

「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2回）議事要旨

1. 日時

令和6年7月8日（月）18時から19時までの間

2. 場所

中央合同庁舎第4号館 共用第4特別会議室

3. 出席者

（委員）

上沼 紫野	LM 虎ノ門南法律事務所弁護士
遠藤 信博	日本電気株式会社特別顧問
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 一般社団法人 電気通信事業者協会参与 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
石川 昭政	副大臣
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
木村 公彦	内閣官房サイバー安全保障体制整備準備室長代理
佐野 朋毅	内閣官房サイバー安全保障体制整備準備室次長
中溝 和孝	内閣官房サイバー安全保障体制整備準備室次長
門松 貴	内閣官房サイバー安全保障体制整備準備室次長
飯島 秀俊	内閣官房サイバー安全保障体制整備準備室次長
室田 幸靖	内閣審議官
関口 祐司	内閣審議官

4. 議事概要

(1) 河野国務大臣挨拶

- 委員の皆様には、お忙しい中、お集まりをいただきまして、誠にありがとうございます。今、座長からお話がありましたように、3つのテーマ別の会合を、それぞれ活発に御議論いただきまして、私も大変興味深く拝聴させていただきました。ありがとうございます。その資料を、今日は全員お集まりの場ですので、共有させていただこうと思います。
- また、3団体の皆様、今日はお忙しい中、御出席をいただきまして、本当にありがとうございます。日本のサイバー安全保障の対応能力の向上をどう実現していくかを検討していく中で、産業界・経済界のお立場から政府に求める役割あるいは制度が、どのようなものが望ましいかという皆様のお考えを、今日、積極的に伺いをし、また、忌憚のない御議論をお願いしたいと思っております。
- 総理から、なるべく早く取りまとめをとということもございますので、引き続き、国民の権利利益をいかに保護を図りながら、我が国の経済社会をサイバー攻撃から守っていくか、この体制の実現に向けて、活発な御議論をお願いしたいと思います。どうぞよろしくお願いいたします。

(2) 関係団体からの説明

関係団体として、

和田 昭弘 一般社団法人 日本経済団体連合会 サイバーセキュリティ強化WG 主査

伊藤 穰一 公益社団法人 経済同友会 企業のDX推進委員会 委員長

岩本 敏男 日本商工会議所 デジタル化推進専門委員会 委員長

の3名からヒアリングを行い、それぞれ資料1から資料3に基づいて説明があった。

ア 一般社団法人 日本経済団体連合会（和田氏）

- 経団連で取りまとめた意見を、要点のみ簡潔に説明したい。詳細については、後ほど資料を御確認いただければと思う。経団連ではサイバーセキュリティは国家安全保障に関わる最重要領域の一つと認識し、「実効あるサイバーセキュリティ対策を講じることは、今や全ての企業にとって、経営のトッププライオリティ」と謳っている。安心・安全なサイバー空間の構築に向けて、「経団連サイバーセキュリティ経営宣言2.0」等を通じて、全員参加型の対策を推進してまいりたい。
- こうした観点から、本有識者会議で取り上げられている7つの論点について、以下のとおり意見を述べたい。
- 第1に、官民連携の枠組みの構築である。官民連携による情報共有は、民間事業者の過度な負担を回避するとともに、片務的ではなく官民双方向なものとするべきである。また、政府の役割を明確化し、インテリジェンス活動やインシデント発生時のアトリビューションは、政府が責任を持って実行すべきと考えている。
- 経団連は、本年1月に派遣した日英サイバー協力ミッションで、英国政府通信本部（GCHQ）のもと主導的な役割を担うNCSCの取組み等を聴取してきた。とりわけ英国のActive Cyber Defenceでは、公共機関が国民向けに多様なサービスは無償提供しているのが特徴である。我が国も現行法制度下で実施可能な政策は躊躇なく取り入れるべきである。例えば「industry100」のような官民人材交流に係る枠組みも参考になろう。
- 第2に、官から民への情報共有の在り方についてである。情報共有の際には、NCSCのCiSP等も参考にしつつ、政府側で情報の重要性を精査し、必要な情報共有先に柔軟に共有することが欠かせない。
- とりわけ、機微情報を民間と共有する上では、コンフィデンシャル級の情報を対象とする重要経済安保情報保護・活用法及びトップシークレット/シークレット級の情報を対象とする特定秘密保護法をシームレスに運用すべきと考えている。
- 第3に、民から官への情報の共有の在り方についてである。現状、事業者は既に複数の政府機関にインシデント報告を実施している。今後、過度な報告義務が課せられることになれば、事業者のインシデント対応能力を毀損しかねない。我が国のサイバーレジリエンスを高める観点からは、報告の簡素化や窓口の一元化など、持続可能かつ実効的な制度設計が必須である。また、事業者から提供される情報は、センシティブ情報として慎重に取り扱うべきである。以上を踏まえ、制度設計に当たっては、経済界、事業者と双方向かつ丁寧なコミュニケーションをお願いしたい。
- 第4に、サプライチェーンに関してである。総合的な国力という観点からは、サプライチェーン全体を俯瞰したレジリエンス強化に向けて、実効的な仕組みを構築することが必要である。その際、実行に必要な費用、人材、技術面での支援等も検討すべきである。また、業界横断で継続的に議論する場を確保し、政府関係部局とともに、双方向で連携可能なプラットフォームを構築していただくよう要望したい。一例として、既存のSC3が有効ではないかと考えている。さらに、企業間での連携や中小企業対策の

観点から、下請法や独占禁止法等の関係や利益供与等についても明確な整理が必要と考えている。いずれにせよ、中小企業の対策状況に鑑み、国による一層の支援が不可欠である。

- 第5に、人材育成・確保についてである。我が国がサイバーレジリエンスを強化する上で人材が要であることはあえて申すまでもない。政府には省庁間や省内の縦割りを排し、中長期的なグランドデザインを描き、横串を刺した取組みをお願いしたい。また、女性のサイバー人材の育成はもとより、地方における人材育成・確保の観点も踏まえ、業界横断的かつ中小企業を含むサプライチェーン全体での演習・訓練等の取組みを強力に推進する必要がある。
- 第6に、通信情報の活用に関する制度設計である。通信を介した攻撃状況のモニターに関しては、事業者の法的安定性を損なわないように、事業者の解釈に委ねることなく、法律での明文化と丁寧なルールづくりが必要不可欠である。あわせて、法制度の運用開始に先立ち、事業者に十分な準備期間を設けていただくようお願いしたい。
- 最後に、諸外国との連携強化についてである。安心・安全なサイバー空間の構築のためには、トラストに立脚した相互運用が不可欠である。この点、SBOMやセキュアバイデザイン・セキュアバイデフォルトを引き続き推進しながら、トラストの輪をグローバルサウスにも拡大することが肝要である。

イ 公益社団法人 経済同友会（伊藤氏）

- 世界中でAIが騒がれる一方で、我々「企業のDX推進委員会」では、サイバーセキュリティが重要だということで、多くの時間をかけて議論をしている。様々な論点が出てきているが、今回は、本会議の論点を絞り、経済同友会として意見を提示したいと思う。
- 現状認識として大きく柱は2つある。1つはロシア・ウクライナ侵攻において武力攻撃の前にサイバー攻撃が使われたとともに、当会の経営者に話を聞くと、中国や北朝鮮が日本企業を攻撃して、暗号通貨等を窃取している事実があることである。やはりサイバー攻撃は一段と巧妙化、高度化、複雑化、組織化されていることが顕在化しているというのが我々の理解である。
- 2つ目は、DXを中心とした経済の活性化を、日本企業全体として進める必要があるが、ここでサイバーセキュリティがきちんとできないと、DX推進が阻害されることになることだ。完全にアナログな中小企業もDXに取り組むとサイバー攻撃という新しいリスクが出てくる。サイバーセキュリティをきちんとやらないと、DXの社会的かつ経済的インパクトを享受することができない。
- そういう意味では国も民間も、サイバーセキュリティを強化しようといういいタイミングである。私自身も何十年前から経営者はもっとサイバーセキュリティを考えなくてはいけないということで様々な取組をしてきたが、今回は本気でやらないと間に合

わない。この危機感を全ての人に「Cyber Security Everywhere」時代であるとして認識してもらう必要がある。まず、今回議論されている能動的サイバー防御は我々も絶対に重要だと考えており、早期に導入すべきである。そして、NISCが発展的に改組して、創設する新組織には大変期待もしている。海外でも米国、英国、豪州を見ていると、国が主導権を持ち、施策を進めている。

- 今までNISCは、とても重要な役割を持っていたのだが、どちらかというと調整のような役割が多かった。海外ではNISCのような組織が、サイバーセキュリティ施策や技術開発に予算をつけるとともに、官民連携でもミーティングやワークショップを行い、リーダーシップを取っている。NISCも同じようにこうした役割を果たすべきである。そのうえで、支える3つのテーマとして、官民連携、人材育成、サイバーセキュリティ産業の振興を詳細に述べたい。
- 1つ目は、官民連携について。まずは重要インフラ事業者に対するインシデント報告義務化を導入すべきである。米国や欧州で、侵害が起きたときの報告義務が法律で定められているように、日本においても義務化する必要がある。特に重要インフラ事業者は、経済も含めて社会にとっての重要な基盤である。しかし企業側は、企業の情報が外に出てしまうと企業価値が下がるなど、経営者や株主も含めてレピュテーションリスクに対する懸念がある。この点は結構慎重に検討すべきである。
- 様々な国や企業の関係者から情報を収集する場合、報告することで情報提供者にどのようなメリットがあるかがとても重要である。報告した内容が外に漏れるリスクがある上、国からのフィードバックがないというのであれば報告義務のメリットがない。報告によって国がきちんと情報提供、助言、支援するとともに、その情報を集約して国全体のセキュリティを強化するのであれば、報告義務のリスクとメリットのバランスが釣り合うという話になる。この意味で、法律を策定しながら、官民が連携し、Give and take の枠組みを作ることが大切である。そうした状況が予見できれば、民間企業のほうも、より協力体制が強化されるのではないか。官民の枠組みでは諸外国にすでに事例がある。米国サイバーセキュリティ・インフラセキュリティ庁（CISA）によって設立された共同サイバー防衛連携（JCDC）やオーストラリア信号局（ASD）によって設立されたサイバー脅威情報共有（CTIS）がある。ともに導入に向けて定期的な会合やワークショップを開催し、参加組織間の情報交換や意見交換を促進し、信頼関係の構築を図るなど組織を作るだけでなく、ソフト面も工夫している。
- 2つ目は人材育成である。我々やその他の経済団体のアンケートでも必ず人材不足という話がでてくるが、国は人材育成するプログラムをたくさん実施している。そこで重要なのは、同じサイバーセキュリティ人材といっても、様々なスキルや役割があることを認識することだ。一般の高校生のリテラシーを上げるところから、プロの人材をつくるまで、あとは、研究者が必要なのかも考える必要がある。ここでは、必要な人材の定義を可視化することが重要だ。米国ではNICEサイバーセキュリティ労働力フ

フレームワーク（NIST. SP.800-181）にて業務、知識、技術を定義している。さらに National Centers of Academic Excellence in Cybersecurity (NCAE-C)プログラムにて米国教育機関のサイバーセキュリティに関する学位認証を行っている。欧州は欧州サイバーセキュリティ技能フレームワーク（ECSF）によりサイバーセキュリティの役割、能力、スキル、知識に関する共通理解、スキル認知促進を実施。また Cyber HEADにて EU 及び EFTA 諸国におけるサイバーセキュリティ高等教育データベースを行い、web 上で大学の見える化もしている。

- 両国とも人材を定義するとともに教育機関と連携していることが特徴である。
- さらに言えば、ヨーロッパの学校では中学校ぐらいから、かなりサポートをしている。このように、サイバーセキュリティ専門家になりたい、その分野の学位もきちんとある、また、そのような最終的な出口もきちんとあることはとても重要である。
- 日本にはサイバーセキュリティの学科を持つ大学はほとんどない。大学も、様々な理由で改革を行うのは難しいが、人材はそもそも足りないので、高校や中学校も含めて同時並行で支援していく必要があると思う。
- 最後になるが、サイバーセキュリティ産業の強化について、ベンチャー企業支援や政府調達の方法、さらに言えば法整備も含めてきちんとやるべき。サイバーセキュリティでは、デュアルユースの安全保障と民間の経済安全保障は技術が重なっていて、このような研究開発は一企業の努力では単独では難しい。ぜひ国や新しい組織に期待したいと考えている。

ウ 日本商工会議所（岩本氏）

- 私からは、中小企業のサイバーセキュリティの現状と、これから何をしたらいいかという要望をお話しさせていただく。
- 最初に、サイバーセキュリティもそうだが、1 ページ目、中小企業は、実はデジタル化の現状は、まだまだ深刻なものがある。もちろん人手不足の問題もあるが、デジタル化が未着手と言われている中小企業も、まだ 3 割程度、このページで見ていただくと分かるが、赤いところ、右端のところの 3 割ぐらい、デジタル化そのものができていないということもあり、我々日本商工会議所としては、セキュリティはもちろん重要だが、それ以前にデジタル化をどう進めるかというのも重要な課題と認識している。
- 次の 2 ページ目に、中小企業のサイバーセキュリティの現状が示されている。東京商工会議所で調査したものだが、ほとんどの企業、86%以上は、自分たちは何らかの対策はしているという認識を持っている。さすがにこれだけ報道されているし、サイバーセキュリティ対策が必要なのは、みんな分かっているが、ただ中身を少し見てみると、いわゆる「ウイルス対策ソフトを入れているよ」とか、「ソフトウェアを定期的にアップデートしているよ」というレベルの基本的なレベルにとどまっていて、本当の意味の専門的な教育も含めてあるいは訓練も含めて、というのは 3 割以下と、進ん

でないというのが実態である。

- 次に3ページ目。やはりそれが進まない1つの理由は、各団体からもあったが、人材不足の問題というのがある。デジタル人材そのものも十分確保できているという企業は、ほとんどおらず、あまり確保できていないとか、全く確保できていないという企業を合わせると6割ぐらいが、そういう状態になっており、セキュリティ人材の確保は一層深刻な状況というのは言うまでもない。
- また、情報システム担当者の設置というのは半分ぐらいの企業が兼任で、担当者がいないという企業も25%ぐらいはある。規模の小さい企業では、半分ぐらい、48.2%とより深刻な状況になっており、中小企業においては自分自身の業務の他、兼務でセキュリティを担う、プラスセキュリティの人材育成というのが、重要と考えている。
- 次に4ページ目。まさにサプライチェーンで狙われる中小企業ということで、どうしても中小企業は、サイバーセキュリティ対策が弱いということで狙われてしまう。日本商工会議所の委員会でも、大手企業のサプライチェーンを担う中小企業の委員、その会社の社長さんだが、深刻な生々しい話もヒアリングをしている。このところランサムウェアの被害件数等が非常に伸びてきているということは、大きな問題である。ランサムウェア攻撃の被害の6割ぐらいは中小企業というデータもあり、対策が必須というのは言うまでもない。
- 次の5ページ目に、要望事項を示している。今後どんなことを国と連携しながらやる必要があるかということだが、まず、1つ目は、中小企業の対応強化に向けた政府の支援ということである。サプライチェーンの中で、どうしても脆弱なセキュリティ体制の部分がやられるので、中小企業のサイバーセキュリティ対策が重要なことは私が言うまでもない。先ほど申し上げたように多くの中小企業では、対策が基本的な状況であり、より支援を強化していただく必要がある。
- 今回も議論されている経済安全保障上の基幹インフラの維持は極めて重要だが、重要インフラのサプライチェーンを担う中小企業は特定されていると思うので、対象を絞って個々の企業のポテンシャルに合わせた実効的な支援、配慮が効果的かと思う。なお、中小企業には過度な負担とならないような制度設計が望まれる。
- 2つ目は、中小企業の事業継続に向けた官民連携というポイントである。多くの中小企業は、能力、リソースが不足しており、何かインシデントが発生しても、中小企業単独だけで原因を解決して、その対応策を打つということが困難である。日々、中小企業のセキュリティ対策をサポートするベンダーなど、そういった組織の支援も必要と考えている。政府から昨今のサイバーセキュリティに関する動向や対策事例など、情報発信を強化していただいて、官民連携のもとで、中小企業の事業継続という形で支援していただければと思っている。
- 3つ目はサイバーセキュリティの人材育成の確保についてである。これは、もう今までも話が出ているとおりであり、中小企業の場合は、専担ではない兼務という、そう

いうことを前提にせざるを得ず、その専門人材の育成と併せて「プラスセキュリティ人材」という、こういった概念での育成を進めていただければと思う。

- 最後の4つ目は、政府からの情報提供の強化についてである。個々の政策だけではなく、サイバー安全保障に関わる背景とか、経済安全保障推進法や国家安全保障戦略との関係性、現在の取組状況などを踏まえて、分かりやすく丁寧な説明を実施していただければと思う。特に、関係する企業及び対応を促したい団体等へは、プッシュ型での周知を政府から実施していただければと思う。

(3) 質疑応答

座長から、関係団体による説明について、各委員に対して質問や意見を求めた。主な発言は以下のとおり。

- 2点質問したい。1点目は、人材の件。お三方とも人材は大変不足していると仰ったが、いつもこの話題は出てくる。それだけ足りないのならば、優秀なセキュリティ人材に、例えば、倍の給与を支払ったらどうかと思う。私の知っている限り、やはりサイバーセキュリティをやっているからいい給与がもらえているということがないので、ほかの仕事に移ってしまう経験がこれまでもあるが、何かここにボトルネックや、何かブレーキをかけている要素を、官民の連携で、解決できることはあるか、これが1点目の質問。
- 2点目、日本経済団体連合会に伺いたい。クリティカル・インフラストラクチャーのサイバーセキュリティに関するいろいろな相互関係や連携について。インフラストラクチャーは、デジタルインフラストラクチャーによって、皆つながっている状況にある。つまり、官が調整をすると、先ほど窓口の一本化が必要という話があったが、民のインフラストラクチャー事業者同士で、サイバーセキュリティの課題に取り組んでいるようなこと、あるいは取り組む計画などはあるか。
- 今の論点について、まず、人材不足についての給料の話があった。もう一つは、インフラの窓口で、官は一体化するとして、民はどうなのだという話だったと思う。

日本経済団体連合会（和田氏）より回答

- まず、人材育成に関してであるが、サイバーセキュリティは、全員で取り組むべきものということが、まず根底にあるのではないか。企業においては「特化したサイバースキルを持つ人材がひとりいればよい」というわけではない。例えば、発注伝票・受注伝票がランサムウェア攻撃を受けた場合に、事業が止まる可能性がある状態であれば、プラスセキュリティ人材を育成するための教育は必須ではないかと思う。給料を3倍に上げるべき人材は特化したスキルを持つ人材だと思うが、各企業に数名ずつ必要かといえ、特にユーザー企業においては、そうした人材が常に活躍できる場があるわけではない。その人材を雇い続けることは、大企業であっても非常に厳しいので

はないか。

- クリティカル・インフラストラクチャーの団体についてであるが、1つは先ほど申し上げた、SC3（サプライチェーン・サイバーセキュリティ・コンソーシアム）である。これは、各企業団体が集まってサプライチェーン全体でのサイバーセキュリティの強化に向けた取組みを推進している団体である。
- このほか、2015年に発足した「産業横断サイバーセキュリティ検討会」では重要インフラ企業も参画し、経営層を巻き込んだ情報交換や人材育成等の活動を行っている。
- チャタムハウスルールのもと、民間事業者間では情報交換は進んでいる。一方、各企業でインシデントが発生した場合、政府への報告が義務付けられているが、報告した情報がどのように使われているのか、企業にとって何かしらメリットがあるのか、といったところが不透明である。今後の官民連携・情報共有にあたっては、こうした観点も踏まえていただけるとありがたい。

経済同友会（伊藤氏）より回答

- セキュリティ分野では多くの企業でROI議論がある。企業でも被害が見える化されておらず、ROIの中で考えると投資ができておらず、結果的に人材も獲得できていないという状況がある。
- 取組みを強化している大企業の場合は社外取締役にサイバーセキュリティの専門家を入れる事例もある。社内人材をより活性化するためには海外人材を活用することも検討するべきである。

日本商工会議所（岩本氏）より回答

- 御存じのとおり、中小企業といってもかなり幅があり、一概には言えないが、給与を上げるというのは、ほとんど現実的ではないと思う。ただ、先ほど申し上げたように、中小企業はデジタル化も進んでおらず、デジタル化を進めている企業は、トップが意識的に取り組んでおり、実際のビジネスをしながら、どんどん進めている。サイバーセキュリティも同じことだと思う。
- サプライチェーンで考えると、非常に重要な中小企業の場合は、中小企業自らが何かやるわけではなく、大手の企業のサプライチェーンとして受けているケースが多い。サプライチェーンを考える中で、重要な中小企業はかなり特定できると思うので、発注が上がってくるときに、このサイバーセキュリティは、ここのレベルまでやってほしいとなれば、その部分を嵩上げしてもらうことが、必然的に中小企業のサイバーセキュリティ対策に回ってくると思う。
- 経団連の方から出されていた資料の4ページで、日英サイバー協力ミッションで得られた知見というところで、私もこういった話を伺った。
- その中で、最後の官民人材交流に関する枠組みは、人材交流というより、官と民の知見と技術をとともに使ってこの国を守るというニュアンス。人材交流だけ、情報共有だ

けではなくて一緒に守るというニュアンスであることは強調させていただきたいと思う。現状もNISCの中に民間の方はいるが、NISCのお仕事をしている人という役割なので、もっとタスクフォースというか、技術者、専門集団がそこにいるというイメージである。

- 続いて6ページの情報共有の在り方のところについて、ここに加えるとすれば、運用後の定期的な民間からのフィードバックの仕組みであろう。共有した情報が有益だったか、無益だったか等を必ず反映させる仕組みがあればよいと思う。
- 8ページの3つ目の項目で、民から官への情報共有に際しては、考え方の整理とともに、日本はコンフィデンシャルな情報の扱い方に慣れていないので、ルールだけではなくてトレーニングも必要なのかなと思う。恐らく、米国とか英国ではやっていらっしゃるのではないかと推測する。
- 続けて、経済同友会の説明について。1つ目の官民連携強化のところについては、新たな司令塔組織であるNISCを中心にすることは大賛成。合意が取れているところと思う。
- 他方、その下に官民連携の組織創設を求めるとあるが、ここは新たに官民連携の組織創設を求めるのか、あるいは新たな司令塔組織であるNISCを中心に官民連携の機能を持つグループを求めるのか。自分としては、新たに別の組織が導入されることはあまり期待しておらず、1つの組織で完結したいなと思っている。

経済同友会（伊藤氏）より回答

- 視点は異なるが、セキュリティクリアランス制度は重要である。経済同友会でも2月にセキュリティクリアランス法制に関する意見を出した。いま、委員が述べたとおり、機密情報のトレーニングを民間も含めて行うとともに、理想は1つの組織で全部できたらいいと思う。ただし、1つの組織が実施することにした場合、例えばそのルールが厳し過ぎて、民間企業が運用しにくくなってしまうリスクも考えられる。またルールを柔軟にしすぎると安全保障などは運用しにくいと思う。そういう意味では1つの組織でできるかどうか、できるだけたくさんの人たちが関わって、多面的に議論すべきであり、実務的に設計していただけると有難い。
- 非常に秘密度の高いものと、中ぐらいと、そうでないものと、恐らくどこの国でも扱いが違っていると思うため、その連続性をどうしてやるのかというのは、工夫が必要な問題ではないかと思う。これは政府のほうでも考えることかもしれない。
- 2点お伺いさせていただきたい。
- 1点目は、いずれの皆様からも、政府の情報発信、提供に非常に多く期待をされている、それが必要であるという発言があった。全くそのとおりであると思う。問題は、そこでどのような情報の提供あるいは情報提供の在り方をイメージされているのか。
- 例えば、日本経済団体連合会の資料の5ページには、精査された情報という表現があ

る。他方、精査をしていると、政府の側でタイミングが遅れることもあろうかと思う。また、中小企業においては、それほど細かい情報というよりも、ざっくり、今、こういう状況だということを教えてほしいといった希望もあるかと思う。

- そして、それぞれいろいろな希望があると思うが、同時に、それらの希望にきちんと対応しようとする、今度は政府の側にコミュニケーションセンターのようなものを設けて、うまく分けていかなければいけないといったことも必要かと思う。例えば、どういうタイミングで、どういう方法で、どの程度の情報をどのように発信してもらいたい、提供してもらいたいという希望が、具体的に幾つか出そろってくると良いのではないか。もし、この場であれば、伺いたい。これが1点である。
- 2点目は、重要インフラに関するサプライチェーンにおけるサイバーセキュリティの実現について、日本経済団体連合会の資料でいうと9ページの(3)、また、日本商工会議所からは5ページで御指摘があったことについて、端的に伺いたい。
- 重要インフラに係るサプライチェーンを守っていくという観点から見たときに、ありていに述べれば、日本経済団体連合会に加盟しているような大企業があり、また、その大企業と取引のある中小企業があるという状況をプロトタイプとして考えたときに、ある程度体制が整っている大企業のほうで、サプライチェーンで取引のある中小企業のサイバーセキュリティまで、ある意味でいろいろな形で見えていく、そして、そのことが、競争法上問題ないという整理をしてほしいとか、あるいは中小企業のほうで、そういうこともある程度受け入れることができるとか、あるいはそれは問題があるといったことが具体的に問題になろうかと思うので、もしお考えがあれば、お聞かせいただきたい。

日本商工会議所（岩本氏）より回答

- 2つ大きく分けて考える必要があると思う。2つの質問にまとめてお答えできると思うが、政府から情報発信するといっても、いわゆる安全保障に関わるもので、具体的にサイバーセキュリティにこういうことがありますよということは、一種の啓蒙的な要素があるので、これは一般的な話として、いろいろな機会をとらえて出していただければいいと思うし、今もそれなりに提供頂いていると思う。
- 2つ目は、例えば大企業から中小企業に1つのサプライチェーンがあって、それが重要インフラに関わっているようなものだとすると、もちろんNISCなどは、いろいろなアタックの情報は出してくれるし、それは有効である。仮に政府サイドが何らかのアタック情報を入手したときに、中小企業においても、具体的にこういう部分についてチェックすべきだとか、あるいは単純に、自分たちの持っているプログラムのリストを全部、ディレクトリを洗う必要があるかなど示唆することができる。そして潜伏しているウイルスをハンティングすることもできるわけだ。そういう情報は中小企業からは絶対分からないので、これは政府が集めたところから対象を特定した上で、サプライチェーンで上から下に流していくような形で情報提供をしていくと、現実的にか

なり効率的な対応が打てることになる。これはぜひ考えてほしい。

日本経済団体連合会（和田氏）より回答

- 情報提供の質のレベルについては、今議論があったとおり、私も同意である。例えば、ロシアのウクライナ侵攻において潜んでいるマルウェアを取り除いたという話などを聞くが、如何に対処したのかなど、安全保障に関わる情報を入手できているのであれば、ぜひ共有いただきたい。各所からいただいている一般的な脆弱性情報などについては、企業が取り組むべきと考えている。
- 2点目の重要インフラのサプライチェーンの件については、やはり、下請法や独占禁止法の関係もあり、SC3等でも課題として認識されている。例えば、サイバーセキュリティ対策を強化することによって部品価格を値上げすることが下請法で許容されるのか、独占禁止法に抵触しないのか、といった判断について事業者は苦慮している。先ほど御提示があったとおり、サプライチェーンの上流企業が下流企業を助けてあげようとするのが利益供与に当たらないか。現行法に課題があると認識しており、今後検討していただければ、という趣旨である。
- 官民連携における安全保障が何かということを明確にすべきではないか。日本の場合、この問題に限らないが、安全保障という意味では国防、国民の生命や安全に関わるものだということを規定し、そのうえで重要インフラとは何か、基幹インフラとは何かを定義し、そのうえで官民協力は不可欠なものである、やってしかるべきものであるということをはっきりさせた方がよい。その前提として、何が能動的サイバー安全保障の対象になるのか、それは国民の生命、財産、安全にかかわるものだとハッキリさせた方がよいのかと思う。
- サイバー安全保障に関する認識は東京でさえこの状況ならば、ほかの地方は推して知るべしではないか。全国あまねくとはいかないのだろうが、例えば大阪、愛知、福岡などの中核都市で、能動的サイバー安全保障の重要性を周知させる取組をお願いしたい。
- 重要性の高いセキュリティ対策として、脆弱性情報を踏まえたアップデート、いわゆるパッチ適用を適時に運用するという点があるが、その重要性が中小企業においてはまだ十分に認識されていないという印象がある。
- 例えば、日本商工会議所の資料3の4ページをみると、ランサムウェアによる被害というのが2021年から4年連続で第1位になっており、かつ、中小企業の被害が6割と記載されている。その感染原因についていえば、警察庁の公表データによると、VPN経由が6割とされている。このVPN経由の内容として、脆弱性が公表されたにもかかわらず、パッチを適用せず、脆弱性が放置されていたがゆえに当該脆弱性が悪用されたものが含まれていると推測される。
- 「VPN経由」といってもいくつか原因はあると思うが、大げさに言えば、VPNについて

パッチを適時に適用すれば、このランサムリスクを6割近く減らせるということではないか。

- 資料3の2ページで、ソフトウェアの「定期的な」アップデートは72.6%とあるが、これと「適時の」アップデートとは違うかなと思う。「定期的」に加え「適時の」アップデート」が重要となる。
- なぜ脆弱性についてのパッチ適用が進まないかを考えたときに、1つの仮説として、脆弱性という概念と、パッチという概念が企業のセキュリティ担当者にとって理解されにくいと思っている。
- セキュリティの普及・促進にあたっては用語や概念を分かりやすく説明する工夫が重要だと考えている。自動車に例えて言うと、深刻な脆弱性とは、自動車のブレーキに不具合があること、アップデート通知というのは、当該不具合の存在が発覚してリコールがかかった状態であるということ。そうすると脆弱性があるのにパッチを適用しないということは、ブレーキに不具合のある自動車を乗り回している非常に危険な状況であるといえるのではないか。
- もう一点申し上げると、資料1の9ページ目に独占禁止法の話があったが、サプライチェーンを構成する企業に対して、セキュリティ対策を推奨するときに、確かに優越的地位の濫用や下請法に抵触するのではないかというのが論点になる。
- この論点について、公正取引委員会から2022年10月28日に、「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」という有益なガイドラインが出ている。それでも企業としては、サプライチェーンを構成する企業に対して、例えばEDRの導入を求めたり、サイバー保険の加入を求めたりするにあたって、優越的地位の濫用や下請法への抵触が気になって、二の足を踏んでいるという実情があるという印象である。
- 自然災害への対策と同様、サイバー被害についてもその対策として自助、共助、公助があると考えているが、このうち共助を遅らせている要因として、図らずとも優越的地位の濫用や下請法の論点があると思っている。この論点をもっと整理する必要は高いのではないか。

日本商工会議所（岩本氏）より回答

- 基本的には委員のおっしゃるとおりだと思う。ただ、これは私の経験だが、パッチでいうと、単にセキュリティ上の単純な脆弱性を直すだけのパッチもそうだが、多くのソフトウェア提供会社が、提供ソフトにもともと内在していた不具合のパッチを数多く出していく。
- ところが、今は様々なソフトウェアが多段式に組み合わせられているので、どこかの会社のソフトを直すと、実はシステム全体に悪い影響を及ぼすということが山のようにある。したがって多くの企業では事前のテストを入念にやらざるを得ない。そのパワーと効果とがトレードオフみたいなもので、どこまでパッチ対応するかという判断は、

どちらかというと、ネガティブになっているところが多いと思う。基本原則は、委員のおっしゃるとおり、脆弱性が出たら、それは無条件に当てて、そこで何か出たら、提供側のパッチのミスだと割り切ることが必要だが、パッチを当てることによって大きな障害を引き起こすことが皆無でないので、この辺のところは、いたちごっこの要素があるように思う。

- 官民連携の枠組みの在り方であるが、政府の役割を明確化するという点で、政府にサイバー空間の安全を確保する責務があるということを、法律に明記して、その上で政府の体制としては、これまで御議論されているように、NISCを発展的に改組して、政府の司令塔組織としていくことが考えられると思っている。
- さらに、その下に、官民の新たな協議体をつくると、先ほど、他の委員からお話があったが、官民が力を合わせてともに守るという在り方を目指す方向へ向かっていくのではないかと考えた。
- お尋ねであるが、企業に過度な負担を負わせないという意見があるが、その過度な負担を負わせないということの中には、情報を提供する企業が、法的なリスクを負わずに済むようにするということも含まれるのではないか。
- 以前、政府の要請に応じて、プロバイダー会社がブロッキングを行うと表明したところ、訴訟を起こされたということがあった。そうしたことが起きないようにしなければならないのではないか。国益、公益のために協力した事業者が、訴訟リスクやレピュテーションリスクにさらされるということはあってはならないと、そうした制度設計が求められる。
- それで、協力した場合に、サイバー防御に必要な情報を政府に提供した企業が、社会の安全のために貢献しているのだと、肯定的に評価されるという方向を目指すべきではないか。その点についてお尋ねする。

経済同友会（伊藤氏）より回答

- もちろん正直者をフェアに扱うことも重要であるが、EUではNIS2指令において違反した場合は売上の数パーセントの支払いや経営者交代なども起きている。それを通じてサイバーセキュリティが強化されている現実もあると聞く。
- 日本にはそのような罰則は現時点ではない。様々な論点はあるが、アメとムチの両方が必要であり、バランスを取りながら進めることが必要である。
- 経済同友会の説明において、高専、大学、大学院で人材育成の強化をすべきだという話があり、全くそのとおりでと思っているが、人材流動性の低さが非常に課題である。
- セキュリティ研究の場合は、大学の中だけで研究をやるのは難しく、実務経験や社会人経験がある人材が大学に戻って、更に高い技術を身につけるということで、海外では良い成果、良い技術が出ていると思うが、日本はなかなかそうはなっていないとい

うことがある。このような人材にとって、そういうキャリアパスを取るということが非常にリスクがあり、かなり志のある人でなければ、それができない。大学に戻った後、大学で教員になるポストも少なく、学位取得した場合に企業に戻った後も、それがキャリアアップになるという保証が全くないという中で、かなり人材が停滞しているという印象を持っている。

- 人が来ないから教育が充実しないのか、教育が充実しないから人が来ないのか、鶏と卵のようなどころもある気がするが、一方で、高額な海外のセキュリティ・トレーニングは非常に人気だということも聞いている。
- また、国産のセキュリティ技術を強化すべきという話もあったが、これも似たような話があると思っており、国産のセキュリティ技術は、確かに十分でないと思うが、一方、海外の技術に頼り切っている面もある。技術がないから導入が進まないのか、導入が進まないから、知見、経験、データがたまらない、データがなければ、研究も技術もできないということで、この負のスパイラルに陥っているという印象を持っている。
- 人についても、技術についても、このような一種の負のスパイラルになっているように見えているが、国家安全保障の観点では、国内の人材や国産の技術が重要だと思うるので、どこかでこれを打破する必要がある。こういった人を雇用する立場、また、技術を導入する立場の企業から見て、突破口はどこにあるかについて、考えをお聞きたい。

経済同友会（伊藤氏）より回答

- 人材育成について現実的にはそのとおりだと思う。ひいては、どうすればいいかというと、やはり全体的に人材資金や投資が足りない。欧米に比べて、国も企業も人材投資が不十分である。
- 国がリーダーシップを取って、適切なところにお金をつけて、企業もキャリアステップを考え、給与水準を上げる必要がある。また経営層にもセキュリティ知識に優れた人材を少なくとも取締役レベルのメンバーにいれるなどしないと、日本のサイバーセキュリティ強化は口だけ終わってしまう。
- 全体を通して思ったことを述べたい。トップ人材、即戦力という話がよくこの業界では出てくるのだが、そういった人たちだけ育てても、その方と共に動く人たちがいないと、どうしても話が回らないというのを忘れてはいけないと思っており、給料が安い、お金が出ないから、とよく言うが、技術者の側の方が技術者の価値を経営者に説得できていないという側面もあるのではないかと考えている。技術だけではなくて、きちんと伝える能力というのが、経営層にしてもそうであり、エンドユーザー、セキュリティのルールを守ってもらう説明をするときも、上から頭ごなしに言うのではなく、きちんと説明できる能力のある人材が必要になってくるのではないかと。

- これは、「プラスセキュリティ」という意味で言えば、セキュリティに関わる人々は、そういった知識が必要なのは、情報システムに関わる人々だけではない。インシデント、事故が起きると、広報をはじめ、営業、財務、法務などいろいろな人たちの手を借りることになる。その人々と共通する言語がないことにより、事故の対応が遅れてしまったり、きちんとした内容を発表できないということにつながっていくところもあるので、政府主導で人材定義の可視化というところは、こうしたことを加味していただくことを検討をしていただきたい。
- 一方で、人材が大事ということは私も思っているが、人材が先なのか、その人材が活用できる情報が流通されるのが先なのかという問題があるかと思っている。答えは両方並行して進めるということだとは思いますが、どこそこで起きた事故が、どういう理由でやられたのかというのが分からないケースというのが、やはり多い。そういったものが流通していないことによって、人材の能力があっても、同じようなことにならないようにするためには、自分たちは何をすればいいのかというのが分からない状況が多く見受けられるように感じる。
- そういった情報の共有も必要だろうというところもあり、また、脆弱性対応に追われるという話が先ほど出ていたが、脆弱性の優先順位がつけられない、つまり、対応の優先順位がつけられないということもある。
- 脆弱性が年間大体どれぐらい出ているかというところ、今年は多分3万件を優に超えると考えられる。その3万件例えば仮にある脆弱性の中で、本当に悪用されている脆弱性というのは何件あるのかという問題がある。理論上危ないと言われている、穴があるかもしれないと言われているものと、今まさに攻撃に悪用されている、また、悪用方法が公知のものであるというもので言うと、全然程度が違う。
- その件数を集計してみたが、2013年から2023年までの間で、発表されている脆弱性の数に対して、悪用されていると米国政府が認めている脆弱性は、どの年においても1%未満である。よって、そういった悪用されている脆弱性から対処しようという広報活動みたいなものを国がやっていく必要があるのではないかな。
- もちろん、米国が言っているだけなので、日本独自のアプリケーション等、アジアでよく使われるものは入ってこないのですが、こういったところは、IPAなりJPCERTなりに頑張ってもらいたくなるのかもしれないが、その何万件もある脆弱性の中で数パーセント対処すれば、多くの事故に遭わないということであれば、なかなか対処できない、パッチを当てたくないというものも、少なれば一筋の光明が見えるのではないかな、そういった情報の発信の仕方ということも大事かと思う。
- 他方で、情報は出すだけでは駄目であり、どうやって広報していくか。また、有益な情報でも、その使い方が分からない人々もいる。そういったものも含めて、手厚いケアをしつつ、あとは国とか国に関係する組織で何かしら事故が起きたら、積極的に自分たちが見本になるように、こういう原因でやられましたというのを、恥ずかしいか

もしれないが、発信していくことが大事なのではないか。

- また、民間事業者から政府への情報共有の在り方ということだが、これは窓口一本化にしないと、手間がかかり負担がかかるという話があったが、窓口一本化に加えて、フォーマットの統一化というものも併せて考えたほうが良いのではないか。
- 経団連の資料の5ページにもあったが、民間と政府との間で共有すべき情報例はいろいろある。情報共有は、民間サービスとしても存在するので、政府から出す情報と民間から出す情報の両方を企業は見ることになるが、信憑性、希少性、リアルタイム性がないと政府の情報の信頼性は失墜すると思う。ここをどう担保するかが重要であり、例えば、そういうサービスを行う民間企業と一緒に連携して、これはより重要ですと後押しするとか、そんなところなのかなと想像する。いずれにせよ、官民それぞれから情報が来たときに、受け取る側は両方審査しないといけないので、それも手間がかかるので、御協議をいただければと思う。

日本経済団体連合会（和田氏）より回答

- 今日は経団連の立場で出席しているが、普段は航空会社に勤めている。民間事業を推進する観点から、サイバーセキュリティ人材が特別に優遇されるかという点、必ずしもそうではない。航空会社には他にもあらゆるリスクがあるため、ワン・オブ・リスクを対策する人材として活動するというのが現実的なところではないか。
- 例えば航空会社などユーザー企業の立場から言えば、非常に高い専門性を持つというよりも、航空運送ビジネスをいかに推進していくかという観点から活動することが重要である。プラスセキュリティ人材育成の推進はもとより、先ほど委員からお話があった情報の提供に関しては、先ほど申したとおり、雑多な情報ではなく「ここぞ」というときに精緻化された情報をぜひ期待したい。

（４）河野国務大臣挨拶

- 今日は、いろいろ活発な御議論をいただいてありがとうございます。確かに高度なセキュリティ対策をやらなければいけないという話はよく伺うのですが、他方で、実はかなりの部分、簡単にパスワードが流出していたりパスワードが簡単だったりしたところを破られて裏を取られたという、高度なセキュリティをやっている前の段階でいろいろなことが起きているということを、考えていかなければいけないのかなと思います。
- まず、多くの中小企業を始めとする企業には、当たり前のことを当たり前にやっていただく、二要素認証なら二要素認証をやっただけで、表門をきちんと閉めておいていただく。その上で、どうしてもゼロデイやら何やらで防げないものはあるのだろうと思います。
- ワクチンをやっていたときに、どうしてもゼロリスクなのかという話に必ずなるので

すけれども、ここまでサイバー攻撃が活発化してくるとゼロリスクというわけには多分いかなくて、やるべきことをやって、それでも防げないものについてはどう復旧するかということを考えていかなければいけないのかなと思います。

- どのようにやっていったらいいのかということと、いかにセキュリティな情報を持っているのかという、幾つかのマトリックスを頭に描きながら、どこをどれだけ注力していったらいいのかということを考えないといけない。お金も人的リソースもかなり限界のある中で、我々は、これからやっていかなければいけないということになるのだと思います。あらゆることをパーフェクトにというのはできないという前提で、とセキュリティ担当大臣が言ってしまっているのかどうか分かりませんが、そのあたりのことを少し頭の中に描きながら、優先順位をつけて対応していくことが必要なのかなと感じた次第です。

（５）テーマ別会合の開催状況

事務局から、テーマ別会合（官民連携、通信情報の利用、アクセス・無害化措置）について、資料４から資料６を使用して開催したとともに、今後もテーマ別会合での議論を継続し、その結果を次回以降の有識者会議に報告することとされた。

以上