高度情報通信ネットワーク社会推進戦略本部　情報セキュリティ政策会議
第38回会合　議事要旨

１　日時

平成26年１月23日（水）　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
古屋	圭司	国家公安委員会委員長
岸	信夫	外務副大臣
亀岡	偉民	内閣府大臣政務官
藤川	政人	総務大臣政務官
磯﨑	仁彦	経済産業大臣政務官
木原	稔	防衛大臣政務官
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株式会社代表取締役会長
中谷	和弘	東京大学大学院法学政治学研究科教授
林	紘一郎	情報セキュリティ大学院大学教授
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
前田	雅英	首都大学東京法科大学院教授
村井	純	慶應義塾大学教授

（その他出席者）

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
米村	敏朗	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	内閣官房副長官補
古谷	一之	内閣官房副長官補
佐々木	良一	内閣官房情報セキュリティ補佐官
徳田	英幸	内閣官房情報セキュリティ補佐官
篠田	陽一	内閣官房情報セキュリティ補佐官

４　議事概要

(1)　議長冒頭発言

本日は、お忙しい中、ご出席いただき感謝申し上げる。

この１年をとっても政府機関や独立行政法人に対するサイバー攻撃が多数確認された。残念なことに、その一部で情報漏えい、情報流出のおそれもあるなど、サイバーセキュリティは国家の安全保障・危機管理上ますます重要な課題になっている。

このような状況を踏まえ、「サイバーセキュリティ戦略」や、昨年１２月に閣議決定した「国家安全保障戦略」に掲げる、政府機関や重要インフラにおける情報セキュリティ対策やこれらを支える人材の育成・体制等について、一層の強化が必要と考えている。

今回は、新体制での初めての会合となるが、活発な御議論をいただきたい。

(2)　討議

・　「サイバーセキュリティの日（案）」について（決定）
・　サイバーセキュリティ政策の評価等について（決定）
・　「情報セキュリティ人材育成プログラム」の改訂の方向性について
・　「政府機関の情報セキュリティ対策のための統一基準群（案）」の検討状況について
・　「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（案）」の検討状況について
・　ＮＩＳＣの機能強化に関する検討について
・　情報セキュリティ月間について
・　政府の情報セキュリティに関する予算案について
・　ＩＴ利活用セキュリティ総合戦略推進部会の開催について

上記について、事務局より資料に基づき説明が行われるとともに、構成員より意見が述べられた。

○　人材育成及びＮＩＳＣの機能強化について述べる。

長期的視野に立つと、人材の育成が最も重要である。これらの人材を育成するには、大学等の教育現場と、産業界とが連携し、正のスパイラルを形成していく必要がある。

大学等の教育機関に対しては、セキュリティに対する教育のあり方を変革して、実務に長けた人材の育成を特にお願いしたい。単に知識としてのセキュリティを詰め込むだけではなく、実習や体験を通じ、現実に起こる現象、インシデントに対応できる能力を獲得していくことが極めて重要である。

また、特定の情報系の学部、学科にこだわるのではなく、こういった人材を全分野で広く育成することが必要である。これは、同時に日本の将来の産業力の基盤強化にもつながる。

既に学生を対象としたセキュリティキャンプ、学生と社会人の両方が参加できるＣＴＦ大会など、全国規模での活動が行われているが、さらに突出した人材を育てていくためには、全国の大学や高校に優秀な指導者を育成・配置、学生の個性と才能を育成し、トップ選手を輩出するような、地道な活動を継続していくことが重要。産業界において

も、これらの人材を有効に活用し、才能を開花させる体制の整備を図ることにより、正のスパイラルを形成していくことが必要である。

ＮＩＳＣについては、的確な情報の共有と解析、それに基いたリアルタイム且つダイナミックな対処の方向性を打ち出していくことが非常に重要なミッション。その観点からのＮＩＳＣの機能強化に取り組んでいくべきである。

また、政府の情報セキュリティ予算については大幅な増額を図ってもらっているが、米国と比べると、まだ約１４倍程度の開きがある。ＧＤＰ比と同様のレベルである３倍ぐらいの差にまで縮めていく更なる努力が必要。そのバックグラウンドとして、2020 年の東京でのオリンピック・パラリンピックを念頭に置き、それまでの間に開催される 2016 年サミット、2019 年プレオリンピック、ラグビーワールドカップといった節目のイベントにおけるセキュリティ対策の観点からも、我々が長期的視点に立って、どうあるべきかを考える必要がある。

現在、Ｊ－ＣＳＩＰという情報共有の枠組みに参画しているが、アクティブな活用、解析を通じたさらなる有効な活用という観点から、ＩＰＡにおけるサイバーレスキュー隊の活動においても攻撃の情報、ノウハウを活用していくことにより、さらに強固なセキュリティのシステム、サイバーセキュリティシステムを構築していけるのではないかと考えている。

○　皆さんの努力でかなり情報セキュリティの重要性への関心は高まっている。サイバーセキュリティの日を設けることは大変良いことであり、より関心を持ってもらえるだろう。しかし、今回のサイバーセキュリティの日の普及・啓発活動に、ＰＣの基本ソフトのWindowsＸＰのサポートが今年の４月９日で切れる件について記載されていない。現在、この問題について、大手企業では既にかなり対策が講じられてきているが、中小企業や個人レベルでは未だ必ずしも十分ではない。したがって、このサイバーセキュリティの日を活用して、意識啓発をもっとやらないと危ないのではないか懸念している。

また、情報セキュリティの人材育成プログラムについては、以前から様々なことを申し上げてきた。特に情報セキュリティ人材の不足数が引用されているが、そもそもソフトウェア、ＩＣＴの人材の公的な統計というのがほとんどなく、実態を捉えきれていないという実情が懸念される。ＩＰＡのＩＴ人材白書でもこの点が指摘されている。ＩＰＡは、ＩＴ提供側、いわゆる企業側からＩＴ利用者、ユーザー企業側に分けて、それなりの推計値を発表している。しかし、これは公的な統計データではない。これは大きな問題である。

例えば、情報セキュリティとも非常に関係が深くなりつつある、いわゆる組み込みソフトウェアの分野を例に取る。経済産業省が平成 22 年度に調査した組み込みシステム産業実態把握調査では、組み込み関連製造業が国内総生産名目に占める割合は 10.5%、組み込み以外の製造業は 7.5%となっており組み込み関連産業の方がずっと割合が大きくなっている。つまり、ほとんどの製造業がこの組み込みソフトウェアを使っているということが、実態として明らかになっている。しかも組み込み関連製造業において、製品開発に占める組み込みソフトウェアの開発費の比率は経年的に上昇しており、経済産業省による平成 23 年度の調査では 49.6%、つまり、開発費の約半分をソフトウェアが占

めるという結果がある。ところが、ソフトウェアの開発が一体どこでどのようにされているのか。また、どういう人たちが行っているのかという人材統計、オフショア開発がどうなっているかという産業の統計はほとんどないというのが実態である。大学の先生からは、仮に人材を育成した場合、産業界が全員を雇用するか問われることが多いが、その問に答えるためにはソフトウェアに関する産業統計をきちんととっていく必要がある。さらには、情報セキュリティそのものの根本のところを理解するためには、まずはソフトウェアに関する産業統計をきちんととり、その上で、例えばこういう重要なソフトウェアについてはオフショア開発の是非を議論する必要があると考えている。どういう統計が必要なのか、どういう数値、情報が必要なのかというのは、まだまだ議論しなければいけない問題であるが、少なくとも国としてソフトウェアの産業統計をもう少しきちっととっていくことを、ぜひお考えいただきたい。

○　５点申し上げる。

第一に、経営層の意識改革に関連して、企業が情報セキュリティについてしっかりした対応を行うことは、単にその企業にとって重要であるのみならず、社会全体にとって重要であるということを再認識する必要がある。この意味で、情報セキュリティ対策を講じることは、企業の社会的責任、CSR の一部をなすと言えるだろう。企業、特に中小企業にとっては、安全保障輸出管理と同様に、厄介で、コストがかかる主題と思われるかもしれないが、CSR の一環として考えて欲しい。

第二に、重要インフラの情報セキュリティに関しては、特に力を入れて万全の対策をとる必要がある。さらに、防護に関する国際標準や規格の作成については、日本が積極的にイニシアティブをとって進めていく必要がある。特に、国際ルールの作成は作成者に必然的に有利に作用するので、先手を打って積極的に進めていくことが望ましい。

第三に、人材育成に関連し、大学に籍を置く者として、大学教育においても情報セキュリティ関連の授業を増やすべきだと実感している。情報セキュリティ関連の事業は主に理系においてなされていると理解しているが、文系においても今後積極的に取り上げていく必要がある。

また、将来の人材に関しては、この分野において、優秀で、基本的に善良だが官庁や企業での通常の生活にはなじまず、より自由なライフスタイルを求める若者が相当数いることを考慮する必要がある。彼らや彼女らをうまくリクルートできるよう、官庁や企業の側でも一層の工夫をする必要がある。

第四に、安全保障上の重大な脅威となり得るサイバー攻撃に対しては、ＮＩＳＣと国家安全保障会議との連携強化を含め、十分な対応の体制を整えることが喫緊の課題である。また、各官庁においても危機意識を一層高めることが望まれる。

第五に、WindowsXP のサポート終了について、十分注意を促す必要がある。

○　４点申し上げる。

本日のテーマの中で最も重要なのは、人材育成の体制をどのようにしっかりつくっていくかということである。

まず１点目、人材の量的拡大と質的向上の重要性についての記載があり、その解決方

策としてボリュームゾーンに当たるＩＴ技術者全体のセキュリティ技術向上を目指す方針は、事務局案のとおり最も効率が高いと考える。ＩＴ関連の技術者は 106 万人ほどいると言われており、人材の不足を補う上で効果があるし、言うまでもなく、ＩＴ技術者自身が情報セキュリティに関する能力を向上することが非常に重要である。その上で、その具体的な方法として、資格や評価基準の整備が挙げられている。その内容としては、時々刻々と移り変わる情報セキュリティの状況に対し、適時的確にキャッチアップできるよう、情報セキュリティに関する更新制の資格の導入や、定期的なセミナーの受講を義務づけるといったことを考えていると伺った。しかし、むしろその資格を持っている人たちが常に新しいインシデント情報や新しい技術情報をしっかりと入手できて、最新の情報やスキルを身につけて動くことができるよう、どういう体制をつくるのか、そして、キャッチアップできるようにどう導くのかということをしっかり検討し、埋め込んでいくことのほうが、重要だと考える。

２点目に、ＮＩＳＣの機能強化においても人材の話題として、「専門的人材の配備・育成」が挙げられている。具体的には、専門的人材として分析研究などを行う職をＮＩＳＣに配置したいところであるが、現状では置くことが難しいため、可能となるよう措置したいとの趣旨があると伺った。大変重要なことであり、しっかりと整備していただきたい。その上で、政府については、国際会議や交渉の場において、我が国の情報セキュリティの担当者としての顔を持って存在する人材が重要である。しかし、我が国の官庁では、１年半から２年の期間で人事異動があり、定期的な国際会議があっても会合のたびに異なった者が我が国を代表して出席するということとなり、その結果、会議の場で何年間かかけてつくった計画等において、我が国だけがクレジット上、前半・後半を担当した２人の名前が記載されている、といったことも実際に多々発生していると聞いている。

今のような２年での異動ではなく、４年、５年といった長期間しっかり腰を据えて情報セキュリティの顔として活躍してくれる人材をしっかりと置き、それで体制をつくっていくことが、政府機関の中にとても重要である。

３点目に、情報セキュリティに関する普及・啓発活動を通じた経営者の意識改革が重要である。昨年、経団連でシンポジウムを行い、経営層に向けて情報セキュリティについての実態や対策の在り方についてディスカッションをした。関心は非常に高く、参加者は多数で、興味を持っていると実感するが、同時にどちらかというと様子見や横並びの意識が強く、積極的に自分の会社で経営戦略として情報セキュリティを位置づけてやっていこうというところまでにはまだ至っていないと感じた。

そこで、今回のサイバーセキュリティの日や情報セキュリティ月間の間、積極的に情報セキュリティの普及・啓発に関するイベントを開催するが、さらにいろいろな場での活動に取り組み、経営層の意識改革を進められたい。

４点目に、普及・啓発の取組である「セキュリティ対策９カ条」を一般の国民、ビジネスマンに周知するための工夫について述べたい。この９カ条はコンパクトであり、その内容も確かであるが、実際に我が国のどれだけの人の手に渡り、受け取った人達のうちどれだけがそのとおりに動いてくれるか、疑問なしとできない。どうやったらわかりやすく、最も関心のない人たちのところまできちんと届くのかを工夫して施策を打って

いく必要がある。

○　人材育成プログラム改訂の方向性について、２点述べたい。

第１点は、政府機関にもキャリアパスの一端を担って欲しい、という意見である。情報セキュリティ大学院大学は、今年度末で開学から 10 年を経過することとなり、修士号取得者を約 250 名、博士号取得者を 23 名世に送り出したことになる予定である。この 10 年間、学部レベル等で情報セキュリティについて専攻やコースとして設定したところはあったが、大学院レベルでは他に登場せず、情報セキュリティ大学院大学が独占した状態にあった。したがって、そもそも我が国において、情報セキュリティに関する大学院のコースに応募する者数はこの程度であり、本日の会議資料上にある人材の需要と供給のミスマッチに符号していると考えられる。このミスマッチについて院生から聴取する限りで考えると、セキュリティ専門家としてのキャリアパスが非常に漠然としているので、将来に不安があるということが最も大きな障壁ではないかと捉えている。

情報セキュリティ大学院大学のみならず、既にセキュリティ教育を部分的に取り入れている大学、大学院、専門学校も含めて、供給サイドに問題があれば、少なくとも自力で解決する努力をすべきであり、また、自力で解決する覚悟をしている。しかし、需要サイドの問題については、中央官庁を含めた方々にある種の呼び水を提供してもらい、ミスマッチ解消のための手助けをして欲しい。具体的には、米国では、10 年以上の歴史がある政府機関におけるインターン制度がある。２つのプログラムがあり、１つはインフォメーション・アシュアランス・スカラシップ・プログラム、もう一つは、ＣＩＯユニバーシティプログラムという大学間の特別な教育の連携である。それぞれに連邦予算がついて、奨学金あるいは連邦政府で働く機会が提供されている。韓国なども同種のプログラムを提供していると聞き及ぶので、我が国でもこの点を検討いただきたい。

第２点は、産官学が協調してインシデント情報や検体を共有することについてである。資料５－１でも「情報共有体制の強化」が挙げられているが、教育機関の実感として、セキュリティ教育は座学で終わることはほとんど不可能であり、無意味である。そのため、実習が必須だということは認識されており、例えば、文部科学省のプログラムである enＰｉＴも、実習を重視した実戦向きのものとなっている。

そのため、教育の場でのウイルスの検体そのもの、あるいは少なくとも最新のインシデント情報あるいはフォレンジック情報を用いた解析技術の実習等が必要になる。この点では、やはり米国が進んでおり、警察関係ではＮＣＦＴＡ、防衛関係ではディフェンス・インダストリアル・ベースという仕組みがあり法執行・防衛機関と産業界とが協調している。

我が国でも、逐次産官学連携の仕組みが導入されつつあり、警察の関係では警察庁の有識者懇談会における検討や、各都道府県警察レベルでの自主的な取組がある。防衛省関係では、サイバーディフェンス連絡協議会が設置されている。

産官学連携というと産官連携に注目がいきがちであるが、先ほど申し上げたように、実習のためには最新の情報が必要だという観点から、こうした取組において「学」も忘れないでいて欲しい。

○　まず我が国の治安に関する現下の情勢に触れたい。

我が国の今後のサイバーセキュリティ政策の決定において、2020 年に予定されるオリンピック・パラリンピック東京大会は極めて重要である。

第一に、治安に関する国民の意識に対し、オリンピックが安全に開催されることの影響は重大である。治安に対する国民の意識は、一時期治安が悪かった時期から変化し、「我が国にとって世界に誇るべき最大のよさ」とは何かという調査結果における第１位は、昨年の春から「治安のよさ」に戻った。その原因としては、犯罪の実数が減ったこともあるが、それだけではない。例えば、オウム真理教による事件のときには、犯罪全体の事件数は増えていないにも関わらず、国民の不安感は大きく高まった。一般に、一定のテロ等の発生は国民の不安感に最も大きく影響を与えることが、研究の結果判明している。

第二に、現在ソチで開催されている冬季オリンピック・パラリンピックについての各国のスタンスからも、また、我が国がオリンピックの招致に成功した理由の一つに間違いなく治安のよさがあることから考えても、オリンピックが安全に開催されることは、我が国に対し外国からも当然の前提として求められることとなる。

そのため、オリンピックにおける治安の確保のためには、国民全体の安全を守り、さらに世界に向けて日本が安全な国だと発信していくだけの基盤を築く必要がある。その基盤は、結局のところ我が国全体の国力であり、産業界が安全なものをつくり上げていくなどのウェイトが大きく、警察といった特定の機関だけの問題ではない。そして、オリンピックにおける治安の確保とサイバーセキュリティの確保は密接不可分であるとの認識に基づき、少なくとも 2020 年に向けてのサイバーセキュリティ対策を考えていかなければならない。

もう一つサイバーセキュリティ政策を考える上での重要な転機として、特定秘密の保護に関する法律が成立したことが挙げられる。現在でも厳しい論調はあるが、いずれ国民はこの法律の意義を理解し、この法律が我が国の安全を守る上でどのような意味があるかを理解できるようになるだろう。そして、その意味が理解されれば、この法律の意義を担保するため、情報を確かに守ることのできる人材と組織の必要性が理解されていくであろう。

以上の認識の下、情報セキュリティ人材の育成とＮＩＳＣの機能強化について、所見を述べる。

情報セキュリティ人材の育成について、本日の議論は従来よりも一歩前に進んだものであり、非常に高く評価する。この方針に基づき具体化を進めていく上では、情報セキュリティ大学院大学などが目指すべきトップレベルの人材育成と並行して、トップレベルとはいかないが、多様な背景を持つ人材の両方を育成することが重要であり、このような多層的な人材を育成していく方策が課題となる。現在、法学分野においてもサイバーセキュリティの講義をするなどの取組も進めているところであるが、さらにどのような人材を、どこでどのように育てていくか、という方策を検討しいかなければいけない段階に来ていると考える。

その上で、最も重要なところがＮＩＳＣの機能強化である。ずっとこの会議に参画しているが、内閣の中で、こんなに横断的な組織で、にもかかわらずこんなにうまくいっ

ているものはない。各省庁せめぎ合いや利害調整があり、しかしなおその枠を超えて、内閣として一つにまとまって動く基盤ができている。国全体でサイバーの脅威に対応するために、各省庁の力量が高くなることは当然であるが、同時にＮＩＳＣの総合調整の権限のもとに、事案対処省庁、情報セキュリティ関係省庁の機能が最大限発揮される制度をつくっていく必要がある。その一歩として、今年の春から夏にかけての期間が非常に大事な時期となる。

そして、そのときの視点として、重大なインシデントが発生した際、原因の究明と再発の防止のために行われる調査活動と、攻撃者、すなわち被疑者を特定し、検挙して脅威を根源から断つために行われる捜査活動との整合性をどうしていくかが、１つの大きなポイントになってくるであろう。原因究明・再発防止のための調査活動をＮＩＳＣが中心となって広く行うことは当然であり、対処官庁等による捜査活動との調整が非常に重要となる。

その上で、特定秘密保護法、人材の育成、ＮＩＳＣの機能強化全ての結論として、政府部内における人材の確保と育成の重要性について述べる。ＮＩＳＣの機能強化を行う上では、当然人員増を伴わなければならない。そして、ＮＩＳＣの職員が安全保障にかかわる非常に重要な情報を取り扱う上で、その職員が民間から任期付職員の形で出向となることは、国家の安全保障の基盤に穴を空けてしまうおそれがあり、非常に問題がある。したがって、政府機関においても人材の確保と育成は必須であり、きちんと遂行しなければならない。

○　情報セキュリティ普及啓発ロゴマークを見ると、「知る・守る・続ける」と書かれている。人材育成では、「ワクワクする」という気持ちが大事である。「守る」、「続ける」というと、何となく「頑張らなくては」という気持ちになるけれども、この「知る」というのは楽しいことだと思う。

ところで、最近多くの産業分野で、新しくＩＴというものを「知らなければいけない」事情が生じた。これは、今回、ＩＴ総合戦略本部における議論を通じて「世界最先端ＩＴ国家創造宣」を閣議決定したことを受け、医療、農業といったいろいろな分野で新たにＩＴ化を進めるところが現れているためである。この具体的なＩＴ化を進めることは大変重要である。例えば、もともと最近の農業機械は、作物を刈り入れたときに、水分含有量など作物の品質情報等がその場でわかるようになっている。そこで、もしこの作物の情報がネットワークにつながっていれば、農業は産業として大きく生まれ変わる可能性がある。

このように農業のＩＴ化が起こると、農地の中のあらゆるところにセンサーがあって、育てている農作物等に関するデータが生まれてくるといった状況が生まれる。そして、こうした新たにＩＴ化された局面においては、これまでのセキュリティとはまったく別の守備範囲が出てくる。したがって、ＮＩＳＣはこうしたＩＴ化の新しい展開と今後の展望を「知る」ための体制を持たなければならない。

今、例として農業を挙げたが、医療も同じである。医療分野では電子カルテがあるが、この電子カルテの情報がそのほかのいろいろな個人の情報と一緒になると、これら個人の情報を守るためのセキュリティは大変重要となる。この、ＩＴ化の新たな展開と今後

の展望という要素をＮＩＳＣに入れていくことは、人材育成の面でも、国の使命という面としても大変重大である。

また、ＩＴ技術の進展は日進月歩である。先週、ＣＥＳという展示会が米国で開催された。そこで、インテルがデジカメに入っているメモリ１つがフルＰＣとなっている商品を発表した。すなわち、ネットワークとブルートゥースに接続し、ＣＰＵを持つ電子計算機として機能する製品がデジカメのメモリのサイズで生まれたわけで、この機器は以降どんな「もの」にも入ってくることとなるだろう。こうなったときに情報セキュリティをどうするかを考えるには、ＩＴ化の展開と展望を持った体制が必要である。

次に、2020 年オリンピック・パラリンピック東京大会について、1996 年のアトランタオリンピックと 1998 年の長野オリンピックにおける情報システムの構築をＩＢＭと一緒に行った経験に基づき、コメントしたい。オリンピックの情報システムの構築では、調達としてスポンサー制が採られている。1964 年の東京オリンピックのときは、会場の至るところに我が国の会社の名前が書いてあったことを思い出して欲しい。ところが、情報システム構築についてはフルスポンサーでエクスクルーシブであるため、１社が占めると別の会社は一切参入することができない。したがって、システムも構築できないし、ロゴも出せないことになる。そこで、今度のオリンピックではどの会社がスポンサーとなるかが問題となる。オリンピックの開催地と、そこで作業を担当する企業の国籍とは別のロジックで定まるものであるので、スポンサーとして海外の会社が入る可能性は十分ある。それでは、この状況に対してどういうセキュリティ対策を行うか。

さらに将来の災害対策の基盤はオリンピックの際に構築可能である。そこで、オリンピックの対策チームの一環として、ＩＴの観点から何をするべきかを検討する場についてＩＴ戦略本部と連携して情報セキュリティ政策会議として設けるのはいかがだろうか。オリンピックの開催においては、情報だけ見ても、しなければならない対策は大変多く、それをきちんと取りまとめることが望ましいと考える。そして、東京オリンピックを守るためには、オリンピックのスポンサーで情報システム関係を構築・運用することになる民間の方と連携して進めるしかないのであるから、そういう体制をつくることをお願いしたい。

○　２点申し上げる。

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３次行動計画（案）」についてである。サイバーテロの脅威が現実のものとなる中、この行動計画は極めて重要である。

私は、これまで、警察に対し、高度化・深刻化するサイバーテロに対処していくことができるよう、民間の知見の積極的な活用、セキュリティコンテストへの警察職員の参加、重要インフラ事業者との共同訓練などを通じ、人材育成の観点から、その専門的能力を高めるよう、強く督励をしてきたところである。

現在、こうした取り組みの成果が徐々にあらわれてきているところであるが、引き続き、６年後の東京オリンピック・パラリンピックにおけるサイバーテロ対策も視野に入れ、重要インフラ防護について、その役割を果たしていくよう、警察庁を督励してまいる。

２点目は、ＮＩＳＣの機能強化についてである。

現下のサイバー脅威の高度化・深刻化に対応するためには、ＮＩＳＣの機能強化は重要な課題である。今後、具体的な検討を進める際には、機能が強化されたＮＩＳＣが各政府機関と有機的に連携して、国全体のサイバーセキュリティを強化するものとする必要があると考えている。

警察は、事案対処を担う機関として、サイバー攻撃の捜査に当たっているが、今回のＮＩＳＣの機能の強化が、警察による捜査と調和をして、国全体としてサイバー攻撃への対処能力を向上させるものとなる必要があると考えている。その検討に積極的に貢献できるよう、警察庁を督励してまいる。

○　昨年末策定された国家安全保障戦略において、サイバーセキュリティの強化が打ち出された。外務省としても、同戦略に基づき、サイバー分野での国際連携を図るとともに、省内におけるサイバー防護・対応能力の強化に努めている。

国際連携としては、昨年10月、サイバー空間に関するソウル会議に三ツ矢外務副大臣を長とする政府代表団を派遣して、日本の取り組みを紹介した。また、12月の日・ＡＳＥＡＮ特別首脳会議においては、新たに日・ＡＳＥＡＮサイバー犯罪対策対話を開催することを始め、サイバーセキュリティ分野における協力強化に合意した。

本年の取組としては、二国間では、日米サイバー対話第２回会合、日露サイバー安全保障協議の立上げ等を通じて関係国との連携を強化してまいる。多国間でも、国連やＡＳＥＡＮ地域フォーラム（ＡＲＦ）などにおける議論に参画していく。本年も、サイバー空間における国際的なルールづくりに積極的に参画してまいる考えである。

サイバー攻撃対策としては、現在、外務省では来年度予算でのインシデント対応チームの発足に向けた準備を進めている。外務省としても、ＮＩＳＣとの連携のさらなる強化を図りつつ、情報セキュリティ対策のための人材育成等においては関係府省庁の御協力を得つつ、推進していく考えである。

○　情報セキュリティの確保は、ＩＴの利活用を進めるＩＴ政策の推進に当たって不可欠な要素である。そのため、ＩＴ政策担当大臣が中心となって、ＩＴ利活用セキュリティ総合戦略推進部会を主宰し、専門家の横断的議論と相互理解を深め、官民関係の連携を強化することとしたところである。

また、人材育成も喫緊の課題であり、昨年末の第63回ＩＴ総合戦略本部においては、高度なＩＴ人材創出等に取り組むための「創造的ＩＴ人材育成方針」が決定されているところであり、「情報セキュリティ人材育成プログラム」と双方向で連携し、効果的な展開を図ってまいりたいと思っている。

こうした観点から、引き続き、情報セキュリティを確保したＩＴの利活用を積極的に推進してまいりたい。

○　サイバーセキュリティはＩＣＴの基盤であり、重要な課題である。特に、サイバーセキュリティを支える人材の育成は、サイバー攻撃防御の要であり、政府全体で全力を挙げて取り組んでいくことが必要である。

具体的には、標的型攻撃など新たなサイバー攻撃からの防御が可能となるよう、一組織のネットワーク管理者の対応能力の向上が必要である。

このため、総務省では、昨年９月から職員数千人規模の組織内ネットワークを模擬した、ネットワーク管理者参加型のサイバー演習 CYDER（サイダー）を実施したところである。このようなネットワークを用いた演習は、日本初であり、これまで、官公庁や大企業などから多くのご参加をいただいているところである。

一方、本演習への参加状況を踏まえると、省庁によって、未だに情報セキュリティに対する意識に温度差があるように感じられたところである。政府全体の取りまとめ役であるＮＩＳＣにおかれては、引き続き、各省庁への情報セキュリティ対策の働きかけなどをお願いしたい。

また、人材育成という目標の達成に向けては、一度限りの演習では足りず、参加経験から得られた知識・技術をいかに定着させていくか、ということが課題と認識している。

このため、今後は、サイバー演習への参加者に対して、反復的にフォローアップを行うなど、習得した知識・技術の維持・向上を図る仕組みについて検討していきたいと考えている。

総務省としては、このような人材育成を通じて、我が国の情報セキュリティ水準の向上に貢献してまいりたいと考えている。

○　先ほど御説明があった、サイバーセキュリティ戦略に基づいた、重要インフラの対策強化、人材育成、普及・啓発等の取組みは非常に重要なものである。2020 年の東京五輪を視野に入れると、社会インフラを含めたセキュリティ対策はますます重要になっていく。

経済産業省としても、当省の独法でありますＩＰＡ（情報処理推進機構）などの専門家集団を活かして、しっかりと取り組んでいく所存である。

また、ＩＰＡがハブとなり、電力・ガス等の重要インフラ５業界で標的型攻撃に対する情報を共有している「Ｊ－ＣＳＩＰ」、この取り組みについては、他の重要インフラ分野との情報の共有も含めて充実、強化をしていく。また、今回、重要インフラ分野に追加となった石油、化学、クレジット分野についても、業を所管する立場からもしっかりと対応してまいりたい。

また、来年度はＩＰＡの予算を増額し、セキュリティ対策の体制についても倍増していく予定である。巧妙化するサイバー攻撃に対処するため、サイバーレスキューチームを設置し、重要インフラ等を始め産業界の防御能力を強化する。

なお、２月は情報セキュリティ月間ということで、２月 19 日にロンドンオリンピック時の英国のセキュリティ責任者を招致し、国際シンポジウムを開催する予定である。東京五輪を盛り上げていこうという企業の方々を始め、多くの方々の参加を期待している。

○　自衛隊の任務遂行上、サイバー空間の安定的な利用は当然不可欠であると認識しており、来年度予算案としても、サイバー攻撃対処に関連した事業で約 205 億円を計上している。とりわけ米国との協力は極めて重要だと位置づけている。

既に昨年の２月から約１年間かけて、副大臣を委員長とした「サイバー政策検討委員

会」を設置して、人材の育成、確保を対話の中からしっかりとやっており、また、防衛産業、各装備品のメーカーなどともこういった課題について検討をした結果、本年３月に「サイバー防衛隊」という１つの組織を新設することが決定している。

また、自衛隊のサイバー攻撃対処能力の強化に向けて、これからも積極的に取り組んでまいる所存である。

⑶　議場締め括り挨拶

本日は、限られた時間であるが、さまざまな観点からの有意義な御意見をいただき、本当にありがとうございました。

その中で、特にＮＩＳＣの機能強化については、サイバー空間の防護及びサイバー攻撃への対応能力の一層の強化を図る上で極めて重要であるということである。

関係省庁においても、その趣旨にのっとって、議論に参画し、前向きな結果が得られるよう、御協力をいただきたい。

また、有識者の構成員の皆様におかれては、どうぞ今後とも忌憚のない率直な意見をお聞かせいただきますようお願いする。

本日は、ありがとうございました。

－　以上　－