第２章 情報セキュリティ基本方針

２．１．目的

基本方針は、本市が保有する情報資産の機密性、完全性およ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。

２．２．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、その構成機器（ハードウェアおよびソフトウェア）をいう。

⑵ 情報システム

コンピュータ、サーバ、ネットワークおよび記録媒体で構成され、情報処理を行う仕組みをいう。

⑶ 個人番号利用事務系ネットワーク

庁内ネットワークのうち、個人番号利用事務および戸籍事務等に供する情報システム専用のネットワークセグメントをいう。

⑷ 内部情報系ネットワーク

庁内ネットワークのうち、ＬＧＷＡＮに接続でき、インターネット環境を分離したネットワークセグメントをいう。

⑸ インターネット接続系ネットワーク

庁内ネットワークのうち､インターネットメール､ＷＥＢ閲覧等に利用するため、インターネットに直接接続できるネットワークセグメントをいう。

⑹ 秋田市ネットワークシステム

個人番号利用事務系ネットワーク、内部情報系ネットワーク、インターネット接続系ネットワークおよびこれらのいずれかと接続するすべての情報システムをいう。

⑺ 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維持することをいう。

⑻ 情報セキュリティポリシー

本基本方針および情報セキュリティ対策基準をいう。

⑼ 機密性

情報にアクセス（データの書き込み又は読み出し）することを正当に認められた

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。

(10) 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。

(11) 可用性

情報にアクセスすることが正当に認められた者が、必要なとき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。

(12) 基幹業務システム

住民生活に直接関係する事務に係る情報システムであって、相互に連携が必要なシステムをいう。

(13) 通信経路の分割

内部情報系ネットワークとインターネット接続系ネットワークの両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

(14) 無害化通信

インターネットメール添付ファイルの pdf 化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

２．３．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) 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則違反、プログラム上の欠陥、委託管理の不備、操作ミス、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、破棄等

(3) 地震、落雷、火災、豪雨、豪雪等の災害によるサービスおよび業務の停止等

(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

２．４．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、市長事務部局、行政委員会、議会事務局、

消防および上下水道局とする。

(2) 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

ア　秋田市ネットワークシステムおよびこれに関するソフトウェア、ハードウェア等

イ　秋田市ネットワーク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　秋田市ネットワーク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

２．５．職員等の遵守義務

職員および会計年度任用職員等（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、各々の業務の遂行にあたって情報セキュリティポリシーおよびその業務に係る情報セキュリティ実施手順を遵守しなければならない。

２．６．情報セキュリティ対策

２．３．の脅威から情報資産を保護するために、本市は、以下の情報セキュリティ対策を講じる。

(1) 組織体制

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

本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) 情報システム全体の強靭性の向上

情報システム全体に対し、次の三段階の対策を講じる。

ア　個人番号利用事務系ネットワークにおいては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

イ　内部情報系ネットワークにおいては、ＬＧＷＡＮと接続する業務用システムと、インターネット接続系ネットワークとの通信経路の分割を実施する。なお、両システム間で通信する場合には、無害化通信を実施する。

ウ　インターネット接続系ネットワークにおいては、不正通信の監視機能の強化等

の高度な情報セキュリティ対策を実施する。

(4) 物理的セキュリティ

コンピュータを設置した部屋、汎用コンピュータ、サーバ、通信回線およびネットワークに接続されたコンピュータの管理について、物理的な対策を講じる。

(5) 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。

(6) 技術的セキュリティ

コンピュータ等の管理、アクセス制限、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。

(7) 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。

(8) 外部委託と外部サービスの利用

外部委託する場合には、外部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、外部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じる。

外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

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

(9) 評価・見直し

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および自己点検を実施する。情報セキュリティポリシーの見直しが必要な場合は、情報セキュリティポリシーの見直しを行う。

２．７．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、本市は、定期的又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。

２．８．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および自己点検の結果、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およ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、本市は、情報セキュリティポリシーの見直しを行う。

２．９．情報セキュリティ対策基準の策定

２．６.、２．７．および２．８．に規定する対策等を実施するために、本市は、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。

なお、情報セキュリティ対策基準は、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恐れがあることから原則非公開とする。

２．10．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、本市は、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本市の行政運営に重大な支障を及ぼす恐れがあることから非公開とする。