産業サイバーセキュリティ研究会WG１・重要インフラ専門調査会
合同ワーキンググループ　サイバーインフラ事業者に求められる役割等の検討会　第３回会合
議事要旨

１．日時・場所

日時：令和７年２月 18 日（火）15:00～17:00

場所：オンライン開催

２．出席者

委員：　土居委員（座長）、阿部委員、稲垣委員、鴨田委員、木谷委員、立石委員、津田委員、板東委員、日高委員、古田委員、山口委員

オブザーバ：　総務省、厚生労働省、防衛装備庁、一般社団法人 日本医療機器産業連合会

事務局：　経済産業省 商務情報政策局、内閣官房 内閣サイバーセキュリティセンター

３．配付資料

資料１　議事次第・配布資料一覧

資料２　委員名簿

資料３　サイバーインフラ事業者に求められる役割等の検討の方向性

資料４　サイバーセキュリティ基本法改正案に係る関連事項

参考資料１ サイバーインフラ事業者に求められる役割等に関するガイドライン案（委員限り）

参考資料２ サイバーインフラ事業者に求められる役割等に関するガイドライン案補足資料（委員限り）

４．議事内容

事務局から、資料 3、4 に基づき説明の後、自由討議を行われたところ、概要は以下の通り。

＜ガイドライン案（更新版）について＞

・　自己適合宣言の範囲が、会社単位か分野単位か明確にした方がよい。例えば、システム子会社のみでよいのか、それとも親会社を含めた全社で取得しなければならないのかにより負担が大きく変わる。また、制度を検討するに当たり、本ガイドラインにおいても各要求事項間の記載内容の深さ、細かさのレベルを合わせることが必要ではないか。

・　重要インフラ事業者の CISO など関係者と議論してみたが、明確なセキュリティの評価基準としてどこまで取り組めばよいかという対応レベルが定義されているとよい、SOC2 や ISMAP といった既存の制度のように認定が仕組み化されるとサイバーインフラ事業者を選ぶ基準となり契約等で選定し易くなる、ガイドラインにポジティブに対応できるような施策や税制優遇などのメリットが享受できる仕組みがあるとよいという話があった。

・　本ガイドラインの適用範囲として、その委託先、再委託先、再々委託先含めて、どこまでその基準を求めるべきか明確する必要があるのではないか。

・　要求事項としての PSIRT（Product Security Incident Response Team）の設置とあるが、小規模な委

託先ではそうした組織まで作ることが難しいケースもあり、PSIRT 活動に必要な「機能」を求めるという形にしてはどうか。

- 海外の類似基準とのクロスウォーク（相互確認）がなされるとよい。欧米の国だけでなく、インド、シンガポール、マレーシアなどアジアの国々も考えられる。
- 本ガイドラインで対象とするサイバーセキュリティリスクの定義を明確にしておく必要があるのではないか。サイバーセキュリティ基本法第２条の定義が脅威をサイバー攻撃に限定していないのと比べて、ガイドラインでは脅威をサイバー攻撃に限定しているように読める。
- 自己適合宣言制度の検討に際して、パイロットプロジェクトを実施することが重要であり、検証項目を明確にするとよい。一度ガイドラインを作って終わりでなく、定期的にガイドラインの見直しが必要かどうかを検討することを制度として盛り込んではどうか。
- セキュアバイデザインという概念は重要である。本ガイドラインの中でより明確に取り上げてはどうか。例えば「開発」とともに「設計」の言葉を明示することが考えられる。
- ガイドラインの中には事業者と顧客間で合意が必要な場面が幾つかある。例えばパッチを当てるのにシステムを止める必要があるなどの状況では、事業者側の十分な説明と顧客側の判断があり、そうした状況での具体的な合意方法のノウハウが、ガイドラインの活用の中で指摘され、共有される必要がある。また、EOL もある中でのサポートについては、事業者側と顧客側とで常に状況確認しながら合意していくことが必要。
- ガイドラインでは責務の順に並んでいるが、契約締結前やその後など、事業者と顧客がお互いに、各リスクを重要視する／しない、システムで対処する等を決めるべき幾つかのタイミングがあるので、そのときどきに必要な材料となる要求事項等の関連表があるとよい。
- 契約のフローとして、あるポイントでリスク分析を実施し、その結果に基づいた仕様書の策定プロセスを現時点で整理することは難しい。周辺の必要な概念の範囲が決まるのを待ちながら、だんだんに詰めていくことが必要である。

＜普及施策、今後の事業などについて＞

- レジリエンス強化とサプライチェーン全体のセキュリティレベル強化というガイドラインの目的がどの程度達成されているのか有効性を意識した普及策や有効性の検証評価を進めてほしい。
- 本ガイドラインの実施に必要な契約プロセス、そのプロセスの中で考えるべきことは何かということを充実させることが、このガイドラインが利用される前提となるだろう。一つのプロジェクトを新たに立ち上げ、取組を実施してほしい。
- ガイドラインを使用してうまくいった事例や我が国では出てきづらい失敗事例を集めて、ノウハウを蓄積し共有できるとよい。
- ベンダー側でどこまで取り組めばよいか聞きたいというニーズがあるようである。普及策として、パイロットプロジェクトの実施結果、これをやれば OK という線を引いて、これを各種イベントや講演で紹介する等が考えられる。

- 普及啓発事業は地方で行ってほしい。できればできるだけ小さな街で、場合によっては離島など中山間地域でも工夫次第で人は集まると思われる。
- 中小事業者向けに金銭的なものを含めた支援策が重要である。中小事業者を含めて自己適合宣言し、プライムベンダーが宣言した事業者から委託先を選定することで、自己適合宣言がメリットとなるような形態が考えられる。
- 自己適合宣言があることで、事業者と顧客が共に判断した結果であるということの証拠とし、場合によっては、サイバー攻撃を受けた場合の損害の補填等で両者の比率を策定する仕組みがあれば、事業者も進んで自己適合宣言をしたいと思うのではないか。
- ガイドラインはリスクについて参考情報を提供するもので直接義務を課すものでないから、ここまで取り組めばよいということは言えず、社会の皆が自らリスクを下げていこうよという取組である。それゆえに、自己適合宣言の制度設計に当たっては、セキュリティレベルがどのように向上したのか、費用支出、社会的支出が適正なのか、誰が負担していくのか、そういったことを併せて議論しなければ、単にセキュリティ情報の提供で終わってしまうのではないか。
- ベンダーが費用をかけるには、ユーザーからの具体的なニーズがあり、ユーザーがお金を出さなければならない。ユーザーに対する強力な教育が考えられるとよい。
- 別事業のガイドラインに係る認知度や活用度のインタビューでは、顧客からの要求があれば事業者は対応するという意見が多かった。
- ガイドラインを知っている人は研修・セミナーなどを通じて知ったという人が多い。知らない人に対しては SNS（Social Networking Service）などに情報を流すことも一つの普及策と考えられる。
- SNS などの電子媒体が普及しているが、紙媒体の効用も大きいので、簡単でよくわかる冊子を作ることも考えてほしい。
- 普及策の働きかけ先は、セキュリティ担当者やシステム部門等の専門家だけではなく、調達部門を考えるとよいだろう。セキュリティ調達というプロジェクトを作り、この利用について広めていくとよいのではないか。また、セキュリティプロジェクトマネジメントという言葉を作り、企業の実務の中で、プロジェクトマネジメントのときに PMO（Project Management Office）が必ず考えるべきこととして紹介してはどうか。

以上