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(制度・技術・標準化)(第5回) 議事要旨

１．日時・場所

日時：平成31年4月4日（木）　14時00分～16時00分

場所：経済産業省　本館17階第1特別会議室

２．出席者

委員　　：佐々木委員（座長）、澤井様（岩見委員代理）、上原委員、江崎委員、太田委員、岡村委員、片山委員、九野委員、小松崎委員、白石委員、其山委員、髙倉委員、坂委員、平田委員、松尾委員、松本委員、渡部委員

専門委員　：瓜生専門委員、坂下専門委員、田中専門委員

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、金融庁、総務省、外務省、文部科学省、厚生労働省、農林水産省、国土交通省、防衛装備庁

経済産業省：商務情報政策局　西山局長、大臣官房サイバーセキュリティ・情報化審議官 三角審議官、奥家サイバーセキュリティ課長

情報セキュリティ大学院大学： 後藤学長（内閣府 SIP「IoT社会に対応したサイバー・フィジカル・セキュリティ」 プログラムディレクター）

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 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～

資料6 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）

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）

資料8 「サイバー・フィジカル・セキュリティ対策フレームワーク」策定後のＷＧ１の進め方（案）

資料9 IoT 社会に対応したサイバー・フィジカル・セキュリティ

４．議事内容

冒頭、西山局長から以下のとおり挨拶。

・ 国際面では今年、G20 の会合を開催することになっている。それを踏まえて今年１月に安倍総理が出席されたダボス会議で、一つのコンセプトとして「データフリーフロー・ウイズ・トラスト」、信頼性を担保した上でのデータ流通が打ち出された。

・ 元々、一つのあり方としてデータフリーフローというものがあったが、まさに昨今のサイバーセキュリティ、あるいはプライバシー等の単にデータが流通すれば良いというわけではなく、産業サイバーセキュリティ研究会で議論いただいているように、サイバーとリアルの世界が一体化していく中で、データフリーフロー・ウイズ・トラストを一つのお題として様々な施策を進めていくことになっている。

・ ダボス会議の演説の中で総理は、特に、WTO の場で様々な交渉を進めていく、大阪トラックと言われまし

たが、サイバー、あるいはリアルの世界が結合していくことはファンダメンタルな面ですので、それらを支えるインフラすべてを WTO で議論できるわけではないが、3 月に開かれた G20 の姉妹会合である B20 の会合でも次世代のデータガバナンスのフレームワークが必要だということを提唱された。まさに、産業サイバーセキュリティ研究会の WG1 で議論いただいているサイバー・フィジカル・セキュリティ対応フレームワークは、こうした国際的な環境の中で新しいデータガバナンスのフレームワークを作ろうということの一つとして取り組んでいる。

- もう一つは、前回の会合と前後するが、昨年末に久々に総理以下、各閣僚が出席する IT 戦略本部が行われ、様々なことが議論された。その中で一つの大きなメッセージは、サイバーセキュリティを含めた対応について個々の省庁、個々のセグメントだけではなくて横割り的に対応する必要があるということについて議論が行われ、方向性が打ち出されたということ。それを踏まえて今年の 6 月頃に、データ、デジタル周りの政府の様々な政策について短期中期を含めて、IT 政策大綱として方向性を打ち出そうとしている。
- その中で、まだどのように実施するかは決まっていないが、本日御議論いただくサイバー・フィジカル・セキュリティ対策フレームワークは、特定のセグメントに限らない包括的にサイバーセキュリティに関る事象を把握できる、あるいは具体的な対策を検討できる一つの基盤になることができると思っている。また、国内政策のこれからの議論においても、一つの大きな柱になっていくと思っている。
- 国際関係、後で追加的な説明があると思うが、国際的な動向や国内的な動向の中で益々、こうしたフレームワークの必要性が高まっていることと思っている。本日も熱心なご議論をお願いしたい。

事務局の奥家サイバーセキュリティ課長から、配布資料の確認、委員の出欠の紹介に続き、以下の配布資料について説明。

- 資料 3 に基づいて、サブワーキンググループ等の設置・検討状況を説明。
- 資料 4 に基づいて、サプライチェーンサイバーセキュリティに関する海外の動きを説明
- 資料 5 に基づいて、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について説明
- 資料 8 に基づいて、今後のＷＧ１の進め方を説明。

また、後藤学長から、資料 9 に基づいて、サイバー・フィジカル・セキュリティの確保に向けた研究開発について説明があり、その後、以下のとおり自由討議を行った。

○片山委員

- 事務局から今後のスケジュールの話があったが、今後 1 年間のスケジュールを簡単に教えていただきたい。
- パブリックコメントについて、我々の方からコメントしたところも修正いただいているようで感謝したい。
- 奥家課長もおっしゃっていたが、EU の認証フレームワークについては、これからどのようなフレームワークになるか気になるところ。2 週間後に EU サイバーフォーラムに行くので EU 関係者の声などを探ってみたい。
- トラストに関しては、個人的にも会社的にも賛成。データフリーフロー・ウイズ・トラストも理解できる。ご存知かと思うが、トラストについては一部に異なる解釈が存在する。昨年の 11 月、フランスのマクロン大統領がサイバー空間におけるトラストセキュリティという宣言をしている。日本政府は当然サポートしているが、一部の国ではサポートしていない。「トラスト」という言葉は、一部の国では解釈の仕方が違うことに留意して欲しい。

○奥家課長

- 可能であれば、フレームワークはこの会合を以って、バージョン 1.0 として 4 月中にリリースしたいと思っている。これに続く形でタスクフォースを 3 つほど、メンバ等について御相談させていただきながら速やかに立ち上げていきたい。
- IoT 周りのところは、認証フレームワークや英国の行動規範があって、一方で第 2 層の世界では、Functional Safety と連動させた上で、物やシステムが生み出す価値のところをみないといけないので、セキュリティだけではなく、Functional safety とどう絡むかという議論を立てられるようにしないといけない。
- ソフトウェア周りのところは、アメリカは Software Component Transparency という議論を開始しているので、キャッチアップしていかなければいけない。ゆっくりは考えられないと思っている。
- 各 SWG では、ビルはパブコメ中で、4 月は難しいかもしれないが、5 月にはバージョン 1.0 をリリースしていきたい。ビルは関係者の中で、こうした活動を継続するための体制も議論している。その他、スマートホーム SWG では、今年度中にガイドまでいきたいと議論している。それぞれの SWG は具体的な形、今年 1 年の中でマイルストンを建てている。個別の動きは WG1 で報告をさせていただいて、色々なコメントを頂いて取り組みに反映するという形でこの 1 年を進めていくことができたらと思っている。

○小松崎委員

- 悩み相談のようになるが、スマートホームを 1 年間やってきて、サプライチェーン等、我々にとって一番馴染みやすいところを考えているだけでは、結局 Society5.0 が目指す、サイバーとフィジカルが融合した新しいサービスというのがなかなか具体的には登場してこない。バリュークリエイションプロセスについては、共感しているが、バリューを作るためのチェーンと考えると、サプライチェーンとは多少違って、供給する側だけではなく享受する側の視点で見ていくことも必要。そうするとリスクマネジメントの見え方も変わってきて、諸外国から非常に良い反応というのも腑に落ちる。
- そういう観点からいくと、今日の後藤先生の話は、絵の右側にもう少し生活などを見せる必要があると思う。供給側にフォーカスするのは至極納得できる話だが、それらのアクティビティが何のために行われているかというと、日々の生活のためであり、生活の主たる基盤になるのが家庭であると、スコープを少し広げたら、スマートホームの WG の議論は、途端に大変なものになった。
- したがって、スマートホームは、2 段構えでやっていこうということで、一つは具体的なガイドラインを期限までに作り上げること。これは皆様が苦労して作り上げたフレームワークに準拠して、それを具体的にブレークダウンして実用性に富んだものを作っていくことを目標に定めている。
- もう一つは、このために検討していると言っても過言ではないライフ、生活、家庭、これらに対する取り組みが従前と同じでは Society5.0 には届かないと 1 年間の議論を通じて感じている。JEITA では、スマートホームは、いったい何なのだろう、スマートであるかは自分が決めることではなくて、他人が決めるものだという点からいくと、言葉を変えると、社会から見て家がスマートになることによって、非常に大きなベネフィットが出てくる、それはヘルスケアであったりゴミの問題であったりする。逆の言い方をすると、我々は Society5.0 を実現するための一番の基盤となるのが家庭と考えているので、生活の場である家庭がどのようになれば良いのか、それを実現するための技術基盤は何か、どういうところと連携していったらよいのかなど、社会サービスから見た家庭という切り口で、技術をもう少し異なる角度から見ていくという活動を続けていくのが今期の大きな流れ。
- 我々の参考になるような情報等あれば、是非頂けるとありがたい。生活や社会をもう少し全面に出すことが大事なのではと思って取り組んでいる。

○岡村委員

- 資料 4 で紹介いただいたアメリカの大手電力会社が、CIP 基準違反で、罰金を支払ったということだが、これは業法違反の話か、それとも一般的な話か。
- 関連して、基準として取りまとめられた技術について、次の段階では実装してもらうためにどうしていくか、すなわち実効性をどのように確保するかが重要な課題であるのは言うまでも無い。通常は、何らかのインセンティブとペナルティとの組み合わせという形で行われるように思うが、関連して法制度や標準化対応なども、当然、視野に入ってきていると思う。例えば、サプライチェーンを取り上げると、経済産業省が所管する法律の中では、不正競争防止法があり、その中に、これまでは営業秘密をスタンドアロンで、自社の秘密を守っていくことが、中心となってやってきた。昨年度に成立した改正で、限定提供データという、どちらかというと、サプライチェーンが使いやすい枠組みを作ったが、今後のインセンティブとペナルティという点でどのように考えていくべきか、一層踏み込んで考えていく必要があると思う。
- オープンになっている情報なので申し上げるが、NISC で SWG を作って、今の法制度が、果たして合っているのか、についてもう一度検証してみるというプロジェクトを開始した。この背景にあるのは、せっかくサイバーセキュリティ基本法ができたにもかかわらず、各省庁の責務にギャップがあり、そろそろ制度整備が十分かを考えなければいけない時期にきている。
- また、各業法の中では様々な基準があるが、どちらかというと従前の「メンテナンス」的な発想に業法が留まっていることが多い。一部見直している省庁はあるが、電力業界などはスマートメーター、あるいはサプライチェーンが大きな要素を占める中で、メンテナンス的なものではなくセキュリティまで盛り込んだものを施行するような形になっているのか、そういう点も今後の検討課題になる。それを視野に入れつつ検討作業を進めていかなければいけないと思っている。

○奥家課長

- Duke Energy のケースは、業法か一般法かという区分では、業法に当たると思われる。アメリカの場合は、特に電力は、各州にある公益委員会で審査等が行われるが、連邦ベースで統一させなければならないというのがあり、実質的に FERC という機関が州で行われている規制を取りまとめて整合性を取る役割を果たしている。法律上、FERC が規制のようなものを作るに当たっては、電力業界の研究開発機関のような所がある場合には、技術的なアドバイスをそこに委託する。それが良ければ業法の規制に持ち上げるということで、官民の間で、それぞれの能力を活用した形で妥当なもの、例えば、民間では絶対にやらないこともあるわけで、かなり柔軟な形で規制を動かし効果的にしている。官だけで頭でっかちで作るのではなく、民間が創意工夫することで、公益的でコストも抑えられた案が上がってくる仕組みを元々作っている。
- この FERC が作ったものに対して NERC がお墨付きを与える、認証を与えるという形でルールという形になる。この基準違反をすると罰金ということになっている。今回のケースで言うと、Duke Energy は自己申告を行っている。実態は 8 割が自己申告。モニタリングをして違反として発見されるケースは 20%。これはペナルティの大きさが変わるという部分の他に、自分たちの間で、これがベストと決めたものを守らないこと自体が企業倫理上、問題だろうという形で理解されているようで、基本的に CIP は自らが合意して作ったもので、それを守らなかった場合はどんどん申告していくべきだという形に基づいている。それで 20 万ドルの罰金を払うというのは、ある意味普通で、アメリカの電力はそのような構造になっている。
- 頂いたコメントは、今後、こういうシステムが参考になるのではないかということも含めて、ご質問いただいたのではないかと思う。まさにご指摘の通り、このフレームワークを作る中で、もしくは WG2、WG3 の

中で、サイバーフィジカルが一体化した社会において責任分界点をどうするのかという話があった。結局、データを共有する中で、どちらに責任があるかは不明確になっていく。責任分界点がきれいに切りきれない中で、責任をシェアする、ベネフィット、コストもシェアする、そういう社会になっていくときに、いったいどのようなルールのセッティング方法が良いのか、そうしたところまで視野に入れていかないといけないだろうというのが、こちらの WG1 で議論させていただいた中で浮かび上がってきた論点だった。

- その中で、TF でのデータカテゴリーに基づいたリスクアセスメントは、その典型例と捉えている。御指摘いただいたように不正競争防止法の中で限定提供データという区分ができて、営業機密に準じた形の法的保護を与えるという考え方に基づいた場合に、法的保護に値する条件とは何か。逆に言うと、法的保護に値する条件を皆がクリアしないと、法的保護を与えられるデータの部類にはならないことになる。データのカテゴリ毎にセキュリティ要件を設定して、それを皆が満たすという、ある意味責任のシェアリングの話と思うが、そういった議論をしていかないといけないと思っている。
- 法制度のあり方もお話しいただいたが、各業法の中には電事法の法律、電力の世界では省令とか告知レベルになってくると思うが、ここではセキュリティ対応を要求しているが、他の分野では、まだそこまで行っていない。一方的な押しつけ型の規制体系で、本当に合理性があるのかも議論しなければいけない中で、まさに商務情報政策局として Society5.0 を考えたときに「法とコード」というものも西山局長を中心に議論している。ある意味プロアクティブな形で、合理性があり、効果が高いものを抜き出したものについてコミットメントしたら、それをコミットメントした方は破ってはいけない、コミットメントしたのだから逆にきちっと守る仕組みを考えているという FERC と NERC の考えに近い議論が今後行われていくだろうと思っている。
- このフレームワークを議論させていただいていく中でサイバーフィジカルが一体となっていく社会はいったいどうなっていくかが、比較的見えてくる議論が多かったと思っている。この点は TF 等で引き続き議論していきたいと思っている。

○岡村委員

- 個人的な思いとしては、法規制で厳罰化を推し進めようという意味で申しあげているわけはなく、もちろん、マルチステークホルダーの形で議論することも重要。頑張ったものが高く評価されるインセンティブを与えることも大変重要になるのではないか。従って、あまり規制というよりは、高く評価するという形になるようなスタイルを考えて欲しい。
- それと共に、伝統的な方法ではあるが、例えば、税制優遇などメリットが生まれる部分についても、総合的に考えていかなければいけない。
- もう 1 点、あまり窮屈になって、イノベーションが阻害されることになると逆効果なので、あくまでも、信頼性が高いところはマーケットで非常に評価される、他方で、水準を守っていれば責任を問われない、というようにして頂きたい。そういう形のものが確立していく方向であればイノベーションを阻害しないので良いのでは、と思っている

○太田委員

- フレームワークがまとまることで、産業界、特に、アメリカを中心としたレギュレーションが様々な形で現場にて求められていて、それに対して日本としてはこうする、ということを示す点で非常にありがたい。
- 次につなげていく話として、今回、作っていただいたフレームワークの実装を進めると、ISO 27000 ベースで進めている産業界にとって、かなり大きな変更や変革をしないとついていけないところがたくさんある。

フレームワークはできたのだが、社会実装はこれからどこまで進むかという面を含めて、難しいものがたくさんあると認識している。さらに、新しい流れとして西山局長からありました DFFT のようなものも、このプラットホームが実現していくときに、個社で一つずつを取り組んでいくところはあるが、社会全体として共通であった方が得なものを少し整理しながら、その部分の開発等や、制度などを考えていく必要があるのではないかと、常々悩んでいる。

- アメリカでは、航空宇宙防衛産業のメンバが、マルチステークホルダーで情報の管理の仕組みを作っている。また、ヨーロッパでは、エストニアで X-Road という仕組みを見てきた。そこでの共通点は、個人の信用に基づいて、ここから全て人間の信頼の基点を作っていく。したがって、人間が法人に入って、法人としての業務をすれば、法人としての責任は当然あるが、エストニア国民としての責任の下でという、日本でいうマイナンバーに近いような本人をしっかりと認証する仕組みがベースになっている。
- 今後、第 3 層、第 2 層の信頼性を確保するための検討において、認証という、認証・認可は一つになるが、それを基点になる部分を含めて共通点を取り組んでいかないと、個社単位でセキュリティを頑張れと言うと、恐らく、コストが上がることにしかにつながらない。それこそ DFFT の足を引っ張ることになってしまう。このたすきがけを上手くやっていくためにも、検討会のテーマに社会全体で共通にやる仕組みの検討を入れていただけるとありがたい。

○江崎委員

- ビル SWG では、奥家課長から紹介があったように、グループを作って、インセンティブの設計とかエコシステムをどう作っていくかを次のターゲットにしようという意味で、社会実装する際のルールで縛る方向ではない方向を探っていくことに向かうわけだが、そのようなコンセンサスを形成することがとても重要。
- 岡村委員の発言を聞いていて思ったのは、良いフレームワークができているが、原則のようになっていないこと。例えば、インターネットでは、ネットワークの中立性というルールがあって、4 個か 5 個ぐらいのポイントを出している。これから具体化をしていくと、「具体化すると対応が厳しい」と言う人達が出てきて、いわば蛸壺状況になるので、本来目指してきたものと違うものと捉えられる。そういう時にもう一回見返すためのバイブルみたいな部分をしっかり作っておくと具体化を進める部隊がやり過ぎない。ガイドやチェックリストにできるものを作っておくのが大事ではないか。原則みたいな、例えば、コストではなくて、投資でバリューをクリエーションしましょう、みたいなことを書いておくと、バリュークリエーションを阻害するような事項が入っていないかをチェックするような、そういう大きな原則を作ると良いのではと思った。

○坂委員

- 自動車 SWG の状況を述べさせていただくと、自動車も自動車産業も昨今、非常に大きく変わろうとしていて、どこを対象として取り組んでいくのかという議論をしている中で、抜け漏れがあってはいけない、とか深堀が必要とか様々な議論があったが、できることはどんどんやっていこう、ということで、他の SWG から 1 年ほど遅れて立ち上がることができた。これから加速して進めていきたいと思っている。
- 一方で、どこを取り組んでいくかに関しては、大きく自動車産業の活動が広がっていく中で、皆さまの安全、皆が安心できるところ、そこにフォーカスすることになった。最初は、第 1 層の部分を中心としたサプライチェーンのところを取り上げるが、活動の範囲としてはどんどん広げていきたいと思う。
- 自動車の場合だけではないと思うが、海外の方では既に先行してアメリカで、この分野の標準のガイドラインが出ている。そういうところと連携しながら進めるという意味でも、まず、このフレームワーク自体が海外でも認知される、その辺りも含めて全体としての活動の中で、我々も連携していきたいと思っている。

・ これから立ち上げる 3 つの TF についても、元々、気にしている部分が多い。是非加速して、早めに活動の成果を出していただきたい。自動車分野でもそれを使いながら、逆に言うと我々はそこを検討しないで、こちらの TF に託したいと思うので、よろしくお願いしたい。

○上原委員

・ フレームワークができたということで、最近の講演や、現場に入ったりする時に、御紹介させていただく機会が多い。そのときの反応を見ると、大きな枠ができて、整理学としても良くて、具体策は SWG が動いているというところまではすんなりいくが、次の段階がある。
・ 既に IoT 時代は始まっていて、既存のシステムに対して、ネットワークはどんどん入り込んで、結局、自動制御がどんどん IoT 化しているという現実が目の前にある。システムは既に動いてしまっていて、ここにフレームワークがやってきて「To-Be はこれです」となっても Transition が問題になるという現実があり、これをどうするかという質問を受けたことがある。
・ ここ一ヶ月ぐらいの間に受けたインシデントの相談は、まさにそのようなパターンであり、既存のシステムにほぼ無秩序にネットワーク接続が行われたことが原因になって発生した事故を何件か見てきた。そうすると、岡村委員から御指摘あったように、インセンティブ設計という話が凄く大事と思っていて、あるシステムが既に動いてしまっている時に、これをセキュアにするためのインセンティブが無かったら、リスクが残ったまま、ずっと稼働し続けてしまうことになる。To-Be に引っ張っていくための、インセンティブ設計が非常に大事になる。
・ Transition Plan を含めて検討してなければならない中で、さらに困ったことに、少し大きなシステム、例えば、ビルなどは多くのステークホルダーがいて、システムは動いていて、もう動いているから仕方ないという世界になっているところに「このままでいけない」という、見える化する仕組みとして、リスクアセスメントをしっかりして、「これでは駄目です。病院へ行ってください」と言う、医者のような人達が必要だと感じた。
・ これを今、ここで発言したからといって、すぐに答えが出るとは思わないが、恐らく WG で議論が進んで具体案が見えたときに、割りとすぐに取り組まなければならない課題になると感じている。

○奥家課長

・ 特に、工場系などの制御系では、ボルトオンでないと対応できないというところもあり、その辺の研究開発のところも考えないといけない。
・ ビル分野は、ベータバージョンができた段階で、リスクアセスメントに使うことができる状態。リスクアセスメントをすぐにやって欲しいということで、急いでご議論いただいて、すぐにベータバージョンを作った。一部で使い始めている段階。一回でもリスクアセスメントをすると、穴がどこにあるのかが分かる。分かりさえすれば、完璧にはならないし、入れ替えができる訳ではないが、Mitigation するための工夫が始まる。
・ できるだけ現場で使っていただいて、リスクアセスメントに使えるものにしたい。その後に、インセンティブ、技術的なものなどはきちんと用意していきたい。
・ 特に、WG3 で議論しているが、これからの時代、Society5.0 は、開発への投資よりも検証のための投資が大きくなる社会で、これまでとは逆になると思っている。そうなると、検証ビジネスが大きくなって然るべきで、Checked by Japan という旗を掲げて、産業政策として進めていってみてはどうか、と議論している。
・ 各 WG がそれぞれ、いただいた御指摘を具体的に、お悩みに少しでも貢献できるようにしていきたい。

○上原委員

・ チェックも大事だが、もう一つの金のなる木は運用だと思っている。オペレーションは、今まで割と低く見られていたが、実は、リスクアセスメントの気づきが最初に吸い上げられる部分のはずなので、ここに上手くインセンティブが働くようになれば良いなと思っている。

○渡部委員

・ 今後の進め方として TF を作っていく中で、第 1 層で仕事をしている不動産業界としては、第 2 層の TF を非常に重要視している。ここをきちんと進めて欲しいと思っている。私どもは、不動産業界で建物を建てるだけではなく、ビルのエネルギー制御であるとか、エレベータ制御等など基本ビッグデータを使って様々な制御をしていきたいと考えている。第 3 層の分野まであまり踏み込んでなかったが、社会的要請もあり、IoT まで含めたサービスを今後、我々も考えていかないといけない。我々はデータの扱いに関しては素人で、どこまでできるのかという部分がある。第 2 層と言ったのは、例えば、第 2 層でデータを転写するときに、機器の正確性、機器が認証されている、ということが重要だと思うからである。それから、先ほどの安全計装において、センサの数値しかないということもあるが、実は、センサの置き方や、センサのネットワークの組み方等によってデータがおかしくなることも十分にあり得る。そういう部分の保証をどうするか、どのように考えるか。そこは、第 2 層が大分大きいのではないかと思っている。
・ 信頼の構築に関わってくるが、先ほど第 3 層に踏み込んでと言ったが、ビルの中でも最近、画像解析などいろいろ取り組んでいるが、我々は良く分からないのでベンダに任せている、というところで、サプライチェーンの中で、ベンダがきちんとやってくれる、カメラもベンダがきちんとやっている、データの取り扱いも「こういう手順でやっている」という意味では、機器もプロシージャも良いかもしれないが、ではネットワークをどのように引くのだろうとか、プロシージャに本当に抜けはないのか、などをはっきりしないとお客様に安心していただけないと思っている。
・ テナントから見ると、監視カメラで監視させるとろくなことをしない、ひょっとして悪いことに使っているのではないかと思われかねないこともあり、我々がお客様に提供していく、これもサプライチェーンの一つと思っているが、プロシージャから機器の制御線まで、先ほど言ったデータの使い方、ネットワークの使い方、構築、ネットワークセキュリティの安全性、そのようなところを第三者に評価いただいて、きちんとできている、あそこならば大丈夫かな、と言ってもらえるような仕組みが出てくるとうれしい。
・ そのためには、第 2 層をどのように扱っているのかを、もう一度、我々も考えていきたいと思っている。是非ここを積極的に進めていただきたいと思う。

○九野委員

・ WG1 の今後の取組ということで、TF の設置案を説明いただいて、非常に良い取組だと思っているので、是非進めていただきたいと思っている。
・ 特に、PC システム、ソフトウェアのところで転写機能の信頼性の確認手法、それからソフトウェアの取り扱いに関する管理手法というところで、弊社でも困っているところがある。いわゆるハードウェア、IoT 機器、ソフトウェアの信頼性が担保されているか、脆弱性があるか無いか、ということ以前に、一体何がつながっているのか。ソフトウェアの構成はどうなっているのか、ということが本当に 100%把握し切れているのかというとできていない。
・ しかも、一旦、それが確認できたとしても 1 時間後にはつながっていないはずのものが、つながっている、ソフトウェアのバージョンが変わっているとか、少しお恥ずかしい話だが、不正なソフトウェアがインスト

ールされているとか、ということが目まぐるしく起こっている。上原先生からセキュリティの世界では、運用がキーだという話があったがまったく同感で、このあたりをアセットや構成を管理しながら、脆弱性や信頼性をチェックしながら、担保していく仕掛けや手法を、是非このタスクフォースで検討したら良いのではないかと思っている。

○高倉委員

- 今後の話に意見したい。一つは、ソフトウェアのトランスペアレンシーで、どうしても最後行き着くのは人になってしまう。ちょうど先週、ASUS のマザーボードの件があったが、まだ経緯は分からないが、確実に人が関与していないとできないようなことがサプライチェーンに仕掛けられてしまう。そうすると、恐らく、人を何らかの形で、この仕組みに入れていかなければならないが、欧米では、既にクリアランスがありそれで解決するが、日本とアジアではそのままでは使えない。そうすると、人の信頼性は、どのように担保するのか、今回の議論では、まだ抜けているなという印象がある。そこを何とかして欲しい。
- もう一つ、セイフティとセキュリティの一体化という話があると思うが、是非お願いしたい。今までどちらかというと、リスクアセスメントした結果、問題があると即直そうとする、FIX しようとする動きが顕著に出ている。私が知っている事例では、無理矢理 FIX した結果、壊してしまう、壊してしまったがたまたまセイフティが働いていたので暴走せずに済んだ、という事例がいくつか出てきている。今後、セイフティが、ソフトウェアで制御されることが出てくると思うが、そうすると無理やり FIX することでセイフティを飛ばしてしまうことが今後出てくる。それが駄目だというのではなく、そういう仕組みが今後出てくると想定したときに、どうすればセキュリティも意識しながら、セイフティをきちんと担保できるかということを検討していただきたい。

○平田委員

- 今回のフレームワークは、各分野の事情やセキュリティ要件に合わせて、取捨選択して使えることが非常に重要なことだと思っている。
- 分野をまたがって流通されるデータにフォーカスして TF を作られたのは非常に重要だと思っている。一方、他の分野のデータをどう使っていくかは非常に難しい。守ることと併せて、どのように使っていくかをユースケースベースで検討を進めることを期待する。
- オープン化、マルチベンダ化が進んでくるため、信頼を確認することは非常に重要であるが、一方で確認コストが相当掛かってくるのと思われる。一社で頑張るというのではなく、複数のステークホルダーで協力しながらコストを下げる仕組みや、信頼が確保されているが故に効率化できる等、インセンティブにつながるような方法を考えていただきたい。

○松尾委員

- フレームワークはバージョン 1.0 ということで本格的に活用できるようになった、感謝している。
- データ流通に関しては、国際的なハーモナイゼーションを前提にということなので、国際的なことで活用することを最優先に考えていただきたい。
- 質問として、WG のタイトルにあるように、標準化の関係で、国際的な標準化に対して、我々が何か手を打つことは考えられているか。

○奥家課長

・ 標準化については、分野横断 SWG でも議論になった。実際に、ISO の世界の人たちは、結構フレームワークの原案を読んでいて、逆にそれで各国の提案が早く、激しくなったりするケースもあれば、日本から代表として出ていく人達が、このフレームワークで結構オーバライドしたり、上位概念層でちぐはぐに動いている部分を統合する機能を果たせているので、早く標準化して使いたいという希望などもいただいている。
・ 一方、このフレームワーク自体は、産業社会全体を捉えているので、これそのものが標準として出て行くのは、例えば、ISO 27001 の人たちにとっては、そこはサンクチュアリなので、どうしてもこれだけで全体を捉えたいし、機能安全の世界の人たちも、セキュリティのいわゆるトラディショナルな人達の所など、様々な要素を包含しているので、使い方を工夫するということだろうと思っている。
・ フレームワークはかなり包括的な形で作ってあるので、ある部分だけでも、分野をまたいで存在する標準を繋ぐ働きを十分果たすことができるので、国際標準で動いている方や、皆様と議論させていただいて、ここの部分を日本提案として使っていくことができるのではないか。フレームワークの中で使われている部分を上手く組み合わせて、いくつかの場所に出すということはあるのだろうと思っている。

○其山委員
・ 今後の動きについて数点コメントさせていただきたい。WG1 後にバージョン 1.0 がリリースされるということだが、是非お願いしたいのが、欧米からは意見が結構出ていたが、東南アジアやベトナムとかミャンマーとか、日本の製品・サービスのフレームワークに基づいて作られたときに東南アジアに輸出するなど、東南アジアはサプライチェーン上無視できないので、それを守るための APAC やアジアに対してフレームワークをプロモーションする活動をお願いできればと思う。政府からの話は効果が高いと思うので、是非お願いしたい。
・ TF については、海外の動きを十分見られるということだが、ガラパゴス化しないように気をつけていただき、既存の仕組みや、海外を含めて製品・テクノロジーで、採用できるものがあれば視野に入れて検討いただきたい。

○奥家課長
・ 豪州なども関係が深い。日豪サイバー協議等でも実際話をしているが、結構、フレームワークを読み込んでいる。個別に質問を頂くぐらい理解している。東南アジアは日 ASEAN や APEC の場でコンセプトベースの話はしているが、個別の国について、もう一段の取り組みが、今後必要になると思っている。
・ アジア各国も、シンガポールのように非常に関心が高い国や、タイのようにある意味センターの話をしたいといった様々な思惑を持っている。ベトナムは、地政学的な理由から日本ともっと連携したいと言っている。そういったところをもっと理解した上で、考えていかなければならないと思っている。
・ ERIA という東南アジア版 OECD があり、ERIA とも協力して、東南アジア全体のセキュリティシステムの具合などを把握する仕組みを開始しようとする議論をしている。ビルのセキュリティガイドラインの取組においても、アジア地域でのそういった取組が無いか調べたりしていた。各 SWG でプロテクションプロファイルに落とし込んだときには、視野を広げていくことも大事になってくると思う。

○澤井様
・ 御紹介があったように、オリパラや今年は G20 など重要会合があるが、電力業界として、安定供給に万全を期すということで、電力 SWG にて、情報共有や IT-OT 連携などの議論を行っている。直近に抜本的な設備入替ができるわけではないので、電力設備の運転・運用として、どのようにサイバー攻撃への対処能力を

向上できるかに取り組んでいる。

- 今後の取組ということで TF や SIP の話があったが、我々としても期待している。先ほど上原委員から、既存のモノのネットワーク化という話があった。まさに電力では、すぐに電力ネットワーク全体が入れ替わることはない。新しい設備は接続試験の中で様々なテストをする。我々としては、仮に認証を受けて、それを信頼して接続するのは、簡単であって嬉しいが、使う側としても確認すべき事項は絶対あると思っている。我々買う側、利用する側が確認する事項等、安全確保する上でするべきことを言っていただけると大変助かる。
- また、機能安全との関係は、まさしく重要と思っている。例えば、火力発電では、稼働前に試運転を行い、様々な保安に関するチェックをしているが、その中にサイバー攻撃への対処に関する点検項目はない。運用というキーワードがあったと思うが、例えば、試運転をする中で、サイバー攻撃を受けないために事業者側がチェックすべきことがもしあれば、検討していただければ助かると思っている。

○松本委員

- 第 2 層 TF は、非常に重要だと思う。安全（セーフティ）が担保されるように作ったシステムは、要素のつながりによって、システム全体として安全（セーフティ）をもたらそう、という「機能安全」が実装されたものなので、その要素、あるいは、要素間のつながりを揺るがす攻撃を、攻撃側に許しやすくなる。よって、そこをどう守っていくかが重要だと思っている。プロテクションプロファイル（セキュリティ要求仕様）という話があったが、ポリシーというか、何をどのような用途に使うか、どのような形で安全を担保したいのかに応じてセキュリティ上の攻撃に対応する防御側の要件も変わってくるはず。したがって、同じ製品、あるいは、システムであっても、その目的によって、セキュリティ上どのようなことを要求するかは当然変わってくる。そこで、今回 TF で検討を進めていく場合、対象としてどのような分野のものを重視するのかについて、既に検討されていれば伺いたい。
- また、TF の名称がすごく長いように思われる。省略されるはずなので、初めから短い名前にした方が良いのではと思う。

○奥家課長

- それぞれの TF の名称は考えさせていただく。
- 第 2 層のところは、まったく御指摘のとおりで、物によって使われ方、用途によってプロテクトの仕方とか、どの程度するべきかが、まったく変わってしまう。それを森羅万象全て抑えるのは難しいと思っている。
- 一方で、今のところ議論ができるのは、ビルのエリアと電力のエリア。スマートホームは、ここに入っていく準備はできているということなので、今後、この 3 分野について、共通的に見るべきこと、チェックをかけなければいけないこと、確認の手法等、さらに、機能安全から、製品安全につながっていく部分が出てくる中で、ある意味、どこまで取り組んだことで義務が果たされているという見方となるのかという、そういった一般的な事項を議論として整理しておかなければいけないということになっていくと思う。TF では、メインは、そういったところを議論することになっていくと思う。
- 具体的なプロテクションプロファイルは、物によって、物がどう貢献しようとしているかによって、設計自体が変わってくる。そこは、プロテクションプロファイルを具体的に落とし込んでいけるか、もしくは、SWG の中では、既に検証などをしなければならないから、検証体制などを、検証設備があるところで、どのような検証をするかなど、SWG 側で議論しなければいけないことも出てくると思う。そこに対して TF が、うまくガイドできるかという話になると思う。

○松本委員

- ビルや電力やスマートホームでは、小さなエッジがたくさんつながっていて、たくさんの要素があると思う。それぞれについては、プロテクションプロファイルや、プロテクションプロファイルのようなものの実績が既にあって、整備されてきている分野はあると思っている。大きなシステムになると、これを取り扱うことが非常に難しく、その辺りがチャレンジングかつ重要なところだと思う。

○白石委員

- これからの活動で、是非、国際的なハーモナイゼーションを念頭に置いて検討いただければと思う。実際、私共も、米国の顧客と仕事をすることがあるが、現実に米国のある規格に基づいて社内のサイバーセキュリティ対策を行いなさい、という要求がきている。今後、国内での要件の検討に当たっては、そういった国際的な規格との齟齬が無いような、同調した形で進めていただければと思う。

○江崎委員

- 国際標準化の話があったが、標準化は、目的ではなくツールなので、それをどのように使うかを考えなければいけない。特に、調達の条件として入ってくるのであれば、政策的にどのように入れるかという話をしないといけない。
- 私が経験したのは、世界銀行が、調達条件をお金に加えて KPI として、クオリティやサスティナビリティを高くして、安かろう悪かろうを買わなくて良いようにしている。調達の条件の KPI をどこにするかという話しになる。
- 戦略的にどの部分を標準とするか、海外での KPI の作り方がどうなっているかを十分咀嚼した上でこのツールのコンポーネントをどのように入れるかという考え方で国際標準化に取り組んでいかないと、現場に落ちてきて国際標準化が目的となって予算取りにいく形になってしまう。

○小松崎委員

- 冒頭、局長からデータフリーフロー・ウイズ・トラスト、安倍総理がおっしゃった言葉が引用されていたが、データフリーフローが目的ではなくて、それによって新しい社会システムや社会サービスを作ることをおっしゃった言葉だと思う。そういう意味では、先ほど上原委員がおっしゃったオペレーションは、金のなる木ということだが、汗も沢山落ちる。
- 我々はオペレーションをずっとやってきた会社で、なおかつ、コンピュータネットワークやセンサを、いち早く IoT 的に使い始めた。その経験で申し上げると、つなげばつなぐほど、サービスは大丈夫かなと不安が増す。したがって、サイバーセキュリティにも割りと早く着手した経緯がある。ただ、大切なのは、つながれば新しい価値が出るということは間違い無い。この会議でどこを守るかということではなく、オペレーション、違う言い方で言うとサービス、新しいサービスを作る価値が一方であるからこそ、セキュリティが大事で、逆に言えば、セキュリティがきちんとしているから、新しいサービスを安心して作れるという大きな循環が回ることが最終的には Society5.0 を実現することに非常に寄与するのではないか。
- 昨年、ブラッセルで EC、OECD の合同会議に出席したが、その印象で言うと Society5.0 は、その時点では 40 カ国、500 人の方は、ほとんど知らなかったが、少し説明したところ素晴らしいという予想を超えた反応を頂いた。さらにスマートホームで、さすがに日本といわれるように我々も頑張りたいと思っている。オペレーションを大事にする、サービスを大事にするということはキーワードではないかと思っている。

自由討議の最後に、佐々木座長から以下のとおり総括がなされた。

- 本日も委員から様々な御意見をいただいた。フレームワークについては良くできているが、実際に運用して役に立つようにするためには、誰が面倒を見ていくか、いろいろと決めていかなければいけないところがあるという意見があった。これからも委員の方々、関係者の方々に頑張っていただかなければいけないところもあると思う。
- 本日、御議論いただいたサイバー・フィジカル・セキュリティ対策フレームワークについては、いただいた御意見を踏まえて、修正を行い、修正したものを皆様にお見せした上で、最終的な策定については座長一任とさせていただきたい。

閉会に際して、三角審議官から以下のとおり挨拶。

- 本日は熱心な議論、ありがとうございました。政府全体で、サイバーセキュリティ戦略に取り組んでいるが、一貫して言ってきているのは、サイバーセキュリティは目的ではなく、あくまで手段であり、それはサイバー空間が無限の価値を持っていて、どうやってそこに信頼性や安全性、良い品質を与えていくかを充実させ、如何にサービスを保証していくかが重要だと、ずっと言っている。それを具体的に、どのように実現するかは非常に難しく、このように議論して完成したフレームワークはまさに仕様に使っていけると思っている。いろいろなことができるが、現場では困ってしまう。そのような問題を今後、しっかりと考えていきたいと思っている。

最後に事務局から、今後のスケジュールについて以下のとおり連絡を行った後、閉会した。

- サイバー・フィジカル・セキュリティ対策フレームワークについては、座長と相談し、4月中に策定ということで公表させていただきたい。
- 第6回会合は、別途事務局から連絡する。

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