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3回) 議事要旨

1. 日時・場所

日時:平成30年8月3日(金) 10時00分～11時50分

場所:経済産業省 別館11階 1111各省庁共用会議室

2. 出席者

委員 :佐々木委員(座長)、岩見委員、上原委員、太田委員(代理:飯島様)、岡村委員、片山委員、北川委員(代理:山角様)、小松崎委員、斎藤委員、其山委員、高倉委員、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、三角審議官、奥家サイバーセキュリティ課長

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 3-1 サブワーキンググループ等の設置・検討状況

資料 3-2 Society5.0 実現に向けたスマートライフ分野のサイバーセキュリティ対策の方向性(JEITA 提出資料)

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 5-1 「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)」の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～【非公表】

資料 5-2 「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)」の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)【非公表】

資料 6 WG1の今後の進め方(案)

資料 7 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

4. 議事内容

冒頭、西山局長から以下のとおり挨拶。

- 皆様に申し上げるまでもなく、今回このフレームワークの中で 3 層構造といわれている、まったく新しい物事の捉え方を発信していると思っている。また、今回、パブリックコメントなどを通じて、国内だけではなく海外とも対話をしながらフレームワークを作っていこうとしている。
- この WG で検討いただいていることは、狭い意味でのサイバーセキュリティに留まらず、様々なインパクトのある事柄だと思っている。今後ともよろしくお願いしたい。

事務局の奥家サイバーセキュリティ課長より、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(なお、資料3-2は、JEITAスマートホームサイバーセキュリティWGの主査である小松崎委員より説明)。

- 資料 3-1 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 3-2 に基づいて、小松崎委員からスマートホームサブワーキンググループの検討状況及び今後の方向性を説明。
- 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 5-1 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を説明。
- 資料 6 に基づいて、WG1 の今後の進め方を説明。
- 資料7に基づいて、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を説明。

資料説明の後、自由討議に先立ち、欠席の江崎委員からのコメントを事務局から紹介。

- 本フレームワーク自体が、野心的に全体をカバーする構成をとった。一方で、読む人がすべての対策をやらなければいけないと受け止めると、非常に大きな負担感が出てくるので、そのように受け止められないように、実装時に何をやらなければいけないか使う側の目線で、例えば、調達時や運用時のチェックポイントという形で整理をしてみるなどの工夫が必要ではないか。
- また、対策例のような細かいものは、アーカイブのような形として整理すると良いと思う。

コメントの紹介後、以下のとおり自由討議を行った。

○岡村委員

- 常に問題になるのが責任分界点です。そこを考えていただけるとありがたい。また、企業関係であれば、例えば、会社法上の内部統制の基本方針の徹底、あるいは、それに即した監査役の監査報告書の株主総会への公表の制度もあるので、こういったものになぞらえて、企業に本気で取り組んでいただくためのベース作りというアプローチもあると思う。
- もう一点、スマートホームとビルとの違いとして、セキュリティ専門家の存否という点があると思う。ある程度の大企業であれば、CISO がいると思うが、高齢化社会に入るなかで、おじいちゃんおばあちゃんが家庭の CISO になることは少し難しいと思う。
- 以前から申し上げているが、従前のセキュリティ会社、セキュリティでもホームセキュリティを担当している会社のように、何かあったときには駆けつける、リモートで監視できるというビジネスもこれからは重要になるのではないか。その反面、年老いた親を田舎に残しているという状態が一般化しており、セキュリティそのものとは違うが、サイバーセキュリティというよりは、親の安否確認にも IT が使える部分もあるので、スマートホームを御検討いただくときに、そういう切り口で家庭に入っていくのも理解を得やすいと思う。

○奥家課長

- 責任分界点の議論は WG3 でも出ていて、IPA のアンケートで、SLA、サービス内容やレベルを定めず、責任分界点が明確でなかった結果、ビジネス上の大きな障害になっていることが数字としても出てきている。このような中で、まずは事例の整理を来週の WG3で取り上げたい。ただし、責任分界点を契約時点で全部切り分けきれるのだろうかとも思う。セキュリティは、最初の機器の納入だけではなく、その後にサービスが付随する場合、状況によってお互いの期待値が動く部分がある。その点については第一回のコラボレーション・プラットフォームでも議論になった。海外では契約を結ぶ場合、お金の関係で動けなくならないように、まず保険に入って作業を進めるといった対応をしているとの話があった。複合的なアプローチにより、責任分解点の問題を解いていく必要があると思うので、大きい課題として認識し、しっかり取り組んでいきたい。
- あと、経営環境で取り組んでいく課題は、WG2で取り上げている。いただいたコメントを踏まえながら、様々なアプロ

ーチをしていきたい。

○岡村委員

- 基本的には課長がおっしゃった方向で進めていただきたい。一言加えると、保険一つとしても、自動車の場合には、任意保険もあれば、強制保険もある。負担の問題でもあり、そんなにお金がかかるならいいやと野放し状態になって、機器が踏み台になっても困る。そこは全体的な最適化が必要。

○片山委員

- フレームワークに関して、30 年度末に向けてアップグレードをされるとのことで、最後に奥家課長から 1.0 や 0.9 とおっしゃいましたが、NIST のフレームワークはご存じのとおり 1.0 から 1.1 に改訂するような表現になっております。どういう位置づけや改定により 1.0 から 0.9 に戻るのかコメントをいただきたい。
- 我々からもパブリックコメントを提出させていただいた。今回、パブコメ期間は 30 日でしたが、米国では 60 日程度取るのが普通であり、もう少し長く取るのも一案かと思う。
- 事務局より事前にご質問いただいた、米国商務省から出ているボットネット対策の報告書について、オブリゲーションなのか、レコメンデーションなのかという点について確認したが、基本的にはレコメンデーションであり、オブリゲーションではないと理解していることを報告したい。

○奥家課長

- 今回、お示ししているフレームワーク自体がドラフトですので、今後、ドラフト2をお示しした後できたものも、表現が悪かったかもしれませんが、これで決まりというものではない。コンセプトの部分は相当きちんとしていけると思うが、コンセプトより下の対策例などは変化していくので、それらが固定的なものに捉えられないようにしなければならないという意味合いであり、バージョンが 1.0 から 0.9 に戻ることではありません。
- 米国のサイバーセキュリティフレームワークも 1.0 から 2.0 ではなく、1.1 と言っている。他のフレームワークもそうだが、インパクト度合いで、普通に 1 を加えたのか、0.1 を加えたのか、ということだと思っているので、逆に言うと、それくらい動き、発展があるものにならざるを得ないかと思っている。

○小松崎委員

- 責任分界点に関して、岡村先生からいくつか大事なポイントが出たので、その点に関して意見を申し上げたい。例えば、家の中のセキュリティを考えるときにいつも出てくる話なのですが、お客さんから見たときに、「ここから先は僕の責任ではありません」とか、「私の責任ではありません、あちらに聞いてください」というサービスが良いサービスなのかということ。法的な責任とは別に、お客さんから見たときに、「困ったら、全部私に言ってください」という方がトラストに通じる話であろうと。ですから、サービスの基点をお客様と考えるのであれば、良いサービスかどうかは責任分界点にあまりこだわって無いように見えた方が良いということが私たちが思っている重要なポイントです。
- ところが一方では、何か損失が発生した際に、誰が責任を取るかをはっきりしてないといけない。言葉の上ですが、責任分界点ではなくて、原因分界点ということが必要だと思う。つまり、何かインシデントが起きたときに、何が原因で、どういうプロシージャ、プロセスで、こういう風になったのかを紐解けないと、きちんとした対応ができないという意味合いがある。
- 私たちは責任と言うと、やや腰が引けるのですが、原因をピシッとわかるようにすることが、共同でサービスを提供する人間の務めと言うならば、意味は同じでも感覚はだいぶ変わってくる。JEITA の中でも、まだ完全なコンセンサスは取れていないですが、責任分界点というと、どうも積極的なサービスが作りにくくなるので、原因分界点と呼び変えてい

こうという取組を始めたばかり。

- お客様視点というのは非常に大事で、いろんなものが組み合わさったり、時として結合すらはっきり分かりにくい結合であったりというのは、抵抗のイメージの一つとなり得る。そのような中で、責任を明確にしていこうとすると、シンプルなわかりやすい構図にとどまってしまう可能性があるので、できれば、訳のわからないように見えるような複雑な組み合わせを目指すには、そこに対して少しでもネガティブなインセンティブが働かないような意識づけや表現が大事なような気がします。そこが責任分界点に関する考え方であります。岡村先生がおっしゃるように、きちんと事業をやっていく上では明確にしていくポイントですが、どう表現するかということを工夫したいと思います。
- スマートホームで CISO が置けないというのは大切なご指摘。だからこそ、子供や高齢者が使うかもしれないことを想定したハードウェア面、ソフトウェア面の対策が必要です。
- あと、いざとなった時に人が駆けつけるというのは、とてもわかりやすく、トラストに結びつくプラットフォームになると思う。ICT でどう解決していくかを考えながら、公的サービスと民間サービスとの融合によって、最後は人が駆けつけるところまでつなげると、ICT を中心としたサービスの信頼性が非常に高まり、利用促進につながると思う。
- 高齢者の方の見守りについてのお話がありましたが、もう一歩突き進んで、高齢者の方が誰かのケアを受けるときに家族がいなければならないという状況は、人口が減っていく中では避けたいこと。そうすると、ケアを受ける人が一人で、家族が立ち会わなくてもいいと考えるときに何が起こるというと、第三者が家に入ってくる。そのときに、第三者がフィジカルの世界でも、サイバーの世界でも変なことをしていないことをどのように証明、担保していくかが必要になってくると思う。
- 岡村先生が先ほどおっしゃったことを私たち JEITA でも視野に入れて、それを具体的に実行して、なおかつ商品としてお客様の信頼を得る、という考え方で進めておりますので、アドバイスをいただければと思う。

○佐々木座長

- ありがとうございました。責任分界点、原因分界点と言うと、三層に分けると横だけではなく縦の分界点もあるので、重要になってくると思います。

○高倉委員

- ソフトウェアの信頼性の部分で気になったのは、パブリックコメントでいただいたところですが、すごくセキュアな、完全なソフトウェアを期待されているということ。それが理想ではありますが、一方で型式認定などが関係してきますと、パッチが出ても即適用することができないということは、完全性、安全性の確認がまだ取れてないことに関して、他の方法でどうやってカバーをするのか、もしくは、継続利用する際にどうすればインパクトを抑えられるのか、という視点が入ってこなければならないと思っていて、特に、今回の三層構造の場合、どこかの層でそれを補完できないかという議論ができればいいのではないかと思う。
- そのあたりをうまくやっていくと、例えば、オープンソースを使っている製品がどれだけ存在し、そのうちのいずれかに問題が起こった際に、どこの製品が影響を受けるのか、影響を回避できるのか否かを、製造者側、利用者側、利用者側は難しいかもしれませんが、製造者側が即座に理解でき、緩和策を取ることができる仕組みを是非作っていただかなくてはならないと思う。

○平田委員

- パブリックコメントへの意見を見ると、本フレームワークが、各分野の要件を全て包含したものと捉えた方もかなりいたのではないかと思います。本フレームワークは、Society5.0 において各分野間で流通するデータをどうやって安全に信頼できるデータにしていくかが主眼であり、それをサプライチェーンという切り口で担保していくことだと思うので、そ

れぞれを繋ぐことを想定し、どうデータを信頼していくかにフォーカスした形で各分野の要件と連携するものであることをよりクリアに書いた方がよいのではと思います。

- また、具体的な要件に近い三章の部分に多くのコメントが来ていたと思うが、前段の目標とすべきフレームワークの考え方やコンセプトの部分と、後段の対策例についてドキュメントや位置付けを分け、対策例については各分野がいろいろアドインし易い形にしていただくのがよいのではと思うので、今後の検討をお願いしたい。

○佐々木座長

- ありがとうございました。後半の部分に関しては御指摘の通りと思います。前半について奥家課長からコメントありますか。

○奥家課長

- スライドでもいくつかありましたが、産業社会を三層で捉えることを明確に言うようにしています。三層にしないと一つの会社で全部対応しないといけないと受け止められてしまう。産業社会をサイバー・フィジカルがインテグレイトされた社会と三層で捉えて、柔軟にサプライチェーンが組まれたマルチステークホルダーということをもっときちんと説明し、その局面で関係するところでどうするかということを明示していかないといけない。そこの部分は、御指摘の通り、強くメッセージを出していきたい。

○松本委員

- 世界的にも反響があったということで、非常に喜ばしいと思う。第一層、第二層、第三層とありますが、第一層を企業間のつながり、あるいは、従来型サプライチェーンと表現されています。この時にプレイヤーが企業だけなのか、という印象を与えてしまうので、もう少し工夫されたほうがよろしいのではないでしょうか。つまり、B2B だけでなく、B2C だとか、そのような要素が実際には入っていると思うので、考えてみてはいかがと思った。
- フレームワークのコンセプトを各分野で活用していくために、実際には SWG で御検討いただいているところだと思うが、SWG で具体化するにあたって困難が生じた点があれば、横展開していただけるとよろしいのではないかと思う。関連して、今ある、あるいはこれからできる SWG で十分なのでしょうか。今は、一生懸命、意識高く使命感を持って取り組んでいただいている方々が SWG に集結しているとのことですけれども、これからこのフレームワークを適用するため新たな分野で検討しようとしたときに、何か障害が出てこないでしょうか。トップダウンで考えて、SWG を立ち上げる領域を具体化していくと、かなり広くカバーできることになると思う。
- 最後に、このフレームワークは非常によいので、皆さんがソラで言えるような絵を作りませんか。先ほどの米国の5ステップのものと、こちらの3層の3×5というのは、非常によいと思うのですが、まだ難しいと思う。アイディアがあればお示ししたいのですが、非常に簡単な図ができるとよいと思う。

○其山委員

- 私どもは製造業さんとか電力さんとか、いろんな会社さんへ、例えば、NIST のサイバーセキュリティフレームワークを使って、セキュリティ対策の整理などのサービスを提供させていただいていますが、やはり、この新しく出されたフレームワークの話が出ることが多く、そのときに、総論では賛成だけれども、各論ではいろいろ意見を伺うことがあり、「ここは自分たちには該当しないな」とか、「なかなか使いづらい」とかお伺いすることが多い。見直し方針の方向性については、個人としては問題ないと考えるが、今後、見直すにあたって文書構造を含めた見直しのなかで、誰が実施するのか、や、内容がわかりにくいなどの解消を目指して、例えば、フレームワークは考え方・運用指針に徹した文書にしたうえで、ガイドライン的な具体的な内容を SWG で検討し、文書自体を分けていくなど、そのような形の方が実際に

使う人たちにとっては分かりやすいのではと考えます。

- フレームワークやガイドライン類などの文書類は、一度出されて、そのままになっているものもあり、それらは実態にそぐわなくなっているものがあるなと感じる。定期的に、いつ必ず見直します、ということをフレームワークの中でしっかりとうたっていただくと、その際に実態と整合性を取っていくことができ、生きた文章となり、各業界が、このフレームワークに準拠・活用していれば、自社も最新の対策にアップデートできるという考えになるのではないかと考えます。
- ワークショップを開催してフレームワークのイネーブルメントをしっかりとしてほしい、という意見があったと思う。それに対しての考えですが、フレームワークの考え方とかをしっかり学んで、各企業でイネーブルメントできる方をスペシャリスト認定するといった資格制度のようなものなど、いろいろあると思うが、そういったものを推進してはどうかと考えます。
- あと、以前も発言させていただきましたが、このフレームワークを使うこと自体へのインセンティブを各企業、各組織に与えていただきたいです。今まで議論が出ている法的な位置づけなどに関連していくと思うが、やはり、インセンティブがないと、なかなか採用できない、プロモーションできないといったことがあると思いますので、国としてそのような形を考えていただけると、業界側も動きやすいのかなと考えます。

○奥家課長

- 文書構造について、御指摘いただいていることは非常に重要で、プラグインできるようにすることや、江崎先生からのコメントなどは、そういった趣旨だと思います。哲学的なコンセプト部分は相当固めても良いと思うが、その次の対策例とかは、位置づけを変えていくことになるかと思う。
- そういった中で、インセンティブやスペシャリストのところは、これはマルチステークホルダーで産業社会全体を捉えた時に、産業社会全体でやるわけではない、ということになると、適用局面が部分的になる。ある部分についてはあるものを、という形になると、もう一段ブレークダウンしたところでの議論になっていくのではと考えている。

○飯島様（太田委員代理）

- フレームワークをベースとしたアプローチには賛同します。
- ドキュメントは、フレームワーク→ガイドライン→リファレンスという形で具体化していくものと理解した。コンセプトチックなフレームワークからガイドラインへ落とすというアプローチと並行して、例えば、業界特有のベストプラクティスみたいなものをフレームワークに一回落としこんでガイドラインを作るというアプローチも有効ではないだろうか。
- 今後、分野共通 SWG では具体的なユースケースに基づいて検討していくスタイルとして、抽象的な議論にならないようにして欲しい。

○岩見委員

- フレームワークは、非常に有効なものだと思っており、修正の方向性も概ね賛成できる。今後、様々なサプライチェーンへの適用が視野に入ってくると思うが、その中にも企業の規模の大小があるので、セキュリティ対策のレベル分けは非常に有効だと思う。
- 各サプライチェーンの中には分野をまたがるサプライヤがいるということ、また、サプライヤの中でも規模の大小があることから、セキュリティ対策の基準について、分野横断 SWG で御議論、あるいは一定の基準を示していただければと思っている。

○渡部委員

- ビル SWG に参画している中で、このフレームワークは、製造側、サービス提供側で信頼性を構築し、良いものを作っていく形になっている。そこで、今度はサービスを受ける、製品を提供されるユーザ側から、どのレベルなのかを簡単

に判断できる指標が出てくると、ユーザ側も判断し易くなり、製造側もより取り組み易くなるのではないかなと思う。

- 分かり易い指標ができれば、なかなかセキュリティに取り組みづらかった中小企業にとっても、どうやっていこうか、どこまで協力しようかと検討できると思うので、フレームワークの次かもしれないが、認証となると難しくなると思うが、何かしらの指標ができると良いと思う。

○坂委員

- 自動車 SWG の検討がまだ進んでいなくて申し訳ないが、自動車メーカと部品メーカ、サプヤイヤと全体で議論していかなければならず、それからソフトウェアという観点や従来型サプライチェーンという観点で、どこを議論するかを含め、まだクリアなっていない点の検討を進めている。早く、自動車 SWG を立ち上げていきたい。
- 今回、お示しいただいた見直し方針の 3 点は是非対応していただきたい。特に、目的と適用範囲がはっきりしないと、議論があらぬ方向に行ってしまうので、そこをクリアにしていただきたいのと、サプライチェーン全体を見たときのセキュリティ対策のレベル分け、これは中小企業を含めてという観点で重要だと思うので、これは進めていくべきだと思っている。
- 国際規格というか、NIST のサイバーセキュリティフレームワークなど、もちろん対比することは大事と思うし、それが無いとグローバルでやっていく上では困るが、一方で NIST のフレームワークが万能でもない。NIST もここがまだ、という部分はあるし、NISTもどんどん進化していく。NIST と同じものを作れば良いのであればこのような会議はいらないので、我々としてもこの場でキッチリ議論して進化させたものを作っていきたい。グローバルに一歩先を行けば NIST なども逆についてくる部分もあるのではないかと思う。

○松尾委員

- マルチステークホルダーについて実施者を明確にしていただくという見直し方針は、我々としてもありがたい。既存の規格との逆引きも、大変だと思うが、是非ともやっていただけたらと思う。
- レベル分けをするということは、信頼の確保についてもレベルが分かれてくるということで、レベル毎のトラストリストがそれぞれ作られるイメージになるのか。そういったものを検討していかなければならないかと考えている。

○上原委員

- やはり出てきたかというのが、GDPR との対応を出してくださいという意見。このような話が出てくる最大の原因は、セキュリティの話とプライバシーの話とをサービサーや製品提供者が、すぐに混ぜてしまうことにあると思っている。サイバー・フィジカル・セキュリティ対策フレームワークの守備範囲の中でプライバシーに関わる箇所、恐らく、一番直接的に関係してくる情報の漏洩や開示のところに関して、この部分は関係するから、フレームワークで引き取ります、でも GDPR の他の要件は全部追い出しています、と最初に明確に書いておかないと、セキュリティとプライバシーが混ざったままになると思う。最初の書きぶりで避けられる話であると感じる。
- マルチステークホルダーという言葉がかなり危険な言葉で、利用者やユーザ側もステークホルダーですから、それらを混ぜる話をした途端に、また話が混濁するおそれがある。恐らく、マルチステークホルダーとしてもサービスを提供する側の関係、あるいは、サプライチェーンにいるステークホルダーという話と、それこそ最初に岡村委員がおっしゃった責任分界の話が明確になるような、サービスを提供する側の問題なのか、サービスを利用する側の問題なのか。この切り分けをはっきりさせずに、同じようにマルチステークホルダーの考え方を放り込んでしまうと、また話が混ざるので、一つ線を引く必要があるのではないか。ただし、考え方を明記する際にその書きぶりが難しいと感じる。
- パブリックコメントで一番痛い指摘と思ったのは、レベル分けに関して優先順位があまり明確でないという意見と、例示の仕方が良くないという意見。例示をカバーしていれば全てが網羅されているように読む人もいるだろうし、逆に漏

れている事項にすぐに気が付いて突っ込む人もいて、ここをレベル分けするにも書きぶりがすごく大事だと思っており、結局、「例として、こういうこともある、こういうこともある、詳しくはこちらに」という実際に網羅性が保証できる規格へのリンクを張っておくことが非常に重要になると思う。

○斎藤委員

- 岡村委員や小松崎委員が発言された責任や原因は、インシデントが起きた後の対応で、今回のフレームワークはどちらかというと、インシデントが起きる前にどう取り組むか、そのための対応策をどうするかということで言うと、インシデントが起きる前に重点を置きすぎている感触が若干ある。
- ただ、インシデントが起きた後の原因や責任という前に、原因と責任はどのエビデンスを基に特定するのか、保険にしても、エビデンスに基づいて保険料を払うものなので、その意味では、インシデント後のことを考慮するとなると、エビデンスの取り方をきちんと検討しておかないと上手くいかないと思う。
- インシデント前の話で言うと、今回のパブリックコメントのほとんどが、やはりフィージビリティというか、自分の負担はどうなるのか、ということに集約されていて、つまりは、何をやれば良いのかに始まり、6 つの要素も全て自分には当てはまらないときはどうするのか、マルチステークホルダーの考えの時に自分はどれくらい対応し、他のステークホルダーはどうなのか、負担の構造がわかり難いというのが、今回のパブリックコメントの一つのアウトプットと思う。
- その意味では、今後レベル分けの対策例を出したときに、あなたの場合こういう負担ですよ、ということが併せて書かれると、これは私だねと、私はここまでやればいいんだね、ということが分かり易くなると思うので、対策例のレベル分けの時に併せてフィージビリティの世界、トータルなコスト負担が明示できると良いと思う。
- 其山委員も言われた見直しのタイミングは、1 年に 1 回とか時系列で定期的に行うという話もあるが、もしかすると、例えば、インシデント前のフレームワーク、インシデントが起きて対応したら、フィードバックを実施し見直すとか、見直しのタイミングを必ずしも時期ではなく、なにかしらの PDCA サイクルの中で位置づけるという提言もあり得ると思うので、ご考慮いただきたい。

○岡村委員

- 今の斎藤委員の御指摘はよくわかるのですが、基本的には、まず責任を負う必要が無いように、事前にそうした事故の発生を防止する措置を取っておく必要性については、論を待たないわけで、事前事後をきれいに分けるという問題ではないと思う。CSIRT 活動一つにしても、別にインシデントが起こったから動くというのではなくて、日頃からインシデントが発生しないように社内で啓発を行うことが、NCA などで非常に重視されているので、そこからもお分かりいただけると思う。
- それとともに、ユーザに対して信頼を醸成するために、さらに上積みというか、自主的に良いサービス提供のための、安全、安心なモノを提供していくことは、企業としての国際競争力を保持する上ですばらしいことだと思う。
- ただ、私が申し上げたいのは、どうしてもやっぱりここだけはやっておかないと責任を負わされますよ、という点。職業柄、いざというときに法廷で争わなければならない。「先生、勝ってくださいよ」と言われるが、勝てるものは勝てますし、放置状態にあったものは頭を抱えるしかない、ということになります。

○小松崎委員

- 複数の委員の方がおっしゃったインセンティブとレベル分けについて、個人的には非常に違和感がある。というのは、フレームワークの最初に、フレームワークの策定にあたって、今まではサイバーだけであったけれど、それがフィジカルと繋がるから、今までの様に考えていたのではいけないぞ、と簡単に言えばそう書いてある。そうなると、些細に見える部分でも、そこを攻撃されると全体に大きな影響が出るかもしれない。つまり、私たちが今までサイバーだけに限

定されたものをフィジカルに繋ぐことによって発想を変えなければいけないという、これがフレームワークの一番、憲法のように大事な考え方だと思う。

- 導入のためのインセンティブ、というのは今の段階ではすごく大事。無防備な家庭というのは多い。今はそれが家庭にとどまっているかもしれないが、それがフィジカルとつながると、他へも影響が出てくるというのが今回非常に大事なポイントだと思うので、このインセンティブを果たしてこの委員会で考えることが適正なのでしょうか。もっと考えなければいけないのは、従来とはまったく違う世界観でこれを見なければいけないという、我々の基本的なマインドが変わらない中でこのテーマを考えると、現在の延長線上でやるべきことに終始してしまうのではないか、それを克服するための、基本的な考え方を変えるためのインセンティブが必要という気がします。
- 大・中・小企業のような表現、レベルの表現がありましたが、私は基本的には「安全」に企業の規模が関係してはいけないと思う。例えば、自動火災報知機がありますが、中小企業だからつけなくていいとか、大企業だからつけなければいけない、という考え方はナンセンス。物理的な規模、従来の感覚の規模ではなく、それこそ奥家課長がおっしゃったように、アセットベースではなく、フローで見た時の影響の大きさという規模で、企業の大中小ではなく、サービスネットワークの中で甚大なる影響を持っているところは、たとえ企業の規模が中規模でも、極めて重要な対策を施す必要があり、そのような影響の規模でレベル分けをするのは非常に重要だと思うのですが、それを企業の規模、物理的な規模、従来の企業の規模を判断基準とすると、まったく違う方向に行ってしまうのではないかという気がする。
- 良いサービスを作っていかないと Society5.0 はできないので、そのためのマインドチェンジのインセンティブと、そのインプリメンテーションをする時の実務的な取り組み、そのためには企業の規模ではなく影響度の規模が分かるような策を、この委員会で出すことは、次のステップのために非常に重要ではないかと思う。

○佐々木座長

- ありがとうございました。私のほうからコメントさせていただくと、パブリックコメントやそれに対する反応を紹介いただくとともに、皆様の御意見をいただき、非常に重要な形になってきたと思う。大きな流れとしては良い方向に来ていますが、さらに具体的に検討していくにあたって何が一番重要になってくるかというと、今まで通り、事務局にがんばっていただくことは必要ですけれども、やはり SWG の活動が具体化していく上で非常に必要だと思う。
- それから、横串になるのか縦串になるのか、横断的な形での SWG を作っていくということがあり、おそらく、ここでの作業が非常に重要で、これがうまくいくかどうかで、いろんな形で影響が出てくると思う。そのためには、縦で動いている SWG とも協力しなければならないし、このあたりが非常に重要だと思う。

○奥家課長

- 横串の SWG を立てて進めていくが、もっと頻度が高く、もっと具体的なところを御議論いただく形になると思う。そういった意味で、こちらの WG でも熱心に、かなり細かいところまできちんと見ていただいているが、SWG では実際に手を動かしていただくことも含めて期待を持って作業していきたいと思う。
- 座長については、引き続き、佐々木先生に議論を見ていただきつつ、皆さんにも御相談させていただくことになるかと思うので、よろしくお願いいたします。

○岡村委員

- PDCA なんて言葉を使うと、古臭いと言われるかもしれませんが、C が大事なことは言を待ちませんので、今後の展開の中で、例えば、システム監査あるいは情報セキュリティ監査という制度があるわけですから、監査法人系の方に入っていただき、先ほどのレベル分けの問題も含めて御検討をお願いするような体制作りを改めてお願いしたい。

○山角様（北川委員代理）

- 私の所属する会社は 2011 年に未知のマルウェアによる攻撃を受け、情報流出事案で世間をお騒がせしたことがある。その後も、大事にはなってはいないが、様々な形でサイバー攻撃を受けている。従い、サイバー攻撃には如何なるリスクやダメージがあるか肌身に感じており、安全保障に係る事業を有する自社の生業も踏まえて、強い内的動機を持って我々なりにセキュリティに取り組んで来ている。
- 一方、これまで、当社自身に攻撃を受けた認識はあるものの、ベンダー由来の事案は生じていない。従い、リスクの実感を持つプライムコントラクターである当社と、サブコントラクター、ベンダーとでは、サイバーセキュリティに対する危機意識や深刻度は、おそらく違うだろうと考えている。
- この研究会の場では、全員が危機意識の高いメンバで議論をし、広く産業界を啓発していく方向にあるが、実際にセキュリティへの対応、そのための投資という話になった時に、企業側がそのための費用負担をしようとの強い動機を持つことは、収益を期待する性格の投資ではないがゆえに、特に中小企業の場合、難しいのではないかと考えている。
- 第四次産業革命やコネクテッドインダストリーズの展開を考えると、日本の産業競争力という観点でも中小企業を含めて IoT 対応を進めていかなければならない中で、セキュリティの話は切っても切れない不可分のパッケージとして、IoT 投資を盛り上げていくような政策に取り組んでいただくことが、実効性も高いのではないかと思う。

○高倉委員

- インセンティブについては違和感がありまして、火災報知機にしてもシートベルトにしても役に立ったパーセンテージは本当に低い。私の車はシートベルトが機能することなく廃車になりましたが、シートベルトをつけるのは当たり前だし、今、一般家庭に火災報知機があるのも当たり前でして、なぜかというと、「もしかすると」という意識が国民の中にきちんと根付いているから、皆さん要らないかもしれないと思いながら火災報知機を設置しているし、シートベルトをつけるのも当たり前だし、エアバッグもついている。
- 私は、国民に対してセキュリティ対策をやるのは、当たり前だよね、自分は大丈夫かもしれないが、万が一に備えて必要だよねという意識を啓発していかなければいけないと思っている。それに加えて、きちんと先進的な取組をしているところには、こういうインセンティブが来ますよ、としないと、一生懸命に人参をぶら下げて、これを食べたら安全ですよ、としても、なかなか人は動かないと思う。私どもも国立大学を見張っているが、言うだけでは駄目で、地道に、「これをここまではやって下さい」というのを、啓発し、納得してもらわなければいけない。当然、経営層に対してはお金がかかる話ですと説得しなければいけない。こういったことをずっと行っているので、インセンティブだけをぶら下げれば動く社会ではないことを強く感じている。

○瓜生専門委員

- 今回、初めて参加させていただいた。IPA として経済産業省と共に作業を進めていこうと思う。

○坂下専門委員

- パブリックコメントを全部読ませていただいたが、建設的な意見が多く、皆理解されていることに感心した。
- 先ほどから中小企業の話が出てくるが、中小企業もセキュリティについては、かなり真剣に見ている。日商・東商でもサイバーセキュリティ研究会がこれから立ち上がる動きがある。中小企業は様々な企業から発注を受ける際にセキュリティ対策が契約条項に入ってくるので、どこまでやれば良いのかという問題意識を持っている。今回、フレームワークを作っていただき、SWG で議論していただき、コアな部分がどこなのか、それをどこまで中小企業がインプリメンテーションすれば契約が成り立つのかを考えている。SWG でご議論頂く中で、私どももユースケースや情報などを提供するなどして、協力をしていきたい。

○田中専門委員

- 高倉先生がソフトウェアトレーサビリティの話をされたが、サプライチェーンやバリューチェーンのセキュリティを流れに沿って確認するフレームワークをイメージすることは簡単だが、ハードウェア、ソフトウェアをきちんとトラストアンカーから辿り全部セキュアだと確認するのはかなり難しいと思っている。今の技術でできることもあるし、サイバー攻撃もどんどん進化するので、進化する攻撃に対してきちんとキャッチアップできるようなセキュリティの研究も併せてしていかなければならない。
- 技術だけではなく、制度と組み合わせて検討していかなければならない。どこまでを技術でカバーして、どこから先を制度で担保するのか、我々研究所としてもしっかり検討していかなければならないと思う。

○三角審議官

- 我が国として、こういう分野について新しいフレームワークをきちんと国際的に示すということは、ポリティカルに凄く大きい。日本全体としてどうするのか、という時にわかりやすいもの、コンセプトを示していくのは重要なこと。海外に行って国際的に評価されているところは、非常に良いと思っている。
- 今度は、御議論いただいたような形で具体的にインプリするにはどうするのか、先ほどマルチステークホルダーということだったが、様々な関係者のところに行って、どこがどう適用されるのか、もう少しコンセプトから落とした議論が必要だと思う。

自由討議の最後に、佐々木座長から、以下の発議がなされ、全委員一致で了承された。

- サイバー・フィジカル・セキュリティ対策フレームワーク案に寄せられたパブリックコメントへの対応については、いただいた意見を踏まえて修正を行い、修正したものを委員にお見せした上で、パブリックコメントの考え方として公表する。
- フレームワーク案の修正を含む今後の進め方については、資料6で事務局が示した方針で進める。

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。

- 資料 5-2 のパブリックコメントに対する考え方については、本日いただいた御指摘を踏まえ、特に、構造のところが一番大きくなってくるが、もう少し明確に言うか言わないか、寸止め的な表現、構造も入れ替える点など、より明確に書くなどの工夫させていただいた上で、近日中に公開させていただく。
- 英語での回答は、時間を要するかもしれない。例えば、本社との関係などがある日本法人は上手くフィードバックなど行っていただければと思う。
- 本日の御意見、パブリックコメントを踏まえた原案の第 2 案の御議論を、また WG1 でさせていただくが、詳細な日程については、また追って事務局より連絡させていただく。

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