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１回会合　議事概要

１　日時
平成27年３月26日(木)　10：00～12：00

２　場所
中央合同庁舎７号館　13階　共用第一特別会議室

３　出席者（敬称略）
安部　俊史　委員　（日本通運株式会社）
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　弁護士）
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）
金子　　功　委員　（一般社団法人日本ガス協会）
菊池　篤郎　委員　（明治安田生命保険相互会社）
阪上　啓二　委員　（野村ホールディングス株式会社）
神保　　謙　委員　（慶應義塾大学）
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　（東京工科大学）
寺内　敏晃　委員　（東日本旅客鉄道株式会社）
長島　雅夫　委員　（日本電信電話株式会社）
中山　広樹　委員　（株式会社三井住友銀行）
西村　敏信　委員　（公益財団法人金融情報システムセンター）
野口　和彦　委員　（横浜国立大学）
土生　　尚　委員　（日本放送協会）
筆島　　一　委員　（全日本空輸株式会社）
細川　　猛　委員　（石油化学工業協会）
松田　栄之　委員　（NTTデータ先端技術株式会社）
盛合　志帆　委員　（独立行政法人情報通信研究機構）
與口　真三　委員　（一般社団法人日本クレジット協会）
若林　武夫　委員　（公益社団法人日本水道協会）
渡辺　研司　委員（会長）　（名古屋工業大学）

（事務局）
髙見澤將林　内閣サイバーセキュリティセンター長
藤山　雄治　内閣審議官
谷脇　康彦　内閣審議官
三角　育生　内閣参事官

本間　祐次　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
総務省自治行政局地域政策課地域情報政策室
厚生労働省政策統括官付情報政策担当参事官室
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企画室
警察庁警備企画課
防衛省運用企画局サイバー対処・情報保証企画室
外務省大臣官房情報通信課

４　議事概要

(1)　開会（挨拶）

髙見澤内閣サイバーセキュリティセンター長から挨拶。

○（髙見澤内閣サイバーセキュリティセンター長）重要インフラ専門調査会の第１回会合に当たり、５点ほど申し上げたい。

まず、はじめに、サイバー空間で我々が直面している脅威が、拡散・深刻化していることが、はっきりしてきたこの一年間であったことを申し上げたい。ShellShockと呼ばれるbashの脆弱性の問題、更には、ソニーの米国子会社であるSPEに対するサイバー攻撃、これはある意味前例の無いものであったように思う。海外の重要インフラに対するサイバー攻撃もあった。いずれにしても、非常に脅威が拡散、深刻化しているという年であった。

２点目は、重要インフラ分野はこの一年、様々な取組が進んだということである。昨年の５月に、情報セキュリティ政策会議が「重要インフラの情報セキュリティに係る第３次行動計画」を決定し、これを受け、官民の連携で、安全基準等の整備及び浸透、情報共有体制の強化、障害対応体制の強化といった重要インフラ防護のための５つの施策の取組が強化されてきたということである。

３点目は、全般的な体制強化として、サイバーセキュリティ基本法が昨年の11月12日に公布され、26年度の補正予算への対応も可能となるような形でサイバーセキュリティ戦略本部が発足し、内閣サイバーセキュリティセンターに我々の組織が改組されたということである。これが今年の１月９日であった。戦略本部の第１回会合が２月10日に開催された。ここでは重要インフラ専門調査会を含めて３つの専門調査会の設置が決定され、加えてサイバーセキュリティ基本法に基づく新戦略の策定について安倍総理から指示を頂いた。こうした一連の動きが大きな体制強化に至ったものである。

４点目は、新戦略についてどうしていくかという課題である。NISC内や他省庁を含め、かなり幅広く議論を進めている。今後、戦略本部において、経済・社会の持続的発展、国民の安全・安心、更には国際社会の平和と安定というような議論が行われるであろう。加えて人材の問題であるとか、技術開発の重要性というようなことを含めて議論をしていくこととなろう。パブリックコメントを行った後、今年の６

月頃には閣議決定となる見込みと思われる。このような状況を踏まえ、重要インフラ事業者等におかれても、今回の新戦略の策定過程や、新戦略が策定された段階で、今後の施策の方向性について御協力をお願いしたい。特に事業者の自主的な取組の促進が重要であることから、我々としても一体となって取り組んでいきたい。

最後、５点目として、今回の会合で御審議いただいている、安全基準等の策定指針の改訂について、御審議をお願いしたい。このような計画段階のところは、実際に隅々まで届いて実行されていくことが重要であることから、こうした改訂を重視する観点から深い議論を期待したい。

(2) 会長互選

委員の互選により渡辺委員を会長に選出。

渡辺会長から挨拶。

○（渡辺会長）御指名いただいた会長の役については、これまで以上に邁進していきたい。

センター長からもあったとおり、昨今のサイバーセキュリティを取り巻く環境、これに対応すべく、昨年サイバーセキュリティ基本法が成立し、これまでの重要インフラ専門委員会が、重要インフラ専門調査会に改組された。委員指名も内閣総理大臣から行われるという意味でも、より重要な会合となったわけであり、本日がその第１回目となる。

本重要インフラ専門調査会は、これまでの重要インフラ専門委員会と基本的に同じではあるが、各重要インフラ分野の代表者及び重要インフラ防護に関する有識者の先生方、そして重要インフラ所管省庁をはじめとして政府関係者が一同に会する唯一の会議であり、その会議の重要性はますます増していると認識しており、私自身としても大変身の引き締まる思いである。

また、センター長からの先ほどの御挨拶にもあったように、ソニーハックと呼ばれているような象徴的なサイバー攻撃、新しい脅威が発生している。また、戦略本部において今後策定される新戦略など、環境がどんどん変化していく中で、こうした環境変化を視野にいれながら、本専門調査会の運営に当たっていきたいと思う。

本日の会合では、前回（重要インフラ専門委員会）会合より継続して審議いただいている、安全基準等の策定指針の改訂について取りまとめを行う。また、昨年５月に情報セキュリティ政策会議で決定された「重要インフラの情報セキュリティ対策に係る第３次行動計画」の初年度の取組結果を事務局から報告いただき、皆様方から御審議いただくことになる。

本専門調査会での審議及び検討は、我が国全体の重要インフラ防護において大変重要な役割を担っていることを改めて意識いただいた上で、闊達な御議論をお願いしたい。

(3) 決定事項

【専門調査会の運営について】

事務局から、資料２に沿って説明。

特段の異議なく、「重要インフラ専門調査会の運営について」について、原案のとおり定めることとした。

【第３次行動計画の改訂について】
事務局から、資料３－１から資料３－３までに沿って説明。
特段の異議なく、第３次行動計画の改訂について了解された。

【指針の改訂について】
事務局から、資料４－１から資料４－５までに沿って説明。
特段の異議なく、指針の改訂について了解された。

(4)　報告事項
事務局から、資料５から資料10までに沿って説明。
資料８の説明時に、分野横断的演習の検討会の座長を務めている大林委員から次のとおり補足があった。

○（大林委員）分野横断的演習は、これまで９回実施したことになる。演習という言葉を使っているが、実は訓練と演習というのは意図的に使い分けていて、それが一つの特徴になる。訓練というのは、例えば決められたことを繰り返して習熟するものを目的とする、いわゆるドリル的なものと考えると、演習というのは、決められたことをする習熟というよりも課題を発見するということを重視している。様々なリスクの中で、例えば自然災害のようなものは繰り返しており、水害であったり地震であったり、どのようなことをすればよいのか、対策は比較的分かりやすいが、ハイテクの技術にリスクが起因しているもの、これはリスクの様態がどんどん変わるから、どのようなものが最適な対応なのかということは、随時発見していかざるを得ない。最適なものというのは、必ずしも現状で規定しているものが最適とは限らない。何か課題を見つけることで進歩していく。そのような哲学と言うかフィロソフィーで、課題を発見するということを重視しようというのが演習と、言葉を使い分けている。

課題と言うか、この後どのような発展性があるのかということで言うと、演習と、先ほど言った訓練的なもの、これらを併せて行っていかなければならない。定型的なものの習熟と課題の発見。規模として、この分野横断的演習のような非常に大規模なものと、それほどではなくても小規模で、それぞれの分野あるいは事業者で行える、頻度としては沢山できるようなもの。そうした全体として訓練・演習の集合体として良いものを作っていくという必要がある。

ただNISCでこれが全てできるという訳ではないだろうから、この分野横断的演習は、比較的大規模な、そして、演習というタイプのものを年１回行っているというのが現状かと思う。もちろん、予算や体制が強化されれば、更に強化されると思うが、それでもやはり全てはできないかと思う。それぞれの分野あるいは事業者で行っているものと、全体としてどのような演習群のデザインを考えるのか。要するにそれぞれが単独で行っているのではなく、うまくインターフェイスを考えることによって、より全体として無駄が少なく一貫性がある、そうしたデザインを今後考えていくことができるのではないかと思う。そうすると、この分野横断的演習全体としてすることもできるし、ある程度シナリオをモジュール化できることから、それぞれの分野だけでも演習を繰り返すことができる。そうしたことで、ノウハウの蓄積等も進められ、この辺りが今後の発展性として考えられるかと思う。

また併せてこの演習に参加される方が、それぞれの分野のキーマンになる可能性

が非常に高い。参加される方あるいは運営の側で手伝っていただける方が特にそうかと思うが、実際に障害があった時に、我が国のインフラを守る事実上のキーマンになるような方がこの演習に参加している方と重なるということが多かろうと思う。そういった人材の育成だとか、ネットワーキングの機会にもなるので、この演習をそういった意味で更に活用できると考えている。

報告事項についての質疑応答は次のとおり。

○（有村委員）資料の中で２箇所、確認をしたい部分がある。

まず１点目は、資料８の12ページ、改善点の３番目の項目で、情報共有体制について誤認を思わせる意見が存在した、ということだが、我々としては、制度設計する上では、誤認をされないようにきちんと伝えていかなければならないと思う。その意味でこの誤認の内容がどのようなものだったのか。

もう１点は、資料６で、これは非常に網羅的に浸透状況を調査しており、実態を現している貴重な資料だと思う。その中の31ページ、自由意見の欄で、「その他の意見」の上から５番目のところ、「情報セキュリティの相談窓口の設置をお願いしたい。」という意見が出ている。政府も、それからJPCERTもそうだが、基本的に情報セキュリティの相談窓口であるというつもりではいる。しかしながら、なかなかそうした組織を作った時に、宣伝などができておらず、最終的な末端のところに伝わらない。JPCERTだけではもちろんないが、業界団体でもこうした相談があった時に一次窓口になっているとか、あるいはエスカレーションして、それぞれ専門のところに上がってくるということがあるかと思う。そうした相談窓口を我々は設置していると思っているにも関わらず、こうした意見が出てきてしまうということは直していきたいと思うが、この質問がどのくらいの頻度で出てきているのか。色々調べた結果、たった１個だけで重要だから載せたということもあるだろうし、100箇所調べたら98箇所からこう言われたとか、その点について回答いただければと思う。

○（柳原内閣参事官）１点目の分野横断的演習のところについて説明する。「官民間の情報共有体制について、誤認を思わせる意見の存在。」というのは、重要インフラ事業者等でのインシデント発生時には、所管省庁を通じてNISCに報告が上がってくるという流れになっているのだが、所管省庁にもNISCにも重要インフラ事業者が報告しなければいけないと思っていた事業者がいることがアンケートの中で分かった。要は、そこは理解不足というか、周知が至ってなかったのかもしれない。その点で、あくまで所管省庁のインシデント報告は、所管省庁を通じてNISCに上げてもらっているということなので、流れは１本。２つのところにするということではないということ。この辺りは、我々も分野横断的演習の事前説明会等でも資料を配りながら丁寧に説明していくことで改善していければと思っている。

○（本間内閣参事官）２点目として、御指摘のあった「情報セキュリティの相談窓口の設置をお願いしたい。」という意見について、これは１件のみである。自由意見については、特定の意見を事務局で削除してしまうということもできないので、出ている意見については全部取りまとめたということで、決して頻度が多いものが載っているのではない。今後の課題のところでも述べたように、全般的にまだまだNISCの取組が、事業者に浸透していないということが反省点であり、今後も周知を図っていきたいと思っている。

その他、特段の意見・質問はなく、報告事項について了解された。

(5) その他

本日の決定事項や報告事項を踏まえ、各委員から以下のとおり発言があった。

○（安部委員）分野横断的演習に自職場として参加し、今回から新設されたサブコントローラーの存在が非常に良かった。経験者がサブコントローラーを務め、初めての演習参加者に対して、指導・アドバイスをする形で、その仲立ちするサブコントローラーを通じて、演習のノウハウの継承が図られると感じた。

先ほど（資料６の浸透状況調査の説明において）、Ｐが８割、ＣＡが３割という説明もあったが、こうした、普段起こらない、起こってはならない事象に対する模擬演習というのは、特にＣＡの向上に対して非常に役に立つと思う。プレイヤーの意見など、今後も改善点を取り入れて、より実践的な演習にしていくべきかと思う。

○（有村委員）先ほどの髙見澤センター長の御挨拶の中で、サイバー脅威の拡散・深刻化として、ソニーの事例やbashの話などがあったが、この一年はまさに、インシデントレスポンスの支援をしているオペレーションの現場として、実感・体感している。今後も情報共有や問題解決に向けた対応調整や支援ということで、引き続き貢献していきたい。

今回、資料の説明を通じて思ったことは、第３次行動計画の別表中の重要システムとして、例えば「制御」という言葉が少し入り始め、ITの対象が広がっているということである。また、制御の部分は、ITの情報セキュリティ的な対策がすぐに使えない場所、セキュリティのアップデートができないだとか難しい話がある。そうしたものもいよいよ、こうしたところに挙がってきていることを本日の会合では再認識できた。対象として、こうしたものが出てくるとなると、様々な事を考えていかなくてはならなくなり、何か提案というか、考えていく場をそれぞれの関係者の皆さんと持てればと思っている。

○（伊澤委員）私たちCATVセプターは、活動を開始してまだ新しく、２年少しくらいである。今回、指針類をとりまとめたが、まさに対策途上や中小規模の重要インフラ事業者等をターゲットとして、事細やかな配慮がなされていると感じている。特に、今回新設された手引書は、我々の事業者においても非常に好評である。以前はわかりにくかったという訳ではなく、今回は、そうしたものがより一層身近になったという評価であった。とはいえ、我々の事業者は、約370社のうち（セプターの参加は）まだ約280社である。一定要件を備えていない事業者は入っておらず、自ら手を挙げていただいて入っていただいている。そうした姿勢や準備ができていないところがあるので、そうしたところを今回のこの指針、それから非常に好評な手引書等に基づき広く普及を進め、皆様と一緒にセキュリティについて考えていきたいと思う。

○（稲垣委員）この会議の役割が質的に変わったということに、皆さんと共に深い自覚を持っている。この会議は、今後、第４次行動計画、今までのテンポだと４～５年ごとになろうかと思うが、この前にオリンピックがある。それから御指摘のように脅威の拡散、対策の範囲、制御系の話も出ている。担い手についても、従来のセキュリティ対策を担う部署から、経営層への訴求も含めて、日本を担う重要インフラ事業者等そのものまで広がった。もう一つは、このサイバーセキュリティ対策という考え方から、サイバーセキュリティ政策とか、政府の戦略まで課題が広がっていっている。これは事業者だけでなく国民の課題にもなったということなので、戦略本部の下での限定された機能だが、実際に脅威と戦い、国民と接し、事業を担い、経営層に情報を上げる、こうした現場に近いところが、実際に物を知る者として具体的

な機能を深めていくということができる。ここへ行かなければいけないのだということを今自覚している。

その意味で、今回の資料６の調査は非常に意味のある、しかも有効なものだったと思っている。経営層については運用部分に思いが行かない。これは恐らく、設計は行うけれども、実際のシステム運用は非常に複雑だろうから、外部委託せざるを得ず、そうすると、経営層の目が届かないし、契約部門が仕様決定に届かない。そして監査部門もそこに及ばない。こうした現実を反映したものかと思っている。したがって実際には、こうしたシステム運用、セキュリティ運用については客観化されない。つまり、責任論だけで現実にどうなっているかわからない状態が起こっている。今後はそこに、ここに集う現場を知る者から、経営者が担う課題を具体的に抽出して、経営層が具体的な関与ができるように、対策をきちっと導いていくという作業が、しかもオリンピックを目指して急がれるのだろうと。最終的には、成長戦略の一環ということにもなったわけであるから、こうした取組を深めて、日本国の、あるいは日本の重要インフラ事業者等の競争力、それから日本の平和と安全、国民が安心して暮らせる国。これを、世界的に表出、輸出できるような、そうしたものを担うという、少し大風呂敷に聞こえるかもしれないが、この会議の役割はそこまでやれるという意味で、期待も込めて、皆さんと共有しながら今後も務めていきたいと思う。

○（大高委員）自治体分野の地方公共団体向けの安全基準として、ガイドラインの見直しをほぼ終えて、間もなく公表する予定である。策定に当たってはNISC等から、非常に貴重な御意見をいただき感謝する。今回の見直しをきっかけに、ポリシーの見直しを行うだけでなく、先ほどのアンケート結果にあったように、セルフチェックや監査、そうしたところがやはり全然機能していないので、そこを引き上げることによって、セキュリティ活動が活発になる。こうしたことをうまく進むよう、これから活動していかなければならないと実感している。

分野が政府・行政となっているが、政府統一基準群などの基準等もかなり参考にしているので、自治体だけではなくて、そうした基準も載せていただいたら良いのかなと思う。

○（大林委員）先ほど、IT依存度の調査の際に、IT依存度を人間の労力で代わりにできないと定義をした。それを聞いていて思ったのは、依存度が高まっていく、IT革命が今進行している中で、何世代か前の動力革命がどうなったか、機械力にどれだけ人間が依存することになったかということ。最初は、機械が壊れて人間が手で代わりの仕事をするという時代があったのかもしれないけれども、結局、200年、300年経った今になると、大量の物を運ぶあるいは物を加工するというのは、人間がもう代わりにすることができない。よって機械が壊れそうなものは機械が察知して、あるいは機械が代わりをするか、機械が察知して機械が回避するというところまで進歩させてきた。結局このIT革命においても同じようなところまで対策を立てていかなければいけないのではないだろうか。代わりのITで行う、あるいはIT自体が察知して危険を回避する。既にそういったところまで進歩している分野もあろうかと思うけども、恐らくどの分野もそのような依存に、遅かれ早かれならざるを得ない。そういった意味では、この重要インフラ分野の中でも比較的対策の進んでいる方のノウハウを、例えば横展開して他のインフラのところに展開していくとか、そのような活動もこの場でできるのではないかなと思った。

○（金子委員）私どもガス業界でもサイバーセキュリティの重要さが日々高まっていると感じている。一方で、業界を取り巻く環境として、ガスの小売を全面自由化するという方針が、３月に閣議決定をされたということで、ガス業界はこれから大きな変革期を迎えることになる。こうした状況であっても、というより、むしろこうした状況であるからこそ、サイバーセキュリティの取組を疎かにすることなく、改訂された指針も活用し、全体の底上げにつながるような活動を進めてまいりたいと考えている。

○（菊池委員）生保分野においては保険金の支払といったところを、持続的にサービスを提供できるようにということで取り組んでおり、構成員は42社ある。サイバーセキュリティの取組については、本日の資料６、これは私から見てもちょっと衝撃的である。全般的にやはりまだまだ取り組まなければいけない事がたくさんあるということを認識した。

また、分野の中では個別の事業者別の違いもあり、規模の大きさや取組の深さといったところから差が出てきているところもあるので、この先、この専門調査会で得た情報をフィードバックするということを行っていきながら、逆にこちらにもフィードバックできるようなことができればと考えている。

○（阪上委員）稲垣委員と同じ感想を持っている。法律に基づく組織ということで建て付けがかっちりと決まり、この重要インフラ専門調査会の位置付けを重く受け止めている。

証券の中も、254社と７機関の関連機関があり、全てまだまだ底上げが必要という認識を持っている。１社だけではなかなか前に進まないところも、いわゆる業界の中でCERTのような組織を作る、それから情報連携の仕方を変えるということで、一歩一歩、前に進んで行けるという認識を持っている。こちらの手引書なりを参考にしながら、証券マターで今一歩今一歩という形で進展させていきたいと考えている。また一方で、昨年から活動を開始している金融ISACという業界団体との横のつながりという情報連携もあるので、それも活かして縦横斜めをつないで全体の底上げを図るということを今年は注力していきたいと思っている。

○（神保委員）安全保障政策とサイバー分野の国際連携という立場で研究を続けて来ており、その分野から微力を尽くしたい。サイバー分野の国際連携だと、これから改定される日米防衛協力のガイドラインの中で、日米間では大変重要な政策の柱として位置付けられる予定であり、また、それに加えて、日本とヨーロッパ、そして新興国、特に、ASEANとの関係でも、能力構築といった視点から重要なアジェンダになっていて、特に日本の産業界のサプライチェーンの防護という点においては極めて重要な課題となっている。こうした国際連携と、重要インフラ専門調査会との活動との接点を是非追究し、議論に貢献していきたい。また、私、防衛省のサイバーディフェンス連絡協議会の研究会にも所属しており、他省庁との連携という点においても、是非この重要インフラ専門調査会と他省庁との、特に産業界との連携ということにおいてもプラクティスを共有するような形で議論に貢献していきたいと思っている。

○（鈴木委員）今般、専門委員会から専門調査会に衣替えされたという背景、それから指針について、本編・対策編という体系から、本編・対策編の他に手引書という、より具体的な体系に移ってきているという状況やその目的、そうしたものを踏まえ、ステージが大きく変わったということを認識しており、引き続き業界の対策につい

て進められるように頑張っていきたい。

○（高橋委員）石油セプター・石油連盟は、今年度からの新参者ということで参加しており、皆様にいろいろな御厚意を頂戴したこと、改めて御礼申し上げたい。安全基準については、初めて業界ベースのものとして、「石油分野における情報セキュリティ確保に係る安全ガイドライン」というのを取りまとめた。これらを機会に、より業界のIT基盤の確保・強化に取り組んでいきたい。

○（竹原委員）指針の改訂について、改めて、とりまとめいただいたNISCの皆様、関係者の皆様の御尽力に感謝申し上げる。今後は、私たちがこれをいかに有効に活用していくかということかと考えている。そうした意味では、私ども電力業界では、新たな制御システムに関するガイドラインの策定の準備を進めているが、この指針については、引用規格という位置付けで大いに活用している。また、この指針は、情報セキュリティの重要性に関する啓蒙といった面でも活用できるのかなと考えている。

皆様、御存知のとおり、電力業界は、来年４月から、小売の全面自由化という形になり、新たな事業者の皆様が多数参入を予定されている。このような状況変化に当たっても、電力の安定供給と保安は、サービスの基軸だと考えており、この基軸の上では、情報セキュリティの継続的な確保といったことが非常に重要だと考えている。新規に参入される事業者を含め、本指針等を活用しながら、業界としてのセキュリティ確保の重要性に努めてまいりたい。

○（手塚委員）いろいろ聞いてきて、今回の第３次行動計画を含めて、経営者層にこうした物を知っていただくというところを強調されているという点では非常に重要だと感じている。ただし、やはり経営者層にそこを訴えるにおいては、今、まとめているものだと、まだまだボトムアップ的で、どういうKPIで経営者層に示すのかというところを、もう少し経営者層の視点とのマップをまとめていくと、更に良いものになっていくのではないかと感じている。それはどういうことかと言うと、私の頭の中では、経営者層があり、これを大体まとめているガイドラインレベルは、事務系の管理職ないしは技術系の管理職、どちらかというと事務系の方が強いかと思うが、実際は、技術者サイドで理系の人間がこれをまとめるというところにまで落ちる。そうすると、そういう大きく三階層の人たちに、一気通貫でうまく伝わるようにするには、どういう言葉と言うか、概念と言うか、カテゴリーを設けて、それぞれに言っていくのかというのが、すごく重要であり、それを今後も更に突き詰めていく必要がある。そうした中で、今回まとめているのは、体制的な部分は多く打ち出されていると思うが、先ほど演習とか、実際に流してみるとなかなか届かないとか、そうしたお話もあったかと思うが、要するにリアルタイム性をどうやって確保していくのかというのが、今後ますます重要になるのではないかと思う。その意味では、やはりこうした分野をいかにシステム化していくか、単に体制だけではなく、そうしたITを使ったシステム化をどう整備していくか、というのをやはり今後、各業界を含めて、この場で考えていくことは、非常に意義があるのではないかと感じている。

○（寺内委員）現在、当社は、2020年のオリンピック対応を大きな課題として、対策が少しずつ動き始めている。今後も、分野横断的演習に継続して参加して、先ほど大林先生からあったように、演習で課題をしっかりと発見して、人材育成、ネットワークということで継続していきたいと考えている。

加えて、サイバーセキュリティ対策として、我々事業者が、自主的な取組という

ことで、社内でセキュリティに対する専門性を持った人材を育成していく、そして、情報をしっかりと経営層へ上げていくということを、事業者側で確実に進めていくことが重要なのではないかと考えている。そうした意味でも、今回も資料10で他セプター、インシデント情報等を御提供いただいており活用していきたい。

○（長島委員）通信分野でも安全基準の策定・改定に関しては、日々の見直しの他に、今回決定した重要インフラにおける安全基準等の策定指針を大きなトリガーとして考えている。

また、行動計画の段階から、経営層の在り方の訴求はかなり意識していたが、今回の資料６にあるような調査結果を見ると、やはり、PDCAのところが気付きになって来たので、今日いただいた情報を鑑みながら、是非とも私たちの方でも安全基準の見直しを進めていきたい。

それからもう一つ、分野横断的演習について、私もここ数年程、毎年参加しているが、今回初めて事後の意見交換会にも出席した。演習当日は、業界をまたいで意見交換するという時間はなかなか取れないが、事後の意見交換会のときはかなりその辺りの時間を取って意見交換できたのが非常に参考になったので、次回も是非、そうした営みを進めてほしい。あとは、NISCの施策の他に、例えば通信だとテレコムISACのような組織があり、今回、金融もISACを立ち上げたというのがあり、そうしたところでの連携、あるいは、重要インフラに関わらないが、CSIRTを企業の中で立ち上げている会社が増えてきており、そういった民間間の連携を、こうした場を機会に深めていきたい。

○（中山委員）金融機関に関し、皆様御存知の通り、海外においては大規模なサイバー攻撃を受け、甚大な被害を受けたという脅威も報告を受けている。そうした中で、今回サイバーセキュリティ戦略本部の下、事業者としての自主的な取組を推進していくということが謳われており、そうしたこと含めて、取り組んでいきたい。その中、本日の報告にもあったが、やはりまだ今回の指針の柱にあるようなPDCAがきちんとできていないところがあり、今後、CheckやActに対しては、演習を活用するなり、また、今回の指針手引書を活用するなり、銀行等セプターは1,400以上の金融機関があるが、全体の底上げを監督官庁の金融庁とも連携の上、きちんと図っていきたい。また、金融ISAC等、他分野との情報連携を深めていき、こうしたセキュリティ分野の情報共有もきちんと行っていきたいと考えている。

○（西村委員）現在、サイバー攻撃対応態勢整備に関する「金融機関等コンピュータシステムの安全対策基準・解説書」の改訂を行っており、発刊準備中である。この後、基準を策定した後が、大事だと考えており、対策の実施状況等を調査し、行動計画にもある通り、PDCAを回していかなければならないと考えている。さらに、基準を作った後、新しい攻撃が出てきた場合、基準に合致しているかどうかを確認するなど、これらをいかにタイムリーに対応していくかということも今後の課題だと認識している。

○（野口委員）どのような情報通信社会を作るのか、その情報通信社会の中でどのような活動を行うかということが、国や各企業の方向性や在り方を決めると思っている。そういう意味で情報セキュリティというのは、その情報社会の捉え方、情報社会での取組が、非常に謙虚に出てくる分野であるだけに、この情報セキュリティ分野をどのように設計するかということは、国、企業において本当に大事なものだと思っている。そういう意味から言うと、情報セキュリティが起きたことに対する受

け身的な対策、迅速に対応するということに止まらず、やはり今後の情報通信社会を先取りし、いかに良いものにしていくかという視点での対応が非常に重要だと考えている。特に重要インフラ企業においては、経営者のマネジメント力、情報システム担当者の技術力、それから、各社員一人一人の情報リテラシーという企業総合力が試されることになる訳で、そうした意味でも企業における情報セキュリティの問題というのは、情報システムの問題ではないのだという認識が非常に重要になるし、国としても、特にこの重要インフラの情報セキュリティに関しては、重要インフラ企業の努力だけでは当然できない訳で、行政としての法的制度、法の整備、制度構築、それから研究機関等の技術開発・研究開発という、国を挙げての総合力の勝負だと思っている。この会議がそうしたより良い国の在り方、企業の在り方に対して、少しでも寄与できるようになるべきだと思っており、その観点で私もできるだけ貢献していきたい。

○（土生委員）放送と通信の融合が進むということで、より一層の情報システムセキュリティ対策が必要ということを認識している。放送送出のシステムだけでなくて、数多くの情報システムを持っており、それぞれに運用規程とか、情報セキュリティガイドラインを定め、運用していたつもりだったが、よく見てみると、ネットワークを介した攻撃に対する防御に主眼を置いている。昨今発生している、内部関係者による情報漏えいやシステムダウンというようなこと、悪意を持った視点ということから、足りないということが分かってきて、この指針の第４版は、見直す良い機会になり、非常にありがたく思う。これらのガイドラインを見直すとともに、併せて放送セプターの安全基準等の策定に取り組んでいきたい。

○（筆島委員）航空分野においても、昨年来発生している様々なインシデントや2020年東京オリンピック・パラリンピックを見据える中でも、サイバーセキュリティ対策に対する重要性を非常に強く感じている。そうした中で、従来は今回のような指針、ガイドライン等々を各事業者で解釈して、自主的に取り組んでいたというところから、進んでいる金融分野やテレコムISACの取組を参考にしながら、航空業界の中でも、ノウハウを共有化しようというような取組をまさに今始めようとしている。そこでノウハウを共有化しつつ、更に他の業界の知見を得て、全体の底上げを図っていきたいし、そうした形でいろいろな知見を吸収してやっていくことが、我々を含めた重要インフラの使命を達成することにつながると思っている。

○（細川委員）本日の会議でも説明があったが、化学分野は本年度新たに重要インフラに入り、連絡体制の構築であるとか、安全基準・業界としてのガイドラインについてもようやく策定できた。形はできたが、大事なのはこれから実践していくところ。本日の会議でもあったが、実践しながら改善していくということで、今後、取り組んでいきたい。NISCや他セプターにもいろいろ御教示いただきたい。

○（松田委員）今回、配布された参考資料３の重要インフラ防護に関する諸外国の取組を興味深く拝見した。日本のシステムを考えると、クラウド化によってシステムやデータが、必ずしも日本にある訳ではない。また、様々な業界のシステムに関し、様々な国で使われ、システムも必ずしも日本にあるとは限らないという状況がある。そうした中で、行動計画には国際連携ということが書いてあるが、もう少し、一歩踏み進んで、どう国際連携をすべきかとか、情報共有の方法がどう在るべきかということを今後考えていかなければならない。

○（盛合委員）今回、補完調査のところで、実際に攻撃を受け、Webサイトのトップペ

ージが改ざんされた話があった。重要インフラや各府省庁において、ホスティングサービスを利用しているところも多いかと思うが、今回、例えば契約内容にログ収集が含まれていなくて、原因が特定できなかったという報告があった。ホスティングサービスを使って、重要なサイトを運営しているところについて、そのセキュリティ対策をプロバイダー側に任せざるを得ないというところが脅威ではないかと感じる。実際にこちらから要望をお伝えしても、環境が古いのでサポートできかねるという回答をもらい、契約やプロバイダーを変えたりしないと問題が解決されないという事例もあった。今後、オリンピック・パラリンピックを迎えて、目立つサイトへの攻撃は増えてくる可能性があるかと思うので、プロバイダーの意識向上を促すとともに、我々も改めて点検する必要がある。ホームページの改ざんというのは、古くて新しいというか、近年も進化し続けている攻撃であり、改めてそうした意識が重要である。

○（與口委員）私どもも本年度から参加して、先ほど報告があったセプター訓練であるとか、IT依存度調査、あるいは、分野横断的演習というところに参加して、参加したメンバーも新しい気付きがあったということで、大変感謝している。一方、私ども今回18社ということで、主要大手で参加しているが、実際には中小も含めて250社ほど対象がある。今後、こうしたところに、どうやって広げていくかというのが一つの課題かと思う。また、セキュリティのガイドラインも作成しているが、これも大手18社でスタートした関係で、ある程度できているというか、知識があるという前提でゆるやかに作っているので、中小に広げていくときには、先ほど説明があった指針等を参考に、分かりやすいものを作っていきたい。

○（若林委員）会議に参加して、非常に貴重な知見だとか、知識を私自身が得たかと思うので、協会の会員、事業体に様々な機会を通じて伝えていければと考えている。分野横断的演習の中で中小規模の事業者への拡大であるとか、参加対象の具体的なことを言われており、水道事業も中小の事業体がかなり多くあるので、できればそうした水道事業体が参加できるような環境作りなり、その訓練方法の対策なりを考えていただければと思う。

(6) 閉会

事務局から、今後の予定として、第３次行動計画の改訂、及び指針の改訂については、次回のサイバーセキュリティ戦略本部に諮り決定いただくよう手続する旨を連絡。