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4回）議事要旨

1. 日時・場所

日時：2021年1月13日（水）16:00～18:00

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、
関委員、高田委員、髙橋委員、寺田委員、野山委員、萩原委員、平田委員、松岡委員、渡辺委員

損害保険ジャパン株式会社：小中様

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

経済産業省：大臣官房 江口サイバーセキュリティ・情報化審議官、
商務情報政策局 奥家サイバーセキュリティ課長、鴨田サイバーセキュリティ技術戦略企画調査官

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 損保ジャパンにおけるOSS利活用及び管理手法について

4. 議事内容

事務局から資料3に基づき説明し、損害保険ジャパン株式会社 小中様から資料4に基づき説明いただいた後、自由討議を行った。委員等からの意見は以下のとおり。

●OSS管理手法に関する事例集について

事例集は企業にとって有用。現在は大手の事例が中心。今後は中小事業者や、これから立ち上がるであろうIoT系やスタートアップなどの規模の大きくない会社などにも使いやすくなるように、事例集の拡充を期待。OSSの利用に関するメリットやデメリットを含めた基本的な考え方や、これから始める人が陥りやすいことについての記載があるとよい。

●SBOM活用促進に向けた実証事業について

＜SBOM導入に向けた課題について＞

SBOMそのものがビジネス戦略になる中で、ソフトウェアの構成内容について見せることができるものとそうでないものがあると想定。その中でうまくフォーマットを統一化して活用できるようなガイドラインを目指すことが望ましい。

サプライチェーンの中で、最終製品メーカはサプライヤ側からするとSBOMの内容を教えたくない相手になる。サプライヤをどう巻き込み、どう課題解決したら良いかがまだ見えていない。

SBOM による管理を行うにあたり、開発ベンダーや機器ベンダーを選定する際の要件は契約で決めることになるはずであり、契約条項をどう書くかとそれをどう遵守するかが重要。

SBOMは作るだけでなく運用が必要であり中小企業がどこまでできるかが課題。開発現場ではリポジトリから勝手に引っ張ってくることがよくあり、将来的には国として信頼できるリポジトリの整備等の議論も必要ではないか。

自分たちで作るプログラムを含めて一覧化できたり、どのアプリ・機能がどのモジュールを使っているかまで把握できると、脆弱性等の影響範囲の特定にも役立つため開発エンジニアにとってもメリットになる。皆にメリットがあることが重要。

SBOM 活用について、脆弱性を誰が見つけて対処するか、プレーヤー間でシェアできないとメリットを享受できない。メリットをより享受できるモデルの検証が重要。また、SBOM の管理自動化は必須技術であり、ターゲットに合わせた技術検証が必要。大規模な IoT システムではクラウドネイティブな技術を使う検討も進んでおり、短期間のアップデート、継続的なインテグレーションとデリバリーが前提。PoC は適用技術も見極めながら進める必要がある。

＜ツールの活用について＞
ツールを用いてSBOMを作成する場合、検出精度や誤検出の問題がある。人の判断が介在する運用例を聞いたことがある一方、ツールを信じるという判断もある。ツールを信じる場合、ツールの妥当性については、製品選定の時点で精度が高いものを選ぶことで担保することになる。ツール選定にあたっては、ユーザビリティや言語特性なども考慮するとよい。

中小企業においても SBOM 利活用のためには自動生成など何らかのツールは必要不可欠と考えるが、中小企業を対象に PoC を行うのであればツールありきにしない方がよい。中小企業の場合、SBOM の粒度が浅いレベルでも、製品に含まれる脆弱性を確認できる場面があるはず。NTIA でも、悪用可能な脆弱性に絞り込んで対応した方がよいとの議論もある。また、すべてツール任せとなった場合、ブラックボックス化しツールに依存してしまうリスクを懸念。

ツールに頼るのはよくないというのも一つの見方だが、Exploit コードが公開される場所は限られており、ツール側でも速やかに対応できている。米国は比較的ツールが進んでいる印象。

脆弱性情報を整理する際、アプリ名称だけでもかなりの数がありマッチングがうまくいかない。脆弱性情報や各社で管理しているアプリの名称の付け方の違いが原因であり、名称の問題の解決が重要。また、ツールは安価でないと困るケースもある。

＜SBOM の POC を実施するべき分野について＞
SBOM の実証は反復的に継続して行えることが重要。日本固有であるから合わせられないところ、合わせる必要のないものを分けることを目的の一つとして、事業者の団体や ISAC などとも相談をしつつ、例えば、NTIA の取り組みでも議論や取り組みが先行しているような分野などを視野に入れるなど、できるところから PoC をやっていくのがよいと考える。

特定の業種を対象として、複数組織にまたがって PoC ができるとよい。横断的な取組みの場合には製品識別が必要となるが、そこを検証すべき。JVN の製品識別情報を使った脆弱性情報と資産情報との連携について実証実験が行われているので、うまくつなげられると良い。

産業分野によってはJavaのような広く活用されている言語を使うので対応しやすい業種もあるが、あまり知られていない言語を使うこともあると思われ、そういった分野でSBOMが作れるのか懸念はある。

SBOMにより自らの知識を共有することが、ある意味で企業の競争力の妨げになるという意見もある。そうでない分野として、中小のSIer、ノウハウが関係ない人、Webデザイナー、ネットワーク構築系等のコミュニティでSBOMを使っていくとよいと思う。

サプライチェーンのつながりを考えるときに、自組織で開発する場合と、外部調達する場合では、SBOMでできることに違いがでてくるため整理が必要。アプリとインフラのようなソフトウェア種別で考えた場合、インフラはソフトウェアをそのまま使用・管理するのでメリットは少ないが、アプリはソフトウェアの部品構成をカスタマイズする可能性が高いのでSBOMを適用するメリットがある。他方、製品ベンダーは脆弱性対策のために製品の中で何のソフトウェアを使っているのか等を把握しなければならないという状況。様々な視点から整理しないと議論のレベルが揃わないと思慮。

SBOMは大企業を中心とするサプライチェーンを狙う方がよいかもしれないが、サプライチェーンが長くても、お互いに注意し合えばよく、本当に危ないのは小さなIoTデバイスを作っている中小企業だろう。

＜PoCの実施向けて留意すべき事項＞
SBOMのデメリットの議論も重要。SBOMを利用するときに発生するセキュリティ上の問題について検証してはどうか。SBOMは必ずしもオープンに使われるものではなくクローズドでの利用もあり、OSSだからオープンで良いとも限らない。社内のみ、サプライチェーン内、業界内等の範囲限定で扱う場合の問題も考えてはどうか。

実証事業に関して3点、検証事項として追加してほしい。一つ目は、管理対象の特性（技術的な特性、管理するシステム、パッケージの特性、言語やパッケージ管理の有無など）も踏まえた分析が必要。二つ目にSBOMの管理単位の検証も必要。言語特性上、知的財産管理の面で、脆弱性管理より細かい単位でライセンスが分かれている場合に、どのように脆弱性を紐づけるか明確にできるとよい。三つ目は、運用・更新まで含めたコスト検証。開発中、リリース前・後で、コンポーネントのバージョンアップ等により中身が入れ替わる可能性があり、メンテナンスにもコストがかかる。

事務局にてタスクフォースでの議論をまとめたうえで、SBOM活用促進に向けて検証すべき事項等について検討を進め、次回タスクフォースにて提示することとした。

以上

お問合せ先
商務情報政策局　サイバーセキュリティ課
電話：03-3501-1253