令和４年度「地方公共団体における情報セキュリティポリシーに関するガイドライン」改定の概要

別紙1

１.標準準拠システム等のクラウドサービス利用に対応したセキュリティ対策

○ 地方公共団体情報システム標準化基本方針（令和４年10月閣議決定）において、「地方公共団体が利用する標準準拠システム等の整備及び運用に当たっては、地方公共団体における情報セキュリティポリシーに関するガイドラインを参考にしながら、セキュリティ対策を行うものとする」とされたことから、情報システムの標準化・共通化の動向に対応し、標準準拠システム等をクラウドサービス上で利用する際のセキュリティ対策を整理

○ 新たに第４編に「地方公共団体の情報システムのクラウド利用等に関する特則」として、標準準拠システム等をクラウドサービス上で運用する場合のセキュリティ対策について、クラウドサービスの利用に関する情報セキュリティの国際規格（JISQ27017）を参考に記載

２.外部委託先管理の運用面に関するセキュリティ対策

○ 外部委託先に起因する個人情報流出事案を受け、外部委託先管理の運用面に関して、情報のライフサイクル全般での管理の必要性、サーバルームの入退室管理の徹底、職員・委託先従業員のセキュリティ意識の重要性等について記載

○ 一定のセキュリティ水準を確保するため、外部委託時のセキュリティ要件の確認事項として、委託先に提出を求めるチェックシートを提示

３.昨今のサイバー攻撃に対するセキュリティ対策

○ 昨今、国内外の重要インフラにおいて被害が確認されているサイバー攻撃の特徴と攻撃に対する対策を記載

・ランサムウェア	機器やOS等の資産管理、脆弱性に関する対応の確実な実施、パスワード設定の見直し データ・システムのバックアップ、地方公共団体の庁内ネットワーク構成に応じた対策のポイント 等
・Emotet	マクロの実行禁止、メールの監査ログの取得や定期的な確認、組織内への注意喚起 等
・フィッシング	Webサービスにログイン時の多要素認証設定の有効化 等