情報セキュリティ基本方針

1　目的

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。

2　定義

(1) ネットワーク

ハードウェア（電子計算機、端末機、通信装置、通信回線、周辺機器及び電磁的記録媒体等から構成されるもの）を相互に接続するための通信網及びその仕組みをいう。

(2) 情報システム

ハードウェア、ソフトウェア（コンピュータを動作させる手順及び命令をコンピュータが理解できる形式で記述したもの）及びネットワークにより業務処理を行う仕組みをいう。

(3) 情報資産

情報資産は、次のとおりとする。

ア　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

イ　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。）

ウ　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) 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。

(5) 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。

(6) 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。

(7) 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。

(8) 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。

(9) 部等

三田市の組織及びその事務管理に関する条例（平成 16 年三田市条例第 5 号）第 3 条に規定する部、三田市教育委員会事務局の組織及びその事務管理に関する規則（平成 16 年三田市教育委員会規則第 1 号。以下「教育委員会組織及び事務管理規則」という。）第 2 条の表に掲げる部、市民病院事務局、及び消防本部をいう。

(10) 室等

三田市の組織及びその事務管理に関する規則（平成 16 年三田市規則第 9 号）第 2 条の表及び教育委員会組織及び事務管理規則第 2 条の表に掲げる室及びこれらに準ずる組織をいう。

(11) 課等

三田市の組織及びその事務管理に関する規則（平成 16 年三田市規則第 9 号）第 2 条の表及び教育委員会組織及び事務管理規則第 2 条の表に掲げる課等、市民病院事務局及び消防本部に設置された課、会計課、議会事務局、各行政委員会事務局（教育委員会事務局を除く。）及びこれらに準ずる組織をいう。

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、ウィルス攻撃、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、外部委託管理の不備、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、水道供給の途絶等のインフラの障害からの波及等

4　適用範囲

情報セキュリティポリシー基本方針は、部等、室等及び課等が保有する情報資産並びに当該情報資産に接する全ての職員等について適用する。

5　職員等の義務

本市の情報資産に関する業務に携わる全ての職員等は、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

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ずる。

(1) 情報セキュリティ管理体制

本市の情報資産について、情報セキュリティ対策を推進、管理するための全庁的な組織体制を確立する。

(2) 情報の分類

情報資産である情報（以下「情報」という。）をその重要度に応じて分類し、それに応じた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、物理的な対策を講ずる。

(4) 人的セキュリティ

情報セキュリティに関する権限及び責任を定め、全ての職員等に情報セキュリティポリシーの内

容を周知徹底するため、教育及び啓発を行う等の人的な対策を講ずる。

(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ずる。

(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ずるものとする。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評価及び見直し

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に定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために適宜、情報セキュリティポリシーの見直しを実施する。

９　情報セキュリティ対策基準の策定

本市の情報資産について、上記６、７及び８の情報セキュリティ対策を講ずるに当たっては、職員等及び外部委託事業者が遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

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を確実に実施していくためには、個々の情報資産に関する対策の手順を具体的に定めておく必要がある。そのため、各課等の長はその所管する情報資産に対する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のある情報資産であることから非公開とする。