産業サイバーセキュリティ研究会
WG1分野横断SWG(第1回) 議事要旨

1. 日時・場所

日時:平成30年10月5日(金) 9時00分～11時00分

場所:経済産業省 本館 2階 西3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、粕谷委員、川口委員、桑名委員、後藤(俊)委員、下村委員、小西様(谷委員代理)、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 本会議の運営について(案)

資料4 産業サイバーセキュリティ研究会WG1分野横断SWGの設置について

資料5『サイバー・フィジカル・セキュリティ対策フレームワーク』の見直し方針

4. 議事内容

事務局から、資料3及び資料4による本サブワーキンググループの設置についての説明に続き、資料5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ク』の見直し方針を説明した後、自由討議を行った。委員からの意見は以下のとおり。

(1) 三層構造アプローチについて

- 三層の定義を明確に書き起こしていく必要があるかと思います。各人の思いでブレが生じるので、それぞれが何を指すのか、示す必要があると思います。
- 三層モデルについて、第1層は基本的に従来のサプライチェーンの空間で、適切なマネジメントと信頼という話になっている。第2層、第3層は、それでは立ち行かないものが入ってくる位置づけと理解しました。
- 第2層で使われている、いわゆるサイバーとフィジカルの「転写」という言葉について、IoT機器を販売している観点から見ると、勿論、その「転写」を行っているのですが、いわゆるAIに近い活動を行ったりしていると、事務局がおっしゃる定義も含んでいるのですが、文言で見るとみるとやや狭隘で少々混乱してしまいました。もう少し広い概念を包含するような言葉に変えるのか、それとも、もう少し定義そのものを変えるかについて議論が必要かと思いました。
- 三層六要素について、まず、こういうことから考えてみることには非常に賛成。ただ、今の議論や我々の社内の議論でもそうなのですが、定義が何かという議論が出てきます。今日の皆様の御意見を伺っても、共通の意識をもってスタートした方がいいかなと思います。
- 三層構造の捉え方で、Society5.0を見たときにどのような観点で切るかは相当悩むところだと思います。わかりにくさというのがファンクションなのか、どのような観点で見るのか、まだ皆さん一致が取れないところに、難しさが一つあり、言葉の定義を含めて表現に工夫が必要と思います。

- 六つの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非常にクリアに意識されています。それは、組織にセキュリティ要件が発生すると、その組織に納入するシステムにセキュリティ要件が落ちてきて、そのシステムに組み込む機器にセキュリティ要件が落ちてくる、というクリアな関係があります。IEC 62443 などに慣れている、海外で活躍されている方がフレームワークを見ると、IEC 62443 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います。逆の言い方をすると、IEC 62443 と比較してこの六つの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」といった説明ができるのではないかと思います。ですので、制御システムなどで確立している組織、システム、機器とフレームワークとがどういう関係にあるのかの議論は有用かと思います。

(2) 国際規格等との比較について

- 「最終的なガイドラインの形をこうする」というのではなく、内部の議論として共通となる軸を揃えた上で議論ができるといいと思います。今の時点で言うと、第二部の対策要件のところが、例えば、NISTのCSFの22カテゴリを縦軸に、横軸に六つの要素を取ったような表にして、それを第1層、第2層、第3層と三種類用意します。そうしたときに、それぞれのNISTのCSFの22カテゴリが、六つの要素のどこにマッピングされるか、というものが各層で整理されていたりすると、第3層には多くの要素が入るけど、第2層には組織やプロシージャがあまり入らない、といった違いが見えてくる気がしていて、そのような共通の土台があると、比較的発散しないで議論ができるのではないかと思いました。
- 他国とのフレームワークや構造との違いも明確にあり、違いをどう説明するかを改めて考えると、なかなか説明が難しいと感じます。

(3) フレームワークの構成について

- フレームワークの構成を三部に分けることは賛成。
- フレームワークの全体構成の見直しということで三部構成の話がありましたが、これは非常にありがたいと思っています。いろいろな中小企業・ベンチャー企業含めて個人情報の匿名加工やデータの利活用に関する相談を毎日のように受けていますが、実際に、このような方たちはセキュリティにかけるコストやリソースがなかなか無いという実情がございます。第一部、第二部、第三部ときちんとコンセプトからやってくのがいいと思うのですけれども、実際に使われる段になると、恐らくセキュリティ対策が中心に使われることになると思います。これがきちんとレベル分けされていると、我々も話をしやすいですし、共通認識を持てるのでいいのかなと思います。
- 対策例をレベル分けするという話がございましたが、レベル分けが行われたものと、今、各SWGでガイドラインを作成したり、ブラッシュアップしたりという動きがありますので、フレームワークとしての対策例が二重構造にならないよう、フレームワークを位置付けていただけると大変ありがたいです。

(4) ユースケースについて

- フレームワークなのである程度、抽象化して記述する必要はありますが、具体的なユースケースを踏まえた上で整理していくのが良いと考えています。ユースケースに基づいて、第1層、第2層、第3層がどこにあたり、それぞれの六つの構成要素が何かを、ステークホルダーに示していくのが良いかと思います。
- 三層モデルを皆さんが理解できるようにするためには、ユースケースが一番大事と思います。これをきちんとやっておかないと、リスク源を洗い出すステップで、担当者の知識・力量に依存したリスク源の洗い出しにしかならず、その先のプロセスが上手く回らないと考えています。
- 分野別SWGで三層と六つの要素にユースケースを当てはめていき、事務局で考えていること、あるいは他のSWGで考えていることを落とし込んでいくのも良いかと思っています。

- ユースケースで三層を見ないと理解が進まないという話がありましたが、もう一つの観点としてデータの信頼、機能の信頼、組織の信頼の「の」「of」が非常に広く捉えられてしまうのだと思います。この部分については、データのための信頼、Trust for data、using data、機能の信頼はTrust of Function、組織の信頼はTrust established by organizationのように理念というか「ここが守りたい」という部分の説明と、ユースケースとで両脇から支えると非常にわかりやすくなるのではないかと思います。
- ユースケースの話は、全部はできないので、どこをやるのかという話になると思います。ユーズをある程度決め打ちにせざるを得ないと思っています。

（5） 産業分野の特性について

- ファクトリーIoT 的な考え方では、確かに工場の中で「転写」を行ってデータを移動することは、かつてから行われていますが、業界横断で考えるともっと大きなことなのかと感じています。
- ビル分野は二層が多いのですが意図せずやっぱり三層のレベルまでいって脆弱性をさらしているところがあるので、そこはユースケースなどを基にしっかり整理していただきたい。
- スマートホームはコンシューマーIoT モデルで、だんだん中抜きになってきて、機器が見てきたことをクラウドで見るという、中の人、ローカルインテグレーターが存在しないことが問題になっていて、その辺りが他の分野と大分違うのかなと思います。
- 電力制御システムは企業内に閉じて構築しており、サーバ、回線、端末類もすべて企業内に閉じて、外部システムとの接続対策も、電力制御システムのガイドラインに沿って各社で対応しています。そのため電力の世界はかなり第1層の内容が色濃いものとなっています。
- このフレームワーク自体、Society5.0 に反映していくために、社会全体をフィールドシステムと捉えた格好で、それぞれ検討する印象を持っていて、そうすると取り扱うデータが比較的、動的なデータというか、パラメータを扱うことになるので、パラメータの通信なり、なんなりを如何に管理していくのかという印象を持ったのですが、防衛産業では、どちらかというと動的ではなくて、静的なデータ、データそのものをセキュアにどう扱うか、という議論をしています。そういった意味で、お互いがどこを議論しているか混乱しないためにも、ある程度この場での皆さん理解をするためにはユースケースがあったほうがいいと思いました。

（6） セーフティについて

- 第2層でセーフティ的な要素を入れていくという話がありましたが、どの程度行うのか気になっています。例えば、規格でいうとIEC 61508みたいなものを相手にしていかなければならないでしょうか。深掘りすると結構大変なので気になっています。
- 機能安全の話は強いて言うならば、例えば、NISTのサイバーセキュリティフレームワークの22のカテゴリにマッピングしたときに、制御がどこにマッピングされるかという議論をすると、一番始めの「アイデンティファイ」のところにハザード分析が入ってくると思うし、「レスポンド」や「リカバー」のところにも多くの要素が出てくるとか、そうするといろんな議論がし易くなるのではないかと思いました。

（7） ライフサイクルについて

- ライフサイクルについて、セキュリティ要件のガイドラインを見ていると、要件で止まっているガイドラインは、どのライフサイクルで実施するかまで踏み込み切れていないものが多く、対策を実施する時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ことになっているものが多いと思います。そのため、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で初めて入れようとする判断ができるのではないかと思います。

- ライフサイクルの話が出ていますが、ライフサイクルというのは非常によく設計されていて、確実に形としてプロセスが固まったものをどう扱うかという考え方だと思います。それに対して、アジャイルは、その場その場で決まっていくこと、変わっていくことを含むものと思うのですが、そういったものをこのフレームワークで扱うことを意図しているのかどうかは、明らかにしておいたほうがいいのではないかなと思います。
- 様々な産業分野で検討した場合に、「この分野ではこういう影響度があるが、別の分野ではこういう影響度がある」といった形で、環境に依存する可能性が同じ製品でも異なるのではないかと思います。脆弱性については、早期警戒パートナーシップの中で CVSS というスコアが使われていますが、その中ではいわゆるベーススコアの他に、テンポラリー値や環境値というものも本来は評価すべき対象になっています。そういう意味では、例えば、時刻であったり時間によってどう変化するのかであったり、あるいは環境によってどう変化するのかといった問題がこのフレームワークの中のどこで議論されるべきなのか、あるいはそうではなくて、フレームワークでは静的な範囲を検討するのかが整理するポイントとしてあるかなと思います。それらを、脆弱性の中に含めて考えるのか、そうではなくて時刻であったり環境であったり別の軸で考えるべきなのかも、表現の方法としてはあるのかなと思いました。

（8）その他

- どうしてもセキュリティの観点で見ていまして、相手への信頼確認、この部分は今までのフレームワークやガイドラインを見ていても信頼をどう確保するかはあまり書かれていない。ここは今回すごく大きいところの一つだと思いますので、表現をどうしていくかポイントだと思います。

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