機	完	可
1	2	2

門真市情報セキュリティポリシー

情報セキュリティ基本方針

平成17年２月１日　制定

令和８年３月19日　改定

＜改定履歴＞

版数	制定／改定年月日	制定／改定	制定／改定内容
01	平成17年２月１日	新規制定	新規制定
02	令和２年４月１日	一部改定	情報セキュリティ基本方針の一部改定
03	令和４年12月１日	全部改定	情報セキュリティ基本方針の全部改定
04	令和７年４月１日	一部改定	情報セキュリティ基本方針の一部改定
05	令和８年３月19日	一部改定	情報セキュリティ基本方針の一部改定 情報セキュリティ基本方針の表紙・目次追加

目次

情報セキュリティ基本方針 1
1　目 的 1
2　情報セキュリティポリシーの構成と位置付け 1
3　定義 2
4　対象とする脅威 3
5　情報セキュリティ対策 3
6　情報セキュリティポリシーの適用範囲 5
7　情報セキュリティ組織体制 5
8　職員等の遵守義務 5
9　情報セキュリティ監査及び自己点検の実施 5
10　違反に対する措置 6
11　情報セキュリティポリシーの見直し 6
12　情報セキュリティ対策基準の策定 6
13　情報セキュリティ実施手順の策定 6

情報セキュリティ基本方針

１　目 的

本市は、法令等に基づき、市民の個人情報や事業者の経営情報等の重要な情報資産を多数保有し、他の組織主体が代替することのできない行政サービスを提供している。このため、本市が保有する情報資産を適切に保護し、市民生活及び地域の社会経済活動を情報セキュリティ上の脅威から守ることは、本市の重要な責務である。

情報セキュリティの確保には絶対的な安全が存在しないことを踏まえ、情報セキュリティに関する障害・事故やシステム上の欠陥の未然防止に努めるとともに、インシデント発生時にはその影響の最小化、迅速な復旧及び再発防止に向けた取組を継続的に実施する必要がある。

以上を踏まえ、本市が保有する情報資産の機密性、完全性及び可用性を確保するため、本市が実施する情報セキュリティ対策に関する基本的な事項をここに定める。

２　情報セキュリティポリシーの構成と位置付け

情報セキュリティポリシーとは、本市が所有する情報資産について、その機密性、完全性及び可用性を維持するための対策について､総合的､体系的に取りまとめたものである。

本市が所有する情報資産に係る業務については、情報セキュリティポリシーに即して実施することとし、当該業務に携わる職員等が遵守するよう浸透、普及、定着を図るものとする。

情報セキュリティポリシーは一定の普遍性を備えた部分（情報セキュリティ基本方針）と情報資産を取り巻く状況の変化に対応する部分（情報セキュリティ対策基準）から構成する。これらに基づき、ネットワーク及び情報システム等毎に具体的な情報セキュリティ対策の実施手順を策定することとする。（次表参照）

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的かつ基本的な方針。
	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ネットワーク及び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		ネットワーク及び情報システム等毎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。

３　定義

情報セキュリティポリシーにおける用語の意義は、次に定めるところによる。

⑴　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。

⑵　情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

⑶　情報資産

業務遂行の過程で生み出される価値のあるものを言い、以下の切り口で抽出する。

ア　直接的情報資産：データベース、データファイル、手順書、監査証跡など

イ　ソフトウェア資産：業務用ソフトウェア、システムソフトウェア、開発用ツールなど

ウ　物理的情報資産：コンピュータ装置、通信装置、電磁的記録媒体など

エ　サービス資産：ユーティリティ（空調、電源、照明）など

オ　人的資産：資格、技能、経験など

カ　無形資産：組織の評判、イメージなど

⑷　電磁的記録媒体

情報システムでデータ等を記録するための磁気ディスク､磁気テープ､フロッピーディスク等をいう。

⑸　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をいう。

⑹　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。

⑺　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。

⑻　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。

⑼　マイナンバー利用事務系（個人番号利用事務系）

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をいう。

⑽　LGWAN接続系

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。）

⑾　インターネット接続系

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。

⑿　通信経路の分割

LGWAN接続系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。

⒀　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。

４　対象とする脅威

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。

⑴　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

⑵　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、マネジメントの欠如、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

⑶　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

⑷　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

⑸　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

５　情報セキュリティ対策

上記４の脅威から情報資産を保護するため、以下の情報セキュリティ対策を講じる。

⑴　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。

⑵　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。

① マイナンバー利用事務系においては、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。

② LGWAN接続系においては、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。

③ 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、大阪府及び府内市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。

⑶ 物理的セキュリティ

サーバ室等、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。

⑷ 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。

⑸ 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。

⑹ 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、業務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。

⑺ 業務委託と外部サービス（クラウドサービス）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。

外部サービス（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。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソー

シャルメディアサービスごとの責任者を定める。

⑻　評価・見直し

情報セキュリティ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。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

６　情報セキュリティポリシーの適用範囲

⑴　機関の範囲

情報セキュリティポリシーが適用される機関は、市長の権限（水道事業及び公共下水道事業を含む。）に属する事務を所掌する部（情報セキュリティポリシーにおいて「市長部局」という。）、農業委員会、会計管理者、教育委員会事務局、選挙管理委員会、固定資産評価審査委員会、監査委員、公平委員会及び議会事務局とする。

⑵　情報資産の範囲

情報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　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

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

⑶　職員等の範囲

情報セキュリティポリシーが適用される職員等の範囲は、一般職常勤職員、一般職非常勤職員、臨時的任用職員及びこれらの職員に準じて情報資産を取り扱う特別職の職員（情報セキュリティポリシーにおいて「職員等」という。）とする。

７　情報セキュリティ組織体制

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ものとする。

８　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。

９　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。

10　違反に対する措置

情報セキュリティポリシー及びこれを受けて規定する情報セキュリティ実施手順に違反した者については、当該違反と過失の重大性に応じて、懲戒処分の対象とする。

11　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、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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

12　情報セキュリティ対策基準の策定

基本方針で定める情報セキュリティ対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

13　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。
なお、情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。