サイバーセキュリティ戦略本部
第16回会合　議事概要

１　日時

平成30年１月17日（水）　　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
鈴木　俊一	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
小此木 八郎	国家公安委員会委員長
松山　政司	情報通信技術（ＩＴ）政策担当大臣
佐藤　正久	外務副大臣
武藤　容治	経済産業副大臣
小林　史明	総務大臣政務官
大野 敬太郎	防衛大臣政務官
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	慶應義塾大学環境情報学部教授　大学院政策・メディア研究科委員長
西村　康稔	内閣官房副長官
杉田　和博	内閣官房副長官
髙橋　清孝	内閣危機管理監
遠藤　紘一	内閣情報通信政策監
中島　明彦	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

早朝からお集まりいただき、感謝申し上げる。

本日は、２点について御議論をいただきたい。

１点目は、「次期サイバーセキュリティ戦略の策定」についてである。現行戦略の策定後、サイバー空間と実空間の一体化が急速に進んでおり、将来像を見据えた対策が必要である。また、東京オリンピック・パラリンピック競技大会を控え、大会後も見据えた対策が求められている。このような点を踏まえ、次期戦略の検討に当たっての基本的な考え方について、御議論をいただきたい。

２点目は、「政府機関等の情報セキュリティ対策のための統一基準の見直し」についてである。サイバー攻撃は急速に深刻化・巧妙化し、攻撃のリスクが飛躍的に高まっている。政府機関等においても、システムの多層防御を導入するなど、情報セキュリティの強化が不可欠になってきている。今後の見直しの方向について、ぜひ御意見を賜りたい。

限られた時間ではあるが、よろしくお願い申し上げる。

（２）討議

【決定事項】

・次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方（案）について

【討議事項】

・次期サイバーセキュリティ戦略の検討について

・政府機関等の情報セキュリティ対策のための統一基準群の見直しについて

【報告事項】

・政府のサイバーセキュリティに関する予算（2018年度政府案等）について

・2018年サイバーセキュリティ月間について

・2020年東京オリンピック・パラリンピック競技大会に向けての取組状況について

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。

○（前田本部員）

２つの討議事項のうち、政府機関等の情報セキュリティ対策のための統一基準の見直しについては、御提案のとおりで全く異存はない。もう一つの次期サイバーセキュリティ戦略の検討についても、資料１－１に基づき御説明いただいた整理に異存はないが、基礎的なことに関して、意見を１つ申し上げる。

資料１－１の検討事項の一つに「サイバー空間の将来像と新たな脅威の予測」とあるが、我々のような解釈学者には将来がどうなるかといった未来学的なことは苦手で、我々は現実

に起こったことに対して、問題点を摘出してどう解決するかという動き方をしているものの、AIの発展、ビッグデータ、その他いろいろな報道があり、社会が激しく動く中、それらに対しての様々な攻撃があれば、その被害が指数関数的に大きくなるという御指摘はそのとおりだと思う。その大きな流れの中で着実に押さえておかなければならないこととしては例えば、先月19日にホワイトハウスがWannaCryは北朝鮮の関与があったと断定したと報道されたことが挙げられる。

安倍内閣総理大臣がエストニアに訪問し議論されたが、２年前にもエストニアとサイバーの脅威についての協議を開始していた。それはエストニアが、日本とは違いあれだけの被害に遭って危機意識を持っているからであり、現状を考える上で非常に重い事実と思う。先ほど御紹介があった各国のサイバー政策をいろいろな国が出している。多種多様だが、一つのトレンドははっきりしている。

一番分かりやすいのは英国で、その国家サイバーセキュリティ戦略では、防御、抑止、開発を柱に据え、積極的防御の他、抑え目に言っている面はあるが攻撃的防護についても触れている。どこの国もサイバー犯罪、テロの分析は実施しているが、様々な研究を しなければならない。これを世界に向かって発信している。

中国は、日本と同じように重要インフラが保護されなければならないことや、サイバー犯罪に対応しなければならないこととしながら、サイバー空間の主権の確保ともしている。諸外国では基本的に国家安全保障を重視するのが潮流になっている。

このような潮流がしばらくは消えることはない。日本のサイバーセキュリティ戦略を考える上で、NISCの本来の問題として考えると多少広過ぎるかもしれないが、内閣のサイバーセキュリティの一番の土台はそこ（国家安全保障）にあり、（それに関する）日本の立ち位置が重要なのだと思う。防衛省は、１月に報道されたものを拝見すると、宇宙・サイバー部隊のような新たな統合組織に向かって動き出している。警察関係もサイバーに関する組織を着実に構築している。５年前、10年前から見ると、警察庁の変化は、予想だにしないものである。

サイバーセキュリティ政策は着実にキャッチアップしながら取り組めてきたと思うが、日本のサイバーセキュリティの施策が国際的なトレンドにある程度乗らなければならないという中で、今までのサイバーセキュリティの基本原則の一部である情報の自由な流通の確保、法の支配、開放性については国家安全保障とぶつかる部分がある。どのようにトレードオフするかという問題がいずれ出てくるかもしれない。その意識を持って、サイバーセキュリティ戦略を考えていくべきである。

東京オリンピック・パラリンピック競技大会に関しては、資料１－１で、対応をすべきだということが明示されて、非常に妥当なものになっていると思うが、仄聞したところでは、東京オリンピック・パラリンピック競技大会の準備の中でも、建物の警備や、会場警備や、物理的な警備のほうが、確実にステップが進んでいる由である。

サイバーについては情報共有の仕方も含め、新しい組織の構築に取り組んでいるが、これ

は、緊急事態に対応して対処するときの組織である。組織で対処するためには上は１本化したほうが良く、もう少し大所高所から見たほうが良いと思う。しかし、間違いなく取組は着実に前進しており、問題があるという指摘ではないが、その点は御留意いただければと思う。

○（村井本部員）

昨年12月22日にIT総合戦略本部、官民データ利活用推進戦略会議の合同会議があり、行政サービスのデジタルファースト化など、ITを活用した社会システムの抜本改革について議論した。その関係から、サイバーセキュリティをどのように考えなければならないかという点について、お話ししたい。

資料１－１を踏まえて申し上げると、AIが劇的に進化するというのはそのとおりだと思う。さりながら、現在、最も重要なのは、データを送り続けるIoTデバイスがインターネットにつながってきたということである。家庭の中の機器、街頭のカメラのような所有者が不明確な機器、あるいは公共空間に置いてあるような機器がインターネットに直接つながってくる。このようなIoTデバイスが送ってくるデータを分析するのがAIということになる。問題は、ネットワークの観点から言うと、今までつながっていなかったモノがどんどんつながってくる点である。この状況がIoTでは重要なことである。現在、情報通信事業者は、IoT用の新しいインフラを作ろうとしているが、さらにこれがWi-Fiでつながってくると、これまで単独で使われていたデバイスが新たにつながってくるため、これにどのように対応するかということが、このAIとIoTの劇的進化における課題だと思う。

また、IT総合戦略本部でも、サプライチェーンマネジメントや、コネクテッドインダストリーなどのキーワードが出てきている。その結果何が起こるかというと、今まで横につながっていなかったものがつながって効率を上げる一方で、その中にはセキュリティの弱いエンティティーも存在する。中小企業や地方の企業などが全てつながってくるため、そこではお金のやりとりも発生する。ここがフィンテックの出番となる。お金が関わるため犯罪の対象になりやすく、また、強いところと弱いところが一緒につながることになる。サプライチェーンの中には必ず地方の中小企業がいるため、地方が強くなってこないと困る。そのようなことが変化として出てくるため、対応しなければならない。地方の活性化にも直結するため、そのあたりに気をつけなければならないというのが１点だと思う。

資料１－１に、「サイバー空間と実空間の一体化」という文言が出ているが、何度も申し上げているとおり、各産業分野が全て関係してくる。農業、医療も全てがつながってくるため、これに対応するためには、内閣の立場としては、各省庁が確実にサイバーセキュリティのプロセスを行うという体制を徹底する必要があると思う。

2020年東京オリンピック・パラリンピック競技大会に関しては、資料１－１に書いてあるとおりではあるが、先ほどの前田本部員の発言にも関連して、世界の中で以下のように整理されることがある。サイバーセキュリティの体制、サイバーディフェンスの体制、サイバークライム対応の体制の３つであり、それぞれの命令系統その他は違うところはあるが、例え

ば、重要インフラ部分などでは重なるところがある。そのような場合、オペレーションの問題や命令系統の問題の体系をまず整理し、その中で役割分担をすることが大変重要だと思う。そのようなこともNISCの守備範囲の一つだと思う。

最後に、国際対応について申し上げる。現在、国際関係のやりとりの中で、どのような場面でも、サイバー空間のセキュリティについては議論される。したがって、日本として統一したメッセージが出せるよう取りまとめることが重要だと思う。今は交渉や議論の入口がばらばらであり、調整をする際に様々な部門が関係しているため、この政策論理一本化を進めることが内閣の組織としてのNISCのミッションの一つだと思う。

○（小野寺本部員）

全体の方向性はここに書かれているとおりだと思う。

先ほど、村井本部員から発言のあったIoTの問題については、事業者サイドでは既に準備を進めているところではあるが、問題はやはりそこにつながるモノが、我々の管理のできない状態に既になってきていることである。今回の資料１－１の最後に記載されているとおり、国民全体のセキュリティマインドの醸成が非常に重要になってきていると思う。ネットワークにつながると、攻撃する側は一番弱いところを狙ってくる。その弱いところとは、先ほど村井本部員からも発言があった地方であり、サプライチェーンにつながっている中小企業であり、場合によると街中に設置されたカメラのようなモノまで既に狙われている。そのため、国民のセキュリティマインドの醸成というのは非常に重要で、急がなければならないと思う。

2016年に、総理から初等中等教育でプログラミング教育、コンピューター教育をやるということをおっしゃっていただき、文部科学省からは、2020年からと聞いている。ただ、既に一部の学校では開始しており、既に幾つかのベストプラクティスが出てきているのではないかと思う。ところが、残念ながらここの部分を一体誰がどう取りまとめているのか、率直に申し上げて全く分からない。カリキュラムを決めれば動き出すということではなく、実際の教育の現場で一体何がどうされているのか、確実に見ていく必要があるのだろうと思う。そのため、セキュリティマインドの醸成というのは非常に重要だと思う。

関連して２点申し上げる。１点目は、これは毎回申し上げているが、自動車が普及し始めてから、交通安全教室というものがいまだに開かれていると思う。これは保育園や幼稚園でもやっている。サイバーセキュリティ、プログラミングについてもそのレベルから教育していかないと、なかなか大人になってからは難しいところがあるのではないかと思う。

２点目は、AIの問題、村井本部員からも発言があったが、我々は危惧していることは、AIに誤った情報を与えることによって、結果が全く違ってしまうということである。米国だと思うが、既に実際にそのようなことが起きているようである。単純に言うと、AIで見せる映像に人間には分からないような雑音を加えることによって、AIの判断が違ってきているということが実態のようである。このAIをどう考えるかという点については、技術の問題、政策の問題も含め、早目に取り組むことによって、日本の国際競争力という意味でも、産業競争

力という意味でも、重要になってくるのではないかと思う。

○（中谷本部員）

次期サイバーセキュリティ戦略の基本的な考え方については、AI、IoT、フィンテックの普及といったサイバー空間をめぐる新しい一体化状況に適応したものであって、支持したいと思う。その上で、以下の５点について申し上げたい。

第１は、企業や団体や個人によるサイバー攻撃への対処能力の強化が重要である。まさに、企業や団体や個人の活動全般がサイバーと何らかの形で結びつく時代となった以上、個々の企業や団体や個人がきちんとサイバー攻撃への対応能力を身につけるということは、単なる自己防衛にとどまらず、社会全体の秩序を防衛するという重大な意義をも有する。無防備な企業や団体や個人の中に大きな脆弱性が潜んでおり、その放置が大惨事につながりかねないと言っても過言ではない。このため、政府としては、この点を国民に周知して理解してもらうことが、今後極めて重要であると考えている。もちろん対応能力を身につけてもらうよう、政府が必要な支援を積極的に行うことが重要である。

第２に、諸外国の動向の中で特に注目したいのが英国である。英国は国家サイバーセキュリティ戦略において、攻撃的サイバー能力の強化に言及し、攻撃的サイバー能力における世界のリーダーになることを目指すとしている。我が国とは安全保障全般をめぐる位相は異なるものの、英国のこのような動向をフォローしていくこと自体は有用であると考える。

第３は、今後サイバー攻撃の能力が向上し、制御系への大規模攻撃が発生するということが強く懸念される。直接の被害を極小化するとともに、第２次被害を防止するため、被害を受けた者は情報共有を可能にするため、直ちにJPCERT/CCに通報することが何よりも重要であると考えている。

先ほど述べたことも関連するが、通報することは社会防衛という公益に合致するものである、通報しないことは公益に反するものであるといった意識を、企業、団体、個人に持ってもらうことが重要である。また、企業内部での隠匿を防止するためにも、通報は義務的なものとするほうが望ましいと考えている。

第４に、サプライチェーン全体の対策を強化することが重要であり、各製品・サービスやシステム管理、データ管理などにおけるサイバーセキュリティに関して、国際標準規格をISOなどで作成していくことになると思われるが、日本政府及び日本企業がオールジャパンで規格作りを主導していけるよう、国際標準化戦略を積極的に進めていくことが重要である。産業サイバーセキュリティ研究会が立ち上がったと聞いているが、ここを核として、産業分野におけるサイバーセキュリティ政策において、日本が世界をリードするよう期待したい。また、重要インフラに係る業界においては、例えば米国金融業界のシェルタード・ハーバーを一つのモデルとして、サイバー攻撃の被害が当該業界のシステム全体に及ばないようにする体制を構築するようにしてもらえればと思う。

第５に、北朝鮮問題は予断を許さず、最大限の警戒をする必要がある。とりわけ、重要イ

ンフラへの攻撃が最も懸念されるため、万一の場合にも被害を最小化できるように、常に備えておく必要がある。

○（野原本部員）

本会合の決定事項や討議事項である、次期サイバーセキュリティ戦略の検討について、また、事前検知や情報システムの資産管理の自動化を含めた政府機関等の情報セキュリティのための統一基準群の見直しについて、それぞれの方向性は資料のとおりで異存はない。これに沿って、しっかり検討を進めて欲しいと思う。しかし、どう具体策にするかが重要で、この点について３点申し上げる。

１点目は、情報共有・連携ネットワークの構築・運用についてである。今まで何度も申し上げてきたが、サイバーセキュリティの脅威が今後も深刻化・巧妙化していくことは間違いなく、被害をゼロにすることは不可能なため、インシデント情報等を共有、連携するネットワークを構築することは非常に重要である。

まず被害に遭った人が迅速に情報を共有して、周囲が被害に遭わないようにすることが何よりも重要であり、それをやりやすくするために、体制作りを実効的なものにすることが重要だと思う。そのために、NISCが主導権を持って、必要に応じて情報共有を義務化することも必要ではないかとも思う。また、共有するのはインシデント情報のため、それを提供することを必要以上に恐れることはないということを、しっかりと理解できるように周知していくことも重要だと思う。そして、被害を受けた情報を迅速にオープンにすることは正義であり、大きく見れば、社会にとって非常にメリットがあり、すばらしいことだと評価をする文化の醸成も必要だと思う。民間企業の経営トップの方々も、そうした考え方をしていると伺っている。是非リアルタイムに機能する実質的なルール、体制を構築していただきたいと期待している。

２点目は、先ほど小野寺本部員の発言にもあった国民全体のセキュリティマインドの醸成についてである。この点は私も大変重要な課題だと思っている。セキュリティマインドの醸成については、今まで普及啓発という形で取り組んできているが、是非、次期戦略の中で、NISCが中心となって普及啓発のための様々な組織と連携する体制を作るべきではないかと考えている。

サイバーセキュリティ月間にイベントを行うなど、NISCが自ら国民に向けて啓発活動をすることは重要だが、それだけでなく、関係省庁、ネットやテレビなどのメディア、教育機関、サービスベンダー、そして、自治体などを組織化して、国民全体に訴求したほうが効果は大きいため、そのような体制におけるネットワークをしっかりと構築して、プロデュースすることがNISCの役割ではないかと思う。

例えば20代、30代のビジネスパーソンであれば、ネットやビジネス誌、商工会議所を経由して伝わることもあり、30代、40代の主婦層であれば、テレビの情報番組経由のほうが伝わる。それぞれのカテゴリーによって、どのように、どのメディアで、あるいはどの組織から

啓蒙していくかは、随分違うと思う。したがって、国民をカテゴリー別に分類して、各層にアプローチできる組織体制を作ることが大事であり、直接ではなく代理店のような方式でやることにしてはどうかと思う。是非、そのような考え方で、しっかり予算をとって、実行力のある普及啓発の戦略を作っていただきたいと思う。

３点目は、中小企業のサイバーセキュリティ対策の促進についてである。これはNISCだけではなく経済産業省にも是非、取り組んでいただきたいと思うが、中小企業のサイバーセキュリティ対策の促進は、セキュリティマインドの醸成や、サプライチェーンの一部を担ううえでも、とても重要だと思う。しかし、個別にサイバーセキュリティ対策を整備しようとしても、現状では、玉石混交のサービスがあり、どれを選べば良いのかよく分からない。どの程度のセキュリティ対策を、どこに、どのように相談して、幾らぐらいのコストで整備すれば適切なのかが分かりにくい環境にある。

したがって、各社の状況に応じた環境を整備するために、サイバーセキュリティ関連のベンダーやサービスの特徴、効果、評価を示すような情報の提供、あるいは、そのサービスを評価する指標作りをすると良いと思う。また、相談できる専門家、コンサルタントのような人材を育てること、あるいは、そのような人がどこにいるのかをしっかり示すことで、各社がサイバーセキュリティ対策を準備しやすくなるよう情報の環境整備が必要だと思う。そして、これらのような取組によって、サイバーセキュリティ関連のツールやサービス自体が充実し、関連の産業育成にもつながると思うため、是非ともしっかり進めていただきたいと思う。

○（林本部員）

御提案に異存はないが、決定事項である次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方（案）に関して、補足的な意見を申し上げる。

１点目は、グローバルな視点である。現在は国境を越えて進展し、後れをとると負けてしまうという技術革新と、一方で、原則として国境の中しか管理できない法や政治や制度との間の不整合が、史上最も顕在化した時期ではないかと思う。国際協調によってこのギャップを埋める努力が続けられていることは承知しており、評価すべきだと思うが、第５回目となった国連のサイバーセキュリティ専門家会合であるGGEが、昨年合意に達することができずに散会したことは、ギャップを埋めることがいかに難しいかを示している。当面は、西欧型のシステムと非西欧型システムとの間のシステム間競争の時代を経なければならないと思う。

そこで、西欧型の情報の自由な流通モデルを守ると同時に、仲間を増やす努力が必要だと思う。守る側では、政府調達においてセキュリティ要件を厳格に管理することが重要で、要件はかつて技術的なものを中心としていたが、サプライチェーンを含めた情報管理体制も対象にすべき時期に来ていると思う。また、攻める面では、アジアを中心にして、当該国のキャパシティビルディングに貢献することは、仲間作りとして有効であるばかりか、アジアに

展開する我が国のサプライチェーンのセキュリティ向上のためにも重要だと思う。西欧型システムに積極的に賛意をあらわさない国でさえも、完全な鎖国政策をとることや情報通信技術の最新動向に目をつぶることは、失うものの方が得るものよりも大きいと思うからである。

２点目として、以上のグローバルな視点を国内モデルに照らし合わせた場合について申し上げる。システム間競争の中にあっても、西欧諸国が一様であるとは思えない。各国は地政学的位置などを所与の条件として、他国よりも優位に立とうとして、国別モデルを追求することになると思う。そこで、日本型モデルを提案し、模索するためには、まず、自国の優位と劣位を自覚する必要があると思う。

次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方（案）の三の項目として、「サイバーセキュリティ戦略中間レビュー」における指摘を取り込んでいくのは、そのような視点から評価できる。2016年から2020年の戦略を策定した英国の例を調べたところ、英国政府自体が、オックスフォード大学が開発した「Cybersecurity Capability Maturity Model」を使って自己点検していた。しかも、自己採点では５段階評価で２点しかとれない項目があり、そのドキュメントがそのまま公開されていることに驚いた。その中で特に驚いたのは、レスポンシブルレポーティングが２点になっていることであり、恐らく弱点だということを自ら公表しても、それを克服する自信があったのではないかと思う。

各国のモデルは、それぞれの国の歴史文化を反映したものであり、それを直輸入するべきものではないと思う。しかし、前田本部員、中谷本部員の発言にあった通り、英国モデルから多くを学ぶことができるのではないかと考えている。その理由は、情報の役割を重視する伝統があること、島国であり経済規模も似通っていること、議院内閣制であること、オリンピックを経験したか、直前に控えていること等の類似性である。

あるセキュリティの専門家は、インテリジェンス機関であるGCHQの配下に設置されたナショナルサイバーセキュリティセンターが次々と打ち出す施策が、ロンドンオリンピックで採用されたものと非常に似通っていると言っている。今回検討する戦略が、2020年東京オリンピック・パラリンピック競技大会という時間と空間の制約の中で試されて、その後は全国展開されていくことに期待する。

○（鈴木東京オリンピック・パラリンピック競技大会担当大臣（副本部長））

2020年の東京オリンピック・パラリンピック競技大会の成功には、サイバーを含むセキュリティの確保が不可欠であり、政府においては、「大会に向けたセキュリティ基本戦略」や先般決定した「オリパラ・テロ対策推進要綱」に基づき、諸対策に取り組んでいる。

具体的には、サイバーセキュリティ対処調整センターの構築や技術者との連携態勢の整備、電力、通信、交通などの重要サービス事業者におけるリスク評価を進めている。

加えて、我が国全体としてリスク対策を最適化するため、優先順位の明確化など横断的なリスクアセスメントを、着実かつ計画的に進めている。これまでの関係省庁の御協力に御礼を申し上げる。

また、サイバーセキュリティ戦略本部の副本部長として、統一基準群の見直しを含め、次期戦略の策定に向けて、施策の総合的かつ効果的な推進を図ることができるよう取り組んでいきたいと考えており、関係省庁の引き続きの御協力をお願い申し上げる。

○（小此木国家公安委員長）

昨年は、世界的規模のランサムウェア感染事案が発生し、国内でも被害が確認されるなど、サイバー空間における脅威が深刻化している状況にある。

また、サイバー空間と実空間との一体化が急速に進展する中、国民一人一人がその脅威を認識し、主体的に対策を講じていただくための取組を推進することが重要と考えている。

本日決定される「次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方」を踏まえ、次期戦略をより効果的なものとするため、警察が把握した脅威の実態を共有するとともに、2020年東京オリンピック・パラリンピック競技大会の安全・安心の確保のため、サイバー空間を含めた治安の維持に万全を期すよう、警察庁を指導していく。

○（松山情報通信技術（IT）政策担当大臣）

昨年末に開催したIT総合戦略本部において、「電子申請に係る添付書類の撤廃」、「行政保有データのオープン化」を柱として「ITを活用した社会システムの抜本改革」に取り組む方針を決定した。この方針を具体化し、IT利活用を推進するに当たっては、セキュリティの確保は必要不可欠、大前提である。

また、IT総合戦略本部では、各府省の情報システムの運用コストの削減を推進しており、削減分をセキュリティ対策などの重要な分野に活用するよう、働きかけている。

引き続き、サイバーセキュリティ戦略本部の取り組みに全面的に協力してまいりたい。

○（佐藤外務副大臣）

外務省としては、国連をはじめとする様々な場において、サイバー空間に関する国際的なルールや規範を実践・確立させ、国際社会の平和と安定を実現すべく、関係国との協力を深めてきている。

国家の関与が疑われる事案や高度化・巧妙化する脅威に官民一体とって取り組む戦略を策定するに当たり、関係国との協議等を通じ、関連する情報の収集や協力枠組の構築に引き続き取り組んでまいりたい。

○（武藤経済産業副大臣）

サイバー攻撃の起点の急激な拡大、攻撃手法の高度化は日々進展しており、今や、どこからどのような攻撃が来るのか把握することすら容易でなくなっているのが実情だと承知している。

このような問題意識のもと、経済産業省では、日本の産業界を代表する経営者、日本のイ

ンターネット時代を切り開いてきた第一人者等を構成員とする「産業サイバーセキュリティ研究会」を設置し、昨年末に第１回研究会を開催した。参考２に概要を記載したが、問題意識を共有し、縦割りを超えて、関係省庁が一丸となってサイバーセキュリティ政策に取り組むよう、NISCを初めとする関係10省庁にも出席をいただいた。

研究会では、複数の委員の方からサイバー攻撃に関する情報共有の体制を強化すべき、との指摘があった。現在、NISCが中心となって、更なる情報共有対策の強化に向けた取組が進められていると承知をしているが、サイバー攻撃に関する情報が関係者に迅速に共有され、実際の被害を抑制できる実効的な制度になることを強く期待している。そのためには、経済産業省としても最大限貢献してまいる所存である。

また、本日の配付資料では、次期サイバーセキュリティ戦略策定に向けた検討課題として「サプライチェーン全体におけるリスクの増大」が挙げられている。冒頭に述べたようにサイバー攻撃の深刻度が急増する状況から、当省の研究会においても、サプライチェーン全体でサイバーセキュリティを強化すべき、社会全体として取り組むべき、との指摘があった。

経済産業省では、サプライチェーン全体のサイバーセキュリティ強化に向けた具体策について、関係省庁とも連携をしながら、早急に検討を進めていく。次期サイバーセキュリティ戦略にも反映できるよう取組を進めていく上で、この本部及びNISCのリーダーシップのもと、状況変化を踏まえた意義のある次期サイバーセキュリティ戦略の策定を進めていただきたい。

○（小林総務大臣政務官）

参考１について、先ほど、本部員の皆様からもIoTに関する危機についてお話をいただいたが、本件については、昨年10月に、IoTに関するセキュリティ対策の総合的な推進に向けて、取り組むべき課題を整理した「IoTセキュリティ総合対策」を取りまとめている。これについては、NISCをはじめ、関係省庁と連携して、IoTセキュリティ確保に必要な政策を着実に進めてまいりたい。特に、IoT機器の脆弱性についてのライフサイクル全体を見通した対策、また、法改正も含めて、脆弱性調査の実施等のための体制整備を進めてまいりたいと思っている。

また、人材育成に関しては、国立研究開発法人情報通信研究機構において、当機構の有する大規模演習環境やサイバーセキュリティに関する知見を活用し、各種サイバー演習を実施しているところである。

2020年東京オリンピック・パラリンピック競技大会に向けては、大会関連組織のセキュリティ担当者等を対象とした実践的サイバー演習（サイバーコロッセオ）を、本年２月から本格的に実施する予定である。今年度は約60人を対象としているが、回を経るごとに段階的に規模を拡大していき、最終的には約220人のセキュリティ担当者等を育成することを予定している。

総務省としては、これらの取組を通じて、引き続き、関係省庁と連携しつつ、サイバーセ

キュリティの向上に尽力するとともに、次期戦略の策定に向けて協力してまいりたい。

○（大野防衛大臣政務官）

我々もサイバー空間にかかわる技術の進展が、国民生活のみならず、防衛政策の執行という意味でプラスの側面をもたらすという一方で、その脅威もますます深刻化、巧妙化しているという認識を共有している。

特に、安全保障という分野においては、陸・海・空という伝統的なドメインに加えて、宇宙・サイバーというドメインがそれと同等程度に重要になってきているという意味で、サイバーセキュリティが安全保障における重要な課題であると認識をしている。

そこで、防衛省では、より一層サイバー攻撃対処能力を高めるという意味で、直近で申し上げれば、サイバー防衛隊の約40名の増員や、基幹システムのサイバー防護装置への人工知能の活用に関する研究など、様々な施策を計画し、体制及び対処能力の強化を図っている。

今回課題になった、次期サイバーセキュリティ戦略の検討等、我が国全体のサイバーセキュリティへの取組は安全保障上も極めて重要だと認識をしており、防衛省としても、内閣官房をはじめ関係省庁と連携して、引き続き積極的に協力してまいりたい。

○（村井本部員）

先ほど野原本部員が発言されたことと関連するが、サイバーセキュリティ月間が２月１日から３月18日まである。これは政府で決めたサイバーセキュリティ月間のため、各省庁は全て何か企画してほしいという主旨だったと思うが、これはとてもいいアイデアだと思う。各省庁それぞれ大臣表彰のようなものをこの時期に実施する、あるいは、先ほど申し上げたように、各分野でこのITとサイバーセキュリティに対する意識を上げなければならないため、省庁が担当している産業分野で広く伝わるような何かのイベントを計画していただけると、政府で企画したサイバーセキュリティ月間が盛り上がり、国民への浸透が本当にうまくいくのではないかと思う。今年は間に合わないかもしれないが、来年の予算には入れていただき、少し考えていただいて、政府全体でまとまると良いと思う。

（３）決定事項の決定等

決定事項１件につき、案のとおり決定した。

（４）本部長締め括り挨拶

活発に御議論をいただき、厚く感謝申し上げる。

政府としては、本日いただいた御意見を踏まえ、次期戦略の策定に向けた検討と、統一基準の見直しを速やかに進めていきたい。

村井本部員から御発言のあったサイバーセキュリティ月間については、今年から間に合うことを取り組みたいと思う。

有識者本部員の皆様には、今後ともよろしくお願い申し上げる。

－　以上　－