湖南広域行政組合
情報セキュリティポリシー
【基本方針】

湖南広域行政組合

情報セキュリティ基本方針

1.1　目的

本基本方針は、湖南広域行政組合（以下、「当組合」という。）が保有する情報資産の機密性、完全性および可用性を維持するため、当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。

1.2　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（ハードウェアおよびソフトウェア）をいう。

（2）情報システム

コンピュータ、ネットワークおよ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、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

本基本方針および情報セキュリティ対策基準をいう。

（5）機密性

情報にアクセスすることが認可された者だけが、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、改ざんまた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。

（8）庁内LAN接続系

人事給与、財務会計および文書管理等庁内LANに接続された情報システムおよびその

情報システムで取り扱うデータをいう。

（9）インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システムおよびその情報システムで取り扱うデータをいう。

（１０）通信経路の分割

庁内 LAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

（１１）無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の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。

1.3　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）サイバー攻撃をはじめとする部外者の侵入、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、重要情報の搾取、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、内部・外部監査機能の不備、業務委託管理の不備、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および業務の停止等

（4）大規模・広範囲にわたる疫病による要因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、水道供給の途絶等の提供サービスの障害からの波及等

1.4　適用範囲

（1）機関の範囲

本基本方針が適用される機関は、湖南広域行政組合総務部、湖南広域行政組合出納室、湖南広域消防局、湖南広域行政組合議会、湖南広域行政組合公平委員会および湖

南広域行政組合監査委員とする。

（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、情報システムおよびこれらに関する設備、記録媒体

②ネットワークおよ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およびネットワーク図等のシステム関連文書

1.5　職員等の遵守義務

職員、非常勤職員およびその他組合にかかる業務に従事する者（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および情報セキュリティ実施手順を遵守しなければならない。

1.6　情報セキュリティ対策

上記１．３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

当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全庁的な組織体制を確立する。

（２）情報資産の分類と管理

当組合の所有する情報資産を機密性、完全性、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行う。

（３）情報システム全体の強靭性の向上

情報システム全体に対し、次の二段階の対策を講じる。

①庁内 LAN 接続系においては、庁内 LAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

②インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。

（４）物理的セキュリティ

サーバ等、情報システム室等、通信回線等および職員等のパソコン等の端末の管理について、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、職員等が遵守すべき事項を定めるとともに、十分な教育およ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

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。

（7）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、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

（8）外部サービスの利用

業務委託する場合には、業務委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、業務委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

約款による外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

（9）評価・見直し

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および自己点検を実施し、運用改善を行い情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、情報セキュリティポリシーの見直しを行う。

1.7　情報セキュリティ監査および自己点検の実施

情報セキュリティポリシーの遵守状況を検証するために、必要に応じて情報セキュリティ監査および自己点検を実施する。

1.8　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および自己点検の結果、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およ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。

1.9　情報セキュリティ対策基準の策定

上記１．６、１．７および１．８に規定する対策等を実施するために、具体的な遵守事項および判断基準等を定める情報セキュリティ対策基準等を策定する。

1.10　情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより当組合の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。