産業サイバーセキュリティ研究会WG1分野横断SWG(第5回)
議事要旨

1. 日時・場所

日時:令和2年9月11日(金) 16時00分～18時00分

場所:TKP虎ノ門駅前カンファレンスセンター ホール9A／オンライン併催

2. 出席者

委員 :佐々木委員(座長)、石原委員、岩﨑委員、大久保委員、大友委員、岡田委員、粕谷委員、川口委員、菊池委員、桑名委員、後藤俊二郎委員、後藤里奈委員、古原委員、谷委員、中尾委員、田島様(平田委員代理)、洞田委員、山田委員、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: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層タスクフォース及びソフトウェアタスクフォースの検討状況等について

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について

セキュリティとセーフティを組み合わせた取り組みとして先進的。IoTの標準や規格、ガイドラインが乱立気味だが、それぞれに対応するときにガイドしてくれるようなものだと尚良い。

特に中小企業においては、セキュリティに関する情報へのアクセスが限られているとどうしても限界があり、情報が豊富であれば相乗効果も期待できる。IoTデバイスのセキュリティを検討する上で情報の共有や活用についても検討されることに期待。

フレームワークを運用するにあたり、解釈の部分の議論が必要。ステークホルダー間で合意する必要があるとの記載があるが、実際には非常に難しい。合意をするというのは具体的にどういう風な形で誰が何をするなどということを解釈し、一塊の業務に落としていく、といった検討を分野横断的に行う必要がある。

インシデント発生時には、システムを復旧させることが目的ではなく、ビジネスをどう継続させていくかが重要で、システムのインシデント対応だけでは解決できない問題がある。その点で社会的サポート等の第4の観点も含めて検討することは

重要であり、深堀に期待。

IoTが今までのセキュリティと一番違うのは、エンドユーザーとして多くの一般の人がいる点。NIST IR8259にも顧客というキーワードがあるが、顧客を念頭に設計することが重要。IoT-SSFでもそれが踏まえられている。

安全とセキュリティはなじみが薄いところがある。場合によってはセキュリティ分野においても安全におけるPSEマークやSGマークのような新たな仕組みが必要になるかもしれない。

IoTのセキュリティにまつわる国際標準の関係では、米国は、NIST IR8259がベースにIoTセキュリティ&プライバシーに係るISO/IEC 27402を提案し、議論を強力に推進。日本は、IoT推進コンソーシアムが作ったガイドラインをベースにISO 27400を推進。さらにCPSFをベースにした提案を日本から行っており、TRとして進めようと議論しているところ。

●ユースケースの検討について
インシデントの被害の大きさと、経済影響で整理するのは非常に良いやり方。他方で、実際にどういうインパクトが起こるのか、かなり多様な軸の切り分けがあるため、業界毎の検討が必要。業界に閉じないものは分野横断SWGで扱うことも考えられる。

フレームワークを活用するのにベンダー目線だけでなくユーザ目線でも考える必要があるが、ユースケースを考えるにあたって、ビルはユーザ目線からいろいろ入っていたりするので最初に検討する対象として適切かもしれない。

実際の活用にはユースケースが重要。工場をひとつの制御システムと捉え、IoT機器のそれぞれの役割や、それを使う運用者が何をしないといけないのかなどを考えると、良い例になるのではないか。

セクター・バイ・セクターでの検討から、将来的には、クロスインダストリーに展開していくことを期待。

異なる分野がつながる時にセキュリティを検討する枠組みとして有益。今後、電力やモビリティなど様々なユースケースが出てくると考えられるが、ユースケースが融合してさらに複雑化することも想定される。そのような中で、IoTに関するセキュリティ対策を一律に規定していくのは難しいため、柔軟に対応できることが重要。

多重の委託関係など、ステークホルダーとサプライチェーンの整理が重要。関係者間の認識の違いによる設定ミスなども多くなってくる。ユースケースにおいて関係者の責任分解等も含めた深い議論が行われることを期待。

ユースケースは非常に重要。IoT-SSFは、技術だけに留まらずライセンスやその先の保険等絡んでいて、実際に脆弱性があった際の対応について、ライセンスに基づく責任や財務的にどう転嫁するのか等、総合的に考えられる。いくつか具体例を挙げてそういう議論ができれば良い。

●ソフトウェアについて
脆弱性対応に関して誰にコンタクトを取るべきかという窓口の問題がまだ解決できていない。誰に連絡を取れば適切に対応できるのか、コンタクトポイントを適切なところにおいて伝えていくことが重要。

OSSの利活用が増える中で、もはやシステムについて1社ですべてを対応できない。中小企業を含むサプライチェーンにおける対応等の課題が重要になってくる。海外の動向も含め、低コストで有効な管理手法など、サプライチェーン全体に展開していけるような検討が重要。

脆弱性対応は大企業でも大変であり、中小企業には尚更。ヒアリング成果が中小にも参考になることを期待。

車載機器にもOSSを使う機会が増えており脆弱性管理は大きな課題となっている。個社での活動にとどまらずISACなどでも議論しているが、機密の問題など情報共有に課題。ISAC等における脆弱性管理等についても議論がなされることを期待。

●分野別トピック
電力業界では、NISTのCSFの適用に向けカスタマイズ作業等の準備をしているところ。IoTについては、点検やモニタリングの効率化、家庭におけるスマートメーターやその先のIoT機器など、様々な分野にIoT技術を適用していこうと挑戦中。IoT-SSFについても自分たちのモデルにうまく適応できないかアプローチしていきたい。

AIセキュリティに関し、産総研が機械学習品質マネージメントガイドラインを発行している。機械学習の品質として、それを利用する際の品質なのか、外部的に求められる品質なのか、そもそも機械学習が持っている品質なのかというところで分類して考え方を整理したもの。

ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインはチェックリストとして機能しており、設計段階での活用のみならず、それを見た色々なメーカーが新しいソリューションを開発する状況も生まれているが、なかなか社会実装が進んでいないという課題がある。これはアセットオーナーや投資家に届いていないため。ユースケースとして、セキュリティも含めて適切に管理されたビルのアセットの価値が向上することが示せればエコシステム的に価値がある。

防衛産業に関し、米国ではCMMCと呼ばれるセキュリティの認証制度が正式に動き出した。NIST SP800-171のような一律の規程ではなく、小さい企業でも少しレベルを下げて取得すれば防衛省と契約できるという制度であり、リーズナブルで参考になる。

資料5で事務局から示されたフレームワーク案を産業サイバーセキュリティ研究会ワーキンググループ1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