亀山市電子行政情報セキュリティポリシー
（電子行政情報セキュリティ基本方針）

（目次）

本基本方針は、地方自治法第 244 条の 6 に基づく「サイバーセキュリティを確保するための方針」として取り扱います。

亀山市長
亀山市教育委員会
亀山市選挙管理委員会
亀山市監査委員
亀山市公平委員会
亀山市農業委員会
亀山市固定資産評価審査委員会
亀山市水道事業　亀山市長
亀山市工業用水道事業 亀山市長
亀山市病院事業管理者

1. 目的

本基本方針は、本市が保有する電子行政情報資産（以下「情報資産」という。）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、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） 電子行政情報セキュリティポリシー

本基本方針及び電子行政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） 住民情報系

総合住民情報システム、総合保健福祉システム、戸籍システム、住民情報系ネットワーク等の主に住民情報を取り扱う事務で利用するためのネットワーク、システム、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） 内部情報系

統合型内部情報システム、内部情報ネットワーク、統合型地理情報システム、インターネットメール等の、主に内部事務等で利用するためのネットワーク、システム、データをいう。

（１１）業務委託

本基本方針においては、情報資産を取り扱う業務委託を指す。

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

本基本方針の適用範囲は次の各号に定めるものとする。

（1）行政機関の範囲

本基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局、消防本部・署、地方公営企業及び小中学校とする。

（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。ただし、個別にセキュリティポリシーを策定している情報資産については除く。

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電子行政情報

5. 職員等の遵守義務

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電子行政情報セキュリティポリシー及び電子行政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. 関係者の遵守義務

職員等以外で、委員、教職員、委託事業者等の本市の情報資産を管理、運用、利用する者（以下、「関係者」という。）は、情報資産の利用範囲に応じて、職員等の義務と同様の義務が生じ得るものとする。

7. 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

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、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住民情報系においては、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。

②LGWAN 接続系においては、LGWAN と接続する業務用システムと、内部情報系の情報システムとの通信経路を分割する。

③内部情報系においては、原則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、自治体情報セキュリティクラウド等の活用を原則とする。

（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、電子行政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、電子行政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、緊急時対応フローを整備する。

（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（クラウドサービス）を利用する場合には、利用環境に応じた必要な対策を講じる。

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。

（9） 評価・見直し

電子行政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電子行政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。電子行政情報セキュリティポリシーの見直しが必要な場合は、適宜電子行政情報セキュリティポリシーの見直しを行う。

8. 電子行政情報セキュリティ監査及び自己点検の実施

電子行政情報セキュリティポリシーの遵守状況を検証するため、必要に応じて電子行政情報セキュリティ監査及び自己点検を実施する。

9. 電子行政情報セキュリティポリシーの見直し

電子行政情報セキュリティ監査及び自己点検の結果、電子行政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、保有する電子行政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、リスクを検討したうえで、電子行政情報セキュリティポリシーを見直す。

10. 電子行政情報セキュリティ対策基準の策定

上記 7、8 及び 9 に規定する対策等を実施するために、必要に応じて具体的な遵守事項及び判断基準等を定める電子行政情報セキュリティ対策基準を策定する。

11. 電子行政情報セキュリティ実施手順の策定

電子行政情報セキュリティ対策基準に基づき、必要に応じて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電子行政情報セキュリティ実施手順を策定するものとする。

なお、電子行政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。