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6回）議事要旨

1. 日時・場所

日時：2022年3月3日（木）11:00～12:45

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、
関委員、高田委員、髙橋委員、寺田委員、野山委員、萩原委員、平田委員、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、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 江口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、石垣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。

●来年度以降の取組の方向性について

- SBOM が社会で機能を発揮するには、時間軸、産官学、個々のユーザー、ベンダー、事業の受益者がなすべきことの整理、SBOM 実装を支える人材の育成強化、社会制度との連携等、様々な課題を克服する必要があり、今の取組はその出発点である。SBOM によってリスク分析の基礎情報が共有され、リスクコミュニケーションが可能になり、サプライチェーンのリスクを統制できるようになることを踏まえれば、我々は、経済安全保障を含む我が国のセキュリティ政策全般を支える重要不可欠なインフラ構築を論じていることを自覚すべきと考える。よって、今後の我が国のセキュリティ政策全般を進めるための根拠として、3～5 年で SBOM の社会実装に必要な具体的な目標を「旗」として立て、それに見合う予算を獲得し、誰の、何のために、どのような人材で、どのような社会制度と関連付けて行くのか目的を明確にし、現実的に推進していただきたい。また、対象範囲とその根拠等も現実の分析を踏まえた意思決定が必要。浸透方法も様々な手法が考えられるため、どこを目指すか明示いただけるとよい。国際競争上も重要であり、日本が優位をとれるよう進められるとよい。

- 業界毎にローカライゼーションするのではなく、全体として「旗」を立てる方向が望ましい。

- SBOM の運用に関し、ライセンスを確認するのは主に製品リリース前・開発中と考えられ、委託先と SBOM をやり取りしながらメーカが最終確認するような運用イメージである。製品リリース後、脆弱性有無を正確に確認するためには、

SBOM が最新であること（プログラム更新と同期）と、SBOM と突合する脆弱性情報（VEX など）が最新であることが条件と考えられ、脆弱性をリアルタイムで確認するために必要な情報の管理方法や体制についても議論する必要。

- SBOM の必要性について、脆弱性やライセンスコンプライアンス等、負の側面の担保のほか、開発生産性の向上や脆弱性に関する問合せ対応の短縮化のような正のメリットも共有して普及を進められるとよい。

- 先行する米国等における権利関係の工夫、著作権法や企業秘密などをクリアする方法についても調査いただきたい。

- これまで各自が取り扱ってきた課題をソフトウェアの透明化で解決できることが、SBOM の基本概念であることを示していけるとよい。

●中小企業等への普及について
- 中小企業への浸透についても今後検討していく必要があり、実証にも協力したい。来年度以降の対象の選定にあたって、中小のソフトウェアベンダーにも参加いただき、事例を作成できると良いのではないか。

- 中小企業の状況も考慮したうえで、SBOM の活用モデルの構築やノウハウ共有を行っていただきたい。特に SBOM 作成ツールに関するノウハウが重要である。

- 今後 SBOM は必須になると考えているので、必要性をより強く示していただきたい。Log4j の脆弱性等では依存関係の情報を含む SBOM が必要になる一方で、中小企業では SBOM を手動で構築する労力を確保できないため、自動で確認できるツール等が必要。ツール利用に関する施策を、ナレッジを共有しスピーディに進められるとよい。「旗」を振る際も、中小企業を含めて実施いただけるとよい。

- 中小のソフトウェア事業者における SBOM の認識状況やセキュリティ意識なども調査していただきたい。OSS を利用する危険性の認識度合いを確認できると次の取組も考えられる。

●SBOM に必要な要素等について
- どのような粒度で SBOM を作るべきかが重要。

- 標準的なフォーマットの検討も重要。活用モデルと合わせて検討されると理解。

- SBOM が改ざんされていないことを示す電子署名が必要ではないか。

●SBOM ツールや自動化について
- 資料で紹介された Log4j のような脆弱性も検出される必要。有償ツールを利用して厳格に管理している場合は、再帰的に Log4j を使っているケースも含めて迅速に脆弱性を特定でき、SBOM の効果を感じた。

- 脆弱性のレポジトリとの連携も重要。脆弱性対策情報データベース JVN iPedia と SBOM における製品との対応付けについては従来から取り組んでおり、現状、DB に登録されているソフトウェアには製品 ID が振られているが、DB に登録されていない場合は製品 ID が無いことが課題。経済産業省とも別途相談して、検討状況を報告したい。

・ ツールによって検出精度に差があるため、どのようなツールでどこまで対応していれば自分に非が無いか、免責について具体的に記載されているガイドラインがあるとよい。

・ Cyclone DX のプロジェクトにおいて、脆弱性の発動条件を示す VEX というフォーマットが提唱されており、脆弱性の発生を点ではなく範囲で確認可能。VEX の活用による脆弱性確認の自動化の方向性も検討する必要。

・ 元々ライセンス管理をしていた IT 資産管理ツールベンダーが、脆弱性管理やセキュリティへも対応し始めているため協力できるとよい。

・ ライセンス購入以外にマネージドサービスとしてスポット利用可能なツールも作成されてきている。

・ 米国ではツールによる自動化の議論が進んでいるため、国際的な平仄を合わせておくとよい。

●OSS の管理等について

・ OSS のディストリビューターとの連携も重要。

・ 2022 年 1 月にホワイトハウスが OSS コミュニティや関連企業を集めて OSS を守るための会議を実施している。日本でも同様の取組を実施できるとよい。

・ OSS を有償で構築している人も多く、米国では OSS に対するファンドについても議論されている。また、Linux Foundation が実施したアンケートでは、8 割以上が米国大統領令に向けて体制を構築していると回答。Log4j の影響もあり、各企業はフォーマットの統一化や SBOM の普及を米国政府に求めている。

・ Linux Foundation が 2022 年 2 月に SBOM は必須となったとのアナウンスを出している。

・ OSS を作る側だけでなく、利用者側の義務も重要。ソフトウェア開発においても、プロジェクトマネジメント義務に関しユーザーの義務が理解される傾向にある。ユーザー側が実施すべき項目もあることを考慮いただきたい。

●人材育成について

・ 無償の SBOM ツールである Syft を利用した際、バージョン情報の結果が様々であり、最終的に手動で判断する必要があった。官民だけでなく、アカデミーを利用し人材育成を含むエコシステムを構築できるとよい。

・ SBOM は、中長期的にはソフトウェア技術者のコンピテンシーの問題。この問題を解決しない限り後追い対策になってしまう。ソフトウェア技術者に認識いただくためにも、IPA の情報処理技術者試験等に組み込めるとよい。

・ SBOM に関わる者の意識は、時間をかけて形成する必要があり、研究機関や高度教育機関の役割が重要。大学等におけるセキュリティの基礎教育や研究の体制に SBOM を組み込むよう文部科学省へも働きかけていただきたい。

●政府機関等における取組について

・ サイバーセキュリティ政策に関する日米の政府間対話でも、本内容について意見交換できるとよい。

- 情報セキュリティ早期警戒パートナシップで届けられたソフトウェアの脆弱性を JPCERT/CC が確認し、各ソフトウェアベンダーへ連絡する取組においても SBOM が活用できるのではないか。

- デジタル庁が実証候補に含まれていないが、影響力の大きいチャレンジは国で実施すべきではないか。

以上