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4回) 議事要旨

1. 日時・場所

日時:平成30年12月25日(火) 10時00分～12時00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、江崎委員、太田委員、片山委員、北川委員、小松崎委員、石原様(斎藤委員代理)、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 :小川様(瓜生専門委員代理)、岡田様(坂下専門委員代理)、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、土屋サイバーセキュリティ課企画官、加畑サイバーセキュリティ課長補佐

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 サイバー・フィジカル・セキュリティ対策フレームワーク(第二案)について

資料6 サイバー・フィジカル・セキュリティ対策フレームワーク(第二案)

資料7 サイバー・フィジカル・セキュリティの確保に向けた取組

4. 議事内容

冒頭、西山局長から以下のとおり挨拶。

- Society5.0 という大きなテーマのもとに様々な政策を検討している。また、グローバルでアーキテクチャ構築競争が起こりつつあると考えている。そういった中で、サイバー・フィジカル・セキュリティ対策のフレームワークとして、企業のつながりの層、フィジカル層とサイバー層の間を転写する層、そしてサイバー層の三層構造としている。このように三層に分けてサイバーセキュリティの全体像を議論することは、狭い意味でのサイバーセキュリティの対策にとどまらず、様々なアーキテクチャの構築に日本として発信、貢献することが出来る大きな機会と考えている。
- このワーキンググループの下で、様々なサブワーキンググループで具体的な課題を議論が行われているとのことで、本ワーキングにおいても活発な議論をよろしくお願いする。

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。

- 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 及び資料 6 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(第二案)の修正ポイントにつ

いて説明。
・ 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。

江崎委員からビルサブワーキンググループ、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活動状況について、また、松本委員から産業技術総合研究所サイバーフィジカルセキュリティ研究センターの概要についてそれぞれ紹介いただいた後、以下のとおり自由討議を行った。

○片山委員
・ 元々の夏前に出た案を、ある意味 3 倍に増したと言うか、ポリシーと対策も付け加えた形になっているので大変な作業だったと思われる。
・ 奥家課長からもヨーロッパ、米国の動きの話がいろいろとございました。事実、例えば、ヨーロッパの場合は IoT に関して認証という言葉もキーワードとして出てきている。これから各国で議論がいろいろ進む中で、グローバルの協調を是非続けていただきたい。奇しくも先週の金曜日 12 月 21 日に米国、英国、日本が協調して APT10 に対して声明を出したようにグローバルでの動きというのは非常に大事になっている。
・ 質問とお願いですが、ファイナルのバージョンに向けてパブリックコメントを出すと思いますが、その辺りのスケジュール感を教えていただきたいのと、英語になった段階で私自身も米国、ヨーロッパの同僚にも見せたいのですが、さすがに 30 日では、ほかの国では 60 日という期間が多い中、グローバルで色々対応していくと考えた時には短いので、インプットできる時間が十分あれば良いと思っている。

○加畑課長補佐
・ パブコメに関しては、資料5の最後のページに、この後のスケジュール概要を記載している。本日のワーキンググループでいただいた議論の内容を取りまとめて、年明けにはパブコメを開始したいと思っている。パブコメの期間については、前回も海外の方から、30 日だと短いという御指摘をいただいており、2 月末まで実施できないかと考えている。今の想定としては、1 月の上旬に開始し、2 月末まで、日本語、英語共にパブリックコメントを出したいと思っている。
・ グローバルの状況は、御説明したとおりかなり動きがあり、かつ米国も欧州も、まだこれと言って完全に方向性を固めているような状況ではない。そうした中だからこそ、その進捗を見ながら、ハーモナイゼーションをとりながら進めていきたいと思っている。引き続き御指摘いただきたい。

○江崎委員
・ 資料 5 の 5 ページですが、背景の Society 5.0 におけるサプライチェーンの構造変化というところで一番下のところに、奥家課長からもございましたけども、インターネット接続されないシステムと認識していても、このような脅威が入ってくるということを、ここに書いていただいているということは、いわゆる本当に危ないセクションの方々へのメッセージで、とても重要になっていくと思う。できれば本文の方にもしっかりと書き込んだ方がよいのではないかと思う。
・ つまり、このドキュメントを読むべき人のステークホルダーとして、当然セキュリティ専門家以外の人達にしっかりと認識いただくことがとても重要だと思う。みんな最初の部分しか読まないので、そこでその人達が読まなきゃいけないですよ、というところを認識していただく形が重要ではないかと思います。
・ 先程グローバルな話が必要だと片山委員から御指摘があったが、グローバルな観点では少しバイアスのかかった意見が今サイバーセキュリティに関しては起きているということを、少し気にした方が良いかなと思う。このドキュメントは、リスクアセスメントに対して、各国の法律の問題を含めてアセスメントをしっかりやりなさいというスタンスで書いてあり、

それを事実関係に基づいてガバナンスも含めた形でやりなさいというのがこのベストスタンスと思います。そこはしっかりと抑えておくべきだろうと思う。ニュートラルに、グローバル視点で、どうやってサプライチェーンのサイバーセキュリティを守っていくかということを客観的に示しているものだ、というスタンスをしっかり持った方が良いと考えます。

○加畑課長補佐

- ご指摘いただいた、従来のサプライチェーンで閉じたシステムであってもセキュリティ対策をやらなければいけないというメッセージについては、概要の方には入れさせていただいたこともあり、奥家とも相談するが、本文の方にもその趣旨を取り入れた形で出せるようにしたいと思っている。
- 色々な委員の方や、サブワーキングの委員の方と話をしていても、このフレームワークを誰が読むべきかが議論に出る。Society5.0 の社会で、データを共有する人だけがやれば良いのかというと、そうではなく、これから先、Society5.0 を目指していく方はやらなければいけない部分はあると思っており、そこの部分はしっかりと書き込んでいきたい。

○江崎委員

- 目指す人じゃなくて目指さない人も繋がってしまうということ言わなければいけない。

○加畑課長補佐

- 御指摘のとおり、これからSociety5.0の社会になっていくと、目指していない人も繋がっている部分はあると思うので、そこは表現を工夫する。
- 二点目はまさにおっしゃるとおりで、このフレームワークは、特定の国を排除するとかそういった目的ではなく、Society5.0 のアーキテクチャの中で、しっかりセキュリティ対策をしなければいけないものを整理したもの。これはニュートラルな形でやっているものなので、その点を強調していきたいと思う。

○小川様(瓜生専門委員 代理)

- 添付 C で SP800-171 との比較対応付けがなされているが、SP800-171 は理解するところでは、SP800-53 のインパクトモデル等に対応する CUI の保護規則であり、このフレームワークはリスクインパクトとして、やはりモデル限定なのか、それともそういう縛りはないのか。
- 対策の Basic、Advanced、High Advanced という分け方の基準があれば教えていただきたい。

○加畑課長補佐

- 質問はリスクの回避とか軽減などを比較してモデレートの部分、提言を取り上げているのかということの確認か。

○小川様(瓜生専門委員 代理)

- 添付 D-2 での比較では、モデレートをカバーしているという理解だけで良いのか、フレームワーク自体はモデルだけではなく、もっと危ないリスクも考えているかという確認をしたい。

○加畑課長補佐

- 添付 D-2 は、SP800-171 が対象としているモデレートのところの比較。フレームワーク自体は、もう少し危ないところも含めている。フレームワークの中では対策の種類は全体を網羅できるように挙げており、レベルも High から Basic まで挙げているが、どの水準までやらなければいけないかについては、分野ごとの検討の中で決めていく必要があると思っている。フレームワーク自体は、高いレベルから低いレベルまで全体をカバーできるような形を目指している。

・ 対策の Basic、Advanced 等の基準の説明は、SP800-53 や、中小企業向け対策ガイドラインなども参照しながら、この辺りは確実に全部やって欲しいところは Basic、難しいが今後やっていて欲しい対策は、High Advanced にしている。NIST の SP800-53 等の既存の文書にもないものについては、事務局の判断で決めており、例えば、今時点で、全ての方にとり入れてもらうことではないが、セキュリティ対策を考えると実施してほしいことについては、High Advanced のところに入れている。

○岩見委員

・ フレームワークについては、初版と比べて非常に見やすく、分かりやすくなったという印象。特に、対策例についても、範囲、それから Advanced、Basic 等に分けられて、ユーザーの立場から見やすいものになったと思っている。
・ これからまた、パブリックコメントを実施して様々な意見を反映していただければと思っているが、これだけ膨大なものになっていると、見直しが非常に大変になってくる。体制も含めて、検討していただければと思っている。

○奥家課長

・ 見直しは想定しなければいけないと思っている。経済産業省の関係機関の支援も受けながら、しっかりとやっていく。今回、この三部構成に直したのは、見直しやすくするというのも目的であった。見直しに関しては、視野に入れてしっかりやってきたいと思う。

○坂委員

・ 見直しについては、このフレームワーク案のエクゼクティブサマリーの最後にも書かれているが、改正は重要なので、できれば本文のどこかに改正についてまとめると分かりやすいのではないかと思う。
・ 今回のユースケースとして、製造過程の例と将来のコネクテッドカーの例を挙げているが、我々自動車産業は、両方共にかかわっている。今まで自動車サブワーキングが設置できおらず、どうやっていこうかというところがあったが、ここにユースケースを挙げていただいたので、今後、これらを参考に進めていきたいと考えている。
・ 自動車産業として、この第 1 層、第 2 層、第 3 層に分けているところについてコメントだが、まさにユースケースや、このフレームワーク案のとこにも書かれているが、第 1 層がフィジカルというケースもあるし、企業間、組織間というところとあって、少しそこが分かりにくく混乱している。
・ 図においても、特にこのユースケースの所で、緑の線が第 1 層だと思われるが、これが第 3 層の中にも多く描かれている。例えば、このフレームワーク案の 14 ページなどの概念図のところも、第 1 層のところに、サイバー間の中にも赤い線で描いているもの、無いものもある。フィジカル空間のところしか無いように見えるものもあるので、その辺りが混乱するのではないかと思う。

○奥家課長

・ 第 1 層では、信頼性のアンカーポイントを組織のマネジメントに置いています。したがって、今の世界で言うと、企業単体での取り組みはもう第 1 層だと思っていただたい。それが、14 ページで、例えば、第 1 層のところで、上側のサイバー空間のデータの取引のところが入っているのは何故だという質問をいただいたが、これは、信頼できる企業間でのデータのやり取りはこれまでも ISMS とかそういった取り扱いになっていたということを示している。
・ 第 1 層の特徴を明確に図として書いているのは 29 ページで、基本的にバリュークリエーションプロセスという動的なサプライチェーンが来る前のサプライチェーンにおいては、直線的・定型的なサプライチェーンの中で、各企業自体が信頼できるのであれば、そのサプライチェーンは信頼できるものであるという世界が第 1 層である。したがって、フィジカルに閉じ込めるという発想ではなくて、むしろ、企業単体の取り組みとして第 1 層を捉えていて、これは一貫して

いる。

- 一方で、30 ページにあるとおり、バリュークリエーションプロセスという形でサイバーフィジカルが一体化した産業社会になってくると、サイバー空間とフィジカル空間の境界線というのが出てくるのと、データを扱うサイバー空間というのは拡大して、データのやり取りというのが固定された決まった企業間だけではなく、世界に広がっていく。即ち、新しい観点からの取り組みを加えていかないといけない。今までの工場内にあった機器も、そういったデータを使うようなところに接続させられていったりする中で、第 2 層の境界にどんどん巻き込まれていく。また、サイバー空間に広がっているデータを自由に使えるようになる。ここの新しい層を第 1 層にはめていくと、新しくリスク原因が出てくるというのが基本的な考え方である。
- したがって、第 1 層をフィジカル空間と捉えるのは、ややずれていると理解していただけると思う。第 1 層のところは ISMS 等をしっかりやってきたことがベースになった上で、更に、第 2 層の観点、第 3 層の観点を追加で乗せていくという取り組みができ、ステップアップしていくことができる。
- この資料や、委員からも御指摘をいただいたが、今までの既存のシステムだから良いのだと思っていたら、データに繋がったり、サイバー攻撃の色々なパターンが出てきたりすると、今まで独立していたはずのシステムに、新しいリスク源というのが出てくる、この観点も外さないで欲しいというような議論にも繋がってくると思っている。

○江崎委員

- 第 1 層が現状の企業体に近いということだと思う。第 2 層、第 3 層は、いわゆる新しいビジネスセクターと言うか、領域だというようなところが、書かれていると良いのではと思う。
- フレームワークに含めることではないと思うが、政策的な考え方からすると、第 1 層のところというのは、As-Is の今の企業体としての話になり、第 2 層と第 3 層は今でもあるが、新しく伸びるところ。それに対してそこのマネジメントするところが、サイバーセキュリティとしては新しいビジネスセクターだというところがあると、産業政策としての立ち位置というのが凄く明確になっていく。また、そこへの活動が投資として成立していくという話を少し整理しておくと、非常に産業界の方々が動きやすくなるのではないか。
- そういった観点で言うと、企業ガバナンスの中に、特に、企業会計の中にこれをどうしていくか、企業ガバナンスの中にどう埋め込んでいくかというところは、まだ書かれてないところで、手が付けられてないところ。例えば、企業会計の基準の中に、どういうふうにサイバーセキュリティを入れていくかという話は、一応は出てきたと思うが、あまり書かれてない。私も社外取締役などをやっているが、その辺りの議論はなかなか取締役会で出てこない、暫定的にどう捉えれば良いのかというシステムが、まだでき上がっていない。
- いわゆるサイバーセキュリティの専門家としての議論としては良いが、それこそ今後のアップデートだと思うが、企業ガバナンスという観点が、少し議論の中から抜けていたと思う。

○奥家課長

- 企業ガバナンスとサイバーセキュリティの取り組みを結び付けるというテーマについては、主にワーキンググループ 2 で議論している。今までのところ、例えば、投資家から見てサイバーセキュリティがビジネスリスクであるということを理解いただいた上で、投資家から見たいと思ってもらうような環境を作っていかないと、ということで投資家へのアプローチを仕掛けたり、もしくは取締役会の実効性評価の項目にサイバーセキュリティの取り組みを入れてみたり、様々な取り組みを進めてきている。
- 更に現在、コーポレートガバナンスシステムガイドラインの見直し作業が経済産業政策局で進められている。新しくグループ企業のガバナンスという概念を入れないといけない。そのグループガバナンスの中にサイバーセキュリティを反映しようという方向で議論していただいている。年度内に新しいガバナンスガイドラインが出てきた時に、サイバー

セキュリティが位置付けられていくようなフッキングをする。そうなってくると、このフレームワークが固まると、リスクアセスメントのツールとして使っていただくことができ、より強いタイを結んでいける、というように一応視野に入れて、それぞれ各ワーキンググループの検討のところを上手くフッキングしながら進めていきたいと思っている。

○小松崎委員

- グローバル化に関して、実際にそれを適用する側に立ってみると、作られたポリシーだけではなくて、そのポリシーがどこの国で、どういうふうに採用されるであろうというところまで読めていくと大変助かる。電気や通信の基準は、旧盟主国が作ったものを基本的に踏襲する傾向が見られる。本件に関しても、どう作られているかということに加えて、その実際の産業を考えると、それがどのように使われそうだという分析も加えていただくとありがたい。
- セコムの業務で申し上げると、フィジカルな仕事を中心にやってきた会社であるので、ユースケースの中も含めてフィジカル領域に書かれているものが、実は供給側が殆どで、受益者側があまり出ていないことが少し物足りない気がする。
- 極論すると、今、第 1 層の世界では、一切 ICT を使わずに人間対人間で提供されているサービスというのもある訳だが、これは長期的に見ると Society 5.0 で最も対処しなければいけないサービスである可能性がある。そこに ICT を入れて、根本的に変えれば、国の負担は減っていくという意味では、最も対処しなければいけないのは、フィジカルの世界でしか動いてないような仕組みという見方もできなくはないと思う。したがって、利用者側の状態と、供給側の状態が、フィジカルの世界だけに留まり、殆ど ICT が使われてない領域というのも、スマートホームとしては考えていきたいと思っている。
- そのようなことを、できればフィードバックをして、そこに対して、このフレームワークの中で触れていただくことができれば、Society 5.0 へタッチする領域が広がるかと考えている。奥家課長のお考えを少し聞かせていただければと思う。

○奥家課長

- 一点目の各国の取り組み状況に関しては、ご案内のとおり、ISMS については日本が一番認証を取得している。BSI から発祥しているので、イギリスとか欧州の国がその後に続いている状況。こういう状況の中で、やっぱり PDCA サイクルというよりも、実際のインシデントハンドリングを意識したような形で、ファイブステップアプローチを取っている米国の NIST サイバーセキュリティフレームワークは、使いやすいという評価を米国国内では受けており、皆が参照して実際に使っている。米国は、ここの部分を今、国際標準として提案している。また、シンガポールでも、結構積極的に動いているという実態がある。
- 一方で国際標準の世界は、過去に整理したこととの整合性などの議論が中心になっているので、かなり苦労している。実態としては、より使いやすいもの使っていこうという方向で動いていると思っている。おそらく、最初に説明した様に、欧州もベストプラクティスとタキソノミーにかなり注力しているのも、やっぱり参考になるものを、まずは出していこうとしている印象を持っています。
- 私達のサイバーセキュリティフレームワークは、新しい社会になってきた時のコンセプト部分が、みんな無いまま、やや突っ込んでいるところもあるので、全体を整理した上で、比較的使われている NIST サイバーセキュリティフレームワークの繋ぎ込みなどをかなり意識した形で作ることで、定着できるようにしていく、というのが基本的な考え方。海外との関係では、頻繁に海外に行っていることに加えて、ほぼ毎日、海外からのゲストが当課を来訪し、情報が相当集まっている。この辺りの情報をきちっと理解しながら進めていこうと思っている。
- 二点目の、受益者側という点ですが、まず、我々の一番のポイントは、サイバー、フィジカルが高度に融合した社会、Society 5.0 で併用したサプライチェーン、バリュークリエーションプロセスの信頼性を確保しようというのが、まずベースポイント。従って、どうしても旧来のサプライチェーン的なところから捉えていって、それが柔軟になり、動的に構成さ

れる、そこへの対応を示そうとしているので BtoB 的な色彩が非常に強い。

- 一方で、コンセプトの中でも書いてあるとおり、サプライチェーン、いわゆるバリュークリエーションの基点が企業の企画部だけではなく、消費者の人達からのアイデアで回っていく、そういう世界観になるということも述べている。付加価値の創造に参加する人達に求めることが、念頭に置かれているので、どうしても対策ベースは企業とか、組織ということにならざるを得ないが、一般の人達も意識をしてほしいリスク源になっているところもあることは、理解をいただきたいと思う。
- ただし、スマートホームのところは消費者の人達が一緒になって使っていくという BtoC の色彩がかなり入ってくる。かなり特徴的な部分があるので、スマートホームサブワーキンググループの議論が今後、どう展開していき、また取り込んでいくことができるのかということは、よく見ていきたいと思っている。

○松本委員

- 第 2 層に当たるところで、フィジカル空間とサイバー空間の間の対応関係の部分が、重要であると思うので、今回のサイバー・フィジカル・セキュリティ対策フレームワークの中でも、きちっと取り上げていただくべきところかと思う。
- 少し細かい話になるが、添付 B のリスク源と対策要件の対応関係について、添付 B の 6 ページ、7 ページのところ、2.1、2.2 で、「フィジカル空間の物理事象を読み取り、一定のルールに基づいてデジタル情報へ変換し、三層に送る機能」というところで、想定されるセキュリティインシデントが幾つか挙げられているが、センサの段階で、情報を物理的なところから読み取る部分のセキュリティ、これを「計測セキュリティ」と呼んでいますが、それを明示していただいた方がよいかなと思っています。これは既に入っているのでしょうか。

○奥家課長

- L2_3_b_COM ということで耐タンパー性というようなところが対応する。

○松本委員

- センサ等で読み取る段階で何か誤認してしまうとか、間違ってしまうということは、セーフティの分野でも重要。それを意図的に仕組まれると困る。計測セキュリティの部分は非常に重要な概念なので、項目としてあっても良いのではないかと思う。

○奥家課長

- L2_3_a_ORG の対策要件の CPS.DS-16 の中に計測セキュリティの観点が考慮された製品というのは一応対応している。

○松本委員

- 想定されるセキュリティマネジメントというのがその左側にあるのですが、これはセンサで読み取った後でセンサで読み取る過程そのもののことは書かれてないので、あまりそれに引きずられないようにしておいた方が良いと思う。

○奥家課長

- 検討する。

○松尾委員

- 今回のフレームワーク改定案、国際標準との約束事や、想定読者、実装の実体など実際するものが、分かりやすくな

っていて大変良いと思う。

- 国際的にもベストプラクティスがまとめられていると思うが、今後、このフレームワークにベストプラクティスなどが何らかの形で入ってくるのか、それとも業界ごとに作っていくのか、考え方をご教示願いたい。関連して、我々のワーキンググループは、元々制度、技術、標準化なので、制度にどの様に関わるか、考え方をご教示願いたい。

○奥家課長

- 対策事例としてメソッドに並べているものは、一応プラクティスになっている。その他としては、ワーキンググループ 2 の方で、現在プラクティス集を作成している。趣旨は、実際の現場で、同じ業種や同じ企業規模で実施できる観点で、他の企業が何を実施しているかを集めている。元々は、ベストプラクティスと言っていたが、ベストとは何かという議論になって、結局のところ、置かれている環境とかコスト的な制約などを踏まえた上で判断せざるを得ないので、ベストと言うよりもプラクティスをまとめて、使うか使わないか判断できるのが一番良いということになった。その考え方を踏まえて、一般社団法人　日本情報システム・ユーザー協会とか、産業横断サイバーセキュリティ人材育成検討会とか、日本商工会議所とか、そういった人達にも参加していただいて、今年の7月からこの検討を開始している。できれば年度内に、このプラクティス・コレクション・ブックをまとめようと思っている。
- ただし、当然、業界の中では一致したセキュリティ要件があると思うので、サブワーキンググループを、今まで立ち上げてないところも、立ち上げてみて、プロテクション・プロファイルを自分達でまとめてみたらどうか、というようなことも一応ポジションとしては持っていて、提案をしているケースもある。
- 恐らく、業界とか、もしくは、ある目的で、サブワーキンググループを組んでいるベースになってくるところは、制度とのリンケージが明確になってくる。例えば、紹介した電力サブワーキンググループは、まさに、そのガイドラインに反映するということで提言をまとめる形になっている。
- 制度的なところに結び付けられるところは結び付けていくことで、できるだけ具体的に落とし込んでいくと、そこで制度とのリンケージが明確に見えてくる。そこは、それぞれの状況などを踏まえた形で、しっかりと進めていきたいと思う。サブワーキンググループでの検討は、ワーキンググループ 1 の下にぶら下がっていくので、そういった中で方向付けをしていくとか、逆に、提案いただいたものを下にうまく伝えていくことを進めていければと思っている。

○平田委員

- バリュークリエーションプロセスに着目して、従来型も含んだフレームワークになっていて、非常に幅広く適用可能になっている様に思っている。コンセプトとリスク分析と対策を分けて、ブラッシュアップしやすいようにして、非常に良かったと思う。一方で、幅広く適用可能ということがあるので、サイバー空間が広く捉えられる場合があるのではないか。要は、従来型のシステムの情報処理の部分もサイバー空間と捉えてしまい、検討が複雑になるようなケースがあるではないかと思う。
- 今後の展開に当たっては、やはりインターネットの仮想的な空間で、このようにデータがマルチステークホルダーでやり取りされるという、サイバー空間というところや、IoT という、その違いに特化して検討が進められるような形で始めて、その上で、先程お話しいただいた、従来型システムに展開していくというようなストーリーが見えると、より分かりやすいものになると思う。
- 資料 6 の 22 ページの信頼のチェーンのところは、どのようにして負担が少なく確認していくかというところが難しい問題と思っている。特に、この辺は、サプライチェーンが、既にグローバルも含めてやってくる時代なので、そこの信頼関係をどうするのかといったところも非常に重要になってくるので、そういったところの考え方を、多少書いて頂きたい。
- また、図 9 がかなり従来型のサプライチェーンをイメージした図になっているので、もう少しコンセプトベースで書かれると幅が出てくるのではないかと思う。

○奥家課長

- データをどう捉えるかというのは非常に重要で、データが持っている価値は、使われている時によって価値が変わってくる。それを、カテゴライズして管理していくという考え方が、やはり出てこざるを得なくて、そうなった時に、そのあるカテゴリーの中で管理されるべきデータが、組織ごとにセキュリティ要件が違う訳はないので、カテゴライズされたもので要求される要件などを整理していくとか、幾つかのディメンジョンで深掘りしていかなければならないものが出てくるだろうと思っている。
- ここでデータの価値自体を議論するというのはややずれると思う。他で検討されているものに対して、どういうセキュリティ要件を求めるべきなのかというような形で、例えば、今、経済産業政策局で議論している、限定提供データのようなものも視野に入れながら考えていかなければいけないと思っている。
- 信頼性のチェーンについては、まさに工数とのバランスで、更に言うと、国際的な紐付けというようなところになってくるので、例えば、制度的に何かをやるということになったら、相互承認などを視野に入れてつなぎ込んでいくということになる。海外との議論をかなりしているのも、実はそこの部分。まずは検証技術について共同でいろいろできないかとかという話を持ちかけている。検証技術があって、初めて認証に至るようなところがあるので、引き続き、ベースをしっかりと整えていきたい。コンセプチュアルなという形になるのは、少し検討させていただきたい。
- 最初の御指摘については、その通りだと思っている。サイバー空間をより明確に定義してあげれば、スムーズに入るのではないかと思っている。

○渡部委員

- 今回、この第 1 層、第 2 層、第 3 層というところが、だいぶ奇麗に整備されたのかなと思っている。
- このフレームワークは、セキュリティ意識の高くない人達、セキュリティにこれから取り組もうという人達に広めていかなければいけない、そういう概念だと思う。その際に、これをきちんと読み込めるのは、おそらくかなりの大企業かなと感じている。中小企業の方々も、これを読んでいかなければいけない訳で、少なくとも、第Ⅰ部をどういうふうに納得していただくかというところは、非常に大きな課題に思っている。
- 新しい概念も入ってくるので、ここをどう伝えていくか、このフレームワークをどのように普及させていくかという中でだと思うが、分野別のサブワーキンググループがあるところでは、そこでもブレークダウンができるとは思うが、サブワーキンググループがない分野も多数あるので、例えば、プラクティスができた時に、それと関連させながら話をしていくなどもあると思う。
- サプライチェーンの重要な位置を占める中小企業に、いかにこの概念を理解していただくか、そういうところがこれからの課題になると思うので、是非よろしくお願いしたいと思う。

○奥家課長

- 今回のフレームワークは、本日指摘いただいた修正を加えた上でパブリックコメントを実施したいと思っているが、パブリックコメントの期間中には、先程紹介したコラボレーションプラットフォームなども活用しながら、しっかりと紹介していきたい。
- 中小企業にどう伝えるかは、どの政策でも常に大きい課題。経営ガイドラインについても、中小企業のためのガイドラインという形で簡略化した形で伝えて、それを踏まえたセキュリティアクション、自分で自己チェックを掛けましょうということにして、長らく動かなかったのが、ここに来て急激に増えて 56,000 社まできた。動く瞬間に一気に動くというのもあって、どういうアプローチを取っていくかは、今後大きい課題として認識したい。引き続き、アイデアもいただきながら進めていきたいと思う。

○高倉委員

- 先程ご説明で、海外の方で参照すべきものがまだ無いので、これが凄く新しい先を行っているという話だったが、一方で、皆が NIST 見ているということは、CSF に載ってないところやらなくても良いのではないかというコメントが来そうな気がする。その載っていないけども敢えてやるという説明が必要と思う。
- また、海外の方で検討されている事例が載っていないという指摘が来そうな気もする。カリフォルニア州の州法の話が出てきたが、海外の弁護士と話をしたところ、実はさらにダークホースがいて、今、米国議会上院に提出されている IoT のサイバーセキュリティインプルーブメント法案に、かなり厳しいことが書かれている。連邦政府の調達に限定だが、要は独自プロトコル禁止など、凄いガチガチに書いてあり、これが通ると大変なことになるぞと言っている。本日最後に出たホワイトハッカーの活用に関しても、実は、法案を読むと凄い制約を掛けようとしていて、国のガイドラインに従った調査以外は求めないという書き方になっている。見方によれば、ガイドラインに従えば何やってもいいと受け取れ、逆の見方をすると国の方針に従わなかった場合は摘発するぞと書いてあるわけで、海外の動きとしてこういう法案が出ている。今すぐ反映して欲しいということではないが、こういう法案が今審議されてきていて、少し注目を浴びているというのが出てくれば、それは適宜アップデートしていただきたい。

○奥家課長

- 新しいモデルでサイバーとフィジカルが完全に一体化した社会で発生するサプライチェーン、バリュークリエーションプロセスは、やっぱり新しいリスクを抱えざるを得ない。それを捉えにいくモデルを適用しようとすると、やはり新しく今まで見てなかったことはある。これは実は海外の米国や欧州の人達にも結構明確に伝えています。NIST のサイバーセキュリティフレームワーク自体は、インシデントへの対応をベースとしたステップで捉えているので、第 2 層的なところとかはやや苦手にしているなというのは、率直にこう見えていると話をしています。
- いわゆるデータビジネスをやっている人達は、第 3 層のところもがもう少しという意見も米国内にあるので、そこはお互いにそうだよね、というような形で議論はできている。NIST の方もこの前に来てくれたりしていて、よく議論しながら進めていこうと思っている。
- 海外の取り組みは、まさしく気にしないといけなくて、この取り組みを開始した去年の年末ぐらいとか、それ以前からいろいろとお話をさせていただいていた時とか、まさに当時はサプライチェーンというものを捉えましょうということで、まさに NIST が初めてサイバーセキュリティフレームワークの中で項目として捉えた。それを正面から新しい産業におけるバリュークリエーションプロセスと言って取り組んでいるのが実は日本であり、ある意味、斬新な取り組み。それを踏まえて米国や欧州も動いている部分がある。法律が動いてくると、また次元が変わったところで制度を落とし込んで行かないといけない。
- 今、ワーキンググループ 1 の電力分野のサブワーキンググループの中で明確に見えているのは、米国の FERC という規制機関がルールを作っているのですが、その FERC が指示をするのが NERC であり、NERC が実際に出しているガイドライン、これが公にオーソライズされると CIP という形で決まってくるが、この春の終わりから秋にかけて CIP はかなり連続に出てきているのが実態としてある。ここのところは電力サブワーキンググループの方で、私達がどう捉えているかを御紹介させていただきながら、おそらく制度化は避けられないということは随分議論している。米国の法案の場合は、成立率が大体五パーセントに満たないくらいで、議員の皆さんが自由に投げ込めるので、即、法律になるという訳ではないが、法案までできたということは、このような問題意識を持っている人達が複数グループいるということでもあるので、ここはよく見ていかないといけない。
- ものによっては、やはり、NISC とか法務省とか他省庁のところに向けていかなければならないとは思うが、私達のところに比較的情報が入ってくるので、そこは常に反映しながらしっかりと対応していかないといけない。ここは極めて重

要な問題だと思っている。逆に、議員の皆様も見えてきていて、私達が見えていないものがあったら、気をつけろとワーニングをいただけると非常に助かる。

○高倉委員

- 用語について、やはり、我々日本で使っている用語と海外で使っている用語はかなり違ってきている。実際、今月、EU・NATO の会議に出席したが、会議のうちの多分 8 割が、この用語はどういう定義かという議論。用語定義のために人が集まるぐらい。実は標準を決める時は英語で決めていくが、その英語の持つニュアンスが国によって捉え方が違う。更に、日本はそこからまたかなりずれた解釈をしているので、この手の話をするときには、後でいいから、この用語は日本語ではこういう意味だということをかなり厳格に決めてかないと、言葉が独り歩きしていきそうな予感がします。

○奥家課長

- 全く御指摘のとおり。例えば、脆弱性という言葉の使い方については、日本の脆弱性は強さ弱さも含んでいるが、米国ではバルネラビリティーと言うとかなり限定されている。米国と話をしている時に、日本の感覚で言うと誤解をされていたりするケースが多い。
- その他にも、データという言葉も、他者に利用できるような形で使われる情報については、データと表現するとか、かなり注意している。とはいえ、完璧ではない。おそらく、ここでも様々な意見をいただくと思うが、十分注意していきたいと思っている。

○佐々木座長

- 用語集も付いているので、その辺もご検討いただいたらいいかと思う。

○其山委員

- 中小企業の方に対して少し分かりにくいと言うか、読み込みにくい部分もあるのではないかと、正直感じるところがある。サプライチェーンなど企業間の取引を対象としているので、一企業で本フレームワークへ対応しようとすると対応しにくいところがあるのではと感じる部分がある。本フレームワークをどのような運用に乗せればうまく回っていくのかという検討を、是非、実態のある企業で PoC を実施して、フィードバックを取り込んでいただきたい。
- 他の委員からも出ているが、特に付録の部分は、技術や脅威の動向によってブラッシュアップが頻繁に必要なところがあるので、できるだけ明確に、どのタイミングで見直していくのかを示して欲しい。それによって、このフレームワークが信頼を置けるもので、様々な企業が、これを活用していれば安心してセキュリティ対策ができているという認識になると思う。
- 中小企業や、体力の弱い企業だと、セキュリティはまだまだコストという認識が強くあると思うので、各企業が自らこれはやらなきゃいけないということを認識して推進できるまで、社会に対してしっかり本フレームワークをプロモーションしていただく努力をお願いしたい。当然、何らかのインセンティブや、プロモーションのために必要なことがあれば是非、実施をご検討いただきたい。
- このフレームワークが世に出てから、研究開発をしていく際の懸念として、独自開発に伴うガラパゴス化がある。海外に既存技術があるのであれば、それらを確認してから研究開発を押し進めていただきたい。やたらと独自開発というところに向かってガラパゴス化してしまうと、その開発期間が無駄になり、実は海外はもっと進んでいましたという事態になりかねない。そのような事態に陥らないように、気を付けていただければなという点を、意見させていただきたい。
- 今後の方向性というところで、確認をさせていただければと思うが、本フレームワークは、まずはリリースされて、参考として皆さん使ってくださいという位置付けだと思うが、今後、実際にリリースされた後に、強制力を持たせるのかとか、

規制化するなど、どのような位置付けで運用されていくのか、また、電力のガイドラインに反映する話など、サブワーキンググループでこのフレームワークを使ってアウトプットを出されていくと思うが、それをどういった位置付けにしていくのか、もしお考えがあればお聞かせ願いたい。

○奥家課長

- 中小企業の皆さんに使えるようにという点については、まさにこれができた後に解説なりが必要ということだと思う。PoC については、実は、ビルセキュリティガイドラインについては実際、今使ってもらって、フィードバックを掛けた上でβ版を正式版にするという取り組みをしている。皆様においても、こう試してみたら、もしくは会社の今の規定類と突き合わせてみる、というようなことを行っていただいたりしてフィードバック等を頂けると、とても嬉しいと思っている。
- 見直しについては、フレームワークの使い方の箇所などに書き加えておくべきかと思っている。ここは検討させてください。
- プロモーションとインセンティブは、強制力と表裏一体的な要素がある。そういう中で、このフレームワーク自体は、条件がかなり幅広く、全体のリスクへの洗い出しになっているので、包括的に行うことはなかなか苦しいと思っている。一方で、各産業分野や各用途のところでは、添付 B、添付 C の中で、このぐらいのレベルの対応をしないといけないと言って、自分たちでプロテクション・プロファイルを組めるようになってくると、具体的な名称などの形に結び付けやすくなると思うので、サブワーキンググループ、更に言うと各分野の取り組みというのが重要になってくるだろうと思っている。強制力という意味では、電力のところは比較的、制度との結びつきが強いが、それ以外のところも、例えば、ビル分野でも独自の認証のようなものなどを、考えていっても良いはず。必ずしも制度で強制するだけではなくて、自分で自らの状況を確認するという形で進めていくというようなことを、各分野でブレークダウンして、特に、添付 C は選んでくださいというメニュー的な形になっているので、そこをうまく使っていただけると良いなと思っている。
- 海外の技術については、御指摘のとおりで、検証基盤を作るという話をさせていただいている。私達の方では、米国、イスラエル、フランスや、あとイギリスなど、どの国がどの分野が強いかということをベンチマークしている。特に、日本についてはハードウェアトロージャンやブラックボックステストの分野について強みが明確に見えてきている。どの分野に強く、どの分野については海外と協力していった方が良いか取り組んでいて、IoT 時代の検証技術は、あまりにも多様で、シングルカントリーで全部用意するのは効率的ではないし、むしろ、これを機会に相互承認とかを取りにいって、マーケットをきちんと築いていけるようにする方が良いのではと思っている。
- 海外の動向については御指摘のとおり、我々ももっと深堀していきたいと思っている。

○上原委員

- 今付いている用語集は、一般的な定義をそのまま引っ張ってきているが、このフレームワークの中の文脈で使われている用語のニュアンスと、少しずれがあるものが幾つかあるように思う。少し思い切って「このフレームワークの中ではこういう使い方をしている」という用語集にしていかないと、読み方が少し難しいかなという気がする。
- 例えば、肝になる「信頼」、「トラスト」という言葉も、業界によって様々な捉えられ方をする。しかも、こちらはサイバーフィジカルの世界なので、実際にそのフィジカルのビジネスの中で「トラスト」という言葉を使っておられる方と、サイバーで使う「トラスト」は、かなりニュアンスが違っていたりすることによる齟齬が心配。それを埋めることが、読んだ時に語弊が生じないようにするために必要と感じた。
- 中小企業の話が度々出ているが、特に、想定読者という意味では、役職として「こういう人」ということは書いていただいたことは良い。しかし怖いのは、「このような新しいビジネスを始めます」ということを、大企業に言われ、その下に参画する中小企業が本当はきっちり読まなければいけないが、それが徹底できるか不安。その段階で、自分は分業の一部分を担うという立場の人に、例えば、「第 1 層のここしかやっていないから関係ない」、「第 2 層のここしかやって

いないから関係ない」という言われ方をされるとつらい。特に、サイバーフィジカルという言葉は、凄くキャッチーなので、「それは上の人が考える」、「元請けが考える」のように、私が考えることではないみたいな捉え方をされるとつらいので、広報の仕方が難しいと思っている。PoC を使う方法もあると思うが、それよりもやはり具体例を幾つか持ち込むことで、「あなたにも関係ある話ですよ」ということを中小企業の方に分かっていただくための仕掛けが必要と感じた。

○奥家課長

- 用語は、どこまでキャッチアップできるか、というのもあると思っている。一方で、むしろパブリックコメントでもおそらく意見が出てくると思っていて、今回、第 1 次原案から第 2 次原案でここまで分厚くしていますので、パブリックコメントが出てきたらそれに回答する形で検討させていただければと思っている。
- 具体例のところは、今後も引き続き、まさに普及と啓発の中で検討していきたいと思う。

○石原様（斎藤委員代理）

- 気になったのが信頼の部分。資料 6 の 23 ページにあるサプライチェーン全体のフレームワークの中で「信頼」という言葉を使っていることと、セーフティに関する事項を取り込んだことが新しいと思うが、やはり「信頼」という言葉の中に 5 つ定義があるとか、様々な議論がされていて、このフレームワークでどこまでおさえていけるのか。
- 海外でもやはり、セキュリティとセーフティを考えましょうという動きもあれば、Trustworthiness は SC41でも動いており、IoT ベースかもしれませんが、やはりそこを追いかけていくということが、今後必要だろうと思っている。やはり、「トラスト」、「信頼」という言葉の定義が、一番難しい問題かなと思っている。その辺、少し考えていけたらと思う。

○奥家課長

- 信頼については、米国のこの分野のエキスパートも、「セキュリティ」という言葉はあまり使わないように避けていると言っていて、Trustworthiness だと、実は第 1 次原案が一番それに近かったというコメントを貰っている。かなり思い切った領域に足を踏み込んでいるのは事実だと思っている。
- 国際標準も結局、セキュリティ、インフォメーションセキュリティのところと、ファンクショナルセーフティのところで、交錯しているところをどうしていこうかということがおそらく 1 番難しい問題になっている。Trustworthiness とか、昔で言うディペンダビリティとか、リライアビリティ、アベイラビリティがここに含まれるのかなど、かなりテクニカルな議論に落ち込んでしまうのではと思っている。
- 今回について言うと、サイバーとフィジカルが一体になって、バリュークリエーションプロセスときちんと付き合って、そこから出てくるものが、きちんとしたものかどうかを保障するためにどうしようというところで、ややそういった議論から外れた上で取り組んでみた結果、Trustworthiness に限りなく近い中身になっていったのが率直なところだと思う。
- 神学論的なところに踏み込んでいくと、足が抜けなくなるというのが率直な感想。むしろ、やや使えるような形にすると、やはり Trustworthiness という言葉が鍵になってくる。今後、様々な分野で言葉が熟してきて、ある人達はむしろセキュリティとプライバシーの融合を意識しますし、今この資料の中では B to B 的な色彩が強いと申し上げましたけども、セキュリティとファンクショナルセーフティの融合領域を比較的認識している。そういった議論の中で、Trustworthiness についての形式的な捉え方が間違いになってくるのを少し待たなければならないのかもしれない。

○小松崎委員

- 中小企業の議論が前回も出てきたと思うが、それこそ抽象的過ぎるという気がする。大事なことはバリュークリエーションプロセスという概念が大事で、その中に一か所でも信頼ができないものがあると全体の信頼が喪失されてしまうというところが一番の出発点。この価値を失った時に、誰がビジネス側で損するかと言うと、関係する全員である。そして、

本当の被害者は利用者、つまり、それを使う人、買う人となりますから、まず、フレームワークを見る時の視点というのは、買う人、使う人に迷惑が掛からないようにするというのが一番大事な価値である。

- 皆が関連して仕事をしている訳で、その中に 1 人でも不勉強な人がいた結果として全体の信頼性が落ちたら、著しい問題であるというのがこの基本スタンスだと思う。大とか中とか小じゃなくて、全体の Trustworthiness に応えられるレベルかどうかということを客観的に測れるかどうかが大事である。
- 非常に良いものを作るが、この分野は弱いという会社があれば、それをサポートする体制など、新しい価値を作る訳なので、もちろん有償でも良いと思うが、そこに新しいコスト要素が入ることは見込んでおかなくてはいけない。そのコストをどのようにシェアするか、関連する新しい価値を作る仲間同士で分担をどうするかが、今までなかった新しいアクションとして必要になってくる。
- 弱者とかそういう見方で中小企業を見るのは正しくなく、どのようにこれをシェアして全体として新しい価値を作っていくか、新しい仕組みをどうやって考えるかというアプローチをしたいと思っています。

○片山委員

- 用語の話が何回か出ましたが、そもそも「サイバーセキュリティ」という言葉自体も、世界によって意味が違う。来年 6 月の G20 は、日本がホストをしますので、用語、少なくとも「サプライチェーンリスクマネジメント」は、様々な国との整合性が取れる言葉だと思うので、是非、日本がそういうところを進んでサポートしていただきたいと思う。サプライチェーンリスクマネジメントの重要性は、二十か国で合意できることを願います。

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。

- 前回の指摘に対し、サブワーキンググループ並びに事務局が非常に意欲的に検討いただいたということで、しっかり読み込めば、ずいぶん分かるようになったという気がしている。どのくらいの人にしっかり読み込んでいただけるかという問題もあるが、これはパブリックコメント等で色々と対応していくかなと思っております。
- 本日ご議論いただいた、サイバー・フィジカル・セキュリティ対策フレームワーク第 2 原案については、頂いたご意見を踏まえて修正を行い、修正したものを皆さんにも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行うフレームワークの最終的な案については、座長一任ということでお願いいたします。
  （上記発議に対して、全委員一致で異議無し）

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。

- 本日の指摘を反映した第 2 案について、座長とも御相談させていただいた上で、恐らく年始になるが、パブリックコメントを開始したい。前回同様、英語版も公開する。期間は 2 月いっぱいでは、という声もあるので、できればそうしたいと思っている。
- 第 5 回会合については、パブリックコメント終了後の 3 月頃を目処に開催予定。詳細はまた、別途事務局の方からご連絡をさせていただく。

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