サイバーセキュリティ戦略本部
第23回会合　議事概要

１　日時

令和２年１月30日（木）　　８：00～８:40

２　場所

総理大臣官邸４階大会議室

３　出席者（敬称略）

菅	義偉	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
武田	良太	国家公安委員会委員長
高市	早苗	総務大臣
茂木	敏充	外務大臣
梶山	弘志	経済産業大臣
竹本	直一	情報通信技術（ＩＴ）政策担当大臣
渡辺	孝一	防衛大臣政務官
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
前田	雅英	日本大学大学院法務研究科教授
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	慶應義塾大学環境情報学部教授　大学院政策・メディア研究科委員長
西村	明宏	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
和泉	洋人	内閣総理大臣補佐官
前田	哲	内閣サイバーセキュリティセンター長
古谷	一之	内閣官房副長官補

４　議事概要

（1）本部長冒頭挨拶

早朝からお集まりいただき、感謝申し上げる。本日は２つの決定事項などがあるため、皆様には活発な御議論をいただきたい。

また、私から、３点お願いを申し上げる。

第１は、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についてである。本制度の所管であるNISC、IT総合戦略室、総務省、経済産業省は、各府省庁が安心して安全なクラウドサービスを使えるよう、実効性の高い制度を整備するようお願いする。また、各府省庁は、この制度を生かし、新しい技術を活用した効率的な業務の実現を推進していただきたい。

第２は、いよいよ本年開催される2020年東京オリンピック・パラリンピック競技大会についてである。実践的な訓練や演習の実施など、必要な作業を着実に進めるとともに、しかるべきタイミングで、体制の総括的な確認を行うようお願い申し上げる。

第３は、官民一体となったサイバーセキュリティの一層の確保である。大手電機会社へのサイバー攻撃事案の発生や、2020年東京オリンピック・パラリンピック競技大会の開催も踏まえると、政府内での円滑な情報共有はもちろん、官民が一体となったサイバーセキュリティの一層の確保が重要である。2020年東京オリンピック・パラリンピック競技大会後も見据え、速やかに検討を進め、取組を進めていただきたい。

橋本大臣のリーダーシップの下、引き続き、関係大臣が連携して取り組むようお願い申し上げる。

（2）討議

【決定事項】

・「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について（案）」について
・「重要インフラの情報セキュリティ対策に係る第４次行動計画」の改定（案）について

【討議事項】

・次期年次報告・計画の策定に向けた進め方等について

【報告事項】

・政府のサイバーセキュリティに関する予算（2020年度政府案等）について
・2020年サイバーセキュリティ月間について

・2020年東京大会に向けた取組状況について
・サイバーセキュリティ協議会の取組状況について
・サイバーセキュリティに関する国連政府専門家会合（第１回会合）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。

○（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。

○（前田本部員）
２つの決定事項の原案に異存はない。このまま進めていただきたい。
全体の将来的な計画について、今、具体的な課題のないときに、まさにこういうことを取り組んでいただきたいと思うが、総務省が6Gを前向きに検討されていることは、一番大事な将来計画の要だと思う。日本の国力を上げていくためにも、AIやそれを伸ばすためにもボディーの部分は計画を前倒しして、村井本部員などを中心に、ぜひ頑張っていただきたい。これ抜きにセキュリティはないということである。
ただ、セキュリティ、技術力の一方で、前から小野寺本部員などが御指摘になる、セキュリティの穴は人から開く、人が情報を漏えいさせると。先日、ソフトバンクに対してのアプローチと三菱電機に対するサイバー攻撃が発生している。ソフトバンクのほうが端的だが、5Gの時点でこのようなことが起こるのであれば、6Gになるとより情報をとりに来る。そのときに、理系の方等の審議会などを見ていると、やはり我々のほうが猜疑心が強いのかもしれないが、AIの自動運転などでも、悪事を働く人間のことを考えるよりも、まずは技術を高めることだけをやるのだが、我々は、日頃犯罪者を相手にしているため、世の中には悪いことをする人ばかりだという考え方で、警戒心をより強めていく。
ファーウェイを巡る議論でも、安価であれば良いとか、世界スタンダードであるなどといっても、国の存立が危うくなるのではないか、という感覚が我々は強い。国によってはいろいろな考えがあると思うが、全体の大きな流れとしては、国家安全保障とサイバーセキュリティ、これはより一層一体化していく視点でぜひ検討を進めていただきたい。

○（宮澤本部員）
決定事項に関しては賛成であり、非常に良いものであると思っている。その上で、２つ申し上げたい。
１つ目は、今後、全国の小中学校にパソコンが配られるということであるが、サイバーセキュリティの観点から述べると、今のままではかなり危険なのではないかと思っている。子供たちにピストルを渡すようなものではないかと思う。
先日、中学生が学校のサーバに侵入して、自分の成績を３から４に変えたというかわいい事件があったが、これも不正アクセスである。海外と日本では、学校でパソコンやタブレットを渡すときに大きな違いがある。海外では危険なものだと学校から渡しているが、日本では便利なものとして渡している。日本はそもそもセキュリティに関しての考え方がかなり浅いのではないかと思っている。
そのような状況の中で、やみくもに全員に渡すと、未成年によるハッキング等の犯罪などが増えるのは明白である。また、誰からも知られず、外部から乗っ取りによって犯罪に使用されるかもしれない。そうであれば、児童生徒たちにIT教育、セキュリティ教育をしっかりと教え、端末とネットワークを監視するIT用務員などを学校に配置してはどうかと思っている。
そして、まさにそのITセキュリティ用務員こそ、氷河期世代の引きこもりやニートの人たちは適任ではないかと思っている。ある程度研修は必要であるが、彼らは皆、学校というものに少なからずトラウマがある。だからこそ、仕事として学校ともう一度関わることで、トラウマから抜け出すきっかけになるかもしれない。また、先生達の負担を減らし、生徒と教員だけという特殊な環境に一般人、特に、当時いじめを受けた経験がある人が入ることによって、いじめを相談しやすかったり、なくしたりする環境をつくることができるかもしれないと思っている。ぜひ御一考していただきたい。
２つ目は、三菱電機へのサイバー攻撃の問題であるが、中国のプロハッカー集団による攻撃である可能性が濃厚であると見ている。完全に狙い撃ちされたようだ。今後、政府、企業は、ペネトレーションテストというホワイトハッカーによる実際の侵入テストを繰り返し、空手で言う組み手で実践の経験を積むしかないと思っている。
はっきりと１つ言わせていただくと、現在のNISCでは、これらに対抗するような攻めのサイバーセキュリティを担うことはできない。何かをなぞるような教科書的な運営では、毎回、事後の対応が精いっぱいである。今、この国のサイバーセキュリティの土台を固めなければ、経済の発展はないと思っている。なぜならば、どんなものをつくっても他国に壊されて、全て盗まれてしまうの

であれば、セキュリティが弱い日本で商売をするのは不利だということになりかねない。セキュリティ分野の人手不足は明らかであり、即戦力の人材が不足しているのであれば育てるしかない。ただ、ちまちまやっていても世界のスピードには合わない。今、我が国は、受け身のサイバーセキュリティから攻めのサイバーセキュリティに転換する決断のときではないかと思っている。

○（村井本部員）

内閣官房でサイバーセキュリティを取り扱うということは、各省庁にまたがって横をつなぐ重要な役割がある。本日は予算の資料が出ているが、今、農業や医療関係等は非常に情報化が発展している分野で、農地もセンサーがついて新しい農業に生まれ変わってくると思う。このような、今までIT関係と関わっていなかった省庁が、様々なネットワークでつながるIT機器やAIを使った新しい産業の発展に進んでいく。このときに、各省庁の連携を担うのはこの本部であるため、そういった意味でのサイバーセキュリティに対する体制が必要であり、そのことは、予算、それから調達に表れる。このような統一的な取組はこれまでこの本部で進めてきたことであり、これからも非常に重要になるだろうというのが１点である。

次に、先週、パシフィック・テレコミュニケーション・カンファレンスという世界中から人が集まる大きな会合があり、サイバーセキュリティの大きな議論として、海底ケーブルの議論があった。衛星は電波を使うため規制が全て各国でかかるのだが、海底ケーブルというのは直接つながっている。北極海の氷が解けたときに、北極経由でカナダ回りのケーブルができたのである。また、北欧回りのケーブルが今回お披露目されている。これは北海道に上がる予定だ。来週には、ジャパン・グアム・オーストラリア（JGA）というケーブルが陸揚げされて、今年中に動き出す。このことは何を意味しているかというと、地政学的な構図が変わるということである。ヨーロッパと直結する回線、グアムからアメリカへ行く回線というのは、今は全て日本海から北へ延びているケーブルで、東シナ海を通って東南アジアにつながっている。これが変わるというところが大きなことであり、これも各省庁が力を合わせないといけないという内容だと思う。

○（遠藤本部員）

３点申し上げる。

１点目は、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に関してであるが、政府でのクラウド使用がこれから頻繁になってくるということで、その安全性の評価の仕組みというのは非常に重要

であると私も考えている。アメリカは約10年前からクラウドを積極的に使っており、その調達基準であるFedRAMPというものがあるが、これも一つ参考にしていただくのが良いかと思う。さらに、米国ではこの10年間の失敗事例等も含めて、SP800シリーズのドキュメントというものがある。ぜひこれらを御参考にしていただき、早急な立ち上げと確立をお願い申し上げたい。

２点目は、11月に菅官房長官も注意喚起をされたが、中小企業向けのEmotetという攻撃が盛んになってきている。クリスマスから正月、14日ぐらいまでほとんど攻撃がなかったが、14日以降、また攻撃が盛んになってきている。これらは、我々が一つ一つの企業を守るということから、サプライチェーンまたはバリューチェーンを結ぶことによって価値を出すという観点で、非常に危険な、弱いところを攻めるという手段に出てきているということであろうと思う。ぜひこの弱い部分、中小企業、それから地方団体、これらを強化していく、その方法論を世界と確立していくことが必要だろうと思う。

３点目は、サイバーセキュリティ協議会に関してである。昨年４月にスタートし、今まで私どもが得られなかった秘匿性の高いセキュリティ情報を共有することができ始めている。日本全体で守るというコレクティブ・アクション、コレクティブ・ディフェンスの教育をぜひ皆さんにしていただきたいと思うとともに、一点できていないのはデータのリアルタイム性での共有である。これから、リアルタイム性での共有が更に増してくると思う。

STIXという構造化されたフォーマットがあるが、まだまだこれを使ったリアルタイム性の情報共有ができていないため、NISCを中心に、これのアクセラレーションを含めて我々官民一体で対応させていただきたい。

○（小野寺本部員）

決定事項については、異存はない。

２点申し上げる。１点目は、宮澤本部員がお話しになったIT用務員と似ている話かもしれない。NHKが放送した中で、ウェブカメラの映像が平気でネット上に流されていたという放送があったが、個人宅も含めて多くのカメラ映像が漏えいしているのは間違いない。それを本人は全く気づいていない。ユーザーは、パスワードやIDがあることすら知らない。これは余りにもひどいことだが、これは日本に限った話ではなく、多くの国で同じような状況があると思う。そういう意味では、日本が先行してそういう教育をどう行っていくのかということが非常に大きな問題だと私は思う。

宮澤本部員からはIT用務員という話が出たが、国立大学の教員養成課程の卒業生は年間約１万人で、そのうちの７割から８割は教員になり、残りは教員にならないのだが、この方々はまさしくデジタルネイティブの世代で、少し教え

れば相当のことを中学生や小学生に教える能力を十分身につけられるだろう。ところが、省庁としては文部科学省であると思うが、残念ながらここの部分を一体誰が担っているのかわからない。

その意味で、先ほどの宮澤本部員のIT用務員の話もそうなのだが、それ相応の人がまだいるにもかかわらず、そこをどう使うのだという施策が残念ながらまだできていないというのが私の実感である。ぜひ、そういうことをやっていただきたい。

２点目は、今の話に絡むが、ウインドウズ７は１月14日にサポート終了になっているが、XPも3.1もまだ相当数残っていると聞いている。実は、最初のNECの98シリーズのコンピューターすら一部には残っている。もちろんインターネットにつながっていないため、すぐに問題を起こすようなことにはならないだろうが、そういう現実があることをもう一度捉え直すべきではないか。

この事は、我々IT系をやっている人間の常識と世の中の常識のスピードの差だと思う。我々が通信をやっていて一番困るのは、通信は第３世代、第５世代と変わってくると、システムも変わる。ところが、例えば車につけられるシステムは、車のほうは30年の差が出ると、一体誰の責任でどう載せかえるのだと。常にそういう問題を抱える。明らかにIT系とそれ以外では、タイムフレームに対する考え方が大きく違うため、この点についても考えていただきたい。

○（後藤本部員）

決定事項は２点とも賛成である。

３つ目の討議事項、次期年次報告・計画の策定に向けた進め方等について、現行のサイバーセキュリティ戦略の仕上げとして、DX with Cybersecurityの考え方をぜひ前面に出したものをお願いしたい。

その観点で３点申し上げる。１つは、担う人材である。まず、経営層のDX with Cybersecurityの意識改革が重要である。これは当然であるが、加えて、幅広い産業分野で、各企業のDX推進役、例えばDX事業本部長、こういう方の必須要件としてサイバーセキュリティを位置づけるための啓発活動、育成策を、予算配分を含めてお願いしたい。

２つ目は、難題であるが政府自身のDXである。まず、本日決定される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について、この議論には私も関係してきたが、利用部門が主体性を忘れずに継続して安全性を確認できる仕組みづくりが大事だと考えている。同時に、常に進化しているクラウド関連技術に柔軟に取り組み、それによって政府のDXを推進する。これが要である。つまり、安全性を確保しながら、同時にフレキシブルにクラウドを活用するようなDX。この取組が、DXの本来意義である業務プロ

セスや組織に至るまでの大変革につながる。ぜひお願いしたい。

３つ目は、政府のIT調達に関して。既にサプライチェーンを含めて重要性が指摘されているが、気になっているのは対象とするITの範囲である。机の上のパソコンやノートパソコンだけではなくて、例えば、国立病院の医療機器からトンネルやダムの災害用のセンサーも全てITといえる。そういう意味で、ITの範囲を最大限に広げて、そのサプライチェーンも含めた安全性確保にしっかり取り組む。こういう計画をぜひお願いしたい

○（中谷本部員）

決定事項について賛成である。その上で、４点申し上げる。

第１に、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について、クラウドサービス提供者及び監査主体の双方の信頼性の担保が必要であると考える。最終的には、昨年12月のIT調達に関する申し合わせに基づくチェックがなされると思うが、遺漏のないように運用していただくことを強く希望する。

第２に、サイバーセキュリティ協議会に、航空、空港、医療、水道を含む全ての重要インフラ分野が参加するようになったことを大いに歓迎したい。さらにより多くの企業や団体に参加してもらうよう推進していただきたい。

第３に、高等専門学校における教育の重要性について、一言述べたい。高専の卒業生は制御システムの開発従事者の中核になるため、彼らにサイバーセキュリティ教育を施すことは我が国の将来のサイバーセキュリティにとって非常に重要であると同時に、サイバーセキュリティに強い高専と、高専の売りにもなる。政府には、高専への一層のサイバーセキュリティ教育と産学官の連携を進めていただきたい。

第４に、習近平国家主席の来日に合わせて、日中間でサイバー分野での信頼醸成の合意形成を、特に2015年に米中間でサイバー手段による知財窃盗をしないと合意したことを参考にしつつ進めていただきたい。

○（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、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。

2020年東京オリンピック・パラリンピック競技大会の開会まで、半年を切った。大会の成功のためにはサイバーセキュリティ対策は不可欠である。

昨年立ち上がった「サイバーセキュリティ対処調整センター」では、関係機

関と連携した訓練を実施し、G20サミット、ラグビーワールドカップ、即位の礼でも運用を行った。

これらの経験を生かし、関係機関との連携のもと、必要な対策を推進してまいりたい。

本日御決定いただく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については、各府省庁が安心して安全なクラウドサービスを使えるよう実効性の高い制度の整備を進めてまいりたい。

また、昨今の事案の教訓を踏まえ、政府内における円滑な情報共有のための取組を進めてまいりたい。関係各府省庁の引き続きの協力をお願い申し上げる。

○（武田国家公安委員長）

近年、減少傾向にあったインターネットバンキングの不正送金事犯の発生件数及び被害額が、昨年９月から11月にかけて急増するなど、サイバー空間における脅威は深刻な情勢が継続している。

こうした脅威に対し、警察組織の総合力を発揮した効果的な対策を推進している。

特に、今夏には、2020年東京オリンピック・パラリンピック競技大会が開催されるところ、関係省庁等と連携し、大会を標的としたサイバー攻撃に関する脅威情報の収集・分析を行うとともに、大会の運営に関連する事業者等との情報共有、共同対処訓練を実施するなど、詰めの調整・確認を進め、大会の安全・円滑な開催に万全を期す所存である。

また、この度の大手電機会社に対する不正アクセス事案が発生したことも踏まえ、警察としても改めて内閣サイバーセキュリティセンターなどの関係機関との緊密な連携を図り、間近に迫る2020年東京オリンピック・パラリンピック競技大会のサイバーセキュリティの強化にしっかりと取り組んでまいりたい。

○（高市総務大臣）

サプライチェーン対策や被害拡大防止のためには、重要インフラ14分野全てにおいて、「サイバーセキュリティ対策」の義務や、「インシデント発生時の報告」の義務を、法令に位置付け、着実に実施することが重要だと考えている。

総務省が所管する「電気通信事業法」及び「放送法」では、省令によって両方を義務付け、またローカル5Gについても、セキュリティ対策を講じることを免許の条件にするなど、「電波法」の省令を整備している。

ぜひ、他の重要インフラ分野においても、各所管大臣のリーダーシップにより、速やかに各業法の省令整備をお願いしたい。

なお、三菱電機のように所管省庁が複数にまたがる場合、インシデント発生

時の報告を行う政府窓口が曖昧になっている可能性があるため、ここをしっかりと明確化する必要がある。

また、既に自動運転がレベル４、レベル５へと進んでいくのが目前になっている。貨物分野は物流分野で重要インフラだが、人を運ぶ自動車や船舶は重要インフラから外れているため、ぜひペネトレーションテストを繰り返すなど、対策を強化していただきたい。

○（茂木外務大臣）

外務省は、法の支配、信頼醸成、能力構築を３本柱とするサイバー分野における外交を推進している。

第１の法の支配に関連し、G20、GGEや、国連等のマルチの場でも主導的な役割を果たし、ルール強化による自由で安全なサイバー空間の実現に努めていきたい。

第２の信頼醸成に関しては、米国・豪州・欧州など有志国との二国間協議を実施し、双方のサイバー政策に関する理解を深め、サイバー防衛や5G時代のセキュリティ確保に向けた協力を進めてまいりたい。

第３の能力構築に関しては、国際的なサイバー対策の穴を塞ぐため、特にASEAN諸国を中心に、行政官や法執行機関の能力構築支援を積極的に推進していく。

○（梶山経済産業大臣）

クラウドサービスのセキュリティ評価制度については、関係省庁と連携しつつ、実務を担うIPAの監督等をしっかりと行っていく。

また、クラウドサービスの安全な利用において、政府機関自らのセキュリティ対策も大変重要であり、引き続き議論を深めてまいりたい。

サイバーセキュリティ対策全般については、サプライチェーン全体で対策を進めるため、昨年策定した「グループ・ガバナンス・システムに関する実務指針」において、サイバーセキュリティ対策の推進が経営者の責任であることを明確化し、攻撃の起点になりやすい中小企業向けの対策として、「サイバーセキュリティお助け隊」事業を推進していくとともに、日本とサプライチェーンを共有するASEAN向けに、米国と共同したハイレベルなセキュリティ演習の開催などを行っている。

また、大手電機会社へのサイバー攻撃事案を踏まえ、産業界全体への情報の横展開など、関係省庁と連携して適切に対応してまいりたい。

○（竹本情報通信技術（IT）政策担当大臣）

国民が安全で安心して暮らせ、豊かさを実感できるデジタル社会の実現に向け、セキュリティ対策を十分に講じ、安全性及び信頼性を確保することが必要と考えている。

また、デジタル・ガバメントの実現に向けて、政府情報システムにおけるクラウドサービスの利用の検討を原則としているところであるが、関係者が安心してクラウドサービスを利用するために、セキュリティ評価制度を構築することが重要であると考えている。

引き続き、IT政策担当大臣として、IT戦略本部とサイバーセキュリティ戦略本部の積極的な連携を図ってまいりたい。

○（渡辺防衛大臣政務官）

防衛省・自衛隊は、防衛大綱及び中期防に基づき、令和２年度予算案において、サイバー防衛隊を約70名増の約290名の体制に拡充するとともに、サイバーコンテストの開催など、高度な能力を持つ人材を発掘する取組を進めていく。

また、2020年東京オリンピック・パラリンピック競技大会については、サイバー防衛隊が、組織委員会が維持・管理する情報システムのサイバーセキュリティ対策に協力しており、引き続き、政府全体のサイバーセキュリティの強化に貢献してまいりたい。

（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。

－　以上　－