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5回）議事概要

1．日時・場所

日時：令和3年11月29日（木） 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、岩崎委員、綿田様（大友委員代理）、荻野委員、梶屋委員、神余委員、北澤委員、宮寺様（教学委員代理）、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、防衛装備庁、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、一般社団法人 JPCERTコーディネーションセンター

経済産業省：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技術戦略企画調査官、塚本サイバーセキュリティ課長補佐

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（抜粋）

4．議事内容

事務局から資料3に基づき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。

●ユースケースの作成について

・ ガス給湯器の回復困難性の度合いが大、経済的の影響の度合いが小となっているが、マッピングするにあたり、損保や生保、判例を調査し、参考にしてほしい。回復困難性の度合い、経済的の影響の度合い、セキュリティ・セーフティの観点からどのようなレベルのセキュリティ確保が必要となるか、対策の深さは違ってくるというメッセージを出すべきだと思う。

・ これからのDXの社会では、どのレベルのセキュリティを目指し最終的にどこまで投資するかと、最終的なユーザ責任も含めて考える必要があるというメッセージが出ると良い。今までのように全て同じレベルで対処するのではなく、イン

フラや機器の重要度によって、対処するレベルが違うという構造を見せた方が良いのではないか。

- 回復困難性の度合いと経済的影響の度合いの大中小には例外があることと、相対的な評価であるということを伝えると良い。

- 脅威分析やリスク評価について、「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」の別冊2やIPA 「IoT開発におけるセキュリティ設計の手引き」を参考にしていただきたい。守るべき資産があり、どの資産を守っていくのかを決め、その上で、どこに攻撃ポイントがあるのかを示し、どのような脅威が発生するかというモデルがあると思う。この考えを押さえたうえで、文書化していただきたい。

- 対策をする方ばかりが重要視されているような書き方になっているので、被害を受ける方を考慮した工夫をして資料を作成した方が良いのではないか。守るべきユーザと、ユーザに対してどんな危険性があるかを最初に述べないといけないのではないか。

- どのような観点でユースケースを書いているかを明確にしておくことが最低限必要だと思うが、そのうえでエクザンプルとして、どのような観点のものを取り上げるべきかに課題があると感じる。

- ユースケースの選定の考え方を工夫し、もう少しバラエティに富むユースケースができないか。

- 対策を実施すべき主体を決めるにあたり、まずステークホルダーが責任分担、リスク分担について話をするというプロセスも入れた方よいと思う。

- ガス給湯器に限らないが、挙げられているユースケース候補で、ステークホルダー間の関係が特に難しいものがあれば、それをユースケースとしてはどうか。

- 機器の設計者や全体設計者からユーザまでセキュリティ担当者が幅広くいるという事例としてガス給湯器、1回のトラブルで多くのステークホルダーが絡む事例としてプラント設備を選定したという説明で十分ではないか。経済的影響の度合いは、誰の視点で見るかが大事で、説明の仕方は工夫した方が良いのではないか。

- どの程度のセキュリティを守ったら良いかの考え方はメーカの分野によって違うが、最近は、つながる機器としてセキュリティの考え方もつながることを意識しているので、このようなユースケースの事例は、良い参考資料になると思う。

●脆弱性、リスク、責任などの考え方について

- インシデント、事故として、ガス漏れや水漏れなどが抜けている。セーフティ、セキュリティの観点からセンサーやアクチュエータが正常に動かないが故に事故が起こってしまうというところが本ユースケースでは汲み取れていない。アクチュエータで制御が行われなかった、完了しなかったものがインシデントになると考える。つまり、どのような観点で「回復困難性の度合い」、「経済的影響の度合い」を導きだすのかを、ユースケース例で示した方がよいのではないか。

- 脆弱性があるから攻撃を受けるということではなく、攻撃されやすいということもあり、説明の仕方を考えた方が良いの

ではないか。また、これからのDXの社会では、脆弱性がなくても攻撃されうるということをメッセージとして出していかないといけない。加えて、サイバー・フィジカルの問題は攻撃を前提に考えているが、故障や誤作動というのは、攻撃以外の設計、運用ミスの中でも起こるもので、第2層でも攻撃だけを対象にして考えるところから脱局しないといけないのではないか。

・ 問題は機器にあるという考え方に見えるが、スマートホーム全体の設計者、スマートホームを供給する事業者の重要さを階層的に見ておく必要があると思う。また、ユースケース案ではスマートホーム向けのIoT機器の事業者が重要だというように見えるが、住まい手自身が利便性と危なさを理解して選択することも考えられ、全責任がIoT機器の事業者にあるのではなく、それぞれに負うべき責任があるという図にしないといけないと思う。

・ ユースケースの候補には、ガス給湯器やドローン、ピッキングロボット、センサーなどが挙がっており、それぞれリスクの大きさも変わってくる。IoT機器を導入する現場というパラメータや、色々な機器の故障が相まって、リスクの大きさの計測が非常に難しくなるのではないか。また、機器の特定方法では、機器・システムとまとめて書かれていたが、リスクの大きさを算定する段階においては、分けて考えた方が良いかもしれない。産業界で使われると経済的影響が大きくなるといったリスクの大きさを予測できれば、学問的に面白く、実用的にもなると思う。

・ 回復困難性の重大なダメージの基準に、プライバシーとセーフティの観点が書いてあるが、それらを混ぜて考えるのは難しく、分けて考えた方が良いのではないか。また、IoT-SSFにおける想定される脅威に応じてそれぞれのリスクの大きさを分析していると分かりやすい。リスクのレベル、リスクの大きさが分かるようになると良い。

・ 実際に講じる対策にマストのものがあるかを示さないのであれば、全部講じなさいという意味ではないことをメッセージとして伝えた方が良い。また、主に対策を実施すべき主体を決めるのは難しいのではないか。ステークホルダーが複数いる中で、責任分担、リスク分担は、実務でははっきりしないこともある。

・ リスクの大きさは使い手によって変わってくる。住まい手が仕様書と手順書を把握せず、想定された用途・方法で使用しなくても誰も咎めることができず、住まい手で設定するものには、現時点ではかなり大きなリスクがある。

●その他

・ 経済的影響という言葉は違和感がある。ガス給湯器の遠隔操作の経済的影響の度合いはどこまで考えてこのような評価にしているのか。経済規模などに観点が偏っているのではないか。

・ 実際に利用する局面になってわかる課題があると思うので、経済産業省主催の研修会などで普及することが重要だと思う。

・ まずはユースケースをきちんと作り、その過程でいくつかのユースケースにIoT-SSFとのギャップがあれば、そのギャップについてフィードバックをするというように作業時期をずらした方がよいのではないか。

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