藤沢市情報セキュリティポリシー
対策基準
＜基本編＞

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

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対策基準』を策定する。

また、「サイバーセキュリティ基本法」第五条では、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ものとする。

本対策基準は、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、特別職非常勤職員及び臨時的任用職員等を含む。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対策基準＜基本編＞』
『藤沢市情報セキュリティポリシー対策基準＜詳細編＞』

２　対象範囲

（１）組織の範囲[1]

本対策基準が適用される行政機関は、市長部局、行政委員会、議会事務局、市民病院、教育委員会、消防局とする。

（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、藤沢市情報セキュリティポリシー対策基準＜詳細編＞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。

３　組織及び体制

（１）役割・責任

ア　最高情報セキュリティ責任者（ＣＩＳＯ）

（ア）藤沢市副市長事務分担規則第２条第１項第１号に規定する副市長が担う。

（イ）『藤沢市情報セキュリティポリシー』の対象範囲における全ての情報資産の

[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は、本対策基準の適用範囲から除く。

情報セキュリティの活動を統括する。
（ウ）『藤沢市情報セキュリティ緊急時対応計画』の承認を行う。
（エ）職員等及び関係する者に対し、『藤沢市情報セキュリティポリシー』についての啓発を行う。
（オ）情報セキュリティインシデントに対処するための体制（ＣＳＩＲＴ[2]）を整備し、役割を明確化する。
（カ）最高情報統括責任者（ＣＩＯ）を兼ねる。

イ　情報セキュリティ責任者
（ア）総務部長が担う。
（イ）最高情報セキュリティ責任者（ＣＩＳＯ）を補佐する。
（ウ）情報統括責任者を兼ねる。

ウ　情報ネットワーク・セキュリティ管理者
（ア）『藤沢市情報システム管理運営規程』第2条第10号に規定する情報システム調整主管課の長が担う。
（イ）最高情報セキュリティ責任者、情報セキュリティ責任者を補佐する。
（ウ）ネットワークに係る開発、設定の変更、運用、更新等の統括を行う。
（エ）ネットワークに係る情報セキュリティの維持及び向上を行う。
（オ）ネットワーク及び情報システムに関し、サーバ等ハードウェア及び配線等の構成情報を把握する。
（カ）ネットワーク及び情報システムに関し、ソフトウェアの配布状況、ライセンス等の情報を把握する。
（キ）情報システム・セキュリティ管理者及び情報システム・セキュリティ担当者に対して情報セキュリティに関する指導及び助言を行う。
（ク）情報資産を侵害される又は侵害のおそれがある場合には、最高情報セキュリティ責任者の指示に従い、必要かつ十分な全ての措置を行う。最高情報セキュリティ責任者が不在のときにあっては情報セキュリティ責任者の指示に従い、情報セキュリティ責任者が不在の際は自らの判断に基づき措置を行う。
（ケ）『藤沢市情報セキュリティ緊急時対応計画』の策定及び見直しを行う。
（コ）『藤沢市情報セキュリティポリシー』の遵守に関する意見の集約並びに職員等に対する研修、訓練、助言及び指示を行う。
（サ）情報ネットワーク・セキュリティ管理者が不在時に権限を代行する者は、情

[2] 情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、その問題を正確に把握・分析し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能とするための機能を有する体制。

報ネットワーク・セキュリティ管理者が指名し、最高情報セキュリティ責任者が認めた者でなくてはならない。

エ　情報システム・セキュリティ管理者（情報システム利用管理者）

（ア）『藤沢市情報システム管理運営規程』第 10 条第 2 項に規定する情報システム利用課の長が担う。

（イ）情報ネットワーク・セキュリティ管理者を補佐する。

（ウ）所管する情報システム及びネットワークに係る開発、設定の変更、運用等を行う。

（エ）所管する情報システムに係る情報セキュリティの維持及び向上を行う。

（オ）所管するネットワーク及び情報システムに関し、ソフトウェアの配布状況、ライセンス等の情報を把握し、管理する。また、当該情報に変更等が生じた場合は、速やかに当該変更等に係る箇所を修正するとともに、修正履歴を記録する。

（カ）課内職員等の育成方針を決定し、課内職員等への研修の受講・訓練への参加等を指示する。

オ　情報システム・セキュリティ担当者

（ア）『藤沢市情報システム管理運営規程』第 10 条第 3 項に規定するＩＴ推進リーダーが担う。

（イ）情報システム・セキュリティ管理者の職務を補助し、課内の情報化事業の効率的な推進及び情報セキュリティ向上を行う。

カ　職員等

（ア）『藤沢市情報セキュリティポリシー』に定めた事項を遵守する。

（イ）定められた研修・訓練を受講する。

（ウ）日常業務において、種類にかかわらず業務・プロジェクトの実行時に、情報セキュリティ対策を心がけ実行する。

キ　情報セキュリティ推進事務局（ＣＳＩＲＴの役割を含む）

（ア）『藤沢市情報システム管理運営規程』第 2 条第 10 号に規定する情報システム調整主管課の職員が担う。

（イ）情報ネットワーク・セキュリティ管理者に従い、全庁の情報セキュリティの推進に関する事務を行う。

（ウ）情報セキュリティ戦略の意思決定が行われた際は、その内容を関係各課等に提供する。

（エ）情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて報告を受けた場合には、その状況を確認し、最高情報セキュリティ責任者に報告を行う。

（オ）情報セキュリティインシデントとして認知した場合には、最高情報セキュリティ責任者へ報告するとともに、ＣＳＩＲＴとしての活動を開始する。

ク　ＣＳＩＲＴの設置・役割

（ア）最高情報セキュリティ責任者は、ＣＳＩＲＴを整備し、その役割を明確化するために、ＣＳＩＲＴに所属する職員を選任し、その中からＣＳＩＲＴ責任者を置く。また、ＣＳＩＲＴ内の業務統括及び外部との連携等を行う職員を定める。

（イ）情報セキュリティインシデントによる影響範囲や原因を明確化し、対策及び再発防止策を講じる。

（ウ）最高情報セキュリティ責任者による情報セキュリティインシデントに対する意思決定が行われた際には、その内容を関係各課等に提供する。

（エ）認知したインシデントの重要度や影響範囲等を勘案し、関係省庁、都道府県等へ報告する。また、必要に応じ報道機関への通知・公表対応を行わなければならない。

（オ）情報セキュリティに関して、関係機関[3]や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行う。

（２）情報セキュリティに関する委員会等

ア　情報セキュリティ委員会

（ア）情報セキュリティ委員会の役割

委員会は、定期的に年２回開催し、委員長が必要と認めた場合には臨時で開催することができる。会議の議事は、委員の総意により決するものとする。委員会は、情報セキュリティの維持及び改善を推進するために、次に掲げる事項に関し、全庁的に指示をする。

a　情報セキュリティに関する国や社会動向の把握及び対応
b　組織全体としての情報セキュリティ推進の明確化
c　情報セキュリティを強化するための推進策の承認
d　『藤沢市情報セキュリティポリシー』に関する見直しの実施
e　リスクマネジメント、組織の連携、指導

[3] 総務省、神奈川県、県内他市町村、内閣官房情報内閣サイバーセキュリティセンター（ＮＩＳＣ）、地方公共団体情報システム機構（Ｊ－ＬＩＳ）、情報処理推進機構（ＩＰＡ）、警察、委託事業者等を関係機関として想定している。各関係機関については藤沢市情報セキュリティポリシー対策基準＜詳細編＞別表２を参照。

f　重大な障害発生等の緊急対応

g　その他、本市の情報セキュリティに関する重要な事項の審議

（イ）情報セキュリティ委員会の構成

委員会は、委員長、副委員長、委員及び事務局をもって構成する。

また委員会は、議事に関する関係課の職員又は情報セキュリティに関して専門的知識を有する者の出席を求めることができる。

名称	構成員・担当者	役割の概要
委員長	藤沢市副市長事務分担規則第2条第1項第1号に規定する副市長	委員会を代表し、会務を総理し、会議の議長を務める
副委員長	藤沢市副市長事務分担規則第2条第1項第2号に規定する副市長、及び教育長	副委員長は委員長を補佐し、委員長に事故あるときはその職務を代理する
委　員	「藤沢市庁議規則」第2条第1号政策会議の委員(ただし、市長を除く)及びデジタル推進室長並びに委員長が必要と認める者	情報セキュリティの維持及び改善を推進する
事務局	情報セキュリティ推進事務局が担う。	委員会の運用支援を行う

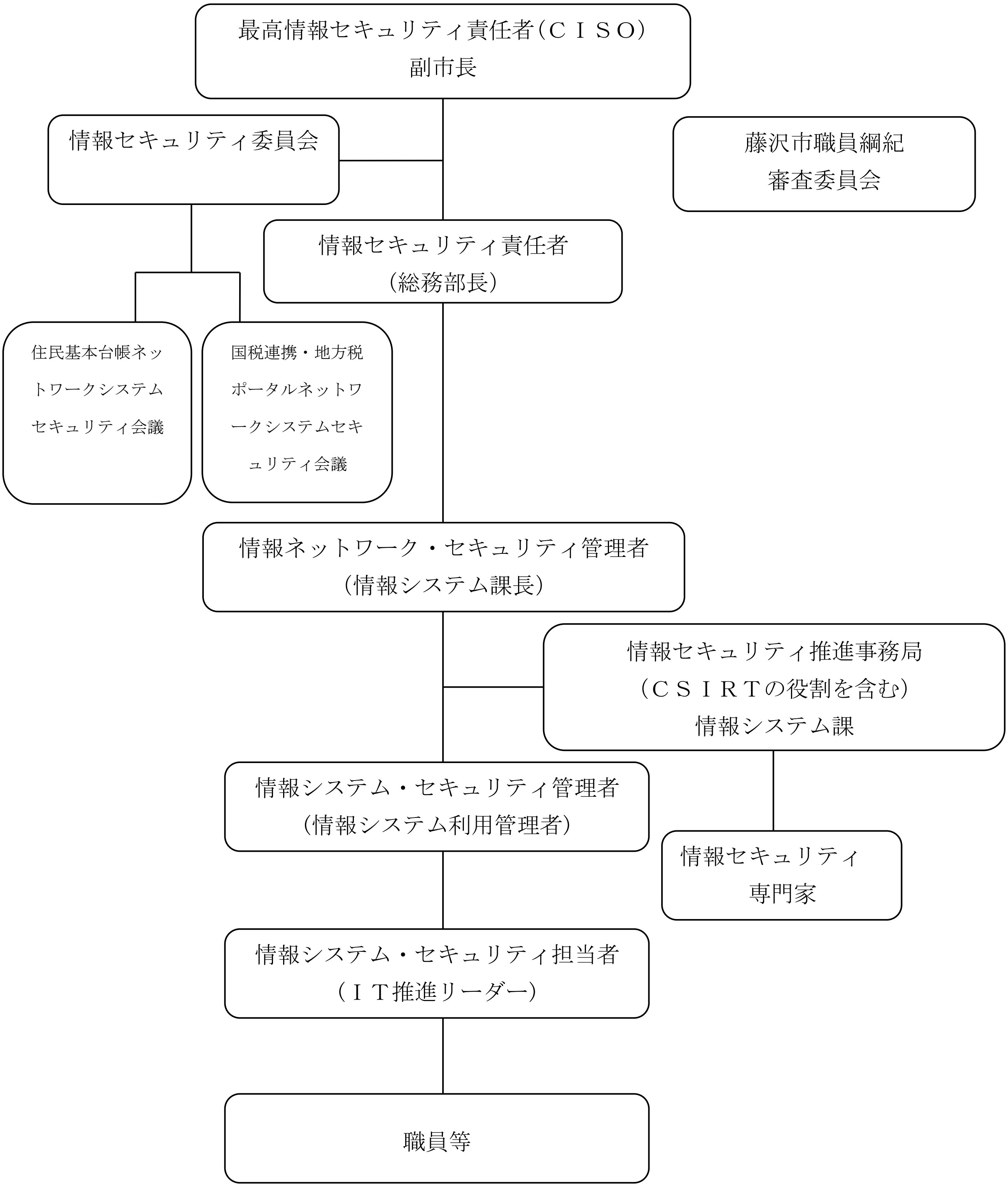
イ　住民基本台帳ネットワークシステムセキュリティ会議

『藤沢市住民基本台帳ネットワークシステムのセキュリティに関する規程』に基づき、同規程に定められた内容を審議する会議。

ウ　国税連携・地方税ポータルネットワークシステムセキュリティ会議

『藤沢市国税連携・地方税ポータルネットワークシステムのセキュリティに関する規程』に基づき、同規程に定められた内容を審議する会議。

■情報セキュリティ推進体制図



４　定義

本対策基準において、次の項番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）情報システム

コンピュータ機器、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）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。

（3）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。

（4）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。

（5）通信ネットワーク（以下、「ネットワーク」という。)

コンピュータ機器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。

（6）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。

５　情報資産への脅威

本対策基準を策定する上で、特に認識すべき脅威は、次のとおりとする。

（1）部外者による故意の不正アクセス、サービス不能攻撃、標的型攻撃等のサイバー攻撃や不正操作によるデータ又はプログラムの持出し、盗聴、改ざん及び消去、機器又は媒体の盗難、サービス妨害等。

（2）職員等、委託事業者による意図しない操作、故意の不正アクセス、不正操作によるデータ又はプログラムの持出し、盗聴、改ざん及び消去、機器又は媒体の盗難及び

許可されていない端末の接続によるデータの漏えいや情報システムの停止等。

（3）マルウェア、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）著作権法等の法令に反するソフトウェアの保持、複製、利用等。

（5）インターネット等の公共ネットワークにおける公的秩序に反する発言等による社会的信用の低下等。

６　情報セキュリティ対策

５で示した脅威から情報資産を保護するために、情報資産を『情報セキュリティポリシー対策基準＜詳細編＞』に基づき、重要度で分類し、重要度に応じ、人的・物理的・技術的の観点から情報資産への脅威の対策を講ずるものとする。

7　『藤沢市情報セキュリティポリシー』の例外措置

（1）情報ネットワーク・セキュリティ管理者及び情報システム・セキュリティ管理者は、情報セキュリティポリシーを遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合には、最高情報セキュリティ責任者に許可を得て、例外措置を取ることができる。

（2）情報ネットワーク・セキュリティ管理者及び情報システム・セキュリティ管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに最高情報セキュリティ責任者に報告しなければならない。

（3）最高情報セキュリティ責任者は、例外措置にかかる手続等の記録を適切に保管しなければならない。

８　『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対策基準＜基本編＞』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＜詳細編＞』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。

９　情報セキュリティポリシーの更新

　最高情報セキュリティ責任者は、現状の情報セキュリティ対策に新たに対策を講ずる必要が生じた場合、『藤沢市情報セキュリティポリシー』の実効性を評価し、必要な部分の見直しを行う。情報セキュリティ委員会の承認を得て、内容及び更新の時期についての決定を行う。