サイバーセキュリティ戦略本部
第36回会合　議事概要

１　日時

令和５年７月４日（火）　　１７時００分～１７時３５分

２　場所

総理大臣官邸４階大会議室

３　出席者（敬称略）

松野　博一	本部長（内閣官房長官）
谷　　公一	副本部長兼国家公安委員会委員長
大串　正樹	デジタル副大臣
柘植　芳文	総務副大臣
山田　賢司	外務副大臣
太田　房江	経済産業副大臣
木村　次郎	防衛大臣政務官
上沼　紫野	弁護士（虎ノ門南法律事務所）
後藤　厚宏	情報セキュリティ大学院大学学長
酒井　啓亘	京都大学大学院法学研究科教授
櫻井　敬子	学習院大学法学部教授
田中　孝司	KDDI（株）代表取締役会長
松原　実穂子	日本電信電話（株）チーフ・サイバーセキュリティ・ストラテジスト
村井　純	慶應義塾大学教授

（※高市経済安全保障担当大臣、遠藤本部員及び土屋本部員はご欠席。）

磯﨑　仁彦	内閣官房副長官
村田　隆	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
岡野　正敬	内閣官房副長官補

4　議事概要

（1）本部長冒頭挨拶

本日はご多忙の中、お集まりをいただき、感謝申し上げる。

本日は、「サイバーセキュリティ2023」、「令和６年度予算重点化方針」、「政府統一基準群」、「重要インフラの安全基準等策定指針」のそれぞれの案について、ご審議いただく。

安全保障環境が厳しさを増す中で、サイバー攻撃を行う側の攻撃手段等も変化しており、サイバー攻撃の深刻化・巧妙化が一層進んでいる。

こうした情勢も踏まえ、セキュリティ政策の在り方について、本日も限られた時間ですが、活発なご討議をお願い申し上げる。

（2）討議

【決定事項】

・「サイバーセキュリティ2023（2022年度年次報告・2023年度年次計画）（案）」及び「サイバーセキュリティ関係施策に関する令和６年度予算重点化方針（案）」について
・「政府機関等のサイバーセキュリティ政策のための統一基準群（案）」について
・「重要インフラのサイバーセキュリティに係る安全基準等策定指針（案）」について

○谷副本部長兼国家公安委員会委員長

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。

○上沼本部員

「サイバーセキュリティ2023（案）」及び「関係施策に関する予算重点化方針（案）」の取りまとめに感謝。現状及び重点ポイントに非常に目配りがされている計画だと思う。

それに加えて、「政府機関等のサイバーセキュリティ政策のための統一基準群（案）」及び「重要インフラのサイバーセキュリティに係る安全基準等策定指針（案）」、いずれも充実した内容であると考えている。

その上で、具体的な施策についてコメントを若干述べさせていただければと思う。

日本は、安全と水はタダだという環境で生活できていて、これは非常に幸せなことだとは思うが、その一方で、今、ネットワーク化、グローバル化の環境の中で、セキュリティが危険に非常にさらされており、それに対する対策が必須であるという状況である。

特に、サイバーセキュリティの最前線に位置するにも関わらず、最前線であるという認識のない中小企業における対策というのが非常に重要で、その意識をどのように啓発していくことが難しいところなのだと思う。その意味で、昨年に引き続き、中小企業のサイバーセキュリティ対策が重点施策とされていることは、非常に心強いと思っている。

また、これまでの取組実績として、セキュリティにつき、「コスト」から「投資」への発想転換が必要だということが挙げられていた。確かにサイバー攻撃がないことが当たり前という時代であれば、セキュリティ対策は「費用」と理解されることになると思うが、それを守ることが必要だという時代である現在においては、セキュリティ対策は「投資」と理解されることになるのだと思う。特に、弁護士を含めた士業もまた、中小企業、実際上は個人事業主に当たるため、セキュリティ対策への投資の重要性については非常によく分かり、身につまされる思いがする。その意味で、中小企業の方々に対する対策というのを今後とも充実させていただくのは、自分のことを思っても、非常に重要なことであると思う。

○後藤本部員

まず、本日の決定事項３件全てに賛同する。特に、今回は様々なサプライチェーンセキュリティ対策がしっかりと明記されていて、非常に頼もしい思いである。

そこで少し気が早いが、さっそく次のステップとして複合的なリスク対策のためのセキュリティへの拡大を考えていただきたい。ここでは短く「複合的セキュリティ」ということとするが、これはサイバー攻撃や自然災害の区別なく、時には複数重なり合うことを含めた、社会的インパクトが大きい事故への対応である。その対策に向けて、例えば国全体でリスクの洗い出しをする、被害予測をする、代替システムを事前に準備する、また、事故対応や復旧の優先度付け等、国全体を俯瞰したレジリエンス施策作りが狙いとなる。

今回の文書でも、政府情報システム又は重要インフラにおいて、サイバー事故への対応策はしっかりあるが、例えばサイバー事故に加えて地震や水害が同時に発生するような、そういった事態を想定し、入念な事前シミュレーションと対応訓練が重要であると考えている。

次に、このような複合的なセキュリティに向けた対策案作りにおいては、様々な資産や経済活動・重要インフラの設備等のデータを、国内外にわたって収集・蓄積・分析できる土台が必要と考える。これらのデータは、デジタル庁が現在整備中のベースレジストリに紐付くものと考えていえるが、元々は各府省庁又は産業界でそれぞれの目的ごとに収集・分析されてきていたため、複合的セキュリティの観点で統合的に活用できるデータとしては、まだ十分に整備できていないと懸念している。支援技術も含め、データの収集・蓄積・分析をしっかりと継続していくことが重要であり、そこ

からの分析結果は、いわば安全保障上のハザードマップにも相当する、機微で重要なものといえるため、ぜひ国主導で進めていただきたい。例えば、今回の強化施策の一つであるナショナルサート機能では、サイバーインシデント情報の収集・共有に加えて、複合的セキュリティに必要な幅広いデータの収集・分析を、大学等を巻き込む形で主導すべきと考えている。

最後は人材育成についてである。地域や中小組織では、今でもサイバーセキュリティ人材が大幅に不足している。今回提示された様々な施策を通して人材を育成することは最重要。加えて、今回、複合的セキュリティにおいて、関係する専門領域をまたがって活躍できる人材、例えば法制度・経済・ビジネスといった色々な領域をまたがってサイバーセキュリティに結び付けられる人材を育成していくことが必要であり、ぜひご検討をお願いしたい。

○酒井本部員

主として私の専攻分野である国際法の立場から、今回の決定事項３件についての若干の意見を申し上げる。

まず、昨今の厳しい安全保障環境の下、サイバー空間での不正規な活動もまたその一因とされるところ、そのような状況に照らし、今回の決定事項の案を取りまとめていただいたことについて、関係者の皆様に敬意を表したい。

自由、公正かつ安全なサイバー空間の実現のため、法の支配の推進、サイバー攻撃抑止のための取組の推進、能力構築支援などの取組と並んで、国際連携協力の取組を取り上げていただいたことは非常に重要な点だと考える。したがって、今後の取組において、「サイバーセキュリティ2023（案）」においても、同盟国・同志国との間で、様々なレベルで重層的に国際協力を推進していくことは、極めて説得力のある方針であると考える。

また、昨年12月に決定された国家安全保障戦略において、我が国を全方位でシームレスに守るための取組の強化を行うことが謳われており、この取組が国家安全保障戦略に基づいた形で行われている点にも留意したい。今後の課題の一つは、こうした国際連携・協力をより具体化し強化していく作業ではないかと考えている。インド・太平洋地域における能力構築支援や、日本など４か国の上級サイバーグループ会合などでの国際連携がこれまで行われ、我が国の安全保障にも大きな貢献をなしているが、こうした取組を継続し、更に強化していくことも重要である。

また、サイバー安全保障の分野で対応能力の向上に努めつつ、欧米主要国との連携も強化し、世界最先端の技術等の活用や、政府内外における人材の育成の促進を図ることも、これまで以上に求められることではないかと思う。

他方で、サイバー空間の脅威に対して、法の支配を強化する観点から、いかなるルールがサイバー空間での活動に適用されるのかということを関係国間で議論を進めて

いくことも重要ではないかと考えている。

本年４月18日に採択されたG7外相コミュニケでも、国連憲章を含む既存の国際法がサイバー空間にどのように適用されるかについて、全ての国が実質的な議論を深めることが求められており、今後のサイバーセキュリティ戦略の策定においてもこの点に留意することが必要ではないかと思われる。

このためにも、今後のサイバーセキュリティの年次計画において、国家安全保障戦略におけるサイバー空間での取組と、サイバーセキュリティ戦略の３つの方向性との関係を整理し、明確に位置付けることも重要な課題となると考える。

○櫻井本部員

今回の「サイバーセキュリティ2023」等については、全体に穏当な内容であり、了としたいと考えている。私からは最近の新しい動きもあるので、今後に向けてコメントをさせていただければと思っている。

サイバーセキュリティについては、今の国際協調の問題もそうなのだが、アクティブサイバーディフェンスの議論など、憲法を含めた法律論が問題となり得る。私としては、こうした新規の問題に対するロジックの立て方について、例えば「通信の秘密」といった、みんなが知っていると思っている伝統的な概念について、分かったふりをしないで、そもそもそれがどういう議論で、何を守ろうとしてきたのかについて、技術面に目を向けて精査をする必要があるだろうと考えている。

「通信の秘密」は、遡ると19世紀、1889年の明治憲法にいう「信書の秘密」に行き着くのだが、これを技術面に踏み込んで考えると、人類史的に言えば、紙と、文字を書く道具の発明を前提に、明治時代になり近代的な郵便制度が導入されて、そうした制度的前提の上で語られるようになった概念であると承知している。そこでの基本的な想定というのは、人間が手で書いた書面を、人間が関与する形で運ぶということになる。これに対して、現代では、例えば電子メール等が登場しているが、電子メールの秘密というのは、秘密とはいっても、技術的には、サーバ管理者やメールの管理者が閲覧することは、システム上は可能であるし、情報の伝達というのは、グローバルなネットワークを通して、機械的、自動的に行われる仕組みとなっている。そこでは膨大なデータがほぼ瞬時に桁違いの多数者に送付され、到達するという状況が現出しており、伝統的な郵便と異なって、いわゆる住所はもはや意味を持たない。

技術面に目を向けると、電子メールというのは、やはり客観的には信書とは似て非なるものであり、信書とは異なる何物かであるということになるのであって、それが議論の出発点にならなければならないだろうと思う。そうすると、100年以上前の「信書の秘密」の議論を持ち出すとすると、それにはかなりの留保が必要であると考える。こういう暗黙のアナロジーというものを一旦取り払った上で、従来の議論を分解して、その上で、サイバー空間でやり取りされる情報の流通に関して、守られるべき利益と

は何かということを、憲法論を踏まえて検討することが大切だと思う。外国法に安易に飛びついたり、あるいは昔ながらの法律論に拙速に入り込む前に、行政としては、こういうテクニカルで地道な作業をしていただきたいと考えており、ご留意いただければと思う。

○田中本部員

まずは、決定事項３件について異論はない。サイバー空間を巡る昨今の情勢と状況変化をタイムリーに捉えた上で、現時点で必要となる施策が丁寧にまとめられていると思う。今後は、現戦略の完遂、次期戦略の策定の両面を見据えて進めていくフェーズになると思うが、これからの進め方に関して、通信事業者として、現場の声として、コメントする。

昨今、特定の脆弱性、あるいはそれを狙ったサイバー攻撃が引き起こす被害が甚大なものとなり、一企業ひいては社会全体に影響を与えるような事案も発生している。多くの企業においてランサムウェアをはじめとするサイバーインシデントが猛威を振るっており、100％の防御というのが非常に困難な状況である。こうした状況にも鑑みつつ、現行の３か年の戦略も既に後半へと差し掛かっていることから、各施策の到達点とマイルストーンを明確にした上で、確実にこれをやりきって、次期の戦略につなげていただきたい。

次に、次期戦略においては、サイバーインシデントが猛威を振るっている現状に鑑み、ユーザ企業でできる範囲や一般国民ができる範囲などは、現実的なところを見据えた対応も必要であると考えている。また、ご存じのとおり、昨今、守るべき対象である情報資産を有する情報システムだが、クラウドへの移行が進んでいる。また、生成 AI などの新しい技術が登場し、情報システム自体を取り巻く環境が急速に変わろうとしている。基本的には、各企業の経営者がセキュリティを経営課題として捉え、リーダーシップを発揮し、主体的にセキュリティ対策を取っていくべきではあるが、先ほどご意見があったとおり、中小企業等の、リソースやノウハウが不足しているユーザ企業においては、厳しいところがある。中小企業に対しては、啓発や直接手が届く支援をしていくことも重要ながら、大きなインシデントを防ぐための実効的な対策という意味では、中小企業に対して IT 環境を提供しているクラウド事業者や ICT ベンダーの強化が鍵になる。クラウド事業者への依存度が高まる中、ユーザ企業で現実的にセキュリティ対策ができる範囲はどこまでで、それ以降はクラウド事業者などでどう対策してもらうかなど、責務の線引きをした上で、その範囲内の対策をそれぞれ確実にやってもらうことがポイントではないかと考えている。具体的には、クラウド事業者に高度なセキュリティ対策を実施してもらうことで、ユーザ企業側は、必要なセキュリティ対策をやってもらいながらも、自らのビジネスに注力いただく。このようなことができれば、日本全体として、今後の経済成長を支える DX 化の更なる進展とセキ

ュリティ強化の両立が図れるのではないか。

次期戦略においては、現実を見据えた実効性の高い戦略、施策を考えていただくことで、さらに一段階、我が国のセキュリティレベルを引き上げていく時期に来ているのではないかと思う。

○松原本部員

今回取りまとめられた３点全ての決議事項に賛同する。関係者の尽力に感謝する。その上で、取りまとめられた３点にも出てくる重要インフラの防御、後藤本部員も仰られた複合的セキュリティのリスクが重要インフラ企業にどのような影響を及ぼしているかを述べる。

ウクライナで続いている戦争を見ても、重要インフラ企業に対して、情報を窃盗するためのサイバースパイ活動、そして重要インフラ企業を妨害するためのサイバー攻撃活動が、有事、平時の境目がはっきりとしていない形で行われており、平時から国内外の官民連携、サイバー攻撃に関する最新情報の共有や、実際に有事に対応することを念頭に置いた演習の実施が必要となる。

例えば台湾では、1980年代から有事に備えた演習が行われてきた。この演習ではかなり前の段階から、シナリオにサイバー攻撃に関する内容が盛り込まれている。ウクライナの例を見ても分かるとおり、有事の際には重要インフラも巻き込まれることから、2021年からは、重要インフラ企業も加えて、実際に有事の際に重要インフラを守れるのかということを試すシナリオが組み込まれている。この事例は日本においても参考になると考える。

ウクライナの方々を見ていて心打たれるのは、有事の最中であっても、政府高官や重要インフラ企業の社長達が、国際会議や国際メディアに対し、この戦争を通じて得たサイバーセキュリティなどに関する教訓を積極的に発信していることだ。このように、ウクライナでは、少なくともサイバーセキュリティに関し、一方的に支援を受ける立場に甘んじていないのである。

我が国でも、本年６月のシャングリラ会合では岡野官房副長官補、そして昨年10月のシンガポールでのサイバーセキュリティ国際会議では吉川NISC副センター長が登壇し、日本の存在感を示された。ぜひウクライナを見習って、日本も官民からスピーカーを輩出し、日本は頼りになる協力すべき国であると世界に存在感を示すべきである。

○村井本部員

私も松原本部員の意見に賛成で、外から見ている時に、日本は何をしているかということに関して、やはり自信のあるドキュメントを作らなすぎで、今回の年次報告・年次計画も、民間事業者にとってもとても重要なものである。英語での発信も重要だ。

NISCができた時から、アメリカではホームランドセキュリティのためにISACを作っ

て、重要インフラの情報を全て取りまとめるようにした一方、日本では、その時セプターというものを作って、重要インフラに対する情報交換など、重要インフラ事業者の横の連携をきちんと構築する取組をずっと続けてきている。そうしたことを踏まえれば、今回の年次報告・計画は、長い間関わってきている者としては、「慎ましすぎる」ということを最初に指摘したいと思った。

また、現在のウクライナの状況を見ていて、２つの大変重要なことが分かってきていると思う。それは通信と電力のインフラの優先度である。前回の戦略本部会合でも申し上げたが、デジタル社会になって、全ての国民、全ての産業、それらを支える全てのインフラ産業にデジタルインフラすなわちコンピュータとネットワークが関わるようになった。

ウクライナの政府高官のメッセージも全てインターネットを通じて発信される。しかし、そもそもインターネットは電気がなければ動かない。電力インフラをきちんと守ることに関して、今回、ウクライナは、ロシアによる侵攻が起こる１週間ほど前から、かなり大掛かりにスマートグリッドの再編を計画し、これをやり遂げた。このように、早い内から計画し、実際に再編をやり遂げたので、ウクライナにおける現在の電力インフラの安定がある。

本戦略本部会合はサイバーセキュリティを議論する場なので、サイバーセキュリティの高度な体制のために、日本全国の電力の最高の知恵といえるほどのスマートグリッドに相当する環境があることがとても大切である。これも重要インフラの議論のすぐ先の議論として、また、ウクライナからのレッスンとして、そこに取り組むべきだというのが１点目である。

もう１点は、GPSに関してである。今回、サイバー攻撃の一環としてGPSジャミングとGPS電波妨害が行われている。現在、例えば一日GPSが止まった場合、アメリカによる試算だと10億ドル、約1,300億円の経済損失が生じると言われている。現在インターネット上のサービスで用いられる位置情報と時刻は、２万キロほど上空にある衛星による、GNSS（注：Global Navigation Satellite System。衛星測位システム）というシステムに依存している度合いが非常に大きい。これはアメリカ海軍の運用によるものだが、アメリカのE911（注：Enhanced911）への要求でも、つまり110番と119番の時に通話者の位置が分かるようにしようとしている。また、例えば津波から逃げるときにも、位置の把握が重要であり、消防士の命を守るにも、位置が大事である。ただし、GNSSの衛星からでは、何階にいるのかなどの、高さの情報が分からない。そこで、高さの情報も読み取れるように取り組みなさいと、アメリカでもヨーロッパでも指示が出された。こうした動きの一つの契機になったのも、ウクライナの件である。

要するに、GPSなどの衛星によるGNSSの提供する位置情報インフラに依存して、我々の社会が成り立っている。さらに高度な安全を確保するために、それに加えて、GPSの代替に取り組もうという動きが、ヨーロッパやアメリカで出始めている。ぜひ我々

の国でも取り組んだ方がいいのではないか。これもサイバーセキュリティやデジタルコンテンツ、ひいては国民や国土を守るということにつながる重要な取組といえるのではないか。

【閣僚本部員発言】

○谷副本部長兼国家公安委員会委員長

引き続き、副本部長・閣僚本部員から、御発言をお願いする。なお、本日は会議時間が限られているため、あらかじめ、書面でいただいた御発言内容を、資料として配布している。こちらについては、議事録に掲載することで、御発言に代えさせていただく。

（※なお、高市経済安全保障担当大臣は当日ご欠席だったが、あらかじめ、御発言内容の提出があったため、併せて掲載する。）

（以下は閣僚本部員から提出された発言内容）

○谷副本部長兼国家公安委員会委員長

サイバーセキュリティ戦略を着実に推進していくに当たり、多様化・複雑化するサイバーリスクに対応していくため、

・政府機関においては、政府統一基準群を踏まえ、ソフトウェア利用時の対策やDDoS対策の強化等、

・重要インフラ分野に関しては、重要インフラの安全基準等策定指針も踏まえ、組織統治の観点からの取組の強化等

に取り組むことにより、政府機関及び重要インフラ分野のレジリエンスの更なる向上に努めてまいる。

また、国家公安委員会委員長として申し上げる。警察では、昨年設置されたサイバー警察局及びサイバー特別捜査隊を中心に、民間事業者、国内外の関係機関と連携し、サイバー事案への厳正な取締りや実態解明、被害防止対策を推進しているが、今後も、関係機関等との連携をより一層強化し、サイバー空間における安全・安心の確保に努めてまいる。

さらに、サイバーセキュリティ担当大臣である副本部長として、引き続き、関係省庁とも連携し、これまでNISC をはじめとする関係省庁が培ってきた取組実績を生かしつつ、政府一体的に取組を着実に推進してまいる。

○高市経済安全保障担当大臣

昨年成立した「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」においては、国際的にサイバー攻撃等の脅威が増大している状況も踏まえ、基幹インフラ役務の安定的な提供を確保する観点から、基幹インフラ事業者における

重要設備の導入等を国が事前審査する制度を措置しており、現在制度の円滑な施行に向けて準備を進めている。

また、サイバー攻撃対策を含む様々な分野で、今後利用可能性がある先端的な重要技術の研究開発を促進し、その成果を活用していくことは重要であり、経済安全保障重要技術育成プログラムの支援対象となる重要技術として、研究開発ビジョン（第一次）において、不正機能検証技術等を指定し、研究開発を推進しているところ。

サイバーセキュリティに関するリスクへの対応は、経済安全保障の観点からも極めて重要であり、特に国際情勢の変化等を踏まえたサイバーセキュリティの確保に向けた官民連携や分析能力の強化について、政府全体として取組を進めていく必要がある。引き続き、関係大臣と連携して、必要な取組を行ってまいりたい。

○大串デジタル副大臣

デジタル庁としては、本日ご議論いただいた「政府機関等のサイバーセキュリティ対策のための統一基準群」を踏まえ、NISC 等の関係省庁と緊密に連携しながら、デジタル庁が所管する情報システムの整備・運用やセキュリティ対策を着実に実施していく。

先般閣議決定された「デジタル社会の実現に向けた重点計画」を着実に実施する中で、サイバーセキュリティ等の安全・安心のための対策をしっかりと講ずることで、「マイナンバー情報総点検本部」における再点検と再発防止の取組とあわせて、デジタル社会の実現に対する国民の信頼を得られるよう取り組んでまいりたい。

○柘植総務副大臣

本日の決定事項である「サイバーセキュリティ2023」など３点については、昨今の国際情勢や国内でのリスクの高まりを踏まえた、必要な施策が盛り込まれていると考える。

総務省では、「今年度特に強力に取り組む施策」として位置付けられた、

・国産セキュリティソフトにより政府端末から収集した情報をNICTに集約・分析し、政府機関を含む我が国全体の対処能力を向上させる取組
・ASEAN地域におけるノウハウを生かした大洋州島しょ国への支援の検討など、開発途上国のサイバーセキュリティ能力構築支援を強化する取組
・通信分野におけるSBOM導入に向けた取組

などを重点的に進めるとともに、IoT機器の脆弱性等の調査の延長・拡充に関する法案の提出も検討している。

これらの取組を通じて、NICTにおいて積み上げてきた知見も生かしつつ、NISCをはじめとする関係省庁・機関と一体となって、同志国とも連携しながら、我が国のサイバーセキュリティの確保に貢献してまいる。

○山田外務副大臣

あらゆる活動に不可欠な社会基盤であるサイバー空間の重要性及び公共性がますます高まる中、多様なインシデントが発生し、サイバー攻撃が甚大な影響を与えるリスクは増大している。これは我が国にとっても例外ではない。

また、ウクライナにおける政府機関や重要インフラに対するサイバー攻撃に見られるように、組織的かつ周到に準備された高度なサイバー攻撃の脅威も存在する。

こうした状況下では、同盟国・同志国との連携が今まで以上に重要。５月の日米豪印首脳会合では、サイバー事案及び脅威への地域の能力及び強靱性を高めるための各種取組を強化することを確認したほか、2022年度には、英、仏、印等と協議を実施。サイバー空間における法の支配の推進や途上国の能力構築支援にも努めている。

引き続き、同盟国・同志国と緊密に連携しつつ、サイバーセキュリティ上の課題に対応していきたい。

○太田経済産業副大臣

今回のサイバーセキュリティ2023において、特に強力に取り組む施策として、「 中小企業のサイバーセキュリティ対策促進」を選出いただいた。

サイバー攻撃の手法は年々高度化しており、昨今は、サプライチェーンの中でセキュリティが脆弱な部分が狙われるようになっていることから、中小企業を含むサプライチェーン全体でセキュリティのレベルを強化する必要がある。

サイバーセキュリティ対策の強化のためには、まずは 、経営者自身が責任を持って対策に取り組むことが重要である。経済産業省では、経営者向けの「サイバーセキュリティ経営ガイドライン」を策定しており、昨今の情勢等を踏まえ、本年３月に改訂を行ったところ。

本ガイドラインを活用した経営者の意識改革に加え、中小企業向けのセキュリティサービス、「サイバーセキュリティお助け隊サービス」の普及促進・運用改善を通じ、引き続き、中小企業を含めた、産業界全体のセキュリティ対策の強化に取り組んでまいる。

このほか、「サプライチェーンリスクの増大を踏まえたソフトウェアセキュリティの高度化」や「インド太平洋地域における能力構築支援」についても、関係省庁と連携して、強力に進めてまいる。

○木村防衛大臣政務官

防衛省においては、昨年12月に国家安全保障戦略とともに閣議決定した防衛力整備計画等に基づき、常時継続的にリスクを管理する「リスク管理枠組み（ＲＭＦ）」の導入、「防衛産業サイバーセキュリティ基準」に従って実施される防衛関連企業のサイバーセキュリティ対策を強化するための取組などを推し進めているところ。これら

の取組により、本日の議題である「政府統一基準群」でも参考にされている米国のセキュリティ基準と同じ水準のセキュリティを担保する。

また、防衛省としては、2027年度を目途にサイバー専門部隊を約4,000人に拡充するなど、自らのサイバー防衛能力の抜本的強化に取り組んでいるところ。今後、サイバーセキュリティ戦略本部の一員として、我が国全体のサイバーセキュリティの強化にも引き続き積極的に貢献してまいる。

（３）決定事項の決定

○谷副本部長兼国家公安委員会委員長

それでは、本日お諮りした３件の決定事項について、異議はないか。

（「異議なし」と声あり）

○谷副本部長兼国家公安委員会委員長

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、年次報告・計画である「サイバーセキュリティ 2023」のほか、「サイバーセキュリティ関係施策に関する令和６年度予算重点化方針」、「政府機関等のサイバーセキュリティ対策のための統一基準群」、「重要インフラのサイバーセキュリティに係る安全基準等策定指針」について決定した。

これに関連して、私からは以下の点について皆さんにお願い申し上げる。

まず、国家安全保障戦略に基づき必要な取組を進めていただくよう、お願い申し上げる。

また、「サイバーセキュリティ 2023」において「特に強力に取り組む」とされた６つの施策を中心に、関係省庁において着実に取組を進めていただくよう、お願いする。

その際、全省庁が一体となって連携・協力するとともに、民間事業者をはじめとする関係者の理解と協力を十分に得ながら取組を進めていただくよう、留意をお願い申し上げる。

また、各施策を適時適切に見直すことも大事である。その検討に当たっては、本戦略本部の下で、関係者が連携して取り組んできた、これまでの取組実績を生かしつつ総合的な視点から進めていくよう、お願い申し上げる。

次に、昨今のマイナンバーを巡る事案やランサムウェア攻撃による機能停止等の事案を踏まえると、セキュリティを十分に確保した上で政府のデジタル化を推進し、行政への信頼の向上を図ることが重要になっている。

また、今日の国民生活の基盤を成す経済活動や社会の安定性を支える重要インフラの安定的な供給を確保することの重要性がより高まっている。

サイバー空間上のリスクが多様化する中で、我が国の政府機関や重要インフラ分野における情報システムの防御力やレジリエンスの向上がますます重要になっている。本日の決定文書を踏まえた取組を着実に進めていただくよう、お願い申し上げる。

－ 以上 －