矢吹町セキュリティポリシー（第１章　情報セキュリティ基本方針）

目次

第１章　情報セキュリティ基本方針

1.1　目的

本基本方針は、本町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、本町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。

1.2　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（ハードウエア及びソフトウエア）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）　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）　矢吹町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。

（５）　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。

（６）　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。

（７）　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。

（８）　マイナンバー利用事務系

個人番号利用事務（社会保障・地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

（９）　ＬＧＷＡＮ接続系

人事給与、財務会計及び文書管理等ＬＧＷＡＮに接続された情報システム及びその情報システムで取り扱うデータをいう。

(10)　インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(11)　通信経路の分割

ＬＧＷＡＮ接続系とインターネット接続系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。

(12)　無害化通信

インターネットメール本文のテキスト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。

(13)　テレワーク

情報通信技術（ＩＣＴ）の利用により時間・空間を有効に活用する多様な就労・作業形態をいう。

(14)　情報セキュリティインシデント

情報流出、フィッシングサイト、不正侵入、ウイルス感染、Ｗｅｂサイト改ざん、その他ネットワークを介した攻撃など、情報および制御システムの運用におけるセキュリティ上の問題として捉えられる事象をいう。

(15)　ＢＹＯＤ

私用パソコン、タブレット端末及びスマートフォン等の、支給端末以外の端末を用いて業務を行う働き方をいう。

1.3　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・消去等
（２） 情報資産の無断持ち出し、無許可ソフトウエアの使用等の規定違反、プログラム上の欠陥、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
（６） テレワーク実施時の支給端末並びに支給端末以外の端末（ＢＹＯＤ）の盗難・失・売却時の情報漏えい等

1.4 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、内部課室、行政委員会及び議会事務局とする。

（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。

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

1.5 職員等の遵守義務

職員、会計年度任用職員、再任用職員、任期付職員、その他町長が必要と認める者（以下「職員等」という。）並びに部外委託者は、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矢吹町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。

1.6 情報セキュリティ対策

上記1.3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

本町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

本町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） 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。

① マイナンバー利用事務系においては、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。
② ＬＧＷＡＮ接続系においては、ＬＧＷＡＮと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。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。
③ インターネット接続系においては、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。高度な情報セキュリティ対策として、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（４） 物理的セキュリティ

情報システムを設置する施設への不正な立入り、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

（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、十分な教育及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。

（７） 運用

情報システムの監視、矢吹町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、矢吹町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。

（８） 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。

1.7 情報セキュリティ監査及び自己点検の実施

矢吹町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。

1.8 矢吹町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、矢吹町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、矢吹町セキュリティポリシーを見直す。

1.9 情報セキュリティ対策基準の策定

上記1.6、1.7及び1.8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。