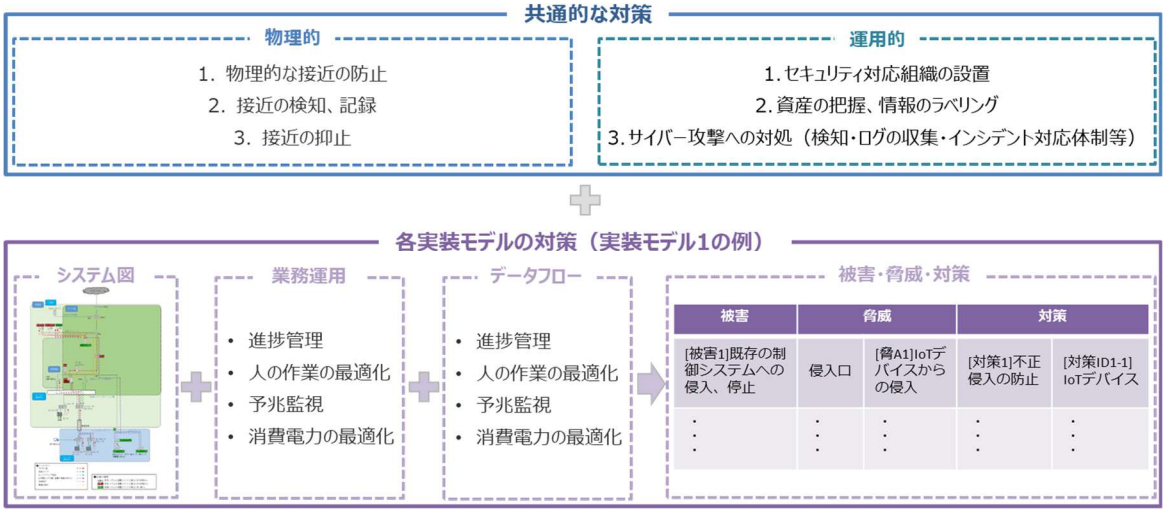


図 2.1-51 実装モデルごとの対策の概要 [3]

イ） 今すぐ実践できる工場セキュリティハンドブック リスクアセスメント編

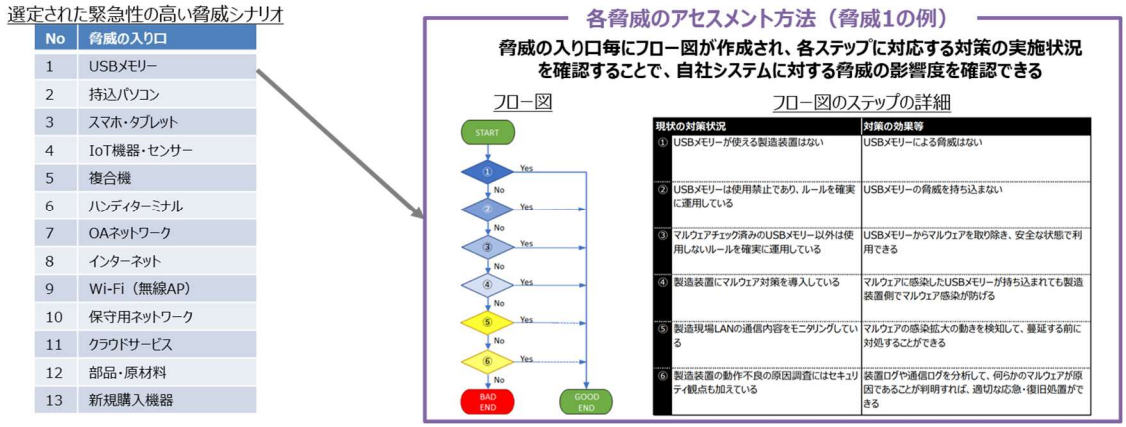
2022 年 6 月に、JNSA が工場セキュリティリスクアセスメントを自らの手で実践できるようになるための参考書として活用されることを目的にハンドブックを公表した。初級者向けに工場セキュリティリスクアセスメントの概要が記載されている。また、緊急性が高いと考えられる脅威シナリオを抽出し、シナリオ毎にアセスメント方法が詳細に記載されている。本ハンドブックは、洗い出された特定のリスクに対するアセスメントを実践しやすいようまとめられている。

検討メンバーより選定された緊急性の高い 13 個の脅威シナリオ毎にアセスメントを簡易的に実施できるフロー図が示されている。フロー図の各ステップに対応する対策の実施状況を確認することで、自社システムに対する脅威の影響度を確認できる。今後、本ハンドブックの続編として、リスクに合わせた具体的な対策実施の事例が記載されたリスク対策編、工場セキュリティに着目した BCP 策定のヒントを記載されたサイバーBCP 策定編が公表される予定である。

[3]「スマート工場のセキュリティリスク分析調査」調査報告書、
https://www.ipa.go.jp/security/controlsystem/controlsystem-smartplant.html

No	脅威の入り口	脅威が引き起こす可能性のある事象	懸念されるリスク
1	USBメモリー	制御システム等にマルウェア感染拡大	工場停止
2	持込パソコン	制御システム等にマルウェア感染拡大	工場停止
3	スマホ・タブレット	マルウェア感染による意図しない動作	情報漏洩
4	IoT機器・センサー	IoT機器などが第三者に遠隔操作	工場停止
5	複合機	複合機が第三者に遠隔操作	情報漏洩
6	ハンディターミナル	マルウェア感染によるデータ等の改竄	情報漏洩
7	OAネットワーク	OAネットワークからのマルウェア拡大	工場停止
8	インターネット	インターネットからのマルウェア拡大	工場停止
9	Wi-Fi（無線AP）	通信の傍受・妨害	情報漏洩
10	保守用ネットワーク	保守ネットワークからのマルウェア拡大	工場停止
11	クラウドサービス	認証情報の不正利用	情報漏洩
12	部品・原材料	部品のセキュリティ不具合が悪用	品質低下
13	新規購入機器	制御システム等にマルウェア感染拡大	工場停止

図 2.1-52 今すぐ実践できる工場セキュリティハンドブック リスクアセスメント編の概要[4]



No	脅威の入り口
1	USBメモリー
2	持込パソコン
3	スマホ・タブレット
4	IoT機器・センサー
5	複合機
6	ハンディターミナル
7	OAネットワーク
8	インターネット
9	Wi-Fi（無線AP）
10	保守用ネットワーク
11	クラウドサービス
12	部品・原材料
13	新規購入機器

図 2.1-53 選定された脅威シナリオとそのアセスメント方法の概要[4]

ウ）セキュアな ICS クラウド導入指南書

2022 年 9 月に、ICSCoE 中核人材育成プログラム第 5 期受講生が製造現場のクラウド活用における「データ利活用促進」と「セキュリティの向上」を両立することを目的に指南書を作成した。本指南書では、制御システムへのクラウド導入などの事例やデータ利活用とセキュリティに関わる課題や乗り越え方が整理されている。また、整理結果を用いて、制御システムとクラウドを融合させた際の脅威分析・セキュリティ対策を実施し、総合的なアーキテクチャを検討している。本指南書は、工場システムにおけるクラウド導入という先進的な取組に注目した資料である。

アーキテクチャの要件を、調査したクラウド導入事例を基に「データ可視化」、「予知保全」、「最適設定演算」、「データ連携」と定義している。アーキテクチャの設計は、Purdue モデルを基にオンプレミス領域（企業 IT エリア・工場）、クラウド領域（IT クラウド基盤・ICS クラウド基盤）、DMZ の計 4 階層＋DMZ の構成を仮定した。設計されたアーキテクチャに対してシナリオベースによる脅威分析である CCE1 を参考に、脅威分析・セキュリティ対策を実施している。

[4] 今すぐ実践できる工場セキュリティハンドブック リスクアセスメント編、
https://www.jnsa.org/result/west/2022/index.html

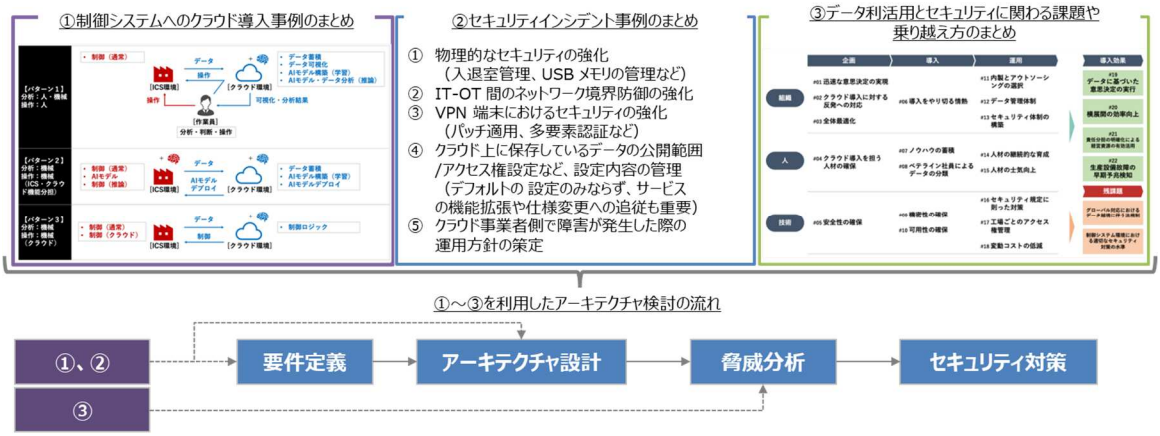


図 2.1-54 セキュアな ICS クラウド導入指南書の概要[5]

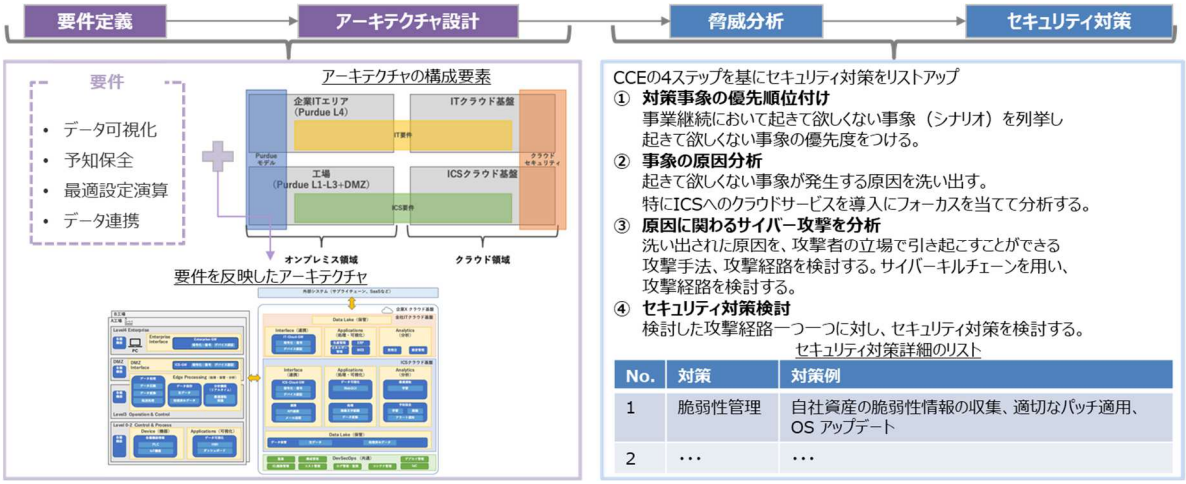


図 2.1-55 セキュリティ対策までの具体的なステップ [5]

b. 工場システム関連セキュリティサービス

ア） スマートファクトリーにおけるセキュリティ製品・サービスの動向の概要

近年、スマートファクトリーにおいて活用可能なセキュリティに関する製品・サービスが数多く提供開始されている。「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」がサービスに活用される、プレスリリース等のサービス説明にガイドが参照される等の事例も見られる。以下に現在のスマートファクトリーにおけるセキュリティ製品・サービスを取りまとめる。ガイドを活用・参照している 3 つのサービスを詳細に確認する。

表 2.1-22 近年の主なスマートファクトリーにおけるセキュリティ製品・サービス、事業者の動向

開始日	企業名	製品・サービス、取組概要
2022/9	Fortinet	工場セキュリティに関する経産省ガイドラインに従ったコンサルティン

[5] セキュアな ICS クラウド導入指南書、
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/secure-ics-cloud.html

		グサービス「OT セキュリティアセスメントサービス」のノウハウを、販売パートナー向けトレーニングプログラムとして提供開始（ガイド活用）
2022/8	TXOne Networks	日本市場への本格参入と展開戦略を発表。製造業や重要インフラ向けセキュリティ企業、「OT ゼロトラスト」の普及に向けて、国内体制を強化（ガイド参照）
2022/8	NRI セキュア（ Nozomi Networks）	Nozomi Guardian を活用し、工場の制御システム（OT/IoT）のセキュリティを可視化・監視するマネージドサービスを提供開始（ガイド参照）
2022/7	シスコシステムズ	製造業に対して、CVD（Cisco Validated Design）という検証済みの設計指針に基づき、ネットワーク設計から導入、運用、人材のリテラシー向上まで顧客のセキュリティ対策を包括支援
2022/6	ゼットスケーラー・シーメンス	ゼットスケーラーとシーメンスの提携により、OT 環境の安全なデジタライゼーションを加速するオールインワンソリューションを提供開始
2022/5	シーメンス	シーメンスは、AGEST、アイデン、ネットワークバリューコンポネンツ（NVC）、Nozomi Networks の 4 社と協業し、サイバーセキュリティのモデルラインとなる、DX（デジタルトランスフォーメーション）工場ネットワークを日本国内に構築し、実証ラインでの提供を開始したと発表
2022/5	東京エレクトロンデバイス（日本マイクロソフト）	工場現場へのサイバーセキュリティ対策強化を推進：日本マイクロソフトが提供する「Microsoft Defender for IoT」の導入支援を行う「Microsoft Defender for IoT 導入支援サービス」を提供開始
2022/2	大日本印刷・三菱電機	産業制御セキュリティの対策スキルを体験型で学べる演習を開発
2021/10	ゼロゼロワン	内部ネットワークの IoT 機器セキュリティ評価サービスを提供開始
2021/8	NEC ネッツエスアイ（トレンドマイクロ）	工場ネットワークのセキュリティ運用を支援する「産業セキュリティ運用サービス for トレンドマイクロ EdgeFire/EdgeIPS」の提供を開始
2021/6	Tenable	Deloitte と提携して Fortune 500 企業の製造環境のセキュリティを確保
2021/6	情報セキュリティ	スマートファクトリーの安定稼働に向けたセキュリティ対策支援サービス「i-Cybertech コンサルティングサービス」の提供開始
2021/6	Blue Planet-works	産業システム向けのセキュリティ製品「AppGuard Industrial」を新たに販売開始

イ） OT セキュリティアセスメントサービス（Fortinet）

2022 年 5 月より、Fortinet が工場セキュリティガイドラインを活用して最短 15 分で実施可能な工場に関する OT セキュリティアセスメントサービスを構築した。OT セキュリティアセスメントサービスは、4 カテゴリ計 32 問の設問に回答することで、各カテゴリのスコアと全体のスコアが結果に表示される。2022 年 9 月より、本サービスのノウハウを用いて販売パートナー向けトレーニングプログラムの提供を開始している。

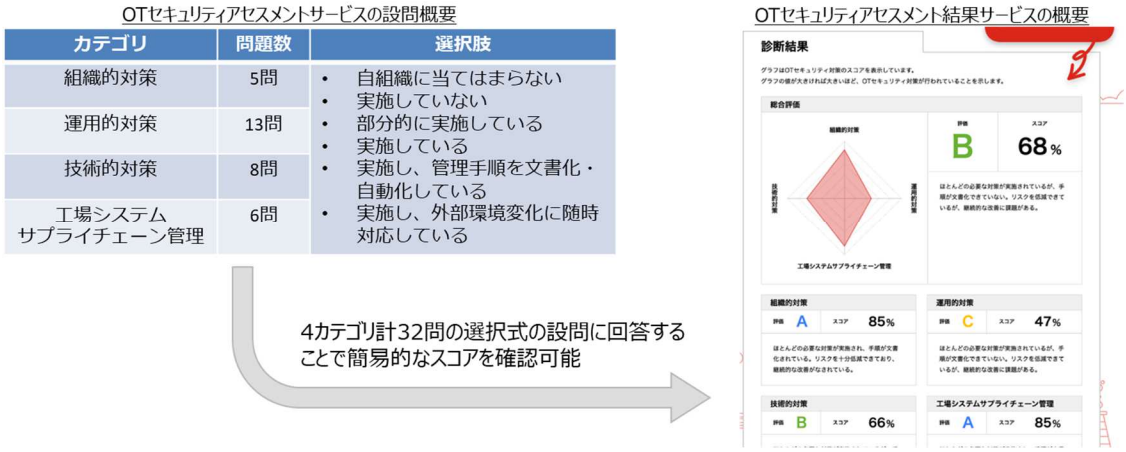


図 2.1-56 OT セキュリティアセスメントサービスの概要[6]

ウ） TXOne Networks OT セキュリティのトータルソリューション

2022 年 8 月より、産業制御システム向けのセキュリティソリューションを提供する TXOne Networks が、日本市場への本格参入と今後の展開戦略を発表した。産業向け次世代ファイアウォール、産業向け次世代 IPS、産業向けエンドポイントプロテクション、ウィルス検索・駆除ツール等を含めたトータルソリューションが TXOne Networks より提供されている。国内への本格参入の背景の一部として、「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」の公表予定が挙げられている。

図 2.1-57 TXOne Networks のトータルソリューションの具体事例[7]

[6] OT セキュリティアセスメントサービス、https://www.fortinet.com/jp/promos/ot-security-assessment
[7] OT セキュリティのトータルソリューション、https://prtimes.jp/main/html/rd/p/000000001.000103304.html

エ）NRI セキュアテクノロジーズ　Nozomi Networks for OT/IoT

2022 年 8 月より、NRI セキュアテクノロジーズが工場の設備等を制御・運用するためのシステムのセキュリティを可視化・監視する「マネージド NDR（Nozomi Networks for OT/IoT）」サービスの提供を開始した。Nozomi Networks for OT/IoT は、工場システムの稼働に影響を与えない形で導入可能な監視サービスである。工場システムの設備や端末等を可視化したうえで、異常を NRI セキュアが 24 時間 365 日体制で監視する。サービス提供開始の背景の一部として、「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」の公表予定が挙げられている。

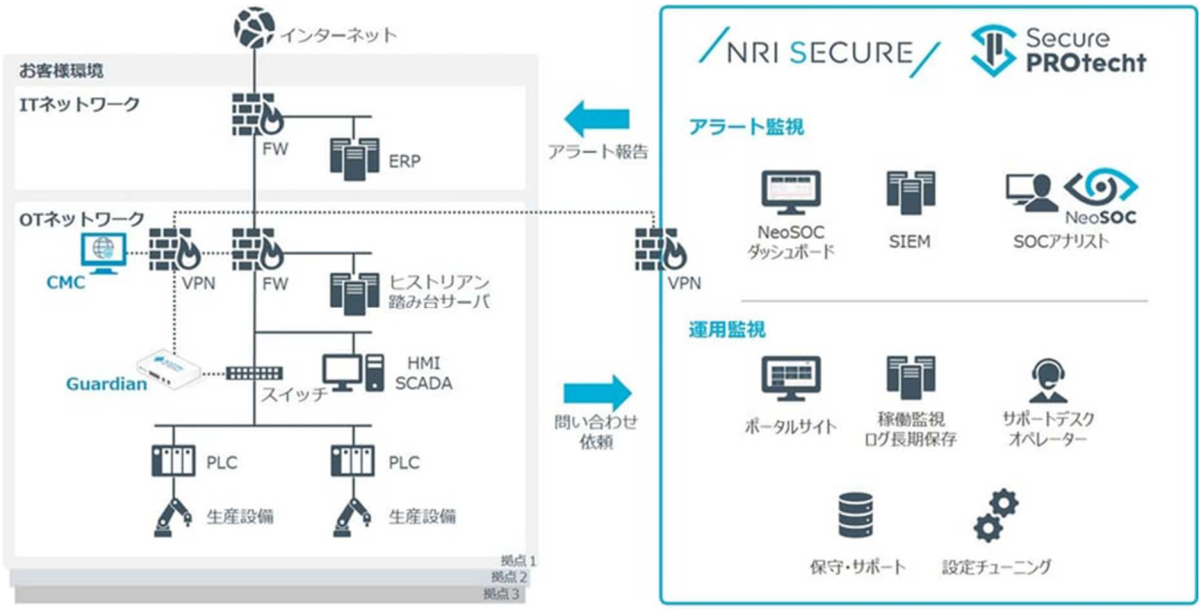


図 2.1-58　Nozomi Networks for OT/IoT のサービスイメージ[8]

2）国外

a. 工場セキュリティに関する関連組織の取組

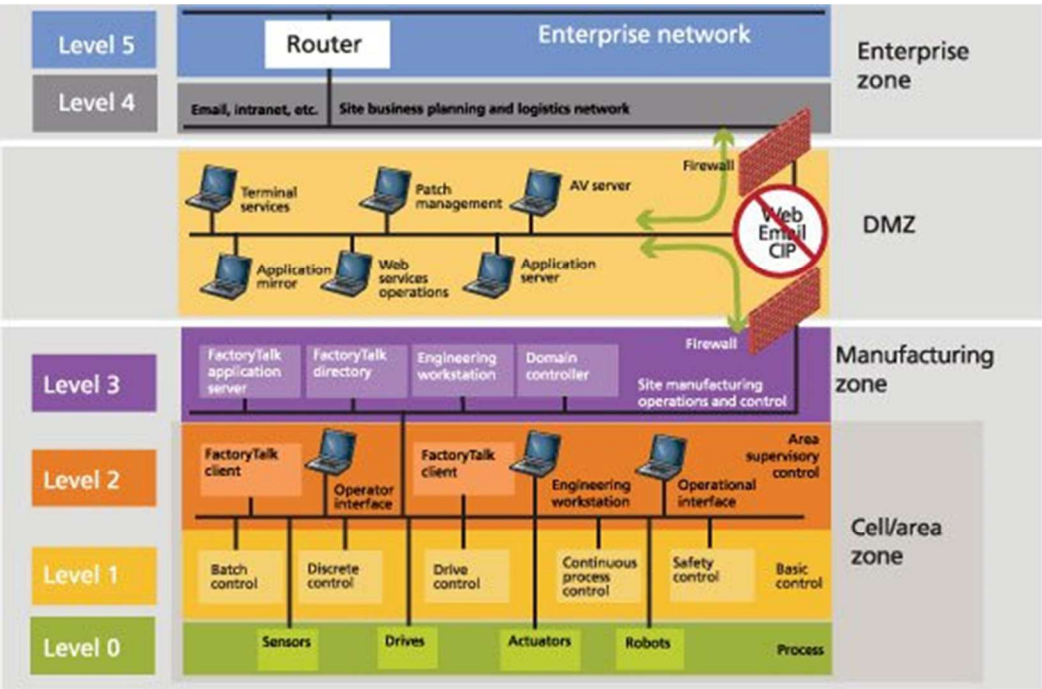
ア）IEC 62443

IEC 62443 は制御システムを対象とするセキュリティの代表的な国際規格である。IEC において Horizontal Standards（横断的に参照される規格）に指定されている。

4 つのシリーズ「一般：62443-1」「ポリシーと手続：62443-2」「システム：62443-3」「コンポーネント：62443-4」で構成される。62443-2-1、2-4、3-3、4-1、4-2 を元にした認証制度が、各国の複数の認証機関で運用されている。

IEC 62443 では、Purdue Enterprise Reference Architecture（PERA）と呼ばれるシステムのアーキテクチャを採用しており、レベル 0～4 までの 5 階層で構成される。この各レベル間をファイアウォールや DMZ で制御することでシステムを防御する。また、各要素については、ネットワークセグメンテーションのために、ゾーン（Zones）とコンジット（Conduits）に分類し、共通のセキュリティ要件毎にグループに資産を分け、グループ間の連結部分の要件を規定することで、セキュリティを確保する。

[8] Nozomi Networks for OT/IoT、https://www.nri-secure.co.jp/service/mss/managed-ndr-nozomi



- レベル4、5（及びインターネット）からレベル3へのアクセス制限
- レイヤー2、3からレイヤー4、5へ通信可能
- レベル0、1（機械とプロセス）は制御システム内で通信

図 2.1-59 IEC62443 のシステムモデル[9]

イ） NIST SP800-218

システム開発におけるセキュリティ確保のための関連規格として、NIST SP800-218 がある。セキュアソフトウェア開発フレームワーク（SSDF）は、各 SDLC の実装に統合可能な、高レベルのセキュアソフトウェア開発プラクティスのコアセットである。これらのプラクティスに従うことで、ソフトウェア製造者は、リリースされたソフトウェアの脆弱性の数を減らし、未検出または未対処の脆弱性が悪用された場合の潜在的な影響を軽減し、将来の再発を防ぐために脆弱性の根本原因に対処することができる。

表 2.1-23 NIST SP800-218 概要

内容	プラクティス
1. 組織の準備（PO）： 組織は、組織レベルで安全なソフトウエア開発を行うために、人材、プロセス、技術を準備する必要がある。多くの組織は、個々の開発グループやプロジェクトなど、ソフトウェア開発のサブセットにも適用可能な PO プラクティスがあると考える。	ソフトウェア開発のセキュリティ要件を定義する（PO.1） 役割と責任の実施（PO.2） 支援ツールチェーンの導入（PO.3） ソフトウェアのセキュリティチェックのための基準を定義して使用する（PO.4） ソフトウェア開発のための安全な環境を導入・維持する（PO.5）：
2. ソフトウェアの保護（PS）： 組織は、ソフトウェアのすべてのコンポーネントを、改ざんや不正アクセスか	あらゆる形態のコードを不正なアクセスや改ざんから保護する（PS.1）： ソフトウェアリリースの完全性を検証する仕組みを提供する（PS.2）：

[9] https://blog.isa.org/the-internet-of-everything-delivers-smart-manufacturing

ら保護する。	各ソフトウェアリリースのアーカイブと保護(PS.3):
3. 安全なソフトウェアを作成する(PW): 組織は、リリースされるソフトウェアのセキュリティ脆弱性を最小限に抑え、十分なセキュリティを備えたソフトウェアを製造すべきである。	セキュリティ要件を満たし、セキュリティリスクを軽減するようにソフトウェアを設計する(PW.1): ソフトウェア設計をレビューして、セキュリティ要件とリスク情報への適合性を検証する(PW.2): <サードパーティソフトウェアはセキュリティ要求を満たす(PW.3)はPW.4 に移動> 実現可能な場合には、機能を重複させるのではなく、既存の十分に保護されたソフトウェアを再利用する(PW.4): セキュアコーディングの実践を遵守してソースコードを作成する(PW.5): 実行可能なセキュリティを向上させるために、コンパイル、インタプリタ、およびビルドプロセスを構成する(PW.6): 人間が読めるコードをレビューおよび/または分析して、脆弱性を特定し、セキュリティ要求事項への準拠を検証する(PW.7): 実行コードをテストして脆弱性を特定し、セキュリティ要求事項への準拠を検証する(PW.8): ソフトウェアをデフォルトで安全な設定にする(PW.9):
4. 脆弱性への対応(RV): 組織は、リリースするソフトウェアに残存する脆弱性を特定し、適切に対応する。	脆弱性の継続的な把握と確認(RV.1): 脆弱性の評価、優先順位付け、修正(RV.2): 脆弱性の分析とその根本原因の特定(RV.3):

ウ) NIST SP800-161 r1

工場システムにおいては多くの構成要素や連携先があることから、サプライチェーンにおけるリスク管理が必要となる。NIST の基本的なサイバーセキュリティ・サプライチェーン・リスク管理(C-SCRM)ガイダンスの新しい更新版は、企業がテクノロジー製品やサービスを取得・使用する際に、自らを守ることを目的としている。

組織がサプライチェーン内およびサプライチェーン全体のサイバーセキュリティリスクを管理する能力を開発する際に採用すべき重要な実践方法を提示している。

主な読者は、製品、ソフトウェア、サービスの取得者とエンドユーザーである。

このガイダンスは、組織が取得プロセスにサイバーセキュリティのサプライチェーンリスクの考慮と要件を組み込むことを支援し、リスクに対する監視の重要性を強調している。

なお、4. 参考文献の附属書 A に、具体的な C-SCRM のセキュリティ管理策が記されている。

表 2.1-24 NIST SP800-161 r1 概要

1.はじめに	2. エンタープライズ全体のリスクマネジメントへの C-SCRM の統合	3.重要成功要因
1.1 目的 1.2 対象読者 1.3 クラウドサービスプロバイダのためのガイダンス 1.4 対象者プロファイルと文書利用ガイダンス	2.1 C-SCRM のビジネスケース 2.2 サプライチェーンを通じたサイバーセキュリティリスク 2.3 マルチレベルのリスクマネジメント	3.1 取得における C-SCRM 3.1.1. C-SCRM 戦略及び実施計画における取得 3.1.2. 取得プロセスにおける C-SCRM の役割 3.2 サプライチェーン情報の共有

（1.4.1～1.4.5 各対象者） 1.5 背景 1.5.1. エンタープライズのサプライチェーン 1.5.2. エンタープライズ内サプライヤーとの関係 1.6 NIST SP 800-39; NIST SP 800-37, Rev 2; 及び NIST SP 800-53, Rev 5 を用いた C-SCRM ガイダンス構築のための方法論 1.7 他の出版物との関係及び出版物の概要	2.3.1. 3 つのレベルにわたる役割と責任 2.3.2. レベル 1 - エンタープライズ 2.3.3. 2.3.3. レベル 2 - ミッションとビジネスプロセス 2.3.4. レベル 3 - 運用 2.3.5. C-SCRM PMO	3.3 C-SCRM の訓練と意識向上 3.4 C-SCRM の主要実施事項 3.4.1. 基礎的な実践 3.4.2. 持続的な実践 3.4.3. 強化された実践 3.5 能力発揮の測定と C-SCRM 対策 3.5.1. パフォーマンス指標による C-SCRM の測定 3.6 専用リソース

エ） NIST SP 1500-201

サイバーフィジカルシステム（以下、「CPS」という）とはデジタル、アナログ、物理的な構成物および人間が相互作用したうえで機能するように設計されたシステムを意味する。

NIST SP 1500-201 のフレームワークでは、スコープを全システムエンジニアリングプロセスとし、コアコンセプトである「ファセット」、「アスペクト」に基づいた CPS の分析手法を提示している。

表 2.1-25 NIST SP1500-201 概要

主な内容	詳細
CPS の分析手法： CPS の分析は 4 つのステップで構成される	手順 1. ステークホルダが懸念を持つドメイン（製造業、農業等の分野）を特定する 手順 2. 社会的、ビジネス的、技術的といった分野横断的な懸念を特定する 手順 3. 分野横断的な懸念を分析する、もしくは関連する懸念をグループ化し、アスペクトを作成する 手順 4. 3つのファセットを通して、グループ化した懸念（アスペクト）に対処する
ファセット： システムエンジニアリングプロセスで 特定された責任を網羅する CPS の見解	＜ファセットの内容＞ 1 概念化 CPS がどうあるべきか、および何を行うべきかについて、目標・機能要件・構成に関連する活動を把握する 2 実現 対象の CPS に対する詳細設計、製造、実装および運用に関わる活動を把握する 3 保証 CPS が、「概念化」で開発されたモデルを満たすか確認する。
アスペクト： 分野横断的な懸念をグループ化したもの	＜アスペクトの内容＞ ・機能：制御、通信および物理等の機能に関する内容 ・ビジネス：企業、市場投入にかかる時間、コスト等に関する内容 ・人間：CPS と人間の間の相互作用、および CPS の一部としての人間に関する内容 ・信頼性：セキュリティ、プライバシーおよび安全性等を含む CPS の信頼性に関する内容 ・タイミング：タイムスタンプおよびレイテンシー管理等の CPS における時間と周波数に関する内容 ・データ：データの相互運用性に関する内容 ・境界：機能的、組織的あるいはその他相互作用の境界に関する内容 ・構成：選択された特性を計算する能力に関連する内容 ・ライフサイクル：CPS のライフサイクルに関する内容

b. 工場システム関連セキュリティサービス

2021 年の産業用制御システム(ICS)セキュリティの世界市場規模は 177 億 9000 万米ドル。2022 年から 2030 年までの予測期間において年平均成長率(CAGR)6.4%で成長し、2030 年には 309 億 1000 万米ドルに達すると予測されている。同レポートでは 25 の主要な事業者が挙げられている。(REPORTOCEAN、2022/3/25)

The Forrester Wave™: Industrial Control System (ICS) Security Solutions, Q4 2021 によると、12 のベンダが強力な製品を提供している事業者として挙げられている。

＜産業用制御システムセキュリティ世界市場における主要企業[10]＞

- ABB, Limited
- Airbus CyberSecurity
- Applied Security, Incorporated
- BAE Systems plc
- Belden Incorporated
- Check Point Software Technologies
- Cisco
- Claroty, Limited
- CyberArk
- Cyberbit
- Darktrace
- Dragos, Incorporated
- FireEye
- Forescout Technologies
- Fortinet
- Honeywell
- Kaspersky Labs
- Lockheed Martin Corporation
- Nozomi Networks Incorporated
- Palo Alto Networks, Incorporated
- Positive technologies
- Radiflow
- Raytheon Technologies Corporation
- Sophos Group plc
- Verve Industrial Protection　他

2.2 検討会の運営

「2.1 工場等の製造現場におけるサイバーセキュリティ対策の検討」の調査の実施及び取りまとめにあたり、専門的な見地からの検討、分析、助言を得ることを目的に、工場等の製造現場のサイバーセキュリ

[10] https://prtimes.jp/main/html/rd/p/000005795.000067400.html

ティに係る有識者等からなる工場 SWG を開催した。各検討会の概要及び運営業務の内容について以下に報告する。

なお、2023 年 3 月現在、工場 SWG は、下記の委員により構成される。

岩﨑 章彦	一般社団法人電子情報技術産業協会 セキュリティ専任部長
江崎 浩	東京大学大学院 情報理工学系研究科教授
榎本 健男	一般社団法人日本工作機械工業会 技術委員会 標準化部会 電気・安全規格専門委員会委員（三菱電機株式会社 名古屋製作所ドライブシステム部 専任）
桑田 雅彦	日本電気株式会社 デジタルネットワーク事業部門 兼 テクノロジーサービス部門 サイバーセキュリティ事業統括部 シニアプロフェッショナル(サイバーセキュリティ)（Edgecross・GUTP 合同 工場セキュリティ WG リーダー）
斉田 浩一	ファナック株式会社 IT 本部情報システム部五課 課長
佐々木 弘志	フォーティネットジャパン合同会社 OT ビジネス開発部 部長（IPA ICSCoE 専門委員）
斯波 万恵	株式会社東芝 サイバーセキュリティ技術センター 参事（ロボット革命イニシアティブ(RRI)産業セキュリティ AG）
高橋 弘宰	トレンドマイクロ株式会社 OT セキュリティ事業部 OT プロダクトマネジメントグループ シニアマネージャー
中野 利彦	株式会社日立製作所 制御プラットフォーム統括本部 大みか事業所 セキュリティエバンジェリスト
市岡 裕嗣	三菱電機株式会社 名古屋製作所 ソフトウエアシステム部 部長
藤原 剛	DMG MORI Digital 森精機株式会社 制御開発本部コネクティビティー部 副部長
松原 豊	名古屋大学大学院 情報学研究科准教授
村瀬 一郎	技術研究組合制御システムセキュリティセンター 事務局長
渡辺 研司	名古屋工業大学大学院 社会工学専攻教授

2.2.1 第4回工場 SWG の運営

（1） 開催概要

日時 2022 年 11 月 1 日 16:30～18:00

場所 Teams 会議(Web 会議)

議題

1. 開会
2. 「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(案)」に対する意見募集で頂いたご意見への対応について
3. 工場セキュリティに関する動向について
4. デジタル臨時行政調査会における取組みについて
5. 制御セキュリティ関係の最近の動向及び「工場セキュリティガイドライン」の普及啓発について

6. 自由討議
7. 閉会

配布資料：

資料1　議事次第・配付資料一覧
資料2　構成員等名簿
資料3　「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（案）」に対する意見募集で頂いたご意見への対応について
資料4　半導体セキュリティ規格「SEMI E187」について
資料5　経済産業省「工場セキュリティガイドライン」を活用したサプライチェーンセキュリティ向上の取組
資料6　デジタル臨時行政調査会作業部会　テクノロジーベースの規制改革推進委員会の取り組み
資料7　制御セキュリティ関係の最近の動向及び工場セキュリティガイドラインの普及啓発に向けて
参考資料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（案）」に対する意見募集で寄せられた御意見に対する考え方
参考資料2　「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」概要資料
参考資料3　「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）議事要旨

産業サイバーセキュリティ研究会 WG1（制度・技術・標準化）工場 SWG（第 4 回）議事要旨

日時：令和 4 年 11 月 1 日（火）16 時 30 分～18 時 00 分
構成員：
（座長）江崎　浩　東京大学大学院 情報理工学系研究科 教授
市岡　裕嗣　三菱電機株式会社 名古屋製作所 ソフトウエアシステム部 部長
岩﨑　章彦　一般社団法人電子情報技術産業協会 セキュリティ専任部長
榎本　健男　一般社団法人日本工作機械工業会 技術委員会 標準化部会 電気・安全規格専門委員会 委員（三菱電機株式会社名古屋製作所ドライブシステム部 専任）
桑田　雅彦　日本電気株式会社 デジタルネットワーク事業部門 兼 テクノロジーサービス部門 サイバーセキュリティ事業統括部 シニアプロフェッショナル（サイバーセキュリティ）（Edgecross・GUTP 合同工場セキュリティ WG リーダー）
斉田　浩一　ファナック株式会社 IT 本部情報システム部五課 課長
佐々木　弘志　フォーティネットジャパン合同会社 OT ビジネス開発部 部長（IPA ICSCoE 専門委員）
斯波　万恵　株式会社東芝 サイバーセキュリティ技術センター 参事（ロボット革命イニシアティブ（RRI）産業セキュリティ AG）

高橋　弘宰	トレンドマイクロ株式会社 OT セキュリティ事業部 OT プロダクトマネジメントグループ シニアマネージャー
中野　利彦	株式会社日立製作所 制御プラットフォーム統括本部 大みか事業所 セキュリティエバンジェリスト
藤原　剛	ビー・ユー・ジーDMG 森精機株式会社 制御開発本部コネクティビティー部 副部長(代理:菅野 靖洋)
松原　豊	名古屋大学大学院 情報学研究科准教授
村瀬　一郎	技術研究組合制御システムセキュリティセンター 事務局長
渡辺　研司	名古屋工業大学大学院 社会工学専攻教授

議題:

1. 開会
2. 「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(案)」に対する意見募集で頂いたご意見への対応について
3. 工場セキュリティに関する動向について
4. デジタル臨時行政調査会における取組みについて
5. 制御セキュリティ関係の最近の動向及び「工場セキュリティガイドライン」の普及啓発について
6. 自由討議
7. 閉会

要旨:

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(案)」に対する意見募集で頂いたご意見への対応について

・ 資料3を事務局より説明

2.工場セキュリティに関する動向について

・ 資料4を高橋委員・今野様(TXOne)、資料5を佐々木委員より説明

3.デジタル臨時行政調査会における取組みについて

・ 資料6をデジタル臨時行政調査会事務局より説明

4.制御セキュリティ関係の最近の動向及び「工場セキュリティガイドライン」の普及啓発について

・ 資料7を事務局より説明

5.自由討議

(1)普及啓発に関するご意見

・ 本ガイドラインは重要インフラに係るような工場といった特にインパクトが大きいところから普及させていくとよい。
・ 工場におけるセキュリティ対策は、投資の判断が必要なため経営層を積極的に巻き込んで行うべきである。
・ 本ガイドラインを読み対策まで取り組んでもらえるよう、付録のチェックリストを簡易チェックリストとしてご提示いただき、工場セキュリティの担当者が手を動かせるところから活用できるような形で公表できるとよい。

・ 工場のセキュリティ対策においては、工場の製造装置自体のセキュリティ対策も推進する必要がある。製造装置のメーカーの方々に対しても普及啓発を進めていけるとよい。
・ 半導体の SEMI 規格と本ガイドラインは整合性が取られているのか。
  ➢ SEMI の規格については半導体の業界団体の中で策定されたものであるため、現時点では、経済産業省のガイドラインとは未連携だが、今後、情報が整理できたら共有したい。
・ 製品ごとに国際規格・国際法規が整理されている分野とそうではない分野がある。セキュリティの規格動向や国際規格について分野毎に取りまとめることが必要ではないか。また、海外の工場におけるセキュリティについて、部品の調達要件や工場誘致の際に満たすべきガイドラインの動向を把握できると、今回のガイドラインの重要性をより分かりやすく示せると思う。
・ 本ガイドラインはユースケースとして利用できる一方で、業界によって制約や要件が異なっており、業界ごとの特徴を整理すると良い。

(2)ガイドラインの承認

・ ガイドラインについては江崎座長と相談の上、速やかに公表する。
・ (一同承認)

(以上)

(3) 会議運営業務

会議運営業務として、日程調整、Web 会議環境確保、会議運営に必要な備品等準備、資料準備、Web 会議室設営、出欠確認、会議運営、議事録作成、委員に対する謝金支払い等を実施した。

2.2.2 第5回工場 SWG の運営

(1) 開催概要

日時　2023 年 3 月 10 日 9:30～11:15
場所　Teams 会議(Web 会議)
議題

1. 開会
2. 制御システムにおけるセキュリティ対策推進の取組について
3. ガイドラインの普及について
4. 令和4年度に行った調査結果及び今後の取組について
5. 自由討議
6. 閉会

配布資料:

資料1　議事次第・配付資料一覧
資料2　構成員等名簿
資料3　制御システムセキュリティ対策支援活動のご紹介
資料4　工場セキュリティガイドライン普及活動とフィードバック紹介
資料5　令和4年度に行った調査結果及び今後の取組について

（2）議事要旨

産業サイバーセキュリティ研究会 WG1（制度・技術・標準化）工場 SWG（第 5 回）議事要旨

日時：令和 5 年 3 月 10 日（金）9 時 30 分～11 時 15 分
構成員：
（座長）江崎　浩　　東京大学大学院 情報理工学系研究科 教授
市岡　裕嗣　三菱電機株式会社 名古屋製作所 ソフトウエアシステム部 部長
（代理：松田　規、柴田 陽一）
岩﨑　章彦　一般社団法人電子情報技術産業協会 セキュリティ専任部長
榎本　健男　一般社団法人日本工作機械工業会 技術委員会 標準化部会 電気・安全規格専門委員会 委員（三菱電機株式会社名古屋製作所ドライブシステム部 専任）
桑田　雅彦　日本電気株式会社 デジタルネットワーク事業部門 兼 テクノロジーサービス部門 サイバーセキュリティ事業統括部 シニアプロフェッショナル（サイバーセキュリティ）（Edgecross・GUTP 合同工場セキュリティ WG リーダー）
斉田　浩一　ファナック株式会社 IT 本部情報システム部五課 課長
佐々木　弘志 フォーティネットジャパン合同会社 OT ビジネス開発部 部長（IPA ICSCoE 専門委員）
斯波　万恵　株式会社東芝 サイバーセキュリティ技術センター 参事（ロボット革命イニシアティブ（RRI）産業セキュリティ AG）
高橋　弘宰　トレンドマイクロ株式会社 OT セキュリティ事業部 OT プロダクトマネジメントグループ シニアマネージャー
中野　利彦　株式会社日立製作所 制御プラットフォーム統括本部 大みか事業所 セキュリティエバンジェリスト
藤原　剛　　DMG MORI Digital 株式会社 制御開発本部コネクティビティー部 副部長
（代理：菅野 靖洋）
松原　豊　　名古屋大学大学院 情報学研究科准教授
村瀬　一郎　技術研究組合制御システムセキュリティセンター 事務局長
渡辺　研司　名古屋工業大学大学院 社会工学専攻教授

議題：
1. 開会
2. 制御システムにおけるセキュリティ対策推進の取組について
3. ガイドラインの普及について
4. 令和 4 年度に行った調査結果及び今後の取組について
5. 自由討議
6. 閉会

要旨：

1.制御システムにおけるセキュリティ対策推進の取組について

・ 資料3を IPA 高見様より説明

2.ガイドラインの普及について

・ 資料4を高橋委員より説明

3.令和 4 年度に行った調査結果及び今後の取組について

・ 資料 5 を事務局より説明

4.自由討議

(1)調査結果を踏まえた取り組みの方向性に関するご意見

・ アンケートの結果について、本社のポリシーと現場オペレーションの乖離が確認できるよう、回答者の属性ごとの分析を行ってほしい。
・ 経済産業省主催の各業界団体向けセミナーの実施や SC3 との連携等により、業界団体を通じて広く企業に周知できるとよい。業界団体から、より具体的な対策を展開いただくことが有効な普及策になりうる。
・ 各業界特有のリスクと設備や製造等守るべきものの優先度に応じた対策の検討をするべきである。また、同じ業界の事業者間で情報を共有できるような場を作ってほしい。
・ 中小企業の現場を巻き込むために、KYT のようなヒヤリハット面の教育も有効である。セキュリティを検討している者や経営層と、現場とのギャップが明確になる点でも有効である。
・ 事業者毎にリスクが異なる点について、BCP の考え方やシステムの差異を踏まえた工場システムのマトリックスを整理することで、ガイドラインの活用ができるのではないか。
・ 製薬会社等、セキュリティに対する関心が高い業界にもアプローチしてほしい。
・ 工場 SWG でも発表いただいた半導体とプラント等の業界にもアプローチを進めていただきたい。

(2)工場のスマート化に向けた対応(仮説)に関するご意見

・ デジタル臨調は、現状のアナログベースの工場のオペレーションを、どのようにデジタル化していくかという観点でテクノロジーマップを作り、要求条件を整理している。IoT デバイス等やシステムのセキュリティ要件を提示した上で、スマート化を進めるという考え方。経済産業省所管の業界と情報交換をしながらデジタル臨調の検討を進めていけば、各社の内規を含めた見直しが必要になるのでデジタル臨調の取組と経済産業省の歩調を合わせて、戦略的に検討できるとよい。
・ Society5.0 を背景としたスマート化やサプライチェーン上の脅威の観点は重要。工場を持つ顧客から聞くと、対策が IT･OT 間にファイアウォールを設置して完了することが多いようだが、PC や USB メモリ等により工場内部で感染する場合もある。工場のスマート化においても工場の内部対策について検討できるとよい。アンケート結果からデータ利活用が進められていることが明らかになったが、日本の工場のほとんどがオンプレミスのデータセンターでデータ利活用を行っており、クラウドの活用が進んでいない現状がある。クラウドにどのように移行するとよいか、そもそもクラウドに移行する必要があるか、クラウド化により本当に儲かるか等を今後議論する必要がある。また、スマート化は大手を想定していると思うが、中小企業では取引先から要請されて OT･IT を切り離しているケースも多い。どのように安全に OT･IT を繋げるかを示せると、中小

規模の方々の DX 化を推進できるのではないか。

- 自動化に完全に移行する形に近づいた際、プログラム的には正しいが、製品として正しくない事態を人間がどう確認するかが重要であり、全体の枠組みの中にスマート化した結果を検証する人材を入れていく必要がある。工場では、熟練工としてのノウハウを少ない人数に継承する流れがあるが、自動化の落とし穴にはまらないよう注意する必要がある。人間のノウハウや匠の知恵を考慮する点について記載できるとよいのではないか。
- スマートファクトリーを議論の対象にするという点は重要。資料で記載されているスマート化とスマート化により発生するリスクについての共通理解が重要と考える。具体的な例が入るとわかりやすい。配送関係の工場であると、ロボット間・工場間の連携が高まることでサイバーセキュリティのリスクの対象範囲が広がり、人材が減ることでインシデント対応の必要性が高まる。また、製造業の場合は、これまで人とロボットの間に仕切りを置くことで安全性を担保してきたが、スマート化によりロボットと人間の距離が近くなると、ロボットの停止だけではなく人に危害を与えるリスクが高くなる。従来のリスクと、スマート化した際のリスクを深掘りできるとよい。
- 海外進出に重きを置く事業者が多いと考えるが、日本のセキュリティ対策が海外でも通用するということを、データを基に示せるとよい。国によって労働者の意識も異なり、適切なセキュリティ対策も異なる。日本の工場の海外進出を後押しできるとよい。
- 大規模システムにおける人間とシステムの関係においては、人間を重視した考え方や人間の日頃の判断力が大切であるということも記載できるとよい。
- 自動化が進展すると、異常やシステム障害に対する人間の対応能力の養成が求められる。資料の多様なインシデントの経験に類するが、異常をいかに検知し、どのようにリカバリーをするかは重要であり、そのために演習・訓練が有効である。異常な事態に対応できる能力の養成に向けた人材教育・訓練の必要性を強調いただきたい。
- 重要インフラ保護の観点では技術の研究開発に注力しがちだが、運用技術をどのように養成していくかも非常に重要である。CSTI の研究開発においても、運用という観点での研究開発と、それを実現するためのソフトウェアを含めた人材の必要性を指摘している。運用での人材開発はスマート化の中でも強調する必要がある。
- セキュリティの専門人材だけではなく、DX に関わるクラウドや AI など幅のある人材の育成が重要。
- スマート化について、大企業以外の Tier2・3 サプライヤーや中小企業では人材・金銭的制約があるものの、サプライチェーン上で対策が求められているのが実態である。スマート化以前のセキュリティ対策でも同様だが、具体的な対策方法に加え、有効なアウトソーシング先や人とお金に限りがある中でどのような対策が有効か示せると、よい支援になるのではないか。
- 今後自動化システム系を納める際に、お客様への説明に向けてクラウド化の指針を示せるとよい。中小企業においてクラウド化に対して拒否反応がある現状、そのような指針を示すことで、企業が次のステップに進む後押しができると考える。
- クラウド化の成功事例があると理解してもらいやすい。今後、可能な範囲で成功事例について共有いただけるとよい。
- スマート化により外部との接続が増え、サプライチェーンでの連携が増していく中、個々のセキュリティ対策の連動をどのように行うか検討していただきたい。

・ プロダクトやコンポーネントに対するセキュリティ対策も諸外国の法規制によって要請されており、工場側の義務にも影響しているので諸外国の規制を踏まえて検討する必要がある。
・ Tier2・3 や中小企業の状況を紹介すると、ある工程にセンサーを付けて、データを取りながら、なぜ不良が生じるか等の分析をし始めたところであるが、人間が見るとすぐわかる不良を AI はまだ判別できず、人間と AI のギャップがあるのが現状である。人口減少の中で DX 化が進み、セキュリティ対策の必要があるが、Society5.0 のような世界を実現するために、どのようにTier2,3 サプライヤーを巻き込めるか、どのように底上げしていくかを常に念頭に置いて検討を進める必要がある。
・ 中小企業を含め支援することが重要である。Tier2・3 がセンサーを導入しつつある段階であれば、セキュリティが確保されたセンサーを導入いただく方向に誘導することも、工場 SWG の重要なミッションである。

（以上）

（3）会議運営業務

会議運営業務として、日程調整、Web 会議環境確保、会議運営に必要な備品等準備、資料準備、Web 会議室設営、出欠確認、会議運営、議事録作成、委員に対する謝金支払い等を実施した。

3. ビル分野関係の調査

ビルシステムのサイバーセキュリティ対策の更なる高度化、広範化、個別化に向けた調査を実施するとともに、その推進に資する体制構築に向けた調査を実施し、その成果を取りまとめ、ビルシステムにおけるサイバーセキュリティの一層の確保を図った。

3.1 ビルガイドラインの高度化のための調査

今年度は、空調編の策定、及びインシデントレスポンス・ガイドラインの策定のための各種調査、検討会の運営等を行った。

3.1.1 インシデントレスポンスに対する要求の整理

(1) 昨年度までの検討経緯

本年度の検討を開始するにあたり、昨年度までの検討経緯、結果について以下に整理した。

1) 昨年度の検討スケジュール

昨年度の検討では、4 回の小グループ検討会(作業グループ(以下、作業 G))と 2 回のビル SWG を開催した。

表 3.1-1 昨年度の検討スケジュール

開催日時	検討会	主なテーマ
2022/3/4	第 12 回ビル SWG	JDCC 建物設備システムインシデント対応ガイドを紹介
2022/3/18～24	ビル SWG 小グループ検討会(第 1 回～第 3 回)	インシデントレスポンス・ガイドラインの検討方針等について
2022/3/28	第 13 回ビル SWG	インシデントレスポンス・ガイドラインの検討の進め方について
2022/3/29	ビル SWG 小グループ検討会(第 4 回)	インシデントレスポンス・ガイドラインの検討方針等について

2) 昨年度の検討における主なご意見

a. 対象とするビルの種類

- 病院等の電源を落とせないビルでは、A 系、B 系を持っており、それらの状況について調査が必要。建物種別により、共用部は優先度が低くてよい、低層階エレベータは止まっても良い、入退館管理は警備員が見る等もある。一般ビルの場合、復旧を早くするためのフローというものを意

識するとよい。

- ビルの大きさによって、インシデント対応をフルパッケージで内製化できるところと、そうではないところが存在している。非常に細かいフルパッケージにすると取組意欲が湧きにくいので、ミニマムに出来るようにすると良い。

b. 対象とする主な読者

- フォローアップが非常に重要。インシデントの発生の後の報告や情報公開に関して、会社としての体制、ルールを会社のガバナンスの中に組み込むことが重要。フローに社内の経営層も含めるとよい。
- どのようにして常時議論、情報共有ができるチームをつくるか、ということが非常に重要。
- 設計の立場、運用の立場からそれぞれ意見交換しながらセキュリティを考える体制が今後必要。ビルオーナーが全体の調整をして、運用側、設計側を含めた体制を組めると良い。

c. 想定する攻撃

- ガイドラインの中に事例を書き込むと、緊急性の高い、重要性の高いビルの守るべきポイントを中心に、インシデントレスポンスの対応フローの検討や、データのセパレーション等の封じ込めがやりやすい。

d. 攻撃の検知方法

- 実際にはサイバーによるインシデントなのか故障によるインシデントなのかの区別がつかないということが大きな議論のポイント。汎用的なインシデント対応フローのようなものを用意し、これをベースに各社で体制等を議論してもらうという方法もある。

（2）インシデントレスポンス・ガイドラインの作成方針

1） 検討方法

ガイドラインの作成にあたっては、①事務局案の作成、②作業 G による検討、③ビル SWG における検討のサイクルで実施した。

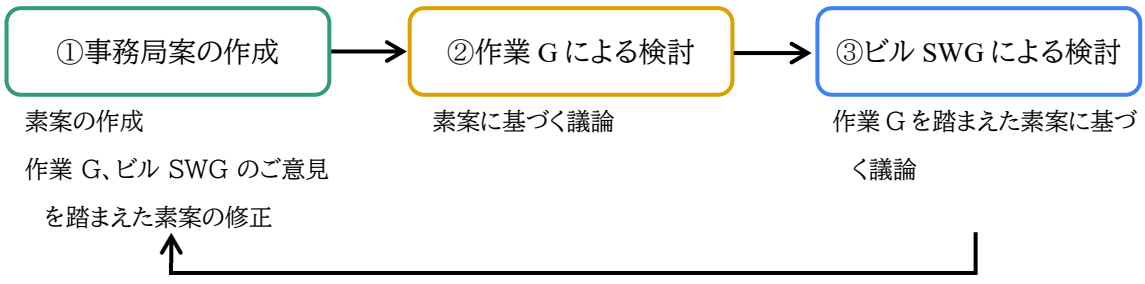


表 3.1-2 ガイドラインの検討方法

2）検討スケジュール

今年度のインシデントレスポンス・ガイドラインの検討スケジュールは以下の通りであった。インシデントレスポンス・ガイドラインを主な議題とした作業 G を 7 回、ビル SWG を 1 回開催した。

さらに、ガイドライン案について、SWG の場でのメンバーからの意見聴取、パブリックコメントによる意見募集を実施した。

表 3.1-3 今年度の検討スケジュール

開催日時	検討会等	主なテーマ
2022/10/3～4	ビル SWG 小グループ検討会（第 1 回～第 2 回）	昨年度の検討のおさらい、今年度の検討方針について
2022/10～11	（ビル管理者等への事務局ヒアリング）	ビル管理業務の実態など
2022/12/6～9	ビル SWG 小グループ検討会（第 3 回～第 4 回）	ガイドラインの作成方針について
2022/12/26～27	ビル SWG 小グループ検討会（第 5 回～第 6 回）	ガイドライン素案について
2023/1/16	ビル SWG 小グループ検討会（第 7 回）	ガイドライン素案について
2023/1/31	第 15 回ビル SWG	インシデントレスポンス・ガイドライン案について
2023/2/1～7	ガイドライン案への意見募集	－
2023/2/15～3/17	パブリックコメントの募集	－

3）ビル管理者等へのヒアリング調査

2022 年 10～11 月にかけて、ビル管理の現状を把握することを目的に、複数のビル管理者等を対象としたヒアリング調査を実施した。以下に、ヒアリング調査結果の概要を示す。

a. ビル管理の現状

- 障害が発生した場合は、まずは現場で対応し、必要に応じてベンダに連絡、社内関係部署にエスカレーションを行う（影響範囲等を踏まえて連絡先を決定・拡大）。
- 障害別に詳細なマニュアルを整備しているケース、細かいマニュアルは整備せずに概ね現場の判断に任されているケースあり。設備類の挙動は概ねパターン化されているので、現場で対応できることが多いとのこと。

b. サイバー攻撃の経験

- いずれの事業者も攻撃を受けたと認識した経験はなかった。サイバー攻撃ではないが、テナントが独自アプリで設定ファイルを意図せず変更してしまったケースはあった。
- 実被害が無ければウィルスとの共存もありうる（年 1 回の点検時に駆除など）

c. サイバー攻撃への対応

- 常にサイバー攻撃を疑って LAN ケーブルを抜くような対応は難しいし、むしろ別のリスクになる可能性がある。したがって、後手後手の対応になってしまうかも知れないが、これまで同様にベンダで原因究明してからの対応が現実的ではないか。
- 現場には、まずは「サイバー攻撃もありうる」ということを知ってもらう教育が必要ではないか。

d. インシデントレスポンスガイドについて

- 現場の管理者が読むのではなく、現場のためのマニュアルをオーナーが作成する際に参考になるものがよい。
- 参考となるような事例が多く掲載されていると良い。
- 設計時／更新時のセキュリティ対策についての情報があると良い

4）ガイドラインの作成方針

ヒアリング調査の結果、ビル SWG 及び作業 G における検討の結果、以下の方針でガイドラインを作成した。

a. ガイドラインの位置づけ

共通編ガイドラインを「第 2 版」に改定してインシデントレスポンスのエッセンスを追加し、ポイントを「付属書　インシデントレスポンス・ガイドライン」に記載することとした。

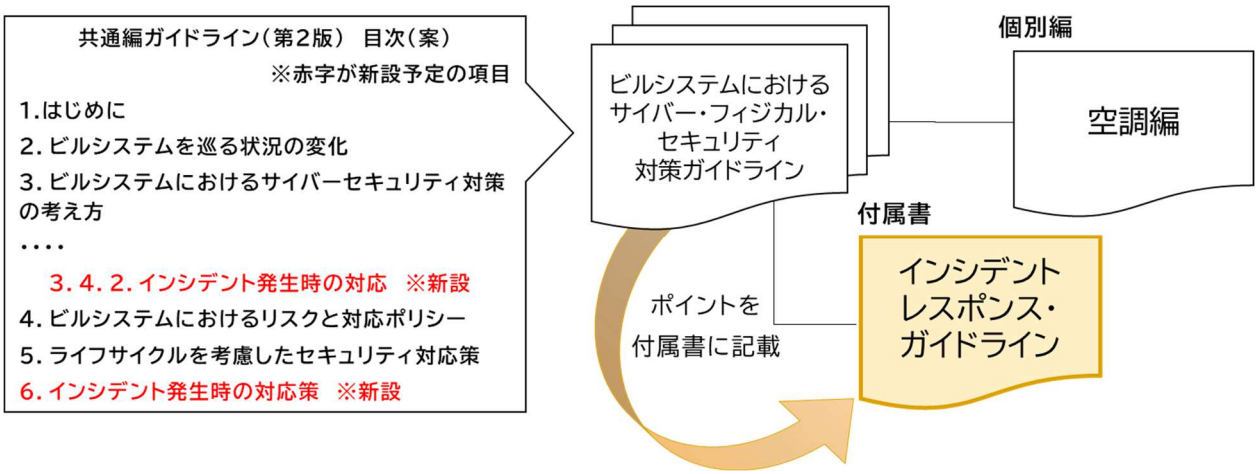


図 3.1-1　ガイドラインの位置づけ

b. 想定する読者

主な読者は「ビルオーナー」を想定し、ビルオーナーが『インシデントレスポンス・マニュアル』等を作成する際の参考としていただく。

c. ガイドラインの作成方法

日本データセンター協会（JDCC）が策定した「建物設備システムインシデント対応ガイド」をベースに、ビル管理の実態等を踏まえながら、ビル管理用のガイドラインとして作成した。

インシデント対応の流れとして、JDCC のフロー（図 3.1-2）を取り入れた。ビルシステムについては、故障等発生時に、現状では、最初からサイバー攻撃を疑うことは現実的でないため、通常の故障等対応からインシデントレスポンスへ移行するフローを想定した。

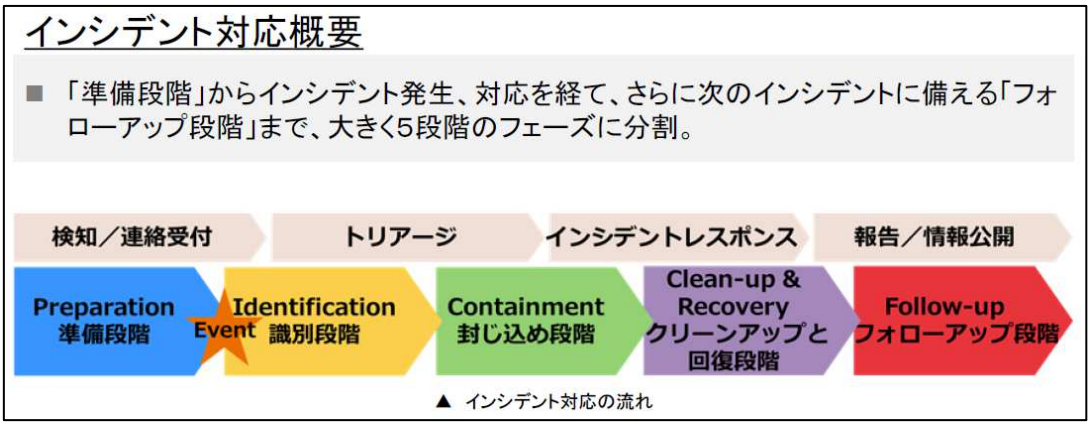


図 3.1-2 インシデント対応のフロー

d. ガイドライン（付属書）の構成（案）

表 3.1-4 付属書の目次構成

第1章 はじめに
背景・目的、本ガイドラインの位置づけ など
第2章 サイバーインシデントへの対応
インシデント対応の全体フローを示すとともに、各段階で実施すべき事項について記載
第3章 サイバーインシデント対応体制
セキュリティベンダ等における受け入れ体制等について記載
付録 A 用語集
付録 B 参考文献
付録 C 検討体制

（3） インシデントレスポンス・ガイドラインの概要

インシデントレスポンスのポイントについては、共通編に追記した（表 3.1-5）。

また、インシデントレスポンス・ガイドラインの中心であるインシデントへの対応部分について、付属書の概要を以下に示した。通常の故障対応からインシデントレスポンスへ移行するフローを図 3.1-3 に示した。

表 3.1-5 インシデントレスポンスを追記した共通編の目次

a. 準備段階

ビル管理の体制や対応フローの準備を行い、最終的にインシデント発生時に適切な初動対応を行うことができるよう準備を整える。

ア） 対応体制(インシデント対応チーム)の整備

- 対応フローの実行を想定した、インシデント発生時のチーム(社内、サブコン・設備ベンダ、セキュリティベンダ等も含む)について検討し、役割や責任等を(契約書等で)文書化する
- SOC や CSIRT、社内の各部署との連携体制についても検討する

イ） コミュニケーションルールの整備

- 誰といつどうやってコミュニケーションを行うか、関係各所の連絡先一覧・ツールを整理する
- 社内の広報、法務、営業等とのコミュニケーションルートや情報の管理ルール等も決めておくと良い

ウ） システムのバックアップ及び封じ込め方針等の検討

- 設備の設定等のシステムのバックアップを定期的に取得する
- 封じ込めにあたり、インシデントの発生個所(設備・端末、システム)毎のネットワークの切断の可否等、切断した場合のテナント等への影響、これらを踏まえた対応方針等についても検討する

エ） 教育・研修(訓練／演習等)

- 事前に検討した対応フローを正しく機能させるためには、訓練や演習が有効である

b. 識別段階

通常の故障対応では原状回復しない場合や、一旦は回復するも同様の故障が繰り返し発生する等により原因が特定できない場合は、以下の手順に進む。

ア） 現状確認・影響分析

- ビルオーナー及びビル管理者は、サブコン、設備ベンダ、セキュリティベンダ等の専門家と協力しながら、原因調査、今後の対応方針を決定するとともに、原状回復を行う。
  - 現状確認：いつ、どこで発生したか、現象の内容等を確認する　等
  - 影響分析：インシデントにより侵害された他の領域はあるか、テナント等への影響は何か　等

イ） 原因調査（ベンダ等による事象確認・影響調査等）

- 設備ベンダ等で対応（機器交換、再インストール等）し、事象確認・原因調査を行う
- 設備ベンダ等では対応できない、あるいは現象が再発する場合、複数の設備に原因・影響がある場合は、セキュリティベンダ等に支援を依頼して原因調査を行う

c. 封じ込め段階

ビル管理者は、損害を最小限に留めて、更に被害を拡大しないように、影響を受けたシステムを切り離し、その他のシステムへの被害の拡大を防ぐ。

ア） システムバックアップ

- 影響範囲や被害状況を正確に特定し、さらにはインシデントの原因を詳しく調査するフォレンジック（データの保全・解析等）を行うために必要なデータの収集を行う。
  - 影響を受けたシステムのログデータ等のコピー
  - インシデント発生後に実行したコマンド等の記録・文書化　等

イ） 封じ込め

- ビル管理者は、各設備を担当するベンダやサブコンに確認の上、「準備段階」において予め検討した方針で、ネットワークの流れを物理的に遮断（ネットワークからの隔離）する
- さらに、最終ステップとして、影響を受けたシステムにセキュリティパッチ等の対策を行い、通常運用を行えるようにする

d. クリーンアップと回復段階

影響を受けたシステムをクリーンアップ（マルウェアの駆除等）し、復元する。テナント等への実被害が認められないと判断した場合は、後日の定期点検時等においてクリーンアップすることでも構わない。

ア） クリーンアップ

- 「識別段階」において判明した原因に対処し、影響を受けたシステムへの侵害を根絶する
- 可能であれば、パッチやその他の対策でセキュリティの強化を行う
- なお、復旧にはクリーンなバックアップがあると、復旧に要する費用が安く済むとともに、時間の節約にもなる

イ） 追加調査

- 原因不明の場合は、クリーンアップと同時に、必要に応じて更なる原因究明を行い、再発防止のための情報を収集する

e. フォローアップ段階

システムの復旧後に、同じインシデントが発生しないよう対策を行う。また、インシデントに係る対外発表や外部組織への報告等もこの段階に含まれる。

ア） ビル管理者等における対策検討・実施内容の情報共有

- システム全体を本来の運用状態に回復させるために実施した事項について、ビル管理者およびサブコン、設備ベンダ等で情報共有を行う
  - 元のシステムや運用にどのような対策を行うかについて検討・実施
  - システム復元後も、再発が無いか等について定期点検等で確認・報告してもらう 等

イ） ビルオーナーにおける社内情報共有

- ビルオーナーは、発生したインシデントに係る各種情報を社内で共有する
  - インシデントとその影響（テナントへの影響等も含む）や対策についてのすべての事象に関する文書（インシデント対応レポート）を作成する
  - 対外発表や外部組織への報告を想定し、必要に応じて想定問答集を作成する
  - インシデントに対応した社内関係メンバー（法務、広報、営業など）を集め、検証会議を開催する 等

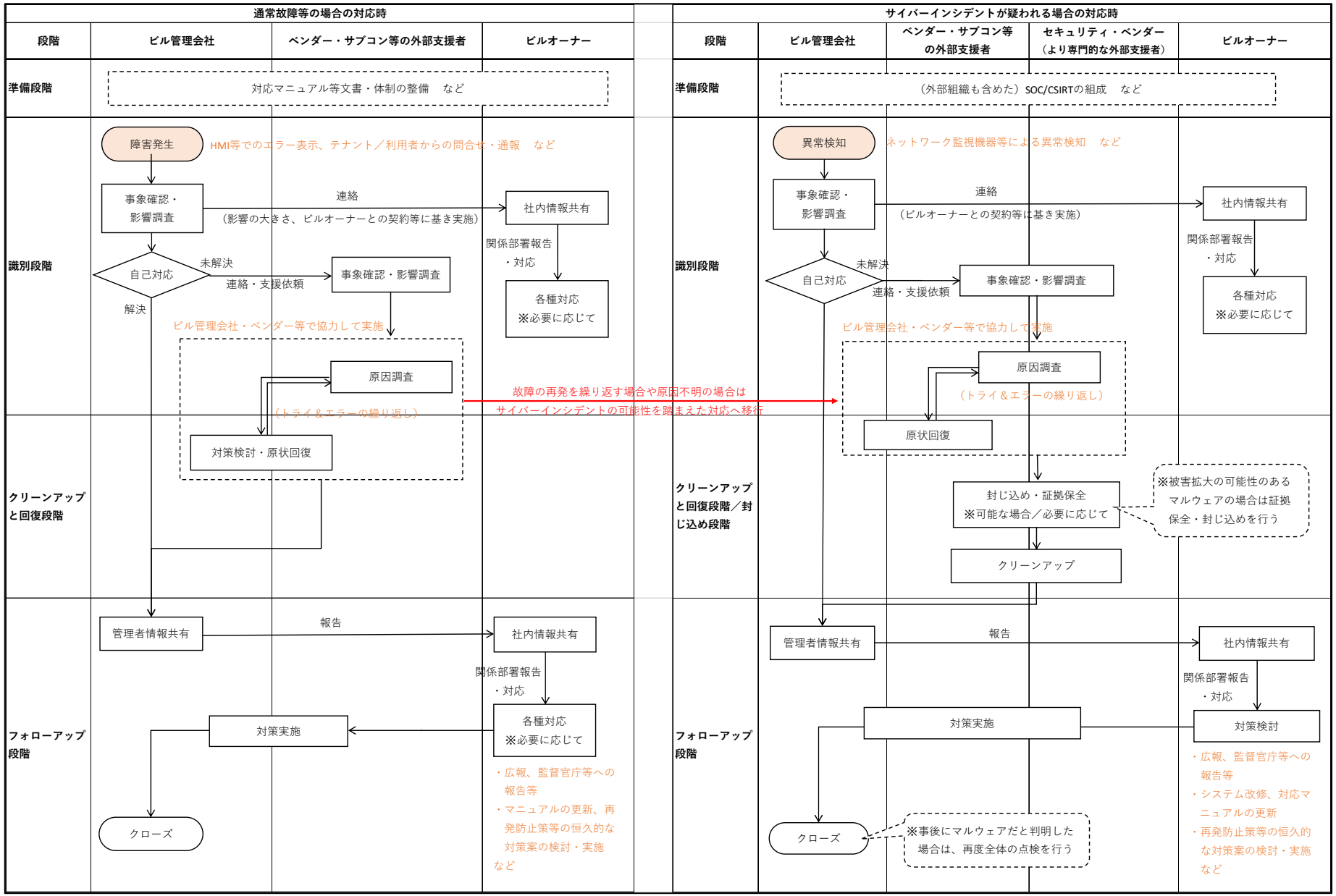


図 3.1-3 インシデントレスポンスのフロー

3.1.2 現在のガイドラインへの追加情報の充実化

（1） ビルガイドライン空調編の策定

1） パブリックコメントに基づくビルガイドライン空調編の修正作業

前年度に開催された第13回ビル SWG（令和4年3月28日開催）において「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（個別編：空調システム）（案）」について基本的な承認を得たことを踏まえて、パブリックコメントを実施した。

表 3.1-6 パブリックコメントの実施概要

「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（個別編：空調システム）（案）」についての意見募集	
期間	2022 年 5 月 10 日～2022 年 6 月 11 日
意見数	15 件

パブリックコメントの結果、全部で 15 件のコメントを受領した。コメントとしては、文書の位置づけに関する説明不足や構造のわかり難さからくる誤解と思われるコメントも存在した。また、より強い対策措置を求めるコメントなども存在した。

以下にコメントにおける主な指摘内容とその対応方針について報告する。

表 3.1-7 コメントにおける主な指摘及びその対応方針

指摘の主旨	指摘の原因	対応方針
対策要件の記述を全て完全に実施するのは非現実的である。	空調編の位置づけとして、共通編と同様に、記述はマストではなく、それぞれの状況に応じて、必要な内容をアレンジして利用することを期待しているが、その説明が不足していた。	共通編の記述を参照しつつ、ガイドラインの位置づけについての説明を追記した。特に個別サブシステムにおいても、ビル全体のセキュリティニーズに合わせる必要性があることなどを追記した。
上位ガイドラインである共通編で実施済みの対策を空調編でも個別に実施するのは過剰感がある。	空調編は共通編との差分を中心にまとめているが、利用時の利便性を考慮し、1 冊だけ見れば済むように共通編の一部を再掲している。これが、共通編同等の対策を二重に求めていると誤解される余地が生じていた。	該当記述を付録に移動し、共通編相当の記述は参考である点を明らかにするとともに、一方で同じ冊子の中で共通編の記述内容を直接に参照できるようにした。
サイバー攻撃によるシステム破壊という最悪の事態を想定し、フルバックアップ、代替機による復旧を検		重要度の高い場所への二重化による最低限の空調機能の維持や優先度に応じた対応を既に求めており、優先度の中で検討す

討するべきである。		るべきとの旨を追記した。
（その他、個別の指摘）		個別に判断が必要なものについては、個別に検討して対応をした。

上記対応方針に従い、以下のような点を修正した。なお、本編と合わせて整備した別表については特に指摘事項はなく、パブリックコメント版をそのまま公開版とすることとした。

- 1.3 節： 共通編の記述を参照しつつ、空調編ガイドラインの位置づけを追記
- 2.2 節： 空調システムを統合ネットワーク等から切り離して“単独で”操作できるようにする点の明確化
- 3 章： 空調システムの復旧の“優先順位”を考えて、必要なバックアップを準備する点を明確化
- 3.2.1.1 項： 指摘に基づく例示の追記（ただし記述内容は全体の記述方針に合わせて調整）
- 4.1 節／付録 B： 共通編の 4 章（対策ポリシー表）を再掲
- 全般： 主に誤字・脱字や日本語としての読みやすさに関して修正

これらの修正を実施した公開版（案）について、第14回ビル SWG（令和4年10月7日～10月14日に書面開催）において報告し、承認を得た。

2）ビルガイドライン空調編の概要

「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（個別編：空調システム）」（以下、ビルガイドライン空調編という）は、令和4年10月24日、経済産業省ホームページにおいて公表された。以下ではその概要を報告する。

a. ビルガイドライン共通編と空調編の関係

「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」（以下、ビルガイドライン共通編という）は、「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」に対応した分野別ガイドラインの1つとして、ビルシステム全般に共通するサイバーセキュリティ対策を体系的に整理して 2019 年 6 月に策定されたものである。

このビルガイドライン共通編に対して、個別設備固有のサイバーセキュリティ対策をまとめた個別編の1つとして、空調システムを対象としたビルガイドライン空調編を策定した。

両者の関係を下図に示す。

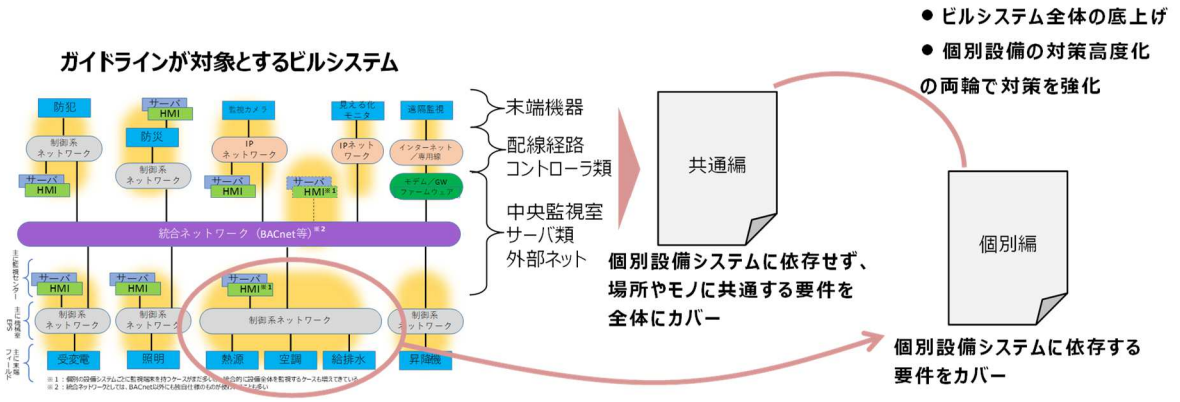


図 3.1-4 ビルガイドラインにおける共通編と個別編の関係構造

b. 想定するシステム構成

ビルガイドライン空調編は、ビルガイドライン共通編と同様に、サイバーセキュリティ対策検討の拠り所となる情報を与えるものであり、個々のビルやシステムの状況に応じて対策を調整するものとの考え方を継承している。

そのうえで内容面では、セントラル空調方式と個別分散空調方式の大きく分けて2方式があるという空調システム固有のシステム構成を考慮して、対策の整理を行っている。それぞれの方式の概略及び想定するシステム構成を以下に紹介する。

熱源機器（冷凍機、ボイラー等）で集中的に作った冷温水を給排水機によって空調機（エアハンドリングユニット、ファンコイル）に送水して空調する方式。熱源設備、給排水設備、空調設備を連携して制御する。

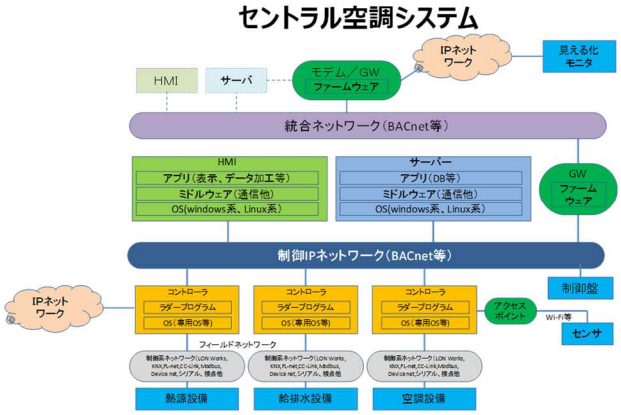
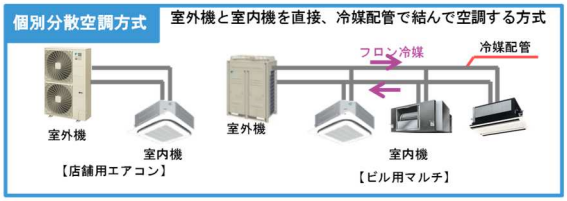


図 3.1-5 空調システムに固有なシステム構成（セントラル空調方式）



部屋に空調機（ルームエアコン、パッケージエアコンごとん、ビル用マルチエアコン等）を設置する方式で、熱源は必要箇所に分散して設置される。部屋やフロアごとに独立して運用されるが、大規模ビルでは統合ネットワーク経由で一括管理する場合もある。

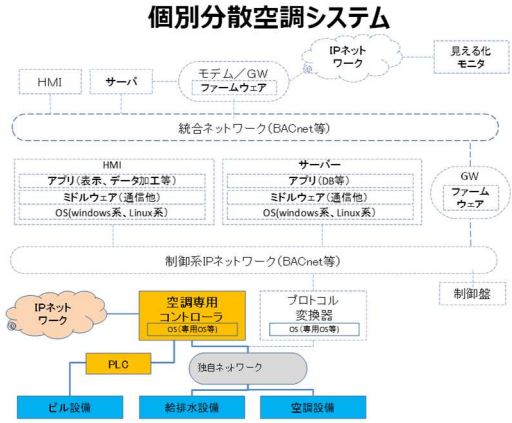
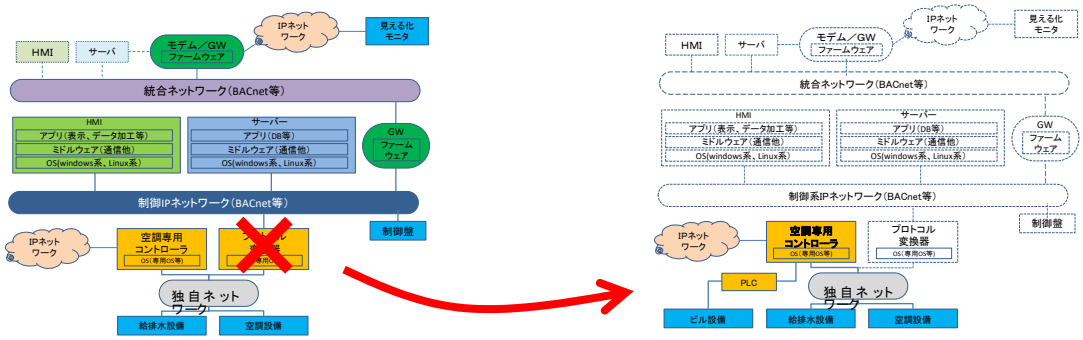


図 3.1-6 空調システムに固有なシステム構成（個別分散空調方式）

c. 空調システム特有の対策

前述のシステム構成を前提として、ビルガイドライン共通編と同様の考え方で、場所や場所に置かれる機器に対して、どのようなインシデントが発生する可能性があり、その原因となるリスク源が何で、どのような対策が求められるかという観点から、対策の整理を実施している。なお、具体的な対策としては、空調システムに求められる要求や空調システム特有の構成の基づく対策などについても考慮しており、その例を以下に紹介する。

図 3.1-7 機器自身やセンサーによる設定値逸脱の監視



上位ネットワークからの攻撃や障害波及が明らかな場合には、プロトコル変換器で切り離し、空調専用コントローラ以下を独立して運用する（個別分散空調の場合）。

図 3.1-8 緊急時の独システム専用コントローラによる運用

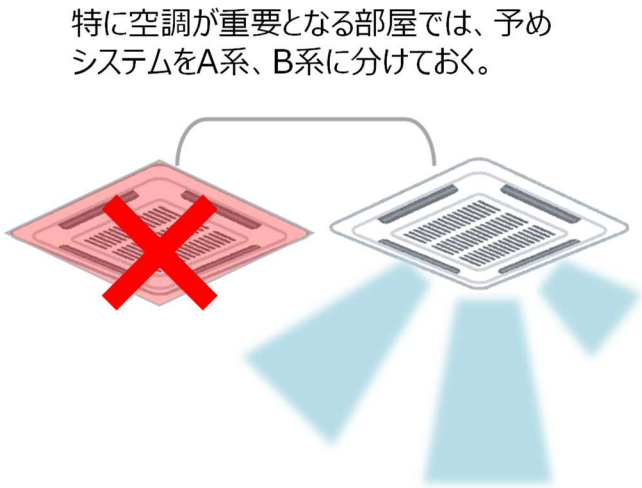


図 3.1-9 システム冗長化による最低限の運転継続

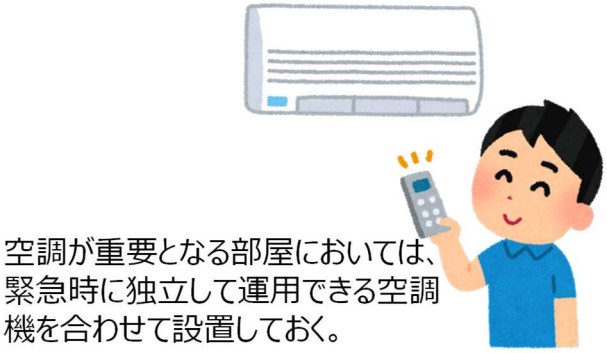


図 3.1-10 独立空調機による緊急時対応

d. 空調編の全体構成

ビルガイドライン空調編の記載内容は空調システムに特化している。ただし、空調システムのセキュリティ対策の状況をチェックし、必要な対策をビルのライフサイクルに応じて検討できるように、構成面ではビルガイドライン共通編に準拠し、ポリシー表＋別表という構成を維持している。ガイドラインの全体構成は下図のようになる。

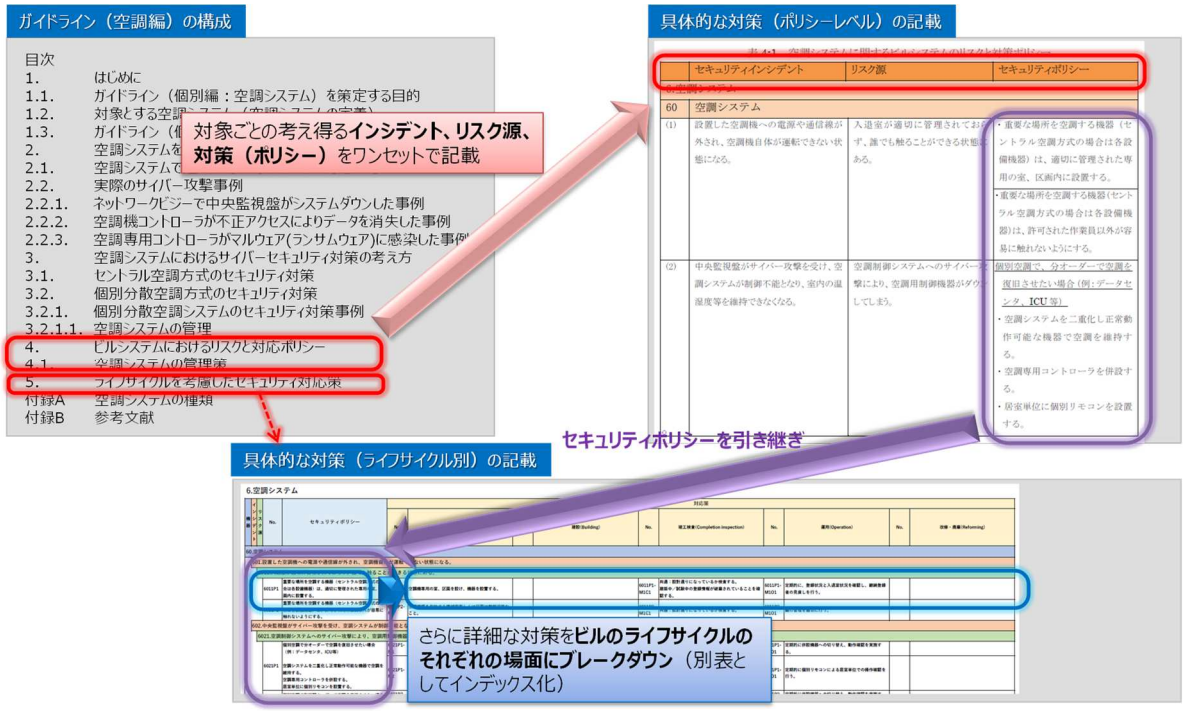


図 3.1-11 ビルガイドライン空調編の全体構成

（2）ビル関連設備の基準やガイドラインの策定状況調査

ビルシステム全体に対するサイバーセキュリティ対策立案の拠り所となるものとしては、ビルガイドライン共通編があり、今年度は個別設備に対応する個別編の1つとしてビルガイドライン空調編も正式に公開された。

それに加え、いくつかの組織では個別設備向けに何からの基準やガイドライン等を策定しているケースも存在する。ビルガイドライン共通編の付録には独立行政法人情報処理推進機構（IPA）が策定した「ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト」（2017 年 12 月 7 日初版発行、2018 年 3 月 30 日一部改訂）及び「入退管理システムにおける情報セキュリティ対策要件チェックリスト」（2019 年 5 月 20 日初版発行）が紹介されており、これらでは監視カメラシステムや防犯システムを構成する入退管理システムの導入にあたって、サイバーセキュリティ対策要件を検討・確認するためのチェックリストを提供している。このような個別設備向けに他の組織で策定されたガイドライン類についても有効活用をすることで、ビルシステム全体のサイバーセキュリティ対策のレベルを向上させることが期待される。

本調査では、ここ数年の間に新たに策定されたビル関連設備についてのサイバーセキュリティ対策の基準やガイドライン等について調査をし、取りまとめを行った。

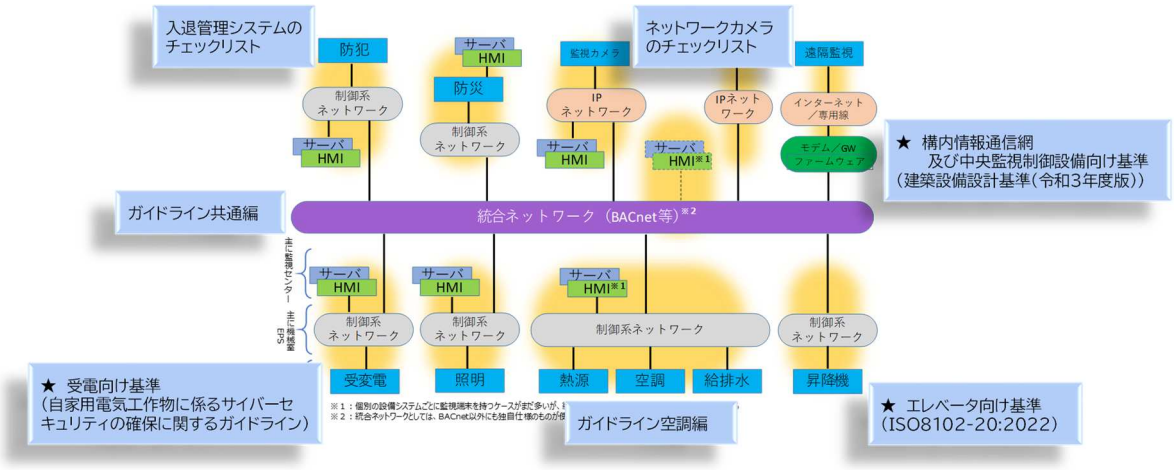


図 3.1-12 ビルシステムや関連設備システムのサイバーセキュリティに関する基準やガイドライン等（★印のものを今回調査対象とした）

1） 建築設備設計基準（令和3年度版）

国土交通省大臣官房官庁営繕部設備・環境課制定（令和 3 年 3 月 16 日国土交通省国営設第 138 号）にもとづき、一般社団法人公共建築協会が令和 3 年 8 月 12 日第 1 刷発行したもので、通称として茶本と呼ばれる文書である。国が調達する建築物について、その設備の設計基準を示したものであるが、民間ビルにおいても広く参照されており、ビル業界全体に対する影響力が非常に大きな基準である。

こちらの設備設計基準において、構内情報通信網設備及び中央監視制御設備において、情報セキュリティ／サイバーセキュリティについて言及がされており、今後、これらの設備についてはサイバーセキュリティの確保が強く意識されることになると思われる。

具体的な言及箇所、言及内容を以下に紹介する。

第3編 通信・情報設備／第1章 構内情報通信網設備／第1節 基本事項

［設計基準］

構内情報通信網設備は、必要な業務システムの利用形態を把握し、ネットワークの要件を適切に設定するものとする。

［設計資料］

構内情報通信網の設計は、次に示すシステム要件について検討及び把握を行う。

④ 安全性要件（情報セキュリティのレベル及び対象の確認）

ア 認証、暗号化等のセキュリティ対策

イ V-LAN によるセキュリティ対策

ウ VPN（Virtual Private Network）の構築

エ ワクチンソフト、アンチウィルス、アンチスパム、IPS、コンテンツフィルター等の導入

オ ファイヤウォール又は UTM の設置

カ ルータ、ファイヤウォール等のパケットフィルタリングによるアクセス制御

キ 不正防止接続システム、検疫ネットワークの構築

ク 専用の室や鍵付き専用架へのネットワーク機器の配置

第8編　共通編／第1章　中央監視制御設備／第1節　中央監視制御装置
［設計基準］
　中央監視制御装置の形式及び機能は、設備システム、管理体制等を考慮して選定する。
［設計資料］
　1－2(3)　ネットワークの安全性要件については、第 3 編第 1 章第 1 節④「安全性要件」によるほか、入居官署と協議の上、必要なサイバーセキュリティへ対策を検討する。

図 3.1-13　建築設備設計基準(令和3年度版)(通称茶本)における関連記述抜粋

建築設備設計基準(令和3年度版)では、これ以上に詳しい記述はなく、セキュリティ要件について検討を行うにあたっての具体的方法や求める対策レベルまでは示されていない。従って、実際の検討に当たっては、ビルガイドライン共通編を参照して検討が行われるケースが増えるものと想定される。

2）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

経済産業省産業保安グループ電力安全課が令和 4 年 6 月 10 日に公開したもので、自家用電気工作物についてサイバーセキュリティの確保と保安規程への記載を令和 4 年 10 月 1 日より求めるものとなっている。

ガイドラインの対象は自家用電気工作物の遠隔監視システム及び制御システム、付随するネットワークで、これらに関係する設置者、保安管理業務委託先、遠隔監視サービス事業者等とされていて、具体的にはビルの非常用発電設備や受電・配電設備が対応を求められる状況である。

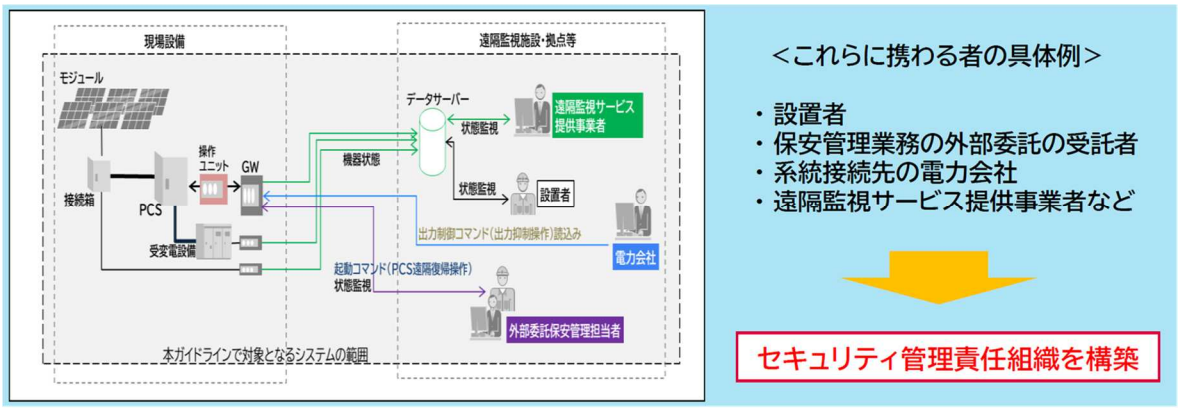


図 3.1-14　想定するシステム構成例と対象者の例
（出典：　経済産業省・家用電気工作物に係るサイバーセキュリティの確保に関するガイドラインの制定について【リーフレット】）

求められるセキュリティ水準は、遠隔監視システムや制御システムが発電設備に付随するものなのか、発電設備以外の設備に付随するものなのか、系統連携するものなのか、しないものなのかにより異なっており、最も厳しいものでは勧告的事項、それ以外では推奨的事項として提示されている。

		系統連系するもの	系統連系しないもの	ー
発電設備（需要設備の非常用予備発電装置を含む）	制御システム	区分A	区分B	
	遠隔監視システム	区分B	区分B	
発電設備以外の設備（需要設備の受配電設備等）	制御システム			区分C
	遠隔監視システム			区分C

区分A	一部勧告的事項
区分B	推奨的事項
区分C	推奨的事項

図 3.1-15 対象システムと求められるセキュリティ水準

ガイドラインでは対策を主に機器における対策、通信における対策、運用面での対策、物理的な対策の各区分に分けて整理している。

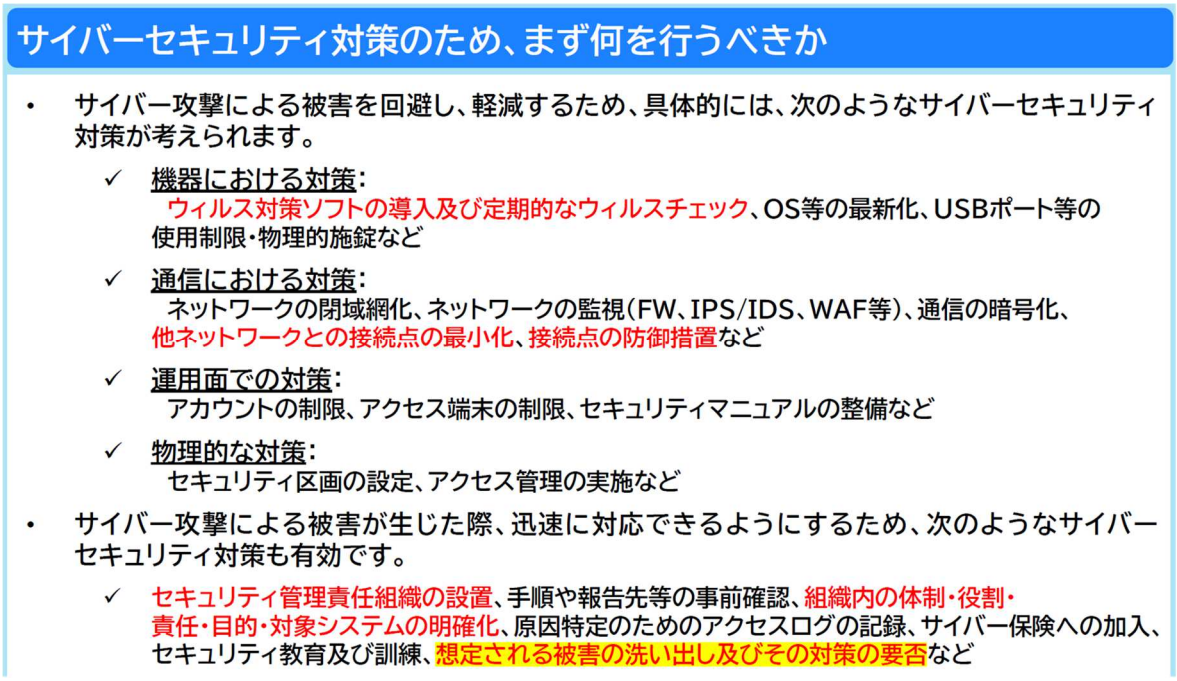


図 3.1-16 ガイドラインで示す主な対策の区分

（出典： 経済産業省・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の制定について【リーフレット】）

この自家用工作物に係るガイドラインとビルガイドライン共通編の比較を実施した。その結果、次のようなことがわかっている。

- ビルガイドライン共通編第4章の対策ポリシー表との比較の結果、大部分は相互に対応づく項目となっている
- ビルガイドライン共通編別表のライフサイクルフェーズに分けた対策については、建設及び改修・廃棄を除く設計・仕様、竣工検査、運用の各フェーズについて、対象個々についてではなく、まとまった言い方ではあるが、対応づく言及がある
- 組織や教育、セキュリティ事項の対応など、ビルガイドライン共通編ではあまり触れられていない事項への言及もみられる
- 記述レベルについては、本質的にはそれほど大きな差はないと思われるが、自家用電気工作物に係るガイドラインの方が若干詳細化されている印象である

3）Electrical requirements for lifts, escalators and moving walks -- Part 20: Cybersecurity(ISO8102-20:2022)

ISO8102シリーズとして、昇降機、エスカレータ、動く歩道についての電気的要件等を定める規格のうち、サイバーセキュリティの要件を定めるサブ規格として 2022 年 8 月 9 日に ISO から発行されたものである。その構成は以下の通りである。

1. 対象範囲
2. 参考文献
3. 用語、定義及び略語
4. リフト、エスカレータ、動く歩道の安全な開発ライフサイクル
5. セキュリティ要件
6. 使用上の注意

このうち、第 4 章及び第 5 章が具体的なサイバーセキュリティ要件を定めている部分であるが、その具体的記述においては、制御システムのサイバーセキュリティ要件をまとめた規格である IEC62443 をほぼ全面的に引用したものとなっている。

表 3.1-8 ISO8102-20:2022 の第 4 章の内容と IEC62443 の対応関係

項番及び表題	内容	IEC62443 との関係
4. リフト、エスカレータ、動く歩道の安全な開発ライフサイクル		
4.1 一般	適用対象をコンポーネント開発とシステム統合と規定し、附属書の意味づけとして安全な開発ライフサイクル(附属書 A)、セキュリティリスク評価(附属書 B)、セキュリティプラクティス(附属書 C)と規定している。	
4.2 セキュリティ管理	開発プロセス、責任の所在と明確化、適用範囲の特定、セキュリティに関する専門知識、スロセススコーピング、ファイルの整合性、開発環境のセキュリティ、秘密鍵の制御、外部提供部品に対するセキュリティ要件、サードパーティサプライヤからのカスタム開発部品、セキュリティ関連問題の評価と対処、プロセス検証、継続的改善の 13 項目	62334-4-1:2018 5 章の SM-1～13 の適用を要求
4.3 セキュリティ要求事項の仕様	製品セキュリティの背景、脅威モデル、製品のセキュリティ要件、製品セキュリティ要求事項の内容、セキュリティ要求事項の見直しの 5 項目	62334-4-1:2018 6 章の SR-1～5 の適用を要求
4.4 セキュリティバイデザイン	セキュアデザイン原則、ディフェンスインデプス設計、セキュリティ設計審査、セキュアデザインのベストプラクティスの 4 項目	62334-4-1:2018 7 章の SD-1～4 の適用を要求
4.5 セキュア実装	セキュリティ実装の見直し、セキュアコーディング標準の 2 項目	62334-4-1:2018 8 章の SI-1～2 の適用を要求
4.6 セキュリティ検証・妥当性確認テスト	セキュリティ要求テスト、脅威軽減のためのテスト、脆弱性テスト、ペネトレーションテスト、テスターの独立性の 5 項目	62334-4-1:2018 9 章の SVV-1～5 の適用を要求
4.7 セキュリティ関連問題の管理	連事項の開示、セキュリティ不具合管理業務の定期的な見直しの 6 項目	62334-4-1:2018 10 章の DM-1～6 の適用を要求
4.8 セキュリティアップデート管理	セキュリティアップデート資格、セキュリティアップデートに関するドキュメント、依存コンポーネントや OS のアップデートに関する文書、セキュリティアップデートの配信、セキュリティパッチのタイムリーな配信の 5 項目	62334-4-1:2018 11 章の SUM-1～5 の適用を要求
4.9 セキュリティガイドライン	製品防御の深化、環境に期待される深層防御対策、セキュリティハードニングガイドライン、安全な廃棄のためのガイドライン、セキュア運用ガイドライン、アカウント管理ガイドライン、ドキュメンテーションレビューの 7 項目	62334-4-1:2018 12 章の SG-1～7 の適用を要求

表 3.1-9 ISO8102-20:2022 の第 5 章の内容と IEC62443 の対応関係

項番及び表題	内容及び IEC62443 との関係
5. セキュリティ要件	
5.1 一般	
5.2 基本要件	
5.3 EUC 機能のドメイン	EUC であるエレベータ等の機能を安全性（SIL 規格（安全度水準：Safety Integrity Level）に準拠した制御機能）、基本（エレベータ等の利用可能性や安全規制への適合性を確保する機能）、警報（異常を確認し救助要請や救出のための機能）の3つのドメインに分類
5.4 EUC のセキュリティレベル要件	62443-3-3 の 7 つの基本要件（FR1～FR7）に対して、EUC 機能の 3 つのドメインのセキュリティの要求レベルを整理
5.5 セキュリティ管理・対策の選定	上記のセキュリティ要求レベルに対して、62443-3-3（システム全体に適用される要件）及び 62443-4-2（コンポーネントに適用される要件）から必要なセキュリティ制御と対策を選択することを要求
5.6 一般的なセキュリティ制約	システム要求及びコンポーネント要求の実装に際し、62443-4-2 CCSC-1（Support of essential functions）、CCSC-2（Compensating countermeasures）、CCSC-3（Least privilege）、CCSC-4（Software development process）の適用を要求

3.1.3 ビルシステム及び関連するシステムへの攻撃事例の収集

ビルシステムにつながるビルオーナーや管理会社の IT システムへの攻撃は、一般企業への様々な攻撃と同様に多いと言われており、中にはランサムウェアに感染して一部の PC が動作不能に陥るようなケースもあると言われている。しかし、ビルシステムを直接的な対象としたサイバー攻撃については、その事実が表面化し、一般に明らかになった事例はほとんどない状況である。

このため、関連事例として、ビルシステム関連機器の脆弱性についての報告やビルシステムが別の攻撃の踏み台となったケースについて紹介する。

（1） ビルシステム用コントローラの脆弱性報告事例

空調システム及びビルサービスプラント向けのシーメンス PXC4.E16 コントローラで、ABT Site Engineering 及び Commissioning Tool が DoS 攻撃に悪用される可能性を持つことが指摘されており、CVE-2022-24040 として識別されている。

この脆弱性により、コントローラの使用状況によっては、例えば火災警報システムに壊滅的な攻撃を仕掛ける可能性があるとされている。

図 3.1-17 シーメンス PXC4.E16 コントローラ

※情報出典： https://www.securityweek.com/hackers-can-make-siemens-building-automation-controllers-unavailable-days
https://www.nozominetworks.com/blog/nozomi-networks-discovers-vulnerability-in-siemens-building-automation-software/

（2）入館認証システムの脆弱性報告事例

Aiphone の建物向けインターホンシステム GT-DMB-N、GT-DMB-LVN、GT-DB-VN について、NFC 機能を備えたモバイルデバイスを使用したブルートフォース攻撃で管理者パスワードが発見される可能性があることが指摘されており、CVE-2022-40903 として識別されている。

この問題に対応するためにはハードウェア交換が必要とされている。また、スマートロックについては、当該製品以外にも多数の脆弱性報告がされている。

図 3.1-18 Aiphone GT-DMB-N、GT-DMB-LVN、GT-DB-VN

※情報出典： https://www.securityweek.com/aiphone-intercom-system-vulnerability-allows-hackers-open-doors
https://promon.co/security-news/aiphone-vulnerability/

（3）BA システムを踏み台に利用された攻撃事例

2021 年 3 月～10 月にかけて、一連の攻撃キャンペーンとして、パキスタンの製造業者、電気通信業者、アフガニスタンの通信事業者、マレーシアのロジスティクスおよび輸送組織（港）への不正侵入事案が発生した。

原因としては、Microsoft Exchange の CVE-2021-26855 脆弱性を悪用し、ShadowPad バックドアを各事業者のエンジニアリングコンピューターにダウンロードし、感染を広げたことが分かっている。

そのうちの1つ、パキスタンの電気通信事業者では、BA システムのエンジニアリングコンピューター経由での侵入が実行されていた。

各組織ではドメイン認証資格情報が窃取され、中国語を話す攻撃アクター（HAFNIUM という指摘と PKPLUG という指摘があり）へ、認証情報が送られていたものと推定されている。攻撃者の最終目的は不明だが、情報収集が目的と推定されている。

※情報出典： https://www.securityweek.com/chinese-hackers-target-building-management-systems
https://ics-cert.kaspersky.com/publications/reports/2022/06/27/attacks-on-industrial-control-systems-using-shadowpad/?utm_source=press-release&utm_medium=email&utm_campaign=attacks-on-industrial-control-systems-using-shadowpad/

（4）監視カメラシステムに対する攻撃事例

ビル設備ではないが、河川用の監視カメラシステムが 2023 年 1 月以降、不正アクセス被害により運

用停止状態に追い込まれている。

国土交通省近畿地方整備局が管理する河川監視用のカメラのうち、2020 年 4 月 1 日以降順次整備が行われてきた「簡易型河川監視カメラ」と呼ばれるインターネット接続タイプのカメラ 261 台が被害にあったほか、中国地方や四国地方でも被害が確認され、同じタイプの監視カメラ 300 台以上が運用を休止している。「簡易型河川監視カメラ」の画像は、国土交通省の「川の防災情報」サイトで公開され、豪雨時の河川状況の把握や避難判断等の防災に活用されているが、一部の河川画像が配信されない状況となっている。

原因としては、工場出荷時の初期パスワードから変更されておらず、メモリー容量の制限からウィルス対策ソフトの導入も難しいことなどが挙げられている。

通信事業者から通常時の100倍近い異常な通信量が発生しているとの指摘を受けて調査した結果、海外サーバを経由したアクセス試行が確認され、不正アクセスが判明したもの。サイバーセキュリティの専門家によると、が別のサイバー攻撃の踏み台として悪用された可能性が指摘されている。

ビルシステムに直接接続している監視カメラであれば被害発生の可能性は少ないと考えられるが、4G 回線や 5G 回線経由でつなぐタイプを後付けで設置する場合などには、同様の状況に置かれる可能性もあるため、注意が必要である。

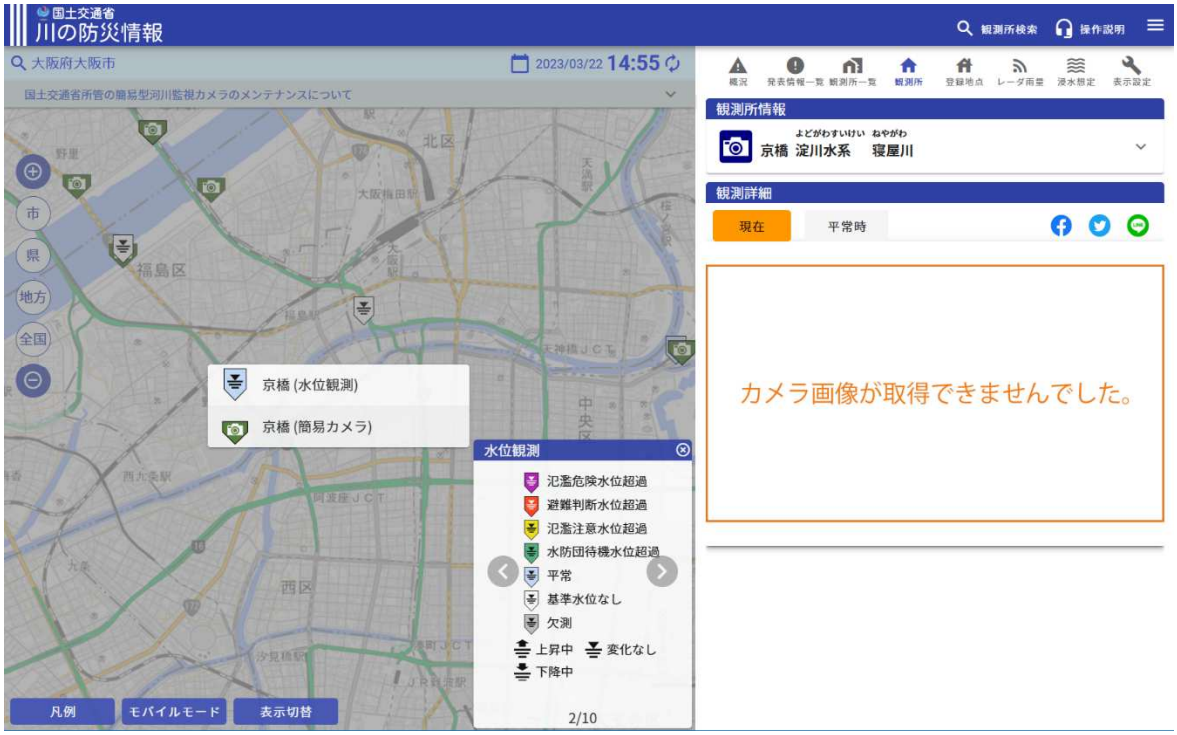


図 3.1-19 簡易型河川監視カメラの画像配信が停止中の「川の防災情報」サイト

※情報出典： https://mainichi.jp/articles/20230302/k00/00m/040/206000c
https://www.sankei.com/article/20230302-XGKIZ6F5JFPLVDMNGCYWW4S7RY/
https://www.yomiuri.co.jp/national/20230302-OYT1T50160/
https://www3.nhk.or.jp/news/html/20230303/k10013997691000.html
https://www3.nhk.or.jp/news/html/20230304/k10013998191000.html
https://xtech.nikkei.com/atcl/nxt/column/18/00142/01554/

3.2 ビルシステムのサイバーセキュリティ推進体制の調査

ビルガイドライン共通編が 2019 年 6 月に公開されてから 3 年以上が経過し、「3.1.2(2)現在のガイドラインへの追加情報の充実化」で紹介したようにビルの個別設備に関するサイバーセキュリティ対策のガイドライン類の整備も進みつつある。

このような状況にあわせて、ビル業界のサイバーセキュリティ対策も大手ビルオーナーの新築ビルを中心に進みつつあるが、さらなる対策推進のためには、ビル業界全体としてサイバーセキュリティ対策を推進する体制を整えることが急務である。特にビルでは、ビルオーナー、建設会社、設計事務所、各種設備ベンダ、運営会社等、多くの立場の異なるプレイヤーが関わっており、このようなマルチステークホルダーの世界においてサイバーセキュリティ対策を推進し、ガイドラインを維持・高度化していくためには、特定のステークホルダーによらず、マルチステークホルダーからなる相応の推進体制を整備していくことが必要である。

重要インフラを中心に各業界において ISAC 設置が進みつつあり、サイバー攻撃に関する各種情報共有、サイバーセキュリティへの意識啓発や教育活動、対策実装に向けた相談・コンサルティング、ガイドライン類の整備・普及等の活動を実施している。

本調査では、他業界におけるサイバーセキュリティ推進活動について調査をし、その動向を参考にしつつ、ビル業界として望まれるサイバーセキュリティ推進体制について整理を実施した。

3.2.1 他業界における ISAC の動向

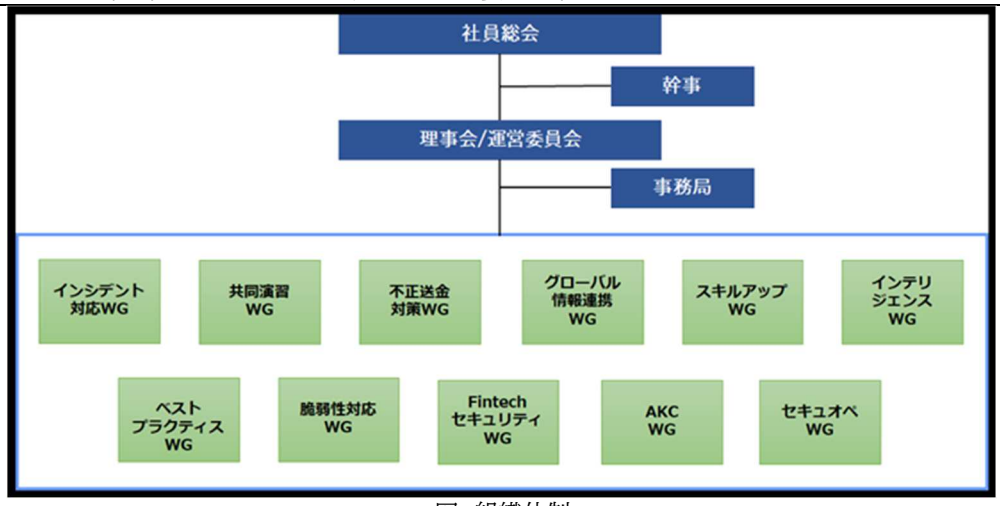
他業界における ISAC の動向として、以下 ISAC について情報を整理した。カッコ内は設立年月である。

- 金融 ISAC(2014 年 8 月)
- ICT-ISAC(2016 年 3 月)
- 日本貿易会 ISAC(2016 年 4 月)
- J-Auto-ISAC(2017 年 1 月)
- 電力 ISAC(2017 年 3 月)
- ソフトウェア ISAC(2018 年 8 月)
- 医療 ISAC(2019 年 10 月)
- 交通 ISAC(2020 年 4 月)

(1) 金融 ISAC

表 3.2-1 金融 ISAC の概要

設立年月	2014 年 8 月
ホームページ	http://www.f-isac.jp/index.html
目的	金融 ISAC は、日本の金融機関の間でサイバーセキュリティに関する情報の共有・分析、及び安全性の向上のための協働活動を行い、金融サービス利用者の安心・安全を継続的に確保することを目的としている。 金融 ISAC では専用のポータルサイトを通じ、日々のインシデントや脆弱性情報等をリアルタイムに共有している。また、特定の重要課題について、テーマごとにワーキンググループ(WG)を設け、会員共同で対策検討等を行いながら、知見と対応力を高めている。これらの成果はワークショップやアニュアルカンファレンス等の場で発表し、ポータルサイトに成果物の蓄積を行っている。
活動内容・機能	● 情報セキュリティに関する情報の分析及び共有

	● 物理セキュリティに関する情報の分析及び共有 ● 金融機関の情報セキュリティ及び物理セキュリティを含む安全対策に関するコンセンサス作成 ● 情報セキュリティ及び物理セキュリティに関する啓発 ● その他当法人の目的を達成するために必要な事業
組織体制	 図 組織体制 正会員(427 社) ● ホールディングス ● 銀行 ● 証券 ● 生命保険 ● 損害保険 ● カード・ファイナンス ● 信金・信組 ● 労働金庫 ● その他 賛助会員 ● 一般社団法人 JPCERT コーディネーションセンター アフェリエイト(ゴールド、シルバー、ブロンズ) ● 主にセキュリティベンタ
WG 等の活動内容	● インシデント対応 WG 従来は危機管理対応や BCP の一環として行っていたインシデント対応をサイバーセキュリティ特有のインシデントという観点から見直し、基本手順の検討やマニュアルの作成について議論し、成果物を会員間で共有している。 ● 共同演習 WG 会員各社が連携して行う「共同サイバー演習」の企画・運営をするとともに、国内外で行われているサイバー演習の事例やノウハウの収集と共有を推進している。 ● 不正送金対策 WG 主にバンキングマルウェアによる攻撃の最新手口とその対策の収集と共有を行いながら、不正送金対策のベストプラクティスを検討している。 ● グローバル情報連携 WG 米国 FS-ISAC との情報共有範囲の拡大を図り、共有可能な各種情報のローカライズ(日本語化)を行うなどの活動を実施している。 ● スキルアップ WG 金融機関のセキュリティ担当として必要な知識やスキル、金融 ISAC において共有された情報を活用するスキルの確保・向上に取り組み、各種勉強会などを企画・実施している。 ● インテリジェンス WG 様々な情報ソースから攻撃傾向や近い将来に発生が想定される攻撃、攻撃手法等を類推・予測することを試み、加えて効果的な防御体制の準備・構築についても検討・議論している。 ● ベストプラクティス WG

	金融機関におけるサイバーセキュリティ対策として、会員各社のノウハウ・知見に基づいた、「実践力のある、生きた取り組み」をベストプラクティスとしてとりまとめる。 ● 脆弱性対応 WG 製品プログラム・システム物理機器に焦点をあて、脆弱性対応の方法を検討します。また、脆弱性に関する会員間の情報共有・連携の方法についても検討し、とりまとめる。 ● FinTech セキュリティ WG 新しい技術及びその利用方法を表す用語として広がっている FinTech について、セキュリティ上のリスクと強化について検討します。また、関連諸団体、FinTech 企業との連携を図る。 ● AKC （Active Knowledge Center）WG サイバーセキュリティ対策について、どのように進めればよいか分からないという悩みを持つ会員企業に対し、各々の身の丈に合った施策が実行できるよう、各地域に出向きつつ、機動的かつ具体的なサポートを実現している。 ● セキュリティオペレーション高度化（セキュオペ）WG サイバーセキュリティ運用の高度化、効率化に役立つツール、プログラム等を開発し、会員全体に提供すること。また、活動を通じ社内でツールやプログラムを内製できる人材を増やし、金融機関が独力でオペレーションできる土壌を作る。 ● 直近の主な活動 2021 年 11 月 15 日-12 月 27 日 「フォールカンファレンス 2021」を開催 2021 年 5 月 27 日-6 月 30 日 「金融 ISAC アニュアル・カンファレンス 2021」を開催 2021 年 2 月 19 日 会員合同演習 「Fire 2020」を実施 2020 年 11 月 9 日 「フォールカンファレンス 2020」を開催 2020 年 5 月 28 日 「金融 ISAC アニュアル・カンファレンス 2020」を開催 2020 年 3 月 24 日 大手町ビル3F に移転 2020 年 2 月 12-13 日 会員向け危機対応トレーニング『サイバークエストⅣ』を実施 2019 年 10 月 21-22 日 京都にてフォールカンファレンスを開催
ガイドライン等整備状況	－

活動費の状況	表　会費一覧(出典:金融 ISAC ホームページより)

		会員区分					
		正会員	トライアル会員	賛助会員	アフィリエイト会員		
					ゴールド	シルバー	ブロンズ
1	会員資格(＊1)	日本国内で営業する金融機関	日本国内で営業する金融機関	当法人の活動を賛助する法人または個人	金融機関を除く法人(ITセキュリティに関連する企業等)	金融機関を除く法人(ITセキュリティに関連する企業等)	金融機関を除く法人(ITセキュリティに関連する企業等)
2	入会方法	会員からの申込	会員からの申込	当法人からの依頼	会員からの申込	会員からの申込	会員からの申込
3	年会費(＊2)	80 万円(不課税)	初年度のみ加入可(無料)	－	300 万円(不課税)	200 万円(不課税)	100 万円(不課税)
4	理事への選任	可	不可	可	不可	不可	不可
5	運営委員への選任	可	不可	可	不可	不可	不可

(2) ICT-ISAC

表 3.2-2 ICT-ISAC の概要

設立年月	2016 年 3 月
ホームページ	https://www.ict-isac.jp/
目的	● 情報通信技術の普及、発展により、日常生活、経済、行政、安全保障・治安確保などのあらゆる活動がサイバー空間に依存するようになり、高度化・複雑化するICTへの脅威は深刻な社会的脅威となっている。当法人は、このような現状に鑑み、ICTに関わるセキュリティの対策・対応レベルの向上に資する活動を行うために、社員間の幅広い相互連携を図り、安定した情報流通、情報伝達を維持することで、安全なICT社会の形成に寄与することを目的とする。 ● 前項の目的に加えて、サイバー攻撃に対処する社員である電気通信事業者を支援することにより、電気通信役務の円滑な提供を確保し、その利用者の利益を保護することを目的とする。
活動内容・機能	(1) ICT分野の情報セキュリティに関する情報(インシデント情報を含む。)の収集、調査、分析 (2) 情報セキュリティに関する情報を目的に応じて共有し、それを活用しつつ、社員間で相互協調する仕組みを整備し、それを促進する活動 (3) 社員の情報セキュリティ人材育成の促進及びユーザが安全にICTを利用するための普及啓発活動 (4) 社員が情報セキュリティ対策を円滑に行う上で必要となるガイドラインの検討及び法制度に関する政府研究会等への参画 (5) 電気通信事業法の規定による総務大臣の認定を受けた認定送信型対電気通信設備サイバー攻撃対処協会(以下「認定協会」という。)としての業務(以下「認定協会業務」という。) (6) その他当法人の目的を達成するために必要な事業

組織体制

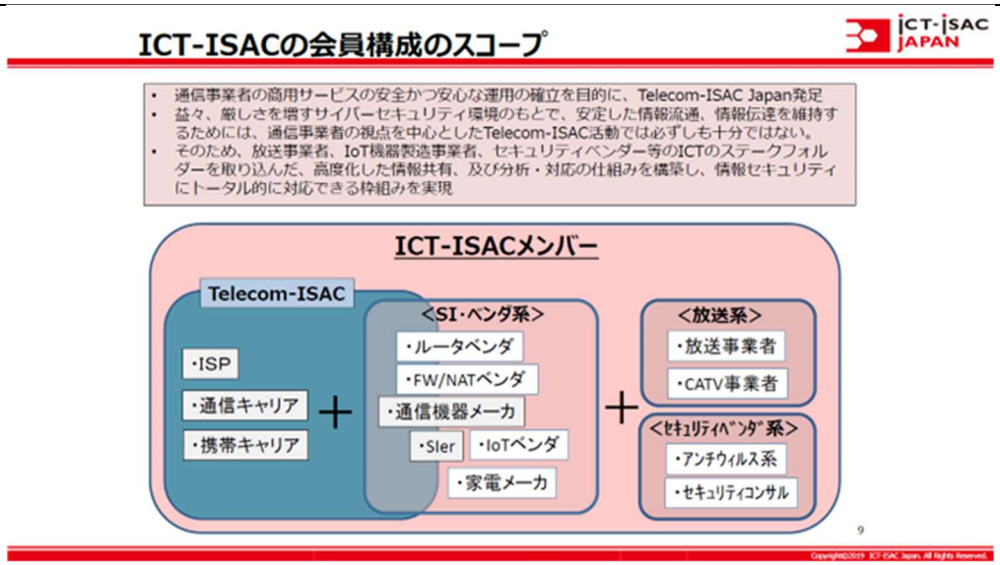


図　ICT-ISAC の会員構成のスコープ（出典：ICT-ISAC ホームページより）

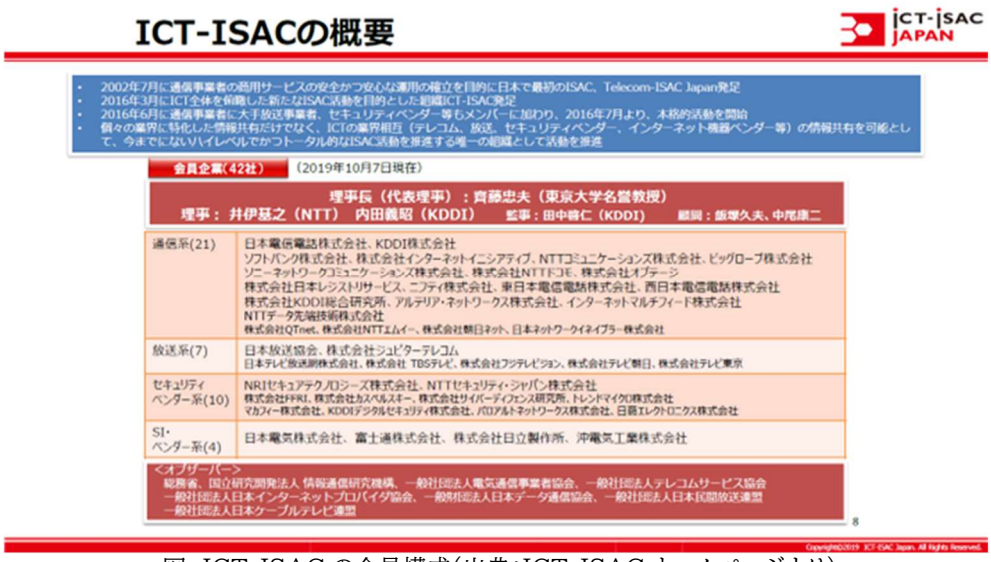


図　ICT-ISAC の会員構成（出典：ICT-ISAC ホームページより）

WG 等の活動内容

● WG 及び SIG において分野別活動を実施

WG の構成

1. **経路情報共有-WG(BGP-WG)**

設置	2005 年 7 月
責任会社	エヌ・ティ・ティ・コミュニケーションズ株式会社
活動内容	ISP 間の経路情報の共有、経路情報異常時の迅速な対応、経路奉行システムの運用

2. **ACCESS-WG**

設置	2007 年 4 月
責任会社	KDDI 株式会社
活動内容	インターネットアクセス NW サービスの運用品質向上のための情報交換、ベストプラクティス共有や有識者を交えた意見交換

3. **SoNAR-WG(Society of Network Abuse Response-WG)**

設置	2007 年 12 月
責任会社	楽天モバイル株式会社 ソニーネットワークコミュニケーションズ株式会社 エヌ・ティ・ティ・コミュニケーションズ株式会社
活動内容	ネットワークを利用した不正・不法行為対応(ABUSE 対応)に関する情報の共有、インシデントの拡大を抑止するフレームワークの策定

4. **サイバー攻撃対応演習-WG(CAE-WG)**

設置	2009 年 5 月
責任会社	株式会社 QTnet
活動内容	サイバー攻撃を想定した対応演習の企画および実施

5. **DoS 攻撃即応-WG**

設置	2011 年 10 月
責任会社	株式会社インターネットイニシアティブ
活動内容	DoS 攻撃への迅速かつ適切な対応の実現を目指し、複数事業者による協調対処の仕組みの検討、日本国内における DoS 攻撃発生の予測と早期検出

6. **通信の秘密 WG**

設置	2013 年 12 月
責任会社	エヌ・ティ・ティ・コミュニケーションズ株式会社
活動内容	総務省の各種研究会等へ参画し、電気通信事業者におけるサイバー攻撃対策を推進

7. **WiFi リテラシー向上-WG**

設置	2013 年 9 月
活動内容	情報セキュリティの観点から公衆 WiFi サービスが備えるべき要件を検討し、実現に向けて必要な取り組みや継続的な普及啓発活動を実施

8. **放送設備サイバー攻撃対策 WG**

設置	2016 年 10 月
責任会社	日本テレビ放送網株式会社
活動内容	日々変化していくサイバー攻撃に対処するため、放送事業者全体のレベルアップを推進していくことを目的とし、その時勢に対応した活動を実施

9. **IoT セキュリティ-WG**

設置	2016 年 8 月
責任会社	エヌ・ティ・ティ・コミュニケーションズ株式会社
活動内容	IoT セキュリティ強化を推進するため、脆弱な IoT 機器の実態を把握するためのアーキテクチャ検討およびシステム構築の実施、実態調査から対策検討および ICT-ISAC 他 WG との連携(通信の秘密の整理含む)や国の施策との連携の推進、定期レポートの公開等によるセキュリティリスク情報の展開、セキュリティ意識の向上のための啓発活動の実施検討

10. **セキュリティベンダ課題検討 WG**

設置	2016 年 11 月
責任会社	NRI セキュアテクノロジーズ株式会社
活動内容	セキュリティベンダ各社相互理解、個社または業界共通の課題の検討、セキュリティトピック等の情報連携の在り方について議論

11. **情報共有 WG**

設置	2016 年 11 月
責任会社	株式会社日立製作所
活動内容	情報共有に関する国際連携や各 ISAC 間連携の推進、ICT-ISAC 内での情報活用の在り方の検討

12. **交流促進 WG**

設置	2016 年 11 月
責任会社	日本電気株式会社
活動内容	ICT-ISAC 会員内の交流(ICT-ISAC 活動活性化、会員間相互理解、ノウハウ共有)と ICT-ISAC 外との交流(ICT-ISAC 活動のアピール、会員勧誘)を推進

13. **認定協会業務推進-WG**

設置	2018 年 9 月
責任会社	KDDI 株式会社
活動内容	電気通信事業法に基づく認定協会業務の推進と、NOTICE 業務を円滑に推進するための ISP 注意喚起業務の実施支援、改善策等の検討を推進

14. **サイバーセキュリティ協議会対応-WG(CSA-WG)**

設置	2019 年 3 月
責任会社	エヌ・ティ・ティ・コミュニケーションズ株式会社
活動内容	内閣サイバーセキュリティセンター(NISC)が設置するサイバーセキュリティ協議会(CS 協議会)に ICT-ISAC が構成員として参加し、CS 協議会との情報共有、ICT-ISAC 会員間の情報共有を推進

15. **国内外 ISAC 連携-WG**

設置	2019 年 4 月
責任会社	KDDI 株式会社
活動内容	国内外の信頼できる組織等と連携できる体制を整備し、継続的な連携活動を通して ICT-ISAC に貢献

16. **5G セキュリティ推進 G**

設置	2020 年 2 月
責任会社	日本電信電話株式会社
活動内容	全国規模の 5G サービスやローカル 5G など、様々な事業者が多様なサービスを提供していくことに対応し、5G セキュリティに係る情報共有を推進

SIG の構成

17. **DNS 運用者連絡会-SiG**

設置	2008 年 6 月
世話役	日本電信電話株式会社
活動内容	DNS 運用者間の組織間の情報共有・連絡体制の整備(顔の見える範囲での信頼関係の構築を含む)

18. **若手活躍-SiG**

設置	2018 年 7 月
世話役	KDDI 株式会社
活動内容	若年層に ICT-ISAC に参加する意義を伝え、また若年層が参加する環境を改善し、若者のセキュリティ離れを食い止める活動を実施

19. **NOTICE-SiG**

設置	2019 年 1 月
活動内容	「NOTICE」業務推進のための参加事業者間での情報共有

20. **法人 IoT 機器脆弱性対応 SiG**

設置	2020 年 6 月
世話役	株式会社東陽テクニカ
活動内容	IoT 機器の脆弱性放置によるセキュリティ事故リスクについて、法人向けに注意喚起する仕方について検討

21. **業界横断可用性可視化 SiG**

設置	2021 年 12 月
世話役	ソフトバンク株式会社
活動内容	契約者向けに広報周知している障害等状況情報を基にした、業界全体の稼働状況の見える化に向けた仕組みの構築と情報共有のシステム(ダッシュボード)化

ガイドライン等整備状況	● ローカル 5G セキュリティガイドライン ● 電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン ● 家庭内で安全快適に在宅勤務を行うためのリファレンスガイド ● International Anti-Botnet Guide(IABG)日本語版
活動費の状況	貸 借 対 照 表 令和 3 年 3 月 31 日現在 (単位：円) 資産の部 / 負債の部 科目 / 金額 / 科目 / 金額 【流動資産】 【 278,489,430】 【流動負債】 【 33,684,266】 現金及び預金 240,277,131 未払金 19,463,230 前渡金 108,000 未払費用 8,976,776 前払費用 1,370,580 源泉預り金 131,560 未収入金 36,733,219 預り金 20,200 預け金 500 法人税等充当金 5,092,500 負債の部合計 33,684,266 【固定資産】 【 19,859,380】 純資産の部 (有形固定資産) (11,936,978) 工具器具備品 11,936,978 【純資産】 【 264,664,544】 (無形固定資産) (2) (利益剰余金) (264,664,544) ソフトウェア 2 繰越利益剰余金 264,664,544 (投資その他の資産) (7,922,400) 敷金 7,922,400 純資産の部合計 264,664,544 資産の部合計 298,348,810 負債及び純資産の部合計 298,348,810 図 活動費の状況(出典:ICT-ISAC ホームページより)

(3) 日本貿易会 ISAC

表 3.2-3 日本貿易会 ISAC の概要

設立年月	2016 年 4 月
ホームページ	https://www.jftc.or.jp/shosha/isac/
目的	インシデント情報の入手ならびに共有、相互の対応協議を行う商社業界全体の枠組みとして、日本貿易会の会員商社におけるサイバーセキュリティ対策をサポートする。 巨大なグローバルサプライチェーンを形成し、多種多様な取引を行う商社業界にとってサイバーセキュリティ対策は不可欠との認識を共有、こうした高い危機意識のもとでそれぞれの企業において最大限の対策が取られていたものの、情報の収集・分析や対応手段の検討には相当のリソースを確保する必要があり、業界共通の課題となっていたため、「共助の精神」により業界全体でリソースを共有し、一体となってサイバー攻撃の脅威に立ち向かう枠組みを求める会員商社からの声に答えるべく、ISAC の発足に至ったものである。
活動内容・機能	①情報や事例の収集・分析・共有を図るコレクティブインテリジェンス機能 ②リソースやノウハウの共有を図るリソースシェアリング機能 NEC と JPCERT/CC の協力を得て、実務部会と技術部会を中心に活動を実施している。毎月の会合開催の他、NEC の情報提供ポータル NELP と、JPCERT/CC が提供する情報共有ツール SIGNAL を使って日常的な情報共有も実施している。

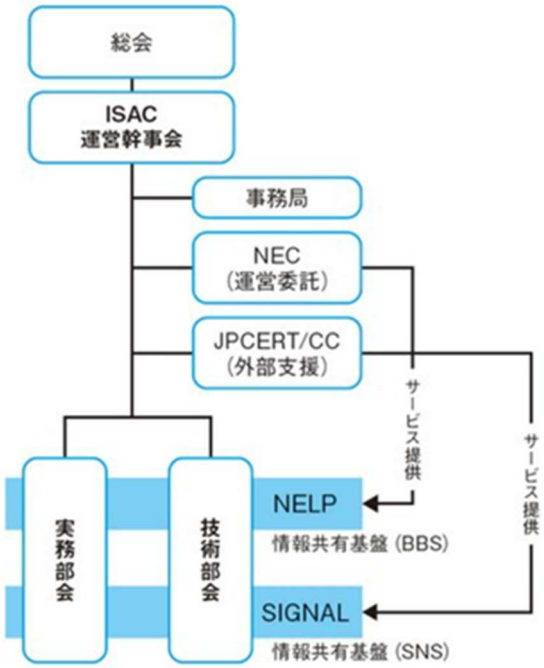
組織体制	 図　組織体制(出典:日本貿易会 ISAC ホームページより) 2021 年 3 月時点の会員は 24 社。 伊藤忠商事、伊藤忠丸紅鉄鋼、稲畑産業、岩谷産業、兼松、興和、CBC、JFE 商事、神鋼商事、住友商事、全日空商事、双日、蝶理、豊田通商、長瀬産業、日鉄物産、野村貿易、阪和興業、ホンダトレーディング、丸紅、三井物産、三菱商事、メタルワン、八木通商
WG 等の活動内容	● 実務部会は、情報システム部門の管理者を対象として、専門家との情報・意見交換を通じてサイバーセキュリティに関する動向把握、知識向上を図っている。 ● 技術部会は、情報システム部門の実務者を対象として、ワークショップやグループディスカッションを通じて相互の知見共有、スキルアップを図っている。

表 2019 年度～2020 年度の主な活動内容(出典:日本貿易会 ISAC ホームページより)

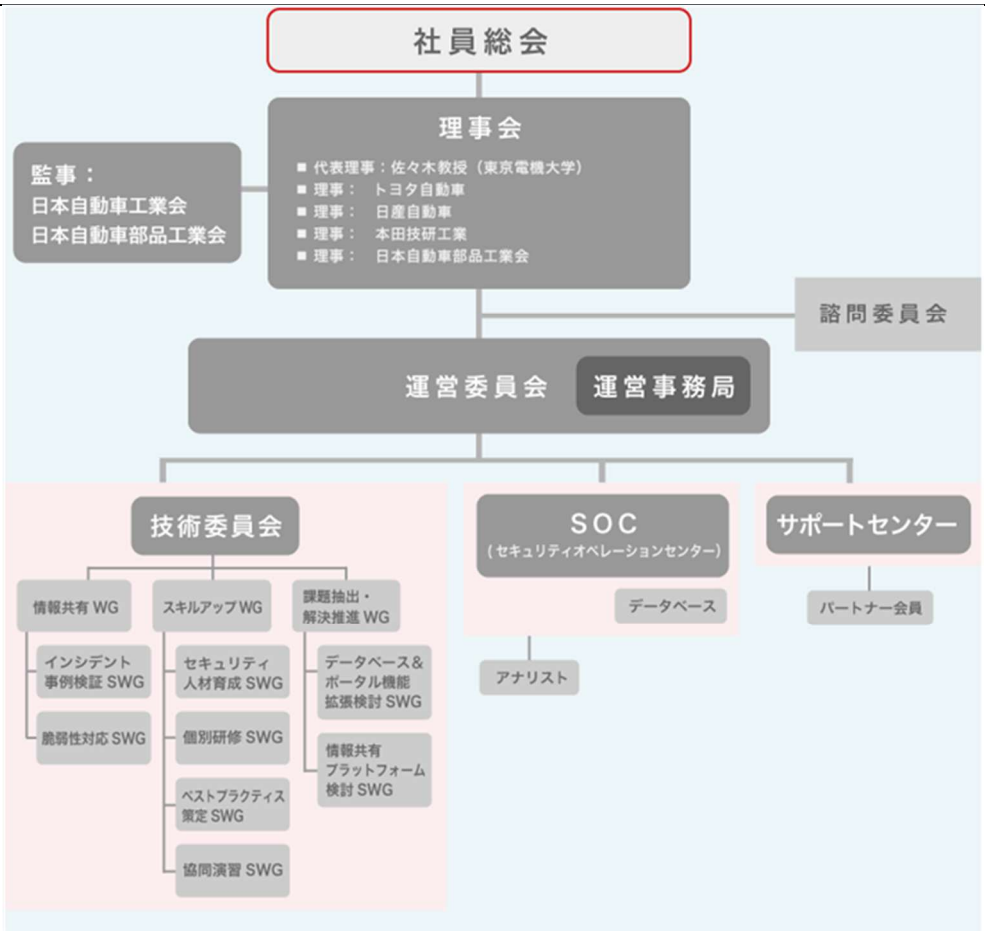
2019/3/15	第6回技術部会	・実機演習「インシデントハンドリングトレーニング 講師：NECネクサソリューションズ㈱ 技術開発事業部 マネージャー 小峰光氏 主任 駒崎修氏
2019/4/19	第7回実務部会	・情報交換「セキュリティ施策」
2019/5/24	第7回技術部会	・講演「セキュリティ担当者として知っておきたいこと」 講師：(一社) JPCERT/CC 早期警戒グループ 情報セキュリティアナリスト 森淳太郎氏
2019/6/21	第8回実務部会	・講演「徹底解説、サイバー空間をめぐる脅威」 講師：日本電気㈱ サイバーセキュリティ戦略本部 エグゼクティブディレクター 木村公也氏
2019/7/19	第8回技術部会	・講演「最新の攻撃事例から学ぶ、明日から始める防衛策」 講師：日本電気㈱ サイバーセキュリティ戦略本部 セキュリティ技術センター 小池倫太郎氏 ・講演「電子決裁サービスに関する振り返りと教訓」 講師：(一社) JPCERT/CC 早期警戒グループ 情報セキュリティアナリスト 森淳太郎氏 ・グループディスカッション「最近警戒している攻撃と明日からの対応について」
2019/8/16	第9回実務部会	・講演「近隣諸国における情報収集・分析について」 講師：(一社) JPCERT/CC 早期警戒グループ 脅威アナリスト 米澤詩歩乃氏 ・情報交換「海外動向における情報収集について」
2019/9/20	第9回技術部会	・講演「NEC CSIRTにおけるサイバーセキュリティ対策」 講師：日本電気㈱ 経営システム本部 深澤大輔氏 ・グループディスカッション「各社におけるセキュリティ運用について」
2019/10/18	第10回実務部会	・情報交換「ITガバナンスについて」
2019/11/15	第10回技術部会	・講演「BEC実態調査について」 講師：(一社) JPCERT/CC 早期警戒グループ 情報セキュリティアナリスト 森淳太郎氏 ・グループディスカッション「SIGNALの活用」
2019/12/20	第11回実務部会	・講演「最近のサイバーセキュリティ関連法制の動向」 講師：情報セキュリティ大学院大学 湯淺墾道氏
2020/1/17	第11回技術部会	・実機演習「インシデントハンドリングトレーニング」
2020/2/21	第12回実務部会	・講演「2019年セキュリティトピック」 講師：(一社) JPCERT/CC 早期警戒グループ 脆弱性アナリスト 土居啓介氏 ・2019年度総会
2020/3/13	第12回技術部会	・講演「2019年度の攻撃状況の総括」 講師：日本電気㈱ 経営システム本部 谷川哲司氏
2020/4/17	第13回実務部会	・情報交換「IT部門におけるパンデミック対応とセキュリティ対策」
2020/5/22	第13回技術部会	・演習「ゲーム演習で学ぶCSIRTの動き」
2020/6/19	第14回実務部会	・講演「完ぺきなセキュリティが不可能なら、いったい何を目指せば良いのか」 講師：㈱アスタリスク・リサーチ 岡田良太郎氏
2020/7/17	第14回技術部会	・講演「NECのリモートワークセキュリティ」 講師：日本電気㈱ 経営システム本部 本部長代理 田上岳夫氏
2020/8/21	第15回実務部会	・講演「2020年度上半期の攻撃動向について」 ①ランサムウェアの動向について ②脆弱性について 講師：(一社) JPCERT/CC 早期警戒グループ 脆弱性アナリスト 土居啓介氏
2020/9/18	第15回技術部会	・講演「NECが取り組んできた海外現地法人、グループ会社へのセキュリティガバナンスのきかせ方」 講師：日本電気㈱ 経営システム本部CISOオフィス 宮本智氏
2020/10/23	第16回実務部会	・講演「ビジネスメール詐欺の事例と手口」 講師 独立行政法人情報処理推進機構 セキュリティセンター 竹内智子氏
2020/11/20	第16回技術部会	・ログ分析に関するハンズオントレーニング
2020/12/18	第17回実務部会	・講演「サイバーセキュリティの動向からみるリスクマネジメント」 講師：日本電気㈱ サイバーセキュリティ戦略本部 本部長代理 淵上真一氏
2021/1/18	第17回技術部会	・「NECサイバーセキュリティ演習」
2021/2/19	第18回実務部会	・講演「最近のセキュリティ動向」 講師：(一社) JPCERT 早期警戒グループ 脅威アナリスト 土居毅彦氏 ・2020年度総会
2021/3/19	第18回技術部会	・「NECサイバーセキュリティ演習」

ガイドライン等整備状況	－
活動費の状況	－

(4) J-Auto-ISAC

表 3.2-4 J-Auto-ISAC の概要

設立年月	2017 年 1 月
ホームページ	https://j-auto-isac.or.jp/
目的	IoT の進展に伴い、自動車は車載機器にとどまらず、外部の様々な機器や設備と通信でつながるようになってきている。 今後、自動車および関連するサービスを安全かつ安心に使っていただくためには、サイバーセキュリティリスクへの対応能力を強化することが不可欠である。 OEM やサプライヤーおよび関連サービスを提供する事業者は、サイバーセキュリティ専門家等と強固な協力体制を構築し、タイムリーな施策を常に実現していかなければならない。 わが国の自動車および関連するサービスを安全かつ安心にお使いいただけるよう、サイバーセキュリティリスクの情報共有・分析およびサイバーセキュリティ対応能力の強化を推進する。
活動内容・機能	● 活動内容 1. セキュリティインシデントの発生および被害拡大の抑止

	… 脅威・脆弱性情報の収集および解析や関連情報の共有など 2. サイバーセキュリティ施策の企画・立案および支援 … 管理施策やシステム施策の紹介など 3. サイバーセキュリティ人材の育成施策の企画・立案および支援 … 各種教育プログラムの提供や紹介など 4. 体制整備の支援 …方針やガイドラインの策定、SIRT の構築および強化など 5. 外部連携 …官公庁、他の ISAC、日本シーサート協議会、IPA、JPCERT/CC など ● 提供情報概要 会員企業向けにセキュリティ上の脅威・脆弱性に関する情報を定期的に配信。さらにコンサルによる分析レポートやアナリストによる解説も適宜提供。またダーク Web に関する情報も提供。
組織体制	 図 組織体制図（出典：J-Auto-ISAC ホームページより） ● 総会員数：102 社（2022 年 5 月 20 日現在） 幹事会員（正会員）4社 OEM 会員（正会員）9社 プラチナ会員（正会員）15社 関係会社会員21社 ゴールド会員（正会員）6社 シルバー会員（準会員）19社 ブロンズ会員（準会員）6社 パートナー会員15社 賛助会員5社 学術会員2名

WG 等の活動内容	● 技術委員会 3 つのワーキンググループ(以下、「WG」)と 8 つのサブ WG を編成。業界全体としてリソースを効率的に配分するだけでなく、パートナー企業の専門的な知見をプラスすることで、より高度な課題解決を図っている。またインシデント演習などを通じて有事体制を強化している。 76 社から、のべ 283 名の方が参画し、3つのワーキンググループ(以下、「WG」)と8つのサブ WG が活動 ◆情報共有 WG ◆スキルアップ WG ◆課題抽出・解決推進 WG ◇インシデント事例検証 SWG ◇脆弱性対応 SWG ◇セキュリティ人材育成 SWG ◇個別研修 SWG ◇ベストプラクティス策定 SWG ◇協同演習 SWG ◇データベース＆ポータル機能拡張検討 SWG ◇情報共有プラットフォーム検討 SWG ● セキュリティオペレーションセンター インシデント発生時の被害最小化を第一義に、サイバー攻撃等の脅威情報や日々発見される新たな脆弱性情報の収集や詳細分析を行なっている。関連情報の収集・分析・配信・管理は費用面でも工数面でも負担が大きいため、合同で実施することで高いサービスレベルの確保とコスト削減を同時に図っている。 週次レポートに加えて、四半期毎に分析レポートを発行している。 ● サポートセンター 会員各社の活動をサポートすることを通じて、業界全体としてのレベルアップを図り、当面は啓発活動から現状診断、コンサルティングまで、パートナー企業と連携しながら、会員各社の体制整備をサポートする。 全会員を対象に(パートナー会員、賛助会員、学術会員を除く)、「IT リスク診断(簡易版)」を無償で実施している。自己診断(オンラインでの問診)と会員各社の HP をシステムによる自動診断した結果と併せて統合評価している。
ガイドライン等整備状況	－
活動費の状況	－

(5) 電力 ISAC

表 3.2-5 電力 ISAC の概要

設立年月	2017 年 3 月
ホームページ	https://www.je-isac.jp/
目的	電力 ISAC は、会員間で信頼と互助の精神に基づきサイバーセキュリティに関する情報等を交換や分析することにより、事故の未然防止、発生した事故に対する迅速な対応等を実現し、電気の安定供給及び電気事業に係る情報の安全性や業務の継続性の確保に資する事を目的としている。
活動内容・機能	(1) サイバーセキュリティに関する情報の収集 (2) 収集した内容を踏まえた情報の分析 (3) 収集・分析の結果の会員間での共有 (4) 会員間での情報共有に伴う、ルールの策定及び相互協調活動の促進 (5) 電力セプター事務局 (6) その他、上記の目的を達成するために必要な事業
組織体制	● 組織体制 総会 理事会 事務局 ● 会員構成 (1) 正会員 アからエまでに掲げる法人であって、本会の目的に賛同して入会した者 ア 一般送配電事業者(電気事業法第2条第9号) イ 送電事業者(同条第11号)、特定送配電事業者(同条第13号)、発電事業者(同条第15号)及び小売電気事業者(同条第3号) ウ アからイまでに掲げる者の発行済み株式の全部又は持分の全部を有する者 エ アからウまでに掲げる者が営む事業と関連する事業を営む者であって、本規約前文及び本会の目的(本規約第2条)に照らし、特にその入会が望ましいと理事会が判断した者 ※電力会社他 39 社

	（2）特別会員 正会員となる資格を有しない法人であって、本会の目的達成のために欠くべからざる事業を営み、本会の目的に賛同し、かつ、特にその入会が望ましいと理事会が判断した者 ※送配電網協議会、電力広域的運営推進機関、一般社団法人日本卸電力取引所 （3）テクニカル会員 正会員及び特別会員となる資格を有しない法人であって、サイバーセキュリティに関し専門的な技術・知識を保有し、かつ、本会の目的に賛同し、特にその入会が望ましいと理事会が判断した者
WG 等の活動内容	● イベント活動 電力 ISAC オープンセミナー（2021 年 3 月 1 日） 電力 ISAC サイバー演習（2021 年 1 月 28 日） 第3回 電力 ISAC 総会カンファレンス（2020 年 11 月 26 日） 電力 ISAC サイバー演習（2019 年 12 月 02 日） ● WG 活動 ➢ 火力システム WG 火力の発電所監視制御システム等のサイバーセキュリティに関するグッドプラクティス等を共有し、課題解決に向けた意見交換を行う。 ➢ 水力システム WG 水力の発電所監視制御システム等のサイバーセキュリティに関するグッドプラクティス等を共有し、課題解決に向けた意見交換を行う。 ➢ 需給・系統システム WG 需給制御システム及び系統制御システムのサイバーセキュリティに関するグッドプラクティス等を共有し、課題解決に向けた意見交換を行う。 ➢ 共通・IT システム WG 最新のサイバーセキュリティに関するトレンドや電力分野に係る IT/OT 全般に関するグッドプラクティス等を共有し、課題解決に向けた意見交換を行う。 ➢ リスクアセスメント WG 様々なリスクアセスメント手法の概要・特徴を理解し、各社で効果的に実施していくために、課題の共有とともに解決に向けた意見交換を行う。 ➢ SM システム脆弱性情報共有 WG スマートメーターシステムに関して、重大な脆弱性・セキュリティ事故・事象が発生した際に、必要に応じて関係者間で情報交換を行う。
ガイドライン等整備状況	－
活動費の状況	－

（6）ソフトウェア ISAC

表 3.2-6 ソフトウェア ISAC の概要

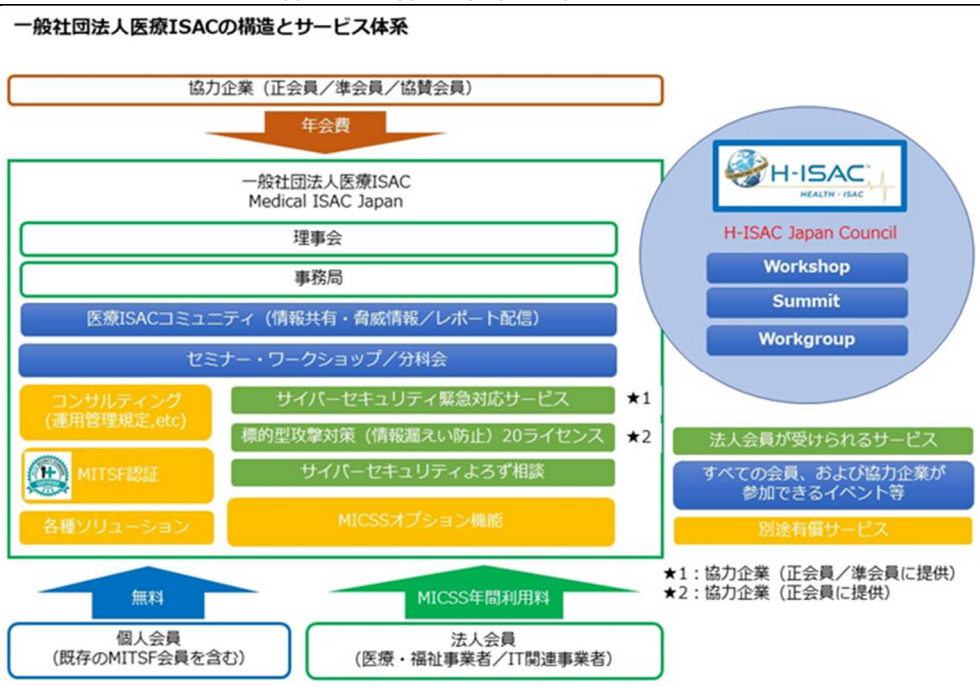
設立年月	2018 年 8 月
ホームページ	https://softwareisac.jp/
目的	サイバーセキュリ ティに関連する情報整備や連携を通じ、わが国のソフトウェア産業が安全かつ迅速に発展することを目的とする。
活動内容・機能	1. 脆弱性・脅威情報等の集約・分析・展開等の調査研究 2. サイバーセキュリティ向上のための人材育成 3. 開発上流工程にセキュリティを組み込むための調査研究 4. サイバーセキュリティに関係する外部機関との情報交流と連携 5. サイバーセキュリティに関係する政策提言 6. その他、当 ISAC の目的を達成するために必要な事業
組織体制	● 組織体制 幹事会 運営チーム 事務局 ワーキンググループ ● 会員種別 ➢ 正会員は、一般社団法人ソフトウェア協会（以下、「SAJ」という。）の正会員として加入している 法人とする（SAJ 正会員及び正会員として SAJ に入会したものは当 ISAC に

	正会員として入会したものとみなす。)。 ➢ 協力会員は、前項に該当しないもので、当 ISAC の目的に賛同し、当 ISAC に貢献・協力しようとす る法人、組合、社団等の団体とする。 ➢ 個人会員は、当 ISAC に貢献・協力する意志を有する個人とする。 ※SAJ 正会員は 539 社
WG 等の活動内容	● OSS 委員会 OSS の汚染や侵害の調査・研究、SBOM の研究を通じて、安全な OSS の普及を推進している。 ● ガイドライン委員会 Software ISAC は、IPA 社会基盤センターの社会実装推進委員会の中で、民法改正対応モデル契約見直し WG(ワーキング・グループ)の下に設置された「セキュリティ検討 PT(プロジェクトチーム)」に対し積極的な支援活動を実施しており、これまでになかった新しいセキュリティガイドライン「情報システム開発契約のセキュリティ仕様作成のためのガイドライン」の策定に取り組んでいる。 ● セキュリティ経営委員会 有識者によるセミナーを開催し、サイバーセキュリティの現状を正しく理解し、正しく人・モノ・金を配分できる経営者の育成を目指している。また、セキュリティを協調領域としてとらえ、経営者同士の情報交換や交流を深めている。 ● AI 安全利活用研究会 最先端のテクノロジーとして注目されている AI だが、未だ厳密な定義はない。そして、AI 利活用は情報セキュリティの検討が不十分な状況である。こうした中また、業界・企業規模に関わらず、AI 利活用において情報セキュリティを検証できるツールが必要である。総務省が作成した「AI 利活用ガイドライン」を参考にしつつ、AI の利用形態を整理し、アクターや責任分界点を研究している。 ● セキュアコーディング研究会 セキュア開発を実現するための情報共有、セキュアコーディングガイドラインの策定を通じて、シフトレフトを推進している。具体的には、Spring Framework のセキュアコーディングガイドの作成、セキュアなアプリケーションの定義、ビルド、テスト、 検証に使用できるアプリケーションセキュリティ要件またはテストのリストである、OWASP Application Security Verification Standard (ASVS) 4.0 の日本語化や、 セキュア開発セミナーを開催している。 ● PSIRT 推進研究会 Product Security Incident Response Team の普及を推進している。
ガイドライン等整備状況	● 情報システム開発契約のセキュリティ仕様作成のためのガイドライン(IPA 内のセキュリティ検討プロジェクトチームとして取りまとめ) ➢ 詳細設定対策に必要な措置(上記ガイドラインの一部として、サイバー攻撃防御としての詳細な緩和策を解説) ➢ MITRE ATT&CK に基づく詳細設定対策(上記ガイドラインの一部として、サイバー攻撃防御としての詳細な緩和策を解説) ● ソフトウェア出荷判定セキュリティ基準チェックリスト Ver.1.2 ● OWASP AVSV4.0 日本語版 ● 「シン・テレワークシステム」向けセキュリティポリシー ● PSIRT 成熟度評価シート ● 「PSIRT Services Framework 1.0 Draft」日本語翻訳
活動費の状況	正会員 年間売上高に応じて6～45万円 個人会員 1万円 賛助会員 種別に応じ一口5万円以上～一口35万円二口以上 準会員 無料

(7) 医療 ISAC

表 3.2-7 医療 ISAC の概要

設立年月	2019 年 10 月
ホームページ	https://m-isac.jp/
目的	医療分野における情報セキュリティの重要性を啓発するために 2013 年に活動を開始したメディカル IT セキュリティフォーラム(MITSF)を前身とし、2019 年 10 月に医療 ISAC に改称したものである。 現在(2020 年 4 月時点)まで通算 14 回のセミナーと、9 分野の分科会を開催し、関係各機関への提言や、ガイダンスの公表等を実施、実際の医療分野で情報セキュリティに関連する問題を解決する

	ための、具体的なサービスの提供を行っている。
活動内容・機能	● 厚生労働省、総務省、経済産業省のガイドラインを統合して、医療機関および医療機関を顧客とする事業者に対する実質的な“TO BE MODEL”を示す。 ● 医療介護福祉関連の関係各団体との情報交換、情報共有を行い、会員に周知を行う。 ● IT セキュリティ製品を扱う各種事業者からの最新情報を紹介し、その機能と適合する事例、期待される効果を、国際的なセキュリティ評価基準と照合して分類・表示し、医療機関や医療従事者がセキュリティ製品を採用する際の判断材料を提供する。 ● 具体的な課題とその対策について問題を解決可能なソリューションの紹介をする。 ➢ 医療情報システムにおけるセキュリティ上の喫緊の課題と思われる、地域医療連携システムおよび職員の私物 PC 端末による外部よりの電子カルテシステムアクセスについて ➢ 内部ネットワーク対策について ➢ 内部ネットワークにおけるウイルス・マルウエア対策について ➢ 医療機器やシステムの遠隔保守におけるセキュリティ対策について ➢ ASP, SaaS, BPO を利用したサービスを利用する際の、セキュリティ対策について ➢ ガイドラインに適合した運用管理規程集の提供
組織体制	 図 医療 ISAC の全体構造（出典：医療 ISAC ホームページより）

医療ISACの会員種別

医療ISACでは、法人/一般別に会員種別を以下の通り、定義しています。

会員種別		活動内容
法人会員		医療ISACが提供するサービス（無償・有償）を受けることができる医療・福祉事業者 （2022年4月改定）
個人会員	医療等従事者	医療・福祉の従事者で、個人的に医療ISACコミュニティに参加する会員
	サポーター	医療情報を取り扱う情報システム・サービス事業者等に所属し、個人的に医療ISACコミュニティに参加する会員
協力企業	正会員	セミナー・ワークショップ／分科会を開催（企画等）する権利を有し、医療ISACの運営に積極的に参画していただく企業様
	準会員	セミナー・ワークショップ／分科会を開催する権利は有さないが、医療ISACの運営に積極的に参画していただく企業様
	協賛会員	資金面での支援をお考えの企業様

会員の有する権利（セミナー・ワークショップ）

会員種別		セミナー・ワークショップへの関わり				企業広告	
		企画	主催 （共催）	セッション 提案	参加	資料配布	プログラム 広告
法人会員		×	×	○	○	×	×
個人会員	医療等従事者	×	×	○	○	×	×
	サポーター	×	×	○	○	×	×
協力企業	正会員	○	○	○	○	持参	有料
	準会員	×	×	○	○	持参	有料
	協賛会員	×	×	×	○	持参	有料

会員の有する権利（分科会）

会員種別		分科会への関わり		
		企画	主幹	参加
法人会員		○	○	○
個人会員	医療等従事者	○	○	○
	サポーター	×	×	○
協力企業	正会員	○	○	○
	準会員	×	×	○
	協賛会員	×	×	○

会員の有する権利（その他）

会員種別		その他の有する権利	
		医療ISACへの アドバイザー派遣	医療ISACの ホームページへの バナー広告
法人会員		×	×
個人会員	医療等従事者	×	×
	サポーター	×	×
協力企業	正会員	○	○
	準会員	×	○
	協賛会員	×	×

医療ISACの会費、および年間利用料

会員種別		入会金 （消費税込み）	年会費 （消費税込み）
法人会員		無料	
個人会員	医療等従事者	無料	
	サポーター		
協力企業	正会員	330,000円	1,320,000円／年
	準会員	330,000円	330,000円／年
	協賛会員	無料	110,000円／年

図　会員種別（出典：医療 ISAC ホームページより）

WG 等の活動内容

- ワークショップ等の開催

表 セミナーやワークショップの開催状況(出典:医療 ISAC ホームページより)

開催日	イベントタイトル	開催場所	主なプログラム
2022年3月23日	医療ISAC Security Lecture 2022 #003	配信	2022年4月施行の改正個人情報保護法が医療機関に及ぼす影響とは（江原）
2022年2月22日	医療ISAC Security Lecture 2022 #002	配信	徳洲会グループ：セキュリティの取り組み～システム監査を中心に（TIS）
2022年1月25日	医療ISAC Security Lecture 2022 #001	配信	サイバー攻撃への備え！AI免疫システム（Darktrace）
2021年12月16日	医療ISAC Security Lecture 2021 #009（IDF共催）	配信	「医療機関向けランサムウェア対応検討ガイダンス」の解説（IDF／深津／江原）
2021年11月24日	医療ISAC Security Lecture 2021 #008	配信	セキュリティアンケート結果から見る国内病院の構造的な課題（江原）
2021年10月27日	医療ISAC Security Lecture 2021 #007	配信	脅威を未然に予期・検知・予防する、「脅威インテリジェンス」サービスの概要とコア技術、そして医療業界への導入について（伊藤）
2021年9月21日	医療ISAC Security Lecture 2021 #006	配信	ランサムウェア攻撃に備えて病院関係者がするべき準備と取るべき行動（深津／山崎／舟橋／江原）
2021年7月21日	医療ISAC Security Lecture 2021 #005	配信	エンドポイントセキュリティの新潮流 Prevention Firstとは（Blue Planet-works）
2021年6月25日	医療ISAC Security Lecture 2021 #004	配信	医療分野の情報セキュリティ規格ISO27799の改訂作業について（深津）
2021年5月26日	医療ISAC Security Lecture 2021 #003	配信	クラウド・バイ・デフォルトとISMAP制度について（山崎）
2021年4月16日	医療ISAC Security Lecture 2021 #002	配信	3省2ガイドラインの都市伝説と真実（江原）
2021年3月24日	医療ISAC Security Lecture 2021 #001	配信	厚生労働省「医療情報システムの安全管理に関するガイドライン第5.1版」エンハンスで新たな問題提起となったツボ（伊藤）
2020年10月31日	医療ISACウェビナー・2020秋	配信	医療DX、特に患者情報の二次利用に伴うセキュリティ・コンプライアンスガバナンスのベースラインについて（江原）
			医療グループにおけるDXの取り組み事例紹介（徳洲会）
			オンライン診療におけるセキュリティ対策（MICIN）
			テレワークにおけるセキュリティ最新事情（山崎）
2020年5月16日	医療ISACウェビナー・2020春	配信	医療ISAC・2020年度の取り組みについて（深津）
			医療情報の安全管理に関する事業者向けガイドラインの統合に関する政策動向（経産省）
			医療情報を取り扱う情報システム・サービス提供事業者における安全管理ガイドラインの要点（江原）

- 会員向け提供サービス

表　医療 ISAC サイバーセキュリティサービス（出典：医療 ISAC ホームページより）

MICSS

医療ISACサイバーセキュリティサービス：MICSS

Medical **I**SAC japan **C**yber **S**ecurity **S**ervice

基本サービス	医療ISACコミュニティ （情報と経験の共有）	国内外の最新の脅威情報とそれに対する防護策を適時に注意喚起するとともに、セキュリティインシデント情報、および対応結果などの貴重な経験をみなさんで共有できる信頼のおけるコミュニティに参加できます。 また、最新のサイバーセキュリティ動向や、国内の医療機関で起こったセキュリ ティインシデント情報やトピックをEメールで受信できます。 （daily／weekly／monthly）
	サイバーセキュリティ 緊急対応サービス	サイバー攻撃を受けている、あるいはその他のセキュリティインシデントが発生した可能性がある場合、まずは電話によるセキュリティインシデントの相談、必要があればお客様のもとに駆け付けて、応急処置を施し事故の状況を分析した詳細な報告を受けられます。これにより、セキュリティインシデントによる被害状況などが明らかになります。 本サービスは内部犯行などにも対応します。
	標的型攻撃対策 （情報漏えい防止）	万一、悪意のあるEメールや汚染されたUSBメモリなどによりコンピュータウイルスに感染した場合、危険な接続先へのアクセスをブロックし情報漏えいを防ぐ、クラウドソリューションをPC20台分利用できます。セキュリティ担当者無しでも運用可能で、故意、過失に係わらず不正サイトへの接続を遮断します。
	サイバーセキュリティ よろず相談	医療ISACによる、サイバーセキュリティに係るよろずコンサルティング面談（年2回：1セッション1時間程度）を直接受けることができます。 高額な費用をかけず3省ガイドラインに対応するには？運用管理規程はどうすれば？などの様々なお悩みにお答えします。
	各種イベントへの参加	医療ISAC主催セミナー・ワークショップやH-ISACとの共同Workshop、およびSummitなどにご参加いただけます。 また、遠方で参加の難しいお客様には、ストリーミング配信を検討しています。

医療ISAC認証サービス

医療ISACは、当団体関与の下で、以下の各ガイドラインに基づく運用管理規程の整備、システム運用管理態勢の維持、または監査を通した運用管理状況の改善に関する取組を図る医療機関、及び医療情報システムを開発・運用する情報処理事業者に対して、＜医療ISAC認証＞を付与する取組を行います。

・厚生労働省「医療情報システムの安全管理に関するガイドライン」
・経済産業省／総務省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」

医療ISAC認証の主旨

医療情報システムを利用する医療機関、または開発・運用する情報処理事業者は、官庁が策定する上記の３省２ガイドラインへの準拠、つまり各ガイドラインの要求事項を反映した運用管理規程を策定し、当該規程に基づき医療情報システムの利用、開発/運用を行うことがコンプライアンスとして求められています。 従来まで、このコンプライアンスは、院内や事業者内部で実務的に対応すること（＝管理責任）に重点が置かれていました。しかしながら、当今のサイバー脅威の増大や地域医療連携に伴うサプライチェーンリスクの高まりなどを背景に、今や、単に「実務的に対応している」ことのみでなく、何らかのインシデントが発生した場合、外部のステークホルダーに向けて確実にその対応状況を説明できる水準で維持すること（＝説明責任）の必要性が高まっています。

当団体ではこのような状況を鑑み、医療機関や情報処理事業者によるコンプライアンスに向けた取組状況の信頼性を独立した第三者機関として審査した上で、外部のステークホルダーに向けた説明責任を果たすための一助として、「医療ISAC認証」を提供します。

医療ISAC認証のカテゴリー

医療ISAC認証は、＜医療ISAC規程認証＞、＜医療ISAC監査認証＞、＜医療ISAC態勢認証＞の三つのカテゴリーから構成されます。

認証名称	認証内容	対象組織	認証条件
医療ISAC規定認証	ガイドライン対応に向けた整備/見直し、レビュー等、何らかの支援が行われた運用管理規定を有する組織体に対して、「ガイドラインに基づく運用管理規定の整備が行われているという事実」について認証を行う	・医療機関等 ・医療情報システムを開発/運用する情報処理事業者	組織としての運用管理規定の整備を完了すること
医療ISAC監査認証	ガイドライン対応状況について何らかの(外部監査、または内部監査支援)が行われた組織体に対して、「運用管理プロセスの改善に向けて、ガイドラインに基づく対応状況に関する監査が実施されてるという事実」について認証を行う	・医療機関等 ・医療情報システムを開発/運用する情報処理事業者	監査を実施すること
医療ISAC態勢認証	医療ISAC規格認証を取得した組織が策定した「運用管理規定」に基づくシステム運用管理を実施し、かつ、医療ISACが企画・開催するセキュリティセミナー（Webセミナーを含む）を一定回数受講した組織体に対して、「ガイドラインに基づくシステム運用管理態勢を有する事実」について認証を行う	・医療ISAC規程認証を取得した組織体から提供される「運用管理規程」に基づき、自組織のシステムの運用管理を実施する組織体	以下2つの条件を充足すること ・医療ISAC規格認証を取得した組織体による「運用管理規程」に基づくシステム運用管理の実施 ・医療ISACが企画・開催するセキュリティセミナーの一定回数の受講

図　医療 ISAC 認証サービス(出典:医療 ISAC ホームページより)

ガイドライン等整備状況

表　公表資料や提言(出典:医療 ISAC ホームページより)

発表(公表)日	提言
2022/3/31	四病院団体協議会の加盟病院を対象としたセキュリティアンケートの調査結果
2022/1/20	Report：クラウド時代の医療情報セキュリティの考え方 ～国内病院の課題解決を志向するリスクコミュニケーションの重要性～
2021/12/20	Report：国内病院に対するセキュリティアンケート調査の結果と考察
2021/12/2	ランサムウェア対策に関する注意喚起
2021/12/1	国内病院に対するセキュリティアンケート調査の結果と考察
2022/11/25	医療機関向けランサムウェア対応検討ガイダンス（IDFサイト）
2021/7/8	遠隔業務委託システムにおけるサイバーセキュリティの再点検（注意喚起）
2021/1/31	医療・介護関係施設におけるコミュニケーションツールを介した患者個人情報の公開事故について（提言）

<table>
<tr><td></td><td>表 分科会報告(出典:医療 ISAC ホームページより)
<table><tr><th>発表(公表)日</th><th>報告書</th></tr><tr><td>2017.1.20</td><td>データダイオード分科会報告書</td></tr><tr><td>2017.1.20</td><td>匿名化分科会報告書(分科会報告・提言書案)</td></tr><tr><td>2017.1.20</td><td>地域医療連携・地域包括ケア分科会報告書(分科会報告・提言書案)</td></tr></table></td></tr>
<tr><td>活動費の状況</td><td>法人会員 無料
個人会員 無料
協力企業
正会員 132 万円／年
準会員 33 万円／年
協賛会員 11 万円／年
協力企業(13 社)
Cohesity Japan 株式会社、PwC あらた有限責任監査法人、Tenable Network Security Japan 株式会社、健康サロン株式会社、ゼットスケーラー株式会社、ダークトレース・ジャパン株式会社、デル・テクノロジーズ株式会社、徳洲会インフォメーションシステム株式会社、株式会社トマーレ、日本ダイレックス株式会社、日本電子株式会社、三井物産セキュアディレクション株式会社、株式会社ワイ・イー・シー
想定される活動費 1,716 万円／年</td></tr>
</table>

(8) 交通 ISAC

表 3.2-8 交通 ISAC の概要

<table>
<tr><td>設立年月</td><td>2020 年 4 月</td></tr>
<tr><td>ホームページ</td><td>https://t-isac.or.jp/</td></tr>
<tr><td>目的</td><td>交通・運輸業界において、サイバーセキュリティに関する会員相互間の広範な連携・協力を行うことにより、サイバー攻撃等に対する分野横断的な集団防御力の向上に資する活動を推進し、もって我が国における交通・運輸サービス全体の安全・安心の向上に寄与することを目的としている。</td></tr>
<tr><td>活動内容・機能</td><td>● サイバーセキュリティに関する情報の収集及び共有
● サイバーセキュリティに関する課題に対する共通認識の醸成及び共同対処
● 前各号に掲げるもののほか、当法人の目的を達成するために必要な事業</td></tr>
<tr><td>組織体制</td><td>● 組織構成
社員総会
｜
理事会 － 事務局(外部委託可)
｜
運営委員会

● 会員構成
会員数 89 会員
うち正会員 68 会員
賛助会員 11 会員
オブザーバー会員 10 会員</td></tr>
<tr><td>WG 等の活動内容</td><td>－</td></tr>
<tr><td>ガイドライン等整備状況</td><td>－</td></tr>
<tr><td>活動費の状況</td><td>表 活動費の状況
<table><tr><th>会員の種別</th><th>対象者</th><th>年会費</th></tr><tr><td>正会員</td><td>当法人の目的に賛同する、航空、空港、鉄道、物流、その他の交通・運輸分野に属する団体</td><td>50 万円</td></tr><tr><td>賛助会員</td><td>当法人の目的に賛同し、当法人の事業を賛助するため、正会員 1 団体以上の推薦を受けた団体又は個人(正会員向けにサイバーセキュリティに関する情報や知見等を積極的かつ自発的に提供していただける方が対象)</td><td>50 万円</td></tr></table></td></tr>
</table>

	オブザーバー会員	当法人の事業に協力するため、当法人の要請を受けた団体又は個人	なし

（9）各 ISAC の主な提供機能の整理

ビルのサイバーセキュリティ推進体制の参考とするため、前述の調査結果をもとに、各 ISAC の主な提供機能を横並びで整理した。この結果、いずれの ISAC も情報の収集・分析機能や情報共有機能を持っており、これらがまず基本的な機能であることが推測される。より高度な機能を提供するにはリソースや運営費が掛かるため、会員の積極的な同意、参画が必要となるということもあり、まずはサイバーセキュリティに関する情報分析や情報共有から始めることが肝要と思われる。

表 3.2-9 国内の代表的な ISAC における設立目的や主な提供機能

ISAC 名	目的	運営母体	主な機能					
			情報の収集・分析	情報の共有	人材育成の支援	セキュリティの啓発	ガイドライン等の策定	外部組織との連携
金融 ISAC	サイバーセキュリティに関する情報の共有・分析及び安全性の向上のための協働活動を行うこと	一般社団法人 金融 ISAC	✔	✔		✔		
医療 ISAC	情報セキュリティの重要性を啓発すること 情報セキュリティに関連する問題を解決すること	一般社団法人 医療 ISAC	✔	✔			✔	✔
ICT-ISAC	幅広い相互連携を図り、安定した情報流通、情報伝達を維持すること サイバー攻撃に対処する社員である電気通信事業者を支援すること	一般社団法人 ICT-ISAC	✔	✔	✔	✔	✔	✔
電力 ISAC	会員間で信頼と互助の精神に基づきサイバーセキュリティに関する情報等を交換や分析すること	電気事業連合会	✔	✔				✔
交通 ISAC	サイバーセキュリティに関する会員相互間の広範な連携・協力を行うこと	一般社団法人交通 ISAC	✔	✔		✔		
J-Auto-ISAC	サイバーセキュリティリスクの情報共有・分析およびサイバーセキュリティ対応能力の強化を推進すること	一般社団法人 Japan Automotive ISAC※	✔	✔	✔		✔	✔
ソフトウェア ISAC	サイバーセキュリティに関連する情報整備や連携を行うこと	一般社団法人 ソフトウェア協会	✔	✔	✔	✔	✔	✔
日本貿易会 ISAC	インシデント情報の入手ならびに共有、相互の対応協議を行うこと 日本貿易会の会員商社におけるサイバー	一般社団法人 日本貿易会	✔	✔	✔			

	セキュリティ対策をサポートすること							

3.2.2 ビルオーナーへのヒアリング調査

ビルのサイバーセキュリティ推進体制の検討にあたり、その中心的プレイヤーになると想定されるビルオーナー会社を対象にヒアリングを実施した。各社のサイバーセキュリティに対する姿勢や取組について聞くとともに、望まれる推進体制やその構築手順についての意見を聞き取った。

その結果は以下の通りで、意見は各社各様だが、何らかの推進体制を考える上では、公的な組織が母体となる案への意見が最も多い結果となった。

表 3.2-10 推進体制についての各社ヒアリング結果

	A社	B社	C社	D社
1．取組状況				
自社の取組	新築ビルの仕様に利用。	既存ビルのアセスメントに利用。	既存ビルのアセスメントと改善に利用。	新築ビルの仕様に利用。
（取組の詳細）	40～50 階建てクラスの建物で業者に発注する仕様に組み込んで利用している。	ビルシステムの管理規定を整備しており、その中で METI ガイドラインと NIST CSF から 400 項目のチェックリストを作成し、管理物件のリスクアセスメントに使っている。	元々自社独自ガイドラインを持っていたが、METI ガイドラインでブラッシュアップし、管理下の全物件のチェックを定期的（年 1 回）に行っている。大型物件では、FW、DMZ、検知装置の導入などの改善も行っている。	新築物件において、一部設計変更もして貰う形で、ガイドラインへの適合を追求している。新築については今後はガイドラインを意識して行くことになる。 SOC も事業者委託の形で設置する予定で、うまく行けば今後も広げたい。
取組における課題	多くの事業者が関係するが、セキュリティに関する仕様を理解出来るのがごくわずかで、思い通りに行かない。	チェックリストは、ビルオーナー編、建物管理会社編、メーカー・保守会社編の 3 種類を作っている。 建物管理会社には更にブレークダウンして伝えているが、理解してもらうのが難しい状況。	当初はまごつく事もあったが、3 回目の検査になり、今では問題なく回せている。	ビルの全体像を把握している者がいない。設計事務所でも管理しきれておらず、設備単位の勝手なネット接続等を制御しきれない。 また既存ビルでは、リニューアルのタイミングであっても現状は適用が難しい。
2．推進体制				
望まれる／ありえる推進体制	ビル関連団体に情報交換が出来る部会を作り、新たなコスト負担なく情報交換レベルからスタートできる形で進めると良い。既存の部会を利用するのでも良い。	ビルシステムの情報共有／推進体制という枠組は不要。 個別設備がそれぞれ対応してくれれば良く、ビルシステムという単位で枠をはめていくことは良くないと思う。	公的な組織が持てると良いと思う。ただし、現状では共同化することで効率化やコスト削減できる部分は少ないと思う。 ビル SWG で行ってきた各社の取組の共有やビルに係る脆弱性情報の配信は有用であり、継続して欲しいと思う。	産学連携組織でやるのが良い。オープンオペレーションを追求している組織であり、最終的に大学マークの認証／お墨付きが出るようなら、テナントにも強いアピールになり、インセンティブになる。

その他推進方法	サイバーセキュリティに取組むことで容積率のようなボーナスがもらえるなら各社とも真剣に取組むだろう。あるいは外資系のようなところが厳しく要求してくれれば変わるかもしれない。	電力保安や監視カメラなどの個別システムから上がってきた情報をビルに展開すれば良い。 これらは法的根拠があり優先順位が高いので、ビルガイドラインの優先順位は必然的に下がる。一方、これらはビルオーナーに多くの裁量を認めているが、ガイドラインは裁量がないように見えるので、逆転しているように思える。		制御セキュリティ関連団体で認証をしてもらうのも一案だが、ビジネスモデルとしては継続しないだろう。大手ビルオーナーは本気で取組んでいる感じではないので、幹事役が強力に引っ張っていく必要があるので難しい。 IoT の世界で Matter が普及すれば、ビルも対応せざるを得なくなるが、ビルシステムには繋げないという対策になってしまうかもしれない。

3.2.3 ビルシステムのサイバーセキュリティ推進体制の在り方整理

国内の各種 ISAC の調査及びビルオーナーへのヒアリング調査の結果、いわゆる ISAC の機能のうちミニマムな部分について、ビルに関する公的な組織を活用して始めることが望ましく、その活動が広がるのに合わせて、プレイヤーを増やし、体制の機能も拡充していくことが良いのではとの整理に至った。以下では基本的な考え方や望まれる機能、実際の構築手順について整理して示す。

（1） 基本的な考え方

ビルシステムのサイバーセキュリティ推進体制についての基本的な考え方としては、以下のように取りまとめた。

- ミニマムな機能、取組から始めるのが良い。
  - 最低限の情報共有、関係者間の信頼関係醸成等のコストを掛けずに出来ることから開始
  - サイバーセキュリティの基本的知識の教育など各社個別にやるよりも共同化した方が効率化できることを実施
  - ビルシステムのセキュリティに関する具体的な課題点、解決策についての議論の場を提供
- ビルオーナーを中心に始めて、必要に応じて他のプレイヤーにも参加してもらう。
- 既存のビル関係組織において興味のある関係者を集める部会や WG 等を活用する。

（2） 望まれる機能

各種 ISAC の調査結果から、ビルシステムに関するサイバーセキュリティ推進組織として考えられる機能は以下の通りである。このうち、初歩的なものとして分類した部分から始めることが望ましいと考えられる。

- 情報の共有 （★初歩的な取組として期待される機能）
  - 各社間での攻撃事例等の知見の共有（同業態への攻撃は順番的に行われることが多いので、いち早い情報共有で 2 次、3 次被害を防止する）
  - 各社取組み状況、対策／ソリューションの方法、対策事例等の知見の共有（多くの会社が同

じ悩みを持つので、対策に向けた悩みごとの共有、解決策の関連情報の共有をする）
    - 会員向け相談サービス／ベンダ等紹介
- 人材育成 （★初歩的な取組として期待される機能）
    - 教育プログラム／コンテンツの提供（ベーシックな教育コンテンツの共用化）
    - サイバー演習の提供
- セキュリティの啓発
    - 業界に係るサイバー全般の情報提供（規制やガイドライン動向、内容紹介等）
- 情報の収集・分析
    - ビルシステムに係るインシデント情報、脆弱性情報の収集、分析、ビルシステムに特化した整理、共有
- ガイドライン等の策定
    - ガイドラインの整備、普及啓発、何らかの認定、お墨付きの提供
- 外部組織との連携
    - ビルに係る業界団体、関係省庁、他のサイバーセキュリティ関連組織との情報交換、働きかけ、連携作業

（3） 実際の推進体制構築手順

これらを総合し、次のような手順で、ミニマムな機能の提供から始めることが望ましい。

- ビル関連団体において、部会等として議論を実施する（既存部会の活用でも新規部会でも良い）
- サイバーセキュリティ対応についての悩みや実際の取組等の情報交換レベルから開始し、更に高度な取組については将来的に検討する
- 基本的な教育を共同提供する（現場向け教育コンテンツ、ベンダ向けセミナー等）
- 既に実施されている IoT 対応など新たな技術への対応の議論に加える形で実施する方法もある
- さらに必要に応じてゼネコン、ベンダ等と連携し、情報入手出来る場にもなると良い

3.3 検討会の運営

今年度に実施したビル SWG および作業グループについて、それぞれの概要を示す。

3.3.1 ビルSWGの運営

今年度のビル SWG は合計 2 回開催した。

初回では、空調編の作業について説明をするとともに意見募集を行い、インシデントレスポンスの議論についての頭出しを行った。

その後、作業グループを活用してインシデントレスポンス・ガイドラインの素案作成を行い、その結果を第 2 回ビル SWG で説明した。空調編に関しては公開に向けた作業に進むことへの了承を得た。またインシデントレスポンスについては今後議論を本格化させる必要があるので、そのための意見やアドバイスを頂戴した。

以下に各 SWG の開催概要について記載した。

（1） 第 14 回ビル SWG の運営

1） 開催概要

日時　2022 年 10 月 7 日～14 日

場所　書面開催

議題

1. 開会

2. ビルガイドライン（個別編：空調システム）の公開に向けて

3. 閉会

配布資料：

資料1	議事次第・配付資料一覧
資料2	構成員等名簿
資料3-1	ビルガイドライン（個別編：空調システム）の公開に向けて
資料3-2	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（個別編：空調システム）（パブコメ対応版）
資料3-3	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（個別編別紙：空調システム）（パブコメ対応版）
参考資料1	ビルガイドライン・コメント対応表

2） 構成員

安斎　幹	株式会社日建設計 アソシエイト
岩城　保直	一般社団法人ビルディング・オートメーション協会 理事
植竹　務	アズビル株式会社 主任
江崎　浩	東京大学大学院情報理工学系研究科 教授
大西　克保	鹿島建設株式会社 課長
大矢　誠	日本生命保険相互会社 専門課長
奥住　俊明	株式会社きんでん 技監
加井　隆重	ダイキン工業株式会社 産官学連携専任部長
忽那　裕之	一般社団法人日本ビルヂング協会連合会 事務局次長
蔵方　律	三菱地所株式会社 ユニットリーダー
後神　洋介	株式会社竹中工務店 専門役
佐藤　芳紀	ICSCoE2期ビルチーム有志（森ビル株式会社） 課長
柴田　純	一般社団法人不動産協会 事務局長代理
中野　利彦	株式会社日立製作所 セキュリティエバンジェリスト
林　和博	株式会社九電工 副本部長
福田　次郎	横浜市 CIO 補佐監
二名　信彰	株式会社 NTT ファシリティーズ 部門長
松浦知史	東京工業大学学術国際情報センター 准教授

後藤　要二　　三井不動産株式会社　グループ長(←　202210 より変更)
横田　和典　　三菱電機株式会社 専任
渡部　宗一　　イーヒルズ株式会社 取締役
(オブザーバー)
国土交通省(総合政策局情報政策課サイバーセキュリティ対策室)
内閣サイバーセキュリティセンター 東京 2020 グループ
中部国際空港施設サービス株式会社
中部国際空港株式会社

3）議事要旨

産業サイバーセキュリティ研究会 WG1 ビル SWG（第 14 回）
議事概要

日時　：　（書面開催）令和 4 年 10 月 7 日（金）～10 月 14 日（金）
構成員　：
（座長）江崎 浩 東京大学 教授
松浦 知史 東京工業大学 准教授
アズビル株式会社
イーヒルズ株式会社
鹿島建設株式会社
株式会社九電工
株式会社きんでん
技術研究組合制御システムセキュリティセンター
セコム株式会社
ダイキン工業株式会社
株式会社竹中工務店
株式会社日建設計
日本生命保険相互会社
株式会社 NTT ファシリティーズ
一般社団法人日本ビルヂング協会連合会
株式会社日立ビルシステム
一般社団法人ビルディング・オートメーション協会
一般社団法人不動産協会
三井不動産株式会社
三菱地所株式会社
三菱電機株式会社
横浜市
ICSCoE 第 2 期ビルチーム有志

（オブザーバー）
国土交通省（総合政策局情報政策課サイバーセキュリティ対策室）
内閣サイバーセキュリティセンター 東京 2020 グループ
中部国際空港株式会社（欠席）／中部国際空港施設サービス株式会社

議題 ：
1．ビルガイドライン（個別編：空調システム）の公開に向けて

要旨 ：
書面開催のため、議事要旨なし

（以上）

4）ロジ業務の実施

会議運営のためのロジ業務（日程調整、資料準備、会議運営、議事録作成、有識者委員に対する謝金支払い等）を実施した。

（2）第 15 回ビル SWG の運営

1）開催概要

日時 2023 年 1 月 31 日 15:00～17:00
場所 Web 会議（Teams）
議題

1. 開会（3分）
2. 各構成員より挨拶・1年間の振り返り（25分）
3. インシデントレスポンスの検討状況について（20分）
4. 委託事業調査の中間報告（5分）
5. 森ビルにおけるビルセキュリティの取組について（5分）
6. 自由討議（60分）
7. 閉会（2分）

配布資料：

資料1	議事次第・配付資料一覧
資料2	構成員等名簿
資料3	インシデントレスポンス・ガイドライン（案）について
資料4	委託事業調査の中間報告
資料5	森ビルにおけるビルセキュリティの取組 ～ここ数年の update～（投影のみ）
参考資料1	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／インシデントレスポンス・ガイドライン（案）
参考資料2	ビルにおける障害発生時の対応フローとサイバー事案への対応

参考資料3　ビルガイドラインと自家用電気工作物ガイドラインの比較表

2）構成員

秋山 琢磨	三菱地所株式会社 専任部長
安斎 幹	株式会社日建設計 アソシエイト
池田 宜之	日本生命保険相互会社（大星ビル管理株式会社）
岩城 保直	一般社団法人ビルディング・オートメーション協会 理事
植竹 務	アズビル株式会社 主任
江崎 浩	東京大学大学院 教授
大西 克保	鹿島建設株式会社 課長
加井 隆重	ダイキン工業株式会社 産官学連携専任部長
忽那 裕之	一般社団法人日本ビルヂング協会連合会 事務局次長
後神 洋介	株式会社竹中工務店 専門役
佐藤 芳紀	ICSCoE2期ビルチーム有志（森ビル株式会社） 課長
高山 雅士	一般社団法人不動産協会 事務局長代理
中野 利彦	株式会社日立製作所 セキュリティエバンジェリスト
林 和博	株式会社九電工 副本部長
二名 信彰	株式会社 NTT ファシリティーズ 部門長
松浦 知史	東京工業大学 准教授
村瀬 一郎	技術研究組合制御システムセキュリティセンター 事務局長
森永 昌義	三菱電機株式会社 担当課長
柳田 貴行	三井不動産株式会社 統括
渡部 宗一	イーヒルズ株式会社 取締役

（オブザーバー）
国土交通省（大臣官房官庁営繕部設備・環境課、総合政策局情報政策課）
内閣サイバーセキュリティセンター 東京 2020 グループ

（欠席）
株式会社きんでん、セコム株式会社、横浜市、中部国際空港株式会社、中部国際空港施設サービス株式会社
部国際空港株式会社

3）議事要旨

産業サイバーセキュリティ研究会 WG1 ビル SWG（第 15 回）
議事概要

日時： 2023 年 1 月 31 日 15:00-17:00

場所： オンライン開催（Teams 会議）
構成員（敬称略）：
（座長）江崎 浩 東京大学大学院 教授
松浦 知史 東京工業大学 准教授
アズビル株式会社
イーヒルズ株式会社
NTT グループ（株式会社 NTT ファシリティーズ）
鹿島建設株式会社
株式会社九電工
株式会社きんでん（欠席）
技術研究組合制御システムセキュリティセンター
セコム株式会社（欠席）
ダイキン工業株式会社
株式会社竹中工務店
株式会社日建設計
日本生命保険相互会社
一般社団法人日本ビルヂング協会連合会
一般社団法人ビルディング・オートメーション協会
株式会社日立製作所
一般社団法人不動産協会
三井不動産株式会社
三菱地所株式会社
三菱電機株式会社
横浜市（欠席）
ICSCoE 2 期ビルチーム有志

（オブザーバー）
国土交通省（総合政策局情報政策課サイバーセキュリティ対策室）
内閣サイバーセキュリティセンター（東京 2020G）（欠席）
公益財団法人東京オリンピック・パラリンピック競技大会組織委員会（欠席）
中部国際空港株式会社（欠席）
中部国際空港施設サービス株式会社（欠席）
（事務局）
経済産業省（商務情報政策局サイバーセキュリティ課、製造産業局産業機械課）
株式会社三菱総合研究所

議題：
１． 開会
２． 各構成員より挨拶・１年間の振り返り
３． インシデントレスポンスの検討状況について

４． 委託事業調査の中間報告
５． 森ビルにおけるビルセキュリティの取組について
６． 自由討議
７． 閉会

議事：
２． 各構成員より挨拶・１年間の振り返り

- 電気事業法の改正や個人情報保護法により、サイバーセキュリティ対策を求められるようになった。空調編の対応など、OT のサイバーセキュリティに地道に取り組んでいる。
- 顧客から建設設備のサイバーセキュリティに係る要望が増えている。全体的に意識が高まってきていると思う。
- SOC を備えたビルの計画を行っている。建設の観点からはサイバーセキュリティの意識がある程度進んできたが、運用の観点からはまだ実感がなく、サイバー攻撃の事例等の共有が必要ではないか。
- ビルオーナーからのサイバーセキュリティに係る問い合わせが増えている。
- 利用者のサイバーセキュリティに係る意識が高まってきていると感じる。脆弱性情報があると、システムへの影響や対応方法についての問い合わせを多く受けるようになっている。ユーザの関心が高まっており、早いレスポンスも期待されているため、対応体制の強化を図っている。
- スマートビルや DX の問い合わせが増えており、付随して外部設備との接続とセキュリティに係る問い合わせが増えている。
- 不動産会社からクラウドシステムを導入する際のチェック項目が提示されるようになったが、対応に苦慮している。欧州では法制度化され、対応が大変になっている。
- 中小ビルでは、まだサイバーセキュリティの意識が高まっていない感覚である。
- スマートシティ、スマートビル、ビル OS が何をするのか、議論が活発になっている。CO2 削減も盛んになっており、セキュリティと合わせたビジネスが生まれそうである。
- 工場 SWG でサイバー・フィジカル・セキュリティ対策ガイドラインを策定・公開した。ビルと工場は両輪になると考えている。
- 建築設備設計基準に追加される設備では、エネルギー管理関係が多い。これらの設備はネットワークと関連するので注目している。令和 5 年版にはサイバーセキュリティ対策の記述を提案しており、本 SWG での議論をインプットしたい。
- ロボット導入や自動化のニーズが高まっており、クラウド連携が必要になっている。ヒヤリハットが発生しており、基本的な対策が重要だと実感している。
- IPA のデジタルアーキテクチャ・デザインセンター（DADC）ではデータ交換、認証技術なども含めて議論がされており、活動が盛んになっていると感じる。JEITA ではスマートホームの議論が行われている。建物とサイバーセキュリティの議論が多くなっているように感じる。
- ビル以外では、ランサムウェアが情報系のサーバに感染して、制御系を止めざるを得ない事例が出ている。今後、クラウド連携がいろいろな分野で進化しつつあり、その辺りも注目が必要と思っている。
- 電気事業法対応の問い合わせが増えており、プロダクトのセキュリティ対策を本格化に取り組んでいる。顧客からの工場セキュリティに係る問い合わせも増えていると感じる。
- 共通編のガイドラインに倣って独自の OT セキュリティガイドラインを作成し、適合状況の点検を年 1 回実施している。電気設備のサイバーセキュリティ対策の対応をどうするか、検討中である。電気事業法の

保安規定にどう盛り込むか、独自の OT のセキュリティガイドラインをどう変更するか、検討している。ビルにおいて一番リスクが高いのは、公開サーバのある物件であり、悪い動きをした時に即座に検知できるようなシステム構築を進めている。

- 大規模ビルでは情報系の通信を利用する業者が増えており、ビル単体でも 30 数社になる。そのため、セキュリティの統制が取れない。業者による対応レベルの違いをどうするか、構築段階で頭を悩ませている。

3．インシデントレスポンスの検討状況について
（事務局より説明）

4． 委託事業調査の中間報告
（事務局より説明）

5． 森ビルにおけるビルセキュリティの取組について
（構成員より説明）

6． 自由討議
（1）体制について

- システムを止める場合に、本当に止めてよいのか、誰の責任で止めるのか。アクションを起こす場合の権限の明確化を整理しておくと良い。
- ビルのサブシステムで起こったインシデントで、ハンドリングを誰が行うかで時間がかかってしまったことがあった。ガイドラインでは、どのような関係者が統制を取るのが良いのか、触れてほしい。ビルオーナーか管理者かベンダか、ビルによって決めればよいと思う。
- ビルや企業の規模、対象設備により同一の施策は難しい。セキュリティ施策だけでなくインシデントレスポンスについてもレベル感が必要ではないか。

（2）ログ及びシステムバックアップの取得・活用について

- ログを取っておくことも重要である。ログをどう取って、分析・検索するのか、ログを取らなければできないことを示さないと、現場で実際に対応してもらえないのではないか。
- バックアップについては、取り方がポイントである。コントローラはリセットすれば戻ってしまうことが多いので、設定値のバックアップが重要である。
- バックアップは、基本的にはベンダに対応してもらうしかない。そのため、どこを対象にしてどこを対象外にするかを決めておく必要がある。頻度は、定期的にやることが重要である。これらは保守契約等で決めておくと良い。
- バックアップに対して、①誰が実施するか、②対象はどれか、③頻度はどのくらい実施するか、の 3 点について検討することを明記されると良い。

（3）ビル全体のシステム関係情報の整理について

- 「準備段階」で、ビルのシステム的に観た全体図を整理することを記載して欲しい。IT と同様に、OS やミドルウェアやバージョンも記載する必要がある。

- システムの全体像について、ネットワークの全体像（セグメンテーションなど）もあるとよい。少なくとも、誰に聞けば分かるかだけでも整理しておくと良い。
- システムの全体像は、現状では外部の委託がない。ガイドラインの中でも、準義務ぐらいに書くと、全体像を描くという作法が根付くのではないか。
- あるビルで全体像を描いたことがある。その時はネットワークから調べて作成した。いろいろな設備ベンダが入るため、全体像を作るのは、全体をまとめているゼネコンが良いのではないか。
- システムの全体像については、ニーズがあれば各事業者が対応するようになるのではないか。OA や FA 業界の事例を記載してはどうか。

（4）インシデント発生後の対応

- インシデントの起きた状況を社内の他のビルの部門と連携して、注意喚起を最初にやるべきではないか。自社だけでなく、協会等で共有できるとなお良い。
- ビルは可用性が重視されるので、根本的な対処ができなくても監視を強化して運用継続する、手動で運用することもありうる。
- 「c.封じ込め段階」の中で、「影響を受けたシステムは、切り離した後、詳細調査用データを取得完了するまではマシンの電源を切らずに置いておく」ことも、明記したほうが良い。電源を落とすと消えてしまう侵入痕跡もある。

（5）その他

- 「フォレンジック」と書くと重い作業に思われる可能性がある。目的を明確化してログを取る例を示すぐらいでも良いのではないか。
- インシデントなのか故障なのかの切り分けは困難であるが、BA システムがランサムウェアに感染したら何が起きるか等も記載してはどうか。
- 参考まで、故障をふくめて FTA を整理することが必要ではないか。
- ログは、なにを取るかを整理しないと「ログ貧乏」となるため、何を見つけたいからログを取るのかを整理する必要があると思う。

以上

4）ロジ業務の実施

会議運営のためのロジ業務（日程調整、Web会議環境確保、会議運営に必要な備品等準備、資料準備、Web 会議室設営、出欠、会議運営、議事録作成、有識者委員に対する謝金支払い等）を実施した。

3.3.2 作業グループの運営

空調編作業グループ、インシデントレスポンス・ガイドライン作業グループの運営を行った。

（1） 空調編作業グループの実施

ビルガイドライン空調編のパブリックコメント実施後に、その対応についての確認と意見集約のために合計 2 回の空調編・作業グループを開催・運営した。

1） 第1回

a. 日時　2022 年 8 月 5 日 13:00～15:00

b. 場所　Web会議（Teams）

c. 出席　ダイキン工業、アズビル、九電工、イーヒルズ

d. 主な議題・検討内容

- 空調編の構造について（共通編の再掲をやめることについて）
- パブリックコメントにおける個々の指摘への対応の確認

2） 第2回

a. 日時　2022 年 8 月 8 日 10:00～12:00

b. 場所　Web会議（Teams）

c. 出席　ダイキン工業、アズビル、九電工、イーヒルズ

d. 主な議題・検討内容

- 空調編の構造について（共通編の再掲をやめることについて）
- パブリックコメントにおける個々の指摘への対応の確認

（2） インシデントレスポンス・ガイドライン作業グループの実施

以下の日時で合計 7 回のインシデントレスポンス・ガイドラインに係る作業グループを開催・運営した。

1） 第1回、第 2 回

a. 日時　2022 年 10 月 3～4 日

b. 場所　Web 会議（Teams）

c. 出席　イーヒルズ、九電工、きんでん、竹中工務店、CSSC、ICSCoEビル有志

d. 主な議題・検討内容

- 昨年度までの議論の振り返り
- 検討スケジュール（案）について
- 策定方針、構成（案）について

2）第３回、第４回

a. 日時　2022 年 12 月 6 日、9 日

b. 場所　Web 会議（Teams）

c. 出席　九電工、きんでん、竹中工務店、CSSC

d. 主な議題・検討内容

- ビル管理者へのヒアリング結果の共有
- 対応フロー（案）について
- ガイドラインの対象者について
- ガイドライン（素案）について

3）第５回、第６回

a. 日時　2022 年 12 月 26 日、27 日

b. 場所　Web 会議（Teams）

c. 出席　きんでん、九電工、竹中工務店

d. 主な議題・検討内容

- 対応フロー（修正案）について
- ガイドライン（修正案）について

4）第７回

a. 日時　2023 年 1 月 16 日

b. 場所　Web 会議（Teams）

c. 出席　九電工、きんでん、竹中工務店

d. 主な議題・検討内容

- ガイドライン（案）について

4. 宇宙分野に係る調査

産業分野別SWGとして令和3年1月に新たに立ち上げた「宇宙産業SWG」及び当該SWGの下に設置をした「宇宙産業SWG作業部会」の事務局として会議開催や資料案作成を行った。

4.1 宇宙分野における海外のサイバーセキュリティ対策等についての調査

米国、英国、欧州等における宇宙産業のサイバーセキュリティ対策に関する政策動向等について調査を行った。

4.1.1 宇宙分野における海外のサイバーセキュリティ対策等

（1）【米国】商用衛星システムに対するサイバーセキュリティ対策に関する法案の提出

2022 年 1 月、ゲイリー・ピーターズ上院議員により、CISA に対して、商用衛星システムの開発・保守・運用に関するサイバーセキュリティ勧告の策定を求める「衛星サイバーセキュリティ法」の法案が上院に提出された。同法案では、CISA 長官に対し、商用衛星システムのサイバーセキュリティに関する情報やシステムの安全な開発・運用・保守を支援する情報をオンラインで提供する「商用衛星システムに関するサイバーセキュリティ情報センター」を法案成立から 180 日以内に構築することを求めている。加えて、米国会計検査院（GAO）に対して、連邦政府による商用衛星産業に対するサイバーセキュリティ支援の状況を調査・報告することも求めている。2022 年 4 月には、トム・マリンノースキー下院議員及びアンドリュー・ガルバリーノ下院議員により、同様の法案が下院にも提出された。

（2）【米国】NISTIR 8270: 商用衛星運用のためのセキュリティ入門書ドラフト第 2 稿の発表

2022 年 2 月、米国 NIST は、商用衛星運用のためのセキュリティ入門書である NISTIR 8270 のドラフト第 2 稿を発表し、パブコメを開始した。パブコメは 4 月 8 日まで実施された。

文書では、NIST の Cybersecurity Framework（CSF）を実践するための 7 つのステップに基づき、図 4.1-1 に示すとおり商用衛星運用におけるサイバーセキュリティリスク管理の基本ステップを示しているほか、本ステップに基づく具体的なリスク管理の例として、地球低軌道上の小型衛星に適用した場合のケーススタディも示されている。

NISTIR 8270における商用衛星運用におけるサイバーセキュリティリスク管理の基本ステップ

Step 1：優先順位付けを行い、範囲を決定する	• 商用衛星システムアーキテクチャの構成要素を把握する。 • 組織のミッションや事業目標に応じたサイバーセキュリティプログラムの範囲を決定する。
Step 2：方向付けを行う	• 対象となるシステムに関連する資産及び規制要件や、全体的なリスクアプローチを特定する。 • 対象となるシステムや資産に適用される脅威及び脆弱性を特定する。
Step 3：現在のプロファイル※を作成する	• 対象となるシステムや資産に対して既に実施している対策をCSFのサブカテゴリーに基づきリスト化する。 • サブカテゴリーへの対応状況を踏まえ、CSFの5つの機能（識別・防御・検知・対応・復旧）に対する対策実施状況を評価する。
Step 4：リスクアセスメントを実施する	• 商用衛星システムの運用環境を分析し、新たなサイバーセキュリティリスクを特定する。 • 内外のサイバー脅威情報を使用し、セキュリティインシデントの可能性や当該インシデントが組織に与える影響を分析する。
Step 5：目標のプロファイルを作成する	• 組織に期待されるサイバーセキュリティの成果について記述した目標となるプロファイルを作成する。 • 組織固有のリスクに対処するために、組織独自のサブカテゴリーを追加することができる。
Step 6：ギャップを判断・分析し、優先順位付けを行う	• 現在のプロファイルと目標のプロファイルを比較し、サイバーセキュリティの取組に関するギャップを特定する。 • 目標のプロファイルに記された成果を達成するための行動計画を策定する。
Step 7：行動計画を実施する	• Step 6で特定されたギャップに対して取るべき行動を決定する。 • プロファイルの見直し、ギャップの再評価、行動計画の更新は、2年に一度、又は重大なインシデント等があった際に実施する。

※ プロファイルとは、現在のセキュリティ対策と目指すべきセキュリティ対策を、自組織の事業上の要求事項やリスク許容度、割当可能なリソース等に踏まえて整理したもの。

図 4.1-1　NISTIR 8270 における商用衛星運用におけるサイバーセキュリティリスク管理の基本ステップ
（出典：NIST, “NISTIR 8270 (Draft) Introduction to Cybersecurity for Commercial Satellite Operations (2nd Draft)“に基づき三菱総合研究所作成）

（3）【米国】国際衛星通信ネットワークへの脅威に対するセキュリティアドバイザリーの発表

2022 年 3 月、米国 CISA 及び FBI は、国際衛星通信のネットワークに対するサイバー攻撃の脅威に関する緩和策や関連情報をまとめたセキュリティアドバイザリーである AA22-076A を発表した。本セキュリティアドバイザリーでは、衛星通信ネットワークのプロバイダーに対し、衛星通信機器における異常なトラフィックを検出するための追加監視を実施すること、サイバー脅威活動を把握するために ODNI レポート[11]を参照することを強く推奨している。また、衛星通信ネットワークのプロバイダー及び顧客に対して、すべてのアカウントに対する安全な認証方法を使用すること、最小特権の原則を適用すること、IT サービスプロバイダーとの信頼関係を確認すること等の緩和策の実施を強く推奨している。

[11] Office of the Director of National Intelligence（米国国家情報長官官房）の“Annual Threat Assessment of the U.S. Intelligence Community”のこと。最新版は 2022 年 3 月 8 日に公開。

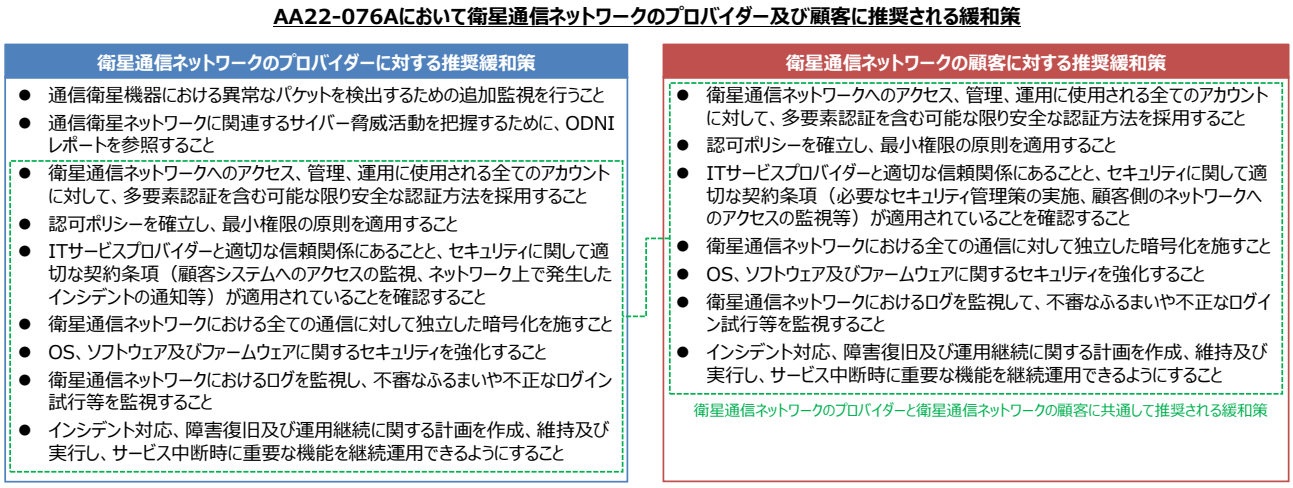


図 4.1-2　AA22-076A において衛星通信ネットワークのプロバイダー及び顧客に推奨される緩和策
（出典：CISA, “Alert （AA22-076A） Strengthening Cybersecurity of SATCOM Network Providers and Customers”に基づき三菱総合研究所作成）

（4）【米国】NISTIR 8401: 衛星地上セグメントに対する CSF プロファイルの発表

2022 年 12 月、米国 NIST は、NIST CSF に基づく衛星地上セグメントのためのプロファイルに関する文書である NISTIR 8401 を公開した。文書では、特に宇宙機運用管制及びペイロード運用管制の 2 つに焦点を当て、NIST CSF で規定されたサブカテゴリ毎に、衛星地上セグメントに対する対策項目及び対策の参考となる文献が明記されている。

NIST は、本プロファイルを活用する組織に対し、自組織のシステムに対して適用する際に、すべての対策項目をレビューすること、組織の事業目標に基づくサイバーセキュリティ活動を実践するために、各組織固有のプロファイルを開発することを奨励している。

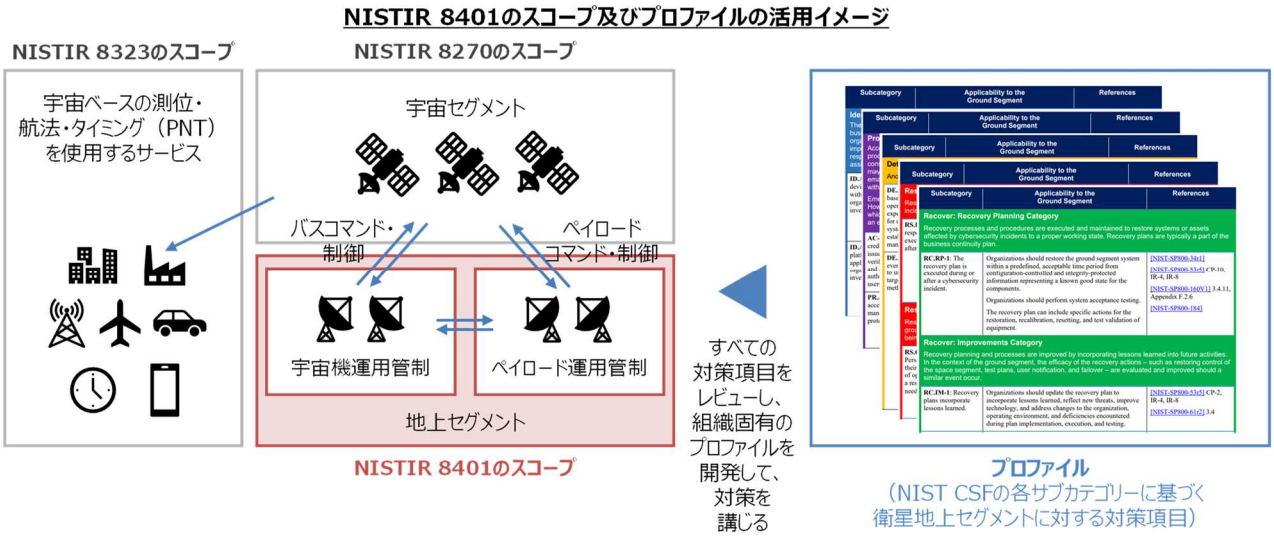


図 4.1-3　NISTIR 8401 のスコープ及びプロファイルの活用イメージ
（出典：NIST, “NISTIR 8401 Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Control”に基づき三菱総合研究所作成）

（5）【米国】国土安全保障に係る宇宙政策を示す文書の発表

2022 年 4 月、米国 DHS は、国土安全保障に係る宇宙政策を示す文書である“DHS Space Policy”の更新版を発表した。同文書では、米国の国土安全保障において宇宙システムが果たす重要な役割と関連省庁間の取り組みにおける DHS の役割を再定義しており、DHS は以下の 3 つの分野で主導的役割を果たすとしている。

A） 宇宙システムのサイバーセキュリティの推進

B） 国土安全保障に係る機能保証（Mission Assurance）の計画と実行

C） 宇宙環境が破壊又は劣化した場合の国土への潜在的影響の対応と緊急時計画の策定

「A） 宇宙システムのサイバーセキュリティの推進」に関して、宇宙システム関係企業に対するセキュリティ原則の採用を奨励するとともに、SPD-5 に沿ったベストプラクティス、教育教材、標準を開発する旨を明記している。

国土安全保障に係るDHSの宇宙政策（DHS Space Policy）の概要

A) 宇宙システムのサイバーセキュリティの推進	● DHSは、宇宙システムの設計、開発、取得、配備、運用の全ての段階において**サイバーセキュリティの原則を取り入れるよう企業に対して奨励**し、さらに多様な政府・産業界のパートナーとの密接な関係を維持し、**宇宙政策指令5（SPD-5）に沿ったベストプラクティス、教育材料、標準を開発**する。
B) 国土安全保障に係る機能保証（Mission Assurance）の計画と実行	● DHSは、意図的又は偶然の干渉や有害な操作に対し、NEF(National Essential Functions)やNCF(National Critical Functions)における**安全かつレジリエントな器材や能力の使用を奨励**し、連邦政府機関や民間セクターとの協力を重視する。 ● さらに、能力や機能が低下又は拒否された宇宙環境におけるNCF等の継続性を評価するため、**重要な宇宙システムの損失に対する手順と継続計画(Continuity Plan)を策定**し、**内部演習を実施**するとともに、宇宙システムの損失に対するDHSのレジリエンスを高めるため、**宇宙システムの代替案を検討する継続計画を策定**する。
C)宇宙環境が破壊又は劣化した場合の国土への潜在的影響の対応と緊急時計画の策定	● DHSは、原因の如何を問わず、宇宙環境が悪化した場合の**緊急時対応計画(Contingency Plan)を策定**し、宇宙空間における規範と責任ある国家の行動に関する**省庁間及び国際的な議論に参加**等を行う。

図 4.1-4 国土安全保障に係る DHS の宇宙政策（DHS Space Policy）の概要

（出典:DHS, “DHS Space Policy”, https://www.dhs.gov/sites/default/files/2022-06/DHS%20Policy%20Statement%20063-01%20Revision%2001%20-%20DHS%20Space%20Policy.pdf

SPACENEWS, “Department of Homeland Security publishes space policy”, https://spacenews.com/department-of-homeland-security-publishes-space-policy/）

（6）【米国】宇宙軍による商用衛星通信サービスの事前セキュリティ評価プログラムの試行

2022 年 5 月、米宇宙軍宇宙システムコマンドは、米国 DoD が調達する商用衛星通信サービスのセキュリティ確保のための取組みである IA-Pre（Infrastructure Asset Pre-Approval）の試行を開始したことを発表した。2025 年 9 月までにセキュリティ評価を IA-Pre に完全に移行することを目指している。

従来の DoD の商用衛星通信サービス調達では、同一のサービスであっても、契約ごとにアンケート回答によるセキュリティ評価を実施していたが、IA-Pre では、NIST SP 800-53 に基づくセキュリティ管理策を用いて、商用衛星通信サービスごとの対策状況が事前に評価される。評価を踏まえ、対策状況が承認された場合、宇宙軍のサービスリストに登録され、以後は契約の都度のセキュリティ評価が不要となる。

図 4.1-5　IA-Pre の目的、現状及び今後の予定等／IA-Pre におけるセキュリティ評価のフロー
（出典：SSC, “SSC CSCO reaches critical milestone for IA-Pre, roll-out begins today”等に基づき三菱総合研究所作成）

（7）【米国】商用宇宙システムのサイバーセキュリティに関する公聴会の開催

2022 年 7 月、米下院科学・宇宙・技術委員会の宇宙・航空小委員会は、米国の宇宙領域における商用システムの重要性の増大や 2022 年 2 月の Viasat への攻撃等の脅威の増大を受け、商用宇宙システムのサイバー脅威に焦点を当てた公聴会を開催した。公聴会では、商用宇宙システムのサイバーセキュリティに関する全体像と政府機関等の取り組み状況を確認するため、MITRE、NIST 及び Aerospace Corporation から 3 名が出席し、質問に対する回答を行った。

公聴会の概要

目的	● 商業宇宙システムのサイバーセキュリティについて、**現在及び潜在的なサイバーセキュリティリスク、宇宙システムのサイバーセキュリティに関する政策やガイダンスの状況、並びに民間及び商業宇宙システムのサイバーセキュリティの促進・強化等の状況**を確認する。
出席者	● Theresa Suloway博士（スペース・サイバーセキュリティエンジニア, MITRE） ● Matthew Scholl氏（チーフ, Computer Security Division, Information Technology Laboratory, NIST） ● Brandon Bailey氏（シニアプロジェクトリーダー, Cyber Assessments and Research Department, The Aerospace Corporation）
主な質問	● 商業・民間の宇宙システムとサイバーセキュリティに関して、**取り組むべき問題の範囲**はどのようなものか？ ● 民間・商業宇宙システムのサイバーセキュリティの強化を**支援するために必要なこと**は何か？ ● 宇宙サイバーセキュリティのための**要員や連携の状況**はどのようなものか、また要員はどの程度まで宇宙システムとサイバーセキュリティの両方の専門知識を必要としているのか？ ● 商業宇宙システムのサイバーセキュリティのための**標準の役割**は何か、そのようなシステムのための**標準の開発状況**はどうなっているか？ ● 宇宙システムにおけるサイバーセキュリティの問題に関して、**政府機関はどの程度まで調整と協力**を行っているのか？ ● 宇宙システムにサイバーセキュリティの原則を**民間企業が採用することを奨励する**ためには、何ができるか？
出席者の主な回答	● 商用宇宙システムでは他社が開発したコンポーネントを活用するケースも有り、**他社のコンポーネントに起因するリスクが知らぬ間に悪用される可能性がある**。また、商用宇宙分野で最も緊急度の高いセキュリティ対策ニーズは、**衛星がハイジャックされ宇宙空間で衝突することへの対処**である。(MITRE) ● NISTは、連邦政府機関、産業界、学術界、国際的なパートナー等と連携し、宇宙分野のサイバーセキュリティに関するツールやガイダンス等を作成・公開している。(NIST) ● **商用宇宙システムのサイバーセキュリティに関して現状で複数のギャップが存在**する。例えば、脅威や脆弱性に関する迅速な情報共有の体制、セキュリティ実装を検証するための方法論、サプライチェーンリスク管理、内部犯行者に対する対応などが挙げられる。商用宇宙システムを保護するために、**国の重要インフラ分野の一つとして宇宙技術の専門的組織が必要である**と考えている。(Aerospace Corporation)

図 4.1-6 公聴会の概要
（出典：SUBCOMMITTEE ON SPACE AND AERONAUTICS COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY U.S. HOUSE OF REPRESENTATIVES HEARING CHARTER に基づき三菱総合研究所作成）

（8）【独国】BSI による衛星システムに対するサイバーセキュリティ対策ベースラインの発表

2022 年 6 月、ドイツ情報セキュリティ庁（BSI）は、衛星システムに対するサイバー攻撃対策のベースラインを定めた“IT-Grundschutz-Profil für Weltrauminfrastrukturen（Basic IT Protection Profile for Space Infrastructures）”を発表した。

文書では、一般的な衛星システムのアーキテクチャを定めた上で、典型的な衛星システムのミッションと脅威シナリオに基づくリスク分析を実施し、衛星システムが実装すべきセキュリティ管理策（推奨事項）を規定している。セキュリティ管理策は、サイバーセキュリティ対策のベースラインを示した BSI の既存フレームワーク“IT-Grundschutz（Basic IT Protection）”を参照している。

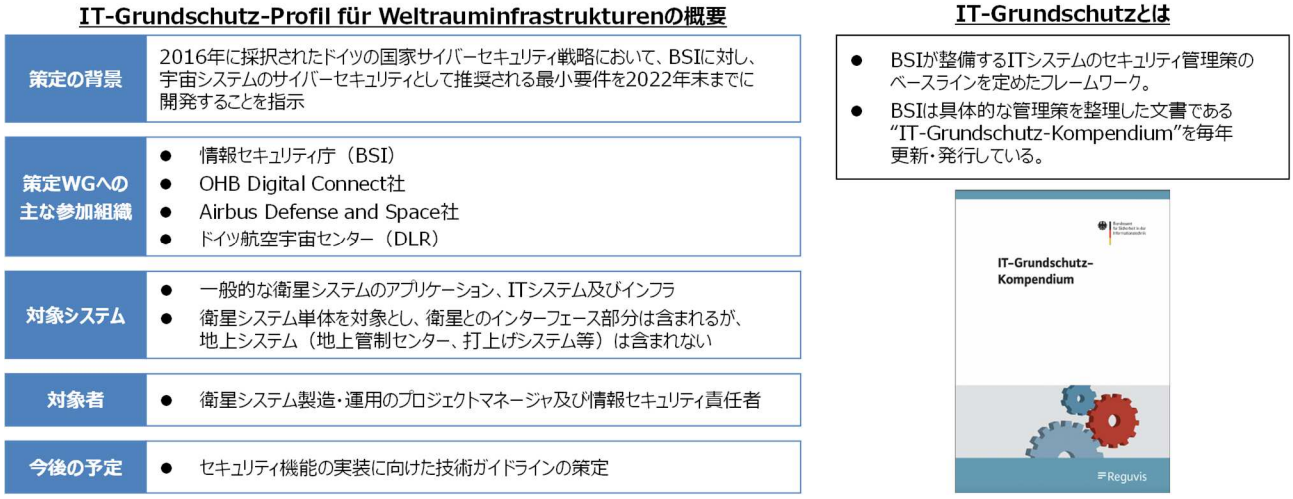


図 4.1-7 IT-Grundschutz-Profil für Weltrauminfrastrukturen の概要

（出典：BSI, “IT-Grundschutz-Profil für Weltrauminfrastrukturen”、“IT-Grundschutz-Kompendium”等に基づき三菱総合研究所作成）

BSI の文書では、衛星システムの参照アーキテクチャを「衛星システムのプロセス」、「各プロセスを実施するためのアプリケーション」、「アプリケーションが搭載される IT システム」、「ネットワークの構成要素」及び「システムが展開される施設」の 5 つの観点で整理している。

この参照アーキテクチャに対して衛星システムの典型的な 5 つのミッション及び 10 種の脅威シナリオを想定し、各ミッションにおける脅威のレベルを分析している。

リスク分析の結果を元に、「衛星システム全体に対して実装すべき推奨事項」及び「参照アーキテクチャの個別構成要素に対して実装すべき推奨事項」を示している。

セキュリティ管理策はあくまで推奨事項であるが、BSI は、具体的なセキュリティ対策の検討や、複数ステークホルダー間でのセキュリティ対策の合意に当たって本文書を活用することを推奨している。

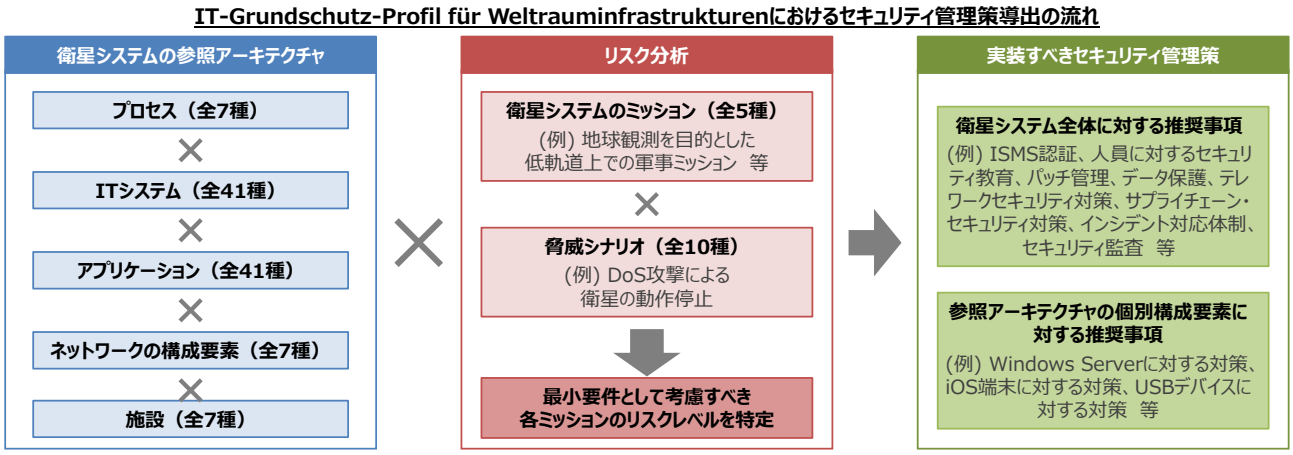


図 4.1-8　IT-Grundschutz-Profil für Weltrauminfrastrukturen におけるセキュリティ管理策導出の流れ
（出典:BSI, “IT-Grundschutz-Profil für Weltrauminfrastrukturen に基づき三菱総合研究所作成）

（9）【独国】BSI による宇宙インフラのサイバーセキュリティ戦略の発表

2022 年 8 月、ドイツ情報セキュリティ庁（BSI）は、宇宙インフラのサイバーセキュリティに関する BSI の戦略や役割、今後の取組み等を示した“Cybersicherheit für Weltrauminfrastrukturen（Cybersecurity for Space Infrastructures）”を発表した。

BSI は今後、本戦略、2022 年 6 月に発表した対策ベースライン及び 2023 年に公表予定の技術ガイドラインの 3 文書を軸とし、2023 年に設立予定の活動拠点を中心に、宇宙のサイバーセキュリティ強化に取り組むとしている。

Cybersicherheit für Weltrauminfrastrukturenの概要

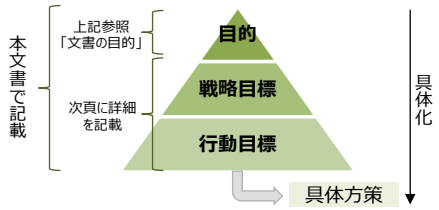
策定の背景	• 近年、**宇宙システムは市民生活や経済活動に不可欠**なものとなっており、**安全保障及び防衛の観点からも重要性**が高まっている • 一方、サイバーセキュリティに関しては、**既存の標準や枠組みがどの程度適用できるかが不明確**である • そのため、国家は宇宙のサイバーセキュリティの戦略を策定し、適切なセキュリティ対策を講じることが必要である
文書の目的	国家、経済及び社会に関連する宇宙インフラのサイバーセキュリティを強化し、安全な通信サービスを確実に提供するためのBSIの戦略及び役割を示す
対象とする脅威	意図的な脅威を対象とする。これは“IT-Grundschutz-Kompendium”やISO/IEC 27005等で示される**一般的なITシステムへの脅威と同様**
文書の位置付け	• 対象とする脅威及び以下に示す既存の宇宙やサイバーセキュリティに関する国家戦略から、BSIの戦略目標及び行動目標を導出している ✓ 内務省のサイバーセキュリティ戦略 ✓ 経済エネルギー省の宇宙戦略 ✓ 国防省の戦略指針 • 具体方策については、BSIが別途定める**対策ベースライン（2022年6月に公表済）及び技術ガイドライン（2023年に公表予定）**によって示される • 本文書は**年次で見直し**が行われ、対策ベースラインと技術ガイドラインとともに、PDCAサイクルを通じた改善が実施される 
今後の予定	• 2023年に宇宙のサイバーセキュリティに関する活動拠点を設置予定 • 2023年に技術ガイドラインを策定予定

図 4.1-9　Cybersicherheit für Weltrauminfrastrukturen の概要
（出典:BSI, “Cybersicherheit für Weltrauminfrastrukturen” に基づき三菱総合研究所作成）

本文書で定める 4 つの戦略目標及びそれらに紐づく行動目標は以下の図 4.1-10 のとおりである。

BSIの4つの戦略目標とそれらに紐づく行動目標

戦略目標	行動目標
1．宇宙産業におけるデジタル化及び新たな宇宙開発を安全に進める	• ドイツにおける宇宙のサイバーセキュリティに関する活動中心拠点を2023年にBSIに設置する。 • 宇宙のサイバーセキュリティに関する総合的な知見を確立する。 • 2022年に宇宙のサイバーセキュリティの最小要件を特定・整理し、2023年に技術ガイドラインへの詳細なマッピングを行う。 • システム開発段階でセキュリティ要件を考慮する（セキュリティ・バイ・デザイン）。 • 衛星アプリケーションの開発者及び運用者が統一的な宇宙のサイバーセキュリティ基準に準拠する。 • 機密システムや機密情報を扱うシステムについて、技術開発動向を踏まえて暗号システム等によるセキュリティ機能で保護する。 • セキュリティが重要な宇宙プロジェクトは“IT-Grundschutz”及びISO/IEC 27001, 27002に基づいた情報セキュリティマネジメントシステム又はこれらと同等の国際規格であるISO/IEC 27000ファミリーに準拠して管理する。 • 衛星アプリケーションやシステムの当局、製造者、開発者及び運用者間でサイバー脅威に関する啓発とセキュリティ意識の向上を推進する。
2．国内の宇宙とサイバーセキュリティの知見を結集し、脅威の全体像を把握する	• 宇宙のサイバーセキュリティに特化したワーキンググループにおける連携を進める。（2022年にキックオフを実施。） • 国内外のネットワークを通じたサイバーや宇宙に関する情報共有により、セキュリティ予防策の計画・導入やタイムリーなセキュリティ対策の実施を可能にする。 • サイバーセキュリティに関する官民の密接な交流を行う。
3．国家としての取組みと経済活動のシナジーを創出する	• 2023年までに、重要インフラのサイバーセキュリティを強化・確保するための確立されたプロセスのうち、必要なものを宇宙インフラに適用する。 • セキュリティが重要となる衛星アプリケーションのライフサイクル全体を通して、セキュリティに関する助言を行う。
4．国際的な協力・貢献により、ドイツの地位を向上させるとともに、他の欧州諸国と連携して標準や規範を策定し、宇宙インフラのサイバーセキュリティに関して欧州全体で協調する	• 宇宙のサイバーセキュリティに関する国際機関等へのドイツの参加を専門的な知見でサポートする。 • パートナー国と協力し（二国間・多国間）、共同ガイドラインを策定する。 • ドイツで策定したセキュリティ要件を国際的に展開する。 • 透明性と一貫性があり、確立された標準に基づいたリスク起点の推奨事項（必要に応じてガイドライン）を提唱する。 • 技術的な観点から宇宙のサイバーセキュリティに関する規格を策定する。 • 欧州における宇宙のサイバーセキュリティの基準に基づき、各国のパートナーと共に欧州における規則的な枠組みを開発する。

図 4.1-10　BSI の 4 つの戦略目標とそれらに紐づく行動目標
（出典：BSI, “Cybersicherheit für Weltrauminfrastrukturen”に基づき三菱総合研究所作成）

（10）【米国】Aerospace 社による宇宙システムのサイバー攻撃フレームワーク SPARTA の公開

2022 年 10 月、Aerospace Corporation が、MITRE ATT&CK ベースの攻撃フレームワークである Space Attack Research and Tactic Analysis（SPARTA）を発表した。STARTA は、宇宙システムに関するシステムの開発者及び管理者を継続的に教育し、宇宙領域で直面する独自のサイバー脅威に対抗できるようにするために作成された。

本フレームワークは、特に宇宙船を対象としたサイバー脅威に焦点を当てており、宇宙船に対するサイバーキルチェーンを攻撃者の視点から詳細に分析し、サイバー攻撃者の戦術・技術・手順を体系的に整理している。

なお本フレームワークは、2021 年同社より米国政府機関に提出された「Cybersecurity Protections for Spacecraft: A Threat Based Approach」を参考に整理されている。

SPARTAの概要

対象セグメント	● 地上セグメント、通信リンクセグメント及び宇宙セグメント
目的	● 宇宙システムに関するセキュリティの向上及び独自のサイバー脅威への対抗
背景	● 近年、宇宙船がサイバー攻撃の標的となっている ● 宇宙領域で直面するサイバー脅威に対抗できるようにする必要がある
対象者	● システム開発者・運用者・管理者・セキュリティ担当者 ● セキュリティ研究者
活用方法	● 本フレームワークを活用することで、サイバー攻撃者の戦術、技術、手順、ナレッジ、スキル等を理解し、攻撃の可能性を分析することが可能になる ● 攻撃者の意図を理解した上で必要な防御策を検討することが可能になる ● 攻撃シナリオに基づく実践的な演習に活用することができる
今後の予定	● V1.2のアップデートに向けた検討がなされている

「Cybersecurity Protections for Spacecraft: A Threat Based Approach」とは

- 地上・通信・宇宙の各セグメントで多層の防護策を講じる必要性を提示した文書。
- NIST SP 800-53等の既存のサイバーセキュリティ基準においてカバーされていない観点を整理した上で、脅威分析の結果に基づいた対策要求事項をまとめている。

図 4.1-11 SPARTA の概要

（出典：Aerospace Corporation, “Understanding Space-Cyber Threats with the SPARTA Matrix”、” Cybersecurity Protections for Spacecraft: A Threat Based Approach”に基づき三菱総合研究所作成）

（参考）SPARTAにおけるサイバー攻撃戦術一覧

戦術 Tactics	概要
偵察 **Reconnaissance**	攻撃者が攻撃を行うための足がかりを得るための技術で構成される。宇宙船の設計の情報・構成するシステム情報・記述子・ミッション等の攻撃する対象を選定するために必要な情報を事前に収集する。
資源開発 **Resource Development**	攻撃者が、攻撃対象を実際に攻撃するために必要なリソースを作成、購入、窃取する技術で構成される。この戦術では、攻撃する際に必要なインフラの購入やレンタル、ボットネットの作成、侵入技術のアップデートを行うことができる。
初期アクセス **Initial Access**	ネットワーク内に最初の足場を築くために、様々な侵入ベクトルを使用する技術で構成される。主要な通信経路や、ペイロード、地上システムなどの侵害による攻撃経路の確保や、宇宙船のセーフモード時に悪意のあるコマンドを送信し、宇宙船の保護機能を無効にすることができる。
実行 **Execution**	攻撃者によって、ローカルもしくはリモートのシステム、デバイス、その他の資産に対して悪意あるコードが実行される。
永続化 **Persistence**	攻撃を半永久的に実施可能とすることを目的とした戦術である。永続化のために、バックドアの挿入、正規のコードの置き換え、乗っ取り、起動コードの追加等、システムへの足場を維持するためのあらゆるアクセス、行動、設定の変更が検討される。
防御回避 **Defense Evasion**	攻撃者が被攻撃者に検知されるのを避けようとする技術で構成される。セキュリティソフトウェアのアンインストール・無効化、データやスクリプトの難読化・暗号化などを通じて、攻撃者は、通常では許可されないコマンドを処理させることを可能にする。
横展開 **Lateral Movement**	攻撃者が、環境内の様々なポイントに攻撃を拡大させる戦術である。
データ流出 **Exfiltration**	攻撃者が、ネットワークからデータを盗むために使用する可能性のある技術で構成される。リプレイ攻撃やサイドチャネル攻撃といった技術で、被攻撃者の所有する機密情報をはじめとするデータを流出される。
影響 **Impact**	一連の戦術の結果として与えられる攻撃の影響を示す。攻撃によって、被攻撃者のシステムやデータ操作・破壊によるシステムのサービス停止やシステムへのアクセス制限、プロセスやデータの完全性や可用性の破壊が行われる。

図 4.1-12 （参考）SPARTA におけるサイバー攻撃戦術一覧

（出典：Aerospace Corporation, “Space Attack Research & Tactic Analysis（SPARTA）”に基づき三菱総合研究所作成）

（参考）SPARTAにおけるサイバー攻撃技術一覧

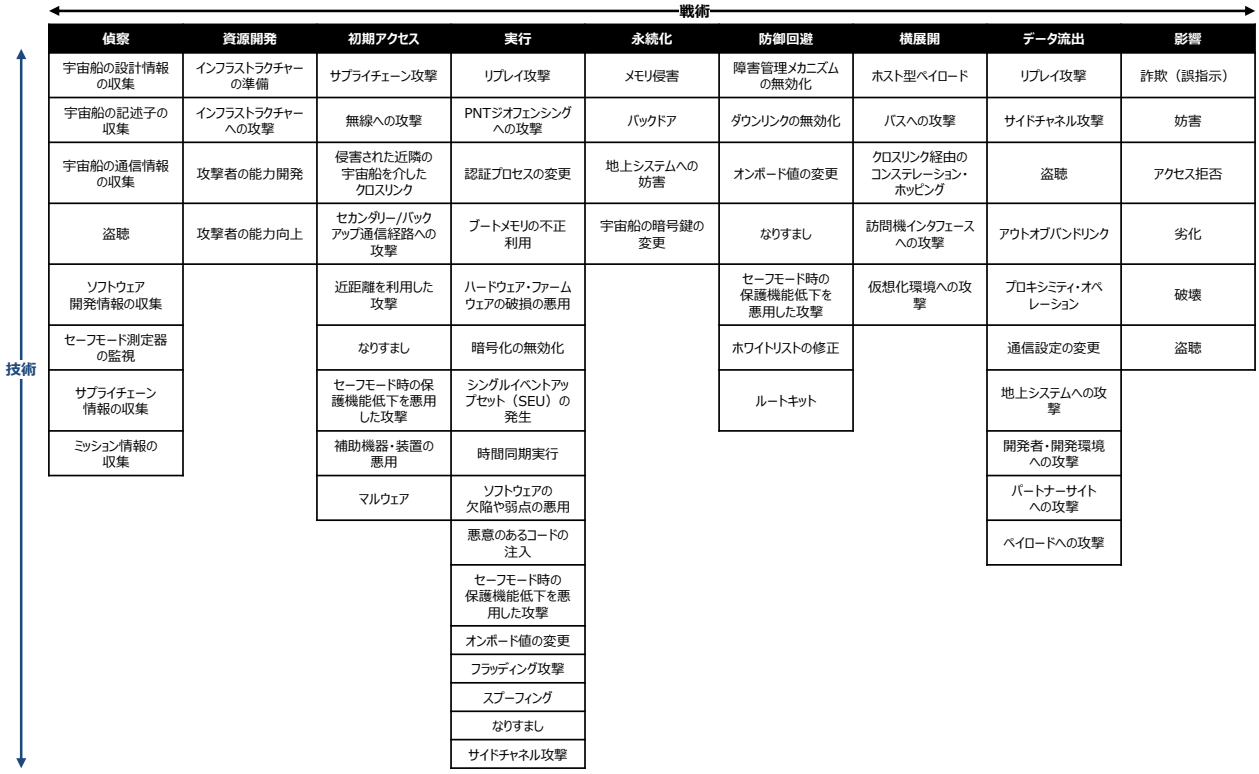


図 4.1-13 （参考）SPARTA におけるサイバー攻撃技術一覧
（出典：Aerospace Corporation, “Space Attack Research & Tactic Analysis (SPARTA)”に基づき三菱総合研究所作成）

(11)【EU】NIS2 指令の可決

欧州議会と欧州理事会は、デジタル化に伴い増加したサイバー攻撃・サイバーリスクに対するセキュリティ強化を目的として、現行の NIS 指令を改定した NIS2 指令を制定することに 2022 年 5 月 13 日に合意した。

NIS2 指令は、対象セクターにおけるセキュリティリスク管理対策の基準と EU 加盟国間の効果的な協力のための仕組みを定めた法案であり、対象として 16 セクター（必須分野：10 セクター、重要分野：6 セクター）を指定し、3 つの目標とそれを達成するための具体案を掲げている。

NIS2 指令では、宇宙セクターを含む複数のセクターを対象範囲に追加し、宇宙セクターにおける対象事業者として、「加盟国又は民間企業が所有、管理、運営する、宇宙サービスの提供を支援する地上インフラ事業者（ただし、欧州電気通信法指令の対象となる通信事業者を除く）」が追加された。加えて、対象セクター・対象事業者に求めるセキュリティリスク管理に関する項目が明記されたほか、罰則内容も具体化された。2022 年 11 月 28 日に欧州理事会は NIS2 指令を可決。EU 各国は 21 か月以内に本指令へ対応した国内法を整備することが求められている。

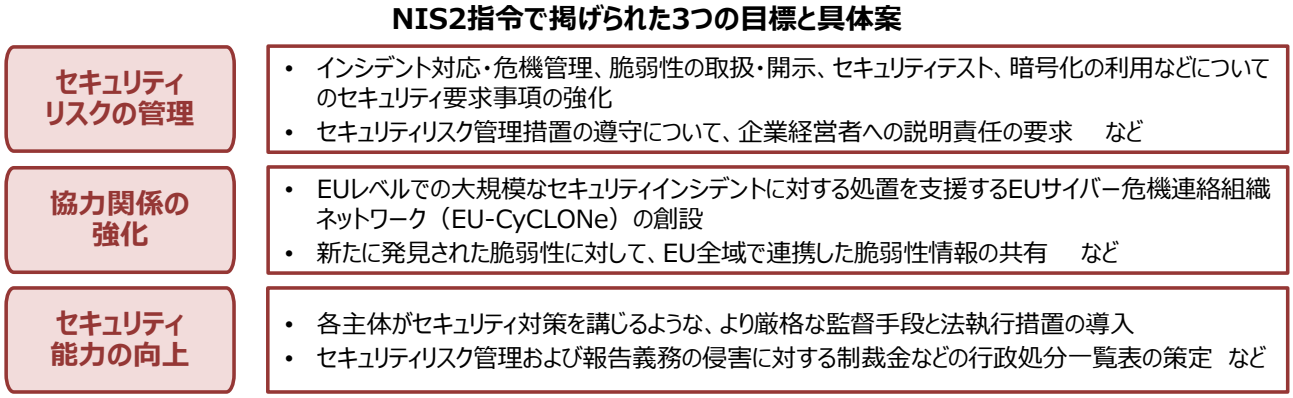


図 4.1-14 NIS2 指令で掲げられた 3 つの目標と具体案
（出典：European Parliament, The NIS2 Directive: A high common level of cybersecurity in the EU）

本指令は、必須分野・重要分野に属する対象事業者に適用されるが、所轄官庁が対象事業者に対して有する権限は必須分野・重要分野で異なり、必須分野に属する対象事業者に対してより厳格な監査・執行を行う権限を有する。

また、本指令では対象分野の事業者に求めるセキュリティリスク管理の 7 項目が定義されているが、これらの項目を満たすための具体的な対策や要件については指令内で定義されず、技術的・非技術的仕様を定めるための実装規則[12]を採択しうることが明記されている。

罰則について、このセキュリティリスク管理や報告義務[13]を侵害した場合は、1,000 万ユーロ又は事業者の前年度世界総売上高の 2%のいずれか高い方を課すと規定している。

（12）【米国】NIST CSWP 27 ：ハイブリッド衛星ネットワークに係るサイバーセキュリティフレームワークプロファイル（アウトライン文書）の公表

2022 年 11 月、米国 NIST は、ハイブリッド衛星ネットワーク（Hybrid Satellite Networks: HSN）に係るサイバーセキュリティプロファイルに関するアウトライン文書を公表した。

文書は HSN を形成するすべてのシステムを対象としており、NIST は関連組織に対して、本プロファイルに従ってサイバーセキュリティの方針を定めつつ、組織の事業継続計画（COOP）に反映するよう推奨している。

今後、NIST CSF に基づき、HSN サービスに関する組織において、組織の目的に応じたサイバーセキュリティ活動の検討に活用できる包括的なプロファイルが作成される予定である。

[12] 欧州全体での統一的な取組を実施するために、実施権限が欧州委員会に付与される規則のこと。
[13] 対象事業者は、所轄官庁や CSIRT に対して、サービス提供に重大な影響を及ぼすインシデントを不当な遅滞なく報告する義務（24 時間以内の通知、所管官庁・CSIRT からの要求があった場合の中間報告、1 か月以内の最終報告）が規定されている。

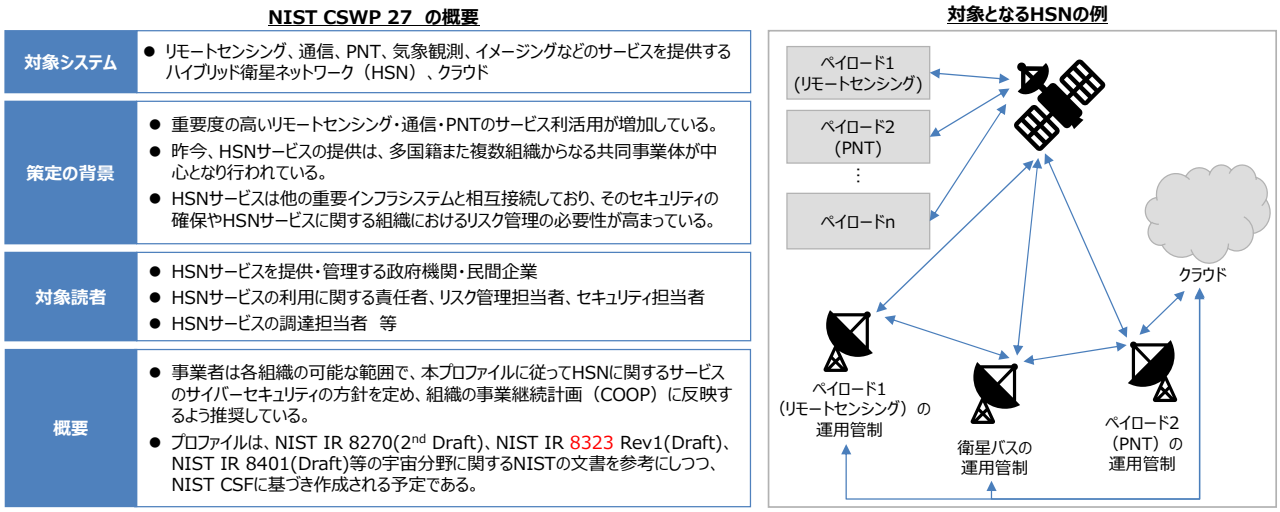


図 4.1-15 NIST CSWP 27 の概要

（出典：NIST, Cybersecurity Profile for Hybrid Satellite Networks (HSN) Cybersecurity, Final Annotated Outline Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN): Final Annotated Outline (nist.gov)）

（13）【米国】NISTIR 8323: PNT サービスに対する CSF プロファイルの改訂

2023 年 1 月、米国 NIST は、宇宙ベースの測位・航法・タイミング（PNT）を使用するサービスに関するセキュリティプロファイルである NISTIR 8323 を Revision 1 として改訂した。

本プロファイルは、米国大統領令 13905 で示されたセキュリティ確保に向けた 4 項目を踏まえ、NIST CSF の各サブカテゴリに基づく、PNT サービスに対するセキュリティ対策項目を明記している。

Revision 1 の改訂では、リスクマネジメント戦略のサブカテゴリに関する対策項目が追加されたほか、付録において、本プロファイルの想定される活用シナリオを追加している。

NIST は、本プロファイルを活用する組織に対して、包括的に対策項目をレビューすることや、組織の事業目標に基づくサイバーセキュリティ活動を実践するために固有のプロファイルを開発することを奨励している。

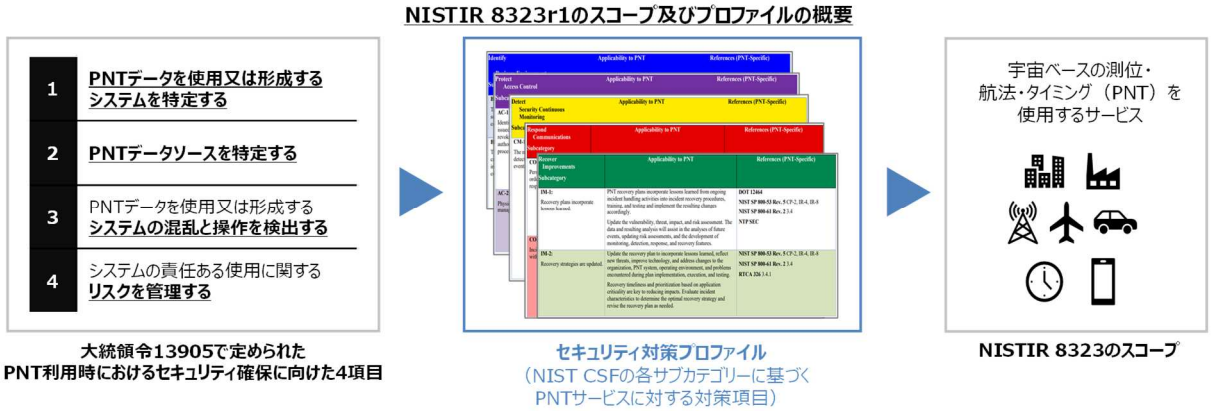


図 4.1-16 NISTIR 8323r1 のスコープ及びプロファイルの概要

（出典：NIST, NISTIR 8323r Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services に基づき三菱総合研究所作成）

（14） 【EU】安全保障と防衛のための EU 宇宙戦略の発表

2023 年 3 月 10 日、欧州委員会は欧州域での初めての宇宙戦略である“EU Space Strategy for Security and Defence”を発表[14]した。本戦略では、宇宙空間の脅威を評価するには、宇宙空間の対策能力を十分に理解した上で軌道上、地上、サイバー領域における能力と関連する行動を包括的に分析することが必要であるとしており、サイバー領域のレジリエンス確保については、NIS2 指令と連携しつつ、レジリエンスや保護能力を高めることが必要であるとしている。

さらに、宇宙システムの保護、情報共有、インシデントに関する協力のための EU 全体の包括的なセキュリティフレームワークの必要性が提起されている。この包括的なフレームワークとして、以下の検討の可能性が明記されている。

- EU 全体の一貫したアプローチを確保するため、また、“EU Approach for Space Traffic Management”に関する共同声明を踏まえ、欧州委員会は、EU 宇宙法の提案を検討する予定である。このような立法案は、国家安全保障上の利益を保護する一方で、EU の宇宙システム及びサービスのレジリエンスレベルを集団的に高め、EU 最外縁地域のような遠隔地の戦略的地上インフラの場所を含めて加盟国間の調整を確実にする枠組みを提供することができる。また、NIS2 指令とともに、包括的で一貫した枠組みを提供することができる。欧州委員会は、利害関係者の協議や影響評価の出発点として、既存制度の主要な特徴やその適用におけるプラクティスを取り上げる。また、この取組は、宇宙分野のセキュリティインシデントを体系的に通知することを可能にするセキュリティ・モニタリング・センターの開発にも及ぶ可能性がある。
- 欧州委員会は、重要サービスを提供するすべての宇宙システムの設計の際に、セキュリティが考慮されていることを確認するための要件について検討する。また、システムの初期設計段階において、関連するセキュリティ基準をより体系的に統合することも想定される。
- 欧州委員会は、宇宙資産やそのサプライチェーンを標的とした脅威に関する情報交換を奨励し、関連するセキュリティ・オペレーション・センター（SOC）への実用的な情報提供に重点を置く予定である。欧州委員会、CERT-EU、ENISA と緊密に協力し、EUSPA（EU 宇宙計画庁）は EU における宇宙分野の SOC として重要な役割を果たすことになる。また、要請に応じて、加盟国の重要な宇宙システムやサービス事業者を支援することも想定される。
- 欧州委員会は、サイバー関連を含むレジリエンス対策に関する認識を高め、業界団体間のベストプラクティスの交換を促進することになる。このような支援措置は、ニュースペースを含む中小企業にとって特に重要である。この観点から、欧州委員会は、EUSPA の支援を受けて、業界団体と、場合によっては ESA を含む関連する公的団体を集めた ISAC の設立を検討する。
- NIS2 指令、EU サイバーレジリエンス法、その他の既存のサイバーセキュリティの枠組みの実施は、宇宙で使用される重要なデジタル製品に対するサイバーセキュリティ要件の取り込みを促進することになる。宇宙分野における特定のサイバーセキュリティ基準や手続きは、関連する場合に EU 宇宙法の一部として考慮されうる。

[14] European Commission, An EU Space Strategy for Security and Defence to ensure a stronger and more resilient EU https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1601

4.1.2 宇宙分野における近年のセキュリティインシデント事例

米国、英国、欧州等における宇宙分野における近年のセキュリティインシデント事例について以下のとおり、調査を行った。

（1）【ウクライナ・欧州】衛星通信大手 Viasat のブロードバンドサービスに対するサイバー攻撃

2022 年 2 月 24 日、衛星ブロードバンドサービス大手 Viasat の通信衛星「KA-SAT」サービスに利用する数万の通信モデムが標的型 DoS 攻撃を受け、当該サービスを利用するウクライナや欧州の組織からの衛星ブロードバンドへの接続が一時的に不能となった。

このサイバー攻撃はロシアがウクライナに侵攻を開始する 1 時間前に発生したため、ウクライナ軍の指揮系統に対しても混乱を巻き起こしたとされている。

また、ドイツでは、当該モデムを使用する複数の風力タービンが攻撃の影響を受け、複数の発電事業者が管理する 7,800 基を超える風力タービンのリモート制御が不能となった。

2022 年 5 月 10 日、EU、英国、米国、カナダ、エストニア、オーストラリア、ニュージーランド等は、当該攻撃がロシアによるものであると正式に発表し、ロシアの行動を強く非難する声明をそれぞれ発表した。

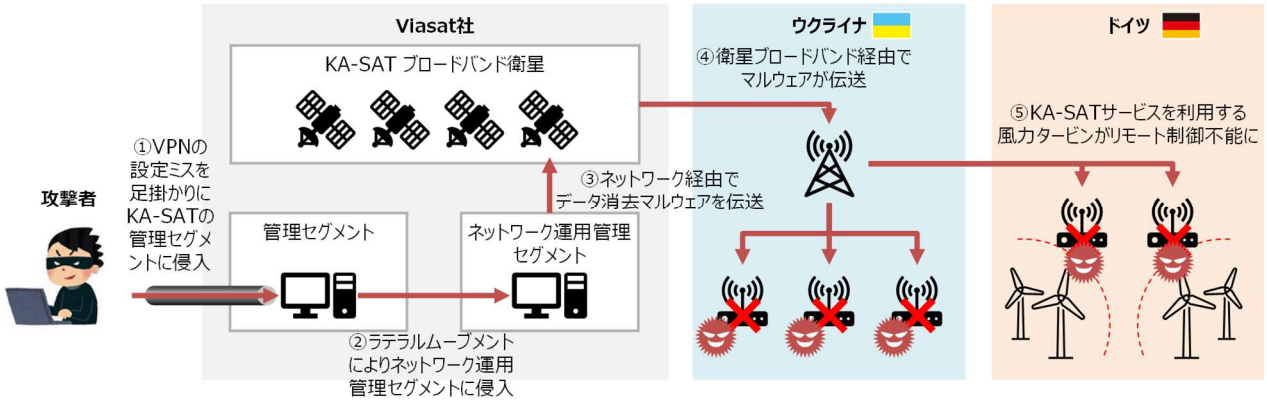


図 4.1-17 KA-SAT へのサイバー攻撃のイメージ
（出典：Viasat 社等の公開情報に基づき三菱総合研究所作成）

（2）【ウクライナ】ロシアによる GPS の地上基地局信号の妨害

2022 年 4 月 12 日、米宇宙軍の作戦担当副本部長を務めるデイヴィッド・トンプソン大将は米 NBC の番組に出演し、アメリカが提供しているウクライナの GPS 信号がロシアから妨害を受けている可能性があると述べた。

ロシアは、大型トラックのような妨害用車両を開発し、地上基地局側が GPS 精度向上のため発信している電波を妨害しているとみられる。

米シンクタンク CSIS は、同様の妨害が 2014 年前後から断続的に行われているとしている。

GPS が機能不全に陥った場合、自動車のカーナビやスマートフォンの地図等が使用不能となり、国民の生活への影響が出るのみならず、ウクライナ軍が使用している攻撃ドローンや偵察用の市販ドローンの飛行制御が困難となり、戦線への影響も懸念される。

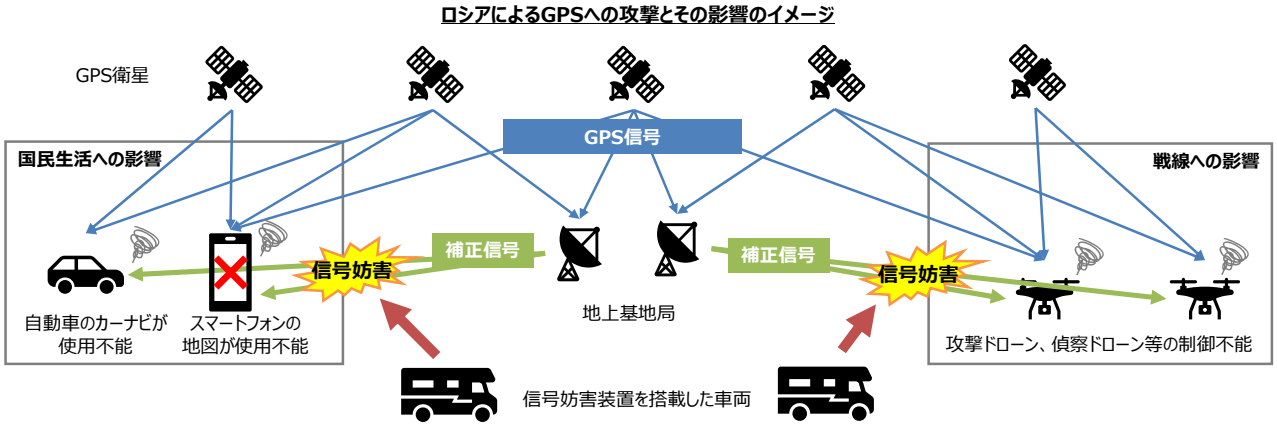


図 4.1-18 ロシアによる GPS への攻撃とその影響のイメージ
（出典：Newsweek 記事等に基づき三菱総合研究所作成）

（3）【ウクライナ】SpaceX 社の衛星インターネットへの攻撃

米 SpaceX 社は、ロシアのウクライナ侵攻直後より、ウクライナ政府の依頼に応じる形で衛星コンステレーションを用いたインターネット接続サービスである Starlink のサービスをウクライナで提供している。

地上設備の設置により利用できる Starlink は、侵攻によって地上ネットワーク回線が断絶した地域においてもインターネット接続を確立できるほか、攻撃用ドローンや偵察用ドローンとの通信にも活用することができる。

他方で、衛星信号を探知することにより、 Starlink の地上設備の位置を特定できるため、ロシアによる攻撃対象となりうる可能性が指摘されており、同社のイーロン・マスク CEO も Starlink の通信に対する電波妨害やハッキングの試みが増加していることを明かしている。

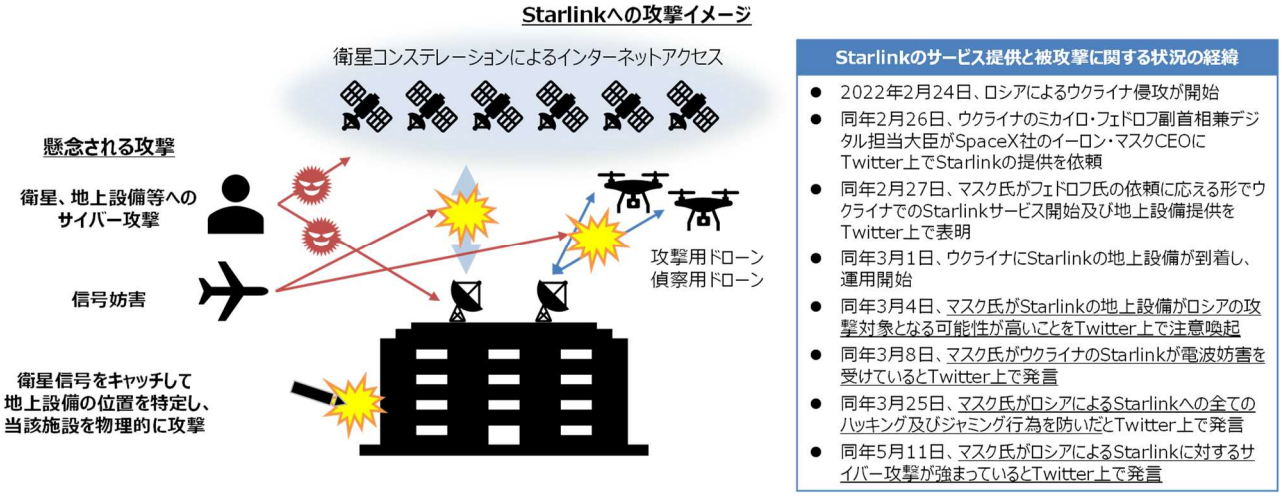


図 4.1-19 Starlink への攻撃イメージ
（出典：CNN 記事等に基づき三菱総合研究所作成）

4.1.3 米国宇宙分野におけるサイバーセキュリティに関する体制・文書等の関係

米国宇宙分野におけるサイバーセキュリティ関する体制・文書等の関係について、以下の図 4.1-20

～4.1-23 のとおり、調査・整理を行った。

（1）【米国】宇宙分野におけるサイバーセキュリティに関する体制・主要政策文書

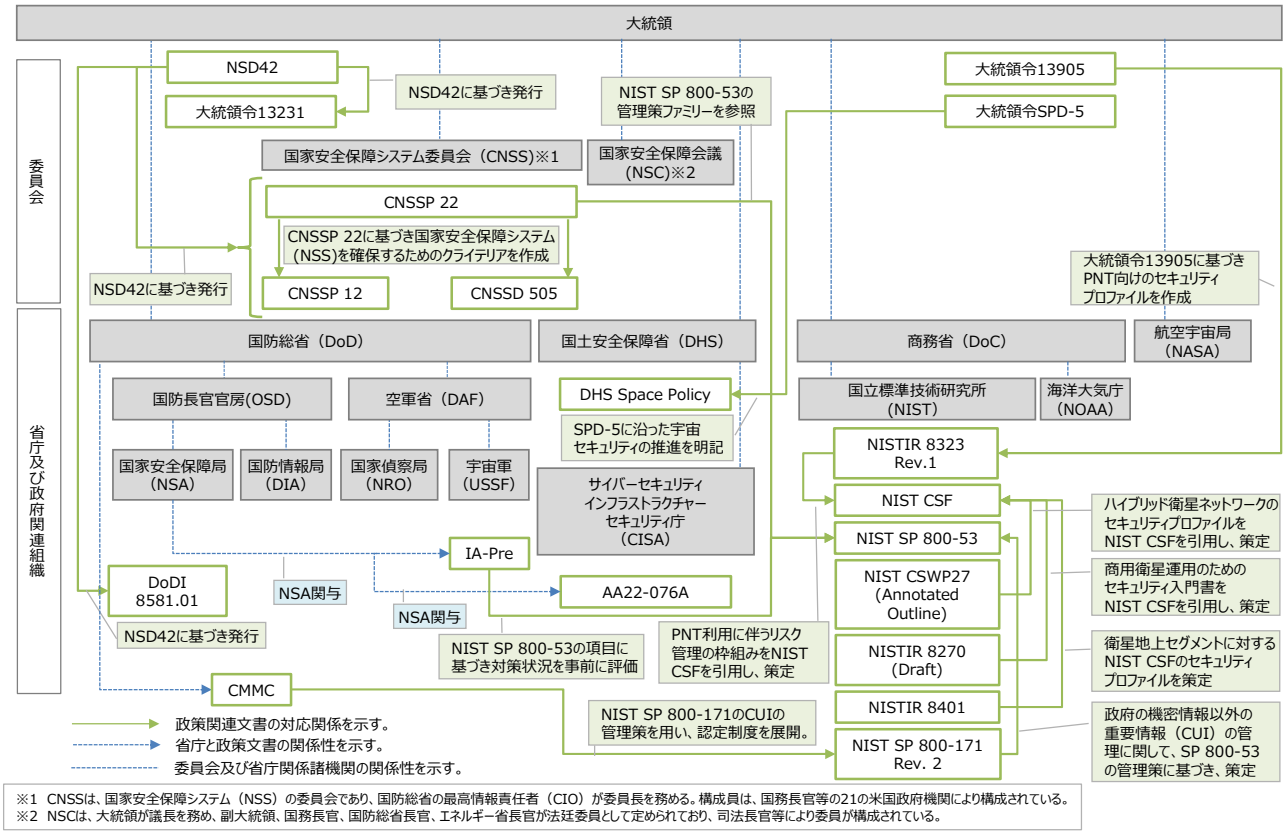


図 4.1-20 宇宙分野におけるサイバーセキュリティに関する体制・主要政策文書

【米国】宇宙分野におけるサイバーセキュリティに関する主要政策文書（1/3）

No	発行時期	分類	名称	発行主体	概要
1	1990年7月 発行	大統領令	NSD42 “National Policy for the Security of National Security Telecommunications and Information Systems”	大統領	国家安全保障システムのセキュリティに関する指示、運用手順、指針を提供する国家安全保障電気通信及び情報システムセキュリティ委員会（NSTISSC）の設立を指示した大統領令。
2	2001年10月 発行	大統領令	大統領令13231 “Critical Infrastructure Protection in the Information Age”	大統領	NSTISSCを、国家安全保障システム委員会（CNSS)に再指定することを指示した大統領令。
3	2005年6月 発行 2010年1月 改定	省庁訓令	DoDI 8581.01 “Information Assurance (IA) Policy for Space Systems Used by the Department of Defense”	DoD・NSA	米国政府及び国防総省が所有する宇宙システムについて、本方針に定められたIA要件を満たすよう求めた文書。
4	2005年2月 初版発行 2020年9月 第5版発行	ガイドライン	NIST SP 800-53 “Security and Privacy Controls for Information Systems and Organizations”	NIST	政府が調達する機器に関して機密情報を保護するために、セキュリティおよびプライバシーに関して詳細な管理策を規定したガイドライン。
5	2007年3月 発行 2012年1月 改訂 2018年2月 改訂	政策文書・政府調達基準	CNSSP 12 “National Information Assurance Policy for Space Systems Used to Support National Security Missions”	CNSS	NSD42に基づき策定された指針で、国家安全保障任務で用いられる宇宙システムに関する最低限度の指針を示している。
6	2009年2月 発行 2012年1月 改訂 2016年8月 改訂	政策文書・政府調達基準	CNSSP 22 “Policy on Information Assurance Risk Management Policy for National Security Systems”	CNSS	NSD42に基づき策定された指針で、国家安全保障システムのための情報保障リスク管理についての指針を示している。NIST SP 800-53の管理策ファミリーを参照している。

図 4.1-21 【米国】宇宙分野におけるサイバーセキュリティに関する主要政策文書(1/3)

【米国】宇宙分野におけるサイバーセキュリティに関する主要政策文書（2/3）

No	発行時期	分類	名称	発行主体	概要
7	2014年 初版 2018年4月 更新	ガイドライン	“Framework for Improving Critical Infrastructure Cybersecurity” (NIST CSF)	NIST	業種や企業規模などに依存せず、サイバーセキュリティ対策の効果を数値で評価するための基準など、汎用的かつ体系的なフレームワーク。
8	2017年7月 発行	政策文書・政府調達基準	CNSSD 505 “Supply Chain Risk Management (SCRM)”	CNSS	NSD42に基づき策定された指針で、国家安全保障任務で用いられる宇宙システムにおけるサプライチェーンリスクマネジメントについての最低限の指針を示している。
9	2020年1月 策定 2021年11月 改訂	フレームワーク（調達プログラム）	Cybersecurity Maturity Model Certification（CMMC）	DoD	防衛産業基盤企業のサプライチェーンにおけるFCI（連邦契約情報）とCUI（管理対象非機密情報）の保護を目的としたフレームワーク。DoDが調達する際の要件として、請負業者に対して適合を求めている。
10	2020年2月 発行	大統領令	大統領令13905 “Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services”	大統領	PNTサービスを利用するシステム等におけるセキュリティの確保に向けた取り組みの推進を指示した大統領令。本大統領令を元にPNT向けのセキュリティプロファイル（NISTIR 8323）が作成された。
11	2020年9月 発行	大統領令	大統領令SPD-5 “Cybersecurity Principles for Space Systems”	大統領	国家安全保障上の理由から、宇宙システムにおけるサイバーセキュリティの確保の重要性が強調し、悪意のあるサイバー活動による攻撃を想定して、システムの設計、開発、保護を行う必要がある旨を指示。
12	2020年2月 発行 2021年1月 更新	ガイドライン	NIST SP 800-171 Rev. 2 “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations”	NIST	非連邦政府の組織及びシステムが扱う「一般情報（Unclassified）」のうち、一部を「保護すべき情報（CUI：Controlled Unclassified Information）」として管理することを目的に、詳細な管理策を規定したガイドライン。
13	2021年2月 発行 2023年1月 改訂	ガイドライン	NISTIR 8323 “Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services”	NIST	大統領令13905に基づき作成されたPNT向けのセキュリティプロファイル。NIST CSFを元に、PNTサービスの利用者がサイバーセキュリティに関するリスクを管理するための枠組みを示している。

図 4.1-22 【米国】宇宙分野におけるサイバーセキュリティに関する主要政策文書(2/3)

【米国】宇宙分野におけるサイバーセキュリティに関する主要政策文書（3/3）

No	発行時期	分類	名称	発行主体	概要
14	2021年6月 第一草稿発行 2022年2月 第二草稿発行	ガイドライン	NISTIR 8270 (2nd Draft) “Introduction to Cybersecurity for Commercial Satellite Operations”	NIST	商用衛星運用のためのセキュリティ入門書。NIST CSFを実践するための7つのステップに基づき、商用衛星運用におけるサイバーセキュリティリスク管理の基本ステップを示している。
15	2022年3月 発行	セキュリティアドバイザリー	AA22-076A “Strengthening Cybersecurity of SATCOM Network Providers and Customers”	CISA、FBI	国際衛星通信のネットワークに対するサイバー攻撃の脅威に関する緩和策や関連情報をまとめたセキュリティアドバイザリー。衛星通信ネットワークのプロバイダー及び顧客に対する緩和策が提案された
16	2022年4月 第一草稿発行 2022年12月 最終発行	ガイドライン	NISTIR 8401 “Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Control”	NIST	NIST CSFの各サブカテゴリーに基づき、衛星地上セグメントに対する対策項目を示した文書。
17	2022年4月 発行	政策文書	“DHS Space Policy”	DHS	国土安全保障に係る宇宙政策文書。宇宙システムのサイバーセキュリティの推進に関して、宇宙システム関係企業に対するセキュリティ原則の採用を奨励するとともに、SPD-5に沿ったベストプラクティス、教育教材、標準を開発する旨を明記。
18	2022年5月 発表 2023年1月 最初のサービスを登録予定 2025年9月までに完全移行予定	調達プログラム・政府調達基準	“Infrastructure Asset Pre-Approval” (IA-Pre)	DoD・USSF	米国DoDが調達する商用衛星通信サービスのセキュリティ確保のための取組で、NIST SP 800-53に基づくセキュリティ管理策を用いて、商用衛星通信サービスごとの対策状況が事前に評価するプログラム。
19	2022年7月 第一草稿発行 2022年11月 最終発行	ガイドライン	NIST CSWP 27 “Cybersecurity Profile for the Hybrid Satellite Networks (HSN) Cybersecurity Annotated Outline”	NIST	ハイブリッド衛星ネットワーク（Hybrid Satellite Networks: HSN）に係るサイバーセキュリティプロファイルに関する概要ドラフト。NIST CSFに基づき、セキュリティプロファイルが作成される予定。

図 4.1-23 【米国】宇宙分野におけるサイバーセキュリティに関する主要政策文書(3/3)

4.1.4 その他関連事例

宇宙産業のサイバーセキュリティに関するその他関連事例について、以下のとおり調査を行った。

（1） Starlink のユーザ端末における脆弱性をついた攻撃の実証

2022 年 8 月に開催された Black Hat USA 2022 にて、Starlink のユーザ端末[15]の脆弱性を悪用することで、ユーザ端末への侵入及び任意コードの実行が可能であることがベルギーのセキュリティ研究者である Lennert Wouters 氏により報告された。

本攻撃は、ユーザ端末のアンテナに安価で自作可能なチップを物理的に取り付け、異常な信号を入力することで実現される。

SpaceX 社は、この攻撃の必要条件や影響範囲を踏まえ各ユーザでの対応は不要としている。

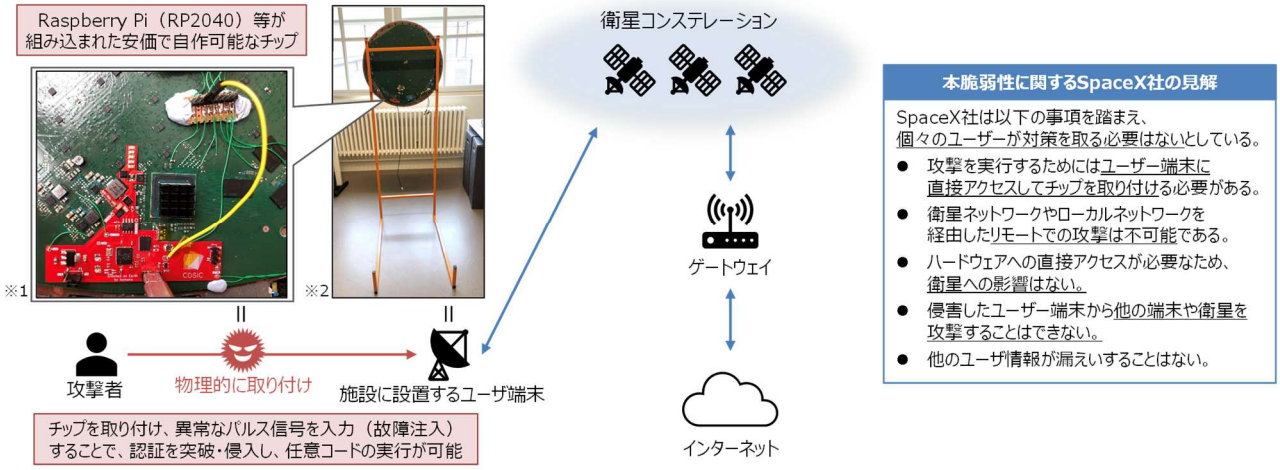


図 4.1-24 Starlink ユーザ端末への攻撃イメージ
（出典：Black Hat 2022 プレゼンテーション資料等に基づき三菱総合研究所作成）

（2） 退役した静止軌道上の放送衛星に対するハッキング

2022 年 8 月に開催された DEF CON 30 にて、退役後の放送衛星に信号を送信することで、任意の映像の配信や通話を行う攻撃の実証に成功したことが報告された。

本攻撃手法は、認証機構が無く、受信した信号を地上へ配信する放送衛星に適用されうる。攻撃には送信設備が必要であるが、信号自体は安価なソフトウェア無線で作成可能である。退役後の衛星は墓場軌道と呼ばれる地上からの信号が届かない高軌道に移動するが、墓場軌道への移動を待機している静止軌道上の衛星に対する攻撃が比較的容易に実施できることが示唆された。

[15] Starlink の衛星インターネットを使うための専用アンテナのこと。

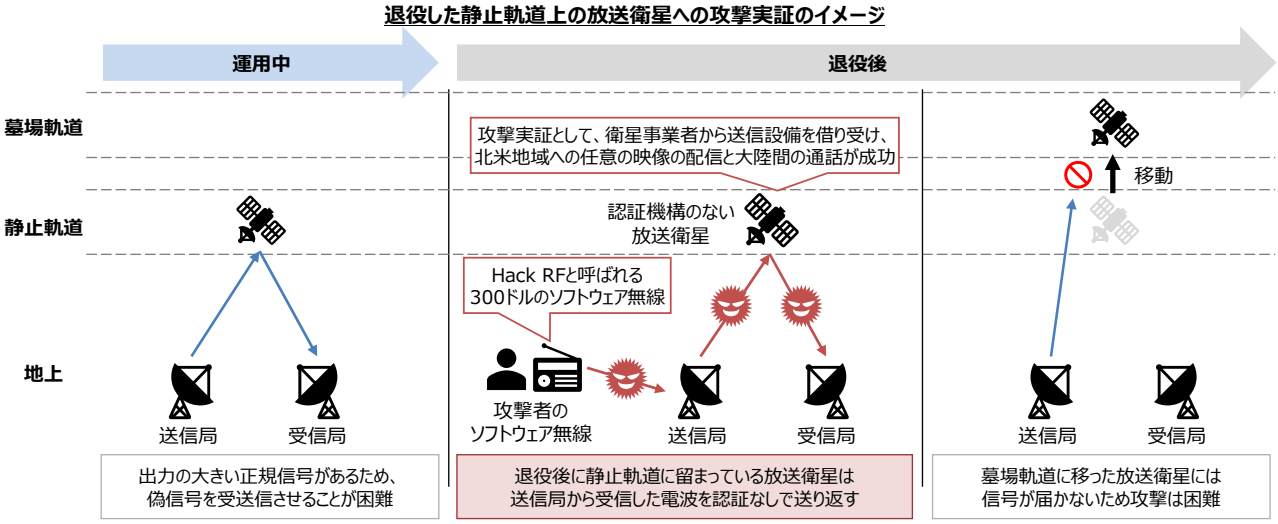


図 4.1-25 退役した静止軌道上の放送衛星への攻撃実証のイメージ
（出典：Newsweek 記事等に基づき三菱総合研究所作成）

（3）PCspooF：ミシガン大学及び NASA が TTE プロトコルに対する攻撃手法を発表

Time-Triggered Ethernet（TTE）は、飛行制御や生命維持装置等のクリティカルな基幹機器と、一般旅客の Wi-Fi やデータ収集等のベストエフォート（BE）で十分な機器を同一のスイッチやネットワーク上で共存させるプロコトルであり、NASA の Orion や Lunar Gateway、ESA の Ariane 6 等に使用されている。

ミシガン大学及び NASA は、TTE 上に設置した BE デバイスを悪用し電磁干渉（EMI）を発生させ、クリティカルな TT メッセージをドロップさせる攻撃手法（PCspooF）を発表した。

PCspooF による攻撃は航空機や自動車等のクリティカルなシステムの事故につながる可能性があるとされ、発表では、宇宙飛行のシミュレーションにおいてミッションの成功や安全性を脅かす制御不能なマニューバを引き起こす様子が示された。

対策として、電磁干渉を防ぐフォトカプラーやサージ防護機器を TTE スイッチに導入すること等が示されている。

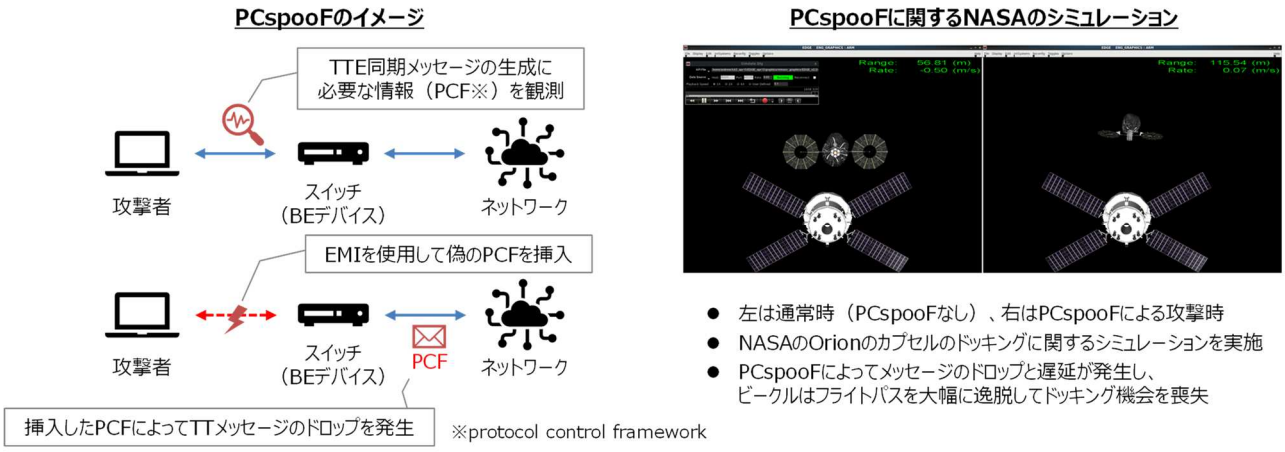


図 4.1-26　PCspooF のイメージ

（出典：A. Loveless, L. Phan, R. Dreslinski and B. Kasikci, ”PCspooF: Compromising the Safety of Time-Triggered Ethernet,” in 2023 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, US, 2023 pp. 572-587. https://web.eecs.umich.edu/~barisk/public/pcspoof.pdf）

4.2 検討会の運営

「4.3 民間宇宙システムにおけるサイバーセキュリティ対策ガイドラインの開発・更新」や、「4.5 情報共有・教育訓練のあり方などの検討」を行うにあたり、専門的な見地からの検討、分析、助言を得ることを目的に、宇宙分野及びサイバーセキュリティに係る有識者等からなる宇宙産業 SWG を運営した。なお、宇宙産業 SWG には実務者から構成される作業部・コアメンバー会議を設置し、技術的な論点においては、作業部会において検討を進めた。各検討会の概要について以下に報告する。

4.2.1 宇宙産業 SWG

本年は宇宙産業 SWG を 2 回開催した。
なお、2023 年 3 月現在、宇宙 SWG は下記の委員により構成される。

岩﨑　章彦	一般社団法人電子情報技術産業協会　セキュリティ専任部長
鹿志村　修	一般財団法人宇宙システム開発利用推進機構（JSS）衛星観測事業本部　本部長
片岡　晴彦	株式会社 IHI　顧問（元防衛省航空幕僚長）
木下　仁	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　セキュリティ対策推進部脆弱性対策グループ　主任研究員
来原　聡文	東北大学大学院工学研究科　航空宇宙工学専攻　准教授 NPO 法人大学宇宙工学コンソーシアム（UNISEC）　理事長
小山　浩	三菱電機株式会社　電子システム事業本部　主席技監
坂下　哲也	一般財団法人　日本情報経済社会推進協会（JIPDEC）　常務理事
佐々木　弘志	フォーティネットジャパン合同会社　OT ビジネス開発部　部長
名和　利男	株式会社サイバーディフェンス研究所　専務理事・上級分析官

丸山　満彦　　PwC コンサルティング合同会社 パートナー
満永　拓邦　　東洋大学 情報連携学部 准教授、IPA 産業サイバーセキュリティセンター専門委員
吉松　健三　　技術研究組合制御システムセキュリティセンター（CSSC）

（1） 第5回宇宙産業 SWG

1） 開催概要

日時：令和 4 年 7 月 21 日（木） 10 時 00 分～11 時 30 分
場所：オンライン開催

議題
1. 開会
2. 委員及び経済産業省からのプレゼンテーション
3. 事務局資料説明
   （ア） 海外動向及びインシデント事例について
   （イ） ガイドラインの修正案内容について
   （ウ） 今後の予定について
4. 自由討議
5. 閉会

配布資料:

資料1　議事次第・配付資料一覧
資料2　委員等名簿
資料3　第 4 回宇宙産業 SWG 議事要旨
資料4－1　名和委員からの情報提供（攻撃目的の着目した「ウクライナ情勢におけるサイバー攻撃」の分類と分析）【非公表】事務局説明資料
資料4－2　名和委員からの情報提供（ウクライナ情勢と連動して発生したサイバー攻撃から得るべき教訓）
資料5－1　経済産業省からの情報提供（工場システムにおけるサイバーセキュリティ対策の検討状況について）
資料5－2　経済産業省からの情報提供（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（案）第1版）
資料6　事務局説明資料
（1）宇宙分野における海外のサイバーセキュリティ対策等
（2）宇宙分野における近年のセキュリティインシデント事例
資料7－1　ガイドラインの修正内容【非公表】
資料7－2　民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.0（案）
資料7－3　民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.0 概要

資料（案）

資料7－4　民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン　Ver 1.0 概要資料英語版（案）

資料8　今後の予定について

2）議事要旨

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）
宇宙産業SWG（第5回）議事要旨

1. 日時・場所

日時：令和4年7月21日（木）　10時00分～11時30分

場所：オンライン開催

2. 出席者

委員　　：坂下委員（座長）、鹿志村委員、片岡委員、木下委員、栗原委員、小山委員、佐々木委員、名和委員、丸山委員、満永委員、吉松委員

オブザーバー：内閣府　宇宙開発戦略推進事務局、国立研究開発法人宇宙航空研究開発機構（JAXA）
宇宙産業SWG作業部会コアメンバー及び拡大メンバー

経済産業省：製造産業局宇宙産業室　室長　伊奈　康二
商務情報政策局サイバーセキュリティ課　課長補佐　塚本　大介

3. 議事内容

1）　宇宙産業SWG開催挨拶

事務局から、現下の状況を踏まえて、オンラインで開催を行うとの説明があった。

2）　委員及び経済産業省からのプレゼンテーション

（1）名和委員から『ウクライナ情勢と連動して発生したサイバー攻撃から得るべき教訓』の情報提供があった。

（2）経済産業省サイバーセキュリティ課塚本課長補佐から『工場システムにおけるサイバーセキュリティ対策の検討状況について』の情報提供があった。

3）　事務局資料説明

（1）**海外動向及びインシデント事例**

事務局から、宇宙分野における海外のサイバーセキュリティ対策や近年のセキュリティインシデント事例について情報提供があった。

（2）**ガイドラインの修正案内容**

民間宇宙システムにおけるサイバーセキュリティ対策ガイドラインβ版に対する意見募集結果の概要、及び具体的なガイドラインの修正内容について報告された。

（3）**今後の予定**

民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.0及び概要資料（日本語版・英語版）の正式公開スケジュールや国際調和に向けた海外関係機関との議論やガイドラインのアップデートに向けた議論の始動について報告された。また、将来的な情報共有体制の構築に向け、海外や他分野でのサイバーセキュリティに関する情報共有に関する取組について、調査及び宇宙産業SWGでの情報共有を進めることや宇宙産業SWG作業部会の物理開催など、実務者レベルでの信頼関係の醸成に向けた取組を進めることについて報告された。

4） 自由討議

（1）**ガイドライン及び今後の取組について**

各委員からは、ガイドライン及び今後の取組について、以下のご意見を頂いた。
ガイドライン及び概要資料の正式公開については、座長に一任とすることとなった。

（2）**各委員からの主な意見**

- 現状のガイドラインは、サプライチェーンの観点が弱いと認識している。Tier1のセキュリティ対策はしっかりと行われている一方、Tier2・Tier3ではセキュリティ対策が疎かであることが多く、サイバー攻撃の対象として狙われやすい。
- セキュリティ要件をどれくらいのレベルで実装すれば良いかについてのコンサルティングといった政府による支援が無ければ、ガイドラインの内容を実践することは難しいと思われる。
- 日米で協力を行う際には、サイバーセキュリティを含めたセキュリティ評価がキーポイントになる。契約を行う際にはセキュリティ評価が求められるが、評価を受ける際には1年以上の契約が求められるため、新規参加がしづらいという状況が発生する。米国には、セキュリティ評価や契約の方法についてオールドスペースがニュースペースに指導するという枠組みが存在する。このようなコンサルティングを行うような企業が出てくれば良いと思われる。
- ガイドラインのアップデートを行う際、記載されていることをうまく実装していくための方法についても議論を行う必要がある。
- 様々な分野でガイドラインが作成されているが、改訂といった維持管理の部分で負荷が生じると思われる。各ガイドラインで共通する部分と分野個別の部分とに分離し、各分野では個別の部分を中心に改訂の議論ができれば良いと考えている。こういった取組について、経済産業省の中で検討いただきたい。
- ガイドラインを改訂していく際、現状どれくらい実施できているのかについて把握する必要がある。情報共有体制に集った人の状況を把握し、それをガイドラインのアップデートに繋げれば良いと思われる。ガイドラインの中で取組が難しい部分が明らかになれば、コンサルティングに関する整理も進むと考えられる。
- ISAC はインシデント情報の共有を行うものであり、いきなりの参加は腰が引けると考え

られる。情報のレベル感を整理し、例えば海外の規制動向のような従来は各企業で独自に調査していた情報を持ち回りで調査したり、調査を行った企業に対して報酬を支払ったりといった形で情報共有を行えば良いと思われる。このような取組から始め、信頼関係の構築と共に機微情報の共有を少しずつ行っていけば良いと考えられる。

- ロシアや中国との関係性が大きく変化している中で、米国や欧州の動向に合わせる必要はない。自身の脅威を自ら見定め、それに必要な対策を考えていくことが必要である。
- 経済産業省には、調整役というよりも、実際に汗をかくような役割を担っていただきたい。例えば、宇宙ビジネス投資マッチング・プラットフォームでは、内閣府が費用を負担し精力的な取組を進めている。一方、サイバーセキュリティに関しては、相談や調整といったことが行われ続けていると感じている。米国の DC3（Department of Defense Cyber Crime Center） DCISE（The DoD Defense Industrial Base （DIB） Collaborative Information Sharing Environment）では、サイバーセキュリティに関する 5 つのサービスを政府として提供しており、それによって各社のコストメリットや最低限のセキュリティ確保を実現している。これは ISAC とは異なる取組であり、英国のワークは DCISE の形に変容しつつある。
- 民間の中で強くリードできる人の出現を期待し懇親会を開催するといった旧来の日本的な方法ではうまくいかないと他の ISAC の活動から感じており、施策についてはまだ検討の余地があると考えている。
- 本ガイドラインはライフサイクルを考慮して作られており、運用部分のセキュリティについて多く記載されているため有用であると感じている。一方、ものづくりに関する企画から廃棄に至るまでのライフサイクルについては、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の内容を採用する方針だったと記憶しているが、それで十分なのか憂慮している。開発における環境や実施すべき取組、出すべきアウトプット等について、これから議論が行われれば良いと思われる。
- コミュニティで日本として取り組むべき方向性が明確化され、そこからガイドラインの更新に関する議論にも繋がれば良いと感じている。
- 今回まとめられたガイドラインを色々な方に知っていただく必要がある。そのため、委員の皆様にもご協力いただき、ガイドラインを対外的に広めていきたい。
- ガイドラインの社会実装を具体的に進めていくためには、宇宙産業サブワーキンググループ作業部会の物理開催が必要だと感じている。新型コロナウィルスの感染が拡大しているが、しっかりと対策を行ったうえで物理開催を実施することでネットワークが強固になり、社会実装が進むことを願っている。

4．次回予定

- 最後に事務局から、今後のスケジュールについて以下のとおり連絡を行った後、閉会した。
  - 次回の第 6 回会合については、今回の議論を踏まえた検討を行ったのち、事務局から日程調整を行わせていただく。

以上

（2）第6回宇宙産業 SWG

1） 開催概要

日時　令和 5 年 3 月 16 日(木) 13 時 30 分～15 時 00 分

場所　オンライン開催

議題

1. 開会
2. 事務局資料説明
   (1) 宇宙分野における海外のサイバーセキュリティ対策等について
   (2) 今年度の作業部会での活動について
   (3) ガイドライン Ver 1.1 のアップデート内容について
   (4) ガイドライン Ver 2.0 に向けたアップデート方針について
   (5) 今後の予定について
3. コアメンバーからのプレゼンテーション
4. 自由討議
5. 閉会

配布資料:

資料1	議事次第・配付資料一覧
資料2	委員等名簿
資料3	第5回宇宙産業 SWG 議事要旨
資料4	事務局説明資料
資料5－1	民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.1(案)
資料5－2	対策要求事項チェックリスト【ガイドライン添付資料1】
資料5－3	NIST Cybersecurity Framework(NIST CSF)と宇宙システム特有の対策との対応関係【ガイドライン添付資料2】
資料5－4	民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.1 概要資料(案)
資料6－1	コアメンバー粟津様からの情報提供
資料6－2	コアメンバー小出様からの情報提供(配布なし・投影のみ)
資料6－3	コアメンバー國母様からの情報提供

2） 議事要旨

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)

宇宙産業 SWG(第 6 回) 議事要旨

1. 日時・場所

日時：令和 5 年 3 月 16 日（木） 13 時 30 分～15 時 00 分

場所：オンライン開催

2. 出席者

委員　　：坂下委員（座長）、鹿志村委員、片岡委員、木下委員、栗原委員、小山委員、佐々木委員、 名和委員、吉松委員

オブザーバー：内閣府 宇宙開発戦略推進事務局、国立研究開発法人宇宙航空研究開発機構（JAXA）

宇宙産業 SWG 作業部会コアメンバー及び拡大メンバー

経済産業省：製造産業局宇宙産業室 室長 伊奈 康二、室長補佐（総括） 小原 夏美

3. 議事内容

1）宇宙産業 SWG 開催挨拶

経済産業省伊奈室長から、闊達な議論を期待する旨挨拶があった。

2）事務局説明

宇宙分野における海外のサイバーセキュリティ対策等について

事務局から、宇宙分野における海外のサイバーセキュリティ対策や政策動向について情報提供があった。

（1）今年度の作業部会での活動について

事務局から、今年度の作業部会での主な検討内容として、ガイドラインのアップデート方針、情報共有体制の構築に関する検討概要について説明がなされた。

（2）ガイドライン Ver1.1 のアップデート内容について

ガイドラインの Ver1.1 のアップデートとして、添付資料の追加と細部の文言修正を実施した旨が報告された。

（3）ガイドライン Ver2.0 に向けたアップデート方針について

事務局から、ガイドライン Ver2.0 に向けたアップデート方針について、検討予定の論点が紹介された。

（4）今後の予定について

民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.1 及び概要資料（日本語版・英語版）の正式公開スケジュール、国際調和に向けた海外関係機関との議論やガイドラインのアップデートに向けた議論の始動について報告された。また、将来的な情報共有体制の構築に向け、2022 年 12 月に開催したコアメンバー会議で挙げられた意見を踏まえつつ、情報共有体制の在り方について検討を進めることや、宇宙産業 SWG 作業部会の物理開

催など、実務者レベルでの信頼関係の醸成に向けた取組を進めることについて報告された。

3） 情報提供

コアメンバー粟津氏、小出氏、國母氏から『民間宇宙システムにおけるサイバーセキュリティ対策ガイドラインの活用状況及び課題』について情報提供があった。

4） **自由討議**

・ NIST CSF の対応表について、現状は CSF を軸に整理しているが、本ガイドラインを軸に NIST CSF をマッピングする対応表を整理してほしい。

➢ コアメンバー会議の中でも議論したが、NIST CSF と本ガイドラインの粒度に差があり、整合性をとるのが難しく混乱を生むことを懸念したため、NIST CSF を軸に整理した。逆引きに使えるというわけではないが、Excel のフィルタリング機能を利用することは可能である。

・ 情報共有体制の成熟度モデルについて、フェーズ 1、2 では、会員に対する情報共有が求められているが、同時に対外発信も重要である。より多くの組織に参画を望む場合、閉鎖的な組織では規模の拡大は難しく、記載を検討いただきたい。

➢ 情報共有体制の在り方について本年度検討を続けてきたが、官主導のメリット、デメリットがあり、どのような体制で行うかについて結論が出ていない。本年度は、コアメンバー間の信頼関係を構築するための取り組みを実施しており、情報共有体制の構築に向け取り組みを推進している。今後は、米国、欧州とも情報を共有していけると良い。そういった取り組みを後押しするために政府間交流も積極的に行っていきたいと考えている。

・ 衛星において、インターネットとは分離されている現状がある。SPARTA の攻撃戦術に対して、どのような構造の衛星であれば対処しなくてはならないかなど、衛星のアーキテクチャとの対応をどのように考えていくのかを伺いたい。また、今年度 NIST CSF との対照表を作成していただいたが、SPD-5や商用衛星のガイドライン等との対応表の作成も検討していただけると良い。

➢ 衛星のアーキテクチャについては議論が進んでいない。他方、SPARTA のサイバー攻撃のキルチェーンは網羅的に整理されており、衛星、光通信においても一部適用され得る技術があると考えている。

➢ NIST の商用衛星のガイドラインとの対応表については、アメリカ政府と調整していきたい。どういう場合に何を求めているのか、米国政府と言語を合わせていく努力が必要だと考えている。

・ 経済産業省と公正取引委員会が公表している「サプライチェーン全体のサイバーセキュリティの向上のための取引先とのパートナーシップ構築に向けて」に関する内容は入っているか。
入っていないとしたら、同じ経済産業省から公表されているものなので、確認をお願いしたい。
現状のガイドラインは、取引先に過剰な要求事項を整理している可能性もあり、下請法に配慮するような記述も重要である。また安保関連 3 文書で議論されている特定社会基盤事業に宇宙が入れられるのか。

➢ 前者の指摘は、内容を確認し記載ぶりを検討したい。後者の指摘について、米国や欧州で

宇宙を重要インフラの一部にするか否かの議論がある。宇宙分野の全てが重要インフラとなるかは、議論が行われている段階であり、内閣府の宇宙事務局とも調整している。政府全体の方針としてまだ定まっていないため、今後も議論が望まれる。

・ ガイドラインの対象範囲を観測衛星に限定しているが、対象範囲を広げる議論をしてほしい。Ver2.0 で対応することも考えられる。

  ➢ 所管省庁が異なる問題がある。経済産業省のみで検討すると現在の対象になってしまうため、政府全体で取り組みが進められると良いと考えている。

・ 本ガイドラインは、安全保障の分野でも非常に参考になる取り組みであると感じている。本ガイドラインの取り組みを宇宙政策委員会安全保障部会、防衛省・自衛隊にも発信してほしい。ウクライナ Viasat の事案を念頭に入れると、執拗にネットワークの脆弱性を突くという攻撃が見られ、対策を重ねても、脆弱性を突かれる可能性があるほか、内部の工作員による実行可能性があることなどの問題があると考えている。そのため、業界内でのサイバーセキュリティの情報共有は重要であり、P18 で示されるフェーズ 3 に速やかに移行する必要があると考えている。今後のタイムラインについて考えがあれば教えてほしい。

  ➢ 情報共有体制の検討においては、まず信頼関係の構築が重要であり、顔を突き合わせて、議論することが求められると考えている。信頼関係を構築できるような取り組みを続けることで、情報共有体制の構築を後押しできるのではないか。

・ ガイドラインについて今後どのように運用していくかが重要である。サプライチェーン上の小規模な事業者に対しても対策の検討が必要とされており、対策を必須で行うべき項目と対策が推奨される項目とが明確になると良い。

  ➢ ガイドラインの中では、要求事項、基本対策事項、解説を記載しており、要求事項は関与している全事業者に対策を求めていく予定である。他方、サプライチェーンをどこまで巻き込むか、またどのレベルまで対策を求めていくのかについては、今後の検討課題である。

・ 大学発の技術を使った小型衛星が民間に利用されることもあり、大学と民間の協同において、情報の取り扱いに関するルールの策定が求められると考えている。法令の対応について、大学では所管部署が異なることが多く、難易度が高いものの、今後体制構築が必要なことを実感した。

  ➢ 文科省と議論しながら産学間連携における学の体制構築の負担を減らせるようにしたい。

・ ガイドラインのまとめにあたり、ご尽力いただいたことに感謝したい。ガイドラインの適用について普及活動をどのように行っていくか、また適用範囲の拡大等の課題があることが本 SWG で明らかとなった。皆様と共に検討を進めていければと考えている。

4. 次回予定

・ ガイドライン Ver1.1 について、座長に一任することが全会一致で承認された。

・ また、事務局から、今後のスケジュールについて以下のとおり連絡を行った後、閉会した。

  ➢ 次回の第 7 回会合については、今回の議論を踏まえた検討を行ったのち、事務局から日

程調整を行わせていただく。 以上

4.2.2 宇宙産業 SWG 作業部会コアメンバー会議

本年は、宇宙産業 SWG 作業部会を 1 回、宇宙産業 SWG 作業部会コアメンバー会議を 5 回開催した。なお、2023 年 3 月現在、コアメンバーは、以下の会員によって構成される。

粟津昂規	スカイゲートテクノロジズ株式会社　代表取締役
上杉謙二	PwC コンサルティング合同会社　テクノロジーコンサルティングシニアマネージャー
永島　隆	株式会社アクセルスペース　上席研究員
木下 仁	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　主任研究員
小出　祐輔	株式会社 Synspective　IT セキュリティスペシャリスト
佐々木 弘志	フォーティネットジャパン株式会社 OT ビジネス開発部　部長、IPA 産業サイバーセキュリティセンター専門委員
髙橋　康夫	三井物産セキュアディレクション株式会社　コンサルティングサービス事業本部公共事業部宇宙防衛グループ　プリンシパルアナリスト
田中　洋吏	三菱電機株式会社電子システム事業本部鎌倉製作所　宇宙技術部技術第三課暗号・セキュリティ技術チーム　チームリーダー
濱田　剛	株式会社アークエッジ・スペース、東京大学空間情報科学研究センター特任教授
平松 敏史	株式会社パスコ衛星事業部システム技術部　部長
三好 弘晃	日本電気株式会社社会基盤ビジネスユニット　主席技師長
吉松 健三	技術研究組合制御システムセキュリティセンター(CSSC)

(1) 宇宙産業 SWG 作業部会

1)開催概要

日時:令和 4 年 10 月 31 日(木) 16 時 30 分～18 時 00 分
場所:オンライン開催

議題

1. 開会
2. 宇宙分野のサイバーセキュリティ対策等について
3. ガイドライン Ver1.0 の概要及び今後のアップデートに向けた取組について
4. ガイドライン活用に関するコアメンバーからのプレゼンテーション
5. 自由討議
6. 今後の取組方針について
7. 閉会

配布資料:

資料1　議事次第・配付資料一覧
資料2　委員等名簿
資料3　宇宙分野のサイバーセキュリティ対策等について
資料4－1　ガイドライン Ver 1.0 の概要及び今後のアップデートに向けた取組について
資料4－2　民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.0（概要版）民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.0
資料4－3　民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.0
資料5－1　コアメンバー粟津様からの情報提供
資料5－2　コアメンバー小出様からの情報提供（配布なし・投影のみ）
資料5－3　コアメンバー國母様からの情報提供
資料6　今後の取組方針について

（2）第6回コアメンバー会議

1） 会議概要

日時　令和4年 6 月 7 日（火） 13 時00 分～14 時 00 分

場所　オンライン開催

議題

1. 開会
2. 宇宙 SWG は作業部会名簿の更新について
3. 「民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン」の修正内容について
4. 自由討議
5. 日本版 Space ISAC について
6. 自由討議
7. 閉会

配布資料:

資料1　議事次第・配付資料一覧
資料2　作業部会名簿（更新版）
資料3－1　ガイドラインの修正内容
資料3－2　「民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン」（見消版）
資料3－2　「民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン」（溶込版）
資料4　日本版 Space ISAC について

（3）第7回コアメンバー会議

1） 会議概要

日時　令和4年7月 29日（金） 15時 30 分～18 時30 分

場所　MRI 会議室・オンライン開催

議題

1. 開会
2. 宇宙航空研究開発機構（JAXA）仁尾様からの情報提供
3. ガイドラインのアップデートについて
4. 自由討議
5. 閉会

配布資料:

資料1　議事次第・配付資料一覧
資料2　作業部会コアメンバー名簿
資料3　JAXA 仁尾様からの情報提供（JAXA の宇宙システムセキュリティ標準の概要）
資料4　ガイドラインのアップデートについて
参考資料1 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.0
参考資料2 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.0 概要資料
参考資料3 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.0 概要資料英語版

（4） 第8回コアメンバー会議

1） 会議概要

日時　令和4年 9 月 16 日（金） 17 時 00 分～19 時 00 分

場所 オンライン開催

議題

1. 開会
2. 宇宙航空研究開発機構（JAXA）様標準に対する質疑応答及び経済産業省ガイドラインへのフィードバックについて
3. ガイドラインのアップデートに向けた取組について
4. 閉会

配布資料:

資料1　議事次第・配付資料一覧
資料2　作業部会コアメンバー名簿
資料3－1　JAXA 様標準に対する質疑応答及び経済産業省ガイドラインへのフィードバックについて
資料3－2　JAXA 様標準に対するご質問一覧

資料4　　ガイドラインアップデートに向けた取組について
参考資料1 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.0

（5）第9回コアメンバー会議

1） 会議概要

日時 令和4年 12 月 22 日（木） 16 時 30 分～18 時 00 分

場所 三菱総合研究所 大会議室 B・C

議題

1. 開会
2. 宇宙分野のサイバーセキュリティ対策等に関する動向について
3. ガイドラインのアップデート方針について
4. ガイドラインのアップデートに関する自由討議
5. 宇宙航空研究開発機構（JAXA）仁尾様からの情報提供
6. 宇宙分野の情報共有体制（宇宙 ISAC）構築に向けた取組について
7. 宇宙 ISAC 構築に向けた取組に関する自由討議
8. 閉会

配布資料:

資料1　　議事次第・配付資料一覧
資料2　　作業部会コアメンバー名簿
資料3　　宇宙分野のサイバーセキュリティ対策等に関する動向について
資料4　　ガイドラインのアップデート方針について
資料5　　JAXA 仁尾様からの情報提供
資料6　　宇宙分野の情報共有体制（宇宙 ISAC）構築に向けた取組について

（6）第10 回コアメンバー会議

1） 会議概要

日時 令和5年 2 月 1 日（水） 16 時 30 分～18 時 00 分

場所 オンライン会議

議題

1. 開会
2. 宇宙分野のサイバーセキュリティ対策等に関する動向について
3. ガイドラインのアップデート方針について
4. 自由討議

5. 閉会

配布資料:

資料1　議事次第・配付資料一覧
資料2　作業部会コアメンバー名簿
資料3　宇宙分野のサイバーセキュリティ対策等に関する動向について
資料4　ガイドラインのアップデートについて
参考資料1 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.1(案)【見消版】
参考資料2 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.1(案)【溶込版】
参考資料3 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.1 概要資料(案)
参考資料4 対策要求事項チェックリスト【ガイドライン添付資料1】
参考資料5 NIST Cybersecurity Framework(NIST CSF)と宇宙システム特有の対策との対応関係【ガイドライン添付資料2

4.3 民間宇宙システムにおけるサイバーセキュリティ対策ガイドラインの開発・更新

宇宙分野においても民間企業におけるサイバーセキュリティのリスクが拡大している。また海外でも議論や取り組みが活発化する中、宇宙システム全体の機能保証強化の一環として、民間宇宙システムにおけるサイバーセキュリティ対策ガイドラインを開発することとなった。

図 4.3-1 に示すように、2022 年 7 月に、民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver1.0 が公開された。以降のアップデートの方針について、 Ver 1.0 から Ver 1.1 へのアップデートと、 Ver 1.1 から Ver 2.0 へのアップデートの 2 フェーズに分けて対応することとしている。

今年度は、Ver1.1 へのアップデートを行うにあたり、全体の記載内容を精査し、細かな文言修正を行った。またコアメンバー会議及び作業部会における議論を踏まえ、添付資料を充実化させている。来年度には、より高度な対策や対象範囲の拡大等の検討を含めた Ver2.0 への更新が期待される。

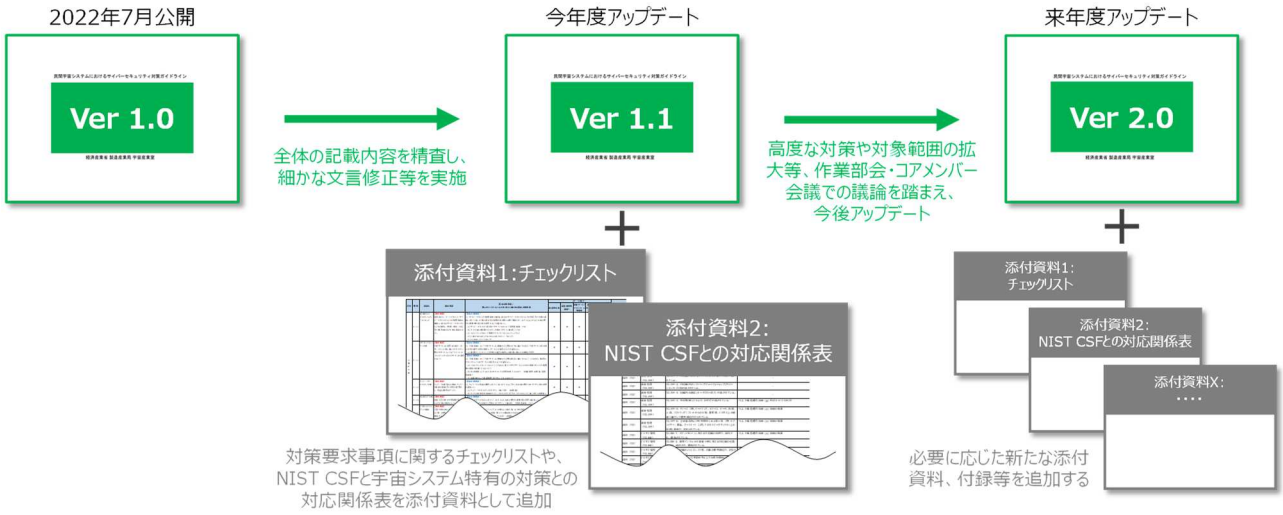


図 4.3-1 民間宇宙システムにおけるサイバーセキュリティ対策ガイドラインアップデート方針

4.3.1 ガイドライン Ver.1.0 策定に向けた作業

2022 年 2 月から 3 月にかけて経済産業省は、「民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン β 版」に対しパブリックコメントを募集した。パブリックコメントを受け、第 5 回、第 6 回コアメンバー会議にて対応方針を検討した。

表 4.3-1 パブリックコメント及びコアメンバー会議で出された主な意見

#	パブリックコメントで寄せられた意見	コアメンバー会議での主な意見
1	・ 本ガイドラインを参照した場合、適用要否が不明瞭である項目には、「適用しない」という選択を行うことは難しく迷った場合には「適用」を選択せざるを得ない。各項目について「必須」または「必須ではない」が明確に判断できるようになると良い。 ・ 複数の基準や枠組みの活用が示唆されているため、何を活用すべきか絞り込むための考え方や優先度を明示してほしい。 ・ 衛星タイプによる必要最低限のセキュリティに係る検証レベルを検討して欲しい。	・ ガイドラインの位置付けとして、必須／推奨はガイドラインの読者が決めるべきであると理解している。コメントにあるように、「迷った場合には『適用』を選択せざるをえない」ということは記載していない。他方、読者にこの意図が十分に伝わっていない懸念があるため、あくまで自主的な対策を促すことを目的としたガイドラインであることを明確化した方が良い。 ・ システムの特性や重要性に応じて、対策をテーラリングして活用いただくようガイドラインの意図を丁寧にかみ砕くことが必要である。 ・ 現状のガイドラインでは、How to Use に当たる部分がない。ガイドラインの活用ユースケースを加えていく方針も一案である。

#	パブリックコメントで寄せられた意見	コアメンバー会議での主な意見
2	・ チェックリストなど要件の明確化や認定制度を検討してほしい。	・ チェックリストを使って、個社の弱点の把握や全体のレベル底上げをすることが重要だが、あえて抜き出してチェックリストを作るのではなく、参考文献として引用するというのが、本ガイドラインの当初の設計指針ではないか。 ・ 要求仕様によって異なるので、チェックリスト自身のレベル感は検討課題ではないか。 ・ 認定制度は現状検討していない。
3	・ 修理・不具合修正や改修用の計算機など事業者が自前で所持する設備について要件を明確化してほしい。	・ 衛星運用設備や開発・製造設備に属さない設備は存在しないのではないか。 ・ 3.2.5 で工場ガイドラインを引用し対応できるのではないか。
4	・ 「セキュアコーディング」が課せられた場合、適用ができないCOTS/OSS が生じることを懸念している。	・ セキュアコーディングは残しておくべきだと思う。ポリシーを作ってインテグレーターに依頼するとしたとき、全面的な記載をガイドラインに含めることは難しく、「セキュアコーディングに配慮すること」等の記載に修正し、実際は実績を踏まえて折り合いをつけることになる。

パブリックコメントとコアメンバーの主な意見は表 4.3-1 に示すとおりである。これらの意見を踏まえ、事務局は主に以下の加筆・修正を行った。

- 本ガイドラインは自主的な対策を促すことを目的としていることを明確に示す。
- 本ガイドラインをテーラリングして良いことを加筆する。
- 工場ガイドラインを引用し、開発製造設備についての対策を言及する。
- セキュアコーディングについて、解説を加筆する。

なお、本ガイドラインの対策要件に準じたチェックリストの作成、本ガイドラインに基づく対策事例集の作成について、パブリックコメント及びコアメンバー会議にて意見が挙げられたが、十分な議論を要すると判断し、Ver1.1 以降で、検討を進めることとなった。

第 5 回宇宙産業 SWG にて、修正案を基に議論を行い、「民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver1.0」及び「概要資料」の正式公開を座長に一任することが全会一致で承認された。これを受け、2022 年 7 月に経済産業省により公表された。

4.3.2 ガイドライン Ver.1.1 策定に向けた作業

ガイドライン Ver1.0 公表以降、作業部会及びコアメンバー会議にて、ガイドライン Ver1.1 更新に向け議論がなされた。ガイドラインの次のステップとして、前述した残課題に加え、どのような対策を検討すべきか、どのような文書を参照すべきかについて、広く意見が挙げられた。

表 4.3-2 ガイドライン Ver1.1 に向けた作業部会及びコアメンバー会議の主な意見とアップデート方針

#	作業部会／コアメンバー会議での主な意見	アップデート内容
1	・ チェックリストに関する要望があった。ガイドラインで記載している対策要件だけを抜き出してチェックリスト化する方法が想定される。 ・ チェックリストにおいては、要求事項の達成度をプルダウンで入力できる形式だと使いやすい。	・ ガイドラインの要求事項や基本対策事項に関する簡易的なチェックリストを作成し、ガイドラインの添付資料として追加した。
2	・ 第 3.2 節で記載されている宇宙システム特有の対策について、その他のガイドラインとの関係性が示されると事業者にとってはありがたい。整理するガイドラインについて、NIST CSF とのマッピングが取られていると大変ありがたい。 ・ NIST のガイドラインは広く活用されているため、使う立場としては NIST CSF を軸に整理していただく方が使いやすい。 ・ NIST CSF を軸に経産省ガイドラインを整理いただいた方が事業者としては、使いやすい。 ・ 全社的観点では、CSF 全体をみており、その中で宇宙の部分はどこに該当するのかを見ていく必要がある。そのため、NIST CSF を軸に整理していただく方が使いやすい。	・ NIST CSF のフレームコアにおける各サブカテゴリと、経産省ガイドラインにおける宇宙システム特有の対策（3.2.2～3.2.5）との対応関係を整理し、ガイドラインの添付資料として追加した。
3	・ チェックリストを使用する際、ガイドラインよりも Excel を見るような形態で使うことが多い。 ・ NIST CSF との整理について、Excel でご提供いただければ、自分で使いやすいように整理をすることができる。	・ 上記の対策要求事項チェックリスト及び NIST CSF 対応関係整理について、Excel 形式にて公開する。

作業部会及びコアメンバー会議の主な意見また、アップデートの方針は表 4.3-2 に示すとおりである。これらの意見を踏まえ、事務局は主に以下の作業を実施した。

- 対策要求事項に関するチェックリストを添付資料として追加する。
- NIST CSF と宇宙システム特有の対策との対応関係表を添付資料として追加する。
- ガイドライン全体を再精査した上で、細かな文言修正を行う。

第 6 回宇宙産業 SWG にて、修正案を基に議論を行い、「民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver1.1」及び「概要資料」の正式公開を座長に一任することが全会一致で承認された。ガイドライン Ver1.1 公表時には、併せて英訳版も公表される予定である。

4.3.3 ガイドラインの今後の更新に向けた論点整理

次年度のコアメンバー会議において、次のステップとして実施すべき高度な対策を議論しつつ、議論

した結果を Ver 1.1 から Ver 2.0 へのアップデートで反映する予定である。

表 4.3-3 ガイドライン Ver2.0 に向けた作業部会及びコアメンバー会議の主な意見とアップデート方針

#	作業部会/コアメンバー会議での主な意見	アップデート方針
1	・ 衛星間や衛星地上間の光通信について、現行のガイドラインではカバーされているわけではなく、一言でも触れられていると良い。 ・ 光通信では鍵の有効期限が早くなるため、鍵のリニューアルを早く行う必要がある。また、衛星軌道上で鍵の生成をする必要もある。	・ 衛星間光通信システムにおける暗号鍵生成や認証に関する対策の具体的な実装手順や留意事項等を整理し、手順書として取りまとめ、ガイドラインの付録や別冊として追加する。
2	・ どのような対策を次のステップとして実装すべきかについて、記載がなされると良い。例えば、暗号の実装について、どの実装であれば許容されるか、すぐに読み取ることは難しく、間違った実装をしないための補足説明があると良い。 ・ 暗号の実装に関する補足説明の要望は理解するが、本ガイドラインのスコープからずれる恐れがあるため、追記するか否か、慎重に議論すべきである。	・ 衛星システムにおける暗号実装に関する補足説明について、本ガイドラインのアップデート対象とするか、検討を行う。
3	・ 小型衛星以外の衛星に対しても本ガイドラインを適用できるのか、また、衛星ごとに求める対策要求事項が異なるのか、議論できると良い。	・ ガイドラインの適用範囲に関して、小型衛星以外の衛星に対する適用可能性を検討するとともに、衛星ごとに求められる対策要求事項を検討する。
4	・ サプライチェーンの中で外部委託する場合や購入品に対して、気を付けるべき事項を整理すると良い。 ・ 衛星運用やアンテナを外部委託するケースがあるため、宇宙特有の議論ができると良い。	・ 宇宙特有のシステムやコンポーネントのサプライチェーン対策として留意すべき内容に関して追記を行う。
5	・ 対策事例集を追加すると、読み手にわかりやすいガイドラインになるのではないか。	・ 本ガイドラインに基づく対策の事例集を取りまとめ、ガイドラインの付録又は別冊として追加する。
6	・ 国内事業者においては、NIST CSF だけでなく、リモセン法ガイドラインとの比較ができると分かりやすい。	・ リモセン法ガイドと経産省ガイドラインとの対応関係を整理し、ガイドラインの付録として追加する。

作業部会及びコアメンバー会議の主な意見また、アップデートの方針は表 4.3-3 に示すとおりである。議論を踏まえ、事務局は、衛星間光通信システムにおける通信方式や暗号の実装方式等のより高度な対策の実装方法について、その追記の必要性も含めて次年度以降検討する予定である。また、ガイドラインの適用範囲に関して、小型衛星以外の適用可能性を議論するほか、宇宙分野特有のサプライチェーンセキュリティ対策に関する検討、リモセン法ガイドラインとの対応関係を整理することが必要と考えられる。さらに、Ver1.0 のパブリックコメントにも意見が挙げられたように、本ガイドラインに基づく対策事例集の作成を検討する意向である。

4.4 ガイドラインの英訳

国際調和等を目指し、策定したガイドラインの英訳を行った。Ver 1.0 のガイドラインについては、概要資料のみの英訳、Ver 1.1 では、概要資料に加えて本編の英訳も行った。

4.5 情報共有・教育訓練のあり方などの検討

宇宙システムのサイバーセキュリティに関する脅威・脆弱性・インシデントなどに関する情報共有、普及啓発、教育訓練のあり方などについて検討を行った。本事業では特に、国内宇宙セキュリティ分野における将来的な情報共有体制のあり方について検討を行った。

4.5.1 米国 Space ISAC の調査

宇宙分野におけるセキュリティに関する情報共有体制として、米国では、Space ISAC（Information Sharing and Analysis Center）が 2019 年に発足している。Space ISAC は脆弱性、インシデント及び脅威に対する準備や対応能力の強化のために世界中の宇宙産業全体の協力を促進し、さらに、メンバー企業間でのタイムリーかつ実用的な情報の共有等を行うための組織であり、2019 年 4 月にコロラド・スプリングスで開催された 35th Space Symposium において設立が発表され、その後、2019 年 11 月、NASA や米宇宙軍（旧空軍宇宙軍団）、米国家偵察局（National Reconnaissance Office）がスポンサーとなり、正式に発足した。Space ISAC による情報共有と分析のエコシステムは図 4.5-1 に示すとおりであり、特にサプライチェーン、ビジネスシステム、宇宙密書に対する脅威について焦点を当てている。

図 4.5-1 Space ISAC による情報共有と分析のエコシステム
（出典：Space ISAC, “Space ISAC Membership” https://s-isac.org/membership/）

表 4.5-1 に示すとおり、Space ISAC の会員企業は宇宙やサイバーセキュリティに関連する企業・大学・機関等によって構成される。このうち、創設メンバーは 14 組織であり、ガバニング・ボードに参加するために年間$75,000 を支払い、Space ISAC は自己資金によって運営されている。なお、Space ISAC は、サイバーセキュリティの啓発を行う非営利団体である National Cybersecurity Center（NCC）[16]によって運営されている。

表 4.5-1 Space ISAC の会員企業一覧（2023 年 3 月 14 日時点）[17]

区分	組織名
宇宙関連企業	● Aerospace Corporation ● Kratos Defense & Security Solutions, Inc. ● L3Harris Technologies, Inc. ● Lockheed Martin Corporation ● Northrop Grumman Corporation ● Parsons Corporation ● SES S.A. ● 14bis Supply Tracking ● Astroscale U.S. Inc. ● Axiom Space Inc. ● The Boeing Company ● Envistacom, LLC ● Innoflight, LLC ● IntelSat S.A.

[16] John Hickenlooper コロラド州知事（当時）の主導によりコロラド大学コロラド・スプリングス校（UCCS）を中心として 2016 年に設立された非営利団体で、サイバーセキュリティに関する教育・訓練プログラムの提供や調査・研究を主に行う。
[17] Space ISAC 公式ページに基づき作成したもので、このほか、国際パートナーメンバー（国内では JAXA）が含まれることに留意。

区分	組織名
	● Intuitive Machines, LLC ● Kongsberg Satellite Services(KSAT) ● Maxar Technologies Inc. ● Peraton ● Planet Labs PBC ● Raytheon Company ● RS21 ● SAIC ● SpaceLink Corporation ● Steely, Inc. ● Synspective Inc. ● System High Corporation
サイバーセキュリティ関連企業	● Booz Allen Hamilton Inc. ● Microsoft Corporation ● MITRE Corporation ● Thinklogical LLC ● Chip Scan Inc. ● Constellation Network Inc. ● Cyber Inflight ● IronNet, Inc. ● NetRise, Inc. ● Proof Labs ● Red Balloon Security ● Sophinea Corporation ● Sentinel Blue ● SolarWinds, Inc. ● Spark Mindset Inc. ● SpiderOak
アカデミア	● Johns Hopkins Applied Physics Laboratory(APL) ● Purdue University ● Space Dynamics Laboratory ● University of Colorado Colorado Springs(UCCS)

※ 下線の組織は創設メンバーを意味する。

（出典：Space ISAC, “Space ISAC Membership”に基づき三菱総合研究所作成）

Space ISAC のメンバーには4つの区分（プラチナ、ゴールド、シルバー及び中小企業（Small Business））が存在する。図 4.5-2 に示すとおり、メンバーの区分によって年会費、Web ポータルへのアカウント数、トレーニングのディスカウント等が異なる。Space ISAC のメンバーとして加入を希望する場合、まずは問合せの上、初会合（introductory meeting）を実施し、その後、応募・審査を経て、メンバーとして参加可能となる。なお、2022 年 2 月 28 日には、Peraton が Space ISAC 初のプラチナメンバーになったことが発表された。

プラチナ	ゴールド	シルバー	中小企業 (Small Business)
● 年間$50,000 ● Webポータルアカウント×15 ● Space ISACサミットパス×5 ● トレーニングコース 無料 ● 重要インフラレポートの入手 ● メンバ調査の実施 ● メンバ名簿へのアクセス ● 分析Working Groupへ参加	● 年間$25,000 ● Webポータルアカウント×5 ● Space ISACサミットパス×2 ● トレーニングコース 50%オフ ● 重要インフラレポートの入手 ● メンバ調査の実施 ● メンバ名簿へのアクセス	● 年間$10,000 ● Webポータルアカウント×1 ● Space ISACサミットパス×1 ● トレーニングコース 25%オフ ● 重要インフラレポートの入手 ● メンバ調査の実施 ● メンバ名簿へのアクセス	● 年間$2,500 ● Webポータルアカウント×1 ● Space ISACサミットパス×1 ● トレーニングコース 25%オフ ● 重要インフラレポートの入手 ● メンバ調査の実施 ● メンバ名簿へのアクセス ※Small Businessは年間の収益が$3M以下の企業に限られる

図 4.5-2 Space ISAC の 4 つのメンバー区分分
（出典：Space ISAC, “Space ISAC Membership”に基づき三菱総合研究所作成）

Space ISACは、参画することで図 4.5-3に示す4つの利点を享受できるとしている。また、2022年 5 月には、コロラド大学コロラド・スプリングス校（UCCS）のキャンパス内に宇宙セキュリティの脅威やインテリジェンスに関する情報共有機能を担う新たな施設を開設し、Space ISAC のメンバーはこれらの情報に物理的又はリモートでアクセス可能となる。加えて、Space ISAC メンバーが商業宇宙システムの脆弱性検証を行える検証ラボを建設中であると発表している。

図 4.5-3 Space ISAC への参画による 4 つの利点
（出典：Space ISAC, “Space ISAC Brochure”に基づき三菱総合研究所作成）

公開されている Space ISAC の具体的な活動について、定期的な Webinar の開催、ニュースレターやホワイトペーパーの発表のほか、Value of Space Summit（VOSS）と呼ばれる年次会合を開催している。そのほか、複数の会議体を構築することで、会員企業での情報共有を促している。会議体の区分として、COI（Communities of Interest）、ワーキンググループ、タスクフォースの 3 つの区分があり、に示すとおり、それぞれにおいて複数の会議体が設置されている。

表 4.5-2 Space ISAC に設置された会議体(2023 年 3 月 14 日時点)[18]

区分	会議体名	会議体の目的
COI (Communities of Interest)	小型衛星 COI	小型衛星のセキュリティ緩和策を特定、分析及び開発すること。
	AI・機械学習 COI	宇宙インフラの開発、配備、運用、保守及び保護のための AI 技術・機械学習技術の論理的な使用を支援する役割を担うこと。
	ブロックチェーン COI	ブロックチェーンの知識及び宇宙分野への応用を学び、さらに理解すること。
	ワークフォース COI	宇宙分野のサイバーセキュリティ・物理セキュリティに関する人材について、中長期的なニーズと関連する教育・訓練のポートフォリオを開発すること。
ワーキンググループ	情報共有ワーキンググループ	Watch Center の活用方針やベストプラクティスを開発すること。
	サプライチェーンリスク管理ワーキンググループ	サプライチェーンを可視化し、信頼できるサプライヤーネットワークを促進するための連携活動を展開すること。
	アナリストワーキンググループ	脅威の情報を定期的に共有すし、脅威や危機的な行動への呼びかけを行うこと。
タスクフォース	SPD-5 タスクフォース	SPD-5 を踏まえ、宇宙コミュニティのためのサイバーセキュリティのベストプラクティスと標準を開発すること。
	机上演習タスクフォース	机上演習(宇宙でのサイバーセキュリティインシデントを想定したシナリオについて、メンバーが集まり、ファシリテーターが中心となって議論する机上でのサイバー演習)に向けたシナリオを作成すること。
	本部タスクフォース	Watch Center や Cyber Vulnerabilities Lab を含む Space ISAC 全体の活動を監督・開発すること。
	Watch Center タスクフォース	宇宙分野に関連するデータ、情報、インテリジェンス、指標及び警告を収集すること。
	CMMC タスクフォース	CMMC レベルへの適合に向けた活動をするとともに、CMMC のプロセスに関する情報を共有すること。
	Space Symposium タスクフォース	毎年開催される Space Symposium のプロモーションを行うほか、関連する情報コンテンツを作成・配布すること。
	Space ISAC Summit タスクフォース	年次会議である Value of Space Summit (VOSS)の議題やセッションの作成を支援すること。

(出典:Space ISAC, "Collaborative Groups"に基づき三菱総合研究所作成)

[18] Space ISAC 公式ページに基づき作成したもので、このほか、国際パートナーメンバー(国内では JAXA)が含まれることに留意。

また、Space ISAC の背景や取組について詳細に把握するために、Space ISAC の Deputy Director である Ms. Mairead Levison に対してヒアリングを行った。

4.5.2 国内における他分野 ISAC の調査

サイバーセキュリティに関する情報共有体制について、国内他分野では ISAC が設立されている。国内の代表的な ISAC の目的・主な機能は表 4.5-3 に示すとおりであり、各 ISAC は、情報の収集・分析・共有の基本的な機能を持ち合わせていることに加え、一部の ISAC では、人材育成の支援、セキュリティの啓発、ガイドライン等の策定、外部組織との連携に係る機能も有している。

表 4.5-3 国内の代表的な ISAC における目的・主な機能

注： 各 ISAC の会則・定款等に基づき整理したものであり、実際の活動と異なる点があることに留意。

名称	目的	運営母体	主な機能					
			情報の収集・分析	情報の共有	人材育成の支援	セキュリティの啓発	ガイドライン等の策定	外部組織との連携
金融 ISAC	● サイバーセキュリティに関する情報の共有・分析及び安全性の向上のための協働活動を行うこと	一般社団法人 金融 ISAC	✔	✔		✔		
医療 ISAC	● 情報セキュリティの重要性を啓発すること ● 情報セキュリティに関連する問題を解決すること	一般社団法人 医療 ISAC	✔	✔			✔	✔

名称	目的	運営母体	主な機能					
			情報の収集・分析	情報の共有	人材育成の支援	セキュリティの啓発	ガイドライン等の策定	外部組織との連携
ICT-ISAC	● 幅広い相互連携を図り、安定した情報流通、情報伝達を維持すること ● サイバー攻撃に対処する社員である電気通信事業者を支援すること	一般社団法人 ICT-ISAC	✔	✔	✔	✔	✔	✔
電力 ISAC	● 会員間で信頼と互助の精神に基づきサイバーセキュリティに関する情報等を交換や分析すること	電気事業連合会	✔	✔				✔
交通 ISAC	● サイバーセキュリティに関する会員相互間の広範な連携・協力を行うこと	一般社団法人 交通 ISAC	✔	✔		✔		
J-Auto-ISAC	● サイバーセキュリティリスクの情報共有・分析およびサイバーセキュリティ対応能力の強化を推進すること	一般社団法人 Japan Automotive ISAC[19]	✔	✔	✔		✔	✔
ソフトウェア ISAC	● サイバーセキュリティに関連する情報整備や連携を行うこと	一般社団法人 ソフトウェア協会	✔	✔	✔	✔	✔	✔

[19] 日本自動車工業会と日本自動車部品工業会を中心として運営されている。

名称	目的	運営母体	主な機能					
			情報の収集・分析	情報の共有	人材育成の支援	セキュリティの啓発	ガイドライン等の策定	外部組織との連携
日本貿易会 ISAC	● インシデント情報の入手ならびに共有、相互の対応協議を行うこと ● 日本貿易会の会員商社におけるサイバーセキュリティ対策をサポートすること	一般社団法人日本貿易会	✔	✔	✔			

（出典：各 ISAC の会則・定款等の公開情報に基づき三菱総合研究所作成）

国内宇宙分野における情報共有体制の構築に向けた検討にあたって、ISAC に関する有識者にヒアリングを行った。具体的には金融 ISAC 専務理事の鎌田 敬介氏とフォーティネットジャパン合同会社 OT ビジネス開発部長の佐々木 弘志氏に対し、主に以下の項目に関して意見を伺った。

- 情報共有体制構築の背景
- 情報共有規模の拡大に向けた取組
- 活発な情報共有を促す仕組み

4.5.3 宇宙産業分野における情報共有体制構築に向けた検討

これまで記載のとおり、サイバーセキュリティに関する情報共有体制について、米国では Space ISAC が 2019 年に発足し、宇宙分野における情報共有体制が構築されているほか、国内においても、複数の産業分野ではすでに ISAC が設立されている。国内宇宙分野における情報共有体制の構築について、コアメンバー会議にて議論を行ったところ、以下のような意見が主に挙げられた。

- いきなり情報共有体制の設立を目指すことは敷居が高い。まずは、定期的な勉強会の開催や対面での打ち合わせ等の取組から始め、信頼関係を醸成することが重要である。
- 情報共有体制を構築することで、セキュリティ業界と宇宙業界の両方における情報共有の活性化が期待される。まずは協議会を立ち上げ、定期的に勉強会を開催したり対面での打ち合わせを設けたりといった取組から始めるのが良いと思われる。
- ベンチャー企業も含めた各民間宇宙企業の情報共有・分析に関するニーズをヒアリングすることから始めても良いのではないか。
- 信頼関係を醸成する中で、各社のニーズを掘り起こしていく必要がある。信頼関係が構築され

れば、情報も出しやすくなる。

- 情報共有を行う上では、そこに参加している社のニーズが一致していることが重要となる。
- コアメンバー会議には様々な立場の事業者が参画しているため、まず各社のニーズを整理する必要がある。
- サイバーセキュリティに関する情報の共有だけではなく、各社が抱えている悩みや課題を共有する役割もあるのではないか。
- 情報共有体制の構築を前提とした議論ではなく、必要性の議論も必要であろう。

これらの意見の踏まえ、国内宇宙分野における情報共有体制の構築に向け、まず「信頼関係の醸成」の重要性に着目し、前述のとおり、一部のコアメンバー会議は対面を含む会議形式とするなど、まずはコアメンバー間での信頼関係醸成に向けた取組を行った。

この取組と並行しつつ、既存の ISAC に関する机上調査やヒアリングを踏まえ、情報共有体制構築に向けた成熟度モデルを作成するとともに、本モデルに基づき、国内宇宙分野の情報共有体制構築に向けたプロセス案を整理した。作成した成熟度モデルを図 4.5-4 に示す。この図に示されるとおり、情報共有体制の成熟度は大きく 4 つのフェーズに分類される。フェーズ 0 の萌芽期では、正式な情報共有体制でないものの、限定した関係者間で信頼関係を醸成し、情報共有を一部実施する。フェーズ 1 の設立期以降、体制を組織化し、複数組織間での相互の情報共有を実施する。フェーズ 2 の成長期では、情報共有に加え、情報分析活動を一部実施するとともに、他の組織と連携することが期待され、最終的には、フェーズ 3 の自律期として、会員企業の会費に基づく自律的な組織運営を行うことが期待される。

	フェーズ0:萌芽期	フェーズ1:設立期	フェーズ2:成長期	フェーズ3:自律期
状態	**限定した関係者間で信頼関係を醸成し、情報共有を一部実施する**	**情報共有体制を組織化し、複数組織間での相互の情報共有を実施する**	**情報共有に加え、情報分析活動を一部実施するとともに、他の組織と連携する**	**会員企業の会費に基づく自律的な組織運営を行う**
詳細	• 限定した関係者間で、情報共有コミュニティの必要性を認識しつつ、信頼関係の醸成を図る。 • 情報共有に積極的なキープレイヤーが小さなコミュニテイを形成し、情報の共有を行う。 (初期はキープレイヤーからの情報提供が中心。)	• 限定した関係者から参加者を広げ情報共有体制を組織化し、ビジョン・ミッション、事業内容、情報共有ルールの策定等を行う。 • 策定したルールに基づき、組織間での相互の情報共有を実施する。	• 加入する組織が増加し、相互の情報共有がより活発化する。 • 情報共有の仕組みを評価・改善する。 • 脅威情報の分析を行い、分析結果を会員企業に共有する。 • 海外の関係組織や他分野ISACとの連携を行う。	• 業界内の多くの事業者が参加し、会員企業の会費に基づき、自律的な組織運営を行う。 • 多数のWG活動やサイバー演習の実施など、情報共有・分析の枠組みにとらわれない活動を実施する。
求められる取組例	• 勉強会や懇親会など顔が見えるネットワークの構築を行う。 • キープレイヤーを中心に、当該分野のセキュリティに関する情報の共有を始める。 • 将来的な情報共有体制構築に向け、必要な事項を整理する。	• 情報共有体制のビジョン・ミッション、事業内容、情報共有ルール等を策定する。 • 情報共有の仕組みを明確化し、相互の情報共有を促す。 • 会員区分や料金体系を整備する。 • 参加者拡大に向けた広報活動を行う。	• 会員数の増加に応じて、情報共有の仕組みを評価・改善する。 • 組織内での脅威情報の分析体制を構築する。 • 組織のセキュリティやコンプライアンスの確保を目的に、ルールの追加整備や見直しを行う。 • 海外の関係組織との連携を図るため、MOUを締結する。	• 会員数や組織規模の拡大に応じて、必要な場合には、資金メカニズムの見直しを行う。 • 会員のニーズを踏まえ、情報共有・分析の枠組みに囚われない活動を行う。（WG活動、サイバー演習、検証環境の整備など）

国内宇宙分野の現状

図 4.5-4 情報共有体制の成熟度モデル

成熟度モデルに記載のとおり、国内宇宙分野の現状はフェーズ 0 の萌芽期であり、情報共有体制の組織化に先立ち限定した関係者間での信頼関係醸成や情報共有の一部実施が必要となる。国内外の既存 ISAC の構築事例を参考にすると、フェーズ 0 における情報共有体制構築に向けた体制は、図

4.5-5 に示すように①民間企業主導による構築、②政府機関主導による構築、③業界団体主導による構築の 3 つの類型に分類される。それぞれにおいて構築のプロセスは異なるが、共通する点として、どの類型においても、初期段階から積極的な情報発信を行うキープレイヤーの存在が重要となる。そのため、国内宇宙分野における情報共有体制構築にあたっても、キープレイヤーが初期段階から積極的な情報発信を行うことが重要となる。

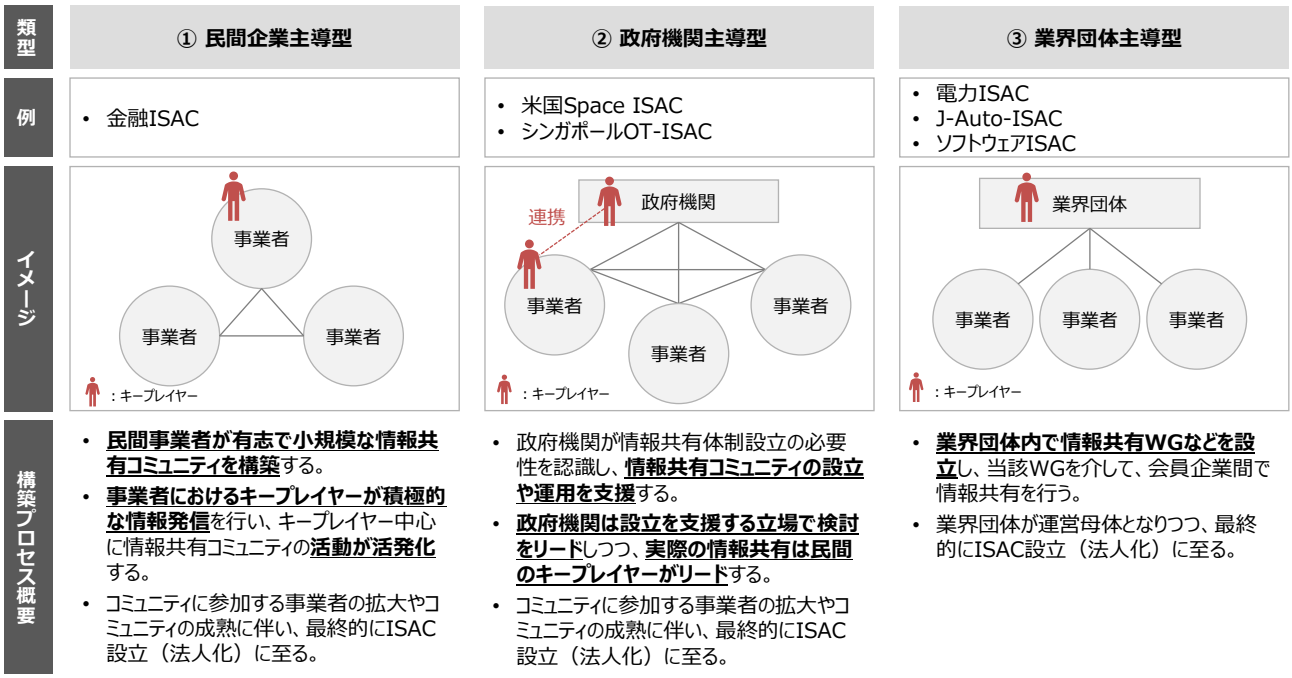


図 4.5-5 フェーズ 0：萌芽期における体制の類型

前述した成熟度モデルに基づく、国内宇宙分野の情報共有体制構築に向けたプロセス案は図 4.5-6 に示すとおりである。フェーズ 0 としては、キープレイヤーを中心に、宇宙分野のセキュリティに関する情報共有を実施するとともに、勉強会や懇親会など顔が見えるネットワークの構築を行い、信頼関係を醸成することが必要と考えられる。共有する情報について、コアメンバー会議で意見が挙げられたとおり、宇宙関係企業各社における情報共有ニーズの深掘りを行うことが望まれる。また、将来的なフェーズ 1 への移行に向け、関係者間で必要な事項を整理することが望まれる。

		フェーズ0:萌芽期	フェーズ1:設立期	フェーズ2:成長期	フェーズ3:自律期
事業運営	情報共有	• キープレイヤーを中心に、宇宙分野のセキュリティに関する情報を共有する。	• 策定した情報共有ルールに基づき、組織間での相互の情報共有を実施する。	• 効率的な情報共有のためにプラットフォームを導入する。 • 必要に応じて、共有された情報のサマリーを作成する。	• フェーズ2から継続した情報共有を行う。
	情報分析			• 宇宙分野に関する脅威情報を分析し、会員企業の分析結果を共有する。	• フェーズ2から継続した情報分析を行う。
	その他	• 勉強会や懇親会など顔が見えるネットワークの構築を行い、信頼関係を醸成する。	• 定例会議、勉強会や懇親会など、顔が見えるネットワークの構築・強化を行う。	• 会員のニーズを踏まえ、WG活動やサイバー演習等の活動を実施する。	• 会員のニーズを踏まえ、複数WG活動、サイバー演習、検証環境の整備等の取組を行う。
組織運営	関係者の拡大	• 関係者間で、将来的な情報共有構築に向けて必要な事項を整理する。	• 初期の関係者以外の組織の参画に向けた広報活動を行う。必要に応じて、経産省から参加を促す。	• Space ISACとMOUを締結し、海外との連携を始める。 • 宇宙SWG関係者以外の組織の参画を促す。	• 宇宙分野への参画に際して、宇宙ISACへの参画を促す。必要に応じて、経産省から参加を促す。
	仕組み構築		• 情報共有のビジョン・ミッション、事業内容、情報共有ルール（TLP）等を策定する。 • 会員区分や料金体系を整備する。	• 組織のセキュリティやコンプライアンスの確保を目的に、ルールの追加整備や見直しを行う。 • 必要に応じて、会員区分や料金体系を見直し、新規参画がしやすい仕組みを構築する。	• 会員数や組織規模の拡大に応じて、必要な場合には、資金メカニズムの見直しを行う。

図 4.5-6 国内宇宙分野の情報共有体制構築に向けたプロセス案

5. 総括

本調査では、工場システム、ビルシステム、宇宙システムの各分野において、サイバーセキュリティの確保とその対策向上のための各種調査やガイドライン等の策定を実施した。特に工場及び宇宙においては、サイバーセキュリティ対策についての初のガイドラインを取りまとめ、公表するまでに至っている。またビルにおいては、2019 年に既に経済産業省において策定・公表しているビルシステムに共通する部分についてのガイドラインに加えて、個別設備の1つとして空調設備向けのガイドラインを公表するとともに、既存ガイドラインにおいてこれまで不足していたインシデントレスポンスの対策要件を新たに追加するなど、より高度な取組を進めるものとなっている。

これからは、これらのガイドラインが広く関連産業において活用され、サイバーセキュリティの確保や取組レベルの向上に寄与することが期待されるが、本調査を通して更なる課題も明らかになってきている。

工場においては、製造物の種類によってさまざまなタイプの工場システムが存在するため、さらに分野別の対策について検討を進める必要がある。また、スマート工場化の進展に伴い、従来とは全く異なる部分、全く異なるレベルにおいてサイバーセキュリティが課題となると考えられており、スマート工場を対象とした対策立案も喫緊の課題である。

ビルにおいては、監視カメラ、入退館セキュリティ、受配電設備、エレベータ、空調設備など、個別設備単位での基準やガイドライン類も整備されつつあり、サイバーセキュリティ対策を進めるための参照情報は整いつつある。今後は取組を業界全体にどのように広げていくかが課題である。

宇宙においては、ロケット、衛星、衛星利用システム等の民間開放が進む中で、拡大する市場に混乱を及ぼさないよう、如何に初期段階からサイバーセキュリティを組み込んでいくように誘導していくかが課題となっている。ガイドラインの普及活動が重要である一方、先行する欧米との国際的なハーモナイゼーションも意識した形で、業界を巻き込んだ体制づくりが急務である。

サイバーセキュリティの世界は、対策が進んでもまた一歩先を行く攻撃手法が新たに登場するなど、ゴールの見えない世界である。今回の各分野向けのガイドライン策定を契機に、各業界、事業者において、可能なところから対策を進めていくとともに、対策の高度化と展開については、さらに検討を進めていくことが重要である。

令和4年度サプライチェーン・サイバーセキュリティ対策促進事業
（産業分野別のセキュリティガイドライン等の整備） 報告書

2023 年 3 月

株式会社三菱総合研究所
デジタル・イノベーション本部
TEL (03)6858-3637

（様式２）

二次利用未承諾リスト

令和４年度サプライチェーン・サイバーセキュリティ対策促進事業（産業分野別のセキュリティガイドライン等の整備）報告書

令和４年度サプライチェーン・サイバーセキュリティ対策促進事業（産業分野別のセキュリティガイドライン等の整備）

株式会社三菱総合研究所

頁	図表番号	タイトル
46	図2.1-51	実装モデルごとの対策の概要
47	図2.1-52	今すぐ実践できる工場セキュリティハンドブック リスクアセスメント編の概要
48	図2.1-54	セキュアなICSクラウド導入指南書の概要
48	図2.1-55	セキュリティ対策までの具体的なステップ
50	図2.1-56	OTセキュリティアセスメントサービスの概要
50	図2.1-57	TXOne Networksのトータルソリューションの具体事例
51	図2.1-58	Nozomi Networks for OT/IoTのサービスイメージ
68	図3.1-2	インシデント対応のフロー
84	図3.1-17	シーメンスPXC4.E16コントローラ
85	図3.1-18	Aiphone　GT-DMB-N、GT-DMB-LVN、GT-DB-VN
86	図3.1-19	簡易型河川監視カメラの画像配信が停止中の「川の防災情報」サイト
88	図	組織体制
90	表	会費一覧
91	図	ICT-ISACの会員構成のスコープ
91	図	ICT-ISACの会員構成
94	図	活動費の状況
95	図	組織体制
96	表	2019年度～2020年度の主な活動内容
97	図	組織体制図
101	図	医療ISACの全体構造
102	図	会員種別
103	表	セミナーやワークショップの開催状況
104	表	医療ISACサイバーセキュリティサービス
105	図	医療ISAC認証サービス
105	表	公表資料や提言
106	表	分科会報告
106	表	活動費の状況
124	図4.1-3	NISTIR 8401のスコープ及びプロファイルの活用イメージ
127	図4.1-7	IT-Grundschutz-Profil für Weltrauminfrastrukturenの概要

（様式２）