「サイバー安全保障分野での対応能力の向上に向けた有識者会議」（第３回）議事要旨

1. 日時

令和６年８月６日（火）17時00分から18時18分までの間

2. 場所

内閣総理大臣官邸２階　大ホール

3. 出席者

（有識者）

| | |
|---|---|
| 上沼　紫野 | LM 虎ノ門南法律事務所弁護士 |
| 落合　陽一 | 筑波大学デジタルネイチャー開発研究センター長/准教授 |
| 川口　貴久 | 東京海上ディーアール株式会社主席研究員 |
| 川添　雄彦 | 日本電信電話株式会社代表取締役副社長 副社長執行役員<br>一般社団法人 電気通信事業者協会参与<br>一般社団法人 ICT-ISAC 理事 |
| 酒井　啓亘 | 早稲田大学法学学術院教授 |
| 佐々江　賢一郎 | 公益財団法人 日本国際問題研究所理事長【座長】 |
| 宍戸　常寿 | 東京大学大学院法学政治学研究科教授 |
| 篠田　佳奈 | 株式会社 BLUE 代表取締役 |
| 辻　伸弘 | SB テクノロジー株式会社プリンシパルセキュリティリサーチャー |
| 土屋　大洋 | 慶應義塾大学大学院政策・メディア研究科教授 |
| 野口　貴公美 | 一橋大学副学長、法学研究科教授 |
| 丸谷　浩史 | 株式会社日本経済新聞社常務執行役員 大阪本社代表 |
| 村井　純 | 慶應義塾大学教授 |
| 山岡　裕明 | 八雲法律事務所弁護士 |
| 山口　寿一 | 株式会社読売新聞グループ本社代表取締役社長 |
| 吉岡　克成 | 横浜国立大学大学院環境情報研究院/先端科学高等研究院教授 |

（政府側）

| | |
|---|---|
| 河野　太郎 | 国務大臣 |
| 村井　英樹 | 内閣官房副長官 |
| 石川　昭政 | 副大臣 |
| 栗生　俊一 | 内閣官房副長官 |
| 秋葉　剛男 | 国家安全保障局長 |
| 阪田　渉 | 内閣官房副長官補 |

市川　恵一　　内閣官房副長官補
鈴木　敦夫　　内閣官房副長官補
飯田　陽一　　内閣審議官
小柳　誠二　　内閣官房サイバー安全保障体制整備準備室長

4. 議事概要

（１） 河野国務大臣挨拶

○ 皆様には、お忙しい中、今日も御参集いただきまして誠にありがとうございます。

○ この会合、これまで全体会合を２回、テーマ別会合を６回、大変活発に御議論いただいておりまして本当にありがとうございます。今日は、皆様のこれまでの御議論を事務局の方で整理させていただきました。今回、それに沿いまして、今後重点的に御議論いただくところ、あるいは検討の進め方、こういったことについて皆様の御意見を頂戴したいと思っております。取りまとめに向けまして、言わば足場固めになる会合でございますので、活発な御議論を賜りたいと思います。

○ 最近、民間企業への大規模なサイバー攻撃というのも明らかになってきております。日本のサイバー対応能力の向上も、ますます急を要する課題となってまいりました。この会合の取りまとめも喫緊に行わなければならないというような状況になっていると思いますので、本日も活発に御議論いただき、知見を賜りますようお願い申し上げたいと思います。

（２） 事務局説明

事務局より、【資料１】に基づき、有識者会合の開催状況について、【資料２－１】に基づき、これまでの議論の整理（案）について説明があった。

座長から、有識者の了承があったことから、【資料２－１】及び【資料２－２】の案を取る形で「これまでの議論の整理」が公表される予定であるとの発言があった。

（３） 討議

座長から、「これまでの議論の整理」を踏まえ、取りまとめに向けて重点的に議論されるべき点や検討の進め方などについて意見を求め、有識者より、以下のような意見があった。

○ 「サイバー攻撃への対応能力を欧米主要国と同等以上に」という目標のために検討を重ねてきたが、特に制度面において主要国との差を実感し、日本のセキュリティ制度・体制の大幅な強化が必要なことを再認識している。

○ 官民連携を根付かせるためには、官民双方にとって連携がメリットのあるものとし、現場の技術者だけでなく、経営層やアナリストの総合的な判断や解析に必要な具体的情報が共有される必要がある。また、両者が双方向で活発に意見を交わし、さらに

英国の「i100」のような大胆な人材交流の実現が望まれる。

○ 官民での情報共有をより有効なものとするため、セキュリティ・クリアランス制度などをうまく活用することに加え、民側から安心して情報提供が行えるよう、共有に伴う情報漏えいリスク等を限りなくゼロに近づけることも必要である。同時に情報のリアルタイム性と精度を上げるための、情報提供における「フォーマット化」、「用語統一」、「自動化ツールの導入」、利便性に配慮した「窓口一本化」などが重要である。また、官民が連携して、自組織のサイバーセキュリティ成熟度の把握・向上に努め、欧米主要国以上にすることが、レジリエンスの強化につながると思う。

○ 通信情報の利用においては、「対象とする通信対象」「対象とする通信内容」といった前提を明確にした上で、さらなる議論を進めるべきではないかと思う。また、今後電気通信事業者への「具体的な協力依頼内容」「攻撃対象となった場合の支援・補償」「必要となる設備の試算」などの現実的な検討も必要となる。

○ アクセス・無害化措置には、攻撃側を上回る「技術力」と「人材」が必要である。特に高度な人材の育成には長い時間が必要だが、欧米主要国のカリキュラム・教材などを参考にして、知識教育だけでなく実習を通じて実務・コミュニケーション力を習得する必要がある。また、これらは、将来のグローバルサウス等への国際貢献も視野に入れて計画すべきだと思う。

○ 攻撃側組織は環境寄生型攻撃（LotL）のような検知回避技術を使っているが、アクセス・無害化措置の実施場面においても高度なプログラミング技術が必要になってくる。これらの技術は、セキュリティ対策企業等もノウハウを持っており、情報・人材だけでなく技術面においても官民の連携を視野に入れておく必要があると思う。

○ 最後に、日本は現在大幅な人口減少の問題を抱えており、この状況の中で国家のレジリエンスを維持していくためには、関係する事業者の理解・協力を得て、効率的な官民連携の仕組みを構築することが重要となる。ついては、本有識者会議におけるこれまでの議論を経済団体やインフラ事業者に丁寧に説明し、認識の共有を図っていくことが必要だと思う。

○ 「これまでの議論の整理」は非常によくできているものだと思う。他の有識者が指摘のとおり、具体的な制度化あるいは運用の具体化に向けて議論を進めていくべき。

○ そのうえで、２点申し上げたい。

- １つは、通信情報の利用に関する同意に関連する箇所。資料２－２のほうでいうと、９ページの上から５ポツ目になるが、「なお、以上の議論は通信当事者の同意がない場合の通信情報の利用を前提としたもの。通信の秘密の制限に対する通信当事者の有効な同意がある場合の通信情報の利用は、そもそも憲法上許容されると考えられる。その場合の同意の在り方は更に検討していく必要があるが、制度により規格化された内容による同意が方法として考えられる」というところ。

- １点御注意いただきたいのは、「なお」以下の意味合いである。同意さえあれば、様々な規律の内容が全部底が抜けるという話なのかというと、そうではないであろうということ。同意さえあれば何やってもいいという話では、この制度を安定的・実効的に運営することは、一般的なデータ保護法の考え方から見てもおそらく難しいだろう。
- むしろ、ここに「規格化された内容による同意」と書かれているように、何を通信当事者が同意をすれば、その後、通信情報が利用されてこういうよいことが起きるのだ、あるいは、こういうリスクの低減措置が取られているのだということがしっかりと分かることが大事である。
- その場合には、単に同意した、白紙委任というのではなく、自分が同意したとおりにしっかり運用されるという意味で、この「なお」の前に書いてある、また、その下に書いてある、ある種のガバナンス、例えば独立機関による監督が、結局あったほうがよいのではないか。
- ２点目は、これは全体に関わることであるが、先ほど他の有識者からも御指摘のとおり、様々なプレーヤー間の効果的な連携・協働こそが、このサイバー安全保障の対応能力の向上の肝であるということ。今のところ、それぞれの論点をそれぞれのテーマ別会合で掘ってきたわけであるが、本日、議論の整理から「案」が取れるということで、ぜひ事務局においては、通信情報、フロー情報を「平時」において通信事業者が取得し、政府に提供し、政府が分析し、それの共有、結果を返す、そして「有事」の場合に無害化措置を取るときに、どういうオペレーションが起きてくるのか、その具体的な流れや、そこにおけるプレーヤーの役割、連携とか均衡、抑制を整理していただきたいと思う。
- というのは、この種の議論で概念図を書く、あるいはプロセスをイメージする場合には、国、企業、重要インフラ事業者といったように、一個一個の主体を確立して考えがちであるが、例えば国においても司令塔になる部分、司令塔からあらかじめのきちんとした指示を受けた上で、専門家の部隊が具体的な措置をばしばしとやっていく部分、そして、それを全体としてチェックする第三者機関といった部分に詳細化することが可能。また、企業、例えば重要インフラ事業者においても、平時から情報提供をする部門、経営層のように、それぞれの主体の中の具体的なプレーヤーが、実際のプロセスの中でどのような役割を果たし、どういう連携をして、目詰まりがないようにするかが制度的に重要である。一度それを整理していただいて、具体的に法制化、あるいは制度整備等においてどこに手当する必要があるのかを洗い出していただき、オープンにしていただくことが、有用なのではないか。

○　イの「通信情報の利用」について２つ、それから「アクセス・無害化」について１

つコメントする。

○　「通信情報の利用」について、まず１つ目。資料２－１の11ページの４番「電気通信事業者の協力」というところ。

○　こうした電気通信事業者の協力を得ることは本当に重要。ここで、この電気通信事業者の範囲、定義はどこまでなのか問題となる。つまり、「電気通信事業者」が広い意味で使われているのならいいが、旧来型のキャリアだけでいいのかというと、多分そうではなくて、いわゆるプラットフォーマーと言われているような事業者からもデータを取れるようにするということも非常に重要だと思う。もちろん、GAFAMのようなプラットフォーマーが日本にあるかと言われれば、非常に限定的ではあると思うが、そうした事業者の通信情報の利用を最初から諦める必要はないと思う。

○　例えば、マイクロソフトはアメリカの企業だと我々は思いがちだが、彼らは自分はグローバル企業で、各国政府の規制には従うんだということを言っている。そうしたときに、我々が、そうした事業者とどこまで話し合い、有用なデータを得られるかということは考えておいてもいいのではないか。

○　「通信情報の利用」について２つ目。資料２－１の５番「国民の理解を得るための方策」というところ。これまで私たちの議論は、能動的サイバー防御というのが通信の秘密を侵害してしまうのではないかという、ある種のおそれを抱きながら議論をしてきたと思うが、しかし、もともと考えてみると、犯罪者や外国政府などがサイバー攻撃やサイバースパイ活動を使って我々の通信の秘密を既に侵害しているという状況がたくさんある。その状況を改善するために、この能動的サイバー防御というのをやろうとしているわけであるから、そこの説明の仕方は少し変えるというか、つけ足してもいいのではないかと思う。

○　日本国民の通信の秘密を侵害するようなことが、既に行われている場合、これを止めていくかというために、政府が適切な形で、通信情報を利用し、未然にそうした形の侵害、漏えいといったことを防いでいくという説明の仕方もあり得るのではないか。

○　３点目は、「アクセス・無害化」について。既に事務局からの説明で、未然に、あるいは、平時と有事で境がないということは強調していただいているが、それに対処できる組織の在り方というのは、もう一段深めて議論する機会があるといいのかなと思う。事態認定の前後にこだわって、前はこの組織でやります、後になったらこの組織でやりますと言っている猶予は全然ない。何かが起こる前に、何かを始めようとしたときにできる組織はどのようなものであるべきかということは、私たちはしっかり議論をして、それが警察なのか自衛隊なのか、あるいはもっと違う別の組織なのか、そういったことを議論していくことが必要ではないか。

○　この会議でも「官民連携」という言葉はよく出てくるのだが、ぜひ「官官連携」とい

う言葉も忘れずにどんどん使っていただきたいなと、自分たちがやっていくんだというところを示していただけるとすごくうれしいなと思っている。

○ サイバーセキュリティにおいて、やるべきことを、もしくは、できていないことを挙げるということはできると思うが、欧米と同等、またはそれ以上というのは、そもそも欧米と同等とはどれぐらいかというのをあまり分かっていない部分があるので、そういったところではなく、日本としてこうだとか、何をしていくべきかなど、日本独自のみたいな見せ方のほうが、いいのではないかと思いながら聞いていた。

○ 通信の秘密は基本的には透明化というところがすごくキーになってくるのだと思う。独立機関の監督というものはどのようにするのか、このようにしているから大丈夫ということを、安全の部分だけではなくて、どれだけ、安心を与えられるかということがキーになってくる。国民が、どのように運用されているのかなど知りたいと思うようなことを公開するようにするべきで、年次なのか月次なのかは分からないが、透明性レポート、トランスペアレンシーレポートのようなものを出していく。その中には、どういう仕組みで運用されていて、何を見て、どういう判断をして、どういうアクションをしてどのような効果が出たのか、そういったものをきちんと示せるようなものをしないと、やったけれども何がよかったのか分からないで終わってしまうのではないかなと思っている。

○ 「アクセス・無害化」に関して、これは、対象が国内、国外の可能性は共にある。その場合国内の通信業者が攻撃インフラにされてしまう場合があるだろう。そういった場合に、加害者の片棒を担がされてしまった状態になったときにはどういう備えが自分たちに必要なのか。どんな連絡が来て、どれぐらいのコストがかかるのかというのを示してあげないと、あまり同意を得られないのではないかなと思っている。

○ また、「アクセス・無害化」において、今ある状態で、通信の秘密の扱いを変えた場合、通信業者が協力できるようにするには事前の備えを費用をかけないとできないのか、かけずにもできるのか、そこは結構民間は気にしているところなのではないかなと思っているため可能な限り早期に伝える必要があるだろう。

○ 基本的に、人材に関しては、絵に描いた餅であるとか、幸せの青い鳥のようなものを探す、言い換えれば、優秀で安く使えるような人とか、そんなのは基本的にいなくて、どんどん専業のほうに移っていったり、給料のいいほうに、最悪、海外に行ってしまう可能性があるということを考えつつ、本当に、お金とセットで必要な人材を定義していく必要があるのではないか。

○ その人材とはどういうものですかという話を聞いてみたが、セキュリティだけから始めたセキュリティのみをしている人ではなくて、ネットワークの構築、サーバーの設計・運用、そういったものに関わって、プラスセキュリティをしていくという人材にしていく必要がやはりあるのではないか。

○ それはなぜかというと、セキュリティだけを学んでも、セキュリティ至上主義みたい

な人が生まれてしまって、運用の人たちの気持ちが分からずに、こういうことをすればいいのですよだけでは伝わらない。伝える力を持たない人材がたくさん出てしまうのではないかという意見をいただいた。

○ プラスセキュリティという言葉の逆のことをおっしゃっている人がいて、非常に面白いなと思った。皆さんがいろいろな仕事をしている中にプラスセキュリティを意識していただく、これは非常に大事なことだと思うし、続けるべきだと思う。ただ、この人たちにセキュリティの力をつけることもしつつ、セキュリティのことを学んできた、知識のある方を自分たちの事業に当てはめて仕事をしてもらう。例えば、危機管理部門など、そういうところに入ってもらってやっていくというやり方も意外と現実的なのではないかなと。

○ 映画「アルマゲドン」を観ていると、採掘する能力がある人間に宇宙に行く技術を身につけさせるか、宇宙に行く人間に採掘技術を身につけさせるか、どちらが早いかよく分からないなと思ったことがあるが、サイバーセキュリティにおいてはその両面からやっていくということはできるのではないかと思った。

○ 総じてビジネスの観点を持つセキュリティ人材がやはり少な過ぎるというところで、人材をどうしていくかということに加えて、組織でどのようにその人たちを育てていくか、受け入れていくかということも検討し、求める人材のスキルマップだけではなく、自身の成長した姿が想像でき、動機付けができるキャリアプラン・パスを、示していく必要があるのではないか。

○ 全体についてだが、こうした会議で検討してルール・仕組みをつくっていく、非常に大事なことである。ただ、それだけだと、やはり仏造って魂入れずという形になってしまうと思っているので、運用に加えて、有識者を入れながら進めていこうみたいなことが取りまとめにあったが、検討し続けられるような、分からなかったら専門家・有識者にすぐに聞けるような仕組みづくりも今後考えていただきたいと思っている。

○ 私から３点、重点的にさらに検討を加えていただきたいと思う点をコメントさせていただく。

○ １点目は、官民連携の強化、あるいは今日説明のあった横断的な課題にも含まれている人材育成について、御承知のとおり、今、このサイバー攻撃の分野というのは、日々、常に攻撃が高度化している。これに対応するために、防御する側の最新の技術を駆使していくと。それに対応する人材をつくっていくということが非常に重要だと思う。

○ 例えば、つい最近まで、いかにしてサイバーセキュリティ人材を増やすかということにかなり注力してきているが、今や攻撃する側がAIを利用してきているので、防御する側もAIを使わなくてはいけないということで、最後まで人で守っているところは、もしかしたらセキュリティホールになってしまうかもしれないというような時代に

なってきている。したがって、いかにこういう最新の技術を中長期的に研究開発を進めていくかということも重要で、こういう技術をいかに駆使できるかという人材を育ててつくっていくかということが非常に重要なことかなと思っている。

○ ２つ目は、ソフトウエアの脆弱性対応、ベンダーの責務について、皆さん御承知のとおり、今、ベンダーの製品の中のソフトウエアを見てみると、必ずしもベンダーが作ったソフトウエアではなくて、いわゆる標準パッケージみたいなものが使われていて、それで成り立っているようなものが多くある。最近起きた事例で、皆さん記憶に新しいところだと思うが、１つの標準パッケージに不具合があって大きく社会のシステムがダウンしてしまったという事例があったと思う。したがって、こういうブラックボックス化されたようなソフトウエアに対応するためには、それに対するやり方も非常に複雑で、難しいところではあるが、例えば、サプライチェーンの中で、一つのパッケージだけを利用するのではなくて、場合によって、こういうことが起きたときに、その冗長性を高めるために複数のパッケージを利用して対応していく等、省庁を含めて検討する必要があるかなと思っている。

○ 最後、３つ目「通信の秘密との関係」で、情報処理のプロセスについて、他の方からもコメントをいただいたが、まさに今回、必要な各プロセスにおいて、例えば準備・承認、通信事業者への措置、処理・分析等、このそれぞれのプロセスにおいて、その実施主体というのを明確にしていく必要があると思っている。また、各プロセスの遂行にあたり、実施主体によらずどういうことが例えば法的に必要なのか、あるいは国民の同意を得ることが、こういう点で重要なのか等が変わってくると思うので、それぞれに対応していくということをぜひ考慮していただきたいと思っている。

○ これまで国のレベルでサイバーセキュリティに関してここまで集中的に、非常に多様な議論をしたことはなかったと思っており、そういう意味では、本日報告していただいた内容は、大変重要な内容を網羅しているのではないかと思う。それを前提に申し上げる。

○ まず背景だけをお話する。IT政策は、日本では2000年から始まっており、最初は民主導と言っていた。通信の民営化から始まっているため、民主導という表現を使ってきたと思うが、それが2000年の状況。

○ ところが、実態が民任せになった。そのため、民間に任せてあるから国としてあまり関わらなくてもいいだろうという認識があり、IT環境そのものがそういう形になった。多くの重要インフラも、もちろん民任せとは言わないが、かなり民が主導で進めているということだと思う。

○ そして、今、DXが起こってデジタル社会になり、デジタルアーキテクチャがあらゆる産業の機能の基盤となり、インターネットは隅々まで普及したということを前提にすると、民主導でも民任せでもなく、官民が連携をしてこの問題に取り組む時代となっ

たということだ。まさに、それがサイバーセキュリティの課題だという背景がある。

○ もう一つの背景は、この会議でも申し上げたが、そうしてできたデジタル社会のインフラストラクチャは、先ほどから他の方からも発言が出ていたが、基本的には、昔、通信と言っていたものはパイプである。土管という言い方をするときもあったが、今のインターネット時代は、両端でデータを処理してサービスを作り、そしてコンピュータでAIなどを使って計算をする。こういう時代、その間をつなぐ通信も重要であるが、両端、つまり、利用者とクラウドの中身も重要であり、また、サービスそのものも重要であり、全体がデジタル社会のインフラストラクチャである。したがって、狭義の通信にとらわれず、この全体像を見ながらサイバーセキュリティのことを議論することが重要であり、土管だけが通信だと思って取り組んではいけないということである。

○ さらに、昔はコンピュータであったが、今はGPUという、非常にエネルギーを使うものをどれだけ持っているかでデータの処理の能力が変わる、これがAIの世界である。つまり、電力があるところだからこそ、データを守る、あるいはデータのサービスを持続できるということであるので、通信、データ、コンピュータやデータセンター、クラウド、これに電力を加えたものがデジタルインフラストラクチャとしてサイバーセキュリティの対象になるべきだということを、改めて主張したい。

○ 次に、この問題をこの場で議論をしてきて大変すばらしいと思ったのは、冒頭に述べた官民が連携をしてサイバーセキュリティの体制を作ろうという、言わば覚悟を決める会議でもあるかと思う。どうすれば連携できるのか、今まではどうして連携できなかったのかも全て考えると、やはり、これはお互いの信頼であると思う。民間企業が、あるデータについて相談しに行く相手が国の一部であったときに、信頼してデータを出せますかと。そのデータを使って国がいい仕事をしてくれるので、国を頼りにして安心して事業を進められますかと。こういう信頼を官と民の間で作る、こういう組織を是非作っていただきたい。

○ それを実現するためには、民間側の共通認識が必要である。信頼感と共通認識の形成が必要であるため、いろいろな価値のある議論がこの場であった。ここで議論されている共通認識を社会全体の共通認識にするためには相当な時間が掛かかると思うが、是非、事務局の方は、しっかりと伝わるように、取り組んでいただきたいと思う。

○ 最後に、共通認識の形成には、国際的な信頼感も必要である。国際的な信頼感がないとサイバーセキュリティのグローバルな体制は形成できない。私がこのサイバーセキュリティの会議で必ず言っていたのは、関連省庁の大臣が多く参加する会議もあったが、皆さんに同じ言葉で世界に対して発言をしていただきたいということを繰り返し申し上げてきた。つまり、ポリシーも共通の認識をしているということ、また、世界に対して一つの言葉で対応できる、そのためには、やはりセキュリティの新しい組織ができた際に、その人材の所属が２年で変わってしまうようなことがないように、何

とかいろいろな方法を駆使して、同じ人が世界と話ができる、こういう体制を作っていただきたいと思う。

○ これまで２回の親会議、６回のテーマ別会合の中で論点は漏れなく議論されてきたと考える。これまで申し上げてきた点も含めて論点を３つ案内させていただければと思う。

- １つは、資料２－１の９ページの２番にある通信情報の利用についてである。これは第１回の会議から、どのような通信情報が対象になるのかということが論点であったが、改めて見解を述べると、やはり事務局案にあるとおり、外国が関係する通信、外国・国内、そして外国・外国の通信は利用していく、収集していく必要がある。
- 国民やメディアに勘違いされているかもしれないのは、どういう通信を収集するかという観点である。通信の本質的な中身までは収集する必要がないかもしれないが、それ以外については全て収集、分析していく必要がある。例えば、ペイロードかメタデータかという区分であれば、メタデータだけではなくペイロードの一部についても活用していくことが重要と考え、改めて意見を申し上げたいと思う。
- ２つ目が、無害化措置について、資料２－１の14ページの２番である。やはり優先順位付けが必要ということであり、特に社会のレジリエンスに関わるサイバー攻撃、安全保障の基盤に関わるサイバー攻撃については、優先的に対処、無害化をしていくということが必要かと考える。
- その上で新たな論点を追加するならば、これはサイバー攻撃だけではなく、幅広いサイバー活動、例えば偽情報や影響工作という問題もスコープに入ってくるのではないかと考える。具体的には、外国が特定のサーバーやインフラを用いて、意図的な情報操作を試みている場合、そうしたインフラは無害化措置の対象になるのではないのか。特に、日本国内では、サイバーセキュリティと情報安全保障の問題は別個に議論される傾向にあるが、諸外国の一部では、サイバーセキュリティと情報安全保障の問題を区別せず、一体として対応してくるケースもある。外国勢力によるサイバー空間を通じたディスインフォメーションも無害化措置の対象になるのではないかと考える。
- 最後の３点目について、これも細かい新たな論点になるが、資料２－１の18ページの人材パートである。過去にサイバーセキュリティに関わる人材は、アナリストや技術者だけではなく、経営者やそのほかのコーポレート部門もということであった。特に今回の取組の（イ）と（ウ）の実施という観点では、例えば国際法とサイバーセキュリティ、中国・ロシア・北朝鮮等の地域研究とサイバーセキュリティ、国際関係・外交とサイバーセキュリティ、これら学際的な分野の専門家、

人材の育成も重要である。

○ 官民連携については、重要基幹インフラだけではなく、地方のいろいろな企業にも幅広く参加してもらうのが重要ではないか。そうしないと、どうしてもサーバー攻撃の穴があるため、自分事ではないと思う可能性があるのではないか。
○ 通信情報の活用については、外外はもちろんであるが、外から内に入ってくる通信というのも参照しなければ、本当にサイバー防御の実効性があるのかという疑問がある。中と中の通信についても、あまり対象をはっきりさせてしまうと、そこはある種のサンクチュアリというか、ほかの人たちがここから攻撃してもいいと、国内のサーバーみたいなものをつくる可能性も出てくるということもある。その場合、その対策も並行して進めなければ、なかなか実効性が上がらないのではないか。
○ いわゆる事態認定についても、これは何度も話が出ているが、これをやっていると、実行に移すと非常に対処が遅れるので、この方式は恐らく能動的サイバー防御についてはなじまないと思う。
○ 事態認定方式をとらないとすると国の安全保障とサイバー防御を両立するシステム、国家安全保障とどう関係するか。この概念ないしシステムを政府にはぜひ検討していただきたい。
○ 例えば自衛隊が無害化の措置を取る場合、これは海外での武力行使に当たらないのかといった疑問や批判もあるかもしれない。こうした部分も整理していただきたい。
○ これから政治的なイベントもいろいろ控えており、この問題があまり政治的に利用されるのもよくないのではないか。

○ 今後の検討課題について２点申し上げたい。
○ １点目は、官民連携の組織としては、NISCの後継組織あるいは新しいNISCの下に何らかの官民協議会をつくるということになると思われるが、今後、日本のサイバー安全保障分野での対応能力の向上を図り、かつ、官民が力を合わせるという方向に向かうためには、この官民の協議体をどのように発展、充実させていくかが非常に重要ではないかと思う。あまり前例のない、お手本のない組織活動になると思われるが、先ほど申し上げたように、官民が力を合わせて守るという方向を目指して、そのために有意義な情報共有、意見交換を行って、それを通じてセキュリティ人材の交流が発展する場としても機能していくというような方法が望ましいのではないか。
○ ２点目は、国民の理解を得ていくためには、アクセス・無害化についても重要なポイントになるのではないかという点である。そう申すのは、通信情報の利用に関しては独立機関を設けて、憲法に保障された通信の秘密の適切な保護が担保されるといった体制を構築することは検討されているわけだが、アクセス・無害化は、こう

した独立機関による事前審査、承認によらない現場対応が想定されていると思う。そうすると、法制度としては、警察官職務執行法を参考とした即時強制の制度づくり等が考えられるわけだが、この点に関して、現行の警職法には能動的サイバー防御を全く想定していないということもあり、国民の理解を得ていくための方策がいろいろ必要だろう。具体的には、こうした措置を取る場合に例えば警察であれば警察庁長官への報告をルール化するとか、独立した立場からの監督の仕組みが設けられるとか、あるいは、意図せず、あまり好ましくないような結果になった場合のその報告、判断を誤った場合などの事後報告についても、何らかのルール、制度が設けられると、そういった方向の議論、検討がさらに煮詰められるべきではないかと考えている。

○　この３つのテーマは当然だが独立したものでなく非常に関連が深いと感じた。そして、それぞれについて議論があったが、これを組み合わせて見たときに初めて出る視点とか課題というのもあるかもしれないと感じた。よって、この３つの重要なテーマの検討課題が同時に成立したときに、それが全体として何を意味しているのか、サイバー安全保障に関する我が国の対応の在り方として、全体としてどのようなものをつくろうとしているのかというのを、改めて全体像を振り返るということも必要だと感じた。

○　もう一つは、逆なのだが、今回まとめられた議論は、時間も限られていた中で、具体的なところまで踏み込んでない部分が多いとは思う。概論としてはこの内容は優れたものと思っているが、実際のところは、やはりディテールまで見て、初めて是非というのが分かる部分というのもあると思う。今後そういった議論がされると思うが、より具体的な内容についても理解したいと思っており、そのような機会がいただけるとありがたい。

○ 完璧を目指さなくても良いのではないかという視点でお話をさせていただければと思う。どうしても日本の法制度は、つい完璧を目指しがちなところがあるが、基本的にサイバーの分野は変化が激しいので、完璧を目指してうまくいかないところがあり、まずはできるところから始めてみるという考えでも良いのではないかと思う。その上で、有識者等の不断の随時的な検討を組み合わせることで修正をしていくという形でもいいのではないかと思う。

○ その意味で、重点的な対策としては、あまり議論のないところから始めるのもありだと思っており、通信の分野で言えば、先ほどの議論や事務局の取りまとめにもある外国との通信、外国が絡む通信を対象とすることについて争いはないし、説明もつく。なぜならば、日本の国外については日本の国家権力が及ばないから情報収集をするしかないという説明が可能であるので、まずそこから始めるということで良いと思

っている。

○ もう一点言うと、独立機関の話が非常によく出ているので、独立機関について早めに検討をすることが重要だと思う。独立機関は、通信の関係やアクセス無害化についても議論に出ている話なので、この意味で、具体的にどのようなシステムが必要なのかというのを検討していただくのが良いかと思う。

○ 感想を１点と、今後の議論について２点、お話させていただく。

○ これまでの会議に参加させていただいた感想は、他の有識者も話していたとおり、全ての会合の議論が、相互に関連し、共通の問題意識に基づいたものであったということである。とくに感じたのは、今回の一連の議論が、サイバー空間において必要な手立てや措置は何かということについて、具体的に論じる場となっていたと振り返っている。これまでの会議において印象的であったのは、このような会議体においてありがちな、まず組織論、とにかく司令塔を作るべしといった議論に終始するのではなく、まず、具体的な作用法の領域に係る議論、すなわち、共有すべき情報の内容や各主体の連携のあり方、無害化措置の内容やそのイメージについて議論することができたのではないかと考えている。

○ 本日の取りまとめに異存は全くない。これを早く公開していただき、さまざまな関係者の方の御意見を、広くいただくというプロセスが重要になってくると考えている。

○ 今後の会議の方向性について、期待することを２点述べさせていただきたい。

- １点目は、運用を意識した制度設計について。
- 当然ながら今後法制度を考えていくことになると思うが、情報の収集や共有、監督機関の監督権限の行使、それから、実働部隊の無害化措置について、法律を考えていく際には、いわゆるハードロー、制定法はもちろんだが、ソフトロー、例えば内部基準、ガイドライン、場合によっては関連の業界において必要となる業界基準のモデルの立て方なども含めて、ソフトローについても考慮に入れて検討を進めていただきたい。法律をつくったからそれで制度づくりは終わりということではないということである。
- ２点目は組織について。
- これまでかなり作用法の話が進んできたので、ここからが、具体的な組織法の議論をする段階と考えている。組織の規模、体制、置き方、人材の配置、権限、権限行使の手続等の組織法の話を具体的に展開していくことが必要と考える。
- この点に関して、これまでの議論を踏まえると、２つの組織の話をしなければならないことは明らかである。１つは、強い執行力と統率力を有する司令塔、かつ、実働もできる組織。それから、もう一つは、平時から緊急時を通じてサイバー空間及びそこで行われるサイバー領域における様々な措置を監視・監督する独立機

関たる第三者機関としての組織である。今後、これらの２つの組織に関する議論について、国家行政組織法などの組織法、それから、既存の組織の整理、調整、執行機関の持ち方も含めて、組織、組織法の話をぜひ具体的に進めていただきたい。

○ 資料２－１の18ページ目の「５．中小企業を含めた対策強化」に関連して、サイバーリスクは自然災害に近い深刻度ゆえに、自助・共助・公助の観点から、自助には限界があり、そのために共助・公助をどう考えるかというところで、まさにこの５．にあるような論点が整理できたのは大きな前進である。もっとも、自助に限界があるとはいえ、まだ自助にも伸びしろがあるように思う。
○ 共助･公助が強化されることで､かえって自助努力が減ることは避けるべきであり、個別の企業においてもサイバーセキュリティへの取り組みを強化する必要がある。その観点から、成果物の中で、「サイバーセキュリティは経営層の法的義務」であるというところを、しっかり明記することは一案ではないかと思う。
○ 重要インフラに関しては2022年６月17日サイバーセキュリティ戦略本部「重要インフラのサイバーセキュリティに係る行動計画」において既に記載されているが、こちらは重要インフラなので、一般民間企業は関係ないと思われがちである。重要インフラ以外の企業においてもサイバーセキュリティが取締役の法的義務であることを明記することで、経営層によるサイバーセキュリティへの投資及び取り組みを促すことを期待できるのでは。

○ デザインが経営課題だったという話がよく出てくるが、セキュリティが経営課題だということが経営上非常に重要だと思う。その上で、どこをセキュアにするのかの議論が、一般的な会社経営や、委員会の運営などで出てくるようにするには、実際、どういうワークフローが起こるのかというイメージが必要で、例えばセキュアのシステムを考えるときに、ここは証明書を出すとか、ここはどういった攻撃があるのかとか、そういった議題が経営課題としてより議論されるべきである。重要な契約を見るときは、取締役会でこれを見ると思うのだが、そうではなくて、重要なインフラを見るときに、サイバーセキュリティの議論ができるボードメンバーを会社組織の中で､取締役会で揃えることが､今後､社会においてすごく重要になってくる。
○ 例えばAWSのパッケージが新しくなったからここはどうするのだとか､ここはジェイルブレークするからリバースエンジニアリングが可能だとか、個人情報を誤って学習に使ってしまっているとか､いろいろなハードからウェブのAPIまで全然違った論点が出てくるが、そういったことを俯瞰できる人材を経営層に持ってこれるのかということ、社会としてどう取ってくるかということなのだと思う。そういう層を育てるのには結構時間がかかってしまうので、おそらくチームの中にスポットでフレ

キシブルに、例えばクロスアポイントメントで人が入るとか、未踏IT人材発掘・育成のようなところから人材があっせんされるのか、そういったような人材をスポットで、分からないところを聞いていくような組織体制を霞が関で構築していかないといけないのだと思う。

○ そういったものが、実際どういうフローで決まっていくのか、やっていくのかというイメージの共有をするための、ある程度のワークフローや考え方の図というのが、次の議論の方針では出てくるといいなと思う。

○ 今まで大事だとずっと伝えてきたところは資料２－１の横断的課題の中にあると思う。この資料の17、18ページにある、物理的な組織を持つことや、人材の長期化について、これは他の有識者も発言していたが、世界に向けて同じ声で、同じ人と話をするとき、これは民間でも世界でも同じだと思うが、また一から話さなくてはいけないというのが今までの常だったので、それは避けられたら良いと切に思っている。

○ １点加えるとすれば、人材育成について、ここに反映されていないものとして、政府の姿勢がある。人材育成というのは、これまでも政府諸機関が実施しており、IPA、経済産業省、総務省、防衛省、その他もそれぞれ実施していると思う。NPOも実施しているし警察も実施している。このようにばらばらに実施していることを政府の中央組織、中央政府が把握していないということが重要な問題で、中央が把握して、施策が似ていることから相乗効果を狙うべき点、欠けているので補うべき点を見てとれ、そしてサイバーセキュリティを学びたい/学ばせたい人たちも、１か所を見れば何があるか分かっているという状況に持っていけたら良いのではないかと強く思っている。

○ 人材については、本当にいろいろな人がいろいろな意見を言うと思うので、優先度というのはそれぞれあると思うが、ここに書いてあるとおりだと思う。今もやっているとおり人材の定義づけ、資格による可視化等を通じてやっていくというのはこれからも変わらないと思う。政府がサイバーセキュリティの人材育成に具体的に取り組む姿勢を出すというところは、ぜひお願いしたい。

○ 今、一番言われているのは、警察の中でも、OSINTの人材が必要ということで、警察も全然サイバーとは関係ない人、例えば交通や経理からも人を持ってきてサイバー人材に育てなくてはいけないと伺っている。そういうことも全国的に実施していかなくてはいけないとも思っており、それは粛々とやっていこうと思っているが、まず政府が人材を育てたいというメッセージを強く伝えていくことが最も重要なことの一つだと思う。

○ 国際協力の観点を決して失ってはならない。サイバーセキュリティの分野における

オペレーショナルなレベルでの国際協力だけではなくて、組織としてどのように対処していくかという点がやはり重要ではないだろうか。それは、相手国のカウンターパートがどれだけ日本に信頼を寄せるかという点と密接に関わっているということでもある。

○ したがって、どのように組織を再編していくかということは、これからの議論を深めていくところだろうと思うが、決して内向きな議論だけではなく、また、省庁間の調整などに限るのではなくて、むしろ開かれた形での議論の発信ができるような、そして、強力なリーダーシップを取れるような組織を構築していくべきではないだろうか。

（４） 河野国務大臣挨拶

○ 今日も本当に活発な御議論をいただきましてありがとうございました。最後は時間が足りず大変申し訳ございません。

○ これまでの議論の整理を土台として早い時期にしっかりと取りまとめをお願いしたいと思いますので、取りまとめに向けて精力的な御検討を引き続きお願いしたいと思っております。最後の直線に入ってくるような段階でございますので、どうぞよろしくお願いいたします。

以上