産業サイバーセキュリティ研究会
WG1分野横断SWG(第3回) 議事要旨

1. 日時・場所

日時:平成31年3月27日(水) 14時00分～16時00分

場所:経済産業省別館 2階 218各省庁共用会議室

2. 出席者

委員 :佐々木委員(座長)、青木委員、石原委員、大久保委員、岡田委員、粕谷委員、川口委員、桑名委員、後藤(俊)委員、後藤(里)委員、古原委員、下村委員、谷委員、中尾委員、田島様(平田委員代理)、舟山委員、洞田委員、吉田委員

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:奥家サイバーセキュリティ課長、土屋サイバーセキュリティ課企画官

3. 配付資料

資料1 議事次第・配付資料一覧

資料2 委員等名簿

資料3 サブワーキンググループ等の設置・検討状況

資料4 サプライチェーン・サイバーセキュリティ等に関する海外の動き

資料5 第2回パブリックコメントで寄せられた御意見に対する考え方(案)～概要～【非公開】

資料6 第2回パブリックコメントで寄せられた御意見に対する考え方(案)【非公開】

資料7 サイバー・フィジカル・セキュリティ対策フレームワーク(案)【非公開】

資料8 サイバー・フィジカル・セキュリティ確保に向けた研究開発の動き【非公開】

4. 議事内容

事務局から資料3～7に基づき説明、石原委員から資料8に基づき説明を行った後、自由討議を行った。委員からの意見は以下のとおり。

(1) セーフティとセキュリティについて

- セーフティとセキュリティについてのコメントだが、ビルの立場で発言するとBCPは大きなスケールになる。地震、免振等のモニタリングは専門業者がいる。今回のビルガイドラインではあえてフィジカルをスコープから外している。セーフティはどの範囲まで考慮するのか、その辺を明らかにしていただきたい。
- 本SWGの議論では車の話しが良く上がるが、セキュリティの視点からリスク分析を掛けていったときに、インシデントがあって、インシデントのインパクトがセキュリティについて出る場合とセーフティについて出る場合がある。セキュリティの世界でセーフティの議論をする場合は、そういう形で議論をしている。ただし、セーフティとしての議論では、もっと広くなる。さらにトラストワースネスの議論はもっとスコープが広くなり、プライバシーやレジリエンスも含まれる。これら全部を議論するとこの分量では収まらない。そういう意味で、今回のアプローチは良く、セキュリティの観点から、その文脈でセーフティを考える範囲が適切である。トラストワースネスリストは、少しミスリードされるかもしれない。

(2) プライバシーについて

- プライバシーに関して、日本は個人情報保護法があるが、プライバシーのルールと今回のフレームワークとの関係をはっきりさせた方がいい。

(3) セキュリティ対策について

- 走行中に攻撃をリアルタイムで検知するという発表が学会であったのだが、その場合のセキュリティ対策はどうするのが適切なのだろうか、止めるべきなのか、ネットワークを切り離すべきなのか、安全に停止する方法はあるのか、考え方を整理する活動が必要であり、何らかの指針が求められる。
- 車のセキュリティインシデントを考える場合、インシデントのせいで、カーナビが黒くなる、エンジンが止まる等の影響が発生するかもしれないが、これらは今まで品質問題として経験し、学んできている。つまり、セキュリティから発生するハザードが、既に経験済みの事象である場合、感覚的に8割は、品質問題として考えることができるのではないか。
- パブリックコメントに関して、プロファイリングとデータ保護について、プロファイリングは産業分野ごとの議論が中心であると考えるが、データは分野を横断する。自動車会社としては、会社、製品、車とこの3つを守ることが大方針。将来に向けてつながる車になったときにモビリティプラットフォームにおいてどうセキュリティを確保するのか、本SWGではいろいろな業界で集まって相互に議論しているのでその点も期待している。
- フレームワークには、セキュリティ対策が具体的に書かれているが、具体的に書かれていると、改訂の問題もある。セキュリティ対策のテクノロジは日々進歩する。改訂について明確化すべきであると考える。
- RA3の脅威を特定するという表現は一般からは難しいと思う。自社への影響を特定する等へ表現を直すと良い。
- セキュリティは、一番弱い箇所が狙われるので、トータルで確保することが重要。

(4) フレームワークの活用について

- フレームワークの議論は抽象度が高くなりがちであり、SIPの実証実験など、ものを作りながら考えると議論が具体的になるので、そこでフレームワークを使えればいいと考える。
- フレームワークの活用に関して、SIPは国のプロジェクトでやっており、一部NDAの関係もあり、公開できるところとできないところがあるが、いろんな形で検討できればいいと思う。
- データインテグリティもフレームワークにあると思うが、トラストの点からも検討を進めていただきたい。日本からやっていくことが大事。

(5) 今後の取組みについて

- 今後の話しだが、それぞれの分野のユースケースに基づいて、共通のテーマを捉え、共通部分を見ていくフェーズになると思うが、省庁間の連携も益々必要になると考える。
- フレームワークを策定後の活動をどのように考えているのか。ISACでどのように活用するのか考えることも重要。重点14業種以外でも中小企業もあり、どう取組むのか、クロスインダストリーでデータ継承なども検討が必要であると考える。
- セキュリティを考えるときに、モデルが必要であり、このフレームワークの標準化についても考えるべきであ

る。

- ソフトウェアセキュリティについては、ソフトウェアをどう信頼するのかが難しい。ソフトウェアのベンダが信頼できれば大丈夫なのだろうか、ソフトウェアだけでなくチップまで確認すればいいのだろうか、考慮すべき点は多くスコープが限りなく広がる。ただ、これはきちんと議論すべきことだと認識している。

最後に、平成31年4月のWG1で報告するフレームワーク案を座長一任とすることで委員一同から同意を得た。

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