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39回会合　議事要旨

１　日時

平成26年５月19日（月）　８：45～９：30

２　場所

総理大臣官邸４階大会議室

３　出席者（敬称略）

安倍　晋三	内閣総理大臣
菅　義偉	内閣官房長官
山本　一太	情報通信技術（ＩＴ）政策担当大臣
古屋　圭司	国家公安委員会委員長
新藤　義孝	総務大臣
小野寺 五典	防衛大臣
石原　宏高	外務大臣政務官
磯﨑　仁彦	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
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

４　議事概要

(1)　総理大臣冒頭挨拶

大変お忙しい中お集まりいただき、感謝申し上げる。

サイバー空間における脅威が一層深刻化している中、サイバーセキュリティの確保は、国家の安全保障・危機管理の観点から極めて重要な課題である。同時に、政権が掲げる成長戦略の重要な柱である、世界最高水準のＩＴ社会の実現のためには、サイバーセキュリティは必要不可欠な基盤と言える。さらに、2020 年のオリンピック・パラリンピック東京大会に関し、サイバーセキュリティについても万全の態勢で臨むことは、我が国の重要な責務である。

周到に準備をするためには時間を要する。６年前の今から本腰を入れて、強力に取り組んでいかなければならない。

こうした状況のもと、本日御議論いただく事項はいずれも重要かつ喫緊の課題である。

内閣では、世界を率先する、強靭で、活力あるサイバー空間の構築に向け、サイバーセキュリティ政策を今まで以上に加速してまいる。政治のリーダーシップのもと、皆様や与党の議論を踏まえ、法制の検討を含め、サイバーセキュリティについての政府の機能を強化し、これまで以上に積極的に取り組んでまいる。

構成員の皆様方におかれましても、どうか活発な御議論をいただきますように、よろしくお願い申し上げる。

(2)　討議

【討議事項】

・　「我が国のサイバーセキュリティ推進体制の機能強化（素案）」について

【決定事項】

・　「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）」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）」について
・　「新・情報セキュリティ人材育成プログラム（案）」について
・　「サイバーセキュリティ 2014（案）」（パブリック・コメント案）について

【報告】

・　「情報セキュリティ研究開発戦略（改定版）（案）」の検討状況について
・　「情報セキュリティ普及・啓発プログラム」の改定の方向性について
・　政府の情報セキュリティに関する予算について
・　全府省庁等の参加による大規模な政府サイバー攻撃対処訓練【３・１８（サイバー）訓練】について
・　日・ＡＳＥＡＮ情報セキュリティ意識啓発アニメーションの制作について

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。

○　人材育成及びサプライチェーン・リスクへの対応に関連し、ソフトウェアに関する産業統計の整備の必要性について述べる。

人材育成における課題は、需要サイドと供給サイドの間の循環がうまくいっているの

だろうか、という点にある。特に、人材が国内でどれだけ雇用されているのか、実はわからないということは問題である。

資料４の「人材の量的・質的不足」において、セキュリティ人材が量的にも８万人不足していることが挙げられている。大学の先生方とお話しする機会があると、大学側としては供給することについては恐らく可能である、ただ、その人材をきちんと産業界が引き受けてくれるのかが問題である、と盛んに言われる。

例えば、自動車産業であれば国内生産台数や、生産に携わる国内・海外の人数がはっきりしている。ところが、様々なデータを見ても、ソフトウェア関係についてはそういう資料がほとんど見当たらない。統計上、ソフトウェアについてはサービス産業にくくられており、サービス等の輸出の中に含まれているようであるが、そのうちのソフトウェア部分がはっきりしない。これは大変大きな問題であり、総務省、経済産業省にも話をしているが、何とかこういうソフトウェアに関する産業統計をとる必要があると考えている。

ソフトウェア産業の労働力に関する国内外の統計は、資料２にある政府機関等におけるサプライチェーン・リスクへの対応、すなわち、「情報システムの構築等の外部委託の際、委託先における不正機能の混入防止のため、厳正な管理を要求」という点に関連する。現在、国の基幹システムの調達において、その整備・開発・運用等の一部分が我が国の外に出ているのは間違いない。元請は我が国の日本企業であり、問題ないとしても、その先でどこの国に業務委託しているか、よくわからないという状況は、非常に危険である。

したがって、産業全体としてのソフトウェア産業の輸出入や産業構造を明確にしていく必要があると考えているので、よろしくお願いしたい。

また、我が国のサイバーセキュリティ推進体制の機能強化に関連し、現在ＮＩＳＣで行っている政府機関情報システム横断監視等の現業を大事にして欲しい、ということについて述べる。

資料１では、サイバーセキュリティ政策会議の下に内閣サイバーセキュリティ官及び同官室となっており、現在の業務がどうなるか、この資料からでは明確ではない。ＮＩＳＣのようにまさしくセキュリティそのものを監視している機能と同時に、政策を決定し、方針を出すところがないと、どうしても頭でっかちの議論になりかねない。ぜひ、ＮＩＳＣがきっちりと国のセキュリティを常に見ているということを明確にしていただきたい。

○　５点申し上げる。

第一に、第３次行動計画において、中小企業に遵守を呼びかけたこと、また、重要インフラの分野を拡大したことは、情報セキュリティ対策として重要な進展である。情報セキュリティ対策は、人員や経費の面で中小企業にとっては少なからぬ負担となると思われるが、単なる法令遵守、コンプライアンスを超えて、企業の社会的責任、ＣＳＲの一部にもなりつつあるという意識を持って取り組んでいただきたい。

また、化学、クレジット、石油の各分野が今回、重要インフラ分野に追加されることになったが、これで十分か、さらに追加すべき分野があるかもしれない。

第二に、人材育成について、国内のみならず、海外からも優秀で善良な人材を獲得すること自体は望ましい。その観点から、今回、グローバル水準の人材について言及がなされたことは評価できる。その上で、海外人材については、当該人材の母国の政治的、経済的状況にも十分配慮した上で決定すべきである。例えば、安全保障輸出管理の場合と同様に、ＯＥＣＤ諸国からの人材と、それ以外の諸国からの人材との間で異なる判断をすること自体には合理性があると考えられる。

また、情報セキュリティマネジメント試験を実施して国家資格を付与するというアイデアが報道されていりが、試験好き、資格好きという勤勉な日本人の性格ともフィットして、よいインセンティブとなり、人材の増加に貢献するよいアイデアと思われる。

第三に、統一基準群におけるサプライチェーン・リスクへの対策として、官庁の情報システム構築の外部委託において、部品組み立て、ソフト、下請、インストールが多国籍でなされる場合、マルウェアなどに対して脆弱になりかねないため、厳格な管理要件を課すという今回の改定は、一般競争入札の原則を維持した上での現時点における最善の対策だと考える。

なお、万一、こういう管理要件の厳格化でも不測の事態が生じる場合がもしあれば、特に安全保障に直結する府省庁のものについては、安全保障を理由として指名競争入札とすることも考えられる。

第四に、ＡＳＥＡＮとのサイバー総合連絡体制の構築について報道があったが、被害状況の情報を共有し、ＮＩＳＣとホットラインを結んで迅速に対応し、被害の拡大を防止することは、我が国自身のサイバーセキュリティに資するのみならず、サイバー分野での国際貢献ともなる、非常に評価できる政策である。また、ＡＳＥＡＮ諸国とのサイバー以外でもポジティブな効果をもたらすだろう。

最後に、安全保障会議と情報セキュリティ政策会議の連携の強化、緊密化は、非常に重要であり、評価できる。万一国外からのサイバー攻撃が発生した場合の国際法上及び国内法上の対応、特に対抗措置をどうするかについては、今後詰めていく必要がある。

○　２点申し上げる。

第一に、政府、自治体のクラウド化に関するセキュリティ対策について。

「世界最先端ＩＴ国家創造宣言では、国・地方の情報システムについてクラウドを徹底活用するということをうたっており、2021 年度をめどに原則全ての情報システムをクラウド化するということを打ち出している。

一方、「サイバーセキュリティ 2014」中には「政府機関におけるクラウドコンピューティングのセキュリティ対策の強化」を掲げているが、その内容は政府共通プラットフォームにおけるセキュリティ対策が主になっている。しかし、クラウド化の推進には民間のパブリッククラウドの利用も必要であり、その利用環境の整備も必要であると考えている。

現状では、各省庁、自治体が個別に民間のクラウド事業者のセキュリティ対策を評価し、その中から各自が良いと判断するものを選択するという仕組みになっている。その形態では効率が悪いと思われるため、米国や英国等でも行われているように、パブリッククラウドの認定プログラムを構築し、既に認証を得た事業者の中から各自治体や府省

が選択する方式の必要性についても検討されたい。

第二に、研究開発戦略に関連し、事業化の支援策をさらに検討する必要性について。知られているとおり、米国の研究開発（Ｒ＆Ｄ）予算は、国防高等研究計画局（ＤＡＲＰＡ）の予算が大きな割合を占めており、イノベーションやベンチャービジネスの創出に軍事技術の民間転用が重要な役割を果たしている。

また、イスラエルに行き、ＩＴベンチャーの支援環境について意見交換をしてきたが、イスラエルでは、優秀な若者が兵役中にサイバーディフェンスの研究を担うとのことである。その部隊に在籍したというだけで、周囲から羨望の的になることから、サイバーディフェンスに優秀な人材が集まる素地となっている。さらに、起業のごく初期、スタートアップに対する支援環境が整っており、官民でベンチャーキャピタルが林立しているため、兵役終了後に彼らがサイバーディフェンスに加え、ハイテクベンチャーとして成功するという例も輩出されている。

一方、我が国では、Ｒ＆Ｄを研究機関における「研究」というイメージで捉えており、結果的に「開発」の要素が非常に弱いと考える。研究開発戦略でも、「研究成果の社会還元の推進」を掲げ、と「事業化等に向けて研究者等を支援するための環境整備」を挙げているが、今後は研究、技術開発だけではなく、そこから新たな成長産業が生まれるような事業化の支援策をさらに検討する必要がある。

○　２点述べる。

第一に、我が国のサイバーセキュリティ推進体制の機能強化のキックオフに当たり、何をするかについて。今回の改革の方向性は、まさに時宜にかなったものであり、賛成である。そこで、折角機能強化を図り、しかも官の公益的貢献が従来以上に期待されているのであれば、本組織の第２のスタートにふさわしい新機軸があると、一般にも理解されやすい。

そこで、2020 年のオリンピックに備える時期でもあることから、各政府機関の情報システムの脆弱性の総点検を再度実施し、民間にも範を垂れることを検討するべきである。そして、その過程や結果を踏まえて、政府全体の果たすべき役割について検討することが、我が国全体としての施策の検討の上で大変重要であると考える。

第二に、サイバー空間の脅威に対する防御側における官民協調の在り方について。サイバー関連の事象はなかなか線引きができないという特徴がある。例えば、サイバーインシデント、サイバー犯罪、サイバー攻撃、さらにサイバー戦争まで、一貫して視野に入れた対策を講じないと、サイバー空間の安全を維持することは難しい。

しかも、一般的に、サイバー空間では攻撃側と防御側に著しい非対称がある。すなわち、攻撃する側は匿名性を悪用し、一点突破しただけでも成功との立場にあり、法律に触れることに躊躇せず、多数の仲間を動員して人海戦術を採用し、緩やかな形で国際的に連携しているという状況にある。これに対して、防御側は相手を特定することが困難で、一点でも突破されれば非難される立場にあり、法律を遵守しながら防御せざるを得ず、対策要員と能力が限られており、縦割りの組織で対応するしかない。

そこで、防御側における官民協調がより期待されることになる。しかも、個々の組織が対応するだけでは不十分であり、組織を横断した対応が求められるが、これは私たち

がまだ経験したことがない分野である。

連携上の問題は、インシデント情報など民間の事件、事故情報も含めて、それらを共有し、対策に生かすプロセスであり、民の側から自主的に協力してもらえるかどうかが大事である。民間企業にももう少し国家的な視点を持ってほしいところであるが、他方で、利潤動機で動いている以上、コストと時間に敏感なのはやむを得ない面もある。

そこで、従来どおり、民間主体の原則は堅持する以上、情報を提供する側にも何らかのメリットを提供することが大切である。多くの会社等から提供された情報の分析結果を提供者にフィードバックすることはもとより、ワンストップサービスで共通窓口１カ所に届け出れば、二度手間三度手間が避けられるような工夫も検討されたい。

○　法律の観点から述べる。

現在、国民の最大の誇りは、我が国の治安のよさである。サイバーセキュリティに関して言えば、「何か事態が発生したら、国が適切に対応してくれる」という国民の安心感を裏切ってはならない、そこがポイントになる。その観点から、今回の基本法制定は非常に時宜にかなったものである。

国民が求めているのは、実際に脅威に直面したとき、国が対応する能力を持っているということである。そのためには、防衛省・警察庁を中心とした対処官庁に加え、ＮＩＳＣを中心とし、内閣全体が情報を共有し、連携しなければならない。

特に、防衛・捜査といった特定の機関でしか実行できない対処もあれば、基本法の下であればＮＩＳＣが広く行うことのできるようになる調査もあるところ、我が国のサイバーセキュリティの進歩のためには、それらの間で情報が共有され、連携することが必要である。

そして、その前提として、ＮＩＳＣの強化を通じ、国を支える人材をＮＩＳＣで育てて欲しい。情報分析官をＮＩＳＣに配置するということは非常に良いことであり、いかに優秀な人材をそろえて、分析官の力量を確保するかが重要となる。

また、重要インフラにおける情報セキュリティ対策に際し、オリンピック・パラリンピック東京大会開催は絶対のポイントである。ロンドン大会の教訓についても勉強する機会があったが、ロンドン大会でも開会式に際し、電源システムに対するサイバー攻撃があった。そういう経験を踏まえれば、６年後というのはそんなに先ではない。ＮＩＳＣを中心とし、重要インフラと各官庁との連携を始めなければいけない。英国の事例以外では、いろいろ言われている国もあるが、我が国の官民連携は世界一であり、それを示すためにも、ぜひ東京大会開催を通じて実績をつくっていただきたい。

○　私はグローバル情報社会において、今回の政策がどういう意味を持っているかという観点で、３点申し上げたい。

第一に、マルチステークホルダー体制の整備と、サイバーセキュリティに関する我が国の窓口が一つに定まることの意義について。機能強化に向けた方針中、最も重要な点は、「国の主導的役割を定め、各ステークホルダーの相互連携によるサイバー空間の防護が必要」という箇所である。これは、マルチステークホルダーがそれぞれの明確に定められた役割を果たし、その体制に国が責任を持つということである。その上で、サイ

バーセキュリティ会議が、ＮＳＣとＩＴ戦略本部の間で緊密に連携するという体制は、世界の中でも大変珍しい、先導的なアプローチだと考える。実際、米国を含むどの国でも、サイバーセキュリティをどの省庁が、どこが担当するかは難しいし、外から見ても分かりにくい。ところが、今後サイバーセキュリティ政策会議が整備されれば、外から見ても我が国のサイバーセキュリティを代表する窓口が一つに定まることになる。このコンセプトは、とても重要なステップである。

第二に、我が国が新たにＩＴ化する分野において、課題をいち早く解決し、世界で先導的な立場を確立する重要性について。かつて、我が国は国語を守る観点から、世界を先導して電子メールの多言語化を主張し、その方式を提案したことがある。その時から多国語化は日本に聞けと言われた。「世界最先端ＩＴ国家創造宣言」の評価が高いのは、全ての分野がＩＴによって変化することを宣言しているためである。例えば今、農業における米作機械で、稲を刈り取った瞬間に、米のたんぱく質含有率を測ることができる機械を持っているのは我が国だけであり、世界の中で、農業のＩＴ化を先導している。たとえばこのように情報セキュリティのいろいろな分野での新しい課題が出て来るであろうし、我が国がその課題を解決していけば、いずれ世界がそういう新しい課題に直面した時に、日本に聞け、日本に任せろ、日本人を呼んで来い、と日本を頼りにするようになる。外から見て頼りにされる情報セキュリティにしたい。

第三に、「情報」に関する教育について。先日、全国の高校生を対象に、1 から 10 までの整数全てを足し算するというようなプログラムを書かせる試験を実施したところ、正解率が 10%程度であった。これは非常に問題のある実態である。情報リテラシーと同様に、これからのビッグデータ時代の統計分析を支える人材を育成する上で、技術としての数学や統計、プログラミングの力を小学校、中学校、高校で全ての生徒に植え付ける必要がある。私たちも教育に携わる者として、この問題には引き続き取り組んでいくが、思い切った改革が必要であり、政府にもぜひそのことを意識しておいて欲しい。

○　サイバーセキュリティの推進体制の機能強化は、オリンピック・パラリンピック東京大会開催の観点からも極めて重要。オリンピックという大きな事業をするときには、幾つかの機関が一緒になって防護し、サイバーセキュリティを確保する必要がある。まずは、ＮＩＳＣを中心とした推進体制の機能強化を図って、我が国の基盤を形成し、この基盤をしっかりと本物にしていくことが重要である。

また、推進体制については、リアルタイム性とダイナミクス性をいかに組織の機能に入れ込んでいくかが重要である。事案が起きたとき、中心となるＮＩＳＣがしっかりと情報を収集・分析し、対策の方向感について全ての関係機関及び民間と共有する。このプロセスがリアルタイム且つダイナミックに行われることが必要。その機能に関する検討については、今後とも是非参画していきたい。

次に、サイバーセキュリティを始めとしたソフトウェア人材全般の育成について述べたい。今後、IOT も含め、産業界においては、サイバー空間から価値を取り出すことが大きなポイントになる。さらに、全てのインフラにおいて、いわゆるＳＤＸ（Software Defined X）、全てのインフラがインターネットとつながりさらには、それらが生成するデータを基盤とし、ソフトウェアが自律的に判断をしてインフラを動かしていくという

形になる。そのような社会では、ソフトウェアを中心としたインフラ、ソフトウェアで何らかのサービスをつくっていくインフラというものが求められる。その観点からも、ソフトウェアの人材は、サイバー空間を守るだけではなく、全ての社会機能を動かしていくための人材として、今後非常に多く必要となってくる。

そこで、できれば中央のみではなく、地方の産業界を活性化する上でも、ソフトウェア人材を育てる大学または機関を地方に設けて欲しい。その結果、人材をそこに集め、かつ、そこで雇用を生み出すこともできるようになる。例えば、沖縄にはクラウドデータセンターを集積する動きがあるし、北海道でも可能。また、会津大学では非常に優れたソフトウェアの研究、授業を行っていると聞いている。地方の活性化等を含めたソフトウェア人材の育成には大きな可能性があると思われ、是非そのような検討も今後していただきたい。

最後に、研究開発についてであるが、現在我が国で使われているセキュリティ関係のソフトウェアは、国産よりも海外製のほうが多い。我が国を守るという観点からは、国産のソフトウェアによりセキュリティを構築していくことが非常に重要であり、我が国発のソフトウェア開発を推進していく上で、是非象徴的なものを何らか打ち出し、社会の方向感を創り出すことを検討いただきたい。それにより、ソフトウェア人材も自然に育ち、目指す人も増えていくようになると考える。

○　先日、米国出張に行き、サイバーセキュリティ関係者、国防総省、ＤＨＳ、ＮＳＣその他の方々との意見交換を通じ、日本におけるサイバーセキュリティの推進体制の機能強化の重要性を改めて認識した。サイバーセキュリティ基本法の話やＮＩＳＣの機能強化の話題もありましたけれども、ぜひその方向で取り組みを進めていただきたい。

さらに、我が国が世界最高水準のＩＴ利活用社会を目指すには、ＩＴを安心安全かつ便利に利用できることが不可欠である。

本年２月から、ＩＴ政策担当大臣であり、本会議の議長代理である私が主催で、ＩＴ利活用セキュリティ総合戦略推進部会を開催している。これまで、ＩＴ利活用とサイバーセキュリティに関する技術開発、人材育成などのさまざまな課題について、横串を通して、専門家の方々と議論を行ってきた。

今後も、当該部会で活発な議論を行い、本年７月を目途にＩＴ利活用とセキュリティの両面から、また、産業競争力強化にどう結びつけていくかということをしっかりとフォーカスしながら、政策を総合的に取りまとめ、本会議に提言いたしたい。

こうした観点等から、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。

○　２点申し上げる。

１点目、我が国のサイバーセキュリティ推進体制の機能強化については、極めて重要な課題であると認識している。特に原因究明に関する機能については、これが警察による捜査と連携、調和したものとなるとともに、警察との情報共有等を通じて、国全体のサイバーセキュリティ対策を強化することにつながるようにする必要があると考えている。

今後、オリンピックの開催も見据えつつ、我が国のサイバーセキュリティ推進体制の機能強化に貢献できるよう、警察庁を強く指導してまいる。

２点目、重要インフラの情報セキュリティ対策に係る第３次行動計画の決定について、サイバー攻撃の手口が巧妙化、多様化するなど、サイバー空間における脅威が深刻化している中、この計画に掲げられた取り組みを着実に進めることが極めて重要と認識している。

警察が、今回追加された新たな重要インフラ分野とも連携強化をして、情報共有や共同対処訓練などを行うなどして、本行動計画の施策を着実に推進していけるよう、警察を指導してまいる。

○　参考資料１を御覧いただきたい。総務省では、東京オリンピック・パラリンピックを見据え、サイバーセキュリティの推進体制の強化も含めた五輪の推進本部を立ち上げている。

今後、我が国のサイバーセキュリティ推進体制を強化するに当たり、言わずもがなのことであるが、先端的、実用的な研究開発をより意識して強化すべきだと考える。

また、既に一部実施を始めているが、政府や企業を対象としたサイバー攻撃に対する組織的な実践演習や、個人の自発的な対応を促すような仕組みの構築を推進していかなくてはならない。

あわせて、多国間、二国間の連携を強化することが必要であり、我が国とＡＳＥＡＮとの間でサイバーセキュリティに関する閣僚政策会議を開催し、そういったネットワークをつくり始めているところである。

ＩＣＴの推進に必要なのは、利活用と情報セキュリティを両輪としてうまく連携させること、それを意識しながら進めていくことである。具体的な戦略の実践と、それをいかにスピード感を持ってやっていくかが重要であり、さまざまな提言がなされているが、いかにサイバーセキュリティを強化して実効性を上げるかということをぜひやっていきたい。

その意味において、今回、情報セキュリティ政策会議とＮＩＳＣを法的に位置づけることが重要であって、司令塔機能の強化をしなければいけない。

また、各省にはＣＳＩＲＴという組織がある。そもそも全省になかったのを全省で整備したが、実際に本当に動いているのかという部分がある。そういうまさに実践の部分をしっかりとやっていかなければいけない。

御指摘いただいたソフトウェアに関する産業統計の整備、自治体クラウドの課題、さらにはプログラミング教育や人材育成について、総務省の中でも位置づけてやっていきたい。

○　防衛省では、サイバー空間における常続監視態勢を構築することが大変重要だと考えている。その上で、早急に取り組まなければいけない課題について、３点申し上げる。

第一に、安全保障分野におけるシステムの開発については、今後とも海外からの関与については本体だけではなく、下請、孫請までしっかりチェックをする必要がある。

第二に、サイバー攻撃の分野におけるグレーゾーンの問題である。安全保障の中でグレーゾーンの議論はされているが、一体どこまでが警察権の対応なのか、どこから先が

武力攻撃と判断されるのかということは、まだ国際的にも基準は定まっていない。先般、防衛大臣当局で日米で合意をいたしましたこの協力の中で、米国とともにこの分野についての考え方の構築をすることが大切だと考えている。

第三に、人材の育成について、本年３月に大臣直轄の部隊としてサイバー防衛隊をつくったところであるが、人材の育成は、防衛省としても大変重要な課題である。今後も新しい人材を採用してまいるが、既存の人材の能力構築と、新しい人材を防衛省内でも発掘する中で、例えば本年２月には総務省とＮＩＣＴの協力を得て、大規模エミュレーション環境のスターベッドを活用し、事態対処の腕を複数のチームで競う実践的なサイバー防御演習を行った。今後も、隊員の技術の向上と新たな人材の発掘を、防衛省内でもしっかりやっていくことが重要である　今後とも、御協力をよろしくお願いしたい。

○　外務省としては、昨年情報セキュリティ政策会議で決定された「サイバーセキュリティ2013」及び「サイバーセキュリティ国際連携取組方針」に従い、サイバー分野での国際連携や能力構築支援を推進しているところである。

安全保障分野では、国連サイバー政府専門家会合（ＧＧＥ）の参加国として、国際的なルールづくりなどの議論に積極的に寄与している。

また、二国間協議も進展しており、先月、第２回日米サイバー対話を行い、サイバーに関する幅広い日米協力について議論を行った。ほかにもエストニア、豪州、ＥＵ、仏との間でサイバー協議の立ち上げに新たに合意した。こうした枠組みを通じ、協力体制の構築に向けた議論を深めていく。

サイバー犯罪分野では、昨年 12 月の日・ＡＳＥＡＮ特別首脳会議での合意を受け、今月末に日・ＡＳＥＡＮサイバー犯罪対策対話を立ち上げる予定であり、警察庁及び法務省と連携して対応していく。

また、政府開発援助（ＯＤＡ）のさらなる積極的、戦略的活用も含め、サイバー空間における法の支配の実現、強化の観点から、開発途上国の能力構築に一層寄与するための取り組みを積極的に進めていく考えである。各省庁からの支援をお願いしたい。

本日の会議では、サイバーセキュリティ推進体制の機能強化について議論が行われたが、中でも政府の司令塔としてのＮＩＳＣの体制強化は重要かつ喫緊の課題と考える。現在、与党内で検討中と承知しているサイバーセキュリティ基本法案に向けた動きと連携して進めていくことが重要であり、外務省としても、引き続き議論に積極的に参画していく考えである。

○　成長戦略において、ＩＴの利活用は非常に大きな柱の１つとして位置づけられているが、その大前提はセキュリティの確保である。

今後、自動車や家電、あらゆる機器がネットワークでつながっている時代が到来するが、これは新たな産業革命であるとともに、サイバーセキュリティにおける大きなリスクとなるものである。さらに、サイバー攻撃だけではなく、システム自身のバグによる誤作動などの信頼性のリスクへの対応も大きな課題となる。

今回制定された第３次行動計画に従い、経済産業省としても、ＩＴセキュリティに関る取り組みを強化してまいる。具体的には、人材の認証、システムの認証の２本柱で取

り組んでまいる。

参考資料２を御覧いただきたい。ＩＴ人材の国家試験である情報処理技術者試験において、セキュリティマネジメントの試験区分を新たに創設することとした。小売や金融など、ＩＴのユーザー企業の人材を対象として想定しており、東京オリンピック・パラリンピックもにらみ、平成28年度からの開始を目指している。

また、発電所などの重要インフラのシステムに対するセキュリティの認証制度を、本年４月１日に立ち上げた。こうした認証制度はＩＥＣの国際標準に基づくものであり、米国に次いで世界で２番目、アジアでは初である。従来、日本企業は米国の機関に申請をして、英語での認証の審査を受けていたが、今後は国内で日本語による審査を受けられるようになった。

(3)　議長締め括り挨拶

本日は、昨年６月に決定をしました「サイバーセキュリティ戦略」を踏まえて、政府機関や重要インフラの情報セキュリティ確保のための施策等を取りまとめいただき、感謝申し上げる。

サイバーセキュリティへの脅威に立ち向かうには、我が国の対処能力、総合力を充実、強化していくことが極めて重要である。

このため、本日御決定いただいた政府や重要インフラにおける対策の強化に加え、特にＮＩＳＣの機能強化など、関係機関の円滑な連携を通じて、我が国のサイバーセキュリティ政策推進体制を強化することが、極めて重要と認識しており、また、自民党からは、基本法を整備する必要性について申し入れを受けているところ。

今後とも、一丸となって、「世界を率先する」、「強靭で」、「活力ある」サイバー空間の構築を目指してまいるので、各構成員の皆様にはぜひとも御協力のほどよろしくお願いする。

－　以上　－