往訪閲覧・縦覧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】

●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、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 取得の有無を確認することが推奨される。また、組織や企業のサイバーセキュリティ管理に関する認証だけでなく、製品・サービスそのものがセキュリティ評価制度に則った評価を受けているかを確認することも推奨される。例えば、ISMAP クラウドサービスリストや ISMAP-LIU[1]クラウドサービスリストへの掲載の有無を確認することが挙げられる。

【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、適切な国内外のガイドラインに沿った検査がなされているかどうかや、製品・サービスにおける脆弱性検査の対象箇所（個別機器、システム、サービス全般など）や脆弱性検査の実施者（自己、第三者）、実施頻度などについての情報提供を求めることが挙げられる。

【製品・サービス全体のリスク】

●製品・サービスの一部に AI を活用している場合の一般的なリスクとして、入力データの認識・処理を行ったあとの、利用者が入力した情報がサービスサイトに残存する、ある

[1] 「ISMAP-LIU」の運用を開始しました｜デジタル庁（digital.go.jp）

いは、残存したデータが漏洩するリスクがある。そのため、こうした製品・サービスについては、リスクを正しく理解した上で調達を行うことだけでなく、事業者側の過失によってデータ漏洩や破損等の回復不能な損害が生じた際の担保的責任財産や損害賠償額の上限規定を確認した上で調達を行うことが推奨される。

【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