サイバーセキュリティ戦略本部
第42回会合　議事概要

1　日時

令和7年2月5日（水）　　17時45分～18時30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
城内　実	経済安全保障担当大臣
武藤　容治	経済産業大臣
坂井　学	国家公安委員会委員長
阿達　雅志	総務副大臣
本田　太郎	防衛副大臣
松本　尚	外務大臣政務官
上沼　紫野	LM虎ノ門南法律事務所　弁護士
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学長
酒井　啓亘	早稲田大学法学学術院教授
櫻井　敬子	学習院大学法学部教授
田中　孝司	KDDI（株）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

（※土屋本部員はご欠席。）

橘　　慶一郎	内閣官房副長官
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　渉	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、まず御礼申し上げる。

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について」、そして「サイバーセキュリティ基本法第13条の規定に基づきサイバーセキュリティ戦略本部が指定する法人」等の一部改正について、ご審議をいただくことになっている。

また、「サイバー安全保障分野での対応能力の向上に向けた提言」そして「2025年サイバーセキュリティ月間」について報告がある。

最近、国家を背景とした高度なサイバー攻撃が発生しているなど、サイバー空間における脅威が高まっており、対応も急務である。

今日も限られた時間であるが、こうした情勢も踏まえて、こ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

【討議事項】

・　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について

【決定事項】

・　「サイバーセキュリティ基本法第13条の規定に基づきサイバーセキュリティ戦略本部が指定する法人」等の一部改正について（案）

【報告事項】

・　「サイバー安全保障分野での対応能力の向上に向けた提言」について
・　2025年「サイバーセキュリティ月間」について

○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

私からは、是非、社会全体のサイバーセキュリティの向上、特に、中小組織のサイバーセキュリティ対策の促進についてお願いしたいと思う。

具体的には、セキュリティ確保のための予防的な支援と、万が一被害に遭ってしまった場合の復旧への支援、というものをお願いしたいと思う。

サイバーセキュリティが確保されることは、現在、事業のみならず、日常生活の前提となっており、避けては通れない課題となっている。

特に、日本の場合、サプライチェーンに組み込まれた、小規模中規模の組織体が産業を支える仕組みとなっており、各事業体がサイバーセキュリティを確保することは不可欠となっている。

ただ、今までは、そのような小規模中規模の組織体が攻撃を受けることはリスクとしてはそれほどないのではないか、と思っていたと思う。自分自身を振り返って、ちょっと反省しているところである。

ところが、最近、身近な事業体で、ランサムウェアの攻撃を受けた、というようなお話をよく聞くようになった。そうすると、認識を改める必要がある。なので、その中小組織体に届くような形で、リスクが自分の組織にも起こりうること、及び実施しうる対策の情報発信を効果的な形でお願いしたいと思う。

情報が集まってくる政府からの効果的な情報発信は、市民全体のセキュリティ意識を押し上げることにもなると思う。

そして、実施しうる対策と申し上げたのは、100%を目指さないということである。ハードルをあげてしまうと、もう無理だということになって、諦めてしまう可能性が高くなる可能性がある。その意味で、可能な範囲、あるいは、これならできる、というところから、是非、情報発信をお願いしていければと思う。そして、ここまで身近にリスクが迫ってきていること、また、100%を目指さないということを合わせかんがえれば、必ず被害は起こることが前提になる。したがって、被害が起こった場合の復旧についての仕組みというのが、どうしても必要ということになる。復旧の場合、過大な労力も必要だし、下手すると、事業全体を諦めなければならない、というようなことになりかねない。これを自己責任といってしまうと、社会全体の活力が低下してしまう可能性があると思う。したがって、そのような被害に遭った場合には、利用しやすい復旧支援の方法というものを、是非、ご検討頂きたいと思う。その中には、例えば、被害に遭った場合の報告の簡便化などという、割と簡単なところも含まれるという風に思っている。

この社会全体を構成する組織のほとんどに届く対応、ということで、社会全体の底上げ、特に日本の場合、足下から底上げをするということが、日本全体の国力を上げていくということになると思うので、そのような形でご検討頂ければと思っている。

〇遠藤本部員

四点申し上げる。

一つ目が中小企業対応である。日本のレジリエンス強化のためには、サプライチェーンを担う中小企業のセキュリティ強化は必須である。しかしながら、中小企業においては、十分なセキュリティ投資は大変困難であり、私が会長を務めるSC3ではサイバーセキュリティお助け隊サービスを実施させていただいており、効果は現状見えているものの、

まだまだ努力が必要である。一方、英国においては、政府が自ら準備をしたセキュリティツールを無償で利用できるACDサービスを提供しており、このような方式が効果的と思われる。これらを参考に日本における即時性の高い、中小企業を含めた国家のレジリエンスの強化方法を検討いただければと思う。

次は官民連携強化である。サイバーレジリエンスの観点からインシデントに対してスピーディに対応し、分析結果や対応方法を周知することは大変有効である。このためにはインシデントが発生した場合の政府機関への届け出の一元化・簡易化、そして政府からの適宜適切な情報の提供を期待している。それに加え、政府内での分析力の強化を図っていただくとともに、IPAやNICTとともに、民間のセキュリティベンダーがより詳細な解析を行う、という官民連携の体制によるスピーディな解析も有効ではないかと考える。

三つ目が産業育成である。我が国のサイバーセキュリティ産業を育て、国内ユーザが忌憚なくセキュリティ強化をするためには、AIや量子技術、特に耐量子計算機暗号(PQC)等の先端技術の研究開発・活用の強化が必要である。それとともにスタートアップ企業の活用を含め日本の国産技術を速やかに立ち上げ、かつ育てるということが日本の自律性の観点からも必須であり、政府が率先して、需要を提供するということも重要ではないかと考える。さらに日本の産業がグローバルで幅広く活用されるためにはセキュア・バイ・デザイン、セキュア・バイ・デフォルトという原則を基に、ソフトウェア産業ではSBOMをはじめとするセキュアなソフトウェアを開発するフレームワーク(SSDF)ガイドラインの普及、さらには安全なIoT機器、Trusted Productなどの活用を促進するとともに、グローバルでの連携を広げるため、海外との相互認証を推し進める仕組みの構築が重要と考えている。

最後に、セキュリティ人材の育成・確保には、高度人材育成とともに、若年層からシニアまでの裾野の拡大、これを両面で考える必要がある。高度人材に関しては、英国のi100やNATOの「ロックド・シールズ」なども参考になるし、人材の裾野拡大に関しては、先月NISCが英国DSIT等と締結した「サイバーセキュリティ人材に関する国際的な連合」の共同声明に従い、役割定義などを共通化するフレームワーク等の活用も重要であると思う。検討いただくようお願いする。

○後藤本部員

私からは５点、提言させていただく。

まず、国産技術開発それからベンチャー産業振興である。ただいま内閣府の経済安全保障重要技術育成プログラム（通称Kプロ）の一環として、「先進的サイバー防御機能、分析能力強化」が進められている。その研究開発の目指す技術は政府機関の日々のサイバーセキュリティ防御に加えて、今後の能動的サイバー防御の土台となる技術である。そこで、サイバー防御技術を必要とする各政府機関はまずは「開発初期から技術要件を提示して、Kプロの成果を自らに引き込む」という姿勢で積極的に導入・活用いただきた

いと思う。

次に、我が国ではサイバーセキュリティ製品に加えて、システム監視や分析から得られるいわゆるマルウェア情報や、脅威情報、それらの海外への依存度が高くなっている。それは逆に主導権を海外に奪われる状況につながっているので、海外との連携を強化しつつ、データ収集・分析から技術開発までをカバーするエコシステムを構築すべきと考える。先ほど遠藤本部員からもあったが、先進的なベンチャーを生み出す新技術を政府機関が率先して活用し、サイバーセキュリティ技術に関連する産業育成を推し進めるには、国としての枠組みの整備が重要と考えている。

２つ目である。これは先ほどもあったが、耐量子計算機暗号(PQC)の社会実装である。政府内で役割分担を明確にして、社会全体でのPQC移行を確実に進める中長期プランを早期に示すことが重要と思う。

３つ目は、サプライチェーンのサイバーレジリエンス・バイ・デザインである。サプライチェーンにおいては、その「防御」、「被害と波及の最小化」、それから「早期回復」、これらの事前準備、つまりサイバーレジリエンス・バイ・デザインが重要となる。そのために、例えばSBOMによるソフトウェアの可視化や中小企業の対策状況の見える化など政府全体で推進する必要があると考える。

４つ目は、最悪ケースを想定した備えである。我が国ではサイバー攻撃被害が複数の重要インフラに波及する可能性や、自然災害・有事などと同時発生することを考慮しなければならない。最悪ケースを想定した被害シミュレーションによる対応プラン策定と訓練など、しっかりした「備え」が必要となる。

最後に「セキュリティ人材の育成」である。これらの取り組みにはセキュリティ人材が不可欠である。「エキスパート育成」に加え産業、業界分野ごとの「プラス・セキュリティ人材」の育成から「普及啓発」まで、幅広い取り組みを政府全体で強化する必要がある。

○酒井本部員

私からは、特に国際社会との連携という側面について、４点にわたり意見を申し上げたい。

第１に、諸外国の機関との連携においては、まずは実務的なレベルでの連携が重要となる。潜在的な攻撃可能性も含め、具体的な攻撃に対して、関係国間で協力して情報交換や技術支援などを行う実践的な側面での協力をより深めることは、サイバー攻撃が激化し、攻撃手法が発展している今日において、これまで以上に実現が求められる課題であると考える。

第２に、そうした実務的な国際協力の枠組みと、その実効的な実施とともに、関係実施機関の活動を通じたサイバーセキュリティ分野における議論と実践の架橋を期待したいと思う。実務的な対応においては被害を未然に防ぐための技術的な基準をその手段

の１つとして用いられるが、その際には民間セクターで生成・発展する新しい技術革新やそれを巡っての基準を官民連携の一環として官の側でも取り込み、これを関係国間においてサイバーセキュリティに関連した将来におけるルール作りへと発展させることも重要な点ではないかと考える。

第３に、他の関係国と、サイバーセキュリティに関連する制度上の連携を強化していく際に、相手国と我が国との制度上の違いや、サイバーセキュリティに関する認識の違いについても理解を深めておく必要がある。アメリカ、中国をはじめとした諸国やEUは、国内法制において安全保障概念を広く取り上げる傾向にある。これに対して我が国の国内法制では、例えば、重要インフラや基幹インフラが、安全保障概念のほか、公の秩序概念を通じて対応がなされることがあり、必ずしも安全保障概念で一貫した対応が行われている訳ではない。攻撃対象に対する法整備において、これらが安全保障の観点から抜け落ちてしまう危険もないわけではない。こうした、比較法的な観点からも、国際的な連携にあたって、国内法制上の齟齬が生じることのないような配慮が望まれる。

最後に第４として、サイバーセキュリティに関連して、これまで以上に国民の権利を制限したり、義務を課すことも、国内法上必要となることが今後も生じる可能性がある。その場合には既存の国内法令で改正を要することもあるだろうし、能動的サイバー防御だけでなく、他の問題についても新規立法が必要となる場合があるかもしれない。この点は、既存の国内法令についての具体的な精査やマッピングがさらに必要であることを意味する。サイバーセキュリティの分野において、既存の国内法令の不十分な点を洗い出す作業を、関係省庁間で協力しながら行っていくことが重要ではないかと思う。

○櫻井本部員

有識者会議の提言に関連付けて発言する。

この提言は、大きく、法律に関わる部分と行政運営に関わる部分からなるが、全体に、サイバー問題の特質を踏まえた新機軸の文書として、評価できると考えている。

法的分野としては、近年、海洋、宇宙、サイバーが三大フロンティアであり、この３領域はもとより歴史は同じではないが、共通するのは本質的にボーダーレスである、ということである。このうち、サイバー空間は、海洋や宇宙と異なり、観念的に把握される側面が強く、特定の問題意識を前提として初めて全体像が明確になるという特徴がある。したがって、政策を論ずるにあたっては、そうした前提を共有しておく必要があると考える。そのうえで、２点、申し上げる。

第１に、政府の役割について申し上げる。サイバー事象は国境をゆうに越え、宇宙空間を経由した脅威があり得る以上、問題を地球規模でみることが必須である。政府は、そうした観点から、世界標準の対応を国内的にセットしていくことが求められるわけであるが、立法にせよ、行政運営にせよ、視点が外にあればあるほど真実に近づくのであり、事柄の性質上、アクターとしては政府が前面に立たざるを得ない。司令塔機能とい

う言い方が掛け声に終わらないよう、完成度の高い組織体制と具体的な仕掛けを用意することが不可欠である。

第２に、官民というが、今日、組織論・機能論からは、官民の境界はすでに相対化しており、官が大丈夫で民が危ないといった、二元的発想を脱却することは当然である。両者の要素を併せ持った事業者が多数存在するので、脅威対策にあたっては、官民の形式にこだわらず、各主体のリスクを個別に評価した上で、特徴に応じた対策を打っていくことが必要だ。特に注意が必要と思われるのは境界線上にある政府周辺法人のほか、地方公共団体があげられる。地方は標準化法のもとで、現代的なシステムがようやく整備されることになった段階であり、各自治体がバラバラであること自体が脆弱性となるので、システム整備と同時に、セキュリティ対策をデジタル庁、総務省とともに注視していくことが重要と考える。

○田中本部員

重要インフラ事業者である通信事業者として現場の立場から意見を述べさせていただく。

皆さんもご存じのとおり昨年の年末又は年始において、重要インフラ分野である情報通信、金融、航空においても DDoS 攻撃で障害が発生している。DDoS 攻撃というものは結構レガシーな攻撃であるが、かなり高度化している。防御し続けても違うところから攻撃してくるような状態で、どう対処すべきかを考えされられたというのが我々の認識である。今まではそれなりに人手で攻撃のポイントを決めて止めていくということをしてきた。しかし、波状的に攻撃してくるため、最新技術、特に AI を代表される最新技術を使って、これまで以上に官民が一体となって対応能力を高めていく必要があると考えている。特に国が司令塔として、関係機関と連携を図り、脅威情報を迅速に共有する実践的な演習を通じて防衛能力を高めていくといった包括的かつ実効的なサイバー防御に向けての対応が必要になると思っている。

ところが、このような対応は大手の事業者はいいが、個別分野の通信回線の細い事業者や中小企業はなかなかそういうわけにはいかないだろうと認識しており、これまで以上の支援が必要なのではと考えている。また準備を整えていき対策していくことも手ではあるが、危急的対策が必要であるため、可能な部分から着手していく必要がある。特に個別企業や中小企業の対策は待ったなしの状況であると認識している。

私としては時間軸に基づいて施策の優先順位を設定するなどして、実効性を考えた施策を推進していくことが緊喫の課題だと思っている。特に現場の状況を考慮した時間軸での施策の優先付けと推進加速を期待している。

○松原本部員

私からは２点お願い申し上げたい。まず一点目が、ただいま田中本部員もおっしゃ

ったDDoS攻撃に関する検証、そして二点目が、先程、遠藤本部員も言及されたロックド・シールズ演習の活用である。

一点目であるが、年末年始に基幹インフラを狙い撃ちにした一連のDDoS攻撃は、日本国民と社会経済に非常に大きな影響を及ぼした。今年はこれから能動的サイバー防御に関する議論が本格化し、日本のサイバーセキュリティにとって本当に大事な年になると思われる。その中では、能動的サイバー防御に関わる、関わらない、いずれにおいても、日本の官民連携のあり方、そして、どのような情報をどのようなチャネルを使って、いかなるタイミングで共有をしていくのかそのタイミング、また、司令塔に必要な機能と体制のあり方についても議論は進むものと思われる。それを検証するために、またとない貴重な体験を与えてくれたのが今回のDDoS攻撃であった。ついては、今回のDDoS攻撃に対する官民連携や司令塔としてのあり方について率直に議論できるよう、官民の関係者を集めたクローズドの検証会を是非実施していただければと思う。

そして、二点目だが、官民連携のあり方を理解するだけでは、中々実現は難しいと思われる。そこで大事になってくるのが、演習である。有事シナリオも含めた実践的な検証ができる場というのは、残念ながら民間にはほとんど無い。唯一の機会となっているのが、先程、遠藤本部員もおっしゃったロックド・シールズ演習である。ただ民間企業としては、安全保障の観点からどのように動いていけばよいのか理解することは非常に難しい。そのため、このロックド・シールズ演習に今年も日本も参加するのであれば、是非、日本政府が司令塔として有事の際にどのように連携したいのか示していただければと思う。

○村井本部員

まず、いまの本部員の先生方のお話を伺っていると、サイバーセキュリティの政策というのは、DX がだんだん広がって、全ての分野がデジタルインフラストラクチャによって動いていくと、こういう社会が日本で、また、他の国にも訪れている。このデジタル政策のコアになるのがサイバーセキュリティになるのだろう、ということを思った。

サイバーセキュリティに関して、政策的な位置づけというのは、その政策は重要だということを認識した上で、技術的に 2025 年に起こることの備えをするべきだと思っており、デジタルデータと計算とコンピューテーション（データセンター）、それからネットワークと電力、これが大変重要になるが、そこにどのようなリスクとインパクトがこれから出てくるかという考え方をするのが重要だと思う。

先生方からも色々とお話のあった AI の処理というのは、AI のアプリケーションを使うだけではなく、その裏には、いま申し上げた非常に大規模な計算、分散された計算能力、それからなんと言ってもデジタルデータの利用、これが非常に重要だと思う。いまインターネットのトラフィックを見ていて、映像のトラフィックを除くと、ほと

んどが非常に大規模なAIの学習データとなっている。したがって、こういうことがインフラ全体にインパクトを与えていく。したがってサイバーセキュリティ軸で、デジタル社会を考えるというのと、AI軸でこれのいわば安全性を考えていく、この２つ考え方がとても大事になると思う。

３つ目は、2025年に起こるであろう、もう起こっていることだが、日本は、レストランに行っても配膳ロボットか動いている。レベル４のバスも動き始めた。今年中にはおそらく、もう既にアメリカでは動いている無人運転のタクシーやドローン、こういうものがこの社会の中で動き出すのではないかと思う。

そうなってくると、ロボットと人間が共存しているような社会のいわば先端的な事例は日本から起こるのではないかと思う。サイバー空間はグローバルな空間ですけれども、その中で日本がどのように安全な社会を作り、そして世界に貢献できるか、こういう考え方がとても重要となる。

【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、御発言をお願いする。

○平副本部長兼デジタル大臣

本日討議いただいた「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、いただいたご意見等も踏まえつつ、サイバーセキュリティ戦略本部の副本部長として関係府省庁とも連携し、早急に検討を進めてまいりたい。

なお、説明中にあった関係者・有識者へのヒアリングは、事務局にて実施の上、次回の戦略本部にて報告させる。

サイバーセキュリティお助け隊サービスは、良いメニューである。私の選挙区で、中小企業の方に話をしてみると、知らない方が多い。これは政府広報も含めて、広く広報していただきたい。必要があれば、そのキャパを増やす取組をしていただきたい。

○城内経済安全保障担当大臣

サイバーセキュリティリスクへの対応は、経済安全保障の観点からも急務であると考えている。

まず、「重要インフラ事業者等の対応能力の向上」につながる取組として、経済安全保障推進法の基幹インフラ制度においては、インフラ事業者が重要設備を導入する際に事前審査を行う制度を運用している。一昨年の名古屋港コンテナターミナルへのサイバー攻撃事案を受け、港湾分野を対象に追加したほか、今年の夏までに医療分野の追加についても検討することになっている。

また、本年５月から施行を予定している重要経済安保情報保護活用法により、サイ

バー攻撃に関する情報を重要経済安保情報として指定して保全し、一定の要件の下に民間事業者に共有することができるようになる。今後、関係省庁においてこうした情報の指定等を検討するに当たり、制度所管として適切に助言や調整を行ってまいりたい。

さらに、経済安全保障重要技術育成プログラムにおいては、サイバー空間の状況把握・防御技術など、「サイバーセキュリティ技術の研究開発」に取り組み、国際連携も見据えつつ、国産技術開発と官民の社会実装を支援している。

引き続き、経済安全保障の確保の観点から、内閣サイバーセキュリティセンターをはじめとした関係省庁ともしっかりと連携し、こうした取組を着実に実施するとともに、リスクを把握し、不断の見直しを図ってまいりたい。

○武藤経済産業大臣

昨今のサイバー情勢を踏まえ、本日示された「検討事項」について議論を進めることに異論はない。

その上で、産業界のサイバーセキュリティ対策の強化をミッションとする経済産業省としては、１．セキュア・バイ・デザイン等の観点から、安全なIoT 製品を認証する制度「JC STAR」の３月からの一部制度運用開始や海外連携の推進、２．中小企業のサイバーセキュリティ対策を促進する観点から、NISCなど関係省庁や関係団体とも連携した「サイバーセキュリティお助け隊サービス」等の全国的な普及広報活動の展開、３．我が国のサイバーセキュリティ産業の振興・育成の観点から、大規模な研究開発プロジェクトの推進　など、多くの事項に貢献してまいりたい。

引き続き、関係省庁と連携しながら、必要な政策対応について検討を深めていきたい。

○坂井国家公安委員会委員長

厳しいサイバー空間情勢を踏まえ、警察においては、サイバー特別捜査部等の体制を強化し、国際共同捜査を通じて被疑者を検挙するとともに、国家を背景とするサイバー攻撃を特定・公表することで抑止する取組を推進している。

また、被害の潜在化防止の観点から、関係省庁と連携し、中小企業等に対し、サイバー事案発生時の迅速な警察への通報・相談を促している。

さらに、サイバー人材の確保・育成に向け、高度な知識・技術を持つ民間人材を積極的に登用するとともに、警察職員に対する研修・教育を強化している。

引き続き、サイバー空間における安全・安心の確保を図るため、ご協力をお願い申し上げる。

○阿達総務副大臣

社会基盤に影響を与えるDDoS攻撃の発生など、サイバーセキュリティ対策は国民の関心も高く、喫緊の課題と考える。

サイバー空間そのものと言える通信ネットワークを所管する総務省としても、電気通信事業者と連携し、IoT機器を悪用したサイバー攻撃への対策などを進めてまいりたい。

また、情報通信研究機構(NICT)が有する先端的な分析・研究能力を活用し、政府機関を標的とするサイバー攻撃に対して、我が国が自らの力で検知し対処していく取組を強化してまいりたい。

また、土屋本部員から指摘のあった、ASEAN及び大洋州島嶼国に対しては、実践的サイバー防御演習などにより、ニーズを踏まえた能力構築支援を積極的に実施してまいりたい。

○本田防衛副大臣

サイバー領域における脅威が日々高度化・巧妙化する中、防衛省・自衛隊のサイバー防衛能力のさらなる向上は喫緊の課題。令和５年度から、リスク管理枠組み（RMF）を全省的に導入するなど、サイバーセキュリティ対策を深化させているところ。

また、サイバーセキュリティ人材の育成・確保について、防衛省・自衛隊では、昨年７月に防衛省サイバー人材総合戦略を公表した。防衛力整備計画の下、サイバー専門部隊を令和４年度末時点の約890人から令和９年度を目途に約４千人の体制に拡充するとともに、当該部隊の要員と合わせて、サイバー要員約２万人体制の実現に向け、必要な取組を着実に進めている。

さらに、NATOサイバー防衛協力センター主催のサイバー防衛演習「ロックド・シールズ」に対しても、自衛隊は、知見や技術を持つ関係省庁、独立行政法人及び民間の重要インフラ事業者等と共に参加し、演習の場を通じて官民連携の強化に努めている。

このほか、防衛装備庁において、防衛産業サイバーセキュリティ基準を定め、防衛生産基盤強化法に基づく財政措置を進める等、防衛関連企業のサイバーセキュリティ対策の高度化を図っている。

防衛省・自衛隊としては、このような取組を通じて、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いく所存。

○松本外務大臣政務官

デジタル化の流れを受けて、サイバー空間が社会全体のあらゆる活動に不可欠な基盤となる一方で、国家によるサイバー攻撃が活発化し、近年のAI技術の急速な発展もあり、サイバー攻撃の脅威が質・量ともに増大している。

特に、病院や発電所などの重要インフラの破壊、先端技術に関する情報の窃取、ランサムウェア攻撃といった事案が日々発生していると認識している。

このような中で、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。

また、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を一層推進し、我が国にとって望ましい安全保障環境作りのため、サイバー分野に関する外交を引き続き推進してまいりたい。

（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１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について」ともう一つ「サイバーセキュリティ基本法第 13 条の規定に基づきサイバーセキュリティ戦略本部が指定する法人」等の一部改正についてご審議をいただいたところである。

これに関連して、関係府省庁の皆さんに私からは以下の点についてお願いしたい。

まず「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、本日有識者の皆様からも大変意義あるご議論をいただいたところであるので、この議論等を踏まえて、とりまとめに向けた検討、これを早急に進めていただくようにお願いをする。

もう一つ、サイバー空間上のリスクが高まる中で、我が国の政府機関や重要インフラ分野におけるレジリエンスの向上、これがますます重要になってきている。関係府省庁においては、サイバーセキュリティの確保に向けた取組、これを着実に進めていただくよう、引き続き、お願いをする。

－ 以上 －