サイバーセキュリティ戦略本部
第21回会合　議事概要

１　日時

平成31年1月24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
櫻田　義孝　　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
山本　順三　　国家公安委員会委員長
石田　真敏　　総務大臣
岩屋　　毅　　防衛大臣
平井　卓也　　情報通信技術（ＩＴ）政策担当大臣
佐藤　正久　　外務副大臣
関　　芳弘　　経済産業副大臣
小野寺　正　　ＫＤＤＩ株式会社相談役
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
林　紘一郎　　情報セキュリティ大学院大学教授
前田　雅英　　日本大学大学院法務研究科教授
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　康稔　　内閣官房副長官
髙橋　清孝　　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
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
兼原　信克　　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。

本日の会合では、主に昨年７月に決定した新戦略に基づいて策定する「サイバーセキュリティ意識・行動強化プログラム」や「次期年次報告・計画の策定に向けた進め方」について御審議をいただきたい。

限られた時間ではあるが、よろしくお願い申し上げる。

（2）討議

【決定事項】

・「サイバーセキュリティ意識・行動強化プログラム（案）」について
・サイバーセキュリティ基本法の一部改正に伴う関係規則等の改正について

【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】

・サイバーセキュリティ基本法の一部を改正する法律等について
・IT調達に係る国の物品等又は役務の調達方針及び調達手続きに関する申合せ等について
・「国際社会の平和・安定及び我が国の安全保障への寄与」に係る取組状況について
・政府のサイバーセキュリティに関する予算（2019年度政府案等）について
・2019年サイバーセキュリティ月間について
・2020年東京オリンピック・パラリンピック競技大会に向けての取組状況について

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。

○（櫻田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。

○（中谷本部員）

４点申し上げる。

第１に、次期年次報告・計画策定の方向性は、これで大変結構だと思う。抽象的な説明だと一般の方々には理解しづらいとも思われるため、賢いユーザーとして行動しないと自らにも社会にも損失が生じてしまうということを実感してもらうように、分かりやすく説明することが特に重要であると思う。

第２に、IT調達に係る国の物品等又は・役務の調達方針及び調達手続に関する申合せ等において、重要性の観点の中に、国家安全保障及び治安関係の業務を行うシステムや、機密性の高い情報を扱うシステム、情報漏えい、改ざんによる社会的・経済的混乱を招くおそれのある情報を扱うシステムなどを明示して、政府として5Gに関する政府調達において、国家安全保障上の考慮を重視する方針を示したこと。また、携帯電話大手が自主的に5Gや4Gの基地局などについて、安全保障上、懸念のある企業のものは採用しない方針を固めたことは、いずれも英断であり、評価したいと思う。

これらはサイバーセキュリティの分野において、予防的アプローチが採用されたものであると言えるだろう。政府調達に関しては、WTOの政府調達協定において、安全保障のための例外が認められており、国際法とも整合的である。

独立行政法人・特殊法人、14分野の重要インフラ事業者においては、このような政府及び携帯電話大手の対応に鑑みて、機器の利用について適切かつ合理的な対応をとることを強く望みたいと思う。さらに、安全保障の観点から、各種サーバーの国内補完が望まれる。

第３に、中小企業において、セキュリティ対策について自己宣言する制度である「SECURITY ACTION」の登録事業者数が６万7000に達したことは歓迎すべきことである。さらに、中小企業がサイバー事案に直面した際に、相談窓口の体制を整備し「サイバーセキュリティお助け隊」が迅速に対応していくことは、我が国のサイバーセキュリティ全般にとっても重要であると考える。

第４に、中国を拠点とするAPT10が日本や米国など12カ国にサイバー攻撃を行い、米国司法省が２名を起訴し、我が国も非難声明を発出した。我が国としては、サイバー空間における法の支配の防衛のために、米国を始めとする自由主義諸国と協調して行動をとり、サイバー空間における法の支配を崩そうとする勢力に対しては毅然とした行動をとり続けることが重要であると考える。

○（野原本部員）

３点申し上げる。

１点目は、意識・行動強化プログラムについてである。

これまで普及啓発について何度も申し上げてきたが、このプログラムをまとめていただいたことに感謝したい。

しかし、資料１－１にもラストワンマイルとあるように、普及啓発は容易ではなく、大きな問題である。NISCは自らの施策を実施するのではなく、官民の多様な機関との連携をプロデュース、マネジメントすることに注力して、それによって全体的な大規模な成果を上げるように進めてもらいたいと思っており、こうした観点でPDCAを回してほしい。

２点目は、企業におけるサイバーセキュリティ対策推進体制の重視についてである。

私は何社かの社外取締役をしており、毎月各社の取締役会に出席しているが、一般的にサイバーセキュリティ対策が単独で取締役会の議題となることはほとんどない。あっても全社的なリスクマネジメントシステムの議論の中で、トップリスクの一つとしてサイバーセキュリティが挙げられることや、CISOを任命する旨の議論の場になる程度である。そのように取り上げられるということは、ある種、先進的だと思うが、まだこのような状況がある。

そこで、２つ提案をさせていただきたい。

１つ目は、経営陣とCISOやサイバーセキュリティの専門家の人たちが一緒に議論できるような資料のモデル、つまりどのような資料をつくればいいか、どのような言語を使えばいいか、どのような図で議論すればいいかといったモデルを提示してほしい。

２つ目は、コーポレートガバナンス・コードなどでサイバーセキュリティ対策体制について説明をするように言及をするのも一手かと思う。

３点目は、サイバーセキュリティ協議会についてである。情報共有、連携は大変重要な課題だと日ごろから思っている。インシデント情報など、未確定な情報を迅速に相互に共有し、有効に機能するようにしていただきたい。また、情報報告先はJPCERTや各業界のCERT等もあるので、この協議会に情報提供することが煩雑な対応にならないように気をつけていただきたいと思う。

現段階では、まだ具体的なメンバー構成や活動内容がよく分からないため、今後もそれを随時、進捗状況として報告していただきたい。

○（林本部員）

私は決定事項２件と討議事項１件の方向性に異論はないが、サイバーセキュリティ協議会に関連して１点申し上げる。

今世紀に入ってから急速に展開したサイバー攻撃という故意のインシデントについては、行為者を特定するのが難しいというアトリビューション問題を抱えている。行為者が特定できなければ、刑事訴追はもとより、他の救済手段も十分に効果を発揮できない。

2000年代の初めごろには、こうした行為者優位の状況はなかなか解決できな

いだろうという諦めの雰囲気があったと思う。しかし、2010年代に入ってからは、特に米国のサイバー対処機関やセキュリティベンダー、大手のOTTと呼ばれる企業などが協力して、行為者を特定するまではいかなくても、蓋然性が極めて高い程度まで範囲を絞り込めるようになった。この鍵は、インシデント情報の共有と分析であったと思う。

米国では、9.11の悲劇の際に、インテリジェンス機関がアルカイダの動向に関して重要な兆候を得ていながら、これを生かし切れなかったということで、従来のneed to knowの原則を補足する形のneed to shareの必要性が強調された。

サイバー攻撃という新しい分野については、このような必要性の強調が不可欠との認識が広まって、2015年にサイバーセキュリティ情報共有法が制定されたと理解している。

我が国でも、米国の経験を先例として、かねてからJPCERT/CCとの連携やTelecom-ISACを始めとする業種別の情報共有、あるいは重要インフラ向けのJCSIPなど、多くの情報共有組織があったが、これらを法的に横通しし、さらには秘密情報の保全を担保する仕組みはなかった。

今回、サイバーセキュリティ基本法の改正によってサイバーセキュリティ協議会が設置され、これらの問題を解決する具体的な組織が動き出すことは画期的なことだと思う。

2000年の内閣官房情報セキュリティ対策推進室の設置以来、連綿と続けられてきた官民双方のサイバーセキュリティ対策は2015年の基本法の制定と今回の改正で一応の整備を終え、第２段階に入ることになろうかと思う。

このプロセスの一部に参加させていただいた者として、力不足ながら精一杯やり切ったという考えがある一方で、これからが本番だという緊張感も感じている。

協議会の運営が一日も早く開始され、それが今後の意識・行動強化プログラムや年次報告・計画等に生かされ、できれば2020年東京オリンピック・パラリンピック競技大会にも何らかの貢献ができることを期待している。

○前田本部員

林本部員から発言があったサイバーセキュリティ対策は第２段階に入るという点について、私もこうした流れを感じており、その際のキーワードは国家という視点だと思う。

事務局から説明のあったAPT10について、中谷本部員の発言にもつながるが、年末に外務省が発出報道官談話は非常に重いと捉えている。

サイバー空間の安全を脅かす、中国を拠点とするAPT10の攻撃を、懸念を持って注視してきた。長期にわたって攻撃を行い、民間学術研究機関から情報を窃

取しようしており、そのことは確認している。米国、英国も含め断固非難するという声明を出している。

こうした流れは急に出てきたのではなく、ちょうど１年前に、WannaCryは事案の背後に北朝鮮の関与があったという趣旨を政府が明示しており、方向性に変化がでてきていた。知的財産権、データの保全のため、GAFAをどうするかという議論も、今大きくなっているが、個人の持っている情報や、プライバシー権をどのように守るかという視点であった。しかし、大きくフェーズが変わったと思うのは、視点の主体が国家だということである。

国家安全保障の問題の視点が非常に重要である。先日、NHK取り上げられていたが、ビッグデータについても、大阪の交通事情のデータが企業を通して中国の北京に集まっている。私も若干お手伝いした面もあるが、日本の警察も犯罪対策にAIを使う。これは当然だと思うが、それに対しては、国民の安心・安全の観点からプライバシーを暴くようなもので、非常に危険であり、こうした面はなくさなければいけない。しかし、中国に情報が持ち込まれ、中国の企業が情報を持つことは安全にとって脅威ではないのかとも感じる。

もう一つ大きな視点で、国家的な視点に立っていただきたい。調達に関しても先日、通信関係の企業の方から、国が言いたいことはよくわかる。しかしながら、高い性能と安い価格で提供できる企業はあるのか。誰が保証してくれるのか。といった意見があった。

ただし、そこで思考停止になるのではなく、これから国家の存立に関わる問題につながるという視点から、どう解決するかを考えることが重要である。代わりとなる技術をどう開発するか、また、どこまでお金を補助していくかなど、少しずつで良いから、サイバーセキュリティ対策の第２段階には、国家の視点を入れた方針で取り組んでいただきたい。

○村井本部員

5GやAI、IoTは、全てデータを使って、新しい社会を作っていく。昨日、大坂なおみさんが全豪オープンで活躍され、中継をご覧になった方もいるかもしれないが、例えば、どこでサーブを受けているか、どの位置にいたのか、１試合で何キロ走っているか等、あらゆるデータが利用され、スポーツ中継がされるようになった。

2020年東京オリンピック・パラリンピック競技大会でますます進むことになると思うが、これはほかの産業にも全て当てはまる。あらゆるデータを自由に使えるようになってきたため、農業も医療も大きく変わっていく。本当に多くの人が自由にデジタルデータを使って新しい社会を創っていく時代になる。

そこには２つ大きな問題がある。それはサイバーセキュリティの問題とプラ

イバシーの問題である。この２つの問題に対して、私たちは官民データ利活用推進基本法および個人情報保護法、知的財産関連の法などを使いやすいように修正しながら取り組んできた。サイバースペースがグローバルな空間であるということを踏まえて、非常に重要な体制を整えて、対応してきた。これが１点である。

２点目として、G20が今年開催されるため、そこでメッセージを出したほう良いと思う。日本はデータに対してどのような扱いをしていて、安全、セキュリティ、そして、プライバシーに関する体制についてしっかりと取り組んでいること、あるいはそういう世界を作らなければいけないということを世界に発信する良いチャンスだと思う。今年はそのチャンスを是非うまく利用していただきたい。

調達に関しては、他の本部員からも指摘があったが、私の心配は２点あり、１つは日本企業が厳しい立場になるのではないかということである。例えば既に使用している企業に対して、どのような手だてを考慮するのか、あるいはどのような対応をするのか。調達の中で厳しい条件を明確に入れて、何をしてもらいたいのか、何をしてもらいたくないのかを示すことは重要だと思う。

今回、政府のIT調達におけるサプライチェーン・リスクへの対応がしっかりとできるようになったため、IT戦略的にはとても良いことだと思う。ただ、それを明確にしていく一方、調達額は上乗せしたほうが良いと思う。そうしなければ、日本企業は対応できない。この件をきっかけに日本企業が疲弊するようではいけないので、こうした点を調達の軸で考えることができるようになったことはとても良いことだと思う。

最後に、前田本部員の発言と関連するが、2004年にルーターとスイッチの先端の技術を作らなければいけないということで、日立とNECにお願いして、１つの会社を立ち上げていただいた。それが今、アラクサラという会社で残っているが、そこには我々大学関係者からも先端の人材が輩出されている。即ち、先端の人材が行く場所がしっかりとあった。これが縮小してくる、つまり国産が減ってくると、日本の人材がそこを目指さなくなる。目指さなくなると、その力がなくなってくるので、結局はこうした調達に関する事態が起こったときの対応力が減少する。

情報通信の先端技術を持った産業があるということは良い人材ができるということであり、こうした産業が少し下向きになってきていたことが今回のような課題を難しくしている一つの要因だと思う。サイバーセキュリティと情報通信に関する超トップの人材が育つような環境を作っていくということが必要である。

○（小野寺本部員）

３点ほど申し上げる。

まず、サイバーセキュリティ戦略（2018年７月27日閣議決定）のカラーパンフレットについては、非常に良くなったと思う。これまでは文章ばかりだったが、図や表などが増えて、非常に見やすくなっている。ただ、非常に重要なことが書かれているが、余り世の中に出回っていないため、これをどのように皆に知っていただくか、是非、その点を政府として考えていただきたい。

先ほどG20に関する発言があったが、サイバーセキュリティ戦略は英語版も、作成されており、これも海外に持っていくと海外の関心は非常に高いと思う。こういうものが、在外公館も含めて、もう少し外に出ていく必要があるのではないかと思うため、その点もお考えいただきたいというのが１点目である。

２点目は、今回、サイバーセキュリティ意識・行動強化プログラム（案）を作成されたが、これは非常に結構なことだと思う。他の本部員の発言にもあったように、様々な問題が発生し、マスコミがサイバーセキュリティを取り上げる機会が非常に増えてきている。その中で、サイバーセキュリティ意識・行動強化プログラム（案）を公表するということは非常に重要だと思う。

ただ、サイバーセキュリティ意識・行動強化プログラム（案）に記載されているように、個人についてはインターネット利用への不安感が拡大している。ここがやはり大きな問題であり、この不安感を払拭していかないと、電子決済やキャッシュレス化、電子政府といった、今、政府が進めていこうとしている施策そのものの利用がなかなか進まないのではないかと懸念している。

したがって、個人に対して、この不安感をどのように払拭していくかは非常に重要なことであり、各省庁で積極的に取り組んでいただきたい。総務省で取り組んでいるNOTICEは、実はNOTICEはインターネットにつないだ後の機器について、調査で初めて問題が見つかるわけであり、つなぐ前の処置というものが、残念ながらここではできない。

したがって、インターネットを使った通信販売も多くなっているだけに非常に厄介な問題ではあるが、IoT機器については販売時点で何らかの形で、セキュリティを喚起することを方法論として考えていく必要があると思う。このことは経済産業省だけでできるのかどうか分からないが、ぜひお考えいただきたい。

３点目は若年層の問題に関して申し上げる。文部科学省の学習指導要領では、2020年からプログラミング教科の必修化が始まるが、セキュリティについては、まだまだ取組がほとんどされていないように見える。最も知見を持っているNISCが積極的に関与することによって、若年層にどのようにうまく知らせていくかが重要である。プログラミング教育では、幼少期は楽しむことが先で、その後に、学校で、セキュリティとサイバー空間における倫理の問題を取り扱っ

ていく必要があるのではないかと思う。
高度セキュリティ人材育成については、関係省庁で様々な取組が行われており、その中で既に「サイバーセキュリティ研究における倫理プロセス」などの研究倫理の基準作りが進んでいるが、研究開発だけではなくて、サイバー空間における倫理教育がもう少し重視されていかないと、根本的なところがなかなか理解されないのではないかと感じる。

○（櫻田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。
本日は2020年東京大会までちょうど１年半（547日）という節目を迎えている。大会の成功に向け、着実に対策に取り組んでいく必要がある。
こうした中、１月５日から12日まで、イスラエル、英国、フランスに出張して、関係機関を訪問し、課題の共有や対応策に関する情報交換を行った。
また、昨年末の臨時国会において、協議会を創設し、構成員の守秘義務の適用等を盛り込んだ「サイバーセキュリティ基本法の一部を改正する法律」が成立したところである。
本改正の枠組みを活用した「情報共有・連携体制」や、東京大会の成功に向けた「サイバーセキュリティ対処調整センター」の早期の構築、本日、御審議いただいた「意識・行動強化プログラム」の推進を始め、サイバーセキュリティ戦略本部の副本部長として、全力で取り組んでまいりたい。
関係府省庁の引き続きの御協力をお願い申し上げる。

○（山本国家公安委員長）
国民にとってサイバー空間がより身近なものとなる中で、国民生活の安全・安心を確保するためには、全ての主体が連携・協調してサイバーセキュリティの確保に取り組むことが重要である。
本日の決定事項等を踏まえて、サイバー犯罪等の被害防止のための広報啓発活動を推進するとともに、2020年東京オリンピック・パラリンピック競技大会に向けて、関係省庁、大会組織委員会、重要インフラ事業者等と連携し、情報共有や共同対処訓練を実施するなど、対処能力の向上に努めてまいりたい。

○石田総務大臣
近年、IoT機器を悪用したサイバー攻撃が深刻化いたしており、早急な対処が

必要である。
総務省では、改正NICT法に基づきまして、本年２月より、先ほど御指摘のあったNOTICE、いわゆる脆弱性を有するIoT機器の調査を行い、通信事業者を通じた利用者への注意喚起を行う事業を開始する。
本事業の実施に当たっては、お配りしている資料のとおり、ポスターの掲示など積極的な周知広報を行う。IoT機器の適切なパスワード設定など国民のセキュリティ意識の向上を図り、安全なIoT社会の構築を進めてまいりたい。
総務省としては、引き続き、関係省庁、通信事業者などとも連携しつつ、本事業を着実に実施し、我が国のサイバーセキュリティの確保に尽力してまいりたい。

○（岩屋防衛大臣）
安全保障上の極めて重大な課題であるサイバー攻撃に対し、迅速かつ的確に対応するために、我が国の能力の一層の強化が必要だと考えている。
防衛省・自衛隊としては、昨年12月に策定された新たな防衛計画の大綱並びに中期防衛力整備計画に基づき、有事において相手方によるサイバー空間の利用を妨げる能力の保持、大臣直轄部隊である「サイバー防衛部隊」の新編並びにサイバー要員の大幅な増員、専門教育課程の拡充など、優秀な人材の計画的な育成など、サイバー防衛能力の抜本的強化の対策を進めてまいりたい。
我々としては、申し上げるまでもなく、これらの対策をミリタリーの観点から進めていくが、平素から、関係府省庁と連携を強化し、防衛省・自衛隊の知見や人材の提供、合同の訓練・演習の実施等を通じて、サイバー攻撃に対する我が国全体の防御力、抑止力の向上に努めてまいりたい。

○（平井情報通信技術（IT）政策担当大臣）
昨年12月19日にIT戦略本部を開催し、データの安全・安心・品質、公共・民間部門のデジタル時代への対応の促進を柱とした「デジタル時代の新たなIT政策の方向性について」本部決定した。
この決定に基づき、国内における「個人情報の安全性確保」や「政府調達等における安全性確保」に加え「国際的なデータ流通圏の構築」などの政策の具体化を進め、春ごろを目途に「新たなIT政策大綱」として取りまとめを行う。
引き続き、IT戦略本部とサイバーセキュリティ戦略本部の緊密な連携を図ってまいりたい。

○（佐藤外務副大臣）
外務省として、法の支配、信頼醸成、能力構築を三本柱とするサイバー外交

を引き続き推進してまいりたい。
具体的には、国連において政府専門家会合のメンバー国としてサイバー空間における法の支配の推進に積極的に貢献している。また、米国、英国、豪州、ロシア、韓国、中国など13の国・地域との間でサイバー協議を実施している。さらには、ASEAN地域フォーラムにおいては、サイバーセキュリティに関する会期間会合を立ち上げ、具体的な信頼醸成措置を提案している。
また、一昨年12月の北朝鮮のWannaCry事案に続き、昨年12月には、中国を拠点とするAPT10と言われるサイバー攻撃グループを非難する外務報道官談話を発出し、抑止に向けた行動をとってきている。
また、政府調達に関する申し合わせについても、積極的に関与してきたところである。
また、村井本部員からG20大阪サミット首脳宣言にサイバーセキュリティに関するメッセージを盛り込むようとの提言があり、また、小野寺本部員からはサイバーセキュリティ戦略等の冊子を在外公館などを通じて発信すべきという提案があった。これらの御指摘については、関係省庁とも連携の上、検討してまいりたい。
引き続き、自由、公正かつ安全なサイバー空間の創出・発展に努めてまいりたい。
○（関経済産業副大臣）
「サイバーセキュリティ意識・行動強化プログラム（案）」でも分析がなされているとおり、中小企業のセキュリティ対策強化は非常に重要である。
経済産業省が取り組んでいる、中小企業にセキュリティの自己点検をしてもらう「SECURITY ACTION」の活動には、６万7000社を超える事業者が参加している。さらに、中小企業のトラブル対応を支援する「サイバーセキュリティお助け隊」を中核とした面的支援体制の構築のために新たに実証事業も立ち上げる。
また、サプライチェーン・リスク対策は、次期年次計画で取り組むべき重要課題である。
経済産業省では、Connected Industriesによって実現される新たなサプライチェーンのリスクに対応するための「サイバー・フィジカル・セキュリティ対策フレームワーク」の策定を進めているところである。現在、英語版も含めましたパブリックコメントを実施しており、今年度末をめどに取りまとめていきたいと考えている。
こうした取り組みを通じて、NISCを中心とした関係省庁及び産業界と連携しつつ、サイバーセキュリティ対策の強化に取り組んでまいりたい。

（３）決定事項の決定等

○（櫻田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）
○櫻田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「サイバーセキュリティ意識・行動強化プログラム」を決定することができた。
今後、このプログラムに基づいて、NISCを中心に関係省庁に取り組んでいただきたい、その事項について、３点、指示をする。
第１は、中小企業・若年層・地域に対する施策の推進である。
中小企業の対応を支援するための相談窓口の設置など、新たな仕組みづくりや、若者が法令に関する知識が十分でないまま、被害者から加害者にならないようにするためのリテラシー教育の教科など、関係者が連携して、プログラムの重点対象のニーズに応じた施策を推進していただきたい。
第２は、官民の連携による情報発信の強化である。
普及啓発の対象と関係者の役割を明確化し、ラストワンマイルに情報が行き届くようにするために、サイバーセキュリティに関する施策をまとめたポータルサイトを構築するなど、国民に対する情報発信の強化をお願いしたい。
第３は、プログラムの確実な効果検証である。
本プログラムに基づく各府省の取り組み内容とその効果を、NISCが包括的に評価し、不断の見直しをお願い申し上げる。
２月１日から始まる「サイバーセキュリティ月間」を始め、本プログラムを踏まえて、櫻田大臣のリーダーシップの下、関係大臣が連携して取組を進めるようお願い申し上げる。

－ 以上 －