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９回会合　議事概要

１　日　時

平成 28 年 12 月 15 日（木）16 時～18 時

２　場　所

金融庁１２階　共用第二特別会議室

３　出席者（五十音順・敬称略）

阿部　克之　委員　（電気事業連合会）
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）
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）
鈴木　栄一　委員　（一般社団法人日本損害保険協会）
手塚　悟　　委員　（慶応義塾大学大学院　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）
野口　和彦　委員　（国立大学法人横浜国立大学　リスク共生社会創造センター　兼　大学院　環境情報研究院）
橋本　伊知郎委員　（野村ホールディングス株式会社）
原田　充　　委員　（日本航空株式会社）
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）
盛合　志帆　委員　（国立研究開発法人情報通信研究機構　サイバーセキュリティ研究所）
渡辺　研司　会長　（国立大学法人名古屋工業大学　大学院工学研究科）
渡辺　睦　　委員　（石油連盟）

（事務局）

中島　明彦　内閣サイバーセキュリティセンター長
永井　達也　内閣審議官
三角　育生　内閣審議官
山内　智生　内閣参事官
阿蘇　隆之　内閣参事官
狩俣　篤志　内閣参事官
栁島　智　　内閣参事官
林　　泰三　内閣参事官
瓜生　和久　内閣参事官
伊貝　耕　　内閣企画官

（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流通振興課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
厚生労働省政策統括官付サイバーセキュリティ担当参事官室
厚生労働省医政局研究開発振興課医療技術情報推進室
厚生労働省医薬・生活衛生局生活衛生・食品安全部水道課水道計画指導室
経済産業省商務情報政策局サイバーセキュリティ課
国土交通省総合政策局情報政策課情報セキュリティ対策室
原子力規制庁長官官房総務課情報システム室
警察庁警備局警備企画課サイバー攻撃対策官
警察庁長官官房総務課
警察庁情報通信局情報技術解析課
外務省大臣官房情報通信課
防衛省整備計画局情報通信課

４　議事概要

(1) 開会（挨拶）

中島センター長から挨拶。

○中島センター長　重要インフラ専門調査会の開催に当たり、一言申し上げたい。

本分野の重要な取り組みの１つである分野横断的演習を12月7日に実施したが、参加者は、過去最多であった昨年度を更に大きく上回り、約2,080名となった。大林先生をはじめ、協力いただいた皆様に改めてお礼申し上げたい。

当日は、東京オリンピック・パラリンピックの担当大臣、また、サイバーセキュリ

ティ戦略本部の副本部長である丸川大臣から「東京大会まで既に４年を切ったが、この大会を成功させるためには、サイバーセキュリティの分野においても、万全を期してほしい」旨の発言があった。東京大会は重要なマイルストーンになると考えており、本日議論いただく行動計画の見直しにおいても、念頭に置いて盛り込んでいきたいと考えている。

前回の専門調査会では、第３次行動計画の見直しの骨子として、①先導的な取り組みの推進、②情報共有体制の強化、③リスクマネジメントを踏まえた対処態勢の整備、この３点を重点項目としてまとめていただいている。今回は、その骨子に沿い、第４次行動計画を事務局案として作成した。前回の調査会でも議論いただいた重要インフラの機能保証といった考え方について、前面に打ち出した内容としている。

これから議論いただいた結果については、後日、サイバーセキュリティ戦略本部において審議いただいた上で、パブリックコメントにかけることとなる。委員の皆様方には、本日も活発な議論をお願いしたい。

渡辺会長から挨拶。

○渡辺会長　官民、国内外を問わず、サイバー攻撃の脅威は、ますます巧妙なものになってきているところ。特にランサムウェアによる攻撃として、データを盗むことではなく、企業が提供しているサービス、ソフトウェアを人質にするという形のものが出てきている。

海外の事例でも、サンフランシスコの市営鉄道の発券システムが、ランサムウェアにやられ、発券ができなくなったが、人々の移動は継続しなければならないという状況となり、無料で通すという対応がなされた。サービス的には、機能を維持できたが、システム的には機能させることができなかったという事例である。

鉄道は重要なインフラの１つであるが、実際に事案が海外で起こっていることを鑑みれば、我々も脇を固めて分野横断的にそこを詰めていかなければいけない、というタイミングがいよいよ来たのだと考えている。

先ほどセンター長の挨拶にもあったとおり、前回の第８回会合では、次期行動計画の見直し骨子として、①先導的な取り組みの推進、②情報共有体制の強化、③リスクマネジメントを踏まえた対処態勢の整備、この３つを重点項目として議論いただいた。

今回は、それに基づき、パブコメにかけるための案が提示された。タイミング的には、皆様からのテクニカルな意見を本日出し切っていただきたいという思いがある。

また、第４次行動計画は、東京オリンピック・パラリンピック競技大会に向けての期間に重なるものであるので、最も大切なタイミングだと考えている。本日も闊達な議論をよろしくお願いしたい。

(2) 報告事項

経済産業省より、資料２に沿って、割賦販売法の一部改正について報告。

質疑応答は次のとおり。

○渡辺会長　（情報の適切な管理を）義務づけるということは、ペナルティーや監査義務などというものを検討しているということか。

○経済産業省　罰則は規定していない。ただし、法律に義務づけることで、コンプライアンスという意味で、事業者の取組を促していくことになると考えている。

(3) 討議事項

事務局から資料３・資料４に沿って説明。

質疑応答は次のとおり。

○大高委員　資料４の１ページを見るとわかりやすいが、１つ目として先導的な取組、２つ目としてオリパラ大会を見据えた情報共有体制の強化という形で記載されており、あらゆるところで「オリパラ」という言葉が使われている。時期的にやむを得ないことかもしれないが、「オリパラ」という見方をすると、会場周辺など局所的な形で捉えられてしまう可能性があると思う。それを先導的取組と同様に全体に広げていく、あるいは、「オリパラ」というのは、サイバーセキュリティの観点から見れば地域性は関係ないということを強調しておかなければ、地域的な取組と捉えられ、マイナスイメージだと感じている。

○柳島参事官（事務局）　「オリパラのために」とならないよう、「オリパラ大会を見据えた」などの表現としているが、より良い表現を提案いただければ修正を検討したい。

○渡辺会長　イベントや一過性のものと勘違いされることは避けなければならないので、書きぶりについて提案などお願いしたい。

○稲垣委員　機能保証という概念を前面に打ち出したことについては、（重要インフラの）考え方が変化してきていることが認識されており、努力の成果が現れてきたと感じている。また、ＩＴ障害からサービス障害へ概念を変化させたことについては、内容は緩やかに進むのだとは思うが、関係者が取り組む際の指標になるという意味で、大変有意義な変化だと感じている。これについては、様々な機会に繰り返し言及して普及させていくことが大事であると思う。さらに、全体として、情報共有の際の匿名化に特段の配慮が図られており、さまざまなチャンネルを利用する際の匿名化を考えているということがすばらしい。法的に見ても、企業の保有情報を流通させることには責任というものがついてまわることになるが、それに関わらず対処をしなければならない現実がある。責任から切り離すためには、匿名化が非常に有効な手段であるので、力を入れて取り組んでほしい。それぞれの連携先のチャンネルとの取組において、匿名化がうまく使えないかということをそれぞれに検討すると非常に有効だと思う。

少し心苦しいが、ここからは苦言を呈したい。全体のトーンとして、前段部分では、一生懸命に取り組んできた、今後も取組を強化すると、具体的にやるぞと書いてあるが、後段に進むに従い、「検討する」などの表現となっている。特に、政府機関に関す

る部分のトーンが弱いと感じる。予算や制度など、内閣法の下でのそれぞれの制約があり、ずばり書くことは難しいのかもしれないが、行動計画は、内閣を含めた全体において協議して合意形成を行うメニューであるので、少しトーンを上げるべきではないか。

具体的には、資料３について、次のとおり。

1) P14 Ⅲ 2.1

情報共有体制に関する部分で、「関係主体と共有する仕組みについて、今後検討していくこととする」とあるが、情報共有体制は大事だと繰り返し言及し、匿名化について具体的な事項を記述しておきながら、一方では、「今後検討していくこととする」となっている。例えば、「仕組みを構築する」と書いた場合、役所用語として意味が違ってくるのか。そうでないのであれば、「構築する」にしてほしい。

2) P14 Ⅲ 2.2

1)と同様のことであるが、「情報共有の更なる推進」の項目においても、(「防護範囲についても・・・見直しを検討する」とあり、) 末尾が「見直しを検討する」となっている。見直しは行わなければならないことなのだから、ずばっと書くことが必要だと思う。

3) P16 Ⅲ 3.1.1

(「演習プロセスの改善に向けた検討を行う」とあるが、) 今既に、継続的な演習プロセスがあり動いているのであるから、課題があるならば「改善に向けた検討」ではなく、「改善する」ではないかと思う。英語版にして世界中に発信するとすれば、見る人が見れば日本のレベルが知れる。後に予算がつかなかったということもあるかもしれないが、それは評価を行えばよいだけのことなので、我々が何を目指すのかについては、しっかりと記述してほしい。

4) P17 Ⅲ 3.1.2

「仮想的な演習環境の提供等の検討を進める」とあるが、「提供等を行う」として取組を進めるべき。分野横断的演習が、大規模かつ充実して進められるようになったことから考えれば、しっかりと取り組むことができる体制を確保して実施していかなければならない。そのためには、プログラムについてもしっかりと取り組む必要があると思うので、ぜひ検討していただきたい。

5) P17 Ⅲ 3.1.3

「重要インフラ所管省庁等との連携」の項目については、全般的に腰が引けていると感じる。すべて「期待される」、「検討する」となっており、さらには「検討に着手する」という表現まで。最後には、「ニーズも踏まえ、必要に応じて・・・検討を行う」との表現もあるが、ほとんどやらないと言っていると認

識されてしまうのではないか。これは大事なことなので、民間が一生懸命やろうと、連携を図ろうとするならば、政府機関もそれなりの決意を示すべき。目指したけれどできなかったのであれば、また頑張るということでよいのではないか。

例えば、２段落目の「相互連携の在り方について検討する」は、「相互連携を構築する」ではないか。一緒に連携しようと言ったとしても、「検討する」だけであれば、連携主体は、体制も構築できず、部隊もつくれない。本当に困ると思う。

３段落目の「在り方等についての検討に着手する」は、他との平仄を合わせるにしても、「在り方等を具体化する」ということではないか。ＩＳＡＣが検討に着手する側だとして、話合いの会議だけ持たれても時間の無駄と感じるだろう。やるということで、やらないといけない。

最後の段落の「・・・要する可能性もあるため、関係主体からのニーズも踏まえ、必要に応じて当該部門との連携の在り方に係る検討を行う」は「・・・可能性もあるため、当該部門との適切な連携を構築する」ということなのではないか。やらないということではなく、やると書いてもらいたい。

6) P25 Ⅲ 5.4

セキュリティ・バイ・デザインについては、民間において、第三者認証の制度との関係でいろいろな動きがある。認証制度というのは、国際競争力の観点で非常に大事な要素。これに言及する際に「活用を検討する」ということでは、例えば経産省が促進しようとしても腰が引けてしまうのではないか。経産省にやれというくらいの気持ちで、「活用を検討」ではなく「活用を促進する」とするべきではないか。

例をあげれば、実際、制御系セキュリティの認証制度をつくろうとさまざまな努力がなされるが、予算が続かず事業を継続できないなどの弊害も起こっている。ＩＳＭＳ、ＣＳＭＳ、ＢＣＭＳなど、いずれも未熟で普及していない。原因はさまざまあると思うが、まだまだ手緩いという印象。もっと力を入れて、予算や人的資源を投入できる体制ができれば、より充実していくのではないかと現場にいて感じている。ぜひ力を入れて取り組んでほしい。

7) P25 Ⅲ 5.5

「経営層への働きかけ」の項目に、「実効的なものとするよう努める」とある。企業の経営者がこれを見たら、何を言っているのかと笑ってしまうのではないか。この直前の部分では、一生懸命に取り組み知見を得て、つまり、政府機関が働きかけて民間から知見を得たら、そのお返しとして、政府機関は重要インフラ防護政策を実態に合わせた実効的なものにする、ということが記載されている。つまり、政府機関に協力した対価として、国のためになる、みんなのた

めになると思い、民間企業は一生懸命協力したが、蓋を開けてみれば、「実効的なものとするよう努める」だけでは協力のしがいがない。失礼ではないかと思う。

8) P27 Ⅳ 1.(2) ⑤

（「脅威情報を分野横断的に集約する仕組みの検討」とあるが、）この部分も「集約する仕組みの検討」だけでは、もう間に合わないのではないか。情報共有が大事だと言って、匿名化などさまざまな議論をする一方で、仕組みは検討だけ。そのような段階ではないのではないか。趣旨がよくわからない。さまざまなことをイメージしているのだろうが、ここは「検討」ではないと思う。

9) P29 Ⅳ 2.(1) ②

この部分は、実施に困難が伴うものだが積極的に進めるため、「さらに、必要に応じて情報セキュリティ対策を関係法令等の保安規制として位置付けることや、・・・」と記載してあり、前進させたいという意欲を感じる。しかしながら、書きぶりの中に、さまざまな困難が見えており、少し整理する必要があると考える。

１点目は、「定期的に」以下に、定期的に実施する内容が書いてあるが、ここで、実施する際の視点を明確にする必要があると思う。例えば、「機能保証・サービス障害防止の観点から定期的に・・・」とするなど、この観点からこういうことをやる、ということを明確に記載してはどうか。

２点目は、「必要に応じて・・・」という部分。この意味がわからない。「適切な」という意味なのだと思う。この表現があることで、必要性を検討してみたらやはり必要なかったのでやらない、という読み方となり、腰が引けているような印象を受ける。例えば、「必要に応じて安全基準等の改定を実施」は、「適切な安全基準等の改定を実施」などとするべきではないか。

表現のトーンを上げる話とは別の話として、資料３ P29 Ⅳ 2.(1) ② の「セキュリティ対策を関係法令等の保安規制として位置付けることや・・・」については、関係法令に情報セキュリティ対策を位置付けることは非常に大事なことだと思うが、「保安規制として位置付ける」に当たっては、今までの法制度との整合性を十分に検討して、法制度の不足があれば果敢に法改正に挑戦していただきたい。

例えば、電事法の保安規定は、電力の供給、人損の防止、物損の防止、電磁波障害の防止、を目的とするもの。その保安規定に情報セキュリティ対策を位置付けると、電力の供給、人損・物損・電磁波障害防止を目的とするためのセキュリティ対策になってしまう。一貫体制のもとではこれでよかった。ところが、電力改革は、発送電小売業者が電力を取り引きすることによって実現される。つまり、改革後は、電力事業は、電力だけでなく、取引情報やスマートメーターから上がる電力量データによって、

実現される。機能保証のために必要なセキュリティ対策の範囲は、電力だけでなく、取引情報、事務情報、経営情報、スマートメーターの情報に及ばなければならない。これらをサイバー攻撃から守ることができなければ、電力改革のもとでは、電気事業の機能保証はできない。そのため、保安規定の中に情報セキュリティ対策を位置付けるには、電事法の「保安」の目的に、取引や電力市場の機能保証に必要な情報のＣＩＡを入れるか、「保安」の目的を従前どおりにしておき、電事法を改正して、これらのＣＩＡも入れなければならない。

大切なので繰り返すが、今の電事法の保安規定にサイバーセキュリティを位置付けても、例えば、スマートメーターの情報や事業者の取引、経営情報をサイバー攻撃から守る措置を執り得ない。電気は流れ、人損・物損はないし、電磁波による影響もないからである。しかし、これでは電気事業の機能保証にならない。金融も鉄道も同じ。「保安規制として位置付ける」という書きぶりは非常に良いと思うが、そのような意味では、これが保安規定の検討と認識されてしまうことで、同じ問題を生じるのではないかと危惧する。したがって、「関係法令等の保安規制として位置付ける」との書きぶりは残しつつ、「保安規定の改正については、機能保証の観点から再検討」、「・・・一層の検討を要する」など、どこかに注釈を入れておく必要がある。

最後に、資料３ P50 以降の「重要インフラサービス障害の例」について。ここに、障害の事例が記載されているが、取引情報や経営情報に関する障害が含まれていない。注釈を入れるなどして、これらが含まれることを明確にすべきではないか。機能保証とは、現実に組織や企業が果たしている役割を国民に確実に届けることだと思う。そうだとすれば、経営、人事、給与、業務、契約などをつかさどる情報システムも、力を入れて大事に守らなければならない。サイバーセキュリティの対象としなければならない。そうでなければ完結しないと思う。

制御系に関する記述が増えたのは、情報だけではなく制御の部分も重要である、エレベーターを動かす、電気をつける、水を出す、機械を守るということなども重要なことであると気づいたということであり喜ばしい。機能は、経営、取引、人事なくして保証できない。ここでもう一つ気づいてもらい、経営、取引、人事などに関するシステムもサイバーセキュリティ対策の対象になるということを考えてほしい。

○栁島参事官（事務局）　なるべく前向きに書くということについては、指摘のとおりであると思うので、語尾については必要な修正を行いたい。

経営に関する取引情報なども機能保証の観点から非常に重要であるということも、指摘のとおりだと考える。今回の案では、機能保証という観点から、これまで業法に限られていたような部分について、保安法にも拡張したところ。委員の指摘は、それをもう少し乗り越え、更に経営に関する情報まで範囲を拡げるべきではないかということと理解。実際問題として、業法などの現状を踏まえれば、この点について、今すぐこうすると結論を出すことは難しいが、取引情報をしっかり守らなければ、実際の

ビジネスとして回らないということは、指摘のとおりだと思う。今後、検討していく中で、「こういった点にも着目をしていく」という趣旨を注釈するなどの対応を検討したい。必ずしも法律である必要もなく、ガイドラインなどへの記載も案としてはあると考える。

○野口委員　第３次行動計画からの視点の転換も含め、本会議で議論した内容をよく取り入れた計画になっていると思う。２点、コメントさせていただく。

１点目は、Ⅲ章の4.「リスクマネジメント及び対処態勢の整備」について。4.2.2「新たなリスク源・リスク等に関する調査・分析」の項目において、「新たな」をつけたことを高く評価。これまでは、リスク分析を行っていると言っても、基本的に、点検したものをリスク分析の格好にまとめただけのものが多く、新たなものになっていなかったということを考えると、この捉え方は良いと思う。

ただ、4.2.2と4.2.3「対処態勢整備の推進」とで少しトーンが変わっていると感じており、4.2.3にある文章をつけ加えることを提案したい。これまでは、どういうことが発生するかということをリスクとして捉え、それを分析することをリスク分析と言っていた面がかなりある。しかしながら今は、セキュリティの実行においては、ある事故が顕在化したときに、ある行動をとろうという行動計画の実効性が本当にあるかどうか、というところのリスク、不確定性を確実に捉えることが非常に重要なこととなっている。意外なことだが、日本のリスク分析はそこができていない。地震の発生確率を算定したり、地震が起きたときにはどうするかということは検討する。しかし、それは本当にできるのかという視点がない。したがって、リスク対応の確実性を高めるために、例えば、4.2.3に「対処態勢の整備においても、対応の実効性に関する不確定性をリスクと捉えて、リスクマネジメントを活用する」という趣旨の一文を入れてほしい。「リスクは、物事が発生するという現象だけでなく、それらの対処の中にもある」という趣旨を表現することを提案したい。

２点目は、多少議論がある部分だと思うが、Ⅲ章の2.「情報共有体制の強化」について。日本のリスク管理等においては、情報連絡や情報共有が非常に重要視されており、実際にその努力も行われている。このことは重要なことではあるが、我が国の場合、ややもすると情報共有自体が目的化する傾向にある。そうすると、各事業者は、どの状況までは連絡すべきかなどという枠組みを気にし過ぎてしまい、その枠組みに合致しているかどうかという議論に終始することとなる。リスクマネジメントや危機管理の立場から言えば、情報共有はあくまで手段であり、大事なことは、共有した情報によって何ができるか、何をするかであるので、これを明示することが非常に重要となる。Ⅳ章「関連主体において取り組むべき事項」の「「情報共有体制の強化」に関する施策」に、幾つか書いてあるようにも見えるが、一方で、表題からは、あくまで情報共有体制の強化を目的とした施策に見える。例えば、2.3「重要インフラ事業者等の活動の更なる活性化」の項目に、情報共有自体が目的と見えないよう、「共有した情

報をリスクマネジメントや危機対応において、いかに活用するかということを明確にしていく」という趣旨の文章を加えていただきたい。情報をどのように使うかということと、どのような情報をどのように共有するかは異なるもの。日本では、情報連絡を早くすべき、共有すべきというところから発想しており、集めた情報をどのように使うかは、その後で考えるという構造。しかしながら、本来、危機管理、リスクマネジメントにおいては、何をしたいからどのような情報を集めるという形になるべきだと思っている。このことは、情報の共有自体に重要性がないと言っているわけでは全くなく、章の構成は原案で良いと考えているが、この中で、「情報共有自体が目的ではなく、共有した情報をいかに活用するかが重要で、そこに対処していく」という趣旨を盛り込むことを提案したい。

○柳島参事官（事務局）　提案いただいた事項については、追記したい。特に、１点目の「リスクの対処におけるリスク」は、最先端の概念を盛り込んでいくもので、非常にすばらしいことなのではないかと感じた。

○野口委員　工学系の技術者が分析を行うと、発生の部分の分析は得意なのでさまざま手を尽くすが、対処の実効性検証で重要な視点である、実行しようとしたことがさまざまな要因でできないという、防災や事故対応のリスク分析が非常に弱い。この点は、ぜひ盛り込んでいただきたい。

○有村委員　JPCERTは、１年間に多数のインシデントレスポンスの情報を収集しており、この活用に努力しているところなので、「情報共有体制の強化」についてコメントしたい。

具体的なコメントの前に、資料４　P5の図を見ながら、これまでの経緯を含めて少し話したい。セプターカウンシルの整備は、2008年から2009年にかけて行われた。聞くところによると、当時、NISCや各省との協議、業界で、どのような情報共有体制をつくるか、簡単に言えば、矢印をどうするのかという話になった。非常に議論になったのが、今回トライをしている上向きの矢印をどうするか、という点であったと理解している。さまざまな議論の結果として、まずは体制設置を重視し、ゼロから始めるに当たっては、上から下向きの情報提供だけで良しとした。それから７年ほど経過し、基本法ができ、状況の変化や要求の変化があり、今回、この矢印新設の再検討を行うものと理解をしている。これは非常に大きな方針転換であるというのが私の理解であり、そういう意味で言えば、官民の中で、あるいは委員の皆様の中で、相互理解しておくことは、絶対に必要なことであると思っている。これを前提に、３点プラスアルファのコメントをしたい。

１点目は、情報共有において使用目的と方法を明示するという課題について。情報の提供を受ける際、情報を提供する側が必ず聞くのは、受け取り側がそれを知ってどうするのかということ。先ほどのお話（野口委員）のとおりであるが、この点は、検討を具体的に進めていく中で、この整理は、避けては通れない課題だと思う。

２点目は、取得側の情報の取扱いについて。つまり、知った後でどうするのか、どのようにこれを扱うのか。先ほど匿名化に関する指摘もあったが、これを補完する論点だと思う。適切に取り扱うということについては、我々民間も必要なこととして行っている。これを官に渡したとき、安心して預けられるのかという問題。官には、国家公務員法を含め既に情報保全に関するさまざまなルールが存在し、多重に的確に情報をコントロールしているのだと思っている。大きな方針転換を行うのであれば、この機を捉え、「官には情報を多重に的確にコントロールするルールがあり、厳正に実行している、安心して我々に預けて大丈夫だ」ということを、もう一度、民間に対してしっかりと言っていただくのはどうか。例えば、P13に「政府機関からの指導等につながるのではないかといった懸念を払拭できず、情報共有の活性化を阻害する一因ともなっていた」との記載がある。これも2008年当時に既に出てきていた論点であるが、今、冷静になって改めて考えてみると、それだけではなく、預かったデータを確実に保全するということを伝えることも必要なのではないかと思う。そのようなルールが既に存在しているので、それを再確認するという発想で考えていただければと思う。

３点目は、ヒヤリハットの収集について。いわゆるヒヤリハットの情報も広く収集していきたいという趣旨は理解。ただ、実際を考えてみると、事業法等で報告義務があるものは、ヒヤリの規模や状況が定義されており、不幸にしてその状況に達した場合には、何の疑いもなく、自動的に報告をしなければならないのに対して、事業法以外のいわゆるそれ未満の事象について情報を求めようとする場合には、線引きの問題が必ず生じる。難しいことを言うようだが、できるだけ現場が迷わずに情報を出せるよう、明確な線引きを望みたい。例えば、単純なスパムメールがきたとき、これをヒヤリハットとして報告するのかという話になる。そこにはある程度案配があるのだが、その案配をできるだけ明確な線引きとして提示してほしい。そうすることで、実務上、判断のストレスが軽減できると考える。

更に言えば、報告のタイミングとコストの負担の問題がある。事業法で報告義務とされているものあるいは重大なものと言われているものについては、24時間365日発生の都度、報告しなければならない。他方、ヒヤリハットは件数も多く、それを一件一件集めるのは、非常にコストがかかる。これも都度報告にするのか、例えば月まとめとするのか。このような実務的なオペレーションについては、今後、矢印をつくり設計する上では、必ず検討しなければならない事項になると思う。

加えて、ヒヤリハットの概念も、もうちょっと冷静になって考えた方がよい。JPCERTは、制御システムも何年か対応しているので、ＩＴと制御の両方を見ているという観点から話をするが、ここで示しているヒヤリハットは、ＩＴ障害の中で脅威度の低いものを知りたいというイメージになっていると感じている。資料４　P5の図に５段階のレベルが表現されているが、レベル４、５は当然の報告対象であり、それをレベル３若しくは２程度まで報告してほしいというイメージなのではないかと想像

する。しかしながら、保安設計の概念で言えば、ヒヤリハットは、放置すれば保安事故や生産設備を阻害するなどの事象につながってしまう、その事前兆候だと理解されていると思っている。そうであるならば、例えば、生産設備がマルウェアに感染して拡がったとしても、重大な保安事故につながらなければ、報告対象にしなくてもよいという発想もある。そのようなものも含めて求めているのか、というのが論点。マルウェアが制御システムのネットワークに蔓延したが、安全に動いているという状態のとき、報告が義務となるのか。このような事項は、関係者間で少し認識がずれるところがあるので、ヒヤリハットについて、ＩＴからの目線と保安の大きいところからの目線に関し､慎重に擦り合わせをしなければ難しい問題が生じるのではないかと思う。

JPCERTは、NISCとのパートナーシップも締結し、情報セキュリティ関係機関としても位置付けられ、セプターカウンシルの事務局支援も務めさせていただいている。今後、上向き矢印の在り方を検討する中で、多少なりとも貢献をしなければならないと感じている。2008年以来の課題であり、解決できると明言することはなかなか難しいが、先ほど稲垣委員が政府も決意を示すべきと発言されていたことも踏まえ、NISCとともに知恵を出していければと思う。

○渡辺会長　決意表明と今後取り組むに当たっての論点を提示していただいた。これらは、ガイドライン作成など、今後の具体的な検討の中で反映していくことになろうと考える。

○柳島参事官（事務局）　JPCERTからの今後とも一緒に取り組んでいただけるという強い決意表明に大変感謝。

実際の運用に当たり、どのような方法で取り組んでいくべきかについては、矢印ごとに、それぞれの関係者と相談させていただくこととしたい。

公務員が情報保全を確実に行うことは当然であり、罰則も厳しいものが待っているということではあるが、これを主張し過ぎると反発もあろうかとの思いもある。理解を得ることの必要性は感じているところ。

ヒヤリハット情報については、例えば、件数だけで報告という方法もあろうかと思う。どのようなレベルまでをヒヤリハットとして報告するのかについては、NISC内でも議論を行っているところ。例えば、ヒヤリハットのレベル感を決めてしまうと、決めたことによって、それ以下のものが全く出てこなくなる可能性もあり、第３次行動計画では、あえてそこを決めず、事業者が出すべきと判断したものを出してほしい、という方法とした。

実際の運用上、マルウェア付きのメールがきたとの報告を受けることもあるが、その際、我々は、対応が十分であるかを確認する。その結果、対応が不十分、つまり、事業者はヒヤリハットだと思っていたものが、そうではないと判明するケースもあることから、JPCERTも含め、我々に限らず、なるべく幅広に、相談してほしいと考えている。正に気づいていなかった点に気づくことができるのではないかという思いも

あり、幅広の対応をしているところ。一方、明確化した方が取り組みやすい部分もあることは理解している。すぐに結論が出せる話ではないことから、この点に関しても、引き続き、相談させていただきたいので、よろしくお願いする。

○阿部委員　情報共有体制に関して２点お願いしたい。

今回、セキュリティの事象を含め、初動として、NISCや所管省庁と速やかに情報を共有する体制になるということで、これに対しては、我々も努力していかなければならないと認識しているところ。機能保証の部分でも話題となったが、我々電気事業者には、電気を安定的に届けるというミッションがある。一方で、例えば大規模停電に至るような事象が発生した際には、原因がサイバーなのかを瞬時に判断できない場合もあると認識している。初動として速やかな情報共有を行うことは、非常に重要であると認識しているが、その後の復旧に至る過程におけるNISCや所轄省庁との連絡体制とその運用については、少し慎重な検討をお願いする。その検討には我々が入ることもよいと思う。

今回の取組を行うことにより、NISCにはヒヤリハット情報を含め、定期的にさまざまな情報が集まることになると思う。P8「防護基盤の強化」の部分でも触れられているとおり、我々電気事業者は、セプターにおける取組に限らず、国際的な枠組みまで連携を拡めていく認識であり、電力ISACの設立などの検討も含め、関係機関の協力を得て取り組んでいきたいと考えている。国際的な連携において、相手との信頼関係を構築していく時間も必要となることから、国で行っている国際的な連携の中で共有された海外の情報などについても、我々にフィードバックしていただけるようお願いしたい。

○柳島参事官（事務局）　どちらも検討していきたい。

○大林委員　３点コメントしたい。

１点目は、「安全で持続的な重要インフラサービスの提供」について。今回、「安全で」という用語を加えた点は、今後、インフラの安全管理の部分においても情報システムに依存することが増えていくであろうことを踏まえれば、良い方向だと思う。

２点目は、P21に記載がある「事業継続計画」（ＢＣＰ）と「コンティンジェンシープラン」について。これも非常に重要であると思う。その下の定義も良く書かれている。コンティンジェンシープランは、具体的な出来事に対して具体的にどのようなアクションを起こすのか、ということの事前のプランニングという性質がある。これに対し、ＢＣＰは、理想的な考え方としては、あらゆるリスクに対しサービスレベルを維持するということになる。日本企業の場合は、どちらかというと、ＢＣＰを、そのような理想形があったとしても、例えば首都直下地震でマグニチュード幾つのものが起きて、というかなり具体的な想定をつくり、それにこだわってしまう傾向があり、ある意味、大規模コンティンジェンシープラン的なＢＣＰをつくってしまっている事業者が結構多い。そういう意味では、ここで示している機能保証を実現させるための

取組というものに限りなく近いのはＢＣＰであろうと思う。このような状況を踏まえれば、改めて、望んでほしいものはこういうものであると示しながら、コンティンジェンシープランを対照的に示すことで、むしろ、機能保証という考え方をもっと突き詰めていってください、その手法としてＢＣＰがある、というＰＲの仕方も効果的なのではないかと思う。行動計画案の文章自体を修正する必要があるかはわからないが、そのような趣旨のことをつけ加えると効果があるのではないかと思う。

３点目は、先ほど、有村委員からも発言があったヒヤリハットの情報共有について。必ずしも被害の大小でヒヤリハットを提示するか否かを判断するのではなく、それ以外の定義の仕方もあるのだと思う。最終的な被害という結果が出る手前の段階で、非常に危険な状況が存在する。危険な状況であったが悪条件が重ならず被害が発生しなかったというものにも、実はヒヤリハットとして共有すべきものがあるのではないか。例えば、ゼロデイを発見したとしても悪用される前は被害が発生しないが、事業者がゼロデイを発見したのであれば、それは重要インフラの中で共有した方がよいと思う。例えば、セキュリティに穴が開いてしまい、侵入された形跡もサービスに影響が出た形跡もないとしても、このような経緯でセキュリティの穴が一定期間開いてしまったという事例があれば、そのようなものがヒヤリハットで共有すべき典型的な例だと思う。そのようなものがカバーされるよう、ヒヤリハットの定義の仕方を考えてほしい。

○渡辺会長　３点目については、予兆的な、何かが起こったがヒヤリハットしなかったもの、イベントとして損失が出た出ない、あるいは焦った焦らなかったということを除外して、その事象を報告してもらえなければ、予兆として捉えることができないという意見だと理解。そこにどうやってインセンティブ若しくはモチベーションを付与するかということも重要だと思う。

○柳島参事官（事務局）　指摘について理解。

○稲垣委員　先ほど、資料３　P27　Ⅳ　1.(2)　⑤　について、「・・・仕組みの検討」ではなく、「構築」という言うべきだと申し上げたが、「構築」だけでなく、「構築・資源の提供」などとするべきだと思う。内閣官房としても、調整機関としての役割を果たすため、さまざまなところに協力を求めなければならない。内閣全体でこのようなことが必要であることをしっかりと認識し、成長戦略の中に位置付ける。それが、強い日本、スマートな日本、役に立つ日本、ということにつながる。日本の企業、重要インフラが世界の中で役に立っていくというところに位置付けることが、本当に必要だと感じている。

案文には、「情報共有体制」という言葉はあるが、よく読んでみると、情報の流れは政府でつくったが、体制の構築や維持に責任を持つのは事業者という構造になっている。「構築」というところまでいけていない。NISCはもともと金がない。所管省庁もやらされている感がある。しかしながら、金や資源を集める、国として責任を持って集めること、配分をすることが必要。所管省庁も、その施策として取り組むのであれ

ば、その分の予算を確保することが必要。そうすることにより、国として体制づくりに責任を持つ。しかし、情報共有については、事業統制とは違って事象に対して行うので、責任とは切り離すという切り分けをして、取り組みやすい情報共有を行うと同時に責任を持つ、ということを宣言すべきだと思う。今回は記載していないが、書けるようであれば、時期についても書いてほしい。「構築」だけでなく「構築及び必要な資源の確保」と表現してほしい。

重要インフラ所管省庁の施策として記載されている、資料３ P29 Ⅳ 2.(2) ① も同様。ここでは「情報共有体制の運用」となっている。どこかが責任を持ってつくったもの、あるいはできてしまったものを運用することについて、所管省庁は頑張るという記載になっていると感じる。所管省庁としても、体制整備に責任を持つ、必要な資源を提供する、という宣言をしなければ協力は得られない。そのように宣言することによって初めて、経営層の責任として、「情報セキュリティ対策は経営層の責任である」ということが書けるのではないか。そうなれば、場合によっては、そこに「情報共有体制の構築」というものも書き込めるかもしれない。金のことを言葉にしたくないことも理解できなくはないが、「体制構築に責任を持つ」ということは宣言していただきたいと強くお願いする。

○渡辺会長　「検討」から一歩進んだ「構築」のみならず、その先の運用に関する「資源の確保」までコミットすべきだという意見と理解。今の段階では難しい点もあろうかと思うが、基本的な路線としては、そのように書き込んでいかなければ、行動計画としての我が国の対外的な意思表明のトーンが見えてこないということだと思う。

○栁島参事官（事務局）　応援を頂いたと感じている。現在進めている情報共有システムについては、まずオリパラのために整備し、終了後には、それをレガシーとして重要インフラ事業者に活用することを意図して構築を進めており、そのための予算を確保しているところ。これについては、オリパラ後も継続的に活用することになるので、予算を含め、これをどのように構築し運営していくための資源確保が必要だという点は、指摘のとおり。この部分については、どのように積極的な表現とすることができるのかについて調整したい。

○手塚委員　機能保証とサービス維持のレベルの考え方について高く評価。今後、詰めていかなければならない事項もあると思うが、資料３ P44 に記載しているように、深刻度判断基準としてレベル１からレベル５に分けて１つの基軸を設けており、このようなものをＫＰＩ的に提示することが非常に大事だと思う。

この中で、機能保証のための情報共有の対象は、資料３ P43 に記載しているように、ヒヤリハットレベルのもの、その中間的なもの、サービスの安全かつ持続的な提供への支障という、大きく３つの層となる。単に、サービス継続の可否や支障の有無というゼロイチの考え方でのレベル分けであると、そのサービスが今どのような状態かということがよくわからない。その意味で、大きく３つに分け、更に判断基準とし

ての深刻度を５つに分けた点を評価したい。これを更に具体化するため、どのようなデータがどのようにそれぞれに該当するのかについて、ぜひ共有してほしい。これを分野横断的に重要インフラとして定義できれば、さまざまな分野で共通的に活用でき、正に横串で見ることができる環境になると思うので、この考え方を更に推し進めていただきたい。

○柳島参事官（事務局）　委員指摘のとおり、重要インフラに限らず、具体的なレベル感も含めて、どのような形で活用することが適切かについて、今後、検討を進めていきたい。

○平田委員　これまでの議論も踏まえ、情報共有におけるヒヤリハット等のレベル感について。情報を上げる側として一番悩むことは、これを上げてよいかどうかという判断であるので、先ほど発言があったとおり、どこまで広くとるかというバランスを見ながら決めていただきたい。若しくは、具体的な事例を提示していただければ判断材料として有効であるので、検討願いたい。また、資料３ P44の深刻度のレベルについても、それぞれの分野で重大な障害についてそれぞれの定義があるので、それらを活用しつつ決めていただければありがたい。

次に、資料３ P6に記載された「重要インフラ事業者等における先導的取組」というキーワードについて。資料を読み進めると、その事例のようなものが散見されるが、「先導的取組」とは何か、ということがクリアに書かれていないと感じる。これをもっとクリアにした方がよい。「先導的取組」は、時期に応じて変わるものだと思うが、マイルストーンを踏まえながらクリアにしていくことが必要なのではないか。

○渡辺会長　「先導的取組」については、何か具体的な記述が必要ということでしょうか。

○平田委員　どのようなものを先導的と捉えるかについて、コンセンサスをとるプロセスがあればよいと思う。

○柳島参事官（事務局）　これについては、委員指摘のとおり、時代によって変わるものでもあり、我々としては、先導的取組とはこれだと具体的に示すことで、それ以上の努力を阻害するという悪影響もあるのではないかと考え、トートロジー的な部分もあるが、あえて、「先導的に取り組んでいる事業者が行っていることが先導的」と捉え、具体的には記載しないこととしたもの。前回の骨子の段階では、例えば、ISACの取組を行っている、リスクマネジメントにしっかりと取り組み対処態勢を整えている、なども、ある種、先導的取組だと説明はしてきたところであるが、前述の理由もあり、この中で具体的な事例をあげることは控えたというのが現状。

○平田委員　本文の修正というよりは、コンセンサスを得る場を設けつつ進めていただければよいと思う。

○増子委員　放送分野も制御系であるので、今回、制御系について強調されたことは、当方の経営陣に対してもインパクトのある内容であると感じており感謝。

資料３ P26「人材育成」について。我々としても制御系が重要だとの認識に基づいて継続的に取り組んでいるところであるが、特に大手に関しては、制御系のセキュリティ人材は、ＩＴと比べて更に少なく、極端に言えば、ほとんどないに近い。ベンダーでも同様の状況が続いていると感じる。日本においては、ＯＴ、特に電力や空調などを含め、人材について同様の状況であるということを痛感しながらも、今、手探りで一生懸命に取り組んでいる状況。ここに記載されているとおり、国を含めてさまざまなレベルでの人材育成や支援などを、是非ともお願いしたい。

次に、資料４ P3「重要インフラ事業者等の経営層の在り方」について確認したい。当方の経営層に説明すると考えたとき、この部分の表現はわかりにくいと感じた。３番目の項目の後半に「インシデント発生時の対応に関する情報の開示」とあるが、これは具体的に何を意味しているのか教えていただきたい。

○柳島参事官（事務局） 重要インフラで言えば、これまで直接的にサービスに影響があるインシデントは発生していない。しかしながら、仮にシステムに侵入されウェブを書き変えられたとしても、それだけであれば大したことではないが、システムに侵入されたこと自体は、その先が更にあり得る。サービスへの影響につながりかねない。例えば、そのような事案については、早期に公表して対策をとっていることを周知するということが考えられる。

○増子委員 対策をとっていることを発表するということか。

○柳島参事官（事務局） 事案が起こっているということだけではなく、それにしっかりと対策しているということがなければ、情報が漏れ続けているということだけを伝えることとなり、世の中に不安を与えることにしかならない。しっかりと対応しているということを伝えることは、当然必要だと思う。

○増子委員 理解。

○大平委員 資料３ P49 別紙１・P53 別紙２について。クレジット分野の部分において、「クレジットカード決済システム」という表現があるが、現在、我々クレジットセプターでは、「オーソリゼーション」という用語を使っている。クレジットカードの利用について、有効・無効を瞬時に判断するシステム。「オーソリゼーション」という言葉・範囲がわかりにくいということは認識しており、今後、所管省庁とも相談しながら改定を検討しているところではあるが、現時点では、「オーソリゼーション」で記載願いたい。

○渡辺会長 実態に合わせて修正をお願いする。

(4) その他

○渡辺会長 本日の議論はここまでとするが、その他、コメント等があれば、12月22日までに事務局へお願いしたい。本日の議論及び追加のコメントを踏まえ、事務局と相談しながら、修正を加えさせていただくこととするが、最終的な取りまとめについて

は、私に一任いただきたい。

○一同　異議なし。

○渡辺会長　冒頭の説明のとおり、取りまとめられた「重要インフラの情報セキュリティ対策に係る第４次行動計画」は、パブリックコメントの手続を踏み、世の中から幅広く意見を求めることとしたい。

○柳島参事官（事務局）　今後の予定について。本日の議事概要については、事務局にて作成後、委員の皆様に確認いただいた上、公表させていただく。

本件、行動計画の見直しについては、本年度末をめどに結論を得ることとしていることから、年明けに開催される予定の戦略本部において、パブリックコメント案として決定いただき、パブコメを踏まえた上で、次回の専門調査会で最終案について了解を頂きたいと考えている。次回の専門調査会の時期としては、３月頃と考えており、現在のところ、3月16日の午前を候補としているが、決まり次第、連絡させていただく。

(5) 閉会

○渡辺会長　これにて、第９回「重要インフラ専門調査会」を閉会する。

以　上