サイバーセキュリティ推進専門家会議 第２回会合 議事概要

1. 日時：令和７年 10 月 30 日（木）10 時 30 分～12 時 30 分

2. 場所：中央合同庁舎４号館共用第２特別会議室

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
上沼　紫野	ＬＭ虎ノ門南法律事務所 弁護士　（オンライン出席）
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
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】
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（オンライン出席）
土屋　大洋	慶應義塾大学大学院政策・メディア研究科 教授 （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　（オンライン出席）
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　（オンライン出席）

（大臣）

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

小柳　誠二	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
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）
積田　北辰	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）

4.　議事概要

（1）松本サイバー安全保障担当大臣挨拶

○ このたび、サイバー安全保障担当大臣を拝命。今後ともお願い申し上げる。

○ 委員の皆様におかれましては、御多忙のところ御参集いただき感謝。

○ 前回の会合から一月たったが、その間、民間レベルで大きなサイバーインシデントが発生している。国民生活が非常に乱れるこういったサイバー脅威に対して我々はしっかりと施策を取り、人を総動員して、官民一体で対策を整えていかなければいけない。

○ そのためにも戦略をしっかり定めておく必要がある。本日の議論を基に戦略を作り、それに基づき、国民生活の破綻が起こらないような、しっかりした対応を政府としても取っていきたい。ぜひ皆さんの積極的な御意見をお伺いしたい。

（2）事務局説明

事務局から、配付資料によりサイバーセキュリティ戦略（案）について説明があった。

（3）意見交換

○ 短期間のうちに充実したものを用意していただき感謝。

○ 本文の注釈に関して、特に国際関係に関わる部分については、出所を明らかにして、丁寧に情報発信をしていくことが必要。そのような意味で、例えば５ページの注釈などを充実してもらっているのは良い。

○ 官民連携で信頼関係を醸成していくことは、これから国が十分な役割を果たすために非常に重要。その観点からは、概要版にも「信頼関係」という言葉をぜひ掲載していただければと思う。「官民の信頼関係と協働体制を基盤とした官民連携エコシステムの形成」、「緊急時に初めて連携を模索するのではなく、平素から信頼関係を築き」といった言葉が重要。呼応して対応いただく民間事業者に一定の負担が生じることを考えると、このようなメッセージ性の高いワードを盛り込んでいただきたい。

○ サイバーセキュリティ戦略（案）の全体構成、概要について賛同。
○ 国が積極的な役割を果たすといっても、NCO がサイバーセキュリティインシデントに関して隅々まで関与するということを意味するわけではないということは、意識的に展開すべき。国、基幹インフラ事業者における能動的な防御・抑止を行っていくことに重点を置き、それを主眼とした積極的な役割を果たすということだと思っている。

○ 今回の戦略（案）に強く賛同する。サイバー安全保障については、2022 年の国家安保戦略や、ACD 法案と整合性がある内容で、「国が要となって」という点も非常に心強い。
○ 今回の戦略（案）では、「コストを負わせ」、「コストを課す」という表現が複数回出現するが、例えば「平時から」「継続的に」といった副詞をつけてはどうか。今回戦略（案）は、「防御・抑止」の文脈でコスト賦課を位置づけていると理解をしている。いわゆる懲罰的抑止でいうコスト賦課という考え方も有用である一方で、今問題となっているのは、こうした形態の抑止が効かないということ。サイバー攻撃発生や応酬を前提としつつ、サイバー攻撃者のサイバーインフラや能力に継続的にコストを課していくというニュアンスを強調する必要がある。アクセス・無害化だけではなく、テイクダウン、攻撃手口の暴露、侵害指標の共有というやり方もある。戦略（案）は同盟国・同志国もしくはライバルにある国家の関係者も読む ことが想定され、意図を正確に伝える必要がある。
○ 「サイバー攻撃キャンペーン」というキーワードは非常に重要であり、脚注等とかで用語の定義や、背景に触れていただくほうが良いのではないか。経済産業省「攻撃技術情報の取扱い・活用手引き」によれば、キャンペーンとは一定期間内に、特定の目的のために、特定のターゲットに対して、特定の手法を使って、繰り返し行われる攻撃。サイバー攻撃キャンペーンは、ワンショットのサイバー攻撃に比べ予防が可能と考える。NCO がこういったキャンペーンを抽出、特定し、分析して、産業界にフィードバックしていくというニュアンスでキャンペーンを捉えているのであれば、ぜひ強調すべき。

○ インシデントレスポンスにおいては、自社ではなくサプライチェーン内の他社が被害を受け、その対応に追われることがほとんど。そのため、サプライチェーンリスクに非常に高い関心を持っている。
○ 演習結果の政策への取り込み、脅威ハンティングの生態系構築、AI 活用について反映いただき、感謝。
○ 本編の 12 ページや 15 ページにエコシステム構築や悪意のあるサイトのテイクダウンについて記載があるが、テイクダウンが難しい場合には、リークサイトにデータが公開された後、政府やセキュリティベンダーがそのデータを収集・リスト化し、関係組織に通知する役割もご検討いただけるとありがたい。サイトに一度公開されると、ダウンロードや解凍に数日から数週間、場合によっては 1 か月以上かかることもあり、各社が対応している。直接情報窃取された被害企業ではなくてもサプライチェーンの関係で自社の情

報が掲載されている可能性があるため、各社が同じ対応をしている状況なので、こうした対応をまとめて実施いただけると助かる。

○ 情報発信にあたっては、中小企業などは大量の情報を咀嚼するのが難しいため、行動設計まで支援いただけるとありがたい。例えば、パッチや脆弱性対応については、「この脆弱性が何か」という情報だけでなく、どのような考え方で優先順位をつけ、どのように対応すべきかといった行動計画まで含めた情報発信をお願いできると助かる。

○ 官民連携エコシステムの形成のところで、日頃からの関係性をつくることが重要ということはそのとおり。情報の発信だけではなく、それに対してどういう対策をお互いにやっていくか等、具体的な意見交換ができる場もつくるようにしていただきたい。そのために官民連携エコシステムが機能している、というような形となるよう、反映していただければと思っている。

○ 全員参加型のサイバーセキュリティ向上に関しては、中小企業、大学、会社等によって、同じようにはならない。中小企業に対して「支援」という言葉があまり使われていなかったと思っているが、全員参加型でやるのであれば、全員が同じようなレベルになるために明確に同じ手当てができるような記載の仕方がいい。ここは、一番最低限のレベルを全員がやっていけるのだという形にしていただくべきと考えている。

○ 情報共有だけではなく、何をしなければいけないのかも分からない中小企業の方も含めて、みんなで同じ情報で、しかも同じ行動が起こせるような形に進んでいければと考える。

○ 量子技術について、具体的な記載がされたことはいい。量子技術については先を見据えて対応していかなければ、暗号が破られるという形になってしまう。年度ごとに計画に組み込んでいくというアンテナはしっかりと張りながら、どんな計画で、どういうスピードでやるのかは、逐次変更していけるような体制にしていくことが重要。

○ 今回、全体の強化として現在、さらに、エコシステムとして将来を見据えた内容になっているところが良いと感じている。特に青少年についての言及があることは今後の人材育成という面でも非常に重要。

○ 国産技術・サービスを核とした、ということも明記されているが、国外企業のサービスは日本の市場が魅力的でなくなれば撤退する可能性があるといったことも考えると、必要な部分について国産技術・サービスが確立していることは非常に重要なこと。

○ 分かりやすいバージョンもあってよいかと思うが、全ての部分にある必要はなく、例えば中小企業向けのところについて、中小企業向けに分かりやすいバージョン、青少年向けのところについて青少年向けのバージョンをつくるといったように、切り出すということがあってもいいのではないか。

○「演習の体系的な実施」についてはどんどんやっていくことを期待。基幹事業者の中でも、認識が薄いが重要な事業者がある。政府全体の演習があればそういった事業者のセキュリティ対策も進むと期待されている。
○官民連携時の責任範囲の分岐点については、通信事業者等が気にしており、またその他の事業者からは、政府と民間でやりとりされる情報の保全ルールについて明確化を期待する声もあるため、引き続き、議論や調整をお願いしたい。
○全員参加型でサイバーセキュリティの向上を実施するには、基幹インフラと重要インフラの区分や分野の整理が諸外国に比べて複雑で、民間側からは全体像や報告先が非常にわかりづらい状況にある。業法や所管が分かれ、定義も重複しやすいようで、できるだけわかりやすく整理してもらいたい。一度にすべてを整えるのは難しいと思うが、複雑さは形骸化・脆弱性につながるため、中長期でこなれていくことを期待しており、みんなで同じ行動を起こせるようにすることが大事。
○英訳についても、適切な形で実施いただきたい。

○全般についてはよくまとめていただいていると思う。
○地方公共団体では、地方自治法の改正があり、国が少し関与する格好でサイバーセキュリティ対策の計画をつくり、実行していくための支援をすることとなっている。しかし、地方公共団体は人口減少に伴い規模をあまり大きくできない中、人員の確保をしなさいといっても非常に難しい。
○共同で互いに支え合いながら自分たちを守っていく仕組みを支えていく、という書きぶりになっていると、とにかくやれと言っているような雰囲気にならないかなと思う。例えば、基礎自治体に対して都道府県がある程度支援をしていくという議論も出ているので、そういうものをうまく汲んでほしい。
○地方公共団体全体のシステムを見ている J-LIS のほうも関わっていくのではないかと思うが、名前が出ていないのが気になった。
○大学のサイバーセキュリティ強化については経済安全保障の観点が強めに出ているかなと思う。この観点では、それぞれ各大学のほうで、技術流出のためのスクリーニングみたいなことはやっているけれども、サイバーとの関わりという意味ではまだまだ弱いので、サイバーセキュリティの観点からうまく打ち込みができるような支援をしていただくようお願いしたい。
○人材を育成するためのエコシステムの形成等については、既存の取組を支援するような枠組みになっている。CYDER、CYROP など、NICT が持っている基盤の活用とか、官民連携で行っているセキュリティ・キャンプ、CTF 等もあるが、そもそも、大学自体がうまく人材をつくって打ち出していかなくてはいけないということについて、どう受け止め、どういうしていけばいいのかがもう少しクリアになるといい。
○大学の悩みというものは、つくり出した人材を社会にどうやって受け取ってもらい活躍

してもらうかという、パスつくれていないところにある。いわゆる大学と民間との連携によって人が育っていくパスがクリアになり、学生にとって自分のキャリアパスがよく見えるような取組もしていくような書きぶりが入るといい。

○ キャンペーンに関しては、同じアクターが繰り返し長期間にわたって攻撃することがあるので、攻撃者情報を蓄積していく仕組みというものが必要ではないか。特に政府の場合は担当者がすぐに入れ替わってしまうことがありうるので、過去にどうだったかをちゃんと参照できることが重要。
○ 何か攻撃をされ対応しなければいけないといったときに、何ができるのかを即断できるように、いわゆるツールキット、あるいはプレーブックといったものを整備しておくことが必要ではないか。
○ 人材の問題については、サイバーセキュリティに関わる技術者が足りないことは分かった上で、周辺的なサポートをする人、意思決定層とのつなぎをする人、法的な判断が求められた場合にこの分野に詳しい法律家等が必要になる可能性がある。外交問題に備え外交の専門家、パブリックアトリビューションに備えては広報の専門家など、様々な技能を持った専門家を集め政府内に配置していくことも必要ではないか。
○ ユーロポールの記載があったが、インターポールとの関係も重要ではないかと思うので、これも入れてもよいのではないか。
○ 偽情報に関して、関連するような言葉はあるが、記載はあまりなかったのではないか。国家安全保障戦略では偽情報について詳しく対応するというふうに書いてある。サイバー攻撃と偽情報の問題は、同じアクターが同じインフラを使ってやってくる場合もあると思われ、そこについても一言あってもよいのかなと思う。

○ サイバーセキュリティ戦略（案）に賛成。
○ ５つの原則を堅持すること、さらにその原則をどのようなものとして理解しているのかについても丁寧に書き下している点は非常に重要。
○ これまでの戦略から一歩進んで、能動的サイバー防御を含め、国の主導がより強く出てくる中、法の支配あるいは民主主義を守るためということとの関係で、内閣、サイバーセキュリティ戦略本部、NCO、関連省庁、また、独立行政法人等、この戦略を実施される方々が、最終的には内閣の統括の下、一体となって、説明責任等を果たしていくことが非常に必要ではないか。この点、「国の対応・施策の推進に当たり、関係者と連携しつつ、広く国民の理解と協力を得るよう努めていく」と書いていることは、説明責任を果たしていく趣旨が込められているものと理解。
○ 官民連携というときに、様々な事業者あるいは政府機関の中でも、その問題に関わっているレイヤーがある。具体的には、経営者層同士の連携もあるだろうし、経営者の理解の下、各企業で実務者が情報交換をしたり、また、サイバー対象能力強化法の協議会に参加

したりといったことがある。組織ごとの連携だけでなくて、こういう様々なレイヤーでの連携を推進していかなければ、この戦略が実施できないのだということが非常に重要なポイント。

○ 人材の確保に関わることで、例えば公務員の中でサイバーセキュリティ人材を担う上で、これまでの公務員法制のある程度の見直しとか柔軟化が必要になってくる部分もあるのではないか。人事院あるいは公務員法制との調整が必要であろうと思うが、この戦略の下でそういった点も適宜実施されていくべきと考える。

○ サイバーセキュリティ戦略（案）において、国の行政機関等について書き込んでいるが、国会あるいは裁判所のサイバーセキュリティをどう考えるかというのも大きな論点。憲法上の権力分立の建前からは、国会あるいは裁判所の在り方に対して、行政、内閣が口を出さないということは大切。一方、憲法第 73 条第 1 号に書いてあるように、国務の総理を担う内閣として、国会あるいは裁判所の機能を維持するための助言や基盤整備といった活動をすることについては、地方公共団体や民間と同程度にしっかりとした支援を行っていくことも大切ではないか。

○ 戦略（案）に賛成。

○ 戦略（案）にある「我が国のサイバーセキュリティ政策は、能動的サイバー防御等の法制化等により、大きな転換点を迎えることとなった」という評価はまさにそのとおり。その前提となるのは、サイバー空間が自由、公正かつ安全な空間であることをいかに確保していくかであり、そのために、5 つの原則を基本原則とすることは変わりない。今回の戦略（案）において、この重要性が改めて確認されたことは何よりも評価されるべき。

○ 国際的なルール形成の推進に関し、我が国がサイバー空間において適切なルール形成に貢献すべきと戦略で明記されていることは評価できる。関連して、既存の国際法規則あるいはルールがどこまで適用可能なのかを改めて精査することが必要。

○ サイバー空間に適用される国際的なルールの形成に際しては、自律的な主体によるサイバー空間における自由な活動の確保を前提としなければならず。国家間の合意により、過度な縛りを行うことで民間事業者に不必要な負担を強いることは避けなければならない。ルール形成過程で、できるだけ民間の意見を取り入れることで、国家によるサイバー空間の管理というようなネガティブな状況を回避するような施策が望ましい。

○ 戦略の有効期間については「今後 5 年間に取るべき施策の目標や実施方針を示すもの」とされているが、サイバーセキュリティという問題は、その期間において様々な新たな課題を惹起せしめるもの。期間が問題というよりも、その後の対応ということが非常に重要。今回の戦略（案）はサイバーセキュリティ全般についての大きな枠組みを設定しているものと承知している。新たな具体的な課題について、別の文書で評価し、これに対処する場合に、この戦略との整合性を図ることが重要であり、この戦略を中心として、様々な文書を有機的に組み合わせ、しかも対外的に分かりやすい形で提示するべき。

○ 一般の方には難しい文章になっているところもあるので、高校生が勉強できるくらいのレベルを目指して、易しいテキストをつくってもよいのではないか。
○ 海外発信は非常に重要であり、こちらで複数言語版を作成、配布していただくとよいのではないか。
○ 改めて強調しておきたいのは、レジリエンスという言葉。防御も大事だが、特に政府機関がどうあっても維持できる、レジリエンスを保つというところを示していただきたい。重要インフラは当然だが、企業など模範になるという意味でも、何があっても早期に復旧できるという姿勢を示していただければと思う。
○ AI の時代になっても人材が重要であることは変わらない。プラス・セキュリティの感覚で、サイバーセキュリティの専門家が以外にも、専門家の言うことを理解して自分の仕事に落とし込める人が国だけでなく、自治体、企業、教育機関にも必要。そういう人材を増やしていくことが重要である。
○ 経営層、現場それぞれでセキュリティのことを理解しておかなければならない。それぞれに必要なスキルがあることをしっかり普及していくことも今後大事になっていくのではないか。
○ 特に AI や量子コンピューターによって、どんどん技術・社会も変わり、国際情勢も変化していく。そういう中で、5 年間を見通した戦略という観点で、戦略は常に自己点検をして、必要があればちゅうちょなく見直していくという姿勢が大事。
○ 戦略に基づく施策に関しては、関連する戦略、例えば国家安全保障戦略、宇宙基本計画、AI 基本計画といった、並行してあるものと連携し互いに話が通るような進め方を期待したい。

○ 新しい戦略（案）を現行の戦略と読み比べてみると、自由、公正かつ安全なサイバー空間の確保のために、具体的に何を実施していかなければならないかが明確にされており、戦略、積極的なメッセージと言える内容になっているのではないか。
○ 法改正の中で、組織として内閣サイバーセキュリティセンターがサイバー統括室へと改組され、そのトップとして内閣サイバー官が設置されている。この内閣サイバー官が国家安全保障局次長を併任することが内閣法第 16 条第 7 項に規定されており、国家安全保障局とのブリッジが法的な仕組みとして構築されていることは極めて重要。この点に触れることで、制度的に国家安全保障局との緊密な連携を可能とする状況になっていることを示すことができ、連携の必要性を裏打ちできるのではないか。
○ 地方公共団体に関しては、サイバーセキュリティ基本法では重要社会基盤事業者と並列されているが、今回の戦略（案）での記載は、重要社会基盤事業者の記載に比べるとやや控え目になっているように感じる。国と地方の役割分担の議論を踏まえなければならないと理解しているが、例えば自治体の方針策定について定められる総務大臣指針、策定

に関する総務大臣指針に着目をして、その指針のレベルアップやフォローアップについて見ていくということであれば、国と国との間の話として整理できるのではないか。

○ サイバー犯罪対策に関しては、犯罪対策を幅広い主体の議論と捉えれば現在の戦略（案）のようにⅢ.２の位置に置くという整理になるのだろうと思うが、やや唐突感がある。サイバーの脅威への対応の流れとして、まず、一般的な予防策があり、次に、能動的な防御・抑止の対応が出てきて、その次に、脅威が現実化して攻撃となり、被害が発生した場合に、犯罪としての取締りの手法や被害者の救済といった手法が出てくる、という流れで捉えるならば、（Ⅲ.1 の）「国が要となる防御・抑止」の項目の中に位置づけるという考え方もあり得るのではないか。

○ 今回まとめられたサイバーセキュリティ戦略（案）について賛同。

○ 官民連携、特に官から民への情報共有について、高度化しているサイバー攻撃に対して、早期の対処・対応というものが非常に大事になってくる。これから国際連携あるいは官民連携が進むことで官に情報が集約されてくることになるかと思うが、そのような情報は重要インフラを担う民間企業にも非常に価値があるものとなるので、早期の情報共有やアドバイスをお願いしたい。

○ 人材育成について、研究開発でポイントとなる人材の育成にはかなりの時間を要する。企業や国を守るという意味では、セキュリティに加えて、ネットワークや AI といった専門知識を有する高度な人材を育成する仕組みが必要。業界連携といった横のつながりはもちろんのこと、大学と民間との縦の連携、経験豊富なエンジニアあるいは指導者が縦のラインで弟子に教えていくような、縦の連携の仕組みが大事である。

○ 今回策定する戦略は、しっかり実行してこそ意義があるもの。時間軸でターゲットを明確に定めて、政策それぞれの優先度も意識しながら実行していくことになろうかと思うが、NCO の方のほうで主導的に牽引してもらうことを期待している。

○ 民間部門でもサイバーインシデントの脅威というものが重要になってきつつあるなか、情報収集の面もある一方、サイバー犯罪捜査という面もあり、両立していく形で対処していくという記載であると理解している。対応主体として、NCO および協議会が対応していくことなのか、あるいは並行して刑事司法機関が対応していくことなのか違いという点で、サイバー犯罪についての記述は今の位置であまり違和感は覚えなかった。

○ 「犯罪対策」というと、警察のことと受け取られる。しかし、書き方を例えば「サイバーの脅威に対する安全・安心の確保」という風にすると、社会全体でそれぞれのアクターができることをして、安全で安心な不安のない状態を醸成していきましょうという受け止めになる。そういった御意見があったと思っており、表現によって随分違ってくると考える。現在の位置に入れられていることから、「犯罪対策」という言葉のイメージよりも広いお話をされているのだとすると、サイバー犯罪への対策というだけではない言葉が

表題として出てくるとよいのではないか。記載はこの位置のまま、犯罪対策も含めた広い話だというふうにするのはどうか。

○ 基本的にはサイバー犯罪への対策は、警察庁、都道府県警がやると同時に、政府全体のレベルでは犯罪対策閣僚会議で御議論いただいていると思う。サイバーセキュリティ戦略と、この間の匿名・流動型犯罪グループ対策等を含む犯罪対策閣僚会議の決定は、それぞれの分野から追及していくという観点で重要であると同時に、内閣の下で一体的に運営され再度統合されているのだろうと考える。犯罪対策閣僚会議等、また警察庁等の取組と連携するということが大前提で、その犯罪対策が同時にサイバーセキュリティの確保につながっているということを書くのであれば、(「犯罪対策」の記載は) 今の位置でもいいのではないか。

○ サイバー犯罪の対策を通じてサイバーセキュリティに貢献するとか、あるいはサイバー犯罪の対策で、犯罪を予防するためにどうするかを、現在、犯罪対策閣僚会議で議論いただいている。そういったものをこちらに連携していくのだということが見出し、あるいは中身レベルで分かるようにしていくべき。

○ 犯罪対策閣僚会議の下での内閣の方針ということであれば、広いサイバーセキュリティの中での犯罪捜査なのだという書きぶりがあるとよりいいのではないか。

○ 政府がどうやって AI を使って、どういうルールを徹底させていくのかということや、情報の機微のレベルにも応じたソブリン AI といった議論が諸外国でもあるが、これは、AI 基本計画で進むと期待している。

○ サイバーセキュリティは全てに横串であるので、色々な計画や戦略が関わってくる。戦略を進める上で政府のほうでも横連携を取って進めていくことが必要。

（政府側出席者　鈴木内閣参事官）

○ 戦略 (案) の重要インフラ統一基準に関する記載箇所における「重要インフラ事業者等」の「等」に地方公共団体が入っており、重要インフラ統一基準は地方公共団体も対象となっているので、補足させていただく。

○ サイバー犯罪への対策の記載箇所に関しては、前回のサイバーセキュリティ戦略では「社会全体のレジリエンス」の記載のある箇所に、サイバー犯罪の項目が記載されていた。今回の戦略における「国が要となる防御・抑止」の項目は、新法に基づく取組を主体として書いているところ、サイバー犯罪についての記述は、新法に基づくというよりは、それよりも広い、一般的な犯罪対策といえるため、現在の位置に記載することとした経緯がある。

○ プラス・セキュリティに関しては重要な点であるから、脚注で「専門的なセキュリティスキルを有していない人材についても、組織内外のセキュリティの専門家と協働する上で必要な知識を習得したプラス・セキュリティ人材となれるような学習機会の充実化を

図る」として、言及している。

○ 偽・誤情報に関しては、この戦略全体を進める上の留意点の箇所において、生成 AI 技術の進展に伴う、偽情報を含む影響工作の脅威の増大について言及した上で、我が国のサイバーセキュリティ確保の観点から必要な取組については、この戦略に基づく対応を行うとしていった記述をしている。

（政府側出席者　飯田内閣サイバー官）

○ サイバー犯罪対策の位置づけについては、受け止め方も色々もあるということで皆様の御意見を伺った上で編集をしていきたい。

（４）松本サイバー安全保障担当大臣挨拶

○ 本日は活発な御議論をいただき感謝。

○ 国会と裁判所のサイバーセキュリティについて御意見があった。三権分立等、様々な原則的なルールがあるので、どれぐらい関与できるかといった課題はあるが、重要な案件であると認識。

○ サイバー官とNSS次長との関係は､確かに戦略に書き込んであると､分かりやすいので､検討する。

○ 海外発信については、勝手に訳されて誤解を生むと困る場合があるため、言語数は限られるかもしれないが、関係機関と協働して、こちらで訳出することも一案。

○ 分かりやすいバージョンの作成に関しても、どういう作成の仕方をするかは検討したいと思うが、御意見は十分に尊重してまいりたい。

○ いずれにしても、よい戦略を策定することが国民生活を守ることにつながる。そういった思いで今後の作業を引き続き続けていきたい。

（５）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