サイバーセキュリティ戦略本部
第７回会合　議事概要

１　日時

平成 28 年３月 31 日（木）　８：30～９：30

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
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
島尻 安伊子	情報通信技術（ＩＴ）政策担当大臣
松下　新平	総務副大臣
武藤　容治	外務副大臣
若宮　健嗣	防衛副大臣
星野　剛士	経済産業大臣政務官
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
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、お忙しい中、早朝から御参集いただき、感謝申し上げる。

サイバー空間への依存が高まる中、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、官民が連携してサイバーセキュリティを確保することが不可欠である。

特に重要インフラ防護については、近年、諸外国で電力施設を対象にしたサイバー攻撃事案が発生するなど深刻化している。我が国においても、更なる対策の強化が急務である。

また、サイバーセキュリティ対策を担う人材は、政府機関・民間事業者を問わず不足していることも事実である。

優秀な人材を確保するためには、必要となる人材像を明確にした上で、産官学が連携して、能力向上と、それに応じた適切な処遇を図るなど、まさに人材の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る必要がある。

政府機関においても、このような観点を盛り込んだ人材育成方針を初めて策定したいと考えている。

本日の会合では、これらの点について御議論いただき、方針について決定したい。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人材育成総合強化方針（案）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向けたロードマップ（案）について

【報告事項】

・　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。

○（村井本部員）人材、重要インフラはとても重要な領域であるため、コメントを３点申し上げる。

まず、サイバーセキュリティ人材の育成について。IT 人材の育成は 2000 年からずっと取り組んでいるが、なかなか具体的な成果が上がらない。その理由の一つに、KPI、何をどこにいつまでにつくりたいか、それを決めておき調整していくということが必要だと思うが、これがなかなか難しいということがある。資料１－２「サイバーセキュリティ人材育成総合強化方針」の 15 ページに、橋渡し人材としての研修受講者数を今後４年間で 1,000 人を超える規模とする、という記述がある。こうした具体的な方針があり、かつそれを目標時期になったときにチェックし、評価する。こうしたことをやっていかないと、具体的な成果が出てこない。できれば概要のところに少し具体的な目標を書いた

ほうが良いのではないか。産官学の力を合わせて推進すべきだと思う。

２点目は、人材育成について考えるときに、知識も重要であるが、本当に大事なことは現場経験であるということ。大学院での専門知識修得などももちろん重要ではあるが、インターンシップなどでいろいろな企業の方のきちんとした指導のもと、重要な現場に入る。インフラの運用、ネットワークサービスの運用、あるいはIoTに関することやユーザー機器の利用など、サイバーセキュリティに取り組んでいる現場を経験するということを人材育成のプロセスに入れていくというのはとても重要なことだと思う。これは、実は東京オリンピック・パラリンピック競技大会に向けて、といった期限のあるスケジュールの中で人材が力をつけるためにも大変重要なことである。我々も大学のサイバーセキュリティの授業では、現場にインターンシップでお世話になって経験を積むことを計画しているが、政府を含め、社会全体でトレーニングのために人材を流通させ、経験を積ませるということが、とても重要だと思う。

最後に、第４回会合でも申し上げたが、ネットワークそのものは分散処理であり、全国に散っているものである。そのため、本日の内容からすると、地域や自治体を中心としたサイバーセキュリティ人材育成の施策や、重要インフラの施策に関して、地域、自治体、各都道府県がどのようにかかわるのかということがとても重要である。この戦略本部会合の場で議論していると、どうしてもそれぞれの地域での基準、目配り、方針についてなかなか議論しにくいところもあるが、サイバー空間は全国にそれぞれの重要な拠点があると考えて取り組むべきだと思う。

○（遠藤本部員）人材育成とインフラという観点で少しお話をさせていただきたい。

まず、人材育成であるが、今回、経営者層、橋渡し人材というところに焦点を当てていただいた観点は非常に高く評価できる。一方で、実際に攻撃に対応できる実務者の教育のあり方、この部分がまだまだ練れていないのではないかという感じを持っている。

その教育のあり方としては、分析能力、さらには対応技術のあり方、そして技術の維持という観点で実習できる環境、または実務実習の場を設ける必要があると考えている。

実際の人材像としては、一般的にはトップガン、中間エリート層、さらには予備群と大きく３つぐらいに分けることができるが、日本の中では、トップガンの関係で約30名、中間者層で約300名いると言われている。米国では予算自体も非常に大きくとっているが、人数でもこれの10倍から15倍ぐらいはいるのではないかと推定される。そういう意味では、私どもも人口比等もあるが、先ほど村井本部員から御指摘があったような明確なターゲット、目標を持って、人材の育成に当たる必要があると思う。

その中で、我々が倣うべき点は海外にもある。我々の人材育成の予算を効果的にどうやって使っていくかという観点では、例えば米国を参考にすると、米国のNIST（National Institute of Standards and Technology）が2011年に開始したプロジェクトであるNICE（National Initiative for Cybersecurity Education）において、ナショナル・サイバーセキュリティ・ワークフォース・フレームワークが立ち上げられており、各省庁の協力のもと、人材の育成、特に本格的なサイバー攻撃対策演習というものを行っていると承知している。こうしたノウハウを我々も見習う中で、日本ではNICTがNISTに当たる組織になると思うが、官民を挙げてこれに似た形のフレームワークをつくり上げながら、

人材を育成するということも必要であろう。

２つ目は、インフラ関係であるが、重要インフラが攻撃されることよって非常に大きな社会インパクトを受ける。残念ながら、今、セキュリティの専門家が制御システム自体を理解するための教育等が余りない。制御システムセキュリティセンターが多賀城市にあるが、そういうものをうまく使うことよって、さらにはそうした教育の場を設けることによって、セキュリティの専門家に制御系システムの特殊性というものを御理解いただく機関または機会を設けることが非常に重要であろう。

○（小野寺本部員）人材育成に関して２件、それに関連することを１件申し上げる。

まず、人材育成について、このような方針をきちんとまとめられたことは非常によろしいことだと思う。このように人材を育成していく中で、一つ問題となるのは、今、いろいろなところで人材育成ということを考えているが、それの連携、分担するのであれば分担の内容、そこをはっきりしていかないと、実効性、効率性を高めていく上で問題になるのではないかということが１点目である。

同じようなことであるが、先ほどもお話があったように、演習といったことの重要性をもっと理解していかないとだめではないかと思っている。これについても、例えばNISC が整理して、NICT が中心になってやるのかもしれないが、そうしたやり方を実務レベルできちんと詰めていくことが必要であろう。

高度人材育成についてはこういう方向で非常に結構だと思うが、第６回会合でも申し上げたように、セキュリティについてはリテラシーの問題、ここをしっかりやっていかなければならない。実際に自分のパソコンがどうなっているかもわからないで運用されるのは非常に怖いと思っており、そういう意味でセキュリティ人材だけではなく、そのベースとなる ICT の人材をどう育てていくか、これをもう一回しっかり考える必要があるのではないか。

皆さん御存じのように、アップルのロックの問題について、イスラエルの会社が解いたということになっているが、イスラエルは 1990 年代の終わりから高等学校の教育で義務化を始め、それが次第に広がり、結果的に今、ICT では注目される国になってきている。英国では、昨年の新学期にあたる９月より、５歳から義務教育の中でコンピューター教育を義務づけている。こういうことをしっかりやっていかなければならない。高度人材だけではなく、リテラシーや運用の部分も含めた人材育成を是非やっていただきたい。

２点目であるが、重要インフラに関連し、先ほどのセキュリティ人材育成にも関連するが、今回経営層に対して橋渡し機能ができる人材を育成しようということになっている。既に皆さん御存じだと思うが、コーポレートガバナンス・コードで非財務情報をできるだけ出していくという方向性が、今、示されている。この非財務情報の中でサイバーセキュリティ、個人情報保護も含めたところを各社にもっと書き込むようにさせていくべきではないか。形式的にやるのではなく、書いたことが逆に経済界だけではなく、社会から認められるような環境、例えば女性活用をやっているところの銘柄だけを集めたなでしこ銘柄というものがあるが、そのような方法も一つの方法だと思う。セキュリティ、個人情報に対してしっかり取り組んでいるところをリストアップするようなことも考えてはいかがか。

○（中谷本部員）サイバーセキュリティ人材育成と重要インフラについて幾つか申し上げる。

まず、人材育成について、今回の「サイバーセキュリティ人材育成総合強化方針」は時宜を得たものであり、内容的にも支持できるものである。そう申し上げた上で４点ほど指摘させていただく。

第１に、サイバーセキュリティ人材の需要に関して、安定的な職場を保障し、キャリアパスを確立していくことが、サイバーセキュリティ教育なども含むサイバーセキュリティ全般にとって極めて重要であるため、経営層、橋渡し人材層、実務者層の連携の構築を政府としてバックアップしていただくようにお願いしたい。

第２に、サイバーセキュリティ人材には、残念なことにまだ女性が非常に少ないのが実情であるので、サイバーセキュリティが女性にとっても魅力的なキャリアであることをアピールできる方策を一層考えていく必要がある。

第３に、高等専門学校は有力なサイバーセキュリティ人材の供給の宝庫となり得ると思われ、高専における演習環境の整備が一層なされることが、今後のサイバーセキュリティ人材の確保にとって特に有意義である。

第４に、情報処理安全確保支援士制度の創設は、良きサイバーセキュリティ人材の供給を奨励し、保証するものであって、非常に有意義であるが、名称はやや硬過ぎるかと思う。いかにもお役所的な名称だという理由で、能力ある若者が敬遠してしまうことが懸念される。正式名称はたとえこのままだとしても、スマートな通称をつけるといった工夫が望ましい。

次に、重要インフラについて、機能保障の考え方を基軸に据え、面的防護に向けた連携体制強化を重視するとしたことは、切れ目のないサイバーセキュリティ対策にとって重要なステップアップであると言える。そう申し上げた上で２点を指摘したい。

第１に、資料２－２ロードマップ案10ページの国の安全等の確保の観点からの取組にあるように、核物質防護等の措置が要求される安全保障上重要な企業や、先端技術の知的財産や営業秘密を保持する企業、研究機関、大学等への情報共有体制の整備はとりわけ重要である。重要インフラの指定業種を今後増やしていくことが望ましいことは、第２回及び第４回会合でも申し上げたが、重要インフラに指定されなくても、情報共有体制の整備などのサイバーセキュリティ対策は不可欠であろう。

第２に、米国を舞台とした最近のサイバー攻撃に関連して、2013年にニューヨーク近郊のダムの制御システムにハッカーが侵入したとして、米国司法省が先週起訴したということである。また、バングラデシュ中央銀行のシステムにハッカーが侵入し、ニューヨーク連邦準備銀行に保有する口座から約91億円が今年２月に不正送金されていたということである。日本の重要インフラも、いつ誰によって侵入を受け、攻撃されるかわからないので、インフラ事業者や業界団体と政府が緊密に連携して、さらに可能な限りの対策をとる必要があり、短期的には伊勢志摩サミットに向けて盤石の防御体制をとる必要があるかと思われる。

○（野原本部員）３点申し上げる。

まず、サイバーセキュリティ人材育成については、橋渡し人材は非常に重要で、それ

に対して特効薬的な施策と長期の施策をしっかり分けて、それぞれの目標数値を挙げてしっかり進めていくことが大変重要だと思う。

特効薬的な施策の中では、橋渡し人材への支援ツールとして、説明用のコンテンツであるとか、演習、セミナーといったもの等々いろいろ挙げられているが、これらは非常に有効だと思うので、しっかり構築、作成し、それを常に更新しながら進めていっていただきたい。

長期的な点については、米国などを見ると、IT 人材と同様にサイバーセキュリティの分野でもMBA とサイバーセキュリティとのダブルメジャーは決して珍しい話ではなく、セキュリティ人材は技術系の人といったようなイメージではない。日本の大学あるいは大学院、情報セキュリティ大学院大学があるが、そういった課程でもビジネスやマネジメント、経営についての知識をバランス良く持つ人材を育成できるような課程をつくっていっていただきたい。

２点目は、重要インフラについてである。重要インフラの取り組むべき方向性、強化すべき取り組みの方向性については、基本的に資料２－２のとおりだと思っている。重要なことは、情報共有の体制を実効性のあるものとしてうまく運用し続けること。その際、情報共有の強化策として、業界によっては既存の業法をうまく使い、その報告義務を使って体制をつくっているというお話もあったが、たまたまあった報告義務がサイバーセキュリティの趣旨にぴったり沿っているということはなかなか考えにくいわけで、改めてサイバーセキュリティ対策に照らしてどういう形が適切なのかということをしっかり検討し、ガイドライン等にまとめていただきたい。

３点目は、サイバーセキュリティ月間についてである。今年は例年以上にきめ細かないろいろな施策をしていただき、楽しいイベントもたくさんあって大変良かったのではないかと思う。いろいろな施策があったが、国民の意識向上のために若い世代にもリーチできるものが多かったのではないか。中でも、情報セキュリティハンドブックは、表紙の色が話題になった東京都の防災ハンドブックと全く同じ色になっていて、そのこと自体がネットで話題になったりして、小さいことではあるが、それによって効果がぐっと上がったと思う。こうした工夫の成果がどの程度あったのかということを国民各世代、各層へのリーチをしっかり把握するという形で検証し、今後に活かしていただきたい。

○（林本部員）私は大学に勤めているので、今回の決定事項の一つである「サイバーセキュリティ人材育成総合強化方針」に的を絞って３点ほど申し上げる。

まず、総合という方針ができたということ自体は、これまでいろいろ努力してこられた施策の方向性を一致させるという意味で大変意義がある。その上で、第１点目として、今回案のうちサイバーセキュリティ・情報化審議官を置き、定期会合を行うという案は、政府内におけるセキュリティ対策の歴史の上で画期的な意義があるのではないかと考える。担当ポストの新設によって、庁内の調整が一元化され、官庁横断的に同一機能が確保されることから、効率的で整合のとれた施策の実施が期待される。既に同種の審議官が置かれている官庁の例を見ても、その効果は十分実証されていると思う。また、中央官庁が動き出すと、自治体も民間も非常に敏感であるから、右に倣え的な同種のアイデアを検討すると思われ、そうした波及効果も入れると効果が何倍にもなるということを

期待している。

２点目として、橋渡し人材についてである。これは主として民間を念頭に置いたものと思われるが、第１点目で申し上げた官においても、審議官の機能を補佐するためにも必要なことは良くわかる。我が国の組織は一般的に中間管理者の能力と献身的な努力に大きく依存しているということは広く知られている。私も実はアメリカ企業の役員をしたとき、なかなか日本的にいかないと、中間管理者がいれば助かるなという気持ちを感じたことがある。この面ではこうした人材は不可欠なのであるが、ある意味では便利屋という機能もあるわけで、その後のキャリアをどう考えるかが際どいところかと思っている。現在の案では、実務者層と経営層の橋渡しをすると言いつつも、どちらかと言えば、実務者層のリーダー的なニュアンスがうかがえるような気がする。とすると、先ほどの便利屋となってしまい、その後のキャリアパスが不明確になるため、かえって不利益になるということもあり得る。特に我が国の組織はいわゆる主流派、あるいは売り上げが非常に多い事業部門が中心に運営されているため、そこから外れると損をするということをよく言われる。そのようなことで尻すぼみにならないように、逆に橋渡し人材の中から将来の役員や審議官級の人が生まれるように、側面援助を含めた特段の配慮が必要かと思う。

最後に３点目として、人材育成について産学官の協調がうたわれ、それなりに効果を上げてきたことは事実であるが、全体として供給不足であることは否定できない。情報セキュリティ大学院大学でもやっと修士を 300 人出すまでに至ったが、いろいろな計算をしてもちょっと桁が違うのではないかと言われかねない。特に官庁の人材確保のためには、サイバーセキュリティに特化した奨学金や官庁自身での長期インターンシップ、村井本部員もおっしゃったが、そういうことで新機軸を訴えていくことが必要ではないか。

アメリカでは、この種の奨学制度は 10 年近く前から行われているようである。一例として、インフォメーション・アシュアランス・スカラーシップでは、コース終了後２年間官庁に勤務すれば、授業料が無料になるということで、セキュリティ教育に強いインセンティブを与えている。また、CIO ユニバーシティという官民連携プログラムでは、修了後に政府機関で働く義務はないが、受講生が政府と民間が半々であるということから、交流がその場で行われるということになっているようである。オリンピックまでの時間的制約の中で、優秀な人材を呼び込むためには、時限的でも良いが、この種の制度化が必要ではないか。

人材が払底しているのは民間も同じであるが、第１点目で述べたように、政府が始めれば民間でも機運が高まるため、その際には、例えば教育訓練費用の非課税とか減免措置などの促進策も有効になるものと考える。

○（前田本部員）今日のメインテーマは人材育成かもしれないが、これに関しては今までの本部員の方々の御意見に加えるものは余りないが、一つだけ感想を申し上げると、このサイバーセキュリティ戦略本部でずっとお手伝いさせていただいていて、人材育成についての方針としては格段にレベルが上がった、具体化した、一歩前に進んだと思う。今後どうなっていくかというのは、ニーズに合わせて動いていくと思うが、この「サイ

バーセキュリティ人材育成総合強化方針」を非常に高く評価したい。

私の専門の立場から第３次行動計画の見直しに関して１点申し上げたい。キーワードはテロの問題で、テロの問題はサイバー世界と完全に不可分である。先ほど菅官房長官のお話にあった電力施設を対象にしたサイバー攻撃の問題、これと海外のマスコミで報道されているテロの問題とは非常につながっており、テロ組織が原発を攻撃しようとする際、サイバーが非常に深く結びついてくると思う。

伊勢志摩サミットのテロ対策でソフトターゲットということを言われているが、今回の第３次行動計画の見直しで一つだけ申し上げたい。第３次行動計画の中で演習が大事だと書かれており、そのとおりだと思うが、今までの演習を一歩深める、一歩前に出る、ということを検討いただきたい。その前に出る方向性の最大のポイントは、これだけテロがあって国民がテロの脅威を認識しているということ。テロだけではなく、いろいろな問題や事故の想定もあるのだが、その中でもテロ対策に結びつく演習、大規模なインフラをテロからどう守るかという視点、外国からどう守るかという視点も取り入れ、この第３次行動計画の見直しを具体化していく中で、そうした視点を盛り込んでいただきたい。

もう一つは、こうした具体的なテロ対策のような目前のもの以外に、大きな安全という意味では、やはり産業基盤の半導体といったものが世界に冠たる日本の技術力をもって他国に支配されないということが、ある意味でサイバーセキュリティの一番土台にあると思う。それは経済産業省を始めやってくださっていると思うが、当面私の立場からは、サイバーテロだけではなく、テロにつながる、あるいはそれに関連するサイバー領域での安全に係る施策、それをいつも申し上げているが、官庁の壁を取っ払って国全体としてオールジャパンで守っていくことが何より大事だと思う。

○（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本年２月に国会に提出し、昨日、衆議院の委員会で可決した。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、2020 年のオリンピック・パラリンピック東京大会を成功させるためには、様々な分野で必要となるサイバーセキュリティ人材を育成するとともに、重要インフラの防御能力を高めることが必要であり、関係機関との連携を進めていく。

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ので、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。

なお、先ほど中谷本部員からわかりやすい通称という話があった。昨日も委員会で多くの方からあったので、検討する必要があるかと思っている。

○（河野国家公安委員会委員長）平成 27 年においては、警察が事業者等から報告を受けた標的型メール攻撃が過去最多となるなど、サイバー空間の脅威は深刻な情勢にある。加えて、一段と厳しさを増す国際テロ情勢にあって、関連するサイバー攻撃が行われるお

それにも留意しなければならない。

間近に迫った伊勢志摩サミット開催に向け、警察では、関係省庁、重要インフラ事業者と連携してサイバー攻撃対策を進めている。引き続き御協力をよろしくお願い申し上げる。

また、４年後の2020年東京オリンピック・パラリンピック競技大会等、大規模な国際行事の開催を見据えれば、警察を始めとした対処機関において、高度な専門性を有する人材を適切に処遇し、確保・育成を図ることが喫緊の課題である。

本日決定される「サイバーセキュリティ人材育成総合強化方針」も踏まえ、人的基盤を強化するように警察庁を指導していく。

また、この資料２－１に対して一言意見を述べる。同資料中に「セプター」という用語が使われているが、この部屋の中でも「セプター」が指す内容がわからない人がいると思う。どういうスペルにするかわからない人がほとんどではないか。99%の国民がそのままでは理解できない言葉をこのように使うということに、私は断固反対である。

○（島尻情報通信技術（ＩＴ）政策担当大臣）本日、決定される「サイバーセキュリティ人材育成総合強化方針」の中で示されたセキュリティ・IT人材育成策は、近年のサイバーセキュリティ事案の増加等を受けて、サイバーセキュリティ対策と情報システムの適切な運用管理等の喫緊の課題への対応の核となるものである。

また、遠藤政府CIOを中心に取り組んでいる政府情報システムのスリム化や業務の効率化を一層推進する観点からも、セキュリティ・IT人材の育成は重要である。

今後、本方針に基づき、専門性を有する人材育成に向けて、各府省庁からの出向者をIT総合戦略室に受け入れるとともに、外部人材確保の観点から、一元的に採用・管理している政府CIO補佐官を各府省庁に派遣し、その積極的活用を図る等、貢献していきたい。

○（松下総務副大臣）総務省では、先ほど御説明いただいたサイバーセキュリティ月間結果報告でもあったが、昨年に引き続き、３月18日にNISCと共同でCYBER EKIDENを実施した。今回の大会では、課題を制限時間内に終えることができたチームの数が増える等、各府省担当者のサイバーセキュリティの対処能力に着実な向上が見られたところである。

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３月１日に閣議決定し、国会に提出している。

自治体における情報セキュリティ対策の抜本的強化については、交付申請のあった1,671市区町村及び45道府県に対し、３月８日に、対策支援のための補助金の交付決定を行ったところである。また、今回申請のなかった残りの72団体についても、新年度早々申請するものと聞いている。

今後も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く。

○（武藤外務副大臣）G7伊勢志摩サミット開催が目前に迫っている。政府機関や重要インフラ関係事業者等のホームページに対するサイバー攻撃が連続的に発生している。今後

も我が国に対してサイバー攻撃がなされる可能性は依然として高いと認識している。外務省としても、G7 の関連大臣会合の先陣を切って、来月 10 日、11 日に開催される G7 外務大臣会合、引き続いて５月 26 日、27 日に開催される G7 首脳会議に向けて、万全のサイバーセキュリティ対策を講じていく。

サイバーセキュリティ・IT 人材の育成・強化が喫緊の課題である中、本日、政府全体として「サイバーセキュリティ人材育成総合強化方針」が打ち出されたことは大変大きな意義があると認識している。外務省としても、サイバーセキュリティ・IT 人材の育成・強化に向けて、所要の取り組みを行っていく。

また、外務省としては、サイバー空間における法の支配や信頼醸成、ODA 等を活用した開発途上国の能力向上支援について、関係府省及び同盟国たる米国や友好国と連携をしつつ、引き続き積極的な取り組みを進めていく考えである。

○（若宮防衛副大臣）皆様方御指摘のとおり、深刻化が進むサイバー空間の脅威に備え我が国全体のサイバーセキュリティ推進体制を強化していくことは、極めて重要だと認識している。その中でも、今回の人材育成・確保はまさに喫緊の課題である。

今般提示された「サイバーセキュリティ人材育成総合強化方針」は、我が国全体のサイバーセキュリティ人材の育成・確保について、必要な取り組みが網羅的に示されているものと考えており、まさに時宜にかなったものである。

防衛省・自衛隊としても、本日決定される本方針を踏まえ、自らのサイバー攻撃対処能力を一層強化するのみならず、サイバーセキュリティ人材の育成・確保に積極的に取り組んでいく。

○（星野経済産業大臣政務官）東京オリンピック・パラリンピックに向けて、重要インフラ対策の抜本的な強化が必要である。

第１に、経済産業省は、重要インフラ事業者の制御システムを中心に、高度なサイバー攻撃に対する防御力を確認するためのテストを、IPA を通じて実施する。こうした取り組みを広げ、経営者を含めた攻撃リスクの認識を共有していくことが重要である。

第２に、国家やテロリスト集団が日々高度な攻撃シナリオと攻撃技術を考案している中、守る側も攻撃者側の視点に立った対策が必要である。このため、高度なサイバーセキュリティの技術開発や人材育成を強化し、攻撃と対策の見える化を通じて、重要インフラ事業者の積極的な対策への投資を促していくことが重要である。

第３に、対策を実装させるためには、業法による規制や対策の実施が市場から評価される仕組みが必要である。例えば、電力の制御システムにおけるセキュリティ対策を保安規定に位置づける取り組みや、企業の対策の度合いに応じてサイバーセキュリティの保険料を割り引く仕組みの普及などを進めていく。

第４に、今通常国会での情促法改正を通じた資格制度の創設とその普及を図り、重要インフラを守る人材の育成や質の担保を強化していく。

最後に、このような一連の取り組み以外も含めて、セキュリティのベンダー（供給者）のみならず、重要インフラ事業者の積極的なコミットメントを得ながら、セキュリティの産業化による対策の強化を進めていく。

○（河野国家公安委員会委員長）サイバー関係の政府の文書は日本語として読んでもよくわからない。英語でも意味がよくわからないという単語が非常に多く、読む人によってはばらばらな概念でとっているものもあると思う。国民が読んでわかるよう、意味の不明なところはきちんとした日本語にしっかり置きかえていただきたい。これは行革でも問題提起をしている。「セプター」という用語がわかっている人は手を挙げてみていただきたい。これが現状である。これでそのまま議論しろと言ってもわからないのである。当該文章は日本語にきちんと置きかえていただきたい。

○（遠藤本部員）先ほども演習または教育機関みたいなお話を少し申し上げたが、レベルを上げていくという観点で考えたとき一番重要なことは、攻撃者がどのように攻撃をしてくるかをしっかりと理解するということ。そういう観点では、攻撃者がどのように攻撃してくるのかをしっかり身につける施設、設備というものが常備されている必要がある。我々のサイバーセキュリティの人員自体がそういうものにアクセスして、中のシステムがどうなっているのか、どういう形で攻撃を受けそうなのか、それを実体験できる施設または設備というものを常時持っていないと、そういう能力は上がってこない。

そういう部分は、かなりお金もかかる領域だと思うので、それが公共的に使える、常時使えるシステム、設備として整えることが非常に重要であろう。官民一体になってそうした施設、設備をつくり上げていき、それを維持していくことが非常に重要であると思う。

○（前田本部員）先ほどの小野寺本部員のお話にも出てきたアイフォンとFBIの関係で、国家の存立の問題と通信の秘密、個人のプライバシーはどちらが重要か、みたいな議論がアメリカであり、高い技術力で解決したから議論が消えたように見えるが、これは根本的な問題として残っている。憲法などいろいろな考え方があるため、この議論に関して、政府としてお考えを固めていただかなくてはいけないと思う。そのときに世界的レベルで見ると、いろいろな国がある。アメリカは一番個人情報を保護するという考えであり、憲法の理念からもそうなっているが、それとは逆の立場の国もある。ヨーロッパはヨーロッパで違うのである。一番大事なことは、日本型をどうつくるか、日本の現状に合わせて、日本の文化、伝統も踏まえてどうしていくかということ。最後は国民が決めることだと思うが、さきほどテロの問題で今、日本の情勢としては安心・安全が大事であると強調した。一方で、これだけスマホが広がって、これを政府に見られたくないという意識ももちろんあるが、そうしたことの対策について是非きちんと軸を考えていっていただきたい。これは情勢で、いろいろな動きの中で揺れていく問題だと思うが、今の日本で何が軸なのか。起こらなければ気にならないが、起こってしまったらもうおしまい、大勢の方が亡くなるというような問題なのである。そこのところの視点を是非よろしくお願いしたい。

○（林本部員）これは私自身の反省でもあるが、12年前に情報セキュリティ大学院大学をつくったときに、最初からセキュリティ問題というのは技術問題だけではない。もちろん技術問題が中心ではあるが、それ以外に法律とか技術標準や慣行というソフト的な法

律とか、いろいろなものが関係してくるので、それをトータルでコースを設定した。その当時としては先見の明があったかと思っており、韓国などに行くと、自分たちのほうは技術では進んでいると自負しているが、あなたのところは総合的にやっているのはまいったねと言われたこともあり、そこそこだったかと思う。

ところで、大学院であるから若い人を採りたかったが、大学から大学院に進学するところは、それぞれの大学ががっちり固めているので、情報セキュリティ大学院大学に来ていただくようなことは難しかった。結果として、ビジネスマンが８割ぐらいということになって、これも結果であるが、授業をやってみると、会社で仕事をしたことがあるかないかということは大変違うものだということがよくわかった。セキュリティのような問題は、これを持って帰って会社に報告したときに、その情報をどこまでどのような手順で上げるとか、情報共有機関に出すとか出さないとか、いろいろな決断があるわけで、そういうことの勘が働くか働かないかは非常に大きいと思った。

そうしているうちに、だんだんと今度は官庁の方も私どもの大学院に来てくださるようになり、今はナショナルセキュリティ絡みのところはほとんど全部出していただいているような状況になっていて、その人たちから今度は情報セキュリティとナショナルセキュリティということの接点のようなことを学びたい、という要請が出てきた。

そこで、はたと困っているのが、そういうことを教える先生をあらかじめ教育しておかなかったということ。たまたまここで本部員をさせていただいているので、前田本部員とか中谷本部員とともに非公式な会合を持ったりして、そういうことに関心のある方のリストアップであるとか、相互交流であるとかを進めているのだが、そこでわかるのは、先ほどの河野大臣のお話ではないが、同じような事象についてそれぞれの縦割りの組織の中で違った表現をされているということである。例えばプロアクティブ、これは日本語に訳しにくい。これを警察がどう考えているか、防衛省はどう考えているかは微妙に違うのである。違うのは違う理由があるからいいのであるが、教えるということになると、そこのところは揃えておく必要がある。せっかく「サイバーセキュリティ人材育成総合強化方針」ができ、これは大変良いことなのであるが、自問自答でもあるが、それを教える人の育成はどうするかということに大変頭を悩ませている。

○（村井本部員）まず、少し気になっていることは、組織の名称が、河野大臣がおっしゃったようにいろいろあり、例えばCSIRTという言葉は普通名詞であるが、JPCERTという言葉は固有名詞である。セキュリティのインシデントレスポンスチーム、これは一般名詞であるが、これを大体全ての組織にきちんとつくろう、例えばオリンピック・パラリンピック委員会の中にもつくろう、経団連や経済産業省は各企業につくろう、政府では各政府の機関の中につくろうということである。インシデントに対応するチームをつくるのは重要で、これをネットワーク化していき、世界とつないでいく必要がある。これはJPCERTから見るとFIRSTという組織があるが、２つ問題があり、一つはこの国際ネットワークが世界のネットワーク、地方のネットワーク、いろいろな組織のネットワークと、サイバー空間上でうまくネットワークをして、情報交換をして助け合わなくてはいけない。この仕組みを誰がどこで責任を持つのかということである。

JPCERTは、独立した中立の組織としてつくって運営してきたが、今の実態は、主に経

済産業省にサポートしていただいている。そうすると、JPNIC というネットワークアドレスを扱っているところもあるが、サイバー空間で比較的中立の機関として行政や各企業、産業分野、つまり縦割りを横につなぐための良いことをする組織がナショナル CERT としての JPCERT である。これをどうやって維持していくのか。その維持の体制を考えなくてはいけないということが一つある。

資料１－１の右下を見ていただくと、人材の供給ということで資格を与え、評価をする。これが大変重要なサイクルであるが、これを議論していると、人材育成 R&D とよく言うが、リサーチ・アンド・デベロップメント、つまり今年の課題は何であるかということを調べるリサーチと、そのための教材や制度をつくるデベロップメント、教育というのはこのリサーチ・アンド・デベロップメントをいつも回転させ続けなくてはいけない。これのコストは結構高いのである。例えば通信会社が小野寺本部員のところで行ったとすると、現場のトップガンを連れてきて社員教育の仕組みをつくり、これを回さなくてはいけないので、コストがものすごくかかる。そうすると、国全体で持続していかなければならない必要な機関を、どういう環境で用意して、持続させていくのかという課題が幾つか浮かび上がってきていると思う。CERT みたいなものや NIC みたいなものが対象だ。それから、R&D をやりながら教材をつくるというのは大学の使命であるから、大学もかなり積極的にやらなくてはならない。そういうことを少し確認して明らかにすることはとても重要ではないかと思った。

特に JPCERT の件は、皆の問題だと思うので、考えていただきたい。

(3)　決定事項の決定等

決定事項２件につき、必要な用語を修正の上、決定した。

(4)　本部長締め括り挨拶

本日は、大変活発な御意見をいただき、「サイバーセキュリティ人材育成総合強化方針」並びに「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に向けたロードマップ」が取りまとめられた。感謝申し上げる。

政府としては、この決定に基づき、NISC の機能強化を初め、サイバーセキュリティの強化に全力で取り組んでいく。

有識者の皆様においては、今後とも戦略本部の取り組みについて、引き続き御指導賜るよう、お願い申し上げる。

－　以上　－