産業サイバーセキュリティ研究会 WG3
サイバーセキュリティ・サービス事業者の信頼性強化に向けた検討会 第4回
議事要旨

■ 第4回意見要旨

① 認定制度の構造・位置づけ・運用方法等に関する論点

- 制度の趣旨は「信頼性のある事業者を把握するため」であり、認定取得企業の規模感や想定される認定企業数の規模を明確にし、制度が実効性をもって活用される状態を想定すべき。
  - ✓ 経済安全保障に関連する重要な情報の取扱いについては、別途セキュリティクリアランス制度が既に存在する。制度を活用するユーザーを想定すると、認定の要件を厳しくすることで認定を受ける事業者は限定しすぎない方が良いのではないか。
  - ✓ 制度が大企業のみを対象とするような印象を与える可能性や、逆に対象が広くなりすぎて審査負担が甚大となる可能性を避けるため、想定される認定企業数の規模の明確化が必要。
- スキームオーナーにおいて最も重要な業務は、苦情受付業務であると考えられる。
- 有効期間を3年とした場合、制度更新タイミングによって、現行の情報セキュリティサービス審査登録制度と同期を取りづらくなるとの課題が想定される。有効期間途中での認定更新を許容するとともに、申請受付体制を強化するなど、事業者側の負担を踏まえた運用設計が必要ではないか。
- インシデント報告を求める対象範囲については、原則として認定を受けたサイバーセキュリティ・サービスに関する事業について発生した場合でよいと考えるが、認定されたサイバーセキュリティ・サービスに関する事業以外で発生した場合であっても、社会的に与える影響等によっては報告を求めることができるようにすべきである。

② 再委託・委託禁止の扱いに関する論点

- 認定を受けたサイバーセキュリティ・サービスに関する事業に係る業務の委託を原則禁止とする方針案について、顧客への開示・説明責任を軸に例外を整理し、顧客がリスクを判断できる仕組みを整えるべき。
- 認定を受けたサイバーセキュリティ・サービスに関する事業に係る業務を委託する可能性がある旨をあらかじめ顧客に明示することや、顧客から開示請求があった際には、NDA の締結有無にかかわらず、どの企業に、どのような事情で委託しているのかを説明できる仕組みとすることが望ましい。そうすることで、サイバーセキュリティ・サービス提供事業者が認定を受けているかどうかは、あくまで考慮要素の一つとなり、顧客への説明責任が確保された上での顧客の判断責任とできるのではないか。
- デジタル・フォレンジック調査では高度な技術を有する外部企業への照会・調査依頼が発生するため、顧客の了解を得た場合や一定事項について報告をする場合には例外として許容しても良いのではない。
- 一方で、デジタル・フォレンジック業務の全部を外部委託する事例はあまり想定されないため、必要な場合は発注者がそうした高度な技術を有する外部企業に直接委託すればよく、その旨を発注者がデジタル・フォレンジック業務を行うサービス提供者に明示すればよいのではないか。
- フリーランス活用や「出向による委託逃れ」などのケースへの対応について、整理が必要。
- 認定を受けたサイバーセキュリティ・サービスに関する事業に係る業務の委託は、認定を受けたサービス提供事業者間のみ許容されるべき。つまり、脆弱性診断・SOC・デジタル・フォレンジック等の同一分類で認定された事業者間に限定すべきと考える。（例えば、脆弱性診断の認定しか取得していない

サービス提供事業者は、脆弱性診断について他の認定サービス提供事業者から委託を受けても良いが、SOC 業務の委託を受けるようなことがないようにすべき。）。

- 業務の再委託に関して現状問題になっているのは、個人情報の取扱いであると考えている。サイバーセキュリティ・サービス提供事業者はそのオペレーションを通じて大量の顧客情報を入手することになるため、本制度においてもＰマークの取得を認定の要件にしてはどうか。

以上