サイバーセキュリティ戦略本部
第19回会合　議事概要

１　日時

平成30年7月25日（水）　　９：00～９:40

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
河野　太郎	外務大臣
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
小野寺　正	ＫＤＤＩ株式会社相談役
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
三輪　昭尚	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。

本日の会合では、次期サイバーセキュリティ戦略関係で４件、その他、政府の統一基準の改定や重要インフラ行動計画の改定など４件について、さきに行ったパブリックコメントの結果などを踏まえ、御審議をいただきたい。

限られた時間であるが、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関係＞

・次期サイバーセキュリティ戦略（案）について

・サイバーセキュリティ 2018（案）について

・サイバーセキュリティ政策に係る年次報告（2017 年度）（案）について

・サイバーセキュリティ関係施策に関する平成 31 年度予算重点化方針（案）について

＜その他＞

・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改定（案）について

・重要インフラ分野の追加に伴う「重要インフラの情報セキュリティ対策に係る第４次行動計画」の改定（案）について

・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（初版）（案）について

・国立研究開発法人情報通信研究機構の中長期目標の改正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

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。

○（中谷本部員）

今回の「次期サイバーセキュリティ戦略（案）」を全般的に支持したい。

その上で、４点申し上げる。

第１に、安全保障の現実の文脈との関連で特に注目したいのが、資料１－６の34ページにあるように、Ｇ７（ルッカ）宣言を踏まえて、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ついて、同盟国・諸外国とも連携し、断固たる措置をとると指摘していることである。対応措置の内容は、経済的な措置を中心としつつ、状況に応じて多様であると思うが、実効的な対応を迅速に採れるように、オールジャパンでの取組を一層進めていただければと思う。

第２に、今回、重要インフラ分野に空港が追加され、民間事業者が運営する主要空港が重要インフラとなったことを歓迎したいと思う。空港は物理的なテロの標的に最もなりやすい施設であると同時に、サイバー攻撃の対象にもなりやすいため、今回の決定を機に、空港のサイバーセキュリティの一層の強化が望まれる。また、港湾については、所有・運営形態が複雑であり、コンテナ物流で既にカバーされている港湾も相当あると思うが、遺漏なく重要インフラに今後指定していくことが重要であると思う。その他にも重要インフラに速やかに指定することが望ましい分野があるとも思うため、関係省庁においては適切な対応をお願いしたい。

第３に、資料１－６の21ページに、国際海底ケーブル等のインフラ設備の防護の強化を含めた整備を促進する旨が明記されたことを評価したい。海底ケーブルの切断を始めとする攻撃がなされないように、また、万一なされた場合でも速やかに復旧できるように対応を整えておくことは、サイバー空間の円滑な利用を保障する上で極めて重要であると考える。

第４に、資料１－６の24ページに、政府機関等のIT投資の効率化によって得られた原資をセキュリティ強化に充当する旨を明記したことは、IT投資の効率化に良いインセンティブを与える意味でも望ましい合理的な方針であると考える。

○（小野寺本部員）

「次期サイバーセキュリティ戦略（案）」、「サイバーセキュリティ2018（案）」、「サイバーセキュリティ戦略に係る年次報告（2017年度）（案）」、そして「サイバーセキュリティ関係施策に関する平成31年度予算重点化方針（案）」については、全て賛成である。

その上で、３点申し上げる。

１点目は、「次期サイバーセキュリティ戦略（案）」は全体的によく取りまとめられており、戦略そのものは毎回大きく改善してきていると思う。また、サイバーセキュリティ戦略に基づく年次計画も毎年改善されている。これはNISCの現状認識が正しく反映されていると思っており、NISCの努力に感謝申し上げる。同時に、関係省庁の理解が進み、記載している点も多くあるのだろうと思う。しかし、実際のところ、NISCはもう少し記載したいと考えていながら、関係省庁の理解が得られず、記載できていない点があるのではないかと思う。サイバーセキュリティに関しては、NISCが圧倒的に情報を持っており、閣僚の皆さんにはNISCのこの点を是非お考えいただき、可能な限り具体的な記載ができるようにしていただきたいと思う。

２点目は、サイバーセキュリティ分野は他の分野に比べれば政府として統一的な動きができていると思うが、予算制度の関係もあり、個々の施策が実行段階になると、各省庁が独立して行われる傾向があることは否めないと思う。その際に、その施策を実施すること自体が目的化されることのないように、サイバーセキュリティ戦略として全体が有機的に連携して機能させるように、NISCが適宜確認し、必要に応じて軌道修正が行われるようにしていただきたい。

３点目は、サイバーセキュリティ政策に係る年次報告（2017年度）（案）にも記載されているように、ハッカーと呼ばれる犯罪者の低年齢化が進んでいる。幸いにも、安倍総理の指示で、初等中等教育からのプログラミング教育の必修化が始まるが、初等中等教育の中で、サイバー

時代のモラルをどのように教えるのかは大きな課題だと思う。文部科学省が中心になり、各界の知恵を集めて、効果的な教育をぜひ検討していただきたい。

○（野原本部員）

今回の決定事項については、十分に検討を重ねてきた内容であり、このとおりで全て異存はない。しっかりしたサイバーセキュリティ戦略ができたと評価している。今後は、この戦略を基に、具体的な施策に落とし込み、着実に推進していくことが重要であり、人材育成、普及啓発アクションプランなどを含め、しっかりチェックしていく必要があると考えている。

その上で３点申し上げる。

１点目は、多様な主体の情報共有・連携の推進についてである。サイバーセキュリティ基本法の改正案は、今回の通常国会では審議できず、残念ながら成立しなかったが、速やかに成立させていただき、それに基づいてサイバーセキュリティ協議会を創設し、官民の様々な主体が安心して相互にサイバーセキュリティに関する情報を共有し、その結果としてサイバーセキュリティ対策が向上し、強くなるようにお願いしたい。

２点目は、サイバーセキュリティビジネスの強化が重要という点である。サイバーセキュリティ対策レベルを向上させるためには、質の高いセキュリティ製品やサービスが提供されている環境が重要である。そのために経済産業省を中心に、製造事業者や重要インフラ事業者、サービス事業者といったニーズを抱える事業者と、セキュリティベンダー等のシーズを持つ事業者をマッチングするコラボレーションプラットフォームを設置するといったプロジェクトも行うと伺っている。こうしたプロジェクトを通じて、セキュリティビジネス環境の整備を行うと伺っており、是非充実した検討を行い、有効な施策を進めていただきたい。

３点目は、先ほど中谷本部員からも発言があったように、政府機関等のセキュリティ強化・充実のために必要な予算を十分に確保すべきという点である。資料１－６の24ページには、政府機関等のIT投資の効率化により得られた原資をセキュリティ予算に充てるという記述もあるが、それはやりくりの提案であり、それだけではなく、政府機関が何をしなくてはいけないのか、そのためにどれだけ予算が必要なのかということを十分に説得し、必要かつ十分な予算を確保することが重要だと考える。

○（林本部員）

「次期サイバーセキュリティ戦略（案）」に関連する２点についてコメントをさせていただく。

まず、戦略そのものは、事務局で練った上で関係省庁と十分協議され、また、私たちも複数回にわたって討論に参加させていただいた上、パブリックコメントをも経たもので、そのプロセスごとに論点が明確になってきたと思う。とりわけ積極的サイバー防御の観点から資料１－６の「4.3.　国際社会の平和・安定及び我が国の安全保障への寄与」が、現行の戦略よりも、より具体的かつ詳細になり、方向性が明確になった点を評価する。今後の実践を通じて具体的

成果となって現れることを期待している。

同じように、インシデント情報の共有についても、第２フェーズに入ったとも言われるような進展が見られたことにも注目している。電気通信事業法等の一部改正法は既に成立し、情報通信研究機構等でIoT端末等の脆弱性を検知して、その情報を資格のある電気通信事業者等と共有する仕組みが導入された。そして本日の資料７にあるとおり、NISCの意見も生かしつつ、運用が開始される。また、野原本部員から発言があったサイバーセキュリティ協議会については、これが産業や分野の壁を乗り越えるものだということに注目している。中央官庁、地方自治体、重要インフラ事業者、サイバー関係事業者、教育研究機関などが積極的に参加するもので、また、同種の海外の機関との連携等を通じて、セキュリティ対策の第一歩である情報共有を抜本的に強化するものと思う。この基本法であるサイバーセキュリティ基本法の改正が早期に実現すること等に伴って、情報共有の更なる高みに登ることに期待をしている。

○（前田本部員）

「次期サイバーセキュリティ戦略（案）」については、パブコメを踏まえ、非常に密度の高い、今までで一番レベルの高いものができ上がっているという印象を持った。

2020年東京オリンピック・パラリンピック競技大会を成功させることは、サイバーセキュリティのいわばショーウインドーや、看板のようなものであり、ここで失敗してはいけないということだと思う。着々と準備が進められており、その主体として自治体、スポーツ団体、そして各官庁があり、その上に内閣がある構造である。単線的なものにすれば良いということではないと思うが、これを機に、新しい組織のスタイルができてくればと思う。

2020年東京オリンピック・パラリンピック競技大会と、更にその後を見据えて、考えていかなければいけないところに差しかかってきている。そのうえで痛切に感じることとして、非常に細かいことではあるものの、私は刑事法の学者なので申し上げる。例えば、DNA鑑定というものは非常に大事な手法ではあるが、今度大きく変わるかもしれない。DNA鑑定はアメリカが一手に握っていて、やり方を変えたら、もうその試薬は日本に売らないと言ってくる可能性がある。サイバーの世界でも、GoogleとEUの間で様々なことがあるように、ノウハウを出さないといったこともあり得る。

やはり真剣に考えなければいけないことは、この場でも何回も申し上げているが、セキュリティ人材だけではなくて、科学技術の基本を支える人材も含めた人材育成である。先ほど小中学校からの教育に関する発言にもあったが、更に裾野を広げていかなければいけない。腰を据えてこうした人材育成の議論をする一つのタイミングとして、2020年東京オリンピック・パラリンピック競技大会の後は、一段落つくため、その前からこうした議論をしていただきたい。

AIを始め、様々な大きな潮流の中で、人材が何より大事であるが、理系分野だけではなくて、日本の優れたところは、規制をし、マネージができている点である。事前規制というと評判が悪く、規制緩和して事後救済に変えろといった意見もあるが、原発にしろ、サイバーにしろ、起こってから考えれば良いということだけではない。起こらないようにシミュレーションする

官僚の能力の高さは、日本は世界に冠たるものがあり、その意識は持って、理系分野と併せ人材育成を考えていただきたい。

その軸はやはりNISCなのだと思う。今まで何回も申し上げてきたが、縦割りの各省庁の中で、唯一、NISCは非常にうまくいっている。まだ規模が小さいものの、様々な人材を集めて、新しい施策を作っていく必要がある。2020年東京オリンピック・パラリンピック競技大会が成功する中で、次の日本の基盤になるような政策を作っていっていただきたい。

○（村井本部員）

資料１－６の21ページに重要なことを書いていただいたので、その点について申し上げる。

21ページには「国際海底ケーブル等のインフラ設備の防護の強化」と記載されている。今、国際海底ケーブルに関する問題が大変大きな話題になっており、私は長い間このことを政府の様々な部署で話をしているが、なかなか扱っていただけない部分があったため、ここに書いていただいて大変感謝している。

北極海の氷が解けたため、光ファイバーを敷設して、日本とヨーロッパを結ぶルート、及び日本とアメリカ東海岸を結ぶルートが、海底ケーブルだけで実現できるようになった。日本とニューヨークを結ぶには、今まではロシアを通るかアメリカ大陸を渡る必要があったが、このようなルートができるようになった。

今、主たるルートは、日本から太平洋を経由しアメリカの北の方を結ぶ北側のルートと、台湾の横の海域を通ってシンガポール経由で結ぶ南側のルート、これらが日本の生命線だったが、今、ここに大きな変化が生まれている。一つは北極海の関係で、北側の新しいルートができるということであり、南側の方も、近隣の状況を鑑みて、ハワイからグアムを経由して日本を結んでいたグアムルートという海底ケーブルがあり、遠いルートになるものの、検討されるようになった。これはアメリカも非常に真剣に考えているところである。

つまり、ケーブルのトポロジーと、言わば政治のトポロジーとの関係で、このサイバースペースをどう考えていくかということになる。これはヨーロッパの大学ではジオポリティクスの学部がコンピューターサイエンスやネットワークのトポロジーに加えて研究をするようになっており、サイバートポロジーとジオトポロジーとの関係をしっかりと考えていくということが進んでいる。

一方で、問題はこれらのことを誰が責任を持つのかということである。外務省も関係があり、総務省も関係があり、もちろん安全保障としても関係がある。このことを誰が担当するかということに対しては、やはり力を合わせられる体制を持って、地球全体にどのようなデータの流れる道があって、どのように使われているのかを日本として考えていかなければいけないと思う。

もう一点、私は知的財産戦略本部で漫画とアニメの海賊版対策の委員会の共同座長を仰せつかっているが、漫画とアニメは、日本の大切な宝である。ただ、この問題を解決するためには、出版事業、法制、行政、それから、海賊版サイトは海外で運用されることが多いため、国際関

係の調整も非常に重要になってくる。そして、通信事業者も力を合わせないと、一つの技術では解決できない。つまり、皆がよく理解をして力を合わせなければいけない課題になっている。今、サイバーセキュリティは全ての分野、ここにいらっしゃる方々からすれば、全省庁の守備範囲の分野の課題になっているということのいい例だと思う。こうした課題に関する情報共有をこの本部のような場でしていただいき、力が合わせられる体制作りを進めていただきたい。

○（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））

昨日、2020年東京オリンピック・パラリンピック競技大会まであと２年という節目を迎えた。

大会の成功に向け、現在、リスク評価と対策の促進、演習の実施、脅威情報の共有等を担うサイバーセキュリティ対処調整センターの構築を推進しており、大会におけるサイバーセキュリティ確保に万全を期すべく取り組んでまいりたい。

本日の議題である「次期サイバーセキュリティ戦略（案）」については、大会の成功とその後を見据え、これまでの議論を踏まえた各種施策が盛り込まれている。

サイバーセキュリティ戦略本部の副本部長として、これまでの皆様の御尽力に感謝申し上げるとともに、これらの各種施策を関係府省庁において積極的に推進していただくよう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）

サイバー空間と実空間の一体化が進む中、サイバー空間の脅威への対処無くしては、国民生活の安全・安心は確保できない状況となっている。

本日の決定事項等を踏まえ、サイバー空間の脅威への対応強化、警察における組織基盤の更なる強化、国際連携及び産学官連携の推進に努め、2020年東京オリンピック・パラリンピック競技大会及びその後の社会を見据えた戦略的なサイバーセキュリティ対策を推進するよう、警察庁を指導してまいりたい。

○（野田総務大臣）

総務省では「IoTセキュリティ総合対策」に基づき、サイバーセキュリティ対策に取り組んできたが、2020年東京オリンピック・パラリンピック競技大会に向け、今後は、官民の総力を結集して対応する必要があると考えている。

特にIoT機器が急速に普及していく中、サイバーセキュリティ上の脅威に対抗するには、関係者の連携・協働による対策が必要不可欠である。

この点、サイバーセキュリティ分野に深い知見を有しているNICTは、その先進的な研究の成果を活用してIoT機器の脆弱性の調査を行うことを予定しており、総務省として、関係省庁、電気通信事業者、機器製造事業者等とも連携しつつ、IoT機器のセキュリティ対策に取り組んでまいりたい。

本調査の実施状況については、今後、可能な限り、サイバーセキュリティ戦略本部に報告さ

せていただく。

○（河野外務大臣）
国家の関与が疑われるものも含め、サイバー空間における脅威がますます深刻化する中、今後我が国を含む国際社会にいかなる事態が生起するか、予断を許さない。「次期サイバーセキュリティ戦略（案）」には新たに「抑止」の概念が盛り込まれたが、外務省としても、深刻なサイバー事案に対し、有志国または国際社会と連携して、最大限の実効的な対応を取り得るよう、国際法を始めとする法的論点の整理も含め、検討を加速させる考えである。
また、外務省としては引き続き「自由、公正かつ安全なサイバー空間」の実現に向け、関係国・関係省庁・民間企業との協力の下、サイバー空間における法の支配の推進、信頼醸成措置の推進、能力構築支援を含むサイバー外交に鋭意取り組んでまいりたい。

○（世耕経済産業大臣）
「次期サイバーセキュリティ戦略（案）」には、経済産業省が５月に提示した「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」がしっかりと反映されており、感謝申し上げる。
これを受け、経済産業省では、中小企業がトラブルなどについて相談できる仕組みの強化や技術・サービスの適切な評価に係る仕組みの構築によるサイバービジネスの振興などに取り組んでまいりたい。
「次期サイバーセキュリティ戦略（案）」では、政府のIT投資の効率化によって得られた原資をセキュリティの取組に充てる方針が示されているが、今後、予算編成の中でこれを具体化していくことが重要であると考える。

○（小野寺防衛大臣）
防衛省・自衛隊では、これまでに米軍サイバー部隊との共同訓練を始め、NATO多国間サイバー演習「サイバーコアリション」演習や「ロックド・シールズ」演習に参加するなどサイバー防護に係る訓練を実施してきた。また、NATOのサイバーセンター（CCDCOE）に、防衛省の専門家を今年度派遣する。
今後、次期サイバーセキュリティ戦略に沿って、積極的サイバー防御の観点から、自衛隊サイバー防衛隊が保有するサイバー演習環境を活用した対抗戦を実施するとともに、他省庁のシステムにハッキングを試み、脆弱性の確認を行うペネトレーションテストを実施するなど、政府全体のサイバー攻撃に対する防御力、抑止力、状況把握力の向上に貢献してまいりたい。
また、こうしたサイバーセキュリティ戦略の内容は、本年末に策定する新防衛大綱・次期中期防にも反映させ、我が国のサイバー能力を着実に整備してまいりたい。

○（松山情報通信技術（IT）政策担当大臣）

IT政策担当大臣として、先月６月15日に「世界最先端デジタル国家創造宣言・官民データ活用推進基本計画」をIT戦略本部で決定した上で、同日に閣議決定した。

本計画では、デジタル技術とデータの利活用を通じて、安全・安心で豊かな社会の実現を目指している。

本計画実施に当たっては、IT利活用とサイバーセキュリティ双方を強力に推進することが必要であり、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の緊密な連携を図ってまいりたい。

（３）決定事項の決定等

決定事項８件につき、案のとおり決定した。

（４）本部長締め括り挨拶

本日、サイバーセキュリティ戦略（案）を決定することができた。貴重な御意見を賜り、有識者本部員の皆様には感謝申し上げる。

現行戦略を決定して以降、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、様々な恩恵がもたらされた一方で、サイバー攻撃により多大な経済的・社会的損失が生じる可能性が飛躍的に高まっている。

新たな戦略はこのような認識の下に、今後３年間に取り組むべき施策を取り入れたものである。全ての主体がサイバーセキュリティに関する取り組みを自律的に行い、サイバー空間が持続的に発展していくよう、個人・組織の参加、連携・協働を進めてまいりたい。

経営者の意識改革を推進し、サイバーセキュリティの費用から投資への転換を図るほか、脅威に対して事前に対策を講じる積極的サイバー防御を推進する。さらに、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対策も見据えて、サイバーセキュリティ対処調整センターや、従来の枠を超えた官民による新たな情報共有・連携体制を構築し、効果的に運用してまいりたい。このほか、高度人材の育成、サイバー攻撃の検知・防御能力の向上に向けた研究開発、積極的な情報発信等、横断的施策を推進する。

NISCを中心に次期戦略を確実に実施するよう、各府省の積極的な取り組みをお願い申し上げる。

－　以上　－