大和郡山市
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５年 11 月改正

目次

情報セキュリティ及び特定個人情報等の安全管理に関する基本方針

1　目的

情報セキュリティ及び特定個人情報等の安全管理に関する基本方針は、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並びに個人情報及び特定個人情報等の適正な取扱いについて基本的な事項を定めることを目的とする。

2　適用範囲

(1) 行政機関の範囲

本基本方針が適用される行政機関は、市長部局、教育委員会、議会事務局及び地方公営企業とする。

(2) 情報資産の範囲

本基本方針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

④ 特定個人情報等を含む文書、媒体、データ等

3　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ウトウェア）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。

(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) 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。

(5) 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。

(6) 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。

(7) 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。

(8) 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。）。

(9) 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。
(10) 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。
(11) 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　職員等の責務

　職員、非常勤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及び特定個人情報等の適正な取扱い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を遵守しなければならない。

５　情報セキュリティ対策

　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及び特定個人情報の適正な取扱いに関する対策を講じる。

(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し、特定個人情報等の適正な取扱いを確保するために全庁的な組織体制を確立する。
(2) 情報資産の分類と管理
　情報資産を、その重要度に応じて区分し、当該区分に応じた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の導入等を実施する。
(4) 物理的セキュリティ
　サーバ、マシン室、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) 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（再委託を含む）を行う際のセキュリティの確保及び安全管理措置等、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又は情報漏えい等の事案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。

(8) 業務委託と外部サービスの利用

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。

6　情報資産への脅威

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・設計ミス、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因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

7　情報セキュリティ対策基準及び特定個人情報等の保護に関する管理規程及び手順書の策定

情報セキュリティ対策又は特定個人情報等の適正な取扱いを行うために、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及び特定個人情報等の保護に関する管理規程を策定する。これらに基づき、各部局においては、各々の扱うネットワーク及び情報システム又は携わる業務において具体的な手順を定めた手順書を策定するものとする。

なお、手順書については、本市の情報セキュリティ対策の機器構成等に係る記述が含まれており、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。

8　情報セキュリティ監査及び自己点検の実施

この基本方針及び対策基準等の遵守状況を検証するため、定期的又は必要に応じて監査及び自己点検を実施する。

9　評価及び見直しの実施

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、情報セキュリティポリシーを見直す。