

# 富士川町情報セキュリティポリシー

平成22年 3月 8日 策定

平成27年 4月 1日 全部改定

平成28年 4月 1日 一部改定

# 目次

第1章 情報セキュリティ基本方針 .....	1
1. 目的 .....	1
2. 定義 .....	1
3. 対象とする脅威 .....	2
4. 適用範囲 .....	2
5. 職員等の遵守義務 .....	2
6. 情報セキュリティ対策 .....	2
7. 情報セキュリティ監査及び自己点検の実施 .....	3
8. 情報セキュリティポリシーの見直し .....	3
9. 情報セキュリティ対策基準の策定 .....	3
10. 情報セキュリティ実施手順の策定 .....	3
第2章 情報セキュリティ対策基準 .....	4
1. 対象範囲 .....	4
1.1 行政機関の範囲 .....	4
1.2 情報資産の範囲 .....	4
1.3 峡南広域行政組合計算センターとの連携 .....	4
1.4 住民基本台帳ネットワークシステムとの関係 .....	4
2. 組織体制 .....	4
2.1 最高情報統括責任者(CISO) Chief Information Security Officer .....	4
2.2 統括情報セキュリティ責任者 .....	5
2.3 副統括情報セキュリティ責任者 .....	5
2.4 情報セキュリティ責任者 .....	5
2.5 情報セキュリティ管理者 .....	6
2.6 情報システム管理者 .....	6
2.7 情報システム担当者 .....	6
2.8 富士川町情報セキュリティ委員会 .....	6
2.9 兼務の禁止 .....	6
2.10 情報セキュリティ体制体系図 .....	7
3. 情報資産の分類と管理 .....	8
3.1 情報資産の分類 .....	8
3.2 情報資産の管理 .....	9
4. 物理的セキュリティ .....	11
4.1 サーバ等の管理 .....	11
4.2 管理区域(情報システム室等)の管理 .....	12
4.3 通信回線及び通信回線装置の管理 .....	13
4.4 職員等のパソコン等の管理 .....	14

5. 人的セキュリティ.....	14
5.1 職員等の遵守事項.....	14
5.2 非常勤及び臨時職員への対応.....	15
5.3 情報セキュリティポリシー等の掲示.....	15
5.4 外部委託事業者等への対応.....	15
5.5 研修・訓練.....	15
5.6 事故、欠陥に対する報告.....	16
5.7 ID及びパスワード等の管理.....	16
6. 技術的セキュリティ.....	17
6.1 コンピュータ及びネットワークの管理.....	17
6.2 アクセス制御.....	21
6.3 システム開発、導入、保守等.....	22
7. 運用.....	26
7.1 情報システムの監視.....	26
7.2 情報セキュリティポリシーの遵守状況の確認.....	26
7.3 侵害時の対応.....	27
7.4 外部委託.....	27
8. 例外処置.....	28
8.1 例外措置の許可.....	28
8.2 緊急時の例外措置.....	28
8.3 例外措置の申請書の管理.....	28
9. 法令遵守.....	28
10. 懲戒処分等.....	29
10.1 懲戒処分等.....	29
10.2 違反時の対応.....	29
11. 評価・見直し.....	29
11.1 監査.....	29
11.2 自己点検.....	30
11.3 情報セキュリティポリシーの見直し.....	30

# 第1章 情報セキュリティ基本方針

## 1. 目的

富士川町の各情報システムが取扱う情報には、町民の個人情報、行政運営上重要な情報など、外部への漏洩、消失、破壊、改竄、情報システムの停止等が発生した場合、極めて重大な結果を招くものが含まれている。これらの情報及び情報を取り扱うシステムを様々な脅威から防御することは、事務の安定的な運営を図り、町民の財産、プライバシー等を守るため不可欠である。また、情報技術の進歩にともない、より高度で広範囲な行政の情報化が進められている。富士川町がこれに対応していくためには、全ての情報システムの運用に対して十分な安全性を維持していくことが求められる。この要求に答えるため、富士川町職員等が情報資産を安全に取り扱うための規範である富士川町情報セキュリティポリシーを定める。富士川町情報セキュリティポリシーは、これを職員等に浸透、普及、定着を図ることにより、取り扱われる情報資産の安全性を高め、町民からの信頼の維持向上に寄与するためのものである。

## 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情報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。

### (5) 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。

### (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、情報にアクセスできる状態を確保することをいう。

### (7) 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。

### (8) 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

情報資産への脅威は、情報を取り扱う環境に広く存在し、その形態も多様であるうえ、新たな種類の脅威が発生する場合もあるので、脅威の存在やその影響を常に監視するように努めるものとする。

本情報セキュリティポリシー策定時に特に考慮した、注意すべき脅威は以下のとおりである。

- (1) 部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報資産の漏えい・破壊・盗聴・改ざん・消去等
- (2) 情報資産の持出、操作ミス、パスワードの不適切管理、故意の不正アクセスまたは不正行為による情報資産の漏えい・破壊・盗聴・改ざん・消去等、搬送中の事故等による機器または情報資産の盗難
- (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

### 4. 適用範囲

- (1) 行政機関の範囲

本セキュリティポリシーが適用される行政機関は、内部の各所属、出先施設、教育委員会、議会事務局及び福祉・保健施設とする。

- (2) 情報資産の範囲

本セキュリティポリシーが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

### 5. 職員等の遵守義務

職員、非常勤職員及び臨時職員(以下「職員等」という。)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。

### 6. 情報セキュリティ対策

上記3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) 組織体制

富士川町の情報資産について、管理職が率先して情報管理対策を推進・管理するための全庁的な体制を確立するものとする。

- (2) 情報資産の分類と管理

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

- (3) 物理的セキュリティ対策

サーバ室、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。

(4) 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、全ての職員等及び外部委託事業者に情報セキュリティに関して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ずる。

(5) 技術的セキュリティ対策

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、コンピュータの管理、情報資産へのアクセス制御、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ずる。

(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ずる。また、情報資産への侵害が発生した場合等に迅速な対応を可能とするための緊急時対応体制を策定する。

## 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が遵守されていることを検証するために、定期的または必要に応じて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により、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を取り巻く状況の変化に対応するため新たに対策が必要となった場合には、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書の見直しを実施する。

## 9. 情報セキュリティ対策基準の策定

富士川町の様々な情報資産について、上記6, 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。

## 10. 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、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富士川町の行政運営に重大な支障を及ぼす恐れのある情報資産であることから非公開とする。