産業サイバーセキュリティ研究会WG１・内閣官房国家サイバー統括室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４回　議事要旨

１．日時・場所

日時：令和８年２月５日（木）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（※1）、木谷委員、立石委員（※2）、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、厚生労働省、防衛装備庁、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　橋本企画官、大久保課長補佐、関戸係長
内閣官房国家サイバー統括室　小澤企画官、油川参事官補佐、竹内上席サイバーセキュリティ分析官

※1　和田氏が代理出席

※2　日向氏が同席

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　事務局説明資料

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（非公開）

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（非公開）

参考資料３　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へのパブリックコメントについて（非公開）

参考資料４　Web 会議注意事項（非公開）

４．議事内容

事務局から、資料４に基づき説明の後、自由討議が行われたところ、概要は以下のとおり。

＜ガイドラインについて＞

・パブリックコメントへの対応方針において、「サードパーティ製ソフトウェアコンポーネントに自組織の要件を課すことは困難」との意見に対し「原案のとおり」では回答として不十分である。本質的リスクであるトレーサビリティ確保の観点から回答を記載すべきである。

・SBOM（ソフトウェア部品表）への懸念は、脆弱性管理や資産管理など、人により想起するイメージが

異なることに起因するとも考えられる。本質はトレーサビリティ確保であり、SBOM はその手段の一つという位置づけを明確にすべきである。

・SBOM は、使用が敬遠されることを避けるため、「必須ではないが、推奨する」という方向性で取扱うことが望ましい。

・SBOM に関連する個別要求は、トレーサビリティの観点から、OSS（オープンソースソフトウェア）等については将来的には必須化も視野に入れ、「推奨する」「標準である」という方向性にしておくべきである。

・実証事業において、ガイドラインの主要な利用者と想定される発注者（顧客側）での検証が行われていない。エンドユーザーである一般企業が適切に活用できるか検証するため、顧客側の実証事業が必要である。

・評価チェックリストの実証が大企業から中規模企業までであったため、リソースの限られる小規模企業における実施可能性についても検証が必要である。

・SIer でありミドルウェアも提供するような業態の企業において、SI 業務全体で評価するのか、個々の製品で評価するのか等、評価チェックリストの適用単位や、発注元との合意に基づく代替手段の可否について明確化が必要である。

・評価チェックリストは事業者のセキュリティ対策レベルを示す機密情報に該当するため、その取扱いには十分な注意を要する旨を明記すべきである。

・評価チェックリストは事業者の対策レベルが判別できる機密情報であり、不正競争防止法上の営業秘密に該当する可能性もあるため、暗号化等の対策とセットで取り扱う必要がある。

・IPA の「情報セキュリティ 10 大脅威 2026」で AI を悪用した攻撃が初めて上位に挙げられた動向等を踏まえ、ガイドラインの冒頭事例や AI に関する内容を今後の改定で拡充していくべきである。

・「責務」「要求事項」「〜すべき」といった表現は、損害賠償請求の根拠等に用いられ、ガイドラインが意図しない法的効果を生む懸念がある。「責任や規制を課すものではない」というスタンスを明確にするため、「要求事項」という言葉は使用せず、「〜すべき」は「〜することが有効である」等の推奨表現に修正すべきである。あるいは、定義集を設けて「本ガイドラインは裁判所の判断や企業の法的責任の根拠となることを意図していない」と明記し、用語の解釈をコントロールする方法も考えられる。

・本ガイドラインと評価チェックリストは、責務実施の可否の表明を通じて、契約相手がリスクを判断するための「リスクコミュニケーションツール」であると位置づけるべきである。一方で、行政機関が行政指導を行う際に尊重すべき要件とするという考え方は、残す余地があるのではないか。

・用語の法的効果について、意図しない法的責任を招かぬよう配慮が必要である。国際標準との整合性について、将来的には、ISO 等で用いられる「SHALL」や「MUST」といった表現と整合性を取ることが望ましい。

・海外にもソリューションを提供するため、ISO 等の国際標準で用いられる「SHALL」や「MUST」といった表現との対応関係を示すなど、国際的な整合性を検討すべきである。

・本ガイドラインの実施が、何らかの認証や認定を標榜できるものであるとの誤解を防ぐため、あくまで

契約関係における確認ツールであることをユースケース等で改めて強調すべきである。

- 金融、産業、重要インフラ分野の顧客 CIO・部長層にヒアリングしたところ、多くが本ガイドラインを認識しており、一定の注目を得ている。
- 評価項目を「実施しないとセキュリティが低下するもの」と、コミュニティ活動など「直接的ではないが推奨されるもの」に分類すれば、企業規模に応じた適用がしやすくなるのではないか。
- 活用シナリオにおいて、顧客が評価チェックリストのどの項目を記入して事業者に提示するのか、意図が明確に伝わるよう表現を修正すべきである。
- 評価チェックリストの評価項目は文書の有無を問うものが多く、内容の妥当性までは確認しないことから、実質的な合意形成には、NDA（秘密保持契約）締結下の資料確認などが必要になるのではないか。
- 企業としての取り組み評価が、個別の案件における実施を約束するものではないことを明確にすべきである。一方で、合意内容を後続の要件定義等に有効活用できる仕組みも望ましい。
- 供給者に含まれる販売店にとって、単独では実現困難な要求事項がガイドラインに記載されている。販売店がチェックリストで「N/A」と回答した場合に不利に扱われないか懸念があり、その点の解釈を明確に説明すべきである。
- 事業者は案件ごとに顧客にも供給者にもなり得るため、「供給者という組織だからこの役割」という固定的な役割分担の誤解を生まないよう、役割は案件ごとに決まることを明記すべきである。
- 評価チェックリストは、利用者の規模や業種に応じて評価方法が異なり、継続的に改善されるものである旨を記載することで、利用しやすくなるのではないか。
- 「セキュアビルド」等の各項目について、具体的に何を実施すべきか利用者が理解できるよう、NIST SP800-218 等の関連ガイドラインを詳細に提示することが、ガイドラインの普及につながる。

＜今後の普及展開に向けて＞

- 普及には、発注元の事業会社がプライム会社やグループ会社に内容を適切に説明できるかが鍵となる。分量の多い文書の読解は困難なため、動画教材のような説明しやすいツールを作成することが有効である。
- 関係者への案内は可能であるが、内容が薄まらないよう、経済産業省等の担当者が地方開催の説明会に直接赴くなど、きめ細やかな対応が求められる。
- 業界でのチェックリスト普及の経験から、説明会、解説書、Q&A、チャットボットの設置など、誤解を生まないための丁寧な説明を繰り返し行うことが不可欠である。
- 経済産業省が推進する「サプライチェーン強化に向けたセキュリティ対策評価制度（SCS 評価制度）」等の他制度と連携し、相互に普及を促進していくことが望ましい。
- 普及施策として、まず自社で本ガイドラインを活用し、サプライヤーである開発会社等にも展開したい。また、顧客の多くは社内規程にない対策は実施しない傾向があるため、顧客の社内規程に本ガイドラインの適用を推奨する等の働きかけが実効性を高める上で重要である。

・プレゼンス活動による認知度の向上が不可欠である。
・厚労省の「医療情報システムの安全管理に関するガイドライン」に基づくチェックリスト（MDS/SDS）は、「顧客である医療機関が、事業者に提出を求めること」という通達により急速に普及した成功例である。顧客側がチェックリストを要求する仕組みが普及には効果的である。
・　業界団体として、経済産業省から講師を招いたセミナーを開催するなど、普及に向けた協力が可能である。

以上