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10回）議事要旨

1. 日時・場所

日時：2023年7月18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、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、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

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 武尾サイバーセキュリティ課長、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、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

参考資料1 「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引（案）」に対する意見募集で寄せられた御意見に対する考え方

参考資料2 ソフトウェア管理に向けた 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 の導入手引案に関するパブリックコメント対応結果について

- パブコメ対応結果の通り、SBOM が部品表としてライブラリ管理や機械学習における学習モデルの管理などに利用されることも期待されている。CycloneDX においては、ML-BOM や SaaSBOM の取組が紹介されており、今後、SBOM 以外の BOM についても必要に応じて追記し、手引案が示している SBOM の対象を明確化できるとよい。
- 手引案については、今後も必要に応じて定期的にパブリックコメントを実施し、内容を更新していくとよい。

●対応モデル案について

- 対応モデル案については、SBOM の管理単位や更新のタイミングを検討できるとよい。ソフトウェアの多くは階層化されているため、ソフトウェア内で複数の SBOM を 1 ファイルとしてまとめずに管理することが想定され、SBOM の内容が更新されるたびに差し替えを行う必要があると考える。そのため、製品全体の SBOM を最新化する方法についてもモデルとして可視化できるとよい。

- SBOM 対応モデル案を利用することで、SBOM の対応状況が可視化されると考える。一方、IoT 機器等の組み込み機器の利用が多い制御分野や重要インフラ分野等の特定分野については可視化が難しい事例が存在すると考える。例えば、約 5 年前に公表された WPA2関連の脆弱性のケースについては、特に制御分野において、契約状況によっては脆弱性対応が実施されない事例等が確認された。

- CSSC において議論されたビル分野の事例では、個人事業主が利用する Windows95 が多く残存している状況にあるが、制御分野は事業を停止することができないため、迅速な脆弱性対応が難しい事例が存在する。

- これらの事例を踏まえると、特定分野については、SBOM 対応状況の可視化が難しい側面があると考える。加えて、情報管理の観点から、可視化された情報に関する取扱いには、分野毎に配慮が必要である。

- SBOM の導入手引案で記載の VEX の他に、大統領令を基に CISA・NIST が脆弱性開示プログラムである VDR について公表している。自動化が難しい箇所においては、VDR の利用も考えられるため、検討いただけるとよい。米国を含め、現状では自動化に向けた技術発展途上であるため、SBOM の活用を完全の自動化には時間がかかると考える。それまでの対応として、既存技術も組み合わせながら SBOM の対応方法を検討する必要がある。

- 日本国内で SBOM の利用を促進する方策について、検討できるとよい。例えば、政府統一基準等含め、政府調達に関して SBOM を利用することなども検討できるとよいのではないか。また、ソフトウェアを調達している SIer にどう浸透させるとよいか、インセンティブとペナルティの両面が検討できるとよい。

- SBOM 利用のインセンティブを検討することが重要であるが、そのためには、米国等の政府調達要件の事例を参考に検討するとよい。特に、ヘルスケアや自動車等の分野では、規制を基に SBOM の活用が広まり、米国では政府が SBOM の導入を求めたことで、事業者への普及が進んでいる状況があるため、そのような事例を参考に検討できるとよい。

- 製品ベンダーによって脆弱性の対応に違いがある状況においては、SBOM や VEX によって対応の違いが可視化されると考える。例えば、SBOM や VEX と、NVD や JVN に登録されている脆弱性を対応づけすることを想定した場合、製品ベンダーは全ての脆弱性を NVD や JVN に登録せず、独自のリリースノートなどで対応している場合もあるため、今後、全ての脆弱性を登録し SBOM で完結する方針なのか、独自のリリースノートなども対応として許容するのかなどを検討する必要がある。

- ソフトウェアベンダー等のソフトウェア開発事業者だけでなく、システムを構築する事業者に対しても啓発が必要である。そのような事業者は、外部のソフトウェア等を利用して構築することが多く、SBOM の活用を理解する必要があると考える。また、SBOM は脆弱性管理だけでなく、ソフトウェア構成管理という点でも重要であり、両面の観点から SBOM 利用に関して検討できるとよい。

- SaaSBOM がクラウドの BOM として検討されており、BOM という広い枠組みにおいては、SBOM 含め利用すべき BOM の検討が必要である。

- RSA カンファレンスや SBOM-a-Rama 等において、日本の規制状況について関心が寄せられているため、規制化を検討する場合には、SBOM 対応モデル案を利用し、現実的なレベルに調整できるとよい。米国は、脆弱性が NVD へ

登録されていない場合、CPE が割り当てられないという状況について課題認識し、解決するための方針を検討している。

・ ソフトウェアのパッケージ運用・管理が SBOM の活用においても課題だと考える。製品としてのソフトウェアを Windows やクラウド環境で利用する場合、Linux 系と同じくパッケージ管理されたソフトウェアをインストールするというアプローチの普及がポイントになると考える。さらに、システムインテグレーションで開発した場合にも、同様な取り扱いができるようにするため、パッケージ管理をどうするべきか等を含めた運用管理の観点からも検討できるとよい。

・ 製品ベンダーからの情報発信と JVN 等の公的な DB からの情報発信の役割を分けて考えた方が良い。理想は、製品ベンダーからの情報発信のみでしかも自動化前提であるが、現実的に難しい。民間ではなかなか対応できない領域は常に存在するので、その領域を公的な DB が部分的にでも代行し対応できるとよいと考える。例えば、影響の大きい、あるいは、良く利用されているソフトウェアについては、自動化を含めた詳細な情報発信を先導するというのは、その一例になると考える。

・ 海外の SBOM 活用アプローチについて、ヘルスケアや自動車等の規制がかけられている分野で求められる対応を整理できるとよい。日本の JVN の取組は NVD を参考に同様の仕組みを構築している。SBOM 活用についても米国と日本で強制力の差はあっても、分野毎の規制の状況はあまり変わらないことから、米国の規制の対応状況を整理できると、同様の仕組みを構築している JVN の取組に順次取り込みつつ、連携することもできるのではないか。

・ 対応モデル案の普及の観点では、制度全体の方針を誰が決め、責任をもって推進するかという点について検討するよい。制度というのは、SBOM や脆弱性情報の活用・共有における全体の仕組みを示しており、責任というのは、他者から侵されないという権利と資金を示していると考える。米国では、大統領令を基に実施しているが、日本においてはどの機関が責任を持って実施するかが重要である。また、機能や要件を設定する責任を明確にし、責任を担う場合は何を実施する必要があるかを検討する必要がある。さらに、各プレイヤーの責任に関する点についても検討できるとよいのではないか。利用者が複数の開発者から SBOM を納品し、利用者が SBOM を利用する際にミスが発覚した場合どう対応するか等含め検討する必要がある。また、SBOM の免責についても検討する必要がある。完璧な制度は難しいが、完璧ではない部分の責任をどうするかなどを検討する必要がある。購入者が求められる脆弱性強度との対応の責任を誰が持つかなども重要と考える。

・ 利用者が複数開発社から SBOM を納品する場合、複数事業者分の責任を商品に重ねることになるため、コストは増加すると考える。このため、社会インフラとして運用できるコスト負担の仕組みを検討することが重要である。今後、実際に制度を動かす上で、責任・免責の範囲、コストの問題、制度の強制・任意を検討することが重要である。

・ SBOM は脆弱性管理で利用したいというのが主目的の1つであると考える。脆弱性修正やパッチ適用の時間を減らせることが大きなメリットと考える。これらのメリットを享受する上で、機械処理できないことが 1 つの課題と考える。そのため、国や政府において、SBOM に関して誰が先頭に立ち、予算や責任を持って実施するかは、明確にすることが重要である。

●今年度の実証方針等について

・ 今年度の実証項目として、責任や費用の観点からも検討するとよい。

・ SBOM の対応ツールついては、複数のツールで検証することも検討できるとよいのではないか。

・ SBOM の脆弱性管理において、NVD とのマッチングにより脆弱性が発見された場合、脆弱性の発動の有無を検討する必要がある。その場合、NVD や JVN の突合のタイミングの検討が必要だと考える。NVDやJVN等のデータベースが更新されるなか、どの程度の頻度で突合を行い、どのデータベースにアクセスすればよいかなどを検討するとよい。ゼロデイ脆弱性や実証コードがない脆弱性においては脆弱性の発動の判断が難しい場合がある。このような場合は、脆弱性の識別者によって誤差が出る可能性があるため、SBOM の品質に影響があると考える。つまり、コンポーネントの脆弱性をどの程度の頻度でどのデータベースを参照すればよいのかという点と、コンポーネントの脆弱性の発動有無をどの材料をもって判断するかという点を確認することが重要であると考える。

・ SBOM の構成に変更がない状況であっても、特定のコンポーネントの呼び出し方次第で脆弱性の発動は変わると考える。そのため、製品ベンダー側がVEXについては作成する必要があると考える。また、VEXには実証コードが含まれていない場合、VEXを公開してもよいかという点について検討できるとよいのではないか。ユーザにとって VEX は有用であるが、悪用可能と判断された場合 VEX を限りなく早く提供する必要があると考える。また、現状の VEX のステータスの種類では、製品ベンダーにおける製品の優先順位や脆弱性対応の優先順位が表面化される。そのため、ベンダーに対しても VEX の活用方法については啓蒙・普及や手引が必要であると考える。

・ 情報共有のフェーズで、契約書の作成・構築・条項モデルについて実証項目として追記するとよい。

・ ユーザ企業が、サプライヤーや最終ベンダーから調達・SBOM を納品する場合、規制等によってユーザ企業側から要求が行くことも多いため、そのような観点でも実証項目を検討するとよい。

・ SBOM について、中小企業を含む多くの企業が活用できる状態を醸成することが重要である。一方、脆弱性管理プロセスを体力がない中小企業がすべて実施するのは難しいと考えるため、プロセスごとに、最低限、どこまで実施をするのがよいかのレベル分けを明示することを検討できるとよいのではないか。

・ 脆弱性管理プロセスにおける情報共有フェーズについて、サプライヤーに修正を要請する場合は、他の開発者の製品も同様の部品を利用し、同様の脆弱性の影響を受ける場合があるため、パートナーシップの活用を含めて検討できるとよい。

・ 脆弱性管理プロセスにおける暫定対処や本格対応のフェーズにおいて、ユーザに周知、提供をする方法として、パートナーシップの活用を含めて検討できるとよい。

●QUAD における共同原則等を踏まえ今後取り組むべき事項

・ 本タスクフォースで議論されている SBOM の内容と QUAD の枠組みの関係性を整理できるとよい。また、QUAD と同様に EU のサイバーレジリエンス法も規制の一種であるため、それも含めて本タスクフォースの参考にするとよい。

・ QUAD において SSDF と類似の内容が記載されているが、日本での対応を検討する際には、SSDF を参考にしながら方針を検討していくのがよいのではないか。

- QUAD の対象として、クラウドの SaaS におけるソフトウェアも含まれると考えられる。SaaS 事業者への影響度は、ISMAP 制度との整合性や SaaS 事業者の体力も考慮する必要がある。既に SaaS 事業者は数百項目のチェックリストに回答しなければならない状況があるため、SaaS 事業者への影響について検討できるとよい。

- QUAD に対しては、本タスクフォースの内容や成果を打ち込むことを検討するとよい。

以上