第２回　サイバーセキュリティ検証基盤構築に向けた有識者会議

日時・場所　　令和元年１０月１６日（水）15:00-17:00　　独立行政法人情報処理推進機構（IPA）

出席者

[委員]　熱海委員、斉藤委員、下村委員、高倉委員、寺原委員、名和委員、政本委員

[事務局]　IPA セキュリティセンター 瓜生センター長、小川グループリーダー、増田主任研究員、島田職員

[オブザーバー]　経済産業省 商務情報政策局 サイバーセキュリティ課 鴨田企画官、尾崎課長補佐、西野課長補佐、野村係長

議事概要

第２回会議では、IPA より評価対象製品候補の抽出方法、ベンチャー等のセキュリティ製品のサイバーキルチェーンへのマッピング、検討スケジュールなどについて説明。その後、評価対象となる製品分野の考え方、日本企業と外資の違いなどについて自由討議を行った。委員からの意見は以下の通り。

【対象製品のマッピングについて】

- サイバーキルチェーンでの整理はこの前より良い。それぞれのフェーズでどんな処理があるかを加味されると網羅性とか実現性が出てくる。MITRE 社の ATT＆CK を参考にすると良い。
- セキュリティでないが、運用、資産管理などサイバーセキュリティをやるための基本の部分も必要。
- サイバーキルチェーンのスコープは企業の基幹システムが対象。それ以外の分野(OT、IoT、５G等)に目を向けても面白い。
- マップを整理する上でのカテゴリーのキーワードは「security landscape」で検索するといろいろと出てくる。
- 参考となるフレームワークとしては、ENISA TOPICS、英国のNCSCのものなどがある。

【ユーザーニーズについて】

- 分野を決めてというやり方もあるが、ユーザーニーズがある分野を絞り込んで探すという手もある。
- 有識者会議で「これから 3 年はここを強化した方がよい」という市場のニーズの方向性を示すのも良いのではないか。
- ユーザーニーズのありそうな分野：可視化(ネットワークトポロジー、IT 資産、イントラネット内の端末間の通信、モバイル機器の移動追跡 等)、ユーザー教育・訓練、脅威インテリジェンスの整理・管理、マルウェアの感染状況・重篤度判定 等

【日本と外資のベンダーの違い】

- 日本のユーザーが海外の製品を好むのは、外資ベンダーのトップセールスの影響があるように思う。
- 日本企業と外資は契約の概念が違う。日本の契約書では「お互い誠意をもって話し合う事」とあるが、外資の場合は過去に何があっても今回の契約書が上書きされると書いてある。
- 外資だと全く使わない機能が実装されてライセンスが2倍に上がったりする。説明も事後でどうなのかと思うところもある。
- 日本企業と外資では商習慣の違いがあるというのを理解する必要がある。

【日本のベンダー、製品の良さ】

- 海外の製品は高くなっていくし、買収で製品がなくなることもある。そのリスクを考えると、事業継続の観点からもコアの物は日本の製品にした方が良いと考えている。
- 日本製という裏に逃げない、価格が上がらないとかが入っている。そこはビジネスモデルの作り方かも知れない。
- いろいろな企業の CIO から、今まで金をかけてきたがもう少しコストを安くしてセキュリティは守れないか、という話を聞く。パフォーマンスの良い日本の製品で重要な情報を守ることに特化すれば、良いものができるのではないかと感じる。
- 海外製品は研究されつくしているので、マルウェアがすり抜けてくる。メジャーなものは攻撃する側も対策を取ってくるのが当たり前になってきているので、売れ筋を買ってくるのが正しいのかというところにきている。

【情報公開の方法、導入実績の公表について】

- メンバー限定などの限定公開とだとしても、情報は外に漏れる。
- 非常に頑張っている日本製品があるが、絶対に名前は公開したくない。公開した方がみんな喜ぶだろうが、難しい。
- 公的機関がある程度言える範囲で導入している製品を公開するのも手としてある。
- 成功しているクローズドコミュニティとしては、米国の DC３(Department of Defense Cyber Crime Center)がある。

以上