米原市情報セキュリティ基本方針

（目的）

第１条　この訓令は、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。

（定義）

第２条　この訓令において、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（文字、図表、画像、音声、映像等を使って表現したものを含む。）。

（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し、維持することをいう。

（５）　情報セキュリティポリシー　情報セキュリティ基本方針と情報セキュリティ対策基準をあわせたものをいう。

（６）　機密性　情報にアクセスすることを認められた者のみが、当該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情報（個人番号利用事務系情報）　個人番号利用事務（社会保障、地方税または防災に関する事務）、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 接続系情報　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情報を除く。）。

(12)　インターネット接続系情報　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のみ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。

(対象とする脅威)

第３条　情報セキュリティ対策の対象とする脅威は、次の各号に掲げるものとする。

（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、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、通信、水道供給の途絶等のインフラストラクチャーの障害からの波及等

(適用範囲)

第４条　この訓令を適用する行政機関は、市長（地方公営企業の管理者の権限を行う市長を含む。）、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および議会事務局とする。

２　この訓令が対象とする情報資産は、次の各号に掲げるとおりとする。

（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またはこれらを印刷した文書

（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

(職員の遵守義務)

第５条　職員は、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第 10 条に規定する情報セキュリティ実施手順を遵守し

なければならない。

(情報セキュリティ対策)

第６条　市は、第３条に規定する脅威から情報資産を保護するため、次に掲げる情報セキュリティ対策を講ずるものとする。

（１）　情報セキュリティ対策を推進する全庁的な組織体制の確立

（２）　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、当該分類に基づく情報セキュリティ対策

（３）　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、次に掲げる３段階の対策

ア　マイナンバー利用事務系情報においては、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の対策

イ　LGWAN 接続系情報においては、LGWAN と接続する業務用システムと、インターネット接続系情報の情報システムとの通信経路の分割。両システム間で通信する場合は、無害化通信の対策

ウ　インターネット接続系情報においては、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とし、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の対策

（４）　サーバ、情報システム室、通信回線および職員のパソコン等の管理における物理的セキュリティ対策

（５）　情報セキュリティに関し、職員の遵守事項を定め、十分な教育および啓発を行う等の人的セキュリティ対策

（６）　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セキュリティ対策

（７）　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

（８）　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の緊急時対応計画の策定

（９）　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するとともに、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いた措置

(10)　外部サービスを利用する場合は、利用に係る規定の整備

(11)　ソーシャルメディアサービスを利用する場合は、運用手順および発信できる情報の規定、利用するソーシャルメディアサービスごとの責任者の選任

（情報セキュリティ監査および自己点検の実施）

第７条　市は、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。

（情報セキュリティポリシーの見直し）

第８条　市は、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。

（情報セキュリティ対策基準の策定）

第９条　市は、第６条、第７条および前条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。

（情報セキュリティ実施手順の策定）

第 10 条　市は、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。

２　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。

付　則

（施行期日）

１　この訓令は、令和６年４月１日から施行する。

（米原市電子計算組織管理運営規程の廃止）

２　米原市電子計算組織管理運営規程（平成 17 年米原市訓令第１号）は、廃止する。