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9回）議事要旨

1. 日時・場所

日時：2023年2月28日（火）14:00～16:00

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、高田委員、髙橋委員、野山委員、萩原委員、松岡委員、渡辺委員

オブザーバ：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

参考資料 SBOM（Software Bill of Materials）の導入に関する手引（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。委員からの意見は以下のとおり。

●SBOM の導入手引案について

・ 本手引案は、従来のドキュメントと比較して読みやすく事業会社向けの啓発にも利用できると考えている。今後も継続的に SBOM の啓発を実施いただけるとよい。経営者向けのメッセージに関して、医療や自動車における規制や制度について追記いただきたい。また、脆弱性管理のメリットの記載について現場は苦労しているため、定量的な費用効果がより重要と考える。

・ 既知の脆弱性が残存している場合は、製品回収の可能性がある点についても記載いただけるとよい。

・ 本手引案は、開発者向けであるが、一般の人への普及にも利用できるとよい。SBOM と脆弱性情報データベースとを突合した結果、確認できる大量の脆弱性について、全て対応する必要はなく、優先度をつけて対応することが重要。このような脆弱性対応に関しても、一般の人に分かりやすく説明できるとよい。また、経営者向けメッセージの中には、効率化だけでなく、今まで発見できなかった脆弱性を管理できるという要素も加えていただけるとよい。

・ 米国の SBOM においても透明性や自動化は重要な要素として捉えられている。そのため、透明性や自動化についても記載いただくとよい。

- SBOM により今まで発見されなかった脆弱性が確認できるようになる可能性が高い。今まで確認できなかった脆弱性が多く発見された場合は、逆に対応工数が増加する可能性があることを懸念している。このような点についても解決する必要性があることを背景で触れていただけるとよい。また、本手引案に SBOM の導入に向けた 6 つの実施項目が記載されているが、初めて実施する人にとってわかりやすい記載方式に変更できるとよい。また、実施項目をベースに SBOM 導入の適用範囲を整理すると認識しているが、これらの整理イメージがあるとよい。

- 脆弱性に優先度を設定して対応することを導入ガイダンスに記載すると、理解できない人が出てくると考えている。そのため、記載すべき内容と記載すべきではない内容があると考えている。

- SBOM の作成に当たり、情報の収集が難しい部品があると考えている。そのため、もし、SBOM がそのままサプライチェーンの下流のユーザに提供される場合には、脆弱性が見えない構成要素が含まれる可能性があるところ、それに関連した記載を追記してはどうか。また、本手引案については、ソフトウェアサプライヤーにおける設計・開発部門や製品セキュリティ担当部門（PSIRT 等）を主な対象としているが、経営者向けのメッセージが記載されている。経営者も一部読者対象であることを考慮した構成としてはどうか。

- 効果を金額で記載すると情報が一人歩きする可能性がある。今回は、工数の視点でまとめられ、金額と比較してよい指標だと考えている。分野毎のノウハウなどを取りまとめると事業者は利用しやすいと考えている。

- SBOM を利用することで脆弱性対応において不足していた箇所を確認できると考えている。そのため、経営者にとっては、人月は重要な指標だと考えている。本来は、ビジネスインパクトなどによってリスク分析を行い、スコープを明確にして対応すべき脆弱性を検討できるとよい。これらの検討に際して、事業者による効率的なソフトウェアの選定方法に関するベストプラクティスを作成できるとよい。サイバーハイジーンの一環として、経営者はコストをかけたくないため、効果を確認できるとよい。

- 本手引案のような文書を早い段階で公開していくことが重要。公表後の事業者の様子を確認しつつ、更なる普及・促進策を検討できるとよい。また、SBOM は、サプライチェーンセキュリティ全体で責任を持つ社会構造を前提にしているため、肌身の感覚で SBOM を語る文書があるとよいのではないか。

- ソフトウェアにおいては、SIer と開発主体の企業に分かれると考えている。今回の経営者は両方を検討していると認識しているが、SIer と開発主体の企業では、メッセージが異なる。そのため、今後は企業形態によってメッセージを書き分けることや普及のプランを検討する際に検討方針を分けた方がよいと考えている。

- SBOM はサプライチェーン全体で実施する必要があると考えている。そのため、本手引が公表されることで、取引先と一定のコンセンサスを得ることができる。また、サプライチェーンセキュリティについて、様々な活動を経済産業省が実施しており、その活動によって、サプライチェーンセキュリティを事業者でも検討しやすくなったと思われる。SBOM についても、サプライチェーンセキュリティの一部として引き続き普及いただきたい。

- ソフトウェア・サプライチェーンは、成熟されておらず、取引先含めて意識が高まっている途中だと考えている。事例や実証から得られた情報を整理して、長めの時間軸で検討すべき内容である。SBOM は部品表であり、単体で社会的な機能を生み出せず、SBOM を活用することが重要であるが、社会全体としては SBOM が普及していない。そのため、SBOM を利用して実現したい社会像を示した上で、SBOM の普及・実装を支えるための官民学の連携イメージ

を旗揚げて示していただきたい。また、SBOM ツールを利用する前提で内容が記載されているが、実際には外部サービスに委託するケースが多いと考えている。そのため、外部サービスを含めて体制を育て上げる必要がある。

・ SBOMを作成することが目的だと誤解されないかを懸念している。SBOM 作成後の対応が難しいことが普及の妨げにならないためにも、SBOM の作成がゴールではないというイメージを伝えることが重要である。また、アップデートを含めた SBOM の継続利用によって SBOM のメリットが大きくなるという観点も経営層に伝えられるとよい。

●対応モデル・取引モデルの要点について

・ ライセンス違反が発生するタイミングとして、開発前ではなく、出荷前に確認できれば問題ないという理解でよいか。また、中小企業が SBOM ツールを購入することは難しく、発注元がツールを提供するケースもあると考えている。そのような場合の契約・取引モデルを検討できるとよい。

・ 作成前・作成後・出荷準備・出荷などの段階があり、市場に出すということを顧客の手元に届くことを想定した場合には少し遅いと考えている。相手に渡す直前の段階で差し止めをする権利がある。

・ 多重構造になっている内部のソフトウェアがライセンス違反である場合、最終的に製品を市場に出す会社が責任を持つと理解している。そのため、市場に出す前に確認する必要があるのではないか。

・ 企業で SBOM を運用するうえで、2 点の課題がある。1 つ目が、ソフトウェアの開発委託における SBOM の開発・運用工数の見積り方法である。2 つ目が、SBOM 管理する企業内の組織である。これらの課題がある中で、見積モデルや組織モデルに関する事例集をガイダンスに関連付ける形式で作成できるとよいのでないか。

・ サプライチェーンでは、事業者が多岐にわたるため、小規模の事業者に負担とならないようにしつつ、また、実現性を高めるためにも、負担の押し付け合いにならないようなモデルの検討が必要と考える。確保する方法を検討するのは難しいが、完璧な状態を求めるのではなく、できるところから実施するという発想が重要。

・ 開発委託先が基本的に弱い立場になるので、SBOM に関する運用が契約期間外においても求められる可能性がある。このような状況を回避できるような契約書のサンプルの作成を検討できるとよい。

・ 米国では、産業界と米国政府間で SBOM の議論が行われている。例えば、VEX の試行環境を提供している事業者もいる。現状ある自動化ツールだけでは、SBOM 社会を構築することができない。サプライチェーン上の全ての企業が SBOM を構築できるには自動化が足りない状況である。日米含め世界的にも取組が進められており、取引モデルを検討する際には、技術的な進展も確認いただきたい。また、SBOM 実装が負担になりすぎないという安心感を事業者に与えるうえでも、日米の産業側においても自動化に関する技術書等を構築できるとよい。

・ SBOM を取引する上で、契約書に取り込むべき内容は多いが、内容としては一般的なソフトウェアの契約書と相違がないと考えている。ソフトウェアの契約の一部として SBOM を取り込むことが重要。ソフトウェアの契約内容とは別に SBOM で特別必要な条項があれば、ガイダンスに明記いただきたい。自動車の分野では OEM がトップにいるサプライチェーン構造のため、中間の企業が SBOM を作成する形式になると考えられるが、これまでも利用 OSS リストの作成などを実施することがあったため、SBOM 導入への違和感はないのではないか。

- 脆弱性管理においては、EOL、EOS に関する課題を考慮する必要がある。事例を作成する際に、EOL や EOS をどのように記載するかを懸念している。SBOM の利用期限も含めて今後検討する必要があると考えている。

- EOL、EOS に関する対応は、SBOM 固有の問題ではなく、ソフトウェア全体の問題であるため、ソフトウェア対応の一部として位置づけられるとよい。また、ソフトウェア開発において SBOM の作成が当然と認識されるようになることが重要。中小企業を補助するとしたら、契約においてSBOMの保守料などを得られるような取引形態を構築できるとよい。

- SPDX などが ISO 化されている中、その他の規格を利用する可能性もある。今後、OSS コミュニティの動向を注視して進めるとともに、可能であれば、OSS コミュニティに参画して情報交換を実施し、要望を出すことも検討できるとよい。

- 取引モデルの意義と位置づけについて、SBOM を提出するだけでなく、ソフトウェアの管理に SBOM を活用することの合意も取れるとよい。中小企業が個別にSBOMを作成するのは難しいため、ISAC 等の枠組みなどで、支援する仕組みが必要である。日本として、SBOMをどのように活用したいかについて示していけるとよい。

- 能力がない事業者に対して SBOM を求めた際に、不均衡な社会にならない仕組みづくりが重要である。サプライチェーン全体で責任を持つという文化を形成し、社会的なシステムとして非競争分野については情報を共有する必要がある。

- 中小企業に限らず、不均衡を是正するための仕組みや支援が必要である。また、利用者側が SBOM を発注要件に含めるためにどのような働きかけが必要かについても今後検討できるとよい。

以上