浅川清流環境組合議会　情報セキュリティ基本方針

１．目的

本基本方針は、浅川清流環境組合議会（以下「議会」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、議会が独自に構築・運用する情報システム及びネットワーク並びにこれらで扱う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。

なお、浅川清流環境組合事務局長及び総務課（以下「事務局」という。）において、浅川清流環境組合（以下「組合」という。）から貸与されているパソコン等の端末及び接続するネットワークについては、浅川清流環境組合情報セキュリティポリシーに準拠することとする。

２．定義

（１）ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

（２）情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

（３）情報資産

ネットワーク及び情報システムで取り扱うデータ、システム関連文書をいう。

（４）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。

（５）機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（６）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。

（７）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、情報にアクセスできる状態を確保することをいう。

３．対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

（１）不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（２）情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（３）地震、落雷、火災等の災害によるサービス及び業務の停止等

（４）大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（５）電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

４．適用範囲

（１）組織の範囲

本基本方針は、議会及び事務局に適用する。

（２）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

②ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③情報システムの仕様書及びネットワーク図等のシステム関連文書

５．遵守義務

組合議会議員及び事務局（以下「組合議会議員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、本基本方針を遵守しなければならない。

６．情報セキュリティ対策

上記３の脅威から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）組織体制

議会の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

（２）情報資産の分類と管理

議会の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

なお、議会の保有する情報資産のうち、浅川清流環境組合情報セキュリティポリシー上「自治体機密３」に準じる情報に関しては、浅川清流環境組合情報セキュリティポリシーに準拠する対策を行うものとする。

（３）情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、適切なセキュリティ対策を講じる。

（４）物理的セキュリティ

端末、管理区域（端末等の保管場所）及び通信回線等へ物理的な対策を講じる。

（５）人的セキュリティ

情報セキュリティに関し、組合議会議員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（６）技術的セキュリティ

端末等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（７）運用

情報システムの監視、本基本方針の遵守状況の確認、事故発生時の緊急対応等の対策を講じるものとする。

（８）業務委託と外部サービス（クラウドサービス）の利用

外部委託やクラウドサービス利用時は、セキュリティ要件を契約に明記し、委託先において必要な対策が確保されていることを確認するなど浅川清流環境組合情報セキュリティポリシーに準拠する

対策を行う。

7．情報セキュリティ監査及び自己点検の実施

本基本方針の遵守状況を検証するため、定期的に自己点検を実施するとともに必要に応じて情報セキュリティ監査を実施する。

8．情報セキュリティポリシーの見直し

自己点検及び情報セキュリティ監査の結果、本基本方針の見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、本基本方針を見直す。