東埼玉資源環境組合情報セキュリティ基本方針

１ 趣旨

基本方針は、セキュリティポリシーの最上位に位置し、情報セキュリティに関する統一的かつ基本的な方針として、東埼玉資源環境組合（以下「組合」という。）における情報セキュリティ対策に対する根本的な考え方及び取り組み姿勢を示すものである。

２ 目的

セキュリティポリシーは、組合が保有する情報資産に係る機密性（権限のないものへの情報資産の提供を防止すること。）、完全性（情報資産の改ざん、破壊等による被害を防止すること。）及び可用性（権限のあるものへいつでも情報資産の利用を可能にすること。）を維持するための対策を総合的、体系的かつ具体的に定めることにより、住民の財産、プライバシー等の保護及び安定的な事務の運営を図ることを目的とする。

３ 用語の定義

セキュリティポリシーにおいて使用する用語を以下のとおり定義する。

(1) 情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

(2) 情報セキュリティポリシー

情報資産を活用するに当たって、セキュリティ上保護すべき対象範囲と、対策や管理運営についての方針を明文化したものをいう。

(3) 情報資産

紙、電磁媒体、フィルム等の記録媒体に記録された全ての情報及び情報システムの総称をいう。

(4) 情報システム

ハードウェア、ソフトウェア、ネットワーク、記録媒体等で構成されるものであって、これら全体で業務処理を行う仕組みをいう。

(5) ネットワーク

電子計算機、関連機器等の多目的利用及び各種オンラインシステムのデータ伝送を目的として構築された情報通信基盤をいう。

(6) 個人番号

行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号。以下「番号法」という。）第２条第５項に規定する個人番号をいう。

(7) 特定個人情報

番号法第２条第８項に規定する特定個人情報をいう。

(8) 特定個人情報等

組合の取り扱う個人番号及び特定個人情報をいう。

４ 対象範囲

(1) 対象機関

管理者、公平委員会、監査委員会及び議会

(2) 対象者

対象機関の職員及び組合が情報資産の取扱いを含む業務を委託する者（以下「職員等」という。）とする。

(3) 対象情報資産

組合行政事務を処理するために取り扱うすべての情報資産

５ 職員等の義務

職員等は情報セキュリティの重要性を認識し、業務の遂行にあたってセキュリティポリシー及び関連する法令等を遵守しなければならない。

また、外部委託業者及び外郭団体に対しても、契約等を通じて、または別途取決めを行うことにより基本方針を遵守させるための必要な措置を講じる。

６ 情報セキュリティ管理体制

東埼玉資源環境組合情報化推進委員会設置要綱第２条（２）の規定に基づき、東埼玉資源環境組合情報化推進委員会（以下「委員会」という。）が管理する。

７ 情報資産の分類

情報セキュリティ対策を確実及び有効にするために、情報資産を明らかにし、かつ重要度別に分類する。

８ 情報資産への脅威

(1) 情報資産に対する脅威の発生度合いや発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

① 部外者による故意の不正アクセス又は不正操作によるデータやプログラムの持出・盗聴・改ざん・消去・機器及び媒体の盗難、故意の障害発生行為によるサービスの停止等

② 職員等及び外部委託業者による意図しない操作、故意の不正アクセス又は不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び媒体の盗難、

規定外の端末接続によるデータ漏洩等

③　地震、落雷、火災等の災害並びに事故、故障等によるサービスの停止等

(2) これらの脅威を十分認識した上で、情報資産の分類の後、各々の情報資産に対する脅威の洗出しを行うものとする。

9 情報セキュリティ対策の実施

情報資産を保護するために、以下の情報セキュリティ対策を講じる。

(1) 人的セキュリティ対策

情報セキュリティに関する権限と責任を定めるとともに、職員等にセキュリティポリシーの内容を周知徹底するなど、十分な教育及び啓発を行うための必要な対策を講じる。

(2) 物理的セキュリティ対策

情報システムを設置する場所への不正な立ち入り、情報資産への危害及び妨害等から保護するために物理的な対策を講じる。

(3) 技術的セキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理、コンピュータウイルス対策等の技術的な対策を講じる。

(4) 運用におけるセキュリティ対策

情報システムの監視及びセキュリティポリシー遵守状況の確認等の運用面における必要な対策を行うとともに、緊急事態が発生した際に迅速に対応するための危機管理対策を講じる。

10 情報セキュリティ対策関連規程の整備

情報セキュリティ対策を講じるにあたり、遵守すべき事項及び体系的かつ効果的な管理のため、以下に示す規程を整備する。

なお、情報セキュリティ対策基準及び実施手順は、公にすることにより組合の事業運営に重大な支障を及ぼす恐れがあることから非公開とする。

(1) 情報セキュリティ対策基準

基本方針に基づき、情報セキュリティを確保するために遵守すべき行為及び判断等の基準を統一的に示すもの

(2) 情報セキュリティ実施手順

基本方針及び対策基準を遵守して情報セキュリティ対策を実施するため、個々の情報資産について、具体的な実施手順を示すもの。

11　情報セキュリティ監査の実施

セキュリティポリシーの遵守及び運用の状況を検証するため、定期的に監査を実施する。

12　違反に対する対応

セキュリティポリシーに違反した者に対しては、その重大性に応じて地方公務員法その他関係法令に基づく厳正な対応を行う。

13　委任

この方針に定めるもののほか必要な事項は、別に定める。