八尾市情報セキュリティ規則

令和８年２月27日改正

令和８年２月27日施行

（趣旨）

第１条　この規則は、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し、本市の情報資産の安全の確保及び保護を図るため、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ものとする。

（定義）

第２条　この規則において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（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）　情報セキュリティポリシー　この規則及び八尾市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）　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、地方税又は防災に関する事務）又は戸籍事務等に関する情報システム及びデータをいう。

（９）　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。

(10)　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す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。

(11)　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、安全性を確保することをいう。

(12)　無害化通信　インターネットメール本文のテキスト化、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ない等、安全が確保された通信をいう。

（適用範囲）

第３条　この規則の適用範囲は、次のとおりとする。

（１）　行政機関の範囲

市長部局、消防本部、市立病院、教育委員会事務局、市議会事務局、選挙管理委員会事務局、公平委員会事務局、監査事務局、農業委員会事務局及び固定資産評価審査委員会事務局とする。

（２）　処理事務の範囲

ア　市の機関が所掌する事務

イ　国、他の地方公共団体その他公共団体又は公共的団体の事務で、市民の福祉の増進に寄与するもの

（３）　情報資産の範囲（市立病院及び市立学校に係る独自のネットワーク及び情報システムに関するものは除く。）

ア　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

イ　ネットワーク及び情報システムで取り扱う情報

ウ　情報システムの仕様書及びネットワーク図等の関連文書

（対象とする脅威）

第４条　情報資産に対する脅威として、次の各号に掲げる脅威を想定し、情報セキュリティ対策を実施するものとする。

（１）　サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報資産の漏えい、破壊、改ざん又は消去、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、設計又は開発の不備、プログラム上の欠陥、操作又は設定の誤り、メンテナンスの不備、内部又は外部監査機能の不備、外部委託管理の不備、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、破壊又は消去等

（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）　大規模又は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提供サービスの障害による波及等

（職員等の責務）

第５条　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等を遵守しなければならない。

（情報セキュリティ対策）

第６条　第４条に規定する脅威から情報資産を保護するために、次の各号に掲げる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、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。

（３）　情報システム全体の強靭(じん)性の向上

情報セキュリティの強化を目的とし、業務の効率性及び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。

ア　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、情報システム端末等からの情報持ち出し不可設定、多要素認証の導入等を実施する。

イ　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の分割を行う。なお、両システム間で通信する必要が生じた場合には、無害化通信を実施する。

ウ　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（大阪府と府内市町村のインターネット接続口を集約した大阪版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

情報システムを設置する部屋又は施設等、通信回線及び職員等の情報システム端末等の管理について、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

情報システム端末等の管理、アクセス制御、不正プログラム対策及び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とともに、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、情報セキュリティ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

ア 業務委託を行う場合には委託事業者を、外部サービスを利用する場合にはサービス提供事業者を選定し、情報セキュリティ要件を明記した契約を締結するとともに、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。なお、外部サービスを利用する場合には、外部サービスの利用に関する規定を整備し、対策を講じる。

イ 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。

（9） 評価及び見直し

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。この場合において、情報セキュリティポリシーの見直しが必要と判断したときは、速やかに情報セキュリティポリシーの見直しを行うものとする。

（情報セキュリティ監査及び自己点検の実施）

第７条 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ものとする。

（情報セキュリティポリシーの見直し）

第８条 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、リスクを検討した上で、情報セキュリティポリシーを見直すものとする。

（情報セキュリティ対策基準の策定）

第９条　前３条に規定する対策等を実施するために、情報セキュリティ対策基準を策定するものとする。

（情報セキュリティ実施手順の策定）

第10条　情報セキュリティ対策基準に基づく情報セキュリティ対策を実施するため、情報セキュリティ実施手順を策定するものとする。

２　情報セキュリティ実施手順は、公にすることによりセキュリティ上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。

（その他）

第11条　この規則に定めるもののほか必要な事項は、政策企画部長が定める。