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11回）議事概要

1. 日時・場所

日時：2023年10月31日（火）15:00～17:00

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、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、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

事務局：　経済産業省 商務情報政策局 上村サイバーセキュリティ・情報化審議官、
山田サイバーセキュリティ課企画官、味木サイバーセキュリティ課補佐、
飯塚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 デジタル庁における Trustworthy なサービス実現のための取り組み

4. 議事内容

事務局から、資料 3 に基づき説明、デジタル庁から資料 4 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。

<u>デジタル庁の取り組みについて</u>

- 先月開催された Open Source Summit Europe では、EU のパブリックセクターが OSS を活用している中で、OSS の利用持続性含めたサステナビリティが重要視されているため、そのような視点でも検討いただけるとよい。
- SBOM が生成されていない OSS を利用することになった場合、SBOM を生成する必要があると考えている。生成後の SBOM についても共有の仕組み等を検討いただけるとよい。
- 取り組まれている活動内容については、対外的に発信いただけるとよい。他の自治体や団体などにも参考になると考える。
- SBOM を社会基盤化できるとよいと考えているが、資金な流れや費用負担について検討する必要があると考える。責任については、レガシーな対応のみではスピードが間に合わないと考える。そのような視点も考慮に入れながら検討できるとよい。
- SBOM が公開されていない OSS を利用する場合、その SBOM の構築は、コストが大幅にかかるため、課題になると考える。
- 内製でソフトウェアを開発している中、開発者がいなくなると維持管理が難しくなると考える。内製開発における維持管理の観点から解決に向けて工夫いただけるとよい。

SBOM 実証の今後の方向性について

- 中小企業では、情報システムが一人しかいないことや IT 知見を持つ人材がいないケースも想定されるため、SBOM の脆弱性対応の自動化ツール含めて中小企業向けの施策も検討いただけるとよい。
- SBOM の自動化においては、有償・無償ツールを組み合わせて安価に精度を上げる方針も検討いただけるとよい。
- 実現性のあるツール関連施策が SBOM 普及には重要であると考える。中小企業向けに無償ツールや企業が利用可能な標準的なツールのモデル等検討いただけるとよい。SBOM は、部品は特定するが、全ての脆弱性を特定できるわけではないと考えるため、脆弱性対応を軸として、SBOM がカバーできる脆弱性の範囲、カバーできない脆弱性の範囲について示すことを検討できるとよい。
- SBOM 作成側と利用側で実施すべき内容が変わると考える。特に SBOM 利用者の手間がかからない手法を検討できるとよい。SBOM 利用者のなかには対応の体制が構築できず、既存の脆弱性のパッチを適用する程度の実施内容の企業も多いと考えるため、組織規模や能力に応じて閾値を決めることも重要と考える。中小企業の観点からも、SBOM 利用者の負担が少なくなることが望ましいと考えるので、その点も考慮いただけるとよい。
- 現場としては、SBOM を作成し、脆弱性と突合する必要があるが、現状、誤検知・過検知が多いと考える。それを解決する手法についても検討いただけるとよい。
- 検討内容については、参考にできる内容のため、文書等でまとめ、整理いただくとよい。対象ソフトウェアについて、今後はより一般化して検討できるとよいと考える。
- CISA から「Software Identification Ecosystem Option Analysis」文書が公表されており、ソフトウェア ID の統一性がない問題等に言及がなされている。自動化等はこのような動向を検討しながら考える必要がある。
- 部品 ID の生成については、例えば、PC やクラウドであれば資産管理団体からインベントリデータをもらい、そこから部品 ID を生成し共用する案もあると考える。また、OSS については関連組織・団体と協力し、部品 ID を作成し共用する、あるいは提供を受ける案もあると考える。そのような視点も考慮しながら検討できるとよい。
- 脆弱性の優先付け判断ツリーは、ユーザ側の視点が強く表れると考える。一方、業界によっては、知見がないユーザの場合、ベンダー側の意思が入ってしまうことで、対応優先度が想定より高いものになることが多いため、配慮が必要であると考える。

SBOM 取引モデルと成果物の活用の今後の方向性について

- SBOM 導入のメリットとしてライセンス管理や脆弱性対応等があるが、加えて、ユーザ・SIer の視点では、業界標準として利用されている ISMS 等に SBOM 要件が含まれるとよいのではないか。また、構成管理において、含めたくない部品が入っていないことを確認できるという点もメリットになると考えている。取引モデルにおける契約の規定事項については、具体的に運用・保守サービスの項目に含まれる範囲との線引きについても検討できるとよい。例えば、現実的に問い合わせ対応の一部として、契約額などが動かない範囲で、脆弱性が公開された時の突合作業を実施する必要があるかなどが挙げられる。
- 取引モデルにおける契約の規定事項については、開発・保守が別の会社に委託されるケースがあるため、企業が変わった場合の対応も規定事項の一部として検討できるとよい。
- EU の Cyber Resilience Act の中で PSIRT を構築することが求められているが、取引モデルにおける契約の規定事項のなかでも言及できるとよいのではないか。
- 取引モデルにおける契約の規定事項において、レベルを基礎と発展の違いと根拠を明確化できるとよい。特に、再帰的利用・直接利用などの部品範囲や免責については、基礎になる可能性もあると考える。提供者の負担を下げるという点も流通上重要であるので検討いただけるとよい。

- 取引モデルは、非常によく全体を網羅しているが、契約書において紛議が起きた場合について、SBOM が正しいかを確認する作業と紛議を解決するための仕組みが重要であると考える。契約後の紛議など含めて仕組みを検討いただけるとよい。金銭、責任、紛議にかかる時間について、現場は問題視しているので、検討いただけるとよい。
- 成果物の活用については、各業界に任せればうまくいく内容ではないと考えるため、経済産業省や関係団体等含め、今後連携しながら進められるとよい。継続的に SBOM や ID などのソフトウェアを管理する組織が必要だと考える。そのような点も考慮し、検討できるとよい。民間で実施すること、政府として対応することなど整理しながら、考慮して検討いただけるとよい。
- 各組織・団体から発信される脅威情報、インシデント情報、アセットマネジメント等の情報について、自動化を行うようなフレームワーク、およびそれらの情報と脆弱性との対応付け、ならびに活用方法については、将来の課題として考慮できるよい。
- 規制については、業界水準とかけはなれた案に対して反発が起こるケースを散見している。SBOM に関する規制を考える場合、業界水準の観点も視野に入れながら、取り組んでいくことが重要であると考える。
- 米国では、SBOM はすぐに実施できるものではない部分や、業界で受け止めきれない部分もあると考えるため、そのような動向も注視しながら、今後検討できるとよい。

以上