侵入痕跡・状況異変を検知する見張りのデジタル化を実現する製品・サービスの調達時におけるサイバーセキュリティ上の留意点

デジタル庁
デジタル法制推進担当（技術カタログ公募担当）

テクノロジーマップ・技術カタログを活用し、業務のデジタル化を進めるにあたって、サイバーセキュリティ確保の観点から、本技術カタログに掲載されているデジタル技術の導入に当たって留意すべき点を整理しました。

規制所管省庁の皆様に限らず、地方自治体や規制対象事業者の皆様におかれては、本資料において提示している点を踏まえ、デジタル技術の導入のご判断に活用いただけると幸いです。

本技術カタログに掲載された製品・サービスを調達する際の留意事項

【セキュリティに関する認証の取得状況】

組織/法人のサイバーセキュリティ管理に関する認証について

●サイバーセキュリティの確保の観点から、製品・サービスの提供事業者が組織としてセキュリティの確保に関する十分な体制・仕組みを整備しているかを確認することは重要である。この際、それを明示的に示す認証である、ISO27001 の取得の有無を確認することが推奨される。

●製品・サービスの一部にクラウドサービスを利用している場合には、提供している製品・サービスにおいてクラウドサービス特有のリスクに対する管理策が講じられていることを確認することが必要である。この際、それを明示的に示す認証である、ISO27017 の取得の有無を確認することが推奨される。そのうえで、取り扱う情報の機密性に応じた適切な利用方法をとることが重要である。

【脆弱性検査の実施に関する情報提供】

●サイバーセキュリティの確保の観点から、製品・サービスにおける脆弱性検査の実施は必須となる。したがって、調達する際には、調達する側自身が製品・サービス利用のリスクを正しく評価するため、判断に必要な情報提供を事業者に求めることが推奨される。その際には、脆弱性検査の実施の有無のみならず、適切なガイドラインに沿った検査がなされているかどうかや、準拠したガイドラインの検査レベルについて把握するための情報提供を求めることが挙げられる。

【データ保存先に関する情報提供】

取扱い業務データの保存国

●取扱い業務データの保存国が日本国外となっている場合は、日本以外の複数国のデータセンタのすべてのサーバーが同時にサービス提供できなくなる場合や国外とのネットワークがすべて途絶した場合には、業務サービスが継続されなくなるリスクがある。
そのため、保存されたデータが適切に保管・管理されるかについて、判断に必要な情報提供を事業者に求めることが推奨される。
　その際には、調達する側自身も、クラウドサービスに保存されるデータの可用性や個人情報が含まれるかどうかの観点からリスクが生じた際の被害度を鑑みた上で、判断することが挙げられる。

以　上