「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 1 回）議事要旨

1. 日時：令和 7 年 9 月 19 日（金）10 時 30 分から 12 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）

平 将明	内閣府特命担当大臣（サイバー安全保障）
岸 信千世	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）平内閣府特命担当大臣（サイバー安全保障）挨拶

○ 構成員各位におかれましては、御多用のところ、お集まりいただき、まずお礼申し上げます。

○ 国家を背景とした高度なサイバー攻撃への懸念の拡大や、社会全体における 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、喫緊の課題です。

○ これらの制度整備により、基幹インフラ事業者等からのインシデント報告や通信情報の収集が可能となり、より早期、かつ、効果的にサイバー攻撃を把握して、対応することが可能になると考えております。

○ こうした「官民連携の強化」や「通信情報の利用」に関する施策を適切に機能させるため、サイバー対処能力強化法では、「重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針」を策定することとしております。

○ この基本方針を年内目途で策定するにあたって、有識者の皆様から御意見を伺い、充実したものとなるよう、本有識者会議を立ち上げることとしました。

○ 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御意見をお願いできればと思います。

（2）座長の互選

構成員の互選により、高見澤構成員が座長に選出された。

（3）座長代理の選出

高見澤座長の指名により、酒井構成員が座長代理に選出された。

（4）事務局説明

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の策定に向けた説明があった。

（５）討議

○　警察に対して情報がどのように行くのかという点が気になっている。今までは、被害が発生していて、これが逼迫した状況になった場合に警察に情報が行くような仕組みであり、その判断においては、警察は普段、裁判所から令状を得るなど司法機関と話をしていた訳だが、今後は、これまでのフェーズとは異なることから、どのようにして情報が行くのかという点を国民にどう見せ、説明していくのかを考えていく必要があると思う。

○　全体として一番気になるのは通信の秘密の話であり、利用する情報がメタデータだから大丈夫ということにはならないため、どのような条件であればこれを利用してよいのかを丁寧に考えることがポイントであると思う。

○　官民連携については、事業者に対する義務であるとしても、民間がついてこられるような形のインセンティブ設計をすることが重要である。また、業界団体の組織率が業界によってまちまちであることを踏まえれば、網羅性という観点から、関係事業者を全部把握して、連絡のパスをつくるのかといった点も含めて、建付けをうまく用意する必要がある。

○　中小企業への配慮の観点から３点申し上げる。先ほどのご説明で、既に基幹インフラ事業者にヒアリングを実施していると伺ったが、その中には中小企業も入っていると認識している。今後、協議会が設置されれば関与する中小企業が増えることになると承知している。中小企業は予算、人員などが大企業と比べて限られることから、制度の実効性を上げるためには、こうした中小企業に情報を提供してサイバー攻撃に対応できるような形にすることが重要。

○　１点目として、中小企業関係者への周知・説明をお願いしたい。経済安全保障推進法、個人情報保護法など関連する法律がある中で、どのように位置づけられ、関連しているか、全体像を分かりやすく説明してほしい。また協議会の対象者だけではなく、協議会の対象者になり得る者に対しても説明をお願いしたい。

○　２点目は、中小企業の過度な負担にならないように実効性を担保できる最低限の負担になるようお願いしたい。いろいろな行政機関が関わると思うが、可能な限り一元化して、中小企業が対応できるようにしていただきたい。

○　３点目は、中小企業に必要な支援をお願いしたい。対象事業者は対応にコストがかかることになるので、どのように支援できるかご検討いただきたい。

○　当団体ではサイバーセキュリティ対策を全ての事業者にとっての経営の最優先課題と位置付けている。官民双方向の情報共有、人材交流を通じて我が国全体のレジリエンスを高めていくことが重要。サイバー空間は経済活動・国民生活の基盤であると同時に安全保障にも直結するので、官民がしっかり連携して実効性ある対策を進めて

いくことが重要。

○ こうした観点から、強化法で官民連携の仕組みを制度的に整備したことは大きな意義があり高く評価している。政府が積極的に情報を提供して官民双方向で共有していくという基本的考え方は、現場の対応力を底上げして、結果として国全体の対応能力を高めると理解している。

○ その上で、基本方針の策定にあたっては、現場の実務をしっかり踏まえて頂きたい。また、事業者に過度な負担が掛からないようにして頂きたい。例えば、資産届出の対象は合理的かつ最小限にして、事業者ごとの実態に即した形で柔軟な運用方法をご検討いただきたい。またインシデント報告についても実態に即した制度設計をお願いしたい。具体的には、個人情報保護法や各種業法といった既存法令に基づく報告との一元化が必要。

○ 実効性と持続性を備えた基本方針となるよう議論に貢献していきたい。

○ まず、3ページの機械的情報の考え方について、通信の秘密の観点からのコメントであるが、手続面による透明性の確保を明確にして頂きたい。本件の事柄の性質上、事項の内容を詳細に出来ないと思われるため、透明性の確保は手続により行うしかないので、その点を明確に記載して欲しい。この点が明確になることで、市民の側においても安全・安心が確保されることになる。

○ 当事者協定のところでメリットを記載しているが、当事者協定に加わる事が国民から批判を受けるような不安・懸念があるようでは、なかなか参加頂けないと思われるため、対象である情報についての手続的透明性の点は4ページの当事者協定の締結にも影響してくるものと考える。

○ その関係で、5ページで他法令の遵守に関する配慮事項に関して、「他の法律に基づき通信情報の提供を求められた場合には、提供しなければならない場合を除き」との記載があるが、提供するかどうか（法律で許すか許さないかの優先関係）について、ある程度の優先関係の考え方を示して頂いた方が安心出来る。

○ 7ページの電子計算機の使用する者に対する周知等と電子計算機等供給者に対する情報提供の部分で、優先的に対応すべきものを特定できるようにとあるが、それに類するものとして、周知情報も、読んだ側で意味づけが分かるような形で出していただきたい。

○ 基本方針の骨子たたき台については、様々な目配りがされていて大枠は賛成。特に通信の秘密への十分な配慮が明記されていることは安心できる。

○ この取組は国が音頭を取る必要はあるが、政治と国民の間の信頼関係が薄くなりつつある中で、国の立場はあくまでハブであるという位置づけを明確にすることも大切。

○ 官民連携について、事業者の立場としては社内で担当する者は極めて限られており、まだ周知が足りていない状況でもあるため、しっかりリスクを周知することが大事。過度な負担にならず判断に迷わないような明確な基本方針であるべき。
○ また、事業者からの情報共有へのフィードバック、適切な情報公開が大切。

○ 今年5月にACD関連二法が成立してから、民間企業から「詳細な制度設計はどうなるのか」という質問をよくいただく。今回の基本方針は、こうした疑問に答えるものになっていると考える。
○ その上で2点コメントしたい。1点目は、同意に基づく通信情報の取得について、骨子たたき台の第2章第1節では、企業には負担発生を理解いただくとともに、メリットを示すことが重要だと記載されている。負担はイメージできる一方で、メリットは想像が難しく、通信情報の取得に同意しないという方向になりかねない。例えば、同意した基幹インフラ事業者に対しては特別な情報が提供される、不審な通信先と接続がある場合に政府が注意喚起を行うなど、何らかの具体的なメリットを示していただくことで、事業者が協定締結に向かうと考える。
○ 2点目は、特定侵害事象等の報告に関するもの。骨子たたき台の第4章第1節（2）にある明確な閾値設定と抽象的な目安というのは、一見矛盾するように見えるが、非常に重要。特に後者については例えば、今、流行しているサイバー攻撃キャンペーンを特定した上で、閾値以下であっても報告を求めるという考え方で、非常に重要だと思っている。
○ 一方、企業からすれば、報告のデッドラインが実務的な論点となる。特定侵害事象等の報告の目的が統計的な分析や総合整理分析のためであれば、それほどの速度は求められず、数日単位だろう。他方で被害拡大防止に役立てる、あるいは注意喚起に使うのであれば、より速報性が求められるのではないか。アメリカやオーストラリアのような時間単位での報告義務化もありうるのではないか。特定侵害事象等の報告の目的が中長期的な統計の分析なのか、素早く被害を防ぐことなのかで大分制度設計が変わると考える。
○ 余談だが、重要インフラ事業者の中には、最初の報告を「第一報」と言わずに「第ゼロ報」として経営層や関係部門に報告している例がある。「第ゼロ報」の意味するところは、事案確定前の不確実な情報でも空振りを前提として報告・共有するマインドを醸成する、ということ。被害拡大防止という観点では、そういったネーミングや設計も必要ではないか。
○ 協議会構成員向けには「経営層の判断に必要となる攻撃の目的や背景等に関する情報」の提供が想定されているが、基幹インフラ向け情報提供や一般向けの注意喚起にも目的や背景に関する情報をより盛り込んではどうか。
○ オペレーショナル、タクティカルな分析結果、技術的情報はサイバー攻撃を防ぐ上で

重要であり、総合整理分析情報でオペレーショナル、タクティカルな技術情報にフォーカスするのは当然。他方、この類の情報はIT・セキュリティ部門、CSIRT、SOC、CISOが用いる情報。この情報が過度に強調されると、経営層の意識が「サイバーセキュリティは経営課題」ではなく「サイバーセキュリティは専門部門の仕事」とミスリードされる恐れがある。

○ 「サイバーセキュリティは経営課題」とするためには、①経営層が理解できる言語・用語で、②経営層の関心にあう情報分析・提供をさらに充実させていくことが必要。

○ これまで経済安全保障推進法に関わってきたが、関連の法整備が進んでいることを歓迎する。サイバー対処能力強化法が経済安全保障推進法の基幹インフラ事業者を義務の対象としていることもいい考えだと思う。

○ 企業にあまり負担を求めないようにとの声があるが、そればかりでは対応できなくなりつつある。中小企業への配慮は必要だが、サイバー空間も変化しており、国民生活、企業の経済活動を守るために、特に大企業は対応しなければ、生き残れないと思う。政府も企業のマインドセットを変えるために、企業がサイバーセキュリティの責任を負っていることを遠慮せず発信した方がよい。

○ 法律は対処を対象にしているが、サイバー安全のためにはもう1歩踏み込んでほしい。コンピテンシーパワーを国が持つために、盾だけでなく矛をつくることが重要。本会議でということではないが、ぜひ考えてほしい。

○ 骨子たたき台については概ね賛成であるが、第5章第1節⑵の「外国の政府等に対する情報提供」の部分でいくつか指摘しておきたい。

○ 同項の②として、「提供する外国政府等が法に規定する情報の取扱いに係る適切な措置を講じていることを明示的に確認する」とあるが、これからサイバー空間の中でのグローバル・スタンダードを構築していくということになると、強化法ほか国内法上の基準というものが国際的にどこまで通用するのかということも考えていかなければならない。他方で、国際関係においては、国際協調の観点から相互主義が働く余地は十分にある。

○ また、「諸外国」については欧米諸国を念頭に置いているように思われるが、サイバー空間のリスクに対しては、例えば、グローバル・サプライチェーンへの影響等、多くの国々が関係することになるため、先進国、途上国を問わずに、関係構築や情報提供をすることを考えなければならない。

○ 国際協力をいかに発展させていくかというのが、外国の政府等へ情報提供する側だけではなくて、逆に提供してもらう側になった場合においても重要な視点となるのではないだろうか。

○　お示しいただいた資料は多くの点がカバーされており、大きなコメントはない。その上で3点話しておきたい。
○　コスト負担について、2013 年 6 月に、企業が米国の情報機関にデータ提供を行っていた事実をエドワード・スノーデンが明かしたが、関係者になぜそんなことが可能なのかを尋ねたところ、間接的な支援することによってある程度バランスを取っているとのことであった。今回我々がやろうとしている同意を取った上での情報共有においては、今の日本政府の立て付けの中では難しいと思うが、そういったことを考える余地はあってもよいのではないか。
○　5ページの通信情報の取扱いについて、情報共有の方法は非常に難しい。10 年ほど前、外国政府の担当者にどのように情報共有を行っているのかを問うたところ、紙に印刷してそれを相手のところに持って行くということであった。ずいぶん昔の話であるので今はそんなことはないと思うが、機微な情報はなかなかネットワーク越しでは共有できないため、対面で会って相手に真意を伝えることが重要だとのことであった。ただ、今回の法で扱うのは機械的情報であり、例えばメタデータがぎっしり詰まったエクセルファイルを印刷して持って行くのは全く無意味であるところ、どのように電子的にデータを共有するのかは難しく、考えておく必要がある。
○　総合整理分析情報について、関係者間で言葉が通じない可能性がある中で、まとめた情報をいかにそれぞれの者が理解するかという点は難しい。例えば、文系と理系の間、タクティカルなレベル、オペレーショナルなレベル、ストラテジックなレベルの間での言葉の違いをいかに乗り越えていくか。また、国際的な情報共有を行う場合には、一層意思疎通が難しくなる点も踏まえて、検討しておくべきである。

○　先ほどのストラテジック、オペレーショナル、タクティカルなインテリジェンスに関する発言を受けて、改めてストラテジックなインテリジェンスの重要性を再確認。

○　個人的な思いとして、この会議が重要だと思っているのは、国境を越えてすごい勢いでアタックがかかっていることに対して危機感を持っているという政府の考え方はよくわかる。ルールがあってフェアにゲームをしているのではなく、ルールのない世界でのたたき合いになっている。何がアンフェアなのかという定義のない中での戦いになっていると承知している。
○　一方で、そういったルールがない中で何をやってもよいわけではなくて、日本国として絶対に守らなければならない民主主義、法の支配といった価値観については、そうした戦いの中でも必ず維持していく必要がある。それがこの法律であり、この会議で討論している基本方針になると理解している。
○　その上で、ベンダーの視点から3点指摘したい。1点目は、7ページ目電子計算機等供給者に対する脆弱性情報の提供について、脆弱性情報の機微の程度はおそらく提

供用情報、周知用情報の両方にまたがるものと考える。ゼロデイアタックが懸念されるような緊急なものはある程度機密が守られるところに迅速に出していただくべきだと思うし、時間が経過した後の情報に関してはできるだけ広く周知するべきと思う。運用がどのような形となるのかが気になる。

○　２点目は、６ページの事業者負担について、インフラ事業者のハードウェアやネットワークを実際に構築するのは Tier１以下の事業者、いわゆるベンダーである。ソフトウェアに関しては頻繁にバージョンアップがされたり、パッチの情報が回ったりする。それをバージョン管理していく必要があるので、丁寧にやればやるほど負担が生じる。Tier１以下の事業者の負担にも目配りいただければと思う。

○　３点目は、６ページの一番下の事務委任について、一部８ページにも事務委任の記載があるが、委任が想定されるということまでしか書かれていない。国家公務員の場合は、国家公務員法に基づいて罰則規定がある形で守秘義務が担保されているが、委任した先も何らかの手段で担保する必要がある。

（事務局）

○　第７２条第５項にはみなし公務員の規定があり、守秘義務以外の収賄などがあった場合には第５項の規定によることになる。

○　２点話させていただく。１点目は、事業者負担（インセンティブ）の話が続いているが、最終的には理解いただくことに尽きる。事業者が業務で車を使う場合に、事故が起こるリスクを理解しているので、躊躇することなく保険料の負担をしている。そういうレベルでの理解を得ていくことが非常に大事である。

○　その意味では、協議会に企業が入ることでどのようなメリットを得られるのか。経済的利得とまで行かなくても、サイバーセキュリティの負担の軽減など、少ない負担で大きな効果を得られるということを、内部での情報共有の在り方あるいは情報提供の在り方、機械的情報のメタデータを羅列しても分からないので、意味のある情報に見えるように加工して提供するという工夫すべき。

○　民間企業もサイバーセキュリティの重要性を分かってはいるが専門家と比べると多少の温度差がある。専門家と一般の方の視点の違いのギャップをいかに埋めていくかが大事だと思っている。

○　２点目は、刑事法の視点だが、広い意味での脅威情報の扱いについてである。強化法は、犯罪捜査を目的とするものではないという位置づけになっているが、脅威情報を守りに使うだけではなく、攻撃者の逮捕や外国に捜査協力を依頼するといった攻めに使うこともありうる。脅威情報の扱いについては、刑事手続、犯罪捜査と相容れない仕組みではないことを強調させていただく。

○ 総括的なお願い事項ではあるが、基本方針として良くできているとしても、全体として分かりやすいものとするためには、できるだけ背景情報を取り入れて、社会全体的な強靱性を高めることにつながるものだという分かりやすいナラティブを作ることが大事。

○ 基本方針の解説になるのかもしれないが、サイバー部門の責任者や組織のトップが分かるようなエグゼクティブサマリー的なものができ、その中にナラティブと企業にとってのメリットが分かる工夫をしていただくことが大事である。

○ 基本方針の策定後、政省令を具体化されると思うが、今のサイバー安全保障環境を考えるとアップデートのスピードが激しいので、基本方針をテンプレートとして、その具体化や進捗状況が電子的にも広がり、検索・理解できる形にすることが非常に大事だと思っている。NCO を中心に関係省庁の色々な施策が有機的につながるものがあればありがたい。

○ 骨子たたき台第 2 章第 2 節⑵に記載されている当事者協定のひな形は大事だが、ひな形で規定する内容が最低限のものになってしまい、運用状況に応じて更に発展させる必要があるにも関わらず、それが一番低い層にそろってしまうことは避けるべきである。すなわち、ユーザなり実際に関わっている分野に応じて求められるレベルの違いがあると思うが、ひな形をうまく発展させるマインドセットが大事。

○ 負担や正当な理由によって協力できないことがあるとは思うが、そのコンテクストの違いにより拒む正当な利用が広がる場合もあれば狭まる場合もあるので、幅があることに留意してもらいたい。プライバシーの問題についても同様だと思う。

○ 負担という概念が良くないと思っている。中小企業支援も必要だが、企業が DX や AI、DB の整備も活用しながら、サイバー分野で積極的に協力することが、実質的な効率化やシステム化につながり、コストが改善するという捉え方ができればと思う。

○ 情報の共有に当たっては、一番大事なのは機微性を一律に捉えるのではなく、総合整理分析情報を生かして、情報の読み方も含めてなるほどという形になるのが大事だと思う。情報共有に伴う時差が起きがちなので、過度に抑制的にならいように、タイムリーに情報の読み方・意味づけをはっきりと伝えたら良いのではないか。そうなると政府側から様々なソースに基づくバックグラウンド情報を出していくのが大事であり、共有していく中で、その当事者にとって光って見える情報として伝えていただきたい。

○ 今回のものは経済安全保障における基幹インフラに対するサイバー対処能力強化ということであって、これをやったからといってサイバー空間が強くなるとは全く思っていない。これをやったら、良くなるというのはミスリードになると思うので、今回あくまでも基幹インフラに対するサイバー対処であって、サイバー対処能力の強化ということを明確にして欲しい。

○　一番問題なのは報道にもでていたが、どうしようもないエッジのデバイスの脆弱性。ここから入ってくることが多いので、今回は今の位置づけが重要なポイントだと思っている。

○　基本的な方針の策定にあたっては、通信の秘密の保護が図られることについての信頼感の醸成が必要であり、その信頼感を損ねるインシデントを招じさせないことはもちろんのこと、偽情報などで通信サービス利用者に不信感が蔓延しないことへの留意と広報が必要になってくると思われる。
○　昨今、犯罪に用いられている機密性の高いアプリケーションは通信の秘密が保障されない体制のもとで開発されていることなどを踏まえれば、特に重視したい項目だと考える。

○　事務局の提示した「サイバー対処能力強化法に基づく基本方針の策定に向けて」は、強化法及びそれに先立つサイバー安全保障分野での対応能力の向上に向けた有識者会議の提言を適切に踏まえたものであり、異論はない。
○　その上で、以下の３点を指摘したい。
○　第１に、法の下で策定が求められている基本方針は、別途策定される新たなサイバーセキュリティ戦略と有機的な結び付きの下で策定・運用されるべきものである。
○　第２に、法の実施に当たっては、①社会全体のサイバーセキュリティの確保が究極の目的であること、②通信の秘密等の国民の重要な基本的人権を制約するものであること、③当事者協定の提供を含め事業者等の協力を得るための前提ともなること等から、法の仕組みについて国民の理解を得るとともに、その運用について可能な限り透明性を高め、政府が説明責任を履行することが求められる。
○　第３に、サイバー通信情報監理委員会が設置された後のことではあるが、同委員会による検査に関係機関が協力すべきことは当然として、同委員会による適法な職権行使に従うことについて職員等の意識を高めるべきである。

○　そもそも、「基本的な事項」として何を定めるべきかという、大きな整理が必要になるのではないか。
○　７つの「基本的な事項」の内容は、これから精査・整理されるのかもしれないが、区々な印象。それぞれの「基本事項」の内容が区々に、ばらばらにならないように、「そもそも、基本的な事項として何を定めるのか」、「定めるべき内容（基本事項）を記述する際の、ある程度の整理のルール（項目の順序や整理）」、を考えておいた方がよいのではないか。
○　また、本日の資料のなかに「基本事項」として挙げられている内容には、「配慮すべき事項」という項目があるが、この部分については、「誰が」配慮すべき事柄になる

のかの宛先が明示されているとよいのではないか。

○ 地政学リスクやサイバー攻撃の激化を踏まえ、「サイバー対処能力強化法」の具体化・早期実現は日本国にとって喫緊の課題である。
○ 能動的サイバー防御を実現し、欧米主要国と同等以上のサイバー対処能力を具備するためには、産官学が連携して取り組むことが必要であり、その第一歩として重要電子計算機の被害防止等に関わる基本的な事項について、本有識者会議にて議論し、方向性を定めていくことは極めて重要である。
○ 基幹インフラ事業者は激化するサイバー攻撃に対抗すべく有限の予算の中で日々尽力しており、サイバーセキュリティ対策に従事する社員の負担も増しているのが現状である。これを踏まえると、官民連携の促進に向けて、事業者からも情報提供などの協力は必須である中、基幹インフラ事業者への過度な負担とならないような配慮もお願いしたい。
○ また、政府には、得られた知見を活用し、日本国の対応力強化につなげるとともに、得られた知見を基幹インフラ事業者に還元することを期待する。これにより、官民連携の必要性への理解が増し、更なる協力が進むと考える。
○ そのためにも、検討の具体化にあたっては、産業界の声、特に現場の声を丁寧に汲み取って頂き、双方向のコミュニケーションを深めて頂くようお願いしたいと考える。

（6）次回会合について

意見交換の後、事務局より次回会合でのヒアリング実施を調整しており、日程は別途連絡する旨発言があった。

以上