情報セキュリティ基本方針

１　目的

本市が取り扱う情報資産には、市民の個人情報のみならず行政運営上重要な情報など、外部に漏えい等した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、これらの情報資産を人的脅威や災害、事故等の様々な脅威から防御することは、市民の財産、プライバシー等を守るためにも、継続的かつ安全、安定的な行政サービスの実施を確保するためにも必要不可欠である。

また、近年のいわゆるＩＴ革命の進展により、番号制度の導入など電子政府や電子自治体の構築が現実のものとなっている。本市がこれらに積極的に対応するためには、本市が管理している全てのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

そのため、本市の情報資産の機密性、完全性及び可用性を維持するための対策を整備するため、情報セキュリティポリシーを定めるものとし、情報セキュリティの確保に最大限に取り組むものとする。このうち、情報セキュリティ基本方針においては、本市の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置づけ等を定めるものとする。

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）　技術的脅威

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、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）　物理的脅威

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）　災害等

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）　パンデミック

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）　インフラ障害

電力供給の途絶、通信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

本基本方針が適用される組織は、本庁の各部課、出先機関、教育委員会事務局、議会事務局及び消防本部とする。

（２）　対象者

本基本方針が適用される対象者は、本市の情報資産を取り扱う職員等とする。

（３）　情報資産

本基本方針が対象とする情報資産は、次のとおりとする。

（ア）　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

（イ）　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。）

（ウ）　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

情報資産の種類と例

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
情報システム	サーバ、パソコン、モバイル端末、汎用機、オペレーティングシステム、ソフトウェア等
これらに関する施設・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
電磁的記録媒体	サーバ機器、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、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
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（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

５　情報セキュリティポリシーの位置づけ

情報セキュリティポリシーは、本市の情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の最高位に位置するものである。

６　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、業務の遂行に当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。

７　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

本市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

本市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）　物理的セキュリティ

サーバ等、情報システム室（以下「電算室」という。）等、通信回線等及び職員等のパソコン等の管理について、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、外部委託を行う際のセ

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　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。

９　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、情報セキュリティポリシーを見直す。

１０　情報セキュリティ対策基準の策定

上記７、８及び９に規定する対策等を実施するために、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。

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市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。

１１　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本市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。