平成 30 年 3 月 20 日

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 14 回会合　議事概要

１　日時

平成 30 年 3 月 20 日（火）13 時 00 分～15 時 00 分

２　場所

中央合同庁舎第４号館 11 階　共用第一特別会議室

３　出席者（五十音順・敬称略）

阿部　克之	(電気事業連合会　情報通信部長)
有村　浩一	(一般社団法人ＪＰＣＥＲＴコーディネーションセンター　常務理事)
安藤伊佐武	(第一生命保険株式会社　ITビジネスプロセス企画部部長)
稲垣　隆一	(稲垣隆一法律事務所　弁護士)
大高　利夫	(神奈川県藤沢市　総務部参事兼ＩＴ推進課長)
大林　厚臣	(慶應義塾大学　大学院経営管理研究科　教授)
荻島　　敦	(日本通運株式会社　ＩＴ推進部　専任部長)
金子　　功	(一般社団法人日本ガス協会　技術部長)
佐藤　　勲	(東日本旅客鉄道株式会社　総合企画本部 システム企画部次長)
鈴木　栄一	(一般社団法人日本損害保険協会　ＩＴ推進部長)
鈴木　　悟	(株式会社三井住友銀行　システム統括部システムリスク統括室　サイバーセキュリティ管理グループ　グループ長　)
手塚　　悟	(慶應義塾大学　大学院政策・メディア研究科　特任教授)
野口　和彦	(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　センター長兼大学院　環境情報研究院　教授)
橋本伊知郎	(野村ホールディングス株式会社　参事　Co-CIO 兼　野村證券株式会社　経営役　業務企画、IT基盤、国内IT担当)
原田　　充	(日本航空株式会社　IT運営企画部　セキュリティ戦略グループマネジャー)
平田　真一	(日本電信電話株式会社　技術企画部門　セキュリティ戦略担当部長)
細川　　猛	(石油化学工業協会　総務部兼業務部　次長)
堀内　浩規	(一般社団法人日本ケーブルテレビ連盟　通信制度部長)
増子　明洋	(日本放送協会　情報システム局　ＩＴ企画部長)
松田　栄之	(ＮＴＴデータ先端技術株式会社 セキュリティ事業部 エグゼクティブコンサルタント)
渡辺　研司	(名古屋工業大学　大学院工学研究科　社会工学専攻　教授)

渡辺　　睦　　（石油連盟　総務部総務グループ長）

（「重要インフラ専門調査会の設置について（平成 27 年２月 10 日サイバーセキュリティ戦略本部決定）」４．による出席）

中島　一郎　（早稲田大学研究戦略センター）
（重要インフラサービス障害に係る対処態勢検討ＷＧ主査）

（事務局）

中島　明彦　内閣サイバーセキュリティセンター長
桑原振一郎　内閣審議官
三角　育生　内閣審議官
雲田　陽一　内閣企画官
越後　和徳　内閣参事官
林　　泰三　内閣参事官
瓜生　和久　内閣参事官

（オブザーバー）

金融庁総務企画局政策課サイバーセキュリティ対策企画調整室
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・生活衛生局水道課
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サイバーセキュリティ対策室
原子力規制庁長官官房放射線防護グループ核セキュリティ部門
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
内閣官房内閣参事官

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　本日は、お足元の悪いところ、また、年度末のお忙しいところ、お集まりいただきまして、ありがとうございます。

あらためて申し上げるまでもないことでありますけれども、ネット利用のスピードが指数関数的に増えています。新たなサービスモデルを考える場合、それから、例えばコスト管理をやる場合にも、ネットの利用というのは、当然の前提として、お考えになっていると思いますし、ましてや一般の消費者の方にとってのインターフェースが、ダイレクトにネットとつながっているということになりますと、どうしてもリスク・脅威を考えざるを得ません。

その中で、脅威というのは、普通、標的型攻撃を考える際には、攻撃に対する防御という何となく攻撃している人を頭に置くようなイメージがあるのですけれども、今、私どもが考えているモデルといいますか、新しいものはそうではなくて、いろんなところに悪意を持った、高度というか、濃度というか、そういうものがある環境の中でやっていることを、よくこの中で議論しています。散発的な攻撃が来るだけではなくて、常にそこに攻撃のリスクがあるのだろうということが、これからの前提になってくるのかと思っています。

そういたしますと、モデルを考える際、それから、実際にオペレーションをやっている際、どうしても定期的な頭のリフレッシュ、セキュリティのマインドセットを持っていなければいけませんし、定期的な教育訓練こういうものを通じて、意識を継続的に高めていくことが重要になるのだろうと思っています。そういう意味で、ここの調査会に御参加いただいている各センターの方々、また、お越しいただいていおります、有識者の先生方の御意見は、非常に貴重なものなのだろうと思います。

また、2020年の東京オリンピック・パラリンピックを目標に、とりあえずここでということよりは、どちらかというと、初めて全体的なリスクのつながりといいますか、そういうことを往々確かめながら、対策を打っていくことをやるのだと思っています。

そういたしますと、ある種、社会全体を最後の観点から見たシステミックなアプローチというのが、必要になると思っております。こういう対策をとる際というのは、政府機関も、要するにそういうシステムの一要素であるわけで、いろんなサービスを提供している方々、また、国民の方々、関係主体間の共通理解を得ながら、進めていく必要があると思っております。

本日の専門調査会は、年度末ということで、多くの報告事項がございますけれども、そのほかに、中心的なことといたしまして、パブリックコメントの御意見を踏まえました安全基準等策定指針、これに加えまして、重要インフラサービス障害の深刻度評価基準について、御議論をいただきたいと考えております。

深刻度評価基準は、いろいろ御議論、御示唆をいただきまして、関係主体の共通理解を得ながら、発生した事案への冷静で適切な対応の促進に利用されることを目標としているものでございます。本日、委員の皆様方に策定の御趣旨を御理解いただきまして、闊達な御議論をお願いしたいと考えております。

渡辺会長から挨拶。

〇渡辺会長　本日は、お忙しい中、御参集いただきまして、ありがとうございます。今、中島センター長からありましたとおり、本日、この資料の分厚さが語っていて、たくさんございますが、報告事項に加え、討議事項が２つでございます。

前回、12月になりますけれども、専門調査会におきまして、皆様方にお認めいただきました、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」の改定案は、パブリックコメントを経まして、コメントをいただいております。それに基づきました変更の案が挙がっておりますので、後ほど事務局から御説明いただいて、御確認、御議論いただいた上で、本日は、了承まで進めてまいりたいと思いますので、御協力をお願いいたします。その後、次回のサイバーセキュリティ戦略本部において、正式決定をするという予定になっております。

それから、もう一つ、センター長から御説明がございましたとおり、第４次行動計画における取り組みの１つとしまして、深刻度評価基準の具体化に向けて、専門調査会に設置しておりますWG、この検討結果が御報告された後に、御議論をいただきまして、先ほど申し上げました戦略本部に報告されて、その後に、パブリックコメントにかかるという予定でございますので、そのパブリックコメントにかかることについての了承を得るというのが、本日でございます。

報告事項につきましては、2017年度の重要インフラグループの取り組みに加えて、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NISCのリスクアセスメントの取り組みについても、あわせて御報告をいたします。それでは、限られた時間でございますが、委員の皆様におかれましては、ぜひとも闊達な御議論をお願いいたします。

なお、本日は、先ほど申し上げました、重要インフラサービス障害に係る対処態勢検討WGの中島主査に来ていただいております。「重要インフラ専門調査会の設置について」の第４項、「専門調査会の会長は、必要があると認めるときは、当該専門調査会の委員以外の者に対し、当該専門調査会の会議に出席して、意見を求めることができる」とございますので、この条項に基づきまして、私が会長として、お呼びしているものでございます。中島主査、本日は、よろしくお願いいたします。

それでは、早速、本日の議事に入らせていただきます。

⑵ 報告事項

内閣サイバーセキュリティセンターオリパラチームより資料２について報告。質疑応答は次のとおり。

〇野口委員　質問が１件と、意見が１件あるのですけれども、質問に関しては、先ほどの５頁のところなのですが、今までリスクアセスメントに留まっていたものを対策までやりますという話と、PDCAをしっかり回すという話は、どういう関係なのでしょうかというのが質問です。

意見は、サイバーセキュリティの場合は、リスクの顕在化シナリオが多様化する、新しいものが出てくるというか、対応すべきものが一定ではなくて、どんどん増えてくる傾向になるのです。そういう状況のときに、１年前に対応したものが、こういうスピード感で本当にいけるのか。従来のリスクを見つけて、１年かけてゆっくり考えてという考え方だと、サイバーセキュリティは追いつかないのではないかと思うのですけれども、この辺のお考えはいかがでしょうか。

○雲田企画官　リスクに関しては、変わっていくという認識はまさに持っておりまして、今回、第２回目ということなのですけれども、オリンピックまでに合計６回予定しているところです。その考え方は、リスクがどんどん変わっていくということで、要は一度、設定したリスクというのは、永遠にレベル感も含めて、不変のものではないと考えておりまして、それで、定期的に見直しをしていきます。

一方で、リスクの見直しをやっていく上で、事業者さんでリスクの見直しを全てゼロから考えてくださいというのは、非常に難しいのです。今、いろいろ個票を見てきても、事業者さんで、リスクの捉え方、粒度も含めて、かなりバラツキ感があるので、そこを埋めていく上で、今後、横断的リスク評価の中で明らかになってきたものを、リスク管理簿という形で、御提供していきます。それは、一度作ったら、作り放しというものではなくて更新をしていくという形で、事業者さんのリスクアセスメントを支援していくことを考えております。

○野口委員　アセスメントを支援するということと、アセスメントをした結果の対策の推進を支援することは、別だと理解しており、そこのギャップはどうなっているのか。

○雲田企画官　御案内のとおり、結局、最終的にはリスクに対して、対策を実施していただくというのは、事業者さんの役割と考えておりますので、そのリスクアセスメントの推進、要は的確なリスクアセスメントによって、現在やっている対策の不備等に気づきを与えることができるのではないかという形で、支援を行っていきたい。対策そのものを見ていくというよりは、きちんとしたリスク評価ができているかどうかを、こちらでも情報を提供して、支援していくことを考えております。

○渡辺会長　いろいろあろうかと思いますけれども、個別に回答させていただくことと、正解のないトライアルの世界でありますので、引き続き、皆様方から御意見をいただくような形で、先に進めさせていただければと思います。ありがとうございました。

事務局より資料３から資料９について報告。質疑応答は次のとおり。

○稲垣委員　非常に多くの課題、それから、多くの方々に対して、支援活動を徹底したというか、具体的に行っていることがどんどん進んでいるという状況で、喜ばしいと思います。また、関係者の御努力は、大変なことだと思いますし、演習などに参加する事業者の意識も非常に高まってきて、いい方向に進んでいるということで、喜ばしいと思います。

ただ、冒頭のオリパラの報告、全体の流れを見たときに、NISCとしての権限、事業者と

の関係については、こうした面の活動はどうだったのかということについても、教えてもらうなり、きちっと総括して、補強していったらどうかと思うわけであります。

それは、具体的にどういうことかというと、民間について、NISCとの関係では、NISCは支援活動を行い、いろいろな情報提供や機会、省庁を通じての予算措置もやっていると思うのですが、北風と太陽だとすると、太陽の面とか、愛と剣（つるぎ）というか、そういう面でいくと、愛の面だと思うのですけれども、もう一つは、叱咤激励するという教育の面にもあると思うのです。

その場合に、例えばNISC自体は、各事業者に対する事業法の執行権限はないわけですが、主務省と連携して、主務省がその権限を発動するかどうかの検討とか、そうした連携、それから、権限の発動の前に、一般行政法に基づく指導とか、連係など、いろいろな行政法上の手段があると思うのですけれども、こうした権限を十分に行使しているのだろうか、これについての点検も、NISCと各省庁でやっていくべきではないかと思うのです。

例えばいろいろな企画、制度を供給して、指針などもこれから検討して出ていくわけですけれども、その結果、オリパラの2020年を前に、３年前の段階でリスクアセスメントを、NISCの考えたものですから、一定の評価というか、社会的な信頼性のあるものを提供したところ、実際にふたを開けてみると、使ってもらえていないとか、いろいろな事情で、前に進めていません。通常の事業者であればいいのですけれども、重要インフラを対象にしたときに、重要インフラについては、事業法に基づく監督権限の発動が背後にあって、その間に軟らかい指導などがあって、事業が行われているわけです。

だから、条文を見ても、主務省庁も、国民に対して、監督権限の発動というのは、責任を持って行うべき立場にいるはずなのです。本当にその権限を適切に行使するための様々な基準とか、あるいはそうした準備をしているのだろうか。

その辺がNISCと国の機関との関係の安全基準とか、取り組みは、それぞれ進んでいると思うのですけれども、官民が連携してやるといったときに、厳しいかもしれないのですが、基準、その他を十分に使えるかどうかは別として、きちっとやっていないところに対しては、きちっとした監督権限とか、指導をしていく必要があると思うのだけれども、そこのところで抜けているとすると、最適化が図れないと思います。その辺は、NISCとしても、各省庁の挙動とか、権限行使、指導状況を把握して、それが十分に行われるような支援策をきちっと講じていくということが必要だと思うので、その辺もぜひ見ていただきたい。

もう一点、先ほどのオリパラの報告にもありましたけれども、民間、あるいはその後の状況についての報告がありましたが、中小企業ができないでいて、成長戦略もあるし、サイバーセキュリティ問題を産業政策としてやっていく側面もあるわけですが、何においても、一番にそうしたところができるような施策を講じていく、支援も「何をやれ」という面の「こういうことをやるといい」という支援もあるけれども、できるようにしてあげるということで、例えば金の問題とか、税の問題、情報の問題で、情報提供はやっていると思うのですが、予算とか、金の使い方が本当に最適化されているかというのは、NISCも関心を持って、各

省庁のサイバーセキュリティに関する最適化ができているのかどうか。その辺は、お金の使い方もそれなりに考えてやっていると思うのですけれども、現実に必要なところに、必要なお金がわたって、結果を生んでくることがきちっとモニタリングされていくことを、NISCとしても、テーマとしてやるべきではないかと思うわけです。今の報告を聞いていると、その面が少し薄いというか、あえてそこについての御報告のテーマではなかったかもしれません。実際にやっておられると思うので、その辺もきちっと御報告いただけると、大変心強いと思うわけです。

○渡辺会長　ありがとうございます。

１点目は、いわゆる自発的なことに対する支援をすること、それから、そうではない部分について、ある意味強制力を効かせてやっていただく部分と、この使い分けについてのモニタリングとか、評価はどうなるかという話です。

２点目は、実際にやることに対して、そのお金であったり、税であったりとか、そういった支援で、具体的な経済的な支援も含めて、そのあたりが妥当に行われているか、あるいはその効果はどうかというところで、このあたりのNISCとしてのモニタリング、あるいは考え方についての御質問だと思いますけれども、どなたかありますでしょうか。

お願いします。

○越後参事官　委員の御指摘の件につきましては、各省庁が、どのような対応をしているのか把握する仕組み、さらには、取組みを促進していく仕組みから考えていかなければなものと思っております。

また、オリパラに関しましても、御指摘がありましたけれども、オリパラの部分につきましては、重要インフラ事業者だけではないところもありましたが、御指摘を踏まえまして、できるだけ取り組めるよう、頑張っていきたいと思っております。

○稲垣委員　オリパラについては報告があったので、議論の例として挙げただけで、基本的には、ここのテーマの対象事業者ということでございます。

○渡辺会長　そのほか、いかがでしょうか。よろしゅうございますか。

報告事項ということですので、また何かございましたら、最後に時間がありましたら、お伺いしますけれども、一応一連の報告事項は、これで了解したということにさせていただきたいと思います。ありがとうございました。

国土交通省より資料 10 について報告。質疑応答は次のとおり。

○渡辺会長　ありがとうございました。この件に関しまして、NISCから、補足等はございますでしょうか。

○林参事官　それでは、私、参事官の林からコメントをさせていただきます。

先ほど国土交通省さんから御報告がございましたけれども、昨年の12月20日、ちょうど３カ月前の専門調査会において、空港の重要インフラ化に関する方針の表明をしていただ

きまして、予定どおり、４月１日から取り組みを開始していただけるということで、NISCとしても、大変良い措置だと受けとめをしております。

御案内のとおり、今後、2020年の東京オリンピック・パラリンピック競技大会、その前にも、2019年には、ラグビーのワールドカップですとか、あるいはG20のサミット、こういった国際関係の重要イベントが予定されている状況でございますので、国際的な拠点空港を対象に、この４月のオペレーションの開始に向けて、盤石な体制を整えていただきたいと考えております。

４月１日に実質的な取り組みを開始していただけることになりますと、この先、第４次行動計画の改定も視野に入ってまいりますが、改定につきましては、４月以降の運用の実態、実績、こういったものを十分にウオッチしながら、具体的なタイミングについては、十分に御相談しながら、調整していきたいと考えている次第でございます。

○渡辺会長　ありがとうございました。それでは、本件の報告事項は、了解したものとさせていただきます。

(3) 討議事項

事務局より、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）」（案）に対する意見募集の結果（資料 11-1～11-4）について報告。質疑応答は次のとおり。

○稲垣委員　パブコメにもたくさんの意見が寄せられて、しかも、その中で、取り上げられるものについては、どんどん取り上げて、修正を加えているという方針は、国民みんなでこれをつくっていくという、それを証拠としても取り上げられるし、非常に望ましい取り上げ方だったと思います。

中身については、読ませていただいたのですが、今の段階のさまざまな制度を取り上げて、よくここまでまとめたと思います。本当に今の最先端のところ、現実的なところを取り上げてきているという印象を受けました。特にセキュリティ・バイ・デザイン、要するに制御系、情報系を含めて、部材、企画、アセンブルの段階から、きちっとセキュリティ対策を講じていくというところについて、目が配られていることと、そこにシステム監査をきちっと位置づけた、PDCAのところですけれども、その辺も現実にシステム監査がそういう活動をしているところを踏まえた記述で、その分野の方は大変励まされると思います。

全体として、努力の結果が見られるもので、すばらしいものができたと思います。ぜひこれを周知徹底するほうに使われるように、努力していただければと思います。

以上です。

○渡辺会長　そのほか、いかがでしょうか。本会議でも相当な議論をした上で、しかも、パブリックコメントをかけた上でということですので、この版としては、これでよろしいのではないかと思います。１つだけ、資料11-1の下のほうに、指針の修正対象外というものが、

幾つか※でございますけれども、この扱いについて、少し御説明いただけますでしょうか。例えば内部犯行の可能性の考慮などがございます。

○瓜生参事官　それとあわせまして、説明不足のところがありましたので、追加します。

パブコメの中で、２つほど、内部犯行の可能性の考慮という４番の話と、あと、経営ガイドラインの内容との統一化というものがありまして、要するにほかのガイドラインがあるものと、どこまで記載を統一化するかということを悩みまして、特に内部犯行につきましては、今のガイドラインの中にも、ログをちゃんととるとか、１人で作業をせずに、２人以上で作業させるとか、ある程度、内部犯行に資するものを書いてはいるのですけれども、さらにそれに追加して、組織風土とか、コミュニケーションとか、いくところまでいってしまうと、クリアランスなど、サイバーではないところまで踏み込んでいることが別途ありますので、そことどこまで合わせるかというところで考えた結果、本当の内部犯行については、別途、IPAから出されているガイドラインもありますので、そちらも参照していただいて、活用いただく形で、特に指針については、内部犯行の部分をさらに強調して書く形はとっていないと、整理させていただいております。

同じように、サイバーセキュリティ経営ガイドライン、経産省が出しているものがございます。これはトップの社長ですとか、経営層の方々に向けた特別なガイドラインでございますので、詳細に全部を取り込んで統一するというよりは、そちらにつきましては、経営ガイドラインもごらんになっていただきつつ、一方で、実施につきましては、経営層以下、現場の方にも使っていただくという位置づけもあるかと思っておりますので、全部を取り込むことはせずに、整理をしたという形にさせていただいています。

先ほど説明を省いてしまって恐縮ですが、資料11-4につきまして、説明をいたします。アセスメントの手引書がありまして、これにつきましては、前回、鉄道分野の方から、後ろの個表のところの例が、鉄道に特化しているものだという御指摘をいただきまして、それを修正させていただきました。具体的に言いますと、別紙３に、緑の字でいっぱい書いていますが、抽象的なシステムの書き方で書いておりますので、特に鉄道に特化しないような形で、修正を加えているところでございます。

以上でございます。

○佐藤委員　JR東日本の佐藤でございます。資料11-3の22頁を見ていたのですが、今、初めて気がついたのですが、別紙１で、対象となる重要インフラ事業消費者等と重要システム例ということで、記載がございますけれども、これは重要インフラ毎に、こういう事業者と重要システムが対象になるということだと思うのですが、これはあくまで例といいますか、そういうふうに捉えてよろしいですか。事業者によって、システムが重要インフラに該当する場合もあるし、そうでない場合もあるという捉え方でよろしいでしょうか。

よく見ると、例えば金融さんなどには「清算システム等」と「等」がついているのですけれども、航空とか、鉄道だと、比較的言い切っているというか、「等」がなくて、４つとか、３つだけなのですが、「等」があるとか、ないとか、特別な意味があるのかということです。

今、初めて気づいたものですから、コメントをいただければと思います。

○瓜生参事官　ありがとうございます。

この表につきましては、もともと第４次行動計画についている別紙１の表でございまして、作成に当たりましては、所管省庁様と業界の方と調整したものでございまして、その辺の並びがとれていないのは、非常に恐縮なのですが、「等」がつく、つかないは、各省庁さんの御判断なり、御意見で書いているものでございますし、御指摘のシステムにつきましても、あくまでも例ということで、書かせていただいているものでございます。

○佐藤委員　ありがとうございます。

○渡辺会長　そういう意味では、例と書いてありますのと、行間を読むまでのものではないということで、よろしいかと思います。

○松田委員　手引書のところなのですけれども、例えば20頁を見ていただくと、上から３行目に「残留リスク値」と書いてございます。用語集も「残留リスク値」なのですけれども、表は「残存リスク値」になっています。言葉が揺らいでいるので、もう一度、見ていただいたほうがいいと思います。

○渡辺会長　御指摘どうもありがとうございます。整合性を見ていただいて、特に用語につきましては、重要だと思いますので、もう一度、事務局に確認をしていただく。

そのほか、いかがでしょうか。よろしゅうございますか。それでは、特段、御意見がございませんでしたら、指針の第５版、手引書につきましては、本専門調査会におきまして、了承したいと思いますが、よろしゅうございますでしょうか。

○一同　（異議なし）

○渡辺会長　ありがとうございます。それでは、１点目の討議事項につきましては、了承いたしましたということで、事務局より、今後の手続につきまして、御説明をお願いいたします。

○瓜生参事官　冒頭、会長からも御発言がございましたけれども、資料11-3の「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」の第５版につきましては、次回行われます、サイバーセキュリティ戦略本部におきまして、正式に決定する予定でございます。

続きまして、資料11-4の「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」につきましては、クレジットにありますように、当専門調査会で決定することになりますので、ただいま御了承いただきましたことをもちまして、専門調査会の決定ということにさせていただきますが、先ほどおっしゃっていただいた用語のずれなどは、修正した上で、決定とさせていただければと思っておりますので、よろしくお願いいたします。

事務局及び中島主査より、サイバー攻撃による重要インフラサービス障害等の深刻度評価基準（試案）について（資料 12-1,12-2）について報告。質疑応答は次のとおり。

○手塚委員　こういう形でまとめていただいて、ありがたいと思っています。今まで基準がない中、とにかく基準を考えてみようという、そのところは非常に重要で、それをこういう形でまとめてきていただいたということは、今後、我が国のいろいろなところで問題が出たときに、それなりの値で、国民の皆さんに話すことができるということは、非常にいい方向性だと思いますので、これをさらに進めていっていただきたいと思います。

その中で１点、評価の観点で、サービスの持続性への影響、サービスに関する安全性への影響があって、その次は、私的には「サービスに対する信頼低下」という言葉を、この指標に持ってきてもいいのではないかと思ったのですが、ここをあえてその他にしたのは、どういう考え方でそういうふうにしたのか、そこだけお教えいただけますか。

○瓜生参事官　ありがとうございます。サービスの持続性と安全性というのは、この会で決定いただいております、第４次行動計画で新しく書いた機能保証の考え方を踏まえ、安全かつ持続的なサービスの提供というものがありまして、それをまず重点的に見るということで、持続性と安全性を大きな柱として書かせていただいております。一方で、何かしら不具合が起きた場合には、安全かつ持続的なサービスの提供以外にも、信頼低下や経済的な第二次波及効果のようなものなど、その他の検討すべき指標みたいなものが幾つかあるのではないかと考えております。この点に関するWGでの議論においては、現時点でそれらを評価の指標とすることは時期尚早であるなどの議論もあり、結果的に「信頼低下」だけが残ったということでございます。

我々としましては、信頼低下については、持続性と安全性に比べてやや小さめの、幾つかある中の指標の１つという形で整理させていただいているというのが、現状でございます。

○大林委員　段階的な取組となっており、今のところは、事後評価の基準として検討が進められていて、将来的には事前のものにも使えるようにということで、承知いたしました。

ただ、共通の認識を持って何かのアクションにつなげるという意味では、将来的には、事前でどれだけ意思の共通化が図られるかというところは、非常に効果が大きいと思いますので、まずはこの段階ということになるのですけれども、将来的にもう一つ、非常に大きな効果があろうというところで、次のステップも、特に大切に考えていただければと思います。現在のところの内容は、承知しました。

○稲垣委員　資料12-2ですけれども、パブコメに際して、深刻度基準がどのように利用されるか、あるいはどのように利用することを想定しているのかを、もう少し具体的に説明していただくと、パブコメをする側も、具体的な意見が述べられるのではないかと思います。区分けをして、みんなが共通認識を持てるようになるというだけだと、抽象的に過ぎると思うので、せっかくの御検討の結果ですので、たくさんのパブコメが得られるように、ターゲットを絞った御説明をもう少し補充していただけると、よろしいかと思います。

○渡辺会長　ありがとうございます。事務局、それでよろしゅうございますか。そこの書き

ぶりを加えていただくということです。その観点から、パブリックコメントにかけるには、この情報しか出ませんので、詳しい背景などは出ない中で、パブコメを出す側の立場として、この情報で、我々が望むパブリックコメントがちゃんと出るかどうかという観点から見ていただいて、いかがでしょうか。余り多くの資料を出すことにはならないのですけれども、これで必要十分であるかどうかということですが、いかがでしょうか。

○大林委員　もしこれを一般の方が読んだとして、ここに深刻度の段階があると、天気予報であれば、予報であるし、地震の発生確率であっても、事前のアセスメントの数字になるので、言葉で上手に説明しておかなければ、それと同じように、事前の評価として使うものを期待してしまう人が多いと思います。事前に使うという前提でのコメントがたくさん来てしまう気がします。よく読むと、ちゃんと書かれてはいるのですけれども、全く予備知識がなしの方が読まれたときには、事前評価に使うという誤解をされる方が多いだろうという気がしました。

○渡辺会長　ありがとうございます。そういう意味では、今の我々の取り組みの段階で、どういうことを聞きたいかという話と、今後、事前のところにもいくという、その辺の説明を一面に少し書くということですね。

○大林委員　書き方は、お任せします。

○渡辺会長　書きぶりを少し工夫するということだと思います。ありがとうございます。

そのほか、いかがでしょうか。特段無いようでしたら、全体も含めて、ここで御意見をいただければと思いますけれども、言い残したことなどはございますでしょうか。

お願いします。

○稲垣委員　安全基準等の策定指針については、これが戦略本部で確定されることを期待したいと思うのですが、確定した暁なのですが、先ほどの繰り返しなのですけれども、これまで我々というか、ここでの議論は、何を民間はなすべきか、あるいは国はなすべきかということで、いろいろななすべきことを検討し、その共通化に向けた基準づくりとか、基準をつくるための指針をつくるとか、そういう取り組みを進めてきたと思います。今回の第４次行動計画で、機能保証という概念ができて、これで事業法などによる規定ぶりとも整合がとれるようになったし、取り組む主体も経営まで巻き込んだものとすることができるようになったし、全体的な取り組みができるようになった段階だと思います。

今後なのですけれども、NISCにおいては、指針が確定された暁には、この指針が使われている状況、あるいはこれに基づく取り組み状況を、先ほどのオリパラのようにきちっと把握していただきたいと思います。

もう一つは、ともすると、これぐらいしかできていないという情報は上がってくるのですが、これしかできない理由が何なのかをきちっと把握してあげる取り組みは、少し弱いような気がします。それは各省庁に任されていると思うのですけれども、NISCでも、これが実現できないでいる理由が何かということも把握すると同時に、これを実現するために必要な要件とか、リソースが何かもきちっと把握して、社会全体でこれを実現できるような環境

づくりの政策も、ここで議論していく。それから、国全体のサイバーセキュリティ政策の整合性を図るための情報を上げていくというところにも、視点を向けていただけるとありがたいと思います。

それぞれの主務省が、それぞれのお考えで行動されていることを伺いますし、感じます。それはそれで１つずつ、大変に有意義なことだと思うのですが、全体としての最適化というか、国全体としての最適化に疑義を抱かざるを得ない場面も出てきたりもします。その辺も含めて、現実にこうしたことがきちっと行われるようにする環境づくりをどうするかという点についても、リサーチを重ねていって、施策をしていっていただけたらと思います。

〇渡辺会長　大変重要な御示唆をありがとうございます。ここまでの活発な御議論、ありがとうございました。まだ言い残しがあろうかと思います。本日はここまでとさせていただきますが、３月26日月曜日まで、事務局で受け付けておりますので、お伝えいただければと思います。

本日議論を行いました、深刻度評価基準（試案）につきましては、本日の議論を踏まえまして、事務局と相談させていただいて、必要な修正を行います。その上で、パブリックコメントの手続に入りますが、一連の手続に関しましては、私に御一任いただくということで、よろしゅうございますでしょうか。

〇一同　（異議なし）

〇渡辺会長　ありがとうございます。それでは、深刻度評価基準（試案）につきましては、いただきました幾つかのコメント、修正案につきまして、修正した上で、パブリックコメントの手続に入ることを次回の戦略本部に報告することといたします。ありがとうございました。

それでは、事務局から、今後の予定につきまして、御説明をお願いいたします。

〇越後参事官　今後の予定でございます。本日の議事概要につきましては、事務局にて案文を作成後、各委員の皆様方に御確認いただいた上で、確定する予定としておりますので、御了承いただければと思います。

次回の専門調査会は、６月頃を予定しておりますが、議事等を含め、別途、御連絡させていただきますので、よろしくお願いいたします。

(4) 閉会

〇渡辺会長　これにて、第14回「重要インフラ専門調査会」を閉会します。

以　上