中央市 情報セキュリティポリシー

中央市

0.2 版

目次

情報セキュリティポリシー
基本方針

第１章　情報セキュリティ基本方針

１　目的

この基本方針は、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、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

(3)　個人情報

個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と照合することができ、それにより特定の個人を識別することができることとなるものを含む。)をいう。

(4)　特定個人情報

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第２条に規定する、個人番号をその内容に含む個人情報ファイルをいう。

(5) 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し、さらに真正性･責任追跡性･否認防止及び信頼性を維持管理することをいう。

(6) 情報セキュリティポリシー

この基本方針及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、改ざん又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)真正性

利用者の本人確認を保証、プロセス及びシステムの処理が仕様どおりであることの保証等、情報又は資源が本物であることをいう。

(11)責任追跡性

情報にアクセスすることを認められた者（アクセス権保持者）のアクセスの記録（アクセスログ）を基にした利用者の行動追跡ができることをいう。

(12) 否認防止

事後に事実を否認できないよう証拠を維持することをいう。

(13) 信頼性

信頼ある計画に基づく動作や結果が整合していることをいう。

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) サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃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、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提供サービスの障害からの波及等

４　適用範囲

(1) 行政機関の範囲

この基本方針が適用される行政機関は、市長部局、議会事務局、選挙管理委員会、教育委員会、農業委員会、監査委員、公平委員会、固定資産評価審査委員会及び地方公営企業とする。３庁舎等の具体的な範囲は、対策基準及び実施手順にて示すこととする。

(2) 情報資産の範囲

この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(これらを印刷した文書を含む。)
③ 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

５　職員等の遵守義務

職員、嘱託職員、臨時職員及び再任用職員(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行う。

(3) 物理的セキュリティ

サーバ等、電算室（サーバ室）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

な教育及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の見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

９　情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及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 特定個人情報の適正な取り扱い

職員等は、特定個人情報を適正に取扱うため、中央市情報セキュリティポリシーに定めるもののほか、関係法令及びガイドラインを遵守しなければならない。