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2回
議事要旨

■ 第2回意見要旨

（審査項目の方向性について）

- 論点の整理の仕方について、組織をどうみるか、人をどうみるか、ツールをどうみるか、及びデータをどうみるかの大きく4つの論点に分けられる。組織という意味では資本関係、すなわち実質的株主がどういう人か。人の観点は組織の中の従業員や派遣もあれば、株主の観点もあり、どこから影響を受け得るか。ツールについては、実質的な製造者が重要である。データについては、データの保存組織及び保存場所がどこかが重要である。これらの善し悪しを一律に決めるのは難しく、グラデーションがあるのではないかと思う。組織内や委託業務に従事する人にどのような人がいるのかなどを契約前に個別に開示してもらうようにすればよいのではないか。それを受けて、契約者側が個々に判断する仕組みであれば柔軟な対応が出来ると考える。
- 最低限これだけは満たしていないと信頼できる組織又はサービスがあるのではなく、この最低限とはどのレベルなのか、それが何かを議論し、その上で、契約者側である各企業・各組織が情報を見て個別に確認するという形にすればよいのではないか。
- 企業全体とサービスの部門とは分けて検討した方がよい。会社の資本関係や従業員の管理方法などは企業全体で捉えることになるが、サービスを担当する部署については、別の項目で捉えた方がよいと考える。
- 承認を得ていない再委託先は認めないようにすべきではないか。承認をどのように得るのかは、個別の実態に即して検討すれば良いと考える。
- 使用ツールに関して、情報管理体制の観点で客先の重要情報の取扱いや保管先については多少踏み込んだ審査項目内容としても良いのではないか。この点、サイバーセキュリティ・サービス提供事業者がよりコストのかかる方法で運用しなければならないことになる。また、地理的な縛りや、場合によっては国家的な縛り等の規定を設けた方がよいと考える。
- データの取扱いに関して、可能な範囲で確認内容を厳格化して欲しい。各クラウドの鍵管理を自分たちの専用のサービスの鍵で行っていることを担保して欲しい。クラウドベンダーが提供する鍵管理システムでも良いが、イメージとしては、少なくともサービスごと、又は自社用のものを使用しているというのが最低限であると考えている。
- 使用ツールに関しては、自己申告制として、後になって事実でないことが発覚すればペナルティを科すということであれば、まだ現実的な運用になると考える。
- 虚偽申請に対するペナルティの導入の話については、監査制度をどうするのかという話がセットになる。登録時の書類審査だけで良いのか、あるいは定期的な監査制度も入れる必要もあるのか、今後、制度の限界として議論の対象としてほしい。
- AI は業務効率化やセキュリティ分野で活用が進んでおり、今後は自律的に作業を行う「AI エージェント」の利用が広がると考えられる。これらは単なるツールではなく、人間のように扱うべきであり、悪意ある動作のリスクもあるため、企業は AI の出自や動作ログをしっかり管理・記録する仕組みが必要。
- 議論の中で、AI、データ及び人などに関する論点が多く挙げられてきたが、一方でリスクの種類を分けておいた方がよいのではないか。例えばデータを流出させないためには、システムで守るのか人で守るのかなどに分けられる。

以上