サイバーセキュリティ戦略本部
第６回会合　議事概要

１　日時

平成 28 年１月 25 日（月）　８：30～９：30

２　場所

総理大臣官邸２階小ホール

３　出席者（敬称略）

菅　　義偉	内閣官房長官
遠藤　利明	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
河野　太郎	国家公安委員会委員長
松下　新平	総務副大臣
木原　誠二	外務副大臣
鈴木　淳司	経済産業副大臣
松本　文明	内閣府副大臣
熊田　裕通	防衛大臣政務官
遠藤　信博	日本電気株式会社代表取締役執行役員社長
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	慶應義塾大学教授
萩生田 光一	内閣官房副長官
世耕　弘成	内閣官房副長官
杉田　和博	内閣官房副長官
西村　泰彦	内閣危機管理監
遠藤　紘一	内閣情報通信政策監
髙見澤 將林	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

本日は、早朝から御参集いただき、感謝申し上げる。

サイバーセキュリティ戦略本部が発足して１年がたった。サイバー空間への依存度が高まる中、国民生活や経済活動の安全を確保し、本年５月の伊勢志摩サミット、2020年の東京オリンピック・パラリンピック競技大会を成功させるためには、サイバーセキュリティの確保が極めて重要である。

政府としては、昨年「サイバーセキュリティ戦略」を策定し、予算、体制の両面から対策を強化しているが、深刻化するサイバー攻撃に備えるためには、更に国による監視対象の拡大、サイバーセキュリティ人材の育成、重要インフラ事業者に対する支援などの取組を強化する必要がある。

本日の会合においては、これらの点について御議論いただき、その内容を踏まえて、これからしっかり強化対策を講じていきたい。

よろしくお願い申し上げる。

(2)　討議

【決定事項】

・　我が国のサイバーセキュリティ推進体制の更なる機能強化に関する方針（案）

【討議事項】

・　政府機関等の情報セキュリティ対策のための統一基準群の見直しについて
・　重要インフラ専門調査会における検討状況について

【報告事項】

・　政府のサイバーセキュリティに関する予算（2016 年度政府案等）
・　2016 年サイバーセキュリティ月間について

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。

○（前田本部員）「我が国のサイバーセキュリティ推進体制の更なる機能強化に関する方針（案）」に賛成であり、統一基準の見直しにも異存はないが、ウェイトの置き方ということで若干私見を申し上げる。

我が国の国民にとって、日本の誇りは安心・安全であり、これが国民の第１順位の誇りである。今、不安が起こるとすれば、サイバー世界で起こるというアンケート調査結果がある。漠然とした不安に対する対応はかなりできてきていると思うが、今日はサイバーテロに絞って申し上げたい。

今まで、サイバーの危機といえば、我々が 20 年前、30 年前にサイバーの研究をやり出したころは、政府のホームページが見にくくされる、企業の情報が抜かれる、個人情報が漏れるといったものであった。そのレベルがだんだん深刻化しており、特に去年あたりから国民にも危機意識が浸透していった。生活の一番重要な基盤がテロによって脅かされるようになり、イスラムの世界などが他人事ではなくなってきた。テロ組織がサ

イバーを利用して日本の安心･安全を覆すという攻撃を仕掛けてくることは､予想外だった、ということでは許されない。

ただし､従来からの日本の法律の考え方は､国外から攻めてくるということに対して、予防的に対応することには、非常に謙抑的である。しかし、いざ安心が害されると、そういう謙抑的なやり方しかできなかったのだから仕方がなかったということにはならず、国は何をやっていたのかという叱責を受けることになろう。

これまでの議論では、事故やトラブルの起こらないシステムをいかに構築するか、その技術をどう高めるかということにウェイトが置かれていた。しかしテロになると、社会を混乱させようとして意図的に攻撃を仕掛けられる。そのような攻撃に対しては、攻撃を行う主体を捕捉し、制裁を加えて抑止していくという観点抜きには対応できない。それは一朝一夕にできることではないが、徐々に進んでおり、今後のサイバーセキュリティの軸にその視点が強まることは絶対に必要である。起こってから何とかするという事後処理の対応だけではもう駄目で、事前抑止も考えていかなければならない。

もちろん攻撃しにくいセキュリティシステムや、IoT なども非常に重要である。IoT などでも、今までのように人間が爆弾を抱いて自爆するといった攻撃と違い、サイバーやロボットといった技術を使って人を攻撃する。サイバーが人命に及ぶということは全然結びつかなかったが、それが大きく変わろうとしている。それは杞憂だ、学者がオーバーなことを言って、という感じがあるかもしれないが、世界的に見れば当然そうしたことも視野に入れて議論されている。その意味で、防衛省、警察庁はもちろんのこと、国全体として対処官庁の力量を高めていく。その中でインテリジェンスの重要性が高まり、それに対応する組織ができたということは、非常に理にかなったこと。さらに、情報収集の関係で非常に悪く言われるが、特定秘密保護法があることの恩恵はわかってくると思う。そういうことを踏まえて、やはり安心・安全の一番土台の部分を守るのがサイバーセキュリティであるということを強調させていただきたい。

それから、連携について、先ほど申し上げたテロ対策ということよりは、事故やトラブル等が起こりにくくするという意味で、インシデント対応、官民連携、民民の連携は非常に重要であり、この取組は着実に前に進んでいて、本会合で決定事項として示された案は非常に合理性があると思う。

一つだけ官官連携に関して、第４回会合でも申し上げたが、強調しておきたいことがある。官官の連携の中でNISC のように省庁間の壁がある程度抜けて、うまくいった組織は余りなく、どうしても最後は省庁間の利害対立が出てくる。これを全面的に否定する気はないが、その風穴をあけていくためにも指定職の設置など、いろいろな案が具体的に出てきている。それをもう一歩血の通ったものにするためには、どういう人材を充てるべきかというときに、そういう情報に詳しいIPA の人がほかの省庁に行って、指定職的なものにつき、キャリアパスをつくっていく。それはもちろん抵抗があると思うが、オールジャパンで見たとき、限られた人材の中でどのような人間をどう配置していくかを考え、官官連携を進めていくということは重要である。

○（村井本部員）全体の体制がこのように整っていくのは大変重要なこと。特に私のような技術を専門にしている者から言うと､この 2016 年というのは大変新しい技術が多く出

てくる年で、いろいろな技術政策の中でもIoTが重要である。IoTというのはモノがデータを取ってくる。皆さんのテレビ周りの機器はインターネットに既につながっており、場合によっては空調などの家電もつながっている。これは基本的にはコントロールのためにつながっているが、実はそこにあるデータも非常に有効で、例えば空調が空気の質やダニの数といったものを測ることができるようになっている。そういうものを使って新しい産業やサービスをつくっていくのは大変重要で、そこにIoTのいわばポジティブな面がある。AI、ドローン、自動運転、新しい技術がどんどん発展していくので、そういう意味でIoTが広がっていく世界というのは経済発展に大変資するものであり、世界の中での競争もあるため、しっかりやらなければならない。一方で、安心なサービスができるか、信頼性のある安全なサービスをつくれるかは、やはり日本に、高い品質を持ったサービスをやってきたという責任があるのではないか。

そのような中で３点、大変重要なことだと思っていることを申し上げる。

一つはリスクの掌握である。たくさんのことをどんどんやりながら、それを守っていくにあたり、全てを受け身で守っていくということはなかなか難しい。新しくできる技術を先取りして守っていくということもまた難しい。そうなると一番大事なのは、多少危険をはらんでいる技術と一緒に進むときに、それが何であるかを知ることである。どのようなリスクが生じるのかというのは調査活動のようなもの。わかりやすい例として、自動車にはたくさんの保険がある。今、サイバー空間における保険がつくりにくいのは、リスクの定量化ができていないからであり、サイバースペースのリスクの定量化を行うための取組は重要である。実際にはあちこちでやっているのだが、問題はそれを結合できるかどうか。それがNISCの大きな仕事ではないか。

それから、今回資料６で「サイバーセキュリティ月間」が出ている。実はNISCは内閣の組織としてはとても珍しいのだが、内外に対してのアウトリーチが非常に良く、大変わかりやすいということで海外でも非常に評判が良い。いろいろな人々がサイバーセキュリティの意識を持つことが重要であるため、とても良いことである。

もう１点、今回参考２として「サイバーセキュリティ経営ガイドライン」がある。これは、経営者がセキュリティに対してどういう意識を持っているかということであり、実は私がこの国で一番心配していることでもある。２頁目に指示が書かれているが、例えば指示９に、経営する組織の中にCSIRTをつくりなさいと書いてある。これは良い指示だと私は思う。資料２にも、オリンピック・パラリンピックCSIRTをつくりましょうと書かれている。CSIRT をつくり、それらが連携するのはとても重要なことである。ただ、これに関してKPIをつくっていただきたい。つまりロードマップをつくる。2020年までには経営者の何%が、中小企業の何%が、大企業の何%がCSIRTを整備して連携しているのか、そういうKPIはつくれると思う。「サイバーセキュリティ経営ガイドライン」をそこまで結びつけるのは政府の仕事であり、経営者が頑張るのは民間の仕事である。そうした官民の連携は、こういったアウトリーチのなかでできると思う。

最後に、これから我々が試されることは、オリンピック・パラリンピックはもちろん、その前にも来年のG7伊勢志摩サミットでの議論があり、その議論の中でサイバーセキュリティに対して、あるいはIoTの時代のサイバーセキュリティに対して、どのようなメッセージを日本が出すかということは、世界に対しての責任を果たす大変大きなチャンス

であり、重要なことである。

○（遠藤本部員）本日示された決定事項及び討議事項には、基本的に賛成であり、これらの方向感が出てきたこと自体、非常にありがたいことだと理解している。

その中で監視等対象の拡大または強化ということについて、必要なことはリアルタイムでの状況の把握と、これに対するダイナミックな体制または情報の横展開によるフレキシブルな対応能力を持つこと。この部分に注力をした監視等の対象の拡大をしていただきたい。

また、セキュリティ人材の強化という観点では、教育機会をつくり、大学を強化し、高等学校と協力することが重要ということであるが、さらに緊急性がある観点から考えると、受けたいときに受けられるシステム、または受けたいときに必要なカリキュラムが組まれていて、そのカリキュラムの一部でも勉強できるといった、自分のステップアップをしていける仕組みを用意することが必要であろう。

２点目、政府のサイバーセキュリティに関する予算が約1,000億円と２年前の約２倍になっていることは非常にありがたいこと。２年前、情報セキュリティ政策会議第38回会合で、日本とアメリカとの比について、GDPの比は１対３ぐらいであるが、セキュリティの費用は１対14であったということを申し上げた。1,000億円になったので少し縮まったかと思ったが、今アメリカは予算が約140億ドル、1.6兆円になっている。そういう意味では、サイバー空間が非常に重要な基礎インフラになってきたと理解すべきであり、我々はこの1,000億円という予算をしっかりと有効に使っていく必要がある。その中でも、人材育成への予算実行がエフェクティブに行われることが非常に重要である。ぜひこうした観点について、官民一体となって実効性を高めていけると良い。

３点目、オリンピック・パラリンピックの対応が今回も資料２で挙げられている。遠藤大臣も本部員に入られたということで非常にオリンピック・パラリンピックに期待する中、一方でサイバーセキュリティに対する意識が必要だと思うが、もう４年半しかないので、ステップ・バイ・ステップで強化をしていくための計画と、さらには重要インフラのどこを注力して守るべきかということの定義を早急にすべき。まずは５月に伊勢志摩サミットがあるので、それをベースに官民一体となって、できることはしっかりとやっていく必要がある。

最後に４点目、我々がサイバー空間のセキュリティを守っていくという観点で重要なことは、先ほど村井本部員からもお話しいただいたが、我々が企業活動をしていく上でも、また、インフラをオペレーションしていく上でも、IoTが絶対的に必要な基礎インフラになっているということである。例えば企業がIoTの中に入らないと、または自社のネットワークがネットワークの中に入っていかないと、オーダーが来たときにそれをリアルタイムで受け取って、自らのシステムの中で自動的にスケジュールをつくるというようなことができず、サプライチェーンマネジメントの中に入れない、または企業活動ができないという状況がすぐに来る。その観点では、各企業が持っているネットワークのセキュリティ度合いがどのぐらいであるのかということがしっかりと外からも内からも見える必要がある。そのためには、企業のネットワークがセキュリティの観点からどうあるべきなのかという方向感が明確に示されることが必要であると同時に、そのセ

キュリティを提供する企業に対する、ある意味での技術のサーティフィケート、どのような能力がある企業がそういうことに対して対応できるのかというようなサーティフィケートを考えるということも、手段として必要になってくるのではないかと思う。

○（小野寺本部員）３点ほど申し上げる。

今回の全体的な方向性については明らかに前進しており、非常に良い方向である。その中で大企業はサイバーセキュリティについて関心が高くなり、かなり守ることができている。ところが最近の犯罪は、大企業のネットワークにつながる、例えば中小企業であるとか、自社の子会社、もしくはサプライチェーン上のベンダー、そうした弱いところを突いて大企業のネットワークに入るためのパスワード等をそちらから盗むという手法が増えてきている。そういう観点で申し上げると、大企業だけがサイバーセキュリティを強化しても全く意味がなく、それは政府についても全く一緒だと思う。中央省庁はかなりサイバーセキュリティの取組を進めているが、問題はやはり地方自治体ではないかと思う。本会合の方向性の中でも、政府の直接の監督がきく特殊法人等については監視等の対象に入ってきたが、地方自治体についてはどのように管理をしていくのか。ここがないと、例えばマイナンバーの問題についても、本省側のシステムはしっかりしているが、自治体側の弱点を突かれ自治体側を経由して何かを抜かれるとか、そういうことは十分にあり得る話だと思う。そういう意味で、地方自治体のところをどう考えるか。これをぜひ皆さんでお考えいただきたいというのが１点目である。

２点目は、先ほどから村井本部員、遠藤本部員からもお話いただいたことと関係するのだが、アタックに対してどういう観測網を敷くかということ。これは今のところ、各省庁なり、NISC なり、NICT なりが、いろいろな方法で行っているが、それを全体的にまとめて、どこまでを監視し、どういう状況になったときにアラームを発すべきかということが定められた観測網、これを日本としてどうつくるかということを考えていただきたい。

３点目、「サイバーセキュリティ月間」や、「サイバーセキュリティ経営ガイドライン」は、非常に結構な方向性だと思う。１点目で申し上げたことと関係し、昨年の日本年金機構の事案でもそうであったが、正直申し上げて地方自治体や日本年金機構の職員の ICT リテラシーが余りにも低いのではないかと思う。以前、官房長官にも申し上げたが、IPA がせっかくいろいろな資格システムをつくり、民間にはぜひ使ってくださいと来ているのに、それを政府や地方自治体では有効活用されていないのではないかと思っている。例えば、マイナンバーで端末を操作する人には最低限この知識レベルを与えておくべき、といったことを政府として示さないと、地方自治体としても何をやれば良いのかということがはっきりしていないのではないか、と思い危惧している。そういう意味で、「サイバーセキュリティ月間」等を利用して、ぜひ ICT のリテラシーそのものを上げることによって、サイバーセキュリティへの関心をもっともっと高めてもらうということをやっていただきたい。

○（中谷本部員）日本年金機構の事案を踏まえ、サイバーセキュリティ推進体制の更なる強化がなされることは、国民生活の安心・安全という観点からはもとより、国家安全保

障の観点からも重要であり、今回の方針を全面的に支持したい。

その上で、次の７点をごく簡単に指摘する。

第１に人材の強化について、各省庁にサイバー担当を担う審議官を置くことは大変結構なことだが、将来的には、公務員試験の総合職に情報セキュリティといった試験区分を設けて採用することも検討すべきかと思う。また、企業、官庁において、サイバーセキュリティのエキスパートのキャリアパスを確立させていくことが重要であり、政府においても、そのための積極的な施策を展開することが望ましい。

第２に、これとの関係で、情報処理安全確保支援士の制度を創設していくことは、サイバーセキュリティのエキスパートをエンカレッジするもので大変結構なことである。同時に、更新制とすることで、動きの激しいサイバーセキュリティの世界で、最新の知見を有する者だけがこの名称を名乗れるようにすることが重要である。

第３に、クラウドサービス利用時の対策事項を規定しておくことに関して、サーバーを国外に置くことを一律に不可とすべきではないが、例えば、重要事項を扱う部分については国内のサーバーに留保し、公開情報についてのみ国外サーバーでも可とする、といったような基準を作成していくことが重要である。

第４に、「サイバーセキュリティ月間」で国民への理解を深めてもらうことに関連し、スマートフォンへのアプリのダウンロードについて注意を喚起することが重要だと思われる。マルウェアの仕込まれたアプリをダウンロードしてしまった結果、スマホが踏み台となって重要インフラへのサイバー攻撃がなされるということも懸念されるため、アプリのダウンロードには十分注意するよう、一層呼びかけていただきたい。

第５に、予算に関して、サイバー外交の展開が積極的平和主義にとって重要であることは言うまでもないが、その割にはサイバー外交の関連予算が 0.1 億円と、いかにも少ないという印象があるため、今後、善処していただくことが望ましい。

第６に、核物質管理センターのパソコンが、職員が導入および使用を禁止されているファイル共有ソフトをインストールしたことが原因で、外部のサーバーと不審な通信をしていた。同センターは、原子力規制庁への報告を怠っていたということである。重要な情報を扱う諸機関において、このようなずさんなことが再発しないよう、政府として厳格な対応をお願いしたい。

第７に、「サイバーセキュリティ経営ガイドライン」に関して、盲点となりかねない日本企業の在外の子会社や支店によるサイバーセキュリティ対策についても、今後、検討していただきたい。

○（野原本部員）３点申し上げる。

先ほど、前田本部員からもサイバーテロのリスクが高まっているという話があったが、その点で、重要インフラ対策はますます重要になっている。対策は、民間事業者が自ら実施するもので、国には強制力がないが、そうした体制が致命的な被害にならないようにしていただきたい。さらに、小野寺本部員からも意見があったが、大企業が自社の責任範囲はしっかりやっていたとしても、一企業の責任範囲を超えた業界全体の脆弱性を把握するという視点が重要なわけで、そのための情報共有、連携強化、そして全体の責任の明確化をしっかり行っていくことが必要ではないか。

また、重要インフラと一言で言っても、リスクの内容が多岐にわたっている。異物混入や運用停止が社会混乱を引き起こしたり、大事故の発生が国民の命に直結したりするような分野もあれば、銀行、証券のように資産消失や経済活動の混乱を来す分野もあるなど、様々である。結果として起こる被害も多様であるが、どこにどういうリスクがあるかという点でも多岐にわたると思われ、個々の現状分析をしっかり的確に行い、それぞれに合った適切な施策、体制構築を行うことが必要である。その点で、重要インフラの範囲や、それぞれの対応策を不断に見直す、そして、情報共有のあり方、訓練、方法を継続的に改善し続けるということをうたっている今回の資料は、非常に重要な視点がしっかり盛り込まれている。それでも、13分野の一つに航空があるが、航空会社は入っていても、空港会社は含まれていないというような実態も既にあると聞いている。そういうことを含め、現状を把握し、現在のリスクの分析をしっかり行い、不断の見直し、改善を行っていただきたい。これが１点目である。

２点目、３点目は、人材育成について申し上げる。

まず２点目であるが、今回、資料２－１でも説明いただいたとおり、政府人材の強化ということで、各府省庁のCISOまたはCIOを補佐する審議官クラスに「情報セキュリティ・情報化推進審議官（仮称）」を設置されることを決めていただいた。重要な対策として、しっかり進めていただきたい。これにより、ポジションはしっかりできたわけだが、今後はサイバーセキュリティ人材全体のキャリアパス整備にも取り組んでいただきたい。外部人材の採用、登用というのも必要であるが、それだけではなく、一種、二種の国家公務員試験を含め、新卒の採用から全体を含めた、人事院なども巻き込んだ長期的な視点に立ったキャリアパスの整備が必要だと思う。それにより、審議官クラスに次々と適任者がきちんと配置できるようにしていくことが必要ではないか。

３点目、業界全体、国全体のセキュリティ人材の育成と整備のために、情報処理安全確保支援士制度という名前で資格制度の運用が提案されており、その創設が現在、国会に提案されるのを待っていると伺っている。これも大変重要な仕組みで、専門人材が国全体で不足し、人材の所在がはっきり見える化されておらず、うまく活用できていないという問題があるため、有意義な施策だと思う。

施策を実行するに当たっては、まず、現在の専門人材の数、質をしっかり把握して、今後もそれを把握し、分析しながら進めていっていただきたい。

また、更新をするということで、３年ごとに更新制度を入れると伺っているが、その講習のやり方には、e-learning等を活用して効率的なやり方で大量の人たちの教育をしていっていただきたい。

さらに、登録簿を作成して、そこに人材の情報をしっかり見える化し、マッチングをしていこうということであるが、それが有効に回っていくよう、環境改善をしていただきたい。

○（林本部員）参考２の「サイバーセキュリティ経営ガイドライン」について、最初に簡単に意見を申し上げたい。このガイドラインは、経産省とIPAのところに設置された委員会で検討され、NISCの佐々木サイバーセキュリティ補佐官が委員長をされ、私も委員として参加させていただいた。一生懸命書いたが、非常に急いでやったので、あるところ

まで書けていると思うが、これからの課題があることも自覚している。それは、現在ある制度、一番の根幹は会社法であるが、そういう会社の仕組みをどう守るかというところとこのガイドラインがどのように連動していくのかということである。それをNISCでも検討されるように伺っているので、ぜひ、早くそういうことを検討いただきたい。

その上で、決定事項については、他の本部員の皆様からも意見があったように、昨今の現状を踏まえ、また、昨年の年金機構の事件の教訓なども取り入れて、NISCがサイバーセキュリティの司令塔にふさわしくなるように提案されているものであり、方向性としては大いに賛成したい。むしろ、問題は攻撃側も日進月歩あるいは分進秒歩で進んでいるので、いかに早く実施するか、あるいはできるかということが大切かと思う。その上で、この中に入っている「サイバーセキュリティ人材育成総合強化方針（仮称）」の策定に関して、３点ほど申し上げたい。

まず、１点目は、政府機関と企業の両方とも、サイバーセキュリティの人材が不足しているということについてである。多分これからはローテーションで、民に入った人はずっと民、官に入った人はずっと官ということではなく、行き来することになるだろうと思う。情報の共有とともに、このような人材の相互交流も必要となっているという現状に照らすと、教育の分野においても、サイバーセキュリティに特化した奨学金制度をつくるとか、あるいはそれと連動した形で政府がその奨学生を優先的に雇用する、あるいは時限的に雇用する、といったことも、既に先進国で行われていることであり、御検討いただきたい。

２点目として、現在までの検討は、どちらかといえば高等教育が主たる対象になっている。私どもも実は情報セキュリティ大学院大学というものを最初につくったわけで、学部を持たないままつくったのだが、徐々に各方面にこういうものが必要だということが理解されてきていると思う。しかし、これだけITが普及している現状に照らせば、初等・中等教育のところからこれに取り組むということが大切であり、また、IoTの時代とか、フィンテックの時代とか言われている時代においては、そのことが我が国の産業競争力の向上に資するという面もあると思う。そのような意味では、既に中教審の部会では検討が始まっていると伺っているが、この点の検討にますます期待しているところである。

３点目は、やや意外なことかもしれないが、日本企業はOJTが得意だということになっている。それはそのとおりだと思うが、実はセキュリティについては、OJTで大丈夫かということが気になっている。たまたま、OECDが2012年に発表した国際成人力調査というものを使って分析した論文を最近目にした。データはやや古い懸念はあるが、IT問題解決能力指数と、職場でのIT利用頻度指数という２つの軸で考えている。OECDの平均が100になるように指数化したところ、日本は、前者のIT問題解決能力指数は104で第１位であるが、IT利用頻度指数のほうは84で最下位になっている。つまり、潜在力はあるのだが、現場でそれを使う頻度はさほどないということを意味していると思う。これは、逆に言えば、それだけまだまだ開発の余地があるというふうにプラスにも見えるが、逆にセキュリティのようなものは必ず演習などをやらなければいけないわけで、むしろ実践の面で見ると、日々通常業務を行っているときに対処が必要な場面に出くわしたり、問題解決を求められたりする頻度が少ないということになってくる。このデータが正しいかとい

うことはもう少し検証が必要かと思うが、残念ながらこの結果は、私がビジネスマンとして長く経験してきた実感と符合していると言わざるを得ない。

以上を踏まえ、教育と日々の実践という両面を通じて、潜在力が十分発揮されるように検討していただければと思う。

○（遠藤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（副本部長））

昨今の政府等に対するサイバー攻撃の激化などを踏まえ、サイバーセキュリティ戦略本部による原因究明調査等の範囲を独立行政法人や特殊法人等に拡大することなどを盛り込んだサイバーセキュリティ基本法の改正案を今国会に提出することとしており、その成立に向けて政府として全力で取り組んでいく。

また、昨年 11 月には、2020 年東京オリンピック・パラリンピック競技大会に向けた政府の基本方針を閣議決定した。大会成功のためには万全のセキュリティによる安心・安全の確保が最も重要な鍵であり、まずは国全体としてのサイバーセキュリティの確保が必要不可欠である。この認識のもと、基本方針の中にも「サイバーセキュリティ戦略」の着実な実施を盛り込んでいる。

引き続き、人材の育成・確保など、各種重要な課題が多くあるため、サイバーセキュリティ戦略本部の副本部長として、政府全体のサイバーセキュリティの強化に向けて全力で取り組んでいく。どうぞよろしくお願い申し上げる。

○（河野国家公安委員会委員長）

スイスのダボスで開催された世界経済フォーラムの年次総会に出席し、昨日帰国した。ダボスでの意見交換等を通じ、サイバー空間の脅威への対処のためには、官民連携等が不可欠であると再認識をしたところ。

2020 年の東京オリンピック・パラリンピック競技大会等の成功のためにも、官民連携を推進し、我が国のサイバーセキュリティに万全を期す必要がある。警察では、全都道府県に設置されたサイバーテロ対策協議会の枠組みを通じ、大会を支える重要インフラ事業者への注意喚起や共同対処訓練等を実施している。

また、主要事業者のみならず、中小事業者に取組の範囲を拡大していくことも重要である。一部の都道府県警察においても、サイバーセキュリティの確保に向け、中小事業者等との間で連携組織を立ち上げるなどをしているところである。

引き続き、関係省庁と連携して、こうした取組を強化するよう、警察庁を指導していく。

○（松下総務副大臣）

総務省では、本年も引き続き、NISC と共同で CYBER EKIDEN を実施予定である。その際には、昨年の年金機構の事案を踏まえ、標的型攻撃にも対応した実践的サイバー防御演習「CYDER」の最新シナリオを用意する予定である。また、こうした実践的演習の規模を拡大して実施できる体制を確保すべく、NICT の業務範囲の見直しに関する法律案を今国会に提出する予定である。

マイナンバー関係では、来年７月から国・地方を通じた情報連携が予定されているた

め、各地方公共団体においては、インシデント即応体制や職員への訓練の徹底などを図るとともに、自治体情報セキュリティクラウドの構築等、情報セキュリティ対策の抜本的強化を推進しているところである。この抜本的強化対策については、平成27年度補正予算などに必要な経費を計上し、成立したところである。また、当初予算案においても、マイナンバー導入に関連するセキュリティ対策に必要な経費を計上している。

先ほど、小野寺本部員から人材育成、地方公共団体に対する重要な御指摘をいただいたが、総務省としても最重要、喫緊の課題として取り組んでいきたい。

総務省としては、関係機関と密接に連携しながら、我が国全体のサイバーセキュリティの一層の強化に尽力していきたい。

○（木原外務副大臣）

昨年９月の米中合意、あるいは11月のG20首脳宣言において、サイバーについて言及されるなど、国際場裡において引き続きサイバー空間をめぐり活発な議論や動きが展開されている。

我が国としても、先ほど御指摘をいただいたG7伊勢志摩サミットを初め、さまざまな国際会議の機会を捉え、サイバー空間における基本原則や法の支配の徹底などについて、関係省庁及び米国等と連携をしつつ国際社会を主導していきたいと考えている。

なお、先ほど予算について御報告をいただいたが、今後、国際会議等への参加の出張旅費の増加なども検討していきたい。

また、途上国との協力について、ASEAN各国に対してサイバー犯罪対策等に関する能力構築支援を一層積極的に進めていく。

さらに、G7伊勢志摩サミットに向けては、専門家の知見も取り入れつつ、万全のサイバーセキュリティ対策を講じていく。

○（鈴木経済産業副大臣）

2020年の東京オリンピック・パラリンピック競技大会に向けて、官民の持つサイバーセキュリティの知見を最大限活用し、対策を強化していくことが重要である。これに関して、以下３点申し上げる。

まず１点目として、経済産業省所管の独立行政法人情報処理推進機構（IPA）は、サイバー攻撃の対処に関しすぐれた知見を有している。今回の法改正を通じ、IPAは独立行政法人等の対策強化に貢献をしていく。また、NISC要員の増強としてIPAの専門家を派遣しているところであり、引き続き貢献をしていく。

２点目として、経済産業省は民間企業のセキュリティ対策の強化を進めていく。本日概要を配付したが、昨年末、経営者のリーダーシップによって対策を推進するための「サイバーセキュリティ経営ガイドライン」を策定した。本日も委員各位から御意見をいただいたが、本ガイドラインの普及を図るとともに、対策を実施する企業が評価されるような仕組みを広げていく。

３点目として、これまでIPAが重要インフラ事業者間のサイバー攻撃に関する情報共有などを実施しているが、事業者任せにしない更なる対策強化が必要である。このため、我が国の専門家を結集し、電力、ガス等の重要インフラに対するサイバー攻撃の可能性

をテストすることで、事業者の具体的な対策強化につなげていく。

○（松本内閣府副大臣）

人材面とシステム面の一体的な対応が重要であるが、人材面においては、本日決定される「我が国のサイバーセキュリティ推進体制の更なる機能強化に関する方針」に基づいて、IT 人材育成のための取組をしっかりと進めていく。

システム面においては、サイバーセキュリティ対策と業務改革の両方の観点から、情報システムを整備・運用管理することが重要と考えている。このため、政府情報システム改革の一環として進めている運用コスト削減等の成果を、本日見直しについて討議された政府機関等の情報セキュリティ対策のための統一基準群等によるセキュリティ強化への投資に活用できるようシステム面の取組を着実に進めていく。

○（熊田防衛大臣政務官）

深刻化が進むサイバー攻撃に備えた政府全体のサイバーセキュリティ推進体制の更なる強化は、我が国における喫緊の課題であり、今後、伊勢志摩サミットや東京オリンピック・パラリンピックなどが開催されることを踏まえれば、時宜にかなったものと考えている。

今般の方針案は、政府機関のシステム及び人材の強化に加え、関係法人等や重要インフラ事業者にまでサイバーセキュリティ確保の対象を広げており、我が国全体としての多角的な対策強化の観点から極めて有効なものと認識している。

今後、決定される本方針を踏まえ、防衛省・自衛隊としても、政府全体の取組に対して保有する知識・技能等を積極的に提供するなどの貢献をしていくとともに、自らのサイバー攻撃対処能力の一層の強化に取り組んでいく。

○（村井本部員）

今、オリンピック・パラリンピック、警察、総務省、人材教育の点からそれぞれ地方自治体のセキュリティの話をいただいた。一方で、マイナンバー法の中で、ついに地方自治体全部に対するマイナンバーのコンテクストでのセキュリティに対する権限が、個人情報保護委員会に与えられた。総務省はもちろん、守備範囲としては警察もそうであろうが、全国の地方自治体との連携が決まっている。

NISCの国の組織に対する権限と連携が明らかになってきた中で、今日伺った話では、やはり国と地方自治体との関係が非常に多岐にわたっており、それぞれ皆さん連携をしてということをおっしゃっていただいたが、その連携が具体的にNISCにおいてどのように把握され、連結されて進んでいるのかということがいまいち明確ではないような気がする。これは大変大事なポイントだと思う。例えば自然災害などが起こったら、国と地方自治体との連携の必要性が出てくるため、そうするとやはり地方自治体の役割は大変重要になってくる。そうしたことを考えていただきたい。

(3)　決定事項の決定等

決定事項１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、今後の取組強化策を取りまとめいただき、感謝申し上げる。

政府としては、この方針に基づいてNISCの機能強化を初め、サイバーセキュリティ対策に着実に取り組んでいく。

有識者の皆様においては、今後とも御協力をいただくことを心からお願い申し上げる。

－　以上　－