認証事業者に望まれるセキュリティ基準について

令和８年〇月　法務省大臣官房司法法制部
審査監督課ＡＤＲ係

認証事業者（新規の申請者を含む。）が独自に情報システムを開発する場合や既存のクラウドサービスを利用する場合のほか、自社でウェブサイトを用意するなどして利用者等の個人情報やプライバシーに関わる情報、営業秘密等を取り扱う場合は、情報及び情報システム等をあらゆる脅威から守るため、セキュリティ上の安全管理措置を講じる必要があります。

ついては、認証事業者においては、以下の基準を参考にセキュリティの確保に努めていただくようお願いします。

なお、デジタル技術は日々進展しており、各機関が公表する要件・指針も随時改訂が行われるため、認証事業者は常に最新のセキュリティの動向に留意し、最新の基準等を適宜参照の上、継続的に安全管理措置の改善に努めていただくようお願いします。

◆望まれる基準

〇全事業者に強く望まれるライン（①及び②両方）

①最新版の「中小企業の情報セキュリティ対策ガイドライン」（ＩＰＡ）に準拠した対応を行うとともに、同ガイドライン「５分でできる！情報セキュリティ自社診断」を１年に１回以上実施し、その結果を当係に報告すること。

②「セキュリティアクション」（★★二つ星）を宣言すること。

〇各事業者の実情に応じて推奨されるライン（実情に応じて①又は②）

①ISO/IEC27001（情報セキュリティ）又はこれに準じる認証を取得すること。

②ISO/IEC27701（個人情報）、プライバシーマーク（個人情報）、ISO/IEC27017（クラウドサービス）、ISO/IEC27018（クラウド上の個人情報）、ISMAP（クラウドサービス）、ISMAP-LIU（クラウドサービス）又はこれらに準じる規格の認証の取得をすること。

※なお、ISO32122は、電子商取引におけるODR規格であり、ODRの基本原則及び技術的推奨事項（個人情報保護やセキュリティ）に関しても触れられていることから、セキュリティの確保に当たっては同規格も参考になると思われます。