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 15 回会合　議事概要

１　日時

平成 30 年 6 月 21 日（木）13 時 30 分～15 時 00 分

２　場所

中央合同庁舎第 4 号館 12 階　共用 1208 特別会議室

３　出席者（五十音順・敬称略）

（委員）

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
石川　広己	公益社団法人日本医師会　常任理事
稲垣　隆一	稲垣隆一法律事務所　弁護士
梅田　康吉	三菱UFJ銀行 システム本部 事務･システムリスク統括室 サイバーセキュリティ推進グループ次長
大高　利夫	神奈川県藤沢市　総務部担当部長兼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
大平　充洋	一般社団法人日本クレジット協会　業務企画部部長
荻島　　敦	日本通運株式会社　ＩＴ推進部　専任部長
小野　森彦	石油連盟　総務部長
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
田中　明良	日本放送協会　情報システム局　CSIRT部長
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
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
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
盛合　志帆	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　セキュリティ基盤研究室長
和田　昭弘	全日本空輸株式会社　業務プロセス改革室　企画推進部　情報セキュリティ・基盤戦略チームリーダー

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
和田　昌昭　　公益財団法人金融情報システムセンター　監査安全部長

（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
山内　智生　内閣参事官
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
総務省情報流通行政局サイバーセキュリティ課
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
文部科学省大臣官房政策課情報システム企画室

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、お忙しいところを御参集いただきまして、誠にありがとうございます。開会に当たりまして、一言御挨拶を申し上げたいと思います。

本日、報告事項として２項目ございます。１つは、平昌オリンピック・パラリンピック競技大会の状況、もう一つは、次期サイバーセキュリティ戦略についてであります。

サイバーセキュリティの取組を進めていく上で、東京オリンピック・パラリンピックは今後のマイルストーンイベントになるわけでございますけれども、その準備の一端といたしまして平昌オリンピック・パラリンピックの状況を情報収集してきたところでございますので、それを御報告させていただきます。

２つ目が次期サイバーセキュリティ戦略ですが、去る６月７日にサイバーセキュリティ戦略本部を開催いたしまして、その中でパブリックコメント案を決定したところであります。

今回の戦略では、サイバー空間の持続的な発展を図るということで、政府機関、重要インフラ事業者だけではなくて、多様な関係主体がそれぞれの役割に沿ってサイバーセキュリティに連携して取り組んでいくということを目指すものとなっております。更に、重要インフラの中での大きな柱としてつくっていただきました任務保証でありますとか、あるいはリスクマネジメントといった物の考え方についても、柱として打ち出しているところでございます。今後、最終決定されます次期サイバーセキュリティ戦略とその関連の取組を踏まえまして、我々の第４次行動計画をレビューしていくというプロセスがあると考えております。

また、討議事項といたしましては、パブリックコメントの御意見を踏まえた障害等の深刻度評価基準の修正案、空港分野における重要インフラとしての取組について、この２つを項目として挙げさせていただいております。この２つにつきましては、本日御承認いただきますれば、次回のサイバーセキュリティ戦略本部にお諮りすることを念頭に置いているものでございます。

委員の皆様方におかれましては、本日も闊達な御議論をいただきますとともに、NISCの施策に対しまして、引き続き御協力をお願い申し上げ、挨拶とさせていただきます。よろしくお願い申し上げます。

渡辺会長から挨拶。

○渡辺会長　本日もお忙しい中、御参集いただきまして、誠にありがとうございます。

本日の専門調査会におきましては、先ほどセンター長からありましたとおり、重要インフラにおける昨年度の取組状況等についてまとめました「重要インフラにおける取組の進捗状況等（年次報告）」について、まず御承認をいただきたいと思っております。

それから、２つの討議事項の１つ目が、前回、３月の専門調査会におきまして「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）」につきまして、御議論いただいたところでございますが、このパブリックコメントの結果が出てまいりましたので、それを踏まえた修正案というものを、事務局のほうから御説明いただきます。御確認・御議論いただきまして、できれば承認まで進めたいと思っていますので、御協力をお願いいたします。その後、先ほどもございましたとおり、次回のサイバーセキュリティ戦略本部におきまして初版として正式決定して、世に出されるという予定

でございます。

もう一つの討議事項は「空港分野における重要インフラとしての取組について」ということで御審議いただきます。前回、前々回の専門調査会でも既に御報告いただいておりますが、現在の第４次行動計画における13の重要インフラに加えて、第14番目として空港を追加することを検討しております。こちらについても、本日御審議いただいた後、先ほどと同様、次回のサイバーセキュリティ戦略本部にお諮りすることを念頭に置いております。

それでは、限られた時間でございますが、今日もぜひとも委員の皆様方の闊達な御議論をお願いいたします。それでは、早速、議事に入らせていただきます。

(2) 報告事項

雲田内閣企画官より資料２「2018 年平昌オリンピック・パラリンピック競技大会における状況について」に基づき報告、山内内閣参事官より資料３「サイバーセキュリティ戦略（案)」の全体概要」に基づき報告。質疑応答は次のとおり。

○野口委員　御説明どうもありがとうございました。資料３と資料２で１つずつ質問があるのですが、まず、資料３で真ん中のグリーンのところの４番目の「大学等における安全・安心な教育・研究環境の確保」で、施策例として「大学等の多様性を踏まえた対策の推進」というのは、大学人としては誠に的を射た方針だと思っているのですが、他と比べて多少書きぶりが違います。うのは「大学等における安全・安心な教育・研究確保の推進」ではなくて「研究環境の確保」ということになっているのは、て、そうすると、大学自身が環境を作れという話なのか、安全・安心な研究・教育を推進しろということなのかがわかりにくい。先ほど山内参事官からは大学の安全に対する問題というお話があったのですけれども、大学の研究等が充実することが社会の安全に関わるということも当然あるわけで、この安全・安心というものの対象が、大学の方針なのか、大学の研究に対するものなのかが判断できない。それから、「環境の確保」という他とちょっと違う書き方をしているという意味を、さらに理解を深めるために、もし可能でありましたら御説明いただきたいというのが最初の質問です。

もう一つは、資料２の平昌オリンピックの資料で時にちょっと気になったのが、赤字で「大会運営に重大な影響を与えるようなサイバー攻撃は発生せず」というところが色を変えて書いてあるのですが、色を変えて強調している意味合いというのを教えてくれませんか。以上です。

○渡辺会長　ありがとうございます。それでは、まず、第１点目の資料３のほうにつきまして「大学における」というところですが、山内参事官、お願いします。

○山内参事官　承知いたしました。今の御質問のところには若干含みがありまして、最初は当然ガバナンスの話もあるのですが、ガバナンス、ガバナンスといっても、正直、私どもから見て、文科省さんともお話をすると、やはり大学の自治といったこともありま

す。ただ押しつけても、何のためにやるのだという問題が必ず発生いたします。であるとすると、研究者の教員でも結構ですが、研究環境をどうやって守るかということ自体が皆さんの役に立つのだと、インセンティブがあるということをちゃんと見ていただいて、やっていただかないと、正直、学長、学部長の方はお分かりかもしれませんが、「なぜ言われてそのまま黙っているのだ」みたいなことになるとまずいので、皆さんにまさに協働して働いていただくために、その位置づけとして、皆さんの環境、皆さんのお持ちの情報を守るためにサイバーセキュリティ対策が必要なのであるということをまず訴えたいがゆえに「教育環境の確保」という言い方をしています。

現実には何かという問題でいうと、大学にある程度フォーカスを当てているわけですから、当然、先ほどおっしゃったとおり、多様性というのはそこの問題もあります。例えば、これは共通する研究開発系の独立行政法人もそうですが、流動性はとても我々政府機関と同じにはみなせない。有期の方もいらっしゃるし、人も代わる。労働環境も一定の場所ではなくて、全然違う所へ色々なアクセスをされているということを考えると、当然、そういうことを念頭に置いた環境でなくてはいけないということと、先ほど申し上げたある程度自由を確保するためにといったことを抱えている組織であるがゆえに、そこを意識していただきながらぜひ進めていただきたいということを書いたつもりでございまして、１行で書くのはかなり難しいのですが、そういう思いを込めてここの中では語っているということでございます。

○渡辺会長　よろしゅうございますか。

○野口委員　ありがとうございます。誠にきちんとまとめた方向性だと思っていて、実は大学というのは、渡辺会長もそうですけれども、ガバナンスという格好で縛るのがなかなか難しいところで、セキュリティを強化すると研究自体が影響を受けるような微妙な関係があって、そこはきちんと踏まえた上で書いていただいたことに感謝します。

○渡辺会長　それでは、続きまして、２点目の御質問ですが、資料２につきまして、赤字にしたその心ということですが、雲田企画官からお願いします。

○雲田企画官　御質問どうもありがとうございます。この下にもちょっと書いてあるのですが、過去の大会を見ても、サイバー攻撃が起きたときに、システムが全く影響を受けないということは、どうもやはり難しいのではないか。これは恐らく東京大会に向けても同じことが言えるのではないかと考えております。

なぜ赤字にしたのかというのは、すなわち、仮にマルウエア等の感染を広げないために、場合によっては一部のシステムを止めなくてはいけない。若しくは短い時間だけストップしなくてはいけない。そのようなことがあっても、これは恐らくこちらのほうで議論されているミッションアシュアランスともつながってくるとは思うのですけれども、やはり全体としてオリンピックの運営が滞るようなことがあってはいけない。そういうことで今回の資料では赤字にさせていただきました。すなわち、私ども、東京大会に向けて、大小の攻撃があってシステムに影響があった場合にも、必ず運営に重大な影

響を与えないような対策を推進していかなくてはいけないというメッセージでございます。

○渡辺会長　いかがでしょうか。

○野口委員　ありがとうございました。メッセージの意味はよくわかりました。誠にそうだと思うのですが、ただ、普通、一般的にこのように赤字で書くとどう見るかというと、要は、「細かい話はいっぱいあるけれども、基本的にサイバー攻撃では重大な影響を与えることは起きないのだよね」というメッセージに見えてしまうのです。あまり過度に心配をして大騒ぎしてはいけないというのは、そのとおりなのですが、ただ、このメッセージの出し方によっては、何となく今までの延長線で、「ここをやっていると、色々あるけれども、結局、大きなことにならないのだ」というメッセージに見えてしまうのをおそれています。特にリスクマネジメントを行っていると、過去、あるレベルで多数発生したということと、東京はその程度だけで留まるということは別問題なので、そこら辺は、おっしゃる趣旨はよくわかりましたが、資料としてはちょっと心配です。以上です。

○渡辺会長　１点確認したいのですが、この資料はどこまで公開すべきかというのはありますか。

○雲田企画官　こちらの資料自体は、基本的には公開しても問題がない内容になっております。ただ、先ほどお話ししたように、色々実際に聞いている部分もあるのですけれども、ちょっとお話ができない部分もあるということを御承知いただければと思います。

○渡辺会長　わかりました。では、今いただいた御意見を踏まえて、ミスリーディングのないような形で御配慮いただければと思います。

そのほか、質問はございますか。稲垣先生、お願いします。

○稲垣委員　あと 10 時間ぐらいということなので、余り申し上げても役立たないかもしれないので、各論の中に書き込めるようでしたら、ぜひお願いしたいことがあります。

それは資料３の一番下の「５　推進体制」の下線が引いてある青字のところなのですが、「関係機関の一層の能力強化」とありますが、ここの所に『関係機関の一層の能力「及び本戦略への適合性の」強化』、要するに戦略適合性を高めるという取り組みも、サイバーセキュリティセンターを中心に国全体で整合性を保って、最適化された形でそれぞれの特に官の取り組みを進めるということを明確にしてもらいたいと思います。もちろん官民連携があるわけですから、当然、民も含まれるわけですけれども、現場の弁護士として最近の状況を見ると、ここでの重要インフラの会議、それから、これまで経産省で、さまざまな主体がサイバーセキュリティ対策とか取り組みの強化を進めてきています。その成果は上がってきたと思うのです。ところが、国全体で整合性がとれていないような事象が生まれている。これは私自身が経験するところでもあり、きっと NISC の目・耳に入っていると思うのです。具体的には法執行機関が、特に刑法の不正

指令電磁的記録に関する保管の罪などについては、これはもう少し慎重に捜査の抑制とか全体の戦略適合性を考えてやってもらわないと困る状況が生じているのです。経産省あるいはこの会議が、いくらセキュリティは経営課題だと、人材育成頑張れと言っても、およそそんなことができないようなことが「警察庁への報告事件」と県警が言っている事件で実際に起きている。つまり、地方警察の司法警察作用に対する警察庁の国家政策との調整のための統制が効いていない事案が生じているということです。

具体的にどういうことかというと、あるセキュリティサービスを提供している会社が行っているネットワーク監視サービスが，不正指令電磁的記録保管罪に該当するとして、何ら予告なしに捜索が行われ、サーバーなどを押収され、運用にあたっていた職員が逮捕された事案がありました。これについては、私は会社の代理人として事件を見ていたわけですけれども、警察は、この会社のこの事業そのものがこの罪にあたるという判断で捜査を展開しました。

法的な論点は細かくなりますので申し上げませんが、この罪は、プログラムなどへの社会の信頼を保護することを目的とし、不正指令電磁的記録を使える状態に置いているだけ、実害が発生しなくても成立します。そこで立法段階から適正な業務の保護，濫用の防止が議論され，故意の外に、正当な理由とか、あるいは第三者の意思に反して不正指令電磁的記録を動作させる目的が要件とされ、法務省は，これらの要件により濫用の危険はないと説明してきたのです。

ところが、この事件では、地方警察は、警察庁に報告した上で、この会社に何の照会もすることなく，事業がおよそ正当な目的に基づかず、こうした加害の目的があると判断し、突然、全くの予告もなしに捜索・差押えを行い、業務を止め、オペレーションしていた人間を逮捕しました。

会社は事業の顧客や株主、従業員の家族、他の従業員、関係者への説明に奔走することになりました。

警察は逮捕した従業員の勾留を求めましたが、検事は勾留請求すらしませんでした。検察庁がなした被疑者の処分は，証拠が集まらない，つまり司法研修所の教材では，嫌疑がない場合の不起訴処分に分類されている嫌疑不十分という不起訴処分でした。起訴猶予ではありません。

この影響ですけれども、同じような事業、つまり、例えばハニーポットをやっているとか、不正指令電磁的記録を集めて研究しているところはたくさんあります。事業に用いているところもたくさんある。大学もそうです。研究所もそうです。正当な目的について、警察は何と言ったか。「警察庁にも相談しながらやっている。有識者に相談もしながらやっている。」と言いながら、「正当な理由は、これは法律問題だからどうぞ争ってくれ」と。つまり、「最高裁までやって決着がついたら、それは結論が出るでしょうよ」という考え方で、全くの説明なく事件は進みました。これが行われたことによる影響というのは何かというと、例えば研究所のウイルスを扱っている技術者、それから、

一番問題になるのは大学とか経営層です。自分の会社で従業員がそうやって逮捕されるかもしれないといった時に、セキュリティサービスを向上させる人材育成の経営課題として一番大きなこと。つまり、「人材を集めるとか、研究をさせるとか、研究者を保護するとか、こういうことが最高裁までやって結論が出たらいいでしょうよ」という環境の中に今あるということを、警察庁に相談して実施した事件で行われたわけです。捜査の必要は当然だと思います。しかし，サイバーセキュリティ戦略，セキュリティ産業や人材育成を図ろうとする国家政策も同じように大切なのです。もう野放しにはできない。やはりきちんと調整する機関が必要だと思います。

ということで、それぞれの役所についても、今の警察庁のは一例ですけれども、やはりこの戦略との全体整合性ということをきちんと把握できる、把握しながら進めるということが必要だと思います。ただ一部だけやれとか、投資として考えろといっても、恐ろしくてできません。セキュリティ分野で著名な先生も検察庁に対して、法理論上この捜査を批判し，研究への脅威を危惧される意見書を出されたわけです。私も実はこの法律の制定に際しての法制審議会に幹事として入って、濫用についてはものすごく危惧があった。法務省も一生懸命対応をして、「濫用は無いように」ということで取り組んだ。しかし、司法警察については国全体としては整合性がとれていない。具体的にどうするかというと、捜査の戦略とか国家戦略とか、国益への適合性を確保する方法というのは今でも様々な方法があります。国家公安規則を作るとか、警察庁に報告が来たら適切な統制を行うとか、あるいは重要事件について、あるいはサイバーセキュリティ産業とか研究者に関する事件については、有識者を入れた会議等をインカメラで作って、NISC の中で議論して、捜査手続等は協議しながらやるとか、検察庁とも協議するとか、そんなことは今もいろいろな役所で行われていることです。そういう今ある取り組みをきちんと NISC として把握した上で、有効に機能させる。そういう形を実現してほしい。警察庁と地方警察の関係もあると思いますが，警察官が安心して捜査ができる。会社も安心して事業や研究をさせられる。国家全体で戦略的な成果を上げられる。こういう仕組みを確保していかないと国全体のロスになる。セキュリティは，ただやれと言うだけ、モデルとか枠組みをつくって思想はこうだと言ったところで現実には動かないです。ということを考慮していただきたいので、ぜひこの戦略適合性というのを推進体制の中で鮮明にしていただいて、下のところで具体的にそれらしいことを一言でも入れていただけると、警察庁も含め，進めやすくなるのではないかなと思うので、ぜひ検討していただきたいと思います。以上です。

○渡辺会長　ありがとうございました。かなり深い御議論だと思いますのと、我々調査会全体と、今の俎上とはちょっと外れるかもしれませんが、ここは重要なポイントだと思いますので、この会議が終わった後に少しやりとりいただいて、どういう書きぶりにするか、あるいは入れるとしたらどんなところがあるかということをぜひ御議論いただければと思います。事務局のほうからは特に何かございますか。どうぞ。

○山内参事官　重要な御指摘ありがとうございました。実は戦略本部の中で戦略の議論をしているときに、本部員の林先生のほうから同様の御指摘があり、今のサイバーセキュリティをめぐる法律については、その法律が元々サイバーを完全に意識したものがない場合、アナログの時代に作られたものに、ある意味、無理やり作った部分が存在することになります。稲垣先生の御指摘について申し上げると、経営層の方々がサイバーセキュリティについて考える場合、何の法律を考えて仕事をしなければいけないのかということが必ずしも明確ではない状態です。

これについては、戦略の 41 ページ、研究開発の項目において、サイバーセキュリティに関する法令解釈の明確化、サイバーセキュリティ対策における制度上の課題を明らかにすることにしておりまして、今の御指摘の点として実際に関係者、特に研究開発の方々が、やっていいのか迷っている旨を内々に聞いております。したがって、ご指摘のポイントとして、このような課題にしっかりと取り組まなくてはいけないと考えております。

他方、関係機関が自ら考えて、皆で連携して取り組むということは、この戦略の推進体制にも書いてあります。（ご指摘の件の発表について）私どもも詳細を承知しておらず、その一報を聞いたときに驚いたことも事実です。特に今回の件が我が国の技術力、基盤の整備という観点でブレーキになりかねないことを少し重く受けとめており、しっかり連携をしていくことが必要です。いずれにせよ、ご指摘の「適合性」は、多分施策を実施する際に何に影響するかということとも関係いたします。これをやったからこれだけで済むという話でもないというのは、ご指摘のとおりかと思いますので、この連携体制をどうやって整えていくのかという点で「柱の中に我々がちゃんと座れ」という御指摘を頂戴したと考えておりますので、（関係機関間で）しっかり連携を進めていくということは間違いなくやっていきたいと思います。よろしくお願いいたします。

○渡辺会長　ありがとうございます。

○稲垣委員　大変頼もしく思いますが、「中に座れ」というよりも「首座に座れ」というのが私の意見です。

それから、昔からサイバーセキュリティに関して何がというのは、民のほうが何をやっていいのか悪いのか、これは自身のリスクで考えなければいけないところが残るわけです。　問題は、執行機関である官と民の間の連携がきちんとできるかどうか。それは捜査ですから、密行性とか色々なことがあるだろう。でも、手順を共有するとか、部屋に入れて密行的にやっていくとか、適正化を図るということは国の中ではできるわけです。ということで、ぜひ民の問題と執行機関の問題を分けて、それから、首座に座っていただいて、国全体としての整合性をとってもらいたいということでございます。以上です。

○渡辺会長　本調査会に来ました報告事項ですので、ここで打ち切らせていただいてよろしいでしょうか。ここまで盛り上がるとは思いませんでしたけれども、大変重要な議

論でございますので、別ラインのほうで少し議論を進めていただければと思います。

御質問はまだあるかもしれませんが、ここで一旦打ち切らせていただきまして、事務局に別途いただければと思いますが、よろしいでしょうか。

○一同（異議なし）

○渡辺会長　それでは、本報告事項自体につきましては、了解したものとさせていただきまして、次に進めさせていただきます。

(3) 決定事項

事務局より、資料４「重要インフラにおける取組の進捗状況等」に基づき報告。質疑応答は次のとおり。

○稲垣委員　各論については、これから各事業者から出てくると思うのですが、まとめ方について意見を述べさせてください。結論としては、機能保証という側面から見た取組がこのように進んだと、あるいは今後の課題はこれからという指摘の部分が目立つところにあるといいなと思うのです。「重要インフラにおける取組の進捗状況」のところにずっと出てくるのですけれども、事実が記載されていると思うのです。ただ、第４次行動計画の思想的な特徴というのは、やはり機能保証ということを重視したことだと思うのです。

そういう意味では、同じ対策をやるのでも、各重要インフラ事業者の戦略目標とか投資の目標とか、そこに影響があるのか。進んだとすると、あったということなのだと思うのです。単純にセキュリティ強度を上げたとか、そういう取組なのか、あるいはセキュリティ強度を上げたという事実は機能保証を目的に行ったものなのかとか、このいずれかでやはり戦略への適合性とか取組の意味は違うと思うのです。それはこれからいろいろ調査をする必要はないと思うので、今までの機能保証という観点から取り組んだことは明らかなので、従前の見方と違って、機能保証からの強度というか、進捗があったという点を言葉としてまとめていただけると、せっかく第４次行動計画で機能保証という概念を入れたので、その部分の進捗があったということは入れていいのではないかと思うのですが、ちょっと御配慮ください。

○渡辺会長　事務局の方からはいかがでしょうか。

○越後参事官　これは、昨年度のご報告ということで、第一に行動計画が策定されたということを書かさせていただいたところでございます。昨年度は、第４次行動計画の１年目であり、機能保証の取組の活動が開始されたということになりますけれども、事実として、機能保証の概念を踏まえた指針を改定したところでございます。そのようなものを目立つように今後気を付けていきたいと思います。

○渡辺会長　それをこのバージョンで追求するということですか。

○越後参事官　来年度以降の改定で目立つようにするということになるかと思います。

○稲垣委員　時間のずれの問題はあると思うのです。だから、１年目は不十分だというこ

とでもいいのですけれども、少し始まったというだけでも足元の一歩を記録しておくということでいいのではないかと思います。

○渡辺会長　では、そこだけ微修正するということで、あとはいかがでしょうか。

○一同（異議なし）

○渡辺会長　ありがとうございます。特段なければ、これをベースに一応決定という形で進めさせていただきますので、また引き続きよろしくお願いいたします。

(4) 討議事項

事務局より、資料５－１「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)」意見募集の結果（概要）について」及び資料５－２「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（初版）について（案)」に基づき報告。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。それでは、ただいまの資料につきまして、フリーディスカッションを行いたいと思いますが、パブリックコメントにつきましては、５、６、７番が石油連盟からいただいておりますので、小野様のほうから何かあればいかがでしょうか。

○小野委員　石油連盟の小野でございます。今回、パブリックコメントを多く出させていただき申しわけなくもあるのですが、真面目に考えさせていただきました。

今回、御配慮をいただけたと思っているのが７番の情報提供の部分でして、こちらにつきましては、これまでも例えば東日本大震災であるとか、その後の熊本の地震であるとか、やはりかなり災害時に石油が必要ということで、情報提供を国の方からも数多く求められました。一方で、その情報に一番詳しい者というのは、正にその対応に当たっている者ということになりますので、ここに御指摘いただいているように、必要なリソースを必要な行動に投入することができるという観点からは、この部分は非常に重要でして、負担というところも御配慮いただいた上での情報収集という形を徹底していただければというのが、これまでの私どもの緊急時対応での経験からのお願いでございます。

一方で、石油は比較的、災害時等に注目を浴びるという経験を踏まえて、５、６番についても申し上げたところではあるのですけれども、今回のこの評価基準において、シンプルに示すことも重要な事だとは思います。一方で、シンプルに示した上で、実は解説が必要となると、それはシンプルではないのではないかというところもあるかと思います。数字から受ける印象みたいなものが、シンプルであるがゆえに一人歩きしやすい。そういった中で、特に「国民社会への影響」というタイトルがついているところを勘案しますと、このままいくと誤解を与える可能性があるのではないかと考えております。例えば地震で言えば、マグニチュードがあって、震度があって、被害がある。国民社会への影響は何かというと、やはり被害なのではないかというのが我々の考え方

です。それを「マグニチュードで計りましょうとか、震度で計りましょう」と。震度はある程度、説得力があるかとは思うのですけれども、例えば、あまり人の住んでいないところで巨大な地震が起きて、それは国民社会に影響がありましたかとなると、無いあるいは少ないといった評価もあるかと思います。そういったところで、でも、これは震度が７だったから７ですよとなると、国民社会への影響は何だと。地震の場合は、目に見えているのでいいのですけれども、サイバーの世界は、何が起きているのかが見えにくいので、特に誤解を生む可能性があるのではないかと。そういった意味合いでは、やはり我々事業者のところで何が起きているかだけではなく、それが実際に国民生活にどういう影響が起きているのかということがあって、初めて国民社会への影響と言えるのではないか。そういった意味合いで、５番などを書かせていただいたところです。これにつきましては、災害時の広報であるとか、国民へのアナウンスメントというのはどうあるべきかという広く大きな議論になるのかなと。サイバーだけではなく緊急時全般の議論なのかなと思っておりますので、今回は試案あるいは初版ということでやっていくということになるのかとは思いますけれども、引き続きどういった影響があるのかということを十分慎重に見ながら、こういったところも進めていただければと思う次第でございます。以上です。

○渡辺会長　実際の事案対応の経験を踏まえてこういった御意見をいただくのは、大変歓迎でございますので、ぜひ今後とも遠慮なくいただければと思います。７番につきましては、ご了解いただいておりますけれども、５、６番について、事務局から何かコメント等ございますでしょうか。

○瓜生参事官　ありがとうございます。公表の仕方も非常に重要だと思っておりまして、今年度、対処態勢ワーキンググループの中で、実際にどのような形で公表していくかという議論を始めようとしているところでございます。しばらく時間はかかりますが、また御相談をさせていただきたいと思っているのですけれども、誤解を与えないわかりやすい公表の方法、適切でわかりやすい方法を考えていきたいと思っていますので、御意見をいただければと思っております。

○小野委員　よろしくお願いいたします。

○渡辺会長　その他の委員の方、コメント、御意見はいかがでしょうか。

○稲垣委員　ピントが合っているところに物を申すわけではないので、敢えて念のためという趣旨です。誤解を生じさせるような表現は良くないのは当然だと思うし、官民連携して誤解を生じさせないように努める、これも大事なことだと思うのです。

　しかし、重要インフラは何を実現するのかという点については、やはり基本認識を一致させないといけないと思うのです。重要インフラとして、石油事業者がやるべきことは、サイバーセキュリティの目的で考えるミッションというのは、重要インフラ事業者に対して石油を提供することなのだという前提に立っていいのだろうかということは、私はちょっと意見が違うのです。各省庁・主務省は国民のために仕事をしているわけで、

ここに重要インフラに関係する全部が集まって議論している。内閣の中の一部ではなくて、内閣のこの問題を統括・調整する部門が集まっているということだとすると、やはり重要インフラ事業者の目的は、国民生活を安全・安心に確保することなのだと。その前提には立つべきではないかと思うのです。その上で誤解が生じるような問題があれば、そうならないようにするという各論の中での対応が出てくるのだと思う。前提が違っていると今後の各論の調整が上手くいかなくなるのではないかと思ったので、敢えて意見を述べさせていただきました。

石油連盟も、私のような理解をしているという理解でよろしいのですよね。あるいは、重要インフラ事業者がここに集った目的、ここに集ってサイバーセキュリティを議論する目的は、国民生活の安全を確保することなのだという理解でよいのですよね。

○小野委員　それは理解しております。おそらくそこの誤解を生じやすい最大の環境というのは、石油業界は、電力、水道というようなその地域を１事業者が担うものとは違っていて、全国展開している会員企業が日々競争しながら石油製品を供給しています。この深刻度評価基準につきましては、被害を受けた企業毎に評価を出していくという形になっています。会社の規模によっては、１つの会社が何か大きな被害を受けた時に、供給途絶、供給不足が発生する可能性がないとは言えないのですが、一方で、１つの会社で少し障害が起きた、何%か供給が止まったということがあったとしても、製品の備蓄等もあり、供給が完全に止まる、つまり、国民の方々の石油の消費に対して影響を与えることは少ない。その影響が極めて小さい水準で留まる可能性が極めて高い。

そういった中で、過大に、１つの会社の状況が国民生活への影響ですよという形で出ていってしまうと、パニックによりガソリンスタンドに行列ができるといったようなことも起き得るのではないか。そういったところも想像しながら申し上げたということで、我々は、自分たちの状況が国民生活に対して影響云々ではなくて、何が起きたかだけを見てくださいということではなく、広域事業である我々の事業の状況も前提として考えながら、このままだと誤解を生んで国民の方々の生活にかえって混乱を起こす恐れがあるのではないか。そういう視点から申し上げたというところです。

○渡辺会長　ほかの委員の皆さん、今の点に対しまして何か御意見はございますか。大林先生。

○大林委員　自分の見解が適切かどうかはわかりませんけれども、あくまでこの表のところで見ると、システムにどのような支障が出たかではなくて、国民へのサービスにどのような影響が出たかということでありますから、この基準によって、適切にこの言葉どおりに評価されれば、それで良いのかなとは思います。

ただ、おっしゃったように、国民社会への影響というものをどういうメジャーで計るかという、何か読み替えなどをする時に誤解が無いような注意というのを、実際の運用上はしていくということで良いのかなと思います。

○渡辺会長　おそらく本日の論点としては、いただいた意見に対しての反映が１つ、それ

から、その他については参考ということになりますけれども、今いただいた論点というのは、今後の実運用において非常に重要な論点かと思います。今回は「試案」が外れるという段階ですので、この後の基準の運用については、また引き続き議論をするということで、本日はこのあたりにさせていただきたいと思いますが、よろしいですか。もし追加のご意見がございましたら、６月27日までにいただければと思います。

いただいた意見についての対応は、１件反映し、残りについては、ここに書いてある考え方に基づいて、参考あるいは今後の検討とさせていただくということにさせていただきたいと思いますが、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。今後の事務手続について、瓜生参事官から補足をお願いします。

○瓜生参事官　資料５－２につきましては、重要インフラサービス障害の深刻度評価基準の初版ということで、次回の戦略本部に上げさせていただきまして、決定をさせていただければと思います。

○渡辺会長　ありがとうございました。

事務局より、資料６「空港分野における重要インフラとしての取組について（案)」に基づき報告。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。それでは、今の説明につきまして御意見、御質問等をいただく前に、所管省庁の国土交通省の方から何かございますでしょうか。

○国土交通省　国土交通省でございます。先ほどNISCの林参事官のほうから御説明ありましたように、昨年12月と本年３月の本調査会の場におきまして、国土交通省のほうから空港分野の取組について御説明を申し上げているところでございます。具体的には、空港関係者の方々に協議会を立ち上げていただいて、この４月から実質的に重要インフラに対するサイバーセキュリティの取組をスタートさせていただいているところです。このようなタイミングのもとで、今回、第４次行動計画を改訂していただいて、その中に空港分野を航空とともに重要インフラの位置づけにしていただいたということは、大変タイミングが良いものだと考えております。

国土交通省といたしましては、既存の航空と同様、空港分野につきましても、東京オリパラを見据えた上で、サイバーセキュリティ対策をやっていく必要なインフラだと考えておりますので、関係者の皆様とNISCとともに連携を密にして対応してまいりたいと考えております。以上です。

○渡辺会長　ありがとうございました。それでは、本件に関します御意見、御質問をお聞きしたいと思いますが、委員の皆様、いかがでしょうか。

○野口委員　御説明ありがとうございました。まず、空港を重要インフラに加えることに関しては、賛成です。その上で質問があるのですが、空港の中の対象とするシステムに

関して、どちらかというと、直接的に警備とかバゲージハンドリングシステムというような安全にかかわるような話が多いのですけれども、運用ということから考えると、チケットの発券管理・変更システムという実際の乗客が利用するシステムというのは必要ないのでしょうかという質問です。

もう一つ、もう航空という分野が入っているので、こちらに入っているかもしれませんが、空港における飛行機の誘導とか、そういう管制にひっかかるようなことは航空のほうで入っていましたかという質問です。以上です。

○渡辺会長　これはいかがでしょうか。国土交通省、お願いします。

○林参事官　代わりまして、事務局のほうから御説明申し上げます。航空の関係のチケット発券等につきましては、現行の「航空」の分野でカバーをされている、ということでございます。

飛行機の誘導と申しますか、管制につきましては、国土交通省航空局関係の事項になりますので、事業者という範疇からは外れてまいります。

○野口委員　わかりました。ありがとうございました。

○渡辺会長　そのほか、いかがでしょうか。お願いします。

○有村委員　JPCERTコーディネーションセンターの有村です。いろいろとお世話になっております。今の空港分野が重要インフラ化されるということについては、非常に良いことだと思っていますし、まさにオリパラのことを控えてタイムリーだと思っておりますので、セプターカウンシル等を支援している私どもとしましても、応援させていただきたいと思っております。

１点確認させていただきたいのですが、今回、構成員になっている空港・空港ビル事業者については、私の理解では民間の会社が運営している空港だと思っております。ただ、日本全般を見たときに、これは国交省様の管轄だとは思うのですけれども、例えば、いわゆる国際線を扱っているところがこれ以外にもあるということがございます。ですので、協議会としては民間の中で活動するということについては、良いと思うのですが、そういうところで出てきているセキュリティに関連する情報の流通とか、その他、いわゆる役に立つ情報については、広く空港に対して出していくということがあると思いますし、業界特有の状況であると思っていますので、そこの部分については、協議会の運営あるいは御指導ということで、国交省様と協議会との間で密に連絡をとるような御配慮をぜひお願いしたいと思っております。以上です。

○渡辺会長　事務局の方からいかがでしょうか。

○林参事官　ありがとうございます。大変貴重な御指摘だと思っております。実際の協議会の運用あるいは運営の仕方、これは非常に重要なポイントになってまいります。重要インフラとして指定がなされて、十分な防護なりプロテクトがなされるのかどうか。実際に関係機関ともきちんと情報共有がなされて、それが実際の取組にしかるべく反映されるように私どもとしても十分注意をしてまいりたいと考えております。

〇渡辺会長　よろしゅうございますか。そのほか、いかがでしょうか。よろしいですか。

〇一同　（異議なし）

〇渡辺会長　資料６にございました空港分野を新たな分野として加えること、それに伴う改訂につきまして、御了解いただいたと思っております。ありがとうございました。

それでは、今後の予定につきまして、事務局の方から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。

また、次回の専門調査会は９月頃を予定しておりますけれども、議事等を含め、別途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。以上です。

⑸ 閉会

〇渡辺会長　ありがとうございます。これにて、第15回「重要インフラ専門調査会」を閉会します。

以　上