サイバーセキュリティ戦略本部
第22回会合　議事概要

１　日時

令和元年５月23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
山本　順三　　国家公安委員会委員長
石田　真敏　　総務大臣
岩屋　　毅　　防衛大臣
平井　卓也　　情報通信技術（ＩＴ）政策担当大臣
佐藤　正久　　外務副大臣
磯崎　仁彦　　経済産業副大臣
遠藤　信博　　日本電気株式会社代表取締役会長
小野寺　正　　ＫＤＤＩ株式会社相談役
後藤　厚宏　　情報セキュリティ大学院大学学長
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
前田　雅英　　日本大学大学院法務研究科教授
宮澤　栄一　　株式会社デジタルハーツホールディングス取締役会長
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
沖田　芳樹　　内閣危機管理監
三輪　昭尚　　内閣情報通信政策監
和泉　洋人　　内閣総理大臣補佐官
前田　　哲　　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
兼原　信克　　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、主に昨年７月に決定した新戦略に基づく年次計画である「サイバーセキュリティ2019」や「重要インフラにおける安全基準等策定指針」について御審議をいただきたい。

限られた時間ではあるが、活発な御議論をお願い申し上げる。

（2）討議

【決定事項】

・サイバーセキュリティ2019（2018年度報告・2019年度計画）（案）について
・重要インフラにおける安全基準等策定指針の改定（案）について
・サイバーセキュリティ関係施策に関する令和２年度予算重点化方針（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】

・サイバーセキュリティ基本法の一部改正に伴う関係規則等の改正について
・サイバーセキュリティ協議会について
・2020年東京大会に向けた取組状況について
・サイバーセキュリティ研究・技術開発取組方針について
・2019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

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。

○（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））

それでは、意見交換に移りたい。

まず、有識者本部員よりコメントをいただきたい。

○（野原本部員）

３点申し上げる。

１点目は、決定事項の１番目の「サイバーセキュリティ2019（案）」についてである。この点については、何度も議論を重ねた結果、しっかりとした良い年次計画が作られたと思っている。今回は、１部１章に動向や事例を加え、２部１章では今年度の主な取組についての全体の方向性を示したことで、全体として読み物としても興味深い冊子になったと思う。サイバーセキュリティ政策は、言うまでもなく、関係者を含め、経営者から若年層まで幅広い層を巻き込んで実施していくべきであるため、是非多くの人に読まれるように、サイト上の見せ方等も工夫して周知に努めていただきたい。よろしくお願い申し上げる。

２点目は、報告事項の２番目の「サイバーセキュリティ協議会」についてである。長い間、重要施策の一つとして議論してきた情報共有や連携体制が形になったものであり、適切に構築され、初期の構成員が決定したということで、関係者の皆様には感謝を申し上げたい。

本施策の成否を分けるポイントは細部にあると私は思っている。資料６－２に書かれているが、本協議会の一般構成員の幅広い人たちが、サイバー攻撃ではないかとちょっとした違和感を覚えた段階や、不安を感じた段階でも気軽に相談できる体制をつくる必要がある。そして、それに対して細々とした相談に丁寧に対応することで、企業に参加してもらい、情報を収集してもらえる協議会にしていくことが最も重要だと思っている。丁寧な対応をしていくことは容易ではないと思うが、是非真摯に取り組み、その進捗状況も御報告いただきたい。それにより、活動が実のあるものになっていくと思う。

３点目は私は社外取締役をしている関係で各社の取締役会に出席するのだが、前回、企業の中で経営層とサイバーセキュリティ担当者の間に共通言語が不足しているのではないかと申し上げ、一緒に議論できるような資料のモデルを作成してほしいと申し上げたところ、経済産業省を中心に、経営層やCISO等向けのガイドラインや事例集を作成しておられ、今年度はさらに、その進捗状況の可視化ツールを整備しようとしており、それによって他社の状況との比較も可能になると聞いている。それらを活用して、皆さんがしっかりとコミュニケーションが取れるように、是非周知し、内容についても、更にブラッシュアップしながら進めていただきたい。

○（前田本部員）

年次計画に絞ってコメントさせていただく。2020年東京オリンピック・パラリンピック競技大会について、対応の内容としては最終段階で、その後、どうするかという話に移行しているが、やはりここでうまくいくかどうかが評価さ

れるところになる。今までの計画が順調に進んでいるということはよく理解している。

また、今回、小さなことかもしれないが、サイバーセキュリティに関する技術力の向上や人材を広げていくということを強調した点も非常に高く評価したい。ただ、一番強く感じているのは、非常に評価はしているが、積極的サイバー防御に関して、具体的に対処することにつながらないと意味がないという観点で、防衛省、警察庁などとNISCとの役割分担がいずれ問題になってくると思う。今の流れはこのような形で進めていくのが一番良い。

その象徴がサイバーセキュリティ協議会である。これは大きくカーブに差しかかる可能性もあり、まさにNISCのNISCたる政策判断に直面するだろう。特定の企業の問題が取り沙汰されているが、協議会の構成員にどこまで入れるかが問題だと考える。我が国とサイバーセキュリティに係る基本的な考え方を共有していない国に関連する企業も多く存在する中で、どこまで秘密を守っていけるか。5Gに関して、やはり日本は自由、公正かつ安全なサイバー空間に向けてアメリカと組んでいかなければいけないというのは分かるがその一方で我が国とサイバーセキュリティに係る基本的な考え方を共有していない国とはどう向き合うのか。そのバランスをとるのは、まさにNISCのような、内閣官房の立場であるべきだ。形式的に危ないから協議会に加入させないということでもいけないし、国益につながるから防衛的な企業等はどんどん加入してもらわなければいけないというだけでは日本の将来が危ぶまれるだろう。

まさに日本のサイバーセキュリティは正念場に差しかかってきている段階だと思う。サイバーはグローバルだからナショナルな国益に直結しているのだと思う。やはり最後は政治の決断ということで、今、道を誤らないでいただきたいということを強く申し上げたい。

○（宮澤本部員）

私の考えは、少し皆様の見方とは違うかもしれないが、2001年からゲームデバッグの事業を成長させてきた経験に基づき意見をさせていただく。

5Gの世界によって通信機器を握られることは命を握られることと一緒だと思っている。現状、各国は独自に国内の機関で調べ、生の情報を手に入れているが、残念ながら、我が国はその部分では後れをとっている。しかし、サイバーセキュリティにおいては、まだ日本は一発逆転の立場を狙える鍵が眠っていると思っている。それは日本人ニートの活用である。

アメリカのマカフィーの調査では、７カ国のセキュリティスペシャリストのおよそ1,000人のうち92％が、「ゲーマーがサイバーセキュリティの仕事に必要なスキルを備えている」と考えているという結果がある。また、以前からアメ

リカの国防総省は自らゲーム大会を開き、トップゲーマーをリクルーティングしている。既に世界ではゲーマーの活用を始めている。

幸いなことに、日本はオタク、ニート、ひきこもりの数は圧倒的である。ひきこもりの多くは一日中、家でゲームをしている。超ハードゲーマーが100万人以上いるとも言える。私はいわゆるゲームオタクと呼ばれるデジタルネイティブの人たちとおよそ20年向き合ってきた。バグとはシステムの穴のことであり、デジタルハーツではそのバグを見つけることだけに特化してきた。バグを見つけることをデバッグ、バグを見つける人をデバッガーと呼んでいる。

我々が創業して半年経った頃、当時はプログラミングなどの知識がなければバグは見つけられないと考えられており、仕事を得ることができなかった。しかし、米国マイクロソフト社のXboxというゲーム機を日本で発売する際に、選考会でシアトル本社のトッププログラマーたちと同じ条件下でバグを見つける競争をして、彼らより10倍以上のバグを見つけて勝利することができた。その結果もあり、マイクロソフト社から日本で初めて公認をもらい、大きな仕事を任されることになった。しかし、なぜ、ただのゲームオタクが彼らに僅差ではなく、10倍以上の圧倒的な差で勝てたのか、当時の私には本当に疑問だった。

この答えの１つ目は、日本人であることだ。マイクロソフトのプログラマーからの「どうしてあんなにバグを見つけられたのか」という質問に、そのデバッガーの子は、「あなたたちに教える価値はない」と答えた。センスがないということだと思うが、私は仕事がなくなると思ったものの、アメリカの方たちはみんな、「グレート」と言って盛り上がった。サイバーセキュリティの、特にハッキングにおいては、この資質が重要である。彼らはバグを見つけた理由を、「におったから」と言う。日本人は皆、駅に売られている平積みされた雑誌を上から２番目とか３番目あたりを抜いて買う、この「気になってしまう感覚」が重要な資質だと思っている。

そして２つ目の答えは、彼らがコンピューターサイエンスを学んでいないということだ。ソースコードを読めないからこそバグを見つけることができた。福島原発では、なぜ予備電源を高いところに設置しなかったのか。時にプロフェッショナル、スペシャリストたちは、その道のプロだからこそ一般的な何かを見失いがちだ。時に穴を見つける際には真逆のアプローチが必要なのだと思う。今や、スペシャリストの考える想定外は想定内にある場合が多い。我々がバグを見つけると必ずプログラマーが言う言葉が、「そんなはずがない」である。今では、弊社では8,000名以上のテスターが登録されており、デバックの仕事に従事している。先日、某企業のシステムエンジニアが嫌がらせで強力なパスワードをかけて退職してしまい、我々にその対応の依頼があったが、元ひきこもりだった子が、わずか２分でパスワードを解いた。彼らは間違いなく技術

者である。スーパーハッカーになれる素養を持った人たちだ。
私が考える一発逆転のサイバーセキュリティシステムとは、コンピューターサイエンティストでない日本人の感覚を持つニートを最大限に生かした独自体制の確立だ。そして、これは新しいビジネスとして世界に打って出る産業の創出。「made in Japan」に替わる「checked by Japan」の構想である。私は、今、まさに即効性のある対策として、即戦力になれる日本のニートたちを国が生かしていくべきではないか、そのような時が来たのではないかと強く思っている。

○村井本部員
大学にも多くの元ニートの方が入学してくるが、その状況も随分様変わりしてきた。慶應義塾大学の湘南藤沢キャンパスでは、30年前に日本で初めて全学生にコンピューターを持たせ、ネットワークを利用させるという、当時、1990年としては非常に先進的なキャンパスだった。当時の高校生の大半はパソコンを使えなかった。そのため、入学してからパソコンのキーボードの打ち方であるブラインドタッチを教えた。それが30年前のことだ。
30年前には、高校生のパソコン利用率は10％だった。その後、パソコンを使っている高校生の人数は一旦増えたあと、現在では再び減って30％しかいない。ただし、その代わり、スマートフォンの利用率は100％である。つまり、これはインターネットの使い方が大きく変わってきたということであり、わずか30年でこれほど変わってきている。もはやインターネットを利用している人口は日本では90％を超えていると言っていいと思う。そういう意味では大半の人が使っているということだが、その使い方には様々な変化が日々起こっているわけだ。
日本の中にはインターネット、サイバースペースの影響がない人はもうほとんどいなくなったとして、その影響度、あるいはその役割が多様になっており、それぞれの人がどのような意味でのサイバーセキュリティに対する感覚を、あるいは力を持っているかを整理する時代になっていると思う。変わり行く現場を我々が把握していくのはとても重要である。
また、IoTや5Gが普及し、IoTの適用範囲が広がると、やはり全く新しい分野がこのサイバースペースに参加してくる。農業のように、その他の新しいデバイスがつながったり、新しいデータを利用したりすることで、新しいサイバースペースの仲間はどんどん増えていく。この中でサイロとしての分断が起きたり、分野のつなぎめに穴がないようにするというのは非常に重要なことで、全産業にまたがるということに関してはこの内閣官房の役割は非常に強くなると思う。
最後に、G20が控えているが、データの利用や、サイバーセキュリティに関し

ての体制、そして準備という点では、世界から見れば日本には学ぶところが多くあると思っている。この共通のメッセージは各大臣会合等々でも、データ利用とサイバーセキュリティに関しての共通のポリシーをしっかりと世界に対して影響を与えられるように伝えていただきたい。

なぜならば、これは何度も言われているが、サイバースペースはグローバルなため、良い見本がそのメッセージの中にあるということは世界全体への貢献、あるいは日本の活躍につながると思う。その大事なタイミングがG20だと思う。

○遠藤本部員

「サイバーセキュリティ2019（案）」について、少しコメントをさせていただく。

まず、取りまとめいただいたこと、大変感謝申し上げたい。デジタルトランスフォーメーションの推進も背景に、サイバー空間と実空間の一体化が進んで、産業及び人間社会の生活そのものの基盤になっていくということを示されていると思う。そのような中で、サイバーセキュリティそのものが人間の生活に密着し、また、産業にも密着をしてくるということで、年次報告でこれがリマインドされることは非常に重要なことで、国民の意識向上においても意味があると思う。本当にサイバーセキュリティそのものが人間中心の生活を支えているのだということを意識することが重要だと思う。

その中で、少し予算の話に触れるが、平成25年から３倍ぐらいの予算が今、取られている。しかしながら、世界に比べると、まだまだそのレベルは十分ではない。今後、Society 5.0の構築、さらには地方、中小企業、そのようなところを含めて全体が世界のトップレベルになっていくためには、それなりの予算の執行が必要ではないかと考える。

次は人材である。先ほど即戦力ということでニート活用の話があったが、私もそのとおりではないかと思っている。また、即戦力という観点で、IPAでも産業サイバーセキュリティセンターの中で２期目の卒業生が出て、２年間でトータル約160名の卒業生が出ることになる。これによって、企業での即戦力はシステムとして動き始めたなという気がしているが、まだまだコアの人材というものが育つ仕組みができ上がっていない。この件に関しては、サイバーセキュリティ2019（案）で書いてある、イノベーションを推進する人材育成とほぼ等価であり、ぜひサイバーセキュリティのコア人材についての教育システムの構築というものにも力を入れていきたい。産官学一緒になってやらないといけないことだと思うが、方向性をつくってまいりたいと思う。

それから、サイバー・フィジカル・セキュリティ対策に関して、経済産業省がまとめて、デジタルトランスフォーメーションの実現に向かうための考えを

整理しているが、これは海外などで非常に高い評価をいただいていると聞いている。ポイントとしては、特に信頼性の起点がデータであるということをリマインドしているところはとても重要だと思っており、これからAIがリアルタイムで動いて、5Gの上で動いて、いろいろなロボットや車を動かすということになると、サイバーセキュリティは本当にデータそのものである。今までのITネットワークの中でのサイバーセキュリティの方法論とは全く違う方法論をここで取り入れなくてはいけない。その辺りは明確にされているため、ぜひこの部分は我々が新しいサイバーセキュリティを検討する上で考えていかなければいけないと思う。

最後に研究開発だが、サイバーアタックというのは、新しい技術が出てくると、方法論を対策に取り入れるということが起きている。私が最近懸念しているのは、技術の進化の上では量子コンピュータの実用化が迫っているのではないかという気がしている。そうすると、いろいろな観点で暗号の意味合いというものが全く変わってきてしまう。そのような状況において、量子暗号みたいな新たな技術の開発が絶対的に必要である。

これらのことを考えると、最先端の領域の研究を日本単独で進めることはとても難しいと思うし、海外の大学や研究機関と研究コミュニティなどを形成して、世界最先端の技術の力を維持することが必要であると思っている。これを産官学で方向感を決めていく必要があると思う。

○（小野寺本部員）

まず、宮澤本部員が加入されたことを評価したい。やはり当本部も多様性を重視していくべきだと思うため、そういう点で宮澤本部員に入っていただいたことは大変すばらしいことだと思う。

次に、年次報告に関し１点申し上げる。第１章を今回設けたことは非常に大きいと思っている。というのも、１章を読めば、ある程度、全体の動向を掴めるため、イノベーションを進めるに当たって、この程度の状況を把握した上で対応を取れば良いということを簡単に言えるのではないかと思うためだ。

その中で、今回のデジタルトランスフォーメーションの時代の流れとサイバーセキュリティを組み合わせた記載を入れたことを非常に私は評価している。正直言って、企業も政府も含めてデジタル化が明らかに遅れており、その点で、このような言葉は意外と企業経営者に響くのではないかと思っている。その意味で、今回、第１章を作ったことを大変評価している。

重要インフラについて１点申し上げると、今回「法令・政策の不認識」という項目を入れた事は非常に重要だと思う。というのも、各事業者は、自分の業界のことについては法令を含めて知っているはずだが、その周辺についてどこ

まで理解しているかということに非常に疑問がある。今回、特にGDPRについて取り上げているが、GDPRに限らず、周辺情報について理解する機会をここで作ることが非常に重要だと思う。

○（後藤本部員）

「サイバーセキュリティ2019（案）」に関連して、一言申し上げたい。

まず、重要インフラと政府機関、自衛隊などでサイバーセキュリティ戦略に沿ったキャパシティビルディングの取組が着実に進んでいると思う。今後も防御及び攻撃対処態勢の強化に向けて、幹部層、経営層への意識づけと、戦略マネジメント層の育成、IoT分野の実務者層の育成などの推進策を、地域にも拡大し、しっかりと継続していくことが重要と考えている。

次に、昨今、重要と言われているサプライチェーンのセキュリティ確保に向けて２点申し上げたい。

１点目は、サイバーセキュリティ2019（案）にあるように、グローバルな連携や協調関係の中で、セキュリティ対策のフレームワークや、それを支える技術開発の取組を確実に進めて、サプライチェーンのセキュリティ確保に向けて、我が国がリーダーシップを発揮できるようにすることが重要だと思っている。

２点目は、具体的な強化策として、PSIRTの立ち上げと、PSIRT、CSIRT連携です。PSIRT、プロダクトサートとは、サプライヤーにおいて製品の構成部品のセキュリティ管理とか、プロアクティブな脅威分析及び製品の購入者、利用者への脅威情報の積極的な配付や対策支援等を担当する組織のことであるが、本格的なPSIRTを持っているサプライヤーは世界にも限定的である。PSIRTは、セキュリティ品質の向上によって、我が国の製造業全体の競争力強化にも貢献するため、中小の製造業も含めて、しっかりとした促進策が重要と考えている。また、大規模化、広域化しているサプライチェーンにおいては、サプライヤーのPSIRTと事業者のCSIRTが相互にしっかりと連携していく枠組みづくりがセキュリティ確保にとって重要と考えている。

○（中谷本部員）

「サイバーセキュリティ2019（案）」及び「重要インフラにおける安全基準等策定指針改定（案）」は、いずれも妥当であり、承認したい。その上で、以下の４点について申し上げる。

第１に、サイバー外交について、本年のG20において開催国としてサイバーセキュリティに関する議論をぜひ主導していただきたい。また、国連のサイバー政府専門家会合において、責任ある国家の行動規範の結晶化に向けて引き続き努力をしていただきたいと思う。

第２に、サイバーセキュリティ協議会に様々な企業や団体が参加することをうれしく思う。オールジャパンの取組として望ましいことである。今後、メンバーは増加していくと思うが、例えばJAXAやGPIFといった独立行政法人なども参加することがより望ましいと考える。

第３に、外為法の投資規制業種にIT分野も加えるという方針が報道されているが、望ましい対応であると考える。安全保障に関連する技術流出の防止に資するのみならず、サイバーセキュリティ対策としても重要であり、早期の対応がなされることを希望する。

第４に、2022年度から高校で情報Ｉが必修科目となり、2024年度からは大学入学共通テストでパソコンでの出題、解答が出される方針であると報道されている。今後の高校教育のあり方として、よい対応であると思う。カリキュラムでも入試の出題でも、相当部分はサイバーセキュリティに充てていただくよう希望する。

○（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））

引き続き、副本部長、閣僚本部員から御発言をいただきたい。

まず、私から、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及びサイバーセキュリティ担当の大臣として、発言させていただく。

今月９日からは、オリンピックの観戦チケットの抽選申し込みが開始され、いよいよ2020年東京オリンピック・パラリンピック競技大会が近づいている。大会の成功には、サイバーセキュリティ対策が重要であり、本年４月に立ち上がった「サイバーセキュリティ対処調整センター」と「サイバーセキュリティ協議会」の運用を着実に行ってまいりたい。

このほか、政府調達におけるサプライチェーン・リスク対策や技術検証体制の整備を進めるとともに、重要インフラ事業者等における望ましいデータ管理のあり方の検討や、研究・技術開発、人材の確保・育成などにも取り組んでまいりたい。

本日の議題であるサイバーセキュリティ2019には、こうした取組が盛り込まれており、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も見据え、サイバーセキュリティ戦略本部の副本部長として、対策に万全を期すべく、関係大臣と連携してしっかり取り組んでまいりたい。

○（山本国家公安委員長）

今や、サイバー空間は国民の日常生活の一部となっており、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、G20大阪サミット、ラグビーワールドカップ、2020年東京オリンピック・パラリンピック競技大会等も見据えながら、関係省庁等と連携し、サイバー犯罪対策、サイバー攻撃対策等を推進してまいりたい。

○石田総務大臣
安心・安全なSociety 5.0のためには、IoTなどの新たな技術のサイバーセキュリティの確保が必要不可欠である。
本年２月より開始した、脆弱なIoT機器の対策である「NOTICE」は、これまで日本全体の２億のIPアドレスのうち約9000万について調査を実施しており、今後とも着実に進めてまいりたい。
他方で、地域においては、サイバーセキュリティの人材が都市部と比べて不足しているなど、課題が残されている。そのため、県や広域的なエリアにおいて、協力して人材育成を行うとともに、複数の企業等がサイバーセキュリティの専門家をシェアできるようにマッチング等を実施し、各地域で持続可能なサイバーセキュリティの確保を進めてまいりたい。

○（岩屋防衛大臣）
防衛省・自衛隊は、新たな防衛大綱及び中期防に基づいて、令和元年度には、サイバー攻撃対処を行う部隊等を約150名増員し、全体として約580名の体制とする。また、５年後を目途に、千数百名の規模まで拡充する目標である。
また、諸外国との協力に関する取組として、本年度よりNATO主催の多国間サイバー防衛演習「サイバー・コアリション」に参加することになった。
また、先月の「日米２プラス２」においては、サイバー攻撃が日米安保条約第５条にいう武力攻撃に当たり得ることを確認したところである。これによって、サイバー空間における日米共同対処の可能性を明確にした。この分野における日米間の防衛協力をしっかり進めてまいりたい。
最大の課題は、人材の獲得と育成であり、宮澤本部員のお話を聞いて、多様な人材を活用することの重要性を改めて感じているところである。
引き続き、防衛省・自衛隊として能力の強化に努めつつ、政府全体のサイバーセキュリティの強化に貢献してまいりたい。

○（平井情報通信技術（IT）政策担当大臣）
デジタル手続法案が国会審議中で、本日の参議院の内閣委員会の審議を経て明日の参議院の本会議で成立ということになると思うが、この法律は単に手続

をデジタル化するという意味ではなくて、要するに今の行政をデジタルに置きかえても意味がないため、社会全体をデジタル化したものに切りかえるという思想でつくった法律といえる。

その中で、システム予算・調達の一元化を謳っている。これは予算要求の段階から内閣官房に一元化をしていこうということで、それはやはり予算の効率的な運用や、新たな考え方の大前提として、安全なクラウドの利用やデータの復旧も含めた基盤などのセキュリティは非常に重要だと思っている。IT戦略本部とNISCほか、関係者と緊密な連携を図りながら、今後の調達に生かしていきたい。

○（佐藤外務副大臣）

外務省は関係省庁と緊密に連携しつつ、国際的議論に積極的に関与していく。

本年６月の国連政府専門家会合に我が国は引き続きメンバー国として選出されたほか、本年４月のG7ディナール外相会合において、悪意あるサイバー活動を非難し協力を強化すべき旨を確認し、また、５月初めにチェコ主催で開催された5G国際会議では、我が国が積極的に関与する形で、5Gネットワークの安全指針を定めた議長声明「プラハ提案」が採択されたところである。

また、G20大阪サミットの機会に、信頼性に基づく自由なデータ流通の考え方を各国と共有するほか、ICTの利用におけるセキュリティの問題についても引き続き議論を進めてまいりたい。

米国を初め関係国と緊密に連携し、サイバー空間における法の支配、信頼醸成、能力構築のため引き続き積極的に貢献してまいりたい。

○（磯崎経済産業副大臣）

「サイバーセキュリティ2019（案）」及び「重要インフラにおける安全指針基準等策定指針の改定（案）」に関して、一言付言させていただく。

サイバーセキュリティ2019には、本年４月に提示した経済産業省の「産業サイバーセキュリティの加速化指針」の内容をしっかりと反映していただいた。

また、経済産業省では、年次計画に基づいて「サイバー・フィジカル・セキュリティ対策フレームワーク」の具体化・実装、「Proven in Japan」の推進によるセキュリティビジネスの成長産業化、「サイバーセキュリティお助け隊」を初めとする中小企業・地域の対策強化等を進めていく。

また、データ管理に関するルール整備が各国で進む中、「重要インフラにおける安全基準等策定指針」の改定において、データ管理の必要性を盛り込んだことを高く評価する。

引き続き、こうした方針に基づき、各省庁と連携をして、産業サイバーセキ

ュリティの強化に向けて取組を加速してまいりたい。

（３）決定事項の決定等

○（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））

それでは、本日お諮りした４件の決定事項について、異議はないか。

（「異議なし」と声あり）

○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）

異議なしということで、本案を決定させていただく。

今後、本決定に基づき、取組を進めてまいりたい。

（４）本部長締め括り挨拶

本日の会合では、サイバーセキュリティ戦略に基づく今年度の年次計画等を決定することができた。これらに基づき、関係省庁に取り組んでいただきたい事項、３点を指示する。

第１は、本日決定した計画の対処方針に基づく取組強化である。サイバー空間と実空間の一体化が進展し、脅威が一層深刻化している。そこで、社会全体としてデジタル化とサイバーセキュリティの確保が一体のものであり、自らのこととして対策をとる必要があるとの意識を醸成し、それぞれが積極的な防御策を講じること。

第２は、2020年東京オリンピック・パラリンピック競技大会を初め、国際的なイベントの成功に向けた体制を確実に機能させることである。2020年東京オリンピック・パラリンピック競技大会や、本年のラグビーワールドカップなど、国際的なイベント開催時に、サイバー攻撃のリスクが高まる。こうしたイベントの成功に向けて、本年４月に設置したサイバーセキュリティ協議会やサイバーセキュリティ対処調整センターなどを、官民一体となって効果的な対策を講じること。

第３は、サプライチェーン・リスク対策の充実である。サイバー攻撃は複雑化・巧妙化をしており、今後、サプライチェーンを狙う攻撃がますます高まることが想定される。そこで、技術検証を行うための推進体制を強化させるなど、サプライチェーン・リスク対策を充実させること。

以上３点を踏まえ、本日、決定した計画に基づき、鈴木大臣のリーダーシップの下に、関係大臣が連携して取組を進めるようお願い申し上げる。

－　以上　－