サイバーセキュリティ戦略本部
第14回会合　議事概要

１　日時

平成29年7月13日（木）　　８：30～９:30

２　場所

総理大臣官邸４階大会議室

３　出席者（敬称略）

菅　　義偉	内閣官房長官
丸川　珠代	東京オリンピック競技大会・東京パラリンピック競技大会担当大臣
松本　　純	国家公安委員会委員長
鶴保　庸介	情報通信技術（ＩＴ）政策担当大臣
岸　　信夫	外務副大臣
松村　祥史	経済産業副大臣
金子　めぐみ	総務大臣政務官
宮澤　博行	防衛大臣政務官
遠藤　信博	日本電気株式会社代表取締役会長
小野寺　正	ＫＤＤＩ株式会社取締役会長
中谷　和弘	東京大学大学院法学政治学研究科教授
野原 佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
林　紘一郎	情報セキュリティ大学院大学教授
前田　雅英	日本大学大学院法務研究科教授
村井　　純	慶應義塾大学環境情報学部長・教授
萩生田 光一	内閣官房副長官
杉田　和博	内閣官房副長官
髙橋　清孝	内閣危機管理監
中島　明彦	内閣サイバーセキュリティセンター長
古谷　一之	内閣官房副長官補

４　議事概要

（１）本部長冒頭挨拶

早朝からお集まりいただき、感謝申し上げる。

本日は、３点にわたり、御議論をいただきたい。

１点目は、「サイバーセキュリティ戦略中間レビュー」についてである。これは次期戦略の策定を見据えつつ、現行の戦略で加速・強化すべき施策を取りまとめるためのものである。本年１月及び４月の会合における議論を踏まえ、IoT機器を遠隔操作しサイバー攻撃を実施する際に用いられる、いわゆるボットと呼ばれる不正プログラム対策の推進、また、官民が連携し、分野を超えたサイバーセキュリティに関する情報の共有を図るためのネットワークの構築・運用、そして、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体制の整備、ここを柱としたいと考えている。

２点目は、2017年度に重点的に取り組むべき施策を取りまとめた「サイバーセキュリティ2017」のパブリックコメント案である。ただいま申し上げた「サイバーセキュリティ戦略中間レビュー」に掲げた施策についても盛り込みたいと考えている。

３点目は、「サイバーセキュリティ研究開発戦略」についてである。これは将来的な研究開発のビジョンを提示するものであり、「サイバーセキュリティ戦略中間レビュー」で示す方向性を踏まえつつ、既存の研究開発戦略の見直しを行いたいと考えている。

限られた時間ではあるが、是非よろしくお願い申し上げる。

（２）討議

【決定事項】

・サイバーセキュリティ政策に係る年次報告（2016年度）について
・サイバーセキュリティ2017（案）について
・2020年及びその後を見据えたサイバーセキュリティの在り方について
・サイバーセキュリティ研究開発戦略について

【報告事項】

・サイバーセキュリティ基本法第25条第１項第２号に基づく監査の報告について

上記について、事務局から資料に基づき説明が行われるとともに、本部員より意見が述べられた。

○（林本部員）

決定事項等に異論は全くないが、2020年以降を見据えたサイバーセキュリティの在り方に関して、３点ほど補足させていただく。

まず、第１にボットネット撲滅対策を取り上げるのは、かつて成果を上げたサイバークリーンセンターを復活させることが、誰もが知っているが実際に行うことは難しいテーマに注意を

喚起する施策として、有効だと考える。しかし、せっかく取り上げるなら、情報システムを総点検して、ウイルスに感染したり踏み台にされたり、知らないうちにデータが漏えいしていないかなどを確認しておくことなどを、包括的に国民的な共通認識にしていく必要があると思う。

アメリカのサイバーセキュリティ情報共有法は、私企業は自身が所有する情報システムはもとより、相手方の書面による同意を得れば、他社のシステムをモニターすることができ、これには連邦政府のシステムが入ることを明確にしている。一見すると義務を強化しているように見えるが、その義務を履行するための措置を合法化したり、あるいは免責したりする機能、つまり、権限を強化する面もあることも忘れてはならないと思う。我が国にも、不正アクセス禁止法におけるアクセス管理者による防御措置があるが、これに該当しない方法によるセキュリティ侵害も含めて、システム所有者の権限を明確にすることがよいのではないかと思う。

第２点は、インターネットの自律・分散・協調という仕組みは、何らかの策を講じなければ防御側が攻撃側よりも不利にならざるを得ない点である。先ほどのボットネットはまさにその好例であるが、守る側は100％の防御を求められるが、攻める側は一点突破を狙ってくる。しかも、一点突破されれば次第に拡散していくため、不利にならざるを得ない。

これに対して、先進諸国は適切な防御策を考えるため、いろいろな工夫をしているが、中でも注目されるのが、イギリスのレギュラトリー・サンドボックスではないかと思う。これはブロックチェーンなど、いわゆるフィンテックの普及促進を図るために、官民合同であらかじめ安全な実験的空間を設定して、その中で不確実な技術を使ってみようという試みだが、サイバー対策にも適用可能ではないかと思う。

例えば、検体を捕捉してワクチンを開発することや、対策として何が有効かを試すことは、社会的には有益だが、法に触れる実験が含まれることもあり得る。開発者、教育者、あるいは演習に携わる人は、その点で苦労していると思う。こうした懸念を払拭して、心置きなく開発や教育に携わることができるような工夫として、一考に値するのではないかと思う。

このような仕組みは、あくまでも民間主体の努力を政府が支援するという形をとるため、時間がかかったり即効性が劣ったりしがちである。そこで、第３点として、強制力のある措置についてどう考えるべきかを明確にしておく必要があると思う。コンピューターウイルスもウイルスの一種であるという比喩を使えば、感染症予防法にあるように、患者を発見した医師の保健所への通知義務とか、重症の患者の隔離といった、いわゆる強制的な措置が頭に浮かぶこともある。

しかし、反面教師になるが、他国のサイバーセキュリティ法では、情報の自由な流通よりも国の安全が優先される結果、国家の直接規制が前面に出て、加えて、刑事罰も法定されているものがある。強制措置をここまで強化すると「角を矯めて牛を殺す」ということにもなりかねない。

これらの施策はいずれも、一義的には民間の自発的取り組みを基本にして、政府はその支援や助成に徹することを併せて明確にしておくことが必要だと思う。

以上、何らかの御参考になれば幸いである。

○（前田本部員）

私も、林本部員と同じように、この決定事項４点に全く異存はない。ここでの御議論を踏まえて、非常に洗練されたものになっていると思う。

これに関連して、「サイバーセキュリティ戦略中間レビュー」を中心に、ボット撲滅の推進、情報共有・連携ネットワーク（仮称）の構築・運用、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体制の整備について１つずつ、最後に「サイバーセキュリティ研究開発戦略」について一言申し上げたいと思う。

私は犯罪関係が専門だが、業界に「検挙に勝る防犯なし」という言葉がある。捕まえる、たたくということが、何より犯罪のようなものをなくすために大事だという考え方である。学問の世界も動きがあり、起こらないように抑止することも大事であり、起こるような環境をなくしていくことも大事とされている。ただし、いろいろな局面があるため、どれが一番大事かは決められないと考えている。

今の状況の中で、ボットネット対策を講じて、そこに力を入れるということは、時宜を得た非常に正しい政策であり、是非前向きに進めていただきたい。ただ、起こらないようにする、起こった後にどうするかということにも関連して、情報共有・連携ネットワーク（仮称）は、最終的に起こったことに対処する機関に向けて、そこに収れんする形の連絡といったような、情報の合理的な配分が重要である。NISCはだいぶ洗練されてきたといっても、霞が関にはまだ合理性のない障壁が残っているような感じがしており、是非一体となって解決することにつながるようなシステムの実現を目指してほしい。そのときには、NISCの存在は非常に大きいと考えている。

2020年東京オリンピック・パラリンピック競技大会の関連で、資料３－２の中で使っている「連接融合情報社会（連融情報社会）」という言葉がある。これが意味するところは、実社会と情報との連続性というか、もう分けて考えられない完全にまじり合っている状況である。こういう新しい状況の中でどうしていくか。それぞれの悪いものと悪いものが足して２になるのではなくて、それが何乗にもなっていくようなもので、それに対応することが必要だという御指摘は非常にそのとおりだと思うが、まずは2020年東京オリンピック・パラリンピック競技大会に向けて実社会と情報社会とのつなぎ合わせで若干気になるのは、それぞれがばらばらにやっていることである。

警備をきちんとやらなければいけないし、事故が起こらないようにしなければいけないし、事故はサイバーの中で起こるものもあるし、そうではないものもある。それを全体として見る制度や仕組み、そこの運用の仕方についても、いろいろなところで伺っていると血管が通っていないような感じがする。抽象的な言い方で申しわけないが、サイバーの情報収集の中の連続性、もう一つは実社会とサイバー社会の関連性の強化を是非お願いしたい。

それにつながるのは研究開発の問題であり、今回の御提案も非常に私はタイミングがいいものだと思う。人文科学、社会科学も入れて、サイバーの問題について根本から考え直すことに

取り組んでいかれるということは、まさに必要だが、御承知のようにこういう問題について、人文とか社会科学も含めるとだけ言うと百家争鳴になりかねない。それをどうまとめ上げていくかというと、やはり軸が必要なのだと思う。

その中で、NISCの存在は非常に大きい。今までの伝統的な学派とか業界の利害とか、自分たちの学問から見て絶対に許されないということにこだわっていると前に進めないため、そこはひとつ上から少し強引でも前に進める主体としてのNISCのサイバーセキュリティの将来像構築が必要になる。ただ、一つだけ申し上げておきたいことは、急いではいけないということである。取り組まなければいけないが、事態の動き方はものすごく速い。NISC自体が権威になって固定化してしまうと、足を引っ張ることになるため、一番大事なのは、人材を集めること。村井本部員が前から発言されているように、サイバーの問題の日本の最高の知能をNISCに集めるのだと述べていたことを、今こそというか、ここの分野こそ考えていただきたい。

○（村井本部員）

ボットが話題になるが、基本的に我々専門家にとっても、IoTの時代がこれだけ早く到来するとは思っていなかった。例えば、ボットは監視カメラを攻撃の踏み台にしたが、これは監視カメラがフルスペックのコンピューターになったということである。インターネットはコンピューターのネットワークだったが、監視カメラ自体、すなわちモノ一個一個がインターネットにつながっているフルスペックのコンピューターになるため、そこが乗っ取られると、そこから攻撃が可能になる。昔はパソコンとかコンピューターだったが、今は監視カメラ、すなわち全てのモノがボットになり得るというのが、このボット対策の意味であり、それだけ小さなコンピューターが発達してIoTの時代が来たということだと思う。

IoT時代を背景にすると、最も重要なことは、各分野がそれぞれの恩恵を受けるということである。例えば医療の分野では、今まで薬を間違えてはいけないということで、RFID（電子タグ）をはじめとしたいろいろなデジタル技術を使っていたが、それぞれが自動化、装置化すると、これが先ほど申し上げたフルスペックのコンピューターになる。誤りは少なくなり、今まで手動でやっていたものが自動化されるということでもある。農業も、今、肥料や農薬をまくために使うファーティライザーは、センサーで土壌の状態を測り、肥料の量をコントロールする。これは肥料会社にとっては、肥料の在庫が農家にあるかどうかを自動制御してそれを配送するようなことにつながっていく。つまり、農機がロボット化している。

このように現場が全てIoT化していくなか、現場のオペレーションは、それぞれ所管の省庁が違う。したがって、縦割りが起こってしまい、これを共通に解決することができない。サイバーセキュリティもそれをやらなければならず、「サイバーセキュリティ研究開発戦略」が議題に挙がっているが、研究開発も同様である。研究開発も農業の研究開発、医療の研究開発、農林水産の研究開発とそれぞれあるため、それぞれがサイバーセキュリティに対応しなければいけない。きちんと縦を横につなぐことを考えることが、内閣やNISCの役割ではないかと思う。交通、エネルギーは当たり前だと思うが、これもそれぞれ担当が違うため、きちんと連携する

こと。これが内閣の大変重要な役割だと思う。

もう一つは、IoTで恩恵を受けるのはどこか。CeBITでもヨーロッパの人々と議論したが、恩恵を受けるのは地方である。SME（中小企業）が変わる。ここに期待がある。しかし、ボットは分散化する。つまり、IoTは分散化するため、地方自治体との強い連携が必要である。民だけではできないため、地方のSMEを強くし、サイバーセキュリティの面での連携を推進していくことが必要だと考える。

最後に、人材の件について申し上げる。人材に関しては、様々なことができてきており、進んでいると思う。ただ、私が是非準備すべきだと思うことは２つあり、１つは、母数がいくつかということの明確化である。この国はどういうクラスの人材が何人必要なのか。例えばオリパラまでにどの程度必要なのか。この母数を目標値として、その目標を追いかけ、その達成度を見ていかなければいけない。いろいろなレベルがあるので、母数の調査をきちんとしておいたほうが良いと思う。何人育成できるかというフォアキャスト（予想）よりも、何人必要なので、何人育成するというバックキャスト（調査に基づく再構成）が望ましいのだから、母数の目標値を持つべきである。

更にもう一つ、教材が古くなってきている。教材が古くなると、それを使用して育った人材は、教育が不十分な人材になってしまう可能性がある。したがって、そのリポジトリ（集積所）を持っておいたほうがいいと思う。教材リポジトリである。それをよくしていくのは、みんなの力でできる。技術がどんどん変わっていくため、教材のR&Dが必要である。人材育成の仕組みのR&D、調査をして、開発する。この仕組みが全体として必要ではないかと思う。

○（遠藤本部員）

決定事項に関することに異論はないが、その中から幾つかコメントをさせていただきたい。

まず、情報共有・連携ネットワーク（仮称）には非常に大きな期待をかけている。この中で官民を挙げて作り上げていかなくてはいけないと思っていることは、このネットワークの機能の充実化である。ここでは、集約・分析、対策ということが挙げられているが、特に分析などはビッグデータ、AIというものが絶対に必要になってくるため、こういうものを入れ込んだネットワークの機能の充実化が必要であろうと思う。しかし、これは日本だけではできない状況になってきているのではないだろうか。そうすると、海外との連携を含んで、こういう部分のレベルアップを図っていくことが必要だろうと思う。

２つ目は、村井本部員も発言していたが、人材の観点である。情報処理安全確保支援士というものが、この４月１日に初回登録が実施され、約4,200名の方が登録した。弊社もこれのうち10％ぐらいの人数を出しており、貢献をさせていただいているが、実際には、村井本部員の発言にあったように、この登録者のレベルアップをどのように図っていくのか、ただ登録して何人いるかという確認だけではなく、どうやってレベルアップをしていくのかが重要である。その中では、先ほども申し上げたように、海外との連携または海外にも派遣をしながらレベルアップをしていくというような仕組みも、この中で作っていく必要があるのではないかと思う。

我々日本としては、国際的なセキュリティ資格の標準を日本で作るのだというぐらいの意気込みを持って、人材の育成に関しては積極的に関わっていく必要があろうと思う。

３つ目は、いわゆるIT立国日本の構築に関する件である。これは既にSociety5.0という日本の大きな方向感を定めており、資源を持たない日本として非常に重要な方向感が示されたと思う。その中で、IT立国としての底上げが必要だが、ICTが順調に力をつけて、価値を創るものができ上がってくるためには、サイバーセキュリティに対応したセキュリティプラットフォームの上にサイバー空間が乗っかっていないと、価値を創り上げることができないと思う。

その中で、我々が一番注力しなければいけないことは、中小企業のITの強化であろうと思う。中小企業がITの力を付けていかないと、これは前も申し上げたが、IoTというのは実は排他的な仕組みである。IoTに入るためのインターフェース、IoTに入るためのネットワークのセキュアードというものを自ら保っておかないと、IoTの中には入れない。IoTの中に入れないということは、IoTで創り上げるサイバー価値を受け取れないということなので、中小企業のITの強化は絶対に必要である。

そのためには、サイバーセキュリティのサービスがどういうサービスを提供しているのかという認定、または認証制度の確立が必要であろう。今は手を挙げて、とりあえずこういうセキュリティの対応をしているというところをまず一つのベースにしているが、そのレベルが一体どのぐらいのレベルなのかという認定の仕組み、これは経済産業省がいろいろ考えているが、是非その部分の確立が必要であろうと思う。

また、Society5.0を創り上げていく上では、研究開発は絶対に必要である。サイバー空間は特別な空間ではなくて、人間社会の価値を創る空間であるという定義の基に、人間社会とサイバー空間のなじみ方、人間社会の価値の観点からのサイバー空間の必要性、またはサイバー空間への貢献の有様、その部分をしっかりと考えていくということが必要であろうと考えている。

最後は2020年東京オリンピック・パラリンピック競技大会について申し上げる。あと３年ということと、その前年にはラグビーワールドカップも開催される。そのことを考えると、サイバー空間でのセキュリティの指揮命令系統の早期の構築が必須であろうと思う。

これはステップ・バイ・ステップの確認が必要だが、特に人のアサインメントが重要である。ハイアラーキーになったときに、上のほうのレベルでのアサインされた方たちがどういう機能を持って、次の実際の物理的な領域の人たちにどういう命令をするとか、どういうオーダーを出して、どういう確認をするのか、そこのところの確認が絶対に必要であり、３年というのは非常に短い期間であるという気がする。予算も含めた実効的な行動が必要だと思っており、是非官民を挙げて取り組んでまいりたいと思う。

○（小野寺本部員）

今回の決定事項について全く異論はなく、ステップ・バイ・ステップではあるが、サイバーセキュリティについてそれなりに進展はあると私は思っている。

その中で３点申し上げるが、１つはIoTの問題である。IoTの産業面では遠藤本部員の発言の

とおりだが、通信事業者側から見ると、全く認証も何もなしの監視カメラなり、ビデオレコーダーなりが既に普及しており、全くわからないうちに入ってしまっている。これをどうするのかということが非常に頭の痛い問題に既になっている。

移動体通信事業者のグローバルな集まり、GSMAという業界団体があるが、ここの中でもIoTをどうするかという議論がある。特にこれは米国の事業者が一番危機感を持っており、全てを監視するということは不可能に近い。オペレーターが幾ら取り組んでもどうしようもない部分が既にあるということが、通信事業者から見たIoTのセキュリティの非常に大きな問題点と既になっている。

その中でも議論があったのは、誰がどこを守っていくのかということである。つまり、誰かが全てできる話ではなく、多層的にやらざるを得ない。例えば、通信事業者はネットワークについてはここの部分はきっちり守りましょうということや、IoTの端末が全くわからなくなっているから、これをどうコントロールするのかは一体誰がやるのだということ。この辺を考えていかないと、既に問題になっている。

監視カメラでは、御存じのとおり、セキュリティも何もなしに平気で設置されていて、一般の人も見られてしまうというような、いわゆる個人情報も含めた問題が既に発生している。この多層的な防御のやり方については、国として、NISCとして考えざるを得ないだろうと思う。

それに関連して、皆さんも御存じのとおり、サイバーセキュリティとフィジカル空間が一緒になって、サイバーフィジカル空間という言い方が既にされている。そのサイバーとフィジカルの連携の部分について今回は余り議論になっていないし、これからの問題だと思うが、やはりそこをどうしていくのかを国として考えていただきたい。考えざるを得ないと思っている。

２点目は技術開発に関することだが、AIについてである。サイバーセキュリティの世界でもAIの利用が検討はされている。このAIにウイルスを仕込まれると、ウイルスという言葉がいいかどうかは別にして、AIがとんでもない誤判断をする。しかも、人間の目ではわからないものが仕込まれてしまっている。それをどうするのか。特にディープラーニングについては攻撃の対象になり得るということが、これはアメリカが中心のようだが、既に問題となっている。

日本はどちらかというと性善説にたって利用するほうを進めるが、それを悪用されたらどうなるのかということのほうがどうしても弱くなっているのが現状ではないかと思っている。このAIについても、産業界ではどんどん利用していくため、それが悪いほうに使われたときにどうなるのかということを、是非国として検討を始めないとまずいのではないかと思う。

３点目は2020年東京オリンピック・パラリンピック競技大会である。これは皆さんが既にいろいろ取り組まれており、どんどん進むのだろうと思っている。しかし、これは産業界、企業もそうだが、実はそういう組織を作れば作るほど、現場のほうは１つのままで、指示をする上のほうは組織がどんどん肥大化する。いろいろなところからいろいろなことが現場のほうに行ってしまう。現場のほうは、何かが起こったときに、上からの指示などに対応できないという状況のところに、あちこちからいろいろな問合せや指示が来る。これは民間企業も一緒である。そうなると、もう混乱するだけで、実行が伴わなくなってしまう。当然、組織をいろいろ

作らなければいけないが、その役割と指示命令系統をどこかに一本化しないと、重要インフラ事業者を含め、現場のほうは正直言って対応し切れなくなる可能性があるため、是非その点をお考えいただきたい。

○（中谷本部員）

私からは５点申し上げる。

第１に、大学におけるサイバーセキュリティ対策についてである。大学の多様性を反映して、各大学のサイバーセキュリティへの取り組みには差異があると思われるが、個人情報の保護は各大学に共通の課題であり、主に理系においては特許を初めとする知的財産権の保護や、実験施設が機能不全になったり、暴発したりしないようにすることが非常に重要なサイバーセキュリティ対策となる。大学が必要なサイバーセキュリティ政策を推進できるよう、政府には必要な予算や人員をつけていただくことを、大学に籍を置く者の一人としてもお願い申し上げる。

第２に、サイバーセキュリティ対策のための法整備の在り方に関連して、不正アクセス禁止法に適用除外規定を置くことが望ましいと考える。現在の不正アクセス禁止法第３条では、何人も不正アクセス行為をしてはならないと規定するだけで、政府による正当行為についての除外規定がない。政府がボット撲滅のために実態把握をしようとしてアクセスすることは、解釈上、正当業務として正当化されると個人的には考えるが、同法に適用除外規定を置いてこの点を明確化することが望ましいと考える。もっとも、政府がこのような行為をしなくても、官民連携で必要かつ十分な対応が民間によってなされるのであれば、それがより現実的な対応だとも思われる。

第３に、2020年東京オリンピック・パラリンピック競技大会に向けて横断的リスクアセスメントを行うことは重要であり、特に電力、通信、運輸といった分野を先行組織として先に実施することは、これらの分野が社会・経済活動全般に影響を及ぼす分野であるために、非常に妥当な方針であると考える。さらに、匿名を含む形でのサイバー脅威情報の提供を促す環境を整備することで、情報共有、連携のネットワークを早急に構築・運用していただければと思う。

第４に、安全なIoTシステムの創出による国際競争力の強化について申し上げる。国際標準化の提案がIoT推進コンソーシアムで進められているようであり、それ自体は非常に望ましいことであるが、海外でも提案の動きがあるようだ。国際標準化は早い者勝ちの側面が強いため、完璧なものを求めて時宜を失してはならず、日本のイニシアチブのもとでの国際標準化に向けて迅速な行動がなされることを強く望む。

第５に、サイバーセキュリティの中長期的な研究開発戦略について申し上げる。資料４－１には各学問分野が位置づけられていて興味深いが、今後も一層混迷を深めることが懸念される国際社会において、我が国の中長期的な研究開発戦略において最優先させることは何かと考えたとき、いかなる未知のリスクに直面した際にも、日本国と日本人、日本企業のサバイバルにとって必要最低限の対応ができるように備えること、これを最優先させるべきだと考える。

○（野原本部員）

本会合の議題についてはは全て賛成であり、このとおりでいいと思う。

その上で、４点申し上げたい。

１点目は情報共有・連携ネットワーク（仮称）の構築・運用について申し上げる。今回、制度整備を含めた形で情報共有体制を構築・運用するということで、これは大きな進歩だと思う。しっかり検討していただきたい。

このテーマで重要なことは、脅威情報、インシデント情報を事業者サイドからどうやって具体的にどのように情報提供してもらうか、そのルール化だと思う。それについては、どういう主体がどんな情報を誰に提供するのかということ、そしてそのルールの強度というか、罰則があるのかないのか、債務規定なのかといったようなルールの強度をどうするのかといったことをどう決めるかが重要な論点だと思う。

情報提供者が提供しやすい環境を整備すると資料３－１に記載されており、システムベンダーやセキュリティ事業者に義務を課すという案があると聞いているが、そうではなく、できれば情報を持つ重要インフラ事業者が情報提供するという形で制度を作り、主体者が責任を持つような形にすべきではないかと思う。

ベンダー経由だと、クライアントである事業者との関係を配慮して、報告しにくいといった状況が生まれる可能性もある。情報を持つ事業者に責任を持たせて、日ごろから主体的にシステムの仕様や要件を決め、マネジメントをするといった環境を育てていくことのほうが重要ではないかと思う。

いずれにせよ、いろいろな案があるはずで、検討課題もいろいろあると思うので、どういう案があってそれぞれのメリットとデメリットはどうなのか、それをどういうふうに検討して最終案になったのかという検討の過程を、しっかり見える化して進めていただきたいと思う。

２点目は、2020年東京オリンピック・パラリンピック競技大会に向けて体制の整備が進められているが、それを契機にしてサイバーセキュリティ体制の見直しを一部したらどうかということである。例えば、本会合では説明がなかったが、添付されている資料３－１の中に「リスクマネジメントの促進のための取組概要」というものがあり、その中に東京オリパラ大会における重要サービス分野が設定されている。それは19分野が選定されているが、この中には８分野、重要インフラ分野ではない分野が入っている。例えば、陸海空の交通管制とか、緊急通報などがあるが、そういったものは既に国とか自治体、独法に含まれているからという話もあるようで、やはりこういう重要なところはきちんと別出しをして体制を作っていったほうがよいのではないかと思う。したがって、こういうことも含めて、2020年東京オリンピック・パラリンピック競技大会開催のために構築したセキュリティ体制をうまく契機にして、新たに全体のセキュリティ体制を見直していくということも行ってはどうかと思う。

３点目は、普及啓発、情報発信についてである。資料３－２に記載をされており、普及啓発はNISCが関係省庁と連絡し、産官学民のいろいろな主体と連携を図ることによって行うと書かれているが、これだと大変抽象的であり、これはパブリックリレーションズだと思う。メディ

ア関係者の影響力はすごく大きく、メディアがどういう報道を行うかということが一般利用者や中小企業の人たちの常識に大変大きな影響を与える。しかし、メディアの担当者が必ずしも専門家というわけではないので、適切にここでどういう報道をしたらいいのかという判断ができるというわけでもないと思う。したがって、メディア関係者の理解を深めるようなコミュニケーションというか、活動を行ってはどうかと思う。懇談会など、いろいろ考えたが、これは結局、パブリックリレーションズを戦略的に行うということだと思うので、そういう担当部署を作るとか、場合によっては報道官を置くとか、そういった形で、どうやってセキュリティ関係の普及啓発を行っていくかということをしっかり課題として受けとめて対応していけるような、戦略的な広報活動ができるといいと思う。

最後、４点目である。ボット撲滅の推進については皆さんも発言されており、私も非常に重要な施策だという意味では同意である。けれども、既に普及しているネットワークカメラやセンサー機器がボット化することを防ぐという形を、国内だけで一生懸命実績を上げても、その効果は非常に限定的だということをしっかり認識して、ボット撲滅の推進は重要だけれども、それをやったからといってIoTシステムに関連するサイバー攻撃がなくなるわけではない。それを前提に、先ほど小野寺本部員が発言したように、多層的にしっかりと対策を考えていくことのほうが重要で、IoTの環境を整備していくにはボット撲滅だけではないということをしっかり認識して進めていただきたいと思う。

○（丸川東京オリンピック・パラリンピック競技大会担当大臣（副本部長））

サイバーを含むセキュリティの確保は、2020年東京オリンピック・パラリンピック競技大会の成功の大前提であり、先般決定した大会に向けたセキュリティ基本戦略に基づき、各種対策を加速しているところである。

大会に向けたサイバーセキュリティ対策については、本日、御議論いただいている「サイバーセキュリティ戦略中間レビュー」においても重要な課題として位置づけられている。

サイバーセキュリティ対処調整センターの構築に向けた技術者との連携体制の整備や、電力、通信、交通などの重要サービス事業者におけるリスク評価の促進に加え、我が国全体としてリスク対策が最適化をされ、優先順位づけが明確となるよう、国としても横断的なリスクマネジメントを着実かつ計画的に進めていく。関係省庁のこれまでの御協力に御礼を申し上げるとともに、引き続き御協力をお願い申し上げる。

サイバーセキュリティ戦略本部の副本部長という立場で、中間レビューを踏まえ、政府全体として最適な予算や人員の確保を図るほか、必要となる制度整備の検討等、特に御指摘をいただいた、アサインされた人の権限や指揮命令系統を明確にするべき、あるいはフィジカルとサイバーの連携についてより踏み込んだ議論をするべき、また、どの分野でどのレベルの人がどのくらい必要なのか、バックキャストで必要な人材について考えるべきということについては、既に私としても意識を持ってNISCと話をしているところであり引き続き全力で取り組んでまいりたい。

○（松本国家公安委員長）

本年５月、世界規模のランサムウェア感染事案が発生し、国内でも病院、企業等で一定の被害が確認された。この種事案の捜査、実態解明、関係省庁と連携した注意喚起、啓発等を引き続き推進していく。

また、2020年東京オリンピック・パラリンピック競技大会開催時を狙った大規模サイバー攻撃に備え、関係省庁、団体、民間事業者等と連携し、情報収集、分析の強化、ボット撲滅のための取組、その他の諸対策を推進するなど、大会の安全・安心な運営のため、サイバー空間の脅威への対処に全力を尽くしていく。

○（鶴保情報通信技術（IT）政策担当大臣）

IT戦略本部官民データ活用推進戦略会議では、本年５月30日に決定した世界最先端IT国家創造宣言・官民データ活用推進基本計画に基づき、官民データの利活用を推進している。この推進に当たっては、安心・安全なデータの利活用の環境整備のため、サイバーセキュリティ対策を同時並行的に講じることが不可欠であると認識している。

また、科学技術イノベーション推進の観点から、国立研究開発法人や大学の保有する最先端の技術情報を守ることが喫緊の課題であると認識するとともに、戦略的イノベーション創造プログラム（SIP）により、重要インフラ等のサイバーセキュリティ強化に向けた研究開発をいち早い社会実装を念頭に、関係機関との連携を進めているところである。

今後も、データの利活用の推進と合わせて、セキュリティ対策が着実に実施されるよう、引き続きサイバーセキュリティ戦略本部と連携して取り組んでまいる所存である。御協力をよろしくお願い申し上げる。

○（岸外務副大臣）

我が国は、法の支配によって貫かれた、自由、公正かつ安全なサイバー空間を実現すべく、国連の枠組みを活用するとともに、有志国との連携を一層強化し、国際法の適用や規範に係る議論を深めていく。

また、夏以降、米国を始めインド、英国、豪州との間で協議を実施し、国連での議論も踏まえ、戦略的に日本のサイバー外交を進めていく。サイバーに係る議論は国際的にも様々な分野に広がりつつある。外務省としては、国際的な議論を分野横断的に把握し、得るべき成果、守るべき利益について、関係省庁と綿密な情報共有、意見交換を行い、国際場裏におけるサイバーセキュリティ問題について、関係省庁一丸となって連携対応をしていく所存である。

○（松村経済産業副大臣）

本日の会合では、2020年東京オリンピック・パラリンピック競技大会及びその先を見据え加速・強化すべき施策が決定されたと認識している。

そこで、業種横断的な情報共有、分析体制については、情報共有・連携ネットワーク（仮称）という形でイメージが示されたが、今後、NISCにおいては情報提供者の実態をよく把握した上で、より効果的な情報共有体制の構築に向けて、今後、法的措置も含めた制度設計の具体化を進めていただきたいと考えている。

また、セキュリティに係るビジネス環境の整備の内容は、とても充実したことを高く評価したいと思う。我が国のサイバーセキュリティ対策を強化するためにも、当省としても、関係省庁と連携しつつ、サイバーセキュリティがビジネスとして成り立つ環境の整備にしっかりと取り組んでいきたいと考えている。また、「サイバーセキュリティ2017（案）」に記載の施策については、各省庁が責任を持って着実に取り組むことが重要であると考えている。

そこで、経済産業省としては、IPAを所管する立場として、NISCや関係省庁と一体となって、重要インフラ事業者等への情報共有など、具体的な取組を進めていく。また、この７月からIPAの産業サイバーセキュリティセンターにおいて、実際の教育カリキュラムを開始した。米国の知見等も活用しつつ、このセンターから我が国のサイバーセキュリティの将来を担う人材を輩出していきたいと考えている。

○（金子総務大臣政務官）

総務省においては、ボット撲滅の推進に関して、本年４月、サイバーセキュリティタスクフォースから、IoTセキュリティ対策に関する提言が出されたところである。

当該提言に基づき、関係府省庁と連携してボット撲滅に向け、緊急に取り組むべきIoTセキュリティ対策を検討、実施していく。

また、人材育成については、本年４月に総務省所管のNICTにナショナルサイバートレーニングセンターを組織し、国の行政機関や重要インフラ事業者を主な対象とした実践的サイバー防御演習、通称「CYDER」の取組を強化するとともに、将来のサイバーセキュリティ分野の研究者や起業家を育成する新たな取組を開始した。私も先日、CYDERの演習を見学したが、参加されていた自治体職員の熱心な様子が大変印象的であった。

今後、総務省としては、これらの取組を通じて、引き続き関係府省庁と、また先ほど村井本部員の御指摘にあったように、とりわけ地方自治体とも連携しつつ、我が国のサイバーセキュリティの向上に尽力してまいりたいと考えている。

○（宮澤防衛大臣政務官）

我が国を取り巻く安全保障環境は一層厳しさを増しているところであり、この状況はサイバー空間においても全く変わるところはないものと認識している。

特に、最近のサイバー攻撃は高度化、巧妙化が進んでおり、実際に大規模サイバー攻撃によって世界各国でさまざまな被害が確認されているところである。我が国においても、サイバー攻撃によって国民生活や経済活動が大きな打撃を受ける可能性は否定できない。

このような情勢を踏まえ、防衛省、自衛隊としても、例えば人材育成のために実践的なサイ

バー演習環境を整備し、24時間態勢で情報システムネットワークの監視対処に当たるなど、さまざまな活動を行っている。

このたびまとめられた「サイバーセキュリティ2017（案）にもあるとおり、自らのサイバー攻撃対処能力の向上のみならず、諸外国との連携や関係機関との協力を深め、政府全体の取組に協力してまいりたいと考えている。

（3）決定事項の決定等

決定事項４件につき、案のとおり決定した。

（4）本部長締め括り挨拶

本日は、大変貴重な御意見をいただき厚く感謝申し上げる。

政府としては、ただいま御決定いただいたサイバーセキュリティ戦略の中間レビューを踏まえて各施策をしっかりと実行に移してもらいたいと思う。

有識者の皆様には、今後ともよろしくお願い申し上げる。

－　以上　－