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】

組織/法人のサイバーセキュリティ管理に関する認証の取得状況

その他製品・サービスに関する認証

●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。

【製品・サービス全体のリスク】

日本における担保的責任財産の概要

損害賠償額上限規定の概要

●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。

以 上

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