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2回) 議事要旨

1. 日時・場所

日時:平成30年3月29日(木) 9時00分～11時00分

場所:経済産業省 本館2階 西3共用会議室

2. 出席者

委員 :佐々木委員(座長)、上原委員、江崎委員、太田委員、岡村委員、片山委員、北川委員、小松崎委員、斎藤委員、其山委員、高倉委員、野村委員、坂委員、平田委員、松尾委員、松本委員、渡部委員

専門委員 :江口専門委員、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、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:伊東大臣官房審議官、商務情報政策局 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、田中デバイス・情報家電戦略室長

日立製作所:石原セキュリティ戦略本部統括本部長、畠中IoTプロジェクト推進本部サイバー・フィジカル・システム部担当部長

3. 配付資料

資料1	議事次第・配布資料一覧
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の概要
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の原案
資料6	WG1の今後の進め方(案)
参考資料1	社会インフラ(水道)のサプライチェーン(プロファイル例)
参考資料2	COCN「Society5.0を支えるセキュアトラスト基盤」最終報告
参考資料3	ITサプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査～概要説明資料～

4. 議事内容

冒頭、伊東審議官から以下のとおり挨拶。

- サイバー攻撃の脅威が急激に高まっており、これに対して米国ではSP 800などの取組、欧州でもフレームワークの検討が始まっている。欧米の動きに対して何もせずに後手に回っていると、コストが上昇するだけになる。この動きで先手を取りたい。「セキュリティ対策はコストである」という指摘は違う。新規に工場を建設するのは投資だが、工場を建てる時には屋根と壁が必要。この屋根と壁は投資の一部であり、同様に、セキュリティ対策も投資の一部。
- セキュリティ品質の向上により日本の強みである信頼性を付加価値まで高めることで、日本の国際競争力のアップにつなげたい。
- データの信頼性の確保、複雑なサプライチェーン全体での信頼性の確保については世界でもまだ定まっていない。我々が先手を取って世界をリードしたい。事務局からサイバー・フィジカル・セキュリティ対策フレームワークの原案を示

すが、皆様から忌憚のない意見をいただきたい。

次に、事務局の奥家サイバーセキュリティ課長より第1回会合の説明資料の事後修正について報告があった後、佐々木座長より本日の趣旨として、事務局で作成したサイバー・フィジカル・セキュリティ対策フレームワークの原案について議論をしたい旨を説明。

続いて、事務局より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(以下、SWG)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5－1に基づいて、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概要について説明
- 資料6に基づいて、今後の進め方について説明
- 日立製作所より参考資料1に基づいて、CPS/IoTサプライチェーン適用事例、参考資料2に基づいて、COCNでの検討状況について説明

資料説明の後、以下のとおり自由討議を行った。

○小松崎委員

- 参考資料1に、水を使う側の「家庭」がフローチャートに存在せず、バリュークリエーションプロセスを考えた時に、この事例が何を何から守ろうとしているのか、どのような新たなバリューを作り出そうとしているかが読み取れない。家で水をより便利に使う、災害に強くなるなど、最終的に消費者側のバリューを生むためにこのようなアプローチをしているという流れが今回の重要な意味付けだと思う。
- フィジカルな世界である水道の供給システムの中で、今どのようにサイバーが関わっていて、今後どのような関わりになったら良い、というのが読み取れると良い。
- 参考資料1のp.2は給水システムの絵だと思うが、サイバーで今制御している部分がどこで、新しい姿ではサイバーで制御する範囲が広がるとか、サイバーの制御の質が上がるとか、バリューが読み取れないので補足説明してほしい。

○日立製作所　畠中部長

- 「家庭」が見えてこないという指摘について、参考資料 1 の p.4, 5 にあるが、水道が持続可能な形で、毎日安全な水を供給するというのがいかに難しいことかが、企業体の方々と話をして分かってきた。
- 1 日も水を止めずに供給し続けることを 50 年後も続けてやっていけるかは大変な問題。ここに対して設備投資、IT 投資を考えてやっていこうとすると、日本では 0.7%の投資しかできておらず、120 年、130 年かかる投資しかできない現状で、国の中でどう補っていくかは大きな問題。

○佐々木座長

- 後半の質問は 3 層あるという中で、どのように関わってきて、どういう形でフィードバックされるかを示すのがよい。

○奥家課長

- 今回、水道の事例を紹介したのは、三層構造の 2 層目までを地道に積み上げるとこういう取組になるという紹介。水道で一番大きいのは、アセットが古くなる中で入替えを上手く行うためにどのように管理するかにトライしている点。そういう意味では供給者側の切り口であり、苦労している点のソリューションになっている。
- 米国の CPS フレームワークは、第 2 層の途中までしかなく、第 3 層がない。米国の関係者と意見交換した際に、この

構造は非常に正しい、特に第 3 層はアンビシャスだ、と言っていた。サプライチェーンはノンリニアになっているが、認識の仕方がリニアになっていて、そこに限界がある。米国もその辺りに悩んでいる。

- 今回、第 2 層まではこうした形の積み上げでアプローチしたが、さらにその先に踏み出そうとしている事例として紹介させていただいた。

○小松崎委員

- 水道のネットワークのようにフィジカルにしか見えない世界が、実は、サイバーと連携していて、Society5.0 になると、水道というフィジカルの塊にしか見えないものでもバリューを生むプロセスになる、ということが伝わると実に効果的な事例だと感じる。
- サイバーセキュリティの観点では、家の水栓が全て制御される世の中になったとすると、悪者が一斉に水を出すというようなフィジカルな DDoS 攻撃も起こりえる。水の確保、安定供給を考えた時に、サイバー攻撃を受けた際にはフィジカルの世界で混乱が起きることを想定すべき、という問題意識で質問した。

○岡村委員

- これまで経済産業省では、安対制度から ISMS、その ISO/IEC 化をしてきた。他方で情報セキュリティ管理基準、監査基準、システム管理基準、監査基準を定めてきた。さらには、最近 Ver2.0 となったサイバーセキュリティ経営ガイドラインがある。産業界としては、どの規格に準拠したら良いか分からない。前に進める意味でも、従前の規格と関係を明確化し、整理して、どの規格に準拠すればよいのかを示すべき。
- 良いものを作っても、実効性が確保されないと意味が半減する。インセンティブをどうするのか、公的責任の振り分けをどう考えるかを整理すべき。何を、どう対策しておけば、セーフハーバーとなるのかが産業界としては大事。既存制度との関係で、例えば、電気製品安全法、PSE マーク等がある。端末、IoT 機器には明確な基準となりうるものとして、無線においては技適もあるが、そういった省を超えた連携で基準を整備し、それに合わない製品は場合によっては流通させない、さらには安全性に重大な問題のある製品は回収することで、IoT セキュリティの CIA＋S にかなうものにならないかと思う。
- 国際調和の話が出ているが、GDPR などの後追いをするのではなく、日本がリードする形で、日本の産業界の国益を考えた取組として欲しい。

○太田委員

- 各階層を整理して、階層の価値に関する 3 つの要素を整理してもらったので、フレームワークとして見えてきた。各階層におけるフレームワークの全体像は理解できるが、リスクに応じて様々な対応が存在する産業界において、そこに対する厳格度のようなもの、情報管理でだけではないので、BCP の観点とかもあり一概に厳格度という表現がよいか分からないが、どれぐらいの強度でフレームワークを守らなければならないかを示すガイドがないと、民間企業に落ちた時に最低限守ればいいだろう、という低い水準に合わされていくのではないかと懸念がある。
- それぞれの企業やデータにクレデンシャル・資格をどう与えていくか、その仕組みも課題。様々な分野で業界・業態別で ID が付与されて、その ID が付与する信頼度、厳格度がバラバラだと、集まったデータは一番低い厳格度に基づいたデータの塊にしか見えず、結果、そのようなトラストにしかならない。日本の場合、セキュリティクリアランスという観点では、民間企業はデータを持っていないので、その辺りを含めてどういう資格・権利を与えてデータを参照・送信できるという仕組みを整理すべき。
- 機器の ID についても同じような考え方で、我々が認識できるのは MAC アドレスや、IP アドレスしかないが、これらを踏み越える何かがあっても良い気がする。

○江崎委員

- 水道の話をすると、計量法との関係も大切。責任分界点をどこに置き、データがどこに上がるのかを法的根拠を含めて考える必要がある。計量法では、チャージングとコントロールに関係するのでネットワークに影響を与えないようにするために、機器の認証やメンテナンスプロセスが法的に決まっている。そういう類のところでIoT機器を考えていくこととなる。
- 優先度の話で、どの部分が高く、どの部分が低いのかをガイドラインで示さないと、詳しくない人が適切に対応できないし、機器ベンダに対してもガイドできない。
- 奥家課長から紹介のあった、欧州でのアプローチがセルフアセスメントとマルチステークホルダでやっていくことは大きなポイント。マルチステークホルダの形でやっていく中で、そこにユーザサイドが入ることが大事。ある部分はセルフアセスメントにすることで、ボトムアップ型で自立して動いていくアプローチをこの中に盛り込むと良い。マルチステークホルダの関係が上下あるという観点と、「チェーン」という言葉が適切でないとのお話もあったが、ネットワークにするか、サプライだけでなくデマンドという観点を日本から発信していくことが大事。
- 「サプライチェーン」というと結局上流から下流に流れる。インドでスズキとトヨタが協業するのは象徴的で、スズキはサプイチェーンでトヨタはデマンドチェーン。
- バリュークリエーションは良いキーワードだが、プロセスと言うとFA屋は単方向で考える。プロセスネットワークと言った方が、双方向なメッシュ型ネットワークを意識するのではないか。
- バリュークリエーションはポジティブなインセンティブだが、法的に免責をどう担保するのかという仕組みが出てくるとネガティブなインセンティブのリリースをどうするか。
- G7、その後の G20 をどう使うかが重要。コンセプト形成のためのキーワードを出していけると良い。
- 資料 5-1 の p.4 の「大量のデータの流通・連携⇒データプロテクションの重要性が増大」という表現は「プロテクション」という言葉が強すぎるので、データ管理とか少しポジティブな面とネガティブな面のバランスをとった表現がよい。

○片山委員

- 取りまとめに感謝。また、英語のパブリックコメントを出すということも、本当にすばらしいこと。世界でバラバラの規格ができても日本企業はじめ多くの企業が困る。グローバルハーモナイゼーションは重要と思う。
- 質問になるが、ISO/IEC27103 という規格の策定に日本が積極的に参加していると聞いている。こちらについて情報があれば教えていただきたい。
- 参考情報だが、リスクマネージメントを三層構造、サプライチェーンでみるという話の中では若干マイナーだが、脆弱性の存在をどう公表していくか、Coordinated vulnerability disclosure の議論が進んでいる。今年の 1 月 4 日に Spectre と Meltdown というCPUに関する脆弱性が公表されたが、どういうタイミングで誰が、どのように言うのかが課題。NIST の新しいサイバーセキュリティフレームワークでも取り上げているが、国際的なプログラムとも整合性を取る必要があると理解している。

○高倉委員

- 水道の例で話すと、先ほどの表にはレジリエンスの話がまったくない。IoT デバイスに何かあった場合、安全に止めるとあるが、弁のことを見ていない。水道では、水道圧が上がりすぎると水を川に捨てる。IoT デバイスが切れた時に、そういうメカニズムや、もしくはパッチを当てる際に不具合がおきた時に、制御不全を見据えたバイパスの水道管の有無を考えて設計しないと本当はだめだと思っている。別に、水道の話がだめだと言っている訳ではなく、たまたま水道で 2 層の話をしているので、1層から 2 層に転写する業務、作業を一方的に止めてしまうのは実は怖い作業になってしまう。
- また、資料にある「ベンダからパッチが適用されたら当ててください」は、制御屋さんに言ったら猛反対される。

○奥家課長

・ 頂いた御質問ですが、標準化、ISO を巡る動きについては、内閣官房の結城企画官が中心となって SC41 などでの取組を進めている。コメントがあればお願いしたい。

○内閣官房 内閣官房セキュリティセンター 結城企画官

・ 先ほど片山委員から「安全なIoTシステムのためのセキュリティに関する一般的枠組」のパブリックコメントの話もあったが、おかげ様で日本よりもむしろ外国で人気が出た。一般的枠組については、ISO/IEC 化すべきという話があり、現在、NWIP の投票準備に入るまでに至った。
・ 国際規格に提案するときに日本の強みは何かというと、米国への追従ではなく日本らしさがあって、岡村委員が言われた通り、特に、安全の部分は日本が担当して欲しいという話がある。そうすると、世界の市場における日本の立ち位置がはっきりし、世界への貢献というところも変わってくる。このような会議では裏でネゴシエーションするが、「じゃあわかった。このところは日本に協力する。」ということもあり、SC41 では安全な IoT のフレームワークが規格化される。
・ また、経産省・総務省が作成したガイドラインについても SC27 の方で新しい規格化がされる。現状、そういう良い流れになっている。

○奥家課長

・ 一言付け加えさせていただくと、その流れの中で NIST に、この三層構造でアプローチしたいという話をしたところ、米国からと思われる提案書に参考として「METI フレームワーク」と記載されていると聞いた。日本が前に出てくるようになっているというようにポジティブに見られ、評価され始めていると感じている。

○其山委員

・ セキュリティリスクの洗い出しが少し弱いのではないかという印象。他の委員の方からもご意見があったが、今後、リスクベースでの検討や、各 SWG における各産業のリスクの洗い出しとか、製品リスクをどう洗い出すかという点が重要になってくると思うが、そのためのリスクの洗い出し方法をフレームワークの中で示すべきなのではないか。
・ Security by Design についても、もう一歩踏み込んだ記述にしても良いのではと感じた。Security By design が対策自体かというと、対策自体ではなくもう一段うえの「概念」という気もするため、具体化した対策として示す必要があると考える。製品を作り出すときにセキュリティを考えるのは、一番安全な製品を出す第一歩であると考えるため、Security By design の考えは踏み込む必要があると考える。
・ IT と OT の融合というか、IT 側がやられたとしても OT 側で何か、レジリエンスを保ち被害を防ぐ仕組みはあって然るべきと考える。OT に関しては、我が国の強みでもある。そういった点も含めてフレームワークで対策基準の例として示されるのが良い。
・ 国際ハーモナイゼーションについて、他の委員から意見あったがやはり欧米の各基準との突合せ結果が、最終的に出てくると、使う側としては大変助かる。また、現状のサプライチェーンを考えると、日米欧だけでは足りないと思うところはあるので、将来的には考慮いただきたい。
・ 事務局からの説明にもあったが、やはり世界的に見ると IIC などが Trustworthiness などの観点を打ち出し、セーフティ、セキュリティ、リライアビリティ、プライバシー、レジリエンスについて重視をしている。本フレームワーク案では、セーフティとレジリエンスに関する言及が弱いと思うので考慮頂きたい。また、・国際ハーモナイゼーションを考えると先ほど申し上げた 5 つの観点との紐付けを考えた方が良い。
・ 今後、詳細化されると思うが、誰がどう、いつ行い、どう責任範囲を持ったら良いのか、ということが多少わかりにくいというのが感想。責任範囲等を、整理しないとふわっとしたものになってしまう。誰が、どうやってこのフレームワークを渡

して、どこに責任範囲があって、逆に、何をすれば実施者にとってインセンティブになるかを明確化にしていただきたい。

- 最終的にフレームワークをまわす際に、認証機関や MSS の活用があるが、そもそも信頼性を保つための組織自体の信頼性の担保についても、もう少し踏み込んで考えたほうが良いのではないか。MSS 等が明記されているが、現在大手企業ではプロダクト SOC を作る動きもあり、対外的な組織による対策の他に自前での対策についても認める記載してはと思う。

○松本委員

- 3 層というか、フィジカルな世界とサイバーな世界とを結ぶところということで、以前からそのようなモデルで議論すべきだと主張している者としては、それを明確に図示しており、良いと思う。
- その中で、特に、レジリエンスも言葉としてはあるが、現在洗い出されている脅威とは異なる脅威が将来出てくる可能性がある。これはいくら頑張っても出てくる。しかし、対策技術は今から作る、あるいはパッチを当てるという形もあるかもしれないが、新たに導入するものは、現在の技術でベストを尽くすことが上限であり、後は、コストであるとか、開発期間など様々な事情で、そこからグレードダウンしたものが実際は適用されることになる。そうすると将来の時間経過とともに、どうなるのかわからない部分が必ず出てきてしまう。そこをどのように底上げをするかという視点は、今回の整理の中には入っているのか。どのあたりを見ればそれがわかるか、そのような観点がなければ補足して欲しい。

○奥家課長

- L1 の 005「セキュリティ対策の PDCA 実施」というところで、常に情報をリフレッシュしながら見ていくというところ。ただ、それで十分かは検討の余地がある。

○松本委員

- PDCA というと、現在ある程度見えている世界の議論と普通は思ってしまうので、これから発見されてくる事柄があるということを見越すとサイクルではないと思う。そのあたりをどう書けば良いのかが課題。

○江崎委員

- ビル SWG で議論となったが、今あるレガシーシステムへの対応と、今から作るものを区別してやらないと混乱する。いわゆるパッチで対応するのか、あるいはデザインするのかをきちんと区別しなければならない。
- デザインしたとしても松本委員の御指摘のように未知の脅威が入ってくることが前提としてある。マーケットにおいても同じで、先進国でも当然今から作るものはあるが、存在しているものに対してどうするかということが必要。水道の例でもこれは出ていた。水道の例は、いわゆる AS-IS のものに対して対策しているが、新たに作るのであればデザインの仕方がまったく異なってくるので、区別した方が良いのではないか。
- 自助と共助と公助を組織的に考える必要がある。つまり、自分で行うこと、協力して行うこと、最後にバックアップしてくれるのは何かという点をもう少し整理すると良いのではないか。

○上原委員

- この三層構造の図を理解する上で事業者の皆さんの障害になると思われるのは、この図の抽象度がかなり高いので、この図から、事業者がそれぞれ抱えている IoT システムへマッピングするときに混濁しかねない。特に、第 2 層の図が、比較的自分たちが持っているシステムと対応がつけられそうな図に見えてしまうので、じっと眺めて自分たちのシステムにどうはめ込むかを考え込んでしまうことが、スタックしやすい原因なのかと思う。
- この図自体は凄く良いが、実際のシステムとの対応をつけるような図が必要と思う。つまり、実際のシステムにおいて、

こういうシステムのデザインがあり、そこに実装があり、運用があり、運用の中でインシデントに対する監視があり、それに対してインシデントレスポンスがあり、場合によっては BCP がある、というタイムライン、あるいは、システムのライフサイクルのような流れがある。その流れと、このフレームワークがどうマッピングされているのか、例として一枚図を描いてもらうだけでも、きっと理解がより深まる。

- 図 5 で三層ある右側に少しタイムラインが入っていて、比較的読み込める人には理解しやすいが、事業者によっては、ここでもスタックしてしまう。大変な作業をしていることは分かるが、もう一枚図が必要と思う。

○佐々木座長

- 御指摘のとおり、例がいくつかあると良いと思う。
- ハードだけの世界とソフトだけの世界はこの図でいけると思うが、例えば、SNS のようなサービスの話ではデータが上に行くのか、下に行くのか微妙だと思う。そういったことも含めて、例があった方が良い。

○野村委員

- 3 層に分けた整理は、今後検討を進めるにあたって、頭の整理の第一歩となるので非常にありがたい。電力会社においても、スマートメータにより計測した電気使用量を公共財として活用いただくこともありうると考えており、電力設備の調達に関するサイバーセキュリティのみとは考えていない。
- 電力は社会インフラであり、電力が止まると公共交通機関など地域への影響が非常に大きい。先ほど新しい設備、レガシーな設備への対応という意見があったが、電力設備自体は非常にライフサイクルが長いものなので、長い目でみた運用保守の観点でのサイバーセキュリティ確保というのは、非常に重要である。新旧機器が混在する中で実効性を確保した上で、優先度付けをする必要がある。
- セキュリティ対策項目が提示され、今後、詳細検討を進めていくことになると思うが、制度ができたときに浸透させる仕組みが重要である。認証かもしれないが、そういった仕組みを考えていく必要がある。我々の電力設備での現場業務をイメージすると、例えば、検査項目を整理しないと実効性が伴わない。
- 質問だが、米国や欧州では、中小企業を中心にどういった対策を進めているか、教えてほしい。

○奥家課長

- 質問についてお答えしたい。欧米、特に米国についてはしっかりしている。中小企業については、同じように悩んでいる。米国の場合、連邦政府レベルではガイドラインで閉じざるを得ず、直接のリーチはできていない。州政府レベルで支援をするしかないが、中小企業支援政策全体の流れの中で米国の識者と意見交換をしているとサイバーセキュリティは経営リスクである、サプライチェーンからはじき出されるかもしれない、というところまで理解している州政府自体が少ないと思う。したがって、ニューヨーク、カリフォルニア、マサチューセッツぐらいだと州政府も少し理解をしているかもしれないが、あまり目に見えるような政府側の支援は聞いたことがない。
- 一方で、中小企業を含めたセキュリティ対策をしなければならないと考えている NPO から、中小企業のセキュリティ対策を支援するための可視化ツールを作ってみたということで、日米で連携できないかという相談がきている。日本も同じように悩んでいて、IPA でも可視化ツールなどを作ったりしているが、どうにかして支援ツールを普及させることで、レベルを上げていくことができないかという問題意識があると理解している。

○渡部委員

- 非常に項目が多く、実際にどれを実施するかというときに、重み付けをしていかなければならない。
- 優先度という話が多く出てきたが、リスクの共有が重要だと思うのでそれについて説明する。リスク分析をした後、対応するものの優先度を決めて、我が社としてこれから対策していこうという項目が出てくることになる。其山委員からもリス

ク分析が甘いという話があったが、自分たちのリスクを考えることは非常に簡単だと思うし、第1層は非常にわかりやすいが、これが第2層で自社から出たデータが第3層に行ったとき、どこでどんなことが起きるのか私には想像がつかない。

- 他のところで起きていることを知らないと、そこに対する対策が自分の組織の中では取られないというか、遅れてしまうことがあるので、どういうところで自分たちの取組がリスクだと思われているのか、そういったリスクの共有を、業界を超えてできると、「ここに対策をしよう」というのが出てくるのではないか。自社のリスクを人に言うのは辛いことだが、そういう場がどこかに出てくるとよいと思う。

○坂委員

- グローバルハーモナイゼーションについて、我々自動車産業としてグローバルに製品を製造して売っていく中で、さらに従来型のサプライチェーンをグローバルに幅広く持っている中で、グローバルな動きを取り入れて進めていただき、相互認証が実現できる、ということに期待している。というか、現実にそうならないと我々としてやっていけないが、一方で単なる追従では意味が無いので、早く進めていただくのが大事。遅いと逆に独自性を出さなければいけなくなり、我々としては他の地域で使いにくいものになってしまう。今のスピード感で進めていただけるとありがたい。
- トレーサビリティについては、L1で生産したものの管理という観点で述べられているが、自動車産業は幅広い部品を使っているので、どこまでやるのかという点については、自動車産業だけではなく製造業全般になるかもしれないが、議論をしていかないといけないし、全体の視点、産業別などの細かい例などを今後示していかなければならないと思う。
- バリューチェーン全体の中でのデータのトレーサビリティについて、L1のところに書かれているが、当然のようにL2、L3のところにも入って、様々なところに書き込まれているように見えるが、同じ形ではないと思うので、もっと明確に打ち出す必要があるのではないかと思う。

○平田委員

- Society 5.0を具体的にどう進めていくかの目標が示された点は良いと考える。
- 資料5-1の「Society 5.0が実現する社会」の後、いきなり「サイバー攻撃の脅威の拡大」の話になっているが、Society5.0が生む価値について、具体例でよいのでもう少し補足したほうが良いのではないか。
- 流通させなければいけないデータを明らかにし、提供側の倫理だけでなく受け手側の視点で何が信頼に足るだろうか、という点を考えていただけると良い。サイバー空間に上がったデータを受け取る側でどう使うかでリスクの大きさが変わってくるので、そういった視点があっても良いのではないか。
- サプライチェーンを考える上では、責任分界点を整理していく必要があると考える。CPS、企業、業界それぞれ責任範囲があって、どう関係していくかを示してもらえると事業者として取り組みやすい。
- トラストの考え方は、今の図で見ると第1層のトラストに近いものに見える。層毎で「トラスト」の考え方が異なるのではないか。
- 中小企業でも実現できる対策としてコストやスピード感が重要。ダブルスタンダードにならないよう、今のルールでできているものと、これから決めていかないといけないもの、これらを決めることでデータ流通が促進するものは何か、という視点で考えていただきたい。

○小松崎委員

- 責任分界点を明確にする必要性はそのとおりと思うが、逆に今まで馴染んできた考え方で整理しても今までと同じことしかできないという問題意識も必要。
- 米国が非常に期待しているというのは、彼らが従来やっている手法と違う手法をやるから興味を持っているのではないか。我々が慣れ親しんでいた従来の方式を少し否定してかからないと、面白みが出にくいのではないか。そういう意味

ではもう少し違和感があってもよいと逆に考える。フレームワークのアプローチや考え方は、特に、その方面の人にとっては違和感があり、具体的にどのようにすればよいか当惑もある。逆に言うとそういう風なことだから、日本の力を持たせるための新しい試みとして価値があるに違いない。我々がみんななじむような考え方、いいねと思うことだったら新鮮味がないので価値が出ないだろう。

- 責任分界という点では、従来のアセットベースのリスクマネージメントではなくてネットワークのバリューチェーンで考えるのは非常に大事な考え方だと思う。それが今までできなかったのは、責任分界点を決めないと各企業は具体的なアクションを起こせないので分断せざるを得なかった。サプライチェーン全体でリスクを考えれば、必ず接合点には曖昧な部分があるわけで、それが明確になっていないのは当たり前だという見方をしなければいけないと思う。
- 従来の感覚で明確に慣れている私たち企業は、曖昧であることには不慣れなので、チェーンとして物を見たときにどうなるのか、各企業の責任分界点という従来の仕組みで始末するのではなく、もう一段上のレベルで、はっきりしない部分については共有する等、お互いのマナーみたいなことが決まれば、もう少しオペレーションチェーンでリスクを見るという考え方ができるのではないかと思う。今日、この分野で研究されてきた方々が違和感を抱くことをあまり気にしないで欲しい。むしろ違和感があるということが必要条件ではないかと考えている。
- ただし、解決の方向感に甘い部分もあることも間違いないと思うので、方向性が感じられる記述を少し加えていただくことがとても重要ではないかと思う。

○松尾委員

- フレームワークの6つの構成要素のうちデータについて、データ区分が新たに決まるとのことで、これが法令に従ってとのことだが、データを流通するためには共通的な定義・区分が必要と思う。
- 人の定義に関しては、L3のレベルではユーザーという言葉が出てくるが、ユーザーであり価値を創造する提供者ということになると思うので、組織の中の人というのは正しいと思うが、ユーザーというのが組織の中の役割を持った人なのか、個々の人なのかを明確にする必要がある。特に、個人という者については訓練とか教育とかある程度資格をアサインするとか底上げが必要と思う。

○太田委員

- 国際ハーモナイゼーションという観点で、米国も日本の積極的な活動について評価しているという話があったが、現実のところ日本企業においても防衛産業においてはNIST SP 800-171を要求されているという現実がある。
- 今回のフレームワークという位置づけとSP 800-171の両方を現場では見ていかなければならない企業が多く出てくる訳で、そのとき今回のフレームワークそのものは、SP 800-171をにらみながら、そこの要件も踏襲していくぞという意思を確認させていただきたい。

○奥家課長

- SP 800-171は当然参照している。SWGで防衛産業の取組も進めていくものと思っている。

○岡村委員

- 今、太田委員がおっしゃった点は、全体で検討するにはあまりに重過ぎるので、一般企業向けの基本的な基準の上に、対象領域企業向けのサブセットみたいな形で特則的な基準を設けるという考え方もひとつにはあるのではないか。
- 産業構造審議会不正競争防止小委員会において、営業秘密を拡張する形で限定提供データ保護に取り組んでいる。これは、これまでのスタンドアローンの企業が持つノウハウというよりは、グループまたはサプライチェーンでデータを共有する場合に、どのように安全性を確保する一方で、利活用ができるようにするかという観点を取り組んでいる。パートが違うといっても同一省内での取組なので、そういう新制度も利活用していただければと思う。

・ 片山委員から情報提供のあったソフトウェア製品等の脆弱性関連情報については、昨年、新たにソフトウェア製品等の脆弱性関連情報に関する取扱い規定ができた。それを踏まえて、情報セキュリティ早期警戒パートナーシップガイドラインということでIPAへまず通報の後、JPCERTがベンダとの調整を図って安全になった段階で公表するという協定がある。国際的には、FIRSTといった組織に人も派遣しているので、そういう制度を利活用すべきということも言うべきだと思う。同様に、CSIRT協議会あるいはフィッシング対策協議会等々に情報共有体制があり、公助と並んで民間の共助ということも、背後には国際的なネットワークが控えているので、もう少しそれらの情報を共有していただくことも重要。

○江崎委員

・ 民間共助はとても重要なこと。一方で、グローバルハーモナイゼーションの中でのルール形成はとても大事だと思う。今回、防衛省の調達関係がほぼ米国と同じようなサプライチェーンに関してやっていくことができたことも非常に意味があると思う。
・ 政府として調達をどうやっていくのか。現状のドキュメントではほとんど民へ放り投げているように見受けられる。特に米国が政府調達のインパクトを考えながら取り組んでいることを考えると、今日御同席いただいている各省庁すべてが適切に対応してくれるとかなりのマーケットになると思う。国として調達をコントロールできると大きいと思うので、サプライチェーンの中の1つのセグメントとして国を考えると良いのではないか。特に、ガラパゴスではなく、グローバルハーモナイゼーションに沿った形での調達の部分をきちんと作っていくことでマーケットスケールとしても大きくなり、官と民の協調関係が出来ていくのではないか。
・ 報告書の方向性として、単純にサービスセクター(民)がどうしなさいということだけではなくて、それをリーディングしていくパブリックセクター(官)があるのかについても意識してほしい。今回、調達に関して防衛省が取組を始めたのは大きなインパクトだと思うので、それも戦略に入れていくことが大事だと思う。

○斎藤委員

・ 三層構造で素晴らしいなと思うのは、各層の生み出す価値をきちんと分けて、それに対して信頼の要素がどうあるべきかの議論ができるフレームワークになっていること。
・ 今後の検討に向けて、資料5-1のp.5にある「フレームワークを策定する目的」の「必要な要件」の特に①、実際にこの検討会を含めて出来上がった制度や仕掛けがあったときに、本当に各事業者含めてステークホルダーがフィージビリティを持ってオペレーションできるのかがとても関心事で、そういう意味では②のコストの話も、実は中小企業を含めて実施したいけれど、お金がない、人がいない、リソース問題も含めてフィージビリティがあるかについて、今後どうすればフィージビリティが向上するのか、上げる方策の検討が必要と思う。
・ 今までのサプライチェーンが上流から下流という一本のチェーンというのは、江崎委員はネットワークという言葉も使っていたが一本ではなく、サプライだけでなくデマンドという方向も含めると、どの時点で、例えば、製造業では工場で組み立てる時点の信頼を誰がどう担保するのかという意味で言うと、工場は当然部品を調達することと、エンドユーザー又は次のお客様にサービスをデリバリーするという両面を持っていて、デマンドチェーンの世界とサプライのチェーンの世界を両方持っている。
・ 家庭、エンドユーザーから見た時は、基本的にデマンドチェーンしかない。デマンドチェーンを見たときにどこまで遡るのか。例えば、牛肉が本当に国産であるかとか生産地保証とかそういう話までやるとすると、どこまでチェーンを追いかけてどこまで責任を負っていただくのか、どこまでを責任範囲としてカバーするのか、そこが無いと我々企業も含めてどこまで担保すれば十分かという、皆さんの心配が解決しないと思っている。
・ これからは、どこからのポイントで、どちらの方向のベクトルで、どこまでの範囲で、どれぐらいの深さでという観点が三層構造の中にそれぞれ埋め込まれる必要がある。また、三層構造で言うと三層の中は良いが、層を超えた部分、先ほど、一層の人が三層で何が起きているかわからないことをどうやって担保するのか。そもそも知る必要があるのか、ある

いは知る権利があるのか、知ろうとするとどうすればよいのかという観点を含めて今回、良いところまで到達している感じはするが、まだまだこれから検討する課題もあると思う。

○北川委員

- 経営管理側の立場、防衛・宇宙基盤の一企業の人間として、防衛・宇宙事業に関わり、磐石な安全保障を我が国が関係する諸外国と構築する上で、この委員会で検討していただいている情報セキュリティは非常に重要な分野の一つであると考えている。
- 本日、防衛装備庁に御陪席いただいているが、同庁主催の第6回官民合同検討会が本日開催され、本研究会のSWGの位置づけでこのWG1の成果を受けながら、防衛装備庁から御指導を頂戴しつつ、防衛装備品に対しての情報セキュリティを磐石のものとすべく、議論する予定。
- その中で、防衛装備庁が特に重視しているのが資料5の第1階層の部分と認識している。具体的な企業間のつながりにかかるセキュリティ対策から第一層、二層、三層に対しての具体的対策をどう実装していくのか、誰がインターフェースを確保しながら落とし込んでいくのかが重要。
- 先ほど民間に放り投げているという御意見もあったが、防衛産業に関しては、官民合同検討会は既に6回を数え、昨年度から防衛装備庁から御指導いただく中で、官民一体となって検討を進めている。確かに、米国向けの輸出適合という点においては、米国政府と契約した米国プライム企業と我が国民間企業との民々契約の話なので、防衛省に相談する話ではなく民間企業として進めねばならなかったが、その中で得た教訓もいろいろあった。それに加えて今回の委員会で皆様から出た御意見・御提案を反映しながらSWGのなかで、防衛産業環境におけるセキュリティ対策を、速やかに実現すべきと思っている。先手を取らねばならないとおっしゃった審議官の言葉をお借りするとしたら、先手を取る上で、いかに早く真に実行に足る具体的な方策に落とし込むかをしっかり考えていくのが、この委員会を受けての後流側、下流側でのSWGの動きとして不可欠と思う。
- SWGあるいはこのWG1でブラアッシュアップいただくと思うが、並行してSWGがいかに有効に機能するかという点に、防衛産業における、あるべき情報セキュリティの成否がかかっていると思う。そこは防衛装備庁さんと連携を強化しながら、本日先生方からいただいた御意見にあるように、政府としての御支援をいただきつつ、防衛産業としても取り組んでいきたい。

○江口専門委員

- 参考資料3として、「ITサプライチェーンの業務委託におけるセキュリティインシデントおよびマネジメントに関する調査」の報告書を今週公表したので皆様に概要を配布させていただいた。この調査で分かったこと、感じたことを3点お伝えしたい。
- 1点目は、様々なインシデント・トラブルが発生するが、自社で何かトラブルが起きる以外、業務委託先、さらにはパートナーが問題を起こして自社のトラブルにつながっていくというのが多々あること。
- 2点目は、他社・関係会社でトラブルが起こるということを事前に理解していないといけないが、外部に委託する際にリスクを事前にきちんと分析をしているかをアンケートしてみると、まだまだできていない企業の数が多いこと。業種によっても相当違い、金融など規制が強いところは分析をした上で発注しているところが多いが、一般的に見るとまだまだ低い。
- 責任分界点という話になるが、どこまで何をやったら良いかは、通常であれば契約書の中に盛り込むのが一般的だと思う。今日の議論の中で責任分界点を少し曖昧にして何か別の方法もあるのではないかという御意見もあったので、そういう方法もサプライチェーン全体で見たらあるのではないかと私自身も考えながら聞いていた。ただし、責任関係をはっきりさせることができる部分においても、事前に契約で取決めを適切に行っている企業はさほど多くないといのが実情というのが3点目。

○岡村委員

- IPAから責任範囲の明確化が課題だという話があったが、実際のところ、これが明確化されないと、メーカ等の企業としては、いわゆる損害保険の付保によるリスクへのカバーができず、被害を填補することすら困難になる。そういった点からも、企業にも消費者にも大きな点だと指摘する。

最後に、佐々木座長から以下のとおり自由討議の総括がなされた。

- 本日の議論を一言でまとめるのは難しいが、三層モデルについては大筋良かったのではと思う。
- 変更管理みたいな形をSecurity by Designで行うことは大変で、必ず変わっていくので、そこを考えられるといいねとか、法的な問題、制度的な問題、グローバルの関係でもいろいろ意見を頂戴した。ここに書かれたフレームワークをそれぞれ様々な立場の人がいる中で、どのように使っていくのかを明確にしていくのが大事という御指摘は、非常に重要だと思う。
- サプライチェーンだけでなくデマンドチェーンという形で考えたらどうなるのか、という御指摘もなるほどと思い、どのように反映したら良いか考えたいと思う。
- 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の原案については、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パブリックコメントを行いたい。パブリックコメントを実施するフレームワークの最終的な案については、座長一任とさせていただきたいですが、よろしいでしょうか。
  （上記発議に対して、全委員一致で異議なし）

最後に事務局から、パブリックコメントを4月下旬に実施予定である旨、第3回のWG1をパブリックコメント終了後以降に開催する予定である旨、連絡を行った後、閉会した。

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