恵庭市情報セキュリティ基本方針

（目的）

第１条　この基本方針は、市が保有する情報資産の機密性、完全性及び可用性の確保並びに維持に関し必要な事項を定めることにより、当該情報資産の管理を徹底し、もって安全及び安定的な行政サービスの実施を確保することを目的とする。

（用語の定義）

第２条　この基本方針において、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)　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。

(2)　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。

(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確保及び維持をすることにより、当該情報資産を様々な脅威から保護し、危険及び不安のない完全な状態に維持することをいう。

(4)　情報セキュリティポリシー　この基本方針及び情報セキュリティ対策基準をいう。

(5)　機密性　情報資産を利用することを許された者のみが当該情報資産を利用することができる状態をいう。

(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　情報資産を利用することを許された者がいつでも当該情報資産を利用することができる状態をいう。

(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。

(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（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等、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。

(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だけ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。

(13)　行政機関　市の執行機関（市長、教育委員会、選挙管理委員会、監査委員会、公平委員会、農業委員会、消防長及び会計管理者をいう。）及び議会事務局とする。

(14)　情報資産　この基本方針が対象とする情報資産は、次に掲げるものとする。

ア　情報システム、ネットワーク並びにこれらに関する設備及び電磁的記録媒体

イ　情報システム及びネットワークで取り扱う情報（これらを印刷した文書を含む。）

ウ　情報システムの仕様書、ネットワーク図等のシステム関連文書

（対象とする脅威）

第３条　情報資産に対する脅威として、次に掲げる脅威を想定し、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及び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、改ざん及び消去、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、設計及び開発の不備、プログラム上の欠陥、操作及び設定ミス、メンテナンス不備、内部及び外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥並びに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)　大規模及び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

（適用範囲）

第４条　この基本方針を適用する範囲は、行政機関及び情報資産とする。

（情報セキュリティ対策）

第５条　市長は、情報資産を保護するため、次の各号に掲げる区分に応じ、当該各号に定める対策を講じるものとする。

(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構築する。

(2)　情報資産の分類及び管理　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分類し、当該分類に基づき情報セキュリティ対策を講じる。

(3)　情報システム全体の強靭性の向上　情報システム全体に対し、次の三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。

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には、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、都道府県及び市区町村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、職員、会計年度任用職員等（以下「職員等」という。）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な対策を講じる。

(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、外部委託を行う際のセキュリティ確保等の情報セキュリティポリシーの運用面の対策を講じ

る。この場合において、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切に対応するため、緊急時対応計画を策定するものとする。

（情報セキュリティ対策基準の策定）

第６条　市長は、前条に規定する対策を行うため、恵庭市情報セキュリティ対策基準（以下「対策基準」という。）を策定するものとする。

２　対策基準は、恵庭市情報公開条例（平成６年条例第１８号）第１０条第６号の規定により非公開とする。

（情報セキュリティ実施手順の策定）

第７条　市長は、第５条に規定する対策を行うに当たっての具体的な実施手順等を記載した恵庭市情報セキュリティ実施手順（以下「実施手順」という。）を策定するものとする。

２　実施手順は、恵庭市情報公開条例第１０条第６号の規定により非公開とする。

（情報資産の管理体制等）

第８条　市長は、情報セキュリティに関する対策を推進及び管理するための体制を講ずるとともに、情報資産の重要度に応じた対策を講ずるものとする。

（遵守義務）

第９条　職員等は、情報資産を利用するにあたっては、情報セキュリティの重要性を認識するとともに、情報セキュリティポリシー及び実施手順を遵守しなければならない。

（評価）

第１０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ものとする。

（見直し）

第１１条　市長は、情報セキュリティ監査及び自己点検の結果、情報セキュリティ対策の実施状況の評価及び当該情報セキュリティ対策の見直しが必要となった場合並びに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、情報セキュリティポリシーを見直すものとする。

（補則）

第１２条　この基本方針に定めるもののほか必要な事項は、別に定める。

附　則

この基本方針は、平成１５年１２月１９日から施行する。

この基本方針は、平成１７年　２月　３日から施行する。

この基本方針は、平成１８年　２月２０日から施行する。

この基本方針は、平成１８年　４月２５日から施行する。

この基本方針は、平成１９年　５月２８日から施行する。

この基本方針は、平成２３年　５月１日から施行する。

この基本方針は、平成２９年　２月８日から施行する。

この基本方針は、令和４年　４月１８日から施行する。