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8回）議事要旨

1. 日時・場所

日時：2022年11月28日（月）13:00～15:00

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、
鈴木委員、関委員、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、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 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

資料4 JVNiPedia_MyJVN 機能拡張について

資料5 製品識別子を用いた脆弱性対策情報データベースと資産管理との連携に関する検討

4. 議事内容

事務局から、資料3に基づき説明、渡辺委員及び寺田委員からそれぞれ資料4及び資料5に基づき説明いただいた後、自由討議を行った。委員からの意見は以下のとおり。

● SBOM と脆弱性情報等との関連について

- 製品識別子は、セキュリティに限らず、SBOM 利活用における共通課題である。世界を巻き込んだデファクトの製品識別子が必要だと考えている。OSS は、問題意識を持つ人々を巻き込んで大きな活動にしていく必要がある。OpenChain や OpenSSF などの OSS 関連団体を巻き込みながら普及できるとよい。

- ソフトウェアの名寄せはセキュリティ面からも、ライセンス面からも長年の課題と認識しており、非常によい取組である。

- 近年は、ISO の規格よりデファクトが強くなる傾向がある。寺田委員の活動の普及を進めていただくのも一手と考える。

- 脆弱性情報をエンドユーザーは製品単位で参照・認識するため、製品を特定するための識別子が重要。開発側は部品単位で脆弱性を管理しなければならないため、識別子で部品が特定できる必要がある。開発者やサプライチェーンに求められる体系とエンドユーザーに求められる体系には相違があり、開発者やサプライチェーンとエンドユーザーでユースケースが分かれると考えている。

・ SBOM を浸透していく上では、部品表をチェックする制度が必要ではないか。制度がない場合は、適当な部品表が生成される可能性がある。また、海外連携も重要だと考えている。加えて、システム開発の面では、中小企業が所属しているIT 団体連盟を巻き込む必要があると考える。

・ ソフトウェアの ID を解決するのは難しさについては他の SBOM の WG でも議論されており、明確な解は出てきていない。CISA から、ID のコンバージョンによる解決方針についての文書が公開される予定であり、検討を進めているところ、連携できるとよい。

・ 世界的に統一できるのが理想だが、難しいのであれば、日本独自で ID を吸収する組織を構築し、展開できるとよい。また、マッチングの命名規則が構築された場合においても、各企業内の命名規則との整合性が必要である。社内のアプリケーションを自動収集する仕組みが必要となる。既存のアプリケーションでも解決は可能だが、コストが高く、大手でないと対応が難しい。また、情報の粒度も重要となる。IT 管理部門では、細かな内容は不要だが、開発部門は細かい情報が必要であり、どうハンドリングしていくかが課題。SBOM と脆弱性情報をマッチングするマニュアルやオープンソースのツールが提供されることが、ユーザ組織としては望ましいと考える。

・ SBOM のメリットである脆弱性対応に関しては、日常的な業務ではない。そのため、資産管理などの日常的な業務とSBOM を連携できるとよい。

● SBOM 実証の課題等について

① VEX 等について

・ SBOMと脆弱性のマッチに関して、製品識別子の重要性は理解した。SBOMから得られた脆弱性リストへの対応に関する議論が足りていないと感じる。例えば脆弱性診断ツールでは必要以上の脆弱性情報が出力されることが多いため、対処すべき重要な部分のみを絞り込まなければいけないという状況と似ている。製品開発において問題が発生する部品・ライブラリや関数を呼び出していない場合など、部品の脆弱性が製品に影響を及ぼさない場合もある。そのため、SBOM から発見された脆弱性に対して、VEX を利用して絞る必要がある。ベンダが VEX を提供するのが理想だが、セキュリティ研究者などの第三者機関における提供も検討すべきだと考えている。メーカー・SIer においては、一般ユーザに部品単位の脆弱性のアラートが開示された際に、製品への影響の問合せを多く受けて窓口が飽和することが懸念される。そのため、VEX 含めて製品への影響有無情報と、脆弱性がどのように悪用されうるかユーザへの影響、メーカーがどのような工程でアップデートを提供するのかといった、脆弱性対処方法に関する一般への啓蒙が必要と考えている。

・ ツールの整備を懸念している。Log4j に関する調査では、有償ツールが高く、無償ツールを利用して確認を行った。無償ツールは専門的すぎるため、各部署に対応いただくのが難しかった。VEX などの出力結果がわかりやすい形式できるとよい。中小や企業ではない団体を考慮したツールごとのユースケースの整理も検討できるとよい。

・ 先日 CISA から発表された TRANSFORMING THE VULNERABILITY MANAGEMENT LANDSCAPE において、SBOM、VEX、SSVC のような情報が提示された。SSVC 使用の検討も重要と考えている。

② ノウハウ集等について

・ 実証を踏まえてノウハウ集や取引モデルをまとめることを検討しているが、サプライチェーンが多様化しているなか、誰にとっても理解しやすい文書を作成することが大事な目的だと考えている。

・ 立場によって SBOM のメリットに相違があると考えている。そのため、関係者の立場ごとのメリットを示せるとよい。

③ SBOM のインセンティブ、コスト等について

・ SBOM を使う意義を浸透させることが重要。開発元・提供元が実施する必要があることも理解されている一方で、中小ベンダからすれば、インセンティブや費用が伴わないと、促進するのは難しい。SBOM の本格化に向けて関係機関の事業の精査も検討できるとよい。

・ 実施すべき取組であることは認識しているが、実施する上での資金フローについて今後検討する必要がある。時系列含めて資金や取組にどのように国が関わるかについて検討する必要がある。

・ 今後、自動化の取組も必要ななか、コスト的に継続できるかは、米国内でも検討していると考えている。日本・米国間でもコストに関する情報共有を行う必要がある。

・ 米国 OMB の覚書に対して、技術的な課題が多く、運用ができないという意見がある。どのくらいの資金で各課題に対応していくかを検討する必要がある。米国においても同様の検討が進められている。また、Log4j の反省から、OSS のトップレベル階層でのリスク管理の限界について CSRB のレポートでも課題提起されている。例えば、OSS のコンポーネントも入れ子で管理できるようになるとよい。

以上