サイバーセキュリティ戦略本部
第10回会合　議事概要

１　日時

平成28年10月12日（水）　８：00～９：00

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
岸　　信夫	外務副大臣
宮澤　博行	防衛大臣政務官
橋本　　岳	厚生労働副大臣
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
野上 浩太郎	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

本日は早朝から御参集いただき、感謝申し上げる。

日本年金機構に対する悪質極まりないサイバー攻撃による個人情報流出事案を受けて、先の通常国会で成立した改正サイバーセキュリティ基本法が今月から施行され、独立行政法人のほか、指定を受けた特殊法人、認可法人が新たにNISCによるセキュリティ監査等の対象となる。

政府としては、改正法を着実に運用し、これらの法人のサイバーセキュリティ対策に、しっかりと取り組んでいく必要があると考えている。

また、2020 年東京オリンピック・パラリンピック競技大会の開催まで、いよいよ４年を切った。これらの大会を見据え、国民の社会生活の基盤となる重要インフラについて、事業者との情報共有や連携を進め、防護対策をしっかりと行うことは不可欠である。

そこで、本日の会合では、新たにNISCによる監査の対象となる特殊法人等の指定について御議論いただくと同時に、「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」の見直しの骨子について意見交換を行い、今後の検討の参考としたい。

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基本法第 13 条の規定に基づきサイバーセキュリティ戦略本部が指定する法人について
- サイバーセキュリティ基本法の一部改正に伴う関係規則等の整備について

【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号に基づく監査の状況について
- 高度サイバー攻撃対処のためのリスク評価等のガイドラインの改定につい
- 「各府省庁セキュリティ・IT 人材確保・育成計画」の作成状況について
- 「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」の見直し骨子について
- 安全なIoTシステムのためのセキュリティに関する一般的枠組について
- 2016年リオデジャネイロオリンピック・パラリンピック競技大会における状況について
- 国際社会の平和・安定及び我が国の安全保障に係るサイバーセキュリティ戦略の推進状況について
- 政府のサイバーセキュリティに関する予算について

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。

○（小野寺本部員）３点申し上げる。

まず、今回のサイバーセキュリティ基本法第13条に基づいて、新たに法人が指定され

た。これは大変重要なことだと思っている。その中で少々気になることがある。マイナンバー関係で J-LIS が指定されており、これは当然といえば当然のことであるが、心配なのは、マイナンバーを直接取り扱う地方自治体を誰がどのように取り扱っているのかということ。地方自治体の自治という問題との絡みがあるようには伺っているが、サイバーセキュリティに関しては、やはり何らかの地方自治体の統一基準的なものをつくっていただいて、それを誰かがきちんと見ていかないと、非常に難しいのではないかと思う。今回、戦略本部が指定する法人について、資料２－１の２ページに①から④の要件が書かれているが、まさしく地方自治体はこの①から④の要件に該当する機関であるのは間違いないのではないか。そういう意味で、地方自治体をどのように取り扱うのか、よく御検討いただきたい。

２点目は重要インフラに関連することであるが、相互依存性を追加して考慮するということで、大変良い方向に動いていると思っている。実は重要インフラ分野間での共通領域がある。それは、重要インフラ事業の運営に当たり、各分野の IT、OT におけるクラウド、仮想化、IoT といろいろな技術が進んでいるが、その中でも OS、具体的に言うと、マイクロソフトであるとか、グーグル、アップルであるが、これらへの依存度がますます高まっているのが実態である。これらの共通領域について重要インフラ間で情報共有をすることは、非常に大きな意義がある。各重要インフラが個別にやっていたのでは時間と人の無駄になると思うので、是非この共通領域部分の情報共有についてどのような体制をとっていくべきか、御検討いただきたい。

３点目は、監査についてである。監査の一つの大きな要素というのは継続実施にある。今回、年金機構等の監査の中間報告にもあったが、この監査を次にどういう方法で、どういう格好でやるのかを明示することによって、監査を受ける側が、まずこういうことをもっとちゃんと考えなければならない、ということを理解できるのではないか。そういう意味で、監査報告を書くときに、次回以降の監査計画も、具体的にこういう監査計画を今後予定している、ということを書くことが、監査を受ける側にとって非常にプレッシャーにもなり、良い方向に動くのではないかと思う。是非、報告の中には次回以降の監査計画も織り込んでいただきたい。

○（中谷本部員）６点申し上げる。

第１に、監視、原因究明調査、監査の対象になる指定法人について、公的年金関連の８法人及びマイナンバー関連の１法人を今回指定したことは、まことに適切だと考えるが、今後、更に重要インフラに関連する特殊法人や認可法人は、必要に応じて小まめに、速やかに指定していくことが大切であると考える。

第２に、政府の IT 人材確保、育成計画が作成されることは大いに結構なことであるが、将来的には、国家公務員の採用に際してサイバーという試験区分を設けることが望ましい。大学教育や大学院教育とも連動する問題であるため、一朝一夕にはいかないであろうが、長期的な検討には値する。

第３に、「サイバーセキュリティ政策に係る年次報告（2015 年度）」を改めて拝見し、「国際社会の平和・安定及び我が国の安全保障」に記された各省庁の取組が着実に進められていることを心強く感じた。欧米諸国やアジア諸国との連携やキャパシティ・ビルディ

ングに進展が見られるのは大いに望ましいことであるが、そう申し上げた上で、更に強いて特定の地域との関連で付言すれば、今後は更に湾岸 GCC 諸国とのサイバー対話やキャパシティ・ビルディングにも積極的に取り組んでいただきたい。単にホルムズ海峡に近接する世界最大規模の原油供給源であるのみならず、巨額の資金の政府系ファンドを有しているため、GCC 諸国がもしサイバー攻撃を受ければ、世界経済に重大な悪影響を及ぼすことは必至であり、我が国として予防的な支援を進めることは、我が国自身の国益にもかなうものである。

第４に、中国の南シナ海や東シナ海での野心的な活動や、北朝鮮によるミサイル発射、核実験など、我が国を取り巻く国際環境は、以前にも増して厳しくなっていることは否定できない。こうした力による現状変更、国際秩序への挑戦は、海や空を舞台にするのみならず、サイバー空間における脅威も今後更に増大することを覚悟しなければならない。また、先週、米国は、「ロシアが米国大統領選挙の妨害のためサイバー攻撃を指揮した」と非難する声明を出しており、今後の動向を注視する必要がある。

第５に、今後の国際社会において懸念されることの一つとして、人工知能を悪用したサイバー攻撃が高度化することが考えられる。防御側も人工知能を指導して行うため、人工知能対人工知能の戦いが展開されると思われるが、今後、人工知能についての国際ルールを作成する際には、サイバー攻撃との関連にも十分に配慮することが求められるであろう。

第６に、富山大学の水素同位体科学研究センターに対するサイバー攻撃がなされたことは遺憾である。大学は、安全保障輸出管理についてもそうであるが、サイバーセキュリティについてもやや甘いところがあることは否めないと、大学人の一人として感じている。早急な対策が必要であるが、政府としても必要な支援をお願いしたい。

○（野原本部員）４点申し上げる。

まず１点目は、小野寺本部員、中谷本部員も発言されたので一言にするが、今回の指定法人を９法人指定したという取組は非常に適切だと思うが、この９法人だけでなく、随時必要に応じて柔軟に追加していくというような姿勢を保つことが重要である。

２点目は、重要インフラ関連の体制や施策展開についてである。今年６月に行われたサイバーセキュリティ戦略本部第８回会合で、今年度の施策について、重要インフラの施策は業界共通の施策が大半であるが、各業界それぞれに固有の対策をもっと追加、充実すべきと発言をした。今回の行動計画の見直しについては、全体の取組方向としては、３つの重点を始め、適切だと思うが、第８回会合での発言同様、今後の取組を進めていく過程で各業界、分野に固有の問題点及び課題を把握、分析して、特有の課題を解決する取組をしっかり実施していただきたい。

また、一方で、重要インフラ分野の取組体制は基本的に全体計画、進捗管理を NISC が行い、具体的な検討、取組を所管省庁が担当するという構成になっているが、先ほど小野寺本部員も発言されたが、共通領域のやり方として、そのやり方では縦割りの弊害が出やすいと考える。既に省庁間で適宜連携されていると思うが、共通的な施策の部分について、もっと NISC が踏み込んで、適切な取組ができるような体制を考えるべきではないか。

３点目は「各府省庁セキュリティ・IT 人材確保・育成計画」についてである。資料５の

内容については、情報セキュリティ政策会議においても、８、９年前からずっと私は発言をし続けてきたことで、ようやく人材育成強化方針や各省の計画にその内容がしっかり組み込まれたことを感慨深く、うれしく思っている。当時申し上げたことは、政府機関のセキュリティ関連部署を一般的なキャリア官僚の通過職務とするのではなく、セキュリティ専門の人材を育成、確保すること、関連部署への計画的な異動などをさせてオン・ザ・ジョブ・トレーニングで育成していくこと、セキュリティ専門人材のキャリアパスを構築することなどで、折に触れ、提案してきた。したがって、今回の内容について全く異存はないが、まだこの計画内容だけで十分とは言えない。例えば体制の整備について見ると、本省全体で約100人の増員要求とあるが、それでも各省平均にすると数名の増員に過ぎず、これで十分とは言えない。その上、この実現は2019年からということで、先の話でもある。一説には、潜在的な必要増員数は全体で何千人の規模とも言われており、とても十分とは思えないので、更に強化していただきたい。

４点目は、IoTシステムのためのセキュリティについてである。NISCが各省庁に対して提示している一般的枠組としては、資料７にまとめられたとおりだと思う。これまでも論じてきたとおり、IoTシステムに関するプレーヤーというのは非常に幅広いので、ネットワークセキュリティを考えたことのないプレーヤーも多いというのが特徴で、その特徴を踏まえたものとして、今回の枠組は適切であり、これに沿ってガイドラインづくり等が進むことで、適切な対応が進んでいくと期待している。

しかし、一方で、ネットカメラやデジタルビデオレコーダー、いわゆるハードディスクレコーダーであるが、これらのIoTデバイスを踏み台にしたDDoS攻撃が既に発生している。攻撃者がインターネットをスキャンして、ポートを開いているデバイスを見つけて、デフォルトのアドミンなどでログインすると、簡単に乗っ取ることができるというのが現状である。つまり、既に普及しているIoTデバイスを狙った攻撃が発生しているので、関係者への取組だけではなく、一般ユーザーに対してもパスワードの設定の仕方など適切な対応をとるように、でも、過度な不安を煽ることなく、わかりやすく伝えていくということが重要で、この周知の仕方が必要だと思う。

○（林本部員）本日の決定事項等には全く異論がないことを申し上げた上で、インシデント情報の共有が非常に大切だという認識が深まる中で、昨年末から今年の夏にかけて、アメリカとEUの両方で画期的とも言えるサイバー関係の法律が制定されたので、その点に絞ってコメントさせていただく。

アメリカでは従来から、サイバーインシデントの情報を共有しようとしても、幾つかの障害があると言われてきた。まず、①民間が政府と共有したデータが情報公開されるのではないか、②共有データに含まれる個人データのプライバシーが心配だ、③独禁法違反の可能性があるのではないか、④提供情報によって違法行為が摘発されるのではないか、といった懸念があり、共有が期待どおりに進まなかった。

そこで、これまでも何本もの法律案が提案されてきたが、ようやく昨年末に2015年サイバーセキュリティ法の一部として、サイバーセキュリティ情報共有法が制定された。この法律は、先の４点の要請に応えるものだと思う。

独禁法上の免責に加えて、民間企業が情報ネットワークシステムをモニタリングするこ

とや、政府と脅威指標（サイバー・スレット・インジケーター、CTI）や防護手段（ディフェンシブ・メジャーズ）に関する情報を共有したことで、裁判で訴追されることはないというようにしている。そして、これを民間から政府へ情報が提供されるインセンティブとするほか、政府機関もセキュリティクリアランスを条件に、機密指定の情報を民間にも提供するなど、互恵的な仕組みをつくっている。

一方、EUのDirective on Security of Network and Information Systems、通称NIS指令も、2013年早々以来の長い検討を経て、去る７月６日に欧州議会で可決された。これは加盟国に以下の５つの義務を課すものである。

１点目は、NISに関する国家戦略の策定。

２点目は、所管官庁、シングル・コンタクト・ポイント、CSIRTの指定。

３点目は、協調あるいは協力グループの設置。

４点目は、CSIRTネットワークの構築。

５点目が注目されるが、基本サービス事業者（オペレーター・オブ・エッセンシャル・サービス、OES）とデジタルサービス提供者（デジタル・サービス・プロバイダー、DSP）という事業者を指定して、それらのセキュリティ要件と事故通知義務を定めている。

このNIS指令は、加盟国が多いため、そのセキュリティレベルの差を認めた上で、CSIRTやシングル・コンタクト・ポイントの指定など、最低限の協調の仕組みを整えると同時に、従来、重要インフラとしてきた産業の中から、先ほど述べたOESとDSPに特に注目して、セキュリティレベルの統一と事故通知の義務を課している点が注目される。

ここで、DSPを取り上げ、EU内に施設や本社があるかリプレゼンタティブがいる場合にNIS指令を適用するとしていることは、先行するアメリカ企業にも同様の義務を課すという意思を強調したものと思われる。

両者を比較すると、インターネット発祥の地であり、安全保障と一体化しているアメリカでは、自律、分散、協調という理念を守って、情報共有に参加するかどうかは民間企業の任意としている。一方、EUでは、国家安全保障は主権国家の役割で、EUとは別だという制約もあるが、民間企業であるOESやDSPに法的義務を課し、罰則もあるという点で大きな違いがある。

我が国の方針は、今後、これらを十分検討した上で決定すべきだと思うが、私個人はインターネットの歴史と情報という見えないものを扱うという点から、少なくとも当面はアメリカ方式のほうがよいのではないかと思っている。

○（前田本部員）私は、刑事法、犯罪に関する研究をしており、その角度から、今までの本部員と若干違うトーンでコメントをさせていただく。

まず初めに、基本法13条に基づく指定法人の件、全く異存はない。

それを踏まえて、最近のテロも含めたサイバー犯罪情勢に関して感じることは、ロシアによる米国大統領選挙への介入や、先ほど御指摘があった富山大学における情報漏えいなど、いろいろ問題が起こっているが、国内では少し風向きが変わってきたということ。我々が一番着目するのは、サイバー犯罪という観点から見ると、犯人が捕まるようになってきたということ。先日も、世界的なホテルに侵入し、データを盗み、その情報からクレジットカードを作った上で、日本人の名前で大量に購入したという外国人集団が現に捕

まった。ホテルにサインしたことによって情報が抜かれる怖さを煽るというのはまずいと思うが、犯人が捕まったということが重要なのだと思う。今年の春には、いわゆるセキュリティホールをついた佐賀の少年の事件があったが、これも捜査によって犯人を捕まえることができた。まだ道は半ば、大変だと思うが、先ほど野原本部員が強調されてきたことの一つの反映だと思うが、人材育成は、もちろん十分ではないけれども、前向きに進んでいる。更に頑張って進めていただきたい。

事前に予防して、引っ掛からないようにすることを徹底するだけではなく、こういう不正をすると最後は捕まるという意味で、情報のトレーサビリティというか、ネットの世界では何をやっても大丈夫だと思わせない、ということが最後にどうしても必要なことだということを強調しておきたい。

その意味で、オリンピックに向けていろいろな対策をとる中で気になるのは、スマホやWi-Fi を使っていろいろな攻撃がある中で、そのトレーサビリティ、そうしたものにどう対応するかということ。もちろん動き出してはいるものの、やはり意識的にそうした攻撃に対して対応を展開していく必要があると思う。

一方で、ただ勢いよく進めていけば良いわけではない。クラウドにある情報から税務状況を把握する、証拠資料などを押さえるということが財務省から出されると、国民の反応は、国家権力が情報を管理するということについて、非常に厳しい反応というか、警戒心を持つのは当たり前だと思う。情報共有して、問題があったものをいかに有効に内閣としてつかまえて動いていくかということは大事であるが、先ほど林本部員が発言されたように、その進め方は検討すべきだと思う。アメリカ型、ヨーロッパ型と御紹介があったが、国柄に合わせて、日本に最も適した情報の有効な集め方、強制して集めるというのが日本でいいかどうかを慎重に検討しながらも、ただ、最後の最後のセーフティーネットとして、トレーサビリティの問題はきちっと押さえるということを一番申し上げたいと思う。

最後に１点、先ほどホテルから情報を抜かれたと申し上げたが、ここでは大きな企業、重要インフラにしても大企業ばかりであるが、ホテルにしても、情報を取られた被害者である。被害者を守るという視点ももちろん必要であり、その意味で、今までは能力から仕方がなかったが、中小企業のサイバーにおけるセキュリティを国がいかにバックアップするかという視点をもう少し強めていいのではないか。警察庁などではサイバー対策の中に中小企業を対象にしたものを取り組んでいると伺っており、非常に高く評価したいと思う。企業活動の中で財務関係、情報関係抜きに成り立っている企業はほとんど考えられない。それに関連する安心・安全を国の側から与えていくということは非常に重要なことだと考えている。

○（村井本部員）この夏、いろいろなサイバーセキュリティ関連の学会や研究活動に参加し、気がついたことがある。個人情報の漏えいなどに関して、匿名化したデータを使った上でも個人を特定される確率は何％かというようなことが研究成果として出てくるようになっている。確率が出てくるということが何を意味するかというと、リスクの確率が出るため、保険が成立するようになる。民間の保険でサイバーセキュリティのリスクをヘッジするという考え方は前からあるが、これが具体化してきた。

今、日本でも損保ジャパンでサイバー保険というものができ、その背景には、ケンブリッ

ジ大学等で作ったサイバーリスクシナリオを基に、そのときの損害、被害額を予想するという研究の手法を用いている。今回、重要インフラを対象にした議題があるが、重要インフラについて、政府は被害の予想額を出している。例えば何日間水がとまったら、それは産業インパクトとして、運輸、電気、工業などのどの分野にどれだけのインパクトがあり、営業停止の日数が分かると幾らの損害があるのか、重要インフラでは大体明確な数字を持っている。そうすると、重要インフラとサイバーセキュリティを掛け合わせ、サイバーセキュリティによってどの部分が停止すると、幾らの損害になるか、非常にはっきりと出てくる。そうすると、保険会社は動きやすくなる。

例えば、先日史上最大のDoSが発生したが、それは何をしているかというと、先ほど野原本部員から御説明があったように、設置してあるウェブカメラのパスワードが初期設定から変えられていないものがあり、それをスキャンし、踏み台にしてDoSを仕掛けると、最大のトラフィックになったということである。これについて被害総額はそこまで大きなものではない。何かが起こったとき、被害総額ときちんと結びつけて、対策に対する投資が決まってくる。まず一つは、このようなスタイルの調査をしなければならない。つまり、評価は必ず被害総額、被害額の予想やシナリオとともにやっていく必要があるというのが１点。そして、その調査と評価に政府が最初に投資をすると、民間の保険会社が動けるようになるため、以降は民間と民間との間で、サイバーセキュリティに対するより強い社会ができる。初期投資を国がすることによって、その後の回転は民間の間で向上していく。保険を入れるとこの考え方ができるため、特に重要インフラをきっかけにそのような方向へ進むことができるのではないかと思う。

もう一つは、小野寺本部員が発言された地方行政の件である。これも何度も議論になっているが、例えば自然災害の気象データや、個人情報の匿名化の部分は、やはり基礎自治体から発生する管理であるため、あらゆる地方行政に対して、サイバーセキュリティの考え方をどのように徹底できるかということは、非常に重要である。NISC の守備範囲が増えてくることはとても重要であるものの、繰り返しだが、地方行政に対する体制を、サイバーセキュリティに関して考えるということも、大変重要になるのではないかと思う。

○（遠藤本部員）まずは、基本法の一部改正により、対象が明確になった、または広がったということに対して、我々のサイバーセキュリティに関する意味合いというものが進歩したということであろうと思い、評価をしたい。

その他、６点申し上げる。

まず、最初は予算について、今回、平成28年度当初予算額よりも20%アップ、601億円の予算となった。非常に力を入れて評価していただいた結果ではないかと思う。

ただ、他国との比較という観点では、一番進んでいるアメリカにおいては、2017 年のサイバーセキュリティ予算は２兆円で今回の予算はその３％である。人口比率３分の１としても、我々がサイバーセキュリティにもう少し力を入れていく必要があるのではないかということと、一方では、アメリカはこれだけの予算が必要だと考えているのは、ICTを使った効率化が世の中で進んでいるということの対になる一つの評価であるとも思う。日本では、人口減少という問題があって、その中でいろいろなインフラ、そのメンテナンスも含めて、いかに我々がICTを使って省力化、または効率化をしていくかということが大

きな課題になっている。これらのことを意識しながらも、サイバーセキュリティに関する予算というものの今後の意味合いを考える必要があると思うし、重要な予算をとなった部分をいかに有効に使うかということにまた力を入れるべきであろう。

２番目は、今回の基本法の改正による省庁間、さらには法人の新たな指定をしたことについて、重要インフラについても同様に我々が意識すべきサイバーセキュリティ対応のインフラというものの明確な定義をしていく必要があると思う。電力、交通、さらには病院、大学。特に大学と病院が一体化しているところもある。これらを明確にイメージすることがとても重要ではないかと考えている。

現在、経済産業省では、仮称であるが、産業系サイバーセキュリティ推進センター、これをプラットホームとし、ペネトレーション試験や、人材育成をするという構想を持っていると伺っている。これを一つの重要インフラのサイバーセキュリティを守るためのプラットホームとしてお使いいただくことが、先ほど申し上げたような予算を有効に使う、さらには、共通化した情報を取っていくという観点で非常に重要であろうと思うことから、是非その観点を入れて推進をしていただきたい。

３番目は、人材である。これは、いつも話題になるが、総務省でもナショナルサイバートレーニングセンターというものをお考えいただいており、これも先ほどの経済産業省の考えている産業系サイバーセキュリティ推進センターとどのようにコラボレーションするかによって、その人材の育成というものが更に高いものになっていくかということをお考えいただくとありがたい。今は幅広い IT の知識、実践の能力、さらには倫理観というものが教育の基本であろうと思うが、これはまず、最初のステップの教育であり、更に高いレベルの、いわゆるホワイトハッカーと言われるような人材を育てていく能力が、日本の国家にも必要であろう。その観点から、国家を中心としたそういう設備または施設を持った機関を作り上げていくことが絶対的に必要であり、先ほど申し上げた経済産業省の産業系サイバーセキュリティ推進センターというものに期待を寄せたい。

４番目は、中小企業についてである。人材が非常に日本の国の中には少ない。本当に力のあるアナリストは日本では 200 人ぐらいではないかという話も聞いている。そうすると、200 人を大企業で一人ずつ分けても足りない。ということは、日本にいる人材をいかに共有して、日本の国家のサイバーセキュリティを守っていくかということが非常に重要な案件であろうと思う。

私が中小企業と申し上げたのは、IoT の時代になってくると、サプライチェーンマネジメントが IoT でされることになる。IoT でされるということは、逆に言うと、IoT に入らないとサプライチェーンマネジメントに入れないということになる。そうなると、中小企業のネットワークが安心・安全である、セキュアであるということが確認できない限りは IoT に入れない。IoT に入れないということは、サプライチェーンマネジメントに入れないということと等価になってしまう。そういう観点で、中小企業のネットワークをいかにサイバーの観点からセキュアに保つかということが非常に重要な課題になってくると思う。その観点では、共通な形でペネトレーション試験をする機関による評価、または 24 時間監視をするサービスなどを受けていれば中小企業のネットワーク部分がセキュアである、というアプルーバルみたいなものを本来は国家でお与えいただくのがいいのではないか。是非お考えいただきたい。先ほど、保険に関する発言があったが、ある意味でのア

プルーバルというものが出されたときに、保険がそれについてくるという可能性もあるため、それも含めてお考えいただくとありがたい。

最後２つは技術関係について申し上げる。リオオリンピックでは、2,000 万回のサイバー攻撃があったと聞いている。ロンドンでは２億回と言われているが、実際のセンサーのレベル等を考えると、2,000 万回という数字がロンドンの２億回とどの程度なのかということは、明確な評価はできないと思う。ただ、明確なのは、DDoS 攻撃が非常に多かった。かつ、200Gbps～540Gbps と聞いており、さらには IoT 機器を乗っ取った形でこれらの DDoS 攻撃が行われているという。欧米では非常に当たり前に攻撃がされているが、日本では重要インフラはいまだ大きな攻撃を受けていない。その観点から、オリンピックでは重要インフラに対する DDoS の対応という準備が必要であろう。現在、日本の技術だけでは DDoS に対応することができないが、この４年間に向けて日本の技術の向上のあり方、それからパートナーのあり方が非常に重要であろう。是非この辺を御配慮いただくとありがたい。

最後は AI について申し上げる。DEFCON24 というセキュリティカンファレンスが開催された。その中で、DARPA が主催の、Cyber Grand Challenge という、AI だけを使ったサイバーセキュリティのコンペティションがある。これは３年間で 55 億円の費用がかかっており、優勝賞金が２億円である。これで優勝したところが、いわゆる DEFCON のコンペティションに出て、最下位ではあったものの、非常にいい対応ができたという評価をされているようである。AI というものが、今後、サイバーセキュリティにも非常に重要な領域の技術になっていくため、これらも含めたサイバーセキュリティの対応、技術の蓄積、または育成というものが重要になってくると思う。

○（丸川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））

本年４月に成立したサイバーセキュリティ基本法の一部改正法には、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が盛り込まれており、今月 21 日に施行される。改正法の着実な運用に向けて、政府として全力で取り組んでいく。

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ためには、セキュリティの万全は必須である。そのため、サイバーセキュリティ対策の強化に向け、関係省庁の御協力の下に、電力、通信、交通など、東京大会において重要なサービスを御提供いただく事業者に対して、自らのサイバーリスクの評価に取り組んでいただくよう、要請を始めたところ。

関係省庁にあっては、東京大会におけるサイバーセキュリティの確保のため、引き続き御協力をよろしくお願い申し上げる。

引き続き、重要インフラ防護など、各種重要な課題が多くあるので、サイバーセキュリティ戦略本部の副本部長として、我が国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。

○（松本国家公安委員会委員長）近時、不正アクセスによる個人情報の流出事案等が発生しているほか、標的型メール攻撃の手口の一層の巧妙化やサイバー空間における探索行為等の活発化がうかがわれるなど、サイバー空間の脅威は依然として深刻であり、その対処は

急務である。

2020年東京オリンピック・パラリンピック競技大会の開催等を見据え、引き続き人的、物的基盤を強化するとともに、日本サイバー犯罪対策センターと連携して情報分析等を推進するほか、サイバーセキュリティの確保に向け、産学官の連携により、主要事業者のみならず中小企業者に対する取組を一層拡大するなど、関係省庁と連携して、サイバー空間の脅威に的確に対処するよう、警察庁を指導していく。

○（世耕経済産業大臣）今回の法改正で、国による監視対象が独立行政法人、特殊法人に広がったというのは大きな前進であるが、やはり重要インフラをしっかり守り切るためには、最終的には民間産業界での業界横断的な取組が重要である。

経済産業省では、その拠点として、独立行政法人情報処理推進機構（IPA）に、先ほど遠藤本部員から御指摘いただいた「産業系サイバーセキュリティ推進センター（仮称）」を設立する方向で準備中である。米国などの海外の専門家の知見も活かしながら、我が国の重要インフラ、産業基盤のサイバーセキュリティ対策の根幹を担う人材、技術、ノウハウを生み出す拠点、プラットホームとして育てていきたい。トヨタなど産業界からも前向きに活用したいとの声をいただいている。

ただ、そのときに少し気になるのが、業界別縦割りということで、すなわちそれを所管する省庁縦割りが少し見えているということである。今の時点でも、当省ではIPAに「サイバー情報共有イニシアティブ（J-CSIP）」というもの等を設けており、サイバー攻撃に関する情報を各業界を超えて共有して、早期の防御体制を構築する、あるいは、個別の者で気づかずに攻撃を受けているということがわかった場合はこちらからアラートを鳴らしてあげる、そういう仕組みを既に立ち上げているが、これらの枠組みに参加いただいているのは電力、ガス、石油、化学、自動車など、経済産業省所管の業界だけであり、重要インフラというからには、本来金融や通信、交通、医療、幅広く入ってもらわなくてはいけないのであるが、今のところ入っていただいていないという状況である。各大臣におかれては、是非所管の枠を超えて参加をするように呼びかけていただきたい。その際には、先ほど林本部員から御指摘があった、欧米における法的枠組みづくりというのも参考にしていかなければいけない面もある。

今後は、是非業界や所管官庁を超えて、重要インフラにおけるペネトレーションテストを含む徹底的なリスク評価、そして、攻撃者目線を持ってサイバーセキュリティ対策を立案、実装できる中核人材の育成、サイバーインシデントが発生した場合の省庁、業界横断的な情報の集約、分析能力の強化などについて、「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」の見直しに際して早急にNISCを中心に、突っ込んだ検討を行うべきものと考えている。

IPAに関しても、あれは経済産業省の独立行政法人だという見方ではなくて、政府全体の公共財という観点で、積極的に各省に御活用いただきたい。

○（鶴保情報通信技術（IT）政策担当大臣）近年、スマートフォン、IoTの普及とAIの進展等により、いわゆるビッグデータの収集、活用が容易、かつ重要になってきている。

このビッグデータの有効活用によって、個人のニーズに対応した新サービスの創出や、

我が国産業の生産性向上をもたらし、超少子高齢化社会における諸課題の解決にも貢献できると考えている。

このため、先月、私の主宰でIT本部の下に、「データ流通環境整備検討会」を立ち上げ、新たなデータ流通の仕組みについて議論を開始したところである。

その一方で、データを安全、安心に使えることも重要であり、「官民のデータ流通の推進」と「セキュリティの確保」を車の両輪と考え、努力をしていきたい。

引き続き、サイバーセキュリティ戦略本部と緊密に連携しつつ、政府全体のIT戦略を強力に推進していく。

○（あかま総務副大臣）IoT、人材育成、平成29年度予算の取組について、御紹介させていただく。

まず、IoTセキュリティの取組については、総務省ではIoT推進コンソーシアム及び経済産業省との連名で、本年７月に、「IoTセキュリティガイドライン」を公表した。当ガイドライン及び事務局から報告があった、「安全なIoTシステムのセキュリティに関する一般的枠組」を踏まえ、IoTセキュリティの確保に向けた取組について、着実に進めてまいりたい。

人材育成については、国立研究開発法人情報通信研究機構（NICT）を通じて、官公庁、地方自治体及び重要インフラ事業者等を対象に、実践的なサイバー防御演習（CYDER）を実施している。

今後も、官公庁、地方自治体及び重要インフラ事業者向けに、セキュリティ人材の育成に貢献してまいりたい。

これらの取組に加え、NICTが持つ最先端のサイバーセキュリティの技術や知見を更に活用し、将来のサイバーセキュリティの研究者や起業家の創出に向けて、若手セキュリティエンジニアを育成するべく、NICT内にナショナルサイバートレーニングセンターを構築する事業等を平成29年度概算要求に盛り込ませていただいた。

○（岸外務副大臣）外務省としては、サイバー分野における国際連携に積極的に取り組んできている。特にサイバー空間における法の支配の推進に向けて、G7伊勢志摩サミットにおける合意を踏まえ、近くG7伊勢志摩サイバーグループ（ISCG）第１回会合を開催する。

また、米国とは、昨年の日米新ガイドライン作成を踏まえ、７月にサイバー協議を実施し、協力強化について議論している。さらに、８月には豪州、９月にはドイツとサイバー協議を実施した。本日も、英国との間で二国間協議を実施する。

能力構築支援については、９月の日ASEAN首脳会議を踏まえ、関係府省とともに、政府横断的な「サイバーセキュリティ分野における開発途上国に対する能力構築支援の基本方針」を策定した。今後はこの基本方針の下、政府開発援助をはじめとする様々な政策手段を活用しつつ、オールジャパンで政策的・効率的な支援を行っていく。

７月にサイバー安全保障政策室を外務省内に設置したことも踏まえ、今後とも、関係府省及び同盟国たる米国や友好国と連携しつつ、サイバー分野における外交を推進していく考えである。

○（宮澤防衛大臣政務官）サイバー攻撃は、自衛隊や米軍の任務遂行の大きな阻害要因等となり得る。今後、日米防衛協力を一層推進していく上では、サイバー空間の安定的な利用、効果的な利用を確保することは大変重要であると考えている。

今後は、新ガイドラインに明記されている、迅速かつ適切な情報共有、自衛隊及び米軍が任務遂行上依存する重要インフラの防護といった具体的な協力項目について、日米サイバー防衛協力をより一層加速していく考えである。

また、米国以外については、NATO のサイバー防衛演習への積極的な参加や、ASEAN 諸国に対するサイバー分野での支援を検討するなど、この分野での国際連携を強化していきたいと考えている。

○（橋本厚生労働副大臣）

本日は、厚生労働省と日本年金機構に対する監査の中間報告について、取りまとめいただき感謝申し上げる。

昨年６月１日に公表した日本年金機構における個人情報漏えいの事案では、大変多くの国民の皆様に御心配、御不安、御迷惑をおかけしたこと、おわび申し上げるとともに、その原因究明あるいは再発防止策の検討等を踏まえ、昨年 12 月に策定した業務改善計画に基づいて、組織面・技術面・業務運営面から情報セキュリティ対策に取り組んでいる。

NISC において、御報告のとおり、年金個人情報を取り扱う業務において、インターネットへの接続をできないよう分離策が講じられていること、また、その上で、記録媒体に書き出す場合には、全て暗号化措置が講じられているなどの技術面での対応について監査していただき、年金機構の情報セキュリティについて、しっかり御確認をいただいたと認識している。

今後は、これまで講じてきた対策のみならず、日々刻々と変化する情報セキュリティ環境に対し、不断の見直しを行い、年金機構において情報セキュリティの確保を最優先として業務が行われるよう、厚生労働省としてもしっかり監督を行ってまいりたいと考えており、また、同時に、厚生労働省という業務の都合上、大量の個人情報を保管している業務はほかにもあるため、本省、そのほかの機関においても同様に取り組んでまいりたい。

本日御出席の皆様方におかれては、今後とも、厚生労働省、日本年金機構に対し、御指導のほどよろしくお願い申し上げる。

(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)　本部長締め括り挨拶

本日は、活発な御意見をいただき、感謝申し上げる。

政府としては、本日の議論を踏まえ、改正法により新たに監査対象となる特殊法人等のサイバーセキュリティ対策を強化するとともに、重要インフラ防護に着実に取り組んでいく。

有識者の皆様におかれては、今後とも御協力のほど、よろしくお願い申し上げる。

－　以上　－