情報セキュリティ政策会議　基本計画検討委員会
第９回会合議事要旨

１．日　時

平成 20 年 7 月 29 日（火）　16 時 00 分～ 19 時 10 分

２．場　所

内閣府本府　地下１階講堂

３．出席者

【委　員】

有賀　貞一　委員　　株式会社ミスミグループ本社代表取締役副社長
井川　陽次郎　委員　読売新聞東京本社論説委員
木内　里美　委員　　大成ロテック株式会社常勤監査役
下村　正洋　委員　　ＮＰＯ日本ネットワークセキュリティ協会事務局長
須藤　修　委員　　東京大学大学院情報学環・学際情報学府教授
高橋　伸子　委員　　生活経済ジャーナリスト
富永　新　委員　　日本銀行金融機構局参事役・上席考査役
中尾　康二　委員　　テレコム・アイザック推進会議委員（KDDI 株式会社情報セキュリティフェロー）
満塩　尚史　委員　　環境省情報化統括責任者（ＣＩＯ）補佐官
（各府省情報化統括責任者(CIO)補佐官等連絡会議情報セキュリティワーキンググループリーダー）
三輪　信雄　委員　　綜合警備保障株式会社参与
和貝　享介　委員　　監査法人トーマツ

（五十音順）

【政　府】

内閣官房情報セキュリティセンター
警察庁
総務省
経済産業省
防衛省

４．議事概要

⑴ 重要インフラ分野の取組みに関する質疑

○ 政府機関と重要インフラとの関係だが、重要インフラの中にも地方公共団体を含む行政サ

ービスがあり、この関係がどうなっているかが疑問である。問題意識は、政府機関と重要インフラを跨った重要度評価の必要性である。前回印象的だったのは、政府機関では「ＩＴを支える内部人材をどう育成するか」が課題で、「国の根幹を司るものであっても未だコンティンジェンシープランがなく、早急に構築しなければならない」ということである。これに比べ、例えば金融機関では、システムの２０～３０年選手など内部からＩＴやリスク管理を支える人がそれなりに存在する。本当に動くかは確認する余地があるが、コンティンジェンシープランも一通りは作っている。この差が何故生まれるかを考えると、金融や通信、交通に比べて、政府や行政サービスで、止まった場合に国民が困るものが実は少ないのではないか。この仮説が成り立つとすれば、これまで「政府機関が一番頑張り、背中を見せなければならない」と力説してきた話の筋が違ってくる。行政を含む重要インフラ全体を横並びで比較し、重要度の格付けやリスク評価を行った結果、重要インフラの方が重要で、政府機関に大したサービスはない、と整理できるのであれば、「行政サービスは重要インフラ中のこじんまりした一分野として、身の丈にあった対策をしていけば良い」ことになる。大括りで切り出されている政府機関と、この重要インフラの１０分野の１つである行政サービスは違うのか。

⇒そこに示している重要インフラの政府・行政サービスは地方公共団体のことである。政府における対策は、政府統一基準に基づいて総合対策の中でみる。地方公共団体に関しては、これまでも述べさせていただいたように、地方分権の中で同じレベルに立っていることがあり、「あれをしないさい」、「これをしなさい」ということは言えない。地方公共団体には、止まると困るサービスが山のようにあり、その意味では重要インフラに位置づけ、その中で自主的な取組みを頑張っていただくということを考えている。ここはあくまで、重要インフラが重要で、政府の方が大したことをやっていないとは一切思っていない。第一回目でも説明したが、政策の影響力行使が直接的であるか間接的であるか、その関与度が高いか低いかということで括っているとご理解いただきたい。そのサービスが重要、重要でないということは、政府機関と重要インフラの間では特に意識していない。また、普通の企業と重要インフラ企業との間で重要度の差は多少あるが、業法の存在によって、ある程度直接関与できるが、非常に関与しにくい、間接的にしかできないということでも切れている。

○　重要インフラにおいて、ＩＴ障害ではない別の要因によりＩＴが機能しない場合などについては、別の観点での対策を行っているのか。ここでは、ＩＴの障害に限定するという捉え方なのか。例えば、４年ほど前に江戸川の架線が切れて、大規模停電が発生した。あのようなことが起こると、これは直接のＩＴ障害ではない。電力の障害が起こると、通信も機能しということが起こる。あのような障害をどう関連付け、取り扱うのか。

⇒　当然、電気が来なければコンピュータが動かない、もちろん備えをして無停電電源装置などをおいていればよいが、ＩＴを安定して動かすためのリソースにどういったものがあるか、それが途絶えたときに脅威となるかという観点で、相互依存性解析というものを行っている。電気が途絶える、通信が途絶えることによる脅威は当たり前のことかもしれないが、

他の点では水が途絶えて加湿や空調に影響が出るとコンピュータを動かせなるといった問題があることが、検討の結果として出ており、脅威として捉えている。安全基準策定の指針においては、電気と通信については既に書かれており、それに基づいて、各分野の安全基準にも盛り込まれている。当時、指針を作った際には、水については書かれておらず、いろいろと検討した結果分かってきたことであり、今後盛り込み、各分野でも認識いただいて、対処を考えていただいてはどうかというところである。水道が途絶えることも脅威として捉え、検討して対策の中に盛り込むということになるので、演習や情報共有を行う等の対処を考えている。

⇒　江戸川の架線事故による停電などは、重要インフラ専門委員会でも議論がある。いろいろな重要インフラ事業にとって、キーリソースが途絶することはリスクとして考えていただきたいということは言える。ただし、電力については、業法がありその中で頑張ってやっている中で、内閣官房のこの計画で、「であるから電力は頑張れ」ということを書くのは、つらいところがある。根っこにあるキーリソースが、他にとっての重要インフラであるということを、この計画の中で強く言うことは難しく、一般には業法の中で読まれていく。その中で、電力は安定供給機能が付いており、既にやらされている。さらにその上に、内閣官房の計画で、「だから電力はがんばれ」というようなことを、無説法に書くのはどうかということは付け加えておきたい。

○　電力と通信の途絶はＩＴを根本から止めてしまうということがあり、他の重要インフラとは違うところがある。そこが議論の対象でもあり、そこを直接狙われれば、相手を止められる。直接相手のサーバではなく、そこを止めることによって、いろいろなものを機能不全に陥れる脅威は極めて高いと思われる。その扱いが他と同じでよいのか、ということが気になる。

⇒同じでよいかということで、おそらく計画の中でそれらを特別な形で出すことはできないと思う。ただし、電力と通信の業法は厳しく書かれており、そのバランスの中で考えられればよいのではないか。これは第１次計画の考え方でもある。安全基準等の策定の指針を書く場合に、業法を変えるのではなく指針の中で、キーリソースとしてなくなる可能性がリスクとしてあるので、それに対して各事業が、それを利用しているユーザサイドが、きちんと見てくださいという構造で対応してきている。それに応じて、電力と通信は期待されているということは、示すことができるのではないかと考えている。自主性を重んじている分野であり、何でも政府がやれということは言えないので、知恵を絞って考えてください、という形になっている。

○　資料３－２の７頁において、政府への提言要望等が書いてあるが、制御系システムに関する監査範囲や内容等を記載したマニュアルの整備を行って欲しいとある。マニュアル整備の話ではなく、範囲として、電力、ガス、また通信では交換機系はそうかと思うが、いわゆる制御系が関わるところと、純粋にコンピュータで計算しているだけのところもある。これをみると、制御系のところはあまりカバーできていないのか、個別の議論では制御系も入って

いるのか。状況を伺いたい。

○　そのシステムについては行動計画の中で具体的に示されている。参考資料２の別紙１で、各分野にどのような脅威があり、対象となる重要システムの例にはどういうものがあるのかということが示されている。その中では、重要インフラたるサービスに直接関係するシステムについて、“対象となるシステム例”として書いており、これを踏まえ各分野で、そのシステムに関わることで安全基準を作っていくということである。その要望については、アンケートで回答いただいた結果をそのまま載せたものであるが、監査を行うというときに、どのような範囲、どのような内容について行えばよいかというマニュアルがあればよい、というご要望があったということである。行動計画や指針の中では、監査は検討課題と位置づけられており、実際どれくらい行われているかについては調べてはいるが、監査をやりなさいということにはなっていない。実際やる際に、そういったものがあれば便利なのではないかということで、ご意見・ご要望があったということである。

○　いろいろな国の重要インフラの活動を拝見しても、各国様々である。最近、韓国や台湾の活動について話を伺った。彼らは国の統制、運営がしっかりしており、一声かけると重要インフラの皆さんが言うことを聞き、ある要求事項を守っていくという体制はできているようである。それはある意味では、コントロールがしやすい環境にある。アメリカもそうであるが、日本ではそうなっておらず、個々の重要インフラの管理のやり方、考え方が異なっている。日本のＮＩＳＣがとってきたアプローチは正しいと思っている。安全基準等という、ある意味では柔らかな基準を提示して、それに基づき、自主性に基づいた基準を策定して、自分で回していただき、相互依存性解析や演習と通じて依存関係や重要度を認識しようとしている。その中で最も重要なことは、アメリカでも重要だと言われているが、情報の共有のスタイルであり、米国ではＩＳＡＣと呼ばれている。全てではないが部分的には上手くいっている。最近話しを伺ったところでは、匿名というシステムをうまく使い、何かのインシデント、物理的な問題、脅威等があった場合に、誰が話したかということを隠した状態で、自由に言えるという情報共有のスタイルをいくつかのＩＳＡＣで既につくっている。日本のＣＥＰＴＯＡＲ、ＣＥＰＴＯＡＲ－Ｃｏｕｎｃｉｌもそうであるが、いいところまでいき始めているが、まだまだこれからかという印象である。各重要インフラのＣＥＰＴＯＡＲがそこまで活性化していない。今のタイミングは、それを活性化するためにどういったことをするかを考えていくべきであり、活性化しなければＣｏｕｎｃｉｌというところまでは行けない。活性化しない状態で、いくらＣｏｕｎｃｉｌを考えても回らない。Ｃｏｕｎｃｉｌでは、いろいろな情報交換、横だけではなく、縦の情報交換も必要である。ＣＥＰＴＯＡＲの活動をいかに活性化させるかという施策を具体化していくことが重要である。

○　監査について、安全基準等をどれくらい遵守しているかを重要インフラの主管庁がみないことはないと思うが、やはり、重要インフラの事業者の中で、自らの内部的な監査なり、外部監査を使ってしっかりやっていくものではないかと思う。立ち上げのときに、そういった仕組みを作ったことは非常によいことであり、うまく自主性をもって使っていくことが重要

ではないか。

⇒米国のＩＳＡＣにおける匿名の情報共有は、流通する情報を増やすための一つの方策であるかもしれない。しかし、もう一つは米国の従業員も含めた外的プロテクションの問題があり、その中で匿名というチョイスをした苦渋の選択だと思っている。例えば事故調査委員会、米国におけるＮＳＴＰでは、その対象領域は鉄道と航空、キーリソースであるが、それ以外のところになると、司法取引によって、情報を明らかにすることで罪にはならないということがある。取引をすることによって Liability(ライアビリティ)をプロテクトできるところまでは、匿名でなくてもよい。その先に行くと、匿名にしない限り、責任を問われる仕組みになっている。日本の場合はさらに状況が厳しくてできない。これは私見であるが、この問題の解決のためには、重要インフラの障害に関しての情報を提供することで業界も含めシステムが良くなっていく益と、過失を追及することの益が、コンセンサスを経て書かれるか、法律として、あるいは社会的に形成されるか、というところまで行かなければならないと思っている。匿名は、単に情報流通を促進させるためだけのものではないという議論がおそらくあると思っている。私は、米国は仕方なく匿名になっているという見方をしている。いろいろな考え方があり、法益との関係もあり、今はそこまでは行かず、現実的にできる範囲でがんばってやっていこう、というのは事実である。委員が述べられたＣＥＰＴＯＡＲが活性化しなければならいというのは本質であり、そこはいろいろと考えているところはある。

⑵ 現在の重要インフラ１０分野の分類や位置づけの適切性に係る検討、重要インフラとしての対策と企業としての対策の境界についての検討について

○ 重要インフラ１０分野については、この裏に必ずＩＴベンダーの情報技術があるので、協力を求めるべき業界として、何らかの形で位置づけることが適当である。

○ 重要インフラとしての対策と、企業としての対策の境界は、どういった事態を想定するかによって変わる。「分野横断的な新たな法制を検討する必要がある」との記述にも絡むが、要するに、どれだけ大ごとであるか、全ての分野に共通する事案かによって、政府が重要インフラに命令するような制度要請が高まるか、「余計なお世話だからほっといてよ」が決まるのだろう。例えば、パンデミック（新型インフルエンザの大流行）が発生したときには、政府が音頭をとっていただかなければ、各企業が勝手に対応できる世界ではない。一種の戦争状態に入るのと同じで、戒厳令のような措置すら必要になるかもしれない。先ほど電力が止まれば全てに影響するという話があったが、空気が殺人的病原菌によって汚染される状態が国中に広がれば、企業も個人も含めて大変な事態なのだから、政府が指揮を明示していただくしかない。そういった分野かどうかを判断する必要がある。一方で、特定の業界で起こっているシステム障害のようなものは、(事後的な情報共有は別にして) 銀行のトラブルが鉄道を止めることは有り得ない。自ずと合理的あるいは自然な姿で関係が決まってくるのではないか。

○　現在の重要インフラ１０分野の分類や、位置づけの適切性に係る検討についての考え方の方向性は、ここに書かれているようなことだとは思う。ただ、違う観点を述べると、今何か起こった場合には、日本の国内だけでは片付かないということがある。ほとんどの会社では、ＯＳはマイクロソフト、データベースはオラクル、ＥＲＰはＳＡＰであり、何かしらトラブルの対策を立てようとすると、全て外国依存型になる。先ほどの１０分野の分類もそうであるが、対策の立て方を、皆さんがお考えになっているかということは大きな問題である。そういった思考が抜けているということは感じる。

○　これは私の持論であるが、規制緩和の取組みと皆さん言われるが、規制がなかった分野まで緩和という必要はない。もともと、ＩＴや情報通信の分野は新しいジャンルであり、規制もなにもなく、むしろなければ作るべきである。そこは古い既存の規制があるところと、分けて考えるべきである。そこが相当こんがらがっており、規制がもともとないところに、規制緩和も何もない。作るべきルールや、ガイドラインがあれば、それはむしろ作らなければならない。

○　業法で決められていると皆さん言うが、業法にはＩＴや情報通信に関しての配慮は何もない。業法で決められている業界は古い業界なので、ＩＴのことを考える前から成立しており、業法がそういうことを考慮して作られているとは思えない。逆に業法にＩＴや情報通信に関する規制を入れてもいいくらいだと思う。この辺りも、識別して議論をしなければ、すぐ規制緩和という話になり、おかしいと思う。

○　１０分野の分類について、証券取引所のような類は入っているのか。入っているのであれば、法律を作るというよりも、監督官庁は業法に基づいてしっかり指導しているのかという疑問、この情報セキュリティセンターは何をやっているのかと感じる。証券取引所は、トラブル続きというか、何かボロボロという印象を受ける。何を述べたいかというと、新たな構成よりも、しっかり業法に基づいて、規制、監督指導しているのかという状況で、注文をつけるということはできない。業法を上乗せして作るよりも、関係省庁がしっかりやっていないときに、統一的に見ている情報セキュリティセンターは何かを言うべきではないか。その機能を、ここ自身が持つことが重要ではないか。もし、政府から“しっかりやれよ”と言われれば、担当省庁は必死でやるだろうから、それで十分ではないかと思う。

○　１０分野の分類について、海外では地方公共団体は入っているのか。アメリカは政府を重要インフラに入れるなどしているようだが。先ほどから地方分権の話をされているが、やはり一般の国民が公共的なＩＴに接するのは、地方自治体が一番大きい。先ほどの説明でも、業界標準などの枠組でしか安全基準がない上に、規制が厳しくないという状況であるとすると、政府とネットワークを繋ごうというときに、非常に不安感がある。これは関係国では、どのようになっているか教えていただきたい。

⇒各国の枠組は様々であり、日本とは必ずしも同じような枠組にはなっていない。イギリスであれば、WARP といって、ワーニング、アドバイス、レポーディングといったアプローチがあるが、地方行政機関、警察、救急等がある。アメリカについても、詳細は分からないが、

州政府といったところが入っている。他の国についても、ある程度、地方の政府が入っているところはあるということである。

○　入っているということであれば、その規制の程度はどうなっているか。資料３－１では重要インフラ分野の安全基準というのは業界横断的なガイドラインであり、①業法に基づき業法が定める「強制的基準」や、②業法に準じて国が定める「推奨基準」及び「ガイドライン」、でないものが多く、低いレベルになっており、各国もこの程度になっているのか。

⇒　米国におけるＩＳＡＣの場合は、連邦政府と州政府の関係は非常に緊張関係になっており、各州政府が何をやっているかに関しては、勧告を出すのではなく、ＩＳＡＣを作って、後は頑張ってねというような、日本よりも更に低いレベルでやっていると思う。イギリスの場合は、日本の関係と結構似ていると言われているが、全体の重要インフラの政策を作っている委員会で、日本より、もう少し強いのではないかと予測している。千差万別である。

○　アメリカは緩いガイドラインでやっているという話であったが、アメリカは訴訟社会であるので、ガイドラインだとしても、トラブルが起きた場合に簡単に訴訟ができる、あるいは、集団訴訟という形で責任を負わされる。日本の場合は、政府を訴えても、あまり勝てるということもないので、全く事情が違う。そのように相対的に考えなければならないのではないか。それはおそらく、どこかの局面で切るのではなく、総合的にトラブルが起きたときにどう対応しているかまでを含めて、考慮しなければならない。ＩＳＡＣがガイドラインでやっているのだからということでは、紋切り型の一面的な見方になるのではないかという危惧がある。

⇒　日本での構造では地方分権であるということを建前としており、現実にはきちんとやらなければならないということで、総務省の自治行政局、自治体の方、あるいはＬＡＳＴＥＣという組織が一緒になって、ガイドラインを作り、いろいろな勉強会を行い、取組みは広がってきている。これは実施の取組みとしての現状であり、これはベストプラクティスになるが、今のところ国が地方行政に対して、「あれをやれ」というようなことは言えない。その中で、でき得る最大限のことはこのような現状の取組みである。これは法律の下でコンセンサスがとられており、政府の計画としては法律を逸脱できない。その原則の中で、どこまでできるかということを、次期計画の中で考えていくべきだということである。

○　考えられる方向性として、「分野横断的な新たな法制を検討する必要があるのではないかという意見もある」とあるが、それは、地方自治体は除くということか。

⇒　ここにあるのは、こうした議論が重要インフラ専門委員会の中で出ているということであって、事務局としてこれをやりたいと表明しているわけではない。

○　今の委員の意見にコメントしたい。東京証券取引所が一番よい例であるが、現在、裁判が進行している中で、証券取引所というのは、証券会社に取引の場を提供する機能を有しているのみであって、そこで何が起きても責任は負わない、ということを言っている。情報システムを提供するのは本業ではないということである。そんなばかなと、皆さん思われるかもしれないが、厳密に法律を解釈すると、設置基準であるとか金融商品取引法上では、ある意

味でもぎりぎりである。情報システムを駆使して、証券取引マーケットを形成して、サービスを提供していると思うことは全くの幻想である。だからこそ、業法上やルールの中に、そういったことまで入れなければ、やる気はおきないし、やらせられない。

○　関係者として発言させていただきたい。ＪＳＯＸがそこまで規定していないということと、東証に何かＮＩＳＣが関与してはどうか、というご意見だと理解している。２００５年の東京証券取引所のシステムダウンの後に、社外取締役ということで務めている。先日、７月２２日の派生商品のシステムが止まったことについて、金融商品取引法１５１条に基づいて、金融庁に報告を求められ、原因究明等をどうするかということを行っている。ただ、規制を強化すれば、これがなんとかなるのかと言えば、そういった問題ではなく、システムが止まるというのは、ここでも議論されたことではあるが、ゼロにすることはできないので、起きたときにどうするかということである。日本が特別にたくさん起きているわけではなく、アメリカや他の国でも同じ程度で起きている。だいたい１時間以内で回復しているが、日本は半日、あるいは１日止まったりする。その対策、システム障害が発生した場合のフォール・バックをどうするかということを、今日も話し合ってきた。それは規制でやるということではなく、市場原理で、システムダウンを起こしたので世界から信用をなくし、まさに東証でなくてもよいと、使われなくなるわけであるから、そういう形で内部規律をきちんとし、システムをやらなければならないということで動いている。規制すればどうにかなるというものではないのではないかと思っている。取引所自体、証券業界自体がシステムをきちんとやってこなかったということは、その通りであると思う。重要インフラ専門委員会に東証のＩＴ企画部長が入っているが、経緯をみると、これは２００５年１１月のシステムダウンの後に入っているということで、それまでは金融と言えば、銀行しか入っていない。今、東証のシステムを直している人たちも、全銀のシステムをやっていた人たちであるという現状である。規制でなんとかなるものではない、ということだけは申し上げておきたい。

○　先ほど別の委員からパンデミックの話があった。災害、天災、事案その他の非常事態にどうするかについて、示されている資料には書かれていない。総務省では、重要通信の高度化に関する研究会を行っており、この５月に報告書を出している。これは、まさに横断的に何をやるべきかとうことである。重要通信は天災、事案その他の非常事態が発生し、また発生の虞があるときに、災害の予防、交通や通信、若しくは電力の供給の維持のために必要な事項を定めるということで、電気通信事業者法で定めている。その研究会では、輻輳が発生した場合の帯域制御、優先順位を付けるということで、通信時間を制限する、その時に、皆さんセキュリティについても言われるが、優先順位ではなく、それを止めたりだとかという必要もあるということ、ＩＴ化の中でのネットワークで停電時にどうするかということを定めていった。この辺はきちんと接続して、やっていかなければならない。ＩＴセキュリティということで、情報通信の世界で横串を通しているので、そことの関係を整理していくことが必要である。

○　規制をすればトラブルがなくなると申し上げているのではなく、裁判所に提示された資料

の中で、自分たちの位置づけは場を提供することであり、システムを提供することは仕事ではないという規定をしている。裁判所に東京証券取引所として、正式に提出された資料に明記されており、そういうことをやっておられるところで、情報システムに期待するということは、まさに間違いである。一般的世の中で、東京証券取引所というのは、証券取引のシステムの場を円滑にして、スムーズな取引を成立させるシステム提供サービスをやっているものと思っている。そういうことではないということを、ご自分で定義しているわけであるから、その意味では、再定義をし直して、ルールを変えるということが必要だろうと思う。先ほどの電力の話もそうだが、そういったことは他の業界にもあり、業法自体が、これだけ情報通信を活用する世界になることを想定して作られていないので、そこを配慮すべきだということを指摘した。ある程度規制を強化しなければ直らないと思っているので、そう申し上げたい。

○　第１次提言では、合理的水準の対応策を検討してはどうかということを言っており、ミスのない絶対的な水準を求めるものではないということを報告している。したがって、規制強化とまでは言わないまでも、重要インフラ事業者については重要インフラとして、合理的水準の対策をとるべきである。それを規制と呼ぶのであれば、その必要があるだろうと思う。

○　分野横断的という表現があるが、各重要インフラはそれ程共通的なものはなく、それぞれリスクが異なり、事業形態、業態が違う。規制という形で対策をとるのであれば、それは分野横断的ではなく、各業態、重要インフラ毎に決めればよろしいのではないか。

○　証券分野において、先の委員が述べたように、担当省庁がやっていて、潰れたら自分のところで弁償すればよいという考え方であれば、重要インフラから外せばよいが、そういうわけではないのだろう。重要であるから特別な体制を組んでやっている。重要インフラに入れて、自主的にやらせてますというのであれば、むしろ外し、内閣官房情報セキュリティセンターとしては不作為であるとすべきである。重要インフラというものに挙げたことに、情報セキュリティセンターとしての責任を自覚すべきであり、挙げたものに対して、責任をもって動くようにすることが仕事である。ここまでやればいいんですよ、とするのではなく、動くということが目的であれば、その目的が達成されていないということについては、自省すべきところではないかと思う。

○　最近の傾向を見ていると、規制が民間活力を阻害し、経済の活性力を衰えさせ、国力を奪われることに繋がってくるのではないかと感じるほどである。先ほどの東証の情報システムのビジネスインフラとしての認識の欠如は、全くそれとは違うレベルであると感じる。

○　規制を受ける必要があるのは、サービスを提供しているＩＴ事業者であると思う。品質を担保していく仕組みが何もない中で、ソフトウェアが作られており、トラブルが起こると、事業者の方が積極的にバッシングを受けている。その実態がプログラムミスであっても、発注者側が謝っており、それは非常に変だと感じる。むしろ、そういった品質を確かめるような自主性が必要であるが、全体に欠けている。その規制は、自主管理型を強化するというところへ、もっていくべきである。

○　インシデントレベルでも、アクシデントレベルでも、またそれを超えるような大きなレベルでも、基本的には自主的にやるべきである。しかし、さらに大きなレベルで、国レベルでの対応、対策本部を作らなければならないようなレベルになったときに、官民が一体となって統制を働かせる枠組はいるだろうと思う。ただ、通常時における様々な問題については、民間が自主管理を強化する、相互に刺激し合って、自分たちできちんとやるというような仕組みが必要である。規制ではなく、民間の自主活動のような形で行うのが、あるべき姿のような気がする。

○　今述べられた委員の意見に同意である。特に重要インフラのＩＴシステムの構築事業者等に関しての責任が、明確になるような仕組みが必要ではないか。規制するのがよいかについては分からないが、そういった仕組みがいる。例えば、情報処理システムに事故が起こったときに、報告書を出すというようなことが必要ではないか。それをやってもまだ直らないようであれば、三振アウト、三回続ければその業者はだめであるとか、そういったペナルティを課すようなものまで必要なのではないかと思う。

○　いろいろご意見あろうかと思う。事務局が想定した規制に関する両極については、委員の間からも両極、その間のご意見が出されている。ここは今日フィックスするということではないので、このように出していただいた意見を事務局で整理していただこうと思う。

○２週間前、元検事である郷原弁護士と日本経営協会で、内部統制とコンプライアンスについてパネルディスカッションを行った。郷原弁護士も著書でよく述べられているそうだが、コンプライアンスが日本企業をだめにする、あまり規制をやると、日本人は細分化した規制法をたくさん作って身動きがとれなくなる。基準の大まかな括りというのは重要であり、指標というのはきちんと作る必要がある。作った上で、自主的な行動のフレキシビリティは認めた上でやる、細かくやってはだめだということを述べられている。その時、パネルディスカッションをやった監査法人の監査人の方々も、日本人はそのような指標を作ると、更に細分化した規則を作る、これは行政もそうであるが、身動きをとれなくし、計画能力を失っていくというパターンに陥るのが、今までの例であるということである。グローバライゼーションの関係で言えば、大まかなIndication(インディケーション)はおそらく必要であろう。その中で、世界の動きとの連携がとれるような柔軟さは必要である。指標を作って、可視化をしなければ、自由に各業界でやりなさいということでは、これもだめである。規制といってよいか分からないが、指標で“見える化”をし、行動基準をその方向に合わせられるような体制を作らなければならない。何でも自由にやってよいというわけではない。そこは、今までの業法では困難を伴うので、これまでのご意見を踏まえると、ＮＩＳＣが積極的に動くべきということではないか。そのあたりの考慮は必要であろうと思う。

○　これまでのところ、まだご意見あろうかと思うので、メール等で出していただければと思う。

⑶ 重要インフラ対策に係る監査のあり方について

○　自己点検、内部監査、外部監査について、分野や事業者毎に適切な方法は異なるとあるが、方法は分野毎に同じになるのではないかと思う。ただし、そのときの点検や監査を行う基準は重要インフラ、事業者毎に異なる。監査のやり方は、良い方法があれば、それは共通で使えるのではないか。

○　監査についてはコストが必要であり、負担に耐えられるか、ユーザへの転嫁がどの程度容認されるかとあるが、重要インフラ事業者は大きな社会的責任があるので、監査を実施するのであれば、自らのコストとして当然に負担すべきではないか。仮にユーザ転嫁ということを考えたとしても、重要インフラは比較的公共的なサービスであるので、利用者がたくさんあり、各ユーザ毎の負担はそれ程多くないのではないか。ユーザが極僅少な負担を負うことによって、信頼を買うといったことにもなるのではないか。したがって、監査に対するコストは、それ程問題にはならないのではないか。

○　監査の妥当性や有効性を外部から検証することは困難とあるが、意味合いとしては、監査はやるが、やった効果であるとか、監査を監査するようなことが難しいのではないかということだと思う。これは困難ではないと考える。監査人、監査する者を規制するようにすればよいと考える。例えば、監査基準、監査する人の行動基準を明確に定め、それを守るようにすればよい。実際に基準を遵守して監査が行われているかを、審査のような形で検討すれば、監査の妥当性を検証することは、それ程困難ではないと思う。そのことをもって、監査をやらないというのは誤りである。

○　今の委員の意見に賛成である。多少質問も含む意見になるが、ＩＴベンダや通信事業者に対する監査はどうなっているのか。金融分野においては、金融庁が検査や監督を実施しているうえ、日銀考査もあり、監査は行われている。最近では外部委託の進展に伴い、（本来は経産省や総務省の領域かもしれないが、監査されていないようなので）金融業に関わるＩＴベンダのセンターにも立入調査を行っている。重要インフラの重要度にもよるだろうが、もし金融界だけが金融庁と日銀のダブルで監査し、他方で何の監査も行われていない業界があるとすれば、全体バランスとしては甚だ均衡を失している。「監督官庁がしかるべくチェックに行けよ」という筋合いになるのではないか。

○　監査の負担を強調する意見については、監査を受検し説明する負担を言っているのであれば別だが、金融庁の検査も、日銀の考査も無料で行っているので、そういう仕組みを作ればその意味での負担は出ず、ユーザーへの転嫁を考える必要もない。

○　ここに自治体のことも書いてあるが、自治体の外部監査は結構金がかかり、それを市場で評価を得て取り返す、それで税金を上げてよいということにはならないので、結構負担になっていることは確かである。自治体の監査の経費については、少し考慮する必要はあるかと思う。共通のフレームワークで、監査法人にやってもらえないかということは、まだ検討途上であるが、自治体の方からもお願いはしているところである。

○　重要インフラ事業者が、フレームや目標をある程度設定して、その中で“見える化”して

達成していくということであれば、それは数の裏打ちであると思うので、監査の考え方も、情報セキュリティ管理基準を更に細かくするという議論に行くのではなく、自己宣言した上で、監査をしてもらう方がよいのではないか。自分たちがどうやるべきだということを定義した、検査として見てもらうということはある。最低限としてのレベルは別にあるだろうから、大枠の流れはそのように考えた方がよい。

○　監査の話がセキュリティではよく出てくるが、監査する側の組織のリスクをどう考えていくかということがある。会計監査法人は、会計法や会社法といったもので最後は責任を取らなければならないとなっている。それと同じように情報セキュリティに関して問題が起きた場合、情報セキュリティ監査を行ったところがどこまで責任を取るのか、取れるのか、取るべきなのか、といった議論がなされていないと思っている。重要インフラに限らない話かもしれないが、そういった仕組みをどう考えるか。今の会計監査法人に被せていくというのが一番手っ取り早いかと、正直思っている。それでよいのかという確認はしたいので、そのような仕組みを含め、リスクを社会としてどう吸収していくかということを、構造上考えておかなければならない。

○　先の委員も述べられていたが、いろいろな業界のマップが作られているようだが、その中で監査をしているところ、検査をしているところ、セキュリティに関しての監査が含まれているという意味であるが、それを一度表として整理した方がよいのではないか。金融界も感覚的なところで言えば、毎日のように監査を行っている。日銀、金融庁の監査、証券関係であれば証券業協会監査があるが、それをご存じない業界の方もいるので、重要インフラとしては、これくらいはやっているということを認識し、では我々はどうするかということを決めていただきたい。整理をしていただいた方がよいかと思う。

○　ここで取り上げる議論かということはあるが、情報処理技術者試験の委員をずっとやってきて、情報システム監査に関する部分には異論がある。情報システムを監査しようとすると、相当高度な技術力がないと監査できない。ほとんどの会社のデータベースはオラクルなり、ＳＱＬサーバなり、ＤＢ２を使っている。基本的にその中に企業の活動の痕跡が残っているので、そこからのデータをサンプリングし、トレースして、正しい処理が行われるかということを、監査人が独自にきちんとできるか。情報システム部門に頼めばよいという話もあるが、やはりある程度自分でできる技術力がないとできない。失礼な言い方になるが、今、内部監査人、外部監査人でそのようなレベルが備えられている方は非常に少ない。非常に形而上学的な、形式的な監査、ステップや手順だけはおっしゃるが、中の技術についてお分かりになってない方が非常に多い。その中で、監査を義務付けるなり、やりましょうといっても、極めて表層的なものにならざるを得ない状況が想定される。どうするかについて名案はないが、ＩＴであるから、ある程度そのような技術を考慮した監査をきちんとやるということを、明確に打ち出さなければ、監査をやらせても効果がないのではないか。

○　基礎的なことを伺いたい。先ほど自治体については、監査がかなりの負担になっているというお話があったが、どのくらいの費用がかかるものなのか。今の委員が述べられたような、

あまり資質がよくないというということであれば、どういうことなんだという感じがするので、どのくらいの費用がかかるのかお伺いしたい。

○　記憶の範囲では、検証レベルで、一つのシステムで一千万、二千万かかる。したがって、毎年はできない。それが複数のシステム全部であるとか、いろいろあり、全ては毎年できない、順次実施するというようなこともある。

○　そのような高い額であり、業界に資質のばらつきがあるのであれば、監査という言葉は聞こえはよいが、前段として、システム監査というのはどのようなレベルかということを、専門委員会なりを作って検討、調査していただいき、それに基づき体制を考えるといったことしか、ここは書けないのではないか。金融分野は確かに進んでおられるだろうが、ここはそのくらいしか書けないのではないかという危惧をもつ。

○　コストについては、分野によるだろうが重要な問題であることは確かである。それに値する能力を監査法人が持っているかということも深刻な問題である。それをどうモニタリングするかということも重要なことである。

○　監査にはいろいろある。技術レベルの高い、不備を指摘する監査もあれば、事故が起こった場合に、このような原因で事故が起こったので、こういう対策をとったという企業の報告書について、それが正しいか、事故報告書では本当のことを言わない可能性があるので、正しいことを言っているかという監査もある。また、自治体において、自分でセキュリティ基準を定めたとして、それが守られているかという、いわゆるコンプライアンス、準拠性の監査がある。どのような監査を適用するかをまず検討しなければならず、いろいろある。ある程度不備がなくなったところに対し、成熟したセキュリティについて、毎日きちんと運用されているかどうかを検討する監査もある。それはいろいろなレベルがあり、先ほどあった、一千万というレベルの監査もあれば、自治体によっては数百万というオーダで助言型の監査を行っているところもある。どれを適用するかということも、検討の一つではないかと考える。

○　監査について、まず自主点検と内部監査をベースにすべきではないかと、実際に経験して感じる。これにはPDCAが重要であり、形骸化しないマネジメントをきちんとやるということが一番基礎になるのではないか。例えば、情報セキュリティだけが対象になっているわけではないが、コビットによって対応することにより、プロセスの品質が格段に向上する。何よりも、可視化ができ、やっていることが見え、PDCAが回しやすくなる。何らかの形でフレームワークがなければできない。日本できちんとしたフレームワークがあるとよいが、フレームワークといえばアメリカが得意なので、すぐアメリカからもってきたりしてしまう。セキュリティで言えば、ISMSより先にBS7799といった仕組みが動いていたので、それを取得するといったことをやった。ISMSでもよいが、なにか分かりやすいフレームワークがあって、それに準じてきちんとやるということがベースになるのではないか。自分たちがやっているプロセスの妥当性があるかどうかという、アセスメントのようなものは外部からみてもらう。そうすれば、コスト負担はそれ程かからないし、かなりのレベルのことができるのではない

かと感じている。

○　監査にもいろんな種類がある。技術的な監査も確かにあり、外部からの侵入テストのようなものは、ＯＳや通信プロトコルなどが分かっていなければならない。一方で、一般的な監査では技術的なところまで突っ込まないことが多い。一定のPDCAなり、リスク管理のフレームワークを前提として、それが適切に回っているかを点検することが、メインマーケットというか中心であって、その周りに惑星のように各種タイプの監査が有り得る。その一部は技術的な裏打ちが必要で、そうなればコストもかかる、という整理になるのではないか。

○　金融界以外では、事故が起こらなくても、定期健康診断のように２年に１回くらい監督官庁が点検に入っている業界はないと理解してよろしいか。もしないとすれば、何故実施しないのか。

⇒　確認しなければならないが、基本的に事業免許の更新がついている基盤に関しては、免許制度の中で、更新時に適切に検査が入っているケースはあると考えている。情報通信などでも、無線を使っているところにはあるし、一定規模のサービスを提供しているところの免許に関しては点検を行っている。発電についても更新の免許はあるので、その事業に関しては免許の中で確認をするということはある。事業に関してＩＴがどのように使われているかに関しては、業法毎に異なっており、例えば電力事業においては、電気工作物については含めて免許になっている。電気通信事業では、理由がない限り検査は行っていないと思う。分野毎にまだらになっているが、金融以外ではないのかといわれれば、そのようなことはないと思っている。

○　ＩＴベンダに対する監督官庁の監査はないのか。

⇒　ＩＴベンダを統制する業法が存在するとは理解していない。

○　基本的には、ＩＴベンダや情報サービス業者に関しては業法はないので、そういった監査は全くないと理解しよいと思う。自主的に行われているとも思えない。いま説明があったことに関して、それは業法上の免許更新に必要な検査、監査はあるだろうが、情報セキュリティであるとか、情報システムの安全性、信頼性に関しての監査が業法上行われているとは思えない。

⇒　法律の専門家ではないので、事務局には補足していただきたいが、業法では業について書かれており、業を構成するシステムに関してあるが、そこで情報セキュリティという言葉では書かれていない。例えば、参考資料１－２の１１頁目に、電力であれば電気事業法の中に書かれているが、電気を発電して売っていくことについて安定してやりなさいとなっている。その中に、電気工作物というものがあり、これは発電事業に伴うシステムのことを表しているとのことであり、なにをやるべきかということが書かれている。それは、安定供給に関してきちんとやりなさいとなっている。実際これに関して、木曽川水系でダムのコントロールシステムがバグで落ちたことがあった。これは電気事業法に基づく事故報告が行われており、安定供給面で何が問題であったかに関して、中部電力が事故報告書を作り、監督側が検査に入るということを行った。そういった構造をもっている業法もあるが、情報セキュ

リティということでは書かれていない。それが、第１次計画において事業継続性というところへフォーカスをおいた理由である。そこを外していくと、業法をてこに作用していくということでは、業法と業法に伴うガイドラインがあるが多くの場合それは効かない。事業におけるサービス供給を安定化しなさい、事業継続をきちんとやりなさいということに関しては機能する可能性があったので、そこを捉えて安全基準等に書いているのが、第１次基本計画の作戦であった。全部についてあるわけではなく、ばらばらなので、参考資料３にある安全基準等の指針において、安定供給に関してないのであれば考えて欲しいということをやりながら、業法、強制基準、ガイドライン、業界基準でもよいのでやっていただきたいということである。世の中的に問題があれば、それがエスカレーションされていくという読みの中で作っている。業法の改善の道というのは、明確に示していないが参考資料３の２頁目の上の方にある、強制基準を踏まえているというところが、業法に対して何かあったときに作用できるフックは残してあるということが、第１次基本計画の枠組みであるという理解である。明確に情報セキュリティと書けないところで、どのように泳ぎきるかということでかいてあるので、ご理解いただきたい。

○　「自己点検等に関する基準としては、経済産業省が情報セキュリティ管理基準を策定している」とあるが、この記述には不満があり、経済産業省が情報セキュリティ“監査制度”を作っている。基準だけを作っているわけではなく、監査する仕組みを作っているはずである。これを書かれて、もし良しとしているのであれば、大きな誤解をされている。監査というものを誰が担保するのか、誰が責任をとるのかということに関して、経済産業省は新しい監査制度をつくり、その受け皿としてＮＰＯの監査協会であるＪＡＳＡを作り、そこでできる限り信頼に足るものを作るべく、仕組みを作っているところである。監査人がそこで資格をとって、それは何の業法もないが、監査をしたときに、不適切な監査を行ったときにはそれを剥奪するなど、ピュアレビューをするといった仕組みが作られている。これをより活用する方向で考えていただけないだろうか。業法がないので、情報セキュリティの監査というのはつらいが、業法を作ればよいということは言わない。それをやるべきとは全く思っていない。ぐるぐる回ることによってスパイラルアップしていく、その時にどうしても第三者の目は必要である。

○　先ほどの委員からＩＴベンダには監査はあるのかというご質問があり、それはありませんということであった。ＩＴ業界がどう考えているかというと、私が関連している方々、政府等から出ている指針によれば、ＩＳＭＳへの取組みということになる。ＩＳＭＳを否定するわけではないが、これでは先の委員も納得されないと思う。私も同感であり、ＩＳＭＳは自分のセキュリティマネジメントであり、自分の情報資産が中心である。今問題になっているのは、ＩＴベンダから発注者側に対しての情報資産の取り扱い、情報知識のキャッチアップであり、情報技術の維持である。そこに関しての視点がないので、なかなか上手くいかない。その中で、この基準であれば使えるというもの、そういった制度があれば使えると思う。

○　今のご意見も含めて考えると、監査のイメージについて、世の中でいろいろなパターンが

あると認識されているのではないかと思う。技術的なところをみるレベルもあれば、プロセスをみるレベルもある。監査がどうなるべきか、どうあるべきか、どのような状況にあるべきか、どのような監査があるのか、技術的監査なのか、プロセス監査なのかという整理は、ここ何年かでしておくべきだと考える。

○　重要インフラをみたときに、現状は各業界の自主性を重んじるということであれば、各業界での Audit（オーディット）ガイドライン、金融関係では既にあると思っているが、これを作るべきである。これは管理基準と変わらないようにも思えるが、違うところは、どのように監査をするかというところまで示せれば、この業界は技術的なところまで監査するというレベルもあるだろうし、ある業界ではプロセスまでしかみませんというレベルが見えてくる。その意味で、管理基準とは意味合いが違う Audit ガイドラインが必要である。

○　いろいろな意見を伺って、データセンターの位置づけは今後どうなるかということを考えていた。米国法人を顧客とするデータセンターは、各業界のセキュリティ基準よりも遥かにレベルが高い、ここで議論されていることよりもはるかに上をいく。これは国際競争力にも繋がるものである。この辺りの動向を踏まえて議論しておかなければならない。

○　いただいたご意見は事務局の方でまとめていただき、今後の議論の方向付けに使わせていただきたい。

（4）重要インフラ関連の情報システムを含めて、事業過程の信頼性を高めるための機能に関する検討について

○　素朴な疑問であるが、「情報共有の整理イメージ」の図で、「障害の拡大防止・復旧のため必要となる情報」として整理してある事項が、「１．サイバー攻撃」の欄にしか記述されておらず、「２．非意図的要因」、「３．災害」　に関しては、必要となる情報の事項が空欄のように見受けられる。空欄であるのなら、ここを早く埋めなければ大変なことになるかと思う。

○　図の表記の仕方であり、文字を枠内で上詰めにしている。青い網掛けの範囲で、ここに記載されている必要な情報の列記は、「２．非意図的要因」、「３．災害」の場合にも含まれるものである。この図はあくまで、整理のイメージではあるが、脅威の種類と、その際にどのような共有すべき情報があるかということで示している。表の白い部分については、ここはないのではないかということで空欄で示している。「３．災害」についての「予兆・警報に関する情報」は、地震といったものを想定しているが、ＩＴに関してお知らせするものはないのではないか、事務局として、イメージ、考えが至っていない部分である。「インターネットの基幹システム（ＩＸ、ルートＤＮＳ等）への攻撃」については、こちらで担うところではなく、一般に公表されているということもり、ここでの対象としては考えにくいかということで、空欄にしている。

○　同じく、情報共有の整理イメージで、「１．サイバー攻撃」については、過去にあったホームページ改ざんやウィルスが炸裂したなど、そういったことから整理されていると思われる。

サイバー空間で、非常に閉じているハッカー、ウィルスにとどまっている気がする。一方で、重要インフラに関しては、やはりサイバーテロといった脅威があり、もしテロがあるとしたら大変だということが起点であれば、国内外の犯罪組織の情報、テロ組織の情報といったことを含めて、情報は共有すべきだと思う。銀行が止まる、証券取引所が止まるといった攻撃はあるにせよ、サイバーを使ったリアルに関係するような攻撃が一番怖い。そういった海外の情報、国内における犯罪の情報等を含めた情報は共有すべきであり、それが起きたときどうすべきかという技術的な情報も加えるべきである。

○　起きた後の情報、「障害の拡大防止・復旧のため必要となる情報」について、事業者等から所管省庁を経てNISCに行くようになっているが、内容にもよると思うが、明らかにテロのようなものがあった場合に、本当にこのフローで良いのか。本当にこれはテロ行為だ、というようなものがあったとすれば、事案対処省庁のようなものがいち早く情報を掴み、対応すべきだと思う。ものにもよるが、そこは随時きちんと判断をした上で、手遅れにならないようなフローになればよいと思う。

○　今の委員の意見に全く同意である。「障害の拡大防止・復旧のため必要となる情報」が１つの枠で括られ、「１．サイバー攻撃」、「２．非意図的要因」、「３．災害」の場合の全てに掛かっていることがピンとこない。サイバー攻撃に対しては、これはある意味で犯罪なので、犯罪に対処する話と、非意図的にプログラムがバグったというような話は、対処方法が異なる。そこを明確にしなければ、起きたときに対応できない。ＤｏＳ等が連続的に起きているときは、迅速に動かなければならず、後でのんびりやるというような話ではない。示されているフローは、先の委員が述べられたように、のんびりしている気がする。具体的に申し上げれば、犯罪捜査に関係する官庁は当然警察になるので、そういったところと相当緊密に情報連携しながら、迅速に動かなければ、防げない、かつサイバーツールに対する逆アッタクもできない。「障害の拡大防止・復旧のため必要となる情報」の括りは、「１．サイバー攻撃」、「２．非意図的要因」で異なるのではないか。

⇒　現在の第１次基本計画における行動計画の中で仕切り、やり方があり、参考資料１－１の５頁に示している。この全体の構造を検討したときに、犯罪対策やサイバーテロに関しての迅速な事案対処省庁に関しては、この計画外であるということを、当時いろいろな理由から決めた。他の省庁がやっていることを全て含めて、この計画に書いているわけではなく、また犯罪対策については、第１次基本計画の中でも取り扱う部分、横断的な情報セキュリティ基盤の形成において犯罪の取締り及び権利利益の保護・救済がある。犯罪捜査に関しては、警察庁が警察組織として行っており、第１次基本計画の犯罪対策の枠で取り扱うことが前提であろうということである。これは評価との関係があり、計画を立てた場合には、評価を行うことが政府の中では必要であり、犯罪対策は別にしてまとめておかなければ、犯罪があって、それに対してどう動いているのかを評価するためには、ちらばっているのはよろしくないということが、警察庁との話の中でもあった。また、事案対処省庁を含めた、この計画の一番大きいところは、レスポンスよりもプリペアードネスというところがあり、情報提供を

どのように行い、それが事業者の自主的な取組みの中での事業に対して適切に展開していくかというところで作られている。レスポンスに対して、どのようにやっていくかということは、これからの議論を待っているところである。実際、警察庁さんの方から提案があり、プリペアードネスだけではなく、レスポンスを考えたときに、警察庁を含めた事案対処省庁の取組みに関して議論していただけないか、ということがあった。今度、重要インフラ専門委員会の下に、ワーキンググループを設置し議論していくことになっている。行動計画の中では、犯罪対策という観点では、全て外枠であるとした。これは、はっきり言えば、政府の都合上である。サイバーテロについては、業法では具体的にどうするか書いていない。唯一あるとすれば、武力事態等に対する対処法というものがあり、国家でどう動くかということが書いてあるが、武力事態と書いてあるくらいなので、その事態には、ＩＴに起因する事態は定義されていない。そこに定義されれば、他のフレームワークがあるかもしれない。そういったことも含め、合理性と適切性の中で、法律との関係も含めてどうするか、もう一度考えるワーキンググループである。第１次基本計画のときには、各種いろいろな経緯から、このような枠組になり、その中で動いている。経緯について、私は当時不適切であったと思っているが、何も動いていない中で、動かす必要があったので、その中で考えた。

⇒　世界中が失敗している重要インフラ政策は何かというと、ビジネス・コンティニュイティーに中心を置いているところと、法執行機関の活動に中心を置いているところを混ぜたときに、世界中が失敗している。個人としては、分離して作るほうがよいと思っている。実際に、そうでなければ身動きが取れなくなるケースがたくさんある。よく言われるが、トラブルが起きているときに、その証拠を採るのか、復旧にがんばるのかという取捨選択は事業者に任されている。それが参考資料１－１の５頁にある、「犯罪被害等の通報は自主的な判断に基づくもの」というものである。これは事業者から書いてくれと言われたことでもあり、外枠にしている。そのような経緯もある中で、ここはセンシティブな部分であり、いろいろな意味で事業者の都合というものがあり、不都合が起きないようにした結果である。主張としては委員が述べられる意見は分かるが、計画として調整していく中で、コンセンサスの形成ができなかった。そこはご理解いただきたいというのが、私からの意見である。

○　状況と第１次計画時の判断は分かった。第１次計画の時と比べると、はるかに状況が複雑になってきており、大変な状況が起きうる状況にもなってきていると判断している。この中でさりげなく書かれているが、IX やルート DNS が攻撃されれば、完璧に止まってしまう。こういったところを、なんとなく“犯罪らしいよ”ということでのんびりやっていてよいのか、非常に危機感を覚える。

○　「インターネットの基幹システム（IX, ルート DNS 等）への攻撃」に関して、共有する情報が空白になっているのは、何もやらないということではなく、情報共有のイメージとしては書きようがなかったということである。ルート DNS である M-Root のオペレータとして言わせていただくと、ルート DNS を攻撃する方法はオペレータとしてまじめに考えており、国際的な枠組でもやっている。IX にしても、いろいろなことを考えてやっており、どう整理するか

ということに関して、この空白の部分は何もやらないということではない。ルートDNSのオペレータが日本国政府から何か言われても、困るだけである。ルートDNSの実態については世の中は無理解であり、その意味では、この空白部分をどう実行的にやるかということは考えなければならない。しかし、この部分について事務局を含めて、日本国政府が計画として書くことがあるのかといったときに、ルートDNSは書きにくい。IXは総務省の方とかなり相談したが、非常に書きにくい。政府に付き方がなかったので、空白にしている。

○　「障害の拡大防止・復旧のため必要となる情報」の書きぶりが、「１．サイバー攻撃」、「２．非意図的要因」では、やはり違うのではないかということである。「障害の拡大防止・復旧のため必要となる情報」もしくは対応は、1.と２．では違うのではないかという気がする。

○　サイバー空間上のことで考えれば、今述べられたようなことだと思うが、私は物理的なテロと併用するであろうと思っている。そのような対処法は極めて複雑で難しくなるのではないか。そこまで書くかどうかはあるが、「障害の拡大防止・復旧のため必要となる情報」の書き方は、かなり違うのではないかという気がする。

⇒　事務局としては、この委員会と重要インフラ専門委員会の担当の切り分けをしている。重要インフラの行動計画の中で関係省庁をどう位置づけるかについて、重要インフラ専門委員会の下にワーキンググループを作っており、そちらで、専門家、関係省庁を入れて検討させていただきたい。ただ、ここは非常に悩ましいところだと思っている。原因を究明することを考えると、①まずどういうことがなぜ起きたのかを明らかにして、早期復旧、再発を防止する、他の人に影響が及ばないように障害の拡大を防止するというものと、②誰がミスをしたか、誰が悪いのかという責任追及の２つがある。どちらも大事なことで、両方やらなければならないことである。しかし、しばしばその両方が現場サイドで矛盾するため、今の基本計画では事業継続性を扱う重要インフラ部分と、責任追及を扱う犯罪対策部分を書き分けている。

○　当事者の警察庁として発言させていただきたい。先ほどご説明があったが、重要インフラ事業者の方々が警察が入ることについて、どうお考えかということに関して、我々としてはそこまで嫌われているという認識はないが、入ってくれるなというご意見があるのかもしれない。ただ、先ほどあったように、「事故前提社会への対応力強化」ということで、何か起きたときにどうするのかという対処になると、一般的な事故は格別、サイバー攻撃ということになれば、警察が対処せざるを得ない。平成１２年に起きた各省庁のホームページ改ざん事件、某国からソラリスのカレンダーマネージャ・デーモンのセキュリティホールを突いて改ざんされるという事案が続き、実際は警視庁が行ったが、そういった情報を総務省へ提供し、対処したという経験もある。こういった我々が持っている知見、技術、海外から寄せられる情報、警察が実施する２４時間監視におけるネットワーク上のボット、ウイルスの情報を使い、そういったものの防止、あるいは被害が発生したときの対処について、２４時間営業している警察としてどのようなことができるかについて発表して欲しいと、重要インフラ専門委員会の浅野委員長の方からお話があり、7月18日の重要インフラ専門委員会において発表

させていただいた。7 月 24 日には、何かできそうだということで、警察と防衛について、どのように組み込むかということについてお話があった。先ほどあったように、概念的には犯罪捜査は切り分けられるが、現場での対応は一体となって行われる。確かに、平成１２年にあったホームページの際も、警察がいろいろ行い、また、確かに平成４年頃には、プロバイダーへ行き、捜索、差し押さえすると、サーバそのものを持って帰ってしまうという暴挙を行ってしまい、その後の信頼を失ってしまった。現時点では 1,000 名を超える技術者がおり、そういったことは決してないので、ご信頼いただければと思う。今後、皆さんのご議論の中で、我々事案対処省庁として、どういったことができるのかということも、横串という形でご検討いただければと思う。

○　事務局から説明があったように、これについては、責任追及と早期復旧の再発防止という両面を区別して検討いただく、重要インフラ専門委員会でも検討いただくことになっているので引続きそれを注視していきたい。本日発言いただいた意見も、当然の発言であるので、要ウォッチということになろうかと思う。我々の基本計画検討委員会の方でも、考察を深めて行きたい。

○　本日発言いただいた意見も事務局でまとめ、委員の方々が一覧できるようにし、今後の基本計画策定に役立てたい。

（５）防護すべき重要インフラサービスの定義と維持すべきサービスレベルの検討について

○　先ほど監査の話の中で、コストについての話があったが、完璧にするということではコストがかかるというのは問題の一つだと思っている。セキュリティはやればやるほど金がかかる、かけない方法もあるにせよ、基本的には金がかかる。どのようなサービスでどこまでやるかと考えるときに、大きな問題として、コストは検討するお題目の一つにしなければならない。なんとなくこのサービスはこのくらいか、と決めてもどうかと思う。

○　セキュリティホールを突き詰め、ＩＴ業界はだめだからバグだらけだといっても、結局は同じ人間がやっていることなので、自分たちで工夫し、品質向上することについては自動車会社のように一生懸命やるにせよ、いずれはコストに跳ね返ってくる。そんな金は払えないが、セキュリティレベルはこれだけにせよ、例えば５分で復旧する証券システムを作れ、と言われても無理なので、無理なものを提起しないようにしていただければと思う。

○　これは大括りの抽象論でも議論されたところであり、それを踏まえられたご発言だと思う。無理難題を事業者に押し付けても、これは実行不可能になるので、その辺は考慮しなければならない。

○　サービスレベルを出していただき、理解していただける形にしていくことには賛成である。手法的な話になるが、広くサービスを洗い出す、客観的にやることには無理があるかと思う。このサービスレベルとはセキュリティ上のサービスレベルだと思うので、セキュリティ報告書を出していただくということ、これらを収集するなり何年か重ねていただくことにより、

結果として日本の電力会社や通信事業者のセキュリティにおけるサービスレベルはこのようなものであると、現実とマッチングさせていかなければならないと思う。その意味では、セキュリティ報告書を広く公開しながら、それをもってサービスレベルを定義していくという形にもっていくべきである。

○　５分で立ち上がるシステムは確かに難しいが、そういった業界で何年も仕事をして、概念を変えるべきだと思っているのは、バグのないシステムは作れないという話と、バグを発生させてトラブルを起こしても構わないというのは別問題であり、その意識改革をきちんとしなければならないということである。そうしなければ、すぐ金をかければよいという話になってしまう。知恵を使えば、完全にバグを除去することはできないが、技法によっては極めて精度の高い、品質の高いシステムを作る方法はいくらでもある。現実に研究もされている。ただ、それをきちんと担って、実行していく人材が育っていないという大きな問題はあるが、技法がないわけではない。そういったところも勘案しながら、重要インフラをどう作っていくか、システムどう作っていくかということを議論していただかないと、バグのないシステムは作れないということを金科玉条のように言われるのは、非常におかしな世界であると思う。むしろ、バグが出ても止まらないシステム、バグで止まった場合に人手でカバーするということも含めたトータルシステムコンサルなど、考えなければならないことはたくさんある。バグがないシステムは作れないということを許すと、思考が停止してしまうので、その意識改革は非常に必要だと思う。

○　今の話を伺って、思ったことであるが、政策として重要インフラにおける人材教育というものは何かやっているのか。やっていないとなると、今の話も含めて、重要インフラとしての人材育成は少し違うので、考えるべきかと思った。

　⇒　行動計画の中では人材育成をきちんとしなさいということは書いてあり、それを受けて人材の委員会では議論をしていた。そこから各省庁を含め、政府として何か組織だった対応ができているかというと難しいというところではある。正確に述べると、情報セキュリティ人材に関しては、行動計画の中でがんばろうねということであるが、先の委員が述べられた意識改革型についてはないということである。

○　人材育成をしましょうということでレポートをまとめさせていただいた一人であるが、それを受けて産業構造委員会で、情報処理技術者育成等々に関する審議や仕掛けをいろいろ作り、その中で、情報セキュリティ人材を育成していくということ自体は反映させたつもりである。まだ実行がかかっているところまでいっていないが、育成のカリキュラムというか、スキルレベルの話や試験制度等々については、経済産業省、ＩＰＡを中心に、進捗中であると認識している。

○　先ほどデータセンターの信頼性に関する話があったが、アメリカではデータセンターのレイティングをティア（Tier）１からティア（Tier）４までやっている。日本のデータセンターでは認定を受けたところはまだないと思っているが、そのような枠組でレベルを保証していくとか、重要なものはこのレベルであるとか、そういったものと関連づければ、分かりやす

くなるかとは思う。

○　公式か非公式かは分からないが、アメリカの基準による水準を公開している日本のデータセンターもある。ただし、日本のデータセンターでそこまでいっている、自信のあるところは少ないと思う。

○　それを使ってやるということは、ものすごく敷居が高いが、レイティングとしては分かりやすい。何らかの形としてのレイティングがあれば、非常に分かりやすい。

○　あの基準での一番目は、ものすごくレベルが高く、軍事的にあらゆる攻撃に耐え得るということで、国防総省以外ではほとんど不可能ではないかと思っている。２番目であれば、ビジネス施設としては最高水準だと思う。指標がたくさんあるので、そういったもので可視化できるので、それらを見て動いていただくということも、今委員が述べられたように重要かと思う。政策的にも、そういったものはウォッチし、取り入れられるものは取り入れるということだろうと思う。

○　SLA、サービスレベルアグリーメントという形で、セキュリティについてもアウトソーシングを行う場合には、SLA で規定しないといけなくなる。私が関わったところで、甲府市役所の新しいシステムは、全面的にサービスレベルアグリーメントも含めて、セキュリティ水準の数値的指標を作り、それを達成できれば、契約どおり支払うが、例えば月単位に達成できない場合は、契約以下の金額を払うということを決めている。これは業界、ＮＩＳＣ、総務省が何か言ったというわけではなく、個別契約において自治体と複数の事業者で決めている。もちろんこれは、総務省のガイドラインをはるかに上回る水準で設定されている。そのような動きも出てきているということである。今日の議論で規制か自由か、ということがあったが、そういった動きも念頭に置きつつ、契約というものが今後重要になる。グローバルな動きへの対応を、どう考えるかという意見もあったが、そういう動きでソフトロー的な動き、ハードロー的な動きの両面をにらんで検討すべきだろうと思う。その辺を無視して議論すると、おかしなことになるだろうということであると思う。

○　これまでの議論を事務局でまとめ、整理し、基本計画のために発言を活用する形になる。そこで、この委員会でまたご検討いただきたい。さらにご意見がある方は、いつものように事務局にご提出いただきたい。

（６）今後のスケジュール説明

○　事務局から、今後のスケジュールについて説明がなされた。

－　以　　上　－