サイバーセキュリティ戦略本部
第17回会合　議事概要

１　日時

平成30年４月４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
坂井　　学	総務副大臣
西銘 恒三郎	経済産業副大臣
あかま 二郎	内閣府副大臣
堀井　　巌	外務大臣政務官
大野 敬太郎	防衛大臣政務官
遠藤　信博	日本電気株式会社代表取締役会長
小野寺　正	ＫＤＤＩ株式会社取締役相談役
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
野上 浩太郎	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、３点について御議論をいただきたい。

第１点は、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」の改定についてである。重要インフラサービスの安全で継続的な提供を実現するためには、事業者が参照すべき安全指針の不断の見直しが不可欠である。これまでの議論を踏まえ、対策を進める上で、経営層が積極的に関与することなどを盛り込んだ安全指針の改正案を作成した。本日は、この改定案の御審議と御決定をお願いしたい。

２点目は、「次期サイバーセキュリティ戦略骨子」について、３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群の見直しの骨子」である。前回の会合で、これらについての基本的な考え方や見直しの方向性について御議論いただいた。本日はこれを踏まえて、事務局で作成した骨子について御意見をいただきたい。

限られた時間であるが、本部員の皆様には、積極的な御議論をお願い申し上げる。

（２）討議

【決定事項】

・「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」の改定について

【討議事項】

・次期サイバーセキュリティ戦略骨子について
・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（骨子）

【報告事項】

・サイバー攻撃による重要インフラサービス障害等の深刻度評価基準（試案）について
・2018年サイバーセキュリティ月間について
・「各府省庁セキュリティ・IT人材確保・育成計画」の実施状況の概要等について
・サイバーセキュリティ基本法の一部を改正する法律案について

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）

まず、重要インフラに関して、資料１－１を見ていただくとともに、現在のSociety5.0、Connected Industriesも踏まえると、重要インフラの各分野が独立して動いている状況ではないということが、サイバースペースにおける認識として進んできた。これはとても良いことだと思う。

そのような状況の中で、リスクは非常に多様化している。多様な役割と関連する組織や省庁が複雑に絡み合っているということは、内閣あるいはNISCの役割が増えているということではないかと考えている。

この総合的な連携はどうするか、各々の役割がどうなっているか、力を合わせて解かなければならない問題になってくる。このように力を合わせる場所が従来、なかなか見つからなかった。横につなぐという役割をNISCが積極的に果たさなければならないということだと思う。

昨今「漫画村」というサイトのことが話題になっている。これは様々な漫画のオンラインバージョンを閲覧できるサイトであるが、このサイトが非常に人気になってくると、最も残念なのは、子供たちに知財に対する意識が芽生えず、無料で閲覧できるから良いのではないかということを思い始めることである。このサイトをよく分析すると、海外で運営されていて、実際にその漫画を集めていない等、様々な技術を使っており、これは知財、ネットワークのオペレーション及び国際関係の問題、そして、社会の中での子供たちに何を意識してもらいたいのかという問題、これらが複雑に絡み合った中で解いていかなければならない問題である。

したがって、この問題も重要インフラと同時に、社会の中で様々な役割を担っている人間が力を合わせるために、どこで議論して、どう対処するのかを考えなければならないことである。

先日、オタワで「Global Internet And Jurisdiction Conference」という大きな会議があった。そこで議論された「アブユーズ（abuse）」、乱用や悪用という意味であるが、新しいテクノロジーが出てきて、それを悪用するということはどういうことなのかという議論が出た。驚いたことに、悪用する人はいるが、悪用する組織、悪用する企業というのも出てきた。様々な視点で、ある種の企業はそのような悪用を行っているのだろう。更に驚いたことは、悪用する政府という議論もある。

アブユーズという問題に対しては、何が悪用かを識別し、その識別した悪用の議論が十分行なわれ、それに対してどのように対応をするかを決めるというプロセスの明確化が、新しい考え方であると思った。技術はますます進化して社会はよくなっていくが、良い技術が生まれれば必ずその裏をかく者が出てくるため、それが何かを識別し、対応するという考え方は、サイバーセキュリティ全般を考えるためには大変重要であり、多様化にも対応できるプロセスではないかと思う。このような流れも重視していくことが重要ではないか。

最後に、３月29日と30日に慶應義塾大学で、アメリカ大使館、イギリス大使館、イスラエル大使館、インドネシア大使館の協力のもと、産官学が国際的に集まるサイバーセキュリティの会議を開催した。「次期サイバーセキュリティ戦略骨子」に国際的な協力という内容があるが、一定の役割を果たしているいくつかの大学が、イギリス版、アメリカ版、日本版と、各々集まり、大学の連携として、サイバーセキュリティにどう対応できるかという活動を始めた。

私はこの活動は大変貴重だと思う。大学から見ると、複合性、融合性という内容は議論する環境があり、また、そのような内容は我々大学の使命でもある。このような活動が、これからNISCとどのように連携し、体制を構築するかということは大きな課題だと思うため、相談しながら進めたい。

○（遠藤本部員）

まず、「重要インフラにおける情報セキュリティ確保に係る安全基準策定指針（案）」については、資料１－１にある「NISCによる調整・連携」という部分が大きな核であると思う。ただ、調整・連携という観点だけではなく、各関連の部門が同一のプライオリティを感じるということが重要であり、この中では、やはりリーダーシップというものがとても重要であると思う。単なる調整・連携というだけではなく、例えば、重要インフラ所管省庁が集まったチームを作り、そこでリーダーシップをとりながら動かすことや、何かリーダーシップを強く発揮するチームの存在も今後考えていただければ大変ありがたい。そのうえで、この方針自体については賛成である。

その他、幾つかについてコメントを申し上げる。

参考資料１をご覧いただきたい。経団連で私自身が情報通信委員会の委員長を務めていることもあり、是非こちらについて御紹介をしたいと思う。

サイバーセキュリティ月間に合わせ、私ども経団連は「経団連サイバーセキュリティ経営宣言」というものをまとめた。この基本的なところは、経営者としての、経営層としての覚悟表明であり、一層の理解の促進のために、これをまとめてある。この宣言では、サプライチェーンの対策や積極的な情報の共有、さらには、国際連携などを通じて、社会全体のサイバーセキュリティ強化に貢献する点も強調している。また、賛同する企業については、各社のウェブサイトとの連携等も図っていこうと考えている。

次に、サイバーセキュリティにおける我々日本の技術の向上という観点で申し上げる。

まず、現状のサイバーアタックを振り返ると、2017年は、５月にはWannaCry、６月にはNotPetya、10月にはBad Rabbitというような強力な感染能力を持ったランサムウェアが猛威を振るった年であった。さらには、金銭目的だけではなく、背景には、先ほどあったように、政治的意図が裏に見えるようなものも指摘されている。

もう一つの特徴は、仮想通貨に関連するサイバーアタックである。多数のPCにマルウェアを感染させて仮想通貨を発掘する攻撃、さらには、ウェブサイトにアクセスしたPCのCPUのリソースを借りて仮想通貨を発掘する攻撃が頻繁に発生した。

更にDDoS攻撃についても、非常に高い増幅率を実現したリフレクションタイプの攻撃というものが出てきており、GitHubというところには、１Tbpsを超えるDDoS攻撃、実際には２Tbpsに近いところまでのDDoSをかけられるようなことが発生してきており、あるネットワークを瞬間的に止めてしまうというような攻撃が出てきた。

いずれにしても、このような攻撃が出てきたということは、常に新たなマルウェアが開発されているということであり、一方、日本のセキュリティビジネスの現状としては、2016年には3,000億、2021年には4,000億弱というセキュリティの製品市場がある。セキュリティサービスでは、2016年では7,000億、2020年では１兆円弱と予想されており、セキュリティサービスまたはセキュリティの部品における年間の成長率は、大体５％／年となる。しかしながら、サイ

バー空間自体の拡大速度はこれ以上のものがあり、カバーし切れないネットワーク、カバーし切れないデータというものが出てきているのだろうと思う。

その中で、日本の中のセキュリティ技術といえば、これらの対策として海外製の製品を使っている場合が多く、日本の中でこのような技術を自ら開発する能力を更に高める必要があると思う。その観点から、高度な分析技術を持った技術者が必要であり、引き続き問題になるが、人材の育成の観点でも、この部分が非常に重要な領域に更になってきたと考えている。

また、サイバーセキュリティの観点で、今後のIoT時代に入ったときに起こることとして、我々が認識しなければいけないことは、第５世代の通信の登場により、遅延も短くなり、マシン・ツー・マシンでのコミュニケーション、マシン・ツー・マシンでのAIを取り入れた動きというものが出てくる。その結果、マシン同士で自ら判断をし、自ら行動をすることになる。

今は、サイバーセキュリティは人間が介在している場合が多いが、マシン・ツー・マシンでリアルタイムのやり取りをしながら、AIが入り、この中へ向けた攻撃が出てくるため、より一層、サイバーセキュリティに対しては、ネットワークを含めた領域のケアをする必要が出てくる。したがって、セキュリティ・バイ・デザインという方針をベースとしたIoT機器一つ一つのセキュリティを高めていくことも含めて、セキュリティを積み上げていくという考え方を、より一層我々の中に取り込む必要があると考えている。

最後に政府のセキュリティについて申し上げる。今、政府ではデジタル・ガバメントの整備・構築に方向感を持っている。ただし、この中でどのようなことが行われているかについては、一つの観点として、地方自治体との連携の部分が少し書き切れていないのではないかと感じる。中央省庁のデジタル化は必要であるが、それと同時に地方とのリンケージをどのように進めるべきか、また、地方のデジタル化はどのように構築するべきか、その中にサイバーセキュリティも入るが、そこの部分が、いま一つ、まだ明確化されていない。

申し上げたいこととして、例えば、そのプラットフォームを村で作るのか、町で作るのか、市で作るのか、あるいは県で作るのか。プラットフォームであれば、かなり大きな投資も要るほか、メンテナンスも要る。そうであれば、ある程度の人口を含めたレベルの、例えば1,500万人、1,000万人という単位のプラットフォームの作り方などが重要になり、その辺りの大きなアーキテクチャーと方向感などを見据えて作っていくことが重要だと思う。最終的にはこのようなプラットフォームがインターネットで日本全体を結ぶことにより、地方創生にも大きな貢献をすると期待しており、是非この辺りも官民一体となって考えていければと思う。

○（小野寺本部員）

今回の重要インフラ関係の議題について、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（案）」は非常に的確に書かれていると思う。特に資料４で説明された「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準（試案）」について、これを定めることは、重要インフラを深刻度でもって横で連携がとれるということになり、大変評価できる。是非、この深刻度評価をうまく使って、横連携を強めてほしいと思う。

２点目として、「次期サイバーセキュリティ戦略骨子」については、非常によくできていると思う。他の本部員からも御指摘のあることだが、今のサイバー空間と実空間の一体化、資料では別紙に記載がある内容について、このサイバー空間とフィジカル空間がまさしく一体化していくことに伴う問題点、これを事前に検討しておかないと、非常に危ないのではないかということが言える。

従来、サイバー空間だと、例えばIoTという関係で我々事業者も関わって、閉じた場での議論で十分だったわけであるが、この資料２－１の３ページの図の通り、サイバー空間とフィジカル空間が一体化していくと、通信、IoTの部分と全てのものが結びついてくる。その際、リスクをどう予測するかということが、従来とは違ったリスクが出てくるのでないか。例えば、金融とサイバーをとってみても、金融から見たときのリスクとサイバー空間から見たときのリスクが必ずしも一致するわけではなく、むしろそこに差分が出てくるのではないか。その部分が落とし穴になり、サイバー攻撃を受ける要因がますます増えてくるのではないかと思われる。

サイバー・フィジカル空間の一体運用となってくると、従来のように、例えば通信ならば総務省、機器ならば経済産業省というような枠組みの中の議論では済まなくなってきており、既にそういう時代に入ってきているのだろう。省庁の枠を超えた新しい枠組みの中で議論しなければ、抜け落ちが出てくる可能性が十分に考えられると思う。

これは技術的な問題だけではなく、施策面でも同様のことが言えるのだろうと思っている。省庁の枠を超えたところでの議論をどうやって進めていくか。一つは、NISCが主導的な役割を担うべきだと思うが、政府として、省庁をまたがったこのような問題をどう取り扱っていくかという制度的な枠組みまで入っていかないと、なかなか進まないのではないかという懸念を持っている。是非、この省庁の枠組みを超えたところでの議論をどのように進めていくか、検討してもらえればと思う。

○（中谷本部員）

「次期サイバーセキュリティ戦略骨子」は、Society5.0へのパラダイムシフトに呼応したものであり、全般的に支持したい。

その上で、以下の４点について申し上げる。

第１に、国際社会の平和、安全、及び我が国の安全保障に関連して、我が国としては、引き続き、自由、公正、かつ安全なサイバー空間の理念の発信を行い、サイバー空間における法の支配を推進していくことが重要であると考える。価値観が異なる一部の国や途上国のスタンスに鑑みると、国連の場ではルールづくりの進展は困難であると言わざるを得ないが、価値観を共有する西側諸国の枠組みで、例えば、OECDの場においてルール作成を進めるということは有用であると考える。

第２に、新興国への能力構築の一環として、例えば、東南アジア諸国、中央アジア諸国、湾岸諸国などから、サイバー人材を日本に招聘してサイバー分野での研修や訓練を行うことは、長期的に見た場合には賢明なサイバー外交の方策であると考える。

第３に、国民社会を守るための取組に関連して、今後、一層信頼できる通信インフラの整備を進めていくことが望ましいと考える。特に、今後、5Gへの移行に当たり、国家安全保障の観点から、体制の異なる国家の企業の通信機器や通信ソフトに安易に依存するべきではなく、日本企業の通信インフラの整備を進めることが非常に重要であると考える。さらに、この分野での政府調達の在り方についても検討していくことが望ましいと考える。

第４に、官民横断的、業界横断的な情報共有や連携体制の構築は特に重要である。比喩的に申し上げると、各人がパズルの各パーツを持ち寄ってパズル全体が初めて解けるように、様々なステークホルダーが一堂に会することで、サイバー攻撃に対して攻撃源を突きとめたり、適切な対応をとることが容易になったり、可能になったりすることが期待できると考える。政府は、そのようなフォーラムの組織化を一層積極的に進めていただきたいと思う。

○（野原本部員）

今回の決定事項について、資料のとおりで異存ない。討議事項についても、既にこれまで活発な意見交換がなされており、それを踏まえての資料となってきているため、概略については、異存ない。その上で、今後に向けて、４点申し上げたい。

１点目は、人材育成体制の一層の強化と関連人材のイメージアップ策、社会的地位向上策を実施してはどうかという提案である。人材育成の体制の強化は、マネジメント面、技術面をあわせた幅広い人材を育成する必要があるということは何度も議論されてきた。しかし、文部科学省系の予算を見ても、まだまだ不十分だと思う。そして、有望な人材が多く関心を持つように、セキュリティ関連人材のイメージアップ施策を実施することを提案する。一般社会では、いまだに「ハッカー＝クラッカー＝悪」というイメージが残っている。そのため例えば、ホワイトハッカーのスター、成功者にスポットを当てるなど、セキュリティ関連の職業や人材の成功モデルを示し、イメージアップを図ってはどうか。

２点目は、サイバーセキュリティ関連産業の育成・振興策と、関連業界のイメージ向上策についてである。先ほど遠藤本部員からもこの点について強い発言があったが、私もこれまでにも何度も発言しているように、サイバーセキュリティ関連産業の育成・振興策を推進するべきだと思う。今回の「次期サイバーセキュリティ戦略骨子」の中では、先端技術を利活用したイノベーションのセキュリティを確保するためのサイバーセキュリティビジネスの強化としてしか、「ビジネス」という言葉が記載されていない。遠藤本部員の発言では、既に１兆円を超える機器、サービスの市場規模があるという話だったが、今後もサイバーセキュリティ関連の脅威が深刻化・巧妙化すればするほど、セキュリティ対策関連のサービス、産業へのデマンドが生じ、市場が増大する。例えば、IDアクセス管理、ハッカーの分析・対策、エンドポイントのセキュリティ、内部統制やコンプライアンスという対応は既に様々な体制があるが、今後はクラウドセキュリティやネットワークセキュリティ、データの保護、喪失の防止、モバイルセキュリティなど、事業領域も広がっていく。さらに、情報の提供、セキュリティ施策の導入コンサル、施策の導入後監視を行い対策を打つというような対応、それから、教育・育成事業等、

幅広い新たな関連産業が増大していく。これらがスムーズに急速に成長していくよう育成振興策を積極的に実施する必要があると思う。例えば、中小企業がサイバーセキュリティ対策を講じやすくするための仕組みとして、サイバーセキュリティ関連のツールベンダーやサービスに対して比較情報を提供すること、そのための指標をつくり、相談できる専門家がどこにいるかを示す情報の提供を行うことが必要ではないかと、前回も申し上げた。こうした各社のサービス、ツールの比較を行うことは、関連サービスの育成、競争、適切な淘汰を促し、振興・育成策にもつながる。そして、人材だけでなく関連業界、各種サービスについても、イメージ向上策を推進することが効果的だと考える。

３点目は、国民や組織や各々のための啓発、育成施策についてである。次期サイバーセキュリティ戦略の基本的な在り方のイメージで示されているように、関係者それぞれが主体的にセキュリティ対策に取り組むことが重要ということが、今回の戦略の骨子である。そのような個人や組織を育てるためには、NISCが中心となって普及啓発戦略を立案し、それを様々な組織と連携する体制を構築してはどうか。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も大変重要だが、それだけでなく、関係省庁、メディア、ソフトベンダー、教育機関、自治体等と積極的に連携体制を作り、個人や組織等々に訴求するようにしてはどうか。

４点目は、海外に向けての情報発信方法についてである。次期サイバーセキュリティ戦略が海外でどのように受けとめられるのか。海外への情報発信について、用語の使い方やコンセプトの見せ方などは、ぜひ戦略的に行っていただきたいと思う。

○（林本部員）

「次期サイバーセキュリティ戦略骨子」を中心に４点申し上げる。

第１に現在の戦略は事案が発生してからの対処策が中心であったが、今回は、先端技術の活用による先取り対応への挑戦を掲げている点に、新しい方向感と意欲を感じた。この点にも関連して、脅威情報等の共有について、サイバーセキュリティ基本法の一部改正と、電気通信事業法及び国立研究開発法人情報通信研究機構法の一部改正によって、マルウェアに感染したIoT機器などを検知して、ISPなどがその情報を共有することによって、事情を知らない利用者に注意を喚起する他、攻撃をブロックする道を拓いたことは、具体的な進展だと思う。このような施策を政府自身が示したことは、民間との協調の上で主導権を発揮する契機となり、国全体として大いに効果があると思われる。ただし、先端技術の活用による先取り対応そのものではなく、対応への挑戦という表現には試行的なニュアンスが残っているため、今後の更なる展開を期待する。

そこで、第２に、情報を守るための基本動作を定め、官民がそれぞれ日常的に繰り返して実践するべきことを強調したいと思う。まず、政府側では、本会合で議題になっている「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」の改定や「政府機関等における情報セキュリティ対策のための統一基準群」の見直しは、その目的に沿ったものだが、セ

キュリティ要件とともに、情報アシュアランスの手順も制定し、政府調達に生かすべきだと思う。米英両国では、この両者を政府調達と結びつける動きが軍から始まって政府全体に急速に拡大しつつあり、サプライチェーン全体のセキュリティを要求していることに留意しなければならない。こうした動きに共同歩調をとらないと、我が国の企業が外国政府に売り込むチャンスを失うおそれがある。一方、民間の側では、経済産業省がサプライチェーンの間で情報を共有しつつ、共有範囲外への情報流出を避けるため、従来の営業秘密の範囲より広い、相手方を限定しアクセス制限を付して業として提供するデータという概念に関して、その不正取得などの侵害に対して差止め請求権等を付与する新しい制度を検討して、不正競争防止法の一部改正法として提案しているが、これも具体的な進展と考えられる。

３点目として、以上を踏まえて、官が主導する仕組みがトリクルダウンをして民間の競争力強化に役立つことを期待している。既に複数の本部員が競争力強化の点に触れたが、先ほど申し上げた政府調達は一見規制強化に見えるが、その厳しい条件に合格することが長期的には企業の競争力強化につながる面があると思う。同様に、情報通信研究機構から始まるマルウェア検知等が、やがて民間にも開放され、マネージドセキュリティサービスプロバイダーの体力強化の基礎となることを期待する。また、経済産業省の所掌する情報セキュリティサービス基準の制定も、同様に、マネージドセキュリティサービスやセキュリティ監査の業務に関して、サービスレベルを向上させる契機になるものと思う。

最後に、４点目として、縦割り行政を打破して、政府全体として統合する仕組み、あるいは心構えが必要な点について、既に小野寺本部員から発言があったので、簡単に申し上げる。サイバー空間には境目がないため、総務省は多分レイヤーの下のほうからアクセスし、経済産業省はレイヤーの上のほうからアクセスをすると思うが、それは理解できるものの、両者を突き合わせたときに初めて矛盾や欠落が明らかになるということもあると思うため、更なる協調と調整をお願いしたい。

○（前田本部員）

まず、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」について、非常によく練られており、今までの議論を踏まえ全く異存はない。

「次期サイバーセキュリティ戦略骨子」について、幾つか簡単に触れるが、資料２－１の２に記載の通り、AIなどを中心にした国民が恩恵の得られる科学技術の推進をしなければならない。それはその通りであるが、それに対抗する脅威を踏まえ、AIの開発自体も慎重に行わなければならない。AIの開発は進めなければならないことであるが、テスラやウーバーの自動運転による車の事故が、どういう反応を起こすか。必要悪であって発展のためには犠牲が出るのは当たり前という認識でいると、政治の世界も同じであるが、思わぬブレーキがかかってしまう。日本のスタイルとしても、慎重なAIの発展、大事だからこそ慎重にならなければならない。仮想通貨問題もそうであるが、西欧に比べるとむしろ日本のほうが前のめりのように感じる。全体として間違った方向に行くことはないと思うが、まず、サイバー空間から得られるものは大

きいけれども、それを大きく実らせるためには、育てるところから慎重にということを一つ申し上げたい。

また、目的達成のための施策という意味で、サイバーセキュリティに対応するチームをつくる際、人材には限りがある。例えば、サッカーも、全日本の代表のＡクラスのようなメンバーだけでチームをつくっていくというわけにはいかなく、様々なリーグがあり、それぞれの人材でチーム構成をしていかなければならない。サイバーというものは、プログラムの正確性や数学的な問題のほか、入力作業など、トータルのシステムでできている。トータルで戦えなければならず、その戦うチームの中にはやはり凸凹がある。その凸凹をなくすのは理想ではあるが、なくすことはあり得ない。全体の能力を上げていくことが重要であるが、ここまでやれて当然であるという認識だけで突き進んでいくと、大きな穴があく。フェイスブックから5,000万人分の情報が漏れたという報道があったが、例えば、水道というのはかなりの水を流しているが、何%かは抜けて流れている。抜けることを前提にシステムはできている。もちろんインテリジェンスの世界などでは、絶対に漏れてはいけないもの、漏れてはいけない程度という内容は様々あると思うが、サイバーの世界でもどう制度設計をしていくか。

そのような中で、先ほど遠藤本部員が紹介された、経団連のサイバーセキュリティ経営宣言については、すばらしいものだと思う。重要インフラの対策を実施しながら、財界は、１歩くっついていく印象だったが、半歩か１歩か前へ出られた印象になった。

もう１点、官のあり方に結びつけて申し上げると、欧米から比べて、日本のサイバーセキュリティのガバナンスは少し歯がゆいところがある。国家が一体となって強力に推し進めるところが足りない。各省庁がばらばらである。本日も複数の本部員から意見が出ているが、私の感想を申し上げると、その国家による統制を推し進めている国もあるが、日本が同じ統制を行うことはあり得ないと思うとともに、国民の幸せになるとも思わない。ただ、イギリス型、イスラエル型など、前回会合でも議論が出たが、日本は日本型を目指すべきである。

日本のよさは、少しばらばらのように見えて、総合的に各々の担当省庁の側から突き合わせると全体像が見えてくるところである。各省庁の主体性は維持しながら、それを統合するためにNISCがどうあるべきか。サイバーセキュリティ戦略本部のもとNISCが主導的役割を担いつつ各省庁も主体的に取り組むということに尽きる。キーワードは、NISCの主導的という、主導の中身である。NISCはますます大きくなり、また、新しい時代に合わせて変わっていくと思うが、一挙にトップダウン式で変わるのではなく、いかに省庁の力を引き出すか。チームがあって勝てるのであって、指揮官がいるだけではうまくいかない。そのバランスだと思う。省庁間で役割が固定化する傾向があるため、その調整をNISCができるのか、サイバー政策のトップの部分をどう考えるか。そのようなチェックは常に大事だと思う。

これまでの取組を見ても、日本のサイバー政策は、基本的には非常にうまくいっている。この方向性を伸ばしていくという観点から、今回の「次期サイバーセキュリティ戦略骨子」は、その方向性として半歩進めたものとして、高く評価したい。

○（鈴木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））

2020年東京オリンピック・パラリンピック競技大会の成功には、セキュリティの確保が不可欠である。

先般閉会した2018年平昌オリンピックの開会式においても、サイバー攻撃が発生しており、サイバーセキュリティ対策の重要性がさらに増したと考えている。

現在、「サイバーセキュリティ対処調整センター」の今年度中の運用開始に向けたシステムの構築等を進めるとともに、重要サービスに対する横断的なリスク評価の検討も進めており、優先順位を明確化し、我が国全体としての対策の最適化を推進してまいりたい。

また、官民の多様な主体が、サイバーセキュリティに資する情報を安心して共有できるようにするため、本年３月、「サイバーセキュリティ基本法の一部を改正する法律案」を国会に提出した。

引き続き、サイバーセキュリティ戦略本部の副本部長として、施策の総合的かつ効果的な推進を図るとともに、基本法の一部改正案の早期成立に向けて、政府として全力で取り組んでまいりたい。

○（小此木国家公安委員長）

昨年中のサイバー犯罪の検挙件数は9,000件を超え、過去最高となった。また、本年１月、国内の仮想通貨交換業者から、多額の仮想通貨が不正に送信されたと見られる事案が発生するなど、一般国民にとってサイバー空間がより身近なものとなる中で様々な事案が発生している。

さらに、2018年平昌オリンピックの開会式で、サイバー攻撃によるシステム障害が発生したことなどを踏まえ、2020年東京オリンピック・パラリンピック競技大会等に向けて、サイバー攻撃への対策を強化することが重要であると思う。

本日の決定事項等を踏まえ、関係省庁等としっかりと連携をし、各種事案に的確に対応していくとともに、大会組織委員会、重要インフラ事業者等と連携し、情報共有や共同対処訓練を実施するなど、対処能力の向上に努めるよう、警察を指導していく。

○（坂井総務副大臣）

総務省では、電気通信事業者間のサイバー攻撃に関する情報共有の促進のための制度整備を行うこと、及び、NICTの業務にパスワード設定に不備のあるIoT機器の調査等を追加すること等を内容とする電気通信事業法及び国立研究開発法人情報通信研究機構法の一部改正案を今国会に提出している。

また、人材育成に関しては、NICTにおいて、当機構の有する技術的知見を活用して、サイバーセキュリティ演習等を実施している。

このうち、行政機関等に対するサイバー攻撃への対処方法を体得する実践的サイバー防御演習（CYDER）については、平成30年度から、重要インフラ事業者向けのコースを新設するなど、更なる内容の充実を図ることとしている。

総務省としては、これらの取組を通じて、引き続き、関係府省庁と連携しつつ、次期戦略の策定に向けても協力してまいりたい。

○（西銘経済産業副大臣）

これまで経済産業省が主張してきた、情報共有体制の強化、サプライチェーン全体のサイバーセキュリティ対策強化、セキュリティビジネスの強化等が「次期サイバーセキュリティ戦略骨子」に盛り込まれていることは、高く評価する。

情報共有体制の強化については、先日、「サイバーセキュリティ基本法の一部を改正する法律案」が閣議決定されたが、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よう経済産業省としても協力してまいりたい。

サプライチェーン全体のサイバーセキュリティ対策については、経済産業省でSociety5.0、Connected Industriesにおけるサプライチェーンに対応したサイバーセキュリティのフレームワークの原案を提示した。今後、英訳した上で国内外に広く意見を求め、フレームワークの詳細化を図る。

これらの取組を通じて、サイバーセキュリティの確保と、Society5.0、Connected Industriesの実現に努める。

○（あかま内閣府副大臣）

現在、IT総合戦略本部の下で、行政手続のオンライン化など、行政サービスのデジタル改革を急ピッチで進めている。

また、急速に技術開発が進む自動運転の実現に向けた関係する法制度の見直しの方針を決めたところである。

このような取組において、ITを活用しやすい環境を整備していくことが大切だが、その一方でセキュリティ確保は必要不可欠であり、また、大前提であると考えている。

IT総合戦略本部は引き続き、サイバーセキュリティ戦略本部の取組に全面的に協力をしてまいりたい。

○（堀井外務大臣政務官）

外務省としては、本日頂いた有識者本部員の御意見も踏まえつつ、サイバー空間における法の支配の推進、関係各国及び地域とのサイバー協議やアジア地域を中心とする信頼醸成措置の推進、能力構築支援といった「サイバー外交」を引き続き実施していく。

直近では、本年１月に、サイバーセキュリティに関するASEAN地域フォーラム（ARF）会期間会合第１回専門家会合を東京で開催し、今後取り組むべき信頼醸成措置の在り方について議論した。また、３月に実施したEUや英国との協議では、それぞれの取組や戦略について意見交換を行ったほか、適切な枠組みを通じ、悪意のあるサイバー活動を抑止、軽減、原因を特定するための情報交換を含む協力強化のコミットメントを再確認した。

サイバーに係る議論や取組は、国際的にも様々な分野に広がりつつある。次期戦略の作成などに当たり、外務省としても、国際情勢に即した戦略を作成するため、関係省庁と綿密な情報共有・意見交換を行い、官民で連携しつつ取り組んでいきたい。

○（大野防衛大臣政務官）

高度化・巧妙化するサイバー攻撃の態様を踏まえれば、今後サイバー攻撃によって物理的なものも含めて極めて深刻な被害が発生する可能性も否定できず、サイバー攻撃への対応は我が国の安全保障にかかわる重要な課題であると認識している。

こうした認識の下、防衛省としては、サイバー防護部隊の体制強化、あるいは、先ほど野原本部員を中心に発言があった、高度な知識・経験を有する人材の教育・育成・確保等、様々な観点から能力を強化する必要があると考えている。

このため、先般も御報告したが、サイバー攻撃対処を担当する部隊を約430名に拡充するほか、国内外の教育機関への留学等を通じた人材育成、あるいは、役務契約等を通じた外部人材の活用等、人材育成・確保に今後とも努めるとともに、所要の装備品等の研究開発など、サイバー攻撃対処能力の向上のために、あらゆる能力の強化、あらゆる面での強化を図っていきたいと認識している。

また、一方で、重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針の改定についても、情報通信、航空、鉄道、電力等の重要インフラが正常に機能することは、自衛隊の部隊等が任務を遂行するさまざまな場面において極めて重要であると認識しており、防衛省としても我が国全体のサイバーセキュリティを強化する取組に対しては、引き続き全力で積極的に協力をしてまいりたい。

（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、いただいた御意見を踏まえ、重要インフラ防護の取組を進めるとともに、次期戦略の策定に向けた検討と、政府機関等のセキュリティ対策基準の見直しを速やかに進めていきたい。

有識者本部員の皆様には、引き続き、よろしくお願い申し上げる。

－　以上　－