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3回）議事概要

1. 日時・場所

日時：令和元年12月4日（水） 16時00分～18時00分

場所：経済産業省　別館9階別館944共用会議室

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(代理：遠藤様)、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、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　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　OpenChain ProjectにおけるOSSのTransparency向上への取組

4. 議事内容

事務局から、資料3に基づき説明、遠藤委員から、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。

●OSSとライセンス/品質等に係る責任主体について

OSSをどう使うかというのは、企業単位というよりは、プロジェクト単位で選択することが多い。一方で、使っていいOSSかどうか、事前に法務チェックを実施して内部共有している会社もある。ライセンスについても、プロジェクト単位ではなく、企業の法務としてどう見るかという形でのプラクティスを推進出来ればよいのではないか。

かつてOSSは、ソースコードを読める人、ビルド環境を持っている人が使うもので、力量のある人同士で協力してやっていたように思う。ところが、昨今はバイナリだけで配布されるようになったり、コンテナや仮想イメージ、設定情報までセットになっていたりして、一行のコマンドで実行することができてしまう。非常に便利になっている反面、ライセンス等が識別しにくくなっている。

マネタイズや、コミュニティを支えるのは難しい。バグバウンティやハッキングコンテストみたいなもので、OSSを作る人たちにお金やリソース面で協力できるようなやり方をもっと広めてはどうか。また、OSSのライセンスについて皆に理解してもらうには、OSS絡みで大きな判決が下った、損害が出たというようなケースがあれば、そういうことを紹介し、OSSライセンスに関して啓蒙していくようなことを続けてはどうか。

OSSを利用する場合、その品質やライセンス条件を正確に理解した上で利用する必要があるが、なかなかそれがうまくいかず問題が生じている。こうしたベンダ等が共通して抱えている問題や作業を分散して対応していると無駄が多いので、それらを一元的にやる一つの拠点、責任の主体のようなものを作ったらどうか。例えば情報センターみたいなものがあれば、OSSを使ってみたらOSS同士のライセンスが競合していたという話がなくなるのではないか。

SIerとしては、ディストリビュータにリスクの転嫁をしており、これをそういう主体として考えることは出来るのではないか。具体的にはLinux系だとRed HatやOracleが挙げられるが、そういうところが品質やセキュリティ脆弱性のリスクは代わりに負ってくれている。その代わりに、ライセンスフィー、サブスクリプションという形で機能していると思慮。

OSSは、そもそもはオープンソースであり、責任というものがないから色々なイノベーティブなものが出てくるという面があり、これを殺してはいけない。規制をかけると、楽しいこと、好きなことをやりたいという人が、また違うところに行ってしまう。トレーサビリティをきちっとやりすぎると、責任の話につながり、それでは持続しない。OSSそのもののところに手を突っ込むことは良くないと考える。

ライセンス変更等に関し、オープンソースは著作権者が何百人とか何万人とかいて全員の同意を取るのは困難。期間を設けてこの期間に連絡がなかったら同意というようなことをネットに掲載する形で進めるファウンデーションもある。

オープンソースを作る人たちは、そもそも皆に使ってもらいたいから作っているわけで、法律の専門家ではないためライセンスは用意されたものをなんとなく付与しているケースが多い。付与したことで使われなくなってしまうのであれば、避けたいと思う人がほとんど。他方、一度流通した以上は対応する必要があるが、今はコミュニティがその対応を担っている。特に、Linux Foundationは経済的にも豊富であり、責任があるわけではないが、メンテナンスがされなかった部分を引き取り、お金も人もつけてメンテナンスするということも実施している。各会社からの拠出により、オープンソースの世界をしっかりガバナンスをしていきたいという意思のもと推進されているのが現状。

OSSを組み込んだ製品の競争力を上げていくことが目的であると認識。OSSを作る人とOSSを組み込む人にとって、全体の負担をいかに下げていくかが重要。それぞれ責任があるため、そこには必ず対価が必要であり、そこをうまくシェアするようなものがいるのではないか。

ライセンスの干渉はもちろん大きな問題ではあるが、逆に、より使いやすいものを新たにオープンソースとして作るというモチベーションになったりする。必ずしもそれがすぐクリティカルな問題になるかというか、そうとは限らない。

基本的に企業がOSSを使用しようとすると、ディストリビュータでしっかりサポートしてもらうことが多い。その結果、高額な費用がかかるため、ディストリビュータ自身が自分たちの負荷を下げ、ディストリビューションしたソフトの競争力が上がるような仕組みがあると良い。

OSSを作る立場としては使って欲しいというのがあり、リーズナブルな努力で使ってもらいやすくなるのであれば喜んでやる。ただし、あくまで無料でやっているため、責任を問われるのならやらない。例えば、このようなSBOMのフォーマットが出来たから、これに合わせて出してくれと言われるのであれば、それほど負担ではない。

責任を取るのはお金のインのある世界であるから、やはりディストリビュータのようなところが、きちんと品質保証なり、責任なりを持つというのがリーズナブルであると考える。ディストリビュータという業態が出来て、競争領域になっていることから、それを公的なものとして作るというのは馴染まないのではないか。ただ、お金を取らない、保証もしない、情報センターのようなものは有益であると考える。ディストリビュータの競争を促して、良いディストリビュータが生まれるのは非常に健全。

ディストリビュータが存在出来るのは、ビジネスとして成り立つからである。問題なのは、組み込みなどの小さなパーツ等を扱う分野で、サービサがいても多分ビジネスにならない。クリーンセンターのようなものをやるか、コンソーシアムを作らせてチェックするようなことをやるか。一番初めの信頼性というものを誰が、どこで、どうやって作るのか、そのコストを誰が負担するのか、その解がないとどんなツールを作ろうがうまく動かないのではないか。

GPL v4が出てきた時の受け皿に関しては我々も危惧。推進フォーラムに参加している各社のメインはエンジニアであり、テクニカルな部分で、それをどうビジネスに転用していくかというところが議論の中心。各社の知財部門や法務部門、弁護士の方が参加しているような段階ではない。法律の専門家をどう巻き込んでいくかということがひとつの大きな課題。

企業間の情報流通やサプライチェーンを、SPDXでどうやるかというような議論は何度もなされているが、実際の運用と照らし合わせてみると様々課題がある。例えば、OSSは、その中に他のオープンソースやライブラリを含んでいてライセンスが違うようなケースがあり、そういう多段構成をどの粒度で管理するのか。バージョンによってライセンスが変わるようなものについてどういうタイミングでSPDX等を見直していくのか。コンテナやパッケージについて、知らないうちに多段の依存関係が出来てしまっているケースがあり、これをどう管理するのか、等。ライセンスも、独自事項や例外条項付きのものなど、非常に複雑なライセンスが多い。

●OSSコミュニティへの貢献について
お金を集める方法として、電子マネー等を使った投げ銭など、貢献してくれた人にコミュニティから何かを返すような仕組みがあるといい。既存のやり方のどれかを採択するだけでなく、コミュニティの人達のやる気を維持させ、パフォーマンスを引き出す工夫ができればと考える。ただ、なかなか難しいということも理解している。

OSSコミュニティとの関わり方として、参加することが大事だが、日本の場合、言語の問題・障害があり難しいところもある。OpenChainのJAPAN WGでやっている日本語で議論し英語でアウトプットするという形のように、やり方は色々あると思うのが、どうやったら参加できるかという部分で成功例のようなものがあれば共有できれば良いのでないか。

OMG(Object Management Group)の場において、日本企業の人に集まってもらい日本語で検討した結果を向こうにもって行くという形式で実施したことがある。ダイレクトに海外へ行くよりも有効。

●OSSに関するベストプラクティスについて
コミュニティ活動について、中小・中堅ベンダでは、そもそもコミュニティへ貢献するという意識は希薄。コミュニティ活動から対価が得られるのかと考える企業は結構多く、経営者がある程度理解していて、参加するように指示された人しか出られないのが現状。そこら辺の活動もプラクティス集に含められると、経営者の意識向上にも役立つ。

推進フォーラムでも、なかなかフォーラム外での活動が出来ていない。会員企業の中で、そういったプラクティスやコミュニティにどう参加をしていけば良いのか、という情報共有とかはやってきた。どういう風に発信していけばいいか等、どう協力

すれば良いか考えていきたい。

ライセンス管理のベストプラクティスに関しては、OpenChain のJAPAN WGがまさにそれをやっているので、そこで声をあげて作るというのは可能ではないか。

色々なところに声掛けして、雛形みたいなものを作ってもらうのが良いと思う。

●その他
資料3のp.19で製品・サービスで括られているところに、SIerが必要。SIerで組み込んだものがユーザでは分からないという部分が残ってしまい、放置されてしまう可能性がある。この部分には、OpenChain Projectの取組が適用できるのではないかと思う。SPDXにしろ、SWIDにしろ、フォーマット変換は可能だが、紙から脱しきれないところが大きな課題ではないかと思う。

IPAの2016年の調査報告書「ソフトウェア識別管理に向けた分析事業」のバージョンアップや、OpenChainで識別子としてのSPDXの利用ルールができれば、JVNにおいて関連した情報の電子化などを一部分でも具体化し動く可能性を示すとか、協力できるのではないか。

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