サイバーセキュリティ戦略本部
第11回会合　議事概要

１　日時

平成29年1月25日（水）　８：30～９：30

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
丸川　珠代	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
松本　　純	国家公安委員会委員長
世耕　弘成	経済産業大臣
稲田　朋美	防衛大臣
鶴保　庸介	情報通信技術（ＩＴ）政策担当大臣
あかま 次郎	総務副大臣
岸　　信夫	外務副大臣
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長・教授
萩生田 光一	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

早朝から御参集いただき、感謝申し上げる。

本日、御議論いただきたいのは次の２点である。

１点目は、「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」のパブリックコメント案についてである。前回の会合では、2020 年東京オリンピック・パラリンピック競技大会を見据え、国民生活の基盤となる重要インフラの防護のための行動計画について、見直しの方向性を御議論いただいた。これを踏まえ、パブリックコメント案を作成したため、御意見を賜りたい。

２点目は、「サイバーセキュリティ政策の在り方について」である。一昨年９月に策定した「サイバーセキュリティ戦略」は、策定後、３年程度の間に実施するべき政策を取りまとめたものであり、来年に見直しの時期を迎える。また、日本年金機構に対する悪質極まりないサイバー攻撃による個人情報の流出を受けて、昨年の通常国会で成立した改正サイバーセキュリティ基本法については、国会の附帯決議で施行後２年以内に見直しの必要性を検討することになっており、来年までには結論を得る必要がある。

本日は、これらの点について、今後の検討の進め方について御議論を賜りたく、活発な御討議をお願い申し上げる。

(2)　討議

【決定事項】

・　「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」のパブリックコメント案について

【討議事項】

・　サイバーセキュリティ政策の在り方について

【報告事項】

・ 2020 年東京オリンピック・パラリンピック競技大会のサイバーセキュリティの確保に向けたリスク評価への取組状況
・ 2017 年サイバーセキュリティ月間について
・ 政府のサイバーセキュリティに関する予算（2017 年度政府案）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）４点申し上げる。

第１に、「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」案の３つの重点はいずれも重要なものであって、大いに推進していただきたい。特に、情報共有体制の強化のためのホットライン構築は、緊急時対応にとって不可欠な重要性を有するものであり、可能な限り早期に確立することを強く求める。

第２に、大学等のセキュリティ水準向上支援について、私自身は、安全保障輸出管理について経済産業省で検討する機会があったが、大学の安全保障輸出管理には温度差があ

り、一部の大学の対応はまだ十分とは言いがたい面がある。サイバーセキュリティについても同様ではないかと懸念している。大学に対しては、できれば安全保障輸出管理対応とサイバーセキュリティ対応を有機的にリンクして、合理的な対応を進めていただくのがよいのではないか。

第３に、IoT セキュリティの国際標準化の推進について、ISO（国際標準化機構）などにおいて、日本及び日本企業がこの分野での国際標準化を主導することを強く望む。

第４に、ロシアがサイバー手段により米国大統領選挙に干渉したとして、米国が昨年末にロシアの外交官を国外退去処分にしたという事件について、ここから得られる教訓としては、第１に、我々としても、ロシアに限らず外国がサイバー攻撃を仕掛ける可能性が常にあるという前提で、緊張感を持ってサイバーセキュリティを推進する必要があるということ。第２に、サイバー攻撃に対する主たる手段は、経済上の措置と外交上の措置であるため、万一サイバー攻撃を受けた場合には、これらの措置を遅滞なく発動できるように体制を整えておく必要があることだと考えている。なお、一連の外交上の措置は、国際法違反の存在を前提とすることなく、国家が裁量的に発動できる措置であることに留意する必要があることを申し上げておきたい。

○（野原本部員）大きく２点申し上げる。

最初に、重要インフラのサイバーセキュリティの情報共有体制の強化について、重要インフラのサイバーセキュリティ対策では、インシデント情報や共有情報を速やかに共有し、類似被害の拡大を防ぐことが重要である。そのために情報共有体制の充実・強化が極めて重要であり、「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」の案でも、「サイバーセキュリティ政策の在り方」の検討においても、最も重要なテーマとして位置づけられている。

しかし、実際には、個々の事業者から見ると、マルウェア感染や被害の情報を共有したくないと考える事業者もおり、十分な情報共有がなされているとまでは言えない。今回の行動計画の内容を見ても、少し具体性や実現力、スピード感に欠けるのではないか。情報共有体制の強化・充実は喫緊の課題であるため、実行力のある形でしっかり取り組んでいただきたい。

具体的には、３点の施策をお願いしたい。

第１に、分野ごとに民間主導で情報共有を行う ISAC を、それぞれの分野で設立していただく方向で進めていただきたい。金融 ISAC、情報通信では ICT-ISAC など分野によってはISAC があるが、それ以外の医療、水道、物流、航空、鉄道などの分野には ISAC 等がないので、ぜひ充実させていただきたい。

第２に、ISAC は、まずは民間の中できめ細かな共有を行い、そこから先は NISC が中心となって、省庁や分野横断的な情報共有の体制を作るということを今回は強調しているが、共有すべき情報を明確化し、しっかりと取り組んでいただきたい。JPCERT/CC 等の専門機関を活用することで、より事業者の方に情報提供しやすくするという形も重要なのではないか。

第３に、インシデント情報を適切に共有し、被害の拡大や連鎖を防ぐように行動することは、全ての組織にとっての社会的責任だということを明確にし、啓蒙をしていくことが

重要である。そのためには、それぞれの役割分担や責任を明確化して、必要に応じて制度化すべきではないか。米国では、2015 年 12 月に成立したサイバーセキュリティ法で、DHS（米国国土安全保障省）がサイバーセキュリティ情報を自動的に取得することも認められたという経緯もあり、昨年４月に、DHS は重要インフラのサイバーセキュリティの情報共有を迅速化するため、新しいシステムの導入を検討すると発表している。これは、サイバーセキュリティの情報共有を自動化するシステムの導入であり、ここまで米国の場合は踏み込んでいることから、我が国でもしっかりと取り組んでいただきたい。我が国の法制度は異なるが、迅速な情報共有の重要性をしっかり認識して、実効性のある体制をスピーディーに実現していただきたい。

もう一点、議題の２つ目であるサイバーセキュリティ政策の在り方の検討において、今回は重要インフラの分野と IoT のセキュリティ強化について主眼を置いているが、できれば重要インフラを主眼に置くというよりも、企業全体の中の重要インフラ、のように強弱を変えたほうがいいのではないか。また、人材育成等についても触れて、重視するべき点は入れ込んでおく必要があるのではないか。引き続き今後も議論していきたいと思う。

○（林本部員）先ほど野原本部員が発言されたアメリカのインシデント情報の共有の仕組みと、EU の仕組みができたということを前回の会合で紹介したが、さらにその後、11 月末には、イギリスで Investigatory Powers Act 2016 が成立したので、昨年は３つの国でサイバーセキュリティに関する新しい制度枠組みが生まれた。

本年は、米国の新大統領の誕生のほか、EU 圏内の複数の総選挙や英国の EU 離脱など、政治的にも大きな変化があって、サイバーセキュリティにも影響すると思われる。また、先ほど話題になった米大統領選挙へのサイバー攻撃に象徴されるように、従来では考えられなかったような異例の展開も予想されると思う。

こうした予期せぬ変化に対応できる体制をつくることは大変重要であるが、一方で、サイバーセキュリティは日常業務における情報の安全をどうやって守るかということを粛々と実行するという、地道で継続的な作業でもあると思う。大きな変化に鈍感であってはいけないが、着実な実行をおろそかにすることもいけないと思う。

本日の大きな課題である決定事項の「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」のパブリックコメント案と、討議事項の「サイバーセキュリティ政策の在り方について」は、いずれも時宜を得たテーマ設定だと思い、両者をあわせてコメントするが、その要点は、統合化と個別化の調和という点になる。

まず、統合化については、サイバーセキュリティがどの産業にも、どの地域にも、あるいはどの組織や個人にも起き得るものである以上、何らかの統合化が欠かせないと思う。保証すべき対象を機能保証とすることや、重要インフラ 13 分野を中心にしつつも、2020 年東京オリンピック・パラリンピック競技大会の対策としては 19 業務を対象にするという原案は妥当なものだと思う。深刻度といった指標で、分野横断的な手続の標準化を施行するとなると、概念や用語や手法の統一化も必要になってくると思う。

しかし、他方で、重要インフラに限ったとしても多くの産業等を網羅しており、それぞれに固有の事情もあると思う。例えば、プラント型のスタンドアローンの産業と、ネットワーク型で全国的な展開のビジネスでは、リスクも対応も違ってくる。ネットワーク型に

限っても、運ばれたり処理されたりする対象が人や物である有体物の輸送型なのか、エネルギーといった無体物の輸送なのか、さらには、情報そのものの伝達なのかによって大きく３つに分かれると思う。

また、対策の基本として、サービスを止めることを優先するのか、ベストエフォートで継続することを優先するのか。さらには、人命に危害が及ぶかどうか、対策を専門家に委ねたほうがいいのか、全員参加が必要になるのかは、産業によって差が生じ、結果的に産業別にセキュリティ文化の差を生んでいると思われる。

この点について、私自身もいろいろな経験をしている。例えば、安全工学会という主として化学プラントの安全を研究されている学会の会員向けに、情報セキュリティの特集を企画したときには、保安という側面を重視する会員の方々と、私どものようにビジネスコンティニュイティー（事業継続）を当然視する発想とがかみ合わなかったように感じた。同じように、私が属しているリスク研究ネットワークという研究集団でも、それぞれの業界の専門用語がどこまで同じでどこから違うのか、いまだに判然としないところもある。

まずは横通しによって標準的な対処方針を仮設定した後で、個々の事情を参照しつつ改定していくというプロセスが、時間がかかるように見えても急がば回れの格言にマッチするのではないかと思う。米国 FEMA におけるナショナル・インシデント・マネジメント・システムなどの前例を生かしつつ、我が国の環境にフィットした分野横断的でありながら個別事情を勘案したシステムを志向するということは、十分可能と思うため、そのような方向で検討されることを期待する。

○（前田本部員）刑事法の学者の立場から申し上げる。

第１に、決定事項の「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」のパブリックコメント案については、非常によくできたもので異存はない。日本サイバー犯罪対策センターなども関係主体に位置づけていることは、非常に高く評価できる。

第２に、「サイバーセキュリティ政策の在り方について」申し上げる。林本部員が発言されたことと同様ではあるが、国際社会の変化は、地球規模の動きを感じており、サイバー攻撃が経済上のみならず、政治、治安上の脅威を増している。情報共有が重要なことは誰しも異存がないものの、国内はともかく国際的には、誰と、どこの国と、どうやって情報共有するのかという議論まで踏み込む必要があると思う。今までの方向性はアメリカについていけば良いというものであったが、アメリカが本当に今までどおりなのか。そういう問題は外務省や国家安全保障会議などの議論であり、口を出すことではない面もあるが、そこでの結論がどうなろうと、大事なのは情報共有をするときの主体としての日本である。

日本のサイバーセキュリティ力を強化する上で、主体性を持つということが一番重要である。どのような時代になっても、これが根底である。前から何回か申し上げているが、国際的なレベルの側からも明らかになってきており、下の刑事の検察レベルでもかなり変化してきていると思うのは、サイバーセキュリティの概念の変化である。

私が 15～16 年前から感じていたことは、サイバーセキュリティは地震対策とか大災害対策に近い認識ということである。地震発生時に対処するために防災訓練を行う。その前に建物をいかに強固にするか、情報をいかに集めるか、地震の発生を防ぐという発想はな

い。地震は防ぎようがない。

サイバーの問題も防ぎにくい。情報を集めるといっても、海の中に落ちているくぎを拾うようなものだという感じが強かったが、それが変わってきたと思う。それぞれの国がそれぞれの形で情報を集める。したがって、情報共有は大事だが、それの分析とそれに基づく対応力が必要だと思う。

もちろん一方で、AI の進歩や IoT に関しての日本の技術力を世界に冠たるものにしていく。それを維持するということは、車の両輪の一方のようなもので、非常に大事だが、それだけを取り組んでいれば、日本がサイバーセキュリティにとって重要な位置を占めていけるのか。アメリカとの距離がどのようになろうと、無駄にならないものは、インテリジェンスの問題とつながった形のサイバーに対する意識である。国家としてそこにどれだけ投資していくかである。

テロ等準備罪も我々専門家から見たら、あって当然のものだと思う。2020 年東京オリンピック・パラリンピック競技大会に向けて必要だというのも良いが、これだけ国際環境が大きく変化する中でサイバーセキュリティを考えるときに、そういうコンテクストの中でテロ等準備罪も考えていければ、この議論の話題からちょっとずれてしまうが、基本的には、日本で大きな変化が生じる際は、国益を守ることの重要性をより意識せざるを得なくなってくる。そのときに、サイバーセキュリティは非常に大きな国益だということを申し上げておく。

○（村井本部員）決定事項と討議事項とで一つずつ申し上げる。まず、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（案）の概要の１ページ目を見ていただくと、「①先導的取組の推進（クラス分け）」という重点施策がある。これは重要インフラなどの事業者ごとにしっかりとした ISAC 等を設立した上で、それをどのように連携させるかを説明しているが、一方で、10 ページ目を見ていただくと、セプターとセプターカウンシルというものがある。セプターとは、DHS が ISAC を設立したことを受けて、日本ではどうするべきかということを議論して定めた、NISC と事業者で構成された、各分野で情報共有をするための仕組みである。国との連携、情報の共有をするために、トップダウンで領域を定め、各セプターと連携する。１ページ目に戻っていただくと、ISAC という本来 DHS が使っていた名称だが、この ISAC を強化して展開をしていく。そうすると、おそらく一番重要なことは、各事業分野のグループと国との情報共有が、セプターと ISAC ではそれぞれどのようになされるかの違いである。セプターと ISAC はそれぞれ活動していくように見受けられるが、アメリカの DHS のセプターも ISAC も、事業者との情報共有はなかなか難しい。そうすると、セプターと ISAC を２つに分けて進める体制の運用に気をつけ、実態としてトップダウンで分野を設けたものと、事業者ごとに取り組んでいることが両立していくということを確実に進めていくべきである。ISAC という言葉とセプターという言葉を運用上わかりやすくしていくことは、とても重要ではないか。

もう一点は、今後の政策について。私は 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このような計画ができ、見直しに対する準備が今から始まり、基本法等の体制ができるということは大変重要だと思う。なぜなら、例えば以前、情報産業は６次産業と産業論で言われていたことがある。これは１次産業と２次産業と３次産業を掛け合わ

せて６次産業になるということである。このことは、情報産業の時代になると大変大きな意味を持つ。１次産業が情報によって生まれ変わり、流通、その他サービスの産業に生まれ変わることにより、業界を超えて情報がサービスの基盤となる。これがサイバースペースの意味である。サイバースペースに関しては、人類は新しく情報文明を創っている時期だとおっしゃる方もいる。そのぐらい大きな意味を持っているということであり、国としては、国民一人一人がどのように幸せになっていくかということを創っていくことが文明であるから、横のつながりはとても重要になる。横のつながりがサイバーセキュリティやサイバー空間のマネジメントの中で、国のマネジメントとして十分にできているかどうか。この NISC の体制あるいは NISC の強化だけで実現ができるのか。ホームランド・セキュリティのために 9.11 の後、アメリカ政府は DHS を作った。これによりサイバー空間の全体を見渡せる体制になって、法的なバックアップもできている。こういう体制に向けて、我が国も 2020 年を目標に基本法の改正を含めた見直しをする。このぐらいの強い意志で進めるべきではないかと思う。2020 年に向けてこのスケジュールが出てきているということは、大変意味のあることだと思う。

○（遠藤本部員）３つの観点でコメントを申し上げる。

まずインフラについてである。2020 年東京オリンピック・パラリンピック競技大会の開催にあたり、実際のプレパレーションは２年程度だと思うが、それに向けてインフラ攻撃への対応、または準備というものが絶対的に必要である。

ただ、日本は大きなインパクトのあるインフラ攻撃というものを受けたことがない。インフラが攻撃を受けたときにどのようなことが起こるのかということを完全に理解できている状況に日本はないと思う。さらに、そのことを本当に理解できている経営者がどの程度いるのかは、少し問題点であると思う。

インフラ攻撃は増えているが、攻撃に対して実際にリスクを把握するということ、それに対して基準を決めて達成度を評価して、その結果としての課題を浮き彫りにして、それをさらにまた繰り返していくというルーチンを確実にしていくことが重要で、リスク把握が初期で一番重要なポイントである。

今まで日本は大きな攻撃を受けていないため、攻撃者の立場に立ってどういうところが攻められやすいのか、またはどういう攻撃を受ける可能性があるのか、基本に立ち戻ってインフラの攻められる場合のリスクの評価を行っていく必要があると思う。攻撃者側は弱いところ、また、インパクトが大きいところ、その辺りを狙って攻撃を仕掛けるため、その視点で我々はサイバーセキュリティのサービス等を行っており、その辺のリスクアセスメントについて、政府主導も含めて確実に行っていくことが重要だと思う。今回、拝見した資料は、精度の高いリスクアセスメントができるので、この部分は非常にいい資料ができたと考えている。

２点目は、予算にも少し関係するが、このインフラに対する体制整備、または人材の育成というものが、２年間ということで非常に切羽詰まっているというのが現状である。２年間でやるべきこと、これはある一定数の指導者ができるレベルの人材を育てなくてはいけない。この２年間の教育の在り方というものを、再度官民一体でこれをつくり上げて、人数に対するイメージも明確に持って、この２年間でやり遂げるべきであり、とても重要

な時期になってきている。その観点で、予算を今回は 20%増やしているが、この有効利用という部分も人材育成について考えていただく、または我々等もそれに参加することはとても重要だと思う。

３点目は、サイバー攻撃というものはいわゆる国内での物理的な犯罪というよりも、国際間でのサイバー空間を通した犯罪であり、その犯罪の意味合い、または犯罪の重さ、犯罪に対する法の適用の在り方、これらの部分は国際協調がより一層必要な状況になってきているのではないかと思う。これは前田本部員の領域だが、現状ではサイバー犯罪の国際間の共有性がまだ捉えられていないように見受けられる。今後、共有性をどのように日本が主体となって築いていけるかが、非常に重要な領域になってくると思う。本来は法というものは何かに対してパニッシュメントがあるというだけではなくて、その行為自体を行わせない、または抑制させるためのものであり、これは国際間での共有性もある程度持つ必要があり、サイバー空間でリモートによる他国からの攻撃も思慮すると、その部分は非常に重要になってくる。

○（小野寺本部員）３点申し上げる。

まず１点目は、一昨日、イスラエルの方のサイバーセキュリティの講演会に出席したところ、経済同友会が主催であるが、参加している経済界の方が非常に少なかった。はっきり言って経済界のサイバーセキュリティに対する関心度合いというものがまだまだ低いのではないか。どうしても重要インフラが中心に議論される。これは当然ではあるが、イスラエルではNational critical infrastructure and manufacturingとして、重要インフラに加えて製造業も入れて考えている。特に日本の場合には、ものづくり大国と言われているだけに、製造業のサイバーセキュリティが本当に大丈夫なのか、日本の経済にとっては非常に重要な要素になるのではないかと考えている。今後は、重要インフラ事業者と主要製造業を一体で取り扱い議論することを検討してはどうか。

２点目はIoTについてである。IoTにおいて一番問題なのは、IoTの機器が一旦売り切りで導入が進んでいくと、その後、はっきり言ってどこにあるかわからない。したがって、何か問題があってファームウェアを更新しようとしたときに、そのアクセスすらうまくできなくなる可能性があるのではないか。これはユーザー側が十分認識していれば、自らアップデートを実施すると思うが、そこまで日本の企業、個人の意識は上がっていないと思う。IoT機器の脆弱性が発見されたときの対応について、今から検討しておくべきではないか。その際、制度上の問題を日本として先行的に考え、その制度をうまくIoTの製品に織り込むことによって、国際標準化していくことがある意味では可能ではないかと思う。IoT機器の制度面のルール作りを先行することが、国際化にとっても非常に重要ではないか。

３点目は、人材育成についてである。「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」の案でも人材育成については非常によく検討されており、各部門で人材育成が強化されているということは大変好ましいことである。

ただし、問題は、例えば総務省のナショナルサイバートレーニングセンター構想や、大学では enPiT という大学・大学院での成長分野を支える情報技術人材の育成拠点の形成など、各部門でいろいろな対策が出てきている。今の時点では各省庁がそれぞれ取り組む

方向性で良いのだろうが、今後はそれらの教育研修について、ある程度横連携をとりながら、例えば教材についてのレベル合わせや共通化を図るなども考える段階に来ているのではないか。今後、国として統一感を持った教育ができる形に少しずつ持っていっていただきたい。

○（丸川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））
本部員の皆様方には日頃から大変お世話になっており、感謝申し上げる。また、今後引き続き、法の見直しも含めたさまざまな議論にお力をお貸しいただきたく、よろしくお願い申し上げる。

先日、英国に出張し、サイバーセキュリティ関係機関を訪問した。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、特に演習・訓練をしっかりやる、オペレーションが重要であるという意識づけを受けてきたので、これを速やかにスタートさせたいという思いである。加えて、過去の大会に比べてもかつてない状況にさらされるということを、十分に想像力をもって備えなければいけないということも同時に感じてきた。万全を尽くしたいと思うため、引き続きの御協力をよろしくお願い申し上げる。

特に、サイバーセキュリティ対策の強化に向けて電力・通信・交通など、重要なサービスを御提供いただく事業者における自らのサイバーリスク第１回目の評価が終了した。今後、評価結果を基に対策を促進していただけるように、我々としてもお願いをしてまいりたい。

加えて、民間の皆様の御協力はますます重要になってくるため、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情報共有体制の構築については、特に即時性、あるいは信頼性の高い共有体制についても意識を向けてまいりたい。どの情報を、どこまで共有するか、仕切りというものが必ずしも明確になっていないが、大変ステークホルダーの多い大会をやっていく上では非常に重要なため、よくその点を検討してまいりたい。

また、リアル（フィジカル）とサイバーを、相互に関連するリスクとして捉え、取り組むことも、特にコンティンジェンシープランが重要なため、意識をしてまいりたい。

関係省庁のこれまでの御協力には御礼を申し上げるとともに、引き続き御協力をお願いしたい。

○（松本国家公安委員会委員長）不正アクセスによる情報流出事案等のサイバー攻撃事案が相次いで発生しているほか、インターネットバンキングに係る不正送金事犯等のサイバー犯罪も多発しており、サイバー空間の脅威は深刻化している状況にある。

３年後に迫った 2020 年東京オリンピック・パラリンピック競技大会の開催を見据え、関係機関とより密接に連携し、大会組織委員会や重要インフラ事業者等との情報共有・共同対処訓練の実施等による官民連携の推進を図るとともに、情報収集・分析の強化、捜査・実態解明能力の向上を図り、サイバー空間の脅威への対処に万全を期すよう、警察庁を指導していく。

○（世耕経済産業大臣）重要インフラ事業者による情報共有体制の充実が大きな課題だと思う。独立行政法人情報処理推進機構では、J-CSIP という情報共有体制を構築しており、

ここには今、電力、ガス、石油企業など業界横断的に参加をしていただいている。また、金融、通信分野では業界独自の取り組みとしてISACというものが構築されている。しかし、医療、水道、物流、航空、鉄道といったインフラ分野は、こうした仕組みがまだないのが現状である。このため、これらの業界については、J-CSIPの利用やISACの構築など、情報共有の方針について検討し、次回のサイバーセキュリティ戦略本部において報告してはどうか。

なお、経済産業省所管のクレジット分野については、J-CSIPに加盟をしていただき、情報共有を行う予定である。先ほど、小野寺本部員から御指摘のあった製造業についても、どういう形がいいのか検討していく。

また、分野横断的に政府において脅威情報の集約を行うことも重要である。NISCの情報収集・分析体制の抜本的強化が必要と考えている。事業者から政府へ一定の情報提供を求める責務規定の整備、あるいはIPAやJPCERT/CC等の専門機関の活用など、サイバーセキュリティ基本法の改正等を含めてNISCを中心に検討すべきと考えている。

加えて、2020年東京オリンピック・パラリンピック競技大会開催を見据えれば、リスク評価の徹底も重要である。NISCにおいて、リスク評価の対象者を含めた工程表を策定し、2018年度中に全ての重要インフラ分野でリスク評価を実施すること、NISCが第三者を活用してリスク評価の結果を確認することなどの検討を進めるべきである。この際、IPAに設置する産業サイバーセキュリティセンターの機能も御活用いただきたい。

さらに、サイバーセキュリティの強化に当たっては、海外との協力を通じて幅広い知見や経験を共有すべきである。経済産業省も産業サイバーセキュリティセンターを活用し、米国国土安全保障省との間で重要インフラ防護に関する共同演習などを実施していくが、政府全体としてサイバーセキュリティ分野における日米、日ASEANの国際連携を積極的に推進していくべきだと考えている。

2020年東京オリンピック・パラリンピック競技大会は国が責任を持って実現をしていくものであり、経済産業省もできることには取り組んでいくが、サイバーセキュリティ戦略本部としてトップダウンで進めていただきたい。

○（稲田防衛大臣）高度化・巧妙化するサイバー攻撃に適切に対処するため、防衛省・自衛隊においては実践的サイバー演習を目的としたサイバー防衛隊の増員や、高度人材育成のための各種研修への参加など、さまざまな取り組みを進めている。

また、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、さまざまな場面において自衛隊の部隊等が任務を遂行する上で極めて重要となる。

こうした重要インフラの防御体制の強化等、東京オリンピック・パラリンピック競技大会が開催される2020年を見据えた我が国全体のサイバーセキュリティを強化する取り組みに対して、防衛省としても情報共有などの協力を積極的に行っていきたいと考えている。

○（鶴保情報通信技術（IT）政策担当大臣）先月、「官民データ活用推進基本法」が公布・施行された。AIやIoT、ビッグデータの時代においてデータの円滑な流通・利活用を強力に推進するためには、重要インフラにとどまらず、幅広いセキュリティ対策に取り組む必

要がある。
　このことは先日、ドイツを訪問し、当地の教育研究大臣と会談した際も、データ利活用の推進とともにサイバーセキュリティの重要性について共通認識を持ったところである。また、同国では大企業はおろか、中小企業に対してでもサイバーセキュリティのリテラシー向上に努力しているという実態も印象深い。
　これを踏まえて我が国としても、例えば機密性の高い研究データを有する研究開発法人や大学等におけるサイバーセキュリティ対策や、サイバーセキュリティ対策に十分な投資ができない中小企業等における対策、また、こうした対策を支える若手のサイバーセキュリティ人材の発掘や育成などの取組を、データ利活用推進とあわせて一体的かつ迅速に推進していく必要があると考える。

○（あかま総務副大臣）総務省は今月 17 日に「IoT サイバーセキュリティアクションプログラム 2017」を公表した。この件について御紹介をさせていただく。
　このプログラムは、昨今、サイバーセキュリティの脅威が増大し、その被害が深刻化している中、IoT 時代に対応した対策を早急に確立すべく、総務省において策定したものである。
　総務省としては、このプログラムに基づき IoT/AI 時代を見据えて必要な方策を推進する「サイバーセキュリティタスクフォース」の開催、脆弱性のある IoT 機器を把握し、管理者に注意喚起を行うなどの IoT 機器セキュリティ対策の実施、さらに重要インフラ企業等に対する実践的なサイバー防御演習や 2020 年東京オリンピック・パラリンピック競技大会の適切な運営に向けたセキュリティ人材の育成などの人材育成のスピードアップなどに取り組むこととしている。
　こうした取り組みを通じて引き続き関係府省と連携し、我が国のサイバーセキュリティの向上に尽力していきたい。

○（岸外務副大臣）外務省として、関係省庁と連携しつつ、サイバー分野における国際協力を積極的に推進している。政府全体として重視している重要インフラについて、昨年 12 月には日米韓の３カ国の専門家会合を開催し、脅威認識についての意見交換や、仮定のシナリオに基づく議論等を行った。
　また、昨年 10 月には韓国、12 月にはウクライナとの二国間協議でも各国の取り組みを聴取しつつ、議論した。11 月にはロシアとも信頼醸成の観点から協議を実施した。
　サイバーをめぐる国際情勢は厳しさを増している。米大統領選に関する米国のロシアへの対応を含め、各国におけるサイバー攻撃事案や各国の対応などについて、引き続き情勢を注視していきたい。

○（村井本部員）繰り返しになるが、横のつながりを持った、社会の基盤がサイバースペースであり、各省庁あるいは各事業セグメントの縦割りに対して、横で共通に考えていくことというのは、サイバースペースのマネジメントとしてとても重要なため、その体制をどうするのかが課題である。
　また、国と地方行政、地方との関係も横のつながりだと思うが、分野を超えたところで

新しい産業が発展していく。それを私は文明と言ったが、その基盤であることの認識を持って国全体での取り組みを考えていただきたい。

(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

本日は大変貴重な御意見をいただき、感謝申し上げる。

政府としては、本日の議論を踏まえ、重要インフラの防護に着実に取り組むとともに、2020 年及びその先を見据えたサイバーセキュリティの在り方について議論を進めていく。

有識者の皆様におかれては、今後ともご協力のほど、よろしくお願い申し上げる。

－　以上　－