富士見市監査委員

情報セキュリティポリシー基本方針

令和８年３月３１日　代表監査委員決裁

目次

1　目的

本基本方針は、本機関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、本機関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

本基本方針及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

情報にアクセスでき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）マイナンバー利用事務系（個人番号利用事務系）

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）第２条第１０号及び第１１号に規定する個人番号利用事務又は個人番号関係事務に関する情報システム及びデータをいう。

（9）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（マイナンバー利用事務系で取扱うものを除く。）をいう。

(10) 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。

(11) 通信経路の分割

ＬＧＷＡＮ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。

(12) 無害化処理

インターネットメール本文のテキスト化やサービス等により脆弱性を突いた悪意あるコード等が実行されるおそれがある危険因子を取り除く処理をいう。また、特に無害化処理が行われ安全が確保された通信を「無害化

通信」という。

(13) 端末

情報システムの構成要素である機器のうち、委員、職員、会計年度任用職員及び臨時職員（以下「職員等」という。）が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りが無い限り、本機関が調達又は開発するものをいう。また、端末の形態を問わず、特に業務上の必要に応じて移動させて使用することを目的としたものを「モバイル端末」という。なお、特に断りが無い限り「端末」は「モバイル端末」を含むものとする。

(14) 外部サービス（クラウドサービス）

事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。クラウドサービスのサービス提供形態として、ＳａａＳ（Ｓｏｆｔｗａｒｅ ａｓ ａ Ｓｅｒｖｉｃｅ）、ＰａａＳ（Ｐｌａｔｆｏｒｍ ａｓ ａ Ｓｅｒｖｉｃｅ）、ＩａａＳ（Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ ａｓ ａ Ｓｅｒｖｉｃｅ）が存在する。

(15) Ｗｅｂ会議サービス

専用のアプリケーションやＷｅｂブラウザを利用し、映像又は音声を用いて会議参加者が対面せずに会議を行える外部サービスをいう。なお、特定用途機器同士で通信を行うもの（テレビ会議システム、ネットワークカメラシステム、ＩＰ電話システム等）は含まれない。

(16) ソーシャルメディアサービス

インターネット上で展開される情報メディアのあり方で、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった社会的な要素を含んだメディアのことをいう。利用者の発信した情報や利用者間のつながりによってコンテンツを作り出す要素を持ったＷｅｂサイトやネットサービスなどを総称する用語で、ソーシャルネットワーキングサービス（ＳＮＳ）や電子掲示板(ＢＢＳ)、ブログ、動画共有サイト、動画配信サービス、ショッピングサイトの購入者評価欄などを含む。

3　対象とする脅威

情報資産に対する次の脅威を想定し、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、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、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）機関の範囲
本基本方針が適用される機関は、監査委員及び監査委員事務局とする。
（２）情報資産の範囲
本基本方針が対象とする情報資産は、次のとおりとし、主な情報資産の例は下表のとおりとする。
①ネットワーク、情報システム、これらに関する設備、電磁的記録媒体等
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

情報資産の種類	情報資産の例
ネットワーク	通信回線、ルータ等の通信機器等
情報システム	サーバ、パソコン、モバイル端末、汎用機、複合機、オペレーティングシステム、ソフトウェア等
ネットワーク及び情報システムに関する施設・設備	コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル等
電磁的記録媒体	サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体、ＵＳＢメモリ、外付けハードディスクドライブ、ＤＶＤ－Ｒ、磁気テープ等の外部電磁的記録媒体等
ネットワーク及び情報システムで取り扱う情報	ネットワーク、情報システムで取り扱うデータ等（これらを印刷した文書を含む。）
システム関連文書	システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等

（３）適用範囲の例外
「教育学習に利用するネットワーク(校務系､学習系､校務外部接続系等)」、「医療情報系ネットワーク(レセプトオンライン､オンライン資格確認等)」等の情報セキュリティ対策の基準が別途示されている専用ネットワーク及び専用情報システムは、本基本方針の適用範囲から除外し、別途示されている専用ネットワーク及び専用情報システムの情報セキュリティ対策の基準を優先する。

５　職員等の遵守義務
職員等は、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

上記３の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

本機関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

本機関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行う。

（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、次の三段階の対策を講じる。

①マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

②ＬＧＷＡＮ接続系においては、ＬＧＷＡＮ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。

③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。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（４）物理的セキュリティ

サーバ、情報システム室、通信回線及び職員等の端末等の管理について、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

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切に対応するため、緊急時対応計画を策定する。

（８）業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、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、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。

外部サービス（クラウドサービス）を利用する場合には、利用に係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、定期的又は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、適宜情報セキュリティポリシーの見直しを行う。

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、定期的又は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になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

9　情報セキュリティ対策基準

監査委員事務局の情報セキュリティ対策基準については、市長の事務部局の情報セキュリティ対策基準において定めるところによる。

なお、情報セキュリティ対策基準は、公にすることにより本機関の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。

10　情報セキュリティ実施手順

監査委員事務局の情報セキュリティ実施手順については、市長の事務部局の情報セキュリティ実施手順において定めるところによる。

なお、情報セキュリティ実施手順は、公にすることにより本機関の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。