

富士吉田市 情報セキュリティ基本方針

平成15年10月制定

平成20年 6月改定

平成28年 2月改定

令和 2年 2月改定

富士吉田市

平成28年 2月

富士吉田市 情報セキュリティ宣言書

富士吉田市長

基本理念

本市が取り扱う情報資産には、市民の個人情報を始めとし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おり、これらの情報資産を人的脅威や災害、事故等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、継続的かつ安全・安定的な行政サービスの実施を確保するためにも必要不可欠である。このためには、本市が管理しているすべての情報資産が高度な安全性を有することが不可欠な前提条件となり、職員一人一人のセキュリティ意識の向上なしにはあり得ない。このため、本市の情報資産の機密性、完全性及び可用性を維持するための対策を整備するため、富士吉田市情報セキュリティポリシーを定めることとし、情報セキュリティの確保に最大限取り組むこととする。

第1編 情報セキュリティ基本方針

第1章 情報セキュリティの必要性

情報技術の進歩により、多くの業務が情報システムに依存するようになっており、今後は ICT を活用した各種手続のオンライン利用の本格化や情報システムの高度化等、電子自治体の進展が見込まれる。その中でコンピュータウィルスやシステムへの不正侵入など外部からの攻撃や、組織内部の者や委託事業者による人為的なミスでの情報漏洩や盗難が考えられ、情報に対してのリスクは高まる一方である。

これらの問題に有効かつ効果的に対応するために、情報セキュリティ対策に取り組むための全庁的な体制を確立すると共に、富士吉田市としての方針を明確にした情報セキュリティポリシーを策定し、これに基づく総合的・体系的な情報セキュリティ対策を図る必要がある。

第2章 情報セキュリティ基本方針

2.1 富士吉田市長による声明

情報セキュリティに対しての組織としての意思を統一するために、「情報セキュリティ宣言書」により富士吉田市長から基本理念を宣言する。

宣言書の目的は、富士吉田市としての情報セキュリティに対する取り組みの基本理念を定めること及び、情報セキュリティに対する富士吉田市長の支持を明確にすることを目的とする。

2.2 適用範囲

情報セキュリティポリシーを適用する範囲を以下の通りとし、業務で利用する情報とその情報を処理する情報システムとし、これらの情報を取り扱う全ての者（常勤、非常勤及び臨時の職員（以下「職員等」という。）及び外部委託事業者）を対象とする。

拠点	機関
市役所本庁舎	全ての所属機関
市役所東庁舎	全ての所属機関
市役所西別館	全ての所属機関
福祉ホール・子育て支援センター	ファミリーサポートセンターを除く全ての所属機関
保育園・マザーズホーム	全ての所属機関
環境美化センター	全ての所属機関
し尿処理施設	全ての所属機関
看護専門学校	全ての所属機関
学校給食センター	全ての所属機関

図書館	全ての所属機関
ふじさんミュージアム	全ての所属機関

情報資産の範囲
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
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。）
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

2.3 用語の定義

情報セキュリティポリシーで使用する用語は、付表1「用語の定義」に定める。

2.4 情報セキュリティポリシーの公開

富士吉田市の情報セキュリティに対する姿勢と一定の対策を実施していることを示す意味において、情報セキュリティポリシーは公開できるものとする。

しかし、実際の取り組み内容を具体的に記載した実施手順や情報資産台帳、リスク評価結果などセキュリティレベルや脆弱性の判断に活用できる文書については、情報セキュリティ対策の一環として公開しないものとする。

2.5 指針

情報セキュリティ事故の発生を防ぐとともに、発生してしまった場合の対策も定める。また、情報資産の変化や新たな脅威に対して継続的に対策を講じていくために、運営の体制を整えるとともに、定期的に見直しについても定めるものとする。

上記内容及び「情報セキュリティ基本方針」を受けて、管理すべき事項についての指針を以下の通り定める。

(1) 法律上及び契約上の要求事項への適合

関連法規を明確にして遵守する。及び、契約で取り交わした内容を遵守する。

(2) 職員等の遵守義務

全ての職員等は、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基本方針、情報セキュリティ対策基準及び情報セキュリティ実施手順を遵守する。

(3) 情報セキュリティ教育の実施

情報セキュリティポリシーを遵守する上で必要となる教育、訓練を実施する。

(4) 情報システム全体の強靱性の向上

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

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、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

(5) 悪意のあるソフトウェアの検出及び予防

コンピュータウィルス及び他の悪意のあるソフトウェアの検出の予防対策を実施する。

(6) 外部サービスの利用

外部委託する場合には、外部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、外部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。

約款による外部サービスを利用する場合には、利用にかか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。

(7) 緊急時対応計画

情報セキュリティインシデントが発生した場合又はその予兆があった場合に速やかに対応するため、緊急時対応計画を定める。

(8) 事業継続管理

災害など対策しえない事項による事象が発生した場合に、事業を継続していくための計画を策定する。

(9) 報告責任

情報セキュリティの事件・事故について報告を行うことを義務付ける。

(10) 違反に対する措置

情報セキュリティポリシーに違反した場合の措置としての懲戒処分を明確にし、適用する。

(11) 評価と見直し

情報セキュリティポリシーは普遍的な理念を除き、外部要因の変化や情報資産の変更を受けて定期的に見直しを行う。

また、ポリシーに従った運営が継続していること及び、情報セキュリティに対しての効果の状況を評価し改善を実施する。