サイバーセキュリティ戦略本部
第12回会合　議事概要

１　日時

平成29年４月18日（火）　17:00～18:00

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
世耕　弘成	経済産業大臣
鶴保　庸介	情報通信技術（ＩＴ）政策担当大臣
あかま 次郎	総務副大臣
武井　俊輔	外務大臣政務官
宮沢　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
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

４　議事概要

⑴　本部長挨拶

本日は御多忙のところお集まりいただき、感謝申し上げる。

本日、御議論いただきたいのは次の３点である。

１点目は、「重要インフラの情報セキュリティ対策に係る第４次行動計画」についてである。前回の会合で2020年東京オリンピック・パラリンピック競技大会を見据えて、重要インフラ防護のための行動計画の見直し案を御議論いただいた。本日は、前回会合後に実施したパブコメの結果を踏まえて御審議いただき、行動計画の決定をお願い申し上げる。

２点目は、サイバーセキュリティ人材育成プログラムである。官民を問わず不足している人材について、需要と供給の好循環を生み出す人材育成システムを構築すべく、昨年３月に人材育成総合強化方針を策定し、８月には行政機関における人材育成・確保計画を決定していただいた。本日は、これに引き続き企業を始め、社会で活躍できるサイバーセキュリティ人材の育成のあり方について御審議をいただき、人材育成プログラムとして決定をお願い申し上げる。

３点目は、今後のサイバーセキュリティ政策のあり方についてである。前回の会合で、来年９月に策定後３年になるサイバーセキュリティ戦略の見直しの進め方を御議論いただいた。その結果を踏まえて、まずは現行の戦略で加速・強化すべき施策について、本年夏を目途に中間レビューとして取りまとめ、できるものから実施をしていきたいと考えている。この取り組みは、次期戦略につながっていく重要なものであり、皆様方の忌憚のない御意見を賜りたく、活発な御討議をよろしくお願い申し上げる。

⑵　討議

【決定事項】

・重要インフラの情報セキュリティ対策に係る第４次行動計画（案）について
・サイバーセキュリティ人材育成プログラム（案）について

【討議事項】

・「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」の検討状況

【報告事項】

・2017年サイバーセキュリティ月間について
・「各府省庁セキュリティ・IT人材確保・育成計画」の実施状況等について
・2020年東京オリンピック・パラリンピック競技大会のサイバーセキュリティの確保に向けた取組状況について

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。

○（野原本部員）

１点、申し上げたい。

「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」に関してはうまくまとまっていくと期待している。特に各論については、（バーチャル）サイバー情報連携センター（仮称）の構築を始め、重要な施策をしっかり検討しており、今後更に具体的な内容や目標設定、あるいはスケジュールを明確化することによって、しっかりと推進できるようにしていっていただきたい。

「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」をまとめる中で、各論に入る前の総論や現状認識で記載する内容について、我が国のサイバーセキュリティに対する戦略の方向性やスタンスがこれまでとどう変わるのか、どう深まるのかということをもっと明確に冒頭で述べたほうが良いのではないかと思う。サイバーセキュリティ戦略中間レビュー概要でもまとめているとおり、今の脅威の変化というのは凄まじいものがあって、複雑化や防護対象の拡大化、あるいは脅威のグローバル化が進んでいるだけでなく、各国との政治的あるいは経済的な関係の変化もあって、非常にサイバーセキュリティの問題は重要になってきていると思う。そうした環境変化に対して国のサイバーセキュリティ対策を充実させ、進化させていくことが重要であることは言うまでもない。

具体的には、サイバーセキュリティ戦略中間レビュー（骨子素案）のサイバー攻撃対策や重要インフラ、政府機関防護対策や国の安全確保についての基本的方針を述べている２ページ目のあたりに、スタンスをしっかり書いてはどうかと思う。国が、NISCがより積極的に役割を果たしていく方向で取りまとめてはどうかと思う。

それによって、これまで以上にNISCが具体的に関与して、調整機能だけではなくて必要に応じてリーダーシップをとり、アドバイスやチェック機能を果たす。そして、重要インフラや政府機関のような、重要なサービス全体にたくさんの人が関わるような場合に、重要なサービスを構成する業務や経営資源及び情報システム、制御システムといったようないろいろなものを鳥瞰図的に把握、分析して、それを安全の観点から整理してフィードバックをかけて、全体をコントロールしていくというような役割を行う、あるいはサポートしていくことが大変重要だと思う。そうしたスタンスでNISCが中核となって、しっかりと機能を果たしていくのだということを冒頭で述べてはどうかという意見である。

○（林本部員）

決定事項には異論はなく、サイバーセキュリティ戦略中間レビュー（骨子素案）について３点ほど意見を申し上げる。

まず第１に、総論のところで、我が国が立脚する基本原則の主張に向けた方針として、インターネットのガバナンスに関する基本方針を再確認されたことは喜ばしいと思う。しかし、私が参加したGGEの予備的な会合においてさえ、基本原則としての情報の自由な流通を市場に任せるのではなく、国家の関与が避けられないという意見の人がいて、合意が容易でないことを

実感した。現に2013年末に開催されたITUの規則制定会議では、国家主義色が強い規則ができ上がり、西側の諸国が署名を拒否するという異常な事態が起きたことは忘れてはならないと思う。

今後、IoTやAIの発展とともに、これらに関する標準化や法的責任に関する制度的すり合わせが必要になると思われ、交渉に従事される方々が問題意識を共有していただくとともに、NISCの調整機能にも期待したい。

第２は、各論の冒頭にある（バーチャル）サイバー情報連携センター（仮称）におけるNISCの役割に関してである。頂いた骨子素案には、官民連携の活性化を進める結節点として機能するよう、専門機関の活用等による体制の抜本的強化を図るという表現になっているが、この表現は前段と後段の結びつきがやや弱いような印象を受けた。確かにマルチステークホルダーによる官民協調等は不可欠で、それぞれの組織の自主性を重んじることは必要だが、NISCが頼りになる存在でなければ結節点の役割は果たせないと思う。

また、専門機関を活用するだけでは体制の抜本的強化にはならないのではないかという心配がある。次の文章にある制度的枠組みの構築を含めた環境整備に、今申し上げた点も入っているのかもしれないが、全体にNISCが控え目に過ぎないかという印象を持った。今一歩、前に出る姿勢が必要と感じた。

最後に、第３点として、この資料の５ページに個別的、基盤的項目として（イ）の中に「ｃ．地方公共団体におけるセキュリティ対策の向上」「ｄ．大学におけるセキュリティ対策の向上」が書かれている。ここには書いていないが、中小企業におけるセキュリティ対策の向上を加えた３テーマが、我が国のサイバーセキュリティの弱点対策として喫緊の課題ではないかと思う。

セキュリティ対策、とりわけ能力向上策としては、まず１点目として競争力がある部分を伸ばす。２点目として平均的な部分を底上げする。３点目として弱い部分を早急に改善するという３つがあると思うが、それぞれが改善されるのが望ましいものの、中でも最後の弱点改善が最も緊急度が高いのではないかと思う。2020年に向けて時間が足りないことに加えて、攻撃側は弱いところを意図的に突いてくるからである。しかし、これらの組織は数も多く、国が隅々まで目を光らせることはできないと思う。

そこで、１点目の競争力のある組織に手伝ってもらって底上げを図ることも検討すべきではないかと思う。費用の分担など難しい問題があるとは思うが、こうした調整をNISCが担うことも、先に述べた一歩前に出るアプローチになり得るのではないかと考える。

○（前田本部員）

まず決定事項については、私もこれで全く問題ないと思う。

一言だけ触れさせもらうと、重要インフラの情報セキュリティの確保は、事案が起こったとき、発生時のオペレーションの問題まで含めて考えることが重要であって、NISC、重要インフラ事業者と対象機関、警察を初めとする省庁との連携がさらに緊密化されるべきだと思っていたのだが、それが盛り込まれたということで非常に望ましい。さらに一層、実効性のある連携

に高めていっていただきたいと思う。

討議事項である「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」に関しては、これはどう変わっていくかということで、そんなに大きくは変わらないと思うが、今、二つの大きな力が働いていて、一つはサイバーセキュリティの状況が、厳しさをむしろ増している。先日、海外の組織がインターネットテレビを使って盗聴しており、これは先ほど提示されたボットの対策がいかに大事かということに直結していると思う。また、我々大学関係では私立大学で４万人分の個人情報が漏えいしたりとか、民間でも不正アクセスで個人情報が漏えいしたり、５万件の情報が漏えいした報告があった。ますます深刻化しており、それに対してどう対処するかという意識は大事である。

もう一つは2020年東京オリンピック・パラリンピック競技大会が、サイバーセキュリティの方針に、本格的に大きく影響してくるであろう。

今回、セキュリティ情報センターを警察庁に設置して、現実の具体的な対応を図る。そのために動き出すということになると、ほかのセンターとのバランスをどうしていくか、いろいろな問題があると思うが、情報は何のために集めるかといえば、問題を解決するために役立つ情報でなければ意味がない。もう2020年東京オリンピック・パラリンピック競技大会は絶対に失敗の許されない背水の陣で臨まなければいけない。それを成功させるために、どういう情報をどう集めて、どう利用していくかということが明確に意識する。これは、この討議事項にある「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」に大きく影響してくると思う。2020年東京オリンピック・パラリンピック競技大会への対策ということではなくて、（1964年の）東京オリンピックがその後の日本を変えたように、セキュリティの問題もこれが一つのきっかけとなっていく。そういう大きな力をばねとして生かしていくべきなのだと思う。

最後に一つ、林本部員が発言した中小企業対策のことを一言申し上げておく。方針が大きく変わるというのは、これまで携わってきて、重要インフラであり、政府でありと言ってきたが、最近のいろいろな事件でも、例えば企業の不正アクセスで個人情報が75万件抜かれただけではなくて、ビットコインで130万円払えといったものが発生しており、中小企業の社長たちは困っている。困ったときに、どこにどう相談して、誰がどう助けてくれるか。今までは国民に大きな影響を与える重要インフラを守ることが第一で、それはそれで正しいが、そろそろ企業の主体、中小企業という言い方は良いか悪いか分からないが、その方々に対しても、国は頼りになり、サイバーの問題で解決してもらうという動きが必要ではないだろうか。地方公共団体では少しずつ動き出しているが、やはり国で、むしろ経済産業省の仕事かもしれないが、このNISCの視野が少し広がっていかないといけないのではないか。重要インフラで大事なものだけではなく、その周辺を広げるニーズが出てきているのではないかと感じている。

○（村井本部員）

３点ほど申し上げる。

一つは、いろいろな計画が立てられていてすばらしいけれども、計画はすばらしくてもきち

んと評価がされなければ意味がない。サイバーセキュリティの評価というものはだんだん成熟してきている。国別の安全度はサイバーグリーンという、もとはJPCERT、すなわち経産省のもとでできていたものが、今や世界レベルでいろいろな物差しを作るようになった。物差しで計るということがいつでも大切であり、ある施策を実行したら、その効果が１年後に出たとか、２年後に出たとか、こういう競争も重要である。そういうことを指標として持っておくことは非常に重要だと思う。

アメリカはDHSが幾つかの指標を作っており、それを用いて評価をしている。ちなみに、NISCは昔から各省庁の成績表をつけて公開していたが、最初はとても嫌がられたものの、政府のシステムの安全性や取組状況を公開していた。このようなものは継続的にやらなければいけないが、一つ問題点があって、NISCの守備範囲が政府の省庁だけではなくて、例えば地方公共団体はどうなのかとか、民間セクターはどうなのかという議論がある。

もう一つ、新しいことが出てきている。それは民間セクターの中でも農業がIT化されたり、医療が情報化されたりしている。そうすると、医療機器の担当省庁というのは当然、厚生労働省である。農業機器というのは自動車と似たようなものだけれども、これは経済産業省ではなくて農林水産省である。そうすると、責任を持つ省庁が違うことになる。当然、そこに対する産業の結びつきも違う。つまり、このIoT時代になって、今まで余り関係のなかった省庁がかなり主要な役割を果たすようになってくる。そこで重要になることは２つあると思う。

一つは、縦割りだったものを、サイバーセキュリティを横軸にしっかりと考えること。このような時代なので、内閣にあるNISCの役割はとても重要であり、そのことを考えなければいけない責任がある。つまり、守備範囲を広げる。先ほどの大企業と中小企業という発言も、縦と横の関係になると思う。それから、新産業がIT化する。そうすると、やはり省庁の責任が広がるため、この民間に対する連携の仕方が重要になる。

そして、地方行政。これは何度もここで申し上げているが、いろいろなレベルの地方自治体が、市民の大切な情報を持っており、この階層構造をどのようにしてつなぐかは、内閣でしかできないということだと思う。

最後に、2020年東京オリンピック・パラリンピック競技大会は、この縦を横につなぐということの一番象徴的な目標を、2020年に結びつけることができるという意味で、非常に重要だと思う。しかし、「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」に関する資料を見てもセンターが３つも出てくるが、中心になると思われるセンターがたくさんあるというのは、担当が縦割りだということを感じるので、横につながるように是非うまく進めていただきたい。

○（遠藤本部員）

行動計画及び人材育成、決定事項については賛成である。

サイバーセキュリティの戦略、中間のレビューということでまとめていただいており、これに関して少しコメントを申し上げる。

まず、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サイバーセキュリティの整備というものが非常に重要なポイントであり、このような計画もまとめていて、実際に実行フェーズに入ったと考えるべきであろう。特に現在、重要インフラに対してはライフラインの観点、人の安全の観点、そして、国民の安全の観点から、国家による積極的なサポート、または支援というものが必要であろうと考える。

重要インフラに関しては、現在、リスクマネジメントの促進ということでリスクのチェックをしていただいているが、常に継続的にリスクをチェックするという機能が必要で、これをどういう形で継続させるのか、またはしてもらうのか。この辺りは、場合によっては立法が必要かもしれない。

さらに、リスクを挙げた以上は、これを処置する必要があるが、この促進をどういう期間内にやるべきなのか。そのためには、場合によっては促進をするための援助、お金の援助も含めたアクセラレーションが必要であろう。これも立法が必要かもしれない。

最後はメンテナンスという観点で、情報の収集、さらには処置に対する、施設等に関する情報の提供。この仕組みをしっかりと作り上げる。これも重要であり、この３つに関しての国家による積極的なサポートをお願い申し上げる。

時期に関して、2020年東京オリンピック・パラリンピック競技大会というものが一つのターゲットだが、その前年のラグビーワールドカップ2019で一度確認をするというフェーズを考えることがとても重要で、ラグビーワールドカップ2019をベースに一旦レビューをいただく。それで2020年東京オリンピック・パラリンピック競技大会に対応するということが、実行の日程上は考えることが重要であろうと思う。

それから、村井本部員の発言にもあったが、やはりNISCの役割というものが非常に大きいと私も思う。「サイバーセキュリティ戦略中間レビュー（骨子案）」の中の６ページの（ウ）という項目の中に「ａ．我が国の安全の確保」という項目があるが、その中に「国全体として、関係機関相互の連携強化及び役割分担の明確化を図りつつ、組織・分野横断的な取組を総合的に推進する」と記述されている。まさにそのとおりで、これの役割の主体は、やはり私はNISCだと思う。取りまとめ的な役割ということから、実効的な統括・指示ができるという役割をもNISCが負っていただくこと、または国家主体で動いていただくことを期待したい。

最後は、サイバーセキュリティの整備というお話を申し上げたが、情報の共有化の観点である。これについては何回も私は申し上げているが、現在もAIの進化というものもあって、技術の進歩を先取りした情報の収集のあり方、または情報の提供のあり方を考えていくべきではないか。そこでやはり一番気にしなくてはいけないのは、情報収集のリアルタイム性という観点であろうと思う。実際には、情報の共有によっていろんなサーバーのマルウェアの撲滅作戦が成功しており、共有の重要性は我々も既に理解している。その中でも、いかにリアルタイムにそういうものを実行していくかということがとても重要で、そのためにはAI等を使った戦略が必要であり、解析の部分を開発していくという戦略が必要であろうと思う。

もう一つ問題なのは、情報を提供していただくためにはそれの匿名性が必要であり、その匿

名をしたものを解析するのは、マルウェア分析の相当高度な技術を持った者が必要ということ。その観点からは、やはり今申し上げたように、AIを使ったマルウェア分析というものの導入が必須ではないかなというように思う。

もう一点申し上げる。情報の共有をした後に、それが漏えいしてしまっては困るので、その漏えい対策というものも一つ考えておかなければいけない。

その対策というものは幾つかフェーズがあると思うが、最初は、できれば情報処理安全確保支援士を有する組織が参加されることが必要かと思う。最低限のセキュリティ対策を実施されている組織に最初は限定して共有化というものもあり得るのではないか。いずれにしても、実行フェーズに入っており、まさに村井本部員の発言にあるようなKPIを含めたことを実行ができる体制を作ることに、いろいろな観点で御支援賜りたい。

○（小野寺本部員）

決定事項については特に大きな問題はないと思う。

今回いただいたサイバー戦略中間レビュー（骨子案）について、３点申し上げたい。

まず１点目は、総論の文章についてである。これは下から３分の１くらいのところに「また、サイバー空間の関係主体は」という表現があるが、この表現でいくと、これまでは事業者などの技術を有する者だけではなく、一般企業、個人にも拡大し、その数がさらに拡散するとともにという書き方で、今までは技術がある人がやっていたけれども、技術のない人がどんどん入ってくるように読めてしまうので、ここの表現は少し改める必要があるのではないかと思う。

先ほどの村井本部員の発言に関わることだが、今まではどちらかというと、ここに書かれているような、通信にしろ、コンテンツとかアプリケーションにしてもそうだが、いわゆる業としてサービスをしていた人たちが主で、それを利用する人との関係だったと思う。しかし、どうも今後は、先ほどの農業の話や、医療関係がそうであるように、自らの業の中にそれを使っているだけで、ICTが表に出ない形にどんどんなってきてしまう。そうなってきたときの、このサイバーセキュリティをどう扱うのだということが非常に厄介な問題になってきているのだろうと思う。

各省庁横断というものはもちろん、先ほどからお話のあることと関係するが、いわゆるリテラシーという言葉がいいかどうかは別にして、最低限のものを国民全体に伝えていかないとまずいのではないかなと思う。これは大分昔に私も申し上げたことがあるが、車の普及期には、今でもやっていることだが、幼稚園から交通安全教室をやっている。これは命にかかわるので多分そうなっているのだろうと思うが、実はこのサイバーの問題というものは、本当はそれに匹敵するぐらい重要なことであって、そのためにはやはり何かきちっとした仕組みをつくっていかないと、国民全体のリテラシーが上がらないのではないかなと危惧している。

２点目は、情報共有対策である。これは皆さんの発言のとおりなので、バーチャルな情報連携センター、こういうものをつくっていくことは非常に重要だと思う。

皆さんが発言していることと関係することだが、この情報提供する人が不利にならない、不

利益にならないような仕組みを何かつくっていかないと、民間のほうから見ると、正直、自分のところの情報が漏れているということを公に言いたくはないと思われる。それによってデメリットが出てくるとなると、情報提供しなくなるのではないかなと思う。まず情報提供者が不利益をこうむらないような何らかの方法を検討する必要があるのではないかという点。それと、やはりインシデント情報を交換するためのフォーマット。これをまず標準化していかないと、なかなかそこまでたどり着かないだろうと思う。

この不利益を被らないということと、そのフォーマットというものは実は関係してくるのではないかと思っており、インシデント情報の加工手法のガイドラインとか、そういうものがますます必要になってきているのではないかなと思う。

３点目は、今回、情報社会の活力の向上及び持続的発展のところで、２番目に安全なIoTシステムの創出をうたっているが、私はここが非常に重要だと思っている。産業界にとっては、この安全なIoTシステムをつくることによって国際競争力の強化が図られるのは間違いないと思っている。特に日本の場合にはものづくりが得意だということが昔から言われており、そうすると、このものづくりと結びついて、このIoTシステムをどうやって構築していくのかということが非常に重要になってくるのではないかと思う。

現状でも、実は例えばどこにどこの会社のルーターが設置されているかというのがわからなくなってしまって、そのために、そのルーターの脆弱性がわかっても、そのルーターにアクセスすることができなくなってしまっている。これは非常に大きな問題だと思っており、言葉の点から言うと正しいかどうか、私も分かりかねるが、トレーサビリティーのような考え方を導入して、どこに何があるのかということが後からでもわかるようにしておかないと、とんでもない数のIoTが入って来たときに、セキュリティを守る前の段階で、どこに何があるかわからないということになってしまう方が非常に恐ろしいのではないかなと思う。

安全なIoTシステムの創出というものは非常に重要であり、また、そこに日本として貢献できる要素が非常に大きいのだろうと思うので、ぜひその辺を検討していただきたい。

○（中谷本部員）

私からは５点申し上げたい。

第１に、重要インフラサービス障害に係る深刻度判断基準を５段階で明示することは非常に結構なことであり、早期に導入していただきたいと思う。一口にサイバー攻撃といっても、その程度は地震同様に様々であり、震度１と震度７では社会へのインパクトも必要な対応も大きく異なるため、国民のサイバーセキュリティに対する意識を真の意味で高めるためにも、基準の明示は重要であると考える。

第２に、サイバーセキュリティ戦略中間レビュー（骨子素案）において、IoT機器がサイバー攻撃の踏み台として悪用されないようにするためのサイバーセキュリティ強化が今後の推進強化において挙げられたことは、今後の社会を見据えた対応として評価したいと思う。更に一歩進めて、IoTが踏み台になってサイバー攻撃が生じてしまった場合に製造物責任を課すこ

とができるか、あるいはどの範囲でできるかについての法的検討も、今後進めることが望まれるかと思う。

第３に、小野寺本部員も御指摘の安全なIoTシステムの創出による国際競争力の強化に関して、日本としてぜひ、この分野で国際標準をとっていただきたいと思う。国際標準を制する国や企業団体は、その分野の業界を事実上制すると言っても過言ではなく、IoTに限らず、国際標準戦略を一層強化する必要があると考えるが、安全なIoTシステムの国際標準をとることは日本政府と日本企業、オールジャパンで連携することで可能であると思う。また、何よりも世界全体のサイバーセキュリティに対する日本の重要な貢献にもなり得るので、ぜひイニシアチブをとって進めていただきたいと思う。

第４に、国際的な動向に関して、エストニアにあるNATOのサイバー防衛センターの協力を得て、米国のマイケル・シュミット教授を中心とした国際法の専門家がまとめたタリン・マニュアル2.0が２月に公表された。これはサイバー行動に関連する各分野の国際法を包括的に記述し解説するものであり、全154条から構成されている。私自身、メンバーとして３回、タリンの会議に出席し、作成に関与した。日本政府を初め、多くの国の政府が参考にしていただければ幸いである。

第５に、サイバーセキュリティ人材育成に関して、人材育成プログラム案は非常に結構なものであって、支持したいと思うが、特に国家公務員志願者のサイバーセキュリティへの意識を高めてもらうための手っ取り早い一つの簡単なアイデアとして、国家公務員試験の択一式の問題の中に、必ず１問はサイバーセキュリティ関連の問題を出題するように配慮することが望ましいと思う。

○（丸川東京オリンピック競技大会・パラリンピック競技大会担当大臣（副本部長））

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「大会に向けたセキュリティ基本戦略」を決定して、内閣総理大臣を本部長とするオリパラ推進本部において報告をした。

その中では、大会に向けた各種のテロ対策やサイバーセキュリティ対策の強化に加えて、大会の安全・円滑な準備、運営、継続性を確保するため、大会運営に影響を与える可能性のある重要サービスを継続させるための諸対策を促進することとしている。

電力・通信・交通など、重要サービス事業者におけるサイバーリスクの評価については、各事業者による評価のみならず、今後、我が国全体としてリスク対策が最適化され、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に行っていきたいと考えている。関係省庁におかれましては引き続き、御協力をよろしくお願い申し上げる。

○（松本国家公安委員長）

昨年中は、サイバー攻撃が世界規模で発生したほか、インターネットバンキングに係る不正送金事犯等のサイバー犯罪も多発しており、サイバー空間の脅威は深刻化している状況にある。

2020年東京オリンピック・パラリンピック競技大会の開催を見据え、大会組織委員会や関係省庁、重要インフラ事業者等との情報共有・共同対処訓練の積極的な実施等による官民連携の推進を図るなど、サイバー空間の脅威への対処に万全を期すよう、警察庁を指導していく。

○（世耕経済産業大臣）

従来から訴えてきた医療、水道、物流、航空、鉄道、クレジットなどの各分野において、J-CSIPを活用して情報共有を強化していくこととなったことをまず歓迎したいと思う。経産省としても、IPAを所管する立場として、NISCや関係省庁と一体となって進めていきたいと思う。

あわせて、業界・業種横断的な情報共有・分析体制についても、これを強化していく方針とのことだが、NISCにおいて、速やかに実効的な情報共有の制度的枠組みを具体的に御提示いただいて、来年の通常国会への法案提出も含めて、早期に実現を図っていただきたいと思う。

また、リスク評価について、2018年度までに全ての重要インフラ分野で実施する方針であると伺っているが、経産省では、昨年度は当省所管のエネルギー関係の２分野について先行的に実施した。今年度は、当省所管の重要インフラの少なくとも２分野について、新たにIPAの産業サイバーセキュリティセンターの機能を活用してリスク評価を進める方針である。他の分野についても、このセンターの機能を積極的に御利用いただきたいと思う。

更に国際連携について、当省としても、今月IPAに開所した産業サイバーセキュリティセンターを活用し、米国と共同演習などを進めていく。このセンターには、経産省の所管業種に限らず、放送・通信、鉄道など、幅広い分野から80名程度の受講生が集まっている。我が国のサイバーセキュリティの将来を担う人材を、このセンターから輩出していきたいと思う。

本日のこの戦略本部の決定で、サイバーセキュリティの取り組みに一定の進歩があったと思うが、これは最初の第一歩にすぎないと思う。経産省としても人材育成や国産技術の発掘、育成などを通じた、サイバーセキュリティ産業の競争力強化に取り組んでいきたいと思う。

特に人材育成について、先ほど申し上げたサイバーセキュリティセンターの80名であるが、これはまだ３桁から４桁足りないと思う。本日のアメリカのウィルバー・ロス商務長官との会談の中でも、私のほうからサイバーセキュリティ人材育成での日米協力を持ちかけ、合意をしたところである。

今後、こういったアメリカの力もか借りながら、政府全体として、先ほどIoTになったときにどう管理するのかというお話も出てきたが、第４次産業革命の進展に合わせて、サイバーセキュリティの強化と、そして、やはり国産の技術力の強化ということをしっかりと取り組んでいかなければならないと思う。

○（鶴保情報通信技術（IT）政策担当大臣）

昨年12月に施行された「官民データ活用推進基本法」に基づき、先月末、総理を議長とする「官民データ活用推進戦略会議」を立ち上げた。官民データ活用推進に向けた推進体制を整備したところである。

官民データ活用の推進とセキュリティの確保は車の両輪であり、本日のテーマの一つである人材育成プログラムは、安全・安心なデータの利活用の環境整備において、重要なポイントである。

プログラムの実施に当たっては、人材の需要と供給を相応させる具体的な目標と計画を設定し、PDCAをしっかり回していく必要があり、IT政策担当大臣として「官民データ活用推進基本計画」にも反映させてまいりたいと考えている。

○（あかま総務副大臣）

人材育成について、総務省の取り組みを御紹介する。

平成25年度から国の行政機関や重要インフラ事業者を主な対象として、実践的サイバー防御演習（CYDER）を実施している。平成28年度においては、地方自治体等に対象を拡大して、約1,500名に対して実施した。今年度は約3,000名に対して実施する予定である。

また、４月１日に、総務省所管の国立研究開発法人である情報通信研究機構に「ナショナルサイバートレーニングセンター」を組織し、CYDERに加えて、新た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こととしている。今月３日から28日まで、若手セキュリティエンジニアの育成について受講生を募集したが、既に募集定員の５倍を超える応募があった。

総務省として、これらの取り組みを通じて、引き続き関係府省と連携をして、我が国のサイバーセキュリティの向上に尽力をしてまいりたいと思う。

○（武井外務大臣政務官）

我が国は「法の支配」が貫徹された、自由で公正かつ安全なサイバー空間を求めている。他方、現実には、国家主権に基づく国内管理を優先する国も多数存在している。

今月11日のG7外相会合では「サイバー空間における責任ある国家の行動に関するG7（ルッカ）宣言」を発出した。G7として、アクセス可能で開かれた、信頼できる、安全なサイバー空間の実現に向けたメッセージを世界に発信した。

２月には、信頼醸成を進めるため、日中韓サイバー協議を、また３月には、アジア大洋州地域における能力構築支援の一環として、第２回日・ASEANサイバー犯罪対策対話を実施した。

外務省としては、サイバーセキュリティ戦略中間レビュー、また、今日の御議論も踏まえ、引き続き、米国を含めて、二国間・多国間のサイバー協議を通じて、国際ルール策定、信頼醸成、能力構築支援に取り組んでまいりたい。

○（宮澤防衛大臣政務官）

防衛省から一言申し上げる。

自衛隊の部隊等がさまざまな場面において任務を遂行するに当たり、情報通信、航空、鉄道、電力等の重要インフラが正常に機能することが極めて重要となる。

このたび、重要インフラの情報セキュリティに係る第４次行動計画が決定され、重要インフラの情報セキュリティ対策が強化されることは大変望ましいことであり、防衛省としても情報共有等の協力を引き続き行ってまいりたいと考えている。

また、サイバー攻撃が高度化・巧妙化する中で、それに適切に対処するためには、防衛省としてもサイバーセキュリティ人材の育成が喫緊の課題と認識している。

取組としては、実戦的なサイバー演習を目的としてサイバー防衛隊を増員すること、高度な人材を育成するため各種研修へ参加すること、部外の人材でコンピューターセキュリティに高い知見を有する者を佐官や尉官クラスで幹部自衛官として採用するためにその枠組みを整備することなど、さまざまな取り組みを進めている。

東京オリンピック・パラリンピック競技大会が開催される2020年も見据え、我が国全体のサイバーセキュリティを強化する取り組みに対して、防衛省としても、情報共有などの協力を積極的に行っていきたいと考えている。

(3)　決定事項の決定等

決定事項２件につき、案のとおり決定した。

(4)　副本部長締め括り挨拶

本日は活発な御意見をいただき、厚く御礼申し上げる。

政府としては、本日の議論を踏まえ、重要インフラ防護及び人材育成に着実に取り組むとともに、2020年及びその後を見据えたサイバーセキュリティのあり方についても議論を進めていく。

有識者の皆様におかれては、引き続き御協力のほどをよろしくお願い申し上げる。

－　以上　－