花巻市情報セキュリティ基本方針

平成 30 年３月 26 日副市長決裁

改正

令和２年３月 30 日副市長決裁

令和５年５月 22 日副市長決裁

花巻市情報セキュリティ基本方針

花巻市情報セキュリティ基本方針（平成 18 年８月 30 日制定）の全部を改正する。

1. 目的

この花巻市情報セキュリティ基本方針（以下「基本方針」という。）は、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、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。

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、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、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。

(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

この基本方針及び花巻市情報セキュリティ対策基準をいう。

(5) 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。

(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。

(8)　職員等

市の情報資産を取り扱う職員（非常勤職員、会計年度任用職員及び臨時的任用職員を含む。）をいう。

(9)　実施機関

市長部局、教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会、消防及び議会をいう。

(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) 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。）。

(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. 対象とする脅威

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ものとする。

(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、重要情報の詐取盗難及び内部不正等

(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、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、破壊及び消去等

(3) 地震、落雷、火災、水害、停電等の災害若しくは事故による情報資産の破壊、消去、サービス又は業務の停止等

4. 適用範囲

(1) 対象範囲

この基本方針が適用される範囲は、実施機関の全ての職員等とする。

(2) 情報資産の範囲

この基本方針において対象とする情報資産の範囲は、次に掲げるとおりとする。

①ネットワーク、情報システム及び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（情報を印刷した文書を含む。）

③ネットワーク図及び情報システムの仕様書等のシステム関連文書

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、業務の遂行に当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

市の情報資産を保護するため、次に掲げる情報セキュリティ対策を実施するものとする。

(1) 組織体制

市は、保有する情報資産について、統一的な情報セキュリティ対策を推進及び管理するための全庁的な体制を整備するものとする。

(2) 情報資産の分類と管理

市が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実施するものとする。

(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。

②LGWAN 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、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

ネットワーク、情報システム、サーバ室及び職員等が使用するパソコン等の管理について、物理的セキュリティ対策を講じる。

(5) 人的セキュリティ

情報セキュリティに関して職員等が遵守すべき事項を定め、職員等に対する研修の実施、情報システムの運用方法及び委託事業者に対する指導監査等の人的セキュリティ対策を講じる。

(6) 技術的セキュリティ

情報システム及び職員等が使用するパソコン等の管理、情報システム等

のアクセス制御、不正プログラム対策及び不正アクセス対策等の技術的セキュリティ対策を講じる。

(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、情報セキュリティインシデント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。

外部サービスを利用する場合には、利用に係る規程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

情報セキュリティ対策の運用において、情報セキュリティポリシーの遵守状況を定期的に確認するものとする。

7.　情報セキュリティ監査及び自己点検の実施

情報セキュリティが維持されていることを検証するため、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行うものとする。

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を評価した結果、情報セキュリティポリシーの見直しが必要になった場合又は情報システム等の変更や新たな脅威等情報セキュリティを取り巻く状況が変化した場合は、情報セキュリティポリシーを見直すものとする。

9.　情報セキュリティ対策基準の策定

この基本方針に基づき情報セキュリティ対策を実施するため、具体的な遵守事項及び判断基準等を定める花巻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。

対策基準は、公にすることにより市の行財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. 情報セキュリティ実施手順の策定

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、具体的な手順を定める花巻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。

実施手順は、公にすることにより市の行財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。

附　則

この基本方針は、平成 30 年４月１日から施行する。

附　則（令和２年３月 30 日副市長決裁）

この基本方針は、令和２年４月１日から施行する。

附　則（令和５年５月 22 日副市長決裁）

この基本方針は、令和５年６月１日から施行する。