産業サイバーセキュリティ研究会
WG1分野横断SWG(第2回) 議事要旨

1. 日時・場所

日時:平成30年12月7日(金) 16時00分～18時00分

場所:経済産業省別館 2階 218各省庁共用会議室

2. 出席者

委員 :佐々木委員(座長)、青木委員、石原委員、大久保委員、岡田委員、川口委員、桑名委員、
後藤(俊)委員、後藤(里)委員、古原委員、下村委員、谷委員、中尾委員、平田委員、
舟山委員、洞田委員、吉田委員、米田委員

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、総務省、防衛装備庁

経済産業省:商務情報政策局 三角審議官、奥家サイバーセキュリティ課長、土屋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・配付資料一覧

資料2 委員等名簿

資料3 サイバー・フィジカル・セキュリティ対策フレームワーク(案)の修正概要

資料4 サイバー・フィジカル・セキュリティ対策フレームワーク(案)

参考資料 産業サイバーセキュリティを巡る国外の動向

4. 議事内容

事務局から、資料3及び資料4に基づいて『サイバー・フィジカル・セキュリティ対策フレームワーム(案)』について説明を行った後、自由討議を行った。委員からの意見は以下のとおり。

(1) 三層構造アプローチについて

- 第Ⅱ部のp.28の図13にいくと、苦労されているのはわかるが、第1層が縦にまたがる。何が正解というわけではないが、第1層は従来型のサプライチェーンをつなぐところ、製造業のEDIや金融のSWIFTが第1層に落とし込まれていて、モデルを分析するところで第3層に飛ぶと、今は第1層でいいけど今後は3層だよね、と言えるのではないか。
- 第1層がなかなか分かりにくかったが、大分整理されてきたと思う。第2層と第3層、と第1層の次元が違っていて、オーバーラップしている部分があって企業の中で完結する転写もありSoceity5.0で他者と共有するものもある。

(2) ユースケースについて

- ユースケースの議論になっていくと思うが、ごく普通の通信が第3層になっている。普通の通信が第1層にあると大分楽になるのかなと思った。
- 定義やユースケースは多く書いていただいて明確になったと思う。第1層のとらえ方がポイント。フィジカル空間と企業のつながりがすっと落ちてこない。現実世界でも第1層で結ばれているケース、インターネットの先で加工されているケースで違う、そのあたりを整理いただくと良いかと思う。
- ユースケースを書いていただいて良かったが、難しいケースに挑戦しているように見えた。もうちょっとバリュークリエイションプロセスに従うもののシンプルな方が、スマートホームも色々な機器が入ってくるのでシンプルにしてあげた方が

良い。
- 電力のユースケース図も作っていただいたが、一つの会社に閉じたものだと第2層と第3層の概念の整理が難しい。
- ユースケースの第3層の捉え方を確認したい。キーとなるのは加工メーカと完成メーカの第3層のつながり、サーバ間のつながりだと思う。仮につながりにない状態において、企業内の機器のつながりにおいても社内のセキュリティ対策として第3層の対策が必要か明確にして欲しい。

(3) 信頼性について
- 信頼のチェーン、アンカーポイントを3つの観点で例示していただいているが、そこの考え方をもっと書いていただけるといい。
- p.39 の信頼性の基点の確保に関して、信頼できないデータが来たときにどう安全を確保するのか、を第三層でもやらないといけないのかもしれない。極論を言うとフィルタリングだが、あまりそういうところが書かれていない。
- 何をもって信頼するのかが信頼の基点に関わってくると思うが、物理・トランスクリプション・サイバーが少しずれているのかと思った。組織で対策するのか、データで対策するのか、手続きで対策するのか。対策が先に出ているのでセキュリティ・バイ・デザインがしにくい。
- p.20 の信頼の創出、証明については、コンセプトの段階と思っている。一つの機能や産業分野だけでなく全産業で歩調を合わせて取りくんでいくものだと思うが、分野横断 SWG などを活用していくものだと思う。

(4) リスクアセスメントについて
- リスクアセスのときに守るべきものから、もう少し書いていただいた方がいいと思った。モノがあって、そこに対するアクセス手段がある。外部に影響を与えない、悪影響を与えないことをはっきりさせると、守るべきものとセキュリティ対策をしっかり書けると思った。
- p.16 に価値創造過程の6要素があるが、IoT の時代になるとバリュークリエーションのチェーンがどんどん変わる。個々の資産を特定したリスク分析はやっておらず、その中で6要素でリスク分析ができるのではと思った。

(5) セキュリティ対策について
- セキュリティ事象において、 6要素は守るべき部分でもあるが、 穴になる部分にもなり得ると思った。
- 6要素をセキュリティ対策の要素と考えてしまいがちである。セキュリティ対策の対象は、組織かシステムになる。SP 800-53 v5 のドラフトが出ているが、組織に対するインプリか、システムに対するインプリか記載されている。組織への適用か、システムへの適用か明示してくれると誰がやるか明確になる。
- 事業者視点では、添付Cの対策例、アメリカのフレームワークを軸にしながら High、Middle、Low を分けているので、辞書的に使いやすくなっている。添付Dで網羅性も担保できるのではないかと思っている。この対応表があるとありがたいので継続して管理していただきたい。
- 添付Cで High、Middle、Low を分けている。Low だけやればいいのか、変に理解されないか不安。このあたりの表現は考える必要がある。
- セキュリティの対策として、High、Middle、Low、共通と分けている。これは大きな議論があって、ISO/IEC 27001でもappendixにmandatoryとshall がある。
- IoTのセキュリティに関しては、ISO/IEC 27030の検討が進んでいる。セキュリティだけでなくプライバシーも含めたガイドラインであり、セキュリティの対策とプライバシーの対策を書いている。米国カリフォルニア州では、IoTデバイスセキュリティ対策を義務付ける州法が成立した。セキュリティについてはベースラインというものがあり、selectiveやrecommendationもあるのかと思う。ただ、どういう観点でHigh、Middle、Lowを付けたのか分かっていないが、慎重に考

えた方がいい。

- 6要素を考えるときに制御の分野は組織とシステムと機器で対策が非常にクリアに意識されている。それは組織にセキュリティリクワイヤメントが発生すると、その組織に納入するシステムにセキュリティリクワイヤメントが落ちてきて、そのシステムに組み込む機器にセキュリティリクワイヤメントが落ちてくる、というクリアな関係がある。たぶん、IEC 62443に詳しい海外で活躍されている方がこれを見ると、あの組織、システム、機器とどう違うのかという質問を沢山受け付けると思う。逆の言い方をすると、それらと比べてこの6要素はどういう関係にあるのか対比して考えると、新しい機器と機器とのつながりが出てくるからこういう要素が新たに出てくるのだと、そういう説明の仕方ができると思う。よって、制御システムなどで確立している組織、システム、機器とどういう関係にあるのかという議論は有用かと思う。
- ライフサイクルに関して、セキュリティ要件のガイドラインを見ていると要件の記載に留まるガイドラインは、ライフサイクルのどの段階でやるかというところまで明確化されていないのが多く、セキュリティ対策を実際にやる場合に、初めてライフサイクルのどこで対策を実施するか考える場合が多いと思う。今回の第一部、第二部、第三部というまとめをするときに、ライフサイクルの概念を第三部に取り入れるという判断はできるのではないかと思う。そうすると実は第三部の対策例は分野毎に非常に異なるところと深く連携していて、橋渡しができるのではないかと考える。
- 機能安全の話に関して、NISTのサイバーセキュリティフレームワークの22のカテゴリとのマッピングをしたときにそのカテゴリのどこに制御が入るかなという議論をすると、最初のアイデンティファイのところでハザード分析が入ってくると思うし、そのレスポンドやリカバーのところにかなりの要素が出てくるな、とその様にすると議論がしやすいと思う。

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