サイバーセキュリティ戦略本部
第３回会合　議事概要

１　日時

平成 27 年７月 23 日（木）　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
山口　俊一	情報通信技術（ＩＴ）政策担当大臣
山谷 えり子	国家公安委員会委員長
高市　早苗	総務大臣
宮沢　洋一	経済産業大臣
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
中山　泰秀	外務副大臣
左藤　　章	防衛副大臣
塩崎　恭久	厚生労働大臣
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
加藤　勝信	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

本年５月の日本年金機構に対するサイバー攻撃事案により、国民の皆様の貴重な個人情報が流出してしまったことは、政府として大変重く受けとめなければならない。

各府省庁や関係政府機関においてもサイバー攻撃事案が発生しており、海外でも深刻な攻撃が発生しているといったことを考えると、その対策は極めて急務である。

このため、先日意見募集を行ったサイバーセキュリティ戦略（案）について、日本年金機構の事案等を踏まえて改めて見直し、国民の皆様に安心していただけるよう、我が国のサイバーセキュリティ政策の抜本的な強化を図る必要があると考えている。

皆様においては、活発な御討議をお願いしたい。

(2)　討議

【討議事項】

・　サイバーセキュリティ戦略（案）の見直しについて

【決定事項】

・　サイバーセキュリティ政策に係る年次報告（2014 年度）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）私から３点申し上げる。

１点目として、日本年金機構の情報流出事案は大変残念なことであるが、これを契機に、政府機関などのサイバーセキュリティ対策の抜本的な体制見直しを図ることが最も重要と思っている。しっかり検討したい。

２点目として、セキュリティ対策に当たっては、情報の重要度を踏まえた上で、業務遂行への影響、組織人員のスキル等も考慮して、適切な対策・体制を判断することが重要ではないか。

例えば、今回の事案の場合、ファイルサーバーに原則として個人情報を置いてはいけないというポリシーがあったにもかかわらず、業務遂行上の使い勝手を理由に、そのポリシーが形骸化して守られていなかった点が重要である。したがって、セキュリティ対策の強化としては、情報を一律にネットから分離するのではなく、先に述べたような適切な判断をした上でルールを策定するという柔軟性が重要かと思う。

３点目として、政府機関、独立行政法人、特殊法人、地方公共団体、重要インフラ事業者といったところだけでなく、一般企業も含めて、全体の中で絶対守らなければいけない重要情報はどれかということをしっかり再検討して、対策を構築し直すべきである。

これまでの標的型メール攻撃は、政府機関などの機密情報や、大手企業の先端技術情報が狙われることが多かったが、今回の事案では、基礎年金番号、氏名、生年月日、住所という個人情報が流出した。昨年発生した航空会社におけるマイレージ会員の個人情報流出も標的型攻撃によると言われている。このように、標的型攻撃の使われ方が拡大している中で、民間企業の経営層、IT 担当者の意識改革を進めていくことが非常に重要である。

経産省が経営層を対象としたサイバーセキュリティ経営ガイドラインを年度内に策定すると聞いている。是非とも実効性の高いものにして経営層の意識改革をしていただきたい。

○（林本部員）２点申し上げたい。

１点目として、今回の日本年金機構の情報流出事案に関しては、これにどのように対応していくかということが大事である。この事案を警鐘として捉える気概で、即効性の対策と同時に長期的な対策にも取り組んでほしい。

本日の参考資料に、申合せとしてサイバーセキュリティ対策強化の継続的な取組をうたっていることは、失敗から学ぶという点で、長期的な仕組みとして大変意味があると思う。

２点目は、内閣サイバーセキュリティセンター（NISC）の機能強化について。今回、司令塔としてかなりの機能強化を図ることで、ヒトとカネも要することになる。この問題をどうするかは大変重要なことである。

まず、カネについて。幸い、最近はコンピュータシステムや通信の費用は急速に減少しており、クラウドなどを活用することにより、システム更改時には設備投資と運用費用の両方でかなりの節減が可能ではないかと思う。その分のお金をセキュリティの方に回すことができれば、大胆な予算の見直しと兼ね合って大きな効果があると思われる。

大規模なシステムは、かつては構築に費用が大変かかり、配慮が必要であったが、段々と運用が大事になり、最近は更にセキュリティが大事になっていると思う。そうした機能のどこが大事かを重視することが必要であるが、日本では、古い言葉になったが、ビジネスプロセス・リエンジニアリングというものが案外徹底していないのではないか。

例えば、工場のラインを変える場合は、ジョブを見直して統合するとか、分けるとか、再構築するとか、あるいは廃止してしまうとか、別ルーチンにするとか、そのようなことが当たり前のように行われるが、コンピュータを入れたときのオフィス業務については、そのような理解が進んでいない感じが私はしている。それらも含めて実施すれば、カネについては、片方で大幅な削減を図り、片方でセキュリティを強化することが可能ではないかと思っている。

これに対し、ヒトについては、難しい課題。事務局からは、急速に養成することも難しいので、他の組織との連携を図るという案もあるが、そういうことも含めてこの急場を乗り切るということで対応いただきたいと思っている。

○（前田本部員）今回の日本年金機構の問題は、重大なものであると思う。もし、もう一回こういうことが起これば、国民の信頼を回復できなくなってしまう。一般的に事故への対応は、何か起こったらまた直していけばよいというものと、起こる可能性を排除はできないが絶対に起こらない意気込みで取り組まなければいけないものの二通りがあると思う。今回のような問題は、やはり後者型の意識を持たなければならない。

具体的には、システムの強化により対応していくことになる。「事故」という言葉が使われるが、刑事法学者の立場から言えば、攻撃を行った犯人がいることを忘れてはならない。事故が起こらないようなシステム設計などに目が行きがちであるが、警察に早

く情報を伝えることが重要である。

今後、どのような体制で進めるかについて、官民連携で取り組むことは正しいと思うが、より迅速にできるはずの官官連携をもっと進めるべき。もはや省庁間の壁のようなことを言っている段階ではないと感じる。

人材育成に関しては、これまでも足りないとか、どう育てるかとかいう議論を行ってきたが、もう一歩具体論に踏み込む段階に来ていると思う。人数が少ないなら少ないで、その人材をどこでどのように活用すべきか。必要ならばやはり育成しなければならないが、単に何万人足りないといった抽象的な議論では前へ進まない。どの組織にどのような人材が必要であるかを論ずる必要がある。

具体的に今回、独立行政法人情報処理推進機構（IPA）の活用を検討している点を非常に高く評価したい。人材のレベルは高いので、どのように組織化するかといった課題を検討しつつ、当面、最善の手として打っていくことができると考えている。

最後に一言述べたいのは、平均値を上げることは無意味ということである。今まで我々は、例えば大学では学生の全体の偏差値で捉えがちであり、公務員については情報に対する力を一般的に高めることに目が行きがちである。犯罪の視点で考えると、一番弱いところが狙われ、そこから情報が流出する。弱いところを直すことが必要であり、そのときのリーダーシップはやはりNISCであると思う。

野原本部員が発言されたように、どこまで対策するかを情報の種類によって分けるべきであることは確かであるが、今の段階では少し慎重気味でいたほうがよい。何かまたトラブルが発生した場合、政府でどのような対処ができるかについて、シミュレーションをしておくことが最も大事であると考えている。

○（村井本部員）情報システムの面からは、今回の日本年金機構の事案は、情報システムに対する国民のトラストの問題であると思う。今後、このような情報システムを安心して活用できる体制をつくりだすことが一番重要である。

情報システムがほかのシステムと違うのは、必ず新しくなっていくということ。新しい技術を取り入れながら進化していくため、常時定期的な点検等が必要である。特に今の情報システムは、相当以前から使われているもので、変えることができないものも交ぜて使われるということがある。

私がずっと申し上げていたのは、年に１回、期間を定めて洗い出しの作業を行って棚卸しをし、当該期間に政府は何を行い、どのような手を打って、何を発見し、何を改善したかなどを国民に対して公表すべきではないかということ。情報セキュリティの分野では、このような棚卸しのアクションが、信頼を得るために最も効果的な方法であるということがわかっている。

IT 総合戦略本部でもそのような議論をしてきた。本日配布の参考資料「継続的なセキュリティ対策強化の考え方について」２ページの図を見ると、一番右に「自己点検（毎年２月）」と書いてある。２月はサイバーセキュリティ月間。この月に日本中の公的なシステムは全部棚卸しをして、それぞれの組織が使っているシステムがどのくらい古いか、業務用システムとメールシステムとが分離されているかなどを確認する。悪いところを見つけた場合は、この期間だけは褒めるぐらいの方法が有効だ。ただ、これは現時

点での課題の例であり、来年にはまた違う課題が出てくるであろう。これらを思い切って実施・報告し、PDCA のサイクルを回してレポートすることが重要である。

図の「事案への対処」にある「緊急策」は、日本年金機構の事案に対して現在行っているようなことである。その後の「報告」、「確認」で、「緊急策」からの知恵が生かされることは非常に重要であり、今から準備して、２月に１か月間点検をするというのは時期的にもよいと思う。その結果を国民に公表することが、トラストを生んでいく一つの重要な道ではないか。

もう１件、CSIRT（Computer Security Incident Response Team）について。CSIRT は一般的な総称で、JPCERT/CC もその一つである。CSIRT 政策は、まず、政府内各組織に CSIRT を作るということから始める。そして、そのそれぞれの組織の CSIRT が連携し、NISC 等を中心としたまとまった報告体制づくりという政府全体の連携体制を含めたものでなくてはならない。

これは世界的な貢献活動でもある。世界では FIRST という組織があり、CSIRT の国際連携ができているので、国際的に日本がきちんと貢献していくというメッセージにもなる。CSIRT の強化は、今や世界中の動きである。どの国でも、各組織が内部にきちんとチームをつくり自分の責任で自律的に対処し、更にそれが連携する、この２段構えが非常に重要であると思う。

本日は、遠藤大臣が御出席であるが、2020 年は社会全体へのオリパラインパクトが問われるときである。今、世界で最も関心が高いのは、このときどのようなサイバーセキュリティの体制ができるかということ。このためには、各組織内の CSIRT が連携することが、オリンピックというインパクトに一番大きなコミットメントをするという具体策になると思う。

○（遠藤本部員）各本部員が発言されたように、今回の日本年金機構の事案は大変残念なことであるが、これを教訓として、体制をしっかり整えることが重要である。

まずは、各外部団体を含め、重要な防御組織の見直しが必要と思う。何が重要でどこがどのような重要情報を持っているのか、それに対する対応が本当にできているのかといった確認がまず必要であろう。

我々が一つ認識しなくてはならないのは、現在受けているいろいろな攻撃が、漢字系、いわゆる２バイト系と言われる日本専用の攻撃であるということ。当社が提供するネットワーク監視サービスで見ていても、非常に日本専用の攻撃が多くなってきている。

このようなネットワーク監視の対応をしていくときに最も重要な点は、新しい情報をリアルタイムで集めることである。米国の会社と提携して海外の情報を集めてもいるが、増えてきている日本専用の攻撃の情報は、残念ながら日本でしか集めることができない。そのような状況変化を我々はもっと強く意識して、日本の国の中で産官学が本当に情報を共有できる仕組み、それもリアルタイムで共有できる仕組みを強化していく必要があろうと考える。

そのような観点から、先ほどの村井本部員の御発言にあったような CSIRT に対する意識も高まってきており、各企業の経営者が自ら CSIRT をつくり込もうと、当社にもコンサルの依頼が来ている。これは非常に良いことであると思う。

我々は、多層の防御や縦方向に深く防御する縦深防御の両方の観点を重視しているが、自ら防御体制を組むことができる企業とそうでない企業があることの認識が重要である。これから我々もIoTという世界に入り、企業同士がパートナーシップを結びながら新たな価値を出していくことになるが、その中で、本当に安心できるネットワークをお互いに持っていると企業間で理解することが、今後日本の価値をつくり上げていく上で非常に重要であると思う。一方、対応する力が足りない企業においても、しっかりしたサポートを受けることができ、受けていればネットワークが大丈夫であるという承認が得られる仕組みが、日本全体の企業力という観点で絶対的に必要であろう。自ら防御システムを持っていること、または外部の力を借りてネットワークが防御できていることを確認する、この二つのタイプの防御体制に対する政府機関等の承認が今後必要ではないか。

また、IoTは、今後価値を生む本当に重要な領域になっていくが、そのとき最も重要なことは、T（Things）から出てくるデータが成り済まされていないことである。これまでの攻撃は、データの窃取などが目的であったが、IoTの世界になると、データ自体が何かに成り済まし、違うデータとして相手に伝わるという攻め方も必ず出てくる。データ自体がどのように守られた形で相手に届くかについて、データ自体の暗号化を含めた方法論を考え、この評価をもう一つ考える必要がある。ネットワーク側の防御とともにデータ自体の防御のありようも、我々がもっと注力すべきところである。

最後が、人材育成について。本日まさに遠藤大臣が御出席であるが、オリンピックに向かって我々が攻撃を受ける可能性が非常に高くなってくる。その観点で、人材育成が大変重要なタイミングに入ってきた。今までのレベルの人材育成の数では、絶対的に足りない。この３年ぐらいで急速に数を積み重ねていくためにはどうしたらよいか考える必要があろう。先日、NTTが「産業横断サイバーセキュリティー人材育成検討会」というものを立ち上げ、当社も参加しているが、官と民が一緒になってどのようなターゲットを持ち育成をすべきかを検討する必要が本当にあろう。また、総務省などが強いリーダーシップを取って行っているサイバーに対する教育についても、更なる強化が必要であろうと思う。

○（小野寺本部員）今回の日本年金機構の事案を見ても最後は人である。今回、インシデントの検出・通知までは行われており、その後の連絡や対処の体制に問題があった。恥ずかしい話であるが、当社も2006年に窃盗による情報流出事案があった。以降、当社は、情報セキュリティ、特に個人情報を守ることに取り組んでおり、社長をトップとした情報セキュリティの社内会議を月１回開催している。

世の中で今回の事案のようなことが起きたとき、当社では全社員にｅラーニングを実施している。未受講の社員については上司に自動的に通知が行き、全員受けさせる仕組みをつくっている。ｅラーニングは、簡単なシステムであまり負荷なく受講できる。国の全職員や関係者のレベルアップを図り、事が起きた場合にとるべき行動や、わからない場合には上司に報告するといったことをしっかり意識付けしないと、この問題は最後まで続くのではないかと思っている。

遠藤本部員が発言されたように高度な技術ももちろん必要である。インシデント情報を通知するような際にはこのような技術がベースになっている。一方、そのインシデン

ト情報の受け手側にある問題が非常に大きいことも是非考えてほしい。

先ほどの遠藤本部員の御発言にもあったように、人材育成の問題は非常に大きい。もちろん情報セキュリティに関する人材育成が急務であることも事実であると思う。ただ、以前から申し上げていることであるが、日本全体でソフトウェアやプログラミングに対する教育がほとんど行われていないことを私は懸念している。当社の研究所に入ってきた社員が、大学や大学院でどのようなソフトウェアやプログラミング教育を受けたかを５年前と今年にそれぞれ調査した。多少改善されてはいるが、残念ながら根本的なところは改善されていない。

御存じのように、イスラエルでは、2000 年から高等学校課程でプログラミング教育を必修化している。それが、情報セキュリティ、IoT といった、ICT 関係の新しい技術が、今どんどんイスラエルで芽生えてきている大きな理由であろうと私は思っている。それを見習ってエストニアやニュージーランドなども始め、英国も御存じのように５歳から16 歳の義務教育全学年でソフトウェアやプログラミング教育が義務化されている。

産業面から見ても、情報セキュリティや個人情報の問題を見ても、今こそ、もっとしっかりソフトウェア教育、プログラミング教育をすべきと思う。IT 総合戦略本部で、既に義務化を図る案が出ているようであるが、残念ながらまだ実行には至っていない。最後は人であるということをもう一回考え直さないと、抜本的なところはなかなか直っていかないのではないか。

やはり個人情報を守ることが重要と考えている。センターシステムが多重防御で守られていても、端末側に情報の一部が置かれるようなことが重大な問題。当社の場合、コールセンターの端末には一切情報が残らない仕組みをつくっている。今回の日本年金機構の事案などを考えると、個人情報をサイバー攻撃からどのように守っていくかをもう一度全体で考え直す時期であると思うので、是非御検討いただきたい。

○（中谷本部員）私からは、大きく分けて次の２点を申し上げたい。

第１に、今回の年金機構の個人情報流出は残念な事態であり、サイバーセキュリティ戦略案を迅速に見直し、対策を強化することに全面的に賛成である。

最も重要な情報はネットワークから切り離してリスク分散をすること。完璧な対応は無理であるので、攻撃を受けた際の被害を極小化できるように多重防御の対応をすること。サイバー攻撃演習の回数の増加などが特に重要であると考えている。

総務省がオリンピックを想定したサイバー攻撃の模擬演習を行う方針との報道に接したが、これは非常に有意義であると思う。

サイバー人材を急速に増加できない以上、いわゆる予備役に該当する即応予備チームを作成して登録しておいてもらい、いざというときには活動してもらうこともまた重要である。

また、今回のことではなく、将来においてであるが、サイバーセキュリティ対応に明らかに過失のある組織に対してはドラスティックではあるが、何らかのペナルティーを課すことも検討せざるを得ないかとも思われる。

第２に、米国では2,100 万人の政府職員の個人情報がサイバー攻撃により流出し、人事管理局長の辞任に至った。日本においてもいつ同様の事態が起きるかわからない。サ

イバーセキュリティの強化は不可欠であるが、同時にサイバー外交を積極的に展開し、特に米国との同盟関係をサイバーの分野でも一層強化するとともに、幾つかの国との間で信頼醸成措置を確立することもまた重要であると考える。米国は2013年７月にロシアとの間でコンピュータ緊急対応チーム間のリンク、核リスク削減センターを通じて通報の交換、ホワイトハウスとクレムリンの直接対話ラインの創設を内容とするICT分野での信頼醸成措置について合意している。この合意を一つの参考にして、適切な信頼醸成措置について検討していくことが望まれる。

信頼醸成措置が合意されたからといって、サイバー攻撃が大きく減少する保障はないものの、合意がなされればより迅速な対応が期待できるとともに、相手国に対して一定の透明性と説明責任を求めることができるようになるという利点があると思う。

他方で、ある国家が関与した我が国へのサイバー攻撃が明らかとなった場合には、対抗措置の中心をなすであろう経済制裁措置を適切かつ迅速に発動できるよう、外為法を初めとする国内法令をいま一度、整理、確認しておく必要があるかと思う。

○（山口情報通信技術（ＩＴ）政策担当大臣（副本部長））いろいろと参考になる御意見をいただき、感謝申し上げる。

御発言の一部にも出たが、IT総合戦略本部では、先月６月30日に「世界最先端IT国家創造宣言」を決定した。今回の創造宣言には、ビッグデータの利活用等、IT利活用の裾野拡大を推進するための基盤強化とともに、政府機関等の対応能力の抜本的強化を含むサイバーセキュリティ関連施策も盛り込んでいる。

特に、マイナンバー制度の推進のためには、個人情報保護の徹底が必要であるが、マイナンバー制度のセキュリティ確保はまさに表裏一体に関係にあるわけで、極めて重要な課題であると認識をしている。

今回の年金情報流出事案を踏まえ、国会でも議論をしてきた。このサイバーセキュリティ対策の強化のために、サイバーセキュリティ基本法のあり方を含めてしっかり検討して、出していくことが必要であろうと思っている。

○（山谷国家公安委員会委員長）

日本年金機構に対するサイバー攻撃事案については、現在、警視庁において所要の捜査を推進しているところである。また、そうしたサイバー攻撃事案による被害の未然防止・拡大防止のため、警察庁及び都道府県警察において、関係機関や民間企業等と連携し、サイバー攻撃事案を想定した共同対処訓練や情報の収集・分析に基づく注意喚起等の実施に努めていく。

さらに、国民や民間企業等のIT利活用における安全・安心の確保は、我が国の成長戦略を確固たるものとするための前提であり、それを脅かすサイバー犯罪に対する対策を強化していく。

本日の討議を踏まえ、警察がその役割を十分に果たしていくことができるよう、引き続き取り組んでいく。

○（高市総務大臣）

まず、日本年金機構における情報流出事案に対して、総務省ではその報告を受けた直後に、早急に住基ネット全体の安全確認を行った。総務省では金曜日の夕方にNISCから連絡を受けたので、金曜日の夕方、土曜日、日曜日とかけながら、翌週も含めて２巡、安全性を確認した。

本年 10 月からのマイナンバー制度の導入に向け、先月、全国の自治体に対してインターネットのリスクから住民情報を分離する取組の着手を早急にということでお願いをした。それだけでは足りないので、専門家による「自治体情報セキュリティ対策検討チーム」を立ち上げ、抜本的な対策の検討を開始したところである。先ほどの小野寺本部員の御意見も十分に参考にさせていただきたいと思う。

「テレコムISAC」の発展形として、新たに「ICT-ISAC」（仮称）の整備を進めるつもりである。これはICT分野全体にわたる情報共有体制の構築を図るということであるが、日本では通信と金融、２分野のISACということであるが、米国では電力、水、輸送など、19分野のISACを整備しているので、より幅広くということを考えている。

また、東京オリンピックも見据えた大規模サイバー演習の実施を通じ、実践的セキュリティ人材の育成を進めていく。

総務省としては、以上のような取り組みを通じ、マイナンバーに関するセキュリティの確保を初めとして、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する。

先ほど遠藤本部員よりIoTのT（Things）の方のデータをきちんと守るというお話があって大変参考になった。T（Things）と言ってもいろいろあるが、先般、総務省で私が指示したことで、例えば人型ロボットが集めたいろいろな情報というものはどのように保護されるのかという点も含めて、今、研究中である。

○（宮沢経済産業大臣）経済産業省所管のIPAでは、セキュリティ政策の実施機関として、サイバー攻撃に関する情報収集・分析や対策方法の提案・普及に取り組んできている。

このため、本戦略に盛り込まれているNISCによる監視・調査などの対策強化に当たり、IPA の知見などを活かして貢献すべく、連携体制を整備するための方策について、速やかに検討していく。

また、中小企業を含めた民間分野におけるサイバーセキュリティ確保について、３点申し上げる。

１点目、「サイバーセキュリティ経営ガイドライン」を年内早期に策定し、経営層のリーダーシップによる対策強化を促していく。

２点目、このガイドラインを踏まえた企業の取り組みが、第三者認証などにより客観的に評価される仕組みを来年度から実施する。

さらに３点目、「セキュリティマネジメント試験」を来年春に導入し、企業におけるセキュリティ対策従事者の実践力の向上に貢献していく。

○（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）このたび、サイバーセキュリティ戦略本部に加えていただいた、東京オリンピック・パラリンピック大臣の遠藤です。どうぞよろしくお願いいたします。

ロンドンオリンピックの際のサイバー攻撃の状況を見ても、また、先ほど来、本部員

の皆さんから話があったように、2020年東京大会の成功にはサイバーセキュリティの確保が必要不可欠である。そのためには、大会に係るサイバーセキュリティ上のリスクの明確化、大会運営及びこれに関係する諸機関等へのサイバー攻撃を予防、検知し、対処するための情報共有を担う中核的組織の整備。特に人材の育成・確保。事前の十分な訓練等を進めていくことが重要であるので、これらの施策の着実な実施について、関係者の皆様の御協力をお願いしたい。

これからも有識者の皆様の知見をお借りし、関係省庁等と緊密な連絡を図りながら、2020年東京大会の準備を着実に推進していく。

○（中山外務副大臣）岸田外務大臣に成りかわり、外務省の意見を申し述べる。

我が国においても、広範囲にわたるサイバー攻撃事案が継続して発生している。外務省としても、G7の伊勢志摩サミットに向けたサイバーセキュリティ対策をしっかりと進めていく。また、サイバー分野に関する情報収集・分析機能の強化、能力構築支援等を引き続き実施していきたいと思う。

さらには、国際的なルール作りの観点から、先ほど御指摘もあったサイバー外交を含め、我が国はP5（常任理事国）を含む20か国の政府専門家による国連の会合に参加し、サイバー空間に関する国際法の適用や、国家の責任ある行動の分野において、議論を積極的に主導している。

米国との関係においては、7月21日及び22日に第３回日米サイバー対話を実施した。日米間の情報共有、重要インフラ防護や国際場裡における日米連携等についても議論をしている。今般の対話を踏まえ、今後も様々な機会に米国との連携を深めていく考えである。

最後に、途上国との協力については、７月上旬にサイバーセキュリティに関する能力構築支援について、調査団をベトナムへ派遣している。対処能力を向上させ、日本を含む世界全体のサイバーセキュリティのリスク低減を図っていくために、引き続き途上国のニーズ等を踏まえ協力していきたい。

今後とも御指導よろしくお願い申し上げる。

○（左藤防衛副大臣）中谷防衛大臣に代わり、副大臣の左藤が発言をさせていただく。

日本年金機構における情報流出事案、日本経済を継続的に成長させるための成長戦略及び国民からいただいた意見を受けた見直しや、本日有識者本部員の先生からお話をいただいた論議は、サイバーセキュリティ戦略をより時宜にかなったものへ修正する上で有意義なものと考えている。今後決定される本戦略を踏まえ、防衛省・自衛隊はサイバーセキュリティの確保に一層気を引き締めて取り組んでいく。

また「サイバーセキュリティ政策に係る年次報告」については、当該報告にある施策評価を踏まえ、今後ともサイバーセキュリティ関連施策に関して、不断に見直しを行っていきたい。特に村井本部員から御指摘があった棚卸しやCSIRTの問題を含め、防衛省もしっかり対応できるように頑張っていく。

○（塩崎厚生労働大臣）日本年金機構の事案に関し、数々の御指摘をいただき、誠にあり

がとうございます。
日本年金機構を監督する厚生労働大臣として、まずおわびを申し上げたい。また、何よりも原因究明と再発防止が重要であると考えている。御指摘をいただいた点について、正面から受けとめて、しっかりとその実現に向けて全力投球をしてまいりたい。
今回の事案では、NISC との連絡調整が極めて不十分であった、日本年金機構、厚生労働省ともに、高度な標的型攻撃を念頭に置いた対応が甚だ不十分であった。あるいは責任者への報告がそれぞれの組織の中で極めて遅くなっているなど、反省すべき点が多々あったと思っている。
このため、６月１日の本事案公表後は、まずは緊急対応として、NISC から来る注意喚起とその後の対処結果についは、全て大臣に報告するように指示をしたことに加え、上司への報告や専門機関との連携など、情報セキュリティ事案の発生時の連絡体制など、既に現行の手順書にあるべき運用について、少なくとも省内では徹底するということを指示したところである。
高度な標的型攻撃に対応できるように、指揮命令系統の明確化など、組織体制を強化し、専門的かつ迅速な判断が可能なセキュリティ体制の抜本的な見直しをする。あるいはシステムを強化して、高度な標的型攻撃を想定した内部対策あるいは出口対策の強化を行う。
職員の意識、リテラシーの向上のための対策として、幹部も含めた情報セキュリティ教育の一層の充実などを行う。
そして、ルールの見直しとして、インシデント対処手順書の見直しなどの検討を進めているところである。
さらに、外部の有識者からなる「日本年金機構における不正アクセスによる情報流出事案検証委員会」の検証報告も踏まえ、今後機構のセキュリティ体制強化、そして厚生労働省の監督強化に抜本的に取り組んでいきたいと考えている。

⑶　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。
また、サイバーセキュリティ戦略（案）は、本日の討議の結果を踏まえ、次回会合において再度討議を行った上で閣議決定案を決定することとした。

⑷　本部長締め括り挨拶
本日は、活発な御意見に感謝申し上げる。
本日の討議も踏まえ、次回会合において、現在取りまとめ中のサイバーセキュリティ戦略（案）を決定したいと考えている。
具体的にはNISCの機能強化、さらには政府機関の防御能力や人材育成なども戦略に盛り込んでいきたい。引き続きよろしくお願いする。

－　以上　－