サイバーセキュリティ推進専門家会議 第７回会合 議事概要

1. 日時：令和８年６月１５日（月）９時00分～12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 （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
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（オンライン出席）
神保　謙	慶應義塾大学総合政策学部　教授
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	一橋大学理事・副学長、法学研究科教授（オンライン出席）
星　周一郎	東京都立大学法学部 教授（オンライン出席）

（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
大村　真一	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）
小久保　勝之	内閣官房内閣参事官（国家サイバー統括室）
杉本　貴之	内閣官房内閣参事官（国家サイバー統括室）
雲田　陽一	内閣官房内閣参事官（国家サイバー統括室）
積田　北辰	内閣官房内閣参事官（国家サイバー統括室）
庄司　周平	内閣官房内閣参事官（国家サイバー統括室）
間仁田　裕美	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）
小澤　亮二	内閣官房内閣企画官（国家サイバー統括室）

（関係府省庁）

柳瀬　護	金融庁統括審議官
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
三田　一博	総務省サイバーセキュリティ統括官
原口　剛	厚生労働省政策統括官（統計・情報システム管理、労使関係担当）
野原　諭	経済産業省商務情報政策局局長
長井 総和	国土交通省政策立案総括審議官

4. 議事概要

（１）松本サイバー安全保障担当大臣挨拶

○　本日はこの夏のサイバーセキュリティ戦略本部の取りまとめを予定している中、その検討案について御議論をいただく。

○　また、Project YATA-Shieldというミュトス関係の対応策も打ち出しているところであり、その報告等もさせていただきたい。

○　ますますサイバーセキュリティが重要な局面を迎えているため、皆様方からの活発な御意見を伺いたい。

（２）事務局説明（サイバーセキュリティ 2026（2025 年度年次報告・2026 年度年次計画）（案）について、政府機関等の監査結果（案）について、重要インフラ統一基準（案）について）

事務局から、配付資料により説明があった。

（３）意見交換

（２）により事務局から説明された議題に関して、委員から主に以下の旨の意見があった。

○　一つは、政府機関及び独立行政法人などを対象とした監査結果について、結果を拝見すると、まだまだ基本的な対応について浸透し切れていない状況が明らかになったように思う。こうした監査の扱いは、例えば「外部起点についての問題などはおおむね発見されなかった」とあるが、おおむねで安心するのではなく、発見された幾つかの細かい問題点についても、完全になくしていく姿勢が重要だと思う。また、この結果を基に改善のために必要な助言を行うということであるが、果たしてそれで必要十分なのか、今後、重要インフラ統一基準の施行に向けてより強力な是正を求める形も検討していく必要性を感じた。

○　二つ目は、政府機関等の対策基準策定のためのガイドラインについて、改定事項の脆弱性対策の箇所に、「迅速な適用が必要な場合、情報システムの運用を一時停止することも検討する」と記載があった。これは非常に重要なことだと思っている。今回、ミュトスなども出てきた中で、ある大手銀行の関係者などは、「自分たちのシステムに穴が見つかった場合は、システムを一旦ダウンさせても、やるべき解消を実施する」と話しているとのことである。銀行業界全体にシステム停止は悪という固定観念があったが、それに捉われずにやる必要があると危機感を述べていた。今回、ある意味ミュトスのおかげで、一般にもサイバーセキュリティに対する危機感が広まったと思っている。政府機関だけではなく、一般の企業に対しても、脆弱性の早期発見・対応においては、一時停止をしたり、銀行のシステムを止めたり、公共交通機関を止めたりすることも辞さないとの発信を政府からしていただきたい。政府、関係機関、事業者などの意識改革、さらに一般の人たちの意識改革も進めていく良いチャンスだと思うため、ぜひそのような発信をしていただきたい。

○　サイバーセキュリティ2026（案）について、非常によくできており、内容に異議はない。取りまとめいただいたことに感謝申し上げる。第４部は、2025年度のサイバーセキュリティ関連施策の取組実績及び今年度の取組は調整中ということで、これから公表されると思うが、ぜひしっかりしたものを公表していただきたいと思う。ミュトスなどの高性能AIの登場などに見られるように、この分野での技術発展は日進月歩であるため、これに対応するような努力を引き続きよろしくお願い申し上げる。

○　政府機関等の監査結果（案）について、マネジメント監査、ペネトレーションテスト、レッドチームテストの３種類の監査がいずれも順調に実施されている点は、評価されるものだと思う。他方、独立行政法人に対するマネジメント監査において、過年度と同様の問題点が指摘されている点は留意すべきところもあり、実施とその後の対応について十分な配慮が必要ではないかと思う。今後、レッドチームテストが独立行政法人等にも実施されると思うが、適切に準備を行うことが求められると思う。

○　重要インフラ統一基準（案）について、この案がパブリックコメントに付され、建設的な議論が行われたことは大変有益だと思う。そこで受けた意見を踏まえて作成されたことは高く評価したい。なお、前回の第6回CS推進専門家会議において提出された重要インフラ統一基準（案）では重要インフラに郵便分野が追加されていなかったため、この点についてもう少し丁寧な説明が必要であったように思われる。
○　そのうえで、重要インフラ統一基準の中身について３点申し上げる。
○　まず重要インフラの定義について、サイバーセキュリティ基本法や今回の重要インフラ統一基準（案）、これまでの重要インフラの情報セキュリティ対策に係る行動計画や国家サイバー統括室のウェブ上での定義については、やや違いがある。事務局の説明では内容に違いはないとのことであったが、定義は独り歩きするため、齟齬がないよう整理をお願いしたい。
○　２点目は、新たに追加された郵便事業には、日本郵政の郵便事業が該当するという説明をいただいたが、信書便事業者が行う信書の送付も含まれる必要はないのか。もしここに含まれないとすれば、それは物流というカテゴリーに含まれることになるのか。それが経済安全保障推進法で言う基幹インフラの定義とどれだけ整合的なのかどうかということについても、引き続き検討をお願いしたい。
○　３点目は、重要インフラの内容も対外的に明確にし、主張していく際の他の外交上の文書との整合性の問題である。重要インフラの英語名はクリティカル・インフラストラクチャー（critical infrastructure）であるが、この文言はこれまで日本が締結した五つの経済連携協定の中に含まれている。2002年のシンガポールとの間の経済連携協定、2008年のASEANとの包括的経済連携協定、2011年のインドとの包括的経済連携協定、2020年のRCEP協定、そして、2026年の日本とバングラデシュとの経済連携協定である。対外的に重要インフラを説明するのであれば、とりわけ国内法では基幹インフラと区別した定義が設けられていることからも、これらの対外的な協定の定義との関係を適切に整理しておくことが、その説明のためにも必要ではないか。

○　１点目は、サイバーセキュリティ2026について、内容を拝見して、関連施策が着実に進行しているということをまとめていると思った。資料の中には、サイバー対処能力強化法等の着実な実施と書いているが、これは文字通り着実に実施をしていただきたいと思った。一方、サイバーセキュリティの脅威の状況に対して、即時的・緊急的な対応が必要となる場面も多くあるのではないかと思う。法律の施行日を早めることはできないのはもちろんであるが、可能なことは可能な時点から着手し、機動的・弾力的に必要となる施策を考え、躊躇なく実施するルートを確保していくことも必要ではないか。全体としての法制度のフレームを崩さないように、必要な場合には事後に実施された施策を法律の仕組みの中に位置づけて取り込んでいく、そういう方策も必要になると思った。

○　２点目は、監査について、具体的に立てられている実施の基本方針の中には、監査結果の報告は、攻撃者を利することにならないよう配慮した形で取りまとめるものとされており、現在の内容はこれに配慮した報告となっているとお伺いしているが、監査の適正性を確保することからすると、監査の方式や項目自体、または対応の在り方などについても、見直し・改善を考えていく必要があるのではないか。今回御説明いただいたものは、従来のフォーマットどおりだと思うが、報告の内容や項目についても、監査制度そのものを改善するという視点から見直しをするといった検討も進めてみるとよいのではないか。簡潔に言えば、今後のよりよき監査のために、監査の今後の在り方自体についても、継続的に、つまり複数年度にわたる形で分析を進めてはどうかということである。歴年の報告のデータを並べてみると、新しく見えてくるものもあるのではないかと考えた。

○　３点目は、統一基準（案）のパブリックコメントの結果を見て感じたことである。まず今回の統一基準（案）に関するパブリックコメントを実施し、統一基準（案）に必要な改正を加えていただいたことに感謝を申し上げる。今回、コメントの中には、その他という項目に、必ずしも統一基準（案）に関するコメントではないものもあった。制度全体の改善のための意見も複数含まれていたと思う。既にお計らいいただいているかと思うが、そのような意見も大切にして、制度全体の向上に結びつけていただければと思う。

○　全体としては大きな異論はないが、コメントが一つと、質問を二つしたい。

○　一つ目、レッドチームテストをやっていただいたのは本当に良いことだと思う。ご存じのとおり、1997年にエリジブル・レシーバーというアメリカ政府の非常に大きなレッドチームテストで、アメリカ政府が簡単に陥落してしまったことがサイバーセキュリティ施策を考えていく大きな転換点だったと思う。その面では、このようなことを積極的にやっていくべきだと思うが、NCOの能力を疑うわけではないものの、本気のプロに攻められて、本当に落ちないのか、少々疑わしく思う点もあった。その点で、本気のプロに頼むととどうなるか興味がある。本当にそれで守られているのであればすごいことだと思った。

○　質問の一つ目は、監査の指摘事項に、「無許可のウェブメールを利用した」というのはやはり気になる。恐らくGmailか何かだと思うが、このようなサービスは便利なため、多く利用されている部分だと思う。どのような状況でどのように利用されていたのかを教えていただきたい。

○　二つ目の質問は、GSOCは10年以上存在していると思うが、現在の体制と、どのような方が対応しているのか、差し支えのない範囲で教えていただきたい。また、アクセス・無害化措置が始まった際に、GSOCはどういう役割を果たしていくのかも若干気になっており、別のチームが対応するということなのかもしれないが、情報共有はあ

る程度必要だと思うため、そのあたりの役割について聞きたい。

○　今日御説明いただいた資料について、いずれも賛同したいと思っている。
○　監査関係だが、資料について幾つかコメントをしたい。マネジメント監査を丁寧に行っていただいており、その結果をより効果的なものにするために申し上げたい。
○　1点目は、独立行政法人等について、ISMAP未登録サービスや未許可のWebメールなどが使われている指摘事例が多いということであった。なぜそれが使われるのかの真因分析、「便利だから」や、「関係する事業者で使われている」など、何か事情があると思われるため、その真因分析をし、適切なセキュリティ要件の指摘を行った上で、適切なサービスが選ばれるよう促進していく必要があると考えている。
○　２点目は、ISMAP未登録サービスについて、統一基準でいうと、ガイドラインの第４部に指摘が集中しているようである。独立行政法人等のシステムの運営については、どうしても委託先任せになっているのではないかについても考慮が必要と思われる。
○　3点目であるが、全部で96法人の対象先がある中で、３年に一度のサイクルで、34法人について監査いただいたとのことであった。１年を通じて監査ができる法人数は限られるが、監査のPDCAのサイクルをより効果的なものにするために、残りの62法人についても、ほかの法人であったような問題点も含めて呼びかけをし、自主的な点検を進めてもらう形での助言をいただくことが望ましいのではないか。既に実施されているかもしれないが、改めて申し上げる次第である。
○　また、クラウドについて今回丁寧に見ていただいたと思うが、クラウドとともにAIの利用についても、同様の利便性を追求するあまり、許可されていないものやセキュリティの要件を充足していないものが利用される懸念がある。デジタル庁にて、生成AIの調達に関してのチェックシートが整備されているため、それに準拠した形でサービスの選択が行われているかについても、今後、点検の対象にしていくことが望まれるのではないか。

○　監査結果について、政府機関と独立行政法人等の指摘事項は、１位が主体認証、２位が脆弱性対策で、非常によくあることであるが、かなり基本的な指摘がされているという状況は変わっていない印象を持った。もちろん事情があることは分かるが、ここはかなり力を入れないと、今後非常に困る面でもあると思う。ご案内のとおり、政府全体の情報システムもゼロトラストの考え方に持っていく動きがあるが、これは主体認証が回っていること、脆弱性対策できていることが大前提になって初めて始められるものである。これらがあるレベルに達しないと、その方向には進みにくいということが基本ではないかと思うため、単に監査の結果だけではなく、改善のために何かNCOの方からできることがあれば対応頂けないかと思った。
○　またサイバーセキュリティ2026だが、こちらもよく取りまとめていただいた。やはり

今、AI絡みの動きが非常に速いことが気になった。半年後どうなっているかよく分からない状況の中で、「年1回この手の計画を作り、今年度これをやる」というペース感だと間に合わないような事態が発生するのではないか。その時にどう対応するのかが、もう少し強めに出ても良いのではないかという印象を全体として受けた。もし付け加えられること、運用の中で対応できることがあれば、心がけていただきたい。

○　監査結果に関して、２点コメントさせて頂く。監査結果を踏まえて、今後、各省庁や独立行政法人で基本的には自己対応することが想定されると認識している。しかし、対応は、今回のみならず、常時する必要があると思うため、組織内部のセキュリティ担当がもう少しプロアクティブに組織内部のセキュリティ対策に関与できないかと思った。ウェブメールのようなサービスの利用に対しては、転送設定がされれば内部のセキュリティ担当でチェックができるはずだと思う。内部のセキュリティ担当者がそのような動きを常時チェックし、自己申告がなくても修正させるような関与が必要ではないか。

○　２点目は、常時使っている様々な機器などに関して調査をされたかと想像するが、日本国内でも、出張時に使うようなSIM、レンタルWi-Fiに脆弱性のあるものが多く見られるようになったと思う。そういった機器に関しては調査の対象とされたのか。もしされていなければ、今後ぜひそこについても対象に含めていただきたい。

○　監査結果について、レッドチームテストは私たちも何年か実施しており、防御にもかなり投資し、レッドチームのテストも高額な費用をかけているが、昨年ここまで対策したのにも関わらず今年また侵入されるといったことを繰り返しているのが実態である。マネジメント監査で、「認証機能に問題がある」、「脆弱性に問題がある」、と見えている中で、資料にある「インターネットから直接侵入されるような問題等は発見されなかった」というのはかなり違和感がある。今回のテスト運営はNCO単体で行われたのか、委託されたのか不明だが、監査の際は委託先の実力、計画の妥当性や、計画段階のところも見て頂ければいいのではないかと思う。演習の制約で、本物の攻撃者が使う手法を一部禁止していたり、影響がでる可能性がある攻撃を禁止しているような前提を積み込んだ計画になっていると、本来見つけるべきものが見つけられなくなるため、そういった観点でも監査いただけるとありがたい。

○　サイバーセキュリティ2026について、AI時代の急激な変化にどう対応していくのかは難しいが、良いと思ったのはAI時代においても、最後は人との関係が頼りである。その意味では、国際会議などに幹部が参加し、自ら直接的に発信・交流することは非常にすばらしいと思う。このような取り組みはぜひ大事にしていただきたい。

○　議題１と議題２に関わるが、サイバーセキュリティ人材フレームワーク2026がまとま

ったが、これはあくまでも出発点である。本番はこれをいかに活用して政府で人材に関わる実務を進めていくかがポイントであるため、そこはお願いしたい。

○　政府機関監査は気になるところが多くあった。まずテストのカバレッジだが、全部を実施するのは非常に大変なのは理解している。ただ、見つかった問題や対処したものは、ほかの未実施のシステムにとって有益なはずである。業界ではISACをつくって横連携をしているが、同じことを政府の機関間でやっていただかないと、レッドチームテストが一巡する間に攻撃されてしまうということになりかねない。ぜひ横展開をお願いしたい。

○　それから、重要インフラについては、有益な連携が可能なので良いと思うが、意見の多くはこの先にあるガイドラインの中身でどう対応していくかであるため、ガイドラインの作成チームの方にはこれをしっかり受け止め、ガイドラインに反映していただきたい。

○　追加で監査について、資産台帳は非常に大事だが、世の中では台帳に載っていない、いわゆるシャドウITが問題になる機会が多い。そういうものを探す取組は省庁の中で行われているのか。民間では抜き打ちの身体検査に近いところもあるやに伺っており、出口のところを全部監視して端末をチェックすることも可能だと思うが、そのあたりは対策をしているか。

○　非常に詳しい説明で、心強い思いもした。

○　監査について、１点だけコメントさせていただく。「政府機関等の対策基準策定のためのガイドライン」の改定事項について、最初に脆弱性が記載されているが、他方、監査結果の指摘事項の２位がソフトウエアに関する脆弱性対策ができていないということは、少々気になる。単純にパッチを当てればいいはずのものが、当てられていない背景であるが、以前、「他の機器との整合性が合わなくなるため、簡単にアップデートできない」とのお話を伺った。そのような背景があるとすると、簡単にパッチを当てられないという事情があることになり、無理をしてもなかなかうまく回らないということになる。そのため、機器全体の更新が必要ということになる可能性もあるが、その背景も含めて御検討いただければよいと思った。

○　重要インフラ統一基準については、評価制度と整合性を取って進めていただきたいということと、監査に関しても、ここで指摘された五つのポイントについて、ベストプラクティスなどについていろいろとつくっていただけるのではないか、監査結果は報告のみで終わらず、そういう使い方をしていってはどうか。

これら委員の意見に対して、NCO事務局から以下の旨の発言があった。

○　レッドチームテストに関しては、担当者に対してテストを行うことを事前に伝える、

伝えないといったテスト実施に関する事前告知の有無を含め様々なシナリオを前提に行っている。

○　監査のカバーリングの件について、システムは省庁だけでいうと、1,000を超える多くのシステムを持っている。私どもが１年間で実施できるテスト数は数十件程度であり、全体に占める割合は非常に少ない。この制度が始まって約10年となるが、国家サイバー統括室としては、監査結果の横展開をし、対象となるシステムだけではなく、各省が管理するシステム全体に横展開をしていただくために、担当者クラスの勉強会や、高い役職者が集まる会議を活用し、今回示した監査結果について、トップに現状を知ってもらい指揮を執っていただくという、上からも下からもという形での指導をしている。各府省の内部監査において、結果を横展開する方向で取り組んでいるところである。

○　出張時の端末等も監査の対象であるかという点について、各府省においては、システム管理台帳を整備しており、私どもの監査はシステム全てが台帳に載るという制度になっているため、台帳に載っているシステムについては確認をしているところである。そのため、出張時に使っているシステムに限らず、監査の対象としている。また、ウェブメールについては、改善を求めているところである。主体認証や基本的な事項の指摘が多く確認できているところである。AI時代においても、基本的な事項が守られて、初めてシステムの運用が安全にできると認識をしているため、基本的な事項をまず徹底していただく方向性で各機関が改善に努めていくよう、国家サイバー統括室としても寄り添って対応しているところである。

○　GSOCについて、主には府省庁からの出向者で対応している。アクセス・無害化措置との関係について、国家サイバー統括室では、GSOCが監視・インシデント対処している政府のシステムだけなく、重要インフラも含めて、日本を対象としたサイバー攻撃等の情報を集約して対処している。この集約した情報を国家サイバー統括室全体として集約・分析をした上で、アクセス・無害化措置等を行うこととなる。国家サイバー統括室全体で、情報共有をしながら対処する仕組みとしている。

○　監査に関連し、もともと政府統一基準というもの自体、ベースラインになっているところあり、ベースラインを満たしているかという基礎的なチェックが中心になってしまう点はご容赦いただきたい。そのうえで、先ほどウェブメールに限らず、ISMAP対象外サービスのお話があったかと思う。ISMAP制度は手間暇がかかる制度であるが、ようやく昨今、103サービスが登録されるようになり、ISMAPの中から多くのサービスを選択していただけるようになったところである。一方、ISMAP登録のためには一定の金額がかかるため、サービス規模があまり大きくないものや、新しいサービスは間に合わないというところがある。政府統一基準に照らし、そのような場合にはISMAPと同等であることを各政府機関等で確認をしてもらう運用になっているが、簡単ではない。そうしたこともあり、こういった規模が小さなサービス、あるいは最先

端のものが比較的簡単に登録できるようなISMAPの新しい制度をつくるべきだということで、今、作業をしているところである。当然ある種の簡便なものになるため、正式のISMAPに比べるとセキュリティ的には一段落ちるかもしれないが、最低限のセキュリティは確認されているとのことで、現状よりはよくなるのではないか。この簡便な制度と本格的なISMAPで、２段構成にしたく、制度改正を考えているということだけお伝えさせていただく。

○　監査に係る報告書の中でも触れているが、昨年９月に会計検査院がシステムに関する調査を行っており、公表もされている。その中でも台帳の不備というのは多くの指摘事項となっている。また、私どもが行う監査においても、同様の監査結果となっているところである。これらを踏まえた対策については、我々の監査の結果を踏まえ、各府省にはしっかり管理していただくという点で要望をしているところである。この点については、私どもの監査の中でしっかりとフォローさせていただくとともに、会計検査院の結果についても、３月に一旦フォローアップさせていただいたが、進捗が進んでいない組織もあるため、今後、半年に一遍のペースで指摘の改善も含めた確認を行っていく予定である。

○　監査結果や、あるいは最近のインシデントの事例に基づき、政府機関の場合は外局や、地方支分局について、しっかりとチェックをするよう要請している。必要があれば、NCOとその部局の間で具体的な改善に向けた取組について綿密な打合せを行い、定期的にフォローアップしている。どの組織でも完璧というのは難しいが、できる限り漏れがないようにさせていただきたい。

（４）意見交換の後、「政府機関等の監査結果（案）について」の議題に関して、サイバーセキュリティ基本法に基づく本推進専門家会議への意見聴取事項となっているところ、本日の会議を踏まえ所要の検討・調整等を行った上で、必要があれば事務局と後藤議長で調整等を行う等、その取扱いについて後藤議長に一任することで、了承された。

また、「重要インフラ統一基準（案）について」の議題に関して、サイバーセキュリティ基本法に基づく本推進専門家会議への意見聴取事項となっているところ、基準（案）について異議ないことを確認し、本案をベースに作成することを了承された。

「サイバーセキュリティ2026（2025 年度年次報告・2026 年度年次計画）（案）について」の議題に関して、本日の会議を踏まえ所要の検討・調整等を行った上で、必要があれば事務局と後藤議長で調整等を行う等、その取扱いについて後藤議長に一任することで、了承された。

（５）事務局等の説明（脅威ハンティングの普及促進・実施等に係る基本方針（案）

について、大阪・関西万博の振り返りと今後の大規模国際イベントに向けた取組について、AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化について）「脅威ハンティングの普及促進・実施等に係る基本方針（案）」及び「大阪・関西万博の振り返りと今後の大規模国際イベントに向けた取組」の議題について事務局から、「AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化について」の議題に関して事務局及び関係省庁（金融庁、総務省、厚生労働省、経済産業省、国土交通省、デジタル庁）から、それぞれ説明があった。

（６）意見交換

（５）により事務局等から説明された議題に関して、委員から主に以下の旨の意見があった。

○　AI性能の高度化を踏まえた対策について、現在どのような動きをしているかということをシェアする。

○　組織について、サイバー先端部隊で一つの部に150人ほど在籍者がいるが、同部隊では対応しきれないため、関連部で対応できる人材がオーナーとなり、ほかの部の人材を動かしていくという体制を組んでいる。つまり、各部の調整を飛ばし、動かせる人材が動かすというタスクフォースを立てて対応している。実装について、構成管理などは基本的な事項とは言いながらもできていないシステムが多くある。そのようなシステムについて、従来であれば、各署との調整を経てテスト環境で検証し、本番環境で実施するステップで進めているが、今回は、一旦本番環境で実施してみることや、それぞれが分担し対応方針を考え持ち寄るなど、短期間で対応する必要があることから今までのやり方は踏襲しない形で動いている。その中で、今、一番大変なのが脆弱性のトリアージである。今までは単発の脆弱性をCVSS、範囲や攻撃の実績などを評価して個別にトリアージするという運用をしていたが、ミュトスなどが出てくると、一つ一つは深刻な脆弱性ではないが、合わせると深刻な影響を及ぼすということがある。実際、Project Glasswingに参加しているメーカーからその懸念のあるものの連携があり、急いでパッチを当てたみたいなことがあるが、短期間で実施できるものでもないため、まずは自分たちもAIを使い攻撃シミュレーション、自動レッドチーミングを行い、どのように脆弱性に対して評価をしていくのかというフレームワークのヒントとして、自分たちもAIで攻撃をしてみる、脆弱性がないということを検証してみるということをやっていきたい。今まで３年から５年かけてやろうとしたことを、１年という短期間で様々なことを並行して進めているが、良いチャンスだと捉えて取り組んでいきたい。

○　脅威ハンティングについて。能動的サイバー防御の考え方が導入されて、従来のセキ

ュリティ対策を一歩踏み込えて、脅威が顕在化する前の段階から脅威のレーダースクリーンを広く取り、能動的にこれを明らかにしていくという試みがコンセプトとして導入されるということは、大変望ましいことであろうと思っている。重要なことは新しい概念を機能させる体制を併せて作っていくということ。脅威ハンティングというのは、GSOC や、一部の高度な専門部隊だけの活動ではないということだと思う。それを可能にするのは組織的な体制としての資産管理、ログ管理、リスクアセスメント、そして、その後のインシデント対応という基本的対策と一体で普及させる必要がある。つまり脅威ハンティングをうまく機能させるための組織体制が重要だということだと思う。今日いろいろと伺った話で、仮に新しい体制で実施したときの実施件数と、兆候が把握できた後で何をするのかという、次のステップをセットで考える必要があると思っており、その際の経営判断、政府への報告、他組織への注意喚起、ベストプラクティスを共有する仕組みを脅威ハンティング全体のスキームとしてどう整えていくのかということが大変重要だと思う。可能であれば、この会議で、脅威ハンティングを導入した結果、一体何が変わったのかというレビューが定期的になされ、さらによいプラクティスが何かという、その仕組み作りを考えていただければと思う。

○ フロンティアAI性能の高度化への対応について、本件に係る 4 月の報道以降、数週間で政府が基本方針を全省庁的に取りまとめるというスピード感は大変重要なことであり、政府全体の危機感が大変伝わるものであった。危機感を攻撃者や国際社会もよく見ているので、このスピードと体制が整えられているということ自体、非常に重要だと思っている。しかし、高性能AIに関して、新たな動きが今後数か月、半年以内にも相次いで生じることが想定されるときに、基本的には脆弱性を発見してから対応するまでのスピード、そして、体制を整えていくという方針は正しいと思う。今後は、仮に既存のフロンティアAIと同等の性能を持つAIモデルが、我々の知っている大手フロンティアAI企業以外からも出てくる時代になった際に、「既存の対応で間に合うのか」、「対応は可能なのか」という、さらに次のフェーズの対策をいろいろな形でブレーンストーミングをしておく必要があるのではないかとの問題提起をさせていただく。

○ 他の委員からもはなしがあったが、Project YATA-Shieldについて、バランスの取れた取組が示され、全省庁が一斉に動き出していることは素晴らしい。一方で、「優先的に対応する脆弱性を選べる・取り上げができる」、「パッチ適用を実際できる」、「サービス優先度を考えられる」人材は日本ですごく限られている。そのため、全省庁が一斉に動き出すことで人材の取り合いになることに危機感を覚えており、このような状況であることを強く認識いただきたい。今すぐやれることは限られているため、中長期でリスクが高い状態が続くという覚悟が必要だと考える。その意味で、いわゆるレジレンスの考え方で準備する必要があると全体として思った。

○ また、Project YATA-Shieldについて、短期的取り組みと、中長期的取り組みにメリハ

リをつけて表現いただくと、国民にも伝わりやすいと思った。

○　Project YATA-Shieldを迅速に取りまとめたことはありがたく思う一方、英語の発信見当たらない気がしている。今はXなどでも、そのまま日本語の投稿が英語になるため、日本の取り組みをぜひ海外に発信していただきたい。発信することで、攻撃者に「日本への攻撃はコストがかかる」という姿勢を取ることができるため、各対策も含めぜひ英語でも発信していただきたいと思う。
○　また、人材育成に関する対策について、恐らく「対応できない」という現場からのSOSだと思う。直接「うちでは対応出来ない」と言えないため、言い方を変え表面化するところがあると思う。その場合、現状いる人材をどう最適配置するかという発想にならざるを得ないと思うため、その観点を少し強めに言って頂きたく思う。

○　監査について、他の委員が指摘したシャドウAIという実装的課題について、基本の徹底が重要との認識が示された点は、政府内での改善につながるものと期待している。そのうえで後半のAIについて、脆弱性の発見から悪用までの期間短縮を踏まえ、パッチ管理に焦点を当てた点を評価する。一方、パッチ公開そのものが攻撃者の解析材料となりうるとの指摘もあり、AIによるエクスプロイト化が加速する中では、パッチ適用の迅速化を大前提としつつも、速度で追いつけない領域や適用できない領域が残ることも踏まえた評価が論点となる。その点で、制御系や医療現場の機器など即時適用が難しいシステムは一定数あり、そうした環境では脅威ハンティングに加え、BCP・レジリエンス・ネットワーク分離・監視といった代替統制が中心的な位置づけになると考える。これらは重要インフラ向けの注意喚起においても既に方針に位置づけられており、今後の動きを期待している。脅威ハンティングに対応できない組織については、まずログを取ることから始めることが重要である。
○　そのうえで2点質問したいが、まず、脅威ハンティング等、パッチ管理以外の対策の実効性を評価対象に組み込んでいく考えはあるか。チェックリスト・アウトカム指標・CYDER等の演習活用を検討しているか。また、GSSにおいて脆弱性発見から修正提案・検証まで一気通貫でAI活用が進んでいると理解しているが、これを各府省庁の対応水準・評価基準の共通の土台として展開する考えはあるかをお聞きしたい。Project YATA-Shieldはその要となる枠組みと受け止めている。パッチ管理の迅速化だけでなく、侵害されても機能を止めない力をどれだけ備えたかという観点も評価・浸透させていくことが、政府全体・重要インフラを含めた強化の鍵だと思う。

○　ミュトスの報道が出てからの政府の迅速な対応に敬意を払いたい。また、Project YATA-Shieldをめぐる各省庁の取組も引き続き進めていただきたいと思う。こうした中、今週、フランスではG7の首脳会議が開かれ、そこではAI、サイバーセキュリティ

も議題の一つになると聞いている。特にサイバーセキュリティの分野では、ミュトスのような危険な先端モデルの提供停止基準や、国際的なAIの安全基準も検討されると聞いているが、こういった国際ルールの策定にどれだけ日本として関与していくのか。手をこまねくと米中のG2の世界に生きることになるため、日本としても規制と、民間の技術力・産業基盤の強化の両面から外交力を発揮し、ルールづくりに関与していくことが非常に大切になるのではないか。

○　さらに、こうした高性能AIに関して、安全保障的な側面から政府としての情報発信は抑制的にならざるを得ないことは重々承知している。今日の資料にある、各省庁ではどのような取組をしているのかということも、具体的な内容は非公表にせざるを得ないかもしれないが、公表可能な内容は積極的に発信した方が良いと思う。この問題に関しては、多くの事業者、国民にある程度の制約を課すようなこと、協力してもらわないといけない側面があるため、透明性に配慮した情報発信をお願いしたい。

○　脅威ハンティングの基本方針について、実施体制として警察組織と防衛省・自衛隊が出る点は、能動的サイバー防御同様、ゆくゆくは重要なポイントになる。シームレスな対応という観点から両者の連携は重要であるため、その点を強調して進めていただきたい。

○　大阪・関西万博の振り返りと関係して、今後行われるイベントに関して、主管官庁と関係団体が主宰する状況と、NCOがどのように関わるのかという問題を詰めて考えていただきたい。NCOがリエゾン的な役割にとどまり続けるのか、サイバーセキュリティ関して指示、要請を出すような、一定の権限を用いることが可能な制度を構築するのか、その点を考えていただきたい。

○　AIの話に関連して、各省庁の取り組みについて、国民にどのように伝えられるのかという点が非常に重要と思う。これは国民の協力を得るためにも重要であり、例えばマイナンバーカードを持つ国民が、どのようにこのサイバーセキュリティ上の問題に関わるのか、対して各省庁がどのように問題に対応しているのかを示すことで、国民にとって非常に身近な問題として考えやすいと思う。この観点も取り入れて強化を進めていただきたい。

○　2点質問がある。

○　一つは、脅威ハンティングに関して今回取りまとめる基本方針の位置付けは、サイバー対処能力強化法に基づく基本方針のように、法律上特定されて政府に義務付けられているものではなく、サイバーセキュリティ基本法第26条第１項第６号におけるサイバーセキュリティ戦略本部の所掌事務の一つとしての「施策の実施に関する指針」であるという理解でよいか。

○　また、施策実施に関わることであって、既存の法律で定められている義務を超える情

報共有等の新たな義務を事業者等に創設させるものではないか、確認したい。

○　脅威ハンティングの基本方針案についてのコメント１つと、NCOのリクエストを１つ、計2点を発言させていただく。脅威ハンティングの普及促進・実施等に係る基本方針（案）について、案の本文に、脅威ハンティングの活動について「十分な理解が未だ浸透していない状況」と記載されている。脅威ハンティングは能動的・積極的な政策であり、関係者の理解浸透は政策遂行の必須要素となる。そのため国全体への理解の浸透というのは、普及促進の大きな課題の一つになると思っているが、方針案を読み進めると、理解浸透・意識改革についての記載が十分に出てきていないように感じた。体制整備については記載があるが、どのように理解を浸透させるか、どのような方針で取り組むかについても、まとめた形で記載することで方針の方向性が明確になるのではないか。
○　2点目はNCOへのリクエストとなるが、現状の複雑な制度状況を踏まえ、関連政策を分かりやすく整理・見える化する工夫を講じてほしい。サイバーセキュリティの政策分野は他の政策領域と比較にならないスピードで新しい方針・取組・プロジェクトが展開されている状況と伺っている、他方、サイバーセキュリティに関わる関係者は民間にも広がっており、各関係者に制度に理解してもらうことが肝要となる。新規参入者にも制度の全体像が一見してわかるよう、個々の政策の位置付けが一目でわかり、かつ時系列での変化も把握できるような、施策の縦展開・横展開が見える立体的なマッピングの工夫を検討してほしい。ルール・ツール・規則・基準・計画等の適用関係や位置付けも含め、制度全体としてマッピングする工夫を考えて頂きたい。

○　言うまでもないが、想定外のタイミングで攻撃されることがサイバー攻撃の一番つらいところだと思う。大企業が攻撃を受けると、非常に大きなインパクトが出ることを我々は理解する時期だと思う。その意味では、オリンピックや万博では「攻撃を受ける」と分かっている中で準備をしているため、被害に遭いにくいのではないかと思った。ウクライナの事例を見ると、サイバー攻撃が意味を持ったのは、物理的な手法が始まる前後１か月だと思う。その後の３年数か月ではサイバー攻撃の意味がほとんど無くなっていると考えており、今後開催する大きなイベントに際し、備えることである程度攻撃をしのげると思う。
○　また、東京オリンピックを開催する際に、イギリスから、2012年のロンドン五輪の経験をもとにサービスの売り込みを受けたと思う。今回の万博やオリンピックでの、外国のサービスの利用実態を把握できていないが、日本のサービスを逆に売り込む機会ではないかと思う。松本大臣や飯田サイバー官には、積極的に海外で日本のサービスを売り込んでいただくことが良いと思う。
○　1点質問だが、脅威ハンティングの資料は対外非公開であることが若干気になる。もち

ろん中身を伝えてはいけないと思うが、実施すること自体は、ある種の抑止として発信すべきではないかと思う。また誰がやるのかについて、警察、自衛隊が平時から行うとの話があった認識だが、これは自衛隊が平時からやるということかお聞きしたい。

○　フロンティアAIへの対応であるが、これほどまで早く必要になるとは予想できていなかったこともあり、これまでに立ててきた人材育成プラン等が追いつかないというのが各省の状況と受け止めた次第。非常に危惧しているのは、地方への影響であり、来年度から地方版ASMを全国展開するとのことだが、各団体が個別に専門人材を確保する必要がないという意味で、早期の整備が必要だと思う。この考え方を他の分野にも応用できないかというのは、ジャストアイディアだが、例えば医療分野なども同じように多数のステークホルダーがいる中で、人材育成や、対象となるシステム資産の全貌がわからないといった、同じような悩みを抱えていると思うため、医療分野でのASM、国土交通省所管分野でのASMといったものを整備していく必要があるのではないか。
○　大阪関西万博への対応について、セキュリティのために利便性を犠牲しなければいけないことについての認識が共有できる面もあったのではないかと思う。今後も大規模なイベントが予定されている中で、今後ますます周知されることが必要ではないかと思った。

○　脅威ハンティングについて、良い取り組みだと思う一方、普及が進まない中で、率先して政府が活用方法を提示するべきだと思っており、実装に合わせた理想の姿を見せてほしいと思う。そのときに重要なのは、脅威情報を得た後の動きについて、外部委託に頼っている状況で動きが遅くなる現実を踏まえ、可能な限りリスク関係とシステムの関係が分かる人間を手元に置く体制作りが必要になってくると思う。そこを強く推していただきたい。
○　二つ目は、Project YATA-Shieldであるが、ここまで素早い動きが国にできるというのは驚きでもあったが、非常にすばらしいことだったと思う。一方で、粒度感がばらばらになってしまっているという点が気になっている。短期間でやる話と少し時間がかかること、例えば人材育成の話や、技術開発の推進の話は、今動き出しても成果が出るのはかなり先というお話になると思う。それが混ざっているのが気になっており、どのようにタイムラインを切るかという話と、整理するという話はこの後に出てくればいいと思った。あと、Project YATA-Shieldに関しても、ミュトスを契機に現れたが、ミュトスはもう問題ではなく、この後に恐らくオープンウェイトでそれなりの性能のものが出てきてしまい、それが悪い人たちの手に渡り活用される。そう捉えるのが一番重要であり、そのときにどういうことが起きて、私たちは何をしなければいけないかという、頭の体操をしなければいけないところだと思う。ミュトスばかりになり、

ほかの観点が落ちているのが気になった。

○　脅威ハンティングに関して、脅威ハンティングは脅威を未然に防ぐものであるが、フォレンジックとは異なる未知を探る技術のため、非常に高いスキルが求められ、重要インフラ企業といえども、全社が持てるようなものではないと思う。技術を持っている人材がどこにいるのかなどの情報も必要ではないか。また、このようなスキルを持った人をAI化して、利用可能とすることが必要ではないか。
○　Project YATA-Shieldに関して、官民連携と脆弱性対応における指針をこのスピードで提示するのは非常にすばらしいと思う。一方で、我々企業はサイバーリスクを低減するために守るべきデータ、脆弱性対応と脅威の低減の３要素で対応している。脆弱性対応が極めて難しくなる中では、Project YATA-Shieldの考え方を進めつつ、守るべきデータをしっかり暗号化やバックアップすること、また、脅威を低減するためのゼロトラストや侵入されても発生させない無害化や無効化の措置を施すなど、官民それぞれが役割に応じて責任を持って対処することは重要である。

○　AI性能の高度化を踏まえたサイバーセキュリティ対策の強化について、高性能AIに関して留意しておくべきこと、踏まえる点、特に注力すべきと思われる点についてコメントする。
○　１点目は、高性能AIを適用することによりリスクを意識する必要がある点について、高性能AIを適用することは、ソースコードや出力結果など、機微な情報を先方に渡すことになる点を認識する必要があること、高性能AIを適用した結果として、事業者自身の情報が外部へ漏えいする可能性があることについて、あまり考慮がされていないのではないかと懸念している。高性能AIを適用することについては、リスク面を含めて正しく理解・認識することは重要である。
○　もう一点は、各社・各セクターが高性能AIへの対応に取り組む中、共通する部分について国に音頭を取っていただきたいという点である。高性能AIに関する基本的な分析や評価は各セクターに共通する部分かと思うため、国で実施して、各セクターに展開していただくことで対応の効率化が図られるのではないかと考えている。各セクターに共通するガイドライン作成などの点で、国の一層の取組を期待する。

これら委員の意見に対して、NCO事務局から以下の旨の発言があった。
○　サイバーセキュリティ戦略本部が今回決定予定である脅威ハンティングに関する基本方針は、委員認識のとおり、第26条第１項第６号に基づく「施策の実施に関する指針」として策定するものである。また、事業者等に新たな義務が創設されるものではなく、政府の取組において、対象組織から情報提供を求める取組については、いずれも対象組織の合意を前提としたものとなっている。

○　脅威ハンティングに関する資料が対外非公開となっているのは、現時点における検討中の案であるためであり、当該資料はサイバーセキュリティ戦略本部で決定された後に公表する予定である。

○　脅威ハンティングにおける自衛隊の活用については、防衛省・自衛隊は自組織が運用する情報システムへの脅威ハンティングを既に実施している。警察も同じであるが、防衛省・自衛隊が保有する脅威ハンティングの能力を自組織以外の組織が運用する情報システムにおける脅威ハンティングへも活用することについて基本方針においても記載した。この点、国家サイバー統括室が総合調整し、警察、防衛省・自衛隊、各省庁との連携を進めていきたい。

○　脅威ハンティングに関する人材についての意見も多くいただいた。ユーザー企業である重要インフラ事業者等において、自組織の職員のみで脅威ハンティングに必要な全ての作業を担うことは現実的ではないという点については委員と同意見であり、基本方針においても、外部委託先の事業者を活用することを記載した。外部委託先の事業者を活用するためには、保守ベンダーやセキュリティベンダーの取組がビジネスとして成り立たねばならないと考えており、既にSIerやセキュリティベンダーが所属する団体において、脅威ハンティングに関する講演を行っているほか、様々な協力を進めているところである。一方、ユーザー企業である重要インフラ事業者等における人材育成については、外部委託先となる事業者を管理することが非常に重要だと考えており、基本方針においても、橋渡し人材の役割、システム部門とセキュリティ部門の連携に加えて、経営層の理解について記載した。こうした人材育成は、研修、実習や、ガイドブックの普及を通じて推進するべきだと考える。また、サイバーセキュリティ人材不足への対策として、サイバー攻撃から守る側の組織でもAIを活用する必要性があるため、脅威ハンティングにおけるAIの活用可能性についても基本方針に記載しており、しっかりと進めていきたいと考えている。しかしながら、政府内での脅威ハンティングのAIの活用については、将来的には取り組まねばならないことだと思っているものの、脅威ハンティングの普及が十分にできていない現状においては、脅威ハンティングの普及を優先すべきだと考える。

○　脅威ハンティングが普及していないことについて、意識改革の必要性が委員から指摘されたが、基本方針においても、官民での役割分担、深刻なサイバー脅威に関して認識すべき事項、従来対策との関係等に関して、意識改革をしてもらうためにいろいろと記載している。ただし、基本方針で意識改革の必要性を書いて終わりという話ではないと考えており、今後、協議会、ISAC等での講演、今後作成するガイドブックの普及等の地道な活動を通じて意識改革を進めていきたい。

○　AIについて英語の発信が見つからないという委員からの指摘について、我々が同盟国や関係当局に説明する際に使用する英語の資料が公表できていないとのことだと思うので、公表できるよう努めてまいりたい。また、パッチの適用が速度で追いつけない

時代が来るのではないかという指摘について、注意喚起ではネットワーク隔離や復旧、あるいはBCP的な考え方を取り入れたものとして作成しているが、それでは追いつけない時代がいずれ来るのかもしれない。AIがどう発展していくのかが分からない中で、我々としてはAIの動向を注意深く注視していく。

（７）川崎内閣府大臣政務官コメント

○　本日は早朝から、そして、長時間にわたり御議論いただき感謝申し上げる。

○　クロード・ミュトスやChatGPTの5.5など、これらの事業者は、善意によりオープンに出してくれている話かもしれないが、世の中でみると、水面下でどのようなものが開発されているのかは分からない。その意味においては、必要に応じて開発モデルを確認できるような、機動的に動ける体制をいかに日本でつくっていくか、そして、先ほど委員より「松本大臣はサービスを売りに行け」という話があったが、サービスのみならず、体制も整備していることを多くの方に知ってもらうことが重要である。取組の積極的な発信の件ももっともだと思う。

○　今日お集まりの皆様のおかげでいい整理ができ、日本のプレゼンスが上がるのではないかと思っているため、引き続き先生方のご意見をいただきたく思う。

（８）松本サイバー安全保障担当大臣コメント

○　今日はありがとうございました。大変参考になった。

○　特に監査結果について、委員の皆さま同様、私も非常に基本的なところがまだできていないのは問題があるため、次に向けてしっかりと対応していかなければいけないと思った。

○　監査について、先ほど委員が話していたが、本気のプロの攻撃に耐えられるのかというのは結構耳の痛い話だと思っており、その意味では、やり方そのものも少し考えていかなければいけないのかもしれない。これもぜひ検討させていただきたいと思う。

○　同じ観点でカバレッジについて、横展開をしろという意見があったが、どのようにカバレッジを増やしていくのかということはぜひ考えていきたい。その他、私に刺さるキーワードがあったため、我々で直していきたいと思う。

○　Project YATA-Shieldについて、外部の専門家の協力を得て、必要な体制を構築していきたいと思う。一方で、政府の部内にもさらに人材を確保していく必要は非常に強く感じており、我が国が将来にわたって他国と同等以上の対処能力を持つためには、政府の中でそのような人材を抱えておくことは必要だと思う。短期では厳しいと思うが、中期目標として今から手をつけていこうということで、これから動き出しをしたいと思っている。

（報道関係者入室）

（９）松本サイバー安全保障担当大臣締めくくり発言

○　本日は活発な御議論をいただき、感謝申し上げる。

○　高性能AIを踏まえたサイバーセキュリティ対策の強化として、Project YATA-Shieldを各国に先駆けて策定してから約１か月が経過した。この間、NCOや重要インフラ所管省庁をはじめとする関係省庁において、各業界団体等との意見交換を実施するなど、産業界の課題や懸念に向き合いながら、取組を進めていただいている。

○　本日、本パッケージを念頭に政府機関等の監査結果の取りまとめを含めたサイバーセキュリティ2026や重要インフラ統一基準、脅威ハンティングの普及促進・実施等に係る基本方針など、各種基準・ガイドライン改定等について、貴重な御意見を委員の皆様からいただいた。今後のサイバーセキュリティ戦略本部の決定に向けた準備をさらに加速してまいりたい。

○　加えて、NCOが中心となり、政府全体の重要システムの点検を開始する。まずはNCOに官民の専門家を集めた実施体制を構築し、各府省庁において点検対象となる重要システムを特定し、デジタル庁で先行して取り組んでいるAIを活用した脆弱性対応の知見を政府内で共有するなど、フロンティアAIモデルを活用した脆弱性チェックを速やかに実施する体制の準備を進めたい。

○　AIの進化スピードは目覚ましく、今後想定されるフロンティアAIによるサイバー攻撃は、我々の準備を待ってはくれない。本日の議論を踏まえ、引き続き最大限の緊張感とスピード感を持ってProject YATA-Shieldを実行していきたいと思う。

○　その他の議題についても、いただいた御意見を踏まえ、今後のサイバーセキュリティ施策のさらなる強化や見直しに取り組むなど、官民総力を挙げて、日本全体としてサイバーレジリエンスの強化を目指していく。

○　引き続き委員の皆様の御知見を賜ることができればと思うので、お力添えをお願い申し上げる。

（報道関係者退室）

（１０）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