経済産業省　御中

令和6年度産業サイバーセキュリティ強靭化事業
（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

先進技術・セキュリティ事業本部

2025年3月31日

目次

図　目次

図表目次項目が見つかりません。

表 目次

図表目次項目が見つかりません。

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年度内にはIoT適合性評価制度を立ち上げ、運用を開始する予定であり、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、ビル、宇宙）のサイバーセキュリティ対策の検討やIoT機器の適合性検証制度の普及促進、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の推進を実施した。

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・整理
3. 工場SWG関連
   (1) 工場等の製造現場におけるサイバーセキュリティ対策の検討
   (2) 検討会の運営
4. ビル SWG 関連
5. IoT適合性評価制度関連
   (1) IoTセキュリティ適合性評価制度の利活用における調査・普及啓発
   (2) IoT開発・検証に関するセキュリティ関連ガイドライン類の制度との整合性確保
6. 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 ビル SWG 関連
第 5 編 IoT適合性評価制度関連
第 6 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、SBOM 導入・活用に関する国内外の動向調査、SBOM を活用した脆弱性管理に関わる実証を通じて関連する課題と解決法に関する整理を行った。また、ソフトウェア利活用に関わるセキュリティリスク、課題及び対応策について調査、検討を行った。具体的には、システムやソフトウェアの開発ベンダー、ツールベンダー、業界団体に対するヒアリングを中心として、文献情報なども加えて、開発現場の実態、課題について整理し、課題に対する解決アプローチ、今後の施策・調査課題などについて整理した。これらの調査・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、OSS の利活用等について議論を実施し、以上の取組みを通じて、SSDF 導入ガイダンス案（中間整理）を取りまとめた。

宇宙 SWG 関連においては、「宇宙産業 SWG 作業部会コアメンバー会議」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動向を調査したほか、民間宇宙事業者に対するヒアリングを通じて、「民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン」の活用状況やセキュリティ対策上の課題を聴取した。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。

工場 SWG 関連においては、工場セキュリティガイドラインに関して、今後も新たなテーマを取扱う別冊を追加可能とするための構成変更を行った。この構成変更に合わせ、中小製造事業者を中心に経営者のセキュリティへの理解不足を解消し製造現場へのセキュリティ普及を目的として、必要最低限の内容構成で工場セキュリティについて簡潔に解説したガイドラインの別冊：Appendix【工場セキュリティの重要性と始め方】を策定した。また、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・底上げを目的とした「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活動や Appendix に対する意見集約を行った。これらの活動を踏まえ、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」の本編及び Appendix が活用され、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ことが望まれる。

ビル SWG 関連においては、活動主体の移行先として兼ねてより検討中であったスマートビルのコンソーシアムが、2025 年度からスマートビルディング共創機構として本格稼働することが決まり、同機構のセキュリティ WG への合流に向けてビル SWG メンバーへの説明会を実施した。その結果、ビル SWG メンバーの多くについて合流意思を確認することができ、スマートビルディング共創機構セキュリティ WG においてビル SWG を引継いだ活動が実施されることがほぼ確実なものとなった。

IoT 適合性評価制度関連においては、IoT 製品に対するセキュリティ適合性評価制度となる JC-STAR 制度に関し、制度の利活用に向けた調査・普及啓発として、JC-STAR 制度の活用が期待される業界団体である JBMIA、JUAV、セキュアドローン協議会と制度活用に向けた調整を行ったほか、特定分野システムにおける制度普及を目的として、「特定分野システムの IoT 製品における JC-STAR 制度活用ガイド」を作成し、公開した。また、既存のセキュリティ関連ガイドライン類との整合性確保のため、国内の IoT 関連セキュリティガイドの調査・整理を行うとともに、経済産業省が発行する「IoT 機器を開発する中小企業向け製品セキュリティ対策ガイド」及び「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 制度との整合性確保や制度の活用促進を目的とした記

載内容の見直し及び改定を行った。

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担当省庁やナショナル CSIRT の担当者を招聘し、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サプライチェーンセキュリティへの取組等について、セミナー・ハンズオン演習・ワークショップ等を東京で対面にて実施することで、インド太平洋地域の人材育成及びこれらの地域と日米 EU を含む国際ネットワーク形成を図ることが出来た。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、6 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6年度産業サイバーセキュリティ強靭化事業

（ソフトウェアのセキュリティ確保等に関する調査） 調査報告書

全体概要

2025 年 3 月

株式会社三菱総合研究所
先進技術・セキュリティ事業本部
TEL (03)6858-3578

経済産業省 御中

令和6年度産業サイバーセキュリティ強靭化事業（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

先進技術・セキュリティ事業本部

2025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 SBOM の導入や活用に関する調査・検討を行うとともに、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課題や対応策等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、令和 5 年度事業で作成した「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引」の英訳を行った。

2. SBOM の利活用における調査・普及啓発

本章では、企業やサプライチェーンにおける SBOM の導入や活用等に関する動向の調査結果を示す。また、「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引」の改定に関する業務の実施結果を示す。

2.1 SBOM 等に関する国内外動向調査

本事業で調査対象とした国内外の SBOM 等に関する取組動向等は下表に示すとおりである。以降では各取組の概要を示す。

表 2-1 国内外の SBOM 等に関する取組動向の調査対象

※ 取組年月順

#	取組名・文書名	取組年月	国・地域	取組主体
1	Call for views on the Code of Practice for Software Vendors[1]	2024 年 5 月発表	英国	DSIT（科学・イノベーション・技術省）
2	Software Acquisition Guide for Government Enterprise Consumers: Software Assurance in the Cyber-Supply Chain Risk Management (C-SCRM) Lifecycle[2]	2024 年 8 月発表	米国	ICT SCRM Task Force[3]
3	Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem[4]	2024 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）、FBI（連邦捜査局）
4	SBOM-a-rama Fall 2024[5]	2024 年 9 月開催	米国	CISA
5	ウィルミントン宣言（The Wilmington Declaration）[6]	2024 年 9 月発表	QUAD（日米豪印）	外務省等

[1] https://www.gov.uk/government/calls-for-evidence/a-code-of-practice-for-software-vendors-call-for-views/call-for-views-on-the-code-of-practice-for-software-vendors
[2] https://www.cisa.gov/resources-tools/resources/software-acquisition-guide-government-enterprise-consumers-software-assurance-cyber-supply-chain
[3] ICT Supply Chain Risk Management Task Force の略で、CISA が組織し、共同議長を務めるタスクフォースのこと。国家リスク管理センター（NRMC）や IT 及び通信の重要インフラ部門の代表者が参加し、連邦政府や重要インフラの民間部門の所有者及び運営者に助言や勧告を行う。
[4] https://www.cisa.gov/resources-tools/resources/secure-demand-guide
[5] https://www.cisa.gov/news-events/events/sbom-rama-fall-2024
[6] https://www.mofa.go.jp/files/100728100.pdf, https://www.mofa.go.jp/mofaj/files/100728333.pdf（仮訳）

#	取組名・文書名	取組年月	国・地域	取組主体
6	Framing Software Component Transparency (2024)[7]	2024 年 10 月発表	米国	CISA
7	Safe Software Deployment: How Software Manufacturers Can Ensure Reliability for Customers[8]	2024 年 10 月発表	米国	CISA
8	Cyber Resilience Act[9]	2024 年 11 月正式発行	EU	欧州委員会、欧州理事会
9	Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles[10]	2025 年 1 月最終版発表	米国	BIS（商務省産業安全保障局）
10	Strengthening and Promoting Innovation in the Nation's Cybersecurity[11]	2025 年 1 月発表	米国	バイデン前大統領

（1）英国：Call for views on the Code of Practice for Software Vendors

2024 年 5 月、英国 DSIT は、ソフトウェアの開発、構築、保守の方法と、ソフトウェアを調達する顧客との情報提供方法に関するベンダーの行動規範案とその想定利用方法等を示し、パブリックコメントを募集した。行動規範案は、4 つの原則に分類された 21 の事項から構成される。具体的な原則は下表に示すとおりである。各事項に対して、(1)必須と推奨の 2 段階で定めた要求度、(2)客観的評価可能な技術的管理策、(3)実務レベルで示した実施ガイダンスが示される予定である。

表 2-2 英国 DSIT によるソフトウェアベンダーに対する行動規範の概要

原則	目的	ベンダーへの必須、推奨事項	技術的管理策	実施ガイダンス
1. 安全な設計と開	ソフトウェア製品やサービス	必須事項 6 件 例）1.2 サードパー	各必須事項に対し、例が示されて	必須事項 2 件について、例が示されている。

[7] https://www.cisa.gov/resources-tools/resources/framing-software-component-transparency-2024
[8] https://www.cisa.gov/resources-tools/resources/safe-software-deployment-how-software-manufacturers-can-ensure-reliability-customers
[9] https://eur-lex.europa.eu/eli/reg/2024/2847/oj
[10] https://www.federalregister.gov/documents/2025/01/16/2025-00592/securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles
[11] https://www.federalregister.gov/documents/2025/01/17/2025-01470/strengthening-and-promoting-innovation-in-the-nations-cybersecurity

原則	目的	ベンダーへの必須、推奨事項	技術的管理策	実施ガイダンス
発	を提供する際に、適切な安全性を確保する	ティコンポーネントの取り込み及び保守に関連するリスクを、ライフサイクル全体を通して評価する。	いる。 例）1.2 サードパーティ製コンポーネントのインベントリを保有し、既知の脆弱性がないか定期的に確認する。	例）1.2 必須の実装手段として、(1)SBOM 等を利用したサードパーティコンポーネントの把握、(2) 把握したコンポーネントに対する定期的な検証。ほかに推奨の実装手段 2 件と有用なリンクを例示。
2. 構築環境のセキュリティ	構築環境が危険にさらされるリスクを低減し、ソフトウェアの完全性と品質を保護する	**必須事項 1 件、推奨事項 2 件** 例）2.1 環境を不正アクセスから確実に保護する。	各必須事項に対し、例が示されている。 例）2.1 開発環境とビルド環境において、ID とアクセス管理を実装する。開発者に多要素認証を義務付ける。	記載なし
3. 安全なリリースと保守	脆弱性の可能性と影響を最小化する	**必須事項 5 件、推奨事項 1 件** 例）3.1 ソフトウェアが顧客に安全に配布されるようにする。	各必須事項に対し、例が示されている。 例）3.1 ソフトウェアとアップデートは、信頼できるチャネルを通じてのみ配布する。	記載なし
4. 顧客への情報提供	効果的なリスク管理とインシデント管理を可能にする	**必須事項 6 件** 例）4.1 組織は、販売するソフトウェア製品/サービスに対して提供されるサポートと保守のレベルを明記した情報を、利用しやすい方	各必須事項に対し、例が示されている。 例）4.1 EOL のポリシーを公表する。	記載なし

原則	目的	ベンダーへの必須、推奨事項	技術的管理策	実施ガイダンス
		法で確実に提供する。		

（2）米国：Software Acquisition Guide for Government Enterprise Consumers: Software Assurance in the C-SCRM Lifecycle

2024 年 8 月、ICT SCRM Task Force は、政府機関のソフトウェア取得プロセスにおいて、担当者がサプライヤーの保証やサイバーセキュリティ透明性の管理状況を把握するためのガイドを発表した。ガイドでは、5 つの領域において、サプライヤーの管理状況を把握するための確認事項（質問事項）が示されている。5 つの管理領域と、確認事項の概要を下表に示す。質問形式の確認事項に回答することでサプライヤーの状況が把握できるとし、米政府機関以外での利用も推奨されている。

表 2-3 米国 ICT SCRM Task Force によるソフトウェア取得ガイドの概要

管理領域	確認事項の概要
（1）サプライヤーガバナンスと認証	（2）以降の確認事項で不要なものを除外するための確認項目。CISA により規定されたセキュア・ソフトウェア開発証明書を提供しているか、内部及びサードパーティ部品の出所データを保持しているかなどの体制に関する確認事項が主である。
（2）ソフトウェアサプライチェーン	サプライヤーが、ソフトウェアのライフサイクルを通じたリスク管理を行っているか、及びそのためのプロセス等を整備しているかの確認事項。特にサードパーティ製ソフトウェアの設計開発実装の意思決定の透明化を重視している。
（3）セキュアなソフトウェア開発	「セキュアバイデザイン」を実現するために必要な基準の管理をサプライヤーが行っているかの確認事項。開発手法や開発環境への確認事項が主である。
（4）セキュアなソフトウェアデプロイメント	ソフトウェアのデプロイメントの前後に、リスクの特定と軽減を目的としたプロセスと手順が適用されているかを確認する事項である。
（5）脆弱性管理	新たな脆弱性が報告されると、顧客（ソフトウェア取得者）がリスクを評価するためのセキュリティ勧告をサプライヤーが発行する。サプライヤーは脆弱性を継続して監視し対処する必要があり、そのためのプロセスと手順が適用されているかを確認する事項である。

（3）米国：Secure by Demand Guide

2024 年 8 月、CISA と FBI は、ソフトウェア製造者がセキュアバイデザインの原則に従っているか否かをソフトウェア利用者が判断するためのガイドである「Secure by Demand Guide」を発表した。

本ガイドでは、ソフトウェア利用者が、製造者に対して確認すべき事項(質問事項)が 6 つの項目別で整理されている。項目別の確認事項の概要を下表に示す。

表 2-4 米国 CISA・FBI による Secure by Demand Guide の概要

項目	確認事項(質問事項)の概要
1.一般的な質問	・ ソフトウェア製造者が CISA の「セキュアバイデザイン誓約書(Secure by Design Pledge)」を取得しているか。 ・ ソフトウェア利用者がセキュリティパッチを簡単にインストールできるようにしているか。
2.認証サポートに関する質問	・ ソフトウェア製造者は、安全な認証をサポートしている必要がある。そのため、ソフトウェア利用者としては、以下のような確認事項が想定される。 ・ シングルサインオン(SSO)を追加コストなしに提供しているか。デフォルトのパスワードを廃止しているか。 ・ ソフトウェア製造者が認証を管理する場合、他要素認証などのフィッシング耐性のある形式を有効にしているか。
3.脆弱性への対処に関する質問	・ ソフトウェア製造者は、ソフトウェアの欠陥のクラス全体に体系的に対処する必要がある。そのため、ソフトウェア利用者としては、以下のような確認事項が想定される。 ・ どのような脆弱性のクラスに組織的な対処を行っているか。 ・ どのような脆弱性のクラスを排除する予定かを示すロードマップが存在するか。
4.セキュリティログに関する質問	・ ソフトウェア製造者は、セキュリティログをソフトウェア利用者が利用できるようにすべきである。セキュリティログは、構成の変更や構成設定の読み取り、アイデンティティと該当する場合にはネットワークフロー、データアクセス及びビジネス関連データの作成などの情報を含むべきである。
5.ソフトウェアサプライチェーンのセキュリティに関する質問	・ ソフトウェア製造者は、サードパーティの依存関係の出所データを維持、共有する必要がある。そのため、ソフトウェア利用者としては、以下のような確認事項が想定される。 ・ SBOM を標準的な機械可読可能な形式で作成し、ソフトウェア利用者が利用できるようにしているか。 ・ OSS のセキュリティをどのように保護しているか。そのためのプロセスを保有しているか。
6.脆弱性の開示と報告に関する質問	・ ソフトウェア製造者は、脆弱性報告の透明性と適時性を示すべきである。そのため、ソフトウェア利用者としては、以下のような確認事項が想定される。 ・ ソフトウェア製造者の製品の全ての共通脆弱性識別子(CVE)に共通脆弱性タイプ一覧(CWE)と共通プラットフォーム一覧(CPE)を含むか。 ・ ソフトウェア製造者は脆弱性開示ポリシーを公開し、一般のメンバーによるテストを許可しているか。

（4）米国:SBOM-a-rama Fall 2024

2024 年 9 月、SBOM に関するイベントである SBOM-a-rama が、米国デンバーでの対面及びオンライン配信によるハイブリッド形式で開催された。本イベントは SBOM コミュニティの醸成を目的としており、計 18 のセッションが行われた。具体的なセッション一覧は下表に示すとおりであり、SBOM に関するコミュニティ活動、米国の政府組織における取組、米国の事業者における取組、韓国政府の取組等が発表された。

表 2-5 SBOM-a-rama Fall 2024 のセッション一覧

発表者	発表概要
Office of the Deputy Assistant Secretary of the Army for Data Software & Engineering	米軍においてはソフトウェアの活用の広がりに合わせて 2025 年 2 月以降に SBOM をソフトウェアに求める予定である。
OWASP	SBOM や VEX 等のソフトウェアの透明性確保に関連する情報を交換できるよう専用 ID と API プラットフォームを構築している。
SBOM Sharing Tiger Team	SBOM 共有ライフサイクルにおける SBOM 作成者、ディストリビューター、利用者での役割を整理したガイド作成予定である。
SBOM Generation Tiger Team	様々なソフトウェアを対象に OSS ツールを利用して SBOM 生成したところ、複数の SBOM 形式への対応コスト、NTIA の最小要素の不明瞭さなど課題として確認している。
AIBOM Tiger Team	コンプライアンス対応、セキュアバイデザイン等複数の観点の AIBOM を検討して、ガイドラインを作成している途中である。
BOMOPS Tiger Team	SBOM の利用者目線からインシデントレスポンスやコンポーネントの活用分析等の様々なユースケースを検討して、ガイドラインに取りまとめている途中である。
Lockheed Martin	SBOM を自社で検討して、組み込み機器向けのプログラム、手動の SBOM 作成、SBOM の可視化などを課題として確認している。
Healthcare SBOM PoC Team	ヘルスケア業界では、25 の SBOM と 3 つの VEX を PoC で構築して様々なガイドラインを構築している。
Finite state	携帯電話業界に関連する SBOM のガイドラインが構築されている中、モバイル業界の国際的な業界団体の GSMA と活動している。
FDA	SBOM を医療機器に要件化している中、SBOM に記載するデータの標準化が必要不可欠であることを確認している。
Korea University	ソフトウェアサプライチェーンのセキュリティ確保における SBOM の利用方法を記載したガイドラインを作成している。
SBOM VEX Group	公開されている VEX を調査し、VEX フォーマットの多様性、公開脆弱性データベースとの連携などを課題として確認している。

発表者	発表概要
SBOM Tooling Cataloging Group	SBOM ツールのカタログを作成に向けてツールの機能のリストを現状の SBOM ツールにある機能と今後の SBOM ツールに必要な機能の 2 軸で検討している。
SBOM Tooling Implementation Group	アンケートなどを基に SBOM の最小要素への期待、SBOM データの成熟度、SBOM の追加要素についてガイドラインとして取りまとめている途中である。
Carnegie Mellon University	様々なツールが同じソフトウェアに対してどのように異なる SBOM を生成するかを調査し理解することを目的とした Plugfest を開催する予定である
Splunk	自社のソフトウェアのソースコードとバイナリファイルで作成した SBOM を 2 種類公開している。VEX の利用や SBOM 生成の精度などを課題として認識している。
CISA On Ramps & Adoption WG	ポッドキャスト・講演発表・イベントなどの普及における活動を実施状況について報告している。

（5）QUAD：ウィルミントン宣言

2024 年 9 月、QUAD（日米豪印戦略対話）の首脳会合が米国ウィルミントン近郊で開かれ、会合後、共同声明として「ウィルミントン宣言」が発表された。ウィルミントン宣言では、インド太平洋地域の平和と安定の維持のために、「善を推進するグローバルな力」を発揮するとともに、「地域及びグローバルな課題への取組に向けた協力」を推進することを宣言している。また、このために、日米豪印が「インド太平洋のための永続的パートナー」であることも宣言している。宣言内の「サイバー」の項目では、2023 年のソフトウェアセキュリティに関する日米豪印共同原則[12]に基づき安全なソフトウェア開発要件及び認証に向けたコミットメントを拡大していること、当該要件の国際調和により、政府用ソフトウェアだけでなく、サプライチェーン、デジタル経済及び社会のサイバー強じん性を全体として向上させることが宣言されている。

（6）米国：Framing Software Component Transparency（2024）

2024 年 10 月、CISA は、SBOM の概念と実装に関するレポートである「Framing Software Component Transparency」の第 3 版を公開した。主な改定のポイントは以下のとおりである。

- SBOM ベースライン属性について全面的な改定が行われた。具体的には、「ライセンス」と「著作権」の属性が追加されたほか、各属性に対する期待事項を明確化し、3 段階の成熟度レベルを導入した。
- 「未知のコンポーネント属性」「再編集されたコンポーネント」「不明な依存関係」の 3 項目に対し、既知のユースケースにおける扱いを基にした 3 段階の成熟度レベルの推奨事項を提示した。
- SBOM ベースライン属性とのマッピングを示した既存 SBOM フォーマットから、SWID タグが

[12] https://www.mofa.go.jp/mofaj/files/100509255.pdf

削除された。

- SBOM 利用プロセスにリスク管理の概念が追加され、SBOM 普及の全体的な目標として、「リスク管理の改善」が明記された。

（7）米国:Safe Software Deployment

2024 年 10 月、CISA は、ソフトウェアやクラウドサービスの製造者を対象に、安全なソフトウェアデプロイメントを実施するためのガイダンスを発表した。ガイダンスでは、安全なソフトウェアデプロイメントの目的が、(1)堅牢な品質保証プロセスの確立、(2)コストと影響の適切な管理、(3)デプロイの制御及び計測、(4)包括的なテストの実施、(5)継続的な改善、(6)迅速な対応、(7)開発エコシステムの保護の 7 つの目標を達成することにあると明記している。これらの目標達成のために検討・実施すべき内容を 6 つの主要フェーズに分けて記載しているほか、関係者における責任の所在や対応すべき内容を記したプレイブックを紹介している。6 つの主要フェーズにおいて検討・実施すべき項目に関する概要は下表に示すとおりである。

表 2-6 米国 CISA による Safe Software Deployment ガイダンスの概要

主要フェーズ		検討・実施すべき項目とその内容
1. 計画	オペレーショナル・リスク評価	ソフトウェアを環境にデプロイする際のリスクと結果について、包括的かつ継続的な評価を実施する。 システムの関係と相互依存、潜在的な脅威、安全性、セキュリティ、信頼性、性能要件及び一般的な欠陥に関連するリスクを理解する。
	故障予知レビューの実施	以前の経験から得た洞察を基に故障予知レビューを行う。この際、チームが潜在的な失敗を特定するのに役立つ。
	プラットフォームの規模と多様性の検証	プラットフォームの多様性のほか、デバイスの数、OS の種類、ハードウェアブランド、ファームウェアのバージョン、ファームウェアの設定、帯域幅の速度と信頼性、環境設定、地理的な環境などの多様性を検証する。
	オンライン・サービスの多様性の検証	データセンター地域やネットワーク構成のほか、必要に応じて、フェイルオーバーやバックアップ・ソリューションに関する多様性を検証する。
	計画デプロイメントの間隔	ソフトウェアデプロイメントを行う時間的な間隔を正式に決定し、社内外に明確に伝達する。
	モニタリングとレポーティングの戦略	システムの健全性を示す信号を特定し、特定された問題を報告して、継続的改善プロセスにフィードバックする。
	人材確保	ソフトウェアデプロイメントと安全なプロセスの改良の両方を監視できるチームを確保する。

主要フェーズ		検討・実施すべき項目とその内容
	フォールト・トレランス	悪意のあるコード等が組み込まれても安全に機能するようなシステム設計を行うための、レジリエンスを組み込む方法を検討する。
	機能廃止と製品寿命の計画	機能の廃止や製品の寿命をあらかじめ計画し、顧客に早期に警告を行うことで悪影響を小さくする。
	パッチ計画	パッチ適用の計画と、パッチの適用プロセスの可能な限り迅速な実施するための手段を確立する。
2. 開発とテスト		顧客の典型的な環境に近い環境でテストを行い、テストにおいてソフトウェアデプロイメントプロセスを積極的に失敗させることにリソースを割く。
3. 内部でのロールアウト		組織内部でのみロールアウトすることで、外部ユーザーに届く前に問題を発見する。十分なカバレッジを得るため、以前のリリースサイクルを基に調整された標準を組織内で確立すべきである。
4. デプロイメントとカナリアテスト		カナリアデプロイメント(限られた数の顧客又はシステムに対する小規模なデプロイメント)によって、大規模なロールアウトの前にパフォーマンスを監視し問題を解決する。顧客のリスク許容度に応じてバリエーションを検討する。
5. 管理されたロールアウト		カナリアデプロイメントの成功を確認の後、デプロイするデバイスやシステムを段階的に増やすことで、突然の広範囲な障害を防ぐ。この際、適切な速度を考慮する。
6. 計画へのフィードバック		リリース後の継続的なフィードバック(ステークホルダーからの洞察、ログ、異常動作の例)を、次の開発サイクルの計画段階に直接フィードバックする。

(8) EU:Cyber Resilience Act

EU 市場に上市されるデジタル製品に対してサイバーセキュリティ対策を義務付ける Cyber Resilience Act(CRA:サイバーレジリエンス法)について、2024 年 10 月 10 日に欧州理事会により正式に採択、2024 年 11 月 20 日に EU 官報に掲載され、正式発行された。20 日後の 2024 年 12 月 11 日に発効となった。発効より 36 ヶ月後の 2027 年 12 月 11 日以降、CRA で規定されたサイバーセキュリティ対策が義務付けられる。ただし、第 14 条で定められる製造者の脆弱性報告義務については、21 ヶ月後の 2026 年 9 月 11 日以降の適用となる。

対象製品について、下図に示すとおり、ソフトウェアやハードウェアを含む、他の製品やネットワークへの直接的・間接的な接続が存在するあらゆるデジタル製品が対象となるが、既存の EU 法により要求事項が課されている医療機器、自動車関連製品等は除外される。対象製品の上市にあたって、当該製品に対するセキュリティ要件への適合性証明(自己適合宣言又は第三者認証)が求められる。

図 2-1 EU サイバーレジリエンス法の対象製品

対象となるデジタル製品に対する要求事項として、リスクに応じた適切なレベルのサイバーセキュリティを確保するように設計・開発・生産することや、悪用可能な既知の脆弱性がない状態で提供することを求めている。また、製造業者に対する要求事項として、デジタル製品の脆弱性ハンドリングに関する要求、製品のセキュリティ評価に関する要求、利用者への情報提示に関する要求、製品の適合性評価に関する要求、脆弱性の報告義務に関する要求等が規定されているほか、SBOM や OSS 管理に係る要求も規定されている。

製造業者が本法案のセキュリティに関する要件を遵守にしない場合、最大 1,500 万ユーロもしくは前会計年度の世界全体の総売上高の最大 2.5%のいずれか高い方が罰金として科される。

（9）米国:Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles

2025 年 1 月、米国 BIS は、中国とロシアの企業等によって製造・開発された技術[13]を用いたコネクテッドカーの輸入や販売を禁止する規則の最終版を発表した。本規則は、2024 年 9 月に発表された規則策定案公告（NPRM）[14]へのパブリックコメント結果を反映したもので、2025 年 3 月 17 日に発効された。商務省長官は、本規則の背景として、外国の敵対者が、運転手・同乗者等の大量の機密データを収集・記録するおそれがあること、コネクテッドカーを遠隔操作・遠隔無効化するおそれがあることを挙げている。

規則では、対象技術に関して中国・ロシアが関与していないことを証明するため、製造者等の情報や

[13] 中国・ロシアの企業などによって製造・開発された車両接続システム（テレマティクス制御ユニット、Bluetooth、セルラー、衛星通信、Wi-Fi モジュールなど車両が外部との通信を可能にする一連のシステム）と自動運転システム（運転手なしで車両を自律的に運転できるようにするためのシステム）が対象となる。中国・ロシアの所有、支配下にある又は司法権が及ぶ、或いはこれらの国からの指示に従う者によって設計、開発、製造、供給される場合も対象となる。

[14] https://www.federalregister.gov/documents/2024/09/26/2024-21903/securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles

デューデリジェンス文書からなる適合宣言書の提出を義務化する。ソフトウェア[15]に関して、2027 年モデルからの適用が開始となり、ハードウェアに関して、特定の車両モデルに依存しない車両接続システム製品の場合は 2029 年 1 月より、その他は 2030 年モデルからの適用開始を提案している。

NPRM では、全ての製品について SBOM の提出を義務付ける内容が含まれていたが、パブコメを通じて産業界の負担増加が懸念されたため、最終規則では SBOM の提出義務化の条項は削除されている。一方で、対象ソフトウェアのコンポーネント名やサプライヤー名などを特定するための文書（SBOM 又はその他の方法による）を作成すること、BIS が要求した場合には当該文書を提出することを求めており、SBOM に関する要件が完全に削除されたわけではない。

なお、製造業者が最低限管理すべき情報は、文書の作成者、タイムスタンプ、コンポーネント名及びサプライヤー名であり、これらは NTIA 最小要素より限定的である。

（10） 米国：Strengthening and Promoting Innovation in the Nation's Cybersecurity

2025 年 1 月 16 日、米国バイデン前大統領は、その退任前に、デジタルインフラの防御、デジタル領域の重要サービスの能力確保、脅威に対処するための能力の構築に取り組むことを目的に、サイバーセキュリティ改善のための追加措置を命じる大統領令（Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity）に署名した。本大統領令では、ソフトウェアとクラウド・サービス・プロバイダーの説明責任を改善し、連邦通信と ID 管理システムのセキュリティを強化し、革新的な開発とサイバーセキュリティのための新技術の利用を行政府・省庁間及び民間セクターとの間で促進することに重点を置いており、特に下表に示す項目に注力することが示されている。

表 2-7 米国大統領令の注力項目

項目	概要
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
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
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

[15] 本規則の対象ソフトウェアは、車両レベルで車両接続システム又は自動運転システムの機能をサポートするソフトウェアコンポーネントであり、アプリケーション、ミドルウェア、OS 等のシステムソフトウェアが含まれる。ファームウェアは対象外であるほか、OSS も対象外となる。ただし、ライセンスのある OSS が、再配布を意図しない特定の用途で、プロプライエタリなエンタープライズソフトウェアを作成するために用いられる（改変される）場合、OSS を改変する者が中国・ロシアに所有されている、支配下にある又は司法権が及ぶ、或いはこれらの国からの指示を受ける場合、結果として生じるソフトウェアは禁止の対象となる可能性がある。

項目	概要
サイバー犯罪及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
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
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
国家安全保障システムや重要システムにおける対策	国家安全保障システムなどの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
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

本表に示すとおり、新たな大統領令では、政府調達ソフトウェアのセキュリティ対策に関する指示が複数含まれている。政府調達ソフトウェア関連の指示内容及びタイムラインを下図に示す。

大統領令では、連邦調達ソフトウェアの開発に関するセキュリティについて、「機械可読ソフトウェア開発証明（machine-readable secure software development attestations）」[16]を利用したセキュリティ対策証明書の提出をソフトウェア開発事業者に義務付けること、本義務化を講じるために連邦調達規則（FAR）を改正することを求めている。関連して、CISA に対して、セキュリティ対策手法の評価やフォーマット等の指針の提供を求めている。

また、連邦調達ソフトウェアの提供やソフトウェア自体のセキュリティ対策に関して、パッチやアップデートに関する NIST SP 800-53 の更新、ソフトウェア運用に関する事項について SSDF の更新、SSDF の更新を踏まえた OMB（行政管理予算局）覚書 M-22-18[17]や CISA 自己証明フォームの改訂を求めている。

さらに、連邦調達ソフトウェアのサプライチェーンリスクについて、各省庁に対して NIST SP 800-161 の遵守を義務付けることや、連邦政府と契約する業者に対する最低限のサイバーセキュリティ要件を新たに策定し、その遵守を義務付けることを求めている。

[16] 大統領令の中で詳細は触れられていないが、CISA の「セキュアなソフトウェア開発に関する証明書フォーム（Secure Software Development Attestation Form）」を機械可読形式とし、ツールで生成や管理を容易にしたものであると考えられる。

[17] https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf

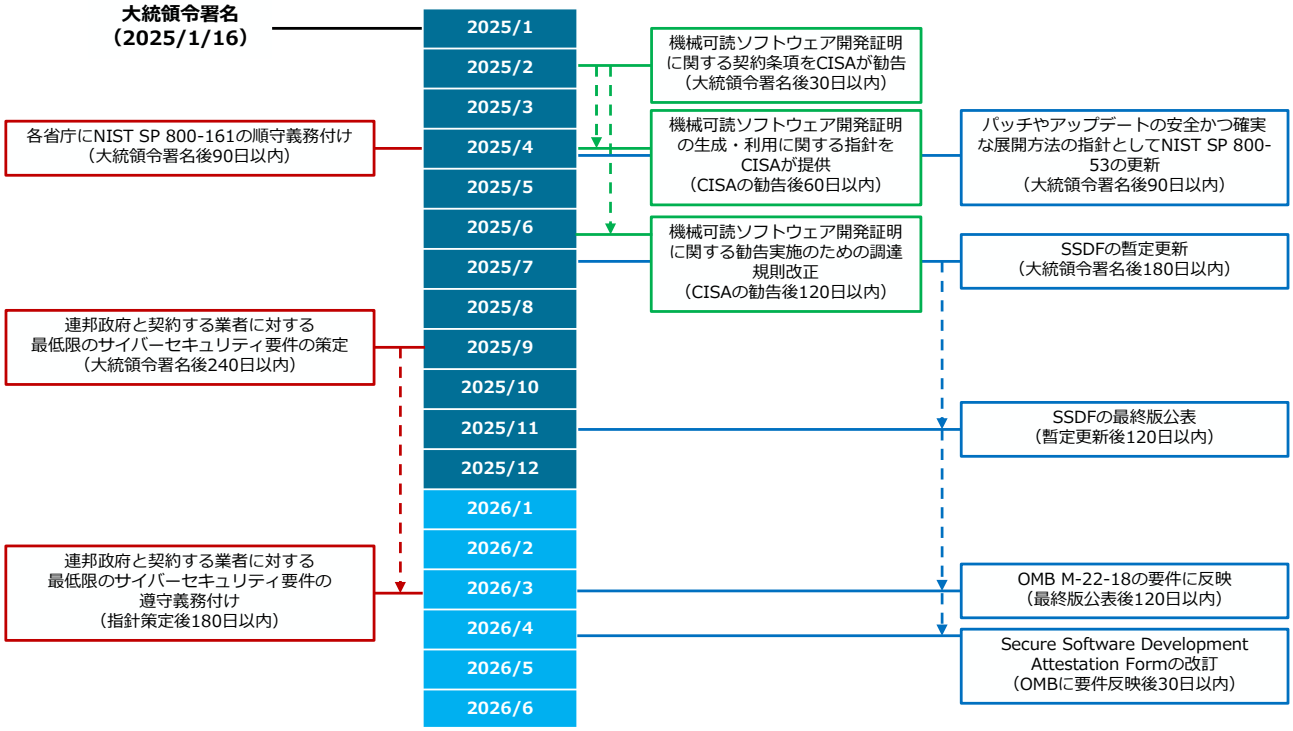


図 2-2 連邦調達ソフトウェアのセキュリティに関する大統領令の指示内容・タイムライン

2.2 安全なソフトウェア開発手法(SSDF)に関する米国取組の関係性

本事業では、安全なソフトウェア開発手法(SSDF: Secure Software Development Framework)の実践に向け、調査・整理及び実証事業を実施した。本実証に関連して、SSDF に関する米国取組の動向を調査し、概観を整理した。整理結果を下図に示す。

図に記載のとおり、SSDF は、2021 年 5 月の大統領令 14028「Improving the Nation's Cybersecurity」に基づき作成された。その後、OMB の覚書 M-22-18 及び M-23-16 において、政府機関が調達するソフトウェアについて、ソフトウェアベンダーにおける SSDF 実装の自己適合証明を確認することが要求された。本自己適合証明にあたっては、2024 年 3 月に、CISA より共通フォームが発表されている。

SSDF には様々な展開が存在し、例えば、NIST より、CI/CD パイプラインにおいて推奨されるタスクを SSDF プラクティスとマッピングしたガイドが発表されているほか、生成 AI モデルとデュアルユース基盤開発のための SSDF プラクティス例が NIST SP 800-218A にて示されている。加えて、調達者視点では、SSDF に則って開発されたソフトウェアの調達に向けたガイドが CISA(ICT SCRM Task Force)より発表されている。

SSDF に基づく国際的な取組としては、2023 年 5 月の QUAD Cybersecurity Partnership において、SSDF に類する 4 つのプラクティスに基づく実践を政府方針に取り入れることが合意され、上述のとおり、2024 年 9 月のウィルミントン宣言において、本合意に立脚しつつサイバー強じん性を向上させることが宣言された。

上述のとおり、2025 年 1 月の大統領令 14144「Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity」において、SSDF の更新が指示され

ているほか、SSDF 更新結果を踏まえ、OMB 覚書を更新することが指示されている。

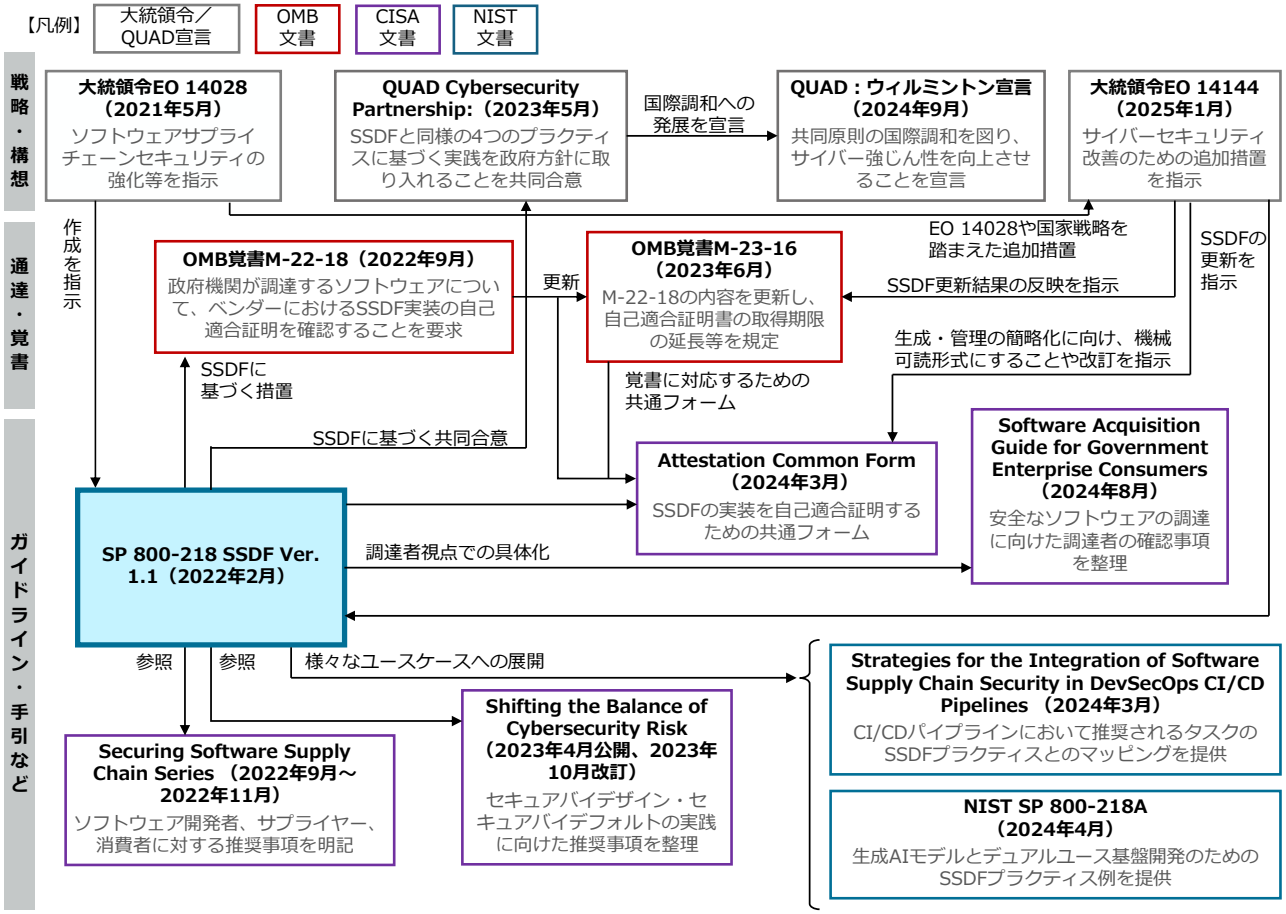
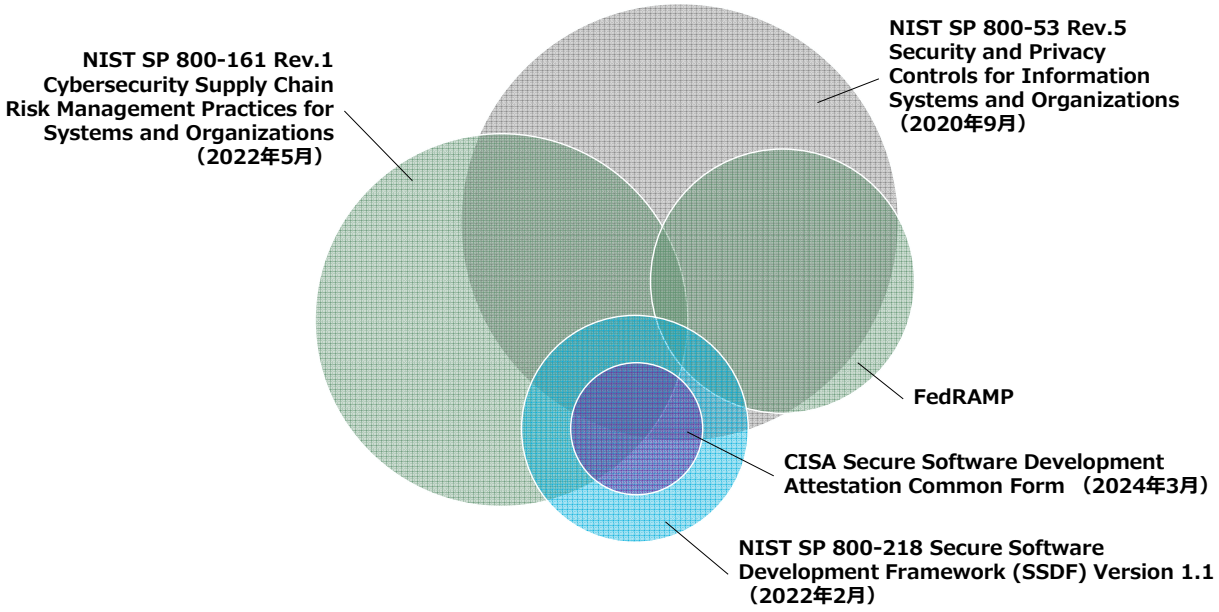


図 2-3 SSDF に関連する米国の取組の俯瞰図

SSDF と関連する NIST 文書等の包含関係は下図のように示される。NIST SP 800-53 は網羅的な管理策を示している一方で、SSDF の対象範囲はあくまでソフトウェア開発に関する内容のみであり、その対象範囲は SP 800-53 と比較すると限定的である。ただし、OMB 覚書によって、政府調達ソフトウェアのベンダーが対応する必要がある CISA の「Attestation Form」で求められる項目は、いずれも SSDF がカバーしていることに留意したい。



出所）ICT SCRM Task Force, “Software Acquisition Guide for Government Enterprise Consumers: Software Assurance in the Cyber-Supply Chain Risk Management (C-SCRM) Lifecycle”に基づき三菱総合研究所作成

図 2-4 SSDF と他の NIST 文書等要件との包含関係

2.3 SBOM の導入に関する手引の改定に向けた業務

「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引」の ver2.0 への改定に向け、パブリックコメントで得られた意見に基づく修正対応等を実施した。パブリックコメントの実施概要と主な意見は以下のとおりである。

表 2-8 SBOM 導入手引 ver2.0 に関するパブリックコメント実施概要・主な意見のカテゴリー

実施期間	2024 年 4 月 26 日 ～ 2024 年 5 月 27 日
意見数	100 件（20 者）
頂いた主な御意見のカテゴリー	① 背景と目的 ② SBOM の概要 ③ 3.～6. SBOM 導入における実施事項・認識しておくべきポイント ④ 7.脆弱性管理プロセスの具体化 ⑤ 8.SBOM 対応モデル ⑥ 9.SBOM 取引モデル ⑦ 全体

パブリックコメントで寄せられた代表的な意見と、それらに対する対応の考え方は下表に示すとおりである。本対応方針を踏まえつつ、手引 ver2.0（案）を作成のうえ、第 13 回ソフトウェアタスクフォースでの議論を以て、2024 年 8 月 29 日に ver2.0 を正式公開した[18]。

[18] https://www.meti.go.jp/press/2024/08/20240829001/20240829001.html

頂いた主な意見のカテゴリー	頂いた主な意見	意見への対応の考え方
1. 背景と目的	消費者視点での SBOM の必要性について触れるべきである。	消費者保護に関する重要性を追記する。
2. SBOM の概要	SBOM の例において、依存関係は番号ではなくコンポーネント名で示すべきである。	コンポーネント名に基づく依存関係に修正する。
	SBOM にはセキュリティ管理だけでなく、ライセンス管理や輸出管理のメリットがあるが、観点が異なる。SBOM が必要以上に肥大化して運用が手間になる可能性もある。	SBOM の全てのメリットを享受しようとするとかえって運用が手間になる可能性を踏まえ、SBOM 導入の目的を踏まえて、具体的な運用方法を検討する重要性を明記する。
	クラウドサービスに対する SBOM が議論されているが、クラウド環境特有の課題も存在する。	クラウド環境特有の SBOM の課題を追記する。
	SBOM の公開は、製品のセキュリティだけでなく、知財に対するリスクをもたらす可能性があることを強調すべきである。	SBOM に専有情報が含まれる場合、適切な管理が必要であることを明記する。
3. ～ 6. SBOM 導入における実施事項・認識しておくべきポイント	SBOM ツールにより実現できることについて、どの機能で実現できるのかを明記すべきである。	対象機能が限定される記載については、対象となる SBOM ツールの機能を補足する。
	サプライチェーン上でのコンポーネントの書き換えや改ざんを把握するために、SBOM を突合することの重要性に言及すべきである。	サプライヤーから SBOM とソフトウェアを受け取る場合の整合性確認に関する記述を追記する。
7.脆弱性管理プロセスの具体化	脆弱性特定を繰り返し行う際に、過去に対応済の脆弱性や優先付けの情報の管理が重要である。	脆弱性対応に関する情報管理については、VEX 活用や SBOM ツールの向上を通じて実施することの重要性を記載する。
	部品 ID 標準に対応しない SBOM については、部品名、ベンダー名によるあいまい検索が必要。	部品 ID の非統一の課題を挙げ、部品名、ベンダー名による部分マッチングによる現実解を挙げる。
	サプライヤーが脆弱性管理を保証する限り、SBOM は不要ではないか。	サプライヤーに依存せず脆弱性を特定することを目的に SBOM を取得することも有効であることを示す。
	脆弱性管理プロセスに、脆弱性マッチング結果の検証を入れることが望ましい。	脆弱性マッチング結果の検証、検証結果の通知について説明を追加する。
	脆弱性対応プロセスに基づくケーススタディの追加が望ましい。	事例依存のデータや機微情報を含むため、現状版ではケーススタディの追加は

頂いた主な意見のカテゴリー	頂いた主な意見	意見への対応の考え方
		見送る。
	(2)表 7-2「脆弱性対応優先付けに必要な情報一覧」と、(3)「組織カテゴリーごとの優先付け判断方法」の関係の解説があるとよい。	表 7-2 と表 7-3 の関係と位置づけを示す。
7.脆弱性管理プロセスの具体化	セキュリティ・バイ・デザインを実施済のソフトウェアは、SBOM 管理の対象外とする。	SBD 実施済でも、脆弱性管理の必要性があること、SBD と SBOM の併用の考え方もあるため、現状版のままとする。
8.SBOM対応モデル	調達者の SBOM 要求が、供給者の過剰な負担とならないように基準を確立すべき。	調達者の SBOM 要求は、調達者が対価を負担するなど供給者に過度な負担とならない仕組みが期待されることを明記する。
	著作権管理、輸出管理、ライセンス管理、特許管理のプロセスと、SBOM 管理を統合することを示唆する。	SBOM 用途の箇所に追記する。
	SBOM は脆弱性管理よりも、資産管理のソリューションではないか。	SBOM の活用範囲として、脆弱性管理、ライセンス管理、資産管理を挙げているため、現状版のままとする。
	金融分野の PCI-DSS や PCI-SSF など、SBOM 観点の留意事項、関連動向の解説の追加は可能か。	実証分野として、金融は含んでいないため、金融分野のみの追加は現状版では見送る。(実証分野については記載済)
9.SBOM取引モデル	提供側と利用側の二者間の債務定義と合意形成、透明化の仕組みが期待される。	合意形成等に関しては、重要な課題であり今後の課題とする。
	サプライヤーが脆弱性情報を提供する場合、SBOM の取得は不要ではないか。	SBOM を活用して、サプライヤーに依存せず脆弱性を特定することも有効であるため、改訂なしとする。
全体	手引の位置づけや SBOM 導入を進めることを「期待する」主体を明確化すべきである。	経済産業省が発行しているため、経済産業省が「期待する」ことの主体となる。
	文書を内容に応じて分割した方が良いのではないか。	章の間で、情報の依存関係があるため、この版では分割なしとする。
	パブコメ以外にも、産業界や企業の意見を取り入れる必要がある。	6 つの実システムを対象とした実証や、委員会形式で民間企業の意見に対して改訂を行っている。
	サプライチェーンを通じたコスト負担、最適化、OSS 管理の効率化などについて継続的な検討が重要。	重要な課題として、中長期の課題として取組む。

頂いた主な意見のカテゴリー	頂いた主な意見	意見への対応の考え方
	・ 最近にリリースされた SPDX 3.0 や CycloneDX 1.6 についても言及すべきである。 ・ SDPX は、2.3 までは「Software Package Data Exchange」の略称であったが、3.0 では「System Package Data Exchange」の略称として扱われているため、修正すべきである。	・ SPDX 3.0 や CycloneDX 1.6 のリリースに関する情報を追記する。 ・ SPDX の正式名称に関する補足説明を追記する。 ・ フォーマットは今後も継続的にアップデートされることが予想されるため、最新バージョンの把握が望まれることを追記する。

3. ソフトウェア開発手法の実践に向けた調査・実証

3.1 安全なソフトウェア開発手法の実践に関する調査・整理

3.1.1 SSDF の概要

2022 年 2 月、NIST は、ソフトウェアの脆弱性を軽減するためのソフトウェア開発者向けの手法をまとめたフレームワークである SSDF（Secure Software Development Framework）の Ver. 1.1 を公開。

各手法は 4 つに分類され、手法を実践するためのタスクが体系化。各手法の実践により、脆弱性を低減するとともに、未対処の脆弱性が悪用された場合の影響を軽減し、脆弱性の再発を防ぐ根本原因に対処可能。

また、大統領令の記載事項と SSDF の手法との対応関係を整理。大統領令の記載事項に対処するために、SSDF を活用可能であるとしている。

表 3-1 セキュアなソフトウェアを開発するための手法をまとめたフレームワーク（SSDF）

分類	手法
1. 組織の準備（PO） ソフトウェアを開発する組織は、組織レベルで安全なソフトウェアの開発を行うために、適した人材、プロセス、技術を準備する必要がある。	• ソフトウェア開発におけるセキュリティ要件を定義する（PO.1） • ソフトウェア開発における役割と責任を明確化する（PO.2） • ソフトウェア開発を支援するツールチェーンを明確化する（PO.3） • ソフトウェアのセキュリティを確認するための基準を定義し、活用する（PO.4） • ソフトウェア開発のための安全な環境を導入し、維持する（PO.5）
2. ソフトウェアの保護（PS） ソフトウェアを開発する組織は、ソフトウェアのすべてのコンポーネントを、改ざんや不正アクセスから保護する必要がある。	• あらゆる形態のコードを不正アクセスや改ざんから保護する（PS.1） • ソフトウェアリリースの完全性を検証する仕組みを提供する（PS.2） • 各ソフトウェアのリリースをアーカイブ化し、保護する（PS.3）
3. 安全なソフトウェアの開発（PW） ソフトウェアを開発する組織は、脆弱性を最小限に抑え、十分なソフトウェアを備えたソフトウェアをリリースする必要がある。	• セキュリティ要件を満足するとともにセキュリティリスクを軽減できるよう、ソフトウェアを設計する（PW.1） • ソフトウェア設計をレビューし、セキュリティ要件やリスクへの適合性を検証する（PW.2） • 実現可能な場合、機能を重複させずに既存の保護されたソフトウェアを再利用する（PW.4） • セキュアコーディングのプラクティスを遵守してソースコードを作成する（PW.5） • 実行可能なセキュリティを向上させるために、コンパイル、インタプリター及びビルドプロセスを構築する（PW.6） • コードをレビュー・分析することで、脆弱性を特定し、セキュリティ要求事項への準拠を検証する（PW.7） • 実行コードをテストして脆弱性を特定し、セキュリティ要求事項への準拠を検証する（PW.8） • ソフトウェアをデフォルトで安全な設定とする（PW.9）
4. 脆弱性への対応（RV） ソフトウェアを開発する組織は、リリースするソフトウェアに残存する脆弱性を特定し、適切に対応する必要がある。	• 脆弱性に対する継続的な把握と確認を実施する（RV.1） • 脆弱性の評価、優先順位付け及び修正を実施する（RV.2） • 脆弱性を分析することで、その根本原因を特定する（RV.3）

※ PW.3 は PW.4 の手法に統合されたため、定義されていないことに留意。また、PS.3 のタスクの一つとして、SBOM 等を用いたコンポーネントリストの生成・維持・共有に関するタスクが含まれている。

出所）NIST, SP 800-218 Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf

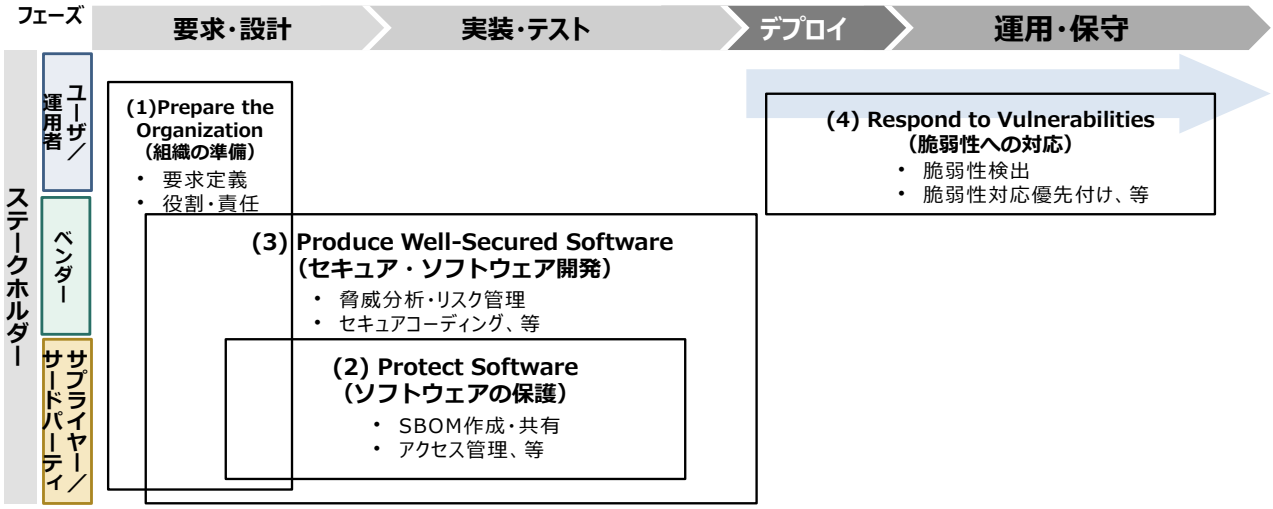


図 3-1 ライフサイクルプロセス全体における SSDF のスコープ

SSDF のプラクティスの構成は、下記のとおりタスクにブレークダウンされ、実装例と参考文献と対応付けられる。

プラクティス(実践項目)	タスク(要件)	実装例（手法・プロセス等）	参考文献
Practices	**Tasks**	**Notional Implementation Examples**	**References**
Provide a **Mechanism for Verifying Software Release Integrity (PS.2)**: Help software acquirers ensure that the software they acquire is legitimate and has not been tampered with.	**PS.2.1**: Make software integrity verification information available to software acquirers.	**Example 1**: Post cryptographic hashes for release files on a well-secured website. **Example 2**: Use an established certificate authority for code signing so that consumers' operating systems or other tools and services can confirm the validity of signatures before use. **Example 3**: Periodically review the code signing processes, including certificate renewal, rotation, revocation, and protection.	**BSAFSS**: SM.4, SM.5, SM.6 **BSIMM**: SE2.4 **CNCFSSCP**: Securing Deployments—Verification **EO14028**: 4e(iii), 4e(ix), 4e(x) **IEC62443**: SM-6, SM-8, SUM-4 **NISTCSF**: PR.DS-6 **NISTLABEL**: 2.2.2.4 **OWASPSAMM**: OE3-B **OWASPSCVS**: 4 **PCISSLC**: 6.1, 6.2 **SCSIC**: Vendor Software Delivery Integrity Controls **SP80053**: SA-8 **SP800161**: SA-8 **SP800181**: K0178
Archive and Protect Each Software Release (PS.3): Preserve software releases in order to help identify, analyze, and eliminate vulnerabilities discovered in the software after release.	**PS.3.1**: Securely archive the necessary files and supporting data (e.g., integrity verification information, provenance data) to be retained for each software release.	**Example 1**: Store the release files, associated images, etc. in repositories following the organization's established policy. Allow read-only access to them by necessary personnel and no access by anyone else. **Example 2**: Store and protect release integrity verification information and provenance data, such as by keeping it in a separate location from the release files or by signing the data.	**BSAFSS**: PD.1-5, DE.1-2, IA.2 **CNCFSSCP**: Securing Artefacts—Automation, Controlled Environments, Encryption; Securing Deployments—Verification **EO14028**: 4e(iii), 4e(vii), 4e(ix), 4e(x) **IDASOAR**: 25 **IEC62443**: SM-6, SM-7 **NISTCSF**: PR.IP-4 **OWASPSCVS**: 1, 3.18, 3.19, 6.3 **PCISSLC**: 5.2, 6.1, 6.2 **SCSIC**: Vendor Software Delivery Integrity Controls **SP80053**: SA-10, SA-15, SA-15(11), SR-4 **SP800161**: SA-8, SA-10, SA-15(11), SR-4
	PS.3.2: Collect, safeguard, maintain, and share provenance data for all components of each software release (e.g., in a software bill of materials [SBOM]).	**Example 1**: Make the provenance data available to software acquirers in accordance with the organization's policies, preferably using standards-based formats. **Example 2**: Make the provenance data available to the organization's operations and response teams to aid them in mitigating software vulnerabilities. **Example 3**: Protect the integrity of provenance data, and provide a way for recipients to verify provenance data integrity. **Example 4**: Update the provenance data every time any of the software's components are updated.	**BSAFSS**: SM.2 **BSIMM**: SE3.6 **CNCFSSCP**: Securing Materials—Verification, Automation **EO14028**: 4e(vi), 4e(vii), 4e(ix), 4e(x) **NTIASBOM**: All **OWASPSCVS**: 1.4, 2 **SCSIC**: Vendor Software Delivery Integrity Controls **SCTPC**: MAINTAIN3 **SP80053**: SA-8, SR-3, SR-4 **SP800161**: SA-8, SR-3, SR-4
QUAD内で共通項目として期待されると想定		実装例。必要に応じて各国の検討が求められる。	タスクに対する確立された手法の文献例。必要に応じて各国の検討が求められる。

3.1.2 ガイドラインのマッピング

以下「表 2.2.8-1 マッピング対象の国内ガイドライン」に示す 7 つの国内ガイドラインの各項目について、SSDF タスクの内容にどの程度適合しているのかマッピング調査を実施した。

表 2.2.8-1 マッピング対象の国内ガイドライン

No	国内ガイドライン	出典
1	SBOM 導入手引 Ver.1.0, Ver.2.0	経産省（METI）
2	情報システムにおけるセキュリティコントロールガイドライン	Software-ISAC
3	政府情報システムにおけるセキュリティ・バイ・デザインガイドライン	デジタル庁
4	サイバーセキュリティ経営ガイドライン	経産省（METI）
5	政府機関等のサイバーセキュリティ対策のための統一基準群	内閣サイバーセキュリティセンター（NISC）
6	サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）	経産省（METI）
7	クラウドサービス提供における情報セキュリティ対策ガイドライン	総務省（MIC）

これらガイドラインのマッピング結果は以下「図 2.2.8-2 国内ガイドラインのマッピング結果」のとおりであり、SSDF のタスクを全て網羅するガイドラインはないという結果であった。しかしながら、各ガイドラインについて部分的に SSDF タスクを満たしている項目はあるため、これらガイドラインに準拠していれば、一から SSDF タスクに対応するのではなく、SSDFタスクに対する不足項目について対応することでセキュア・ソフトウェア開発の要件を満たすことが可能と考えられる。

3.1.3 ガイドラインマッピング表の改訂

マッピングするにあたり、国内ガイドラインに使用されているキーワードの読み替えを行っている（解釈を変換している）部分がある。これは国内ガイドラインが特定のサービス（例えばクラウドサービスの提供など）に関する内容を含んでおり、それらに関連したキーワードでガイドラインが作成されているため、そのままの表現・内容ではマッピングが難しいためである。

（キーワードの読み替え例）

国内ガイドライン： クラウドサービス提供における情報セキュリティ対策ガイドライン（MIC）

読み替え対象キーワード	読み替え後のキーワード
クラウドサービス事業者	ソフトウェア開発元、開発主体
クラウドサービス利用者	ソフトウェア調達・利用者
サプライチェーン（クラウドサービス提供者）	サードパーティ
（クラウド）サービス	ソフトウェア
システム	ソフトウェア（コンポーネント）
アプリケーション	ソフトウェア（コンポーネント）

ガイドライン内容の読み替え例：（ガイドライン項目）Ⅱ．3．1．1.【基本】リスク対策と文書化

読み替え前の内容	読み替え後の内容
サプライチェーン事業者が提供するクラウドサービスについて、事業者間で合意された情報セキュリティリスク対策及びサービスレベルを文書化するとともに、サプライチェーン事業者に	サードパーティソフトベンダーが提供するソフトウェアについて、サードパーティソフトベンダー間で合意された情報セキュリティリスク対策及びソフトウェア（品質）レベルを文書化するととも

よって確実に実施されることを担保すること。	に、サードパーティソフトベンダーによって確実に実施されることを担保すること。

上記の例のような読み替えを行うことでガイドラインが本来意図している内容と異なる解釈となっている可能性がある。よって、実際の開発プロジェクトにおいてガイドラインマッピング表の包含関係を参考に SSDF タスクへの対応を行った場合、すでに対応済みと想定されるタスク項目であっても実際は対応が不完全である可能性があり、想定していたタスク対応に必要な内容について、大きなギャップがあるかもしれない。よって、ガイドラインマッピングの表における包含関係に関しては今後も定期的に見直しをかけていく必要があると考えられる。

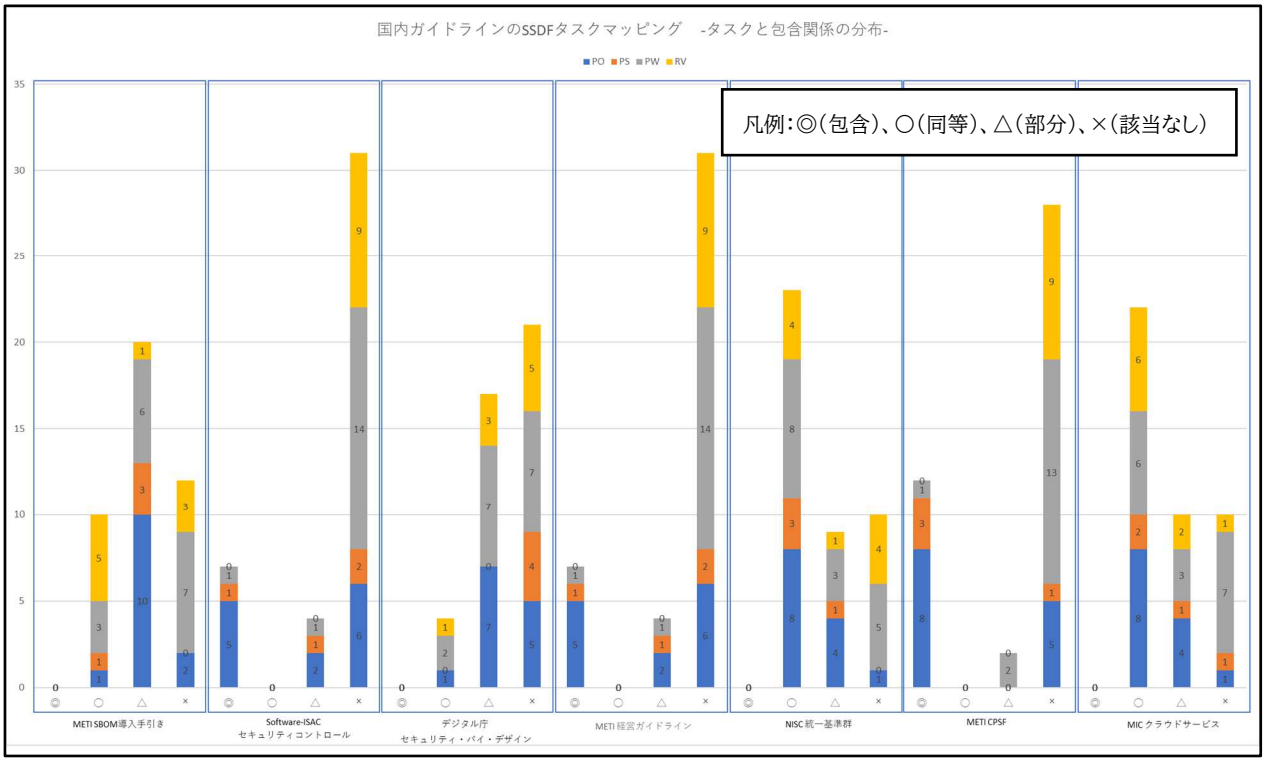


図 2.2.8-2 国内ガイドラインのマッピング結果

- SBOM 導入手引 Ver.1.0, Ver.2.0 に関するマッピング結果
- 情報システムにおけるセキュリティコントロールガイドラインに関するマッピング結果
- 政府情報システムにおけるセキュリティ・バイ・デザインガイドラインに関するマッピング結果
- サイバーセキュリティ経営ガイドラインに関するマッピング結果
- 政府機関等のサイバーセキュリティ対策のための統一基準群に関するマッピング結果

本ガイドラインでは SSDF タスク総数 42 件に対して、23 件は同等と想定されるガイドライン項目があり、半数以上の SSDF タスクを満たしている状況にあると考えられる。残りの 19 件については部分的な対応のガイドライン項目もしくは該当するガイドライン項目がない状況にあり、これらについては該当する SSDF タスクに対応していく必要がある。
本カイドラインは他のガイドラインと比較して、SSDF タスクに対する不足項目は少なく、セキュア・ソフトウェア開発のベースとなる組織の準備（PO）タスクの不足項目も少ないことから、本ガイドラインに準拠していれば比較的スムーズに SSDF タスクへの対応が可能なのではないかと想定される。ただし、本ガイドラインはソフトウェア開発を主眼においたガイドラインではないため、SSDF タスクへの対応にあたっては SSDF タスクの項目と同等と想定されるガイドライン項目を含め、各項目についてその妥当性を確認・検証する必要がある。

- サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）に関するマッピング結果

- クラウドサービス提供における情報セキュリティ対策ガイドライン（MIC）に関するマッピング結果
本ガイドラインでは SSDF タスク総数 42 件に対して、22 件は同等と想定されるガイドライン項目があり、半数以上の SSDF タスクを満たしている状況にあると考えられる。残りの 20 件については部分的な対応のガイドライン項目もしくは該当するガイドライン項目がない状況にあり、これらについては該当する SSDF タスクに対応していく必要がある。
本カイドラインは他のガイドラインと比較して、SSDF タスクに対する不足項目は少なく、セキュア・ソフトウェア開発のベースとなる組織の準備（PO）タスクの不足項目も少ないことから、本ガイドラインに準拠していれば SSDF タスクへの対応も比較的スムーズにできるのではないかと想定される。ただし、本ガイドラインはソフトウェア開発を主眼においたガイドラインではないため、SSDF タスクへの対応にあたっては SSDF タスクの項目と同等と想定されるガイドライン項目を含め、各項目についてその妥当性を確認・検証する必要がある。

3.1.4 海外における SSDF 導入実態に関するヒアリング調査

（1） 主旨

様々な分野でサイバーセキュリティを確保する上で、情報システムや機器に組み込まれるソフトウェアのセキュア開発の重要性が認識されてきている。QUAD4 カ国共同原則においては、政府調達におけるセキュア・ソフトウェア開発プラクティスの導入について合意されている。NIST SSDF（Secure Software Development Framework）は、今後のセキュア開発において、そのベースとして重要になると考えられる。一方で、中小企業や産業分野によっては、SSDF 導入には困難や課題があると想定される。本ヒアリングでは、セキュア開発や SSDF への取組み状況についてご確認させて頂くとともに、サプライチェーンを通じた対応の困難や課題、現実的な対応ステップなどについてご意見を聴取し、今後整理する SSDF への対応ガイドの参考とする。

（2）ヒアリング項目

1）セキュア・ソフトウェア開発に関する取組み状況

以下の開発フェーズで、重点的に対応している事項、対応が十分ではない事項の内容について。
①プロセス・環境構築、②要件定義・設計、③実装テスト、④運用保守・脆弱性対応
組織の先進的な取組にどのようなものがあるか。

2）SSDF への対応状況（自己適合証明を含む）

貴組織の SSDF 対応状況の段階・レベルについて。レベル分けの必要性。
①調査・準備段階、②試行導入、③実践導入、④委託先への展開
重要と考えられる Task やそれに対応する実装例、参考文献の要求事項の主な例はどうか。
OMB の自己適合証明への対応状況はどうか
業界における SSDF の取組状況や関連する統計データはあるか。

3）セキュア・ソフトウェア開発や SSDF への取組みにおける課題・困難

セキュア・ソフトウェア開発への取組みにおける課題・困難はあるか。
SSDF への取組みにおける課題・困難にどのようなものがあるか。
自社内の取組における困難とサプライチェーンを通じた委託先における困難とその違いはあるか。

4）今後の取組みの方向性

SSDF について、今後、重点化を予定する領域（SSDF Practice、Task）にどのようなものがあるか。
サプライヤー、委託先、中小企業などにおいて認識される課題・困難と解決策にどのようなものがあるか。

5）国の取組やガイダンスに対する要望

SSDF 実証において評価すべき事項はあるか。
SSDF Task と国内ガイドラインのマッピングに関して期待するものはあるか。
SSDF 対応についてガイダンスをまとめるとすれば、要望はあるか。

3.2 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

3.2.1 背景と問題認識

SSDF 活用のための考え方等をまとめた国内事業者向けの文書(ガイドライン等)を策定するとともに、自己適合宣言の仕組みを構築し、政府調達等へ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。

今年度は、SSDF と国内ガイドラインのマッピング、実ソフトウェアに対する実証等を通じて、国内ガイドラインの不足事項や課題・対応方法の具体化等について整理し、国内事業者向けの文書(ガイドライン等)の初版案を作成。

来年度以降は、残課題の整理・対応、国内事業者向けの文書の初版案の成案化、初版改訂に向けた検討と改訂案策定、自己適合宣言の仕組みの検討・構築、政府調達等への要件化などを検討。

今年度実施予定の内容		来年度以降実施予定の内容
• SSDFと国内ガイドラインの対応関係を示すマッピング • マッピング表を用いたSSDF活用方法・対応フローの整理 • 実ソフトウェアに対する実証、課題・対応方法の具体化等の整理 • 国内ガイドラインの不足事項の明確化と対応方針案の検討 • 事業者のSSDF自己適合宣言文書作成に関する参考情報等の提示、など	<成果物例> 国内事業者向け文書(ガイドライン等)の初版案 • SSDFと国内ガイドラインのマッピング表 • SSDF活用の考え方等をまとめた文書 ✓ マッピング表を用いたSSDF活用方法 ✓ 課題・対応方法の具体的内容 ✓ 国内ガイドラインにおける不足事項・対応方針案 ✓ 事業者のSSDF自己適合宣言文書作成に関する参考情報、など	• 残課題(不足項目の対応方法の更なる具体化等)への対応 • 国内事業者向け文書の初版案の成案化 • 初版改訂に向けた検討と改訂案作成 • 自己適合宣言の仕組み検討・構築 • 政府調達等への要件化の検討、 など

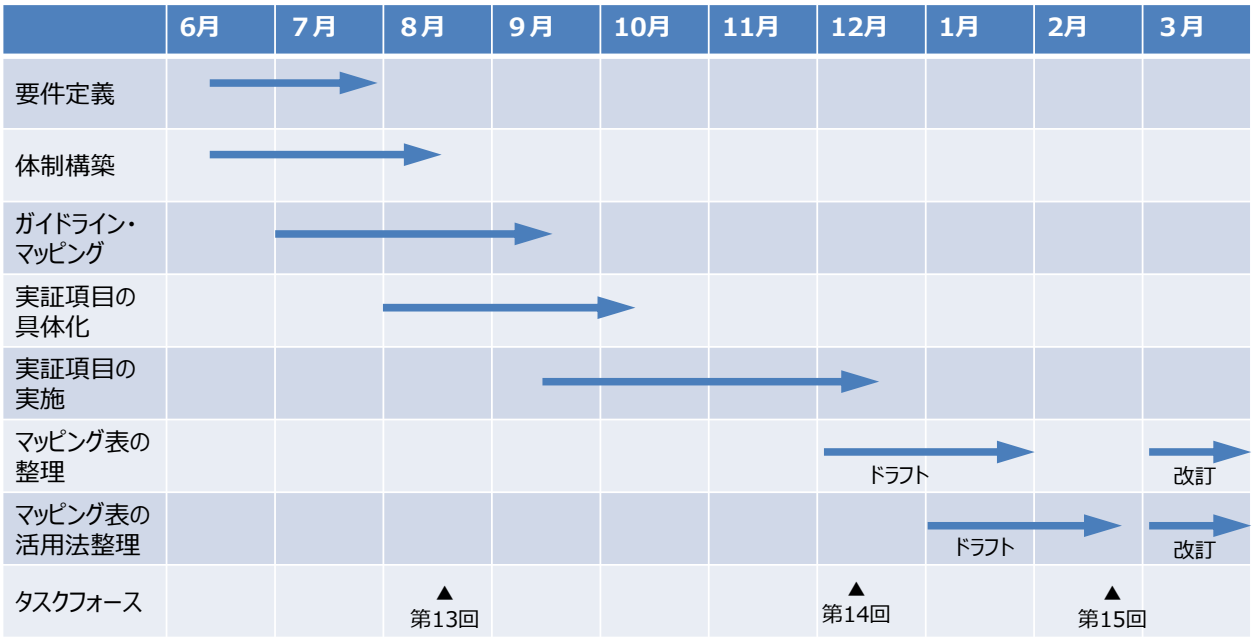
国内外で多数のセキュリティガイドライン、基準等が存在し、複数分野の事業、国際展開を行う事業者にとって、様々な基準において重複する部分の効率的な対応が期待される。

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。

3.2.2 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。



3.2.3 実証対象システム

実証対象システムは製品に含まれるソフトウェアコンポーネントやそのライセンス、ソフトウェアコンポーネント間の依存関係を一覧化したソフトウェア部品表（以下、SBOM）を管理する「SBOM.JP」システムである。

本システムの全体構成概要とそのソフトウェア開発範囲を以下「図 2.2.7-1 SBOM.JP システム全体像と開発範囲」に示す。

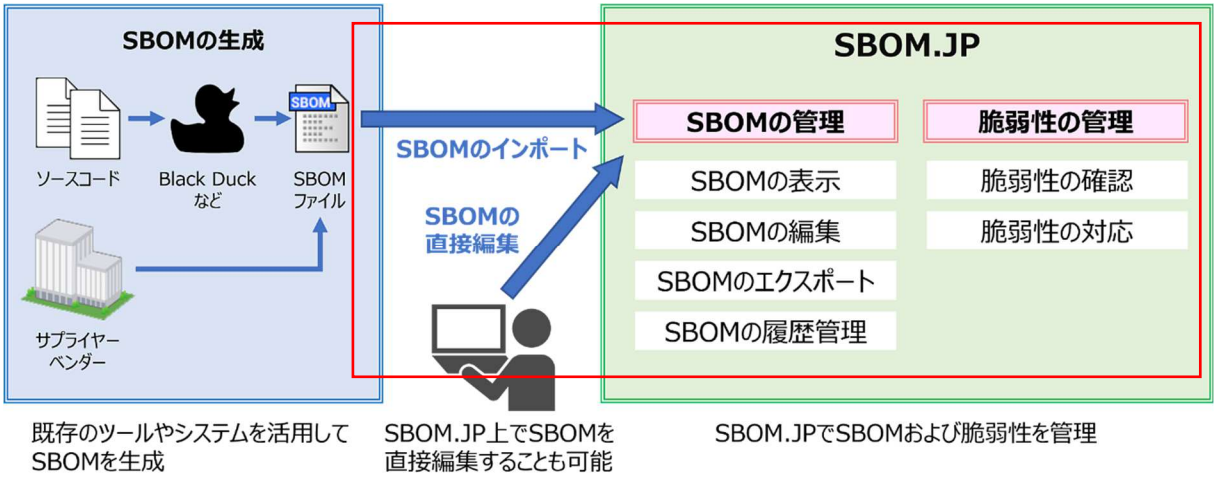


図 2.2.7-1 SBOM.JP システム全体像と開発範囲

上記赤枠の部分が本システムのソフトウェア開発範囲となる。本開発を通して SSDF 全 42 タスクについて、どの程度対応できているのか検証し、検証の結果として得られた知見や問題点、課題について

整理する。

3.2.4 達成基準の定義

達成基準は、基本的な考え方を示す指針とそれに対応する具体例に分けて定義する。

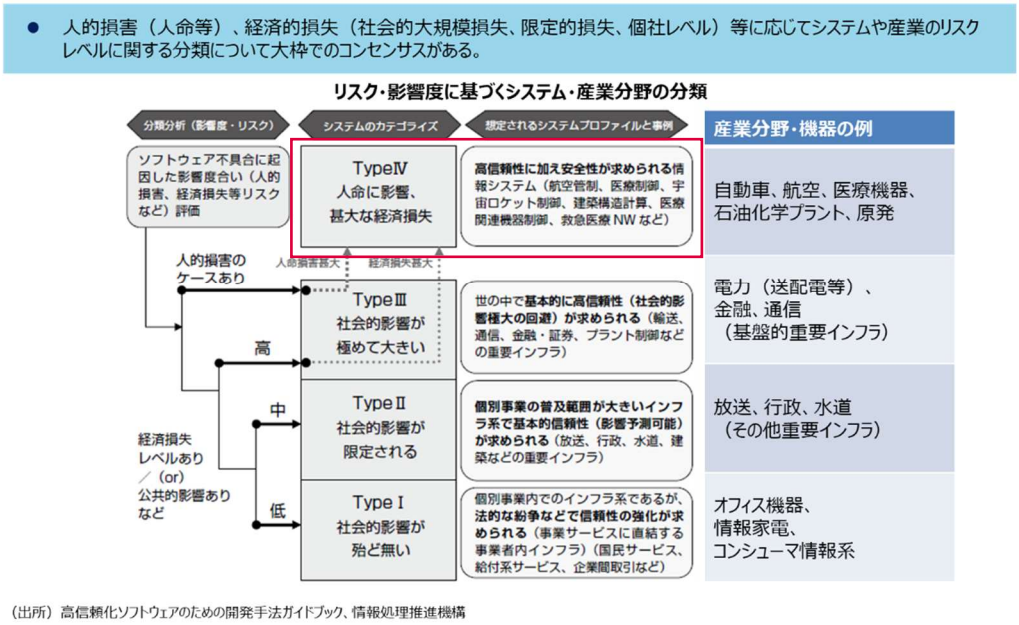
- 指針

  SSDF タスクの達成度を測るために達成レベルを定義する。達成レベルは 3 段階とする。

  タスクの達成において最も本質的な重要事項、影響の大きい事項は複数の観点(軸)が考えられるが、それらの組合せを全て考慮すると、レベルは多段階に発散するため、全ての軸のいずれか 1 つでも満たすかそれ以外かの 2 分類としてレベル 1、レベル 2 の分類を行う。

  レベル 2 以上については、※高信頼化ソフトウェアのシステムカテゴリ TypeIV(人命に影響等)に求められる特別高度な対策が求められる場合をレベル 3 とする。

【参考】リスク・影響度に基づくシステム・産業分野の分類



（出所）高信頼化ソフトウェアのための開発手法ガイドブック、情報処理推進機構

※【参考】リスク・影響度に基づくシステム・産業分野の分類

達成レベルの考え方とその定義について、以下「表 2.2.9-1 タスクの達成レベルの考え方とその定義」に示す。

表 3.2.9-1 タスクの達成レベルの考え方とその定義

レベル	実施事項の網羅性	属人性/再現性	プロセス成熟度・最適化	備考
0	最低限に達していない	属人的	最低限に達していない	最低限に達していない。
1	最低限	属人的	最低限の管理	最低限の Task 内容を実施している。

2	網羅的	標準化・体系化されている。	定量管理可能	十分な対応ができている。
3	網羅的＋高度	自動化	最適化可能・改善済	特別高度な対応ができている。

達成レベル定義の例として、SSDF のタスク「PO.1.2：ソフトウェアのセキュリティ要件定義」について、以下「表 2.2.9-2 SSDF タスク PO.1.2 に対する達成レベル定義」に示す。

表 3.2.9-2　SSDF タスク PO.1.2 に対する達成レベル定義

達成レベル	定義
1	対象ソフトのアーキテクチャなどの設計開発段階の基礎的なセキュリティ要件を定義・文書化している。（設計開発段階の基礎的なセキュリティ要件定義）
2	レベル 1 に加え、ソフトウェアの運用・保守段階を含む体系的なセキュリティ要件を定義・文書化している。（運用保守段階を含む、SDLC 全体のセキュリティ要求定義）
3	ポリシーの見直しタイミングなどで継続的にポリシーの改善・最適化を図る。（ポリシーの見直しに基づく継続的なセキュリティ要件の最適化）

- 具体例
  SSDF タスクの実装例を具体化した例及び実証内容で示す具体的なアウトプット・活動を洗い出し、それらを達成レベル 1～3 に対応して列挙することで、一般の開発者が具体的にイメージできる内容を示す。列挙された具体例は、あくまで例示であり、達成レベル 1～3 を厳格に分類するものではない。各達成レベルで満たすべき具体例については、個社の事情や環境によって硬直的な判断に陥らないよう、固定的に決めるのではなく、最低限満たすべき具体例と列挙された全ての具体例のうち、満たすべき具体例の件数のみ指定し、どの具体例を満たすかはタスク実施者が選択可能とすることによって柔軟性を持った基準とする。

達成レベルに対応した具体例の例として、SSDF のタスク「PO.1.2：ソフトウェアのセキュリティ要件定義」について、以下「表 2.2.9-3 SSDF タスク PO.1.2 の達成レベルに対応した具体例」に示す。

表 3.2.9-3　SSDF タスク PO.1.2 の達成レベルに対応した具体例

達成レベル	具体例
1	ソフトウェアのセキュリティ要件定義に関して、内製のソフトウェアに対して、以下の項目を満たしていること。 ■開発ソフトウェアのセキュリティ要件定義 開発ソフトウェアのセキュリティ要件の資料や文書がある。 [対応必須]★の項目は満たしていること。 [開発ケース毎に選択]▲の項目については必須ではないが、2 つ以上の項目を満たしていることを推奨。

	※以下の例示で同等の対策を実施している場合は、達成度基準としてカウント可能。その場合、同等性の説明が必要。 (1)開発するソフトウェアについての説明がある。例えば以下のような内容が記載されている。 ★①開発するソフトウェアの概要説明 ★②開発するソフトウェアコンポーネント（一覧） ★③ソフトウェアの構成概要 ・構成の概要説明 ・構成図など ▲④開発言語、ツールなどの環境 ・使用する開発言語とツール ・選択肢が複数ある場合、機能比較履歴など ▲⑤使用するサードパーティ製（OSS 含む）ソフトウェアコンポーネント（一覧） ・セキュリティ対応情報（脆弱性、セキュアコーディング対応実績など） ・サポート期間の情報など ★⑥開発スケジュール ・開発期間 ・製品リリース予定日 (2)開発するソフトウェアのセキュリティポリシー・要件が定義されている。例えば以下のような内容が記載されている。 ★①ソフトウェアのセキュリティ確保のための施策・要求事項 ・ソフトウェアやデータ等の暗号/復号化対応 ・データの冗長化対応 ・ソフトウェアやデータの完全性確保対応など ★②セキュリティガイドラインの定義 ・外部のガイドライン（NIST や OWASP など）に準拠するなど ★③(セキュア)コーディングガイドラインの定義 ・外部のコーディングガイドラインを採用する（CERT-C など）など ▲④開発工程毎のセキュリティ関連の実施作業 ・セキュア観点レビュー実施時期の明記 ・静的コード解析実施時期の明記など ▲⑤セキュリティ要件に準拠できない場合の例外処置（逸脱等）に関するプロセス定義 ★⑥製品リリース後のサポート方針 ・サポート期間 ・セキュリティインシデント対応窓口 ・脆弱性情報公開の方針など
2	レベル 1 に加え、[開発ケース毎に選択]▲の項目についても全て満たしていること。
3	レベル 2 に加えて、以下の項目を満たしていること。 ■ソフトウェアのセキュリティ要件の見直しプロセス定義と実施 ソフトウェアのセキュリティ要件見直しプロセスに関する資料や文書があり、実施履歴がある。

	(1)ソフトウェアのセキュリティ要件の見直しプロセスが定義されている。例えば以下のような内容が記載されている。 ★①定期的なソフトウェアのセキュリティ要件見直し ・見直すトリガやタイミング ・見直しに伴う対応など (2)ソフトウェアのセキュリティ要件の見直し実施履歴がある。例えば以下のような資料や情報がある。 ★②ソフトウェアのセキュリティ要件の見直し履歴

3.2.5 実証事項の定義

実証内容は「2.2.9 項 達成基準の定義」で示した各タスクの具体例の内容を参考に定義する。「2.2.9 項 達成基準の定義」で示された各タスクの具体例はタスク実施者が満たすべき具体例について選択可能となっており、柔軟性のある基準としているため、実証内容についても柔軟性をもった内容となっている。このため、列挙された全ての実証内容の項目を満たしているかを検証するのではなく、それぞれ個々の項目毎に達成基準の定義に照らして、必要な内容が満たされているのか検証していくことになる。

上記を踏まえ、実際の「SBOM.JP」システムのソフトウェア開発において、各タスクに定義された実証内容に基づき、どの程度の達成レベルにあるのか実証検証していく。

実証検証は以下の 2 つの検証方法にて実施する。

1. 実践による検証
   ・文書化・資料化等を網羅的に実施してタスク内容を検証。
   ・プログラム等を動作させ、タスク内容を検証。
2. 机上による検証
   ・文書化・資料化等を一部実施してタスク内容を検証。
   ・プログラム等を動作させずにタスク内容を推定検証。

実証内容の具体例として、SSDF のタスク「PO.1.2:ソフトウェアのセキュリティ要件定義」について、以下「表 2.2.10-1 SSDF タスク PO.1.2 の実証内容」に示す。

表 3.2.10-1 SSDF タスク PO.1.2 の実証内容

実証内容
①内製ソフトウェアのセキュリティ要件に関して以下の内容を記載した文書・資料があるかどうか確認する。 【開発ソフトウェア情報】 ・開発するソフトウェアの概要説明 ・開発するソフトウェアコンポーネント（一覧） ・ソフトウェアの構成概要 ・開発環境のセキュリティ要件

-開発に利用する言語

・使用するサードパーティ製（OSS 含む）ソフトウェアコンポーネント（一覧）

・開発スケジュール

【開発ソフトウェアのセキュリティ要件】

・ソフトウェアのセキュリティ要件

-ソフトウェアやデータ等の暗号/復号化対応

-データの冗長化対応

-ソフトウェアやデータの完全性確保対応など

・セキュリティガイドラインの定義

-外部のガイドライン（NIST や OWASP など）に準拠するなど

・(セキュア)コーディングガイドラインの定義

-外部のコーディングガイドラインを採用する（CERT-C など）など

・開発工程毎のセキュリティ関連の実施作業

-セキュア観点レビュー実施時期の明記

-静的コード解析実施時期の明記など

・セキュリティ要件に準拠できない場合の例外処置（逸脱等）に関するプロセス定義

・製品リリース後のサポート方針

-サポート期間

-セキュリティインシデント対応窓口

-脆弱性情報公開の方針など

・脆弱性対応

-対応要件（体制構築やプロセス構築に関して）

・セキュリティ要件の見直しプロセス

など

3.2.6 実証実施

実証事項の定義に従い、実施した内容については、下記の例で示すようにタスクごとに実証結果・成果物、達成度評価、ガイドラインマッピングに関する評価、課題と対応策に分けて整理した。

（1） 組織の準備

1） PO.1.1：開発インフラとプロセスのセキュリティ要件定義

a. 実証結果・成果物

【実践検証（成果物）】

・SBOM.JP ソフトウェア開発計画書

【該当する項目】

2.1.1. 開発プロセス

2.1.2. 開発プロセスのセキュリティ要件

5.1. 開発基盤（インフラ）

5.1.1. ネットワークシステム環境

5.1.2. 開発ベースシステム構成

5.1.3. 開発用サーバ

5.1.4. 開発エンドポイント

以下、開発インフラのセキュリティ要件定義例を「図 PO.1.1-1 開発インフラのセキュリティ要件定義」に示す。

開発拠点は「3. 開発体制」で示したように分散しており、各拠点をインターネットで結び、開発を進めていくことになる。
ここでは開発のネットワークシステム環境について説明する。以下、「図 5.1.1-1 開発ネットワーク構成」を示す。
開発用ネットワークはソフトウェア開発元の社内業務用ネットワーク（社内 LAN）を利用し、構築する。

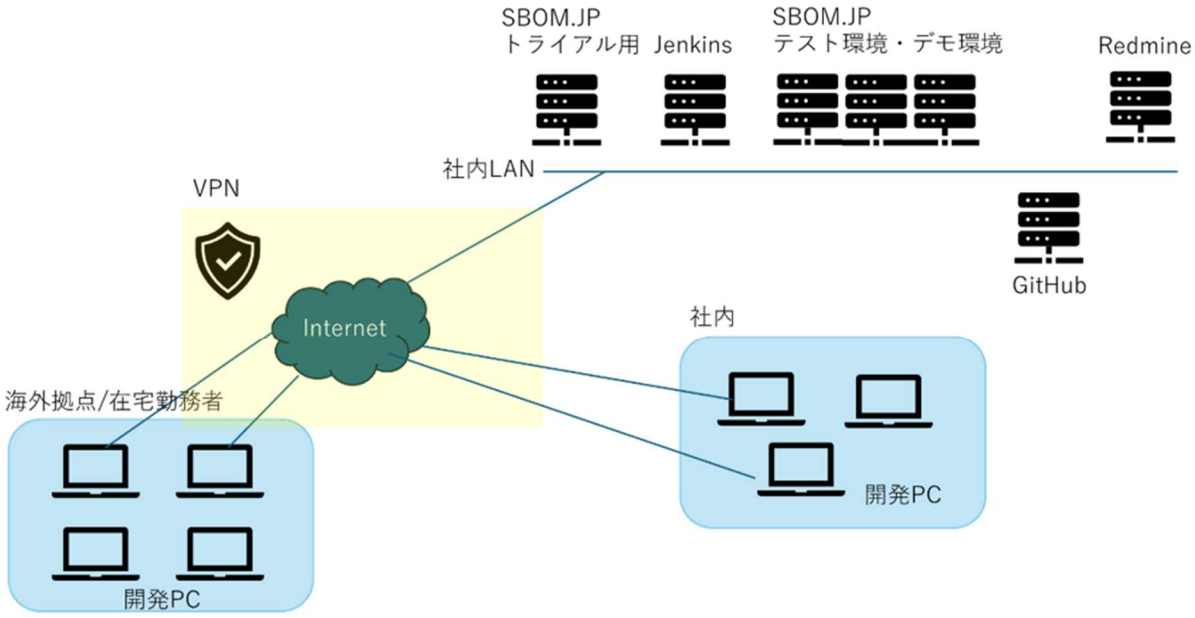


図 5.1.1-1 開発ネットワーク構成

【セキュリティ保護要件】

(1) 通信の盗聴・通信データの改ざん・通信相手のなりすましを防止すること。
(2) 外部からの不正アクセスを防止すること。
(3) 不正アクセスを検知できること。

【セキュリティ保護対策】

(1) セキュリティ保護された社内業務用ネットワーク（社内 LAN）を開発用ネットワークとして利用する。
(2) 各開発拠点からはインターネットを経由して社内業務用ネットワーク（社内 LAN）に接続する。インターネット経由の接続は VPN 接続とし、通信の保護を行う。
(3) 社内業務用ネットワーク（社内 LAN）のセキュリティ保護対策は社内システム管理部門のポリシーに従う。

図 PO.1.1-1 開発インフラのセキュリティ要件定義

また、開発プロセスのセキュリティ要件定義例を「図 PO.1.1-2 開発プロセスのセキュリティ要件定義」に示す。本プロセスに則り、セキュアなソフトウェア開発を実行し、開発ソフトウェアのセキュリティを担保していく。

アジャイル開発プロセスにおいて、開発機能のセキュリティ関連要件がある場合には、以下、「表 2.1.2-1 各開発プロセスフェーズにおけるセキュリティ要件」に示す対応を行う。

表 2.1.2-1 各開発プロセスフェーズにおけるセキュリティ要件

開発プロセスフェーズ	情報管理	対応内容
設計フェーズ（DESIGN）	Redmine(※)チケット発行	機能要件からセキュリティに関する要件の有無を明確化。 セキュリティ要件有の場合、設計に盛り込み、記録。
製造フェーズ（DEVELOP）	GitHub(※)にてコード管理	GitHub にて開発コード管理。開発者は設計時のセキュリティ要件を満たす実装になっているか確認。
テストフェーズ（TEST）	UT にてテスト実行	機能テスト用コード作成・実行。セキュリティ要件に対応したテストを実施できているか確認。
反映・展開フェーズ（DEPLOY）	GitHub にてコード提出・レビュー依頼	テスト OK となったコードを登録し、第三者にレビュー依頼。
レビューフェーズ（REVIEW）	GitHub にてレビュー	レビュー責任者・担当者（第三者）によるレビュー実施。セキュリティ要件を満たしているか確認。問題がある場合、指摘事項とともに開発者に差し戻し。
リリースフェーズ（LAUNCH）	GitHub にてコード正式登録	レビュー結果で OK となったコードは正式登録。システムリリース版に盛り込む。

図 PO.1.1-2 開発プロセスのセキュリティ要件定義

b. 達成度評価（適合性の説明）

レベル 2 相当。理由は以下のとおり。

達成レベル	判定	判定理由概要
1	○	開発基盤とプロセスのセキュリティ要件に関する基本的な情報が文書化されている。
2	○	外製ソフトウェアコンポーネントを含めたソフトウェア開発プロセスのセキュリティ要件定義がされている。本実証検証においては、商用サードパーティ製ソフトウェアを使用しておらず、OSS のみであるため、本タスクでのセキュリティ要件は内製ソフトウェアと同等となる。
3	×	ソフトウェア開発基盤や開発プロセスのセキュリティに関する見直しプロセスは明確には定義されていない。

c. ガイドラインマッピングに関する評価（不足事項）

国内ガイドライン（マッピング対象ガイドライン総数：7 件）とのマッピングでは同等又は包含の関係となっているものが 4 件あり、該当ガイドラインに準拠した開発を行っているケースでは、本 SSDF タスクを満たすことができると考えられるが、マッピング対象ガイドラインはセキュア・ソフトウェア開発に主眼を置いたガイドラインではないため、その妥当性については確認・検証が必要である。

残り 3 件のガイドラインについては一部包含している関係となっており、本 SSDF タスクを満たすに

は不十分な内容となる可能性がある。不足項目となる可能性のある内容は以下のとおり。

【主な不足項目】

・セキュリティ要件について**文書化**すること

凡例:◎(包含)、○(同等)、△(部分)、×(該当なし)

国内ガイドライン	SSDF タスクとの包含関係	出典
SBOM 導入手引 Ver.1.0, Ver.2.0	△	経産省（METI）
情報システムにおけるセキュリティコントロールガイドライン	△	Software-ISAC
政府情報システムにおけるセキュリティ・バイ・デザインガイドライン	△	デジタル庁
サイバーセキュリティ経営ガイドライン	◎	経産省（METI）
政府機関等のサイバーセキュリティ対策のための統一基準群	○	内閣サイバーセキュリティセンター（NISC）
サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）	◎	経産省（METI）
クラウドサービス提供における情報セキュリティ対策ガイドライン	○	総務省（MIC）

d. 課題と対応策

No	課題カテゴリー	内容	
1	組織	前提条件	開発時のネットワーク環境は社内の業務用ネットワーク環境上に構築されている。
		課題概要	開発時のネットワーク環境に関するセキュリティ要件についての詳細は明記できない場合がある。
		課題詳細	開発基盤には開発時のネットワーク環境が含まれると解釈しているが、開発で使用するネットワーク環境は社内の業務用ネットワーク環境上に構築される場合があると想定される。この場合、社内の業務用ネットワーク環境はこれを一括管理する社内システム部隊が存在することが多く、それら部隊は個別の開発プロジェクトやチームに属することはない。また、社内の業務用ネットワーク環境がどのようなセキュリティポリシーで対策を行っているのか等の詳細な情報は公開されないケースも多い。このため、開発プロジェクトの当事者は社内の業務用ネットワーク環境の詳細については分からず、その情報を明示・文書化するのは難しいと思われる。よって、開発基盤の一部としてのネットワーク環境のセキュリティ対応は社内の業務用ネットワーク環境を使用する場合においては、すでに担保されている前提となる場合が多いと想定される。 上記の理由から、開発時のネットワーク環境に関する内容については、例えば、「社内ネットワーク環境の要件に準ずる」など概要レベル程度の内容になると思われる。（詳細については明記されない。）

		対策案	（開発元の対策） ・社内の業務用ネットワークをベースとして開発環境を構築した場合、ネットワーク環境のセキュリティ対策については、把握しうる範囲で文書化する。 ・開発に必要なセキュリティ要件が満たせない場合には社内システム部隊が提供する社内の手続き等に従い、対応を依頼・相談する。
		関連タスク	PO.5.1
2	技術・コスト	参照タスク	PO.1.2 の課題 No.1 と同様の課題あり
3	技術・組織	参照タスク	PO.1.2 の課題 No.2 と同様の課題あり

3.2.7 実証結果の要点

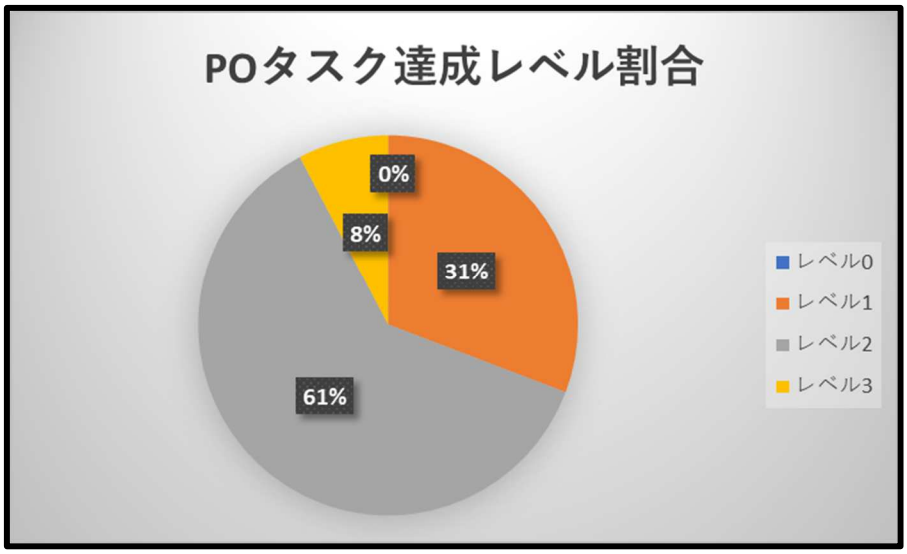
（1） 実証結果と成果物の要点

SSDF の 4 つのタスクカテゴリー（PO/PS/PW/RV タスク）の達成レベルの内訳は以下のとおりである。

	達成レベル				タスク数
SSDF タスクカテゴリー	レベル 0	レベル 1	レベル 2	レベル 3	
PO	0	4	8	1	13
PS	1	1	2	0	4
PW	0	8	8	0	16
RV	0	5	4	0	9
合計	1	18	22	1	42

【PO タスク】

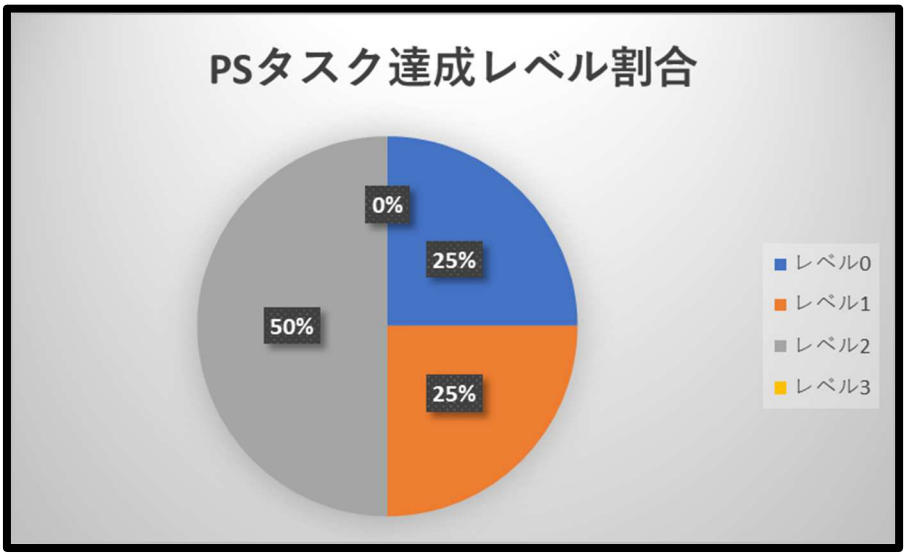
本タスクは他のタスクのベースとなるタスクがあり、難易度が高いタスクが多い。タスクの達成レベルはレベル 2 が多く、セキュア・ソフトウェア開発のベースが構築できていると考えられる。本タスクは開発を開始するにあたって必要な環境定義（セキュリティ要件等の定義）に関するタスクが多く、対応する成果物として主に開発を開始するにあたり作成されると想定される開発計画書内に必要な情報が盛り込まれている。



【PS タスク】

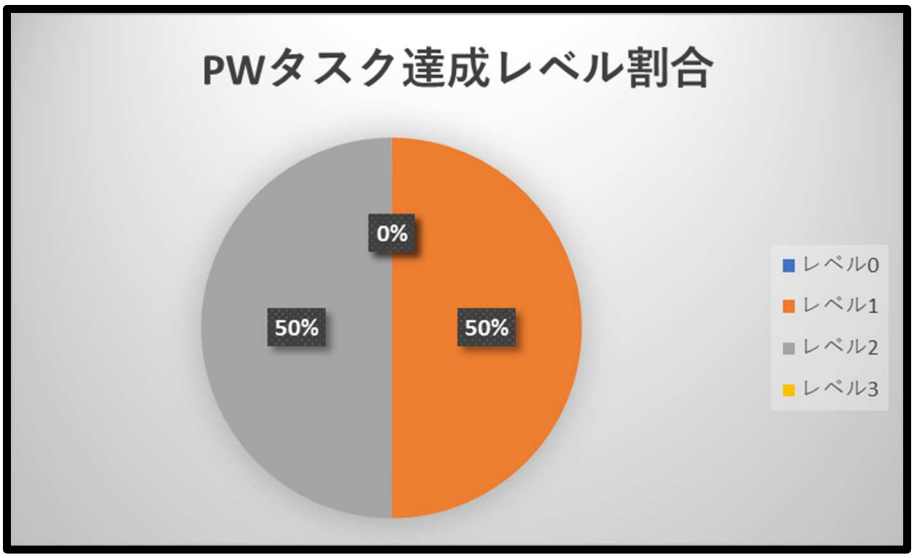
本タスクには達成レベル 0 のタスクがあることが特徴的だが、これは実証検証対象の開発ソフトウェアのビジネスモデルによるものとなっている。今後のビジネスモデル変化に対応できるよう本タスクについては対応する予定となっている。

タスクの達成レベルとしてはレベル 2 が多いが、これはセキュア・ソフトウェア開発に有用なツール（構成管理ツールの GitHub 等）を導入している効果が大きいと考えられる。本タスクはソフトウェアの情報管理が主であり、導入した情報管理ツールの構成情報が主な成果物となっている。



【PW タスク】

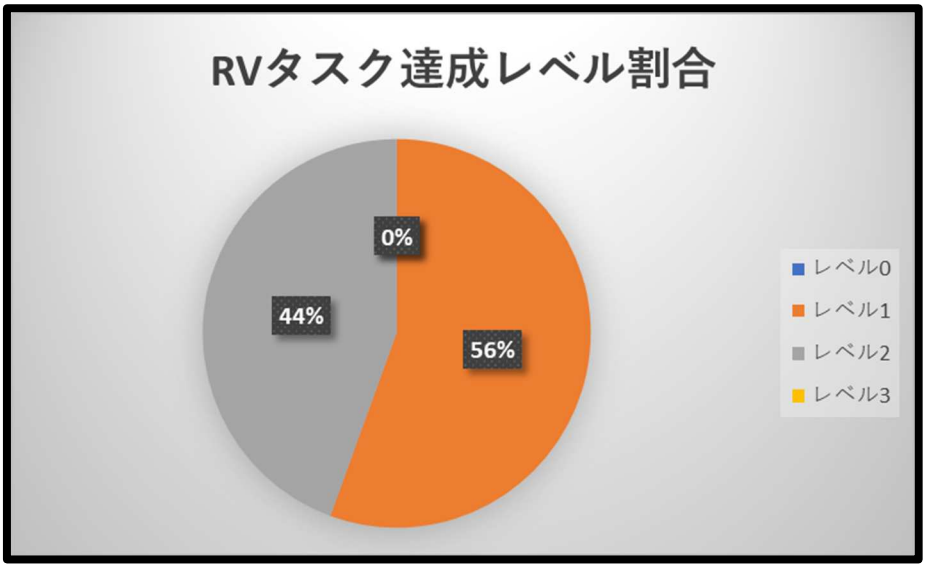
本タスクはソフトウェア開発に直接関連するタスクだが、タスクの達成レベルはレベル 1 とレベル 2 のタスクが同数となっている。よって、基本的なセキュア・ソフトウェア開発は実施できており、今後はタスクの成熟度を高めていく段階にあると考えられる。本タスクはセキュア・ソフトウェア開発に直接関連するタスクのため、各タスク項目に応じた個別の成果物が作成されている。



【RV タスク】

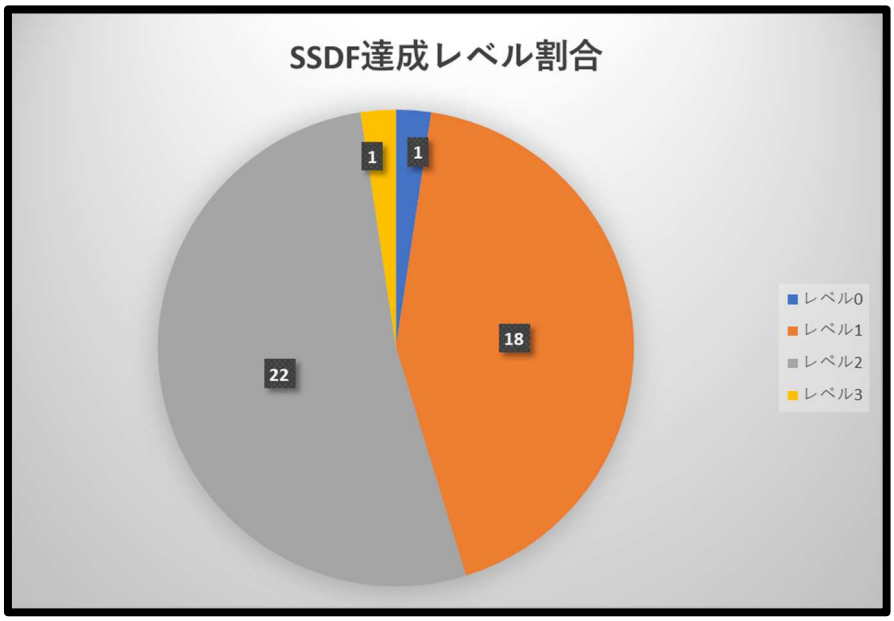
本タスクの達成レベルはレベル 1 のタスクが若干多い。これはセキュリティ専門事業者が行うと想定されるような難易度の高いタスク（RV3.1～3.3）があること、実証検証対象の開発ソフトウェアが現状試用フェーズであり、新規脆弱性の検出はソフトウェア開発社内に閉じていることなどが影響している。今後、本格的な運用に移行後、本タスクの活動が活性化し、タスクの成熟度も高まると想定される。

本タスクは脆弱性情報の管理が主であり、その管理のために導入しているツール（問題管理ツールの Redmine 等）による脆弱性情報管理に関する資料や脆弱性検出に関連する PW タスク（PW.7.1：静的テスト（コードレビュー）方法の決定及び実施等）の再実施結果に関する情報が主な成果物となっている。



（2）達成度評価

実証検証における全 SSDF タスクの達成レベルの割合は以下のとおりとなっている。



達成レベルの内訳としてはレベル 2 が最も多く、次いでレベル 1 となっている。

SSDF タスクの実施状況としてはレベル 0 が 1 件あるものの、今後対応予定ということもあり、全体として網羅されている。よって、セキュア・ソフトウェア開発のベースは構築できており、タスクの成熟度を向上させる段階にあると考えられる。

一般的にセキュアなソフトウェア開発を実践するのはハードルが高いと想定されるが、このような達成レベルでタスクを実施できている要因は以下によるところが大きいと考えられる。

【セキュア・ソフトウェア開発の実践が可能となっている主な要因】

① 実証検証対象のソフトウェア開発元がセキュリティ専業の組織であったため
- セキュリティに関する知見・ノウハウがすでにある

② セキュリティ関連資格をもつ人材が多いため
- 情報確保支援士，CISSP，CISA 等公的セキュリティ関連資格をもつ人材が開発部隊に所属しており、セキュリティの要件チェック等を行っている

③ 企業としてセキュリティ関連の認証を受けており、セキュリティに対する関心度が常に高いため
- ISO9001，ISO27001，プライバシーマーク，JCMVP 暗号モジュール試験機関登録等の認証を受けており、セキュリティに関するケアが常態化している

（3）SSDF ガイドラインマッピングの評価

SSDF タスクと国内ガイドラインのマッピング結果は「2.2.8 ガイドラインのマッピング」に示したとおり、全ての SSDF タスクを満たすようなガイドラインはない。また、ガイドライン毎に不足している SSDF タスクの内容も異なっているため、一律に「こう対応すれば SSDF に対応できる」といった処方箋は存在しない。よって、マッピング対象の国内ガイドラインに準拠している開発プロジェクト等を SSDF タスクに対応させるには、各 SSDF タスク項目と国内ガイドラインの項目の内容のギャップを分析し、不足タスクを洗い出した後、これに対応していくことが求められる。

逆に SSDF タスク項目にはなく、国内ガイドラインにのみ規定されているガイドライン項目がいくつか存在する。その中で、SSDF タスクの項目として追加検討すべきと思われる項目について以下に示す。

【国内ガイドラインでのみ規定されているタスク項目】

①ソフトウェア更新・削除時のソフトウェア設定内容を含む管理に関するガイドライン

国内ガイドライン	タスク項目	関連 SSDF タスク項目
政府機関等のサイバーセキュリティ対策のための統一基準群（NISC）	Ⅱ. 3.1.10.【基本】システムコンポーネントの廃棄 データ、ドキュメント、ツール又はシステムコンポーネントを廃棄する方法を確立するとともに、廃棄方法についてサプライチェーン事業者と合意し文書化すること。	PO.3.2：ツール及びツールチェーンの導入・運用・保守 PW.9.1：ソフトウェアのセキュリティに影響を及ぼす設定の決定 PW.9.2：デフォルト設定の実装と利用者向けの設計の文書化
クラウドサービス提供における情報セキュリティ対策ガイドライン（MIC）	5.2.4 情報システムの更改・廃棄 目的・趣旨 情報システムの更改・廃棄において、情報システムに記録されている機密性の高い情報が廃棄又は再利用の過程において外部に漏えいすることを回避する必要がある。情報システムに機密性の高い情報が記録されている場合や、格付や取扱制限を完全に把握できていない場合等においては、記録されている情報の完全な抹消等の措置を講ずることが必要となる。 5.2.4(1)情報システムの更改・廃棄時の対策 (a)情報システムセキュリティ責任者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下を全て含む措置を適切に講ずること。 （ア）情報システム更改時の情報の移行作業における情報セキュリティ対策 （イ）情報システム廃棄時の不要な情報の抹消	同上

【SSDF タスクの課題】

現状の SSDF タスクでは開発ソフトウェアの更新時や削除時（アンインストール時）の設定について言及していない。

開発ソフトウェアの設定について、ソフトウェア使用時（インストール時）の設定情報だけでなく、ソフトウェアの更新時や削除時（アンインストール時）の設定内容を含めた情報も同時に明確化しておくことが重要と思われる。これは更新時に書き換えられる設定や削除時の設定（設定がそのまま残るのか、一部削除されるのか全て削除されるのか等）の状態によって、セキュリティを含めた他の機能への影響が変わる可能性があると考えられるためである。

【SSDF タスクへの提案】

以下のタスクに本件に関する説明や実施内容例を追加する。もしくは、タスク項目を新設する。

- PW.9.1:ソフトウェアのセキュリティに影響を及ぼす設定の決定
- PW.9.2:デフォルト設定の実装と利用者向けの設計の文書化

開発ソフトウェアの設定について、ソフトウェア使用時(インストール時)の設定情報だけでなく、ソフトウェアの更新時や削除時(アンインストール時)の設定内容を含めた情報も同時に明確化するタスクとする。

②事業・運用継続に関するガイドライン

国内ガイドライン	タスク項目	関連 SSDF タスク項目
政府機関等のサイバーセキュリティ対策のための統一基準群(NISC)	Ⅱ.9. 事業継続マネジメントにおける情報セキュリティ Ⅱ.9.1. 情報セキュリティの継続 ～Ⅱ.9.2. 緊急時対応計画 事業者及び利用者は、クラウドサービスに大規模障害が発生した場合に備え、バックアップデータをクラウドサービス提供地とは異なる地域に保管する等の物理的対策事項と情報セキュリティ面での対策事項を統合した事業継続計画を策定する必要がある。	PO.5.1:開発インフラの分離及び保護
クラウドサービス提供における情報セキュリティ対策ガイドライン(MIC)	5.3.1　　情報システムの運用継続計画の整備・整合的運用の確保 目的・趣旨 業務の停止が国民の安全や利益に重大な脅威をもたらす可能性のある業務は、地震、火災、感染症、情報セキュリティインシデント等の危機的事象発生時でも継続させる必要があり、国の行政機関においては、府省業務継続計画と情報システム運用継続計画を策定し運用している。独立行政法人及び指定法人においても、業務の特性に応じて、中期目標による指示等により、法人の業務継続計画と情報システムの運用継続計画を策定し運用している。 危機的事象発生時に情報システムの運用を継続させるためには、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順を検討し、定めることが重要となる。 なお、こうした業務継続計画や情報システムの運用継続計画が定める要求事項と、情報セキュリティ関係規程が定める要求事項とで矛盾がないよう、それぞれの間で整合性を確保する必要がある。 5.3.1(1)情報システムの運用継続計画の整備・整合的運用の確保 (a)統括情報セキュリティ責任者は、機関等において非常時優先業務を支える情報システムの運用継続計画を整備する場合は、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順の整備を検討すること。 (b)統括情報セキュリティ責任者は、情報システムの運用継続計画に沿って、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順が運用可能であるかを定期的に確認すること。 (c)統括情報セキュリティ責任者は、情報システムの運用継続計画に沿って、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順を定期的に見直すこと。	同上

【SSDF タスクの課題】

現状の SSDF タスクでは開発ソフトウェアの運用継続に関する項目がない。

【SSDF タスクへの提案】

本件に関するタスク項目を新設する。もしくは、以下のタスクに本件に関する説明や実施内容例を追加する。

- PO.5.1:開発インフラの分離及び保護

開発ソフトウェアの運用(継続)に関するタスクも SSDF のタスク項目として追加し、セキュア・ソフトウェア開発のタスクの一部として認知させる。

(4) 課題と対応策

SSDF タスクを実施する上での課題は以下 4 つのカテゴリーに大別される。

① 開発/テスト環境関連
- 開発インフラやツールに関する課題など

② 難易度が高い
- タスク実施の難易度がそもそも高く、対応が難しい

③ 開発プロセス関連
- 開発を進めるにあたって必要な手続きに関する課題など

④ その他
- 上記以外

実証検証時に抽出したタスク実施時の課題を上記のカテゴリーを元に分類した結果は以下のとおりである。

	SSDF タスク課題				課題件数
SSDF タスクカテゴリー	①開発/テスト環境関連	②難易度が高い	③開発プロセス関連	④その他	
PO	5	7	4	1	17
PS	1	1	1	0	3
PW	4	9	6	0	19
RV	1	1	0	0	2
合計	11	18	11	1	53

「②難易度が高い」と想定されるタスクの課題が 18 件と最も多く、次いで「①開発/テスト環境関連」、「③開発プロセス関連」が 11 件となっている。

「②難易度が高い」と想定されるタスクの課題については、そもそもタスクを実施すること自体が難しいと想定されるため、タスク対応時の障害となる可能性が高く、これらへの対策は優先的に検討・対応が必要と思われる。

「①開発/テスト環境関連」、「③開発プロセス関連」の課題については、実施可能な対策について検討

し、できるところから対策に着手していくことが重要である。

タスクカテゴリー別の課題としてはPOタスクが17件、PWタスクが19件と多く見えるが、これは以下の理由によるものと考えられる。

【PO/PWタスクの課題が多い理由】

- タスク項目数(POタスク項目数:13、PWタスク項目数:16)が他のタスクに比べて多いため
- POタスクは組織横断型・共通型のタスクとなっており、セキュリティ要件やプロセス、インフラ環境等を定義するタスクがあるため、検討事項が多く、難易度も高いため
- PWタスクはセキュア・ソフトウェア開発作業に直接関係するタスクが多く、ある程度のセキュア・ソフトウェア開発に対する知見と開発経験がなければ対応できないタスクとなっており、難易度も高い傾向にあるため

抽出されたこれら課題における主な問題点とその対策案は以下のとおりである。

No	問題点	対策案	関連タスク
1	タスク対応時の具体的な参考情報が不足している。 【説明】 タスクを実施する際に参考となる具体的事例の情報があれば、それら参照しつつ対応することも可能なケースがあると思われるが、現状はそのような情報は整備されてないケースが多く、セキュア・ソフトウェア開発の経験が浅い企業等では対応に苦慮することが想像される。結果としてタスクに十分対応できないリスクが高い。	【開発元の対策案】 ・セキュリティ専門業者等に作業委託する。(※コストが問題となる可能性がある) 【公的対策案】 タスク対応時に参考となる具体的な情報を整備し、提供することで、対応の難易度を緩和する。	PO.1.1, 1.2, 1.3 PW.1.1, 1.3, 7.1, 7.2, 8.1, 8.2 など
2	タスク対応できる人材の育成と確保が難しい。 【説明】 タスクに対応するにあたっては、ある程度のセキュリティ関連スキルや開発経験がないと対応できないと考えられる。よって、そのような人材の育成や確保が必要だが、人材不足の昨今において、実際に対応するのは難しく、また、コスト面でも課題がある。	【開発元の対策案】 ・人材の教育を積極的に行い、スキルアップを促し、人材を育成し、適格者を確保していく。 ・資格取得に向けたインセンティブを設ける。(受験費用の補助や資格取得者への奨励金支給等) ・社内リクルータ制度やFA制度の導入等を行い人材の確保を行う。 【公的対策案】 ・セキュリティ関連人材の増加を促進するための施策を実施する。 　-セキュリティ関連資格にかかる費用の補助(公的資格受験費用・資格保持費用の補助や低額化等) 　-無償又は低コストのセキュリティ教材・教育講座の開設 ・セキュリティ人材の紹介/技術系人材活用センター等の開設 　-多様な人材の活用(ハンディがある人、引退世代の活用など)	PO.1.1, 1.2, 1.3 PW.1.1, 2.1 RV.1.3 など

これら対策案を実施することによって、各タスクへの対応ハードルが下がり、SSDFに準拠可能となることを期待したい。各タスクの課題と対策の詳細については「2.2.11　実証結果」を参照のこと。

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 全体スケジュール

4.2 第 13 回ソフトウェアタスクフォース

4.2.1 開催概要

第 13 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 6 年 8 月 21 日 10:00～12:00
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
参考資料 1　「ソフトウェア管理に向けた SBOM(Software Bill of Materials)の導入に関する手引 ver2.0(案)」に対する意見募集で寄せられた御意見に対する考え方
参考資料 2　ソフトウェア管理に向けた SBOM(Software Bill of Materials)の導入に関する手引 ver2.0(案)

4.2.2 要旨

当日はパブコメ対応版について、実証の方向性について、今後の事業についての 3 点について議論が行われた。下記に議事要旨を示す。

- パブコメ対応版について
  - パブコメで頂いた意見のうち、注目すべき意見が 3 つある。
    1 点目は、動的なコンポーネントは SBOM 管理が難しいという意見である。ソースコードやコンパイル済みのバイ ナリ以外にも、実行可能なスクリプト(VBA、マクロ等)やローコー

ドなど、ソフトウェアには様々な形態が存在する。 SBOM で管理できるものと管理できないものを具体的に例示できると良い。

2 点目は、ボリュームが多いため、分冊を検討すると良いという意見である。パブコメで頂いた意見の中に、ソフトウェアの脆弱性はメーカーが対応すれば良いというコメントがあったが、SBOM の活用イメージが定着していないことに起因して提出された意見なのかもしれない。啓蒙の観点から、ユーザー視点でメリットが得られるものを分冊するのが有効だと考える。分冊のコストを考えると、目次レベルでユーザー視点のメリットが書かれた章を作成するという案も考えられる。

3 点目は、SBOM の導入をより強く推進できると良いという意見である。米国では大統領令の影響が強く、旗振りがうまく機能しているものと考える。例えば、SBOM 導入手引の冒頭部分等に、SBOM の推進をより強調するような趣旨の文言の追加を検討しても良いと考える。

- 米国における政府と産業界の共通の理解として、SBOM は有望ではあるが、実証において課題が見つかっており、あくまで機能する範囲でのみ利用することが現実的という認識となっていると考える。産業界にとって SBOM が安心して使えるものとなるように、有効であると確認できる範囲で SBOM を活用する等、具体的な方針を提示していくことが有効であると考える。例えば、クラウドソフトウェアは継続的にアップデートが行われることが多いため、SBOM の効果がどこまであるか不明であると考えるため、実証により効果が確認できたものを示せると良い。
- パブコメで頂いた意見（No.71）への対応の考え方の「対価を負担」という記載について、費用と責任の観点から、現時点で調達者が対価を負担するという表現は具体性が強いと考える。例えば、「一定の負担をする」又は「中長期の課題として取り組む」等の表現の方が良いと考える。
- また、費用に関しては、パブコメで頂いた意見（No.94）への対応の考え方において、「重要な課題として、中長期の課題として取組む。」と記載されている。国際的なハーモナイズや実証の中で、対価を負担するのか、全体に掛かるコストの一部を負担するのか、現時点で断定してしまうのは時期尚早と考える。SBOM は社会基盤として重要な役割をなすため、対価を負担するという表現は適していない可能性がある。今後、どういったファンドから、どういった当事者が、何を負担するか等を設計することが重要であると考える。加えて、SBOM の費用負担の問題は、X-Y といった単純な取引当事者間の問題ではなく、サプライチェーン全体に関わる問題であるため、サプライチェーン全体でどのようにして利益を享受できるかを検討できると良い。そのため、政府として重要性を認識していることを示しつつ、考慮すべき事項を示した内容として示せると良い。
- 一方的に「調達者が対価を負う」と記載すると、SBOM の活用意向低下につながる可能性がある。SBOM の利用価値を明確化し、社会的な共通認識の醸成を図ることで、自然な形で調達費用を捻出可能となるのではないかと考える。例えば、利用価値を明確化し、利用方法に応じた対価の社会合意を図るなど、課題提起にとどめるような形が良いと考える。関連して、パブコメで頂いた意見への対応で「中長期的な課題」に関する対応が一定数ある。SBOM 導入手引の中で発信することが適切か否かについて検討が必要だが、中長期的な

課題を何らかの形で発信し、社会から意見をもらうのも良いと考える。

- 費用負担について、すぐに結論を導くのは難しいと考える。SBOM に対する社会的な意識のレベルが上がっている中で、SBOM のコストをいかに下げるかが重要であると考える。サプライチェーン全体で SBOM の取組を進めることが重要である理由は、最もコストのかからない形でサプライチェーン全体に利益をもたらすことが理想であるためと考える。サプライチェーンにおける SBOM の費用負担は中長期的に考えるという記載を検討できると良い。

・ 実証の方向性について

- 8/6 に実施された「サイバー安全保障分野での対応能力の向上に向けた有識者会議」においてこれまでの議論に関する整理結果が公開されたと認識している。「ソフトウェア等の脆弱性対応」の項において、「安全な製品開発や脆弱性の対応に関するベンダーの責任を規定すべきではないか。」という記載がある。このような考えは、早期警戒パートナーシップの運用が開始した 20 年前から議論してきたことであるが、脆弱性が発見されたからといって一方的に責任を取らせることはできないと考える。そのため、SSDF のような統一的な開発フレームワークが政府から提示されることは良いことだと考える。
- 一方で、最近米国 CISA が Secure by Demand Guide を発表した。これは、ソフトウェアの調達者視点でのセキュリティの考慮事項を示したものであると認識している。米国は Secure by Design、Secure by Default から Secure by Demand までを検討しており、先行して取組を行っている印象である。日本ではまず Secure by Design、Secure by Default を推進し、その上で調達者側のセキュリティ向上を目指すことが適切であると考える。
- 実証でのマッピングの対象が国内文書と記載されているが、米国 CISA が発表した Secure by Design、Secure by Default の文書に対して、日本からは NISC と JPCERT/CC が共同署名を行っている。本文書に関して、サイバーセキュリティ戦略本部は「いずれの項目もサイバー空間の昨今の状況変化を踏まえた妥当なものと考えられる」との意見を発表しており、日本としても重要な文書と位置づけられていると認識している。本文書で記載された内容と、本事業の実証で作る成果物の内容に齟齬が生じないよう、考慮しながら検討できると良い。
- SSDF と国内ガイドラインのマッピングは重要だと考える。1 つのガイドラインに従うことで SSDF に準拠できれば、事業者の負担が減ると考える。まずは国内ガイドラインと SSDF との差分を洗い出すことが重要であると考える。
- また、自動車のソフトウェアは国連の UN-R155 と ISO/SAE 21434 への準拠が求められるが、これらと SSDF の比較についても将来検討できると良い。
- マッピングの対象とするガイドラインについて、現状提示されている文書には、調達側の文書と開発側の文書が混在しているように見受けられるため、例えば、開発側のガイドラインと調達側のガイドラインを分類してマッピングした方が良いと考える。また、SSDF を推進するうえでは IT ベンダーによる活用が重要であるため、関連する検討会と連携しながら進められると良い。その際には、SBOM の対価負担を IT ベンダーが行うべきか、ユーザーが行うべきかといった点についても考慮できると良い。

- QUAD の共同原則を前提とした取組は承知しているが、一方で、欧州ではサイバーレジリエンス法の取組があるほか、国際間のガイドラインとしては、ENISA、FIRST、OWASP 等の文書も本来は考慮するべきであると考える。SSDF との比較の重要性は理解できるが、今後は欧州にも目を向けると良い。
- 様々な業界において、様々なガイドラインが作成されているが、作成された文書の運用も考慮できると良い。加えて、全体コストの最適化が重要であると考える。コスト面を実証で確認することにより、実現性の高い文書の作成が可能となると考える。来年度以降は、インセンティブや補助の在り方を検討できると良い。
- マッピングされた成果物の運用方法は難しい問題であると認識している。まずは大枠の考え方について、マッピングすることが現実的である。
- サイバーレジリエンス法では、脆弱性の報告が罰則規定として位置づけられていると認識している。サイバーレジリエンス法が今後施行される中で調和についても検討する必要があると考える。また、中小企業の取組に対する支援策を並行して検討する必要があると考える。
- 米国 CISA では自己適合証明という表現をされているが、事務局資料中では自己適合宣言となっている。自己適合証明と自己適合宣言について関係性を明確化し、検討できると良い。
- QUAD の取組が先ではあるが、米国 CISA の Secure by Design、Secure by Default の文書では、より厳格な内容が記載されており、脆弱性コーディネーションに関する記載もあると認識している。SSDF のマッピングから始めつつ、Secure by Design、Secure by Default の取組につなげていく方向性が良いと考える。
- SSDF は汎用的な共通言語であるため、具体的な実装は組織ごとで異なると考える。米国 NSA では Enduring Security Framework（ESF）という具体的な手法を含んだ文書を発表している。SSDF とのマッピングを進めた上で、中小企業に向け、もう一段具体化したプラクティスや手順が必要になってくると考える。実施するか否かという 0-1 の議論ではなく、OSS のみ SBOM を作成するなど、ステップを踏んだ導入の仕方も想定される。二極化させるのではなく、改善の方向性を示せると良いと考える。例えば、NSA の ESF では、例えば、NSA の ESF では、パッケージリポジトリ サービスを活用して社内で承認された部品だけを利用する手法なども示されており、開発ツールの利用等で中小企業が取り組みやすいよう、敷居を低くする配慮も必要であると考える。
- ESF は、大統領令 14028 を踏まえ、NSA が業界団体に作成させたものであると認識している。

・ 今後の事業について

- Secure by Design、Secure by Default の文書は上位の視点から記載されており、SBOM はその取組の一部である。求められる取組の全体感と SBOM の位置づけを説明していく必要があると考える。
- 部品 ID の標準化について、商品を流通させる仕組みに組み込むことが有効であると考える。米国では purl ベースの検討が進められていると認識している。SBOM のみならず脆弱性対応を進めるうえで NVD（CVE 採番と脆弱性の分析）への依存が強いため、NVD

の運用が停滞したときの影響が大きいと考える。国内で脅威インテリジェンスを共有する仕組みを作ることが良いと考える。

- 早期警戒パートナーシップ側の検討において、部品 ID に関する検討を進める予定である。
- SBOM について、日本の政府統一基準等に記載の内容で適用を考える際に、米国の基準との相互運用性があるかを今後実証の対象とできると良いと考える。
- 前回の本タスクフォースにおいて、総務省から通信機器を対象に SBOM の導入を検討するという趣旨の説明があった。今後も引き続き、必要に応じて総務省と経産省で連携して取組を進められると良い。
- グローバルサプライチェーンにおける対策の検討が必要であると考える。SSDF や Secure by Design、Secure by Default の文書等、様々な文書や取組があるが、つながりが分かりにくい状況にあると認識している。グローバルサプライチェーンに関与する事業者を支援する目的で、情報の整理が必要であると考える。ソフトウェアのセキュリティを担保することが、企業の取組における最低条件になりつつあると考える。SBOM に課題があることは理解するが、政府調達要件に含めるなど、需要側へのシグナルを増やしていくことが重要であると考える。
- SBOM や SSDF をサイバーハイジーンにつなげる際、中小企業への展開が重要となると考える。コスト面を考えれば、現在使われている脆弱性スキャンツールとの併用で SBOM を普及させていくのが良いと考える。中小企業の規模感は様々であるが、金融に関して言えば、企業全体の規模ではなく、情報システムに関わる担当者の人数が重要となると考える。従業員数が多くても、セキュリティを 2～3 名で回している企業も存在すると認識している。
- 他産業でも、従業員が数万人の規模でも、セキュリティ担当者が 10 名程度の場合もある。SBOM 導入手引や SSDF を受け止めることができない企業を、規模の小さい企業として考えると良い。
- XZ Utils に悪意のあるコードが挿入された問題が明らかになったが、これは、攻撃者が OSS のコミュニティ活動に積極的に関与し、OSS のメンテナーになったあと、バックドアが仕掛けられた事例である。OSS では、活動のピークと利用のピークが異なるため、脆弱性が発見される時期がずれるおそれがある。これは OSS 開発の構造的な問題であると認識している。すでに OpenSSF がこの問題に取り組んでおり、コミュニティへの働きかけは重要であると考える。また、利用者側での省力化も今後検討できると良い。例えば、静的解析を自動化する AI を活用すれば、効率的な脆弱性の検出が可能となると考える。
- XZ Utils のメンテナーの問題は、商用ソフトウェアでも発生する問題である。悪意ある内部犯行者の問題は、IT に限らず発生していると考える。

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。

4.3 第 14 回ソフトウェアタスクフォース

4.3.1 開催概要

第 14 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 6 年 12 月 25 日 10:00～12:00
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　SBOM の国際共同ガイダンスについて（委員限り）
参考資料 1　SSDF と国内ガイドラインのマッピング表（委員限り）
参考資料 2　SBOM の国際共同ガイダンス「フェーズ 1」（委員限り）
参考資料 3　SBOM の国際共同ガイダンス「フェーズ 2」案（委員限り）

4.3.2 要旨

当日は今後の成果物の方向性、今年度以降の事業についての 2 点について議論が行われた。下記に議事要旨を示す。

- 今後の成果物の方向性
  - 例えば、SBOM が普及した際に、ソフトウェアやソフトウェアを含んだ製品を購入することは、SBOM 情報を購入することと同義になると考える。そのため、事業者の SBOM の管理等の取組に係るコストを適正に負担することが必要になると考える。さらに政府調達に SBOM を用いるとなると、会計法に従って適正な価格で競争性のある入札を行う必要があると考える。その際に基準価格の設定のためにどの程度のコストで調達することが適正かを検討する必要があると考える。これらのような現実的な施策を行うために実施できていないことも含めてまとめて頂くと良い。
  - 資料 3 の p16 に記載されている SSDF の達成基準に関しては ISMS 認証制度のような PDCA サイクルの確認等が考慮されているが、実施している具体的な手段（管理策に相当する情報）の確認も必要ではないかと考える。
  - 粒度が細かいが、SSDF が抽象的であるために包含できていない部分が具体的に 5 つあると考える。

1 つ目は、「PO.2.1：役割と責任の定義」において、プロジェクト要員の教育について記載があるが、要員を集める段階で各個人に対するクリアランスの観点が必要だと考える。

2 つ目は、「PO.5.1：開発基盤の分離および保護」において、データ保護も重要であり、本番データとテストデータを分ける必要があると考える。特に、個人情報等の重要な情報を開発環境に利用することの是非やアクセス権限の管理等が求められるとよい。

3 つ目は、「RV.2.2：脆弱性に対するリスク処置の決定と対応計画および実施」のリスクの深刻度の判定において、脆弱性のみを見て判断してしまう懸念があると考える。重要な情報資産につながる脆弱性に関してはCVSS が低くても対応するなど、対応の優先度付けの判定基準には注意を払う必要があると考える。

4 つ目は、「RV.3.3：類似の脆弱性の積極的な検出」において、Microsoft が公表していたとおり、CWE を元にした手法の紹介を検討できると良いと考える。

5 つ目は、リリースするプログラムにデバッグ用のコードや仕様にないモジュールが残存していると脆弱性につながる可能性があるため、不要なコンポーネントを SBOM で検出できると良いと考える。

- 1 つ目についてだが、要員のクリアランスを求めるには、日本の文化的な観点から個人情報などに敏感であり困難であると考える。
- 国内ガイドラインを SSDF へマッピングすることは賛成である。ただし、包含関係の「◎」に関しては再度検討できると良い。例えば資料 3 の P20 に書かれている、SSDF の PS3.1 と CPSF の IP-4 のマッピングに関しては「◎」というよりは「〇」か「△」が妥当と考える。SSDF の PS3.1 ではソフトウェアリリースの完全性検証情報等を安全に保管するといったタスクであるのに対し、CPSF の IP-4 は定期的なバックアップといった対策要件となっていると認識している。データを保存するという観点では同じかと思うが、保存するデータに関しては同等以上とは言い切れないのではないかと考える。こういったミスリードはクロスリファレンスに原因があるのではないかと考える。CPSF の対策要件を満たしている事業者が SSDF への対応を行う際に、「◎」と記載されていると対策を行わないといった事例も考えられ、「◎」の評価に関しては再度検討が必要だと考える。
- SSDF は大統領令が出た段階で改訂されていると認識している。マッピングの中で改訂前後における齟齬を埋めていく取組ができると良い。
- 導入ガイダンスの基礎編など国内関係者が現実的に取り入れることが可能な取組に関しては賛成である。国際的な取組により国内の事業者が振り回されないようにして頂けると良い。SSDF に限った話ではないが、対応の優先度付けに関しては課題が残っているので議論が必要であると考える。
- 今回のマッピング等には賛成である。SSDF 実証の事例数に関しては増やしていくことは必要であると考える。また、業界団体の会員で同様の実証を行った場合、対応レベルが低くなることが想定される。そのため、各社が SSDF を考慮できる段階までに持っていくといった何らかの支援が必要となると考える。中小企業のベンダーの負担が増える可能性もあるため、そういった面を考慮しながら今後の方向性を検討頂けると良い。
- SSDF のタスクに関して経営陣の関与の記述が薄いと認識している。経営層の関与についてもっと強調すべきと考える。暗号分野でも経営層の関与を行う方向性としていると認識し

ている。

・ 今年度以降の事業について

- 政府調達の要件化等を考えると、今後の課題として、「サプライチェーンにおける責任の問題」「脆弱性情報の最新状態の維持のための体制」「国際競争力確保のための情報収集体制」「サプライチェーン上のコスト転嫁の仕組み」を入れて頂きたいと考える。重要インフラのサイバーセキュリティに係る行動計画の中でサプライチェーンのセキュリティ対応を行うことが求められている認識だが、コスト転嫁や責任が明確でないとずさんな情報管理となり、施策として成立しないと考える。何を行えば皆の役に立つかの議論ではなく、次のフェーズとしては具体的にステークホルダー、実施内容、役割と責任、コスト負担などを議論できると良い。また、国際的な協調も考慮して日本の施策を検討する必要があると考える。このような検討が行える体制が敷かれているかを検討できると良い。他国の制度を真似しているだけでは、独禁法や下請法などの法的課題が出てくると考える。今後の検討に掲載されているものもあるが、具体的な姿が見えてこないため、検討できると良い。
- 米国では政権移行に伴い、政策の動向に変化がある可能性がある。具体的には、一般教書演説から落とし込まれて いくことであるが、今後の SBOM を担当する部局や QUAD のような複数国の枠組みに関しての動向に関しても見極めていく必要があると考える。規制・技術上の垣根を他国と作らないことが重要であると考える。少なくとも日米間では平仄（ひょうそく）を合わせると良い。
- 脆弱性のハンドリングに関して、ソフトウェアを提供する会社にとってメリットがある形にしないと SBOM は普及しないのではないかと考える。メリットとして脆弱性情報を提供することも検討できると良い。
- SSDF を実施することは相当難しいと考える。特に、中小企業でセキュアなソフトウェア開発を実施するための施策等を考えていくうえで、中小企業のセキュア・ソフトウェア開発のレベル感の調査が必要であると考える。ガイダンス等の提供の前に、業界団体などを通じてどういった課題感やニーズがあるのかを把握頂けると良い。
- 規模の大きい企業であってもPSIRTが存在する企業は多くないと認識している。これが実情であると考えると、SSDF が現実的なものなのかを考えていくべきであり、実態も含めて調査できると良い。また実装のコストや実装に向けて相談するステークホルダーがどこにあるのかは明確にして頂けると良い。
- 調査の面では、国際的な調査も行って頂けると良い。コスト負担のあり方というのは国際競争力にも影響するので、どういう仕掛けでどういったコスト負担を行っているかを調査頂けると良い。それから情報について虚偽の情報があった際の責任についての動向についても調査頂けると良い。
- 今後作成予定の SSDF の導入ガイド基礎編の普及は、政府調達の要件とすることを検討するのであれば、早い段階で普及できればと考える。ガイドは業界団体等を通じて紹介頂ければと考える。
- 生成 AI によるコード生成に関して知財面の課題があると考える。SSDF 導入ガイダンスの応用編では生成 AI の自動生成コードの管理に関して踏み込んで整理頂きたいと考える。

4.3.3 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。

4.4 第 15 回ソフトウェアタスクフォース

4.4.1 開催概要

第 15 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 3 月 4 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	サイバーインフラ事業者に求められる役割等の検討会について
参考資料 1	セキュア・ソフトウェア開発フレームワーク（SSDF）導入ガイダンス 案（中間整理）
参考資料 2	SSDF 導入ガイダンスタスク整理シート
参考資料 3	11.付録 SSDF 導入の実証例

4.4.2 要旨

当日は今年度の成果物について、今年度以降の事業についての 2 点について議論が行われた。下記に議事要旨を示す。

- 今年度の成果物について
  - SSDF の具体化に伴い、例示された対策のみ実施すれば良いと受け取られてしまう可能性があると考える。例えば、今回の資料においては、タスクのレベル 1 は例として中小企業向けとしている内容があると理解した。PO1.1 のタスクレベル 1 で任意としているテスト環境について、任意を理由に中小企業が対策しなくても良いと誤解してしまう可能性がある。本来 SSDF を元に主体的に考えてもらうことが望ましい。そのために検討いただきたい点が 2 つある。
    - 1 つ目は、各タスクに検討すべき観点や実施しない場合のリスクを列挙することが考えられる。CVSS のみならず、自社へのシステムの影響を考えると良い。経営者や顧客

サポート等の観点を含めることができればなお良い。

- ✧ 2 つ目は、達成レベルに関して、項目として内容的な部分のレベル分けの観点も必要と考える。例えば、ポリシーの文書化の項目において、文書化がセキュリティとしての効果を高めるわけではないので、深さに関する観点を追加いただけると良い。また、システム全体に対して対策を実施するか、システムの一部に対策を実施するかなどの広さの観点でもレベル分けをしていただけると良い。資料 3 の P12,13 に関してはプロセスの成熟度とリスクといった別の観点での記載がなされていると考える。

- ➢ 成果物のまとめ方に関して検討いただけると良い点がある。参考資料 1 では会計監査における原則主義アプローチ（comply or explain）を採用するとあるが、SSDF を適用する場合に大企業においても未実施の項目が多いと考える。そのため、explain のみが実施され、安易な説明が行われる懸念があり、アカウンタビリティベースアプローチの有効性が揺らぎかねないと考える。解決策として、explain としてどういった説明を行うべきかといった想定例を記載できると良い。具体的な対策実施時期や代替案の提示といったような妥当性の説明に関する例を記載いただけると良い。
- ➢ 説明責任という言葉の意味や趣旨が多様的であるために難しいと感じる。リスクベースアプローチからアカウンタビリティベースアプローチに変わった場合の趣旨の差分を示すべきと考える。リスクベースアプローチからアカウンタビリティベースアプローチへの変化は自社のセキュリティ対策の合理性ではなく、相手との関係で契約に従い、誠実になることが重要となると考える。しかし、一般的には分かりにくいため説明が必要となると考える。
- ➢ 会計監査における原則主義アプローチの考え方が、今回のアカウンタビリティベースアプローチに合うかどうかは検討が必要かもしれないと考える。監査等の専門家が対応を行う分野の言葉を使うことは様々な解釈が生じる可能性があると考える。アカウンタビリティアベースプローチ自体は合理的で良い考え方だと理解しているため、会計監査における原則主義アプローチを用いず、分かりやすい言葉で説明いただけると良い。機能安全のアシュアランスケースに関しても同様の事項があると考える。
- ➢ SSDF の内容で、例えば RV3.1 の脆弱性の根本原因の分析など、難易度の高いものが掲載されている。難易度の高い項目に関して、できて当然といったメッセージにならないように注意いただけると良い。
- ➢ SSDF とは別に NIST SP800-216（Recommendation for Federal Vulnerability Disclosure Guidelines）の資料がある。米政府へシステムを納品する際に SSDF の Self attestation を実施することになるが、脆弱性情報は開示しなければならないため、SP800-216 に準じる形で脆弱性を開示する手続を取ると理解している。それに関しては SSDF 単体でハンドリングするわけではないと理解しているが、従来の JPCERT の枠組みを拡張する形で検討を行うのか、別の形で検討を行うのか考えていただけると良い。
- ➢ SSDF の和訳に関して、「プラクティス」を実践策、「タスク」を課題とするのには違和感があるため、今後も検討できると良い。
- ➢ NIST SP 800-218 におけるプラクティスはカテゴリーとしての要素を含めたプラクティスであり、タスクはプラクティスの具体策や項目ではないか。
- ➢ SSDF の和訳に関しては国語学者等にも意見を伺うべきと考える。その国特有の文化を知

らずに外国語を引っ張ってくるというのはユーザーに責任を押し付けてしまう可能性があると考える。

- 難しいかもしれないが、この機会に国内ガイドラインの用語を整理してはどうか。
- 用語の改訂や整理が必要な時期に来ていると思われる。SSDF の他、CISA SBD の用語との関係整理も有用。
- 資料 3 の P3 において、SSDF を参照する形で Shifting the Balance of Cybersecurity Risk 文書が記載されている。ソフトウェア業界全体がどういった方向に向かうかに関しては Shifting the Balance of Cybersecurity Risk 文書に記載されていると理解している。その文書においては、セキュアなソフトウェア開発ライフサイクルに関する記述の中で SSDF を推奨する形になっていると理解している。Shifting the Balance of Cybersecurity Risk 文書との関係がわかるように明示いただければと考える。Shifting the Balance of Cybersecurity Risk 文書に関しては NISC が署名していることもあり、国内での認知度もあると考える。そのため Shifting the Balance of Cybersecurity Risk 文書からどういった取組が行われるかを示すことで全体が見えやすいと考える。

・ 今年度以降の事業について

- 広報や普及促進策については、認証制度の準備が検討予定とされているものの、完成するまでには時間がかかると考える。本認証制度を必ず利用しなくても、自己適合宣言の形で表示する案も考えられるが、そうでなくても自分自身で「SSDF に準拠しています」や「その一部を実施しています」といったことを示すことが大切だと考える。取引先に対する表示の方法についても検討することが、特に中小零細企業にとって重要となり、説明責任を果たすことが難しい場合、どのように対応すべきか検討する必要があると考える。製品開発の際に、SSDF への適合性を表示・宣言した場合、その内容が品質とも関係し、契約の一部として効力を持つと考える。そのため、問題が発生した場合に取引 先に対して SSDF に関する実施状況を説明する責任が生じると考える。したがって、認証を取得していることや、その表示方法も契約内容になると考える。SSDF の適合性を表示していくことが、利用する際に便利で良い取組になると考える。
- 米国の産業界の状況について、義務の程度や導入のスピード感など、新しい政権における方針をさらに注視していく必要があると考える。日本だけが先行してしまうと、日米間でギャップが生じる可能性があるため、連携できる事項や相互の投資関係などについても、調和を図ることが重要だと考える。
- SSDF については、政府調達での活用が考えられるが、政府調達以外に浸透させる場合にどのレベルを求めるのか、 緩和策等も含めて検討できると良い。政府調達以外への浸透も検討するのであれば、目的やスタンス等も設定し、明示することも検討できると良い。
- 政府調達での活用に関して、レベル設定の段階で海外と差異が出てしまうことがないように検討できると良い。
- レベルが設定されている場合、調達の基準としての使われ方が想定されるが、一方で、本来のモチベーションとしては、あるレベルを超えることにより、安全性の向上等が狙えることを示すべきであると考える。そこで重要なのは、自ら考え、必要な対策を選択するという観

点を提示し、その観点に基づいて選択した対策が具体的にどう安全性や準備に役立つかを明確に示すことだと考える。現状のレベル 1 には難易度の高いものがあるため、今後の実証において具体的にどの項目が実行可能であり、どの項目が負担となるかを見極めるべきであると考える。

- セキュアであるということがその企業等への信頼につながる、といった感覚をセキュリティ関係者以外の人たちも含めて共有できないと、SSDF を利用する目的が調達等に引っ張られてしまう恐れがある。
- 次年度として、モデルケース等を設定して SSDF の利用ケースやどういったリスクを抑えられるかを可視化できると良い。
- 政府調達に関連して政府がガイドラインや基準を公開する場合、政府機関に限らず、民間企業にも責任が伴う。そのため、(SSDF 実装のためのレベルの記載が)あくまでも例示であるのであれば、ガイドラインの使い方について説 明を記載したほうが良い。例えばコンサルティングが行われる場合、「政府がこう言っているからこれは必須だ」として、 レベル 1 の適合も難しい状況であることを本アウトプットを出すときに理解しておきながら、適合を求める可能性があると考える。レベル 1 でさえも難しい場合があることを明記するなど、ガイドラインの正しい使い方をしっかりと記載する必要があると考える。
- SSDF やその他のガイドラインがしっかりと浸透するためには、SSDF の内容をきちんと学ぶ場を提供することが重要であると考える。業界団体や開発企業、SIer などを含めた勉強会やセミナーが必要となると考える。
- 自己適合宣言の整合性についても重要であり、Security Action や JC-STAR などの既存の取組とバランスを保つことも必要となると考える。
- 現場の意見としてはツールチェーンが気になるため、具体的に検討すると良い。
- 政府調達において民間製品を多く使用している現状を考慮すると、「政府調達に限る」という制限を設けるべきではなく、民間全体での導入を目指すべきであると考える。そのためには、政府だけでなく、民間の取引が SSDF の基準を尊重し、利用可能な状況を作ることが求められると考える。また、経済合理性を持たせ、自然と普及していく環境を整えることが大切であると考える。強制的な法律は最後の手段とし、経済が循環する形での普及を目指すアプローチ が理想的だと考える。
- ビジネスの課題であると経営陣が認識しなければならないと思うが、なかなかうまく行かない。米国大統領令含め昨今の欧米の規制や義務化の流れは、他に短期的に実現する手段が無い事を示しているように思える。日本政府としてどのように実現するかについては、自主性に任せるだけでは課題が多いと感じる。
- Secure by Design の観点で、特にビジネスプラクティスの結果を公表することや、ソフトウェア開発ライフサイクルの良い事例や悪い事例を記録として活用することは、非常に有意義なアプローチとなると考える。今回の SSDF においても、具体的な事例を挙げることで、実際の取組に即したガイドラインを構築することが可能となると考える。具体的な事例を集めて提示することは、Secure by Design が求める必須事項とも合致し、実効性のある普及策に繋がると考える。実際の開発現場での成功事例、失敗事例を蓄積し、それを基にしたフィードバックループを作ることが、今後の改善や新たな取組の指針になると考える。

4.4.3 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

パブリックコメントを経て 2024 年 8 月に正式公開した「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引 ver2.0」について、その概要資料・付録を含めて英訳を行った。

6. 総括

第 2 章では、SBOM 導入・活用に関する国内外の動向調査、SBOM を活用した脆弱性管理に関わる実証を通じて関連する課題と解決法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、検討を行った。本章では、システムやソフトウェアの開発ベンダー、ツールベンダー、業界団体に対するヒアリングを中心として、文献情報なども加えて、開発現場の実態、課題について整理し、課題に対する解決アプローチ、今後の施策・調査課題などについて整理した。

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、OSS の利活用等について議論をした。

以上の取組み全体を通じて、SSDF 導入ガイダンス案（中間整理）を取りまとめた。

令和6年度産業サイバーセキュリティ強靭化事業
（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

2025 年 3 月

株式会社三菱総合研究所
先進技術・セキュリティ事業本部
TEL (03)6858-3578

経済産業省 御中

令和6年度産業サイバーセキュリティ強靭化事業
（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

先進技術・セキュリティ事業本部

2025 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」の下に設置をした「宇宙産業 SWG 作業部会コアメンバー会議」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」の下に設置をした「宇宙産業 SWG 作業部会コアメンバー会議」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、作業部会コアメンバー会議を 1 回開催した。

2.1 作業部会コアメンバー会議の構成員

今年度見直しを行ったコアメンバー会議の構成員を以下に示す。近年の環境変化等を鑑み、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 7 名のコアメンバーを新たに追加し、コアメンバー会議を開催した。

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
井関　健太	日本電気株式会社 エアロスペース事業部門
木下　仁	独立行政法人情報処理推進機構(IPA)セキュリティセンター 専門委員
小出　祐輔	株式会社 Synspective
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)
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
鈴本　遼	株式会社アークエッジ・スペース 執行役員
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
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
西野　聰	内閣府　宇宙開発戦略推進事務局　参事官
水野　勝成	スカパーJSAT 株式会社
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
堀口　展弘	航空自衛隊　航空システム通信隊　システム管理群　クラウド基盤管理隊長
八木　晴信	株式会社アストロスケール　Cyber Security Manager

2.2 第 15 回作業部会コアメンバー会議の開催概要

第 15 回作業部会コアメンバー会議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、事務局及び JAXA より紹介した後、国内における既存の取組として、JAXA、経済産業省、防衛省及びスペースセキュリティ勉強会の取組を紹介した。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 6 年 10 月 17 日 16:45～18:15
場所：三菱総合研究所本社会議室＋Microsoft Teams 会議によるハイブリッド開催

議題

1. 開会
2. 宇宙産業 SWG 作業部会コアメンバー名簿の更新について
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
   （2）Value of Space Summit 出張報告
4. 国内における既存の取組について
   （1）JAXA における取組
   （2）経済産業省における取組
   （3）防衛省における取組
   （4）スペースセキュリティ勉強会における取組
5. 自由討議
6. 閉会

配付資料:

資料 1　　議事次第・配付資料一覧
資料 2　　作業部会コアメンバー名簿（更新版）
資料 3-1　諸外国における政策動向・脅威動向について
資料 3-2　Value of Space Summit 出張報告
資料 4-1　JAXA の宇宙システムセキュリティ標準
資料 4-2　民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 2.0 概要資料
資料 4-3　情報保証訓令の概要について
資料 4-4　一般社団法人 Japan Space ISAC（仮）について

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」の活用状況や課題の調査・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	取組主体	概要
1	宇宙事業者に対するセキュリティ対策の推奨事項の発表[1]	2024 年 3 月	米国	サイバーセキュリティ・インフラセキュリティ庁（CISA）	各セグメントにおけるサイバーリスク・推奨対策を概説した文書。
2	防衛産業基盤のサイバーセキュリティ戦略の発表[2]	2024 年 3 月	米国	国防総省（DoD）	DoD の内部及び産業界に向けたサイバーセキュリティ活動の道筋を示した戦略。
3	商業宇宙統合戦略（Commercial Space Integration Strategy）の発表[3]	2024 年 4 月	米国	DoD	商業宇宙システムに関するソリューションを、国家安全保障に関する宇宙アーキテクチャに統合することを目的した戦略

[1] CISA, Recommendations to Space System Operators for Improving Cybersecurity
https://www.cisa.gov/sites/default/files/2024-06/Recommendations%20to%20Space%20System%20Operators%20for%20Improving%20Cybersecurity%20%28508%29.pdf
[2] DoD, Defense Industrial Base Cybersecurity Strategy 2024
https://media.defense.gov/2024/Mar/28/2003424523/-1/-1/1/DOD_DOB_CS_STRATEGY_DSD_SIGNED_20240325.PDF
[3] DoD, Commercial Space Integration Strategy
https://media.defense.gov/2024/Apr/02/2003427610/-1/-1/1/2024-DOD-COMMERCIAL-SPACE-INTEGRATION-STRATEGY.PDF

No	動向名称	時期	国	取組主体	概要
4	衛星地上セグメント用のセキュリティ対策プロファイルの公表[4]	2024 年 4 月	ドイツ	情報セキュリティ庁(BSI)	衛星の地上セグメント用のセキュリティ対策プロファイルを定めた文書。
5	衛星システムに対するセキュリティ管理策のテーラリング文書の発表[5]	2024 年 4 月	米国	Aerospace Corporation	RMF(リスク管理フレームワーク)を効率的に適用できるよう、衛星システムに対する管理策のテーラリングを独自で行った報告書。
6	Race to Resilience の発表[6]	2024 年 5 月	米国	宇宙軍(Space Systems Command)	2026 年までの対応能力向上に関する目標達成の緊急性を訴求するための Web サイト。
7	NASA のサイバーセキュリティの取組を評価したレポートの発表[7]	2024 年 5 月	米国	会計検査院(GAO)	NASA の宇宙開発プロジェクトのサイバー脅威に関する取組を評価し、今後求められる推奨事項を提示した文書。
8	防衛予算増額・防衛力質的向上に向けた白書の発表[8]	2024 年 5 月	米国	ロジャー・ウィッカー上院議員	北朝鮮、中国、ロシアからの脅威に対処するため、議会・国防総省に対し、防衛予算増額・防衛力質的向上を求めた白書。
9	最優先リスク事項と最優先リスク軽減策に関する戦略覚書の発表[9]	2024 年 6 月	米国	国土安全保障省(DHS)	DHS が今後 2 年間で焦点を当てるべき最優先リスク事項と、それに対する緩和策をまとめた文書。

[4] BSI, IT-Grundschutz-Profil für das Bodensegment von Satelliten https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Bodensegment-Satellit.pdf
[5] Aerospace Corporation, Space Segment Cybersecurity Profile for National Security Systems – Revision A https://sparta.aerospace.org/resources/TOR-2023-02161-RevA%20Space%20Segment%20Cybersecurity%20Profile.pdf
[6] Space System Command, Race to Resilience https://www.ssc.spaceforce.mil/About-Us/Race-To-Resilience
[7] GAO, Plan Needed to Update Spacecraft Acquisition Policies and Standards https://www.gao.gov/assets/gao-24-106624.pdf
[8] Roger Wicker, 21st Century Peace Through Strength A generational Investment in the US military https://www.wicker.senate.gov/services/files/BC957888-0A93-432F-A49E-6202768A9CE0
[9] DHS, Strategic Guidance and National Priorities for U.S. Critical Infrastructure Security and Resilience (2024-2025) https://www.dhs.gov/sites/default/files/2024-06/24_0620_sec_2024-strategic-guidance-national-priorities-u-s-critical-infrastructure-security-resilience.pdf

No	動向名称	時期	国	取組主体	概要
10	宇宙システムに対するサイバー攻撃の網羅的整理に関する研究論文の発表[10]	2024 年 6 月	米国	カリフォルニア州立ポリテクニック大学	宇宙システムに対して想定されるサイバー攻撃の脅威アクター、攻撃の動機、攻撃手法等を網羅的に整理したマトリックスを提案した論文。
11	NASA の宇宙システムに対するサイバーセキュリティ対策に関する法案の提出[11]	2024 年 7 月	米国	マクスウェル・アレハンドロ・フロスト下院議員、ドン・ベイヤー下院議員	NASA の宇宙システム及びサービスの開発・製造業者のサイバーセキュリティ対策を義務付けることを提案した法案。
12	宇宙資産に対する脅威をリアルタイムで検出するシステムの開発[12]	2024 年 11 月	米国	Aerospace Corporation	複数の機械学習モデルを用いたリアルタイム異常検知システムの開発。
13	Japan Space ISAC の設立[13]	2024 年 11 月	日本	一般社団法人 Japan Space ISAC	宇宙のサイバーセキュリティを中心とするプラクティス、課題、情報等を共有する ISAC（Information Sharing and Analysis Center）団体の設立。
14	国家のサイバーセキュリティにおけるイノベーションの強化と推進に関する大統領令の発表[14]	2025 年 1 月	米国	ホワイトハウス（バイデン大統領）	連邦政府機関に対し、国家のサイバーセキュリティを改善するための行動を指示した大統領令。

[10] Cal Poly Ethics + Emerging Sciences Group, Outer Space Cyberattacks: Generating Novel Scenarios to Avoid Surprise https://ethics.calpoly.edu/spacecyberattacks.pdf
[11] H.R.8965 - Spacecraft Cybersecurity Act https://www.congress.gov/bill/118th-congress/house-bill/8965/committees
[12] Aerospace Corporation, Space Threat and Risk Detection and Reporting 等 https://aerospace.org/sites/default/files/2024-11/Detection%20and%20Reporting%20System%20%28DARS%29.pdf
[13] 一般社団法人 Japan Space ISAC https://japan-space-isac.jp/
[14] 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

No	動向名称	時期	国	取組主体	概要
15	米国宇宙産業界へのサイバーセキュリティに関する調査結果の発表[15]	2025 年 1 月	米国	国家宇宙会議（National Space Council）、国家サイバー長官室（Office of the National Cyber Director）、大統領府	宇宙システムのサイバーセキュリティ要求事項の見直しに当たり実施された米国宇宙産業界へのヒアリング調査結果。
16	宇宙システムを重要インフラ分野に位置づける法案の提出[16]	2025 年 2 月	米国	ケン・カルバート下院議員	DHS 長官に対して重要インフラとして宇宙システム・サービスに関するガイダンスを発行することを提案した法案。
17	商用衛星におけるサイバーセキュリティ脅威や推奨事項をまとめた文書の発表[17]	2025 年 3 月	EU	欧州ネットワーク・情報セキュリティ機関（ENISA）	商用衛星のライフサイクルや資産、衛星に対するサイバーセキュリティ上の脅威、脅威に対して求められる対策を整理した文書。

以降では、それぞれの取組について詳説する。

1）米国 CISA：宇宙事業者に対するセキュリティ対策の推奨事項の発表

2024 年 3 月、米国 CISA は宇宙事業者に対するセキュリティ対策の推奨事項を示した「Recommendations to Space System Operators for Improving Cybersecurity」を発表した。本文書では、商業宇宙システムが、国家安全保障から金融、教育、通信に至るまで日常生活において存在感を高める中、宇宙に関連する資産の所有者、運用者、利用者、製造者がサイバーセキュリティを最優先に考慮することが重要である旨が示されている。文書では、表 3-2 に示すように、4 つのセグメントごと（宇宙、地上、アップリンク・ダウンリンク、ユーザーセグメント）の一般的なサイバーリスクを概説し、各アクターに対して、NIST の関連文書に記載の推奨事項に沿った対策を行えるよう、セキュリティプロファイルの作成を推奨している。

[15] National Space Council 等, Space System Cybersecurity Space Industry Perspectives https://bidenwhitehouse.archives.gov/wp-content/uploads/2025/01/Space-System-Cybersecurity-Industry-Perspectives-Report.pdf
[16] H.R.1154 - To direct the Secretary of Homeland Security to issue guidance with respect to space systems, services, and technology as critical infrastructure, and for other purposes. https://www.congress.gov/bill/119th-congress/house-bill/1154/text
[17] ENISA, ENISA Space Threat Landscape 2025 https://www.enisa.europa.eu/publications/enisa-space-threat-landscape-2025

表 3-2 CISA 文書におけるセグメントごとの脅威・推奨事項

	宇宙セグメント	地上セグメント	アップリンク・ダウンリンクセグメント	ユーザーセグメント
脅威	・ コマンド侵入/ペイロード制御 ・ マルウェア感染	・ ハッキング、ハイジャック ・ マルウェア感染	・ ジャミング/スプーフィング ・ リプレイ攻撃	・ スプーフィング ・ サービス拒否
推奨事項	・ ネットワーク分離とセグメンテーションの原則の適用、暗号化の実装 等 ・ 最小機能原則の適用、サプライチェーンのセキュリティ管理 等	・ 不正アクセスを防止するための技術の活用、IDS(侵入検知システム)の活用等 ・ 最小機能原則の適用、サプライチェーンのセキュリティ管理 等	・ CRPA(制御受信パターンアンテナ)等のハードウェアベースのソリューションの採用、暗号化通信の使用 等 ・ 暗号化の実装	・ ハードウェアベースのソリューション(地上からの信号を無効にするGPS 受信機等)の採用、暗号化通信の使用 等 ・ 暗号化の実装、ハードウェアベースのソリューションの採用 等

2) 米国 DoD:防衛産業基盤のサイバーセキュリティ戦略の発表

2024 年 3 月、米国 DoD は、2024 年度の防衛産業基盤(DIB)[18]のサイバーセキュリティ戦略を発表した。同戦略は、2024 年度から 2027 年度を対象とした DIB のサイバーセキュリティの確保と悪意のあるサイバー活動からの回復力を強化するための戦略であり、包括的な 4 つの目標とそれに基づく具体的な目的を示している。4 つの目標の概要と、それに基づく詳細な目的は表 3-3 に示すとおりである。

表 3-3 DIB サイバーセキュリティ戦略における 4 つの目標と目的

目標	目標の概要	目的
1. DIB のサイバーセキュリティに関する国防総省のガバナンス体制強化	DIB のサイバー空間の安全性確保に向け、多数の関係省庁、部局が連携し、支援目的と活動を同期させるために権限を調整する	1.1 分野横断的なサイバーセキュリティの問題に対する省庁間協力の強化
		1.2 請負事業者及び再々委託先のサイバーセキュリティ責任に関する規制策定の推進
2. DIB のサイバーセキュリティ体制の強化	契約上のサイバーセキュリティ要件への準拠及び定期的な評価を行う。その結果	2.1 DIB による請負事業者及び再々委託先の国防総省のサイバーセキュリティ要件の準拠の有無の評価
		2.2. 国防総省及び DIB 間の脅威、脆弱性、サイバー

[18] Defense Industrial Base の略称であり、米軍に対する研究開発支援、軍事兵器システム、サブシステム、部品・コンポーネントの設計・生産・納入・保守を行う複合体であり、請負事業者、政府運用施設等により構成される。

目標	目標の概要	目的
	を元に、DIB はベストプラクティスを作成する	関連インテリジェンスの共有の改善
		2.3 DIB の IT システムに関する脆弱性の特定
		2.4 悪意のあるサイバー活動からの回復
		2.5 サイバーセキュリティの規制、ポリシー、要件の有効性の評価
3. サイバー競合環境における重要な DIB 機能の回復力の維持	多層的なサイバーセキュリティ・エコシステムにおいて、各分野のパートナーと緊密に連携する	3.1 重要な DIB 生産機能を悪意のあるサイバー活動から保護し、回復させる能力の構築
		3.2 政策における重要なサプライヤー及び施設のサイバーセキュリティの重点化
4. DIB とのサイバーセキュリティ連携の改善	サイバーセキュリティの啓発に使用されるコミュニケーションの体制を合理化し、評価する	4.1 商用インターネット、クラウド、サイバーセキュリティサービスプロバイダーとの連携を活用した DIB サイバー脅威の認識の強化
		4.2 DIB とのコミュニケーションとコラボレーションの改善
		4.3 DIB との双方向コミュニケーションの改善及び官民サイバーセキュリティ協力の拡大

DIB のサイバーセキュリティの確保とサイバーレジリエンスの強化に当たっては、国防総省と DIB の密接なコミュニケーションを可能にする組織体制の整備、関連する省庁・民間事業者との協力関係の構築、また将来的に CMMC（Cybersecurity Maturity Model Certification）を通じた請負事業者のセキュリティ体制を評価・認証する方針が示されている。

3）米国 DoD：商業宇宙統合戦略の発表

2024 年 4 月に、米国 DoD は、商業宇宙統合戦略（Commercial Space Integration Strategy）を発表した。本戦略は、米国国家安全保障戦略及び 2022 年の国防戦略に準じて作成されており、米国のレジリエンスと抑止力強化に向けて、商業宇宙システムに関するソリューションを国家安全保障に関する宇宙アーキテクチャに統合することを目的に、4 つの基本原則、優先順位、アプローチ方法、関連するミッション領域を示した。4 つの基本原則は以下のとおりである。

- 政府機関と商業ソリューション間の適切なバランスの確保
- インターオペラビリティの確保
- 国家安全保障アーキテクチャにおけるレジリエンスの優先順位付け
- 国際的な責任ある行動

これらの基本原則の下で、特に優先して取り組むべき事項として、以下の 4 点を挙げている。

- 紛争の範囲全体に対して、商業ソリューションへのアクセスを確保する
- 有事の前に統合を達成する
- 商業ソリューションを統合するための安全性を確立する

- 使用する新しい商業ソリューションの開発を支援する

同省は商業宇宙システムに関するソリューションを統合するために民間事業者と協力して、リスクを軽減するようまた、必要に応じてリスクを受け入れる方針を示している。

4）ドイツ BSI：衛星地上セグメント用のセキュリティ対策プロファイルの公表

2024 年 4 月、ドイツ情報セキュリティ庁（BSI）は、衛星の地上セグメント用のセキュリティ対策プロファイルを定めた文書を発表した。本プロファイルでは、図 3-1 に示すように、衛星システムのアーキテクチャを整理のうえ、典型的な衛星システムのミッションを整理している。そして、ミッションの特性に基づいて、地上局システムの対策を決定するよう推奨している。対策検討例として 3 つのケーススタディが示されているほか、地上セグメントに関連する業務プロセス、アプリケーション、IT システムを整理のうえ、実践すべきセキュリティ管理策をマッピングしている。

なお、2023 年 5 月には、衛星システムに対する対策ベースラインを定めた文書[19]が BSI から発表されている。この文書では、3 つの脅威シナリオに基づく脅威分析が実施されているほか、脅威が与える影響度合い・影響範囲の分析、脅威に対して衛星システムが実装すべきセキュリティ対策を規定している。

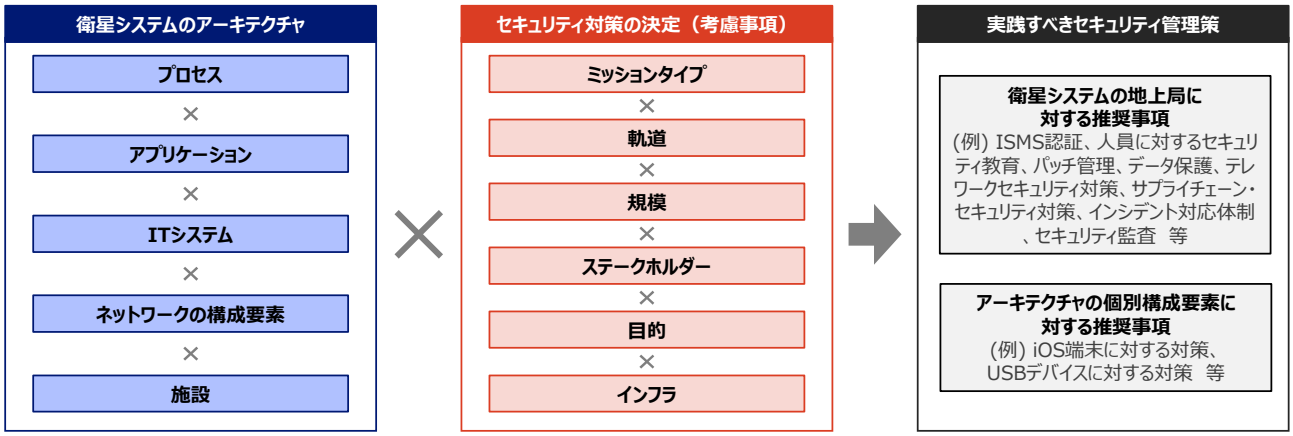


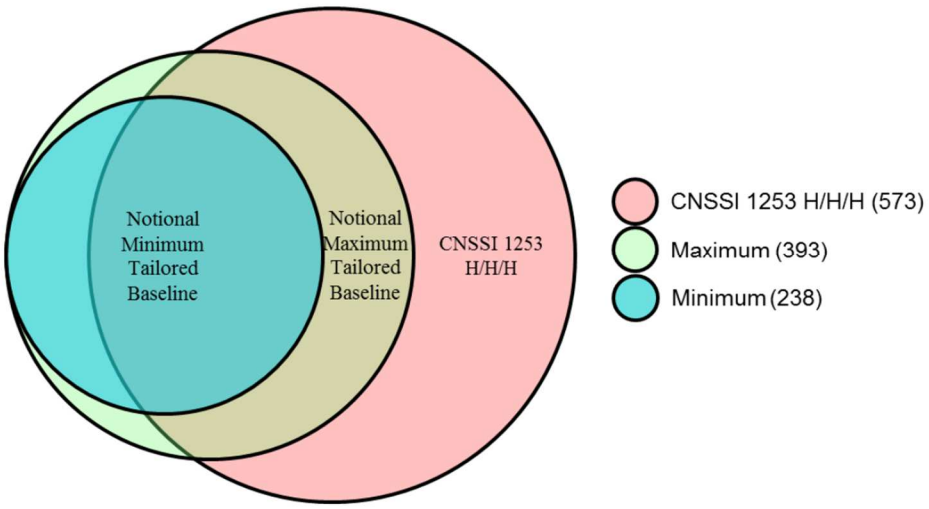
図 3-1 ドイツ BSI の地上セグメント向け対策プロファイルにおけるセキュリティ管理策検討の流れ

5）米国 Aerospace Corporation：衛星システムに対するセキュリティ管理策のテーラリング文書の発表

2024 年 4 月、Aerospace Corporation は、衛星システムに対して、NIST SP 800-37 で規定されたリスク管理フレームワーク（RMF）を効率的に適用できるよう、衛星システムに対する管理策のテーラリングを独自で行った報告書を発表した。同社は、CNSSI 1253（Security Categorization

[19] BSI, TR-03184 Informationssicherheit für Weltraumsysteme
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03184/BSI-TR-03184.pdf

and Control Selection for National Security Systems)[20]の管理策ベースラインを衛星システムにテーラリングするには多大な労力が必要であること、CNSSI 1253 では衛星システム特有の脅威を考慮できていないことを課題として挙げている。この課題に対し、同社が開発した SPARTA フレームワーク[21]を活用し、衛星システムに想定される脆弱性や脅威といったリスクを分析・評価のうえで、当該リスクに対して求められる管理策を整理(テーラリング)している。テーラリングされた管理策は、「最低限」の管理策と「最大限」の管理策に分かれる。それぞれの管理策に、CNSSI 1253(NIST SP 800-53 の「高」の管理策)には含まれない、衛星特有の管理策(例:「AC-3 (2) 二重認可」、「SC-7 (15) ネットワーク化された特権アクセス」など)が含まれる。テーラリングされた管理策と CNSSI 1253 管理策との関係性は図 3-2 のとおり整理されている。



出所) Aerospace Corporation, Space Segment Cybersecurity Profile for National Security Systems – Revision A https://sparta.aerospace.org/resources/TOR-2023-02161-RevA%20Space%20Segment%20Cybersecurity%20Profile.pdf (閲覧日:2025 年 2 月 19 日)

図 3-2 Aerospace 社によってテーラリングされた管理策と CNSSI 1253 管理策との関係性

6) 米国宇宙軍:Race to Resilience の発表

米国宇宙軍(Space Systems Command)は、よりレジリエントな宇宙システムの開発を目指し、2026 年に運用能力を最大化することを短期目標として掲げられている。2026 年度の目標設定は、中国の急速な成長や昨今の地政学上のリスクの高まりを受けて定められている。

Race To Resilience は、民間宇宙事業者を含めた各関係者に、2026 年の目標達成の緊急性を訴求するためにはじめられたプロジェクトである。運用能力の最大化に当たっては、軌道上の脅威に対して迅速に対応する能力の向上や、軌道上のアセットが劣化又は破壊された場合に短期間でその能力を増強する能力を持つことが目標とされている。

具体的な取組内容は明記されていないものの、民間宇宙事業者が提供するソリューションとの統合、

[20] CNSS(国家安全保障システム委員会), CNSSI 1253: Security Categorization and Control Selection for National Security Systems https://www.dcsa.mil/portals/91/documents/ctp/nao/CNSSI_No1253.pdf
[21] Aerospace Corporation, SPARTA https://aerospace.org/sparta

重要な他産業（AI や機械学習の分野）、同盟国との連携の重要性等が強調されている。なお、2026 年の目標達成が強調されているものの、達成できなかった場合の罰則は規定されていない。

7）米国 GAO：NASA のサイバーセキュリティの取組を評価したレポートの発表

2024 年 5 月、米国会計監査院（GAO）は、NASA に対して、NASA の宇宙開発プロジェクトのサイバー脅威に関する取組について評価した結果を「NASA Plan Needed to Update Spacecraft Acquisition Policies and Standards」として発表した。GAO は、NASA が開発した宇宙船がソフトウェアと IT に依存しており、サイバー攻撃の対象とされるおそれが増加している背景から、3 つのプロジェクト[22]をピックアップし、（1）調達要件にサイバーセキュリティに関する要件をどの程度組み込んでいるか、（2）調達方針や基準におけるサイバーセキュリティ関連項目の追加更新の必要性を、どのように判断しているかの 2 点について評価を実施した。評価を基に、GAO は、宇宙船の調達時に必要な方針とセキュリティ要件に関するアップデートをいつまでに行うかを具体的に示すよう、NASA に勧告している。

NASA は、本勧告に基づいて、方針を更新することに同意する一方、具体的な対応のタイムラインを提示することには同意をしていない。これに対し、GAO は、タイムラインがなければいつ実施されるか不明であるという反論を示している。

8）米国ウィッカー上院議員：防衛予算増額・防衛力質的向上に向けた白書の発表

2024 年 5 月、米国上院軍事委員会のメンバーであるロジャー・ウィッカー上院議員は、議会及び国防総省に対し、米国の防衛力を強化し、北朝鮮、中国、ロシアからの脅威に対処するために、防衛予算を増額し、防衛力の質的向上を図ることを目的に白書を発表した。

宇宙分野について、本白書では、中国の人民解放軍の脅威の高まりに対抗するために、宇宙軍（US Space Force）の役割強化、衛星のサイバーセキュリティと妨害防止機能の向上、商業宇宙システムを利用した軍事宇宙の回復力と経済性の向上等が必要である旨が示されている。

9）米国 DHS：最優先リスク事項と最優先リスク軽減策に関する戦略覚書の発表

2024 年 6 月、米国 DHS は、今後 2 年間で同省が焦点を当てる最優先リスク事項と最優先リスク軽減策をまとめた戦略覚書を発表した。

最優先リスク事項として挙げられている事項は以下の 5 つであり、中国がもたらす脅威や AI 等の新興技術に伴うリスクが挙げられているほか、重要インフラにおける宇宙システムへの依存性の高まりに伴うリスクも最優先事項の一つとして明示されている。

- **中国がもたらすサイバー脅威やその他の脅威：**
  中国は、米国の国防インフラや他の重要インフラを標的とする意思がある。また、スパイ活動な

[22] Gateway Power and Propulsion Element（月面宇宙ステーション化に向けて、ゲートウェイ化を推進するミッション）, Orion Multi-Purpose Crew Vehicle（打上時もしくは帰還時に船員の安全性を担保するミッション）, Spectro-Photometer for the History of the Universe, Epoch of Re-ionization and Ices Explorer（近赤外線等を利用し、天の川銀河にある 1 億個以上の星に関するデータを収集し調査するミッション）

ど、その他の悪質な活動の脅威も存在する。

- **AI 等の新興技術がもたらすリスク：**
  AI 等の新興技術が重要インフラに及ぼす影響を分析・検討する必要がある。また、量子コンピューターの登場によるリスクも考慮する必要がある。
- **サプライチェーン脆弱性：**
  将来の公衆衛生やその他の危機への備えの一環として、サプライチェーンの効率性を再考するとともに、レジリエンスを強化する必要がある。
- **気候変動リスク：**
  異常気象、洪水、干ばつ、ハリケーン、山火事等、様々な気候変動リスクに対し、重要インフラを持続可能かつ強靭なものにする必要がある。
- **宇宙システムへの依存性の高まりに伴うリスク：**
  ウクライナ侵攻に伴う商用衛星通信システムへの攻撃など、宇宙システムにおける潜在的なリスクは増加している。宇宙システムは重要インフラに分類されないが、宇宙システムを保護することは米国政府の責任である。DHS は、宇宙システムへの依存度や障害時の影響を評価するほか、関連する民間セクター組織と連携した作業部会の取組を拡大する。

これらのリスクに対する最優先リスク軽減策として、以下の 4 つの緩和策が挙げられており、あらゆる脅威に対抗できるレジリエンスを構築すること、セキュリティやレジリエンスに関する基本要件を採用すること等が挙げられている。

- **あらゆる脅威やハザードに耐え得るレジリエンスを構築する：**
  DHS は、他の連邦政府機関や重要インフラ事業者と協力して、有害なインシデントが連鎖的に及ぼす影響度合いを予測し、あらゆる脅威やハザードから迅速に回復するための対応計画を策定する。
- **セキュリティとレジリエンスの基本要件を採用する：**
  DHS の CPGs（Cross-Sector Cybersecurity Performance Goals）、NIST の CSF 2.0（Cybersecurity Framework ver.2.0）などは基本要件を提供する好例である。DHS は、他の規制当局や民間団体と連携して、これらの基本要件の採用を支援するツールを開発する。
- **サービス提供者にインセンティブを与え、リスクを軽減する：**
  DHS は、製品・サービスにおけるセキュリティ・バイ・デザイン及びセキュリティ・バイ・デフォルトの原則を推進する。また、新たな製品・サービスのセキュリティとレジリエンスを高めるために、関係者と継続的に協力する。
- **リスクが集中する地域やシステム上重要な事業者を特定する：**
  DHS は、システム上重要な地域や事業者を特定し、優先順位を付け、政府のリスク管理能力に反映する。これに際し、セクター内・セクター間の依存関係や相互依存性をより深く理解するよう努める。

10）米国 Cal Poly：宇宙システムに対するサイバー攻撃の網羅的整理に関する研究論文の発表

2024 年 6 月、カリフォルニア州立ポリテクニック大学（Cal Poly）の研究グループは、宇宙システムに対して想定されるサイバー攻撃の脅威アクター、攻撃の動機、攻撃手法等を網羅的に整理した ICARUS マトリックス（Imagining Cyberattacks to Anticipate Risks Unique to Space）を開発した。ICARUS マトリックスの概要を図 3-3 に示す。また、各カテゴリにおける要素の一覧を図 3-4 に示す。ICARUS マトリックスの要素を組み合わせることで、400 万以上の脅威シナリオが作成できるとしている。同研究グループは、42 の具体的な脅威シナリオを例示しているほか、宇宙領域におけるサイバー攻撃増大の 7 つの背景も整理している。

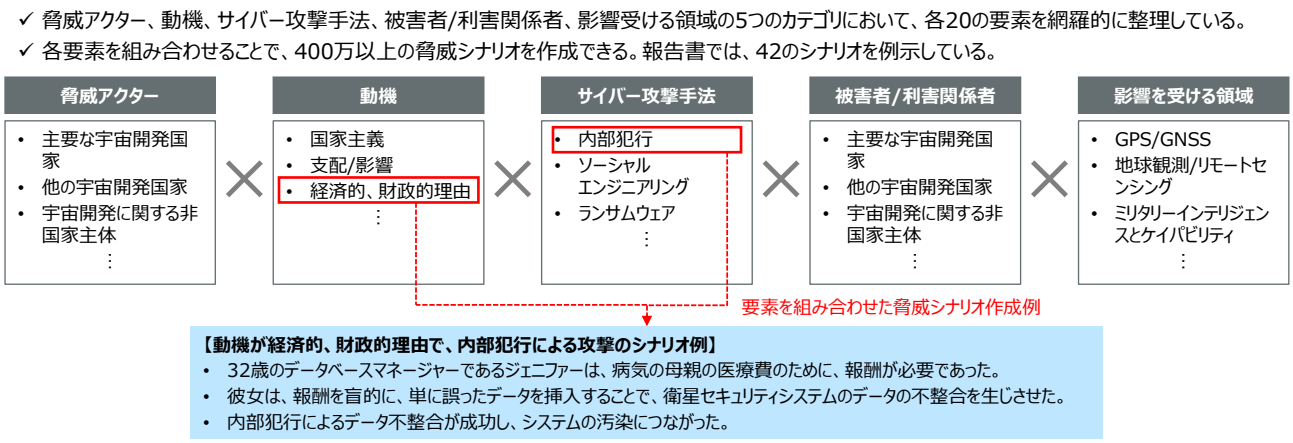


図 3-3 ICARUS マトリックスの概要

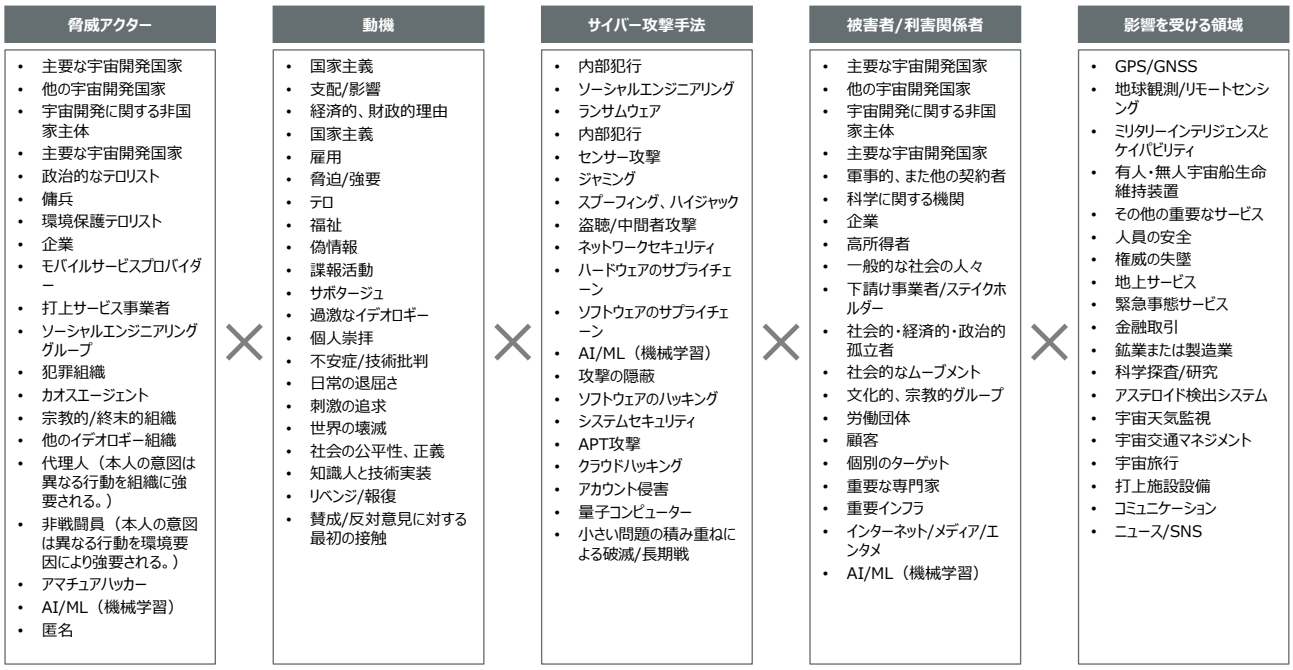


図 3-4 ICARUS マトリックスの具体的な要素

11）米国フロスト下院議員等：NASA の宇宙システムに対するサイバーセキュリティ対策に関する

法案の提出

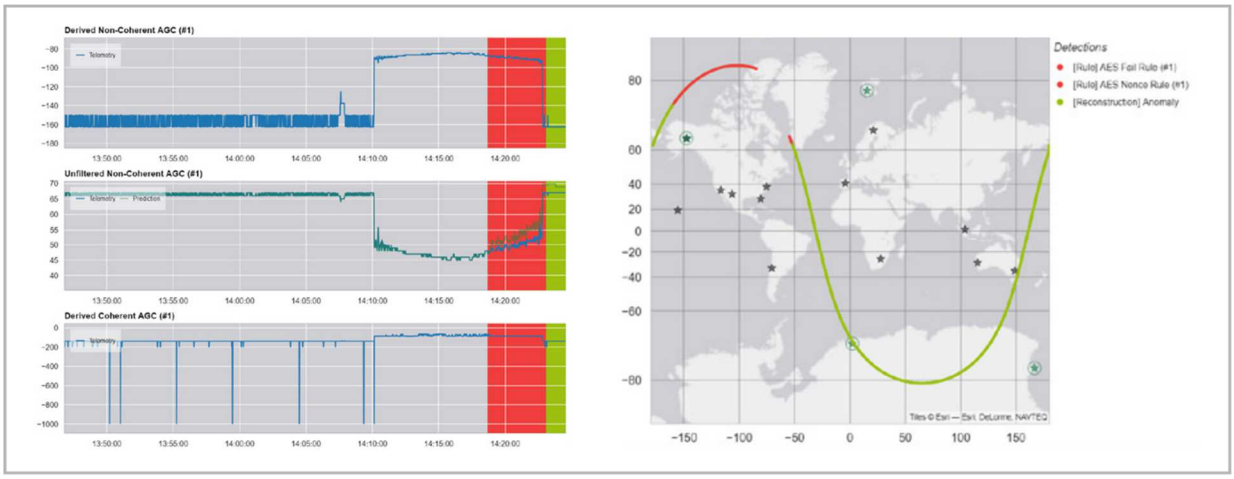
2024年7月、マクスウェル・アレハンドロ・フロスト下院議員とドン・ベイヤー下院議員により、NASAに対して、NASA の宇宙システム及びサービスの開発・製造業者のサイバーセキュリティ対策を義務付ける「Spacecraft Cybersecurity Act」の法案が下院に提出された。同法案は、2024 年 5 月に米国 GAO が発表したレポート(第 3.1 節 7)参照)に基づき、中国やロシアの攻撃アクターが NASA を標的としているものの、NASA の調達ポリシー・調達基準の更新に関する明示的なタイムラインが示されていないことを背景としている。同法案では、NASA 長官に対し、法案成立から 270 日以内に、NASA の宇宙システム及びサービスに関する調達ポリシーと調達基準を更新すること、調達ポリシー・基準に対して脅威から保護するために必要なガイドライン及び管理策を組み込むための実行計画を完成させることを求めている。

12)米国 Aerospace Corporation:宇宙資産に対する脅威をリアルタイムで検出するシステムの開発

2024 年 11 月、米国 Aerospace Corporation は、宇宙資産に対するサイバー脅威や物理的脅威(GPS 妨害、コマンド受信機干渉、レーザー照射など)をリアルタイムで検出するシステム「Detection and Reporting System(DARS)」の開発を発表した。DARS は、地上側と宇宙側を統合して運用する分析システムであり、複数の機械学習モデルを用いてデータを分析することで、誤検出と異常との効果的な区別を可能としている。また、老朽化した宇宙船や変化する宇宙環境に自動的に適応することが可能である。

Aerospace 社は、NOAA-20 及び NOAA-21[23]のデータを使用してモデルを訓練し、大規模衛星における脅威の検出・特性化に成功したほか、テレメトリデータを活用した高度な脅威検出の有効性が確認された。なお、本システムは今後、ハードウェア故障の予測機能を追加するほか、商業宇宙システムへの適用拡大を目指し、宇宙分野における包括的なセキュリティ基盤の構築を企図しているものの、具体的な実施時期は示されていない。

[23] NOAA-20 と NOAA-21 は、アメリカ海洋大気庁(NOAA)と NASA が共同で運用する極軌道環境観測衛星(JPSS: Joint Polar Satellite System)の一部である。これらの衛星は、地球環境の観測や気象予測、災害対応支援のための重要なデータを提供している。



出所）Aerospace, Space Threat and Risk Detection and Reporting https://aerospace.org/sites/default/files/2024-11/Detection%20and%20Reporting%20System%20%28DARS%29.pdf（閲覧日：2025 年 2 月 19 日）

図 3-5 DARS によるコマンド受信機への干渉の検出例

13）日本：Japan Space ISAC の設立

2024 年 11 月（登記完了は 2024 年 12 月）、宇宙事業者で構成する非法人コミュニティ「スペースセキュリティ勉強会」を母体とし、より積極的かつ宇宙業界の発展に寄与するサイバーセキュリティ等に関する情報交換のため、ISAC 機能（Information Sharing and Analysis Center）を有する社団法人として、一般社団法人 Japan Space ISAC が設立した。国内の宇宙業界における広範なセキュリティ課題等を解決するために、現状では、勉強会の開催やコミュニティ運用を行っているほか、将来的には脅威情報等に関する情報共有・分析機能を提供することが発表されている。

14）米国ホワイトハウス：国家のサイバーセキュリティにおけるイノベーションの強化と推進に関する大統領令の発表

バイデン大統領は、退任前の 2025 年 1 月 16 日に、国家のサイバーセキュリティを改善するための行動を指示した大統領令「Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity」を発表した。大統領令では、敵対国や犯罪者による米国政府や企業、国民を標的としたサイバー攻撃によって、米国の国家安全保障上の脅威が生じているなどと指摘しつつ、特に中国については、最も活動的で常習的な米国のサイバーセキュリティ上の脅威だと位置づけた。この背景に基づき、以前の大統領令及び国家サイバーセキュリティ戦略をさらに加速させる目的で、本大統領令では、以下に関する取組方針が示されている。

- ランサムウェア攻撃者を含むサイバー攻撃者への制裁の実効性強化
- ソフトウェア安全性の強化
- 何十億ドルものサイバー犯罪への対抗、米国民のオンラインセキュリティの確保
- AI を活用したセキュリティの推進
- 政府のサイバーセキュリティ対策に関する官僚主義及び無駄の削減
- 米国消費者の安全の維持

- 連邦政府システムのセキュリティ向上
- 宇宙システムに対する脅威からの防衛
- ポスト量子技術の導入促進

このうち、「宇宙システムに対する脅威からの防衛」に関する具体的な指示内容は以下のとおりであり、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・更新等、宇宙セキュリティに関する内容が含まれる。

- Sec.3-(e)-(i)　本命令の日付から 180 日以内に、内務長官、商務長官、NASA 長官は、それぞれ連邦調達規則(FAR)の民間宇宙契約要件を検討し、民間宇宙サイバーセキュリティ要件及び関連契約文言の更新を FAR 審議会及びその他の適切な機関に勧告すること。推奨されるサイバーセキュリティ要件及び契約条項は、新たな民間宇宙システムすべてに対して、リスクベースの段階的アプローチを用いること。また、要件は、最低限、民間宇宙システムの軌道上セグメント及びリンクセグメントに適用されるよう設計されるものとし、少なくとも最もリスクの高い段階においては、以下の要素を含むこと:
  (A) バックアップ又はフェールオーバーシステムを含む、民間宇宙システムの指令及び制御の保護を、以下の方法により行う:
    (1) 通信の機密性を保護するためのコマンドの暗号化
    (2) コマンドが転送中に変更されないことの確保
    (3) コマンドの送信元が権限のある当事者であることの確保
    (4) 権限のないコマンド及び制御の試みの拒否
  (B) 異常なネットワーク又はシステム活動の検出、報告、回復のための方法の確立
  (C) NIST SSDF[24]又はその後の文書に準拠した、安全なソフトウェア及びハードウェア開発手法の使用
- Sec.3-(e)-(ii)　FAR 審議会は、(e)-(i)に基づき作成された推奨契約条項の内容を検討し、適用法に合致する場合、FAR 審議会の各機関のメンバーは共同で FAR を改正するための措置を講じること。
- Sec.3-(e)-(iii)　本命令の日付から 120 日以内に、国家サイバー長官(NCD)は、連邦文民政府機関(FCEB 機関)が所有、管理、運用する宇宙地上システムに関する調査結果を行政管理予算局(OMB)に提出すること。この調査結果には、以下の内容を含めること:
  (A)宇宙地上システムのインベントリ
  (B)各宇宙地上システムが、44 U.S.C. 3505(c) で定義された「主要情報システム(major information system)」に分類されているかどうか
  (C)各宇宙地上システムのサイバー防御と監視を改善するための勧告事項
- Sec.3-(e)-(iv)　OMB 長官は、(e)-(iii)に記載された調査結果の提出から 90 日以内に、FCEB 機関が所有、管理、運用する宇宙地上システムが、OMB が発行した関連するサイバー

[24] Secure Software Development Framework の略。https://csrc.nist.gov/projects/ssdf

セキュリティ要件に準拠していることを保証するための適切な措置を講じること。

- Sec.8-(c)　宇宙に関する安全保障システム(NSS)を新興の脅威に対応するサイバーセキュリティ対策で保護するために、本命令の日付から 210 日以内に、国家安全保障システム委員会(CNSS)は宇宙システムのサイバーセキュリティに関する関連政策及び指針を適宜見直し、更新すること。適切な更新に加えて、CNSS は、連邦政府が調達した宇宙 NSS において、侵入検知、セキュアブートのためのハードウェア・ルート・オブ・トラストの使用、セキュリティパッチの開発・展開の観点でサイバー防御を実施するための適切な要件を特定し、対処すること。

(Sec.は、大統領令におけるセクション番号を意味する。)

15)米国国家宇宙会議等:米国宇宙産業界へのサイバーセキュリティに関する調査結果の発表

2025 年 1 月、米国国家宇宙会議等は、米国宇宙産業界に実施したサイバーセキュリティに関する調査結果を発表した。本調査結果は、米国内や国際的に実施されたワークショップを介し、宇宙関連企業 125 社・約 300 名の意見を踏まえて作成されたもので、現行の政府のセキュリティ要件、脅威に対する対策状況、事業者における対策の課題等について、以下のような示唆が与えられた。

- 民間及び政府が契約した宇宙システムに対するサイバーセキュリティ要件は、非常に断片的であると多くの人が認識している。現在、多くの企業は、既存のガイドラインやフレームワークの解釈に基づいて、社内のサイバーセキュリティ品質要件や機能セットを独自に開発している。
- リソースに制約のある宇宙システムについて、ミッションクリティカルな要件に適用可能なサイバーセキュリティ運用技術が不足していると、多くの人が感じている。侵入検知システムやセンサーなどの一般的な地上のサイバー防衛技術は、宇宙ミッションの展開や統合に適切なレベルの精度、リソース、保守仕様を満たしていないと、多くの人が考えている。
- 米国政府の既存のサイバーセキュリティ運用ガイドラインやフレームワークは、宇宙システムではなく、企業の IT セキュリティに幅広くに適用可能であると、多くの人が考えている。宇宙産業界の多くは、宇宙システムはユーザー、地上、データ/リンク、軌道上といった複数の相互接続されたセグメントを包含しているため、地上の重要なインフラストラクチャと比較してユニークな特性があることを認識している。
- レガシー宇宙システムにサイバーセキュリティ運用要件を遡及的に課すことや、サイバーセキュリティ機能を追加しようとすることは、あまりにも困難であると考えている人が多い。宇宙とサイバーの専門家は、レガシー宇宙システム(多くが設計予定寿命から数十年を超えて運用されている)は一般にサイバーセキュリティを考慮せずに構築されたものであるという点で、大方の意見が一致している。
- 宇宙産業のサイバーセキュリティ専門家の多くは、サイバーミッションと宇宙ミッションが切り離されていると認識している。多くの人々は、サイバーセキュリティが安全で回復力のある民間、商業、防衛の宇宙ミッションの基本であるとの理解を深めるために、文化的な転換が必要であると考えている。
- 多くの人々は、宇宙ために定義されたサイバーセキュリティ・ガイドラインを遵守するための説明

責任を強化することによって、ベースラインのサイバーセキュリティ運用衛生を改善することができると考えている。大まかに言えば、宇宙産業界は、自主的なガイドラインでは、企業が宇宙ミッションのための最低限のサイバーセキュリティ要件に投資する動機付けにはならないと報告している。

- 宇宙産業は、サイバーセキュリティ運用のベストプラクティスを積極的に開発・実施することよりも、コンプライアンスや既存の要件の解釈に、多くの時間とリソースを割いていると多くの人が考えている。宇宙産業は、コンプライアンス活動が、机上演習や侵入テストなど、サイバー脅威や脆弱性を軽減するための生産的な活動の妨げになっていると広く考えている。
- 宇宙サイバー脅威に関する情報は、一貫性がなく、時宜を逸しているほか、実用的でなく、文脈に欠け、場合によっては過剰に分類されていると多くの人が考えている。多くの宇宙企業が、サイバー脅威情報へのアクセスに大きな差があると報告している。大規模な宇宙会社と小規模な宇宙会社では、アクセスに明らかな格差があることが報告された。
- 一方で、小規模な企業の中には、宇宙ミッションの目的とサイバーセキュリティ対策との間の、リソースのトレードオフを認識しているところもある。小規模な企業ほど、宇宙システムを開発する際、安全なソフトウェア言語の使用などサイバーセキュリティ品質に対する最新のアプローチを採用する可能性が高いと回答した。しかし、資金を維持するための宇宙ミッションの基本を達成することと、サイバーセキュリティの確保との間にトレードオフがあると認識されていることから、サイバーセキュリティ機能の実装はより困難である可能性がある。
- 多くの企業が、下請企業含むソフトウェアや技術のサプライチェーンリスク管理に懸念を抱いている。宇宙産業のプライム契約者は、下請業者によってもたらされる可能性のあるサプライチェーンリスクに対し、可視性の一貫した懸念を表明する一方で、大企業が明確なサイバーセキュリティ要件を下流に伝えないことがあることを認めている。
- 多くの人々は、航空宇宙工学とコンピューター工学及びその他の関連分野の専門知識が、産業界や政府の人材に不足していると考えている。宇宙産業の代表者は、宇宙ミッションにサイバーセキュリティ設計が確実に組み込まれるように、コンピューターサイエンスと航空宇宙工学の横断的な専門知識を有する人材が重要だが、この人材が限られていることを広く認識している。

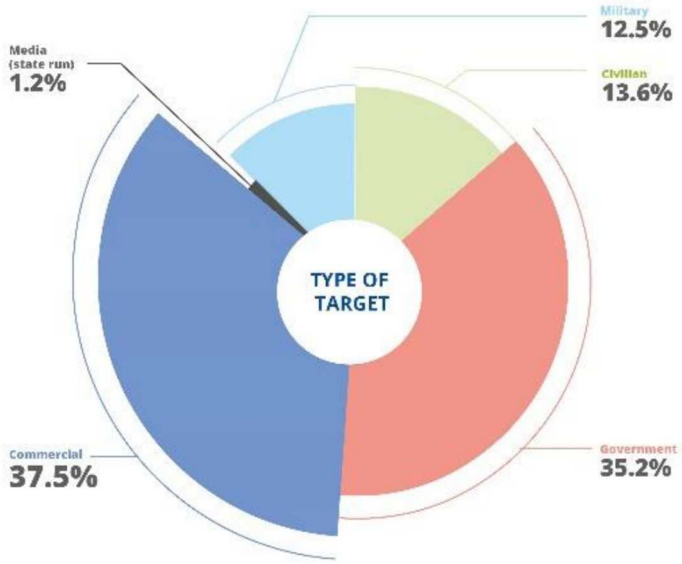
16）米国カルバート下院議員：宇宙システムを重要インフラ分野に位置づける法案の提出

2025 年 2 月、米国ケン・カルバート下院議員は、国土安全保障長官に対して、宇宙分野を重要インフラ分野に位置づけ、宇宙システム、サービス、技術を保護するためのガイダンスを発行するよう指示した法案「H.R. 1154: To direct the Secretary of Homeland Security to issue guidance with respect to space systems, services, and technology as critical infrastructure, and for other purposes」を下院に提出した。

17）EU ENISA：商用衛星におけるサイバーセキュリティ脅威や推奨事項をまとめた文書の発表

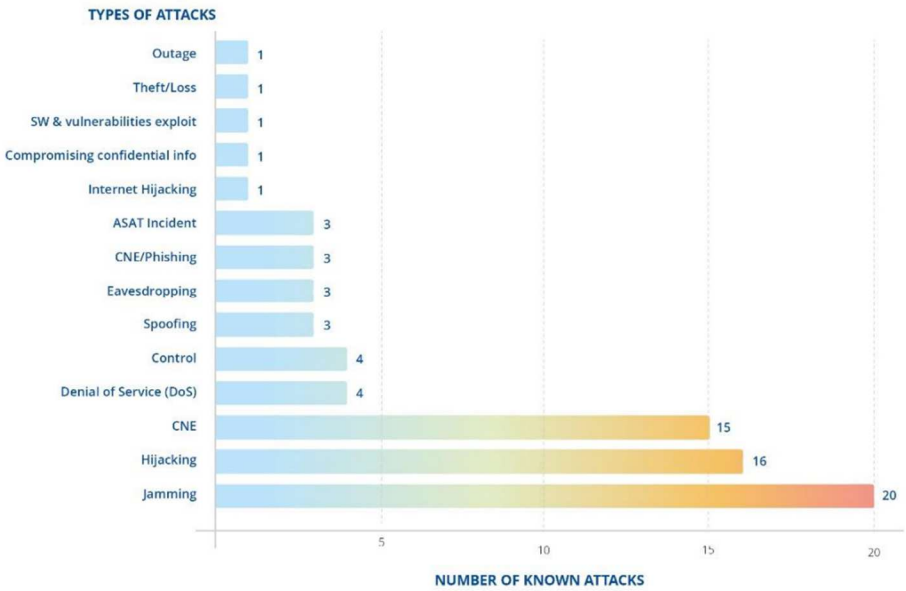
2025 年 3 月、ENISA は、商用衛星におけるサイバーレジリエンスの向上に向け、商用衛星におけ

るサイバーセキュリティ脅威を網羅的に整理したうえで、セキュリティ対策に関する推奨事項を示した文書「ENISA Space Threat Landscape 2025」を公開した。文書では、商用衛星のライフサイクルや資産を整理しているほか、Space Attacks Open Database Project[25]のデータを参照し、宇宙分野において 1977 年から 2019 年の間に発生したセキュリティ脅威を統計的に示している。文書では、下図に示すとおり、商用分野を対象としたセキュリティ脅威が増加していること、脅威の種類として、ジャミングや CNE（Computer Network Exploitation）が増加していることを強調している。



出所）ENISA, ENISA Space Threat Landscape 2025 https://www.enisa.europa.eu/publications/enisa-space-threat-landscape-2025（閲覧日：2025 年 3 月 27 日）

図 3-6 宇宙分野に対するセキュリティ脅威の標的カテゴリ（1977 年～2019 年）



出所）ENISA, ENISA Space Threat Landscape 2025 https://www.enisa.europa.eu/publications/enisa-space-threat-landscape-2025（閲覧日：2025 年 3 月 27 日）

図 3-7 宇宙分野に対するセキュリティ脅威の種別（1977 年～2019 年）

[25] https://www.spacesecurity.info/en/space-attacks-open-database/

ENISA の文書では、これまでに発生したセキュリティ脅威等を踏まえ、商用衛星に対する脅威として、以下の脅威カテゴリを挙げ、各カテゴリにおける詳細な脅威を列挙している。

- 悪質な行為/不正使用（Nefarious Activity/Abuse）：ICT システム、インフラ、ネットワークを標的に、盗用、改ざん又は破壊することを目的とした意図的な悪意ある行為
- 盗聴/傍受/乗っ取り（Eavesdropping/Interception/ Hijacking）：第三者の通信を、同意なく傍受、妨害又は制御を奪う行為
- 物理的攻撃（Physical Attacks）：インフラ、ハードウェア、相互接続などの物理的資産を破壊、暴露、改ざん、無効化、盗難又は不正アクセスを試みる行為
- 不慮の損害（Unintentional Damage）：財産又は人に対する破壊、損害、傷害を引き起こし、結果として機能不全や有用性の低下をもたらす行為
- 障害又は機能不全（Failures or malfunctions）：資産（ハードウェア又はソフトウェア）の部分的又は完全な機能不全
- 停止（Outages）：予期せぬサービスの中断、又は要求レベルを下回る品質の低下
- 災害（Disaster）：大きな損害や人命の損失を引き起こす突発的な事故・自然災害。
- 法的措置（Legal）：行動を禁止したり損失を補償したりすることを目的とした第三者による措置

文書では、脅威に対するリスク評価の例として、複数のシナリオにおけるリスク分析結果を示しているほか、それぞれの脅威に対して想定されるセキュリティ対策が網羅的に整理されている。対策は、以下の 18 のクラスターに分類される合計 125 個が挙げられている。

- ポリシーと手順（Policies and procedures）
- コンプライアンス（Compliance）
- リスク管理（Risk management）
- セキュリティ・バイ・デザインとセキュリティ・バイ・デフォルト（Security by Design and by Default）
- 環境及び物理的なセキュリティ（Environmental and Physical security）
- ネットワークセキュリティ（Network security）
- データセキュリティ（Data security）
- 脆弱性管理（Vulnerability management）
- アクセス管理（ゼロトラスト）（Access management(zero trust)）
- 資産管理（Asset management）
- サプライチェーン管理（Supply Chain management）
- 監視とアラート（Monitoring and Alerting）
- インシデント対応（Incident Response）
- 事業継続管理／災害復旧（Business Continuity Management/Disaster Recovery）
- キャパシティ・ビルディング（Capacity building）
- テスト（Testing）
- 継続的改善（Continuous improvement）
- 防衛能力（Defence capabilities）

合計 125 個の網羅的な対策は既存の標準やガイドライン等をベースに整理されており、参照先のガイドラインとして、経済産業省の「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」も挙げられている。特に重要な推奨事項として、脆弱性情報をタイムリーに把握するための情報共有・報告を行うこと、セキュリティ・バイ・デザインとセキュリティ・バイ・デフォルトに基づく最低限の標準を導入すること、サプライチェーン・ライフサイクル全体を通じてより厳格な管理を実施するために NIS2 指令に規定されたセキュリティ対策を講じること、製造環境にコンポーネントを導入する前に分析とテストを行うこと、検証された暗号化手法を導入することが挙げられている。

3.1.2 米国・EU の重要インフラ分野における宇宙分野の位置づけに関する調査

米国・EU におけるサイバーセキュリティ政策上の重要インフラ分野に関して、宇宙分野がどのように位置づけられているかを調査・整理した。整理結果を表 3-4 に示す。

本表に記載のとおり、米国では、宇宙分野は重要インフラに指定されていない。一方、EU では、Network and Information Systems 2 Directive（NIS2 指令）の改訂により、宇宙分野が新たに重要インフラとして指定された。より具体的には、加盟国又は民間企業が所有、管理、運営する宇宙サービスの提供を支援する地上インフラ事業者のうち、中規模以上（従業員数 50 名以上、組織の年間総収益が 1,000 万ユーロ以上）の事業者（ただし、欧州電気通信法指令の対象となる通信事業者を除く）が対象となり、セキュリティリスク管理、セキュリティインシデント時の所管省庁への報告等が義務的に求められる。これらの義務を違反した場合の罰金も定められており、宇宙分野が含まれる「主要セクター」の場合、1,000 万ユーロ又は事業者の前年度世界総売上高の 2%のいずれかの高い方の罰金が科される。NIS2 指令は重要インフラにおけるセキュリティ保護に関する指令であるが、重要インフラに物理的なレジリエンス向上を求めた Critical Entities Resilience Directive（CER 指令）も存在し、CER 指令においても宇宙分野が対象に含まれている。CER 指令では、レジリエンス向上のための計画を整備すること、国が定めるリスク評価を 4 年ごとに実施すること、評価に基づいた対策を実行すること、インシデントを起こした際に定められた期限内に政府に報告をすることが求められるが、指令上においては、罰則は規定されていない。

表 3-4 米国・EU の重要インフラ分野における宇宙分野の位置づけ

国／地域	米国	EU
重要インフラ分野を規定する根拠法	・ Homeland Security Act of 2002 （2002 年国土安全保障法）	・ Network and Information Systems 2 Directive（NIS2 指令） ・ Critical Entities Resilience Directive（CER 指令）
宇宙分野の対象有無	対象ではない	対象 ※ NIS2 指令の改訂において、新たに宇宙分野が追加

国／地域	米国	EU
宇宙分野の対象事業者	―	加盟国又は民間企業が所有、管理、運営する宇宙サービスの提供を支援する地上インフラ事業者のうち、中規模以上（従業員数50名以上、組織の年間総収益が1000万ユーロ以上）の事業者
全対象分野	化学、商業施設、通信、重要製造業、ダム、防衛産業基盤、緊急サービス、エネルギー、金融サービス、食料・農業、政府サービス・施設、医療・公衆衛生、情報技術、原子炉・材料・廃棄物、輸送システム、上下水道システム	【主要セクター】エネルギー、運輸、銀行、金融市場インフラ、保健医療、上水道、下水道、デジタルインフラ、行政、宇宙 【重要セクター】郵便・配送サービス、廃棄物管理、化学薬品、食品※、製造、デジタルサービス提供者 ※ CER 指令では、「主要セクター」として位置づけられている。
備考	・ 超党派メンバーによって構成される委員会において、宇宙分野を重要インフラに指定すべきとする提言が発表されている。 ・ DHS が今後取り組むべき最優先リスク事項の一つに、宇宙システムにおけるサイバーリスクが位置づけられている。	・ EU 加盟国各国は、2024 年 10 月 17 日までに本指令に対応した国内法の整備が求められている。 ・ 対象となる「宇宙サービス」の定義は指令では示されておらず、各国法において、具体的な対象や閾値が示される。

米国では、現状では重要インフラ分野に宇宙分野が含まれていないが、官民超党派メンバーで構成される「サイバースペースソラリウム委員会2.0」が、宇宙分野を重要インフラの対象に追加することを提言する報告書を 2023 年 4 月に公開した[26]ほか、第 3.1 節 9)に記載のとおり、DHS も最優先リスク事項の一つに宇宙システムにおけるサイバーリスクを位置づけており、宇宙分野におけるサイバーリスクへの対応に向けた機運が高まりつつある。

3.2 民間宇宙事業者に対するヒアリング

民間宇宙事業者に対して「民間宇宙システムにおけるサイバーセキュリティ対策ガイドラインVer2.0」の活用状況やサイバーセキュリティ対策における課題についてヒアリング調査を行った。

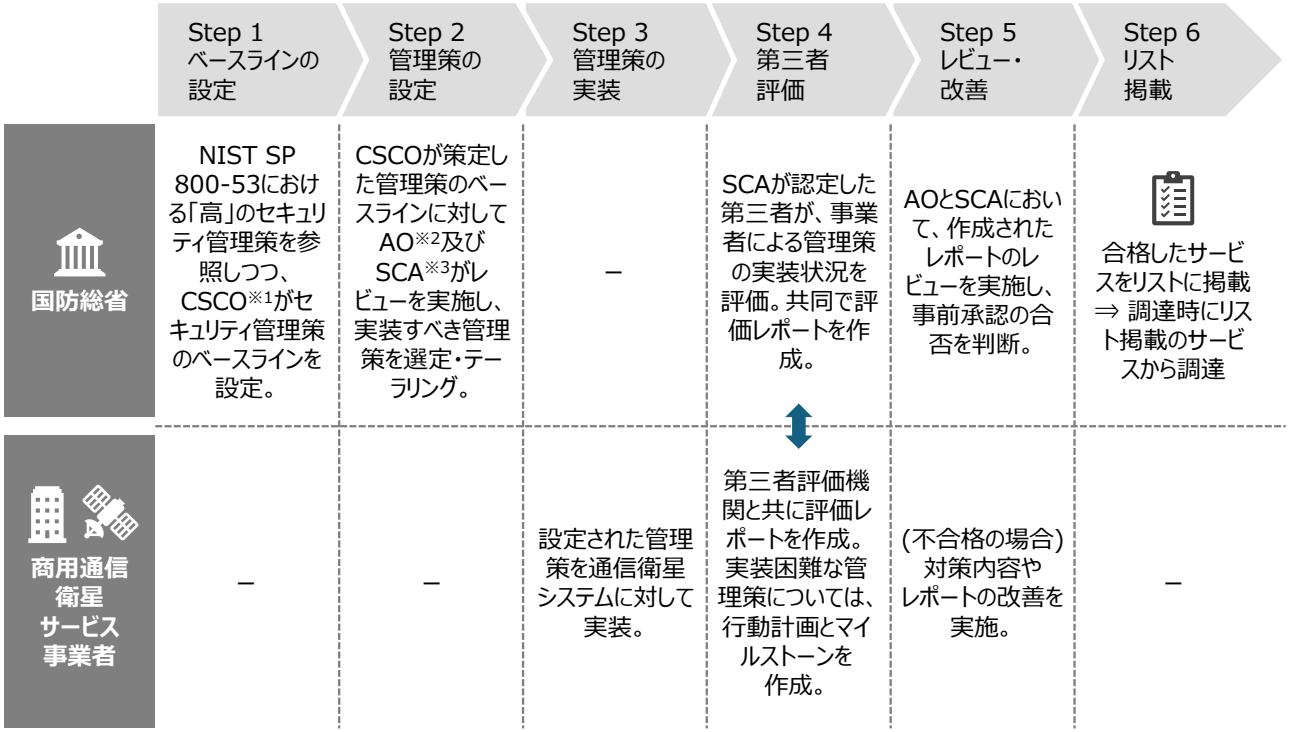
ヒアリングの結果、セキュリティ対策に関する全般的な課題として、既存ガイドライン等のカバレッジの確認が困難であることや対策の属人性に関する課題が明らかとなった。クラウド利用における課題に関

[26] Cyberspace Solarium Commission 2.0, Time to Designate Space Systems as Critical Infrastructure https://cybersolarium.org/wp-content/uploads/2023/04/CSC2.0_Report_SpaceCriticalInfrastructureSector.pdf

して、現状のリモセン法の要求事項がクラウド前提の考え方になっていないことの懸念が示された。サプライチェーン対策の課題について、統一的な基準が無いことへの懸念が示されたほか、適切なサプライヤーを選定する基準が無いことが意見された。その他の対策における課題として、衛星側でのジャミング対策が困難であるとの意見や、開発・製造環境における物理的セキュリティ対策に関する課題が示された。

また、NIST SP 800-53/171 を調達要件とした際に生じ得る課題や関連するニーズ等を聴取したところ、現状では、民間宇宙事業者が NIST SP 800-53/171 の管理策/対策要件のすべてに対して対応することは、リソース的・コスト的観点から現実的に困難であることが明らかとなった。ベースラインが示されることで取り組みやすくなる一方、テーラリング等の余地が残っていることが望ましいとの意見が挙げられたほか、システムに想定されるリスクを踏まえたリスクベースでの対策検討が必要との示唆が得られた。

民間宇宙事業者に対するヒアリングを踏まえ、NIST SP 800-53 を調達要件とする場合の調達のあり方について検討を行った。この検討に先立ち、米国における宇宙分野に関連する取組状況について調査した。宇宙分野における調達プログラムのうち、NIST SP 800-53 をセキュリティ調達要件として設定したプログラムとして、米国 DoD における IA-Pre（Infrastructure Asset Pre-Approval）のプログラムが挙げられる。本プログラムは、DoD が調達する商用衛星通信サービスを対象としたもので、2025 年 9 月までに本調達プログラムに完全移行することを目指している。IA-Pre におけるセキュリティ評価のフローは図 3-1 に示すとおりである。DoD の従来の商用衛星通信サービス調達では、同一のサービスであっても、契約ごとにセキュリティ評価を実施し、調達可否を判断していた。一方、IA-Pre では、NIST SP 800-53 に基づくセキュリティ管理策を用いて、商用衛星通信サービスごとの対策状況を事前に評価する。評価を踏まえ、対策実装状況が承認された場合、サービスリストに登録され、以後は契約の都度のセキュリティ評価が不要となる。



※1 Commercial Satellite Communications Office：宇宙軍における商用衛星通信サービス利用の統括者
※2 Authorizing Official：システム運用の承認者
※3 Security Controls Assessor：セキュリティ管理策の評価者

図 3-8 IA-Pre におけるセキュリティ評価のフロー

IA-Pre の取組及びヒアリング結果を踏まえ、宇宙システムに対するセキュリティ実装・評価に基づく望ましい調達プロセスは図 3-9 のように整理できる。ヒアリング結果を踏まえ、ベースラインの基準として NIST SP 800-53 や SP 800-171 等を設定した場合でも、対象システムの特性・リスクを踏まえ、管理策を選定・テーラリング可能とすることが望まれるほか、事業者と調達者との間でリスクのすり合わせを行ったうえで、求められる管理策を設定することが必要である。さらに、実装困難な管理策については、実装に向けた行動計画やマイルストーンの作成を求め、想定リスクに対する対応状況の評価（リスク評価）を官民連携して実施することが望ましい。

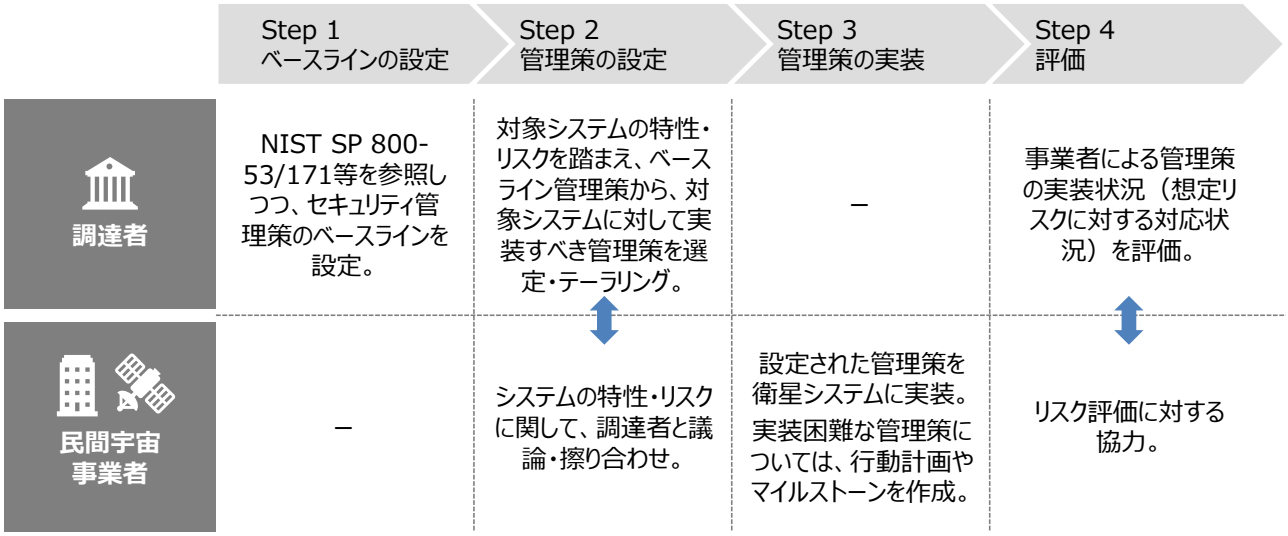


図 3-9 宇宙システムに対するセキュリティ実装・評価の取組の素案

3.3 クラウドセキュリティ要件に関する調査・分析

民間宇宙事業者のクラウドセキュリティ対策状況等を踏まえ、政府情報システムのためのセキュリティ評価制度(ISMAP)[27]が求めるセキュリティの要求内容に対して ISO/IEC 27017[28]の要件を比較・分析し、不足している部分を明らかにした。「ISMAP 管理基準マニュアル」の別紙を参照しつつ、ISO/IEC 27002 の要件を介して以下のイメージのとおり、ISMAP と ISO/IEC 27017 の要件の比較分析を行った。

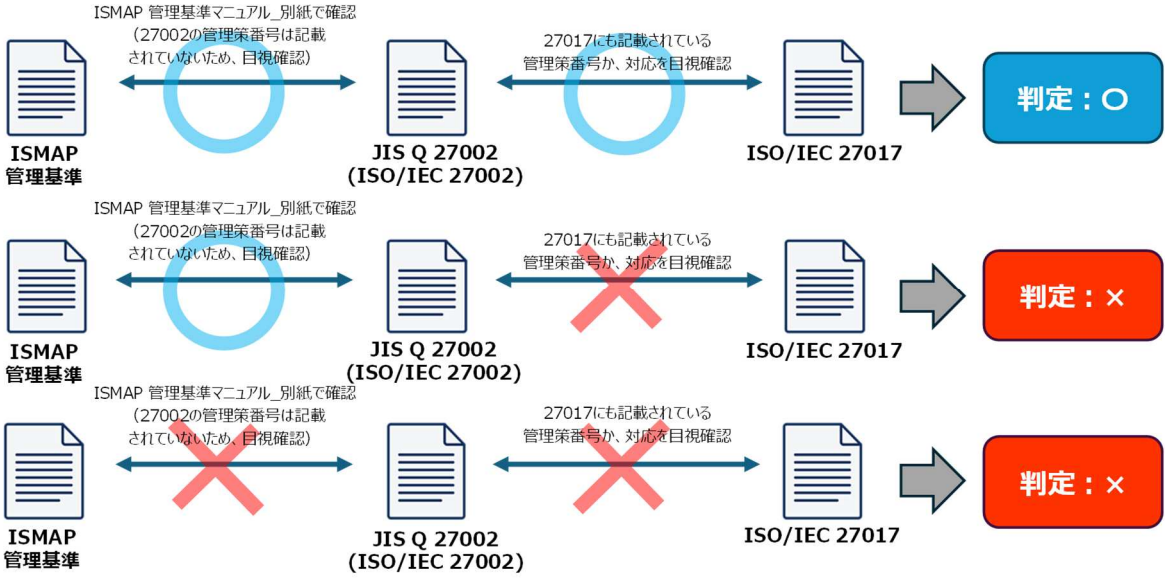


図 3-10 ISMAP 管理基準と ISO/IEC 27017 要件との比較分析

比較分析の結果、ISMAP 管理基準(第 5 章の管理策基準)のうち、「9 アクセス制御」、「11 物理的及び環境的セキュリティ」、「12 運用のセキュリティ」、「14 システムの取得、開発及び保守」、「16 情報セキュリティインシデント管理」、「17 事業継続マネジメントにおける情報セキュリティの側面」、「18 順守」の管理策項目については、概ねその内容が ISO/IEC 27017 の要件にも含まれていることが確認できた。

3.4 調査結果の総括及び今後の取組

ロシアのウクライナ侵攻における Viasat 衛星システムに対するサイバー攻撃をはじめとして、宇宙システムに対するサイバー脅威は拡大・高度化している。この状況に対し、宇宙分野のサイバーセキュリティに関する取組が国内外で進められている。特に先進的な取組を推進しているのが米国である。米国

[27] 政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、政府機関等におけるクラウドサービスの円滑な導入に資することを目的とする制度。https://www.nisc.go.jp/policy/group/general/ismap.html
[28] クラウドサービスに関する情報セキュリティ管理策のガイドライン規格。
https://www.jqa.jp/service_list/management/service/iso27017/

は、中国やロシアがサイバー脅威源であると明確に主張し、この脅威に対抗するために、第 3.1 節に示すとおり宇宙セキュリティに関する戦略文書やガイドラインが DoD、DHS/CISA 等により発表されている。また、非営利組織の Aerospace Corporation は、宇宙システムに特化した攻撃フレームワークである SPARTA や、宇宙資産に対する脅威を検出する DARS システム（第 3.1 節 5）参照）を開発するなど、宇宙分野のレジリエンス向上に向けた取組を進めている。さらに、米国の注目すべき動向として、バイデン前大統領が発表した大統領令（第 3.1 節 14）参照）が挙げられる。本大統領令では、「宇宙システムに対する脅威からの防衛」が取組の一つに位置づけられ、民間宇宙システムの政府調達に関する FAR の改定や CNSS 文書の見直し・更新等が指示されている。トランプ大統領の新政権に変わり、この大統領令の位置づけは流動的であるが、米国宇宙業界にもたらす影響は大きいと考えられ、今後も動向を注視すべきである。

米国では、宇宙分野は重要インフラとして位置づけられていない一方で、EU では、宇宙分野も重要インフラの一分野に含まれる。重要インフラに対するセキュリティ対策を義務付けた NIS2 指令[29]では、「EU 加盟国又は民間企業が所有、管理、運営する、宇宙サービスの提供を支援する地上インフラ事業者」を宇宙分野の対象事業者と定義しており、事業者がセキュリティ対策を怠った場合の罰則も規定されている。EU 全体の取組を受け、特にドイツ BSI は宇宙セキュリティに関する複数のガイドラインを発表（第 3.1 節 4）参照）するなど、積極的な取組を進めている。

国内においてもいくつかの取組が進んでおり、民間宇宙事業者は「民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン」等を活用しつつ、脅威に対抗するための対策を進めている。一方で、ヒアリングの結果、様々な対策上の課題が明らかとなった。特に注目すべき課題として、対策の属人性に関する課題、クラウド利用における課題、サプライチェーンに関する対策上の課題が挙げられる。これらの課題の解決に資する今後の取組として、以下のような取組を検討することが望まれる。

1. **対策実装例集の開発等による対策内容の具体化**
   「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」では、要求事項や対策事項のほか、それらに対する補足説明や参考情報を示しているが、事業者における効果的・効率的な対策の実装に向け、対策実装例集等を作成し、具体的な対策内容を提示することが想定される。クラウドシステムの対策やサプライチェーンに関する対策等、民間宇宙事業者が課題を抱えている技術や分野に絞って対策実装例を示すことが効果的である。

2. **官民連携の高度化と国際連携の推進**
   近年、民間宇宙事業者を支援する大型の国家プロジェクトが複数開始しており、民間宇宙事業者におけるサイバーセキュリティ対策は安全保障上も重要な位置づけとなりつつある。宇宙産業の成長を促進しつつ、宇宙活動の自立性を確保するために、サイバーセキュリティの観点においても、密な官民連携が不可欠である。情報共有の枠組みに関して、民間事業者中心の取組である「スペースセキュリティ勉強会」を母体として、宇宙分野におけるサイバーセキュリティに関する情報共有を行う「一般社団法人 Japan Space ISAC」が 2024 年 11 月に設立した。Japan Space ISAC における脅威情報の収集に資する観点から、経済産業省だけではない関係府省

[29] EU, NIS2 Directive: new rules on cybersecurity of network and information systems
https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

や国内外の関係機関との連携も進めることによって、宇宙関連事業者全体の意識向上を図ることが重要であり、また、必要に応じて、官民での対応が必要な施策等についても検討することが望まれる。また、宇宙システムに対するサイバー脅威は拡大・高度化する状況において、サイバー関連情報を適切かつ迅速に共有することが重要である。この役割を担う ISAC について、Japan Space ISAC、米国 Space ISAC、EU Space ISAC と、日米欧それぞれの国・地域で設立された状況にある。今後、グローバルな脅威ベクトルを効率的に同志国間で共有するために、ISAC 間の国際連携を推し進めることが想定される。

3. **宇宙分野におけるセキュリティ人材の確保・育成**

国内ではセキュリティ人材が不足している。宇宙産業においてもこれは同様であり、大企業であっても、セキュリティ人材が不足しているとのデータ[30]がある。今後さらにサイバー脅威が洗練化することを踏まえると、宇宙分野・セキュリティ分野の両方に長けた人材の確保・育成が必要となる。現在内閣府は「宇宙スキル標準」[31]の開発を進めており、セキュリティ対策に関連するスキルも含まれる。本スキル標準等を活用しつつ、宇宙分野におけるセキュリティ人材の確保・育成に向けた具体的施策の検討が望まれる。

4. **宇宙分野における新興セキュリティ関連技術に関する動向分析**

高度化するサイバー脅威に対し、サイバーセキュリティの技術も革新している。しかし、この技術をそのまま宇宙システムに適用することは困難な場合が多い。例えば、量子コンピューターへの耐性を有した耐量子計算機暗号（PQC）の研究開発が進められているが、この技術では、暗号計算のために多くのメモリを有することとなる。衛星システムの場合、サイズ、重量、電力の制約（SWaP 制約）により、十分なメモリを搭載できないことが想定されるため、衛星システム特有の PQC の開発が必要となる可能性もある。米国では、宇宙分野に特化したサイバーセキュリティの研究開発が積極的に進められている。Aerospace Corporation による研究開発[32]のほか、MIT の Lincoln Laboratory では、「Space Systems Cyber-Resiliency」[33]という名のイニシアチブにて、衛星システムのサイバーセキュリティに関する研究開発を行っている。将来的な脅威に対しても頑健な宇宙システムを構築し、国内宇宙活動の自立性を確保するために、引き続き、我が国産業振興への影響を注視しつつ、国内外の宇宙分野における新興セキュリティ関連技術に関する動向について情報収集を継続する必要がある。

[30] 内閣府，宇宙業界における人材関連の課題に関するアンケート結果 https://www8.cao.go.jp/space/skill/questionnaire.pdf
[31] 内閣府，宇宙スキル標準について
[32] Aerospace Corporation https://aerospace.org/cybersecurity, https://aerospace.org/software-cybersecurity, https://aerospace.org/sparta など
[33] MIT Lincoln Laboratory, Space Systems Cyber-Resiliency https://www.ll.mit.edu/r-d/projects/space-systems-cyber-resiliency

4. 全体総括

本事業では、「宇宙産業 SWG 作業部会コアメンバー会議」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、民間宇宙事業者に対するヒアリングを通じて、「民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン」の活用状況やセキュリティ対策上の課題を聴取した。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 6 年度産業サイバーセキュリティ強靭化事業

（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

2025 年 3 月

株式会社三菱総合研究所
先進技術・セキュリティ事業本部
TEL (03)6858-3578

経済産業省 御中

令和6年度産業サイバーセキュリティ強靭化事業（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

三菱総合研究所

先進技術・セキュリティ事業本部

2025 年 3 月 31 日

目次

図 目次

表 目次

1. はじめに

本調査では、2022 年 11 月に公表した「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」（以降、工場セキュリティガイドライン）と 2024 年 4 月に公表した「工場セキュリティガイドライン【別冊：スマート化を進めるうえでのポイント】」（以下「ガイドライン別冊」という）について、今後も新たなテーマを扱う別冊を追加可能とするため、構成変更を行った。また、構成変更に伴い、新規テーマの Appendix を作成した。

また、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。

工場セキュリティガイドラインの構成変更・新規の Appendix 作成・SC3 と連携した普及・啓発にあたり、経済産業省「産業サイバーセキュリティ研究会ワーキンググループ1（制度・技術・標準化）工場サブワーキンググループ（以下、工場 SWG）」を開催し、資料の取りまとめ等を実施した。

これらを通じて、工場システムにおけるサイバーセキュリティ対策を推進することを本調査の目的とした。

2. 工場等の製造現場におけるサイバーセキュリティ対策の検討

2.1 工場セキュリティに関する最新の動向と課題の調査

2.1.1 業界団体・有識者へのヒアリング・アンケート

事業者へのヒアリング(7 社)と工場セキュリティ共創セミナー(詳細は 2.3.2(1)2))の参加者へのアンケート結果より、工場セキュリティにおける課題、工場セキュリティガイドラインの課題、今後取り上げるべきテーマが確認できた。

工場セキュリティにおける課題として、経営者の理解不足・社内での推進役不足・現場のセキュリティ意識の低さなどがあげられた。また、工場セキュリティガイドラインを理解するには一定レベルの知見が必要であるという指摘が多くあった。

表 2-1 ヒアリング・アンケート結果

工場セキュリティにおける課題について	・ 経営者の理解不足・セキュリティ対策への投資不足・セキュリティ攻撃の影響度の理解不足、中小企業へ取組を拡げていく難しさがある。 ・ トップの理解不足に加えて、推進役の不在や現場の機動力不足が課題である。 ・ 工場システムを検討する自社内組織・外部委託先含めてセキュリティ意識がまだ低い。 ・ 目指すべき工場セキュリティの理想像を分かりやすく示せていない。責任と役割・全社的なスコープが明確でない。
工場セキュリティガイドラインの難易度について	・ 一定レベルの読者には読める内容だが、初学者にとってはコンサル等の支援がないと難しそうである。 ・ 一定レベルの担当者が対策を立案するときに網羅性を確認するリファレンスとしては使いやすいが、0 から対策を立案するには難易度が高い。 ・ 現状のガイドラインは汎用的な内容であり、現場に適したものに落とし込むのが難しい。
工場セキュリティの観点で取り上げるべきテーマについて	・ サプライチェーン上重要である企業は多く、経済安全保障に関する言及は必要である。 ・ 外部からの攻撃の入り口になりうるネットワーク機器は、遠隔監視において必要な機器であり、セキュリティ対策の検討が必要である。 ・ 委託を受ける組織の観点に加えて、組織の中の人員のセキュリティ意識向上も重要である。 ・ サプライチェーンの個社に、自分事化してもらうことが非常に難しい。 ・ 経済安全保障に関連するのは現状数百社しかいないが、今後、下流にまで影響がある企業が多く、懸念している。

2.1.2 工場セキュリティに関するガイドラインの調査

工場システムやセキュリティに係る政府関係機関や業界団体が好評している工場セキュリティに関する文書に関して調査した。

(1) スマート工場化でのシステムセキュリティ対策事例調査報告書

工場セキュリティ対策の実装を支援し、国内企業のスマート工場化を促進することを目的に、IPA で

は 2023 年 7 月「スマート工場化でのシステムセキュリティ対策事例調査報告書」を公表した。本報告書は、経済産業省が発行している「サイバー・フィジカル・セキュリティ対策フレームワーク」や「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」に沿った工場のセキュリティ実践例を紹介している。

表 2-2 「スマート工場化でのシステムセキュリティ対策事例調査報告書」の全体構成[1]

構成	全体概要
第 1 章 手引き作成の背景と目的	本手引きの作成の背景や目的・ねらい、構成について説明
第 2 章 侵入検知製品等の基本事項	産業用制御システム向け侵入検知製品等の導入検討を行う上でポイントとなる、侵入検知製品等の基礎知識、導入の目的と留意点、導入にあたって考慮すべき基本事項について説明
第 3 章 侵入検知製品等の導入の進め方	産業用制御システム向け侵入検知製品等の導入の進め方について、「構築」、「試験運用」、「本格運用」の各フェーズにおける検討のポイントを説明
第 4 章 侵入検知製品等の導入後の留意点	産業用制御システム向け侵入検知製品等の本格運用を開始した後に留意すべき点ついて説明
付録：本手引きで用いている主な用語の説明	本手引きで用いている主な用語の定義について説明

（2）「スマート工場のセキュリティリスク分析調査」調査報告書 第 2 版

スマート工場化を実施中、または、検討中の企業に対し、スマート工場化によって生じるセキュリティリスクを正しく認識して対策するための情報を提供することを目的に、IPA では 2024 年 10 月に「スマート工場のセキュリティリスク分析調査」調査報告書を公表した。本報告書は、スマート工場化の形態（目的、業務運用およびシステム変更内容）を類型化した実装モデルに対してセキュリティリスク分析を行い、分析結果から確認できたリスクとその対策案を紹介している。

表 2-3 スマート工場の実装モデルと内容の一覧[2]

実装モデル	内容
実装モデル 1:IoT 機器から収集した情報の利用（単一工場モデル）	単一工場内で、既存の設備や IoT デバイスから情報を収集し、生産や制御の最適化を実施することを想定したモデル
実装モデル 2:IoT 機器から収集した情報の利用（複数工場モデル）	複数の工場から、既存の設備や IoT デバイスから情報を収集し、生産や制御の最適化を実施することを想定したモデル

[1] 2023 年度 制御システムセキュリティ対策 支援活動のご紹介、IPA、https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_kojo/pdf/006_04_00.pdf をもとに三菱総合研究所が作成

[2] スマート工場のセキュリティリスク分析調査調査報告書、IPA、https://www.ipa.go.jp/security/controlsystem/ug65p90000019e7c-att/pkin3a0000002xix.pdf をもとに三菱総合研究所が作成

実装モデル	内容
実装モデル 3:遠隔からのシステム監視・制御	WAN を経由して、既設機器のプロセス値や IoT デバイスから情報を収集し、遠隔からシステムの監視や制御を行うことを想定したモデル
実装モデル 4:遠隔からの設備の保守	リモートアクセスによる接続を経由して、設備の遠隔保守をすることを想定したモデル
実装モデル 5:遠隔からのソフトウェア更新	スマート工場化にかかわる機器の内部のソフトウェア構成を収集し、必要に応じて新しいソフトウェア（脆弱性対策のためのパッチを含む）をオンラインで配布することを想定したモデル
実装モデル 6:ロボットの利用	既設設備にアドオンする形で、ロボットアームや搬送機などを追加し業務効率の改善を行うことを想定したモデル
実装モデル 7:ドローンの利用	ドローンでフィールド上の設備の異常がないかをカメラで監視し、監視記録をクラウドで経由して保存することを想定したモデル

（3） 今すぐ実践できる工場セキュリティハンドブック

JNSA では、2020 年 10 月より現場実態を考慮したセキュリティ対策の考え方や新たなサイバー対応 BCP 策定に必要な観点などを整理し、中堅・中小製造現場のセキュリティ向上を支援する目的で「今すぐ実践できる工場セキュリティ対策のポイント検討ワーキンググループ」を運営している。本ワーキンググループでは、以下の 3 部作のハンドブックの作成を進めている。2025 年 3 月現在、リスクアセスメント編、リスク対策編が公表されている。

① リスクアセスメント編
　セキュリティリスクアセスメント自らの手で実施できる参考書
② リスク対策編
　自社の環境にあったセキュリティ対策が選択・実行できる参考書
③ サイバーBCP 策定編
　従来の災害対応 BCP にセキュリティ観点を加えるための参考書

リスクアセスメント編のハンドブックは、初級者向けに工場セキュリティリスクアセスメントの概要が記載されている。検討メンバーより選定された緊急性の高い 13 個の脅威シナリオ毎に、アセスメントを簡易的に実施できるフロー図が示され、フロー図の各ステップに対応する対策の実施状況を確認することで、自社システムに対する脅威の影響度を確認できる。

リスク対策編のハンドブックは、リスクアセスメントで紹介された 13 個の脅威シナリオに対する対策の一覧が記載されている。各対策は、3 つの対策の種類（被害に遭わないための対策、被害を早期発見するための対策、被害から早期復旧するための対策）と 3 つの対策の分類（物理的対策、人的対策、技術的対策）に応じて整理されている。

2.2 工場セキュリティガイドラインの改訂

2.2.1 より効果的なガイドラインの在り方

ヒアリングやアンケートより工場セキュリティにおける課題は多岐にわたるため、今後も新たなテーマを扱う別冊を追加する可能性がある。そのため、今後も新たなテーマを扱う別冊を追加可能とするため、工場セキュリティガイドラインの構成変更を行った。

また、ヒアリングやアンケートより、ガイドライン本編は工場の規模に寄らず広く参照されるドキュメントを目指して作成したが、中小規模事業者の中には難易度が高く使いづらいとの意見が挙げられた。また、工場セキュリティにおける課題として、経営者の理解不足・社内での推進役不足・現場のセキュリティ意識の低さなどがあげられた。

政府関係機関や業界団体が公表している工場セキュリティに関する文書の調査より、中小規模事業者に対して工場セキュリティの重要性を説明する文書が確認できなかった。

そこで、経営者への理解不足や現場へのセキュリティ普及を目的に、中小規模事業者の経営層と、工場セキュリティ担当者（OT 技術には詳しくとも、IT 技術を含むセキュリティに関する知識は十分ではない従業員を想定）に向けて、必要最低限のページ数で簡潔に解説した新規 Appendix【工場セキュリティの重要性と始め方】を策定した。

2.2.2 工場セキュリティガイドラインの新たな構成

工場セキュリティガイドラインにガイドライン別冊の Step1 の一部を統合して、工場セキュリティガイドラインの Ver1.1 として更新した。工場セキュリティの基本的な考え方を示す工場セキュリティガイドラインに対して、その補足資料という位置づけで新たなテーマに関する内容を Appendix として整理した。

具体的には、ガイドライン別冊のうち、工場セキュリティガイドラインの Ver1.1 に統合しなかった部分に関しては「Appendix：スマート化を進めるうえでのポイント」として再整理した。今回の新規 Appendix である中小規模事業者向けのドキュメントに関しては、「Appendix：工場セキュリティの重要性と始め方」として整理した。

また、ガイドラインの違いが明確化されるよう、Appendix の色味を変更した。

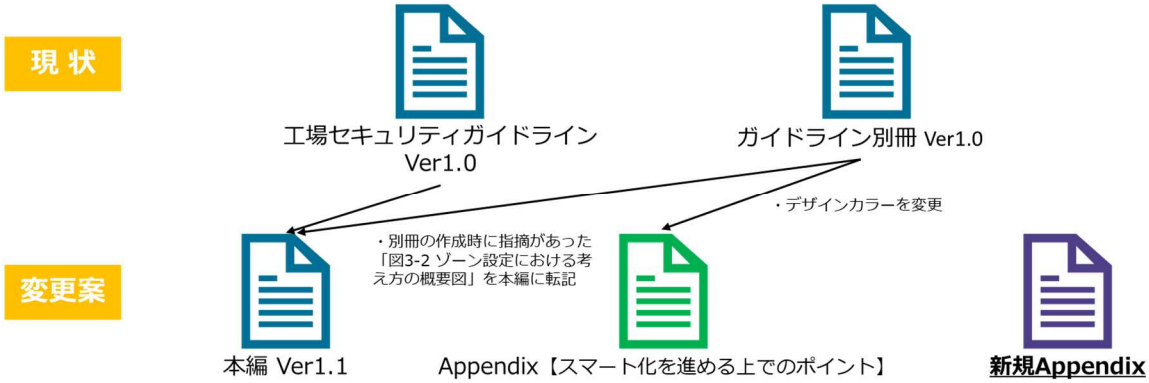


図 2-1 ガイドラインの構成変更のイメージ

2.2.3 Appendix：工場セキュリティの重要性と始め方の概要

（1） Appendix の概要

工場セキュリティガイドラインが一定レベルのセキュリティの知見を持つ読者向けであることから、より初学者向けに工場セキュリティの必要性や始め方を解説する導入文書として、Appendix を作成した。Appendix の目次を図 2-2 に示す。

「はじめに」では、Appendix の目的と中小事業者が主な想定読者であることを 1 ページで簡潔に記載した。「工場セキュリティの重要性」では、経営層向けに工場セキュリティの必要性について、被害事例を交えながら 7 ページで簡潔に解説した。「工場セキュリティの始め方」では、工場セキュリティを始めるうえでの重要な考え方を示すとともに、工場セキュリティガイドラインの STEP1 に沿って、具体的な工場セキュリティ対策に先立って実施すべき内容を示した。

図 2-2 「Appendix：工場セキュリティの重要性と始め方」の目次

（2） Appendix の英訳の作成

新規 Appendix についても、工場セキュリティガイドラインやガイドライン別冊と同様に英訳を行った。

2.3 工場セキュリティガイドラインに関わる普及・啓発の実施

2.3.1 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）と連携して、「業界連携 WG」の元「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 は、製造業におけるセキュリティ関係者を集め、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・拡充に係る情報提供、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提供などを行っている。

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や Appendix に対する意見集約を行った。

表 2-4 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提供、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・拡充に係る情報提供 ➢ 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提供 ➢ 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・自社の情報提供による、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 ・ 2024 年　ガイドライン拡充版の普及、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、関連制度等の情報提供

2.3.2 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における普及・啓発活動

1） 開催概要

日時　2024 年 9 月 24 日（火）15:00～17:30

参加人数：77 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　基調講演

経済産業省商務情報政策局サイバーセキュリティ課サイバーセキュリティ制度企画室

見次 正樹　氏

3　関連団体による工場セキュリティ普及の取組

3.1　【中小工場のセキュリティ普及の取組」はじめての工場セキュリティ（中小の工場に向けた

ガイドライン)】
一般社団法人電子情報技術産業協会(JEITA)サイバー・フィジカル・セキュリティ専門委員会　渡辺　裕之(NEC)氏

3.2　【「中小工場のセキュリティ普及の取組」はじめての工場セキュリティ(中小の工場に向けたガイドライン)】
特定非営利活動法人日本ネットワークセキュリティ協会(JNSA)西日本支部　工場セキュリティ WG リーダ　岡本　登　氏(富士通株式会社)

4　企業における工場セキュリティ取組事例

4.1　【パナソニックグループの製造システム(OT)セキュリティの取組み】
パナソニックホールディングス株式会社　松本　哲也　氏

4.2　【工場セキュリティ対策の取り組み紹介】
NEC プラットフォームズ株式会社セキュリティ・IT 統括部　森　淳子　氏

2）アンケート結果概要

セミナー参加者に対して表 2-5 の通り、講演に対するフィードバックや参加者の工場セキュリティに関する課題を把握するためにアンケートを実施した。なお、本取組は、集計を行うものではなく、個別の事例として意見を確認した。

表 2-5 セミナーに関するアンケート概要

調査項目数	15 項目
主な調査項目	A） 回答者の属性情報 B） 講演の感想 C） 工場セキュリティ推進における課題 D）「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」の認知状況 E）「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」に関する課題や今後の期待
調査手法	セミナー参加者に対して、Web アンケート調査(任意回答)
調査期間	2024 年 9 月 24 日(火)から 9 月 30 日(月)

アンケートに関する主要な結果概要は表 2-6 に示す通りである。

表 2-6 セミナーに関するアンケートの結果概要

講演の感想 (一部抜粋)	1.　基調講演について ➢　国の方向性を知ることが出来た点で良かった 2.　JEITA 講演について ➢　良い取り組みだとおもった。工場は早期事業復旧を主軸としたセキュリティ施策が必要であると考えていたので、方向性が一致し、大変参考になった。 3.　JNSA 講演について

	➢ リスクベースの考えでとても参考となった。どんな詳細リスク分析しても優先度の高いリスクは 13 種の脅威のどれかに包括される。(原子力、電力などの重要インフラ以外であれば十分に通用する内容と思う)また、サイバーBCP の基本計画書の生成 AI はとてもユニークな発想であり参考になった。特定、防御、検知、対応、復旧の中で、経営者の根底となるキーは「(早期の事業)復旧」だと思う。そのために、特定、防御、検知、対応を、資産の重要度に応じて強弱をつけ最適化することが重要である。 ➢ 中小製造業の感覚を知ることができ有益だった。サプライチェーン全体でセキュリティレベルを向上するためには中小企業のセキュリティレベルを上げることが必須である。 4. パナソニックホールディングス講演について ➢ インシデント対応の確立で現在弊社としても取り組んでいる内容などがあったので非常に参考になりました。 ➢ セキュリティのサプライヤーでもある会社の自社取り組みは興味深かった。 ➢ 製造システムのセキュリティと製品のセキュリティの組織や機能を連携させているところが参考になった。 5. NEC プラットフォームズ講演について ➢ 最先端の機器などに頼らず、基本的な内容を着実にやることの重要性が参考になった。また、少人数で社内のセキュリティ対策を推進している点も参考になった。 ➢ 管理・運用面で現実的にまずやれることから対策を実行し始めていることや、BCP の中にサイバーセキュリティ対策を取り込んだことなどが参考になった。
工場セキュリティ推進における課題 (一部抜粋)	・ 経営者の理解不足、セキュリティ対策への投資不足、セキュリティ問題による影響度の理解不足、中小企業へ取組みを拡げていくことの難しさなどを認識した。 ・ 積極的な推進役の不在が課題である。 ・ 一般的に工場は、改善(効率化)や品質に関して予算は立てやすいが、セキュリティ提案してもどこかでつまずく。経営者には BCP と紐づけた提案となるが、現場は改善や品質に紐づけた提案が必要となる。交渉相手によって見方が変わる。 ・ 工場セキュリティ推進にあたって、目指すべき工場セキュリティの理想像を分かりやすく示せていない事が課題である。どの部門がその役割を担うのかも明確になっていない。全社部門と事業所部門のスコープの境目が明確でない。 ・ トップの理解に加えて、現場の機動力をどのように高めるかが課題である。
「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」に関する課題や今後の期	・ 汎用的なものを如何に現場に適したものに落とし込めるか難しい。 ・ 現場への浸透度合いを上げて欲しい。 ・ 業界の指針ができた意義は大きい。一方、日本のガイドラインなので、グローバルにサプライチェーンが広がる製造業では、CSF、62443 等と紐付けないと海外取引先に説明し難いのではないか

待（一部抜粋）	と感じる。 ・ NIST CSF2.0 の Tier のようなガイドがあるとうれしい。

なお、2.1.1で示したように、今回のアンケート結果において、工場セキュリティ推進に関する課題としては、経営者の理解不足、社内での推進役の不在、現場におけるセキュリティ意識の低さが指摘された。特に、経営層のセキュリティ対策への投資不足や、セキュリティ問題が事業へ与える影響への認識の不足、中小企業への取り組み拡大の難しさが認識された。また、セキュリティの提案においては、経営層にはBCPとの関連性を、現場には改善・品質との関連性を訴えるなど、相手に応じた伝え方が求められるという意見もあった。さらに、目指すべき工場セキュリティの理想像が明確でなく、全社部門と事業所部門の役割やスコープの境界が不明瞭である点、現場の機動力向上も重要な課題であることが確認できた。これらの意見を踏まえ、「Appendix：工場セキュリティの重要性と始め方」では、工場セキュリティガイドラインの理解を補助する目的で、特に中小規模の製造業者における経営層およびセキュリティ担当者を主な読者と想定し、経営層向けには、工場がサイバー攻撃を受けた際の被害や実例、低コストで可能な対策を紹介し、担当者向けには、基本的な考え方から実施すべき事項までを具体的に説明している。

（2）第１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　2024 年 11 月 18 日（月）16:00～18:00
参加人数：39 名
議題

1　業界、企業における工場システムセキュリティ取組事例紹介
　1.1　【工場領域セキュリティに関する取組】
　　一般社団法人 日本自動車工業会サイバーセキュリティ分科会 工場セキュリティ課題検討タスクリーダー 嶋村 繁生 氏
　1.2　【OT セキュリティの動向調査から見える IT&OT 統合セキュリティの必要性と対策】
　　トレンドマイクロ株式会社 高橋 弘宰 氏
　1.3　【「工場に IDS が導入されない理由」を考えた NTT の IDS】
　　NTT コミュニケーションズ株式会社 秋山 和秀 氏、加島 伸悟 氏
2　ガイドライン別冊の検討内容の紹介
　【工場セキュリティガイドラインの追補について】 三菱総合研究所

（3）第２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　2025 年 2 月 12 日（水）15:00～18:00
参加人数：30 名

議題

1　業界、企業における工場システムセキュリティ取組事例紹介

1.1　【「スマート工場のセキュリティリスク分析調査報告書」第 2 版】
独立行政法人情報処理推進機構（IPA） 木下　弦　氏

1.2　【住友化学が実践する工場のサイバーレジリエンス強化に向けての取り組み】
住友化学株式会社　門田　あおい　氏

1.3　【JFE スチールにおける制御事故対応について】
JFE スチール株式会社　飯塚　禎彦　氏

2　ガイドライン別冊の検討内容の紹介
【工場セキュリティガイドラインの Appendix の概要】 三菱総合研究所

2）アンケート結果概要

SC3 工場セキュリティ共創 SWG 参加メンバーに対して、表 2-7 の通り、SC3 工場セキュリティ共創 SWG に対する期待及び、工場セキュリティに関するガイドラインや工場を含めた製造業のサイバーセキュリティ政策に関する課題と期待を把握するためにアンケートを実施した。なお、本取組は、集計を行うものではなく、個別の事例として意見を確認した。

表 2-7 SC3 工場セキュリティ共創 SWG の活動振り返りアンケート概要

調査項目数	14 項目
主な調査項目	A） SC3 工場セキュリティ共創 SWG に対する期待 B）「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン【別冊：スマート化を進める上でのポイント】」の活用状況 C） 工場セキュリティに関する課題や今後の期待 D） 工場を含めた製造業のサイバーセキュリティ政策に関する今後の期待する取組
調査手法	SC3 工場セキュリティ共創 SWG 参加メンバーに対して、 Web アンケート調査（任意回答）
調査期間	2025 年 2 月 3 日（月）から 2 月 14 日（金）

アンケートに関する主要な結果概要は表 2-8 に示す通りである。

表 2-8 SC3 工場セキュリティ共創 SWG の活動振り返りアンケート結果概要

SC3 工場セキュリティ共創 SWG に対する期待（一部抜粋）	・ 他の民間事業者や関係団体とのネットワーキングを期待する。 ・ 工場のセキュリティ対策、運用、組織体制に関する最新の知見やベストプラクティスの共有を期待する。
工場セキュリティに関する課題や今後の期待	・ 「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン【別冊：スマート化を進める上でのポイント】」

（一部抜粋）	のガイドラインのアップデート （例：工場システムの構成事例の増加、具体的な対策の例示、対策の優先度付け、対策毎の具体的な実施方法の例示、リスク分析の具体的な実施方法の提示、など）。 ・ 業種別のガイドラインの策定（例：半導体工場、化学工場、など）。 ・ 業務に応じた重要度・優先度のつけ方に関する具体的な実施方法の提示。 ・ 工場におけるセキュリティガバナンスや、工場を守るための組織体制（例：PSIRT、FSIRT）に関する検討。
工場を含めた製造業のサイバーセキュリティ政策に関する今後の期待する取組 （一部抜粋）	・ OT セキュリティ人材育成（例：サイバー演習・研修など） ・ OT セキュリティ対策の必要性の周知活動 ・ OT セキュリティに関する情報共有等を行うコミュニティ等の形成

本取組は、本年度の SC3 工場セキュリティ共創 SWG の活動を振り返り、次年度以降の取組に向けたフィードバックを得ることを目的としたものである。SC3 工場セキュリティ共創 SWG に対しては、他事業者・団体とのネットワーキングや知見の共有に対する関心が高く、次年度以降も継続的な実施が望まれている。また、工場セキュリティに関しては、対策やリスクアセスメントの具体的な実施方法に関する要望が多く寄せられており、現行のガイドラインを踏まえつつ、より実践的な手法の提示が求められている。加えて、工場のガバナンス確保や組織体制の在り方など、新たなテーマについても検討が必要である。また、製造業におけるサイバーセキュリティ政策への今後の期待される取組としては、OT セキュリティ人材の育成や、必要性喚起のための周知活動、ならびに OT セキュリティに関する情報共有を促進するコミュニティの形成など、幅広い支援策への期待が寄せられた。

3. 検討会の運営

前述の調査の実施及び取りまとめにあたって、工場等の製造現場のサイバーセキュリティに係る有識者等からなる検討会（工場SWG）の開催・運営を行った。工場 SWG の構成員は、専門的な見地からの検討、分析、助言を得ることを目的に、学識者、工場など製造現場を管理する企業、産業機械ベンダー、セキュリティベンダー、その他の事業者及び業界団体のメンバーで構成されている。また、「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別冊」の策定にあたり、工場 SWG の下に作業部会を設置し、開催・運営を行った。

3.1 工場 SWG の構成

工場 SWG の委員構成を以下に報告する。（2025 年 3 月現在）

	市岡 裕嗣	三菱電機株式会社 FA システム事業本部 DX 推進プロジェクトグループ Chief Expert
	岩﨑 章彦	一般社団法人電子情報技術産業協会 セキュリティ専任部長
（座長）	江崎 浩	東京大学大学院 情報理工学系研究科教授
	榎本 健男	一般社団法人日本工作機械工業会 技術委員会 標準化部会 電気・安全規格専門委員会委員（三菱電機株式会社 名古屋製作所ドライブシステム部 専任）
	桑田 雅彦	NEC セキュリティ株式会社 IoT/OT セキュリティユニット ディレクタ（ユニット長） （Edgecross・GUTP 合同 工場セキュリティ WG リーダ）
	斉田 浩一	ファナック株式会社 IT 本部情報システム部 部長
	佐々木 弘志	フォーティネットジャパン合同会社 OT ビジネス開発部 部長 （IPA ICSCoE 専門委員）
	斯波 万恵	株式会社東芝 サイバーセキュリティ技術センター 参事 （ロボット革命イニシアティブ（RRI）産業セキュリティ AG）
	高橋 弘宰	トレンドマイクロ株式会社 OT セキュリティ事業部 OT プロダクトマネジメントグループ シニアマネージャー
	中野 利彦	株式会社日立製作所 制御プラットフォーム統括本部 大みか事業所 セキュリティエバンジェリスト
	星野 友基	DMG MORI Digital 株式会社 品質開発管理本部 ソフトウェア運用管理部 部長
	松原 豊	名古屋大学大学院 情報学研究科准教授
	村瀬 一郎	技術研究組合制御システムセキュリティセンター 事務局長
	渡辺 研司	名古屋工業大学大学院 社会工学専攻教授

3.2 工場 SWG の運営

（1） 第 8 回会合

1）開催概要

日時　2025 年 3 月 4 日(火)15:00～16:45

場所　Teams 会議(Web 会議)

議題

1. 開会
2. 工場セキュリティにおけるガバナンスの取組について
3. ガイドラインの構成変更と新規 Appendix について
4. 工場セキュリティの普及について
5. 自由討議
6. 閉会

配付資料：

資料1　議事次第・配付資料一覧
資料2　構成員等名簿
資料3　製造業の DX について
資料4　工場におけるサイバーセキュリティガバナンスについて
資料5　リコーにおけるファクトリーセキュリティの取り組み ※投影のみ
資料6　SC3における工場セキュリティの普及活動について
～工場セキュリティ共創SWG～
参考資料1　工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン Ver1.1 ※暫定版
参考資料2　Appendix【スマート化を進める上でのポイント】Ver1.1 ※暫定版
参考資料3　Appendix【工場セキュリティの重要性と始め方】Ver1.0 ※暫定版

2）議事要旨

産業サイバーセキュリティ研究会 WG1(制度・技術・標準化)工場 SWG(第 8 回)議事要旨

日時　：令和 7 年 3 月 4 日(火)15 時 00 分～16 時 45 分

構成員　：

(座長)江崎　浩　東京大学大学院 情報理工学系研究科教授

市岡　裕嗣　三菱電機株式会社 FA システム事業本部 DX 推進プロジェクトグループ Chief Expert

岩﨑　章彦	一般社団法人電子情報技術産業協会 セキュリティ専任部長
榎本　健男	一般社団法人日本工作機械工業会 技術委員会標準化部会電気・安全規格専門委員会委員 （三菱電機株式会社名古屋製作所ドライブシステム部 専任）
桑田　雅彦	NEC セキュリティ株式会社 IoT/OT セキュリティユニット ディレクタ（ユニット長） （Edgecross・GUTP 合同 工場セキュリティ WG リーダ）
斉田　浩一	ファナック株式会社 IT 本部 情報システム部 部長
佐々木　弘志	フォーティネットジャパン合同会社 OT ビジネス開発部 部長 （IPA ICSCoE 専門委員）
斯波　万恵	株式会社東芝 サイバーセキュリティ技術センター 参事 （ロボット革命イニシアティブ（RRI）産業セキュリティ AG）
高橋　弘宰	トレンドマイクロ株式会社 OT セキュリティ事業部 OT プロダクトマネジメントグループ シニアマネージャー
中野　利彦	株式会社日立製作所 制御プラットフォーム統括本部 セキュリティエバンジェリスト （名古屋工業大学 ものづくり DX 研究所 客員教授）
星野　友基	DMG MORI Digital 株式会社 品質管理本部ソフトウェア運用管理部 部長
松原　豊	名古屋大学大学院 情報学研究科准教授
村瀬　一郎 （代理：高橋　唯）	技術研究組合制御システムセキュリティセンター 事務局長
渡辺　研司	名古屋工業大学大学院 社会工学専攻教授

議題 ：

1. 開会
2. 工場セキュリティにおけるガバナンスの取組について
3. ガイドラインの構成変更と新規 Appendix について
4. 工場セキュリティの普及について
5. 自由討議
6. 閉会

要旨 ：

1. 工場セキュリティにおけるガバナンスの取組について

・ 資料3を中野委員より説明

・ 資料 4 を株式会社リコー若杉様より説明

2. ガイドラインの構成変更と新規 Appendix について

・ 資料 5 を事務局より説明

3. 工場セキュリティの普及について

・ 資料 6 を SC3 武智様より説明

4. 自由討議

(1) ガイドラインの構成変更と新規 Appendix に関するご意見

・ スマート化のガイドライン別冊を作成する際には、本編との整合性を重視し、ダブルスタンダードを避ける工夫を行った。今回、Appendix を用いた形で全体が整理され、簡潔にまとまった。
本編の内容が充実するほど中小企業にとってのハードルが高くなるという課題があったが、新たに中小企業に向けて Appendix を設けたことは評価できる。

(2) 工場セキュリティの普及に関するご意見

・ BCP の策定率は東日本大震災以来向上しておらず、簡易版の「事業継続力強化計画」が推奨されている。サプライチェーンのリスク対応が求められる中で、サイバーとフィジカル両面の対策が中長期的に重要である。サイバーセキュリティのみを強調するアプローチでは、企業にとって優先順位が下がりかねないため、BCP の枠組みとの連携が重要である。中小企業にアプローチする際には、事業継続のために自然災害対応もサイバーセキュリティ対応も不可欠であるという考え方で、関係部局と連携しながら推進していくことが望ましい。

・ サイバーセキュリティへの取組を進める企業が増え、実践的な方法論が蓄積されつつあると感じた。中小企業に対してサイバーセキュリティの観点から直接アプローチしても、情報にたどり着けない、あるいは読まれないという課題がある。事業継続や補助金・融資制度といった企業にとって身近な経路を活用し、Appendix を普及させることが有効であると考えられる。

- セキュリティの推進に関しては、本音で語り合うことが非常に重要と考える。個社や関係者が悩みや課題を共有できる場として SC3 工場セキュリティ共創 SWG があり有効に活用してほしい。また、安全（Safety）とセキュリティ（Security）の融合、そして現場との連携は、中小企業を含め大きな課題であるため、議論を進めていけると良い。
- 中小企業に対しては、サプライチェーンを通じたセキュリティの重要性の理解促進が効果的である。企業にとっては、最終的に売上に影響する問題であり、多くの中小企業がこの必要性に気づき始めている。サプライチェーンセキュリティが今後の対策の重要な鍵となる。
- セキュリティ対策は単独の施策だけでなく、複数の取組を適切に組み合わせる必要がある。サプライチェーン全体を包括的に捉えた対策が鍵となる。

（以上）

4. 総括

本調査では、今後も新たなテーマを扱う別冊を追加可能とするため、工場セキュリティガイドラインの構成変更を行った。また、経営者への理解不足や現場へのセキュリティ普及を目的に、中小規模事業者の経営層と、工場セキュリティ担当者に向けて、必要最低限のページ数で簡潔に解説した新規Appendix【工場セキュリティの重要性と始め方】を策定した。

また、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や Appendix に対する意見集約を行った。

今後、「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」の本編及び Appendix を活用し、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 6 年度 産業サイバーセキュリティ強靭化事業

（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

2025 年 3 月

株式会社三菱総合研究所
先進技術・セキュリティ事業本部
TEL (03)6858-3578

経済産業省　御中

令和6年度産業サイバーセキュリティ強靭化事業
（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

ビル SWG 関連

三菱総合研究所

先進技術・セキュリティ事業本部

2025 年 3 月 31 日

目次

図　目次

図表目次項目が見つかりません。

表 目次

1. はじめに

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「ビルSWG」については、昨年度開催されたビルSWG会合において、情報処理推進機構（以下、「IPA」）のデジタルアーキテクチャ・デザインセンター（以下、「DADC」）で検討され、今後設立予定のスマートビルのコンソーシアムに合流する方針が決められた。これを受けて本調査では、コンソーシアム設立準備会事務局との打合せを通じて、コンソーシアムの体制や活動内容の具体化に向けた情報を収集するとともに、ビルSWGとの合流に当たって望まれる検討テーマについての助言等を実施した。

また、コンソーシアムがスマートビルディング共創機構（以下、「機構」）として2025年3月末～4月初旬の時期に設立登記を予定し、2025年3月上旬には会員募集が開始されるのにあたり、ビルSWGメンバー組織への説明会を実施した。説明会ではスマートビルディング共創機構の概要や活動開始後に想定されるビルセキュリティに関する検討テーマを共有するとともに、今後のビルSWGの検討体制は機構に設置されるセキュリティ WG となる予定であるため、ビル SWG メンバー組織に対して機構への参画を促す取組を実施した。さらにその結果を整理し、とりまとめた。

2. 設立準備会事務局との打合せ

コンソーシアムの設立に向けた検討は、2022 年より DADC の「スマートビル将来ビジョン検討会[1]」において枠組みの検討が続けられてきた。その後、2024 年 1 月には、コンソーシアムへの参画が期待される、あるいは希望する事業者・組織等を集めて、スマートビル・アソシエーション（仮）の設立準備会[2]が立ち上がり、コンソーシアムの具体的な活動目的、組織形態、組織体制、責任体制、各種活動体制（WG体制）、活動テーマ、成果目標、設立に向けた各種手続き・手順等についての検討が行われてきた。

その結果、2025年3月末～4月初旬の時期に機構として設立されることが決まっている。

本調査では、適宜メール等で設立準備会事務局とコミュニケーションを取り、検討の進捗状況についての情報収集を行うとともに、検討の節目においては直接に設立準備会事務局との打合せを行い、機構の検討状況について情報共有をいただき、機構におけるビルセキュリティの検討に向けての調整を実施した。打合せ実施の概要を以下に記す。

2.1 設立準備会事務局との打合せ①

2.1.1 開催概要

日時　2024 年 8 月 8 日 16:00-17:00
場所　Teams 会議
参加者　設立準備会事務局
　　経済産業省サイバーセキュリティ課
　　株式会社三菱総合研究所
主な論点

- コンソーシアムの概要について
- サイバーセキュリティに関する検討について
- ビルSWGメンバーへの説明について

2.1.2 議事要旨

（1） コンソーシアムの概要について[3]

- 役員（発起人）、一般会員、スタートアップ等で会費を分けることを想定している。また、大学、官公庁、地方自治体、有識者等は、無料のアドバイザー等として参加してもらうことを想定している。
- ビルSWGメンバーについては、どのように移ってもらうかを個別に検討する必要がある。要不要

[1] スマートビル将来ビジョン検討会
https://www.ipa.go.jp/digital/architecture/conferences/smartbuilding-fv/smartbuilding_conference.html
[2] スマートビル・アソシエーション（仮）の設立準備会
https://www.ipa.go.jp/digital/architecture/conferences/smartbuilding-association/launch.html
[3] 打合せ時点での検討途中の情報であり、最終的に決定されたこととは異なる点に留意

で決められるものではない。会費を払って入ってもらえることがベターだが、払えない場合の対応をどうするかは要検討である。
- ビルSWGにはグループ会社から複数の会社が個別に出席している。グループ会社枠についても検討している。

（2）サイバーセキュリティに関する検討について

- サイバーセキュリティWGは優先度が高く、初年度から活動を始める予定である。準備会において、WGでの議論として重要と思われる論点についてアンケートを取っている。
- ビルSWGにはレガシービルの関係者が多い。スマートビルのコンソーシアムのサイバーセキュリティWGに入っても、彼らにとって有意義な検討はされるのか。
- レガシービルの関係者への説明の際には、スマートビルを中心としたコンソーシアムである点を説明したうえで意思確認する必要がある。
- 実施内容としては、ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインをスマートビル編へアップデートしていくのだろう。
- データ連携に関する議論もある。レガシービルにおいてもその方向であれば検討テーマとしてプッシュできるのではないか。

（3）ビルSWGメンバーへの説明について

- コンソーシアムの設立準備会の資料はメンバー・オブザーバー限りとしているので、ビルSWGメンバーへの説明はサマリ的なものに留めて欲しい。
- ビルSWGのメンバー組織も設立準備会に参加いただいている組織は複数あるが、参加部署でいうと、サイバーセキュリティに興味のある組織がどれくらいいるかは不明である。ビル業務、不動産管理あたりの部署の人が多い印象である。
- サイバーセキュリティの議論をけん引してくれそうな会社を新たに誘うことも考えられる。あるいはセキュリティの部署の人を引っ張ってくることも考えられるだろう。

2.2 設立準備会事務局との打合せ②

2.2.1 開催概要

日時　2025 年 1 月 16 日 11:00-12:00
場所　経済産業省会議室
参加者　設立準備会事務局
　　経済産業省サイバーセキュリティ課
　　株式会社三菱総合研究所
主な論点
- 機構の設立に向けた状況について
- セキュリティWGのリーダー候補について

- セキュリティWGの活動方針について
- 今後の対応について

2.2.2 議事要旨

（1） 機構の設立に向けた状況について[4]

- 設立準備会事務局として、会員募集を前提に広く一般企業に対して説明を実施している。日程を調整してもらえれば、ビルSWGメンバーに概要説明をすることは可能である。
- ビルSWGメンバー向けの説明会は機構の活動内容が固まった後で良い。
- 会員区分は、幹事会員、一般会員（1号、2号（ベンチャー等が対象））、賛助会員（協会等の団体が対象、会費不要）である。企業は一般会員以上となる。
- 2月後半から入会案内を発出する見込みである。
- 第1回の設立総会を5月に予定しており、それまでに入会申込が間に合えば設立初年度から参加可能である。それ以降も参加は可能だが、正式な入会承認は翌年の総会になる予定である。

（2） セキュリティWGのリーダー候補について

- 各WGの主査は幹事会員である必要がある。サイバーセキュリティに関するケイパビリティやモチベーションがある方に主査になっていただきたい。
- ビルSWGメンバーのうち、数社が発起人、幹事会員となっており、その人たちがリーダーの候補となる。
- ビルSWG側から依頼等の話をすることも可能である。
- ベンダ色が強くなり過ぎないように注意する必要もある。
- セキュリティWG以外も含めてWG／SWGの全体体制は、発起人と一般幹事を含めて全体で20 名程度の座組を作ろうとしている。中核メンバーが固まったら有識者とも相談していく予定である。

（3） セキュリティWGの活動方針について

- 以下を活動内容の候補としてセキュリティWG設立時に引き継いで調整していく。
  - ビル SWG で作成したガイドラインのメンテナンス
  - 新たなガイドラインの作成（スマートビル編を想定）
  - JC-STAR のビル分野における★2以上の検討、作成
  - ビル SOC、ビル ISAC に関する議論
  - レガシービルに関する検討

（4） 今後の対応について

- セキュリティ WG のリーダー候補となるビルSWGメンバーと個別に調整する。

[4] 打合せ時点での検討途中の情報であり、最終的に決定されたこととは異なる点に留意

- ビルSWGメンバーへの機構参加についての説明会を実施する。説明内容が異なる部分があるので、基本的に準備会参加メンバーと準備会不参加メンバーで分けて実施し、なるべく全メンバーに説明できるよう複数回の説明会を設定して実施する。

3. ビルSWGへの説明会開催

機構の概要がほぼ固まりつつあった段階の 1 月 16 日の設立準備会事務局との打合せを受け、その後の設立準備会参加組織向け／一般向けの説明会と会員募集開始のタイミングに合わせて、ビル SWG メンバーへの説明会を実施した。説明会では、個人の有識者メンバーを除く法人メンバーの他、一部のオブザーバー参加企業にも説明を行った。

3.1 ビルSWG説明会

3.1.1 開催概要

日時（合計9回実施）
2025 年 2 月 27 日 16:30-17:00
2025 年 2 月 27 日 17:00-17:30
2025 年 2 月 27 日 17:30-18:00
2025 年 3 月 6 日 10:00-10:30
2025 年 3 月 7 日 13:30-14:00
2025 年 3 月 7 日 15:00-15:30
2025 年 3 月 12 日 17:00-17:30
2025 年 3 月 14 日 9:00-9:30
2025 年 3 月 14 日 17:00-17:30
場所 Teams 会議
参加者 経済産業省サイバーセキュリティ課
株式会社三菱総合研究所
ビルSWGメンバーの参加者は以下の通り

表 3-1 ビル SWG 説明会開催状況

開催日時	参加者
2025 年 2 月 27 日 16:30-17:00	一般社団法人不動産協会、中部国際空港テクニカルコネクト株式会社
2025 年 2 月 27 日 17:00-17:30	ダイキン工業株式会社
2025 年 2 月 27 日 17:30-18:00	株式会社 NTT ファシリティーズ、森ビル株式会社、三井不動産株式会社、技術研究組合制御システムセキュリティセンター
2025 年 3 月 6 日 10:00-10:30	株式会社日立製作所、三菱地所株式会社、一般社団法人ビルディング・オートメーション協会
2025 年 3 月 7 日 13:30-14:00	イーヒルズ株式会社、株式会社きんでん、日本生命保険相互会社、中部国際空港株式会社
2025 年 3 月 7 日	アズビル株式会社、株式会社日建設計

15:00-15:30	
2025 年 3 月 12 日 17:00-17:30	一般社団法人日本ビルヂング協会連合会、横浜市
2025 年 3 月 14 日 9:00-9:30	鹿島建設株式会社、三菱電機インフォメーションネットワーク株式会社
2025 年 3 月 14 日 17:00-17:30	三菱電機株式会社

※株式会社九電工、セコム株式会社は欠席

3.1.2 主な議題

- ビルSWGはスマートビルディング共創機構のセキュリティWGへ移行することの確認
- 新機構の会員種別について
- セキュリティ WG への参加について
- セキュリティ WG の活動予定
- 新機構設立に向けた今後のスケジュールについて
- 留意点

3.2 説明会実施結果とりまとめ

3.2.1 説明会参加状況

説明会への参加状況は以下の通り。

表 3-2 ビル SWG 説明会への参加状況

	説明会参加	説明会欠席
設立準備会参加メンバー	13組織	2組織
設立準備会不参加メンバー	8組織	0組織

※個人の有識者メンバー、官公庁等のオブザーバーは含まず、企業オブザーバーは含む

3.2.2 機構への参加意向の取りまとめ状況

ビル SWG 説明会参加組織のうち、説明会時点での機構への参加意向をまとめた結果は以下の通り。

表 3-3 機構への参加意向（ビル SWG 説明会参加組織）

参加意向	検討中	不参加意向（当面様子見）
14組織	2組織	5組織

4. 総括

本調査では、ビル SWG のスムーズな移行を実現するために、その受け皿となる機構について、設立に向けた検討状況、検討の結果として想定される機構の概要、ビル SWG の直接的な移行先となるセキュリティ WG の建付けや今後の検討テーマ等について、機構の設立準備会事務局からの情報収集や調整等を実施した。

また、機構の会員募集開始に合わせてビル SWG メンバー向けの説明会を実施し、移行先である機構及びセキュリティ WG の概要や計画について情報共有するとともに、引き続きビルセキュリティの議論に参加していただくために機構への参加検討を依頼した。その結果、説明会時点で不参加意向を示したのは5組織であったが、自治体及びグループ企業が参加予定の組織、ビル SWG へオブザーバー参加していた企業等であり、大部分は機構へ参加し、セキュリティ WG での議論に参加していただけるものと想定される状況である。

これまでの官主導のビル SWG での議論・活動から、民間主導の機構での議論・活動へと転換するものであり、各社が自身のビジネスと直結する立場・視点から議論をすすめ、現実的かつ地に足の着いた活動へと展開し、ビルセキュリティの着実な実施へと結びつくものと期待している。

令和6年度産業サイバーセキュリティ強靭化事業

（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

ビル SWG 関連

2025 年 3 月

株式会社三菱総合研究所
先進技術・セキュリティ事業本部
TEL (03)6858-3578

経済産業省　御中

令和6年度産業サイバーセキュリティ強靭化事業
（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

IoT 適合性評価制度関連

三菱総合研究所

先進技術・セキュリティ事業本部

2025 年 3 月 31 日

目次

図 目次

表 目次

1. はじめに

本事業では、IoT 製品に対するセキュリティ適合性評価制度となる「セキュリティ要件適合評価及びラベリング制度（JC-STAR 制度）」[1]に関して、制度の利活用に向けた調査・普及啓発を行うとともに、既存のセキュリティ関連ガイドライン類との整合性確保を行った。

制度の利活用に向けた調査・普及啓発においては、企業・組織の IoT 製品調達における制度活用に関する調査・検討を行ったほか、制度普及を目的として、「特定分野システムの IoT 製品における JC-STAR 制度活用ガイド」を作成した。

既存のセキュリティ関連ガイドライン類との整合性確保について、JC-STAR 制度に製造業者や検証事業者等が対応できるよう、国内の IoT 関連セキュリティガイドの調査を行うとともに、経済産業省が発行する「IoT 機器を開発する中小企業向け製品セキュリティ対策ガイド」及び「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」の記載内容の見直し及び改定を行った。

[1] https://www.ipa.go.jp/security/jc-star/index.html

2. JC-STAR 制度の利活用に向けた調査・普及啓発

本項目では、JC-STAR 制度の利活用に向け、制度の活用が期待される IoT 製品類型や業界団体を調査したほか、特定分野システムにおける制度普及を目的として、「特定分野システムの IoT 製品における JC-STAR 制度活用ガイド」を作成した。

2.1 制度活用が特に期待される IoT 製品類型の特定

JC-STAR 制度は、インターネットに直接接続されない製品も含め、インターネットプロトコルを使用する通信機能を持つ幅広い IoT 製品を対象としている。また、消費者向け、企業・産業向けを問わず様々な用途の IoT 製品を対象としているため、広範な分野において制度の活用が期待される。本事業では、制度の効果的な普及促進に向け、制度活用が特に期待される分野を特定した。

経済産業省の「IoT 製品に対するセキュリティ適合性評価制度構築方針」[2]に記載のとおり、本制度ではまず、政府機関等、重要インフラ事業者、地方公共団体等に対してラベル付与製品の選定・調達を働きかけるとともに、それらの IoT 製品ベンダーに本制度のラベルを取得することを促していく。したがって、政府機関等、重要インフラ事業者、地方公共団体等において調達されうる IoT 製品について、積極的な制度の活用を促していくことが望まれる。併せて、上記方針文書に記載のとおり、特定分野のシステムに組み込まれて調達される IoT 製品のうち、優先度の高いシステム（分野）において、制度の活用を促していくことが望まれる。

政府機関等や地方公共団体等における調達製品のうち、サイバーセキュリティ対策を留意すべき製品やサービスの類型としては、関係省庁で申合せがなされた「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」[3]の別紙 2 に記載の内容が参考となる。このうち、本制度の対象となる IoT 製品[4]を考慮すると、政府機関等や地方公共団体等において制度活用が期待される IoT 製品類型として、ルーター等の通信機器、ネットワークカメラ及びプリンター等の複合機が挙げられる。加えて、同様に関係省庁で申合せがなされた「政府機関等における無人航空機の調達等に関する方針について」[5]を踏まえ、ドローン等の無人航空機においても、積極的な制度活用が期待される。

特定分野のシステムにおける制度活用に関して、「IoT 製品に対するセキュリティ適合性評価制度構築方針」に記載のとおり、セキュリティ対策が十分でない IoT 製品を利用している中小企業や消費者が多いと考えられる分野のシステムや、インシデント発生時の社会的な影響が大きい重要インフラ分野のシステムの優先度が高いと考えられる。具体的な対象システムとして、スマートホームシステム、電力システム、工場システム、ビルシステム等が候補となりうる。

したがって、JC-STAR 制度活用が特に期待される IoT 製品の類型（分野）は、下表のとおり整理される。

---

2 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240823.html

3 https://www.nisc.go.jp/pdf/policy/kihon-2/IT_moushiawase.pdf

4 JC-STAR 制度では、利用者が購入後にセキュリティ機能を追加することができる PC、スマートフォン、タブレット等の汎用的な IT 製品は対象外であることに留意。

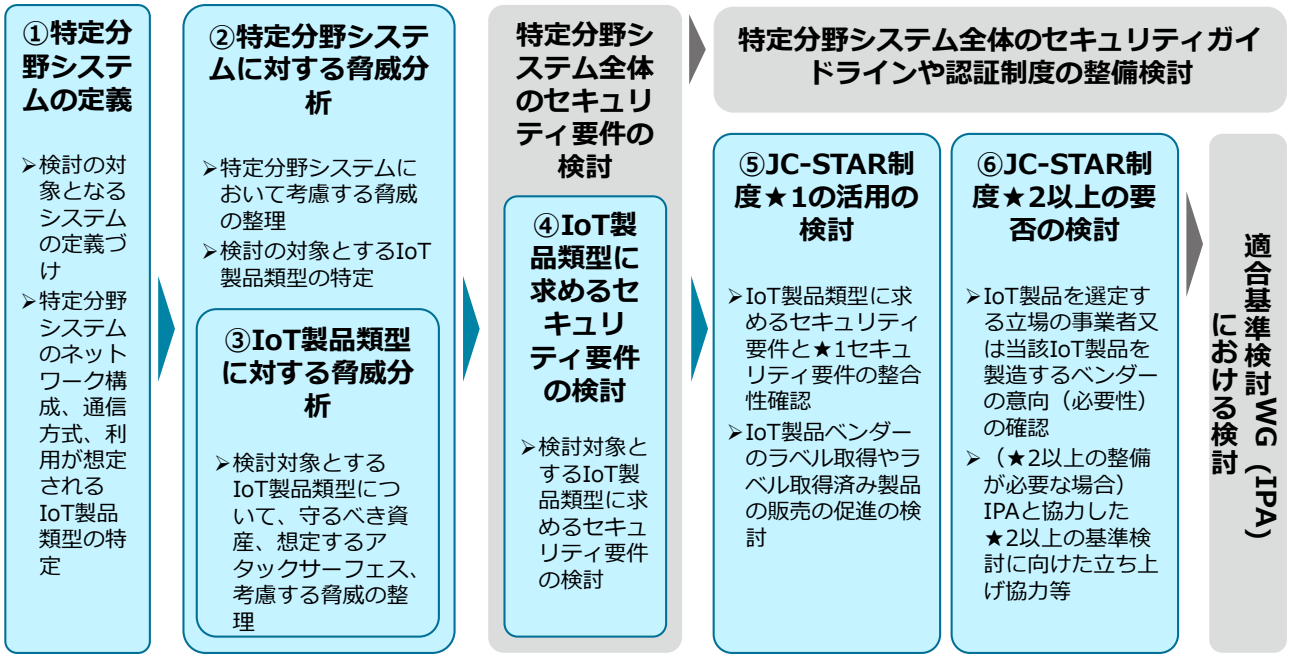
5 https://www.kantei.go.jp/jp/singi/kogatamujinki/pdf/siryou15.pdf

表 2-1 JC-STAR 制度活用が特に期待される IoT 製品類型

目的	活用が期待される IoT 製品類型
政府機関等や地方公共団体等における政府方針に従ったセキュリティ水準の IoT 製品の確実な選定・調達	・ ルーター、スイッチ等の通信機器 ・ ネットワークカメラ ・ プリンター等の複合機 ・ ドローン等の無人航空機
特定分野システムに組み込まれる IoT 製品において、一定のセキュリティ水準を満たした製品の普及促進	・ スマートホームシステムで利用される IoT 製品 ・ 電力システムで利用される IoT 製品 ・ 工場システムで利用される IoT 製品 ・ ビルシステムで利用される IoT 製品

2.2 「特定分野システムの IoT 製品における JC-STAR 制度活用ガイド」の作成

特定分野システムにおける制度普及を目的として、「特定分野システムの IoT 製品における JC-STAR 制度活用ガイド」を作成した。「特定分野システム」とは、特定の分野や業界において類似の汎用的な構成で利用されるシステムを指し、具体例としては、スマートホームシステム、工場システム、ビルシステム等が挙げられる。ガイドでは、IoT 製品が組み込まれている特定分野システムのセキュリティを検討している業界団体やワーキング・グループ（WG）などを想定読者と位置づけている。想定読者に対し、特定分野システムに組み込まれて調達・利用されるような IoT 製品に対するセキュリティ要件を定め、JC-STAR 制度の活用を検討する際に参考となる情報を提供している。具体的には、図 2-1 に示すように、特定分野システムにおける IoT 製品セキュリティ要件検討の流れを整理したうえで、それぞれのフェーズで参考となる情報を提供している。



※ ガイドで概説している部分は水色の①～⑥である。

図 2-1 特定分野システムにおける IoT 製品セキュリティ要件検討の流れ

作成したガイドは、経済産業省の HP で公開されている[6]。

6 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20241106.html

3. IoT 開発・検証に関するセキュリティ関連ガイドライン類との整合性確保

本項目では、JC-STAR 制度に製造業者や検証事業者等が対応できるよう、国内の IoT 関連セキュリティガイドの調査を行うとともに、経済産業省が発行する「IoT 機器を開発する中小企業向け製品セキュリティ対策ガイド」及び「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」の記載内容を見直し、改定を行った。

3.1 IoT 開発・検証に関する既存のセキュリティ関連ガイドラインの調査

国内関係機関が発表する IoT 開発・検証に関する既存のセキュリティ関連ガイドラインについて調査を行った。調査結果を表 3-1 に示す。

表 3-1 IoT 開発・検証に関する既存のセキュリティ関連ガイドラインの一覧

文書タイトル	発行者	発行年	最新更新年	位置づけ（スコープ）	目的	対象	主な記載内容
IoT セキュリティガイドライン ver 1.0	IoT 推進コンソーシアム、総務省、経済産業省	2016 年	-	全般	IoT 機器やシステム、サービスについて、その関係者がセキュリティ確保等の観点から求められる基本的な取組を、セキュリティ・バイ・デザインを基本原則としつつ明確化すること	・ IoT 機器・システム、サービスの供給事業者の従業員及び経営者 ・ IoT 機器・システム、サービスの利用者	・ IoT セキュリティ対策の指針及び要点 ・ 一般利用者のためのルール
つながる世界の開発指針	IPA	2016 年	2017 年	設計・開発フェーズ	IoT 製品の開発時に考慮すべき安全安心に関わる事項を指針として示すこと	・ 機器やシステムに関わる企業の開発者（主な対象読者） ・ 機器やシステムの開発に関わる企業の経営者 ・ 機器やシステムの開発に関わる企業の保守者	・ IoT 製品の開発時に考慮すべき安全安心に関わる事項

文書タイトル	発行者	発行年	最新更新年	位置づけ（スコープ）	目的	対象	主な記載内容
IoT 機器を開発する中小企業向け製品セキュリティ対策ガイド	経済産業省	2024 年	2025 年 ※ 本事業にて改定	全般 （中小企業）	IoT 製品のセキュリティ対策を行おうとする中小企業をはじめとした企業が、対策の第一歩として取り組むべきことを示すこと	・ IoT 機器等を開発する中小企業の経営者 ・ IoT 機器等を開発する中小企業のセキュリティ担当者・開発担当者・品質管理者	・ 各ライフサイクルフェーズで求められる対策
IoT 開発におけるセキュリティ設計の手引き	IPA	2016 年	2024 年	設計・開発フェーズ	IoT のセキュリティ設計を担当する開発者に参考となる情報を示すこと	・ IoT のセキュリティ設計を担当する開発者	・ 脅威分析・対策検討・脆弱性への対応方法
脆弱性対処に向けた製品開発者向けガイド	IPA	2020 年	-	方針・体制構築フェーズ、設計・開発フェーズ、運用・保守フェーズ	製品開発者がセキュリティ対策として実施すべき項目や一般消費者に自組織の取組状況をアピールするためにすべきことを把握できるようにすること	・ 対象製品（一般消費者が利用するようなインターネットやホームネットワーク等のネットワークに接続する機器）の開発を行う事業者（主に中小規模）の製品開発者	・ 製品開発者が実施すべき脆弱性対処 ・ 脆弱性対処の実施内容の開示方法

文書タイトル	発行者	発行年	最新更新年	位置づけ（スコープ）	目的	対象	主な記載内容
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	2021 年	2025 年 ※ 本事業にて改定	検証フェーズ	セキュリティ検証サービスの高度化	・ 検証のマネジメントを行う担当者 ・ 検証の実務に係る担当者 ・ IoT 機器の開発責任者 ・ IoT 機器の開発・品質保証、検証、セキュリティ担当者 ・ IoT 機器の設計・構築の担当者 ・ IoT 機器のサプライチェーン管理に係る担当者	・ IoT 機器のセキュリティ検証において検証サービス事業者が実施すべき事項 ・ より良い検証サービスを受けるために検証依頼者が実施すべき事項や持つべき知識 ・ 検証サービス事業者・検証依頼者間の適切なコミュニケーションのために二者間で共有すべき情報や留意すべき事項
つながる世界の品質確保に向けた手引き	IPA	2018 年	-	設計・開発フェーズ	開発段階での品質の作り込みと保守・運用での品質の維持・改善に向けた考慮ポイントを示すこと	・ 開発・保守時のテストのプロジェクト管理者 ・ 開発・保守時のテスト担当者 ・ IoT 機器・システムの運用に関するプロジェクト管理者 ・ IoT 機器・システムの運用担当者	・ 開発部門が作成した要求仕様や開発要件などの妥当性確認やテスト設計、テストの実施及び検証・評価に関するマネジメントの考慮事項 ・ リリース後に発生する様々な変化や IoT 機器の故障、セキュリティ問題などに対応するための品質視点の考慮事項

3.2 経済産業省が発行するガイドラインの改定

表 3-1 に示したセキュリティ関連ガイドラインのうち、経済産業省が発行する「IoT 機器を開発する中小企業向け製品セキュリティ対策ガイド」及び「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 制度に製造業者や検証事業者等が対応できるよう、記載内容の改定を行った。各文書の改定概要を表 3-2 に示す。

表 3-2 経済産業省が発行するガイドラインの改定概要

文書名	改定概要
IoT 機器を開発する中小企業向け製品セキュリティ対策ガイド	・ IoT 製品に対して一定のセキュリティ対策を進めている中小企業において、より高いレベルのセキュリティ対策として、JC-STAR のラベル取得が望まれることを明記した。 ・ JC-STAR 制度の概要をコラムとして追加した。 ・ 付録において、JC-STAR★1 取得に向けた「IoT 機器を開発する中小企業向け製品セキュリティ対策ガイド」の活用方法を追記した。具体的には、★1 適合基準とガイド記載事項との関係性を示すとともに、★1 準拠に向けたガイドの活用方法や自己適合宣言に関する参考情報を追記した。
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	・ JC-STAR★1 適合基準のうち、脆弱性スキャンが求められる S1.1-13 について、「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」を活用した評価に関する補足説明を追加した。

改定した文書は、経済産業省の HP で公開されている[7]。

[7] https://www.meti.go.jp/policy/netsecurity/vendor.html

4. 総括

本事業では、IoT 製品に対するセキュリティ適合性評価制度となる JC-STAR 制度に関して、制度の利活用に向けた調査・普及啓発を行うとともに、既存のセキュリティ関連ガイドライン類との整合性確保を行った。

制度の利活用に向けた調査・普及啓発として、JC-STAR 制度の活用が期待される業界団体である JBMIA、JUAV、セキュアドローン協議会と制度活用に向けた調整を行ったほか、特定分野システムにおける制度普及を目的として、「特定分野システムの IoT 製品における JC-STAR 制度活用ガイド」を作成し、公開した。

既存のセキュリティ関連ガイドライン類との整合性確保について、国内の IoT 関連セキュリティガイドの調査・整理を行った。また、経済産業省が発行する「IoT 機器を開発する中小企業向け製品セキュリティ対策ガイド」及び「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 制度との整合性確保や制度の活用促進を目的に、記載内容の見直し及び改定を行った。

令和 6 年度産業サイバーセキュリティ強靭化事業

（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

IoT 適合性評価制度関連

2025 年 3 月

株式会社三菱総合研究所
先進技術・セキュリティ事業本部
TEL (03)6858-3578

経済産業省　御中

令和6年度産業サイバーセキュリティ強靭化事業
（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 6 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

三菱総合研究所

先進技術・セキュリティ事業本部

2025 年 3 月 31 日

目次

図　目次

図表目次項目が見つかりません。

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

2024年秋に4日間にわたって開催され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・ウィークのうち、開会・基調講演・セミナー・ワークショップ・閉会式を東京にて対面で実施した。インド太平洋地域からのサイバーセキュリティ担当省庁、ナショナルCSIRTを含むサイバーセキュリティ事業者等からの受講生38名が受講した。

日米 EU 各国のサイバーセキュリティ政策や標準化の動向、産業制御システムにおけるセキュリティ規制・基準のあり方、サプライチェーンリスク・マネジメント等について、米国・EU やインド太平洋諸国ともセミナー及びワークショップ形式での国際的な議論を行うことで、諸外国の重要インフラを含む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、我が国セキュリティ政策との国際調和を図ることを目的に、産業制御システムに係るセミナー・ワークショップを 2024年11月12日と15日の 2 日間にわたり対面形式で開催した。なお、2024年11月13日及び14日に開催された産業サイバーセキュリティセンター（ICSCoE）主催のハンズオントレーニングとあわせ、全体とし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 2024（以下、サイバーセキュリティ・ウィーク）」として、全4日間のプログラムとして実施している。

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））の協力の下、2024年11月12日から15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7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らが参加しており、本年も日米 EU の様々な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 - ICSCoE によるハンズオントレーニング - CISA 及び ICSCoE によるワークショップ
(3) セミナー - 政策セミナー - サプライチェーンリスクマネジメントセミナー
(4) ワークショップ - 受講生からの発表 - ワークショップ(セクター毎の議論)

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・ウィークの主な招聘参加者(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38名である。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。インド太平洋地域からの受講生の内訳を下表に示す。

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 12 日(火)		
9:00-9:30		受付
9:40-10:00	C1	オープニングセレモニー・開会の辞
10:00-10:10		ショートブレイク
10:10-11:00	C1	基調講演
11:00-11:30		写真撮影
11:30-13:00		昼食
13:00-14:00	S1	政策セミナー
14:00-15:00	S2	サプライチェーンリスクマネジメントセミナー
15:00-15:10		ショートブレイク
15:10-17:10	W1	受講生からの発表

2 日目 ： 11 月 13 日(水)		
9:00-9:30		受付
9:30-12:00	H1	ハンズオン(JP-IPA)
12:00-13:00		昼食
13:00-17:30	H2	ハンズオン(JP-IPA)
17:30-18:00		会場移動
18:00-19:00	O1	ネットワーキングセッション

3 日目 ： 11 月 14 日(木)		
9:00-9:30		受付
9:30-12:00	H3	ワークショップ(US)
12:00-13:00		昼食
13:00-17:30	H4	ワークショップ(JP-IPA, US)

4 日目 ： 11 月 15 日(金)		
9:00-9:40		受付
9:30-12:00	W2	ワークショップ(セクター毎の議論)
12:00-13:30		昼食
13:30-14:00		施設見学受付
14:00-15:30	O1	施設見学(IPA)
15:30-16:00		ブレイク
16:00-16:30	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

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. Jean-Eric PAQUET, Ambassador,EU Embassy ● 松尾 剛彦，経済産業省 経済産業審議官 ● Ms. Katherine E. MONAHAN, Deputy Chief of Mission, U.S. Embassy
基調講演	● Mr. Maciej STADEJEK, Director for Security and Defence policy of the EU, the European External Action Service ● 奥家 敏和，経済産業省 商務情報政策局担当 審議官 ● Mr. Jeff GREENE, Executive Assistant Director for Cybersecurity, CISA

1.3.2 政策セミナー／Policy Seminar

日本、米国、EU のスピーカーがサイバーセキュリティ政策と戦略について最新情報を提供した。サイバーセキュリティのレベルを高めるためには、どのようなインセンティブや規制が効果的なのか。特にデザインによるセキュリティに関連する制度は、各国でどのように取り組まれているのか。国際調和の観点から、3 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 政策&ガイドラインセミナーの講演者一覧

モデレーター	前田智美 経済産業省 商務情報政策局 サイバーセキュリティ課 課長補佐
講演者及びタイトル	1. “Cyber security strategy and policy ”, Mr. Brent McCONNELL, Senior Advisor, CISA 2. “Japan Cyber Policy Updates ”, 金田祐加子 経済産業省 国際サイバーセキュリティ 企画官 3. “STRENGTHENING EU CYBER RESILIENCENIS2 framework, Cyber Resilience Act, ECCF”, Ms. Raluca STEFANUC, Deputy Head of Unit for cybersecurity and digital privacy policy, European Commission

1.3.3 サプライチェーンリスクマネジメントセミナー／Supply Chain Risk Management Seminar

ICS サプライチェーンリスクマネジメント（SCRM）は、近年、国際的なパートナーの間で最大の課題の一つとなっている。サイバースペースを構成するシステムのサプライチェーンが複雑化・グローバル化する中、サプライチェーンの脆弱性を突いた大規模な攻撃や、産業制御システムを標的とした攻撃など、国家の安全保障のみならず、経済・社会活動に広く影響を与えかねないインフラへの攻撃が横行している。

政府も民間セクターもそれぞれ、リスクを軽減するためのサイバーセキュリティ・ガイドラインや製品・ソリューション認証を策定しようとしている。企業や組織において、セキュリティ・バイ・デザインはどのように導入されるべきなのか、取り組み事例をもとに、この問いについて議論が行われた。

（1） 講演者一覧

表 1-10 サプライチェーンリスクマネジメントセミナーの講演者一覧

モデレーター	Dr. Allan Friedman, Senior Advisor, CISA
講演者及びタイトル	1. “Railway Systems with Secure-by-design”,西澤 優里 西日本旅客鉄道株式会社 デジタルソリューション本部システムマネジメント部 2. “Software supply chain risks and Transparency through SBOM”, Dr. Allan FRIEDMAN, Senior Advisor, CISA 3. “SUPPLY CHAIN RISK MANAGEMENT: AN ENISA PERSPECTIVE”, Dr. Ioannis AGRAFIOTIS, Cybersecurity Expert at European Union Agency for Cybersecurity（ENISA）

1.3.4 受講生からの発表／Presentation from Participants

本プログラムの受講生より、以下のプレゼンテーションが行われた。

- 自己紹介
- 職業上の経歴
- 自国における取組等の報告

1.3.5 ハンズオン（JP-IPA）／Hands-on（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、OT システムを保護するために人工知能（AI）を活用する方法を学ぶ。

1.3.6 ネットワーキングセッション／Networking Session

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分かち合う交流の機会を持った。11 月 13 日のハンズオン（JP-IPA）の後に実施した。

1.3.7 ワークショップ（US / JP-IPA, US）／Workshop （US / JP-IPA, US）

本ワークショップは以下を目的として開催された。

- さまざまなセクターにわたるサイバーセキュリティの脆弱性管理の重要性、プロセス、脆弱性分析との関連性等の理解。

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

表 1-5 ワークショップ(セクター毎の議論)講演者一覧

ワークショップ（セクター毎の議論）	● 門林 雄基 奈良先端科学技術大学院大学先端科学技術研究科 教授

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。

1.3.9 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。また、受講生代表にもスピーチしていただいた。

(1) 講演者一覧

表 1-13 閉会の辞の講演者一覧

閉会挨拶	● 澤田 純 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（ICSCoE） センター長 ● 参加者代表

1.4 プログラムの総括

プログラム全体を通じ、日米 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や標準化、サプライチェーンリスクマネジメントに関する様々な取組の紹介や解説が行われた。また、ICSCoE 及び米国 CISA による実践的な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、昨年に引き続き、受講生全員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等についてのセミナー・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、演習実施結果の取りまとめと評価を実施した。

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非常に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が、最大の成果だと言うことも出来る。サイバー攻撃やその対策は日々進化をしているため、インド太平洋地域において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を拡大していくことが重要である。

令和6年度産業サイバーセキュリティ強靭化事業

（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6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

2025 年 3 月

株式会社三菱総合研究所
先進技術・セキュリティ事業本部
TEL (03)6858-3578

（様式２）

二次利用未承諾リスト

令和６年度産業サイバーセキュリティ強靭化事業（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６年度産業サイバーセキュリティ強靭化事業（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2編 P.11	図3-2	Aerospace社によってテーラリングされた管理策とCNSSI 1253管理策との関係性
第2編 P.16	図3-5	DARSによるコマンド受信機への干渉の検出例
第2編 P.20	図3-6	宇宙分野に対するセキュリティ脅威の標的カテゴリ（1977年～2019年）
第2編 P.20	図3-7	宇宙分野に対するセキュリティ脅威の種別（1977年～2019年）