藤沢市情報セキュリティポリシー
基本方針
＜詳細編＞

藤沢市

文書の新規発行／改定

版数	改定／施行年月日	文書の新規制定／改定内容	承認者	作成部署	文書整理番号
00	改定：平成　年　　月　　日 施行：平成 18 年　3 月 22 日	新規制定	久世助役	ＩＴ推進課	17fj1305hi0388
01	改定：平成 19 年　4 月　1 日 施行：平成 19 年　4 月　1 日	助役名称の変更 （助役→副市長）	久世 副市長	ＩＴ推進課	181305001938
02	改定：平成 20 年　2 月　6 日 施行：平成 20 年　4 月　1 日	組織改正及びネットワーク 更新に伴う変更	久世 副市長	ＩＴ推進課	191305001380
03	改定：平成 21 年　2 月　5 日 施行：平成 21 年　4 月　1 日	組織改正に伴う変更	新井 副市長	ＩＴ推進課	201305001418
04	改定：平成 22 年　2 月　2 日 施行：平成 22 年　4 月　1 日	別表 2 の追加	新井 副市長	ＩＴ推進課	211115001794
05	改定：平成 23 年　2 月　2 日 施行：平成 23 年　4 月　1 日	総務省セキュリティポリシー ガイドライン改定に伴う変更	新井 副市長	ＩＴ推進課	221115002437
06	改定：平成 24 年　2 月　1 日 施行：平成 24 年　4 月　1 日	メール転送機能に関する追記	山田 副市長	ＩＴ推進課	231115002167
07	改定：平成 25 年　1 月 31 日 施行：平成 25 年　4 月　1 日	地域イントラネットに関する記述を修正	石井 副市長	ＩＴ推進課	241115002107
08	改定：平成 28 年　2 月　1 日 施行：平成 28 年　2 月　1 日	全面改定	石井 副市長	ＩＴ推進課	271115002217
09	改定：令和　元年 9 月　1 日 施行：令和　元年 9 月　1 日	総務省セキュリティポリシー ガイドライン改定に伴う変更	小野 副市長	ＩＴ推進課	011115000567
10	改定：令和　3 年 4 月　1 日 施行：令和　3 年 4 月　1 日	関連規程の改定及び組織改正に伴う変更	和田 副市長	情報 システム課	031115000022
11	改定：令和　4 年 3 月 11 日 施行：令和　4 年 4 月　1 日	組織改正及び総務省セキュリティポリシーガイドライン改定に伴う変更	和田 副市長	情報 システム課	031115001279
12	改定：令和　4 年 12 月 1 日 施行：令和　4 年 12 月 1 日	総務省セキュリティポリシーガイドライン改定に伴う変更	和田 副市長	情報 システム課	041115000981
13	改定：令和　5 年　4 月 1 日 施行：令和　5 年　4 月 1 日	関連法の改定に伴う変更	和田 副市長	情報 システム課	051115000214

14	改定：令和　7 年　2 月 28 日 施行：令和　7 年　4 月 1 日	組織改正に伴う変更	中山 副市長	情報 システム課	061115001594
15	改定：令和　7 年　6 月 1 日 施行：令和　7 年　6 月 1 日	総務省セキュリティポリシーガイドライン改定に伴う変更	中山 副市長	デジタル 戦略課	071321000447
16	改定：令和　8 年　3 月 18 日 施行：令和　8 年　4 月 1 日	関連法の改正及び総務省セキュリティポリシーガイドライン改定に伴う変更	中山 副市長	デジタル 戦略課	071321002259

目次

1　目的

藤沢市が保有する情報資産の機密性、完全性及び可用性を維持・向上するための対策について、遵守すべき行為や判断等の基準を統一的なレベルで定め、統合的、体系的かつ具体的に取りまとめるため、『藤沢市情報セキュリティポリシー』（以下「本ポリシー」という。）を策定する。

また、「サイバーセキュリティ基本法」第5条では、地方公共団体は「サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有する」と定められていることから、本ポリシーでは、藤沢市のサイバーセキュリティに対する対策の基準及び実施の責務を定めるとともに、「地方自治法」第244条の6の第1項において、「普通地方公共団体の議会及び長その他の執行機関は、それぞれの管理する情報システムの利用に当たってのサイバーセキュリティを確保するための方針を定め、及びこれに基づき必要な措置を講じなければならない。」と定められていることから、『藤沢市情報セキュリティポリシー基本方針＜詳細編＞』を「地方公共団体におけるサイバーセキュリティを確保するための方針」と位置付けるものとする。

本ポリシーは、藤沢市が保有する情報資産に関する業務に携わる全ての職員（会計年度任用職員、特別職、臨時・非常勤職員、派遣職員等を含む。以下「職員等」という。）及び委託事業者に対し、情報セキュリティの維持、強化を促すものである。

『藤沢市情報セキュリティポリシー』の体系を以下のとおりとする。

『藤沢市情報セキュリティポリシー基本方針』

『藤沢市情報セキュリティポリシー基本方針＜詳細編＞』

『藤沢市情報セキュリティポリシー対策基準』

2　定義

本ポリシーにおける用語は、当該各号に定めるところによる。

（1） 情報システム

サーバ及び端末並びにそれらの周辺機器、通信ネットワーク等により電子情報を処理するシステム（クラウドサービスその他のハードウェアが本市の管理下にないものを含む。）をいう。

（2） 通信ネットワーク（以下「ネットワーク」という。）

サーバ及び端末等を接続してデータ通信するための情報通信網並びにその運営に必要な設備及び機器をいう。

（３） データ
情報システム又は電磁的記録媒体及び紙媒体等に記録されている情報をいう。

（４） 情報セキュリティ
組織で保有している情報資産を機密性、完全性、可用性が損なわれるような脅威から守ることをいう。

（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。

（８） 基幹系システム
個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータ（本ポリシー対策基準で定める重要性分類Ａの情報）をいう。

（９） 情報系システム
ＬＧＷＡＮに接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く）。

（１０） インターネット接続系システム
インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

（１１） 通信経路の分割
情報系システムとインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

（１２） 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

（１３） 情報資産

組織が持つ情報と情報システム及びこれらが適切に保護され機能するために必要な要件の総称をいう。

（１４） 電磁的記録媒体

情報システムを利用して行うデータの処理に係る磁気ディスク、光ディスクその他これらに準ずる方法により一定の事項を確実に記録しておくことができる物をいう。

（１５） 端末

端末とは、パーソナルコンピュータ及び利用者がコンピュータにデータを入出力するための機能を備えた装置をいう。

（１６） オフィス機器

業務で使用する機器(複合機、プリンタ、スキャナ、電話、ＦＡＸ、コピー機等)をいう。

３　対象とする脅威

本ポリシーを策定する上で、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） 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等の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） 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、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） 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） 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） 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

４　適用範囲

（１） 行政機関の範囲[1]

本ポリシーが適用される行政機関は、藤沢市情報公開条例（平成 13 年 6 月 25 日条例第 3 号）第 4 条第 2 項に規定する実施機関とする。

（２） 情報資産の範囲

藤沢市が所有する情報資産の全てを対象とする。ただし、本ポリシー対策基準の別表 1 に掲げるネットワーク及び情報システム等情報資産については、対象外とする。

５　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本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

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実施する。

[1] 市民病院における病院採用職及び教育委員会における県費負担教職員、指定管理者及び藤沢市土地開発公社は、本ポリシーの適用範囲から除く。

（３） 情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

ア　基幹系システムにおいては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

イ　情報系システムにおいては、ＬＧＷＡＮと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

ウ　インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（４） 物理的セキュリティ

重要なシステム、ネットワーク基幹機器が設置されている領域や、通信回線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。

（５） 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。

（６） 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。

（７） 運用

情報システムの監視、本ポリシーの遵守状況の確認、本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正に対応するため、緊急時対応計画を策定する。

（８） 業務委託・クラウドサービス等の利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

クラウドサービスを利用する場合には、利用に係る規定を整備し対策を講じる。

（９） その他の情報セキュリティ

紙媒体文書の取扱いや電話、ＦＡＸ、会話におけるセキュリティ対策を講じる。

（１０） 評価・見直し

本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し、運用改善を行い、情報セキュリティの向上を図る。本ポリシーの見直しが必要な場合は、適宜本ポリシーの見直しを行う。

７　情報セキュリティ監査及び自己点検の実施

本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。

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、本ポリシーを見直す。

９　情報セキュリティ対策基準の策定

本ポリシーに基づき、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本ポリシー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

本ポリシーに基づき、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。

１１　『藤沢市情報セキュリティポリシー』の公開

『藤沢市情報セキュリティポリシー基本方針』及び『藤沢市情報セキュリティポリシー基本方針＜詳細編＞』は公開とするが、『藤沢市情報セキュリティポリシー対策基準』及び各情報セキュリティ実施手順は、公にすることにより藤沢市の行政運営に重大な支障を及ぼすおそれがあるため、非公開とする。