サイバーセキュリティ推進専門家会議 第5回会合 議事概要

1. 日時：令和8年3月19日（木）10時00分～13時00分

2. 場所：赤坂グリーンクロス　4階会議室

3. 出席者

（委員）

赤荻　真由美	株式会社みずほフィナンシャルグループ サイバーセキュリティ統括部 部付部長
市原　麻衣子	一橋大学大学院法学研究科 教授
上沼　紫野	ＬM虎ノ門南法律事務所 弁護士
上原　哲太郎	立命館大学情報理工学部 教授　（オンライン出席）
大谷　和子	株式会社日本総合研究所 執行役員 法務部長 （オンライン出席）
加藤　恭子	全日本空輸株式会社 上席執行役員 グループ ＣＩＯ デジタル変革室長　（オンライン出席）
川口　貴久	東京海上ディーアール株式会社 主席研究員 （オンライン出席）
後藤　厚宏	情報セキュリティ大学院大学 教授【議長】
酒井　啓亘	早稲田大学法学学術院教授【議長代理】
宍戸　常寿	東京大学大学院法学政治学研究科　教授（オンライン出席）
篠田　佳奈	株式会社ＢＬＵＥ代表取締役
土屋　大洋	慶應義塾大学大学院政策・メディア研究科教授
星　周一郎	東京都立大学法学部 教授
松田　浩路	ＫＤＤＩ株式会社 代表取締役社長 ＣＥＯ 一般社団法人 ＩＣＴ－ＩＳＡＣ 理事

（大臣・政務官）

松本　尚	サイバー安全保障担当大臣

（事務局）

飯田　陽一	内閣サイバー官
木村　公彦	国家サイバー統括室統括官
門松　貴	国家サイバー統括室統括官
安藤　敦史	国家サイバー統括室統括官

関口　祐司	国家サイバー統括室審議官
中溝　和孝	国家サイバー統括室審議官
斉田　幸雄	国家サイバー統括室審議官
佐野　朋毅	国家サイバー統括室審議官
鈴木　健太郎	内閣官房内閣参事官（国家サイバー統括室）
伊藤　建	内閣官房内閣企画官（国家サイバー統括室）

（関係府省庁）

齊藤　大地	内閣府科学技術・イノベーション推進事務局 人工知能政策推進室企画官
小野寺　健一	警察庁長官官房審議官（サイバー警察局担当）
森田　稔	デジタル庁戦略・組織グループ統括官付総括審議官
赤阪　晋介	総務省サイバーセキュリティ・情報化審議官
道方　孝志	総務省サイバーセキュリティ統括官付参事官（政策担当）
中山　貴洋	総務省自治行政局住民制度課サイバーセキュリティ対策室長
森田　光枝	外務省大臣官房情報システム総括課課長
藤吉　尚之	文部科学省大臣官房 サイバーセキュリティ・政策立案総括審議官
新畑　覚也	厚生労働省医政局参事官（医療情報担当）付医療情報室室長
野村　由美子	厚生労働省医薬局医療機器審査管理課長
奥家　敏和	経済産業省大臣官房審議官（商務情報政策局担当）
武尾　伸隆	経済産業省商務情報政策局サイバーセキュリティ課長
荒　心平	防衛省整備計画局サイバー整備課長

4.　議事概要

（1）松本サイバー安全保障担当大臣挨拶

○本日は、特にAI技術の進展に伴うサイバー脅威への対応、サイバー分野の技術、研究開発、産業育成、そして、中小企業や地方公共団体などへの対策等々について御議論いただく。

○サイバーセキュリティは、成長戦略の分野横断的に、全ての事柄に関わる問題である。それに加えて、中小企業、地方自治体、大学、特に総理も心配されている医療機関、こういったサイバーセキュリティに脆弱だと言われているところの対応を決めなければ、成長戦略そのものがぼろぼろになってしまう可能性もあるため、ぜひそこは意識的に御議論いただきたい。

○もう一つは、AI サイバー攻撃をどうするか。今、この点も世界中でどうするのかという話になっているため、できるだけ世界の最先端に立てるような方向で我々も進めていきたい。
○最後に人材の確保。それぞれ皆さまがフォーカスしている分野があるかと思うため、それぞれの御専門の知見をぜひ議論の中でぶつけていただきたい。

（２）事務局および各府省庁説明（ＡＩ×サイバー、技術・研究開発/社会実装/産業育成）
事務局、経済産業省、総務省、内閣府から、配付資料により説明があった。

（３）意見交換
○政府機関における AI を活用したサイバー対処能力について、相手の攻撃力に対応する観点から、サイバー対処能力強化のため AI の利活用が喫緊の課題であることは言うまでもなく、これに深く賛同する。
○AI 開発の鍵となるデータについて、データセキュリティの観点から検討することも必要である。その点で我が国が主張する信頼性のある自由なデータ流通を確保し、維持することが重要である。そのためにも、内閣官房国家サイバー統括室を中心に、総務省、デジタル庁、経済産業省、警察庁、その他様々な官庁を取り込み、政府全体で AI を活用したサイバー対処能力強化のために、個人の権利侵害の回避などを念頭に置きながら、AI による情報収集・分析に際しての方針・基準、その具体的な施策を整備しなければならない。ただし、民間セクターへの過度な干渉となり得るような政府による規律は、できる限り避けるべきであり、この点での政府の役割は、民間の活力を活性化させる投資を行うというイメージになると思う。
○他方で、AI を利用したサイバー攻撃に対しては、一国だけでの対応には限界があり、この点での国際協力は政府相互間のみならず、政府と民間との間、民間相互間のレベルでそれぞれ促進が図られるべき。その際には、自国の安全保障上の利益に配慮し、外国への過度な依存を排しながらも、他国政府や外国企業等との協力を深めていくことになる。
○政府は、その時々において、いかなる分野でどのレベルでセキュリティ技術が発展して、我が国のセキュリティの質がどのレベルに位置しているのかを常に念頭に置く必要がある。そのような評価を可能とするためにも、ステークホルダーとの情報交換・意見交換を定期的に行いつつ、海外の活動とのインターフェースの共通化、セキュリティやリスクの評価基準の共通化などにも留意すべき。
○サイバー分野での国際的なガイドラインや標準の策定は、AI 技術の進展と密接な関連がある以上、我が国がこうした国際規範の策定に積極的に貢献するためには、民間セクターのイノベーションとセットで考えなければならず、AI セキュリティについて官民連携の強化が不可欠となる。
○官民連携の強化も喫緊の課題ではあるが、資料に示された内容では、短期と中長期に分け

て考えられているものの、なおタイムスケジュールが不明確である。スピード感を持って実施に当たるためにも、およその時間を明示しておくことも一考に値するのではないか。

〇Security for AI について、多くの企業が AI の活用や実装を進める中で、AI 関連リスクマネジメントに関わる各種ツールやフレームワークの公開は、間違いなく企業の成長に資する。これまで AISI や経済産業省、総務省が取り組んだインシデントレスポンスのフレームワークや、LLM・AI サービス出力結果に関するリスク評価、リーガルチェックはどれも重要である。一方で、ツールやフレームワークが散逸している印象もあり、サービス開発者・提供者および利用者・利用企業の目線で AI 関連リスクマネジメントのプロセスの全体像を示した上で、プロセスごとに必要とされるツール等を示すことができれば、より民間企業の AI 活用やリスクマネジメントを支援できるのではないか。
〇また、AI for Security とサイバー攻撃対処に関して、AI 含むテクノロジーのイノベーションは、当然キャッチアップする必要があるが、同時にサイバーセキュリティをめぐる戦い方のイノベーションもフォローすることが重要。例えば、ゼロデイを検出するヒューリスティック・ビヘイビアの解析、EDR、アトリビューションなど、今では当たり前のような概念や戦い方・守り方も発表された当時は常識を覆すようなものあった。技術そのものと戦い方・守り方の双方のイノベーションを注視することが、サイバーセキュリティ向上につながる。

〇AI for Security は大切な取組であるが、そのガバナンスが大事。AI ガバナンスでの議論から、AI for Security は学ぶことが多いのではないか。安全保障やセキュリティのために AI を使う場合、透明性を事業者やステークホルダー、国民に対して確保することが決定的に重要。理由は 3 点。 第 1 は能動的サイバー防御で膨大な量のデータが入ってくるため、AI を使うのは当たり前だと思う。他方で、例えばアクセス・無害化措置をしたが、その対象を間違えていた場合に、AI を使っていたために間違えたということが議論となると、AI for Security の障害になる。AI を使っている立場から、この範囲でこの程度のものを使って、こういうことには使っていないということを、透明性を持って説明することが必要。第 2 に、研究開発について、例えば国費でセキュリティに役立つ AI の開発があるとすると、補正予算や単年度予算のレベルではなく、継続費を使うことまで踏み込む必要がある。その場合、なおさら透明性について説明することが必要。第 3 は、自由を保障すること。民間の中でデータが流通し開発される自由な機運の中から、役に立ち、権威的な勢力による AI 利用に対抗できる『自由に基づく優れた AI』を開発するという環境を整備することが競争政策・産業政策として日本国が取っていく AI の方針だと思う。以上の 3 点から、透明性・説明責任についても御検討いただきたい。
〇Security for AI は、逆にセキュリティ分野の議論を AI 政策・AI 戦略の方向に反映していただきたい。例えば AI 適正化指針があり、そこにセキュリティの観点をもう少し強く書

くか、AI 適正化指針に書けない場合は、NCO 等で用意する Security for AI の考え方を反映した AI セキュリティに関する文書を AI 適正化指針の方で参照する等、相互で連携することが必要だと思う。

〇また、能動的評価基盤をめぐる議論もある。AI をめぐり、様々なステークホルダーからの情報を共有する場合、基盤モデルの研究開発を行うグローバル企業なのか、それともそれを利用して AI 開発を行う企業なのか、共有先については見定める必要がある。企業側からすると、AI 戦略本部、総務省、警察庁、NCO 等のさまざまな担当が個々に来ると、誰が何を話しているのか分からず、誰にも話したくないということになりかねないため、窓口を必ずしも一本化する必要はないのかもしれないが、整理を明確化し、受けた話の情報共有範囲を明確にしていく必要があると思う。AI 政策・AI 戦略と、NCO で議論しているセキュリティ関係の議論が相互に学び合い連携しあうことが大事。

〇AI の利活用に欠くことのできない国内のデータセンターについて、地域によっては住民反対運動が巻き起こっているということは気がかりである。賑わいが必要な駅前などに建設計画が生じており、海外でも同様の事例があるが、電力需要がきっかけとなっていると思う。

〇ただ、経済安全保障の観点からも、一定の規模のデータセンターの国内設置は不可欠であり、今後、必要な場所にデータセンターを設置することが可能となるよう、住民の不安を払拭し、また、済々とした建設が進められるよう、制度上の課題がないか点検することも、この段階で必要になってくるのではないか。

〇政府機関における AI を活用した対処能力強化は大賛成である。早く始めて、失敗を経験しながらノウハウを高めることも大事。その際に確認すべきは、いわゆるヒューマン・イン・ザ・ループが本当に回るのか、AI のスピードについていけるのか、または AI における小さなエラーの累積の怖さをどう捉えるか。また、それが特にアトリビューションや無害化措置に適用される場合などに非常に深刻な状況となるため、ここについての経験を早く積み上げることが大事。

〇また AI のためのセイバーセキュリティ技術に関して、K プロの先進的サイバーでは、集中的に AI を使った、または AI 攻撃に耐える技術を最重要課題として取り組んでいる。それをしっかりやると同時に、政府機関などによる国産技術の先行的な活用、それを使ったノウハウ・フィードバックを R&D に戻すというエコシステム、そういったループを早く回すことが大事。これが成長戦略につながるのではないか。

〇大量のデータを集めて分析するところに関しては、NICT が非常にいいシステムを開発して、運用ノウハウをためている。そういう基盤技術をしっかり活用していき、K プロなどの研究開発をしっかりマージさせていくことが、政府機関での AI 活用、AI を使ったセキュリティ基盤づくりに非常に有益。

〇そして、AI エージェント、またはそのベースとなるエージェンティック AI について、エージェンティック AI は自律的な AI であるが、これは当然ながらロボットやフィジカル AI で日本でも頑張っている。その技術で培ったセキュリティの考え方を逆にサイバーセキュリティの防御に使うのも大事ではないかと思う。そういう形でうまくやっていただきたい。

〇AI エージェントについて、エージェントの AI そのものよりもエージェント間の通信部分は本当に脆弱であり大変なことになっている。一方、エージェント AI は、人口減少が見込まれる地方や、中小企業には助け船であり、争って活用が進んでいる。この結果非常に危ない AI エージェントが民間に広まってしまう恐れがあり、実際に広まっていると思っていたほうがいい。

〇今、10 年前の野良 IoT と同じことが起こっている。一旦広まってしまうと、それを回収するのは非常に困難。そういう意味で、METI からもガイドラインをつくるという話があったが、もう一歩踏み込んで、実際に AI サービスをどうやって安全につくるかという仕組みも全部作ってしまわないと、大変なことになるのではないかと危惧している。

〇資料 1 の 1 ページについて、私たちは①と③をセットで考えており、③の AI を悪用して行われるサイバー攻撃は、従来の攻撃が加速して増加、かつ高度化すると分析しており、それに対応できるよう、①で AI を活用することを進めている。攻撃の早期検知や、スレッドハンティングで見つけた攻撃を防御側に回すことは AI を使い、SIEM やブロックするソリューションのほうに組み込むというのは、職員自身が手を動かして対応するという活用を行っている。

〇②の AI に係る安全性確保は、AI の活用は過去より継続しているが、当組織内利用をしている分については、ガイドラインは示しながら安全に使っており、今年度は商用にも AI を使いたいと思っている。その場合、担保すべき安全性のレベルが引きあがるため、現在、各種並行して整備している。

〇ガイドラインの整備については、AI コールなどが入ると、AI による AI、AI モデルの呼び出しや、AI 同士の通信といったところまで踏み込むと、ガイドライン化するのがかなり難しいため、関係者で議論しつつ、システムアーキテクチャーの安全性も審査を進め、同時並行で AI レッドチーミングをつくって、AI の脆弱性をあぶり出すということを進めている。この取り組みで獲得したノウハウについては、ぜひシェアしていきたい。

〇どのように NCO に情報を集めるかについて、方向性はそのとおりであるが、今、インセンティブという話もあった通り、これをどう民間から与えていくかということは大事。先ほどの総務省の資料でサイネックスという、非常に先進的な基盤で産学官の結節点みたいなものがあったが、これは共有いただくという基盤になっており、これをどのように民間側からも収集するかということが一つのポイントなので、その仕組みづくりは大きい。

〇またその後の官民の連携は本当に大事になると思うが、AI の安全性に関する評価結果等を共有いただくと非常に有意義だが、逆に詳細過ぎる内容が共有され、外部に漏れてしまうと、対策が講じられ、バイパス攻撃の原因にもなりかねないため、適切な秘密保持みたいな枠組みがあると民間側も参加しやすいと思っている。協議会の中の関係者、参加者、構成員もベンダーという範疇で、参加者は幾つか異なってくると思うので、ここも適切な仕分けをしながら、こういった枠組みができていくと、民間側も参加しやすく情報提供しやすいと思う。

〇予算について、先ほど見せていただいた外国との比較において、最終的に補正予算などで対応されているが、長期間での視野も要ると思う。そのため、予算をどのように確保するかという観点での検討が必要。民間委託に関しても、委託事業で行う際に、短いスパンの場合投資が十分に図ることができないため、投資スパンのバランスをどのように取るのかについては、ぜひ考えていただきたい。
〇国産についていろいろと御議論いただけるのは非常に安心である。現在、情報ツールのほとんどが外国企業のものである点については、市民として非常に心配しており、実際に大手外国企業が日本に進出したが早期に撤退することは過去に何回もあったため、外国企業に国内データが任されているのは安心できないと思う。少なくとも政府が利用する情報ツールは、例えば入札の際に国産ということで点数の加点や、事業の継続性を加味する等の対策を考えていただきたい。
〇現在、非常にたくさんの取組がされていると思うが、ユーザーから見るといろいろなところでばらばらと行われている印象がどうしてもあり分かりづらい。司令塔で統括していくことを示せば、ユーザーから見て分かりやすいと思う。

〇AI 戦略について、アウトプットをどのように民間に提供し活用するかは、ヒアリング次第。普段から問題意識を持っている方はヒアリングでどんどん答えで出てくると思う。先ほど他の委員が話した商用の AI モデル作成の話もヒアリングで出てくると思う。その中で、一緒にこういうふうにしていければいいのではないかという答えが出てくるのではないか。問題意識を持っていない方は、ヒアリングの中から見えてきた想定アプリ、想定顧客などでヒアリングを固めることで、マーケットインのサポートになっていくと思う。
〇経済産業省の発表内容は全て合意する。振り返ると日本が一番弱いのは、マーケットイン。業界構造として SI 事業者が存在するため時間がかかる。イスラエルはガバメントの下にすぐ製品を開発する方がおり、ガバメントがファーストカスタマーとなり世界に広がっていくというアプローチで、日本よりレイヤーが少々大きい。変えようがないのであれば、先ほど言われたように IPA が評価後、政府がファーストカスタマーとして購入しマーケットインのサポートを行い、使えるレベルまで政府で行えばいいと思う。しかし、世界に

出す際に、日本の仕様は気にいられない。いわゆるオーバーエンジニアリングと言われる観点も加味して、よりシンプルなシャープな製品が海外には好まれると思う。

〇ICSCoE の点、あるいはセキュリティ・キャンプの点だが、海外からは非常に評判がいい。なぜ日本の講師、日本の修了生はこんなに優秀なのかとお褒めにあずかる中で、ICSCoE から、シンガポールにまねされたとの話があったが、実績はどんどん伝えていっていただきたいので、まねされない仕組みをつくる必要がある。

〇マザーモデルについてもおっしゃるとおりであり、その部分の強化について、別の委員が話していた AI ブートキャンプ等の運営者として大賛成。講師の確保については、AI のスペシャリストは引く手あまたであるため、政府としていろいろな有識者にお願いしたいところだと思う。

〇総務省が話した点も、そのとおりに進めていただきたい。国産セキュリティ技術の自給率を上げる点について、日本企業のも関わらず懸念国の人材がいる問題は明らかになっている。国籍で排除したいとは全く思っていないが、このあたりは慎重に考えていきたい。

〇今後のサイバー対処能力強化の基本的な方向性を示しており、全て賛同する。

〇純国産のビッグテック企業が残念ながらない中で、そのような企業との付き合い方は考えていかなければいけない。その場合、恐らくはギブ・アンド・テイクの関係にどうしても持っていかざるを得ない。日本の国内だけではなく、海外、同盟国・同志国に対して、日本から提供できる内容も含めて対応しなければ、対等な関係はできてと思う。それも含め、何をもって国産と考えるかということ自体は難しいが、最終的には日本の利益を損なわないという形であるということが国産ということの意味である。

〇アンソロピックやパランティアといった二つの会社は、アメリカ政府、国防総省、戦争省と非常に緊張関係にあり、イランやベネズエラの問題で彼らのシステムが使われたことに対して、アンソロピックが抵抗している。こうしたシステムを我々がどう使うかは非常に緊張感を持って考えなくてはいけない倫理的な問題である。また、アンソロピックのシステムは、中国が悪用してサイバー攻撃に使っているとの報道も出ている。今、アメリカ政府がアンソロピックのシステムを外すときに、数か月かかるという報道もあり、「明日からやめます」と言われても外せないというロックインが起こる。

〇物理的なセキュリティもかなり重要であり、今回、イランがアラブ諸国に対する物理的な攻撃を始めた中で、UAE にある AWS のデータセンターがミサイルによる攻撃を受けた。データセンターが破壊された場合、AI、あるいはその他の IT サービスに大きなインパクトが発生する。また、UAE にある AI に非常に力を入れている大学と意見交換をしていたが、今そういったところに大きな影響が出ていることを考えると、システム、インフラとしての AI をどう守っていくかということが問われている。

〇最後に、サイバーセキュリティ、サービス提供事業者の信頼性確認の説明があったが、こ

れは非常に心配をしており、下請や孫請まで辿ると、非常に問題のある諸外国の業者が入り込んでいる。またセキュリティチェックをする会社が、そのデータをどこか別の会社に流す可能性があり、実際に発生していると思う。誰に私たちのセキュリティを任せるかということは、非常にリスクのある問題であるため、経済産業省には引き続きこの問題に力を入れていただきたい。

〇人材育成の問題について、各種キャンプなどそれぞれ長い実績があり、それなりの人材を生み出し続けていると思う。しかし、これを社会が十分に役立てているかという点に関してはいささか疑問がある。組織の中で活躍してもらうためには、セキュリティだけではなく、いろいろな分野の現場の仕事を覚える必要があり、これに対して時間がかかるが、それをやっている間に知識が霧散してしまうようなところが多少あり、これはよくないと思っている。重要なのは、CYDER のようなリスキリングの仕組みで現場に送り返した人材がどう処遇されているのかという点である。セキュリティの人材はその組織の中核となり、いろいろなところに目配りしたうえで、それなりに処遇されるべきであるが、うまくいっていない気がする。AI についても、リスキリングの仕組みをちゃんと整えなければならない。セキュリティや AI の分野で育った人材が組織の中で適切に処遇されることに対して、何らかのインセンティブが与えられやすいような制度設計が必要になってくるのではないか。
〇データ提供の問題も同じ話がある。データは集めれば集めるほどいいが、能動的サイバー防御のように比較的強制力のある仕組み以外のデータ収集にはやはりインセンティブが必要で、昔から言われているデータマーケットがなかなかうまく立ち上がっていないということを考えると、データマーケットをつくる際に立てたさまざまな施策をもう一度見直し、セキュリティのために必要なデータをどのようにうまく集めるか工夫した仕組みも必要ではないかと思っている。

〇機密性の高いデータを AI に読ませていく場合、AI のアルゴリズムについて、第三者による監視体制の構築を可能にする必要があると思う。つまり、国側が社会に対して AI を監視に使用しない意図を明確にすることである。
〇関連して、読み込ませるデータと同時に、読み込ませないデータについても考えていく必要があると思う。特に LLM グルーミングをやっている情報源をはじく等を念頭に入れる必要がある。
〇日本国内でデータを抜き取られる場合もあるが、海外でデータをハッキングされることもある。データが窃取される可能性の高い国に行く方々に対して、研修のようなものを設けたほうが良い。

（4）松本サイバー安全保障担当大臣コメント

〇何回かブートキャンプのお話が出ていたが、人材を育成する際には、ある程度集中的に育てることが必要。今、だらだらやっているわけでは決してないにしても、専門に強い人間を育てようと思うと、そういったやり方は非常に効果的だと思う。しかも、少ない人数で集中的にやると、人は育つのだろうと思う。しかし、学んだことを生かす場所もちゃんと準備してやらないと、ただ集めて、お前やれと言っても駄目なので、ただキャンプを行うだけでなく、先もちゃんと見据え、なおかつ講師をきちんと選ぶという、システマチックな進め方にできればいいと聞いていて思った。

〇それから、データセンターのお話をいただいたが、これは私の選挙区でも大問題になっていて、二つほど訴訟になった。確かに住んでいる人にとってはとんでもない話だと思う。データセンターの在り方は、建築基準法の改正などこれから制度的にもちゃんと決めなければいけないと思っているため、これは私の担当になるかというと、また微妙で、いろいろなところに手を突っ込むと怒られるが、考えたい。

〇制度や法律も変えなければいけないし、これは全くの私見であるが、ものすごい電力をあそこに流し込むが、将来ワットビット連携等で「周辺の人に電気はタダで与えるから、そこに置いてくれ」というトレードオフみたいなものもアイデアとしては面白いと思っているので、将来、このようなことも見据えながら、データセンターはないと困るため、御意見は大事にしていきたい。

〇後で議事録は拝見するので、引き続き活発な御意見をいただきたい。

（松本サイバー安全保障担当大臣は公務のため退出）

（５）各府省庁説明（より一層対策が必要な分野）

総務省、経済産業省、厚生労働省、文部科学省から、配付資料により説明があった。

（６）意見交換

〇文部科学省の件は、重要な取組だと思っている。

〇サプライチェーンで脆弱性の高い中小企業が狙われるのと同じように、大学で教員などが雇用するリサーチアシスタントやTAとして雇用する大学院生も狙われるケースがある。ハッキングやフィッシング詐欺のような形で入ってこようとするケースがあるため、大学職員向けのサイバーセキュリティ研修のみならず、学生を含む構成員向けのサイバーセキュリティ研修があったほうがよいと思う。

〇共通の課題、特に人材は大変だと思った次第だが、資格者が地域に偏在しており、ますます資格者が少ない地域の病院にどのようにスキルのある方を育成していくかというのは、大変なことだと思う。一方で、大学においての課題として、学生はどこまで所属し

ているのかというコントロールが難しいと思っており、そういった意味では、どこまでのネットワークをコントロールして使ってもらえるのかは難しい。

〇屋外に置かれている機器や、家庭内に入り込んでいる機器について、学生も普通の利用者も気づいておらず、この意識レベルをどのように高めていくのかが課題。また、全国的にクリーンにしていくための時間軸が大事であり、時間軸を決めながら対症療法から最終的には根治療法をどのように行うかを議論できればいい。

〇まずサプライチェーンセキュリティの件は、本当に大事なことと重々理解している。特に中小企業は、現場の声を聞くとついていけているのはほんの僅かで、大部分はまだまだ難し過ぎて何も手が出せない。「こういう対策が必要だ」ということを、すぐに盛り込んでしまう一方、削ることはなかなかできず、本当にてんこ盛りになってしまっている。そのため、現場に合わせたものをもう一度見直していくことが必要であることはつくづく感じている。実はSCSのもとの自工会の取り組みをつくったメンバーから、まだまだ中小企業がついてきてくれないという声を聞いているので、ぜひ考えていただきたいと思う。

〇セキュリティ人材について、国全体として専門性の高いセキュリティ人材を増やすことは一番大事なことであるが、まだまだ地方自治体や中小企業ではそれが全く遠い話で、自分たちには関係がない話に聞こえているという声も聞こえてきた。CYDERのような研修等のいろいろな取組は、まだまだ強化を考えなければいけないだろうと思っている。その意味では、前回の専門家会議で人材フレームワークの件がNCOから出ており、今パブコメが終わったところ。これからまとめられると思うが、最初のフレームワークができたのであれば、それを今度は本当の中小企業にも使えるようなものにしていかなければならない。そのときに思い出すのは、NISCの時代につくったプラス・セキュリティという言葉であり、例えば自治体職員の方がプラス・セキュリティ人材になるにはどうしたらいいかとか、中小企業の総務部長がプラス・セキュリティ人材になるにはどうしたらいいか、現場の人に対してどうセキュリティの取組を考えていただけるのか、を今回の人材フレームワークをベースにキャリア育成や、教育プログラムを含めてもう一度強化していくような考え方が必要なのではないかと思った。

〇地方公共団体の支援に関して、引き続き充実していただきたいと思うが、支援を受ける基礎自治体が果たしてそれを受容する能力や人材が確保できているのだろうかという問題は考えていかなければいけないのではないか。そうすると、特に基礎自治体でも指定都市や中核市のような大きな場所であればできるかもしれないが、そうでないところは、例えば都道府県レベルで対処するなどの共通化を図っていかなければ、せっかく支援を提供してもそれを生かすことができないという問題が出てくると心配している。

〇大学に関しては、認証評価という制度があり、認証評価の一つのチェック項目の中に、例えばサイバーセキュリティにどれぐらい取り組んでいるかという項目を入れることによって、大学の経営層、あるいは担当者レベルでも意識を高めていくための一つの仕組みとしてあり得るかもしれないと思う。

〇サプライチェーンの問題について、非常によく対策を立てられており、特に SCS 評価制度は非常にすばらしく、サプライチェーンの安全性確保に大きな寄与をされるのだろう。しかし、「これは格付ではない」と念押しをされていることから、制度の結果を見る先をサプライチェーンの中の話として考えているとすれば、やや視野が狭いのではないか。むしろ出来上がったものにいかに付加価値をつけて、製品なり、情報に結びつけていくかを考えたほうがユーザーや消費者のためになるのではないか。
〇文部科学省にて機微情報の流出防止目的で支援を強化することは、大変いいことだと思う。ぜひ進めていただきたいが、限られた予算の中で行っていくことになるわけであり、大学全体の取組の充実を阻害する要因にもなりかねないことから、予算全体でどれだけ配分するかという視点の中で考えているのであろうが、足腰の充実が弱くなってしまったら本末転倒との意見を持った。
〇サイバーセキュリティは、分野横断的な課題であり、個別の課題に対してどの程度の予算がつけられるのかという話から、これは分野横断的な対処の仕方なのだろうかとの疑問を持っている。全体を見て予算を取り、それを機能的に分配する視点がどこでどのように行われるのかについては、今日の話から見えてこなかったというのが率直なところ。お金と人はとても大事だということは、繰り返しここで言われているとおりであるが、それをどのように生かしていくのか、限られた財源の中でサイバーセキュリティが転んだ場合、ほかの分野も全部転んでしまうと言われるぐらい重要なのであれば、まずサイバーセキュリティ全体につけることをどのように考えていくのかを、ぜひ考えていただければと思う。

〇認証評価は本当に大変であり、ある大学には 3 万 2000 人ほどの学生がいるが、CSIRT の担当者は数人。インディアナ大学を訪問した際、インディアナ大学はインディアナ州の全ての州立大学のセキュリティネットワーク監修を請け負っている、と話を聞いた。ほかの大学から上納金をもらい、それを使ってほかの大学を全部監視する。得た上納金を使い、100 人のエンジニアを雇って 24 時間常時監視する。必要なシステムもその 100 人がつくっている。これを自前で全部やるというのは無理だと思うが、そういうやり方もありだと思う。例えば神奈川県は、情報セキュリティ大学院大学がセキュリティ業務を全部請け負うことで、情報セキュリティ大学院大学にお金が入り、同時に人材育成もできると思うので、このようなことも考えてもいいのではないか。

〇経済産業省の面的な対応が有効であるという提言は、そのとおりであり、お役立ち感のあるIPAのサイバーセキュリティお助け隊サービスなどは、さらに利用層を分厚くしていく必要があると思う。
アイデアとしては、地方の商工団体などを介してアピールしていくことや、当然であるが発注者の力をお借りする、あるいは地方の情報サービス協会との連携も強めていければよいと思う。
〇地方自治体について、J-LISなどを通じて手厚く対応いただいていると認識しているが、特に気になっているのは公立病院などの地方独立行政法人である。例えば公立大学の附属病院のような医療機関について、厚生労働省のセキュリティに関する基準もあるところ、公立大学病院などは、大学自治も尊重しながらの対応となるが、地方自治体として責任を持って対応していくのか。医療機関だから厚労省に任せるのではなく、どのように手を携えていくのかというところが課題だと思うため、ここでポテンヒットが起こらないように対策も併せて検討する必要があると思う。

〇主に地方自治体、医療機関、大学について、いずれも問題になっているのは小さなところをどうやって支えるかという話であり、基本的に人をそれぞれに配置するのは難しいため、外部に人を置き、集約してフォローしたほうがいい。しかしポイントは、フォローをSI事業者にさせてしまうことで、価格のたたき合いが発生し、クオリティーコントロールできない問題が起きてしまう危惧がある。いずれの機関にせよ、セキュリティ対策を自分事として考えられないところに任せても、結局価格競争に陥り、安かろう悪かろうになっていくのは目に見えているため、そういう仕組みにならないような集約をそれぞれの組合せのつくりに合わせて設計していかないと無理だろう。

〇総務省があげた脆弱な機器について、放置機器をどうするか、壊れるまで待つのかというところが長年の課題である。十何年待てば、最新機器はセキュリティ機能を持ったものが普及されるため、将来設計を見ることができると思った。あと、加速させるためには加害機器になったときの罰則がまだないため、その点を促進するのか否かも検討したい。
〇自治体について、個別ではなくまとめて対応することが必要だと思う。特に病院のインシデント対応や演習は、病院が一つ壊れた場合、そのコミュニティー全てに影響するため、どの病院に搬送するのか等も含め、町のインシデントレスポンスの対応が国の演習としてコミットするべきではないか。
〇港湾の場合、我々は貿易の99%を海運に依存している関係で港湾の評価も待ったなしであり、ここもマルチステークホルダーが多いため、効率化が求められている。いろいろなところと組み、町としてどうやっていくべきかについて、米国などはサンプルがよく

できており、軍と町を中心にして演習をやっている。そういったサンプルも踏まえて我が国もよくしていけたらと思う。

〇地方自治体について、市町村はどんどん小さくなっているなかで、共通でできるところはどんどん共通化しないとお金と人がもたないだろうと思う。

（7）各府省庁からのコメント

（経済産業省）

〇SCS 制度について、当該制度を取得した中小企業からすると、セキュリティ対策に取り組んでいることをアピールできる。既存の取引先に加え、新規の取引先を開拓できるような使い方もできると考えており、付加価値が付くような仕組みにしていきたい。
また委員より発言があった、中小企業は当該制度に取り組むハードルが高いという指摘は、我々も非常によく聞いている。当該制度を詳細に落とし込もうとするほど、難しく分かりづらい文章となるため、わかりやすいガイドラインの作成等を通じて普及に努めていきたい。さらに制度自体も必要に応じて継続的に見直していくことを想定している。

〇また本会合で委員より、お助け隊サービスについて関係者と連携しながらより普及に努めるよう指摘を受けた。本件は経済産業省としても、認知度が足りないと認識しているため、NCO や関係省庁を始めたとしたステークホルダーと連携をしながら普及していきたい。

（総務省）

〇小規模市町村をどのようにサポートするのかについて、セキュリティ人材の確保が難しく、予算だけ与えても対応できない、という各委員からの指摘はその通りである。そのため、県単位でまとめてサポートすることは、我々も非常に重要だと思っている。例えばセキュリティクラウドでインターネットからの脅威を防ぐ仕組みを、都道府県単位で構築し、域内の市町村とのインターネットの間口を集約する取組を継続しており、県と域内市町村で連携する土壌ができつつあるため、今後も県を中心とした調達や利用の共同化や、人材面についても、県単位でプールして市町村に派遣する取組を進めていく。
また、国として基盤整備を全国的に進めるべき事項については、我々総務省が進めていき、国と県とで重層的に小規模市町村をサポートするという基本的な考え方で今後も取り組んでいきたい。

〇また、公立病院などの地方独立行政法人に関してどのように対応していくのか、という委員からの指摘について、まさにポテンヒットにならないよう、各省所管の厚生労働省、あるいは文部科学省と日頃からの連携をしながら取組を進めているところである。
さらに改正自治法に基づいて作成する方針について、地方独立行政法人も作成いただく

ことになっている。その方針に基づいて具体的に何をやるのかについては、各省の対策ガイドラインなども踏まえ、連携しながら引き続き取り組んでいく。

（文部科学省）

〇各委員より大学について指摘を受けたが、多様な大学の構成員に対しどのような方法で周知したらよいか考えているところである。

〇また、委員から話があった認証評価は、現場に負担がかかり過ぎないよう留意したい。

〇さらに別の委員よりインディアナ大学への集約化の話があったが、これは先ほどの地方自治体の県単位の集約化と非常に似ている話だと思う。確かにマンパワーがかなり小さい大学もあるので、どのようなことができるのかというのも研究していきたい。

〇あわせて特定研究開発プログラムの機微な情報を扱う事業について、当該プログラムに採択された大学がサイバー予算を使いすぎて、大学全体の予算が減ってしまうようなことがないよう、どのような予算の取り決めができるか、例えば採択された大学に別途予算を付与する対応が可能なのか等を検討したい。いずれにしても、大学の経営層から構成員までが自分ごととしてサイバーセキュリティの重要性というのを考えることが大事だと改めて認識した次第である。

（厚生労働省）

〇多くの委員から指摘を受けたとおり、医療機関における人材育成については、それぞれの医療機関で専門家を確保することは難しいため、専門家と連携ができるような仕組みを引き続き検討していく。

〇あわせて、現在、研究事業者含む地域の医療機関とサイバーセキュリティの訓練をするような取組も進めている。その取組成果を踏まえながら地域でどのように支えていけるのかということも引き続き検討する。

（８）飯田内閣サイバー官挨拶

〇今回、成長戦略の策定に向けて、全体を支える基盤であるサイバーセキュリティ全般にわたっての御議論をいただいた。本日の御議論を踏まえてしっかりと進めていきたい

〇我々は何のために議論をしているのかについて、最終的には日本が社会全体としてサイバーの視点からどうレジリエンスを上げて、それをまさに成長戦略の支えにするかということで御議論をいただいていたと思う。その中で、それはばらばらではないかという御指摘であるとか、あるいは限られたリソースを全体で見たときに、人材や予算をどう最適に配分して、全体としてレベルをどう上げていくのか。そのプロセスの中で小規模な組織に対してどのようなアプローチをするのが最も効果的であり、効率的なのかという様々な視点から御意見をいただいた。

〇あわせて、ガイドライン等のいろいろなルールをつくってみても、それが現場で実際に実施をされなければいけないということであり、どういう形でインセンティブをつけるのかという御議論も多々様々なアイデアをいただいたと思っている。
〇関係省庁は、それぞれの分野の特性を頭に入れながら、ある意味、政策競争をしているようなところもあると思うが、それぞれの政策の着眼点なり、インセンティブの設計でよいところは相互に活用しながら全体として進めていくことだと思うとともに、全体最適を目指していくのであれば、私ども国家サイバー統括室がしっかりと省庁間の調整や連携を進められるように今後も対応してまいりたい。
〇今日いただいた御意見は、まさに今後の成長戦略の柱となるサイバーセキュリティ政策をどのように運営していくかという観点から、全て様々な形で我々の政策に組み込んでいきたい。

（６）最後に、事務局から、次回の会議日程は、調整の上、追って連絡する等の発言があった。

以上