湖周行政事務組合情報セキュリティポリシー
（基本方針）

令和８ 年３ 月

湖周行政事務組合

目　　次

１　目的

今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は、生活、経済、社会のあらゆる面で拡大している。その一方で、個人情報の漏えい、不正アクセスや標的型攻撃など新たな攻撃手法による情報資産の破壊・改ざん、操作誤りなどによるシステム障害等が後を絶たない。また、自然災害によるシステム障害やシステム運用の機能不全も事例として発生している。

本組合では、市民の個人情報や行政運営上必要な情報など、重要な情報を多数取り扱うとともに、電子自治体の構築が進み、多くの業務が情報システムやネットワークに依存していることから、これらの情報資産を様々な脅威から防御することは、市民の利益及び財産を守るため、また、行政の安定的かつ継続的な運営のために不可欠である。

これらの状況を鑑み、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、湖周行政事務組合情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）を策定し、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

情報セキュリティポリシーにおける用語の定義は、次のとおりとする。

（１）ネットワーク

端末等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェアを含む。）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等で構成され、これらの全部又は一部で業務処理を行う仕組み（構成及び仕様に関する資料等を含む。）をいう。

（３）標的型攻撃

情報セキュリティ上の攻撃で、無差別に攻撃が行われるものでなく、特定の組織あるいはグループを標的とした攻撃をいう。

（４）個人情報

当該情報に含まれる氏名、生年月日その他の記述等により、特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができるものを含む。）をいう。

（５）特定個人情報
番号法第２条第９項に規定する特定個人情報をいう。

（６）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。

（７）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。

（８）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。

（９）可用性
情報にアクセスすることが認められた者が、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。

（１０）マイナンバー利用事務系（個人番号利用事務系）
個人番号利用事務（社会保障、税若しくは防災に関する事務）等に関わる情報システム及びデータをいう。

（１１）ＬGWAN接続系
ＬGWANに接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く。）。

（１２）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及びその情報システムで取り扱うデータをいう。

（１３）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。

（１４）職員等
職員、嘱託職員、非常勤職員等の任用形態、職制を問わず、本組合の全職員をいう。

（１５）情報セキュリティインシデント

外部からの攻撃や、職員のミスや不正、天災などによって情報セキュリティに対して起こる事故や事象をいう。

事故や事象の大小にかかわらず、情報セキュリティインシデントという。

３ 対象とする脅威

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

① 不正アクセス、ウィルス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漏えい・破壊・改ざん・消去、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程違反、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、外部委託管理の不備、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 電力供給又は通信の途絶等のインフラ障害からの波及等

４ 適用範囲

（１）行政機関の範囲

本基本方針が適用される行政機関は、組合事務局、議会事務局とする。

（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、情報システム及びこれらに関する設備、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 職員等及び外部委託事業者の遵守義務

職員等及び外部委託事業者は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に関し、情報セキュリティポリシー及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。

６ 情報セキュリティ対策

第１編の３に規定する脅威から情報資産を保護するために、次の情報セキュリティ対策を講じる。

（１）組織体制

本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

本組合の情報資産をその内容に応じて分類し、当該分類に応じた情報セキュリティ対策を行う。

（３）物理的セキュリティ対策

情報システムを設置する施設への不正な立ち入り、情報資産の損傷、妨害等から保護するための物理的な対策を講じる。

（４）人的セキュリティ対策

情報セキュリティに関する権限や責任を定めるとともに、職員等及び外部委託事業者が遵守すべき事項を定め、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対策

ネットワーク等の管理、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）運用におけるセキュリティ対策

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、外部委託を行う際のセキュリティ確保等、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切に対応するための危機管理対策を講じる。

７ 情報セキュリティ対策基準の策定

本基本方針に基づく情報セキュリティ対策を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

８ 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必要により策定する。

９ 特定個人情報等の取り扱い

情報セキュリティポリシーのほかに、特定個人情報等の適正な取扱いを定めるため、特定個人情報等の安全管理に関する基本方針及び特定個人情報等取扱規程を別に定める。

１０ 情報セキュリティ自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ自己点検を実施する。

１１ 情報セキュリティポリシーの評価、見直し

情報セキュリティ自己点検の結果、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な対策が必要となった場合は、適宜情報セキュリティポリシーの見直しを実施する。

１２ 情報セキュリティ対策基準及び情報セキュリティ実施手順の非公開

情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより、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。