下呂市セキュリティポリシー

（基本方針）

下呂市

2026年3月

下呂市情報セキュリティ基本方針

1. 目的

本基本方針は、本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します。

2. 定義

本基本方針における主な用語の定義は以下のとおりです。

用語	定義
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。
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。
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。
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。
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。
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。
マイナンバー利用事務系	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）、戸籍事務及び総合行政情報システム（財務会計を除く）に関わる情報システム及びデータをいう。
LGWAN 接続系	しらさぎネット（ファイルサーバ等）、GIS システム等 LGWANに接続された情報システム及びデータをいう。
インターネット接続系	総合行政情報システム（財務会計）、GoogleWorkspace、SmoothFileCloud、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データをいう。
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。
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、添付ファイルの無害化等により、コンピュータウイルス等の不正プログラムの付着がないこと等、安全が確保された通信をいう。

特定個人情報	行政手続における特定の個人を識別するための番号の利用等に関する法律第2条第9項に規定する特定個人情報をいう。

3. 対象とする脅威

情報資産に対する脅威として、以下の要因を想定し、情報セキュリティ対策を実施します。

1. **意図的な要因による脅威**：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. **非意図的要因による脅威**：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、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. **災害等による脅威**：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. **人的及びインフラの障害による脅威**：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。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

本情報セキュリティポリシーの適用範囲は以下の通りです。

(1) 組織 情報セキュリティポリシーの適用範囲となる組織は、市長部局、教育委員会、選挙管理委員会、公平委員会、監査委員、農業委員会、固定資産評価審査委員会及び議会を含む市の機関とします。

(2) 情報資産 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です。

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、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。

5. 職員等の遵守義務

職員、会計年度任用職員及び臨時職員等（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

対象とする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ます。

(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体制は、**部長会議を中心に確立します**。

(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します。

(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ます。

1. **マイナンバー利用事務系**：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ぎます。
2. **LGWAN 接続系**：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します。両システム間で通信する場合には、**無害化通信**を実施します。
3. **インターネット接続系**：通信パケットの監視及びふるまい検知等不正通信の監視機能を強化し、感染時には端末を自動的に隔離し感染ログを残すなど、高度な情報セキュリティ対策を実施します。更に庁内ネットワークからインターネット接続口を集約した上で、岐阜県情報セキュリティクラウドの導入等を実施します。

(4) 物理的セキュリティ 電算室、通信回線及び職員のパソコン等の管理について、物理的な対策を講じます。

(5) 人的セキュリティ 情報セキュリティに関して、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ます。

(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ます。

(7) 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、外部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します。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します**。

(8) 業務委託と外部サービス（クラウドサービス）の利用

1. 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、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ます。
2. 約款による外部サービス（クラウドサービス）を利用する場合には、利用にかかる規定を整備し対策を講じます。
3. ソーシャルメディアサービスを利用する場合には、運用手順を定め、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ます。

(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ります。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います。

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、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ます。また、定期的（3年に1度）に**外部監査を実施**します。

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します。

9. 情報セキュリティ対策基準の策定

情報セキュリティ対策、情報セキュリティ監査、自己点検及び情報セキュリティポリシーの見直しを実施するために、具体的な遵守事項及び判断基準等を定める基準を策定します。

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定めるものとします。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**とします。