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
（第13回）議事要旨

1. 日時・場所

日時：2024年8月21日（水）10:00～12:00

場所：オンライン開催

2. 出席者

委　　員：土居委員(座長)、出雲委員、伊藤委員、稲垣委員、猪俣委員、大場委員、木谷委員、下村委員、
中嶋委員、関委員、高田委員、髙橋委員、寺田委員、萩原委員、松岡委員、渡辺委員

オブザーバ：内閣官房　内閣サイバーセキュリティセンター、警察庁、総務省、厚生労働省、
一般社団法人　日本医療機器産業連合会

事　務　局：経済産業省　商務情報政策局　見次サイバーセキュリティ制度企画室長
味木サイバーセキュリティ課補佐、飯塚サイバーセキュリティ課補佐

3. 配付資料

資料1　議事次第・配布資料一覧

資料2　委員名簿

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

参考資料１「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引 ver2.0（案）」に対する意見募集で寄せられた御意見に対する考え方

参考資料２　ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引 ver2.0（案）

4. 議事内容

事務局から、資料３に基づき説明した後、自由討議を行った。各委員からの意見は以下のとおり。

● パブコメ対応版について

- パブコメで頂いた意見のうち、注目すべき意見が３つある。
  - １点目は、動的なコンポーネントは SBOM 管理が難しいという意見である。ソースコードやコンパイル済みのバイナリ以外にも、実行可能なスクリプト（VBA、マクロ等）やローコードなど、ソフトウェアには様々な形態が存在する。SBOM で管理できるものと管理できないものを具体的に例示できると良い。
  - ２点目は、ボリュームが多いため、分冊を検討すると良いという意見である。パブコメで頂いた意見の中に、ソフトウェアの脆弱性はメーカーが対応すれば良いというコメントがあったが、SBOMの活用イメージが定着していないことに起因して提出された意見なのかもしれない。啓蒙の観点から、ユーザー視点でメリットが得られるものを分冊するのが有効だと考える。分冊のコストを考えると、目次レベルでユーザー視点のメリットが書かれた章を作成するという案も考えられる。

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

・ 米国における政府と産業界の共通の理解として、SBOM は有望ではあるが、実証において課題が見つかっており、あくまで機能する範囲でのみ利用することが現実的という認識となっていると考える。産業界にとって SBOM が安心して使えるものとなるように、有効であると確認できる範囲で SBOM を活用する等、具体的な方針を提示していくことが有効であると考える。例えば、クラウドソフトウェアは継続的にアップデートが行われることが多いため、SBOM の効果がどこまであるか不明であると考えるため、実証により効果が確認できたものを示せると良い。

・ パブコメで頂いた意見（No.71）への対応の考え方の「対価を負担」という記載について、費用と責任の観点から、現時点で調達者が対価を負担するという表現は具体性が強いと考える。例えば、「一定の負担をする」又は「中長期の課題として取り組む」等の表現の方が良いと考える。

・ また、費用に関しては、パブコメで頂いた意見（No.94）への対応の考え方において、「重要な課題として、中長期の課題として取組む。」と記載されている。国際的なハーモナイズや実証の中で、対価を負担するのか、全体に掛かるコストの一部を負担するのか、現時点で断定してしまうのは時期尚早と考える。SBOM は社会基盤として重要な役割をなすため、対価を負担するという表現は適していない可能性がある。今後、どういったファンドから、どういった当事者が、何を負担するか等を設計することが重要であると考える。加えて、SBOM の費用負担の問題は、X-Y といった単純な取引当事者間の問題ではなく、サプライチェーン全体に関わる問題であるため、サプライチェーン全体でどのようにして利益を享受できるかを検討できると良い。そのため、政府として重要性を認識していることを示しつつ、考慮すべき事項を示した内容として示せると良い。

・ 一方的に「調達者が対価を負う」と記載すると、SBOM の活用意向低下につながる可能性がある。SBOM の利用価値を明確化し、社会的な共通認識の醸成を図ることで、自然な形で調達費用を捻出可能となるのではないかと考える。例えば、利用価値を明確化し、利用方法に応じた対価の社会合意を図るなど、課題提起にとどめるような形が良いと考える。関連して、パブコメで頂いた意見への対応で「中長期的な課題」に関する対応が一定数ある。SBOM 導入手引の中で発信することが適切か否かについて検討が必要だが、中長期的な課題を何らかの形で発信し、社会から意見をもらうのも良いと考える。

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

● <u>実証の方向性について</u>

・ 8/6 に実施された「サイバー安全保障分野での対応能力の向上に向けた有識者会議」においてこれまでの議論に関する整理結果が公開されたと認識している。「ソフトウェア等の脆弱性対応」の項において、「安全な製品開発や脆弱性の対応に関するベンダーの責任を規定すべきではないか。」という記載がある。このような考えは、早期警戒パートナーシップの運用が開始した 20 年前から議論してきたことであるが、脆弱性が発見されたからといって一方的に責

任を取らせることはできないと考える。そのため、SSDF のような統一的な開発フレームワークが政府から提示されることは良いことだと考える。

- 一方で、最近米国 CISA が Secure by Demand Guide を発表した。これは、ソフトウェアの調達者視点でのセキュリティの考慮事項を示したものであると認識している。米国は Secure by Design、Secure by Default から Secure by Demand までを検討しており、先行して取組を行っている印象である。日本ではまず Secure by Design、Secure by Default を推進し、その上で調達者側のセキュリティ向上を目指すことが適切であると考える。

- 実証でのマッピングの対象が国内文書と記載されているが、米国 CISA が発表した Secure by Design、Secure by Default の文書に対して、日本からは NISC と JPCERT/CC が共同署名を行っている。本文書に関して、サイバーセキュリティ戦略本部は「いずれの項目もサイバー空間の昨今の状況変化を踏まえた妥当なものと考えられる」との意見を発表しており、日本としても重要な文書と位置づけられていると認識している。本文書で記載された内容と、本事業の実証で作る成果物の内容に齟齬が生じないよう、考慮しながら検討できると良い。

- SSDF と国内ガイドラインのマッピングは重要だと考える。1 つのガイドラインに従うことで SSDF に準拠できれば、事業者の負担が減ると考える。まずは国内ガイドラインと SSDF との差分を洗い出すことが重要であると考える。

- また、自動車のソフトウェアは国連の UN-R155 と ISO/SAE 21434 への準拠が求められるが、これらと SSDF の比較についても将来検討できると良い。

- マッピングの対象とするガイドラインについて、現状提示されている文書には、調達側の文書と開発側の文書が混在しているように見受けられるため、例えば、開発側のガイドラインと調達側のガイドラインを分類してマッピングした方が良いと考える。また、SSDF を推進するうえでは IT ベンダーによる活用が重要であるため、関連する検討会と連携しながら進められると良い。その際には、SBOM の対価負担を IT ベンダーが行うべきか、ユーザーが行うべきかといった点についても考慮できると良い。

- QUAD の共同原則を前提とした取組は承知しているが、一方で、欧州ではサイバーレジリエンス法の取組があるほか、国際間のガイドラインとしては、ENISA、FIRST、OWASP 等の文書も本来は考慮するべきであると考える。SSDF との比較の重要性は理解できるが、今後は欧州にも目を向けると良い。

- 様々な業界において、様々なガイドラインが作成されているが、作成された文書の運用も考慮できると良い。加えて、全体コストの最適化が重要であると考える。コスト面を実証で確認することにより、実現性の高い文書の作成が可能となると考える。来年度以降は、インセンティブや補助の在り方を検討できると良い。

- マッピングされた成果物の運用方法は難しい問題であると認識している。まずは大枠の考え方について、マッピングすることが現実的である。

- サイバーレジリエンス法では、脆弱性の報告が罰則規定として位置づけられていると認識している。サイバーレジリエンス法が今後施行される中で調和についても検討する必要があると考える。また、中小企業の取組に対する支援策を並行して検討する必要があると考える。

- 米国 CISA では自己適合証明という表現をされているが、事務局資料中では自己適合宣言となっている。自己適合証明と自己適合宣言について関係性を明確化し、検討できると良い。

- QUAD の取組が先ではあるが、米国 CISA の Secure by Design、Secure by Default の文書では、より厳格な内容が記載されており、脆弱性コーディネーションに関する記載もあると認識している。SSDF のマッピングから始めつつ、Secure by Design、Secure by Default の取組につなげていく方向性が良いと考える。

- SSDF は汎用的な共通言語であるため、具体的な実装は組織ごとで異なると考える。米国 NSA では Enduring Security Framework（ESF）という具体的な手法を含んだ文書を発表している。SSDF とのマッピングを進めた上で、中小企業に向け、もう一段具体化したプラクティスや手順が必要になってくると考える。実施するか否かという 0-1 の議論ではなく、OSS のみ SBOM を作成するなど、ステップを踏んだ導入の仕方も想定される。二極化させるのではなく、改善の方向性を示せると良いと考える。例えば、NSA の ESF では、例えば、NSA の ESF では、パッケージリポジトリサービスを活用して社内で承認された部品だけを利用する手法なども示されており、開発ツールの利用等で中小企業が取り組みやすいよう、敷居を低くする配慮も必要であると考える。

- ESF は、大統領令 14028 を踏まえ、NSA が業界団体に作成させたものであると認識している。

.

● <u>今後の事業について</u>

- Secure by Design、Secure by Default の文書は上位の視点から記載されており、SBOM はその取組の一部である。求められる取組の全体感と SBOM の位置づけを説明していく必要があると考える。

- 部品 ID の標準化について、商品を流通させる仕組みに組み込むことが有効であると考える。米国では purl ベースの検討が進められていると認識している。SBOM のみならず脆弱性対応を進めるうえで NVD(CVE 採番と脆弱性の分析)への依存が強いため、NVD の運用が停滞したときの影響が大きいと考える。国内で脅威インテリジェンスを共有する仕組みを作ることが良いと考える。

- 早期警戒パートナーシップ側の検討において、部品 ID に関する検討を進める予定である。

- SBOM について、日本の政府統一基準等に記載の内容で適用を考える際に、米国の基準との相互運用性があるかを今後実証の対象とできると良いと考える。

- 前回の本タスクフォースにおいて、総務省から通信機器を対象に SBOM の導入を検討するという趣旨の説明があった。今後も引き続き、必要に応じて総務省と経産省で連携して取組を進められると良い。

- グローバルサプライチェーンにおける対策の検討が必要であると考える。SSDF や Secure by Design、Secure by Default の文書等、様々な文書や取組があるが、つながりが分かりにくい状況にあると認識している。グローバルサプライチェーンに関与する事業者を支援する目的で、情報の整理が必要であると考える。ソフトウェアのセキュリティを担保することが、企業の取組における最低条件になりつつあると考える。SBOM に課題があることは理解するが、政府調達要件に含めるなど、需要側へのシグナルを増やしていくことが重要であると考える。

- SBOM や SSDF をサイバーハイジーンにつなげる際、中小企業への展開が重要となると考える。コスト面を考えれば、現在使われている脆弱性スキャンツールとの併用で SBOM を普及させていくのが良いと考える。中小企業の規模感は様々であるが、金融に関して言えば、企業全体の規模ではなく、情報システムに関わる担当者の人数が重要となると考える。従業員数が多くても、セキュリティを 2～3 名で回している企業も存在すると認識している。

- 他産業でも、従業員が数万人の規模でも、セキュリティ担当者が 10 名程度の場合もある。SBOM 導入手引や SSDF を受け止めることができない企業を、規模の小さい企業として考えると良い。

- XZ Utils に悪意のあるコードが挿入された問題が明らかになったが、これは、攻撃者が OSS のコミュニティ活動に積極的に関与し、OSS のメンテナーになったあと、バックドアが仕掛けられた事例である。OSS では、活動のピークと利用のピークが異なるため、脆弱性が発見される時期がずれるおそれがある。これは OSS 開発の構造的な問題であると認識している。すでに OpenSSF がこの問題に取り組んでおり、コミュニティへの働きかけは重要であると考える。また、利用者側での省力化も今後検討できると良い。例えば、静的解析を自動化する AI を活用すれば、効率的な脆弱性の検出が可能となると考える。

- XZ Utils のメンテナーの問題は、商用ソフトウェアでも発生する問題である。悪意ある内部犯行者の問題は、IT に限らず発生していると考える。

以上