「サイバー対処能力強化法の施行等に関する有識者会議」（第３回）議事要旨

1. 日時：令和７年 10 月 30 日（金）８時 30 分から 10 時 10 分までの間

2. 場所：中央合同庁舎４号館

3. 構成員

岩村 有広	一般社団法人日本経済団体連合会 常務理事
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
大谷　和子	日本総合研究所 執行役員 法務部長
川口　貴久	東京海上ディーアール株式会社 主席研究員
酒井　啓亘	早稲田大学法学学術院教授【座長代理】
宍戸　常寿	東京大学大学院法学政治学研究科教授
高見澤　將林	公益財団法人笹川平和財団 上席フェロー【座長】
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	一橋大学副学長、法学研究科教授
畠山　一成	日本商工会議所　常務理事
平井　淳生	一般社団法人電子情報技術産業協会 業務執行理事／常務理事
星　周一郎	東京都立大学法学部教授
星野　理彰	NTT 株式会社代表取締役副社長 副社長執行役員 一般社団法人 ICT-ISAC 理事

（政府側）

松本　尚	内閣府特命担当大臣（サイバー安全保障）
飯田　陽一	内閣サイバー官
木村　公彦	内閣府政策統括官（サイバー安全保障担当）
門松　貴	内閣府大臣官房審議官（サイバー安全保障担当）
佐野 朋毅	内閣府大臣官房審議官（サイバー安全保障担当）
小柳 誠二	内閣官房内閣審議官／内閣府

4.　議事概要

（1）松本尚内閣府特命担当大臣（サイバー安全保障）挨拶

○　おはようございます。このたび、サイバー安全保障担当の内閣府特命担当大臣を拝命いたしました松本尚でございます。今後とも、どうかよろしくお願いを申し上げます。

○　構成員の皆様におかれましては、本日も御多用の中、御参集いただきまして、誠にありがとうございます。

○　この国家を背景とした高度なサイバー攻撃への懸念の拡大は社会不安に陥れるということで、国民の関心も高かろうと思います。

○　DX の進展を踏まえると、我が国のサイバー対処能力の強化は国民にも目に見える形で進めていかなければいけないと思っております。先般の通常国会では、サイバー対処能力強化法が成立しました。

○　官民連携の強化、そして、通信情報の利用について施策をきちんと国民に示していくということを我々は使命としております。

○　本日は、これまでの意見の交換、ヒアリングを通して、事務局が作成した基本方針案について皆様に御議論をいただきたいと思います。議論を基に、今後、パブリックコメントを実施し、基本方針案をしっかりまとめていきたいというふうに思っております。私もしっかりとコミットしていきたいと思っておりますので、今日はどうかよろしくお願いを申し上げます。

（2）サイバー対処能力強化法に基づく基本方針について

事務局から、配付資料によりサイバー対処能力強化法に基づく基本方針（案）の説明があったのち、各構成員から以下の意見があった。

○　前回の発言を反映いただき感謝。基本方針案に賛同することをまず表明させていただく。

○　まず、当事者協定の締結によるメリットの理解・普及を図っていくことの重要性について改めて申し上げる。専門家の視点と実社会との間に温度差があることは否定できず、すり合わせのためには一定の時間が必要である。

○　第 2 章第 1 節の基本的な考え方にも当事者協定の締結に向けて丁寧に協議を行うとの指摘があるが、粘り強く誠実に対応いただきたい。

○　次に、現実にサイバー被害に遭った場合におけるサイバー犯罪捜査との関係については、センシティブな問題もあろうかと思うが、サイバー犯罪捜査自体は刑事訴訟法上の法的な枠組みにのっとった対応となる。これは従前どおり行われ、それ以上でも以下でもないということを改めて指摘をさせていただく。

○　最後に、協議会について。NCO における従前のサイバーセキュリティ協議会でのノウハウを生かしつつ、今般のサイバー対処能力強化法の趣旨にのっとった形での制

度設計をいただけると理解しており、ぜひ、その方向で対応をお願いしたい。

○ 基本方針案は、これまでの意見を踏まえて、事業者負担の軽減、実務の観点にも配慮した内容が盛り込まれており、本案に賛成する。
○ 特に第４章第２節で、報告等情報収集の考え方に、第１回で申し上げた届出対象の絞り込みや報告の一元化について明記いただき感謝申し上げる。
○ 引き続き、幅広い事業者との対話を重ねながら、制度の実効性を確保しつつ、現場の実情を踏まえた運用をお願いする。

○ 基本方針案の取りまとめに感謝申し上げる。全体的な方向性について同意する。
○ その上で、文言についてコメントさせていただく。基本方針案の概要（資料１）の４頁の当事者協定の締結を推進させるための基本的な事項の（２）「内閣府は、協定当事者がいわれのない非難を受けることがないよう」という記載がある。趣旨としては同意するが「いわれのない」は表現として強いので、単に「非難」としてもいいのではないか。
○ 基本方針案の概要の５頁の第３章第１節の基本的な考え方について通信の秘密への配慮の箇所で「通信の秘密等にも」と記載があるが、「も」は削除して「通信の秘密等に十分に配慮して」でいいかと思う。
○ 今回、クラウドサービスについて言及されているが、日本のクラウドサービスはほぼ外国企業ベースのものであり、例えば外国のクラウドサービス事業者が協議会の参加を希望することも十分考えられるので、外国事業者に対する対応について考えておく必要がある。

○ 基本方針案に関しては、全体をよくまとめていただき、大きな問題もないので、賛同する。
○ 特に原理原則の基本的な考え方の記述が充実し、非常に分かりやすくなった。その上で、今後、運用に関わるところが出てくるので、コメントさせていただく。
○ 本件は、国民を守るための制度だが、その原理原則と国民の権利であるところの通信の秘密の問題のバランスをうまく取っていかなくてはならないところが難しい。
○ 制度の原理原則が国民にとってメリットがあるものであるということを事あるごとに打ち出していけるような運用をしていただきたい。
○ まず、特定重要電子計算機の定義について、運用に入るといろいろな例が出てくると思う。これが業界別に、定義されていくことになるが、運用でぶれが出てしまうと、制度そのものがうまく回らなくなる可能性があるので、定義については、少しずつ丁寧に細かくしていっていただきたい。
○ 協議会については、参加は任意のものであるという原則は保たれるべきだが、一方で

参加を促さないといけない。参加した事業者にフィードバックが返るところが一番のインセンティブになると思う。参加することが自分たちの事業にとって利益になるのだということが分かるような広報に努めていただきたい。

○ それから、通信の秘密への配慮に係る規定を遵守するためには、第３章第３節の通信情報の適正な取扱いに関する配慮事項の中でサイバー通信情報監理委員会による監理の項目があり、こちらで監理されているということについて広報に努めることが重要である。

○ 他法令の遵守については、特に警察との関係があるかもしれない。このような運用に係る事実は、透明性の観点からつまびらかにしなくてはいけない。少なくともサイバー通信情報監理委員会に対してこういう運用がされたということがうまく伝わるような運用をしていただきたい。

○ 最後の項目にあるアクセス・無害化措置との連携も非常に重要な点。その細部はこれから詰めるということになると思うが、本当に肝になってくる部分であると思うので、丁寧な実装をお願いしたい。

○ 基本方針案、全体の構成について十分に練られたものだと考えており賛成する。

○ その上で本件は、能動的なサイバー防御という考え方を全面的に打ち出した制度なので、これから起こることへの備えという意味合いが大変強いものである。

○ 実際に既に生じた被害、それから、まだ解決していない被害の状況等からどのような知恵をすくい取るのか、また、被害組織が被害を受けたままに放置されないようにするといった信頼関係を醸成するためにどうしたらいいのかといった発想も大変重要になってくると思う。

○ ランサムウェア攻撃は、特定社会基盤事業者でなくても社会的に大きな影響が及ぶ。社会全体がサイバーに依存して成り立っているということを昨今実感させられるような出来事が続いているので、そこを協議会がどのように対応するかが、重要になってくる。

○ 特定事案に関して、被害組織との間で被害状況や対策に関する協議を行うこと、それから、平素からの対策についての協議が行われることが重要。

○ 我々全体にとってメリットがある制度だと思っているので、その点について分かりやすい説明がなされていくこと、そして、協議会で十分な情報が共有されるような運営がなされていくことが必要になってくると思う。

○ 特定社会基盤事業者や被害組織の負担が小さくなるようにということを明記していただいたので、実際にどのような負担が生じているのかといった実態についても、制度の発足時点だけではなく、運用開始後も含めて、定期的に情報を吸い上げていく努力が必要になる。

○ 事務の委託について、IPA や NICT への委託について、これらの組織にはこれまで

もセキュリティに関する知見が非常に集約されている組織なので、こういった機関との協力関係は非常に重要。

○　ただ、そこにも十分なリソースが必ずしもあるわけではないので、一定の分野については再委託が必要になってくる。再委託先の組織をどのように選定していくのか、どこまで許容するのかといった基準も今後設けていく必要がある。基本方針に盛り込むべき内容でないとしても、今後御検討を進めていく必要がある。

○　３つの総合整理分析情報について定義していただいたのはよかったと思う。これを混同しないようにしながら、うまく使い分けていくということが重要だと思う。

○　特に提供用総合整理分析情報を提供した場合、相手がその情報をどのように保護してくれるかということが重要である。提供した相手から情報が漏れてしまったり不適切な管理をされたりすると、制度全体にダメージがあるので、よく考えていかなくてはいけない。

○　特に協議会やサイバー通信情報監理委員会ができたときに、そこで情報がどのように扱われるかということは少し今後の懸念として、あるいは関心事項として持っておきたい。

○　犯罪捜査のための通信傍受法が既に 20 年以上使われているが、そことの切り分けを、国民やマスコミが混同しないように、丁寧に説明しながら、この制度の周知を図っていただきたい。

○　基本方針案の取りまとめ、ブラッシュアップに感謝申し上げる。

○　第１章第２節のまとめは非常に分かりやすく拝読した。２点コメントさせていただく。

○　１点目は、総合整理分析情報の幅広い提供について。法律で指定した事業者や自ら情報取集に積極的な事業者、つまり、基幹インフラ事業者、情報共有枠組みに入る者、協議会に入る企業は制度で十分カバーされているが、それ以外の事業者、国民にも広く周知をいただきたい。

○　基幹インフラ、協議会参加者以外の企業にどのようにアプローチするのか。経済団体、やサイバーセキュリティに限らない業界団体にもアプローチできるといいのではないか。

○　２点目は、秘密の管理の在り方について。やはり民間として期待するのは、政府しか持ち得ない情報の提供、つまり、特定侵害事象や通信情報を利用したもの、もしくは外国政府から提供されたもの。

○　様々な情報提供先がある中で、ある程度共通の秘密管理の枠組みがあると企業としては分かりやすい。機密レベルが一定以上のもの、例えば、今年５月に施行された重要経済安保情報保護活用法の対象となるものは、どの情報提供枠組みであれ、情報管

理の在り方は同様であろう。

○ それ以下の機密レベルの情報の扱いが、例えば協議会参加者向けと、基幹インフラ事業者向けで違うと分かりにくいので、今後、重要経済安保情報以下の秘密についても横串を刺すような制度を検討いただきたい。

○ 基本方針案に賛成する。２点、確認のために発言をさせていただく。

○ １点目は、当事者協定についてであるが、既に議論されてきたように、官民連携の強化という観点からも、広くステークホルダーに関与していただくことが肝要と思われる。

○ 当事者協定への参加を促進するためにも、どのような理由で情報を収集し、それをどのように活かしていくか、官と民が Win-Win の関係となるように、主として官が民に対して説明を尽くしていくということがまずは必要となる。この点は基本方針案においても、当事者協定を締結しようとする者の判断に資するように、できる限り丁寧に協議を行うと記載されており、十分考慮されていると考えるが、ここでも強調させていただく。

○ それとともに、当事者協定が即座に締結されないとすれば、この協定を締結するまでの期間においても、重要なステークホルダーとの関係で、サイバーセキュリティを確保するための施策を取ることも検討すべきである。この点は基本方針に書き込むべき事項というよりも、基本方針の実施という運用のレベルで対処していただくことが適切なように思われるので、ここで確認させていただきたい。

○ ２点目は、アクセス・無害化措置との連携に関する記述が追加されたことについて、能動的サイバー防御の効果的・効率的な実施に向けては、その前提として、アクセス・無害化措置の実施のために、関連する情報の共有が不可欠であり、この点が基本方針案の第７章第３節で明確にされたことを歓迎する。

○ ここで関係する情報は非常に機微な性質を有すると考えられるため、効果的かつ適正に行政機関に提供すると記載されているが、そこには機密性にも留意した取扱いも含まれるべきであるということを改めて強調させていただく。

○ 私も基本方針案に賛成する。その上で３点、コメントさせていただく。

○ １点目は、基本方針案の６頁の４行目から「全てのステークホルダーがメリットを実感できるサイバー攻撃対応のエコシステムを、官民を横断して構築する」との記載があるが、これが今回の法律あるいは施策を考える上で非常に重要な強調すべきポイントだと思う。

○ もちろん、これは国家が国家としてやるべきことであると同時に、デジタル社会において、国も企業等と対等な一員という部分があり、そうであればこそ協力をいろいろと求めていくことが必要である。

○　また、その際に、今回の基本方針全体を通じて、それぞれの事業者の方々等の負担等にも配慮し、また、丁寧な説明を行うといったことにつながっている重要なポイントだと思っており、この点を強調しておきたい。
○　２点目は、エコシステムの構築についてであり、基本方針案の概要（資料１）の２頁の下にある、その施策が適切に機能するための事務を適正に実施するという箇所について、基本方針案の第３章において、かなり丁寧に加筆をいただいている。また、とりわけ第３章第３節（４）でサイバー通信情報監理委員会による監理についても言及されたことに感謝を申し上げる。
○　この点について、適正な実施を支えると同時に、官民全体を通じた今回の施策の実効性を高める上で重要なもう一つの視点は、周知・啓発を丁寧に実施していくということである。資料１においても、また、基本方針案についても何か所かで丁寧に周知・啓発を行っていくという記載があり、これは非常に重要だと考える。
○　基本方針案の18頁の１行目だが、制度の運用について可能な限り透明性を高めていく旨書かれているが、これは政府の今回の施策の姿勢としては、重要なポイントだと考えており、もし概要版に書けるようであれば追記いただいてもいいかと思う。
○　３点目は、こうして情報を収集・分析し、提供して活用していただく。しかも、それをフィードバックを受けて見直していくことも非常に重要なポイントである。
○　その観点で、基本方針案の表現で気になったのは、27頁の15行目以降で「情報提供を受けた機関」という表現が何か所かで出てくる一方、27頁の３行目で「情報の提供を受けた者において」という表現もある。情報提供を受けた機関というと、より広く提供先のことを意図しているのだろうと思うのが、精査いただいくとよいと思う。

○　基本方針案について、ほかの構成員と同様に、賛成させていただきたく。
○　サイバー対処能力強化法に基づく基本方針ということで、改めて同法を読み直した。この法律はなかなか難解である。サイバー空間に関する情報を適正にやり取りする法律であるということで、詳細な書きぶりにはなるのであろうが、基本方針は、民間の事業者にも関わる制度ということもあり、できる限りシンプルに分かりやすいものとしていただく必要があるのではないか。
○　その意味で、章立てを整理していただいて、それぞれに基本的考え方を入れていただいたということは大変よいことであると考える。
○　これからパブリックコメントが予定されているということで、これは大変重要で大切なプロセスになると思う。ぜひたくさんの意見を酌み取っていただきたい。
○　３点ほど、意見を述べさせていただく。
○　１点目は、並行して議論が進んでいるサイバーセキュリティ戦略への呼応についてという点である。戦略のほうは、アクティブサイバーディフェンスの制度ができてから策定される戦略ということで、より積極的で能動的な、まさに戦略というものを考

えていくという議論が、今、進んでいる。そのような動きにこちらも呼応するようなメッセージが、例えば、基本方針案の３頁のはじめにの辺りに、出てくるとよいのではないかと思う。

○　２点目は、今の話とも関わるのだが、この基本方針案の「方針」のなかには、積極的であるべきという方針と、慎重であるべき方針というものがあると考えられる。例えば、当事者協定や協議会の展開については積極的たるべき方針というものになると思うが、ただ、その中の情報の取扱いや守秘義務のような話は慎重たるべき方針ということになるのではないか。また、取得する情報の管理や取扱いについては慎重であるべきだが、情報の分析・検討ということは積極的に進めていかなければならない、といえるのではないか。このような方針のメリハリが文章からも見えてくると、より分かりやすくなるのではないか。

○　３点目は、本基本方針の見直しについて、である。見直しについては、38頁の最後の辺りで言及されている。

○　本基本方針は、法律に基づいて立てられる基本方針ということからすれば、軽々に見直すべきものとはいえないともいえる。しかしながら他方で、このような領域の基本方針なので、時宜に応じた見直しも必要となってくるはずである。この見直しの時期をどう判断するのか、どのような時に見直しをしないといけないのかということは、少し意識的に、考えておいたほうがよいのではないか。例えば、法律について大きな動きがあったときや、サイバーセキュリティ戦略の見直しがあったときなどが例として挙がるかと思っており、このような記述が入ると見直しについてより明確になると思う。

○　第１回会合で中小企業の配慮の観点から申し上げたが、それについて盛り込まれており、基本方針案には基本的に賛成させていただく。その上で幾つか申し上げたい。

○　基本方針案の概要の３頁目に、事業者等との連携の中で「周知など中小企業も含めて広く様々な事業者が対象となり得るため、必要な周知・広報を行う」という記載がある。実行段階においては、しかるべき人にしかるべき情報が届く必要があるので、広く周知する視点が必要であるが、影響が想定されるような事業者、中小企業者等に対しても情報が確実に届いて、具体的な行動につながるようなプッシュ型の情報発信をぜひお願いしたい。

○　その上で、その発信の中身についても、対象となる人によって変わってくるため、どの者に何を発信するのかはっきりと仕分けるのは難しいと思うが、情報を受け取った者がどう行動すれば良いのかが分かるような形で工夫していただきたい。

○　また、６頁目で、届出等も含めて、事業者の負担にも留意するということや、報告窓口の一元化をすることが示されている。必要な中小企業に対する支援があれば、引き続きお願いしたいということで改めて申し上げる。

○　非常に丁寧に書いていただいており、この後、パブリックコメントを実施する際に、これを見れば、何が問題だと考えているのかということからしっかり理解できるという意味で、よくできた形になっている。
○　他方で、分量が多くなってしまっているので、期間中にどれだけの方が読んでいただけるのかというところは不安なので、丁寧な広報をお願いしたい。
○　その上で、4点ほど、文章についての意見ではなく、確認的なところを申し上げたい。
○　1点目は、委託に関連して、第5章第6節のIPA等への委託に関して前回、いろいろ意見交換させていただいた。それに加えて、第3章第2節に、実際にこの運用に従事する職員についての項目が8行目から10行目辺りに書かれている。
○　NCO自身の知見の向上、職員の充実は非常に重要なテーマだと思っているが、この辺は時間もかかる話で、採用してから教育していくのは難しいと思っている。中途採用の方とか、あるいはルール上可能かどうかは分からないが、民間の専門家の出向等による登用など、いろいろな考え方があると思うので、守秘義務がしっかり守れる形で、様々な専門家が育つような形で考えていただきたい。この点に関して、民間のインテリジェンス関係のベンチャー企業の育成みたいな話も観点としては入ってきてもいいと思う。
○　2点目は、ネットワークやシステムのインテグレーターの関係。例えば第4章第2節のところに、中小企業も含めた基幹インフラ事業者からの相談などの対応と書かかれているが、今、想定されている事業者に中小企業が含まれるか。あるいは、基幹インフラ事業者からシステム構築・運用を委託されているネットワーク事業者等に中小企業が含まれており、そこからの相談を受けるのか。このような質問が、パブリックコメントの中で寄せられる可能性もあるので、頭の片隅に置いていただきたい。ネットワークのインテグレーターについては、第4節でも特定事業者と取引等がある事業者が協議会に参加されることが想定されるような文面になっている。協議会に参加して意見を聞きたい、情報交換をしたいという趣旨であれば、その旨、広報等で明らかにしていただきたい。
○　3点目は、できるだけ協議会に参加するメリットが感じられるようにしていただきたい。例えば、ゼロデイアタックが懸念されるような情報、こういうものも危ないという情報をいただけると、それだけでも確かにメリットではあると思うが、そこからのアクションが取れない、セキュリティパッチがないのにどうやって対応するのだというような話もある。できれば、こういうリスクがあるからこうしたほうがいいというアクションにつながるような情報まで含めていただけると、よりメリットが高まる。
○　4点目は、第6章第5節にセキュリティクリアランスについての記載があり、これを読めば、重要経済安保情報については、協議会の参加者全員にセキュリティクリアランスを求めるわけではなく、特定の話題になるときにはクリアランスを求めるとい

うふうにも読める。あるいは協議会に入るのだったら一律でセキュリティクリアランスを求めたほうがいいではないかという議論もあるかと思う。この点も今後の議論かとは思うが、パブリックコメントの中でいろいろ意見は出てくるかと思うので、御留意いただきたい。

○ サイバー攻撃は日々激化しており、能動的サイバー防御の必要性や、基本方針案で記載されている内容の重要性について、賛同申し上げる。
○ 能動的サイバー防御は日本としての新たな試みなので、大臣や何人かの構成員が主張されているとおり、官民双方にとっての有益な取組にしていただきたい。
○ 日々進化するサイバー攻撃に対して新たに考慮すべきことが出てきたり、運用を続ける中で、民間側の理解の進展も伴って環境等も変化してきたりすることを考えると、枠組みについて不断の見直しをしていく、こういったコミュニケーションを引き続き取っていくということが非常に重要である。今回の取りまとめに当たっても、事務局において丁寧にいろいろな意見を聞いていただいて文章を直していただいていることに感謝を申し上げる。
○ インシデントについて、急ぎ報告するとともに、正確性が必要だとなると、どうしても報告が難しくなる。急いでいる場合は簡易に、まず、初報を出して、内容が分かってから続報を後で出すといった分け方は必要。
○ 電気通信事業者が使っている特定重要計算機、ルーターや通信機器は膨大な数になるので、これらを製品やバージョンをその都度変更するために報告しているとすごく大変になる。インターネットに接している面だけの装置を出すとか、目的と必要性に照らして報告の範囲を限定化するといったことが必要。
○ このような議論があり、これから細部について皆様と御相談し、現実性のあるものを一緒につくり上げていきたい。
○ いずれにしても、この仕組みを機能させていくためには、企業側もメリットを感じるとともに、双方で協力し合うことでメリットが出るという関係をつくっていきたい。その意味では、我々はしっかりこういうところへ参加させていただいているので、取組は進めるつもりだが、他の者も取組に協力の姿勢となるように、今回、パブリックコメントも実施し、こういった会合も含めて、意見を収集して反映していくということを引き続きやっていきたい。

○ 構成員からの指摘と問題意識は基本的に共有しており、全体的な構成として分かりやすくなり、かつ、これまでの議論の指摘事項の多くを反映していただいたので、基本的には賛成する。
○ 一方、まだ分かりにくい部分が残っていると思うので、パブリックコメントのプロセス等を活用して、できるだけ分かりやすくなるような工夫をしていただきたい。

○　また、構成員からの指摘事項の中で反映されていないのは、基本方針のスコープによるものだと思うので、基本方針の枠を超えて提言されているような部分については、法執行全体の場面で、可能な限りその実現に努めていただきたい。

○　文章の表現になるが、資料２の６頁のところで、負担に関する議論も考慮すると、「全てのステークホルダーが、サイバーセキュリティの一翼を担うとともに、そのメリットを実感できる」というような関係者全員が当事者意識をもってやっていくのだという意義づけを入れると全体の流れがよくなるのではないか。

○　11頁の21行目以降に関して、当事者協定については、できるだけ早く締結するのが大事だと思うが、あくまでも運用の想定等に応じて、しかも、情勢の変化もあるので、その内容を発展させていくということが重要だと考えており、ここにある記述はそのような観点から非常に大事なものだと思う。

○　17頁の第３章について、説明を工夫しているが、文章が長いところが多い。一文が７行以上、６行以上あるところはチェックをしていただいて、分かりやすくしてほしい。つまり、文章の幹の部分と具体的な事例の部分を分けて書いてほしい。細かな基準が文章の中に溶け込んでしまっていて、かえって分かりにくくなっているところがあるので、ぜひ確認していただきたい。

○　それから、21頁に届出の考え方とか、いろいろな話の中で「柔軟な」という言葉がある。この「柔軟な」というものは非常に便利な言葉だが、ブレークダウンが必要ではないか。柔軟性の中にはアジリティとか、アダプタビリティとか、インプロビゼーションとか、あるいはテクノロジカルなブレークスルーとか、そういうものが全て入っていると思うので、そういう形で機器の指定などもダイナミックに展開していくのだというところをぜひ反映していただきたい。

○　第５章については非常にうまく記載していただいて、特に政府から積極的にフィードバックを行い、情報共有がより活発となるように取り組むという点は非常に大事だと思う。

（３）官民連携の強化に向け今後具体化が必要な論点について

事務局から、配付資料により官民連携の強化に向け今後具体化が必要な論点の説明があったのち、各構成員から以下の意見があった。

○　新協議会について、情報を共有するときに、どうやって情報を守るか。例えば、共有された情報を保つために専用のデバイスを持ってもらうようなことがセキュリティを考えたときには必要かもしれない。セキュリティと利便性はなかなか両立しないが、配慮が必要な場合もある。

○　新協議会について２点申し上げる。

○　１点目は、この新協議会の構成員は、個人である場合や事業者、法人団体組織の場合もある。法人団体組織で入るといっても、実際には高い知見を持ち、組織内でサイバーセキュリティ等の問題に関わっている個人であることが多い。そのようなときに、新協議会の構成員たる団体組織と実際に出てくる個人との関係を整理しておくことが重要。
○　守秘義務についても、構成員たる団体組織にかける部分と、実際に来た方にかける部分、あるいは団体組織の中で共有された情報を共有する範囲について整理することが重要。そこがはっきりしていると、参加を検討しやすくなる。
○　２点目は、地方自治体について。新協議会に地方公共団体が参加する、あるいは参加しない地方公共団体もこの新協議会で共有される情報の一部の提供を受けるといったことがあり得る。
○　地方公共団体がそれぞれの地域でインフラ事業者的な側面で自分のシステムを守るというだけではなく、その地域のサイバーセキュリティの向上に取り組んでいただく必要がある。
○　例えば、都道府県がその区域にある市区町村のサイバーセキュリティの取組に連携して、底上げしていくような助力をすることもありえる。
○　あるいは地域の重要な事業者と連携して、全体の底上げを図るといった、地域協議会のようなものを通じた情報提供もありえる。逆に言うと、この情報は地域でも出さないようにといった縛りも含めて検討することが重要。

○　事務局から示された論点のうち、１．と４．について、指摘させていただく。
○　電子計算機の考え方に関しては、VPNでの対象範囲など、特にアタックを受けるサービス入口になる部分は、類型化して整理する必要がある。
○　一方で、基本方針案にあったとおり、専用設計されており、実行コードの動作が分からないようなものであれば、労力をかけて守るほどのものではないと思う。
○　その点において、エアギャップしているケースに関しても同様で、攻撃が成功する可能性が高くなく、現にアタックを受けているものとの比較において、後回しにするのもやむを得ない。特に、エアギャップしていれば、物理メディアを介して攻撃を受けて破壊的な動作をすることはあり得ても、それがネットワークを通じてほかに出ることは基本的には考えられないので、被害の大きさとリスクの可能性から考えても、ある程度の裾切りは合理的。
○　クラウドに関しても同様の考え方かと思うが、例えば行政機関で使われているクラウドに関しては、ISMAPのような標準でセキュリティガバナンスが規定されていることが前提になっていると承知している。それができていれば裾切りは通っていると考えていいのか、あるいはそれにもさらに上乗せが必要なのかという議論を今後積んでいただきたい。

○ 協議会に関しては、情報提供に関してはメリットを感じるような形でいただきたく、情報を受け取ったCISO等が社内に具体的にこういうふうにしろという指示が出せるような具体的な形での情報提供をいただけるとありがたい。
○ ただ、即応性を考えると、ここが見つかったので注意すべきというアラートだけでも、意義がある情報だと思っているので、時間軸と情報の即応性みたいなものとの比較で考えていただきたい。

○ 中小企業も含めて、事業者との対話を繰り返していただいているということに感謝する。
○ 一般論になるが、本件が実効性を上げていくためには、事業者側での対応、特に影響力のある事業者における対応が非常に重要。分かりやすいこと、双方向でやり取りが行われること、中小企業に限らないが、キャパシティに限度があることを踏まえて、対応に向けた支援が行われることを併せて考えていただきたい。

○ １．と２．についての、官民連携で実効性を高めるために、アタックサーフェスになる機器と報告対象物とは少し限定していただいき、民間企業と協力して守っていただけるとありがたい。
○ 報告対象物を少し絞って、機器ベンダーとか製品名等にとどめて、バージョンの都度変更等については民間企業の運用側が確認をするような、現実性を求めて運用していただけるとありがたい。
○ インシデント報告について、即応性と対処と分けていただいて、初報では限定した内容を素早く報告をして、内容が分かってから改めて報告とした方が、報告を受ける側もタイミングがずれてアラートの情報をもらってもしょうがないということにならないと思う。
○ もう一つは、この報告はこの目的に使うということを言っていただけると、報告側もその内容に絞ってうまく出すこともできるようになると思う。最初はやりながらなので、やり方が変わっていっても構わないと思うので、ぜひ民側と協力してやっていけるような対応を取っていただきたい。
○ 協議会について、資料１の７頁に提供先の一覧で出ているが、電子計算機を使用するものとなると広くあまねくみたいなイメージになってしまう。情報を提供する側がある程度選択できるような仕組みをつくっていただいて、もしそれ以上求めるときは、相談いただくことにしていただくと、安心して情報を出せるではないかと思う。そういう工夫をしていただきたい。
○ セキュリティクリアランス下で情報共有というと、紙ベースでの情報共有が想起されるが、地方自治体等、首都圏以外の者に情報を暗号化して渡すことを含めて、紙ベース以外の情報提供も考慮しながら、実効性のある方法を考えていくことが必要。

○　制度をよく動かすにはという観点から３点コメントさせていただく。
○　１点目は、この仕組みをうまく動かすには事業者にとって負担にならないこと、負担軽減が、必須ということ。当然のことながら、申請を重複させないで統合して効率よくやることが必要である。負担を減少するような技術的な支援も必要になるだろう。
○　２点目は、４．について、一般論として、まず、新協議会を「作ってもらう」ということが重要。協議会をつくることについて、メリットが感じられるようにしなければならないというのはその通りである。併せて、国ができる周辺支援も重要になる。
○　例えば、協議会に関するモデル規定をつくること、関係者のマッチングをすること、参加者を横でつなげる仕組みを設けること、といったことをすると、そこで議論が活性化していくのではないかと思う。
○　３点目は、１．について。冒頭の説明で、下位法令を見据えた議論をするという話があった。つまり、類型を規定、すなわち、文字にするということになると思われるが、サイバーセキュリティのような技術が進化していく領域において文字化するのは難しくなることのあるのではないかと思う。だからといって、ブランクの規定にするわけにはいかないので、何かしらの規定を立てる必要があることになる。具体的なアイデアはないが、一ついえることは、最初につくる仕組みが非常に重要になってくるということである。最初に立てる下位法令・基準が後々のこの制度の継続や発展において障害にならないように、長期的な視点で考える必要があると考える。

○　特定重要電子計算機が整理学として、この言葉のまま理解されると、各事業者の事業にとって重要な計算機というふうな捉えられ方がされる。
○　これを守ることは各事業者にとって非常に重要だが、法全体の立てつけからすると、アタックサーフェスをどうやって守るか、また、アタックサーフェスから侵害された兆候があったときにどうするか検討することが重要。
○　特定重要電子計算機は２つの整理学をうまく組み合わせて指定する必要がある。
○　業界・業態によってシステム構成がかなり違うので、整理学はそれぞれ考えていただくしかないが、文字通りの事業そのもののコアになる計算機というところだけに目を向けていると、侵害が進んでしまう。
○　アタックサーフェスのところをうまく分類した上で指定の仕方を考えていただくことが重要。

○　２頁目の３．について意見を申し上げる。
○　事業者の負担軽減及びサステーナビリティが重要だということは承知しているが、この項目については、ある程度、事業者に頑張っていただく必要があるかと思う。
○　個情法の報告期限、これは個人の権利・利益を害するおそれがある場合、速やかに報告は３日から５日という時間軸を想定している。

○　この情報をもらって政府がどう行動するかにもよるが、やはり政府としては、サイバー攻撃キャンペーンを見つけ、特定し、分析し、短期的には将来を予測し、関係者に配付することを考えた場合に、指摘のあった早期発見・早期対応が目的であるとすれば、３日から５日というは遅いのではないか。

○　特定重要電子計算機の届出について、大多数の事業者が使っているソフトウェアについて、届出義務の対象とするのではなく、国が情報を取りに行くことが必要。このようなソフトウェアの利用状況について国は調査で確認する必要がある。
○　これらのソフトウェアの脆弱性情報については、国としても積極的に情報を取りに行くべき。
○　国からのプッシュ型の情報提供や、官民協働でプラットフォームを運用しそこに情報が登録されていくという在り方が目指すべき姿に近いのではないか。

○　特定重要電子計算機の考え方について申し上げる。対象機器の範囲について、現場実務の視点からなお不明確な部分があり、今後議論を深める必要がある。特に、情報系（IT）と制御系（OT）が融合した環境では、システム間の境界が曖昧であり、単純にシステム単位で指定するだけでは、実態を十分に反映しきれないと認識している。このため、事業継続への影響度やシステム間の相互依存性を軸に、リスクベースの柔軟な指定が重要。
○　特定重要電子計算機の届出について、中小企業を含む事業者にとって分かりやすく、過度な負担とならないことが制度の実効性の鍵となる。届出項目は、リスクベースの観点から合理的かつ最小限に整理し、経済安全保障推進法など関連法令との整合を確保することで、頻繁な更新や重複手続きが生じないよう配慮をお願いする。
○　インシデント報告について、報告の目的を明確にしたうえで、適時・適切な情報共有を行うことが重要。速報と終報など、目的に応じた報告区分を設けることで、スピードと精度の両立を図っていただきたい。
○　新協議会については、官から民へのフィードバックの充実をお願いする。具体的には、事業者が脆弱性対応や経営判断に活用できるような、実務的かつ戦略的な情報提供を期待する。あわせて、基幹インフラ事業者などが提供する情報の取り扱いについては、諸外国の先例も参考に、共有範囲や管理ルールを明確化することで、提供された情報が必要最小限の範囲で適切に活用されることが重要。

（４）松本尚内閣府特命担当大臣（サイバー安全保障）挨拶
○　構成員の皆様の活発な議論に感謝申し上げる。
○　私が印象に残ったところを何点か申し上げる。構成員からの発言にもあったが、非常に早いスピードで物事が変わっていく案件なので、状況の変化に応じて、弾力的な対

応が必要ということは私も同じように考える。

○ 協議会の構成員にセキュリティクリアランスをどれぐらい求めるか。できるだけ最初の段階であまりハードルを高くしたくない。一方で、秘密を扱う問題なので、日本人全体としてもそのような意識を高くしていく必要がある。ここは十分に検討させていただきたい。

○ インシデント報告のタイミングについては、個人的には早くやったほうがいいのではないかなと思うが、個情法との関係もあるので、注意深く見ていかなければいけないと思う。

○ 特に中小企業に対して十分に説明と周知をしておかないと、そもそも、我々がやろうとしていることの多くができなくなってしまう。パブリックコメントも分からない、わざと分からなくしているのではないかというふうな批判がでることもあるので、注意したい。

○ 引き続き、よろしくお願い申し上げる。

（５）次回会合等について

○ 意見交換の後、事務局より本日の議論を踏まえてパブリックコメントを実施すること、次回会合は１２月上旬で日程調整すること等について発言があった。