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7回)
議事概要

1. 日時・場所

日時：令和5年2月17日（金） 14時00分～16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、庄治様(大浪委員代理)、荻野委員、神余委員、北澤委員、教学委員、高橋委員、西貝委員、野口委員、松元委員

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、独立行政法人 製品評価技術基盤機構、一般社団法人 日本自動車工業会、一般財団法人 日本品質保証機構

経済産業省：大臣官房 上村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

積水ハウス：藤岡様

ダイキン工業：蓮池様、藤本様

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-SSF 適用実証報告－医療機器－（松元委員からの発表）

参考資料1 IoT セキュリティ・セーフティ・フレームワーク Version 1.0 適用実証報告書

参考資料2 IoT セキュリティ・セーフティ・フレームワーク Version 1.0 適用手順書

4. 議事内容

●機器・システムの運用・管理を行う者の能力に関する確認要求（第3の観点）及びその他、社会的なサポート等の仕組みの要求（第4の観点）について

- 第3軸の第3の観点では、主に人材の話について書かれているが、人材に加えて、機械と組織の3点についての認定や認証も重要と思う。

- リスク分析におけるリスクの影響を受ける者の分析をこれから改善していく必要があるのではないかと感じた。リスクの影響が瞬く間に広がったときに何が起こり得るかは今までと全く違った状況だと思うので、影響を受ける者の知識を持った分析チームを組まないといけないと感じた。

・ IoT-SSFの有効性は、フレームワークそのものの有効性だけでなく、このフレームワークを適用する者やチームの能力をどうやって確保するかということとセットだと思う。さらには、重要なセキュリティ対策がたやすくできるものでもないという認識を持たないと、IoT-SSFは不完全になると思う。

・ 第3軸の第3の観点でいきますと、色々な損害が起きたときに、IoT-SSFでは多くのステークホルダーが存在する中、発生した損害が誰の責任かを明確にすることは非常に難しいと思うが、今後はその線引きを明確にしていくことが必要ではないかと感じた。

・ 第4の観点で保険制度の必要性が論じられているが、保険制度である以上、誰かが保険料を負担しなければならず、その負担をユーザに求めるのか、事業者に求めるのか、または、自賠責のような公的制度にするのか、そこの論点もあると思う。

・ 3番目の適用実証は産業機器向けの事例として分かりやすく、産業機器向けにIoT-SSFが使えることを示していると思う。一方で、1番目の適用実証でいうと、どのように専門の運用者ではない住まい手に第3軸の第3の観点を適用するかということがポイントになると思う。最近は消費者に対して情報提供する、消費者向けのサポート窓口を開設する等の動きもあるが、消費者向けの機器において、第3軸の第3の観点の取り扱いが整理しづらいことが今回の適用実証で見えたと思う。

●IoT-SSFについて

・ IoT-SSF でステークホルダーという概念をしっかり定義したのはリスクを考える上で有効だと思う。また、IoT-SSF の構造からして、IoT-SSF は基本的に事業リスクを考えるフレームとする方が適しているのではないかと感じている。今後は、社会情勢等にスピード感を持って対応できるフレームワークにすることが課題と思う。

・ ある事象が生じたときに誰がどの程度責任を負うのかということについて、それぞれのステークホルダーが個別で結んでいる契約の内容を誤解して事業リスク等を誤って評価することがあると、正確なリスク評価ができない可能性があると思う。

・ IoT-SSFにおいて、インシデントの起こりやすさをそう位置づけるかが難しいという指摘がされているが、前例があるインシデントであれば、ある程度定量的な判断ができる可能性がある。だたし、未知のインシデントや前例のないインシデントも想定する場合は、定性的な判断をせざるを得なく、考慮することが難しいと思う。

・ インシデントの起こりやすさを考慮せずともIoT-SSFを適用すること自体が有用であったかどうかということを示すべきではないか。

・ 様々な観点があり、整理が必要だが、具体的な事例の検討をしていく中で、IoT-SSFが有用と示すことができていてよい。

・ 本当に機器のリスクが無くなったのか、あるいは機器に対して攻撃できないのかということを検討する必要があるが、未知のインシデントが起きるかは誰も予見ができない以上、議論がまとまらないのではないかと思う。

●IoT-SSFの活用、適用について

・ IoT-SSFのプロモーションも併せて考えないといけない。セキュリティ対策は重要と認識しているが、IoT-SSFの内容を関係部門の幹部が理解しないと採用されにくくなるので、IoT-SSFの内容を分かりやすくまとめた資料を用意していただけるとありがたい。

・ インシデントの起こりやすさやレピュテーションリスク等の議論については、予めテンプレートを用意しておくと、リスク分析に要する時間やコストが減るのではないか。

・ 運用やオペレーションに依存する部分が多いというところがセキュリティの特徴なので、工業会等でティピカルなものを決め、関連するベストプラクティスやリコメンデーションを作っていき、細部はそれぞれの事業者、アセットオーナで進めるということであればできるかもしれないが、各工業会でセキュリティの専門家が不足している。

・ サイバーの対策もフィジカルの対策も両方とも必要で、両方のバランスをとれていることがIoT-SSFの良い点と思うので、インシデントの起こりやすさよりもこの点に注力して特徴を出していった方が良いと思う。

・ 優先順位や価値観はステークホルダーごとに違うので、リスク情報や対策情報をステークホルダー関係者と共有することが大事だが、基本的にリスクマネジメントはマネジメント主体が責任をもって行うものだと思う。

・ スマートホームやビル、工場、宇宙といった産業分野毎にガイドラインを作られていると思うが、IoT-SSFで触れられているインシデントの起こりやすさやステークホルダー、責任分界点等は産業分野毎でも検討してもらうと良いのではないか。

・ 医療分野では、国際規制フォーラム等の影響もあり、ステークホルダー間の情報共有の重要性は近年認識が進んできているかと思う。医療分野でIoT-SSFの考えを広げていくために、引き続き検討していきたい。

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