多賀城市情報セキュリティポリシー

・情報セキュリティ基本方針

平成２９年１２月

多賀城市

Ⅰ　はじめに

本市では、効率的で質の高い行政サービスを提供するため、各種業務の情報システム化を進めてきており、多くの情報を電子的な情報として管理している。

また、行政サービスのオンライン化に向けた取組により、情報の電子的な管理と情報通信ネットワークを活用した情報システムの導入は、今後さらに進展するものと予想される。

情報の電子的な管理と業務の情報システム化の進展は、事務処理の迅速化及び効率化をもたらす反面、容易に大量の情報を記録し、又は複製し、持ち出すことが可能となるほか、瞬時に破壊し、又は消去することができるなど、セキュリティ面での脆弱さも併せ持っている。

本市の情報資産には、市民の個人情報や行政運営上重要な情報など、外部に漏えいした場合に極めて重大な結果を招くおそれのあるものが多く存在する。これらの情報資産を人的脅威、災害その他の様々な脅威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、行政事務の安定的な運営のために必要不可欠であり、ひいては、本市の行政に対する市民からの信頼の維持向上に結びつくものである。

このため、多賀城市情報セキュリティに関する規程（平成２６年３月１８日訓令第５号。以下「規程」という。）第３条の規定に基づき、ここに多賀城市情報セキュリティポリシー（以下「ポリシー」という。）を策定するものである。

なお、ポリシーは、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示す「情報セキュリティ基本方針」と、情報セキュリティを実施するための基本的な遵守事項、判断基準等を示す「情報セキュリティ対策基準」により構成する。

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

多賀城市個人情報保護条例（平成９年多賀城市条例第１０号）第２条第２号に規定する実施機関の職員（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) 外部委託事業者

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　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、外部委託管理の不備、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) 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、職員及び外部委託事業者（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) 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。

(4) 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。

(5) 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、外部ネットワークからの不正アクセス対策その他の技術的対策を講じる。

(6) 運用

情報システムの監視、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その他のポリシーの運用面の対策を講じる。

6　情報セキュリティ監査及び自己点検の実施

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する。

7　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、情報セキュリティに係る新たな対策が必要なことが判明した場合その他ポリシーの見直しが必要な場合は、ポリシーの見直しを実施する。

8　情報セキュリティ対策基準の策定

５、６及び７に規定する対策等を実施するために、具体的な遵守事項、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。

9　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。

１０　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。