甘楽町情報セキュリティポリシー

（概要版）

甘楽町情報セキュリティ委員会

目次

情報セキュリティ基本方針

１　目的

甘楽町の情報資産の機密性、完全性及び可用性を維持するための対策を整備することを目的として、甘楽町情報セキュリティポリシーを定め、情報セキュリティの確保に最大限取り組むものである。

このうち情報セキュリティ基本方針は、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、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ものとする。

２　用語の定義

（１）ネットワーク

コンピュータ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）で構成され、情報処理を行う仕組みをいう。

（２）情報システム

町の各種コンピュータ、ネットワーク及び電磁的記録媒体で構成され、処理を行う仕組みをいう。

（３）情報資産

情報資産とは次の①から③をいう。

①ネットワーク、情報システム及びそれらの開発と運用に係るすべての設備、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すべての情報、及びそれらを印刷した文書

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

（４）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。

（５）情報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。

（６）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。

（７）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。

（８）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。

（９）職員等

地方公務員法で規定された職員、会計年度任用職員及び、臨時的任用職員で、町が管理する情報資産を職務で利用する者の総称をいう。

（１０）外部委託者

職務委託先社員（地方自治法（昭和 22 年法律第 67 号）第 244 条の２第３項に規定する指定管理者を含む。）等、契約に基づいて町の機関で作業する者の総称をいう。

（１１）部外者

職員等及び外部委託者以外の町の情報資産に接することが認められていない者の総称をいう。

（１２）不正アクセス

不正アクセス行為の禁止等に関する法律（平成１１年法律第 128 号）第３条第２項に規定する不正アクセス行為その他の不正な手段により利用者以外の者が行うアクセス又は利用者が行う権限外のアクセスをいう。

（１３）マイナンバー利用事務系（個人番号利用事務系）

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。

（１４）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。

（１５）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。

（１６）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うえで、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。

（１７）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、コンピュータウィ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。

３　情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、町が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の頂点に位置するものである。

４　情報セキュリティポリシーの対象範囲

情報セキュリティポリシーの適用範囲は、次の各号に定めるものとする。

（１）適用組織

町の内部部局、教育委員会、行政委員会、議会事務局及び地方公営企業とする。

（２）適用資産

前号に定める組織において行政事務を処理するために取り扱う情報資産とする。ただし、小中学校においては、本庁とネットワーク接続された範囲のみを適用対象とする。

（３）適用対象者

前号に定める情報資産に接する職員等とする。

５　職員等の義務

町が所掌する情報資産に関する業務に携わる職員等は、情報セキュリティの重要性について共通の認識をもつとともに業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負うものとする。

６　情報資産への脅威

情報資産に対する脅威として、次の各号の脅威を想定し、情報セキュリティ対策を実施する。

（１）部外者の侵入による情報資産の破壊、盗難、不正アクセス、コンピュータウィルス攻撃、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、盗聴、改ざん、消去、重要情報の搾取、内部不正等

（２）職員等及び外部委託者による情報資産の無断持ち出し・誤操作、設計・開発の不備、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、アクセスのための認証情報又はパスワードの不適切管理、規定外の端末接続や無許可ソフトウェアの使用等の規定違反、プログラム上の欠陥、搬送中の事故等による情報資産の盗難、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、火災等の災害並びに事故、故障等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、通信の途絶等のインフラの障害からの波及等

7　情報セキュリティ対策

町の情報資産を第６に示した脅威から保護するために、次の各号の情報セキュリティ対策を講じるものとする。

（１）組織体制

町の情報資産について、情報セキュリティ対策を推進・管理するための全庁的な体制を確立するものとする。

（２）情報資産の分類と管理

町が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）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うえで、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うえで、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対策

情報資産及びそれらの設置場所等の管理について、物理的な対策を講じる。

（５）人的セキュリティ対策

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対策

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、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、情報セキュリティポリシーの運用面の対策等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正に対応するため、緊急時対応計画を策定する。

（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書を締結し、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。

約款によ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。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。

8　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。

9　情報セキュリティポリシーの見直しの実施

情報セキュリティ監査及び自己点検の結果等により、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、リスクを検討したうえで、情報セキュリティポリシーの見直しを実施する。

１０　情報セキュリティ対策基準の策定

町の様々な情報資産について、第７から第９まで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。

１１　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。

１２　情報セキュリティポリシーの情報公開

情報セキュリティ対策基準及び情報セキュリティ実施手順は、公開することにより町の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。