サイバーセキュリティ推進専門家会議 第１回会合 議事要旨

1. 日時：令和７年９月19日（金）８時30分～10時15分

2. 場所：中央合同庁舎４号館

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）
漆間　啓	三菱電機株式会社 代表執行役 執行役社長ＣＥＯ
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
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　（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、大臣政務官）

平　将明	サイバー安全保障担当大臣
岸　信千世	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
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）

4.　議事概要

（1）平サイバー安全保障担当大臣挨拶

○　委員各位におかれては、本日御多用の中、御参加いただいたこと、御礼申し上げる。
○　サイバー空間をめぐる脅威は、国民生活・経済活動、国家安全保障に深刻な影響を及ぼしている。サイバー空間を取り巻く切迫した情勢に対応するには、サイバー対処能力強化法に基づく取組を含め国が対策の要となって、我が国全体を牽引するとともに、官民一体で対策を推進していくことが不可欠となる。
○　このため、政府の取組を総合的・一体的に推進するとともに、広く国民や関係者の理解と協力を得るべく、新たなサイバーセキュリティ戦略を策定し、中長期的に政府が取り組むべきサイバーセキュリティ政策の方向性を内外に示していきたいと考えている。
○　本戦略が激しさを増すサイバー情勢に的確に対応し、我が国のサイバーセキュリティ向上に資するものとなるよう、委員各位には幅広い専門的見地から活発な議論をお願い申し上げる。

（2）議長の互選

委員の互選により、後藤厚宏委員が議長に選出された。

（3）議長代理の選出

後藤議長の指名により、酒井啓亘委員が議長代理に選出された。

（4）サイバーセキュリティ推進専門家会議の運営

事務局から、「サイバーセキュリティ推進専門家会議運営規則（案）」についての説明があり、原案の通り決定された。

（5）事務局説明

事務局から、配付資料により新たなサイバーセキュリティ戦略の策定に向けた説明があった。

（６）意見交換

○　戦略の新しいものをつくる流れは理解しており、そこに特に違和感がある箇所はない。

○　国が要となって推進する取組について、既に能動的サイバー防御の話で出ているとおり、実際に現場に立つことになるのは警察と思われる。今回、無害化措置などが実施できるようになるということで、それは重要なことだと思っているが、緻密な制度設計が重要だという点は、戦略の中でも分厚めに書いていただきたい。

○　官民連携の話について、従来から旧ＮＩＳＣを中心とした連携があり、信頼関係の醸成が非常に重要。民間からすると、参加するためのインセンティブ、特に提供した情報へのフィードバックが少ないという意見が非常に多いのが現在の状況であるため、いかに官から民に対する情報提供ができるかが大きな鍵になる。新たな協議体の立ち上げに当たっては、より多くの情報が集まるような体制を作っていただきたい。

○　「幅広い主体によるサイバーセキュリティ及びレジリエンスの向上」について、重要インフラ事業者は既に取組みが進んでいるが、重要インフラ事業者の下にはサプライチェーン、いわゆる委託関係になっているIT事業者がおり、目配りが必要となる。重要インフラ事業者は体力もあり、国と連携できるが、その下にあるサプライチェーンに対し、重要インフラ事業者からどうセキュリティ対策を流してもらうのかという点は、意外と目配りができていないように感じる。

○　地方公共団体においても、同じようにサイバーセキュリティ対策は必須。小さな基礎自治体から特別地方公共団体といったものまで、これらに対するサイバーセキュリティ対策の強化は、取りこぼしなく対策が行き届くような枠組みを入れた戦略にして欲しい。

○　レジリエンスの確保に手が挙がらない中小企業には、ＩＴ化に対する支援と同じように財政的な支援を行わなければいけなくなると思う。

○　人材育成については、プログラムはこれまでも幾つもあったが、出口が十分に考慮できていたかという側面がある。我が国自身のセキュリティ産業をどうやって育成していくのかという一つの大きな観点で、人を生み出す、ユーザー企業の中でセキュリティを上げるといった話はあるが、そもそもセキュリティを担える事業体をどうやって育てていくかという観点は少し薄いため、その点を指摘する。

○　サイバー脅威の防止・抑止が具体的に何を守るのか、例えば国民の財産などについて、具体的なイメージを一致させたほうが良い。

○　深刻化するサイバー脅威に対する防止・抑止の実現に関しては、日本全体のサイバーレジリエンスを高めていくかがポイントで、社会全体での取組が必要。民間の人材レベルや役割について、企業の大きさや脅威レベルに応じて一律では難しく、それぞれがどの程度の役割を担うのかを明確化したほうが良い。

○　サイバーセキュリティの社会全体のレジリエンスでは、経済団体や業界団体が海外と比較した日本の強みと考えられるため、その活用や、業界別のＩＳＡＣの活用も効果的と考えている。

○　高度なサイバー攻撃というのは、重要インフラのみならず、製造業の供給網にも及び得るという危機感を持っている。サイバー安全保障を実現する上で高度なＯＴセキュリティ対策を製造業全体でいかに早く実装していくかが鍵になる。
○　サイバー攻撃については、供給網の途絶を狙うケースもあり、これに対して供給網全体のＯＴセキュリティ対策が必要。これを社会全体が実装するには、経営サイドの明確なビジネス戦略に加えて、政府サイドのガイドラインや導入支援策もぜひ御検討いただきたい。また、中小企業を含めたサイバーリスクに関する危機意識の共有も課題。例えば専門用語を使わない実践的なリスクコミュニケーションも鍵と考えている。
○　防衛事業のサイバー対策も重要であり、官民協調の防衛サイバーシステムの構築の仕組みが供給網サイバーシステムの確立のヒントになると思う。
○　人材と技術開発について、サイバー分野で高度な攻撃情報を共有するクリアランスホルダーを育成していくことも必要。日本の理科系については、人口減少も含めて激減をしている。サイバー領域で官民のクリアランスホルダーのコミュニティーを構築し、グローバルな人材交流、あるいは技術提携につながるサイバーエコシステムを築いていくことが技術・人材開発の基盤になるのではないか。
○　サイバーの安全保障のリスク認識を経営レベル、社会レベルまで高めていくことと、経営サイドがセキュリティビジネス加速にコミットをすること、そして政府サイドについては、政策面で腰を据えた支援を検討いただきたい。

○　サイバーセキュリティ戦略の骨子（たたき台）やその前提となる議論については、基本的に違和感はない。
○　内政の話、外交防衛の話といった縦割りの議論ではなくて、サイバー空間をめぐる様々な政府、あるいは国内外の取組と本戦略の有機的な関係を意識することが大事である。
○　人材育成やリスキリング、組織の体制強化、アジャイルガバナンス等の取組みが、エコシステムとしてつながっていくことが大事である。
○　我が国の行政サービスのかなりの部分は地方公共団体で担っているところが多く、国と地方公共団体の連携、いわゆるＧ　ｔｏ　Ｇや、民間の企業も関わるＧ　ｔｏ　Ｂ　ｔｏ　Ｇのような場面でサービスが提供される中での、サイバーセキュリティ上のリスクに配慮することが必要。
○　例えば、大きな企業が取引先である中小企業と連携してサプライチェーン全体のレ

ジリエンスを確保することに競争法上の問題がないのかなど、現場レベルでの連携の目詰まり、様々な支障に丁寧に対処する政府の姿勢が大事である。それぞれの主体間の連携を適切に実現していく上で、政府の役割を強く押し出していく必要がある。

○　演習の体系的な実施を通じた継続的な改善について、業界横断のインシデントレスポンス共同演習などでは、例えば監督官庁のガイドラインが改定されると、それがきちんとできているのかなどかなり細かくチェックしている。それらは継続しつつ、演習で出てきた課題については、インシデント対応の実効性を上げるために政策に反映するような動きもあったらいいのではないか。
○　脅威ハンティングについては、手始めとしてオンプレミスのシステムに対し力を入れて取り組んでいるが、クラウドのシステムはオンプレのシステムよりは相対的に可視性が落ちる。今後はそこに対してもしっかりと取り組んで行く予定。中小の組織では脅威ハンティングの取り組み自体のハードルが高いと思われるので、先行する大企業が確立したやり方などをシェアする枠組みは重要。
○　脅威ハンティングで、レッドチームとブルーチーム、および脅威インテリジェンスも含めたパープル活動を行っているが、重要インフラ事業者では膨大なログを保有しているので、それらを活用しＡＩを使った攻撃予兆の予測モデルの作成といったことも長期目線で行えれば良いと考える。
○　エコシステムの部分で、各業界の ISAC 活動で共助として知見共有や協働も行っているが限界はあり、システム投資が困難な中小企業がセキュリティ弱者になりがち。セキュリティ体制や投資額の格差を埋めるプラットフォームを作ろうという動きもあり、それらも視野に入れながら動いていけると良い。

○　全体的にきちんとまとまっていて、全く異論はなし。
○　「演習訓練のさらなる充実」について、既にたくさんあるものを、一つのポータルのようにまとめ、どの年齢層、どのキャリアの方にどのように役立つのかが分かりやすくなると、いろいろな方に資するものになる。
○　若者たちからは、政府がセキュリティ人材は必要だと叫んだことで、このキャリアを選んだということが聞かれる。政府が本気だということが示され、若者たちがこのパイプラインに乗っていけば、自分はサイバーセキュリティのエキスパートになれるのだ、あるいは違うキャリアになれるのだということが示されると、目標になり、若者たちや企業もついてくるのではないか。
○　国際連携、国際協力が必要というのはどの国も同じ感覚を持っている。既に政府レベルでは情報共有などをしているかと思うが、そこに学生等にリーチする道を持つ民間も入って拾い上げるという協力関係もあると良い。
○　ＡＩに関しては、非常に新しくて、ガイドラインに落とし込むのが非常に難しいが、

それでも走り続け、現段階のものだということを示し続けていくことが大事。

○　７月、Ｘを舞台に参院選を利用して外国勢力がＳＮＳを使った介入工作を行っているのではないかということが非常に話題になり、皆さんの懸念として広がった。今回ターゲットとするものは、基幹インフラなどに対する重大なサイバー攻撃ということだが、まだまだそのリスクが知られていないのではないか。知られていないがゆえに、一旦火がついたときにサイバー攻撃に対する恐ろしさが広まるのか、あるいは国が主体になって対策を取っていくことへのリスクに火がつくのか、今、まだそこが非常に危うい段階なのではないか。このリスクを幅広い主体に、きちんと分かりやすい形で、具体的な問題として伝えていくことがまず大切なのではないか。
○　サイバー対処能力強化法が成立する段階で、通信の秘密の箇所は、衆議院で修正を加えて、不当に制限しないような形で明記されたが、依然として懸念は残っている。基幹インフラ事業者に新たな義務が生じる形になり、そういった懸念にもきちんと配慮した制度設計にしておかなければ、余計なハレーションが生まれ、迅速で臨機応変な対応にはつながらない事態も起きかねない。そのため、その点のリスクの広報、そして国の積極的な対応への懸念に対する丁寧な配慮について議論できればと考えている。

○　　今回のサイバーセキュリティ戦略の骨子の方向性については賛成。特にⅢの１の（１）に「国が要となって」と明確に言及いただいている箇所は非常に心強いと思うため、ぜひこの点を今後ともお願いしたい。
○　地方公共団体や中小企業等のサイバーセキュリティの強化の中身として人と知識と財政的な支援を具体的に書いていただければと思う。地方公共団体はどんどん人口が減り、その中で高度なサイバーセキュリティ技術の知識を持った人も乏しいため、その点の支援をお願いしたい。
○　中小企業に関して、セキュアバイデザイン原則は非常に重要だが、例えばＳＢＯＭの話をしたときに、実際にＳＢＯＭとは何でしょうかというレベルだったりする。そのため、幅広いチャンネルを通じた支援をして、まずはセキュリティバイデザインの考え方を広めることが必要。
○　戦略の見直しについては、この分野は非常に変化が激しいため、変化の激しいものをどのように織り込むのかという点を具体的に検討いただければと思う。

○　行政の継続や安定性という観点からすれば、個別の施策領域の原則は軽々に変更すべきものではないと考えられ、このことからすれば、今回示されている、５つの原則を引き継ぐという姿勢はとても大切。他方において、やはりこの分野は非常に流動的であり、今回の戦略の策定が、サイバー対処能力強化法に基づく初の戦略であるとい

うこともある。戦略の策定に当たっては、このことを強く意識していかなければならない。示された既存の５原則を引き継ぎつつも、従来の原則自体もサイバーセキュリティ対策を一層力強く積極的に進める姿勢で発展的に見直すことがあり得るのではないか。

○　全体的にこの骨子で異存はない。
○　サイバーセキュリティと影響工作を連携して考えると、特にハック・アンド・リークという、情報をハッキングして、それを一つの政党、あるいは候補者に流していくという問題が大きくなっている。他国ではハッキングのターゲットとして選挙管理委員会や政党、政治家、秘書の方々、ボランティアの方々、こういった方々が対象になる傾向がある。その観点から、こういった組織の役割なども考える必要があるのではないか。
○　現在サイバー攻撃として基本的に想定されているものは、一回性であり、突然、攻撃が来て、それが分かりやすい形で何かしらの被害を生むもの。一方、今年の２月あたりから指摘されているものとして、ＡＩを対象としたＬＬＭグルーミングというのがある。これも常習的なサイバー攻撃と思われるため、情報共有する。
○　官民連携に関して、重要な点は情報共有。例えばアトリビューションなどは、民間のアクターにとっては非常に難しいものであるため、政府でサイバー攻撃に関してアトリビューションができるとき、それを民間に対して情報共有することもあるだろうし、また、サイバーセキュリティ会社との間で、こういった観点で連携をすることも重要である。

○　サイバーセキュリティ戦略の策定に際して五つの原則の継承が非常に重要。
○　産業の視点からは、ＤＸの取組を加速するためのデータの自由な流通が確保されるために、データガバナンスやセキュリティ対策が必須。
○　データガバナンスにおいては、デジタル庁から今年６月にガイドラインが示されており、そこでは人材育成が課題となっている。他方で、ＤＸと人材が重なる部分もあるため、人材フレームワーク策定に当たっては、サイバーセキュリティ人材とデータ人材の奪い合いにならないよう、複数の専門性を備えた人材育成の仕組みが必要になるのではないか。
○　セキュリティに関しては、バイデザイン、バイデフォルトの必要性を痛感している。現在はカルチャーを浸透させるフェーズであり、非機能要件に振り向けるＩＴ投資を許容するカルチャーの定着が必要。

○　事務局が作成したサイバーセキュリティ戦略の骨子、たたき台については、きちんと要点を示しており、大方は賛同。

○ これまでの戦略が策定された後に決定・公表された文書等について、これを考慮してその内容と整合的な中身としつつ、新たなサイバーセキュリティ戦略の独自の意義を明確にすることが必要。2022 年の「国家安全保障戦略」、今年の戦略本部が策定した「サイバー空間をめぐる脅威に対応するために喫緊に取り組むべき事項」、「サイバー対処能力強化法等に基づく施策」といった文書等は、その目的や対象、時間的枠組みなどが異なるため、各々の位置づけや性格を明確に意識し、新たなサイバー戦略の策定を目指すことが肝要。

○ 新たなサイバーセキュリティ戦略の策定に当たって、自由公正かつ安全なサイバー空間の確保を改めて強調する必要がある。サイバー脅威への防止と抑止に対しては、日本国内での官民の信頼関係と協働体制が重要であることは既に指摘されているところであるが、サイバー空間の利用は国内・国外を問わず行われ、それが自由公正かつ安全な空間であることは、強調してもし過ぎることはない。官民の間での情報共有と対策強化の制度化のほか、セキュアバイデザイン原則という観点からも信頼のおけるハードウエアとソフトウエアの開発提供に向けて、事業者の方々と共に政府が協力して、一致団結して行っていくことが必要。

○ 日本自身の能力を向上するのはもちろん、途上国を含めた他の諸国の能力の底上げに支援を行うことも重要。グローバルサプライチェーンの展開により、日本国内だけでサイバーセキュリティの強化を行うことは不十分であることは明らかであり、日本国内のみの視点に陥らず、自由公正かつ安全なサイバー空間の確保に向けて、広く国際社会への貢献という観点からもサイバーセキュリティの情報共有、技術支援を積極的に行っていくことも戦略の中に位置づけることが重要。

○ 今回のサイバーセキュリティ戦略において、国家安全保障の観点は非常に重要なのは当然だが、サイバーセキュリティの脅威はそれだけに限られるわけではなくて、むしろ数から言えば、もっと日常的な、サイバー犯罪に該当するようなサイバー攻撃が非常に多いのではないかと認識している。

○ 「深刻化するサイバー脅威に対する防止・抑止の実現」における「防止・抑止」はイメージが非常に似ているが、ここでの「防止」は、被害者目線、被害者の観点からいかに防ぐかいうこと。対して「抑止」は、攻撃をする側に攻撃をさせないことということであり、こちらのほうが現実性も含めてより重要になってくるのではないか。もちろん、1 回目の攻撃を防ぐのは難しいわけだが、繰り返しの攻撃に関して攻撃元を追及し、そこに何らかの働きかけをしていくことが大事になっていく。

○ 国家サイバー統括室での対応、あるいはサイバー対処能力強化法での枠組みが重要な意味合いを持つが、これまでも行われてきたサイバー犯罪捜査と並行で進んでいくことが大事。もちろん国会審議でもサイバー対処能力強化法での情報の扱いについて、捜査のために使うものではないという審議があったことはそのとおりだが、そ

れは、従前からあるサイバー犯罪捜査と相入れない枠組みを構築していることを意味するものではなく、それとの並列を視野に入れた形でのサイバーセキュリティ戦略を考えていくことも重要。

○　戦略の骨子について、国として推進すべき要素が盛り込まれているということで、賛同する。基本的な考え方、五つの基本原則については、継続していくことに賛同。一方で、地政学的な緊張感の高まりを踏まえると、より一歩踏み出した積極的なサイバー防御によって社会インフラを守っていく姿勢が必要。

○　今年の初めに情報通信、金融、航空系の重要インフラ分野へのＤＤｏＳ攻撃が社会問題化したが、その背景には攻撃の多様化・高度化がある。攻撃と防御では、圧倒的に攻撃側の立場が優位になるため、個社で対応するのは非常に難しい。特に日本は中小企業、ここに強さの源泉があると思っており、個社ではなかなか対応が厳しい状況だと思われるため、この点について官民が連携して現状把握・分析をして、脅威情報等を共有していく仕組みが必要。さらには官民連携によって、実践的な演習を通じて防衛力を高めていく必要がある。

○　先端技術に関して、技術分野というのは先が見えているものの、一朝一夕で進化するものではなく、この戦略の最終年度がどのような世界になるのかということを意識しながら先読みした技術の種を植えていくことが非常に大事。安全なＡＩ、ＡＩのガバナンス、情報資産を守るための暗号化技術、耐量子計算機暗号、量子の暗号通信等は国としても強化をすべき領域ではないかと思っており、必要に応じて国産でも研究開発していく仕組みも必要。

○　令和３年のサイバーセキュリティ戦略を読み直すと、その多くの部分はいまだに当てはまるが、今、今後５年を見通したときに、私たちは何を考えるべきかというと、非常に分かりにくい。サイバー戦場の霧がどんどん深くなってきている中でいかに未然にサイバー攻撃を予知できるかというところが能動的サイバー防御として問われていることと思う。

○　注意すべき点は、サイバー攻撃を一過性のものではなくて、サイバーキャンペーンとして繰り返し行われ、長期にわたって行われるものとしてとらえること。今回はそれにいかに対応していくかということを考えるべきではないか。

○　ＡＩ等の新たな技術も大きな撹乱要因になる。特に国境を越えた認知介入・干渉というのは日常化してきている。我々はその影響から逃れられないという側面も忘れてはいけない。そうした中、国際連携をいかにやっていくかということが重要で、二国間、多国間の連携は行っていただきたい。その際にコミュニケーションのポイントとなるのは顔役の存在。外務省にはサイバー大使がおり、ＮＣＯも海外から見たときに一つの顔役になる。日本でサイバーを担っていることをしっかりアピールしながら、

海外との連携を行うことが重要。

○　インド太平洋は我々にとって重要な地域であり、ＱＵＡＤがある。そこで日本がこの能力を高め、引っ張っていける形をつくっていければと思う。

○　令和３年戦略は 40 ページを超えて長かったのではないか。今回、委員 18 人の指摘を全て盛り込む必要はないと思う。ここがポイントなのだということに絞り、みんなに読んでもらえるような戦略にして欲しい。

○　2022 年の国家安保戦略で掲げられたアクティブサイバーディフェンス体制の整備が始まってから初のサイバーセキュリティ戦略となるため、国民、企業の期待は非常に大きい。今回の戦略のたたき台に強く賛同。

○　サイバー空間の脅威評価について、これまでの戦略にも国家背景のサイバー脅威に関する評価があったが、ＮＣＯとして総合評価のさらなる拡充・詳細化の検討をお願いしたい。新戦略の期間中に評価手法の高度化や、戦略ベースではなく年次評価も必要だと考えているため、こういったことも検討いただきたい。

○　サイバー攻撃を抑止することは非常に重要だが、現実に直面しているサイバー攻撃の多くはレッドラインを越えず、抑止や予防が利きにくいものが大半。抑止や予防だけではなく、サイバー攻撃の被害や応酬を前提として、攻撃者にいかにコストを課すのか、攻撃者の能力を削るのかという考え方もぜひ盛り込むべき。その際、注意喚起、情報共有、被害関連組織への通知、事業者と協力したテイクダウン等の技術的な措置もさることながら、パブリックアトリビューション、司法訴追、経済制裁等の非技術的側面についてもオプションを整備し、攻撃者にとって望ましくない環境を形成していくという考え方も入れてはどうか。

○　サイバーセキュリティ戦略の骨子について、この案に賛同する。策定の趣旨、背景から基本的な考え方、目的の達成の施策、推進体制まで適切にカバーできるものと考える。この構成に沿って、ページ数は少なく充実ということでお願いしたい。

○　今後５年間を見据えるのが大事。ただし、予測困難や想定外のことが雨あられのように起きる状況であるため、戦略そのものもレジリエンス、つまり適応力、適切にアジャイルに適応できる力を持っていないと、この５年間をしっかり対応できない。そういう意味での戦略の推進体制における柔軟性、フレキシビリティーと俊敏性、アジリティーをぜひ大事にしていただきたい。

○　国が主体的に役割を果たすという言葉が非常に大事で、ここを明確に宣言いただきたい。

○　社会全体のセキュリティのレジリエンスの向上に関しては、民側のインセンティブをいかに引き出すかという観点が非常に大事である。

○　国の主体となる防衛の施策、重要インフラ機能における対策強化においては、重要性

や効果をちゃんと測る、推計して示す取組も並行して行うことが重要。日本の場合、自然災害、巨大地震の被害シミュレーションなども非常に盛んに行われている。サイバー攻撃に関しても、これからはそういうものが必要な時代であり、そういう取組が今回の戦略の下支えになるではないかと期待している。

○　分量的な目標像は今の時点では早過ぎるかと思うが、コンパクトにすることは非常に難しいことであり、そのためにしっかりと意見を出したいと思っている。

○　いわゆる情報戦とか、コグニティブセキュリティという分野に関しては、今回の戦略の中でどのように取り扱っていくのかというのは結構大事で難しい課題。事務局のご意見はいかがか。

（政府側出席者　木村統括官）

○　海外での選挙に対する民主的なプロセスへの介入や干渉のような記述は、実は前回の戦略でも一部述べられていた。その後につくられた国家安保戦略の中でも、いわゆる認知領域における情報戦等に対処するかということで、その対応能力を強化しなければいけないような記載もある。そういったことを受けて、政府としても必要な対策や取組を行っている。

○　一方で、例えばＡＩ技術の進歩などの技術的な進展、あるいは外国の取組の変化を踏まえると、その脅威が増大してきていることは間違いないことだと思っており、政府としても、先般、官房長官が会見で発表したり、自民党で緊急提言が取りまとめられたりしている。

○　サイバーセキュリティ戦略の中で、どのあたりまで実際に認識した上での対策として取り組んでいき、どのように書いていくかは、議論を踏まえながら検討していきたい。

（政府側出席者　平サイバー安全保障担当大臣）

○　民主主義の根幹の選挙で当然政府は中立的でなければいけないため、政府や与党が突出して関与すると、気持ち悪いと思う人もいると思う。とはいえ、例えば、直近ではルーマニアの選挙は無効になった。

○　与党や政府が突出して関与するよりは、アカデミアやメディアや国民も含めて、みんなで民主主義を守らないといけない。絶対に守られなければならない言論の自由の脆弱性を突いてくるかなり深刻な問題であるため、皆さんから広く意見をいただき、政府はこの範囲でこういうことをやれと言っていただくのがいいという印象を持っている。

（７）岸内閣府大臣政務官挨拶

○　本日は活発な議論をいただき、感謝申し上げる。

○　今般は、国民及び事業者において、サイバー脅威を感じていない人はいないのだろうと思う。そうした中で政府が力強く方向性を示すことが何より重要と、深く認識した。
○　様々な各論があり、特にまだまだ知られていないところの情報工作や認知分野において、これだけ攻撃側のコストが安く、何の分野でも守る側のコストが本当に高くなっているという、この構造をしっかりと認識して、まさに攻撃側に対して望ましくない環境を形成するという考え方はとてもいいと個人的に感じている。
○　５年単位を念頭においた「サイバーセキュリティ戦略」の策定については、これだけ変化のスピードが速いため、ぜひとも適応力を重視して進めていければと思っている。

（８）平サイバー安全保障担当大臣挨拶
○　まずサイバー対処能力強化法はおかげさまで成立した。私も４、５年前にこの問題に関わるようになり、この国で本当にセキュリティ・クリアランスやアクティブ・ディフェンスの法律がつくれるのかと思ったが、結果として、40 時間の審議で 400 回の答弁をして成立した。やはり国民のほうが危機意識は強いのだろうと思った。
○　国会における論戦を通じて法案修正もしたが、参議院においては９割の国会議員の賛成を得た。我々もアンテナを上げて、こんな法案は難しいと思うのではなく、危機対応をしっかりやっていくことが大事なのだろうと感じた。
○　ただ、法律はできたが、キャパシティビルディングはまさにこれからである。その人材確保も含めてお願いするとともに、政府としては同盟国・同志国との連携をしっかり進めていきたい。私は法律が成立してすぐに、イギリス、インド、オーストラリアに訪問した。各国の担当大臣と色々な話をしたが、特にイギリス、オーストラリアは大歓迎ということだった。インドともいろいろなお話をして、いろいろな分野で連携ができるだろうということが分かったので、しっかり進めていきたい。
○　２つ目の課題認識はＡＩだ。私はＡＩの政策も担当しているが、生成ＡＩの進化が指数関数的に伸びていく中で、今後、サイバー分野においても、まさにＡＩ対ＡＩの戦いになっていくのだろうと思う。ＡＩの視点も同盟国・同志国としっかり連携をしながら、防御能力を高めていくことが必要だろうと思っている。その点も指摘や意見をいただければと思う。
○　重要インフラを守るのも大事だが、議論にも出ていた通り、サプライチェーンの中で中小企業をどうやって守っていくかという点では、明確なソリューションを我々はまだ持っていないため、ぜひその辺りもいろいろな示唆をいただければと思う。
○　最後に、官民連携が非常に重要だと思うため、政府のこういう箇所を直すべきといったものがあれば、忌憚なく言っていただければと思う。皆さんの意見をいただきながら、しっかりと計画をつくっていきたいと思う。

（９）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