八幡浜市情報セキュリティ基本方針

令和８年２月１０日改定

１　目的

八幡浜市情報セキュリティ基本方針は、八幡浜市（以下「本市」という。）の情報資産の機密性、完全性及び可用性を維持するために必要な対策に関する基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

２　定義

（１）ネットワーク

コンピュータ等を相互に接続させるための通信網及びその構成機器（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（ハードウェア、ソフトウェア及び記録媒体）やネットワークで構成され、情報処理を行う仕組みをいう。

（３）情報資産

情報システム及び情報システムの開発と運用に係る全ての情報並びに情報システムで取り扱う全ての情報をいう。なお、情報資産には紙等の有体物に出力された情報も含むものとする。

（４）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。

（５）情報セキュリティポリシー

本基本方針及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、改ざん又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）外部委託者

業務委託先社員（システム開発職務を委託する外部委託事業者）等、契約に基づいて市の実施機関で作業する者の総称をいう。

（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、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

（11）総合行政ネットワーク（以下「LGWAN」という。）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。（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、ホームページ管理システム等に関わ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。

（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や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無い等、安全が確保された通信をいう。

３　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、市長部局、委員会及び委員、議会及び地方公営企業等とする。

（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、これらに関する設備、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及びネットワーク図等の情報システム関連文書

４　職員等及び外部委託者の遵守義務

職員等及び外部委託者は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たっては、情報セキュリティに関する法令等、情報セキュリティポリシー及び情報セキュリティ実施手順を遵守する義務を負うものとする。

５　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

６　情報セキュリティ対策

上記５で示した脅威から情報資産を保護するため、以下の対策を講ずるものとする。

（１）管理体制

適切な情報セキュリティ対策を推進・管理するための体制を確立するものとする。

（２）情報資産の分類とその管理

情報資産を機密性、完全性及び可用性に応じて分類し、その分類に基づき情報セキュリティ対策を行うものとする。

（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。

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。

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。

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、愛媛県及び県内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）人的セキュリティ対策

情報セキュリティに関して職員等が遵守すべき事項を定め、職員等及び外部委託者に内容を周知徹底する等、十分な教育及び啓発が講じられるように必要な人的対策を講ずる。

（５）物理的セキュリティ対策

情報システムを設置する情報システム室への不正な立入り、情報資産を損傷、盗難等から保護するために物理的対策を講ずる。

（６）技術的セキュリティ対策

情報資産を不正アクセスやコンピュータウィルス等から保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術的対策を講ずる。

（７）運用におけるセキュリティ対策

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

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。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。

７　情報セキュリティ監査及び自己点検の実施

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。

８　情報セキュリティポリシーの見直し

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、リスクを検討したうえで、情報セキュリティポリシーを見直す。

９　情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及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。