サイバーセキュリティ戦略本部
第31回会合　議事概要

１　日時

令和３年９月27日（月）　　９時00分～９時40分

２　場所

Web会議形式での開催

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
平井　卓也	デジタル大臣
梶山　弘志	経済産業大臣
新谷　正義	総務副大臣
宇都　隆史	外務副大臣
土本　英樹	防衛省整備計画局長
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
石倉　洋子	デジタル監
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
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WEB形式での開催とさせていただいている。お忙しい中、お時間をおつくりいただき、感謝申し上げる。

本年２月以来、皆様に大変熱心に御議論いただいた次期サイバーセキュリティ戦略については、パブリックコメントも終了して、最終案を整えることができた。本日は、この案

について御審議をいただきたいと考えている。
また、東京オリンピック・パラリンピック競技大会においてサイバーセキュリティが大変、課題が懸念されておりましたが、その対策の結果についても併せて報告する。
本日も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（案）等について
・政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みの一部改正（案）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（結果報告）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。

○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。

○後藤本部員
最初に、この夏のオリパラ大会は、特別の環境下での開催であったが、先ほどもあったように、大会運営に影響を与えるような攻撃がなかった。これは我々も実感している。大会のサイバーセキュリティ確保に向けて大変な努力を続けてくださった大会関係者の皆様、重要インフラ事業者の皆様、それから、特に現場にて24時間体制で対応いただいた皆様に深く感謝申し上げる。また、このオリパラの合間の時期であったが、８月17日の海外メディアには「The Tokyo Olympics are a cybersecurity success story」、東京大会はサイバーセキュリティの成功ストーリーだと高く評価する記事が出ていた。私も誇らしく感じたところである。
さて、次期戦略（案）であるが、この大会を無事に乗り越えた実績とともに、次のステップに向けた取組を示しており、充実した内容と考えられ、賛同する。次期戦略（案）には「国全体のリスクの低減とレジリエンスの向上に精力的に取り組む」など、大規模リスク対応の重要性を明記されている。我々は、日常生活の中では大規模リスクや最悪の事態を想定することを避けがちである。しかし、今回のオリパラへのサイバー攻撃を抑止できたのは、最悪の事態をも想定し、基本動作からの訓練を愚直に繰り返し、１年の延期決定後も、練度を高めながら対応チームを維持し続けた、その成果だと考える。同じ緊張感を

継続することは容易ではないが、昨今の状況はそれが必要であることを強く示している。私自身も、緊張感を継続して、人材育成や技術開発の実務を担いたいと考えている。

最後に、資料４－２にセキュリティ確保の取組の活用策を議論する場があるが、これは大変重要と考える。これに加えて、関係各所の現場のチームにて、その取組の詳細を記録するよう、幅広く声がけいただきたい。今後の大規模リスク対応においては現場での活動記録が最も有用であり､次世代のセキュリティ人材にとって大きな財産になるためである。

○田中本部員

最初に、次期戦略（案）は、パブコメを経て、さらにブラッシュアップされており、良い戦略ができていると考える。事務局の皆様は、様々な御意見を取りまとめて、大変苦労されたと思う。感謝申し上げる。

また、オリパラも大会運営に影響を与えるサイバー攻撃が確認されなかったということであるが、弊社としてはNISCからタイムリーに脅威情報などを展開いただいたおかげで、弊社内でも特に影響なく、対応を完了することができた。この点についても感謝申し上げる。

政府情報システムのセキュリティ評価制度の一部改正を含め、決定事項２件について、異論はない。

今後、実行フェーズになるが、これからの進め方に関して、通信事業者の経験からコメントさせていただく。

昨今、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いるのは御承知のとおりであり、重要インフラを守る点でもサイバーセキュリティの重要性はますます高まっている。

サイバーの世界は急速に変わってきており、セキュリティ分野だけでなく、グローバル的にも技術の革新が急速に進んでいる。例えば自動運転やAI、量子コンピューター、5G、6Gなどの話である。また、働き方も大きく変わり、テレワークが一般的になり、我々を取り巻く通信環境もここ数年で大きく変化した。

今後、戦略を実行していくフェーズになるが、このような世の中の流れ、技術の流れをグローバルに、タイムリーに、しっかりつかんで、臨機応変に対応していく必要があると考えている。

昨今は地政学的な緊張が増しており、国主導での対応・連携が重要になっている。しっかりと戦略をつくっていただいたので、実行フェーズを成功させるべく、柔軟かつ実質的な観点で取り組んでいただければと考えている。

○中谷本部員

次期戦略（案）など２件について賛成する。また、オリンピック・パラリンピックが大規模なサイバー攻撃を受けることなく無事終了して安心した｡その上で５点申し上げたい。

１点目は、８月にアルジェリアがモロッコとの外交関係を断絶した。西サハラ問題をめぐる両国の長年にわたる対立を背景として「モロッコの情報機関が、イスラエルのサイバー企業が開発したスパイウエアを使ってアルジェリア当局を諜報していた」とアルジェリアは主張して断交に至った。サイバー行動が外交関係断絶に至った初のケースとして注目されるが、他の地域においても今後このようなドラスチックな動きが現れる可能性があるので、注視しておく必要があると考える。

２点目は、サイバー攻撃元の特定に関して、JAXAへのサイバー攻撃につき「中国人民解放軍の部隊が関与した可能性が高い」と４月に警察庁長官が言及したことは画期的であった。今後、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により、アトリビューションの能力が一層高まることを期待したい。

３点目は、サイバー犯罪に関するブダペスト条約の第２追加議定書が近く採択予定と聞いている。従来の外交ルートや中央当局間ルートやICPOルートによる国際捜査共助を補完して、他国のプロバイダーとの直接的な協力、相手国からの照会の執行、緊急時の捜査共助、オンライン取調べなど、国境を越えたサイバー犯罪の捜査を円滑に進めるために大いに期待される国際合意である。採択された場合には、必要な留保を付した上で速やかに加入していただきたいと考える。

４点目は、ランサムウエアについては、前回申し上げたが、身代金の大半は暗号通貨による支払いが要求されていることに鑑み、今後利用が増大する暗号資産においては、犯罪に悪用されないように十分な対応をしていただきたい。

５点目は、コロナ禍ゆえテレワークが日常になっているが、テレワークを行う社員のデジタル機器の設定や管理は十分とは言えないと懸念する。ここから重要な企業情報が盗まれたりサイバー攻撃が発生したりしかねないため、企業においてはテレワークを狙ったサイバー攻撃への実効的な対策を取っていただくことを希望する。

○野原本部員

これまでの関係者の尽力のおかげで適切な次期戦略（案）がまとまったと考えられ、賛成する。今後は、この戦略（案）に沿ってしっかりと施策を推進していただきたい。そして、先日、日米豪印首脳会合で４か国首脳による会合があり、共同声明がなされた。その中でもサイバー攻撃対策での連携・協働が含まれており、国際連携に注力することは重要であると考える。本会合でもその進捗を適宜、共有していただければ幸いである。その上で３点申し上げる。

１点目は、東京オリンピック・パラリンピックがコロナ禍により延期及び無観客で、想定外の事項が多かった中、大きなサイバー攻撃もなく無事に済んだことは本当に良かったと考える。感謝申し上げる。異例ずくめの大会だったからこそ得られた貴重な経験・スキルを整理して今後にしっかり生かしていただきたい。

２点目は、DXとサイバーセキュリティの同時推進についてである。２つの視点があると

考えている。１つ目は、個々の業務、製品・サービス等のシステムにおける企画・設計段階から完了して運用する段階まで全行程で同時推進を行うことが重要で「セキュリティ・バイ・デザイン」であり、「セキュリティ・バイ・運用」となると考える。２つ目は「全社的なサイバーセキュリティ統括機能」の充実である。社会経済におけるDXの進展や、自社の個々の業務･サービス等のDXの進展による変化に対応して､全社のセキュリティ戦略、体制、対策を柔軟に更新していくことが重要である。その点についてもしっかりと重視していきたいと考える。そして、どちらに対しても、各企業等での体制づくりと人材確保や育成、そして、ガイドラインの周知・啓蒙が重要である。次期戦略（案）においては「横断的施策」の中の「人材の確保、育成、活躍促進」の各施策も極めて重要であると考えるのでよろしくお願い申し上げる。

３点目は､アトリビューションのための体制整備についてである｡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。この点について、政府全体で議論・整理をした上で、具体的には、海外との協力体制、人材育成体制、関連技術・サービス提供体制、必要に応じて法制度の見直しも行うべきであると考える。

○前田本部員

今回の次期戦略（案）については、まとめていただいて感謝申し上げる。全く異存ない。

次期戦略（案）で述べられているように、国民生活の中でのサイバーの重要性はもともと高まっていたが、まさにサイバーセキュリティは国家の仕事の中の非常に枢要なものになったということである。逆に言うと、国民はサイバーセキュリティの専門性のある国家機関が国民を守ってくれるという期待を強く持ってきていると考える。そのためにも、例えば警察庁のサイバー局構想のようなものは非常に時宜を得た対応であるが、さらにブラッシュアップしていただきたいと考える。

ただ、問題は、日本の安全を守るときに地域と国家の関係が、微妙に変化してきていると考える。当たり前であるが、国家を背景にした攻撃や、日米豪印首脳会合の声明に関連して､国家安全保障､経済安全保障につながってくる｡国家が表に出てくるのは当然だが、その中で国民の信頼を得ながら前に進めていく。個人情報はまだまだ今後様々な展開があると思うが、欧米の議論などを見ていると、国家監視という言い方をする人が必ず出てくる。銀行のシステムダウンのようなことがあれば国家は信頼がないのは当たり前である。私は日本の公務員の信頼感は非常に高く、日本は大丈夫であると考えるが、公務員の信頼感をいかに上げていくか、という点に配意していくことは非常に重要であると考える。

プライバシーの感覚や不安感は国家によって非常に差がある。ワクチンパスポートに対しての反応を見ていても文化の差のようなものが出てくるので、サイバーセキュリティを考える上でも日本人の日本文化に則った視点が最後はないとならないのではないか。その意味でも、サイバーだけではなく、オリパラのセキュリティは完璧であった。これはじわじわと国民にも浸透していくと考えられるし、国民から信頼されることの積み上げがサイ

バーセキュリティの基本になければならないと考えている。

○宮澤本部員

今回はシンプルに２点提案させていただきたい。

１点目は、次期戦略（案）の理念、体制、取組は本当に良いが、実践訓練を全くしないのは問題であると考えている。年に１～２回、民間からの攻撃を受け付けて訓練を行えば、ほかに何が問題であるのかはすぐに明らかになる。また、その際に民間から優秀なハッカーを見つけてリクルーティングすれば一石二鳥であると考える。

２点目は、今後DXにおいて増えるであろう政府調達でのデジタル機器について、ハードウエア、ソフトウエア、アプリケーションを問わず、あらゆるものにセキュリティチェックが必要になってきたと考える。始めている省庁もあるようだが、日本版NIST SP 800-171は今後早急に必要になると考えている。

○村井本部員

私からもシンプルに４点申し上げる。

１点目は、技術の進展があり、その悪用ということでサイバーセキュリティに対する事象が出てくるが、この２年間、パンデミックがあって、いろいろな意味でDXは５年、10年、場合によっては20年前倒しされたという議論がある。今までも技術の進展に対し、サイバーセキュリティは、言わば尻尾を追いかけるようなことを行ってきた。ところが、技術の進展が前倒しされることが分かった今、デジタル庁など、閣僚・本部員・省庁の所管部門、すべてのステークホルダーが力を合わせて、中長期でどのような体制で何をするのかを再考すべきである。これは今までの尻尾を追いかける型よりも、ゼロトラストを含めた、頭を押さえる型にするべきである。それには知見が必要であるが、体制をつくって、動く準備を進めるべきである。

２点目は、DXが進むということは、デジタル庁も誰一人取り残さないということを掲げているところ、鍵になるのは地方である。47都道府県および、すべての基礎自治体に対する人材配置も含めた、誰がどこで何を担うのかという明確な定義が必要になる。本日報告された警察でのサイバー局の新設は大変力強いインフラである。地方自治体、基礎自治体はもちろん、民間の郵便、保険、金融といった機関が力を合わせる体制が今こそ必要ではないかと考えている。

３点目は国際である。今、経済安全保障がキーワードになり、どういう視点で我が国が進んでいくかが重要である。我が国は太平洋に位置していること、光ファイバーで主なインターネットの接続ができていること、新たに作られる低軌道衛星などのインフラができること、さらに災害に必ず対面しなければいけない国であること。この中から、グローバルパンデミックの経験を経て、日本がサイバーセキュリティに対して非常に強い体制を構築し、それが世界に貢献していくといった議論を進めることが必要であると考えている。

４点目は、NISCは過去に、関係省庁のサイバーセキュリティへの取り組みついて評価軸を決め、戦略本部会合で議論することを行ってきた。この会議は関係省庁には嫌がられていたが、これは他に誰もできないことだった。民間の有識者がいる場で各省庁の状態を把握し、評価を行うという、言わばサイバーセキュリティ通信簿を復活させて、取り組んでいただきたいと考える。

○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。

東京大会は円滑に運営が行われ、大会に影響を与えるようなサイバー攻撃は確認されなかった。皆様のこれまでの対策強化への御尽力に敬意を表するとともに、政府における情報共有等への御協力に感謝を申し上げる。

本日の議題である次期戦略（案）においても、大会に向けて行ってきた取組の活用を含めて、今後の取組を進めていくこととしている。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「誰も取り残さないサイバーセキュリティ」の確保に向けた取組を進めてまいりたいと考える。

戦略として取りまとめたことを実現するため、関係府省庁と協力して取り組んでまいりたい。

○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の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。サイバー空間においても、実空間と変わらぬ安全・安心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なものとなっている。

先ほど有識者本部員の先生方からも警察におけるサイバー部隊の対応に対する期待について改めて言及いただいたが、警察としてはその実現に向けて、令和４年度に警察庁にサイバー局を設置するなど体制の整備を図るとともに、全国に配置された高度な専門技能を有する人材を機動的に活用するための解析基盤の整備等を進めるなど、対処能力のさらなる強化を検討している。

サイバー事案の厳正な取締りや実態解明、国内外の関係機関等との連携を推進するとともに、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。

○平井デジタル大臣

９月１日にデジタル庁が設立されて、国の重要なシステムはデジタル庁が自ら設計・開発を行って、セキュリティの専門チームと一緒にシステムの設計・開発段階からセキュリ

ティ対策を強化していくことになった。

また、デジタル庁としては「品質・コスト・スピード」を兼ね備えた行政サービスを実現するために、行政システムのアーキテクチャを根本から見直すことになる。このために、必要な機能をレゴブロックのように柔軟に組み合わせられるようにしつつ、最先端クラウド基盤やネットワークなど行政システムが共通で必要とする機能を基盤として整備する。最新のクラウド基盤を常に確保するためには相当な投資が必要になってくる。今後、クラウド事業者との契約なども含めて整備する必要があると考えている。

特にデジタル庁においてはネットワーク、テレワークが普及拡大しているので、端末のID管理等の検討も進め、各府省にも今後拡大していく。今、VPNが狙われたりしているが、テレワークがここで失速しないようにするためのセキュアな環境が必要であると考える。

そして、従来型のセキュリティ、境界型のセキュリティにとどまらない、いわゆるゼロトラストと呼ばれる新しいセキュリティアーキテクチャの実現をしていかなければいけないが、技術検討や脅威情報の収集等について、さらなる議論を進める必要があると考える。

デジタル庁は、そうした学びの場にもならなければいけないと考えているので、セキュリティ人材の育成にも協力していきたいと考えている。また、セキュリティクリアランスの問題を何らかの形で確保しないと今後の国際連携は非常に難しい面もあると考える。長年の課題であるが、そろそろ真剣に検討すべきときではないかと私自身は考えている。

○梶山経済産業大臣

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、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、昨年産業界が設立したサイバーセキュリティ対策を推進するコンソーシアムと連携し、引き続き、経営層の意識改革などに取り組んでまいる。

また、重要インフラ等へのサイバー攻撃が生じた場合の高度な原因究明機能の整備に加えて、本年10月には、米国やEUと共同して、インド太平洋地域の国・地域などにも御参加いただく４回目となるサイバーセキュリティ演習を開催し、関係国との連携強化も進めてまいる。

いずれも、今般の戦略（案）の実現に向けた重要な取組である。引き続き、関係省庁の御協力もいただきながら、サイバーセキュリティ対策を強化してまいる。

○土本防衛省整備計画局長

本日、防衛大臣が出席の予定であったが、諸事情により、出席できなくなったので、代読させていただく。我が国の周辺の中国・ロシア・北朝鮮において、軍をはじめとする各機関がサイバー能力を増強する中で、サイバー空間における脅威も日々高度化・巧妙化しており、我が国として、サイバー攻撃対処能力の向上は喫緊の課題である。

次期戦略（案）においても、我が国の安全保障の観点から、サイバー攻撃に対する防御

力、抑止力、状況把握力について、具体的な取組強化の方向性を示したことは非常に意義があると考える。

防衛省・自衛隊においても、サイバー能力を抜本的に強化するため「自衛隊サイバー防衛隊（仮称）」の新編をはじめ、各種システムの強靱化、サイバー人材の確保・育成や訓練を進めている。

今後、本課題の実効化に向け、これらの取組を着実に進め、政府全体、そして我が国としてのサイバー能力向上に貢献してまいる。

○新谷総務副大臣

本格的なデジタル社会が到来する中で、次期戦略（案）に基づき、官民が一体となってサイバー攻撃の巧妙化・複雑化に対応し、自由、公正、かつ安全なサイバー空間を確保していくことは極めて重要であると考えている。

総務省としては、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の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、また、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、また、国、地方公共団体、重要インフラ事業者等の情報システム担当者等を対象とした、体験型の実践的サイバー防御演習（CYDER）の実施等に係る施策を来年度の概算要求に盛り込んだところである。

これらの取組を通じて、引き続き、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と考えている。

○宇都外務副大臣

取りまとめ、感謝申し上げる。

先週行われた日米豪印首脳会合においては、菅内閣総理大臣から、サイバー攻撃が国家や民主主義の根幹を揺るがすような国家安全保障上の事態に進展し得る重大な課題であること、国家を背景に持つサイバー攻撃が深刻な脅威であること等を発言され、４か国の首脳間で協力強化を確認したところである。

外務省として、引き続き、パブリック・アトリビューションを含め同盟国や同志国と連携するとともに、サイバー空間における法の支配を含む我が国の安全保障に資する国際ルールの形成等を通じ､サイバーセキュリティの強化に一層貢献していきたいと考えている。

また、個人として、推進体制が肝であると考えている。特にデジタル庁とNISC、NSSの連携をしっかりと図って、船頭多くして船山に上るにならないようにお願いしたいと考えている｡また､宮澤本部員のコメントにあった実践的訓練の重要性については強く賛同する。

（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）

○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。

（４）本部長締め括り挨拶

本日の会合では、次期戦略（案）を決定した。次期戦略（案）の検討に当たって、本部員の皆様方には御尽力をいただき、感謝申し上げる。

初めに、東京オリンピック・パラリンピック競技大会についてであるが、事前の準備、また、期間中の対応を適切に行った結果、運営に影響を与えるようなサイバー攻撃は確認されなかった。関係者の御努力に改めて感謝を申し上げる。大会に向けた様々な取組の経験は、次期戦略（案）にも反映されているが、得られた成果や教訓について、今後の我が国のサイバーセキュリティ確保のためにしっかりと活用していきたい。

戦略（案）の実施に当たっては、次の３点を念頭に置いていただくようお願い申し上げる。

１点目は、政府一丸となった取組の推進である。サイバーセキュリティの推進はデジタル改革と一体となって進める必要があり、限られた人的リソースを有効に活用するためにも関係機関の一層の対応能力強化・連携強化が重要になる。NISCを中心に、そして先般発足したデジタル庁とも緊密に連携する形で、政府が一丸となって取組を進めていくようお願いする。また、サイバー攻撃のさらなる実態解明の推進のため、警察庁におけるサイバー局新設など、アトリビューション能力の向上が重要である。そのためには特に人的資源の確保が重大な課題になる。人材の育成・確保について、長期的な視点を持って進めていただきたい。

２点目は、国内外の関係者との緊密な連携である。グローバル規模でサイバーセキュリティを確保するためには国際協調が重要である。同盟国・同志国をはじめ各国政府など様々なレベルで重層的に協力・連携を行うとともに、国際社会に対して「自由、公正かつ安全なサイバー空間」の確保という我が国の考え方を積極的に発信していくようお願いする。また、クラウドサービスなど、日進月歩に変化する技術やサービスを的確に把握し、一方で、個人情報や知的財産を狙ったサイバー攻撃などに適切に対処するためにも、民間部門との協力、情報交換などは不可欠であり、さらに連携を進めていただきたい。

３点目は、取組の進捗の検証とその結果に基づく取組の着実な実施である。本戦略（案）で示された方針に基づき、関係府省庁の政策が着実かつ効果的に実施されるよう、３年間の計画期間内においても、毎年、取組の進捗状況を検証し、その結果を次年度の計画に反映させることにより、戦略（案）の具体化を着実に進めていくようお願いする。

最後に、今後、これまでサイバー空間とはつながりが薄かった方々も含め、あらゆる方々がサイバー空間に参画することが見込まれる。本戦略（案）のコンセプトでもある「誰も

取り残さないサイバーセキュリティ」の確保のため、政府としても、国民の信頼に十分に配意しつつ、また、各地方自治体とも連携し、戦略（案）に掲げられた各種の取組をしっかり進めていただきたい。

本部員の皆様には、今後の取組に当たっても、引き続き御助言、御提案をいただくようお願いを申し上げる。

－ 以上 －