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2回）議事概要

1. 日時・場所

日時：令和元年11月6日（水） 16時00分～18時00分

場所：経済産業省　本館17階第5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　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　OSS の脆弱性・継続性の実態とその管理

資料5　早期警戒パートナーシップと JVN について

4. 議事内容

事務局から、資料3に基づいて、本タスクフォースの検討の方向性について説明、明石委員、渡辺委員と伊藤委員から、それぞれ資料4、資料5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。

○脆弱性の定義について

制度設計等を進める上で、脆弱性の定義や把握の方法が重要。脆弱性情報のオーナーを誰と考えるべきなのか。現実には見つけた人がオーナーだが、それを離れて誰が統制すべきなのかという議論が必要。

脆弱性届出制度では、資料5のp3のような定義を考えているが、製品会社が脆弱性として認めたり、認めなかったり議論はある。攻撃を受けることを考えると、製品会社自らが脆弱性を判断して対応するのがいい。

資料5のp3の上2つを想定すれば、通常の脆弱性としてこのタスクフォースでは十分ではないか。

コストを誰が負担するのか検討が必要。米国では有志がお金出しあってやっている。我が国では、どういう仕組みにするかこの会議で検討してはどうか。日本におけるSBOMのアライアンスの様なものを作りその会費を取る、製品から回収する、などあると思う。一般消費者は、脆弱性はバグでありメーカが直すのが当然と思っている傾向がある。IoTが普及し一般の家電において瑕疵担保の責任の範囲ではないとなった場合、誰がコストを負担するのか。また、ベンダがSBOMにちゃ

んと取り組んでいることを最終消費者がどうやって判断するのかという課題もある。

脆弱性の評価に関し、少なくとも3つの問題、設計の問題、コードの問題、設定の問題がある。ID やパスワードのチェックについて、仕組みはあっても機能しないのがコードの問題で、どんな値を与え得るかというのは設定の問題。対策アプローチが異なるので整理しないといけない。単に weakness としてまとめてしまうのはよくない。

CVSS について、人によって評価にブレがある。製品に組み込まれた際にも、脆弱性が影響するケースとしないケースがあるので、最近は製品ごとに CVSS の値が違うことも許容される。また、評価の仕組みがあっても、組み込んだ時の状況や事前情報の有無によっても、攻撃出来る、出来ないが変わってくるため、運用上の課題はある。

自動車の制御ソフトに不具合がある場合、自動車メーカの責任が除外されるということは無い。脆弱性が原因でリコールすることになった例もある。

中小企業では自身を守るためにバイナリ納品をしている企業もあり、SBOMを提供するのは簡単ではない。ソースコード納品をして、このOSS使っているのであればもっと安く出来たのでは、みたいな話は現実にある。企業間の契約が対等でない等の根本的な問題にも取り組まないと、SBOMを提供するのは難しいと思う。

自社の製品に脆弱性が発見されると検証しなければいけないが、中小企業が検証環境を 5 年も 10 年も維持するのは極めて難しい。脆弱性対応など検証したいタイミングで検証が行える場があるといい。

サーバでもIoTでもOSSを使う中でソフトウェア更新は必須だが、SBOMをどう追随させるかという仕組みを考えなければいけない。

脆弱性対策はスピード勝負。優先度を判断しながらOSSの管理チームとセキュリティのチームが連携して対応する。管理チームは、どうやってバージョンアップするか、システムを止める必要があるか等考える一方、セキュリティのチームは攻撃コードが存在するかを探し、存在する場合にはWAFにシグネチャなどを充ててバージョンアップまでの時間を稼ぐ。こうした体制が整っていないと、SBOMだけでは実効上機能しない。

脆弱性対応で一番問題なのがテスト。テストの時間を稼ぐためにその前の判断にかかる時間を出来るだけ短くしたい。SBOMみたいなもので判断をするための時間を短くできるツールが欲しい。SBOMの情報にある程度の粒度や、更新の早いOSSにも追従できる仕組みがないと難しい。

SBOMを運用するための仕組みを作る必要がある。SWIDタグ等が流通するような仕組みを使いたい人向けに共通の識別子、仕組みやインターフェイスは必要。CVEはグローバルでユニークであることで、結果、脆弱性を識別するための仕組みとして活用されているのが良い。

Open SSLのように比較的更新頻度の高いオープンソース等は、非常に細かい枝番でアップデートされていく中で、それらの細かい枝番の違いをもって、全く別なものとして評価すべきなのかの観点を考える必要があり、恐らくそのままのSBOMでは解決が難しく、例えば点数付けのようなものを追加するなどのサポートが考えられないかと思っている。

脆弱性情報は社会の資産でありそれを伝達することはマナーのようなもの。それが当たり前なことだという雰囲気を醸成するとことが必要な気がする。その後にいろいろ仕組みが出てくる。

OSS について、きちんと開発が継続されるものを選ぶのは大前提だが、活発に開発され広く広まっているものもいつの間にか廃れ開発が止まったり、個人開発者に依存する部分が多く開発が停滞したりすることがある。Linux ファンデーションのコミュニティブリッジなど、コミュニティを直接支援するプログラムやスタートアップ等があるが、そういった活動に対する後押し等も議論したい。

OSSを商用で使う場合、コミュニティが動かないからといってサービスを止めるわけにはいかないので、自社内にOSSのチームを組んで対応する必要があるが、そういうところで連携できると事業としては助かる。

攻撃されるリスクのあるものは対処しなくてはいけない。悪用されて困るもの、或いは悪用される可能性の高いものというのは統一的にハンドリングする必要がある。その上で中小企業などリソースがないところに対して、平等に脆弱性やリスクを伝達できる仕組みがないと、対応出来るところと出来ないところで格差が生まれ、ここにもサプライチェーンのリスクが生じうる。SBOMを利用して、広く使われているOSSに対する重要な脆弱性対応に必要なものを提供できれば、有効活用につながるのではないか。

脆弱性が見つかったとき、攻撃を受けないために WAF などの暫定対策が必要になる。しかし、同じ脆弱性を同じコードばかりで攻撃されるとは限らず、暫定対策に用いる情報も暫定的でしかなく、根本改善がされるまでの間は暫定対策も追加更新しないといけない。そういった情報を画一的にみんなに伝達できるのか、スピード感も重要。

Linux のディストリビューションによっては、パッチが出るまでに一週間くらい差があり、脆弱性があるとわかっているのに対応出来ない時期が生じる。そういったタイムラグをどうやって圧縮できるのかということも議論出来ればいい。

SBOMを作ったとして、それをどう流通していくのかが見えない。流通させることをみなさん良い方向で捉えていると思うが、それは脆弱性情報を丸裸にする可能性があり、攻撃者を資することにもなる。うまく流通させないといけない。

SBOMには第三者に見えてはいけないものも含まれうるので、そこの秘匿性を確保する、見えていいものといけないもののレベルをつけるなどして、脆弱性が見つかって直すまでの猶予期間の間だけでも秘匿しておくとかできるといい。

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