産業サイバーセキュリティ研究会WG1
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7回）議事要旨

1. 日時・場所

日時：2022年7月26日（火）14:00～15:50

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、
鈴木委員、関委員、高田委員、髙橋委員、寺田委員、野山委員、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、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

経済産業省：大臣官房　上村サイバーセキュリティ・情報化審議官、
商務情報政策局　奥田サイバーセキュリティ課長、佐藤サイバーセキュリティ課企画官、
塚本サイバーセキュリティ課補佐、三田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

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。委員等からの意見は以下のとおり。

●今年度の実証のイメージについて

・　商用ソフトウェアの場合は作成した SBOM をサプライチェーンに沿って横流しすると考えている。しかし、資料に記載しているように開発委託元を完全に信用するのは難しい。そのため、資料3の P.20 に記載の「独立に検査」における監査方法も検討いただきたい。

・　ツールによるSBOM精査・活用を検討するためには、SBOMを活用するユーザの意見も必要ではないか。エンドユーザ（企業の情報システム部等）がSBOMを管理・メンテの役割を担うため、エンドユーザの考えを考慮する必要がある。

・　サプライチェーンの階層が深い場合、OS・ライブラリ・ファームウェアなどの細かい部品を中小企業が利用するケースがある。その中では、SBOMを構築しない海外部品を利用するケースもあり、中小企業が全ての責任を負うのは難しいと考えている。

・　責任問題については、国際ルールに従うことが望ましい。入れ子構造においては、全体を見渡すのは難しい。開発委託元がリスクを検討して、開発委託先がリスクに関する情報をSBOMで提出するという構造ができるとよい。責任の

限定や保険などの損失分担についても今後検討する必要がある。また、ソフトウェアが含まれている製品においては、製品基準でソフトウェアについても対応できるとよい。また、監査についても、コストが効率化できるようにSBOM判定できる第三者を仲裁契約等で活用できるとよい。

・ ソフトウェア分野の実証に関連して、修正版のコミットなど、OSS文化との関わりについて日本独自となっている部分がある。独自にフォークしたバージョンでの SBOM の扱いや、製品としてのトランスペアレンシーの確保など、SBOMの利用方法や考え方にも影響を与えるかもしれない。日本特有の考え方や姿が国内だけで通じる SBOM とならないよう、そういった問題についても実証等で明らかにしていけるとよい。

・ ISOでセルフアテステーションができる認証の仕組みがある。NISTのガイドラインに従う場合は、検討いただきたい。

・ 多層関係でSBOMをやり取りする場合は、SBOM自身の整合性や発行者の署名などの改ざんの有無を確認する体制が必要である。また、SBOMが一般ユーザに開示されることで知り得なかった情報がオープンになることが予想される。そのため、最終ベンダの対応量が増えると考えられる。最終ベンダが責任を持つうえで、ユーザ側においても、対処が必要・不必要な脆弱性の判断や OSS のリスクや脆弱性の取扱いなどの知識や認識が必要である。

・ 直接利用部品においても、サブパッケージ・サブサブパッケージなどの2次・3次利用部品が存在する。これらをどのように整理するかも検討いただきたい。また、複数の企業間でSBOMを作成する際に、パッケージの名称やバージョンの付け方に表記ゆれについても検討いただきたい。

・ SPDX、SPDX-lite で内容の粒度が大きく違う。CVSSとの比較を行うと、SPDX-lite では影響が大きな脆弱性が含まれている。医療分野は、CVSSのスコアを重要視している。出力フォーマットによって相互運用性が変わると考えている。実証では、フォーマットごとの特徴も踏まえていただきたい。

・ 脆弱性特定については、ツール利用・手動のどちらの想定か。また、それに関するドキュメントをまとめる予定はあるか。CVSSについても、環境によるスコアの揺れや脆弱性の中間的なデータベースについて検討が必要と考える。

・ 実証の成果から、SBOM に限らず、脆弱性対策のための国内の基盤・仕組みについて、あるべき姿、あるとよい姿について言及できるとよい。SBOM に関連する部分が機械処理できたとしても、機械処理が一部だけに留まるとなかなか普及しない。

・ 米国での大統領令をもとに SBOM を想定したセッティングを取り込んだソフトウェア等を展開し始めるところが出てくることが予想され、セルフアテステーションなどの要素も重要になると思われる。米国企業の中には早期に日本企業のソリューションの中に組み合わせる形で展開する製品サービスも出てくると思われるが、早い段階で情報を共有しながら、今後の進め方を協議していきたい。

・ 自動車メーカーによる契約の違いもあるが、制御と情報分野で大きな違いがあると考えている。ナビシステム等の情報系か制御系システムかによって大きく違いがあるため、意識していただきたい。

●ノウハウ集、活用モデル、取引モデルのイメージについて

- SBOMの例・SBOM導入に関して典型例を具体的な内容も含めて記載いただけるとよい。1から実施する企業に向けて参考になる資料にしていただきたい。

- 医療業界・自動車業界・ソフトウェア業界で実証を行う中で、取引のしきたりが違うと考えている。取引形態によって責任関係を明確にできるとよい。

- SBOMの目的も含めてSBOMを説明できるとよい。また、契約・サプライチェーンの透明化、脆弱性管理やコスト・リソース削減におけるSBOMのメリットも記載いただけるとよい。特に契約面においては、SBOMの公表がデメリットにつながると考えている企業も存在する。中小企業含め、これらの企業にも考慮いただけるとよい。既存のシステムに追加する方法も紹介できるとよい。

- ドキュメントの題名を考えていただきたい。ユーザに読んでいただける題目・表紙にできるとよい。

- ソフトウェアの商流の国際ルールに沿って検討を進めていただきたい。実例等のサンプル・責任関係等を集めて公開いただけるとよい。SBOM によって取引の手間がかかるという前提があるが、各企業においてサイバーセキュリティは経営課題として捉えるだけでなく、経営の一部として捉えているケースが増えてきた。SBOMも引き続き進めていただきたい。

以上