サイバーセキュリティ戦略本部 第43回会合 議事概要

1 日時

令和7年5月29日（木） 8時00分～8時40分

2 場所

総理大臣官邸2階大ホール

3 出席者（敬称略）

林 芳正	本部長（内閣官房長官）
平 将明	副本部長兼デジタル大臣
坂井 学	国家公安委員会委員長
城内 実	経済安全保障担当大臣
阿達 雅志	総務副大臣
加藤 明良	経済産業大臣政務官
小林 一大	防衛大臣政務官
生稲 晃子	外務大臣政務官
上沼 紫野	弁護士（LM虎ノ門南法律事務所）
遠藤 信博	日本電気（株）特別顧問
後藤 厚宏	情報セキュリティ大学院大学教授
酒井 啓亘	早稲田大学法学学術院教授
田中 孝司	KDDI（株）取締役相談役
村井 純	慶應義塾大学特別特区特任教授

（※櫻井本部員、土屋本部員、松原本部員はご欠席。）

青木 一彦	内閣官房副長官
佐藤 文俊	内閣官房副長官
小島 裕史	内閣危機管理監
鈴木 敦夫	内閣サイバーセキュリティセンター長
阪田 涉	内閣官房副長官補
市川 恵一	内閣官房副長官補
飯田 陽一	内閣サイバーセキュリティセンター長代理

4 議事概要

（1）本部長冒頭挨拶

本日はご多忙の中、ご参加いただいたこと、まず御礼申し上げます。

今日は、「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項」、「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」そして「サイバーセキュリティ対策を強化するための監査に係る基本方針の一部改正」について、ご決定をいただくことになっている。

報告案件にある通り、前回会合の後、サイバー対処能力強化法案等が国会に提出され、成立しているところである。

今日も限られた時間であるが、こうした情勢も踏まえて、今後のセキュリティ政策の在り方について、活発なご討議をお願いする。

(2) 討議

【決定事項】

- ・ 「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項（案）」について
- ・ 「「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対策を強化するための監査に係る基本方針」の一部改正について

【報告事項】

- ・ サイバー対処能力強化法等について
- ・ インシデント報告様式の統一について
- ・ 政府のサイバーセキュリティに関する令和7年度予算

○平副本部長兼デジタル大臣

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

本会合で示された案について賛成する。

また、サイバー対処能力強化法及びその関連法が成立したことは、日本国民の生命身体に対する重大な危機をもたらさうるサイバーテロに対する防御態勢の基本ができたものとして、非常に期待している。

そのうえで、以下の通り3点意見を申し上げます。

まず、1点目は事務局からご説明があった新司令塔機能についてである。

サイバーセキュリティに関する対策はその性質上迅速な対応が必須である。また国外を含め、多くのソースからの情報を集め、分析し、これを効率的に利用することが求め

られる。

これを実施するためには、リーダーシップを持った組織がその全体を統括することが必須である。

新組織には非常にこれを期待しているので、今後人材も含め拡充することを期待している。

2つめが国民への告知である。今回の法律の成立を機に、国民への丁寧な告知をお願いしたい。

今回、新法に関し、個人的にはとてもカッコいいリーフレットを作っていただいたと思っている。

このような取り組みはサイバーセキュリティという言葉や事象に関する国民のハードルを下げ、当事者意識を高めると思う。

特に喫緊の課題にも記載されているように、サプライチェーンを構成する中小企業に対策していただくことが重要である。その際には、是非とも「がんばりすぎなくてよい」というメッセージを意識的にお願いしたい。日本は、水と安全はタダという非常に幸せな社会環境で暮らしてきたので、その状況から「レベルの高い対策を取れ」と言われてしまうと、それだけでなかなか抵抗感を示してしまう。

かつ、日本の社会は減点方式になりがちなので、完璧じゃないとやってもしょうがないという風になりがちなので、そうではなくて、「ゼロよりは良い」ということを是非意識的に伝えていただければと思う。

特に今回のヒアリング等で、ちょっとした対策で効果があるということがわかっているので、そういうことを、ちょっとでもよいのだということを是非お伝えいただければと思っている。

最後に柔軟な対応をお願いしたいと思う。最初にも申し上げたとおり、サイバー対策はスピード感が重要で、かつ、変化の激しい領域である。扱う内容も重要ではあるけども、その重要であるが故に、あんまり慎重になりすぎることなく、法制度でも組織体でも柔軟な対応をしていただきたいと思います。

今回、インシデント報告の簡易化をしていただいたが、そういうような柔軟な対応を今後とも是非していただければと思っている。

○遠藤本部員

まず、今日ご説明頂いた資料に関してはすべて賛成を致したい。特に各団体へのヒアリングの内容をこの中に盛り込んで頂いたことに感謝を申し上げたい。特に官民のインシデントの報告等について、フォーマットの統一、さらには窓口の一本化等の負担軽減策を入れて頂いた。感謝を申し上げる。

私からは3点申し上げたい。

1つは、司令塔の機能に関してである。次期NISCには、CISA、NCSCとい

うような求心力のある司令塔を目指して頂きたい。その中でも特に注力すべきなのは情報収集機能であって、国内外で発生したサイバー攻撃、ネットワーク探索活動を余さず把握して、さらには技術の進化、これらの新たな活用などを推定して少し先の未来を先読みした対応を出来るようなセキュリティ戦略を立てる仕組みをお作り頂きたいと考えている。

2つ目は官民連携である。官民連携で重要なのは官と民との目標の共有化と思う。国家のレジリエンス強化といった一つレベルを上げた官民が共に求める目標というものを掲げて、危機感の共有のもと、目指すサイバーセキュリティを明示化し、共にそれに向かって努力する関係を構築することが大きな効果を生むと考える。特に、官民連携においてはセキュリティ・クリアランス制度を活用して防御が必要なサイバー攻撃を、さらにはインシデント情報の官民の間での共有化、さらには官民で共同した備えと対処に期待をしたいと思う。さらに諸外国の情報共有に対する国際社会へのリーダーシップを持った貢献というものをお願い申し上げたい。

最後は人材育成。日本は多くの分野で優れた技術を持っているが、ソフトウェア技術に関しては未だ欧米の先進諸国に追いつけていないのが実情ではないかと理解している。その点に関しては「欧米諸国と同等以上」といった明確な目標を持ち、幼少期からのプログラミング教育の実施というような観念、さらにはロックド・シールズのような日本主導の本格的なサイバー演習等、今までになかった思い切った教育施策が必要と考える。また、日本の高いレジリエンスの自律性、国際競争力向上による海外への貢献の為の国産技術および国産のサービス、これを育成・強化・活用することも重要であろうと思う。ぜひご検討をお願いしたいと思う。

○後藤本部長

まずサイバー対処能力強化法の成立に向けて、これまで準備や国会審議の支援をなされたご担当者の皆様に厚く御礼申し上げます。

まず決定事項1番、喫緊に取り組むべき事項だが、これについてはいずれも最重要である。賛同する。また具体的なアクションが一部ではあるが目標時期を含めて明示されていることを頼もしく思う。その上で今後の期待をいくつか述べさせていただく。

まず先ほどから出ている新たな司令塔機能だが、私どもとしては、サイバー・フィジカル両面でのレジリエンス、その観点から、特に他の領域、防災等の領域との連携をしっかりと果たしていただきたいと思う。次に官民対策連携強化の6項目、これはいずれも重要だが、まずは一刻も早く実務を回していただきたい。官民合わせた国全体としての経験値、いわゆる実務を通して得られる知恵とかスキルを蓄積して改善していく、そういうサイクルを早く回していくことが重要と考えている。

次に人的・技術的基盤の強化である。これについては内閣府主管で経済安全保障重要技術育成プログラム、K P r o g r a mが動いており、サイバー空間の状況把握、応

用技術など、今後の能動的サイバー防御の土台となる技術開発に我が国の主要な研究開発組織や実務組織が共同で取り組んでいる。その社会実装に向けて、まず各政府機関の皆様には、自組織や所管の重要インフラのニーズをしっかりと把握していただき、また内閣府には、それらのニーズと研究開発者のシーズを共有し、すり合わせていくなどの力強い伴走支援を期待したいと思う。

また耐量子計算機暗号PQCの社会実装について、政府機関はもちろんのこと、金融などの社会基盤システム、さらにはインターネット全体が安全かつ早期に移行できるよう、国内外の産業界やインターネット関連機関との連携体制をしっかりと構築いただきたい。

また人材育成については、施策の開始から成果が具体化するまで5年、10年、20年と時間がかかってしまう。早期着手とともに、中長期プランを持って継続的に進めていくのが重要と考えている。

決定事項2番「「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、3番「サイバーセキュリティ対策を強化するための監査に係る基本方針」の一部改正について、いずれについても重要な課題であるので全面的に賛同する。

○酒井本部長

まず、「サイバー空間を巡る脅威に対応する喫緊に取り組むべき事項（案）」などの原案をおまとめいただいた戦略本部の関係者の皆様に対して、その多大な貢献に敬意を表したいと思う。提示された原案は、いずれも本部長からの様々な意見をはじめとして、今回特に行われた各団体からのヒアリングの結果などの確に反映された内容となっており、良く練り上げられたものとなっていると高く評価し、賛同する。その上で、ここではさらに以下の2点につき、今後の課題として意見を申し述べたいと思う。

第一に、これまでの本部長の方々も指摘されているところだが、NISCを発展的に改組して新設される新組織についての件である。その人員構成、適切な規模、求められる規模、付与される権限等を定期的に評価していく制度的枠組みを備えるべきではないかと思われる。新しい組織は、我が国において、サイバー分野では前例のないほど強力な権限を有することが想定されている。政府部内における各省庁との協力、サイバー関係に関する民間部門との連携、国際関係においては諸外国のカウンターパートとの密接な交流など、いずれも司令塔として重要な役割を担うことになるわけだが、それ故に急速に変化するサイバー分野での外的環境への対応や、今般国会で可決されたサイバー対処能力強化法とその整備法の施行による、実践的な活動の遂行とその効果についての評価を踏まえて、逐次、その時代の情勢に 대응できるように、新組織のあるべき理想像を検討し、修正すべきところを修正していくというを行うことが必要となるように思われる。強力な権限を有することになる新組織を整備する段階にある今だからこそ、今

後の組織の強化やその適正化に資するような制度を考案しておくことが肝要なのではないかと考える次第である。

第二に、今申し上げた新組織と、サイバーに関連する活動を手がける他省庁との作業協力や棲み分けなども今後検討していく必要が生じると思われる。これは「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」というところにも関わるが、例えば、デジタル庁では信頼性のある自由なデータ流通、D F F Tを掲げて、データセキュリティの強化を中心とした課題に取り組んでいる。そこでの作業は、多くの場合、サイバー攻撃からの防御を目的とするN I S Cや新組織の考え方と類似し協力しうるものと思われるが、デジタル空間におけるデータの自由な流通をサイバー防御の観点からいかに実現していくかという観点やその場合の考え方も、双方の機関で共有していくことが不可欠と思う。こうしたことは一例ではあるが、新組織が多くの機能を抱え、強力な権限を携えることになればなるほど、こうした関係機関との密接な連携はより具体的な作業において重要になるのであり、それぞれの機関の機能が孤立することなく、有機的な連携を行っていくということについて実際上の配慮が望まれると思料する。

○田中本部員

まず最初に、決定事項3件について賛同する。内容的には我々もコメントさせていただいたが、非常に網羅的で、深いものであると、このように見ている。

その上で、1点だけコメントさせていただくと、これから実装・実行に向かっていくわけだが、まだまだ実行に対して詰めないといけないことがある。

一方、ご存じのとおり、我々を取り巻く環境は初見のいろいろなサイバーインシデントがあるように、どんどん高度化され、大きくなってきている。そういう意味で、実行に際しては、時間軸に基づいて施策を優先順位付けすると、実行性という観点をメルクマールで進めていただければと思っている。

またもう一点。これは短期的ではないが、サイバー人材の不足がやはり言われているが、これも一朝一夕にできるものではないので、是非とも早い段階から強力で推進をお願いしたい、という点である。

○村井本部員

昨今、世界で話題になっているのは海底ケーブルが切られる事件が頻発しており、各国は安全保障の観点、あるいはサイバーセキュリティの観点からも海底ケーブルの切断に関する対応を始めているところだと思う。我が国は特に日本から東南アジアに向かうフィリピンへのケーブルがたくさんあり、冗長性は確保しているが、やはり多くの切断が発生しており、もう少し東にシフトしようというのが新しいケーブルの敷設動向である。一方、EUと日本の接続というのは、今まではロシア周りで2本の線

があったが、これらは随分古くなっており、いま様々な事情で使えないとなると、全てアメリカ大陸経由でヨーロッパの主なトラフィックは動いている。ここだけに依存しているのは遅延も大きい。先日のEU-Japanデジタルパートナーシップフォーラムでも議論されたと思うが、北極海からのケーブルの可能性が出てきたので、EUと日本、あるいは日本を経由してアジアとつなぐこともできる。また、なんといっても陸揚げ局が東京と三重に集中している現状があり、南海トラフ地震の可能性等を考慮すると、これも北海道、九州、あるいは和歌山、こういったところに分散して、冗長性を持つことだけが海底ケーブル敷設における非常に簡単で重要な戦略である。この戦略をデジタル安全保障政策として捉えることが大変重要である。

もう一つ、インフラの話としては、スターリンクで地表の大部分がつながるようになった。宇宙からのインタラクティブなインフラをNTN (Non-Terrestrial Trial Network) という。この技術がどんどん発展してきている。それにより島嶼部や近海がカバーされるのはとてもよい。一方、別の宇宙から来ている電波で、我々のデジタルインフラを支えているのは、GPS衛星から来ている位置情報と時刻の情報である。今回のウクライナの有事では、これをジャムして壊すという攻撃が行われた。日本は、幸い「みちびき」という非常に強い、GPSと補完関係にある衛星があるが、それに加えて、地上での測位インフラを作ることによって、津波から逃げる時、何メートルの高さまで逃げる必要があるかが分かる、そういうインフラを作ることができる。そういう意味では、測位環境もデジタルインフラの一つであり、守るべきインフラとして考えるべきである。

最後にAIについて。AIは、デジタルインフラとしてのコンピュータ、データセンター、ネットワーク、これらを支える電力などとセットで議論されるようになったが、まだ十分に議論されていない部分があると私は認識している。それは、AIの本丸は、デジタルデータであるということ。デジタルデータは、国・各省庁のものもあり、民間のものもあり、特にクリティカルインフラのデータベースは、産業のデータベースとして、民間の側にある。これら全体が日本のAIの未来を担っている大変貴重なデータなのだが、このデジタルデータをどのように守っていくのか。もちろんデータは持って行かれてしまう。見えないだけに、きちんとした体制を作って、デジタルデータをデジタルインフラストラクチャーの一部の重要な要素として捉えて、サイバーセキュリティの文脈で、国民のため・国のために守っていく、こういう体制を準備するのが重要である。

【閣僚本部員発言】

○平副本部長兼デジタル大臣

引き続き、副本部長・閣僚本部員から、御発言をお願いします。

○平副本部長兼デジタル大臣

「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項」については、取りまとめにあたり有識者及び関係府省庁の皆様にはご協力をいただき、誠に感謝する。

今後、新たなサイバーセキュリティ戦略の策定やサイバー対処能力強化法及び同整備法の施行も見据えつつ、取り組んでいく。

○坂井国家公安委員会委員長

警察では、極めて深刻なサイバー空間をめぐる情勢を踏まえ、サイバー対処能力の向上に努めてきたところ。先日、サイバー対処能力強化法・同整備法が成立したが、整備法により警察官職務執行法が改正され、アクセス・無害化措置という、サイバー攻撃に対処するための強力な手段が新たに定められた。今後、警察と共にアクセス・無害化措置を担う防衛省・自衛隊及び国際法規の解釈を所掌する外務省との連携の強化を図るとともに、国家公安委員会の管理の下、その能力の一層の向上を図っていくよう、警察庁を指導することにより、サイバー空間における安全・安心の確保を図ってまいります。

○城内経済安全保障担当大臣

サイバー攻撃は、経済社会、国民生活及び安全保障に深刻な影響を及ぼしており、「喫緊に取り組むべき事項」を踏まえ、経済安全保障に関する施策についても、しっかりと対応をする。

具体的には、本年8月に施行から3年を迎える経済安全保障推進法について、医療分野を基幹インフラ制度の対象とする検討も含め、その施策の充実・強化に向けて、関係省庁の先頭に立って取り組む。

また、今月16日に施行された重要経済安保情報保護活用法についても、民間へのサイバーセキュリティに関する情報共有や、同盟国・同志国との情報協力が円滑に進むよう、その制度の運用に万全を期す。

今後、関係省庁ともしっかりと連携し、サイバーセキュリティの確保にも貢献できるよう、経済安全保障施策の強化に取り組む。

A Iを活用した新たな攻撃手法などサイバー攻撃が巧妙化・高度化しており、先端技術の動向を踏まえた対応能力の強化が重要である。このため、さきほど後藤本部員からも言及があったが、経済安全保障推進法の枠組みの下、経済安全保障重要技術育成プログラム、いわゆるK P r o g r a mにおいて、先進的なサイバー防御機能や分析能力の強化に向けた研究開発や社会実装を進めている。また、昨日成立したA I法ではA Iのリスクに関して国が情報収集、そして調査などを行う新たな枠組みを設け

た次第である。

高度なサイバー攻撃への対応能力の強化に向けて、平大臣はじめ、サイバーセキュリティの関係省庁の皆様としっかり連携して取り組んでいく。

○阿達総務副大臣

今回、「喫緊に取り組むべき事項」がとりまとめられ、いずれも重要な施策と認識している。

総務省としても、情報通信研究機構（N I C T）と連携し、N I C Tが開発した検知ソフトを、N I S Cと協力して政府端末等へ導入を進めてまいる。また、収集したデータの分析能力を強化し、そのデータを活用して、新たな国産の技術・サービスを生み出すエコシステムを構築してまいる。さらに、高度人材の育成のため演習環境の構築にも取り組んでまいる。

また、単独での対策が困難な小規模自治体も念頭に置いた人材確保等の支援など、重要インフラ分野への対策にも取り組んでまいる。このような取組を通じ、サイバー安全保障分野に係る政府の取組に積極的に貢献してまいる。

サイバー攻撃を被害発生前に阻止するには、未知の脅威情報や脆弱性情報を自律的に発見・提供できるようにしていくことが重要である。

総務省では、これまでも、N I C Tと連携し、インターネットの恒常的かつリアルタイムな観測・分析を通じて、我が国独自の脅威情報や脆弱性情報を生成してきており、今後も観測・分析能力の強化を行ってまいる。

また、サイバー対処能力強化法では、政府機関とN I C Tとが相互に緊密に連携し協力することが明記されたこと等も踏まえ、引き続き、N I S Cを始めとする関係機関との情報連携を図ってまいる。

○生稲外務大臣政務官

サイバー攻撃の脅威が深刻化する中で、サイバー安全保障分野の対応能力の強化は喫緊の課題であると認識しており、外務省として、関係省庁と連携しつつサイバーセキュリティの更なる強化に取り組んでまいりたいと思う。

我が国のこうした取組は、同盟国・同志国を始めとする国際社会からも高く期待されている。外務省として、同志国連携や国際的なルール形成の一層の推進、A S E A N諸国や太平洋島嶼国などに対する能力構築支援の実施を通じて、我が国にとって望ましい安全保障環境を構築すべく、サイバー分野に関する外交を引き続き推進していく。

また、今般成立したサイバー対処能力強化関連法に基づき実施されるアクセス・無害化措置についても、内閣官房、警察庁及び防衛省などの関係省庁と連携して、適切に対応していく。

○加藤経済産業大臣政務官

昨今のサイバー情勢を踏まえ、本日示された各事項について異論はない。

その上で、特に「喫緊に取り組むべき事項」について、経済産業省としては、セキュア・バイ・デザインの実現の観点から、3月に制度運用を開始した、安全なIoT製品を認証する制度「JCS-TAR」について、政府調達の要件化や外国制度との相互承認に向けた調整の加速化、サプライチェーン全体での対策強化の観点から、「サイバーセキュリティお助け隊サービス」の普及や見直し、各企業が満たすべきセキュリティ対策の水準を提示し対策状況を可視化する枠組みの整備を含めた中小企業向け施策の拡充、サイバーセキュリティ供給能力の強化の観点から、政府機関等による有望なスタートアップ製品等の積極的な活用等、3月に策定した「サイバーセキュリティ産業振興戦略」の推進など、多くの事項に関係省庁と連携しながら取り組み、我が国全体のサイバーセキュリティ向上に貢献していく。

○小林防衛大臣政務官

今次国会で、重要電子計算機に対する不正な行為による被害の防止に関する法律等が成立したところ、防衛省・自衛隊も重要な役割を担うことに、改めて身が引き締まる思いである。他方、新法の施行の準備に並行して、官民で対応すべきものについて、喫緊に取り組むべき課題が取りまとめられた。取りまとめに協力いただいた関係諸団体や有識者のみなさまに感謝を申し上げる。

本部員省庁として、この文書案を、年次計画及び骨太の方針に打ち込むとともに、確実な予算措置及び機構定員措置が成されるよう努力してまいり。

防衛省・自衛隊としては、関係機関等と緊密に連携し、サイバーセキュリティ人材の確保・育成をはじめとしたサイバー防衛能力の抜本的強化を着実に推し進めてまいりたい。

また、ご指摘のあったNATO主催の「ロックド・シールズ」については、引き続き教訓等を踏まえ、幅広い官民の参加を得つつ、更に発展させてまいりたい。

(3) 決定事項の決定

○平副本部長兼デジタル大臣

それでは、決定事項の確認に移る。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)

○平副本部長兼デジタル大臣

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

今日の会合では、「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項」、「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」、「サイバーセキュリティ対策を強化するための監査に係る基本方針の一部改正」について決定をしたところである。

特に「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項」については、取りまとめにあたり、有識者の皆様にはご協力をいただき、誠に感謝する。

関係府省庁におかれては、これを踏まえた施策の推進について、引き続き、ご協力をお願いしたい。

また、今般、サイバー対処能力強化法及び同整備法成立したことを踏まえ、NISC及び関係府省庁におかれては、法律の施行に向けて万全を期すようお願いする。

また、年内の新たなサイバーセキュリティ戦略の策定に向けた準備をお願いする。

－ 以上 －