松江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

令和８年４月　改定版

松江市

目次

松江市情報セキュリティ基本方針の新規制定／改定一覧

版数	制定／改定日	主な改正内容	承認者	備考
初版	平成 26 年 3 月 24 日	制定	市長	
第 2 版	平成 27 年 9 月 10 日	「地方公共団体における情報セキュリティポリシーに関するガイドライン」の H27.3 改定による変更	市長	CISO の設置 CSIRT の設置等
第 3 版	平成 28 年 9 月 9 日	情報セキュリティ副責任者の追加等	市長	
第 4 版	平成 30 年 9 月 27 日	H30.4 保健所設置による変更	市長	
第 5 版	平成 31 年 2 月 13 日	「地方公共団体における情報セキュリティポリシーに関するガイドライン」の H30.9 改定による変更	市長	パスワードの取扱いについてのみ
第 6 版	令和元年 9 月 30 日	「地方公共団体における情報セキュリティポリシーに関するガイドライン」の H30.9 改定による変更	市長	平成 31 年 2 月に改定した「パスワードの取扱い」以外の変更
第 7 版	令和 5 年 4 月 1 日	「地方公共団体における情報セキュリティポリシーに関するガイドライン」の R4.3 改定による変更	市長	
第8版	令和 7 年 4 月 1 日	「地方公共団体における情報セキュリティポリシーに関するガイドライン」の R6.10 改定による変更	市長	・クラウド対応 ・業務委託先 ・機密性再分類 ・NW 強化
第９版	令和８年４月１日	ガス事業譲渡に伴う変更	市長	ガス事業該当部分削除

1. 目的

本基本方針は、松江市（以下「本市」という。）が保有する情報資産の機密性、完全性及び可用性を維持するため、本市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

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。

(4) 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。

(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) 重要性

情報資産の取扱いの実効性を高めるため、機密性、完全性、可用性に応じて分類し、本市独自に使用している重要性指標（レベル）のことをいう。

(9) 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。

(10) LGWAN（Local Government Wide Area Network）

総合行政ネットワークのこと。総合行政ネットワークは地方公共団体の組織内ネット

ワークを相互に接続する行政専用の高度なセキュリティを備えたネットワークであり、インターネット網からは切り離されている。

（11）　LGWAN 接続系

LGWAN（Local Government Wide Area Network）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。）。

（12）　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。

（13）　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。

（14）　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。

（15）　クラウドサービス

クラウドサービスは機関等の外部の一般の者が、一般向けに情報システムの一部又は全部の機能を提供するサービスであり、クラウドサービスには IaaS（Infrastructure as a Service）や PaaS（Platform as a Service）だけではなく、SaaS（Software as a Service）等を含む。

IaaS は、システム開発やソフトウェアの稼働に必要な IT インフラをインターネット上のサービスとして提供を行うもの

PaaS はアプリケーション実行用の基盤機能をインターネット上のサービスとして提供を行うもの

SaaS は既に出来上がったソフトウェア機能をインターネット経由でサービスとして提供するもの

（16）　CSP（Cloud Service Provider）

クラウドサービスを提供する事業者のこと。代表的な CSP としてはアマゾン、グーグルやマイクロソフト等がある。なお、CSP は Cloud Solution Provider とされることもあるが、意味は同一。

（17）　ASP（Application Service Provider）

インターネットを経由してソフトウェアやソフトウェア稼働環境を提供するビジネスモデルや事業者のこと。

（18）　ISMAP（Information system Security Management and Assessment Program）

政府情報システムのためのセキュリティ評価制度の略称。この評価制度は、政府機関が利用するクラウドサービスなどの情報システムを対象に、その安全性を評価・認証する。本市では、ク

ラウドサービスは ISMAP に登録されたサービスを原則として使用する。なお、リスクの小さな業務・情報の処理に用いる SaaS を対象とした仕組みとして、ISMAP-LIU（Low-Impact Use）もある。

（19） ガバメントクラウド

国の行政機関（中央省庁・独立行政法人など）、及び地方自治体が共同で行政システムをクラウドサービスとして効率的に管理・運用するための「IT 基盤」。

（20） ソーシャルメディア

インターネットを利用して誰でも手軽に情報を発信し、相互のやりとりができる双方向のメディア。ソーシャルメディアには、LINE や X のような SNS（Social Networking Service）、電子掲示板、ブログ、投稿サイトなどさまざまなものが含まれる。

（21） 業務委託

本市の業務の一部又は全部について、契約をもって外部の者に実施させることをいう。ここでいう業務委託には、情報システムの運用に関する業務委託も含まれる。

3. 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。

（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） 実施機関の範囲

情報セキュリティポリシーが適用される実施機関は、市長事務部局、議会事務局、教育委員会事務局、選挙管理委員会事務局、その他の行政委員会事務局、消防本部、及び上下水道事業管理者、交通事業管理者、病院事業管理者とする。

（2） 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。

なお、独自の情報セキュリティポリシーを持つ組織については、松江市の内部情報系ネットワークに関係する情報資産以外に関しては、本ポリシーの適用対象外となる。

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
（本市が所有せずサービスとして利用しているものを含む）

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

正規職員、任期付任用職員、暫定再任用職員及び会計年度任用職員等の松江市職員（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と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 の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自治体機密性、自治体完全性、自治体可用性及びそれに応じて重要性を分類し、当該分類に基づき情報セキュリティ対策を実施する。

(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。

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、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（しまねセキュリティクラウド）を導入する。
ただし、自治体情報セキュリティクラウドによらない場合、個別に情報セキュリティ対策を実施する。

(4) 物理的セキュリティ

サーバ、情報システム室、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)　システム運用

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、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。

クラウド上の情報システムに関してはクラウドのマネージドサービスによって、高度なセキュリティの実現と、運用の自動化を図る。

(8)　業務委託と外部サービス(クラウドサービス)の利用

①　業務委託

業務委託する場合には、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。

②　外部サービスの利用

一般的な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。

③　クラウドサービスの利用(自治体機密性2以上の情報を取り扱う場合)

クラウド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

④　ソーシャルメディア

ソーシャルメディアを利用する場合には、ソーシャルメディアの運用手順を定め、ソーシャルメディア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ごとの責任者を定める。

(9)　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、情報セキュリティ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

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。

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、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。

9.　情報セキュリティ対策基準の策定

上記6、7及び8に規定する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。

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。