羽島市監査委員及び監査委員事務局・公平委員会・固定資産評価審査委員会・選挙管理委員会・農業委員会サイバーセキュリティを確保するための基本方針

令和８年３月３０日　策定

≪目次≫

サイバーセキュリティを確保するための基本方針

1. 目的

本基本方針は、地方自治法第 244 条の 6 第 1 項の規定に基づき、羽島市監査委員及び監査委員事務局、公平委員会、固定資産評価審査委員会、選挙管理委員会、農業委員会（以下、「委員会」という。）が利用する情報システム（ガバメントクラウドを含む）及びネットワークの安全かつ適正な管理を図るため、情報セキュリティを確保するための基本方針を定める。これにより、住民の権利利益を保護し、行政サービスの継続性を維持す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）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。

（5）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。

（6）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。

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

（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、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

（1）行政機関の範囲

本基本方針が適用される行政機関は、羽島市監査委員及び監査委員事務局、公平委員会、固定資産評価審査委員会、選挙管理委員会、農業委員会とする。

（2）情報資産の範囲

本基本方針が対象とする情報資産は、委員会が取り扱う次のものとする。

ただし、市長部局が設置し、かつ管理運用する情報資産を取扱う場合は、羽島市情報セキュリティポリシーを遵守するものとする。

①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

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. 委員及び委員会事務局職員の遵守義務

委員、委員会事務局職員は、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本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 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

委員会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。

（2）情報資産の分類と管理

委員会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。

（3）物理的セキュリティ

委員等のパソコン等の管理について、物理的対策を講じる。

（4）人的セキュリティ

情報セキュリティに関し、委員会が遵守すべき事項を定め委員等に啓発を行う。

（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）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セキュリティ対策が確保されていることを確認する。

外部サービス（クラウドサービス）を利用する場合には、セキュリティ対策が確保されていることを確認する。

（7）評価・見直し

本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。本基本方針の見直しが必要な場合は、適宜見直しを行う。

7. 情報セキュリティ監査及び自己点検の実施

本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. 本基本方針の見直し

情報セキュリティ監査及び自己点検の結果、本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、本基本方針を見直す。