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１回会合
議事要旨

１．日時・場所

日時：令和６年９月 24 日（火）10:00～12:00

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、淵上委員、古田委員、山口委員

オブザーバ：　警察庁、総務省、デジタル庁

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　本検討会の議事運営について

資料４　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

参考資料　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素案（委員限り）

４．議事内容

冒頭、事務局より、本検討会の趣旨についての説明があった後、経済産業省 商務情報政策局 見次室長及び内閣官房 内閣サイバーセキュリティセンター 山田企画官より挨拶があった。次に、事務局から、資料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。

＜責務と要求事項について＞

・ サイバーインフラ事業者は提供者であったり顧客であったりする。顧客がエンドユーザーを表しているのか、サイバーインフラの基盤を提供している人を表しているのか、明らかにした方がよい。読者がどちらの視点で見ればよいのかを分かりやすくしてほしい。

・ （ソフトウェアの）ライフサイクルの段階に応じて事業者と顧客による責務に濃淡があることが考慮されるとよい。

・ 顧客にも責任が伴うところ、自社内製の場合など顧客が同時にサイバーインフラ事業者であるケースもあり、ガイドラインの対象範囲が明確になるとよい。

・ 契約形態を踏まえて、どのようなステークホルダーがどのような責任を負うのか明確になるとよい。

・ ソフトウェアの対象になっている領域を、想定する事業者を意識した粒度感で整理すると、ステークホルダーにどのような責務を求めるべきなのかということがもう少し整理できるのではないか。

・ 特に運用段階でインシデントが発生することが多いことから、運用のライフサイクルと要求事項をよ

り明確に含めるとよい。
  - ガイドラインを満たそうとすると、これまで以上にコストがかかるはずである。経営者によるコスト配分の考え方を入れるとよい。
  - 本ガイドラインの位置付けが明確であるとよい。事業者が本ガイドラインを使う根拠を示すことが大事である。今回、サイバーセキュリティ基本法７条の事業者について議論している点が明確になった。その上で、ガイドラインが事業者の責務に関する解釈を示したものなのか、７条による政策を進める上での参考情報を提供するものであるのか、はっきりさせるとよい。
- サイバーセキュリティ基本法７条の位置づけを明確化する方が、レベルの差が大きい事業分野では業界全体として非常に良くなるのではないか。何らかの強制力、若しくは、裁判になったときにどこまでやっていたのか、といったあたりをなるべく明らかにできるように、そのような位置づけで検討されると非常に有り難い。責務と責任という２つの用語があるが、注意書き等でしっかりと言葉の定義を入れてもらいたい。
- 本ガイドラインが裁判で利用される可能性もある中、「法的な責任を意図するものでない」との表記が、行政権の発動とか行政指導の根拠となるべきでないということであれば、その点は具体的にきちんと書いた方がよい。
  - サイバーセキュリティを経営の中に組み込むという発想があるところ、経営者がきちんと考えるべきという項目を独立して一つ作ってはどうか。本ガイドラインを参照することとなる、事業者や経営者の視点があるとよい。
  - 「重要インフラのサイバーセキュリティに係る行動計画」と平仄（ひょうそく）を合わせるとよい。
  - 要求事項を実施すべき背景として、脅威シナリオやリスクと紐（ひも）づけられると理解しやすい。
- ガイドラインの普及・適用のための指針（考え方、求めること等）があるとよい。
  - ガイドラインを適用する際の、より具体的な対象システムの考え方、システム例のようなものがあるとよい。
  - クラウドサービスの場合には、事業者が圧倒的に情報を保持しており、顧客と情報の非対称性が発生している。サイバーインフラ事業者側の責務に顧客への十分な情報提供という責務が含まれるとよい。
  - 顧客側と事業者側の、特にコスト割合をどのように考えるのか整理するとよい。
  - 継続的なサービス提供を責務として検討する必要があるのではないか。

＜検討の進め方について＞

- CISA（Cybersecurity and Infrastructure Security Agency）から Secure by Demand という文書が発行されている。内容はユーザー側だけに影響があるものではなく、難しい取組も記載されており、すぐには実現できないことも多いが、方向性を見ていくという意味で、参考レベルとして参照してはどうか。
- 海外事業者を、本ガイドラインにおいてどのように取り扱うのかを整理する必要がある。
- 各国で各種ガイドラインが実際に使われた場面や、その効果について文献調査できるとよい。
- どのような事業者・事業者団体がどのような用途でガイドライン類を使用しているのか、それらの事業

者・事業者団体から意見を聞くとよい。
・ 経済安全保障推進法のリスク管理措置でもソフトウェアの脆弱性管理などガイドライン案と同じような要件が書かれている。記載内容を確認し平仄（ひょうそく）を合わせた方が良い。
・ 先行して特定重要設備を供給している企業があるので、そのような民間企業に成功事例や失敗事例のようなものをヒアリングする機会を設けてはどうか。

＜その他今後の事業などについて＞
・ 事業者と顧客の要求というのは表裏一体になっており、共に努力してレベルを上げるような観点が多分にある。事業者向けが主体であるとは言いながら、顧客がやるべきところにもう一歩踏み込む方が次の工程に進みやすいのではないか。次のステップで、具体的なイメージを持てるようにある程度の粒度での記載が必要ではないか。
・ ソフトウェア開発の個別案件の単位で実現できる話と、そもそも考え方を改めて体制やコスト、あるいは従来のビジネスモデルも見直しが求められるケースもあるという観点も含めて、時間をかけて啓発していく必要がある。
・ ガイドラインの適用を 1 回で終わらせず、継続的に適用できるような仕組みがあるとよい。短期的には、サイクルで誰がどのような評価と確認をするのか、中期的には、顧客とインフラ事業者側が双方でガイドラインをチェックできるような仕組みがあるとよい。
・ 実行力のあるガイドラインにするには、サイバーインフラ事業者のインセンティブ、メリットも必要である。責務だけでなく、取組による免責等も考えるとよいのではないか。
・ （本ガイドラインの内容について）広報をどのように進めるのか、特に地方の零細企業にどのようにリーチするのか非常に難しい。
・ 中小のソフトウェア事業者は、（サイバーセキュリティに）コストがかけられず、施主もお金がかからないからと思っているので、政府としてもう少し責務を強く求める必要があるのではないか。
・ 今後の事業としては、Web サイトの制作の領域にも取り組む必要があるだろう。
・ 自己適合宣言を議論・設計する場合、どのような限度で責任を負うのかを明確に示すことが、使いやすさにつながると思う。
・ 米国 CIS Benchmarks、国防総省の STIG（Security Technical Implementation Guide）のように具体的な実装まで言及しているものがある。自己適合宣言の場合にも、具体的に、例えば CIS Benchmarks のどのバージョンを使って、セキュリティの実装をしたといったものがないと、対応内容がまちまちになってしまうのではないか。

以上