サイバーセキュリティ戦略本部
第28回会合　議事概要

１　日時

令和３年５月13日（木）　　８時00分～８時40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
小此木　八郎	国家公安委員会委員長
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
新谷　正義	総務副大臣
宇都　隆史	外務副大臣
長坂　康正	経済産業副大臣
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
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
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

〇お忙しい中お集まりいただき、感謝申し上げる。本日の会合では、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の骨子について討議いただくこととしている。

サイバー空間は、量的に拡大をするとともに、質的にも進化し、実際の空間との融合が進んでいる。あらゆる国民、セクター、地域等においてサイバーセキュリティの確保が必要とされる時代であり、全ての人が「自由、公正かつ安全なサイバー空間」を享受できるような環境をどのように確保するのかといった観点からの議論もお願いしたいと考えている。

本日は、活発な御議論をよろしくお願い申し上げる。

（2）討議

【討議事項】

・次期サイバーセキュリティ戦略の骨子について

【決定事項】

・ サイバーセキュリティ研究開発戦略（一部改訂案）について

【報告事項】

・サイバーセキュリティ協議会の取組状況について

・2021年サイバーセキュリティ月間について

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。

〇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。

野原本部員は、本日は御都合により御欠席となった。

〇村井本部員　まずは昨日のデジタル法案の通過についてお慶び申し上げる。これで紛れもなくDXに対するプロセスが日本全体で進むということになり、この意味は、サイバーセキュリティの面でも非常に大きなインパクト、そして意味があるのだと思う。その視点から３点申し上げる。

１点目は、DXというのは何を目指しているかという点である。基本的には一人も残さないということもあるが、全産業分野、どのような視点で見ても全て

の分野にデジタル技術のインパクトが出てくるということで、例えば省庁で言えば霞が関の全省庁であり、行政分野で言えば全ての自治体、産業で言えば全てのサプライチェーン内の企業、人で言えば全員、このようなところがデジタルテクノロジーの恩恵を受ける、あるいはテクノロジーを使って発展する日本というモデルができるのだと思う。

同時に、それは全てテクノロジーであることから、善用の反対側であるアブユーズ、悪用、乱用というのが必ず出てくるので、それに対応するのがサイバーセキュリティである。つまり、守備範囲がきわめて広範になる。この体制をどのようにつくるかということを政府の中でもきちんと考えなければいけない。

例えばスマートシティといっても、今まではエネルギーや移動だけを見ていたのかもしれないけれども、これからは同じスマートシティといっても、農業も産業も移動も、健康も教育も全て含めた中で、このデジタル化の基盤が動いていくわけであるから、そこにきちんと対応していく必要がある。

２点目は地方が重要である。全ての地方を100％網羅することが必要であり、それをきちんと進めていかなければいけない。例えば、お助け隊は保険の方にお願いしている。そのほか、全国で安心して生活できる国であることは、警察の方がどこにでもいるとか、郵便局の方がいるとか、いろいろ協力していただく方がいる。その方たちにサイバーセキュリティに関してどういうことを担っていただくかを決めなければいけない。

最後に、国際関係である。国際関係は様々な緊張関係の中にあり、新しい米国駐日大使も決まり、日本の役割ははっきりしている。その中で、国家間の関係等を背景にした、ハッカー集団による攻撃というのがインフラを目がけて行われてきているということがあるため、これに対しても関係省庁と力を合わせた体制をつくらなければならないと考えている。

〇遠藤本部員

骨子の作成に感謝申し上げる。デジタル庁を中心として、National CSIRTやサプライチェーン、また重要インフラの防御等、非常にバランスよく取り上げ、つくられていると感じる。特に「Cybersecurity for All」ということを中心に据えており、この方向感は大変いい方向でつくっていると思う。

今、村井先生からお話いただいたが、我々のサイバーアタックというものに対するサイバーセキュリティという観点が、人間の生活に非常に大きくインパクトを与えてくると考えている。今までは経済活動を中心にサイバーセキュリティというものを強く意識してきたが、これからは国民の生活そのものに対するインパクトという観点でサイバーセキュリティを見る必要があると思う。

先日、米国の石油パイプラインへの攻撃があった。また、去年にはイスラエ

ルでの水道に対するインパクトがあった。これらを踏まえ、攻撃の対象がライフラインにまで及んできているということを考えると、我々の国民生活の観点からのサイバーセキュリティというものを強く意識し、それに対する対応をさらに強めていくということが重要だと思う。

そういう意味で、デジタル庁を中心としてサイバーセキュリティのありようを意識し、その方向感をつくっていくということが重要だと思う。

最後に、これらのことを実行していく中で、セキュリティクリアランスに関する考え方を明確にしていく必要があると考える。さらには、国民生活に対するインパクトや災害が出てきたときには、場合によっては自然災害に対して自衛隊が出ていただいているが、それと同様に、サイバーアタックの関連で国民生活にインパクトがあったときに自衛隊の対応ができるような法整備や、体制についても考えなくてはいけないと思う。

〇後藤本部員

この次期戦略の骨子案についてはしっかりできていると思う。サイバーセキュリティ確保のための基本動作を個人、組織、国全体で継続することや、DXによるサイバーセキュリティを推進、加えて途切れることのない人材育成と研究開発が盛り込まれており、いずれも重要と考える。

今回、特に評価したいのは、サイバーセキュリティに起因する大規模リスクについて、複数の視点からの施策が示されていることだと思う。これについて申し上げたい。

まず、米国を揺るがしているソーラーウインズ事案では、連邦政府機関や主要産業が大きな被害を受けた。昨日のワクチン接種のシステムトラブルはセールスフォース社の障害だったのだが、国、社会、経済、生活、全てでデジタル依存度が高まる時代において、特にソフトウェアサプライチェーンのセキュリティは最重要項目になる。担当は経済産業省だと思うが、しっかりとした対応をお願いしたい。

また、国全体のセキュリティリスクをデータ主導で提示できる組織を検討していただきたいと思う。先ほど遠藤本部員からもお話があったが、先日の米国の石油パイプラインのサイバー攻撃では、結果的にガソリンの価格、経済まで影響が出ているようである。1か所のサイバー攻撃が大規模な実被害の連鎖や、経済の混乱につながりかねない。これを改めて認識したところである。

このため、国全体を俯瞰してリスクを分析し、例えばあるところがサイバー攻撃を受けた場合のシミュレーション予測をしっかりし、想定される被害範囲や規模をデータで示すことができるデータ主導のレジリエンス強化策が重要であると思う。

シミュレーションの事前予測では、社会経済やICTシステムに関わる現状データを集約するということが前提となるが、この件について、ぜひNational CSIRTの機能の明確化などとともに検討いただきたい。

○田中本部員

３点申し上げる。１点目は、サイバーの世界は急速に変わってきており、5Gも入ってきて、これから10年を見ると主体が大きく変わっていくのではないかと見ている。そういう意味で、このサイバーセキュリティ対策であるが、臨機応変に主体の変化に合わせて対応していく必要があると考えている。昨今、クラウドはもうありきであるが、これからは特に金融のサイバー空間におけるサプライチェーンが本当に長くなってきているため、気にしなければならないと思っている。

２点目は、なかなか心苦しいのだが、通信事業者の経験から、100％完璧なサイバーセキュリティ対策を実施するというのは相当困難であり、サプライチェーンにしても、トレーサビリティにしても、やはり限界があると思っている。そういう意味で、二重、三重、複層的、多層的な防御対策が必須であると思っており、ぜひとも柔軟かつ実質的な観点で対応が必要だと思っている。

最後は少し話題が変わるが、サイバーセキュリティの人材育成である。部署の中でセキュリティの専門家というのは本当にこれから人を育てていかなければいけないのだが、ぜひとも産学官の育成のエコシステムやキャリアアップのエコシステムをつくってほしい。

○中谷本部員

戦略本部が発足した６年前と比べてサイバーセキュリティ対策は相当進展したと思うが、我が国を取り巻く地政学的状況は厳しさを増しているため、今後、特に力を入れて一層取り組むべきことは、３本の柱のうち、我が国の安全保障への寄与であると考える。今月に入り、米国の最大級の石油パイプラインがサイバー攻撃を受けたが、我が国においても、重要インフラへの中規模以上のサイバー攻撃が生じた場合には遺漏なく対応できるように準備しておく必要がある。

また、自然災害のさなかにサイバー攻撃が生じるといった複合的危機にも首尾よく対応できるように準備しておく必要がある。国際法を無視して力による現状変更を行おうとする国家は現に存在し、それらの国家がまさに国家ぐるみで我が国に対してサイバー攻撃を行うおそれを我々は決して過小評価してはいけないと思う。

サイバー攻撃に対しては、責任を有する個人や団体の金融資産の凍結措置を

外為法に基づき、また、入国禁止措置を出入国管理及び難民認定法に基づいて行うことはもとより、ハックバックを含む積極的な対応措置を技術的にも、法的にも取れるように整備しておくときが既に来ているのではないかと考える。

自衛隊法、電気通信事業法をも含む関係法令がサイバー攻撃に首尾よく対処し運用できるか否かを官邸主導で国家安全保障会議やこの戦略本部をも利用して早急に着手することが必要だと考える。国内法の不備ゆえにサイバー攻撃への十分な対応ができずに国益が損なわれることがあってはならない。サイバー攻撃の高度化に伴い、一国だけではサイバー攻撃に完璧に対処することが不可能になり、友好・同盟国との協調が不可欠になっている。その際に留意すべきことは、十分な協力を得るためにはギブ・アンド・テイクの観点から、我が国自身が十分な対処能力をサイバー関連の各分野において実際に有しておくことが必要だということである。各省庁においては、それぞれの分野において具体的な対処能力を高めていただきたいと思う。

また、いわゆるサイバー事故調については、今回の米国の石油パイプラインへのサイバー攻撃のような事案に鑑みると、早期に立ち上げることが必要だと考える。

さらに、サイバー関連の機密情報を扱う個人や団体についてはセキュリティクリアランスを行えるように体制を整備する必要があると考える。

○前田本部員

今回の骨子は、私は非常にすばらしいと思った。「Cybersecurity for All」というのは、初めの頃は重要インフラをどうするかというところがどうしてもあり、国民全体に対しての視点というのが、弱かったと思う。ただ、もう国民全般にサイバーセキュリティというのが不可分であると考える。象徴的な言葉は公共空間という言葉である。それとデジタル庁ができたことと、軌を一にしているのだと思う。

まさにこの公共空間を守るのは誰かと言うと、それは内閣、国家である。そのことをしっかり認識していくことが重要で、やはり国の調査でも日本人の誇りは何かと聞けば、安心・安全な国家であるということが長らく第１位ではないかと思う。この中でもサイバー空間というのは一番重要な部分になってきており、その意味で今回の中身として規制というか、リスクをコントロールする意味でトレーサビリティを強調したのは高く評価したい。

また、公共の場で、今までは被害に遭わないように注意して歩こうという言い方が中心だったが、そうではなくて、ワナクライやエモテット事案のような悪事を行う人間は捕まえると、悪は絶やすという方向にすでにカーブを切っているし、現に警視庁が中国の共産党員という名前を出して送検した。これはや

はり非常に大きな転換であると思う。これは国際的に、菅総理がバイデン氏と会談して、半歩前に出たというか、一歩前に出たと考える。どこの国とも良好な関係でなければならないけれども、対中国の姿勢は非常に重要だと思う。

最後に申し上げたいのは、国家が前に出るということは、やはり経済、技術のシステム自体も国がサポートしていくことである。様々な技術で、軍が関与しなかった技術発展は世界中どこを見てもない。もちろんそのまま受け入れるということではないが、半導体など様々な技術発展のサポートをお願いしたい。

〇宮澤本部員

キャッチコピーは本当に良いと思う。それと、様々な施策内容も本当にすばらしく、よく考えられていると思うが、1点気になることがあった。それは、全てがあまりにもきれい過ぎることである。きれいな施策だけでは、日々進化するサイバーの世界は捉え切れない。そもそもネットの世界は不浄であり、デジタルは完璧ではないからである。よどみが必要だと思う。

私が思うデジタルのよどみとは、通常ではない、勉強しただけでは得られない特殊な能力を持つ天才ハッカーたちの存在である。今や世界各国の政府機関、企業はこのような人材を抱えている。ニューロダイバーシティとも呼ばれ、台湾のオードリー・タン氏は日本でも有名である。先日のアメリカのパイプラインの話もあったが、特殊なサイバー犯罪は年々増えており、そういった犯罪は、そういった特殊な者でしか理解し得ないという世界が現実にある。犯罪者の手口は犯罪者しか知らないのと似ている。

我々のこのきれいな施策には、そういったスペシャルな人材を発掘し、採用していく具体的な取組はまだ全く書かれていないとはっきり言える。学校で教えられるような通常の教育、育成ではない。そこからは絶対に生まれない。仕事柄、20年、５万人以上の彼らを見てきて自信を持って言える。通常の教育では生まれない。では、どうしたらいいか。探す場所を変えなくてはならないと思う。通常の世界の外、常識の外に彼らはいる。それはいわゆるニート、ひきこもりの中である。しかも、100人や200人を探すだけでは全く話にならない。サイバー攻撃も防御も、最終的には人海戦術である。千、万単位で必要である。日本にはニート、ひきこもりと言われる人たちが100万人以上と言われている。世界でも断トツでトップである。将来的には世界に通用する産業にできるほどの数である。いち早くこの層にアプローチし、ひいては日本のニート、ひきこもり問題、8050問題も解決できる、この一石二鳥の施策を早く始めたほうが良いと思っている。

なかなか採用等も難しいと思うが、デジタル庁を設立できる柔軟な現政権だからこそ、本当に誰も取り残さないデジタル改革をなし遂げ、さらには世界に向けて新しい産業として発信できるのではないかと思っている

○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71日となった。聖火リレーを含め、安全・安心な東京大会に向けて、サイバーセキュリティの確保に万全を期す必要がある。

そのため、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に、東京都、組織委員会などと連携し、最新の情勢も踏まえて、取組を進めている。

また、次期サイバーセキュリティ戦略では、東京大会から得られる知見やノウハウを生かすことで、我が国のサイバーセキュリティに関する全体的な能力の底上げを行うこととしており、サイバー攻撃に対し、国全体として網羅的な対処を可能とするNational CSIRTの枠組み整備も含め、検討を加速してまいりたい。

今回示した「Cybersecurity for All」、「誰も取り残さないサイバーセキュリティ」の実現に向けて、変化するサイバーセキュリティリスクに対応した具体的な対策の実施につながる戦略となるよう、引き続き各大臣と連携をして進めてまいりたい。

○小此木国家公安委員長

デジタル化の進展に伴って、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。サイバー空間に実空間と変わらない安心・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である。

先般、警察の捜査等を通じて国内企業等への攻撃を実行したサイバー攻撃集団の背景組織として、中国人民解放軍「61419部隊」が関与している可能性が高いと結論づけるに至った。警察では、このようなサイバー攻撃、サイバー犯罪の厳正な取り締まりや実態解明を進めるとともに、国内外の関係機関や関係事業者等とともに、緊密に連携しつつ、今後とも被害防止対策の実施など、組織の総合力を発揮した対策を推進してまいりたい。

○岸防衛大臣

デジタル改革の推進が、新たな価値・創造をもたらすことが期待されている一方で、社会のデジタル化が進めば、サイバー攻撃の対象も広がる。このため、サイバー空間の安定的利用の確保がこれまで以上に安全保障上も重要になっている。

防衛省・自衛隊では、サイバー部隊等の体制強化やシステム・ネットワークの充実・強化といった施策に取り組んでおり、AIなどの最新技術も活用しながら、サイバー防衛能力の抜本的強化を図ってまいりたい。

次期サイバーセキュリティ戦略は、官民含む我が国全体としてのサイバーセキュリティの取組を方向づけるものであり、我が国安全保障上も極めて重要なものと認識している。防衛省としても、引き続き積極的に参画をしてまいりたい。

○平井デジタル改革担当・情報通信技術（IT）政策担当大臣

昨日、デジタル社会形成基本法改革法案が成立し、９月１日にデジタル庁が設置されることが決定した。その中で、私はやはり大きなことであると思うのは、今回のデジタル社会形成基本法は、2001年に施行されたIT基本法を廃止して制定しているということである。要するにデジタルのインフラの概念というものが変わっていくということであると思う。情報通信ネットワークからクラウドをベースとしたデジタル社会の基盤となるシステム全体は、常にサイバーフィジカルにいろいろな問題を考えなければならないと思う。

そうなると、セキュリティの考え方も変わっていくのは当然のことであり、デジタル庁としては、デジタル改革の中でセキュリティを最重要課題と認識して徹底的に進めていきたいと考えている。

NISCとは、次期GSOCの共同開発などで緊密に連携する。そして、昨今の組織化、洗練化、ゼロデイ化するサイバー攻撃に対して、デジタル庁が統括・監理する政府情報システムをゼロトラストの考え方に基づいてセキュリティを見直す必要があると考えている。

また、デジタル庁にはセキュリティの専門チームを設置して、政府情報システムのセキュリティの強化のために脆弱性情報等の知見や情報を効率的に利用するとともに、自治体を含む関係機関とも一緒に展開していきたい。

デジタル庁は国民が豊かさと安全・安心を実感できるデジタル社会実現を目指していくので、今後ともサイバーセキュリティ戦略本部と緊密に連携していきたいと考えている。

○新谷総務副大臣

総務省では、ICTがますます重要な役割を担うようになる中、骨子にもあるとおり、まず、国民の自由な経済社会活動を保障し、その利便性の確保を図ること、また、適時適切な法執行により国民を保護すること、この２点をバランスよく両立させることが、国民から期待されるサイバーセキュリティ政策のあるべき姿であると認識をしている。こうした観点から、IoTや5Gなどにおける施策

を総合的に推進している。
　また、NICTの知見や技術を広く活用し、情報収集・分析や人材育成のための共通基盤であるCYNEXを構築し、産学官の結節点として開放していくこととしている。
　総務省としては、これらの取組を通じて、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、次期戦略の策定に向けて協力してまいりたい。

○宇都外務副大臣
　昨今の米国ソーラーウインズ社、石油パイプライン、JAXA等を含む大規模サイバー事案を踏まえても、自由・公正かつ安全なサイバー空間を確保し、国際社会及び我が国の平和と安定を維持・推進する重要性はかつてなく高まっている。
　米国もサイバーセキュリティを最優先事項の一つに掲げており、先月の日米首脳会談では、同分野における協力強化、また、第三国の能力構築の重要性を確認した。
　外交当局として、引き続き、我が国の基本的な考え方を発信しつつ、サイバー空間における法の支配の推進のための議論や規範の実践の普及に取り組んでいく所存である。
　同時に、サイバーセキュリティを含む我が国の安全保障の観点からも、平素から同盟国、有志国と連携をし、特に日米同盟の抑止力を維持・強化しつつ、サイバー空間における脅威について外交的手段を含め、取り得る全ての有効な手段と能力を活用し、断固たる対応を取ることが重要と考える。

○長坂経済産業副大臣
　本日示された骨子では、高度化・巧妙化が進むサイバー攻撃に対して国が対処していく体制を構築し、同盟国・同志国と協力していく方向が明示されており、経済産業省として、これに賛同する。
　経済産業省では、３月に、米国と連携し、インド・太平洋諸国の制御システムセキュリティのキャパシティ・ビルディングのため、特別演習を実施した。
　また、国としての対処能力の強化への経済産業省の貢献としては、第１に、サイバー攻撃を受けた組織へ支援を行うIPAサイバーレスキュー隊、通称J-CRATの情報収集・分析能力の提供、第２に、制御システムセキュリティの中核機関であるIPA産業サイバーセキュリティセンター、通称ICSCoEにおけるサイバーインシデントの観点から事故原因の究明を行う機能の整備について検討を進めている。
　経済産業省は、産業界のセキュリティ対策強化に加え、国の対処能力の強化

や、制御システムセキュリティ分野の国際連携の強化にも最大限貢献してまいりたい。

（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１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骨子を議論した。今後、本日の議論も踏まえ、戦略の案を作成することとなるが、検討に当たって、次の３点について特に念頭に置いていただくようお願い申し上げる。

１点目は、今回提示した「Cybersecurity for All」、「誰も取り残されないサイバーセキュリティ」の具体化である。経済社会の環境が大きく変化していく中、デジタル改革による利便性の向上だけではなく、自由、公正かつ安全なサイバー空間について、国民一人一人が実感できるよう、セキュリティ施策の具体化を進めていただきたい。

２点目に、国全体としての網羅的かつ積極的な対処の実施である。国民生活における安全・安心の根幹を揺るがすような深刻なサイバー攻撃に対しては、オールジャパンで実効的な防御を行うことが必要でる。限られたリソースを最大限有効活用し、包括的な対処を講じることができるよう、人材の発掘・育成を含め、体制の強化について具体的な検討をお願いしたい。

３点目は、安全保障の観点からの取組の強化である。我が国の安全保障をめぐる環境は厳しさを増し、サイバー空間が国家間の競争の場の一部となっている中で、攻撃者優位とされる非対称な状況を看過するわけにはいかない。外交・安全保障上のサイバー分野での取組をこれまで以上に優先して進めていくよう検討をお願い申し上げる。

以上３点申し上げたが、こうした観点をも踏まえ、本部員の皆様には、今後、鋭意検討を重ねていただけるよう改めてお願い申し上げる。

－　以上　－