経済産業省

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

令和６年12月25日

経済産業省　商務情報政策局

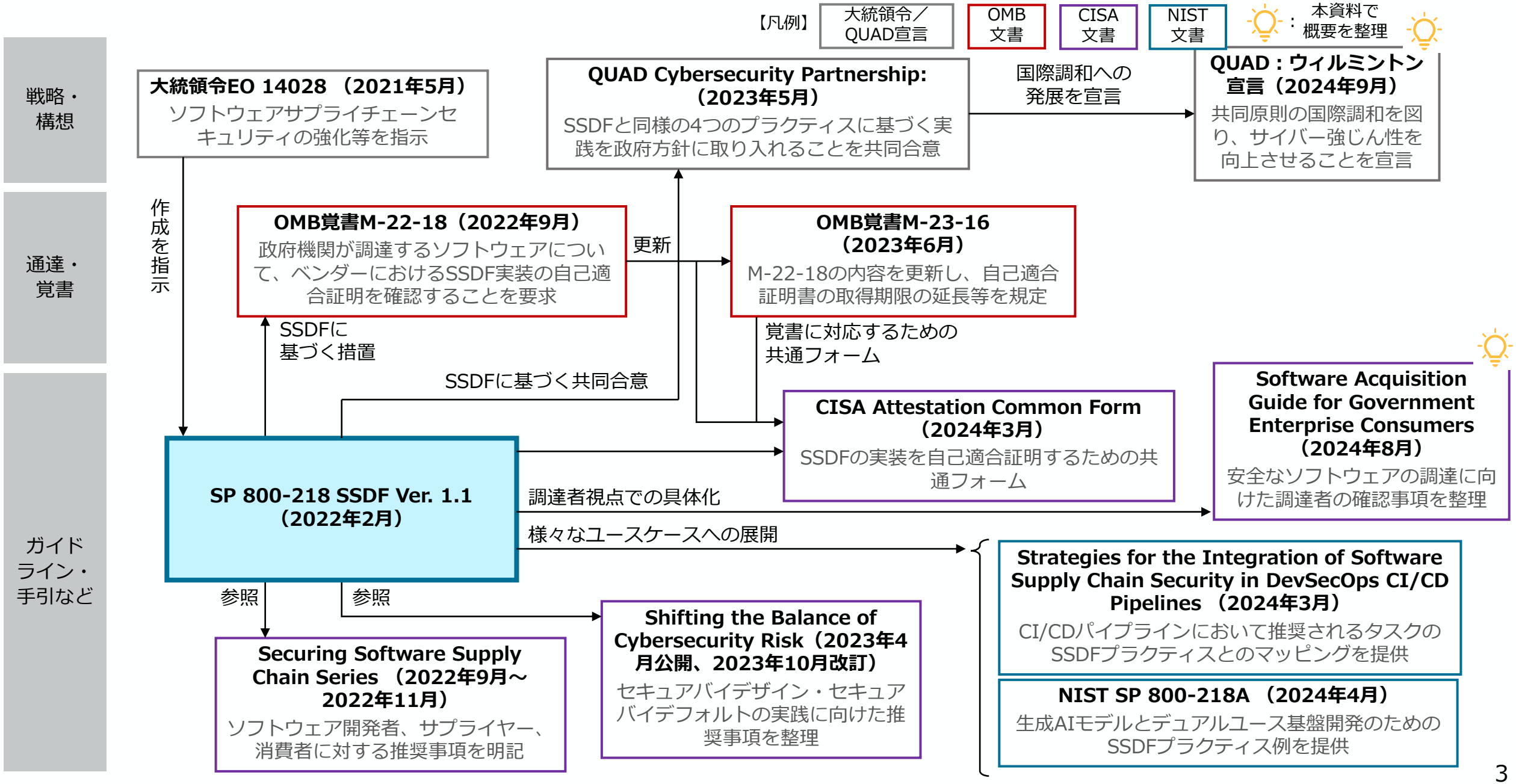
サイバーセキュリティ課

１．ソフトウェアの管理手法等に関する海外の動向

２．実証の中間報告と成果イメージ

３．今後の取組案

ソフトウェアセキュリティに関する米国の取組の俯瞰図



【米国】SBOMに関するイベント“SBOM-a-rama”の開催

2024年9月、SBOMに関するイベント“SBOM-a-rama”が開催、各国の取組等が発表された。

- 本イベントはSBOMコミュニティの醸成を目的としており、計18のセッションが行われ、**SBOMに関するコミュニティ活動、米国の政府組織における取組、米国の事業者における取組、韓国政府の取組等**が発表された。

SBOM-a-ramaの各発表の概要

発表者	発表概要
DASA(DES)※1	• 米軍においてはソフトウェアの活用の広がりに合わせて2025年2月以降にSBOMをソフトウェアに求める予定である。
OWASP	• SBOMやVEX等のソフトウェアの透明性確保に関連する情報を交換できるよう専用IDとAPIプラットフォームを構築している。
SBOM Sharing Tiger Team※2	• SBOM共有ライフサイクルにおけるSBOM作成者、ディストリビューター、利用者での役割を整理したガイド作成予定である。
SBOM Generation Tiger Team	• 様々なソフトウェアを対象にOSSツールを利用してSBOM生成したところ、複数のSBOM形式への対応コスト、NTIAの最小要素の不明瞭さなど課題として確認している。
AIBOM Tiger Team	• コンプライアンス対応、セキュアバイデザイン等複数の観点のAIBOMを検討して、ガイドラインを作成している途中である。
BOMOPS Tiger Team	• SBOMの利用者目線からインシデントレスポンスやコンポーネントの活用分析等の様々なユースケースを検討して、ガイドラインに取りまとめている途中である。
Lockheed Martin	• SBOMを自社で検討して、組み込み機器向けのプログラム、手動のSBOM作成、SBOMの可視化などを課題として確認している。
Healthcare SBOM PoC Team	• ヘルスケア業界では、25のSBOMと3つのVEXをPoCで構築して様々なガイドラインを構築している。
Finite state	• 携帯電話業界に関連するSBOMのガイドラインが構築されている中、モバイル業界の国際的な業界団体のGSMAと活動している。

発表者	発表概要
FDA	• SBOMを医療機器に要件化している中、SBOMに記載するデータの標準化が必要不可欠であることを確認している。
Korea University	• ソフトウェアサプライチェーンのセキュリティ確保におけるSBOMの利用方法を記載したガイドラインを作成している。
SBOM VEX Group	• 公開されているVEXを調査し、VEXフォーマットの多様性、公開脆弱性データベースとの連携などを課題として確認している。
SBOM Tooling Cataloging Group	• SBOMツールのカタログを作成に向けてツールの機能のリストを現状のSBOMツールにある機能と今後のSBOMツールに必要な機能の2軸で検討している。
SBOM Tooling Implementation Group	• アンケートなどを基にSBOMの最小要素への期待、SBOMデータの成熟度、SBOMの追加要素についてガイドラインとして取りまとめている途中である。
Carnegie Mellon University	• 様々なツールが同じソフトウェアに対してどのように異なるSBOMを生成するかを調査し理解することを目的としたPlugfestを開催する予定である
Splunk	• 自社のソフトウェアのソースコードとバイナリファイルで作成したSBOMを2種類公開している。VEXの利用やSBOM生成の精度などを課題として認識している。
CISA On Ramps & Adoption WG	• ポッドキャスト・講演発表・イベントなどの普及における活動を実施状況について報告している。

出所） CISA, ” SBOM-a-Rama Fall 2024”, https://www.cisa.gov/news-events/events/sbom-rama-fall-2024

※1: DASA(DES)とは、米国のDX化を促進する組織である。
※2: Tiger Teamとは、CISAが主催する民間事業者が集まり特定のテーマに関して検討するWGである。

【英国】 ソフトウェアベンダー向けの行動規範案及び実施ガイダンス案

英DSITが、ソフトウェアの開発・構築・保守方法等に関するガイダンス案を発表した。

- 2024年5月、英DSITは、**ソフトウェアの開発、構築、保守の方法**と、**ソフトウェアを調達する顧客への情報提供方法に関するベンダーの行動規範案**とその**想定利用方法等**を示し、**パブリックコメント**を募集した。
- 行動規範案は21の項目からなり、各項目に対して(1)**必須と推奨**の2段階で定めた要求度、(2)客観的評価可能な**技術的管理策**、(3)**実務レベル**で示した実施ガイダンスの3点の**公表を予定**している。
- ソフトウェア開発に関する実施ガイダンスの一例としてSBOMの活用が挙げられている。

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

出所） DSIT, “Call for views on the Code of Practice for Software Vendors” https://www.gov.uk/government/calls-for-evidence/a-code-of-practice-for-software-vendors-call-for-views/call-for-views-on-the-code-of-practice-for-software-vendors

【米国】 ソフトウェア取得プロセスにおける確認事項を整理したガイド

米CISAが、ソフトウェア取得時のセキュリティ確認事項に関するガイドを発表

- 2024年8月、CISAが組織する官民横断組織※は、政府機関のソフトウェア取得プロセスにおいて、**担当者がサプライヤーの保証やサイバーセキュリティ透明性の管理状況を把握するためのガイド**を発表した。
- 質問形式の確認事項に回答することで状況が把握でき、米政府機関以外での利用も推奨されている。
- サプライチェーン管理や脆弱性管理に関する確認事項として、SBOMに関する言及がある。
- **SSDF自己適合証明との整合性**について注意深く配慮されている。

※ CISAが組織し共同議長を務めるICT SCRM Task Force。国家リスク管理センター（NRMC）やIT及び通信の重要インフラ部門の代表者が参加し、連邦政府や重要インフラの民間部門の所有者及び運営者に助言や勧告を行う。

各管理領域におけるサプライヤーへの確認事項

管理領域	確認事項の概要
(1) サプライヤーガバナンスと認証	• (2)以降の確認事項で不要なものを除外するための確認項目。CISA により規定されたSSDF自己適合証明を提供しているか、**内部及びサードパーティ部品の出所データ**を保持しているかなどの体制に関する確認事項が主である。 • 確認事項の一つとして、サプライヤーによる、機械判読可能で「最小要素」を満たした**SBOM**の提供有無に関する事項が明記されている。
(2) ソフトウェアサプライチェーン	• サプライヤーが、ソフトウェアの**ライフサイクルを通じたリスク管理**を行っているか、及びそのための**プロセス等を整備**しているかの確認事項。特に**サードパーティ製ソフトウェア**の設計開発実装の意思決定の透明化を重視している。 • 確認事項の一つとして、機械判読可能で「最小要素」を満たしたSBOMであることの、サプライヤーによる検証有無に関する事項が明記されている。
(3) セキュアなソフトウェア開発	• 「**セキュアバイデザイン**」を実現するために必要な基準の管理をサプライヤが行っているかの確認事項。開発手法や開発環境への確認事項が主である。
(4) セキュアなソフトウェアデプロイメント	• ソフトウェアのデプロイメントの前後に、**リスクの特定と軽減を目的としたプロセス**と手順が適用されているかを確認する事項である。
(5) 脆弱性管理	• 新たな脆弱性が報告されると、顧客（ソフトウェア取得者）がリスクを評価するための**セキュリティ勧告をサプライヤが発行**する。サプライヤは**脆弱性を継続して監視し対処**する必要があり、そのためのプロセスと手順が適用されているかを確認する事項である。

出所）ICT SCRM Task Force, “Software Acquisition Guide for Government Enterprise Consumers: Software Assurance in the Cyber-Supply Chain Risk Management (C-SCRM) Lifecycle” https://www.cisa.gov/resources-tools/resources/software-acquisition-guide-government-enterprise-consumers-software-assurance-cyber-supply-chain

【米国】 ソフトウェア利用者におけるセキュリティ確認事項を示したガイド

米CISA・FBIが、ソフトウェア利用者視点でのセキュリティ確認事項に関するガイドを発表

- 2024年8月、CISAとFBIは、**ソフトウェア製造者がセキュアバイデザインの原則に従っているか否かを、ソフトウェア利用者が判断するためのガイド「Secure by Demand Guide」**を発表した。
- ソフトウェア利用者が、製造者に対して確認すべき事項（質問事項）が6つの項目別で整理されている。

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

出所） CISA, “Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem” https://www.cisa.gov/resources-tools/resources/secure-demand-guide

【QUAD】 安全保障等に関する共同声明「ウィルミントン宣言」の発表

2024年9月、QUADが共同声明を発表。安全なソフトウェア開発に関する内容も盛り込まれた。

- 2024年9月、日米豪印戦略対話「QUAD」の首脳会合が米国ウィルミントン近郊で開かれ、会合後、共同声明として「ウィルミントン宣言」が発表された。
- ウィルミントン宣言では、インド太平洋地域の平和と安定の維持のために、「善を推進するグローバルな力」を発揮するとともに、「地域及びグローバルな課題への取組に向けた協力」を推進することを宣言している。また、このために、日米豪印が「インド太平洋のための永続的パートナー」であることも宣言している。
- 宣言内の「サイバー」の項目では、**2023年のソフトウェア・セキュリティに関する日米豪印共同原則※1に基づき安全なソフトウェア開発要件及び認証に向けたコミットメントを拡大している**こと、**当該要件の国際調和**により、**政府用ソフトウェアだけでなく**、サプライチェーン、デジタル経済及び社会の**サイバー強じん性を全体として向上させる**ことが宣言されている。

※「ソフトウェア・セキュリティに関する日米豪印共同原則（概要）」 https://www.mofa.go.jp/mofaj/files/100509255.pdf

「ウィルミントン宣言」のうち「サイバー」に関する記載

日米豪印諸国は、サイバー領域における悪化する安全保障環境に直面し、**国家に支援された主体、サイバー犯罪者及びその他の悪意ある非国家主体**による共通の脅威に対処するため、我々のサイバーセキュリティ・パートナーシップを強化する意図を有する。我々の国々は、更なる脅威情報の共有と能力構築を通じて、**集団的なネットワーク防衛を強化**し、技術的能力を向上させるための具体的な措置を講じることにコミットする。我々は、脆弱性を特定し、国家安全保障ネットワーク及び重要インフラ・ネットワークを防護し、並びに日米豪印共通の優先事項に影響を与える重大なサイバーセキュリティ・インシデントへの政策対応を含め、より緊密に協調する共同の取組を計画している。

日米豪印諸国はまた、**2023年のソフトウェア・セキュリティに関する日米豪印共同原則に基づき、安全なソフトウェア開発要件及び認証の追求に向けた我々のコミットメントを拡大するために、ソフトウェア開発者、業界団体及び研究機関と連携**している。我々は、これらの要件の国際調和を図ることで、**政府ネットワーク用のソフトウェアの開発、調達及び利用の安全性確保のみならず、サプライチェーン、デジタル経済及び社会のサイバー強じん性を全体として向上させる**。日米豪印諸国は、今秋を通じて、責任あるサイバー・エコシステム、公共資源、サイバーセキュリティ意識の向上を目的とした年次日米豪印サイバー・チャレンジを記念するキャンペーンをそれぞれ開催することを計画する。我々は、ケーブルの連結性及び強じん性のための日米豪印パートナーシップを補完する取組として、日米豪印上級サイバー・グループで策定された商用海底電気通信ケーブルの防護に関する日米豪印アクションプランに建設的に関与している。このアクションプランに導かれた世界の電気通信インフラの保護に向けた我々の協調行動は、将来のデジタル接続性、世界的な商取引及び繁栄に向けた我々の共通のビジョンを前進させる。

（外務省発表の仮訳からの引用。ただし、強調は独自に追加。）

出所）外務省、ウィルミントン宣言 オーストラリア、インド、日本及び米国の首脳による共同声明（仮訳）https://www.mofa.go.jp/mofaj/files/100728333.pdf

１．ソフトウェアの管理手法等に関する海外の動向

２．実証の中間報告と成果イメージ

３．今後の取組案

実証を含む取組の全体像

第13回ソフトウェアTF
資料より

- SSDF活用のための考え方等をまとめた**国内事業者向けの文書**(ガイドライン等)を策定するとともに、**自己適合宣言の仕組み**を構築し、**政府調達等への要件化**を通じて実効性を強化することにより、QUAD共通原則を履行することが目標。
- 今年度は、SSDFと国内ガイドラインのマッピング、実ソフトウェアに対する実証等を通じて、国内ガイドラインの不足事項や課題・対応方法の具体化等について整理し、国内事業者向けの文書(ガイドライン等)の初版案を作成。
- 来年度以降は、残課題の整理・対応、国内事業者向けの文書の初版案の成案化、初版改訂に向けた検討と改訂案策定、自己適合宣言の仕組みの検討・構築、政府調達等への要件化などを検討。

今年度実施予定の内容

- SSDFと国内ガイドラインの対応関係を示すマッピング
- マッピング表を用いたSSDF活用方法・対応フローの整理
- 実ソフトウェアに対する実証、課題・対応方法の具体化等の整理
- 国内ガイドラインの不足事項の明確化と対応方針案の検討
- 事業者のSSDF自己適合宣言文書作成に関する参考情報等の提示、など

＜成果物例＞

国内事業者向け文書(ガイドライン等)の初版案

- SSDFと国内ガイドラインのマッピング表
- SSDF活用の考え方等をまとめた文書
  - ✓ マッピング表を用いたSSDF活用方法
  - ✓ 課題・対応方法の具体的内容
  - ✓ 国内ガイドラインにおける不足事項・対応方針案
  - ✓ 事業者のSSDF自己適合宣言文書作成に関する参考情報、など

来年度以降実施予定の内容

① 残課題(不足項目の対応方法の更なる具体化等)への対応

② 国内事業者向け文書の初版案の成案化

③ 初版改訂に向けた検討と改訂案作成

④ 自己適合宣言の仕組み検討・構築

⑤ 政府調達等への要件化の検討、 など

実証の目的

サイバーセキュリティを確保する上で、システムの構成要素であるソフトウェア、ハードウェア、人のセキュリティ確保が必要となる。その中でも、ソフトウェアは重要な基盤であるため、ソフトウェアのセキュリティ確保は、極めて重要である。

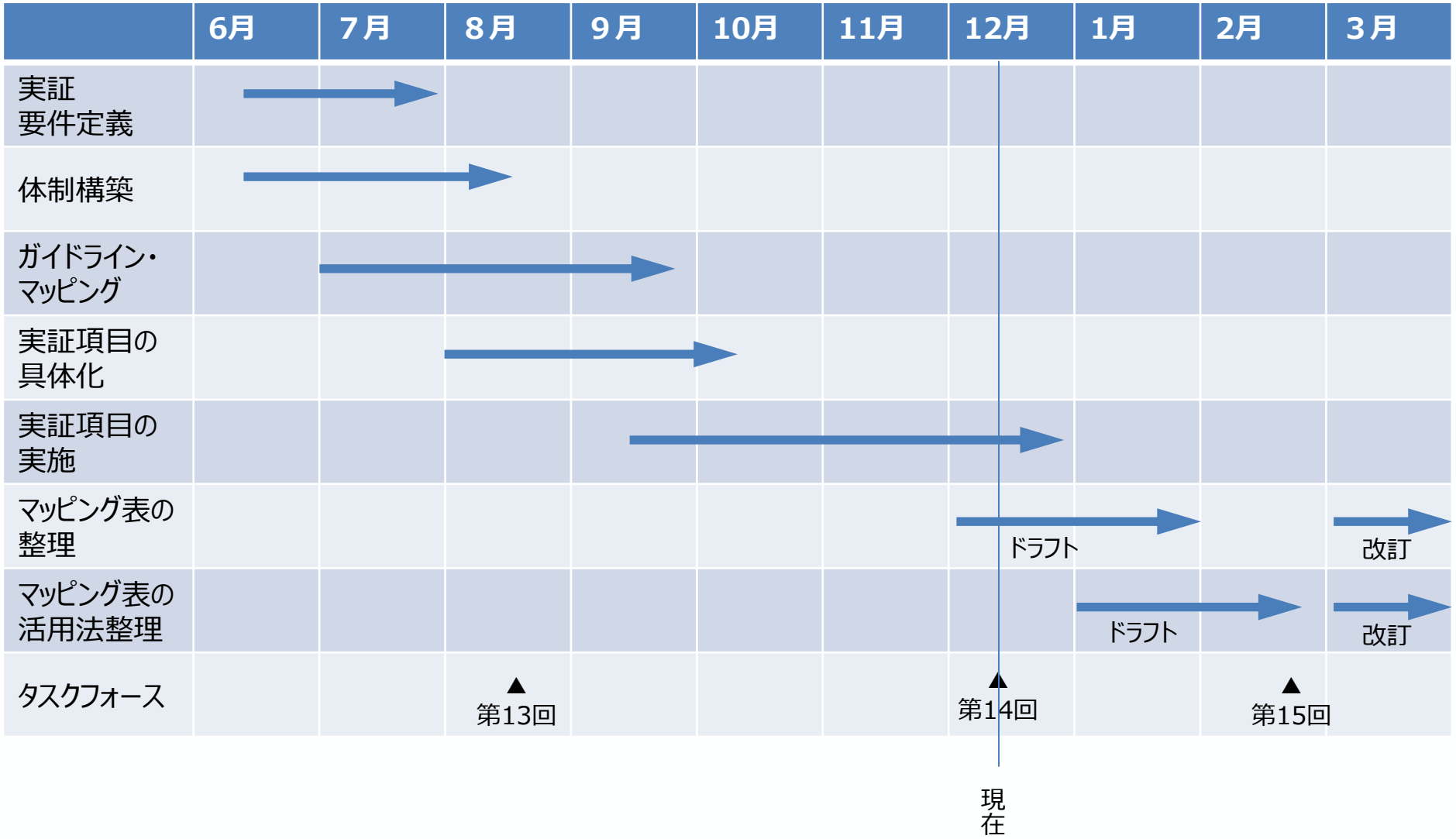
そのようなことから、 SAFECode Secure Software Development Practice, OWASP Software Assurance Maturity Model, BSA Framework for Secure Softwareなどのセキュアソフトウェア開発の実践ガイドラインが多数策定されてきた。それらを**包括するセキュア・ソフトウェア開発フレームワークと共通言語の役割**を果たすものとしてSSDFが取りまとめられた。SSDFは開発プロセス全体を対象としており、要求・設計工程に重点を置くSecure by DesignやSecure by Defaultを包含する。

QUAD共同原則においては、**セキュア・ソフトウェア開発プラクティスを政府調達方針とすることに合意**している。そのベースとしてSSDFが主要なフレームワークとして活用することができる。

一方で、SSDFは、幅広い分野で適用できるように、汎用的で、抽象度の高い、包括的なフレームワークを提供するものであるため、組織において**実践導入する上で具体的な方法や達成基準が明確ではない**といった課題がある。

このようなことから、本事業では、実ソフトウェアを対象に、SSDFの導入実証を行い、実証を通じて得られた**具体的な導入方法、達成基準の具体例、課題の解決策**等の整理を行う。また、SSDF導入の参考情報として、SSDFと国内ガイドラインの対応関係を整理した情報を整理することで、すでに対応済みの国内ガイドラインを参考とした導入方法について考え方を整理する。

スケジュールと現在のフェーズ



本実証で予定する成果物

成果物の概要と構成

① **SSDF Task 達成レベルと達成基準（暫定版作成）**(p.10 成果物例：SSDF活用の考え方等をまとめた文書)
SSDFは網羅性高く体系化されているが、抽象的であり具体的に実施すべきことが明確ではなく、実施主体により実施内容に大きな差が出ることが想定される。SSDF Task項目ごとに達成レベルを３段階に分け、達成基準案として判断指針と具体例を示すことで、実施事項が明確で具体的なものにする。

② **Task実証の具体例(ケーススタディ)と達成評価（暫定版作成）**(p.10 成果物例：SSDF活用の考え方等をまとめた文書)
本実証において実施した具体的な内容をケーススタディとして示し、セキュリティ向上の効果、達成レベルとその評価、SSDF導入企業に対して参考情報を提供する。

③ **SSDF・国内ガイドラインマッピング表（案作成）** (p.10 成果物例：SSDFと国内ガイドラインのマッピング表)
国内ガイドラインを実践する企業の参考となるように、国内の関連ガイドラインの項目とSSDFのTaskの対応関係、包含関係とその説明を整理したマッピング表を整理する。また、NIST AI版SSDF, CISA SBD[2]とのマッピングも示す。

④ **SSDF Taskの課題（整理中）** (p.10 成果物例：国内ガイドラインにおける不足事項・対応方針案、課題・対応方法の具体的内容)
SSDF Task自体の課題（Task過不足、運用フェーズなど）、Task実施上の課題を整理し、課題に対する対応策、今後期待される施策を整理する。

⑤ **SSDF導入ガイダンス基礎編（整理中）** (p.10 成果物例：国内事業者向け文書(ガイドライン等)(マッピング表を用いたSSDF活用方法、事業者のSSDF自己適合宣言文書作成に関する参考情報を含む))
成果物①②③④を活用してSSDFを導入するための手順を示すガイダンスを整理する。本年度は、1つのケーススタディに基づき、成果物①②③④をどのような順序でどのように活用するか基礎的な流れを示す。

実証対象ソフトウェアの概要：SBOMツール（構成イメージ）

委員会限り

委員限り

【参考】SSDF（セキュア・ソフトウェア開発フレームワーク）の構成

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

①SSDF Task 達成レベルと達成基準（まとめ方と例）

達成レベルを定義する意義

SSDF Taskは、抽象度の高い要件を記載しているため、**用途や環境に応じて求められるレベルに大きな違い**がある。これらの違いを把握し、**求められるレベルを判断**して、それが**達成されることが判断できる基準**が重要になる。

達成レベルと達成基準の定義方法

SSDF Taskの達成レベルを実証検討をもとに３段階に分類した。各段階を区別する本質的な違いを**判断指針**として定め、各段階の**具体例**を示すことで、**曖昧性を解消し、具体性を高める**。ただし、多様な分野に渡る**唯一の正解は存在しない**ため、参考例を提示することで、利用者のカスタマイズを通じて活用することを想定する。

達成基準の判断指針、具合例の記載例（Task 組織の準備PO1.1の一部抜粋）

Practice（実践策）		Task（タスク日本語訳）	達成レベルと達成基準	
Group	ID		達成基準（判断指針）（レベルを明確に区別する観点）	達成基準（具体例）（用途や環境により、基準は固定的に決められないため、必須の事項と達成件数の2つの観点で判断する）
組織の準備 (PO: Prepare the Organization)	PO.1	PO.1.1：組織のソフトウェア開発基盤とプロセスのすべてのセキュリティ要件を特定、文書化し、要件を最新の状態に保つ。	1. 内製ソフト開発に関して、開発基盤などの基礎的なセキュリティ要件を定義・文書化している。**（内製ソフトの開発基盤の最低限のセキュリティ要件定義）** 2. 1.に加え、SDLC全体の外製ソフト（OSSやサードパーティ等の部品）も含めた開発基盤と開発プロセスのセキュリティ要件全般が体系的に定義・文書化されている。**（外製ソフトを含むソフト全体の開発基盤のセキュリティ要件の十分な定義）** 3. 2.についてセキュリティ要件が継続的に改善・最適化される仕組みが確立している。**（セキュリティ要件が最適化されている）**	【達成度基準レベル１】 内製ソフトウェア開発に関して、以下の項目を満たしていること。 ■ソフトウェア開発基盤のセキュリティ要件定義 ソフトウェア開発基盤とそのコンポーネントのセキュリティ・ポリシー（要件）定義の資料や文書がある。 [対応必須]★の項目は満たしていること。 [開発ケース毎に選択]▲の項目については必須ではないが、2つ以上の項目を満たしていることを推奨。 ※以下の例示で同等の対策を実施している場合は、達成度基準としてカウント可能。その場合、同等性の説明が必要。 (1)ソフトウェア開発環境の内容についての文書化されている。例えば以下のような内容が記載されている。 ★①使用HW、OS等のベースシステム環境 ★②開発基盤のシステム/ネットワーク構成 ▲③開発ツール ▲④テスト環境 ▲⑤使用する管理システム ・ 構成管理システム（ソース管理、文書管理など） ・ 問題管理システム（バグ管理、インシデント管理など） ▲⑥使用する情報共有・伝達手段（メール、WEB、チャットなど） (2)上記に対するセキュリティ要件/ポリシーが定義されている

②Task実証の具体例(ケーススタディ)と達成評価（例・抜粋）

達成基準（指針、具体例）を参考に実証内容・項目を定義し、実施結果に対して達成度とその判断理由を整理した。

SSDF Task	達成基準（指針）	達成基準（具体例）	実証内容・項目	達成度	達成度判断理由
PW.4.1：商業的、オープンソース、およびその他の第三者から、セキュリティが確保されたソフトウェア部品（ライブラリ、モジュール、ミドルウェア、フレームワークなど）を取得し、最新の状態に保つ。	1. 使用する外製ソフトウェア**部品がリストアップ**されており、それらの**セキュリティが担保されていることを確認**したうえで取得・管理している。 2. 1.のため**管理システム等を導入**し、履歴管理やコードの完全性を確保している。 3. 定期的にシステムの運用内容を見直し、**継続的に改善**が行われている。	【達成基準レベル１】 安全性の高いサードパーティ製コンポーネントの取得に関して、以下の項目を満たしていること。 ■外製ソフトウェアコンポーネントリストとその身元確認データ [対応必須]★の項目は満たしていること。 [開発ケース毎に選択]▲の項目については必須ではないが、満たしていることを推奨。 ※以下の例示で同等の対策を実施している場合は、達成度基準としてカウント可能。その場合、同等性の説明が必要。 (1)利用するソフトウェアコンポーネント（外製）の由来データの情報やセキュリティチェック結果がある。例えば以下のような資料や情報がある。 **★①ソフトウェアコンポーネント情報リスト一覧（外製）** ・コンポーネント名 ・バージョン情報 ・提供元情報 ・身元情報（由来データ） -信頼のおける入手経路・情報がある -提供元の公式・正式サイトからダウンロード -完全性検証用データ（ハッシュ値等）を入手など **▲②ソフトウェアコンポーネント（外**	①ソフトウェア開発にあたり使用する外製ソフトウェアコンポーネントがリストアップされており、それらのセキュリティが担保されていることを確認したうえで取得・管理されているかどうか確認する。 **・ソフトウェアコンポーネント一覧（外製）** **-提供元情報（取得バージョン情報など）** **-完全性検証用データもしくは信頼のおける入手経路情報**など ・格納場所情報 ②①の外製ソフトウェアコンポーネントのシステム管理に関する資料があるかどうか確認する。 **・構成管理システムでの管理** -外製ソフトウェアコンポーネントの**管理リポジトリ**がある ・SBOMシステム等で管理・運用 ③②の運用内容や（ソフトウェアコンポーネントの更新手続きや商用リリース時の手続き等）や**利用環境・設定等についての見直し履歴**があるかどうか確認する。取得処理が自動化され、管理されているかどうか確認する。 ・運用等の見直し履歴情報 ・ソフトウェアコンポ	**2**	■判定 以下の理由から、達成度はレベル2と判断した。 ■前提情報 検証プロジェクトではサードパーティ製コンポーネントとして**OSSコンポーネントのみを使用**している。 ■理由概要 レベル１：◎利用している外製ソフトウェアコンポーネントの情報リスト管理し、入手手段・入手時の情報を明確化。 レベル２：◎**GITHUBによる外製ソフトウェアコンポーネントの管理と情報共有を実施**。脆弱性情報の更新・管理も実施。 レベル３：×運用の見直しやソフトウェアコンポーネントの更新自動化は未対応。 ■理由詳細 ①ソフトウェアコンポーネント一覧（外製） 使用しているOSSコンポーネントはリスト一覧を作成し、取得時の情報を管理している。リスト一覧には以下の情報があることを確認している。 ・コンポーネント名 ・バージョン情報 ・提供元情報 ・身元情報（由来データ） コンポーネントの取得には以下の手段を使用している。 (1)Python関連コンポーネント（ライブラリ等） 【入手手段】 PyPIパッケージマネージャにより取得 (2)Javascript関連コンポーネント（ライブラリ等） 【入手手段】 npmパッケージマネージャにより取得

②Task実証の具体例(ケーススタディ)と達成評価
SSDF実証の実施状況（達成レベルの可視化）暫定評価

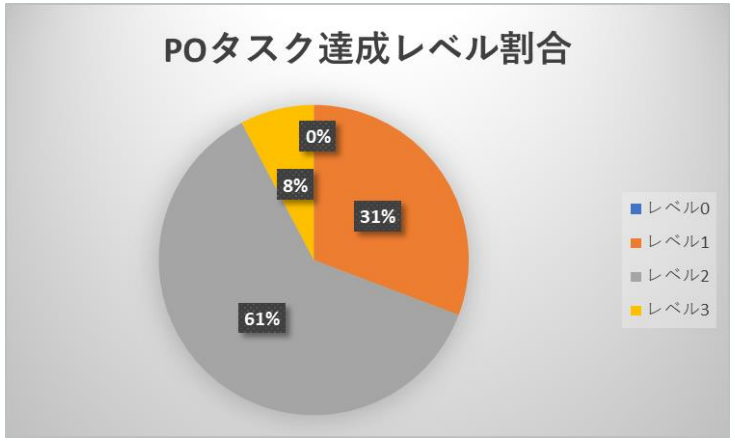
実証済みタスクの達成レベル分布

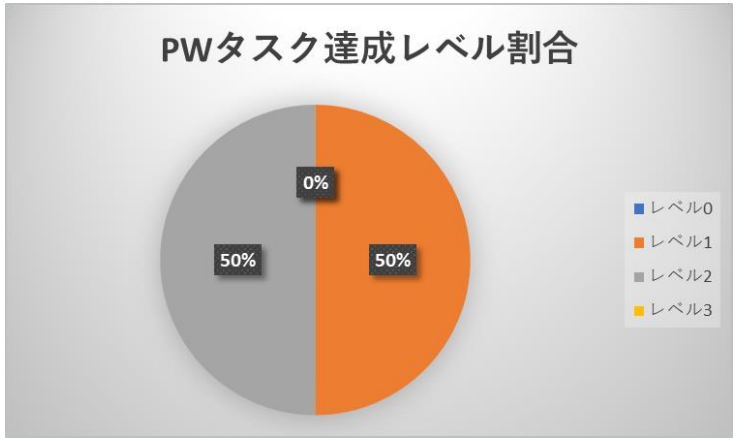
タスクカテゴリ

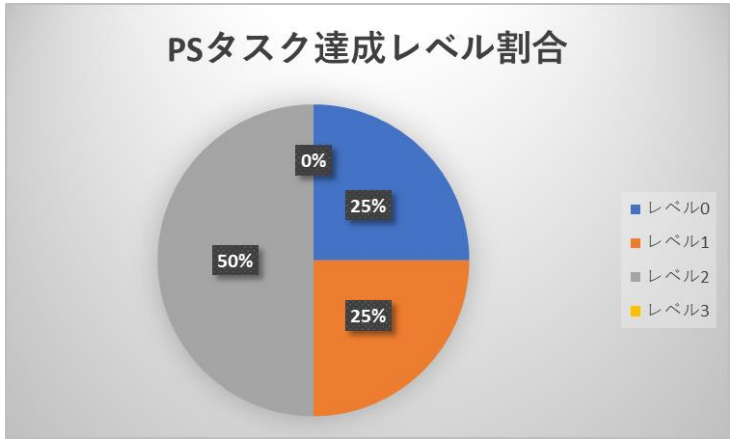
組織の準備 (PO: Prepare the Organization)
ソフトウェアの保護 (PS: Protect Software)
セキュアソフトウェアの開発 (PW: Produce Well-Secured)
脆弱性対応 (RV: Respond to Vulneravilities)

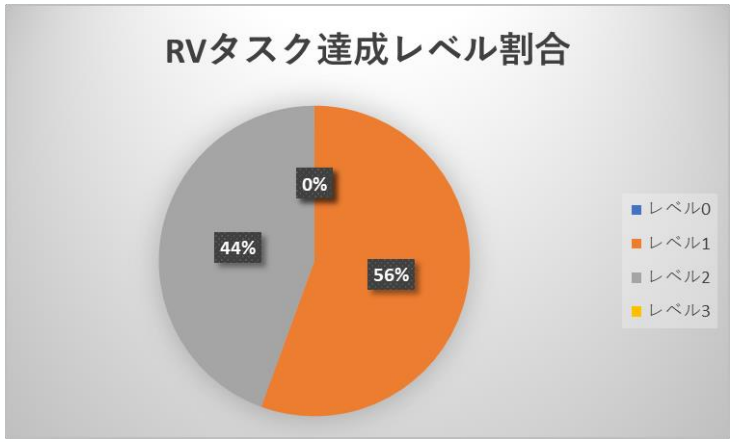
実証評価完了タスク毎の達成レベルの割合は以下の通り。

	SSDFタスク課題				
	達成レベル				合計
Task	レベル0	レベル1	レベル2	レベル3	合計
PO	0	4	8	1	13
PS	1	1	2	0	4
PW	0	8	8	0	16
RV	0	5	4	0	9
合計	1	18	22	1	42









③SSDF・国内ガイドラインマッピング表(全体イメージ)

SSDF Taskと国内ガイドラインの章項目最小単位を対象に対応関係を整理する。これにより、各組織が対応済みの国内ガイドラインを起点に、SSDFの対応Task、未対応Taskを特定し、未対応Taskについては、他の国内ガイドラインで関連する事項を特定し、自社の導入における参考情報として活用できるようにする。

対象の国内ガイドライン

発行者	ガイドライン名
METI	SBOM導入手引き　Ver.1.0，Ver.2.0
Software-ISAC	情報システムにおけるセキュリティコントロールガイドライン
デジタル庁	政府情報システムにおけるセキュリティ・バイ・デザインガイドライン
METI	サイバーセキュリティ経営ガイドライン
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
METI	サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）
MIC	クラウドサービス提供における情報セキュリティ対策ガイドライン

対応項目の包含関係区分

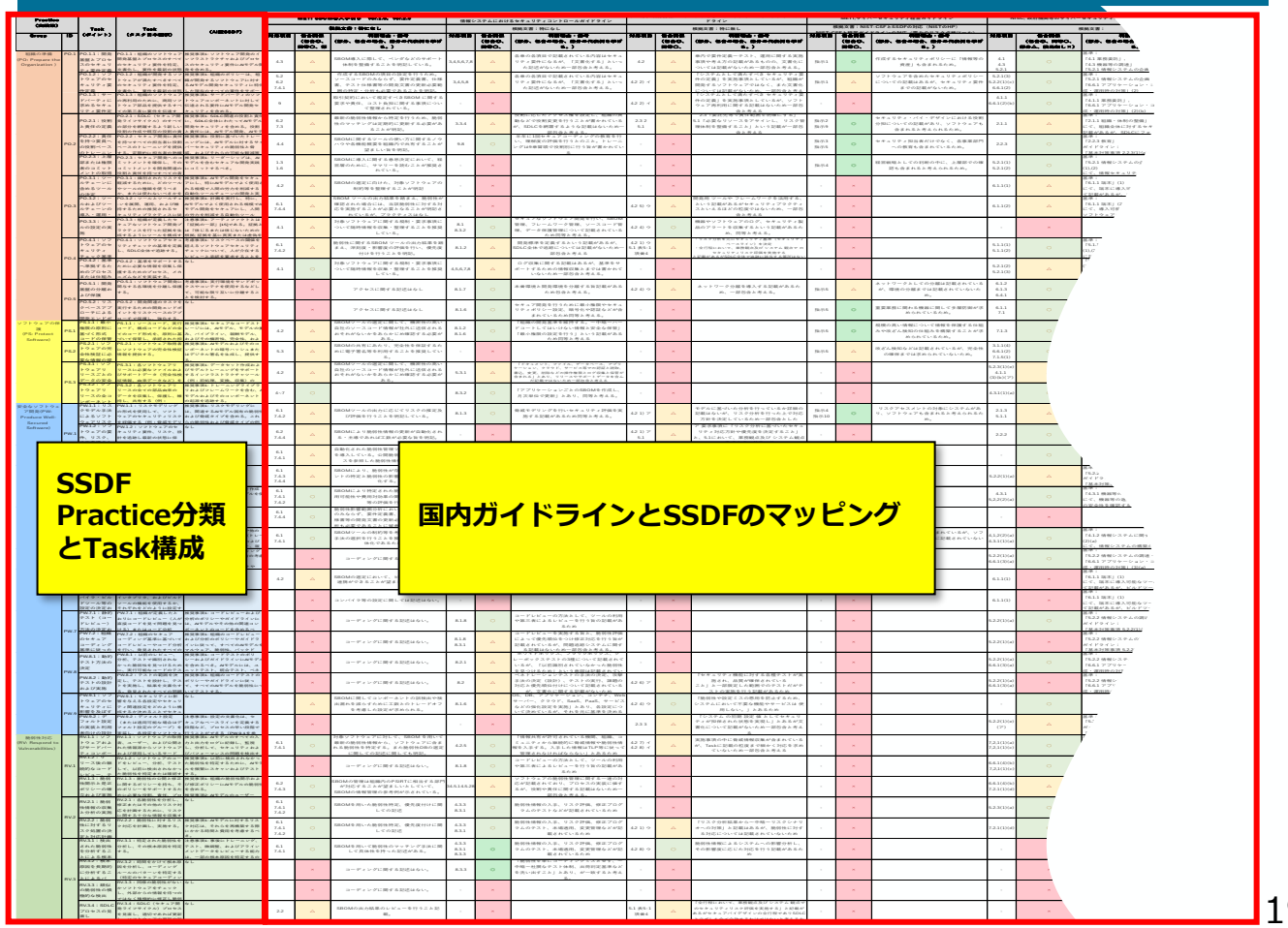
対応項目は以下の包含関係に分類しその判断理由を示す。

◎:包含	ガイドライン該当章は、SSDF taskを含みより広い
○:同等	ガイドライン該当章は、SSDF taskと同等の範囲
△:部分	ガイドライン該当章は、SSDF Taskの部分のみ
×:該当なし	SSDF Taskに該当する章は含まれない

凡例：SSDF　Taskカテゴリ

組織の準備 (PO: Prepare the Organization)
ソフトウェアの保護 (PS: Protect Software)
セキュアソフトウェアの開発 (PW: Produce Well-Secured)
脆弱性対応 (RV: Respond to Vulneravilities)

SSDF Taskと国内ガイドラインのマッピング表（全体イメージ）



③SSDF・国内ガイドラインマッピング表（例・抜粋）

- SSDF Taskに対応する国内ガイドラインの該当章を特定し、内容の包含関係について整理

◎:包含	ガイドライン該当章は、SSDF taskを含みより広い
○:同等	ガイドライン該当章は、SSDF taskと同等の範囲
△:部分	ガイドライン該当章は、SSDF Taskの部分のみ
×:該当なし	SSDF Taskに該当する章は含まれない

マッピングの例（抜粋）政府統一基準

SSDF	NISC 政府統一基準		
Task	対応項目	包含関係	包含関係判断理由
PW.1.1：リスクモデリングの形式を使用して、ソフトウェアのセキュリティリスクを評価する（例：脅威モデリング、攻撃モデリング、攻撃面のマッピング）	2.1.3 5.1.1	△	「5.1.1 情報システムの分類基準等の整備」にて、リスクの評価を行い、対応方針を決定する旨の記載があるが、**リスク評価の詳細な記載はない**。また、 「2.1.3 情報セキュリティ関係規程の整備」ガイドライン： 「（解説）遵守事項 2.1.3(1)(a)」にて、リスク評価の方法が記載されているが、**システム構築時のリスク評価ではない**ため、一部包含と判断した。
PS.1.1：ソースコード、実行コード、構成コードなどの全てのコード形式を、原則に基づいて保管し、承認された担当者、ツール、サービスなどからのみアクセスできるようにする。	7.1.3	○	「7.1.3 権限の管理」にて、**権限の最小化に基づいた情報の保護**について記載があるため。 ※ソースコード等を管理するシステムを情報システムの一種と考える。

マッピングの例（抜粋）METI　CPSF

SSDF	METI, サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）		
Task	対応項目	包含関係	包含関係判断理由
PS.3.1：各ソフトウェアリリースに必要なファイルおよびサポートデータ（完全性検証情報、由来データなど）を安全に保管する。	CPS.IP-4	◎	CPSFの「**構成要素」の一部としてソフトウェアも含まれる**と考えられるため。 根拠文書：NIST-CSFとSSDFの対応（NIST Cross-Reference Comparison Report）、NIST-CSFとCPSFの対応(METI CPSF Ver.1.0 添付D)
PS.3.2：各ソフトウェアリリースの全ての部品由来のデータを収集し、保護し、維持し、共有する（例：SBOM）	×	×	根拠文書：NIST-CSFとSSDFの対応（NIST Cross-Reference Comparison Report）、NIST-CSFとCPSFの対応(METI CPSF Ver.1.0 添付D)

④SSDF Taskの課題
SSDF実証を通じて特定された課題（例）

実証やガイドラインのマッピングを通じてSSDFに関する課題が多数特定された。大きく分類すると
「SSDFの記述や構成に係る課題」と**「SSDF実施時の困難等に係る課題」** に分けられる。その例を示す。

SSDFの記述や構成に係る課題（例）

観点	SSDFは開発フェーズに重点があり、運用フェーズでは、脆弱性管理に重点が置かれているが、その他の項目に不足がみられる。
課題	国内ガイドラインの政府統一基準、クラウドサービスのセキュリティ・ガイドラインにおいては、**ソフトウェア廃棄**に関する対策やサプライヤーとの合意などを要件化しているが、SSDFでは、その点が明記されていない。
SSDF改訂案（提言）	SSDFのTaskカテゴリ**「セキュアソフトウェアの開発(PW)」を拡張**して**「セキュアソフトウェアの開発・運用」**とするか、SSDFに「脆弱性対応(RV)」カテゴリを含めるか、新しいカテゴリとして**「ソフトウェアの運用・保守」**を作成し、ソフトウェア廃棄に関する要件を含めることが考えられる。 あるいは、 「PW.9.1：ソフトウェアのセキュリティに影響を及ぼす設定の決定」において、ソフトウェアのインストール時の設定だけでなく、ソフトウェアの更新時や削除時（アンインストール時）の設定も同時に要件化する。

SSDF実施時の困難等に係る課題（例）

Task	PO.3.1：リスクを軽減するために使うツールの特定とツールの統合に関して定義する。
課題	ツールの範囲が不明確であり、解釈の仕方によって、範囲が異なるため、ツールの範囲と位置づけを明確化したほうが良い。
対策案	想定するツールのカテゴリやツールの具体名等を列挙し、何をツールの対象にしているのかイメージしやすい内容に修正する。 具体的には、ツールカテゴリを、開発環境関連ツール、クラウド等の外部環境ツール、セキュリティ基盤**ツールの３カテゴリに分け**、各カテゴリの**具体的なツール区分とツール例**を示す。 **[1] 開発環境関連ツール** ① 統合開発環境（EClipse, VisualStudioCode等） ② プロジェクト/問題管理ツール（Redmine, JIRA, Trac等） ③ トレーサビリティツール（In-toto, TERAS等） ④ 構成管理ツール（GitHub等） ⑤ SBOM管理ツール（BlackDuck, SBOM.JP等） ⑥ ビルドJOB管理ツール（Jenkins等） ⑦ 文書作成ツール（MS Office等） ⑧ 会議システムツール（Teams, Slack等） **[2] クライド等外部環境ツール** ① 提供ライブラリ ② 提供基盤サービス ・・・・

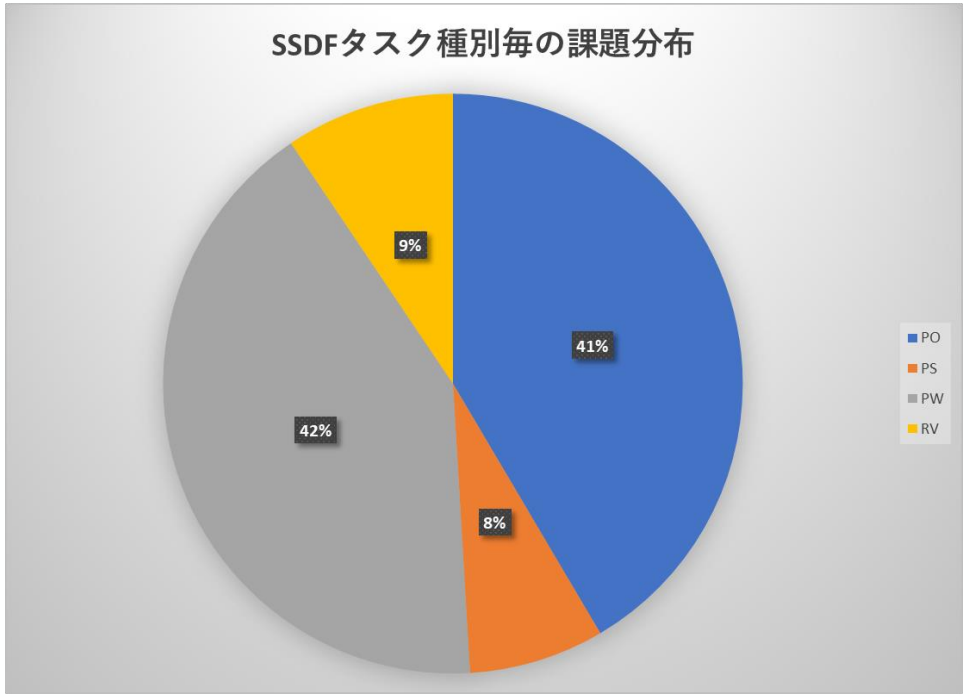
※ここで例示するツール製品等はあくまでも参考例です。

④SSDF Taskの課題
SSDF実証を通じて特定された課題（分布概観）（暫定版）

SSDF Taskの課題　- 概要 -

SSDF Taskの課題は、「SSDFの記述や構成に係る課題」と「SSDF実施時の困難等に係る課題」に分類される。 **「SSDF実施時の困難等に係る課題」の件数は多く**、特に**「難易度が高い」と想定される課題**が多い。 「SSDF実施時の困難等に係る課題」については、課題を解消するための環境整備、ガイダンスの充実などの施策が期待される。

	SSDF Taskの課題								
	SSDFの記述や構成に係る課題				SSDF実施時の困難等に係る課題				合計
Task	内容改善	定義不足	実施困難	タスク重複	開発/テスト環境	難易度が高い	開発プロセス	その他	合計
PO（13件）	1	1	0	3	5	7	4	1	22
PS（4件）	0	1	0	0	1	1	1	0	4
PW（16件）	1	2	0	0	4	9	6	0	22
RV（9件）	0	1	1	1	1	1	0	0	5
合計	2	5	1	4	11	18	11	1	53



SSDF Task種別毎の課題の件数はPO(組織の準備）/PW(セキュアソフトの開発) Task が多い。理由として、両Taskの件数が多いことのほか、以下が挙げられる。

- PO Task：他のTaskのベースとなる組織、環境の整備に係るものであり、**検討事項が多く、難易度の高い**。他のTaskは、このTaskを実施することで、効率化される。
- PW Task：**開発の実作業に直接関係**するもので、他のTaskに比べ**技術的に高度で複雑**なため。

SSDF導入の効果（中間整理）

セキュリティ・アシュアランス全体の向上

1. **体系的なフレームワークによる弱点の網羅的なチェックと解消**
   SSDF Taskは、セキュアソフトウェア開発プラクティスについて体系的、網羅的に実施すべきことを整理したものであり、本実証でそれらを適用することにより、多数の弱点やリスクを解消することができた。例えば、静的解析、動的解析などの対策においては新たな脆弱性を特定することができた。

2. **組織・ツール環境の整備によるプロセスの効率化**
   SSDFプラクティスのうち、「**組織の準備 (PO: Prepare the Organization)**」においては、組織体制やツール環境のリスクに関わる対策が示されている。これらの取組は、**「ソフトウェアの保護 (PS: Protect Software)」、「セキュアソフトウェアの開発 (PW: Produce Well-Secured Software)」、「脆弱性対応 (RV: Respond to Vulnerabilities)」**を効率的に確実に実施する上で基盤となり開発プロセスの効率化につながった。

3. **組織間の共通言語としての効果**
   SSDFにおいては、実施すべき対策について、包括的な整理を通じて共通言語を整理しているため、開発部署、品質・セキュリティ管理部署などにおける技術者と管理者のコミュニケーションを円滑に行い、対策を効率的に確実なものとすることに有効であった。

4. **（本事業の成果活用）セキュリティレベルの可視化**
   SSDFのプラクティスカテゴリおよびタスクに関して、セキュリティレベルを可視化することができ、取引相手やユーザなどの他のステークホルダに対してセキュリティレベルに関する確信を与えることができる。

個別効果（例）

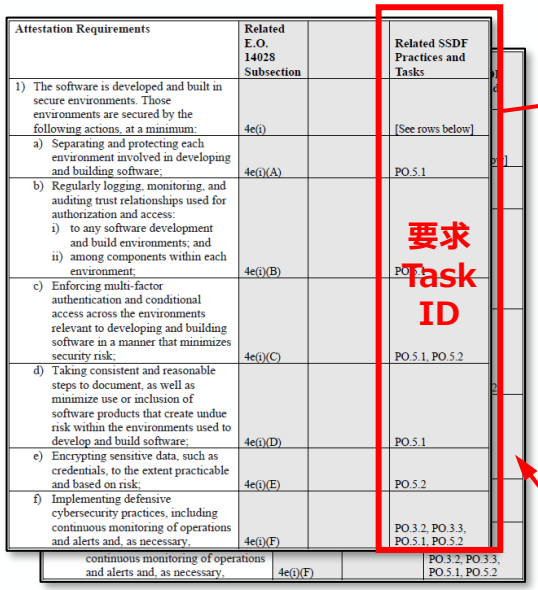
5. **OSS等のサードパーティ部品の脆弱性の特定と解消（テクニカルな効果の例）**
   本実証では、OSSサードパーティ部品についても検査を行い、多数の不具合を発見することができた。このようなテクニカルな対策により脆弱性の解消など具体的なセキュリティ向上に効果が確認できた。

⑤SSDF導入ガイダンス基礎編（整理中）
成果物を活用したSSDF導入ガイダンス（導入プロセス）

SSDF導入プロセスの手順

SSDF導入にあたり、SSDFと国内ガイドラインのマッピング表（成果物）を活用し、対応済項目、未対応項目について参考にできる国内ガイドラインの項目を特定する。SSDF Task毎に、自社にとって必要な達成基準（成果物）を特定し、実施すべき事項の基準や具体例を参考に、カスタマイズを加えて実践する。必要に応じて、CISA SSDF自己適合証明フォームに示される対応項目との関係を元に、自己適合証明書を作成する。SSDF導入プロセスの流れを以下に示す。

CISA SSDF自己適合証明フォーム



Attestation Requirements	Related E.O. 14028 Subsection		Related SSDF Practices and Tasks
1) The software is developed and built in secure environments. Those environments are secured by the following actions, at a minimum:	4e(i)		[See rows below]
a) Separating and protecting each environment involved in developing and building software;	4e(i)(A)		PO.5.1
b) Regularly logging, monitoring, and auditing trust relationships used for authorization and access: i) to any software development and build environments; and ii) among components within each environment;	4e(i)(B)		PO.5.1
c) Enforcing multi-factor authentication and conditional access across the environments relevant to developing and building software in a manner that minimizes security risk;	4e(i)(C)		PO.5.1, PO.5.2
d) Taking consistent and reasonable steps to document, as well as minimize use or inclusion of software products that create undue risk within the environments used to develop and build software;	4e(i)(D)		PO.5.1
e) Encrypting sensitive data, such as credentials, to the extent practicable and based on risk;	4e(i)(E)		PO.5.2
f) Implementing defensive cybersecurity practices, including continuous monitoring of operations and alerts and, as necessary,	4e(i)(F)		PO.3.2, PO.3.3, PO.5.1, PO.5.2
continuous monitoring of operations and alerts and, as necessary,	4e(i)(F)		PO.3.2, PO.3.3, PO.5.1, PO.5.2

要求task ID

SSDF導入プロセス

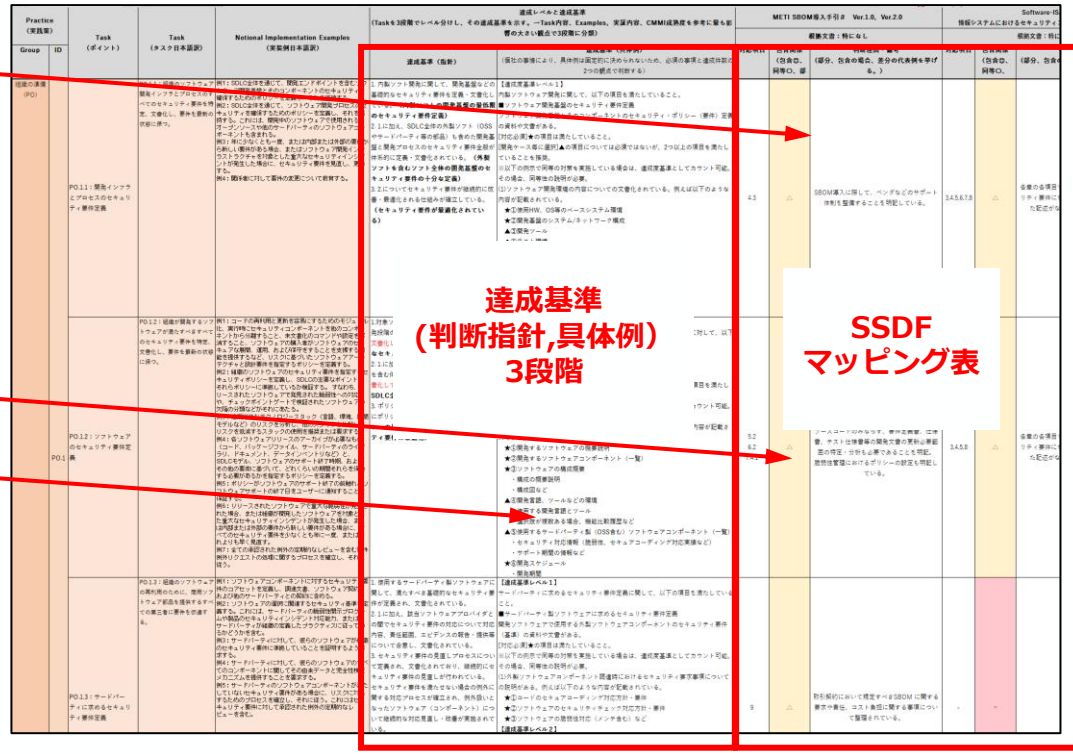
自社の国内ガイドライン対応状況、SSDFマッピング表を参考に自社のSSDF対応項目を特定

Task不足項目の特定

Task不足項目への対応
① SSDFマッピング表を基に参考となる国内ガイドラインを活用
② 実証SSDF実施内容、達成基準を参考に対応

SSDF自己適合証明の作成
① 妥当な達成基準(案)を選択
② 達成基準(案)を参考に適合基準を定義し、理由説明を作成

本実証SSDF Task達成基準（案）



達成基準（判断指針,具体例）3段階

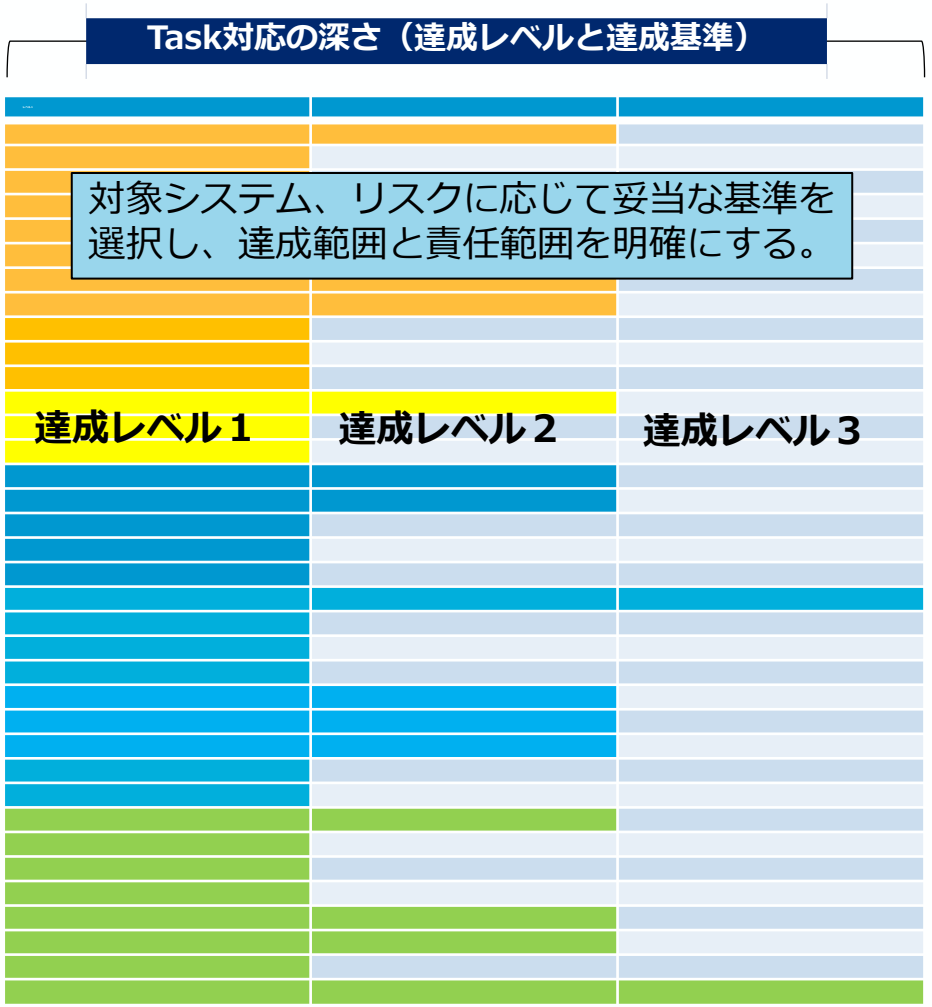
SSDFマッピング表

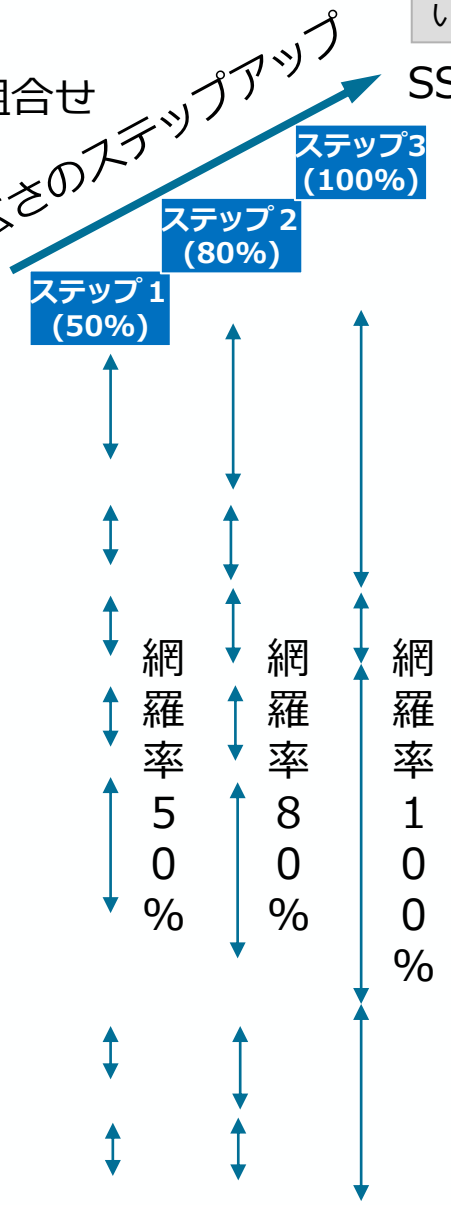
⑤SSDF導入ガイダンス基礎編（整理中）
SSDF導入ガイダンス（基礎編）使い方

ステップアップアプローチ（イメージ）

SSDFの達成度は、Task対応項目の範囲（広さ）と各Taskの達成レベル（深さ）の組合せで決まる。現場に導入する際は、Task項目は段階的に拡大することが想定される。

SSDF Task一覧





Task難易度をベースに５０%、８０%、１００%に暫定分類できないか。

SSDF自己適合証明

広範なTaskを最初から網羅することは難しいため、Taskの網羅性は個社の状況に応じてステップアップ

１．ソフトウェアの管理手法等に関する海外の動向

２．実証の中間報告と成果イメージ

３．今後の取組案

今後の取組項目案

(1) 国内事業者向けSSDF導入ガイダンスの整備

・SSDF導入ガイダンス基礎編の成案化
・SSDF導入ガイダンス応用編の作成
・国内ガイドラインの不足項目（残課題）の特定と対応方針の検討

(2) 自己適合宣言の仕組みの検討・構築

・SSDFの達成レベル識別の可視化をベースとした自己適合宣言の仕組みの検討・構築
・自己適合宣言の仕組みの政府調達等への要件化の検討

(3) 基準の国際調和の検討

- 9月日米豪印首脳共同声明に言及された通り、「ソフトウェア・セキュリティに関する日米豪印共同原則」について官民連携し、政府調達要件における国際調和を図る。
- SBOM導入手引2.0(英語版)を国際文書から参照させることにより、国際的な成果の普及を図る。

(1) 国内事業者向けSSDF導入ガイダンスの整備(次年度以降)

- 次年度以降、国内事業者向けにQUAD等で求められるSSDFを導入するためのガイダンスの整備を進める。具体的には以下の事項を想定する。

  - **SSDF導入ガイダンス基礎編の成案化**
    今年度策定するSSDF導入ガイダンス基礎編について、タスクフォース委員からの意見およびパブコメの意見を反映し成案化する。

  - **SSDF導入ガイダンス応用編の作成**
    今年度の実証と異なる分野の実践例を通じて、SSDF導入方法に関する拡充するとともに、具体性を高めることで応用編を作成する。また、SSDFにより体系化されるベストプラクティスを根拠にして、ソフトウェアのセキュリティの説明責任を果たすためのアカウンタビリティベース・アプローチの考え方やセキュリティ確保の方法についてまとめる。

  - **国内ガイドラインの不足項目（残課題）の特定と対応方針の検討**
    SSDFと国内ガイドラインのマッピング結果に基づき、国内ガイドラインにおいて不足する項目を特定し、関連ガイドラインの拡充の方策について整理する。
    例えば、国内ガイドラインにおいて不足する項目としては、ツールチェーンのセキュリティ確保やトレーサビリティ確保などが挙げられる。

（２）自己適合宣言の仕組みの検討・構築（次年度以降）

- 次年度以降、SSDF導入の実効性を高めるための自己適合宣言の仕組みの検討・構築を行う。実証を通じてSSDFの課題を多数特定している。
- **達成レベルの識別をベースとした自己適合宣言の仕組みの検討・構築**
  特に、SSDFの抽象度の高さに伴なう解釈の幅や導入組織のレベルの差の問題について、本年度実証を通じて達成レベルと達成基準の整理を行った。このようなSSDFの課題を解消しつつ、SSDFの達成レベル識別と可視化をベースとした自己適合宣言の仕組みや制度について検討する。
  また、発注者と調達者によるSSDF達成レベルの決定者の責任を前提とした仕組みの効果と影響について考慮して検討を行う。
- **政府調達等への要件化の検討**
  策定した自己適合宣言の仕組みを政府調達等の要件とすることについて検討する。具体的には、NISC政府統一基準等への記載案を検討し、調整を図る。

(3) 基準の国際調和の検討

QUAD共同原則をベースにセキュア・ソフトウェア開発に関する基準の国際調和、産業競争力強化や国際戦略を意識した国際連携の方策を検討する。

具体的には、SBOM導入手引2.0(英語版)が国際文書から参照されるよう調整し、国際的な成果の普及を図る。また、QUAD共同原則においては、政府調達基準の整合性が求められるため、（２）で検討する内容と関連付けて進める。政府調達基準には以下のような選択肢が考えられる。

	ケース1 国内政府調達基準を米国政府調達基準に揃える	**ケース２ 国内政府調達基準を米国政府調達基準より条件を緩和する**	**ケース3 国内政府調達基準を米国政府調達基準よりも高い基準**	**ケース４ 国内基準は、実証で定義した達成レベル３段階を活用し柔軟に設定する**
概要	米国政府調達におけるSSDF自己適合証明に揃え国内政府調達基準も、SSDF自己適合証明と同等とする。	国内政府調達基準では、米国SSDF自己適合証明で指定されるTask項目の条件を緩和しそのサブセットとする。	国内政府調達基準では、SSDFについて定義したレベルのうち、レベル２，３など高い条件を含める。	企業の判断に応じて達成レベルを定義する。
メリット	米国に輸出する国内企業は、国内製品と同等のセキュリティ対策を行うため、異なる基準への対応の非効率が避けられる。	国内では緩和された条件で対応コストが抑えられる。	米国より高い国内基準を満たしていれば、そのまま米国政府に納入できる。	リスクに応じて柔軟に達成レベルを定義し、コストを抑えられる。
デメリット	ー	米国に輸出する場合、国内より高い基準に対応しなければならなくなる。QUAD共同原則および安全保障確保の観点から、米国は日本に対して米国のSSDF自己適合証明より高い基準を要請する可能性がある。	国内市場のコストが上昇し、競争力に不利。	ー

（参考）SSDF対応に関するヒアリング

委員会限り

委員限り

（参考）「ソフトウェア管理に向けたSBOMの導入に関する手引ver2.0」英語版のご紹介

2024年12月13日に以下の経産省HPにて「ソフトウェア管理に向けたSBOMの導入に関する手引ver2.0」英語版を公表。
(公開HP) https://www.meti.go.jp/english/policy/safety_security/cybersecurity/index.html

ver. 2.0

Specification of vulnerability management process

Background and Objectives

- Provide specific process-based examples of methods and procedures for vulnerability management using SBOM.
- There are **currently unresolved** issues in vulnerability management using SBOM. New **technology development, standardization, and tool environment development** will be necessary to fully resolve these issues.
- In this chapter, we present the concept and the best practices that are currently possible in order to avoid the issues by operations on the SBOM user side, including those issues.

Major issues and solution approaches and know-how

Issue	Solution approaches and know-how
Failure in matching with vulnerability DB due to coexistence of part IDs	Use of ID conversion tools such as Purl2cpe and partial ID matching using APIs
Ensuring coverage of diverse vulnerability databases	Presentation of vulnerability DB selection method based on risk and cost reduction benefits
Prioritizing vulnerability responses for rapid response and efficiency	Presentation of a prioritization category decision method using a decision tree based on SSVC
Information sharing and role-sharing throughout the supply chain	Presentation of the steps for information sharing and implementation items by developers and users
Division of roles in vulnerability response	Presentation of items to be implemented by developers and users in provisional and full-scale response

Vulnerability Management Process and Step using SBOM (Overview)

Phase 1 Vulnerability Identification

1. **Selection of a matching method category**
   Organizations should choose a method from (i) the Use of existing SBOM tools, (ii) API utilization scripts, and (iii) Web UI based on their technical capabilities, budget, and available resources.
2. **Identification of available SBOM data**
   Determine how to obtain the SBOMs that will be utilized.
3. **Selection of a target vulnerability database**
   Choose the vulnerability databases that will be used for vulnerability identification and prioritization of responses.
4. **Selection and implementation of a matching method**
   Based on the results from Steps 1 to 3, decide on the organization's specific method for vulnerability identification.

Phase 2 Vulnerability Response Prioritization

1. **Vulnerability filtering**
   Narrow down vulnerability information that needs to be addressed from known information prior to prioritization using external information.
2. **Selection and acquisition of prioritization information**
   Based on the components of risk, select and acquire the necessary information according to the company's policy, such as the existence of incidents, Exploit code distribution status, CVSS, and VEX information.
3. **Category determination based on prioritization decision tree**
   Prioritize category judgments according to (developer, user organization) x (high/low technical capability) according to the judgment tree organized based on SSVC.
4. **Priority score evaluation**
   In parallel with steps 1 through 3, perform detailed prioritization by prioritizing within categories by quantitative scoring as needed.

Phase 3 Information Sharing

1. **Identification of shared information and recipients**
   - Identify shared information such as vulnerability information, load information, and prioritization results.
   - Identify sharing parties and the order of sharing, such as social organizations, external parties (users, vendors, suppliers), etc.
   - Identify sharing triggers such as triggers for sharing (push type/pull type).
2. **Identification and implementation of the sharing method**
   - Identify the sharing method for file sending/receiving, SaaS, etc.
   - Specify access privileges: Specify the private and disclosure scope, privileges, etc., depending on the confidentiality.
   - Implement sharing based on the determined sharing method and access privileges.

Phase 4 Vulnerability Response

1. **Temporary Vulnerability Response**
   - Establish temporary measures, such as such as suspension of use, reduction, and workaround.
   - Apply the temporary measures, after informing stakeholders of the temporary measures decided upon.
2. **Fundamental Vulnerability Response**
   - Implement a fundamental response by identifying the developer of the software involved in the vulnerability and having the developer fix the vulnerability.
   - Update SBOM/VEX information upon fixing vulnerabilities.
   - Share updated SBOM/VEX with the supply destination and conduct SBOM history management as necessary.

論点

ご議論いただきたいこと

- 今年度の成果物の方向性
- 今年度以降の事業について

付録

【米国】 安全なソフトウェアデプロイメントの実現に向けたガイダンスの発表

米CISAが、安全なソフトウェアデプロイメントに向けたガイダンスを発表した。

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

主要フェーズ		検討・実施すべき項目とその内容
1. 計画	オペレーショナル・リスク評価	ソフトウェアを環境にデプロイする際のリスクと結果について、包括的かつ継続的な評価を実施する。 システムの関係と相互依存、潜在的な脅威、安全性、セキュリティ、信頼性、性能要件及び一般的な欠陥に関連するリスクを理解する。
	故障予知レビューの実施	以前の経験から得た洞察をもとに故障予知レビューを行う。この際、チームが潜在的な失敗を特定するのに役立つ。
	プラットフォームの規模と多様性の検証	プラットフォームの多様性のほか、デバイスの数、OSの種類、ハードウェアブランド、ファームウェアのバージョン、ファームウェアの設定、帯域幅の速度と信頼性、環境設定、地理的な環境などの多様性を検証する。
	オンライン・サービスの多様性の検証	データセンター地域やネットワーク構成のほか、必要に応じて、フェイルオーバーやバックアップ・ソリューションに関する多様性を検証する。
	計画デプロイメントの間隔	ソフトウェアデプロイメントを行う時間的な間隔を正式に決定し、社内外に明確に伝達する。
	モニタリングとレポーティングの戦略	システムの健全性を示す信号を特定し、特定された問題を報告して、継続的改善プロセスにフィードバックする。
	人材確保	ソフトウェアデプロイメントと安全なプロセスの改良の両方を監視できるチームを確保する。
	フォールト・トレランス	悪意のあるコード等が組み込まれても安全に機能するようなシステム設計を行うための、レジリエンスを組み込む方法を検討する。
	機能廃止と製品寿命の計画	機能の廃止や製品の寿命をあらかじめ計画し、顧客に早期に警告を行うことで悪影響を小さくする。
	パッチ計画	パッチ適用の計画と、パッチの適用プロセスの可能な限り迅速な実施するための手段を確立する。
2. 開発とテスト		顧客の典型的な環境に近い環境でテストを行い、テストにおいてソフトウェアデプロイメントプロセスを積極的に失敗させることにリソースを割く。
3. 内部でのロールアウト		組織内部でのみロールアウトすることで、外部ユーザーに届く前に問題を発見する。十分なカバレッジを得るため、以前のリリースサイクルを基に調整された標準を組織内で確立すべきである。
4. デプロイメントとカナリアテスト		カナリアデプロイメント（限られた数の顧客又はシステムに対する小規模なデプロイメント）によって、大規模なロールアウトの前にパフォーマンスを監視し問題を解決する。顧客のリスク許容度に応じてバリエーションを検討する。
5. 管理されたロールアウト		カナリアデプロイメントの成功を確認の後、デプロイするデバイスやシステムを段階的に増やすことで、突然の広範囲な障害を防ぐ。この際、適切な速度を考慮する。
6. 計画へのフィードバック		リリース後の継続的なフィードバック（ステークホルダーからの洞察、ログ、異常動作の例）を、次の開発サイクルの計画段階に直接フィードバックする。

出所）CISA, “Safe Software Deployment: How Software Manufacturers Can Ensure Reliability for Customers” https://www.cisa.gov/resources-tools/resources/safe-software-deployment-how-software-manufacturers-can-ensure-reliability-customers

【米国】 SBOMの概念と実装に関するレポート（第3版）の公表

米CISAが、SBOMの概念・実装に関し、ベースライン属性や成熟度を示したレポートを改定した。

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

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

ベースライン属性		各成熟度レベルで期待される事項		
		レベル1: 最小限	レベル2: 実施推奨	レベル3: 目標
SBOM メタ情報	著者名	名前と、電子メールアドレスなどの一意的な識別情報を含める。	SBOMの作成において作成者を支援したツール及びバージョンを特定する。	―
	タイムスタンプ	ISO 8601のような共通の国際形式を使用する。	―	―
	タイプ（省略可能）	―	―	（項目自体が目標）
	主要コンポーネント	（各SBOM属性の期待事項に従う）	（各SBOM属性の期待事項に従う）	（各SBOM属性の期待事項に従う）
SBOM 属性	コンポーネント名	コンポーネント名はコンポーネントの一般的なパブリック名を宣言する。	―	―
	バージョン	サプライヤーが提供するバージョン文字列を宣言する。	―	―
	サプライヤ名	すべてのコンポーネントについてサプライヤ名が宣言する。	―	―
	一意の識別子	各コンポーネントに対して少なくとも1つの一意な識別子を宣言する。グローバルに一意な識別子が望ましい。	コンポーネントに対し利用可能な限り多くのグローバルに一意な識別子を列挙する。	―
	暗号ハッシュ	ハッシュ又はハッシュを生成するのに十分な情報を提供する。十分な情報が得られない場合は不明とする。また、再現性を可能にするため、ハッシュアルゴリズムとハッシュされるコンポーネントオブジェクトを提供する。	主要コンポーネントのハッシュを少なくとも1つ提供する。ハッシュアルゴリズムは、SBOM に記載されているすべてのコンポーネントおよびシステム依存性に対して、暗号的に安全なSHA2ファミリー（SHA-256 以上）を用いる。	―
	関係性	主要コンポーネントと直接の従属コンポーネントについて、関係及び関係の完全性を宣言する。	SBOMに記載されているすべての構成要素について、関係及び関係の完全性を宣言する。	可能な限り多くの動的及びリモートコンポーネントとの関係及び関係性を特定する。
	ライセンス	主要コンポーネントのライセンス情報を提供する。	できるだけ多くのコンポーネントのライセンス情報を提供する。	リストされたすべてのSBOMコンポーネントのライセンス情報を提供する。締結済みライセンス情報、すなわちライセンステキストおよび締結済み条件が SBOM に含まれていることを証明する。
	著作権	主要コンポーネントの著作権表示を行う。	できるだけ多くのコンポーネントに著作権表示を行う。	リストされたすべてのSBOMコンポーネントの著作権表示を提供する。

出所） CISA, “Framing Software Component Transparency (2024)” https://www.cisa.gov/resources-tools/resources/framing-software-component-transparency-2024

【EU】 サイバーレジリエンス法（CRA）の正式発行

CRAが2024年11月に正式発行。2026年9月に脆弱性報告義務が適用、2027年12月に全面適用。

- EU市場に上市されるデジタル製品に対してサイバーセキュリティ対策を義務付けるサイバーレジリエンス法（CRA）について、2024年10月10日に欧州理事会により正式に採択され、2024年11月20日にEU官報に掲載され、正式発行された。20日後の2024年12月11日に発効となった。
- 発効より36ヶ月後の**2027年12月11日以降、CRAで規定されたサイバーセキュリティ対策が義務付け**られる。ただし、第14条で定められる**製造者の脆弱性報告義務については、21ヶ月後の2026年9月11日以降の適用**となる。
- 対象製品について、**ソフトウェアやハードウェアを含む、他の製品やネットワークへの直接的・間接的な接続が存在するあらゆるデジタル製品が対象**となるが、既存のEU法により要求事項が課されている**医療機器、自動車関連製品等は除外**される。対象製品の上市に当たって、**当該製品に対するセキュリティ要件への適合性証明（自己適合宣言又は第三者認証）が求められる**。
- 対象となるデジタル製品に対する要求事項として、**リスクに応じた適切なレベルのサイバーセキュリティを確保するように設計・開発・生産すること**や、**悪用可能な既知の脆弱性がない状態で提供すること**を求めている。
- また、製造業者に対する要求事項として、デジタル製品の脆弱性ハンドリングに関する要求、製品のセキュリティ評価に関する要求、利用者への情報提示に関する要求、製品の適合性評価に関する要求、脆弱性の報告義務に関する要求等が規定されているほか、**SBOMやOSS管理に係る要求**も規定されている。
- 製造業者が本法案のセキュリティに関する要件を遵守にしない場合、**最大1,500万ユーロもしくは前会計年度の世界全体の総売上高の最大2.5%のいずれか高い方が罰金として科される**。

EUサイバーレジリエンス法の対象製品

サイバーレジリエンス法の対象となる「デジタル製品」

デジタル要素を備えた全てのソフトウェア製品・ハードウェア製品で、デバイスやネットワークに直接的/間接的に接続されるコンポーネントも含む。

▶ **自己適合宣言もしくは第三者認証を選択**

重要な「デジタル製品」（クラスⅠ）

重要な「デジタル製品」であるが、リスクが低い製品。産業用以外のルーター・スイッチ、VPN装置、SIEMなど。

▶ **EUCCやEN規格の対象外の製品は第三者認証が必要**

重要な「デジタル製品」（クラスⅡ）

重要な「デジタル製品」のうち、リスクが高い製品。産業用ルーター・スイッチ、産業用制御システム、PC用のOSなど。

▶ **第三者認証が必要**

対象外の製品

- 医療機器
  （Regulation (EU) 2017/745の対象機器）
- 体外診療用医療機器
  （Regulation (EU) 2017/746の対象機器）
- 自動車
  （Regulation (EU) 2019/2144の対象機器）
- 航空機関連機器
  （Regulation (EU) 2018/1139の対象機器）
- SaaSなどのソフトウェアサービス
  （NIS2指令の対象サービス）等

出所） EU, Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) https://eur-lex.europa.eu/eli/reg/2024/2847/oj

今年度の実証の目的

第13回ソフトウェアTF
資料より

QUAD合意で対応が想定されるセキュア・ソフトウェア開発フレームワークSSDF(NIST SP800-218)をベースに、国内企業のソフトウェア・セキュリティの促進を図るため、SSDFと国内ガイドラインのマッピングを行い、実ソフトウェアを対象に、SSDFタスクの実践、机上評価、マッピングの妥当性確認、課題等の整理を行う。

サプライチェーンのライフサイクルプロセスを通じてSSDFのスコープに対応した実践と課題等の評価を行う。

マッピング表や評価結果は、SSDF国内ガイドラインにおいて不足する項目、米国に対する提案項目の検討に活用し、制度調和につなげる。

ライフサイクルプロセス全体におけるSSDFのスコープ