サイバーセキュリティ戦略本部　重要インフラ専門調査会
第７回会合　議事概要（素案）

１　日時

平成 28 年 6 月 15 日（水）16 時～18 時

２　場所

中央合同庁舎第４号館１１階　共用第１特別会議室

３　出席者（敬称略）

有村　浩一　委員　（一般社団法人ＪＰＣＥＲＴコーディネーションセンター）
伊澤　雅和　委員　（一般社団法人日本ケーブルテレビ連盟）
石川　広己　委員　（公益社団法人日本医師会）
稲垣　隆一　委員　（稲垣隆一法律事務所）
大高　利夫　委員　（神奈川県藤沢市）
大林　厚臣　委員　（慶應義塾大学　大学院経営管理研究科）
大平　充洋　委員　（一般社団法人日本クレジット協会）
荻島　　敦　委員　（日本通運株式会社）
門野　健治　委員　（株式会社みずほフィナンシャルグループ）
金子　　功　委員　（一般社団法人日本ガス協会）
真田　博規　委員　（住友生命保険相互会社）
神保　　謙　委員　（慶應義塾大学　総合政策学部）
鈴木　栄一　委員　（一般社団法人日本損害保険協会）
高橋　泰宏　委員　（石油連盟）
竹原　　達　委員　（電気事業連合会）
手塚　　悟　委員　（慶應義塾大学　大学院政策・メディア研究科）
西村　敏信　委員　（公益財団法人金融情報システムセンター）
西村　佳久　委員　（東日本旅客鉄道株式会社）
橋本　伊知郎委員　（野村ホールディングス株式会社）
平田　真一　委員　（日本電信電話株式会社）
細川　　猛　委員　（石油化学工業協会）
増子　明洋　委員　（日本放送協会）
松田　栄之　委員　（ＮＴＴデータ先端技術株式会社）
若林　武夫　委員　（公益社団法人日本水道協会）
和田　昭弘　委員　（全日本空輸株式会社）
渡辺　研司　会長　（名古屋工業大学　大学院工学研究科）

（事務局）

高見澤將林　内閣サイバーセキュリティセンター長
永井　智哉　内閣審議官
谷脇　康彦　内閣審議官
三角　育生　内閣参事官
栁島　智　　内閣参事官
柳原　拓治　内閣参事官

（オブザーバー）

金融庁総務企画局政策課
総務省情報流通行政局情報セキュリティ対策室
総務省地域力創造グループ地域情報政策室
厚生労働省医政局研究開発振興課医療技術情報推進室
経済産業省商務情報政策局情報セキュリティ政策室
国土交通省総合政策局情報政策課
防衛省運用企画局情報通信・研究課サイバー対処・情報保証企画室
内閣府防災・災害緊急事態対処
外務省大臣官房情報通信課
警察庁
文部科学省
原子力規制庁

4　議事概要

(1) 開会（挨拶）

高見澤センター長から挨拶。

○（高見澤センター長）NISCの前身である内閣官房情報セキュリティ対策推進室の初代情報セキュリティ補佐官として、国の情報セキュリティ向上に尽力された、奈良先端科学技術大学大学院教授の山口英先生の訃報があった。最初に謹んで御冥福をお祈りしたい。

一昨日、サイバーセキュリティ戦略本部が開催され、サイバーセキュリティ政策に係る年次報告が決定されたところ。この中で、第３次行動計画に基づく、重要インフラを守るためのこれまでの取り組みがいろいろ期待されており、今後これに基づいて、見直しをしっかりできるようにしたい。特にサイバーセキュリティ戦略本部の会合の中では、PDCAのサイクルがしっかり回っていくことが非常に大事だという御指摘があった。

今回、JTBの案件が明らかになったが、責任あるプレイヤーとしてやっている企業なりがそういったことになるというのは、非常に残念なこと。我々自身、改めて原点に帰って、やるべきことをやるということを徹底しなければいけないのかということを思っている。

伊勢志摩サミット、関係閣僚会合は、まだ２つ残っているが、各重要インフラ事業者、関係機関、適切に対策を実施されて、滞りなく進められたと認識。これからのオリンピック・パラリンピックは全体の規模が違うので、さらに徹底して、対応していかなければいけない。

最後に、今回のサミットの成果文書として、サイバーに関するＧ７の原則と行動というものが合意をされた。サイバー空間の安全と安定の促進のためのＧ７のワーキンググループを立ち上げることになっており、我が国自身もこれにしっかり取り組んでいかなければいけない。国際連携を政府全体として、あるいは重要インフラの企業の皆様も含めて、しっかりとした核になる体制を構築しなければならないので、皆様の御協力をいただきたい。

渡辺会長から挨拶。

○（渡辺会長）前回、第６回の専門調査会は、持ち回りのため、今回は第７回。

前々回の本年３月の専門調査会で、行動計画の見直しに向けたロードマップに御議論・御承認をいただいたところ。

本年度は第３次行動計画の最終年度に当たることから、第３次行動計画そのものの評価を行う必要がある。それから、次期行動計画について、ロードマップに従って、どのような改定作業を行うかを議論していく必要がある。

センター長の挨拶にもあったが、重要インフラ分野に対するサイバー攻撃のリスクは、さらに高まっており、実際の事案も、現れ始めた。

一方、IoT、あるいはAIなどの発展もあり、重要インフラを取り巻く状況は、常に変化しており、そのスピードもますます上がってきている。一方、重要インフラ事業者のシステム更新が絶えずあり、コストダウン等の必要性から、必ずしも業績維持が容易でない中、システム更新に関しても、必ずしも更新前と同等の環境を維持できず、そこが脆弱性になる可能性もあるというような状況も進展している。本日は、このような状況も踏まえ、ぜひ次期行動計画に向けての積極的な御議論をいただきたい。

山口先生に関しましては、私もこの会議体の前の会議体の初期のころに、大分熱い御意見をいただいた。彼が言い残したことは何だろうかということを咀嚼しながら、今後の活動に生かしたい。

(2) 報告事項

【Ｇ７伊勢志摩サミットにおける取組等について】

事務局から資料２－１に沿って説明。

警察庁から資料２－２に沿って説明。

【2020年東京オリンピック・パラリンピック競技大会に向けた取組について】

事務局から資料３に沿って説明。質疑応答は次のとおり。

○（増子委員）２点、お伺いしたい。１つは、伊勢志摩の報告について、皆様に体制を組んでいただき、特に目立った攻撃もなく終わりました。サミットが終わってしばらくしてから、セキュリティベンダーから、伊勢志摩のサイバー攻撃に関しては、全体的に防げましたという話をしていたときに、これは成功したのではない、こなかっただけであって、成功でも、失敗でもないということを複数耳にした。

サイバー攻撃というのは、量と質と両方の面があり、量的にはかえって少なかったというのが実感。そういったことも含めて、政府のほうではどう考えているのかが、１つ。

もう一つは、オリパラのところ。オリンピックのCSIRTを作るということが書かれているが、それと重要インフラの私どもとの関わりみたいなものを、どのように考えているのか。

ベースとして、ロンドンオリンピックでは、業界ごとのISAC的な横連携の中で、攻撃者が渡り歩くみたいなことが結構あったそうで、それを国家的な情報共有体制の中で、ある程度防いだという話を聞いているので、そういったことを含めて、オリパラのCSIRTと重要インフラの私どもとのかかわりを、どのように考えているのかをお聞きしたい。

○（栁島参事官）大きな攻撃がなかったのは、事実だが、我々としても、準備を十分にとっており、それが若干のトラブル時に機能していることも確認できたので、前向きに捉えて、今後も引き続き体制をきちんと整備して、運用していくということで、そういう意味では、うまくいっていたのではないか。

オリンピックCSIRTについては、試験的運用という話をした際には、現時点では、いわゆる所管省庁や、サイバーセキュリティのベンダーといった関係機関の方に入っていただき、情報共有を試験的に運用しているところ。このような形の運用で、個々の事業者の方にまで入っていただくのは、運用上、かなり無理がある。今後、情報共有のためのシステムといったものができてくる中で、重要インフラ事業者の連絡が、どのような形で運用されるのか、検討していかなければいけない。

【関係省庁及びセプターカウンシルの取組状況について】

金融庁から資料４に沿って説明。

総務省から資料５に沿って説明。

経済産業省から資料６－１から資料６－３に沿って説明。

金子委員から資料７に沿って説明。

(3) 討議事項

【行動計画の見直しについて】

事務局から資料８に沿って説明。質疑応答は以下のとおり。

○（稲垣委員）サイバーセキュリティ2016に関して、２つほど、御検討いただきたい。

１つは、IoT。関連する予算の投資、社会の発展を踏まえたものであり、IoTをターゲットにした取り組みが大事だと思うので、一層深く検討していただきたい。

その際に、我々が考えているセキュリティ対策のスコープを慎重かつ積極的に検討していただきたい。

具体的には、IoTと今までのものの違いについては、IoTつまりネットワークの先にあって、IoTに接続されるものが非常に多様になってくるのと、環境も変わってくる、責任主体も多様になってくるところが、質的な変化に結びついてくる。質的な変化が量的な変化につながり、その産業が発展する仕組みだと思う。

そうしたときに、今までのセキュリティ対策のスコープ、IoTにたどり着く接続点までで、IoTを利用した機能は、端末接続者あるいは製造者の責任として、区分けしていた。今後こういう区分けが本当に通じるのか、検討していただきたい。

ある地裁判決で、例えばコンピュータシステムを利用してビジネスを行う、システムに依存してビジネスを行う事業者は、利用者に対して、安全なシステムを提供する義務があるということを述べたものがある。この視点は、非常に大事。旧来の民法の理論から、接触する者は、相手方を保護する義務があるという、このシステム版であり、技術的には非常に難しいことだとは思うものの、チャレンジとして、スコープを広げ、考えていく必要がある。

もう一つは、全体を通じて、今までの研究成果はすごくよくできてきたと思うので、新しい課題の検討をお願いしたい。これが２点目。

成長戦略の中にサイバーセキュリティを位置づけたというのは、セキュリティに関して、質的な変化があったと思う。成長戦略の中に位置づけたというのは、こうした技術をサービスや、製品の価値に転嫁し、国内のみならず海外での市場でも、積極的に日本のメーカーあるいは販売者を知っていただいて、評価していただくものの中に位置づけるということだと思う。

ここの研究テーマをずっと見ていってみると、要素技術の研究とか、国際的な事業者の環境整備は出ているが、消費行動、あるいはその消費環境整備についての研究にも、十分に資金を出すことが必要ではないか。

今まで私たちはユーザー側や、攻撃を受ける側が何をすればいいのかというところから始まって、全体環境の整備、経営問題等に展開してきたが、セキュリティと

いうのは、技術と人によって支えられて、技術、人材はきているが、これを接続してビジネスに結びつけていく、ビジネス自体を研究するというテーマもあっていいはず。このため、課題の１つに、セキュリティ技術とセキュリティ人材の活用、販売、浸透、そうした技術の基礎的・応用的・実務的な研究にもきちっと資金を出す方向で、進めていけば、ユーザー側のセキュリティ環境の整備に資すると思われる。

○（渡辺会長）具体例に基づいた知見をいただいたと思うが、１点目の安全なIoTシステムということで、安全性をどこまで確保するかというスコープを能動的に広げるという御意見だと思うが、追加のコメント・御意見は。

○（谷脇内閣審議官）IoTのセキュリティはとても大事。御紹介したように、今、総務省と経産省でIoTセキュリティのガイドラインの案を出しているところ。包括的なセキュリティガイドラインを両省でつくったが、スコープそのものに立ち返って、IoTのセキュリティを考える上でのフレームワークを明確にする必要があると考え、NISCで、先般、10日、IoTセキュリティのための一般的枠組みというもの、５ページほどの文書を公表し、パブリックコメントに付しているところ。

その中では、今、御指摘があったように、１つのIoTシステムから別のシステムにリスクが及んだときに、システミックリスクをどう考えるかとか、責任分解点をどのように考えるか。それから、セキュリティに求められる要件を段階的に実装するものと、全ての領域に求められるもの、こういったものを少し分けて考える必要があるのではないかとか、こういった問題提起をさせていただいている。皆様方にもコメントを頂戴できれば、大変ありがたい。

また、今回の一般的枠組みのパブリックコメントについては、案文を日本語と英語の両方で用意して、公表している。アメリカあるいはイギリスも含めて、海外からもコメントを求めている。こういった国際的なコンセンサスづくりも含めて、できれば日本で主導したい思っているので、そういった強い意識を持って、我々も取り組んでいきたい。

○（渡辺会長）　パブコメにかかっているとのこと、ぜひごらんいただいて、積極的な御意見をいただきたい。

稲垣委員からあった、２点目については事務局で、コメントとして受けて、御検討いただきたい。

○（稲垣委員）最近の状況との関係で、お願いしたいことがある。

セキュリティの分野でも、合理的なセキュアなシステムをつくるという意味だが、法律家がセキュリティを議論したときに、CIAというのは、コンプライアンスの問題でもあるという捉え方をする。そうしたときに、これを支えるシステムは、目的に従って最適なものでなければならないということが、派生する。

具体的には、開発なり、運用、保守に当たって、これがきちんと責任を負った主体のもとで、その責任が全うできるような内容でシステム開発が行われて、そして、

それによって可用性が確保され、法令を遵守し、かつ契約を実現するシステムがセキュアに動く。それによって、CIAが実現されると理解されているが、最近、重要インフラのシステム開発に当たっては、必ずしもこれが十分に行われているとは、認められないケースが出てきたりもする。

例えば非常に大きなシステム開発に当たって、それが障害を起こす、あるいは十分に機能しない。こうした開発が行われて、それが特に国の予算で行われていたような場合には、大きな損失を国民に与えている。しかし、損害の賠償もきちっとできているかどうか、よくわからない。こういうシステムの存在が散見される。

国民の基盤をつくるとか、国民に大きな影響を与えるシステム開発、運用、保守に当たっては、きちっと責任を負った主体が十分な評価をしながら進める。高い能力の人がサインした、確実なシステム開発のプロセスが必要だと思う。

例えば実際に制度としては、調達の適合性評価は行う。同様に、品質、要件、開発プロセス、開発リスク、こうしたことを把握して、場合によっては、とめろ、あるいはつくれ、でも、これはこういうリスクがあるということを国民に対してきちっと責任を持って伝える、あるいは国民に対してはなくても、国に対して、あるいは重要インフラの利用者に対して伝えるという、そういう機能を持った公的な存在があっていいのではないかと思う。もちろんそれは限定された、非常に大事なシステムだけに適用すればいい。

やはり大事なシステムについては、この人あるいはこの組織がうんと言わないと前に進めないという制度をつくるべきではないかと思う。国がつくるか、自主的にやるものを国が支援するかこれはやり方の問題。

○（渡辺会長）私も冒頭に申し上げたが、システム開発への費用が、満額で通らないときに、スペックをどこへ落とすかというと、セキュリティは最低限というところがありがちな世界において、オペレーションでそれをどう担保するかといったときに、CIOではない現場のオペレーターで、その人がうんと言わないと運行できないとか、歯どめになるような人材を同時に育成しなければいけないというところの御示唆だと思う。

○（高見澤センター長）今の稲垣先生の問題提起というのは、サイバーセキュリティに限らず、日本政府の様々な事業に当たって、構造的問題があるのではないかと思う。これは個人的な見方だが、実際の事業のやり方を見ると、最近の入札制度の中で、３種類ぐらいに分かれてきているのではないかと思う。

１つは、システムを設計する側とユーザーである政府が、ある程度対話をしながら、システムをつくり上げていくやり方。

もう一つは、いわば企業の売り込みに対して、政府側が比較的それを丸飲みするような形でやっていくやり方。

それから、最近あるのは、いろんなスペックなり、リクワイアメントを出して、そ

れに対して入札をして、事業を進めていくこと。

そのいずれも、かなり問題を抱えているのではないかと思っているが、特に最近多いパターンでいえば、リクワイアメントを出して、それに対して、いろいろやっていくときに、客観的に評価するシステムができていないということと、政府側からリクワイアメントを出すときのディテールを要求する能力がないということで､その結果､できたものに対する評価を客観的にしようにも、前提となるリクワイアメントというのは、どこまで具体性があるのかというところの問題にかなり直面してしまっているのではないか。

先ほど現場がうんと言わないからという、ストッパーという話があったが、現実のストッパーというのは、システムに問題があるのではないかと現場が考えているときに、これでいいのではないかという形で、トップダウン的にそのシステムが採用されていくことがかなりあるのではないかという感じを持っている。私自身はいわゆるシステムの設計といったときに、評価をするということは、非常に大事だが、いわば事業を方向転換できるのかどうかというところが、非常に大事でありまして、方向転換をするためには、プロセス管理というのか、常にリクワイアメントについて見直しをしながら、スパイラルにそれを変えていくような、トレードオフスタディーをやりながら、スケジュール管理も、遅れてもしようがないものは遅れるということも許容した上で、全体をマネジメントするというところが、非常に大事になってくるのではないかと思っている。

この問題は、何十年もそういうふうに感じているが、改善されない。そろそろ改善されないことが、許されなくなってきている。特にサイバーセキュリティの問題は、災害の問題と似たところがあると思うが、一旦事が起きてしまうと、取り返しがつかないということだと思うので、そういった問題意識を持ってやっていく必要があるのではないかと思う。

○（渡辺会長）もし見直し案に入れるとすると、人材育成とか、その体制とかの辺になると思われる。

○（大高委員）オリンピックに向けての体制について、2019年度にCSIRTの試験的運用というお話がありましたが、実際にオリンピックに向けての協議というのは、リオが終わった段階から、日本において始まるのではないかと、よく言われている。藤沢市もオリンピックの会場なので、矢面に立つのではないかと危惧している。この４年間の間に、IoTを中心とした、さまざまなものが新たに導入されて、システムは膨らんでいくが、それに伴い、リスクがふえ、脅威になっていくという課題がある。

具体的にいうと、各自治体は、今、外国人観光客の誘致のために、Wi-Fiの整備に躍起になっている。そこで、認証もないようなWi-Fiを入れると、それが踏み台になる。そういうリスクがこれから増大するという課題が常にある。オリンピックまでということではなく、今後、行動計画の中で、セキュアなものは、きちっと導入するような

仕組みにして、攻撃に対する対策ではなくて、その前に、踏み台にされないとか、環境を守っていくというスタンスをとっていくことが、必要だと思う。そういう意味で、オリンピックに対する対策は、既に始まるという考え方を何か盛り込めないか。

○（渡辺会長）大変貴重な御意見。

外国観光客誘致のために、少し前のめりになっているオープン型のシステムについては、既に攻撃対象になっているということ等、オリパラに向けての対応というとこで、行動計画に反映すべきことだと思う。

○（渡辺会長）議長だが、簡単に、素朴な疑問がある。

民営化が進んでいる重要インフラにおいて、民業としてやるところには、限界がある中で、先ほどのセプターの組織の改定も含め、基本的には、民業が、自主的に行動するのが、大きな流れになっている。一方で、昨年、金融庁のガイドラインを策定後、分野横断的演習に大量の地銀が参加する等かなり大きな影響がある中で、先ほどの金融庁の発表の中で、いろいろアンケートをとりながら、「これは検査とは別です。」と言って実施するのは、大変よいことと思われるが、ある段階で、ソフトプレッシャー、例えばシステムの運用方法、評価の方法を確認するということをある程度行わないと、金融機関、当局対応としては、最低限までということになってしまう。

この辺のさじかげんというのは、金融分野の感応度が一番高いと思われるところ、どのような考えをお持ちかについて、金融庁にお伺いしたい。

○（金融庁）サイバーについては、こういった取り組み方針を打ち出してから、まだ１年というところ。いきなり検査で入っていて、けしからぬとか、そういうことは、金融庁としても、まだ言える立場になく、官民一体となって、あるいは民も、一金融機関だけではなくて、金融ISACのように、様々な情報を共有しながら、共助の考えで、互いに連携していくことが非常に大事な分野だと思っている。金融庁としては、もう少し現状を把握した上で、底上げを図ることが先決だと考えている。

○（渡辺会長）官民で日本の市場とか、システムを守るというスタンスは、大変重要と思うので、継続実施と同時に、タイミングを見て検査を入れると、逆に当事者としては、話が通りやすく、予算や人の手当をしやすいので、今後その辺のさじかげんをお願いしたい。

○（稲垣委員）今の情報の共有と育成に使うという話に関連して、そろそろ重要インフラのシステム事故調を検討する段階にきたのではないか。事故調については、具体的な機能は、いろいろな脅威・攻撃が日本全国に入っていて、それをある程度把握できる状況であり、日本全国の重要インフラで、事故がいろいろ起こっている。それはそれぞれの主務省の監督と対話だけではなく、重要インフラというのは、やはり公共財だと思う。会社も皆さんの市場から集めた資金を使い、かつ行政も国家もそこに関心を持ち、国民も信用する。そして、その便益を国民がみんなで受けるということだから、そうした公共財のもとで起こっている課題を吸い上げて、集約して、ほかに転用

していく。これも重要インフラの機能というか、大事な役割だと思うし、CSRと言うまでもなく、そうした機能を果たすべきではないか。

それをどうするのかといったときに、主務省というよりも、むしろこれはシステムやセキュリティに関する問題のため、非常に高い能力を持った技術者、あるいは知見を持った専門家、社会制度との関係を理解する経済法分野、さまざまな人が入って、原因を分析し、かつそれが成果として生きるように、社会に還元する。例えばそれを成長戦略の中で、評価、認証に結びつけてもいいし、そうした戦略の中で使っていく。そういう社会の中での情報を収集して、利用できる形に翻訳するという、そうした組織があっていいのではないか。

それをやるときに、重要インフラにおけるシステム障害ということになれば、警察事象であったり、防衛の話も出てくるかもしれないが、そこも相互に協力することで、警察の現場は障害事象を事件の捜査の中で全部把握している。こういうものもきちっと提供してもらって、公共財にしていく。法令が必要であれば、改正もするし、刑訴法のさまざまなものを使って、今の段階でもできることはやっていく。あるいは犯罪捜査規範の検討等でも、そうした組織との協力はできると思うので、情報収集と利用できる成果にしてための組織としての事故調をきちっとつくっていったらどうかと思う。

○（渡辺会長）NISCあるいは警察庁から、何かコメントがあれば。

○（高見澤センター長）答えはなかなか出ないと思うが、システム事故調というのが、今、色々な事案が起きているときに、それがある種それぞれの企業の中でハンドリングされて、実際の原因究明であるとか、本来、共有すべきものが、必ずしもうまくいかないまま処理されて、同じようなことが繰り返されている。一方で、重要インフラの関係についていえば、それぞれの所管省庁に責任があるが、いわばそれを越えたシステム的なところで見ると、センターがどこかにあって、それでやっていくという形のものがないと、なかなか共有されないという部分はあるのではないかと思う。稲垣委員ご指摘のアイデアについては、方向性としては、重要と思う。

一方、例えばセイバーセキュリティ基本法が改正されて、マネジメント監査やデイトレなどを実施する中で、うまくいく分野は協力的なところで、それぞれの段階に応じた形での信頼関係なりをつくりながらやっていくという部分がどうしても中心になっており、経営層、中心になる人が理解していない場合は、逆に余計なことをやっているのかという部分が、まだまだ残っている。だから、社会的な責任についての情報公開の考え方というのは、もう少し徹底して、いわゆるピースの情報を追及して、それが企業のリスクになるような、今の状況の中で、非常に厳しいとは思うが、少なくとも本質的に問題があるところについは、それが追及され、そうでないところについては、風評的なことにならないような形のものをつくっていく。そういう厳しいルールと、同時に、信頼性を高めていくためのことというのは、非常に大事だと思う。

そのためには、金融庁が努力しているような、これは全業種、我々についても言えることだと思うが、実態把握といったものがどこまで進められるか。そういった努力とあわせて考えていくことだと思う。そういったことをやらないと、何か起きてからでは、なかなかうまく対応できない。いわゆるサイバー台風的なものが起きてから、全体の制度をつくるということでは、ちょっと悲しいので、個人的には、探究してみるアイデアを含んでいるのではないかという印象。

○（稲垣委員）調達ガイドライン、調達契約の中で、事故が起こったとき、ベンダーに当然分析を行ってもらうが、ベンダーには、品質ガイドラインのような形で、そうした情報を国家的なシンクタンクみたいなものをつくって、そこへフィードバックする。それがベンダーのサービス品質になっていく。そうすると、例えば営業者は、そういうシンクタンクを利用しながら、さまざまな経験や、日本あるいは世界の知見を利用しながら、ビジネスができる。そういう環境をつくってあげて、さまざまな技法はあると思うが、もちろん今の話がベースにあると思うので、時を見ながら、進めていただきたい。

○（橋本委員）金融の証券分野の橋本と申します。

会長と金融庁の質疑があったが、私も日本証券業協会の場で、１年間の実態把握のフィードバックを教えていただき、会社実情を踏まえたかなり具体性のあるフィードバックをいただいているので、対話から始めるというところも含め、私どもには非常にありがたい状況。

そうした中、社内をさらに取りまとめていくためには、どうしてもサイバー犯罪のハードルを上げる必要があると感じる。攻撃されっ放しという感じがものすごくしていて、社内でも、「守るのに努力や金が必要なのはわかるが、そもそも攻撃してくる奴らが悪い奴らなのだろう」と言われてしまうと、なかなか返す言葉がない。私の知らない御努力もたくさんあるのだと思うが、取組をより強めていただきたい。

○（竹原委員）電力セプターの竹原でございます。

サイバーセキュリティ2016の案で、１点、御要望という形で、お話させていただきたい。20ページの下から（３）ということで、サイバー空間を悪用した国際テロ組織の活動への対策ということで、サイバーのインテリジェンス関係の機能の強化といった話があるが、こういった情報収集とか、分析した内容は、民間側、我々のほうにもぜひ提供していただきたいというのが、要望の結論。

電力については、電力の安定供給を阻害するというか、制御システム等が狙われて、事例であったような、ウクライナのようなことになって、広域的な大規模停電といったものにつながるということが、懸念であり、これらが全く発生しないように、業界内で様々な対策を積み上げているといったところ。

サイバー攻撃と言ってしまうと、あたかも１つに見えてしまうが、それはサイバーテロというジャンルのもので、犯罪者、国家、あるいはテロ組織などとは、違う質のものではないかと考えているところ。できれば、そういったものを未然にといったところで

は、そういった組織、国家レベルのところで、そういった攻撃が企図されているのではないか、もし企図されているのであれば、彼らはどういった攻撃手法というものを持っているのか、狙われる時期とすれば、どういったときが、どういった理由で候補にされているかといったインテリジェンスというか、分析される情報をぜひ民間側にも情報提供いただきながら、一緒に防備していくといった流れを御検討いただきたい。

こういったものが、恐らく伊勢志摩の中でも、実際にスキームとしてはやられていたものと理解しており、2020年のオリパラに向けては、ぜひ官民の相互協力というか、役割分担みたいなところも交えながら、一致して安全にやっていく、取り組みを目指すといったことではないかと考えており、ぜひよろしくお願いしたい。

○（渡辺会長）そういう意味では、国家安全保障の枠組みの中で、国家テロレベルになると、事案対応のところと実際のオペレーターのところとの連携強化ということになると思うので、文言上はあるが、実際に具体的なコミュニケーションラインや、訓練も含めて、実態を伴うような努力をいただきたい。

○（平田委員）通信の平田です。

情報共有について、今回、サミットがあったが、今回、我々重要インフラとして、たくさんのプレイヤーが連携して、情報共有体制をつくって、そこを情報が流れたというのは、今後に向けて、非常に大きなスタートだったと捉えている。

今回、見直しに向けた検討事項でも、情報共有ということで、色々な検討テーマが設定されているが、今後、検討するに当たって、流す中身と、それを受け取ってどう活用するかというところをセットで議論すると、非常によいと思う。

○（渡辺会長）実際は訓練等でやっていく話になると思うが、情報のレベル規定とか、事務局はぜひ具体的なアクションとして反映できるような形で、お願いしたい。

○（有村委員）JPCERTコーディネーションセンターの有村です。

機能保証の話の関連だと思うが、事故調査、いわゆるオープンインテリジェンスではなくて、グレーな部分を含めての議論があったと思う。行動計画、あるいはサイバーセキュリティ戦略を年度ごとに出していくに当たり、事象の変化を当然キャッチアップしていかないといけないということで、新しいコンセプトがそれぞれ入ってくるのが、宿命だと思っている。ついこの間のものでいうと、連接融合情報社会というコンセプトが入っていて、IoTという言葉を使わずに、努力をしようとしていたところがあった。それから、今回の部分でいうと、まさに議論を深めていただきたいところで、機能保証という話がある。

機能保証という言葉を、今のようなワードの中で、サブテーマに分けると、いろいろ出てくると思う。重要インフラ事業者が、社会に対してどう機能を保証するのかということだが、その言葉は、コンセンサスがとれていないまま、話が進んでいるような気がする。

例えば航空とか、あるいはプラントなどの話でいうと、インシデント、重大インシデント、シビアインシデント、アクシデントという形で、どんどんエスカレーションが上がっていく中で、そこのエスカレーションにいかないようにするために、どうすればいいかと

いうところは、情報セキュリティが言っているインシデントとは、全く違う概念のような気もする。そういうことを考えると、言葉１つとっても、なかなか理解ができない、あるいは用語が違うというところは、JPCERTがインシデントの重要インフラの皆さんとお話をして、現場に行くときにも、そこの部分での乖離感を大きく感じる。そういう意味でいうと、金融庁と證券のような、わかり合うために理解をするところから進めていくということは、非常に大事なことだと思っており、我々もそういう意味合いで、オペレーションの立場で努力している。

現場ベースでいうと、大変難しい話だと思っていて、私がJPCERTのメンバーに対して言っているのは、重要インフラの皆さんに徹底的に寄り添えと言っている。知らなければいけないことというか、知らせなければいけないことも当然るし、それは国に対して、業界団体に対して、ほかのところに対してということはあるが、事故が起きている現場に対して寄り添わないと、結果的にいうと、どんどん穴蔵にこもっていくというのが、日本のカルチャーのような気がする。そういうことをある程度解消する言葉として、機能保証を使うならば、今回のところで、この言葉を使って、少し深堀をしていきたい、あるいは深堀をするための場をぜひ持っていただきたい。

非常に拡散的な話をして、まことに申しわけないが、今、私はそのように感じている。

○（渡辺会長）これは本当に貴重な意見。言葉の定義もさることながら、実際にその言葉のすり合わせをすることによって、利害関係者がレベルを合わせようとするというのは、大変重要な話なので、また別の機会に検討するということで、事務局にお願いしたい。

範囲拡大という意味では、中小零細も含めて、先ほど金融庁のほうで、信金信組まで出てくるという意味では、だんだん裾野が広がってきているが、同じような動きで、ケーブルテレビでも、結構小さいところまで既に入り、かなり積極的に展開されていると認識。取り組みの現状や、中小も入れて、範囲拡大を積極的にやっていく上での課題があれば、簡単にコメントをいただきたい。

○（伊澤委員）伊澤でございます。

ケーブルテレビでは、組織名とか、役職の方の名前を入れれば、とりあえず策定できるケーブルテレビセクター事業者用の情報セキュリティポリシーのひな形をつくった。まずその形をつくり、回し方はいろいろあっていいのでPDCAを回してください、という話を、いろんな事故が世間一般であったので、そちらにかぶせるようにしてお願いをし、今、332社、９割近くまできた。

ケーブルテレビみたいな小さな会社では、まず余裕がない。なので、そういうところに手が回らない。差し伸べれば、とりあえずはやるようになるといった流れはあるというのを、この１年半、重要インフラ事業者への転換で感じた。

○（渡辺会長）そういう意味では、例えば電力ように、プレイヤーが限られて、それぞれに体力があるところと、そうではない、中小も含めて、面的防護に対して、脆弱点がいっぱいあるところがある。重要インフラといっても、１つのパターンではないところ

で、今後この取り組みを展開するために、いろいろなパターンがあろうかと思うので、そういったところも、ぜひ共有いただきたいという思いで、少し話していただいた。

(4)その他

その他、各委員からの特段の発言はなかった。

(5)閉会

谷脇審議官から挨拶。

○（谷脇内閣審議官）NISC副センター長としまして、３年間仕事をさせていただいた。その間、2014年５月に重要インフラ関係の第３次行動計画の策定、またサイバーセキュリティ基本法を制定・施行、その改正も行った。

NISCの機能強化ということで、いろいろと取り組みをしてきた。ただ、昨年５月に起きた、日本年金機構事案の教訓も踏まえた、昨年９月のサイバーセキュリティ戦略もあった。なお、行っていくべき課題は非常に多いと思っている。とりわけNISCとしては、これからの１年ないし２年、重要インフラの防御の強化ということは、恐らくトッププライオリティの仕事になると思っており、その際、情報共有を初めとするさまざまな強化策を講じる必要がある。

ただ、これを実施するためには、重要インフラ事業者の皆様方に、情報共有のメリットをいかにわかっていただくのか。実感できるようなシステムであったり、あるいはそれを阻む制度であったり、こういったものがあれば、それを取り除くのが政府の役割だろうと思っているので、今後ともNISC、あるいは関係省庁の重要インフラ関連のサイバーセキュリティ対策につきまして、格段の御協力、御配慮を頂戴したい。

３年間、どうもありがとうございました。