経済産業省　御中

令和5年度産業サイバーセキュリティ強靭化事業
（IoT機器や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

2024年3月29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Operational Technology（以下「OT」という。）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、産業分野毎の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。

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、米国では、2022年10月にホワイトハウスにおいて、消費者向けIoT製品のラベリング制度の構築に向けた企業、団体及び政府機関間の議論が行われ、EUでは、EU市場に投入されるあらゆるデジタル製品のセキュリティ対応を義務付けるEUサイバーレジリエンス法の草案が2022年9月に発表されるなど、諸外国で制度の検討が加速している。我が国でも2022年11月から「IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会」が設置され、我が国の課題や制度の方向性について、2022年度に計3回の議論が行われている。

OTにおいては、経済産業省に設置している産業サイバーセキュリティ研究会配下の産業分野別サブワーキンググループ（SWG）や独立行政法人情報処理推進機構（以下「IPA」という。）にて、分野別のガイドラインや規程類の検討・策定を進めているほか、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・IoT・OT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うとともに、産業分野別（工場、宇宙、ビル等）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検討、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、IT・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. SBOMを導入・活用するサプライチェーンモデルの構築に向けた調査・実証
   (1) SBOMの利活用による脆弱性管理の効率化に向けた調査・実証
      ① SBOMを導入・活用した場合における効果・課題等の調査・整理
      ② SBOMと脆弱性情報等の情報の紐づけを効率的・効果的に行う仕組みの構築に向けた実証事業の実施
      ③ 調査結果の取りまとめ
   (2) ソフトウェアの利活用に係るセキュリティリスク、課題及び対応策の検討
   (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) 民間宇宙システムにおけるサイバーセキュリティ対策ガイドラインの開発・更新
   (3) 情報共有のあり方などの検討
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. IoT適合性評価制度関連
   (1) IoT機器のセキュリティ確保に向けた適合性評価制度の検討
      ① 調査
      ② 適合性評価制度の検討
      ③ 検討会の実施
5. インド太平洋地域向け日米EU産業制御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産業制御サイバーセキュリティ・ウィークの開催
6. ビルSWG関連
   (1) 検討会の運営

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見ていく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　SBOMを導入・活用するサプライチェーンモデルの構築に向けた調査・実証
第 2 編　宇宙 SWG 関連
第 3 編　工場 SWG 関連

第 4 編　IoT適合性評価制度関連
第 5 編　インド太平洋地域向け日米EU産業制御サイバーセキュリティ関連
第 6 編　ビル SWG 関連

2. 総括

SBOM 関連においては、SBOM 導入・活用に関する国内外の動向調査を行い、SBOM を活用した脆弱性管理に関わる実証を通じて、関連課題とその解決法について整理した。

また、システムやソフトウェアの開発ベンダー、ツールベンダー等の開発現場の実態、課題について整理し、ソフトウェア利活用に関わるセキュリティリスク、課題に対する解決アプローチ、今後取組むべき施策等について整理した。これらの調査・実証及び検討に当たっては、企業の現場責任者・担当者や専門家からなるソフトウェアタスクフォースにおける、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の議論を反映する形で実施している。

宇宙関連においては、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を更新し、対象となる衛星システムのスコープを拡大したほか、民間宇宙事業者が活用できるセキュリティ関連規程の雛形を追加した。また、宇宙システムのサイバーセキュリティに関する情報共有のあり方について検討を行い、民間事業者を中心とした取組と連携しつつ、より踏み込んだ内容の情報共有の実現のための検討を行った。国内宇宙事業者のセキュリティ対策を支援し、高度化するためには、まだまだ多くの検討と取組の相互作用が必要であり、将来的に求められる取組の全体像を整理すると共に、国際的な動向にも留意して、国際的な水準に劣後しない形での検討が引き続き必要であることを明らかにした。

工場関連においては、工場のスマート化によって制御システムのシステムアーキテクチャが変化し、サプライチェーンによる脅威が増すなど、工場がサイバー空間に密接に繋がる世界におけるセキュリティ対策の考え方を示した「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【別冊：スマート化を進める上でのポイント】」を取りまとめた。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、工場セキュリティの普及の場を設置する方向性で検討を行った。今後、工場システムのユーザに向けて様々なコンテンツを展開し、提供側・有識者・ユーザ側等、工場システムに関わる関係者が連携しながら工場システム・セキュリティを推進することを目指すこととしている。

IoT 適合性評価制度関連においては、IoT 機器のセキュリティを確保するための適合性評価制度の構築に向けた検討を実施した。そして、☆1 セキュリティ要件・適合基準を公開するとともに、制度構築方針案に対する意見公募を行っている。今後は、制度構築方針や☆1 セキュリティ要件・適合基準を見直すと共に、☆1 のラベル付与開始や、☆2 以上の検討を行うことが期待されており、IoT 機器のセキュリティを実効的に確保する仕組みの実現への道筋を示すことが出来た。

日米 EU-ICS 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、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取組等についてのセミナー・演習を実施することで、人材育成及び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。

ビル関連においては、今後ますます進展すると考えられるビルのスマート化の議論と歩調を合わせ、今後の検討を進めていくとの方向性を得ることが出来た。

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5年度産業サイバーセキュリティ強靭化事業

（IoT機器やソフトウェアのセキュリティ確保等に関する調査） 報告書

全体概要

2024 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5年度産業サイバーセキュリティ強靭化事業
（IoT機器や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

SBOMを導入・活用するサプライチェーンモデルの構築に向けた調査・実証

MRI 三菱総合研究所

先進技術・セキュリティ事業本部

2024年3月29日

目次

図 目次

表 目次

1. SBOM の利活用による脆弱性管理の効率化に向けた調査・実証

本項目では、特に SBOM と脆弱性情報等の情報の紐づけに着目し、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および実証事業を通じ、我が国における SBOM の普及への課題や効果等について、以下の①から③に沿って調査・実証を行いとりまとめた。

① SBOM を導入・活用した場合における効果・課題等の調査・整理
② SBOM と脆弱性情報等の情報の紐づけを効率的・効果的に行う仕組みの構築に向けた実証事業の実施
③ 調査結果の取りまとめ

1.1 SBOM を導入・活用した場合における効果・課題等の調査・整理

SBOMと脆弱性情報等の情報の紐づけに着目し、効率的・効果的な脆弱性管理を行うための手法を検討し、得られる効果、メリットに加え、規制、課題、リスク、懸念点及びそれらへの対策等について調査・整理を行った。

1.1.1 国内外の動向調査

（1） 調査結果を踏まえた分析

後述する動向調査結果を踏まえ、SBOM 等を活用した脆弱性管理に係る規制の状況や、脆弱性管理に係る手法、効果、メリット、課題等に関する分析結果を示す。

SBOM 等を活用した脆弱性管理に係る規制に関して、政府調達ソフトウェアに対する SBOM 要件化に向けた動きがある。諸外国における要求状況の比較を表 1-1 に示す。米国では、OMB の覚書（M-22-18 及び M-23-16）に基づき、政府調達の対象となるソフトウェアベンダーに対して、Secure Software Development Framework（SSDF）に対する自己適合宣言が今後求められる。自己適合宣言において活用するフォームの概要は、本節の「（2）23）CISA：Secure Software Development Attestation Form」に示すとおりである。自己適合宣言における対応の一環として、SBOM 等を用いてコンポーネントリストの生成・維持・共有することを推奨している。また、連邦調達規則（FAR）の改正案に関するパブリックコメントが 2024 年 2 月 2 日まで実施され、改正案の一つとして、政府調達対象ベンダーに対して、SBOM を作成・維持し、SBOM に対する連邦政府機関のアクセスを許可することを要求する内容が含まれていた。FAR の改正には比較的長期間を要すると想定されるが、将来的に、政府調達対象ベンダーに対する SBOM の作成・維持・提供が義務化される可能性がある。欧州では、EU サイバーレジリエンス法に基づき、政府調達のみならず、EU に上市する製品については、少なくともトップレベルの依存関係を網羅する SBOM の作成が求められる予定である。英国[1]・

[1] 英国では、2023 年 5 月までに実施していたパブリックコメント（Call for views on software resilience and security for businesses and organizations）にて SBOM 作成・提供を求めていく可能性を示唆していたため、今後、EU サイバーレジリエンス法と同様の法案を検討する可能性がある。

豪州[2]においても、今後 SBOM 作成・提供を求めていく可能性はあり、引き続き動向を注視することが必要である。

参考として、各国における SBOM に関する要求事項の概要を表 1-1 に示す。

表 1-1 政府調達ソフトウェア等に対する SBOM の要求状況

国/地域	米国		EU	英国	豪州	【参考】日本
状況	間もなく SBOM 作成が推奨化、将来的には SBOM 作成・提供が義務化される見込み		SBOM 作成・提供を義務化する可能性あり	SBOM 作成・提供を義務化する可能性あり	将来的に SBOM 作成・提供を義務化する方針	対策の参考情報として SBOM を位置付け
根拠文書	【推奨化】 OMB 覚書（M-22-18 及び M-23-16）	【義務化】 FAR 改正案（FAR: Cyber Threat and Incident Reporting and Information Sharing）	EU Cyber Resilience Act（サイバーレジリエンス法）	現状未定 注）2023 年 2 月のパブコメにて、SBOM 作成・提供を求めていく可能性を示唆	Information Security Manual（ISM）	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
SBOM に関する内容	・ SSDF に対するベンダーの自己適合宣言を要求。 ・ SSDF の対応に関して、SBOM 等を用いてコンポーネントリストの生成・維持・共	・ SBOM を作成・維持し、SBOM に対する連邦政府機関のアクセスを許可することを要求。	・ 少なくとも製品のトップレベルの依存関係を網羅する SBOM を作成することを要求。		・ SBOM の作成し、ソフトウェアの利用者が SBOM を活用できるようにすることを要求。 ・ SSDF に関連する対策を要求。	・ サプライチェーンリスクを低減するために、SBOM を参考情報として活用可能であることを解説にて明記。 ・ SSDF に関する

[2] 2030 年までのサイバーセキュリティ戦略文書（2023-2030 Australian Cyber Security Strategy）にて、SBOM 要件を含む情報セキュリティマニュアル（ISM）を政府全体で実装していく方針を明確化しており、2030 年までに要件化される可能性がある。

国/地域	米国		EU	英国	豪州	【参考】日本
	有することを推奨。					言及はなし。
要求対象	ソフトウェア製品（OSS 等は除外）	ICT 製品及びサービス	デジタル製品（医療機器等は除外）		ソフトウェア製品	機器等

表 1-2 各国における SBOM 要求事項の概要

国・地域	取組	SBOM に関する要求事項の概要
米国	【推奨化】 OMB 覚書（M-22-18 及び M-23-16）	・ 機関[3]は、指定された期限までに、ソフトウェアベンダーが SSDF に適合していることを示す自己証明を取得する必要がある。 ・ 機関は、必要に応じて、SSDF への適合を実証する成果物をソフトウェアベンダーから入手することができる。 ➢ SBOM は、ソフトウェアの重要性に基づき、または各機関の判断により、公募要件において要求される場合がある。要求された場合、SBOM に関するリンクを機関に提供しない限り、SBOM データが機関に提供され、機関において保持されるものとする。 ➢ SBOM は、NTIA の「The Minimum Elements for a Software Bill of Materials」または CISA が発行しうる後継のガイダンスで定義されたデータ形式の一つを採用して作成されなければならない。 ➢ 機関は、他の連邦機関によって維持されているソフトウェアベンダーの SBOM 及びその他の成果物の相互性を考慮する必要がある。
米国	【義務化】 FAR 改正案	・ 連邦政府調達の請負業者は、契約の対象となるソフトウェアが最初に使用される際に、当該ソフトウェアの最新の SBOM を契約担当者に提供するか、SBOM に対するアクセス権を提供しなければならない。各 SBOM は、機械可読可能な業界標準フォーマットで作成され、次項で記載の頻度を除き、商務省が発行する「The Minimum Elements for a Software Bill of Materials」の最新版のセクション IV で特定されるすべての最小要素に準拠しなければならない。 ・ 契約の対象となるソフトウェアの一部において新しいビルドまたはメジャーリリースの更新がなされた場合、請負業者は、ソフトウェアの

[3] 44 U.S.C. § 3502(1)で定義される「機関（Agency）」を指し、連邦政府、軍関係省、行政法人、行政管理法人、政府行政部門のその他施設（大統領府を含む）、独立規制機関が含まれる。

国・地域	取組	SBOMに関する要求事項の概要
		新バージョンを反映するために、SBOMを更新し、更新されたSBOMを契約担当者に提供(またはアクセス権を提供)しなければならない。これには、更新されたコンポーネントまたは依存関係を統合するためのコンピュータソフトウェアビルドが含まれる。 ・ SBOMが基本契約レベルで契約担当者に提供されている場合、SBOMを契約ごとに契約担当者に提供する必要はない。
EU	サイバーレジリエンス法	・ EUに上市されるデジタル製品の製造業者は、製品に含まれる脆弱性とコンポーネントを特定し、文書化しなければならない。これには、少なくとも製品のトップレベルの依存関係を網羅する、一般的に使用され機械で読み取り可能な形式のSBOMを作成することが含まれる。ただし、SBOMを公開する義務を製造業者が負うべきではない。 ・ 製造業者は、SBOMを利用者に提供することを決定した場合、SBOMへのアクセスに必要な情報を利用者へ提示しなければならない。 ・ 欧州委員会は、SBOMの様式及び要素を実施法によって規定することができる。 ・ 各国の市場監視当局は、専門の行政協力グループ(ADCO)[4]によって指定される特定カテゴリのデジタル製品の製造業者に対し、SBOMの提出を求めることができるようにすべきである。
豪州	Information Security Manual (ISM)	・ 管理策ISM-1730:ソフトウェアベンダーは、SBOMを作成し、ソフトウェアの利用者に提供すること。
日本	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	・ 基本対策事項 4.3.1(1)-1 a)「原因を調査・排除できる体制」について:OEM(Original Equipment Manufacturer)によって提供される機器等についても、OEM製品の製造者においても不正な変更が加えられないよう、OEM 製品の販売者が機器等のサプライチェーン全体について適切に管理していることも含めて、要件を定めることが考えられる。また、SBOMを参考とすることも考えられる。

脆弱性管理に係る手法、効果、メリット、課題等に関して、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)を中心に、米国にて活発な検討が進められている。効果的な手法に関して、2023年 11 月に、ソフトウェアサプライチェーンのセキュリティ確保のための SBOM 利用に関するガイダンス

[4] EU サイバーレジリエンス法に基づき設置予定の専門グループであり、加盟国各国の市場監視当局と、必要であれば各単一連絡事務所の代表者を加えて構成される予定である。

文書が発表された他、2023 年 12 月には、OSS や SBOM の管理に関する推奨プラクティスをまとめた文書が発表された。また、VEX に関する手法として、2023 年 11 月に、VEX 情報を発行する組織・機能（Who）と VEX 情報が発行されるタイミング（When）の例示を整理した文書が発表されている。加えて、セキュアバイデザイン・セキュアバイデフォルトの実践に向けた推奨事項をまとめたガイダンスが、日本を含む様々な機関が共同で発表していることは注目すべき動向であり、今後、世界的にセキュアバイデザイン・セキュアバイデフォルトの重要性がより高まると想定される。

効果やメリットに関して、2023 年 8 月に CISA が発表したサイバーセキュリティ戦略（2024-2026 年度）において、CISA として「信頼できるソフトウェア製品の開発を推進する」ことの効果として、SSDF の実装を宣言する製品開発者の数が増加する等の効果を期待するといった内容が示されている。しかし、具体的な KPI は示されておらず、また、これまでの国内の実証で整理してきたようなリスク低減効果・コスト低減効果等を定量的に示した取組はない。

これまで、SBOM の作成に関する文書が米国電気通信情報局（NTIA）や CISA より多く発表されてきたが、近年は、SBOM の共有に関する文書や SBOM の利用に関する文書が発表される等、作成された SBOM を効果的に活用するための取組にシフトしてきている。CISA が主導する SBOM に関するイベントである SBOM-a-rama で議論されたとおり、作成された SBOM の品質や SBOM の共有等、SBOM の活用に当たっての方法論は諸外国でも課題と捉えているところ、国内においても、SBOM 活用に係る課題解決に資する取組推進が望まれる。

（2）各動向等の調査結果

本事業で調査対象とした諸外国政府機関等における近年の取組動向等は表 1-3 に示すとおりである。以降では各取組の概要等について示す。

表 1-3 諸外国政府機関等における取組動向等の調査対象

※ 取組日・発行日順

#	取組名・文書名	取組日・発行日	国	取組主体
1	National Cybersecurity Strategy[5]	2023 年 3 月 1 月	米国	ホワイトハウス
2	Software Bill of Materials (SBOM) Sharing Lifecycle Report[6]	2023 年 4 月 17 日	米国	CISA、DOE
3	Types of Software Bill of Material (SBOM) Documents[7]	2023 年 4 月 21 日	米国	CISA
4	Minimum Requirements for Vulnerability Exploitability eXchange (VEX)[8]	2023 年 4 月 21 日	米国	CISA

[5] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[6] https://www.cisa.gov/resources-tools/resources/software-bill-materials-sbom-sharing-lifecycle-report
[7] https://www.cisa.gov/resources-tools/resources/types-software-bill-materials-sbom
[8] https://www.cisa.gov/resources-tools/resources/minimum-requirements-vulnerability-exploitability-exchange-vex

#	取組名・文書名	取組日・発行日	国	取組主体
5	Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices[9]	2023 年 6 月 9 日	米国	OMB
6	SBOM-a-rama 2023[10]	2023 年 6 月 14 日	米国	CISA
7	Quad Cybersecurity Partnership: Joint Principles for Secure Software[11]	2023 年 6 月 26 日	QUAD（日米豪印）	QUAD 各担当政府
8	SBOM startersgids[12]	2023 年 7 月 5 日	オランダ	蘭 NCSC
9	National Cybersecurity Strategy Implementation[13]	2023 年 7 月 13 日	米国	ホワイトハウス
10	SBOM-Anforderungen: TR-03183-2 stärkt Sicherheit in der Software-Lieferkette[14]	2023 年 8 月 4 日	ドイツ	BSI
11	CISA Cybersecurity Strategic Plan FY2024 – 2026[15]	2023 年 8 月 4 日	米国	CISA
12	CISA Open Source Software Security Roadmap[16]	2023 年 9 月 12 日	米国	CISA
13	Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing[17]	2023 年 10 月 3 日	米国	DOD、GSA、NASA

[9] https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security-1.pdf
[10] https://www.cisa.gov/news-events/events/sbom-rama
[11] https://www.mofa.go.jp/mofaj/files/100509254.pdf 【日本語訳】 https://www.mofa.go.jp/mofaj/files/100509255.pdf
[12] https://www.ncsc.nl/documenten/publicaties/2023/juli/5/sbom-startersgids
[13] https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/13/fact-sheet-biden-harrisadministration-publishes-thenational-cybersecurity-strategyimplementation-plan/
[14] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03183/TR-03183_node.html
[15] https://www.cisa.gov/cybersecurity-strategic-plan
[16] https://www.cisa.gov/resources-tools/resources/cisa-open-source-software-security-roadmap
[17] https://www.federalregister.gov/documents/2023/10/03/2023-21328/federal-acquisition-regulation-cyber-threat-and-incident-reporting-and-information-sharing

#	取組名・文書名	取組日・発行日	国	取組主体
14	Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software[18]	2023 年 10 月 25 日	米国、日本等	CISA、NSA、FBI、NISC、JPCERT/CC 等
15	Software Identification Ecosystem Option Analysis[19]	2023 年 10 月 26 日	米国	CISA
16	Securing the Software Supply Chain: Recommended Practices for Software Bill of Materials Consumption[20]	2023 年 11 月 9 日	米国	NSA、ODNI、CISA
17	When to Issue VEX Information[21]	2023 年 11 月 6 日	米国	CISA
18	Joint Guidelines for Secure AI System Development[22]	2023 年 11 月 26 日	米国、英国、日本等	CISA、英 NCSC、NISC 等
19	The Case for Memory Safe Roadmaps[23]	2023 年 12 月 6 日	米国、英国等	CISA、NSA、FBI、英 NCSC 等
20	Securing the Software Supply Chain: Recommended Practices for Managing Open-Source Software and Software Bill of Materials[24]	2023 年 12 月 11 日	米国	CISA、NSA、ODNI

[18] https://www.cisa.gov/resources-tools/resources/secure-by-design?utm_source=Blog&utm_medium=CISA.gov&utm_campaign=Secure%20by%20Design%20and%20Default%20Update【日本語仮訳版】https://www.nisc.go.jp/pdf/policy/kokusai/Provisional_Translation_JP_Principles_Approaches_for_Security-by-Design-Default_October.pdf

[19] https://www.cisa.gov/resources-tools/resources/software-identification-ecosystem-option-analysis

[20] https://media.defense.gov/2023/Nov/09/2003338086/-1/-1/0/SECURING%20THE%20SOFTWARE%20SUPPLY%20CHAIN%20RECOMMENDED%20PRACTICES%20FOR%20SOFTWARE%20BILL%20OF%20MATERIALS%20CONSUMPTION.PDF

[21] https://www.cisa.gov/resources-tools/resources/when-issue-vex-information

[22] https://www.cisa.gov/news-events/alerts/2023/11/26/cisa-and-uk-ncsc-unveil-joint-guidelines-secure-ai-system-development【日本語仮訳版】https://www.nisc.go.jp/pdf/policy/kokusai/Provisional_Translation_JP_Guidelines_for_Secure_AI_System_Development.pdf

[23] https://www.cisa.gov/resources-tools/resources/case-memory-safe-roadmaps

[24] https://media.defense.gov/2023/Dec/11/2003355557/-1/-1/0/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN%20RECOMMENDED%20PRACTICES%20FOR%20MANAGING%20OPEN%20SOURCE%20SOFTWARE%20AND%20SOFTWARE%20BILL%20OF%20MATERIALS.PDF

#	取組名・文書名	取組日・発行日	国	取組主体
21	Guidance on Assembling a Group of Products[25]	2024 年 1 月 26 日	米国	CISA
22	SBOM-a-Rama Winter 2024[26]	2024 年 2 月 29 日	米国	CISA
23	Secure Software Development Attestation Form[27]	2024 年 3 月 11 日	米国	CISA

1）ホワイトハウス：National Cybersecurity Strategy

2023 年 3 月、米国バイデン大統領は、米国における国家のサイバーセキュリティ戦略を公表した。表 1-4 に示すとおり、戦略では大きく 5 つの柱が掲げられており、それぞれに対応する形で計 27 の戦略目標も示されている。なお、本戦略に基づく実施計画が 2023 年 7 月に発表された。この実施計画の内容については本節の「9）ホワイトハウス：National Cybersecurity Strategy Implementation」を参照のこと。

表 1-4 米国国家サイバーセキュリティ戦略の 5 つの柱と 27 の戦略目標

柱	戦略目標
柱 1. 重要インフラの防衛	1.1 国家安全保障と公共安全を支えるためのサイバーセキュリティ要件の確立 1.2 官民協力の拡大 1.3 連邦政府のサイバーセキュリティセンターの統合 1.4 連邦政府のインシデント対応計画やプロセスの明確化 1.5 連邦政府における防衛の近代化
柱 2. 脅威主体の破壊と解体	2.1 破壊的活動の統合 2.2 脅威主体を破壊するための官民協力強化 2.3 情報共有や被害者通知の速度と規模の拡大 2.4 米国拠点のインフラ悪用の防止 2.5 サイバー犯罪への対抗とランサムウェアの撲滅
柱 3. セキュリティとレジリエンスを促進させるための市場原理の形成	3.1 データ管理者への説明責任の付与 3.2 セキュアな IoT 機器の開発促進 3.3 安全でないソフトウェア製品とサービスに対する責任の再構築 3.4 連邦政府の補助金やその他のインセンティブを利用したセキュリティの構築 3.5 連邦政府調達を活用した説明責任の向上 3.6 連邦政府によるサイバー保険市場の支援検討
柱 4. レジリエンス	4.1 インターネットの技術的基盤の確保

[25] https://www.cisa.gov/resources-tools/resources/guidance-assembling-group-products
[26] https://www.cisa.gov/news-events/events/sbom-rama-winter-2024
[27] https://www.cisa.gov/resources-tools/resources/secure-software-development-attestation-form

柱	戦略目標
な未来への投資	4.2 サイバーセキュリティのための連邦政府研究開発の活性化 4.3 ポスト量子暗号への備え
柱 5. 共通的な目標の追求のための国際的なパートナーシップの構築	5.1 デジタルエコシステムへの脅威に対抗するための連合体の構築 5.2 国際的なパートナーの能力の強化 5.3 同盟国やパートナーを支援する米国の能力の拡大 5.4 責任ある国家行動の世界的規範を強化するための連合体の構築 5.5 情報・通信・運用技術製品及びサービスのための安全なグローバルサプライチェーンの構築

2）CISA：Software Bill of Materials（SBOM）Sharing Lifecycle Report

2023 年 4 月、米国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）と米国エネルギー省（DOE）は、SBOM 共有に関わる組織が利用可能なコスト、リソース等に基づき適切な SBOM の共有方法を選択することを目的として、SBOM の共有ライフサイクルに関するレポートを発表した。具体的には、SBOM が作成者から利用者に共有されるまでに 3 つの基本フェーズ（Discovery→Access→Transport）があるとし、各フェーズの概要とフェーズごとの洗練度合いの具体例が示されている（表 1-5）。洗練度合いは、各フェーズを実施するために必要なコスト、リソース等の相対量を表しており、低・中・高のいずれかで定義される。

表 1-5 SBOM の共有ライフサイクルにおける各フェーズの概要と洗練度合いの具体例

フェーズ	洗練度合い		
	低	中	高
Discovery SBOM 利用者が、SBOM の存在とアクセス方法を認知するフェーズ	・ SBOM 利用者が主導的に、SBOM に関する情報を取得している状態 ・ SBOM 提供者によって提示される SBOM に関するガイダンスの内容が限定的であるまたはガイダンスが存在しない状態	・ ソフトウェアのソースコード内に、SBOM の参照先が記述された状態 ・ SBOM 利用者が利用可能なリポジトリに、SBOM が配置された状態 ・ SBOM 提供者の Web サイトに、SBOM が配置、関連情報が公開された状態	・ SBOM に関する情報の認知が自動化され、SBOM 利用者への負担が軽減された状態 ・ Publish/Subscribe パターンで SBOM 利用者が認知する状態 ・ 分散型台帳の技術によって SBOM に関する情報が同期化された状態

フェーズ	洗練度合い		
	低	中	高
Access SBOM 利用者が、SBOM へのアクセス権限を得るフェーズ	・ アクセス制御が欠如した状態 ・ アクセス制御が手動で処理されている状態 ・ SBOM の提供依頼に対し、個人の判断で提供可否を判断している状態	・ SBOM 利用者が、アクセスを試行した際に、認証が求められる状態 ・ アクセス権限の粒度（例：非公開/一部公開/公開）が統一されていない状態	・ アクセス制御を、証明書を用いた公開鍵基盤等の別組織へ委任している状態 ・ アクセス権限の粒度が統一された状態
Transport SBOM 利用者が、SBOM を受け取るフェーズ	・ SBOM 提供者が利用者へ手動（電子メール等）で送信している状態 ・ SBOM が提供者から利用者へ、提供される流れは 1 対 1 である状態 ・ SBOM が口頭や郵送で提供されている状態	・ 一貫性のない、多様な手段や文書によって SBOM が提供されている状態 ・ SBOM の提供が、一部分のみ自動化された状態	・ 標準的なルールに基づく手段や文書によって SBOM が提供されている状態 ・ 提供する手段を自動化するプロトコル（REST/RESTful/SOAP API 等）を活用している状態 ・ 分散型台帳の技術によって、SBOM が提供者と利用者で同期された状態

3）CISA：Types of Software Bill of Material（SBOM）Documents

2023 年 4 月、CISA は、ソフトウェアライフサイクルの各フェーズで生成される可能性がある SBOM をタイプ分類し、各タイプの一般的な SBOM 生成方法を示した文書を発表した。具体的には、SBOM のタイプをソフトウェアライフサイクルの 6 つのフェーズで分類し、各タイプの定義と一般的に生成される方法が示されている（表 1-6）。なお、各タイプはソフトウェアライフサイクルフェーズと厳密に対応付けたものではないとしており、タイプによっては、複数のライフサイクルフェーズで利用可能な場合があるとしている。

表 1-6 SBOM のタイプの定義と一般的な生成方法

SBOM のタイプ	定義	一般的な生成方法
設計 (Design)	・ 新たに開発予定または計画中の段階におけるソフトウェア製品の SBOM。	・ 設計仕様書、RFP、初期コンセプトに基づき生成。

SBOM のタイプ	定義	一般的な生成方法
	・ 本タイプの SBOM は、SBOM に含まれるコンポーネントの一部が今後開発される予定のため存在しない可能性がある。	
ソース (Source)	・ ソフトウェア製品の開発に使用される開発環境、ソースファイル、ソースファイルの依存関係を基に生成される SBOM。	・ ソフトウェア構成分析(SCA)ツールに基づき生成された後、生成者による手作業で修正・補完。
ビルド (Build)	・ ソースファイル、依存関係、ビルドされたコンポーネント、ビルドプロセスの一時的なデータ、他のタイプの SBOM 等を基に、リリース可能なアーティファクト(例:実行ファイル、パッケージ)を作成するためのソフトウェアを構築するプロセスの一部として生成される SBOM。	・ ビルドプロセスの一部として生成。 ・ ソフトウェア製品のリリース時の SBOM となり、中間的なビルド時の SBOM や、ソースタイプの SBOM を統合して構成されることがある。
解析 (Analyzed)	・ ビルド後のアーティファクト(例:実行ファイル、パッケージ、コンテナ、仮想マシンイメージ)を解析して生成される SBOM。 ・ アーティファクトの解析では、マニュアル解析(ツールによる解析結果の補完等)が必要となることが多い。本タイプの SBOM は、サードパーティ SBOM と呼ばれることもある。	・ サードパーティツールによるソフトウェアの解析を通じて生成。
デプロイ (Deployed)	・ システムに存在するソフトウェアのインベントリーが記述される SBOM。 ・ 本タイプの SBOM は、構成オプションの解析や仮想的なデプロイ環境での実行動作の検証を組み合わせ、他の SBOM の集合体となる可能性がある。	・ システム上にインストールされたソフトウェアの SBOM や構成情報に基づき生成。
ランタイム (Runtime)	・ ソフトウェアを実行するシステムを解析して生成される SBOM。 ・ システム内に存在するコンポーネントだけでなく、外部呼び出しまたは動的にロードされるコンポーネントも記述される。本タイプの SBOM は、Instrumented SBOM や Dynamic SBOM と呼ばれることがある。	・ システムと相互作用するツールから生成。 ・ 実行環境に存在するアーティファクトや実行されたアーティファクトが記述される。

4）CISA：Minimum Requirements for Vulnerability Exploitability eXchange（VEX）

2023 年 4 月、CISA は、Vulnerability Exploitability eXchange（VEX）ドキュメントの最小要件を示した文書を公開した。具体的には、VEX ドキュメントを構成する項目と、各項目に含まれる要素が示され、それぞれにおける必須項目・必須要件が定義されている（図 1-1）。なお、本文書では、必須要件を VEX ドキュメントの最小要件と位置づけている。

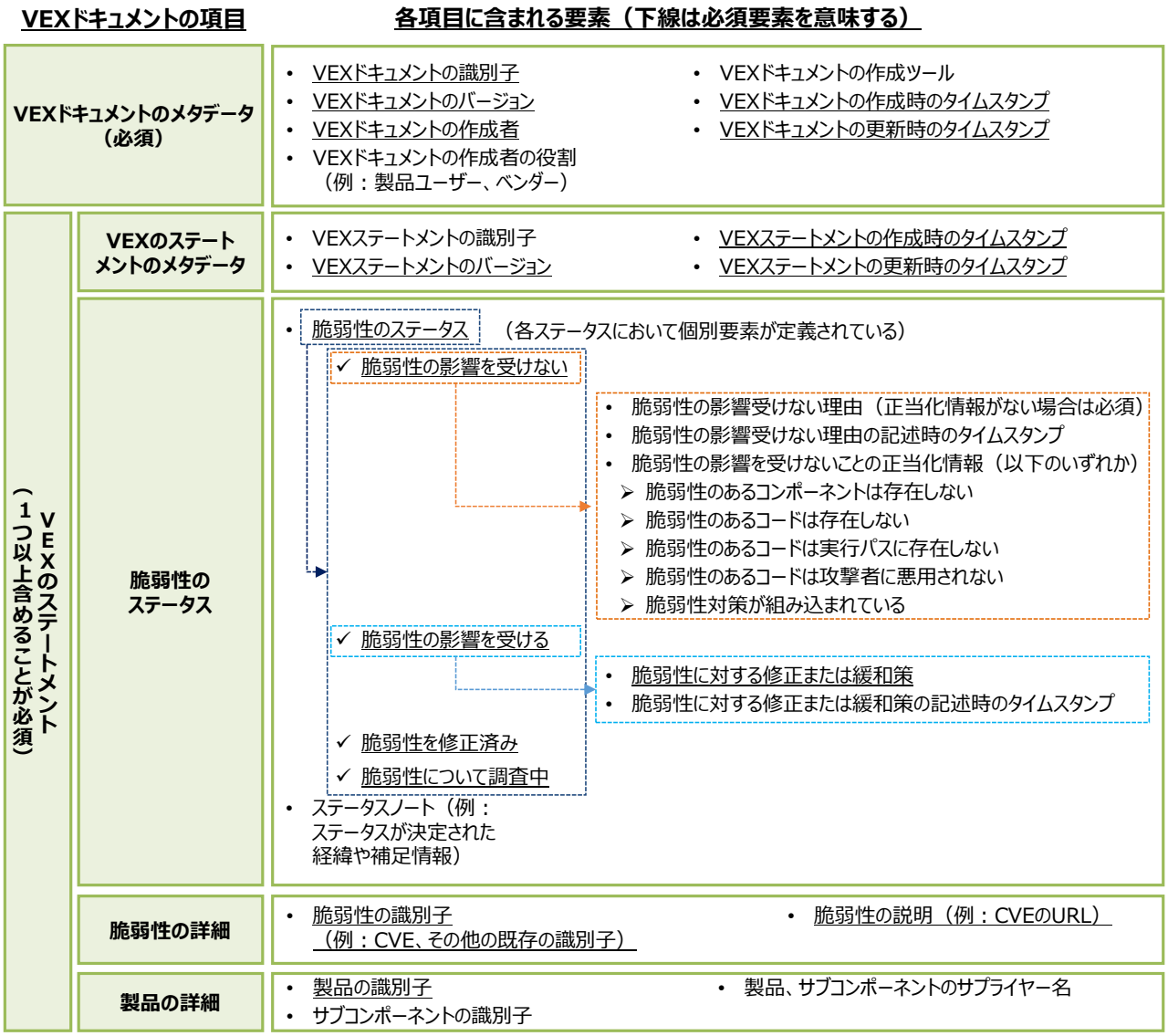


図 1-1 VEX ドキュメントの最小要件

5）OMB：Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices

2023 年 6 月、米国行政管理予算局（OMB）は、安全なソフトウェア開発手法の実装を通じたソフトウェアサプライチェーンの確保に関する覚書（M-22-18）の内容を更新する新たな覚書（M-23-16）を

発行した。具体的には、連邦政府機関がソフトウェアベンダーから SSDF に準拠していることを示す自己適合証明書の取得期限の延長の他、M-22-18 の要求事項の明確化や補足的なガイダンスについて示されている（表 1-7）。

表 1-7 覚書（M-23-16）の記載概要

項目	内容
自己適合証明書の取得期限の延長	M-22-18 によって連邦政府機関が求められているソフトウェアベンダーからの自己適合証明書の取得期限に関して、以下のとおり延長する。 ・ **「重要なソフトウェア」の自己適合証明書:** 当初予定：M-22-18 発行後 270 日以内である 2023 年 6 月 11 日まで **⇒延長後：CISA が発表した自己適合証明書フォームの承認後 3 ヶ月以内** ・ **すべてのソフトウェアの自己適合証明書:** 当初予定：M-22-18 発行後 1 年以内である 2023 年 9 月 14 日まで **⇒延長後：CISA が発表した自己適合証明書フォームが承認後 1 年以内**
M-22-18 の要求事項の明確化	・ **サードパーティコンポーネントに対する自己適合証明書の取得について** 自己適合証明書は、機関が使用するソフトウェアの最終ベンダーから取得されなければならない。そのため、機関は、使用するソフトウェアに組み込まれるサードパーティコンポーネントのベンダーから自己適合証明書を取得する必要はない。 ・ **無償で入手可能なプロプライエタリソフトウェアと一般に公開されているソフトウェアに対する自己適合証明書の取得について** 一般に無償で入手可能なプロプライエタリソフトウェアは自己適合証明書の取得の対象外とする。また、一般に公開されている Web ブラウザ等のソフトウェアについても、自己適合証明書取得の対象外とする。ただし、機関は、このようなソフトウェアのリスクを評価し、適切な対処を講じなければならない。なお、自由に入手可能な場合でも、無償で入手できないソフトウェアのデモやパイロット版は自己適合証明書の取得の対象となる。 ・ **連邦政府の請負業者によって開発されたソフトウェアに対する自己適合証明書の取得について** 連邦契約の下で開発されたソフトウェアが、M-22-18 において対象外としている「機関によって開発されたソフトウェア」に該当するかは、機関がソフトウェア開発ライフサイクルを一貫して、安全なソフトウェア開発手法を実践することを実行できるかによる。
ソフトウェアベンダーが自己適合証明できない場合における補足的なガイダンス	ソフトウェアベンダーが自己適合証明書フォームに記載された事項の実施を証明できない場合であっても、証明できない事項を特定し、リスクを軽減するための実施事項を文書化し、自己適合証明書フォームの提出までの行動計画・マイルストーン（POA&M）を提出することで、機関はそのソフトウェアの使用が許可されている。本内容に関して、以下のとおり補足的なガイダンスを示す。 ・ 機関は、自己適合証明の期限延長を OMB へ申請しなければならない。

項目	内容
	・ リスクを軽減するための実施事項をまとめた文書が不十分または POA&M が未提出の場合は、機関はソフトウェアの使用を中止しなければならない。また、機関が自己適合証明の期限延長を申請しない場合は、提出された POA&M は有効とならず、機関はソフトウェアの使用を中止しなければならない。 ・ 自己適合証明できず、複数機関が影響を受ける場合、OMB は主導機関を指定し、主導機関に対して自己適合証明に関する調整・管理を要求する。 また、本覚書発行後 1 年以内に、OMB は、各機関の POA&M の承認、自己適合証明の期限延長(免除含む)に関する状況把握を開始する。

6) CISA:SBOM-a-rama 2023

2023 年 6 月、CISA の主催により、SBOM コミュニティの醸成を目的とし、第 2 回「SBOM-a-rama」がリアルとオンラインのハイブリッドで開催され、合計で 30 か国 900 名以上が参加した。本イベントでは、各国の SBOM に関する取組状況、米国の自動車・金融・ヘルスケア分野における SBOM の検討状況、SBOM に関する個別課題の検討 WG の状況について発表された。なお、各国の SBOM に関する状況の発表の一部として、日本の SBOM に関する取組状況について経済産業省より発表された。

各発表内容は以下に示すとおりである。

1. **各国の SBOM に関する状況**
   - 米国:SSDF の自己適合宣言フォームの状況、FDA における医療機器の SBOM 対応状況について発表された。
   - 欧州:サイバーレジリエンス法の検討状況、サイバーレジリエンス法における SBOM に関する要件について発表された。
   - 日本:2022 年度の実証と今年度の実証予定について発表された。
2. **米国の産業分野の SBOM の検討状況**
   - 金融:金融分野における SBOM の PoC の実施状況、PoC から見えてきた課題について発表された。
   - ヘルスケア:ヘルスケア分野における SBOM の PoC の実施状況、PoC を基に開発した OSS について発表された。
   - 自動車:自動車 ISAC で実施した SBOM の PoC の実施状況、SBOM ツールのワークショップなどの実施したイベントについて発表された。
3. **SBOM に関する個別課題の検討 WG**

   以下の WG における活動状況、文書の公表状況、WG への参加募集について発表された。
   - VEX 検討 WG、SBOM 共有 WG、クラウド・オンラインアプリケーション WG
   - SBOM ツール・実装 WG、SBOM 初心者サポート WG

また、表 1-8 に示すとおり、SBOM が実装された社会と実装に向けて CISA に求める施策や課題に

ついて議論された。

表 1-8 「2023 SBOM-a-rama」において主に議論された課題

発表・議論内容	発表・議論内容を基に確認された主要な課題（抜粋）
米国の PoC	・ SBOM の品質（SBOM がカバーしている部品の範囲など） ・ SBOM における ID 付け（脆弱性 ID、製品 ID 等の対応付け）
SBOM の各種検討 WG	・ SBOM の適切な共有方法 ・ SBOM の品質（SBOM の最小要素の定義や SBOM が発行されたタイミングなど） ・ SBOM・VEX 連携の実装方法 ・ SaaS・クラウドにおける SBOM の在り方・標準 ・ SBOM の自動化におけるベストプラクティスの作成 ・ SBOM についての企業間における検討のギャップ
ディスカッション	・ 経営層向けの SBOM に関する説明資料の必要性 ・ PoC における成果や各企業の SBOM 成功事例の取りまとめ ・ 検討 WG で出た仮説の検証の実施 ・ 共通的な定義となる SBOM の成熟度モデルや SBOM における用語の定義

7）Quad：Quad Cybersecurity Partnership: Joint Principles for Secure Software

2023 年 5 月、Quad（日米豪印戦略対話）は、政府調達ソフトウェアのセキュリティ確保に向け、ソフトウェアの安全な開発・調達・運用に関する方針を示した共同原則を発表した（表 1-9）。安全なソフトウェア開発に関して、SSDF と同様の 4 つのプラクティス（組織の準備（PO）、ソフトウェアと開発環境の保護（PS）、安全なソフトウェアの開発（PW）、脆弱性への対応（RV））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。

表 1-9 Quad におけるソフトウェアセキュリティに関する共同原則

項目	内容
ソフトウェアベンダーによる安全な開発の実践に関する原則	安全なソフトウェア開発手法が実践されたソフトウェアを調達するため、当該手法を実践することを政府方針に取り入れるとともに、ソフトウェアベンダーに対して、当該手法の実践を推奨することを目指す。 ・ 組織の準備 安全なソフトウェア開発手法を実践するため、適切な教育を受けた人材、プロセス、技術を適切に整備する。 ・ ソフトウェアと開発環境の保護 ソフトウェアに含まれるコンポーネントを、改ざんや不正アクセスから適切に保

項目	内容
	護する。また、ソフトウェアは、リリースされたバージョンごとに管理し、バージョンごとに使用されているコンポーネントの詳細情報（SBOM 等）やサプライチェーン情報を適切に管理する。 ・ 安全なソフトウェアの開発 脆弱性を最小限に抑え、セキュリティに関するテストを経て十分なセキュリティを備えたソフトウェアをリリースする。 ・ 脆弱性への対応 ソフトウェアに存在する脆弱性を特定し、特定した脆弱性に適切な対処を行い、同様の脆弱性が今後発生することを防止する。
安全なソフトウェアの調達に関する原則	ソフトウェアまたはソフトウェアを含む製品の政府調達に関して、国際的義務、国内における法律・規制及びサイバー空間の成熟度に合わせ、各国は、以下の事項をソフトウェアベンダーに対して要求することを目指す。 ・ 安全なソフトウェア開発手法の実践に準拠していることを示す自己適合証明書を要求する。（第三者評価を受けた場合を除く） ・ 各国の脆弱性開示プログラム（脆弱性情報の報告や開示プロセスを含む）に準拠することを要求する。
ソフトウェアの運用におけるセキュリティ対策に関する原則	政府がソフトウェアを運用する際には、以下のセキュリティ対策を実施することを目指す。 ・ ソフトウェアやソフトウェアプラットフォームへの不正アクセス及び使用を防止するため、適切な管理とプロセスを実施する。 ・ ソフトウェアやソフトウェアプラットフォームが使用するデータの機密性、完全性、可用性を保護するため、適切な管理とプロセスを実施する。 ・ ソフトウェアが悪用されるのを防ぐため、ソフトウェアプラットフォームやプラットフォームに展開されるソフトウェアを特定し、管理する。 ・ ソフトウェアやソフトウェアプラットフォームに関するインシデントを迅速に検出・対応・回復する。 ・ ソフトウェアやソフトウェアプラットフォームのセキュリティ対策を推進する者へのサポートを強化する。

8）蘭 NCSC：SBOM startersgids

2023 年 7 月、オランダの国家サイバーセキュリティセンター（NCSC）は、組織における SBOM 導入を支援するガイドである「SBOM-startersgids（SBOM スターターガイド）」を公開した。本ガイドでは、SBOM や VEX に関する基礎知識が概説されている他、組織が SBOM を作成・管理・共有するためのプロセス、サプライヤーとの連携に向けた Tips を概説している。加えて、代表的な脆弱性識別子に関する解説がなされている他、組織内の脆弱性管理において SBOM を活用する方法についても示されている。

9）ホワイトハウス：National Cybersecurity Strategy Implementation

2023 年 3 月、ホワイトハウスは、国家サイバーセキュリティ戦略を発表し、2023 年 7 月には、同戦略の実施計画を発表した。国家サイバーセキュリティ戦略では５つの柱と 27 の戦略目標が示されており、実施計画では、各戦略目標の実施計画（どの連邦政府機関が、何を、いつまでに実施するか）が整理されている（表 1-10）。

表 1-10 米国国家サイバーセキュリティ戦略の実施計画の詳細

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
柱 1. 重要インフラの防衛					
戦略目標 1.1：国家安全保障と公共安全を支えるためのサイバーセキュリティ要件の確立	1.1.1 サイバー規制の調和に関するイニシアチブの設立	国家サイバー長官室（ONCD）は、行政管理予算局（OMB）と連携し、規制当局と協力し、重要インフラのサイバーセキュリティ基本要件の調和を図る機会を特定する。また、ONCD は非政府の利害関係者を巻き込み、規制の重複に関する既存の課題を理解し、基本要件の相互承認の枠組みを検討する。	ONCD は、OMB と連携し、サイバーセキュリティ規制の調和に関する行政の取組を主導する。 また、サイバーインシデント報告協議会は、連邦のインシデント報告要件を調整、対立を解消し、調和させる。	国家サイバー長官室（ONCD）	24 年度第 1 四半期（2023.10.1～12.31）
	1.1.2 重要インフラセクター全体におけるサイバーセキュリティ要件の確立	国家安全保障会議（NSC）を通じて、重要インフラセクターのリスク管理担当省庁（SRMA）と規制当局は、業界のサイバーリスクを分析し、リスクを軽減するためのサイバー要件を確立するために、既存の権限の活用方法を概説する。また、セクター固有のニーズを考慮し、権限における問題点を特定し、解消するための提案を作成する。	連邦政府は、重要インフラセクターにおいて、サイバーセキュリティ要件を確立するため、既存の権限を活用する。また、サイバーセキュリティ要件を実施する上で、連邦政府機関の権限に問題点がある場合、連邦政府は議会と協力して問題点を解消する。	国家安全保障会議（NSC）	25 年度第 2 四半期（2025.1.1～3.31）
	1.1.3 規制の整合性を示すためのフレームワークや国際基準の活用促進	国立標準技術研究所（NIST）のサイバーセキュリティフレームワーク（CSF）は、継続的に更新されている。更新内容は、パフォーマンスベースである CSF が、技術や脅威のトレンドに対応し、得られた教訓を統合し、ベストプラクティスを標準的なプラクティスへ移行するのに役	規制はパフォーマンスベースであるべきであり、既存のサイバーセキュリティに関するフレームワーク、ボランタリー的に合意された基準、既存のガイダンス（CISA の Cybersecurity Performance Goals、NIST CSF 等）を活用す	国立標準技術研究所（NIST）	25 年度第 1 四半期（2024.10.1～12.31）

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
		立つ。NIST は、フレームワークの大幅な更新版（CSF 2.0）を策定中である。NIST は、CSF 2.0 を発行し、連邦政府機関から要請があれば、国際基準や CSF との規制の整合に関する技術支援を提供する。	る。		
戦略目標 1.2：官民協力の拡大	1.2.1 セキュアバイデザイン・セキュアバイデフォルトに基づく技術の開発と採用を推進するための官民パートナーシップの規模拡大	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）は、技術メーカー、教育者、非営利組織、学術界、OSS コミュニティ等との官民パートナーシップを主導し、セキュアバイデザイン・セキュアバイデフォルトに基づくソフトウェアやハードウェアの開発と採用を推進する。CISA は、NIST、SRMA を含む他の連邦機関、民間セクターと協力し、既存の標準やプラクティスを活用し、セキュアバイデザイン・セキュアバイデフォルトの標準やプラクティスを策定する。その後、策定した標準やプラクティスの採用に関する問題点を特定し、解決するための官民パートナーシップの主導を含む推進を行う。	連邦政府は、より高いセキュリティとレジリエンスを実現するため、ソフトウェアやハードウェアのサプライヤー、マネージドサービスプロバイダーとの協力関係を深める。	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）	24 年度第 4 四半期（2024.7.1～9.30）
	1.2.2 重要インフラセクターと重要インフラセクターのリスク管	Federal Senior Leadership Council（FSLC）は、合意された SRMA 基準に基づいて SRMA の機能	連邦政府は、CISA と各 SRMA との連携を継続して強化する。	サイバーセキュリティ・インフラストラクチャセ	24 年度第 1 四半期（2023.10.1

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
	理担当省庁（SRMA）の指定に関する推奨事項の提言	を見直し、民間セクターのパートナーと協議し、重要インフラセクターの SRMA に関する推奨事項を国土安全保障長官へ提出する。		キュリティ庁（CISA）	～12.31）
	1.2.3 既存の報告メカニズムを活用した、または、重要インフラセクターのリスク管理担当省庁（SRMA）のセクター固有のシステムとプロセスを統合・運用するための単一のポータルを構築するかの評価	CISA は、SRMA と協力し、情報共有に問題が存在するか、SRMA 及び他の省庁間での情報共有のための相互運用可能なシステムの要件を理解する。SRMA が強固な情報共有能力を有していない場合、CISA は SRMA と協力して、その能力を強化させるプロセスを開発する。	CISA と SRMA は、民間セクターとのパートナーシップの下、Machine to Machine（M2M）による情報共有を強化・発展させるための技術的・組織的メカニズムを追求する。	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）	24 年度第 3 四半期（2024.4.1～6.30）
	1.2.4 情報共有や連携のためのプラットフォーム・プロセス・メカニズムを新たに改善する機会の調査	CISA は、官民協力のメカニズムを見直すセクター横断的な取組を主導する。SRMA は、Sector Coordinating Councils（SCCs）、Information Sharing and Analysis Centers（ISACs）、Information Sharing and Analysis Organizations（ISAOs）、新しいセクター協力イニシアチブ、その他の事業体等のセクター内の活動を代表し、官民協力の成熟度モデルを CISA へ提供する。	ISACs や ISAOs との長年の協力関係を基に、連邦政府は他の組織とも協力して、ISACs や ISAOs との協力モデルがどのように発展すべきかに関する共通のビジョンを策定する。	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）	26 年度第 1 四半期（2025.10.1～12.31）

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
	1.2.5 重要インフラセクターのリスク管理担当省庁（SRMA）に対するサポート機能の確立	CISA は、すべての SRMA をサポートする機能として、単一の窓口となる SRMA サポート事務局を確立する。本事務局は、SRMA の能力に応じて、SRMA ごとに提供するサービスを調整する。また、CISA は、各 SRMA と協力し、サービスの選択肢と機会の評価を含めて、事務局による SRMA への支援に対するニーズと優先順位を定義する。さらに、必要に応じて、定義した内容に基づき、CISA のサービス一覧を更新する。	連邦政府は、CISA とその他の機関との連携を引き続き強化する。SRMA は、SRMA の能力開発に投資し、SRMA が各分野の重要インフラ所有者・運用者のニーズに積極的に対応できるよう整備する。	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）	25 年度第 2 四半期（2025.1.1～3.31）
戦略目標 1.3：連邦政府のサイバーセキュリティセンターの統合	1.3.1 連邦政府のサイバーセキュリティセンター及び関連センターの能力と、スピード・規模を持った協力に必要な計画の評価・改善	ONCD は、連邦政府のサイバーセキュリティセンターと関連センターを評価し、能力に関する問題点やその他に関する重要な問題点を特定する。	ONCD は、サイバーセキュリティセンターの統合を強化するための行政の取組を主導し、能力に関する問題点を特定し、スピードと規模を持った協力を可能にするための実施計画を策定する。	国家サイバー長官室（ONCD）	23 年度第 4 四半期（2023.7.1～9.30）
戦略目標 1.4：連邦政府のインシデント対応計画やプロセスの明確化	1.4.1 国家サイバーインシデント対応計画（NCIRP）の更新	CISA は、ONCD と連携し、PPD-41「United States Cyber Incident Coordination」の下位に位置する国家サイバーインシデント対応計画（NCIRP）の更新を主導する。本更新により、PPD-41 の方針の一つである「一	CISA は、NCIRP の更新を主導する。	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）	25 年度第 1 四半期（2024.10.1～12.31）

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
		つへの呼びかけはすべてへの呼びかけ」をより完全に実現するためのプロセス、システムが強化される予定である。また、本更新には、インシデント対応とレジリエンスにおける連邦政府機関の役割と能力に関する外部パートナーに対するガイダンスも含まれる。			
	1.4.2 重要インフラ向けサイバーインシデント報告法（CIRCIA）の最終規則の発行	CISA は、重要インフラセクターのリスク管理担当省庁（SRMA）、DOJ、その他の連邦機関と協力し、重要インフラ向けサイバーインシデント報告法（CIRCIA）を実装する。CISA は、法的な要件にしたがって、CIRCIA の規則制定案通知（NPRM）、最終規則を公表し、インシデント報告の適切な活動（機関とのインシデント情報の共有を含む）を進めるプロセスを策定する。	CISA は、CIRCIA の規則策定と実装において、SRMA、DOJ、その他の連邦機関と協議する。	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）	25 年度第 4 四半期（2025.7.1～9.30）
	1.4.3 サイバーインシデントへの対応を改善するための演習シナリオの開発	ONCD は、省庁及びその他の関係者と協力し、複数の机上演習シナリオを開発し、省庁がサイバーインシデントに対する政府全体の対応に継続して改善できるようにする。	連邦政府の支援が必要な場合、連邦政府は、統一され、調整された政府全体の対応を示さなければならない。	国家サイバー長官室（ONCD）	24 年度第 1 四半期（2023.10.1～12.31）
	1.4.4 サイバーセーフティレビュー委員会（CSRB）に必要な権	国土安全保障省（DHS）は、議会と協力し、サイバーセーフティレビュー委員会（CSRB）を明文化する。	政権は連邦議会と協力し、DHS 内に CSRB を明文化する法案を成立させ、重要なインシデントの包	国土安全保障省（DHS）	23 年度第 2 四半期（2023.1.1～

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
	限を付与するための法案の作成		括的レビューを実施するための必要な権限を与える。		3.31）
戦略目標 1.5：連邦政府における防衛の近代化	1.5.1 非機密な連邦文民行政機関（FCEB：Federal Civilian Executive Branch）システムのセキュリティ確保	OMB は、CISA と連携し、集団的な運用防御を通じて、非機密な FCEB システムを保護し、集中型共有サービス、企業ライセンス契約、ソフトウェアサプライチェーンリスク軽減の利用拡大を促進するための行動計画を策定する。	OMB は、CISA と連携し、集団的な運用防御、集中型共有サービスの利用拡大、ソフトウェアサプライチェーンのリスク軽減を通じて、FCEB システムの安全を確保するための行動計画を策定する。	行政管理予算局（OMB）	24 年度第 2 四半期（2024.1.1～3.31）
	1.5.2 連邦文民行政機関（FCEB：Federal Civilian Executive Branch）のテクノロジーの近代化	OMB は、FCEB が有するテクノロジーの近代化を加速させるための複数年にわたるライフサイクル計画の策定を主導する。なお、計画では、維持コストが高く、防衛が困難なレガシーシステムの排除に連邦政府の努力を優先させる。	OMB は、FCEB が有するテクノロジーの近代化を加速させるための複数年ライフサイクル計画の策定を主導し、維持コストが高く、防衛が困難なレガシーシステムの排除に連邦政府の努力を優先させる。	行政管理予算局（OMB）	24 年度第 4 四半期（2024.7.1～9.30）
	1.5.3 FCEB における国家安全保障システム（NSS）の安全化	国家安全保障局（NSA）は、NSS の管理者の責任を果たすに当たり、FCEB における NSS のセキュリティに対処するための計画を策定し、実行する。	NSS の管理者は、OMB と調整し、NSM-8「国家安全保障、国防総省、情報コミュニティのシステムのサイバーセキュリティ向上に関する覚書」において指示されている、サイバーセキュリティに関する要件の実施を確保するため、FCEB における NSS に関する計画を策定する。	国家安全保障局（NSA）	24 年度第 4 四半期（2024.7.1～9.30）

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
柱 2. 脅威主体の破壊と解体					
戦略目標 2.1：破壊的活動の統合	2.1.1 国防総省サイバー戦略（DOD Cyber Strategy）の最新版の発表	国防総省（DOD）は、国家安全保障戦略、国家防衛戦略、国家サイバーセキュリティ戦略に沿った最新版のサイバー戦略を策定する。最新版のサイバー戦略では、他国やその他の悪意ある攻撃者の能力や攻撃活動が、米国とその利益に戦略レベルの脅威をもたらす可能性のある課題に焦点を当てる。	DOD は、国家安全保障戦略、国家防衛戦略、国家サイバーセキュリティ戦略に沿った最新のサイバー戦略を策定する。	国防総省（DOD）	24 年度第 1 四半期（2023.10.1～12.31）
	2.1.2 国家サイバー調査合同タスクフォース（NCIJTF）の能力強化	国家サイバー調査合同タスクフォース（NCIJTF）は、より迅速、大規模、高頻度に、排除や破壊的活動を調整するための能力を強化する。	NCIJTF は、政府全体の破壊的活動を調整する省庁の中心的存在として、より迅速、大規模、高頻度に、排除や破壊的活動を調整する能力を拡大する。	連邦捜査局（FBI）	25 年度第 4 四半期（2025.7.1～9.30）
	2.1.3 破壊的活動に特化した組織的なプラットフォームの拡大	司法省（DOJ）は、サイバー犯罪者、国家敵対者、その他攻撃者（例：マネーロンダリング犯罪者）による脅威に特化した組織的なプラットフォームを拡大し、サイバー業務に特化した弁護士の数を増加させることによって、脅威に対する破壊的活動の量とスピードを向上させる。	脅威に対する破壊的活動の量とスピードを向上するため、連邦政府は、継続的で協調的な活動を可能とする技術的・組織的なプラットフォームを開発しなければならない。	司法省（DOJ）	25 年度第 1 四半期（2024.10.1～12.31）
	2.1.4 サイバー犯罪及びサイバー犯罪に繋がりうる犯罪を破壊し、抑止するための	DOJ は、省庁と協力し、サイバー犯罪を破壊し、抑止するにあたって、米国政府の能力を強化する立法案を作成する。	脅威に対する破壊的活動の量とスピードを向上するため、連邦政府は、継続的で協調的な活動を可能とする技術的・組織的なプラット	司法省（DOJ）	23 年度第 4 四半期（2023.7.1～9.30）

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
	法律の提案		フォームを開発しなければならない。		
	2.1.5 破壊的活動のスピードと規模の拡大	国家サイバー調査合同タスクフォース（NCIJTF）、法執行機関、米国サイバー軍、国家安全保障局（NSA）、その他のコミュニティは、破壊的活動のスピードと規模を向上させるため、破壊的活動を調整し、実行するための追加的な機能の開発を主導する。	脅威に対する破壊的活動の量とスピードを向上するため、連邦政府は、継続的で協調的な活動を可能とする技術的・組織的なプラットフォームを開発しなければならない。	連邦捜査局（FBI）	24 年度第 2 四半期（2024.1.1～3.31）
戦略目標 2.2：脅威主体を破壊するための官民協力強化	2.2.1 官民協力を通じて、脅威主体の破壊を増大させるためのメカニズムの特定	国家サイバー長官室（ONCD） は、省庁や民間セクターと協力し、悪意あるサイバー攻撃者の破壊的活動を増大するために、官民の協力を強化するための既存メカニズムを活用する機会を特定する。	脅威に特化した協力体制は、少数で信頼の置ける人員で構成され、関連するハブによってサポートされ、機敏で、個の形を取るべきである。仮想的なコラボレーションプラットフォームを使用し、メンバー間は相互に情報を共有し、脅威主体を破壊するために迅速に活動する。また、連邦政府は、本協力体制をサポートし、活用する上での問題点（セキュリティ要件や記録管理方針等）を速やかに解消する。	国家サイバー長官室（ONCD）	24 年度第 2 四半期（2024.1.1～3.31）
戦略目標 2.3：情報共有や被害者通知の速度と規模の拡大	2.3.1 セクター固有の必要な情報と優先事項の特定、プロセスの開始	2021 年度の 国防権限法（NDAA） Sec.9002 (c) (1)に規定された要件に従い、国家安全保障会議（NSC）は、重要インフラセクターのリスク管理担当省	SRMA は、CISA、法執行機関、サイバー脅威情報統合センター（CTIIC）と連携して、セクターにおける必要情報と優先事項を特定	国家安全保障会議（NSC）	25 年度第 1 四半期（2024.10.1～12.31）

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
		庁（SRMA）がセクターにおける必要情報と優先事項を特定するための合意されたアプローチを確立するための政策策定プロセスを主導する。	し、警告や技術的指標を共有するプロセスを開発する。		
	2.3.2 重要インフラの所有者や運用者に対するサイバー脅威に関する情報を共有するための障壁の解消	国家情報長官室（ODNI）は、大統領令13636「重要インフラのサイバーセキュリティ改善」Sec.4 の実施から得られた成果物や教訓を活用し、司法省（DOJ）や国土安全保障省（DHS）と連携し、重要インフラの所有者や運営者との間でサイバー脅威に関する情報を共有するための政策や手順を見直し、情報を共有するための問題点の解消や情報へのアクセス権の拡大の要否を判断する。	連邦政府は、機密解除のポリシーとプロセスを見直し、サイバー脅威に関する実用的な情報を共有するために、問題点の解消や機密情報へのアクセス権の拡大の要否を判断する。	国家情報長官室（ODNI）	24 年度第 3 四半期（2024.4.1～6.30）
戦略目標 2.4：米国拠点のインフラ悪用の防止	2.4.1 IaaS のプロバイダーと販売代理店に対する要件・基準・手続きに関する立法案公告（NPRM）の公表	商務省（DOC）は、IaaS のプロバイダーと販売代理店の要件を明示し、免除資格を得るためのリスクベースのアプローチが十分であると判断するための基準・手続きを明らかにする、大統領令 13984「Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities」の実施に関する立法案公告（NPRM）を公表する。	行政は、既知の悪意のある活動の手法や指標を対処することを含む、大統領令 13984 の実施を通じて、IaaS のプロバイダー全体でのリスクベースのサイバーセキュリティアプローチの採用と実施を優先する。	商務省（DOC）	23 年度第 4 四半期（2023.7.1～9.30）

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
戦略目標 2.5：サイバー犯罪への対抗とランサムウェアの撲滅	2.5.1 ランサムウェア犯罪者にとっての安全地帯の排除	国務省（DOS）は、ランサムウェア対策合同タスクフォース（JRTF）と連携し、司法省（DOJ）や他の関係者と協力し、国々がランサムウェア犯罪者にとっての安全地帯として機能することを阻止し、国際的なサイバー犯罪に対する国際協力を強化するための計画を策定する。	ランサムウェアへ対抗する 4 つの方針のうち、主に次の方針に従う。（1）国際協力を通じ、犯罪者にとって安全地帯となる国を孤立させる。	国務省（DOS）	23 年度第 4 四半期（2023.7.1～9.30）
	2.5.2 ランサムウェア犯罪の撲滅	連邦捜査局（FBI）は、JRTF と連携し、米国シークレットサービス（USSS）、DOJ、CISA、国際機関、民間セクターと協力し、ランサムウェア犯罪で得た収益の暗号資産によるマネーロンダリング、ランサムウェア活動のための初期アクセス認証情報提供等を実行可能とする環境を含むランサムウェアのエコシステムに対する撲滅を実行する。	ランサムウェアへ対抗する 4 つの方針のうち、主に次の方針に従う。（1）国際協力を通じ、犯罪者にとって安全地帯となる国を孤立させる。（2）ランサムウェアを捜査・撲滅するための法執行機関の権限等を活用する。（4）ランサムウェアによる収益のマネーロンダリングを可能とする暗号資産の悪用に対処する。 また、JRTF は、ランサムウェアの活動を混乱させるため、各省庁の取組を推進する。	連邦捜査局（FBI）	24 年度第 1 四半期（2023.10.1～12.31）
	2.5.3 ランサムウェア犯罪を調査し、ランサムウェア活動のエコシステムの破壊	司法省（DOJ）は、刑事共助条約（MLA）、国内の法的手続き、没収手続き、刑事告訴の権限を活用し、連邦政府、国際機関、民間セクターと協力し、ランサムウェア犯罪で得た収益の暗号資産	ランサムウェアへ対抗する 4 つの方針のうち、主に次の方針に従う。（1）国際協力を通じ、犯罪者にとって安全地帯となる国を孤立させる。（2）ランサムウェアを捜査・撲	司法省（DOJ）	24 年度第 2 四半期（2024.1.1～3.31）

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
		によるマネーロンダリング、ランサムウェア活動のための初期アクセス認証情報提供等を実行可能とする環境を含むランサムウェアのエコシステムを撲滅するための計画、調整、能力を強化する。	滅するための法執行機関の権限等を活用する。(4)ランサムウェアによる収益のマネーロンダリングを可能とする暗号資産の悪用に対処する。		
	2.5.4 民間セクターや SLTT(state, local, tribal, and territorial)が抱えるランサムウェアのリスクを軽減するための取組支援	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)は、ランサムウェア対策合同タスクフォース(JRTF)、重要インフラセクターのリスク管理担当省庁(SRMA)と連携し、重要インフラセクター、SLTT 等のランサムウェアの高リスクとなる対象に対し、教育、セキュリティサービス、技術評価等を提供し、被害や被害時の規模を低減する。	ランサムウェアへ対抗する 4 つの方針のうち、主に次の方針に従う。(3)ランサムウェア攻撃に耐えられるよう、重要インフラのレジリエンスを強化する。 また、JRTF は、ランサムウェアへ対抗するための民間セクターや SLTT の取組を支援する。	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)	25 年度第 1 四半期(2024.10.1～12.31)
	2.5.5 暗号資産プロバイダーによる国際的なマネーロンダリング及びテロ資金供与対策(AML/CFT)の基準の採用と実施に向けた他国の取組支援	財務省(USDT)は、DOJ、DOS 等を主導し、二国間及び金融活動作業部会(FATF)への代表団を通じて国際的なパートナーと協力し、ランサムウェアによる収益のマネーロンダリングを可能とする暗号資産プロバイダーの機能停止を含め、暗号資産プロバイダーに対するマネーロンダリング及びテロ資金供与対策(AML/CFT)の基準及び監督の世界的な採用と実施を加速させる。また、2024 年発表予定の文書を含め、関連する 15	暗号資産が犯罪行為に利用されないよう、国際的な AML/CFT の基準の実施を支援する。	財務省(USDT)	24 年度第 4 四半期(2024.7.1～9.30)

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
		の文書作成と貢献に取り組む。なお、文書には、能力が不足する国や FATF 加盟国へ技術支援を提供することを推奨する旨が含まれる予定である。			
柱 3．セキュリティとレジリエンスを促進させるための市場原理の形成					
戦略目標 3.2：セキュアな IoT 機器の開発推進	3.2.1 IoT サイバーセキュリティ改善法（2020）に基づく連邦調達規則（FAR）要件の実施	行政管理予算局（OMB）は連邦調達政策室（OFPP）を通じて連邦調達規制委員会（FARC）と協力し、IoT サイバーセキュリティ改善法（2020）に沿った連邦調達規制の変更を提案する。	政権は、 IoT サイバーセキュリティ改善法（2020）の指示に従い、連邦研究開発（R&D）、調達、リスク管理の取組を通じて、IoT サイバーセキュリティを引き続き改善する。	行政管理予算局（OMB）	23 年度第 4 四半期（2023.7.1～9.30）
	3.2.2 米国政府の IoT セキュリティ・ラベリング・プログラムの開始	本件に関する 2022 年 10 月のホワイトハウスイベントを踏まえ、国家安全保障会議（NSC）は、米国政府の IoT セキュリティ・ラベリング・プログラムの概要、及びそれを主導する機関を特定する。	さらに、政府は大統領令 14028「国家のサイバーセキュリティの改善」の指示に従い、IoT セキュリティ・ラベリング・プログラムの開発を引き続き推進する。	国家安全保障会議（NSC）	23 年度第 4 四半期（2023.7.1～9.30）
戦略目標 3.3：安全でないソフトウェア製品とサービスに対する責任の再構築	3.3.1 長期的で、柔軟性のある、永続的なソフトウェア責任の枠組みを開発するためのアプローチの模索	国家サイバー長官室（ONCD）は、学術界や市民団体と協力して、様々な分野の規制法を参考に、ソフトウェア責任の枠組みを導くアプローチを模索し、ソフトウェア責任が他の制度とどの程度似ているのか/似ていないのかについてコンピュータ科学者からの意見を反映させるためのシンポジウムを開催する。	安全なソフトウェア開発のための基準の策定を開始するため、政権は、ソフトウェア製品とサービスを安全に開発・保守する企業を責任から保護するための、セーフハーバーの枠組みの開発を推進する。政権は、議会及び民間セクターと協力して、ソフトウェア製品及びサービスの責任体制を確立する法	国家サイバー長官室（ONCD）	24 年度第 2 四半期（2024.1.1～3.31）

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
			律を策定する。		
	3.3.2 ソフトウェア部品表（SBOM）の推進、サポート対象外ソフトウェアのリスク軽減	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）は、重要インフラセクターのリスク管理担当省庁（SRMA）を含む主要な利害関係者と協力し、重要インフラを支えるサポート対象外のソフトウェアの使用状況を収集し、SBOM の規模及び実施における問題を特定し、解決を推進する。また、CISA は、世界的にアクセス可能な EOL や EOS のソフトウェアに関するデータベースの要件を検討し、SBOM に関する国際的な作業部会を開催する。	行政は、SBOM のさらなる開発を促進し、広く使用されているまたは重要インフラを支えるサポート対象外のソフトウェアがもたらすリスクを特定し、軽減するためのプロセスを開発する。	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）	25 年度第 2 四半期（2025.1.1～3.31）
	3.3.3 協調的な脆弱性開示（CVD）の実施	CISA は、国際的な脆弱性コーディネーターに関する実践共同体の創設を含め、あらゆる技術タイプやセクターにわたる官民の組織間で、協調的な脆弱性開示（CVD）を実現するための国内的・国際的な連携を確立する。なお、本事項には、国際的な CSIRT やその他の機関を支援し、協調的な脆弱性開示に関する世界的な認識と能力を確立することも含まれる。	安全なソフトウェア開発の実践を奨励するため、行政は、あらゆる技術タイプ及びセクターを対象に、CVD を奨励する。	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）	25 年度第 4 四半期（2025.7.1～9.30）
戦略目標 3.4：連邦政府の補助	3.4.1 インフラにおけるサイバーセキュリ	ONCD は、連邦政府の補助金プロジェクトに、サイバーセキュリティの明確化、	インフラ法によって資金提供するプログラムを通じて、米国はインフ	国家サイバー長官室	23 年度第 4 四半期

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
金やその他のインセンティブを利用したセキュリティの構築	ティを向上させるために連邦政府の補助金の活用	促進、組み込みを奨励するための文書を作成する。	ラとインフラを支えるデジタルエコシステムに対し、一世一代の投資を行っている。政権は、集団的なシステムレジリエンスを向上するような投資を行うことを約束する。	(ONCD)	(2023.7.1～9.30)
	3.4.2 サイバーセキュリティに関する研究のための資金調達	科学技術政策局(OTSP)は、ONCD 及び OMB と連携し、2025 年度予算編成プロセスを通じて、重要インフラのセキュリティとレジリエンスの強化を目的としたサイバーセキュリティの研究、開発、実証の優先順位付けを奨励する。	連邦政府は、重要インフラのサイバーセキュリティとレジリエンスを強化することを目的としたサイバーセキュリティの研究・開発・実証(RD&D)プログラムへの資金提供を優先する。	科学技術政策局(OTSP)	23 年度第 4 四半期(2023.7.1～9.30)
	3.4.3 サイバーセキュリティにおける社会的、行動的、経済的な研究、開発、実証	国立科学財団(NSF)は、24 年度の助成金を活用し、サイバー経済学、ヒューマンファクター学、情報完全性、その他関連テーマの研究を通じて、サイバーセキュリティが個人や社会に与える影響についての理解を深めることへ投資する。	連邦政府は、重要インフラのサイバーセキュリティとレジリエンスを強化することを目的としたサイバーセキュリティの研究・開発・実証(RD&D)プログラムへの資金提供を優先する。	国立科学財団(NSF)	24 年度第 4 四半期(2024.7.1～9.30)
戦略目標 3.5：連邦政府調達を活用した説明責任の向上	3.5.1 大統領令 14028「国家のサイバーセキュリティの改善」に基づく、連邦調達規則(FAR)の変更	OMB は、連邦調達局を通じ、連邦調達規制委員会(FARC)と協力し、大統領令 14028 に基づく、FAR の変更を提案する。なお、変更前に、規則案(サイバーセキュリティに関するインシデント報告・契約要件、安全なソフトウェアに関する内容を含む)を公表し、パブリックコメントを実施する。	大統領令 14028「国家のサイバーセキュリティの改善」は、本実施内容を拡大し、サイバーセキュリティに関する契約要件を強化し、連邦政府機関全体で標準化することを保証するものである。	行政管理予算局(OMB)	24 年度第 1 四半期(2023.10.1～12.31)

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
	3.5.2 ベンダーによるサイバーセキュリティを向上させるための不正請求防止法（FCA）の活用	司法省（DOJ）は、連邦契約及び助成金における、サイバーセキュリティ要件の故意による不履行を監視する取組を拡大する。この取組によって、レジリエンスの構築、脆弱性情報の開示の促進、ベンダーの競争的不利益の軽減、影響を受ける連邦政府のプログラム・機関の損害からの回復を目指す。	Civil Cyber-Fraud Initiative（CCFI）は、FCA に基づく DOJ の権限を利用し、セキュリティの義務を果たさない契約者や助成金受給者に対して民事訴訟を起こす。また、CCFI はセキュリティが欠如した製品やサービスを故意に提供、プラクティスへの遵守を虚偽表示、インシデントを監視・報告する義務に故意に違反することで、米国の情報やシステムを脅威にさらした事業体や個人を取り締まる。	司法省（DOJ）	25 年度第 4 四半期（2025.7.1～9.30）
戦略目標 3.6：連邦政府によるサイバー保険市場の支援検討	3.6.1 壊滅的なサイバー事象に対する連邦政府保険の必要性の評価	連邦保険局（FIO）は、CISA 及び ONCD と連携し、既存のサイバー保険市場を支援する等、壊滅的なサイバー事象に対する連邦政府による保険の対応の必要性を評価する。	政府は、既存のサイバー保険市場を支援する等、壊滅的なサイバー事象に対する連邦政府による保険の対応の必要性と対応可能な構造を評価する。	連邦保険局（FIO）	24 年度第 1 四半期（2023.10.1～12.31）
柱 4. レジリエンスな未来への投資					
戦略目標 4.1：インターネットの技術的基盤の確保	4.1.1 ネットワークセキュリティのベストプラクティスの採用促進	行政管理予算局（OMB）は、CISA と連携し、M-22-09「ゼロトラスト戦略及び成熟モデル」に従い、連邦政府と協力し、DNS のリクエストの暗号化を優先することを取り組む。	Border Gateway Protocol（BGP）の脆弱性、DNS のリクエストが暗号化されていない、IPv6 の普及遅延等の懸念のうち、緊急性が高い事項に対処する。連邦政府は、米国のネットワークが持つセ	行政管理予算局（OMB）	24 年度第 2 四半期（2024.1.1～3.31）

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
			キュリティリスクに対する対策を推進する。また、インターネットエコシステムのセキュリティを向上するソリューションを開発・採用するため、関連研究を支援する。		
	4.1.2 OSS のセキュリティとメモリ安全なプログラミング言語の採用促進	国家サイバー長官室（ONCD）は、Open-Source Software Security Initiative（OS3I）を設立し、OSS のセキュリティとメモリ安全なプログラミング言語の採用を推進する。また、CISA は、OS3I や OSS コミュニティと連携して、連邦政府や重要インフラにおける OSS の安全な利用を可能にし、OSS エコシステムのセキュリティ水準を高める。加えて、CISA は OSS コミュニティの取組と統合を図る。	連邦政府は、米国のネットワークが持つセキュリティリスクに対する対策を推進する。また、インターネットエコシステムのセキュリティを向上するソリューションを開発・採用するため、関連研究を支援する。	国家サイバー長官室（ONCD）	24 年度第 1 四半期（2023.10.1～12.31）
	4.1.3 基盤となるインターネットインフラ機能と技術に対する開発・標準化・採用の促進	National Standards Strategy に従い、国立標準技術研究所（NIST）は、国際的なサイバーセキュリティ標準化における課題を調整し、連邦政府機関の参加を促進するため、Interagency International Cybersecurity Standardization Working Group（IICS WG）を開催する。	非政府の標準化団体（SDO）を支援することで、業界リーダー、同盟国、学術機関、専門団体、消費者団体、非営利団体と協力し、新技術のセキュリティを確保し、相互運用性を実現し、グローバルな市場競争を促進し、国家の安全と経済的優位性の保護を図る。	国立標準技術研究所（NIST）	24 年度第 1 四半期（2023.10.1～12.31）
	4.1.4 基盤となるイ	NIST は、省庁、産業界、学術界、その他	BGP の脆弱性、DNS のリクエス	国立標準技術	24 年度第 4

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
	ンターネットインフラ機能と技術に対する開発・標準化を加速、採用促進	のコミュニティと協力し、Border Gateway Protocol（BGP）の脆弱性や IPv6 のセキュリティ課題に取り組む。	トが暗号化されていない、IPv6 の普及遅延等の懸念のうち、緊急性が高い事項に対処する。オープンで、自由で、グローバルで、相互運用可能で、信頼性があり、安全なインターネットを維持・拡大するためには、標準開発プロセスに持続的に関与し、我々の価値観を浸透させ、技術標準がよりセキュアでレジリエントな技術を生み出すようにする必要がある。	研究所（NIST）	四半期（2024.7.1～9.30）
	4.1.5　主要な関係者と協力した、安全なインターネットルーティングの推進	ONCD は、主要な関係者や連邦政府機関と連携し、次の方法により、安全なインターネットルーティング技術と技術の採用の拡大するためのロードマップを策定する。（1）セキュリティ上の課題を特定する。（2）インターネットルーティングと Border Gateway Protocol（BGP）の脆弱性に対処するための手段とオプションを検討する。（3）ベストプラクティスの開発を特定し情報提供する。（4）必要な研究と開発を特定する。（5）採用における問題と解決手段を特定する。	BGP の脆弱性、DNS のリクエストが暗号化されていない、IPv6 の普及遅延等の懸念の中で緊急性が高い事項に対処する。そのためには、システム上のリスクを低下させるために、セキュリティ上の懸念事項の中で最も緊急性のある事項の特定、効果的なセキュリティ対策の開発、及びインフラ上に構築されたプラットフォームやサービスを中断することないよう、公共や民間セクターとの協力が必要である。また、インターネットエコシステムのセキュリティを向上するソ	国家サイバー長官室（ONCD）	24 年度第 3 四半期（2024.4.1～6.30）

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
			リューションを開発・採用するため、関連研究を支援する。		
戦略目標 4.2：サイバーセキュリティのための連邦政府研究開発の活性化	4.2.1 メモリ安全なプログラミング言語の成熟度、採用、セキュリティの加速	連邦政府サイバーセキュリティ研究開発戦略計画（Federal Cybersecurity R&D Strategic Plan）を通じて、科学技術政策局（OTSP）は、NSF、NIST、助成金提供機関、OS3I、その他の関連省庁と協力し、アプリケーション、OS、重要インフラにおけるメモリ安全なプログラミング言語の成熟、採用、セキュリティを加速するための投資を優先する。	連邦政府サイバーセキュリティ研究開発戦略計画の更新の一環として、連邦政府は、既存及び次世代の技術におけるサイバーセキュリティリスクを予防し、緩和するために、研究・開発・実証（RD&D）のコミュニティを特定し、優先させ、活性化させることを目指す。また、信頼性のある製品とサービスから成る市場を形成するために、連邦政府の投資手段・購買力・規制を包括的に活用することで、より大規模な現代産業やイノベーション戦略を支援する。	科学技術政策局（OTSP）	24 年度第 1 四半期（2023.10.1～12.31）
戦略目標 4.3：ポスト量子暗号への備え	4.3.1 NSM-10「脆弱な暗号システムへのリスクを軽減し、量子コンピュータにおける米国のリーダーシップの促進に関する覚書」の実施	OMB、国家安全保障システム（NSS）の管理者は、ONCD と連携し、NSM-10 の実施を継続して優先し、脆弱な公共ネットワーク及びシステムを耐量子暗号ベースの環境へ移行することを推進する。本取組では、まず、連邦政府機関の情報システムと NSS に重点を置く。OMB は、NIST と協力して、将来の未知のリスクに直面した際に暗号の柔軟性	連邦政府は、脆弱な公共ネットワーク及びシステムを耐量子暗号ベースの環境へ移行することを優先し、将来の未知のリスクに直面した際に暗号の柔軟性を提供するための補完的な戦略を開発する。	行政管理予算局（OMB）	25 年度第 1 四半期（2024.10.1～12.31）

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
		を提供するための補完的な戦略を開発する。			
	4.3.2 国家安全保障システム(NSS)のための NSM-10 の実施	NSS の耐量子暗号への移行を実施する。	連邦政府は、脆弱な公共ネットワーク及びシステムを耐量子暗号ベースの環境へ移行することを優先し、将来の未知のリスクに直面した際に暗号の柔軟性を提供するための補完的な戦略を開発する。	国家安全保障局(NSA)	25 年度第 3 四半期(2025.4.1～6.30)
	4.3.3 ポスト量子暗号アルゴリズムの標準化と移行に向けた支援	NIST は、量子耐性を持つ公開鍵暗号アルゴリズムを求め、評価し、標準化するプロセスを最終化する。新たな公開鍵暗号標準は、世界中で利用可能とし、量子コンピュータの出現後の将来にわたって政府の機密情報を保護する能力を持ち、一般公開された、一つまたは複数のデジタル署名、公開鍵暗号化、鍵確立アルゴリズムを規定する。	デジタルシステムに対する脅威と量子コンピュータ技術の推進と進展をバランスさせるために、NSM-10「国家安全保障、国防総省、情報コミュニティのシステムのサイバーセキュリティ向上に関する覚書」は、国の暗号システムを相互運用可能な耐量子暗号へ迅速に移行させるための責任と監督を確立する。	国立標準技術研究所(NIST)	25 年度第 1 四半期(2024.10.1～12.31)
戦略目標 4.4:クリーンエネルギーの未来におけるセキュリティ確保	4.4.1 サイバー・セキュアバイデザインの原則の連邦政府プロジェクトへの組み込み、サイバー・セキュアバイデザインの採用促進	エネルギー省(DOE)は、ONCD 及び CISA と協力し、サイバー・セキュアバイデザインのパイロットプロジェクトを実施し、サイバー・セキュアバイデザインの経済的な利益やサイバー・セキュアバイデザインを適用するために必要な技術手段を特定し、重要インフラに対するサイ	DOE は、Clean Energy Cybersecurity Accelerator、Energy Cyber Sense program、National Labs 等の取組を通じて、将来のクリーンエネルギーグリッドを保護するための政府の取組を主導して	エネルギー省(DOE)	24 年度第 1 四半期(2023.10.1～12.31)

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
		バー・セキュアバイデザインの取組の国家的実施の進展を測定する。	おり、他の重要インフラセクターへ拡大するセキュリティのベストプラクティスを生み出している。また、DOE は、業界、州、連邦政府の規制機関、議会等と協力して、電気配電及び分散エネルギー資源におけるサイバーセキュリティの推進を継続する。		
	4.4.2 デジタルエコシステムによる米国政府の脱炭素化目標の支援、達成へ導くための計画策定	ONCD は、DOE や大統領行政府と連携し、デジタルエコシステムがクリーンエネルギーへの移行を支援するための新技術やダイナミクスを取り入れるための計画を策定する。本計画では、既存取組を関連付け、優先付けのための問題や要件を特定する。さらに、インフラ投資・雇用法（BIL）、インフレ削減法（IRA）、CHIPS 及び科学法（CHIPS & Science Act）を通じた国家投資が、セキュアで、設計上のレジリエンスがあり、クリーンエネルギーエコシステムの新しい運用をサポートできるよう関係者と連携する。	National Cyber-Informed Engineering（CIE） Strategy の実施を通じ、「国家サイバーセキュリティ戦略」の機会を活用する。連邦政府、業界、SLTT 全体の関係者と協力し、電気自動車、ゼロ・エミッションの燃料インフラ、ゼロ・エミッションのトランジットバス・スクールバスの安全で相互運用可能なネットワークを展開する。	国家サイバー長官室（ONCD）	24 年度第 2 四半期（2024.1.1～3.31）
	4.4.3 Cyber-Informed Engineering	DOE は、National CIE Strategy を基づき、開発者が安全でレジリエンスのある運用技術や制御システムを設計・構	National CIE Strategy の実施を通じて、「国家サイバーセキュリティ戦略」の機会を活用する。	エネルギー省（DOE）	25 年度第 4 四半期（2025.7.1～

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
	(CIE)の原則を用いた、エンジニアや技術者のためのトレーニング、ツール、サポートの構築・強化	築・運用することを可能にするために、教育やツールの支援を推進する。			9.30)
戦略目標 4.6: サイバー人材強化のための国家戦略の策定	4.6.1 国家サイバー人材と教育の戦略の策定、実施の追跡	ONCD は、国家サイバー人材と教育の戦略策定を主導し、策定した戦略を実施するための初期段階を推進、調整、報告する。ONCD は、サイバー人材及び教育に関する活動の主導者として機能する。	ONCD は国家サイバー人材及び教育の戦略策定を主導し、策定した戦略の実施を監督する。	国家サイバー長官室(ONCD)	24 年度第 2 四半期(2024.1.1～3.31)
柱 5. 共通的な目標の追求のための国際的なパートナーシップの構築					
戦略目標 5.1: デジタルエコシステムへの脅威に対抗するための連合体の構築	5.1.1 国際間におけるサイバー協力や調整に向けた省庁間のサイバーチームの設立	国務省(DOS)は、サイバー空間とデジタル政策に関連する職員の知識と能力を向上させ、国や地域による省庁間のサイバーチームを設立・強化し、パートナー国との協調を促進する。	米国とパートナーは、サイバー脅威に関する情報の共有、サイバーセキュリティの事例の交換、セクター固有の専門知識の比較、セキュアバイデザインの原則の推進、政策とインシデント対応活動の調整によって、サイバーセキュリティに関する共通の利益を得られる。	国務省(DOS)	25 年度第 1 四半期(2024.10.1～12.31)
	5.1.2 国際サイバー空間及びデジタル政策戦略(International Cyberspace and Digital Policy	2023 年度国防権限法(NDAA)に従い、DOS は、二国間及び多国間の活動を盛り込んだ国際サイバー空間及びデジタル政策戦略を公表する。	国家のサイバーセキュリティ関係者による協力モデルの拡大するため、国際コミュニティと協力する取組を強化する。国際間の連携を強化することで、国際的なサイバー犯罪者の活動を協力して破壊し、	国務省(DOS)	24 年度第 1 四半期(2023.10.1～12.31)

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
	Strategy)の公表		国際的な同盟国やパートナーの能力を構築し、サイバー空間における国家の行動に対する既存の国際法の適用を強化し、平時の責任ある国家の行動のグローバルな基準を支持し、悪意あるサイバー攻撃者を処罰する。		
	5.1.3 同盟国やパートナーとの連邦法執行機関の協力メカニズムの強化	連邦捜査局(FBI)は、サイバー犯罪者、国家敵対者、関連する犯罪者(例:マネーロンダリング犯罪者)に対する国際法執行による破壊活動の規模とスピードを向上する取組において、同盟国やパートナーとの連携を確保するためのメカニズムを開発または拡大する。	米国は、同盟国やパートナーと協力して、デジタル時代の新たな共同法執行機構を開発するために取り組む。(1)米国と国際的なパートナーは、サイバー脅威情報を共有し、政策とインシデント対応活動を調整することで、共通のサイバーセキュリティの利益を得ることを可能とする。(2)米国は、国際的なサイバー犯罪者やその活動を協力して破壊し、国際的な同盟国やパートナーの能力を構築し、サイバー攻撃者に対処する。	連邦捜査局(FBI)	25 年度第 4 四半期(2025.7.1～9.30)
	5.1.4 地域のサイバーハブに関する研究	国家サイバー長官室(ONCD)は、European Cybercrime Centre に関する調査を委託し、将来のサイバーハブの構築に役立てる。	本取組を成功させるためには、地域のパートナーとともに、効果的なハブを構築するための活動を支援する必要がある。	国家サイバー長官室(ONCD)	24 年度第 4 四半期(2024.7.1～9.30)
戦略目標 5.2:	5.2.1 国際的なパー	DOS と関連省庁は、既存の	同盟国やパートナーが、重要イン	国務省(DOS)	24 年度第 1

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
国際的なパートナーの能力の強化	トナーのサイバー能力の強化	Interagency Cyber Capacity Building Working Group を活用し、サイバー空間における現在の世界的・政策的動向を評価する。これまでの進捗や投資を確認し、米国のサイバー目標（「国家サイバーセキュリティ戦略」の戦略目標 5.2 の 6 つの目標を含む）を達成するため、将来の国際的な能力強化の支援を優先する。	フラネットワークを保護し、効果的なインシデント検出や対応能力を構築し、サイバー脅威情報を共有し、外交的な協力を追求し、法執行能力を構築することを可能にさせる必要がある。さらに、国際法を遵守し、責任ある国家の行動の基準を強化することで、サイバー空間で得られた利益を支える。		四半期（2023.10.1～12.31）
	5.2.2 法執行機関の実働的な協力を通じた、国際的なパートナーのサイバーセキュリティ能力の拡大	最も重大なサイバー脅威を迅速に大規模に排除するために、連邦法執行機関は、国際的に同等な法執行パートナーとの実働的な協力を増加させることにより、国際的なパートナーの能力を強化する。	同盟国やパートナーが、実働的な協力を通じて、法執行能力と有効性を構築することを可能にさせる必要がある。	司法省（DOJ）	26 年度第 4 四半期（2026.7.1～9.30）
戦略目標 5.3：同盟国やパートナーを支援する米国の能力の拡大	5.3.1 サイバーインシデント対応における支援を迅速・柔軟に提供するための対外支援メカニズムの構築	DOS は、サイバーインシデント対応における支援を提供するため、柔軟で、迅速な対外支援メカニズムを特定または開発する。	政府は、対外に向け、サイバーインシデント対応における支援を提供することによる国家の利益を判断するための方針を定める。また、サイバーインシデント対応における支援において必要な、省庁のリソースを特定・展開するメカニズムを構築する。構築の際には、必要に応じて、既存の財政的・手続き的な課題を迅速に解消することを推	国務省（DOS）	24 年度第 1 四半期（2023.10.1～12.31）

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
			進する。		
戦略目標 5.4：責任ある国家行動の世界的規範を強化するための連合体の構築	5.4.1 無責任な国家に対する責任追求	DOS は、オープン・エンド作業部会（Open-Ended Working Group）を通じて、サイバー空間における国家の責任ある行動の枠組みを推進し、悪意のあるサイバー攻撃者に責任を追求する意思を持つ連合体へ強化する。	米国は、再活性化された積極的な外交の中核として、無責任な国家に対して、責任を追求する。敵対勢力を効率的に拘束し、武力紛争の範疇を超えた悪意ある活動に対抗するため、同盟国やパートナーと協力し、非難の声明と処罰を対とする。	国務省（DOS）	25 年度第 4 四半期（2025.7.1～9.30）
戦略目標 5.5：情報・通信・運用技術製品及びサービスのための安全なグローバルサプライチェーンの構築	5.5.1 安全で信頼性のある情報通信技術（ICT）ネットワーク及びサービスの開発促進	DOS は、International Technology Security and Innovation Fund（ITSI Fund）を通じて、安全な ICT エコシステムのための政策や規制の枠組みの国際的な採用を促進するため、同盟国やパートナーと協力する。	Indo-Pacific Economic Framework for Prosperity（IPEF）、Quad Critical and Emerging Technology Working Group、Trade and Technology Council（TTC）のような、地域間パートナーシップを通じて、同盟国やパートナーと協力し、グローバルサプライチェーンリスク管理におけるベストプラクティスを特定・実装し、安全なグローバルサプライチェーンを構築することに取り組む。	国務省（DOS）	24 年度第 2 四半期（2024.1.1～3.31）
	5.5.2 信頼性のある情報通信技術（ICT）のベンダーか	DOS は、ITSI Fund を通じて、同盟国やパートナーとの協力を拡大し、オープンで相互運用可能なネットワークアーキテ	DOS は、ITSI Fund を通じて、半導体と情報通信のための安全で多様なサプライチェーンを構築	国務省（DOS）	24 年度第 2 四半期（2024.1.1～

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
	ら成る、多様で、強靭なサプライチェーンの促進	クチャーの開発と展開を促進する。	の支援を加速させる。		3.31）
	5.5.3 Public Wireless Supply Chain Innovation Fund（PWSCIF）の運営開始	電気通信情報局（NTIA）は、10 年間で 15 億ドルの予算を持つ PWSCIF の管理を通じ、オープンで相互運用可能な標準に基づいたネットワークの開発と採用を促進する。本プログラムを通じ、NITA はサプライチェーンのレジリエンスを強化し、イノベーションを推進し、競争を促進する。なお、NTIA が 2023 年 8 月に授与を開始する最初の資金提供では、オープンで相互運用可能なネットワークのテストや評価機能の推進、オープンで相互運用可能なネットワークの性能・セキュリティ・効率性のテストや評価手法の開発を支援する。	NTIA は、PWSCIF を通じて、オープンで相互運用可能な標準に基づいたネットワークの開発と採用を促進する。	電気通信情報局（NTIA）	23 年度第 4 四半期（2023.7.1～9.30）
	5.5.4 重要インフラセクター全体及びセクター内での、Cybersecurity Supply Chain Risk Management（C-SCRM）の主要なプ	Software Supply Chain Security National Cybersecurity Center of Excellence Project を通じて、C-SCRM に関するプラクティスを普及させ、海外のサプライヤーに対する信頼性を高める。	信頼できないサプライヤーからの重要な外国製品やサービスへの依存は、デジタルエコシステムに様々なリスクをもたらす。リスクを軽減するために、国内外の官民が長期的かつ戦略的に協力して、グローバルサプライチェーンのバランスを調整し、透明性、安全性、レジ	国立標準技術研究所（NIST）	25 年度第 2 四半期（2025.1.1～3.31）

戦略目標	具体目標	概要	戦略の参照	担当省庁	完了日
	ラクティスの普及		リエンス、信頼性を高める必要がある。		

10） 独 BSI：SBOM-Anforderungen: TR-03183-2 stärkt Sicherheit in der Software-Lieferkette

ドイツの連邦政府情報セキュリティ庁（BSI）は、EU サイバーレジリエンス法によって将来的に製造業者に課される要件を事前に周知する目的で、製造業者に対する技術指針（BSI TR-03183 Cyber-Resilienz-Anforderungen）を検討している。2023 年 8 月、当該技術指針のパート 2 として、SBOM の要件を示した技術ガイドライン「SBOM-Anforderungen（SBOM 要件）」を公開した。

技術ガイドラインでは、ソフトウェアベンダーを主な対象とし、SBOM のフォーマットに関する要件及び技術的な要件を記載している。なお、フォーマットに関する要件については、CycloneDX v1.4 以上及び SPDX 2.3 以上を求めている。また、SBOM に含めるべき情報については、米国 NTIA「最小要素」で定義された「データフィールド」に加え、本ガイドラインでは各コンポーネントのライセンスに関する情報を「必要最低限のデータフィールド」として含めることを求めている。

11）CISA：CISA Cybersecurity Strategic Plan FY2024 – 2026

2023 年 8 月、CISA はサイバーセキュリティ戦略計画（2024-2026 年度）を発表した。本戦略計画では、CISA の取組の指針として、3 つの目標と 9 つの目的を示している（表 1-11）。さらに、本戦略計画では、各目的を実行するための手段と期待する効果を示しており、将来的に実行した手段がもたらす効果を測定することに重点を置いている。

表 1-11 CISA サイバーセキュリティ戦略計画の目標と目的

目標	目的
目標 1： サイバー攻撃からの差し迫った脅威に対処	1.1 サイバーセキュリティに関する脅威やサイバー攻撃活動の可視性を高め、対処能力を向上させる 1.2 重大で悪用可能な脆弱性の開示・探索・対策を推進する 1.3 合同サイバー防衛作戦を計画、演習、実行し、重大なサイバーセキュリティインシデントへ備える
目標 2： デジタル環境のセキュリティ強化	2.1 サイバー攻撃がどのように発生し、どのように防ぐかを理解する 2.2 効果的なサイバーセキュリティ投資の実施を推進する 2.3 サイバーセキュリティ強化における問題を解決に導き、解決の進捗を測定するのに役立つ情報やサービスを提供する
目標 3： 広範囲にわたるセキュリティ確保の推進	3.1 信頼できるソフトウェア製品の開発を推進する 3.2 新興技術がもたらすサイバーセキュリティリスクを理解し、低減する 3.3 国のサイバー人材育成の取組に貢献する

なお、目的 1.2 及び 3.1 では、実行手段と期待する効果として、脆弱性管理や安全なソフトウェア製品開発に係る事項として、既知の悪用された脆弱性（KEV）の評価、協調的な脆弱性開示（CVD）の推進、

安全な製品を開発するための基準の策定等が示されている(表 1-12)。

表 1-12 目的に対する実行手段と期待する効果(脆弱性管理や安全なソフトウェア製品開発に係る事項抜粋)

目的	目的に対する実行手段と期待する効果
1.2 重大で悪用可能な脆弱性の開示・探索・対策を推進する	【実行手段】 ・ 重要インフラや連邦政府システム全体の脆弱性、特に既知の悪用された脆弱性(KEV)に関する可視性を評価する。 ・ 協調的な脆弱性開示(CVD)の取組を推進することによって、研究団体や民間企業との連携を高める。 【期待する効果】 ・ 重要インフラと連邦政府システムにおける既知の悪用された脆弱性に対する対処時間を短縮する。 ・ CISA の脆弱性評価及びリスク評価からの推奨事項が、採用される割合が増加する。 ・ 適切な調整や必要な緩和策なしに開示される脆弱性の数が減少する。
3.1 信頼できるソフトウェア製品の開発を推進する	【実行手段】 ・ 安全な製品を開発・維持するための基準と方法を策定する。また、製品が、策定した方法をどの程度採用しているかを評価するため、関係者と連携を進める。 【期待する効果】 ・ 製品開発者が脅威モデル(何を、誰から守るかを説明したもの)を公開した数が増加する。 ・ SSDF の実装を宣言する製品開発者の数が増加する。 ・ 製品に関する脆弱性情報が、正確で完全であることのコミットメントを公開する製品開発者の数が増加する。 ・ セキュリティバイデザインのロードマップを公開した製品開発者の数が増加する。 ・ MFA(他要素認証)の採用、安全でないレガシープロトコルの使用、未サポート製品を使用している顧客の割合等、セキュリティ関連の統計やトレンドを定期的に公開する製品開発者の数が増加する。

12) CISA:CISA Open Source Software Security Roadmap

2023 年 9 月、CISA は、OSS の安全な使用や開発を支援するための CISA の取組を示す OSS セキュリティロードマップ(2024-2026 年度)を発表した。本ロードマップでは、連邦政府内外における OSS の使用及び開発においてセキュリティ強化を推進するための CISA の取組として、4 つの目標と 15 の目的を示している(表 1-13)。SBOM や脆弱性管理に係る事項として、OSS のサプライチェーン全体での包括的な SBOM 共有に向けた要件整理・課題解決、OSS の脆弱性情報開示・対処を促進するための取組等が示されている。

表 1-13 CISA OSS セキュリティロードマップの目標と目的の概要

目標	目的	概要
1. OSSのセキュリティを支援するための CISA の役割の確立	1.1 OSS コミュニティとの連携	OSS コミュニティとのリアルタイム連携を可能にするチャンネルを設立する。
	1.2 中央集権型の OSS エンティティのセキュリティ確保の推進	中央集権型の OSS 関連システムのセキュリティ確保のための原則を策定する。
	1.3 国際的なパートナーとの連携と協力の拡大	国際的なパートナーや同盟国と、共通の関心分野での協力機会を拡大する。
	1.4 CISA の OSS セキュリティに関する業務の組織化	CISA 内に、OSS セキュリティワーキンググループを設立する。
2. OSS の使用状況とリスクの可視性の向上	2.1 OSS の使用状況の把握	政府や重要インフラにおける OSS 使用状況の評価方法を開発し、状況を把握する。
	2.2 OSS におけるリスク評価のためのフレームワークの開発	OSS のリスクを評価するためのフレームワークを開発し、OSS 使用に関する分類を行う。
	2.3 連邦政府や重要インフラ組織における OSS のリスク評価	政府や重要インフラで使用される OSS のリスク評価結果リストを作成する。
	2.4 OSS に含まれる重要なリスクの理解	リスクとなりうる重要な OSS を継続的に評価するプロセスを開発する。
3. 連邦政府の OSS 使用のリスクの削減	3.1 OSS の安全な使用を支援するソリューションの評価	OSS の安全な使用を支援するソリューションの実現性や効果を評価する。
	3.2 OSPO[28]の実装ガイダンスの策定	政府機関が OSPO を実装するためのベストプラクティスをまとめたガイダンスを策定する。
	3.3 OSS 使用におけるセキュリティ強化のための連邦政府の取組推進	OS3I[29]と連携し、OSS エコシステムのセキュリティやレジリエンスを強化する。
4. OSS エコシステムのセキュリティ強化	4.1 OSS サプライチェーン内での SBOM の推進	サプライチェーン全体での SBOM 共有に向け、自動化の要件整理・課題解決を行う。
	4.2 OSS の開発者のためのセキュリティ教育の促進	OSS の開発者がセキュリティに関する情報を収集するためのツールキットを公開する。
	4.3 OSS を安全に使用するためのベストプラクティスの公表	政府や重要インフラ等が OSS を安全に使用するためのベストプラクティスを公開する。
	4.4 OSS における脆弱性の情報開示や対処の促進	OSS コミュニティと連携して、OSS の脆弱性特定や情報開示プロセス等を確立する。

13） DOD 等：Federal Acquisition Regulation: Cyber Threat and

[28] Open Source Program Office の略で、OSS 活用環境の整備、関連部署との OSS 活用における連携、OSS コミュニティとの連携等、OSS 関連活動を支援する組織のこと。
[29] Open Source Software Security Initiative の略で、OSS のセキュリティを強化し、政府のリソース活用拡大を目的とした省庁間のワーキンググループのこと。

Incident Reporting and Information Sharing

2023 年 10 月、DOD、GSA、NASA は、大統領令 14028 を受け、サイバー脅威・インシデント情報に関する情報共有の強化に向けて、FAR（連邦調達規則）の改正案を公開し、パブリックコメントを開始した。（当初予定から 2024 年 2 月 2 日まで期限を延長した。）表 1-14 に示すとおり、本改正案では、政府が調達する ICT 製品・サービス（例：通信サービス、電子メディア、IoT デバイス、運用技術）の請負業者に対して、SBOM の作成・維持、SBOM への政府機関のアクセスの許可、サイバー脅威の調査やインシデント対応に関連する CISA への協力、インシデントに関する報告等を求めている。

表 1-14 FAR（連邦調達規則）の改正案における政府調達の請負業者への要求事項（下線）と補足

項目	内容
SBOM の作成・維持	セキュリティインシデント発生の有無に関わらず、契約の履行において連邦政府が使用するすべてのソフトウェアについて、SBOM を作成・維持し、SBOM に対する連邦政府機関のアクセスを許可すること。 SBOM は、迅速に既知の脆弱性を特定することを可能とするため、セキュリティインシデント対応において重要である。
CISA のエンゲージメントサービスへ協力	サイバー脅威の調査やインシデント対応に関連する CISA の取組（エンゲージメントサービス）へアクセス・協力すること。 本改正案において、請負業者が CISA のエンゲージメントサービスへアクセス・協力するためのメカニズムを提供している。CISA のエンゲージメントサービスは、サイバー攻撃者による活動を監視し、可視化することを目的としており、サイバー攻撃によるリスクの削減を推進することに役立つ。
請負業者の情報・情報システム等へのアクセス	請負業者によって報告されたセキュリティインシデントや政府によって特定されたセキュリティインシデントに対応するため、CISA、FBI、契約先連邦政府機関による、請負業者の情報・情報システム・人員に対するアクセスを許可すること。
外国で事業を行う場合のコンプライアンス遵守	外国で事業を行う請負業者やその下請業者は、CISA にセキュリティインシデントを報告し、インシデントの対応を支援するための追加的な行動をとること。 DOD、GSA、NASA は、特定の外国で活動する請負業者が国の法律や規制によって、米国政府へ提供可能な情報に制限が発生することを留意する必要があると認識している。
セキュリティインシデント報告	請負業者は、セキュリティインシデントが発生した可能性を示すすべての指標を調査し、インシデントの発見から 8 時間以内に CISA のインシデント報告ポータル※を使用して報告すること。 報告後も、請負業者、政府、調査機関等がすべての対応を完了するまで、72 時間ごとに報告内容を更新すること。

14） CISA 等：Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software

2023 年 10 月、CISA 及び米国内外の 17 のパートナー機関[30]は、セキュアバイデザイン[31]・セキュアバイデフォルト[32]の実践に向けた推奨事項をまとめたガイダンスを改訂し、ソフトウェア開発者に対し、安全な製品を出荷するために必要な措置を講じるよう促した。日本からは、NISC 及び JPCERT/CC が共同署名している。表 1-15 に示すとおり、本文書では、ソフトウェア開発者に対し、セキュリティに関する 3 つの基本原則と各原則を実施するためのプラクティスが示されている。一部のプラクティスでは、経産省の文書（OSS 事例集及び SBOM 導入手引）が参考文書として引用されている。加えて、ソフトウェア開発者に対してセキュアバイデザイン・セキュアバイデフォルトを実践するための手法を示している他、ソフトウェア利用者に対する推奨事項も示している。

表 1-15 セキュアバイデザイン・セキュアバイデフォルトの実践に向けた推奨事項の概要

項目		内容 ※下線：経産省の文書が参考文書として引用されているプラクティス
ソフトウェア開発者に対する推奨事項	3 つの基本原則	**原則 1：顧客にもたらされるセキュリティの結果に責任を負う** 【セキュアバイデフォルトのプラクティス】 ・ 共通のデフォルトパスワードの廃止 ・ 実地テストの実施 ・ ハードニングガイドの縮小 ・ セキュアでないレガシー機能の使用停止 など 【セキュアな製品開発のプラクティス】 ・ 安全な SDLC の枠組み（SSDF 等）への適合の文書化 ・ 脆弱性管理の実施 ・ 責任を持った OSS の利用 など 【ビジネス上のプラクティス】 ・ 追加費用なしでのログ記録機能の提供 ・ 隠された負担の排除 ・ オープンスタンダードの採用 ・ アップグレードツールの提供 など
		原則 2：徹底的な透明性と説明責任を果たす 【セキュアバイデフォルトのプラクティス】 ・ セキュリティ関連の総合的な統計・傾向の公表 ・ パッチ適用の統計の公表 ・ 未使用の管理者特権データの公表 【セキュアな製品開発のプラクティス】 ・ 内部セキュリティ管理の確立 ・ ハイレベルな脅威モデルの公表

[30] 米 NSA、米 FBI、豪 ACSC、加 CCCS、英 NCSC-UK、独 BSI、蘭 NCSC-NL、諾 NCSC-NO、新 CERT NZ、新 NCSC-NZ、韓 KISA、以 INCD、日 NISC、日 JPCERT/CC、米 OAS/CICTE、昭 CSA、捷 NÚKIB
[31] IT 製品（特にソフトウェア）が、設計段階から安全性を確保されていること。
[32] ユーザー（顧客）が、追加コストや手間をかけることなく、購入後すぐに IT 製品（特にソフトウェア）を安全に利用できること。

項目		内容 ※<u>下線</u>:経産省の文書が参考文書として引用されているプラクティス
		・　安全な SDLC の枠組みへの自己適合証明の公表　など 【ビジネス上のプラクティス】 ・　担当取締役の指名・公表 ・　セキュアバイデザインのロードマップの公表 ・　メモリに安全なプログラミング言語の使用に関するロードマップの公表　など
		原則 3:トップ主導 ・　財務報告に対するセキュアバイデザインのプログラムの詳細の追記 ・　取締役会に対する定期的な報告 ・　担当取締役の権限強化 ・　意味のある企業内インセンティブの構築　など
	セキュアバイデザインの手法	・　メモリに安全なプログラミング言語の使用 ・　セキュアなハードウェア基盤の構築 ・　セキュアなソフトウェアコンポーネントの使用 ・　セキュリティ保護機能を持つ Web フレームワークの使用 ・　パラメータ化されたクエリの使用 ・　SAST/DAST によるセキュリティ評価の実施 ・　コードレビューの実施 ・　SBOM の作成 ・　脆弱性開示プログラムの確立 ・　CVE の完全性を担保多層防御による保護 ・　CISA の Cyber Performance Goals を満たす
	セキュアバイデフォルトの手法	・　共通のデフォルトパスワードの廃止 ・　管理権限のあるユーザーに対する多要素認証 ・　シングルサインオン（SSO）の実装 ・　セキュアなログの管理 ・　ソフトウェア認可プロファイルの役割や使用例に関する利用者への提示 ・　後方互換性ではなく将来を見据えたセキュリティの優先 ・　ハードニングガイドの縮小 ・　ソフトウェア利用者によるセキュリティ設定の負担軽減、UX の向上
ソフトウェア利用者に対する推奨事項		・　セキュリティ上の結果に関するソフトウェア開発者の責任の追求 ・　セキュリティバイデザインやセキュリティバイデフォルト慣行を取り入れた製品の優先購入 ・　開発者と戦略的な連携関係の構築、要望の調整、セキュリティの優先 ・　（クラウド利用の場合）責任分担の明確化、透明性の高い企業の優先

15） CISA:Software Identification Ecosystem Option Analysis

2023 年 10 月、CISA は、ソフトウェア識別のエコシステムを実現するための主要な要件と具体的な方法(「パス」と呼ぶ)に関するホワイトペーパーを発表し、パブリックコメントを開始した(期間は 2023 年 12 月 11 日まで)。具体的な要件・パスとして、識別子の可用性と粒度に関する要件と各要件に対応するパスが示されている(図 1-2)。本文書では、可用性と粒度の 2 つの要件を適切に満たす識別子は現在存在しないとしている。一方で、要件の一部に対応している既存識別子として、固有識別子を付与可能な OmniBOR、グループ化表現を利用可能な CPE、分散モデルや完全な識別子列挙が可能な purl が挙げられており、これらの識別子がエコシステム確立の出発点として機能すると結論づけている。

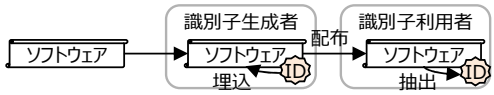
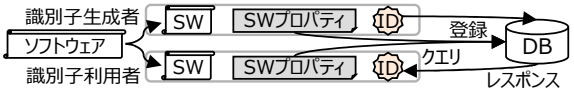
要件1: 可用性 必要なときに、必要な場所で識別子を使用可能にする	**パス1： 固有識別子を付与する**	任意の関係者が、ソフトウェアのインスタンスから一意に導出可能な固有のソフトウェア識別子を付与する。 
	パス2： 管理されていない分散モデルにより 識別子を付与する	中央機関の支援や調整無しに、複数の関係者によって識別子を付与する。 
	パス3： 管理された分散モデルにより 識別子を付与する	中央機関が複数の識別子生成者を支援や調整の上で、識別子を付与・管理する。 
	パス4： パス2と3の中間的位置づけ	外部調整なし（パス2）と、中央機関による調整有り（パス3）という2モデルの中間的方法で識別子を付与する。 ※ 例：複数の独立した組織において、共通の識別子規格を共有しつつ、各組織が独自に識別子を付与・管理する。
	パス5： パス2,3,4を補完する	識別子の無いソフトウェアについて、ソフトウェア固有の値（例：サイズ、ハッシュ、ソフトウェア名、バージョン）を構造化した情報を識別子の代替として使用する。
	パス6： 複数の識別子フォーマットを使用する	識別子生成者ごとに非結合となるようにグローバルソフトウェア空間を分割することで、過剰識別（単一ソフトウェアに複数の異なる識別子が付与される状態）を防止し、複数の識別子フォーマットの使用を可能とする。
要件2: 粒度 データアーティファクトの粒度をサポートする	**パス1： グループ化表現を用いた 細かな粒度とする**	個々のバージョン単位のように、細かい粒度の識別子をソフトウェアに付与する。 識別子に当該ソフトウェアが属するソフトウェア範囲の情報を埋め込むことで、ソフトウェアのグループを表現する。 ※ 例：CPEの場合、バージョンに「＊（アスタリスク）」を記述することで、別バージョンでも同一グループとして表現できる。
	パス2： 完全な識別子列挙をサポートする 細かな粒度とする	パス1と同様に、個々のバージョン単位のような細かい粒度の識別子をソフトウェアに付与する。 さらに、本パスでは、すべてのソフトウェアに対する識別子を完全に列挙し、ソフトウェアのグループを表現する際は、グループに属するソフトウェアの識別子を全て列挙する。

図 1-2 ソフトウェア識別エコシステムを実現するための主要な要件と具体的な方法(パス)の概要

16） NSA 等：Securing the Software Supply Chain: Recommended Practices for Software Bill of Materials Consumption

2023年11月、NSA、米国家情報長官室（ODNI）、CISAは、ソフトウェアサプライチェーンのセキュリティ確保のための SBOM 利用に関するガイダンスを発表した。ガイダンスでは、ソフトウェア利用者（例：サプライヤー、開発者、OSS・サードパーティ製のソフトウェアを取得する組織）による SBOM の利用に関する原則とベストプラクティスが示されている（表 1-16）。なお、米国政府による義務や推奨を示す位置づけではないとしている。

表 1-16 ソフトウェア利用者による SBOM の利用に関する原則とベストプラクティスの概要

項目		内容
SBOM の利用に関する原則	**自動化による広範囲の SBOM 利用に必要な要素**	・ 規模の拡大 SBOM データ形式や関係者間の運用のルール、SBOM の自動取込・解析の実現手段が必要 ・ ベースライン情報の整備 SBOM に含まれる基本的な情報の設定（例：製品バージョン、依存関係、作成者）が必要 ・ 共有と交換の自動化 SBOM の共有や交換を既存の組織内プロセスやツールへ統合が必要
SBOM の取得・管理・利用に関するベストプラクティス	**SBOM の取得・管理の流れ**	1. SBOM の取得 サプライヤーとの契約による納品物の一部としての受領等で、様々なメカニズムを通じて SBOM を取得する 2. SBOM の検証 SBOM 内に記述された方法や事前に合意されたプロセスによって、SBOM の完全性・真正性を検証する 3. SBOM の有効化 組織内で開発したツールや OSS ツール等を活用し、取得した SBOM を利用可能な状態へ有効化する 4. 組織内プロセス・システムへの SBOM の取込 調達、資産、脆弱性等の管理プロセス・システムへ SBOM を取込む 5. SBOM に基づく資産管理 専用ツールやシステムによって、SBOM に基づく調達、資産、脆弱性等を管理する
	SBOM の利用方法	・ コンポーネント情報の可視化 サプライチェーンリスク管理及び組織内リスク管理を実行する ・ 脆弱性の管理 利用中のソフトウェアに対する特定の脆弱性の影響度を特定する（VEX による脆弱性リスク管理）

項目		内容
	新しい SBOM の取得時における対応	利用中のソフトウェアについて、ソフトウェアのアップデート等により新しい SBOM を取得した際、ソフトウェア利用者は既存の SBOM と比較し、最後のバージョン以降に導入または削除されたコンポーネントや依存関係を特定する。
SBOM に基づくリスクスコアリングに関するベストプラクティス		SBOM を情報源とし、サプライチェーン内のリスクや組織へもたらす現在・将来のソフトウェアリスクを予測する。リスクスコアリングにおいては、脆弱性・ライセンス・コミュニティ（OSS コミュニティやサプライヤー等の開発者情報）・依存関係の 4 つの要素から特定する。
SBOM の運用に関する原則		組織内のすべてのソフトウェアを対象とし、SBOM の利用に関する自動化を実現するためには、組織内のサイバー方針と運用プロセスが必要である。適切な運用プロセスを導入することは、SBOM によって可視化されるリスクを最小化するための意思決定を可能にするための前提条件となる。

17） CISA：When to Issue VEX Information

2023 年 11 月、CISA は、VEX 情報を発行する組織・機能（Who）、VEX 情報が発行されるタイミング（When）の例示を整理した文書を発表した。表 1-17 に示すとおり、どのような組織・機能が VEX 情報を発行するかの例とどのようなタイミングで VEX 情報が発行されるかの例が示されている。なお、本文書では、ソフトウェアサプライチェーンにおける VEX の考慮事項についても示されている。

表 1-17 CISA 文書における VEX 情報の発行組織（機能）及び発行タイミングの例

項目		内容
VEX 情報の発行組織（機能）の例	サプライヤー	・ 製品、ソフトウェアパッケージ、ライブラリ等を提供する組織。具体的には、ソフトウェア開発者、ソフトウェアサプライチェーンにおける下流工程でのソフトウェア利用者、ソフトウェアを再パッケージ化するサードパーティが挙げられる。 ・ ソフトウェアが OSS の場合、コミュニティにおいてアクティブな開発者やメンテナーがサプライヤーとなる。このような役割が存在しない場合、コミュニティメンバーや下流工程での利用者が VEX 情報を発行することがある。
	リサーチャー	・ セキュリティ調査等の評価を実施し、潜在的な脆弱性を発見する個人または組織。具体的には、個人のセキュリティ研究者、学者、バグハンター、セキュリティ企業が挙げられる。
	脆弱性コーディネーター	・ ソフトウェア開発には関与せず、サプライヤー、リサーチャー等が社会全体のセキュリティリスクを最小化するために脆弱性を開示

項目		内容
		することを支援する組織。具体的には、CISA や JPCERT/CC が挙げられる。
	脆弱性検出・管理ツール	・ 脆弱性の検出・管理の機能を持つツール。具体的には、ソフトウェア構成分析（SCA）ツール、バイナリ解析ツール、ASPM[33]、SIEM[34]が挙げられる。
	その他の組織	・ 上記に加えて、セキュリティ検証の責任を負う可能性のある組織が挙げられる。具体的には、規制当局、サービスプロバイダー、監査人、ソフトウェアの販売企業、ソフトウェアのサポート業務を請け負う企業が挙げられる。
VEX 情報の発行タイミングの例	**上流工程に脆弱性が発見された場合**	・ ソフトウェアに含まれる上流工程のコンポーネントに脆弱性が発見された場合、該当コンポーネントに関する VEX 情報を発行するよう、ソフトウェア利用者から開発者へ求められる。
	社会的に大きな注目を浴びた場合	・ 「名前付き脆弱性」など、脆弱性が社会的に注目を集めている場合、VEX 情報の発行が求められる。ソフトウェア利用者は、VEX 情報から悪用可能性や緩和策の情報を入手する。
	積極的な脆弱性の悪用が確認された場合	・ 特定の脆弱性に対して、VEX 情報の脆弱性ステータスが「影響を受ける」となる可能性がある場合、VEX 情報を発行して、関係者へ通知される。通知を受領した者は、VEX 情報から攻撃の可能性を防ぐための方法を入手する。
	脆弱性に対する影響のステータスを変更する場合	・ 新たな脆弱性が公開された場合、VEX 情報として脆弱性のステータスは「調査中」として発行される。調査終了後に、「影響を受ける」または「影響を受けない」へステータスが変更され、更新された VEX 情報が発行される。
	協調的脆弱性開示（CVD）へ VEX 情報を統合する場合	・ CVD と VEX は独立した取り組みであるが、関係者が脆弱性の状態を周知したい場合は、CVD の取り組みの中で VEX を使用することが可能である。
	法的要件や契約条件による義務が生じた場合	・ VEX 情報を発行する義務が生じる法的要件が定まる場合がある。また、契約条件により、サプライヤーが VEX 情報を提供することが要求される場合がある。

18） CISA 等:Joint Guidelines for Secure AI System Development

2023 年 11 月、CISA 及び英国国家サイバーセキュリティセンター（NCSC）は共同で、セキュアな

[33] Application Security Posture Management の略で、アプリケーションの継続的なリスクモニタリングや管理を行うシステム
[34] Security Information and Event Management の略で、ネットワークを監視し、セキュリティインシデントの検知を行うシステム

AIシステムの開発のためのガイドラインを発表した。なお、本ガイドラインは、日本を含む18か国のパートナー機関[35]が共同署名している。本ガイドラインでは、AI システム開発のライフサイクルにおける 4 つのフェーズ(設計、開発、導入、運用・保守)ごとに、セキュアな AI システムを開発し、リスクを防止のための対応方法が示されている(表 1-18)。

表 1-18 セキュアな AI システムの開発のためのガイドラインの概要

フェーズ	内容
セキュアな設計	**脅威とリスクに対する開発者の意識付け** 開発者は、セキュリティ脅威・システムの機能不全に対する意識を持ち、セキュアなコーディング技術や AI に関するセキュアなプラクティスを身につける。
	システムに対する脅威のモデル化 システムに対する脅威を評価するためのプロセス(システムが予期せぬ挙動をした場合の影響範囲の理解や意思決定の方法を含む)を構築する。
	機能性やパフォーマンスに限らず、セキュリティを確保するための設計 外部コンポーネントを使用する場合のリスク、標準的なセキュアな開発・運用のベストプラクティスの実践等によってセキュリティ上の緩和策を考慮する。
	セキュリティ上の利点とのトレードオフを考慮した AI モデルの決定 脅威モデルに基づき、モデルアーキテクチャー、設定、訓練データ、訓練アルゴリズム、ハイパーパラメータを選択し、AI モデルを決定する。
セキュアな開発	**サプライチェーンセキュリティの確保** サプライヤーに対して、自組織がソフトウェアに適用しているのと同基準を遵守するよう要求する。遵守できない場合は、自組織のリスク管理ポリシーに従い対処する。
	アセットの特定・監視・保護 モデル、データ、プロンプト、ログ等の AI 関連のアセットを特定し、機密データとして管理する。また、アセットの監視・認証の他、バージョン管理を行うことで、アセットを保護する。
	データ、モデル、プロンプトの文書化 モデル、データセット、メタプロンプト、運用等に関する内容を文書化する。文書には、訓練データの情報源、ハッシュ値等のセキュリティ関連情報を含める。
	技術的負債(追加改修コスト)の管理 あらゆるソフトウェアシステムと同様に、AI システムの開発ライフサイクルを通じた、技術的負債(追加の改修に係るコスト)を特定し、 管理する。
セキュアな導入	**インフラにおけるセキュリティの確保** 外部 API、モデル、データ、データの訓練、処理パイプライン等のシステムのあらゆる局面に対して、アクセスコントロールを適用し、インフラのセキュリティを確保する。
	継続的なモデルの保護

[35] 米 NSA、米 FBI、豪 ACSC、加 CCCS、新 NCSC-NZ、智 CSIRT、捷 NUKIB、愛沙尼亜 RIA、愛沙尼亜 NCSC-EE、仏 ANSSI、独 BSI、以 INCD、伊 ACN、日 NISC、日内閣府科学技術・イノベーション推進事務局、尼日利亜 NITDA、諾 NCSC-NO、波 MC、波 MASK、韓 NIS、昭 CSA

フェーズ	内容
	標準的なサイバーセキュリティプラクティスを実装した上で、不正アクセス・改ざんを検知・排除するためにクエリインターフェースを監視し、モデル・データを保護する。
	<u>インシデント管理手順の策定</u> インシデントの管理手順を策定し、定期的に評価を行う。また、インシデント対応者に対しては、インシデントの評価や対処のための訓練を実施する。
	<u>責任のある AI のリリース</u> ベンチマークやレッドチーム等による適切で効果的なセキュリティ評価を実施後、AI システムをリリースし、既知の制約や潜在的なリスクについて利用者へ説明する。
	<u>利用者による適切なシステム使用を実現</u> モデルやシステムの適切な利用に関するガイダンスを提供する。ガイダンスには、システムの限界・機能不全、利用者データの使用・保管に関する内容を含める。
セキュアな運用と保守	<u>システムの挙動の監視</u> システムを監視することで、セキュリティに影響を及ぼす可能性のある挙動を検知し、AI システムによるアウトプットやパフォーマンスを測定する。
	<u>AI システムへのインプットの監視</u> AI システムへのインプット（例：推論要求、クエリ、プロンプト）を監視・記録することで、システムの悪用時における調査や対処を可能とする。
	<u>セキュアバイデザインのアプローチを遵守したアップデート</u> デフォルトで自動アップデート機能を実装する。アップデートにより、アウトプット等の AI システムの挙動へ、影響を与える可能性がある旨を利用者へ説明する。
	<u>AI システムの開発や運用に関するプラクティスの収集と共有</u> 情報共有コミュニティへの参加、経済界・学術界・政府のグローバルエコシステムとの協力により、セキュアな AI システムに関するベストプラクティスを共有する。

19） CISA 等：The Case for Memory Safe Roadmaps

2023 年 12 月、CISA は、米国家安全保障局（NSA）、米国連邦捜査局（FBI）、国際的なパートナー機関[36]と共同で、メモリ安全なプログラミング言語への移行に関するガイダンスを発表した。本ガイダンスでは、メモリ安全なプログラミング言語を使用することで、メモリに係る脆弱性を排除・最小化することが可能と位置づけられ、ソフトウェア開発者に対して、メモリ安全なプログラミング言語へ移行するための考慮事項・課題、移行計画の作成に関する事項が示されている（表 1-19）。

表 1-19 メモリ安全なプログラミング言語への移行に関するガイダンスの概要

項目		内容
メモリ安全なプログラ	メモリ安全なプログラミング言語への移行の優	・ ソフトウェア開発者は、移行計画や具体的な方針を通じ、メモリ安全なプログラミング言語への移行の優先順位付けを行う

[36] 豪 ACSC、加 CCCS、英 NCSC、新 NCSC-NZ、新 CERT-NZ

項目		内容
ミング言語への移行を計画する際に考慮すべき事項	先順位付け	べきである（例：小規模プロジェクトから移行を開始、セキュリティ上重要なコードから改修）。
	メモリ安全なプログラミング言語の選択	・ メモリ安全なプログラミング言語は多くの種類が存在し、アーキテクチャー、ツール、パフォーマンス、普及度、コスト等の観点で優位性が異なるため、ユースケースを評価しつつ、最も適した言語を選択すべきである。
	開発者の能力向上と人材の確保	・ ソフトウェア開発者は、選択した言語において、開発者の能力をどのように向上するか、関連スキルを有する人材をどのように優先的に採用するか、選択した言語をサポートするためにどのようなリソースが必要かを検討すべきである。
メモリ安全なプログラミング言語へ移行する際に注意すべき課題	セキュリティへのシフトに伴う影響	・ セキュリティを重視することで、製品の安全性や信頼性が向上し、ソフトウェア開発者・利用者に利益をもたらす。一方で、使用する言語によっては、メモリ安全なコードを記述するために、移行前と比較して時間を要する可能性がある。
	システムパフォーマンスへの影響	・ メモリ安全なプログラミング言語の一部は、メモリの自動開放を実施するが、システムリソースを消費するため、CPU・メモリのパフォーマンスへ影響を与える可能性がある。特に、リアルタイム性が求められる環境下において、パフォーマンスに影響を与える。
	既存のメモリ非安全な言語の取扱	・ メモリ安全な言語は、ほぼ確実にメモリ非安全な言語（C や C++で記述されたライブラリ等）に依存する。メモリ非安全な言語をすべて書き直すことは難しく、メモリ安全な言語とメモリ非安全な言語のハイブリッドで開発を行わなければならない。
	メモリ安全保証の回避の禁止	・ 一部の言語では、メモリ安全保証を回避可能である（例：Rust で記述されたコードにて unsafe コードを使用する等）。 しかし、メモリ安全性に係る脆弱性を排除するためにも、メモリ安全保証を回避すべきではない。
	コンピュータサイエンス教育の加速化	・ 学生へのコンピュータサイエンスプログラムの多くは、メモリ安全に関する教育は不十分となっている。ソフトウェア業界と教育現場の双方でメモリ安全に関する教育機会を創出する方法を考えるべきである。
	OT・低消費電力・IoT システムにおけるメモリ安全な言語への移行	・ メモリ、CPU、ネットワーク接続において制約のある、OT・低消費電力・IoT システムでは、メモリ安全なプログラミング言語の利用が困難な場合があるため、事前に、パフォーマンス、信頼性、リアルタイム保証の実証を行う必要がある。

項目	内容
メモリ安全なプログラミング言語への移行計画の作成に関する事項	・ メモリ安全なプログラミング言語への移行計画（メモリ非安全なコードを削減・排除する計画）を作成・公表すべきである。 ・ 移行計画には以下の要素を含めるべきである。 ✓ 日付・実施事項・成果を定義したフェーズ ✓ メモリ安全な言語のみでコードの記述を開始する日付 ✓ メモリ安全な言語に関する開発者向けの教育計画 ✓ 既存のメモリ非安全な言語の取扱計画 ✓ 移行計画の更新計画 ✓ CVE サポート計画（例：各 CVE への CWE 情報の付加）

20） CISA 等：Securing the Software Supply Chain: Recommended Practices for Managing Open-Source Software and Software Bill of Materials

2023 年 12 月、CISA、NSA、ODNI は、安全なソフトウェアサプライチェーンの確保に向けた OSS や SBOM の管理のための推奨プラクティスを示す文書を発表した。表 1-20 に示すとおり、本文書では、OSS と SBOM の管理に関する 7 つのテーマに関して、推奨のプラクティスが示されている。

表 1-20 OSS と SBOM の管理に関する推奨プラクティスの概要

テーマ		内容
OSS の採用段階（Sec.2、3）	**OSS の選定方法（Sec. 2.1、3.1）**	・ OSS 採用の検討初期段階では、脆弱性 DB2 等の情報を活用し、OSS を事前評価し、採用を検討すべきかを判断する。 ・ 開発するソフトウェア製品や設計要件に基づき、OSS の必要性を開発者が特定する。 ・ OSS の採用決定に当たっては、品質・他者採用事例・ライセンスの種類・脆弱性の履歴・時間やコストの利点を考慮する。
	OSS ライセンスの確認（Sec. 2.2）	・ OSS の採用を検討する際は、OSS のライセンスに関して、以下を明確化する。 ✓ OSS を使用するための法的権利を有していること ✓ コード共有の義務により、自社のプロプライエタリなコードの汚染・知的財産権の侵害が発生しないこと ✓ 関連するライセンスポリシーに遵守していること
	OSS の輸出に関する確認（Sec. 2.3）	・ OSS を組み込んだ製品を輸出する際、OSS が規定に遵守するよう要求される場合があるため（例：輸出管理規則など）、ソフトウェアの輸出に関する法的な確認をソフトウェア開発のプロセスに含める。

テーマ		内容
	OSS のリスク評価 **（Sec. 3.2）**	・ 脆弱性とリスクの評価について、サードパーティの OSS のインベントリーを作成し、OSS コンポーネントのバージョンが最新であるかどうか、既知の脆弱性が含まれるかどうかを脆弱性 DB2 等の情報を参考に検証する。 ・ 各コンポーネントに対し、当該コンポーネントだけでなく、依存関係にあるサードパーティ製のコンポーネントの脆弱性を特定する。なお、サードパーティ製のコンポーネントで発見した脆弱性は、影響を受けるすべての組織へ報告し、脆弱性の状況は継続的に追跡すべきである。
OSS の使用段階 **（Sec.4）**	**OSS のメンテナンス** **（Sec. 4.1）**	・ OSS に含まれる脆弱性の特定方法を定義し、インベントリー管理をどのように実行するかを整理した継続計画を策定・実行する。なお、OSS の SBOM が既に存在する場合、SBOM は、インベントリー管理の自動化、新たな脆弱性が発見された際に活用されることがある。
	OSS に関する危機管理 **（Sec. 4.2）**	・ 脆弱性対応を含む OSS に関する危機管理のための計画（危機の定義・対応方針・体制・プロセス）を立て、危機管理を実行する。 ※危機とは、企業の評判、製品、目標、事業価値、事業運営能力、顧客の評判を損なう可能性がある状況を指す。 ・ 脆弱性の対応に関する SBOM や VEX の作成・提供をソフトウェア開発ライフサイクルに統合する。
安全なソフトウェアの提供と SBOM の作成 **（Sec. 5）**		・ 安全なソフトウェアの開発・提供に向け、SBOM に関する以下の活動を実施する。 ✓ インベントリー管理：製品がどのように構築され、どのようなコンポーネントから構築されているかを理解する。 ✓ SBOM の作成：ソフトウェアに含まれるライブラリやコンポーネントを一覧化し、定期的に追跡を支援するツールを活用する。 ✓ OSS の分析と VEX 情報の活用：ソフトウェア内に含まれる脆弱なライブラリやコンポーネントを特定し、緩和策を特定する。 ✓ ライセンスと輸出管理：OSS を使用するプロジェクトに責任と配布の問題を引き起こす可能性のある情報を管理する。 ✓ SBOM の検証：SBOM が様々なツールに統合可能か、SBOM の内容が正確に記述されているかを確認する。

21） CISA：Guidance on Assembling a Group of Products

2024 年 1 月、CISA は、複数ソフトウェアによって構成される製品に対する SBOM 作成に関するガイダンスを発表した。ガイダンスでは、複数ソフトウェアによって構成される製品の具体例として、組み込みソフトウェア製品、IoT 製品、PC、サーバー等が挙げられている。本ガイダンスでは、複数ソフトウェアによって構成される製品の SBOM を作成するための必須事項・推奨事項が示されている（表 1-21）。

表 1-21 複数ソフトウェアによって構成される製品の SBOM を作成するための必須事項・推奨事項

項目	内容
必須事項	・ 使用する識別子を決定すること。 ・ 識別子に使用するバージョン管理システムを決定すること。 ・ 複数ソフトウェアによって構成される製品に含まれるすべてのコンポーネントを一覧化すること。 ・ 各コンポーネントのバージョン番号を提供すること。 ・ 各コンポーネントの実行可能なソフトウェアファイルに対する SBOM の参照情報を提供すること。
推奨事項	・ 各コンポーネントに対応付けられた、アーティファクトのハッシュを提供すること。（アーティファクトの例としては、tarball、zipfile、コンテナイメージ、インストールパッケージ、ディスクイメージ、ソースファイルが挙げられる。また、マシン固有のもの（例：x86、arm）である場合もある。なお、同じ種類のハッシュを適用することが推奨されるが、必須ではない。） ・ ソフトウェアコンポーネントの識別子は、purl、CPE、SWID タグを使用して提供すること。 ・ SBOM の作成者は、ソフトウェア製品を組み立て、リリースするエンティティであること。

また、図 1-3 に示すとおり、複数ソフトウェアによって構成される製品に対する SBOM のイメージが示されている。

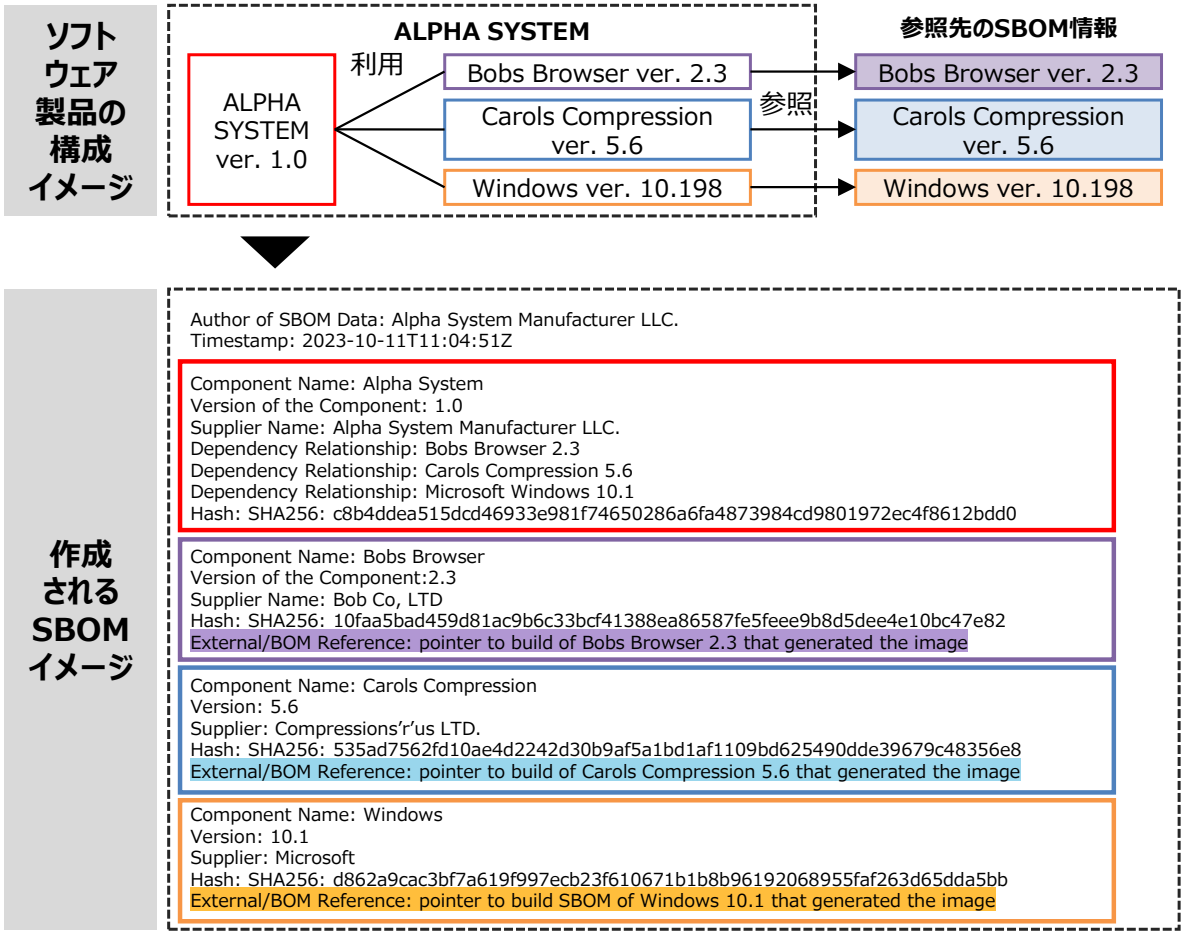


図 1-3 複数ソフトウェアによって構成される製品の SBOM のイメージ

22) CISA:SBOM-a-rama Winter 2024

2024 年 2 月、CISA の主催により、SBOM コミュニティの醸成を目的とし、「SBOM-a-Rama Winter 2024」がオンラインで開催された。本イベントでは、各国の SBOM に関する取組状況、CISA のおける SBOM や VEX の WG の活動状況等について発表された。アジェンダ及び各セッションの概要は以下のとおりである。

表 1-22 SBOM-a-rama Winter 2024 のセッション概要[37]

セッション名（プレゼンテーション名）	概要
Germany's Work on SBOM in EU CRA Context	EU サイバーレジリエンス法（CRA）の SBOM 要件に関する、ドイツ BSI の取組について概説された。具体的には、CRA の概要と、発効に向けた現状の状況（EU 議会による可決が 2024 年 6 月までに期待され、公布後 36 ヶ月で発効する予定）が示された。加えて、BSI の取組として、SBOM の技術ガイドラインが紹介された。本ガイドラインは、製造業者向けの推奨事項とし

[37] CISA より公開されているプレゼンテーション資料に基づき作成 https://www.cisa.gov/resources-tools/resources/sbom-rama-february-2024-session-presentations

セッション名 （プレゼンテーション名）	概要
	て、EU や国際的な議論の基盤とされているとし、SBOM の内容、範囲、フォーマットに関する要件が含まれている。
CISA Tooling & Implementation WG	前回（2023/6/14）の SBOM-a-rama から今回（2024/2/29）の期間における、CISA による SBOM のツール及び実装に関する活動が概説された。具体的には、複数ソフトウェアによって構成される製品の SBOM に対するアプローチ、SBOM ツールの分類、SBOM の最小要素に対する実用的なガイダンス公開に関する活動が紹介された。また、SBOM ツールの評価と分類の基準に関する活動が紹介され、関連するホワイトペーパーと基準のワークシートを含む文書のドラフトを作成している旨が示された。 今後の予定として、WG へのさらなる参加を促進し、SBOM 要素の記述と公開に関する実用的なガイダンスを完成させるとともに、SBOM ツールの分類体系を更新することが挙げられた。
CISA Sharing & Exchanging WG	CISA による SBOM の共有に関する活動が概説された。具体的には、SBOM の共有に関する役割定義、SBOM の共有事例が示された。役割について、SBOM の作成者・配布者・消費者という 3 つの主要な役割を定義し、特に配布者の役割は、SBOM の作成や利用をしない組織の役割を捉えるために新たに追加したとしている。共有事例について、電子メール経由で共有される独自ソフトウェアの SBOM、ベンダーのポータルサイトを通じて共有される SBOM、OSS のツール経由での共有等の事例が挙げられた。 今後の予定として、SBOM の共有事例の文書化、セクター固有のエンドツーエンドの SBOM 共有におけるセキュリティ、ライセンス、運用、監査に関する議論、既存及び新しい PoC の実行が挙げられた。
CISA Cloud & Online Applications WG	CISA による SaaS のソフトウェアの透明性に焦点を当てた議論の活動が概説された。具体的には、SBOM が、クラウド及びオンラインアプリケーションの環境下の場合と、オンプレミスソフトウェアの場合でどのように異なるか、異なる関係者（開発者、セキュリティ専門家、エンドユーザー）ごとに SBOM にはどのような利点があるか等について示された。また、SaaS のソフトウェアベンダーや利用者に対し、SBOM をどのように利用・推進するかについての行動を促した。 今後の予定として、データのガバナンスやリスク指標の議論などが挙げられた。
CISA VEX WG	CISA による VEX に関する活動について概説された。具体的には、VEX の概要、VEX に関する発行文書、今後取り組むべき事項について示された。 今後取り組む事項の具体例として、「エンドツーエンドの VEX の実装」、「脆弱性管理プロセスへ VEX を統合することの利点」、「現時点の VEX の実践に係る評価（VEX の何が機能しているか/何が機能していないか、VEX のユースケース、プロセスモデル、アーキテクチャーの分析）」が挙げられた。

セッション名 （プレゼンテーション名）	概要
CISA ON-Ramps & Adoption WG	CISA による SBOM の普及と採用を促進するための活動について概説された。具体的には、SBOM の採用に関する動向や取組について示された。現在の主な取組として、SBOM に関する FAQ の更新、ソフトウェア利用者が SBOM を活用して意思決定を行うためのガイダンスの作成、政策による義務に対応するために企業が SBOM をどのように活用できるかについての情報提供等が挙げられた。
Software Identification	CISA によるソフトウェア識別のエコシステムの分析と今後の予定について概説された。ソフトウェア識別の問題として、複数の命名規則や識別方法が存在することで、セキュリティや管理の複雑さを引き起こすと指摘し、この問題に対する解決策（パスと呼ぶ）として、「Software Identification Ecosystem Option Analysis」に記載の 6 つのパスが紹介された。
DOD SBOM Collaboration	DOD が組織する Joint Federated Assurance Center（JFAC）が概説された。JFAC の目的は DOD のソフトウェアとハードウェアの保証能力を提供することであり、全ライフサイクルにわたる包括的な保証を実現し、信頼性を構築することとしている。
Open SSF SBOM Activities	Open Source Security Foundation（OpenSSF）による「SBOM Everywhere」イニシアチブが概説された。本イニシアチブの目標は、開発・保守・OSS 利用のセキュリティを持続的に強化することを容易にすることである。また、SBOM の命名とディレクトリ慣行に関するベストプラクティス文書[38]が紹介した。本イニシアチブへの貢献方法に関する情報も含まれており、GitHub リポジトリや Slack、ミーティングへの参加方法についても案内された。
DHS S&T Silicon Valley Innovation Program	DHS S&T が実施する Silicon Valley Innovation Program（SVIP）が概説された。SVIP の目的は、革新的な商業技術への移行を加速し、初期段階のスタートアップ企業の製品ロードマップに DHS の要件を組み込むことで、製品を市場に展開にする際に DHS の要求を満たすようにすることである。本プログラムは、スタートアップ企業に対し、24 ヶ月間で最大 800,000 USD から 2,000,000 USD を提供し、24 ヶ月以内に市場投入準備が整うことを条件としている。なお、DHS はソフトウェアセキュリティ要件において、最小要素を含む SBOM を提供することを求めている。
Healthcare Industry Update	ヘルスケア分野における SBOM の PoC の活動が概説された。本活動は、「調査（2018-2019 年）」、「反復（2020-2021 年）」、「統合（2022 年-現在）」の 3 段階にわたり、SBOM の主要なユースケースを試行し、SBOM 利用者にとっての価値を評価してきた。また、標準フォーマット、データ、ツールの実現可能性を実証することで、実証結果を基に SBOM 生成のためのガイ

38

セッション名 （プレゼンテーション名）	概要
	ドを作成し、SBOM 共有の自動化などを進めてきたことが示された。現在、Health-ISAC と連携し、SBOM および VEX の生成、共有、利用の評価を行っており、医療機器に影響を与えないコンポーネントの脆弱性に焦点を当てた VEX の生成に取り組んでいることが紹介された。加えて、医療機器製造業者が医療機関と SBOM を共有できるプラットフォームとして、Health-ISAC SBOM リポジトリも紹介された。

CISA はこれまで複数の WG を設置して検討を進めてきたが、SBOM-a-rama Winter 2024 後、この検討体制を変更することを発表している。具体的には、5 つの WG やそのサブ WG は多すぎるという意見を踏まえ、週次の会議を一つ設定し、その中で SBOM コミュニティの醸成を図ることを発表している。また、「Tiger Team」と呼ばれるチームを結成し、これまでの SBOM に関する成果物を取り込みつつ、新たな成果物の開発を目指すとしている。

23） CISA：Secure Software Development Attestation Form

2024 年 3 月、CISA は、OMB 覚書（M-22-18 及び M-23-16）を受け、連邦政府機関が調達するソフトウェアに対して、ソフトウェアベンダーが SSDF の実装の適合性を証明するための共通フォームを公開した。本共通フォームは、2023 年 11 月から 12 月にかけて実施したパブリックコメントの結果を反映したものである。表 1-23 に示すとおり、本案共通フォームでは、自己適合証明書フォームの対象となるソフトウェア、フォームの提出方法、提出免除、フォームの具体的な記載事項等が示されている。

2024 年 3 月 18 日には、ソフトウェアベンダーが自己適合証明書フォームをアップロードするためのリポジトリが正式に公開[39]された。

表 1-23 共通フォームの概要

※*青字斜体*は、パブコメ時点のフォーム案からの修正を意味する。

項目	内容
対象ソフトウェア	以下のソフトウェアは、自己適合証明書フォームの提出が求められる。 ・ 2022 年 9 月 14 日以降に開発されたソフトウェア ・ *2022 年 9 月 14 日以前に開発されたが、*2022 年 9 月 14 日以降にメジャーバージョンアップにより変更される既存のソフトウェア ・ ソフトウェアベンダーがソフトウェアコードを継続的に変更し、配信するソフトウェア（例：SaaS 製品） ただし、以下のソフトウェアは対象外であり、自己適合証明書フォームは不要である。

[39] https://www.cisa.gov/news-events/alerts/2024/03/18/repository-software-attestation-and-artifacts-now-live

項目	内容
	・ 連邦政府機関によって開発されたソフトウェア ・ 連邦政府機関が直接、自由に入手できる OSS ・ *連邦政府機関が使用するソフトウェアの最終製品に組み込まれるサードパーティ製の OSS 及びプロプライエタリなソフトウェアコンポーネント* ・ 自由に入手可能で、一般に公開されているソフトウェア
自己適合証明書フォームの提出方法	以下のいずれかで自己適合証明書フォームを提出することができる。 ・ オンラインフォームによる提出 ・ 自己適合証明書(PDF ファイル)を添付したメール送信による提出
自己適合証明書フォームが提出されない場合における連邦政府機関の対処	自己適合証明書フォームを取得できず、ソフトウェアを使用する場合、連邦政府機関は以下の事項を実施しなければならない。 ・ ソフトウェアベンダーから自己適合証明書フォームを取得できない旨を特定する文書を取得 ・ ソフトウェアベンダーから自己適合証明書フォームを取得できないことによって生じるリスクを軽減するため、連邦政府機関が実施している事項をまとめた文書を作成 ・ ソフトウェアベンダーに対して、自己適合証明書フォームの提出までの行動計画・マイルストーン(POA&M)の作成を要求
自己適合証明フォームの提出免除	対象ソフトウェアが、FedRAMP 制度において認定された第三者評価機関または適切な認定機関が認定した第三者評価機関によって、関連する NIST ガイダンスに基づき評価された場合、ソフトウェアベンダーは自己適合証明書フォームを提出する必要はない。ただし、対象ソフトウェアを評価した第三者評価機関が作成した関連文書の提出は必要である。
自己適合証明書フォームにおける記載概要	セクション 1:対象ソフトウェアに関連する情報 セクション 2:ソフトウェアベンダーに関連する情報 セクション 3:SSDF 実装の宣誓、添付文書(提出免除のための関連文書を含む)に関する情報

また、表 1-24 に示すとおり、自己適合証明書フォーム案における具体的な記載事項が示されている。

表 1-24 自己適合証明書フォーム案の記載事項

※*青字斜体*は、パブコメ時点のフォーム案からの修正を意味する。

項目	内容
セクション 1(対象ソフトウェア情報)	当該証明書について、新たな証明書、延長または免除後の証明書、証明書の改訂のいずれであるかを選択する。 対象ソフトウェアについて、以下の情報を記入する必要がある。 ・ 製品名 ・ 製品のバージョン番号

項目	内容
	・ 製品のリリース日
セクション 2（ソフトウェアベンダー情報）	申請者情報について、以下の情報を記入する必要がある。 1. ソフトウェアベンダー ・ 企業名 ・ 住所 ・ 都市名 ・ 州または県 ・ 郵便番号 ・ 国名 ・ 企業の Web サイト 2. 本フォーム及び関連情報の主な連絡先 ・ 名前 ・ 役職 ・ 住所 ・ 電話番号 ・ メールアドレス（メールエイリアスや配信リストでも可）
セクション 3（SSDF 実装の宣誓）	SSDF 実装の宣誓として、以下の内容を確認し、**ソフトベンダーの CEO または COO が**日付と併せて署名する必要がある。 また、本フォームに付録や文書が添付されている場合（提出免除のための関連文書も含む）、添付文書名とその内容を記載する必要がある。 ソフトウェアベンダーは、対象のソフトウェアを開発する際、SSDF から抜粋した以下の実施内容を実装していることを証明すること。 1. ソフトウェアを安全な環境で開発・構築するため、少なくとも以下の事項を実施すること。 a. ソフトウェアの開発・構築に関連する各環境を分離・保護する。 b. 以下に対する認可とアクセスに使用される安全性の定期的な記録・監視・監査する。 i. ソフトウェアの開発・構築のための環境 ii. 各環境内のコンポーネント間 c. セキュリティリスクを最小限に抑えるために、ソフトウェアの開発・構築に関連する環境において、多要素認証や条件付きアクセスによる保護する。 d. ソフトウェアの開発・構築に使用される環境において、過度なリスクを引き起こすソフトウェア製品の使用または包含を最小化するだけでなく、文書化するための一貫した合理的な措置を講じる。 e. 実用的な範囲やリスクに基づいて、認証情報等の機密データを暗号化する。

項目	内容
	f. 運用やアラートの継続的な監視、必要に応じたサイバーインシデント対応等を含む防御的なサイバーセキュリティ対策を実施する。 2. ソフトウェアに組み込まれた内部コードやサードパーティのコンポーネントに対するセキュリティへ対処し、関連する脆弱性を管理するため、自動化されたツールまたは同等のプロセスを採用し、信頼できるソースコード・サプライチェーンを維持するために尽力すること。 3. *実行可能な最大限の範囲で*、ソフトウェアに組み込まれた内部及びサードパーティのコードの来歴を維持すること。 4. セキュリティの脆弱性をチェックするための自動化ツールまたは同等のプロセスを採用すること。さらに、以下の事項を実施すること。 a. 採用したプロセスを継続的、*かつ*製品リリース時・バージョンアップ時・更新プログラムのリリース前に運用する。 b. 発見されたセキュリティ脆弱性をリリース前に対処するためのポリシーやプロセスを構築する。 c. 脆弱性開示プログラムを運用し、開示されたソフトウェアの脆弱性を、脆弱性開示プログラムまたは適用されるポリシーで指定されたスケジュールにしたがって、適時に受け入れ、レビューし、対処する。

1.1.2 SBOM と脆弱性管理に関わる課題等の整理

本事業では、ソフトウェアに関するリスクを適切にコントロール（管理、低減）することを目的としている。ソフトウェアのリスクとしては、脆弱性に起因するセキュリティリスクや、ライセンスに関わる法的リスクなどが存在するが、本調査では、主に脆弱性リスクを管理するための課題や方法について検討する。脆弱性リスクの管理においては、以下のようなことが求められる。

表 1-25 脆弱性リスクの管理区分と目的・要求

リスク管理の区分	リスク管理の目的・要求
リスク回避・受容	・ 脆弱性リスクの高いソフトウェア部品の評価、調達・利用の判断
リスク低減	・ ソフトウェアに残留する脆弱性の特定の網羅性向上 ・ 脆弱性の特定と対応の迅速化
リスク移転	・ 脆弱性リスクの責任分担、損害補償

これらを実現する上で、ソフトウェアの構成や品質の透明性を確保することが基盤となる。そのための手段としてソフトウェアの構成情報を管理・共有するための SBOM が重要になる。

SBOM を活用した脆弱性管理については、本年度調査および過年度の実証、タスクフォースに基づき課題を挙げると以下のようになる。

- 部品 ID の一意性が確保できず、脆弱性マッチングの障害となる。（CISA, Software ID Ecosystem

等）

- 脆弱性 DB が多数存在し、影響を受けるソフトウェアの ID 管理がグローバルに体系化されていない。（実証、SBOM-a-rama 等）
- 脆弱性の悪用可能性、誤検知、検出漏れなどにより脆弱性対応の負担増加、対応遅延などが生じる。（CISA, Minimum Requirement for VEX, CISA, When to issue VEX, 実証等）
- サプライチェーンを通じた SBOM 更新情報、脆弱性負荷情報の共有タイミングや対応法が明確はなく、迅速かつ継続的な対応が難しい。（CISA, SBOM Sharing Lifecycle Report, NSA Securing the Software Supply Chain, 実証等）

以上のような課題について、脆弱性管理プロセスに基づき全体像を示したものが下図である。

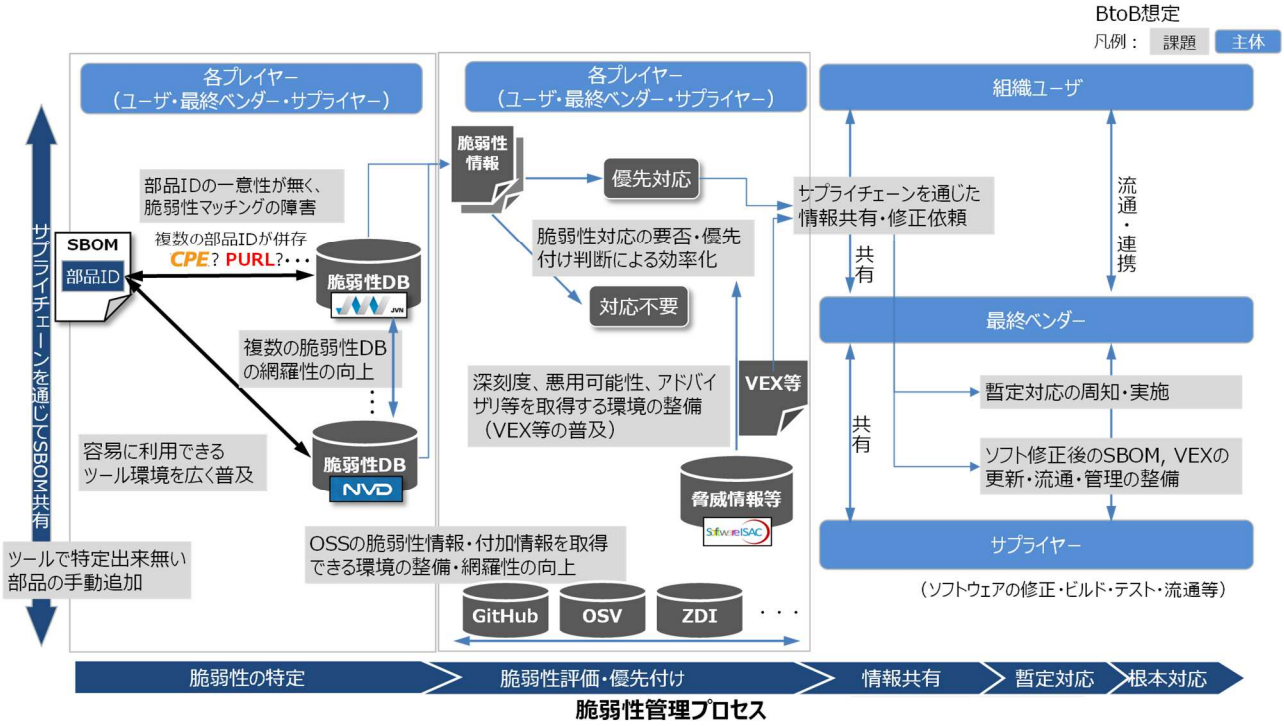


図 1-4 脆弱性管理プロセス全体における主な課題の整理

SBOM を活用した脆弱性管理の効率化・普及促進に向けて、各プレイヤー、ユーザーなどにおいて様々な対応が必要であり、特に脆弱管理プロセス（脆弱性の特定、脆弱性評価等、情報共有、対応）における課題として整理される。

SBOM を活用した脆弱性管理を組織において実現・実装していくため、次章においては、これらの課題の解決のため方法や手順について、実システムに対する具体的な試行を通じて評価すべき事項を特定し、実証を通じて得られた知見、ノウハウ、今後取り組むべき事項を整理する。

1.2 SBOM と脆弱性情報等の情報の紐づけを効率的・効果的に行う仕組みの構築に向けた実証事業の実施

1.2.1 実証の目的

本実証では、脆弱性管理プロセスを俯瞰し、SBOM を活用した脆弱性管理の効率的な方法について検討し、その効果評価、課題の整理を行う。脆弱性情報の提供に係る機関（IPA，ISAC 等）と連携し、脆弱性情報を効率的に取得する方法を検討する。

SBOM を活用した脆弱性管理を広く普及させるため、中小企業を含む多くの企業が活用できるように、脆弱性の深刻度、脅威、アドバイザリなども活用するための方策等について整理する。

実証における脆弱性管理のスコープ、ステークホルダーを俯瞰したものは下図の通りである。

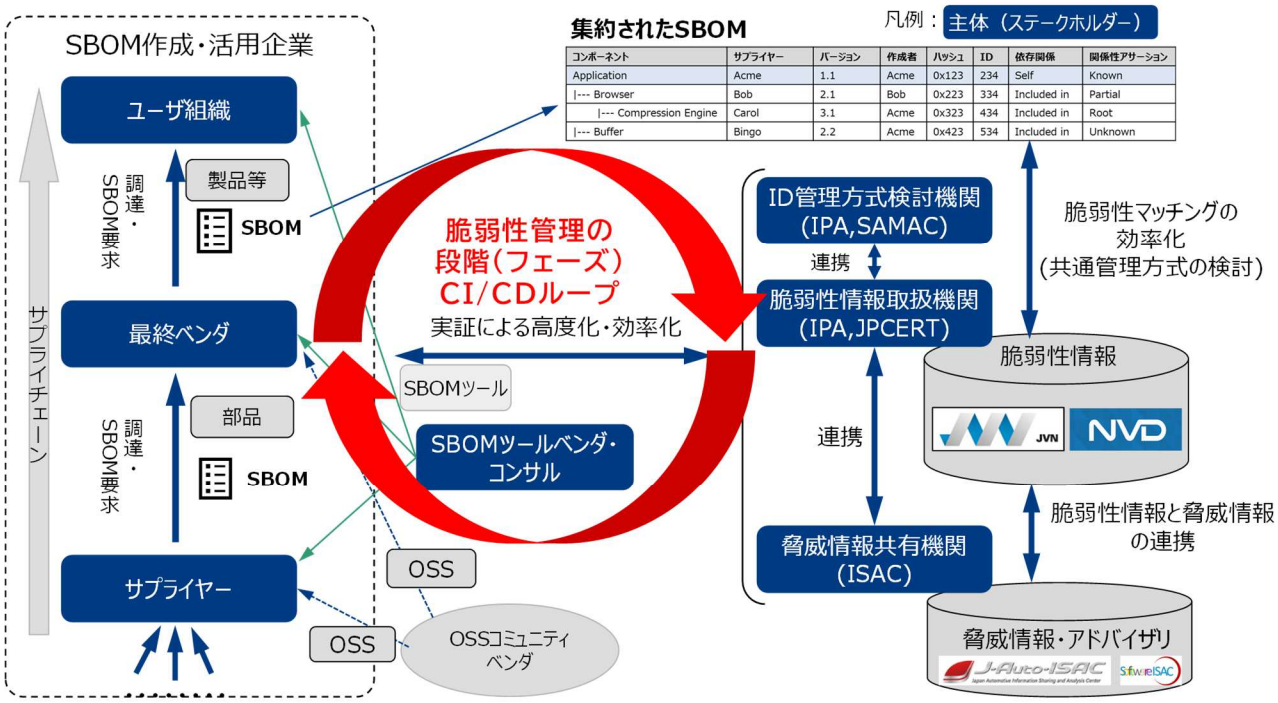


図 1-5 実証における脆弱性管理の全体像

これらのプロセス、ステークホルダー全体を通じて SBOM を活用して効果的に脆弱性管理を行う方法や課題について整理する。

1.2.2 基本方針と実証の進め方

SBOM を活用した脆弱性管理について全体を俯瞰して課題を抽出し、それらの課題に対する解決策、ノウハウ、今後の取組を整理することで、脆弱性管理の効率化、高度化、普及促進を図ることを基本方針とする。

1） 脆弱性管理に係る課題の特定
過年度の実証、タスクフォース、動向調査に基づき SBOM を用いた脆弱性管理に係る課題についてプロセスに基づく全体像を整理する。

2） 実証の要件定義
脆弱性管理に係る課題に基づき、実証において評価すべき事項、課題解決の方法など検討すべき事項についての要件を定義する。

3） 実証の体制と対象システムの検討
実証の要件に基づき必要な体制と対象システムの検討し、関係組織との調整を行う。

4） 実証項目の具体化
実証の体制および対象システムに応じて実証項目の具体化を行う。

5） 実証項目の実施、成果・課題等の整理
実証項目に必要な環境構築、実証項目の実施・計測などの結果に基づき、成果および課題の整理を行う。

1.2.3 実証の要件

（1） SBOM を活用した脆弱性管理の課題

SBOM に関する過年度からの動向調査、実証、タスクフォース議論に基づき、SBOM を活用した脆弱性管理の課題について 1.1.2 にまとめたものを再掲する。

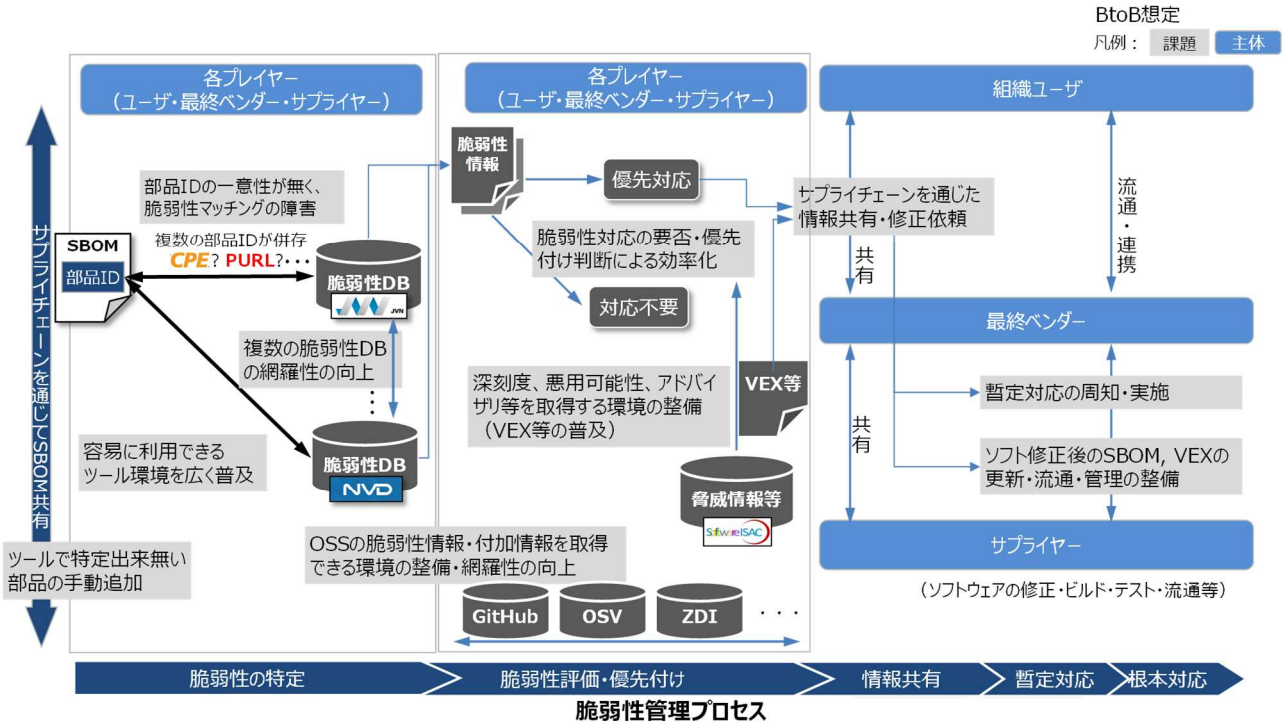


図 1-6 脆弱性管理プロセス全体における主な課題の整理（再掲）

SBOM を活用した脆弱性管理を組織において実現していくため、これらの課題について解決するた

めの方法や手順が求められる。本実証においては、これらの課題について、実システムに対する具体的な試行を通じて得られた知見、ノウハウ、今後取り組むべき事項を整理する。

（2）SBOM 実証の要件定義

前節に示した課題について、課題解決のために実証すべき事項を整理すると下表のようになる。本実証においては、これらを実証の要件として、実システムに対する実証項目を具体化し、各項目に関する解決方法、手順、評価について整理する。

表 1-26 SBOM 実証の要件

脆弱性管理プロセス	課題	課題解決のために実証すべき事項（実証の要件）
(1)脆弱性の特定（VM）	VM1：部品の識別子の一意性	SBOM で用いられる複数の部品 ID 標準（CPE, PURL 等）について、SBOM 作成時の部品 ID 選択の考え方の整理しつつ、脆弱性 DB の API・ツールを用いて脆弱性マッチングを行う方法等を特定する。
	VM2:照合する脆弱性 DB の網羅性確保	複数の脆弱性 DB について、API・ツールを用いることで脆弱性マッチングの網羅性を拡大する方法を整理する。
	VM3：広く利用可能なツールの整備	・ SBOM ツールの選定など SBOM 利用者がすべき事項を特定し、選定観点を整理する（選定観点の例：対応する部品 ID,脆弱性 DB のカバー率など）。 ・ 操作性、ドキュメント、価格などの点で中小企業なども利用しやすいツールの要件や課題について検討する。
(2)脆弱性評価・対応優先付け（VT）	VT1:脆弱性関連情報の活用	脆弱性情報に加え、民間組織、ベンダーにより提供される脆弱性付加情報の種類（深刻度、悪用可能性、アドバイザリ等を）や取得可能性ついて評価する。
	VT2:脆弱性評価に基づく対応方針ロジック	脆弱性対応の優先付けの基本的な考え方を検討し、必要となる付加情報の種類を特定する。（個社の優先付けポリシーの考え方などツールで出来ないことを特定する）
	VT3:OSS の脆弱性付加情報取得	脆弱性 DB から OSS に関する脆弱性付加情報の取得可否、課題を確認する。

(3)情報共有・対応分担方針検討(RP)	RP1:情報共有基盤	特定した脆弱性、付加情報を共有する方法、フォーマット等を検討し、妥当性を確認する。
	RP2:サプライチェーン上の役割分担検討	原因特定、修正・対応などの依頼・役割分担する方法を検討し、ツールでは対応できない情報の共有方法等について整理する。
(4)脆弱性対応(暫定対応、根本対応)	TR1:暫定対応の整理	暫定対応の選択肢を整理し、影響を受ける組織による周知について整理する。
	FR1:根本対応の共有・適用	修正コードに対応した SBOM の更新、通知、履歴管理について整理する。

1.2.4 実施スケジュール

実施スケジュールの全体像を下記に示す。

実証の要件定義に基づき、対象ソフトウェア、実施体制の候補を検討し、実証企業との調整を経て対象ソフトウェアに対応した実証項目の具体化を行う。実証遂行と並行し、タスクフォースを開催し、委員からの意見に基づき、方向性の検討、見直しを行い、成果の取りまとめを行う。

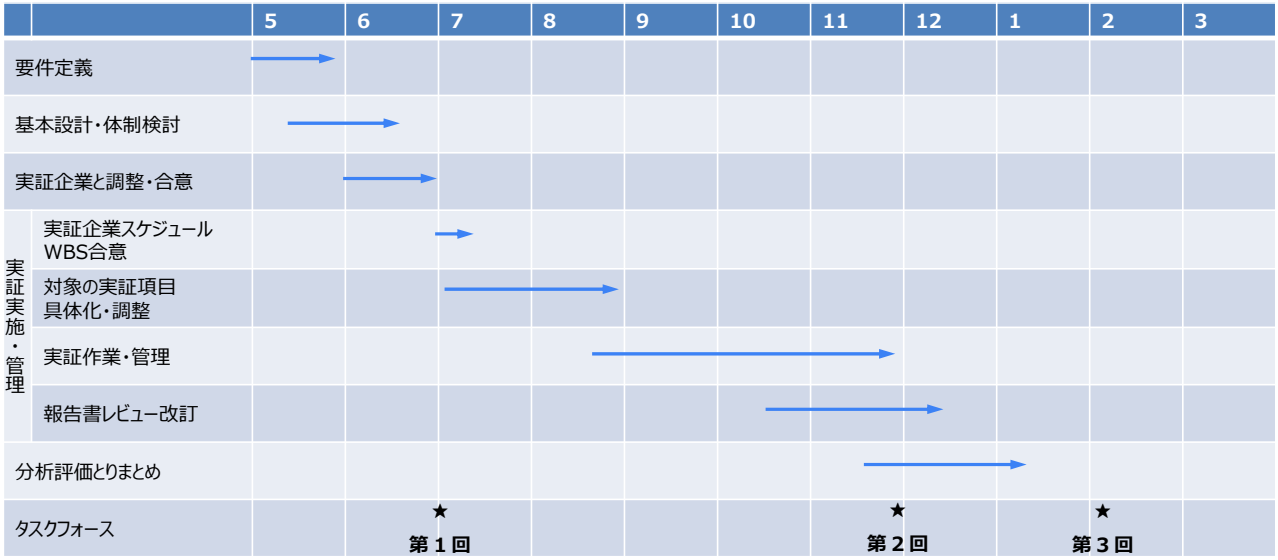


図 1-7 実施スケジュール

1.2.5 実施体制

事業全体を統括する経済産業省の下で、三菱総合研究所が、実証の課題、要件定義、実証項目の設定、脆弱性管理プロセス等の手法の検討、事業者管理、成果の分析、課題の整理などを行った。

1.2.6 実証対象システム

(1) 対象システムの選定の考え方

実証の対象システムとして、分野共通で広く利用される重要なソフトウェアを対象とする。重要なソフトウェアとしては、NIST が定義する重要ソフトウェア、EU CRA で定義される重要なデジタル製品区分から選定する。候補として、基盤的で広く利用されることを重視し、セキュリティ・ソフトウェア、OS を想定し、SBOM の作成または取得ができるものを選定する。

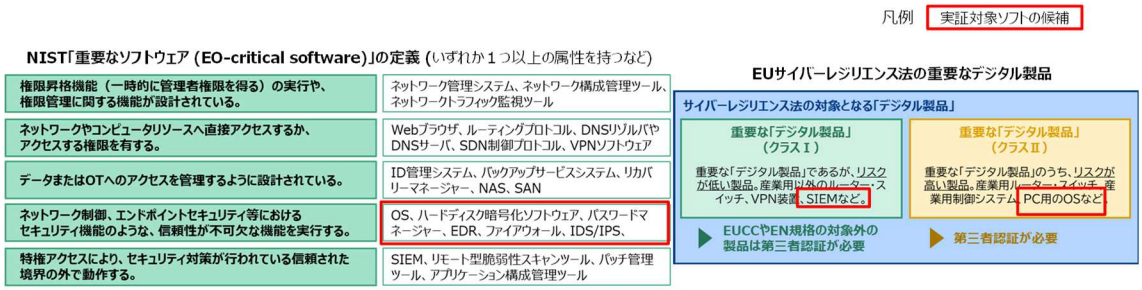


図 1-8 NIST や EU CRA で定義される重要なソフトウェア

今回はこの基準に基づき、OS として様々な業界で利用される Linux 製品 A[40]、およびファイアウォール等の機能を含む**セキュリティ製品ソフト（以下「セキュリティ製品ソフト」）**を選択した。

（2）対象システムの概要と構成

1）Linux 製品 A

Linux 製品 A ディストリビューションであり、Enterprise Server や Enterprise Desktop など複数のエディションがある。

Linux 製品 A Enterprise のシステム構成および SBOM の生成範囲については下図の通りである。今回 Linux 製品 A Enterprise のインストールメディアに対して発行された SBOM を対象としており、インストールメディアは複数エディションのインストールに対応している。インストールメディアには各エディションに必要なモジュールが含まれており、各エディションに含まれるアプリケーションおよび OS コンポーネントすべてを対象とした。

[40] 本ドキュメントに記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。

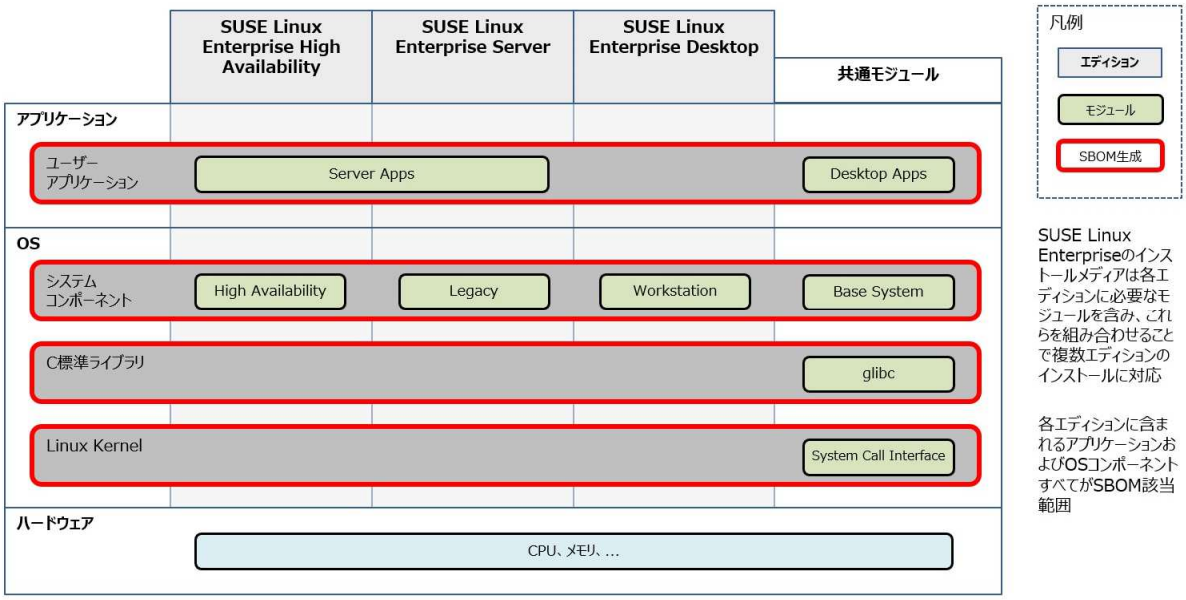


図 1-9 Linux 製品 A Enterprise の構成と SBOM 生成範囲

SBOM は外部サイトから取得し[41]、実証で利用した SBOM は SPDX/json フォーマットである。

2）セキュリティ製品ソフト

セキュリティ製品ソフトは、Windows OS 向けの統合管理機能を備えたクライアント/サーバー向けの総合セキュリティ対策製品であり、不正プログラム、ネットワークウイルス、Web ベースの脅威、スパイウェア、および複合型の脅威の攻撃から企業のネットワークを保護する[42]。

エンドポイントに配置されたエージェントと、すべてのクライアントを管理する管理コンソールで構成され、エージェントはエンドポイントを保護し、エンドポイントのセキュリティステータスをサーバーに報告する。サーバーからは、Web ベースの管理コンソールを使用して、セキュリティポリシーの設定とアップデートの配信を各エージェントに対し行うことができる。

セキュリティ製品ソフトのシステム構成および SBOM の作成範囲については下図の通りである。今回の SBOM 作成の範囲としては管理コンソールを対象とし、自社開発コンポーネントおよび OSS コンポーネントを SBOM 生成の対象とした。

[41] https://www.suse.com/download/sles/
[42] https://www.trendmicro.com/ja_jp/business/products/user-protection/sps/endpoint/officescan.html

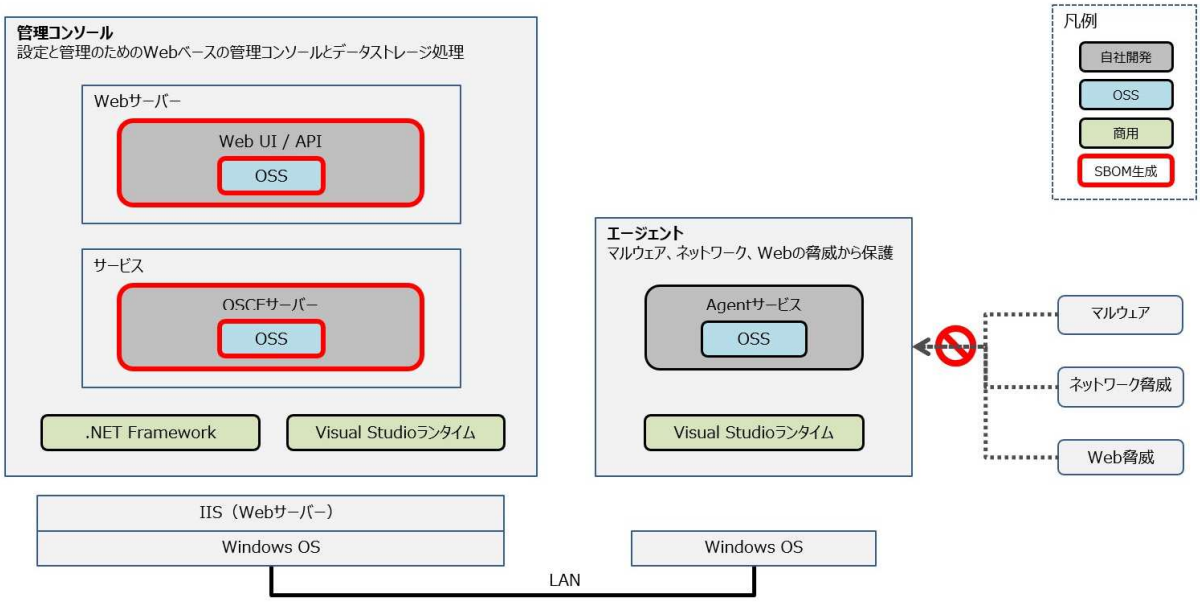


図 1-10 セキュリティ製品ソフトの構成と SBOM 作成範囲

SBOM は社内 SBOM ツールにて生成し、実証で利用した SBOM は SPDX/json フォーマットである。

1.2.7 実証項目の具体化

本実証については、ソフトウェア開発企業とソフトウェアユーザ企業の二つの種類の企業を念頭に実証を行った。本報告書におけるこれら企業の定義を下表に記す。

表 1-27 ソフトウェア開発企業とソフトウェアユーザ企業

カテゴリ	定義
ソフトウェア開発企業	・ OSS やサプライヤーからの提供されるソフトウェアコンポーネントなどを組み込み、ソフトウェアを開発・提供する企業 ・ SaaS 製品、パッケージ製品など不特定多数のユーザーに提供するソフトウェアベンダー、または最終開発ベンダーに対してライブラリやフレームワークなどを提供するソフトウェアサプライヤー、特定の企業の依頼を受けて、受託開発を行う企業など
ソフトウェアユーザ企業	・ ソフトウェア開発企業からソフトウェアの提供を受け、ユーザーとしてそのソフトウェアを利用する企業

脆弱性対応においては、ユーザー向けに提供している製品内に含まれる脆弱性についての対応を実施する必要があるソフトウェア開発企業と、自社が利用している製品やシステムにある脆弱性への対応が必要なソフトウェアユーザ企業では、必要な対応や検討事項が異なる可能性がある。したがって、本

実証では、脆弱性対応の各フェーズにおける、ソフトウェア開発企業ならびにソフトウェアユーザ企業の双方での活動の実情を調査するとともに、SBOM を用いた対応の効率化に関して検討を実施した。各フェーズでの実施内容は以下の表の通りである。

表 1-28 企業タイプ別の実証項目一覧

フェーズ	ソフトウェア開発企業	ソフトウェアユーザ企業
脆弱性特定	・ Linux 製品 A のものを含む複数の SBOM を比較・検証し、他社が作成した SBOM と自社がもつ SBOM の情報を比較、検証し、それぞれから部品 ID またはその同等の意味で使用できる情報の相互交換法の検討を実機調査にて行う(1.2.12(1)3)a、1.2.14(2)) ・ 部品 ID または部品 ID に紐づけ可能な情報によって CVE DB や JVN から API やツールを用いて脆弱性の発見が可能か、実機調査および机上調査にて検証する。これら DB で期待する結果が得られない場合には、ほかの脆弱性 DB で代替できるかを検討する(1.2.12(1)3)a、1.2.12(1)3)c、1.2.14(1)) ・ 脆弱性 DB1/脆弱性 DB2 API/無償 SBOM ツール A に対する入力として用いる場合を確認し、異なるツールから出力された SBOM がある場合にも、特定コンポーネントに関する脆弱性を取得する方法を実機調査および机上調査にて検討する(1.2.12(1)3)a) ・ CVE DB, 脆弱性 DB2 以外で、OSS などの脆弱性情報を扱う DB(KEVC、Google OSV, GitHub, ZDI)について整理し、CVE ID のない脆弱性情報がどの程度あるか机上調査する(脆弱性の数そのもののカバー率に対する寄与度を検証する)。データについては 2022 年に新たに報告された脆弱性の情報をもとに判定する(1.2.12(1)1)、別紙)	・ ヒアリングを通じて、現在実施している脆弱性の特定フローを確認する(1.2.12(1)2)) ・ 中小企業や SBOM の知見が少ないユーザー企業を想定した場合の、無償 SBOM ツール A/脆弱性 DB1 の機能・ドキュメント・操作性について実機調査を元に評価し、自社で利用している製品の脆弱性特定に関する課題や、必要な機能追加・改善について整理する(1.2.14(3)、1.2.14(5))

脆弱性評価・優先付け	・ 脆弱性の評価を実施する際に、優先度付けや修正方針などを決定するフロー、ならびに必要な情報についてヒアリングによりまとめる。また人による意思決定が必要である点について、判断基準や、その妥当性、根拠などに関して例をもとにまとめる(1.2.12(2)2)) ・ 1)で調査対象とした OSS 脆弱性情報 DB に関して、脆弱性付加情報の調査カバレッジにおいて脆弱性 DB2 以外からの情報取得による効果を机上調査にて検討する。また得られた情報を元に脆弱性対応フローの効率化や改善を考えた場合に、既存の DB でカバーできる情報、または追加で必要となる情報や機能について考察する(1.2.12(2)1)、別紙) ・ 各脆弱性 DB からの脆弱性付加情報の取得に関して、机上および実機調査にてその手法をまとめる。また特に対応の効率性向上の観点から、現在の課題やニーズについて整理する(1.2.12(2)1)、1.2.12(2)4)) ・ SBOM または SCA ツールによる脆弱性情報を実機調査にて確認し、優先度付けや修正方針にもたらす効果を検証し、まとめる(1.2.12(2)4)) ・ VEX 情報を ISAC など外部から取得する方法、また脆弱性評価やトリアージへの活用について机上調査にて検討し、現在の課題や活用方法についてまとめる(1.2.12(2)4)、1.2.13(1)) ・ 机上調査および実機調査によって、社内で VEX 情報を作成・提供する場合の方法を検討し、課題や機能ニーズを整理する(1.2.12(3)3))	・ ヒアリングを通じて、脆弱性が公表された場合に対応する際のフローについて情報収集する ・ 評価や優先付けに関して用いている判断基準、情報ソースについてヒアリングにより確認する。また必要と考えている情報について現状の課題についても同様に確認する(1.2.12(2)2)) ・ ユーザー企業の対応フローにおいて、対応のために重要な情報が、現在どこから取得できるかヒアリングする。またそれらの情報を SBOM と紐づけるための方法について机上にて検討する(1.2.12(2)2)、1.2.12(2)4)) ・ 机上および実機調査を通じ、SBOM を活用した場合の、対応の効率性向上、または判断精度の向上などに対する影響を考察する(1.2.14(4)) ・ 机上および実機調査を通じ、ユーザー企業が VEX 情報を取得し活用する場合のフローや、想定される課題などについて整理する(1.2.13(1))

情報共有	・ ヒアリングにより修正コードと関連情報について、影響を受けるステークホルダーや、情報共有の方法において、現在の A 社内プロセスや考え方をベースにまとめる。その中での課題や、SBOM や SCA ツールを介した情報共有を行う場合に関連する内容を同定し、整理する。フローの整理においては脆弱性情報の起点となりうるポイントについても考慮し、起点の違いのよるフローの違いについてもまとめる(1.2.12(3)1)) ・ 社内の共通モジュール開発チームを仮想サプライヤーとみなし、仮想サプライヤー担当のコンポーネント内に存在する脆弱性に関しての想定情報共有フロー、また他チームとの役割分担や脆弱性に関する情報共有プロセスについても合わせてヒアリングを通じて整理する。同様に脆弱性情報の起点となるポイントについて考慮し、フローの違いについて整理する(1.2.12(3)2)) ・ フローの各ポイントにおいて、情報共有に利用される・または利用可能なツールについて整理する。また自社作成の SBOM や SCA ツールが活用可能な部分についてもヒアリングおよび机上調査にて検討する(1.2.12(3)1)) ・ VEX に基づいた情報共有が社内ならびに社外ユーザーにもたらすメリット・デメリットについ机上調査にて検討するとともに、現状の情報共有において VEX 情報を追加した場合のフローと課題について検討する(1.2.12(3)3))	・ ベンダーからの情報提供、またはユーザー企業からの問い合わせの詳細について、実情をヒアリングする ・ 現在 A 社以外のソフトウェアベンダーが実施している情報提供の手法(メール、Web 告知など)と、その内容についてもヒアリングを行う(1.2.12(3)1)) ・ SBOM を介した情報共有を行う場合の、利点と課題について机上調査にて検討する。また同様に VEX 情報が付加されていた場合の、ユーザー側での対応の変化を考察する(1.2.13(1))

暫定対応	・ ヒアリングを通じて得た開発者として製品に対して行う暫定対応策の種類を整理し、選択の判断ロジックと妥当性を確認する。妥当性確認の際には、既存の攻撃コードの有無や、顧客の対応難易度なども考慮に入れる(1.2.12(4)) ・ 暫定対応情報を提供する場合の、情報提供についてフローをヒアリングと机上調査にてまとめるとともに、課題について検討する(1.2.12(4)) ・ ソフトウェア会社から提供される(製品そのものに対処を実施するタイプの)暫定対応策以外で、ユーザー企業がとれる暫定対応策の種類を、机上調査を通じて整理する。またその判断ロジックと妥当性について、同様に確認する(1.2.12(4))	・ 修正モジュール提供前に、ユーザー側で暫定対応を実施する場合、その内容、および実施可否についての判断フローをヒアリングし、整理する。またその決断において重要視される因子について同定する(1.2.12(4)) ・ 現状の情報公開において含まれる情報が、ヒアリングに基づいて同定したユーザーが重要視する情報をカバーしているかどうか確認し、不足している場合には、追加のために必要な対応について検討する(1.2.12(4))
根本対応	・ ヒアリングを通じ、修正コードと関連情報について、影響を受けるステークホルダーや、情報共有の方法において、現在の A 社のプロセスや考え方をベースにまとめる。その中での課題や、SBOM を介した情報共有に関連する内容を同定し、整理する(1.2.12(4))	・ 自社情報システム部門へのヒアリングを通じて、修正モジュール提供後の対応フローについてヒアリングする(1.2.12(4)) ・ 修正適用前後における SBOM の管理について、Linux 製品 A の SBOM を例に机上にて検討および課題の同定を行う(1.2.14(6))
その他共通	・ NIST SSDF、EU CRA の要求事項のうち上記プロセスで対応可能な事項、対応できない事項を机上調査にて特定する(1.2.14(8)、1.2.14(9))	・ 主に EU CRA の要求事項のうち、ユーザー企業で必要なものとして上記プロセスで対応可能な事項、対応できない事項を机上調査にて特定する(1.2.14(9))

1.2.8 実証の手順

前項「(6)実証項目の具体化」に記載した内容を実施するため、以下のような手順で実証を行った。

(1) [脆弱性特定・脆弱性優先付け] 脆弱性 DB の比較・調査

脆弱性特定・および脆弱性優先付けの際の情報源として活用可能な脆弱性 DB とその特質を比較するため、複数の脆弱性 DB の調査を行った。調査に当たっては、各 DB の公式 Web サイトの情報を元に、提供している情報や API などについて確認を行った。対象とした DB は以下の通りである。DB の選定に当たっては、日本や米国で公的機関が提供している DB や、主なセキュリティベンダー、コミュニティが提供している DB，開発者やセキュリティ研究者が利用している DB などについて、Web 検索に基づき選定した。

- JVN
- JVN iPedia
- NVD
- KEVC
- Google OSV
- GitHub Advisory Database
- ZDI Published Advisory
- Snyk vulnerability DB
- Exploit database
- VirusTotal
- vulDB
- CNNVD

(2) [脆弱性優先付け] 脆弱性 DB と SBOM の突合手法の調査

SBOM 内の部品情報と、脆弱性 DB 内の情報を紐づけるために、複数のツールから作成される SBOM 内に含まれるデータについて調査を実施した。また、該当情報を脆弱性 DB 内で検索するための手法について、サーバー、クライアントのシステムインタフェースの形態に基づき以下の 3 つの手法に分けて調査を実施した。

1) 脆弱性 DB の API またはデータフィードを利用する場合(以下、「API 利用」)
2) 脆弱性 DB の Web ページに存在する検索機能を用いる場合(以下、「Web UI 利用」)
3) SBOM をインポートする機能を持つツールを用いて脆弱性情報を突合する場合(以下、「既存ツール利用」)

API 利用については、主に脆弱性 DB2 と脆弱性 DB1 API を用いて検証を行った。例えば、脆弱性

DB2 では脆弱性データベースを検索するための API が提供されている[43]。入手した SBOM の部品 ID から脆弱性 DB2 API を利用して脆弱性を検索する Python スクリプトを作成し、自動化の実証を行った。利用する API は CVE API v2.0 であり、以下の URL を利用する。

URL：https://services.nvd.nist.gov/rest/json/cves/2.0

SBOM 内の packages に含まれる部品 ID（今回の検証では purl）を基に、CVE API のパラメータとして使われる CPE を生成し、それを用いて脆弱性の検索を行っている。以下は検索時の値の例である。

表 1-29 検索時の値の例

項目	値
SBOM 内 packages に含まれる部品 ID（purl）	pkg:rpm/suse/curl@8.0.1-150400.5.23.1?arch=x86_64&upstream=curl-8.0.1-150400.5.23.1.src.rpm&distro=sles-15.5
部品 ID から生成された CPE	cpe:2.3:*:*:curl:8.0.1:*:*:*:*:*:*:*

この検索により、指定された CPE にマッチする脆弱性の一覧、および各脆弱性の詳細などが json フォーマットで取得できる。またレスポンスのスキーマも公開されている[44]。また、脆弱性 DB2 API を利用したのと同様の方法で脆弱性 DB1 API も利用した。

既存ツール利用については、社内で導入済みの有償 SCA ツールである有償 SBOM ツール A の他、IPA 提供のツール無償 SBOM ツール A を用いた確認を行った。加えて、OSV.dev にて提供されている OSV Scanner について公式ドキュメントの情報を元にした机上調査を実施した。

有償 SBOM ツール A については、は Amazon Web Service（以下、AWS）上に構築された Kubernetes 環境上に展開されているサーバーと SaaS 版の双方を用いた。AWS 上の Kubernetes 環境のインフラ仕様は下表の通りである。

表 1-30 有償 SBOM ツール A 展開環境の仕様

項目	値
インスタンスタイプ	r5.4xlarge
vCPU 数	16
メモリ	128GB
ストレージ容量	2 TB
OS	Ubuntu Linux
データベースインスタンスタイプ	db.m5.8xlarge

[43] https://nvd.nist.gov/developers/vulnerabilities
[44] https://csrc.nist.gov/schema/nvd/api/2.0/cve_api_json_2.0.schema

（3）［情報共有］VEX の作成作業

脆弱性情報共有について関連する作業を検証するため、オープンソースで提供されている vexctl[45]を利用して VEX の作成を行った。vexctl はコマンドラインベースのツールであり、実行には Go 1.16 以降の実行環境が必要である。VEX の作成は「go run github.com/openvex/vexctl@latest create」で実行され、下表のパラメータを指定する。

表 1-31 vexctl のパラメータ

パラメータ	値
--product	製品の ID、purl
--vuln	脆弱性の ID、CVE ID
--status	脆弱性ステータス、以下の値から選択 ・ not_affected ・ affected ・ under_investigation ・ fixed
--justification	ステータスが not_affected の場合、以下の値から選択 ・ component_not_present ・ vulnerable_code_not_present ・ vulnerable_code_cannot_be_controlled_by_adversary ・ vulnerable_code_not_in_execute_path ・ inline_mitigations_already_exist

以下は実行コマンドと出力の例である。入力されたパラメータの値に基づき、OpenVEX[46]の形式で出力される。impact_statement のような補足情報については出力結果に手動で追記することが可能である。

>go run github.com/openvex/vexctl@latest create --product=”pkg:swid/trendmicro/officescan@10” --vuln=”CVE-2017-17969” --status=”not_affected” --justification=”vulnerable_code_not_in_execute_path”

{
”@context”: ”https://openvex.dev/ns”,
”@id”: ”https://openvex.dev/docs/public/vex-ebd742a29e90b7ee9d61327d0e5534fcf920c4122011d5c439f83af74be5e1c6”,
”author”: ”Unknown Author”,
”role”: ”Document Creator”,
”timestamp”: ”2023-10-27T08:47:57.909697+09:00”,

[45] https://github.com/openvex/vexctl
[46] https://github.com/openvex/spec/blob/main/OPENVEX-SPEC.md

```
  "version": "1",
  "statements": [
    {
      "vulnerability": "CVE-2017-17969",
      "products": [
        "pkg:swid/trendmicro/officescan@10"
      ],
      "status": "not_affected",
      "justification": "vulnerable_code_not_in_execute_path"
    }
  ]
}
```

なお、vexctl が公開されている GitHub のページには、VEX ファイルの活用ユースケースとして、「セキュリティスキャナーでの読み込みによる、影響のない脆弱性の除外」が挙げられている[47]ものの、本調査では実際に VEX ファイルを読み込んで活用するツールは発見できなかった。

（4）［全フェーズ］ソフトウェア開発企業・ソフトウェアユーザ企業における脆弱性対応

企業における脆弱性対応の実態を把握するため、ヒアリング調査を実施した。

ソフトウェア開発企業での実態については、A 社の開発チームおよび PSIRT チームが実施している対応やプロセスを元に、一般的に実施されていると想定される内容をまとめることとした。

ソフトウェアユーザ企業における実態については、トレンドマイクロ社の情報システム部門担当者にヒアリングを実施し、ソフトウェアユーザ企業の実態として一般化した内容をまとめた。また、中小企業のセキュリティの実態については、A 社内で中小企業のセキュリティについて研究している社員にも実情[48]を聞いた。

また、脆弱性対応のうち、特に脆弱性優先付け対応については、まとめた情報を元に、優先度を決定に参照できるプロセスと判断ツリーを策定した。

なお、脆弱性対応プロセス全般の考察に当たっては、NIST Secure Software Development Framework[49] および欧州のサイバーレジリエンス法[50]（以下、EU CRA）において、脆弱性対応に関してソフトウェア開発企業・ユーザー企業が求められる行動についても合わせて実施した。

---

[47] https://github.com/openvex/vexctl#readme

[48] https://ipsj.ixsq.nii.ac.jp/ej/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=216799&item_no=1&page_id=13&block_id=8

[49] https://csrc.nist.gov/Projects/ssdf

[50] https://www.european-cyber-resilience-act.com/Cyber_Resilience_Act_Articles_(Proposal_15.9.2022).html

（5）［全フェーズ］人的コスト算出

脆弱性対応の各フェーズにおいてソフトウェア開発企業・ユーザー企業で必要となると想定される人的コストを、本実証で実施した作業での実績を元に算出した。算出に当たっては、2021 年度の実証に倣い、一般社団法人日本ニアショア開発推進機構の「エンジニア単価情報 2021 年版レポート」を参照した。技術レベルごとのエンジニア単価の対応は下表の通りである。なお、1 時間当たりの単価を月額参考価格から計算するにあたっては、1 ヶ月の業務時間を 160 時間として算出した。

表 1-32 人的コストの算出方法

技術レベル	説明	1 時間当たりのエンジニア単価（円）
初級者	開発エンジニアまたは IT エンジニアとして 3 年未満の経験があるエンジニア。役割別エンジニア単価情報 2021 の「IT アーキテクト系」エンジニアのレベル 2 に相当	4,820
中級者	開発エンジニアまたは IT エンジニアとして 3-7 年以上の経験を持つ。エンジニアとして自立して業務が可能なレベル。役割別エンジニア単価情報 2021 の「IT アーキテクト系」エンジニアのレベル 3 に相当	5,350
上級者	アーキテクトなど、技術的な方向性を決定する上位エンジニア。役割別エンジニア単価情報 2021 の「IT アーキテクト系」エンジニアのレベル 4 に相当	6,350

1.2.9 実証における制約条件等

（1） ソフトウェア開発企業におけるサプライヤーの扱い

ヒアリング対象であった A 社では、OSS は用いているものの、基本的に外部サプライヤーを利用した製品開発を行っていない。したがって、本実証では、社内で製品共通ライブラリを開発しているチームを仮想のサプライヤーとみなして調査を実施した。そのため、一般的な外部サプライヤーの行動や、最終ソフトウェアベンダーとの関係性について、調査内容と実態が一部異なる可能性がある。

（2） VEX および SWIDtag 形式の SBOM ファイル

本実証で検証するため、VEX と SWIDtag 形式の SBOM ファイルについて、ソフトウェア開発企業が公式に公開しているものがないか調査を実施したが、どちらも発見することはできなかった。したがって、両者に関する調査については、公開されている仕様、またはサンプルとして提供されているファイルの情報を元に、調査・考察を行った。そのため、今後共有・提供される VEX 情報や SWIDtag 形式の

SBOM ファイルとは各種性質が異なる可能性がある。

1.2.10 SBOM 導入の環境整備

本実証で利用した各種環境と、その導入について以下に記す。

（1） ソフトウェア構成解析ツール

セキュリティ製品ソフトの SBOM 作成およびに当たっては、既に社内に導入済みの有償ソフトウェア構成解析ツール（以下、SCA ツール）である有償 SBOM ツール A を利用した。したがって、導入や環境設定、学習に関するコストは今回発生していない。また、有償 SBOM ツール A には SBOM のインポート機能もあったため、SBOM を利用した脆弱性特定においても利用した。

（2） 脆弱性 DB の API 連携

脆弱性 DB の API 連携については、API 問い合わせの結果を解析するために、SIEM 製品 1 を用いた。検証に使用した環境については以下の通りである。

表 1-33 本実証で使用した SIEM 製品 1 検証環境

項目		詳細
SIEM 製品 1 Enterprise	バージョン	9.0.3
	ビルド	dd0128b1f8cd
データ入力	タイプ	ファイルとディレクトリ
	ソースタイプ	json

（3） 無償 SBOM ツール A

中小企業にて、より簡単に SBOM ファイルを利用して脆弱性を管理するために、IPA 提供の無償ツールである無償 SBOM ツール A を用いた検証を実施した。

1.2.11 SBOM の作成

本実証で使用した SBOM およびその入手方法については、以下の通りである。

表 1-34 本実証で使用した SBOM とその入手方法

検証対象	入手可能 SBOM	入手可能ファイル	入手先	実証で利用した

	フォーマット	フォーマット		SBOM
Linux 製品 A 15 SP5	SPDX (2.0)	json	外部サイトから取得[51]	SPDX (2.0) / json
	CycloneDX	json		
セキュリティ製品ソフト	SPDX (2.2/2.3)	json, yaml, tag-value, rdf	社内 SBOM ツールにて作成	SPDX (2.2) / json
	CycloneDX	json		

Linux 製品 A の SBOM ファイルは、いずれも複数のエディションのインストールに使用可能な iso ファイルに対応するものとして一般公開されていた。したがって、エディションにかかわらず Linux 製品 A で使用されるすべてのコンポーネント情報は SBOM に含まれていた。

セキュリティ製品ソフトの SBOM ファイルについては、前述の通り既に社内で導入済みであった有償 SBOM ツール A を利用して、製品のサーバー部分のコンポーネントのみを対象として生成したファイルを利用することとした。Web コンソールから手動で作成可能であり、生成に必要な時間は AWS 上のサーバー上で 1-2 分程度であった。

最終的に、本実証では、どちらの製品についても過去のユーザーへのヒアリングからより対応要望が多かった SPDX(**セキュリティ製品ソフト**の場合は SPDX2.2)の SBOM を対象に実証を行うこととした。

1.2.12 脆弱性管理プロセス

SBOM を活用した脆弱性管理プロセス全体を検討し、整理したものを下図に示す。

[51] https://www.suse.com/download/sles/

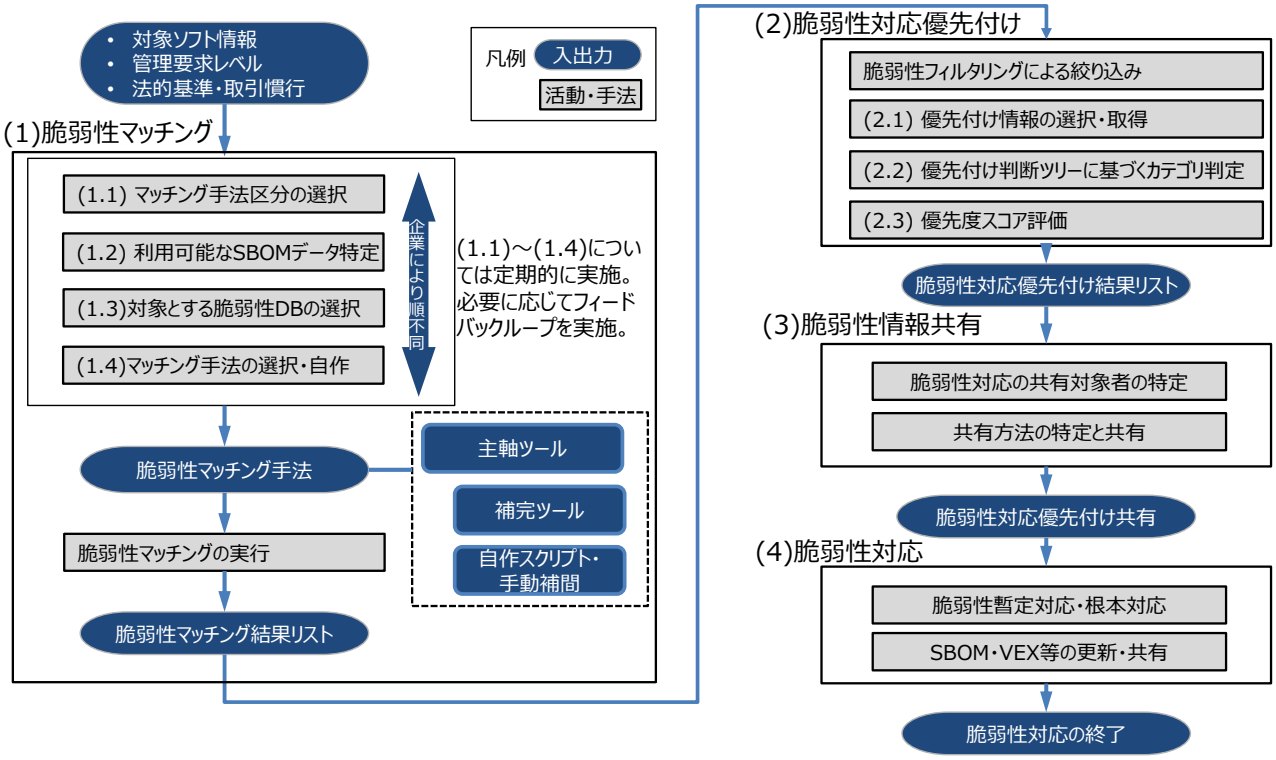


図 1-11 SBOM を活用した脆弱性管理プロセス

以後は、各フェーズでの調査および検証結果詳細について記述する。

(1) 脆弱性特定

1) 脆弱性 DB の比較調査結果

本実証で実施した脆弱性 DB の比較調査を行った。SBOM との突合や脆弱性の調査のためには、確認する DB の数が増えるほど、得られる情報量と、カバーできる脆弱性の数は増える傾向はあるもの、すべての脆弱性 DB について確認することは現実的ではない。対応コスト等も含め、リスク低減やコスト低減の観点から、自社にあった優先度ポリシーを考慮して判断することが望ましいと考えられる。

2) ソフトウェア開発企業・ソフトウェアユーザ企業における脆弱性特定

ソフトウェア開発企業およびソフトウェアユーザ企業における脆弱性特定について、ヒアリングした結果を、以下の表にまとめた。

表 1-35 ソフトウェア開発企業・ソフトウェアユーザ企業へのヒアリング結果(脆弱性特定)

	ソフトウェア開発企業	ソフトウェアユーザ企業

調査の起点	・ OSS 管理ツールからの通知を起点に調査を実施 ・ 外部ニュースや、顧客やセキュリティ研究者からの問い合わせ・指摘から調査が始まるケースもある	・ 基本的には、サプライヤーからのメール、またはインターネットニュースが起点 ・ 有償の脆弱性スキャンサービスの必要性を理解して実施しており、定期的に実施したスキャン結果により特定することもある（ただし脆弱性スキャナーを自社で持っているのは、SOC やセキュリティ対策に投資をしているような大きな企業に限られる） ・ 脆弱性スキャナーを自社で持っていない場合には、外部に依頼して、1 年に一度彼らのサービスでスキャンしてもらうケースはある。スキャンサービスの結果を読み解いて対処方法を判断することが難しいため、対処も含めて依頼していることが多いと想定される
脆弱性情報の参照先	・ SCA ツール ・ （外部からの報告の場合）報告者からの情報および社内での検証結果 ・ 外部ニュースサイトや開発者のアドバイザリなど	・ ベンダーからの報告 ・ 脆弱性スキャナーの検査結果 ・ 外部組織からの情報（CSIRT 協議会など）
課題、その他	・	・ 中小企業の実情としては、「脆弱性」というもの自体を理解できていない場合も多い様子。総務担当者などが掛け持ち、またはたまたま IT に詳しい人材（理系出身、SIer 出身など）がいれば、その社員が担当する形。 ・ 特に中小企業では、SBOM や OSS レベルでの対応をするのはおそらく現実的ではない。システム構成の自動取得、わかりやすい対処方法の表示、一部対処

		の自動化が可能であれば、活用は可能だと想定。費用についての必要性が感じられるかも重要

このヒアリング結果より想定される、一般的なソフトウェア開発企業およびソフトウェアユーザ企業の脆弱性特定の傾向は以下の表の通りである。

表 1-36 想定されるソフトウェア開発企業・ソフトウェアユーザ企業における脆弱性特定の傾向

種別	傾向
ソフトウェア開発企業	・ 製品のリリースやソースコード変更のプロセスにおける脆弱性の確認ポイントや、外部からの報告、セキュリティ組織などによる情報が起点となり脆弱性特定が行われる ・ SCA ツールが導入されている場合には、このツール起点での脆弱性特定の割合が高くなる ・ SCA ツールに加えて、他の脆弱性 DB の情報などを活用している場合もある
ソフトウェアユーザ企業	・ 企業規模や体制で大きく状況が異なる ・ セキュリティ対策に投資をしている企業では、外部からの情報以外に、脆弱性スキャナーなどシステムによる内部での検出も実施している ・ 外部の情報ソースはベンダーからの通知による部分が多いが、ISAC、CSIRT 協議会などの外部組織からの情報提供をきっかけとする場合もある ・ 複数の脆弱性 DB からの定期的な情報取得などは多くの企業では積極的には実施されていない ・ SBOM ファイルをソフトウェア開発企業から受け取り、実際の脆弱性特定に使用している企業はほぼないと想定される ・ 中小企業においては、SBOM ファイルを用いて OSS レベルでの対応をするのは現実的ではない

3）各手法による脆弱性マッチングの結果

各手法によるマッチングの結果概要をまとめた表を以下に示す。

表 1-37 手法別脆弱性マッチング結果概要

(1.1)手法区分	(1.2)利用可能な SBOM データ特定・変換 (1.3)対象とする脆弱性 DB (1.4)マッチング手法の選択・自作	成果・課題	補足
API	(1.2)対象データ:SPDX/json (1.3)対象 DB:脆弱性 DB3，脆弱性 DB2 (1.4)マッチング方法 SIEM 製品 1 を用いて、データ操作や API 連携を実施 SBOM ファイルを読み込ませる SBOM ファイル内の pURL を CPE2.2 または CPE2.3 に変換*1	部品 ID の変換、複数の脆弱性 DB の検査など、API と組合せて柔軟に脆弱性の自動監視可能。SBOM は PURL の採用が多く、脆弱性 DB は CPE の採用が多いため、変換が必要となるケースが多い。PURL 上の部品名と CPE の製品名が一致せず、期待するマッチができない状況も複数確認。Vendor 名に*を入れた CPE の場合、脆弱性 DB1 で検索がマッチせず。 有償 SBOM ツール A 作成の SBOM では pURL がないコンポーネントもあり	pURL から CPE への変換は以下のように実施。OSS*1 の利用(CPE2.3 利用時のみ)1 で変換ができない場合には、pURL の文字列から再構成するコードを作成(python; CPE2.2/2.3)。変換に使えるデータがない場合は*を使用
既成ツール	無償 SBOM ツール A (1.2)対象データ:SWIDtag/xml (1.3)対象 DB:脆弱性 DB3 (1.4)マッチング方法 無償 SBOM ツール A 4.0.0 を利用 説明書をもとに、SWID 形式の SBOM ファイルをサンプルとして作成(CPE を情報として含む)。インポート機能を用いて読み込み	API を用いたコーディングなしにバッチ等による脆弱性監視可能。マッチングができることは確認できたが、以下の理由により、現状中小企業での脆弱性対応に適用することは難しいケースが想定される。無償 SBOM ツール A の入力フォーマットの SWID を提供する例が少ないため、データ変換が求められる。中小企業では IT に詳しくない社員がシステム管理を実施していることが多く、脆弱性という概念の理解そのものが難しい場合もある	－
	有償 SBOM ツール A	読み込んだ SBOM に対して、脆弱性の検出	有償 SBOM ツール A からは、イン

	(1.2)対象データ:SPDX/json (1.3)対象 DB:脆弱性 DB2+KEVC，有償 SBOM ツール A 独自データベース * 有償 SBOM ツール A 側で処理されるため、ユーザー側の作業は不要 (1.4)マッチング方法 SaaS 版 v2023.4.2 を利用。Web コンソール上から SBOM インポート機能を用いて読み込み	が可能であり、手動での脆弱性 DB 連携などは不要だった。同じバージョンの有償 SBOM ツール A で生成された SBOM はインポートできたが、Linux 製品 A の SBOM や、2022 年に有償 SBOM ツール A で生成された SBOM はエラーによりインポートできず	ポートできない SBOM がある問題について認識しており、2023 年 9 月末ごろ修正予定という回答あり。ただし、10/12 現在の時点で、修正は確認できていない(SaaS 版でもバージョンが更新されていない)
Web UI	(1.2)対象データ:SPDX/json (1.3)対象 DB:脆弱性 DB3，脆弱性 DB2 (1.4)マッチング方法 SBOM ファイルよりコンポーネント名(およびバージョン)を抽出し、脆弱性 DB3 および脆弱性 DB2 の脆弱性検索ページにてキーワード検索	試行的に API に近い動作確認、暫定的な脆弱性動向把握が可能。コンポーネント名やバージョン情報との組み合わせなどを用いた検索自体は容易。コンポーネントやマッチしたアドバイザリの数が多いと、手間がかかる。複数 DB を確認する場合に、DB 間の情報差異を確認するのも時間は必要	−

以後はそれぞれの手法での実証に関する詳細である。

a. API 利用による脆弱性特定の自動化

入手した SBOM に含まれるコンポーネント情報と、脆弱性の情報を突合させるためには、製品名・コンポーネント名や、コンポーネントを同定するための部品 ID を何らかの形で用いる必要がある。この目的で利用できると想定される情報は以下の表の通りである。

表 1-38 利用可能と想定される部品 ID(再掲)

部品 ID	開発主体	特徴
Package URL(pURL)	OSS コミュニティ(gitter)	OSS など、パッケージマネージャーを中心にリポジトリに応じて ID が決定される分散割当方式である
Common Platform Enumeration(CPE)	NIST	セキュリティ情報共有標準 SCAP の要素として規定。CVE が割り当てられたソフトウェアが対象となる
Software Identification tag (SWID)	ISO/IEC, NIST	CPE の上位互換で、脆弱性 DB2 において CPE から SWID に移行を宣言しているが、現時点で採用は進んでいない
OmniBOR	OSS コミュニティ (OpenSSF)	アーティファクト(ソースコードファイル、オブジェクトファイル、コンテナイメージなどを含むあらゆるソフトウェアオブジェクト)そのものから ID を生成し、またビルドプロセス中にそのデータをアーティファクトに埋め込むことによって、ID の自動作成と、ユーザー側での検証を可能とする。現状は概念実証中であり、標準仕様もドラフト段階

本実証で利用した SBOM において、抽出可能であった部品 ID は以下の表の通りであった。

表 1-39 実証で利用した SBOM と部品 ID

利用 SBOM	利用可能な部品 ID
Linux 製品 A 15 SP5	pURL
セキュリティ製品ソフト	pURL（一部コンポーネントには存在せず）

Linux 製品 A の SBOM については、すべてのコンポーネントに pURL が存在していた。一方で、**セキュリティ製品ソフト**の SBOM には、対応する pURL が含まれているコンポーネントと、ないものがあった。どちらの SBOM にも、CPE は含まれていなかった。

また、比較のため、Microsoft 社が公開している SBOM ツール[52](以下、MS SBOM ツール)で作成したSBOMについても部品IDを確認した。同ツールで作成されたSBOMについても、他のSBOMと同様 pURL が含まれることを確認した一方で、CPE 情報は含まれていなかった。

一方で、脆弱性 DB2 や脆弱性 DB1 API の利用で利用できる部品 ID は CPE であり、それ以外は製品名などによるキーワード検索となることが判明した。この結果に基づき、API を利用した脆弱性特定の自動化に当たっては、以下の方針で実証を実施することとした。

1. pURL があるコンポーネントについては、pURL を CPE 情報に変換する。具体的な変換方法は以下とする。
   - OSS(purl2cpe)53の利用(API で CPE2.3 が利用できる時のみ)
   - (ア)で変換ができない場合には、pythonで作成したpURLの文字列から再構成するコードによりデータ変換(CPE2.2/2.3)。変換に使えるデータがない場合は該当フィールドにアスターリスクを設定
2. purl がないコンポーネントについては、SBOM 中に含まれるコンポーネント名とバージョン情報を用いて、CPE を生成する

まず初めにそれぞれの SBOM 内の purl について purl2cpe を用いて pURL から CPE への変換を試みたが、SBOM に含まれる pURL は purl2cpe のデータセットとは一致しなかった。次に、python の CPE モジュール及び purl モジュールを用い、SBOM 内の pURL を CPE2.3 に再構成し、脆弱性 DB2 API へ問い合わせを行った。 結果、Linux 製品 A 15 SP5 は該当する脆弱性は検出されなかった。

一方、**セキュリティ製品ソフト**においては、該当する脆弱性が 10 件検出された。API 応答には CVEID に加え、CVEID に対応するクライテリア CPE が複数含まれる。例えば、「cpe:2.3:*:*:gsoap:2.8.117:*」での問い合わせに対して脆弱性マッチングは 0 件であるが、「cpe:2.3:*:*:gsoap:*」での問い合わせに対しては 9 件の脆弱性にマッチングし、112 件のクライテリア CPE を含むデータを応答した。また、応答には脆弱性が該当するバージョン情報の範囲を含むデータが含まれるが、バージョン情報はクライテリア CPE に含まれるケースと「versionStartIncluding」等のパラメータによって出力されるケースが混在した。以下に応答の一部を示す。

表 1-40 CPE「cpe:2.3:*:*:gsoap:*」での脆弱性 DB2 API 問い合わせ 応答抜粋

CVE ID	API 応答に含まれる情報
CVE-2019-7659	{"vulnerable": true, "criteria": "cpe:2.3:a:genivia:gsoap:*:*:*:*:*:*:*:*", "versionStartIncluding": "2.7.0", "versionEndIncluding": "2.7.17", "matchCriteriaId": "6F7E163D-AAFF-45BA-84D8-5BB9EA6DC054"}
	{"vulnerable": true, "criteria":

[52] https://github.com/microsoft/sbom-tool
[53] https://github.com/scanoss/purl2cpe

	”cpe:2.3:a:genivia:gsoap:*:*:*:*:*:*:*:*”, ”versionStartIncluding”: ”2.8.0”, ”versionEndExcluding”: ”2.8.75”, ”matchCriteriaId”: ”8ADB5845-550D-47BF-892B-7BD14F74D2AD”}
	{”vulnerable”: true, ”criteria”: ”cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*”, ”matchCriteriaId”: ”C11E6FB0-C8C0-4527-9AA0-CB9B316F8F43”}
CVE-2019-6973	{”vulnerable”: true, ”criteria”: ”cpe:2.3:a:genivia:gsoap:2.8.0:*:*:*:*:*:*:*”, ”matchCriteriaId”: ”B0D1493E-5DB4-47BF-9687-D8B1F4F9F9C9”}
	{”vulnerable”: false, ”criteria”: ”cpe:2.3:h:sricam:nvs001:-:*:*:*:*:*:*:*”, ”matchCriteriaId”: ”2C2A3DD2-35C1-4DB5-BDCC-C39F4961041C”}
	{”vulnerable”: false, ”criteria”: ”cpe:2.3:h:sricam:sh016:-:*:*:*:*:*:*:*”, ”matchCriteriaId”: ”409B6EF3-1DEB-4548-9CC1-634FCFEF9373”}
	{”vulnerable”: false, ”criteria”: ”cpe:2.3:h:sricam:sh024:-:*:*:*:*:*:*:*”, ”matchCriteriaId”: ”8A7F788B-A89F-48F2-8B3A-060B205C399B”}
	{”vulnerable”: false, ”criteria”: ”cpe:2.3:h:sricam:sh026:-:*:*:*:*:*:*:*”, ”matchCriteriaId”: ”E2EFC9AA-D628-4F3A-AEE5-FF7F4614C895”}
	{”vulnerable”: false, ”criteria”: ”cpe:2.3:h:sricam:sh027:-:*:*:*:*:*:*:*”, ”matchCriteriaId”: ”5B888F17-C358-48EE-A01F-9D9E43BD1A5D”}
	{”vulnerable”: false, ”criteria”: ”cpe:2.3:h:sricam:sp007:-:*:*:*:*:*:*:*”, ”matchCriteriaId”: ”19DE107A-8C7C-46B5-9ECC-8D3CF4C4765E”}
	{”vulnerable”: false, ”criteria”: ”cpe:2.3:h:sricam:sp008:-:*:*:*:*:*:*:*”, ”matchCriteriaId”: ”78272233-1B9B-4057-92E6-4B52377BB681”}
	{”vulnerable”: false, ”criteria”: ”cpe:2.3:h:sricam:sp009:-:*:*:*:*:*:*:*”, ”matchCriteriaId”: ”0D0943E2-82E8-4438-96DD-F107C5BCC7E8”}
	{”vulnerable”: false, ”criteria”: ”cpe:2.3:h:sricam:sp012:-:*:*:*:*:*:*:*”, ”matchCriteriaId”:

	”8D4045D2-04E9-44EC-95A4-647F88A9D87E”}
	{”vulnerable”: false, ”criteria”: ”cpe:2.3:h:sricam:sp015:-:*:*:*:*:*:*:*”, ”matchCriteriaId”: ”8691CACB-052B-43EC-84AA-8D2869BE96B2”}
	{”vulnerable”: false, ”criteria”: ”cpe:2.3:h:sricam:sp017:-:*:*:*:*:*:*:*”, ”matchCriteriaId”: ”363ADBFA-B83B-4B24-A2B0-4C49570DB350”}
	{”vulnerable”: false, ”criteria”: ”cpe:2.3:h:sricam:sp018:-:*:*:*:*:*:*:*”, ”matchCriteriaId”: ”A53AF4CC-21EB-4E61-82FC-9A344DC2AEF5”}
	{”vulnerable”: false, ”criteria”: ”cpe:2.3:h:sricam:sp019:-:*:*:*:*:*:*:*”, ”matchCriteriaId”: ”494FBEB6-617E-44E6-A544-F67EC8280A86”}
	{”vulnerable”: false, ”criteria”: ”cpe:2.3:h:sricam:sp020:-:*:*:*:*:*:*:*”, ”matchCriteriaId”: ”400F51BF-EB0C-4AC8-AEC5-6F311562C7EB”}
	{”vulnerable”: false, ”criteria”: ”cpe:2.3:h:sricam:sp023:-:*:*:*:*:*:*:*”, ”matchCriteriaId”: ”109D9827-0C1A-44AB-B1D2-F9512E93A5A6”}

例で示した「cpe:2.3:*:*:gsoap:*」のように、バージョン情報をワイルドカード指定して問い合わせ、API 応答内の情報を元にフィルタリングを行い該当する脆弱性を検出することで脆弱性マッチングのカバレッジを向上させる方法が考えられるが、現時点では上表のように API の応答構造が一定でなく、脆弱性マッチングの効率向上やカバレッジの向上に繋がるという結果には至らなかった。

脆弱性 DB1 API への API 問い合わせにおいては、問い合わせに対応する CPE の形式がバージョン 2.2 で使用されている「URI 形式」であり、今回使用した python モジュールでは直接的に変換する実装がなされていない。そのため、SBOM 内の purl から文字列を抽出して URI 形式の purl を再構成し API 問い合わせを試みた。今回使用した SBOM の部品 ID には「vendor」に該当する情報が含まれていないため、該当するフィールドにはワイルドカード指定して問い合わせを行った。だが、脆弱性 DB1 API に対する問い合わせにおいて、vendor フィールドをワイルドカード指定して問い合わせた場合、product フィールドを指定していても該当する脆弱性はないという応答になり、脆弱性を検出できなかった。したがって、脆弱性 DB1 API を利用した脆弱性特定の自動化という点においては、ベンダー名のワイルドカード指定を許容するなど、API の仕様の変更が必要であると考える。

b. 無償 SBOM ツール A を利用した脆弱性特定

まず、無償 SBOM ツール A で設定した自社製品の脆弱性情報を収集し脆弱性を特定する手法について検討を行った。まず、脆弱性 DB3 に登録されている情報について、UI 上で確認することはできたが、脆弱性 DB3 に登録されている情報によっては、影響のある製品のバージョンや詳細をベンダーの

サイトでさらに確認が必要な場合があり、無償 SBOM ツール A によって提供される情報だけでは特定を完結することが難しいものもあった。

次に、無償 SBOM ツール A の機能として提供されている SBOM のインポート・エクスポート機能を利用した脆弱性の特定について検討した。本実証で用いた SBOM ファイルは SPDX 形式であったが、無償 SBOM ツール A が現時点で対応しているファイルフォーマットが SWID 形式（ファイルの拡張子が.swid のもの）に変換可能な簡易ツールを発見できなかったため、NTIA の資料に記載されているバイナリサンプル（Time 1.9 for Red Hat distribution）[54] を利用してインポートの確認を試みた。

このファイルのインポート時にフォーマットエラーのダイアログが表示されたため、該当箇所を修正し再度インポートを行った。エラーのダイアログは解消されインポートは行えたが、UI 上の収集対象の製品一覧には情報が表示されなかった。無償 SBOM ツール A のパッケージに同梱されている利用者向けマニュアルにも記載されているが、インポート機能の仕様として、CPE バージョン 2.2 または 2.3 のフォーマットを利用して製品情報をインポートしており、サンプルで使用した SBOM ファイルは CPE フォーマットを使用していないものであったことが原因であった。無償 SBOM ツール A 以外のツールでエクスポートしたファイルをインポートすることを想定する場合は、エクスポートするツールの出力ファイルを確認し、手動で CPE の情報を SBOM ファイルに追記するなどの運用について検討する必要があると考える。

c. 有償 SCA ツールを利用した脆弱性特定

A 社内で導入されている有償 SBOM ツール A は、2023 年 9 月時点で提供されていた最新バージョンにて、SBOM ファイルをインポートする機能が備わっていた。この機能を用いて、外部から提供された SBOM を読み込み、脆弱性を特定する手法について検討を行った。

まず、有償 SBOM ツール A の Web コンソールより、Linux 製品 A の SBOM ファイルをインポートしようと試みたが、SPDX，CycloneDX のどちらのデータフォーマットを用いた場合もエラーによりインポートすることができなかった。また、2022 年に当時のバージョンの有償 SBOM ツール A で作成した SPDX 形式の SBOM ファイルや、Microsoft SBOM ツールで作成した SBOM ファイルもエラーでインポートすることができなかった。インポートできたのは、2023 年 9 月時点で最新の有償 SBOM ツール A で作成された SBOM ファイルのみであった。この問題について、有償 SBOM ツール A のサポート担当に問い合わせたところ、「問題を把握しており、今後対応予定」である旨の回答を得たが、2023 年 10 月末時点で、問題は解消されていない。

なお、正しく SBOM ファイルがインポートされた場合には、ソースコードを自動検出したときと同様に、有償 SBOM ツール A の Web コンソール上で脆弱性の管理が可能であった。新たな脆弱性情報に対する通知機能等も、ソースコードの自動検出時と同様に利用可能であると想定され、効率よく対応が可能であることが分かった。

また、有償 SBOM ツール A では、脆弱性 DB2 DB の情報の他、KEVC に由来すると想定される悪用事例についての情報や、ツールベンダー独自の脆弱性情報が確認できるようになっていた。

[54] https://drive.google.com/drive/folders/1Z364N234jrs36pjDT8xcS5hUGjRmMTN9

（2） 脆弱性評価・優先付け

1） 脆弱性 DB から得られる情報

各脆弱性 DB から取得可能な、脆弱性評価に活用できる情報については、別紙「脆弱性 DB 比較」に記載した。

2） ソフトウェア開発企業・ユーザー企業における脆弱性評価・優先付け

ソフトウェア開発企業・ユーザー企業の脆弱性評価・優先付けに関するヒアリング内容を以下の表にまとめた。

表 1-41 ソフトウェア開発企業・ユーザー企業へのヒアリング結果（脆弱性評価・優先付け）

	ソフトウェア開発企業	ユーザー企業
優先付けの際の判断材料	・ ゼロデイ脆弱性（実際の攻撃での利用、またはリサーチャーなどによる脆弱性公開が修正前に行われる事象が発生しているか）が最初の判断基準 ・ CVSS スコア ・ 脆弱性の製品そのものに対する影響度合い（セキュリティ上重要な機能が無効化されるなど） ・ 顧客からの問い合わせが多いなどのビジネス面からの影響により、優先度が上がることもある	・ 社外に面するシステムかどうかは重要な判断材料 ・ CVSS スコア（Critical/High は対応必須と設定している） ・ 脆弱性の実影響があるかどうか（実際にその攻撃が会社の環境で使えるものかどうか） ・ サーバーなどシステムに影響がある部分か、それともデスクトップ OS のように影響が少ないか は判断に影響する ・ デスクトップ OS が対象の場合は、事前検証作業は情報システム部内に先に修正パッチを適用して様子を見る程度にとどめ、対応速度を優先する ・ ネットワーク機器などで、バージョンアップモジュールの一部として脆弱性修正が含まれるときは適用するか慎重に判断する。Critical Patch のようにセキュリティ修正または重要な修正だと名前からしてわかるものはあてやすい
脆弱性情報の参照先	・ OSS 管理ツール	・ ベンダーからの報告 ・ 脆弱性スキャナーの検査結果

	・ （外部からの報告の場合）報告者からの情報および社内での検証結果 ・ 外部ニュースサイトや開発者のアドバイザリなど	・ 外部組織からの情報（CSIRT 協議会など）
課題、その他	・ 製品が使用される環境はユーザーに依存するため、ユーザー環境での影響度を推測するのは困難	・ KEVC のチェックは現状していない。毎度見に行くほどのリソースはないことが理由 ・ 中小企業では無償 SBOM ツール A で出てくるような脆弱性情報などは理解できない場合がほとんど。 ・ 外部システム（VPN 機器など）がある場合も多くない。 ・ あれば外部システム、または実際インシデント事例がある脆弱性のみ対応するところから始めるのが現実的か？

情報の参照先や判定方法には違いはあるものの、優先付けの判断に影響する要因にはソフトウェア開発企業とソフトウェアユーザ企業の間で共通項が多く見られた。これらから想定される優先付けにおいて利用される要因は以下の通りであった。

- 実際の悪用事例の有無など実際に攻撃として利用される可能性
- CVSS のスコア
- 対象製品・システムの自社におけるビジネスでの重要度

なお、ソフトウェア開発企業において、外部サプライヤーから提供されたコンポーネント、またはソースコードに関する脆弱性が発見された場合には、OSS と同様、まずサプライヤー側から、該当脆弱性の評価情報を取得したうえで、自社製品に対する影響を評価することになると考えられる。ただし、バイナリではなく、ソースコードとして納品されている場合や、ソースコードの著作権が最終ベンダーに移管されているなど契約上ソースコード保守の責任が最終ベンダーにあるケースでは、サプライヤー提供の部品部分も含め、最終ベンダーですべて対応する必要がある可能性がある。

3）脆弱性評価シートの作成と適用結果

ヒアリングを通じて確認できた優先付け判断に利用する情報は、CISA SSVC[55]において判断ツリーの構成要素に利用される情報と共通項が見られた。一方で、CISA SSVC の活用については、一部判

[55] https://www.cisa.gov/sites/default/files/publications/cisa-ssvc-guide%20508c.pdf

断にあたりセキュリティや脆弱性に関する深い経験や知識が必要と想定される部分も存在していた。特に中小のユーザー企業などでは判断が困難と想定される。そのため、今回は CISA SSVC の判断ツリーの考え方をベースに、ソフトウェア開発企業・ユーザー企業の区分、およびセキュリティに関する知識や体制のレベル(上位・下位)の計 4 カテゴリごとに、判断ツリーの分岐点での判断についてまとめた、脆弱性評価シートを作成した(評価シート全体については、別紙「脆弱性対応優先付けシート」参照)。

今回作成した脆弱性優先付けの判断ツリーは以下の通りである。

表 1-42 脆弱性優先付け判断ツリー

悪用可能性	悪用効率性	技術的深刻度	ユーザー影響度	対応優先度
高	高	高	高	即対応
			中	即対応
			低	優先
		低	高	即対応
			中	優先
			低	優先
	低	高	高	即対応
			中	優先
			低	保留
		低	高	優先
			中	保留
			低	保留
中	高	高	高	優先
			中	通常保守
			低	保留
		低	高	優先
			中	保留
			低	保留
	低	高	高	優先
			中	通常保守
			低	保留
		低	高	通常保守
			中	保留
			低	保留
低	高	高	高	優先
			中	保留
			低	保留
		低	高	通常保守

			中	保留
			低	保留
	低	高	高	通常保守
			中	保留
			低	保留
		低	高	保留
			中	保留
			低	保留

また、判断ツリーでの最終的な判断結果区分と、その対応内容は以下の通りである。この表においては、[ユーザー企業、ソフトウェア企業]×[上位 vs 下位]のすべての企業類型において、「基本的な対応内容」に記載の対応が期待されるが、企業類型によっては、すぐにこのような対応が難しい場合があることが予想されるため、「企業類型による考え方・ステップアップの考え方」に示す企業については、次善策として、「基本的な対応内容」に記載の対応を緩和し、「企業類型による考え方・ステップアップの考え方」に示す対応をとることが期待される。なお、「企業類型による考え方・ステップアップの考え方」に記載しない企業類型については、原則「基本的な対応内容」とすることが望まれる。

表 1-43 区分ごとの対応内容

区分	基本的な対応内容	企業類型による考え方・ステップアップの考え方 [ユーザー企業、ソフトウェア企業]×[上位 vs 下位]
即対応 (immediate)	全てのリソースを集中し、 必要に応じて組織の通常業務を停止して可能な限り迅速に応を行う	ユーザー企業(下位):最低限この部分については対応する。 ソフトウェア企業:根本的な問題の修正ができない場合、また多くの時間がかかると予測される場合には、何らかの回避策を先に提供することが望ましい(ソフトウェアの使用中止を含む)
通常保守より優先 (out-of-cycle)	通常よりも迅速に行動し、計画外の次の利用可能な機会に、必要に応じて通常業務時間外を含めて緩和策または修復策を実施する	ユーザー企業(下位):可能な限り対応することが望ましい
通常保守(scheduled)	定期メンテナンス時に対応する	ソフトウェア企業(上位)/ユーザー企業(上位):このカテゴリに入った脆弱性の評価に影響がないかを確認する。インシデント報告など、影響度が変わるような情報が入った場合には、優先度を再評価する。 ソフトウェア企業(下位):該当脆弱性に対するインシデントの情報がないか定期的に確認し、発見された場合には再評価して対応することが望ましい
対応保留 (defer)	現時点では対応しない。状況を注視する	ソフトウェア企業(上位)/ユーザー企業(上位):このカテゴリに入った脆弱性の評価に影響がないかを確認する。インシデント報告など、影響度が変わるような情報が入った場合には、優先度を再評価する。 ソフトウェア企業(下位)/ユーザー企業(下位):該当脆弱性に対するインシデントの情報がないか定期的(1ヶ月に一度など)に確認し、発見された場合には再評価して対応することが望ましい

企業カテゴリごとの優先付けの判断方法は下表に記載した。

表 1-44 企業カテゴリごとの優先付け判断方法

		ソフトウェア開発企業		ソフトウェアユーザ企業	
判断ノード		技術力が高い	技術力が低い	技術力が高い	技術力が低い
悪用可能性(Exploitation)	高	下記のいずれか一つ以上を満たす場合。 ・[インシデント(実攻撃)の有無]自社製品に対して、この脆弱性をついた実際の攻撃事例を把握しているが、まだ修正パッチが準備できていない場合(ハニーポッドに対する攻撃含む。社内での発見、社外からの脆弱性やインシデントの報告含む) ・[インシデント(実攻撃)の有無]製品に含まれる OSS やサプライヤー提供のコンポーネントに対して該当脆弱性をついた実際の攻撃が報告されている(インシデントあり) ・[ゼロデイ脆弱性]自社製品の修正パッチや回避策が準備されていないにもかかわらず、セキュリティ研究者などにより該当製品の脆弱性が公開されてしまった場合(ゼロデイ	下記のいずれか一つ以上を満たす場合。 ・[インシデント(実攻撃)の有無]自社製品に対して、この脆弱性をついた実際の攻撃事例を把握しているが、まだ修正パッチが準備できていない場合(社内での発見、社外からの脆弱性やインシデントの報告含む) ・[インシデント(実攻撃)の有無]製品に含まれる OSS やサプライヤー提供のコンポーネントに対して該当脆弱性をついた実際の攻撃が報告されている(インシデントあり) ・[ゼロデイ脆弱性]自社製品の修正パッチや回避策が準備されていないにもかかわらず、セキュリティ研究者などにより該当製品の脆弱性が公開されてしまった場合(ゼロデイ脆弱性となる場合)	下記のいずれか一つ以上を満たす場合。 ・[インシデント(実攻撃)の有無]製品または製品に含まれる OSS(SBOM から判断)に対して脆弱性をついた実際の攻撃事例が報告されている場合 ・[インシデント(実攻撃)の有無]製品ベンダーから、悪用される可能性が高いと報告されている場合 ・[PoC コード公開(実攻撃なし)の有無][OSS 浸透度]攻撃事例は報告されていないものの、該当製品・コンポーネントが広く使用されていて、PoC コードが存在している(攻撃者が悪用する可能性が高い場合) ・[インシデント(実攻撃)の有無]自社の持つシステムへの攻撃の可能性について、社内外から報告されている	下記のいずれか一つ以上を満たす場合。 ・[インシデント(実攻撃)の有無]JPCERT/CC やニュース、ベンダーからの通知で、実際に悪用事例があることが公表されている ・[脆弱性解説] ベンダーが修正の早期適用を推奨している ・[インシデント(実攻撃)の有無]自社の持つシステムへの攻撃の可能性について、社内外から報告されている

		脆弱性となる場合） ・**[PoC コード公開（実攻撃なし）の有無]**[**OSS 浸透度**]攻撃事例は報告されていないものの、該当コンポーネントが広く使用されていて、PoC コードが存在している（攻撃者が悪用する可能性が高い場合）	・**[OSS 浸透度]**該当のコンポーネントが広く使用されている		
	中	・**[PoC コード公開（実攻撃なし）の有無]**製品に含まれる OSS やサプライヤー提供のコンポーネントの脆弱性に対して、PoC コード（Exploit コード）が存在している場合（ただし、実際の攻撃への使用は確認されていない。また PoC はあるが社内で発見された脆弱性であり、社外公開されていないことが確認されている場合は除く）	・**[PoC コード公開（実攻撃なし）の有無]**製品に含まれる OSS やサプライヤー提供のコンポーネントの脆弱性に対して、PoC コード（Exploit コード）が存在している場合（ただし、実際の攻撃への使用は確認されていない。また PoC はあるが社内で発見された脆弱性であり、社外公開されていないことが確認されている場合は除く）	・**[PoC コード公開（実攻撃なし）の有無]**脆弱性をついた実際の攻撃事例は報告されていないが、PoC コードが存在している場合	上記以外
	低	下記のいずれか一つ以上を満たす場合。 ・**[インシデント（実攻撃）の有無]**[**PoC コード公開（実攻撃なし）の有無]**自該当脆弱性に対して、攻撃事例・PoC コー	下記のいずれか一つ以上を満たす場合。 ・**[インシデント（実攻撃）の有無]**[**PoC コード公開（実攻撃なし）の有無**]該当脆弱性に対して、攻撃事例・PoC コー	・**[インシデント（実攻撃）の有無]**[**PoC コード公開（実攻撃なし）の有無]**該当脆弱性に対して、攻撃事例・PoC コードが発見されていない場合	

		ドともに存在していない場合 ・**[インシデント(実攻撃)の有無]**[PoC コード公開(実攻撃なし)の有無]自自社内で発見された脆弱性で、外部で攻撃に使用された事例が確認されていない場合	ドともに存在していない場合 ・**[インシデント(実攻撃)の有無]**[PoC コード公開(実攻撃なし)の有無]自社内で発見された脆弱性で、外部で攻撃に使用された事例が確認されていない場合		
悪用効率性	**高**	下記のいずれか一つ以上を満たす場合。 ・**[該当システムの設置場所]** 該当脆弱性が、インターネット上からアクセスできる位置にあるシステム内に存在する 例:公開 WEB サーバー、社外ネットワークと社内ネットワークの接点となるシステムに存在する機器(VPN、FW 等) ・**[脆弱性解説]** RCE/コマンドインジェクションの脆弱性である	下記のいずれか一つ以上を満たす場合。 ・**[該当システムの設置場所]** 該当脆弱性が、インターネット上からアクセスできる位置にあるシステム内に存在する 例:公開 WEB サーバー、社外ネットワークと社内ネットワークの接点となるシステムに存在する機器(VPN、FW 等) ・**[脆弱性解説]** RCE/コマンドインジェクションの脆弱性である	・**[該当システムの設置場所]**該当脆弱性が、インターネット上からアクセスできる位置にあるシステム内に存在する 例:公開 WEB サーバー、社外ネットワークと社内ネットワークの接点となるシステムに存在する機器(VPN、FW 等)	・**[該当システムの設置場所]**該当脆弱性が、インターネット上からアクセスできる位置にあるシステム内に存在する 例:公開 WEB サーバー、社外ネットワークと社内ネットワークの接点となるシステムに存在する機器(VPN、FW 等)
	低	上記以外	上記以外	上記以外	上記以外

技術的深刻度	**高**	下記のいずれか一つ以上を満たす場合。 ・**[システムのセキュリティ機能への影響]** この脆弱性を用いることで、攻撃者が対象製品を備えるシステムのセキュリティ機能（ユーザー認証やロール設定によるアクセス制限、改ざん防止機能など）を無効、または回避することが可能となる ・**[脆弱性解説]**この脆弱性を用いることで、攻撃者が対象製品に含まれる情報を入手することが可能となる ・**[CVSS スコア]**（上記の判定が困難な場合のみ）CVSS スコアが Critical または High	下記以外（影響度を自社で判断することができない場合を含む）	下記のいずれか一つ以上を満たす場合。 ・**[システムのセキュリティ機能への影響]**この脆弱性を用いることで、攻撃者が対象製品を備えるシステムのセキュリティ機能（ユーザー認証やロール設定によるアクセス制限、改ざん防止機能など）を無効、または回避することが可能な場合 ・**[脆弱性解説]**この脆弱性を用いることで、攻撃者が対象製品上の情報を入手することが可能な場合 上記の判定が困難な場合は、以下の条件を満たす場合。 ・**[CVSS スコア]**製品開発企業（最終ベンダー）による CVSS スコアが Critical または High（最終ベンダーからの情報がない場合、該当脆弱性を含む OSS に関する CVSS スコアが Critical または High）	（この項目は判定せず、すべて高として扱う）
	低	上記以外	・**[CVSS スコア]**影響のある OSS の CVSS スコアが	上記以外	

			Middle または Low		
ユーザー影響度	**高**	下記のいずれか一つ以上を満たす場合。 ・**[対象システムの性質]**対象製品が、社外ネットワークと社外ネットワークの接点となるシステムである（VPN 機器、FW など） ・**[対象システムの性質]**対象製品が、医療機器のクラス II/III/IV にあたる ・**[対象システムの性質]**脆弱性の影響を受ける自社のコンポーネントは、自社内または他社の最終製品開発チームに利用され、最終製品に組み込まれるものである（ライブラリやフレームワークなど） ・**[問い合わせ数]**（自社 PSIRT やサポート部門などから情報が得られる場合のみ）自社の多数の製品・サービスに影響する、または多数の問い合わせを既に受けている ・「影響度中」の条件に当てはまらない	下記のいずれか一つ以上を満たす場合。 ・**[対象システムの性質]**対象製品が、社外ネットワークと社外ネットワークの接点となるシステムである（VPN 機器、FW など） ・**[対象システムの性質]**対象製品が、医療機器のクラス II/III/IV にあたる ・**[対象システムの性質]**脆弱性の影響を受ける自社のコンポーネントは、自社内または他社の最終製品開発チームに利用され、最終製品に組み込まれるものである（ライブラリやフレームワークなど） ・**[問い合わせ数]**（自社 PSIRT やサポート部門などから情報が得られる場合のみ）自社の多数の製品・サービスに影響する、または多数の問い合わせを既に受けている ・「影響度中」の条件に当ては	下記のいずれか一つ以上を満たす場合。 ・**[対象システムの性質]**該当脆弱性が、漏洩することで会社や社員に致命的な影響を与える情報を扱う製品に存在する（機密度がきわめて高い情報など） ・**[対象システムの性質]**該当脆弱性を持つシステムの停止が自社ビジネスに甚大な影響を及ぼす（8 割以上の社員の業務が止まるなど） ・**[対象システムの性質]**該当脆弱性が社外ネットワークと社内ネットワークの接点となるシステムに存在する（VPN 機器、FW など） ・**[対象システムの性質]**該当システムの故障や不具合が、人間の精神的・身体的健康、環境に致命的な影響を及ぼす可能性がある	下記のいずれか一つ以上を満たす場合。 ・**[対象システムの性質]**該当脆弱性が、漏洩することで会社や社員に致命的な影響を与える情報を扱う製品に存在する（機密度がきわめて高い情報など） ・**[対象システムの性質]**該当脆弱性を持つシステムの停止が自社ビジネスに甚大な影響を及ぼす（8 割以上の社員の業務が止まるなど） ・**[対象システムの性質]**該当脆弱性が社外ネットワークと社内ネットワークの接点となるシステムに存在する（VPN 機器、FW など） ・**[対象システムの性質]**該当システムの故障や不具合が、人間の精神的・身体的健康、環境に致命的な影響を及ぼす可能性がある

			まらない		
	中	・[対象システムの性質]対象製品(自社がサプライヤーとしてコンポーネントを最終製品開発ベンダーに提供している場合を除く)は、個人情報などユーザーから取得したデータや、ユーザーが入力するデータ(センサーからの情報含む)を保存・保管や、データ転送することはないと確定している	・[対象システムの性質]対象製品(自社がサプライヤーとしてコンポーネントを最終製品開発ベンダーに提供している場合を除く)は、個人情報などユーザーから取得したデータや、ユーザーが入力するデータ(センサーからの情報含む)を保存・保管や、データ転送することはないと確定している	下記のいずれか一つを満たす場合。 ・[対象システムの性質]該当脆弱性が、自社の機密情報を扱う製品に存在する ・[対象システムの性質]該当脆弱性を持つシステムの停止が自社ビジネスに無視できない影響を及ぼす(特定部署の業務が止まる、半数以上の社員の業務が止まるなど) ・[対象システムの性質]該当システムの故障や不具合が、人間の精神的・身体的健康、環境に無視できない影響を及ぼす可能性がある(または、その可能性を否定できない)	下記のいずれか一つを満たす場合。 ・[対象システムの性質]該当脆弱性が、自社の機密情報を扱う製品に存在する ・[対象システムの性質]該当脆弱性を持つシステムの停止が自社ビジネスに無視できない影響を及ぼす(特定部署の業務が止まる、半数以上の社員の業務が止まるなど) ・[対象システムの性質]該当システムの故障や不具合が、人間の精神的・身体的健康、環境に無視できない影響を及ぼす可能性がある(または、その可能性を否定できない)
	低	(上の二つから選ぶこと)	(上の二つから選ぶこと)	・[対象システムの性質]該当脆弱性を持つシステムが停止しても、自社ビジネスに軽微な影響しかない(または影響はない)	・[対象システムの性質]該当脆弱性を持つシステムが停止しても、軽微な影響しかない(または影響はない)

開発企業・ユーザー企業ともに、「**技術力が低い**」は「**技術力が高い**」の判断基準のサブセットとしている。また立場や状況により判断が難しいと考えられる判断ノードについては、一部カテゴリで選択肢の数を減らし、単純化を図っている。例えば、多くの中小企業に代表される下位のソフトウェアユーザ企業では、技術レベルにより脆弱性の技術的深刻度の判断が困難だと想定し、「技術的深刻度」はすべて「高」として扱うこととしている。また、ソフトウェア開発企業において、ユーザーが自社開発のシステムをどのような目的・環境で利用しているか、全パターンを把握することから「ユーザー影響度」については、を判断することが難しいという意見があったことから、ソフトウェア企業における「ユーザー影響度」の項目を簡素化するとともに、選択肢を減らした。

なお、上記の選択肢を減らすにあたっては、いずれもリスクを低く見積もることによる悪影響を低減するために、より優先度が低くなる選択肢を取り除いて安全に倒す方針とした。その結果、優先度が高く、対応の必要性が高い脆弱性の数が多くなる可能性はある。この点を懸念される企業の場合には、安全に倒さないことにより危険な脆弱性が見逃される可能性が増えるリスクを理解した上で、本実証での方針とは異なり、優先度が低くなる選択肢を残し、他選択肢の削除を検討するというのも一つのやり方ではあると考えられる。

4）優先付けに必要な情報の取得と効率化について

判断ツリーを用いて優先付けをする場合には、その情報の取得元の整理が重要となる。また、優先付けそのものにかかる時間の効率化や、優先付けした結果、一部のカテゴリに多くの脆弱性が集まってしまった場合の対応についても検討しておく必要がある。

この目的のため、まず、優先付けとその前後のプロセスで活用できる情報とその入手方法について下表にまとめた。上表「企業カテゴリごとの優先付け判断方法」において、太字で表記されている部分は、下表の「確認内容」欄と対応している。

表 1-45 各種評価情報と利用フェーズ

評価カテゴリ			サブカテゴリ	確認内容	説明	情報源		利用フェーズ		
						ソフトウェア企業	ユーザー企業	フィルタリング	優先付け	暫定対応・根本対応
リスク	事故発生確率	外部要因	悪用可能性	インシデント(実攻撃)の有無	実際に悪用・事件が発生している、または悪用される可能性が極めて高く、緊急性が高い。または、悪用事例はなくても、広く使われている OSS の脆弱性で PoC があるなど、攻撃者が悪用に転用する可能性がきわめて高いと考えられる場合	NVD(KEVC)/JVNiPedia/ExploitDB 対象製品・コンポーネントの開発ベンダー/サプライヤー その他信頼のおけるセキュリティ企業・組織からの報告(各種 SAC, CISRT 協議会など含む) 社内 自社運用のバグバウンティプログラム、または脆弱性やインシデント報告窓口への連絡	NVD(KEVC) JPCERT/CC 対象製品・コンポーネントの開発ベンダー その他信頼のおけるセキュリティ企業・組織からの報告(各種 SAC, CISRT 協議会など含む) 社内外からの報告		☆	
				PoC コード公開(実攻撃なし)の有無	悪用コードが存在しており、悪用される可能性が高い				☆	
				ゼロデイ脆弱性	(ソフトウェア企業のみ)自社作成部分のコードにある脆弱性について、対応策が準備でき	自社運用のバグバウンティプログラム、または脆弱性やインシデント報告窓口への連絡			☆	

					る前に、セキュリティ研究者などに外部公開されてしまった場合。準備ができるまでに悪用の手法などが明らかにされる可能性が高い					
			悪用有用性	**OSS 浸透度**	攻撃者から見た脆弱性の有用性。広く利用されている OSS の脆弱性の場合、攻撃者としては利用可能な場所が広くなるため、悪用される可能性が高い	・SCA ツールからの情報 ・ニュースサイトや開発者コミュニティなどからの情報	・ニュースサイトなどからの情報		☆	
			悪用容易性	**該当システムの設置場所**	攻撃者から見た悪用時の展開のしやすさ。上からアクセスできるシステムである場合、そうでないものに比べ、攻撃者がアクセスしやすい	・製品・機能情報 ・ユーザー企業のユースケース ・NVD/JVNiPedia	・システム構成情報		☆	
		脆弱性残留確率（内部要因）	**開発者による脆弱性評価（VEX）**	**VEX 脆弱性ステータス（影響：有・無・不明）**	開発者が判定した VEX ベースでの脆弱性の評価。脆弱性に係る部品を利用した開発者が直接評価したものであり精度が高い。優	・開発者提供の VEX	・開発者提供の VEX	☆		☆

					先付けを実施する前のフィルタとして用いる					
			脆弱性評価(VEX 以外)	**VEX 以外による脆弱性ステータス(影響:有・なしなど)**	開発者または、開発者以外の第三者による脆弱性の評価(VEX 以外)。VEX が取得できない場合、開発者または開発者以外の第三者が VEX 以外の手法で表記した脆弱性評価内容を確認する。特に開発者以外の評価の場合、部品開発主体の作成を前提とする VEX とは異なり、精度が低い可能性が存在する	・該当脆弱性に関するサプライヤーまたはセキュリティ機関などからのアドバイザリ	・該当脆弱性に関する最終製品ベンダーまたはセキュリティ機関などからのアドバイザリ	☆		☆
			脆弱性影響緩和策	**アドバイザリ対処策適用可否(可・否・不明)**	製品やコンポーネントの更新以外に適用可能な、脆弱性の影響緩和策の内容。脆弱性に対する一般的な対処策であり、部品 ID・脆弱性 ID が完全に一致する場合以外は、悪用可能性の精度は高くな	・JVNiPedia/NVD ・該当脆弱性に関するサプライヤーまたはセキュリティ機関などからのアドバイザリ	・JVNiPedia/NVD ・該当脆弱性に関する最終製品ベンダーまたはセキュリティ機関などからのアドバイザリ			☆

				い。優先付け後に対策を検討する場合に利用					
	影響度	**技術的深刻度**	**システムのセキュリティ機能への影響**	システムがもつセキュリティ機能に影響が出ることで、本来の防御機能が働かなくなるなど、被害範囲が拡大する可能性がある	・JVNiPedia/NVD ・該当脆弱性に関するサプライヤーからのアドバイザリ ・システムの仕様	・JVNiPedia/NVD ・該当脆弱性に関する最終製品ベンダーからのアドバイザリ		☆	
			CVSS スコア	OSS 開発者または信頼あるセキュリティ機関による評価により、脆弱性のそのものの深刻度を理解するための情報とする				☆	
			脆弱性解説	アドバイザリに含まれる、CVSS や VEX などでは表現されていない、脆弱性や修正適用に科する詳細情報。RCE/コマンドインジェクションの脆弱性など、脆弱性の種類なども含まれる。最終製品ベンダーや信頼のおけるセ	・最終製品ベンダーのアドバイザリ ・JVNiPedia/NVD ・SCA ツール上のアドバイザリ	・最終製品ベンダーのアドバイザリ ・JVNiPedia/NVD		☆	

				キュリティ機関による情報は、脆弱性に関する影響を判断するのに有用な情報である可能性が高い					
		ユーザー影響度	問い合わせ数	（ソフトウェア企業のみ）既に脆弱性情報が公開されており、製品への影響に関する問い合わせを受けている場合や、自社で扱う複数の製品に影響がある場合には、ユーザーや社内関係者への影響度が高いと考えられる	・社内への問い合わせ情報 ・自社製品全体に対する影響情報（PSIRT などから取得）			☆	
			対象システムの性質	ユーザーのビジネスや情報資産に対する影響度に関連する。ユーザーの情報資産（CIA）に特化した評価であり実態に基づく評価であり精度が高いと想定される。外部提供サービスは、社内システムより影響度が高い	・システム仕様やユースケースに関する情報 ・ユーザー問い合わせ数	・システム構成情報 ・システム使用用途詳細		☆	

			（CIA 各要素 2,1,0 の合計値など）					
修正コスト	**対応方針**	**サービス中断・縮退**	根本対応が何らかの理由でできない場合の手段となる可能性がある	・システム仕様と脆弱性に関する情報 ・現状のシステム配置と利用用途	・システム仕様と脆弱性に関する情報 ・現状のシステム配置と利用用途			☆
		自社作成コード修正による影響軽減	（ソフトウェア企業のみ）OSS やサプライヤーが修正を提供しない場合、または修正版を何らかの理由で適用できない場合に、製品の修正により脆弱性の修正または、影響低減が可能か	・システム仕様と脆弱性に関する情報				☆
		修正の影響テスト・修正の適用	（ソフトウェア企業のみ）修正提供時期やリソースの兼ね合いにより、根本対応ではなく暫定対処を実施する必要がある場合がある	・システム仕様と脆弱性に関する情報 ・修正およびテストに係る工数情報				☆

		悪用可能性評価コスト	（ソフトウェア企業のみ）CVSS スコアの評価コスト	（脆弱性に関する製品への詳細調査中に判断）				☆

「フィルタリング」列に☆印がある情報は、判断ツリーによる優先付けの対象とする脆弱性の数を減らすために活用できる情報である。例えばコンポーネントの開発者からのVEX情報により既に「影響なし」と判断されている脆弱性については、脆弱性優先付けの対象から除外することができる。「優先付け」列に印のある情報については、優先付けツリー利用後に、同一カテゴリ内での対応優先度を判断する必要がある場合に、活用可能と思われる情報である。各企業で、事前に各項目についての比重を決定し、その比重に応じて再評価を行うことで、カテゴリ内での優先順位を設定することが可能だと想定している。

また、「暫定対応・根本対応」列に印のある情報は、優先付け後、各脆弱性に対する対応を決定する際に参照すると想定される情報である。

脆弱性優先付けの自動化という意味では、悪用可能性の一部情報（インシデントの有無や PoC の存在など）、技術的深刻度の一部（CVSS スコア）については API 利用などで脆弱性 DB から情報を取得し、ある程度自動的に処理することは可能である。一方、両選択肢より詳細な脆弱性情報を元に判断をする場合や、ユーザー影響度、悪用効率性、人間による判断が、より正確な情報を元にした判断をする上で不可欠であると考えられる。また優先度付けやその後の対応方針については、自社環境やビジネス、ならびに脆弱性に関する状況も加味した上で実施される、人による判断がやはり重要であると考えられる。

なお、自動化以外の優先付け判断作業の効率化に当たっては、VEX 情報などに基づく事前フィルタリングだけでなく、事前判断が可能な選択肢を先に確定しておくという対応も可能だと考えられる。特にユーザー企業においては、同じシステムであれば脆弱性の内容にかかわらず「悪用効率性」「ユーザー影響度」の判断結果は同一になる。管理しているシステムについて事前に両選択肢の情報を定めておけば、脆弱性ごとに必要な判断ツリーの簡略化も可能だと考えられる。システム対象コンポーネントごとにまとめた判断も一案だと考えられる。

さらに、同じシステム内で使われる同じ OSS に複数の脆弱性が認められ、同じく新しいバージョンのコンポーネントで問題が解決される場合には、残りの悪用効率性と技術的深刻度が一番高いと思われる脆弱性に対してのみ優先付け判断を実施し、同一コンポーネントに関するすべての脆弱性に、便宜上同じ優先付けカテゴリ結果を当てはめてしまうという方法も可能であろう。最優先とされる脆弱性の対応のためにコンポーネントを置き換えれば、他の脆弱性も同時に修正できるからである。無論、根本対応時に必要な検証や関連情報の共有などは、脆弱性ごとに対応する必要がある可能性はあるが、優先付けの労力は一定程度圧縮できると想定される。

（3）脆弱性情報共有

1）ソフトウェア開発企業・ユーザー企業における脆弱性情報共有

ソフトウェア開発企業・ユーザー企業に対して実施した、脆弱性評価・優先付けに関するヒアリング内容を以下の表にまとめた。

表 1-46 ソフトウェア開発企業・ユーザー企業におけるヒアリング結果(情報共有)

	ソフトウェア開発企業	ユーザー企業
社内での情報共有	・ 関連する製品サポート部門や、顧客と接点のある営業部門などが関連 ・ 脆弱性報告当初は、基本的に PSIRT チームと、脆弱性に関係する製品の担当開発チームのみが関連。OSS 管理ツールなどからの通知については、製品チームに直接情報が届けられることになる ・ 対応方針や修正パッチのリリース時期などが見えてきた時点で、サポート部門など他のステークホルダーに情報共有。共有内容は、脆弱性についての解説、対応方針・時期 ・ Log4Shell のように、複数の製品に重大な脆弱性がある場合には、製品チーム横断でのコミュニケーションプロセスを起動。この場合は PSIRT チームから全製品チームへと情報が通知され、確認作業が開始される ・ やり取りは、基本的にメールや、脆弱性管理システムなどを通じて実施される	・ 脆弱性対応を実施する部門(情報システム部門や SOC チーム)と、脆弱性のあるシステムのオーナーが異なる場合、システムオーナーとの間で、脆弱性に関する情報共有や、対応方針・時期についてすり合わせをする必要がある ・
社外との情報共有	・ 外部から脆弱性報告があった場合には、報告者との連携、やりとりが発生する ・ サプライヤー側からの脆弱性報告があった場合、原則的には他の OSS からの報告時と同様に対応する。ただし、サプライヤー提供のコンポーネントが複数の製品に利用されている場合には、製品チーム横断でのコミュニケーションプロセスを起動。全製品チームへと情報が通知され、確認作業が開始される	・ 基本的には最終製品ベンダーとのやりとり。メール通知が主 ・ 所属している外部組織(CSIRT 協議会など)からの情報を得る場合もある ・ ベンダー側からの情報は「事象/リスク/パッチの有無/ワークアラウンド/該当するバージョン/パッチ適用後の再起動の有無」といった情報 ・ ベンダー、SIer からの情報は、まだ脆弱性の詳細情報が揃っていない段階で、初報として連絡が来ることもある

	・ 実際に製品に影響する脆弱性だった場合には、アドバイザリや修正パッチのリリースについて、ユーザー企業およびパートナー企業への告知を実施する。形態はメールと Web サイトでの公開が主であり、場合によっては担当者からの電話連絡を実施する ・ 製品に影響する脆弱性を公開する場合には、JPCERT/CC と連携する。脆弱性情報公開のタイミングや内容などについて足並みを揃える ・	・ 不完全な状態でも、先に第 1 報が送られる方が好まれる。事実確認中だけであっても第一報があるベンダーの方が信頼度は高い ・ 情報が足りない場合には、契約があればベンダーのサポートに直接問い合わせる。ネットワーク機器の場合には、SIer(NIer)の窓口もありえる。もらえる情報は SIer、ベンダー直接でも大きく変わらないが、日本人(ネイティブ)窓口の方がやりやすい。一部の製品の場合はベンダーやインテグレーターによる有償サービスとなる場合がある
課題、その他		・ ベンダーからの通知経路としては基本的にメールだが、MS Teams や Slack のようなコラボレーションツールとの連携や API 連携などはあってもいいのではないか。複数のアドレスを通知先にできるのであれば、よく使われているコミュニケーション機能への連絡手段があるとよいと思われる ・ 中小企業については大手の SI もついていない場合が多く、かなり人依存。地場の SIer の担当者によっては、注意情報をもらえることもある

以上のヒアリング結果より、一般的なソフトウェア開発企業・ユーザー企業における想定対応について以下の表に記載した。

表 1-47　想定されるソフトウェア開発企業・ソフトウェアユーザ企業における情報共有の傾向

種別	傾向
ソフトウェア開発企業	・　脆弱性対応開始から対応実施までと、対応終了後外部発信を検討する段階では、関連するステークホルダーに違いがみられる
ソフトウェアユーザ企業	・　現状は SBOM を用いた情報のやりとりは一般的ではない ・　完璧な情報が揃っていない情報であっても、ユーザーにとっては今後の対応を検討する重要な情報になる可能性がある ・　メール以外のコミュニケーション手段は現状多くない ・　母国語での情報提供の方がより好まれる

SBOM を用いた情報交換については、ユーザー企業においてまだ一般的ではない様子が窺えた。ユーザー企業にとっては、特定の脆弱性による影響についてなるべく早く大まかな状況をつかむことに意味があると想定されるため、SBOM を事前に入手しておくことは、それを実現する有益な選択肢の一つになると考えられる。一方で、脆弱性に関する情報が既にベンダー側から提供されている場合に、(該当の修正パッチ適用前に)自社が現在利用している製品バージョンの SBOM を入手しても活用効果は薄いと考えられる。

ソフトウェア開発企業においては、情報共有に関して「製品に影響する可能性がある脆弱性を認識し、対応について決定する」フェーズの他、「脆弱性に対する影響を同定し、外部へと通知する」フェーズがあることが確認された。特に「脆弱性に対する影響を同定し、外部へと通知する」フェーズについては、社内外の関係者が多く、様々なやりとりが発生すると考えられる。この外部通知に向けた準備において、発生するコミュニケーションと想定される関係者について、次の表にまとめた。

表 1-48 ソフトウェア開発企業の情報公開におけるステークホルダーと活動内容

カテゴリ	担当部署名	役割
対応主体	PSIRT	・　アドバイザリの作成 ・　(外部からの脆弱性報告の場合)報告者とのコミュニケーション ・　JPCERT/CC への脆弱性情報届出 ・　CVE ID の確保と情報提供
	製品チーム	・　修正内容の詳細情報提供

	（＋社内セキュリティリサーチャー）	・ CVSS スコアの決定 ・ 修正モジュールを含んだパッケージ+ readme の提供
社内ステークホルダー	サポート	・ 顧客への告知（Web サイト、メール）
	企業・パートナー向け営業担当	・ 顧客からの問い合わせ対応
	製品セキュリティ施策担当チーム	・ 開発チームを束ねるグループ単位での CVE 情報等の再確認
	広報	・ メディアなどからの問い合わせ対応（特に 0day 攻撃のものなど、緊急度が高い脆弱性の時）
社外ステークホルダー	パートナー・顧客	・ （情報の提供先）
	JPCERT/CC	・ 日本国内での情報周知にかかわる連携

一般的に、外部公開の際に、ソフトウェア開発企業が提供すべき情報としては、以下のようになると考えられる。

表 1-49 外部情報公開時に提供される情報

項目	**情報**
脆弱性に関する情報	CVE ID
	製品・バージョン
	脆弱性の詳細
	脆弱性への対処方法
	軽減要素
	参照情報
	提供情報の更新履歴
	脆弱性を悪用する攻撃キャンペーンの注意喚起
	脆弱性の技術解説・デモ
修正パッチに関する情報	提供開始日
	バージョン・ビルド情報
	修正される CVE ID
	修正パッチの入手方法
	修正パッチの導入手順

2）サプライヤーにおける脆弱性情報共有

社内の共通モジュール開発チームを仮想サプライヤーとみなし、仮想サプライヤー担当のコンポーネント内に存在する脆弱性に関しての想定情報共有フロー、また他チームとの役割分担や脆弱性に関する情報共有プロセスについても合わせて整理した。

脆弱性が報告され、それがサプライヤー担当コンポーネント内に存在する脆弱性であった場合、以下のフローにて情報共有および他チームとの役割分担が行われる。

1. PSIRT チームがサプライヤー担当コンポーネントに対する脆弱性ごとにタスクを起票
2. PSIRT チームは 1 で指定した脆弱性に対し、影響があると考えられる製品に対して情報提供を依頼
3. 製品チームは、利用しているサプライヤー担当コンポーネントのバージョンなどの情報を更新
4. サプライヤーチームは提供された情報を元に、可憐するコンポーネントとバージョンにおいて脆弱性の解析を行い、影響の有無を判定
5. 製品チームはサプライヤーコンポーネントが影響ありと判定された場合には、脆弱性対応を開始し、ソリューションを提供する
6. PSIRT チームまたはサポートチームが作成されたソリューションを提供

本実証ではサプライヤーも製品チームも同じ企業内にあることもあり、PSIRT チーム側が起点となって、該当コンポーネントによる影響がある製品と利用しているバージョン情報の調査をするところから対応が開始されていることがわかった。外部のサプライヤー企業とのやりとりの場合は、最終ベンダー側から脆弱性に関する問い合わせが入った場合であっても、サプライヤー企業側が最終ベンダーに提供しているコンポーネントの履歴や契約情報などを元に、脆弱性情報が提供されるところから開始する場合もあると考えられる。

3）VEX 情報の作成と共有

ソフトウェア開発企業の場合、脆弱性の外部への情報共有において、VEX を用いる可能性がある。vexctl を利用して VEX ファイルの作成を試行したところ、必要な情報さえ揃っていれば、ツールを用いて OpenVEX ファイルを作成すること自体は容易であった。

一方、VEX の配布については、いくつか考慮の必要があると考えられる。1 点目は、SBOM とは異なり、ソフトウェアのリリースバージョンと 1 対 1 の関係性ということはまずなく、対応する情報が増加し続ける可能性があることである。修正パッチなどを含め、複数のリリースパッケージに同じ脆弱性が影響するような場合もあり、VEX の配布時の情報単位がまちまちになる可能性もあり、サポートリクエストなどを通じて問い合わせのあった顧客に都度配布するような運用は、ユーザー企業にとってもソフトウェア開発企業側にとってもプロセスが煩雑になる可能性が高い。専用の API かデータフィードを提供してユーザー企業が取得できるようにするか、github.com のような公開リポジトリに保管し、API などで自動的に取得・更新できる体制を整える必要があるだろう。SBOM のケースで想定できるように、顧客からの問い合わせに応じて VEX ファイルを提供するフローは不可能ではないが、アドバイザリなど他の形態で情報が公開されていることが多いことを考えると、文章でも提供可能な情報をあえて VEX で提供するのは現実的な選択肢ではないと考えられる。

二点目は、SBOMと関連するVEXファイルの関係を容易に同定できるようにする必要がある点である。後述のEU CRA対応などを想定した場合、リリース時のソフトウェアにおける脆弱性情報（例えばインシデントが観測されている脆弱性を持つコンポーネントを内包しているが、実際には脆弱性の影響を受けないことが判明している場合など）をSBOMとともに参照できるようにしておく必要があると考えられる。リリース後に判明した脆弱性については事前にSBOMに含めることが当然ながら不可能であるため、VEXファイル側、またはVEXファイルを提供するAPIやリポジトリ内の情報から、何らかの方法でSBOMファイルまでたどり着ける道筋を設定しておくことが望ましいと考えられる。

（4）暫定対応および根本対応

ソフトウェア開発企業・ソフトウェアユーザ企業に対して実施した、脆弱性の暫定対応および根本対応に関するヒアリング内容を以下の表にまとめた。

表 1-50 ソフトウェア開発企業・ソフトウェアユーザ企業におけるヒアリング結果（暫定対応・根本対応）

	ソフトウェア開発企業	ソフトウェアユーザ企業
暫定対応	・ 脆弱性対応優先付けの結果に基づき、対応保留の場合は暫定対応とし、それ以外の場合は、根本対応まで行う。 ・ 基本的には根本対応（脆弱性のあるコンポーネントの更新や、問題のあるコンポーネント・コードの削除）を実施する方向で検討する。ただし、対応コストや技術的な課題などの問題で根本対応ができない場合、または根本対応の実施に長い時間が必要で、期待される脆弱性対応の時間枠で修正が難しい場合には、暫定対応を実施する可能性がある ・ 暫定対応の内容は、機能や脆弱性によって異なるため一概には言えないが、特定機能の無効化などが考えられる	・ ベンダー提供のワークアラウンドが存在する場合には適用する。社内サービスであれば適用による動作不具合のリスクよりも対応を優先するケースも多い ・ 自分たちでワークアラウンドを考えて適用というのはほぼ無い ・ 特定機能にのみ影響がある脆弱性かつ、該当機能を使っていないケースであれば、該当機能の停止や削除を実施することはある。ただし、回避策のためにシステム利用を止めるまで行けるかというと、よほど大きな問題があるときでなければない ・ 中小企業では、現実的に暫定対応は不可能
根本対応	・ 重要な脆弱性の修正については、Critical Patch（外部公開されるパッチ）にて対応。それ以外の場合には、他の不具合修正などと一緒に提供することが多い ・ 個人向け製品や中小企業向け製品では、製品が持つインターネット経由での自動更新機能を用いて、修正パッチを配信することもある	・ 企業によっては、重要インフラ・サービスへのパッチ適用の目標値を持っている（仮想化サーバー基盤に関する重要な脆弱性なら 72 時間以内に適用するなど） ・ 社外向けサービスにパッチ・ワークアラウンド適用時のダウンタイムがある場合は適用可否や時期についてビジネスオーナーとの協議を踏まえた判断が必要 ・ SaaS 製品の脆弱性の場合、ユーザー側で特にアクションは行わない。やることも特にない。特に脆弱性の通知も無く、いつの間にか修正されている場合がほとんど ・ 中小企業におけるパッチ適用は、情報システム担当部門があれば、そこで行う。該当部門が無く、外部にアウトソースしている企業については、契約している内容によるのではないかという話

課題、その他	・	・　ビジネスに活用するためにシステムを導入しているという前提に立つと、やはり余程深刻な状況でない限り、暫定対応としてシステムの利用を停止するまでは決断できないと想定される

以上のヒアリングから想定される、一般的なソフトウェア開発企業・ユーザー企業における対応を下表に記載した。

表 1-51 ソフトウェア開発企業・ソフトウェア企業で想定される暫定対応・根本対応

	対応内容
ソフトウェア開発企業	・ 脆弱性のあるコンポーネントのアップデートなど、まずは根本対応での対処を検討 ・ 暫定対処は技術的な難易度、検証テストに必要な工数、またはOSS 側での修正の有無などから、根本対応が困難であると想定された場合にやむを得ず選択される場合が多い ・ 暫定対応の例としては、脆弱性の影響がある機能の削除、特定機能の無効化、脆弱性のない最新バージョンの製品への移行を推奨するなどが考えられる。 ・ ネットワーク制御など、ユーザー企業側での環境設定による暫定対処が有効な場合もある。ただし、ユーザー側の対応にゆだねられる部分が高く、必ずしもユーザーに受け入れられない可能性もある
ソフトウェアユーザ企業	・ 製品への悪影響を避けるためにも、基本的にはソフトウェア開発企業から提供される修正モジュール、または問題の回避策を適用することによって対応 ・ ベンダーから対応策が提供されていない場合には、自主的な暫定対処を検討する必要がある。取り得る選択肢としては、(特に外部からの)ネットワークアクセスやアクセスできるユーザーを通常時よりも制限する、システムの一部機能、またはシステムそのものを停止し使用しないなどを想定。 ・ ファイアウォールや IPS、仮想パッチ、アプリケーションコントロールなど、自社に導入済みのセキュリティ製品の機能を活用することで、脆弱性リスクの低減が可能な場合もある ・ ただし、手段があっても実際に採用できるかどうかは、ビジネス影響と脆弱性によるリスクのトレードオフの検討結果次第。かなり深刻な脆弱性である場合を除き、ビジネス影響の方を重く見る傾向がある

1.2.13 コスト・効果の評価

下表は、本実証においてかかった作業コストをフェーズごとにまとめたものである。項目は明示的に記載がないものは、ソフトウェア開発企業・ユーザー企業ともに実施すると想定される内容である。また、作業にかかった時間については、各作業に対して関連する技術分野について知見や経験がある技術者が実施した結果である。関連分野での経験が少ない者が担当した場合には、学習コストなどを含め追加の時間が発生する可能性がある。

なお、情報共有にかかるコストについては、脆弱性の内容などによりかかるコミュニケーションの複雑性や時間が大きく変動すること、それ以外の労力についてはメールやコミュニケーションツールでのやりとりとなり、ほぼ時間的には 0 とみなせることから、表には記載していない。

表 1-52 実証関連コスト一覧

フェーズ	大項目	小項目	作業者レベル	作業工数（時間）	金額（円）	補足
脆弱性特定	API 利用	初期設定	中級者	2.00	10,700	API 利用にかかわる調査など。REST API の呼び出しに経験のある技術者が実施した場合
		SIEM 製品 1 解析環境セットアップ	中級者	4.00	21,400	SIEM 製品 1 のインストールとセットアップ経験がある技術者が実施した場合
		運用	中級者	1.00	5,350	API 利用におけるランニングコスト
	pURL -> CPE 変換	OSS(purl2cpe)の調査	中級者	3.00	16,050	
		pURL から CPE を生成するスクリプト作成	中級者	10.00	53,500	Python にて作成。Python でのコード作成に経験がある技術者が実施
	無償 SBOM ツール A	使用方法の学習＋インストール	初級者	8.00	38,560	ソフトウェアのインストール経験がある者が実施した場合
		SBOM インポートと脆弱性特定	中級者	8.00	42,800	参考値（サンプルとして挙げられていた情報より SBOM ファイルを自分で作成・調整してインポートした場合）。インポートのたびに必要となるコスト
	有償 SCA ツール	SBOM インポートと脆弱性特定	初級者	0.01	48	今回は有償 SBOM ツール A を使用。Web コンソールから実施。インポートのたびに必要となるコスト
脆弱性優先付け	フレームワークを用いた対応	ツリーを用いた優先順位付け（脆弱性 1 件当たり）	中級者	0.20	1,070	本実証に記載したフレームワークに則り、10 件の脆弱性に対して優先付けを実施した結果の平均。学習コスト含む。脆弱性ごとに発生するコストとなると想定。 概算だが、参考までに各項目の確認にあたって参照した情報と、その確認にかかった平均時間を

						以下に記載する 4 分 – 脆弱性 DB2 による脆弱性情報 1 分 – 社内脆弱性情報システムによる Exploit 公開および攻撃状況 4 分 – SCA ツールによる脆弱性情報、アドバイザリ情報およびパッチ情報 1 分 – CVSS スコア
脆弱性対応（暫定対応・根本対応）（脆弱性修正は除く）	**VEX ファイル作成（ソフトウェア開発企業）**	**OpenVEX 形式のファイル作成**	中級者	0.50	2,675	作成に必要な情報がすべて揃っている場合のデータ。OSS（https://github.com/openvex/vexctl）を作成に利用。該当 OSS の操作学習コスト含む学習コスト以外については、VEX ファイル作成のたびに発生するランニングコスト。
	SBOM 管理	**修正パッチ用 SBOM 作成**	初級者	0.01	48	有償 SBOM ツール A の Web コンソールより作成した場合。手動での SBOM ファイル作成ごとにかかるコスト
	CVSS スコア	**スコアの決定（ソフトウェア開発企業）**	上級者	0.25	1,588	判断に必要な情報がすべて揃っている場合。必要情報の調査時間は脆弱性や製品によるため、今回のコストには含めない。脆弱性ごとに必要なコスト
	アドバイザリ作成（ソフトウェア開発企業）	**英語原稿作成**	上級者	3.00	19,050	必要な情報がすべて揃っている場合。開発チーム提供の情報に不明瞭な点があるなどの場合には、確認や調整の時間が追加で必要。アドバイザリ作成・リリースのたびにかかるコストだが、同時に修正された脆弱性についてはまとめて記載することもあるため、脆弱性ごとのコストではない場
		日本語翻訳	上級者	2.00	12,700	

						合もある
		レビュー	上級者	1.00	6,350	アドバイザリ作成ごとに発生

SBOM の情報を脆弱性 DB の API と組み合わせて利用する場合（または既存ツールを活用する場合）、最初の設定完了後は、一つ一つコンポーネント情報を取り出して検索する必要がないため、脆弱性特定の効率を大きく向上できると考えられる。ただし、現状は pURL から正しい CPE への変換が必ずしも可能ではないこともあり、マッチングの精度については API 活用には課題があることも分かった。一方、SCA ツールなどで SBOM ファイルを読み込む場合には、既存の SCA ツールが持つ機能がそのまま使用できる可能性が高く、脆弱性特定の効率は高いと考えられる。

今回の検証で設定した脆弱性優先付けフレームワークを利用した場合、優先付けカテゴリの策定に対して 1 件に対して平均して実測 10 分程度の時間がかかることが判明した。優先付けの実測値は事例によりバラツキが大きく、中でも脆弱性 DB2 や SCA ツールによる脆弱性情報およびアドバイザリ情報の確認の時間が、特に変動が大きかった。概算では、最大で 20 分、最小で 5 分程度が目安となる。

特定された脆弱性が多い場合に、手動ですべての脆弱性に対して優先付けの実施が可能である企業は少ないと考えられ、実際の活用には、如何に自動化できるかが課題となると考えられる。

優先付けフレームワークの判断付けのうち、悪用可能性については、脆弱性 DB との連携ができれば、自動化が検討しやすい領域である。今回の実証では KEVC との連携のみ実施しており、また実際にインシデントが観測されている脆弱性はなかったため実データでの比較はできなかったが、事前に PoC コードやインシデントの有無を判断する情報ソースを固定しておけば、自動化による労力削減が可能だと想定される。また、特にユーザー企業については、システムごとに事前に「悪用効率性」と「ユーザー影響度」を見積もっておくことは可能であるため、実質的には脆弱性ごとに都度判断が必要な項目を 2 種類にまで減らすことが可能である。この下準備をしておくことで、下位のソフトウェアユーザ企業については、「悪用可能性（インシデントの有無のみ）」を判断すれば優先付け判断ができることになり、該当の情報を容易に手に入れる手段さえ確保できれば、人的リソースとスキルに限りがある中小企業でも比較的対応しやすくなるのではないかと考えられる。

一方で、有償 SBOM ツール A を利用した場合、読み込める SBOM ファイルの種類には制限があったものの、脆弱性特定は容易であり、また CPE 変換時の制限などで API 活用時にはマッチしなかった脆弱性を同定することが可能であった。この事象が発生する理由として想定されるのは、正しい CPE 変換ができないようなコンポーネントに対しても、有償 SBOM ツール A が持つ DB では pURL などの情報でのマッチングが可能であるということである。また、まだ CVD ID が Reserved 状態のままで、まだ脆弱性 DB2 DB などには脆弱性の詳細情報が反映されていない脆弱性についても、有償 SBOM ツール A の持つ DB 上では情報が更新されているケースもあるため、このような脆弱性の存在も、API 利用時のマッチング結果との差を生み出している可能性がある。今後、各種 SCA ツールにおいて SBOM インポート機能が拡張され、多くの SBOM ファイルが読み込めるようになった場合には、SBOM 作成だけでなく、管理の面でも活用が期待できると考えられる。有償ツールの場合は価格が課題になる可能性はあるが、SCA ツールの結果に、ツールでは利用されていない脆弱性 DB からの情報を連携させるなどの、さらなる拡張も検討できるだろう。

（1） VEX の自動化について

VEX において機械判読可能なラベルを用いることで自動化されるユースケースが考えられる。例えば VEX のステータスが not_affected な場合に、その VEX を SBOM 脆弱性突合ツールまたは脆弱

性検査ツール(脆弱性スキャナー)に読み込ませることにより、検出された脆弱性が製品に影響ないという状態を反映することができる。またこれにより不必要な脆弱性の通知アラートが抑制するなど、脆弱性管理において効率化が期待できる。

1.2.14 課題・ノウハウ・留意点の整理

(1) 脆弱性突合における誤検知・検出漏れの課題

脆弱性 DB における脆弱性情報に対して影響を受ける部品 ID の対応付けの仕様が明確では無く、脆弱性突合における誤検知・検出漏れの原因となることがある。以下にその要因と課題を示す。

ある製品 X が、下図のように OSS A, B、有償ライブラリ C を含んでいると仮定する。また製品 X の独自コード部分、OSS A の独自コード、OSS B 内で使われる別の OSS E 内にそれぞれ異なる脆弱性が含まれているとする(CVE 1, 2, 3)。また、有償ライブラリ Cにおいては、CVE 2の脆弱性はOSS A の利用方法によって、脆弱性の影響を受けないと仮定する。

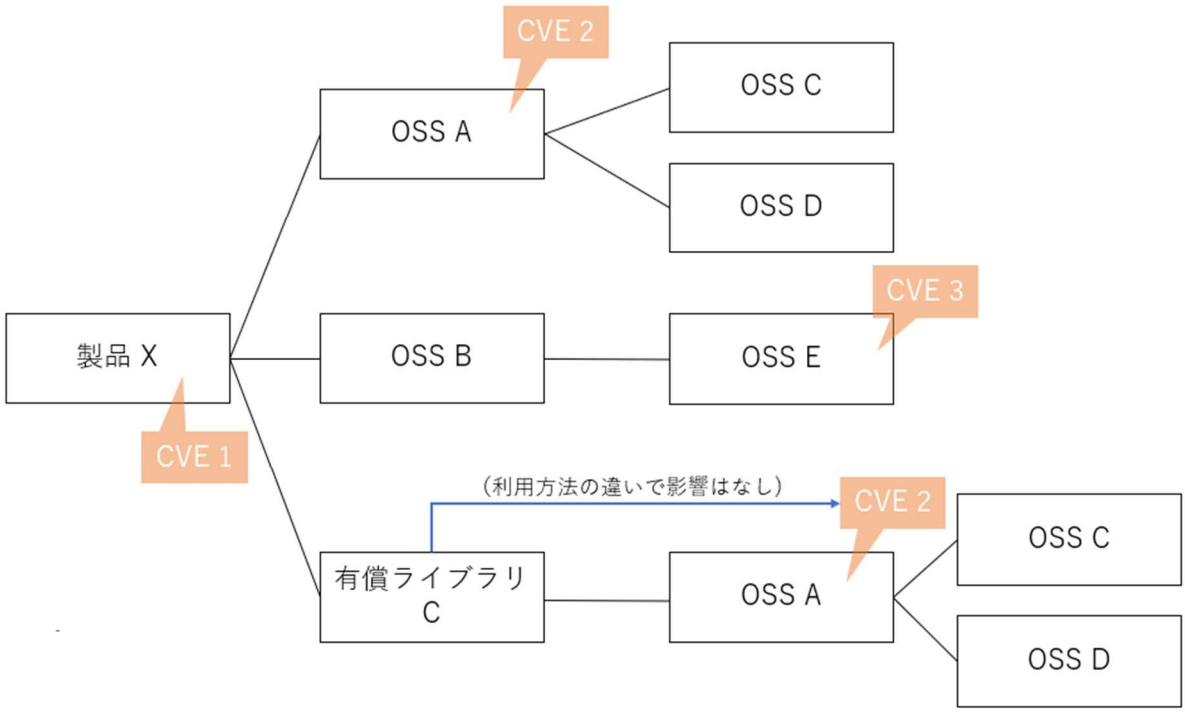


図 1-12 仮の製品 X とコンポーネント階層図

これらの脆弱性が登録された脆弱性 DB に対して、製品、コンポーネントの使用者それぞれの立場で、検索を実施する場合、期待される検索結果は下表のようになる。

表 1-53 製品・コンポーネントに対する脆弱性検索結果の期待値

検索する製品・コンポーネント名	検索結果の期待値
製品 X	CVE 1, CVE 2, CVE 3

OSS A	CVE 2
OSS B	CVE 3
OSS C	（影響なし）
OSS D	（影響なし）
OSS E	CVE 3
有償ライブラリ C	（影響なし）

ところが、現状の脆弱性 DB においては、例えば CVE 3 の脆弱性が製品 X の脆弱性として紐づけられてしまい、OSS E の脆弱性として扱われない可能性がある。原因は現状定かではないが、図で示したような脆弱性とコンポーネントの関係性についての情報を現在は保持していないことによるのではないかと推測される。

この問題に関しては、脆弱性と影響のあるコンポーネントの情報の整理に、グラフデータベースを利用することにより、解決できる可能性がある。例えば製品 X が CVE 2 についての修正や情報公開を行う際に、この脆弱性が製品 X の自前のコード内に存在していたのか、また、外部由来の場合には製品 X 側から見る脆弱性の原因箇所である、OSS A についても同時に情報提供をする。これにより、脆弱性 DB 側はこの段階で実際の脆弱性は OSS A またはその内部コンポーネントにあることを把握できる。この段階で、OSS A の作成者が CVE 2 の脆弱性があること、および OSS A の独自コード内に存在していることを追加で報告すれば、脆弱性 DB は OSS A にあり、仮に OSS C，D が OSS A で利用されていることがのちに判明したとしても、OSS C，D には関係がない脆弱性であることが確かめられていることになる。また、有償ライブラリ C から OSS A については利用しているものの CVE 2 の影響は受けない旨の報告があれば、同様にエッジとして情報を反映させることも可能であろう（下図参照）。API などによる特定製品・コンポーネントに検索については、現状のインターフェースは大きく変えずに、このグラフデータベース上の結果を元に、影響を受けるものだけを検索した結果が応答で返されるようになっていれば利用者側への影響も少ないと考えられる。現状、コンポーネント名のみで CPE 検索を実施した際の誤検出の多さも、脆弱性とコンポーネントの関係を記録できることによって減らすことができると考えられる。

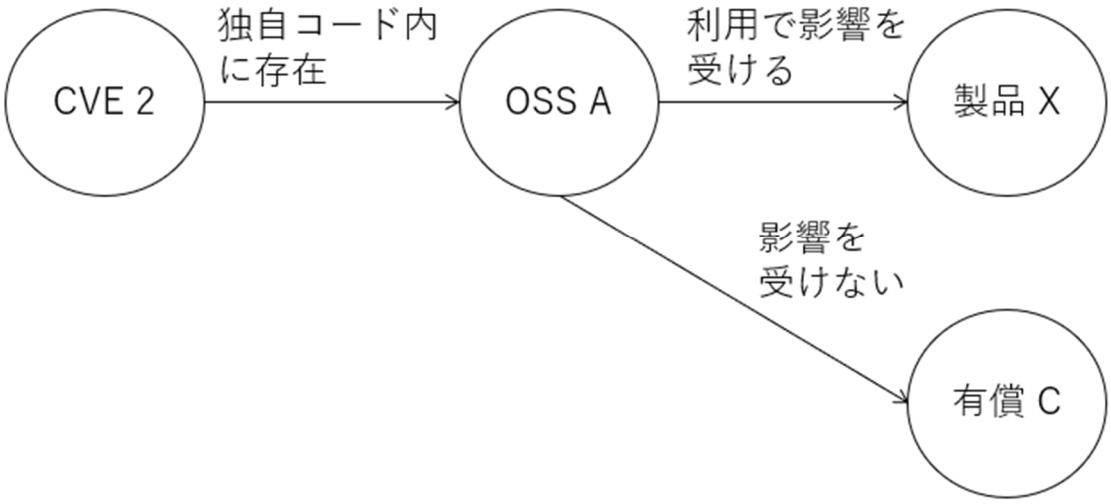


図 1-13 グラフデータベースによる脆弱性とコンポーネントの関係性のイメージ

以上のような問題に対しては以下の 2 通りで解決することができると考えられる。

- 脆弱性 DB の対応
  脆弱性 DB における各脆弱性情報における影響を受ける部品として、部品の依存関係の最も末端（下位）に紐づけることで、脆弱性突合における検出漏れを回避することができる。
- VEX の利用

前述のとおり、脆弱性 DB において脆弱性の影響を受けるすべての部品に脆弱性情報が対応づけられておらず、上位の製品のみに対応づけられている場合、脆弱性の検出漏れが起こり得る。このような場合、VEX 情報に、対象とする部品の上位の部品・製品に対する脆弱性マッチングの必要性などの対処法を明記することが考えられる。ただし、これは誤検知を生じる可能性があるため、根本解決にはならならず、根本対応のためには、（ア）に示す通り、脆弱性 DB における脆弱性情報と影響を受ける部品の対応関係を正確に示すことが期待される。

（2）SBOM の部品 ID と脆弱性 DB の突合について

脆弱性 DB2 や脆弱性 DB1 API の利用に関して念頭に置かれている部品 ID は CPE であるが、本実証において入手できた SBOM に、CPE が記載されているものは存在しなかった。次善策として SBOM に含まれる pURL やコンポーネント名から CPE を生成し、脆弱性 DB との突合を試行した結果、一部では期待する結果が得られたものの、必ずしも当初の期待通り、自動的に脆弱性 DB の情報とマッチングができるわけではないことが分かった。また、CPE 自体についても、プロセス上は、コミュニティのボランティアとソフトウェア開発企業の両方が登録申請を行うことができるようになってはいるものの、すべてのソフトウェア開発企業が自社製品の CPE 登録を体系的に実施しているわけではなく、登録される情報にも設定値のぶれや誤りがある可能性があることが判明した。SBOM による効率的な脆弱性特定が可能になるには、第 1 にこの部品 ID の突合問題についての解決が必要となるであろう。

この問題認識は、本実証内の話にとどまらない。例えば、OWASP は MITRE および脆弱性 DB2 に

対し、現在の CPE による脆弱性マッチングに関する課題と、対案として pURL を用いた DB のクエリについての推奨[56]を行っている（一方で、pURL についても SBOM に必ずしも記載されているとは限らないため、SBOM 内に pURL が確実に記載されるようになるためには、一部 ecosystem での詳細仕様の策定や、内部での浸透も不可欠だと考えられる）。また、2023 年 10 月には CISA が脆弱性やソフトウェアインベントリの管理などに利用可能な部品 ID について、現状と課題の分析を記したドキュメントを公開している[57]。

ソフトウェア業界全体で、より安全で効率的な対応が可能となるように、前述の脆弱性 DB 上でのデータ保持方法の変更や、脆弱性公開情報の変更なども含め、現在の課題の解決に向けて対応していく必要があるだろう。

（3）脆弱性 DB3 および脆弱性 DB1 API に対する機能ニーズについて

1）指定可能な CPE 形式について

脆弱性 DB1 API の「脆弱性対策概要情報一覧の取得」をする際、リクエストのパラメータに cpeName を指定することができるが、指定可能な CPE 表記は URI 形式のみであり、調査時点では Formatted String 形式（バージョン 2.3 で定義）による API 問い合わせには未対応である。また、パラメータ値として採用される文字列は「cpe:/{part}:{vendor}:{product}」と定められており、問い合わせの識別子としてバージョン情報やその他の属性情報を使用することができない。バージョン 2.3 では下位互換性のために URI 形式が包含されているが、Formatted String 形式は URI 形式とは異なる構文であり追加の製品属性もサポートすることから、将来的により詳細な識別子としての活用が広がる可能性が考えられる。そのため、API の提供にあたっては、製品のバージョン情報やその他の属性情報を含め、バージョン 2.3 以降で利用可能な Formatted String 形式でのリクエストを許容することが望まれる。

また、前述のとおりパラメータ値として採用される文字列は「cpe:/{part}:{vendor}:{product}」と定められているが、現時点ではベンダー名をワイルドカード指定できないようになっている。例えば CPE 指定の例として「cpe:/a:apache:http_server」で問い合わせを行った場合、多数の脆弱性にマッチするが、「cpe:/a:*:http_server」とした場合は何れの脆弱性にもマッチしない。API 利用者は本来必要な情報が不足している状態であっても API 問い合わせをする可能性があるため、CPE の解釈を柔軟に広げることも検討されたい。

2）API 応答の形式について

応答に関して、現在の仕様においては、API の応答は XML 形式で定義されているが、一般的な WebAPI システムにおいては JSON 形式での応答も普及している。JSON は XML と比較して同じ情報をよりコンパクトに表現することができる。JSON は今後も普及が拡大していくことが予想されるため、JSON 形式での応答も得られることが望まれる。API 問い合わせ時のパラメータに応答形式を指定で

[56] https://owasp.org/blog/2022/09/13/sbom-forum-recommends-improvements-to-nvd
[57] https://www.cisa.gov/resources-tools/resources/software-identification-ecosystem-option-analysis

きるオプションを加えることで、既存の利用者に影響なく機能の拡充が可能であろう。

3）API で取得可能な情報の拡張について

利用者に対してより有用な情報を届ける手段の一つとして、API の応答に脆弱性の悪用事例や悪用有無の情報を取り入れることを検討されたい。KEVC に掲載された脆弱性のような、悪用事実の確認有無や、具体的に使われた攻撃の種類等が API 応答に含まれていると利用者の脆弱性への対応指標となり得る。IPA や J-CRAT への相談や通報を基に、脆弱性の悪用に関する情報を付加することができれば、特に国内組織において有益な情報になることが予想される。

（4）中小企業における SBOM 活用と脆弱性対応

多くの中小企業、特にソフトウェアユーザ企業では、専任の情報システム部員の不在や、セキュリティ・脆弱性に関する知識の不足により、SBOM ファイルの直接的な活用や、脆弱性対応は困難であると想定される。中小企業において脆弱性を起点としたセキュリティリスクを少しでも低減させるためには、使いやすく、設定や情報取得含め、自分で判断・対応することが少なくてすむ自動化ツールがあると望ましい。例えば、社内環境にある製品の自動検出や、脆弱性に関する重要な情報の自動取得などである。また、実際にインシデントが観測されている脆弱性については最低限対応できるようにすることで、喫緊のリスクを回避できることが可能だと考えられる。JVN などで日本語かつわかりやすいインシデント情報の発信が強化されることを期待したい。

（5）無償 SBOM ツール A ツールの利点と課題

無償 SBOM ツール A は、無償であることも含め比較的簡単に導入可能である。したがって、小規模の企業において、自社システムの状況をまず確認したいようなケース、または脆弱性管理を始めたいが人的金銭的リソースがかけられない場合に、最初の一歩として手に取ってみるのには利用しやすいツールであると考えられる。

一方、同ツールには制限や課題もある。現在対応しているファイルフォーマットが SWID のみのため、無償 SBOM ツール A と SBOM を組み合わせて利用したい企業はこれを前提に SWID 形式および CPE フォーマットで製品の情報を記述している SBOM ファイルの提供をベンダーに要望することになる。仮にベンダー側で SWID 形式の出力に対応していないツールを利用している場合や CPE フォーマットで製品の情報を記述するようになっていない場合、別途変換ツールを入手、あるいは手動で変換作業をおこなう必要がある。また、ベンダー側で利用しているツールで対応ができない場合、ベンダー側で無償 SBOM ツール A を別途導入して対応するかユーザー側での対応が必要になり、いずれの場合においても工数など双方の負担増加が想定されるため、昨今の状況を鑑みて複数のフォーマット形式（SPDX, CycloneDX など）への対応が望まれる。

また、特に 1.2.14（4）で記載したような中小企業での活用を考えた場合には、1.2.14（3）にも記載した、「実際に悪用事例のある脆弱性」についての情報が取得できるようになること、またソフトウェアやセキュリティに詳しくない人物が見たときにもわかりやすいメッセージや機能設定であることが望ましい。

（6）SBOM ファイルの更新管理における課題

ソフトウェアユーザ企業においては、特定システムの脆弱性に対応するパッチが適用された後、更新されたシステムと連動する形で、該当システムの SBOM ファイルを更新する必要がある。一方で、Linux 製品 A の例では、インストールメディアに対する SBOM ファイルは提供されているものの、個別のコンポーネントごとに SBOM を提供している例は発見できなかった。つまり、インストール以降、何らかのコンポーネントを更新した段階で、手元にある SBOM 上の構成情報と、実際に使用する環境に差異が発生することとなる。

この問題を解決するためには、以下の二つの方法が考えられる。

① ソフトウェア企業側で修正パッチリリース時に必ず SBOM ファイルを更新し、リリースする
② ユーザーが自分の環境で SBOM ファイルを更新、または作成できるようにする

ユーザー側での負担を減らすため、基本的にはソフトウェア開発企業側で対応する①が望ましい。一方で、システムで使われるすべてのコンポーネントが修正パッチに含まれず、問題のあった一部のコンポーネントについてのみ更新する修正パッチの場合には、たとえソフトウェア開発企業側でパッチの内容に基づく SBOM ファイルを作成したとしても、ソフトウェアユーザ企業側で手持ちの SBOM ファイルに対して、関連する情報のみを更新する作業（SBOM ファイルのマージ作業）が必要となると考えられる。マージ作業が簡単にできるツール等は現状確認できておらず、実施する場合には手動でファイルを編集するか、自主的に作成したスクリプトファイルなどで対応する必要がある。ユーザー企業における SBOM 管理の効率性の点では、すべてのコンポーネントを差し替え、SBOM ファイルも置き換える方が簡便であるものの、ソフトウェア開発企業、ユーザー企業のいずれも、検証範囲やリスクを限定する目的で修正範囲をより少なくすることを好む傾向があるため、必ずしも全コンポーネントを更新すればよいと言い切れない。

対して、②の場合には、ソフトウェアユーザ企業で実際に利用されているシステム構成にマッチした SBOM ファイルを確実に取得できる利点がある。Linux 製品 A ではこのような目的で利用できるツールは見つからなかったが、Linux の他のディストリビューションに対しては、OS 上で利用できる SBOM 作成ツール[58]が公開されていた。ただし、システムの開発企業が SBOM 作成に使用したツールとユーザー企業側が持つツールが異なる場合には、同じシステムに対して出力される SBOM ファイルの内容やリストアップされるコンポーネントの種類などが異なる可能性もあるため、注意が必要である。

なお、ソフトウェア開発企業側では、パッチやソフトウェアパッケージのリリースごとに、SBOM を作成し、保管しておく必要がある。技術的には目立った課題はないが、インストールパッケージと脆弱性の修正パッチで含まれるコンポーネントの構成が異なる場合に、修正パッチ用の SBOM をどう作成するかなど、事前にリリース形態に合わせた SBOM 作成プロセスを規定しておく必要がると考えられる。

1） パッケージマネージャーベースの SBOM 作成

[58] https://github.com/CycloneDX/cyclonedx-linux-generator

SBOM 作成ツールや CI ツールにおいてパッケージマネージャー、ビルドツールベースの SBOM 作成がサポートされている。各ツールによるパッケージマネージャーのサポート状況を下表にまとめた。いずれのツールにおいても主なパッケージマネージャー等はサポートされている場合が多く、SBOM の作成においてもパッケージマネージャー等のメタ情報から生成される SBOM は精度が高く、基本的に誤検知は発生しない。

依存している OSS コンポーネントが GitHub の公開リポジトリで管理されており、かつそのリポジトリで Dependency graph の機能が有効になっている場合には SBOM をエクスポートすることが可能である。これによりコンポーネントが更新された際の最新の SBOM を取得することが可能であり、更新管理に利用できる。

なお、米国サイバーセキュリティ国家戦略および CISA ロードマップ The Case for Memory Safe Roadmaps においては、メモリーセーフ言語の推進の重要性が示されている。パッケージマネージャーベースの SBOM サポートについて、メモリーセーフ言語（C#、Go、Java、Python、Rust、Swift）の対応が含まれる。

下表、rpm については OS 系パッケージマネージャーであり、それ以外はビルド開発ツールである。「検出ソース」列は、依存関係を検出するために使われるマニフェストファイル、あるいはそれに相当するものを示す。

表 1-54 パッケージマネージャーのサポート状況

パッケージマネージャー	プログラミング言語	検出ソース	有償 SBOM ツール A[59]	MS sbom-tool component-detection[60]	yamory[61]	GitHub[62]
Bazel	Java Kotlin Scala	maven_jar maven_install	○			
BitBake	依存なし	oe-init-build-env	○			
Clang	C/C++	compile_commands.json	○			
Cargo（Rust）	Rust	Cargo.toml Cargo.lock	○	○	○	○
Carthage	Objective-C Swift	Cartfile Cartfile.resolved	○			
CocoaPods	Objective-C Swift	podfile.lock		○		
Composer	PHP	composer.json			○	○
Conan	C/C++	conan.lock	○			
Conda	Python R	environment.yml	○			
Dart	Dart	pubspec.yaml pubspeck.lock	○			○

[59] https://community.synopsys.com/s/document-item?bundleId=integrations-detect&topicId=packagemgrs%2Foverview.html&_LANG=enus

[60] https://github.com/microsoft/component-detection/blob/main/docs/feature-overview.md

[61] https://yamory.io/docs/category/application-library/

[62] https://docs.github.com/ja/code-security/supply-chain-security/understanding-your-software-supply-chain/about-the-dependency-graph

Erlang/Hex/Rebar	Erlang	rebar.config	○			
GoLang	Go	Gopkg.lock gogradle.lock go.mod go.sum	○	○	○	○
GitHub Actions	YAML	*.yml *.yaml				○
Gradle	Java Kotlin Scala	build.gradle *.lockfile	○	○	○	
Ivy（Ant）	Java	ivy.xml	○			
Lerna	JavaScript	lerna.json	○			
Maven	Java Scala	pom.xml	○	○	○	○
npm	JavaScript	package.json package-lock.json npm-shrinkwrap.json lerna.json	○	○	○	○
NuGet	.NET	packages.config project.lock.json project.assets.json project.json *proj	○	○	○	○
pnpm	JavaScript	shrinkwrap.yaml pnpm-lock.yaml	○			○

Pip（Python）	Python	setup.py requirements.txt	○	○	○	
rpm	依存なし	バイナリパッケージ	○			
Ruby	Ruby	gemfile.lock	○	○	○	○
SBT	Java Scala	build.sbt	○	○	○	
Swift & Xcode	Swift	Package.resolved Package.swift	○			○
Yarn	JavaScript	yarn.lock package.json	○	○	○	○

（7）開発形態と脆弱性対応

ソフトウェア開発企業における開発には、大きく分けて汎用的な既製品を提供する形態（パッケージ、SaaS 問わない）と、特定のユーザー企業から開発を受託し、製品・システムを納品する受託開発（OEM 開発を含む）を実施する形態がある。一般的に、既製品を開発・提供する場合には、製品のライセンス契約またはサポート契約に基づき、製品サポート期間中の不具合対応および脆弱性への対応が約束されている。少なくとも、製品のサポート期間中に発見された脆弱性についてはその影響度の判断と対応方針について決定し、契約内容に基づいた対応をする必要があると考えられる。また、脆弱性対応について明示的な記載がない場合でも、ライセンス契約に基づく不具合対応が約束されている場合には、脆弱性対応も不具合対応同様実施することが期待される。少なくとも、重大な脆弱性については何らかのソリューションを提供する必要があるだろう。

一方、受託開発企業で、システム納品後の保守対応や脆弱性対応について明示的な定義や契約がない場合には、納品後の脆弱性対応について開発企業とユーザー企業側でトラブルが発生する可能性がある。納品時には既知の脆弱性が存在しないシステムであったとしても、のちに脆弱性が発見されることは当然発生しうる事態である。少なくてもユーザー企業との間で、脆弱性の扱いや開発企業側での対応範囲について明示的に合意しておくことが望ましい。また、脆弱性の対処にコード修正が必要な場合、現実的にはユーザー企業で脆弱性に対応できる割合は少ないと想定される。そのため、納品後に脆弱性が発見された場合に備え、別途有償の保守契約を結ぶなど、受託開発企業側で対応する場合に必要な体制を見越した契約をしておく方がよいだろう。

いずれの場合であっても、重大な脆弱性への対応とはいえ、サポート対象外となった製品バージョンへも修正パッチを準備することは、ソフトウェア開発企業にとっては負担となる他、サポート対象バージョン・製品への対応が遅れることになってユーザー全体への影響も大きい。サポート対象外のバージョンの利用顧客が多い、また極めて深刻な脆弱性である場合には、臨機応変に対応せざるを得ない場合もあるが、サポート対象バージョンへのアップデート依頼や、古いバージョンの使用不可推奨などで対処を終える判断も必要であろう。

製品の内容更新とともに、本来なら更新が必要な SBOM ファイルの扱いについては、明示的に契約書等で記載がない限り製品付属の readme など他の説明書や管理者ガイド等と同等の扱いとみなされる可能性が高い。特定バージョンリリースの際に SBOM ファイルを提供している場合には、脆弱性対応などでのパッチリリース時にも同様に SBOM が求められる可能性は高いと考えられる。特定の状況でのみ SBOM ファイルをリリース・提供するようにソフトウェア開発企業側で提供を制限する意図がある場合には、契約条項やサポート内容などにその旨が明示されるようにしておく方が、顧客との意図せぬトラブルを防ぐためにも望ましいと考えられる。

（8）NIST SSDF と脆弱性対応

NIST SSDF は、ソフトウェアのセキュア開発に関するフレームワークである。SSDF のうち、脆弱性または SBOM について言及されている内容から、本実証にも関連すると考えられる部分を下表にまと

めた。

表 1-55 本実証に関係する NIST SSDF の記載

項目	関連内容
PO 1.3	・ 「有償ソフトウェアの提供元と要求事項について話す」際の例として、「脆弱性情報の開示や、セキュリティインシデントへの対応能力セキュリティ関連の要件について触れられている。SBOM や VEX 情報の提供について、要件として追加することも考慮に入れる必要がある
PS 3.2	・ ソフトウェアのリリースごとに、すべてのコンポーネントの来歴情報を収集、保持し共有するという要件において、SBOM が例として挙げられている ・ ソフトウェアのリリースともに SBOM を生成し、またその SBOM データに対して改ざんや紛失等が発生しないような管理をすることも求められる
PW 4.4	・ 「無償・有償問わず、外部から取得したソフトウェアコンポーネントについて、組織で定義された要求に適合しているか検証する」という項目 ・ 例として「既知の脆弱性が残存しているかどうかを定期的に確認する」「使用しているコンポーネントが現在もアクティブに保守されているか、サポート終了を迎えていないかを確認する」が挙げられている。SCA ツールや SBOM の活用などに関連するものと想定 ・ 他にも、例えば実際に悪用事例のある（インシデントが観測されている）脆弱性の確認に関するポリシーなどを設定するなども含められると想定される
RV 1.1	・ ソフトウェアと使用している外部コンポーネントについて、サプライヤーや顧客、外部ソースなど様々なところから情報を取得し、信頼できるすべての脆弱性情報について調査を実施することが求められている ・ 本検証での「脆弱性特定」に当たる
RV 1.2	・ 過去検出されていない脆弱性がないか確認するため、レビューや解析、コードのテストなどを実施することが求められている ・ コード解析ツールの使用などの他、SBOM を用いた脆弱性特定などもこの対応と関連すると想定
RV 1.3	・ 脆弱性公開に関連するポリシー設定についての項目。本実証の「情報公開」で記載するような関係者の同定や、外部公開の内容の決定の他、公開プロセスの決定なども含まれると考えられる

SSDF の性質上、関連するのはソフトウェア開発企業に関するものに限られるものの、SBOM の作成や、本実証で検証した SBOM を活用した脆弱性特定と関連する部分が多く見られた。

（9）EU CRA と脆弱性対応

CRA では、ソフトウェア開発企業・ユーザー企業の両方において脆弱性や SBOM に関連する記述がある。今回の実証と関連する記述と、両企業で必要な対応を以下の表にまとめた。

表 1-56 EU CRA と SBOM

企業タイプ	内容
ソフトウェア開発企業	・ 関連ドキュメントは 5 年または製品の EOL のどちらか短い方の間は継続して更新される必要がある。SBOM も同様と考えられ、5 年 または EOL までの保管を念頭におく必要がある ・ 製品に含まれる脆弱性およびコンポーネントの情報を同定し、記録することが求められる。SBOM/VEX などが含まれると考えられる ・ 提供製品は、リリース時に既知の悪用されている脆弱性（Known exploitable vulnerability）がないものであることと指定されている。KEVC などを用いてインシデント事例のある脆弱性が含まれていないことを、必ず確認する必要がある。また、インシデント事例のある脆弱性を持つコンポーネントを含むものの、影響はないと判断されている場合には、SBOM に加えて VEX を用いてその情報を記述することが望ましいと考えられる ・ 修正した脆弱性について情報公開をすることが必要。脆弱性の説明、影響を受ける製品を同定するための情報、脆弱性の影響度ならびに深刻度と、ユーザーが脆弱性の緩和をするための助けとなる情報を含める必要がある ・ 脆弱性の報告窓口を設置する必要がある。外部からわかりやすいところに、報告窓口の情報を公開することが望ましい
ソフトウェアユーザ企業	・ SBOM が取得できる場合には、その場所を確認しておく ・ セキュリティ関連の情報を取得するための窓口や、方法をベンダーに事前に確認しておくことが望ましい

1.2.15 得られた成果の分析と整理

ソフトウェア開発企業・ユーザー企業のいずれに関しても、SBOM を活用することでソフトウェア内の脆弱性特定の自動化が可能であり、また複数の脆弱性 DB からの情報を目的に応じて組み合わせることで、コスト削減やリスクの削減が可能であることが確認できた（1.2.12（2）1））。一方、SBOM に含まれるコンポーネント情報と脆弱性 DB の情報を結びつけることにより、一定程度、脆弱性の特定が可能であることが確かめられたものの、脆弱性 DB と SBOM のマッチングには、双方で主に利用される部品 ID の違いや、登録情報との紐づけの困難さから、期待通りに動作しないケースがあることもわかった（1.2.12（1）3）a）。少なくても現状では有償 SCA ツールは追加費用は発生するが、そのようなツールを用いる場合の方が脆弱性の網羅性が高いケースも多いと推測され、ツールに一定の予算を確保でき

る場合には、まずはツールの導入を検討することが想定される。

脆弱性優先付けについては、ソフトウェア開発企業・ユーザー企業間で、判断材料として用いられる情報に共通項が見られた(1.2.12(2))。一方で、脆弱性に関する調査や判断には一定以上の知識や経験がないと対応が難しい部分も多くみられた。本実証で作成した、企業タイプおよび二段階のスキルレベルごとに判断方法を調整した脆弱性優先付け判断ツリーにより、企業の状況に応じた対応が可能となることを期待したい。ただし、優先付けについては一度に判定する脆弱性の量が多い場合に実施にかかる懸念がある。また、優先付けについては、深刻度、悪用可能性、インシデント有無などの情報から、最終的には人の判断が必要となると考えられるが、その判断に必要な情報の収集、一覧表示など可能な部分を自動化することで、効率化が図れると考えられる。すべて自動で判断するのは難しい部分であるが、VEX 情報の活用や、事前での情報整理などにより、作業効率の向上ができる余地はあると想定される(1.2.13)。

脆弱性に関する情報共有については、ソフトウェア開発企業においては、脆弱性を確認し、対応を判断するまでの社内コミュニケーションと、社外に対するコミュニケーションにおいてはステークホルダーなどに大きな違いがあることが明らかになった。また、現状は SBOM を用いた情報のやり取りは一般的ではないものの、ユーザー企業においては脆弱性に関する詳細で完璧な情報でなくても、まず情報が提供されることで透明性を確保することが、ベンダーに対する信頼感の醸成やのちの対応準備に役立つと考えられていることが分かった(2.1.2 (11) 3))。

脆弱性に関する修正については、根本対応を実施することが基本方針であり、インシデントの回避や、修正や検証にかかるコストなどの理由により、暫定対処をとることが多いことも確認された(1.2.12(4))。またユーザー企業にとっては、ソフトウェアベンダーから何らかの対処策が提供されない場合に、独自の判断をすることは難しい傾向があることも確かめられた。

中小企業での SBOM の活用や脆弱性対応については、情報システム専任者の不在や、スキルレベルなどの事情により、全般的に実施が困難となる可能性がある。実際にインシデントが報告されている脆弱性については、最低限迅速に対応を実施できるような情報、ならびに簡単に利用可能なツールが公開されることが望ましい。

1.3 調査結果の取りまとめ

第 1 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。

国内外の動向については、CISA、DOD、NSA などが従来の SBOM に関する基礎的な情報提供や意識啓発から進展して、SBOM の共有や VEX の活用などに関わる具体的な方法、部品 ID と脆弱性照合に関わる技術的な課題など踏み込んだ検討成果の報告が行われている点が注目される。米国以外においいても、オランダ、ドイツなどにおいて Cyber Resilience Act を背景として、SBOM の導入促進のための文書が発表されており、国際的な取組みに発展しっていることが確認できる。特に、1.1.1(1)にまとめた通り、各国の政府調達基準に SBOM の要件化が進められていることから、政府調達を契機として SBOM ツールや企業の対応人材など基盤が整うことで、他分野への普及、導入の効率化につながることが期待される。

実証においては、SBOM を活用した脆弱性管理の効率化に着目して、従来の脆弱性管理の課題を解決するための方法や手順を具体化について検討・整理した。ここで検討した結果は、SBOM 導入手引き Ver.2.0 として整理し、公開の手順を進めている。

脆弱性管理における SBOM の活用は、サプライチェーンを通じた部品の脆弱性の特定を効率化・迅速化する上で大きな効果が期待できる一方で、グローバルな部品 ID の統一化、脆弱性悪用可能性などの情報取得の観点で、大きな課題が残っており、社会的な基盤整備が求められることが確認された。課題について企業レベルで対応できること、未解決の課題などについて整理した。

2. ソフトウェアの利活用に係るセキュリティリスク、課題及び対応策の検討

本項目では、1 章での調査結果を踏まえ、自社製品・サービスの一部としてソフトウェアを利活用する際に生じるセキュリティリスクや課題、セキュリティリスクに対応するための取組について、調査を実施した。経済産業省と協議した上で、製品・サービスに OSS を活用する企業や、OSS を活用した製品・サービスを利用する企業、業界団体、OSS コミュニティ等をヒアリング対象として選定した。SBOM ツール・OSS の脆弱性対応における課題及びソフトウェアの利活用リスクに関する課題について、公開資料を基に文献調査を実施した上で、現状を整理し、課題・仮説を立てた上でヒアリング項目を作成し、ヒアリング調査を実施した。ヒアリング調査の概要を以下の通り示す。

表 2-1 ヒアリングの概要

カテゴリ	発表・議論内容を基に確認された主要な課題（抜粋）
ヒアリング対象	5 者 ・ SBOM ツールベンダー：1者 ・ 製品・サービスに OSS を活用するソフトウェアベンダー：2者 ・ クラウド、SBOM 関連ツール提供企業：1者 ・ OSS コミュニティ団体：1者
ヒアリング項目の概要	・ SBOM ツール・OSS の脆弱性対応における課題 ➢ SBOM ツールの入出力データについて ➢ SCA ツールと SBOM ツールの連携について ➢ 脆弱性情報の粒度について ➢ OSS の脆弱性対応について ➢ 部品 ID について ・ ソフトウェアの利活用リスクに関する課題 ➢ 利活用するソフトウェアのライセンス（GPLv3 等）に伴う課題 ➢ サプライチェーン上のサプライヤーとの連携 ➢ ソフトウェアのセキュリティリスクに対応するための企業内の体制 ➢ ソフトウェアの信頼性担保に求められる技術的課題

ヒアリング調査した結果を踏まえて、セキュリティリスクへの対応として有効性の高い取組を抽出し、取りまとめた。

SBOM ツール・OSS の脆弱性対応における課題については、ヒアリング項目ごとに想定課題を示した上で、その課題の実態を各企業において確認し、解決へのアプローチを検討することを目的に各企業に確認した。主にシステムベンダー2者、ツール提供事業者である1者、OSS コミュニティ団体1者を対象に課題の実態を確認した。

ソフトウェアの利活用リスクに関する課題については、主にシステムベンダー2者、事業者でツール提供もしている1者、SCA ツール提供企業1者にヒアリングを実施した。前者のシステムベンダーヒアリングでは企業における取組を確認し、有効性の高い取組を抽出して有効な施策としてまとめた。後者にお

いてはシステムベンダー等利用者への支援を確認した上で今後の課題を明確にし、その対応について検討した。

また、ソフトウェアの利活用リスクに関する課題については、必要に応じて近年のソフトウェア業界の動向を踏まえて、追加の文献調査を行った。

本項における調査において、「情報セキュリティ早期警戒パートナーシップ」をはじめとする IPA の取組等、これまでに実施されている対応策との関係を示し、さらに課題解決の方針を検討した。

2.1 脅威情報や脆弱性情報の情報共有体制・流通

脅威情報や脆弱性情報のデータベースに関しては、実証の中で調査を進め、1.2.12(1)1)として取りまとめている。ヒアリングや文献調査の結果より、以下のような課題と解決アプローチが確認できた。1点目の、SBOM の部品の粒度と脆弱性 DB の粒度があっていないため、脆弱性マッチング適切に実施できないという点が挙げられた。各企業からも同様の状況であることが確認でき、現状は脆弱性 DB の独自のデータベースがあるツールとの契約、自社で独自の部品粒度の脆弱性 DB の作成等で対応している。今後課題を解決する上では、SBOMの適切な部品粒度の特定と特定した部品粒度に合わせて脆弱性 DB も対応することである。SBOM の適切な部品粒度の特定方法としては、コストを大幅にかけることなく対応可能な範囲の部品粒度という観点で確認することが望まれる。例えば、ツールにおいて自動で特定可能な範囲や中小事業者においても確認可能な範囲などが考えられる。より細かな粒度で特定を目指す際には、個社での対応を行うという整理ができるとよい。

2つ目の課題については、OSS のバージョンの記載など OSS に関して全体のポリシーが構築できていないことが問題であることが確認できた。本課題の解決方針としては、信頼できる OSS を評価するためのポリシーを作成することが望まれる。OSS の信頼性をポリシーに沿って評価し、個社やソフトウェアの内容に応じて適切な OSS を利用するような環境が望まれる。そのためには、SBOM 管理の有無、メンテナンスの状況、バージョンの記載方法の統一化など複数の観点で評価できるポリシーを構築できるとよい。

表 2-2 脅威情報や脆弱性情報の情報共有体制・流通に関する課題と解決アプローチの整理

調査から確認できた課題	企業における意見	解決アプローチ
SBOMの部品の粒度と脆弱性 DB の粒度があっていないため、脆弱性マッチングが適切に実施できない。	・ 脆弱性 DB2 における部品の粒度が粗いことは問題視しているが、解決法はないと考えているので独自のデータベースを構築して解決している。 ・ SBOM における部品情報が DB より粒度が詳細な場合もあれば、逆もある。脆弱性の重要度にもよるが、現状は網羅的にすべてを確認している。	・ SBOM の適切な部品粒度の特定 SBOM の部品粒度をソフトウェアサプライチェーンで取り決めることが必要である。取り決める際は、部品を特定するためのコストやツールによって特定できる範囲などで検討することが望まれる。 ・ SBOM の部品粒度に合わせた脆弱性 DB の変更

調査から確認できた課題	企業における意見	解決アプローチ
	・ ある程度網羅的に検査してくれる無償ツールもあるが、各業界において必要な部品粒度を決めることが重要であり、その粒度で統一して SBOM を作成できる柔軟なツールが必要である。	SBOM における適切な部品粒度が確認できたうえで、公共の脆弱性 DB においても SBOM に適合するよう脆弱性に対応させる部品粒度を変更することが望まれる。
OSS のバージョンが統一でないことやポリシーが策定されていないため、OSS の脆弱性対応を行うことが難しい	・ Linux Foundation や Apache などは予算があるため、OSS が管理できているが、全体の OSS に関するポリシーがないのが問題だと考えている。 ・ コンポーネントの粒度が合わないことが問題だと考えているが、特にバージョンの記載が違うことを問題している。 ・ OSS が編集されているケースや、ディストリビューターが OSS を公開していないケースの場合、OSS を特定することが難しい。 ・ 今後、OSS は普通のソフトウェアと変わらない対応が行われると考えられ、脆弱性 DB に登録されているなど信頼できるソフトウェアのみが利用されるような世界になると考えられる。	・ 信頼できる OSS を評価するためのポリシーの作成 ソフトウェアにおいて信頼できる OSS を利用することが重要になっていることから、OSS の信頼性を評価できるようポリシー（SBOM 管理の有無、メンテナンスの状況、バージョンの記載方法の確立など）を策定することが望まれる。

2.2 利活用するソフトウェア、ソフトウェア部品の脆弱性管理

ソフトウェア、ソフトウェア部品における SBOM での脆弱性管理では、ソフトウェアを解析して部品情報を抽出する SCA ツールが必要である。SCA ツールにはパッケージマネージャーの構成情報とスニペット解析の 2 種類が存在する。パッケージマネージャーの構成情報の SCA ツールについては、Python の requirements.txt や Javascript の npm などが管理している情報を用いて部品情報を抽出する。スニペット解析の SCA ツールは、ソフトウェアのコードを解析して部品情報を抽出する。

調査によって確認できた課題として、SBOM で脆弱性対応やライセンス管理を行う上では、パッケージマネージャーによる SCA ツールでは情報が足りず、スニペット解析による SCA ツールが必要であるが、スニペット解析の精度や利便性が不足していることが挙げられた。各企業では、スニペット解析に加えて、手動で部品の確認を行うことで対応している。

この課題を解決する上では、スニペット解析の精度・利便性の向上とソフトウェア部品管理の意識の向上が望まれる。手動での確認は最小限とするために、スニペット解析の精度を向上させることが重要である。また、解析結果の透明性も手動での確認を減らす上では重要な観点である。加えて、SBOMでは広くスニペット解析が必要になることが想定されることから、中小企業においても簡易にスニペット解析ができる無償・安価なツールが必要である。

また、SCA ツールなどの自動化のみで全てに対応することは難しく、開発者のソフトウェア部品管理の意識が向上させることで、より解析がしやすいコードの構築や部品管理の情報の取りまとめなどが開発者で行われ、ツールでの自動化を補助できると考えられる。

表 2-3 利活用するソフトウェア、ソフトウェア部品の脆弱性管理に関する課題

調査から確認できた課題	企業における意見	解決アプローチ
SBOM においてスニペット解析ができる SCA ツールが必要だが、精度や利便性が足りない。	・ パッケージマネージャーによってコンポーネントの粒度が違う。 ・ 製造系のシステムは、独自コードでパッケージマネージャーが全く使われていないため、スニペット解析が必要である。 ・ スニペット解析においても現状の技術だと精度は足りない。 ・ パッケージマネージャーのみでは、OSS の持ち込みやディストリビューターが公開していない OSS を認識できない。スニペット解析を併用する必要がある。特にレガシーなソフトウェアほど懸念される。 ・ スニペット解析も完全に信じることはできないため、最終的には手動で確認している。 ・ パッケージマネージャーのコンポーネントの粒度は、セキュリティやライセンス管理が目的でないため、粒度は基本的には足りないと考えている。コード解析がより利用しやすい状況になる必要があることに加えて、ソフトウェアの部品管理の意識が開発者に必要であると考えている。	・ スニペット解析の精度・利便性の向上 手動での確認を最終手段としつつ、スニペット解析の精度を向上させることが重要である。また、中小企業などにおいてもスニペット解析が必要となるケースが多くなることが想定されることから、簡易にスニペット解析が実行できる無償・安価なツールに必要性である。 ・ ソフトウェアの部品管理の意識の向上 今後 SBOM をソフトウェアサプライチェーンで活用することを検討する際に、全てをパッケージマネージャーやスニペット解析で解決するだけでなく、開発者が部品管理を意識して、利用している部品を管理することが重要である。

2.3 利活用するソフトウェアのライセンス（GPLv3 等）に伴う課題

ソフトウェア利活用におけるライセンスリスクについて、経済産業省「令和 4 年度サイバー・フィジカル・セキュリティ対策促進事業 SBOM を導入・活用するサプライチェーンモデルの構築に向けた調査・実証事業報告書」第 5 章で挙げられた課題について、本調査ではシステムベンダーでの実態を確認し、有効な取組を抽出した。

表 2-4 利活用するソフトウェアのライセンス（GPLv3 等）に伴う課題への対応についての整理

課題・仮説	企業にヒアリング結果	有効な施策
OSS を含むライセンス管理等について、訴訟等の充分なリスクマネジメントが実施されていない。	・ SCA ツールは脆弱性管理等に用いる以前からライセンス管理のため導入してきた。 ・ ライセンスリスクに関して、教育プログラムを策定し、組織内で教育を実施している。 ・ 法務部門等の関係部門との連携を行い、GPL ライセンス混入を検出した場合にも適切に対処できる。 ・ 開発工程のフェーズごとにチェックを行うことにより、適切にライセンス管理することができる。 ・ M&A による被買収企業のソフトウェアライセンスについては事例を挙げることはできないが、工程管理や製品出荷の検証で確認できると考えている。	・ 開発工程において SCA ツールを導入してソフトウェア検証を行い、ライセンス管理を行う。 ・ ライセンスリスクに関する体系的教育プログラムを策定し、リスク発見時に適切な対処方法を含めて教育を実施し、組織全体に浸透させる。 ・ 法務部門と連携し、リスク検出した際に関係各所と速やかに連携できる仕組みを整備する。 ・ 開発フェーズごとに検証を行い、開発工程管理の中でソフトウェアライセンスリスクの検出を行う。 ・ M&A の際のデューデリジェンスにソフトウェアライセンスリスクへの対応を含めてビジネスプロセスを確立する。

ソフトウェア利活用に係るライセンスに関するリスクについて、ヒアリング企業のシステムベンダーにおいては GPL ライセンス等の混入によるリスクについてライセンス教育を実施していることが確認された。教育実施により、万一、開発工程において GPL ライセンスが混入した場合であっても、法務部門と連携し適切に対処できたことも確認できた。また、SCA ツールによる解析によって、GPL ライセンス混入のリスク検知に役立つことが確認された。企業の合併・買収（M&A）取引において、買収企業が被買収対象企業のソフトウェア等をレビューするプロセスについては今後の検討課題である。開発におけるフェーズごとにチェック機構があれば、対応は可能であると推測される。ヒアリング企業においては M&A 事例については確認できなかったが、M&A におけるソフトウェア取得におけるプロセスがあるとなおよい。ビジネスプロ

セスについては、OSS 管理の国際標準 ISO/IEC 5230:2020（OpenChain）[63]に基づいて、組織を整備することにより OSS ライセンス管理等コンプライアンス確立に役立つ。また、Linux Foundation は、M&A 取引について、[64]Ibrahim Haddad 氏による電子書籍「M＆A 取引におけるオープンソース監査 必須となるその基礎知識[65]」を公開している。同書は M&A におけるオープンソース監査の概要と実践方法やオープンソースコンプライアンスを強化するための基本指針が示されているため、M&A におけるソフトウェアデューデリジェンスの実務において参考となる。ライセンスリスクへの対応に限らないが、契約締結においては、係争する際の準拠法、管轄裁判所について確認して決定する必要がある。

IPA においては、オープンソースソフトウェア（OSS）の推進サイト[66]で、OSS に関する国内外の有益な情報を発信している。OSS ライセンスを理解するための参考情報として、主要な OSS ライセンスの特色や解説、ライセンス選択におけるガイドなどについて次の 2 つの文書を掲載している。

・GNU GPL v3 逐条解説書（2009 年 IPA 国立国会図書館によるアーカイブ）

・IoT 時代における OSS の利用と法的諸問題 Q&A 集（2018 年一般財団法人ソフトウェア情報センター）

上記資料にはライセンスリスクについても整理されている。今回の調査では、企業の実態をヒアリグ調査した上で具体的な取組を基に有効な解決策を提示した。経済産業省で公表している「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」に、今回調査した結果を基に OSS ライセンスリスクへの対応について追加記載し、広く周知を図ることも今後、検討が必要である。

2.4 サプライチェーン上のサプライヤーとの連携

表 2-5 利活用するソフトウェアのサプリチェーン上のサプライヤーとの連携の課題への対応についての整理

課題・仮説	企業にヒアリング結果	有効な施策
サプライチェーン間における脆弱性情報の特定と情報共有の分担が不明確であることにより、インシデント対応が迅速にできない。	・ The Secure Software Development Framework（SSDF）の考え方は一部の開発や業界団体で PoC のような取組を行っている。 ・ 契約において、開発委託先、委託元の責任関係を明確にし、合意形成を図り、委託先管理を行っている。 ・ クラウド利用においては、クラウド事業者の中には顧客がリージョン	・ 契約において、ソフトウェア開発における責任分界、責任関係を明確にし、合意形成を図る。（クラウド利用においては、責任共有モデルの概念に基づいて、クラウド事業者とクラウド利用者との責任関係を明確にする。） ・ クラウド利用の場合、データセンターのリージョンの場所、係

[63] OPEN CHAIN、Learn More About OpenChain ISO/IEC 5230:2020：
https://www.openchainproject.org/license-compliance
[64] Linux Foundation、M&A 取引におけるオープンソース監査：
https://www.linuxfoundation.jp/resources/open-source-audits-merger-acquisition-transactions/
[65] イブラヒム ハダド（Ibrahim Haddad）, Ph.D.「M＆A取引におけるオープンソース監査 必須となるその基礎知識」：
https://www.ibrahimatlinux.com/wp-content/uploads/2022/01/opensource-m_a-jp.pdf
[66] IPA.オープンソースソフトウェア（OSS）の推進：https://www.ipa.go.jp/digital/kaihatsu/oss.html

課題・仮説	企業にヒアリング結果	有効な施策
	を選択し、準拠法や管轄裁判所を選択できるようにしている。 ・ 脆弱性管理については、開発委託先と連携できるように契約内容に含めている。 ・ 開発委託先には委託元と同等レベルの教育を実施し、同水準でソフトウェア品質を担保している。 ・ サイバーセキュリティに係る情報共有の仕組みについても協力している。	争する際の準拠法、管轄裁判所に留意して決定する。 ・ ソフトウェアサプライチェーン全体に渡って同水準でセキュリティを担保できるよう、ソフトウェア開発に係る教育を開発委託元が委託先に実施する。 ・ 脆弱性管理については、委託先と連携できるように契約条項に含めて、対応内容についても明確にする。 ・ 脆弱性情報等について、既に構築されている情報共有の取組に官公庁等が公開しているガイドラインを基に対応について理解を深めて参画する。

ソフトウェア開発において委託元企業は、契約時に脆弱性対策の取扱いに関して、委託先と合意形成を図り、製品のライフサイクル全体において脆弱性管理を行う必要がある。脆弱性管理については、平成 29 年経済産業省告示第十九号[67]に基づく情報セキュリティ早期警戒パートナーシップの枠組みや、JPCERT コーディネーションセンター（JPCERT/CC）との連携、業界の ISAC 等に加盟し、情報共有に協力を行うなど、社会全体の情報セキュリティ対策活動の向上に貢献することが期待される。サプライチェーン上、特に最終ベンダーである委託元が委託先について同等レベルのソフトウェア開発、セキュリティ対策を確実に実施するため、委託元が委託先を適切に監督する必要がある。今回のヒアリング調査では、委託先に開発に係る教育を実施する等の工夫が確認できた。

ソフトウェア開発においてはソフトウェアサプライチェーン全体に渡って、開発委託元が同水準でリスクマネジメントする仕組みの構築が必要である。ソフトウェア開発を委託する場合、大規模開発においては多重請負となるケースもあり、契約を含めてサプライチェーンリスクに対応するための実質的なリスクマネジメントが必要である。ソフトウェア製品が出荷され顧客が利用し、顧客の下で管理・運用される際には、顧客と最終ベンダーとの連携も必要である。

IPA の取り組みでは、情報セキュリティ早期警戒パートナーシップ枠組みに関わる関係者の行動指針を、JPCERT/CC 及び一般社団法人電子情報技術産業協会（JEITA）、一般社団法人情報サービス産業協会（JISA）、一般社団法人ソフトウェア協会（SAJ）、及び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

[67] 平成 29 年経済産業省告示第 19 号：https://www.meti.go.jp/policy/netsecurity/vul_notification.pdf

（JNSA）とともに、「情報セキュリティ早期警戒パートナーシップガイドライン[68]」として策定、運用している。[69]同ガイドラインはソフトウェア製品及び Web アプリケーションに関する脆弱性関連情報の円滑な流通、および対策の普及を図ることを目的としている。セキュリティ担当者向けに情報セキュリティ早期警戒パートナーシップガイドラインの別冊等も作成されている。セキュリティ担当者がこうした公表資料を通じて理解を深めて、情報セキュリティ早期警戒パートナーシップ等に取り組みことで、より一層サプライチェーン全体でのセキュリティ対策が強化されることが期待される。

また、経済産業省・公正取引委員会では、令和 4 年 10 月 28 日サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて[70]」において、サプライチェーンリスクにおけるセキュリティ対策に関する考え方を公表した。公正取引委員会のサイト[71]において近年、企業から中小企業までを含むサプライチェーン上の弱点を狙ったサイバー攻撃が顕在化・高度化している。企業への攻撃原因の一つに情報システムのサプライチェーンや商流上において、機器等の脆弱性が放置されることにより、その弱点を突かれた攻撃が発生していることを挙げている。サプライチェーンにおけるビジネスパートナー、特に中小企業等の対策が不十分な場合、当該企業の事業活動に支障をきたすだけでなく、また自社が提供した重要な情報が流出してしまうおそれや、当該企業を踏み台にして自社が攻撃されるおそれなどを挙げている。こうした背景を踏まえて発注者が取引先に対するサイバーセキュリティ対策の支援・要請に関する考え方が示されている。発注者が取引先へのサイバーセキュリティ対策を要請するに当たり、一定のサイバーセキュリティ対策の実施を取引の条件とすることや、一定のサイバーセキュリティ対策の実施を要求することついて、独占禁止法上の優越的地位の濫用や下請法上問題とならないか懸念される。そのため取引先への対策の支援・要請について Q&A 方式で整理され、公開されている。発注者は、この考え方を参考とし、取引先のサイバーセキュリティ対策の強化を促しつつ、サプライチェーン全体で付加価値の向上に取り組み、取引先とのパートナーシップの構築する必要がある。

2.5 ソフトウェアのセキュリティリスクに対応するための企業内の体制

表 2-6 利活用するソフトウェアソフトウェアのセキュリティリスクへの企業における対応の整理

課題・仮説	企業ヒアリング結果	有効な施策
開発部署、品質保証、調達部門等の開発段階及び、PSIRT、CSIRT 等の組織間情報連携が未成熟でインシデント対応の高度化ができていない。	・ セキュリティ統括、品質管理部門、法務部門、監査部門、CSIRT、PSIRT 等を設置し、役割や権限について明確にしている。 ・ セキュリティに係る予算を確保し、関係部署に適切な費用、人員等のリソース資源配分を行っている。	・ 組織体制について、セキュリティ統括、品質保証部門、法務部門、監査部門等 CSIRT、PSIRT を設置し、役割や権限について、役割や権限を規定する。

[68] IPA、情報セキュリティ早期警戒パートナーシップガイドライン：
https://www.ipa.go.jp/security/guide/vuln/partnership_guide.html
[69] JPCERT/CC、脆弱性対策情：https://www.jpcert.or.jp/vh/top.html
[70] 経済産業省・公正取引委員会サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて：https://www.meti.go.jp/policy/netsecurity/hontai_1028.pdfl
[71] 公正取引委員会、サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて：
https://www.jftc.go.jp/dk/guideline/unyoukijun/cyber_security.html

課題・仮説	企業ヒアリング結果	有効な施策
	・ クラウド事業者が主体となり、全社横断型クラウド活用推進組織（CCoE; Cloud Centre of Excellence）について提唱している。 ・ 大手企業グループでは、単体だけでなく、グループ全体共通の開発ガイドラインを策定している。 ・ 開発ガイドラインに基づいて開発全体に渡って工程管理を行っている。 ・ 開発フェーズごとにレビューを行い、役割や権限に応じて各関係部署より適切な検証を実施している。	・ 経営層がセキュリティ対策を経営課題として認識し、適切な経営資源の配分を検討する。 ・ 組織内の関係各所と連携が図れるように仕組みを構築する。 ・ クラウド利用については、全社横断型クラウド活用推進組織（CCoE; Cloud Centre of Excellence）の構築を検討する。 ・ ソフトウェアライフル全体に渡ってリスクマネジメントする仕組みを構築する。 ・ セキュリティポリシーの他に、ソフトウェア開発に係るガイドラインを策定し、組織全体に標準化された開発工程管理を明確にする。 ・ ソフトウェア開発においては、開発フェーズごとにレビューを行い、関係部署の役割と権限応じて適切なチェックを行う。

企業内の体制ではグループを持つ大手業の場合には、グループ全体で標準化されたガイドラインを策定し、それに則って開発工程を管理する。開発フェーズごとにチェックポイントを設けて、各工程が適切に管理できているかを検証する仕組みも有効である。また、ソフトウェア開発に係る企業内の体制については、開発部門、品質保証部門、監査部門、セキュリティ統括機能を持った組織が各組織の役割や権限を明確にした上でレビューするチェック機構を有することが望ましいと確認できた。クラウド利用においては、近年、「クラウド活用推進組織（CCoE; Cloud Centre of Excellence）」の構築が注目されている。クラウド事業者は、CCoE の概念等について、サイト上に公表[72][73][74]している。また既に CCoE の組織を組成している企業において、その組織における CCoE の位置づけや考え方、組織機能等について公開している。クラウド戦略を立案し、実行するために必要な知見や経験を持つ人材や経営資源を集中させている。CCoE 構

[72] Microsoft、クラウドのセンター オブ エクセレンス（CCoE）機能：https://learn.microsoft.com/ja-jp/azure/cloud-adoption-framework/organize/cloud-center-of-excellence
[73] Google、Google Cloud Japan が CCoE（Cloud Center of Excellence）研究分科会を発足：https://cloud.google.com/blog/ja/products/gcp/ccoecloud-center-excellence
[74] AWS，今から始める CCoE、3 つの環境条件と 3 つの心構えとは：https://aws.amazon.com/jp/blogs/news/how-to-get-started-your-own-ccoe/

築によりクラウド利用のベネフィットを享受する方策について示されているため、CCoE 構築を検討している企業には参考になる。

IPA 等の取り組みとの関係では、2023 年 3 月に経済産業省と IPA が発行した「サイバーセキュリティ経営ガイドライン Ver3.0（以下、経営ガイドライン）」の指示 2 サイバーセキュリティリスク管理体制の構築に示されている。また、IPA では、「共通フレーム 2013[75]」を公開しており、ソフトウェアライフサイクルプロセスの国際規格等に対応して策定されている。「共通フレーム」の目的と意義は、システムやソフトウェアの構想から企画、開発、運用、保守、廃棄に至るまでのライフサイクル全般にわたって、必要な作業内容を包括的に規定し、そしてソフトウェア、システム、サービスに関わるベンダー（供給者やユーザ（取得者）などの人々が“同じ言葉”で話すことができる共通の枠組みを提供することにある。今回のヒアリング調査では、企業における開発の実態を踏まえて、ソフトウェア開発におけるセキュリティ体制、開発工程管理におけるリスクマネジメントを基に具体的な施策を確認できた。

インシデント対応においては、PSIRT（Product Security Incident Response Team）、CSIRT（Computer Security Incident Response Team）の構築し、関係組織と連携できるような仕組みを整備した上で、セキュリティ事案が生じた際には迅速な連携が可能になるように組織運営する必要がある。

経営ガイドラインの指示 7 インシデント発生時の緊急対応体制の整備においても示されている。また、IPA サイトにおいて「サイバーセキュリティ経営ガイドライン Ver 3.0 実践のためのプラクティス集[76]」も公開され、経営ガイドライン「重要 10 項目」の実践に必要な事例が掲載している。今回のヒアリング調査では、ソフトウェアを開発する上での企業における具体的な取組を確認することができた。

2.6 ソフトウェアの信頼性担保に求められる技術的課題

表 2-7 ソフトウェアの信頼性担保に求められる技術的課題についての対応整理

課題・仮説	企業ヒアリング結果	有効な施策
ソフトウェア構成管理による部品の来歴及び責任関係が不明であることにより、リスクについて充分に把握されていない。	・ ソフトウェア品質の検証の際に、セキュリティ要件も含めて検証する。 ・ SCA ツール検証で検出漏れ、誤検知がある場合、手動で精査する。 ・ SCA ツール検証における誤検知については、脆弱性に関する説明がもとめられるため、精査が必要となる。 ・ ツールによる誤検知については、ツール提供企業において改善の	・ SCA ツール検証では検出漏れ、誤検知もあり、不十分なため、手動による精査を組み合わせる。 ・ SCA ツールによる誤検知については、検証した結果を踏まえてツールベンダーに報告し、改善を提案する。 ・ ソフトウェア透明性確保のため、SBOM を作成・提示する際にリスク評価に応じて、精査

[75] IPA、SEC Book「共通フレーム」：https://www.ipa.go.jp/publish/secbooks20130304.html
[76] IPA、https://www.ipa.go.jp/security/economics/csm-practice.html ：https://www.ipa.go.jp/security/economics/csm-practice.html

課題・仮説	企業ヒアリング結果	有効な施策
	機会となっており、顧客にはレポート報告を行う。	のレベルを見極め、費用対効果を考慮する。 ・ 顧客との契約時に SBOM について契約条項に含め、要求事項を明確にする。

最終ベンダーと顧客との契約においては、規制が厳格化されつつある医療機器分野、自動車分野においては、顧客から SBOM を要求される場合がある。セキュリティ要件は品質マネジメントの一環としてレビューされるため、品質マネジメントのコンテクストの中でソフトウェア透明性を確保することにより、説明責任を果たし、ソフトウェア信頼性が担保できるようになる。ソフトウェア品質について、顧客に説明する際には SBOM 必要に応じて提示する。

SBOM は、プロセス全体の品質確保に係る多くのプロセスに関係し、特に、調達、構成管理、脆弱性、品質管理など外部調達(サプライチェーン)に係るプロセスにおいて重要な手段となる。SBOM が関係するプロセスについて、以下図に示す。

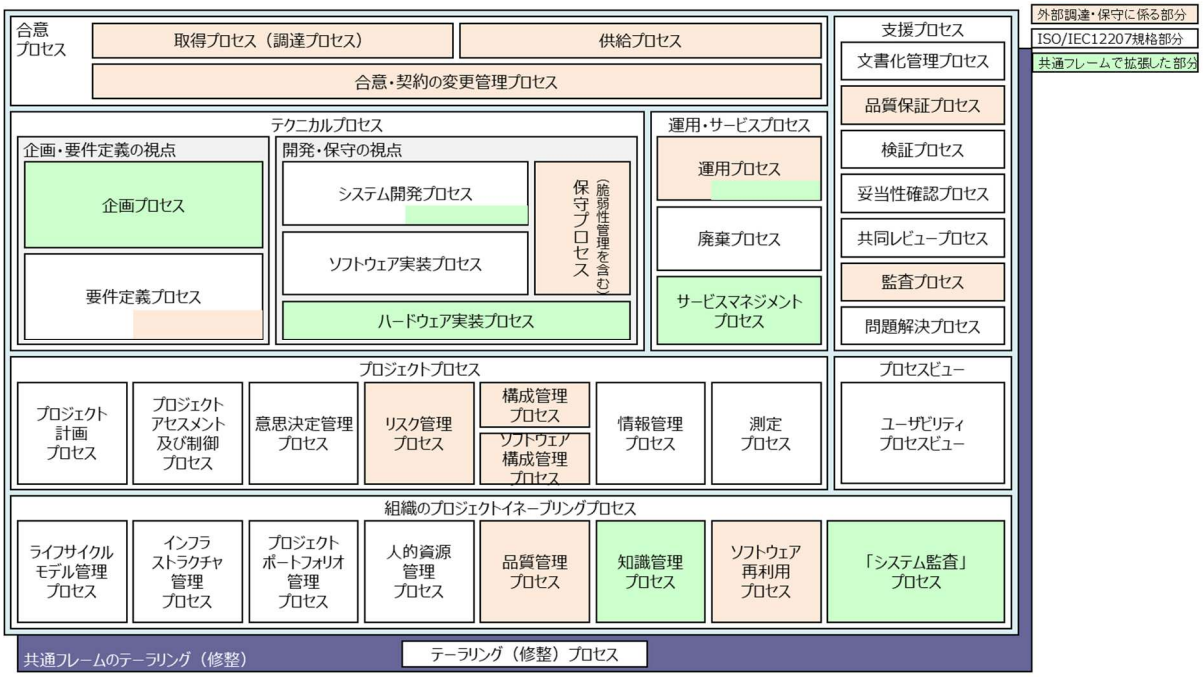


図 2-1 共通フレーム 2013 における SBOM が関係するプロセス

(出所)共通フレーム 2013 の概説「共通フレーム 2013 のプロセス体系」[77]に基づき株式会社三菱総合研究所にて加筆し作成

2.6.1 クラウド事業者が提供するツールの紹介

本節では顧客がクラウド利用してシステム構築を行う顧客の構築環境を検証するツールに一部 SCA 機能が提供されているため、ツールについて紹介する。近年、ソリューションや追加機能がリリースされている。2024 年 3 月時点で確認した公開サイトの情報を基に 3 つのツールの概要等について、抜粋、引用して紹

[77] IPA、共通フレーム2013の概説:https://www.ipa.go.jp/archive/files/000027415.pdf

介する。英語資料等については、邦訳を行っている。いずれのツール、及びツール機能にういては、リリースから間もないため、機能検証が充分に実施されていないことに留意する必要がある。

Microsoft は 2022 年 7 月 SBOM 生成ツール「sbom-tool[78]」をオープンソースとして公開した[79]。2021 年の米国大統領令においても SBOM は重要な要件として挙げられており、SBOM は、ソフトウェアコンポーネントの構成を示すリストであり、組織がサプライチェーンの依存関係を洞察できるようにソフトウェアの透明性を提供する。Microsoft が公開したツールによって生成される SBOM には、SPDX 仕様に基づく 4 つの主要な要素が含まれる。

1. ドキュメント作成情報：ソフトウェア名、SPDX ライセンス、SPDX バージョン、ドキュメントの作成者、作成日など、SBOM ドキュメントに関する一般的な情報。

2. ファイルセクション： ソフトウェアを構成するファイルのリスト。各ファイルには、内容のハッシュ（SHA-1、SHA-256）などのプロパティがある。

3. Packages セクション：ソフトウェアをビルドするときに使用するパッケージのリスト。各パッケージには、名前、バージョン、サプライヤー、ハッシュ（SHA-1、SHA-256）、パッケージ URL（purl）ソフトウェア識別子などのプロパティがされている追加。

4. 関係セクション： ファイルやパッケージなど、SBOM の様々な要素間の関係のリスト。完全な依存関係ツリーをキャプチャするために、他の SBOM ドキュメントを参照することもできる。以下に示すように、SBOM ドキュメントへの依存性参照、または後続のビルドに消費される先行ビルドからの SBOM ドキュメントを含めるための重要な機能である。

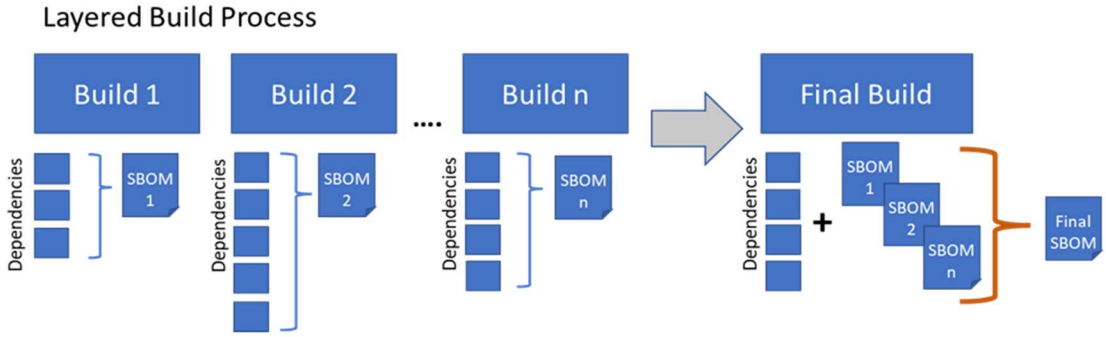


図 2-2 MicrosoftSBOM ツールの Layred Build Proses

（出所）Microsoft、Microsoft open sources its software bill of materials (SBOM) generation tool[80]より引用

Amazon Inspector[81]は、ソフトウェアの脆弱性や意図しないネットワークのエクスポージャーがないか継続的に AWS ワークロードをスキャンする自動脆弱性管理サービスである。仕組みについては、以下に概要図を示す。

[78] Microsoft、sbom-tool：https:/：/github.com/microsoft/sbom-tool
[79] https://devblogs.microsoft.com/engineering-at-microsoft/microsoft-open-sources-software-bill-of-materials-sbom-generation-tool/
[80] Microsoft、Microsoft open sources its software bill of materials (SBOM) generation tool：https://devblogs.microsoft.com/engineering-at-microsoft/microsoft-open-sources-software-bill-of-materials-sbom-generation-tool/
[81] Amazon Inspector：https://aws.amazon.com/jp/inspector/

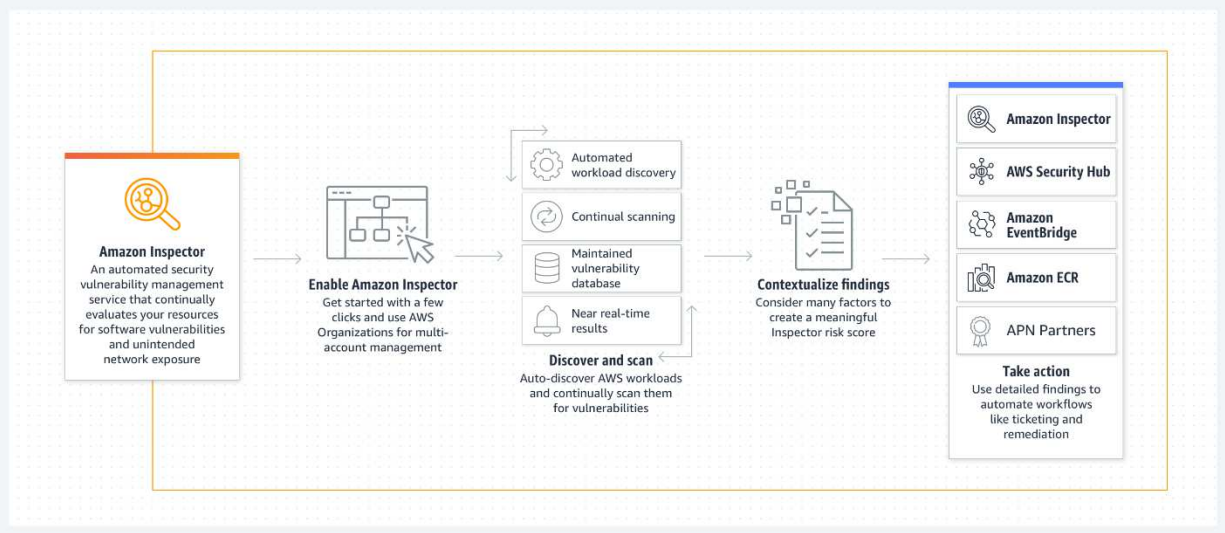


図 2-3 Amazon Inspector の仕組み

（出所）AWS、Amazon Inspector サイトより引用

AWS Inspector は既にリリースされていたツールであるが、2023 年 6 月に AWS re:Inforce 2023 で、新機能である「SBOM Export[82]」が発表された。Amazon Inspector コンソールまたは API を使用し、リソースの SBOM を生成することができる。SBOM の生成対象は、コードベースに含まれるすべてのオープンソースソフトウェアコンポーネントとサードパーティソフトウェアコンポーネントのネストされたインベントリーである。Amazon Inspector は、環境内の個々のリソースについて SBOM を提供する。Amazon Inspector からエクスポートされた SBOM は、最も一般的に使用されているパッケージや組織全体の関連する脆弱性など、ソフトウェアサプライに関する情報を可視化するのに役立つ。Amazon Inspector では、CycloneDX 1.4 および SPDX2.3 互換フォーマットでの SBOM のエクスポートをサポートしている。

Google は 2022 年 10 月、Google Security Blog「Announcing GUAC, a great pairing with SLSA (and SBOM)![83]」の投稿において、ソフトウェアサプライチェーンの安全性を確保するため、オープンソースプロジェクトを立ち上げた。2023 年 5 月に Google のオープンソースセキュリティ・チームは、セキュリティ専門家向けに設計されたツール Graph for Understanding Artifact v0.1（以下、「GUAC」という。）を発表した[84]。GUAC は、ソフトウェアサプライチェーンのセキュリティについて、指示された実用的な洞察を提供することにより、開発者とセキュリティチームを支援する。近年、ソフトウェア攻撃の頻発とオープンソースツールの使用増加により、ソフトウェアサプライチェーンの完全性とセキュリティに対する信頼性が著しく低下している。こうした状況に対応するため、GUAC は、ソフトウェアで何が起きているか信頼できる情報源となることで、この問題に対応する。GUAC は、開発者とセキュリティチーム間の情報ギャップを解消し、ソフトウェアの知識ギャップ、コンプライアンス、脅威の検出に関する共通の理解を提供する。GUAC Doc[85]によれば、ソフトウェア・サプライチェーンのセキュリティ状況について、整理された実用的な洞察を提供する。GUAC は、SBOM 等のソフト

[82] Amazon Inspector による SBOM のエクスポート
https://docs.aws.amazon.com/ja_jp/inspector/latest/user/sbom-export.html
[83] https://security.googleblog.com/2022/10/announcing-guac-great-pairing-with-slsa.html
[84] https://security.googleblog.com/2023/05/announcing-launch-of-guac-v01.html
[85] GUAC doc：https://docs.guac.sh/

ウェア・セキュリティ・メタデータを取り込み、ソフトウェア間の関係をマップ化することで、ソフトウェア・セキュリティのポジションを完全に理解できるようにする。GUAC を使用することで、監査、ポリシー、リスク管理、さらには開発者支援など、より高いレベルの組織的成果を推進することができるとしている。GUAC の詳細は、公開されている GitHub[86]で確認することができる。GUAC の機能については、以下に概要図を示す。

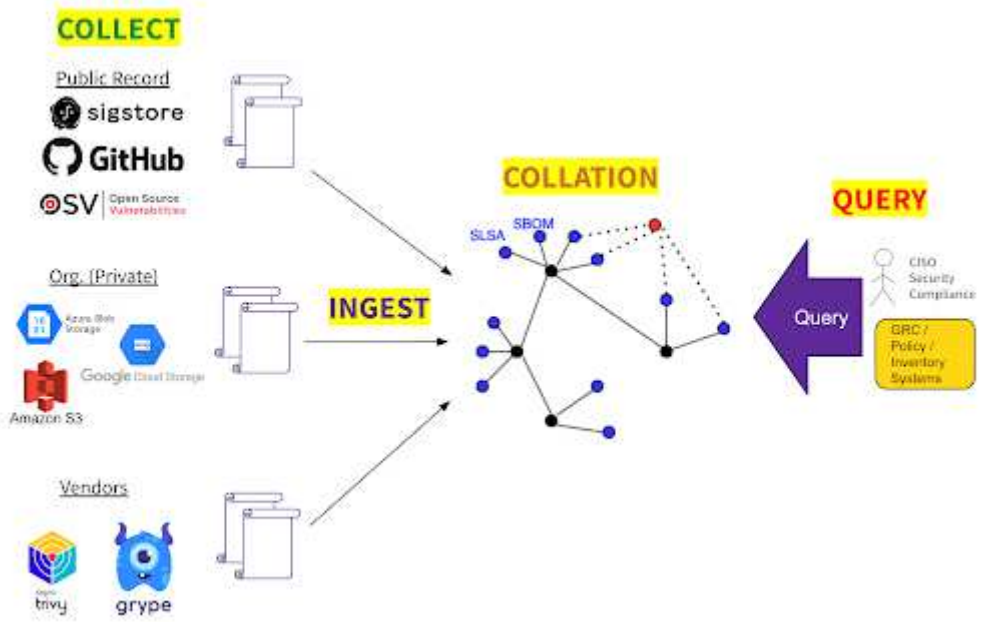


図 2-4 How GUAC works

（出所）Google Security Blog、GUAC doc より引用

GUAC のコミュニティ[87]に立ち上げられており、GUAC について詳細を知りたい場合、GUAC コミュニティの参加及び GUAC のサイト[88]から詳細な情報が入手できる。OpenSSF、SLSA、SPDX、CycloneDX などによるグループにおけるコミュニティの協力により、組織は以下のものにアクセスできるようになっている。

・ソフトウェア部品表（SBOM）（SPDX-SBOM-Generator、Syft、kubernetes bom ツールによる）

・ソフトウェアがどのようにビルドされたかを示す署名入りの証明書（SLSA3 GitHub Actions Builder を使った SLSA、Google Cloud Build など）

・エコシステム全体の情報を集約し、脆弱性をより発見しやすく、アクションを起こしやすくする脆弱性データベース（OSV.dev、Global Security Database（GSD）など）

本節で取り上げた SBOM 関連ツールについては、ツール提供を行う企業からの資料公開、ブログでの発信、動画等による情報提供等が行われている。SBOM 関連ツールの利用が進むに連れて技術者による技術的な検証も進む。実際に、ツールを利用した結果について Web 上に公開しているケースが確認できる。ツール提供を行うクラウド事業者が主体となっている技術コミュニティでの活発な意見交換によって、今後、技術文書の拡充や利用する企業事例の公表が行われることも想定される。技術

[86] guacsec/guacPublic ：GitHub - guacsec/guac: GUAC aggregates software security metadata into a high fidelity graph database.
[87] GUAC Community：https://guac.sh/community/
[88] GUAC：https://guac.sh/

者をはじめとするユーザーのツール利用によって、ツールが抱える課題が明らかになり、今後、ツールの機能改善、機能拡充も見込まれる。ソフトウェア開発企業とツール提供企業等、コミュニティでの活発な意見交換により、よりよいツールやソリューションの提供に繋がること期待される。

2.7 利活用するソフトウェアの安全性を認証するための認証機関の必要性

ISO/IEC 17000(JIS Q 17000)の定義によれば、認証とは「製品、プロセス、システムまたは要員に関する第三者証明」のことである。証明の方法には、認証に位置付けられる第三者証明の他、第 1 者証明や第二者証明も存在する。ソフトウェアに対する安全性の評価を考えたとき、ソフトウェアベンダー自身が安全性を証明する方式が第 1 者証明、ソフトウェアが提供される先の調達者や利用者が安全性を証明する方式が第二者証明となる。そして、第三者の認証機関が安全性を証明する方式が第三者証明、すなわち認証となる。一般的に、第 1 者証明より、第三者証明の方が、証明に要する費用が高価となる。一方で、第 1 者証明や第二者証明の場合、コストを抑えるために評価が甘くなるという品質不正問題やデータ改ざん問題もあり、証明の信頼性を求める場合には、認証機関による第三者証明が必要となる。

ソフトウェアの安全性に関する認証制度として代表的な制度は ISO/IEC 15408 に基づく Common Criteria(CC)である。CC は、ソフトウェアに限らず IT 関連製品のセキュリティ機能の適切性・確実性を評価機関が評価し、その評価結果を認証機関が認証する制度である。CC 認証は国際的承認アレンジメント加盟国(CCRA 加盟国)でも通用するが、国内での認証取得製品数は限定的であり、認証取得に要するコスト・期間が非常に高価・長期間である点が課題[89]である。

ソフトウェアの安全性を証明する方法として、すべてのソフトウェアに第三者証明(＝認証)を求めることは費用対効果の観点から現実的ではない。上記のとおり、認証取得には高コスト・長期間を要することが一般的であるため、認証機関による認証を求めた場合、ソフトウェアに関する産業競争力が著しく低下するおそれがある。事実、米国連邦政府調達の対象ソフトウェアについては、OMB 覚書(M-22-18 及び M-23-16)に基づき、ソフトウェアベンダーによる SSDF の自己適合宣言が求められるが、認証ではなく第 1 者証明の方式を取っている。EU のサイバーレジリエンス法においても、多くの製品が自己適合宣言(第 1 者証明)で対応可能な見込みである。

一方で、一部のソフトウェアについてのみ認証を求めていく方針は想定される。例えば、EU のサイバーレジリエンス法においては、法律の対象となる「デジタル製品」のうちリスクが高い「重要なデジタル製品」は、認証取得が必須となる。また、2024 年 3 月に欧州議会で可決した EU-AI 法[90]においても、ハイリスクな AI のうち、生体認証に使用される AI システム等は第三者機関による評価が必須となる。いずれの制度においてもリスクベースのアプローチを取っていることが重要であり、国内においてソフトウェア製品に関する認証制度を検討する場合も、対象ソフトウェアのリスクを踏まえた検討が必要である。また、その際の認証機関の在り方について、国際的な整合性を考慮した検討が必要である。

---

[89] 評価保証レベル(EAL)にも依存するが、認証費用について、EAL2:1,000 万～2,000 万円、EAL3:1,600 万～2,700 万円、EAL4:4,000 万～1 億円程度となる。また、認証取得にかかる期間について、EAL2:最短 4～6 か月、EAL3:6～9 ヶ月程度、EAL4:12～24 ヶ月程度となる。

[90] https://artificialintelligenceact.eu/

3. ソフトウェアタスクフォースの運営

本項目では、上記 1、2 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、1、2 の調査・実証を踏まえ、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。

3.1 全体スケジュール

3.2 第 10 回ソフトウェアタスクフォース

3.2.1 開催概要

第 10 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 5 年 7 月 18 日 14:00～16:00
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（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（案）

3.2.2 要旨

当日は、SBOM の導入手引案に関するパブリックコメント対応結果について、対応モデル案について、今年度の実証方針等について、QUAD における共同原則等を踏まえ今後取り組むべき事項の 4 点について議論が行われた。下記に議事要旨を示す。

・ SBOM の導入手引案に関するパブリックコメント対応結果について

- パブコメ対応結果の通り、SBOM が部品表としてライブラリ管理や機械学習における学習モデルの管理などに利用されることも期待されている。CycloneDX においては、ML-BOM や SaaSBOM の取組が紹介されており、今後、SBOM 以外の BOM についても必要に応じて追記し、手引案が示している SBOM の対象を明確化できるとよい。
- 手引案については、今後も必要に応じて定期的にパブリックコメントを実施し、内容を更新していくとよい。

・ 対応モデル案について

- 対応モデル案については、SBOM の管理単位や更新のタイミングを検討できるとよい。ソフトウェアの多くは階層化されているため、ソフトウェア内で複数の SBOM を 1 ファイルとしてまとめずに管理することが想定され、SBOM の内容が更新されるたびに差し替えを行う必要があると考える。そのため、製品全体の SBOM を最新化する方法についてもモデルとして可視化できるとよい。
- SBOM 対応モデル案を利用することで、SBOM の対応状況が可視化されると考える。一方、IoT 機器等の組み込み機器の利用が多い制御分野や重要インフラ分野等の特定分野については可視化が難しい事例が存在すると考える。例えば、約 5 年前に公表された WPA2 関連の脆弱性のケースについては、特に制御分野において、契約状況によ って は脆弱性対応が実施されない事例等が確認された。
- CSSC において議論されたビル分野の事例では、個人事業主が利用する Windows95 が多く残存している状況にあるが、制御分野は事業を停止することができないため、迅速な脆弱性対応が難しい事例が存在する。
- これらの事例を踏まえると、特定分野については、SBOM 対応状況の可視化が難しい側面があると考える。加えて、情報管理の観点から、可視化された情報に関する取扱いには、分野ごとに配慮が必要である。
- SBOM の導入手引案で記載の VEX の他に、大統領令を基に CISA・NIST が脆弱性開示プログラムである VDR について公表している。自動化が難しい箇所においては、VDR の利用も考えられるため、検討いただけるとよい。米国を含め、現状では自動化に向けた技術発展途上であるため、SBOM の活用を完全の自動化には時間がかかると考える。それまでの対応として、既存技術も組み合わせながら SBOM の対応方法を検討する必要がある。
- 日本国内で SBOM の利用を促進する方策について、検討できるとよい。例えば、政府統一基準等含め、政府調達に関して SBOM を利用することなども検討できるとよいのではないか。また、ソフトウェアを調達している SIer にどう浸透させるとよいか、インセンティブとペナルティの両面が検討できるとよい。
- SBOM 利用のインセンティブを検討することが重要であるが、そのためには、米国等の政府調達要件の事例を参考に検討するとよい。特に、ヘルスケアや自動車等の分野では、規制を基に SBOM の活用が広まり、米国では政府が SBOM の導入を求めたことで、事業者への普及が進んでいる状況があるため、そのような事例を参考に検討できるとよい。
- 製品ベンダーによって脆弱性の対応に違いがある状況においては、SBOM や VEX によって対応の違いが可視化されると考える。例えば、SBOM や VEX と、脆弱性 DB2 や

JVN に登録されている脆弱性を対応づけすることを想定した場合、製品ベンダーは全ての脆弱性を脆弱性 DB2 や JVN に登録せず、独自のリリースノートなどで対応している場合もあるため、今後、全ての脆弱性を登録し SBOM で完結する方針なのか、独自のリリースノートなども対応として許容するのかなどを検討する必要がある。

- ソフトウェアベンダー等のソフトウェア開発事業者だけでなく、システムを構築する事業者に対しても啓発が必要である。そのような事業者は、外部のソフトウェア等を利用して構築することが多く、SBOM の活用を理解する必要があると考える。また、SBOM は脆弱性管理だけでなく、ソフトウェア構成管理という点でも重要であり、両面の観点から SBOM 利用に関して検討できるとよい。
- SaaSBOM がクラウドの BOM として検討されており、BOM という広い枠組みにおいては、SBOM 含め利用すべき BOM の検討が必要である。
- RSA カンファレンスや SBOM-a-Rama 等において、日本の規制状況について関心が寄せられているため、規制化を検討する場合には、SBOM 対応モデル案を利用し、現実的なレベルに調整できるとよい。米国は、脆弱性が 脆弱性 DB2 へ
- 登録されていない場合、CPE が割り当てられないという状況について課題認識し、解決するための方針を検討している。
- ソフトウェアのパッケージ運用・管理が SBOM の活用においても課題だと考える。製品としてのソフトウェアを Windows やクラウド環境で利用する場合、Linux 系と同じくパッケージ管理されたソフトウェアをインストールするというアプローチの普及がポイントになると考える。さらに、システムインテグレーションで開発した場合にも、同様な取り扱いができるようにするため、パッケージ管理をどうするべきか等を含めた運用管理の観点からも検討できるとよい。
- 製品ベンダーからの情報発信と JVN 等の公的な DB からの情報発信の役割を分けて考えた方が良い。理想は、製品ベンダーからの情報発信のみでしかも自動化前提であるが、現実的に難しい。民間ではなかなか対応できない領域は常に存在するので、その領域を公的な DB が部分的にでも代行し対応できるとよいと考える。例えば、影響の大きい、あるいは、良く利用されているソフトウェアについては、自動化を含めた詳細な情報発信を先導するというのは、その一例になると考える。
- 海外の SBOM 活用アプローチについて、ヘルスケアや自動車等の規制がかけられている分野で求められる対応を整理できるとよい。日本の JVN の取組は 脆弱性 DB2 を参考に同様の仕組みを構築している。SBOM 活用についても米国と日本で強制力の差はあっても、分野ごとの規制の状況はあまり変わらないことから、米国の規制の対応状況を整理できると、同様の仕組みを構築している JVN の取組に順次取り込みつつ、連携することもできるのではないか。
- 対応モデル案の普及の観点では、制度全体の方針を誰が決め、責任をもって推進するかという点について検討するよい。制度というのは、SBOM や脆弱性情報の活用・共有における全体の仕組みを示しており、責任というのは、他者から侵されないという権利と資金を示していると考える。米国では、大統領令を基に実施しているが、日本においてはどの機関が責任を持って実施するかが重要である。また、機能や要件を設定する責任を明確にし、責

任を担う場合は何を実施する必要があるかを検討する必要がある。さらに、各プレイヤーの責任に関する点についても検討できるとよいのではないか。利用者が複数の開発者からSBOM を納品し、利用者が SBOM を利用する際にミスが発覚した場合どう対応するか等含め検討する必要がある。また、SBOM の免責についても検討する必要がある。完璧な制度は難しいが、完璧ではない部分の責任をどうするかなどを検討する必要がある。購入者が求められる脆弱性強度との対応の責任を誰が持つかなども重要と考える。

- 利用者が複数開発社から SBOM を納品する場合、複数事業者分の責任を商品に重ねることになるため、コストは増加すると考える。このため、社会インフラとして運用できるコスト負担の仕組みを検討することが重要である。今後、実際に制度を動かす上で、責任・免責の範囲、コストの問題、制度の強制・任意を検討することが重要である。
- SBOM は脆弱性管理で利用したいというのが主目的の一つであると考える。脆弱性修正やパッチ適用の時間を減らせることが大きなメリットと考える。これらのメリットを享受する上で、機械処理できないことが 1 つの課題と考える。そのため、国や政府において、SBOM に関して誰が先頭に立ち、予算や責任を持って実施するかは、明確にすることが重要である。

・ 今年度の実証方針等について

- 今年度の実証項目として、責任や費用の観点からも検討するとよい。
- SBOM の対応ツールついては、複数のツールで検証することも検討できるとよいのではないか。
- SBOM の脆弱性管理において、脆弱性 DB2 とのマッチングにより脆弱性が発見された場合、脆弱性の発動の有無を検討する必要がある。その場合、脆弱性 DB2 や JVN の突合のタイミングの検討が必要だと考える。脆弱性 DB2 や JVN 等のデータベースが更新されるなか、どの程度の頻度で突合を行い、どのデータベースにアクセスすればよいかなどを検討するとよい。ゼロデイ脆弱性や実証コードがない脆弱性においては脆弱性の発動の判断が難しい場合がある。このような場合は、脆弱性の識別者によって誤差が出る可能性があるため、SBOM の品質に影響があると考える。つまり、コンポーネントの脆弱性をどの程度の頻度でどのデータベースを参照すればよいのかという点と、コンポーネントの脆弱性の発動有無をどの材料をもって判断するかという点を確認することが重要であると考える。
- SBOM の構成に変更がない状況であっても、特定のコンポーネントの呼び出し方次第で脆弱性の発動は変わると考える。そのため、製品ベンダー側が VEX については作成する必要があると考える。また、VEX には実証コードが含まれていない場合、VEX を公開してもよいかという点について検討できるとよいのではないか。ユーザーにとって VEX は有用であるが、悪用可能と判断された場合 VEX を限りなく早く提供する必要があると考える。また、現状の VEX のステータスの種類では、製品ベンダーにおける製品の優先順位や脆弱性対応の優先順位が表面化される。そのため、ベンダーに対しても VEX の活用方法については啓蒙・普及や手引が必要であると考える。
- 情報共有のフェーズで、契約書の作成・構築・条項モデルについて実証項目として追記するとよい。

- ユーザー企業が、サプライヤーや最終ベンダーから調達・SBOM を納品する場合、規制等によってユーザー企業側から要求が行くことも多いため、そのような観点でも実証項目を検討するとよい。
- SBOM について、中小企業を含む多くの企業が活用できる状態を醸成することが重要である。一方、脆弱性管理プロセスを体力がない中小企業がすべて実施するのは難しいと考えるため、プロセスごとに、最低限、どこまで実施をするのがよいかのレベル分けを明示することを検討できるとよいのではないか。
- 脆弱性管理プロセスにおける情報共有フェーズについて、サプライヤーに修正を要請する場合は、他の開発者の製品も同様の部品を利用し、同様の脆弱性の影響を受ける場合があるため、パートナーシップの活用を含めて検討できるとよい。
- 脆弱性管理プロセスにおける暫定対処や本格対応のフェーズにおいて、ユーザーに周知、提供をする方法として、パートナーシップの活用を含めて検討できるとよい。

・ QUAD における共同原則等を踏まえ今後取り組むべき事項

- 本タスクフォースで議論されている SBOM の内容と QUAD の枠組みの関係性を整理できるとよい。また、QUAD と同様に EU のサイバーレジリエンス法も規制の一種であるため、それも含めて本タスクフォースの参考にするとよい。
- QUAD において SSDF と類似の内容が記載されているが、日本での対応を検討する際には、SSDF を参考にしながら方針を検討していくのがよいのではないか。
- QUAD の対象として、クラウドの SaaS におけるソフトウェアも含まれると考えられる。SaaS 事業者への影響度は、ISMAP 制度との整合性や SaaS 事業者の体力も考慮する必要がある。既に SaaS 事業者は数百項目のチェックリストに回答しなければならない状況があるため、SaaS 事業者への影響について検討できるとよい。
- QUAD に対しては、本タスクフォースの内容や成果を打ち込むことを検討するとよい。

3.2.3 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。

3.3 第 11 回ソフトウェアタスクフォース

3.3.1 開催概要

第 11 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 5 年 10 月 31 日 15:00～17:00
議事次第：
1. 開会
2. 事務局資料説明

3. デジタル庁の取り組み紹介
4. 自由討議
5. 閉会

配布資料:

資料 1　議事次第・配布資料一覧
資料 2　委員名簿
資料 3　サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性
資料 4　デジタル庁における Trustworthy なサービス実現のための取り組み

3.3.2 要旨

具体的に、デジタル庁の取り組みについて、SBOM 実証の今後の方向性について、SBOM 取引モデルと成果物の活用の今後の方向性についての 3 点について議論が行われた。下記に議事要旨を示す。

- デジタル庁の取り組みについて
  - 先月開催された Open Source Summit Europe では、EU のパブリックセクターが OSS を活用している中で、OSS の利用持続性含めたサステナビリティが重要視されているため、そのような視点でも検討いただけるとよい。
  - SBOM が生成されていない OSS を利用することになった場合、SBOM を生成する必要があると考えている。生成後の SBOM についても共有の仕組み等を検討いただけるとよい。
  - 取り組まれている活動内容については、対外的に発信いただけるとよい。他の自治体や団体などにも参考になると考える。
  - SBOM を社会基盤化できるとよいと考えているが、資金な流れや費用負担について検討する必要があると考える。責任については、レガシーな対応のみではスピードが間に合わないと考える。そのような視点も考慮に入れながら検討できるとよい。
  - SBOM が公開されていない OSS を利用する場合、その SBOM の構築は、コストが大幅にかかるため、課題になると考える。
  - 内製でソフトウェアを開発している中、開発者がいなくなると維持管理が難しくなると考える。内製開発における維持管理の観点から解決に向けて工夫いただけるとよい。
- SBOM 実証の今後の方向性について
  - 中小企業では、情報システムが一人しかいないことや IT 知見を持つ人材がいないケースも想定されるため、SBOM の脆弱性対応の自動化ツール含めて中小企業向けの施策も検討いただけるとよい。
  - SBOM の自動化においては、有償・無償ツールを組み合わせて安価に精度を上げる方針も検討いただけるとよい。

- 実現性のあるツール関連施策が SBOM 普及には重要であると考える。中小企業向けに無償ツールや企業が利用可能な標準的なツールのモデル等検討いただけるとよい。SBOM は、部品は特定するが、全ての脆弱性を特定できるわけではないと考えるため、脆弱性対応を軸として、SBOM がカバーできる脆弱性の範囲、カバーできない脆弱性の範囲について示すことを検討できるとよい。
- SBOM 作成側と利用側で実施すべき内容が変わると考える。特に SBOM 利用者の手間がかからない手法を検討できるとよい。SBOM 利用者のなかには対応の体制が構築できず、既存の脆弱性のパッチを適用する程度の実施内容の企業も多いと考えるため、組織規模や能力に応じて閾値を決めることも重要と考える。中小企業の観点からも、 SBOM 利用者の負担が少なくなることが望ましいと考えるので、その点も考慮いただけるとよい。
- 現場としては、SBOM を作成し、脆弱性と突合する必要があるが、現状、誤検知・過検知が多いと考える。それを解決する手法についても検討いただけるとよい。
- 検討内容については、参考にできる内容のため、文書等でまとめ、整理いただくとよい。対象ソフトウェアについて、今後はより一般化して検討できるとよいと考える。
- CISA から「Software Identification Ecosystem Option Analysis」文書が公表されており、ソフトウェア ID の統一性がない問題等に言及がなされている。自動化等はこのような動向を検討しながら考える必要がある。
- 部品 ID の生成については、例えば、PC やクラウドであれば資産管理団体からインベントリデータをもらい、そこから部品 ID を生成し共用する案もあると考える。また、OSS については関連組織・団体と協力し、部品 ID を作成し共用する、あるいは提供を受ける案もあると考える。そのような視点も考慮しながら検討できるとよい。
- 脆弱性の優先付け判断ツリーは、ユーザー側の視点が強く表れると考える。一方、業界によっては、知見がないユーザーの場合、ベンダー側の意思が入ってしまうことで、対応優先度が想定より高いものになることが多いため、配慮が必要であると考える。

・ SBOM 取引モデルと成果物の活用の今後の方向性について

- SBOM　導入のメリットとしてライセンス管理や脆弱性対応等があるが、加えて、ユーザー・SIer の視点では、業界標準として利用されている ISMS 等に SBOM 要件が含まれるとよいのではないか。また、構成管理において、含めたくない部品が入っていないことを確認できるという点もメリットになると考えている。取引モデルにおける契約の規定事項については、具体的に運用・保守サービスの項目に含まれる範囲との線引きについても検討できるとよい。例えば、現実的に問い合わせ対応の一部として、契約額などが動かない範囲で、脆弱性が公開された時の突合作業を実施する必要があるかなどが挙げられる。
- 取引モデルにおける契約の規定事項については、開発・保守が別の会社に委託されるケースがあるため、企業が変わった場合の対応も規定事項の一部として検討できるとよい。
- EU の Cyber Resilience Act の中で PSIRT を構築することが求められているが、取引モデルにおける契約の規定事項のなかでも言及できるとよいのではないか。
- 取引モデルにおける契約の規定事項において、レベルを基礎と発展の違いと根拠を明確化できるとよい。特に、再帰的利用・直接利用などの部品範囲や免責については、基礎になる可能性もあると考える。提供者の負担を下げるという点も流通上重要であるので検討いた

だけるとよい。

- 取引モデルは、非常によく全体を網羅しているが、契約書において紛議が起きた場合について、SBOM が正しいかを確認する作業と紛議を解決するための仕組みが重要であると考える。契約後の紛議など含めて仕組みを検討いただけるとよい。金銭、責任、紛議にかかる時間について、現場は問題視しているので、検討いただけるとよい。
- 成果物の活用については、各業界に任せればうまくいく内容ではないと考えるため、経済産業省や関係団体等含め、今後連携しながら進められるとよい。継続的に SBOM や ID などのソフトウェアを管理する組織が必要だと考える。そのような点も考慮し、検討できるとよい。民間で実施すること、政府として対応することなど整理しながら、考慮して検討いただけるとよい。
- 各組織・団体から発信される脅威情報、インシデント情報、アセットマネジメント等の情報について、自動化を行うようなフレームワーク、およびそれらの情報と脆弱性との対応付け、ならびに活用方法については、将来の課題として考慮できるよい。
- 規制については、業界水準とかけはなれた案に対して反発が起こるケースを散見している。SBOM に関する規制を考える場合、業界水準の観点も視野に入れながら、取り組んでいくことが重要であると考える。
- 米国では、SBOM はすぐに実施できるものではない部分や、業界で受け止めきれない部分もあると考えるため、そのような動向も注視しながら、今後検討できるとよい。

3.3.3 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。

3.4 第 12 回ソフトウェアタスクフォース

3.4.1 開催概要

第 12 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 2 月 28 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　　通信分野における SBOM の導入に向けた検討について
参考資料 1　ソフトウェア管理に向けた SBOM の導入に関する手引 Ver2.0（案）

3.4.2 要旨

具体的に、総務省の取り組みについて、今後の普及展開策、SBOM 導入手引 Ver.2.0（案）について、政府調達基準への SBOM 記載案についての 4 点について議論が行われた。下記に議事要旨を示す。

- 総務省の取り組みについて
  - 今後、総務省と経産省で連携を行い、様々なツールを試行、検討いただけるとよい。また今後は、SPDX 3.0 についても話題になることが考えられる中、他の SBOM フォーマットである Cyclone DX 等も考慮し、この点においても総務省と経産省で連携した上で、今後検討を進めて頂けるとよい。
  - 通信機器は総務省などのように、各省が個別に SBOM に関する検討が進められると考えている。業種共通の内容と業種個別の内容を区別し、検討いただけるとよい。
  - 省庁間で縦割りにせず、一般的な内容については共通的に検討いただき、個別の業界事情のみを各省で検討いただけるとよい。
  - システムの全体構成としては、ハードウェアとソフトウェアが混合したシステムになると考えている。同じ型番ハードウェアでもファームウェア構成が異なるケースや、ハードウェア構成と同等のソフトウェアアプライアンスを構成する場合など、製品としての SBOM のみでなくネットワーク構成上における製品利用に関する SBOM も必要だと考えている。
- 今後の普及展開策
  - 保険会社においてサイバー保険を提供しているケースがあるが、SBOM の提供が保険金額の検討の要素になるとよい。
  - 構成管理を実施するうえで、SBOM が求められるようになると考える。供給側による構成管理を促進するためには、ユーザー側で構成管理表の納品など供給側に要求することが重要である。そのために、関連団体と議論し、検討できるとよい。
  - SBOM に関連して、民間主導のコンソーシアムも設立されはじめており、昨年経産省が公表した SBOM 導入手引も活用しながら、SBOM 作成者だけでなく、SBOM 利用者の目線も含めて SBOM に関して議論しているような状況もあると認識している。検討中の SBOM 導入手引 Ver2.0（案）では幅広い内容が含まれ、充実しているが、特に SBOM 実証で示されているコストについては、より多くの事業者が SBOM を利用するためにも、幅広く実証結果を展開する必要があると考える。

- 複数のコミュニティで出ている意見であるが、今後の普及展開のためには、SBOM を含め、セキュリティ担当者だけでなく経営層へのメッセージも必要だと考える。
- 経営層へのメッセージは有効であると考える。ソフトウェアの業界団体のなかで、SBOM を理解して運用しているケースは一部の企業にとどまっている状況と認識しており、投資を行う判断を行うのは経営層であることから、経営層へのメッセージは重要だと考える。SBOM 含めて、経営層のサイバーセキュリティへの意識を向上させるためには、レギュレーションやインセンティブとの関連付けが必要だと考える。
- 日本においては、技術に詳しい人が経営層になる場合が少ない。この考えを変える取組が日本においても必要だと考える。
- CIO、CISO は取締役ではなく執行役員であるため、このような DX やセキュリティを担当できるような人を経営層に加えるという国策が必要であると考える。
- システム構築事業者やソフトウェア開発事業者への普及も重要である。IT に関係する団体のなかには中小含めたソフトウェアハウスが集まっているようなものもあるが、セキュリティのアンケートに対して返答がない企業が多かった状況もあると理解している。そのような関連団体と協力して、実態を把握しながら中小含めた事業者を巻き込みつつ、SBOM の普及を進める必要があると考える。さらに、他の関連団体等も巻き込みながら検討できるとよい。
- SBOM を社会インフラとする上で、SBOM 生成側の敷居を低くすることが望ましいと考える。SBOM 生成は利用者のニーズによって工夫する必要があると考える。そのためには、SBOM 生成・共有のフローを実施した上で、対応モデル含めた議論をすることが重要だと考える。このような内容を手解きできるガイダンスが必要だと考える。また、SBOM を流通させるうえで、SBOM の再利用が重要だと考える。国策ではなく、民間・コミュニティが実施する内容かもしれないが、SBOM 共有プラットフォームが必要であると考える。
- 本タスクフォースやコンソーシアム等で SBOM を検討しているところであるが、SBOM を理解できていないという意見も多い状況と考える。このような状況の中、今後、業界団体等の会員向けにアンケートを実施する際には、SBOM への意識が低い企業に対してヒアリングを行う必要があると考える。なぜ SBOM が浸透しないかを確認し、中小企業への支援等のアプローチを含め、今後の政策を検討できるとよい。
- 過去にソフトウェア関連の団体が実施したアンケートでは、SBOM を生成している企業は多くなかったと記憶している。今後、そのような業界団体と経産省で連携し、普及を進めていけるとよい。
- 2023 年の秋から米国の FDA におけるソフトウェアの市販前認証が更新され、SBOM の提出が求められていると理解している。そのなかでは、全てのソフトウェアが対象であり、米国で重要になってきていると認識している。特に、各メーカーにおいてリスクベースで SBOM を記載することが求められていることに苦労している状況があり、また、全てのソフトウェアが対象であることから、バイナリも対象に含まれている状況であると考える。バイナリについてはツールでスキャンすることが難しいため、現状は様々な手段でバイナリを解析化した上で、管理のみをツールで実施することが求められている状況であると考える。米国の FDA は人命を預かる機器を取り扱っているため、要求レベルが高い傾向にあると考え

る。関連して、SBOM 導入手引においては、どこまでを SBOM で管理すべきかの追記、直接利用・関節利用している OSS までを含めるなど敷居を低くするような文言の追加などを検討できるとよい。加えて、環境に応じて構築が求められる SBOM を紹介するなどの導入のハードルを下げるドキュメントが必要だと考える。

- 米国の FDA の要求レベルのハードルについては下げるのが困難と考えられるため、米国の特性上準拠していただく必要があると考える。また、フリーの OSS は著作物の可能性がある場合もあるので、表現には注意が必要であると考える。
- EU の CRA では、OSS を商用利用する組織が SBOM の責任を持つことが述べられていると理解している。
- そのことについては、ISO と同様の切り分けなので問題ないと考える。
- 施策を進めるにあたって、国内ベンダーに向けたワークショップを経産省もしくは業界団体が主催して開催できるとよい。ワークショップを実施することで、SBOM の啓発やベース基準の向上に繋がると考える。例えば、政府主催の会議体で実施するのも一つのアイデアだと考える。

・ SBOM 導入手引 Ver.2.0(案)について

- フェーズ 2 の脆弱性対応優先付けが重要だと考える。優先付け情報の選択・取得における「インシデントの有無」や「Exploit コードの流通状況」を取得するのは難しいこともあるので、CISA の KEV を利用することなど記載を検討いただくとよい。SSVC の記載においても、FIRST の EPSS を利用して脆弱性対応を減らしていく内容を追記するよう検討頂けるとよい。
- SBOM 対応モデルの分野として、ソフトウェア・自動車・医療機器の 3 つを記載していると理解している。ソフトウェア分野は全ての分野に該当するため、ソフトウェア製品などの文言に変更頂くことを検討するとよい。
- SBOM 導入手引 2.0(案)は、網羅的な文書であると考えているが、エントリーユーザーに必要な最低限の情報のみをまとめた文章も必要だと考える。また、ツールの一覧を手引きに記載しているが、それらのツールを対象に各フェーズで利用できるツールを整理できるとよい。
- 経産省と総務省の検討結果はお互いに連携しながら、SBOM 提供者の立場と SBOM 利用者の立場の意見を明確に区別して整理できるとよい。SBOM 提供側は手引全体について確認する必要がある。一方で、SBOM 利用者側は一部のみが対象であると考える。別冊として、初歩から学ぶ SBOM という観点で、利用者側の敷居を下げるような文書を提供できるとよい。

・ 政府調達基準への SBOM 記載案について

- 現場が適切に対応できるよう、ベースとなる基準はしっかり記載いただけるとよい。
- サプライチェーンという用語が抽象的だと考える。自動車や医療では、サプライチェーンの階層が深い中で、どの階層の SBOM が構築されるかが分かりづらいと考える。SBOM が完全ではない中、「既知の未知」や「未知の未知」への対応という点で、契約不適合責任の状況が分からないことを懸念されるため、このような観点からも明確化を検討するとよい。
- EU の CRA や米国の大統領令では、機械可読形式で SBOM を提出することやリスク分

析実施した上で SBOM を生成・提出することが求められ、具体的な SBOM の目的が確認できると考える。それを踏まえて、目的の明確化や具体的な基準を検討頂けるとよい。

- SBOMへの対応を要件化すると海外製品が優位になってしまうという懸念が考えられるため、国内ベンダーにおいても SBOM 利活用を促進することを検討できるとよい。また、SBOM を受け取った側もどう使うのか、具体的に明確にした方がよい。部品管理を適切に実施すれば、海外製品が出てきたとしても統制につながると考える。
- 米国の FDA の SBOM 要件化については、米国企業からも抵抗感があり、どう対処するかが難しい状況であると考える。日本でビジネスをしている米国企業も対象に含めながら、施策を検討いただけるとよい。また、各省庁とも整合性を取りながら、ハードルを上げ過ぎず実効性を担保できるよう、フィージビリティがあるレベルから検討頂けるとよい。

3.4.3 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。

4. 英訳

令和 4 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 Ver 1.0」及びその概要資料について、英訳を行った。

5. 総括

第 1 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 2 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、課題およ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 3 章では、第 1、2 章の調査・実証及び検討に関連して、企業の現場およ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。

令和 5 年度産業サイバーセキュリティ強靭化事業

（IoT 機器や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

SBOM を導入・活用するサプライチェーンモデルの構築に向けた調査・実証

2024 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5年度産業サイバーセキュリティ強靭化事業
（IoT機器や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

2024年3月29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 月に新たに立ち上げた「宇宙産業 SWG」及び宇宙 SWG の下に設置をした「宇宙産業 SWG 作業部会（又はコアメンバー会議）」を開催したほか、これらの検討会等を踏まえ、民間宇宙システムにおけるサイバーセキュリティ対策ガイドラインの更新を行った。あわせて、検討会等を踏まえ、宇宙システムのサイバーセキュリティに関する脅威・脆弱性・インシデント・対策等に関する情報共有、普及啓発のあり方等について検討を行った。

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」及び宇宙産業 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。

2.1.1 宇宙産業 SWG

今年度は宇宙産業 SWG を 2 回開催した。なお、2024 年 3 月現在、宇宙 SWG は下記の委員により構成される。

安達　昌紀	一般財団法人宇宙システム開発利用推進機構（JSS） 常務理事
片岡　晴彦	株式会社 IHI 顧問（元防衛省航空幕僚長）
木下　仁	独立行政法人情報処理推進機構（IPA）セキュリティセンター セキュリティ対策推進部脆弱性対策グループ 主任研究員
来原　聡文	東北大学大学院工学研究科 航空宇宙工学専攻 准教授 NPO 法人大学宇宙工学コンソーシアム（UNISEC） 理事長
小山　浩	三菱電機株式会社 電子システム事業本部 主席技監
坂下　哲也	一般財団法人 日本情報経済社会推進協会（JIPDEC） 常務理事
佐々木　弘志	フォーティネットジャパン合同会社 OT ビジネス開発部 部長
名和　利男	株式会社サイバーディフェンス研究所 専務理事・上級分析官
丸山　満彦	PwC コンサルティング合同会社 パートナー
満永　拓邦	東洋大学 情報連携学部 准教授、IPA 産業サイバーセキュリティセンター専門委員
吉松　健三	技術研究組合制御システムセキュリティセンター（CSSC）

（1） 第 7 回宇宙産業 SWG

1） 開催概要

日時：令和 5 年 8 月 29 日（火） 16 時 30 分～18 時 00 分
場所：対面開催（三菱総合研究所会議室）

議題
1. 開会
2. 委員及び経済産業省からのプレゼンテーション
   （ア） 産業サイバーセキュリティに関する動向について
   （イ） 情報・サイバーセキュリティの基本と動向
   （ウ） 制御システムセキュリティの最新動向

3. 事務局資料説明
   （ア） 宇宙分野における海外のサイバーセキュリティ対策等について
   （イ） 今年度の作業部会の活動方針
   （ウ） ガイドライン Ver2.0 に向けたアップデート方針について
   （エ） 情報共有のあり方に関する検討方針について
   （ウ） 今後の予定について
4. 自由討議
5. 閉会

配布資料:

資料1　　議事次第・配布資料一覧
資料2　　委員等名簿
資料3　　第 6 回宇宙産業 SWG 議事要旨
資料4－1　経済産業省サイバーセキュリティ課からの情報提供
資料4－2　丸山委員からの情報提供
資料4－3　佐々木委員からの情報提供（一部非公開・投影のみ）
資料5　　事務局説明資料

2）議事要旨

産業サイバーセキュリティ研究会
ワーキンググループ1（制度・技術・標準化）
宇宙産業SWG（第7回） 議事要旨

1. 日時・場所
日時：令和5年8月29日（火） 16時30分～18時00分
場所：三菱総合研究所4F 会議室CR-D・Eにて開催

2. 出席者
委員　　：坂下委員（座長）、安達委員、片岡委員、木下委員、小山委員、佐々木委員、名和委員、丸山委員、吉松委員
オブザーバ：宇宙産業SWG作業部会コアメンバー及び拡大メンバー
経済産業省：製造産業局宇宙産業室 室長 伊奈 康二
商務情報政策局サイバーセキュリティ課 課長補佐 加藤優一

3. 議事内容
1） 宇宙産業SWG開催挨拶
事務局から、対面での開催を行うとの説明があった。

2） 安達委員からの挨拶

鹿志村委員から委員交代に伴い、安達委員より挨拶があった。

3） 委員及び経済産業省からのプレゼンテーション

（1） 経済産業省サイバーセキュリティ課加藤課長補佐から『産業サイバーセキュリティに関する動向について』の情報提供があった。プレゼンテーションに関して挙げられた質問は以下のとおり。

・ IoT製品の適合性評価制度に関して、コモンクライテリアとの連携が記載されているが、現状の認証制度を拡張する予定なのか。コモンクライテリアを用いる場合、プロテクションプロファイルを作成する必要があるのか。

➢ JISEC制度の枠組みを拡張する形でIoT製品の適合性評価制度を構築していくことを想定している。現行のコモンクライテリアの制度をそのまま使うのではなく、適合性評価制度の先のレベルとしてコモンクライテリアが位置づけられる形となる。

・ 宇宙業界においてもSBOMを耳にする機会が増えた。SBOMの内容と目的を確認したく、ソフトウェアパッケージの作成者・所有者及びIDの識別子を明確にする位置づけか。そうであるならば、従来のソフトウェア管理方法とSBOMの根本的な管理方法の違いは何か。

➢ SBOMが特に対象とするリスクはサプライチェーンリスクである。昨今、ソフトウェアを含む様々な製品について、海外を含む委託先に開発をさせるようになっている。米国の大手事業者では、委託先に対してサイバー攻撃がなされた場合、生産・操業が止まる事例があった。ハードウェアであれば文書で管理することができたが、ソフトウェアでは文書での管理が難しい。SBOMを用いることで、ソフトウェアをカタログ化して管理することができる。また米国では、訴訟において関連文書が揃っている場合、訴えを認めるという制度（ディスカバリー制度）がある。SBOMはフォレンジック調査の追跡性の考え方を導入した制度であるため、その制度と親和性があり、サイバーに関する係争状態の解消に活用されることも想定される。他方、日本ではそのような背景がないため、SBOMの活用方法に混乱が生じている。現在は、サプライヤーに対するサイバー攻撃に対抗するためにSBOMの活用が検討されているが、元々は信頼性確保・製品の安定供給が目的であるため、日本では、米国と異なった目的で活用している印象がある。

4） 丸山委員から『情報・サイバーセキュリティの基本と動向』の情報提供があった。

5） 佐々木委員から『制御システムセキュリティの最新動向』の情報提供があった。プレゼンテーションに関して挙げられた質問は以下のとおり。

・ 電子カルテの攻撃事例について、攻撃を受けた全てのシステムがダウンしたのか。

➢ 1,000台程度が停止した疑いがある。

➢ 攻撃を受けた後もシステムの一部は稼働したのか。宇宙分野は安全保障と密接に関係しており、宇宙分野でインシデントが起きた場合、システムを全て止めるのは安全保障上難しいと考える。部分的に一部の機能を稼働させることが必要であるが、技術的にこのような対応は可能であるか。

➢ 技術的には、ゾーニングのような考え方で区域を分けることで対策を行うことはできる。ただし、病院

も工場も全てフラットでゾーニングできていないことが多く、そうなると止めざるを得ない。ミッションクリティカルなシステムはゾーニングする必要があるが、セキュリティ対策にはコストがかかる。そのため、ミッションクリティカルなシステムをネットワーク化する場合等にゾーニングを取り入れる等、段階的な検討ができると良い。

- 以前、病院におけるサイバーセキュリティ対策に関して厚生労働省・経済産業省・総務省が各々でガイドラインを作成しており、整合性が十分ではなかった。ここ数年、経産省・総務省が連携し一つにまとめて、現在は、3省2ガイドラインとなっている。それまでは各ガイドラインに準拠すると過不足が発生するなどして、ベンダーが対応に苦労していた。省庁間の連携が初めから行われていると良かった。
- コロニアルパイプラインの攻撃では、OTは攻撃を受けてないものの、全てのシステムを停止することとなった。管理するためのITが攻撃されるとOTの安全性が信頼できないため、OTも止めるほかない。そのためセグメントで区切ったとしても、全体を見て判断をする必要がある。

・ ゼロトラストセキュリティはどの程度導入されているのか。

- 米国では議論が進んでいるが、実装には一定のハードルがある。

・ Web診断分析結果について、225社の企業規模はどの程度か。

- 企業規模は統一的ではなく、1兆円を超える売上の企業もいれば、1,000億円以下の企業も含まれる。企業規模によって体制が異なり、例えば1,000億円以下の企業では、ITとOTのセキュリティ担当が共通であるため、IT・OTの連携の評価が高いという結果となった。

6） 事務局資料説明

（1） 事務局より、以下のアジェンダに基づいて情報提供があった。

（ア）宇宙分野における海外のサイバーセキュリティ対策等について

（イ）今年度の作業部会の活動方針

（ウ）ガイドラインVer2.0に向けたアップデート方針について

（エ）情報共有のあり方に関する検討方針について

（オ）今後の予定

7） 自由討議

各委員からの主な意見

・ OTの内、宇宙という専門的範囲を検討するのが本SWGと理解している。他方、ITの部分や、IT・OTのコンタミネーションを防ぐという観点は工場SWGや他の重要インフラでも同様に重要であり、その内容をまとめる必要があると理解した。今回事務局からされたプレゼン内容は、宇宙防衛に取り組んできた身としては新しい話ではないものの、今後、このような話に触れてこなかった人にとっても浸透させていく必要がある議論として理解した。高度な対策に加え、最低限実施すべき対策を取り上げるというメリハリを今後のアップデートに加えられると良いのではないか。

・ 今年の取組の中で、セキュリティポリシーの雛形を作成するとあるが、粒度が不明確ではないか。規程の体系を示した上で、対象とする雛形の位置づけを示した方が良いのではないか。

- NISCの「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」では規範、基準、ガイドライ

ンの3段階が位置づけられているが、今回のセキュリティポリシーは「基準」の位置づけの想定であった。

- 企業では、セキュリティポリシーの下に情報セキュリティ規程があり、その下に細則がある。セキュリティポリシーは外部にも公開する文書の位置づけである。規程体系を読者に示した上で、今回の雛形がどこに位置づけられるかを示せると良い。

・ 各国で新しいガイドラインが続々と作成されていると理解した。米国のガイドラインやEUのガイドライン等、それぞれの包含関係や主従関係などの整理をしてほしい。実務者視点では、確認すべき諸外国のガイドラインが一目で分かると良い。前回SWGの資料の米国文書の体系図のような整理があると分かりやすい。

- 米国文書の体系整理の重要性は理解している。以前のSWGで示した米国文書の体系図を米国に提示したところ、先方担当者もあまり整理できていない様子であった。SP800-53、NIST CSF、CNSSPの対応関係を米国関係者に確認したところ、NIST CSFが中心になりそうであるとの話をいただいた。米国の文書の整理をガイドラインのコラムに載せられると良い。
- 米国CISAのCSET（Cyber Security Evaluation Tool）では、米国のガイドラインやポリシーが網羅的にまとめられ、自組織の評価に使われている。GitHubで公開されて頻度よくアップデートされている。独・仏などの欧州のガイドラインは、一部が英語で出ているものの、国内企業向けには母国語のみで発行されているものが目立つ。英国は、米国とは異なり、CiSP（Cyber-security Information Sharing Partnership）などのポータルサイト内でガイドラインやポリシーの適用に関する情報が共有されている。

・ ロシアの通信事業者に対する攻撃事例が紹介されていたが、本事例の影響範囲は、経済産業省ガイドラインが防御したい典型的な事例ではないか。本ガイドラインはCPSFをベースとし、組織だけではなくシステムも対象となっているため、マルチステークホルダーを考慮しているのが強みだと考える。外部へのアピールとして、単なるCSFとのマッピングだけではないということを示していくと良いのではないか。また、事業者としては調達基準になるのかが懸念である。本ガイドラインの位置づけを明記してほしい。

・ 米国ではインシデントが起きるたびに、ガイドライン等がアップデートされている印象がある。日本の技術レベルは米国のセキュリティを単独で実現できるくらいにあるのか。

- サプライチェーンが多岐にわたるため、難しいと考える。
- 日本の組織になじまない技術者が集まればできることが多いように感じる。自社では日本の組織文化となじまなかった技術者が比較的多いためか、海外のハッキング大会でいい成績を残している。
- そのような組織において、米国と同等のセキュリティレベルを実現することは技術的には可能か。
- 条件付きではあるが可能と考えている。一方で、日本の組織文化となじまない技術者もいる印象である。

・ 今後の進め方について、ガイドラインのアップデート方針をSWGにて一度協議をした方が良いのではないか。

- 今後の方針は事務局資料にて示しており、これに基づき、コアメンバー会議で具体的な改定作業を進めていく予定である。記載する内容については、コアメンバー会議にて今後詳細を詰めていく予定である。

- 具体的な改定作業を始める前に、一度確認した方が良いのではないか。
- 承知した。宇宙産業SWG会議とコアメンバー会議の合同会議にするなどの工夫も含めて検討したい。

8） その他

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

次回の第8回会合については、今回の議論を踏まえた検討を行ったのち、事務局から日程調整を行わせていただく。

以上

（2）第 8 回宇宙産業 SWG・第 14 回作業部会コアメンバー会議 合同開催

1）開催概要

日時：令和 6 年 3 月 15 日（金） 16 時 30 分～18 時 00 分

場所：対面開催（経済産業省会議室）

議題

1. 開会
2. 最近のサイバーセキュリティ課の取組について
3. 宇宙分野のセキュリティに関する近年の動向及びガイドラインのアップデートについて
   （ア） 宇宙分野における海外のサイバーセキュリティ対策等について
   （イ） ガイドライン Ver2.0 に向けたアップデート方針について
4. 情報共有のあり方に関する検討について
   （ア） 情報共有のあり方に関する検討について
   （イ） スペースセキュリティ勉強会に関して
5. 宇宙活動法における「サイバーセキュリティの確保」について
6. 統合質疑・討議
7. 今後の予定について
8. 閉会

配布資料:

資料1　　議事次第・配布資料一覧

資料 2　　宇宙産業 SWG 委員/作業部会コアメンバー名簿

資料3　　第 7 回宇宙産業 SWG 議事要旨

資料4　　最近のサイバーセキュリティ課の取組について

（経済産業省サイバーセキュリティ課からの情報提供）

資料5－1　宇宙分野のセキュリティに関する近年の動向及びガイドラインのアップデートについて

資料5－2　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（案）

資料6－1　情報共有のあり方に関する検討について

資料6－2　スペースセキュリティ勉強会に関して（粟津様・小出様からの情報提供）

資料7　宇宙活動法における「サイバーセキュリティの確保」について【非公開】
（内閣府山口参事官からの情報提供）

資料8　今後の予定について

参考資料1　民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 2.0 概要資料（案）

参考資料2　対策要求事項チェックリスト【ガイドライン添付資料1】

参考資料3　NIST Cybersecurity Framework（NIST CSF）と宇宙システム特有の対策との対応関係【ガイドライン添付資料2】

参考資料4　情報セキュリティ関連規程（サンプル）【ガイドライン添付資料3】

参考資料5　ガイドラインに対する意見対応表【非公開】

2）議事要旨

産業サイバーセキュリティ研究会
ワーキンググループ1（制度・技術・標準化）
宇宙産業SWG（第8回）・作業部会コアメンバー会議（第14回）合同開催
議事要旨

1. 日時・場所

日時：令和6年3月15日（金） 16時30分～18時00分

場所：経済産業省 別館2階 227各省庁共有会議室及びTeams会議によるハイブリッド開催

2. 出席者

宇宙産業SWG委員：坂下委員（座長）、安達委員、片岡委員、木下委員、粟原委員、小山委員、佐々木委員、名和委員、丸山委員、満永委員、吉松委員

作業部会コアメンバー：粟津様、上杉様、木下様（SWG委員兼任）、小出様、國母様、合田様、佐々木様（SWG委員兼任）、神宮様、髙橋様、田中様、多賀様、平松様、吉松様（SWG委員兼任）

オブザーバ：作業部会拡大メンバー、防衛省 航空幕僚監部 防衛部 事業計画第2課

内閣府：宇宙開発戦略推進事務局 参事官 山口真吾

経済産業省：製造産業局宇宙産業室 室長 伊奈康二

商務情報政策局サイバーセキュリティ課 企画官 山田剛人、課長補佐 加藤優一、

課長補佐 飯塚智、係長 澤田知子

3. 議事内容

1） 開会

2） 最近のサイバーセキュリティ課の取組について

経済産業省サイバーセキュリティ課飯塚課長補佐、澤田係長から『最近のサイバーセキュリティ課の取組について』の情報提供があった。

3） 宇宙分野のセキュリティに関する近年の動向及びガイドラインのアップデートについて

事務局より、以下のアジェンダに基づいて情報提供があった。

（1） 宇宙分野における海外のサイバーセキュリティ対策等について

（2） ガイドラインVer2.0に向けたアップデートについて

4） 情報共有のあり方に関する検討について

（1） 情報共有のあり方に関する検討について

事務局より、『情報共有のあり方に関する検討について』の情報提供があった。

（2） スペースセキュリティ勉強会に関して

スペースセキュリティ勉強会事務局であるスカイゲートテクノロジズの粟津様から『スペースセキュリティ勉強会』について情報提供があった。

5） 宇宙活動法における「サイバーセキュリティの確保」について

内閣府山口参事官から『宇宙活動法における「サイバーセキュリティの確保」について』の情報提供があった。

6） 統合質疑・討議

- ガイドライン添付資料3の情報セキュリティ関連規程（サンプル）において、機密性1は公開対象なため、誤解を避けるために評価値は2以上とする方が良い。
- 衛星に対するサイバーセキュリティのガイドライン等、様々な文書が次々に公表されている。各文書の要求事項は補完的になっているのか。
  - 昨今のNISTの文書は、データセキュリティとサイバーセキュリティを組み合わせた考え方を示している。他の文書についても、オペレーションの観点で見るのか、ガバナンスの観点で見るのかで規則体系が異なる。
  - NISTも、各文書の関係性整理について課題意識を有している。最近では、NISTIR 8278にて、文書間の関係を自動的にマッピングできるようにする取組が進められている。
  - NIST SP800-53が最も広範なガイドラインであり、要求事項は1,000個を超える。全てに対応しようとすると事業者は疲弊するため、自社でリスク評価を行い対策すべき項目を特定した上で、ガイドラインに立ち返って必要なセキュリティ対策を検討できると良い。
- 情報共有体制の構築に係るフェーズについて、フェーズ0からフェーズ1に移行する際はリーダーシップが必要になる。末端の頑張りに依存するのではなく、初期の構想の段階から中核となる人材の存在

が必要ではないか。政府が主導する場合、政府と民間の間で主導する場合、民間が主導する場合等複数のパターンが考えられるが、いずれにせよ、責任を明確にする必要がある。

- ガイドライン本編と情報セキュリティ関連規程（サンプル）の内容にギャップがあり、サンプルの記載粒度が粗い部分もある。サンプルのうち、セキュリティ規程として活用できる内容もあれば、その下位の位置づけである細則において活用できる内容もある。このような活用方法をガイドラインでも明記できると良い。
- 欧州規制の詳細やNIST文書との整合性について各社で調査することは困難であるため、動向をキャッチアップできる母体があると良い。セキュリティの分野ではIPAが候補として検討しうるが、宇宙分野のセキュリティの動向を恒常的にキャッチアップしていく仕組みを作ることが中長期的な視点では重要になる。
- 主に民間事業者がサイバー攻撃の被害を受けることから、宇宙業界のセキュリティに関するコミュニティは民間が主導して組織化・運用する必要がある。また、日本政府として定めるセキュリティに関する要求事項は、国際競争力を踏まえた議論が必要である。その際、宇宙分野特有のセキュリティがどれだけ存在するかを念頭に置いた議論が必要である。宇宙業界はスタンドアロンだと考えられていたが、現在では様々なシステムと繋がっている。このような状況下においては、特に地上のシステムに対して、既存のIPAの規格等を活用したセキュリティ対策の検討ができる。そのため、宇宙業界のセキュリティのコミュニティで議論する対象は宇宙業界特有のトピックに絞りつつ、宇宙業界特有ではない内容については、既存の文書を活用する方針が望ましい。
- リアルタイムのデータを共有するとなると高度なセキュリティ対策が必要であり、どの事業者がセキュリティ基準を満たすことができるか、誰がそのセキュリティレベルを評価するか等が課題として想定される。
- 国内における情報共有体制に関して、New Spaceに限定されず、規模の大きい事業者も巻き込みつつ、実務的な情報が一元的に集約されると良い。

7）今後の予定について

経済産業省伊奈室長より今後の予定について、説明があった。

- ガイドラインVer2.0について議論を踏まえ修正を行った上で公開する。
- 従来からの事業者に限らず、New Spaceも含め、民間事業者中心に情報共有体制の構築を進められるよう、政府の支援を検討しつつ、体制構築に向けた検討を進める。

8）閉会

以上

2.1.2 作業部会コアメンバー会議

本年は、宇宙産業 SWG 作業部会コアメンバー会議を 4 回開催した。なお、2023 年 3 月現在、コアメンバーは、以下の会員によって構成される。

粟津 昂規　スカイゲートテクノロジズ株式会社　代表取締役
上杉 謙二　PwC コンサルティング合同会社 テクノロジーコンサルティング　ディレクター
木下 仁　独立行政法人情報処理推進機構(IPA)セキュリティセンター　主任研究員
小出 祐輔　株式会社 Synspective　IT セキュリティスペシャリスト
合田 知善　日本電気株式会社 エアロスペース事業部門
スペースプロダクト統括部 プロフェッショナル
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 フォーティネットジャパン株式会社 OT ビジネス開発部　部長
IPA 産業サイバーセキュリティセンター専門委員
神宮 健　NRI セキュアテクノロジーズ株式会社
DX セキュリティコンサルティング事業本部 IoT セキュリティ事業部
鈴本 遼　株式会社アークエッジ・スペース 執行役員 ソフトウェア・基盤システム部長
髙橋 康夫　三井物産セキュアディレクション株式会社 コンサルティングサービス事業本部
公共事業部宇宙防衛グループ プリンシパルアナリスト
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 洋吏　三菱電機株式会社電子システム事業本部鎌倉製作所
宇宙技術部 セキュリティ技術課 課長
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
吉松 健三　技術研究組合制御システムセキュリティセンター(CSSC)

(1) 第 11 回作業部会コアメンバー会議

1) 開催概要

日時:令和 5 年 7 月 5 日(水) 10 時 30 分～12 時 30 分
場所:オンライン開催

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
4. ガイドラインのアップデートについて
5. 自由討議
6. 閉会

配布資料:

資料1　　議事次第・配布資料一覧
資料2　　作業部会コアメンバー名簿（更新版）
資料3　　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_v3
資料4　　ガイドラインのアップデートについて_v8
参考資料 1　民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.1
参考資料 2　民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.1 概要資料

（2）第 12 回作業部会コアメンバー会議

1）開催概要

日時：令和 5 年 11 月 14 日（火） 14 時 30 分～16 時 00 分
場所：オンライン開催

議題

1. 開会
2. 事務局資料説明
    （1）宇宙分野における海外のサイバーセキュリティ対策等について
    （2）ガイドライン Ver 2.0 のアップデートについて
3. 自由討議
4. スペースセキュリティ勉強会に関して
5. 自由討議
6. 閉会

配布資料:

資料1　　議事次第・配布資料一覧 v2
資料2　　作業部会コアメンバー名簿
資料3　　事務局説明資料_v8
資料4　　［2023-11-08］ スペースセキュリティ勉強会に関してガイドラインのアップデートについて_v8
参考資料 1　民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 2.0（素案）
参考資料 2　IPA「中小企業の情報セキュリティ対策ガイドライン」付録 5

（3）第 13 回作業部会コアメンバー会議

1） 開催概要

日時：令和 6 年 2 月 13 日（火） 15 時 00 分～16 時 30 分
場所：オンライン開催

議題
1. 開会
2. 事務局資料説明（1）ガイドライン Ver2.0 のアップデートについて
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	作業部会コアメンバー名簿
資料3	事務局説明資料
資料4	民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 2.0（案）
資料 5	情報セキュリティ関連規程（サンプル）【ガイドライン添付資料3】
参考資料 1	ガイドラインに対する意見対応表

（4） 第 14 回作業部会コアメンバー会議

前述のとおり、第 14 回作業部会コアメンバー会議は、第 8 回宇宙産業 SWG と合同で開催した。開催概要及び議事要旨については 2.1.1（2）を参照のこと。

3. 民間宇宙システムにおけるサイバーセキュリティ対策ガイドラインの更新

検討会等を踏まえ、民間宇宙システムにおけるサイバーセキュリティ対策ガイドラインの更新を行った。

3.1 ガイドライン更新の概要

2023 年 3 月 16 日に開催した第 6 回宇宙産業 SWG において「民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン」の Ver 1.1 案を議論し、2023 年 3 月 31 日に Ver 1.1 の正式版を公開した。ガイドラインに記載のとおり、国内外の最新知見や動向を踏まえ、1 年に 1 回程度の見直しを図っていくところ、今年度は、Ver 2.0 に向けたアップデートを行った。第 11 回作業部会コアメンバー会議の議論を踏まえ、Ver 2.0 に向け、主に以下の項目に関するアップデートを実施した。

- ガイドラインの対象とする衛星システムのスコープの拡大
- セキュリティ関連規程の雛形の追加
- 具体的な対策内容に関する改訂

3.2 ガイドライン更新に向けた取組

ガイドラインの更新に向け、宇宙産業 SWG や作業部会コアメンバー会議にて、更新方針や更新内容に関して議論・確認を行った。更新に向けた今年度の取組概要は以下に示すとおりである。

表 3-1 ガイドライン更新に向けた宇宙産業 SWG・コアメンバー会議の取組

実施日	会議名等	ガイドラインに関する主な議題
2023 年 7 月 5 日	宇宙産業 SWG 作業部会 コアメンバー会議（第 11 回）	・ ガイドライン Ver 2.0 の構成・体裁について ・ ガイドライン Ver 2.0 のスコープについて ・ 高度な対策の実装について ・ 宇宙特有のサプライチェーン・セキュリティ対策について 等
2023 年 8 月 29 日	宇宙産業 SWG（第7回）	・ ガイドライン Ver 2.0 のアップデート方針について
2023 年 11 月 14 日	宇宙産業 SWG 作業部会 コアメンバー会議（第 12 回）	・ 標準的なモデル図について ・ 想定されるリスクシナリオについて ・ セキュリティ対策のポイントについて ・ セキュリティ関連規程の雛形について
2023 年 11 月 10 日 ～2023 年 11 月 17 日	宇宙産業 SWG 委員に対するメール確認	・ 標準的なモデル図について ・ 想定されるリスクシナリオについて ・ セキュリティ対策のポイントについて ・ セキュリティ関連規程の雛形について

実施日	会議名等	ガイドラインに関する主な議題
2024 年 2 月 13 日	宇宙産業 SWG 作業部会 コアメンバー会議（第 13 回）	・ 修正したガイドライン Ver 2.0 の案について
2024 年 3 月 15 日	宇宙産業 SWG（第8回） 作業部会コアメンバー会議（第 14 回）合同開催	・ 修正したガイドライン Ver 2.0 の案について

宇宙産業 SWG や作業部会コアメンバー会議の活動だけでなく、民間宇宙事業者に個別にヒアリングを実施し、更新方針や更新内容に関して意見を伺った。ガイドラインの更新に係るヒアリングの実施概要は以下に示すとおりである。

表 3-2 ガイドライン更新に向けたヒアリングの実施概要

実施日	事業者区分	ヒアリング項目
2023 年 7 月 14 日	輸送・打上事業者	・ 輸送・打上システムにおいて特に考慮すべきセキュリティリスクについて ・ 輸送・打上システムに求められるセキュリティ対策について ・ セキュリティ対策上の課題・悩みについて ・ 輸送・打上システムをガイドラインのスコープに含めることの是非について
2023 年 9 月 26 日	宇宙セキュリティ関連事業者	・ スコープを拡大したモデル図について ・ 想定される脅威シナリオについて
2023 年 10 月 10 日	衛星事業者	・ セキュリティ関連規程の雛形について
2024 年 2 月 5 日	衛星事業者	・ ガイドライン Ver 2.0 案について ・ セキュリティ関連規程の雛形案について
2024 年 2 月 9 日	衛星事業者	・ ガイドライン Ver 2.0 案について ・ セキュリティ関連規程の雛形案について
2024 年 2 月 27 日	通信衛星事業者	・ ガイドライン Ver 2.0 案について

輸送・打上事業者のヒアリングでは、特に考慮すべきセキュリティリスクとして、開発環境におけるセキュリティリスクが挙げられた。このリスクに対して、機密性の高いデータの保護が今後課題になると示唆された。ガイドライン Ver 2.0 で輸送・打上システムをスコープに含めることの是非について、人工衛星と比較すると輸送機は研究段階が中心であるため、スコープに含めることは時期尚早であるとの意見が挙げられた。一方で、業界全体としてサイバーセキュリティ対策に関する意識を高めることの重要性も意見された。

宇宙セキュリティ関連事業者や衛星事業者に対するヒアリングでは、作成したガイドライン Ver 2.0 の案やセキュリティ関連規程の雛形の案について、意見を伺った。特に、スコープの拡大を考慮したモデ

ル図の妥当性や想定される脅威シナリオの妥当性について、Ver 2.0 で新たにスコープとした通信衛星事業者も含めて意見を伺った。また、セキュリティ関連規程の雛形については、実際に活用する民間宇宙事業者にとって使いやすい形式となっているか、項目に過不足はないか等をヒアリングで確認した。

3.3 ガイドライン更新内容

宇宙産業 SWG や作業部会コアメンバー会議の活動及び民間宇宙事業者に対するヒアリング結果を踏まえて、ガイドラインを更新した。ガイドライン Ver 2.0 の目次構成は以下のとおりであり、ガイドライン本編冒頭に「本ガイドラインの全体概要」を加えたほか、添付資料 3 として「情報セキュリティ関連規程（サンプル）」を追加したことを除き、Ver 1.1 からの目次構成に大きな変更はない。

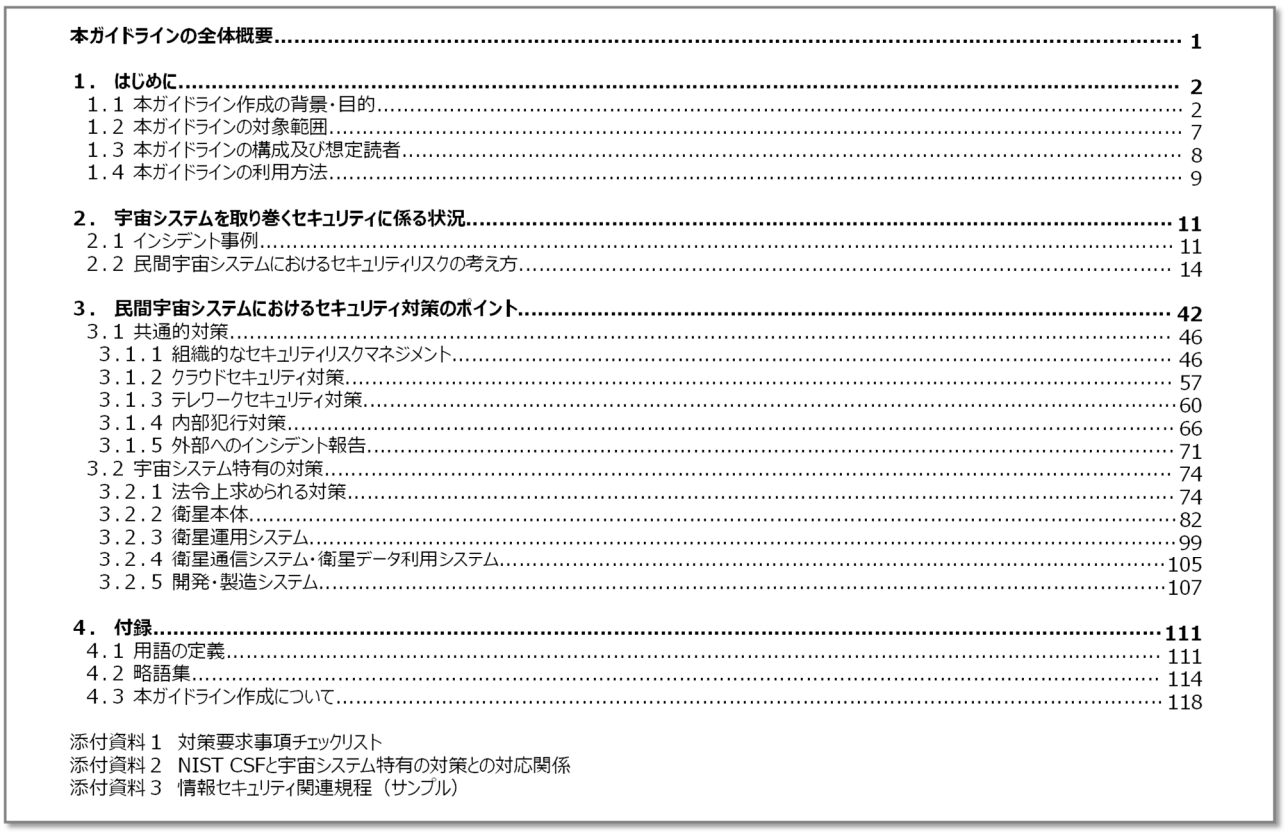


図 3-1 ガイドライン Ver 2.0 の目次構成

以降では、Ver 2.0 における更新内容の概要を示す。

3.3.1 ガイドライン本編に関する更新内容

（1） ガイドライン本編 1 章における更新内容

ガイドライン本編の 1 章における主要な更新内容は以下のとおりである。

- ガイドライン本編や添付資料の記載内容・利用方法が分かる全体概要（エグゼクティブ・サマリー）

を冒頭に追加。【本ガイドラインの全体概要】

- ガイドラインのスコープについて、特定のミッション（観測衛星、通信衛星、放送衛星等）やシステム規模等に限定せず、民間企業が主体となる衛星システム及び地上システムを対象にすることを明記。【1.2】
- 通信・放送衛星を明示的に対象に加えることを踏まえ、「衛星通信利用者」をステークホルダーとして追加。【表 1-2】
- 本ガイドライン及び添付資料の活用方法を明記。【1.4、表 1-3】

これらの主要更新内容のうち、全体概要に関して、ガイドライン本編及び添付資料の記載内容や利用方法が簡易に確認できるよう、以下に示す 1 ページの全体概要（エグゼクティブ・サマリー）をガイドライン冒頭に追加した。

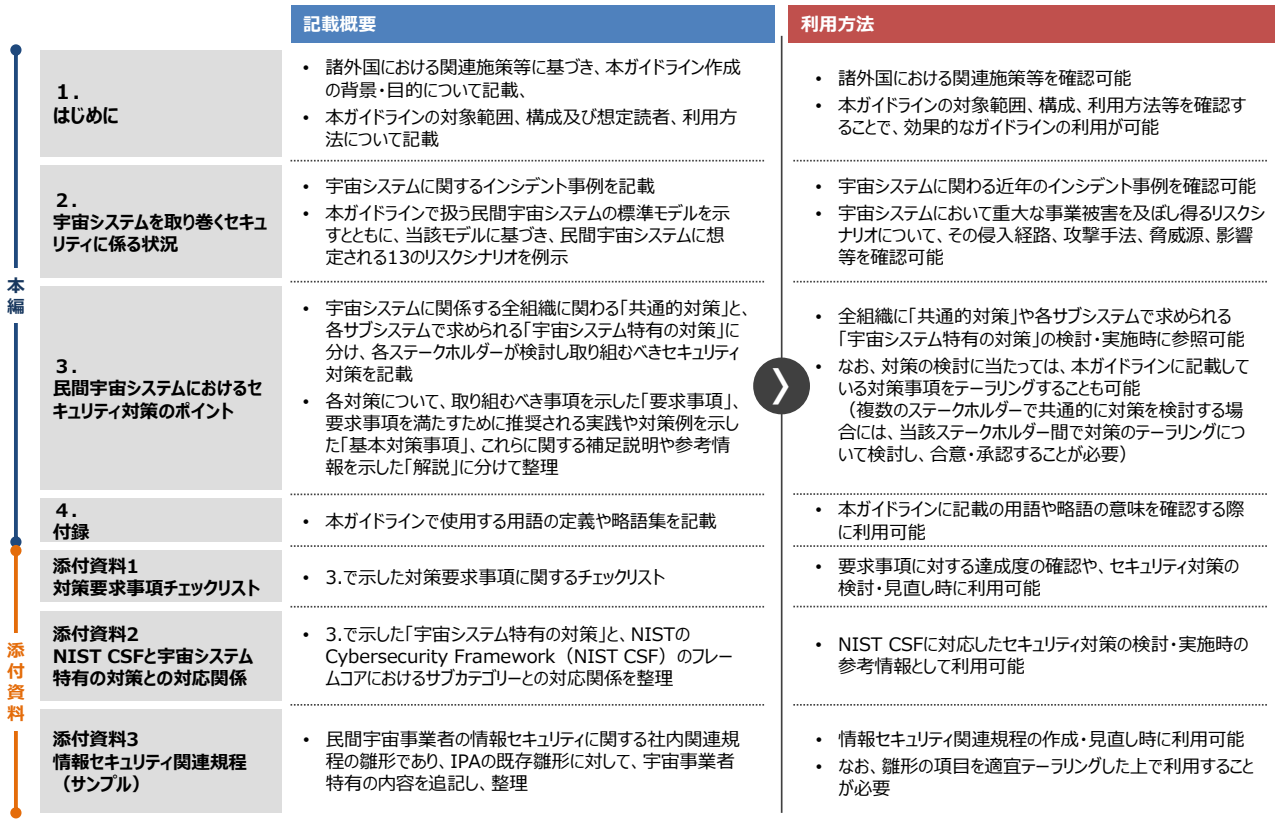


図 3-2 ガイドラインの全体概要

ガイドライン Ver 1.1 では、観測衛星を主なスコープとしていたが、宇宙産業 SWG 及び作業部会コアメンバー会議の議論を踏まえ、Ver 2.0 では特定のミッション（観測衛星、通信衛星、放送衛星等）やシステム規模等に限定せず、民間企業が主体となる宇宙システムを広く対象とした。これを踏まえ、衛星のライフサイクル・ステークホルダーとガイドラインの対象フェーズを以下のように修正した。なお、輸送・打上事業者に対するヒアリング結果を踏まえ、輸送・打上システムは引き続きガイドラインの対象外とした。

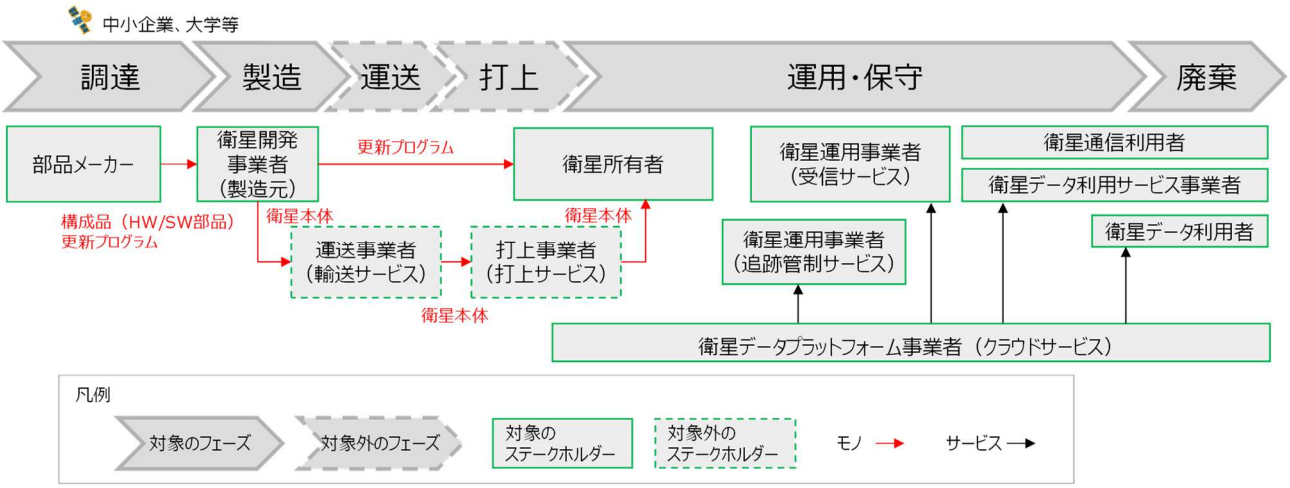


図 3-3 衛星のライフサイクル・ステークホルダーと本ガイドラインの対象フェーズ

ガイドライン本編の 1 章では、その他、以下の内容に関する軽微な更新を行った。

- 宇宙システムのサイバーセキュリティ関連施策について、近年の動向を追加。【表 1-1】
- Ver 2.0 での改訂内容を明記。【1.1 (5)】

（2）ガイドライン本編 2 章における更新内容

ガイドライン本編の 2 章における主要な更新内容は以下のとおりである。

- スコープの拡大を踏まえ、宇宙システムの標準的なモデルを修正し、各システム・ステークホルダーの説明を追加。【図 2-3、表 2-3～2-4】
- 修正した標準モデルをベースに、宇宙システムにおいて「発生してほしくない事象の例」を修正。【図 2-7】
- 想定されるリスクシナリオ例について、スコープの拡大及び近年のインシデント事例を踏まえ、6 つのシナリオ例（例 8～例 13）を追加。また、各シナリオについて、侵入経路、攻撃手法、脅威源及び影響を整理。【表 2-5、図 2-7～2-20】

これらの主要更新内容のうち、宇宙システムの標準的なモデルについて、ガイドラインのスコープを特定のミッション（観測衛星、通信衛星、放送衛星等）やシステム規模等に限定しないことを踏まえ、Ver 1.1 のモデル図から、以下に示す抽象的なモデル図に変更した。

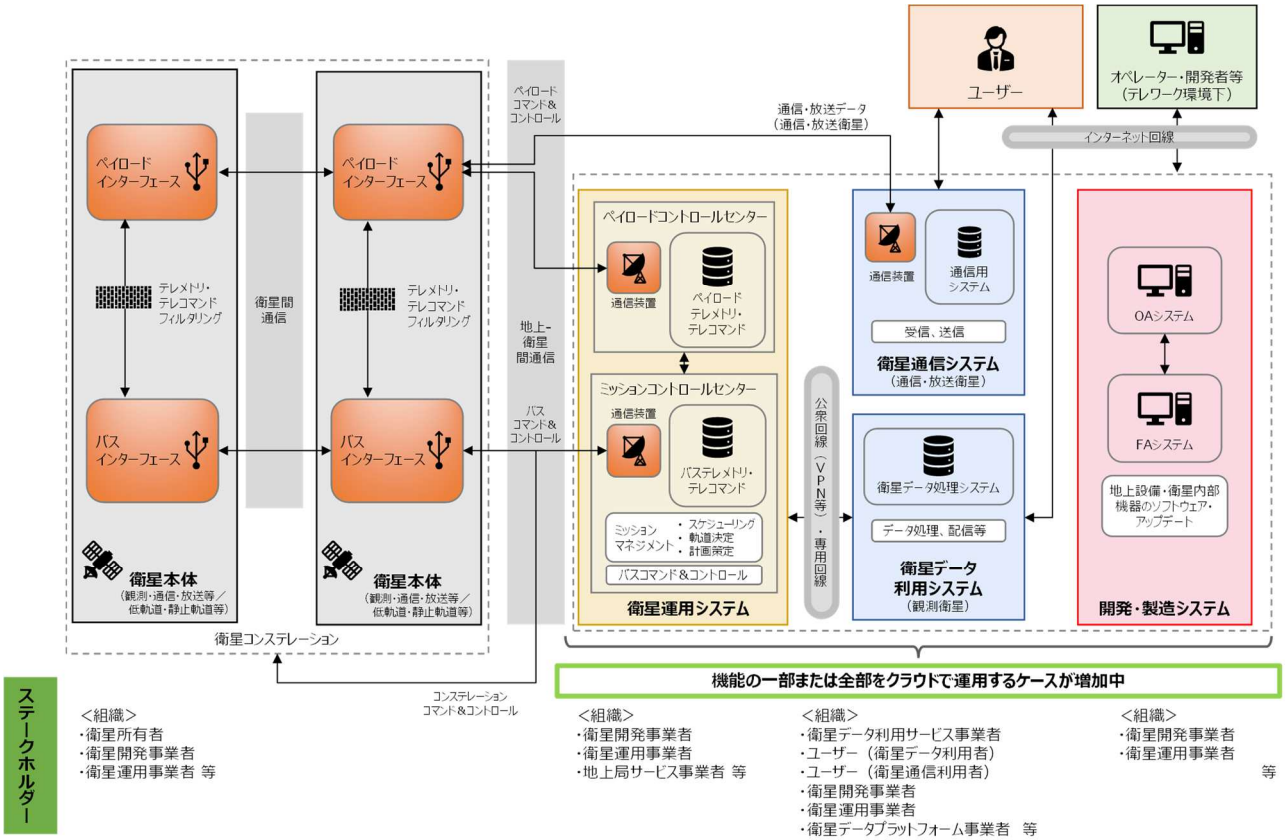


図 3-4 民間宇宙システムの標準的モデル（Ver 2.0 における更新版）

このモデル図をベースに、宇宙システムにおいて想定されるリスクシナリオの例を再検討した。Ver 2.0 の更新においては、Ver 1.1 で示していた 7 つのリスクシナリオ例に加え、6 つのリスクシナリオ例を追加し、計 13 のリスクシナリオ例について、侵入経路、攻撃手法、脅威源、影響等を再整理した。13 のリスクシナリオ例の概要を以下に示す。

表 3-3 民間宇宙システムにおいて想定されるリスクシナリオの例（Ver 2.0 における更新版）

No.	シナリオ例	概要	侵入経路	攻撃手法	脅威源	影響
例1	標準型メール攻撃による衛星軌道制御の喪失	OA 環境の社員端末が標的型メール攻撃を受けてマルウェアに感染。インターネット経由のリモートアクセスにより姿勢制御やミッション機器制御に係る機密情報が窃取される。その後、衛星本体のアップリンクデータが乗っ取られ、窃取情報を使った不正コマンドが衛星に送られ、一時的に衛星の軌道制御を喪失する。	・ 衛星と地上局の間の通信 ・ インターネット	・ なりすまし・リプレイ攻撃 ・ 電子メールを介したマルウェア感染 ・ CNE（諜報・工作活動）	・ 諜報機関又は産業スパイ ・ セキュリティ意識の低い従業員	・ 機微情報の漏えい ・ 衛星制御の喪失
例2	開発製造用端末のマルウェア感染による衛星・ミッション機器制御の喪失	衛星本体のソフトウェア更新に使われる開発・製造用の端末（OAと兼用）がマルウェア感染したため、更新用プログラムに不正プログラム（バックドア）が埋め込まれ、地上からの遠隔操作により、正常な衛星の制御又はミッション機器の制御ができなくなる。	・ 衛星と地上局の間の通信 ・ インターネット	・ 地上からの不正な遠隔操作 ・ 電子メールを介したマルウェア感染 ・ CNE（諜報・工作活動） ・ バックドアプログラム	・ 諜報機関又は産業スパイ ・ セキュリティ意識の低い従業員	・ ミッション機器の制御の喪失
例3	衛星データ利用システムへのサイバー攻撃による衛星制御の喪失	衛星データ利用システムに設置された無許可端末がインターネット経由でサイバー攻撃を受け、システム内部へのインターネット側からの攻撃の起点となった結果、衛星運用を行う地上のインフラシステムを含めた各種サーバーがダウンし、長期間にわたり衛星の制御を失う。	・ インターネット	・ 未許可端末の接続に伴う不正侵入 ・ CNE（諜報・工作活動）	・ 諜報機関又は産業スパイ ・ セキュリティ意識の低い従業員	・ 衛星制御の喪失
例4	データ受付サーバーへの不正アクセスによるサービス提	データ受付サーバーがインターネット経由で不正アセスを受けてランサムウェアに感染。その後、サーバー環境の設定不備によりシステム内の全サーバー及び端末に感染し、起動に必要なシステムデータが消去されたために再起動できなくなり、サービスを提供できなくなる。	・ インターネット	・ Web アプリケーションに対する攻撃 ・ マルウェア感染（ランサムウェア、ワイパー攻撃等）	・ 諜報機関又は産業スパイ	・ 衛星サービスの提供不能

No.	シナリオ例	概要	侵入経路	攻撃手法	脅威源	影響
	供不能					
例5	テレワーク環境下でのメール攻撃による企業機密の漏えい	テレワーク実施中、同僚からのメール（実際は、普段、オフィスで隣に座る同僚を装った差出人詐称メール）の添付ファイルを開き、マルウェアに感染。インターネット経由のリモートアクセスにより衛星製造に関わる企業機密が窃取され、外部に漏えいする。	・ インターネット	・ 電子メールを介したマルウェア感染 ・ CNE（諜報・工作活動）	・ 諜報機関又は産業スパイ ・ セキュリティ意識の低い従業員	・ 企業秘密の漏えい
例6	無許可USBメモリの利用による操業停止	製造設備コントローラに対し、許可されていない私物のUSB メモリを使って設定変更を行ったため、USB メモリ内のマルウェアによって設定やプログラムが改ざんされ、設備の制御が異常となり操業が停止する。	・ クローズド環境における外部記録媒体	・ USB メモリを使ったことによるマルウェア感染 ・ BadUSB	・ 諜報機関又は産業スパイ ・ セキュリティ意識の低い従業員	・ 開発・製造システムの操業停止
例7	不正な衛星搭載機器の受入による衛星コンステレーション崩壊の危機	衛星搭載機器調達の際、不正な基板であることに気付かずに受入れて衛星群に搭載。打上げ後の特定条件成立によりロジックボムが起動し、衛星コンステレーションが崩壊の危機に直面する。	・ サプライチェーンにおける不正部品の調達・組込み	・ 受入検査を怠ったことによる不正基板の受入れ ・ 不正改造基板の製作	・ 諜報機関又は産業スパイ ・ セキュリティ意識の低い従業員	・ 衛星コンステレーション崩壊の危機
例8	VPNの設定不備を悪用したユーザーの衛星機能の喪失	VPN ルータの設定ミスを足掛かりに、衛星運用システムが不正アクセスを受ける。衛星運用システム内のシステムがマルウェアに感染した後、衛星ブロードバンド通信経由でマルウェアが衛星ユーザーに伝送され、通信衛星のサービスが利用できなくなる。	・ インターネット（VPN）	・ VPN ルータの脆弱性を悪用した攻撃 ・ マルウェア感染	・ 諜報機関又は産業スパイ	・ 衛星通信機能の喪失
例9	ユーザー端末の不正改	攻撃者が用意した通信装置に対して、攻撃者が用意した通信装置に対して不正なチップを取り付けることで、	・ 衛星と地上局の間の通信	・ ユーザー端末の不正改造	・ 諜報機関又は産業スパイ	・ 不正情報の伝送

No.	シナリオ例	概要	侵入経路	攻撃手法	脅威源	影響
	造による情報の不正送信	任意コードの実行が可能な状態にする。地上システムから衛星ブロードバンド通信経由で不正情報を伝送する。		・ 地上不正端末からの不正操作		
例 10	衛星通信の傍受による機微情報の漏えい	ユーザーに向けて平文で送信されている衛星のブロードキャスト通信に対して、公開情報を基に通信衛星の場所を特定し、攻撃者が用意したアンテナを用いて通信傍受する。傍受された機密情報が外部に漏えいする。	・ 衛星と地上局の間の通信	・ 攻撃用アンテナの用意 ・ 衛星ブロードキャスト通信の傍受	・ 諜報機関又は産業スパイ	・ 機微情報の漏えい
例 11	衛星放送に対するジャミングによるサービスの停止	通信衛星が衛星放送のために送受信している電波に対して、攻撃者の用意した機器が発する妨害電波によるジャミングが行われる。衛星放送通信が妨害され、衛星放送が停止される。	・ 衛星と地上局の間の通信	・ 攻撃用アンテナの用意 ・ 衛星ブロードキャスト通信のジャミング	・ 諜報機関又は産業スパイ	・ 衛星放送サービスの停止
例 12	内部犯による衛星制御のハッキング	衛星運用に関する従業員が、悪意を持ってシステムに管理者アカウントでログインする。ログイン後、不正なミッションを遂行するコマンドや、ミッション機器制御情報を悪用した不正コマンドを衛星に送信する。	・ 内部犯（特別な侵入なし）	・ 管理者アカウントでの不正ログイン ・ テレメトリ・データの傍受・解析 ・ 衛星本体への不正コマンドの送信	・ 内部犯	・ 衛星通信機能の喪失
例 13	ソフトウェアサプライチェーン攻撃による操業停止	ソフトウェアベンダーが侵害され、宇宙システム開発に利用する SDK のインストーラーにマルウェアが同梱され公開される。ソフトウェア更新を通じて、マルウェアを同梱するインストーラーを実行し、開発環境の端末やサーバーがマルウェアに感染する。	・ サプライチェーンにおける不正部品の調達・組込み ・ インターネット	・ CNE（諜報・工作活動） ・ インストーラーの改ざん ・ マルウェア感染 ・ ソフトウェア更新時のマルウェアチェック不備	・ 諜報機関又は産業スパイ ・ セキュリティ意識の低い従業員	・ 開発・製造システムの操業停止

整理したリスクシナリオ例について、Ver 2.0 で更新したモデル図に基づき、脅威の実行プロセスを整理した。例えば、リスクシナリオ例 8「VPN の設定不備を悪用したユーザーの衛星機能の喪失」における脅威実行プロセスは以下のように整理される。なお、このリスクシナリオ例は、2022 年に発生した Viasat 社 KA-SAT に対するサイバー攻撃をベースとしたリスクシナリオ例である。

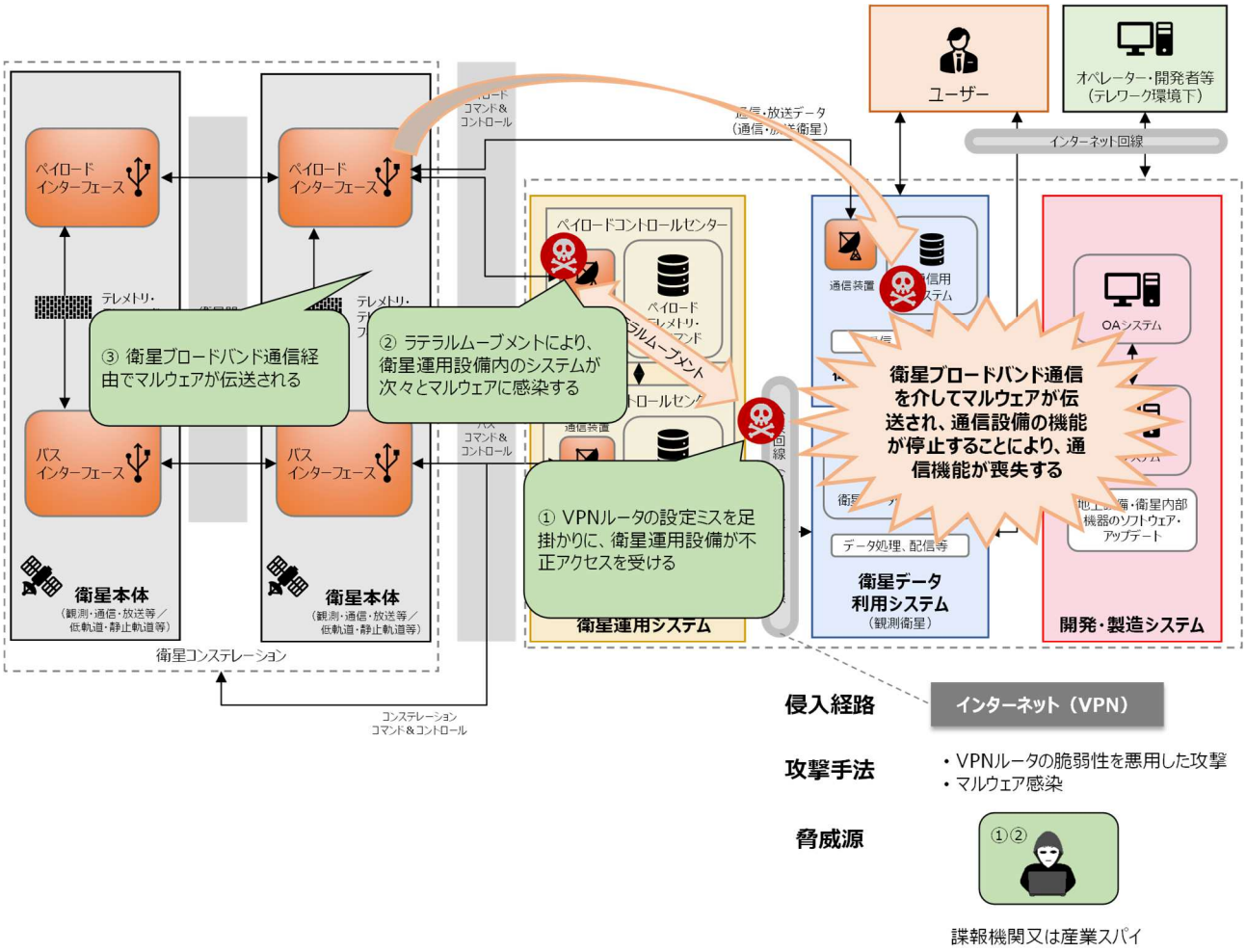


図 3-5 リスクシナリオ例：VPN の設定不備を悪用したユーザーの衛星機能の喪失

ガイドライン本編の 2 章では、その他、以下の内容に関する軽微な更新を行った。

- Ver 1.1 で示していたモデル図について、「観測衛星を分析対象とした場合の詳細モデル図例」として記載。【図 2-4】

（3）ガイドライン本編 3 章における更新内容

ガイドライン本編の 3 章における主要な更新内容は以下のとおりである。

- NIST CSF について、NIST CSF 2.0 の公開を踏まえて記載を修正。【3.1】
- 通信衛星・放送衛星に関して、インシデントが発生した場合の届出に関する情報を追記。また、法

令上求められる対策に関する情報を追記。【3.1.5】【3.2.1】

- 通信衛星・放送衛星に関して法令上求められる対策に関する情報を追記。【3.2.1】
- リモセン法に基づき求められる措置と、参考となる本ガイドラインとの対応関係を追記。【表 3-18】
- 衛星の通信の保護について、地上との RF 通信に限らず、光通信の場合や衛星間通信における対策の解説を追記。【3.2.1】
- 通信の暗号化について、CCSDS（宇宙データシステム諮問委員会）文書に基づく具体的な実装方法や実装に当たっての留意事項を追記。また、耐量子計算機暗号（PQC）に関する参考情報を追加。【3.2.2】
- SBOM に基づく脆弱性管理に関して、経産省の「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」に関する参照を追加。また、継続的な脆弱性管理に関する内容を追記。【3.2.2】
- 衛星システムのサプライチェーン・セキュリティ対策に関して、参考となる情報を追記。また、委託先のセキュリティ対策状況の確認に当たって、添付資料3内のチェックリストが活用可能であることを明記。【3.2.2、3.2.3、3.2.4】
- 衛星通信システム・衛星データ利用システムのセキュリティ対策に関して、複数のステークホルダーが関与する場合の責任分界に関する内容を追記。【3.2.4】

これらの主要更新内容のうち、暗号化に関する記載について、既存のガイドラインや基準等を参照し、宇宙システムにおいて留意すべき事項について追記を行った。特に、CCSDS 文書を中心に、以下に示す文書を参考資料として引用した。

- CCSDS:「CCSDS CRYPTOGRAPHIC ALGORITHMS (INFORMATIONAL REPORT), CCSDS 350.9-G-2」(2023 年 6 月)
  https://public.ccsds.org/Pubs/350x9g1.pdf
- CCSDS:「CCSDS CRYPTOGRAPHIC ALGORITHMS (RECOMMENDED STANDARD), CCSDS 352.0-B-2」(2019 年 8 月)
  https://public.ccsds.org/Pubs/352x0b2.pdf
- CCSDS:「SYMMETRIC KEY MANAGEMENT (RECOMMENDED PRACTICE), CCSDS 354.0-M-1」(2023 年 12 月)
  https://public.ccsds.org/Pubs/354x0m1.pdf
- CCSDS:「SPACE MISSIONS KEY MANAGEMENT CONCEPT (INFORMATIONAL REPORT), CCSDS 350.6-G-1」(2011 年 11 月)
  https://public.ccsds.org/Pubs/350x6g1.pdf
- CCSDS:「THE APPLICATION OF SECURITY TO CCSDS PROTOCOLS (INFORMATIONAL REPORT), CCSDS 350.0-G-3」(2019 年 3 月)
  https://public.ccsds.org/Pubs/350x0g3.pdf
- IPA:「暗号鍵管理ガイダンス」(2023 年 5 月)
  https://www.ipa.go.jp/security/crypto/guideline/ckms.html

- デジタル庁、総務省、経済産業省：「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」（2023 年 5 月）
  https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022.pdf
- デジタル庁、総務省、経済産業省：「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」（2022 年 3 月
  https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022r1.pdf
- NIST：SP 800-57「Recommendation for Key Management」
  https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final

暗号技術に関して、耐量子計算機暗号（Post-Quantum Cryptography: PQC）に関する言及も追加した。PQC について、2022 年 5 月には、量子コンピューターが米国のサイバーセキュリティに及ぼすリスクに対処するための米国政府の計画を示した国家安全保障覚書にバイデン大統領が署名したほか、米国 NIST は耐量子計算機暗号に関する標準化活動を 2016 年から実施しており、2022 年 7 月には標準化する方式の一部として 4 つの方式を決定し、2024 年中には正式な標準仕様が発表される見通しである。今後、宇宙分野においても耐量子計算機暗号への移行準備に動き出すことが想定されることから、参考情報として情報を追加した。

3 章では、衛星システムのサプライチェーン・セキュリティ対策に関する留意事項の追記も行った。以下に示すとおり、衛星のライフサイクルフェーズを整理し、各フェーズで留意すべきセキュリティ対策等を明記した。

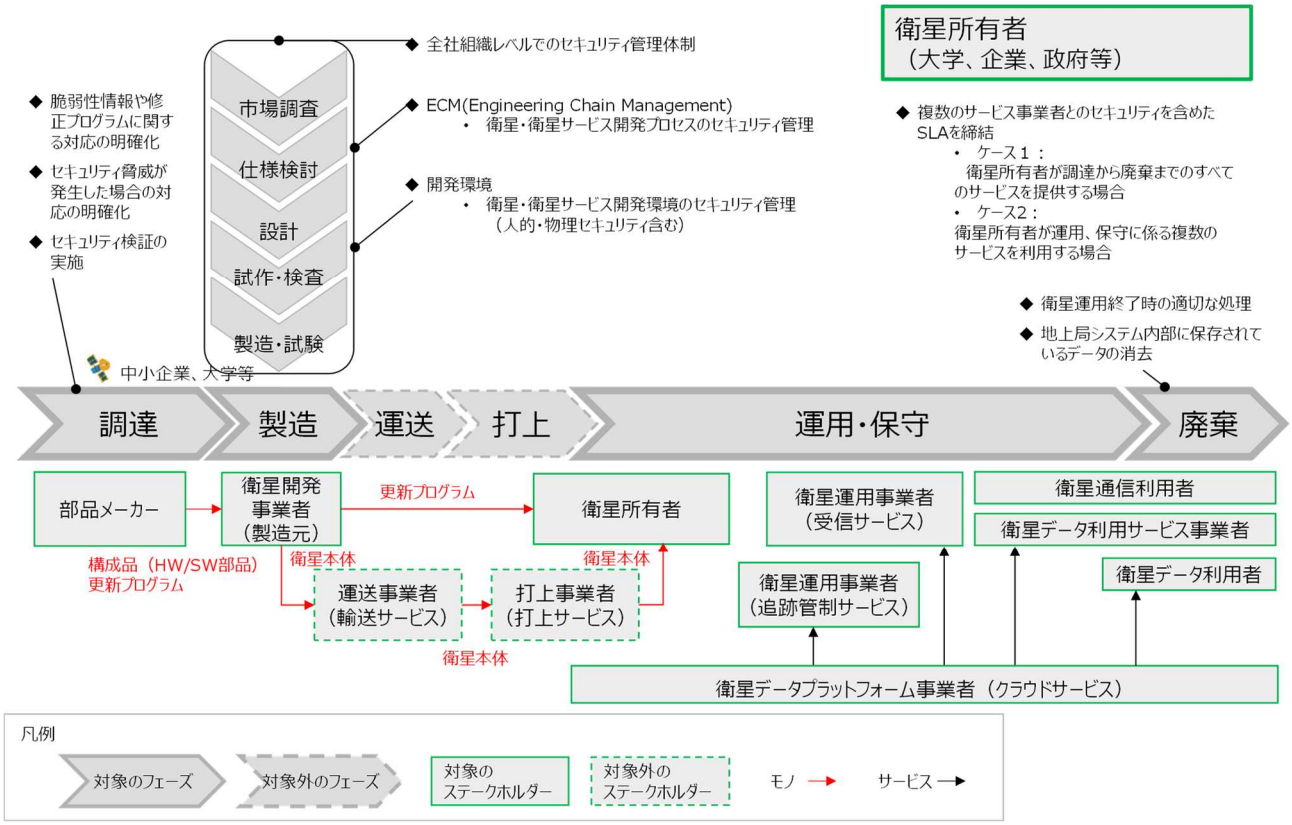


図 3-6 衛星のライフサイクルと調達時のサプライヤーに対するセキュリティ要件マッピング

ガイドライン本編の 3 章では、その他、以下の内容に関する軽微な更新を行った。

- 参照元ガイドラインの改訂を踏まえ、IPA 中小ガイドのバージョンを第 3.0 版から第 3.1 版に修正。【3.1】
- CMMC について、2023 年 12 月に発表された規則案の内容を踏まえた参考情報を追記。【コラム】
- ゼロトラストセキュリティに関して、米国の「ゼロトラスト戦略」を踏まえた参考情報を追記。【コラム】
- 米国 Aerospace Corporation の SPARTA に関する情報を追加。【コラム】

3.3.2 ガイドライン添付資料に関する更新内容

ガイドライン添付資料の内、以下について更新・新規作成した。

- 添付資料 1:対策要求事項チェックリスト
- 添付資料 2:NIST CSF と宇宙システム特有の対策との対応関係
- 添付資料 3:情報セキュリティ関連規程（サンプル）

添付資料 1「対策要求事項チェックリスト」について、ガイドライン本編の内容の更新を踏まえ、本資料の記載内容も修正した。

添付資料 2「NIST CSF と宇宙システム特有の対策との対応関係」について、2024 年 2 月に NIST

CSF 2.0 が公開されたことを踏まえ、NIST CSF 2.0 のサブカテゴリーとのマッピングを示す形式に修正した。

添付資料3「情報セキュリティ関連規程（サンプル）」について、宇宙産業においては、ベンチャー企業、新興企業も多数いることから、作業部会コアメンバーの一部の事業者社から社内のセキュリティ管理規程を作る際に参考となる資料の作成に対する要望が上げられた。作業部会コアメンバー会議の議論を踏まえ、民間宇宙事業者向けの情報セキュリティ関連規程のサンプルを作成した。本サンプルは、IPA「中小企業の情報セキュリティ対策ガイドライン」の付録 5「情報セキュリティ関連規程（サンプル）」をベースに、ガイドライン本編の内容等を踏まえた宇宙事業者特有の内容が追記し、整理した。また、各章の内容と NIST CSF 2.0 との対応関係を末尾にて整理した。

4. 情報共有のあり方等の検討

検討会等を踏まえ、宇宙システムのサイバーセキュリティに関する脅威・脆弱性・インシデント・対策等に関する情報共有、普及啓発のあり方等について検討を行った。

4.1 検討方針

昨年度の作業部会コアメンバー会議において、国内宇宙分野の情報共有体制の構築に向けた議論を行った。その結果、以下のような意見が挙げられ、早急に情報共有体制の設立を目指すのではなく、まずは定期的な勉強会の開催や対面での打ち合わせ等の取組から始め、信頼関係を醸成することが重要であることが示唆された。

- 情報共有体制の構築を前提とした議論ではなく、必要性の議論も必要であろう。
- 情報共有体制を構築することで、セキュリティ業界と宇宙業界の両方における情報共有の活性化が期待される。まずは協議会を立ち上げ、定期的に勉強会を開催したり対面での打ち合わせを設けたりといった取組から始めるのが良いと思われる。
- ベンチャー企業も含めた各民間宇宙企業の情報共有・分析に関するニーズをヒアリングすることから始めても良いのではないか。
- 信頼関係を醸成する中で、各社のニーズを掘り起こしていく必要がある。信頼関係が構築されれば、情報も出しやすくなる。
- 情報共有を行う上では、そこに参加している社のニーズが一致していることが重要となる。
- コアメンバー会議には様々な立場の事業者が参画しているため、まず各社のニーズを整理する必要がある。
- サイバーセキュリティに関する情報の共有だけではなく、各社が抱えている悩みや課題を共有する役割もあるのではないか。

これらの意見を踏まえ、一部のコアメンバー会議は対面を含む会議形式とするなど、信頼関係の醸成に向けた取組を進めてきた。今年度は、信頼関係の醸成を継続しつつ、より具体的な情報共有のあり方に関する検討に向け、ベンチャーを中心とする民間事業者にヒアリングを実施し、情報共有に関する課題やニーズを聴取した。そして、挙げられた課題やニーズを踏まえ、望まれる情報共有体制のあり方を整理した。

4.2 調査結果

国内宇宙分野の情報共有体制のより具体的な検討に向け、(1)事業者に対するヒアリング、(2)民間事業者を中心とした取組「スペースセキュリティ勉強会」に関するヒアリングを実施した。

4.2.1 事業者に対するヒアリング

セキュリティに関する情報収集について、民間事業者が抱える課題や要望を把握することを目的に、

作業部会コアメンバーの内、5 社の民間事業者にヒアリングを実施した。表 4-1 にヒアリング実施概要を示す。

表 4-1 情報共有体制に関するヒアリング実施概要

実施日	事業者区分	ヒアリング項目
2023 年 7 月 4 日	衛星事業者	・ サイバーセキュリティの情報収集に関する現状の取組について ・ 今後の情報共有体制の構築に関するニーズについて
2023 年 7 月 7 日	衛星事業者	・ サイバーセキュリティの情報収集に関する現状の取組について ・ 今後の情報共有体制の構築に関するニーズについて
2023 年 7 月 7 日	衛星事業者	・ サイバーセキュリティの情報収集に関する現状の取組について ・ 今後の情報共有体制の構築に関するニーズについて
2024 年 7 月 12 日	衛星事業者	・ サイバーセキュリティの情報収集に関する現状の取組について ・ 今後の情報共有体制の構築に関するニーズについて
2024 年 7 月 14 日	衛星事業者	・ サイバーセキュリティの情報収集に関する現状の取組について ・ 今後の情報共有体制の構築に関するニーズについて

表 4-2 にてヒアリング結果概要を示す。下表で示すとおり、一部の事業者では、情報収集に関する専任人材・チームを置き、情報収集を日常的な業務として行っている一方で、セキュリティに関する専門職がおらず、情報収集が困難な事業者もいることが明らかになった。事業者によって、取組段階に差異はあるものの、セキュリティに関して、収集すべき情報が多岐にわたっていることから、1 社での取組には限界があり、効率的に網羅的な情報収集が行える情報共有体制に対して、ニーズが示された。特に、脅威情報やインシデント情報のほか、他社においてガイドラインをどのように読み解いているか、基準に対してどの程度まで実装しているか等の各社が抱えている具体的な悩みについて、一定頻度で情報共有を望む事業者が複数見られた。このような踏み込んだ内容の情報共有を行うに当たり、個社間の信頼関係の醸成に加え、事業者間で TLP のような情報共有ルールを明示的に結ぶ必要がある旨が示唆された。また、宇宙に関連する情報共有体制の構築に当たっては、事業者間のビジネスのレイヤーが異なることから、レイヤーごとのグループ分けや全体共通のアジェンダの設定をするなどの工夫が必要である点に留意すべきであることが明らかになった。

表 4-2 ヒアリング結果概要

分類	質問項目	主な意見
サイバーセキュリティの情報収集に関する現状の取組	情報収集の頻度	• 専任の人材を置き、自社が扱うシステムを対象とし、定期的に（毎月～2 か月に 1 回）情報収集をしている • 専任の担当者は置いていないものの、自社が扱うシステ

分類	質問項目	主な意見
について		ムを対象とし日常的に情報収集をしている。 • セキュリティの専門職は現状おらず、セキュリティに関する情報を本格的に収集できていない。 • Space ISAC を主な情報収集源とし、1 日に 1 回メーリングリスト経由で情報収集をしている。 • セキュリティに関するチームを結成し、日常的業務の一環として情報収集をしている。
	情報収集の方法	• 主要なメーリングリスト • ニュースサイト • 有識者の SNS • 省庁、IPA、JPCERT/CC のホームページ • ベンダーの製品情報 • コアメンバー会議 • スペースセキュリティ勉強会
	情報収集の目的	• 社内システムや自社が関わるシステムの安全性の維持 • 脅威動向の把握 • 他業界の動向の把握 • ガバナンスの強化
	自社で収集が困難な情報	• 国内外問わず、政策・規格・規制動向に関する情報 • OSS に関する網羅的な情報 • 自社に関連するシステムに関する網羅的な情報 • 他社の取組内容（制度に対する対応状況、製品の選択方法、導入製品）に関する情報
	自社での情報収集における具体的な課題	• セキュリティ分野のカバレッジが広く、特定の情報を集めたとしても十分性、網羅性が担保されない • 宇宙産業とサイバーセキュリティに関する両方の知見が必要となるが、業界全体として両方に対応できる人材は限られている
今後の情報共有体制の構築に関するニーズについて	共有されると有益な情報	• 各社の悩みや課題 • 脅威情報、インシデント情報 • 制度・ガイドラインに対する対応状況 • システムアーキテクチャの設計や、関連する脅威動向や制約事項 • オペレーションにおける具体的なプラクティスの共有
	他社に展開可能な情報	• 情報共有ルールが適切に設定されていれば、自社の対策状況、脅威・インシデントに関する情報開示が可能 • 自社が収集している情報について情報開示が可能
	望ましい情報共有	• ビジネスのレイヤーが異なることで関心がある情報に差

分類	質問項目	主な意見
	の頻度・場	が出るため、同じようなレイヤーの事業者間での情報交換ができるような場となると望ましい • 多様なレイヤーに対応できるようなアジェンダを設定すると、情報共有に参加できる企業が増えて良い • グローバル対応できるよう、海外の事業者も対象とできると良い • 信頼関係の構築が課題であり、いきなり脅威情報を紹介することは難しいため、各社の悩み等を共有する場から、脅威情報の共有等を検討することができる場にグレードアップしていくのが良い • 負担にならない頻度で定期的に開催することが妥当（例：4 半期に 1 回～半年に 1 回程度、2 か月に 1 回程度）
	情報共有ルール	• TLP などの適切な情報共有ルールの設定

4.2.2 民間事業者を中心とした取組に関するヒアリング

宇宙分野におけるセキュリティに関する情報共有について民間事業社を中心に活動を行うコミュニティ「スペースセキュリティ勉強会」[1]に、現状の取組内容や、課題、今後の展望について伺うことを目的に、ヒアリングを実施した。

【スペースセキュリティ勉強会に対するヒアリング結果概要】

- スペースセキュリティ勉強会には、宇宙分野における主要なベンチャー企業が参画している。
- 脅威動向、情報システム、情報セキュリティ、宇宙システムに関する情報を共有している。今年度アンケートを実施しており、脅威動向の情報共有に関しニーズがあることが明らかになった。
- 今後は、社団法人化を目指しており、海外の Space ISAC をベンチマークにしようとしているが、規模や、ニーズを考慮する必要があると考える。個社のニーズに加え、省庁関係（内閣府、経済産業省、官民協議会等）のニーズも汲み取り総合的にまとめていく必要がある。
- 脆弱性情報や脅威アクターに関する情報を効率的に情報収集したい。大手企業が参画することにより情報共有が加速度的に向上することが期待されるものの、どのように大手企業のニーズを拾い上げるかが課題である。
- 宇宙×サイバーセキュリティの将来像を描く必要がある。その上で、ISAC の構築に必要な手続きや取組について整理したい。また ISAC 構築について既定路線があれば知りたい。立ち上げ期にどのような組織体制を取ることが望ましいのか（法的な社団法人として設立するのが良いのか等）、他機関とはどのような連携体制を構築するのが良いのか等、立ち上げ時に必要な手続きが確認

[1] https://sites.google.com/view/space-sec-japan/top

できると良い。

4.3 情報共有のあり方に係る検討結果

これまで、宇宙産業 SWG や作業部会等において、情報共有体制構築の必要性の認識を醸成するとともに、コアメンバー会議の場等を活用し、限定した関係者間で、国内外動向等に関する情報の共有を行ってきた。以下に示すとおり、次のステップとしては、より開いた関係者間で情報共有体制の必要性を認識するとともに、国内外動向に関する情報共有だけでなく、各社の悩み、課題、プラクティス等、より踏み込んだ情報の共有を検討すべきである。あわせて、将来的により高度な内容の情報（具体的なセキュリティ対策内容、脅威、インシデント等）の共有が実施できるよう、事業者間で情報共有ルールの策定が望まれる。これらの検討においては、民間事業者を中心とした取組である「スペースセキュリティ勉強会」[2]等と目指す方向性や目的が近しいことから、協力して進めることが現実的である。よって、引き続き宇宙産業 SWG や作業部会を通じた情報共有を図るとともに、民間事業者中心の取組に対する政府の支援を検討することで、国内の情報共有体制構築に向けた取組を進めていくことが望まれる。

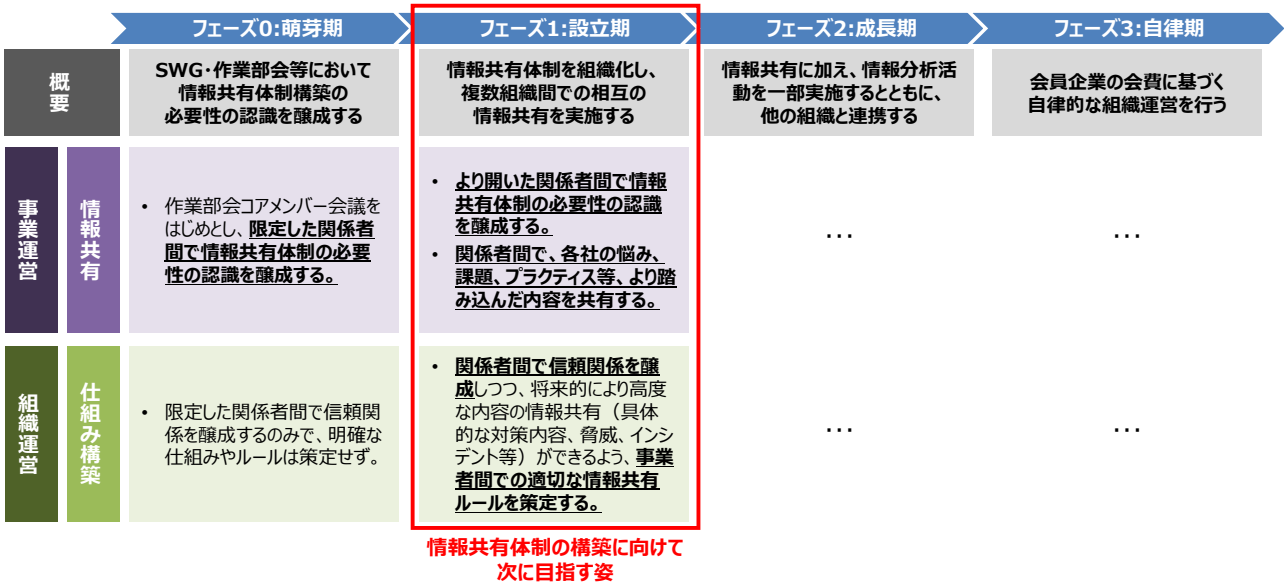


図 4-1 情報共有体制の構築に向けた検討ステップ

[2] https://sites.google.com/view/space-sec-japan/top

5. 総括

本事業では、「宇宙産業 SWG」及び「宇宙産業 SWG 作業部会コアメンバー会議」を開催し、これらの検討会等での議論を踏まえ、民間宇宙システムにおけるサイバーセキュリティ対策ガイドラインを更新した。今年度の更新では、ガイドラインの対象とする衛星システムのスコープを拡大したほか、添付資料の位置づけで、民間宇宙事業者が活用できるセキュリティ関連規程の雛形を追加した。さらに、国際的な動向を踏まえつつ、具体的な対策内容について追記した。ガイドラインに記載のとおり、国内外の最新知見や動向を踏まえ、今後も 1 年に 1 回程度の見直しを図っていくことが重要となる。

また、検討会等を踏まえ、宇宙システムのサイバーセキュリティに関する情報共有のあり方について検討を行った。これまで、検討会等において、情報共有体制構築の必要性の認識を醸成するとともに、コアメンバー会議の場等を活用し、限定した関係者間で、国内外動向等に関する情報の共有を行ってきたが、今後、民間事業者を中心とした取組である「スペースセキュリティ勉強会」等と連携しつつ、より踏み込んだ内容の情報共有を促進していくことが望まれる。あわせて、将来的により高度な内容の情報（具体的なセキュリティ対策内容、脅威、インシデント等）の共有が実施できるよう、事業者間で情報共有ルールの策定が望まれる。

これまで、宇宙産業 SWG ではガイドラインの整備・更新と情報共有体制の構築に係る検討を中心に取り組んできた。国内の宇宙セキュリティに関する取組としては、ほかにも、上述した「スペースセキュリティ勉強会」等の民間主導の取組があるほか、官主導の取組として、「宇宙システム安定性強化に関する官民協議会」等も挙げられる。国内宇宙事業者のセキュリティ対策を支援し、高度化する目的では、これらの取組が連携して相互作用を発揮することが必要であり、現状の取組状況を整理しつつ、将来的に求められる取組の全体像を整理することが必要と考えられる。この整理に当たっては、サイバーセキュリティ対策の義務化等、規制の観点も検討要素となりうるが、規制化の検討に当たっては、民間宇宙事業者のビジネス上のリスクも考慮しつつ、事業者の産業競争力を阻害しないよう、事業者と適切にコミュニケーションを取ることが重要となる。また、国際的な動向を継続的に調査しつつ、国際的な水準に劣後しない形での検討が必要となる。

令和5年度産業サイバーセキュリティ強靭化事業

（IoT機器や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

2024 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5年度産業サイバーセキュリティ強靭化事業
（IoT機器や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

2024年3月29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」について、スマート工場において新たに求められるセキュリティに関して必要な事項を整理し、別冊として取りまとめた。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」の普及・啓発を実施した。

これらの調査を進めるにあたって、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）」の開催や資料の取りまとめ等を実施した。さらに、今年度は、工場 SWG の下に有志による「作業部会」を設置し、「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】」の策定に向けた議論を行った。

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する。

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

工場セキュリティに関する国内外の政策・技術動向を踏まえ、スマート工場において新たに求められるセキュリティ要件をシステム及び人材の観点から明らかにし、システム計画・構築から廃棄までのライフサイクルにおいて必要な事項を整理するとともに、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」の普及・啓発を実施した。

2.1 「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」別冊の策定に関する調査

2.1.1 ガイドライン別冊の策定作業

スマート工場において新たに求められるセキュリティ要件を中心にまとめた「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：スマート化を進める上でのポイント】」（以降、ガイドライン別冊）を策定した。策定に当たり、業界団体・企業へのヒアリング、作業部会での意見、スマート工場に関する調査で得られた事項を考慮した。

（1） 業界団体・企業へのヒアリング

ガイドラインの別冊の作成に当たり、工場スマート化の取り組みを進める企業業界団体に対して計 11 件のヒアリングを行った。ヒアリング調査の概要を表 2-1 に示す。

表 2-1 業界団体・企業ヒアリングの概要

カテゴリ	内容
調査対象	工場のスマート化の取組を進める企業や業界団体
ヒアリング件数	11 件
調査項目数	6項目
調査項目	1. 工場のスマート化に向けた対応（仮説）について ・ 貴業界（主要な企業）／貴社における工場のスマート化の状況 ・ 「工場のスマート化に伴うリスクを管理していくための考え方の仮説」についてのご意見 ➢ スマート化に関する状況、及びセキュリティに関する懸念の有無・対応 ➢ スマート化（自動化）が進む中でのセキュリティインシデント対応の想定（人材、組織、ルール等） ➢ クラウドサービス事業者・調達先等、外部連携先との責任分界や役割分担　　等 ・ 上記以外の工場のスマート化におけるセキュリティに関する課題・ニーズ

	・ スマート化の観点から、「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」への記載が望ましい事項 2. デジタルツイン・制御の高度化に関する現状とセキュリティ課題について 3. ガイドライン拡充に関する検討を行う作業部会（工場 SWG の下に設置）へのご参画や意見出しについて
調査期間	2023 年 6 月～2023 年 7 月

上記のヒアリング得られた意見を以下に示す 7 つの項目で分類し、それぞれ対応方針を整理した。

① 全般
② 接続
③ クラウド
④ 汎用品・データ
⑤ インシデント対応
⑥ 役割分担
⑦ その他

分類、整理したコメントに対する対応方針を以下に報告する。

1） 全般

表 2-2 工場のスマート化における全般に関する意見と対応方針

No	ご意見	対応方針
1	• スマートファクトリーについては、この先こうなるという絵姿を入れてほしい。例えば、クラウドに載せなくてもエッジで処理できることが増えている中、どのような処理を内部で実施し、どこを外部に出すかをそれぞれで判断し、その上で、ゼロトラストやゾーンを考えていくことになるのではないか。	• スマートファクトリーの現状を踏まえつつ将来像を示すとともに、技術の進展と合わせ BC/SQDC/セキュリティの観点も踏まえて、システム全体のデザインを行い、その中で内部/外部の判断、ゾーンの考え方を記載する。
2	• 現場で AI を活用したいニーズがあれば、そのヒントになるような情報があるとよい。	• スマート化の目的（課題の把握・対策等）に応じた対策の考え方を示す。
3	• 国がガイドラインをどのように活用してほしいのかを書けると良い。日本の製造業に何を求めているかを明らかにしてほしい。	• セキュリティを考慮した DX、スマート化の推進のためのガイドである点について記載する。
4	• スマート化を目指す上で、工場側のシステムの構築思想を整理したい。安全に外部と繋げていく前提で、システムの中身をどう構築するべきかを検討している。	• No.1 と同様。
5	• 設備に応じたガイドラインがあれば事業者はガイドラインを使うイメージを	• 設備は個社毎に様々であるので、スマート化の目的に応じた対策の考え

	持ちやすくなると考える。	方を示す。

2）接続

表 2-3 工場のスマート化における接続に関する意見と対応方針

No	ご意見	対応方針
1	• DXと言われる部分は相当進めている。社内では、OTとITをどのようにつなげるかが主な検討内容である。	• OTとIT等、異なるセキュリティが求められるゾーン間の接続における留意点について記載する。
2	• インダストリアルDMZやマイクロセグメンテーションを社内向けガイドラインの中で記載しており、まさにこれから具現化するところである。	• ゾーン設計の考え方と、異なるセキュリティが求められるゾーン間の接続における留意点について記載する。
3	• 工場のライン上で自動化を進めているが、繋ぐ区間のセキュリティはどのように担保するか。	• No.1と同様。
4	• 外部と繋げる場合、セキュリティ確保に向けてどのような回線を使うのか検討を行う。ソリューションはゼロトラスト関連のものが多く、最新のものを導入すべきなのか、限定して利用するか、メーカーが提供するソリューションも複数あり、どれが良いのか判断が難しい。	• No.1と同様。
5	• 外から制御側が操作する場合のセキュリティをどう進めるかが今後の検討課題である。	• 外部から制御を行う場合のセキュリティの考え方を示す。
6	• AGV、自動搬送機、ワイヤレスで繋がっており、どのようなセキュリティ対策が実際にできるか、今後勉強しながら導入したいと考えている。	• ワイヤレス利用の際のセキュリティの考え方を示す。

3）クラウド

表 2-4 工場のスマート化におけるクラウドに関する意見と対応方針

No	ご意見	対応方針
1	• 出口自体がクラウドということも多く、クラウド側にどのようにデータを持って行くのか、またクラウド上の情報をどのように取り込むかが課題となる。	• クラウド利用時のセキュリティに関する確認事項について記載する。
2	• 現場からまだニーズはないが、クラウドに情報を出すならどういうルートで出すか、クラウドから情報を装置に戻すのであれば、どのように行えるかが今後の検討課題である。	• クラウド利用時のゾーンの考え方を示す。
3	• 制御系、情報系のネットワークとは別に、無線センターと無線センサー用の別の通信手段、外部のクラウドを使用できるよう環境を整備している。情報の一部が外部のクラウド上に保管されているが、	• クラウド利用の際のデータに関するセキュリティの考え方を示す。

	設備の状態に関するデータは、運転・制御に係る情報ではなく機微情報ではないので、クラウドに載せたとしてもセキュリティ上の懸念はしていない。	

4）汎用品・データ

表 2-5 工場のスマート化における汎用品・データに関する意見と対応方針

No	ご意見	対応方針
1	• 汎用品において、コストとセキュリティの確保はトレードオフであり、今後の検討課題と認識している。	• 汎用品を利用する際のセキュリティ対策の考え方を示す。
2	• 業務効率化を目的としたタブレットの導入や、設備管理を目的としたセンサーを試験的に導入している。これらは市販品でありブラックボックス状態ではあるが、外部とつなげていないため、特にセキュリティ上の懸念は抱いていない。	• 汎用品のセキュリティ対策については、外部接続との関係においても記載する。
3	• トレーサビリティを確保する必要性がある。IT 側から OT 側へのフィードバックループの信頼性を確保するために、データの品質、改ざんされていないか等も、今後の検討課題として認識している。	• フィードバックの際のデータ品質の確保について記載する。
4	• メンテナンスの際、どこまでデータを見られているか、データを取られているかは懸念している。確認すればよいのだろうが、セットで導入されるケースもある。	• メンテナンスのためのデータ利用時のセキュリティに関して、契約時の確認事項を記載する。

5）インシデント対応

表 2-6 工場のスマート化におけるインシデント対応に関する意見と対応方針

No	ご意見	対応方針
1	• インシデント対応として、CSIRT 規則を作った。会社の危機管理対策規定では、サイバー攻撃があった場合、情報系の対応は従来から含まれていたが、制御系について、工場の生産や安全の確保を優先し、工場側が手動で止める権限を有することを規定した。	• インシデント対応の際の、制御側・情報側の役割分担について記載する。
2	• インシデントが起きた場合、社内の情報系に連絡を行うが、メーカーにも報告する。デバイスや制御装置を作っているメーカーに対しても指導が必要である。	• インシデント発生時のメーカーに求める対応や、保守契約内容について記載する。
3	• 現状、方法を模索しながらサイバーセキュリティ対策の訓練を行っている。ケーススタディを例示していただけるとありがたい。	• 運用時のインシデント対応の考え方や留意点等を記載する。

6）役割分担

表 2-7 工場のスマート化における役割分担に関する意見と対応方針

No	ご意見	対応方針
1	• 責任分界について、検討することは非常に重要である。スマート化により、社内外のプレーヤーが増えたり変わったりすることが予想される。その際、責任範囲や責任を取る主体を切れ目なく検討することは難しい。	• 責任分界の考え方や、主なケース毎の対応について記載する。
2	• 情報システム、生産技術、工場現場で新たな組織を立ち上げた。ベンダーとの利用条件等を含んだ契約時においては、新設組織と外部のベンダーが協力し、システムの導入やどの機器にどうつなぐか等を協議している。	• ベンダーとの契約条件や留意点について記載する。
3	• 制御系の部門と情報システム系の部門があり、社内規則によってハード系とソフト系で社内の役割分担を行っている。 • 制御系と情報系は FW で介しており、役割分担もそれに準じている。制御システムについては、クラウドサービスを現在利用していないため、制御システムに関する管理は、現場の担当者が管轄している。	• 制御側・情報側の役割分担について記載する。
4	• 様々な箇所に監視カメラを導入している。カメラは工場内にあり、ローカルネットワークに繋いでいる。カメラは警備会社が監視しており、警備会社のネットワークと繋いでいる。	• 外部委託の対象に警備会社も想定する。
5	• サプライチェーン上のつながりから、取引先におけるセキュリティ対策の重要性の強調をお願いしたい。（取引先に要請する際に活用できる）	• 取引先におけるセキュリティの重要性を記載し、責任分界に関する考え方を記載し、契約条項として記載する。
6	• 納品機器は IEC62443 がベースで作るものは変わらないが、周辺のロボット・搬送装置・プログラムなどのソフトウェアを構築するにあたって、顧客システムと自社のインターフェースの責任をどのように分けるかが課題である。	• 顧客システムと機器の責任分担の考え方について記載する。
7	• 特に中小企業とのコミュニケーションにおいては苦労することも多く、責任分界に関する基準を提示してもらえるとコミュニケーションを取りやすくなると考える。	• No.5 と同様
8	• IEC62443 の考え方、すなわちセキュリティ対策は誰か一者だけで進めるものではなく、使う側も調達する側も含めそれぞれが実施するものである点について普及してほしい。	• No.5 と同様

7）その他

表 2-8 工場のスマート化におけるその他に関する意見と対応方針

No	ご意見	対応方針
1	• セーフティーの観点が抜け落ちてしまうおそれがある。セーフティー機能があるところをバイパスしてしまうことが懸念される。	• SQDC の観点はガイドでも取り込んでいるが、改めて脅威と対策の検討においては、セーフティーに留意して記載する。
2	• セキュリティ製品に関する情報が氾濫している。どの製品を使うのが良いかを判断することが難しい。適切な判断を後押しすることができるような書きぶりがあることが望ましい。	• 特定の製品の推奨はできないが、有効な対策や機能等、可能な内容を記載する。
3	• 経営者が社内にセキュリティ対策に関する組織体制を検討する際に、検討を後押しできるような取り組みを具体的に示してもらえると良い。	• 経営者が実施すべき組織体制の構築に関する事例等について記載する。
4	• ユーザ側がラインの停止を懸念してパッチを当てないことがある。実験実証用のラインを持てるような業界は持つよう推奨し、そうではない場合、仮想で検証してパッチを当てることを推奨する書きぶりにすると良いか。	• 運用時のパッチ対応の考え方や留意点等を記載する。
5	• 中国で PLC のセキュリティ認証が始まる等、各国の規制にそれぞれ対応しなければならない状況において、メーカーの負担を軽減するような国の施策があると望ましい。経済安全保障の関係でも、製品の保護のために必要なのではないか。	• 今後の工場セキュリティに関連する政策の検討において参考とする。
6	• メーカーの製品や技術の見極めが困難である。ガイドラインや決められた規格に準拠しているなどがあると工場側は導入しやすくなる。	• 今後の工場セキュリティに関連する政策の検討において参考とする。
7	• ある程度の企業になると、自社でガイドラインを作成している。IEC 62443 を参照にしながら、自社でガイドラインを作成した。まだ取り組みが進んでいない中小企業などに対しては、ガイドラインの普及を通じて、セキュリティ確保の取り組みを推奨する必要があると考える。	• 引き続き、ガイドラインの普及啓発を進めていく。

（2）作業部会の実施

スマート化を進める業界・企業におけるニーズ等のヒアリング調査結果を踏まえ、工場のスマート化におけるセキュリティについて関心の高いメンバーによる作業部会を構成し、さらなる課題の深堀や具体的な対策の検討を進めた。計 3 回の会合での議論と 1 回の書面レビューを行い、ガイドライン別冊に関する内容を検討した。

表 2-9 作業部会の概要

カテゴリ	内容
活用目的	スマート化を進める企業等におけるセキュリティ課題や対策の実態等についての、ガイドライン別冊への反映
活動内容	ガイドライン別冊に関する検討・執筆支援、レビュー
メンバー	• 工場 SWG の委員を中心とした、工場セキュリティについて関心の高いメンバー有志 • メンバー形態は以下の 2 形態 ➢ コアメンバー：会合における議論・原稿執筆支援が中心 ➢ メンバー：メール等を通じた原稿レビュー・確認が中心（会合参加は任意）
実績	• 会合開催（対面及びオンライン） ➢ 第 1 回：令和 5 年 10 月 30 日 ➢ 第 2 回：令和 5 年 11 月 22 日 ➢ 第 3 回：令和 5 年 12 月 6 日 • 書面レビュー：令和 5 年 12 月 28 日～令和 6 年 1 月 12 日

（3）スマート工場に関する調査結果からの検討事項

スマート工場に関する調査結果より、以下の 3 点についてガイドライン別冊で検討を深めた。

- サイバー攻撃の早期認識と対処における役割分担
- スマート化による多様な変化に対応できる PDCA サイクルを回す上での考え方
- 外部機器やサービス導入の際に提供先企業に確認すべき内容

1） サイバー攻撃の早期認識と対処における役割分担

ガイドライン別冊では、サイバー攻撃の早期対処と対処における役割分担の重要性を示すとともに、予防保全段階・被害発生段階の 2 つの段階における役割分担の具体例を以下の通りに示した。

表 2-10 サイバー攻撃の早期認識と対処における役割分担例（予防保全段階）

	主な担当部署	意思決定者	実施内容の例
監視 （Observe）	ベンダー、セキュリティ担当部署	-	• 導入している機器の脆弱性情報の収集 • 導入している機器の脆弱性情報に関する連絡
分析 （Orient）	セキュリティ担当部署	• セキュリティ担当部署の責任者	• 脆弱性の悪用可能性の分析 • 脆弱性を悪用された場合、工場に与える影響度合いの分析
決定 （Decision）	セキュリティ担当部署	• 経営者（重要度に応じて） • セキュリティ担当部署の責任者 • 工場長、現場責任者	• 脆弱性に対する対策の検討 • 対策を実施した場合の稼働への影響の分析 • 対策実施の決定
行動 （Action）	製造現場	• 工場長、現場責任者	• 対策の内容に応じて、現場に対策を指示 • 現場に指示された内容に応じて実施

表 2-11 サイバー攻撃の早期認識と対処における役割分担例(被害発生段階)

	主な担当部署	意思決定者	実施内容の例
監視 (Observe)	製造現場	• 工場長、現場責任者	• 通常時と比較した違和感とその理由について都度報告 • 工場システムの構成要素の把握と更新
分析 (Orient)	報告内容に応じて適切な部署	• BCP 担当部署の責任者 • セキュリティ担当部署の責任者	• 報告事象が工場に与える影響度合いの分析 • 報告事象の原因がセキュリティによるものかの分析
決定 (Decision)	セキュリティ 担当部署	• 経営者(重要度に応じて) • セキュリティ担当部署の責任者 • 工場長、現場責任者	• 報告事象に対する対策の検討 • 対策を実施した場合の稼働への影響の分析 • 対策を実施の決定
行動 (Action)	製造現場	• 工場長、現場責任者	• 対策の内容に応じて、現場に対策を指示 • 現場に指示された内容に応じて実施

2) スマート化による多様な変化に対応できる PDCA サイクルを回す上での考え方

ガイドライン別冊では、変化が多い工場のスマート化において、PDCAサイクルを回す上で有効的な取り組みの例を以下の通り示した。

- セキュリティ対策やインシデントレスポンスなどのマニュアル化
- サイバーセキュリティに対応可能な人材育成
- PDCAサイクルを回せる組織体制の構築
- PDCA サイクルの体制に、製造現場の責任者などの製造に関する関係者を組み込む

特に PDCA サイクルを回す組織・人材を育成する上での成熟度モデルの重要性について検討し、以下の通り、組織・人材の成熟度モデルの例を示した。

表 2-12 組織・人材の成熟度モデルの例

組織	成熟度レベル		
	基本	実践	応用
社内外組織連携	例)社内外組織での情報共有	• 例)実践的なインシデントを想定し社内外組織での対応確認	• 例)高度インシデント(未知、複合)のでの社内外組織での対応確認
関係部署関連	例)社内部署間での情報共有	• 例)実践的なインシデントを想定し複数組織での対応確認	• 例)高度インシデント(未知、複合)の複数組織間での対応確認
当該部署内	例)当該部署内でのインシデント対応方法の確認	• 例)実インシデントを想定した当該部署内での行動確認	• 例)高度インシデント(未知、複合)の当該部署内での対応確認

3）外部機器やサービス導入の際に提供先企業に確認すべき内容

ガイドライン別冊では、外部機器やサービスを導入する際の確認すべきポイントを具体的に示した。クラウド・汎用品・ソフトウェアという 3 つの項目について、調達・契約・開発・運用保守の観点で、確認すべきポイントを以下の通り示した。

表 2-13 クラウド利用時に確認すべきポイント

	確認すべきポイント
調達	• クラウドサービス事業者の信頼性が高いか • クラウドサービス利用時のサポートは提供されているか • 自社とクラウドサービスのセキュリティポリシーに矛盾がないか • クラウドサービスに付随して機器・サービスが導入されるか
契約	• サービスの稼働率、障害発生頻度、回復目標時間などのサービスレベルが示されているか • 仮にサービスが終了した場合のデータの取り扱い条件は設定されているか
運用・保守	• クラウドサービスと業務の切り分けや運用ルールを明確化しているか • クラウドサービスで取り扱う情報の機密性は確認しているか • クラウドサービスの利用方法を理解している担当者がいるか • クラウドサービスのユーザを適切に管理しているか • クラウドサービスとの通信を遮断した際の稼働及びデータ復旧プランを準備しているか • クラウドサービスが停止した際のバックアッププランを準備しているか • クラウドサービスを介して調達先や他社のネットワークと接続されているか

表 2-14 汎用品利用時に確認すべきポイント

	確認すべきポイント
調達	• 製品セキュリティポリシーが策定・開示されているか • 製品セキュリティサポート方針が明示されているか • 製品セキュリティを維持するための体制（サポート窓口、脆弱性報告の受付窓口、インシデントへの対応体制等）が整備されているか • 製品セキュリティを確保するための機能（アップデート機能、初期化機能等）があるか • 基準に則ったセキュリティチェックや検証が行われているか • 製品及び構成要素の脆弱性情報が収集されているか • 製品のセキュリティ機能や設定に関する情報が確認できるか • 製品以外に付随して機器・サービスが導入されるか
契約	（汎用品のため、契約等で縛ることが難しいことを想定）
運用・保守	• 導入されている製品を管理できているか • 製品が利用されている業務の重要性に応じて、追加でセキュリティ対策を実施しているか • 製品の脆弱性情報を逐次確認し、必要に応じて対応しているか • 脆弱性の確認・対応できる体制は構築できているか • 製品のサポート切れや販売中止となった場合のバックアッププランは準備しているか

表 2-15 ソフトウェア利用時に確認すべきポイント

	確認すべきポイント
調達	• ソフトウェアに関するセキュリティポリシーを確認できるか • セキュリティを維持するための体制（サポート窓口、脆弱性報告の受付窓口、インシデントへの対応体制等）が整備されているか • ソフトウェアのセキュリティを確保するための機能（アップデート機能、初期化機能等）があるか • 基準に則ったセキュリティチェックや検証が行われているか

	• ソフトウェア及び構成要素の脆弱性情報が収集されているか • ソフトウェアのセキュリティ機能や設定に関する情報を確認できるか • ソフトウェアに付随して機器・サービスが導入されるか
契約	• セキュリティサポート方針が明示されているか • ソフトウェアに不具合が発生した場合のサポートについて明示されているか • ソフトウェアの構成要素の開示について明示されているか • ソフトウェアのライセンス情報について明示されているか
開発	• ソフトウェアで使用する OSS 含めた構成要素を管理できているか • ソフトウェアの構成要素のライセンスを管理できているか • 日々の脆弱性管理、必要なセキュリティ対策の実施が実施できる体制が構築できているか
運 用・保守	• 導入されているソフトウェアを管理できているか • ソフトウェアが利用されている業務の重要性に応じて、追加でセキュリティ対策を実施しているか • ソフトウェアの脆弱性情報を逐次確認し、必要に応じて対応しているか • 脆弱性の確認・対応できる体制は構築できているか • ソフトウェアがサポート切れとなった場合のバックアッププランは準備しているか

2.1.2 ガイドライン別冊の概要

現行の「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」は、各業界・業種が自ら工場のセキュリティ対策を立案・実行することで、産業界全体、とりわけ工場システムのセキュリティの底上げを図ることを目的として作成した。一方で、工場のスマート化が進展するにつれ、制御システムにおけるシステムアーキテクチャの変化やサプライチェーンによる脅威の増加など、既存の工場にはない要素が見られるようになってきた。そのため、スマート化によって工場がクラウドやデジタルツインといったサイバー空間に密接に繋がっていく世界におけるセキュリティのあり方を検討することが必要であるとの課題意識の下、ガイドライン別冊を作成した。

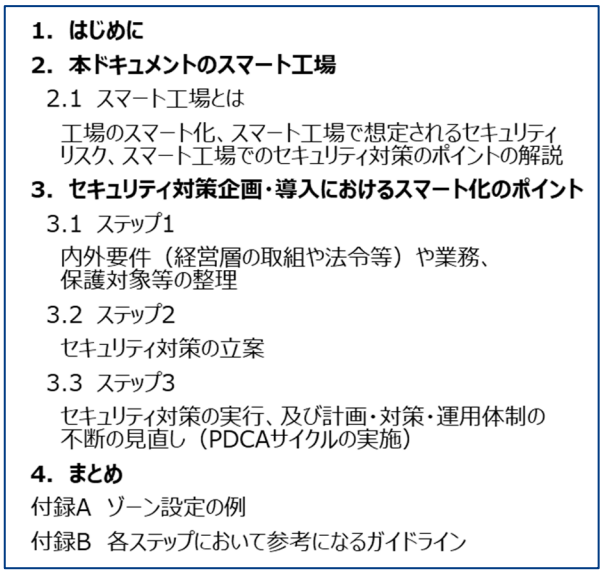


図 2-1 ガイドライン別冊の目次

本ガイドライン別冊の目的は 2 点ある。1 点目は、先進的な事業者が臆することなく工場のスマート化

を進め、工場の価値創造を促進することを後押しすることである。

2 点目は、業界としてのセキュリティ向上の取組や、海外におけるセキュリティ対策推進の具体的な事例を提示し、近年さらに強まっているセキュリティの必要性を訴えることである。

工場のスマート化を先進的に進める業界（例：半導体業界等）では、サプライチェーンにおいて取引先に対するセキュリティ対策を要請している。また、国内外において、機器に対するセキュリティ確保の取組（例：米国 U.S. Cybersecurity Labeling Program for Smart Devices、EU Cyber Resilience Act、日本 IoT 製品に対するセキュリティ適合性評価制度　等）が推進されており、セキュリティ対策の必要性は工場システムにも求められてくると考えられる。

ガイドライン別冊では、スマート工場の概要を示すとともに、ガイドライン本編 3 章に示した各ステップの対策におけるスマート化を進めるにあたっての留意点や具体例を示した。各ステップの青枠にポイントを示すとともに、緑枠にガイドライン本編の記載内容の概要を示した。

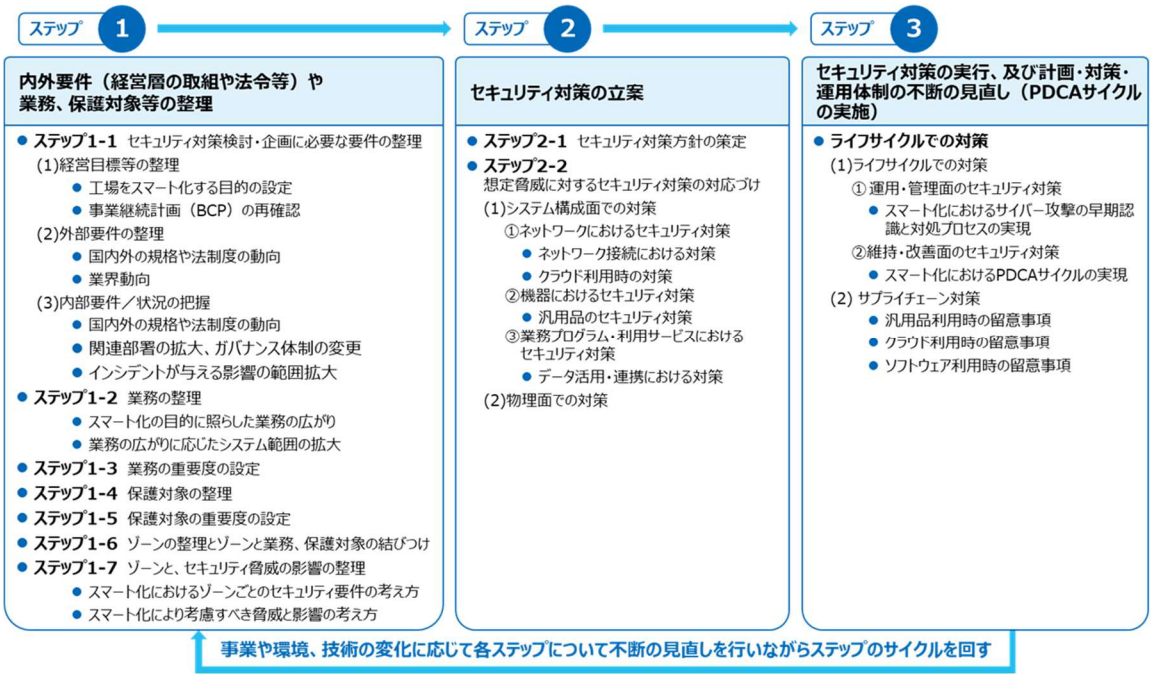


図 2-2 ガイドライン別冊における各ステップの概要

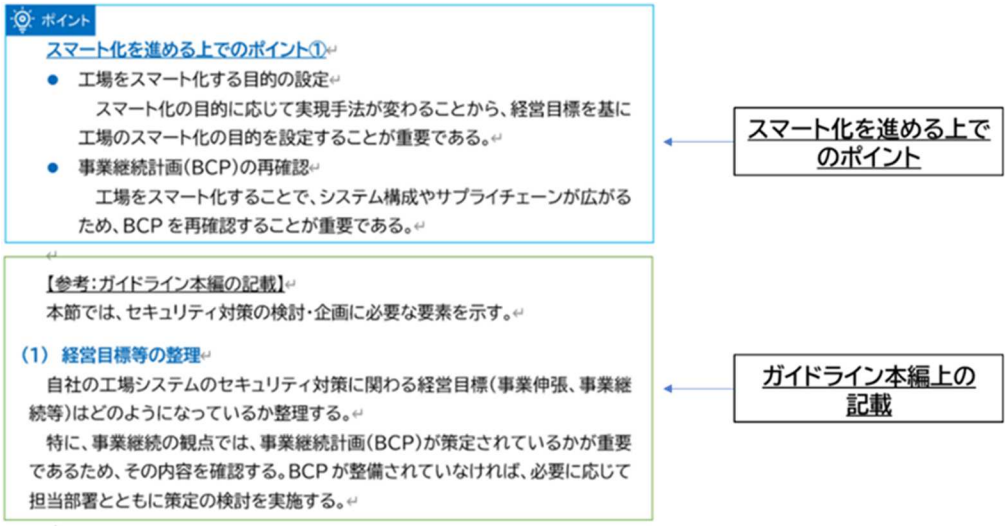


図 2-3 各ステップにおける青枠と緑枠について

2.1.3 ガイドライン別冊の英訳

ガイドライン別冊についても、ガイドライン本編と同様に英訳を行った。

2.2 スマート工場のセキュリティに関する国内外の政策動向

2.2.1 海外

(1) U.S. Cyber Trust Mark

2021年5月12日に発令された「国家のサイバーセキュリティ向上に関する大統領令(E.O.14028)」に基づいてコンシューマ IoT 製品セキュリティの向上に関する政策として U.S. Cyber Trust Mark プログラムが公表された。本取組は、法的遵守義務やペナルティがなく、自主的な取り組みとして位置づけられている。対象製品としては、スマート家電を含めた一般的なコンシューマ IoT 製品が挙げられる。

(2) EU Cyber Resilience Act

2022 年 9 月、欧州委員会は、EU 市場に投入されるデジタル製品のセキュリティ対応を義務付ける「EU Cyber Resilience Act(CRA)」18 の草案を発表した。EU CRA と他の EU 法令との関係性を に示す。EU CRA は、2022 年 5 月に欧州議会・欧州理事会が改訂に合意し、NIS2 指令(Network and Information Security 2 Directive)を補間する目的で策定された。対象となる「デジタル製品」のうち、重要な「デジタル製品」のうちリスクが低い製品をクラスⅠ、リスクが高い製品をクラスⅡとして詳細に定義しており、クラスに応じて、選択できる適合性証明の方法が異なる。既存の EU 法令で対象となっている製品など、一部の「デジタル製品」については、今回の法案の対象外として明記されている。

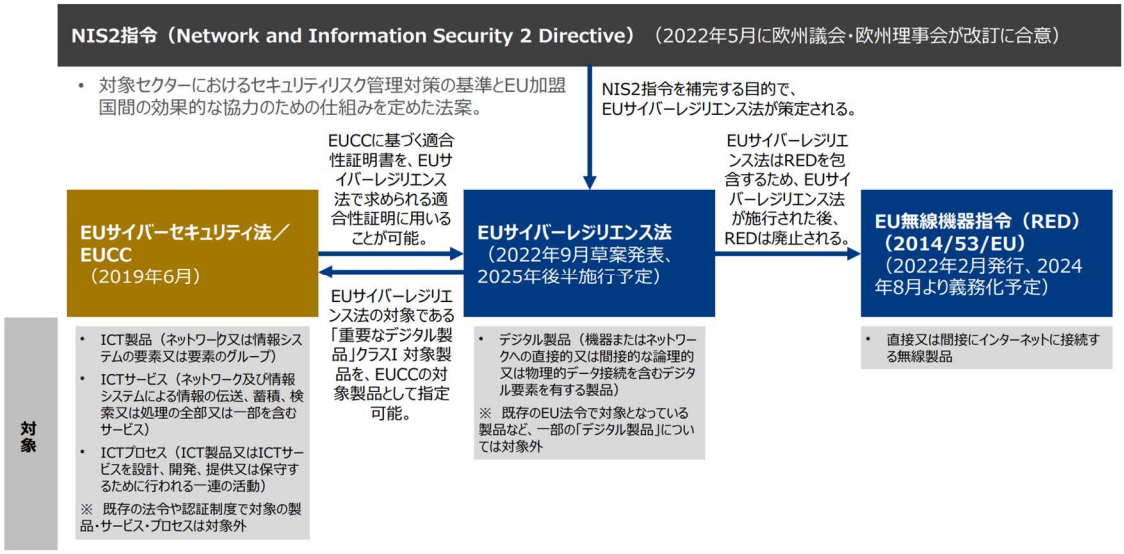
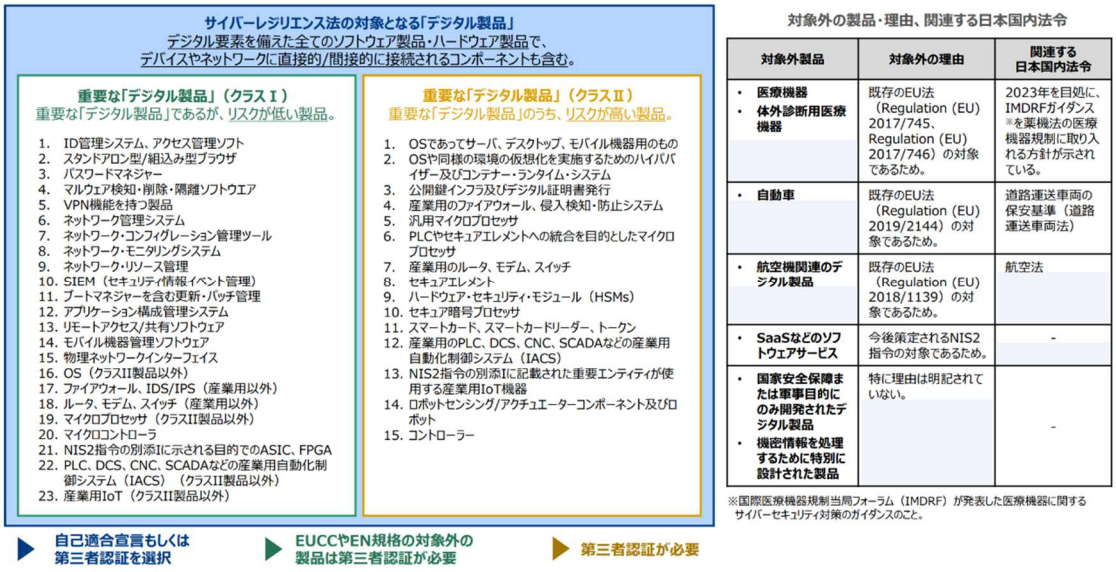


図 2-4 サイバーレジリエンス法の関係図[1]



対象外の製品・理由、関連する日本国内法令

対象外製品	対象外の理由	関連する日本国内法令
• 医療機器 • 体外診断用医療機器	既存のEU法（Regulation (EU) 2017/745、Regulation (EU) 2017/746）の対象であるため。	2023年を目処に、IMDRFガイダンス※を薬機法の医療機器規制に取り入れる方針が示されている。
• 自動車	既存のEU法（Regulation (EU) 2019/2144）の対象であるため。	道路運送車両の保安基準（道路運送車両法）
• 航空機関連のデジタル製品	既存のEU法（Regulation (EU) 2018/1139）の対象であるため。	航空法
• SaaSなどのソフトウェアサービス	今後策定されるNIS2指令の対象であるため。	-
• 国家安全保障または軍事目的にのみ開発されたデジタル製品 • 機密情報を処理するために特別に設計された製品	特に理由は明記されていない。	-

※国際医療機器規制当局フォーラム（IMDRF）が発表した医療機器に関するサイバーセキュリティ対策のガイダンスのこと。

図 2-5 サイバーレジリエンス法の対象範囲[2]

2.2.2 国内

（1） IoT セキュリティ製品に対するセキュリティ適合性制度

政府機関等・企業等における IoT 製品の選定時や調達時に、共通のセキュリティ指標で第三者が評価・認証を付与する制度、及び国民が安心してネットワークを使用したサービスを利用するための最低限のセキュリティ基準を満たす IoT 製品にラベルを付与する制度として、経済産業省において「IoT セ

[1] 経済産業省、第 1 回 IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討会
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/pdf/001_08_00.pdf
[2] 経済産業省、第 1 回 IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討会
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/pdf/001_08_00.pdf

キュリティ製品に対するセキュリティ適合性制度」が検討されている。本制度は、☆というレベルに応じて適合基準が策定されている。☆1 については、2024 年度内での制度開始が検討されている。

（2） 協調的なデータ利活用に向けたデータマネジメント・フレームワーク

経済産業省「協調的なデータ利活用に向けたデータマネジメント・フレームワーク」は、データを軸に置き、データのライフサイクルを通じて、その状態を可視化しリスクを洗い出し、必要なセキュリティ対策を適切なデータマネジメントによって実現するためのフレームワークである。同フレームワークでは、データマネジメントを「データの属性が場におけるイベントにより変化する過程を、ライフサイクルを踏まえて管理すること」と定義し、

- イベント（生成・取得、加工・利用、移転・提供、保管、廃棄）
- 場（各国・地域等の法令、組織の内部規則、組織間の契約など）
- 属性（カテゴリ、開示範囲、利用目的、データ管理主体、データ権利者など）

というそれぞれに影響しあう関係にある 3 つの要素から構成されるモデルとして整理している。データの状態が可視化されることにより、ステークホルダー全体での適切なデータマネジメントの実施につながることが期待されている。

ガイドライン別冊では、フレームワークにおけるデータをゾーン、イベントをゾーン間のデータ移転・処理と置き換え、参照している。

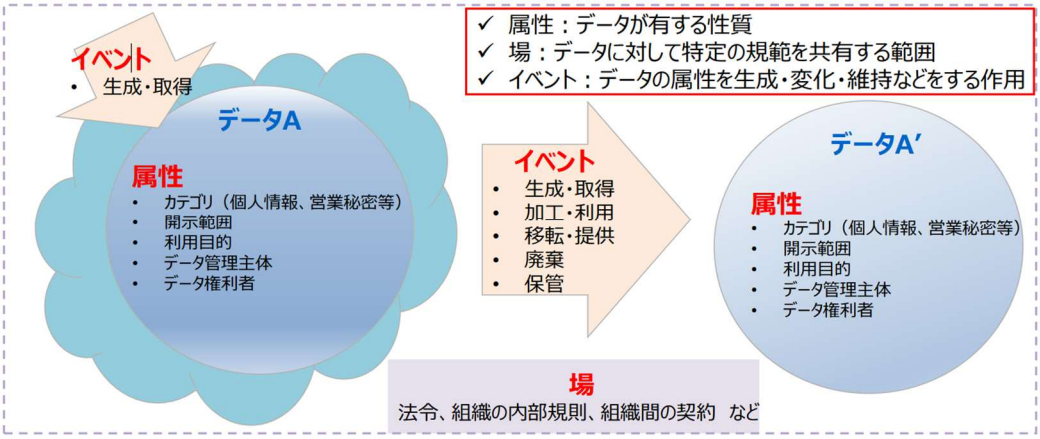


図 2-6　協調的なデータ利活用に向けたデータマネジメント・フレームワークの概要

2.3 スマート工場のセキュリティを目的とした制度やガイドライン等の概要

2.3.1 独立行政法人情報処理推進機構（IPA）

（1） 産業用制御システム向け侵入検知製品等の導入手引書

経済産業省が発行している「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」や「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」において「ネットワークへの不正侵入検知」はセキュリティ対策の 1 つとして記載されており、制御システムにおいて重要な対策と認識されている。このような背景の下、IPA では、2023 年 6 月にインシデント検知に注目した「産業

用制御システム向け侵入検知製品等の導入手引書」が公表した。

本文書は、ユーザ企業への産業用制御システム向け侵入検知製品等の認知度向上、ユーザ企業への産業用制御システム向け侵入検知製品等の普及促進を目指して、侵入検知製品等の基本事項、導入の進め方、導入後の留意点を解説している。具体的には、侵入検知製品などを使う際の導入検討から本格運用までの流れを記載している。

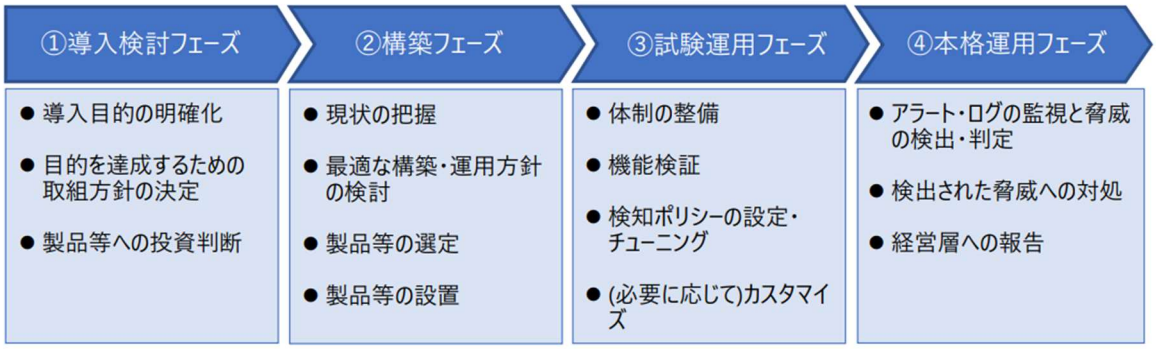


図 2-7 侵入検知製品等を使う際の導入検討から本格運用までの流れ[3]

（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

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。

構成		概要
本編	第1章　全体概要	本報告書の概要、国内フレームワーク・ガイドラインとの関係、モデル事業者内のプロセスと業務の説明、関連システム 、実施例におけるスマート化にあたり発生した課題を説明
	第2章　企画フェーズ	研究開発、営業、事業企画の取り組み状況を紹介
	第3章　設計・開発フェーズ	生産システム設計開発、生産システム調達の各内容での取り組みを紹介
	第4章　運転・運用フェーズ	生産、品質保証、製品出荷、運用・運転時での取り組みを紹介
	第５章　保守フェーズ	保守として資産の管理、変更の管理、情報記憶メディアにでの取り組みを紹介
	第６章　廃棄フェーズ	生産システムでの廃棄時の管理として記憶メディアの廃棄に対する取り組みを紹介
	第７章　その他	情報管理、インシデント対応、エリア人員管理での取り組みを紹介
	第８章　まとめ	全体を通したまとめを記述

図 2-8『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

2.3.2 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）

[3] IPA、産業用制御システム向け侵入検知製品等の導入手引書
https://www.ipa.go.jp/security/controlsystem/ps6vr7000001o2b1-att/icsidshandbook.pdf

（1） 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の取組

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。2024 年 3 月現在、リスクアセスメント編のみ公表されている。

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。

2.4 スマート工場のセキュリティに関する国内外の技術動向

2.4.1 工場セキュリティに関する技術、製品・サービス例

近年、スマート化する工場システムにおいて活用可能なセキュリティに関する製品・サービスが数多く提供開始されている。以下の通り、提供されている製品・サービスの中では、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」が活用・参照されている事例もある。

表 2-16 工場セキュリティに関する技術、製品・サービスの一覧

開始日	企業名	概要	ガイドラインの活用状況
2023/12	NTT アドバンステクノロジ	経済産業省ガイドラインのチェックリストに従ってアセスメントを進める「OT セキュリティアセスメントサービス」を産業分野向けに提供開始。	活用
2023/11	NTT セキュリティ・ジャパン	経済産業省ガイドラインに即した質問項目から構成された「OT セキュリティ簡易診断」を無料で公開。	活用
2023/10	テリロジー・フォーティネットジャパン	制御システム保有の企業や製造業に対し、「Nozomi Networks Guardian & FortiGate 同時評価支援プログラム」を提供開始。	－
2023/5	HPE	クラウドネイティブなネットワーク管理ソリューション「HPE Aruba Networking Central」の次世代版、及び HPE GreenLake プラットフォーム上で導入・展開・管理が可能な Network-as-a-Service（NaaS）を提供開始。	－

2023/5	クロラティ・SB C&S	資産の可視化、脆弱性管理、脅威の検知、多様化するセキュリティ脅威に対する保護と対応等、包括的なソリューションを提供。	－
2023/5	フォーカスシステムズ・フォーティネットジャパン	約 3 ヶ月で工場の現地ヒアリングと実機アセスメントのうえ、経済産業省ガイドライン適合に必要な対策を提示する OT セキュリティアセスメントサービスを提供開始。	参照
2023/4	兼松エレクトロニクス・グローバルセキュリティエキスパート・テリロジー	産業用制御システムのセキュリティコンサルティングから、OT セキュリティ及びネットワーク製品の実装、工場従業員向け教育や緊急時対応、組織体制の構築までをワンストップで総合的ご支援する「Technical Knowledge Guardian for OT セキュリティ」を提供開始。	参照
2023/3	NEC	工場の制御システムのセキュリティを監視する「ActSecure χ（カイ）マネージドセキュリティサービス クリスタル Nozomi Networks Guardian 監視サービス」を提供開始。	参照
2023/3	コンテック	NIST SP800-147 準拠の改ざん予防対策 BIOS 搭載、ランサムウェア対策ソフトウェアを導入したした組み込み用 PC、「ボックスコンピュータ（R） BX-M2500 Trellix モデル」を発売開始。	参照
2023/2	NRI セキュアテクノロジーズ	半導体の製造工程におけるサイバーセキュリティの強化に向けたコンサルティングサービス「半導体業界向け SEMI セキュリティ規格準拠支援サービス」を提供開始。	－

（1） OT セキュリティアセスメントサービス（NTT アドバンステクノロジ）

2023 年 12 月、工場やビル内のセキュリティリスクの現状を把握し、セキュリティ対策を進めることを目的に、産業分野向け「OT セキュリティアセスメントサービス」の提供を開始した。本サービスの実施フローを図 2-9 に示す。リスクの洗い出しに当たって、Web 簡易診断と現状把握・ヒアリングを通して、経済産業省「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」のチェックリストに示された項目について、網羅的に効率よく実情把握を行う。4 つのカテゴリでリスクを把握し、具体的なセキュリティ対策案の策定に向けた情報を提供する。

図 2-9 OT セキュリティアセスメントサービスの概要[4]

（2） OT セキュリティ簡易診断（NTT セキュリティ・ジャパン）

[4] NTT アドバンステクノロジ株式会社、産業分野向け「OT セキュリティアセスメントサービス」の提供開始
https://prtimes.jp/main/html/rd/p/000000274.000023654.html

2023 年 11 月に、Fortinet が公表する OT セキュリティアセスメントサービスの提供を受け、NTT セキュリティ・ジャパンが「OT セキュリティ簡易診断」を公表した。本診断は、経済産業省「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」のチェックリストから構成される。本サービスは、OT セキュリティ対策の初めの一歩として、工場・生産現場の状態、工場内のセキュリティリスクの把握を行うことを目的としている。

2.5 国内外における工場システム及び関連するシステムへの攻撃事例の収集

国内外における制御システムに関連するサイバー攻撃の事例について調査を実施した。

表 2-17 に示す通り、制御システムに関連するサイバー攻撃について、①IT システムを対象としたランサムウェア感染、②サプライチェーンを対象とした攻撃、の 2 つのパターンが傾向として確認できる。

表 2-17 近年の国内外の制御セキュリティに関する主要なサイバー攻撃の事例

No.	時期	国・地域	製造業種	対象	概要
1.	2021/6	米国	食品	IT システム	社内サーバがランサムウェアに感染し、工場での操業を停止した。 身代金 1,100 万ドルをビットコインで支払った。
2.	2022/1	ドイツ	石油	IT システム	IT システムがランサムウェアに感染した。 IT システムを停止したことにより、複数のタンクファームで石油製品の供給を停止した。
3.	2022/2	日本	半導体	IT システム	大手半導体事業者の本社と海外の子会社のサーバに対する不正アクセスが検出された。 社内システムを全面停止し、一部製品の生産及び出荷を停止した。
4.	2022/2	米国	自動車	IT システム サプライチェーン	子会社の社内システムがランサムウェアに感染し、複数の工場で稼働を数日停止した。
5.	2022/3	日本	自動車	IT システム サプライチェーン	大手自動車メーカーのサプライヤーの社内ネットワークが不正アクセスを受け、マルウェアに感染した。 サプライヤーの社内サーバを全て停止した他、発注元の大手自動車メーカーの 14 工場 28 ラインが停止した。
6.	2022/4	日本	自動車機器	IT システム	大手電機機器メーカー及びその子会社は、リモートアクセス機器の SSL-VPN の脆弱性を悪用され、ランサムウェアに感染した。 同社やグループの退職者を含む従業員の情報が暗号化された他、メールや生産・販売に関する社内システム・サーバが一時停止した。
7.	2022/12	タイ	半導体	IT システム	社内サーバが、ランサムウェアに感染し

					たことを受け、一時的なネットワークの遮断により、システム障害が発生し、電子機器製造(EMS)が停止した。
8.	2023/6	台湾	半導体	IT システムサプライチェーン	大手半導体事業者のサプライヤーのネットワーク内の特定のテスト環境が不正アクセスを受け、ランサムウェアの感染を報告した。 攻撃発生後、大手半導体事業者は、サプライヤーとのデータのやり取りを停止している。

2.5.1 IT システムを対象とした攻撃事例

IT システムを対象にサイバー攻撃が行われ、IT システムがランサムウェアに感染した結果、製品の生産や工場の稼働の中止など工場の操業に影響を与える事例が複数の事業者で確認されている。

例えば、2022 年 12 月、電子機器メーカーの海外子会社は、社内ネットワークシステムが不正アクセスを受け、サーバがランサムウェアに感染したと報告した。ランサムウェアの感染を受け、サーバと PC 端末の停止、外部ネットワークとのアクセスを遮断した結果、製品の生産活動を中止した。具体的な中止期間については公表されていないが、10 日後には、ほぼ通常の生産体制を取り戻したと報告している。なお、攻撃されたサーバの中には、同社及び顧客の受発注に関する機密情報や、メールアドレスなどの個人情報が保存されていると報告がなされたが、外部において情報流出などは確認されていない。

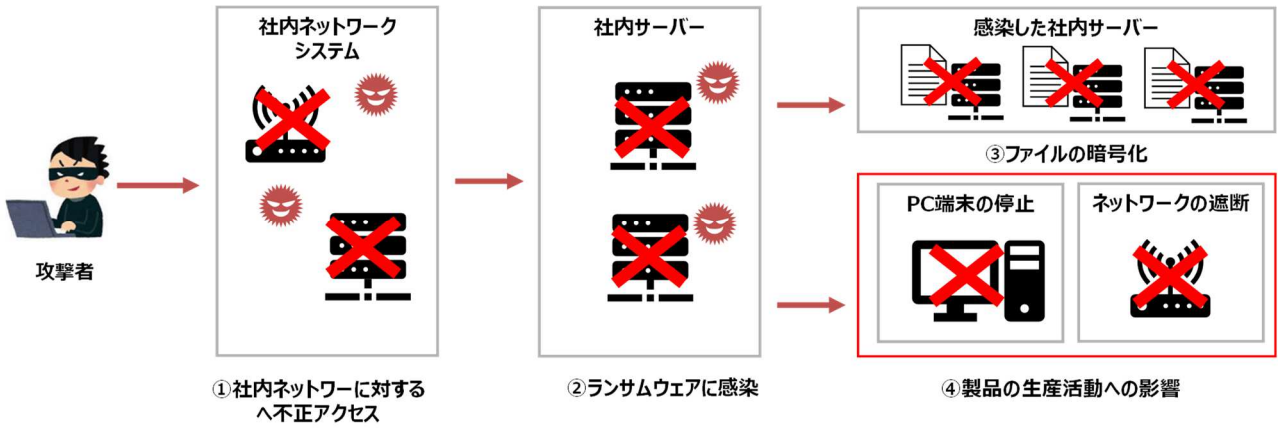


図 2-10 IT システムを対象としたサイバー攻撃のイメージ例
(出典:Secutiy NEXT 記事等に基づき三菱総合研究所作成)

2.5.2 サプライチェーンを対象とした攻撃事例

サプライヤーや子会社の脆弱性の存在する端末への攻撃を通じて、親会社や発注元の工場の操業に影響を与える事例が複数の事業者で確認されている。

例えば、2022 年 3 月、大手自動車メーカーのサプライヤーは、特定外部企業との専用通信に利用していたリモート接続機器の脆弱性を入口に不正アクセスがなされ、マルウェアに感染したと報告した。そ

の後、「生産活動に必要な取引先とのデータ授受」を担うサーバがランサムウェアに感染したことが確認された。ランサムウェアの感染を受け、社内サーバや PC 端末の停止、外部ネットワークとのアクセスを遮断した。その結果、サプライヤーの製品の生産活動が中止した他、発注元への部品提供に遅れが乗じたことにより、発注元の複数の工場でも、製品の生産活動を中止することとなり、大規模な操業停止に繋がった。

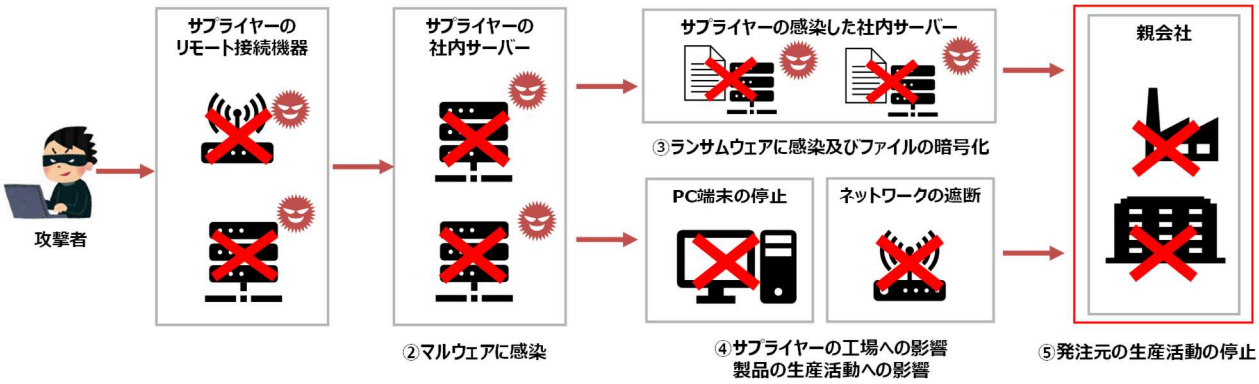


図 2-11 サプライチェーンを対象としたサイバー攻撃のイメージ例
（出典：日経クロステック記事等に基づき三菱総合研究所作成）

2.6 ステークホルダー毎のセキュリティ対策の検討

工場のスマート化において、外部ネットワークの接続の増加などによりセキュリティリスクが増加していることより、サイバー攻撃の早期認識と対処のプロセスを構築することが重要である。また、外部ネットワークとの接続が増加することで、OT セキュリティと IT セキュリティの融合化や外部の事業者との連携が必要となり、サイバー攻撃の早期認識と対処を実践するためには、各プロセスにおける担当部署と意思決定者を明確化し、情報連携の体制を構築することが重要である。被害発生のみではなく、セキュリティリスクの増加に伴い、新たな攻撃手法や脆弱性に関わる情報を収集・把握し、対応することの重要性も増していることから、予防保全段階での役割分担も確認することが必要である。

また、スマート化による変化に応じてセキュリティ対策を評価・検討するために PDCA サイクルを回すことも重要である。変化が多いスマート化に対応するために PDCA サイクルを回す上で有効的な取り組みも検討できるとよい。

スマート化を進める上で、外部機器やサービスの導入、自社の工場間や自社・他社間でのデータ流通が促進され、自社のみで管理が困難かつ責任分界点が曖昧になる可能性が高いため、対策の責任分界や役割分担、インシデント時の対応がより重要である。そのため、外部機器やサービス導入の際には提供先の企業に対して、セキュリティに対する確認を行うことが必要である。

上記のような背景を踏まえて、ガイドライン別冊では以下の論点で検討を深めることが求められる。

- サイバー攻撃の早期認識と対処における役割分担
- スマートによる多様な変化に対応できる PDCA サイクルを回す上での考え方
- 外部機器やサービス導入の際に提供先企業に確認すべき内容

2.7 ガイドラインの普及・啓発

業界団体等と協力し、「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・啓発を行った。また、IPA/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）と連携した、次年度以降の工場システムにおけるセキュリティ普及の取組方針を検討した。

2.7.1 工場 SWG における IPA/SC3 と連携した工場セキュリティの普及の方向性

次年度以降、IPA/SC3「業界連携 WG」（新規設置）の下に設置する、「工場テーマ」において工場システムにおけるセキュリティの普及啓発を図ることを検討した。

以下に、業界連携 WG 工場テーマの活動概要（案）を示す。

表 2-18 業界連携 WG 工場テーマの活動概要（案）

項目	内容
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 ・ 業界毎のリスク分析・対策の具体化等検討に資する情報提供 等 ・ 「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（※ IPA 等関連組織からの情報提供） ・ 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	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 オブザーバー業界団体、SC3 加盟団体（製造業） 等 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ー、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 2～3 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 年は、ガイドライン別冊の普及、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・意見聴取等を実施することを想定。

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、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、工場等の製造現場を管理する製造業の企業、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委員から構成される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。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

2024 年 3 月現在、工場 SWG は、下記の委員により構成される。

岩﨑 章彦	一般社団法人電子情報技術産業協会 セキュリティ専任部長
江崎 浩	東京大学大学院 情報理工学系研究科教授
榎本 健男	一般社団法人日本工作機械工業会 技術委員会 標準化部会 電気・安全規格専門委員会委員（三菱電機株式会社 名古屋製作所ドライブシステム部 専任）
桑田 雅彦	日本電気株式会社 プラットフォーム・テクノロジーサービス事業部門 セキュリティ事業統括部 IoT/OT セキュリティグループ ディレクタ（Edgecross・GUTP 合同 工場セキュリティ WG リーダー）
斉田 浩一	ファナック株式会社 IT 本部情報システム部四課 課長
佐々木 弘志	フォーティネットジャパン合同会社 OT ビジネス開発部 部長（IPA ICSCoE 専門委員）
斯波 万恵	株式会社東芝 サイバーセキュリティ技術センター 参事（ロボット革命イニシアティブ（RRI）産業セキュリティ AG）
高橋 弘宰	トレンドマイクロ株式会社 OT セキュリティ事業部 OT プロダクトマネジメントグループ シニアマネージャー
中野 利彦	株式会社日立製作所 制御プラットフォーム統括本部 大みか事業所 セキュリティエバンジェリスト
市岡 裕嗣	三菱電機株式会社 名古屋製作所 ソフトウエアシステム部 部長
藤原 剛	DMG MORI Digital 株式会社 制御開発本部コネクティビティー部 副部長
松原 豊	名古屋大学大学院 情報学研究科准教授
村瀬 一郎	技術研究組合制御システムセキュリティセンター 事務局長
渡辺 研司	名古屋工業大学大学院 社会工学専攻教授

3.2 工場 SWG の運営

（1） 第 6 回会合

1） 開催概要

日時　2023 年 10 月 6 日(金)10:00～12:00
場所　Teams 会議(Web 会議)
議題

1. 開会
2. 工場のスマート化に関する取組について
3. スマート工場におけるセキュリティ対策推進の取組について
4. ガイドラインの拡充版について
5. ガイドラインの普及啓発について
6. 自由討議
7. 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　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
資料5　「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」拡充版と検討体制
資料6　工場システムのセキュリティ普及啓発に関する取組
資料7　半導体セキュリティ規格 SEMI E187 の動向
資料8　工場セキュリティ啓発セミナ開催概要紹介
資料9　工場セキュリティガイドラインの普及啓発活動
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」拡充版骨子案

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 6 回)議事要旨

日時：令和 5 年 10 月 6 日(金)10 時 00 分～12 時 00 分
構成員：
(座長)江崎　浩　東京大学大学院 情報理工学系研究科 教授
市岡　裕嗣　三菱電機株式会社名古屋製作所ソフトウエアシステム部 部長
岩﨑　章彦　一般社団法人電子情報技術産業協会 セキュリティ専任部長
榎本　健男　一般社団法人日本工作機械工業会
技術委員会標準化部会電気・安全規格専門委員会委員
(三菱電機株式会社名古屋製作所ドライブシステム部 専任)
桑田　雅彦　日本電気株式会社

	プラットフォーム・テクノロジーサービス事業部門セキュリティ事業統括部 IoT/OT セキュリティグループ ディレクタ （Edgecross・GUTP 合同工場セキュリティ WG リーダー）
斉田 浩一	ファナック株式会社 IT 本部情報システム部四課 課長
佐々木 弘志	フォーティネットジャパン合同会社 OT ビジネス開発部 部長 （IPA ICSCoE 専門委員）
斯波 万恵	株式会社東芝 サイバーセキュリティ技術センター 参事 （ロボット革命イニシアティブ（RRI）産業セキュリティ AG）
高橋 弘宰	トレンドマイクロ株式会社 OT セキュリティ事業部 OT プロダクトマネジメントグループ シニアマネージャー
中野 利彦	株式会社日立製作所 制御プラットフォーム統括本部 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）
藤原 剛	DMG MORI Digital 株式会社 制御開発本部コネクティビティー部 副部長
松原 豊	名古屋大学大学院 情報学研究科准教授
村瀬 一郎	技術研究組合制御システムセキュリティセンター 事務局長
渡辺 研司	名古屋工業大学大学院 社会工学専攻教授

議題：

1. 開会
2. 工場のスマート化に関する取組について
3. スマート工場におけるセキュリティ対策推進の取組について
4. ガイドラインの拡充版について
5. ガイドラインの普及啓発について
6. 自由討議
7. 閉会

要旨：

1.工場のスマート化に関する取組について

・ 資料3を経済産業省製造産業戦略企画室より説明

2.スマート工場におけるセキュリティ対策推進の取組について

・ 資料4を IPA 高見様より説明

3.ガイドラインの拡充版について

・ 資料5を事務局より説明

4.ガイドラインの普及啓発について

・ 資料 6 を事務局より説明
・ 資料 7 を今野様（TXOne）より説明
・ 資料 8 を桑田委員より説明

・ 資料 9 を斯波委員より説明

5.自由討議

(1)工場のスマート化に対する取組に関するご意見

・ ソフトウェア分野においても、構成が複雑化している状況においてソフトウェア部品の情報を共有する SBOM という仕組みが国際連携の中で求められている。製造業においてもこのような仕組みがあれば活用すべきであるし、ないのであれば仕組み化を進めていかないと、サプライチェーンから断絶するリスクを把握することが難しいと考える。

(2)ガイドラインの拡充版に関するご意見

・ ガイドライン拡充版骨子案ではスマート化の定義について、レベル別に整理されていた。レベル別の記載があるとスマート化が理解しやすいと考える。どの程度データを蓄積しているのか、そのデータが工場の制御にどの程度影響を与えるのか、自律化されているのか、ロボットが現場にあるのか完全遠隔制御なのか等は脅威に繋がるため、レベル別の図があった方が脅威検討のベースになると考える。また、レベル別の図がないと、どのような状況がスマート化なのか明確でなくなってしまう。ただし、レベル別に整理すると上下関係ができてガイドを記載しにくくなる懸念もある。どのようなことがスマート化の 1 つの活動であるのか、横並びの箇条書きで例として示すことも一案と考える。
・ 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の付録 E のチェックリストを活用しているという顧客が多い。拡充版についても同様のチェックリストを追加いただけると良い。
・ ガイドラインの読者は、スマート化に対して異なるイメージを持つことが想定される。セキュリティ対策の重要性を認識いただくためにも、スマート工場やスマート化という言葉の定義を明確にする必要がある。
・ 経済産業省サイバーセキュリティ課において検討されている IoT 機器に対して求められるセキュリティ要件や、デジタル臨時行政調査会におけるテクノロジーマップに定義される DX におけるセキュリティ要件等、他の取り組みと足並みを揃える必要がある。工場に IoT 機器が導入される場合にこれらの要件を参照するようにすると、整合性が取れるのではないか。
・ 現状スマート工場のレベル分けが 5 段階でなされているが、それぞれのレベルでどのようなリスクが発生するかを示せると良い。例えば、レベル 1・2・3 では、データのやり取りにおいてクラウド利用がなされると、セキュリティが関連する。レベル 4 になると、ロボットの動作による人の安全の影響や、無人化された工場の障害発生時の対応等を検討する必要がある。各レベルの具体的なリスク例を提示できると、読者にとってわかりやすいのではないか。
・ 読者は工場全体がレベル 3・4 になるイメージを持つ可能性もある。しかし、ゾーニングにより、同じ工場内でも部分的にレベル 3・4 にレベルアップができる。中小企業を 1 つのゾーンのように捉え、中小企業が連携することもできる。スマート化のレベルを工場全体で考えるのではなく、システムや実現したい事項毎に検討できると良いのではないか。
・ 中小企業では、工場内の一部のシステムをロボット化して自動化を進める一方で、IT ネットワークを接続していない等、部分的なスマート化の取り組みに止まり、全体としてはまだスマート化が進展していないケースもある。そのような企業でもガイドラインを参照しやすいようにしていただきたい。

・ ユースケース含めて整理いただけるとより使いやすくなると考えられる。
・ 工場 SWG 委員ではない作業部会メンバーについては、工場 SWG にオブザーバーとして参加いただけると良い。
・ SEMI Taiwan のように、調達要件としてセキュリティ認証やガイドラインへの準拠を求める事例が増えているように見える。ガイドラインにおいて、調達要件としてセキュリティが求められる動向を示せると良い。調達要件を国がトップダウンで仕組み化することはあり得ると考える。国の調達要件として求められると、関連する産業がその調達要件を参考にすることもあり、特定の業界で起きたことが別の業界でも導入される可能性はある。特定の業界に関する情報だけでも有益であるため、今後も調達動向に関する情報共有ができると良い。

(3)ガイドラインの普及啓発に関するご質問・ご意見
・ 工場セキュリティの普及啓発においては、中小企業への普及が重要である。そのためには業界団体を通じて、あるいは業界団体のメディアを活用する等して、頻度を高めて情報発信や普及啓発活動ができると良い。業界団体の取組も含め計画化し、それを推進・支援していくことも必要である。
・ 中小企業に対する普及啓発においては、商工会議所にも協力いただけると効果的と考える。
・ 普及活動を行う上で、製造業の大半は中小企業である。普及啓発においては中小企業を巻き込むことが重要であり、IPA のサイバーセキュリティお助け隊サービス制度等と同様に、各地域の商工会議所とも連携できると良い。
・ 1 点目、サプライチェーンに関する議論に、中小企業の工場(含む町工場)における DX 推進とセキュリティ強化を両輪とした取り組みをどのような仕組み・やり方で展開するかという論点をより強く織り込む必要がある(業界別のガイドライン簡易版や取組みに係る経済的インセンティブ等)。2 点目、IT セキュリティ人材よりも絶対的に不足している OT セキュリティ人材をどのように確保するのか、産官学それの役割で、短期的対応と中長期的対応を戦略的に組み合わせた対策を行動に移すことが急務と考える。3 点目、サイバー攻撃関連のインシデントレスポンスの際に有効な警察への通報、及びそれ以前に相談できる体制をどのように各地域で確立し、その実効性を担保・向上できるのか、といった議論も必須ではないものの必要だと考える(特に対中小企業)。
(以上)

(2) 第 7 回会合

1) 開催概要

日時　2024 年 2 月 8 日(木)13:00～14:45
場所　Teams 会議(Web 会議)
議題
1. 開会
2. スマート工場の取組について

3. 工場システムのセキュリティ普及に関する取組について
4. サイバー攻撃による被害に関する情報共有の促進について
5. ガイドラインの拡充版について
6. ガイドラインの普及啓発について
7. 自由討議
8.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　日立製作所大みか事業所におけるスマート工場の取り組みについて
資料4　中外製薬における工場セキュリティの取り組み
資料5　中小製造業のセキュリティ状況と JNSA 西日本支部の取り組みのご紹介
資料6　サイバー攻撃の情報共有にかかる取組について
資料7　「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」拡充版（案）の概要と今後の方針
資料 8　工場システムのセキュリティ普及啓発に関する取組
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」拡充版案

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 7 回）議事要旨

日時：令和 6 年 2 月 8 日（木）13 時 00 分～14 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　三菱電機株式会社名古屋製作所ソフトウエアシステム部 部長
岩﨑　章彦　一般社団法人電子情報技術産業協会 セキュリティ専任部長
榎本　健男　一般社団法人日本工作機械工業会
技術委員会標準化部会電気・安全規格専門委員会委員
（三菱電機株式会社名古屋製作所ドライブシステム部 専任）
桑田　雅彦　日本電気株式会社
プラットフォーム・テクノロジーサービス事業部門セキュリティ事業統括部
IoT/OT セキュリティグループ ディレクタ
（Edgecross・GUTP 合同工場セキュリティ WG リーダー）
斉田　浩一　ファナック株式会社 IT 本部情報システム部四課 課長
佐々木　弘志　フォーティネットジャパン合同会社 OT ビジネス開発部 部長
（IPA ICSCoE 専門委員）
斯波　万恵　株式会社東芝 サイバーセキュリティ技術センター 参事

	（ロボット革命イニシアティブ（RRI）産業セキュリティ AG）
高橋　弘宰	トレンドマイクロ株式会社 OT セキュリティ事業部 OT プロダクトマネジメントグループ　シニアマネージャー
中野　利彦	株式会社日立製作所　制御プラットフォーム統括本部 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）
藤原　剛	DMG MORI Digital 株式会社 制御開発本部コネクティビティー部　副部長
松原　豊	名古屋大学大学院　情報学研究科准教授
村瀬　一郎	技術研究組合制御システムセキュリティセンター　事務局長
渡辺　研司	名古屋工業大学大学院　社会工学専攻教授

議題：

1. 開会
2. スマート工場の取組について
3. 工場システムのセキュリティ普及に関する取組について
4. サイバー攻撃による被害に関する情報共有の促進について
5. ガイドラインの拡充版について
6. ガイドラインの普及啓発について
7. 自由討議
8. 閉会

要旨：

1.スマート工場の取組について

・ 資料3を日立製作所中野委員より説明
・ 資料4を中外製薬筒井様より説明

2.工場システムのセキュリティ普及に関する取組について

・ 資料5を JNSA 西日本支部岡本様より説明

3.サイバー攻撃による被害に関する情報共有の促進について

・ 資料6を経済産業省澤田様より説明

4.ガイドラインの拡充版について

・ 資料7を事務局より説明

5.ガイドラインの普及啓発について

・ 資料 8 を事務局より説明

6.自由討議

(1)工場システムのセキュリティ普及に関する取組に関するご意見

・ 資料 5 の発表について、中小企業に対する取組は重要であり、ワークショップの開催等、素晴らしい活動だと考える。今後も取組を進めてほしい。

(2)ガイドラインの拡充版に関するご意見

・ ガイドライン拡充版骨子案ではスマート化の定義について、レベル別に整理されていた。レベル別の記載があるとスマート化が理解しやすいと考える。どの程度データを蓄積しているのか、そのデータが工場の制御にどの程度影響を与えるのか、自律化されているのか、ロボットが現場にあるのか完全遠隔制御なのか等は脅威に繋がるため、レベル別の図があった方が脅威検討のベースになると考える。また、レベル別の図がないと、どのような状況がスマート化なのか明確でなくなってしまう。ただし、レベル別に整理すると上下関係ができてガイドを記載しにくくなる懸念もある。どのようなことがスマート化の 1 つの活動であるのか、横並びの箇条書きで例として示すことも一案と考える。

(3)ガイドラインの普及啓発に関するご質問・ご意見

・ 工場セキュリティの普及啓発においては、中小企業への普及が重要である。そのためには業界団体を通じて、あるいは業界団体のメディアを活用する等して、頻度を高めて情報発信や普及啓発活動ができると良い。業界団体の取組も含め計画化し、それを推進・支援していくことも必要である。

・ 中小企業に対する普及啓発においては、商工会議所にも協力いただけると効果的と考える。

(以上)

3.3 工場 SWG 作業部会の構成

2024 年 3 月現在、工場 SWG 作業部会は、下記のコアメンバー、メンバーにより構成される。

＜コアメンバー＞

大林 克成	日本電気株式会社 セキュリティ事業統括部 プロフェッショナル
岡山 大河	日本電気株式会社 セキュリティ事業統括部 プロフェッショナル
小川 陽平	日本電気株式会社 セキュリティ事業統括部 主任
桑田 雅彦	日本電気株式会社 セキュリティ事業統括部 ディレクタ
斉田 浩一	ファナック株式会社 IT 本部情報システム部四課 課長
佐々木 弘志	フォーティネットジャパン合同会社 OT ビジネス開発部 部長 (IPA ICSCoE 専門委員)
斯波 万恵	株式会社東芝 サイバーセキュリティ技術センター 参事 (ロボット革命イニシアティブ(RRI)産業セキュリティ AG)
柴田 陽一	三菱電機株式会社 情報技術総合研究所 情報セキュリティ技術部 専任
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)

松田 規	三菱電機株式会社 情報技術総合研究所 情報セキュリティ技術部 部長
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

＜メンバー＞

朝日奈 弘典	三菱電機株式会社 OT セキュリティ事業推進部 グループマネージャー
勝田 正彦	株式会社日立製作所 デジタルシステム＆サービス統括本部 セキュリティリスクマネジメント本部 部長代理
木下 仁	独立行政法人 情報処理推進機構 セキュリティセンター セキュリティ対策推進部 脆弱性対策グループ 主任研究員
小林 泰輔	JFEスチール株式会社 サイバーセキュリティ統括部
鈴木 勝利	三菱ガス化学株式会社 生産技術部 設備技術グループ 主席
玉田 浩毅	三菱ガス化学株式会社 生産技術部 主席
田村 元広	三菱ガス化学株式会社 情報システム部 主席
永松 友重	三菱ガス化学株式会社 生産技術部 プロセス技術グループ 主席
野澤 正晴	東京電力パワーグリッド株式会社 サイバーセキュリティセンター 副所長
後藤 教彰	三井化学株式会社 情報システム統括部 MC-SIRT リーダー
藤井 俊郎	東京エレクトロン株式会社 情報セキュリティ部 担当部長
屋比久 猛	三菱ガス化学株式会社 情報システム部

シスコシステムズ合同会社

3.4 工場 SWG 作業部会の運営

（1） 第 1 回会合

1） 開催概要

日時 2023 年 10 月 30 日(月)13:00～15:00
場所 MRI 4F 大会議室 D 及び Teams 会議(ハイブリッド開催)
議題

1. 開会
2. メンバー紹介
3. 会議運営について
4. ガイドラインの拡充版について
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　本作業部会の議事の運営について（案）
資料4　「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」拡充版と検討体制
資料5　「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」拡充版

（2）第 2 回会合

1）開催概要

日時　2023 年 11 月 22 日（水）13:00～15:00

場所　MRI 4F CR-F 会議室及び Teams 会議（ハイブリッド開催）

議題

1. 開会
2. ガイドラインの拡充版について
3. 自由討議
4. 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　「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」拡充版
参考資料 1　第 1 回工場 SWG 作業部会議事録
参考資料2　第 1 回作業部会意見・対応方針

（3）第 3 回会合

1）開催概要

日時　2023 年 12 月 6 日（水）13:00～16:00

場所　MRI 4F CR-A 会議室及び Teams 会議（ハイブリッド開催）

議題

1. 開会
2. ガイドラインの拡充版について
3. 自由討議
4. 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　　「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」拡充版

参考資料 1　第 2 回工場 SWG 作業部会議事録

参考資料2　第 2 回作業部会意見・対応方針

参考資料3　章構成案

4. 総括

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」を受け、工場のスマート化による制御システムのシステムアーキテクチャの変化やサプライチェーンによる脅威が増し、工場がサイバー空間に密接に繋がる世界におけるセキュリティ対策の考え方を示した「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【別冊：スマート化を進める上でのポイント】」を取りまとめた。

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「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・啓発について検討を行い、工場セキュリティの普及の場を設置する方向性で検討を行った。工場 SWG では主に工場システムやセキュリティの提供側・有識者を中心とした委員により工場システムにおけるセキュリティを向上させるためのコンテンツや普及・啓発方策について議論してきたが、今後 SC3 の場においては、工場システムを有するユーザ側のメンバーに向け様々なコンテンツを展開し、提供側・有識者・ユーザ側等、工場システムに関わる関係者が連携しながら工場システムセキュリティを推進することを目指している。

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」の本編及び別冊を活用し、工場システムのセキュリティのさらなる向上を目指していくことが望ましい。

令和5年度産業サイバーセキュリティ強靭化事業

（IoT機器や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

2024 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5年度産業サイバーセキュリティ強靭化事業
（IoT機器や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

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

2024年3月29日

目次

図 目次

表 目次

1. はじめに

本事業では、IoT 機器のセキュリティを確保するための諸外国の取組やその他国内外のセキュリティ対策等を調査し、IoT 機器のセキュリティ確保に向けた適合性評価制度を検討した。適合性評価制度の構築に向け、有識者による検討会を開催するとともに、複数の IoT 機器について評価検証を実施し、どの程度のコストが発生するか等を検討した。

2. IoT 機器のセキュリティ確保に向けた国内外の動向調査

IoT 機器のセキュリティ確保に関する国内外政府機関や標準化団体等による取組を調査した。

2.1 国内政府機関の動向調査結果

2.1.1 改正 NICT 法

2023 年 12 月 11 日の参議院本会議において、情報通信研究機構（NICT）がサイバー攻撃への対応を目的とした通信機器の調査を延長するための改正 NICT 法が賛成多数で可決・成立した1。

NICT は、2018 年 5 月に改正された NICT 法に基づき、サイバー攻撃に悪用されるおそれのある IoT 機器の調査等を行うこととなっていた。その取組は「NOTICE（National Operation Towards IoT Clean Environment）」と呼ばれる。インターネット上の IoT 機器には、推測しやすいパスワードが設定されているものがあり、これらの機器はサイバー攻撃の標的となりやすく、重大なリスクを引き起こす可能性がある。そのため、NOTICE では、このような機器を特定し、インターネットプロバイダーに通知し、インターネットプロバイダーは、機器の利用者を特定し、セキュリティに関する注意喚起を行う。

現行法では NOTICE の調査期間は 2023 年度末までとされていた。今回の改正により調査期間が延長され、2024 年度以降も調査を継続できるようになり、改正法では、通信機器だけでなく、ソフトウェアや既にマルウェアに感染した機器も新たに調査対象となった。

2.2 諸外国政府機関の動向調査結果

2.2.1 US Cyber Trust Mark

米国バイデン政権は、2023 年 7 月 18 日に、消費者向け IoT 製品に関するサイバーセキュリティ認証・表示プログラム「US Cyber Trust Mark[2]」の導入計画を公表した。本プログラムは、米連邦通信委員会（FCC）が提案しており、サイバーセキュリティ基準を促進し、消費者に安全で安心な購買体験を提供することを目的としている。

事業者に対する本プログラムへの対応は任意と位置付けられており、サイバーセキュリティ基準を達成した消費者向け IoT 製品には、U.S. Cyber Trust Mark のラベルが付与される。このラベリングにより、消費者はサイバーセキュリティを具備する製品を見分け、選択することができるようになる。さらに、FCC は、認証を受けた製品に関する情報を提供する QR コード・システムの導入を行う予定であり、消費者は IoT 製品に関するより詳細な情報を入手することが可能となる。

本プログラムの対象となる製品は、スマート冷蔵庫、スマート電子レンジ、スマートテレビ、スマートフィットネストラッカーなど、消費者向け IoT 製品全般にわたる。

---

[1] 参議院「第 212 回国会（臨時会） 議案情報」
https://www.sangiin.go.jp/japanese/joho1/kousei/gian/212/meisai/m212080212006.htm

[2] FCC「FCC Proposes Cybersecurity Labeling Program for Smart Devices」
https://www.fcc.gov/document/fcc-proposes-cybersecurity-labeling-program-smart-device

具体的な評価基準は明らかにされていないが、NIST の「NIST IR 8425: Profile of the IoT Core Baseline for Consumer Products」がベースとなる。NISTIR 8425 では以下の要件が規定されている[3]。(表 2.2-1 参照)

FCC は、2024 年 3 月 14 日の公開会合で、委員の全会一致をもって本プログラムを承認した[4]。

表 2.2-1 NIST IR 8425 で規定されている要件

分類	項目
IoT 製品に求める機能	資産の識別
	インタフェースのアクセス制御
	製品構成
	ソフトウェアのアップデート
	データ保護
	サイバーセキュリティの現状認識
IoT 製品開発者に求める活動	文章化
	情報・問い合わせ受付
	情報発信
	製品教育と意識向上

2.2.2 EUCC

2020 年に ENISA より、EU におけるデジタル関連商品・サービス・プロセスのサイバーセキュリティ認証制度(EUCC)が公表された[5]。EUCC は、2019 年に施行されたサイバーセキュリティ法に基づく任意の認証制度で、その枠組みも同法に定められており、既存の CC(Common Criteria)のスキームの後継として機能させることを目的としている。

EU サイバーレジリエンス法や Revised Network Code on Cybersecurity においても、EUCC の認証結果を証明書として活用可能である旨が記載されている。EUCC 以外に、クラウドシステムを対象とした EUCS、5G ネットワークを対象とした EU5G の認証制度も検討されている。

2024 年 1 月、欧州委員会が、EU サイバーセキュリティ法に基づき、欧州初のサイバーセキュリティ認証制度を採択した[6]。本制度は EU 官報に掲載され、掲載から 20 日後に発効する。欧州委員会は、本認証スキームの官報掲載と同時に、欧州サイバーセキュリティ認証のための EU ローリング作業計画も発表する。この文書は、最近の法制度や市場の動向を考慮し、将来の欧州サイバーセキュリティ認証制度の戦略的ビジョンと可能な分野に関する考察を示したものである。

[3] NIST「Profile of the IoT Core Baseline for Consumer IoT Products」 https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.pdf
[4] FCC「March 2024 Open Commission Meeting」 https://www.fcc.gov/march-2024-open-commission-meeting
[5] ENISA「Cybersecurity Certification Framework」 https://www.enisa.europa.eu/topics/certification/cybersecurity-certification-framework
[6] ENISA「EU adopts first Cybersecurity Certification Scheme」 https://www.enisa.europa.eu/news/an-eu-prime-eu-adopts-first-cybersecurity-certification-scheme

2.2.3 EU Cyber Resilience Act

欧州委員会は 2022 年 9 月、NIS2 指令を補完する目的で、EU 市場に投入されるデジタル製品のセキュリティ対応を義務付ける「EU サイバーレジリエンス法（EU CRA）」の草案を発表した[7]。

本法案では、デジタル製品を上市する際のルール、製品におけるサイバーセキュリティに関する要求事項、製造業者に課される脆弱性対応の要求事項、当該要求事項への遵守を担保するための市場監督者へのルールを規定している。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。

対象製品について、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（電力システムの PLC や SCADA 等の産業用制御システムを含む）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等は除外される。（図 2.2-1 参照）

対象製品の市場への展開に当たっては、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。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 万ユーロ又は前会計年度の世界全体総売上高の最大 2.5%のいずれか高い方が罰金として科される。

2023 年 12 月、本法案について、欧州議会と欧州理事会の双方の合意に達したと発表された[8]。正式な承認は 2024 年初頭に行われる予定である。その後、法律に基づく義務は段階的な移行期間を経て発効される。脆弱性報告義務は 21 か月後の 2025 年後半に開始され、残りの義務は 3 年後の 2027 年初頭に開始される予定である。

[7] European Commission「Cyber Resilience Act」https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
[8] European Commission「Commission welcomes political agreement on Cyber Resilience Act」https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6168

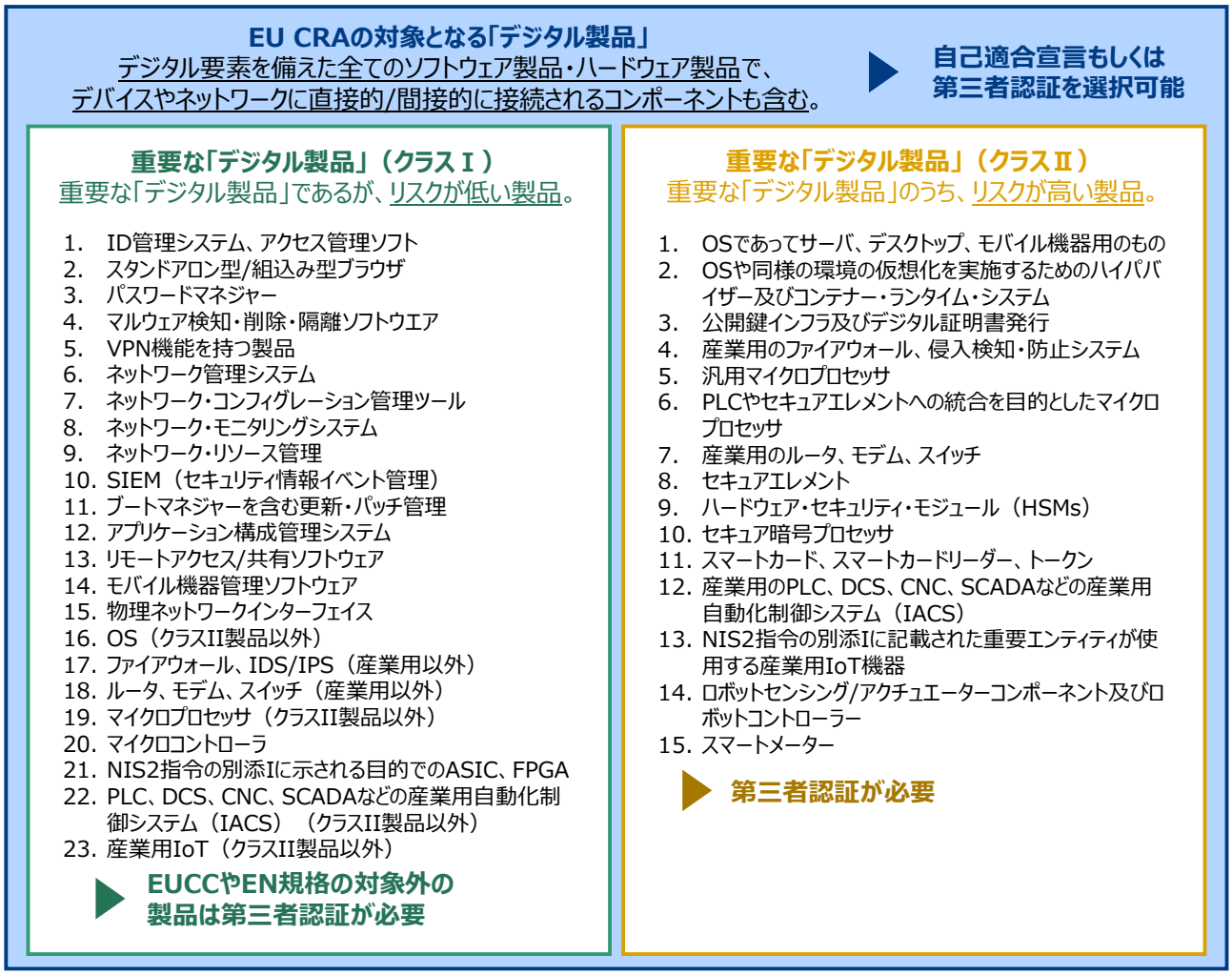


図 2.2-1 EU CRA で対象となるデジタル製品[9]

2.2.4 Product Security and Telecommunication Infrastructure Act

英国は、2021 年 12 月に「Product Security and Telecommunication Infrastructure Act（PSTI 法）」を公表した[10]。本法案は、2022 年 12 月に国王裁可の手続きが完了し、正式に承認された[11]。

同法は、英国の消費者向け IoT 製品に関するセキュリティ体制を構成する二つの法律のうち、最初の法律である。この体制を形成する二つ目の法律は、「Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023（PSTI 規則）」である。これは同法に基づいて制定

[9] European Commission「Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020」を基に三菱総合研究所作成
[10] GOV.UK「The Product Security and Telecommunications Infrastructure (PSTI) Bill – product security factsheet」https://www.gov.uk/guidance/the-product-security-and-telecommunications-infrastructure-psti-bill-product-security-factsheet
[11] GOV.UK「The UK Product Security and Telecommunications Infrastructure (Product Security) regime」https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime

され、IoT 製品ベンダーが自社製品において遵守しなければならないセキュリティ要件の概要を示している。政府は 2023 年 4 月に PSTI 規則の全草案を公表した。これらの規則は 2023 年 9 月 14 日に署名され、法律として施行された。制度は 2024 年 4 月 29 日に開始される。

PSTI 法では、具体的なセキュリティ要件や経過措置の期間は明記されておらず、三つのセキュリティ対策について規定されている。(表 2.2-2 参照) なお、具体的な要件の設定は担当国務大臣が決定するように規定されている。また、英国への上場を行うに当たって、要件に対するコンプライアンス宣言や、違反した場合に科せられるペナルティも明記されており、最大で 1,000 万ポンド又は製造者の全世界総売上 4%の多い額が課せられる。

表 2.2-2 PSTI 法にて求められる三つのセキュリティ要件[12]

分類	規定内容
パスワードについて	パスワードは、製品ごとに一意でなければならない。パスワードは、インクリメンタルカウンタに基づくもの、一般に入手可能な情報に基づくもの、一般に入手可能な情報に由来するもの、業界の優れた慣行の一部として認められている暗号化方法又は鍵付きハッシュアルゴリズムを使用しない限り、シリアル番号などの一意の製品識別子に基づくもの、又はそれらに由来するものであってはならず、その他容易に推測できるものであってはならない。
セキュリティ上の問題の報告方法について	製造者は、製品に関するセキュリティ上の問題を報告する方法に関する情報を提供しなければならない。製造者は、報告者が報告を受領したことの確認と、報告されたセキュリティ問題の解決までの状況更新を期待できる期間に関する情報を提供しなければならない。この情報は、事前の要請なしに、英語で、無料で提供されなければならない。また、アクセスしやすく、明確で透明性のあるものでなければならない。
セキュリティの最低更新期間について	セキュリティの最低更新期間に関する情報は、明確でアクセス可能かつ透明な方法で公表され、消費者が入手できるようにされなければならない。この情報には、セキュリティ更新が提供される最短期間とその終了日が記載されていなければならない。この情報は、事前の要請なしに、英語で、無償で、技術的な予備知識のない読者にも理解できるような形で提供されなければならない。

2.2.5 Cybersecurity Labelling Scheme

シンガポールのサイバーセキュリティ庁(CSA)は、サイバーセキュリティ・ラベリング・スキーム(CLS)を発表した[13]。本制度は、2020 年 10 月に開始されて以降、適宜改訂が行われており、最新の更新は 2023 年 9 月より適用された。IoT 製品ベンダーの本制度への取組は任意の位置付けで、このスキームでは、IoT 製品が規定されたセキュリティ要件に適合しているか評価される。適合しているとされた場

[12] GOV.UK Product Security and Telecommunications Infrastructure Act 2022 を基に三菱総合研究所作成
[13] CSA「Cybersecurity Labelling Scheme (CLS)」https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme

合、製品にはラベルが付与され、消費者はより優れたサイバーセキュリティを備えた製品を識別し、情報を得て、適切な製品の選択ができるようになる。本制度では、ユーザに与える影響が大きい Wi-Fi ルーター及びスマートホームハブを当初の対象製品とし、その後、IP カメラ、スマートドアロック、スマートライト、スマートプリンターなどの消費者 IoT 製品を対象とするように拡張した。

CLS には、IoT 製品を評価するための 4 つのレベル（CLS*，CLS**，CLS***，CLS****）が存在する。各追加のアスタリスクは、IoT 製品が遵守すべき追加のテストと評価レベルを表す。（表 2.2-3 参照）

CLS は、フィンランドとドイツのサイバーセキュリティ認証制度の相互承認が可能である。フィンランドの Transport and Communications Agency が発行したフィンランドのセキュリティラベルを持つ IoT 製品は、CLS***（レベル 3）で承認され、その逆も同様に承認される。また、ドイツの Federal Office for Information Security が発行したセキュリティラベルを持つ製品は、CLS**（レベル 2）で承認され、その逆も同様に承認される。

2022 年のシンガポール国際サイバーウィークにて、サイバーセキュリティ・ラベリング・スキーム・メディカルデバイス（CLS（MD））が発表された[14]。これは、医療分野における IoT 製品のセキュリティレベルを向上させるための、厚生省（MOH）、サイバーセキュリティ庁（CSA）、保健科学庁（HSA）及び Synapxe（旧 Integrated Health Information Systems）の取組の一環である。CLS（MD）の下で、医療系 IoT 製品は 4 つのレベルに基づいて評価され、医療系 IoT 製品のサイバーセキュリティのレベルを示すラベルが提供される。このラベルは、医療ユーザに対して医療デバイスのサイバーセキュリティ規定を透明にし、情報を提供することで、ユーザが情報を元に購買判断を行えるようにすることを目的としている。

2023 年 9 月、CSA は新たな CLS の関連資料「CCC SP-151-4 CLS（IoT） Assessment Methodology v1.0」を公開した[15]。本文書は各セキュリティ要件についての明確な説明を提供するために開発された。本文書では、IoT 製品が各セキュリティ要件を満たすために必要な事項を具体的に指定し、評価者が適合性を評価するためにエビデンスにおいて確認すべき事項について詳細に説明している。

表 2.2-3 CLS の 4 つのレベルと要求される内容[16]

レベル	要求される内容
CLS*	一意のデフォルトパスワードの設定やソフトウェアアップデートの提供など、基本的なセキュリティ要件を満たしていること。
CLS**	CLS*の要件に加え、セキュリティ・バイ・デザインの原則を用いて開発されており、脅威ベースのリスクアセスメントやクリティカル・デザイン・レビューを実施し

[14] CSA「Cybersecurity Labelling Scheme for Medical Devices – CLS（MD）」
https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cls-md
[15] CSA「Cybersecurity Labelling Scheme for IoT Publication No. 4」
https://www.csa.gov.sg/docs/default-source/our-programmes/certification-and-labelling-scheme/cls/publications/-pub-ccc-sp-151-4-cls(iot)-assessment-methodology-v1.0.pdf?sfvrsn=7661147f_1
[16] CRA「Cybersecurity Certification Guide」https://www.csa.gov.sg/docs/default-source/our-programmes/certification-and-labelling-scheme/cls/publications/csa-cybersecurity-certification-guide.pdf?sfvrsn=a486afd5_0

	ていること。
CLS***	CLS**の要件に加え、第三者評価機関によるソフトウェアバイナリの評価がされていること。
CLS****	CLS***の要件に加え、第三者評価機関による構造化されたペネトレーションテストを受けていること。

2.3 標準化団体等の動向調査結果

2.3.1 ISO/IEC 27404 IoT consumer security labelling

ISO/IEC 27404 は、シンガポールが提案した国際標準で、消費者向け IoT 製品のサイバーセキュリティに関するラベリングフレームワークを定義している。本文書では、「消費者 IoT 製品に関連するリスクや脅威」「ステークホルダーの役割と責任」「関連する標準とガイダンス文書」「適合評価の選択肢」「ラベリングの発行及び維持要件」「相互認識の考慮事項」に焦点を当てている[17]。

対象は主に消費者向け IoT 製品で、例えば、IoT ゲートウェイ、ベースステーション、ハブ、スマートカメラ、テレビ、スピーカー、ウェアラブルヘルストラッカー、煙感知器、ドアロック、窓センサー、ホームオートメーション及び警報システム、家電製品、スマートホームアシスタント、子供のおもちゃ、ベビーモニターなどが含まれる。

2024 年 3 月時点で、本文書は、委員会草案（Committee Draft）の段階にある。

2.3.2 IoT Device Security Specification 1.0 及び Product Security Verified Mark

2024 年 3 月、Connectivity Standards Alliance（CSA）は、IoT 製品が基本レベルのセキュリティを確保し、製品の普及を促進することを目標に、IoT 製品向けのセキュリティ標準規格「IoT Device Security Specification 1.0」と付随する認証プログラム「Product Security Verified Mark（PSV Mark）」を発表した。CSA はスマートホームのための IoT 共通規格である matter 規格[18]や、Zigbee などの IoT 業界全体の標準化、相互運用性及びセキュリティの向上を目的に活動している無線通信規格標準化団体である。CSA には、Apple、Google、Amazon をはじめとする IT 企業 280 社以上が参加している[19]。

CSA は、IoT 製品を「一つ以上のトランスデューサ（センサー又はアクチュエータ）で物理世界と直接やり取りし、一つ以上のネットワークインタフェース（例：Ethernet、Wi-Fi、Bluetooth）でデジタル世界と接続する製品」と定義している。本認証プログラムで対象となる製品は、家庭用に製造された IoT 製品（家庭用医療機器を除く）としており、具体的な製品の例としてスマート照明、スマートスイッチ、サーモスタット、ドアロック、カメラなどのスマートホーム製品を挙げている。

[17] ISO「ISO/IEC CD 27404 Cybersecurity IoT security and privacy Cybersecurity labelling framework for consumer IoT」https://www.iso.org/standard/80138.html
[18] CSA「matter」https://csa-iot.org/all-solutions/matter/
[19] CSA「Our Members」https://csa-iot.org/members/

IoT Device Security Specification 1.0 で規定されているセキュリティ要件を表 2.3-1 に示す[20]。これらのセキュリティ要件は、ETSI EN 303 645、NISTIR 8425 及びシンガポールの CLS***以上で定められている要件を含んでいる。要件は、必須要件（Must，Shall）と推奨要件（Should）に区分されるが、ETSI EN 303 645 及び CLS***、CLS****では推奨としている要件でも IoT Device Security Specification 1.0 では必須と位置づけている要件もある。

要件に遵守していると認証された IoT 製品は、PSV Mark を取得することができる。Mark 取得に当たっての認証方法は現状では公開されていない。主な PSV Mark の貼付先として、製品パッケージや店舗の看板、Web サイト上を挙げており、貼付は任意としている。ユーザは、PSV Mark に印刷された URL や QR コードを通じて、IoT 製品のセキュリティ機能に関する詳細情報を入手することができる。

2024 年 3 月 18 日、CSA とシンガポールのサイバーセキュリティ庁は、セキュリティラベルの相互運用に向け、相互承認協定（MRA）に署名した。[21]

表 2.3-1 IoT Device Security Specification 1.0 で規定されているセキュリティ要件

大分類	中分類	小分類	セキュリティ要件
技術的要件	識別	IoT 製品の識別	IoT 製品は、一意に識別可能であること。（必須要件）
			IoT 製品のモデル名は、製品上若しくはインタフェースを通じて明確に認識可能であること。（必須要件）
		IoT システムの識別	IoT 製品が、システムコンポーネントの目録を照合又は保存する場合、システムコンポーネントを一意に識別し、最新の目録を維持すること。（必須要件）
	システム構成	アクセス制御	セキュリティパラメータの変更時には、認証を行うこと。（必須要件）
		範囲	IoT 製品がシステム内の一部として構成される場合、セキュリティ関連の構成変更が IoT 製品自身及び他のコンポーネントに適用されることを実証すること。（必須要件）
		重要なセキュリティパラメータ	セキュリティパラメータは IoT 製品ごとに一意性であること。工場出荷時の共通設定の状態に戻せないこと。セキュリティパラメータをソースコードに埋め込まないこと。（必須要件）
			セキュリティパラメータは、セキュリティベストプラクティスに則って実装すること。（必須要件）
			フルートフォース攻撃に対抗するメカニズムを実装していること。（必須要件）

[20] CSA「IoT Device Security Specification Version 1.0」The Connectivity Standards Alliance Product Security Working Group Launches the IoT Device Security Specification 1.0 - CSA-IOT

[21] CSA「The Connectivity Standards Alliance and the Cyber Security Agency of Singapore Sign Mutual Recognition Arrangement on Cybersecurity Labels for Consumer IoT」https://csa-iot.org/newsroom/the-connectivity-standards-alliance-and-the-cyber-security-agency-of-singapore-sign-mutual-recognition-arrangement-on-cybersecurity-labels-for-consumer-iot/

大分類	中分類	小分類	セキュリティ要件
			ユーザが認証値を容易に変更できるメカニズムを実装していること。（必須要件）
			暗号アルゴリズムの更新が可能であること。（必須要件）
	記憶領域	セキュアな保存領域	IoT 製品に永続的に保存される機密データは、ベストプラクティスに準拠してセキュアに保存されること。（必須要件）
		データ消去	ユーザに関するローカルデータの消去が可能であること。（必須要件）
	インタフェース	セキュアな通信	セキュリティ関連情報へアクセスする場合には、認証と承認を要求すること。（必須要件）
			通信時のセキュリティ関連情報や機密データの機密性を確保すること。ベストプラクティスの暗号化技術を使用すること。（必須要件）
			双方向通信の場合、双方が認証される信頼関係を確立すること。ベストプラクティスの暗号化技術を使用すること。（必須要件）
		未使用インタフェース	未使用のインタフェースを無効にすること。（必須要件）
		入力検証	IoT 製品に入力されるデータを検証すること。（必須要件）
	内部処理	未使用機能の制限	IoT 製品の意図された用途に不要な機能はインストールされない若しくは無効にすること。（必須要件）
		最小特権	ソフトウェアは必要最小限の特権レベルで実行されること。（推奨要件）
		セキュアブート	ベストプラクティスに則り、セキュアなブートプロセスを実行すること。（推奨要件）
		デバッグ機能の保護	デバッグ及びテスト機能の不正使用から保護されていること。（必須要件）
		ソフトウェアの更新	ソフトウェアアップデートが可能であり、真正性と完全性を保証すること。ベストプラクティスの暗号化技術を使用すること。（必須要件）
			ソフトウェアの自動更新が採用されていること。IoT 製品は、初期化後に少なくとも 1 回以上アップデートの有無を確認し、その後は定期的に確認すること。（推奨要件）
			ソフトウェア更新はユーザが容易にインストールできること。（必須要件）
			自動更新・通知機能はデフォルトで有効にすること。認可された主体が、自動更新・通知機能を「有効」「無効」「延期」を選択可能なこと。（推奨要件）

大分類	中分類	小分類	セキュリティ要件
		状態監視	セキュリティ関連のイベントエラーのログを取得すること。ログには何が起こったか特定するのに十分な詳細が含まれること。（推奨要件）
			IoT 製品がセキュリティ関連状態を報告できるようにすること。（推奨要件）
			ソフトウェアの改ざんを検知した場合、認可された受信者に報告すること。（推奨要件）
			ログを IoT 製品上に保存する場合、アクセスを制限すること。（推奨要件）
		レジリエンス	IoT 製品は、停電とネットワーク遮断に対してレジリエンスを有すること。セキュリティに影響が出ないこと。ネットワークが遮断されてもローカル機能は維持されること。障害終了後、正常な運用状態に回復すること。（推奨要件）
			ソフトウェアベースとハードウェアベースのメカニズムを組み合わせた遠隔処理アプローチを採用すること。（推奨要件）
非技術的要件	文書化	設計上の考慮事項	IoT 製品ベンダーは、予想される使用方法等を文書化すること。（必須要件）
		開発プロセス及びツール	IoT 製品ベンダーは、開発の際に用いたプロセス及びツールを文書化すること。（必須要件）
		製品の能力	IoT 製品の能力を文書化すること。（必須要件）
		保守	IoT 製品のサポートに関する事項を文書化すること。（必須要件）
		設置者及び顧客に向けた文書化	ユーザに対して IoT 製品の使用方法などを文書化すること。（必須要件）
	セキュリティに関する開発プロセス	脅威モデリング	IoT 製品ベンダーは、脅威の特定・緩和のために脅威モデリングを実施すること。（必須要件）
		セキュアな開発手法	IoT 製品ベンダーは、セキュアな開発手法を採用すること。（必須要件）
		IoT サブコンポーネントの管理	IoT 製品ベンダーは、IoT 製品で使用されるサブコンポーネントを管理すること。（必須要件）
		サプライチェーン	IoT 製品ベンダーは、安全なサプライチェーンからのサブコンポーネントを使用して開発を行うこと。（必須要件）
		ハードニング	IoT 製品ベンダーは、リリース前に IoT 製品のハードニングを行うこと。（必須要件）
	脆弱性への対処	脆弱性開示	IoT 製品ベンダーは、脆弱性開示プロセスを確立し、公表・実行すること。問題を報告するための方法と、報告の受

大分類	中分類	小分類	セキュリティ要件
			領を確認し、問題の解決状況を提供するタイムラインが含まれること。（必須要件）
		脆弱性対応	IoT 製品ベンダーは、定義されたサポート期間中に、脆弱性を監視し、特定・対処すること。（推奨要件）
		脆弱性評価	IoT 製品ベンダーは、ペネトレーションテスト若しくは脆弱性テストを、リリース前を含めて定期的に行うこと。（必須要件）
	アップデート	適時の更新	IoT 製品ベンダーは、定義された期間中、セキュリティアップデートを提供すること。（推奨要件）
		ユーザ通知	IoT 製品ベンダーは、アップデートの必要性とアップデートによって軽減されるリスクを含めユーザに通知すること。アップデートにより IoT 製品の機能を妨げる場合、通知すること。（推奨要件）
		提供できない場合	アップデートが提供できない場合、IoT 製品ベンダーは、その理由と受ける影響、対処法をユーザに説明すること。（推奨要件）
	プライバシー	ユーザへの情報開示	IoT 製品ベンダーは、消費者に対して、収集される個人データや目的、使用方法についての情報を提供すること。（必須要件）
		同意	個人データ処理についてユーザの同意を得る場合、妥当な方法で得ること。ユーザはいつでも同意を取り下げることができること。（必須要件）
		最小化	IoT 製品がデータを収集する場合は、意図された機能のために必要である最小限にとどめること。（必須要件）
	コンプライアンス	要件への遵守	遵守しない場合は、合理的な理由を文書化すること。理由は、コストや事前の設計上の決定事項等ではなく、リスクとセキュリティ上のベストプラクティスに基づくものであること。システム上の互換性確保等の理由で特定の要件を満たすことができない場合も、理由を提供すること。（必須要件）

3. IoT 機器のセキュリティ確保に向けた適合性評価制度の検討

前章の調査結果、「IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討会」（以降、「検討会」と言う。）における検討結果、実際の IoT 製品に対する評価検証を含む実証の結果、実証の一環として設置した「IoT 製品のセキュリティ適合性評価制度における基準等の策定に向けたプレ検討委員会」（以降、「プレ委員会」と言う。）における検討結果等を踏まえ、IoT 機器のセキュリティ確保に向けた適合性評価制度の構築に向けた検討を実施した。具体的には以下の項目に関する検討を実施した。

- 制度の目的及び位置付け
- 制度の対象製品、要件、基準等
- 制度に関係する主体
- 信頼性確保のための仕組み
- 関連機関や国内外関係制度等との連携の仕組み
- 制度の発展に向けた施策
- 今後の取組

以降では、各項目に関する検討結果を示す。

3.1 制度の目的及び位置付け

3.1.1 制度の目的

IoT 製品のセキュリティ確保に向けては、以下に示すとおり、IoT 製品ベンダーにおける課題、IoT 製品調達者・利用者における課題及び国民全体における課題が存在すると考えられることを検討会に提示した。

- IoT 製品ベンダーにおける課題
  - IoT 製品に対するセキュリティ対策状況が適切に評価されず、製品価値の向上に繋がらないおそれがある。
  - 既存制度の認証取得に対する明確なインセンティブが存在せず、認証を取得してもコスト増のみで、製品売上に繋がらないおそれがある。
  - 特定分野のシステムに組み込まれて調達され、利用される IoT 製品類型において、一般的に求められるセキュリティ要件が明確になっておらず、どこまでセキュリティ対策をすればいいか判断が難しいものがある。
  - 諸外国の制度が開始され、その制度と相互承認された国内制度が存在しない場合、諸外国の制度の適合性評価を当該国で受けるための体制整備及びコスト負担が必要となる。
- IoT 製品の調達者・利用者における課題
  - 現状ではセキュリティ対策状況が可視化されていないため、特に消費者をはじめとするセキュリティに関するスキルや知見が十分ではない利用者において、適切な対策が施された IoT 製品を選ぶことができないおそれがある。
  - 調達する IoT 製品のセキュリティ機能や対策状況を自組織で確認するプロセスを実行できている政府機関や企業等は少ない。

- 本来必要なセキュリティ機能を持たない IoT 製品を利用した場合、又は IoT 製品を適切に利用しない場合、当該 IoT 製品がサイバー攻撃を受け、自ら又は他の利用者に対して悪影響を及ぼすおそれがある。

・ 国民全体における課題

- セキュリティ対策が不十分な IoT 製品が販売され、世の中に広く普及した場合、マルウェア感染により IoT 製品がボット化して他のシステムに悪影響を及ぼすリスク、不正アクセスにより利用者のプライバシー侵害に関するリスク、サイバー攻撃により人体への物理的影響を及ぼすリスク等、IoT 製品をきっかけとしたサイバーセキュリティリスクが顕在化する。
- 諸外国は IoT 製品に対するセキュリティ対策の取組を進めているところ、十分な取組を実施しない場合、我が国の IoT 製品が集中的に狙われ、国内のシステムや国民の生活に悪影響を及ぼすおそれがある。

これらの課題を踏まえ、検討会で議論を行った結果をもとに整理した制度の目的について、以下に示す。

IoT 製品に対する適合性評価制度を国内で構築し、広く普及させ、そして社会に浸透させることが適当である。そのためには、まずは調達者・利用者が自身を守るために、求めるセキュリティ水準のラベルが付与された製品を優先的に選択するようになることが必要不可欠である。そのような需要が生まれれば、ラベルを取得していない IoT 製品は市場で選ばれにくくなるため、IoT 製品ベンダーは積極的にラベルを取得することとなる。また、IoT 製品ベンダーが、自己でセキュリティ評価を行うための人的負担を下げつつ、評価の信頼性、客観性を高めるために、外部の専門家や専門事業者に評価を委託することも考えられる。

このようなサイクルを生み出すため、①政府機関等、重要インフラ事業者、地方公共団体等の社会的にセキュリティリスクが高く確かな制度利用が見込まれる組織の IoT 製品の調達要件の中にラベルが付与された製品の選定を取り入れること、②業界標準として IoT 製品ベンダーと調達者・利用者が、ラベルが付与された製品の製造・販売と選定・調達する分野を確保することが適当である。これらにより制度が着実に広まる中で、民間の大企業の調達要件での活用、中小企業や消費者への普及を図ることが適当である。

また、海外製の IoT 製品も広く利用されていることや国内の IoT 製品ベンダーの海外展開を考慮すると、本制度を国内に閉じたものとするのではなく、③諸外国の制度と協調的な制度を構築して相互承認を図ることが適当である。

以上から、まずは以下の三つの目的を主目的として、それに沿った制度の構築を目指すことが適当である。

① 政府機関や企業等で調達する製品について、共通的な物差しで IoT 製品のセキュリティを評価・可視化できるようにすることで、各組織の求めるセキュリティ水準を満たした IoT 製品の選定・調達を容易にする。

② 特定分野のシステムに組み込まれて調達・利用される IoT 製品に求められるセキュリティ要件を定め、必要な認証・ラベルを各業界団体等で指定できるようにすることで、当該特定分野において求められるセキュリティが確保された IoT 製品のみが採用されるようにする。

③　諸外国の制度と協調的な制度を構築し、相互承認を図ることで、IoT 製品を海外に輸出する際に求められる適合性評価にかかる IoT 製品ベンダーの負担を軽減する。

また、将来的には、以下のような IoT 製品のセキュリティを社会全体として確保していくことの実現に本制度が貢献することが望ましい。

- IoT 製品のセキュリティ対策状況を調達者・利用者が価値として認め、IoT 製品ベンダーが対策に要するコストを適切に製品販売価格に反映できるようになる。
- セキュリティに関するスキルや知見に依存することなく、消費者を含む調達者・利用者が、適切な対策が施された IoT 製品を選べるようになる。
- ラベルが付与された製品を調達・利用することで、調達者・利用者としての一定の責務を果たしたとみなされるようになる。
- 調達者・利用者が、セキュリティ機能を備えた IoT 製品を購入するだけでなく、購入後の適切なパスワードの設定、セキュリティアップデートの実施等、自らのセキュリティ対策・管理も必要であることを理解するようになる。

3.1.2 制度の位置付け

本制度構築に伴う効果や関係者の負担等の観点から、本制度を法令に基づく義務とするか、任意制度とするかという点について、検討会で議論を行った。義務とした場合、中小企業をはじめとする IoT 製品ベンダーの負担が増大する可能性があり、国内産業の成長を停滞させるおそれがあることや、規制要求さえ満たせば良いというマインドに繋がるおそれもあり、結果的に、IoT 製品の本質的なセキュリティ確保に繋がらない可能性があることを提示した。他方で、任意制度とした場合、適合性評価を受けることが製品の付加価値向上に繋がり得るものであるため、能動的なセキュリティ向上に繋がりやすい可能性があることを提示した。検討会での議論の結果、本制度はまずは任意制度として運用することが適当であるとの結論に至った。適合性評価を受けた製品に対してセキュリティ要件に応じたラベルを付与することで、製品の付加価値向上に繋げることを意図する。特に、政府機関等で調達する製品については、各組織の求めるセキュリティ水準に合致するラベルが付与された IoT 製品を選定・調達することを推奨し、将来的には義務化も視野に入れることで、IoT 製品ベンダーにラベル取得のインセンティブを与えることが求められる。

また、本制度と関連する国内制度として、CC（Common Criteria）に基づく IT セキュリティ評価及び認証制度（JISEC）、産業用製品に対する IEC 62443-4-2 に基づく CSA（Component Security Assurance）認証制度等が存在する。IoT 機器を対象としている民間の取組としては、CCDS（重要生活機器連携セキュリティ協議会）のサーティフィケーションプログラムが存在する。加えて、本制度の対象製品の一部は、総務省の端末設備等規則に準じることを義務付けられている。さらに、諸外国では IoT 製品の適合性評価制度の検討が進んでいる。既存の関連制度との関係について検討会で議論を行った結果、諸外国制度や国内既存制度で採用されているスキームや基準と比較検討を行った上で、本制度を構築すべきとの結論に至った。また、端末設備等規則を考慮した制度を設計することで、既存の国内法規制との齟齬が生じない制度とすることが適当である。また、関連する既存の国内任意制度とは、将来的な統合や棲み分け・連携の方針を合意し、IoT 製品ベンダーに制度乱立による混乱や冗長による負担を与えないように考慮することが適当である。

3.2 制度の対象製品、要件、基準等

3.2.1 検討方針

制度の対象製品、セキュリティ要件、適合基準等、制度で用いる技術的な要件等に関して検討するために、実際の IoT 製品に対する評価検証を含む実証を行った。また、実証の一環として、技術的な要件等を議論する検討体制としてプレ委員会を組成し、具体的な議論を行った。プレ委員会では、対象製品の定義や IoT 製品共通のセキュリティ要件を策定する機能(機能 1)と、製品・レベルごとの要求基準を満たしていることを示す適合基準及びそれに対する評価方法を策定する機能(機能 2)の二つの機能を設け、特に、☆1[22]のセキュリティ要件案・適合基準案・評価手順案[23]を議論・策定した。実証の実施体制は図 3.2-1 に示すとおりであり、プレ委員会の構成員は表 3.2-1 に示すとおりである。

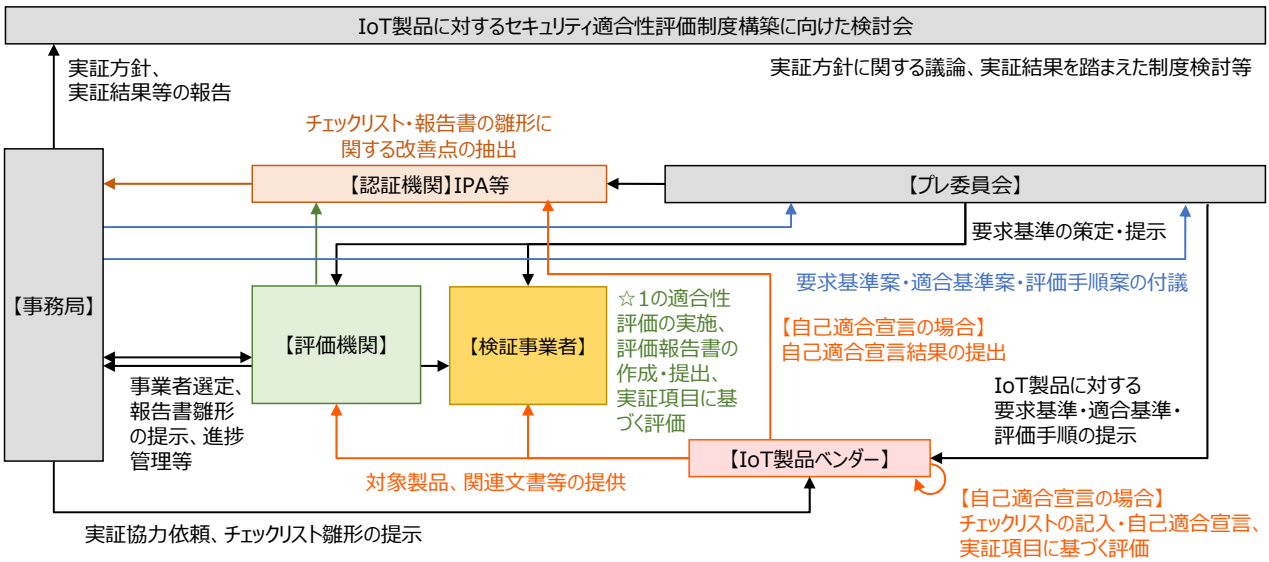


図 3.2-1 実証実施体制

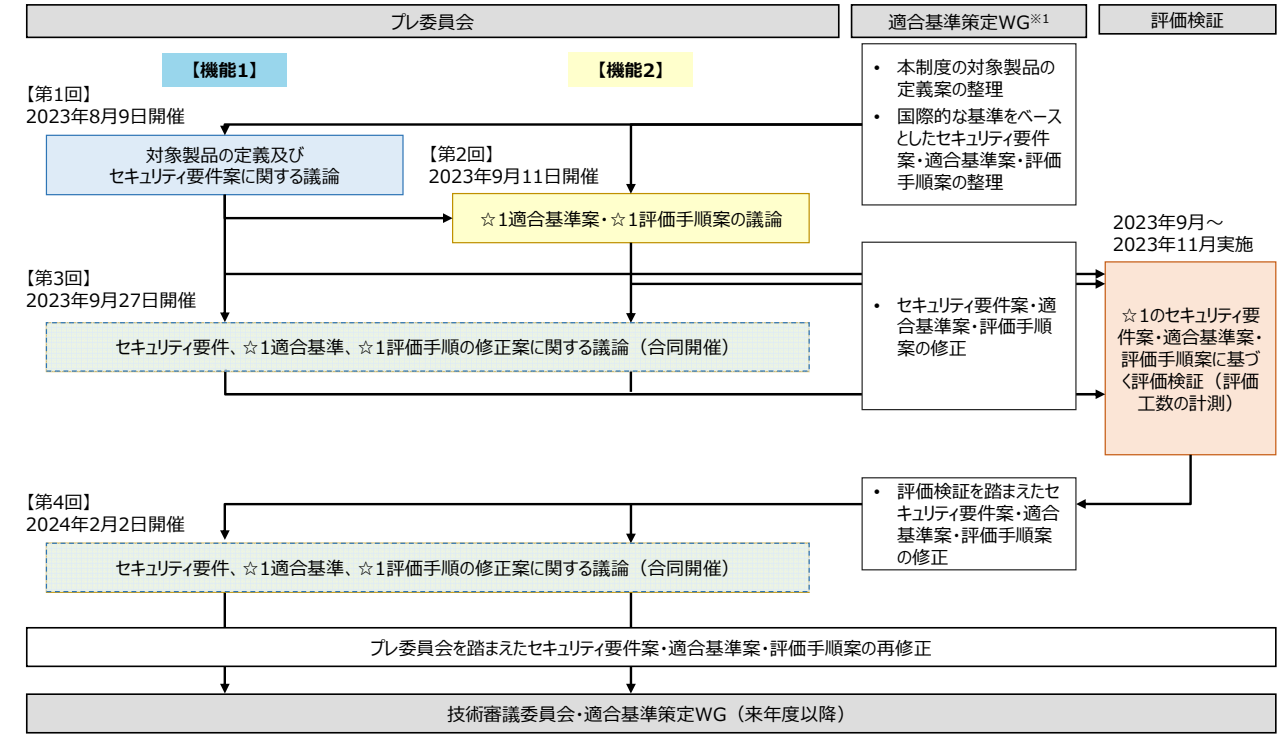
表 3.2-1 プレ委員会の構成員

区分	所属・役職	氏名[24]	機能 1	機能 2
学識者	デジタル庁 シニアエキスパート	江崎 浩＊	●	●
	国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所 主管研究員	中尾 康二＊	●	●
評価機	株式会社 ECSEC Laboratory 評価センター	川岸 敏之	●	●

[22] 本制度における最も低い適合性評価レベル。☆1 の位置付けについては 3.2.3 参照。
[23] セキュリティ要件、適合基準及び評価手順の内容については、3.2.4 参照。
[24] 敬称略、区分ごとに 50 音順。また、「＊」は、検討会においても委員又はオブザーバーとして参画している構成員を意味する。

区分	所属・役職	氏名[24]	機能 1	機能 2
関	長			
	一般社団法人 IT セキュリティセンター 評価部 評価部長	篠崎 明	●	●
IoT 製品ベンダー／ベンダー関連業界団体	一般社団法人電子情報技術産業協会(JEITA)セキュリティ専任部長	岩﨑 章彦＊		●
	一般社団法人日本電機工業会(JEMA)制御システムセキュリティ WG 主査	長島 勝＊		●
	パナソニックホールディングス株式会社 技術部門 テクノロジー本部 製品セキュリティセンター	中野 学＊		●
	一般社団法人情報通信ネットワーク産業協会(CIAJ)	広瀬 良太＊		●
IoT 製品調達関連組織	内閣サイバーセキュリティセンター(NISC)政府機関総合対策グループ 参事官補佐	山出 和豊	●	
	産業横断サイバーセキュリティ検討会(CRIC CSF)副会長	和田 昭弘	●	
既存適合性評価スキーム関係者	PwC コンサルティング合同会社 マネージャー	伊藤 公祐	●	●
	一般社団法人 重要生活機器連携セキュリティ協議会 代表理事	荻野 司＊	●	●
	IPA セキュリティセンター セキュリティ技術評価部 副部長(兼)暗号グループ グループリーダー(兼)評価認証グループ グループリーダー	神田 雅透＊	●	●
	一般社団法人ビジネス機械・情報システム産業協会(JBMIA)情報セキュリティ委員会 委員長	萩原 豊隆＊	●	●

実証の実施プロセスは以下に示すとおりである。本プロセスに示すとおり、まずプレ委員会を開催し対象製品の定義、セキュリティ要件、☆1 適合基準、☆1 評価手順の案について議論を行ったのち、策定した案に基づき、実際の IoT 製品に対する評価検証を行った。そして、評価検証で得られた結果を踏まえセキュリティ要件、☆1 適合基準、☆1 評価手順の案を修正し、再度プレ委員会にて議論を行った。なお、今年度策定したセキュリティ要件、☆1 適合基準、☆1 評価手順については、2024 年度に本制度の技術審議委員会に付議して最終確定する。



※1 今年度は事務局が適合基準策定WGの役割を担い、事務局にて、セキュリティ要件案・適合基準案・評価手順案の検討・作成を行った。

図 3.2-2 実証実施プロセス

評価検証のプロセスでは、以下に示す 10 の IoT 製品に対して、プレ委員会を通じて策定した☆1 のセキュリティ要件・適合基準・評価手順に基づき評価を実施した。評価検証では、全ての製品に対して、ベンダー自身による自己評価のほか、検証事業者及び ISO/IEC 17025 に基づき認定機関より認定された JISEC 制度評価機関による第三者評価を行った。また、一部の製品については、検証事業者による第三者評価を実施した。

表 3.2-2 評価検証対象製品

ベンダー	製品類型	主な提供先
A 社	スマート空気清浄機	消費者
B 社	スマート洗濯機	消費者
C 社	有線 LAN ルーター（2 製品）	法人
	L2 スイッチ	法人
	ワイヤレススピーカー	消費者
D 社	無線 LAN ルーター	消費者
	モバイルルーター	消費者、法人
E 社	有線 LAN ルーター	消費者
	無線 LAN ルーター	法人

以降では、実証を踏まえて検討・整理した制度の対象製品、制度の評価レベル、制度におけるセキュリティ要件・適合基準・評価手順について示す。

3.2.2 制度の対象製品

本制度の IoT 製品の対象範囲を検討するに当たり、消費者向けの IoT 機器を対象にした ETSI EN 303 645 の定義を参考にした。ETSI EN 303 645 の定義では、IoT 製品（IoT product）とは、IoT 機器（IoT device）とその関連サービスを含むものである。IoT 機器とは、ネットワークに接続された（及びネットワークに接続可能な）機器で、関連サービスとの関係を持ち、電子機器として使用される機器のことである。関連サービスとは、IoT 機器とともに IoT 製品全体の一部であり、通常は製品の意図された機能を提供するために必要なデジタルサービスのことである。検討会及びプレ委員会での議論を踏まえ、本制度では国内外の規格や制度の定義を参照し、インターネットプロトコル（IP）を使用したデータの送受信機能を持つ以下の機器を対象に含めることとした。

- インターネットに接続可能な機器：IP を使用してインターネット上でデータを送受信する機能を持つ機器
- ネットワークに接続可能な機器：他の「インターネットに接続可能な製品」や「ネットワークに接続可能な製品」に接続し、IP を使用してデータを送受信する機能を持つ機器

これらの IoT 機器にその関連サービスを含めた IoT 製品を本制度の対象範囲とすることが適当である。対象製品のイメージを図 3.2-3 に示す。

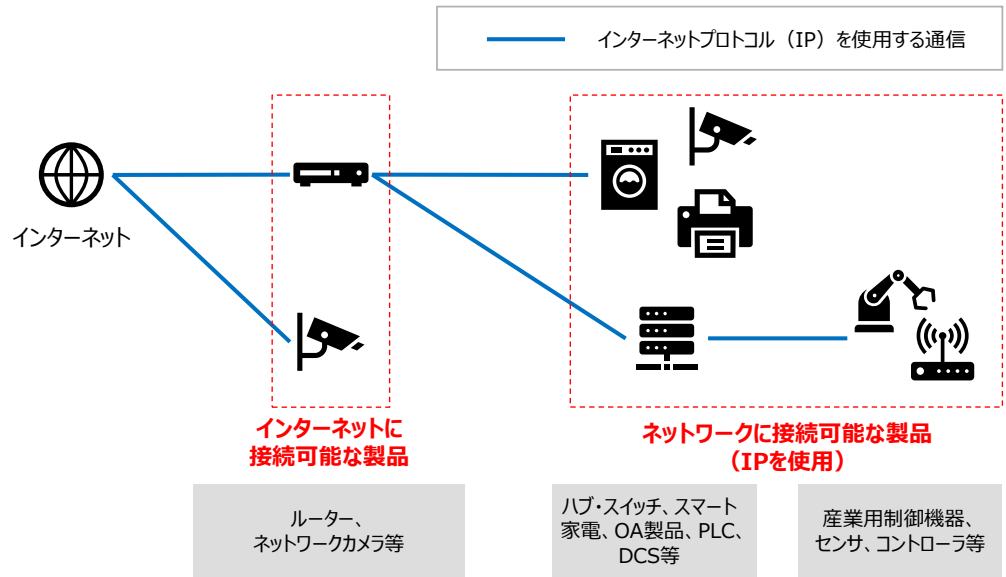


図 3.2-3 本制度の対象とする製品のイメージ

国内外の一部の既存制度と同様に、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的な IT 製品（パソコン、タブレット端末、スマートフォン等）は対象外とした。なお、汎用 OS を搭載した IoT 製品については、利用者が製品本体に対して、容易にセキュリティ対策を追加できない場合は、対象製品としてみなした。

3.2.3 制度における評価レベル

諸外国の制度を見ると、適合性評価レベルが一つのみのパターンもあれば、いくつかのレベルが設定されているパターンもある。例えば、シンガポールの CLS では 4 段階の評価レベルが設定されている一方で、フィンランド、ドイツ及び検討中の米国の制度では、単一の評価レベルのみ設定されている。本制度において適合性評価レベルを複数設定すべきか、複数設定するのであれば、各レベルの位置付けをどのように定めるかについて検討会で議論を行ったところ、以下のような意見が挙げられた。

- 複数のレベルは必要だと思うが、製品の用途を考慮し、各レベルの定義を詳細化する必要がある。同じ型式・製品であっても、用途が違えば求められるレベルは異なる。
- リスクの度合いでレベルを検討する必要がある。
- 最低限のレベルを定めるのであれば、最低限の定義が重要となる。

検討会での議論を踏まえ、製品類型ごとの特性に応じて、求められるセキュリティ要件、適合基準、評価手順や評価方式を設定することとした。各適合性評価レベルの位置付けを表 3.2-3 に示す。本制度では「☆」の数によってレベル分けをする形式とし、☆1 では、IoT 製品共通の最低限の脅威に対応することを想定し、製品類型共通のセキュリティ要件、適合基準、評価手順を整理する方針とした。☆2 以上では、製品類型ごとの特徴を考慮して、セキュリティ要件、適合基準、評価手順を整理する方針とした。また、3.3 節にも記載のとおり、☆1、☆2 では IoT 製品ベンダーによる自己適合宣言を認める一方、☆3 以上では第三者認証を求める方針とした。適合性評価レベルのイメージを図 3.2-4 に示す。

表 3.2-3 各適合性評価レベルの位置付け

レベル	位置付け
☆3 以上	政府機関等や重要インフラ事業者、大企業の重要なシステムでの利用を想定した IoT 製品類型ごとの汎用的な適合基準を定め、それを満たすことを独立した第三者が評価し認証するもの
☆2	IoT 製品類型ごとの特徴を考慮し、☆1 に追加すべき基本的な適合基準を定め、それを満たすことを IoT 製品ベンダーが自ら宣言するもの
☆1	IoT 製品として共通して求められる最低限の適合基準を定め、それを満たすことを IoT 製品ベンダーが自ら宣言するもの

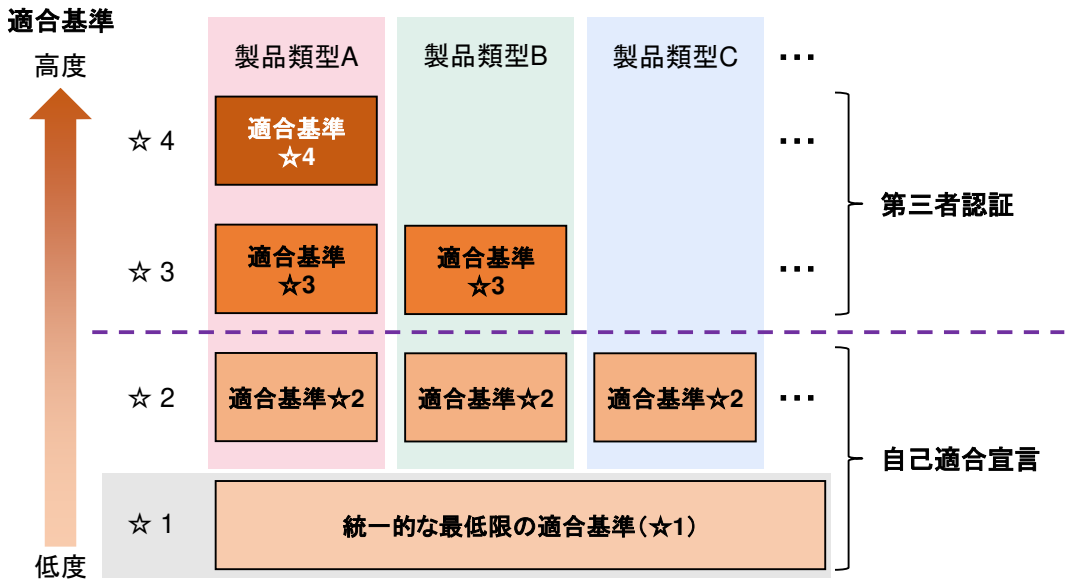


図 3.2-4 適合性評価レベルのイメージ図

3.2.4 制度におけるセキュリティ要件・適合基準・評価手順

本制度で対象とする IoT 製品に求められ得る「セキュリティ要件」、各適合性評価レベルで対象製品が適合すべき基準を示した「適合基準」、当該適合基準に適合しているかを評価するための手順を示した「評価手順」について、検討会及びプレ委員会において議論した。それぞれの関係性を図 3.2-5 に示す。

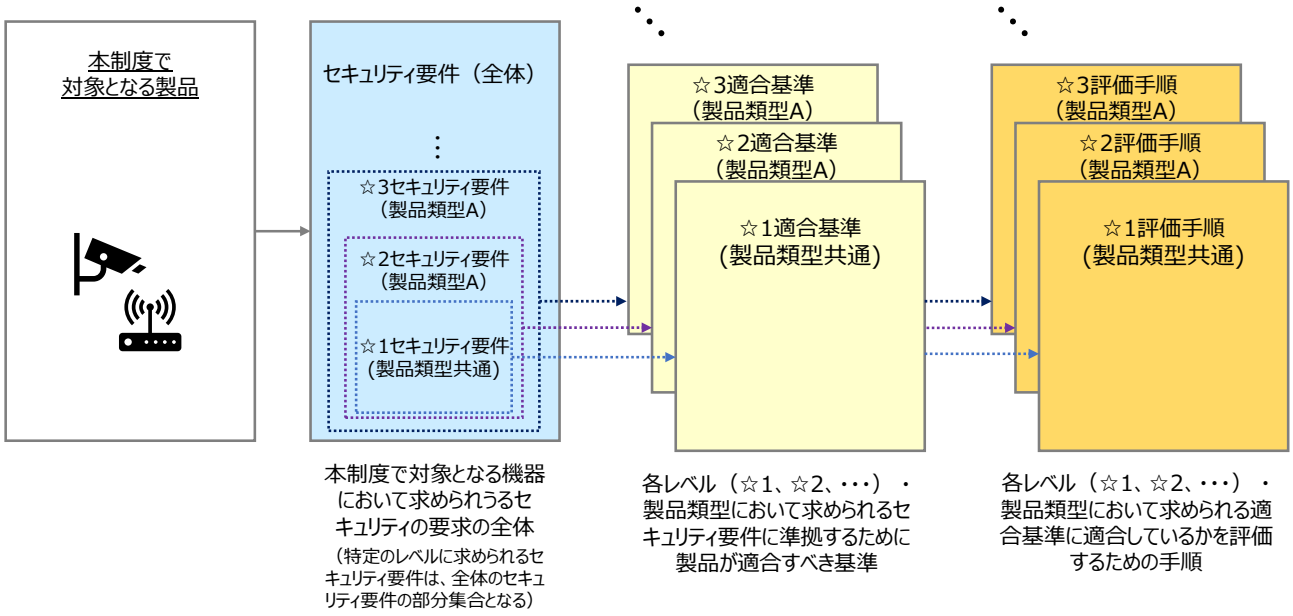


図 3.2-5 セキュリティ要件・適合基準・評価手順の関係性

（1） セキュリティ要件全体リストの整理

2023 年度の検討会及びプレ委員会では、セキュリティ要件の全体のほか、本制度の最低レベルである☆1 のセキュリティ要件、適合基準、評価手順を中心に議論を行った。プレ委員会においてそれぞれの案について議論を行った後、当該案を用いた実証を行った。そして、実証で得られた改善点や修正点を踏まえて修正したセキュリティ要件、適合基準、評価手順について再度プレ委員会で議論を行った。

セキュリティ要件は、本制度で対象となる製品において求められ得るセキュリティの要求事項の全体であり、各適合性評価レベルに求められるセキュリティ要件は、全体のセキュリティ要件の一部となる。2022 年度の検討会の議論を踏まえ、本制度で用いるセキュリティ要件については、国際的な要件と整合的な形で構築する。この方針に従い、まず図 3.2-6 に示すとおり、ETSI EN 303 645、NISTIR 8425、EU-CRA、端末設備等規則等の国内外のセキュリティ要件の集合関係を踏まえ、重ね合わせの関係にあるセキュリティ要件の全体リストを整理した。

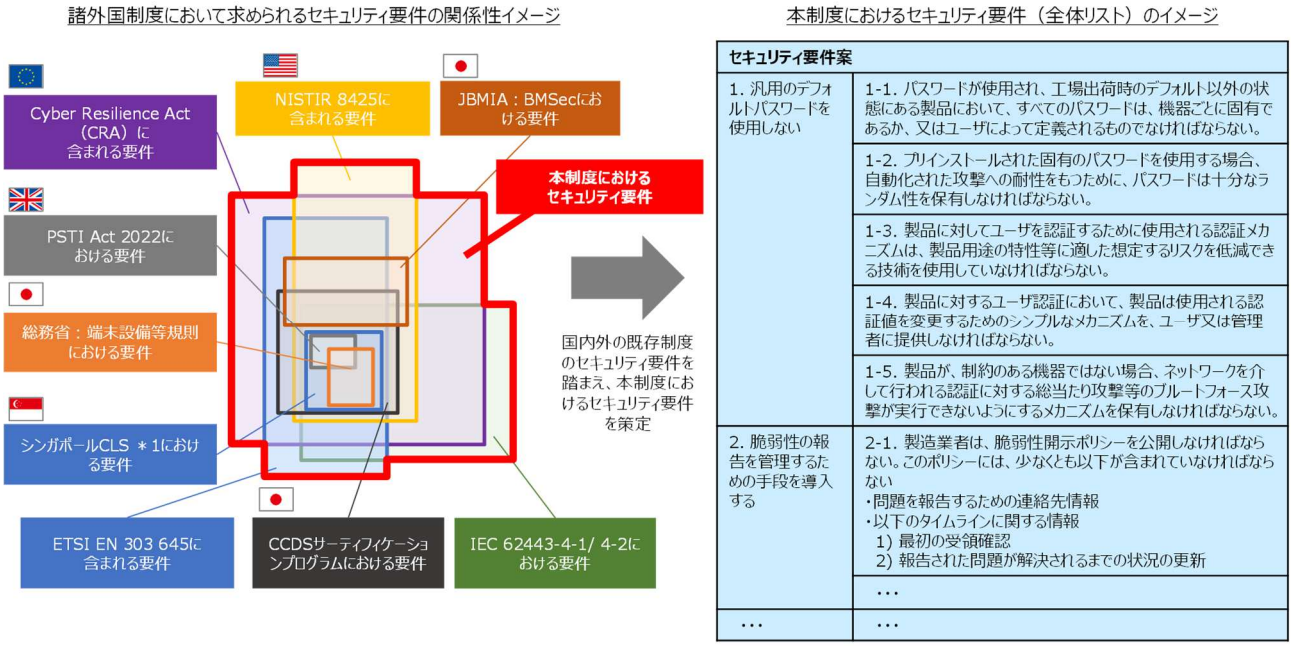


図 3.2-6 セキュリティ要件の整理方針

（2） ☆1 セキュリティ要件の抽出・☆1 適合基準の整理

セキュリティ要件の全体のうち、☆1 で設定するセキュリティ要件を図 3.2-7 に示す方針で整理した。本制度における☆1 の位置付け、☆1 で主に想定する守るべき資産、対象製品におけるアタックサーフェスを踏まえ、☆1 で考慮すべき想定脅威をまず整理した。その上で、☆1 で考慮すべき想定脅威に対して実現すべき対策を整理し、この対策を踏まえ、☆1 で求めるセキュリティ要件を全体リストから抽出した。そして、☆1 セキュリティ要件に準拠するために製品が適合する必要がある基準を、☆1 適合基準として整理した。

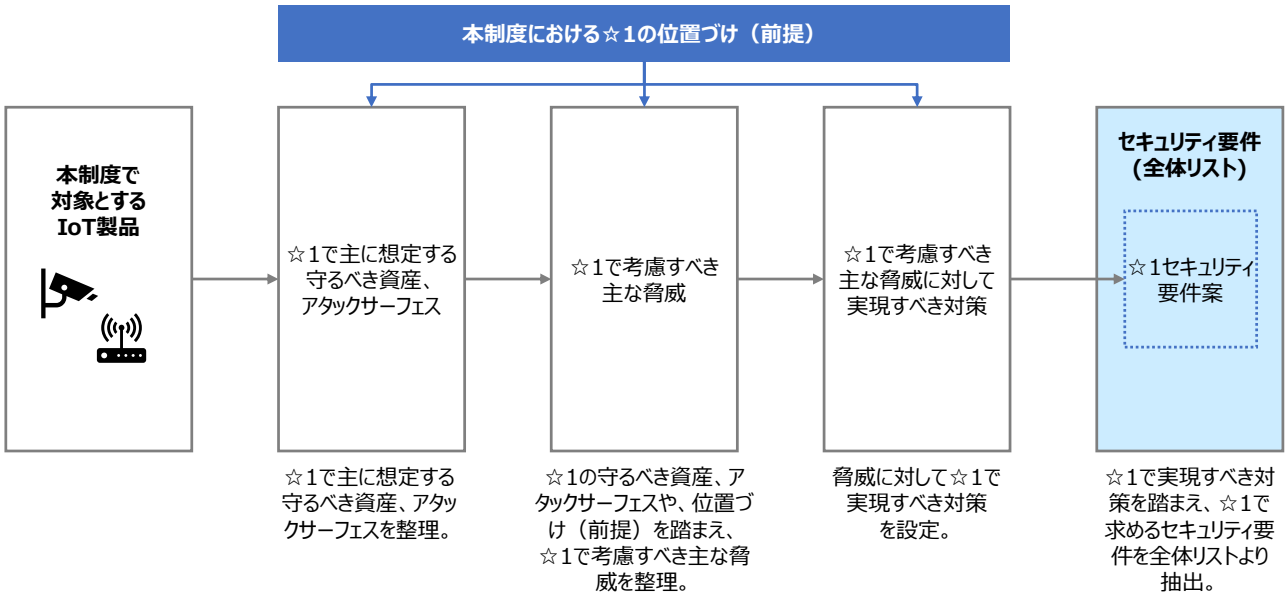
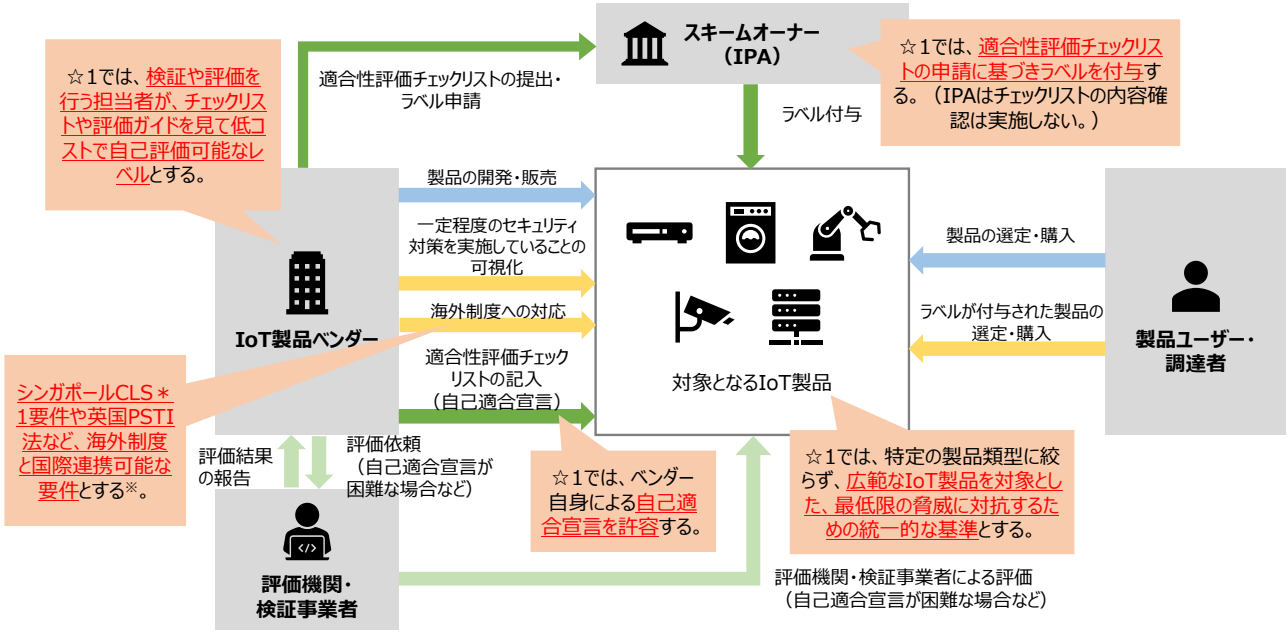


図 3.2-7 ☆1 セキュリティ要件案の抽出方針

本制度における☆1 の位置付け（前提）について、検討会及びプレ委員会での議論を踏まえ、以下の位置付けが前提になると整理した。☆1 では、以下の 3 点を最低限実現することが重要であり、これらを前提条件として、☆1 で守るべき資産、アタックサーフェス、脅威等を整理した。

- ☆1 の適合基準への適合により、最低限の脅威に対抗できる
- ☆1 の適合基準への評価は、低コストかつ自己宣言で対応できる
- ☆1 の適合基準は、海外制度と国際連携可能な基準とする



※ 米国Cyber Trust Mark及びEU CRAの要件は現在検討中であるため、検討状況を注視しつつ、どのレベルで連携するかを検討する。

図 3.2-8 本制度における☆1 の位置付け（前提）

この前提に立脚しつつ、☆1 で想定する守るべき資産を整理した。IPA「つながる世界の開発指針 第

2 版」[25]や CCDS「IoT 機器に対するリスク分析のガイド」[26]等を参照すると、IoT において守るべき資産としては、IoT 機能、本来機能、情報、その他の物理的資産の大きく 4 つの資産分類が存在する。この分類のうち、プレ委員会での議論を踏まえ、☆1 で想定する守るべき資産としては表 3.2-4 に限定した。なお、情報に関する守るべき資産について、IoT 機能やセキュリティ機能に関する設定情報のほか、意図された機器の使用において、機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報を対象とした。

表 3.2-4 ☆1 で想定する守るべき資産

IoT 製品において 守るべき資産の分類	☆1 で想定する守るべき資産	☆2 以上で想定する 守るべき資産
1. IoT 機能: 機器やシステムが IoT につながるための機能	• 有線通信機能 • 無線通信機能	• 有線通信機能 • 無線通信機能
2. 本来機能: 「モノ」本来の機能、セキュリティ対策・セーフティ対策のための機能	• セキュリティ機能	• セキュリティ機能 • 製品本来の機能[27] • セーフティ関連機能[28]
3. 情報: ユーザの個人情報、収集情報、各機能の設定情報など	• 通信機能に関する設定情報 • セキュリティ機能に関する設定情報 • 機器の意図する使用[29]において、機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報[30]	• 設定情報 • 個人情報 • 収集情報 • 接続先機器に関する情報 等
4. その他の物理的資産: ユーザの健康・生命や IoT 機器が内蔵する物理的資産	—	• 人的資産[31] • 物理的資産[32]

次に、☆1 で想定するアタックサーフェス[33]について検討した。前述の IPA 文書や CCDS 文書等を

[25] https://www.ipa.go.jp/publish/qv6pgp000000114a-att/000060387.pdf
[26] https://www.ccds.or.jp/certification/document/ccds_risk-analysis-process.pdf
[27] 例えば、エアコンであれば冷暖房、ドローンであれば飛行のような固有の機能のこと。
[28] 現在の社会の価値観に基づいて、与えられた状況下で、受け入れられないリスクの発生を防ぐ機能のこと。
[29] 製品若しくはシステムとともに提供される情報に従った使用、又はそのような情報がない場合には、一般的に理解されている方法による使用のこと。(JIS Z 8051:2015)
[30] 例えば、個人情報に関する意図する使用はないが、その機器によって扱われるデータに個人情報が含まれ得る機器の場合、想定される運用環境において盗聴の脅威に関して許容不可能なリスクがある場合に限り、対象データを守るべき情報として扱う。具体例としては、防犯カメラが収集する特定の個人が識別可能な映像(個人情報)等が該当するが、ルーターに伝送される個人情報は「意図された機器の使用において、機器が収集」することに該当しないため、対象外となる。
[31] 利用者の健康など、利用者の物理的安全性のこと。
[32] 製品本体や関連する物理的機器のこと。
[33] サイバー攻撃の対象となる攻撃点や攻撃経路のこと。Attack Surface。

参照し、☆1 取得が想定される製品におけるアタックサーフェスとして、(1) 通常使用インタフェース、(2) 保守用インタフェース、(3) 未使用インタフェース[34]、(4) 潜在的攻撃点[35]、(5) 製品廃棄時の物理的接触の 5 つのアタックサーフェスを考慮した。一方、本制度における☆1 で対抗する脅威のレベルを踏まえ、「製品運用時の物理的接触」や「製品開発・調達等のサプライチェーンにおける接触」等のアタックサーフェスは☆2 以上で想定することとした。

☆1 で想定する守るべき資産及びアタックサーフェスを踏まえ、IoT 製品に対して想定される脅威を整理した。☆1 では「製品運用時の物理的接触」のアタックサーフェスを想定しないため、「物理的不正操作(運用時)」や「物理的破壊・窃盗(運用時)」の脅威は対象外となる。同様に、「製品開発・調達等のサプライチェーンにおける接触」のアタックサーフェスを想定しないため、「不正改造」の脅威は対象外となる。加えて、STRIDE モデル[36]では、「否認」が一つの脅威として挙げられているが、☆1 で想定する守るべき資産として「否認」の影響を受ける資産を考慮していないため、当該脅威は対象外となる。以上の整理を踏まえつつ、外部の攻撃者が☆1 で想定する守るべき資産に影響を与えるための脅威のプロセス(ロジックモデル)は以下のように整理できる。本プロセスに基づき、外部の攻撃者が最初に悪用する脅威を踏まえると、対応すべき脅威は 4 つの脅威に集約される。

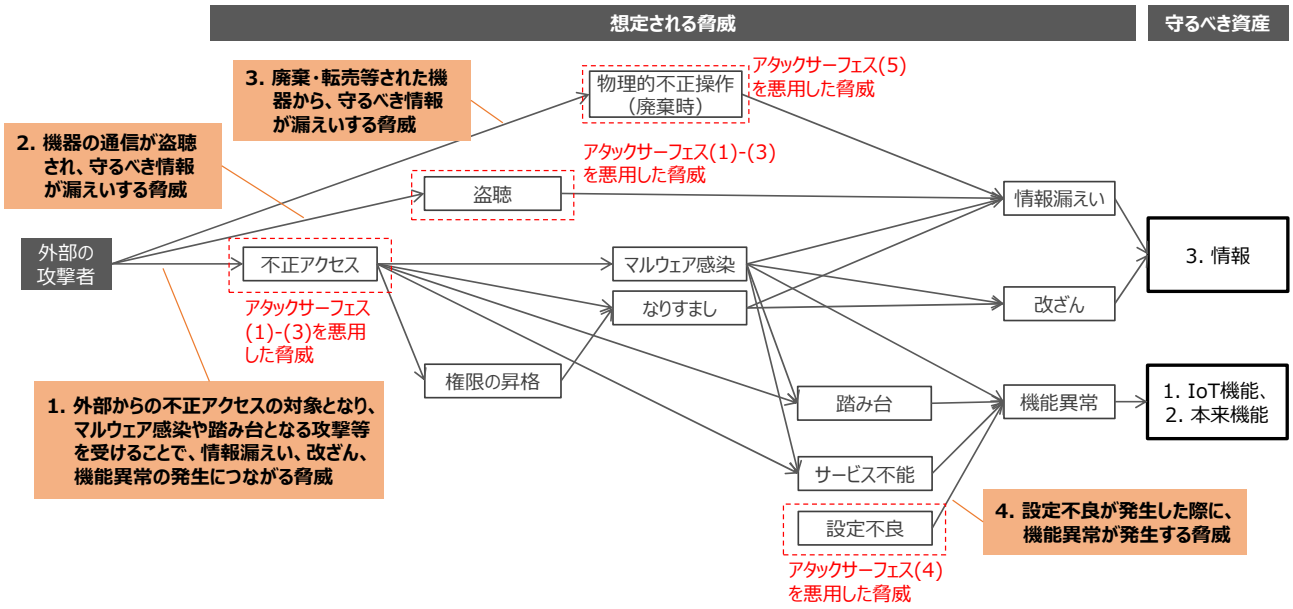


図 3.2-9 想定される脅威と守るべき資産との関係性

これらの 4 つの脅威に対して対応すべきである一方で、☆1 の位置付けを踏まえると、全ての脅威への対応を求めることは困難と想定されるため、☆1 で考慮する主な脅威として絞り込みを行った。これまでのプレ委員会で挙げられた近年のセキュリティ脅威や海外制度を踏まえ、☆1 で考慮する主な脅威として、以下の脅威に絞り込んだ。

[34] 実装されているものの、実際には使用されていないインタフェースのこと。
[35] 故障の原因となるバグ、攻撃対象となる脆弱性、故障や悪用で危害を及ぼす機能等のこと。
[36] Spoofing(なりすまし)、Tampering(改ざん)、Repudiation(否認)、Information Disclosure(情報漏えい)、Denial of Service(サービス拒否)、Elevation of Privilege(権限昇格)の六つの脅威の性質の頭文字から構成され、これら六点の性質から脅威を洗い出していく手法のこと。

想定される脅威	☆1で考慮する主な脅威	☆1での絞り込みの理由
1. 外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威	1. ①弱い認証機能、②脆弱性の放置、③未使用インタフェースの有効化により、外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威	すべての不正アクセスの脅威に対する対策を☆1で求めることは過大であると考えられるため。一方で、近年のセキュリティ脅威の状況や海外制度等を踏まえ、弱い認証機能、脆弱性の放置、未使用インタフェースの有効化に起因する脅威に対しては、最低限対策が必要と考えられるため。
2. 機器の通信が盗聴され、守るべき情報が漏えいする脅威	2. 機器の通信が盗聴され、守るべき情報が漏えいする脅威	–
3. 廃棄・転売等された機器から、守るべき情報が漏えいする脅威	3. 廃棄・転売等された機器から、守るべき情報が漏えいする脅威	–
4. 設定不良が発生した際に、機能異常が発生する脅威	4. ネットワーク切断や停電等の事象が発生した際に、セキュリティ機能に異常が発生する脅威	海外制度等を踏まえ、すべての設定不良への対策を☆1で求めることは過大であり、最低限、総務省の端末設備等規則で求められる対策が必要と考えられるため。

※ 下線部分が「想定される脅威」との差分

図 3.2-10 ☆1 で考慮する主な脅威

☆1 で考慮すべき主な 4 つの脅威に対し、IoT 製品や IoT 製品ベンダーにおいて実現すべき対策を☆1 の位置付けや海外制度の基準等を踏まえて整理した。実現すべき対策に基づき、セキュリティ要件の全体リストから☆1 で求めるセキュリティ要件を抽出するとともに、当該要件に準拠するために製品が適合する必要がある基準を☆1 適合基準として整理した。☆1 で考慮する主な脅威と適合基準との関係性を以下に示す。

表 3.2-5 ☆1 で考慮する主な脅威と☆1 適合基準との関係性[37]

☆1 で考慮する主な脅威			脅威に対抗するために☆1 で求める適合基準			
			IoT 製品に対する適合基準		IoT 製品ベンダーに対する適合基準	
			カテゴリ	適合基準の概要	カテゴリ	適合基準の概要
1.	①弱い認証機能により、	外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を	識別・認証、アクセス制御	(1) 適切な認証に基づくアクセス制御[1-3,5-5] (2) 容易に推測可能なデフォルトパスワードの禁止[1-2,1-1] (3) パスワード等の認証値の変更機能[1-4] (4) ネットワーク経由のユーザ認証に対する総当	情報提供	(16) ユーザへのセキュアな利用・廃棄方法に関する情報提供(初期設定手順、セキュリティ更新、サポート期限、安全な廃棄手順等)[17-12,17-3,17-5,17-8,17-10]

[37] 「適合基準の概要」欄の先頭の”(N)”は対応する☆1 評価項目番号を、末尾の”[N-N]”は対応するセキュリティ要件の番号(複数の場合、代表的な要件を先頭に記載)を示す。また、複数の脅威に対応するための適合基準もあるが、代表的なものにマッピングしている。

☆1で考慮する主な脅威			脅威に対抗するために☆1で求める適合基準			
			IoT製品に対する適合基準		IoT製品ベンダーに対する適合基準	
			カテゴリ	適合基準の概要	カテゴリ	適合基準の概要
		受けることで、情報漏えい、改ざん、機能異常の発生に繋がる脅威		たり攻撃からの保護[1-5]		
	②脆弱性の放置により、		脆弱性対策、ソフトウェア更新	(6) ソフトウェアコンポーネントのアップデート機能[3-1,3-2] (7) 容易かつ分かりやすいアップデート手順[3-3] (8) アップデート前のソフトウェアの完全性の確認機能[3-7,3-2,3-10] (10) ユーザが型式番号を認識可能とする記載・機能[3-16]	情報・問い合わせの受付、情報提供	(5) 連絡先・手続き等の脆弱性開示ポリシーの公開[2-1] (9) セキュリティアップデートの優先度決定方針の文書化[3-8]
	③未使用インタフェースの有効化により、		インタフェースへの論理アクセス	(13) 不要かつリスクの高いインタフェースの無効化(物理的・論理的な通信ポート等)[6-1]	—	—
	①～③共通		データ保護	(11) 製品に保存される守るべき情報の保護(保存データの暗号化、匿名化等)[4-1]	—	—
2. 機器の通信が盗聴され、守るべき情報が漏えいする脅威			データ保護	(12) ネットワーク経由で伝送される守るべき情報の保護(通信の暗号化、保護された通信環境の利用等)[5-1,5-7]	—	—
3. 廃棄・転売等された機器から、守るべき情報が漏えいする脅威			データ保護	(15) 製品内に保存される守るべき情報の削除機能[11-1]	情報提供	※(16)に含む

☆1 で考慮する主な脅威	脅威に対抗するために☆1 で求める適合基準			
	IoT 製品に対する適合基準		IoT 製品ベンダーに対する適合基準	
	カテゴリ	適合基準の概要	カテゴリ	適合基準の概要
4. ネットワーク切断や停電等の事象が発生した際に、セキュリティ機能に異常が発生する脅威	レジリエンス向上	(14) 停電・ネットワーク停止等からの復旧時の認証情報やソフトウェア設定の維持(初期状態に戻らないこと)[9-1]	—	—

(3) ☆1 評価手順の策定

☆1 の評価手順について、シンガポール CLS、CCDS サーティフィケーションプログラム等の国内外の既存制度の評価手順を参照し、「ドキュメント評価」又は「実機テスト」を評価手法として設定し、具体的な評価ガイドを策定した。ただし、☆1 では、IoT 製品ベンダーによる自己適合宣言を許容し、可能な限り低コストでの評価を目標とするため、評価工数が小さいと想定される「ドキュメント評価」を中心とした。

(4) 評価検証結果、プレ委員会での議論等を踏まえた改訂

整理した適合基準及び評価手順の内容について検討会及びプレ委員会にて議論を行うとともに、評価検証において、当該基準及び手順に基づく評価工数を計測した。前述のとおり、10 製品に対する評価検証を行い、IoT 製品ベンダーによる自己評価及び評価機関による第三者評価の両方を実施するとともに、一部の製品については、検証事業者による第三者評価を行った。

評価に要した工数は平均して 23.9 人時間であり、自己評価と第三者評価とで大きな差異はなかった。特に多くの工数を要した評価項目は実機に対するポートスキャン及び脆弱性診断に関する評価項目であったが、これはツール環境構築に多くの工数を要したことに起因しており、2 回目以降の評価は短時間で実施できる見込みであることを確認した。一方で、初回の評価ハードルが高い場合があることは評価検証で明らかとなった結果の一つであるため、このハードルを可能な限り低減するために、環境構築に関するサポート資料(FAQ)等を別途用意することが望まれる。

また、評価の結果、複数の製品における評価項目において、自己評価と第三者評価とで評価結果に差異が生じた。差異の理由は、適合基準や評価手順等が曖昧であったこと、第三者においてドキュメント評価用の文書を受領できなかったことの主に 2 点であった。前者について、実証で得られた結果を踏まえ、可能な限り結果の一意性が保証されるよう適合基準、評価手順等の見直しを行った。後者について、☆1 におけるドキュメント評価用の文書の取扱いについて再整理した。

前述のとおり、今年度のプレ委員会で策定した☆1 のセキュリティ要件、適合基準、評価手順等につい

ては、2024 年度に本制度の技術審議委員会に付議して最終確定する。なお、技術進歩や脅威の状況により求められるセキュリティ対策が日々変化することを踏まえ、本制度開始以降も、セキュリティ要件、適合基準、評価手順等を定期的に見直すことが適当である。☆2 以上のセキュリティ要件、適合基準、評価手順等についても、2024 年度以降、本制度の技術審議委員会及びその配下に設置する適合基準検討 WG で議論を行う必要がある。

また、評価検証結果を踏まえ、本制度における文書の取扱い方針を再整理し、プレ委員会にて議論した。前提として、☆1 では IoT 製品ベンダー自身による自己適合宣言を認め、IoT 製品ベンダー自身による自己評価結果を踏まえて記載したチェックリストに基づきラベル申請を行う。そのため、IoT 製品ベンダー自身で自己評価を行い、ラベルを申請する場合、ラベルの申請段階においては、必ずしも他者にドキュメント評価用の文書を提供する必要はない。ただし、IoT 製品ベンダー自身での自己評価が困難な場合、評価機関等の第三者に評価を依頼し、第三者の評価結果を基にラベル申請を行うことも可能であり、この場合、当該の第三者に対してドキュメント評価用の文書を提供する必要がある。さらに、後述するとおり、ラベル取得後に申請内容に疑義が生じた場合に、IPA が疑義に対する証跡の提出を求める可能性がある。このような場合の文書の取扱いについて、下図における「4.NDA 締結に関わらず IPA 提示不可な文書」をエビデンスとして用いた場合、別途開示可能な説明文書を以て、疑義が生じた場合の説明を行うことを認める方針とした。

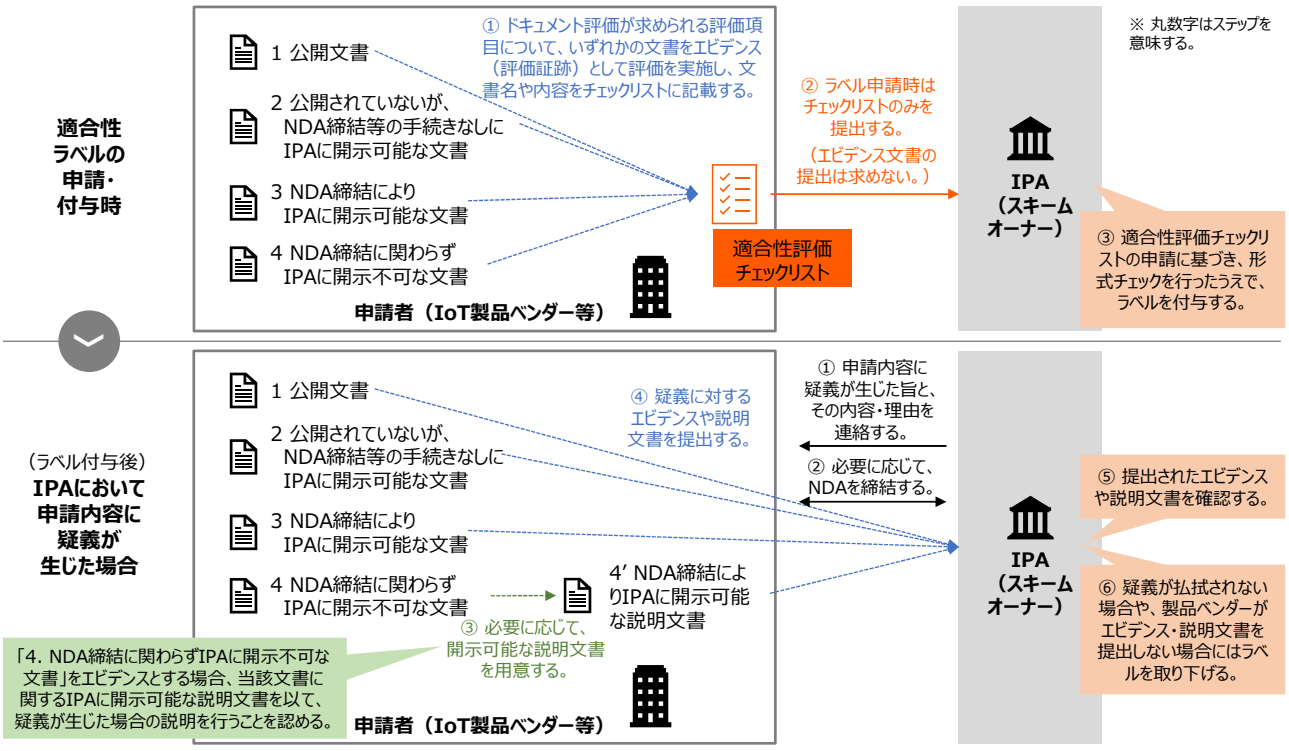


図 3.2-11 本制度における文書等の取扱い

参考として、本制度における適合性評価・申請・ラベル付与のプロセスは図 3.2-12 に示すとおりである。

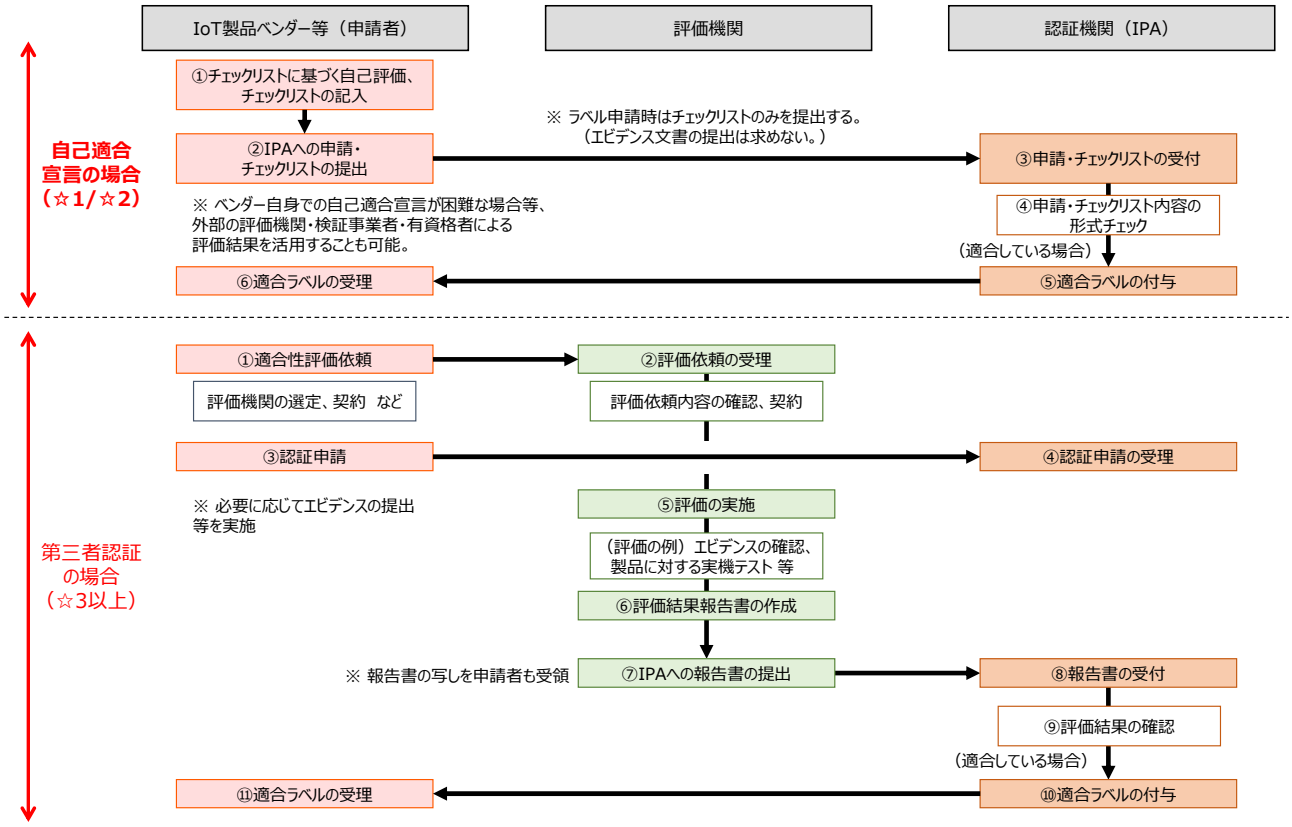


図 3.2-12 本制度における適合性評価・申請・ラベル付与のプロセス

3.3 制度に関係する主体

3.3.1 制度の運用体制

本制度で活用する適合性評価スキームについて、既に運用されている適合性評価スキームの活用と、新たな適合性評価スキームの構築という二つの方針に大別できるが、様々な観点を踏まえ、以下の論点を設定し、検討会で議論を行った。

- 任意制度において、知名度のない制度をゼロから普及させるには高いハードルがあることや、調達者・利用者から見て制度が林立し分かりづらくなる可能性があることから、新たに制度を構築することは避け、既存の適合性評価スキームを活用した制度とすることが適当ではないか。
- 政府機関等が調達時に行う製品セキュリティ評価の代替として活用することや諸外国の制度との相互承認を今後調整していくことから、公的機関である IPA がスキームオーナーの役割を担うことが適当ではないか。
- 現行 CC 認証のみを対象としている JISEC 制度のこれまでの知見やリソースを活用することが適当ではないか。具体的には、本制度を含む形で、JISEC 制度を拡張させる新たな枠組みを立ち上げることが適当ではないか。

検討会での議論の結果、既存の評価スキームを活用した制度とすることが適当であるとの結論に至った。また、本制度に責任を持ち、基本的な規則を維持管理するスキームオーナーには、政府機関等が調達時に行う製品セキュリティ評価の代替として活用することや諸外国の制度との相互承認を今後調

整していくことから、政府のガバナンスが効くことが重要となる。こうした点を踏まえると、経済産業省が所管官庁である独立行政法人情報処理推進機構（IPA）をスキームオーナーとした上で、IPA が運営する JISEC 制度を、CC 認証のみの対象から本制度を含む形に拡張させる枠組み（セキュリティ製品認証・ラベリング制度）とすることが適当である。

運用体制案を図 3.3-1 に示す。IPA の理事長の配下に運営審議委員会と本制度の技術審議委員会を設置することが適当である。運営審議委員会は、既存の JISEC 制度の運営審議委員会を拡張する形で設置し、CC 認証及び本制度の業務運営方針・マネジメントに関する事項等を審議する。本制度の技術審議委員会は、プレ委員会を引き継ぐ形で新設し、本制度についての適合基準の承認・技術的事項等を審議する。また、製品類型ごとの適合基準案の策定は、本制度の技術審議委員会の配下に設置する適合基準検討 WG にて行う。☆2 以上の適合基準検討 WG は、当該製品類型の IoT 製品ベンダーや主な調達組織、それらの関連機関・団体を中心に構成され、策定した適合基準案を本制度の技術審議委員会に付議する想定である。加えて、IPA と経済産業省による本制度の運営事務局を、本制度が軌道に乗るまで設置し、制度拡張、国内既存制度との統合・連携、相互承認等の海外連携の調整、政府調達要件等への働きかけ、民間企業・消費者への制度普及促進、IoT 製品ベンダーへの認証取得促進等について推進することが適当である。

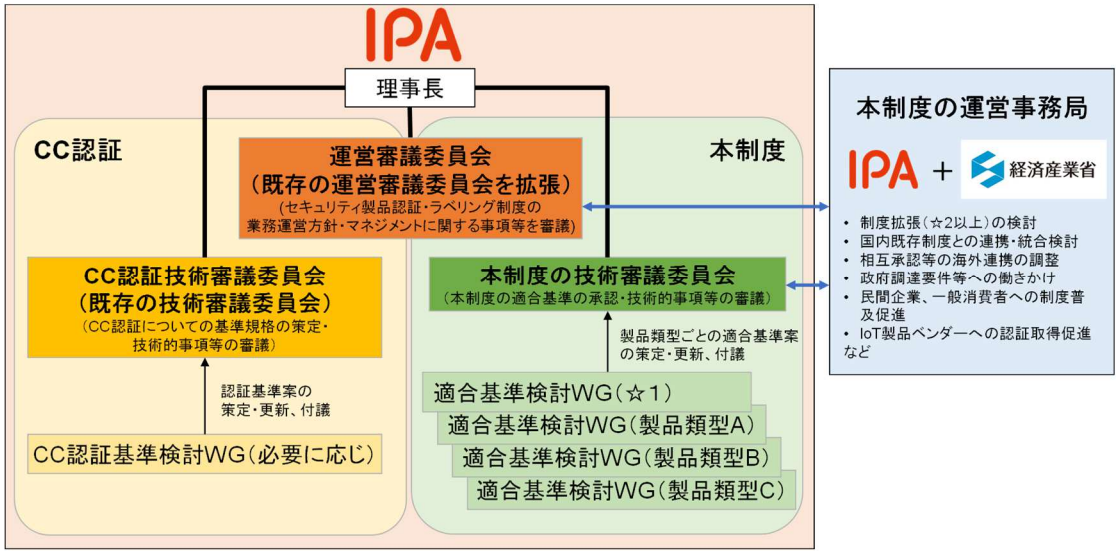


図 3.3-1 セキュリティ製品認証・ラベリング制度の運用体制案

3.3.2 制度における適合性評価の主体

適合性評価において、レビュー及び証明を行う主体が第一者の場合は自己適合宣言、第三者の場合は第三者認証と呼ばれる。各適合性評価レベルにおいて、自己適合宣言を認めるか、また確定活動の実施者を指定するか等について、実効性やコスト、諸外国制度の動向等を勘案して、検討会で議論を行った。各評価活動の定義について、表 3.3-1 に示す。また、各主体が果たすべき主な責務にはどのようなものがあるかについても、議論を行った。

表 3.3-1 各評価活動に関する用語の説明

用語	説明 （ISO/IEC 17000 の記載等をもとに整理）
第一者	適合性評価の対象を提供する人又は組織のこと。
第三者	適合性評価の対象を提供する人又は組織、及びその対象について使用者側の利害をもつ人又は組織の双方から独立した、人又は機関のこと。
確定活動	適合性を判断するために必要な全ての情報を取得する活動、いわば事実を確認する活動のこと。
レビュー	適合性評価の対象が、規定要求事項を満たしていることに関する選択活動（確定活動の準備を整える活動）及び確定活動、並びにこれらの活動の結果の適切性、十分さ及び有効性の検証を行うこと。
証明	レビューに従った決定に基づいて、規定要求事項の充足が実証されたという表明を発行すること。

検討会での議論の結果、本制度を広く普及させる上でも、☆1、☆2 では自己適合宣言を認めることが適当であるとの結論に至った。☆1、☆2 では、IoT 製品ベンダー自身による自己評価を行い、評価結果を記載したチェックリストに基づきラベル申請を行う。申請を受けた IPA は、チェックリストの形式確認を行った上でラベルを付与する。なお、評価を有資格者や検証事業者、評価機関等に委託しても良いこととする。☆3 以上は政府機関等や重要インフラ事業者での活用を想定しており、高い信頼性が求められるため、独立した第三者である評価機関によって評価を行い、IPA が認証機関となり、認証を行うことが適当である。各適合性評価レベルにおける適合性評価の流れを図 3.3-2 及び図 3.3-3 に示す。また、各適合性評価レベルにおける各主体の主な責務は表 3.3-2 が適当である。有資格者の詳細は 3.4.1 項を、検証事業者及び評価機関の詳細は 3.6.3 項を参照のこと。

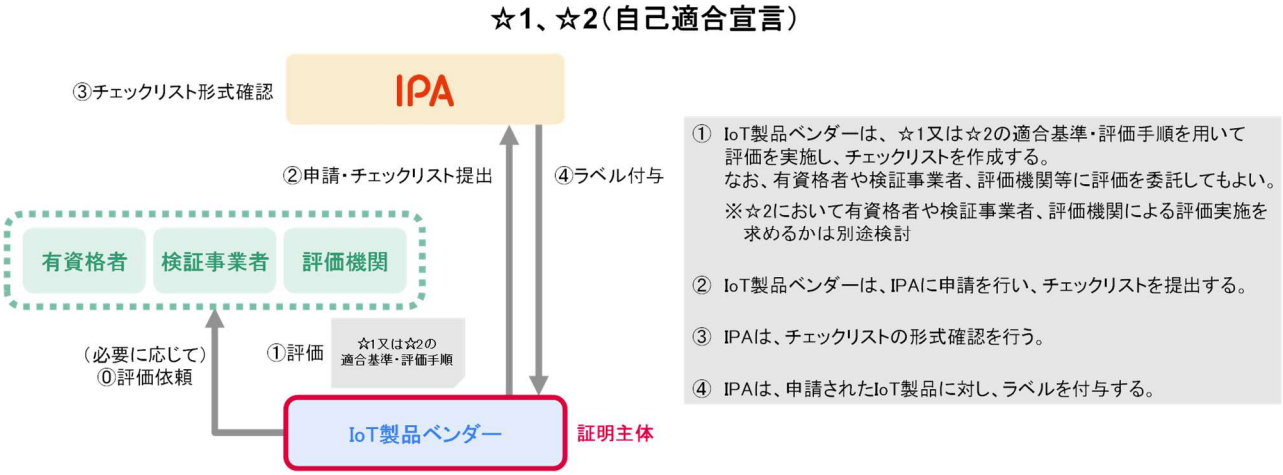


図 3.3-2 ☆1、☆2 における適合性評価の流れ

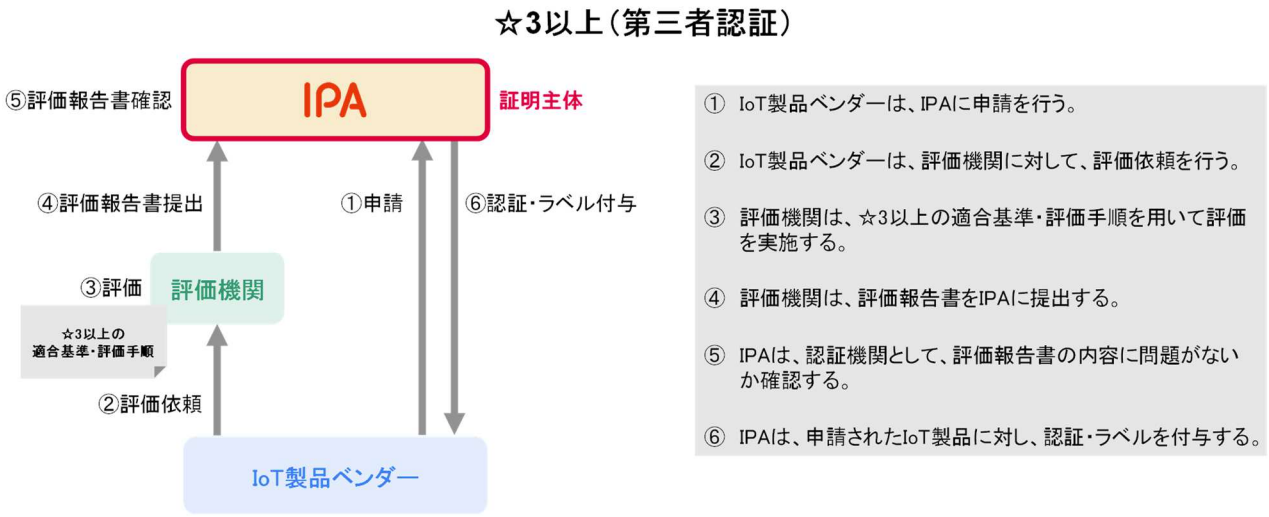


図 3.3-3 ☆3 以上における適合性評価の流れ

表 3.3-2 各適合性評価レベルにおける各主体の主な責務

	IoT 製品ベンダー	評価機関	IPA
☆1、☆2（自己適合宣言）	• 適切に評価を行い、チェックリストに記載した内容について責任を持ち、調達者・利用者から求められれば、それについて説明する責任を持つこと • 付与されたラベルを適切に利用すること • 評価の証跡を、ラベル有効期間中、適切に保管し、評価の適切な実施をスキームオーナーに対して説明できるように情報開示を行うこと • ラベル有効期限内は、申請内容や製品仕様の変更の有無を管理し、変更があった場合、定められた適切な対処を行うこと	－ （評価機関や検証事業者の利用は任意）	• チェックリストの形式を適切に確認した上で、ラベルを付与すること • ラベル付与製品に関する情報を調達者・利用者に対して公開すること • ラベルが適切に利用されるよう管理をすること • ラベルの不適切な利用を認識した場合、適切な対処を行うこと
☆3 以上（第三者認証）	• 付与されたラベルを適切に利用すること • ラベル有効期限内は、申請内容や製品仕様の変更の有無を管理し、変更があった場合、定められた適切な対処を行うこと	• 適切に評価を行うこと	• 評価報告書の内容を適切に確認した上で、認証及びラベル付与を行うこと • ラベル付与製品に関する情報を調達者・利用者に対して公開すること • ラベルが適切に利用されるよう管理をすること • ラベルの不適切な利用を認識した場合、適切な対処を行うこと

3.4 信頼性確保のための仕組み

3.4.1 ラベルのデザインや情報提供方法

IoT 製品が本制度のラベルを取得していることを示すためのラベルはどのようなものが良いか、そのラベルに関してどのような情報を提供すべきか等について、検討会で議論を行った。その結果、本制度

は任意制度であるため、ラベルの表示義務は設けず、IoT 製品ベンダーがラベル取得済みであることを訴求するために、製品本体、パッケージ、マニュアル、パンフレット、Web サイト等に、本制度のロゴ等を任意に掲載できるようにすることが適当であるとの結論に至った。

また、ラベル付与製品に対して、本制度の概要、製品情報、ラベル情報、適合評価結果、安全情報等の多岐に渡る情報を最新に維持しながら調達者・利用者に提供するため、本制度の Web サイトにラベル付与製品ごとの情報提供ページを設け、当該ページの URL を埋め込んだ QR コードを本制度のロゴと合わせて掲示することが適当である。情報提供ページの掲載情報案を表 3.4-1 に示す。ラベル情報の中には、評価者区分を含め、評価能力のある者が評価を行ったかについて調達者・利用者が識別できるようにすることが望ましい。評価者区分としては、IoT 製品ベンダー、IoT 製品ベンダー（有資格者）、外部有資格者、検証事業者、評価機関を想定している。有資格者が評価したと掲載するための条件として、指定資格の保有者（情報処理安全確保支援士等）が、IoT セキュリティ評価に関する研修受講完了又は評価ガイドを理解していることを宣誓した上で、評価又は評価結果の確認を実施することを求めることが適当である。指定資格を情報処理安全確保支援士に限定するか、同等の他資格も許容するかは今後、本制度の技術審議委員会で検討することが適当である。なお、検証事業者、評価機関の説明は、3.6.3 項を参照のこと。

ラベルを掲示している製品に対しては、IoT製品ベンダーの対応負荷を考慮すると、ラベル失効後（再申請予定がない場合の有効期限以降）に出荷予定の製品へのラベル掲載は禁止とするものの、既に製造が完了している製品や製造仕掛中の製品へのラベル掲載の取消は求めず、リンク先の情報提供ページのステータスを「ラベル失効済み」等にすることで対応することが適当である。

表 3.4-1 情報提供ページの掲載情報案

掲載情報	掲載内容
本制度の概要	• 本制度の概要及び詳細説明 HP の URL
製品情報	• 製品名 • 型式番号 • 製造業者名 ※公開/非公開は任意 • 製造国又は地域 ※公開/非公開は任意 • 製品概要 • 製品 Web サイトの URL • 製品の問い合わせ先 • 他認証の認証番号等

掲載情報	掲載内容
ラベル情報	• ラベル識別番号 • 当該製品の適合性評価レベル(☆1～☆4) • 当該製品の製品類型の名称 ※☆2～☆4 の場合 • 評価された適合基準のバージョン • 適合評価結果(チェックリスト又は評価報告書等) • ラベルステータス情報 • ラベル発行・更新日 • ラベルの有効期限 • 申請者名 • 評価者区分
安全情報	• 当該製品に関わる脆弱性情報 • 脆弱性の報告窓口の URL
その他セキュリティ関連情報	• 必要があれば、IoT 製品ベンダーから調達者・利用者に向けたセキュリティ関連情報

3.4.2 ラベルの有効期限

ラベルに有効期限を設けるか、設ける場合、開始日はいつにするか、どれくらいの期限にするか等について、検討会で議論を行った。☆1、☆2(自己適合宣言)については、ラベル取得日を起点として最大 2 年間とする方針としてはどうかという論点を設定し、検討を行った。また、☆3 以上(第三者認証)については、具体案として、「2 年経過後、1 年ごとに製品仕様の変更の有無の自己申告を求め、最大 5 年までの延長を認める(パターン A)」、「2 年ごとに、IPA が指定した項目は評価機関による再評定(攻撃に関わる各種状況(手法、能力、設備)の変化に対し、同じレベルの耐性にあるか確認)、その他の項目は評価機関による形式チェックを行い、問題がなければ追加で 2 年の延長を認める(パターン B)」を提示し、議論を行った。

検討会での議論の結果、☆1、☆2 の有効期限はラベル取得日から最大 2 年間(申請すれば 2 年以内の有効期限も設定可能とする)とし、有効期限を延長したい場合は改めて自己適合宣言を行うことが適当であるとの結論に至った。有効期限内に適合基準のメジャーな改訂(適合基準の項目追加や大幅な変更等)があり、その猶予期間(旧版と並存させる移行期間)が終了したとしても、途中でラベルを失効とはしないことが適当である。ただし、有効期限内に評価に影響を及ぼすレベルでの製品仕様の変更があった場合は、IoT 製品ベンダー自身で確認を行った上でスキームオーナーに報告し、その時点でラベルは失効とすることが望ましい。

☆3 以上の有効期限については、セキュリティトレンドへの対応や、製品のライフタイム、評価に要するコストや調達者・利用者における分かりやすさ等を考慮して、2024 年度以降も引き続き検討を行っていくことが望ましい。

3.4.3 ラベル付与製品への検査やサーベイランス

ラベル付与製品が流通した際に、サーベイランスを実施して不適合の状態でないかを確認し、不適合であった場合には取消措置を行える制度を整えることは、ラベル付与製品の信頼性を担保する上で有効であると考えられる。一方で、特に定期的なサーベイランスの実施については、IoT 製品のライフサイクルによっては効果的ではない場合もあると想定される。このような観点から、ラベルの信頼性確保のための仕組みとして、サーベイランスの実施体制を設けることについて、検討会で議論を行った。また、どのような場合にサーベイランスを実施し、ラベルの取消に至るかについても議論を行った。

検討会での議論の結果、スキームオーナーはラベル付与製品に対して検査やサーベイランスを行える権利を有することが適当であるとの結論に至った。ただし、☆1 に関しては、コストの観点から定期的なサーベイランスは行わないことが適当である。調達者・利用者からの申請やスキームオーナーの判断により、基準への適合に疑義が生じた場合に、申請者に対して評価に使用した証跡の提出を求めることや検査・サーベイランスを実施することが望ましい。証跡の提出に当たっては、必要に応じて秘密保持契約（NDA）を申請者とスキームオーナー間で締結するほか、NDA 締結の有無によらず証跡の開示が困難な場合には、申請者が説明文書を用意し、疑義に対する説明を行うことを認める。また、本制度の信頼性確保のため、付与したラベルを取り消す仕組みを設けることが適当である。具体的には、以下のような状況が発覚した場合、付与したラベルの取消を行う。

- 申請内容が虚偽であることが発覚した場合
- IoT 製品ベンダー等が定められている義務を履行しない場合
- 製品が適合基準を満たさなくなった場合
- サーベイランスで不適合であることが発覚し、猶予期間中に適切な是正措置が行われなかった場合

また、悪質であった場合、若しくは調達者・利用者に与える影響が大きい場合には、スキームオーナーがその旨を一般に周知することが適当である。

3.5 関連機関や国内外関係制度等との連携の仕組み

3.5.1 各組織の調達要件への反映に関する働きかけ

IoT 製品ベンダーのラベル取得を促す仕掛けとして、IoT 製品を調達する各組織の調達要件に本制度のラベル付与製品の取り込みが想定される。調達側としても、ラベル取得を調達要件に含めることで、セキュリティ機能や対策状況を自組織で確認する工数を省くことができると考えられる。調達主体としては、政府機関等、重要インフラ事業者、地方公共団体、大企業等が考えられる中で、本制度の活用を各組織の調達要件へ含めるために、どのような取組が必要か等について、検討会で議論を行った。

検討会での議論の結果、IoT 製品の選定・調達において、本制度をベースとして活用しながら、必要に応じて追加的な確認を実施することで、各組織の求めるセキュリティ水準の IoT 製品を選定・調達できるようになることを目指すことが適当であるとの結論に至った。

政府機関等については、強制力を持たせるため、本制度との連携の必要性及び「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」[38]に盛り込むことを NISC との間で合意した。具体的には、情報システムの重要度に応じて「重要度：低」は☆1 以上、「重要度：高～中」は少なくとも☆3 以上の IoT 製品を各機関等の選定基準に含めることの追加を検討する。なお、ラベル付与製品が普及する時期をめどに、政府機関等では求めるセキュリティ水準に応じたラベル付与製品の調達を必須化する方針で合意した。また、政府機関等の調達において☆3 以上の活用が想定される製品類型として、ネットワークカメラ、ドローン、ファイアウォール、ルーター（有線・無線）等の優先度が高いことを確認した。統一基準群への盛り込みや☆3 以上の整備優先度の高い製品類型の特定に加え、今後、各府省庁の参加する会議の場等で、本制度を活用した製品調達に関する周知を行っていくことも重要となる。

重要インフラ事業者については、NISC と「重要インフラのサイバーセキュリティに係る行動計画」に紐づく安全基準等策定指針及び手引書[39]に本制度の活用に関する記載を追加する方針で合意した。また、各重要インフラ事業者の調達ルールへの反映や重要インフラ分野の特定システムにおける☆2 以上の制度活用の要望について、セプターカウンシル[40]の運営委員会を活用しながら取り組むことを合意した。

地方公共団体については、総務省と調整の上、政府統一基準群が改定された後、地方公共団体の状況に合わせて、「地方公共団体における情報セキュリティポリシーに関するガイドライン」[41]への記載追加を検討した。

本制度の運営事務局と NISC 及び総務省等で協力・連携し、これらの取組を進めることが適当である。その他の民間企業の調達要件に対して直接的にアプローチすることは難しいため、各業界団体や各業種の ISAC 等と連携して取組を促す方針で、本制度の運営事務局が働きかけを行っていくことが適当である。また、政府機関等、重要インフラ事業者、地方公共団体等の調達要件の中にラベル付与製品の選定を取り入れたとしても、実際に調達する際にラベル付与製品が広く普及していないと、セキュリティ面以外の比較ができず、選定時の選択肢が限定されてしまう。そのため、これらの組織で主に調達される IoT 製品を中心に、その関連団体に対して、本制度との連携や会員企業への積極的なラベル取得の働きかけを行うことの賛同を得ることが適当である。

3.5.2 特定分野のシステムに関する業界団体・WG との連携

IoT 製品は、単体で比較・検討されて調達されるだけではなく、特定分野のシステムに組み込まれて調達され、利用されるケースもある。特にリスクの高い分野については、優先的に本制度の活用について検討を行うことが望ましい。このような背景のもと、本制度の初期ターゲットとすべき特定分野や検討の手順等について、検討会で議論を行った。

検討会での議論の結果、セキュリティ知識が不足している中小企業や消費者が、意識しないままセ

---

[38] NISC，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
https://www.nisc.go.jp/policy/group/general/kijun.html

[39] NISC，重要インフラのサイバーセキュリティの確保に関する主な資料
https://www.nisc.go.jp/policy/group/infra/siryou/index.html

[40] NISC，セプターカウンシル総会資料（セプターカウンシルの概要）
https://www.nisc.go.jp/policy/group/infra/siryou/#si09

[41] 総務省，地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会
https://www.soumu.go.jp/main_sosiki/kenkyu/chiho_security_r03/index.html

キュリティ対策が十分でない IoT 製品を利用することでサイバーセキュリティリスクに晒されているという課題を踏まえ、そのような調達者・利用者が多いと考えられる分野のシステムについて、優先的に検討を行うことが適当であるとの結論に至った。また、重要インフラ分野のシステムについても、インシデント発生時の社会的な影響を考慮して優先的に検討を行うことが望ましい。具体的には、スマートホームシステム、ビルシステム、工場システム、電力システム等が候補となり得る。

本制度の運営事務局において、このような検討優先度の高い「特定分野のシステム」について、各システム全体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と連携して、各システムに組み込まれる IoT 製品に求めるセキュリティ要件や☆2 以上の適合基準をその必要性も含めて検討することが適当である。各システムにおいて、IoT 製品を選定する立場の事業者又は当該 IoT 製品を製造するベンダーから、ラベル付与製品の製造・販売と選定・調達について一定割合以上の賛同が得られる場合（業界標準となり得ると判断される場合）、本制度として当該 IoT 製品に対する☆2 以降の整備を進めることが適当である。各特定分野のシステム全体のセキュリティガイドラインの作成や、システム全体の認証制度等の整備は、各業界団体やワーキンググループで検討し、本制度の運営事務局はオブザーバーの立場で連携する方針とすることが望ましい。

3.5.3 諸外国制度との連携

諸外国では IoT 製品の適合性評価制度の検討が進んでおり、海外で IoT 製品を販売している国内の IoT 製品ベンダーは、諸外国制度のラベルの取得のための負担が増えることが想定される。本制度と諸外国の制度の連携を図ることで、負担幅を抑えることが重要と考えられる。諸外国制度の動向（表 3.5-1）を踏まえつつ、国際連携のあり方について議論を行った。

表 3.5-1 諸外国制度の動向

国・地域	シンガポール	英国	米国	EU
制度名	Cybersecurity Labelling Scheme （CLS）	Product Security and Telecommunication Infrastructure Act （PSTI 法）	U.S. Cyber Trust Mark	Cyber Resilience Act （CRA） ※欧州委員会草案の内容
開始時期	2020 年 10 月制度開始	2024 年 4 月施行	2024 年中に開始予定	未定（報告義務を除き 2027 年開始想定）
任意/義務	任意	義務	任意	義務
対象	消費者向け IoT 機器	消費者向け IoT 製品	消費者向け IoT 製品	デジタル製品

国・地域	シンガポール	英国	米国	EU
適合基準	• *:ETSI EN 303 645 の基準の一部[42] • **:*の基準に加え、ETSI EN 303 645 の基準の一部[43] • ***及び****:**の基準に加え、IMDA「IoT Cyber Security Guide」の 9 つのライフサイクル基準	ETSI EN 303 645 の基準の一部（5.1-1、5.1-2、5.2-1、5.3-13）	NISTIR 8425 をベースとした基準となる見込み	• 製造者への「セキュリティ特性要件に従った上市前の設計・開発・製造」、「上市後の積極的に悪用された脆弱性・インシデントの報告」等を義務付ける予定 • 法案の内容について（欧州委員会・議会・理事会間で）政治合意済み。発効後、基準策定機関に対して法案に伴う基準の策定が命じられる予定
評価方式	• *及び**:自己適合宣言 • ***及び****:自己適合宣言及び評価機関による試験	自己適合宣言	第三者認証	• 「重要なデジタル製品」以外の製品:自己適合宣言 • 「重要なデジタル製品」のクラスⅠ（リスクが低い製品）で EUCC や EN 規格の対象外の製品及びクラスⅡ（リス

[42] ETSI EN 303 645 のサイバーセキュリティ規定 5.1-1、5.1-2、5.1-3、5.1-4、5.1-5、5.2-1、5.3-2、5.3-3、5.3-7、5.3-8、5.3-10、5.3-13、5.3-16

[43] ETSI EN 303 645 のサイバーセキュリティ規定 5.4-1、5.4-2、5.4-3、5.4-4、5.5-5、5.5-7、5.5-8、5.6-1、5.6-2、5.6-4、5.8-2、5.8-3、5.11-1、5.13-1 及びデータ保護規定 6.1、6.2、6.3、6.5

国・地域	シンガポール	英国	米国	EU
				クが高い製品)の 製品:第三者認証

検討会での議論を踏まえ、☆1 の制度開始時に既に制度が開始されているシンガポールの Cybersecurity Labelling Scheme(CLS)及び英国の Product Security and Telecommunication Infrastructure Act(PSTI 法)を内包することも考慮し、3.2.4 項のとおり、☆1 の適合基準の策定を行った。☆1 の制度開始時には制度設計途中の見込みである EU の Cyber Resilience Act(CRA)及び米国の U.S. Cyber Trust Mark については、適合基準間の差分を確認し、☆1 の適合基準のメジャーな改訂又は☆2 以上の基準の策定の際に国内基準で包含又は追加対応を要する差分の公表等で対応することで、相互承認の調整を図っていくことが適当である。また、☆1 開始の正式案内時に制度が既に導入されているシンガポールと英国については、正式案内時に相互承認の方向性を提示し、正式案内時に制度設計途中の見込みである欧米については、順次方向性を公表することが適当である。加えて、国際標準化に向けて検討が進んでいる ISO/IEC 27404 等とも連携を図っていく必要がある。

3.6 制度の発展に向けた施策

3.6.1 IoT 製品ベンダーに対するラベル取得促進策

適合性評価を受けるに当たり、IoT 製品ベンダーには様々なコストが発生する。また、適合性評価を受けるために必要なナレッジが足りていない IoT 製品ベンダーも多く存在すると思われる。制度普及を後押しする観点から、コスト抑制やナレッジ提供のための支援策について、検討会で議論を行った。

検討会での議論の結果、特に☆1 は、幅広い IoT 製品ベンダーによるラベル取得を想定しているため、ラベル取得にかかる費用やコストは、大企業だけでなく中小企業でも対応できるような形にすることが適当であるとの結論に至った。IoT 製品ベンダーに対する制度に関する説明や、自己適合宣言時に参考となるドキュメント(ベストプラクティス、評価ガイド等)の提供といった施策の実施について、本制度の運営事務局において検討することが適当である。将来的には、自己評価を行う際に活用できる自動化ツールの提供も検討することが望ましい。また、各種補助金制度との連携や申請費用・第三者評価費用の割引キャンペーンの実施について、本制度の運営事務局において検討し、IoT 製品ベンダーの負担の軽減を目指すことが適当である。加えて、海外の IoT 製品ベンダーへの本制度の普及についても、検討を行っていくことが適当である。

3.6.2 調達者・利用者に対する制度普及促進策

ラベル付与製品が積極的に購入されるようになることが、IoT 製品ベンダーにとってラベル取得の最も大きなインセンティブになる。また、IoT 製品が踏み台攻撃に利用されることも想定されるため、サイ

バー公衆衛生の観点からも、調達者・利用者に対して、IoT 製品のセキュリティリスク、ラベルの意味、ラベル付与製品を選択・購入するメリット、購入後に利用者が実施すべきセキュリティ対策等の啓発を実施することは重要である。調達者・利用者に対する制度の普及促進策について、その効果や他の取組との連携可能性、具体的な喚起方法等について、検討会で議論を行った。

検討会での議論の結果、調達者・利用者に対して、本制度の概要を伝えるのみならず、本制度がどう安全・安心に繋がるのか、ラベル付与製品とそうではない製品とはどのような差があるのかも含めて、本制度の運営事務局が主導し、IoT 製品ベンダーや小売り事業者等と連携しながら消費者に伝えることで、ラベル付与製品の需要を喚起していくことが適当であるとの結論に至った。また、各種補助金制度との連携等を検討し、中小企業・小規模事業者等の調達者・利用者への需要喚起を図っていくことが適当である。

3.6.3 評価機関・検証事業者に対する支援策

☆3 以上では第三者評価を必須とするため、評価機関の本制度への参画は重要である。また、☆1、☆2 でも、自己評価が困難である IoT 製品ベンダーは、評価機関や検証事業者に対して評価を依頼することが考えられるため、評価機関や検証事業者による本制度に対応した評価・検証サービスの提供の後押しが求められると考えられる。以上を踏まえ、評価機関等に対する支援を実施すべきか、また実施するのであればどのような支援策が良いかについて、検討会で議論を行った。

検討会での議論の結果、☆3 以上の評価は、十分な評価・検証能力を保有し、IoT 製品ベンダーから独立した客観的な評価を行える事業者にて実施する必要があり、そのような事業者を継続して確保していく必要があるとの結論に至った。そのためには、独立行政法人製品評価技術基盤機構（NITE）の製品評価技術基盤機構認定制度（ASNITE）の中に、本制度の☆3 以上の評価を行える事業者について ISO/IEC 17025 に基づく評価機関認定制度を設け、適切な能力及び体制を整備した事業者を「評価機関」として認定し、その事業者のみが☆3 以上の評価を実施できるようにすることが適当である。評価機関を継続して確保するためには 3.5.1 項及び 3.5.2 項の取組により、☆3 以上の評価ニーズを継続的に確保することが重要である。

☆1 と☆2 の自己適合宣言では、IoT 製品ベンダー自身による自己評価を許容しているものの、3.4 節で検討した☆1 の適合基準・評価手順にもツールを使用した実機テストが含まれており、☆2 以上では、より専門的な知識や検証環境が求められることが想定される。自社の既存体制や既存設備で十分な評価を実施できない IoT 製品ベンダー向けに、その評価を安心して委託できる一定の評価・検証能力を保有した事業者を「検証事業者」として示すことが適切である。自己適合宣言の対象となる☆1 と☆2 は、☆3 以上よりも多くの IoT 製品がラベルを取得することが想定されるため、評価機関だけではなく、より幅広い事業者を確保していく必要がある。経済産業省が定める情報セキュリティサービス基準への適合性について審査及び登録する情報セキュリティサービス基準審査登録制度の「機器検証サービス」にサービスが登録され、情報セキュリティサービス基準適合サービスリストに掲載されている事業者を「検証事業者」とすることが適当である。また、自己適合宣言における評価機関・検証事業者の活用を促すため、IoT 製品ベンダー向けに以下のような取組を実施することが適当である。

- 自己適合宣言の評価に必要な能力や前提条件、想定工数等を示し、評価を評価機関・検証事業者に委託することのコストメリットを認識させる。

- 自己適合宣言の評価を IoT 製品ベンダー自身が実施したのか、第三者である評価機関・検証事業者が実施したのかをラベル付与製品ごとの情報提供ページに掲載し、調達者・利用者が識別できるようにする。
- 特に自己評価を行う体制や設備が十分でなく、外部に委託する費用の確保が困難な中小企業の IoT 製品ベンダー向けに、評価機関・検証事業者に委託して自己適合宣言を実施する場合の補助金等の支援を検討する。

3.6.4 リスクに対応するための資源の確保策

IoT 製品ベンダー、調達者・利用者、評価機関、認証機関等が各々の責任を果たしていたとしても、サイバー攻撃によって被害が発生する可能性をゼロにすることはできない。事案発生時に適切に対処を行い、被害救済や原因是正に繋がる資源の確保策について、どのような策が効果的か等について、議論を行った。具体的には、社会的にリスク分散するための保険制度や脆弱性関連情報を適切に流通させるための枠組みである「情報セキュリティ早期警戒パートナーシップ」等との連携について、検討会で議論を行った。

検討会での議論の結果、事案が発生した場合に備え、損害を広く分散する社会の構築を目指していくことが適当であるとの結論に至った。例えば、評価機関・検証事業者が提供する評価・検証サービスを受けた製品が原因で発生したサイバー事故による賠償損害や費用損害を補償する商品付帯方式サイバー保険と連携することが考えられる。また、「情報セキュリティ早期警戒パートナーシップ」との連携を図り、ラベル付与製品に関わる脆弱性関連情報について適切な共有体制を設け、早期の対応を促す仕組みを構築することを本制度の運営事務局が中心となって検討することが適当である。

3.6.5 制度全体の効率化

様々な種類のデバイスが IoT 製品として幅広く展開されており、その多様性ゆえに評価対象が増大することが予想される。このような状況においては、本制度における認証・管理業務の効率化が課題となる。効率的なプロセスを確立することにより、製品のラベル付与や認証プロセスにかかる時間とコストを削減し、本制度の持続可能性を確保することに繋がる。以上を踏まえ、認証・管理業務の効率化について、検討会で議論を行った。

検討会での議論の結果、審査から登録廃止に至る業務プロセスの効率化・簡素化を実現するため、ラベル付与機関・認証機関における業務プロセスを具体化し、適用箇所と効率化手法を本制度の運営事務局が検討し、その後、実現可能性を評価することが適当であるとの結論に至った。また、☆3 以上の認証を受けた製品における脆弱性への対処に関して、SBOM や早期警戒パートナーシップの活用も視野に入れ、脆弱性情報を適切に共有し、迅速なパッチ適用を実現するべきである。この際、既に SBOM に関する取組を進めている業界団体との調整に留意する。

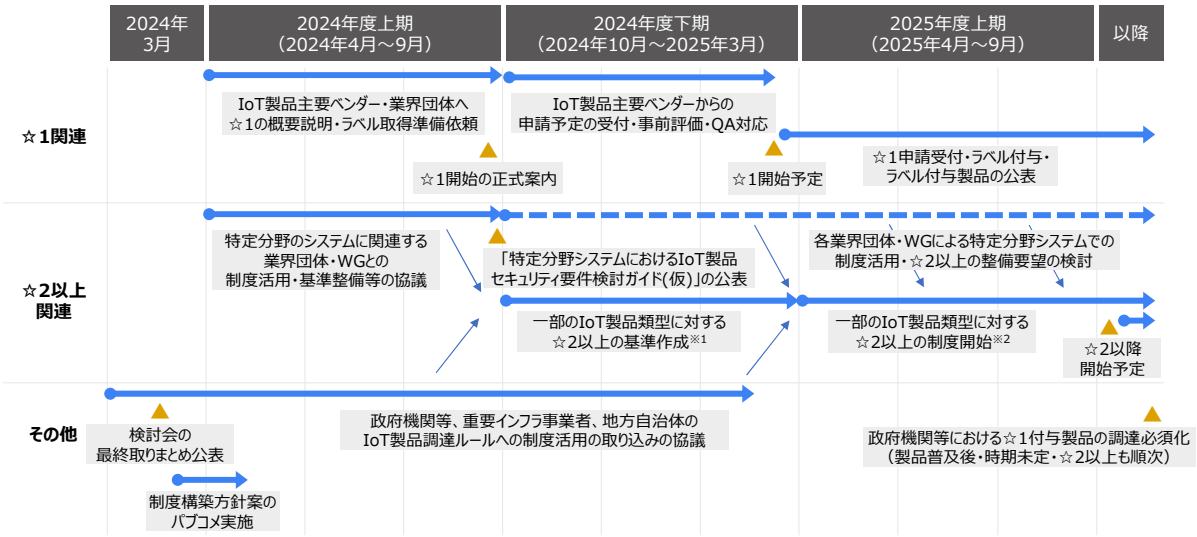
3.7 今後の取組

☆1 に関しては、2024 年度上期に、主要な IoT 製品ベンダーやその業界団体へ概要説明とラベル取得準備の依頼を行い、2024 年度半ば(7 月～9 月頃)に制度開始の正式案内を行う想定である。その際、制度が既に導入されているシンガポールと英国については、相互承認の方向性を提示することが適当である。制度設計途中の見込みである欧米については、順次方向性を公表することが適当である。☆1 のラベル付与の開始は、2024 年度中(2025 年 3 月を想定)を目指す。

☆2 以上に関しては、2024 年度上期に IoT 製品が組み込まれる特定分野のシステムに関連する業界団体・ワーキンググループとの制度活用や基準整備等の協議を行い、2024 年度下期に一部の IoT 製品類型に対する基準を作成する想定である。2025 年度下期以降に一部の IoT 製品類型に対する☆2 以上のラベル付与の開始を目指す。

並行して、政府機関等へのラベル付与製品調達の必須化の調整及び重要インフラ事業者・地方公共団体への IoT 製品調達ルールへの制度活用の取り込みの働きかけを行うことが適当である。

図 3.7-1 に今後のスケジュール案について示す。2024 年度以降の検討は、3.3.1 項で示したように運営審議委員会及び本制度の運営事務局を中心に、本ロードマップに従って推進していくことが適当である。



※1：優先度の高い製品類型(2～3種の想定)が対象、基準が完成次第、順次☆2以降の開始予定を案内
※2：以降、対象となる製品類型を順次拡張

図 3.7-1 今後のスケジュール案

4. 検討会及びプレ委員会の実施

適合性評価制度の構築に向け、昨年度（昨年度内に三回開催）から継続して、有識者による検討会を開催した。今年度は検討会を四回開催した。検討会の開催に当たっては、構成員との日程調整、開催案内謝金支払い等といった事務的な業務を実施したほか、検討会の開催後は、会議の議事録を速やかに作成し、経済産業省に対して提出した。

また、実証の一環として、技術的な要件等を議論する検討体制としてプレ委員会を組成し、具体的な議論を行った。プレ委員会も年度内に四回開催した。検討会と同様に、構成員との日程調整、開催案内謝金支払い等といった事務的な業務を実施したほか、プレ委員会開催後は、会議の議事録を速やかに作成し、経済産業省に対して提出した。

4.1 開催実績

4.1.1 検討会の開催実績

有識者検討会を年度内に四回開催し、IoT 機器のセキュリティ確保に向けた適合性評価制度構築に向けた議論を行った。各回の議事は表 4.1-1 に示すとおりである。構成員からのプレゼンテーションについて、第 4 回有識者検討会では、IPA 神田氏からプレゼンテーションを実施いただいた。第 7 回有識者検討会では、情報通信研究機構 中尾委員からプレゼンテーションを実施いただいた。なお、第 6 回有識者検討会及び第 7 回有識者検討会では、本検討会の最終とりまとめについても議論を行った。

表 4.1-1 IoT 機器のセキュリティ確保に向けた適合性評価制度に関する有識者検討会の開催概要

回・実施日	議事
第 4 回 （2023 年 7 月 19 日）	1. 開会 2. IoT 製品に対するセキュリティ適合性評価制度の構築について 3. 自由討議 4. 閉会
第 5 回 （2023 年 10 月 3 日）	1. 開会 2. IoT 製品に対するセキュリティ適合性評価制度の構築について 3. 自由討議 4. 閉会
第 6 回 （2023 年 12 月 12 日）	1. 開会 2. IoT 製品に対するセキュリティ適合性評価制度の構築について 3. IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討会最終とりまとめについて 4. 自由討議 5. 閉会

回・実施日	議事
第 7 回 （2024 年 3 月 4 日）	1. 開会 2. IoT 製品に対するセキュリティ適合性評価制度の構築について 3. IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討会最終とりまとめについて 4. 自由討議 5. 閉会

4.1.2 プレ委員会の開催実績

プレ委員会を年度内に四回開催し、☆1 のセキュリティ要件案・適合基準案・評価手順案を議論・策定した。各回の議事は表 4.1-2 に示すとおりである。プレ委員会では、対象製品の定義や IoT 製品共通のセキュリティ要件を策定する機能（機能 1）と、製品・レベルごとの要求基準を満たしていることを示す適合基準及びそれに対する評価方法を策定する機能（機能 2）の二つの機能を設けた。各機能の構成員は表 3.2-1 を参照のこと。プレ委員会の第 1 回は機能 1、第 2 回は機能 2 として開催し、第 3 回・第 4 回は機能 1・機能 2 の合同開催とした。

表 4.1-2 IoT 製品のセキュリティ適合性評価制度における基準等の策定に向けたプレ検討委員会の開催概要

回・実施日	議事
第 1 回 （2023 年 8 月 9 日）	1. 開会 2. プレ検討委員会の運営について 3. IoT 製品のセキュリティ適合性評価制度における基準等の策定について 4. 自由討議 5. 閉会
第 2 回 （2023 年 9 月 11 日）	1. 開会 2. IoT 製品のセキュリティ適合性評価制度における基準等の策定について 3. 自由討議 4. 閉会
第 3 回 （2023 年 9 月 27 日）	1. 開会 2. IoT 製品のセキュリティ適合性評価制度における基準等の策定について 3. 自由討議 4. 閉会
第 4 回 （2024 年 2 月 2 日）	1. 開会 2. IoT 製品のセキュリティ適合性評価制度における基準等の策定について 3. 自由討議 4. 閉会

4.2 検討会での主な議論内容

（1） 第 4 回検討会

第 4 回の有識者検討会で挙げられた主な意見は表 4.2-1 に示すとおりである。

検討体制のあり方に関して、ユーザやベンダーの意見を踏まえて検討を行うべきとの意見が挙げられた。制度の運用体制に関して、コストや責任を的確に分担することの重要性やスキームの統合についての意見が挙げられた。適合性評価レベルや製品類型に関して、適合性評価レベルの定義の詳細化や製品類型の括り方、相談窓口についての意見が挙げられた。

セキュリティ要件・適合基準に関して、技術の進歩に従ってセキュリティ要件を更新すべきとの意見や基準の検討に当たり対策の実装段階、製品のライフサイクル、利用者の保守・運用能力を考慮すべきとの意見が挙げられた。評価コストや実証に関して、評価者やベンダーのコストを考慮すべきとの意見や評価コストを検討する上で時間的な流れも考慮すべきとの意見、実証結果から制度の改善点を見つけ出せると良いとの意見が挙げられた。いただいた意見を踏まえ、適合性評価の実証を行った。

ラベルの信頼性確保のための仕組みに関して、ラベルへの QR コードの付記や自己適合宣言の品質を担保するための仕組み、本制度の評価をすり抜けてしまった場合の対応についての意見が挙げられた。諸外国制度との連携に関して、相互承認の重要性、また相互承認ができない場合の対応方針についての意見が挙げられた。IoT 製品ベンダーに対するラベル取得促進策に関して、補助金の導入やセミナー等の開催、自己適合宣言のベストプラクティス等の提示についての意見が挙げられた。調達者・利用者に対する制度普及促進策に関して、消費者への教育・啓発及びラベル取得製品の優先的な購入の重要性についての意見、調達者側に役立つスキーム構築や販売者に対する広報の必要性についての意見が挙げられた。評価機関・検証事業者に対する支援策に関して、評価者の育成や適合性評価に用いるツールの提供についての意見が挙げられた。リスクに対応するための資源の確保策に関して、責任を社会全体で負担する仕組みについての意見や契約書モデルや契約条項モデルについての意見が挙げられた。

表 4.2-1 適合性評価制度に関する第 4 回有識者検討会で挙げられた主な意見

カテゴリ	主な意見
検討体制のあり方について	• 制度の基準に関する議論において、ユーザ（調達者・利用者）組織の参画が重要となる。 • 今年度はプレ検討委員会で適合基準を議論するということだが、運用が始まった後でもベンダーの意見を反映できるような体制を構築していただきたい。
制度の運用体制について	• 社会的にコストを負担する構造も考えていく必要がある。社会の関与の仕方も念頭に置きつつ、本制度について発信することが望ましい。 • 制度において、コストとスケーラビリティは重要な観点である。国が主導する部分と産業界に委譲する部分を分け、運用コストを国に依存し過ぎない仕組みが必要となる。

カテゴリ	主な意見
	• 国内で複数のスキームが林立することは良くないので、スキームの統合について引き続き検討していただきたい。
適合性評価レベルや製品類型について	• 各適合性評価レベルの定義を詳細化する必要があるが、その際、製品の用途を考慮いただきたい。調達者にとって、どの適合性評価レベルの製品を調達すべきかの判断材料となる。 • 全ての IoT 製品の類型に対して基準を作ることは不可能であるため、製品をうまくグルーピングする必要がある。諸外国の取組等を参照すると良い。 • ☆2 以上で製品類型ごとに基準等を策定するとのことだが、どの製品類型に該当するか分からない製品がある場合に相談できる窓口があると良い。
セキュリティ要件・適合基準について	• 技術の進歩に従って、セキュリティ要件を更新していくことが大切である。 • 適合基準の検討においては、対策の実装段階、製品のライフサイクル、利用者の保守・運用能力を考慮していただきたい。
評価コストや実証について	• 評価者が基準の変化に追随するためのコスト、及び評価基準の変化に対応するためのベンダー側のコストも考慮いただきたい。 • 評価コストについて、時間的な流れを考える必要がある。家電業界は機能維持の知見を持っているため、家電業界とも協力しつつ、製品の能力維持に関するコストについて検討していただきたい。 • 実証結果から制度の改善点を見つけ出せると良い。
ラベルの信頼性確保のための仕組みについて	• ラベル付与製品のラベル取得時期や有効期限等の最新情報に辿り着けるような仕組みを検討していく必要がある。QR コードの付与も一つの手段である。 • IoT 製品の脆弱性の検知・共有・活用の課題もある。米国のように、QR コードによる製品の詳細なプロファイルの確認等、脆弱性管理と連動できれば良い。 • ランダムで製品の試買テストを行うなど、自己適合宣言の品質を担保するための仕組みが必要になる。 • 政府調達時に脆弱な製品が紛れた場合の対処法についても検討する必要がある。本制度の評価をすり抜けてしまった場合の対応についても、検討が求められる。
諸外国制度との連携について	• ISO/IEC 27404 においても相互承認の重要性が挙げられている。日本の制度が国際的にガラパゴス化しないようにした方が良い。 • 国際的な相互承認が理想であるが、困難であれば、制度間の要件の差分を確認して部分的に評価するといった仕組みも考えていければ良い。
IoT 製品ベンダーに対するラベル取得促進策について	• コストがかかる取組であるので、インセンティブも検討いただけると良い。補助金など、IoT 製品ベンダーが取組やすくなる仕組みがあると良い。 • セキュリティの知見が不足する IoT 製品ベンダーも多く存在するため、本制度に関する教育プログラムを設けたりセミナーを開催したりすることを検討いただきたい。

カテゴリ	主な意見
	• 自己適合宣言の運用モデルやベストプラクティスが提示されることで、IoT 製品ベンダーとしては対応しやすくなる。
調達者・利用者に対する制度普及促進策について	• 本制度は社会インフラの一部となるので、消費者も社会的コストを担っていく一員としての理解や知識を持つために、行政等からの教育や啓発が必要である。 • 制度の継続的維持のためには、開発・ラベル取得・購入のサイクルを回す必要がある。ラベル取得製品が優先的に購入されるようにしないと制度が利用されず、予算を多く割かなければ維持できない制度になってしまう。 • IoT 機器を活用したシステムやサービスにも対応した適合性評価制度の検討を進める必要がある。調達者側に役立つスキームを構築することで、広く普及すると考えられる。 • 普及活動について、家電量販店や通販サイト等の販売者に対する広報も必要となる。本制度にうまく誘導できるような広報活動が必要となる。
評価機関・検証事業者に対する支援策について	• ISO/IEC 17025 のレベルで全ての評価機関の適格性を担保することは難しいのではないか。評価を行う人材の育成も意識することが重要である。 • 適合性評価に用いるツールを OSS として無償提供することは制度にとってプラスに働く。検証ビジネス事業者にとってはビジネス展開が容易になるほか、制度運用側にとっては評価方法が標準化されることで一定程度の品質保証に寄与する。既存の取組を参照しつつ、本制度を検討していくと良い。
リスクに対応するための資源の確保策について	• 今後、保険等の責任を社会全体で負担する仕組みを考慮しつつ制度を構築していけると良い。 • 責任分界の問題を議論するに当たって、契約書モデルや契約条項モデルを作ることで具体的な議論を行うことができる。

（2）第 5 回検討会

第 5 回の有識者検討会で挙げられた主な意見は表 4.2-2 に示すとおりである。

対象とする製品範囲に関して、制御系製品の取り扱いについての意見が挙げられた。適合性評価レベルに関して、☆1 のユーケースを限定すべきでないという意見や適合性評価レベルによる取得難易度の調整に関する意見が挙げられた。セキュリティ要件・適合基準に関して、☆1の適合基準で個人情報に関する項目も付け加えるべきという意見やレジリエンスについても考慮すべきという意見、データ保護の対策実装可能性について考慮すべきという意見、セーフティに関する要件も加えるべきという意見、開発ベンダーの自由な裁量に委ねるべきだという意見、既に運用されている製品のための要件と今後市場に出る製品のための要件を混同しないようにすべきという意見が挙げられた。

適合性評価の主体に関して、各主体が負うべき責任についての意見が挙げられた。ラベルの信頼性確保のための仕組みに関して、ラベル付与製品の情報提供やラベルのデザイン・掲載方法についての意見が挙げられた。また、サーベイランスは違反の抑止に繋がるとの意見が挙げられた一方、サーベイランスの実施について疑問視する意見も挙げられた。加えて、有効期限の設定について継続的な議論が必

要との意見が挙げられた一方、有効期限を設ける必要はないとの意見も挙げられた。

各組織の調達要件への反映に関する働きかけに関して、ラベル取得製品の使用を強制するよりも、システム設計時に各製品のセキュリティレベルに合わせて、検討すべき要素を訴求する方法が良いとの意見が挙げられたほか、調達要件は普及度に合わせることが重要であるとの意見が挙げられた。調達者・利用者に対する制度普及促進策に関して、セキュリティアップデートの実施を利用者に訴求することの重要性やユーザの性質等に合わせて普及促進策を検討することの必要性についての意見が挙げられた。評価機関・検証事業者に対する支援策に関して、審査を簡素化し評価機関の持続可能性を確保する必要があるという意見が挙げられた。リスクに対応するための資源の確保策に関して、保険や信託制度に関する意見が挙げられたほか、情報セキュリティ早期警戒パートナーシップとの連携に係る課題についての意見が挙げられた。また、被害が発生した場合の責任追及についての意見も挙げられた。

表 4.2-2 適合性評価制度に関する第 5 回有識者検討会で挙げられた主な意見

カテゴリ	主な意見
対象とする製品範囲について	• 制御系の末端機器も技術的に進化している。単純に対象から除外するのではなく、分類の詳細化が必要である。 • 制御系に接続される機器が☆1 の要件を全て満たすことは、現在の技術では実現不可能である。☆1 の要件を求める製品は、インターネット経由でデータを送受信するものに限定すべきである。
適合性評価レベルについて	• ☆1 はホームユースやプライベートユースに限るべきではない。☆1 は IoT 製品に最低限適用すべき基準、☆2 は製品類型ごとに存在する特殊なセキュリティ要件に対応するために満たすべき基準と考える。 • 適合性評価レベルによる取得難易度を調整するためには、責任の量を変更する必要がある。
セキュリティ要件・適合基準について	• ☆1 で考慮すべき主なセキュリティ脅威について、個人情報に関する点も付け加えるべきである。また、扱う個人情報を具体的に列挙することは、☆1 の段階で要求するべきである。 • 防御だけでなく、システムが侵害された場合の復旧力（レジリエンス）も考慮する必要がある。 • データ保護の対策実装可能性は考慮すべきである。一方で、データの汚損が発生した場合、ロボットが正常に停止できるかなど、安全性が確保されているかが鍵となる。 • どの適合性評価レベルで求めるかは今後の議論だが、セーフティ機能に関する要件に含めることも考慮すべきである。 • IoT 製品のセキュリティを製品単体で担保するか、システムとして担保するかは、開発ベンダーの自由な裁量に委ねるべきである。 • サポートの提供方法は開発ベンダーが自由に決定できるようにするべきであり、その判断に資する基準を提供することが重要だと考える。 • 既に運用されている製品とシステムを保護するための要件と、今後市場に出る製品に対する要件を混同しないようにするべきである。

カテゴリ	主な意見
適合性評価の主体について	• 自己適合宣言に関して、負うべき責任の範囲の検討が今後必要である。また、第三者認証についても、責任の範囲や保証内容について検討が必要である。責任の観点をコストとのバランスで考慮することが重要である。 • 日本の競争力を培うためには、責任を負う主体が制度を構築する必要がある。少なくとも IPA においては、制度運営者の監督、製品に関する評価、そして設計レベルの評価等について責任を負う必要があり、そういった責任を果たさない限り、制度自体が活用されない可能性が高い。
ラベルの信頼性確保のための仕組みについて	• 発売後に実施されるファームウェアのアップデートの判断方法について、今後議論したい。ラベルの表示や QR コードの遷移先による情報提供を通じて、前提条件（評価日、評価時のファームウェア等）を確認できると良い。 • ラベルへの有効期限の表示は、ラベルを交換する手間を考慮すると避けるべきである。情報へのアクセスが QR コードを介して行われる場合、小さな製品では本体への表示が難しいこともあるので、梱包箱や取扱説明書に情報を記載する方法も許容いただきたい。 • 責任の所在が明確でない制度でサーベイランスを進めるべきか疑問が残る。 • 製品の寿命が長い場合、サーベイランスが適切だが、IoT 製品など寿命の短い製品に対してサーベイランスを行うことは、コスト面で疑問視される。 • 自己適合宣言において、サーベイランスを行うことでメーカに追加のコストがかかることは問題である。 • サーベイランスに関して、メーカとしては自己適合宣言を得るために必要な要素とも理解できる。サーベイランスによってランダムに検査され、違反があればラベルが取り消されるという抑止策が存在するため、不適切な自己検査は行えなくなる。 • 有効期限は製品のリリース日を起点としている一方、ユーザの視点からは購入日が重要である。期限の設定については、継続的な議論が必要だと考えている。 • 本制度案では有効期限がサポート期限と解釈される可能性がある。アップデートだけがサポートではない。サポート期間に関する要求もメーカに求める場合は、その内容も含めて要件に明示的に記載する必要がある。一方で、セキュリティは時間とともに弱化するものであるため、ラベルはラベル取得時点で設定された要件を満たすことの証明となり、有効期限を設ける必要はないと考える。
各組織の調達要件への反映に関する働きかけについて	• ラベル取得製品の使用を強制するアプローチには違和感がある。システム設計時に各製品のセキュリティレベルに合わせて、検討すべき要素を訴求する方法が良い。初めはラベルを取得していない製品が多いため、調達要件を普及度に合わせることが重要である。

カテゴリ	主な意見
調達者・利用者に対する制度普及促進策について	• セキュリティアップデートの提供は、製造者としての責任と考える。一方で、セキュリティアップデートを適切に適用することも、ユーザとしての責務であることを強調すべきである。 • ユーザの責務について、ユーザを一般消費者と法人とで分けて考えるべきである。☆1 の主要なユーザが一般消費者であることを考えると、ユーザに過度な責務を負わせることは問題だと感じる。ただし、例えばユーザが自動更新を設定でオフにした場合に、ユーザを免責にすることはメーカとしては納得できない。 • ユーザの責任や普及啓発策、需要喚起策について、製品の生活への影響度や消費者のレベル（セキュリティに対する知識への有無）別に考える必要がある。また、セキュリティ対策に受動的な姿勢の消費者がいることも考慮すべきである。それぞれの区分けに基づいて、具体的な対策と費用を考えることが重要である。社会的な資金の流れも考慮しながら検討いただきたい。
評価機関・検証事業者に対する支援策について	• 評価機関が積極的に本制度に参入するかどうかが不明瞭である。国内の企業が国外の評価機関を使用している中で、この制度が普及するかどうか不透明である。責任問題は重要であるが、審査を簡素化し評価機関の持続可能性を確保する必要があると認識している。
リスクに対応するための資源の確保策について	• CCDS のように、制度内で保険を適用し、運用している民間団体が存在するため、公的機関が同じように対応できないことに疑問を感じる。制度の普及を促進するためにも、セーフティネットとしての保険が必要であり、公的機関としてその負担を引き受けるべきだと考える。 • 保険は、技術や制度では対応できない、想定外の事態に備えるためのものである。制度を構築する責任、検査を実施する責任など、責任の範囲を明確にしないと保険制度が機能しない。 • 保険数理と業規制の拘束を強く受ける保険だけでなく、より柔軟な制度設計が可能となる信託制度を資金供給に利用するといった方法も含めて、より幅広い視野で検討することが望ましい。 • 情報セキュリティ早期警戒パートナーシップとの連携について、早期対応に繋がると感じる。しかし、IoT 製品を対象とした脆弱性情報の共有に関して、パッチが完成してメーカの準備が整った段階で情報を提供する仕組みがまだ整備されていないように感じる。今後この点について、具体的に考えていく必要がある。 • 情報セキュリティ早期警戒パートナーシップについて、国内に数が多い製品であれば情報共有が可能だが、国内に数台しかない製品では情報共有が難しい場合がある。輸入の妨げにならない範囲で連携を検討する必要がある。 • 情報セキュリティ早期警戒パートナーシップだけに依存することは難しいと感じる。 • 責任の追及を容易にする制度設計も重要である。被害が発生した場合、集団訴訟のような手続きで被害者全体を救済できる制度も検討するべきである。

（3）第 6 回検討会

第 6 回の有識者検討会で挙げられた主な意見は表 4.2-3 に示すとおりである。

対象とする製品範囲に関して、IoT 製品に組み込まれているソフトウェアも対象に含まれる点について明記した方が良いという意見や汎用 OS が搭載された IoT 製品の取り扱いに関する意見が挙げられた。適合性評価レベルに関して、各適合性評価レベルの定義や意味合い、ターゲットに関する意見が挙げられた。実証に関して、自己評価と第三者評価の実証結果の差に注意し、自己評価が適切に行える体制を整えることが必要であるとの意見が挙げられた。

適合性評価の主体に関して国際的な場で議論した際、自己評価で評価の妥当性が担保されるかについて指摘があったとの意見が挙げられた。ラベルの信頼性確保のための仕組みに関して、ラベル取消に関しては、有効期限を設けて失効させる方針が良いとの意見や定期的な試売テスト、通報制度や苦情処理の仕組みについての意見が挙げられた。

各組織の調達要件への反映に関する働きかけに関して、ベンダーに対して、少なくとも政府はラベル付与製品を確実に使用するという宣言をすると良いとの意見が挙げられた。特定分野のシステムに関する業界団体・WG との連携に関して、セキュリティ要件の検討を進めるための参考資料があると良いという意見や優先度が高いと思われる分野や展開戦略について報告書に記載すべきという意見が挙げられた。また各分野との連携の仕方についての意見も挙げられた。

諸外国制度との連携に関して、ISO/IEC 27404 の活動との連携についての意見が挙げられた。IoT 製品ベンダーに対するラベル取得促進策に関して、開発者向けのガイドブック等の作成についての意見や海外の IoT 製品ベンダーへの普及についての意見が挙げられた。調達者・利用者に対する制度普及促進策に関して、ユーザへのリスク啓発についての意見が挙げられた。今後の検討の進め方及びスケジュールに関して、ベンダーの準備が間に合うか懸念しているとの意見やロードマップの作成についての意見が挙げられた。その他、SBOM に関する意見や NICT との情報共有に関する意見、責任のリバランスに関する意見が挙げられた。

表 4.2-3 適合性評価制度に関する第 6 回有識者検討会で挙げられた主な意見

カテゴリ	主な意見
対象とする製品範囲について	• ハードウェアだけでなく IoT 製品に組み込まれているソフトウェアも対象に含まれる点について、明確に記載しておくと良い。 • 本制度の対象になるかについて、汎用 OS が搭載されたスマート TV のように、第三者がアプリケーションを作成し、組み込むことができる IoT 製品はグレーゾーンだと感じた。
適合性評価レベルについて	• 各適合性評価レベルが具体的にどのような用途で使われる製品を想定しているかを明確に定義する必要がある。各システムにおいて適切な適合性評価レベルを消費者が理解しやすくするために、マトリックスなどを用いて示す必要がある。 • 守るべき資産に関して、人的資産が☆2 以上から考慮されているが、☆1 ではユーザの生命は守らなくて良いと捉えられる可能性があるため、表現の工夫が求められる。

カテゴリ	主な意見
	• 実証の結果から、☆1 の適合基準を満たせば一般的な攻撃には対抗できるという印象を受けた。一般企業においては、☆1 の製品で十分と考える。ただし、センシティブな情報を扱う企業では、☆2 以上の製品を選択することになると考える。 • ☆1 のラベルを取得している製品が☆2 の適合基準を満たせていないとは限らない。☆1 の製品であるから調達しないといった判断が行われないよう調達者側に訴求いただきたい。 • 本制度の☆3 以上と経済安全保障推進法の基幹インフラとの関連性について、検討いただきたい。
実証について	• 自己評価と第三者評価の実証結果の差に注意し、自己評価が適切に行える体制を整えることが必要である。
適合性評価の主体について	• 国際的な場で議論した際、自己評価で評価の妥当性が担保されるかについて指摘があった。
ラベルの信頼性確保のための仕組みについて	• IoT 製品はセキュリティ的に 1、2 年で陳腐化する可能性もある。 • ラベル取消に関しては、有効期限を設けて失効させる方針が良い。 • 自己評価が正確に行えることを前提として、コストとのバランスを取りながら、定期的に試買テストを行い、自己評価の妥当性を確保するための対策を検討いただきたい。 • サーベイランスに加えて、通報制度や苦情処理の仕組みも検討すべきである。
各組織の調達要件への反映に関する働きかけについて	• ベンダーに対して、少なくとも政府はラベル付与製品を確実に使用するという宣言をすると良い。
特定分野のシステムに関する業界団体・WG との連携について	• 特定分野のシステムに組み込まれる IoT 製品に求めるセキュリティ要件の検討を進めるための参考資料があると良い。 • 報告書には優先度が高いと思われる分野についての議論に関しても詳細に記載いただきたい。また展開戦略の詳細についても、明記しておく必要がある。 • スマートホームのセキュリティについて取り組んでいるグループも既に存在するため、実際に動作し、適用されている実例を参考にして、具体的かつ誤解のない形で検討を進めることが良いと考える。 • スマートホームや医療といった個別のケースにおいて、それらの環境への適用方法については、検討の余地がある。これらの点についてもうまくまとめていけるような方針を策定することが望ましいが、まとめきれない領域については一時保留という形も考えられる。
諸外国制度との連携について	• ISO/IEC 27404 の活動に本制度の活動をうまく組み込めれば、相互承認の実現においても理想的である。
IoT 製品ベンダーに対するラベル取	• 評価項目には、企画開発段階で注視すべき事項や、ソフトウェアコンポーネントが最新版であることなど、出荷前に確認が必要な項目が含まれている。このよう

カテゴリ	主な意見
得促進策について	な事柄について、開発者向けのガイドブックなどを作成することも検討いただきたい。 • 本制度を海外ベンダーに対しても普及させることが重要な課題である。
調達者・利用者に対する制度普及促進策について	• ユーザには、リスクがあることを理解いただいた上で、IoT 製品を使用していただくことが重要である。
今後の検討の進め方及びスケジュールについて	• 2024 年度の下期以降に制度運用を開始予定としているが、制度に関する周知期間が半年未満となっている。半年という短い周知期間から、ベンダーとして十分な対応時間が確保できるか懸念している。2024 年度は PSTI 法が義務化されるため、そちらの対応に手一杯になることが予想される。 • 制度構築におけるロードマップを作成いただきたい。ロードマップを作成することで、ベンダー側、消費者側双方で理解が進むと考えている。
その他	• SBOM に関する議論の状況について、報告書に記載いただきたい。SBOM については、プレ委員会で検討しているロングリストにも含まれており、同時に、ほかのグループでも同様のテーマに基づく議論が進行中である。この点を明記すると良い。 • 医療機器の SBOM に関して、JIS T では推奨されており、ベンダーや医療機器団体が対応し始めているため、調整を行い、整合性を確保する必要がある。 • 多くの古いシステムが現存しており、一部の製品は☆1 の適合基準を満たしていない。NICT と情報を共有することが有益であると考える。 • 安全保障や重要インフラの文脈でセキュアなネット社会を築くための制度であると位置付けると、まとまりのある方向性になるのではないか。責任のリバランスの考えは、セキュリティ・バイ・デザインなどに結びついていくものだと考えている。「責任のリバランス」という考えは、セキュリティ・バイ・デザインなどに結びつくものだと考えているが、この言葉を用いることで方針をまとめやすくなり、本制度の検討がスムーズになると考えている。

（4）第 7 回検討会

第 7 回の有識者検討会で挙げられた主な意見は表 4.2-4 に示すとおりである。

対象とする製品範囲に関して、対象製品の表記について、誤解が生じないよう明示すべきとの意見が挙げられた。セキュリティ要件・適合基準に関して、アップデートの時期的な定めについても検討すべきとの意見や☆3 以上のセキュリティ要件の解釈情報についての意見が挙げられた。実証に関して、実証参加企業に対するフォローについての意見が挙げられた。

適合性評価の主体に関して、ラベル発行者や各関係主体のリスクや責任、評価に使用した判断資料の保管及び開示先について明示すべきとの意見が挙げられた。また、IoT 製品ベンダーによる品質の保証の考え方や IPA が負うべき責任についての意見も挙げられた。ラベルの意味合いに関して、付与さ

れたラベルの使い方について明確に示されていると良いとの意見や消費者契約法の観点においても検討が必要との意見が挙げられた。ラベルの信頼性確保のための仕組みに関して、調達者・利用者への情報提供についての意見やラベルの掲示に関する意見が挙げられた。また、☆3 以上の有効期限について、製品のライフサイクルや脅威トレンドの観点を踏まえた意見が挙げられた。加えて、適合基準のメジャーな改訂についての情報共有に関する意見やパッチ適用についての定期的な確認に関する意見が挙げられた。

各組織の調達要件への反映に関する働きかけに関して、システム全体でのセキュリティ担保の基準を設けた上で、☆1 の製品を使用するという判断を認めるべきとの意見が挙げられた。諸外国制度との連携に関して、相互承認は、本制度のガラパゴス化やダブルスタンダードを回避する上で重要な観点となるとの意見が挙げられた。IoT 製品ベンダーに対するラベル取得促進策に関して、本制度に関する説明会を経済産業省や IPA からメーカに対して実施すべきとの意見が挙げられた。調達者・利用者に対する制度普及促進策に関して、家電量販店や販売者と連携したアクションについても検討すべきとの意見が挙げられた。

今後の検討の進め方及びスケジュールに関して、メーカとしての対応可能性や☆2 以上のセキュリティ要件及び適合基準の検討についての意見が挙げられた。そのほか、規格の検討の際にビジネスの観点を意識して動くことの重要性に関する意見が挙げられた。

表 4.2-4 適合性評価制度に関する第 7 回有識者検討会で挙げられた主な意見

カテゴリ	主な意見
対象とする製品範囲について	• 対象製品について、IT 製品の PC やスマートフォン、タブレット等が除外されているが、IT 製品と IoT 製品の違いが不明確である。対象製品の表記について、誤解が生じないよう明確に示していただきたい。
セキュリティ要件・適合基準について	• EU CRA のアップデート期間が 5 年であることも考慮して、本制度においてのアップデートの時期的な定めについても検討いただきたい。 • ☆3 以上はパッケージ化が必要であるため、スキームオーナーはセキュリティ要件の解釈情報を蓄積及び提供することで、適合基準を明確にしていただきたい。
実証について	• 正式版の評価項目が実証時と比べて大きく変わる可能性があると考えているので、実証に参加した企業に対してフォローいただきたい。また、評価項目についてのコメントをどのように反映したのかご教示いただきたい。
適合性評価の主体について	• ラベル発行は責任が伴う行為であり、また偽造といった不正行為を差し止めるため、ラベル発行者に関して明示する必要がある。 • 自己適合宣言の場合、ラベル発行者が法的責任を負わないということであれば、その旨を明示しないとユーザに誤解を与える可能性がある。 • 各関係主体のリスクや責任を明示すべきである。それにより、IoT 製品ベンダーやユーザが安心して制度を利用できる。 • 評価に使用した判断資料の保管及び開示先について明示する必要がある。 • 本制度の任意性を考慮すると、ラベルの掲示は、IoT 製品ベンダーがチェックリストに含まれている要件に関するセキュリティの担保について自己宣言を行うこ

カテゴリ	主な意見
	とに等しいため、品質の保証とみなされる。そのため、品質が満たされていない場合、IoT 製品ベンダーが返金や製品回収といった責任を負うことになると理解している。 • IPA は、自身の認証作業・手続きに関する責任を負うが、それ以外については責任を負わないという整理になる。
ラベルの意味合いについて	• 付与されたラベルの使い方についても明確に示されていると良い。 • 消費者契約法の観点においても、検討が必要である。
ラベルの信頼性確保のための仕組みについて	• 適合性評価の結果は、あくまで評価時の確認結果であり、ユーザが購入するタイミングや将来的なセキュリティまでは担保されていない。その点について、ユーザも同じ認識となるよう、制度開始後を含めて周知等の取組を行っていただきたい。 • 製品開発の際、パッケージデザインは早めに検討を行うため、ラベル取得まで待つと、パッケージの用意が間に合わない。ラベルをシール状にした場合、シールの貼り付けにはコストがかかる点が懸念される。 • ☆3 以上を取得する IoT 製品では、製品寿命が 5 年を超えるようなものが多く存在するため、その点を考慮した方がいい。一方、セキュリティは継続した取組が必要であり、アップデートが必要になる点についても考慮いただきたい。 • ☆3 以上の有効期限について、2 年経過後、1 年ごとに製品仕様の変更の有無の自己申告を求め、最大 5 年までの延長を認める一方、IPA が状況を見ながらトレンドに応じて各自に再確認を依頼する方式が良い。 • ☆3 以上の有効期限について、2 年ごとに、IPA が指定した項目は評価機関による再評定、その他の項目は評価機関による形式チェック（インタビューベースでの確認）を行い、問題がなければ追加で 2 年の延長を認める方式が良い。脅威のトレンド変化に合わせてアップデートを行うことが重要であり、2 年ごとに簡易的に確認を行う形が IoT 製品ベンダーのモチベーション向上にも繋がると考えている。 • 有効期限の長期延長は現実的ではないと考えている。また、トレンドに応じた対応も大変な作業であると認識している。 • 適合基準のメジャーな改訂が行われる前に、改訂内容や時期について、IoT 製品ベンダーに事前公開いただけるとありがたい。 • パッチが適切に適用されているかについての定期的な確認を本制度の評価スキームにどのように組み込むかについては、別途検討が必要である。脅威の変化が本制度に与える影響も、注視すべき重要な観点である。
各組織の調達要件への反映に関する働きかけについて	• 調達要件において、無条件に☆3 以上を必須とするのではなく、☆1 取得製品も利用できる余地を残すようなルールを構築していただきたい。システム全体でのセキュリティ担保の基準を設けた上で、☆1 の製品を使用するという判断を認めるべきである。

カテゴリ	主な意見
諸外国制度との連携について	• 諸外国制度との相互承認は、本制度のガラパゴス化やダブルスタンダードを回避する上で重要な観点となる。
IoT 製品ベンダーに対するラベル取得促進策について	• 本制度に関する説明会を経済産業省や IPA から、メーカに対して実施していただきたい。
調達者・利用者に対する制度普及促進策について	• 米国と同様に、家電量販店や販売者と連携したアクションについても検討いただきたい。
今後の検討の進め方及びスケジュールについて	• ☆1 開始の正式案内が 2024 年 9 月、☆1 開始が 2025 年 3 月であると、メーカとしては対応が難しい。 • 2024 年度以降、製品類型ごとに要求するレベルについて、迅速に検討いただきたい。
その他	• 欧州では規格を検討する際には、ビジネスの観点を重視して動くことが一般的であり、その点で日本が取り残されている印象を受けた。

5. 総括

本事業では、IoT 機器のセキュリティを確保するための諸外国の取組やその他国内外のセキュリティ対策等を調査した。本調査結果、検討会での検討結果、実際の IoT 製品に対する評価検証の結果、プレ委員会での検討結果等を踏まえ、IoT 機器のセキュリティ確保に向けた適合性評価制度の構築に向けた検討を実施した。本検討では、制度の目的及び位置付け、制度の対象製品、求めるセキュリティ要件や適合基準、制度に関係する主体、信頼性確保に向けた仕組み、関連機関や国内外関係制度等との連携の仕組み、制度の発展に向けた施策等の様々な論点に関して検討を行った。検討を通じてとりまとめた検討会の「最終とりまとめ」及び☆1 セキュリティ要件・適合基準は 2024 年 3 月 15 日に公開するとともに、同日より、制度構築方針案に対する意見公募を開始した。

今後、意見公募で寄せられた意見を踏まえ、必要に応じて制度構築方針や☆1 セキュリティ要件・適合基準を見直すことが必要である。また、3.7 に記載のスケジュール案を踏まえ、☆1 のラベル付与開始や、☆2 以上の検討を行うことが必要である。並行して、政府機関等へのラベル付与製品調達の必須化の調整及び重要インフラ事業者・地方公共団体への IoT 製品調達ルールへの制度活用の取り込みの働きかけを行うことが適当である。本制度は、関係するステークホルダーが多岐にわたり、IoT 製品ベンダー、IoT 製品の調達者・利用者、さらには国民全体に広く効果を及ぼすところ、関係者との対話を適切に行いつつ、検討を進めることが重要となる。

令和5年度産業サイバーセキュリティ強靭化事業

（IoT機器や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

IoT適合性評価制度関連

2024 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5年度産業サイバーセキュリティ強靭化事業
（IoT機器やソフトウェアのセキュリティ確保等に関する調査）

報告書 - 第５編

インド太平洋地域向け日米EU産業制御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

2024年3月29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

2023年秋に5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・関係施設視察・セミナー・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、重要インフラ事業者、製造業者、ナショナルCSIRTからの受講生 35 名が受講した。

産業制御システムにおけるセキュリティ規制・基準のあり方について、欧米やインド太平洋諸国とも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ワークショップを 2023 年 10 月 11 日と 13 日の 2 日間にわたり対面形式で開催した。なお、2023 年 10 月 9 日から 10 日及び 12 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 2023（以下、サイバーセキュリティ・ウィーク）」として、全5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）、米国国土安全保障省（DHS）および米国国務省（DOS）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）、欧州委員会の通信ネットワーク・コンテンツ・技術総局（DG CONNECT）の協力の下、2023 年 10 月 9 日から 13 日までの 5 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 6 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 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実施をした。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、本プログラムにより、日米欧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
  - J202 (ICS セキュリティハンズオン＆ディスカッション)
  - J402(プロセスオートメーションセキュリティハンズオン)

(3) ワークショップ(ICS サイバーセキュリティセミナー)

- 政策セミナー
- 標準化セミナー
- インシデントレスポンスセミナー
- サプライチェーンリスクマネジメントセミナー

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、バングラデシュ、インド、スリランカ、モンゴル、台湾)の推薦をうけた 35 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、製造業者や、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。

また、セミナーセッションに関しては、ICSCoE の中核人事育成プログラムの研修生がオーディエンスとして録画受講している。

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 ： 10 月 9 日(月)		
12:20-13:00		受付
13:00-13:30		プレオープニングセッション
13:30-17:30	H1	J202-1 ハンズオン
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

2 日目 ： 10 月 10 日(火)		
9:00-9:30		受付
9:30-12:00	H2	J202-2 ハンズオン
12:00-13:00		昼食

13:00-17:30	H3	J202-3 ハンズオン

3 日目 ： 10 月 11 日(水)		
9:00-9:40		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
10:10-11:20	C1	基調講演
11:20-11:30		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	標準化セミナー
15:00-16:00		バス移動
16:00-17:30	O2	施設見学(IPA)

4 日目 ： 10 月 12 日(木)		
9:00-9:30		受付
9:30-12:00	H4	J402 ハンズオン

5 日目 ： 10 月 13 日(金)		
9:00-9:40		受付
9:40-10:40	S3	インシデントレスポンスセミナー
10:40-10:50		ショートブレイク
10:50-11:50	S4	サプライチェーンリスクマネジメントセミナー
11:50-12:00		ショートブレイク
12:00-12:40	C2	クロージングセレモニー

1.3 各セッションの概要

1.3.1 プレオープニングセッション／Pre-Opening Session

サイバーセキュリティ・ウィークの開始にあたって、イベント全体についての説明等が行われた。

- 司会者挨拶、サイバーセキュリティ・ウィークに関係するプロジェクトチーム紹介。
- プログラム概要の説明。
- ICSCoE とその訓練施設についての紹介、バーチャルツアー。

1.3.2 J202 ハンズオン／J202 Hands-on

本トレーニングは以下を目的として開催された。

- 簡易な ICS テストベッドを用いて、基本的な ICS サイバーセキュリティの知識と技術を習得する。

- ICS サイバーセキュリティに関するベストプラクティス、ガイドライン、教訓について参加者とグループディスカッションを行う。
- ICS 環境におけるセキュリティ対策の課題を共有する。

1.3.3 J402 ハンズオン／J402 Hands-on

本トレーニング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。

1.3.4 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。10 月 9 日の J202 演習後に実施した。

1.3.5 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	● 吉田 宣弘，経済産業大臣政務官 ● Mr. Raymond F. Greene, Deputy Chief of Mission, U.S. Embassy Tokyo ● Mr. Jean-Eric PAQUET, EU Ambassador to Japan
基調講演	● 門林 雄基，奈良先端科学技術大学院大学教授 ● Ms. Jen Easterly, Director, CISA ● Ms. Lorena Boix Alonso, Director for Digital Society, Trust and Cybersecurity, European Commission

1.3.6 政策セミナー／Policy Seminar

日本、米国、EU の政策当局者が、各国のサイバーセキュリティ政策や戦略の最新情報について発表し、どのようにしてサイバーセキュリティに対する意識を高められるのか、どのようなインセンティブや規制が有効か等について、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	金田 祐加子 経済産業省 商務情報政策局 サイバーセキュリティ課 企画官
講演者及び	1. “Introduction to Cybersecurity Policy for Industry”，金田 祐加

タイトル	子 経済産業省 商務情報政策局 サイバーセキュリティ課 企画官 2. “EU Policy on Cybersecurity”, Ms. Karolina KOZŁOWSKA, Policy Officer, Directorate-General for Communications Networks, Content and Technology 3. “CYBERSECURITY POLICY: A SNAPSHOT OF U.S. TRENDS”, Ms. Elke Sobieraj, Associate Chief of Policy, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security

1.3.7 標準化セミナー／Standardization Seminar

日本、米国、EU の政策当局者が、各国におけるサイバーセキュリティに関する規格・適合性評価の策定状況について発表し、サイバーセキュリティ対策向上における規格・適合性評価の役割、あるべき姿等について、議論を行った。

(1) 講演者一覧

表 1-5 標準化セミナーの講演者一覧

モデレーター	Mr. Peter Fatelnig, Minister-Counsellor for Digital Economy Policy, Delegation of the EU to Japan
講演者及びタイトル	1. “Introduction to the Japanese IoT Labeling Scheme” 前田 智美 経済産業省 サイバーセキュリティ課 課長補佐 2. “Vulnerability Management for Industrial Control Systems (ICS)”, Ms. Lindsey Cerkovnik, Chief for Vulnerability Response and Coordination Branch, Cybersecurity Division, CISA 3. Mr. Peter Fatelnig, Minister-Counsellor for Digital Economy Policy, Delegation of the EU to Japan

1.3.8 インシデントレスポンスセミナー／Incident Response Seminar

米国、EU の専門家が、最新のサイバー脅威とその対応策、インシデントレスポンスのための人材育成、官民の連携スキーム等について解説した。

(1) 講演者一覧

表 1-6 インシデントレスポンスセミナーの講演者一覧

モデレーター	Mr. Shaun Long, Deputy Chief, Industrial Control Systems, Threat Hunting Office, CISA
講演者及びタイトル	1. “Improving Threat Hunt & Incident Response Capabilities Through Adversary Emulation”, Mr. Shaun Long, Deputy

	Chief, Industrial Control Systems, Threat Hunting Office, CISA 2. “CERT-EU, incident response and cooperation”, Mr. Alexandros Goniadis, Operational Cooperation Officer, CERT-EU/Mr. Georgios Psykakos, Head of Sector for Operational Cooperation, CERT-EU

1.3.9 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も大きな課題の一つとなっている。COVID-19 によるデジタル化の進展に伴い、日本、米国、EU において、サプライチェーンにおけるサイバーセキュリティリスクが高まっている。政府も民間企業もそれぞれサイバーセキュリティガイドラインの策定や製品・ソリューションの認証取得に取り組み、リスクの軽減に努めている。

(1) 講演者一覧

表 1-7 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. “Enhance supply chain cybersecurity ”八木 晴信／東海旅客鉄道株式会社 アシスタントマネージャー 2. “Software supply chain risks and Transparency through SBOM”, Dr. Allan Friedman, Senior Advisor, CISA

1.3.10 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。

(1) 講演者一覧

表 1-8 閉会の辞の講演者一覧

開会挨拶	● 佐々木 圭一郎 外務省 経済安全保障政策室 室長補佐 ● 遠藤 信博 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

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、サイバーセキュリティ確保に向けた政策、標準化、サプライチェーンリスクマネジメント、インシデントに対応するための情報共有の取組などについて、様々な取組の紹介や解説が行われた。また、ICSCoE 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の取組に触れ、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。さらに今回は、COVID-19 以降で初めてのオフラインでの集合研修を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サイバーセキュリティ確保を主導する人材の育成に貢献するものであり、参加者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、インド太平洋地域の各国の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、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取組等についてのセミナー・演習を実施し、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や評価を実施した。

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、日米EUによるサイバーセキュリティ分野でのキャパシティービルデングを図ることが非常に重要な意味を持っている。

今回は COVID-19 以降初の物理開催となり、国際間で参加者同士がお互いに顔を知る関係を持つ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としての対応も日々進化をしており、1 日としてとどまることはないため、常に最新の情報を取り込んだ活動を継続することが重要であり、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が引き続き重要である。

令和5年度産業サイバーセキュリティ強靭化事業

（IoT機器やソフトウェアのセキュリティ確保等に関する調査） 報告書 - 第 5 編

インド太平洋地域向け日米EU産業制御サイバーセキュリティ関連

2024 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5年度産業サイバーセキュリティ強靭化事業
（IoT機器や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

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

2024 年 3 月 29 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. 検討会の運営

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」をWeb開催した。具体的な事項については、以下のとおりである。

1.1 第16回ビル SWG の運営

1.1.1 開催概要

日時　2023 年 11 月 30 日 10:00～11:50
場所　Teams 会議（Web 会議）
議題

1. 開会
2. 各構成員より挨拶
3. CSSC ビル対策カタログ第 2 版について
4. IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討状況
5. ウラノス・エコシステムについて
6. DADC スマートビルプロジェクトの活動とコンソーシアム組成について
7. ビル SWG 今後の方針について
8. 自由討議
9. 閉会

配布資料：

資料1　議事次第・配付資料一覧
資料2　構成員等名簿
資料3　CSSC ビル対策カタログ第 2 版について
資料4　IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討状況
資料5　ウラノス・エコシステムについて
資料6　DADC スマートビルプロジェクトの活動とコンソーシアム組成について
資料7　ビル SWG 今後の方針について

1.1.2 構成員

江崎浩　　東京大学大学院 教授
松浦知史　　東京工業大学 教授
アズビル株式会社
イーヒルズ株式会社
株式会社 NTT ファシリティーズ
鹿島建設株式会社
株式会社九電工

株式会社きんでん
技術研究組合制御システムセキュリティセンター
セコム株式会社
ダイキン工業株式会社
株式会社竹中工務店
株式会社日建設計
日本生命保険相互会社
一般社団法人日本ビルヂング協会連合会
一般社団法人ビルディング・オートメーション協会
株式会社日立製作所
株式会社日立ビルシステム
一般社団法人不動産協会
三井不動産株式会社
三菱地所株式会社
横浜市
三菱電機株式会社
ICSCoE2期ビルチーム有志

1.1.3 議事要旨

産業サイバーセキュリティ研究会 WG1 ビル SWG（第 16 回）議事要旨

日時： 2023（令和 5）年 11 月 30 日 10 時 00 分～11 時 50 分
構成員：
（座長）江崎 浩 東京大学大学院 教授
松浦 知史 東京工業大学 教授
アズビル株式会社
イーヒルズ株式会社
NTT グループ（株式会社 NTT ファシリティーズ）
鹿島建設株式会社
株式会社九電工
株式会社きんでん（欠席）
技術研究組合制御システムセキュリティセンター
セコム株式会社（欠席）
ダイキン工業株式会社
株式会社竹中工務店
株式会社日建設計
日本生命保険相互会社
一般社団法人日本ビルヂング協会連合会（欠席）

一般社団法人ビルディング・オートメーション協会
株式会社日立製作所
一般社団法人不動産協会
三井不動産株式会社
三菱地所株式会社
三菱電機株式会社
横浜市
ICSCoE2期ビルチーム有志
（オブザーバー）
国土交通省
内閣サイバーセキュリティセンター
中部国際空港株式会社
中部国際空港施設サービス株式会社

議題：

1. 開会
2. 各構成員より挨拶
3. CSSC ビル対策カタログ第 2 版について
4. IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討状況
5. ウラノス・エコシステムについて
6. DADC スマートビルプロジェクトの活動とコンソーシアム組成について
7. ビル SWG 今後の方針について
8. 自由討議
9. 閉会

要旨：

1. 各構成員より挨拶

2. CSSC ビル対策カタログ第 2 版について

・ 資料 3 を CSSC ビル部会澤部様より説明より説明

3. IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討状況

・ 資料 4 をサイバーセキュリティ課木本補佐より説明

4. ウラノス・エコシステムについて

・ 資料 5 を情報経済課鈴木係長より説明

5. DADC スマートビルプロジェクトの活動とコンソーシアム組成について

・ 資料 6 を DADC 粕谷様より説明

6. ビル SWG 今後の方針について

・ 事務局より説明

7. 自由討議

（1）スマートビルコンソーシアムにビル SWG が合流することについて

・ ビル SWG がスマートビルコンソーシアムに合流することは、賛成である。これまでのビル SWG

は、ビル全体のセキュリティを議論してきた。スマートビルコンソーシアムはスマートビルに焦点を当てていると思うが、今後のセキュリティ WG ではスマートビルの観点からの議論になるのか？

→ これまではスマートビルについて議論してきたが、ビル SWG が合流した場合は、従来のビルセキュリティも含めるスコープに広げる必要があると認識している。設立準備会で議論したい。

・ ビル SWG がスマートビルコンソーシアムに合流することは自然で賛成である。しかし、従来のビルのサイバーセキュリティの問題と、未来志向のスマートビルの論点とはギャップがあるのではないか。このギャップを踏まえてスコープを先に決めておくと良いのではないか。

・ ビル SWG は、解散ではなく合流という形で引き続きお願いしたい。合流した後も、既存のビルについて考えないといけない。ビル協とも連携して、既存のビルも連携しながら検討したい。

・ 合流は賛成である。最近の新しいオフィスビルの建設にあたっては非常に多数の IT ベンダが関わっており、現状でも運用の検討は非常に大変である。スマートビルになるともっと複雑になるだろう。スマートビルの運用にあたっては、最初からセキュリティを考えて進めるところが重要である。運用は AsIs から引っ張られており、AsIs をしっかりと見ていくことが大切である。

→ 海外の事例を見ても、IT ベンダが非常に多い。チケットシステムを使ってベンダを制御すること等も考える必要があると思う。

→ AsIs から ToBe へどのようにして移行するかが大切である。

・ AsIs としては、DADC のガイドラインに示しているようなビル OS に対応したスマートビルとなる前に、既に個別のクラウドで対応されている。スマートビルと AsIs の違いはビル OS を持つかどうか程度の違いではないか。従来のビルとスマートビルの切り分けは難しい。AsIs と ToBe がシームレスにつながっていくようなスコープを設定して欲しい。

→ さまざまな API が乱立することを許容するのか、統一的な API とするのか。スマートビルのマイグレーションシナリオに API の議論は含まれているのか。

→ IoT システムは、ほとんどがクラウド化されているのが現実である。統一的な API とするということは、ビルの機能を抽象的に扱うということである。デバイスをデカップリングするためのデータスペースを整備して、データドリブン社会に近づけるのではないか。

（2）スマートビルコンソーシアムについて

・ セキュリティ WG に求める機能として、認証のセキュリティも大事である。認証基盤のセキュリティは他の WG にも関係するので、他 WG との連携機能がコンソーシアムの中に組み込まれると良い。セキュリティは最初にデザインしておく必要があるので、意思疎通の機能が大事である。

・ スマートビルは、例えば都市 OS とも接続することが考えられる。都市 OS は、商業ビルだけでなく家庭や公共施設とも連携することが必要になる。したがって、市民目線、地域運営の自治体目線も加えて欲しい。エリアマネジメントの会社が参加できるようなスキームも設定して欲しい。また、都市 OS の議論が出ているが、補助金が無いと続けられないスキームになっていることを心配している。

→ ToBe 像を検討しているところである。防災の観点から国土交通省とも連携を図ろうとしており、そのほかの関係主体も巻き込みたい。

→ スマートビル側のインセンティブとして、容積率を緩和すること等の議論も出てきている。ビル

SWG の主幹は METI だが、将来はデジタル庁や国土交通省との連携も重要である。

・ 従来のビル（AsIs）とスマートビル（ToBe）では性質が異なるので、セキュリティ WG の中に分科会をつくることも考えられる。

・ スマートビルは新しい概念であり、IT 基盤に加えて運用も検討すべきことが多い。最初からセキュリティ WG が運用面も含めて考える体制が良いのではないか。

（3）IoT 認証について

・ IoT の機器認証の活用方法は、コンソーシアムのスコープに入るのか？

→ プラットフォーム認証を優先的にすすめており、プラットフォームと接続するデバイスの認証の検討をその後に実施するのが自然であると考えている。

→ デバイスの認証部分は制度側で進めていくが、全体の要件部分はプラットフォーム側とも連携して進めたい。制度も徐々に整備していく予定である。

→ デジタル臨時行政調査会のテクノロジーマップにおいて、デバイス認証との連携は既に描かれている。デジタル臨時行政調査会では、規制の見直しや新設も含めて議論することになっている。ビルセキュリティの分野は早い段階で議論が進むだろう。

→ IoT 認証は、認証の手間が大きくなりすぎないようにするべきである。国の関与が必ず必要となるとスケールしないので、そうならないような検討も行っている。

（4）ウラノス・エコシステムとの関係について

・ ウラノス・エコシステムの説明で、競争領域と協調領域の説明があったが、セキュリティ WG では協調領域を扱うのか。

→ いくつかのレイヤーがあり、例えば個人情報やデータの扱いの部分は競争領域であるし、認証は協調領域になると思う。競争領域なのか、協調領域なのかも含めて議論して進めたい。

→ サイバーでベースとなる部分は協調領域になると思うが、アプリなどは国は関与すべきでないと考えている。

→『競争』を盾にしたロックオンは避けなければいけない。協調領域は、ガラパゴス化しないことが重要である。その観点からは、欧米やアジアとの連携も視野とすべきである。

（以上）

1.1.4 会議運営業務

会議運営業務として、日程調整、ビルSWGへの参加、議事録作成、委員に対する委嘱、謝金支払い等を実施した。

2. 総括

本調査では、ビル SWG の運営業務を行った。

ビル SWG では、昨年度に「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（個別編：空調システム）第 1 版」を取りまとめるとともに、インシデントレスポンスについての記述を新たに加えた「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第 2 版」を取りまとめた。これにより、ビル SWG としての業務には一区切りをつけ、今年度の議論では、DADC スマートビルプロジェクトへの協力と今後組織化される予定のアソシエーションへの合流が大きなテーマとなった。

世の中の DX 化の進展にあわせ、ビルもスマート化が進むと考えられており、ビルシステムのサイバーセキュリティの確保はますます重要性を増すものと考えられる。スマートビルのアソシエーションにおいてもビルシステムのサイバーセキュリティ確保は大きなテーマの1つになると考えられる状況であり、今後もこのような議論と歩調を合わせていくことが重要である。

令和5年度産業サイバーセキュリティ強靭化事業

（IoT機器や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

ビル SWG 関連

2024 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５年度産業サイバーセキュリティ強靭化事業（ＩｏＴ機器や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５年度産業サイバーセキュリティ強靭化事業（ＩｏＴ機器や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3編 15	図2-6	協調的なデータ利活用に向けたデータマネジメント・フレームワークの概要
第3編 16	図2-7	侵入検知製品等を使う際の導入検討から本格運用までの流れ
第3編 16	図2-8	『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
第3編 18	図2-9	OTセキュリティアセスメントサービスの概要