

## 米原市情報セキュリティ基本方針

令和6年3月27日

訓令第3号

### (目的)

第1条 この訓令は、本市が保有する情報資産の機密性、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) 情報セキュリティ 情報資産の機密性、完全性およ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 情報セキュリティ基本方針および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のみが、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、改ざんまた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データをいう。
- (9) 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データをいう（マイナンバー利用事務系を除く。）。
- (10) 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。

- (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 情報資産に対する脅威として、次の各号の脅威を想定し、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、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な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、市長部局（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) ネットワークおよび情報システムならびにこれらに関する設備および電磁的記録媒体
- (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

(職員の遵守義務)

第5条 職員（会計年度任用職員および臨時的任用職員等を含む。以下同じ。）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。

(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

ティ対策を講じるものとする。

(1) 組織体制

本市の情報資産の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を実施する。

(3) 情報システム全体の強靱性の向上

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、次に掲げる3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、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。

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を分割する。なお、両システム間で通信する場合は、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を実施する。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のパソコン等の管理における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、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（クラウドサービス）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（クラウドサービス）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。

#### (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し、運用改善を行、情報セキュリティの向上を図る。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う。

##### (情報セキュリティ監査および自己点検の実施)

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 情報セキュリティ監査および自己点検の結果、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およ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は、保有する情報および利用する情報システムに係る脅威の発生の可能性およ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 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。

2 情報セキュリティ対策基準は、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。

##### (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。

付 則 (令和8年米原市訓令第3号)

この訓令は、令和8年4月1日から施行する。