米原市情報セキュリティ基本方針

1　目的

米原市情報セキュリティ基本方針（以下「本基本方針」という。）は、本市が有する全ての情報資産の機密性、完全性およ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およびその構成機器（ハードウェアおよびソフトウェアを含む。）をいう。

（2）　情報システム

コンピュータ、ネットワークおよ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

物事の事情を人に伝えるものをいう。また、それを文字や図表、画像、音声、映像などを使って表現したものも含む。

（4）　情報セキュリティ

情報資産の機密性、完全性および可用性を確保、維持することをいう。

（5）　情報セキュリティポリシー

本基本方針および情報セキュリティ対策基準をいう。

（6）　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。

（7）　完全性

情報が破壊、改ざんまたは消去されていない状態を確保することをいう。

（8）　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。

（9）　通信

ネットワークを介してコンピュータ同士がデータや情報を送受信することをいう。

(10)　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、地方税もしくは防災に関する事務）または戸籍事務等に関わる情報システムおよび情報をいう。

(11)　LGWAN 接続系

総合行政ネットワーク（以下「LGWAN」という。）に接続された情報システムおよびその情報システムで取り扱う情報をいう（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、各種ウェブサイト管理システム等に係るインターネットに接続された情報システムおよびその情報システムで取り扱う情報をいう。

(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、対象者が利用するコンピュータ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こと等の安全が確保された通信をいう。

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、ウイルス対策、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仕様等の規定違反、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および業務の停止等

（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） 行政機関の範囲

本基本方針が適用される行政機関は、各部局、行政委員会、議会事務局およ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、情報システムおよびこれらに関する設備、電磁的記録媒体

② ネットワークおよ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およ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、非常勤職員、会計年度任用職員等（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およ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

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

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

市の保有する情報資産を機密性、完全性およ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行う。

（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。また、高度な情報セキュリティ対策として、滋賀県および本市を含む県内各市町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、情報システム室、通信回線およ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、十分な教育およ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。

（８） 業務委託と外部サービスの利用

業務委託を行う場合は、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は、利用に係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　情報セキュリティ監査および自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的または必要に応じて情報セキュリティ監査およ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

本基本方針の目的を達成するため、新たな情報システムの導入や新たな脅威の発生等、絶えず情報セキュリティを取り巻く環境の変化に対応しなくてはならない。そのため、情報セキュリティポリシーの運用状況を定期的に点検および監査し、その評価結果を踏まえ、情報セキュリティポリシーを適宜見直すものとする。

９　情報セキュリティ対策基準の策定

上記６、７および８に規定する対策等を実施するため、具体的な遵守事項およ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。

施行日

（１） 本基本方針は、平成20年２月１日から施行する。

（平成20年２月１日ＩＣＴ推進会議承認）

（２） 平成29年７月１日改定

（平成29年６月16日ＩＣＴ推進会議承認）

（３） 令和４年10月３日改定

（令和４年10月３日米原新時代デジタルトランスフォーメーション推進本部承認）