浅麓環境施設組合情報セキュリティ基本方針

令和８年３月

情報セキュリティ基本方針

１　目的

本基本方針は、本組合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、本組合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）ネットワーク

コンピュータ等を相互の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。

（４）情報セキュリティポリシー

本基本方針をいう。

（５）気密性

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意図的な要因による情報資産の漏えい・破壊・改ざん・消去等

（２） 情報資産の無断持ち出し、無許可ソフトウエアの使用等の規定違反、プログラム上の欠陥、操作ミス、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　適用範囲

適用範囲は、本組合の全ての職員（会計年度任用職員を含む。）及び関係する全ての機関とする。

5　職員等の遵守義務

職員、会計年度任用職員（以下「職員等」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、業務の遂行にあたって情報セキュリティポリシー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

組合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

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講じる。

（３）物理的セキュリティ

サーバ、通信回線及び職員等のパソコン等の監理について、物理的な対策を講じる。

（４）人的セキュリティ

情報セキュリティに関し、職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。

（５）技術的セキュリティ

コンピュータ等の管理、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。

（６）運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

7　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、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

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシー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、新たに対策が必要となった場合には、情報セキュリティポリシーを見直す。