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37回会合　議事要旨

１　日時

平成25年10月２日（水）　16：30～17：30

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
新藤　義孝	総務大臣
小野寺 五典	防衛大臣
後藤田 正純	内閣府副大臣
岸　　文雄	外務副大臣
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株式会社代表取締役会長
土屋　大洋	慶應義塾大学大学院教授
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
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。

皆様ご存じのとおり、今や国家機密や企業秘密等を狙った「標的型攻撃」や、重要インフラに対するサイバー攻撃が世界中で顕在化し、サイバー空間におけるリスクのグローバル化が顕著に進んでいる。

このような状況の中、これまで、情報通信技術の研究開発や普及等において世界をリードし、また、官民において様々なサイバー攻撃事案にも対処してきた我が国の経験を、諸外国に積極的に発信していくことが極めて重要になっている。

本日は、サイバー空間のグローバルなセキュリティを確保するため、我が国が率先して国際貢献していくための具体的な方策について御議論いただきたい。

(2)　討議

・　「サイバーセキュリティ国際連携取組方針（案）」について（決定）
・　「情報セキュリティ国際キャンペーン」の実施について
・　「政府機関の情報セキュリティ対策のための統一基準群」の今後の在り方について
・　その他

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。

○　本日会合の主題である国際連携に関連し、３点述べる。

第一に、国際的な場における発信の重要性について。インターネットはそもそも成り立ちとしてグローバルな空間に作られたものであり、情報セキュリティは、そこに起因することが少なくない。国際的なアプローチ、メッセージ、戦略等は重要な領域であり、これまでＩＴ戦略関連の多くの検討の場に有識者として参画し、その重要性を訴えてきた。本日の「サイバーセキュリティ国際連携取組方針」の取りまとめはすばらしい。特に、Ｇ８、ＯＥＣＤ、ＡＰＥＣ、ＡＳＥＡＮといった会合において、大臣級のリーダーシップの下、このメッセージを国際的な場で発信していくことが重要であるところ、既に英語版も整備されている点が高く評価できる。

第二に、サイバーセキュリティに関する我が国の文化、特徴を生かした基準と指標について。戦略的な基準作りは、目的を考えて、目的を測るためにどういう指標があり、その指標の中で目的達成度を向上させるにはどう努力していくかという、複合的なものである。今後策定される基準については、サイバーセキュリティに関する日本の文化・特徴を活かした基準を作ると同時に、その基準が世界のものさしになるような作り方が必要である。そのためには、グローバルインデックス化を考えて基準を作り、基準群自体を日本のメッセージとして発信し、我が国からの具体的な貢献としていくことが重要である。

第三に、人材について。今回話題になっている国全体の、政府のセキュリティレベルを上げる際、国際的に対応する場合は交渉ごともふくまれるため、「日本のセキュリティ

の顔」の継続性を保ち、国際的な信頼を作る必要がある。そこで、人事をうまく工夫し、セキュリティのエキスパートとして流通させ、政府の中での人材流通も含めて考えて欲しい。

○　近時、米国国家安全保障局等がインターネット事業者等の保有する情報を収集していた件の報道等を通じ、サイバーセキュリティに関する社会の認知が深まった。また、広くリスク全般に対する意識も高まってきていると感じる。

その上で、先般東京が 2020 年のオリンピック開催地として決定されたことは、象徴的であり、我が国は、サイバーセキュリティの分野においてもリスクを管理することができる国であることを世界に示していく必要があり、そのためには、我が国は様々な観点でサイバーセキュリティの高度化の先端を走っていかなければならない。このような情勢認識の下、２点述べる。

第一に、我が国がこの領域での先端性を保つための組織の在り方について。サイバーセキュリティの分野では、情報の窃取を目的としたと見られるサイバー攻撃が現実のものとして発生している一方、あらゆるインフラがソフトウェアによって制御される時代を迎えつつある中、将来的に顕在化するおそれのあるインフラに対するサイバー攻撃を未然に防止することの重要性が高まっており、サイバー攻撃の脅威に対し、国がリアルタイムかつダイナミックに対応するため、その対応の中心となる組織が求められている。

「サイバーセキュリティ戦略」には、2015 年度を目途にＮＩＳＣをサイバーセキュリティセンターに改組することが掲げられている。立法を含めた対応を急務のものとし、運用にあっては情報を一元的に集約しつつ必要に応じて各省間分野に応じた府省庁に対して展開する組織とし、リアルタイムかつダイナミックな対応の中心とするべきである。情報セキュリティ政策会議でも、今一度「サイバーセキュリティ戦略」に掲げる組織の在り方について、議論していくべきである。

第二に、政府の情報セキュリティ対策予算の状況について。平成 26 年度予算概算要求において、585 億円を要求していることは、大変力強い決定であると言える。一方で、米国と比較した場合、なお 14 倍の開きがある数値であるとも言える。我が国と米国との比較上、ＧＤＰや人口の要素を考えれば、やはりこの数値はせいぜい３倍までの開きになる程度までは、近づくことが望ましい。是非、政府としてさらなる予算の増加について配慮いただくとともに、我々も、この予算の数値をどのようにして更に増やしていくかについて検討するとともに、執行についても検討していく必要がある。

○　まず、「サイバーセキュリティ国際連携取組方針」にあっては、日本語正文に加え、同時に英語版が取りまとめられたことに大きな意義がある。今後の課題は、取りまとめ結果を基に国際的な情報発信にどのように取り組むか、である。先般の「日・ＡＳＥＡＮサイバーセキュリティ協力に関する閣僚政策会議」では、新藤総務大臣が議長を務めたが、この例に倣い、今後も我が国がこの種のポストを占め続ける必要がある。同時に、主要閣僚の外遊に際しては、是非我が国の情報セキュリティ、サイバーセキュリティの取組について、方針を示しながら情報発信に努めて欲しい。

次に、重点取組分野に関連し、多層的な情報共有体制の強化に当たり、次の２点につ

いて検討されたい。

第一に、海外のセキュリティ対策提供事業者との協力関係の在り方について。現在、我が国のセキュリティ対策は、残念ながら主に海外の事業者から提供されている。当然、我が国の事業者を育成する観点の政策も重要であるが、喫緊の課題として、海外の事業者とのつきあい方を検討することが非常に重要である。

第二に、学術界との協力関係の在り方について。現在、情報セキュリティについては、重要インフラ事業者を始めとした産業界と政府との間の連携は進んでいる。これに比較して、学術界と政府との連携状況は、明確ではない。例えば、セキュリティに関する研究会等が設置されている情報処理学会や電気情報通信学会との連携は、今後の課題である。これらの学会は国際連携を推進しているであろうから、関係の学会等に今回取りまとめた「サイバーセキュリティ国際連携取組方針」を配布し、政府の方針をしっかりと伝えた上で、可能なところから政府と学会が連携していくことが必要である。

最後に、サイバーセキュリティに関する人材育成について。独立行政法人情報処理推進機構が各企業の状況を調査した結果、現在、セキュリティについては５万人の人材が不足しているとの報告がある。また、直接セキュリティに関連しないものの、ビッグデータについては将来的に 25 万人の人材が不足する見込みであるとの調査結果もある。しかし、情報通信関連人材の教育界からの輩出状況を調べると、我が国と韓国はほぼ同じ水準にあり、両国間の人口比に照らせば、我が国は毎年韓国の半分以下しか人材が供給されない状況にある。この問題を解決しなければ、我が国の雇用が海外に流出する結果をもたらす危険もあることから、是非喫緊の課題として政府が人材育成に取り組み、産業界が内部で個別に育成する人材に加え、教育界から輩出される人材の基礎的力量及び人数をどのように向上するかについて検討することが必要である。

○　まず、サイバーセキュリティに関する国際規範と信頼醸成措置の構築について。先月、個人的に欧米を訪問し、議論をしてきた。現在、各国ともにサイバーセキュリティに関する国際規範を作る必要性については合意している。しかし、その規範の内容については互いに合意できない国々があり、課題となっている。一方、仮に国際規範作りにおいて合意まで到達できないとしても、サイバー攻撃等が契機となって国際紛争に発展することがないよう、信頼醸成措置を設ける必要性が認められている。しかし、信頼醸成措置とは一体何を意味するのかについての合意が得られておらず、曖昧なままの状況にある。したがって、今月のソウル会議や日米２＋２等、今後のサイバーセキュリティ関連の国際会議においては、この国際規範と信頼醸成措置の構築が議論のテーマとなるであろう。その際、我が国がどのように議論をリードしていくか、さらにはどのように議論していくか、を検討することが重要である。

第二に、サイバーセキュリティに関する新たな法制度等の検討について。本年６月の「サイバーセキュリティ戦略」の取りまとめのための議論の過程を通じ、現行法において可能な対策はほぼ尽くしたものと考えている。そのため、更なる対策には法改正を含めた新たな一歩が不可欠である。現在、政府では特別秘密の保護に関する法律案を検討しているところであると思うが、この法制は、各国と情報を共有する必要があるサイバーセキュリティという分野にあって、我が国が秘密を守ることのできる国であると示す上

で、非常に重要な意味がある。是非立法化されたい。

また、先ほど米国において国家安全保障局等がインターネット事業者等の保有する情報を収集していたとの報道が話題に上った。この報道の背景を読み解く上では、米国における情報通信産業のいわばエコシステムを念頭に置く必要がある。国家安全保障局は国防総省配下にあって、情報通信業界に対して国防予算を投じる窓口となっており、米国における同産業の躍進において、伝統的に大きな役割を演じてきた。だからこそ、米国の情報通信業界は、国家安全保障局から情報提供の要請があったときに協力してきたのだと考えられる。我が国の政府と産業界とのエコシステムとして、サイバーセキュリティに関する人材育成等の分野において、何らかの形で、できることがあるのではないか。

さらに、こうした新たな法制度を考える上では、国会が行政のこうした取組を監査できるような体制が必要である。これまでもいくつかの機会に提言してきたが、是非国会内に、こうした議論をすることのできる委員会を設けるよう検討されたい。

○　今回の政策会議の議論に関連し、４点述べる。

第一に、「サイバーセキュリティ国際連携取組方針」の推進について。今回同方針を速やかに取りまとめたことの意義は大きいとともに、内容としても非常にバランスがとれている。今後は、同方針に基づく取組をしっかりと実施されたい。

第二に、「多層的な情報共有体制の強化」について。この情報セキュリティ政策会議を振り返ると、少し前から外務大臣を始めとした外務省政務が参加するようになった。次回からは、有識者構成員としても外交の専門家が加わると聞いている。

一方、現在のところ事務方である内閣官房情報セキュリティセンターの職員には、外務省からの出向者はいないと伺っている。国際連携においてはいうまでもないことであるが、さらには交渉ごとに関する技術の面からも、コミュニティや人脈の面からも、外務省職員から得ることのできる部分は大きく、是非人事交流を通じて政府の中の国際連携の体制も強化されたい。

第三に、産業振興における中立的な場の活用について。現在、サイバーセキュリティの分野では、ＪＰＣＥＲＴコーディネーションセンターが、行政機関でもなく、純粋な意味での民間団体でもない、という位置づけで中立的に活動している。このように中立性を担保することで、官民のセキュリティインシデントレスポンスチームの間の連携が確保されており、これらの連携は更に充実させていくとともに、人材育成においてもこれらの団体を活用することで、グローバルなキャパシティビルディングに貢献することが重要である。同様に、多賀城市に本拠を置く制御システムセキュリティセンターについても、重要インフラ等における制御システムのセキュリティ技術等について、国際的な基準を担うことができるよう、取組の質を高めていくことが非常に重要である。

第四に、政策に関する資料の英語版を作成することの重要性について。今回、「サイバーセキュリティ国際連携取組方針」については、日本語の正文に加え、英語訳資料についても同時に取りまとめることができた。これはすばらしい取組であり、他の「サイバーセキュリティ戦略」等も、英文で発表していくべきである。今後は、各種のアウトプットに際し、予め国際的な発信を念頭に、英語版等についても併せて作業し、英語版

資料を整備していくよう努めるべきである。

○　刑事法学の観点から、特にサイバーセキュリティの分野における米国との連携の在り方について述べる。

今回の「サイバーセキュリティ国際連携取組方針」の取りまとめにあたり、アジア太平洋地域を中心とする方針は全く正しく、合理的である。その上で、やはり我が国の国際連携を考える上で、当面は米国との連携が非常に重要であることも主張したい。

サイバー空間の脅威が深刻化し、グローバル化する中、我が国は欧米等と情報を共有していかなければならない。その際、特定秘密の保護に関する法律の整備等の情報共有のための枠組みを構築することは必要であり、法案についてはよろしくお願いしたい。その上で、共有した情報に基づく対策にあっても、従来あったように、脅威に対し後手、後手に回った注意喚起に止まる段階から、脅威の原因を特定し、積極的に無害化を図る段階へと変化しなければならない。これまで、サイバー空間に関する議論の上では、こうした脅威の原因を根絶する方策は困難であるとされてきたが、既に米国においてはＮＣＦＴＡ等の取組を通じて動き出している段階にある。

先般、警察庁の行政運営上の懇談会の一つである総合セキュリティ対策会議の場において、米国ＮＣＦＴＡの総責任者を招き、議論する機会を設けることができた。その議論を通じて示された、米国ＮＣＦＴＡの成功の秘訣は、「インダストリーファースト」という大原則である。すなわち、産業界の利益が第一にあり、その原則の下、企業から見て問題を解決し、必要に応じて無害化する実行力が求められている。サイバー空間の脅威に対し、まさにリアルタイムでダイナミックに対応するため、法執行力の裏付けを伴った組織が必要とされているのである。

また、米国ＮＣＦＴＡの総責任者からは、日本版ＮＣＦＴＡとの国際連携の可能性について、強い期待感が示された。これは、今我が国が米国との連携について一歩前に進まなければ、世界の流れに取り残されてしまう、という意味のメッセージであると考える。現在、我が国にも国家安全保障会議を設置するための議論を行っており、その過程で海外の関連機関との連携も議論に上っているが、是非この分野における国際連携も進めなければならない。

また、サイバーセキュリティに関する情報共有に際しては、特定秘密の保護に関する法律の制定に加え、いわゆるインテリジェンスの問題についても、我が国と米国がきちんと共有できる、信頼関係を構築しなければならない。

○　サイバーセキュリティに関する最近の国際展開について評価をいただいたことは大変ありがたく、積極的に進めていきたい。

サイバーセキュリティは、ＩＣＴの基盤である。国境を越えたサイバー攻撃が激しさを増す中、一層の国際連携が必要不可欠との観点から、総務省では、先ほどご紹介があったとおり、先月、初めて、我が国及びＡＳＥＡＮ各国のサイバーセキュリティを所掌する閣僚級が参加する会合を開催した。我が国とＡＳＥＡＮは、両者を合わせると、人口・GDP ともに世界の１割を超える。アジアから、世界のサイバーセキュリティの確保に取り組むことは、日ＡＳＥＡＮの共通の責務である。

会合では、独立行政法人 情報通信研究機構のＮＩＣＴＥＲ（ニクター）の技術を基礎とした ＰＲＡＣＴＩＣＥ（プラクティス）及び ＤＡＥＤＡＬＵＳ（ダイダロス）の２つの国内プロジェクトから成る、日・ＡＳＥＡＮ間の技術協力プロジェクトとして、「ＪＡＳＰＥＲ（ジャスパー）」を新たに開始すること、また、サイバーセキュリティ能力の強化を図る「日・ＡＳＥＡＮサイバーセキュリティ人材育成イニシアティブ」を新たに開始することという、２つの大きな成果が得られた。これにより、ＡＳＥＡＮ各国及び我が国におけるサイバーセキュリティ分野の協力が加速し、安心・安全なサイバー空間の構築、ひいては、成長の原動力につながることを期待している。

さらに、総務省では、多角的な国内プロジェクトを加速し、得られた成果を国際的に展開していくこととしている。

具体的には、国内プロジェクトとして、

① 官公庁や大企業等の組織における対処能力の向上を目指して、数千人規模の組織内ネットワークを模擬して行う、国内初の実践的なサイバー演習の実施

② 一般の利用者を対象に、インターネットサービスプロバイダ（ＩＳＰ）等と連携して、マルウェア配布サイトへのアクセスを未然に防止するプロジェクト「ＡＣＴＩＶＥ（アクティブ）」の実施

③ ものづくりの原動力である中小企業における対策促進を図るため、インターネットサービスプロバイダ（ＩＳＰ）と協力し、小さな負担で運用可能な情報セキュリティ対策モデルの策定

を進めていく。

総務省としては、これらに積極的に取り組むことにより、グローバルに貢献し、「サイバーセキュリティ立国」の実現に寄与していきたい。

○ 自衛隊の任務遂行上、サイバー空間の安定的な利用の確保は不可欠の前提であると認識しており、防衛省では、平成２６年度概算要求として、サイバー攻撃対処に関連した事業について総額約２４０億円を計上しているところ。

また、サイバー空間の安定的利用は、我が国の安全保障のみならず、国際社会にとっても共通の課題となっており、先ほど来御指摘をいただいているとおり、とりわけ同盟国である米国との協力は極めて重要である。

したがって、明日日本で初めて米国国務長官、国防長官を招いて２＋２会合を開催するが、その席上で日米のサイバー防衛政策ワーキンググループを新設することで合意する予定である。このワーキンググループを通じて、日米間でサイバーに関する政策的な協議の推進、情報共有の緊密化、サイバー攻撃対処を取り入れた共同訓練の推進、専門家の育成・確保のための協力等の幅広い分野での協力を一層推進していきたい。合意後、速やかにこの体制についての評価をしてまいりたい。

○ 政府全体のIT政策に関しては、本年６月に策定された「世界最先端ＩＴ国家創造宣言」において、「サイバーセキュリティ戦略」の推進を含め、関係府省が連携して取り組むこととされているところ、今後、「創造宣言」に基づく取組を着実に実施していくことが重要である。

特に、先ほど御指摘いただいた基準作りといった点にしっかりと対応しながら、集団安全保障、集団的自衛権を含めた陸、海、空、宇宙に加えた五大空間の一つであるサイバーに関し、防衛省を始めとして海外との連携も深めながら推進してまいりたい。

○　情報通信技術の進歩は経済成長を促し、生活水準を向上させる一方、個人、企業、国家にとっての新たなリスクともなっている。この国境を超えるリスクに対処していくためには、安全保障分野や貿易投資分野での国際的なルール作りや国際連携が急務となっている。

本会議において策定された「サイバーセキュリティ国際連携取組方針」は、先に策定された「サイバーセキュリティ戦略」とともに、今後のサイバーセキュリティ分野での国際的な取組の大きな方向性を示すものである。先ほど、外務省とＮＩＳＣとの人材交流を始めとした積極的な参画について御指摘があったところであるが、外務省としても、この方針に沿って、引き続き関係府省庁と連携しつつ、米国との協力を推進するとともに、関係国との政策対話やサイバー空間の安定的な利用のための国際的なルール作りといった点に力を入れていきたい。

当面の対応としては、今月１７日、１８日のサイバー空間に関するソウル会議に向けた準備を進めているところ。また、本年が日・ＡＳＥＡＮ友好協力４０周年であることにかんがみ、１２月の特別首脳会議も念頭に、日・ＡＳＥＡＮとの間でサイバー分野の協力を強化していく考え。例えばサイバー犯罪分野については、今年に入り大使級及び閣僚級で日・ＡＳＥＡＮ協力を確認してきており、また、日米共同でも国連専門機関を通じた能力構築支援を実施する予定。

引き続き関係府省庁の協力をお願いしたい。

⑶　自由討議

構成員から以下のような意見が述べられた。

○　先ほど、米国における情報通信産業のエコシステムに関する御指摘があった。今回の会合において、各構成員からの意見中にも色々な形でエコシステムに関する話題が現れていると思っており、我が国のサイバーセキュリティの在り方を考える上で非常に重要な考え方であると感じる。

まず、世界一安全なネットワークとサービスが提供される環境は、海外から企業を誘致する際の魅力となることから、世界一安全なサイバーセキュリティの確保は国の安全保障に資するだけではなく、国全体の産業振興に資するものである。

ところで、御指摘のとおり、現在我が国のセキュリティ対策は主に海外の事業者から提供されている状況にあるため、今後は我が国の技術力を育成する必要があるが、そのためには国内にサイバーセキュリティに関する有力なマーケットがあることが前提となる。米国のエコシステムでは、御指摘のとおりまず政府部門が先端技術を調達し、その結果として更なる投資を呼び込んできた。

米国の事例では国防部門が中心にあることから、そのまま我が国にその方法論を直接適用することは難しいようにも見える。しかし、政府の「世界最先端ＩＴ国家創造宣言」

において、目指すべき社会・姿として「健康で安心して快適に生活できる、世界一安全で災害に強い社会」を掲げるように、我が国が「世界一の安全」を目指すことは相応しい。

したがって、我が国が平和な国を希求し、その中で情報環境における世界一質の高い安全性を求め、そのために制度、技術、運用サービスを整えることで、ひいては我が国全体の産業振興に資することとなり、社会の安全性も向上し、国内のサイバーセキュリティ事業者の技術力も向上することとなる。今後、このエコシステムの考え方についても、是非議論していきたい。

○　本日は、限られた時間にも関わらず、非常に有意義なご意見をいただいたことを、深く感謝申し上げる。

政府としては、本日ご決定いただいた「サイバーセキュリティ国際連携取組方針」に基づき、今後、産業界、学術研究機関等と連携して、国際連携・共助の取組を進めるとともに、情報の自由な流通が確保された、安全で信頼できるサイバー空間の構築に取り組んでまいる。引き続きよろしくお願いしたい。

また、有識者構成員の皆様方の委嘱期間がまもなく満了するため、本日は、現体制での最後の会議となった。「サイバーセキュリティ戦略」の策定をはじめとして、本日に至るまでの皆様方の御尽力に心から敬意と感謝を申し上げる。

－　以上　－