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4回）議事概要

1．日時・場所

日時：令和2年8月6日（木） 13時00分～14時30分

場所：TKP虎ノ門駅前カンファレンスセンター ホール2A／オンライン併催

2．出席者

委員　　：松本委員（座長）、井口委員、伊藤委員、岩崎委員、大友委員、荻野委員、梶屋委員、神余委員、北澤委員、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：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、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、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、一般社団法JPCERTコーディネーションセンター

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技術戦略企画調査官

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 パブリックコメントで寄せられたご意見に対する考え方（案）

資料5 IoT セキュリティ・セーフティ・フレームワーク（案）

4．議事内容

事務局から資料 3-5 に基づき IoT セキュリティ・セーフティ・フレームワークのパブリックコメント結果及び修正方針等について説明した後、自由討議を行った。委員からの意見は以下のとおり。

●IoT-SSF の使い方について

資料 5 の 181-182 行目のマッピングに関し分かりにくいというコメントがあった原因は、機器とシステムというのが常に一緒にして使われているせいではないか。「IoT 機器・システム」という語の説明を付す修正を行うべき。

制御系を扱う事業者が攻撃を受けた際にどのように対応するかが非常に重要。まさかサイバー攻撃を受けているとは思わず、単純な機器の故障のような事象と考えて対応するのと、サイバー攻撃の可能性を検討して対応するのとではまったく違う。そういう教育的要素までカバーできれば、今までにないフレームワークになるのではないか。

資料 3 の p21 がポイント。IoT 機器・システムにおけるセキュリティを考える上での軸を定義し、全体を俯瞰して対策を考えるべきという提案は非常に良い。他の国際標準等は個別の内容を書いているに過ぎず、こういう切り口は実務上有効。

IoT-SSF は、解決の難しい問題がたくさんある中で、そのような課題を議論するときに、フレームワークのどこかに位置づけるという活用の仕方がある。

IoT-SSF はフレームワークらしく色々な議論が吸収できるところがいい。まだ技術屋や専門家しか分からないレベルになっているので、これからのアクションとしてパンフレットなどは作れないか。

●ユースケースの記載について
ユースケースでわかりやすくすることも大事だが、事例を見ないと考え方がわからないようだと、最先端のセキュリティ事象にはついていけない。逆に、コアとなる考え方や社会情勢等から今何が大事かを常に考えて導入する技術を養成することが重要。入門編としてのユースケースと、最先端のプレーヤ向けの考え方のコアの両方を提供できるとよい。

業界などが教育等を行うスキームを作る必要がある。

ユースケースにはメリットもあるが、どうしても文字のみで説明せざるを得ないため、記載が独り歩きしてしまう等の難しい課題がある。もしユースケースを提示するのであれば、基本的な考え方と、ユースケースに関する評価がある程度リンクするような記載があると、応用を考える場合のヒントになり、専門知識が十分でない方でも使いやすくなると思う。

●インテンディッド・ユース（意図された使用）と責任の所在について
使われ方によってリスクは変わるので、インテンディッド・ユース（意図された使用）の概念が重要。ステークホルダと、関連するインテンディッド・ユースを明確にしてリスクを考え、それを提示してディスカッションや教育することが重要と思う。

サイバーセキュリティ対策の責任を機器側が持たなければいけないというような議論もあるが、意図しない使い方をする人たちは一定数いるという状況で、どのように線引きをするかは非常に難しい。

誰が責任を持つかという議論から始まるが、誰が責任を持つかが明らかになったからといって事故が防げるわけではない。最終ユーザに責任を持っていくと、提供側は責任がなくなったように見えるが、それは逆にその機器の普及がユーザ側のレベルに依存することになる。どんなユーザにも使ってもらおうとすると、責任は提供側が引き受けるしかないのではないか。

●リスク及び発生確率について
技術者が考えるリスクと、経営者の考えるリスクは異なる。技術者は発生確率と影響の大きさを常にペアに対応策を考えてきたが、この考え方はセキュリティには合わない。サイバーセキュリティは、攻撃側の事情に寄りすぎており、未来における発生確率は分からない。過去のデータもあくまでも経営者が判断するための参考資料である。発生確率による対応ではない新しいリスクの考え方を示す必要がある。

英語でも以前は probability だったが、likelihood になっている。probability というと、数値で表せる点が強調されるが、likelihood は、社会情勢等の様々な要因も絡む。工学的要素だけでは決まらないというイメージを出すべきであり、「発生

確率」は適切な表現に修正すべき。

ユースケースを作る際、フルスペックで活用していなくても、それぞれの業界やアプリケーションを持っている方々の中で、このような使い方ができるというのを競い合うような形にしてはどうか。

●その他
資料 3 の p7 にある Ripple20 は製造業にとって相当大変。当該脆弱性の有無について、コンシューマ向けに近い製品になるとまるで分からない。サプライチェーンの中でどういう処理をしていくのかは本当に重要。

国際標準の分野でもサイバーセキュリティ対応は最優先の課題として議論されている。サイバーセキュリティは、従来の製品安全等の認証制度と異なり、技術的な認証を与えても全く意味がない。そこで、サイバーセキュリティへの対処能力が所定のレベルに到達しているか否かの認証のシステムが検討されており、一部の認証は運用ベースで行われている。

欧州における認証フレームワークに対して、欧州の産業界などからもコモンクライテリアの仕組みを使うのは賛成しないという明確な立場が示されている。

各委員から頂いた意見を踏まえて座長に相談し、フレームワーク案に修正を加えた上で、産業サイバーセキュリティ研究会分野横断サブワーキンググループに報告することで了承を得た。

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