サイバーセキュリティ推進専門家会議 第4回会合 議事概要

1. 日時：令和8年2月20日（金）16時30分～18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）
小栗　泉	日本テレビ放送網株式会社 スペシャリスト・オフィサー　特別解説委員
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
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】 （オンライン出席・途中出席）
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（オンライン出席）
野口　貴公美	一橋大学 理事・副学長、法学研究科教授
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
川崎　ひでと	内閣府大臣政務官

（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
飯島　秀俊	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）
仙崎　達治	内閣官房内閣参事官（国家サイバー統括室）

（関係府省庁）

赤阪　晋介	総務省サイバーセキュリティ・情報化審議官
奥家　敏和	経済産業省審議官（商務情報政策局担当）
吉野　幸治	防衛省サイバーセキュリティ・情報化審議官
逢阪　貴士	警察庁サイバー警察局長
藤吉　尚之	文部科学省サイバーセキュリティ・政策立案総括審議官
奥田　直彦	デジタル庁審議官

4.　議事概要

（1）川崎内閣府大臣政務官挨拶

○ 委員の皆様におかれましては、本日もご多用の中、ご参加いただき、御礼申し上げる。また、昨年末に決定した「サイバーセキュリティ戦略」の検討にあたっては、委員の皆様に多くの有益なご意見を賜ったことにつき、改めて御礼を申し上げる。

○ 政府では、我が国の供給構造の抜本的強化による「強い経済」を実現するため、 17の戦略分野、8の分野横断的課題において、この夏の「成長戦略」の策定に向けた検討を進めている。この推進専門家会議は、分野横断的課題のひとつである 「サイバーセキュリティ」の検討を任されている。

○ 厳しさを増すサイバー脅威に対する対応強化は、 我が国の経済成長の前提であり、「成長戦略」の成功・失敗を決めるといっても過言ではない。各戦略分野の戦略を下支えし、経済成長を推進すべく、「サイバーセキュリティ戦略」に基づく取組みの具体化・強化・加速に向け、ご議論いただきたい。

○ また、人材フレームワーク案に関しても、これを踏まえた運用の方向性等について、ご意見を頂戴できればと思う。

（2）事務局説明

事務局から、配付資料により説明があった。

（3）意見交換

○ サイバー脅威に対する防衛については、能動的サイバー防御をちゃんと動かしていくことが大きな施策になる。被害を覚知する端緒は警察であり、被害にあった企業の対策にも伴走する可能性があると考えると、警察には力をつけてもらう必要がある。国においては、国家サイバー統括官室が組織として立ち上がったが、まだ足りておらず、それ以上に地方で足りていない。各都道府県の警察の人員が人数的にも規模的にも技術的にも心もとなく、そこに体力をつけてやらないと新たな制度が動かないのではないか。

○ 補正予算でついた設備があるが、このあとその維持費用はどういう枠組みで手当てされるのかが見えない。システムは作ったら運用する方にコストがかかるので、本予算でしっかり手当されるよう仕組みを持っていないと回らなくなるのではないか。

○ 地方公共団体において、人も金も不足する中で行政の IT 化を進めていくとなると、国のサポートが重要となる。大きなインシデントが起きれば国にも波及する。国のバックアップがメニューとしてあるような仕組みにしていく必要がある。

○ 人材フレームワークについて、日本では人材を組織で育成することを苦手とする組織風土があるため、専門派遣企業に丸投げするばかりになってしまう可能性がある。組織の中で専門家を持つことは難しくても、外部の専門家をコントロールできることが大事であり、丸投げにならないようにする必要がある。そのために、責任分界点も含めた仕組みにするような人材のあり方も示してもらわないと、産業全体のセキュリティ向上に行きわたらないのではないか。

○ 人材フレームワークについて、ここまでブレークダウンして手引書までつくるというような形であることは、ありがたい。

○ 人と企業側とを結びつけるという意味で、検定制度のようなものがあると広く広まっていくのではないか。

○ また、ここで考えているようなボトムアップのシステムだけではなくて、いかに専門性の高い人材を国家として確保していくかというところも本当に喫緊の課題ではないか。この観点も今後考えていくべきではないか。

○ 成長戦略の検討において、サイバーセキュリティが位置付けられていることは非常に重要だと思うが、問題となるのは、人と金である。

○ サイバーセキュリティという重要な問題に対しては、補正予算ではなく基本的には本予算でしっかり査定を受けて予算を組んでいただき、その上で次の年度の概算要求・機構定員要求につながっていくことが重要ではないか。

○ 参考資料 1 の 36 頁以降に地方自治体のサイバーセキュリティ対策について書かれてい

る。インシデント発生後のレジリエンスの観点から、都道府県や政令指定都市で対応できる部隊を持っていることはあっても、普通の市町村であらかじめ人と金を用意するのは難しいのではないか。サイバーインシデントが自然災害や感染症等々に匹敵するリスクをもたらすことを考えると、地方公共団体においてそれが発生した場合に備え、被害の拡大防止や復旧支援のレスキュー隊となるような施策を国においてしっかり考えるべき。

○ AI セーフティとサイバーセキュリティの問題は表裏一体なので、AI 分野の戦略の議論と、議論が生き分かれにならないように連動してもらいたい。

○ サイバーセキュリティ人材フレームワークの普及について、官民協議会の取り組みと有機的につながるとよい。例えば、フレンズになるためにフレームワークにおける一定のレベルをもった社員が一定の比率でいること等を要件とするなど、フレームワークに参加することにメリットを感じられるようになるとよいのではないか。

○ 人材フレームワークについて、米国はマップ形式、英国はリスト形式で整備されている。日本では既存のフレームワークと相互参照するとのことだが、米国ではどこにどういう人がいるか、どのようなレベルとなれば掲載対象になるかが明確に示されており、そういった形となれば、使われて普及につながるのでゆくゆくはそういった形になるとよい。

○ 脅威ハンティングの体制強化について、重要インフラ分野でもログ管理の体制が進んでいないとのことである。一定規模以上の企業にはログ監視促進のため、ある程度の厳しさを課しつつ、後押しが必要である。期限を決めて体制構築させるように政府が促せば、企業でも予算もあてがわれ、後押しにつながるのではないか。また、オペレーションを担う省庁（防衛・警察）においても、ハードウェア・トレーニングについて、高額で厳しいと聞くが、抑止力・捜査能力を挙げていくという点で支援を厚くしていく必要がある。

○ 総務省が進めている脆弱性対策はかなり先進的な取り組みで期待している。どこまで実効的に進められるかが重要であり、何年で何割買い換えるなど長い目で見た期待値・目標値をもって、進めていけたらよい。

○ サイバー脅威に対する防御・抑止の強化・加速について、法改正により導入された能動的防御等の措置を今後適法にかつ躊躇することなく確実に行使していく環境を整えることが重要となる。そのために、第 1 に権限行使に必要な人材・リソースを十分に確保すること、第 2 に権限行使にまつわる不安、例えば責任の問題や訴訟リスク等の不安を払拭していくことが必要である。

○ 人材・リソースの確保については、補正予算ではない形で措置すべきである。

○ 権限行使にまつわる不安の払拭については、教練、訓練、演習等の実施に加えて、権限行使時の考慮事項、判断の基準や手続、情報やリソースの取扱いなどを内部規範やマニュアルなどで明確にして整えておくことが有効である。

○ 対策水準・レジリエンスの底上げについては、重要インフラ統一基準等の関係者に対す

る要求達成の水準に、各主体がどの程度適合できているかについて可視化する仕組みが有効だと考える。パフォーマンスがよい部分も十分とは言えない部分も、一定の形で社会に示すことで、基準遵守や改善へのインセンティブが高まり、全体の底上げにつながる。

○ 人材・技術・産業の育成・確保の強化については、人材フレームワークとも関連して、このフレームワークが様々なところで引用され、参照されている状態となり、人材フレームワークに対する社会の認知度や信頼を高めておくことが、実効性確保のために重要になると思う。それによって、人材フレームワークにそぐう人材が労働市場の中で選択され、就業とキャリアアップの機会を得ていく状態となることで、結果として我が国における人材の育成・確保が強化されていくと考える。

○ 本日の資料には、手引書の作成というアイデアが提示されていたが、フレームワーク自体の認知度アップの方法は様々に考えられるのではないか。例えば、相互参照したことがメリットになるような仕組みを講じることが挙げられるのではないか。

○ フレームワークという手法は、人材にとどまらず技術や産業の育成のためにも有効な手法となるのではないかと思うが、いずれにせよ策定して終わりではなく、それらを行政プロセス、施策実施のプロセスにどのように位置づけていくかが極めて重要である。

○ サイバー攻撃は、最終的には国家安全保障とか経済安全保障につながり得る話でもあるが、その発端は数多くある犯罪との境が見えにくいところがある。すなわち、単なる身代金目的でのランサムウェア攻撃なのか、国家的な意図を持った攻撃なのかということが、現実空間での攻撃のように容易に区別できない。

○ そういった中で、警察におけるサイバー犯罪捜査が果たす役割は非常に大きいと考える。これが今の体制で十分なのかについて、成長戦略の中で考慮が必要になってくるのではないか。

○ レジリエンスの強化については非常に重要で、復旧をいかにスムーズにやるかというのが大事なポイントであるから、集中的にサポートすべきである。重要インフラ事業者では、自然災害からの復旧などを通じて、復旧のノウハウが企業文化としてたまっていると思う。これをうまく明文化して、広く産業界に出していくことが非常に有益なのではないか。また、そういうことを行う人材をしっかりサポートする取組が必要である。

○ 現在は AI エージェントを使ったサービスの開発競争に突入している状況であり、一般に新しい技術が普及する段階は非常にセキュリティリスクが高まるタイミングでもある。よって、近々AI エージェントのセキュリティリスクが問題になるような事案が多発すると想像できるが、いかに早く並行してセキュリティ対策を考えて、成長戦略に大事な AI の活用を阻害しないようにすることが非常に大事である。

○ 人材育成に関しては、セキュリティはいろいろな分野との境界領域にあるものである。例えばフェイクニュースなどの問題では認知科学や心理学、経営問題となると経済学と

セキュリティというように、別の分野をまたぐような人材をつくっていくことが非常に大事である。

○ 成長戦略においては、サイバーセキュリティ戦略の中身、掲げられた施策の中で重点的なものを強調していくという方針に賛成である。
○ 資料の８ページに社会全体のサイバーセキュリティ及びレジリエンスの向上という項目があり、この項目はあらゆる産業やあらゆる企業をカバーしていると思っている。この中では大きな項目として「政府」「重要インフラ等」と「それ以外（一層の対策が必要な分野)」と整理されており、「それ以外」の部分に中小企業や大学や自治体が念頭にある整理だと理解している。
○ 産業界の立場としてサイバーセキュリティに関する施策を見たときに、自社自身が重要インフラ事業者、基幹インフラ事業者であれば、「重要インフラ等」の施策を、自身が中小・スタートアップであれば、「その他」の施策が適用されると理解できる。一方で、例えばAI・半導体、合成生物学・バイオ、防災・国土強靱化、創薬、マテリアルといった、重要インフラ、基幹インフラに指定されていないが、日本経済の成長を支える産業分野においてどういう受け止め、反応をされるかというところに留意すべきである。重要インフラ並みの取り組みを求めてもよいのではないか。

○ 「一層の対策が必要な分野」の部分で、資金や人の関係で難しい部分の底上げが必要ではないか。人と知識とお金の共通化を意識的に行うべき。セキュリティを整備するというのは競争分野ではないから、個別に対応するのではなくて、お金と人を共通化してやっていく、ということを、もっと徹底するような形になるといいのではないか
○ 人材フレームワークについて、レベル４のところは確かにこのとおりなのだけれども、業務の最終意思決定の責任を負う人とスペシャリストはもしかして違うのではないか、と思っている。
○ 組織内に必ずいなければいけない人材と、外部にあって必要に応じて外部受託でもよい業務とがあると思われ、例えば捜査などは企業の中に常にいる必要はないと思われる。むしろ横断的に見ていたほうが知識としては上がる。そういったことから、組織内にいるべき職務と、むしろ横断的に組織の外にあったほうがいい職務を整理すべき。組織外にあったほうがいい職務がまさに共通化してやっていける部分となる。

○ 人材フレームワークは、「組織特性に応じてどのような人材像が必要なのだ」といったところまでモデルケースをつくっていくということで、非常に重要。一方、こういったフレームワークは大規模な組織の専任チームの目線で作られており、整理されているものの必要なロールやスキルがあまりに多い。実際は、１人しか情報システム担当がいない組織が日本のボリュームゾーンだと思うので、そういった人たちが実務の中で何からやらな

くてはいけないのか分かるようなものも整備いただきたい。

○「攻撃者にコストを負わせる」という点に関しては、企業の規模や業態に応じてどういったコストの負わせ方をするのかというモデルケースをつくっていくといいのではないか。例えば、重要インフラに対する攻撃への対策としては、IT と OT の分離、徹底したレッドチーム活動等になる。ランサムウェア攻撃のリスクが高い場合は、スレットハンティングをして監視に生かす、横展開をさせない等になる。IT ベンダーであれば、サプライチェーンの中で被害の起点にならないようセキュリティ・バイ・デザインや速やかなパッチの適用が重要となる。そういったカテゴリーで整理をしていくといいのではないか。

○ 中小企業は助成金だけでは何ともし難いようなところが多いと思う。対応にはすごくコストがかかるのではないか、対応が難しいのではないか、と思って尻込みしてしまうのではないか。実査には無償で使えるようなツールもあり、導入もそれほど大変ではないということを、分かりやすく積極的に表現してくれているコンテンツが少ないので、そういったものを作成し、啓蒙していく活動を積極化していくべきではないか。

○ 危機管理の観点に近いところから、サイバーセキュリティに関して考える際、それと一体的にデータの安全性についても考えるべきではないか。サイバー攻撃を未然に防ぐために必要なものであり、インテリジェンスの観点でも必要であり、また越境弾圧のようなことを防ぐ意味でも必要かと感じているところ。

○ 実際に、他国がどのような法制度等を通じていかにして自国にデータを収集するシステムを整備しているのか、それに対してどのような点に気を付けるべきか、といった議論がされている。

○ データの安全性というものに関して人材育成、調査をしていく必要があるのではないか。それから、誰が何に気をつけなければならないのかということを調査に基づいて整理をし、広く社会と共有するような、そういった仕組みが必要ではないか。

○ ピンポイントに重点的施策を行うという観点から、「一層の対策が必要な分野」におけるサプライチェーンや中小企業等における効率的・効果的なサイバー対応の推進が特に重要ではないか。

○ サプライチェーンや中小企業の対策を推進する既存の施策としては、DX 投資促進税制であるとか、IPA のサイバーセキュリティお助け隊サービス、あるいはデジタル化・AI 導入補助金制度などの制度が整備されており、これらの周知や普及を図るために商工会議所などが利用されているが、サプライチェーンがこれらの制度を利用することによって、大企業である発注者や委託者にとっても何らかのメリットを生じるような仕組みによって効率的な普及を図ることが必要ではないか。また、既存の利用者の声を集めて制度のブラッシュアップを図ることも改めてお願いしたい。

○ IPA のサイバーセキュリティお助け隊サービスは、中小企業以外にも、例えば医療機関

などへの活用を検討してもよいのではないか。

○ 人材フレームワークについて、非常によく練られた内容だと感じる。追加するならば、サイバーセキュリティに関する仕組みの陳腐化を防止し、アクティブにスキルを生かすことができる人材を常に確保できる制度が必要だと考える。学び直しの機会を提供し、その利用を促す仕組み、あるいはフレームワークで定性的に評価する制度を加えていくことで、このフレームワークの持続可能性を高めていくことが肝要ではないか。

○ 社会の重要なインフラを止めないよう、レジリエントにするにはどうすべきか、早急に喫緊に具体的に考えていかなければいけない。DX が進展していくことで、制御システム、IoT 等非常に多くの設備が標的になってきている。中小企業の経営者側からすると、そこにどう限られた資源、人・物・金をかけていくのかというのは非常に大事な課題。このセキュリティ対策レベルを技術的に向上できるまで伴走して支援できるような仕組み、かつ持続的に継続できるような仕組みが必要になってくる。

○ 技術のエコシステムという点について、製品等の国産化が非常に大事である一方、AI にしてもセキュリティにしても全てが国産化できるわけではない。グローバルに広がっていくサプライチェーンもある中、現実を見据えた対応が必要である。そういった点から、海外製品を排除するだけではなくうまく利用し、依存しすぎないよう、重要なポイントを国産化するといった両輪の考え方が大事である。こうした中で、国内技術を育てる仕組みを進めるべき。

○ 日本に対する攻撃が非常に多く来ている中、それを網羅的に収集・把握し、重要インフラを守るような製品づくりに活かすスキーム構築ができればよい。例えば国産製品の強化にどのような情報が必要か等、何が必要かという議論から始めて、データ基盤、アーカイブの構築、あるいはこうした分野の成長に資するエコシステムの構築を図ってはいかがか。

（4）川崎内閣府大臣政務官挨拶

○ この後、事務局のほうでこれをまとめていただくと思うが、今日の委員の先生方のお話を踏まえると、自助・共助・公助というステージで物事を考えていただいたほうがいいのではないかと感じた。

○ 自助に通じる事例の必要性については委員から言及があった。公助、つまり国ですべき事項との場合分けについて、例えば暗号資産では、多額の資産が流出したときには当該分野の協会として対応していたことが挙げられる。こういった事例も参考に自助・共助・公助という軸でまとめてもらうことも考えられる。参考までに検討してほしい。

○ 人材フレームワークについてはすごくいいものだと思う。日本ネットワークセキュリティ協会では NICE や IPA のまとめたものを軸に「SecBoK」をつくっており、これが今回の手引書と通ずるものがあるのか、後日教えていただければと思う。この会議体では新し

いものをゼロからつくる余裕はないと思うので、もし既にある「SecBoK」が機能するという判断ができるのであれば、それを活用することも１つの手なのではないか。

（５）松本サイバー安全保障担当大臣挨拶

○ 今日は皆様、お忙しいところをお集まりいただき感謝。

○ サイバーセキュリティ戦略を具体化するのが、この分野横断的課題の一番のポイントだろうと思う。戦略そのものは昨年つくったが、それを具体化する作業はやらなければいけなかったので、この成長戦略の分野横断的課題の中にサイバーセキュリティが入ったことは、ある意味、機を得たり、といったところがある。戦略 17 分野はどれも国益をこれから考えたときに非常に重要で、どの分野もサイバーセキュリティをやっていなければ止まってしまう、あるいは大事な技術が抜かれてしまう等、いろいろな障害が起こる。我々がここでやろうとしていることは 17 分野を下支えする非常に重要な部分を占めているのだということは、既に皆さんの御認識は一致していると思う。より一層実効性の高いものをつくっていかなければいけないのだということで、ここは我々も心してやらなければいけない。

○ 複数年予算で資金あるいは人をしっかり投入しないと駄目だというのはおっしゃるとおり。高市政権は分野によっては複数年度の予算をちゃんと立てると明言をしており、これは来年度予算の構成からしっかりとやる。この分野横断のサイバーセキュリティは絶対にそこの中に入っていかないと駄目なので、スタッフの皆さんもロジックをしっかり組み立てて、複数年度で予算を立ててもらえるように、人がちゃんとつくようなロジックを立てて進めていかないといけない。これは 17 分野を支えるためにもどうしても必要だというストーリーになると思うので、ぜひお願いしたい。

○ AI によるサイバー攻撃がこれから主眼になってくると思う。AI でどう防御するかが大事で、これはある意味、17 分野の AI・半導体の分野のところにも共通するのだが、我々としても AI によるサイバーセキュリティをどうしていくかというところは、もう少し掘り下げて皆さんの御意見を伺いたい。

○ もう一つ、中小企業についてである。どんなに基幹インフラを一生懸命守っても、サプライチェーンにぶら下がっているのは、最後には中小企業である。そこで、中小企業防衛に関して、戦略の中では集団的防御ということで、サプライチェーンの集約点、結節点になっているところを防御しようとなっている。これについて例えば、各企業で CIO を置くなどは絶対に無理であるから、業界かあるいは地域か、そういったところで CIO を共有して、回りながらチェックするとか、ほかにも集団的にやる方法は幾つかあると思うので、そういったアイデアをぜひ委員の皆さんには出していただければと思う。AI と中小企業は具体論の柱になるものではないかと思っている。ここでの取りまとめに向けて、そういったところをもう少し掘り下げて御意見を伺えればと思う。

○ 改めて、本日は長時間のご議論に感謝。

（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