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1回）議事要旨

1. 日時・場所

日時：令和元年9月5日（木） 10時00分～12時00分

場所：経済産業省　本館17階第一共用会議室

2. 出席者

委員　　：　土居委員（座長）、明石委員、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、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、防衛装備庁

経済産業省：　大臣官房サイバーセキュリティ・情報化審議官　三角審議官、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課企画官

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　本タスクフォースの議事運営について（案）

資料4　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

4. 議事内容

事務局から、資料3,4を用いて本タスクフォース（TF）の議事運営及び検討の方向性を説明した後、自由討議を行った。委員からの意見は以下のとおり。

●SBOM 等のソフトウェア管理について

- OSS は、バージョンが変わったタイミングでライセンスが変わってしまうようなケースもあるため、自社のシステムや製品のライフサイクルではなく、OSS 側のライフサイクルに合わせて SBOM 等のメンテナンスや更新が必要。

- SBOM を日本に導入する際は、発生し得る日本固有の問題を先回りして洗い出すことも重要。

- SBOM の必要性は理解するが、中小のソフトウェア開発ではリソースがないので、リソース面には配慮が必要。

- 脅威情報やそれが攻撃に使われた場合のリスクについては、攻撃に実装コードが存在するのか、攻撃が実際に行われたことがあるのか、対策情報が利用可能かといった情報を SBOM 等から参照できれば対策を考えやすい。

- GitHub 等、ソースのリポジトリを管理するシステムでは、そのプラグインやアプリケーションの形でソースの脆弱性チェック等を行うツールが出ている。SBOM 等もそういうリポジトリの中である程度自動生成できれば普及するのでは。

・ 脆弱性が存在しても、研究環境でしか再現しない場合や、ある製品ではその脆弱性に関する機能を使っていない場合など、脆弱性が発動しないケースもあるので、対応不要と判断するケースもある。ただ、SBOM 等で優劣なく全ての脆弱性が列挙されると、一般の方からは、あの製品にはこれだけ脆弱性を残っている、と見える可能性もある点は心配。

・ 脆弱性対応で、CSIRT 等の情報システム部がまず必要とする情報は、ソフトウェア名やバージョン情報など。しかし、実際にそれに対処する場合には、どの関数が使われているか、どういう条件があるか等、より詳細な情報がないとパッチが適用できない。また、パッチの適用にはテストが必要なので、テスト環境をいかに整えるかも大きな問題。

・ JVN を作ったのが 2004 年で、2008 年ぐらいから NIST のマシンリーダブル(機械処理)化にあわせて JVN のマシンリーダブル化に取り組んでいる。登録する製品名の揺らぎの問題についてはまだ解決できていないが、SWID を用いることで揺らぎの解消と共に資産管理と連携できないかを考えている。今は別々に提供される脆弱性関連情報と脅威情報を、なるべく同じ形式で同じデータフローを使って受け取れるように紐づけていきたい。

・ SBOM は最先端の話題で、アメリカでも議論の最中。NTIA が主宰する会議では、議論が白熱して、徹底してやるような方向性になっている。ただ、徹底的にやり過ぎると、製品が作れないのではないかという懸念もある。

●OSS について

・ OSS の開発は、開発者とユーザの利益を折衷させることが非常に大事。ユーザが使いやすくすると開発者に過剰な負担を強いることになり、開発者が自由にやりすぎるとユーザが後ろで負担しなければいけない。その折衷が重要。

・ OSS のプロジェクトは、品質の評価がされておらず将来も約束されていない。良い OSS だと思って使っていても更新が止まってしまう。そうなると、自分でメンテナンスをするしかないので、継続性の問題が大きい。

・ OSS やレポジトリそのものが、そもそも信頼できるかという話がある。また、そこの認証についても、そもそも信用できるのかという大前提がある。開発環境自体が汚染されているという話もあるので、環境がそもそも安全なのかも重要。

・ OSS のサポートは止まる場合がある。Linux Foundation の開発者にファンドするプロジェクトのように、日本として大事なソフトウェアに対しては、戦略的に開発者を抱え込む仕組みを作ることは大事。

・ 最近では専用機器が汎用機器とOSSの組み合わせに置き換わってきているが、利用中の OSS に何かあった場合でも、重要インフラのサービスは継続する必要があるので、OSS コミュニティの対応を待てないケースが多い。そのため、OSS をサポートする専用の技術者を自社で抱え、何かあったときには、最悪、自分たちでも対応できるようにしている。

・ ユーザがOSSに求めるのは、セキュリティパッチがきちんと出て、ユーザがその情報を正しく入手できること。SBOM等があれば、社内のデータベースとマッチングできるため、パッチ情報等の収集ではなく判断に時間をかけられる。

●ソフトウェア開発について

・ ソフトウェア開発モデルに関して、以前は、上流工程から下流工程までウォータフォールモデル的に開発してきたが、最近は、アジャイル的に、非常に短期間でソフトウェアを開発している。以前はバージョンが枝番で綺麗に幹の様に

管理できていたが、最近は少し修正しただけで全く別の機能になってしまうので、バージョン管理が難しくなっている。

- 中間ベンダになると、製品の販売先に対して責任を追うことになるが、製品を構成している部品が別の会社の製品だったりオープンソースだったりすると、範囲を特定した上で、そちら側に責任の一部を振るなど、色々と調整が必要。その重層構造をどのように解くか等を含めて、管理は大変。

- メーカにはソフトウェアに対する責任が当然ある。細かくモジュールや脆弱性を管理することも重要だが、最終的な製品として脆弱性がどうなのかをメーカは担保しなければいけない。

- ベンダが製品として出す場合と、ユーザが自分たちのシステムでOSSを使う場合で、意味合いが違ってくる。まとめて議論をすると混乱するので、これらは分けて考えるべき。

- ソフトウェアのサプライチェーンという観点では、大手企業が中小のソフトウェア企業と取引するときに、中小のソフトウェア企業が全ての品質責任を負うのは非現実的。SBOM等によって一部の責任を発注元に委ねる発想も大事。

●TF の方向性について

- ソフトウェア管理手法のガイドラインのようなものが作れると活動としてはベストだと思うが、なかなか大変なので、まずは SBOM の活用事例集等を作ることができれば非常に有益なのではないか。

- ソフトウェアでは、開発、導入、運用という段階ごとにそれを担う主体が異なるが、攻撃者はそのどこからでも攻撃してくるので、複数の主体が情報を交換し、連携して対応できるような総合的な枠組みも必要。

- OSS 推進フォーラムでは、オープンソースの利活用事例の企業間での情報交換をやっている。ただ、技術面は良いが、ソフトウェア管理やライセンス関係の話になると、デリケートなので難しい面がある。ベストプラクティス等の情報交換は徐々に始まっているが。この TF でそうした活動が加速することを期待している。

- OSS を使っていたとしても重要インフラは止める訳にはいかない。10 年、20 年走っているものがある。なかなか悩ましい面があるが、何もしないという訳にはいかないので、知恵を出しあって活用できればいい。

- SBOM 等の管理手法には賛成だが、ベースとなるものが汚染されていたら意味がないので、参加する人も含め、どのようなプラットフォームを作るかの議論になるのではないか。管理手法だけでなく社会システムまで考えるべき。

- OSS のサポートにおいては、OSS コミュニティの在り方が重要なので、コミュニティに対して、リスクがどういうもので、問題が起きたときにどうすれば良いかなどを議論できると事業者としてはありがたい。また、ソフトウェアによっては関連する OSS コミュニティが複数あるケースもあるので、これらをどうウォッチするか等も議論できるといい。

- 中小のソフトウェア開発者は、ソフトウェアや OSS に関する問題を認識しても、コストをかけて対処するのが難しい。TF を通じて活用事例等がそういう方々に届けばいい。

- お互いのベストプラクティスの共有は是非やりたい。ただ、個人的には自社のためだけではなく、日本のため、お客

様のためにやっていきたいが、会社を動かすには、具体的なメリットも考えながら活動する必要がある。

・ セキュリティは個社の問題であると同時に社会の課題。何をやるべきかという議論と同時に、誰が、どのようにして、それを実現するのかという具体的な議論をしなければならない。

・ ISO27002がベストプラクティス集になっており、これによって情報セキュリティマネジメントとして何をやれば良いかがわかってきた。本TFでも何らかのベストプラクティス集を作るのは有益であろう。

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