Ⅱ　情報セキュリティ基本方針

1　趣旨

情報セキュリティ基本方針は、多賀城市情報セキュリティに関する規程に基づき、情報セキュリティに関する統一的かつ基本的な取組姿勢を定めるものとする。

2　定義

このポリシーにおいて、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) 職員

多賀城市個人情報の保護に関する法律施行条例（令和５年多賀城市条例第１号）第２条第２項に規定する実施機関等の職員（多賀城市立学校の設置に関する条例（昭和３９年多賀城市条例第１０号）第２条に規定する小学校及び中学校に勤務する職員を除く。）をいう。

(2) 委託事業者

情報資産の取扱いを委託された事業者（公の施設の管理を行う指定管理者及び市営住宅の管理を行う管理代行者を含む。）をいう。

(3) 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。

(4) 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。）。

(5) 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。

(6) 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。

(7) 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、以下の事項を想定する。

(1) 不正アクセス、ウイルス攻撃、サービス不能攻撃その他のサイバー攻撃、部外者の侵入、内部不正その他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、詐取等

(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、情報システムの設計・開発の不備、プログラムの欠陥、操作・設定ミス及びメンテナンスの不備、委託管理の不備、機器故障その他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、火災その他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、通信の途絶その他の提供サービスの障害からの波及等

4　適用範囲

ポリシーの適用範囲は、次のとおりとする。

(1) 情報資産の範囲

ポリシーが適用される情報資産は、全ての情報資産とする。

(2) 対象者の範囲

ポリシーが適用される対象者は、職員及び会計年度任用職員（以下「職員等」という。）とする。

5　情報セキュリティ対策

３の脅威から情報資産を保護するために、次の情報セキュリティ対策を講じる。

(1) 情報セキュリティ管理体制の構築

情報セキュリティ対策を推進するため、情報セキュリティに係る責任及び権限を明確にした管理体制を構築する。

(2) 情報資産の分類と管理

情報資産を性格や内容によって分類し、当該分類に基づき管理を行う。

(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。

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対策

サーバ室その他の管理が必要な区域の入退室及び情報システムの管理について、物理的対策を講じる。

(5) 人的セキュリティ対策

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、ポリシーの周知徹底を図るため、十分な教育及び啓発を行う等の人的対策を講じる。

(6) 技術的セキュリティ対策

コンピュータ等の管理、アクセス制御、コンピュータウイルス対策、不正プログラム対策、不正アクセス対策その他の技術的対策を講じる。

(7) 運用

情報システムの監視、ポリシーの遵守状況の確認、セキュリティ侵害が発生した場合の対応に係る計画の策定その他のポリシーの運用面の対策を講じる。

(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

ポリシーの遵守状況を検証するため、定期的に、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。この場合において、ポリシーの見直しが必要な場合は、適宜見直しを行う。

6　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。

7　情報セキュリティ対策基準の策定

５及び６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た情報セキュリティ対策基準を策定する。

8　情報セキュリティ実施手順の策定

情報システムを所管する部等又は課等は、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情報システムごとに策定する。

なお、情報セキュリティ対策基準及び情報セキュリティ実施手順は、公開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。

9　多賀城市行政経営会議との関係

情報セキュリティの運用及び管理を統一的な視点で行うため、情報セキュリティに関する重要な事項は、多賀城市行政経営会議に諮るものとする。