米原市情報セキュリティ基本方針

１ 目的

米原市情報セキュリティ基本方針（以下、「基本方針」という。）は、本市行政サービスに関する全ての情報資産の機密性、完全性および可用性を維持することにより、米原市個人情報保護条例、米原市行政手続における特定の個人を識別するための番号の利用等に関する法律に基づく個人番号の利用に関する条例および米原市情報公開条例の実態的保障を確立し、市民の権利を保障し、市民が安心して自己情報を提供できる情報基盤を構築および維持管理するため、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) 米原市行政情報ネットワーク

各部局、各行政委員会および各教育機関（情報系ネットワークおよび機器設置場所）を相互に接続するための通信網（以下、「ネットワーク」という。）をいう。ただし、教育機関における教育用ネットワークおよびシステムは除く。

(2) 情報システム

ネットワークを利用する構成機器・ソフトウェアおよび電磁的記録媒体（以下、「記録媒体」という。）で構成され、これら全体で業務処理を行う仕組みをいう。

(3) 情報資産

ネットワークおよび情報システムの開発、運用、保守等で取り扱う全ての情報ならびに情報を管理運用する仕組み(以下「情報システム」という。)をいう。

(4) 情報

文書、図面、写真、図書、それらが表示された画面および記録媒体に記録したデータならびに業務遂行上必要な事実、概念、指示をいう。

(5) 情報セキュリティ

情報資産の機密性、完全性および可用性を確保、維持することにより、情報資産を様々な脅威から保護し、危険のない、誤りのない状態で、認可された利用者が必要とするときに利用可能な状態に維持することをもって市民の権利を保障することをいう。

(6) 情報セキュリティポリシー

基本方針および情報セキュリティ対策基準をいう。

(7) 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。

(8) 完全性

情報が破壊、改ざんまたは消去されていない状態を確保することをいう。

(9) 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。

(10) データファイル

情報システムに電磁的に記録されたものおよび記録媒体に記録されたものをいう。

(11) プログラムファイル

パッケージプログラムおよび市独自の開発プログラムのソースプログラム、ロードモジュール、各種定義体およびその実行に必要な指示パラメータ等をいう。

(12) 通信

ネットワークを介してコンピュータ同士がデータや情報を送受信することをいう。

(13) 記録媒体

電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。）の媒体をいう。

3 対象とする脅威

(1) 無権限者による故意の不正アクセスまたは不正操作による情報資産の持出し・破壊・盗聴・改ざん・消去、機器および記録媒体の盗難ならびに否認

(2) 正当権限者による意図しない操作、故意の不正アクセス、目的外利用または不正操作による情報資産の持出し・破壊・盗聴・改ざん・消去、機器および記録媒体の盗難ならびに否認

(3) 人為的なミス（機器の設定誤り、プログラム誤り、操作・処理誤り、データ・機器の取扱い誤り等）による情報漏えい、データの損壊、不正データの提供等

(4) コンピュータウイルス、スパイウェアをはじめとする悪意のあるソフトウェア等による情報資産への侵害行為

(5) Dos攻撃、Webページの改ざん、メールサーバへの不正ソフトウェアや大量データの送信など、ネットワーク経由の不正アクセス、不正操作によるサービス妨害、データ漏えい、データの改ざん等

(6) セキュリティレベルの低いネットワークとの接続に伴う接続先からのデータ漏えい、接続先からの不正アクセス、不正ソフトウェア等による情報資産への侵害行為

(7) 情報の外部提供（提供・業務委託等）による提供先からの情報漏えい等

(8) 取得制限、利用制限、保有制限、提供制限および電子的結合の処理制限に違反する管理者権限の行使

(9) 地震、落雷、火災、水害等の災害ならびに事故、故障等によるサービスおよび業務の停止

(10) 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

(11) 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
(12) その他情報資産へのあらゆる侵害行為

4 適用範囲

(1) 行政機関の範囲

基本方針が適用される行政機関は各部局、行政委員会、議会事務局とする。

(2) 適用対象者

行政事務に関与する全ての者（職員、嘱託職員、臨時職員および委託業務従事者）を対象とする。

(3) 情報資産の範囲

基本方針が対象とする情報資産は、次のとおりとする。

① ネットワーク、情報システムおよびこれらに関する設備、電磁的記録媒体
② ネットワークおよ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およびネットワーク図等のシステム関連文書

5 職員等の遵守義務

職員、非常勤職員および臨時職員（以下「職員等」という。）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およ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

上記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

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。

(2) 情報資産の分類と管理

市の保有する情報資産を機密性、完全性およ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行う。

(3) 物理的セキュリティ

サーバ等、情報システム室等、通信回線等およ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。

(4) 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、十分な教育および啓発を行う等の人的な対策を講じる。

(5) 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

の技術的対策を講じる。

(6) 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、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切に対応するため、緊急時対応計画を策定する。

7 情報セキュリティ監査および自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的または必要に応じて情報セキュリティ監査およ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

本基本方針の目的を達成するためには、新たな情報システムの導入や新たな脅威の発生等、絶えず情報セキュリティを取り巻く環境の変化に対応しなくてはならない。そのため、セキュリティポリシーの運用状況を定期的に点検および監査し、その評価結果を踏まえ、情報セキュリティポリシーを適宜見直すものとする。

9 情報セキュリティ対策基準の策定

上記６、７および８に規定する対策等を実施するために、具体的な遵守事項およ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等の策定

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および対策標準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。

11 市民の権利の保障

(1) 自己情報コントロール権の保障

基本方針は、個人情報保護条例を理念とし、個人情報の取得目的に適合した情報の利用環境構築と運用により、市民の自己情報コントロール権を保障する。

(2) 知る権利の保障

基本方針は、情報公開条例を理念とし、市民に情報セキュリティ対策に関する方針を正確、的確に公開し、市民の知る権利を保障する。

施行日

(1) 本基本方針は、平成20年２月１日から施行する。

（平成20年２月１日ＩＣＴ推進会議承認）

(2) 平成29年７月１日改定

（平成29年６月16日ＩＣＴ推進会議承認）