サイバーセキュリティ戦略本部
第32回会合　議事概要

１　日時

令和３年12月14日（火）　　17時15分～17時45分

２　場所

総理大臣官邸２階大ホール

３　出席者（敬称略）

松野　博一	内閣官房長官
牧島　かれん	デジタル大臣
二之湯 智	国家公安委員会委員長
金子　恭之	総務大臣
林　　芳正	外務大臣
萩生田 光一	経済産業大臣
岸　　信夫	防衛大臣
小林　鷹之	経済安全保障担当大臣
堀内　詔子	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
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
沖田　芳樹	内閣危機管理監
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
石倉　洋子	デジタル監

４　議事概要

（1）本部長冒頭挨拶

本日は御多忙の中、御参加いただき、感謝申し上げる

有識者本部員の皆様におかれましては、本年２月以来、９月に「サイバーセキュリティ戦略」を決定するまでの間、大変熱心に御議論をいただいたと聞いており、まずはこれまでの御協力に改めて感謝申し上げる。

本日は、戦略を決定して最初の会合になる。今後は、戦略に盛り込まれた施策を、いかに実効的に実施し、成果につなげていくかが重要である。皆様には引き続き闊達な御議論をお願い申し上げる。

なお、先般の組閣により、経済安全保障担当大臣が新設された。経済安全保障とサイバーセキュリティとは密接に関係することから、新たに担当大臣に本会議にも加わってもらうことにしたので、御紹介する。

それでは、本日もよろしくお願い申し上げる。

（2）討議

【決定事項】

・デジタル社会の実現に向けた重点計画（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
・サイバーセキュリティ分野における開発途上国に対する能力構築支援に係る基本方針（案）について

【討議事項】

・次期年次報告・年次計画の策定に向けた進め方等について

【報告事項】

・東京オリンピック・パラリンピック競技大会におけるサイバーセキュリティ対策の結果等を踏まえた今後の取組方針について
・2022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。

○牧島デジタル大臣（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

○田中本部員

最初に、決定事項２件について異論はない。特にサイバーセキュリティ戦略を実行する際に、デジタル庁との連携、サイバーセキュリティとデジタル化の一体推進は常に意識して進めていただきたい。

次に次期年次報告・年次計画の策定に関する進め方に関して、今回策定したサイバーセキュリティ戦略は本当によくできており、網羅的にカバーしていると考えている。

一方で、サイバーセキュリティ技術の進歩が激しく、主体の変化で軽重も変わるため、２点コメントさせていただきたい。

１点目、世の中の人々に正しく理解いただく啓蒙活動を強力に推進していただきたい。特にオリパラは国のために業界を横断して皆さんが頑張った結果、何の問題もなく終わったが、このままこういった盛り上がりも終わってしまう危惧があると考えている。情報共有プラットフォームなど、本当に有益な取組があったと思っている。オリパラでの知見、ノウハウを昇華させて、さらによくしていく意識、取組が重要だと考えている。ぜひとも継続できるよう進めていただきたい。

２点目は、サイバーセキュリティ戦略自体も世の中の変化に追従して進化させていく必要がある。特に、サイバーセキュリティでは100％対策は困難であり、複層防御、被害最小化の仕組みが重要と考えている。

以上の観点でしっかりやっていただければと考えている。

○中谷本部員

２つの決定事項について賛成する。その上で２点について申し上げる。

１点目に、サイバーセキュリティ分野における途上国の能力構築支援の基本方針が今回取りまとめられることを高く評価したい。国際社会における法の支配が挑戦を受けているのが、特にサイバー空間と海洋である。途上国へのサイバーセキュリティ分野での人員、資金、技術のキャパシティビルディングは、サイバーセキュリティの脆弱な地域や国を減少させることで、我が国自身のサイバーセキュリティの向上にも寄与するものであるが、単にサイバーセキュリティ分野に限定されることなく、国際社会における法の支配に寄与するという観点からも、また、ひいては日本ファンを増やすという観点からも非常に有益である。

従来はASEAN諸国中心であった支援が、今回はインド太平洋地域を中心に拡大されるが、将来的には他の途上地域にも対象を拡大することが望まれる。各省庁、在外公館、JICAなど関係諸機関と連携してオールジャパンで進めていただくようお願い申し上げる。

また､途上国の中にはSNSなどで反政府情報が流布されることを恐れて情報統制を望む国家もあるが、国連政府専門家会合の報告書やタリン・マニュアルやデータ・フリー・フロー・ウィズ・トラスト（DFFT）の考え方などをベースにして、途上国が国際法を正しく理解した上で、サイバー空間における正当な国際ルールの作成に積極的に参画するように誘導していただきたいと考える。

２点目に、サイバーエスピオナージについて申し上げる。政府や企業の機密情報を盗むというサイバー諜報への対応は、経済安全保障の重大な課題の一つでもある。サイバー諜報の怖さは被害が認識されないことが多いということである。サイバー諜報への法的及び政策的な対応について、本格的に検討を進めることが急務であると考える。

○野原本部員

今回から多くの政府閣僚メンバーが変更になられたので、自己紹介したい。

私は95年からインターネットやデジタルハイテク関連ビジネスについての調査やコンサルを実施してきた。一方で、2006年からNECや損保ホールディングス等の８社の社外取締役を務めてきた。これらの経験を基に、主に民間、企業の立場から、また、国民の目線で発言している。よろしくお願い申し上げる。

本日は１点コメントさせていただく。

本日もサイバー管理ソフトApacheに脆弱性が見つかるなど、新たなサイバー攻撃の原因が次々と出てきている。本日申し上げたい点は、セキュリティ・バイ・デザインの環境整備についてである。政府システムでも、民間でも、システム開発時から整備、運用時まで、全工程にわたってセキュリティ・バイ・デザインを担保することが重要である。しかし、実際にはなかなかそれを実現するのは難しいのが現状である。課題解決のために、各工程での業務を明確化し、それに合わせた体制をつくり、そして、ITとサイバーセキュリティの両方を備える人材から専門分野に特化した人材まで幅広い人材の確保、人材育成の仕組みづくりが必要であると考える。課題は共有されているので、デジタル庁ほかと協力して役割分担を明確にし、早急に推進していただきたいと考える

○前田本部員

決定事項に関しては賛成であるということを前提に、１点申し上げる。

これは、国家がデジタルの世界で一歩前に出るべきであるという点である。一つは、民間との関係で従来より一歩前に出るべきである。今回の案もそういう方向であるが、今後もっとそれを強める必要がある。今まで民間の発展を支えるということを中心にやってきたが、デジタル庁ができて、官民の行動原理の違いが表に出てくると考える。先ほど出てきたプラットフォーム、クラウドをどうするかはセキュリティの視点から厳しい目線が必要であると考える。そのときに一番大事なのは経済安全保障である。この点から、今回の案でも人材の育成推進はごもっともであり、外国の連携強化は当然であると思うが、そこで安全保障の視点がもう一歩入っているほうが、我々としては信頼できるというか安心できる。

もう一つ、国が前に出るという意味では地方との関係である。地方自治は大事であるが、サイバーの世界では、統一的で一元的な管理が何より大事であるので、地方ごとのアプリなどは困る。

今度、警察庁がサイバー局で一歩前に進む。我々、刑事法の学者であるが、これは明治以来の100年に１度の警察の大改革である。地方警察ではなく国家警察が実際に行う。ただ、これはデジタルだから必要なのである。まさにそういう時期であるということを申し上げて終わりたい。

○宮澤本部員

私からは１点申し上げる。御存じのように、昨今、世界的なDXが進む中、サイバーセキュリティへの対応は各国独自の施策、独自の安全保障が進み、世界のサプライチェーンは今や業種を問わず分断の危機にある。私は、近い将来、必ずどこかの国もしくは世界的機関ができて、グローバルのサイバーセキュリティポリシーがつくられて、運用される日が来ると思っている。その日に向けて、日本はサイバーセキュリティのテクノロジーの向上、スペシャルな人材育成を世界に先駆けて今こそ進めるべきだと考える。

日本には、世界のサイバーセキュリティでリーダーシップを取れるチャンスがある。私の20年の会社経営の経験から、理由は２つある。一つは、日本人の気質がそもそもサイバーセキュリティに向いていることである。日本にはひきこもりなど有望な担い手が多い。先日、会社でひきこもり支援などを行うNPOと協力し、ひきこもりの方々を対象にサイバーセキュリティ講習の募集を行ったところ、２週間で600名を超える応募があり、その関心の高さと、自分にもできるのではないかという可能性を見出した方が多いことが分かった。また、かなり厳しい講習にもかかわらず、150名以上のひきこもりの方が難関を突破して講習を終了した。日本には100万人以上ひきこもりの方がいると言われているが、もしサイバーセキュリティ要員として成長できれば、間違いなく世界トップの人材群ができると考える。AIやツールを駆使するが、やはり最後は防御も攻撃も人数である。

ただし、時間はない。イスラエルを含め、サイバーセキュリティのイニシアチブを取りたいと思う国は増えてきている。ジャパンセキュリティ、この機を逃さずに、さらに一歩前進のサイバーセキュリティ政策で、新しい日本の経済成長の基盤をつくるとともに、ひきこもり、ニート問題の解決の糸口になることを願っている。

○村井本部員

いつも楽観的なことを多く申し上げているが、本日は厳しいことから申し上げる。

６月28日にITUがGlobal Cybersecurity Index 2020をまとめており、サイバーセキュリティの評価は、アジアの中で韓国、シンガポール、マレーシアに次いで４位であった。また、エストニアのDXを評価するe-Governance AcademyがNational Cyber Security Indexを作っており、ICTでは日本は世界で10位、ネットワークの整備は16位であるけれども、サイバーセキュリティでは世界の40位であった。イギリスのIISSという戦略研究所について、ここは安全保障に関して非常に厳しい視点で作成したレポートを出すところであるが、インド、インドネシア、イラン、マレーシア、北朝鮮と並んで、評価した15か国中、最低のTier3という評価であった。

今回の重点計画は、こういったインデックスを上げるという指標になるべきであるし、国内のインデックスも同様に作って取り組むべきである。これはいつも申し上げているが、各省庁の正しい評価も考えなくてはいけない。

厳しいことを言った後はもっと褒めなければならないことを申し上げる。オリパラは、

１年延期してコロナ禍の最中に開催したが、ドローンを数多く飛ばすなど、新技術をたくさん導入したすばらしい成果が上がっている。これを軽く考えてはならない。これはレガシーであり、今後、パリ、ブリスベンにどう伝えていくかというのは日本の大きな使命ではないかと考える。

○遠藤本部員

１点目は、私もオリパラ対応は、非常に重要な成果を上げたと思っている。まず、JISPという独自の情報共有システム、さらにはサイバーセキュリティ対処調整センターで行ったサイバー演習、そして、サイバーセキュリティ協議会では、国内セキュリティベンダーを中心に脅威情報を収集、分析、共有してきた。これらの３つの組織が強固な協力体制を組んだということが成功の一番大きなポイントだったのではないかと考える。

これらのノウハウ、経験を国内のほかの領域で共有、活用していただくとともに、特にJISPに関しては中小企業や他業種への参加の組織拡大を図って、階層的なリアルタイムの情報共有、さらには各種団体でのサイバー演習の活用に期待したい。さらに、サイバーセキュリティ協議会に関しては、今後整備が予想されるCSIRTとの関係強化を行うことで、秘匿性が高い情報、リアルタイムの情報の共有化が期待できる。今後とも御配慮、御検討いただきたい。

２点目はバリューチェーン・サプライチェーンに関してだが、全体最適なソリューションをつくる上では、バリューチェーンをどうしてもつくらざるを得ない。その観点で問題なのは、バリューチェーンの中で一番低いところ、サイバーセキュリティで一番低いところがバリューチェーン全体のレベルになってしまうということである。その中で、日本の観点で言うと、中小企業、地方を我々がケアをしなくてはいけないところである。ぜひこの観点を含んで、現在あるサプライチェーン・サイバーセキュリティ・コンソーシアムの強化、さらには、私が今センター長を務めているICSCoEで行っている、ASEANの国々の演習等に対する強化、支援を継続的にお願いできればと考える。

○後藤本部員

決定事項２点には賛同する。

１点目のデータ社会重点計画案に関して一言申し上げると、これはサイバーセキュリティ戦略で打ち出したナショナルサートの機能がますます重要になると認識している。サイバーセキュリティに関する総合的調整の役割を具体化する施策を今後加速すべきと考えている。一例としては、サイバー攻撃が引き起こす連鎖的な大規模リスクに備えるためのサイバー版のハザードマップづくりなどに基づく体制整備を考えていきたい。

２点目の開発途上国向けの能力構築支援については、今回５つの重要性が示されている。この中でも、３つ目のDFFT、５つ目のインド太平洋への拡大は新たなキーワードとして強く認識した。さらに、４つ目に我が国の産業等の現地展開を進める基盤の形成とあるが、

これはまさにグローバルサプライチェーンのセキュリティ確保という面でも非常に重要な観点であり、大きなポイントであると考える。また、海外における人材の育成については、その基となるセキュリティ教育の指導者の人材育成を国内でしっかり進めるべきと考えている。

討議事項、報告事項は全て承知した。いいことであると考える。

オリパラに関して、私も最近の海外メディアで、東京大会のセキュリティ対策は成功であった、北京はどうなのだ、パリはどうなのだという報道をよく耳にする。つまり、この１年はまさにアピールのチャンスであると考えている。先ほど村井本部員からご発言があったが、日本のポジションを上げるためにも、積極的にキャンペーンを海外で張っていく姿勢も大事なのではないかと考えている。

○牧島デジタル大臣

引き続き、副本部長・閣僚本部員から御発言いただきたい。

まず、私から、サイバーセキュリティ担当の大臣及びデジタル大臣として発言をさせていただく。

「誰一人取り残さない、人に優しいデジタル化」の実現のためには、利便性の向上とサイバーセキュリティの両立が不可欠である。

重点計画に沿って、デジタル改革に取り組んでまいる。

また、途上国の能力構築支援、東京オリパラ大会で得られた成果の活用、国民への普及啓発のほか、ナショナルサート機能の強化についても、関係省庁と連携して着実に取り組み、自由、公正かつ安全なサイバー空間の確保に努めてまいる。

○二之湯国家公安委員長

サイバー空間が誰もが利用する公共空間へと進化を遂げつつある中、サイバー空間における脅威は極めて深刻な情勢が続いている。

このような情勢の下で、東京オリンピック・パラリンピック競技大会では、警察を含む各機関が連携して対応した結果、大会運営に影響を与えるようなサイバー攻撃が確認されなかったのは大きな成果である。

今後も、より一層国内外の関係機関等との連携を推進し、サイバー事案の捜査実態解明及び対策を推進するため、令和４年度に警察庁にサイバー局を設置するなどの組織改正を行う準備を進めている。

引き続き、サイバーセキュリティ戦略に沿って、社会の安全、安心の確保に努めてまいる。

○金子総務大臣

総務省では、社会経済活動を支える情報通信ネットワークの安全を確保し、サイバーセ

キュリティの向上を図るため、電気通信事業者における積極的なサイバー攻撃対策の推進や、サイバーセキュリティ情報を国内で収集、分析し、高度な人材を育成するためのNICTにおける基盤CYNEXの構築など、幅広い施策を実施している。

また、本日の議題であるサイバーセキュリティ分野における開発途上国への支援については、自由、公正かつ安全なサイバー空間の確保に向けて極めて重要と考えている。総務省としても、タイに設立した日・ASEANサイバーセキュリティ能力構築センターにおける人材育成の取組などを通じて貢献してまいりたい。

○林外務大臣

国際社会全体において、サイバー空間に対する依存度がより高まる中で、開発途上国に対する能力構築支援は、対象国や地域の脆弱性を取り除くのみならず、我が国も含む国際社会全体のサイバーセキュリティを向上させることに資すると考えている。こうした認識を国連等の場や国際社会で共有しながら、関係国とも連携して、ASEAN諸国等をはじめとする各国への能力構築支援を効果的に行っていくことが重要である。外務省としても、引き続き国連やG7等の場で積極的な役割を果たしていきたい。

○萩生田経済産業大臣

年々高度化、複雑化するサイバー攻撃に対処するためには、相対的にセキュリティが弱いところが攻撃起点となりやすいため、中小企業を含めたサプライチェーン全体でセキュリティを確保することが重要である。このため、経済産業省は引き続き中小企業や地域におけるセキュリティ対策の強化や、経営層の意識改革などに取り組んでまいる。

また、本日、開発途上国に対するサイバーセキュリティ対処能力の構築支援について基本方針が決定される。経済産業省では、本年10月にインド太平洋地域の14の国地域などに御参加いただき、４回目となるサイバーセキュリティ演習を米国やEUと共同で実施した。こうした取組を通じ、サプライチェーン全体での対処能力の向上や、関係国との連携強化に取り組んでまいる。

○岸防衛大臣

我が国を含む世界全体のセキュリティリスクを低減する取組として、防衛省・自衛隊では特にASEAN地域における能力構築支援を進めており、本年度はASEAN各国の国防当局を対象に初のオンラインセミナーを開催予定である。また、先月23日には、ベトナム国防省との間でサイバーセキュリティ分野での協力に関する覚書を署名したところであり、今後、協力の具体化を進めてまいる。

今後も、本日決定された基本方針に沿って、能力構築支援に貢献してまいる。

○小林経済安全保障担当大臣

サイバー空間では、基幹インフラ事業者に対する攻撃や、重要な技術情報の窃取を目的とした企業や研究機関に対する攻撃が増加している。情報通信、電力、金融をはじめとする基幹インフラの安全性・信頼性の確保は、経済安全保障上の課題の一つとして早急に取り組み、法制上の手当を講じてまいる。民間企業の方々の御意見もいただきながら、来年の通常国会への法案提出を目指して検討を進めてまいる。

DXやデータの利活用が社会全体で進む中、サイバーセキュリティに関するリスクへの対応は経済安保を確立する上での基本となるべきものであり、関係大臣と連携してまいる。

○堀内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

東京大会のサイバーセキュリティ対策については、政府における情報共有の対策を強化するなどし、結果として無事に大会を終了することができた。

本日の議題で示されたとおり、大会を契機に推進された取組の成果を、大会後も継承していくことは非常に重要である。９月に決定された新たなサイバーセキュリティ戦略を踏まえ､東京大会に向けて推進した取組がより多くの分野で活用されることを期待している。

（３）決定事項の決定

○牧島デジタル大臣（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）

○牧島デジタル大臣（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。

（４）本部長締め括り挨拶

本日の会合では、本年９月にデジタル庁が設置されて初めてとなるデジタル社会の実現に向けた重点計画の案に対する意見を決定した。

デジタル庁をはじめとする関係省庁においては、デジタル改革を推進する上で、国民の利便性向上とサイバーセキュリティの確保の両立は不可欠であるとの考え方を踏まえて、着実に各種施策に取り組むよう、お願い申し上げる。

また、途上国の能力構築支援に関する基本方針についても決定した。途上国におけるデジタル化が急速に広がる中、自由、公正かつ安全なサイバー空間の確保というサイバーセキュリティ戦略に掲げた理念をグローバルに浸透させていくことが重要である。特に、サイバー空間をめぐる現下の国際動向を踏まえると、我が国が途上国の能力構築支援の強化にコミットすることは大変意義深いメッセージであると考える。

今後、関係省庁においては、この基本方針を踏まえて着実に支援の取組を推進していくとともに、国際社会に対してこうした我が国の取組や理念を積極的にアピールしていくよ

う、お願い申し上げる。

最後に、サイバーセキュリティ確保のためのさらなる機能強化について申し上げる。クラウドサービスなど、技術の高度化に伴うサービスの複雑化や、ランサムウェアの被害に見られるようなサイバー攻撃の専念化が進み、国全体のセキュリティリスクも高まっている。こうした中、自由、公正かつ安全なサイバー空間を確保していくためには、NISCを中心として関係の各政府機関のリソースを結集し、情報把握、分析力、防御力、さらには抑止力の強化を図るとともに、インシデント対応から政策的な措置まで一体的に推進するナショナルサート機能を強化することにより、我が国のサイバーセキュリティの総合力を高めることが重要な課題である。

これらの機能強化に向けて、牧島大臣のリーダーシップの下で、関係の政府機関において、体制強化や連携協力に向けた具体化のための検討を進めていただくようお願い申し上げる。

－ 以上 －