「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 4 回）議事要旨

1. 日時：令和 7 年 12 月 8 日（月）9 時 45 分から 11 時 00 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
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
小柴 満信	公益社団法人経済同友会 幹事
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）
川崎 ひでと	内閣府大臣政務官
飯田 陽一	内閣サイバー官
井上 裕之	内閣府事務次官
木村 公彦	内閣府政策統括官（サイバー安全保障担当）
泉 恒有	内閣府政策統括官（経済安全保障担当）
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）松本内閣府特命担当大臣（サイバー安全保障）挨拶

○ サイバー安全保障担当の内閣府特命担当大臣の松本尚でございます。構成員各位におかれては、本日もご多用中、ご参集いただき御礼申し上げる。

○ サイバー対処能力強化法に基づく基本方針につき、これまで3回にわたって御議論いただき、これを踏まえて先月、パブリックコメントを実施した。その中で、基本方針案の内容や、具体的な制度運用に関するご意見をいただいている。

○ 本日は、これを踏まえて事務局が用意した修正案をご確認いただき、閣議決定に向けて基本方針案をとりまとめたい。

○ 前回の会議では、基本方針案の内容を踏まえて、官民連携の強化に向け、今後より具体化が必要な論点についてもご議論いただいた。本日は、その論点を踏まえて事務局で用意した、サイバー対処能力強化法における資産届出やインシデント報告、協議会等の考え方について、ご議論いただきたい。

○ 有識者の皆様におかれては、それぞれの見地から忌憚のないご意見をお願いしたい。

（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。

○ 今回、パブリックコメントや前回の議論を経て、基本的な方針案をとりまとめて頂いたことは適切だと考える。前回申し上げたとおり、資料3の概要資料は、基本方針案のポイントをわかりやすく反映していただいていると思っている。

○ 特に2頁右下にある「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」との点を概要資料でも強調していただき、また、今回の本文の修正においてもその方向性で修正がなされたと理解している。この点について、政府として民間とよく対話して法律の準備を進めてもらいたい。改めて、この点の重要性を強調しておきたい。

○ 今回のパブリックコメントを踏まえた、サイバー対処能力強化法に基づく基本方針案について賛同する。

○ 本日のご説明内容についても、中小企業等を含めた事業者からの十分な意見聴取を行いながら進めていただき、感謝申し上げる。この度の基本方針案については、賛成する。

○ 今後も引き続き、政省令の策定を含め、本法の運用にあたっては、その実行性を担保するためにも、中小企業を含む事業者から実態や意見を聴取し、必要に応じて適切な

支援を講じていただきたい。

○　特に、経済安全保障推進法と本法との関係については、窓口の一元化による分かりやすい説明を行うことが必要である。また、届出・報告等の事務手続きを、必要最小限にするとともに、重複により事業者に過度の負担が生じないように、関係省庁の十分な連携をお願いしたい。

座長

○　いずれの指摘に対しても今回の基本方針案の中で反映されており、政府として適切に対応していると考える。本日諮られている基本方針案について、異議はありませんでしょうか。

（異議なしの声）

○　それでは、賛同が得られたということで、本有識者会議として本案を了承したい。事務局においては、先ほど大臣のご発言もあったが、今後、閣議決定に向けて作業を進めてもらいたい。

（３）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。

○　基本方針のパブリックコメントの対応についてご案内いただいたように、多数の事業者が関与していくものであり、我が国でも例がない取組であるので、多くの利害関係者から強い関心が寄せられていると認識。基本方針についても制度の認知度が高まり官民連携への期待が高まっているが、事務局でもご配慮頂いているとおり、負担軽減を考えないと機能しにくいと考える。

○　その観点で、資産届出については、４半期に１回の棚卸という仕組みは、実運用に配慮した現実的な仕組みとなっていると考える。また、維持管理を行っているベンダーからの直接の届出なども、負荷軽減に資する仕組みであると考える。ただ、維持管理ベンダーと協力して届出する資料が多いことを考えると、誰が維持管理ベンダーとして届出を出すかの明確化も必要になってくると考える。また、そうした相談に対応する体制の整備も必要になると考える。

○　経済安保推進法の届出についても、政府内連携をしていくということは、行政間の手続の簡素化に資するもので、ワンストップ、ワンスオンリーという理念に沿った仕組みだと感じている。

○　インシデント報告については、報告受領後に、どのようなリアクション・コミュニケーションが期待できるのか、報告する事業者の立場からすると予見性があった方がよいと考える。社内外のリソースを確保する観点からも重要であり、こうした点がよ

り明確になるとよいと考える。

○ この取組みがうまく進めば、日本が被害者となるサイバー攻撃が報じられることも少なくなり、パブリックアトリビューションを行う場合を除き、取組みの成果が表に出ることはなくなることもあるかもしれない。そうなると、国民からみると、この取組みは役に立っているのか、という話になるのかもしれない。しかし、大きな被害が生じていないということでもあり、よいことではある。
○ 官民連携強化に向けては関係者間の信頼構築が重要であり、協議会はそのために非常に重要な組織である。これまでも分野別に様々な情報交換の枠組みがあり、上手くいったものもあれば、そうでないものもあったと思う。新しい協議会が単に従前のものに上乗せされる形となってしまい、形骸化することのないようお願いしたい。
○ インシデント報告については、もちろん出す側の責任が重要であるが、同時に、受ける側の能力、受ける側が理解できているということも重要。この点、国から協議会の運営形態について分かりやすいイメージが示されたことはよいことである。資料5の12 頁の5類型に限るということではなく、情報共有ができる積極的なアプローチを進めて欲しい。また、言うまでもないが、被害者を罰するような形になるとうまくいかない。そうならない配慮をお願いしたい。
○ 専用設計品については、届出義務の対象外ということだが、実際問題、攻撃で狙われる可能性は低いとはいえ、相手が本気ならばまさかという攻撃があるかも知れない。責任が免除された訳ではないことをこの際に確認しておきたい。

○ 官民連携の強化について、行政法の視点から3点コメントしたい。
○ 1点目、情報共有のための法律上の手法は、届出と報告となっている。この手法の検討には、入口と出口の問題があると考える。入口、すなわち、届出や報告を求める場面では、どのような内容をどのようなタイミングで届出、報告しなければならないかを可能な限りわかりやすく示しておくことが重要である。
○ 届出、報告にあたっての負担を減らすという実質的な面から、届出、報告をする者にとって便利な仕組みにしておくべき。加えて、出口であるが、必要な届出や報告がなされていない場合について、情報の提供を、直接に又は間接に強制する措置を講じなければならない。資料の中で言及されている罰則は間接的に履行を担保する手段であるが、罰則のみでは必要な情報が提供されるわけではないことに留意が必要。
○ 官民連携の強化という視点を意識するのであれば、仮に事後的であっても、必要な情報の提供を受けるためにどのような政策が必要か考えていく必要がある。情報共有を図る、促す、場合によっては直接に強制する、という順序で措置を進めていくことについて考慮の必要がある。
○ 2点目、人のつながり・連携をつくるための法律上の手法は、協議会の設置、すなわ

ちチームづくりということになる。これについては、いうまでもないが、まずチームをつくりあげること。その上で、つくりあげたチームを上手く育てていく必要がある。様々な手法が考えられるが、既に基本方針案に記載されているものでは、第６章第２節にある、平時から常設のグループを設置しておくこと。さらに、資料５にある協議会フレンズという、協議会の周辺にあって下支えをする組織作りが重要となる。併せて、協議会の構成員による自発的な情報交換や意見交換を活発化させていくためには、議論を促すファシリテーターを置くことや、各事業者のベストプラクティスといったポジティブな情報の共有を促すといったことも重要だと考える。

○　最後に３点目。施策遂行に必要な長期のツール・インフラの整備・強化については、まずもって政府が責任をもって、人的・物的・経済的なリソースを確保していくことが初めの１歩となる。また、ベースの部分は、横断的なプラットフォームとして統一的でシンプルなものとなるよう、それぞれの分野の専門的見知を活用して、構築していく必要があろう。

○　この取組みが官民双方にとって有益なものとなるためには、運用レベルでの具体化が非常に重要。各企業の現場リーダークラスの人との意見交換を継続的に重ねてもらいたい。

○　有識者会議とパブリックコメントを通じ、基幹インフラ事業者にとっての負担軽減、また、政府に機微情報を集めることはむしろ攻撃の的となるリスクがあることを考慮してほしいことを要望してきた。今回の提案で、特定重要電子計算機で用いられるＩＰアドレスやネットワーク構成図が届出の対象から外れていることは、単に簡素化に止まらず、リスクを下げることにもつながっている。こういったことが、官民のお互いの信頼感や協力関係が制度をよりよいものにしていくことにつながると思うので、引き続き意見交換を続けて頂きたい。

○　基幹インフラ事業者企業の中でもサイバーセキュリティ対策の成熟度に差があることは理解している。このため、平時から広く情報収集して脅威に備える以上に、有事の際に事業者間での速やかに連携が行われることも必要。ＮＣＯのリーダーシップの下、意見交換の場を設けることを要望したい。

○　協議会への参加のインセンティブが重要となるが、この点、一定の配慮がされているものと考える。

○　その一方で、協議会は始まってみないと参加者間でイメージが共有されない部分もある。このため、実際には、始めながら、あるいは手探りで、協議会の在り方、情報共有の在り方が共有されていき、それを通じて信頼醸成が進んでいくことになると思う。この点ＮＣＯがリーダーシップをとるよう、お願いしたい。

○　特に資料５の 12 頁にあるよう、協議会の活動が活発化し、情報交流が進むことは参

加者にとって重要。ありとあらゆる支援をお願いしたい。

○ 事業者は業態によっていろいろと異なるが、そういった声を丁寧に拾って頂いたことに感謝を申し上げる。
○ その上で、事業者側が提供する情報については、システム構成図など色々あると思うが、企業にとっては機微情報も提供するということなので、法律に基づいてしっかり管理することを徹底していただきたい。
○ ２点目、企業が情報を提供することに関して、情報は質も量も異なってくると思うが、そのことで協議会において差別的な取扱いを受けないようにしてもらいたい。
○ また、協議会での官民双方向でのコミュニケーションを円滑化するという観点で、官民双方で立場の違いや情報の非対称性がパワハラと受け取られる事態につながらないよう気を付ける必要があると思うので、協議会の運営にあたって、ご留意いただきたい。

○ 官民連携が極めて重要と認識。これがうまくいかないと情報が提供されず、共有もされない。その上で、協議会について、２点ご留意頂きたい。
○ １点目は継続的な運営をどのように行っていくかについてである。協議会のような会議体については、最初はともかく、途中で尻すぼみになってしまうことがよくある。そうならないように、途中でのてこ入れ策など、継続的な運営策を考えておいていただきたい。
○ ２点目は柔軟な対応についてである。資料５の 10 頁で構成員、協議会フレンズ、その他という二段階、三段階の構成が示されているが、この構成自体は実務上有効な構成だと考える。ただし、準会員的な位置付けの参加者が重要な情報を持っている場合もあり得るため、そうした場合には必ずしも硬直的な対応をせず、柔軟な対応ができるような仕組みづくりの検討もお願いしたい。

○ 今後の官民連携について、協議会に関して意見を申し上げる。基幹インフラ事業者だけでなく、準会員的な位置づけの協議会フレンズをつくるということだが、ネーミングがすごく良いと思う。サイバーセキュリティという肌の温もりが感じづらい分野において、温もりを感じることができるような名前を作っていただいた。仮称となっているがこれを本当の名前にして、血の通った組織にしていただきたい。
○ それから、具体的なフレンズの範囲について。アサヒグループホールディングスがサイバー攻撃を受けて、アサヒだけでないビール業界・飲食業界全体に大きな影響が出て、個人情報も漏えいした、あるいはそのおそれがあるという状況になっている。
○ また、通販サイトのアスクルもシステム停止に追い込まれるというようなこともあった。今後、こうした実際に被害にあった企業にもフレンズに入っていただいて、何

が起きてどういう被害があったのか、そして、どういうＢＣＰが実行できるのかなど経験から学べることを、ぜひシェアして頂ければと考える。各社が、もし同じ立場になったらと考えるきっかけになり、縦方向だけでなく横串を指した形で社会の集合知としていくことが出来るのではと思うので、政府の方からそうした働きかけもしていただければと思う。

○　多くのパブリックコメントを踏まえたブラッシュアップをしていただき感謝。
○　資料５の官民連携の方向性を読み、本当に分かりやすいと感じた。特に資産届出については、具体的なイメージがわくとともに、これが大変だということも改めて確認した。
○　協議会に関して２点ほどコメントを申し上げたい。資産届出やインシデント報告は規律の側面が強い取組だと理解しているが、一方で協議会については、自発的な参加、企業の取組が重要である。
○　基本方針案にあるとおり、構成員のニーズも踏まえた情報提供、これは究極的にはサイバー攻撃を予防するための情報といったことになるかと思うが、例えば、基幹インフラなのかそれ以外なのか、企業内の情報の受け手が SOC なのか、CISO なのか、それ以外のマネジメントなのかなど。基本方針案にも技術情報だけでなく経営判断に資するとある。全てに対応することはできないと思うが、サイバー攻撃の予防に関する企業ニーズを細分化し、情報提供・対応頂けるとより現場にとって有益になると考える。
○　２点目は資料５の 10 頁の協議会構成員（初期）から漏れる企業、協議会フレンズ向けの対応について。例えば、自動車産業、製薬会社、ホテル、旅行業などは協議会構成員（初期）から漏れる。旅行やホテルは、国家背景のサイバー攻撃とは遠いように見えて、先日のソルトタイフーンのパブリックアトリビューションでも通信やホテル、旅行は個人を追跡するための標的とされていた。
○　一番上のレイヤーから漏れている事業者にどうアプローチしていくか。それがフレンズという枠組みだと思うが、場合によっては、協議会構成員そのものとなる可能性も検討してはどうかと感じた。

○　官民連携の強化に向けた今後の方向性についてコメントしたい。協議会について。資料５の 10 頁で、３つのカテゴリーに分けることとしているが、これは実践的に有効な建付けであろう。一方、こうした分類の基準をどれだけ柔軟に現実に対応させるか、基準づくりなり、ガイドラインなりで明確にする必要があるのではないかと考える。
○　どのカテゴリーに入るかは、国側からの要請だけではなく、事業者側からの要望やニーズとの組み合わせで決まることでもあり、その点の配慮が重要。必要な情報が第２カテゴリーであれば得られない、逆に、第１カテゴリーに入ってしまうと、機微情報

まで得られる反面、様々な義務を負うことになるなど、それぞれのカテゴリーで義務や特典が異なることから、事業者側もそれを考慮して行動することになるのであり、これにどのように対応していくかも考える必要があると思われる。現実の状況に即した形で、事業者と協議して、３つのカテゴリーを維持しつつ、柔軟に参加者を確保していくかが、協議会の継続的な運営にとって重要。

○　資産届出、インシデント報告、協議会それぞれについて感想を述べたい。
○　資産届出について、資料 5 の５頁に記載のとおり、業種・業態等に応じて異なるため、それを踏まえて対象範囲を考えていくことが適切。これまでの大規模なインシデント事案において、この業種ではこういうシステム構成をとっていてここがやられたといった情報はＮＣＯに蓄積があると思われ、また、協議会を通じても、ここが危なかったといった情報も新たに入ってくると思われるところ、これらも適切に共有して頂きたい。
○　インシデント報告について、ＥＵにおいては、デジタルオムニバスパッケージの提案がなされているが各種の法令に基づく報告を一元化する、レポートワンスにしていくという提案だと承知している。既に日本でもこの種の取組が進みつつあるところであるが、特に海外においてこの種の対応をされる事業者の方々も踏まえて、グローバルな調整の要否も含めて、検討いただければと思う。
○　協議会について、資料５の 12 頁は情報共有の枠組みがイメージでき、大変分かりやすいと思った。参加するそれぞれの事業者の目線で考えると、その中において経営層、セキュリティ専門家、前線の一般従業員など、それぞれ対象によって刺さる情報が異なると思うので、参加者に情報をきちんと持ち帰ってもらえるような情報発信、運営をお願いしたい。
○　最後に、協議会のガバナンスについては、外からみて不安を持たれぬようしっかりお願いしたい。事務局機能を担うＮＣＯの負担も大きいと思うが、適切に取り組んでもらいたい。
○　また、人の入れ替わりにも留意。構成員たる事業者がＭ＆Ａや会社分割により入れ替わることもあろうし、専門家の退職、異動により入れ替わることもあるので、そうした中でもきちんと引き継がれていくようにしてもらいたい。

○　非常に分かりやすく、かつ簡潔にまとめられていると考える。
○　その上で、協議会が情報の機微度に応じて柔軟な体制が必要だという点は、有識者会議の総意だと思うので、こういう形で整理いただいたことは評価できる。セキュリティ・クリアランスに関しては、重要経済安全保障情報を誰が取り扱うのか、クリアランスが必要なのはどの範囲かという点は整理が必要かと考えるが、重要経済安全保障情報に関しては別な法律によってガバナンスされているので、これはこれで一つ

の整理かと感じる。

○　現実的なメンテナンスの合理性の観点からネットワークが構成されているケースもあり、セキュリティの観点からはメリット・デメリットがそれぞれあると思う。

○　この短期間で、ここでの議論やパブリックコメントも含めて、必要十分な内容をまとめていただき、感謝。

○　今後の方向性にある資産届出やインシデント報告、協議会について、それぞれ事業者に一定の負担をいただくこととなる。

○　例えば、資産届出であれば、当然のことながら、日頃のメンテナンスでいっぱいいっぱいな中で、さらにこうした届出の対応をやらなければいけない、また、システムに電子計算機を新たに導入したり、あるいは変更したりするときに設定の大変さがある中で、さらに届出をいただかなければならないことになる。既に色々と工夫をしていただいているが、その具体的なイメージが事業者に共有されるようにより一層進めてもらいたい。

○　また、インシデント報告についても同様。インシデントといっても大小様々であるが、重大なインシデントであれば、ＢＣＰや顧客対応なりで手一杯な中で、これに加えてインシデント報告いただくことになる。

○　そのため、報告へのメリットを感じていただけるように、日頃からの協議会での信頼関係の構築や、有効なフィードバックなどが重要になってくると考える。インシデント報告が、公共的な利益に資するということだけでなく、報告事業者にもフィードバックがあり、メリットがあると思って頂けることが、本制度を運用していく上で非常に大事になってくると考える。そのため、協議会では、技術的な判断だけでなく、経営問題として事業者に捉えて頂けるように上手く対処していくことが重要。

○　資産届出については、常にその必要性と負担軽減が言われるところ、状況に応じてダイナミックに政策を展開していくためには、政府側が届け出られた情報を効果的に活用することが必要である。新たな項目についても報告が必要になるとか、逆にこの部分は、もう対象外にしてよいのではないかといった判断が出てくることも考えられる。政府の側で報告を主体的に活用し、事業者の負担軽減に留意しつつ、何が必要かについて常に考えていくことが重要である。

○　施行されるまでの間に何か大きなインシデントが起きることもあり得るが、その場合には、そこから得られる教訓を適切に反映させていくような努力もお願いしたい。

○　資料５の 10 頁の協議会構成のイメージは非常に分かりやすい。フレンズについては、専門性のある人たちの集団となるので、その場での双方向の情報流通を積極的に行うことが必要。

○　また、情報共有に際しては、その中身を事業者がどのように理解するかが重要であり、

どうすれば情報の受け手が活用できるようになるのかという観点に留意して進める必要がある。

○ Need to share が重要。情報源の秘匿が必要な場合などもあるが、工夫して共有の範囲をできるだけ広く捉えるようにして頂きたい。

○ サイバーセキュリティそのものに関する情報だけでなく、その背景情報についても積極的に伝え、持ち帰った者が上司に上げやすくなるよう、十分に配慮していただくことが重要。

○ 資料5の協議会の運営イメージは分かりやすいが、(1)～(5)の全てに入っている政府側は全体を見ているのでよくわかるとしても、情報の全体像に触れられない個々のグループにとっては、ポイントが見えにくく、結果的によく理解できない情報が存在する。その意味で背景情報の提供等が重要であり、政府が付加価値を提供することで、信頼関係の構築につながる。

○ 協議会の運営をしっかりガバナンスするため、役所の人事異動はあまり頻繁にしないで頂きたい。継続性があってこそやれることもある。

○ 官民連携に関して、各省庁で行っているガイドラインとの整合性に配慮してほしい。半導体デバイス工場における経産省からのＯＴセキュリティガイドラインは的を射たものであるが強化法との連関を示した方が業界からの理解が得られるのではないであろうか。

○ 報告期限について「速やかに」と記載があるが、時間を明確にすべきである。例えば、米国の重要インフラに係るサイバーインシデント報告法ではサイバー攻撃から72時間、ランサムウェア被害を受けた場合は24時間以内とされている。

（３）川崎内閣府政務官挨拶

○ 本日は活発なご議論に感謝。

○ 私も先般、国会答弁で、官民連携の協議会のあり方について答えたが、技術者だけでなく、経営層もこれを受けてどうするのか、ということを考えることが非常に重要なことだと考えている。内閣府の方でしっかりこの協議会のあり方を考えて頂きたいと思っている。

○ 何人かの構成員の皆様から、チームワークをよくして上手くやっていこうというような議論があったが、それについて、私の個人的な考えを申し述べたい。

○ 資料5の10頁の協議会の構成の部分で、その他協議会構成員の中に、ベンダーと自治体が含まれている。自治体というと基礎自治体のみで1700程度あって、その自治体とお付き合いしているベンダーというのもある。自治体のみが入ってもベンダーが入っていなかったら意味がないが、他方、一度に全ての自治体及びベンダーに入っていただくのは困難だとも思うので、協議会が上手くワークするためにどういう構

成でやっていけばよいのか、この先しっかりと考えていきたい。また皆様のご意見を頂ければと思う。

（４）松本内閣府特命担当大臣（サイバー安全保障）挨拶

○　基本方針案については、閣議決定に向けてとりまとめができ感謝を申し上げる。これを基に、官民連携と通信情報の利用について、より一層実行力のあるものにすべく、我々としても準備を進めてまいりたい。

○　人事異動の話があった。私もこの職について色々と話を深めていく中において、特にNCO のスタッフの専門性の高さということを考えると、きちんと考えていかないといけない。常にレベルを上げていかなければならない部署であるので、御指摘の点は私もしっかりフォローしていきたいと思っている。

○　これから政省令の策定に向けてしっかりと議論を進めなければならないので、引き続きご指導を賜りたいと思う。本日の議論に感謝申し上げる。