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
官民連携に関するテーマ別会合（第３回）
議事要旨

1. 日時
令和６年９月２日（月）12 時 30 分から 13 時 45 分までの間

2. 場所
オンライン開催

3. 出席者
（有識者）

上沼　紫野	LM 虎ノ門南法律事務所弁護士
遠藤　信博	日本電気株式会社特別顧問
佐々江　賢一郎	公益財団法人 日本国際問題研究所理事長
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
辻　伸弘	SB テクノロジー株式会社プリンシパルセキュリティリサーチャー
野口　貴公美	一橋大学副学長、法学研究科教授
丸谷　浩史	株式会社日本経済新聞社常務執行役員 大阪本社代表
村井　純	慶應義塾大学教授
山岡　裕明	八雲法律事務所弁護士
山口　寿一	株式会社読売新聞グループ本社代表取締役社長

（ゲストスピーカー）

谷合　通宏	金融 ISAC 理事長
内田　忠	電力 ISAC 代表理事

4. 議事概要
（１）ISAC からのプレゼンテーション
それぞれの取組等について、金融 ISAC より【資料２】を用いて説明、その後、電力 ISAC より【資料３】を用いて説明があった。

（２）討議
金融 ISAC と電力 ISAC のプレゼンテーションを踏まえ、以下のような発言があった。

〇　ご説明に感謝申し上げる。電力セプターと電力 ISAC の関係性について伺いたい。また、セプターの位置づけ・必要性について確認したい。

電力 ISAC より回答

○　電力セプターは、重要インフラ行動計画に基づき置かれている。電力セプターには、一般送配電会社等が含まれており、電力 ISAC には新電力のほか、テクニカル会員としてセキュリティベンダなども参加している。電力 ISAC では会員等含めて、努めて情報共有を行っているところ。

○　セプターは行動計画に基づいて、電力だけではなく、他の業界でも設置されており、全体として検討されるべきものと考えている。

事務局より回答

○　セプターは行動計画に基づいて、分野ごとに存在しているが、例えば電力セプターの場合には、電力 ISAC が事務局となって活動を進めてもらっている。NISC から行動計画に基づいて各セプターに情報提供しているほか、セプターカウンシルなどのセプター横断的な場が定期的に開催されており情報共有が行われている。

〇　セプターは NISC のイニシアチブで作られた、それぞれのセグメントのセキュリティに対するグループであり、ISAC は業界自律的な独立した組織として設立されたグループであるが、NISC との関係の中で ISAC がセプターの事務局の役割を担っている業界も存在するということか。

事務局より回答

○　一言で言うとその通り。セプターは行動計画に基づく全ての重要インフラ分野に存在している。一方、ISAC は業界ごとに自主的に作られるものであり、全ての分野に存在しているわけではない。ISAC は自主的にやろうという分野において、業界のイニシアチブの下に作られている。

〇　金融 ISAC のプレゼンでは、クリアランスは今のところ必要がないということだが、そもそも情報共有に関する資格が不要ということか、代替手段が機能しているということか。

金融 ISAC より回答

○　我々の取り扱っている情報は、セキュリティ・クリアランスを前提とするほどのものではない。我々も TLP というレーティングに基づき情報交換しているが、守らなくても別に罰則があるわけではなく、いわば紳士協定のようなものである。

○　セキュリティ・クリアランスは、法律の裏付けがあるものでニュアンスが異なる。現在、金融 ISAC が扱っている情報、例えば、A 銀行から不正送金が行われたといった情報が漏れたとしても、致命的なことが起きるわけではない。

○　セキュリティ・クリアランス制度は、本当に限られた中で情報を咀嚼して、それを展開して、対応していく中で秘密を守って考えていかなければならないようなもの

を想定していると考える。今のところそこは我々の範疇とは違うと考えている。

○　電力 ISAC が考える人材育成について、資料３の p.7 に「ＯＴも含め民間サイドが効果的に育成できるような育成機関やコースの継続・新設をお願いしたい」と書かれているが、このように考えられた背景やイメージについてお伺いしたい。

電力 ISAC より回答

○　IPA の産業サイバーセキュリティセンターにおいて、制御系システムのセキュリティについて、我々事業者が 1 年間教育を受けることができるプログラムが提供されている。実際に、過去数期にわたって、電力会社や他の事業者からもプログラム修了者を輩出しており、本教育プログラムを受けるとセキュリティ担当者として一人前に育つことができるという状況を踏まえ、「継続」という言葉を使用した。また、「新設」について現時点で具体的なイメージを持っているわけではないが、例えば、脅威インテリジェンスや新たな脅威等に焦点を当てたものを作る必要があるのではないかという意味を込め、「新設」と書かせていただいた。OT システムを含めた人材育成について、政府側にも力を入れていただけると助かるという意味も含め、コメントした次第。

○　電力 ISAC のご説明にあった育成コースの継続・新設の件については、例えば、イスラエルには OT 専門のセキュリティインシデントに関するトレーニングコースを持っている会社もあると承知しており、こういったものが想定され得るのではないか。

（３）事務局説明

事務局より、資料４及び資料５に基づき、「官民連携」及び「横断的課題」に関する提言素案について説明があった。

（４）討議

○　分かりやすく、多角的な観点から意見をとりまとめていただき感謝。

○　今回の議論は能動的サイバー防御が主目的であるが、重要なのは人口減少も踏まえて、日本のレジリエンス力をどのように強化するかということ。より効果的で、実効可能なサイバー防御について議論できて良かった。

○　この提言案には、能動的サイバー防御の法整備を待たずに実行可能なものもあることから、できるところから始める必要がある。サイバーセキュリティ戦略本部の活用も含めて、政府で主導的にまとめ、実行していただきたい。

○　ソフトウェア等の脆弱性対応について意見を申し上げる。資料４の 76-79 行目にかけて、国内で悪用されている脆弱性情報について触れられているが、これは非常に重要な領域である。企業のセキュリティ関係者はこういった情報を是非とも入手したいと考えているが、現在、日本に関するこの手の情報は入手が困難であり、政府

が入手した情報を提供いただけることは非常に重要。

○ また、これに関連して、資料5の62-65行目にかけて、政府機関自体のセキュリティ強化について記載がある。米国のCISAが公表しているKEVカタログのようなものを、日本の政府機関も脆弱性対策の実施機関を含めて定義し、方向性を示していただくとこが重要である。

○ 資料4の88-89行目にSBOMについての記載がある。SBOMは非常に重要であるが、現状、各国が各々SBOMのフォーマットについてまとめ始めている。我が国企業がソフトウェアを提供する場合、相互運用可能性が重要であり、国が積極的にアレンジいただくことをご検討いただきたい。

○ 資料4の91-92行目に関連する脆弱性を減らす試みとして、ソースコードの検査ツールの利用が考えられるが、こうしたツールは一本一千万円以上するものもあり、これを導入できない人たちもいる。そういう中で、検査のための共同利用できる独自ツールを政府主導で作り、それを共有化ということも考えられると思うので、ご検討いただきたい。

○ 様々な事前のコメントを反映いただき、重要なポイントが明らかになっている提言案となっており良い。

○ インフラは、サービスが持続的に続くということ自体が国民やライフラインを守ることであり、その点が記述されていることが重要。

○ 例えば、資料5の27行目以降において、「インフラの補完・代替・復旧等」を前提に、「重要性の優先順位とともに、新しい分類やデジタル空間の構造を踏まえた検討が必要」である旨記載いただいている。これは重要な視点。

○ 現時点で答えはないが、ここで技術、また技術の構造について捉えられているという点も重要であるが、日常の動きで見ると運用も大事。運用・オペレーションに関わっている人達、それはインフラのオペレーションに関わっている人もそうであるし、サイバーセキュリティのオペレーションに関わっている人もそうであるが、毎日ダイナミックに動いているものを見て、運用している。そこにも、運用の技術や運用のための相互運用可能性が存在。インテリジェンス能力を高め、技術・法律・外交の多様な専門家を官民から結集するということであるが、民間で運用を担っている人に関わってもらいたい。運用に携わっている現場の人の知恵も結集すべきであり、「運用」、「運用技術」、「相互運用性」という言葉の重要性の記述をどこかで入れられないか。オペレーションが持続することでサービスが継続する、そのための人の協力体制も作っていく旨の記載があると良いのではないか。

○ 資料4の88行目以降、「このほか、海外事例等も参考に」の箇所について。最近、セキュリティ製品は導入しているものの、デフォルトでオフなものが多く、これによりインシデントの被害が拡大するというものを沢山見てきている。例えば、シェアが大きいとあるVPN製品について、多要素認証が初期設定でオフなものがある。同様にシェアが大きいとあるEDR製品についても、自動端末隔離が初期設定でオフであり、アラートが鳴るだけで当該端末を隔離してくれないものがある。

○ 導入企業の担当者として当然セキュリティに関する初期設定はオンであると思い、

またオンであれば防げた可能性のあるインシデントが一定数ある。初期設定がオフであることを導入企業の担当者が知らないことが多い。もちろん、ベンダの立場からすると、セキュリティとユーザビリティは相反することが多いので、一概にセキュリティのみを考えるのではなく、ユーザビリティを配慮しての初期設定であると推察するが、EU のサイバーレジリエンス法案のように、オペレーションの負担を前提としつつも、セキュリティ重視に傾倒しつつある法制度というのは参考になるかと思う。そこで、資料 4 の 91 行目「セキュアな製品開発・供給」に加えて「セキュアな設定・運用」という視点も加えてはどうか。

○ 書きぶりについて、細かい点だが一点申し上げたい。先ほどの電力 ISAC の説明からも分かるように、ゼロデイ脆弱性対策が非常に重要。こうした観点から、資料 4 の 72-74 行目までに、ソフトウェアベンダの責務や脆弱性情報の提供等を規定すべきといった旨の記載があるが、これでは規定の手法が必ずしも明確に伝わらない。法的な責務を前提として規定するということと理解しており、その旨記載した方が良いのではないか。
○ 先ほど検査ツールの利用に関して政府からの支援等が必要ではないかという話もあったが、そこまで視野に入れることとのバランスを考えても、そのようにした方が良いではないかと考える。

○ ご説明いただいた内容は、よくまとまっており、良いと思う。
○ これらは、全体として方針が書かれており、今後の方法や運用方式は触れておらずこれからということだと思う。実際にこれらを実施していく上で、どういう方法でやるのか、例えば窓口を一つにして ISAC から吸い上げることができるのか、あるいは監督官庁に上がってきた情報を吸い上げ、必要な情報に加工して展開していくといったような方法の話は、今後、どのような場で検討を進めるのか。

事務局より回答

○ 今後の詳細制度設計の進め方は、政府の中での検討を踏まえながら、今のサイバーセキュリティ戦略本部等の仕組みがある中で、場のあり方についても検討し、ご相談しながら進めていきたい。

○ 中小企業等のセキュリティ対策については、政府によるツールの提供などを含めた支援拡充の検討等を実施するとともに、関係する中堅・中小企業に対し、官民の協議体への参加を呼びかけるべき。幅広い企業が参加しないと協議体の実効性が上がらないことに加え、中堅・中小企業においては、セキュリティ対策は他人事であるという意識もまだまだ強いと思われるため、「促す」・「呼びかける」といった観点も提言素案に含めていただければと思う。

○ 計 6 点申し上げる。第 1 に、資料 4 の①について。官民連携の必要性についてはその通りだと思うが、これまでの議論を聞く限り、官民連携の対象となる「民」の粒度が粗すぎる印象。この後、重要インフラ事業者であったり、サイバーセキュリティ人材であったりの具体的な記載があるが、運用に携わる人など、対象となる民と

は具体的にどのような業種業態を指すのかをイメージし、民の輪郭がはっきりするような書き方としていただきたい。

○ 第2に、資料4の28-29行目について、「産業界をサイバー安全保障の「顧客（カスタマー)」と位置付けることが重要である」 という記載は良いと思う。一方で、以前もＫＰＩの設定について申し上げたが、資料に書き込めるかどうかは別として、カスタマーの満足度を高めていくためにも、カスタマーに役に立つ情報共有ができているかについて、政府自身の取組を把握し、見直していく仕組みについて考えていただきたい。

○ 第3に、資料4の53-55行目について、「セキュリティ・クリアランス制度の活用や、情報共有ポリシーの設定により、適切な情報管理と情報共有を両立する仕組みを構築すべき」との記載について、先ほどのヒアリングを踏まえ、セキュリティ・クリアランス制度の対象範囲や情報共有ポリシー設定等との役割分担等について、もう一歩整理があると良いと思う。引き続き検討いただきたい。

○ 資料5の19-23行目について。以前も申し上げたが、官民の議論をする際に地方公共団体に関する議論が抜けがちだがどう位置付けるのか。サイバーセキュリティに関する全体的な方針について、地方公共団体も今までの国・地方公共団体との関係の中でやっていくのか、それともももっと強いコントロールをかけて国に協力してもらうのか整理すべき。

○ 資料5の39-41行目について、「普段から求められるサイバーセキュリティ対策の質の保証の観点から、基準、ガイドラインという手法により、行政が達すべきと考える水準を分かりやすく示し、誘導していくことが必要」というのはその通り。法律による規律において細かく書くことには限界があり、基準・ガイドライン等で適時適切に、しかるべき方々に議論に入ってもらって見直すべき。しかしながら、同時に重要インフラ事業者にとっては、一定の負担が発生する。基準・ガイドラインで重要インフラ事業者の行動を規律していくということは、ひいては国民生活にも大きな影響を及ぼす。そこで、基準・ガイドライン等についても、例えば第三者機関で、その評価・検証を実施することで、安全な仕組みになるのではないか。

○ 資料5の86行目以降の記載について、サイバーセキュリティ人材について、具体的な育成・確保のための方策としていきなり企業・組織の話に入っているが、まずは国・地方公共団体等において、具体的にどのようにしていくのか示すべきではないか。場合によって、公務員制度を必要な範囲で見直していくことが必要。官についても一歩踏み込んで書かないと、企業・組織に対する説得力が生まれないのではないか。

○ ソースコードの検査ツールについて、共同利用ができる独自ツールの開発について同感である。昨今、AIがコードを書いて、過去のゼロデイ攻撃のパターンを把握しながら、AIが検査し脆弱性がない状態に近くして出荷することが行われている。

○ このようなことを人力でやっていくのは限界がある状況を踏まえて、国内製品の開発を進めていく必要がある。

○ 資料5の64-65行目に「対応の実効性を確保する仕組みを設けることが重要である」との記載があり、これは重要である。これまでも政府から提言はでているが、

実際はそう動いていないことも今まであったと思う。自分の解釈であるが、責任を明確化して、その後どうなったか等の結果のレビューと課題解決をしていき、次の政策、行動になっていくと考えている。

○ 人材育成の部分では、政府が中心となってまとめて見ていただきたい。各省庁でバラバラにやっていること、業界でやっていることを全体で俯瞰して、どう支援するかという観点で見ていただきたい。

（5）その他

○ 本日も非常に良い意見・各論が提示され、具体的な問題について話があった。事務局には、本日の意見について取り入れられるところは取り入れて、更にブラッシュアップした提言としてもらいたい。

以上