富士市情報セキュリティ基本方針

１．目的

富士市情報セキュリティ基本方針は、高度情報化社会における、市民の皆様の安全を守るため、富士市（以下「本市」という。）が取り扱う情報資産の機密性、完全性、可用性を確保し、これを維持していくための基本的な事項を定めることを目的とする。

２．用語の定義

（１） 職員等
本市の情報資産に接する職員その他の利用者

（２） 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、その他構成機器

（３） 情報資産
情報及び情報システム

（４） 情報
職員等が職務上作成し、又は取得した全ての文書等

（５） 情報システム
コンピュータ、ネットワーク、記録媒体等（ハードウェア・ソフトウェア含む）で構成され、これらで業務処理を行う仕組みをいう。

（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。

（７） 機密性
アクセスを認可された者だけが情報にアクセスできることを確実にすること。

（８） 完全性
情報及び処理方法が、正確であること及び完全であることを保護すること。

（９） 可用性
認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。

３．適用範囲

（１） 行政機関の範囲　本市の情報資産に接するすべての組織及び職員等

（２） 情報資産の範囲　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
④その他業務上作成された各文書等

４．対抗する脅威

情報資産への脅威として、以下の脅威を認識し、情報セキュリティ対策を実施する。
（１） 職員等による操作ミス、紛失、物理的及び論理的侵入、窃盗、妨害、破壊、盗聴、なりすまし、改ざん、著作権の侵害、業務目的外使用等
（２） 職員等以外による物理的及び論理的侵入、窃盗、妨害、破壊、盗聴、なりすまし、改ざん等
（３） コンピュータウイルス等の悪意のあるプログラム
（４） 地震、雷、火災、風害、水害等の災害
（５） 停電、回線断、故障、異常動作、容量超過等

５．職員等の遵守義務

本市の職員等は、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を遵守しなければならない。

６．情報セキュリティ対策

本市における情報セキュリティ対策の基本的な考え方を以下に示す。
（１)情報セキュリティ対策の構成
本市における情報セキュリティ対策は、情報セキュリティポリシーに基づき実施する。情報セキュリティポリシーは次のものにより構成する。
① 情報セキュリティ基本方針 （以下「基本方針」という。）
情報セキュリティ対策に関する統一的かつ基本的な方針を定めたもの
② 情報セキュリティ対策基準 （以下「対策基準」という。）
基本方針に基づき情報セキュリティを確保するために遵守すべき行為等の基準について定めたもの
なお、個々の情報資産の情報セキュリティ対策においては、基本方針及び対策基準に基づき、情報システム毎に、より具体的な「情報セキュリティ実施手順（以下「実施手順」という。）」を策定し、実施する。
（２） 組織及び体制
本市における情報セキュリティ対策は、責任や役割を明確にした組織及び体制のもとに行うものとする。
（３） 情報の分類及び管理

本市の情報システムにおいて取扱う情報について、重要な情報を重点管理するため、重要度に応じた情報分類の定義を行い、情報の管理責任及び管理方法を明確にする。

(４) 人的セキュリティ

情報セキュリティに関する役割や責任を明確化し、職員等に基本方針、対策基準及び実施手順の内容を周知徹底するため、研修、啓発等の必要な対策を実施する。

(５) 物理的セキュリティ

情報システムの設置場所について、不正な立入り、損傷及び妨害から情報資産を適切に保護するため、入退室管理等の物理的な対策を実施する。

(６) 技術的セキュリティ対策及び運用管理

本市の所有する情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の必要な対策を実施する。

(７) 記録媒体の取扱い及び管理

本市の情報システムにおける記録媒体について、適正な管理をするための対策を実施する。

(８) 情報システムの開発等

本市の業務に使用する情報システムの開発、導入及び保守においては、情報資産を適切に保護するために必要な対策を実施する。

(９) 委託

本市の情報システムの開発、運用、保守等を外部に委託する場合は、情報セキュリティに関する必要な対策を実施する。

(１０) 情報セキュリティに関する事故等への対応

情報セキュリティに関する事故等が発生した場合の対応をあらかじめ定めるとともに、情報セキュリティに関する事故等が発生した際には、定められた対応を迅速かつ円滑に実施し、その影響を最小限にするとともに、再発防止のために必要な対策を実施する。

(１１) 法令等の遵守

職員等は、基本方針、対策基準及び実施手順に定められた条項のほか、情報資産の利用において、関連法令、本市が定める条例等を遵守し、これに従う。

(１２) 基本方針等に対する違反への対応

職員等が基本方針、対策基準及び実施手順に違反した場合は、その重大性、状況等に応じた罰則(注意、警告及び再教育等を含む)の適用対象とする。

(１３) 基本方針等の見直し

新たな脅威等を踏まえ、定期的に基本方針、対策基準及び実施手順の評価を行い、情報システムの変更及び基本方針、対策基準、実施手順の見直しを実施する。

７．公開範囲

基本方針は、職員等に対して本市の情報セキュリティ対策への指針を示すため、また市民等に対して本市の情報セキュリティ対策への理解を得るため、公開するものとする。