サイバーセキュリティ戦略本部
第４回会合　議事概要

１　日時

平成 27 年８月 20 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
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
西銘 恒三郎	総務副大臣
左藤　　章	防衛副大臣
薗浦 健太郎	外務大臣政務官
塩崎　恭久	厚生労働大臣
金高　雅仁	警察庁長官
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
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

お忙しい中、早朝から御参集いただき、感謝申し上げる。

近年、サイバー攻撃がますます進化する中、日本年金機構に対する悪質極まりない攻撃によって国民の皆様の貴重な個人情報が流出するという事案があった。政府として、我が国の戦略を抜本的に強化しなければならない。

本戦略本部としては、今回の事案究明調査を行うとともに、調査によって得られた教訓を踏まえながら、さきに意見募集を行ったサイバーセキュリティ戦略（案）の見直しを行うことが喫緊の課題である。

本日の会合では、この調査結果を報告するとともに、前回に引き続いて戦略（案）を御議論いただき、2020 年東京オリンピック・パラリンピック競技大会の開催も見据えて、我が国の未来に向けたサイバーセキュリティ戦略をしっかり取りまとめたいと考えている。

皆様には、本日も活発な御議論をよろしくお願いしたい。

(2)　討議

【決定事項】

・　日本年金機構における個人情報流出事案に関する原因究明調査結果（案）について
・　サイバーセキュリティ戦略（案）について
・　サイバーセキュリティ 2015（案）について
・　サイバーセキュリティ関係施策に関する平成 28 年度予算重点化方針（案）について

【報告事項】

・　JPCERT/CC とのパートナーシップによるサイバー攻撃等への対応について

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）迅速にまとめていただいた個人情報流出事案への対策は支持したい。加えて、補足説明１点と、実務的な観点から１点、合計２点お話しする。

まず、今回の事案だけでなく民間企業でも情報流出事故が後を絶たないが、事故の防止策としての情報管理の手順や認証制度も同時に見直すことが必要ではないか。

事故の防止策としては、情報保護の手続や過程が適切であるかどうかについて、第三者認証を受ける、監査を受ける、保険に入るなど、いろいろな仕組みがあると思う。特に我が国では、Information Security Management System（ISMS）という認証制度を高く評価しており、取得している企業が世界的に見てもかなり多い。それ自体は大変価値があるが、ISMS などのマネジメントシステムが求める、経営者のコミットメントが正しく反映されているかについては疑問である。経営者が自分自身の問題として理解していたかどうかは少し疑わしく、いわば社長用のセキュリティと現場用のセキュリティが結びついていなかったのではないかと思われる。そこには２つの側面があるかと思う。

まず、米国では、マネジャーとワーカーが分かれているため、マネジャーは、マネジメントシステムを自分宛の文書として読まなければならない。これに対し、我が国では、取締役も執行役も部長も含めて内部昇進が中心であり、マネジメントの一部が中間管理層（ミドル）に委任されているのが普通かと思う。世の中の度重なる事故の影響で、トップに、自らの問題として対処しなければならないという意識が育っているのは望ましいことであるが、ミドルの役割をその分減じてしまうのは、逆説的ながらもったいない。なぜならば、我が国の経営管理上の比較優位はミドルの優秀さにあると思うからである。トップの責任を従来よりも重視するとともに、ミドルの補佐責任も期待するというハイブリッドが望ましいのではないか。

他方で、手続を重視する余りに経営の本質を忘れることがないようにすることも必要である。環境が激変する中で事業を営む以上、種々のリスクは不可避であり、情報リスクも例外ではない、ミドルにマネジメントシステム運用を任せると、事故を起こさない、手続を守るといった安全サイドに傾きがちになる。それをトップが調整してこそ、リスクをとることが可能になるので、この両機能のバランスがとれるということが大事ではないかと思う。

２点目として実務的な提案をしたい。サイバーセキュリティの人材育成が急務であることは度々指摘されているが、この分野は、自転車に乗ることや水泳やスキーを覚えることと同様、座学だけでなく実習・演習が不可欠である。必要となる演習場、すなわちサイバーレンジは、サイバーの特質からして物理的な場所というより、演習を支援するコンピュータシステム、特にソフトウェアの集合ではないか。更に重要なのは、攻撃手口の進化に即応できる教材や教え方の開発である。

各演習実施機関がこれらのハードウェアやソフトウェアを個々に維持管理するのは不経済であり、既に実績がある独立行政法人などが中心的役割を果たし、演習実施機関が必要に応じて利用できるような道を開いていただきたい。このような仕組みがあれば、全国の大学・大学院等で演習することが容易になり、人材育成の迅速化に役立つものと考える。

○（前田本部員）１か月前の前回会合での発言と重なる部分もあるが、ある意味で重要な点なので重ねて強調しておきたい。

今回の事案の対応として、この短期間にこれだけの調査結果は非常に優れたものであり、高く評価したい。今回の件による見直しとして、官民連携というよりも、官の中でCSIRT体制の強化、独立行政法人情報処理推進機構（IPA）との連携といったものが一歩進むということが挙げられる。

その中で余り強調されなかったが、国民の目から見てある程度の対応がしっかりできたという点では、事案対処官庁が原因究明に関して果たした役割は大きい。ただ、余りその点を強調し過ぎると、今度は逆に、まだ本当の犯人究明ができないのかということになってしまう。国民の目からの安心という意味では、ちゃんと究明してもらえて、さらに踏み込んでもらえるという方向で動いているということが何より重要である。その意味で、内閣サイバーセキュリティセンター（NISC）と事案対処官庁が、タイムラグなくシームレスにと言われるような連携を更に進めていくことが必要ではないか。

もう一つ、マイナンバー制度などのことも視野に入れて考えると、これも前回申し上げたとおり、攻撃者は全体の大きな部分を狙うのではなく、一番弱いところのみを狙う。その観点で、国と地方公共団体との関係をどうするか考える必要がある。地方分権はあるが、国家の存立に関わる情報の保護の観点からすると、単に通達等を出すようなルールによる対応だけでなく、従来の国と地方公共団体の関係とは違って、かゆいところに手が届くように神経がつながらなければならないという感じがする。

今回示されている対策については賛成であるが、これを更に具体化し、実行する中で、国からの情報をより強く浸透させるという道が必要である。法律の解釈論も考えなければならないが、やはりそこを視野に入れないと大きな課題が残る可能性がある。

セキュリティ確保のための財政上の措置について、従来以上に一歩踏み込んだ対応をしていることは非常に高く評価できる。政府機関対策の強化の重点化は、非常に時宜を得た適切な対応である。

なお、先ほどの話に戻るが、この機会に一歩前に出て、連携にIPA等の力を利用することは、非常に重要なポイントであると考えている。

○（村井本部員）今回の日本年金機構の事案をきっかけとして、ある意味、日本政府全体がトラストを内外にきちんとつくり、示さなければならない状況にあると思う。この事案そのものに対応をすることは当然であるが、それにより、具体的に何がこれまでと変わって、これからどうするかというメッセージを、大臣の方々は、機会があるごとに是非発信していただきたいと思う。私もこの事案の後、各国に行った際に状況をいろいろと説明しており、しかるべく対処していることを評価してもらっている。つまり、すぐに事案を分析して、政府全体の新しい対応を決め、継続して進める体制をつくったということが、トラストを生むのである。

前回会合の資料にもあった資料２－１の４ページの図において、この事案への対処を行ったというのが上の赤い箇所である。これができたので、全体をPDCAで回すという緑の箇所、またそのために総点検を毎年２月に実施することを我々は決めた。したがって、全体的な対策を行った、つまり、何かが起こった際に、その事案自体にきちんと対処し、それに基づいてPDCAによる自己点検の仕組みを新たにつくったということで、大変大きな信頼のメッセージになると思う。

対処の具体的内容が同資料の次ページに記載されている。各府省庁、独立行政法人等ですぐに対応したということが具体的に書かれており、これが、先ほど申し上げたこの国はきちんと対処し、新たな対応を講じて継続して進めるということのメッセージになるので、非常に重要なことであると思う。

もう一点、同資料の２ページの一番上にCSIRT体制の強化ということが記載してある。前回会合でも説明したとおり、CSIRTとはセキュリティインシデントのレスポンスチームである。何かが起こったら対応する。つまり、これは事後対応のメカニズムである。この事後対応というのは、セキュリティの上では非常に重要である。必ず何か起こるのであることから、この体制を大小にかかわらず政府における全ての組織に設置するというのが具体的な組織論の対応である。

そして、設置したCSIRTがきちんと連携していることが重要である。今回はそこに問

題があったことがわかっている。中央省庁だけでなく、先ほど申し上げた小さな組織、前田本部員も述べられていたような地方公共団体、そういったところまで広げること、また、各企業もCSIRTをきちんと持っており、それらがつながることが重要であると思う。

そのことが、ネットワークができて全体を統合するということである。資料５でJPCERT/CCという組織の説明があったが、JPCERT/CCは、サイバーセキュリティの民間のコミュニティーが連結できるCSIRTの一部であり、これまでもここで連携は行われていた。ただ、今行おうとしている重要なことは、あらゆる組織のCSIRT体制をつなぎ、一般名詞としてのCSIRTではなく、JPCERT/CCなどとも連携した風通しの良い、何かが起こったらすぐ反応できるレスポンスチームという体制を作ることである。何度も言うように、ダイナミックにレスポンスできる。つまり、どんどん発展する技術に対応できる体制である。

以上２点、すぐに対処して体制ができたという話と、CSIRTをきちんと展開するという話、この２つのメッセージが出ていれば、いろいろなところでの信頼が高まり、ここまでできれば、我が国が世界の中で最先端のサイバーセキュリティ大国と言えるところに近づけるのではないかと思っている。

○（遠藤本部員）サイバーセキュリティ戦略、サイバーセキュリティ2015は、日本年金機構の事案も踏まえて内容が充実したと理解している。また、非常に短い期間で充実させたことに感謝申し上げる。

２年ほど前と比べると、かなり具体的な内容が含まれており、実行の観点からも充実したものになっていると思う。我々は、これを実際にスピーディーに実行することが必要である。そのため、これらをベースに具体的な施策をつくり上げていく必要があろう。その中で、予算の問題、人材育成の根本的な改革の問題が、最も重要であり、考えていかなくてはならない。

2020年に開催されるオリンピック・パラリンピック競技大会に対し、人材育成のため、この５年間で相当数の教育を行っていかなくてはいけない。中学、高校のレベルから、サイバーセキュリティ、またはIoTに対する教育を充実させることが必要であり、即刻実施しなければならないと思う。

さらには、これら技術またはサイバーセキュリティのサービスは、個々の企業または公共団体でレベル感が一致していなければならない。そのため、技術的な標準化や人材に対し、ある意味でのレベル感の同意が必要であり、早急に用意が行われる必要があろうと思う。

また、先ほど村井本部員から、全ての企業がCSIRTを持つべきという御指摘があった。大企業は自組織内でCSIRTを形成できるが、中小企業ではなかなか難しい。民間または公的機関が、中小企業をサポートし、同等レベルのセキュリティを守ることができる仕組みがなければ、日本の国全体の経済界でのサイバーセキュリティが守られたという形にならない。その仕組みを早急に用意する必要があろう。

挙げられている経営トップの意識改革は、非常に重要なことと思う。これを全体に広げるには、経済団体を介して啓発を行っていくこともまた重要と理解している。

２点目として、サイバー空間というものは、価値を生む空間という定義をするべきであり、そのためセキュリティが高いものにしなくてはならないということであろうと思う。資源が少ない日本では、このサイバー空間を最大限活かして我々の技術価値を上げ、国家での企業の価値というものを上げていく努力が必要と考えている。その観点から、日本の各企業がサイバー空間に対しての意識を高く持ち、サイバー空間に対する各企業及びネットワークのセキュリティを高くしなければならないと思う。個々の企業、さらには地方公共団体や国全体がサイバー空間の安全性を守り、その中でさらに高い価値のものを出して日本の価値を上げていくという努力が必要であり、そのような意識の下にサイバーセキュリティを考えるべきである。

また、Industrial4.0 も含め IoT の世界では、各企業のネットワークが他の企業のネットワークとつながり合いながら価値を出していくという形になり、海外とも企業のネットワークがつながる可能性がある。これも村井本部員が発言されていたが、サイバーセキュリティで、日本が海外に対してどのようにリーダーシップをとっていくのか。特にアジアでは、サイバーセキュリティにおける日本へのリーダーシップの期待は非常に高いものがあり、積極的な動きをすべきと思う。

ここ２、３か月の間でも、英国首相がシンガポールを訪問してサイバーセキュリティの協力を提案し、マレーシアに対しては中国が協定を結んでいる。日本が企業価値を上げる上でも、国としてサイバーセキュリティに関するリーダーシップをとっていくことは、非常に重要と考える。

○（小野寺本部員）今回、日本年金機構の事案について大変スピードよく対策等を練ったことは非常に重要であったと思う。

前回会合で発言したこととも関連するが、やはり人材の問題が非常に大きい。今回の事案に関する報告を見ても、NISC ではきちんと検出をしており、その後の対応に問題があったのであろう。

先日、IPA と話す機会があった。IPA は、最も基礎的なレベルの試験として「i パス」と呼ばれる IT パスポート試験を普及させようとしており、我々民間も採用して協力している。i パスを使う理由の一つは企業内の IT の最低限のレベルを上げようということであるが、入社試験のときの i パス受験の有無を申告させることで、英語教育のように大学側が対応せざるを得なくなってくるであろうということを期待している。これは、結構な企業が始めているが、IPA に聞くと国や地方自治体で i パスを使っているところがないとのことである。IPA がこのような試験で底上げをしようとしているのに、民間しか使っていないのは逆のような気がする。まず国や地方自治体がこれを使って、自分のところのレベルを是非確認してほしい。

同じく IPA が、次のレベルとして、職場の情報セキュリティ担当者のためのスキルアップガイドというものを現在つくっている。それと同時に、セキュリティ担当者のための試験をつくろうとしている。これも非常に良いと思っている。マイナンバー制度の導入等で個人情報の問題も発生してくるので、やはり地方自治体を含めてある一定レベルの情報に接する人たちには、必ずそういうスキルを身につけるようにしてもらいたい。

２点目として、既に皆さんが発言されているように PDCA サイクルをしっかり回してい

かなければならないのは正しくそのとおりであるが、監査の手法等について今まで余り議論されていない。今回からNISCが監査もできるようになっており、恐らくきちんと勉強した手法等に基づいて監査すると思っているが、監査手法を統一していかないと、監査のレベルがばらばらになりかねない。民間でも御存じのとおりセキュリティについてかなり厳しく言われており、セキュリティ監査も手掛けている監査法人がかなりあるが、レベルが必ずしも統一されているわけではない。監査のレベルを統一し、必要に応じて改定されていることによってPDCAのCの部分ができるのではないかと思うので、その点をお考えいただきたい。

○（中谷本部員）私からは３点申し上げたい。

第１に、サイバーセキュリティ対策の抜本的強化のための対策として、NISCの業務対象を拡大し、監視、監査、原因究明調査業務の対象を、中央省庁のみならず、独立行政法人及び政府機関と一体となって公的業務を行う特殊法人にも拡大し、三つの対象を拡大する方向でそろえていくことが、司令塔であるNISCによる実効的なサイバーセキュリティ対策にとって必要かつ望ましいことであると考える。なお、具体的な範囲は今後確定していく必要があるとは思う。

今後重要なことは、サイバーセキュリティ政策をいかにきちんと実施していくかであり、そのためにはとりわけ各省庁の連携が大事である。また、マイナンバー制度の円滑な導入のためには、地方公共団体による遺漏なき対応が不可欠であると考える。

また、サイバーセキュリティ2015の13ページにも書かれているように、新たな重要インフラ分野や事業者の候補を選定することも視野に入れつつ、2020年東京オリンピック・パラリンピック競技大会に重要な影響を与えるサービス、事業者、分野の候補を選定し、万全な対策を推進していくことがとりわけ重要と考える。

第２に、今回まとまったサイバーセキュリティ戦略は国際的にも誇ることができるものであると同時に、諸外国の参考になるものでもある。英訳が近く公表されると聞いており、このことはサイバー外交の積極的な推進という観点からも有意義であるということを指摘しておきたい。

第３に、国際的なルールとの関係について、これまで指摘しなかったと思われることを１点補足する。サイバーセキュリティ戦略の「公正なビジネス環境の整備」の項目で14ページにある「セキュリティを理由に国際的な貿易のルールに不適切な影響を及ぼす措置に対しては、国際的な連携のもと、厳格に対処する。」という指摘は特に重要である。国際社会において、偽装された保護貿易は、例えば環境保護を名目にした貿易規制措置となって時々表れているが、今後サイバーセキュリティを名目にした貿易規制措置が出現することも十分予想され、そのような動きに対して国際的に実効的な対応をとる体制を整えることによって、公正なビジネス環境の維持、確保に努めることが重要であると考える。

○（野原本部員）私からは２点申し上げる。

まず１点目、2020年東京オリンピック・パラリンピック競技大会、来年の伊勢志摩サミットもあり、日本の組織がターゲットになる機会が著しく増加する中、今回の日本年

金機構への標的型攻撃の事案を契機に、政府、重要インフラだけでなく、一般企業も含めたセキュリティ対策の強化をしていくことは極めて重要と思う。その意味で今回の戦略の見直しは大変重要で、しっかり取り組んでいただきたい。

その上でもう１点だけ申し上げたい。こうしたセキュリティ対策の強化や拡充は大変重要であり、非常によくわかるのであるが、一方で、利便性、使い勝手とのバランスを保つことも大変重要だと思う。セキュリティ対策を検討していくと、どうしても対策の強化、拡充、ルールの厳格化にばかり話が行き、ルールはあるものの形骸化してしまうこともよく起こると思う。

今回の日本年金機構の事案の場合も、規程上は、原則として個人情報をネット非接続の環境下に置くなどとされていた。多分業務上の使い勝手もよくなかったこともあるかと思うが、あちこちの部署で必要な部分を自分のPCや共有サーバに置いていたことが、大きな情報流出になった一つの原因になっている。このようなひずみをもたらすケースは、一般企業にも見られ、例えば銀行や保険などの金融業界では、社内のPCで、シェアの高いウェブブラウザや一般に皆さんが普通に使っているソフトウェアといったものもダウンロードできない、自由な情報収集がしにくい、端末の持ち出しもできないといった厳しい状況を設定してしまっている。暗号化ツールもあるが、パスワードの管理ツールが未整備で使い勝手が悪いという状況も見受けられる。

リスクが高まって新たなサイバー攻撃も次々出てくる中、対策の強化はとても重要であるが、ただ闇雲にセキュリティ対策レベルを高め、強化するということだけでなく、運用に柔軟性を持たせ、必要なところとそれほど必要でないところをきちんと判断するような仕組みを入れていくといった、使い勝手あるいは利便性とのバランスをきちんと入れ込んでいくことが大変重要ではないかと思う。

もう少し発展して考えると、セキュリティ関連産業が提供するサービスの使い勝手の向上も進めていくとよいのではないか。利用者は、どうしてもセキュリティの機能やコストで選ぶので、セキュリティツールなどソフトウェアやサービスの使い勝手が余り良くなく、現場の使い勝手がないがしろにされがちである。これは、選択する側も考えなければならないし、サービスを提供する側も使い勝手をどうすると高められるのかを検討していく必要があるのではないかと思う。

○（山口情報通信技術（ＩＴ）政策担当大臣（副本部長））

本日の「日本年金機構における個人情報流出事案に関する原因究明調査結果」、また、その改善策を盛り込んだ新サイバーセキュリティ戦略（案）を踏まえ、政府としては関係機関を含む政府機関等の対応能力の抜本的強化に取り組んでいきたい。

特に政府全体として最適な予算や人員の確保を図るほか、サイバーセキュリティ基本法のあり方も含めて、必要となる法整備なども検討していきたいと考えている。また、サイバーセキュリティの強化はIT・データ活用の促進等を通じた我が国の産業競争力強化等のためにも不可欠なものであり、IT担当大臣としても、IT総合戦略本部もこの本部と緊密に連携を図っていきたいと思っている。

さらにマイナンバー制度を円滑に導入して、国民の皆様方に安心をして利用していただけるよう、制度の運用に必要なセキュリティ対策にも万全を期していきたいと考えて

いる。

○（宮沢経済産業大臣）

３点申し上げる。

まず、IPA はサイバー攻撃の対処に関し優れた知見を有しており、独立行政法人や特殊法人などにおける対策を始め、重要インフラの官民の情報共有体制の強化などに貢献すべく、引き続き NISC との連携強化を進めていく。

次に、民間企業のセキュリティ政策については、ユーザー事業者、セキュリティ事業者双方における対策の強化が重要である。ユーザー事業者向けには経営層のリーダーシップによる対策を促すため、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する。セキュリティ事業者向けには政府系ファンドの活用などにより、サイバーセキュリティを成長産業として振興し、対策の強化などにつなげていく。

３点目として、マイナンバーカードを始めとした IC カードは、その秘密情報が解読されないよう、十分なセキュリティを確保されていることが利用の前提となる。IPA は IC カードの安全性の認証を行っており、引き続き安全確保に貢献していく。

○（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）

かねてから、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、サイバー空間を含むセキュリティの確保が最も重要な鍵の一つであると私は考えている。前回・今回の会合における議論を伺い、改めて実空間とサイバー空間の融合、特に IoT システムの急速な普及、進展に伴うリスクの増大について認識を新たにしたところである。

こうした脅威に的確に対応して大会を成功に導くためには、前回の会合でも申し上げたとおり、サイバーセキュリティ上のリスクの明確化、CSIRT の整備、専門家の確保等の推進が重要である。過日８月３日、大会のセキュリティ対策を推進するセキュリティ幹事会においても各省庁に対し一層の取組強化を要請した。

また、皆さんに大変御心配をおかけしたが、先週 14 日に新国立競技場の整備計画の再検討に当たっての基本的な考え方を決定した。サイバーセキュリティの確保についても設計段階から十分考慮されるように配慮していく。

○（西銘総務副大臣）

総務省は、地方自治体の情報セキュリティ対策について専門家及び自治体職員を構成員とする自治体情報セキュリティ対策検討チームを立ち上げて議論を行い、去る８月 12 日に中間報告として緊急強化対策を取りまとめた。また、新たな戦略を踏まえ、政府、独立行政法人、特殊法人等へのサイバー攻撃への検知・対処能力や監視・監査機能の向上に資する人材育成基盤を強化するため、国立研究開発法人情報通信研究機構（NICT）が持つ演習基盤や攻撃観測、分析に係る技術的な知見を活用して、実践的な演習、訓練を行う体制整備を強化する。

総務省としては、このような取組を通じてマイナンバーのセキュリティ確保を始め、我が国全体のサイバーセキュリティを一層強化していく。

○（左藤防衛副大臣）

この度サイバーセキュリティ基本法に基づく初めてのサイバーセキュリティ戦略が取りまとめられ、本日決定されることは、我が国のサイバーセキュリティの確保及び今後の取組にとって大変有意義なことであると思っている。本戦略の策定に関わった方々の御尽力に改めて感謝を申し上げたい。

本日決定されるサイバーセキュリティ戦略及びサイバーセキュリティ 2015 等を踏まえ、防衛省・自衛隊としても、自身のサイバーセキュリティの確保に引き続き努めていくとともに、内閣サイバーセキュリティセンターを中心とした政府全体の取組への貢献にも努めていく。

先ほど話があったサイバー関連予算についても、平成 28 年度予算重点化方針を踏まえ、所要の予算要求に向けて準備したいと思っているので、よろしくお願いを申し上げる。

○（薗浦外務大臣政務官）

今般の戦略の策定においては、国際社会の経済的な繁栄、安全保障に関する諸課題に取り組む上でも大きな意義があると考えている。今後様々な機会に各国の政府、関係機関等に対して、本戦略に基づく我が国の取組を積極的に発信していくとともに、二国間協議、また、ASEAN 地域フォーラム（ARF）等の多国間の枠組みを通じて、各国との協力、連携を推進していく。また、サイバー空間における既存の国際法の適用、国家の責任ある行動について、国際社会における議論を進めていく。さらに、ASEAN 各国を始めとする途上国に対するサイバーセキュリティに関する能力構築支援においても、積極的に取り組む。NISC 及び関係省庁との連携を強化するとともに、外務本省、在外公館のみならず、所管の独立行政法人も一体となって対策を講じていく。

○（金高警察庁長官）

サイバー犯罪、サイバー攻撃等の脅威が深刻化している。国民や事業者が安全で安心して暮らし、活動できる社会を実現するためにも、警察はサイバー空間を含めた治安維持の責務を果たしていく。このため、警察においては内閣官房等の関係機関や事業者等と連携し、サイバー犯罪及びサイバー攻撃事案の捜査を強化するほか、その未然防止、被害拡大防止のため、共同訓練や情報の集約、分析に基づく注意喚起等を強化することとしている。

なお、日本年金機構に対するサイバー攻撃事案については、引き続き鋭意捜査を推進する。

○（塩崎厚生労働大臣）

本日は日本年金機構における個人情報流出事案に関する原因究明調査結果について、取りまとめをいただき感謝申し上げたい。また、有識者本部員の先生方にも御心配をいただいていること、誠にありがたく感謝申し上げたいと思う。

今回の報告書では、NISC による技術面、運用体制面での検証結果で詳細な分析がなされている。この中で、厚生労働省及び日本年金機構における CSIRT 等のインシデントに

対応するための体制の整備が十分ではなかったこと、日本年金機構の情報系ネットワークにおける標的型攻撃に対する多重防御の取組がやはり十分でなかったこと、そして、訓練や研修の充実などの御指摘を多々いただいた。

今後、厚生労働省としては、この報告書を踏まえ、専門人材の確保など、厚生労働省CSIRT を含めた情報セキュリティに関する体制整備、日本年金機構を始めとした厚生労働省関係機関における多重防御の取組の強化、標的型攻撃に対する実践的な訓練の実施などを通じた職員の意識改革など、今回の事案を教訓に日本年金機構を含め、厚生労働省全体として再発防止に取り組んでまいる。

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。

○（遠藤本部員）

野原本部員の御発言、また資料１－２の19ページで「目的に照らし、業務が円滑に実施できるような対策とは何か」として記載があると事務局から御説明があった「利便性」について、個人情報の有り様、情報の出し方の有り様といった部分のインターフェースの標準化がまだできていない。本当にサイバー空間を価値ある空間にしていくためには、その部分の標準化を、サイバーセキュリティのレベルの標準化と同時に進めていく必要があろうと思う。

○（村井本部員）

来年の２月のセキュリティ月間をターゲットに、年１回の自己点検をきちんと行うことは、先ほども述べたように非常に重要であるが、今、現実的に必要なことは、現在の行政のシステムを棚卸しして、全てのチェックをすることである。１回行えば次からは楽になる。よって、PDCA サイクルの中での来年２月の自己点検は、かなり大掛かりで根本的な棚卸しと洗い出しという目標を持つとよいのではないか。

また、棚卸しでどのような結果が出て、どのように対応したかを公表し、メッセージとして発信できれば、トラストをきちんと生むことができるのではないかと思う。

(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。

サイバーセキュリティ戦略（案）は、今後、所要の手続の後、閣議決定をお願いする。

また、サイバーセキュリティ2015（案）は、一般からの意見募集手続を本日から９月３日までの約２週間実施する。その結果を踏まえ、次回会合において最終決定することとした。

(4)　本部長締め括り挨拶

本日は、様々な観点から活発な御意見を頂き、新たなサイバーセキュリティ戦略を取りまとめることができたことについて、御礼申し上げる。

政府としては、今後、新たな戦略に記載されている施策を着実に実行に移していくため、NISCの機能強化を始めとして体制の一層の強化をしっかり図って、皆さんの期待に

お応えをしたいと思っている。
　また、本部長として、関係省庁が本日決定のあった戦略等を踏まえた着実な対応をとるようにしっかり指示してまいりたい。
　今後とも有識者の皆様には、どうぞ御協力をお願い申し上げる。

－　以上　－