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２回会合
議事要旨

１．日時・場所

日時：令和 6 年 12 月 17 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：　総務省、厚生労働省、デジタル庁、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

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＞

- サイバーインフラ事業者側には投資が必要との記述があり、顧客側には運用負荷低減が期待できるとの記述があるが、一見すると顧客側には投資が必要ないと取られかねない。サイバーインフラ事業者が顧客に説明し理解いただいた上で、顧客側にもコストを負担いただくための努力が必要という意味合いを記載するのがよい。
- コスト面等の理由にて顧客に理解いただけず、特定のセキュリティ施策を実装できない場合についても、ガイドラインに示されたミニマム要求水準をクリアすること、あるいは、する必要があるということを加筆してはどうか。
- サイバーインフラ事業者と顧客の双方が、コストについて考える必要があると明記するべきではないか。
- 事業者と顧客の位置づけの整理について、クラウドサービスを連携しているサービスサプライチェーンについても本ガイドラインの対象となることを明確にするのがよい。
- 本ガイドラインを活用することで実現するエコシステム（分野における協調連携関係）として、サイバーインフラ事業者と顧客が脆弱性情報などをいち早く連携し、サイバー攻撃への対応力を強化すると

いう価値共創につながるというイメージがあるとよい。

- サイバーインフラ事業者が採択するパッケージについて、ミニマム要求パッケージを選ぶか標準要求パッケージを選ぶかの判断材料（個人情報がどの程度あるかなどリスクに応じた例）があるとよい。
- 要求事項は、組織の外部から調達する前提でソフトウェアを構築することを前提としているように見える。ソフトウェアの産業振興の観点から、同じ機能のソフトウェアをセキュアな国産ソフトウェアとして開発にチャレンジする前提も想定するべきではないか。
- サイバーインフラ事業者と顧客の役割分担をわかりやすくするために、役割を詳細に整理してはどうか。
- サイバーインフラ事業者が顧客に提供するサービスについても、サイバーセキュリティの確保に努める対象に入ると基本法を解釈した上で、本ガイドラインが基本法や NISC の基本方針に対するより詳細な解釈を示すものであるのか、単に参考として資料を提供するものなのか、位置づけを明確にするとよい。その点で「推進」「望ましい等」言葉の統一も必要。
- 自治体などの顧客側とサイバーインフラ事業者側で知識・情報に相当程度差がある中で、顧客も責任を負うという点については慎重に言葉を選ぶ必要がある。
- ソフトウェアの供給者は開発に関与する組織に見えるが、実際には運用側に近い組織でもあることを表現できるとよい。また、SI 事業者がシステムを構築する際の設定にもリスクが存在する可能性がある。システム構築担当者も対象であることを明確化してはどうか。
- システム設計時のリスク評価と対策に関わる要求事項の役割がソフトウェア開発者となっている。ソフトウェア開発者だけでなく、システム構築に携わる者全部とならないとセキュリティリスクは軽減できないだろう。

＜普及施策、今後の事業などについて＞

- このガイドラインの読者にとっての一覧性があるとよい。どこから読み進めていくべきかを判別しやすくなる。例えば、そのような一覧があれば、GDPR（General Data Protection Regulation）への取組を進めた組織であれば、追加のセキュリティ対策を実施せずとも本ガイドラインへの対応は可能と考えられ、このガイドラインと自社ガイドラインとの差異の調査を効率的に行える。
- 自己適合宣言を運用する際、具体的な成熟指標・項目を示した上での自己適合宣言にならないと、達成水準の判断ができずに制度の運用が先細りにならないかと危惧する。
- 制度普及の時間軸を考えて、本ガイドラインをいつの段階までにどのように整備するのか、使われ方の評価など（ユーザ側に要件反映のため幾ら払うと見積もられるのか等も含めて）の計画を立てるべきではないか。
- 運用を重視しパッチ適用をしないなど顧客判断によりベンダが説明したにもかかわらず採択されなかったセキュリティ対策を、サイバーインフラ事業者と顧客の間で、記録しておくことが必要ではないか。
- 政府等調達時の加点要素や、経済安全保障のリスク管理措置に対する証明文書等に活用できるといったプラス要素としての使い方があれば、普及に貢献するだろう。また、本ガイドラインで脆弱性情報の

公表が多くなるであろうから、こうした情報を普及する機関・団体のリソース増強も必要ではないか。

- クラウドサービスでは、「契約」ではなく、「利用規約」や「SLA（サービスレベルアグリーメント）」という表記が一般的であるため、ガイドライン中の表現は工夫してほしい。
- 制度の普及に当たって作成する附属書は大切な位置づけにある。重要さを伝えるために名称を「附属書」ではなく「ガイドブック」としてはどうか。
- すでに生成 AI を使ったシステム開発、システム運用が当たり前になる時代にあり、その分野を先取したガイドラインとしてはどうか。
- 制度の普及に当たっては、政府の支援が必要。特に中小企業では、SBOM の導入などでツールの負担も大きいと聞くし、政府がツールを無償提供している国（欧州の例）もあると聞いている。
- 調達など活用のシナリオがないと普及せず、政府機関や重要インフラ等で需要が生まれるよう政府のバックアップが必要。
- ミニマム要求パッケージと標準要求パッケージの分類について、顧客要望や対象システムとしてどこまで必要とするかケースバイケースである。ある会社の場合には、ISMS は（全社ではなく）必要なビジネス部門ごとに認証を取得している。今回のガイドラインは内容がより広い。自己適合宣言をどの組織単位で適用するかや、様々なシステム対象に対して実証が必要ではないか。
- 制度の普及前に、自己適合宣言前後の費用感やレベル感が組織によりどの程度差が現れるのか把握した上で、適用範囲などの見定めが必要である。また、一つのソフトウェアでソースをどこまで見るのか（全てかサンプルか）、真面目に取り組む会社が損をすることにならないようにしてほしい。
- 顧客側の責務の一部として、構築に携わる SI 事業者にも脆弱性や攻撃情報を共有する項目があってもよいのではないか。

＜その他今後の事業などについて＞

- 業界別 ISAC（特定の業界に特化した情報共有と分析を行う組織）といった仕組みだけでなく、業界横断的にソフトウェアの構成情報や脆弱性情報をシステム化して連携する仕組みが将来的にあるとよい。期間も費用もがかり、壮大であり、利権も絡むことから、政府主導でプラットフォームが作られることが望ましい。

以上