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1回) 議事要旨

1. 日時・場所

日時:平成30年2月7日(水) 9時00分～11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)、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:商務情報政策局 寺澤局長、伊東大臣官房審議官、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

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 本ワーキンググループの運営について(案)

資料4 産業サイバーセキュリティ研究会WG1(制度・技術・標準化)の設置について

資料5 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の策定に向けて

参考資料1 「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」策定の視点

4. 議事内容

冒頭、寺澤局長から以下のとおり挨拶。

- サイバーセキュリティは攻撃の起点が増え、手法も高度化しており、どこから攻撃があるのか予測するのが難しい。また、IoTでつながりが広がり、インパクトも大きくなっている
- 上記観点から昨年12月27日に産業サイバーセキュリティ研究会を開催し、産業界を代表する方々とNISCを初めとする関係省庁の幹部の方々に集まっていただき、大臣出席の下で会合を実施した。これだけのメンバーが集まるのは例がなく、サイバーセキュリティに関する産業界・関係省庁の関心の高さの表れといえる。当日の会合では、サイバーセキュリティについてはサプライチェーン全体、社会全体での対応が必要との意見があり、本日のWG1は、これを具体化する大切なワーキンググループである。
- Society5.0の実現に向けてサプライチェーン全体のリスクポイントを分析し、産業活動において必要なセキュリティ対策を示す、サイバー・フィジカル・セキュリティ対策フレームワークを是非検討いただきたい。

次に、佐々木座長から以下のとおり挨拶。

- 産業におけるサイバーセキュリティの重要性は議論を待たない状況。昨今のWannaCry、コインチェックでの被害など、現実の問題となっている。今回のWG1では、制度・技術・標準化という面から具体的な対策を明確にしていきたい。

事務局から、資料3及び資料4による本ワーキンググループの設置についての説明に続き、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）及びサイバー・フィジカル・セキュリティ対策フレームワークの策定に向けて（資料6）について説明した後、以下のとおり自由討議を行った。

○江崎委員

- 総合科学技術・イノベーション会議のお手伝いをしている観点から申し上げると、資料4のp.4の右下に「産総研」しかないことに違和感がある。「国研」としていただいた方が良い。産総研が経済産業省として重要な核となるのは理解するが、産業を跨いでくるので他の国研も関係してくると思う。
- フレームワークについては、産業別にセキュリティに関する認識と複雑度が違うので、共通の部分と掘り下げる部分の二階建てになると思う。
- 資料6のp.2で、Step1が必ずデジタルコピーからスタートする絵になっているが、昨今では、いきなりサイバー空間から入ってくるデジタルパスがある。Step1がフィジカルからしか入らないということではなく、サイバーからいきなり入ってくることがあるので、これも検討に入れておくべき。
- 資料6の三層構造については、Society5.0でも議論しているが、デバイス、ストレージとアプリケーションという構造で検討している。ストレージをどう守るかも重要であるし、産業を跨がってのアプリケーションのアクセスとなるとデータ連携の上のアプリケーションからデータレイヤーとデバイスレイヤーという形になるので、これも入れるべき。
  内閣府では、Society5.0における産業界のデータ連携フレームワークについて議論しているので、ここでの検討を反映いただくと、サイバーセキュリティをデータ連携の要求条件に入れることができると思う。整合性を取って進めてほしい。

○岡村委員

- サプライチェーンは大きな要素となっており様々な攻め方があるが、一つの攻め方として不正競争防止法を拡大するという方法を考えている。その検討の中で、企業の支社・支店、子会社を含めてどうするかという課題が出てきた。また、非正規雇用がまだまだ多い中、派遣法の改正などとの関係で、善し悪しは別として、再委託という形でオンプレミスでの作業が増えており、実際のサプライチェーンのあり方を考えていくことが必要。
- 支店と支社の関係では、欧州、アジア諸国との関係でブロック化の動きが出てきている。その中で、しっかりと我々のデータを保護するという観点と共に、外国で日本企業がいらぬ疑いをかけられて法的責任を追及されないようにすることも検討しないといけない。
- 個人データ保護に関して欧州とは相互認証という方向で進められているが、他方、アジア諸国の場合には、国が定める重要データについて輸出制限と共にかなり重い責任を課せられている。JEITA が調査を進めているようだが、グループ企業が日本から調達先としてこれらの国に多く進出しているが、残念ながら法的な脆弱性が見られるので、いつブロック化にかかり、セキュリティという名の下での各国法の責任追及の対象にあってもおかしくない。我が国のデータを守るという視点と共に、変な形での責任追及を受けないような視点がサプライチェーンを考える上では必要。
- 国内の問題に戻ると、むしろ教育の問題になると思うが、IPA が進めている資格制度について、例えば、「こういう企業・支店には、こういった資格の人が何名居ることが相応しい」というような、役割分担の明確化が必要。大企業でもITへの理解が役員レベルでは必ずしも進んでいるとは言えないし、中小企業の経営層には「よきにはからえ」的な考えが良くも悪くも多い。この様なモデルケースを、義務ではなく、指し示すことが大切になる。
- JPCERT の理事として報告を受けていると、制御系のセキュリティが弱い。制御系では保守という考え方から脱し切れていない部分が未だに残っている。IoT のようにコネクティッドになった場合にどう変わるのかという、発想を改めていく必要があるとともに、端末についてもセキュリティ・バイ・デザインという考え方から ISO/JIS の規格化を進めていかない

と、外国で製品を売りにくくなるし、取り残された形で非セキュアな製品がいつまでも出てくることとなりよろしくない。

- ユーザ側では、自ら使用する機器のメンテナンスが前提で、そうすることで、初めてそうしたものがまともに動くと思うべき。車を例に取れば、リスクで言うところの CIA＋S、つまりセーフティという発想でいくと、安全性が強く求められる IoT 機器の重要製品について車検制度のような制度を導入することは、制度的には考え得る対応と思う。

○高倉委員

- 資料 6 の p.19 にある信頼の創出に関して、これは文科省側の人間の発言として聞いていただきたいが、今年度から科学研究費として「情報社会におけるトラスト」の研究が始まっている。その中で法律問題やサイバーの話、医療においてのトラストをどうしていくか、多岐にわたって議論している。これからの研究なので、すぐにこの議論に反映できるかどうかはわからないが参考にしてもらいたい。
- 資料6の p.23 の図は、10 年前、2007 年だったと思うが、航空産業で片が付いている。米国の政策として航空産業で行っているトラストの取組の他分野への展開として、医療、自動車その他諸々へ展開している。この動きをこの WG でどのように考えていくか。喧嘩しても勝てないので、どのように補い合っていくのか、日本でこれは絶対要るなど盛り込むものを詰めていかないと、10 年以上のビハインドがあるので、負けてしまう点を危惧している。

○小松崎委員

- 我々は、リスクマネージメントやフィジカルセキュリティに長年取り組んできているが、簡単に言うとオペレーションが日々継続することが最も重要で、それを危うくする要素は何か、守るものは何かということを明確にすることがリスクマネージメントの効果的なアプローチ。オペレーションに重点を置くことで、フィジカルセキュリティとサイバーセキュリティそしてリスクマネージメントの結節点が明確になってくるという印象を受ける。諸外国でもオペレーション側からサイバーセキュリティを見るという点はまだ弱い。
- 会社の支社、子会社をどうするかという問題は必ず出てくるが、オペレーションから見ると、法人の組織の枠ではなく、実務としての他との連携が見えてくる。結果として、サプライチェーンを意識して「自社の拠点をどうしなければいけないか」という視点と他との連携を意識した課題設定につながるのではないか。オペレーションに重点を置くというアプローチは、非常に実効性があり有効と思う。

○江崎委員

- 具体的な内容について、資料 6 の p.9 にある「セキュリティ対策に必要なコストとの関係を把握する」は、非常に抽象的だが、これをどうオペレーションに落とし込むかがポイントだと思う。一つ、日本の企業で CIO と CISO が同じというのは、経営サイドと監査サイドが同じということ。そう理解すると auditing function をどのようにきちんとガバナンスの中に位置付けるかということになるだろう。
- 米国政府が上手くいっているのは、財務省の下に GAO がいて、NIST と GSA と、横側に DHS が見ているという構造になっていて、まさに財務とオペレーションからの監査ファンクションをどうするかという話になっている。そうゆうところが必要になってくるだろう。
- 企業の方と話をすると、「一体いくらお金をかければよいのだろう」という話になってきている。リスク管理が財務諸表の中に入ってくると非常にやりやすいということで、リスクアセスメントをどうやって会社や組織の財務諸表の中に入れていくかが重要になるので、この点を考えていくと良いだろう。
- また、議論がベンダサイド、供給側へいきがちだが、世の中を決めるのは買う方なので、買う側の意識をどう変えるかが重要。米国のシステムが上手くいっているのは、買う側が調達仕様の管理をしていて、そこにサプライチェーンマネージメントのチェックシーケンスを入れているから。ベンダーは、仕方なく対応しているのが実情。ステークホルダーと

して、買う側の調達のガバナンスをどうするかは重要になるだろう。

- グローバルハーモナイゼーションについて、Society5.0 の会議でもコンセンサスを得たのは、G7 や G20 の場を使って、どうやってグローバルハーモナイゼーションしていくか具体的に戦略を作成する必要があることと、そこへの人的・金銭的な投入をしないと、日本としての活動ができなくなり、グローバルハーモナイゼーションができなくなること。今は、欧州と北米が仲良くしている中でのアジアの拠点としてどう考えるか、アジアエリアでの状況を資料5の最後に入れていただいたが、そういったコンテキストで G7 や G20、その他グローバルハーモナイゼーションに政府としてしっかり投資していくことが大事だと思う。

○岡村委員

- 今の江崎先生のおっしゃっていたことに基本的に賛成であり、もう一度、昔のセキュリティに関する、情報資産価値×脆弱性×脅威の大きさという公式が示す「情報資産の価値」へ戻る必要があるのではと考えている。何でもかんでも「個人情報を守るべき」という形で、一部で極端化の傾向もある。それはそれで大切であることは事実だが、営業秘密のようなもので何千億の裁判沙汰になっている事例もあり、もう一度、資産価値を考えるべきと感じている。
- ISMS 認証規格は、中小企業にとって重過ぎる。扱っている情報や規模などで内部統制を使わなくても直接目の届く中小企業は多いので、次第にセキュリティ水準をステップアップしていくという考え方で、規格を細分化してステップアップしていける仕組みをお願いできればと思っている。

○片山委員

- これからのテーマにもう一つあるとしたら、サイバー攻撃は、国家組織が発端になったと思われるケースが増えてきているので、重要インフラに対する攻撃にどう対処するか、体制をどう考えていくかも一つの側面なのかなと思う。
- フレームワークをグローバルにどう議論していくか。エコシステムという言葉1つ取っても、米国と日本ではその意味が異なる。NIST のサイバーセキュリティフレームワークとなると、凝縮して言えばリスクをどうマネージメントしていくか、サプライチェーンをどのように守るとかということだが、欧米と今後どういう議論をしていくのかも WG のテーマだと思う。

○太田委員

- 欧米サイドはウオッチできているが、ASEAN や中国に関して、まだまだ勉強不足なので、研究会で情報集約し、課題認識を共有すべきではないかと思う。
- 資料 6 の p.3 の図で、3 レイヤーで縦のつながりがあり、左は自動車、右は電力があるが、産業界においては実際には様々なサプライチェーンのユニットが出てくる。ユニットは、業種という観点で括られるものだけではなく、産業と産業がクロスしたもののサプライチェーンなど、要するに N 対 N 型となる。
- データ保護の考え方は、データが一番集まってくるところをカバーすることも大事だが、データを交換するところに脅威を感じる。データ利活用のためのデータのチェーンをいかに安心・安全に作っていくかという論点は、どのレイヤーに入るかわからないが検討していく必要があると思う。

○松本委員

- 資料 6 の p.11 の三階層の図で、時間軸方向に変化していく部分を描くのは難しいが、その視点も重要と思う。特に、IoT 産業フィジカルシステムでは、常に動作しているのが当たり前の姿なので、進度の異なるものが混ざっていることをどう扱うかが非常に難しい課題。
- フィジカル空間とサイバー空間の間のところで、計測のセキュリティの話で、計測したデータの改ざんを脅威としているが、計測の過程自体を揺らがす力が加わることも脅威として重要。サイバー空間からフィジカル空間へ行くときに、末

梢神経・脊髄反射のような早い回転と、大脳まで到達する回転のように回転のスピードが異なるところもある。図に表すのは難しいが気になった。

○小松崎委員

- リスクマネージメントとバリューチェーンで考えると、今回、サプライチェーンを前面に出してきたことは非常に良い。アセット中心で考えると、アセットがやられた際に被害がどの程度発生するかは、比較的見ることができる。ところがバリューチェーン、サプライチェーンで見ると、インシデント発生時に総体としてどの程度の損失が発生するかを見るのは難しい。しかし、実態を知るためには、それを見なければならない。いままで見ることができなかったものを正確に見ることができるようになれば、どこが一番クリティカルなのか、小さな部分に見えても全体としてクリティカルであれば、全体を守るための大きな価値が認識でき、これまでと違ったアプローチができる。
- もう一点、経営者層のこの課題への理解や共感を考えると、プラスの効果のためではなく必要な守りを固めるための費用なので、「コスト」という概念ではなく例えば「引当金」のような概念の方が実態に近いのではないか。将来のリスクに対して継続的に費用をかけて行くという価値観が自然になれば、サプライチェーン、バリューチェーン、リスクの顕在化がすべてつながって経済界が理解しやくすなる感じがする。

○渡部委員

- ビルのシステムを担当してきた。買う側のセキュリティに対する意識は向上してきたが、実際は何をやってよいかわからない部分が大半。特に、サプライチェーンという話を始めると、セキュリティ対策をとらなければならない中小企業が増えてくる。中小企業の方が理解できるフレームワークの共通項が出てくると非常に有意義なものになると思う。
- 産業系のサイバーセキュリティの話になると、システム自体のセキュリティをどうやって高めるかもあるが、実はオペレーション、運用が重要になってくる。システムの強さと運用の正確さのバランスでセキュリティが決まってくる。オペレーションに手間をかけたくなければシステムに投資するなど、費用の感覚も変わってくる。様々な状況の企業がいるので、そこが選択できるような形になると皆さんが使いやすいフレームワークになるのではと思う。

○松尾委員

- 産業界が活用できるセキュリティ対策フレームワークをつくること自体は大変良いことで、そのフレームワークをユーザの皆さん含めて周知していただきたいと思う。
- 一点、資料 6 の p.12 に各分野のライフサイクルで考える必要があるということで、設計、納入とあるが、その後の運用、廃棄も含めたライフサイクルを是非とも考えて欲しいと思う。

○平田委員

- コネクテッドインダストリを繋げる立場として、サイバーセキュリティ対策はエンドエンド全体で考えて対策を打つ必要があると考えている。特に、今まで繋がることを想定していなかった機器が今後接続されていくことを踏まえると、サプライチェーンを含めて繋がる先のリスクの低減を図っていく検討が必要。
- 資料 6 の p.9 にある、フレームワークに必要な要件として、中小企業を含めた事業者が実際に対策を行えるようリスクと対策コストのバランスを取り、競争力を損なわないような配慮は重要と考えている。また、グローバルハーモナイゼーションについては、様々な標準がある中でどのような考え方で整理していくかが重要。

○坂委員

- 資料 6 の p.3 にある三層構造の図は、今後の整理がしやすくなると思っている。今後の WG1 の体制の中で、SWG と

の関係で、全体で議論するところと、インダストリ・バイ・インダストリで議論するところの 2 レイヤーが必要というご意見もあったが、こういうところを含めると、サイバー・トゥ・サイバーのレイヤーは、よりインダストリを跨いでいるところが多い。フィジカル・トゥ・フィジカルのレイヤーも当然インダストリを跨いでいるところもあるが、度合いが若干違うのではと思っている。

- WG1 全体で議論するところ、SWG で議論するところ、自動運転にフォーカスするのか、自動車全般かを含めて、今後整理をさせていただきながら進めていきたいと思う。

○野村委員

- 当社だけでも制御系システムが 700 システム程あり、2 年かけてリスクアセスメントを実施したが、設備寿命が長く、昭和時代の設備から最新の設備まで連携して動いており、一律の対応は難しい。今後、長いライフサイクルの中で、運用保守の視点で、きちんとセキュリティを確保していくのが重要と思う。
- スマートメータの活用や、電力取引の市場が活発・活性化するなど、電力業界においても、設備形成のサプライチェーンだけでなく、資料6にあるような、フィジカルとサイバーの融合、複雑につながるサプライチェーンが存在する。
- 機器を工場で作りこむだけでなく、工事会社がプラントや送変電設備を現場にて形成することも多いなかで、工事会社をサプライチェーンの対象にどう入れていくか、また、制御仕様が外部へ流出するのは非常にリスクなので、その点を含めて議論を進めていきたい。

○江崎委員

- 電力業界からすると OCCTO（電力広域的運営推進機関）のお手伝いもしているが、内閣府からは、SOC をきちんと初めから作れと言われている。産業界を跨いだデータの流通をする拠点となる可能性が高いので、新しい組織をつくるときに、セキュリティ・バイ・デザインでやりなさいということで、SOC を導入した。また、セキュリティアセスメントもやっている。これを一つの事例として取り上げても良いと思う。
- 大事なことは、産業界の産業別データ連携プラットフォームが作られた場合のリスクとして、産業分野を跨いだときの仕様が甘くなるとか、逆に産業分野に縛られてやりにくくなることが起こるので、それとは関係ない、自由なところもしっかりと考えていくこと。産業別のプラットフォームも重要だが、跨いだときにそこに縛られずに、かつ安全なフレームワークを共通の部分で一つ持っておくのは非常に重要と思う。

○高倉委員

- サプライチェーンで真っ先に思いつくのは食肉のサプライチェーン、トレーサビリティで、検討しようとしているフレームワークは、これを大きくしたものという印象。牛とか豚の場合は物理的なモノが動くだけだが、サイバーの場合はそれがデータだったりプログラムだったりするのと、原材料をどこまで追うかで階層が深くなる。岡村委員、太田委員がおっしゃったように、どこまでで妥協するのか、納得するのかの線を決める必要がある。
- 日本はセキュリティクリアランスを導入できない制約がある中で、諸外国の持っているセキュリティクリアランスをもって、「人が認証されるので大丈夫です」と言うのは詭弁だと思う。人に対する認証基盤を持つ海外に対して、日本はどのように対抗していくのかを考えておかないと、「枠組みはできました、人については対応していません」では海外では通用しない。そこへの対応策を考えておく必要がある。

○其山委員

- 資料6の中でグローバルハーモナイゼーションが謳われているが、日本製品を海外に輸出する、良いものを海外から輸入するという観点からも継続して上手く検討すべき。

- サプライチェーンを認証するという案が出ていたが、セキュリティサービスを提供する中で、セキュリティ人材の不足を強く感じている。認証にあたっても人が認証をしているので、フレームワークを考える中で人をコアにした方策を考えなければ空論になってしまうと懸念している。
- 米国のSP800-171の話もあったが、もう一歩進んで検討していただきたいのは、公的機関による監査チェック体制などである。民間企業では出来ない、中小企業などでは体力的にセキュリティ対策をしきれないという部分があると思う。ソースコードに変なモノが入っていないかなど確認しきれない部分を、公的機関により手助けするなどのチェック体制があって良いと思う。
- フレームワークを運用するために、政府からのインセンティブがあって良いのではないかと思う。欧州では、セキュリティ人材を雇用した企業に減税するとか政府の監査を減らすなどの対策が採られている。製造業にはインパクトがあると思う。他方、何か守っていない場合にペナルティを与えるという話も出てくると思われる。その際に、誰がどこの責任を持つかという責任範囲の明確化を進めてほしい。最終ベンダーが全ての責任を持つことになると怖くて調達できなくなり、そのしわ寄せが下側に向かうことになりかねない。
- また、フレームワークを考える中で、技術的な要素が出てくると思うが、技術は陳腐化するので、技術ありきで議論を進めない方が良いと思う。

○斎藤委員
- 先ほど政府調達では調達する側が憂慮するという話があったが、調達する側、調達される側の期待値が合わないとサプライチェーンは成り立たない。政府に期待するのは、国を跨いだ場合どう対応すべきか、欧州、米国も経済圏を組んでいて、これに対して日本単独では対応できないので、どのようなフォーメーションで対抗するのか議論したい。
- もう1点、信頼のメカニズムの構築が焦点になると思う。サプライチェーンの難しいところは、信頼できないからサプライチェーンを切れるのか、というとそうはならない。事業継続、サプライチェーンをつなげるのが主目的であり、切れないことが問題。信頼のレベルも01ではなく、0なら切る、1なら大丈夫という話ではない。
- セキュリティの特徴上、一番弱いところから攻撃されるからといって、一番弱いところを切るとサプライチェーンは成り立たなくなる。信頼のレベルを考慮して進めないとオペレーションレベルの運用ができないと思われるので、この辺りも皆さんと議論していきたい。

ここまでの自由討議に関して、事務局から、以下のとおり回答。

- 高倉委員からも御指摘があったが、航空機の分野は相当進んでいて、防衛が裏で引っ付いて動いていて、相当高い要求が出されている。他の委員の方からも話が出ていたが、国際標準の中でどれを重視するのか、という点とリンクしていると思う。ファンクショナルセーフティみたいなところを中心に押してきた中で、サイバーセキュリティというのはインフォメーションセキュリティとも違うし、ファンクショナルセーフティも満たさないといけないということで、国際標準の世界もきちんとカバーできなくなってきており、守備範囲はどうなっているか混乱しているというのが実態に近い。その中で、米国とは頻繁に意見交換している。米国のサイバーセキュリティフレームワークはその中で一番フィットしているが、マネージメントに寄っていて、オペレーションに落とし込めていないことに苦労しているのが実態。金融業界は、自分たちでプロファイルを作って落とし込んでいる状況。オペレーションにリーチしたいという我々の思いには、関心を持たれており、良い議論ができるだろうと思っている。一方で、これはオペレーションの落とすための手前のところの話で、信頼レベルをどう確保していくのかは個別に検討していくことになるので、各業界で二層構造にならざるを得ないということをご理解いただきたい。現在のフレームワークは、「帯に短し襷に長し」の部分があり、どのようにフィットさせるかをこのWGとSWGでうまくつなぎこんでいきたい。

- 米国のマネージメントサイドは、オペレーションに落とし込むのに相当苦労している。欧州は、データ保護の細かいところに落とし込んでおり、皆が悩みを抱え込んでいるところなので、議論が成り立つと思っている。ここでの議論にちゃんとフィードバックをかけながら検討していきたい。
- フレームワークの中で、トレーサビリティはとても大きな問題で、ソフトウェアを意識している。Software Transparencyという概念を持ち出しつつある動きもあるが、どこまで追いかけることができるか各国も悩んでいる。こういったところについても整理しつつ、最後は個別の具体のニーズ、信頼性の要求度合いが相当大事で、具体論をSWGと連携しつつ、進めていきたい。
- リスクマネージメントとの連動は極めて重要で、フレームワークが使えるか使えないかは、そこにかかってくる。一般的にアセットでリスクポイントが100個あるとしたら、予算との関係で90個に対応したら良いだろうという考え方に近いところを、サプライチェーンで捉えていくとリスクポイントが全部マッピングできる。撃ち抜かれる残存リスクポイント10個のうち、3個が縦列で並んでいると簡単に撃ち抜かれてしまうが、分散していると、どこかでブロックがかかるという発想で捉えることができるのがサプライチェーンで捕らえるところの最大のポイント。スレッドインテリジェンスを使った形でのリスクシナリオベースだと、さらにその中でどう攻撃が来るかを洗い出し、一番効率的な方法で対応する。80個の対応でも守れますというところへ議論を寄せていきたい人たちは相当いる。そういった形で取り込んでいく中で、リスクマネージメント経営に向けていく。コストなのか、発生したときの打撃の影響なのかをうまく嵌めていくことで、インセンティブとの絡みの部分へ使えるようなものにしていきたい。この点については議論を継続していきたい。
- パーソナルセキュリティは、ご指摘のとおりなかなか難しいポイント。技術的には、例えば、画像を解析して行為自体が標準行動とずれているかを確認するツールは、研究がなされており、そこをカバーする方法も考えていくべき。全ての問いに対して、解答の仕方はオプションがいくつかあって然るべきと思っており、それは、まさに研究開発活動、他の国研も参加していただいて、技術的なオプションをきちんと用意していただいた上で議論していければ、実際のオペレーションで効果につなげていけるものになると思っている。
- 国際戦略のところは別途、議論を行っていきたい。

引き続き、自由討議を実施。

○高倉委員
- 2017年1月に米国の電力ISACと金融ISACを訪問したが、電力ISACのオペレーションルームでは、周波数変動と磁気嵐と太陽風の予想画面がメインディスプレイに常時表示され、サイバー系は必要時に切り替わるのみだった。彼らは安定供給に注力しており、異常時に原因を調べて、サイバーが原因ならばサイバー対策チームに割り振るというのがISACの仕事と言っていた。その後、金融系を訪ねたら、政府からの10,000件/日もの情報をさばくために、5,000人のアナリストで処理をしていてコストがペイしないと言っていた。
- 米国も苦労している。うまくすればまだ日本も追いついていけるし、日本からもっと良いものを提案できると思う。

○小松崎委員
- サプライチェーンとかバリューチェーンとか言うと会社をイメージしてしまう方が多いと思う。ビル事業者が使う側と言っていたが、本当のユーザはビルに来る人である。本当のお客さんはみんな共通して「家」に住んでいるので、「家」というものがサプライチェーンで一番大事なもののひとつ、ということでJEITAに声をかけていただいたのだと思う。
- サプライチェーンの一番重要な対象である家庭が仮にスマートホームになったとするならば、全体の系として非常に優れたシステムやサービスを、我が国は先行して実現できるのではないか。従来のように、家電をIT化するとかIoT家電をどうするかという話ではなく、そのお互いの連携であるとか「家」から出て行くもの、「家」に入ってくるものとの連携を意

識してスマートホームを考え、具体的なことに結び付けていきたいというのがJEITAの立場。

- 様々なモノがつながっていく中で、「インターフェースが一番脆弱である」と思いがちだが、そう言っていると自らの課題になりにくい。両側から接続点の信頼性を高めるためにやるべきことが何かを明確化して、 サプライチェーン全体として価値を生み出す具体的な方策を検討したい。その意味でも、家庭をどうするかが非常に重要な課題の一つと思う。

○北川委員

- 昨年度からSP800-171に取り組んでいる。米国企業のベンダーとして契約準備を進めているが、現在の各種取り組みと比べて、非常に厳しい要件があり、対応するための勉強から始める必要があり、非常に大きな金額の先行投資が必要となっている。
- NISTの中で最も重視しなければならないのは、サプライチェーンとして捉えたときにこれをどのように実現していくかということ。サプライチェーンの中には数百社のベンダーがある中、10人、20人という零細企業も存在する。そういう企業に対してまでNISTに対応した新しい情報システムを作り上げろという要求を出す必要がある。
- 防衛産業セクターとしてどうあるべきかを考える上で、一方で社会問題として防衛産業構造をいかに意識していくかが必要。企業経営の観点から見たときにコストバランスが取れた、現に経営可能な合理的な仕組みについて相談させていただきたい。

○江口専門委員

- サプライチェーンの中でいかに信頼を作りながら、信頼を得て業務をしていくか、信頼をどうやって勝ち取っていくか、という仕組みが重要。
- 中小企業を含めて対応が必要だが難しい。他方、中小企業だから対応しなくて良い、ということにはならないので、きちんとソリューションを示した上で、こうすればきちんとセキュリティが確保できるという全体としての仕組みが必要。コストという問題では、信頼の確保を自分で全部行うのでなく、第三者、例えば、公的認証の利用などが効率的な場合もあるのではないか。調達が求めるレベルによって異なると思うし、SWGの場になるかもしれないが考えていくことが必要。

○江崎委員

- 斎藤委員からのアジアでの調達の話に関連するが、世界銀行とアジア開発銀行が調達基準を価格重視からサスティナビリティを継続するための評価軸を強くするようだ。安物を買ってしまって困っている国がODAの国であるので、品質を評価基準に入れていくように意思決定したと聞いている。
- サイバーセキュリティがサスティナビリティに対しても重要であるということが大きな枠組みの中に入れられると、産業の出口として道も見えてくる。

○高倉委員

- この枠組みの最後にエンドユーザーが含まれてくる話になると、欧州で動いている、ITリテラシーに対する一貫した教育カリキュラムの見直しの話にも注目すべきである。我が国と違うのは、新しいものをカリキュラムに入れるために何を削るかを議論していること。次の世代の人に教養として何を教えていくかをしっかり考えていく必要があるので、これを文科省に対して仕掛けてほしい。

○田中専門委員

- 今回のIoTと、トラディショナルなサイバーセキュリティとでは何が違うのかというと、フィジカル(物理)、すなわち、サイバー攻撃によって物理的影響が出てくることが特徴。

・ 一度ばらまいてしまったものを回収するのは難しいのでライフサイクルをうまくマネージするのが大事。サプライチェーンという話になるとハードウェア・ソフトウェアが「正しく動く、安全に動く」ということが確認できないといけないが、○×ではなくどういうレベルなのかという基準を定めてその基準を満たしていることを確認できるなんらかの「メトリックス」を考える必要がある。
・ 認証してOKとなっても、それで十分ではなくて、攻撃の技術も上がっていくので、その後も Up to dateにシステムが安全ということを確認するサイクルをいかに回していくかが大事。各組織が連携して強いところを束ねていけると良い。

○坂下専門委員
・ 過去に準天頂衛星が止まるとどうなるかのリスク分析をしたことがあるが、時刻の同期が止まり、電力や通信系のインフラが止まる。その中で、どのようなリスクがどれぐらい出るかから逆算して、どういう対策を打つかを検討するのも一つの考え方と思う。中小企業においても定量的な数値を示すのが大事。
・ G20が来年日本で行われるので、ここで議論した成果を「日本としてはこうする」と主張すべき。EUの会議で言われるのは執行力。それだけ言うなら「やれ」と言われる。そういうものをどうやって担保していくかも議論していく必要がある。

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。
・ 大体、網羅いただいたと思っているが、一点、「時間」という問題があると思う。特に、IoT等については、一旦設置されると長く変わらない。サイバーセキュリティを最初から導入していくのが難しい。対策されてないモノにどう対応していくか考えていく必要がある。
・ 全体としてサプライチェーンを見ていくと、弱い箇所が見えてくるのはよい。しかし、それを放って置くといけないので中小企業などの弱いところの対策を全体として仕組みとしてサポートできないか。総務省で地方自治体向けのセキュリティ対策を検討していたが、サイバーセキュリティクラウドを作る取組をしている。非常に小さいところに対しても最低限の対策ができる。このような仕組みで信頼の確保ができるとよいと思う。
・ 業種ごとに検討していくことも必要。業種を貫いた検討も必要。SWGを立ち上げての検討が良いか、全体としてWGで検討するかなど、進め方は考えていきたい。

最後に事務局から、第2回会合を年度内に開催する予定であり、スケジュールについて別途連絡する旨、委員に案内した上で第1回会合は閉会した。

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