輪島市情報セキュリティポリシー基本方針

１．目的

本市が取り扱う情報資産には、市民の個人情報をはじめとする行政運営上重要な情報など、部外に漏えいすると極めて重大な結果を招く情報が多数含まれている。これらの情報資産を人的脅威や災害、事故から防御することは、市民の財産、プライバシー等を守るため、また、継続的かつ安全・安定的な行政サービスの実施を確保するためにも必要不可欠であり、高度な安全性を有し維持することで本市に対する市内外からの信頼や評価の向上にも寄与するものである。

本基本方針は、本市が保有する情報資産の機密性、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。

※ 情報セキュリティには、機密性、完全性、可用性の３つの主要な特性がある。

機密性：情報資産に対するアクセス権限を持つ者と持たない者を明確に区別し、アクセスを認められた者だけが、決められた範囲内で情報資産にアクセスできる状態を確保すること。

完全性：情報が処理される過程で、情報の欠落や重複、改ざん、破壊などの異常が発生しないよう、完全である状態を防護・確保すること。

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、アクセスできる状態を確保すること。

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及びその構成機器（ハードウェア及びソフトウェア）をいい、インターネット等外部ネットワークとの接続点から、課室等に設置されている末端のハブやサーバ室設置の情報システムへ接続する配線までをいう。

（２）　行政情報

本市の行政事務の執行に関わる情報で、かつ情報システムで取り扱うものをいう。

（３）　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。

（４）　課室端末等

課室等に設置されているパソコンやプリンタ、複合機等の情報機器端末及びこれらの機器を接続する末端のハブまでの配線をいう。

（５）　情報資産
情報システム及び行政情報をいう。

（６）　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し、維持することをいう。

（７）　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。

（８）　特定個人情報
「個人番号」を内容に含む個人情報の総称をいう。また、特定の保有個人情報を容易に検索することができるように体系的に構成した個人情報のデータベースについては、「特定個人情報ファイル」という。

（９）　マイナンバー利用事務系（基幹系）
個人番号利用事務（社会保障、地方税、災害対策に関する事務）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。

（10）　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）。

（11）　インターネット接続系
インターネットからのメール、ホームページ構築・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。
また、インターネット接続系の中でも、公民館及び図書館システムに関わる情報システム及びデータについては「公開系」という。

（12）　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。

（13）　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．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・重要情報の搾取・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、水道提供の途絶等のインフラの障害からの波及等

４．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、輪島市役所、門前総合支所及び出先機関で、情報資産に関係する設備を有する施設とする。小中学校における教員用・生徒用ネットワーク及びシステム、病院における医療活動に用いるネットワーク及びシステム、市民に利用してもらうことを目的に設置されているネットワーク及びシステムで、本基本方針の対象設備から物理的又は理論的に分離されているものは対象外とする。

また、本市が所掌する情報資産に関する業務に携わる全職員、非常勤職員及び会計年度任用職員（以下「職員等」という。）を、本基本方針の対象とする。

（２）　情報資産の範囲

本基本方針が対象とする情報資産は、以下を含む本市が保有する全ての資産とする。

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システム関連文書

④　行政文書（紙媒体）

５．職員等の遵守義務

職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行にあたって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しなければならない。

６．情報セキュリティ対策

前記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ものとする。

（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、完全性及び可用性を踏まえ、被害を受けた場合　　に想定される影響の大きさをもとに分類し、当該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。

①　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。

②　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。

③　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、石川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。ただし、ここで示すインターネット接続系には、公開系は含まないものとする。

（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ものとする。また、情報資産への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は、必要に応じて適宜見直しを行う。

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

前記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。