羽村市
情報セキュリティ基本方針

目　　次

羽村市情報セキュリティ基本方針

１　目的

羽村市情報セキュリティ基本方針（以下「基本方針」という。）は、市が保有する情報資産を様々な脅威から組織的、体系的かつ継続的に保護するための統一的な方針並びに情報資産の安全管理対策を実践するにあたっての基本的な考え方及び方策を定めることを目的とする。

２　適用範囲

この基本方針は、市が保有する情報資産、情報資産を取り扱う全職員（嘱託員及び臨時職員等を含む。以下「職員」という。）及び市の事務事業の委託を受けた者（以下「受託者」という。）に適用する。

３　用語の定義

この基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1) 情報資産　情報及び情報システムをいう。

(2) 情報　市が保有するすべての情報をいう。

(3) 情報システム　ネットワーク、ハードウェア、ソフトウェア及び記録媒体で構成され、処理を行う仕組みをいう。

(4) ネットワーク　コンピュータを相互に接続するための通信網及びその構成機器をいう。

(5) 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。

(6) 機密性　情報にアクセスすることを認められた者だけがアクセスできることという。

(7) 完全性　情報及び処理の方法が正確及び完全であることをいう。

(8) 可用性　認められた者が必要なときに情報にアクセスできることをいう。

４　管理体制

情報セキュリティ対策を推進及び管理するための組織体制を整備する。

５　情報資産の分類及び管理

情報の機密性、完全性及び可用性を踏まえた情報資産の分類を行い、その重要性に応じて、適切な管理を行う。

６　情報セキュリティ対策

情報資産を、故意、過失、災害及び故障等の脅威から守るため、次に掲げる対策を講ずる。

(1)物理的セキュリティ対策　情報システムの設置場所及び情報の保管場所等への不正な立入り並びに情報資産の損害及び利用の妨害等を防止するための入退室及び機器の管理等の物理的な対策

(2)人的セキュリティ対策　不正行為、操作ミス及び機器の誤使用等を防止するための研修の実施等の人的な対策

(3)技術的セキュリティ対策　不正アクセス又はウイルス感染等による情報資産の損傷及び利用の妨害を防止するための情報資産へのアクセス制御及びネットワーク管理等の技術的な対策

(4)運用面におけるセキュリティ対策　情報システムの監視及び情報セキュリティ対策の実施状況の確認等の運用面の対策

(5)緊急時におけるセキュリティ対策　緊急事態が発生した場合における迅速かつ適切な対応を可能とするための危機管理対策

７　情報セキュリティ対策の体系

基本方針に基づき情報セキュリティ対策を講じるにあたって、以下の基準及び手順を定める。

(1)羽村市情報セキュリティ対策基準（以下「対策基準」という。）

情報セキュリティ対策を実施するにあたっての遵守すべき事項及び判断等の統一的な基準

(2)羽村市情報セキュリティ実施手順　情報セキュリティ対策を実施するための具体的な手順

８ 法令等の遵守

職員及び受託者は、著作権法（昭和 45 年法律第 48 号）、不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）及び羽村市個人情報保護条例（平成 15 年条例第 22 号）等、情報セキュリティに係る関係法令等を遵守しなければならない。

９ 職員及び受託者の責務

職員及び受託者は、情報セキュリティ対策の重要性について共通の認識をもつとともに、業務の遂行において、基本方針及び対策基準（以下「情報セキュリティポリシー」という。）を遵守しなければならない。

１０　情報セキュリティポリシーに違反した職員及び受託者への対応

情報セキュリティポリシーに違反した職員及び受託者については、その重大性及び発生した事案の状況等に応じて、地方公務員法（昭和 25 年法律 261 号）その他の関係法令等の規定に基づき厳正に対応する。

１１　情報セキュリティ監査の実施

情報セキュリティポリシーが遵守されていることを検証するため、定期的に監査を実施する。

１２　評価及び見直し

情報セキュリティ監査の結果等に基づき、情報セキュリティ対策についての評価を定期的に実施するとともに、情報セキュリティを取り巻く状況の変化等に対応して、情報セキュリティポリシーの見直しを実施する。