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5回）議事要旨

1. 日時・場所

日時：2021年10月29日（金）10:30～12:20

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、猪俣委員、大場委員（代理：遠藤様）、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、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、
入江サイバーセキュリティ課長補佐

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。

●SBOM の効果・コストについて

- SBOM 活用のメリットについて、一社に対して効果がある部分、複数社が連携して取り組むことにより効果が上がる部分、官民連携で効果が上がる部分を分析できると良い。

- コンポーネントの把握、対応スピード、効率性の 3 つの観点での向上が見込まれ、OSS を含めて SBOM を活用した構成管理が一般的となる可能性。実証で国内の開発に関し構成管理を含めたものへのレディネスをどう作るか、というところが見えてくると良い。

- コストに関する課題については、規模によるスケーラビリティの方向性が示せると良い。命名規則については何らかの形で統一されることが望まれる。OSS のコミュニティがなくなっているケースなど、長期間修正されないマイナーな脆弱性が存在し、アプリケーションの脆弱性対応度が 100%とならないケースも存在する。

- どれほどのシステム規模であれば SBOM の効果があるかを示せると良い。大規模システムであれば直感的に効果があることが分かるが、SBOM が効果を発揮するシステム規模の境目があるだろう。

●コストや責任の分担について

- サプライチェーン全体としてメリットがあることを示し、コストをどのように分配するかを考えると良い。

・ 脆弱性管理のメリットを分析するにあたって、保守契約がどうなっているのか、曖昧であればどのような解決方法が考えられるかを検討するのが良いのではないか。また、個社が SBOM に関する情報を出せないという問題もある。契約の問題を打破しないと SBOM 活用には結びつかないので、実証で検討いただけると良い。

・ 将来的には、OSS にも SBOM が付属され、製品メーカーはその OSS のコンポーネント解析を実施せず、自身の SBOM と組み合わせて提供できる形が理想。ただし、コミュニティに責任を問わない形で、いかに OSS の SBOM を信頼するかは議論の対象。

・ 最終製品ベンダーが解析を実施する場合、OSS コミュニティが SBOM を提出しても活用されない可能性。ソフトウェアと SBOM の品質保証を一体で考え、ソフトウェアベンダーの責任が問われない場合はその SBOM の責任も問われないなどの仕組みが望まれる。SBOM 生成に係る受発注者間の責任分担のパターンを検討できると良い。

●SBOM に関するノウハウの共有について

・ コストや効果の計測だけでなく、SBOM 利用の際の手間やノウハウも記録し、報告書で記載されると良い。また、SBOM に含まれるソフトウェアコンポーネントの名称や情報が一致しない場合、手動と自動を組み合わせたハイブリッドのケースが多いと考えている。そのようなケースにおける効果やノウハウを可視化できると良い。

・ 今回の実証と並行して、開発者が実際に試せるプラクティス集をオープンソースで公開、共有する等も大切な視点であるし、望まれる進め方の一つ。こうした開発者自らが手を動かせる点についても検討を進めることは、できることからはじめるという観点でも、日本での開発者の態勢の構築していく観点でも重要な課題。

・ 以前同様の実証を行った際、既存の資産管理ツールを使っていることが多く、SBOM ツールを活用する際にシステムやデータの移行をどのように実施するかが難しかったため、何らかの指針があると良い。

●SBOM のツールについて

・ SBOM 活用はツールに依存する部分が大きく、ツール自体の信用性や確からしさを示せると良い。SBOM の活用を促進するという観点では、ツールも OSS であると普及が促進するのではないか。

・ SBOM 実証に関して、ソフトウェア管理に関する取組は進みつつある。実証において、自動化前提で進めないとサプライチェーンの末端の企業は対応が困難。自動化ツールを予算の範囲で試していただきたい。

・ IPA の JVN を改修し、SWID タグ、SPDX、CycloneDX など、ソフトウェアの識別子を登録するデータベースの整備について検討が行われている。脆弱性情報と脅威情報を一緒に送れるよう、フォーマット変換も検討中。ソフトウェアの識別子を使い、ツールベンダーに資産管理だけでなく脆弱性管理をしてほしい。ソフトウェアの識別子の管理課題などで連携できると良い。

・ ツール間の互換性がなく、相互運用する際に、異なるツールを用いることが難しい。

●SBOM のフォーマット・管理項目・粒度について

・ 脆弱性管理において、どの程度の粒度の SBOM であれば効果を得られるか実証で確認できると良い。

・ 運用管理側と開発側で求める SBOM の粒度は異なると考えており、いかに整合性を取っていくかを実証の中で確認できると良い。

・ SBOM の必要な項目とそうでない項目を分類できると良い。また、サプライチェーンの上流と下流で活用する項目や、共有する必要がない項目が分かると良い。実証の結果として不要な項目が明らかになれば、導入の障壁が下がるのではないか。SBOM 生成に関する標準をある程度決めていく必要。

・ SPDX と OpenChain は、Fast-track procedure を活用して標準化され、コミュニティで活発な改定作業が進められている。代表して動向をウォッチする取組があると良い。また、実証において課題が出てきたとき、OpenChain や Linux Foundation のボード企業から実証へのフィードバックが得られるよう、情報共有の仕組みがあると良い。

・ Excel でもあっても管理できるよう、最低限の情報を含む SPDX Lite を開発し、結果的には国際標準に組み込まれる形に。普及活動における連携が考えられる。

・ SPDX の ISO/IEC 標準は完全翻訳の JIS があると良い。

●産業界における既存の取組について
・ 国内企業でも既に SBOM を導入している企業にヒアリングしながら、包括的な課題抽出をした方が良い。

・ どの程度の企業が構成管理を実施しているのか、各構成管理ツールの販売実績を確認することも一案。

●政府機関での SBOM 活用について
・ 実証に関して、政府機関で活用することも一案。その後、政府統一基準に SBOM の要件を入れ込むことを検討できると良い。現状は曖昧な部分が多いため、実証を通じて具体化することがまず必要。

●その他
・ 現状でもソフトウェアの構成管理を独自に実施しているが、SBOM を利用した場合にどのようになるかは非常に興味深い。OSS を活用することでアップデートが頻繁になるほか、構成が複雑になる中で、いかに工数を削減するかが課題。グローバルの規定が厳しくなる中で、事業者の体力を奪うことがない施策になると良い。

・ 防衛産業では、業務発注に関わるすべてを監査するという形で進めているが、民間と齟齬をきたさないように進める必要があり、経済産業省においても、検討の範疇に入れる必要があると考えている。

・ 米国では、自動化が進まないと SBOM 導入が進まないというのが産業側のコンセンサス。既存のコミュニティベースでコンセンサスを醸成しつつ標準を開発することに加え、ユーザーによって SBOM の使い方は変わってくるため、様々なパターンを考えていかなければならない。日米間の情報共有ができると良い。

・ 日米協力について、NTIA のほか、CISA や NIST など複数の組織との関係構築を目指すのが良い。

・ 脆弱性情報は日々変わっており、ベンダー自身が情報を探して活用することは難しく、OSS コミュニティとのコネクションが重要。いかに連携していくかが課題か。

以上