

富 士 見 市
情報セキュリティポリシー
(基本方針)

(平成15年7月10日 富士見市IT推進委員会了承)

(平成15年7月18日 市長決裁)

情報セキュリティポリシーの構成

情報セキュリティポリシーとは、富士見市が所掌する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を総称する。情報セキュリティポリシーは、富士見市が所掌する情報資産に関する業務に携わる全職員、非常勤及び臨時職員に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（対策基準）に分けて策定することとした。

具体的には、情報セキュリティポリシーを、①情報セキュリティ基本方針及び②情報セキュリティ対策基準の2階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づき、情報システムごとの具体的な情報セキュリティ対策の実施手順として情報セキュリティ実施手順を策定することとする（下表参照）。

情報セキュリティポリシーの構成

文書名		内 容
情報セキュリティ ポリシー	情報セキュリティ 基本方針	情報セキュリティ対策に関する統一 かつ基本的な方針。
	情報セキュリティ 対策基準	情報セキュリティ基本方針を実行に移 すための全ての情報システムに共通の 情報セキュリティ対策の基準。
情報セキュリティ実施手順		情報システムごとに定める情報セキュ リティ対策基準に基づいた具体的な実 施手順。

情報セキュリティ基本方針

1 目的

富士見市の各情報システムが取り扱う情報には、市民の個人情報のみならず行政運営上重要な情報など、部外に漏洩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、これらの情報及び情報を取り扱う情報システムを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、また、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが富士見市に対する市民からの信頼の維持向上に寄与するものである。

また、近年のいわゆるIT革命の進展により、電子商取引の発展や電子自治体の実現が期待されているところである。富士見市がこれらに積極的に対応するためには、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、富士見市の情報資産の機密性、完全性及び可用性（注1）を維持するための対策（情報セキュリティ対策）を整備するために富士見市情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については富士見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、位置付け等を定めるものとする。

（注1）：国際標準化機構（ISO）が定めるもの（ISO7948-2：1989）

機密性（confidentiality）：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

完全性（integrity）：情報及び処理の方法の正確さ及び完全である状態を安全防護すること。

可用性（availability）：許可された利用者が必要なときに情報にアクセスできることを確実にすること。

2 定義

（1）ネットワーク

富士見市における内部部局、各行政委員会、議会事務局、各地方公営企業及び各教育機関（事務室及び職員室のみ）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）及び記録媒体で構成され、処理を行う仕組みをいう。

（2）情報システム

電子計算機（ネットワーク、ハードウェア及びソフトウェア）及び記録媒体で構成され、処理を行う仕組みをいう。

（3）情報資産

ネットワーク及び情報システムの開発と運用に係る全てのデータ並びにネットワーク及び情報システムで取り扱う全てのデータをいう。

（4）情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能

な状態を維持することをいう。

3 情報セキュリティポリシーの位置付けと職員等の義務

情報セキュリティポリシーは、富士見市が所掌する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頂点に位置するものである。

したがって、富士見市長をはじめとして富士見市が所掌する情報資産に関する業務に携わる全ての職員等及び部外委託者は、情報セキュリティ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当たって情報セキュリティポリシーを遵守する義務を負うものとする。

4 情報セキュリティ管理体制

富士見市の情報資産について、幹部が率先して情報セキュリティ対策を推進・管理するための体制を確立するものとする。

5 情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

6 情報資産への脅威

情報セキュリティポリシーを策定するうえで、情報資産を脅かす脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

- (1) 部外者による故意の不正アクセスまたは不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び媒体の盗難等
- (2) 職員等及び部外委託者による意図しない操作、故意の不正アクセスまたは不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び媒体の盗難及び規定外の端末接続によるデータ漏洩等
- (3) 地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止

7 情報セキュリティ対策

上記6で示した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ずるものとする。

(1) 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入り、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

(2) 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、全ての職員等に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるように必要な対策を講ずる。

(3) 技術及び運用におけるセキュリティ対策

情報資産を外部からの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技術面の対策、また、システム開発等の外部委託、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等の運用面の対策を講ずる。また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

8 情報セキュリティ対策基準の策定

富士見市の様々な情報資産について、上記7の情報セキュリティ対策を講ずるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

9 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を遵守して情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めていく必要がある。そのため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、内部部局の長等が所掌する情報資産の情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティポリシー及び情報セキュリティ実施手順は、公にすることにより富士見市の行政運営に重大な支障を及ぼす恐れのある情報であることから原則非公開とする。

10 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。

11 評価及び見直しの実施

情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを実施する。