講習・試験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

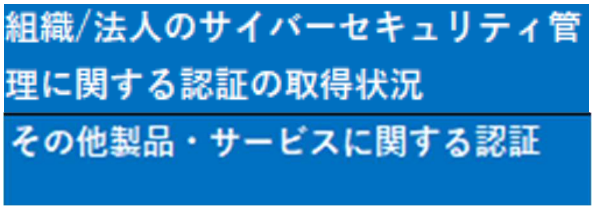
デジタル庁
デジタル法制推進担当（技術カタログ公募担当）

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

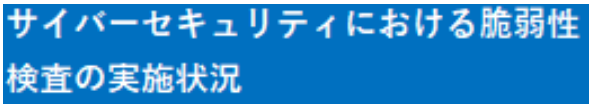
【セキュリティに関する認証の取得状況】



●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、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（ISO27001 を含む）の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。

●個人情報を取得する可能性がある製品・サービスにおいては、個人情報の管理運用体制が整備されていることを確認する必要がある。この際、それを明示的に示す認証である、P マークや ISO27701 の取得の有無を確認することが推奨される。

【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。

以　上

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