経済産業省　御中

令和7年度産業サイバーセキュリティ対策の強化に向けた環境整備事業
（ソフトウェアのセキュリティ確保等に関する調査）

報告書

三菱総合研究所

安全保障政策本部

2026 年 3 月 31 日

目次

図 目次

図はありません。

表 目次

表はありません。

1. はじめに

1.1 調査背景・目的

あらゆる分野でデジタル化が進展し、従来は内部に閉じていた工場現場や、宇宙といった新興分野において、利便性の向上や業務の効率化などを目的として機器がネットワークに繋がるなど、ITとOTが繋がる社会となった。一方で、こうしたネットワーク化の進展は、サイバー攻撃の起点の増加、攻撃による被害の広範化につながるため、ITや、ITとOTを結ぶIoT、OTで、サイバーセキュリティ対策の重要性が増大している。

ITにおいては、近年、オープンソースソフトウェア（以下、「OSS」という。）の利用が一般化する中で、自社製品において利用するソフトウェアであっても、コンポーネントとしてどのようなソフトウェアが含まれているのかを把握することが困難な状況が生じており、脆弱性の管理を事業者単独で実施することは費用対効果の面から困難である。このような状況から、米国を中心として、各国でソフトウェアの成分構成を表すSoftware Bill of Materials（以下、「SBOM」という。）に係る取組が進められる中、経済産業省では、「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース（以下、「ソフトウェアタスクフォース」という。）」を2019年9月に設置し、SBOMも含めたソフトウェア管理手法等に関して幅広い議論を行っているが、ソフトウェア分野における業界構造や商習慣が異なる我が国においては、総論としてSBOMの有用性は理解されているものの、実際の活用に向けては様々なハードルが見えてきている。さらに、2023年にはソフトウェアセキュリティに関するQUAD共同原則が定められおり、政府調達ソフトウェアのセキュリティ確保に向け、ソフトウェアの安全な開発・調達・運用に関する方針が示されている。安全なソフトウェア開発に関して、4つの実践（NIST SP800－218の4つ分類に相当）に基づく安全なソフトウェア開発手法の実践を政府方針に取り入れること、ベンダーに対して同手法の実践を推奨することを目指している。

IoTにおいては、その数が急速に増加している中、IoT製品の脆弱性を狙ったサイバー脅威も増加傾向にあるところ、諸外国においてIoT製品に対する認証制度が開始されており、我が国においても令和6年度にJC－STAR（セキュリティ要件適合評価及びラベリング制度）を立ち上げ、一部運用を開始しており、当該制度の普及促進について、各業界団体とも議論しながら進めていく必要がある。

OTにおいては、諸外国との取組として重要インフラ分野も含めた制御システムに関し、日本企業の多くが事業を展開しているインド太平洋地域を含めた各国と連携し、情報収集や政策検討、能力開発を行う演習を実施している。

本事業では、検討会での議論や国内外のITセキュリティに関する文献等の調査を踏まえ、ソフトウェアの安全な利活用に向けて、必要な調査や手法の検討を行い、ITのサイバーセキュリティ対策を推進するとともに、産業分野別（工場、宇宙）のサイバーセキュリティ対策の検討やIoT製品に対するJC－STARの普及促進、産業制御システムに関してインド太平洋地域の関係者を交えたハンズオン演習・議論等を通して、IoT・OTのサイバーセキュリティ対策を推進することを目的として実施した。

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. ソフトウェアの安全な利活用に向けた調査・実証
   (1) SBOMの利活用における調査・普及啓発
   (2) ソフトウェア開発手法の実践に向けた調査・実証
      ① 安全なソフトウェア開発手法の実践における効果、課題・対応策等の調査・整理
      ② 安全なソフトウェア開発手法の実践に向けた実証事業の実施
      ③ 調査結果の取りまとめ
   (3) ソフトウェアタスクフォースの運営
   (4) 英訳
2. 宇宙SWG関連
   (1) 検討会の運営
   (2) 民間宇宙事業者におけるサイバーセキュリティ対策に関する課題等の調査・分析並びにそれらを踏まえた官民の対応の検討
3. 工場SWG関連
4. JC－STAR活用も含めたIoT製品セキュリティ向上
   (1) 工場関連IoT製品のJC－STAR活用検討
      ① 工場関連IoT製品におけるJC－STAR活用方針及びセキュリティ要件の検討
      ② 工場関連IoT製品におけるJC－STAR活用検討WG(仮)の運営
   (2)「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」の改定
   (3) IoTセキュリティ評価関連制度に関する海外動向調査
5. インド太平洋地域向け日米EU産業制御システムサイバーセキュリティ関連
   (1) インド太平洋地域向け日米EU産業制御システムサイバーセキュリティ・ウィークの開催

1.3 報告書の構成

1.2 に示す各項目が揃うことでIT・IoT・OTのサイバーセキュリティを包括的に俯瞰することが可能であると考えられる。

一方で、各項目単体で見ると、目的や対象範囲、適用技術等は、それぞれ独立性が高い性質も持つと考えられるため、報告書は以下に示すように項目単位の編構成とした。

第 1 編 ソフトウェアの安全な利活用に向けた調査・実証
第 2 編 宇宙 SWG 関連
第 3 編 工場 SWG 関連
第 4 編 JC－STAR活用も含めたIoT製品セキュリティ向上
第 5 編 インド太平洋地域向け日米EU産業制御システムサイバーセキュリティ関連

2. 総括

ソフトウェアの安全な利活用に向けた調査・実証においては、我が国の企業やサプライチェーンにおける安全なソフトウェア開発手法（SP 800-218： Secure Software Development Framework）の実践に向け、調査・整理及び実証事業を実施し、我が国における安全なソフトウェア開発手法の実践に際する対応策等の導入ガイダンスについて取りまとめた。加えて、これらの調査・実証及び検討に関連して、専門的な視点からの検討、分析及び助言を得るために、「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース（ソフトウェアタスクフォース）」の運営を支援したほか、本年度作成した SSDF 導入ガイダンス（案）の英訳を行った。

宇宙 SWG 関連においては、産業サイバーセキュリティ研究会 WG1 傘下の宇宙産業 SWG を開催したほか、民間宇宙事業者におけるサイバーセキュリティ対策に関する課題等の調査・分析・整理を実施した。具体的には、国内外の宇宙セキュリティに関する取組や政策の動向、インシデント等について調査した。また今年度は、毎月の調査結果を月報という形で宇宙産業 SWG 関係者に共有し、即時性の高い情報共有を実施した。

工場 SWG 関連においては、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推進のため、産業サイバーセキュリティ研究会WG1傘下の工場SWGにおいて、工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインや、工場のスマート化を進める上での対策ポイントをまとめた別冊などを作成してきたことを踏まえ、これらガイドラインの効果的な普及・啓発を行うことを目的として、サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）と連携して、工場セキュリティガイドラインを含めた工場におけるセキュリティの普及・啓発を実施した。

JC－STAR活用も含めたIoT製品セキュリティ向上関連においては、近年急速に高まっている IoT 製品の脆弱性を狙ったサイバー攻撃の脅威に対応するために開始された IoT 製品に対するセキュリティ要件適合評価及びラベリング制度である JC-STAR に関し、IoT 製品の活用が進む領域の1つとして、工場システム構成製品におけるJC－STAR活用検討を実施した。また、「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」について、JC-STAR ラベル取得に当たって参考となる情報を追加するための改定に向けた検討、JC-STAR と海外のIoTセキュリティ評価認証制度との調和を進めるための海外動向調査を実施した。

インド太平洋地域向け日米EU産業制御システムサイバーセキュリティ関連においては、インド太平洋地域の各国の重要インフラ事業者、製造業者、ナショナル CSIRT における OT・IT のサイバーセキュリティ担当者や、関連する政府機関における政策担当者等 65 名を招聘し、日米 EU 各国のサイバーセキュリティ政策の動向、産業制御システムにおける重要インフラ企業等のセキュリティ対策、サプライチェーンリスク・マネジメント等について、日 EU の政府高官や企業の実務者等によるセミナーを実施した。また、各業界特有のリスクや事例等を盛り込んだ仮想企業のシナリオを用いた業界別ワークショップや、IPA ICSCoE による産業制御分野における AI を活用したサイバー攻撃に対するハンズオン演習を実施したほか、新規のプログラムとして欧州連合サイバーセキュリティ機関（ENISA）によるワークショップを実施した。インド太平洋地域及び欧米と国際的な議論を行うことで、諸外国の産業制御システム分野におけるセキュリティ政策について情報収集を行うとともに、ネットワーク構築を図り、我が国セキュリティ政策との国際調和とサプライチェーン全体の強靭化を図った。インド太平洋地域は我が国にとって、地政学的にも重要な地域であり、このような地域に最新のサイバーセキュリティ対策を備えた有

志国を拡大していくことに貢献した。

　このように、本調査では、5 つのテーマに関する調査を通じ、IT・IoT・OTの各領域に渡るサイバーセキュリティ対策の推進を実施した。

令和7年度産業サイバーセキュリティ対策の強化に向けた環境整備事業

（ソフトウェアのセキュリティ確保等に関する調査） 報告書

全体概要

2026 年 3 月

株式会社三菱総合研究所
安全保障政策本部
TEL (03)6858-3578

経済産業省　御中

令和7年度産業サイバーセキュリティ対策の強化に向けた環境整備事業
（ソフトウェアのセキュリティ確保等に関する調査）

報告書 - 第１編

ソフトウェアの安全な利活用に向けた調査・実証

三菱総合研究所

安全保障政策本部

2026 年 3 月 31 日

目次

図 目次

表 目次

1. はじめに

本事業では、我が国の企業やサプライチェーンにおける安全なソフトウェア開発手法（SP 800-218：Secure Software Development Framework）の実践に向け、調査・整理及び実証事業を実施し、我が国における安全なソフトウェア開発手法の実践に際する対応策等の導入ガイダンスについて取りまとめた。加えて、これらの調査・実証及び検討に関連して、専門的な視点からの検討、分析及び助言を得るために、「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース（ソフトウェアタスクフォース）」の運営を支援したほか、本年度作成した SSDF 導入ガイダンス（案）の英訳を行った。

2. ソフトウェア・セキュリティに関する動向調査（SBOMの利活用における調査）

本章では、企業やサプライチェーンにおけるソフトウェア・セキュリティに関する動向の調査結果を示す。

2.1 調査対象の全体像

本調査は、本年度の目的である SBOM の普及への課題や効果の検討を目的として、経済産業省との議論を踏まえて、ソフトウェア・セキュリティに関する動向調査を以下の 3 つの観点で実施した。

（1）SBOM

国内外の SBOM に焦点をあてた取組の動向

（2）ソフトウェア・セキュリティ

SBOM 以外のソフトウェア・セキュリティに関する動向

（3）AI セキュリティ

AI を活用したソフトウェア開発におけるセキュリティに関する動向

上記のとおり、本年度の目的に沿って SBOM の動向に加えて、米国の NIST が公表している”NIST SP800-218 Secure Software Development Framework”（SSDF）を含めたソフトウェア・セキュリティ全般の動向を調査した。また、AI セキュリティについては、の通りに整理した。今回の調査では、AI を活用したソフトウェア開発におけるセキュリティ（Security for AI Dev&Ops）に関する動向を調査した。

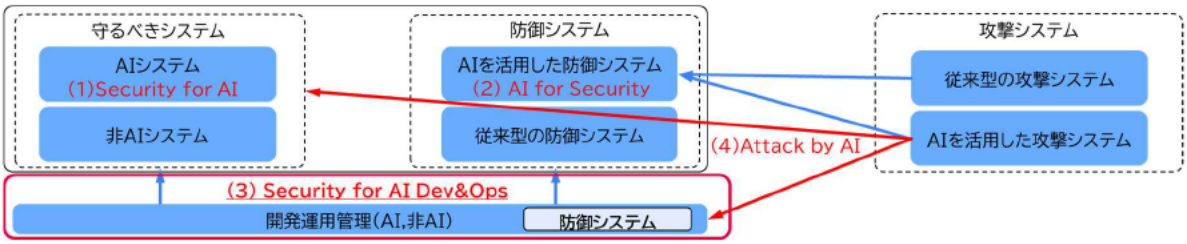


図 2-1 AI セキュリティの考え方

表 2-1 AI セキュリティの類型

類型	対象システム	対策主体	概要	課題	現在の取組例
(1) Security for AI	守るべきシステム（AI システム）	開発者	AI 自体の脆弱性の解消	AI 専門家とセキュリティ専門家の協力による高度な技術が必要	JST K Program AI セキュリティ技術の確立
		利用者	AI 利用者のリテラシー向上	新たな脅威への継続的な対策が必要	AI 事業者ガイドライン別添 AI 利用者向け

類型	対象システム	対策主体	概要	課題	現在の取組例
(2) AI for Security	防御システム	開発者	AI を用いた攻撃検知・防御技術の開発（AI 異常検知）	従来の延長線上の研究開発で継続的な取組みが必要	NEDO K Program 先進的サイバー防御機能・分析能力強化
(3) Security for AI Dev&Ops	開発運用管理システム	開発者	AI コーディング、テスト等の AI 駆動開発で生じるリスクの低減管理	新たな課題であり、入力情報漏洩、データ汚染など AI 駆動開発に固有のリスクがあり、十分に対応したガイドラインが整備されていない	独仏 AI Coding Assistants
	AI システム	開発者	AI プロダクト評価	AI プロダクトを評価できる具体的な基準がない	NIST SP800-218A（SSDF AI Profile）
(4) Attack by AI	攻撃システム	開発者、利用者	AI を活用した攻撃、AI システムへの新たな攻撃	AI を用いた攻撃による新たな脅威への対応や AI システムに対する新たな攻撃手法の整理	総務省 AI セキュリティ分科会

本調査の対象となった候補の文献を取りまとめた。経済産業省と議論の上で、調査対象を絞り、深堀調査を行った。次節以降に深堀調査した内容を示す。

2.2 SBOM に関する動向調査

SBOM に関する動向として調査した内容は下表に示す通りである。以降は各取り組みの概要を示す。

表 2-2 SBOM に関する動向調査の対象一覧

#	取組名・文書名	取組年月	国・地域	取組主体
1	2025 Minimum Elements for a Software Bill of Materials (SBOM)[1]	2025 年 8 月発表	米国	CISA（サイバーセキュリティ・インフラセキュリティ庁）
2	A Shared Vision of Software Bill of Materials (SBOM) for Cybersecurity[2]	2025 年 9 月発表	米国	CISA

[1] CISA, 2025 Minimum Elements for a Software Bill of Materials (SBOM), https://www.cisa.gov/resources-tools/resources/2025-minimum-elements-software-bill-materials-sbom

[2] CISA, A Shared Vision of Software Bill of Materials (SBOM) for Cybersecurity https://www.cisa.gov/resources-tools/resources/shared-vision-software-bill-materials-sbom-cybersecurity

#	取組名・文書名	取組年月	国・地域	取組主体
3	Survey on SBOM State of the Art[3]	2025 年 11 月発表	欧州	ENISA（欧州ネットワーク・情報セキュリティ機関）
4	SBOM LANDSCAPE ANALYSIS[4]	2025 年 12 月開催	欧州	ENISA

（1）2025 Minimum Elements for a Software Bill of Materials（SBOM）

2025 年 8 月、CISA は SBOM の最小要素を更新した。2021 年に NTIA（National Telecommunications and Information Administration）が公開した SBOM の最小要素から、SBOM の機能拡張や実装機会の拡大を踏まえて、今回の更新が行われた。SBOM の「最小要素」には、「データフィールド」、「自動化サポート」、「プラクティスとプロセス」の 3 つのカテゴリが含まれ、コンポーネントを一覧化した部品表に含まれる情報だけでなく、SBOM の利活用者が実施すべき事項も規定されている。SaaS の頻繁な更新による SBOM 共有頻度の増加、AI が組み込まれたソフトウェアにおける最小要素の uncover 具合、SBOM 情報の完全性確保、VEX や CSAF といったセキュリティアドバイザリの利用が今後の課題として挙げられている。

表 2-3 2021 2021 年からの更新概要

カテゴリ	概要	2021 NTIA 最小要素	2025 における更新
データフィールド	各コンポーネントに関する基本情報を明確化すること	以下の情報を SBOM に含めること。 ・サプライヤー名 ・コンポーネント名 ・コンポーネントのバージョン ・その他の一意な識別子 ・依存関係 ・SBOM の作成者 ・タイムスタンプ	以下の情報に更新が行われた。 ・重要な更新：SBOM の作成者、サプライヤー名、コンポーネントのバージョン、その他の一意な識別子、依存関係 ・軽微な更新：コンポーネント名、タイムスタンプ ・新規追加：コンポーネントのハッシュ、ライセンス、ツール名、生成コンテキスト

[3] European Commission, “Survey on SBOM State of the Art”（閲覧日：2025 年 12 月 9 日）, https://ec.europa.eu/eusurvey/runner/enisa-sbom-study2025
[4] ENISA, SBOM Landscape Analysis: Towards an Implementation Guide, https://www.enisa.europa.eu/sites/default/files/2025-12/SBOM%20Analysis%20-%20Towards%20an%20Implementation%20Guide_v1.20-Published.pdf

カテゴリ	概要	2021 NTIA 最小要素	2025 における更新
自動化サポート	SBOM の自動生成や可読性等の自動化をサポートすること	SBOM データは機械判読可能かつ相互運用可能なフォーマットを用いて作成され、共有されること。現状では、国際的な議論を通じて策定された、SPDX、CycloneDX、SWID タグを用いること。	データフォーマットのリストから SWID タグが削除された。
プラクティスとプロセス	SBOM の要求、生成、利用に関する運用方法を定義すること	SBOM を利活用する組織は、以下の項目に関する運用方法を定めること。 ・ SBOM の作成頻度 ・ SBOM の深さ ・ 既知の未知数 ・ SBOM の共有 ・ アクセス管理 ・ 誤りの許容	以下の情報に更新が行われた。 ・ 重要な更新：SBOM の深さ、既知の未知、誤りの許容 ・ 軽微な更新：SBOM の作成頻度、SBOM の共有 ・ 削除：アクセス管理

（2）A Shared Vision of Software Bill of Materials（SBOM）for Cybersecurity

2025 年 9 月、ソフトウェアセキュリティ確保における SBOM の価値を示すことを目的に、米国の CISA より”A Shared Vision of Software Bill of Materials（SBOM）for Cybersecurity”が公表された。本文書は、計 15 か国が共同署名しており、日本においては経済産業省と内閣官房国家サイバー統括室が参画している。本文書は、SBOM の価値を広く普及させるための文書であり、SBOM の説明から始まり、SBOM 導入のメリット・活用すべきステークホルダー・セキュアバイデザインにおける SBOM の重要性を説明している。特に SBOM 導入のメリットはイメージ図も活用しながら、重点的にわかりやすく説明されている。

（3）Survey on SBOM State of the Art

2025 年 12 月19日まで、EU Cybersecurity Agency（ENISA）はアンケート調査「Survey on SBOM State of the Art」を実施している。EU に限らず全世界からの回答を受け付けている。アンケートの目的は、様々な組織や業界での SBOM の現状の把握である。特に、SBOM の導入度・成熟度、活用されているフォーマットやツール、活用シナリオ、価値認識や課題、SBOM 生成と利用の間のギャップ等についての理解を目指している。

表 2-4 アンケートにおける質問事項

セクション	質問内容
組織属性	・組織の種類・業種・規模・主たる地域 ・EU Cyber Resilience Act（CRA）の製品への適用有無
リスク認識・セキュリティ対応体制	・サプライチェーンの懸念度 ・予算・人員などの投資状況 ・SBOM や CRA の認知の有無 ・関連施策の優先順位の認識
SBOM の採用状況・使い方	・SBOM への関与の仕方（生成・利用・関連ツール提供等） ・SBOM 導入の成熟度及び組織内での SBOM の位置づけ
フォーマット・ツール・ライフサイクル統合	・使用している SBOM のフォーマットや生成手法 ・ソフトウェア開発ライフサイクルにおける SBOM 活用 ・製造者からの SBOM の入手頻度 ・SBOM フォーマット・ツールの選定理由
使い方とギャップ	・必要な SBOM の深さ ・実際に得られる SBOM の深さ ・SBOM の主な用途と利用部門 ・CRA に対する対応方針 ・SBOM の生成と利用のギャップ ・SBOM 運用の自動化の方針及び SBOM 活用に関わる課題
障壁・ニーズ・外部支援	・SBOM の大規模導入の障壁 ・SBOM の生成・利用の能力向上に期待する支援 ・脆弱性声明の重要性の認識と希望する受け取り方 ・CRA による SBOM 関連の投資判断への影響 ・SBOM の相互運用性の重要性の認識と希望する方式 ・有効なガイダンスやテンプレートの領域 ・CRA に対応する SBOM 成熟度に達するまでの見込み期間 ・SBOM に関する進捗を加速させると期待される外部支援 ・SBOM 活用のメリット
サプライヤー要求 ＊SBOM 利用者（受領側）のみ回答	・調達契約における SBOM 要求の有無 ・要求基準を満たす SBOM を提供するサプライヤの比率 ・サプライヤの供給する SBOM の主な問題点について
自由記述	・SBOM の価値を高めるために期待する改善点 ・その他コメントについて

（4）SBOM LANDSCAPE ANALYSIS

2025 年 12 月、ENISA は、「SBOM LANDSCAPE ANALYSIS」（Public Draft 1.2）を公開した。本文書は、多様な成熟度・制約条件の組織が SBOM を実装・運用できるよう、実践的なフレーム

ワークや段階的なアプローチを提供することを目的としている。なお、EU CRA の要求事項の法的解釈を提供することは意図されていない。本文書の主要部分である SBOM 実装ガイドの章においては、SBOM 導入のライフサイクルを開始・計画・実行・監視及び制御・終結の 5 つのフェーズに区分し、各フェーズにおける論点や実施事項を整理している。また、本文書には、読者の属性や目的に応じた複数の読解の順番に関するガイドも含まれている。

表 2-5 SBOM LANDSCAPE ANALYSIS の目次構成

目次項目	概要
1. 序論	
1.1 目的と範囲	本文書の目的とスコープを整理。
1.2 定義	用語の定義を整理。
1.3 本レポートの構成	本文書の構成を整理。
2. SBOM 実装ガイド	
2.1 開始フェーズ	取り組み開始時に答えるべき主要論点を整理。
2.2 計画フェーズ	SBOM のフォーマットの比較検討、SBOM に最低限含めるべき要素、ツール選定に資する情報、検証と署名の方法に関して説明。
2.3 実行フェーズ	SBOM の生成、活用、品質担保や、SBOM 自体のセキュリティ確保、SBOM の自動化に関して説明。
2.4 監視及び制御フェーズ	SBOM の更新管理やコンポーネント健全性のアセスメントに関して説明。
2.5 終結フェーズ	SBOM 実装の課題の整理と改善に関して説明。
3. 実践的なヒントと例	
3.1 SBOM 実装パターン	状況に応じた多様な SBOM 実装パターンを提示。
3.2 実装ケース：複数リポジトリ SBOM 集約	複数の生成物の SBOM を集約し管理する方法について説明。
付録	
A 用語集・略語集	SBOM 関連用語・略語を整理。
B 参考文献／参照文献	関連文献等を整理。
C 能力構築と職員スキル育成の例	中小規模企業のスキル構築の方法を説明。
D ステークホルダ区分	ステークホルダごとの SBOM の用途を整理。
E SBOM フォーマットに関する追加情報	SBOM のフォーマットの詳細を補足。
F フォーマット間の詳細マッピングと互換性	SBOM のフォーマット間の対応や変換に関する整理。
G SBOM 標準間の変換・翻訳ツール	SBOM フォーマットの変換ツールについて整理。
H SBOM 検証・品質チェックリスト	SBOM ライフサイクル全体に対するチェックポイントを提示.
I CI/CD 統合例	SBOM 生成ツールを CI/CD に組み込む具体例を提示。

2.3 ソフトウェア・セキュリティに関する動向調査

SBOM に関する動向として調査した内容は下表に示す通りである。以降は各取り組みの概要を示す。

表 2-6 ソフトウェア・セキュリティに関する動向調査の対象一覧

#	取組名・文書名	取組年月	国・地域	取組主体
1	2025 Developer survey[5]	2025 年	国際	Stackoverflow
2	2025 年度ソフトウェア動向調査[6]	2026 年 2 月	日本	IPA
3	SUSTAINING SELECT EFFORTS TO STRENGTHEN THE NATION'S CYBERSECURITY AND AMENDING EXECUTIVE ORDER 13694 AND EXECUTIVE ORDER 14144[7]	2025 年 6 月	米国	White House
4	NIST SP 1800-44 Secure Software Development, Security, and Operations (DevSecOps) Practices[8]	2025 年 7 月	米国	NIST
5	SSDF Version 1.2[9]	2025 年 12 月	米国	NIST
6	OMB 覚書 M-26-05[10]	2026 年 1 月	米国	White House
7	Joint guidance on software security code of practice[11]	2025 年 5 月	欧州	NCSC-UK[12], DSIT[13], Cyber Centre[14]

[5] Stack Overflow, Stack Overflow Annual Developer Survey
https://survey.stackoverflow.co/2025
[6] IPA, 2025 年度ソフトウェア動向調査
https://www.ipa.go.jp/digital/software-survey/software-engineering/software2025.html
[7] White House, SUSTAINING SELECT EFFORTS TO STRENGTHEN THE NATION'S CYBERSECURITY AND AMENDING EXECUTIVE ORDER 13694 AND EXECUTIVE ORDER 14144
https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/
[8] NIST, NIST SP 1800-44 (Initial Public Draft) Secure Software Development, Security, and Operations (DevSecOps) Practices
https://www.nccoe.nist.gov/sites/default/files/2025-07/nist-sp-1800-44a-ipd.pdf
[9] NIST, Secure Software Development Framework (SSDF) Version 1.2: Recommendations for mitigating the risk of software vulnerabilities
https://csrc.nist.gov/pubs/sp/800/218/r1/ipd
[10] Office of Management and Budget, Adopting a risk-based approach to software and hardware security (Memorandum M-26-05)
https://www.whitehouse.gov/wp-content/uploads/2026/01/M-26-05-Adopting-a-Risk-based-Approach-to-Software-and-Hardware-Security.pdf
[11] NCSC, DSIT, Cyber Centre, Joint guidance on software security code of practice
https://www.cyber.gc.ca/en/news-events/joint-guidance-software-security-code-practice
[12] 英国の国家サイバーセキュリティ**センター**の略称
[13] 英国の科学・イノベーション・技術省の略称
[14] カナダのサイバーセキュリティセンターの略称

（1） 2025 Developer survey

ソフトウェア開発者の世界的なコミュニティである Stack Overflow は「Stack Overflow Annual Developer Survey」において、2023 年からソフトウェア開発における AI の利用状況について調査している。当該調査は世界各国のソフトウェア開発者に対する大規模なアンケート調査であり、2025 年の調査においては 49000 人を超える回答を得ている。AI の利用率は年々増加しているとともに、コードの作成等においても AI の利用が広まっていることが明らかになっている。

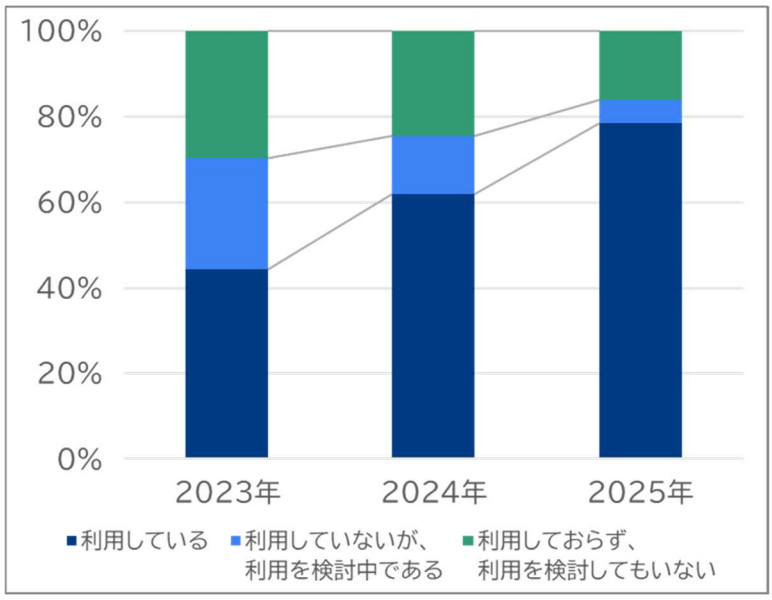


図 2-2 開発工程における AI の利用等の状況[15]

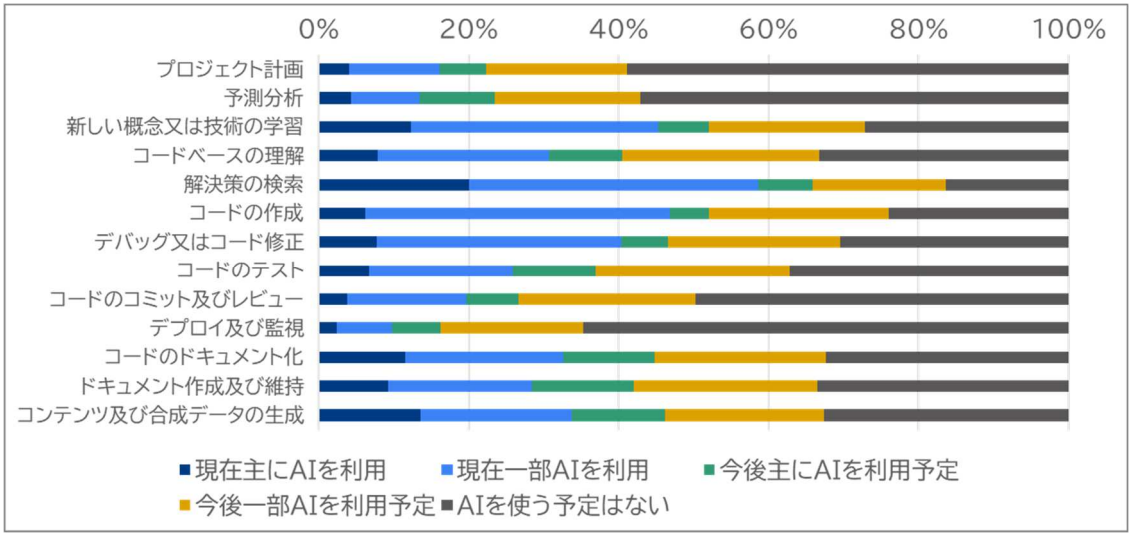


図 2-3 開発での各ワークフローにおける AI の利用等の状況（2025 年）[16]

[15] 2025 年の「利用している」の割合は、3 段階の頻度（日次、週次又は月次若しくは不定期）でそれぞれ利用している割合を合計したものである。
[16] 各ワークフローについて、いずれかの利用等の状況を回答した人数の合計を 100%として集計している。

（2）2025 年度ソフトウェア動向調査

IPA は、ソフトウェアの考え方・開発実態などを把握することを目的に、2023 年度より国内企業向けの調査を実施している。IPA は①「2023 年度ソフトウェア開発に関するアンケート調査」、②「2024 年度ソフトウェア動向調査」及び③「2025 年度ソフトウェア動向調査」において、SBOM 導入に関する国内の動向を調査している。調査結果から、2024 年から 2025 年にかけて、ベンダー企業で SBOM 導入が進展していることが読み取れる。

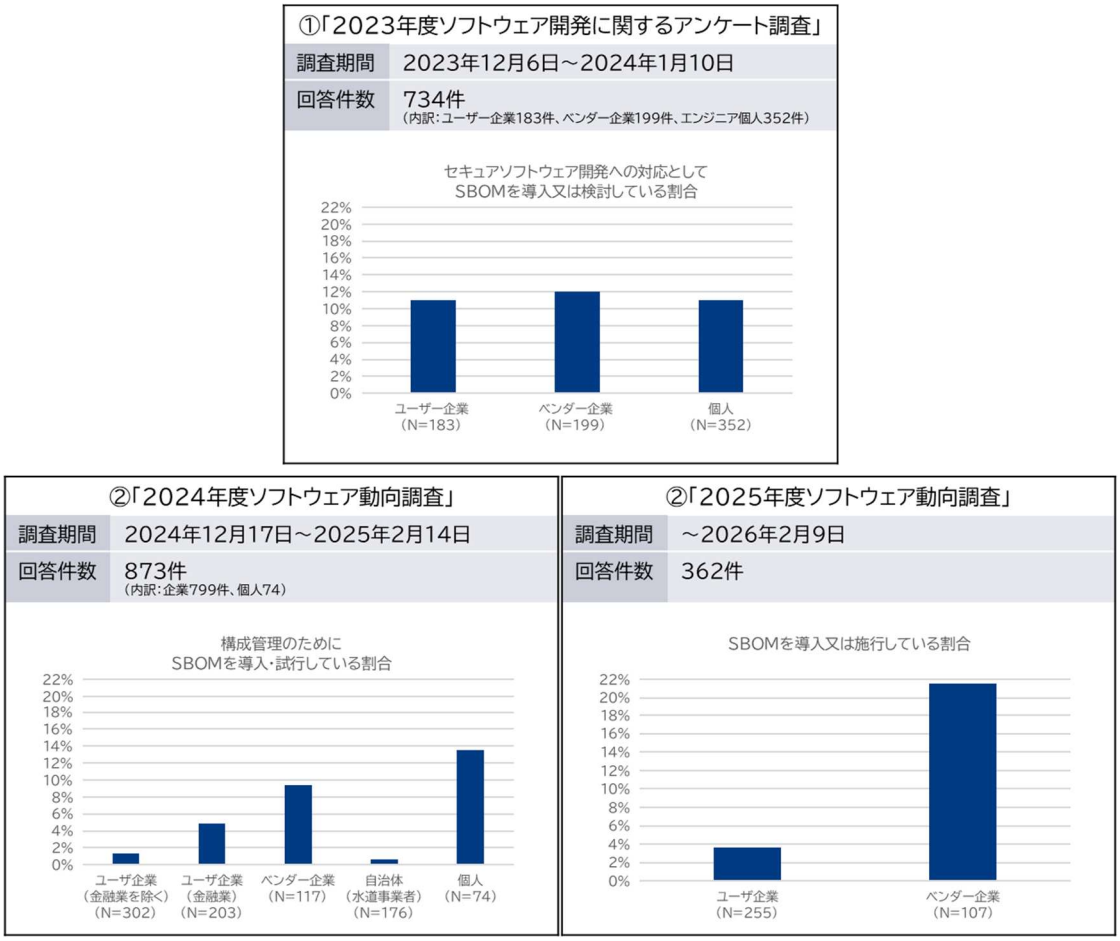


図 2-4 2023-2025 年度のソフトウェア動向調査における SBOM 導入状況

また、IPA は「2024 年度ソフトウェア動向調査」において、システム・ソフトウェア開発の工程ごとの AI 導入状況を調査している。AI を導入・試行している企業は、全体の約 10%以下であり、検討中を含めても 20%以下である。全体的な傾向として、ベンダー企業において AI の導入が進んでおり、製造・テスト工程において活用されているケースが多い。「2025 年度ソフトウェア動向調査」においても、業務一般や開発における工程ごとの AI 導入状況を調査している。全体的な傾向として、業務一般への生成 AI の導入率に対して、開発工程への AI の導入率は小さい。一方で、2024 年度と比較すると開発工程で AI 利用されている割合が増えていることも確認できた。

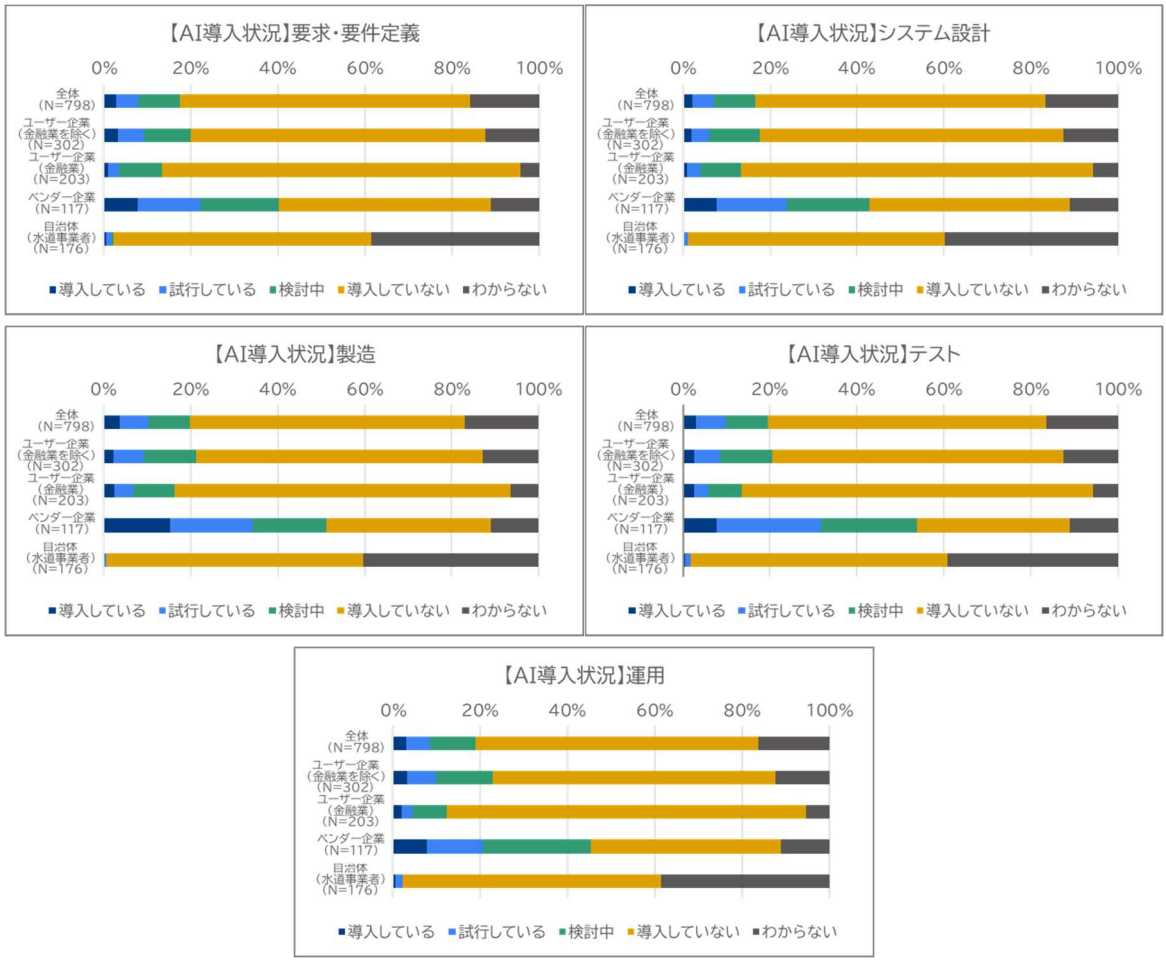


図 2-5 2024 年度のソフトウェア動向調査における AI 導入状況

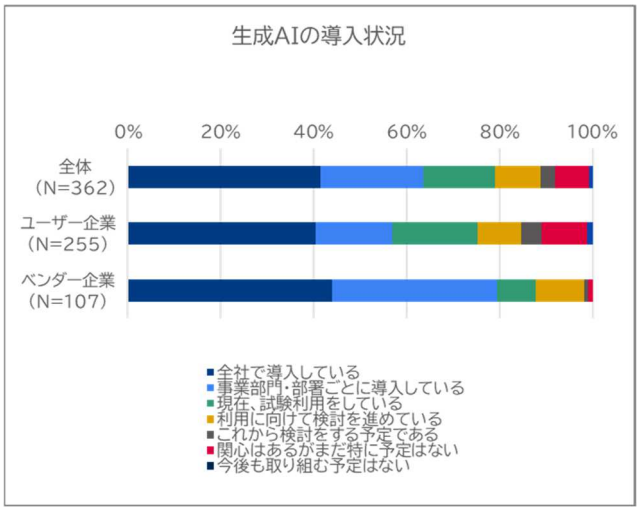


図 2-6 2025 年度のソフトウェア動向調査における生成 AI の導入状況

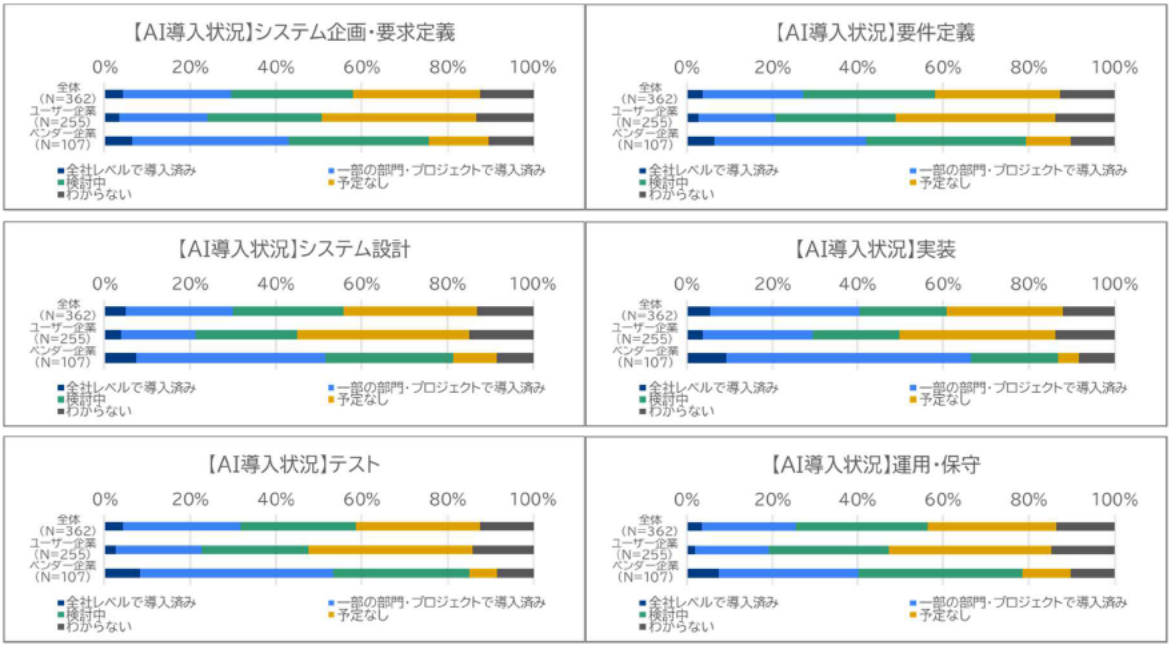


図 2-7 2025 年度のソフトウェア動向調査における AI 導入状況

(3) SUSTAINING SELECT EFFORTS TO STRENGTHEN THE NATION'S CYBERSECURITY AND AMENDING EXECUTIVE ORDER 13694 AND EXECUTIVE ORDER 14144

2025 年 6 月 6 日、米国トランプ大統領は、米国のサイバーセキュリティを強化するための厳選された取り組みを維持する方針で、2025 年 1 月にバイデン前大統領が署名した大統領令 14144 号を改正する大統領令に署名した。大統領令 14144 号の多くを引き継ぎつつも、サイバーセキュリティに関する課題の優先順位の見直しを行っている。不法移民の不正受給を懸念したデジタル ID の義務化廃止、ソフトウェア調達におけるコンプライアンスプロセスの変更などの見直しが行われている。また、大統領令 14028 号を参照する内容については全て削除されている。

表 2-7 サイバーセキュリティ改善に係る大統領令の概要と主な改訂点

項目	概要(大統領令 14144 号)	改訂のポイント
サードパーティ・ソフトウェアのサプライチェーンにおける透明性とセキュリティの運用	ソフトウェア開発・提供方法の確立、ソフトウェアのセキュリティ確保、サプライチェーンリスクマネジメントの組織全体のリスクマネジメントへの統合、OSS の適切な管理など	SSDF を実装するガイダンスの開発は維持しつつ、米国連邦政府が調達するソフトウェアが SSDF に準拠していることを証明する手順に関する記述の一部が削除。
連邦政府システムのサイバーセキュリティの向上	セキュリティ脅威の可視化、連邦政府クラウドサービスや宇宙システムのセキュリティなど	大統領令 14028 に則ったパイロットデプロイメントに関する記述が削除。
連邦通信の保護	連邦政府で用いる通信に対する先進的な認証と暗号化技術の導入など	PQC に関するリスクや今後の政策の内容に関する記述が変更された。

項目	概要（大統領令 14144 号）	改訂のポイント
サイバー犯罪および詐欺に対抗するための対策	デジタル ID の導入、不正取引防止技術のパイロットプログラムの実施など	セクションごと削除された。デジタル ID の導入、不正取引防止技術のパイロットプログラムの実施などが含まれていた。
AI のセキュリティと AI によるセキュリティの推進	AI を活用したサイバーセキュリティ対策の推進、AI ソフトウェアに対する脆弱性管理など	AI を活用したサイバーセキュリティ対策の推進に関する記述が削除された。
政策と実践の整合	連邦政府の IT インフラとネットワークの近代化のための政策遂行、投資や優先順位の整合化など	連邦政府の IT インフラのルール改訂および、OMB、NIST、CISA が策定するポリシー及びガイダンスの機械可読形式化が追加された。
国家安全保障システムや重要システムにおける対策	重要システムに対する特別なセキュリティ要件の検討など	ー
悪意ある重大なサイバー関連活動に対抗するための追加措置	米国及び同盟国に対する悪意あるサイバー活動の対象範囲の特定、活動者に対する差し押さえなど	ー

ソフトウェアに関連する主な変更点は以下のとおりである。

① 連邦政府のソフトウェア調達の際に、ソフトウェア事業者による「機械可読のソフトウェア開発証明」（※1）を利用したセキュリティ対策証明書の提出の義務付け撤回

② 本義務化を講じるために連邦調達規則（FAR）の改正の撤回

③ SSDF の更新を踏まえた OMB 覚書（M-22-18）や CISA 自己証明フォームの改訂に関する事項の撤回

SSDF や NIST SP800-53 の更新、NIST SP800-161 の義務付けに関する記載は修正されなかった（更新・義務付けの時期は延期）。SSDF 適応ガイダンスの作成・更新等は推進されることから、米国政府においてソフトウェア・セキュリティへの注目度は一定程度あると見られる。他方、OMB 覚書や CISA 自己証明フォームの改訂が削除されたことから、負担の増加に関する事項は慎重であると考えられる。

図 2-8 連邦調達ソフトウェアのセキュリティに関する大統領令の指示内容・タイムライン
（変更箇所は赤で記載）

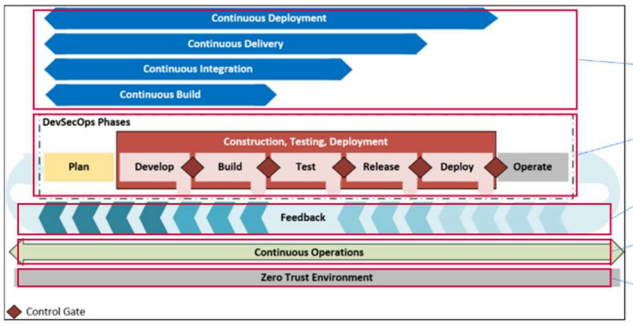
（4）NIST SP 1800-44 Secure Software Development, Security, and Operations（DevSecOps）Practices

2025 年 7 月、米国 NIST の部局である NCCoE（National Cybersecurity Center of Excellence）は、大統領令 14306 号への対応の一環として、「セキュアなソフトウェア開発、セキュリティ、および運用（DevSecOps）の実践」の初期パブリックドラフトを公開した。本文書は、ソフトウェアサプライチェーン及び DevSecOps プラクティスコンソーシアム[17]を通じて、SSDF を参照した DevSecOps の実践に対して、リスクベースのアプローチと推奨事項を実証し、文書化することを目的としている。対象者として、ソフトウェアの開発、提供及び運用に携わる技術リーダー及び実務者並びにソフトウェアの開発、提供及び運用チームの協調促進に携わる人物が想定されている。ソフトウェアをセキュアに開発するための課題として、「統合」、「証明」、「サードパーティ要素の可視化の課題」、「AI ツールの出現」の解決策を実証し、プラクティス例を文書化する。

統合	証明	サードパーティ要素の可視化の課題	AIツールの出現
• 自動化ツール等を適切に協調させ、適切なフィードバックを提供し、セキュリティ要件を守ることは複雑で時間がかかる。	• セキュリティ要件を守ったことを示す証跡を残すことは重要である。一方で、証跡に必要な量、形式及び内容は明確に定義されていない。	• サードパーティ製のコンポーネントを含むことが多く、入れ子構造になっている場合もある。そのため、ソフトウェアサプライチェーン全体のリスク管理が必要である。	• AIツールの導入が進んでいるが、AIツールを活用するためのセキュリティ要件の定義はまだ明らかでない。

図 2-9 コンソーシアムにおいて取り組む 4 つの課題

本文書では、DevSecOps のプラクティスを実装するソフトウェア開発プロセスとして、概念参照モデルを構築している。ソフトウェア開発のプロセスが複数のフェーズに分けられ、各フェーズの区切りには、技術的及び組織的な管理策を実施し、開発・運用・セキュリティ上のタスクに関するフィードバックを得るためのコントロールゲートが設けられる。本プロジェクトの実証において、コントロールゲートにおける管理策を自動化ツールの活用により、現実的で再現可能なメカニズムを実証する。



概念	内容
継続的統合/継続的提供（CI/CD）パイプライン	各フェーズに固有の要素を実行するために使用される自動化されたパイプラインを提供する。
DevSecOps フェーズ群	計画、開発、ビルド、テスト、リリース、デプロイ、運用の7つのフェーズから構成される。
フィードバックサイクル	コントロールゲート又は外部からの信号をDevSecOpsにて先行するフェーズにフィードバックする。
継続的運用	DevSecOpsにおける一連の要素及びアクティビティから構成される。
ゼロトラスト環境	クラウドベース環境のセキュリティ確保に焦点を当て、最小権限アクセスの適用を行う。

図 2-10 NIST SP 1800-44 における DevSecOps の概念参照モデルとモデルをサポートする 5 つの概念

[17] 大統領令 14306 により、設立されたコンソーシアム。AMI、Black Duck、CyberArk、Dell Technologies、DigiCert、Endor Labs、GitLab、Google、IBM、Microsoft、NextLabs、Palo Alto Networks、Sagittal AI、Scribe Security の 14 社により構成。

（5）SSDF Version 1.2

2025 年 12 月17 日に、NIST は SSDF Version1.2（SP 800-218 Rev.1）の初期公開草案を発表した。SSDF の更新は大統領令 14306 号に規定されており、当初の予定を 16 日遅れて暫定版が公表されている。2026 年 1 月 30 日まで、SSDF の Version 1.2 へのパブコメが募集されている。その後、パブコメ対応を行った最終版が 2026 年 3 月 31 日に公表される予定である。

表 2-8 SSDF の Version1.2 への更新スケジュール

時期	出来事	補足
2025 年 6 月 6 日	大統領令 14306 号の発出	大統領令 14306 号は、SSDF の更新について以下のように規定している。 ・ 商務長官は、NIST 長官を通じて、2025 年 12 月 1 日までに SSDF の更新された暫定版を策定し公表する。 ・ 商務長官は、NIST 長官を通じて、暫定版の公表から 120 日以内に SSDF の最終版を公表する。
2025 年 12 月 17 日	SSDF Version1.2 初期公開草案の公開・パブリックコメント募集開始	初期公開草案は、大統領令における規定から 16 日遅れて公表された。
2026 年 1 月 30 日	SSDF Version1.2 初期公開草案のパブリックコメント募集締切	-
2026 年 3 月 31 日（予定）	SSDF Version1.2 最終版の公開	大統領令の規定に従えば、当初の想定としては 2026 年 3 月 31 日までに SSDF Version1.2 の最終版が公開される予定である。（草案の公開が遅れたため、最終的な更新も遅れる可能性がある。）

SSDF Version1.2 における主な更新事項として、以下が挙げられる。

- 新たなプラクティスの追加
- 新たな実装例の追加
- タスクと実装例の文言の更新
- NIST SP800-53,161 との対応関係の更新
- 大統領令 14028 に関する記載の削除
- その他体裁の修正

新規に追加された 2 つのプラクティスは、大統領令 14306 号における NIST SP800-53 の更新目的（2025 年 8 月に更新済み）である「パッチやアップデートの安全かつ確実な展開方法の指針」と関連が深いと考えられる。また、追加された実装例の多くは PW（セキュアなソフトウェアの開発）にあたり、ソフトウェア開発における具体的な実装方法がより補足されている。

表 2-9 SSDF の Version1.2 で新規に追加されたプラクティス・実装例

区分	新規追加項目	概要
プラクティス	PO.6（継続的なプロセス改善計画の定義・実行）	ソフトウェアデザインライフサイクル（SDLC）全体を通じて、SSDF の全プラクティスにまたがるサイバーセキュリティのプロセス及び手順の改善を特定して実行することを推奨
	PS.4（堅牢で信頼できるアップデート）	堅牢で信頼できるアップデート戦略を実装し、可能なら顧客がソフトウェアパッケージやアプリ設定の更新をコントロールできるようにすることや、更新をテストし、責任をもって配布することで、利用者の運用継続と障害・混乱の最小化を支援することを推奨
実装例	PW.1.1 Example 5	リスクや脅威モデルを作成し管理された範囲内で共有することを推奨
	PW.1.3 Example 4	一般に普及している安全なログ形式及び機能の利用を推奨
	PW.1.3 Example 5	最小権限の原則に従うことを推奨
	PW.4.4 Example 8	サードパーティライブラリの所有者変更を定期的にレビューし影響を評価することを推奨
	PW.5.1 Example 10	入力インタフェースで検証やサニタイズしやすい構造化されたフォーマットを用いることを推奨
	PW.5.1 Example 11	必要に応じて形式的な手法や証明器でコードを検証することを推奨
	PW.8.2 Example 10	サードパーティ依存関係を特定し、依存関係を使用する機能を十分に動作させる堅牢なテストの実施を推奨
	PW.9.1 Example 2	デフォルトのパスワードやハードコードされた保護機構の使用を禁止することを推奨
	PW.9.1 Example 3	ログに関する設定や保持期間のデフォルトをセキュアなものとし、管理者が制御できるようにすることを推奨
	RV.1.2 Example 3	顧客から報告される課題を監視し、デフォルト設定の更新や注意喚起を実施することを推奨

（6）OMB 覚書 M-26-05

2026 年 1 月、米国大統領府行政管理予算局（OMB）は覚書 M-26-05 を発出し、米国連邦政府の調達におけるセキュリティの確保のための方針を示した。M-26-05 は、先行する OMB 覚書である M-22-18 及び M-23-16 を無効化した。旧覚書（M-22-18 及び M-23-16）では、政府調達されるソフトウェアに対して省庁横断的な確認手順を適用することを制度化していたが、新覚書（M-26-05）では、政府調達されるソフトウェアおよびハードウェアに対して各省庁ごとのリスク評価に基づく個別的な確認手順を適用する方針が示された。

表 2-10 旧覚書(M-22-18 及び M-23-16)と新覚書(M-26-05)の比較

区分	旧覚書(M-22-18 及び M-23-16)	新覚書(M-26-05)
政府調達時の確認手順	連邦機関は、省庁横断的な確認手順を実施する。連邦機関は、原則として、ベンダから、NIST ガイダンスに沿った政府指定の安全な開発慣行に適合していると自己証明する文書を受領する必要がある。 ・NIST ガイダンスとは、以下の 2 つの文書を指す。 ➢ SSDF ➢ ソフトウェアサプライチェーンセキュリティガイダンス ・連邦機関は、必要に応じて SBOM 等を調達要件として要求できる。	ソフトウェアデザインライフサイクル(SDLC)全体を通じて、SSDF の全プラクティスにまたがるサイバーセキュリティのプロセス及び手順の改善を特定して実行することを推奨
覚書のスコープ	ソフトウェア	ソフトウェアおよびハードウェア

(7) Joint guidance on software security code of practice

2025 年 5 月、英国の NCSC-UK、DSIT 及びカナダの Cyber Centre が共同で、ソフトウェアの開発及び運用においてセキュリティ及びレジリエンスを強化するためのサイバーセキュリティ行動規範(Joint guidance on software security code of practice)を発表した。ソフトウェアセキュリティに関するプラクティスを整理したガイドラインで、SSDF と CRA を参照して作成された。行動規範に従うべきとされる対象者は、ソフトウェアの開発者とソフトウェアの販売者であり、ソフトウェアのユーザーに対し、セキュアな開発を行ったことのアシュアランスを確保するための自己評価フォームが添付されている。

図 2-11 ソフトウェアセキュリティの行動規範を構成している共同ガイダンス

行動規範を実施するにあたって組織の責任者が確認すべき事項を示す。各評価事項に関して論拠と考慮事項を提示する形式を採用。内部コンプライアンス監視における利用やソフトウェアのセキュリティを保証するために顧客と情報を共有することが可能。行動規範は、NCSC の原則主義保証アプローチに基づき、原則(Principle)と言明(Claim)について具体化されている。なお、英国は、自己評価

フォームによるソフトウェア・セキュリティ保証の認証スキームの開発に取り組んでいる。

表 2-11 ソフトウェア・セキュリティの行動規範に関する共同ガイダンスにおける原則（Principle）と言明（Claim）

Theme	Principle	Claim 例
1. 安全な設計と開発	1.1 確立された安全な開発フレームワークに従う。	使用された開発フレームワークは文書化されている。
	1.2 ソフトウェアの構成を理解し、開発ライフサイクルを通じてサードパーティコンポーネントの取得とメンテナンスに関連するリスクを評価する。	サードパーティのコンポーネントはすべて特定され、文書化されている。
	1.3 配布前にソフトウェアのアップデートやテストをするための明確なプロセスを持つ。	すべての要件とサードパーティコンポーネントをカバーするテスト計画が存在する。
	1.4 ソフトウェアの開発ライフサイクルを通じて、Secure by design 及び Secure by default の原則に従う。	ソフトウェアがどのように悪用される可能性があるかを理解するための技術（脅威モデリング）が、ソフトウェアの設計に活用されている。
2. 環境セキュリティの構築	2.1 ビルド環境を不正アクセスから保護する。	役割が限定され、各役割がアクセスできるデータと機能が指定される。
	2.2 ビルド環境への変更を管理し、ログに記録する。	ビルド環境へのアクセスと変更はログに記録される。
3. 安全なデプロイとメンテナンス	3.1 ソフトウェアを顧客へ安全に配布する。	ソフトウェア（アップデートを含む）の完全性は、顧客環境で検証可能である。
	3.2 効果的な脆弱性開示プロセスを導入し、公表する。	脆弱性開示の方針とプロセスを公表する。
	3.3 ソフトウェアコンポーネントの脆弱性を事前に検出し、優先度を付けて管理するためのプロセスと文書を整備する。	公開されている脆弱性に関する情報が常に最新に保たれている。
	3.4 必要に応じて脆弱性を関係者に報告する。	社内のセキュリティ担当に報告する。
	3.5 適切なタイミングで、セキュリティアップデート、パッチ、通知を顧客に提供する。	セキュリティアップデートはできる限り速やかに顧客へ提供される。
4. 顧客とのコミュニケーション	4.1 販売するソフトウェアのサポートとメンテナンスのレベルの情報を顧客に提供する。	すべてのソフトウェアコンポーネントに対して、サポート終了日が公表されている。
	4.2 ソフトウェアのサポート又はメンテナンスが終了する時期について、少なくとも 1 年前にベンダーから通知する。	ソフトウェアがサポートされなくなる時期について、少なくとも 1 年前の通知が顧客に提供される。
	4.3 顧客組織に重大な影響を及ぼす可能性のある注目すべきインシデントに関する情報を顧客に提供する。	関連するインシデントは、適切なタイミングで顧客に通知される。

2.4 AI セキュリティに関する動向調査

AI セキュリティに関する動向として調査した内容は下表に示す通りである。一方で、下表で示す通り、AI を活用したソフトウェア開発に関する各取り組みの概要を示す。

表 2-12 AI セキュリティに関する動向調査の対象一覧

#	取組名・文書名	取組年月	国・地域	取組主体
1	OWASP GenAI Security Project[18]	2024 年	国際	OWASP[19]
2	A shared G7 vision on software bill of material for AI)[20]	2025 年 6 月	国際	G7
3	Cybersecurity Risks of AI-Generated Code[21]	2024 年 11 月	米国	CSET(Center for Security and Emerging Technology)
4	NIST IR 8596 Cybersecurity Framework Profile for Artificial Intelligence (Cyber AI Profile): NIST Community Profile[22]	2025 年 12 月	米国	NIST
5	AI Coding Assistants[23]	2024 年 9 月	独・仏	BSI[24]・ANSSI[25]
6	ETSI EN 304 223[26]	2025 年 12 月	欧州	ETSI[27]

(1) OWASP GenAI Security Project

LLM が急速に社会実装され、敵対的攻撃、データ漏洩などのリスクが増大しているところ、AI に対する整理されたセキュリティのフレームワークを構築することを目的に OWASP GenAI Project が設立された。本プロジェクトでは、非営利団体の OWASP が生成 AI のセキュリティに関する専門家を集め、

[18] OWASP, Home - OWASP Gen AI Security Project
https://genai.owasp.org/
[19] Open Worldwide Application Security Project の略称
[20] G7, A shared G7 vision on software bill of material for AI
https://www.acn.gov.it/portale/documents/20119/56212/PAPER_SBOM+for+AI_19MAY2025_+clean+2.pdf/9889140b-2e05-e0c9-0d24-a90ec7fa48e2?t=1750066144520
[21] CSET, Cybersecurity Risks of AI-Generated Code
https://cset.georgetown.edu/wp-content/uploads/CSET-Cybersecurity-Risks-of-AI-Generated-Code.pdf
[22] NIST, NIST IR 8596
https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8596.iprd.pdf
[23] ANNSI, BSI, AI Coding Assintants
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/ANSSI_BSI_AI_Coding_Assistants.pdf?__blob=publicationFile&v=7
[24] ドイツ連邦政府の情報セキュリティ庁の略称
[25] フランスの国家情報システムセキュリティ庁の略称
[26] ETSI, Baseline Cyber Security Requirements for AI Models and Systems (ETSI EN 304 223 V2.1.1)
https://www.etsi.org/deliver/etsi_en/304200_304299/304223/02.01.01_60/en_304223v020101p.pdf
[27] 欧州電気通信標準化機構の略称

誰もが利用可能な生成 AI のセキュリティに関するガイダンスやツールを公開している。現在は、15 カ国 15000 人以上のメンバが参画し、20 以上のガイダンスが公表されている。

表 2-13 OWASP GenAI Security Project の概要

項目	詳細
経緯	・2023 年 5 月に前身となる取組みが開始した ・その後、取組みを拡大するとともに名称を現在のものに変更し、現在に至る
取組みの内容	・「生成 AI アプリケーションとその導入時におけるセキュリティや安全性に関する懸念を理解し、対策するための、誰でも自由に利用可能なオープンソースのガイダンスとリソースを作成する、グローバルなコミュニティ主導かつ専門家が率いる取り組み」（公式サイトより）
規模	・現在、15 カ国以上から 15000 人以上のコミュニティメンバが参画している ・今までに 20 以上の AI サイバーセキュリティに関する刊行物を公開している
成果物の作成フロー	・世界各国のセキュリティ専門家や実務家のオープンなコミュニティにおける協同により原案が作成され、レビュープロセスを経て公開に至る
成果物の訴求先	・サイバーセキュリティ専門家、生成 AI 開発者、データサイエンティスト、CISO・CTO・CIO 等

2025 年 10 月現在、OWASP GenAI Security Project は領域別のイニシアチブ（作業部会）を擁しており、各イニシアチブでプロジェクトの成果物が作成されている。成果物の内容は、LLM のリスク、LLM のセキュリティ対策、LLM のインシデントレスポンス、LLM のデータセキュリティ、セキュリティツールのカタログなど、多岐にわたる。

表 2-14 OWASP GenAI Security Project のイニシアチブの概要及び関連する成果物の一部

イニシアチブ名	目標	関連するホワイトペーパー・ガイド等[28]
Top 10 for LLM and GenAI	生成 AI および LLM ベースのアプリケーションにおける主要なセキュリティリスクの特定	・OWASP Top 10 for LLM Applications
AI Threat Intelligence and Response	攻撃者による生成 AI の不正利用や新たな脅威パターンの追跡	・GenAI Incident Response Guide ・OWASP LLM Exploit Generation ・Guide for Preparing and Responding to Deepfake Events
AI Security	責任ある生成 AI プログラムの監督の	・LLM AI Cybersecurity & Governance

[28] イニシアチブは改組・改名等を経て変化するため、関連づけの対応関係はおおよそのものである。

イニシアチブ名	目標	関連するホワイトペーパー・ガイド等[28]
Governance	ためのベストプラクティスとフレームワークの策定	Checklist
Secure AI Adoption	責任ある生成 AI プログラムの監督のためのフレームワークとポリシーの策定	・OWASP GenAI COMPASS Play Book ・LLM and GenAI Security Center of Excellence Guide
Agentic App Security	自律エージェントと多段階 AI ワークフローの安全性の確保	・State of Agentic AI Security and Governance ・Securing Agentic Applications Guide ・Agent Name Service (ANS) for Secure Al Agent Discovery ・Multi-Agentic system Threat Modeling Guide ・Agentic AI – Threats and Mitigations ・OWASP Top 10 for Agentic Applications ・A Practical Guide for Secure MCP Server Development
Data Security	トレーニングデータおよび検索用データの情報漏洩や改ざんからの保護	・LLM and Gen AI Data Security Best Practices
Red Teaming & Evaluation	対抗的なレッドチーミング手法による生成 AI システムのテスト	・GenAI Red Teaming Guide ・Vendor Evaluation Criteria for AI Red Teaming Providers & Tooling
AI Security Solution Landscape	主要な生成 AI セキュリティリスクに対応するツールとプラットフォームの一覧化	・LLM and Generative AI Security Solutions Landscape
AIBOM Generator	AIBOM の実用化	・OWASP AIBOM Generator

（2）A shared G7 vision on software bill of material for AI）

2025 年 5 月 12-13 日、イタリアがリードする G7 Cybersecurity Working Group meeting において、AI の SBOM の共有ビジョンを示すことを目的に、“A shared G7 vision on software bill of material（SBOM）for AI”が公表された。AI の高度化に伴い複雑化している AI サプライチェーンのリスクに対応するために、AI の透明性を確保する SBOM が必要である旨が記載されている。AI のための SBOM に求められる 3 つの事項と、その内容を満たすために必要な 8 つの最小項目について記載されている。AI のための SBOM に求められる 3 つの事項は以下のとおりである。

- AIシステムの静的・動的な側面（機械学習、テスト、検証に使用されるデータセットや学習成果など）を捉えることができること。
- 自動処理が容易な機械可読形式で SBOM が生成されること。
- 構造化されたデータ形式を可能な限り活用し、すべての利害関係者が要求に応じて透明性をもって関連情報を入手できるようにすること。

表 2-15 AI のための SBOM に求められる 3 つの事項を満たすために必要な 8 つの最小項目

AI の SBOM の最小項目	項目内容の例
AI システムで使用されるモデル	モデルを特定するための基本情報、モデルの作成方法など
学習に関する情報	学習技術やパイプラインの説明、学習データセットに関する情報など
全ライフサイクルで使用されるデータセット	データの同一性、作成、使用、出所など
安全性とセキュリティの特性	コンプライ アンスの証明、サイバーセキュリティのベストプラクティスのリンクや参照など
システムレベルの特性	AI 要素間のフローや入力データの処理方法など
AI システムの主要性能指標	モデルのベンチマーク評価結果など
ライセンス情報	コンポーネントに関するライセンス情報など
インフラストラクチャー	AI システムを提供するために特に必要なコンポーネントなど

（3）Cybersecurity Risks of AI-Generated Code

米国のジョージタウン大に設置されているシンクタンクである CSET（Center for Seucirty and Emerging Technology）より、AI コーディングのリスクに関するレポートが公表された。本レポートでは、AI コーディングによるリスクを「生成されたコードの安全性への懸念」、「脆弱性のあるコードの流通による不適切な学習」、「安全性の低いコードによる学習」の 3 つに分類している。AI コーディングのリスクに対応における課題を 8 つに整理しているが、具体的な対策については整理されていない。

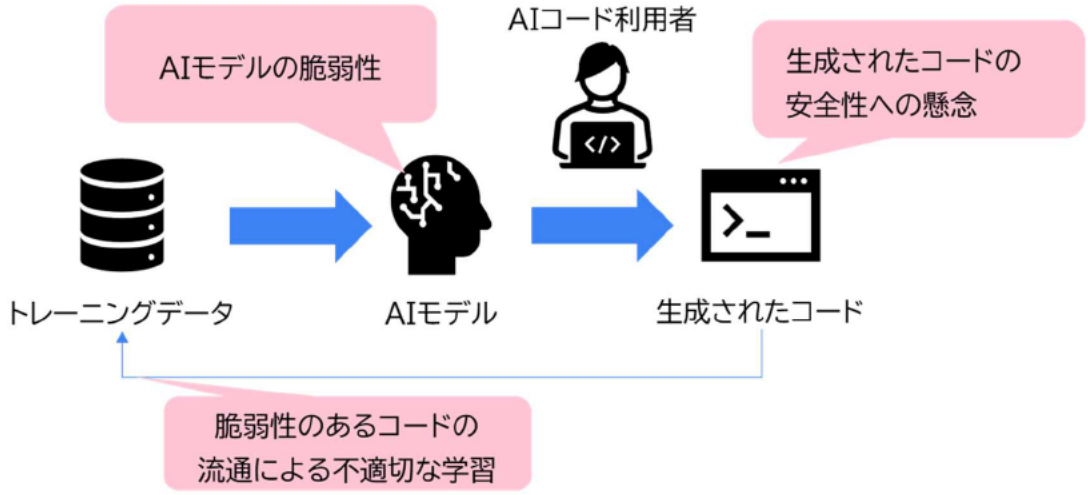


図 2-12 AI コーディングにおけるリスクのイメージ

表 2-16 AI コーディングにおける 8 つの課題

AI コーディングにおける課題	概要
コード言語	Python,C などのコード言語による脆弱性の違い
モデルの種別	モデルによる生成コードの違い
アセスメントルーツ	全てのコード言語を網羅するアセスメントツールの必要性
ベンチマーキング	コードの安全性を示すベンチマーキングの多様性
プロンプト	プロンプトの入力による生成コードの違い
ランダム性と再現性	AI から生成されるコードの再現性
ヒューマンコンピュータインタラクション	AI コーディングが与える開発者への影響

（4）NIST IR 8596 Cyber AI Profile: NIST Community Profile

2025 年 12 月、NIST より AI セキュリティを検討するフレームワークとして、”NIST Cybersecurity Framework”（NIST CSF）を AI セキュリティに拡張した NIST IR 8596（Cyber AI Profile）のドラフトが公開された。本文書では、AI セキュリティを「AI システムコンポーネントの保護（Secure）」、「AI によるサイバーディフェンス（Defend）」、「AI によるサイバー攻撃からの防御（Thwart）」という 3 つの観点で分類して検討されている。具体的な拡張としては、NIST CSF の 106 のサブカテゴリーに対して、AI 観点での解釈を示したうえで、上記の 3 観点それぞれで検討すべき内容と優先度が整理されている。

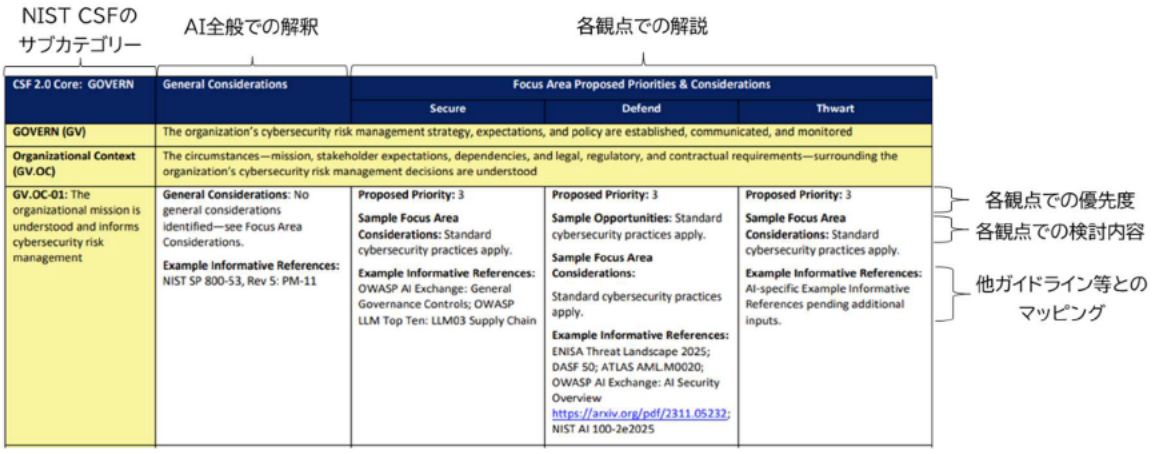


図 2-13 Cyber AI Profile の概要

（5）AI Coding Assistants

2024 年 10 月、ドイツ情報セキュリティ庁（BSI）、フランス国家情報システムセキュリティ庁（ANNSI）は、AI コーディングアシスタントの安全な活用を目的としたホワイトペーパーを発表した。ソフトウェア開発における AI コーディングアシスタントの利用に伴うリスクを挙げ、マネジメント層、開発者、研究者に向けた提言を行っている。

表 2-17 AI コーディングアシスタントの利用に伴うリスクと対策例

カテゴリ	リスクの説明	対策例
機密情報漏えい	入力された情報（コード、API キーなど）が AI の学習データに流用される可能性	・社内利用ガイドラインの整備 ・シャドーIT 対策として、企業アカウントでの契約・利用
自動化による バイアス	AI の出力を過信し、誤ったコードや非現実的な提案を無批判に採用する傾向	・社内レビュー文化の促進 ・プロンプト技術の教育
品質・セキュリティ の欠如	生成コードに脆弱性や非効率な実装が含まれる可能性（例：MD5 などの旧式暗号）	・自動テスト・脆弱性スキャンの導入 ・AI 生成コードの明示・記録（SBOM）
サプライチェーン リスク	AI が提案するライブラリやコードに悪意ある要素が含まれる可能性	・SBOM 作成 ・トレーニングデータの精査
悪用の可能性	攻撃者が AI を使ってマルウェア生成や逆コンパイルを行う可能性	—

表 2-18 AI コーディングアシスタントの利用に向けた提言

対象	推奨事項
マネジメント層	・シャドーIT 対策として、企業アカウントによる契約・利用 ・AI コーディングアシスタント利用におけるリスク分析の実施 ・社内利用ガイドラインの整備 ・品質保証した AI 利用や人員のスケールアップによる生産性向上 ・従業員への教育 ・AI コーディングアシスタント導入による効果測定（新たなコード数やセキュリティチームの作業量等）
開発者	・AI コーディングアシスタントに利用におけるシステムの限界とセキュリティ上の懸念の把握 ・出力されたコードのレビュー及び再現 ・社内での効果的かつ安全な利用に向けた知見共有・教育
研究者	・脆弱性を有するコードや誤ったコードが出力されないような、学習データセットの品質向上 ・別の言語への自動翻訳に特化したデータセットの整備 ・特定の言語に偏らない、多様なソースコードの収集 ・ソフトウェア自動品質管理・セキュリティ管理技術の研究推進 ・AI コーディングアシスタントの生産性向上効果の検証

（6）ETSI EN 304 223

2025 年 12 月、ESTI の AI セキュリティ技術委員会（TC SAI）は、「AI モデル及びシステムのベースラインサイバーセキュリティ要件」（ETSI EN 304 223 V2.1.1）を公開した。本文書は、AI モデル及び AI システムに対する最低限のサイバーセキュリティ要求事項を、AI ライフサイクル全体にわたって整理した ETSI の欧州規格である。参考文献として EU AI Act が含まれている。本文書は、AI ライフサイクルを 5 つのフェーズに分け、13 項目の原則（Principle）と、原則を構成する個別の具体的な要求（Provision）を提示している。

表 2-19 ETSI EN 304 223 における AI ライフサイクルのフェーズごとの原則

フェーズ	原則（括弧書きは要求数）	要求例
機密情報漏えい	入力された情報（コード、API キーなど）が AI の学習データに流用される可能性	・社内利用ガイドラインの整備 ・シャドーIT 対策として、企業アカウントでの契約・利用
セキュアデザイン	1. AI セキュリティ脅威・リスクの啓発（5）	組織のセキュリティ教育プログラムの定期的更新を行うことなど

フェーズ	原則（括弧書きは要求数）	要求例
	2. 機能・性能だけでなくセキュリティも考慮した AI システムの設計（9）	AI システム作成を決定する際に関連する AI セキュリティリスク等を文書化することなど
	3. AI システムに対する脅威評価とリスク管理（7）	AI システムの過剰な機能提供によりリスクを増大させないことなど
	4. AI システムへの人間の責任の確保（5）	AI システムに人間による監視が可能な機能を組み込むことなど
セキュアデベロップメント	5. 資産の把握・追跡・保護（7）	API を介したシステムへの攻撃を軽減するための制御を行うことなど
	6. インフラのセキュリティ確保（6）	システムに利用するモデルやコンポーネントに関連するリスク評価を実施することなど
	7. サプライチェーンのセキュリティ確保（6）データ・モデル・プロンプトの文書化（6）	システムに利用するモデルやコンポーネントに関連するリスク評価を実施することなど
	8. データ・モデル・プロンプトの文書化（6）	訓練データの入手方法を文書化することなど
	9. 適切なテストと評価の実施（6）	システムの展開前にテストを実施することなど
セキュアデプロイ	10. エンドユーザおよび影響される対象に関連したコミュニケーションとプロセス（5）	エンドユーザにデータの用途や管理方法を伝達することなど
セキュアメンテナンス	11. 継続的なセキュリティアップデート・パッチ・緩和策の維持（4）	可能な限りセキュリティアップデートやパッチをエンドユーザに提供することなど
	12. システムの挙動の監視（4）	ログを分析して AI モデルの予期しない動作を検出することなど
セキュアエンドオブライフ	13. データ・モデルの適切な廃棄の実施（2）	システムやモデルの廃止時にデータを安全に削除することなど

2.5 今後の課題

SBOM、ソフトウェア・セキュリティの観点では、米国において大きな動きがあった。特にとについては、トランプ政権に代わり、SBOM を含めたソフトウェア・セキュリティに関する米国の動向が大きく変わったことを示している。次年度以降もソフトウェア・セキュリティを検討するにあたっては、米国の動向を注視していくことが重要である。直近としては、”SSDF Version 1.2”の最終版が公表される予定であり、ドラフト版と比較してどのような修正が入ったかを確認することが望まれる。

AI セキュリティに関しては、ソフトウェアの動向調査などによると、ソフトウェア開発における AI 活用は、国内・海外ともに現在普及が進んでいる段階である。普及促進に合わせて、多くのベンダー企業においては、ソフトウェア開発における AI 活用のメリットを取りまとめレポートなどが公開されている。

AI を活用したソフトウェア開発におけるセキュリティの観点では、ソフトウェア開発に限らず AI 活用におけるセキュリティリスクや対策については、官民問わず様々なレポートが公開されている。一方で、現状ソフトウェア開発における AI 活用をスコープとしたセキュリティ観点のレポートが少ない。理由として、ソフトウェア開発における AI 活用は普及が進んでいる段階であり、セキュリティリスクまで議論がまだ及んでいないと考えられる。

また、米国の SSDF の生成 AI 向けのプロファイルにおいて、人間が記述したソースコードと AI が生成したソースコードを区別しないことが記載されていることから、ソースコードにおけるセキュリティリスクに包含される場合もあると考えられる。

このような AI セキュリティにおける動向も注視して、今後のソフトウェア開発における AI 活用のリスクを整理していくことが望まれる。

3. ソフトウェア開発手法の実践に向けた調査・実証

3.1 実証に向けた背景と問題認識

米国国立標準技術研究所（NIST）の「セキュア・ソフトウェア開発フレームワーク（SP800-218 Secure Software Development Framework（SSDF））」を実践するための具体的な方法や手順等をまとめた国内事業者向け文書を策定するとともに、自己適合宣言の仕組みを構築し、政府調達等での要件化を通じて実効性を強化することにより、QUAD 共通原則を履行することが目標。

昨年度は、SSDF の導入効果等の実証を行ったうえで、国内事業者向け文書の初版案として「SSDF 導入ガイダンス案（中間整理）」を作成。本年度は、産業分野毎の実態に即して効果的に SSDF を導入・実践できること等を目的に複数分野における調査・実証も行ったうえで、ガイダンス案の拡充・成案化など SSDF 導入促進に向けた取組の検討を進めて参りたい。

なお、自己適合宣言の仕組み・政府調達等での要件化等については、今年度は国内事業者向けに自己チェックリスト（第三者による管理・運用を伴わないもの）を検討する。その上で、QUAD 共通原則の履行との関係を踏まえつつも、政府調達での活用のあり方については米国の政策動向等も踏まえ今後検討して参りたい。

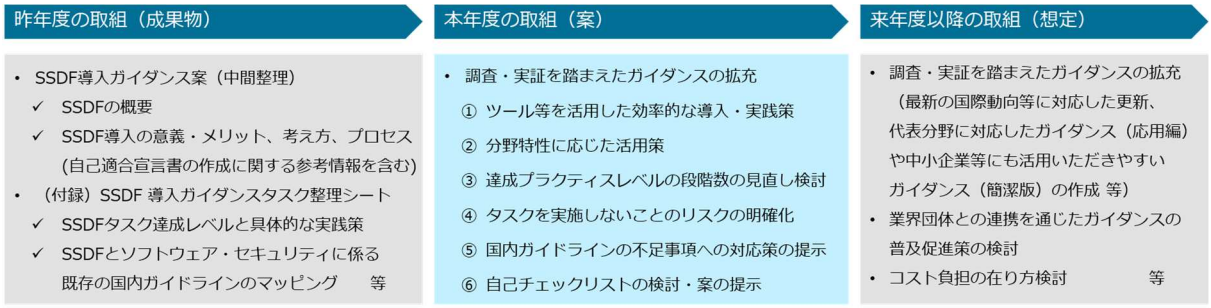


図 3-1 昨年度取組を受けた今年度以降の取組

国内外で多数のセキュリティガイドライン、基準等が存在し、複数分野の事業、国際展開を行う事業者にとって、様々な基準において重複する部分の効率的な対応が期待される。

セキュリティガイドライン、基準の間で項目間の対応関係が明確ではなく、分野間での共通言語となるはずのセキュリティ・フレームワークへの対応付けが行われていない。

QUAD 合意によりセキュリティ・ソフトウェア開発プラクティスを政府調達ポリシーとすることが規定されているが、各国において具体的な実施項目が明確になっていない。

3.2 調査実証の進め方

以下の考え方に基づき調査・実証を進めた。

（4）ツール等を活用した効率的な SSDF の導入・実践の方策の提示

SSDF タスク毎に、適用可能な（実践の自動化・省力化が見込める）ツール等を洗い出し、当該ツール等を活用した効率的な SSDF の導入・実践の実証を行い、ツール等の適用方法などにつ

いて整理する。

（5）個別産業分野の特性に応じた SSDF の活用策の提示

例として金融分野は、セキュリティ・バイ・デザイン、モニタリング検査、サードパーティリスク管理等を重視した対応が求められる特性があると想定。選定した分野での SSDF の導入・実践の実証を行い、当該分野における要求事項等に対応する SSDF の活用策を整理する。

（6）SSDF 達成プラクティスレベルの段階数の見直し検討（3段階 → 2段階（最小限／標準以上等））

現状においてはレベルを3段階としているが、レベル3の難度が高いことにより SSDF 導入のハードルが上がる可能性がある。他方、特定の分野（金融分野など）においては高い達成レベルが求められる可能性もあるため、選定した複数分野で SSDF の導入・実践の実証を行う。

（7）SSDF タスクを実施しないことのリスクの明確化

タスクを実施しないことにより生じるリスクや影響を具体化し、SSDF 導入の必要性の明確化を図る。

（8）国内ガイドラインの不足事項への対応策の提示、各ガイドライン策定主体への働きかけ

ソフトウェア・セキュリティに係る既存の国内ガイドラインの内容で、SSDF タスクを包含できていない部分への対応として、米 NIST Cross-Reference Comparison Report（SSDF Reference）を参照することによって不足分の充足が可能か検討したうえで、当該ガイドラインの改訂が必要か等を経済産業省から各ガイドライン策定主体に検討を促す。

（9）自己チェックリストの検討及び案の提示

米大統領令の改訂を踏まえ、自己適合宣言の仕組み・政府調達等での要件化等ではなく、国内事業者に自己チェックリスト（第三者による管理・運用を伴わないもの）を活用してもらう形とし、同リストの案を作成する。

3.3 実証スケジュール

本実証は、以下のスケジュールで実施した。

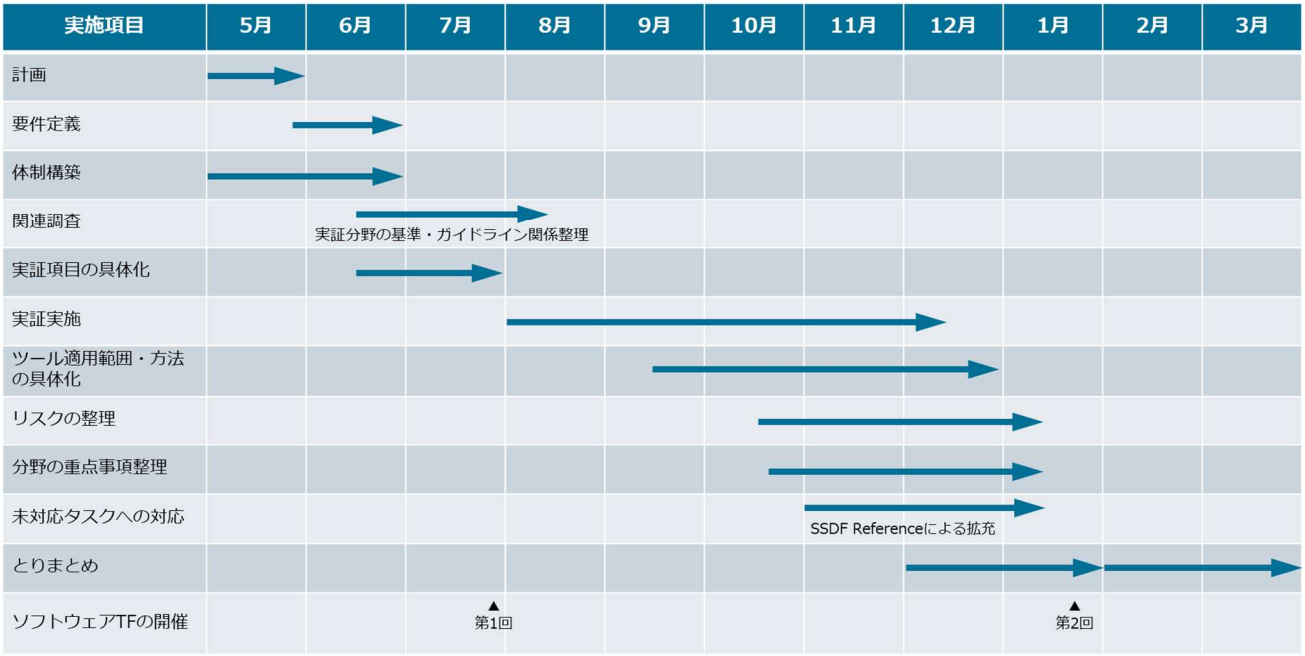


図 3-2 実証スケジュール

3.4 実証体制と対象システム

SSDF の導入におけるツールの活用策、効果、課題について把握し、SSDF 導入ガイダンスを拡充するため、異なる分野の実際の製品やシステムを対象としてツールを主体とした SSDF の導入を実証した。

対象分野と実証内容は以下のとおり。

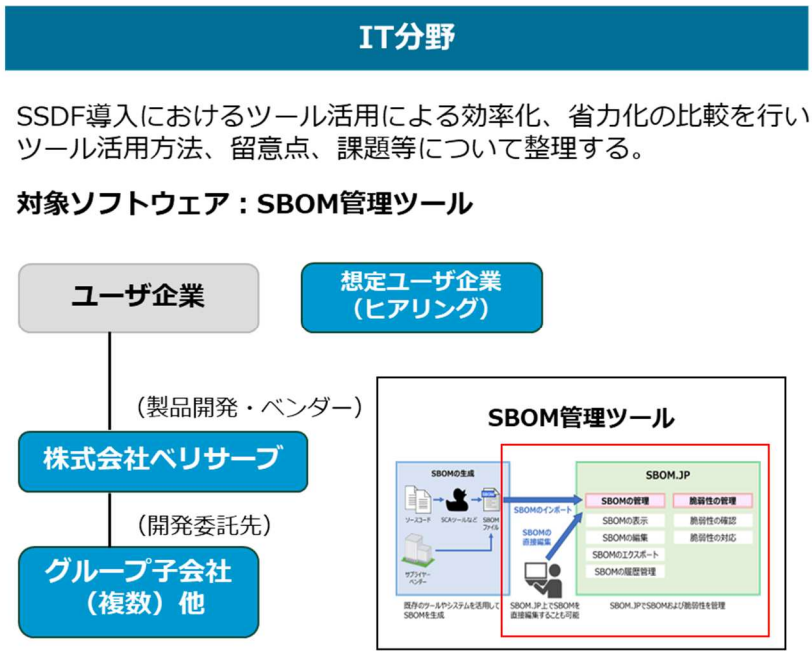


図 3-3 IT 分野の実証体制と対象システム

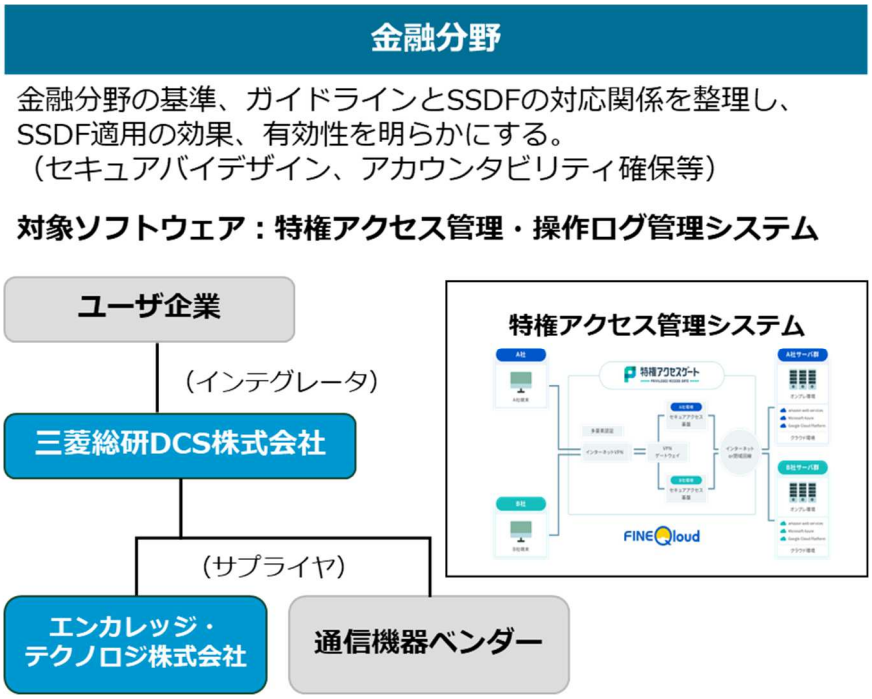


図 3-4 金融分野の実証体制と対象システム

3.5 実証の成果物の関係性

本事業において、セキュアな開発運用プロセス DevSecOps に基づくツール活用の基本モデルを整理し、それに基づき、実際の製品、システムに対する実証を行い、ツールの適用方法の整理、達成レベル目安等を検討した。

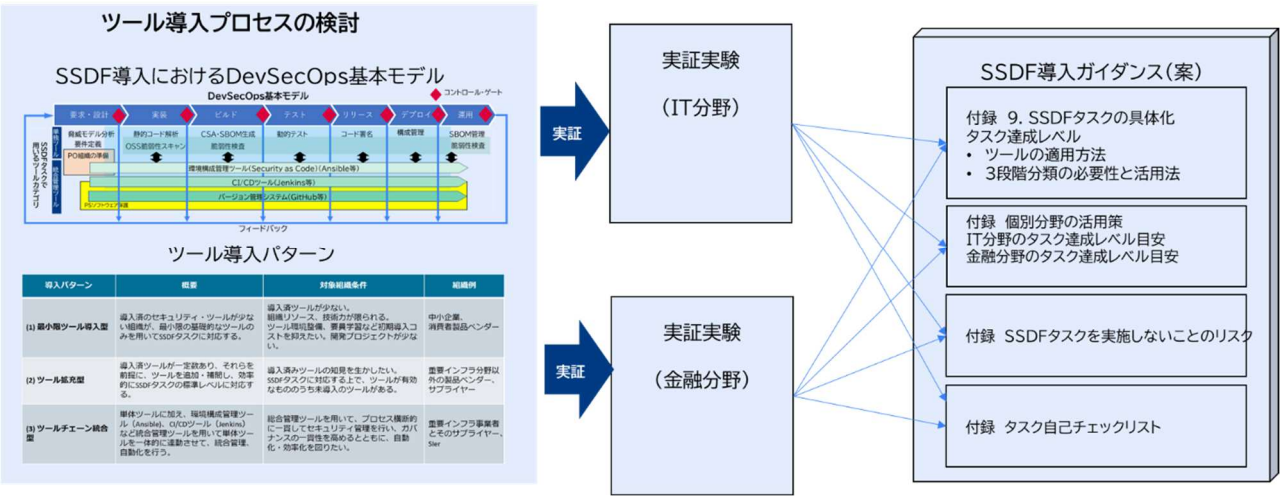


図 3-5 実証成果物の関係性

3.6 SSDF ガイダンス作成に向けた課題、実証を通じた成果の関係性

SSDF の導入に関する課題に対して、実証等を通じた取組事項の成果をとりまとめた。抽象度が高い

SSDF タスクの具体化や対策の見える化等、SSDF 導入ガイダンス案の拡充内容を整理した。

表 3-1 各課題に対する取組成果

課題	今年度取組事項	成果物・検討状況
SSDFタスクは抽象度が高く、現場普及のためには実施の具体化・効率化が必要	①ツール等を活用した効率的なSSDF導入・実践方策の整理**（実証項目）**	ツール主体で実施できるタスクを特定し、ツール適用の考え方や留意点についてSSDF導入ガイダンスにまとめた。
タスクの実施範囲は分野によって異なるため、分野の要求に応じた達成レベルの目安の提示が必要	②個別産業分野の特性に応じたSSDF対策の確認**（実証項目）**	実証結果や各分野のガイドラインの要求事項を基に、分野に応じてタスク毎に期待される達成レベルを導入ガイダンスにまとめた。
達成レベル３の位置付けについて、過度な負担と誤解を招かないような形で示すことが必要	③SSDF達成レベルの段階数の見直し検討**（実証項目）**	実証結果も踏まえ、３段階の達成レベルの識別が必要であることを示しつつ、レベル３の達成は全ての分野で求められるわけではないことを導入ガイダンスで明示した。
SSDF導入の動機付けのため、タスクを実施しないことにより生じるリスクや影響の具体化が必要	④SSDFタスクを実施しないことのリスクの明確化	タスクを実施しないことにより生じる残留リスクとそのリスクレベルを整理するとともに、SSDFの導入により期待できるリスク低減等の効果を整理し、導入ガイダンスにまとめた。
既存の国内ガイドラインでは対応が不足するタスクについて、対策の具体例の拡充が必要	⑤国内ガイドラインの不足事項への対応策の提示	既存の国内ガイドラインが包含できていないタスクについて、SSDF Referenceを参考に対策の考え方や重要性を示し、具体策の情報を拡充。
実施すべきタスク（達成すべきレベル）と達成状況を把握するためのツールが必要	⑥自己チェックリストの検討及び案の提示	実施すべきタスクとその達成状況を網羅的に把握するだけでなく、リスクベースの考え方に基づき、上記②の個別産業分野の特性に応じて重点的に対応すべきタスクや④のリスクレベルに応じて優先的に対応すべきタスクを特定し、必要な対策の検討と対策状況の可視化に活用するためのチェックリストを整備。

3.7 実証の結果とそれを踏まえた SSDF ガイダンス案への反映

実証の結果とそれを踏まえた SSDF ガイダンスへの反映について主なポイントを以下に示す。

表 3-2 実証の結果と SSDF ガイダンス案への反映

実証の結果	SSDF導入ガイダンス案への反映
SSDFタスクについて、実証対象システムに対して、ツールの選定、適用、結果の評価を行い、ツールの適用方法について整理した。 実証の結果得られた知見、留意点、課題の例: ■ **知見(例)** ➢ **(ツールチェーンの有効性)** GitHub等のソフトウェア構成管理ツールや、GitLab CI/CD等のCI/CDツールと連携可能なツールチェーン(静的コード解析、既知脆弱性検査、SBOM生成等)を活用することで、効率的・体系的にSSDFに準拠できることを確認(IT分野、金融分野) ■ 留意点(例) ➢ (開発環境のセキュリティ確保) SSDFにおいては、ソフトウェアそのもののセキュリティのみならず、開発環境ツールのセキュリティ、ツールの使用ログの監視が重視される。Ansible等の環境構成管理ツールを活用することが有効に対応できる。(IT分野) ■ 課題(例) ➢ (自動化の制限)CI/CDパイプラインを構築しても、手動のインタラクションが発生するタスク(ツール)もあり、完全な自動化は困難である。(IT分野) ➢ (SBOMツールの普及) SBOMはサプライチェーン全体を通じて整備・普及しなければ有効に活用できない課題があり、現状では部分的な効果しか得られていない。(金融)	ツール導入プロセスの当初仮説の妥当性を確認し、ガイダンス文書の推敲を行った。(**6.2.4.タスクの実践 (3)ツール導入プロセス**等) 得られた知見を、**9.付録:SSDFに対するタスク達成レベルと具体例 (5)A)ツール適用の考え方**に反映させた。(例:PW.7.1, PW.7.2, PW.8.1, PW.8.2等) 整理した留意点を**9.付録:SSDFに対するタスク達成レベルと具体例 (5)D)ツール導入時の留意点**に反映させた。(例:PO.5.1等) 特定した課題を**9.付録:SSDFに対するタスク達成レベルと具体例 (5)E)課題**に反映させた。(例:PO.4.2, RV.1.1 等)
SSDFタスクの実証を通じて、実証分野(IT分野、金融分野)における期待されるタスク達成レベル案とその判断理由について整理した。 また、金融分野について、金融庁ガイドラインとFISA安全対策基準に従い、金融分野の対策について重要事項を特定し、各ガイドラインとSSDFタスクの対応関係について整理した。	実証に基づき作成した実証分野におけるタスク達成レベルをSSDF導入ガイダンスにおける**11.付録:個別分野で期待されるタスク達成度レベル**として整理した。
実証を通じて、タスク実施のコスト(初期導入コスト、ツール費用)、効果(ツール導入による効率化)について想定値について検討した。	SSDF導入ガイダンスにおける**6.2.3(1)タスク達成レベル設定の前提の整理**のベースとした。
SSDFタスクのチェックリスト案について、実証結果について自己診断を行った。	チェックリスト案の妥当性を確認し、**6.2.5.達成度評価 (1)タスク達成レベルチェックリスト**として整理した。

4. ソフトウェアタスクフォースの運営

本項目では、上記 2 章、3 章の調査・実証及び検討に関連して、専門的な視点からの検討、分析及び助言を得るために、ソフトウェアタスクフォースを以下の要領にて運営した。

ソフトウェアタスクフォースにおいては 2 章、3 章の調査・実証を踏まえ、調査・実証結果、今年度の成果物、次年度以降の事業等について議論した。

4.1 第 16 回ソフトウェアタスクフォース

4.1.1 開催概要

第 16 回ソフトウェアタスクフォースでは、以下の議事次第と資料で議論された。

日時：令和 7 年 7 月 30 日 13:00～15:00
議事次第：
1. 開会
2. 事務局資料説明
3. 自由討議
4. 閉会

配布資料：

資料 1	議事次第・配布資料一覧
資料 2	委員名簿
資料 3	サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性
資料 4	ソフトウェアの安全な利活用に関する海外の動向
資料 5	本年度の調査・実証の進め方（詳細）

4.1.2 要旨

〇事務局から、資料3、4及び5について説明を行った。
〇各委員から、主に以下の意見があった。
＜本年度の調査・実証の進め方について＞

- 実施事項やツールの使い勝手を、実証を通してチューニングすることが重要であると認識している。供給側の目標は、コンテンツが多く利用されることであるため、実証調査では利用者側の立場で、コンテンツに関する意見や使用環境をどのように改善すればよいかについて、情報収集することが望ましい。
- 実証のスコープについて、例えば金融機関では様々な開発手法が導入されており、すべての開発手法について実証を行うことは困難であると思うが、現実に即した実証を実施いた

だきたい。また、SBOM及びSSDFは、国際的なルール、監査ルール等を含めた金融機関を統制する他のルールとの整合性を図ってもらいたい。

- SSDFは非常に範囲が広く、実施に係る労力が大きい。SSDFを実現することは、アプリケーションセキュリティを実現することと同義である。サプライチェーンの中でSSDFをベースにセキュアな製品を組み立てることは、大手メーカは可能であっても、末端でソフトウェアを提供している小規模事業者は難しいのでは。その背景には、コスト、技術、リソース及びノウハウの問題がある可能性が高い。最終製品の中には中小企業のコンポーネントが組み込まれることが多く、本取組のスコープとしてカバーしなければならない。中小企業でSSDFを導入するために、ツールの使用経験や人材の足りていない組織での実証や導入支援プログラムも必要と考える。
- SSDFに準拠する際、発注者か受注者のどちらかがコストを負担する。その際のコストとして妥当な金額の目安が公開されていれば、中小の受託会社は契約額の増分を主張できると考える。例えば、SSDFに準拠せずに開発した際の費用がいくらで、SSDFに準拠して開発した際の費用がいくらであったといった事例があるとよい。SSDFに準拠するためのベースとなる体制を作るにはどれだけのコストが必要かを明らかにすることで、体制整備等に対して補助金を交付するという議論にもつながる。
- 生成AIの進展により、ローコードツールやノーコードツールを使用しなくても、誰もがプログラムの生成を行えるようになってきた。生成AIは、インターネットに公開されているオープンソースソフトウェア（OSS）のソースを学習することで、プログラミング能力を高めているとされている。一方で、脆弱性のあるコードを生成AIが出力してしまうことが多く指摘されている。その原因の一端は、学習対象となっているコードに脆弱性が含まれていることにあると考えている。ある意味では、学習対象となるOSSのコードをSSDF対応にする必要がある。SSDF for AIという発想。AIを活用することが、良質なソフトウェアを基に開発することと同義となるように、まずはOSS開発者へのSSDFの啓発等を検討することも一案と考える。
- 補助金等の枠組みにより、中小企業がSSDFを担保するためのコストを負担できる仕組みを検討してもらいたい。オープンソースのツールでは不十分な場合も当然存在する。そのため、実証において効果の高いツールの組合せ方が明らかになれば、当該ツールの組合せを導入するためのコストを経済産業省が担保することが望ましい。
- AIが社会、特に開発の現場でどのように使用されているか、現在の状況をまず国内で調査してもらいたい。調査結果に基づいて、採るべき指針は変化すると考える。
- リソースの格差を乗り越えるために、ツールの情報は重要である。また、モチベーションの確保や対策の必要性の伝達のために、SSDFのタスクを実施しないことによるリスクを明確化して、コミュニケートすることも重要と考える。その上で、自己チェックリストを使う際に、チェックする担当者の感じる課題点や懸念点等の細かな声を吸い上げる仕組みが存在し、当該の内容がフィードバックされることが望ましい。
- IT導入補助金の対象となるツールにソフトウェア管理ツールが含まれると、円滑に経済産業省の枠組みの中で補助金の交付が可能となるのでは。ひとつのアイデアとして受け止めてもらいたい。

- SSDF及び関連するガイドラインは、地域のSI事業者等にはあまり浸透していない。認知度に関する、現場の立ち位置や財務的な制約を考慮した投資可能額等についての質問調査を実施して、現状を把握し、その結果を踏まえてプロモーションについて議論することが望ましい。
- チェックリストの利用は有効であると認識しているが、ソフトウェアを提供する会社は、様々な負荷が重い対応を実施しているため、全体感を踏まえた認証の統一や差分認証を視野に入れた調査研究を行ってもらいたい。また、省庁等の政府機関がチェックリストを守れるかも論点となる。
- SSDF、SBOM等は、各事業者がISO／IEC27000シリーズに準拠した取り組みを行うこととは異なる性質を有する。中小企業が補助金を交付されても、SSDFの導入は限定的な範囲に留まると考える。大小を問わずベンダーは世界も相手にしており、本当に役に立つという確信がない限り、ルールは定着しない。ルールを実施せよと命じればあらゆる事業者が実施するという発想からの転換が必要。ISO／IEC27000シリーズですら、定着までに数十年の時間がかかり苦労を要した。
- 中小企業がツールを使用することを想定すると、コストだけでなく、グローバルで通用するか、国産であるかなど、ツールの選定基準も論点となる。例えば、工数削減の効果の高いツールを選ぶという趣旨がある場合は、その旨の記述が必要。様々な可能性を踏まえて、どのような母体や選定基準でツールを選定したのか明らかにするとともに、ツールに関する不満点やあるべき仕様を調査で明らかにすることができれば、当該情報を開発ベンダーのイノベーション促進のために活用できると考える。
- 中小企業におけるセキュリティ対策の底上げという観点から考えると、SSDFは、どのような対策をどの程度まで実施するかを議論するための材料となる。発注者と受注者の間で、実施事項や考慮事項を相談する際、SSDFベースで確認することになる。サプライチェーン全体又は会社全体という規模で対策を実施する場合は、コスト及び負担が大きくなるので、まずはプロジェクト、製品又はサービスの単位で実施事項を議論して効果を確認することもひとつの方策と考える。
- 生成AIについては、バイブコーディングと呼ばれる手法の登場により、品質を担保しないのであればプログラムの量産が可能な土壌ができている。一方で品質を担保するには、既存の開発手法と同様にレビューポイントを設けて人がチェックすることが必要であると、一般社団法人情報サービス産業協会（JISA）の勉強会で議論した。勉強会の中では、プロンプトの調整によって品質向上を目指す取組も実施した。生成AI自体の成熟に伴い、利用者の開発手法や契約形態等に様々な変革が生じる可能性を踏まえ、JISAがまとめた提言もあるため参考にしてほしい。
- サプライチェーンやメンテナンスの領域においてSSDFの適用対象となり得るソフトウェアについて、分かりやすく伝えていかなければならない。現在の議論では全てのソフトウェアを対象としているが、例えばカスタムアプリ（システムインテグレーションで開発した業務アプリケーション等）については、自社内で使用するものと顧客に提供するものとの間にも違いがある。
- AIに関しては、システムの重要な部分の脆弱性を検査するためのAIエージェントを強化す

る取組に対し、国として支援を検討することが望ましいのでは。

＜取組の全体像について（次年度に向けた論点）＞

- 先行して取り組みを成功させている海外の事例について、なぜ成功しているか、環境、金銭の流れ、能力等に焦点を当てて情報を得たい。
- 政府調達等での要件化等ではなく、自己チェックリストの検討とするのは、米国の取組の後退が背景にあると理解している。しかしSSDFを普及させるためには、政府調達での要件化が効果的ではないか。自治体等も含めた政府調達により、地方のSI事業者等への普及が進むと考える。導入の仕方の塩梅は論点であり、いきなり高いハードルを課すとハレーションを起こすため、比較的低いレベルから開始することが効果的ではないか。
- AI－SBOMに関する国際的な議論と国内の議論の整合性について注視することが望ましい。

4.1.3 会議運営業務

会議運営業務として、日程調整、事前説明、Web 会議環境確保、資料準備、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。

4.2 第 17 回ソフトウェアタスクフォース

4.2.1 開催概要

第 17 回ソフトウェアタスクフォースでは、以下の議事次第と資料で議論された。

日時：令和 8 年 1 月 22 日 13:00～15:00

議事次第：

1. 開会
2. 事務局資料説明
3. 有識者講演
4. 自由討議
5. 閉会

配布資料：

資料 1　議事次第・配布資料一覧

資料 2　委員名簿

資料 3　サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性

資料 4　SSDF 導入ガイダンスのあり方について

資料 5　AI を活用した SW 開発への対応に関する有識者講演資料（委員限り）

参考資料 1　ソフトウェアの安全な利活用に関する海外の動向

参考資料 2　セキュア・ソフトウェア開発フレームワーク導入ガイダンス（案）（委員限り）

参考資料 3　セキュア・ソフトウェア開発フレームワーク導入ガイダンス付属ツール等（案）（委員限り）

4.2.2 要旨

〇事務局から、資料3及び4について説明を行った。
〇株式会社エーアイセキュリティラボ　青木代表取締役社長から、資料5について説明を行った。
〇各委員から、主に以下の意見があった。
＜SSDF導入ガイダンス案に対する改善案について＞

- SSDF導入プロセスでは様々な段階で分散的にツール導入プロセスが実施される可能性があるのではないか。また、SSDFのRV．2．1の「脆弱性情報の収集と分析の実施」に対応するツールカテゴリとしては、SBOM管理ツールだけでなく、SBOMに非対応の脆弱性データベース検索ツールやセキュリティーレポート情報収集管理ツールなども含まれるのではないか。
- 参考資料2の「セキュア・ソフトウェア開発フレームワーク導入ガイダンス案」において、対象読者の項に具体的な想定読者・組織を指定することが望ましい。
- 既に関連分野の前提知識を有している人がツールについて学習する場合、学習時間が抑制できる可能性がある。この点を踏まえてツールの学習時間の目安を提示することが望ましい。
- SSDFのタスクを担う主体を整理するにあたって、「技術者」を「開発者」「インフラ構築者」「セキュリティ技術者」等に細かく区分することが望ましい。
- 環境構成管理ツールの紹介にあたり、ツール利用時のイメージが湧くようになるよう、Ansibleのプレイブックや Dockerfileのベストプラクティス等を参考情報として合わせて記載するよう改めることが望ましい。
- 国内ガイドラインにおける不足事項への対応策の提示にあたって、米国では規定されていない、より厳格な項目が日本で規定されてしまうと、日米の平仄が合わなくなってしまうおそれがある。十分な検討が必要。
- SSDFで利用できるツールには条件付きで、無償で使用できるものがあるため、その旨を記載しておくことが望ましい。また、中小企業の導入支援において、有償の方がサポート体制等の面で有益である場合もあるので、その旨も言及することが望ましい。さらに、中小企業は当初からツールチェーンを一括で導入しない場合があることも想定されるため、個別のツールの組み合わせの事例等が紹介されているとより有益と考える。
- SSDFのタスクを実施しない場合のリスクとして、プラクティス単位でキーワードだけを抽出した一枚の資料があると、SSDFによってリスクがどのように改善されるか一目でわかるようになると考える。
- ＜SSDF導入ガイダンスの活用策＞
- 米国のSSDFは米国の政府調達のために作成されたガイドである。日本においても、SSDF導入ガイダンスについて日本の政府調達で実証することが適切であると考える。
- 米国や欧州では、政府が資金を拠出して作成させたシステムやソフトウェアは、政府調達とすることが一般的。日本においても、政府が資金を拠出したシステムやソフトウェアは政府が率先して利用すべき。
- 金融機関は、現在金融庁のガイドラインへの対応を優先して実施しているため、SSDFに

ついては金融庁のガイドラインとの対応箇所から実施を進めてもらうことが望ましいと考える。

- 政府調達におけるSSDFの活用は是非進めてもらいたい。
- プロモーションの一環として、企業が自己適合チェックを簡易に実施できるウェブサイトを作ってはどうか。
- 政府調達においては、省庁がシステムやアプリケーションの調達に伴う入札を実施する際に、SSDFに準拠している入札者に対して加点することを検討するとよい。
- 近年は多様なガイドラインが公表されており、ガイドライン間の関係についてマッピングなどは提供されるものの、直ちに明らかではない場合もあり、困惑している人は多い。更に体系立ててガイドライン間の関係を整理することが必要な時期が到来しているのではないか。
- 構造的制約やリソース不足によってSSDFへの対応が後回しになってしまう事象は、往々にして発生する。特にリソースが不足している事業者におけるSSDFの普及及び実装を進めるためには、完璧な実装を要求せず、レベル分け等を設定することが有効。スモールスタートを実施するための最低限度の基準を設定することも一案である。
- SSDF等に関連する仕組みや政策等の対象として、政府調達を実施するようなかっちりとしたシステム開発物が想定されているように感じる。対象としてどのような開発物を想定するかは論点であると考える。
- SSDFの普及に関しては、事業者がSSDFへの対応の達成度を他者にアピールできるようにする必要があると考える。
- 社会実装を進めるためには契約や合意が必要であるが、それらの概念について、ガイダンスでは具体的かつ詳細に解説されていないため、次年度以降具体化する作業を進めてもらいたい。また、テーラリングができる人材を育成することについても検討してもらいたい。

＜次年度以降の取組について＞

- AI駆動開発に係るセキュリティに関する検討は、AIそのもののあり方にもかかわる論点を扱うものと承知している。そのため、AI関連の政策を立てている部局とも適切に情報共有しながら作業を進めていくことが望ましいと考える。
- AI駆動開発は、システム開発の効率化や省人化といったポジティブな側面だけでなく、開発者の裾野を大幅に広げ、脆弱性のあるソフトウェアが大量に頒布されてしまうというネガティブな側面もある。技術面だけでなく政策面でも様々な手当てが実施されることが望ましい。
- AI駆動開発に関する検討が重要であることは理解するものの、継続検討が必要とされていたプロモーションを優先して実施すべき可能性があると考える。検討の内容を拡張していくよりも、SBOMの普及策に焦点を当てるべきではないか。
- 狭義の開発だけでなく、関連する開発・運用・検査等の各フェーズにおいてどのようにAIが活用され、どのような課題があるのか、概観の整理をすることが望ましい。
- 昨今の生成AIの悪用の事例を鑑みると、生成AIは誰でも悪用できるという状況を前提として、悪用への対策をルール面と規則面から論じていくことが求められるのではないか。
- AI駆動開発については、多くのレポートで指摘されているところではあるが、品質を担保するための仕組みについての調査及び実証が必要ではないか。

4.2.3 会議運営業務

会議運営業務として、日程調整、事前説明、Web 会議環境確保、資料準備、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。

5. 英訳

第17回ソフトウェアタスクフォースにおいて、セキュア・ソフトウェア開発フレームワーク導入ガイダンス案に対する議論、検討の結果修正した改訂版に対して、英訳を行った。

6. 総括

第 2 章では、ソフトウェア・セキュリティに関する国内外の動向調査、SSDF、SBOM、AI 等に関する技術動向、課題、対策等に関する整理を行った。

第 3 章では、ソフトウェア利活用に関わるセキュリティリスク、課題及び対応策いついて調査、実証を行い、それらの知見を SSDF 導入ガイダンス（案）としてとりまとめた。

第 4 章では、第 1、2 章の調査・実証及び検討に関連して、企業の現場及び専門的な視点からの検討、分析を行うために、ソフトウェアタスクフォースを運営し、ソフトウェア管理手法、脆弱性対応、AI リスク、OSS の利活用等について議論をした。

第5章では、第3章で取りまとめた SSDF 導入ガイダンス（案）の英訳を行った。

令和7年度産業サイバーセキュリティ対策の強化に向けた環境整備事業
（ソフトウェアのセキュリティ確保等に関する調査） 報告書 - 第１編
ソフトウェアの安全な利活用に向けた調査・実証

2026年３月

株式会社三菱総合研究所
安全保障政策本部
TEL (03)6858-3578

経済産業省 御中

令和7年度産業サイバーセキュリティ対策の強化に向けた環境整備事業
（ソフトウェアのセキュリティ確保等に関する調査）

報告書 - 第２編

宇宙 SWG 関連

三菱総合研究所

安全保障政策本部

2026 年 3 月 31 日

目次

図 目次

表 目次

1. はじめに

本事業では、産業サイバーセキュリティ研究会 WG1 の下の産業分野別 SWG として令和 3 年 1 月に立ち上げた「宇宙産業 SWG 会議」を開催した。また、民間宇宙事業者におけるサイバーセキュリティ対策に関する課題等の調査・分析・整理を実施した。

2. 検討会の運営

産業サイバーセキュリティ研究会 WG1 の下の産業分野別 SWG として令和 3 年 1 月に新たに立ち上げた「宇宙産業 SWG」を開催した。今年度は、議題の趣旨を踏まえて構成員を見直したうえで、宇宙産業 SWG 第 9 回を開催した。

2.1 宇宙産業 SWG の構成員

今年度見直しを行った宇宙産業 SWG 委員を以下に示す。昨年度までの活動成果や宇宙を取り巻く環境変化を踏まえ、SWG の位置づけを見直した。関係府省庁との連携を高めつつ、民間宇宙事業者中心で、宇宙分野におけるサイバーセキュリティのあり方について議論するために、下線で示す 16 名を新たに追加し、会議を開催した。

	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 一般社団法人 Japan Space ISAC
	倉原　直美	株式会社インフォステラ 代表取締役 CEO
	小出　祐輔	株式会社 Synspective Manager of Security and IT 一般社団法人 Japan Space ISAC
	國母　隆一	株式会社アクセルスペース 執行役員 / Co-CTO（情報技術担当）
座長	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	独立行政法人情報処理推進機構（IPA） 産業サイバーセキュリティセンター 専門委員 一般社団法人 Japan Space ISAC
	佐々木　勇人	一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC） 政策担当部長 兼 早期警戒グループマネージャ
	新谷　美保子	TMI総合法律事務所パートナー（弁護士）
	鈴本　遼	株式会社アークエッジ・スペース 執行役員
	高見　穣	独立行政法人情報処理推進機構 セキュリティセンター リスクマネジメント部 制御システムグループ グループリーダー
	多賀　正敏	国立研究開発法人宇宙航空研究開発機構（JAXA） セキュリティ・情報化推進部 セキュリティ統括課 課長
	竹貝 朋樹	日本電気株式会社 エアロスペース・ナショナルセキュリティビジネスユニット スペースプロダクト統括部 シニアプロフェッショナル
	田中　周一	株式会社 QPS 研究所
	田中　洋吏	三菱電機株式会社 鎌倉製作所 宇宙総合システム部 セキュリティ技術課 課長
	谷口　貴之	株式会社 Space Compass
	名和　利男	日本サイバーディフェンス株式会社 最高技術責任者（CTO）

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
水野　勝成	スカパーJSAT 株式会社
八木　晴信	株式会社アストロスケール　Cyber Security Manager

（オブザーバー）
内閣官房 国家サイバー統括室、内閣府 宇宙開発戦略推進事務局、総務省、防衛省、文部科学省

2.2 宇宙産業 SWG(第 9 回)の開催概要

宇宙産業 SWG(第 9 回)の開催概要は以下に示すとおりである。

まず、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、事務局より紹介した後、国内における既存の取組として、経済産業省、IPA、内閣府及び一般社団法人 Japan Space ISAC の取組を紹介した。その後、自由討議において、各取組に関する討議や今後望まれる施策等を議論した。

日時：令和 7 年 9 月 4 日(木) 16 時 30 分～18 時 00 分
場所：三菱総合研究所本社会議室

議題
1. 開会
2. 宇宙産業 SWG 委員の紹介
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
   (1) 諸外国における政策動向・脅威動向について
4. 国内における既存の取組について
   (1) 経済産業省における取組
   (2) IPA における取組
   (3) 内閣府における取組
   (4) 一般社団法人 Japan Space ISAC における取組
5. 自由討議
6. 閉会

3. 民間宇宙事業者のサイバーセキュリティ対策に関する課題等の調査・分析・整理

国内外の関連規格・制度等についての調査・分析を行うとともに、「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」の更新も視野に入れつつ、課題の調査・分析を行った。そして、これらの調査結果を踏まえ、今後必要な取組についての検討・整理を行った。

3.1 国内外の取組に関する調査

3.1.1 近年の取組動向に関する調査

宇宙分野におけるサイバーセキュリティに関する近年の国内外動向について調査を行った。調査対象とした取組等を表 3-1 に示す。

表 3-1 調査対象とした国内外の取組動向一覧

No	動向名称	時期	国・地域	取組主体	概要
1	宇宙システムの地上セグメントに関する技術指針「BSI TR-03184-2 Informationssicherheit für Weltraumsysteme - Teil 2: Bodensegment」[1]	2025年5月	ドイツ	ドイツ連邦情報セキュリティ庁（BSI）	地上セグメントに対してサイバーセキュリティ対策を実施するための手順が示されている文書。

[1] BSI, BSI TR-03184-2 Informationssicherheit für Weltraumsysteme – Teil 2: Bodensegment
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03184/BSI-TR-03184-2.pdf?_blob=publicationFile&v=3

No	動向名称	時期	国・地域	取組主体	概要
2	トランプ大統領による改正大統領令の発表[2]	2025年6月	米国	ホワイトハウス	バイデン元大統領が退任直前の2025年1月16日に発表した国家のサイバーセキュリティ強化とイノベーション促進を目的とした大統領令（Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity）の一部を見直す改正大統領令。
3	Secure Space Act 2025 法案の提出[3]	2025年6月	米国	ベン・レイ・ルハン上院議員及びデブ・フィッシャー上院議員	「外国の敵対者」（foreign adversary）の影響下にある事業体が提供または使用する静止軌道衛星システム・非静止軌道衛星システムや地上局に対して、連邦政府通信委員会（FCC）が衛星ライセンスや米国市場へのアクセスを付与することを禁止する法案を上院に提出。
4	NASAのサイバーリスク管理に対するGAOのレビュー[4]	2025年6月	米国	米国政府監査局（GAO）	米国GAOはNASAに対し、主要プロジェクトにおいて、NIST RMFが完全に実施されていないと指摘し、主要なリスク管理活動を徹底するよう求める16の勧告を実施。

[2] White House, "Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity," https://www.federalregister.gov/documents/2025/01/17/2025-01470/strengthening-and-promoting-innovation-in-the-nations-cybersecurity 、White House "SUSTAINING SELECT EFFORTS TO STRENGTHEN THE NATION'S CYBERSECURITY AND AMENDING EXECUTIVE ORDER 13694 AND EXECUTIVE ORDER 14144" https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/ 、White House "Fact Sheet: President Donald J. Trump Reprioritizes Cybersecurity Efforts to Protect America" https://www.whitehouse.gov/fact-sheets/2025/06/fact-sheet-president-donald-j-trump-reprioritizes-cybersecurity-efforts-to-protect-america/

[3] Congress, "S.1962 - Secure Space Act of 2025" https://www.congress.gov/bill/119th-congress/senate-bill/1962/text

[4] GAO, "CYBERSECURITY NASA Needs to Fully Implement Risk Management" https://files.gao.gov/reports/GAO-25-108138/index.html

No	動向名称	時期	国・地域	取組主体	概要
5	EU Space Act(EU 宇宙法案)の発表[5]	2025 年 6 月	EU	欧州委員会(EC)	EU 域内における宇宙活動の安全性・強靭性・持続性を確保しつつ、EU の宇宙産業の競争力向上を目的として、法案を発表
6	宇宙領域防衛指針と防衛省次世代情報通信戦略[6]の策定	2025 年 7 月	日本	防衛省	宇宙での脅威拡大に対応し、衛星による戦況把握や通信確保、航空宇宙自衛隊への改称等を進める「宇宙領域防衛指針」と意思決定の優越やレジリエンス強化を目指し、新たな防衛情報通信基盤の整備を掲げる「防衛省次世代情報通信戦略」を策定。
7	CNSSP 12、CNSSI 1200、CNSSI 1253 AF-A2 の改定[7]	2025 年 8 月	米国	国家安全保障局(CNSS)	大統領令 14144、14306 に基づき、CNSS が宇宙のサイバーセキュリティに関する 3 文書を見直し。

[5] EUROPEAN COMMISSION, "REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the safety, resilience and sustainability of space activities in the Union"
https://defence-industry-space.ec.europa.eu/EU Space Act(EU 宇宙法案) en

[6] 防衛省, "宇宙領域防衛指針と防衛省次世代情報通信戦略の策定について",
https://www.mod.go.jp/j/press/news/2025/07/28a.html

[7]CNSS, "CNSSP 12, Cyber security Policy for Space Systems Used to Support National Security Missions"
https://www.cnss.gov/CNSS/openDoc.cfm?a=pFxntaV2LyhMbctwgkAIDg%3D%3D&b=183D183987312F6620FB71BC74784ABD2970D05F55FF951266C5742E4BABA9317BB5E17007C3C27CD57937FDFA7FCADC

CNSS, "CNSSI 1200: National Information Assurance Instruction for Space Systems Used to Support National Security Missions"
https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2025/12/cnssi-1200.pdf?rev=b887f8cf41dc4e29913da872329bf5a1&hash=2E34079EA288E6D3C17AB53E1C60EEB3

CNSS, "CNSSI 1253F Attachment 2 Space Platform Overlay"
https://www.cnss.gov/CNSS/openDoc.cfm?a=RRZJYoyM2bQd7D5IvR1HqQ%3D%3D&b=92D827857DCCDB2934A511E782B4209A1317F4169C9D232C5F0DD1E0B44D88C1191875FB93D8377A24E6521C9762D42E

No	動向名称	時期	国・地域	取組主体	概要
8	宇宙能力の確立を目的とした国家宇宙戦略(National Space Strategy 2025-2040)の発表[8]	2025年11月	フランス	宇宙軍(Space Systems Command)	宇宙領域を国家主権・安全保障・経済競争力の中核インフラと位置づけ、2040年までに欧州およびフランスの自律的かつ競争力ある宇宙能力を確立することを目的とした国家宇宙戦略。
9	ドイツにおける宇宙戦略文書(Space Safety and Security Strategy)の発表[9]	2025年11月	ドイツ	ドイツ連邦政府	宇宙が平時のインフラ基盤であると同時に、危機・ハイブリッド事態から武力紛争までを見据えた戦略競争の場になりつつあるとの認識に立ち、民生・軍事の両面でドイツが宇宙領域で長期的に行動できる能力を確保することを目的とした戦略。
10	武力紛争期間における宇宙セクターを狙ったサイバー活動に関する調査結果の発表[10]	2025年11月	スイス	ETH Zürich CSS	宇宙セクター(衛星・地上局・関連企業/機関・サプライチェーン等)を狙ったサイバー活動を、公開情報のみで体系的に整理したレポート。

[8] Republique Francaise, "National Space Strategy 2025-2040" https://www.sgdsn.gouv.fr/files/files/Publications/National%20space%20strategy%202025%20-%202040.pdf

[9] Federal Foreign Office, "Space Safety and Security Strategy" https://www.auswaertiges-amt.de/en/newsroom/news/space-safety-and-security-strategy-2744368 、https://www.bmvg.de/resource/blob/6042580/128dbebd8cce8d7b8e61eb680edf91ad/weltraumsicherheitsstrategie-2025-en-data.pdf

[10] ETH Zürich, "Breaking the Final Frontier: Cyber Operations Against the Space Sector", https://css.ethz.ch/en/center/CSS-news/2025/11/breaking-the-final-frontier-cyber-operations-against-the-space-sector.html

No	動向名称	時期	国・地域	取組主体	概要
11	Satellite Cybersecurity Act 再提出と商用衛星サイバー対策の強化[11]	2025年12月	米国	米国上院	商務省が関係機関と連携して衛星向けの任意のサイバー推奨策を策定し、企業が参照できる公開のオンライン窓口を整備すること、GAO が取組の重複や重要インフラ分野との関係を調査することを求めた法案。
12	Kombinierte Prüfvorschrift für TR-03184（宇宙システム向け統合試験仕様）の公開[12]	2026年1月	ドイツ	ドイツ情報セキュリティ庁（BSI）	宇宙システムのセキュリティ要件（TR-03184-1、TR-03184-2）について、どの項目をどの程度の深さで評価すべきかを示した適合性評価（試験）ガイドライン。
13	Cyber Security Framework and Guidelines for Space Including Satellite Communication の公開[13]	2026年2月	インド	CERT-In	インドの宇宙・衛星通信エコシステム全体を対象に、脅威分析からセグメント別対策、インシデント対応、統治・監査までを体系化した包括的な基準書。
14	Securing space – Cyber security for LEO SATCOM の公開[14]	2026年3月	オーストラリア等4か国	豪州宇宙庁、カナダ Cyber Centre、米 NSA、ニュージーランド NCSC	低軌道衛星（LEO）利用者向けのガイダンス。

以降では、それぞれの取組について詳説する。

[11] Sen. Peters, “S.1425 - Satellite Cybersecurity Act”, https://www.congress.gov/bill/118th-congress/senate-bill/1425/text

[12] BSI, “Technische Richtlinie TR-03184: Prüfanforderungen für Weltraumsysteme”, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03184/BSI-TR-03184.pdf?__blob=publicationFile&v=2

[13] CERT-In, SIA-India, “Cyber Security Framework and Guidelines for Space Including Satellite Communication”, https://www.cert-in.org.in/PDF/CyberSecurityFrameworkGuideline for space.pdf

[14] The Australian Signals Directorate’s Australian Cyber Security Centre (ASD’s ACSC), “Securing space”, https://www.cyber.gov.au/business-government/secure-design/securing-space

(1) 宇宙システムの地上セグメントに関する技術指針「BSI TR-03184-2 Informationssicherheit für Weltraumsysteme – Teil 2: Bodensegment

2025 年 5 月、ドイツ連邦情報セキュリティ庁(BSI)は、宇宙システムの地上セグメントに関する技術指針「BSI TR-03184-2 Informationssicherheitfür Weltraumsysteme-Teil 2: Bodensegment」を公表した。

本文書では、表 3-2 に示すように対象範囲として、バス機器と接続される地上の衛星管制センター、遠隔測定・追跡・コマンドに用いる運用地上セグメント、通信ネットワーク(WAN)が挙げられており、地上セグメントに対してサイバーセキュリティ対策を実施するための手順が示されている。

表 3-2 想定されるビジネスプロセスと対応するアプリケーション

ビジネスプロセス	対応アプリケーション
構想・設計	ソフトウェア・ハードウェア試験ツール
生産	ソフトウェア・ハードウェア試験ツール、衛星モデリング、シミュレーター
運用準備	ソフトウェア・ハードウェア試験ツール、シミュレーター、人員のトレーニングシステム
運用	ソフトウェア・ハードウェア試験ツール、ソフトウェア管理ツール、アンテナ制御アプリケーション、アンテナ管理、人員のトレーニングシステム、衛星モデリング、シミュレーター、運用システム
運用停止	運用システム

特に、表 3-3 に示すように、宇宙分野におけるビジネスプロセスとアプリケーションの対応関係を明示することで、保護すべき IT 資産の特定と必要な対策の導出手順を示し、想定されるリスクシナリオごとに、どのビジネスプロセスやアプリケーションが影響を受けるのかを可視化した例が示されている。

なお、本指針は、2023 年 5 月に発表された「TechnischeRichtlinieBSI TR-03184 Informationssicherheitfür Weltraumsysteme[15]」をさらに詳細化した内容となっている。

表 3-3 リスクシナリオ(例)

項目	詳細
シナリオ	技術的な不具合により搭載ソフトウェアの管理が中断され、仕様から逸脱したソフトウェアが衛星に搭載される。
影響のあるプロセス	運用
被害	情報の完全性の喪失
対応策	• ソフトウェアサプライチェーンの完全性確認 • 通信の暗号化 • 送受信情報の完全性確認 等
原因	技術的なミス

[15] 2023 年 7 月に BSI が公表した、衛星単体ではなく、地上局や通信リンクを含む宇宙システム全体を対象に、脅威分析に基づくセキュリティ要件と対策を体系化した指針。

（2） トランプ大統領による改正大統領令の発表

バイデン大統領は、退任直前の 2025 年 1 月 16 日に、国家のサイバーセキュリティ強化とイノベーション促進を目的とした大統領令（Executive Order on Strengthening and Promoting Innovation in the Nation’s Cybersecurity）を発表した。表 3-4 に示すように本大統領令には、民間宇宙システムの政府調達に関する連邦調達規則（FAR）の改定や、CNSS 文書の見直し・更新など、宇宙セキュリティに関する事項も含まれている。

その後、2025 年 6 月 6 日に発表されたトランプ大統領による改正大統領令では、AI や耐量子技術に関する政策の一部が撤回されたものの、宇宙関連政策の見直しは盛り込まれておらず、当面はバイデン大統領令の内容が維持されると考えられる。

表 3-4 大統領令中の宇宙分野に関連する記載（概要）

大統領令内の宇宙分野に関する記載の要約	● 民間宇宙システムのサイバーセキュリティ要件を強化（180 日以内に FAR 見直し・契約条項更新を勧告、リスクベースで軌道上・リンクセグメントに適用、指令制御保護・異常検知回復・安全な開発手法を要求） ● FAR 審議会が勧告を踏まえ、適用法に合致する場合は共同で FAR 改正を実施 ● 政府の宇宙地上システムについて、120 日以内に調査（インベントリ、主要情報システム該当性、改善提案）し、OMB が 90 日以内に準拠確保措置を実施 ● 国家安全保障宇宙システムについて、210 日以内に CNSS が政策・指針を見直し、侵入検知、セキュアブート、パッチ管理等の要件を整備

（3） Secure Space Act 2025 法案の提出

2025 年 6 月、ベン・レイ・ルハン上院議員及びデブ・フィッシャー上院議員は、「2019 年安心で信頼できる通信・ネットワーク法」（Secure and Trusted Communications Networks Act of 2019）の改正法案を上院に提出した。

本法案は、「外国の敵対者」（foreign adversary）の影響下にある事業体が提供または使用する静止軌道・非静止軌道の衛星システムや地上局について、連邦政府通信委員会（FCC）が衛星ライセンスや米国市場へのアクセスを付与することを禁止するものである。本法案が可決された場合、安全保障上のリスクとみなされる外国政府の影響下にある宇宙関連企業は、米国市場への参入が制限される見通しである。現在、本法案は上院商務・科学・運輸委員会において審議中である。

（4） NASA のサイバーリスク管理に対する GAO のレビュー

2025 年 6 月、米国 GAO は NASA に対し、主要プロジェクトにおいて、表 3-5 に示すように NIST RMF[16]が完全に実施されていないと指摘し、主要なリスク管理活動を徹底するよう求める 16 の勧告を

[16] 政府情報システムにおいて、NIST SP 800-53 の管理策を実装するために、実施すべき項目として参照されている。政府情

実施した。勧告に対して、NASA は今後の取組に関するコンプライアンスを表明し、指摘事項に対する賛否や対応方針を示している。

表 3-5 NASA のサイバーリスク管理に対する GAO のレビュー

RMF Step	実施状況	GAO が指摘した具体的な不足項目
1.準備	部分的	組織全体のリスク評価の欠如
		継続的監視戦略の不備
2.分類	部分的	影響度の不整合
		変更理由の記載不備
3.選択	部分的	ベースライン更新の不適用
		責任の不明確さ
4.実装	実施済	
5.評価	部分的	評価結果の記載不備
		組織共通の管理策のガイダンス不備
		POA&M[17]の遅延
		POA&M のリスクレベル不備
6.認可	部分的	品質管理の情報不備
		重要情報の記載不備
7.監視	部分的	システムレベルのポリシー不備
		ガイダンスの不足

(5) EU Space Act(EU 宇宙法案)の発表

2025 年 6 月、欧州委員会(EC)は、EU 域内における宇宙活動の安全性・強靭性・持続性を確保しつつ、EU の宇宙産業の競争力向上を目的として、EU Space Act(EU 宇宙法案)に関する法案を発表した。本法案は、安全性・強靭性・持続性の 3 本柱を軸としており、EU 加盟国に拠点を置く事業者だけでなく、EU 域外に設立された事業者であっても、EU 域内で宇宙サービスやデータを提供する場合には適用対象となる。これらの第三国事業者には、EU 域内の法的代理人の設置、技術的適合性の確認、e 証明書の取得などが義務付けられている。

また、サイバーセキュリティは強靭性の重要な要素として位置付けられ、本法は NIS2 指令に優先する特別法(lex specialis)として、事業者に対し、リスク評価、インシデント対応、暗号化、復旧計画などの義務を課している。表 3-6 にサイバーセキュリティに関する事項を抜粋した。

報システムにおいて、OMB(行政管理予算局)が NIST RMF の実践を監督している。米国の宇宙・防衛調達では CNSSI 1253 を通じて RMF が前提化しており、日本の宇宙事業者にとっても RMF の実践は国際連携の実務要件となりうる。

[17] 是正措置およびマイルストーン計画。指定された期日までにセキュリティ対策の実装が間に合わない場合に、POA&M の提示により、期日の猶予を得ることができる。

表 3-6 サイバーセキュリティに関する EU 宇宙法案 の概要

Article 75: NIS2 指令及び CER 指令との関係	● 本法は、**宇宙事業者に関するサイバーセキュリティ管理措置の適用は NIS2 指令の特別法(lex specialis)となり、NIS2 より優先して適用**される。 ● **CER 指令とは補完的な適用**が定められており、**宇宙事業者が CER 指令で重要エンティティに指定された場合でも両者の規制が連携・調整される**。 ● 宇宙活動に関するリスク評価及び情報共有は、主管当局間の具体的な協力・連携義務が明記されている。
Article 76: 宇宙ミッションのライフサイクルを通じたリスク管理	● 宇宙ミッションの全ライフサイクルを通じて、**ネットワーク及び情報システムのセキュリティ、物理インフラの保護の両面にわたるリスク管理措置を講じることが義務付けられる**。 ● 宇宙インフラのレジリエンス確保とミッションの統制維持を可能にするために、**事業の規模やリスクの大きさに応じた適切で幅広い対策を行う義務を負う**。
Article 77: 組織的観点	● 宇宙事業者の経営陣は、サイバーや物理的リスクへの対策が適切に行われているかを監督し、最終的な責任を負う。また、職員全体がセキュリティに関する責任を理解・遵守するよう、採用・処分を含めた人的リスク管理体制を整備する必要がある。
Article 78: リスク評価	● ミッションの全期間を通じて、サイバーや物理的リスクを把握・評価し、必要に応じて対策計画を作成する義務がある。欧州委員会は、これを補完するための基準や方法(リスクシナリオ、脅威モデリング等)を委任法で策定できる。
Article 79: リスクマネジメントの簡素化	● **小規模な宇宙事業者等は、特定の高リスク資産・機能に限定して簡易なリスク管理を適用**できる。 ● 対象事業者は各国当局から EU 機関へ報告され、監督の一体化が進められる。要件は最新技術に合わせて更新され得る。
Article 80: 宇宙インフラの情報及び資産の特定と管理	● **宇宙インフラに関連する情報及び物理的資産の特定、分類、管理に関するポリシーを整備・維持し、最新の状態に保つ**義務を負う。これには、情報の機密性・完全性・可用性に応じた分類、物理的位置やクラウド利用状況の把握を含む資産台帳の作成が含まれる。
Article 81: アクセス権の管理と制御	● システムや資産への物理的及び論理的アクセスを管理するための識別・アクセス管理プロトコルを実装しなければならない。これにはアクセス権の発行・変更・取消、監査が含まれる。
Article 82: 物理的レジリエンスの確保	● 地上インフラや関連資産の物理的なレジリエンス(耐性)を確保する技術的・組織的措置を講じる必要がある。これは CER(重要エンティティ)指令との補完的関係にある。
Article 83: インシデントの検知と監視	● **異常・インシデントを常時監視し、検知するシステムを導入**しなければならない。 ● セキュリティイベントは分離された監視システムに通知される必要がある。
Article 84: 予防及び防御措置	● 指令系、状態監視、通信機器に対する技術的制御を安定的に維持するために、**宇宙ミッションの特性およびリスク評価に基づき、宇宙機および地上セグメントに対して適切なサイバー対策を講じる**必要がある。

	● サプライチェーン全体のセキュリティを考慮したリスク管理フレームワークを構築し、EU 域外由来の重要資産のうち、宇宙ミッションに不可欠な資産（例えば軌道制御装置等）を特定・リスト化し、それらへの依存度を分析することが求められる。
Article 85：暗号技術及び暗号管理	● リスク評価に基づき、ミッションごとの暗号方針・鍵管理ポリシーを策定・実施し、通信リンク（地上-衛星）における暗号・認証機構を導入する義務がある。 ● また、暗号鍵のライフサイクル管理やバックアップ体制も必要とされ、将来的に、EUCC（）との整合も想定されており、EUCC に基づき、暗号製品や鍵管理製品の利用促進が見込まれる。
Article 86：バックアップ管理と冗長性	● ネットワーク及び情報システムの復旧を可能にするための包括的なバックアップポリシーを策定・実施し、物理的及び論理的な冗長性を確保しなければならない。これにより、災害・サイバー攻撃・誤操作等からの迅速な回復が可能となる。
Article 87：リスク評価	● リスク管理の一環として、インシデントや危機に対応する事業継続方針（BCP）を策定し、それに基づく具体的な対応・復旧計画を作成・実施する必要がある。 ● これらの措置は、サービス継続性と宇宙セグメントの統制維持を確保するためのものであり、人的訓練・冗長性・障害復旧体制も含まれる。
Article 88：テスト	● ネットワーク及び情報システムのリスク管理の一環として、テスト計画を策定・維持・見直し、脅威主導型ペネトレーションテスト（TLPT）を実施しなければならない。
Article 89：教育・訓練	● 全ての関係者は、役割に応じた継続的な訓練を受ける必要がありインシデント対応の経験からの教訓を訓練計画へ反映しなければならない。
Article 90：危機時の情報開示・連絡方針	● 重大なサイバーインシデント等に対して、対象別に最適化された情報開示・連絡戦略を確立し、社内外の関係者に適切な情報共有を行う必要がある。
Article 91：インシデント対応	● インシデントの即時検知・分類・対応・報告が可能なプロセスを整備し、重要インシデントは経営陣へ報告、第三者のペイロードへの影響時には関係者と連携する必要がある。
Article 92：サプライチェーンリスク管理	● サプライチェーン全体のセキュリティを考慮したリスク管理フレームワークを構築する必要がある。 ● サプライチェーンに連なる EU 域外で宇宙ミッションに不可欠な資産（例：軌道制御機器）を特定・リスト化し依存度を分析する必要がある。
Article 93：重大インシデントの報告	● 宇宙事業者がサイバー攻撃や自然災害等の重大インシデントに直面した場合、速やかに関係当局へ報告する義務が課される。 ● 報告先は、対象資産の属性により異なる。 ● また、NIS2 指令や CER 指令に基づき「重要事業体」または「重要インフラ」に該当する事業者は、それぞれの枠組みに基づき CSIRT や担当当局を通じた

	報告が求められる。
Article 94: EUSRN:宇宙レジリエンスネットワークの構築・連携	● 「宇宙事業の重大インシデント」に対応するため、**EUレベルで官民関係者が情報共有や対策を協議する枠組み(EUSRN)を設ける**。
Article 95: サイバー脅威に関する情報共有	● 宇宙事業者が自発的にサイバー関連情報を共有することを奨励する。情報共有を実施する際には、参加・離脱を主管当局へ通知する義務がある。 ● 欧州委員会及び ESA は、共有体制の整備を支援し、情報共有体制として、「EU Space ISAC」等の運営が想定されている。

(6) 宇宙領域防衛指針と防衛省次世代情報通信戦略の策定

2025 年 7 月、宇宙空間の利用確保と防衛能力強化を目指す「宇宙領域防衛指針」と、新たな防衛情報通信基盤の構築等を推進する「防衛省次世代情報通信戦略」を策定した。「宇宙領域防衛指針」では、①衛星コンステレーション等による迅速な戦況把握、②抗たん性の高い衛星通信の確保、③宇宙領域把握(SDA)強化等の機能保証、④相手の指揮統制等の妨害、の 4 本柱で防衛能力を強化する。

「防衛省次世代情報通信戦略」では、意思決定の優越、領域横断的なエフェクトウェブ構築、レジリエンス強化を目指す。その実現に向け、4 層構造からなる「新たな防衛情報通信基盤(仮称)」を整備し、クラウド化やゼロトラスト導入、データ専門人材の確保、官民連携を推進する方針を示した。

(7) CNSSP 12、CNSSI 1200、CNSSI 1253 AF-A2 の改定

大統領令 14144 および 14306 に基づき、CNSS は宇宙のサイバーセキュリティに関する 3 文書(CNSSP 12、CNSSI 1200、CNSSI 1253)の見直しを実施した。当該 3 文書と付属書の概要と主な改訂点を表 3-7 に記載した。

今回の見直しの特徴は、宇宙システムのサイバーセキュリティを、個別の機器や通信の防護にとどまらず、計画、設計、開発、打上げ、運用、廃棄に至るライフサイクル全体を通じて統合的に管理すべき対象として再整理した点にある。CNSSP 12 では、宇宙 NSS 本体のみならず、これを支える地上設備、関連インフラ、商用・外国政府由来の支援サービスまで対象に含めている。その上で、RMF に基づく継続的なリスク管理、サプライチェーンリスク対策、監視・監査・復旧措置、契約・調達段階での要件反映を最低限講ずべき事項として明確化している。さらに、CNSSI 1253 は、NSS に対するセキュリティ分類として、機密性・完全性・可用性を個別に評価する考え方、プライバシー・オーバーレイ、ならびに保証性・レジリエンスを踏まえたテーラリングを提示しており、宇宙分野におけるセキュリティ要求を一律の固定的基準ではなく、ミッションの性質と脅威環境に応じて調整するリスクベースの枠組みへと発展させている。

すなわち、これら 3 文書の改定は、宇宙システムのサイバーセキュリティについて、政策レベルの方針、実施上の指針、管理策の設定を一体的に整理し、ミッション継続性を重視した包括的な管理体系へと強

化したものといえる。また 3 文書（CNSSP 12、CNSSI 1200、CNSSI 1253）を踏まえた NSS 向けのセキュリティ要求事項に関しても表 3-8 にて整理を行った。

表 3-7 各文書の概要と改訂ポイント

文書名	位置づけ・役割	主なポイント	今回の更新に伴う主な変更点
CNSSP 12	宇宙システムを用いる国家安全保障ミッション向けの上位政策。宇宙 NSS およびそれを支えるサービスに対する最低限のサイバーセキュリティ基準と責任分担を定める。	ライフサイクル全体でのセキュリティ統合、RMF 適用、サプライチェーンリスク管理、監視・監査・復旧、契約・リース・政府間合意への要求事項反映を求める。	2025 年版では対象範囲がより明確化され、商用・外国政府のサービスや、開発・統合・試験・打上げ・運用・保守・退役を直接支える情報システムまで適用対象として整理している。 あわせて参照体系も見直され、CNSSI 1200、CNSSI 1253、Space Platform Overlay を前提とする構成に改められている。
CNSSI 1200	CNSSP 12 を実装するための詳細実装ガイダンス。計画、設計、開発、打上げ、運用、停止までの各段階で何を講じるかを具体化する。	AO（運用を正式に許可する権限者）によるレビュー、保護プログラム、証跡、試験計画、SCRM、商用契約条項、リスク評価、継続監視、IDS/IPS、セキュアブート、パッチ管理、暗号・認証などを具体的に示している。	今回の版では、従来の一般的な実装指針に比べて、ライフサイクル段階ごとの管理など、宇宙システム向けの技術的・運用的要求が大きく具体化・強化されている。
CNSSI 1253	NSS 向け RMF におけるカテゴリ化・統制選定のベースとなる文書。セキュリティ統制ベースラインとオーバーレイ適用の考え方を与える。	機密性・完全性・可用性を個別に評価し機密性・完全性・可用性を分け、独立に評価し、それに基づいて必要なセキュリティ・プライバシー対策を選び、任務に応じて調整・追加するための枠組みを示した文書である。	2014 年版から 2022 年版への更新で、NIST SP 800-53 Rev.5/800-53B 準拠へ移行し、Privacy baseline が明示的に組み込まれた。また、個人識別情報を扱う NSS では Privacy Overlay の適用が必要とされ、オーバーレイは独立文書として整備される構成に変わっている。さらに、NSS では機密性・完全性・可用性を分け、独立に評価している。
（参考）CNSSI 1253 Append	CNSSI 1253 のベースラインを宇宙プラットフォーム	宇宙特有の脅威・脆弱性を踏まえ、追加すべき統制と除外し得る統制を整理する。	旧版は、2014 年版 CNSSI 1253 および NIST SP 800-53 Rev.4 に基づき、運用中の無人宇宙プラットフォームを中心に整理されたものであった。これに

ix F Attachment 2: Space Platform Overlay	向けに具体的に調整する文書。		対し 2025 年版では、C・I・A（機密性・完全性・可用性）すべてのリスクが高いことを前提に、対象範囲を通信インタフェースまで拡張するとともに、SPARTA を用いて脅威モデルを具体化している。さらに、二重承認、アクセス制御の強化、機能分離、セーフモード、ハードウェア保護などの統制が大幅に強化され、侵害を前提とした設計思想が明確になっている。
（参考）CNSSI 1253F Attachment 6 Privacy Overlay	個人の機密情報を扱う NSS に対して、1253 の統制に追加で適用されるプライバシー保護指針。	個人情報の収集・利用・保存・共有といったライフサイクル全体に対するプライバシーリスクを評価し、リスクレベルに応じた追加統制群を適用する。	近年の改定では、プライバシーリスクをセキュリティとは独立した軸で評価する考え方が明確化され、Privacy Baseline に加えて Overlay で追加統制を選定する構造となった。監査ログ、アカウント管理、データ最小化、利用目的制限など、データ取扱いに関する統制が体系的に強化されている。

表 3-8 CNSSP 12、CNSSI 1200、CNSSI 1253 から要求されるサイバーセキュリティ事項

要求事項	主な内容
ライフサイクル全体での統合	セキュリティ要求を、企画、設計、開発、試験、打上げ、運用、棄却まで一貫して組み込む。
RMF の適用	宇宙 NSS にも RMF を適用し、CNSSI 1253 に基づきカテゴリ化、ベースライン選定、テーラリングを実施する。
サプライチェーンリスク管理の強化	ミッションの影響度分析、SCRM の適用、偽造部材の報告、商用プロバイダを含むサプライチェーン対策を要求する。宇宙環境の特殊性を踏まえ、より高い保証水準での設計・製造を求める。
開発・調達段階での保護要求	開発・調達段階から重要情報・重要部品を保護する。取得ライフサイクルの早期から NSA と連携することが求められる。
商用サービス・契約条項への反映	商用衛星サービスやホスト型利用では、契約書にセキュリティ要件、証跡提出、監視、報告、政府による検証・検査などを明記する必要がある。
継続監視・監査・報告	宇宙 NSS には継続的監視戦略、監査ログ、障害時の報告、脅威・脆弱性共有が求められる。運用・システム・ネットワークの各観点からモニタリングを行う。
IDS/IPS および防御サービス	宇宙・地上・打上げ・利用者セグメントを含む全体に対してサイバーセキュリティを求め、宇宙プラットフォーム上ではリアルタイム監視可能な IDS/IPS、イベントログの安全な地上送信、アラート機能を要求する。

セキュアブート	起動時・更新時・実行時にファームウェアや重要ソフトウェアの正当性・完全性を暗号学的に検証し、信頼できる状態へ復旧可能であることを求める。さらに、調達・統合・受入試験でトレーサビリティを維持する。
安全なパッチ・更新管理	脆弱性の特定・優先順位付け・修正、ソフトウェア／ファームウェア更新の安全な配布、署名検証、設定変更の厳格管理を要求する。
エンドツーエンド暗号化と強固な認証	コマンド、テレメトリ、ミッションデータ等について、NSA 承認暗号によりエンドツーエンドで認証・暗号化することを求める。不可逆性をもつコマンドには、より強い認証を要求する。
重要コマンド保護とデュアル承認	宇宙向けオーバーレイでは、単独誤操作や内部不正を防ぐため、二段階認証やアクセス制御などの追加統制が求められる。
宇宙特有の環境を踏まえたテーラリング	宇宙プラットフォームは、資源制約、物理保守不可、非汎用のネットワーク／無線、無人運用といった前提を持つ。このため、一般 IT 向け統制をそのまま適用するのでなく、宇宙向けに追加・除外を整理したオーバーレイベースのテーラリングが必要となる。
セーフモード・代替機構・回復性の強化	宇宙向けオーバーレイでは、セーフモード、代替手段、資源の可用性確保、予測可能な障害の防止、フェイルセーフ手順など、宇宙機の継続性・回復性を高める統制が強化されている。

(8) 宇宙能力の確立を目的とした国家宇宙戦略(National Space Strategy 2025–2040)の発表

2025 年 11 月、フランス政府は宇宙領域を国家主権・安全保障・経済競争力の中核インフラと位置づけ、2040 年までに欧州およびフランスの自律的かつ競争力ある宇宙能力を確立することを目的として、国家宇宙戦略「National Space Strategy 2025–2040」を公表した。表 3-9 に示すように文書では 5 つの方針・15 の戦略目標で体系化した。宇宙を作戦領域と定義し、主権確保と欧州全体のレジリエンスの強化を打ち出し、欧州宇宙政策の中長期的方向性を示している。なお、今後、EU 宇宙法案と国内法を整合させていくほか、サイバーセキュリティは、国家の主権やレジリエンスを担保する上で極めて重要な要素と位置づけられ、地上局の保護が強調されたほか、他規制(NIS2、CER)との整合が掲げられた。

表 3-9 国家宇宙戦略の 5 つの方針・15 の戦略目標

方針	戦略目標	概要
1. 自律的な宇宙アクセスの確保	1. CSG(Guiana Space Centre)[18] からの自律的・競争的アクセス確保	アリアン 6 の確実な運用と CSG の近代化により、欧州の独立した宇宙アクセス能力を維持・強化。
	2. 次世代欧州ロケットの開発準備	再使用型・高推力エンジン等の技術を確立し、2035～2040 年を見据えた次世代打上げ能力を構築。

[18] ギアナ宇宙センター
https://centrespatialguyanais.cnes.fr/en/

2. 仏欧宇宙経済の構築	3. 衛星産業の競争力回復	重要技術の特定と欧州レベルでの産業統合を進め、戦略的自律性を確保。
	4. 宇宙経済の構築	観測・測位・通信データの活用を促進し、公共政策および市場サービスに展開。
	5. 人材・研究基盤の強化	**2040 年を見据えた宇宙人材戦略を策定**し、教育・研究・地域拠点を強化。
3. 軍事的宇宙能力の強化	6. 重要宇宙インフラのレジリエンス強化	**冗長化・危機対応計画を整備し、重大危機下でも宇宙サービスの継続を確保**。
	7. 主権的宇宙資産の運用自律性確保	通信・偵察・早期警戒等の**軍事的宇宙能力を強化**し、作戦自律性を確保。
	8. SSA/SST 能力の強化	宇宙状況監視センサー網を拡充し、**軌道上脅威への自律的評価能力を確立**。
	9. 宇宙におけるアクティブ防衛能力の保有	**抑止・対処のための段階的かつ多様な防衛能力を整備**。
4. 科学・探査政策	10. 有人宇宙飛行・探査への関与	ISS・月・火星探査への関与を通じ、科学・技術・外交的影響力を確保。
	11. 地球観測科学の強化	気候・環境・レジリエンス分野における地球観測投資を拡充。
	12. 宇宙科学政策の推進	宇宙物理・惑星科学等の重点分野で国際協力と技術自立を推進。
5. 国際協力・ガバナンス	13. 規範形成外交の推進	宇宙の安全・持続可能利用に関する国際規範形成を主導。
	14. EU 主導の宇宙ガバナンス強化	EU の政治的リーダーシップを明確化し、ESA との役割整理を推進。
	15. 国際協力の多角化	米国・日本・インド等との協力深化および新興国との連携拡大。

(9) ドイツにおける宇宙戦略文書(Space Safety and Security Strategy)の発表

2025 年 11 月、ドイツ連邦政府は、宇宙における安全保障とレジリエンスを強化するための戦略文書「Space Safety and Security Strategy」を公表した。本戦略は、宇宙が平時のインフラ基盤であると同時に、危機・ハイブリッド事態から武力紛争までを見据えた戦略競争の場になりつつあるとの認識に立ち、民生・軍事の両面でドイツが宇宙領域で長期的に行動できる能力を確保することを目的とする。表 3-10 に示すように戦略的行動分野として、①リスク・脅威の特定と行動オプションの整備、②国際協力と宇宙における持続可能でルールに基づく秩序の推進、③抑止・防衛能力・レジリエンスの構築、の 3 本柱を提示した。サイバーは、宇宙領域における主要な脅威・能力領域として位置づけ、宇宙領域での「サイバー作戦」および「電磁スペクトラム作戦」の能力獲得、レジリエントなサイバーセキュリティ・アーキテクチャの整備、技術面・組織面のサイバー対策の組込み、連邦軍と連邦情報セキュリティ庁の宇宙

関連サイバー防衛能力の強化等を掲げている。なお、実施にあたっては、NATO・EU・ESA 等の枠組みを補完しつつ、政府・軍・産業・学術を横断した「国家の宇宙安全保障アーキテクチャ」を、各省の所掌予算と現行財政計画の範囲で優先順位を付けて推進するほか、国防省は今後数年間で宇宙分野に約350 億ユーロを投資する予定である。

表 3-10 戦略的行動分野の概要

能力確保に向けた取組名	概要（一部抜粋）
政府全体による統合的セキュリティ	● **民間および軍事のすべての関係者を巻き込んだ統合的セキュリティアプローチを採用**するほか、**各省庁が連携し、政府全体の取り組みとして強靭な宇宙安全保障アーキテクチャを構築することを目指す。** ● なお、**優先事項として、宇宙領域での「サイバー作戦（cyber operations）と電磁スペクトラム作戦（electromagnetic spectrum operations）の能力獲得等」が明記**されている。
宇宙インフラの保護と防衛・抑止力の強化	● **日常生活、経済、軍にとって不可欠な衛星などの宇宙システムを保護し、防衛任務を遂行するための宇宙軍事作戦能力を強化**する。 ● 特に、ロシアによる GPS **妨害などの脅威に対抗するため、国防省は今後数年間で宇宙分野に約 350 億ユーロを投資**する予定である。
3 つの戦略的行動分野	宇宙空間の利用から生じる課題や脅威に対処するため、以下の 3 つの行動分野を定めている。 1. **リスクと脅威を特定し、行動オプションを整理**する。 2. **国際協力と宇宙における持続可能な秩序を促進**する。 3. **抑止力を構築し、防衛力と回復力を強化**する。
同盟国・国際機関とのパートナーシップ	**多国籍宇宙部隊、連合宇宙作戦イニシアチブなどのパートナーと連携して宇宙での行動能力の向上**を目指す。
ルールに基づく平和的かつ持続可能な利用	● 宇宙空間での軍拡競争を防ぐため、平和的、持続可能かつルールに基づいた宇宙利用に強くコミットする。 ● 国際法の原則を指針として、宇宙分野における国際法をさらに発展させるために他国と協力する。

（10）武力紛争期間における宇宙セクターを狙ったサイバー活動に関する調査結果の発表

ETH Zürich の安全保障に関する研究機関は、ガザ戦争を軸に、宇宙セクター（衛星・地上局・関連企業/機関・サプライチェーン等）を狙ったサイバー活動を、公開情報のみで体系的に整理した。武力紛争時には、衛星通信や地理空間情報などの宇宙サービスが当事者の通信・状況把握に用いられるため、衛星運用者や地上局、関連企業・機関、サプライチェーンを含む宇宙セクターも、サイバー作戦の標的となり得る。本調査の攻撃対象と攻撃タイプを図 3-1、図 3-2 にて示す。ETH Zürich CSS は、この点を具体的に把握するため、公開情報を用いて 2023 年 1 月 1 日～2025 年 7 月 31 日に観測された宇宙セクター向けサイバー作戦を抽出・整理し、計 237 件（標的 77 組織、脅威アクター73）を特定し

た。さらに、これら 237 件をガザ紛争(2023 年 10 月 7 日以降)との関係性で整理し、紛争への明示的動機が確認できる 145 件と、当事者を狙うが直接の動機は明確でない 92 件に区分した。なお、攻撃の中心は Web サイト等への DDoS 攻撃(約 7 割)で、衛星(軌道上の宇宙機)そのものが侵害された事例は特定されていない。影響面では、特定できた範囲では戦場での軍事作戦を左右するほどの成果は限定的であるとした。攻撃の多くは、衛星(軌道上の宇宙機)ではなく、宇宙システムの地上側 IT(Web、認証、社内 IT など)を狙うものである。したがって平時からの IT 防御(資産・権限管理、脆弱性対応、監視、ログ整備、バックアップ、インシデント対応訓練等)を継続して底上げすることが最重要であり、平時の基盤整備を土台として、必要に応じて紛争時の監視・検証・広報対応まで一体で備えるべき、と結論づけている。

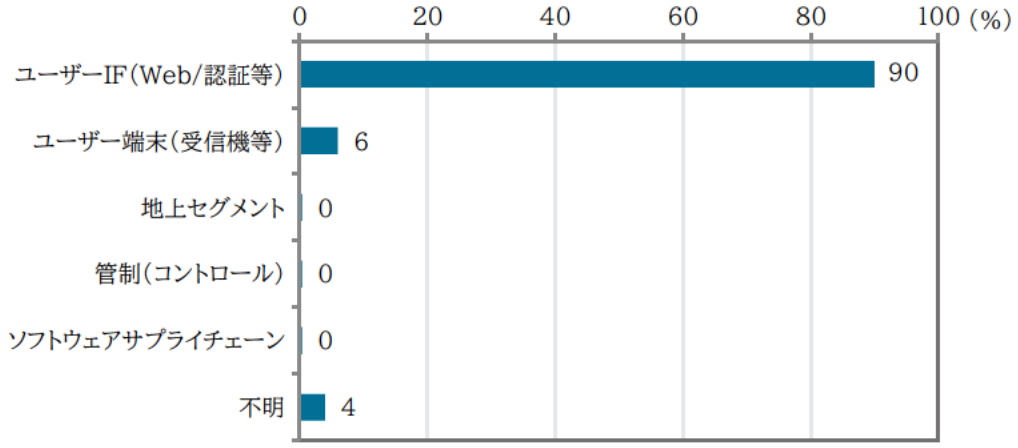


図 3-1 ETH Zürich の調査により観測された攻撃対象セグメント

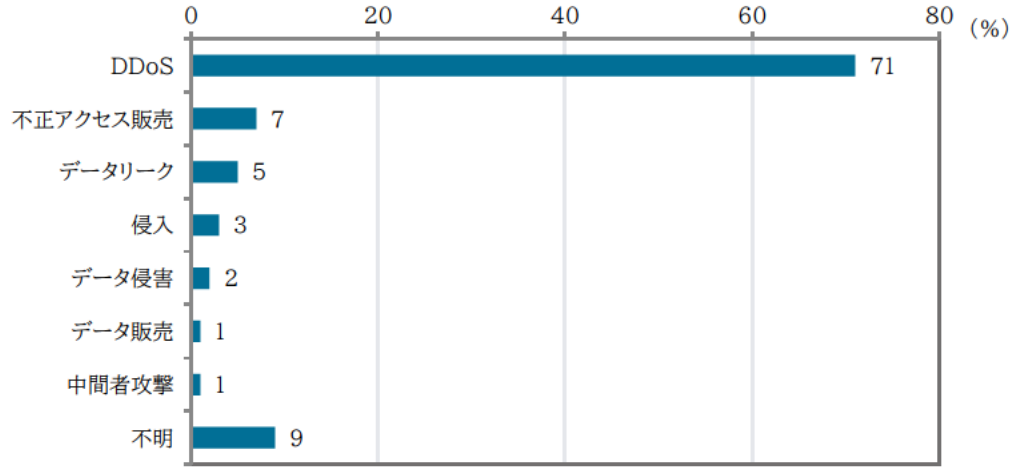


図 3-2 ETH Zürich の調査により観測された攻撃手法

(11) 米上院における「Satellite Cybersecurity Act」再提出と商用衛星サイバー対策の強化

2025 年 12 月、米国の超党派の上院議員らは、商業衛星の所有者および運用者が増大するサイ

バーセキュリティの脅威に対抗するのを支援するため、「Satellite Cybersecurity Act」法案を提出した。表 3-11 に示すように本法案は、重要インフラが宇宙システムに分野横断的に依存していることを背景に、GAO や CISA に対して政府機関や重要インフラの宇宙システムへの依存リスクに関する調査・評価や官民連携の調整等を命じている。なお、現段階では本法案は可決しておらず動向の注視が必要である。

表 3-11 法案の概要

機関	期待される役割	具体的な内容
GAO	**連邦政府の支援策に関する調査・評価**	● 連邦政府が商業衛星システムのサイバーセキュリティを支援するために講じた措置の調査。 ● **衛星システムとサイバー脅威が、連邦・非連邦の重要インフラ保護計画やリスク分析にどのように統合されているかについて評価。** ● 連邦機関間における権限や活動の重複・調整状況の特定。
	議会への報告・勧告	● 法案制定から 2 年以内に、関連する議会委員会へ調査結果を報告し、ブリーフィングを実施。 ● 今後の連邦政府による追加措置や、情報集約サイトで共有すべき情報に関する勧告の提供。
CISA	**情報集約サイトの構築と維持**	● 法案制定から 180 日以内に、**商業衛星システムのサイバーセキュリティリソースを集約したオンラインサイトを構築・維持。**
	サイバーセキュリティ推奨事項の統合・策定	● **商業衛星システムの開発・維持・運用を支援するための、自発的なサイバーセキュリティ推奨事項を統合し、公開リソースとして提供。**
	関係機関および民間との連携・調整	● 国家サイバー長官室（ONCD）や国家宇宙会議等の関係機関と連携し、連邦政府の取り組み方針の一貫性を図る。 ● 関連基準を策定する民間組織や非連邦機関との協議。
	定期的な進捗報告	● 法案制定から 1 年後、およびその後 9 年間にわたり 2 年ごとに、民間連携、機関間調整、サイトの維持状況、民間からのフィードバックをまとめた報告書を議会に提出。

(12) Kombinierte Prüfvorschrift für TR-03184（宇宙システム向け統合試験仕様）の公開

2026 年 1 月、ドイツ連邦情報セキュリティ庁（BSI）は、宇宙システムにおける情報セキュリティの適切な基準を達成するための技術ガイドライン「TR-03184」のバージョン 1.0 を公表した。本ガイドラインは、ナビゲーションや通信等の宇宙ベースのサービスが、現代社会に不可欠なインフラであるとの認識に基づくものである。これらのサービスは、他の IT インフラと同様に、有用性の制限や情報取得を目的とした攻撃の標的となり得る。

このような前提の下、本ガイドラインは、宇宙セグメント、地上セグメント、および利用者セグメントの全

領域ならびにすべてのライフサイクルにおいて、機能的で信頼性の高いサービスを保証するための回復力を構築・確保することを目的とする。

宇宙システムの試験要件を表 3-12 に示す。本表は、システムの保護ニーズを「通常」「高い」「非常に高い」の 3 段階に分類し、要求される審査深度と監査手法を規定する「保護ニーズに応じた審査要件」、「IT 基本保護の手法に基づくリスク分析や受容基準」を定義し、保護目標に応じた適切な暗号化対策を規定する「リスク管理とセキュリティ要件」、および BSI 承認の検査機関の審査員が適合性を審査し、BSI が監督当局として制裁権限等を担う「適合性審査と監督体制」の 3 項目の詳細を整理したものである。宇宙および地上セグメントにおける情報セキュリティの適切な基準を達成し、回復力を構築するための資料として参照される。

表 3-12 TR-03184 の詳細

項目	区分	詳細
保護ニーズに応じた審査要件	審査の基本要件	宇宙システムを構成する各要素の保護ニーズ（通常、高い、非常に高い）に基づき、必要とされる審査要件と審査深度が決定される。
	保護ニーズ「通常」	保護ニーズの侵害が発生した場合の損害は最大でも軽微である。審査は文書および製造者との情報交換のみを基に行われ、審査員による実地監査やシステムの分析は実施されない。
	保護ニーズ「高い」	保護ニーズの侵害が高いまたは中程度の損害をもたらす。実地監査は文書や仮想ワークショップ等で代替可能である。
	保護ニーズ「非常に高い」	保護ニーズの侵害が計り知れない、または潜在的に深刻な損害をもたらす。すべての審査アスペクトが考慮の対象となる。実地監査および審査員によるテストの実施が必要である。
	審査深度	製造者が記述した対策の網羅性や妥当性を検証する。また独立したプロセス分析、ソースコード分析、またはペネトレーションテスト等を実施する。
リスク管理とセキュリティ要件	準拠する手法	宇宙飛行特有の用途に焦点を当てた IT 基本保護（IT-Grundschutz）の方法論に準拠し、リスク分析を実施する。
	リスク管理プロセス	リスク管理プロセスおよび手順の文書化と、定期的なリスク再評価の仕組みが必要である。また、発生確率や損害額などの比較評価基準、およびリスク受容基準を定義する。
	リスク評価と対応	リスクは機密性、完全性、可用性の保護目標に基づいて分類される。特定された全てのリスクに対して影響分析を行い、少なくとも 1 つのリスク対応策を文書化する。
	残存リスク	対策実施後も残る残存リスクについては、定義されたリスク受容基準と一致する根拠を文書化し、利用時の残存リスクとして一覧に要約する。

	暗号化対策	保護ニーズに応じた暗号化対策を実施する。運用期間全体にわたる有効性を考慮し、ポスト量子暗号技術を用いた攻撃からの保護を見据えた対策が求められる。さらに、ソフトウェアやファームウェアの更新を保護するための暗号の俊敏性の実装や、要件を満たす暗号論的に安全な乱数生成器の使用も確認される。
適合性審査と監督体制	審査の対象範囲	適合性審査は、宇宙セグメントおよび地上セグメントを対象として実施される。
	審査員と実施体制	BSI に承認された検査機関から審査員が派遣される。審査員は、該当範囲の能力評価基準を満たすか、BSI の認定を受けている必要がある。
	BSI の監督権限	BSI は検査機関の監督当局としての役割を担い、審査規定の遵守状況の範囲内で制裁措置を行使する権限を持つ。
	審査結果の区分	審査結果は、要件に適合する「PASS」、情報不足等の非適合を示す「INCONCLUSIVE」、要件を満たさない「FAIL」、当該要件が適用されない「NOT APPLICABLE (N/A)」の 4 区分で記録される。
	欠陥の是正と適合性宣言	審査中に「FAIL」や「INCONCLUSIVE」が特定された場合は製造者と協議するが、修正不可能な場合は理由を明記して BSI と今後の対応を調整する。最終的な適合性宣言は、審査要件が満たされている、あるいは十分に考慮されていると判断された場合にのみ発行される。

(13)「Cyber Security Framework and Guidelines for Space Including Satellite Communication」の公開

2026 年 2 月、インドコンピュータ緊急対応支援チーム(CERT-In)は、SIA-India と協力して、宇宙通信資産を保護し、インドの宇宙エコシステムのレジリエンスに貢献するための文書「宇宙および衛星通信に関するサイバーセキュリティフレームワークおよびガイドライン」を公表した。本ガイドラインは、衛星通信ネットワークが防衛、災害管理、ナビゲーションなどにおいて極めて重要であると同時に、商業衛星サービスやクラウドベースのサービスの統合によりサイバーリスクへの曝露が拡大しているとの認識に立ち、民間および戦略的ドメインの両方において安全な衛星技術の展開と信頼できる接続を可能にすることを目的とする。

低軌道衛星通信システムにおけるサイバーセキュリティの課題と対策を整理した表を表 3-13 に示す。本表は、ネットワークの安全な運用に向けた 4 つの側面の概要をまとめたものである。第一に「基本的要件」として、機密性、完全性、可用性の維持と、宇宙特有の脅威に対する専門的なセキュリティアプローチの必要性を確認する。第二に「主要な対象とリスク」として、宇宙、地上、ユーザーの各セグメント、通信リンク、サプライチェーンにおける具体的な脆弱性とサイバー脅威を列挙する。第三に「データ管理お

よび主権」として、ゼロトラスト原則に基づくデータ保護と、国境を越えるデータ送信に伴う法規制遵守の課題と対応策を示す。第四に「調達・利用時の推奨事項」として、プロバイダー向けの質問事項とベンダ多様化の推奨について提示する。

表 3-13 Cyber Security Framework and Guidelines for Space Including Satellite Communication における主要な取り組み

項目	詳細内容
基本的要件	低軌道衛星通信ネットワークにおいては機密性、完全性、可用性の CIA トライアドの維持が不可欠である。機密性には無線周波数や光伝送の傍受による盗聴リスクへの対応、完全性には悪意のあるコマンドの挿入やデータの改ざんの防止、可用性にはジャミングや物理的破壊、サービス拒否攻撃への対策が含まれる。衛星の継続的な移動や頻繁なハンドオーバーにより接続の安全確保が困難であるため、従来の地上モデルを超え、スプーフィングや信号劣化、侵害された地上局といった宇宙特有の脅威に対する専門的なセキュリティアプローチが必要となる。
主要な対象とリスク：宇宙セグメント	衛星自体を指し、ジャミング、不正なコマンドインジェクション、ペイロードやプラットフォームのハイジャック、ファームウェアの改ざんなどのサイバー脅威の対象となる。特にレガシーな宇宙機器は最新のサイバーセキュリティ基準を満たす前に設計されており、セキュアバイデザインのアーキテクチャを欠き、処理能力の制限やソフトウェアの老朽化、暗号化されていない通信プロトコルへの依存により、不正アクセスのリスクが高い。
主要な対象とリスク：地上セグメント	衛星制御センター、地上局、ゲートウェイなどで構成され、地上ネットワークとの広範な接続性により、宇宙システムの中で最も相互接続され脆弱な部分となる。リスクには、マルウェアインジェクション、ソーシャルエンジニアリング、ユーザーの不十分なサイバーセキュリティ慣行のほか、サービス拒否攻撃、侵害された認証情報やソフトウェアの脆弱性を悪用した不正アクセスが含まれる。
主要な対象とリスク：ユーザーセグメント	エンドユーザーのデバイス、アプリケーション、インタフェースで構成され、最も分散しており制御が及ばない環境のため脅威を受けやすい。侵害されたユーザー端末、脆弱なエンドポイントセキュリティ、パッチが適用されていないソフトウェア、安全でない設定が悪用され、不正アクセスやデータ傍受を招く。また、認証情報の盗難、フィッシング、安全でないアプリケーションプログラミングインターフェースやモバイルアプリの使用もリスクとなる。
主要な対象とリスク：通信リンク	衛星と地上インフラ間のデータ転送を担うが、無線通信であるため、ジャミング、スプーフィング、リプレイ攻撃、盗聴の脅威にさらされる。これによりサービスの可用性が損なわれ、データの機密性と完全性が侵害される可能性がある。
主要な対象とリスク：サプライチェーン	複数のベンダや下請け業者が関与するため、ハードウェアやソフトウェアのバックドア、製造中の改ざん、偽造コンポーネントの挿入などのリスクが存在する。サプライチェーンの複雑さとグローバルな性質により、一貫したセキュリティ実践を確保することが困難となる。

データ管理	停止中、移動中、使用中のすべての状態において機密情報を保護する必要がある。リスクには、衛星と地上局間または衛星間のデータ転送への不正アクセス、テレメトリやミッションデータ、ログの操作、侵害された地上局のストレージシステムからのデータ盗難が含まれる。対策として、ゼロトラスト原則に基づくデータ損失防止戦略の導入、データの暗号化、役割ベースのアクセス制御、包括的なネットワーク監視、監査ログの追跡、トラステッドデータゾーンによるネットワークのセグメンテーションが求められる。
データ主権	データが複数の国境を越えて送信され、データの送信元以外の国で処理または保存される可能性があるため、プライバシーとデータ保護規則へのコンプライアンスが複雑化する。プロバイダーが国内に物理的インフラを持たない場合、現地の監視の対象外となる課題もある。対策として、指定された管轄区域内の地上局にのみデータをダウンリンクするジオフェンシングを利用したデータルーティング、マルチテナントの分離、国内のエッジコンピューティングおよびストレージインフラを利用するソブリンデータゾーンの構築、データローカリゼーションポリシーの適用、管轄区域を越えたデータの取り扱いを事前に定義する宇宙トラフィック協定があげられる。
調達・利用時の推奨事項	プロバイダーとの間でセキュリティへの期待と要件を定義し、共有責任モデルにおける役割と責任を明確に理解することが推奨される。クリティカルなネットワークにおいては、特定のプラットフォームへの依存を最小限に抑え、モジュール式で相互運用可能なアーキテクチャを採用してベンダロックインを軽減し、ベンダの多様化を促進する。さらに、暗号化とデータ保護、地上セグメントのアクセス制御、通信ネットワークのセグメント化、脅威の検出とインシデント対応、ソフトウェア部品表やハードウェア部品表を含むサプライチェーンの保証、セキュリティ基準への準拠状況、および契約における法的責任などについて、プロバイダーに対して具体的な質問を行い、組織独自のセキュリティ要件や規制要件に合わせて対策を推進する。

(14)「Securing space – Cyber security for LEO SATCOM」の公開

2026 年 3 月、オーストラリア・サイバーセキュリティセンター(ASD's ACSC)、オーストラリア宇宙庁、カナダサイバーセキュリティセンター、米国国家安全保障局(NSA)、およびニュージーランド国家サイバーセキュリティセンター(NCSC-NZ)は、低軌道衛星通信におけるサイバーセキュリティに関するガイダンス「Securing space – Cyber security for LEO SATCOM」を公表した。本ガイダンスは、低軌道(LEO)衛星通信システムの急速な拡大が新たなサイバーセキュリティ上の課題とリスクをもたらしているとの認識に立ち、商業通信、国家安全保障システムおよび緊急対応機能のレジリエンスを確保し、組織が LEO SATCOM サービスを調達または利用する際に情報に基づいた意思決定を行うことを支援することを目的とする。

主要な要素を表 3-14 に示す。「サイバーセキュリティ原則」、「セグメント別セキュリティ要件」、「規制及び実施の枠組み」の 3 つの要素から構成される。「サイバーセキュリティ原則」では、設計の初期段階からセキュリティを組み込むことや、ゼロトラストアーキテクチャの適用、多層防御、継続的な監視などの

基本的なアプローチを示す。「セグメント別セキュリティ要件」では、宇宙、地上、通信リンク、ユーザー端末の各領域に対し、通信の暗号化、物理的および論理的なアクセス制御、ネットワーク分離などの技術的要件を規定する。「規制及び実施の枠組み」では、インシデント発生から６時間以内の報告義務、定期的なサイバーセキュリティ監査、サプライチェーンの保護、国際的な枠組みとの整合性など、組織的および制度的な要件を定める。

表 3-14 Securing space – Cyber security for LEO SATCOM の主要な取り組み

大項目	中項目	詳細内容
サイバーセキュリティ原則	設計と多層防御	セキュリティ・バイ・デザインおよびデフォルトの原則に基づき、システム設計や開発の初期段階からセキュリティを組み込む。物理的、論理的、手順的な保護を組み合わせた多層防御を採用する。
	アクセス制御とゼロトラスト	最小権限の原則に基づき、ロールベースのアクセス制御と多要素認証（MFA）を実装する。暗黙の信頼を排除し、ネットワークコンポーネントやユーザーの継続的な検証を行うゼロトラストアーキテクチャ（ZTA）を適用する。
	暗号化とシステム完全性	テレメトリ、追跡、コマンド（TT&C）、およびペイロードデータリンクに対してエンドツーエンドの暗号化を適用する。セキュアブートやデジタル署名を通じて、ファームウェアやソフトウェアの完全性を確認する。
	監視とレジリエンス	AI や機械学習を活用したリアルタイムの監視と異常検知を展開する。インシデント対応手順（IRP）と事業継続計画（BCP）を整備し、定期的なサイバー演習を実施する。最高衛星セキュリティ責任者（CSSO）を任命し、サプライチェーンのセキュリティ確保と責任の所在を明確化する。
セグメント別セキュリティ要件	宇宙セグメント	アップリンクコマンドに対する強力な暗号化認証と、地上制御での多要素認証を実装する。TT&C およびペイロードデータリンクにエンドツーエンドの暗号化を使用し、RF 通信でのアンチジャミングおよびアンチスプーフィング技術を採用する。セキュアブートおよびデジタル署名されたファームウェアを使用し、異常な振る舞いを検知するためのテレメトリ監視を継続的に行う。
	地上セグメント	生体認証などの物理的アクセスコントロールを実施し、ミッションクリティカルなネットワークを企業 IT やインターネットから分離する。ネットワーク侵入検知・防御システムを導入する。オペレーターの活動ログを保持する。保存時および転送時のミッションデータを暗号化し、ハードウェアセキュリティモジュール（HSM）で暗号鍵を保管する。
	通信リンク	TT&C およびペイロードデータに対してエンドツーエンドの暗号化と暗号化メッセージ認証を適用する。HSM を用いた鍵の保管やライフサイクル管理を実施する。スペクトル監視やスペクトラム拡散などの RF レジリエンス技術を活用し、暗号化認証と RF レベルのチェックを組み合わせたスプーフィング対策を講じる。

	ユーザー端末	端末は工場出荷時のデフォルト設定からの変更を必須とし、固有の認証情報を使用する。ファームウェアの署名と安全な更新を実施し、安全でないプロトコルやデバッグインターフェースを無効化する。ユーザーデータの送信には耐量子暗号アルゴリズムの使用を義務付ける。ユーザー端末から地上ゲートウェイへの非暗号化バックホール接続を防止する。
規制及び実施の枠組み	インシデント報告	すべての衛星通信運用者およびサービス提供者は、サイバーセキュリティインシデントを認知してから 6 時間以内に CERT-In に報告する義務がある。また、監査やフォレンジック調査のためにインシデントログを最低 180 日間保持する。
	監査とコンプライアンス	CERT-In が認定する監査機関を通じた外部サイバーセキュリティ監査を少なくとも年に 1 回、内部監査を 6 ヶ月に 1 回実施する。国際規格（ISO/IEC 27001 など）や国家規格の要件に従ってコンプライアンスをマッピングし、証拠リポジトリを維持する。
	サプライチェーンとデータ保護	信頼できる供給元からの調達を確保し、統合や展開の前にサプライチェーンのリスク評価と第三者監査を義務付ける。ユーザーデータの取り扱いは「2023 年デジタル個人データ保護法」に準拠し、データの最小化と暗号化を実施する。
	セキュリティテストと認証	設計から運用終了に至るライフサイクル全体にわたり、ペネトレーションテスト、脆弱性スキャン、暗号化の検証などを実施する。ハードウェア、ファームウェア、暗号モジュールは FIPS 140-3 や ISO/IEC 15408（CC）などの認定された規格に従って認証される必要がある。

3.1.2 近年の脅威動向に関する調査

宇宙分野におけるサイバーセキュリティに関する近年の脅威動向について調査を行った。調査対象とした取組等を表 3-15 に示す。

表 3-15 調査対象とした国内外の脅威動向一覧

No	動向名称	時期	国	取組主体	概要
1	Operation CargoTalon[19]	2025 年 7 月	インド	SEQRITE ラボ	SEQRITE ラボの研究者により、ロシアの航空宇宙・防衛企業を標的とする諜報作戦「Operation CargoTalon」が観測された。 航空宇宙・防衛分野においても業務文書を入口にした侵入と情報窃取のリスクが示される事例となった。
2	中国国家関与アクターによる重要インフラへの継続的侵入活動[20]	2025 年 9 月	米国	サイバーセキュリティインフラストラクチャ庁（CISA）等	米国 CISA などが中国国家関与アクターによる重要インフラへの継続的侵入活動を警告した。活動は米国、豪州、カナダ、NZ、英国などで観測され、世界規模での諜報目的（通信・移動の追跡に資する可能性）が示された。・
3	中国による Starlink への電子戦による妨害及び通信を劣化・遮断する手法の検討[21]	2025 年 11 月	中国	浙江大学 北京理工大学	浙江大学と北京理工大学（BIT）所属の中国の研究者が、Starlink を電子戦で妨害して通信を劣化・遮断する手法を検討していると、南華朝郵便紙が報じた。

以降では、各脅威について詳説する。

(1) Operation CargoTalon

SEQRITE ラボの研究者により、ロシアの航空宇宙・防衛企業を標的とする諜報作戦「Operation CargoTalon」が観測された。図 3-3 に示すように攻撃者は運送伝票を装ったメール添付で受信者に開封を促し、ショートカット（LNK）を介して ZIP に偽装した「EAGLET」を実行させる。EAGLE DLL は外部サーバーと通信し、遠隔でのコマンド実行やファイル送受信（持ち出し・追加投入）に利用され得

[19] SEQRITE, “Operation CargoTalon : UNG0901 Targets Russian Aerospace & Defense Sector using EAGLET implant”, https://www.seqrite.com/ja/blog/operation-cargotalon-ung0901-targets-russian-aerospace-defense-sector-using-eaglet-implant/
[20] CISA, “Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System”, https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a
[21] GU Hanqing, YANG Zhuo, ZHANG Peng, WEN Xiaowen, “Simulation research of distributed jamming against mega-constellation downlink communication transmissions”, https://www.spacejournal.cn/xtgcydzjs/article/doi/10.12305/j.issn.1001-506X.2025.11.30

る。航空宇宙・防衛分野においても業務文書を入口にした侵入と情報窃取のリスクが示される事例となった。

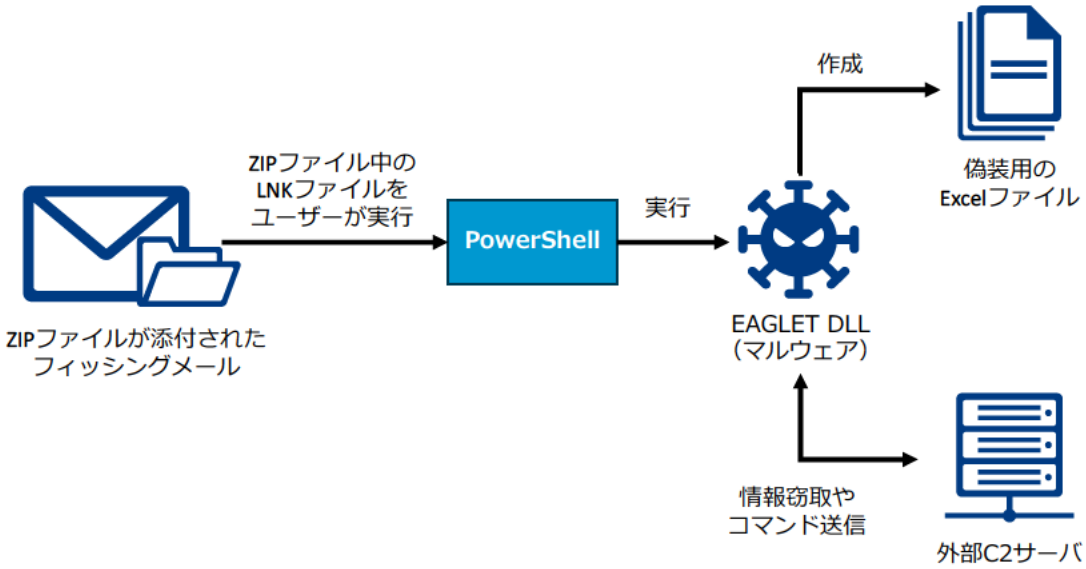


図 3-3 Operation CargoTalo に用いられた攻撃経路(本文[19]より作成)

(2) 中国国家関与アクターによる重要インフラへの継続的侵入活動

米国 CISA などが中国国家関与アクターによる重要インフラへの継続的侵入活動を警告した。活動は米国、豪州、カナダ、NZ、英国などで観測され、世界規模での諜報目的(通信・移動の追跡に資する可能性)が示された。境界機器の更新、ID 連携の最小権限、監査ログ強化などの対策を勧告している。宇宙業界に特化したセキュリティリスクではないが、衛星運用事業者の地上 IT・通信・クラウドへの影響が生じ得る。

(3) 中国による Starlink への電子戦による妨害及び通信を劣化・遮断する手法の検討

浙江大学と北京理工大学(BIT)所属の中国の研究者が、Starlink を電子戦により妨害する手法を検討していると、南華朝郵便紙が報じた。本手法はコンステレーションからユーザー端末へのダウンリンクに対してジャミングを行う手法について検討している。大規模なコンステレーションでは衛星の数の多さと動的な変化により、単一ノードへの干渉が有効でない。そのため、衛星からユーザーへのダウンリンクの通信を標的として、特定のエリアにジャミングを行うという手法をとっている。現状ではコスト面等に大きく制約があるために実行に非現実的であることが示されている。Starlink 依存の指揮統制・状況把握・無人機運用などの通信基盤を広域に攪乱し得るおそれがある一方、必要ノード数が極めて大きく、現実の運用・展開は容易でないことを明らかにした。

3.2 海外調査の実施

宇宙のサイバーセキュリティに関する課題や動向について、米国を対象に海外調査を実施した。昨年度調査を踏まえて、宇宙サイバーやセキュリティ対策における課題、米国における調達要件の動向、技術発展などによる留意すべき特定のトピック(サプライチェーンセキュリティ(SBOM 等)、ゼロトラスト・セキュリティ、AI、(PQC(Post-Quantum Cryptography:耐量子計算機暗号[22])、QKD(Quantum Key Distribution:量子鍵配送[23]))、について、CyberSat25[24]に参加するほか、ヒアリング調査を行った。

(1) 宇宙分野におけるセキュリティに関する課題について

宇宙分野における課題の中心は衛星本体に限られず、GPS ジャミングやスプーフィング、電子戦、サイバー攻撃、物理的妨害が複合的に発生し得る点にある。

昨今の宇宙システムは、宇宙・地上間リンク、地上局、クラウド、ソフトウェア更新基盤、接続端末など多層的な構成をとっており、いずれか一部の脆弱性が全体の障害や侵害につながり得る。とりわけ、認証や暗号化の未整備、クラウドへの依存の高まり、複数ネットワーク横断による攻撃面の拡大は、連鎖的な被害を生じさせるおそれがある。

また、宇宙分野とサイバー分野の連携不足により、設計段階から運用・保守に至るまで一貫したセキュリティ確保が十分でない点も課題として指摘された。

(2) 宇宙分野におけるセキュリティに関する規制・調達・制度動向について

安全保障の領域で民間事業の市場が拡大していることを背景に、米国の宇宙分野における規制・調達・制度の動向について、CNSS から出される文書や DoD の RMF が強い影響力を持つ一方、実際の現場で最も直接的な拘束力を持つのは、契約文書や仕様書に明記された具体的要件であるとの認識が示された。米国では、民間事業者では、NRO、SSC、NASA など顧客ごとに重視される要求が異なっており、統一的な枠組みが不在であることが制度対応を複雑にしている課題が共有された。

また、CNSSP 12、CNSSI 1200、Appendix F Attachment 2 などの見直しでは、宇宙システム本体に加え、サービス提供者も含めた広い対象に対して、異常検知、監視・対応、セキュアブート、安全なパッチ管理、認証情報管理等の具体的要件が強化されつつある。他方で、制度運用上は、従来の文書審査やチェックリストに依存した認証の限界も指摘されており、リアルタイムな可視化や継続的認証を取り入れた仕組みへの転換が求められている。

(3) 宇宙分野におけるサプライチェーンセキュリティに関する動向について

宇宙分野におけるサプライチェーンセキュリティ上の課題としては、まず、元請企業であっても下請企

---

[22] PQC(Post-Quantum Cryptography:耐量子計算機暗号)
従来の公開鍵暗号(RSA、ECC)は量子計算機で破られる可能性があり、量子コンピュータでも解読が困難とされる数学問題に基づいた暗号方式

[23] QKD(Quantum Key Distribution:量子鍵配送)
量子力学の性質を利用して暗号鍵を安全に共有する技術であり鍵そのものを量子通信によって安全に受け渡す仕組み

[24] CyberSat25:衛星、宇宙、サイバー、政府関する話題を融合した唯一のセキュリティイベントであり、脅威の動向や政策について学び、次世代の攻撃を阻止することを目的としている。参加した非機密プログラムの本年度の主要テーマとして安全保障分野における宇宙領域の活用が多く取り上げられた。(https://cybersatsummit.com/program/)

業や再委託先まで含めた対策状況を十分に把握できておらず、サプライチェーン全体の可視性が不足している点が課題として提起された。こうした状況の下では、個別企業が一定の対策を講じていても、下位層の脆弱性を通じて全体が侵害されるおそれがある旨、指摘された。

また、SBOM のような構成情報の可視化手法は重要視されつつあるものの、宇宙産業における理解と実装は限定的であり、提出要求のみで十分な安全性が確保されるわけではないことが問題視された。さらに、市販の汎用製品への過度な依存や、同一の商用基盤を複数の主体が共有する状況は、情報分離や信頼性確保の観点から新たなリスクを生み出すと議論された。

このため、調達段階からのセキュリティ要件の明確化、継続的監視、下位層監査、鍵管理の強化、重要機能の内製化、信頼できる供給者の定義づけを組み合わせ、供給網全体を対象とした一体的な管理を進める必要がある旨示唆された。

（4） 宇宙分野におけるゼロトラスト・セキュリティに関する動向について

宇宙分野におけるゼロトラスト・セキュリティをめぐっては、顧客ごとに求められる要件や契約条件が異なるため、単一のフレームワークを一律に適用することは難しく、各ミッションの特性に応じた段階的な導入が前提となる旨、示された。

特に、宇宙機、通信リンク、地上設備、利用者、打上げといった各セグメントでは、それぞれ異なる運用条件や制約が存在し、可用性、安全性、サイズ・重量・消費電力の制約を踏まえた能力設計が必要である。このため、一般的な地上 IT 向けのゼロトラストモデルをそのまま移植するのではなく、宇宙システムの特性に即して再構成することが求められる。

また、ゼロトラストは既存の安全性や信頼性確保の枠組みを置き換えるものではなく、それらを補完・強化する設計・運用指針として位置付けられている。具体的には、PKI や証明書管理などを組み合わせた多層防御が重要となる。さらに、独自仕様であることを安全性の根拠とみなす考え方は見直されつつあり、認証や再送攻撃対策を含む要件を設計・調達段階から明確に組み込む必要がある。

今後は、侵入を完全に防ぐことのみを目指すのではなく、侵入を受けた後も影響を局所化し、継続的に運用できるゼロトラスト型アーキテクチャへの転換が重要になると考えられる旨、示唆された。

（5） 宇宙分野における AI の利活用や脅威に関する動向について

宇宙分野における AI をめぐる動向としては、まず、攻撃側による AI 活用が急速に進み、脆弱性の探索、攻撃コードの生成、偵察活動、無線信号の操作などが自動化・高速化されつつある点が示された。こうした変化は、宇宙分野においても、従来以上に短時間で高度な攻撃が実行され得ることを意味している。

一方で、防御側でも、テレメトリのリアルタイム分析、異常検知、予兆保全、広域監視などに AI を活用する動きが進んでおり、AI は宇宙システムの運用・防御を支える有力な手段となりつつある。特に、監視対象が静止軌道、月軌道、ラグランジュ点にまで広がる中で、人手のみで全体を継続的に把握することは困難であり、AI は広域かつ継続的な監視を補完する技術として有用である。

他方で、AI の有効活用には、モデル性能そのもの以上に、入力データの信頼性や一貫性、統治の枠組みを確保することが不可欠である。さらに、宇宙側エッジ環境では、傍受、コード注入、モデル汚染など新たな脅威も生じるため、AI 型侵入検知、自律復旧、デジタルツイン等を組み合わせた多層的な防御

と、AI に委ねる判断範囲の明確化を併せて進めることが重要である旨、示唆された。

（6） 宇宙分野における PQC および QKD をめぐる動向について

宇宙分野における PQC および QKD をめぐる動向としては、まず、量子コンピュータの進展により既存の暗号方式が将来的に脆弱化する可能性が高まっていることが指摘された。宇宙システムにおいても耐量子計算機暗号（PQC）への移行準備が重要課題となっている。特に、衛星への指令を送るコマンドリンクは、宇宙システムの安全な運用を支える中核的な通信経路であり、従来型を含めた基本的な暗号化の徹底に加えて、長寿命システムでは将来を見据えた PQC 対応が求められる。

加えて QKD は、地上ファイバーでは難しい長距離の安全な鍵共有を可能にする技術として注目されており、衛星を活用した構成によって広域・国際的な鍵配送基盤を実現し得る可能性が示されている。他方で、衛星 QKD の実装には、波長設計、追尾性能、機器のサイズ・重量・消費電力といった技術的制約が大きく、直ちに広範な実用化には課題がある点も指摘された。

このため、現時点では PQC と QKD のいずれか一方に依拠するのではなく、耐量子暗号、暗号装置、異常検知、遠隔更新機能などを組み合わせた多層的な防護が現実的な方向性として示されている。さらに、中国などが量子技術分野で先行しているとの見方も踏まえると、量子技術は単なる研究開発課題にとどまらず、今後の宇宙通信・安全保障上の競争力を左右する戦略的重要課題として位置付ける必要があることが示された。

3.3 EU Space Act（EU 宇宙法案）に関する調査・分析

2025 年 6 月、欧州委員会は、EU 域内における宇宙活動の安全性・強靭性・持続性を確保しつつ、EU の宇宙産業の競争力向上を目的として、EU Space Act（EU 宇宙法案）に関する法案を発表した[25]。本法案は、EU 域内外を問わず、宇宙オブジェクトの打上げ・運用・サービス提供を行う全事業者が対象となり、第三国事業者には EU 法的代理人の設置や技術遵守の義務が課され、EU 域内と同等の規律が適用される予定である。

そのため、表 3-16 に示すとおり、法法案が求めるセキュリティの要求内容に対して、日本の事業者に対して特に影響の大きいことが想定される項目に絞り、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 2.0 にて定められている内容と比較・分析し、対応の方向性を検討した。

表 3-16 EU 宇宙法案施行に伴う影響の程度（例）

[25] EUROPEAN COMMISSION, “REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the safety, resilience and sustainability of space activities in the Union” https://defence-industry-space.ec.europa.eu/EU Space Act（EU 宇宙法案）_en

項目	EU 宇宙法案で定められている内容	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 Ver 2.0 にて定められている内容	対応の方向性
TLPT 対応力（Article 88：テスト）	**TLPT は打上げ前**（コンステは初回バッチ前）と**少なくとも３年ごとに義務化**されている。 外部ベンダには（加盟国認定の認証または正式な倫理コードへの準拠）に加えて、過失・不正に備える専門職賠償保険への加入が求められる。 さらに、**外部ベンダの高い適格性・独立報告・是正計画の提示**も必要となる。	**脆弱性診断/セキュリティ検証の実施の推奨にとどまる**。 頻度・TLPT 方式・外部テスター資格/保険の**明確な拘束は記載なし**。	**資格要件を満たす外部ベンダ**選定等が必要な可能性がある。
暗号製品・認証スキーム（Article 85：暗号技術及び暗号管理）	暗号の実装は、**EU サイバーセキュリティ法（Reg.2019/881）Art.49 の認証スキーム**で補完され得る（将来の委任法/実装で具体化）。 また**鍵のライフサイクル管理ポリシー（生成・保管・配布・廃棄）、テレコマンドの暗号化、復旧計画に必要な鍵・パラメータの可用性確保等**が求められる。	**CRYPTREC/CCSDS 等の文書を参照するよう推奨**する立て付けであり、**特定の認証取得の義務は設けていない**。	一律の適合義務ではないが、将来的に委任法/実装で具体化し次第、**将来の EU 認証スキーム適合への移行計画・プロダクト選定**が必要な可能性がある。
サプライチェーンの見える化（Article 92：サプライチェーンリスク管理）	サプライチェーンリスク管理フレームワークの構築や、ミッションの技術的統制に不可欠な**「非 EU 原産」の重要資産のインベントリ作成を義務化**する。	**SBOM の確認・管理、取引先のセキュリティ確認を実施する等を推奨**するにとどまる。	使用製品の原産地（EU/非 EU）と代替可否・納期リスクを確認し、依存度分析と代替調達/在庫方針を策定するほか、既存 SBOM を拡張して地政学属性の追加が必要な可能性がある。

通報タイムラインの厳格化（Article 93：重大インシデントの報告）	**インシデント時の報告時限が厳格化**されている。 早期警戒：重大インシデント把握から 12 時間（Union 資産）/24 時間（その他）以内 初報：72 時間以内 中間報告：要請時 最終報告：初報から 1 か月以内（継続中なら進捗＋終了 1 か月以内の最終）	「必要に応じ、外部の組織に報告」や、「ステークホルダーの連絡フロー整理を推奨」等で、**具体時限は未規定**である。	重大インシデントの報告に向けた体制の強化等が必要な可能性がある。

なお、EU 宇宙法案では、NIS2 指令に優先する特別法として EU 宇宙法案が適用される。 EU 宇宙法案では、違反に対して加盟国が効果的かつ抑止力のある罰則を定めることが義務付けられており、違反の重大性や継続性、過去の違反歴、被害の規模などを考慮して行政制裁や罰金が科される。一方、EU 宇宙法案は欧州議会・理事会で審議中であり、適用範囲や要件、適合性評価・証明書制度、監督・執行（行政制裁・罰金などを含む）の運用は今後具体化・変更され得る。

全面施行は 2030 年 1 月 1 日が予定され、発効後 5 年で見直しが想定されるため、審議の進捗、最終条文、委任法・実施法、ガイダンスなどの動向を継続的に注視することが不可欠である。

3.4 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の更新に向けた整理

昨年度の民間事業者に対するヒアリング結果や今年度の調査結果を踏まえて、今後ガイドラインを更新する場合に検討が必要となり得る観点や論点の整理を行い、将来的な更新の方向性について検討を進めた。また、整理した内容を踏まえて、今後関係省庁・機関等とも連携しながら、ガイドライン更新を含む必要な取組を推進し、宇宙産業サプライチェーン全体における適切なサイバーセキュリティ対策の実施と国際競争力の確保に向けた取組を一層推進していくことが求められる。

(1) ガイドラインのスコープの拡大について

現行のガイドラインでは、特定の分野（観測衛星、通信衛星、放送衛星等）やシステム規模等に限定せず、民間企業が主体となる衛星システム及び地上システムを対象としている。

また、衛星システムは、設計・開発・製造、運用・保守、廃棄フェーズを対象としており、地上システムは、運用・保守フェーズを主な対象としつつ、システムの設計から廃棄までの各フェーズで特に注意すべき点は対象としている。

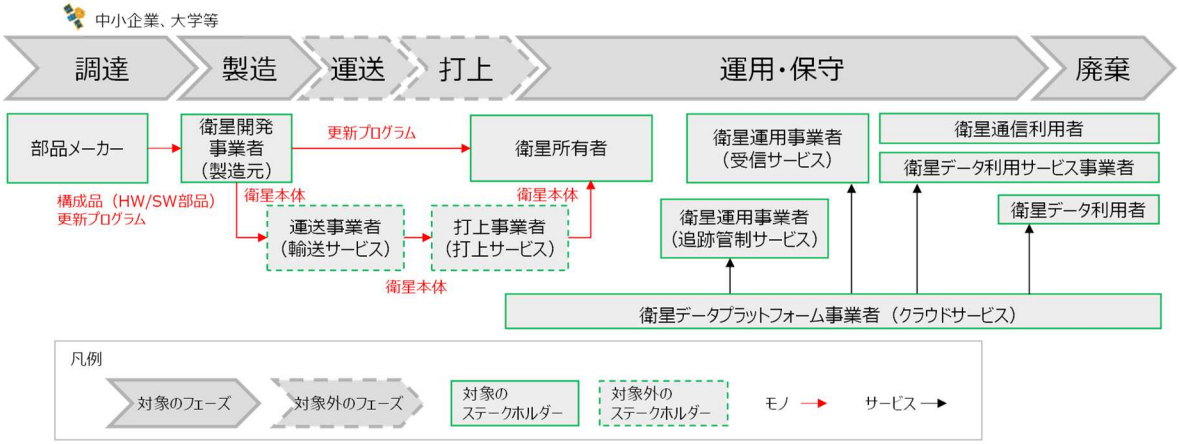


図 3-4 現行ガイドラインの対象

一方、近年は 5G/NTN や光地上局など、宇宙と地上をつなぐ新たな通信インフラが登場し、リスクも複雑化している。そのため関係省庁や民間事業者と連携し、これらの実用化に向けた開発・実証成果や国際動向を反映したセキュリティ対策の強化・制度化に向けた議論を行っていくことが求められる。また必要に応じて、ガイドラインのスコープもこうした新領域を見据えて見直す必要がある。想定される新領域の例について図 3-5 に示す。

項番	システム分類	対象	国内外の動向	想定されるセキュリティ対策
1	輸送システム	小型ロケット	• 日本ではスペースワンが民間射場から打上げを本格化、インターステラは2025年に「ZERO」の初飛行を予定。再使用型ロケットの開発も進み、ISCは米国での試験飛行を計画、ホンダも独自に実験機の打上げに成功。 • 射場インフラ整備や資金調達も進展し、民間による打上げ事業が加速中。 • **国際連携や輸出も視野に、セキュリティ・信頼性確保が一層重要**となっている。	• 通信の暗号化やサプライチェーンセキュリティ等、衛星システムに対するサイバーセキュリティ対策 • 内部犯行対策　など
2	衛星システム	探査機	• 米国では、SpaceX、Blue Originが2025年目標の有人月探査計画「アルテミス」で使用する有人着陸機を開発中。 • 国内では、2025年6月6日、iSpaceにより、Mission 2「RESILIENCE」ランダーが月着陸失敗を発表。	• 通信の暗号化やサプライチェーンセキュリティ等、衛星システムに対するサイバーセキュリティ対策
3		デブリ除去	• 国内では、アストロスケールが、2021年にJAXAと協力して国産実証衛星を打上げ、2023～2024年にかけてADRAS-J による接近・撮影実証を完了。2029年までにADRAS-J2で除去実験計画。	• 同上
4		燃料補給、機器交換修理	• 国内では、アストロスケールとJAXAが、衛星への燃料補給サービスに関するコンセプト共創活動を開始、2030年までに日常的な基盤インフラサービスにする想定。	• 同上
5	有人システム	商業宇宙ステーション	• 米国では、Axiom Station（Axiom Space）はISSドッキング後の切り離しフリー運用を2028年までに予定し、第1モジュール製造が進行中。NASA CLDプログラムにも採択。 • 国内ではDigitalBlastが構想を掲げており、2030年までに最初のモジュールを打ち上げる計画としている。 • 宇宙ホテルなどの構想も含まれるが、早くとも2030年前後の実現予定。	• 同上
6		宇宙旅行用機体	• 弾道宇宙旅行、月周回軌道航行などの宇宙旅行に運用される機体を想定。 • 米国では、Space XのCrew Dragonなどが実用化されている。 • 国内では、SPACE WALKERが2027年の宇宙旅行実現を目指している。	• 同上
7	地上システム	光地上局、5G局	• 米国では、可搬型光地上局の投入が進み、光通信による高スループット（Gb/s超）や量子通信実証が加速中。NASAでも大容量レーザー通信実験成功事例あり。 • 国内はSpace Compassが光データリレーサービス提供に向けて2024年に衛星打ち上げをしてサービス開始予定であるほか、WARPSPACEが2030年を目指し月面開発に向けた光通信サービスを開発中。 • また、NICTが、2022年1～2月に静止衛星（Ku帯）回線を活用した日欧間の5G統合制御に関する共同実証実験を実施。	• 設備の保護やジャミング対策等、衛星運用設備に対するサイバーセキュリティ対策 • 内部犯行対策　など

図 3-5 想定される新領域の例

上記で挙げたもののうち、優先的に取り組むべき領域については、各対象が攻撃を受けた際に及ぼし得る影響度×発生可能性を考慮してリスク評価の上で検討する必要がある。ただし実現までに一定以上の期間を要すると想定される技術よりも、すでに実現されている技術、あるいは実現が近い将来に想定されている技術を優先的に検討することが考えられる。

（2） 想定されるリスクシナリオの見直し、高度な脅威に対する対策について

想定されるリスクシナリオの見直しとして、地上システムのクラウド化の推進が今後も進むことを想定した場合、パブリッククラウド上に構築された地上システムをアタックサーフェスとするリスクシナリオを検討することが考えられる。また、あわせて宇宙分野を中心に近年新たに起こったインシデント事例等を参照して新たな脅威手法によるリスクシナリオを追加検討することも想定される。特に、衛星本体に対するジャミング等の高度な攻撃手法は、攻撃者側のコストの観点から従来は実現可能性が高くないと想定されていたが、近年の緊迫する国際情勢やウクライナ戦争におけるロシア政府系ハッカーによる Viasat へのサイバー攻撃をはじめとする一連のサイバーインシデントの事例を鑑み、衛星に対する国家支援型の高度な攻撃が行われる可能性を考慮する余地がある。こうした高度な脅威に対する対策も検討することが考えられる。

（3） 安全保障用途等に応じたより高度な対策について

安全保障領域向けの衛星、地上設備、関連サービスの市場が拡大する中、今後は経済産業省ガイドラインで示しているベースラインのセキュリティ対策に加え、安全保障用途に応じた、より高度な対策に対応できることが望ましい。昨年度報告書で整理したとおり、NIST SP 800-53/171 の全ての管理策を一律に求めることは、民間宇宙事業者、特に中小規模事業者にとって人員面・コスト面の負担が大きい。このため、まず共通のベースライン要求を明確にし、その上で、システムの重要度やミッションの特性、想定される脅威に応じて追加対策を選定する考え方が重要である。

米国でも、CNSS から公表される文書や DoD RMF が全体方針を示す一方、実際には契約文書や仕様書に明記された具体的要件が最も強い拘束力を持つとされている。また、米国では、対象範囲の拡大や運用面の厳格化、継続的な監視・評価への移行が進みつつある。

我が国においても、こうした動向を踏まえ、関係省庁と協力し、より高度なセキュリティ対策の在り方を検討していく必要がある。

（4） 宇宙セキュリティ確保に向けた高度な対策の実装について

（4）において取り上げる 1）～3）の事項は、現時点での制度化・標準化の進展度を踏まえ、現行ガイドラインの基本的な考え方及び既存の要求事項との整合を確保しつつ、段階的に反映していくことが適当である。

具体的には、サプライチェーンセキュリティは、SBOM の活用、委託先管理、クラウド認証等の観点を既存記載に追加・充実する方向で整理することが考えられる。

暗号の実装は、現時点で特定の方式を一律に求めるのではなく、PQC 移行を見据えた現状把握、影響評価、更新容易性の確保等を推奨事項として位置付けることが適当である。

また、ゼロトラストや AI セキュリティ等は、今後の制度・実務の進展を踏まえつつ段階的に取り込む事項として整理し、あわせて他ガイドラインや将来的な制度要件との対応関係を分かりやすく示していくことが望ましい。

1) サプライチェーンセキュリティについて

昨今のサプライチェーンを取り巻く環境・脅威を踏まえると、調達段階で調達先（委託先・再委託先を含む）のリスクを可視化・評価することが重要となる。

また、国内では、安全保障に関連する市場が拡大していることから、関係省庁との契約の中で、重要経済安保情報を取り扱う場合が想定される。関連法案に基づき、セキュリティクリアランス制度に則った管理が求められる点に関する言及が望まれる。

加えて、海外動向を踏まえ、同盟国・商用パートナーとの連携を前提に、クラウド認証等の要求が求められ得ることを明示することが望ましい。あわせて、ソフトウェアサプライチェーンセキュリティ含めて、構成・部材・ソフトウェア依存関係を把握し、調達後も含めた継続的な管理につなげることが推奨される（例：SBOM の活用等）。なお、関連するガイドラインや制度の動向は変化が速いため、参照文書・要件を定期的に見直すことが望ましい。

表 3-17 サプライチェーンセキュリティ、SBOM（ソフトウェア部品表）について

区分	ガイドライン Ver2.0 までの検討内容	関連する動向
サプライチェーンセキュリティについて	衛星の調達→製造→運送・打上→運用・保守→廃棄に至るライフサイクルの各フェーズにおけるサプライチェーンセキュリティ対策について、具体的な対策内容や留意事項を 3.2.2 (1) (f)「サプライチェーンに対するセキュリティ対策」、3.2.3 (1) (g)「外部サービスの利用」、3.2.4 (1) (e)「外部サービスの利用」、3.2.5「開発・製造設備」に記載。 クラウドセキュリティについて、3.1.2(2)(a)「ISO/IEC 27017 ISO/IEC 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範（ISO/IEC）」にて記載。	**米国 DoD は、2027 年度までに全情報システムでゼロトラストを導入する方針**を掲げており、宇宙を含む安全保障分野での同盟国・商用パートナーとの連携強化が進んでいる。これに伴い、将来的に、日本の衛星通信事業者にも DoD 基準準拠やゼロトラスト対応が求められる可能性がある。 国内では、**経済産業省が重要インフラのレジリエンス強化を目的に、調達先リスクの可視化・評価を行う「SCS 評価制度（セキュリティ対策評価制度）」を整備**。また、**製品・サービスの信頼性を第三者が確認する「JC-STAR 制度」を整備**し、企業のセキュリティ・信頼性向上を促している。 また、関係省庁と契約し、**「重要経済安保情報」を扱う場合には、セキュリティクリアランス制度に則った管理が必要**であるほか、他国の政府と契約する際にも、Confidential 相当の情報を扱う際は同様の対応が求められる。

		EU 宇宙法案で、サプライチェーンリスク管理フレームワークの構築や、**ミッションの技術的統制に不可欠な「非 EU 原産」の重要資産のインベントリ作成が義務化**する。 **クラウドセキュリティは国際的にも強化傾向**にあり、米国では FedRAMP とゼロトラストの統合の検討が進むほか、EU では EUCS（欧州クラウド認証制度）の導入により域外クラウド事業者にも対応が求められる可能性がある。
SBOM（ソフトウェア部品表）について	3.2.2（1）（d）「衛星搭載機器の脆弱性対策」等において、SBOM に基づく対策の概要やコラム等を記載。	**米国・欧州を中心に、SBOM に関する議論や規制が加速化**している。 2023 年 5 月、Quad（日米豪印戦略対話）は、政府調達ソフトウェアのセキュリティ確保に向け、ソフトウェアの安全な開発・調達・運用に関する方針を示した共同原則を発表した[26]。 2023 年 10 月、CISA 及び米国内外の 17 のパートナー機関は、セキュアバイデザイン・セキュアバイデフォルトの実践に向けたガイダンスを改訂し、ソフトウェア開発者に対し、安全な製品を出荷するために必要な措置を講じるよう促した。 2025 年 6 月、EU において EU 宇宙法案が発表された。当該法案では、サプライチェーンリスク管理フレームワークを策定し、特にソフトウェアサプライチェーンセキュリティの実施に向け、ベンダとの契約内容の確認や SBOM による構成管理、署名・ハッシュによる真正性確認、ビルド／配布プロセスの管理などによりソフトウェアサプライチェーンセキュリティの実施が求められる可能性がある。

[26] Australian Government Department of the Prime Minister and Cabinet, "Quad Cybersecurity Partnership: Joint Principles for Secure Software"
https://www.pmc.gov.au/resources/quad-cybersecurity-partnership-joint-principles-secure-software

		また日本においても、欧米の取組に準じて、議論が進められている。

2） 暗号の実装について

近年、量子計算・暗号技術の進展を背景に、耐量子暗号（PQC）への移行に関する議論は国際的に加速している。日本の宇宙サイバーガイドラインでは、諸外国の記載状況や他項目との記載粒度との整合を踏まえ、具体的なアルゴリズム選定や実装手順の記載はこれまで見送ってきた。一方、米国では政府全体として PQC 移行を促す方針文書等が公表され、民間を含めた準備の必要性が高まっている。もっとも、宇宙システム固有の制約（長寿命、通信・更新制約等）を踏まえた具体的要件や分野横断の移行タイムラインは、なお整備途上である。

このためガイドラインには、米国政府や NIST 等の動向を継続的に確認しつつ、将来の PQC 移行に備えて、RSA や楕円曲線など量子計算機の登場により危殆化の可能性が高い暗号アルゴリズムが使われている箇所を洗い出し、関連するデータ・通信・更新手段も含めて整理することを推奨として記載することが望まれる。また、移行の影響を見積もり、後から暗号を切り替えられる設計と遠隔更新の仕組みの検討を推奨として記載することが望まれる。

表 3-18 暗号の実装について

区分	ガイドライン Ver2.0 までの検討内容	関連する動向
暗号の実装について	暗号の実装に当たって参考となる文書や、留意すべき事項を 3.2.2 (1)(a)「RF 通信の保護」が記載。	米国 NIST、CISA、NSA 等関係省庁により、耐量子計算機暗号に関する取組が、加速化している。 2024 年 8 月に PQC に関する標準規格として 3 つのアルゴリズム（FIPS203、204、205）を発表した[27]。 2025 年 11 月、戦争省（旧国防総省）は PQC 移行に向けた準備を命ずる覚書「Preparing for Migration to Post Quantum Cryptography」を発表した[28]。DoD の全てのシステムを対象に PQC への移行を命じている。

[27] NIST, “NIST Releases First 3 Finalized Post-Quantum Encryption Standards”, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[28] DoW “Preparing for Migration to Post Quantum Cryptography” https://dowcio.war.gov/Portals/0/Documents/Library/PreparingForMigrationPQC.pdf https://dodcio.defense.gov/Portals/0/Documents/Library/PreparingForMigrationPQC.pdf

		2026 年 1 月、米国 CISA は、大統領令 14306 号に基づき、PQC の導入を促進するために、「Product Categories for Technologies That Use Post-Quantum Cryptography Standards」を発表した[29]。本文書は、PQC 標準を使用しているハードウェア及びソフトウェアの製品カテゴリのリストを提供している。また、現在移行中であるカテゴリの製品メーカーに対しても、PQC 機能の早期実装とテストを奨励している。

3） その他検討が望まれる項目（ゼロトラスト・セキュリティ、AI セキュリティなど）

米国では、宇宙分野において、ゼロトラスト・セキュリティを既存の安全性・信頼性確保を補完する考え方として位置付けつつ、各セグメントの特性に応じて段階的に取り入れる議論が進められている。

あわせて、AI についても、攻撃側による活用の進展を踏まえ、防御側における異常検知、監視、運用支援等への活用を視野に入れた検討が進みつつある。

我が国においても、宇宙システムの特性や運用上の制約を踏まえながら、今後、こうした要素をどのように取り扱うか検討していくことが考えられる。

4） その他ガイドラインとの対応関係について

事業者負担軽減に向けて、他ガイドラインとの対応関係について、整理方針に関する検討を進める必要がある。また、EU 宇宙法案への対応準備として、現状のガイドラインに対応している場合、どこまで対応できているのか、また対応ができていないかを確認できるようなツールがあることが望ましい。したがって、現状 NIST CSF との対応関係のみ整理しているが、必要に応じて、EU Space Act 等新たな義務的要件のマッピングが望まれる。

表 3-19 その他ガイドラインとの対応関係について

区分	ガイドライン Ver2.0 までの検討内容	事業者による意見概要（一部抜粋）
他ガイドラインとの対応関係について	**ガイドラインの要求事項について、NIST CSF との対応関係の他、リモセン法ガイドの要求事項との対応関係を記載。**	経済産業省・IPA がそれぞれ出しているチェックリストのカバレッジを確認することが難しい。

[29] CISA, “Product Categories for Technologies That Use Post-Quantum Cryptography Standards” https://www.cisa.gov/resources-tools/resources/product-categories-technologies-use-post-quantum-cryptography-standards

（5） 海外政府や関係機関とのやり取り等を想定した英訳版の作成

海外政府及び関係機関との協議・情報共有等を念頭に、2024 年 3 月に公表した「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.2.0」及び添付資料 1～3 の英訳を実施した。

今後、国際的な相互依存が一層進展する中、国際的な協調を推進する観点から、積極的な情報発信を行っていくことが求められる。

3.5 調査結果の総括及び今後の取組

昨今、衛星コンステレーションの拡大や、衛星システムと地上システムのリアルタイム連携、複数コンステレーション間の相互接続が進む中、宇宙システムは従来以上に相互依存性の高いインフラとなっている。

我が国の宇宙分野では、宇宙システムを取り巻く環境に応じて、ガイドラインの見直しが必要となる。共通のベースラインを維持しつつ、システムの重要度やミッション特性に応じた追加対策を明確化するとともに、サプライチェーンセキュリティ、暗号の実装、ゼロトラスト及び AI セキュリティ等に関する記載を、制度・技術の成熟度を踏まえつつ段階的に充実させることが求められる。あわせて、高度化する脅威を踏まえた対象範囲及びリスクシナリオの見直し、他ガイドラインや海外制度との対応関係の可視化を進める必要がある。

相互依存性が高まる中、ある事業者で把握された脅威や脆弱性が他の事業者にも波及し得る一方、攻撃手法も生成 AI の活用等により高度化・多様化していることから、各事業者が個別に最新の脅威動向を収集・分析し、検証や人材育成まで含めて対応することには限界がある。このため、個社ごとの対策を基本としつつも、官民が一体的に脅威情報を共有し、検証や教育・訓練にもつなげていく基盤を整えていくことの重要性が高まっている。宇宙業界のサイバーセキュリティに関する国際的動向、脅威情報等を国内宇宙企業と即時的、効率的に共有する基盤システム技術の開発や、検証技術の開発等も必要になってくる。

海外では、EU 宇宙法案に基づく宇宙インフラのサイバーセキュリティ要件の整備や、EU Space ISAC による情報共有基盤の強化が進んでいる。米国の Space ISAC でも、脅威評価、レポート公表などの取組が活発化している。我が国でも、2024 年 11 月に Japan Space ISAC が設立され、宇宙事業者間の情報共有・分析の枠組みづくりが始まっている。

こうした動向を踏まえれば、我が国においても、国際動向や最新の脅威情報を機動的に取り込みつつ、国内宇宙企業が即時的かつ効率的に情報共有・分析を行える基盤の整備を進める必要性は、今後一層高まっていくと考えられる。また、関係省庁との連携及び国際的な情報発信・協力を通じて、宇宙産業サプライチェーン全体のサイバーセキュリティ向上と国際競争力の確保を図っていくことが求められる。

4. 全体総括

本事業では、「宇宙産業 SWG」を開催したほか、民間宇宙事業者におけるサイバーセキュリティ対策に関する課題等の調査・分析・整理を実施した。特に、国内外の宇宙セキュリティに関する取組動向を調査したほか、宇宙のサイバーセキュリティに関する課題や動向について、米国を対象に海外調査を実施した。そして、調査結果を踏まえ、今後想定される取組について検討・整理した。

令和7年度産業サイバーセキュリティ対策の強化に向けた環境整備事業
（ソフトウェアのセキュリティ確保等に関する調査）報告書 - 第 2 編
宇宙 SWG 関連

2026 年 3 月

株式会社三菱総合研究所
安全保障政策本部
TEL (03)6858-3578

経済産業省 御中

令和7年度産業サイバーセキュリティ対策の強化に向けた環境整備事業
（ソフトウェアのセキュリティ確保等に関する調査）

報告書 - 第３編

工場 SWG 関連

2026 年 3 月 31 日

安全保障政策本部

目次

表 目次

1. はじめに

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普及活動に関し、産業サイバーセキュリティ研究会WG1における産業分野別SWGの1つである「工場SWG」では、これまで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や、工場のスマート化を進める上での対策ポイントをまとめた別冊などを作成してきた。

本調査では、工場セキュリティに関する国内外の政策・技術動向、関係団体の活動を踏まえ、これらガイドラインの効果的な普及・啓発を行うことを目的として、サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）と連携して、工場セキュリティガイドラインを含めた工場におけるセキュリティの普及・啓発を実施した。

2. 工場ガイドラインの普及・啓発のための周知活動

2.1 工場セキュリティ共創 SWG を活用した普及・啓発の概要

サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）の「業界連携 WG」傘下の「工場セキュリティ共創 SWG」と連携して、工場セキュリティに関する普及・啓発活動を実施した。工場セキュリティ共創 SWG は、製造業におけるセキュリティ関係者をメンバーとして集め、サプライチェーンを含んだ製造業における工場システムセキュリティの普及・底上げを目的としている。活動内容としては、工場セキュリティガイドラインの更新・拡充に係る情報共有と議論、工場セキュリティに関する対策事例や最近の攻撃事例等のトピックについての情報共有などを行っている。

本調査では工場セキュリティ共創 SWG の場を活用し、工場セキュリティガイドラインの普及や工場セキュリティにおける課題に関するディスカッションを行った。

表 2-1 工場セキュリティ共創 SWG の活動概要

活動目的	・ 工場システムにおけるサプライチェーン全体のセキュリティ向上 ・ 工場システムに関わる業界や組織が協力した対応体制の構築 ・ 上記の実現を通じた、日本の製造業の競争力強化
活動内容	・ 工場システムに関するセキュリティ関連情報の共有、及び意見の収集 ➢ 「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」の普及啓発 ➢ 「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」の更新・拡充に係る情報共有 ➢ 工場セキュリティに関する対策事例、最近の攻撃事例等トピック等の情報共有 ➢ 業界・企業における工場セキュリティ対策状況の定期的な確認・共有 ➢ セミナー・トレーニング、サイバー演習等を通じた人材育成　　等 ・ なお、活動を通じて得られた課題や要望は、経済産業省工場 SWG や関連組織等において議論を行い、工場システムのセキュリティ向上に向けた政策・仕組み作り等に反映していく。
メンバー	・ リーダ：日立製作所　中野　利彦　氏 ・ サブリーダ：産業サイバーセキュリティセンター　佐々木　弘志　氏 ・ メンバー ➢ 工場セキュリティに関連するユーザ側業界団体（企画・マネジメント対策の推進者） ※工場 SWG オブザーバ業界団体、SC3 加盟団体（製造業） ・ サブメンバー ➢ 工場システムに関わる制御システムベンダ、工作機器メーカー ➢ 工場システムに関わるセキュリティベンダー ➢ 工場システムセキュリティに関わる団体
参加組織のメリット	・ 工場セキュリティ関連情報や、他業界・他社の情報の入手による、自業界・自社の工場セキュリティの向上 ・ 自業界・自社の情報共有による、業界全体としての対策レベルや信頼度の向上
活動計画	・ 年間 2 回程度の会合開催、必要に応じて、配下に検討グループを設置し集中討議 ・ 工場システムにおけるセキュリティ対策状況の把握・共有、関連制度等の情報共有

2.2 工場セキュリティ共創 SWG を活用した普及・啓発の内容

（1） 工場セキュリティ共創セミナー

1） 開催概要

日時　2025 年 9 月 24 日（水）16:00～18:00
参加人数：42 名
議題
1　開催挨拶
　サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）業界連携 WG　松本　哲也　氏
2　企業における工場セキュリティ取組事例（2 件）
3　関連団体による工場セキュリティ普及の取組（1 件）
4　2025 年度の工場セキュリティ共創 SWG の活動方針
　工場セキュリティ共創 SWG　リーダー　中野　利彦　氏

（2） 第 3 回工場セキュリティ共創 SWG

1） 開催概要

日時　2025 年 11 月 24 日（月）16:00～18:00
参加人数：27 名
議題
1　開催挨拶
　工場セキュリティ共創 SWG　リーダー　中野　利彦　氏
2　講演（3 件）
3　フリーディスカッション【工場におけるサプライチェーンセキュリティの課題について】
　工場セキュリティ共創 SWG　リーダー　中野　利彦　氏

2） ディスカッション概要

工場におけるサプライチェーンセキュリティの課題についてディスカッションが行われた。具体的には、「サプライチェーン対策評価制度への期待について」、「OT におけるサプライチェーン対策評価制度の必要性について」、「中小企業のサプライチェーン対策について」、「システム開発の課題について」、「ガバナンスの課題について」、「その他」に関して議論がされた。

（3） 第4回工場セキュリティ共創 SWG における普及・啓発活動

1） 開催概要

日時　2026 年 3 月 4 日（水）16:00～18:00

参加人数：19 名

議題

1　開催挨拶

工場セキュリティ共創 SWG　リーダー　中野 利彦　氏

2　講演（2 件）

3　フリーディスカッション【工場におけるサプライチェーンセキュリティの取組について】

工場セキュリティ共創 SWG　リーダー　中野 利彦　氏

2）ディスカッション概要

工場におけるサプライチェーンセキュリティの課題についてディスカッションが行われた。具体的には、「OT サプライチェーン対策の取組について」、「OT におけるサプライチェーン強化に向けたセキュリティ対策評価制度（SCS 評価制度）の必要性について」、「OT サプライチェーンセキュリティの課題について」、「その他」に関して議論がされた。

2.3 工場セキュリティ共創 SWG を活用した普及・啓発を踏まえた今後の工場セキュリティにおける課題

工場セキュリティ共創 SWG におけるディスカッションを踏まえて、工場セキュリティにおいて以下の 4 点の課題が確認された。

（1） サプライチェーンの可視化と重要度に応じた管理の不足

工場セキュリティにおける課題として、サプライチェーン全体の実態を十分に把握し、重要度に応じて管理する仕組みがまだ不十分なことがあげられる。近年、工場を取り巻く関係者は、直接の取引先だけでなく、グループ会社、保守ベンダー、制御機器メーカー、クラウド事業者、ネットワーク連携先、さらには海外拠点まで広がっており、どの企業がどの設備や情報に影響を与え得るのかを一覧で捉えるだけでも大きな負荷がかかる。実際、工場セキュリティのディスカッションにおいても、自社のサプライチェーンのリスク管理ができておらず、重要度が判断しにくいことや、相手先ごとにアンケートや確認作業を行う工数が大きいことが指摘されていた。また、グローバルに事業を展開する企業ほど、国内外から多様なチェックリストへの回答を求められ、対応が重複しやすいという問題もある。さらに、グループ会社ごとに対策状況の濃淡が大きく、同じ枠組みで管理したくても成熟度の差が障壁になることも確認された。

この課題に対しては、まず自社工場を中心に、どの企業がどの資産・工程・システムに関与しているかを可視化し、重要度に応じて管理対象を段階分けすることが必要である。その上で、アタックサーフェースマネジメントツールの活用に加え、アンケートやヒアリングの実施、既存ガイドラインの参照を通じて評価の精度を高め、グループ会社から海外拠点、さらに取引先へと対象を順次拡大していく進め方が現実的である。加えて、業界共通の質問票や確認項目を整備し、取引先に対して各社が個別に行っている重複的な確認を減らすことで、確認の負荷を抑えながら、実効的なサプライチェーン管理を実現していくことが求められる。最終的には、事故時にどこが止まるのか、誰への影響が大きいのかまで見通せる管理に発展させることが重要である。そのため、管理の起点となる台帳整備を継続的に更新できる体制も欠かせない。このような取組を支援するための取組やガイドの必要性なども検討される。

（2）OT に適した共通基準・評価制度・調達要件の未整備

工場セキュリティにおける課題として、工場や OT の実態に合った共通基準や評価制度、調達時の要求事項がまだ十分に整っていないことがあげられる。現在の制度や評価の枠組みは IT 環境を前提にしたものが多く、そのまま工場へ適用すると、止められない設備や古い制御機器を抱える現場には適合しにくい。

工場セキュリティ共創 SWG のディスカッションでも、OT 領域を既存の SCS 評価制度へ取り込むことへの期待が示される一方で、OT は業界差が大きいため、最初から高い基準を求めるのではなく、最低限守るべき対策から設計すべきだという意見が出ていた。また、製品・部品の製造側と調達側の双方が、何を確認し、どのレベルまで求めればよいか分からないという問題も共有されている。実際には、制御システムの調達仕様書をセキュリティ部門が整備し、調達部門と連携しようとする動きや、業界として共通的な発注書を検討する動きも出ており、標準化への期待は高い。

このため、今後は業界ごとの差異を踏まえつつ、OT 向けの最低基準、共通チェックリスト、標準的なシステム構成例、調達仕様書、共通発注書などを整備し、工場現場で使える形に具体化する必要がある。さらに、こうした取組を進めるに当たっては、認証制度、工場セキュリティガイドライン、半導体分野の既存ガイドラインなどとの関係性を整理し、将来的に評価の仕組みを検討する場合にも、それが単独で存在するのではなく、既存の枠組みや実務と整合的なものとなるようにすることが重要である。加えて、海外と取引する企業にとっては、国内制度を国際的な枠組みやグローバルスタンダードと連携させ、国内外で過度に異なる要求を受けない環境を整えることが、実務上の負担軽減と制度の普及の両面で欠かせない。工場セキュリティの現場改善を促すこと目的とした制度を検討していくことが望まれる。

（3）中小企業を含む費用負担と実装支援の不足

工場セキュリティにおける課題として、サプライチェーンの下流や中小企業において、セキュリティ対策に係る費用負担および実装支援の仕組みが十分に整備されていない点が挙げられる。 工場セキュリティの必要性は理解されつつあるものの、現場では依然として対策が追加コストとして見られやすく、特に収益余力の小さい企業ほど後回しになりやすい。

工場セキュリティ共創 SWG のディスカッションでも、OT セキュリティは現場に普及していない、コスト負担ができない事業者には対策を進めにくい、IT/OT を問わず誰が負担するかが決まらないため前に進まない、といった声が挙がっていた。一方で、サプライチェーン下流の中小工場に対し、自社が費用を負担して対策を進めている例も示されており、個社努力だけに頼る限界も見えている。また、補助についても、全ての中小企業を一律に支援するのではなく、重要な企業に絞って重点的に底上げする考え方が必要だという示唆があった。加えて、現場ではセキュリティ投資が生産量や売上に直結しにくいため、必要性を理解していても予算化に踏み切れないという構造的な難しさがある。

この課題に向けては、まず対策を一律に求めるのではなく、リスクと影響度に応じて優先順位を付け、最低限必要なチェックリストや対策メニューを明確にすることが重要である。その上で、元請企業や中核企業による重点支援、補助制度の活用、教育機会の提供、テンプレートや標準文書の提供を組み合わせ、実装のハードルを下げる必要がある。また、コストとリスクのトレードオフを経営層に見える形で整理し、「対策しないことの損失」まで含めて説明することも重要である。限られた予算の中でも、選択と集中によって影響の大きい中小企業から底上げを図り、業界全体の最低水準を引き上げる取組が求められ

る。

（4）ガバナンス・人材育成の定着不足

工場セキュリティにおける課題として、工場セキュリティを一時的な点検にとどめるのではなく、全社的なガバナンスの下で継続的に運用・定着させる体制が、いまだ十分に整備されていない点が挙げられる。OT セキュリティは情報システム部門だけで完結せず、事業部、工場現場、調達部門、保守部門、ベンダー、グループ会社が連携しなければ実効性を持たない。

各所との連携が必要である中、工場セキュリティ共創 SWG のディスカッションでは、事業部と協力して OT セキュリティを確保することに苦労していること、二次受け・三次受けも含めた支援体制が必要であること、グループ会社ごとに取組の濃淡が大きく教育が難しいことなどが共有された。実際に、教育機会を設けた事例では、各社の理解度や体制に差があり、同じ内容を伝えるだけでは十分に浸透しないという課題も見えている。加えて、外せない設備にどう対策を実装するか、システム開発や保守のライフサイクルにどう組み込むか、点数が高い企業でも被害が起きる現実をどう踏まえるか、といった継続運用上の論点も大きい。さらに、人材面では、製造業のセキュリティ担当者の流動性が高いことや、資格・育成施策のメリットを現場にどう結び付けるかも課題として挙がっており、継続的に担い手を育てる仕組みが不可欠である。

この課題に対しては、まず全社としての責任分担を明確化し、セキュリティ部門と資材・調達部門、事業部門が共同で基準策定と運用を進める体制を築く必要がある。その上で、グループ会社や委託先も含めた定期教育、実務者向け訓練、人材育成施策、知見共有の場を継続的に設け、属人的な運用から脱却することが重要である。さらに、設計、開発、導入、保守、更新の各段階にセキュリティ確認を組み込み、設備停止が難しい現場には後付け対策や段階的改善策を用意するべきである。このような工場セキュリティにおけるガバナンス構築を支援する制度・ガイダンスを整理し、人材育成などのガバナンス構築をサポートする仕組みが必要である。

3. 全体総括

本調査では、サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）と連携して、サプライチェーンを含んだ製造業における工場システムセキュリティの普及・底上げを目的に「工場セキュリティ共創 SWG」を開催した。工場セキュリティ共創 SWG において、工場セキュリティガイドラインの普及・啓発や工場セキュリティにおける課題・取り組みについてディスカッションされた。

今後、2.3 節に取りまとめた工場セキュリティにおける課題を踏まえて、国内の工場システムのセキュリティのさらなる向上につながる支援を行うことが望まれる。

令和7年度産業サイバーセキュリティ対策の強化に向けた環境整備事業
（ソフトウェアのセキュリティ確保等に関する調査）報告書 - 第 3 編
工場 SWG 関連

2026 年 3 月

株式会社三菱総合研究所
安全保障政策本部
TEL (03)6858-3578

経済産業省 御中

令和7年度産業サイバーセキュリティ対策の強化に向けた環境整備事業
（ソフトウェアのセキュリティ確保等に関する調査）

報告書 - 第４編

JC－STAR活用も含めたIoT製品セキュリティ向上

三菱総合研究所

安全保障政策本部

2026年3月31日

目次

図 目次

表 目次

1. はじめに

近年、社会においてIoTの数が急速に増加しており、IoT製品の脆弱性を狙ったサイバー攻撃の脅威も増加傾向にある。その対策として、諸外国においてIoT製品に対する認証制度が開始されており、我が国においても令和6年度にJC－STAR（セキュリティ要件適合評価及びラベリング制度）を立ち上げ、一部運用を開始している。対策を広く進めるためには当該制度を広く普及させることが重要であり、その普及促進のために各業界団体とも議論しながら進めていく必要がある。

本事業では、IoT 製品の活用が進む領域の1つとして、工場システム構成製品[1]におけるJC－STAR活用検討を実施し、また JC-STAR 制度の開始を踏まえた「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」の改定に向けた検討、海外の認証制度との調和を進めるためのIoTセキュリティ評価関連制度に関する海外動向調査の合わせて 3 点の調査を実施した。

[1] 仕様書では、「工場関連 IoT 製品」と記載されているが、経済産業省との議論を踏まえて「工場システム構成製品」に名称を変更。

2. 工場システム構成製品におけるJC-STAR制度の活用検討

2.1 工場システム構成製品におけるJC-STAR制度の活用方針及びセキュリティ要件の検討

本節では、工場システム構成製品における JC-STAR 制度の活用検討に向けて、活用方針と★2 のセキュリティ要件の検討を行った。

2.1.1 工場システム構成製品におけるJC-STAR制度の活用方針

（1） 対象製品・全体像の整理

2.2.1、2.2.2 における事前ヒアリングや検討会での議論を踏まえて、非 IP 通信[2]は IP 通信と比較して外部攻撃到達性が低く相対的なセキュリティリスクは小さいが、OT 環境においては保守端末などを通じた内部攻撃なども確認されていることから、工場システム構成製品における JC-STAR 制度においては IP 通信のみならず非 IP 通信の機能をもつ製品も対象とすること望ましいことが確認できた。そのため、従来の JC-STAR 制度と違い、工場システム構成製品における JC-STAR 制度においては IP 通信のみならず非 IP 通信の機能をもつ製品も対象として整理した。工場システム構成製品としては、工場（≒OT 環境）で設置されている通信機能を持つ産業用製品（例：PLC、センサなど）を対象とする。OT 環境の定義は、Purdue モデルのレベル 3 以下を想定している。PC やタブレットなどの汎用製品、ソフトウェアのみの製品、完全にスタンドアロンな機器は、JC-STAR 制度の対象外であるため、工場システム構成製品の対象外とする。

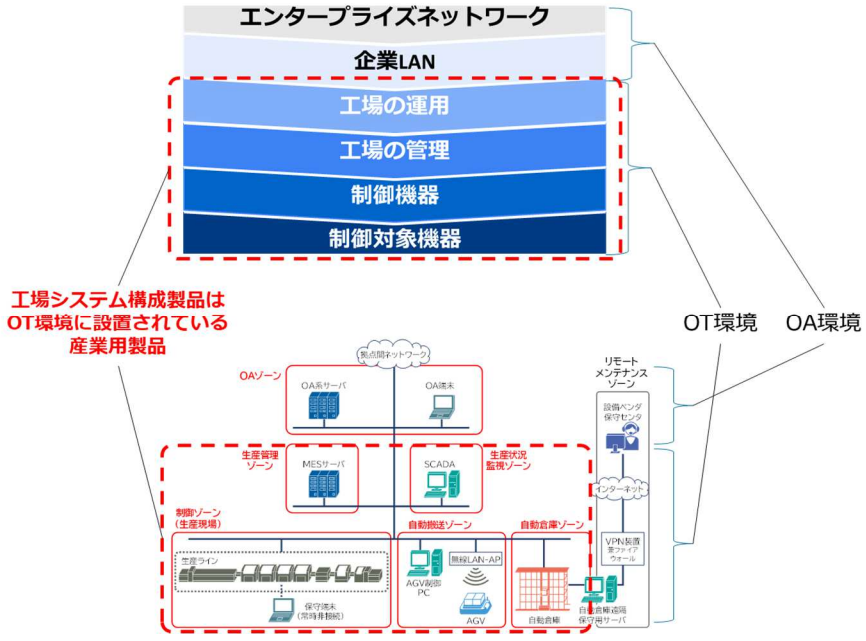


図 2-1 工場システム構成製品の対象

[2] 非 IP 通信とはインターネットプロトコル（IP）を利用していない全ての通信を示し、シリアル通信や USB 経由の通信なども該当する。

工場システム構成製品における JC-STAR 制度については IP 通信のみならず非 IP 通信の機能をもつ工場システム構成製品を対象とするが、現行の JC-STAR 制度の★1 では、工場システム構成製品に限らず全ての IoT 製品を対象とする観点から、対象製品は IP 通信機能を持つものに限定されている。このため、工場システム構成製品における JC-STAR 制度では、★1 は IP 通信機能を持つ製品に限定しつつ、★2 以降は非 IP 通信を含む通信機能を有する製品を対象とした。低リスク業務で利用される非 IP 通信の機器については制度の対象外とするが、相対的なセキュリティリスクの低さを踏まえ、合理的な整理と考えられる。★2 以上については、工場システム構成製品に限定した基準となることから、海外規格も参考に有効期間を当初の 2 年以上とする可能性も今後検討する。

また、工場内で利用される工場システム構成製品のリスクは一定ではなく、そのうちの一部は★1 相当のセキュリティ要件で充足するものも存在すると考えられる。従って、工場内で利用される工場システム構成製品のうち相対的にリスクの高い業務で活用される製品を特定し、それらの製品を想定して★2 基準を策定した。★3 は当初より「政府機関等や重要インフラ事業者で利用される製品」を対象とした基準と定義されているため、当該定義を踏襲する想定である。

	対象製品	セキュリティ要件	有効期間
適合基準★3	下記のうち重要インフラ事業者が調達する製品（例：（重要インフラで設置される）SCADA、DCS、PLCなど）	★2に加えて重要インフラ対応を想定した要件を追加	TBD
適合基準★2	リスクの高い業務で活用される通信機能付きの工場システム構成製品（例：PLC、モーションコントローラなど）	★1に加えて工場システム構成製品独自の要件を追加	TBD
統一的な最低限の適合基準★1	工場に設置されているIP通信機能を持つ工場システム構成製品（例：センサー、リモートI/Oなど）	現状の★1通り	2年

図 2-2 工場システム構成製品における JC-STAR 制度の各レベル(★)の対象製品

上記方針に基づいた各レベル(★)の対象想定製品はあるものの、それぞれの工場システムの構成によってリスクの考え方が変わるため、想定対象製品に限らず、実際には通信機能を持つ工場システム構成製品は全て適合ラベルを取得可能とすることを想定する。(★1 のみ IP 通信機能を持つ製品に限定)

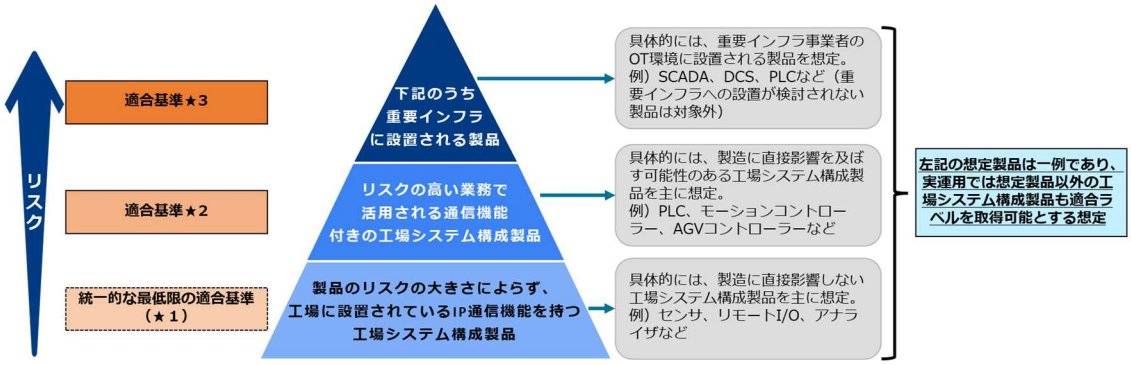


図 2-3 各レベル(★)における対象製品例

(2) JC-STAR 制度の対象の拡大

JC-STAR 制度の対象製品は、機器(ハードウェア)が含まれている製品である必要があり、ソフト

ウェアのみの製品は対象外である。また、セキュリティ機能を購入後に追加できる製品は JC-STAR 制度の対象外であり、汎用の PC、スマートフォン、タブレット等は対象外となり、当該製品群は工場システム構成製品の基準においても対象外となる。JC-STAR 制度の適合ラベルを取得できる製品の単位は、同一バージョンのファームウェアを有するかで判断されることとなっており、1 つのハードウェアに複数のファームウェアが混在する、またはファームウェアの違う複数のハードウェアが組み込まれているような、システム製品については 1 つの製品として適合ラベルを取得することは難しい。

一方で、工場システム構成製品はシステム製品として検討されているケースも多く、JC-STAR 制度の対象を拡大させることが望まれる。

ラベルの対象をシステム製品に拡大した場合には、「システム製品におけるラベル取得単位」、「システム製品の申請方法」の 2 点の検討が必要である。「システム製品におけるラベル取得単位」としては、ハードウェア単位、販売されているパッケージ単位（複数のハードウェアを組み合わせている製品含む）の 2 つの方法が考えられ、販売されるパッケージ単位とする方針で進めることとした。「システム製品のラベル申請方法」としては、システム製品を構成する機器単位でラベル取得の申請書を作成・取りまとめて申請する方法、機器を組合せたシステム製品単位でラベル取得の申請をする方法の 2 つの方法が考えられ「システム製品単位でラベル取得の申請」をする方針で進めることとした。

このように、システム製品の JC-STAR 制度を「販売されているパッケージ単位」かつ「システム製品単位で 1 つのラベル取得の申請書」で運用する場合の課題を「申請書類」、「延長申請の条件」、「有効期間」、「カスタムされた製品の対応」の 4 つに整理した。特に「カスタムされた製品の対応」については、工場システム構成製品独自の課題であり、今後カスタム製品の対応を検討する必要がある。

申請書類	申請時の書類として、従来の申請書類に加えてP.6で示した「システム製品を構成している機器の一覧」を提出することで問題ないか。 また、「システム製品を構成している機器の一覧」もP.6で示した項目以外に必要な情報はあるか。
延長申請の条件	延長申請（期限延長）を実施する場合は、ラベル取得時に提出した「システム製品を構成している機器の一覧」におけるコンポーネント内訳の変更がないこと、という条件を現在検討中の★1,★2における延長申請の条件に加えることで問題ないか。
有効期間	システム製品に対象を広げた場合に有効期間について、現状の2年で問題ないか。
カスタムされた製品の対応	ラベル取得時に提出した「システム製品を構成している機器の一覧」におけるコンポーネントの内訳が異なるカスタム製品の場合は、別途申請が必要と言う整理で問題ないか。

図 2-4 システム製品を対象とした JC-STAR 制度の運用における課題

（3） 普及・促進策の検討

2.2.1、2.2.2 における事前ヒアリングや検討会での議論を踏まえて、具体的な普及・促進策について、「関連制度への組み込み」、「工場システム構成製品に対するセキュリティ意識の向上」、「JC-STAR 制度の取得価値の向上」の 3 つの区分で検討した。特に「工場システム構成製品に対するセキュリティ意識の向上」については、現行ガイドラインにおける JC-STAR 制度の活用推奨（または必須化）に関する

内容の追記に加えて、工場システム構成製品に対するセキュリティ対策の必要性に関する理解を促進するために様々な観点の支援策を以下のとおり検討した。

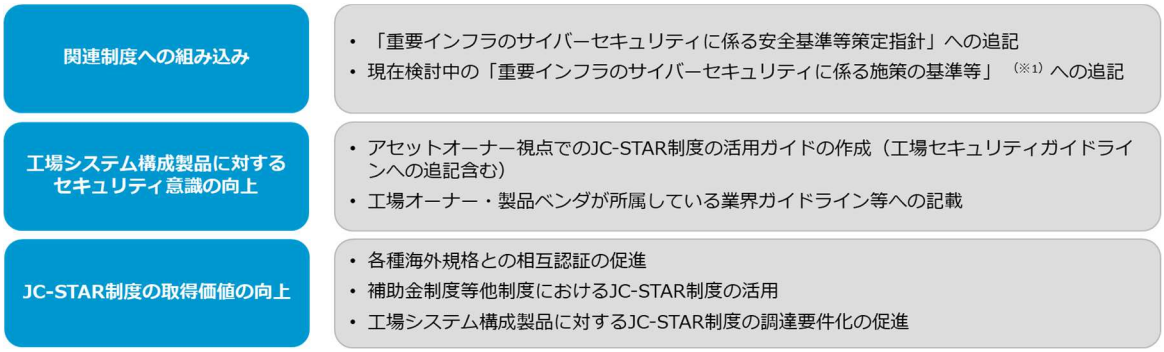


図 2-5 工場システム構成製品における JC-STAR 制度の普及・促進策の整理

上記を踏まえ、また JC-STAR 制度の主目的を踏まえて、工場システム構成製品を調達する「工場オーナー」視点と工場システム構成製品を製造する「工場システム構成製品ベンダ」の双方の視点で JC-STAR 制度活用のメリットを整理した。工場オーナーにとってのメリットとしては、調達製品で必要なセキュリティ要件の検討の簡易化や設備の用途・重要度に応じたセキュリティ要件の検討の簡易化などが挙げられる。工場システム製品ベンダにとってのメリットとしては、調達側への説明コストの低減や海外展開時のセキュリティ評価負担の削減などが挙げられる。メリットを得るためには、工場オーナーと工場システム構成製品ベンダの双方において JC-STAR 制度が幅広く使われることが重要であり、このため JC-STAR 制度の普及・促進を図る必要がある。

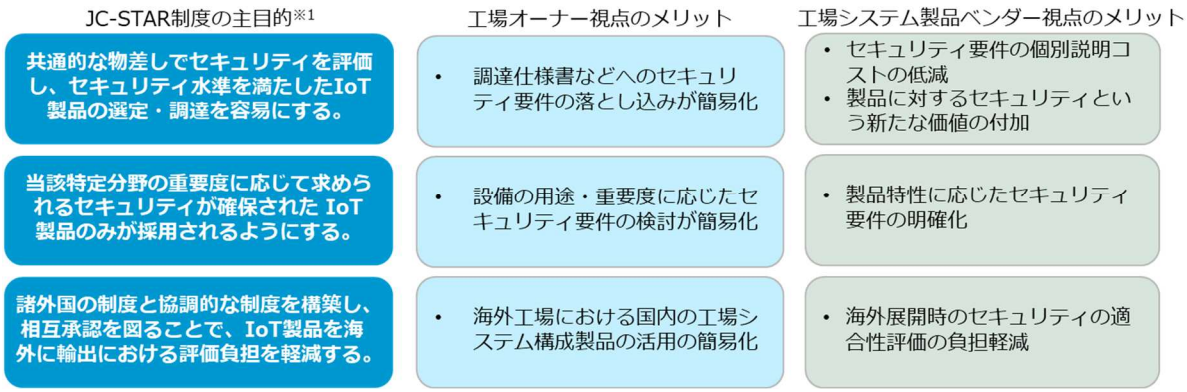


図 2-6 JC-STAR 制度のメリットの整理

2.1.2 工場システム構成製品におけるJC-STAR制度の★2 セキュリティ要件の検討

（1） ★2 のセキュリティ要件の草案検討の対象製品

★2 のセキュリティ要件検討にあたり、今後の要件策定に向けた議論の基本となる草案の取りまとめを実施した。草案策定にあたっては、まずはじめに一般的な工場システムを想定してリスクの高い業務で活用される製品の特定を行った。特定に際しては、経済産業省の「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[3]」（以下「工場セキュリティガイドライン」）におけるリスクの定義を参照した。

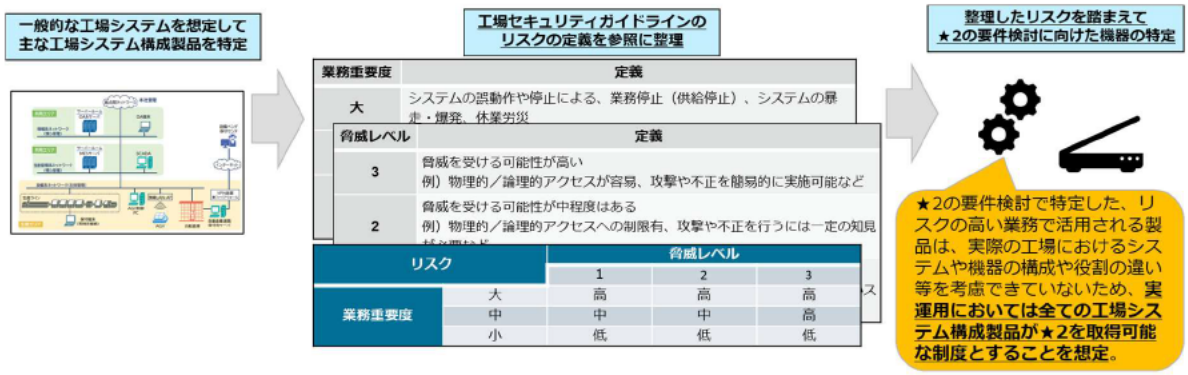


図 2-7 リスクの高い業務で活用される製品の特定イメージ

リスクの高い業務で活用される製品の特定に向けて、主な工場システム構成製品を整理する必要がある。事業分野や生産物に応じて、具体的に設置される工場システム構成製品は変わるため、工場セキュリティガイドラインを参照して、その用途に応じて主な工場システム構成製品を下表に整理した。

表 2-1 主な工場システム構成製品

分類	意見	製品の例
通信管理製品	OT ネットワークにおける通信の制御・管理	VPN 機器、無線 LAN-AP など
生産管理製品	生産計画や品質状況の管理	MES サーバ、品質管理システムなど
監視制御製品	生産状況の生産設備の監視・管理	SCADA、DCS など
制御操作製品	制御先製品の制御・操作	PLC、モーションコントローラなど
生産・運搬製品（制御先製品）	製品の生産・運搬	ロボットアーム、AGV など
計測・検知製品（制御先製品）	工場内のデータの計測・検知	各種センサなど

（2）★2 のセキュリティ要件の草案策定方針・手順

セキュリティ要件の草案策定にあたっては、工場セキュリティガイドラインおよび IPA の「制御システムのセキュリティリスク分析ガイド[4]」（以下「制御システムセキュリティガイド」）を参照し、4 つのステップに沿って★2 のセキュリティ要件の草案を策定した。

[3] 経済産業省、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」、
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_kojo/index.html
[4] 情報処理推進機構、「制御システムのセキュリティリスク分析ガイド 第 2 版」、
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

STEP1	リスクの高い業務で活用される製品の特定	• 工場セキュリティガイドラインの想定工場における工場システム例を参考にリスクの高い業務で活用される製品を特定
STEP2	STEP1で特定した製品の脅威シナリオを整理	• 特定した製品の一般的なユースケースを踏まえて、起こりうる脅威シナリオと発生可能性を制御システムセキュリティガイドを参考にして整理
STEP3	STEP2で整理した脅威に対するセキュリティ要件を整理	• STEP2で整理した脅威シナリオについて、JC-STAR制度の「セキュリティ要件一覧」(※2)をベースにセキュリティ要件を整理
STEP4	★1の要件や海外規格・要件とのギャップを整理	• STEP3で整理したセキュリティ要件について、他の規格（IEC62443やCRAなど）とのギャップを整理

適合基準番号	セキュリティ要件		【参考】海外既存制度・文書で求められるセキュリティ要件との関係性
	カテゴリ	要件	
S3.1-01	○○	××	△△
・・・	・・・	・・・	・・・

図 2-8 ★2 のセキュリティ要件の草案策定に向けた方針

STEP1 では、工場セキュリティガイドラインのシステム例に示されている主な製品とリスクの考え方を参照し、工場内の主要な重要製品を用途に応じて整理・一覧化し、リスクを整理した。一覧化した重要製品の業務重要度や脅威レベルを検討した結果、リスクが「高」となった「監視制御製品」、「制御操作製品」、「生産・運搬製品」を対象として、STEP2 以降を検討した。通信管理製品については、通信機器の製品類型[5]に包含されることから、工場システム構成製品としては対象外とした。

STEP2 では、 特定した製品の一般的なユースケースを踏まえて、想定される脅威シナリオを制御システムセキュリティガイドの脅威の整理を用いて整理した。具体的には、IPA の制御システムセキュリティガイドの脅威をベースに、攻撃の段階を第 1 段階～第 4 段階に分けて脅威シナリオのフローを整理した。また、工場セキュリティガイドラインの脅威との比較も行い、第 4 段階として「外部サーバへの踏み台攻撃」を追加した。各対象製品において、全てのシナリオフローで網羅的に脅威シナリオ（計 28 個）を作成した。

制御システムセキュリティガイドのリスク度の定義を踏まえて、作成した計 28 個のシナリオに対して影響度・脅威発生可能性を評価してリスク度を導出した。また、工場においては一定の物理アクセス制限があることを想定して、当初は★2 の要件策定にあたっては、第 1 段階が「物理的侵入」にあたる脅威シナリオは検討の対象外とした。

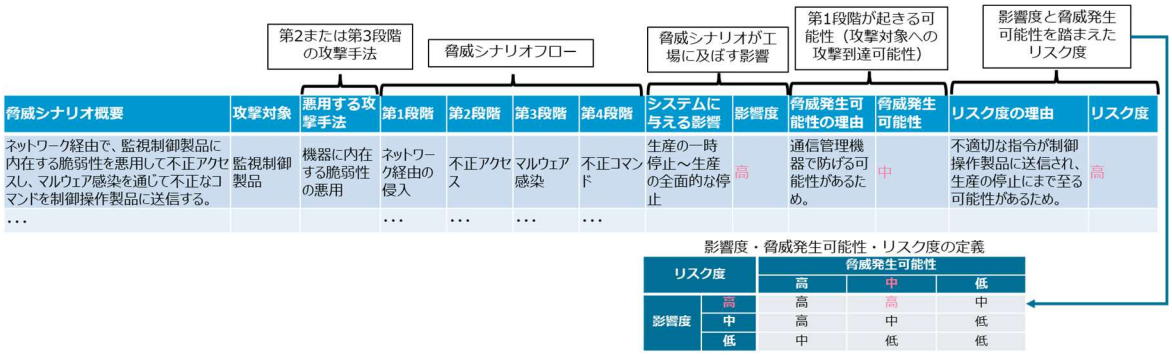


図 2-9 脅威シナリオのリスク度の特定イメージ

[5] IPA、★3（レベル 3）セキュリティ要件・適合基準案へのパブリック・コメント募集、
https://www.ipa.go.jp/security/jc-star/tekigou-kizyun-guide/pubcom/pubcom.html

STEP3、4 では、工場システム構成製品向けに調整したロングリスト[6]より、STEP2 で整理した脅威シナリオを防ぐために必要なセキュリティ要件を抽出し、EU-CRA との整合確認を行った。

ロングリストとは、ETSI EN 303 645、NISTIR 8425 等の国内外のセキュリティ要件の集合関係を踏まえて、JC-STAR 制度で対象となる製品において求められうるセキュリティ要件一覧を示している。それぞれのレベル(★1～★4)においては、各製品の想定脅威等を踏まえ、その脅威に対応するセキュリティ要件をロングリストから抽出し、その要件に準拠するために必要な水準となるよう適用要件を策定している。

一方で、ロングリストは一般消費者向けの製品を想定した海外規格なども参照されているため、工場システム構成製品に対しては適用が難しい要件も存在することから、工場システム構成製品の基準策定に際しては、工場システム構成製品の特徴(一時停止が許容できないなど)を踏まえて調整したロングリストを利用した。これにより、CRA や IEC62443 等工場システム構成製品が参照すべきグローバルスタンダードにより整合した基準とすることを目指した。

脅威シナリオよりセキュリティ要件を抽出するうえで、「悪用する攻撃手法」・「第 2～第 4 段階」とそれらのリスクを低減できるセキュリティ要件を整理した。第 1 段階は、対象製品へアクセスする手法を示しており、対象製品以外のセキュリティ対策状況によるリスクのため、上記の整理より除外した。

STEP2 で網羅的に作成した脅威シナリオのうち、リスク度「高」となったシナリオ(18 件)の「悪用する攻撃手法」・「第 2～第 4 段階」に対して、上記の整理結果を踏まえてロングリストより必要となるセキュリティ要件(48 件)を抽出した。

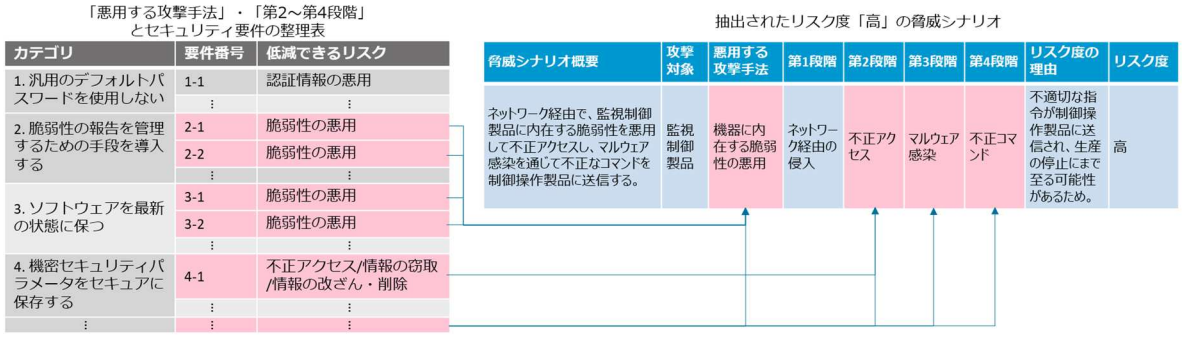


図 2-10 脅威シナリオを踏まえてセキュリティ要件の抽出方法のイメージ

(3) ★2 のセキュリティ要件の草案

2.2.2 の検討会メンバーによるレビュー及び議論を踏まえて、★2 の要件の草案については計 53 件とした。

[6] 経済産業省、「別添 1 セキュリティ要件一覧」、
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/pdf/20240315_2.pdf

2.2 工場システム構成製品における JC-STAR 制度活用検討会

2.2.1 検討会開催に向けた準備

昨今の IoT 製品におけるセキュリティリスクの高まりを受けて、EU では Cyber Resilience Act、米国でも Cyber Trust Mark 等 IoT 製品のセキュリティに関連する法律・制度が構築され、国内においても JC-STAR 制度が開始された。JC-STAR 制度の開始を受けて、JEITA や DLPA 等一部の主要な IoT 製品の業界団体においては、傘下企業に対してラベル取得の働きかけを実施し、多くの申請が出されている。また将来的には、政府機関や重要インフラ事業者等の IoT 製品の調達において本制度のラベルを取得した製品の調達の必須化を予定している。更に上記に例示した諸外国の類似制度との相互認証なども検討中である。

一方、製造業に目を向けると、工場のスマート化等により製造現場における IoT 機器の利用が加速しており、それに伴い製造現場においても IoT 機器の利用に伴うセキュリティリスクが増大している。そのため、製造業においても本制度の活用を通じたセキュア・バイ・デザインの実践が急務である。上記を踏まえ、製造業で活用されている IoT 機器（工場システム構成製品）における JC-STAR 制度の活用・制度構築方針を検討する会合として、「工場システム構成製品における JC-STAR 制度活用検討会」を開催した。

検討会開催に先立ち、メンバー・オブザーバーとして参画いただく各者に対して、工場システム構成製品における JC-STAR 制度活用に関する事前ヒアリングを実施し、検討会における論点の参考とした。

2.2.2 検討会開催結果

本検討会は、特定分野で使用される IoT 製品における JC-STAR 制度活用の一環として、各種工場で利用されている工場システム構成製品における JC-STAR 制度★2 以上の制度構築方針を検討するため、工場オーナーや工場システム構成製品ベンダに加え、それらの業界団体を中心に参加を呼びかけ、非公開で開催した。2025 年度は、工場システム構成製品における JC-STAR 制度活用に向けて、制度の全体像や各レベル（★）の対象製品の整理、★2 セキュリティ要件の草案策定、ならびに制度の普及・促進策の検討等を実施した。

（1） 第 1 回

1） 開催概要

日時　2026 年 1 月 20 日（火）13:00～15:00

議題

1　開会

2　議題

2.1　各レベル（★）の対象製品・全体像の整理について

2.2　★2 のセキュリティ要件の草案策定の方針について

2.3　工場システム構成製品における JC-STAR 制度の普及・促進策の検討について

3　閉会

配布資料

- 資料1　議事次第・配付資料一覧
- 資料2　構成員名簿
- 資料3　第 1 回工場システム構成製品における JC-STAR 制度活用検討会（事務局資料）

（2）第２回

1）開催概要

日時　2026 年 3 月 24 日（火）15:00～17:00

議題

1　開会

2　議題

2.1　JC-STAR 制度の対象の拡大について

2.2　★2 の要件の草案の最終版の確認について

2.3　工場システム構成製品における JC-STAR 制度の普及・促進策の検討について

3　閉会

配布資料

- 資料1　議事次第・配付資料一覧
- 資料2　構成員名簿
- 資料3　第 2 回工場システム構成製品における JC-STAR 制度活用検討会（事務局資料）
- 別紙1　工場システム構成製品の★2 要件の草案
- 別紙2　工場システム構成製品の★2 要件のレビューコメント・対応方針一覧資料1　議事次第・配付資料一覧

3. 「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」の改定

本項目では、「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き（経済産業省、2024年度に改定）[7]」（以下、「手引き」という）に関し、IoT 機器の製造事業者や検証事業者等がJC－STAR★1取得の評価を行う際の参考となるよう必要な見直しを実施した。

3.1 JC-STAR 対応に向けた手引きの現状の確認

手引きの改定にあたり、まず現状の手引きの構成を再確認し、何に対する改定が必要であるかの検討を実施した。

手引きは本編の他に4種類の別冊からなっており、その構成は下表の通りである。

表 3-1 手引きの本編と別冊の構成

本編（本文書） 「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」	• 検証サービス事業者が実施すべき事項や、検証依頼者が実施すべき事項や用意すべき情報、二者間のコミュニケーションにおいて留意すべき事項等を示す。 • 信頼できる検証サービス事業者を判断するための基準を記載する。
別冊 1 「脅威分析及びセキュリティ検証の詳細解説書」	• 検証サービス事業者が実施すべき脅威分析の手法や実施すべき検証項目、検証の流れを詳細に示す。 • 機器全般に汎用的に活用できる整理を目標とするが、対象の例としてネットワークカメラを実例とした手法の適用結果も示す。
別冊 2 「機器メーカーに向けた脅威分析及びセキュリティ検証の解説書」	• 機器メーカーが実施すべき事項や用意すべき情報等、意図した検証を依頼するために必要な事項を詳細に示す。 • 攻撃手法への対策例や、検証結果を踏まえたリスク評価等の対応方針を示す。
別冊 3 「検証人材の育成に向けた手引き」	• 検証人材に求められるスキル・知識を示し、それらのスキル・知識を獲得するために望まれる取り組みを示す。 • 検証人材のキャリアを構想・設計する上で考慮すべき観点を示し、検証人材のキャリアの可能性を示す。
別冊 4 「機器個別のセキュリティ検証プラクティス集」	• 令和 4 年度に実施した中小企業等が開発する IoT 機器等に対する検証の実証結果を踏まえ、代表的な IoT 機器に対して検証事業者が実施すべき事項や留意すべき事項を示す。 • 実証で実際に検出された脆弱性の情報に基づき、当該脆弱性が悪用された場

[7] 経済産業省「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」
https://www.meti.go.jp/policy/netsecurity/wg3/proven_in_japan.html

	合に想定される影響や脆弱性検出に至った検証プロセスを示す。

手引きは令和6年度改訂版において、JC-STAR の開始に伴い一部内容の改定を実施している。JC-STAR に関わる主な改定箇所としては、本編の表 1-3 がそれに当たる。

表 3-2 本編における JC-STAR 関連記述箇所(本編 表 1-3)

JC-STAR★1 適合基準 S1.1-13	本手引きを活用した評価に関する補足
IoT 製品において、外部からサイバー攻撃を受けるリスクを低減するために、IoT 製品の利用上不要かつ攻撃を受けるリスクがあるインタフェースを無効化するとともに、IoT 製品に対する脆弱性検査を実施すること。具体的には、以下の①・②のすべての基準を満たすこと。	—
① IoT 製品において、高頻度で利用され、脆弱性などのリスクが想定される以下のインタフェースについて、IoT 製品の利用上不要かつ攻撃を受けるリスクがあるインタフェースを無効化すること。 A) TCP/UDP ポート B) Bluetooth C) USB	ポートスキャンにおいては、nmap や arp-scan 等のツールが利用可能である。例えば、nmap の場合、下記のコマンドで、TCP/UDP の全ポートをポート 1 から順にスキャンを行うことができる。 `nmap -r -sS -sU -Pn -p 0-65535 "IP アドレス"` nmap のツール導入方法や検証手法については、手引き別冊 1 の「4.5.1 Nmap によるオープンしている TCP、UDP ポートの調査」に記載の内容が参考となる。
② IoT 製品に対して脆弱性スキャンツールによる既知の脆弱性検査を実施し、攻撃に悪用される可能性がある脆弱性が検出されないこと。	脆弱性スキャンにおいては、Greenbone Vulnerability Management (GVM)、Nessus、Vuls、Metasploit Framework 等のツールが利用可能である。例えば、GVM の場合、以下のステップで、Target の設定や Scan Task の設定が実行できる。 ・Target の設定 －Port list :「All TCP and Nmap top 100 UDP」 ※ポートスキャンの結果、上記設定に含まれない UDP ポートが検出された場合には、UDP の対象ポートリストを追加して作成し、設定する。 ・Scan Task の設定 －Scanner :「OpenVAS Default」 －Scan Config :「Full and fast」 Metasploit Framework の場合、指定した CVE をキーワードに、対象製品に対して既知脆弱性を悪用した攻撃が成功するか否かを確認することができる。 既知脆弱性の調査方法や Metasploit Framework による既知脆弱性に対する攻撃の試行については、手引き別冊 1 の「4.6 既知脆弱性の診断」に記載の内容が参考となる。

(★1 適合基準は更新される可能性があるため、必ず IPA の最新版を確認すること。)

3.2 手引き改定に向けた JC-STAR 事務局の要求事項の確認

手引きの改定に向け、JC-STAR 事務局がどのような修正が望ましいと考えているか、ヒアリングを実施した。ヒアリングは、2回実施し、まず改定要望について確認し、それに対する中間調査結果を踏まえて、さらにどのような改定が望ましいかの確認を行った。その結果、

- 主にツールに関しての確認を行う。コードチェックツールと脆弱性確認ツールについて調査して紹介できるようにする。
- Bluetooth 及び USB のスキャンツールに関する問合せが多く、これらのツールは現状では紹介出来ていないので、これらについて確認し、紹介できるようにする。また SBOM ツールについても確認を行う。
- 記述は検証ベンダ向けというよりも、機器ベンダ向けの手引となるが、検証ベンダからも参照されるかもしれない。★3のラボでのペネトレチェックに向けて参照できるようなツールを紹介できると良い。
- ★3検証を受けるにあたって、汎用的な方法について紹介できると良い。
- JC-STAR 取得において参照する方策としては別冊1の4章・セキュリティ検証の詳細手順に追記する形が考えられる。

ということが確認できた。

3.3 手引きの改訂案の検討

手引きの改定案の検討に先立ち、優先度の高い調査から手を付けることとし、手引きにおける Bluetooth や USB に関する記述、JC-STAR★1、★3における Bluetooth や USB に関する要求について確認をした。

表 3-3 手引きにおける Bluetooth や USB のインタフェースに関する記述

文書	Bluetooth・USB に関する記載
本紙	記載なし。
別紙 1：脅威分析及びセキュリティ検証の詳細解説書	• 「6.5 Bluetooth インタフェースに対する検証について」 コンポーネントの脆弱性調査を行い、再現性の確認を行うことを記載しているが、検証手順に関しては省略されている。 • 「6.6 セキュリティ検証に活用できるツール、技術の補足」 Bluetooth 通信の解析ツールを 2 つ紹介している。 • USB インタフェースに関する記載はなし。

別冊 2：機器メーカーに向けた脅威分析及びセキュリティ検証の解説書	• 「3.2 攻撃ポイントの分析」 アタックサーフェイスとして Bluetooth・USB を例示している。 • 「4.7.2 Bluetooth パケットキャプチャ」「5.8 ネットワークキャプチャを踏まえての対応」 Bluetooth 通信で送受信される情報を解析することで仕様等に反していないかを確認している。またその後の対応として、不要なプロファイルの無効化を紹介している。
別冊 3：検証人材の育成に向けた手引き	記載なし。
別冊 4：機器個別のセキュリティ検証プラクティス集	• UTM、GW・ルータ、モバイル端末、スマート家電に関する検証プラクティスにおいて USB を通じた（2,3,5,7 章）

表 3-4 JC-STAR★1、★3におけるインタフェース無効化やプロファイル・クラスの確認要求

★1 要件	★1 適合基準
JC-STAR★1 適合基準 S1.1-13 6-1.「すべての未使用の物理的インタフェース及び論理的インタフェースは無効化しなければならない。」	IoT 製品において、高頻度で利用され、脆弱性などのリスクが想定される以下のインタフェースについて、IoT 製品の利用上不要かつ攻撃を受けるリスクがあるインタフェースを無効化すること。 A）TCP/UDP ポート B）Bluetooth C）USB
★3 要件	**★3 適合基準**
JC-STAR★3 適合基準案 S3.1-23 6-1.「すべての未使用の物理的インタフェース及び論理的インタフェースは無効化しなければならない。」	IoT 製品において、高頻度で利用され、脆弱性などのリスクが想定される以下のインタフェースについて、IoT 製品の利用上不要かつ攻撃を受けるリスクがあるインタフェースを無効化すること。 A）TCP/UDP ポート B）Bluetooth C）USB
JC-STAR★3 適合基準案 S3.1-24 6-2.「初期化状態において、製品のネットワークインタフェースは、認証されていないセキュリティ関連情報の開示を最小化しなければならない。」	初期化状態において、IoT 製品で有効化されたネットワークインタフェースから認証なしで閲覧可能な以下を含むセキュリティ関連情報を最小化していること。 A）機器の設定情報

	B）カーネルのバージョン C）ソフトウェアのバージョン
JC-STAR★3 適合基準案 S3.1-25 6-3.「機器のハードウェアは、物理インタフェースを不必要に攻撃にさらしてはならない。」	IoT 機器は、物理的な攻撃に対して、以下の①・②のすべての保護対策が行われていること。 ①IoT 機器の不必要な物理的インタフェースは、露出から保護する仕組みを有すること。 ②IoT 機器のデバッグインタフェースを物理的または論理的に無効化していること。

また、Bluetooth や USB に関して、インタフェース検査のツールについても調査を行った。

表 3-5 Bluetooth インタフェースに関するツール

機器名	概要	インタフェース無効化確認	プロファイル解析
BlueZ	(掲載済み)Linux に実装されている Bluetooth のプロトコルスタック。Linux で動作する Bluetooth を使用するプログラムを開発する際に活用できる。また、いくつかのコマンドラインツールも提供しており、周囲に存在する機器の検索やペアリング等を行うことができる bluetoothctl や疎通確認に利用される l2ping 等がある。	○	×
Bluefruit LE Sniffer	(掲載済み)Bluetooth Low Energy(BLE)用のスニッフィングツール。このデバイスを使用すると、二つの BLE 対応デバイス間の通信の盗聴を利用したセキュリティ検証が可能である。	×	○
Android OS の HCI スヌープログ	(掲載済み)Android OS に搭載されている Bluetooth デバッグ機能で、Bluetooth ホストコントローラインタフェース(HCI)レベルの通信を記録するログ。Bluetooth スタックとコントローラ間でやり取りされるパケット(コマンド、イベント、ACL データなど)をキャプチャし、問題解析やプロトコルデバッグに利用できる。ログは Wireshark などのツールで開いて詳細解析が可能。開発者やテストエンジニアが Bluetooth 通信のトラブルシューティングや仕様適合性確認に使う。	○	○

Bluetooth SIG PTS	Bluetooth プロファイルやプロトコルの動作を自動化されたテストケースで確認できる。このデバイスを使用して、開発者は仕様適合性や互換性を効率的に評価できる。主に認証試験や開発段階で利用され、Classic Bluetooth と Bluetooth Low Energy(BLE)の各種プロファイルに対応している。	×	○
X240 (Teledyne LeCroy)	Bluetooth Classic と BLE のプロトコル解析に特化したハイエンド機材。専用ハードウェアで無線パケットをキャプチャし、物理層からアプリ層まで詳細解析が可能。暗号化ハンドシェイクやタイムスタンプ精度も高く、認証試験やセキュリティ検証に用いることが可能となる。	○	○
Ubertooth One	オープンソースの Bluetooth 開発プラットフォームで、Bluetooth のパケットをスニッフィングするために設計されたハードウェア。主に Bluetooth Classic(BR/EDR)に対応しており、2.4GHz 帯の無線通信を受信して解析できる。セキュリティ研究やプロトコル解析、Bluetooth 通信のトラブルシューティングに利用される。USB 接続で PC と連携し、Wireshark などのツールと組み合わせてパケットキャプチャや解析が可能。BLE の受信にも対応しているが、機能は限定的となる。	○	×
nRF Sniffer	Nordic Semiconductor が提供するパケットキャプチャツール。nRF シリーズの開発ボードを利用して、BLE 通信をリアルタイムでスニッフィングできる。Wireshark と連携してパケットを解析できるため、BLE アプリケーションの開発やデバッグ、プロトコル解析に役立つ。複数の接続を追跡でき、アドバタイズパケットや接続イベントの詳細を取得可能。主に BLE 専用であり、Classic Bluetooth には対応していない。	○	○

表 3-6 USB インタフェースに関するツール

機器名	概要	インタフェース無効化確認	USB クラス解析
USBTreeView	Windows で動作する USB ポートの状態確認ツール。USB ハブ構造をツリー形式で表示し、各ポートの接続状態や電源供給、速度などを確認できる。USB ポートの開放状況や無効化設定の調査に活用できる。	○	○

USBView	Windows SDK に含まれる USB デバイス情報表示ツール。USB デバイスの記述子や構成情報を確認する際に活用できる。また、ポートの状態や接続デバイスの詳細を取得でき、USB 関連の開発やデバッグに利用される。	○	○
Advisor T3	Teledyne LeCroy が提供する USB プロトコルアナライザ。USB 2.0 および USB 3.2 のトラフィックをキャプチャでき、ハードウェアトリガーによる精密なイベント検出が可能。USB デバイスのデコード、Raw ビットレベルのデバッグ、詳細なレポート生成ができる。アップグレードオプションで、USB 2.0 モデルから USB 3.2 対応へ拡張可能。	○	○
lsusb コマンド	Linux で USB デバイスの情報を表示するためのコマンドで、usbutils パッケージに含まれている。システムに接続されている USB デバイスの一覧を取得でき、バス番号、デバイス番号、ベンダ ID、プロダクト ID などの基本情報を確認できる。-v オプションを付けると詳細情報（デバイスクラス、エンドポイント、設定など）を表示できるため、USB 機器のトラブルシューティングや開発時の確認に役立つ。	○	○

表 3-4 に示したように、Bluetooth インタフェースに対する検証については、別冊1の 6.5 節に関連記述が存在する。したがって、この記述について改定案を整理した。また、USBについては、明示的な記述がないため、追記案として整理した。

これらについては、引き続き、JC-STAR 事務局との調整が必要であり、それを踏まえて最終的な改定手続きへと向かうことになる。

表 3-7 Bluetooth に関する別紙1 6.5 節の改定記述案（赤字：変更箇所）

項目	現状の記述	改定案
検証の必要性	本別冊では、Bluetooth インタフェースに対する具体的な検証手順については示していないが、IoT 機器等には Bluetooth の通信機能が実装されているものが多数存在する。その場合、Bluetooth を対象とした検証も考慮するべきである。 Bluetooth は近距離無線通信の規格であり、通信を行うためには、機器同士を近距離に配置する必要がある。そのため、ネットワーク経由での攻撃と比べると攻撃元に制約はあるものの、近年、	~~本別冊では、Bluetooth インタフェースに対する具体的な検証手順については示していないが、~~ IoT 機器等には Bluetooth の通信機能が実装されているものが多数存在するその場合、Bluetooth を対象とした検証も考慮するべきである。 Bluetooth は近距離無線通信の規格であり、通信を行うためには、機器同士を近距離に配置する必要がある。そのため、ネットワーク経由での攻撃と比べると攻撃元に制約はあるものの、近年、

	Bluetooth を対象とした脆弱性が複数見つかっていることから、Bluetooth 通信における検証の重要性も増してきている。 本節では、Bluetooth における代表的な脆弱性の概要と特徴を示した上で、セキュリティ検証における Bluetooth の脆弱性調査の方法と留意点について示す。なお、ツール等を用いた具体的な検証の手順については解説の対象外とする。	Bluetooth を対象とした脆弱性が複数見つかっていることから、Bluetooth 通信における検証の重要性も増してきている。 また、Bluetooth や USB といったインタフェースは、物理的な接続形態や通信方式の違いはあるものの、いずれも機器に対する直接的なアクセス経路となり得る。そのため、利用上不要なインタフェースが有効化されたままとなっている場合、アタックサーフェイスが不必要に拡大するおそれがある。検証においては、脆弱性の有無だけでなく、インタフェースが適切に制御されているかという観点も含めて確認する必要がある。 本節では、Bluetooth における代表的な脆弱性の概要と特徴を示した上で、セキュリティ検証における Bluetooth の脆弱性調査の方法と留意点について示す。なお、ツール等を用いた具体的な検証の手順については解説の対象外とする。
攻撃事例	近年見つかった Bluetooth を対象とした脆弱性としては、代表的なものに Blueborne や BIAS(Bluetooth Impersonation AttackS) 等がある。Blueborne は Bluetooth に関する複数の脆弱性の総称であり、Linux カーネルにおけるバッファオーバーフローの脆弱性 CVE-2017-1000251 や Linux の Bluetooth のプロトコルスタックである Bluez における領域外メモリ参照の脆弱性 CVE-2017-1000250 を含む。BIAS は Bluetooth のプロトコル仕様における脆弱性であり、ペアリング済みの機器の一方になりすましてもう一方の機器とペアリングを行うことが可能となる。BIAS は Bluetooth のプロトコル仕様における脆弱性であるため、該当の処理が仕様どおりに実装されている場合、原則的には脆弱性が再現する。 上で例を挙げた脆弱性に共通する特徴として、脆弱性の影響範囲が大きいことが挙げられる。Bluborne は OS のカーネルやプロトコルスタックにおける脆弱性であるため、様々な機器に利用されている。また、BIAS においては、プロトコル	（改定不要）

	仕様における脆弱性のため、さらに影響範囲が大きい。そのため、Bluetooth の脆弱性調査においては特定ベンダの製品にとどまらない広範な影響範囲となりうる場合があるという点に留意が必要である。	
検証方法：インタフェース有無	（現状記述なし）	Bluetooth を有する機器に対しては、当該インタフェースが製品の利用上必要であるかを整理することが重要である。Bluetooth は無線という物理的インタフェースであると同時に、プロファイルやサービスといった論理的インタフェースを有している。 そのため、検証に当たっては、製品仕様書や設計書等を基に、利用する Bluetooth プロファイルやサービス、およびそれぞれの利用目的を明確にし、利用しないプロファイルやサービスが有効化されていないことを確認することが望ましい。特に、廃止されたプロファイルや、運用上不要なインタフェースが有効となっていないかについては注意が必要である。
検証方法：コンポーネントの脆弱性診断	Bluetooth の脆弱性調査においては、まず、検証対象機器に脆弱性が存在しうるか否かを机上調査する。方法としては主に二つある。一つ目の方法は、機器のコンポーネントに関する情報を入手する方法である。OS のカーネルやプロトコルスタック等のバージョンの情報を入手し、それらに存在する脆弱性を調査する。この方法は、第 4.6.1 項に示した Web 調査の手法が利用できる。二つ目の方法は、調査対象の脆弱性を選定し、その脆弱性が存在するコンポーネントを特定した上で、検証対象機器が該当のコンポーネントを利用しているかを確認する方法である。 机上調査を行った結果、脆弱性が存在しうるという結論になった場合は、可能であれば、実機に対して脆弱性の再現可否の確認を行う。脆弱性が再現しうるか否かは公開されている PoC を活用する方法がある。ただし、PoC は第三者が作成、公開しているものがほとんどであり、信頼性の高い PoC であるか否かは確認が必要である。脆弱性の原理を調査した上で、検証サービス事業者	Bluetooth の脆弱性調査においては、まず、検証対象機器に脆弱性が存在しうるか否かを机上調査する。方法としては主に二つある。一つ目の方法は、機器のコンポーネントに関する情報を入手する方法である。OS のカーネルやプロトコルスタック等のバージョンの情報を入手し、それらに存在する脆弱性を調査する。この方法は、第 4.6.1 項に示した Web 調査の手法が利用できる。二つ目の方法は、調査対象の脆弱性を選定し、その脆弱性が存在するコンポーネントを特定した上で、検証対象機器が該当のコンポーネントを利用しているかを確認する方法である。 机上調査を行った結果、脆弱性が存在しうるという結論になった場合は、可能であれば、実機に対して脆弱性の再現可否の確認を行う。脆弱性が再現しうるか否かは公開されている PoC を活用する方法がある。ただし、PoC は第三者が作成、公開しているものがほとんどであり、信頼性の高い PoC であるか否かは確認が必要である。脆弱性の原理を調査した上で、検証サービス事業者にて PoC を作

	にて PoC を作成するということも可能であるが、多くの場合、高コストになる点は留意が必要である。	成するということも可能であるが、多くの場合、高コストになる点は留意が必要である。 Bluetooth を通じて IP 通信が成立する構成(例:PAN、IPSP 等)を採用している場合には、Bluetooth 経由であってもネットワークインタフェースとして扱い、ネットワークスキャンや既知脆弱性スキャンの対象に含めることが望ましい。 ⇒IP 通信のネットワークに飛ばす

表 3-8 USB インタフェースに関する別紙1 6.5 節の追記案(赤字:変更箇所)

項目	現状の記述	改定案
検証の必要性	(現状記述なし)	IoT 機器には、保守、設定、更新、電源供給等の目的で USB インタフェースが実装されているものが存在する。USB は物理的な接触を前提とするインタフェースであるが、機器に対する直接的なアクセス経路となり得る。 そのため、製品の利用上不要な USB 機能が有効となっている場合、攻撃面が不必要に拡大するおそれがある。Bluetooth と同様に、USB に対しても、脆弱性の有無の確認に加え、利用上不要なインタフェースや機能が適切に制御されているかという観点を含めて検証する必要がある。
攻撃事例	(現状記述なし)	検証対象機器が USB や SD カード等の外部記憶媒体に関するインタフェースを有している場合、情報の窃取や不正アクセスが実施される可能性がある。このような入力を通じて、情報漏えいや機器の異常動作等が発生するおそれがある。また、USB 経由で IP 通信が成立する構成では、USB が事実上ネットワークインタフェースとして機能し、ポートスキャンや脆弱性スキャン等の対象となり得る。
検証方法:インタ	(現状記述なし)	USB に関する検証では、まず機器の技術文書や仕様情報を基に、USB の利用目的を整理し、利用上不要な機能が含まれていないことを確認する。その上で、必要に応じて実機での確認を行うことが望ましい。 具体的には、USB ポートが存在する場合でも、運用上データ通信を用いないのであれば、利用上不要な機能が有効となっていないこと(例:不要な

フェース有無		USB デバイスクラスや機能が利用できないこと）を確認する。 外部記憶媒体を扱う機器では、不正なファイルを介した入力に対する応答を確認することが望ましいが、ファジングの範囲については、検証依頼者と事前に相談し、対象インタフェースやパラメータを絞って実施することが望ましい。 USB の有無および利用形態については、機器の外観、仕様書、設計資料等を基に把握し、運用上の用途を明確にすることが重要である。 また、USB を通じて IP 通信が成立するか否かは、検証スコープを定める上で重要な観点となる。 USB がネットワーク経路として機能する構成では、当該経路を通信インタフェースとして扱う必要がある。
検証方法：コンポーネントの脆弱性診断	（現状記述なし）	USB に関する脆弱性診断では、USB 経由で提供される機能や経路（外部媒体、更新、保守機能、USB ネットワーク等）に応じて、既知の脆弱性の有無を確認する。 既知脆弱性の検査には、脆弱性スキャンツールを用いた自動検査が有効であるが、影響の有無にかかわらず多数の脆弱性が出力される場合がある。そのため、検出された脆弱性については、実際に悪用可能であるか、再現性の確認を行うことが望ましい。すべての再現確認が困難な場合には、影響の大きい脆弱性に絞って重点的に確認する。 USB を通じて IP 通信が成立する構成では、USB をネットワークインタフェースとして扱い、当該経路上でポートスキャンおよび既知脆弱性スキャンを実施し、攻撃に悪用される可能性のある脆弱性が検出されないことを確認することが望ましい。

まず優先度の高いものとして、Bluetooth 及び USB についてインタフェース検査ツールの調査を行い、別紙の改定案を整理した。またツールの使い方など、検証の実施にあたって実際に参考になる記述も整理が必要である。

また、Bluetooth や USB 以外のものとして、SBOM の他、汎用的なチェックツールなどについても確認し、必要な記述を整理、追加していく必要がある。これらについては、JC-STAR 事務局とも内容、

記述方法、記述粒度などの確認を行い、最終的な改定案にまとめていくことが必要となる。

4. IoTセキュリティ評価関連制度に関する海外動向調査

本節では、JCSTAR の相互認証を目的として、海外の IoT セキュリティ評価関連制度に関する調査を行った。

4.1 欧州

2024 年 12 月、EU はデジタル要素を有する製品のサイバーセキュリティを確保することを目的に「EU Cyber Resilience Act[8]（以下 CRA）」を発効した。CRA は、インターネットに接続される IoT デバイスや非組み込みソフトウェアなど、ハードウェアおよびソフトウェアの両方を含むデジタル要素を含む製品のライフサイクル全体にわたるセキュリティを確保し、消費者と企業をサイバー攻撃から保護することを目的とした規則である。

4.1.1 制度の対象となる製品

対象製品は「デジタル要素を持つ製品」という広い製品概念を採用している。「デジタル要素を持つ製品」を「ソフトウェア又はハードウェア製品およびその遠隔データ処理ソリューション」とし、ソフトウェア及びハードウェアの構成要素が単体で市場に出る場合も含んでいる。遠隔データ処理ソリューションの定義に関しては、当該処理が欠けると製品が機能の一つを果たせない、メーカーが設計・開発している、または責任を負うような機能を定義している。このため、JC-STAR の IoT 製品（IoT 機器＋付随サービス）と同様に、CRA も機器単体に閉じず、製品機能に不可欠な遠隔処理（典型的にはクラウド側）を、定義上取り込む構造を持つ。 また当該規則は、市場に提供されるデジタル要素製品で、意図された目的又は合理的に予見可能な使用において、機器またはネットワークへの直接または間接の論理的又は物理的なデータ接続を含むものに適用される。この接続要件は IP 通信に限定されないため、JC-STAR より通信方式の条件は対象範囲が広くなっている。

CRA に明示的な記載のある対象外製品を表 4-1 に整理した。具体的には医療機器規則（2017/745）、体外診断用医療機器規則（2017/746）、自動車の型式認証等に関する規則（2019/2144）、民間航空分野（2018/1139 に基づき認証された製品）、船用品（Directive 2014/90/EU）、同一仕様の部品交換を目的とするスペアパーツや、国家安全保障・防衛目的のみで開発/変更された製品、機密情報処理向け製品も除外される。

表 4-1 CRA において対象外となる製品カテゴリと関連する法規制及び制度

カテゴリ	関連する EU 法規制・制度
医療機器	Regulation (EU) 2017/745（MDR）
体外診断用医療機器	Regulation (EU) 2017/746（IVDR）
自動車・車載システム・部	Regulation (EU) 2019/2144（型式認証枠組み）

[8] EU, “Regulation 2024/2847”, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847

品・独立技術ユニット	
民間の航空分野製品	Regulation (EU) 2018/1139 に基づく認証枠組み
船用品	Directive 2014/90/EU (Marine Equipment Directive)
同一仕様の交換用スペアパーツ	記載なし
国家安全保障・防衛目的専用の製品	記載なし
機密情報処理専用の製品	Council Decision 2013/488/EU(EU classified information 保護規則)

4.1.2 成熟度における差異

CRA は すべてのデジタル要素を有する製品に対し、設計・開発・生産・市場投入後の脆弱性対応までを通じた必須のサイバーセキュリティ要件を課している。現時点では CRA における成熟度の差は 一部の高リスク製品だけに高度な対策を求める仕組みではなく、すべての製品に共通する基礎要件の上に適合性評価の際に果たすべきコンプライアンスプロセスが異なる。

デジタル要素を含む製品は、サイバーセキュリティリスクのレベルや機能の重要性に基づいて、表 4-2 に示すように一般製品、重要製品、クリティカル製品に区分される。重要製品はさらにクラス I とクラス II に分けられる。重要製品は、以下のいずれかの基準を満たす製品と定義される。第一に、認証、アクセス制御、侵入防止および検知、エンドポイントセキュリティまたはネットワーク保護の確保など、他の製品、ネットワークまたはサービスのサイバーセキュリティにとって重要な機能を主に実行する製品である。第二に、ネットワーク管理、構成制御、仮想化、個人データの処理等のように、直接的な操作を通じて、多数の他の製品、またはそのユーザの健康、セキュリティ、安全性に混乱、制御、損害をもたらす強さおよび能力の点で、悪影響の重大なリスクを伴う機能を実行する製品である。重要製品はサイバーセキュリティリスクのレベルを反映してクラス I とクラス II に分けられ、クラス II はクラス I よりも大きな悪影響をもたらす可能性がある製品が該当する。クリティカル製品は、重要製品の基準を満たす製品のうち、さらに以下のいずれかの基準を満たす製品区分として定義される。第一に、関連する EU 指令に規定される必須事業体がその製品区分に決定的に依存している場合である。第二に、その製品区分に関するインシデントおよび悪用された脆弱性が、域内市場全体の重要なサプライチェーンに深刻な混乱をもたらす可能性がある場合である。一般製品は、重要製品およびクリティカル製品として指定されていない製品である。

表 4-2 CRA の規定する製品区分とその定義

製品区分	定義	具体的な製品例
一般製品	重要製品およびクリティカル製品として指定されていない製品。	

重要製品（クラス I）	以下のいずれかの基準を満たす製品 ● 認証、アクセス制御、侵入防止および検知、エンドポイントセキュリティまたはネットワーク保護の確保など、他の製品、ネットワークまたはサービスのサイバーセキュリティにとって重要な機能を主に実行する製品 ● ネットワーク管理、構成制御、仮想化、個人データの処理などの中央システム機能のように、直接的な操作を通じて多数の他の製品またはユーザの健康、セキュリティ、安全性に悪影響の重大なリスクを伴う機能を実行する製品	ID 管理システム、ブラウザ、パスワードマネージャー、ウイルス対策ソフト、VPN 製品、SIEM システム、OS、ルーター・モデム・スイッチ、セキュリティ機能を持つマイクロプロセッサ等の半導体、スマートホーム製品（カメラ、ドアロック等）、インターネット接続玩具、ウェアラブル端末など。
重要製品（クラス II）	重要製品の基準を満たし、サイバーセキュリティ機能の性質や悪影響の重大なリスクにより、クラス I の製品よりも大きな悪影響をもたらす可能性がある製品	仮想化実行をサポートするハイパーバイザおよびコンテナランタイムシステム、ファイアウォール、侵入検知・防止システム、耐タンパ性マイクロプロセッサ、耐タンパ性マイクロコントローラ。
クリティカル製品	多数の他の製品に混乱や損害をもたらす悪影響の重大なリスクを伴う機能を実行し、かつ以下のいずれかの基準を満たす製品 ● 必須事業体が当該製品カテゴリに決定的に依存している。 ● インシデントや悪用された脆弱性が、域内市場全体の重要なサプライチェーンに深刻な混乱をもたらす可能性がある。	セキュリティボックスを備えたハードウェアデバイス、スマートメーターゲートウェイ、セキュア暗号処理デバイス、スマートカード、セキュアエレメントを含む類似デバイス。

表 4-3 に示すとおり CRA における成熟度の差は製品区分に応じた適合性評価のプロセスの差として現れる。欧州委員会は一般製品については製造者による自己評価を認めている。他方、重要製品については他の製品よりも厳格な適合性評価が求められ、整合規格の適用状況等によっては第三者機関の関与が必要となる。さらに重大製品については第三者機関の関与が常に必要とされており、将来的には欧州のサイバーセキュリティ認証制度の対象となり得る。

表 4-3 CRA の製品区分と評価手法

<table>
<tr><th colspan="3"></th><th>評価方法概要</th><th>概要</th></tr>
<tr><td rowspan="4">適合性評価プロセス</td><td>Critical 製品</td><td colspan="2">欧州サイバーセキュリティ認証制度取得の義務化（未整備の場合、重要製品 ClassⅡと同様の条件）</td><td>欧州サイバーセキュリティ法（Cybersecurity Act）により制定された認証制度となるが、現在、クリティカル製品に適用される具体的な認証スキームを定める委任法はまだ採択されていない。</td></tr>
<tr><td rowspan="3">重要製品</td><td>Class Ⅱ</td><td>第三者評価機関による技術文書レビュー及び実機テスト</td><td rowspan="3">製品の使用目的や予想される寿命に基づき、潜在的なサイバーセキュリティリスクアセスメントを実施する。リスク評価結果に基づいて、附属書Ⅰ掲載の要件を必要に応じて適用する。
製品特性に関する要件
● 既知の悪用可能な脆弱性がない状態で市場投入
● 安全なデフォルト構成での提供
● セキュリティアップデートによる脆弱性対処
● 認証・アクセス管理等による不正アクセス防止と検知
● データの機密性確保
● データ・設定・プログラムの完全性保護及び改変検知
● 目的に必要な範囲に限定したデータ処理
● DoS 攻撃への耐性と基本機能の可用性確保
● 他デバイス・ネットワークへの悪影響の最小化
● 攻撃面を最小化した
脆弱性対処プロセスに関する要件
● 製品に含まれる脆弱性およびコンポーネントの特定・文書化
● 脆弱性に対する迅速な対応・修正およびセキュリティアップデートの提供
● 製品セキュリティに関する定期的かつ効果的なテスト・レビューの実施
● 修正済み脆弱性に関する情報の共有・公開
● 協調脆弱性開示方針の策定および運用
● 潜在的脆弱性情報の共有促進</td></tr>
<tr><td>Class Ⅰ</td><td>整合規格等により実施が完全な場合は自己宣言。整合規格等により実施が不完全な場合は第三者評価機関による技術文書レビュー及び実機テスト</td></tr>
<tr><td>一般製品</td><td colspan="2">自己宣言</td></tr>
</table>

			設計・開発・製造 ● インシデント影響を抑える悪用軽減設計 ● 内部活動の記録・監視とセキュリティ情報の提供 ● データ・設定の安全かつ恒久的な削除の保証	
	対象外製品		CRA の対象となった製品に関しては EU 適合宣言を発行し、CE マークを取得する必要がある。 以下の場合は CRA の適用対象外となる。 ● 国家安全保障及び防衛目的で開発された製品 ● 機密情報を処理する目的で開発された製品 ● 物理製品に依存しないSaaS 及びPaaS ● 非営利目的の OSS や開発モデル ● 他の既存 EU 法により規制済み分野の製品（医療機器、自動車、民間航空、海洋機器）	

4.1.3 試験及び認定の体制

製造者がデジタル要素を含む製品を欧州連合市場に導入するためには、サイバーセキュリティの必須要件を満たし、適合性評価手順を経て CE マーキングを取得する必要がある。CE マーキングとは、製品が欧州連合の基準や法令に適合していることを示す認証マークである。CRA の適合性評価および認定の体制には、図 4-1 に示すような体制が構築されている。また、製造者がCRAを取得する際の手順に関して説明する。

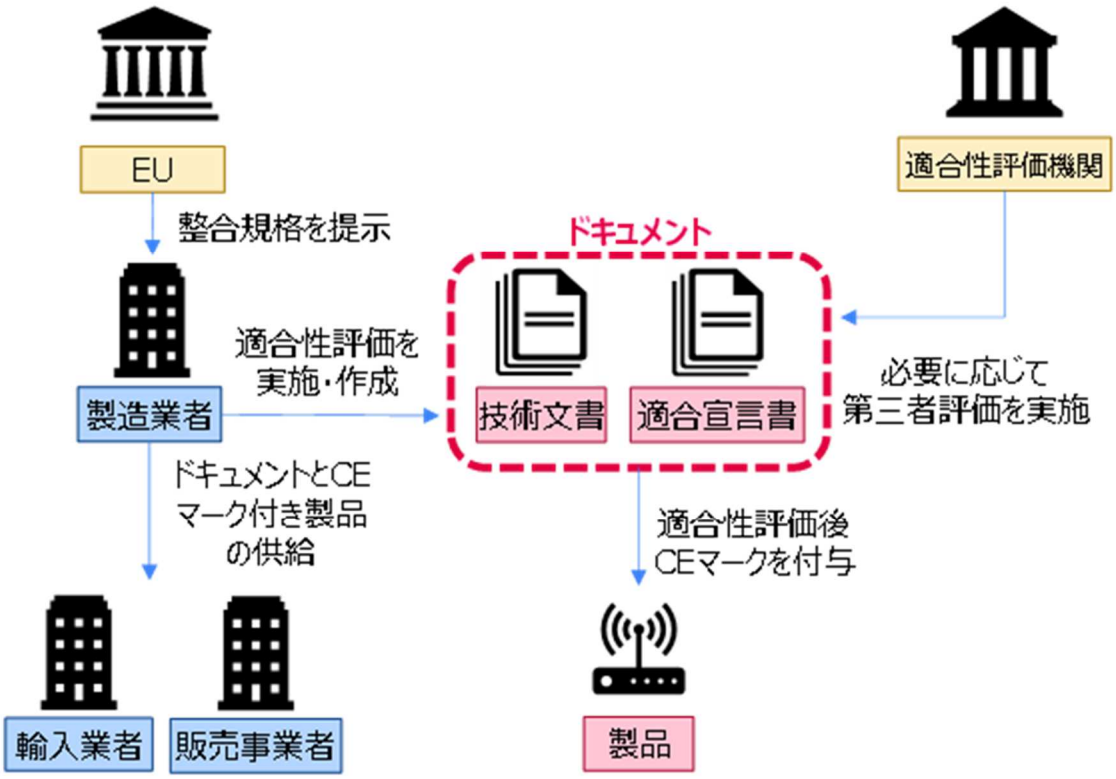


図 4-1 CRA における体制

① 製造者は、製品のライフサイクル全体である計画、設計、開発、生産、納品、保守の各段階を通じて、デジタル要素を含む製品に関連するサイバーセキュリティリスクの評価を実施しなければならない。この評価は、製品の意図された目的や合理的に予見可能な使用環境に基づいてサイバーセキュリティリスクを分析するものであり、文書化される。

② 製造者は、製品のサイバーセキュリティリスクの区分に応じて適合性評価手順を選択する。一般製品の場合、製造者が自らの責任で要件を満たしているかを判断する自己評価手順であるモジュール A を使用できる。重要製品クラス I の場合、指定された整合規格や共通仕様などを適用すれば自己評価手順を使用できるが、適用しない場合は第三者機関による評価が必要となる。重要製品クラス II の場合、整合規格などを一部満たしていても常に第三者機関による適合性評価が義務付けられる。クリティカル製品の場合、欧州サイバーセキュリティ認証を取得するか、重要製品クラス II と同様の第三者評価を受ける必要がある。

③ 第三者機関による評価が求められる場合、製造者は自ら選択した適合性評価機関に対して申請を行い、のいずれかの手順を実施する。モジュール B およびモジュール C に基づく手順では、まずモジュール B による EU 型審査では、適合性評価機関が製品の技術的設計と開発、及び製造者が構築した脆弱性対応プロセスの審査を行う。要件を満たしていれば適合性評価機関から EU 型審査証明書が発行される。その後、内部生産管理であるモジュール C において、製造者は生産された製品が審査で承認された型に適合していることを保証する措置を講じる。モジュール H に基づく手順では、完全な品質保証に基づく適合性評価が行われる。製造者は、製品の設計、開発、生産、および脆弱性対応のすべての段階を詳細に規定した品質システムを確立して維持する。適合性評価機関は、製造者の施設への評価訪問を含む監査を実施し、この品質システムが要件を満たしてい

るかを評価する。

④ 製造者は、製品が必須のサイバーセキュリティ要件に準拠していることを示すためのデータや詳細を含む技術文書を作成する。技術文書には製品の設計、開発、生産、脆弱性処理、およびリスク評価の詳細が含まれ、製品が市場に出た後 10 年間またはサポート期間のいずれか長い方の期間保管されなければならない。要件への適合が証明された後、製造者は EU 適合宣言書を作成する。これは、製品が関連する欧州連合の調和法令に適合していることを宣言する文書であり、製造者の単独の責任の下で発行される。

⑤ 最後に、製造者は製品、その包装、または製品に添付される文書に CE マーキングを可視的、読みやすく、消えないように貼付する。ソフトウェア製品の場合は、EU 適合宣言書またはウェブサイトに貼付することができる。モジュール H に基づく完全な品質保証の手順を用いた場合は、CE マーキングの後に評価に関与した適合性評価機関の識別番号を付記しなければならない。

4.1.4 制度のタイムライン

サイバーレジリエンス法に関する制度のタイムラインを図 4-2 に整理した。以下にそれぞれの要素について時系列で説明する。2022 年 9 月 15 日、欧州委員会はサイバーレジリエンス法の規則案を公開した。2024 年には、本規則の必須サイバーセキュリティ要件の導入を支援するため、欧州連合サイバーセキュリティ機関（ENISA）等により、CRA の要件と IEC 62443 などの既存の国際規格とのマッピングに関する共同調査報告書が公開された。サイバーレジリエンス法は 2024 年 12 月 10 日に正式に発効した。発効後、制度の完全適用に向けて複数の段階的なステップが設けられている。2025 年 12 月 11 日までに、欧州委員会はクラス I およびクラス II の重要製品、ならびにクリティカル製品のカテゴリの技術的記述を規定する実施法を採択する。2026 年 6 月 11 日からは、各加盟国が適合性評価機関を審査、指定、および通知（登録）するための規定の適用が開始される。同時に、欧州標準化委員会（CEN）、欧州電気標準化委員会（CENELEC）、および欧州電気通信標準化機構（ETSI）などの欧州標準化団体は、必須サイバーセキュリティ要件を詳細な技術仕様として表現する整合規格の策定を進めており、それらの採用期限は 2026 年 8 月から 10 月にかけて設定されている。2026 年 9 月 11 日には、活発に悪用されている脆弱性および製品のセキュリティに影響を及ぼす重大なインシデントに関する報告義務が先行して適用開始される。製造業者の報告義務を簡素化するため、ENISA によって単一の報告プラットフォームが設立され、通知はこの電子プラットフォームを通じて提出されることとなっており、それに向けた整備が行われる。2027 年 12 月 11 日には、製品に対する必須サイバーセキュリティ要件への準拠、適合性評価手続の実施、および CE マーキングの貼付義務を含む、本規則の大部分の規定の適用が開始される。最後に、経過規定として、本規則以外の欧州連合調和法令の対象となる製品のサイバーセキュリティ要件に関して過去に発行された EU 型審査証明書および承認決定は、有効期限がそれ以前に切れない限り、2028 年 6 月 11 日まで有効に存続し、同日をもって猶予が終了する。

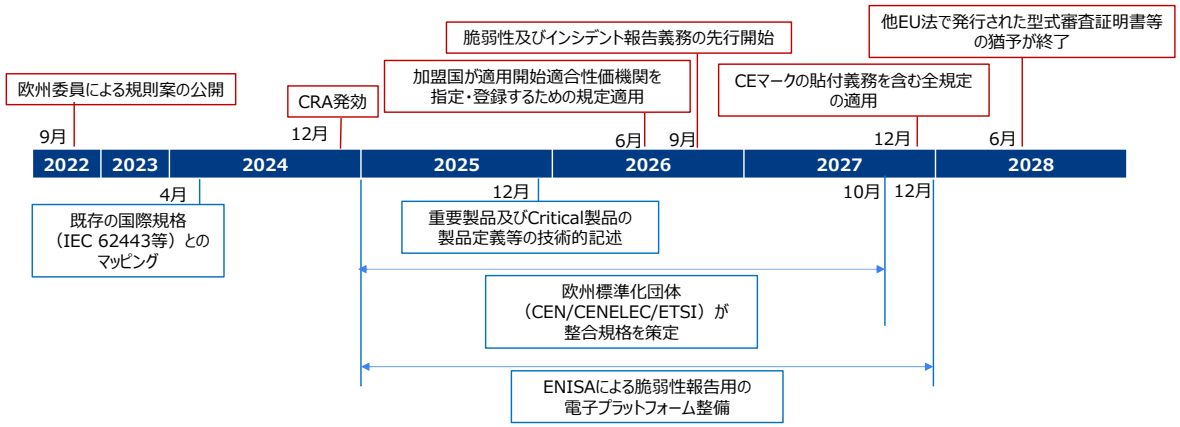


図 4-2 CRA のスケジュール

4.1.5 日本の事業者が必要となる対応

日本の事業者がサイバーレジリエンス法（CRA）に対応するためのステップは以下の通りである。

（1） セキュリティ対策の実装

製造業者は、デジタル要素を含む製品に関連するサイバーセキュリティリスクの評価を実施し、そのリスク評価結果に基づいて、以下の要件を必要に応じて適用する。具体的には、製品特性に関する要件（附属書 I 第 I 部）および脆弱性対処プロセスに関する要件（附属書 I 第 II 部）の適用である。その後、技術文書の整備を実施し、製品そのものの特性や区分から製品に対応した適合性評価手続を選択して実施し、要件への適合が証明された後、EU 適合宣言書を発行し、製品に CE マークを付ける。

（2） EU 域内での責任体制の整備

EU 域外の製造業者が製品を輸出する際、EU 市場における責任の所在を明確にするため、EU 域内に設立された輸入業者を通じた対応等が必要となる。輸入業者は、製品を市場に出す前に、製造業者が正しく適合性評価手順を実施し、技術文書を作成したことを確認する義務を負う。また、デジタル要素を含む製品、その包装、または添付文書に、輸入業者の名称や連絡先を表示しなければならない。さらに、EU 域外の製造業者は、書面による委任によって、EU 域内の公認代理人を任意で選任することができる。公認代理人は、当局の要請があった際に、EU 域外の製造業者が作成した技術文書や EU 適合宣言書を提示する役割を担う。

（3） 報告及び対応体制の整備

製造業者は、製品に影響を及ぼす重大なインシデントや活発に悪用されている脆弱性を認識した場合、ENISA が構築するプラットフォームを通じた通知と報告先として指定された CSIRT に対して通知を行わなければならない。この報告先の決定ルールは、EU 域内における拠点の有無で異なる。域内に主たる拠点がある場合、主たる拠点が置かれている加盟国の CSIRT に報告する。域内に拠点がない場合：製造業者が入手可能な情報に基づき、以下の優先順位に従って、関係の深い加盟国の CSIRT

を選択して報告する。

① 当該製造事業者を代理する認定代理人が設立されている加盟国
② 当該製造業者のデジタル要素を搭載した製品を最も多く市場に出している輸入業者が設立されている加盟国
③ 当該製造業者のデジタル要素を搭載した製品を「最も多く市販している」販売業者が設立されている加盟国
④ 当該製造業者の製品のユーザ数が最も多い加盟国

4.2 米国

2024 年 3 月、米国連邦通信委員会（FCC）は消費者向けの無線 IoT 製品のサイバーセキュリティを確保することを目的に、自発的なサイバーセキュリティラベリングプログラム「U.S. Cyber Trust Mark」の規則を採択し、2025 年 1 月に同プログラムが開始された。本プログラムは、インターネットに接続されるホームセキュリティカメラ、音声起動型アシスタント、スマート家電などの消費者向けの無線 IoT 製品を対象とし、製品が NIST のガイドラインに基づくセキュリティ基準を満たしていることを認証する制度である。消費者が情報に基づいた購買決定を行えるようにすることでサイバー攻撃の脅威から消費者を保護するとともに、製造者に対して Secure By Design の原則に基づく製品開発とより高いサイバーセキュリティ基準の達成を促し、国家全体のサイバーセキュリティ体制を強化することを目的とした取り組みである。

4.2.1 制度の対象となる製品

対象製品の定義は主に次の 3 つのスコープが狭まる。第一に消費者向け IoT 製品であり、産業用向けではないと定義される。具体例として、FDA による規制のある医療機器と、NHTSA による規制のある自動車及び自動車装備品を明示的に除外している。第二に IoT 機器はインターネットに接続される機器であることに加え、意図的に電波を放射する能力と、物理世界と直接相互作用するための少なくとも 1 つのセンサ及びアクチュエータを要求し、さらに Wi-Fi や Bluetooth 等のネットワークインタフェースも要求している。第三に、制度の対象となる製品が無線 IoT 製品に向けられ、現時点では有線 IoT 製品を除外すると明示している。

また、Secure and Trusted Communications Networks Act に基づく Covered List[9]掲載の通信機器等も制度から除外している。また、2025 年 10 月、FCC の公開委員会会議[10]にて「機器認可プログラムによる国家安全保障上の脅威からの保護」という議題が扱われ、Covered List 掲載企業の機器のみならず、カバーリスト掲載企業が製造の過程に関係し、モジュラー型送信機を含む機器の認証取得を禁止した。Covered List 掲載企業の関与がある製品の定義として、FCC はデバイスの存在に至るプロセスの主要な段階における実質的な責任及び管理（例：設計、製造、組み立て、開発）を持つ

[9] 米国連邦通信委員会が作成するリスト。米国の安全保障または米国人のセキュリティと安全に許容できないリスクをもたらすとみなされる通信機器およびサービスが掲載される。カバーリストに掲載された事業者は米国内でのサービス提供が制限される。
[10] FCC, “October 2025 Open Commission Meeting”, https://www.fcc.gov/October2025

場合が含まれるとし、リブランドやホワイトラベリングが行われても、 Covered List 掲載企業により製造された機器というステータスは変わらないという見解を示した。

4.2.2 成熟度における差異

米国サイバートラストマーク(USCTM)プログラムにおける成熟度による認定レベルの差異に関しては、制度上、多段階の成熟度やセキュリティレベルに応じた階層化は採用されていない。連邦通信委員会(FCC)は、シンガポールなどで採用されている多層的なラベリング手法についても検討を行ったが、消費者が最も理解しやすい形式として、製品が最低限のサイバーセキュリティ要件を満たしているか否かを示す単一のバイナリラベル(合格・不合格の二値)を採用している。USCTM の評価フレームワークにおけるすべてのセキュリティ制御要件はバイナリで判定され、リスク評価を理由とした要件の部分的な適用や免除は一切正当化されない。

評価方法及び評価基準について表 4-4 に整理した。評価方法として、FCC は IoT ラベルの使用権限を取得するための 2 段階のプロセスを採用している。第一の段階は、認定および承認された試験所である CyberLAB、社内試験所、またはサイバーセキュリティラベル管理者(CLA)が運営する試験所による、製品の適合性試験の実施とテストレポートの作成である。第二の段階として、製造者は独立した第三者機関である CLA に対して申請書とテストレポートを提出する。CLA は提出された申請書とサポート文書を審査し、製品が FCC のプログラム要件に準拠しているかを確認した上で、ラベル使用の承認または拒否を決定する。評価基準の概要については、米国国立標準技術研究所(NIST)が策定した消費者向け IoT 製品のコアベースラインプロファイルである NISTIR 8425 を基盤としている。評価基準は、IoT 製品自体に実装される技術的な機能要件と、開発者が実施すべき非技術的な活動要件がある。

表 4-4 USCTM の評価手法

	評価方法概要	基準概要
適合性評価プロセス	● CyberLAB、社内試験所、またはサイバーセキュリティラベル管理者(CLA)が運営する試験所による、製品の適合性試験の実施とテストレポートの作成 ● 製造者は独立した第三者機関である CLA に対して申請書とテス	【IoT 製品の機能要件】 ● **資産の識別:** 製品を一意に識別でき、構成コンポーネントのインベントリを維持していること ● **製品構成:** 設定変更が可能であり、かつ安全なデフォルト状態へ復元できること ● **データ保護:** 保存・転送データを保護(暗号化等)し、データ削除機能を有すること ● **インタフェースのアクセス制御:** インタフェースへのアクセスを許可された者のみに制限すること ● **ソフトウェアアップデート:** 安全な更新手段を持ち、自動更新または通知により最新状態を維持できること

	トレポートの提出及び CLA によるレビュー	● **サイバーセキュリティ状態の認識:** インシデント検知に資する状態情報(ログ等)を記録すること **【開発者の活動要件】** ● **文書化:** 開発ライフサイクルを通じてセキュリティ関連情報を文書化・保管すること ● **情報・問い合わせの受信:** 脆弱性報告や問い合わせを受け付け、応答できること ● **情報の普及:** サポート終了や脆弱性情報などをユーザや関係者に通知すること ● **製品の教育と啓発:** ユーザに対し、安全な使用方法やリスクに関する教育・情報提供を行うこと

4.2.3 試験及び認定の体制

製造者が消費者向けの無線 IoT 製品に FCC IoT ラベルを付与するためには、サイバーセキュリティの基準を満たし、適合性評価手順を経て認証を取得する必要がある。FCC IoT ラベルとは、製品がプログラムの要件と FCC の最低限のサイバーセキュリティ要件に適合していることを示す U.S. Cyber Trust Mark および QR コードで構成されるラベルである。U.S. Cyber Trust Mark プログラムの試験および認定の体制には、図 4-3 に示すような体制が構築されている。また、製造者が FCC IoT ラベルの使用権限を取得する際の手順に関して説明する。

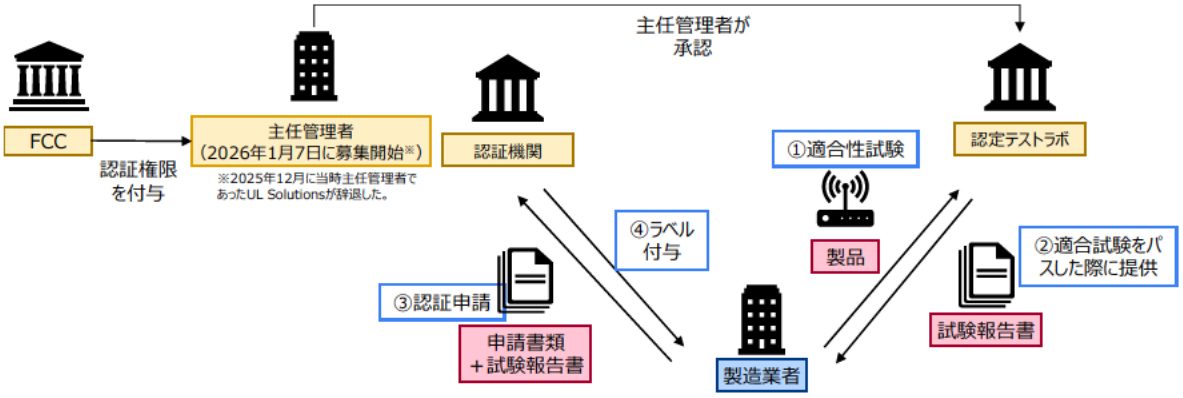


図 4-3 USCTM の体制

① 製造者は、主任管理者から承認された認定テストラボにおいて、対象の IoT 製品のサイバーセキュリティ適合性試験を実施しなければならない。この試験は、FCC が承認したサイバーセキュリティ基準を用いて製品を評価およびテストするものであり、結果は試験報告書として文書化される。

② 製造者は、製品の評価を行う認定テストラボを選択する。認定テストラボには、独立した第三者機関である CyberLAB のほか、認証機関が運営する試験施設が含まれる。また、ISO/IEC 17025 の認定を受け、かつ主任管理者からの承認を受けるという同等の要件を満たせば、製造者の社内試験施設を使用して適合性試験を実施することも可能である。

③ 適合性試験をパスした場合、認定テストラボは製品がプログラムの基準を満たしていることを実証する試験報告書を作成し、提供する。その後、製造者は、試験報告書とともに認証機関へ提出する申請書類を準備する。申請書類には、提出するすべての情報が真実かつ正確であること、製品や製造者が国家安全保障上の脅威とされるリストに該当しないこと、製品の最低サポート期間の終了日まで重大な脆弱性を特定し修正するためのソフトウェアアップデートを提供することなどを宣誓する、偽証罪の罰則を伴う宣誓書を含める必要がある。

④ 製造者は、準備した申請書類および試験報告書を認証機関に提出し、認証申請を行う。認証機関は、製造者から提出された申請書類と試験報告書を受領し、製品がサイバーセキュリティラベリングプログラムの要件をすべて満たしているかを確認するための審査を実施する。申請書類に不備がある場合、要件が満たされるまで申請は承認されない。

⑤ 最後に、認証機関による審査の結果、プログラムのすべての要件を満たしていると判断された場合、認証機関は申請を承認し、サイバーセキュリティ認証を発行する。これにより、製造者に対して対象製品に FCC IoT ラベルを付与する権限が与えられる。ラベル付与が承認された製品は、U.S. Cyber Trust Mark と製品のセキュリティに関する詳細情報を提供するレジストリにリンクする QR コードを含むラベルを製品パッケージ等に表示することが可能となる。

4.2.4 制度のタイムライン

米国サイバートラストマーク（USCTM）プログラムに関する制度のタイムラインを図 4-4 に整理した。以下にそれぞれの要素について時系列で説明する。これに先立つ 2022 年 9 月には、本プログラムのサイバーセキュリティ要件の導入を支援するため、米国国立標準技術研究所（NIST）により、消費者向け IoT 製品のコアベースラインプロファイルである NISTIR 8425 が公開された。2023 年 8 月 10 日、連邦通信委員会（FCC）はスマートデバイス向けのサイバーセキュリティラベリングプログラムの規則案を公開した。サイバーセキュリティラベリングプログラムの規則は 2024 年 9 月 9 日に正式に発効した。発効後、制度の完全運用に向けて複数の段階的なステップが設けられている。2024 年 9 月 11 日からは、連邦通信委員会がサイバーセキュリティラベル管理者（CLA）および主任管理者の指定を求める企業からの申請を受け付けるプロセスの適用が開始された。2024 年 12 月 11 日までに、連邦通信委員会はプログラムの運営を担う主任管理者および CLA を条件付きで承認した。2025 年 1 月 7 日には、消費者が情報に基づいた意思決定を行えるよう支援することを目的とした、米国サイバートラストマークの立ち上げが発表された。続いて、2025 年 6 月 13 日には、主任管理者およびステークホルダー委員会から、サイバーセキュリティ要件を詳細な技術仕様およびテスト手順として表現する推奨事項が提出された。消費者の製品情報の確認を簡素化するため、連邦通信委員会によって QR コードにリンクするレジストリが設立され、製品の詳細は共通の API を通じて提供される。2025 年中には、製品に対するサイバーセキュリティ要件への準拠、適合性試験の実施、および FCC IoT ラベルの付与を含む本プログラムの大部分の手続きの運用が開始され、ラベル付き製品の市場流通が開始される目標が設定されている。

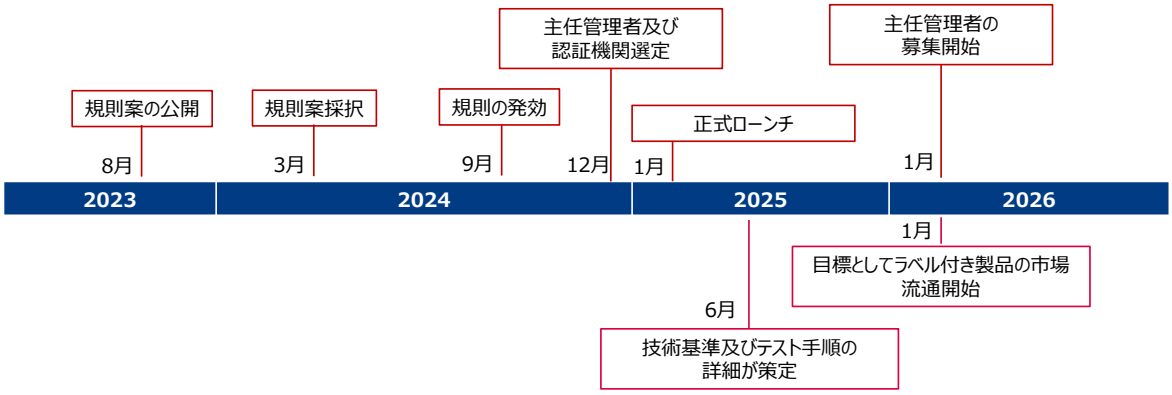


図 4-4 USCTM のタイムライン

4.2.5 日本の事業者が必要となる対応

日本の事業者が米国サイバートラストマークに対応するためのステップは以下の通りである。

（1） セキュリティ対策の実装

セキュリティ対策の実装のステップにおいて、事業者は製品に対するリスク評価を実施し、脅威や攻撃ベクトル、潜在的な影響の評価およびリスク緩和策を文書化することが求められる。ただし、米国の制度では、リスク評価を理由としてセキュリティ制御の要件を部分的に適用したり免除したりすることは正当化されない。評価フレームワークにおけるすべてのセキュリティ制御要件はパスまたはフェイルの二値で判定されるため、リスク評価結果にかかわらず対象となる要件を例外なく実装する必要がある。実装が求められる要件は大きく 2 つに分類される。IoT 製品の機能要件として、資産の識別、製品構成、データ保護、インタフェースのアクセス制御、ソフトウェアアップデート、およびサイバーセキュリティ状態の認識が含まれる。また、開発者の活動要件として、文書化、情報および問い合わせの受信、情報の普及、ならびに製品の教育と啓発を実施する必要がある。

（2） 米国内での報告体制の整備

米国内での報告体制の整備のステップにおいて、日本企業のように米国に拠点を持たない申請者は、申請者の代わりに法的手続きの送達を受け入れる目的で、米国内に所在する代理人を指定しなければならない。この代理人は、連邦通信委員会などの関連機関からの法的書類を受け取る役割を担う。申請者は、指定された代理人の物理的な米国の住所およびメールアドレスを登録したうえで、書面による証明書を提出する必要がある。さらに、該当する機器の米国内でのすべてのマーケティングおよび輸入を永久に終了した後、または製品に関連する行政手続きや司法手続きの終了後のいずれか遅い方から少なくとも 1 年間は、米国内で法的手続きの送達を受ける代理人を維持する義務を受け入れる必要がある。

4.3 シンガポール

2020 年、シンガポールサイバーセキュリティ庁（CSA）は、消費者向けスマートデバイスのサイバーセキュリティを向上させることを目的に、サイバーセキュリティラベル制度「CLS（IoT）」を導入した。本制度は、Wi-Fi ルータ、スマートホームハブ、IP カメラ、スマートドアロックなどの消費者向け IoT デバイスを対象とし、製品が国際規格（ETSI EN 303 645 等）に基づくセキュリティ基準などを満たしていることを 4 段階のレベルで評価・認証する制度である。セキュリティ対策の透明性を高めて消費者が情報に基づいた購買決定を行えるようにすることで基本レベルのサイバー攻撃から消費者を保護するとともに、製造者に対してセキュリティ・バイ・デザインの原則に基づく製品開発とより強固なサイバーセキュリティ対策の組み込みを促し、シンガポール全体のサイバー空間の安全性およびサイバー衛生水準を向上させることを目的とした取り組みである。

4.3.1 制度の対象となる製品

対象製品は、ネットワークに接続された、あるいはネットワーク接続可能なコンシューマ向けのスマートデバイスを採用している。この製品概念には、デバイス本体だけでなく、製品の意図された機能を提供するために通常必要となる関連サービスとの相互作用も含まれる。関連サービスの定義に関しては、モバイルアプリケーション、クラウドコンピューティングおよびストレージ、サードパーティの API などを指す。このため、本制度は機器単体に閉じず、全体的なコンシューマ IoT 製品の一部を構成するデジタルサービスを定義上取り込む構造を持つ。

また当該制度は、一般的に家庭内や電子ウェアラブルとしてコンシューマによって使用されるデバイスに適用される。具体例として、影響の大きさを考慮して Wi-Fi ルータやスマートホームハブを優先的な対象として開始された後、現在では IP カメラ、スマートドアロック、スマート照明、スマートプリンター、スマートテレビ、スマートスピーカー、ウェアラブルヘルストラッカー、接続された家電製品など、コンシューマ IoT デバイスのすべてのカテゴリに拡張されている。接続要件については、インターネットやホームネットワークなどのネットワークインフラストラクチャへの接続を含み、イーサネットや Wi-Fi などの IP 接続、ゲートウェイやハブを経由した非 IP 接続、GSM や LoRaWAN などを介した直接接続も対象としている。

対象外製品として、コンシューマ IoT デバイスではないデバイスは適用範囲から除外される。図 4-5 に関連制度について整理を行った。具体的には、主に製造業、ヘルスケア、またはその他の産業用途での使用を意図されたデバイスは明示的に対象外と定義されている。ただし、会議室に展開されるスマートテレビや小規模ビジネスの施設を保護するホームセキュリティキットのように、ビジネスの文脈で使用されるコンシューマ IoT デバイスは、引き続きコンシューマ IoT デバイスとして分類され制度の対象に含まれる。

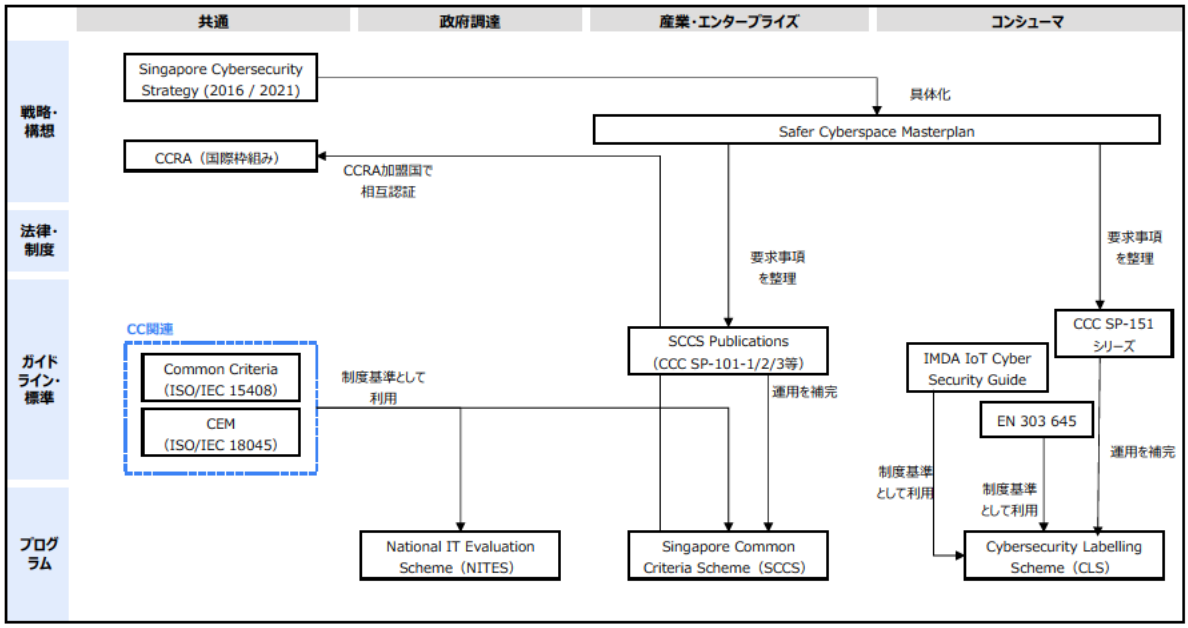


図 4-5 シンガポールにおける IoT セキュリティ関連動向

4.3.2 成熟度における差異

シンガポールのサイバーセキュリティラベル制度（CLS(IoT)）における成熟度による認定レベルの差異に関しては、制度上、4 段階のセキュリティレベルに応じた多層的なラベリング手法が採用されている。消費者が情報に基づいた購買決定を行えるよう製品のセキュリティレベルを可視化するとともに、製造者に対して段階的なセキュリティ向上を促すため、表 4-5 に示すように製品が満たすべきセキュリティ要件と評価の深さに応じてレベル 1 からレベル 4 まで階層化されている。

評価方法及び評価基準について、CLS(IoT)ではレベルに応じた段階的な適合性評価プロセスを採用している。評価方法として、すべてのレベルにおいて製造者は適合宣言書および証拠書類を作成し、承認された試験機関（テストラボ）による審査と評価レポートの作成を受ける。その後、製造者は独立した認証機関であるサイバーセキュリティ認証センター（CCC）へこれらの文書を提出し、CCC が要件への適合を確認した上でラベル発行の承認または拒否を決定する。レベル 1 およびレベル 2 に関する適合性評価は製造者の適合宣言に対するテストラボの書類レビューのみに基づき、テストラボによる独立したテストは要求されない。他方、レベル 3 およびレベル 4 については、テストラボが提供されたファームウェア等を用いて実施するソフトウェアバイナリ解析や、実機に対するブラックボックスペネトレーションテストといった独立したテストの実施が必須となる。

評価基準の概要については、欧州電気通信標準化機構（ETSI）が策定した消費者向け IoT 製品の規格である ETSI EN 303 645 を基盤としている。レベル 1 は普遍的なデフォルトパスワードの禁止等を含むトップ 3 のベースライン要件、レベル 2 は同規格の全必須要件への適合を要求する。さらにレベル 3 およびレベル 4 では、情報通信メディア開発庁（IMDA）のガイドに基づくセキュア・バイ・デザインのライフサイクル要件という非技術的な開発・運用プロセス活動要件が追加される。また、ホームゲートウェイ等の特定の製品群に対しては、ETSI TS 103 848 等の規格に基づく専用の追加要件が適用される構造を持つ。

表 4-5 CLS(IoT)の製品区分と評価手法

		評価方法概要	基準概要
適合性評価プロセス	レベル1	製造業者による適合宣言および試験機関による**書面レビュー**	**製造業者が宣言する事項**：ETSI EN 303 645の3つの要件への適合（汎用デフォルトパスワードの不使用、脆弱性報告の管理手段の実装、ソフトウェアの更新維持）。 **試験機関が検証する事項**：提出された適合宣言書および裏付け証拠の書面レビューによる要件適合性の確認を実施。
	レベル2	製造業者による適合宣言および試験機関による**書面レビュー**	**製造業者が宣言する事項**：ETSI EN 303 645の全必須要件への適合。 **試験機関が検証する事項**：適合宣言書および裏付け証拠の精査を通じた要件適合性の確認を実施。
	レベル3	**試験機関による書面レビュー及びソフトウェアバイナリ解析およびライフサイクルレビュー**	**製造業者が宣言する事項**：レベル2までの全要件への適合、IMDA IoT Cyber Security Guideに基づくセキュリティバイデザインに基づく開発プロセスの実施。 **試験機関が検証する事項**：適合宣言書および証拠文書のレビュー、ソフトウェアのバイナリ解析、パブリックドメインにおける脆弱性調査（OSINT調査）を実施。
	レベル4	**試験機関による実機検証及びペネトレーションテスト**	**製造業者が宣言する事項**：レベル3までの全要件への適合及び実機・ソフトウェアの提供。 **試験機関が検証する事項**：レベル3までの項目とデバイスのセットアップとガイダンス文書の検証、適合性の検証、制度として義務付けられている最小限の実機テスト（ポートやサービス、通信、ファームウェア更新機能への攻撃テストなど）の実施、脆弱性解析及びペネトレーションテスト、暗号化された機密ファイルへのパスワードクラッキングを実施。

※すべてのレベルにおいてホームゲートウェイは別途ETSI TS 103 848への適合が必要となる。

4.3.3 試験及び認定の体制

製造者がネットワーク接続されたスマートデバイスに CLS(IoT)ラベルを付与するためには、一連の評価とテストを受け、レベルに応じた適合性評価手順を経て認証を取得する必要がある。CLS(IoT)ラベルとは、ネットワーク接続されたスマートデバイスのセキュリティレベルの指標を提供するものであり、サイバーセキュリティレベルを示すアスタリスク記号、登録識別子、および製品リストのウェブページへの URL を含む QR コードで構成されるラベルである。CLS(IoT)の適合性評価および認定の体制には、制度の所有者および管理者であるサイバーセキュリティ認証センター(CCC)、製造者、および承認された独立した商業試験機関であるテストラボ(TL)が含まれる。また、図 4-6 に示すような製造者がCLS(IoT)ラベルを取得する際の手順に関して説明する。

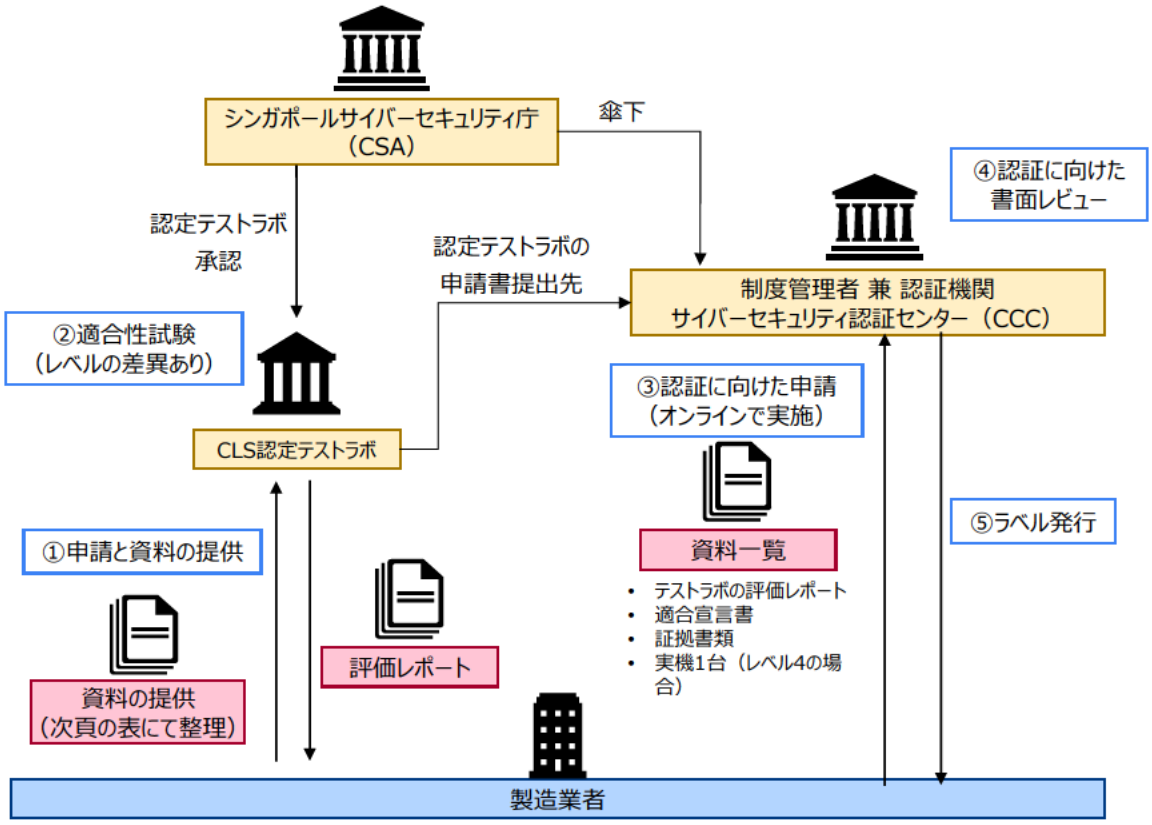


図 4-6 CLS(IoT)の体制

① 製造者は、CCC(Cybersecurity Certification Centre)に承認されたテストラボ(TL)を選択し、契約を結ぶ。製造者は、適用するレベルに応じた適合宣言書(Declaration of Conformity)およびその要件を満たしていることを実証する証拠書類(Supporting Evidence)を作成し、テストラボへ提出する。レベル 3 およびレベル 4 の申請を行う場合は、テストのためのファームウェアおよびコンパニオンモバイルアプリのバイナリファイル、ガイダンス文書、テストラボの要件を満たす十分な数の実機等もテストラボへ提供する。

② テストラボは、提出された適合宣言書および証拠書類をレビューし、それらが要件を満たしているかを評価する。レベル 1 およびレベル 2 の申請においては、テストラボによる独立したテストは要求されない。レベル 3 およびレベル 4 の申請においては、テストラボがソフトウェア(デバイスのファームウェアおよびコンパニオンモバイルアプリ)のバイナリ解析を実施する。さらにレベル 4 の申請においては、テストラボが実機に対するブラックボックスペネトレーションテストを実施する。テストラボは、評価結果、特定された問題、および対応する解決方法を記載した評価レポートやテストレポートを作成する。

③ テストラボが要件を満たしていると判断した場合、製造者は GoBusiness ポータルを通じて CCC へ申請を行う。申請の際、製造者は完成した適合宣言書、証拠書類、およびテストラボが作成した評価レポートを提出する。レベル 4 の申請においては、ペネトレーションテストのレポートもあわせて提出する。

④ CCC は、提出された適合宣言書、証拠書類、およびテストラボの成果物に対する評価レポートをレビューする。CCC は、提出された証拠書類を通じて要件が満たされているという確証を得るための審査を実施する。必要に応じて、CCC はテストラボおよび製造者に対してさらなる明確化やプレ

ゼンテーションを要求する。

⑤ CCC による審査の結果、製品が要件を満たしていると判断された場合、CCC は適合宣言およびテストレポートを承認し、CLS(IoT)ラベルを発行する。ラベルが付与された製品は、CSA の CLS(IoT)ウェブサイト上のラベル付き製品リスト(Labelled Product List: LPL)に掲載される。

4.3.4 制度のタイムライン

サイバーセキュリティラベル制度(CLS(IoT))に関する制度のタイムラインを図 4-7 に整理した。

2020 年 10 月、サイバーセキュリティ庁(CSA)によりネットワーク接続されたスマートデバイス向けのサイバーセキュリティラベル制度がリリースされ、制度開始(v1.0)となった。2021 年 4 月には、アシュアランス継続要件の追加及び改訂(v1.1)が行われた。その後、シンガポールで販売されるすべての住宅用ルータを対象に住宅用ルータのレベル 1 取得義務化が実施された。2022 年にはドイツ連邦情報セキュリティ庁(BSI)と相互承認協定(MRA)を結び、コンシューマ IoT 機器においてドイツと相互認証を締結した。同年 10 月には、フレームワークの見直しによる制度改訂(v1.2)が行われた。2023 年 9 月には、プロセスの改訂と評価手法の発行(v1.3)が実施された。2024 年 10 月には、専用の要件を規定したホームゲートウェイ向け評価手法の発行が行われた。また、韓国インターネット振興院(KISA)とも相互承認協定を結び、コンシューマ IoT 機器において韓国と相互認証を締結した。2025 年 4 月、ラベル表示義務化の告知とプロセスの改訂(v1.4)が実施され、同年 10 月 1 日より物理的およびオンラインの店舗での明確なラベル表示の義務化開始となった。また、相互承認協定の適用範囲として、スマートコンシューマ製品だけでなくホームゲートウェイ等のネットワーク機器においてドイツと相互認証を締結している。2026 年 3 月 2 日、サイバー攻撃の高度化に対応するため、2027 年末までに住宅用ルータレベル 2 取得義務化を発表した。続いて、デジタル開発・情報省の予算委員会において、市民をより保護するため、住宅用ルータと同様に IP カメラに対してレベル 2 取得義務化を検討することが示された。

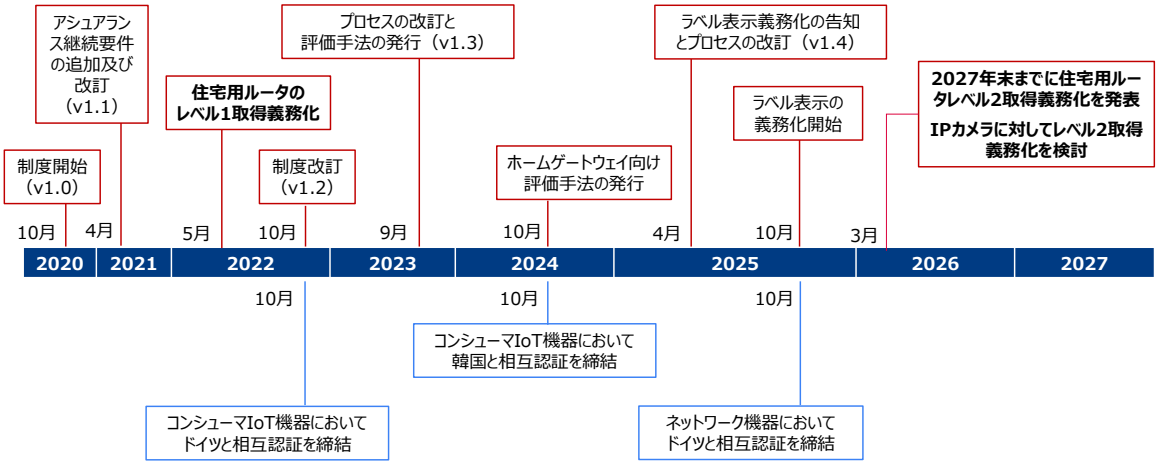


図 4-7 CLS(IoT)のタイムライン

4.3.5 日本の事業者が必要となる対応

日本の事業者がシンガポールのサイバーセキュリティラベル制度（CLS(IoT)）に対応するためのステップは以下の通りである。

（1） セキュリティ対策の実装

セキュリティ対策の実装のステップにおいて、事業者は取得するレベルに応じてセキュリティ要件を実装し、申請に必要な資料を用意することが求められる。シンガポール国内に製品を展開する場合、製品カテゴリの確認が必要となる。住宅用ルータの場合、すでにレベル 1 の取得が義務化されており、2027 年末までにレベル 2 の取得義務化が発表されている。IP カメラの場合、レベル 2 の取得義務化が検討されている。IoT 製品の機能要件として、レベルに応じて ETSI EN 303 645 の必須要件を実装する。レベル 3 以降では IMDA IoT Cyber Security Guide に基づく開発ライフサイクルへの準拠が必須となる。すべてのレベルにおいて、ホームゲートウェイは別途 ETSI TS 103 848 への適合が必要となる。申請資料として、適合宣言書と証拠書類を用意し、レベル 3 およびレベル 4 の場合はレベルに応じたテスト対象物を用意する。

（2） 申請に伴う手続き

申請に伴う手続きのステップにおいて、相互承認協定を結んでいない日本の事業者が申請を行うにあたり、特別に必須となる要件および手続きはない。一方で、テストラボとの契約は民間同士のビジネスとして条件をすり合わせる必要がある。また、認証機関（CCC）への申請作業において、製造業者自身が直接申請する以外にも、関係者がメーカーに代わって申請手続きを行うことが認められている。代わりに申請手続きを行うことができるのは、以下のいずれかである。 ① 代理店 ② 認定テストラボ ③ シンガポール国内に供給する予定の輸入業者（レベル 1 の Wi-Fi ルータの場合） 認証機関への申請はオンラインポータル「GoBusiness」を通じて行うことが可能で、海外の事業者も登録が可能となっている。

5. 全体総括

本事業では、IoT 製品の活用が進む領域の1つとして、工場システム構成製品におけるJC－STAR活用検討を実施し、また JC-STAR 制度の開始を踏まえた「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」の改定に向けた検討、海外の認証制度との調和を進めるためのIoTセキュリティ評価関連制度に関する海外動向調査の合わせて3つの調査を実施した。

工場システム構成製品におけるJC－STAR活用検討では、工場システム構成製品におけるJC－STAR★2のセキュリティ要件について草案をとりまとめた。今後さらに検討を進め、適合要件を含めて最終案として取りまとめ、実際の制度開始に向けて準備を進めることが必要である。

「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」の改定については、特に現状で問合せの多い項目として、Bluetooth や USB 等のインタフェースのチェックツールについて優先的に調査を行い、改定に向けた素案を整理した。さらにこれら以外のインタフェースや脆弱性のチェックツールなどについても調査を進め、JC-STAR 事務局との調整を進め、具体的な改定を進めていくことが必要となる。

IoTセキュリティ評価関連制度に関する海外動向調査では、主に EU、米国、シンガポールの制度について調査を実施した。英国とは既に PSTI 法との相互承認を開始しており、制度が求めるセキュリティ要件の相互の差分を明らかにすることで、他の国における IoT セキュリティ評価制度との相互承認に向けた調整が進むことが期待される。

令和7年度産業サイバーセキュリティ対策の強化に向けた環境整備事業
（ソフトウェアのセキュリティ確保等に関する調査）報告書 - 第 4 編
JC-STAR 活用も含めた IoT 製品セキュリティ向上

2026 年 3 月

株式会社三菱総合研究所
安全保障政策本部
TEL (03)6858-3578

経済産業省 御中

令和7年度産業サイバーセキュリティ対策の強化に向けた環境整備事業
（ソフトウェアのセキュリティ確保等に関する調査）

報告書 - 第5編

インド太平洋地域向け日米EU産業制御システムサイバーセキュリティ関連

MRI 三菱総合研究所

安全保障政策本部

2026年3月31日

目次

図 目次

図はありません。

表 目次

1. インド太平洋地域向け日米EU産業制御システムサイバーセキュリティ・ウィークの開催

2025 年秋に4日間にわたってインド太平洋地域向け日米EU産業制御システムサイバーセキュリティ・ウィークを開催した。今年は、日米欧のサプライチェーンレジリエンス強化及びインド太平洋地域の能力構築を最大限に実現するため、演習の参加人数を拡大。インド太平洋地域の重要インフラ事業者、製造業者、国の CSIRT（Computer Security Incident Response Team）における OT（Operational Technology：制御技術）・IT（Information Technology：情報技術）のサイバーセキュリティ担当者や、関連する政府機関における政策担当者等65名が東京にて対面で受講した。また、初日の開会・基調講演・セミナーについては対面参加が叶わなかった参加希望者等にオンラインで配信した。なお、今年は、米国における連邦政府の一部封鎖の影響により、米国の参加は開会挨拶のみであった。

具体的には、2025 年11月18日から 21 日にかけて全4日間のプログラムを実施。日米 EU 各国のサイバーセキュリティ政策の動向、産業制御システムにおける重要インフラ企業等のセキュリティ対策、サプライチェーンリスク・マネジメント等について、日 EU の政府高官や企業の実務者等によるセミナーを実施した。なお、各業界特有のリスクや事例等を盛り込んだ仮想企業のシナリオを用いた業界別ワークショップや、IPA ICSCoE による産業制御分野における AI を活用したサイバー攻撃に対するハンズオン演習を実施したほか、新規のプログラムとして欧州連合サイバーセキュリティ機関（ENISA）によるワークショップを実施した。インド太平洋地域及び欧米と国際的な議論を行うことで、諸外国の産業制御システム分野におけるセキュリティ政策について情報収集を行うとともに、ネットワーク構築を図り、我が国セキュリティ政策との国際調和とサプライチェーン全体の強靱化を図った。

1.1 開催概要

サイバーセキュリティ・ウィークは、経済産業省、独立行政法人情報処理推進機構（IPA）の産業サイバーセキュリティセンター（ICSCoE）、米国政府（国土安全保障省（DHS）のサイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）、国務省（DOS））及び EU 政府（通信ネットワーク・コンテンツ・技術総局（DG CONNECT）、欧州連合サイバーセキュリティ機関（ENISA）、欧州対外行動局（EEAS））の協力の下、2025 年11月18 日から 21 日までの4日間、インド太平洋地域における産業制御システム（ICS）のサイバーセキュリティに焦点を当てた研修プログラムとして開催された。

今回で 8 回目となるサイバーセキュリティ・ウィークは、インド太平洋地域からの参加者の ICS システムに関するサイバーセキュリティ能力を強化することを目的として毎年実施されている。毎回、インド太平洋地域の各国より OT/IT サイバーセキュリティの専門家、各国 CSIRT のサイバーセキュリティ専門家、関係省庁の政策当局者、重要インフラ関係者らが参加しており、本年も日・EU の専門家からサイバーセキュリティに関する様々なトピックを学び、参加者間でそれぞれの経験や見解を共有するユニークで貴重な機会となった。

本プログラムにより ICS サイバーセキュリティに関する共通認識を確立し、拡大するサイバーセキュリティの脅威に共同で対処するためのさらなる国際協力の基盤となる、インド太平洋地域と日本、米国、EU との関係強化に貢献することが期待されるものである。

全体プログラムの構成を下表に示す。

表 1-1 全体プログラムの構成

(1) セレモニアルセッション
- オープニングセレモニー
- 基調講演
- クロージングセレモニー
(2) ハンズオン演習
- AI を活用した OT システム保護
- SBOM
(3) セミナー
- サプライチェーン・セキュリティ
- サイバー・レジリエンス 等
(4) ワークショップ
- アイスブレーク
- ENISA スマート演習
- CVD(脆弱性開示)
- IoT 脆弱性管理
- SBOM
- 業界別の議論

1.1.1 サイバーセキュリティ・ウィークの参加者

サイバーセキュリティ・ウィークの主な受講生は、インド太平洋地域(ASEAN 加盟国、インド、バングラデシュ、スリランカ、モンゴル、台湾)の推薦をうけた 65 名であった。参加者はそれぞれインド太平洋地域の重要インフラ事業者、国の CSIRT における OT(Operational Technology:制御技術)・IT(Information Technology:情報技術)のサイバーセキュリティ担当者、関連する政府機関における政策担当者などであった。

1.2 プログラムの概要

サイバーセキュリティ・ウィークは以下に示す日程、時間割で実施された。

表 1-2 プログラムのタイムテーブル

1 日目 ： 11 月 18 日(火)		
9:00-9:30		受付
9:40-10:35	C1	オープニングセレモニー・開会の辞、基調講演
10:35-10:50		ショートブレイク
10:50-12:35	S1	セミナー
12:35-14:00		昼食
14:00-15:30	W1	アイスブレーク
15:30-16:00		写真撮影、ショートブレイク
16:00-18:00	W2	ワークショップ(EU(ENISA))

2 日目 ： 11 月 19 日(水)		
9:00-9:30		受付
9:30-12:00	H1	ハンズオン(JP(IPA ICSCoE))
12:00-13:00		昼食
13:00-17:30	H2	ハンズオン(JP(IPA ICSCoE))
18:00-19:30		ネットワーキング

3 日目 ： 11 月 20 日(木)		
9:00-9:30		受付
9:30-10:30	W3	ワークショップ(JP(JPCERT/CC))
10:30-10:45		ショートブレイク
10:45-12:00	W3	ワークショップ(JP(IPA ICSCoE))
12:00-13:00		昼食
13:00-13:40	W3	ワークショップ(JP(METI))
13:40-14:00		ショートブレイク
14:00-17:30	H3	ハンズオン(JP(IPA ICSCoE))

4 日目 ： 11 月 21 日(金)		
9:00-9:30		受付
9:30-12:00	W4	ワークショップ(セクター毎の議論)(JP(IPA ICSCoE))
12:00-13:00		昼食
13:00-14:00	W5	ワークショップ(セクター毎の議論)(JP(IPA ICSCoE))
14:00-14:30	C2	クロージングセレモニー・閉会の辞・修了証授与式・受講生代表挨拶
14:30-15:00		会場から IPA 秋葉原へ移動
15:00-15:15		施設見学受付

4 日目 ： 11 月 21 日(金)			
15:15-16:45	O1	グループ 1:施設見学(IPA)	グループ 2:セミナー
16:45-17:00		グループ交代	
17:00-18:30	O1	グループ1:セミナー	グループ2:施設見学(IPA)

1.3 各セッションの概要

1.3.1 開会の辞・基調講演／Opening Remarks and Keynote Speech

主催者を代表して、日米 EU の各関係組織より開会挨拶があった。また、基調講演が行われた。

（1） 講演者一覧

表 1-3 開会の辞・基調講演の講演者一覧

開会挨拶	● Mr. Thomas GNOCCHI, Minister / Deputy Head of the European Union Delegation to Japan (EU) ● 松尾 剛彦，経済産業省 経済産業審議官 ● Mr. Aaron D. SNIPE, Deputy Chief of Mission (US)
基調講演	● 奥家 敏和，経済産業省 大臣官房審議官 （商務情報政策局担当） ● Mr. Christian VAN HEURCK, ENISA (EU)

1.3.2 セミナー／Seminars

日本・欧州の OT セキュリティに関する取り組みについて、スピーカーが OT サプライチェーン・セキュリティの強化・管理、レジリエンスの強化を中心に最新情報を提供した。OT サイバーセキュリティのレベルを高めるためには、どのようなサプライチェーン管理が効果的なのか。また、組織的なレジリエンスを構築するためにはどのようなアプローチが重要なのか。6 人の講演者がこれらの課題に対するヒントを提供し、議論を行った。

（1） 講演者一覧

表 1-4 セミナーの講演者一覧

講演者及びタイトル	1. “Strengthening OT Supply Chain Security: A Practical Approach Using METI Factory Security Guidelines”, 佐々木弘志 OT セキュリティワーキンググループ, Japan Network Security Association (JNSA) 2. “Integration of OT Cybersecurity into Traditional Safety Culture Strengthening Industrial Supply Chain Resilience”, 竹内陽祐，横河デジタル株式会社 セキュリティ部プリンシパルコンサルタント 3. “Initiatives for Supply Chain Security Management in Control Systems at Daigas Group”, 辰巳大祐 大阪ガス株式会社 システム管理部 アシスタントマネージャー

	4.	“Your Program, Your Power: Build a Path to True Resilience” Mr. Christian VAN HEURCK, Deputy Head of Unit – Capacity Building Unit, ENISA, EU Mr. Gaspare FERRARO, Technical Officer, CINI Cybersecurity National Lab, EU Mr. Ioannis AGRAFIOTIS, Senior Research Associate, University of Oxford, EU

1.3.3 アイスブレーク／IceBreaker

アイスブレークでは、サイバーセキュリティや各国の文化に係るクイズによるビンゴ大会を実施し、ビンゴの揃った受講生から、以下のプレゼンテーションを行ってもらい、相互理解と交流を深める機会を提供した。

- 自己紹介
- 職業上の経歴
- 自国における取組等の報告

1.3.4 ワークショップ（EU（ENISA））／Workshop （EU（ENISA））

本ワークショップは、受講生に以下の能力を獲得してもらうことを目的として開催された。

- マインドセットの転換：組織能力強化を目的とした真に効果的な「スマート演習」と、コンプライアンス重視の「チェックボックス形式の演習」との決定的な差異を認識する。
- 動機付けの獲得：現行の演習計画手法を開始または大幅に向上させるために必要な初期ステップを習得し、意欲を高める。
- 構造の理解及びコミュニティマインドセット：ENISA 手法（迅速に活用できるよう簡素化したもの）から導き出された中核的な計画原則を適用し、効果的な演習を構築する。知識共有と協調的問題解決を促進する専門家同士のネットワークの価値をより深く理解する。

1.3.5 ハンズオン AI（JP-IPA）／Hands-on AI（JP-IPA）

本ハンズオンは以下を目的として開催された。

- プロセスオートメーションに関連する ICS サイバーセキュリティの知識と技術を習得する。
- スクール形式により、人工知能（AI）を活用して OT システムを保護するために方法を学ぶ。

1.3.6 ネットワーキング／Networking

インド太平洋地域からの参加者同士のコミュニケーションを高めるため、お互いの文化や取組を共有する懇親会を実施した。11 月 19 日（2 日目）のハンズオン AI（JP-IPA）の後に実施した。

1.3.7 ワークショップ（JP（JPCERT/CC））／Workshop（JP（JPCERT/CC））

本ワークショップは以下を目的として開催された。

- 調整された脆弱性開示（CVD）について、その世界的な課題と関連活動について学習する。
- ワークショップにおいて、参加者を交えた短いディスカッションセッションを数回実施し、このトピックが日々の業務や関連事項にどのような影響を与えるかを探求する。

1.3.8 ワークショップ（JP（IPA ICSCoE））／Workshop（JP（IPA ICSCoE））

本ワークショップは以下を目的として開催された。

- IoT 脆弱性管理の実践的な能力を構築することを目的としている
- 参加者は、重要な IoT デバイスの脆弱性を含むシナリオベースのワークショップを通じて、現実世界のシナリオに対する準備態勢を整え、組織的な意思決定スキルを身につける

1.3.9 ワークショップ（JP（METI））／Workshop（JP（METI））

本ワークショップは以下を目的として開催された。

- SBOM の基本的な考え方と、サイバーセキュリティの観点から SBOM を導入することの重要性を理解することを目的とする
- 参加者は、ソフトウェアサプライチェーンを含む SBOM の構造的なイメージや、SBOM の議論に関する世界的な政策動向に関する知識を得ることができる

1.3.10ハンズオン SBOM（JP-IPA）／Hands-on SBOM（JP-IPA）

本ハンズオンは以下を目的として開催された。

1. SBOM の構造と生成方法を理解し、関連ツールの使用経験を積む。
2. SBOM と脆弱性データベースを相互参照し、自動化されたリスク特定を可能にする方法を学ぶ。
3. 可視化ツールを使用して結果を分析し、重要インフラ環境における SBOM の実用的なアプリケーションを調査する。

1.3.11ワークショップ（セクター毎の議論）／Workshop（Sector-specific discussion）

本ワークショップは以下を目的として開催された。

- 企業や組織の全体的なレジリエンスを強化するため、サイバーセキュリティ問題への対応とリカバリーの能力を強化する。

1.3.12 クロージングセレモニー／Closing Ceremony

主催者を代表して、日本の関係組織より閉会挨拶があった。次にプログラムを修了した受講生全員に修了証が授与された。その後、受講生代表3名よりスピーチしていただいた。

1.4 プログラムの総括

今年は、70 名を目標に受講生を集めるとともに、一部のプログラムについてはオンラインで受講可能にした。プログラム全体を通じ、日・EU のサイバーセキュリティの専門家から、産業制御システムを中心とするサイバーセキュリティ確保に向けた政策、OT サプライチェーン・セキュリティ、レジリエンス等に関する様々な取組の紹介や解説が行われた。また、IPA ICSCoE 及び EU(ENISA)による実践的なハンズオン、ワークショップも行われ、インド太平洋地域からの参加者にとっては産業制御システムに関する世界の最先端に触れ、それらの具体的手法を体験的に習得する機会となり、非常に高い満足度を得る結果となった。

また、一昨年、昨年に引き続き、今年も受講生を東京に集めての集合研修として実施したことにより、個別の知識習得だけでなく、国際的な人脈づくりにも非常に役立つ結果となり、今後の継続的な連携にも多くの期待が寄せられた。

本プログラムはインド太平洋地域における産業制御システムのサイバーセキュリティ確保を主導する立場の人材育成に貢献するものであり、受講生が今回の経験をそれぞれの国に持ち帰り今後の対策を主導していくこと、国際間の連携を推進することで、インド太平洋地域全体の対策向上に貢献するとともに、サイバーセキュリティの推進という意味においてこれらの国々と日米 EU の連携強化に貢献していくものと期待される。

2. 総括

本調査では、インド太平洋地域各国の重要インフラ関連企業等の制御システム・セキュリティの担当者、サイバーセキュリティ政策担当官庁の担当者、ナショナル CSIRT の担当者を集め、日米 EU の産業制御システムに関するサイバーセキュリティ政策やその取組についてのセミナー、脆弱性管理の他、AI や SBOM 等の最新の技術テーマも含む演習を実施した。そして、人材育成及び国際ネットワーク形成という観点で、相互交流の機会提供や演習実施結果の取りまとめと評価を実施した。

世界を見渡せば、大国間の紛争や大国による他国への威圧はますます増加し、相変わらず地域紛争も絶えない状況にある。これらに合わせてサイバー攻撃は更に増加、高度化が進展している。

このような昨今の世界情勢を踏まえ、我が国にとってインド太平洋地域は地政学的な重要性がこれまでにも増して高まっている地域であり、この地域のサイバーセキュリティの担当者・専門家に対して日米 EU によるキャパシティー・ビルディングを図ることで、インド太平洋地域に最新のサイバーセキュリティ対策を備えた有志国を拡大していくことは非常に重要な取組である。

今回の開催においては前回に引き続き東京に関係者を集めて物理開催をすることで、国際間で参加者同士がお互いに顔を知る関係を築くことが出来たことは、最大の成果だと言うことも出来る。受講生自身もそのことをよく認識しており、クロージングにおける受講生のコメントでもその点は強調されていた。

このような取組を引き続き、そして拡大的に継続し、インド太平洋地域において日々進化するサイバー攻撃やその対策についての最新の情報を相互に共有し、最新のサイバーセキュリティ対策を備えた有志国の拡大、仲間となる関係者の拡大を図っていくことが重要である。

令和7年度産業サイバーセキュリティ対策の強化に向けた環境整備事業
（ソフトウェアのセキュリティ確保等に関する調査） 報告書- 第5編
インド太平洋地域向け日米EU産業制御システムサイバーセキュリティ関連

2026 年 3 月

株式会社三菱総合研究所
安全保障政策本部
TEL (03)6858-3578

（様式３）

二次利用未承諾リスト

令和７年度産業サイバーセキュリティ対策の強化に向けた環境整備事業（ソフトウェアのセキュリティ確保等に関する調査）報告書

令和７年度産業サイバーセキュリティ対策の強化に向けた環境整備事業（ソフトウェアのセキュリティ確保等に関する調査）

株式会社三菱総合研究所

頁	図表番号	タイトル
第１編 P.14	図2-10	NIST SP 1800-44におけるDevSecOpsの概念参照モデルとモデルをサポートする5つの概念
第１編 P.24	図2-13	NIST SP 1800-44におけるDevSecOpsの概念参照モデルとモデルをサポートする5つの概念