八尾市監査委員情報セキュリティ基本方針

1　目的

この基本方針は、八尾市監査委員（以下「監査委員」という。）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、監査委員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

⑴　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及びその構成機器（ハードウェア及びソフトウェア）をいう。

⑵　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。

⑶　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。

⑷　機密性

情報にアクセスすることを認められた者だけが、情報にアクセスすることができる状態を確保することをいう。

⑸　完全性

情報が破壊され、改ざんされ、又は消去されていない状態を確保することをいう。

⑹　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、情報にアクセスすることができる状態を確保することをいう。

3　対象とする脅威

情報資産に対する脅威として、次に掲げるものを想定し、情報セキュリティ対策を実施する。

⑴　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、内部不正等

⑵　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、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

⑶　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

⑷　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

⑸　電力供給の途絶、通信の断絶、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

⑴　行政機関の範囲

この基本方針が適用される行政機関は、監査委員とする。

⑵　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。

ア　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

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

5　遵守義務

職員は、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この基本方針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に掲げる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ずる。

⑴　組織体制

監査委員の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

⑵　情報資産の分類と管理

監査委員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実施する。

⑶　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、情報セキュリティ対策を講ずる。

⑷　物理的セキュリティ

通信回線及び職員のパソコン等の管理について、物理的な対策を講ずる。

⑸　人的セキュリティ

情報セキュリティに関し、職員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ずる。

⑹　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。

⑺　運用

情報システムの監視、この基本方針の遵守状況の確認、業務委託を行う際のセキュリティ確保など、この基本方針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正に対応するための危機管理対策を講ずる。

⑻　業務委託と外部サービス（クラウドサービス）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ずる。

外部サービス（クラウドサービス）を利用する場合には、その利用に係る規定を整備し、対策を講ずる。

ソーシャルメディアサービスを利用する場合には、その運用手順を定め、ソーシャルメディアサービスを利用して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。

⑼　評価・見直し

この基本指針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し、運用改善を行い、情報セキュリティの向上を図る。この基本指針の見直しが必要な場合は、適宜、その見直しを行う。

7　情報セキュリティ監査及び自己点検の実施

この基本方針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　基本方針の見直し

情報セキュリティ監査及び自己点検の結果、この基本方針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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、この基本方針を見直す。