サイバーセキュリティ戦略本部
第18回会合　議事概要

１　日時

平成30年６月７日（木）　　８：00～８:40

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
野田　聖子	総務大臣
世耕　弘成	経済産業大臣
小野寺 五典	防衛大臣
松山　政司	情報通信技術（ＩＴ）政策担当大臣
堀井　　巌	外務大臣政務官
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
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、次期サイバーセキュリティ戦略の策定、情報セキュリティ対策のための政府統一基準の改定に関して、パブリックコメント案を御審議いただきたい。

次期戦略案については、これまでの議論を踏まえ、現行の戦略策定以降、AIやIoTなどによりサイバー空間と実空間の一体化が進み、サイバー攻撃の脅威が一層深刻化しているという現状認識の下に、2020年東京オリンピック・パラリンピック競技大会の成功と、その後のあるべき姿を見据えて、積極的サイバー防御対策の構築や高度人材の確保など、セキュリティ確保に万全を期すための施策を盛り込んでいる。

また、統一基準の改定案については、未知の不正プログラムによる被害の未然防止など、新たな対策を導入することとしている。

本日の御審議を経て、速やかにパブリックコメントを実施し、７月上旬開催予定の次回会合において、次期戦略等を決定したい。

本日は限られた時間であるが、活発な御議論をお願い申し上げる。

（２）討議

【決定事項】

・次期サイバーセキュリティ戦略（案）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（案）について
・官民データ活用推進基本計画の案に対するサイバーセキュリティ戦略本部の意見（案）について

【報告事項】

・2018年平昌オリンピック・パラリンピック競技大会における状況について
・サイバーセキュリティ人材育成取組方針について

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。

○（遠藤本部員）

次期サイバー戦略に関して、サイバーアタックそのものが高度化し、さらには多様化しているという観点から、社会インフラに対する攻撃による国民へのインパクトが十分考慮された、有効かつ効率的な戦略と考えている。

私は2017年がAI元年だと思っており、AIに関するプラットフォームが出来上がり、リアルタイムで動いて、価値を生むことが確認された。ここから先はアプリケーションの開発が急速に進むであろう。これは従来のAIの開発スピードに比較すると、100倍、1,000倍のスピードで進

むのではないかと思う。
この観点から考えると、リアルタイムで動くIoTの世界のサイバー空間内で価値が作られる状況になるため、そこにサイバーアタックがかかった場合の日本経済へのインパクト、さらには国民生活へのインパクトは非常に大きなものがある。
これを踏まえると、我々は今までITのネットワークに関してケアをしてきたが、それだけではなくコミュニケーションネットワークとITネットワーク、総合的な情報ネットワークが提供するリアルタイムで動くサービスに対応、さらにはデータ自体の保護に関するケアも必要であり、そのための戦略的な投資が必要になってくるのではないか。
さらに、我々が注視しなければいけないのは、今、実際に私どもサプライヤーの中でも使っているサイバーセキュリティのソフトウェアは、実は米国のソフトウェアであるが、国家間での交渉をするため、または日本のサイバーセキュリティ能力という本来の能力を高める上では、やはり日本発のソフトウェアが絶対的に必要であろうと考えている。このためにも戦略的な投資が必要である。
２つ目は、経営層に対する教育を一層強化すべきではないか。サービスの任務保証という観点で、一人一人の技術者のレベルはかなり上がってきていると思うものの、経営者はこれを非常に広くケアしないと任務保証は実行できない。その辺りの教育を含めた各種施策が必要である。経団連でも様々な施策を始めているため、それと合わせて官民一体となって実施させていただければと思う。
最後は、若年層の教育である。これは小野寺本部員が前から発言していたが、リテラシーを含めた若年層の教育が必要ということと、若年層の高い能力を持った人々の活躍が可能な社会を作ることが重要と考えている。以前にも申し上げたが、将棋が義務教育だと藤井聡太さんは出てこなかっただろうと思っており、こうした高い能力を自ら育てた方がITの領域でも出てくる。だからITの領域の若い能力を持っている方が社会の中で活躍できる仕組みをどのように作ってあげるか。これが重要と考えている。

○（小野寺本部員）
決定事項については、何ら異存はない。
遠藤本部員の発言にもあった若年層に対する教育については、私も調べてみたところ、既に文部科学省が小学校プログラミング教育の手引きの第１版を、今年の３月に作成していた。これをざっと眺めたところ、なかなかよくできている。ところが、このような場でなかなか報告がされていない。2020年から義務教育化するということで総理が発言され、動き出していることは我々も知っていたが、このようなところまで進んでいるということがわからなかったので、ぜひ皆さんで情報共有する必要があるのではないかと思う。
２点目として、これも人材育成に関連するが、中小企業関連の取組で、企業側は大企業はともかくとして、中小企業の取組が遅いということが実態だと思う。
サイバーセキュリティで問題を起こしたときに、一体自分の会社はどのくらいの被害が出る

のかを逸失利益を含めて金額に換算したほうが、中小企業の経営者にとっては非常に分かり易いだろうと思う。例えば個人情報の漏えいについては、１件当たり大体どの程度の費用がかかっているか実例がある。こういう情報集めて、あなたのところだったらこの程度の被害が出ますよということをお金に換算して伝えたほうが、中小企業の経営者には非常にわかりやすいのではないかと思う。

○（中谷本部員）

今回のサイバーセキュリティ戦略案について、全般的に支持したい。

そう申し上げた上で、次の４点について指摘させていただきたい。

第１に、信頼醸成措置について、特にロシア及び中国との間で信頼醸成のための協定を締結することが、サイバー攻撃に対する抑止力の向上にとって非常に重要であると考える。その際、2013年６月の米露合意は一つのモデルになるのではないかと思う。

第２に、サイバー空間において国際法が引き続き適用されることを確認していただいたことを、国際法研究者としてありがたく思う。国連でのルール作りが頓挫していることは残念であるが、政府としては例えばタリン・マニュアルを一つの参考として国際法の解釈適用を進めていただければ幸いである。

第３に、総理が未来投資会議において、大学入試共通テストに情報科目を導入する方針を示されたことは、21世紀の教育のあり方にふさわしい提言であると思う。中学、高校、高専でのサイバーセキュリティ教育とともに、情報科目の大学入試においても、サイバーセキュリティに関して毎年一定の出題をするということが、次世代のサイバーセキュリティ意識を高める上で効果的な方策であると考える。

第４に、資料１－３の22ページに関連して、政府機関や重要インフラ事業者が提供するサービスの基盤となるような安全保障上、信頼できる5Gインフラの構築が不可欠であり、パブリックセキュリティを確保するための政府調達のあり方を十分検討する必要があると考える。

○（野原本部員）

今回の決定事項については、これまで何度も検討を重ねてきた結果としてよくできており、賛成である。

特に「サイバーセキュリティ戦略（案）」に関しては、前回、私は人材育成の強化について、サイバーセキュリティ関連産業の振興について、そして普及啓発のための戦略策定について発言した。それらを含め、そして、これまでの様々な議論や提案も踏まえたしっかりした戦略ができたと思う。

今後は、この戦略を基に適切な具体的施策に落とし込み、先送りにすることなく着実に推進していくことが極めて重要だと思う。関係各省庁で中途半端になることなく、正しく具体的に施策が進んでいるかどうか、各施策の意図がしっかりと実現されているのかどうか、しっかりとチェックしていく必要がある。その役割はサイバーセキュリティ戦略本部にあると思う。

例えばサイバーセキュリティの普及啓発に向けたアクションプランの策定を盛り込んでいるが、それは効果的な施策として出来上がっているか、適切に実行されているかということのチェック。人材育成施策については、経済産業省を中心に戦略マネジメント層、実務層、経営者層等に分けてしっかりとしたマッピングがされている。その結果、各施策は適切に進んでいるのかどうか、何十万人と推定される不足者数を補えるのかどうかということのチェック。また、小野寺本部員から教育のことで発言があったが、小学校、中学校を含め、大学、高専、高校での人材育成も十分実施できているのかどうかといったことをしっかりチェックしていくことが重要である。

また、「サイバーセキュリティ戦略（案）」の本文を拝見したところ、政府機関におけるセキュリティ強化充実の項目の中に、政府機関のセキュリティ投資額の記載があり、政府機関のIT投資がクラウド化などに移行することによって削減される分を、セキュリティ関連の予算に充ててはどうかと読めるようなコメントがあったが、そのような工夫も重要だと思うものの、それ以上にAIやIoT、データ活用が進み、データトランスフォーメーションも非常に重要になっている中、政府機関でもセキュリティ投資をより強化し、十分な予算を確保して取り組むことが重要だと考えている。

○（林本部員）

本日のメインテーマである「次期サイバーセキュリティ戦略（案）」について、私の個人的な意見を付言させていただく。

今回の案は、現行の枠組みを基本としながら、その後の環境変化や知識、経験の蓄積を踏まえて大幅な変更を加えたものと理解している。そして、大綱において共感する点が多々あり、特に共感する点を５点ほど挙げさせていただく。

１点目は、これまで機能保証という概念で語られてきたことを任務保証と改称して、責任主体を明確にしたことである。

２点目は、事後対応に追われがちだった受け身の姿勢から転じて、積極的サイバー防御を試みる意欲を示したこと。これは英語ではProactive Defenseに対応し、リアルタイム対応がその具体化と思うが、成果は今後の実践にかかっていると理解している。

３点目は、その点にも関連して国際社会の平和、安定及び我が国の安全保障の項目に関して、現行のものよりかなり詳細に記述したことである。

４点目は、従来の枠を超えた情報共有、連携体制の構築を目指し、法整備も含めた具体的手段を準備して情報共有の新しいフェーズに入りつつあることである。

５点目の最後としては、これまで発言があったように大学におけるセキュリティ対策の重要性に触れたほか、初等教育から高等教育まで一貫した人材育成基盤の必要性を明記したことであり、これらの点で大いに共感している。

このように原案は相当なレベルにあると考えているが、サイバーの世界は日進月歩どころか秒進分歩で進んでいる。また、2020年東京オリンピック・パラリンピック競技大会を控えて、

新たな対策の必要が生じるかもしれない。今後はこのような種々の環境変化に対応すると同時に、また、先進国に比べて我が国のレベルを常時モニターし、改善すべき点は年次計画に反映させるといった柔軟な対応を期待している。

○（前田本部員）

今回の「サイバーセキュリティ戦略（案）」については、特に今回は丁寧な準備期間を置き、我々の議論も十分くみ上げていただき、全体に全く異存はない。

ただ、幾つか指摘させていただくと、一つは積極評価であるが、「サイバーセキュリティ戦略（案）」の「4.2.国民が安全で安心して暮らせる社会の実現」の中の７番目の項目に、今回変わった点として大規模サイバー攻撃事態等への対処能力の強化が柱として加わった。これも高く評価したい。

様々な御指摘があったように、非常に速いスピードで動く中で、具体的な攻撃に対して、例えばスーパーコンピューターを活用して防衛するなど、こちらの側も進歩していく必要がある。今まで解析不能でダークウェブに入ってしまったら諦めていたものも、大型コンピューターを使うと尻尾が見えてくる。そういうことに対しての予算について、無駄遣いはいけないが、必要なものには十分使っていただきたい。

また、全本部員が御指摘になったが、基盤になる人材育成に関しては、なかなか進まなかったものの、今回の総理の発言でプログラミングを入試科目に入れることとなった。我々学校の側は入試科目が変わるというと小中高に非常に響くため、非常によかったと思っている。

また、官民データ活用推進基本計画の案に対するサイバーセキュリティ戦略本部の意見（案）に関して、AIや大規模データの活用は、日本が世界に伍して闘っていくために絶対に必要である一方、御指摘のようにセキュリティも重要である。ポイントは、いろいろな側面のセキュリティがあるということ。一つはFacebookのデータが中国の企業に流れているという事例を踏まえて、危険をどのように捉えるかということと、もう一つはデータを１本で捉えるのではなく、データの層を考えて、どのデータはどこまで出すかという視点。データが大きければ大きいほど日本の発展につながるという観点はもちろん認めるものの、官民連携の官のデータをなぜ官が確保してきたかということも踏まえて、どのデータを出して良いかという視点をそろそろ考える必要があるのではないか。セキュリティのことを考える上では、情報通信技術総合戦略室とNISCとの連携をより一層深めていただきたい。

○（村井本部員）

複雑化、巧妙化するサイバー攻撃と事務局から説明があったが、複雑化、巧妙化するのはサイバー攻撃のみならず、そもそも技術が複雑化、巧妙化している。本日AI、IoTという言葉が出てきたが、これもバズワードであり、３年前にはなかった言葉である。ところが、今、全ての産業、全ての領域がAIを使って生まれ変わろうとしている。取り入れようとする動きは非常に速い。

複雑化、巧妙化する技術については、例えば、我々が良い技術をつくると、サイバーセキュリティの世界ではその技術を悪用したり濫用したりする人間が出てくる。これに対してどのように立ち向かうか、どのように準備をするか。これがサイバーセキュリティである。そのため、技術がどのようなところで広がり、どの領域で使われるようになるかを把握し、その悪用を予知して、これを防御するということがサイバーセキュリティでは最も重要である。
大量のデータを使うのが今のAIであるため、これの濫用は、嘘のデータや偽のデータを入れるなどであり、データの品質を高めることが我々にとっては防御になる。この品質管理は日本が得意な分野である。

また、4Kのテレビデータを、インターネットを介して同時配信する実験を来週から実施予定である。これはおそらく、我が国初めての最も大規模な、テレビデータのインターネット配信実験になる。テレビのような大容量のデータと、IoTのようなセンサーのとても小さなデータが複雑に絡まっていく。これをどのようにさばくかということは、5Gというキーワードの一番重要なテーマである。5Gが2020年東京オリンピック・パラリンピック競技大会の開催までに準備できることで、テレビのような大容量でリアルタイムのデータと、センサーのような小さなデータが混在する非常に複雑な処理を、エッジコンピューティングなどを利用しながら全体のトラフィックを調整していく時代に変わっていくため、このことが社会や技術にどのようなインパクトを与えるかという点が課題になっている。

もう一つは、昨今キャッシュレス社会の推進が言われるが、これは言葉がよくないと思っており、ポイントは「キャッシュ」「レス」ではなくて電子的な支払いと決済ができることだと考えている。そうだとすると、ゴールは現金がなくなることではなくて、電子的に支払いと決済ができる社会である。これは全産業に影響がある。お金に関することであり、ここを攻撃された場合にはお金が動く。既に仮想通貨では様々な攻撃が起こっている。

以上のことから、全ての分野でリスクというものが出てくる。5GやIoT、AI等のテクニカルバズワードでどんどん複雑化・巧妙化する技術に対する悪用をどのように防ぐかが重要である。

最後に、アブユーズというのは悪用すると訳されるが、その反対語は何かと考えると、最近技術者の間で未来を語るときに使うethical use、ethicsという言葉ではないかと考えている。これは「良い使い方をする」ということ。これも日本人は得意ではないかと思う。我が国が担わなければならない役割は、技術の進歩と共に様々なものがあるのではないかと思う。

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

本日、報告があった平昌大会の状況からも、サイバーセキュリティ対策を積極的に進めていくことが必要と考える。

このため、現在、大会に影響を与える重要サービス事業者等のリスク評価やサイバーセキュリティ対処調整センターの構築を推進中である。

また、これまでサイバーセキュリティ戦略本部の副本部長として、次期戦略や統一基準群の検討を進めてきたが、2020年東京オリンピック・パラリンピック競技大会の成功とその後を見据え、今後は具体的な施策の着実な実施が重要と考えており、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）

国民にとってサイバー空間がより身近なものとなる中、国民生活の安全・安心を確保するためには、全ての主体が連携・協調してサイバーセキュリティの確保に取り組むことが重要である。

本日の討議を踏まえ、関係省庁や重要インフラ事業者等と連携した対策を推進するとともに、情報収集・分析態勢の強化、事案発生時における対処能力の向上、警察におけるより堅牢な情報セキュリティの確保等に努めるよう、警察庁を指導してまいりたい。

○（野田総務大臣）

総務省では、サイバーセキュリティ対策を強化するため、昨年公表した「IoTセキュリティ総合対策」や、今国会で成立した「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を改正する法律」に基づき、必要な取組を進めている。

これらの施策は、新たに策定されるサイバーセキュリティ戦略にも位置づけられており、引き続き着実に取組を進めてまいりたい。

サイバーセキュリティ対策を進めるに当たっては、セキュリティ対策を牽引するいわゆるトップガンも含めたサイバーセキュリティ人材の育成が、特に重要な課題であると認識している。

2020年東京オリンピック・パラリンピック競技大会まで後２年しかない。大会後も見据えた人材の育成について、政府を挙げて全力で取り組んでいく必要があると考えている。

○（世耕経済産業大臣）

経済産業省では、５月30日、第２回産業サイバーセキュリティ研究会を開催し、サプライチェーンサイバーセキュリティ強化、サイバーセキュリティ経営強化、サイバーセキュリティ人材の育成・活躍促進、サイバーセキュリティビジネスのエコシステム創造の４つのパッケージを柱とする、「産業サイバーセキュリティ強化へ向けたアクションプラン」を提示した。これらの内容が「次期サイバーセキュリティ戦略（案）」に反映されていることを高く評価している。

この戦略を踏まえつつ、アクションプランに基づき日本のサイバーセキュリティ対策強化に取り組んでまいりたい。

○（小野寺防衛大臣）

先月、タリンのNATOサイバー防衛協力センターを訪問し、所長ほか幹部と会談した。今回、

同センターへの防衛省職員の派遣に関して合意をしている。今後、私どもとしてもタリン・マニュアルの議論に積極的に参画していきたい。

また、先月、米軍はサイバー軍を独立した統合軍に昇格させ、その司令官に国家安全保障局長であった日系のポール・ナカソネ陸軍大将が就任した。防衛省としても米軍や関係各国との協力、国際機関との連携、協力を強化するとともに、自衛隊のサイバー防衛対応能力強化に努力し、官民連携をしてまいりたい。

○（松山情報通信技術（ＩＴ）政策担当大臣）

現在、IT戦略本部の下で行政サービスの100％デジタル化など、世界最先端デジタル国家の創造に向けた取組を急ピッチで進めている。その際、IT利活用とサイバーセキュリティの双方を車の両輪として、ITを活用した社会システムの抜本改革を行うことが重要と考えている。

今後も引き続き、IT戦略本部とサイバーセキュリティ戦略本部が緊密な連携を図りながら、我が国のデジタル改革を推進してまいりたい。

○（堀井外務大臣政務官）

外務省としても、「次期サイバーセキュリティ戦略（案）」において、我が国の安全保障を脅かすようなサイバー空間における脅威に対し、取り得る全ての有効な手段と能力を活用し、断固たる対応をとるとの意思を改めて国内外に示したことを歓迎する。

昨年５月に起きた「ワナクライ」大規模サイバー攻撃事案について、我が国は同事案の背後に北朝鮮の関与があったことを非難する声明を関係国とともに発出した。

今後も有志国、関係省庁及び民間部門と緊密に連携しつつ、悪意あるサイバー活動を抑止する取組を進めてまいりたい。

（３）決定事項の決定等

決定事項３件につき、案のとおり決定した。

（４）本部長締め括り挨拶

活発な御議論、そして大変貴重な御意見をいただき、厚く感謝申し上げる。

ただいま御決定いただきました次期戦略案と政府機関等の対策基準の見直し案については、今後パブリックコメントを行い、その結果を踏まえ、速やかに決定できるよう検討を進めていく。

有識者の皆様には、引き続き御協力のほど、お願い申し上げる。

－　以上　－