サイバーセキュリティ戦略本部
第30回会合　議事概要

１　日時

令和３年７月７日（水）　　８時40分～９時20分

２　場所

総理大臣官邸２階大ホール

３　出席者（敬称略）

加藤　勝信	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
棚橋　泰文	国家公安委員会委員長
武田　良太	総務大臣
岸　　信夫	防衛大臣
平井　卓也	デジタル改革担当・情報通信技術（IT）政策担当大臣
長坂　康正	経済産業副大臣
中西　哲	外務大臣政務官
遠藤　信博	日本電気株式会社取締役会長
後藤　厚宏	情報セキュリティ大学院大学学長
田中　孝司	ＫＤＤＩ株式会社代表取締役会長
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
前田　雅英	東京都立大学法学部客員教授
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	慶應義塾大学教授
坂井　学	内閣官房副長官
杉田　和博	内閣官房副長官
三輪　昭尚	内閣情報通信政策監
髙橋　憲一	内閣サイバーセキュリティセンター長
藤井　健志	内閣官房副長官補
滝崎　成樹	内閣官房副長官補

４　議事概要

（１）本部長冒頭挨拶

本日は、次期サイバーセキュリティ戦略のパブリックコメント案、情報セキュリティ対策

のための政府統一基準の改定などについて審議いただくこととしている。また、東京大会のサイバーセキュリティ対策についても報告がある。

本年５月には、米国でサイバー攻撃によって重要インフラである石油パイプラインが停止し、大規模な影響が出たところでもある。また、国内においても、現在調査中であるが、サイバー攻撃によって業務委託先から政府機関関係の情報が流出するという事案も発生している。次期戦略は、こうした直面する脅威の動向にも対応したものとすることが重要であると考えている。

活発な討議を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（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４年度予算重点化方針（案）について

【討議事項】

・サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）(案)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に向けたサイバーセキュリティ対策について

・政府情報システムのためのセキュリティ評価制度（ISMAP）の暫定措置の見直しについて

・政府機関におけるデジタル改革に必要なIT・セキュリティ知識を有する人材の確保、育成総合強化方針について

・IT調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せの改定について

・ランサムウェア対策への取組状況について

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。

○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）

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。

○遠藤本部員

まず、次期サイバーセキュリティ戦略（案）及び統一基準群の改定の検討に感謝申し上げる。基本的には、これに関しては異論ない。

本日、３点申し上げる。

１点目は、オリンピックについて、準備を大変丁寧にしていただいていると考えているが、最後、COVID-19のことを考えると、医療現場に対するアタックが攻撃者にとっては非常にアピールになる可能性が高いということで、再度、医療機関への最終的なレビューや、または関連する施設（例えば空調設備のコントロール等）に対する確認をぜひ行っていただきたい。

２点目は、SBOM、Software Bill of Materialsである。ハードウェア事業者にとってはBill of Materials、要は部品表がハードウェアそのものの品質を定義するが、これからDXも含めてソフトウェアが主体になると、そのソフトウェアが本当に信頼できるものかどうかをSBOMとして定義して、提供することが重要になってくる。非常に難しい領域であるが、私は現在、経団連のサイバーセキュリティ委員長も務めており、後藤本部員にそこで講演いただいた。その中でもバイデン大統領が発効したサイバーセキュリティを強化する大統領令においても、政府調達のソフトウェアに関してはSBOMが必須であるというように動きが変わってきた。サプライチェーンを考慮し、ファイブ・アイズプラスワンも含めて考えると、我々の日本の中でもSBOMについて考える必要があると考える。ぜひ検討いただきたい。

３点目は、英国のシンクタンクのIISSが６月28日に報告書を出し、日本はサイバーセキュリティレベルが残念ながらTier ３であった。Tier ３というと、インド、インドネシア、マレーシア、ベトナムと同等というレベルであり、報告書の観点から言うと、情報共有の取決めは緩やかなルールで運用されている、また、多くの企業が防衛力強化のコストに対して消極的といった点が理由になっている。私がお願い申し上げたいのは、前回でも述べたがサイバーアタックがかかったときに自衛隊も含めて出動して国全体で抑えるというような方法論を考えていただきたいということである。警察関係でも実際に強化を行うということをお伺いしているので、ぜひ被害をうけたときの対応の仕方、法整備などについて、検討をお願い申し上げたい。

○後藤本部員

次期サイバーセキュリティ戦略（案）は大変充実してきたと思う。特に評価したいのは、大規模サイバー攻撃事態等への対処体制の強化の重要性が明記されたことである。

一方、気になったのは、依然としてサイバー空間のためのものという印象が残っている点である。コロニアル・パイプライン社の事案のように、サイバー攻撃が実空間に直接被害を与えるという事案が今、急増している。バイデン政権もCybercriminals are shifting from stealing data to disrupting core operations、つまり、サイバー犯罪がデータ窃取からコア業務への妨害に移っているとはっきりメッセージを出している。コロニアル・パイプライン社の事案では、ランサムウェアに乗っ取られたことを認識した段階で自らの安全優先のためにパイプラインを止めたということであるが、このような判断は我が国の

インフラサービス、鉄道、電力、ガス、全てにおいて同じであると思っている。

ほぼ全てのインフラや経済活動がデジタルに依存している現在、サイバー攻撃はサイバーの世界の話という意識を改めて払拭する必要がある。企業も政府機関もサイバー攻撃によって本業の事業継続ができなくなる事態への備えが必須と考える。我が国でも重要インフラ事業者は大規模自然災害での経験に基づいて緊急対応対策を複数しっかり持っているが、サイバー攻撃のように攻撃者と相対峙するという経験は少ないため、再チェックが必要なのではないかと考える。

また、企業の取組に加えて、国全体を俯瞰したデータ主導のレジリエンス強化策が重要である。先週末以来の豪雨で被災なさった皆様には心からお見舞い申し上げるが、被害を防ぎ切れなかったとはいえ、ハザードマップや非常時対応の体制は非常に大きな意味を持っている。同様に、日本全体の産業や社会経済活動をカバーするサイバー版のハザードマップのようなものが重要なのではないかと考える。セキュリティ分析、リスク分析、社会経済分析の専門家が広く知恵を集めて、そのような体制をつくっていただきたい。

○田中本部員

まず、次期サイバーセキュリティ戦略（案）は前回申し上げたコメントも入れていただき感謝申し上げる。統一基準群改正（案）、予算重点化方針を含めて、決定事項３件について特に異論はない。

その上で、今後の実行に関して２点コメントさせていただく。

１点目は関係各位からも出ているように、社会インフラをターゲットとしたサイバー攻撃が増えており、このサイバーセキュリティ対策も実効性担保が喫緊の課題であると認識している。特にサーバー攻撃がますます高度化してきており、地政学的にも緊張が増しているので、企業側、特にサービス提供事業者にとっては国主導での対応との連携が非常に重要であると考えている。実質的な連携を担保する意味において、企業の中に閉じては月１回程度の頻度で大規模障害の訓練等を行っているが、国との連携を含めてこのような訓練を行う等の検討をぜひともお願いする。どうしても企業の中に閉じてしまうというような経験があるので、ぜひともお願いしたい。

２点目は加えて、次期サイバーセキュリティ戦略（案）は非常に網羅的にまとめられていると考えているが、実行フェーズにおいては想定どおり進まないのが常である。企業の中では当然行っていることであるが、数値目標の設定やターゲットを明確にする等、進捗管理をぜひともお願いする。見える化等も非常に重要であると思っている。今後様々なことが起こりうるので、柔軟に対応していただきたい。

○中谷本部員

次期サイバーセキュリティ戦略（案）を全面的に支持する。その上で５点申し上げたいと思う。

１点目は、警察庁においてサイバー局とサイバー直轄隊が新設されることはサイバー攻撃の特質に合致した対応であって、アトリビューションや国際共同オペレーションにも資するものであり、大いに評価したい。この分野での人材育成を一層推進することを期待したいと思う。

２点目は、５月末に国連の政府専門家会合においてサイバー空間における責任ある国家の行動に関する最終報告書が採択されたことを歓迎したいと思う。西側諸国と中国、ロシアの間には多々、見解の相違があるようであるが、重要インフラに対する攻撃をしないことが、非拘束的な合意としてではあるが、確認されたことなど、サイバー空間における法の支配に向けた貴重な一歩であると考える。

３点目は、ランサムウェアが国際社会において深刻な問題となっている。我が国においてもランサムウェアへの法的・政策的・技術的な対応や身代金支払いの是非について本格的に検討を開始すべきであると考える。

４点目は、遠藤本部員からも言及のあった英国の国際戦略研究所の報告書は、我が国にとっては厳しい通信簿となったが、真剣に受け止めるべき点もあると思う。我が国の法制に関しては、通信の秘密に関する憲法第21条がサイバー諜報能力にとってのバリアになっている、サイバー手段による反撃には自衛隊法の改正を要するという記述があることに留意すべきであると思う。

５点目は、企業の対応については、一方でサプライチェーン・サイバーセキュリティ・コンソーシアムに参加するなど熱心な企業と、他方でサイバー攻撃を受けても通報しない企業という二極化が進んでいるように思われる。サイバー攻撃を受けた企業は、たとえ重要インフラではなくても、また比較的軽微と思われる攻撃であっても、適切な対応を取ることが企業の社会的責任の一部であることを認識して、関係省庁のみならずNISCにきちんと情報を伝達するようにしていただきたいと思う。英国の国際戦略研究所の報告書においても、企業がサイバー攻撃に関する情報を共有しないことが日本の抗たん性向上に対する障害であると指摘されていることに留意すべきである。

○野原本部員

私からは３点申し上げる

まず、次期サイバーセキュリティ戦略（案）など、決定事項には全て賛成する。その上で１点目は、DX with Cybersecurityについてである。DXとはデジタル化があらゆる場面で進むことで、それは組織改革、業務改革、事業開発など、あらゆる開発や改革には常にDXが伴い、そのたびにSecurity by Designが必要になるということである。したがって、政府機関でいえば、デジタル庁とNISCが組織間の壁を感じないよう、デジタルとセキュリティが一体的に個々の案件に係る必要がある。組織の縦割りを排し、有機的な連携体制をしっかり構築してほしいと考える。民間でいえば、セキュリティのトップのCISOとデジタルシステムのトップのCDO・CIOがそれぞれの組織を率いつつも一体的に検討する関係が必要

ということになる。それらの連携体制のベストプラクティスや人材育成のガイドライン等の作成も、しっかりと進めていただきたいと思う。

２点目は、ゼロトラストアーキテクチャへの移行の促進についてである。先日のバイデン大統領の連邦政府機関におけるサイバーセキュリティ改善に関する大統領令の署名があったが、その中に連邦政府が安全なクラウド及びゼロトラストアーキテクチャに移行するための支援も含まれている。御存じのとおり、リモートワーク環境整備にはこれらの整備が必要である。我が国でもゼロトラストアーキテクチャへの転換に関する具体的な対策・方法を明示して普及させることが重要である

３点目は、サイバー空間における攻撃者との非対称性についてである。サイバー攻撃は攻撃サイドが有利で、攻撃者との非対称性が課題になっている。今回の戦略ではトレーサビリティーの確保や仕組みの構築、能力向上など、いろいろな施策が分散して記載されているが、これらについて政府全体で議論を整理した上で、全体を見渡す体制を構築すべきと考える。具体的には、海外との協力体制、人材育成体制、関連技術サービスの提供体制、必要に応じて法制度の見直しも検討する必要がある。

○前田本部員

決定事項３点、全て異存ない。

それを踏まえて、今回の戦略を中心に特に申し上げたいのは、内閣のサイバーセキュリティ戦略が着実に進展してきたと思うが、今回の改定は非常に大きな転換を内在しており、コロナによって動かされたという面はあるが、むしろ積極的に捉えるべきで、これによって日本が良くなるというきっかけであると思っている。

象徴的なことは「Cybersecurity for All」という言葉、つまり国民にとってサイバー空間が不可分の公共空間になったことが確認されたことであると思う。これは、公共空間は国が責任を持って安心・安全を保障しなければいけないという宣言であると考える。従来ももちろん、サイバー空間が発展するには自由な情報流通が何より重要であるが、自由だけでは不十分であり、安心・安全な情報流通という方向にかじを切ってきていると思う。

一番大きな転換点は、国家の主体的な参加の必要性が今回明らかになってきた点である。従来、官民連携は事実として、技術的に先行する民に頼る面があったが、今後は、中国の存在や国家政策の考え方からいって、国家が半歩前に出なければいけないということが今回の戦略で明確に意識されたと思う。

国の仕事は、注意しましょうという国民に警戒を与えるということもあるが、防衛、国を守るという点で、国家によるサイバー攻撃にどう対応するかである。警察はサイバー攻撃への対応に半歩前に出ている。また、総務省がボットネットの指令元を割り出すために取り組んでいるが、非常に高く評価する。

最後に、大きな転換点としては、国と地方の関係も転換する。サイバー空間は地方の特色性も重要であるが、国がやらなければならない。これが、この一会議の提言ではあるが、

国にとって非常に重大な転換点である。

○宮澤本部員

最近、世界各国のサイバーセキュリティ対策が非常に踏み込んだもの、思い切ったものになってきている。アメリカでは５月に大統領令が出され、EUでも大きな施策が３月に出された。中国はその独自性をさらに増し、世界にそのルールを強いようとしている。当面は、自分の家は自分で守るという大前提は変わらないように思う。ビジネスの世界でもサイバーセキュリティへの対応は今や世界では必須で、今後、日本企業はより強力に対応を迫られるだろうと思う。日本でも企業に対する罰則や規制は安全保障上必要である。

また最近、日本のサイバーセキュリティ能力は北朝鮮やインドなどと同列であるいう報道があった。日本が専守防衛の考え方であるからと言う人も見られたが、的外れである。サイバーの世界では攻撃する能力こそが最大の防御だからである。その攻撃スキルはどの程度あるのか。そして、何が必要なのか。どうすれば追いつき追い越せるのか。

１点目は、前回述べたニューロ・ダイバーシティ、つまり日本のひきこもりやニートの活用であると思う。日本は100万人以上いるとされているが、その中にいる突出した能力を持つデジタル人材はまだ埋もれている状況である。

２点目は、デジタルにおいて細分化した分業の徹底であると思う。例えば天才ハッカーという存在も、デジタルのあらゆる分野でオールマイティな力を発揮できるわけではなく、ハッキングに特化している。企業においてもオールマイティな能力を持つ会社はないと思う。GAFAであろうと得意不得意はある。今後、日本のDXにおいては、丸投げはできない時代になってきた。もちろん、営業はできると言わざるを得ないと思うが、現場は困っている。いまだに日本ではプログラマーが全てを行う。例えばプログラマーにテストまでさせるのはナンセンスであると思う。つくる側はつくることだけを特化しないと能力の無駄であると思うし、バグなど到底見つけられるはずがない。分業と細分化で、日本独自のインクルーシブな昔のやり方を変えなければならない。大手、ベンチャーの垣根を越えて、オールジャパンで対応しなくてはならない。今、世界に負けない思い切った政策の実行こそが今後10年、20年の世界での日本の立場を決めるであろうと思っている。

○村井本部員

１点目はあらゆる分野がこのデジタル空間、サイバー空間の中で活躍するという時代になった。本戦略本部ができた初期の頃、各省庁の情報システムのKPIをつくったことがあるが、省庁ごとの通信簿をつけたため、非常に嫌がられた。しかし、今回は各省庁の守備範囲でどのような政策が必要であるかについて、もう一度KPIを定めて評価を実施すべきではないかと思う。この分野ではこのようなことを目標とする、それはいつまでに達成されるのかということである。そのような分野ごとの網羅性が必要になると思う。

２点目は、Allは全ての国民であると思う。そして、全ての国民がデジタル社会の中で生

きていくためのキーワードは地域であると思う。47都道府県の自治体全てで何をすべきか、誰がやるのか、国土全体は誰が責任を持つのか。これを内閣では考えなければいけないと思う。警察や自治体、消防、防災など、人の命を救うという観点で、全ての国民はAllの中に含まれる。これを基盤として考えるべきであると思う。

３点目は方法であるが、今までNISCで行ってきた方法は、サイバーアタックがあるとそれが問題となり、どのように対応していくかを検討する後追いの方法である。しかしゼロトラストの考え方と同じで、頭を抑えることを考えなければならない。頭を押さえるというのは何が起こるかを事前に考えることである。また、パイプラインの事案はランサムウェアであり、ランサムウェアは身代金を取るわけである。本事案では、攻撃者を特定して身代金を取り戻すまで実施した。このように全体が力を合わせるのは、内閣の場でなければできないことであり、そのための能動的体制と協調体制の２つの体制の整備が必要である。

最後４点目は、サイバーセキュリティ月間は、戦略本部で毎年２月ごろに実施しているが、今般、10月10日、10月11日にデジタルの日を実施することとなった。この２つをうまく連携して国民全体に意識を広げるという、デジタルの日とサイバーセキュリティ月間の乗り入れを実施していただくと、いろいろなことを国民に伝える機会になるのではないかと思う。

○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）

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、オリンピック・パラリンピック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。

東京大会まで、あと16日となった。サイバー攻撃による被害が国内外で相次いで確認されるなど厳しい情勢にある。各大臣にあっては、各省庁や所管業界における対策の再確認と徹底をお願い申し上げる。

政府では、東京都、組織委員会等と連携し、訓練を重ねてきた態勢を生かし、サイバーセキュリティの確保に万全を期してまいる。

また、次期サイバーセキュリティ戦略（案）については、引き続き策定に向けて必要な手続を進めてまいる。予算の確保や体制の強化等について、各大臣と連携して進めてまいりたいと考えるので、御協力をお願い申し上げる。

○棚橋国家公安委員長

デジタル化の進展に伴い、サイバー空間が公共空間へと進化を遂げていく一方で、サイバー空間における脅威は極めて深刻である。先ほど前田本部員、村井本部員から警察の活動の重要性について御言及をいただき、また、遠藤本部員、中谷本部員からは後ほど申し上げるサイバー局に対する非常に肯定的な御評価をいただいた。

サイバー空間においても、実空間と変わらぬ安心・安全を確保することは、国民が安心して暮らせる社会の実現のために今や不可欠となっていることは皆様方御承知のとおりである。

そこで、警察としてもその実現に向けて、令和４年度にサイバー空間の脅威に対処するためのリソースを集約したサイバー局を設置するとともに、国際共同捜査への参画や重大サイバー事案への対処を行う国の実働部隊を創設することを検討している。

これにより、組織の総合力を一層発揮し、サイバー攻撃・サイバー犯罪の厳正な取締りや実態解明、関係事業者や国内外の関係機関等と緊密に連携した被害の未然・拡大防止対策を推進し、これまで以上にサイバー空間の安全・安心の確保に努めてまいる。

○武田総務大臣

サイバー攻撃が巧妙化・複雑化する中、これに対応し、サイバーセキュリティ戦略を改定することは時宜を得たものと考えている。

本日示された次期サイバーセキュリティ戦略（案）では「自由、公正、かつ安全なサイバー空間の確保」を基本理念として、国民が安全で安心して暮らせるデジタル社会などを実現するため、政府一体となって施策を推進する必要があるとしている。

総務省としても、安全かつ信頼性の高い電気通信ネットワークを確保するため、サイバー攻撃に対する積極的なセキュリティ対策を推進すること、サイバーセキュリティ情報の収集・分析能力の向上に向け、NICTの知見や技術を活用するとともに、産学官連携を加速することなどを通じて、我が国におけるサイバーセキュリティの確保に貢献してまいりたい。

○岸防衛大臣

国家主体が関与するサイバー攻撃が行われる中、今後、インフラの制御系システムやサプライチェーン等の脆弱性を狙った攻撃によって、安全保障上極めて重大な事案が引き起こされる可能性も否定できず、我が国全体としてサイバーセキュリティを強化することが急務と考えている。

本日の決定事項である次期サイバーセキュリティ戦略（案）、令和４年度予算重点化方針においては､いずれも国全体や政府機関としての対策の方向性をしっかり示されており、極めて意義のあるものと認識している。

防衛省においては、今月１日に、新たな取組として、高度な専門的知見を持つ民間の方２名をサイバーセキュリティ統括アドバイザーに私が任命した。それぞれから助言をいただき、サイバー防衛能力の一層の強化を図ってまいる。また、今年度、自衛隊サイバー防衛隊を新編し、防衛省・自衛隊のサイバー防護機能の一元化に着手するとともに、人員規模も拡充し、体制を大幅に強化する。

また、間もなく開幕する東京2020大会への協力もしっかり行ってまいる。

○平井デジタル改革担当・情報通信技術（IT）政策担当大臣

20年前につくられた旧IT基本法は高度情報通信ネットワーク社会の形成を目的としていたが、5月に成立したデジタル改革関連法案の中核であるデジタル社会形成基本法では、大量かつ多様なデータを利活用して創造的で活力あるデジタル社会を形成することを目的とし、その実現の司令塔としてデジタル庁を設置することとされている。

現在、９月１日のデジタル庁の設立に向けて政策やプロジェクトの整理と組織づくりを進めている。デジタル庁は、国・地方を含めた情報システムの整備方針を策定し、予算一括計上等を通じて統括監理を行うとともに、マイナンバー制度等の企画立案、データ戦略の推進、最先端クラウド基盤やネットワークの整備、国の重要な情報システムの開発・運用等を担うことになる。

こうした政策とサイバーセキュリティの強化は一体的に進めるべきものであって、デジタル庁として、新たな脅威の増大と5G・クラウド化等の技術変化を踏まえつつ、国・地方等を通じたセキュリティの在り方を検討し、整備方針において具体化すること、強力なセキュリティの専門チームをつくり、様々な事案に迅速に対応できる体制を構築するとともに、各国のカウンターパートと技術面を含めた議論を進め、システムの設計段階からの対策強化を実現するなど、具体的かつ実践的な形で、政府一体となってサイバーセキュリティ政策を推進できるように、関係機関との連携を強化していきたいと考えている。

また、村井本部員から御提案があったサイバーセキュリティ月間とデジタルの日との連携というものは非常に良いアイデアだと思う。

○長坂経済産業副大臣

サイバー攻撃は、年々その脅威を増し、社会インフラの機能停止まで引き起こすようになっている。

こうした状況に対して、先ほど本部員からも御指摘があったように、米国政府は今年５月にソフトウェアのサプライチェーンに係るセキュリティ対策の強化や政府システムのセキュリティ強化などを定めた大統領令を発出し、国としての対処機能のさらなる強化に着手した。我が国としても、取組を早急に進めなければならない。

今般の次期サイバーセキュリティ戦略（案）には、サイバー攻撃への対処官庁のリソース結集と連携強化、制御システムのインシデント原因究明機能の整備などが盛り込まれ、時宜を得た内容となっており、経産省としてもしっかりと貢献してまいりたいと考えている。

さらに、昨年設立されたサプライチェーン・サイバーセキュリティ・コンソーシアムとも引き続き連携し、中小企業や地域の企業を含む産業界全体のサプライチェーン対策の強化を後押ししてまいる。

○中西外務大臣政務官

我が国からも委員を出した国連サイバー専門家グループが５月末に提言をまとめた。我が国は、同グループの一員として、その後、国際法のサイバー行動への適用に関する見解を提出し、公表する等、サイバー空間における法の支配の推進に貢献してまいる。引き続き、戦略の着実な実施に向け、同志国・同盟国との連携を強化し、我が国の安全保障に資する環境醸成に貢献してまいる。

ランサムウェア攻撃は、重要インフラを機能不全にする等、国家安全保障の観点からも深刻な問題を起こす。先月のG7サミットでは、各国が自国の国境内から活動するランサムウェアの犯罪ネットワークの脅威に緊急に対処するよう確認されたところであり、国家の領域管理責任を含め、国家の行動規範の強化に向けて取り組んでまいる。

（３）決定事項の決定

○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）

それでは、本日お諮りした３件の決定事項について、異議はないか。

（「異議なし」と声あり）

○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）

異議なしということで、本案を決定させていただき、今後、本決定に基づき、パブリックコメントなどの手続を進めてまいる。

（４）本部長締め括り挨拶

本日の会合では、次期サイバーセキュリティ戦略（案）などについて審議し、また、決定した。当面のサイバーセキュリティに関する取組に当たり、特に次の３点を念頭に置いて進めていただくようお願い申し上げる。

１点目は、東京大会における万全の取組である。いよいよ東京大会の開催が間近に迫ってきた。これまで、度重なる訓練の実施など、リスクを極小化するため、周到な準備を進めてきたところである。その成果を十分に発揮していただき、大会期間中、何らかの異常を探知した場合には速やかな初動対応を講じるなど、基本的な対策を徹底し、関係組織が一丸となって冷静かつ適切に対応していただくようお願い申し上げる。

２点目は、ランサムウェア対策の強化である。世界的にランサムウェアによる攻撃が多く確認されており、経済社会活動、国民生活に影響を与えるような被害も出ている。G7サミットでもランサムウェアの犯罪ネットワークによる脅威の高まりが示され、国際的な協力もますます重要となっている。関係機関が連携し、ランサムウェア被害の防止に向けた取組を推進していただくようお願い申し上げる。

３点目は、サイバー攻撃に対する一層の対応能力と連携の強化である。民間における対応の強化を促すとともに、深刻なサイバー攻撃が発生した場合には、国が持ち得る全ての能力と手段を活用して、初動対応から政策的な措置までを政府全体で一体的に講ずる必要

がある。そのため、日常における訓練を含め、体制や機能のさらなる強化に具体的に取り組んでいただきたい。また、我が国の安全保障上の利益を守るためにも、防御、抑止、状況把握などの個々の能力向上を図ることはもちろん、関係機関の連携のより一層の強化を図っていただきたいと思う。

以上、３点申し上げたが、サイバーセキュリティに関する我が国の取組について、国内外への情報発信にも努めながら、引き続き次期戦略の最終決定に向けた作業を鋭意進めていきたいと思う。

引き続きよろしくお願い申し上げる。

－ 以上 －