サイバーセキュリティ戦略本部
第26回会合　議事概要

１　日時

令和３年２月９日（火）　　17：00～17:40

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
橋本　聖子	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
武田　良太	総務大臣
梶山　弘志	経済産業大臣
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
宇都　隆史	外務副大臣
遠藤　信博	日本電気株式会社取締役会長
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	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
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
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

〇大変お忙しい中、お集まりいただき、感謝申し上げる。　本日は、今年後半に策定を予定している「次期サイバーセキュリティ戦略」に関し、その基本的な考え方を取りまとめていただくこととしている。

本日、デジタル改革関連法案が閣議決定された。サイバーセキュリティの確保は、デジタル改革を支える基盤として、今後ますますその重要性が高まることになると考えている。

また、最近では、利用が拡大しているテレワークを狙った攻撃が確認されること、身代金型マルウェアによる攻撃が活発になっていること、悪意のある機能を持つ部品等が調達のプロセスに紛れ込む懸念が生じていることなど、私どもの社会の様々な局面において、セキュリティリスクに対してより意識的な対応が必要になっていると考えている。

次期サイバーセキュリティ戦略においては、こうした環境の変化を的確に捉えた上で検討を進めることが重要になる。

本日は、活発な議論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の検討に当たっての基本的な考え方（案）について

・国立研究開発法人情報通信研究機構の第５期中長期目標（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

【討議事項】

・次期サイバーセキュリティ戦略の検討について

【報告事項】

・東京2020大会に向けた取組状況について

・政府のサイバーセキュリティに関する予算（2021年度政府案等）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について

・次期重要インフラ行動計画の検討について

・2021年サイバーセキュリティ月間について

・デジタル改革をめぐる動向について（参考）

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。

○（橋本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。

○（宮澤本部員）
COCOAの不具合について、このような不具合がどうして起こるか、どうしてなくならないのか、どうしたら今後起きないようにできるか、この点だけ話したい。
まず、大前提として、バグのないシステムはこの世に存在しない。デジタルのシステムである以上、必ずバグは存在する。そして、大前提のもう一つは、日本人のクオリティーへのこだわりは尋常ではないほど厳しいということだ。
2001年頃、その当時は日本の首相が短い期間で替わっていた時期だが、アメリカの世界的な企業の社長から、なぜそんなに首相が交代するのかと質問されたことがあった。日本人１億2000万人は全員がデバッガーなので、まずはバグを見つけるところから始まると答えたところ、今までの答えで一番納得できたと言っていた。
ジャパン・クオリティーは国民性といえる。それこそが今日の日本の製造業をはじめ、全ての産業を支えてきた。品質へのこだわりは武器だ。だからこそ、COCOAのバグのようなものはどこの国よりも許されない。今後もこのチェックは続くだろう。
それでは、その様な強力な国民デバッガーたちに、今後、DXにおいて新しいシステムをリリースする我々はどうしたらいいのか。答えは２つだと思う。１つは、よりシンプルなシステムの制作と、もう１つはプログラマーでない人たちによる第三者検証、この２つしかないと思う。また、これは同時に実行しなくては意味がない。
システムをつくる上で一番最初に言ってはいけないことは優秀なプログラマーたちに向かい、どうしたらいいかと聞くことだ。そうすると、力のある人ほど様々な方法が思いつき、結果、先進性はあるが、複雑な仕組みをつくりかねない。自らの能力を誇示するようなシステムは必要ない。実用性を最重要視するシステムをつくるのならば、その構造はよりシンプルでなくてはならない。例えば、車のブレーキは油圧が良く、シンプルなものほど壊れにくく、バグは少ないと思う。
この１つ目はすごく分かりやすく、すぐにできることだが、問題はその次で、プログラマーやシステムをつくる側でない人たちで行う第三者検証、システム

を使う側、あえて壊す側からのチェックを行う体制の確立だ。
例として、以前、銀行などにあるATMのタッチパネルのシステムのチェックをしたときに、タッチパネルのボタンを１個ずつ、１本ずつ、ボタンを押していくと大丈夫。10本指で全部ボタンを押しても大丈夫。10本押したまま11本目の指でボタンを押したらシステムが停止するということがあった。これはそのシステムをつくる側からでは絶対に見つけられない。システムをつくる側の想定している想定外のテストだ。これはチェックする方向が１方向のみだから見つからないといえる。
今回のCOCOAのバグも、少し前の東京証券取引所のバックアップシステムのチェックミスに関しても、全く同じといえる。どれだけ優秀なプログラマーを集めても、絶対に見つけられなかっただろう。その理由は、役割が違うからだ。それが日本産のスマートフォンが世界で負けた理由でもあり、今なお続いている日本産デジタルクオリティーの穴であると思う。作る側のプライドや自身が壊す側からのチェックを拒むような、日本の独自の悪しき習慣があるとすれば、壊さなければならないだろう。
作る側だけのテストのデメリットがもう一点ある。開発費の３割以上がテストの費用と言われるが、作る側の単価の高い人たちが残業してテストをすると、結果、高くなる点だ。
今後、政府がリリースしたシステムやソフトウェアにバグが多発し、セキュリティに穴が見つかって不具合が起こるたびに、デバッガーである国民に失望されないように、私はSimple DX with Qualityをしっかりと見据えた上で作っていくのが重要だと思う。

○（村井本部員）
３点申し上げる。１点目は、デジタル庁の準備は平井大臣の下で進んでいると思うが、この中で大変気になってくることの一つが地方のデジタル化だ。これを進めないと、この国は駄目だと思う。そして、地方を元気にしていくためには中小企業が重要といえるため、中小企業という軸と、１次産業を含めた新しい分野のデジタル化が進んでいく社会を作っていくことになると思う。
その上で、それぞれのところに人材がいるのかという問題がある。金融関係は中小企業との関係で大変重要だと思う。それから、教育も地方の中で大変重要な要素だと思う。ここのところのサイバーセキュリティに関する手当てをどういうふうにできるのか。分野が非常に多様になったときに、それぞれの分野、つまりサイバーセキュリティ戦略本部の大臣たちはそれぞれの専門の大臣だが、そうでない分野のデジタル化が進む中で、サイバーセキュリティのことも取り組んでいただきたいというのが１点である。

２点目は、資料１でも、COVID-19で新しいことが起こり、弱いところ、新しいところ、目立つところを狙ってくるという報告だった。ランサムウェアが病院を狙い、Emotetが台頭するといったことがこの１年で起こったが、これは全て目立つところ、弱いところをうまく突くための新しいやり方といえる。したがって、それに対応しなければならない。

３点目は、選挙の問題だ。先日、アメリカの大統領選挙があり、CISA、Cybersecurity and Infrastructure Security Agencyが非常に力強いアナウンスメントをしている。アメリカとの会議の際にも、今回は前回と違って相当頑張ってプロテクトしたと何度もアメリカ政府関係者から聞いている。

今度、東京2020大会の前か後になるかはわからないが、日本でも選挙が行われる。そうすると、日本の場合はエスピオナージみたいな話はあまりないかもしれないが、これは前田本部員に聞かなければいけないが、選挙に対する備えも大事になってくるのではないかと思う。

○（遠藤本部員）

次期サイバーセキュリティ戦略の検討にあたっての基本的な考え方に関して、異存はないが、追加でコメントしたい。

第一の環境変化や国際情勢等を踏まえ時宜を得た対応方針とすることは、我々の課題として、直近のテレワーク、5Gという問題があるが、少し先には量子コンピューター及び量子暗号という長期的な目線が必要だろうと思う。ぜひ、その両方の観点で考えていただきたい。

また、COVID-19ではDX化が加速しようとしている。それも従来では考えられないスピードで加速しており、急速に大組織から中小組織に、そして組織から個人へという広がりが見えている。そのような意味では、DXセキュリティという認識を各組織、そして個人が強く認識してDXを推し進めることが必須であり、そのケアが必要だろう。

特にリモートワーク、リモート教育等の個人端末へのケアが重要であるとともに、サプライチェーンやロジスティックスのような共通DX基盤が出来上がると、その基盤の中に中小または個人の企業等のアクセスがなされて、それによって企業の活動が活性化されるということになると思うが、このような基盤構築による利用というのは一気にアクセス領域が広がるので、そのための対応が必要であろうと考える。

第二の政府の役割を意識した政策立案の基盤となるものにすることについては、攻撃者優位の解消に向けて戦略的な取組に関係するが、犯罪者の協力禁止の法律の制定はもちろんだが、セキュリティ教育や人材育成を通して、サイバー空間での免疫力を高めることも重要であると思う。

私自身も、今、サプライチェーン・サイバーセキュリティ・コンソーシアムや情報処理推進機構の産業サイバーセキュリティセンターで、企業でのセキュリティ人材育成を含めた活動も行っている。それにより人材育成も進んできている。

ただ、一方で、令和２年12月に米国の大手企業や政府機関で発覚したサイバー攻撃は、SolarWinds社のモニタリングソフトのソースコードそのものを改変するといった巧妙なサプライチェーン攻撃と見られていて、数か月の間、どの組織でも見逃していた。特定組織のセキュリティ対策を幾ら強化しても、この手の攻撃を完全に防ぐことが難しい状況で、全ての関係する組織での対策強化が必要だ。

このようなサプライチェーンリスクに対応するためには、日本全体の対処能力を向上して国力を高めることが必要不可欠で、特に政府主導での強い対応をお願い申し上げる。

第三の発信力を意識して我が国の考え方を内外に示すものとすること、については、日本の国際標準策定への貢献とサイバー犯罪撲滅の貢献の２つを強化することが必要であろうと考える。

特に、近年、欧米の司法機関ではサイバー犯罪者の指名手配、それからサイバー犯罪組織の解体を積極的に行っている。我が国においても、国民や企業の国際的なサイバー攻撃から積極的に防御するためには、攻撃や事故の全容を把握して犯人を特定する能力を持つこと、そして各省庁、産業の連携の下、進めていくべきだと思う。

特にｅシール、電子署名等のトラストサービスの需要が高まっているため、国内のみならず、国際的な標準化が重要で、この対応での政府の積極的なリーダーシップも期待したいと思う。

○（小野寺本部員）

２点申し上げる。１点目、COCOAの件については宮澤本部員の発言があったので、それに尽きると思うが、私が申し上げたいのは、このアプリのように一般の人が使うものについて、宮澤本部員からはプログラマー以外の検証という話があったが、ＫＤＤＩでもそういうものについては、一般の社員、技術者ではない社員に使用してもらっていろいろ出てくるというのが実態であるため、ぜひ、技術以外の人たち、本当はまず厚生労働省の職員の方が使ってみるというのが普通だと思う。そこでいろいろ問題が出てくるはずなのだが、残念ながらその点が抜けていたのではないかと思う。この点は、平井大臣がいらっしゃいますが、ぜひよろしくお願いしたい。

２点目は、セキュリティの教育の問題だ。社会経済全体での人材不足、偏在、

リテラシーギャップの顕在化という言葉が使われているが、これはまさしくそのとおりだと思う。先ほどのCOCOAの問題にしても、リテラシーギャップが非常に大きな問題だと思う。ある程度分かっている人が検証すれば、本当に様々なものが即座に発見できるはずだが、そういうリテラシーがなかなかないというのが実態ではないかと思う。

この点は以前も申し上げたが、現在、文部科学省でGIGAスクール構想によって初等中等教育からプログラミング教育の拡充が図られている。これは非常に良いことだと思っているが、問題は教える人だといえる。この教える人をどう育てるのかが重要だ。産業界を卒業した人たちが手伝うことはもう既に動いていると思うが、やはり一番問題なのは、これから教員になるデジタルネイティブ世代の学生に対して、一体どういうデジタル教育がされているのかということだ。文部科学省のデータを見ると、教員養成過程の卒業生は国立大学法人だけでも年間約１万名となり、その中で教員になるのは8,000名程度のようだ。文部科学省では、現在、デジタル教育の指導要領を決めていると思うが、それをしっかりと学生に教えることができれば、年間約8,000人のリテラシーのある教員が育つということだと思う。ぜひこの点についてもう一度検討いただきたい。

○（後藤本部員）

決定事項は適切であり、賛同する。その上で、次期サイバーセキュリティ戦略に向けて２点申し上げる。

１点目は、デジタル時代の安全保障についてである。本日閣議決定されたデジタル庁設置法案、デジタル改革関連法案によりデジタル化が我が国で急進することは明らかで、これは画期的だと思うが、同時に社会全体のデジタル依存度が高まる時代に突入するということを意味している。その意味で、サイバー技術、デジタルサービス、データ、３つの観点から大規模リスクに備える戦略が大事だと思う。万が一に備えて、国産の技術、サービス、データ、それを支える人材を社会インフラとして一定程度確保できるような施策の準備を始めるべきだと考える。

技術については、Society5.0に向けた内閣府の戦略的イノベーション創造プログラム（SIP）などの研究開発や、本日の議題にある国立研究開発法人情報通信研究機構の取組があるが、これらを確実に進めることに加え、デジタル社会の備えとして何が必要なのかを考えるべきだと思う。

２点目は、既に話が出ているが、サイバーセキュリティの人材に関することだ。2020年はMAZE、Emotet、SolarWinds等、経済活動基盤そのものが危険にさらされてきた。

先日、国際協力によってEmotetの拠点がテイクダウンされたことは朗報だが、

我が国の場合は、誰がどのような体制、能力をもって国際的に貢献していけるかが課題だと考える。

まず、国が率先して、高いサイバーセキュリティ能力を有する人材育成をリードし、人材の役割ごとの模範を示していただきたい。その姿勢が広く民間の経営層から現場、一般ユーザーまでの環境づくりに貢献すると考えている。

その意味で、本日の資料を拝見して、国立研究開発法人情報通信研究機構や防衛省などは積極的に取り組んでいるようだが、減額になっている人材育成施策もあるようだ。ぜひ強化をお願いしたい。

○（中谷本部員）

決定事項に賛成である。その上で５点申し上げる。

１点目に、このコロナ禍に乗じて地政学な動きを加速させ、また、経済的利益を得るためにサイバー攻撃を行う勢力が増大しているとの危機感を持っている。サイバー攻撃者の側では組織化・分業化が進み、ランサムウェアの高度化などによりビジネスとして成立するという状況になっているようだ。

このような状況下で、経済産業省が中心となって昨年末に経営者への注意喚起を行ったことは、時宜を得た重要なことだと思う。ランサムウェア攻撃に対して身代金を払っても復旧の保証はなく、また、安易に身代金を支払うと、テロや組織犯罪の支援として米国からペナルティーを科されかねないことを勘案して、コンプライアンスを重視した判断をすること、海外拠点とのシステム統合については、サイバー攻撃懸念国の拠点との統合は避けること、重要情報はオフライン管理をすることが特に重要だと考える、いずれにせよ、経営トップが判断しなければならないことである。

２点目は、サイバー攻撃が発生した後の対応として、航空機事故の場合に設置される事故調査委員会のようなサイバー事故調の創設を検討する時期だと思う。サイバー事故調は攻撃者の特定、アトリビューションにも資するものであり、ひいては国際的な貢献にもなると考える。

３点目は、企業の重要な知的財産権を侵害する経済サイバー諜報に実効的に対処できるようにすることが重要だと考える。経済サイバー諜報は、公正な競争条件をゆがめるものであり、また、WTOのTRIPS協定の39条で規定された、開示されていない情報の保護の侵害にもなると考えられる。有事の際には首尾よくWTOの紛争解決手続に付託できるように、頭の体操をしておくことも有用だと考える。

４点目は、選挙に対する外国勢力によるサイバー手段を用いた干渉が、国際的に深刻な問題となっている点だ。選挙干渉は内政干渉であると同時に、主権侵害にもなり得る深刻な国際法違反といえる。我が国は日本語環境だから選挙

干渉は受けにくいなどと楽観視することなく、政府として万全の防止体制を取っていただくことを強く望む。
５点目は、新しい高校学習指導があり、また、国家公務員総合職試験では2022年度試験から「デジタル職」が新設される方針であると報じられている。いずれも、今後の社会にふさわしい方針だと思うが、ぜひサイバーセキュリティも大いに出題に加えていただくようにお願いしたい。

○（野原本部員）
今日の決定事項の２点はいずれも異論はない。
今日の討議事項の次期サイバーセキュリティ戦略の検討について、３点申し上げたいと思う。
１点目は、サイバーセキュリティ戦略作成のスタンスと戦略の発信についてである。策定に当たっては、サイバーセキュリティ対策に直結する課題について、NISC及びセキュリティ担当部署が検討するだけではなく、政府の総意としての戦略となるよう、警察庁、総務省、外務省、経済産業省、防衛省、デジタル庁等々の各省庁とNISCが頭を寄せ合ってしっかりと議論した上で戦略を策定していただきたい。その結果として、国際状況や環境変化をしっかりと全体として踏まえたものができると思うし、それだけメッセージ性の高い、方向性の明確な戦略が策定できるのではないかと思う。
そうしてできた政府の戦略としてのサイバーセキュリティ戦略をしっかりと発信していただきたい。我が国の考え方を国内外に明確に発信し、特に海外に向けては国際協調の重要性を認識し、攻撃者に対する抑止の効果や、各国政府に対する我が国の立場の理解をしっかりと促せるように、発信についても強く意識してやっていただきたいと思う。
２点目は、アトリビューションのための体制整備である。資料１－１の第２のところに括弧書きで「攻撃者との非対称な状況の改善も含む」と書き込んでいるが、サイバー攻撃は攻撃サイドが有利で、防御サイドは不利と言われている。そのアンバランスを解消するために、我が国としてもアトリビューション、つまり攻撃者を追跡、特定できるような体制を構築する必要があると考える。したがって、アトリビューションについて政府全体で議論、整理をした上で、アトリビューションできる体制を構築すべきだと思う。しっかりと議論していただきたい。
３点目は、コロナ禍を契機に、先ほどからもいろいろ出ているが、リモートワークの浸透など、デジタル・トランスフォーメーションが進んでいる。このリモートワーク前提の環境整備というのがテンポラリーなもの、臨時のものとなってしまうのではなく、ニューノーマルの必須の継続的な環境として浸透す

るように、デジタル庁との連携の下、しっかり進めていくべきと思っている。
一方で、リモートワークやクラウドサービスを狙ったサイバー攻撃が増えているために、サイバー攻撃リスクが高いからという理由で、DXや働き方改革が後戻りしてしまうのではないかという気がしており、そうならないようにしたいと思う。
例えば、リモートワーク体制におけるセキュリティ対策としては、ゼロトラスト・アーキテクチャーへの転換が有効だと言われている。しかしながら、それを具体的にどういうふうにすればよいのかという事は個々に違うということで、なかなか具体的施策が分かりにくいという課題がある。
そのため、次期戦略を検討する上でも、どういう対策をすればいいのか、具体的な対策、方法を明示して、それをしっかりと周知、普及させるという形にしていただきたいと思う。

○（前田本部員）
私は長く犯罪を研究している研究者であるが、今回のパンデミック、コロナの動きで思い出すのは、20年前の治安であり、あの頃はメルトダウンという言葉が使われ、刑務所があふれて留置場がなくなった。日本の犯罪の数は多くはなく、ヨーロッパやアメリカの10分の1や100分の1だという中で、国民は少し犯罪が増えると非常に不安になった。ただ、政府は具体的に手を打って乗り越えたのである。まだ何が起こるか分からないが、今はもう歴史的に最善の状況に近いと考えている。
今回の新型コロナウイルスも必ず乗り越えられるというか、もう乗り越えていると思うが、ここで学ぶべきポイントは有事への備えのスタンスを少しシフトさせることだと思う。もちろん政府は有事への備えをやっており、防衛省も全部有事への備えをしているわけだが、マスコミの影響もあって、短期的な成果主義が求められていることもあり、病院の数、ワクチンの件及び国土の問題で言えば川辺川ダムで動いてきた。最近で言えば、半導体のありようが日本で作らないと言っていたのが変わろうとしている等、様々なものが動くわけであり、そのときの長期的視点が重要である。
我々、大学側から見ると、研究で大事な視点は、額ではなく、成果主義だけでもなく、長期的に育てる視点での基礎研究が一番重要だということである。
ほかに申し上げたい点が２点ある。１点目は先ほど中谷本部員の発言の、国家安全保障の視点である。インターナショナルといっても、国家の対立で米中の関係を無視しては語れないということなのだと思う。
デジタルが進むと必ず外国はデータを盗みに来る。国家の安全保障の観点からサイバーを考えることは重要である。

２点目は、遠藤本部員や野原本部員の発言にあったアトリビューションの問題であるが、我々研究者から見ると、攻撃者優位という言い方は非常に抵抗感がある。最近はビットコインに関して、NEM交換で31人が捕まったり、ドコモの口座について中国を追い詰めていたり、悪事をする人間を捕まえ、そして追い詰めている。努力が足りないといえばそうかもしれないが、確実に実績を上げているため、引き続き頑張っていただきたい。

最後に、その意味で、国家公安委員長の言明をぜひ期待したい。

○（橋本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。

東京2020大会まで半年を切った。政府では、「サイバーセキュリティ対処調整センター」を中心として、関係機関と連携した実践的な訓練などを通じ、対処能力の向上を図ってきた。

一方で、最近も、新型コロナウイルス感染症の感染拡大に乗じたものも含め、国内外で多くのサイバー攻撃が確認されている。

東京2020大会に向け、関係機関との連携の下、訓練の継続に加え、最新の情勢の分析・検証を通じ、サイバーセキュリティ対策をしっかりと仕上げてまいりたい。

次期サイバーセキュリティ戦略案の検討に当たっては、これら東京2020大会に向けた取組の活用に加え、政府全体として推進する「デジタル改革」に寄与するとともに、経済社会の変化や安全保障環境の変化をはじめとする国際情勢、新型コロナウイルスの影響・経験を踏まえて検討を行ってまいりたい。

引き続きの協力をお願い申し上げる。

○（小此木国家公安委員長）

新型コロナウイルス感染症の感染拡大に乗じたものを含め、サイバー攻撃、サイバー犯罪が国内外において発生し、サイバー空間における脅威は極めて深刻なものとなっている。

デジタル化の進展に伴って、サイバー空間は今や広く国民が参画する重要な公共の空間といえる。国民、事業者、公的機関がそれぞれの立場で安全なサイバー空間の確保を目指すとともに、相互に連携して取り組むことが必要であると考える。

警察では、サイバー犯罪の取締りに加えて、関係事業者等と連携した被害防

止対策の実施や、サイバー攻撃の実態解明を推し進めて、深刻化する脅威について利用者などに幅広く注意喚起を行うなど、組織の総合力を発揮した対策を推進している。
引き続き、国民が安心して参画できる安全なサイバー空間の実現を目指して、前田本部員からも御指摘いただいたことも含め、しっかりと取り組んでまいりたい

○（武田総務大臣）
総務省では、昨年７月に「IoT・5Gセキュリティ総合対策2020」を取りまとめ、NISCや関係府省庁とも連携しつつ、IoT・5G時代のサイバーセキュリティ確保のために必要な施策を推進している。
ICTに関する唯一の国立研究開発法人である情報通信研究機構、NICTにおいても、脆弱なIoT機器の調査や実践的なサイバー防御演習による人材育成などを実施しているところであり、本日御議論いただいた中長期目標が着実に達成されるよう、引き続きしっかりと取り組んでまいりたい。
さらに、NICTが有するサイバー攻撃観測網を活用して、不審な通信を検知・通報する仕組みを地方自治体などに広く展開させるほか、NICTの知見や技術を広く活用し、サイバーセキュリティに関する情報分析や人材育成の強化に産学官連携で取り組む拠点の形成を進めていくこととしたいと思う。
総務省としては、ICTが国民生活や経済活動の基盤としてますます重要な役割を担うようになる中、引き続き、関係府省庁と連携しつつ、我が国のサイバーセキュリティの向上に尽力するとともに、次期サイバーセキュリティ戦略の策定に向けて協力してまいりたい。

○（梶山経済産業大臣）
サイバー攻撃はますます増大をしており、今やサイバーセキュリティは最も重要な経営課題となっている。
こうした状況を受けて、昨年12月、私から経営者の皆様に向けて、最近のサイバー攻撃の状況に関して注意喚起を行った。また、産業界の主導でサプライチェーン・サイバーセキュリティ・コンソーシアムも昨年11月に立ち上がったところである。
しかしながら、最近のサイバー攻撃の高度化、激化を考えると、経済活動の基盤そのものが突き崩されるのではないかという不安を感じざるを得ない。次期サイバーセキュリティ戦略では、看過できないサイバー攻撃に対して国が対処するという意思を改めて示し、そのための体制を構築して、有志国と協力して対処していくことを明らかにすべきと考えている。

NISCを中心とした関係機関とともに、経済産業省としても産業界やIPA、JPCERTコーディネーションセンターなどの専門機関との協力関係、制御系セキュリティの知見などのリソースを提供し、できる限りの貢献をしてまいりたいと考えている。

○（岸防衛大臣）
サイバー攻撃の脅威が日々高度化、巧妙化する中で、サイバー空間における能力の向上は喫緊の課題である。防衛省・自衛隊では、防衛計画の大綱及び中期防衛力整備計画を踏まえ、令和３年度予算案において、サイバー防衛隊等の体制強化やシステム・ネットワークの安全性の強化などを計上している。引き続き、サイバー防衛能力の抜本的強化を図ってまいる。
また、社会全体で情報通信ネットワークの活用場面が増えているが、同時にサイバー攻撃のリスクも高まっている。社会全体のサイバーセキュリティの強化は、我が国の安全保障上も重要な課題と認識しており、次期サイバーセキュリティ戦略の検討に防衛省としても積極的に参加をしてまいる。

○（平井デジタル改革担当・情報通信技術（IT）政策担当大臣）
今日は、本部員の皆様の御意見を色々聞かせていただき、私も色々考えなければいけないと思った。
本日、デジタル庁設置法案等、デジタル改革関連の法案が閣議決定されたが、成立すれば９月１日にデジタル庁がスタートする。デジタル庁はサイバーセキュリティ戦略本部と緊密に連携して、サイバーセキュリティに関する基本的な方針を示す。各省庁のシステム予算に関して、今後、デジタル庁で要求の段階から統理するが、システム予算の中のセキュリティの部分は、予算書を見ただけでは分からない。結局、総理が言われている縦割りの打破は、セキュリティ部門で一番必要だと今日改めて思った。
デジタル庁が９月１日からスタートし、システムセキュリティの専門チームを配置する方針は既に決まっているが、このチームの役割が非常に大きいと改めて思ったので、サイバーセキュリティ戦略本部と相談させていただきながら、トータルでこの国として一番いい体制を考えたい。
アーキテクチャーのあり方も全部見直しますので、当然セキュリティも根本的な考え方を変えなければいけないと思う。
その意味で、これからサイバーセキュリティ戦略本部と緊密に連携しながら、９月１日までに考えていきたいと思う。

○（宇都外務副大臣）

新型コロナウイルス感染症の世界的な感染拡大により、サイバー空間への依存度が一層高まる中、技術発展に伴い、サイバー攻撃は高度化、巧妙化している。

デジタル社会の推進に当たり、自由、公正かつ安全なサイバー空間の確保に向けて、我が国自身の強靱性を高めるとともに、国際的な連携を一層強化していく必要があると考えている。

外務省としては、サイバーセキュリティに係る脅威の増大を含む、安全保障環境の変化などを踏まえ、同盟国・有志国との連携を強化していくほか、サイバー空間における国際的なルールづくり、発信力強化などにも引き続きしっかり取り組んでいく考えである。

次期サイバーセキュリティ戦略の策定にもしっかりと貢献してまいる。

（３）決定事項の決定等

○（橋本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２件の決定事項について、異議はないか。

（「異議なし」と声あり）

○橋本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、「次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方」を決定した。今後、具体的に戦略策定を進めることとなるが、検討に当たって特に念頭に置いてほしい事項３点をお願い申し上げる。

１点目は、デジタル改革を支えるサイバーセキュリティという観点からの取組の推進だ。

制度や政策、組織の在り方等のデジタル改革を通じて社会全体のデジタル・トランスフォーメーションを進めるに当たっては、サイバーセキュリティの確保が大前提になる。我が国が目指すデジタル社会のビジョンを実現するため、DX with Cybersecurityという考えを強く意識した戦略となるよう検討を進めていただきたい。

２点目は、組織化・洗練化されたサイバー攻撃の増加や、新型コロナウイルス感染症の影響といった環境変化を踏まえた対応の強化である。

サイバー攻撃から我が国の重要な情報資産を守るためには、攻撃者優位とさ

れる現状を看過せず、国内外の関係機関が連携した包括的な防御策、抑止策を示す必要がある。また、テレワークやクラウド、5Gの利用拡大など、新たな環境の中で、変化するセキュリティリスクの動向を的確に踏まえた戦略にしていただきたい。

３点目は、国内外への発信力の強化だ。サイバーセキュリティ対策を実際に行う方々に向けて具体的な行動につながるメッセージとなるように、また、ますます重要になるこの分野における国際協調に鑑み、我が国の立場や政策を明確に示す戦略となるようにしていただきたい。

以上３点を申し上げたが、こうした観点を踏まえ、本部員の皆様には、意欲的な戦略とすべく、今後、鋭意検討を重ねていただけるよう、よろしくお願い申し上げる。

－　以上　－