五城目町情報セキュリティ基本方針

1. 目的

本基本方針は、五城目町（以下「本町」という。）が保有する情報資産の機密性、完全性及び可用性を維持するため、本町が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

2. 定義

(1) 情報資産：情報システム及び情報システムにより処理又は通信される電子データ、並びにシステム関連文書をいう。
(2) 情報セキュリティ：情報資産の機密性、完全性及び可用性を維持することをいう。
(3) 機密性：情報にアクセスすることを認められた者だけがアクセスできる状態を確保することをいう。
(4) 完全性：情報が破壊、改ざん又は消去されていない状態を確保することをいう。
(5) 可用性：情報にアクセスすることを認められた者が、必要なときに中断されることなくアクセスできる状態を確保することをいう。
(6) マイナンバー利用事務系：個人番号利用事務又は戸籍事務等に関わる情報システム及びデータをいう。
(7) LGWAN 接続系：総合行政ネットワーク（LGWAN）に接続された情報システム及びデータをいう。
(8) インターネット接続系：インターネットに接続された情報システム及びデータをいう。
(9) 無害化通信：電子メールのテキスト化等により、不正プログラムの付着が無い等、安全が確保された通信をいう。

3. 対象とする脅威

情報資産の機密性、完全性及び可用性を脅かす以下の脅威を想定し、対策を実施する。
(1) サイバー攻撃、不正アクセス、部外者の侵入、内部不正等の意図的な要因。
(2) 過失による情報の漏えい、設定ミス、機器故障等の非意図的要因。
(3) 地震、落雷、火災等の災害及び大規模な疾病（感染症）インフラ障害からの波及。

4. 適用範囲
(1) 行政機関の範囲 本方針は、町長部局、議会事務局、行政委員会、消防署、公営企業、及び本町の情報資産を取り扱う関係団体（一部事務組合、指定管理者等）に適用する。
(2) 情報資産の範囲 本方針が対象とする範囲は、本町が保有又は管理するネットワーク、情報システム、設備、電磁的記録、並びにこれらに関連する文書とする。

5. 職員等の遵守義務
職員、会計年度任用職員等及び関係団体の職員（以下「職員等」という。）は、情報セキュリティの重要性を共通認識として持ち、業務の遂行において情報セキュリティポリシー及び実施手順を遵守しなければならない。

6. 情報セキュリティ対策
情報資産を保護するため、以下の対策を講じる。
(1) 組織体制：最高情報セキュリティ責任者（CISO）を中心とした全庁的な管理体制、及び情報セキュリティインシデントに対処するためのCSIRTを整備する。
(2) 情報資産の分類と管理:保有する情報資産を重要度に応じて分類し、適切に管理する。
(3) 三層の対策（強靭性の向上）: ① マイナンバー利用事務系は、他の領域と原則分離し、多要素認証等により住民情報の流出を防ぐ。② LGWAN接続系とインターネット接続系の通信経路を分割し、データのやり取りには無害化通信等を用いる。 ③ インターネット接続系は、自治体情報セキュリティクラウドの活用等により高度な監視を行う。
(4) 物理的対策：サーバや情報システムの設置区域への立入制限、機器の固定、電源対策等を行う。
(5) 人的対策：職員等に対する定期的な研修・訓練を実施し、セキュリティ意識の向上を図る。
(6) 技術的対策：アクセス制御、不正プログラム対策、セキュリティホールの修正等を行う。
(7) 運用の管理：情報システムの監視、緊急時対応計画（BCP）の策定、及び外部委託先の監督を行う。
(8) クラウド利用：ガバメントクラウド等の外部サービス利用に際しては、責任分界点を明確にし、適切な選定基準に基づき利用する。

7. 情報セキュリティ監査及び自己点検の実施
対策の実効性を確保するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

8. 情報セキュリティポリシーの見直し
監査結果や社会情勢の変化、大臣指針の改定等を踏まえ、情報セキュリティポリシーを適宜見直す。

9. 対策基準・実施手順の策定
本方針を実行に移すため、具体的な遵守事項を定める「情報セキュリティ対策基準」を策定する。また、個別の運用手順を定める「情報セキュリティ実施手順」を策定する。
なお、対策基準及び実施手順は、公表することにより行政運営に重大な支障を及ぼすおそれがあるため、非公開とする。

附則 この方針は、令和８年４月１日から施行する。