産業サイバーセキュリティ研究会WG1
『第2層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けた
セキュリティ対策検討タスクフォース(第6回)
議事概要

1. 日時・場所

日時：令和4年3月9日（水） 16時00分～18時00分

場所：Web開催

2. 出席者

委員　　：松本委員（座長）、伊藤委員、岩﨑委員、大友委員、荻野委員、梶屋委員、神余委員、北澤委員、
教学委員、戸枝委員、西貝委員、野口委員、松元委員、渡部委員

オブザーバ：警察庁、総務省、厚生労働省、国立研究開発法人 産業技術総合研究所、
独立行政法人 情報処理推進機構、技術研究組合 制御システムセキュリティセンター、
独立行政法人 製品評価技術基盤機構、一般財団法人 電気安全環境研究所、
電子商取引安全技術研究組合、一般社団法人 日本自動車工業会、
一般財団法人 日本情報経済社会推進協会、一般財団法人 日本品質保証機構

経済産業省：大臣官房 江口サイバーセキュリティ・情報化審議官、商務情報政策局 奥田サイバーセキュリティ課長、
佐藤サイバーセキュリティ戦略専門官、塚本課長補佐、和平課長補佐

日立製作所：秋藤様

日立コンサルティング：木下様、佐々木様

3. 配布資料

資料1 議事次第・配布資料一覧

資料2 委員名簿

資料3『第 2 層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討
タスクフォースの検討の方向性

資料4 IoTセキュリティ・セーフティ・フレームワークVersion 1.0 実践に向けたユースケース集

資料5 IoTセキュリティ・セーフティ・フレームワークVersion 1.0 実践に向けたユースケース集（概要版）

資料6 ユースケース作成における課題等について

4. 議事内容

●リスク対応について

- ランサムウェアの攻撃からいかに守るかということの対策と同時に、ランサムウェアにさらされてもシステムが止まらなければ良く、その手段とは必ずしもサイバー空間の対応とは限らないと思う。

- 第1軸、第2軸は、サイバーシステムの担当者とは必ずしも関係ない判断、経営視点の判断ということを求めているが、第3軸の対策になったときに基本的にセキュリティ、サイバーセキュリティの対策に終始しているという構造になっており、本来のサイバー、リアル空間の持っているマネジメントの範囲から狭まっている。

・ 家庭用の Wi-Fi ルーターのセキュリティの低さに課題があるため、住まい手に対してきちんと対処してくださいということを言及していただきたい。

●ユースケース集の普及について

・ ユースケースを使ってもらうときには、このようなユースケースに対してセキュリティアタックがあった場合、こんなに皆さん大変だということを記載しておいた方が自分ごとに感じてもらえるのではないか。

・ 特に大企業であれば、部門毎に感じているリスクはそれぞれ異なることが想定されることから、実際に我が事として捉えていただくためには、どの部門の人が、どのリスクに対して対応すべきなのかがある程度わかるように所管部などの情報が読み取れるのが望ましいのでは。

・ IoT-SSFのリスクは、世間一般のリスクと異なり、確率論が入っておらず決定論だけなので、KY、ヒヤリハット同様に誰でもできるというのがポイントだと思う。無理にISOに合わせず、ISOの簡略版というスタンスで広めていけば良いのではないか。

・ そもそも、意図的に侵入してくるサイバーアタックに対して、完全に防御することはできない。そのため、セキュリティ対策をインプリメントするときに、どこまでインプレメントすれば管理者、設置者等の責務を果たしたことになるのかという範囲を示さないと、ユーザはセキュリティ対策の重要性を理解しても、対策の取りようがない。その上で、サイバーアタックによって実際に被害が生じた場合には、保険等で補償するというという体系になるのではないか。

●次回以降の改訂について

・ 第 3 軸の第 3 の観点で運用主体、マネジメントする人たちにはユーザも含まれると思う。そのなかで、ユーザをどのように教育するかについても触れていただけるとありがたい。

・ 第3の観点、第4の観点は、保険やセーフティネットが相当するが、まだ多くはない。事例を集めるのは難しいが、ここに注目したのは世界的にも類を見ないので、ぜひアピールしたい。日本が主導するメリットがあるので、ここを拡大、充実させる活動を続けたい。

・ 今回のユースケースはほぼ第1軸と第2軸を見ながら第3軸をどうしたかというところで、第3軸の第3の観点、第4の観点を加えたユースケースがあれば良いと思う。

・ 私が委員長をしている医療用ソフトウェア専門委員会が 3 月 17 日に開催されるので、このユースケースの説明を行い、その後委員でこのユースケースをベースに医療機器を中心としたユースケースを検討したいと考えている。こういった活動を行い、広めていき、また、フィードバックするような形ができれば良いと思う。医療業界でも使えそうだという感触があるので、これを積極的に利活用していきたい。

・ ユースケースを6つ作るだけでも、かなり苦労した気がしており、かつ、評価が主観的になるので、ユースケースを増やすことは非常に労力がかかるのではないか。

・ 誰かがユースケース集をまとめて作るというやり方もあるかもしれないが、それぞれ必要とする人たちが自ら作っていく

ということで、多くの事例が出てくるのかと思う。その時に、フィードバックを集めることができると良いと思う。また、同じ対象であっても違った分析結果が出てくると、なぜ、そのような違いが生まれたのかが分かって面白いのではないか。

・ セキュリティ対応として、何をどこまでどうすれば良いのかを示す良いガイダンスのようなものは無いだろうかという問い合わせを最近頻繁に受ける。その意味で、このユースケースがそのような人たちに対して、どのように役立つかという観点からは、まだまだ改善すべき余地はあると感じる。

●今後のセキュリティ政策について

・ 産業サイバーセキュリティ研究会 WG3 でビジネス化、WG2 で人材育成などを議論されているので、ビジネスにおいて、何が必要か、あるいは保険がいるかという議論があれば、その点を深掘りしたユースケースを作りつつ、保険制度を作ることに結びつけるような活動ができれば良いのではないか。

・ ユースケースを普及させるために、民間あるいは民間企業に何らかのインセンティブがあると非常にありがたい。

・ 例えば、経済産業省が出しているサイバーセキュリティ経営ガイドラインのようなガイドラインというやや強めの位置付けにするなど、よりやらなければならないというような事業者への意識付けをできるような方向性を打ち出せれば良いのではないか。

・ 事業者側としては、過失、もしくは免責されるかどうかというところが裁判所で問題になってくるので、やれることをしたということを説明するための資料として、今回のフレームワークやユースケース集、特に、添付Aや添付Bは非常に参考になると思う。

・ 用途別のサイバーセキュリティガイドラインやガイドラインとの関係性をマッピングしたうえで、評価に主観的な差が生まれないようなガイドラインのためのガイドラインのようなものがあると良い。

・ 今回のようなまとめ方をしている文書は国際的に見てもほとんどない。最終的に、こういうガイドラインを日本が初めて作っているということが、将来的な課題の提起、提案につながれば良いと思う。

・ 多くの人に関心をもってもらい、チャレンジしてもらわなければいけないので、分かりやすく、いろいろなやり方を知らしめていくというのは絶対条件だと思う一方で、セキュリティの考え方は、これまでのやり方から潮目が変わったという思いもあり、簡単にできるものではなく、分かりやすくやれるものではないということを分かってもらわないといけない。また、セキュリティ対策を行うために必要な素養、要件は整理する必要があるのではないか。

・ 一度、私達の業界の各社で利用しているシステムに適用できないかとトライをさせていただいたが、一部限定された活用となった。こういったユースケースがいろいろ積み上がって行ったときに、私達を含め様々な分野で使えるようになるかと思う。

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