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12回）議事要旨

1. 日時・場所

日時：2024年2月28日（水）10:00～12:00

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、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、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 通信分野における SBOM の導入に向けた検討について

参考資料 ソフトウェア管理に向けた SBOM の導入に関する手引 Ver2.0（案）

4. 議事内容

事務局から、資料 3 に基づき説明、総務省から資料 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。

総務省の取り組みについて

- 今後、総務省と経産省で連携を行い、様々なツールを試行、検討いただけるとよい。また今後は、SPDX 3.0 についても話題になることが考えられる中、他の SBOM フォーマットである Cyclone DX 等も考慮し、この点においても総務省と経産省で連携した上で、今後検討を進めて頂けるとよい。
- 通信機器は総務省などのように、各省が個別に SBOM に関する検討が進められると考えている。業種共通の内容と業種個別の内容を区別し、検討いただけるとよい。
- 省庁間で縦割りにせず、一般的な内容については共通的に検討いただき、個別の業界事情のみを各省で検討いただけるとよい。
- システムの全体構成としては、ハードウェアとソフトウェアが混合したシステムになると考えている。同じ型番ハードウェアでもファームウェア構成が異なるケースや、ハードウェア構成と同等のソフトウェアアプライアンスを構成する場合など、製品としての SBOM のみでなくネットワーク構成上における製品利用に関する SBOM も必要だと考えている。

今後の普及展開策

- 保険会社においてサイバー保険を提供しているケースがあるが、SBOM の提供が保険金額の検討の要素になるとよい。
- 構成管理を実施するうえで、SBOM が求められるようになると考える。供給側による構成管理を促進するためには、ユーザ側で構成管理表の納品など供給側に要求することが重要である。そのために、関連団体と議論し、検討できるとよい。
- SBOM に関連して、民間主導のコンソーシアムも設立されはじめており、昨年経産省が公表した SBOM 導入手引も活用しながら、SBOM 作成者だけでなく、SBOM 利用者の目線も含めて SBOM に関して議論しているような状況もあると認識している。検討中の SBOM 導入手引 Ver2.0(案)では幅広い内容が含まれ、充実しているが、特に SBOM 実証で示されているコストについては、より多くの事業者が SBOM を利用するためにも、幅広く実証結果を展開する必要があると考える。
- 複数のコミュニティで出ている意見であるが、今後の普及展開のためには、SBOM を含め、セキュリティ担当者だけでなく経営層へのメッセージも必要だと考える。
- 経営層へのメッセージは有効であると考える。ソフトウェアの業界団体のなかで、SBOM を理解して運用しているケースは一部の企業にとどまっている状況と認識しており、投資を行う判断を行うのは経営層であることから、経営層へのメッセージは重要だと考える。SBOM 含めて、経営層のサイバーセキュリティへの意識を向上させるためには、レギュレーションやインセンティブとの関連付けが必要だと考える。
- 日本においては、技術に詳しい人が経営層になる場合が少ない。この考えを変える取組が日本においても必要だと考える。
- CIO、CISO は取締役ではなく執行役員であるため、このようなDXやセキュリティを担当できるような人を経営層に加えるという国策が必要であると考える。
- システム構築事業者やソフトウェア開発事業者への普及も重要である。IT に関係する団体のなかには中小含めたソフトウェアハウスが集まっているようなものもあるが、セキュリティのアンケートに対して返答がない企業が多かった状況もあると理解している。そのような関連団体と協力して、実態を把握しながら中小含めた事業者を巻き込みつつ、SBOM の普及を進める必要があると考える。さらに、他の関連団体等も巻き込みながら検討できるとよい。
- SBOM を社会インフラとする上で、SBOM 生成側の敷居を低くすることが望ましいと考える。SBOM 生成は利用者のニーズによって工夫する必要があると考える。そのためには、SBOM 生成・共有のフローを実施した上で、対応モデル含めた議論をすることが重要だと考える。このような内容を手解きできるガイダンスが必要だと考える。また、SBOM を流通させるうえで、SBOM の再利用が重要だと考える。国策ではなく、民間・コミュニティが実施する内容かもしれないが、SBOM 共有プラットフォームが必要であると考える。
- 本タスクフォースやコンソーシアム等で SBOM を検討しているところであるが、SBOM を理解できていないという意見も多い状況と考える。このような状況の中、今後、業界団体等の会員向けにアンケートを実施する際には、SBOM への意識が低い企業に対してヒアリングを行う必要があると考える。なぜ SBOM が浸透しないかを確認し、中小企業への支援等のアプローチを含め、今後の政策を検討できるとよい。
- 過去にソフトウェア関連の団体が実施したアンケートでは、SBOM を生成している企業は多くなかったと記憶している。今後、そのような業界団体と経産省で連携し、普及を進めていけるとよい。
- 2023 年の秋から米国の FDA におけるソフトウェアの市販前認証が更新され、SBOM の提出が求められていると理解している。そのなかでは、全てのソフトウェアが対象であり、米国で重要になってきていると認識している。特に、各メーカーにおいてリスクベースで SBOM を記載することが求められていることに苦労している状況があり、また、全てのソフトウェアが対象であることから、バイナリも対象に含まれている状況であると考える。バイナリについてはツールでスキャンすることが難しいため、現状は様々な手段でバイナリを解析化した上で、管理のみをツールで実施することが求められている状況であると考える。米国の FDA は人命を預かる機器を取り扱っているため、要求レベルが高い

傾向にあると考える。関連して、SBOM 導入手引においては、どこまでを SBOM で管理すべきかの追記、直接利用・関節利用している OSS までを含めるなど敷居を低くするような文言の追加などを検討できるとよい。加えて、環境に応じて構築が求められる SBOM を紹介するなどの導入のハードルを下げるドキュメントが必要だと考える。

- 米国の FDA の要求レベルのハードルについては下げるのが困難と考えられるため、米国の特性上準拠していただく必要があると考える。また、フリーの OSS は著作物の可能性がある場合もあるので、表現には注意が必要であると考える。
- EU の CRA では、OSS を商用利用する組織が SBOM の責任を持つことが述べられていると理解している。
- そのことについては、ISO と同様の切り分けなので問題ないと考える。
- 施策を進めるにあたって、国内ベンダーに向けたワークショップを経産省もしくは業界団体が主催して開催できるとよい。ワークショップを実施することで、SBOM の啓発やベース基準の向上に繋がると考える。例えば、政府主催の会議体で実施するのも 1 つのアイデアだと考える。

<u>SBOM導入手引 Ver.2.0（案）について</u>

- フェーズ 2 の脆弱性対応優先付けが重要だと考える。優先付け情報の選択・取得における「インシデントの有無」や「Exploit コードの流通状況」を取得するのは難しいこともあるので、CISA の KEV を利用することなど記載を検討いただくとよい。SSVC の記載においても、FIRST の EPSS を利用して脆弱性対応を減らしていく内容を追記するよう検討頂けるとよい。
- SBOM 対応モデルの分野として、ソフトウェア・自動車・医療機器の 3 つを記載していると理解している。ソフトウェア分野は全ての分野に該当するため、ソフトウェア製品などの文言に変更頂くことを検討するとよい。
- SBOM 導入手引 2.0(案)は、網羅的な文書であると考えているが、エントリーユーザーに必要な最低限の情報のみをまとめた文章も必要だと考える。また、ツールの一覧を手引きに記載しているが、それらのツールを対象に各フェーズで利用できるツールを整理できるとよい。
- 経産省と総務省の検討結果はお互いに連携しながら、SBOM 提供者の立場と SBOM 利用者の立場の意見を明確に区別して整理できるとよい。SBOM 提供側は手引全体について確認する必要がある。一方で、SBOM 利用者側は一部のみが対象であると考える。別冊として、初歩から学ぶ SBOM という観点で、利用者側の敷居を下げるような文書を提供できるとよい。

<u>政府調達基準への SBOM 記載案について</u>

- 現場が適切に対応できるよう、ベースとなる基準はしっかり記載いただけるとよい。
- サプライチェーンという用語が抽象的だと考える。自動車や医療では、サプライチェーンの階層が深い中で、どの階層の SBOM が構築されるかが分かりづらいと考える。SBOM が完全ではない中、「既知の未知」や「未知の未知」への対応という点で、契約不適合責任の状況が分からないことを懸念されるため、このような観点からも明確化を検討するとよい。
- EU の CRA や米国の大統領令では、機械可読形式で SBOM を提出することやリスク分析実施した上で SBOM を生成・提出することが求められ、具体的な SBOM の目的が確認できると考える。それを踏まえて、目的の明確化や具体的な基準を検討頂けるとよい。
- SBOM への対応を要件化すると海外製品が優位になってしまうという懸念が考えられるため、国内ベンダーにおいても SBOM 利活用を促進することを検討できるとよい。また、SBOM を受け取った側もどう使うのか、具体的に明確にした方がよい。部品管理を適切に実施すれば、海外製品が出てきたとしても統制につながると考える。
- 米国の FDA の SBOM 要件化については、米国企業からも抵抗感があり、どう対処するかが難しい状況であると考える。日本でビジネスをしている米国企業も対象に含めながら、施策を検討いただけるとよい。また、各省庁とも整合性を取りながら、ハードルを上げ過ぎず実効性を担保できるよう、フィージビリティがあるレベルから検討頂けるとよい。

以上