朝日町情報セキュリティポリシー
情報セキュリティ基本方針

令和６年４月（改定）

山形県朝日町

目　次

１　目　的

情報セキュリティ基本方針（以下「基本方針」という。）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。

２　用語の定義

（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）情報セキュリティポリシー

組織における情報資産の情報セキュリティ対策について、総合的及び体系的に取りまとめたものであり、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

権限のない者への重要な情報の漏えいを防止することをいう。

（６）完全性

情報の改ざん、破壊による被害を防止することをいう。

（７）可用性

権限のある者に対し、必要なときに情報の利用を可能とすることをいう。

（８）マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税又は防災に関する事務等）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）総合行政ネットワーク（LGWAN）接続系

総合行政ネットワーク（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（マイナンバー利用事務系を除く。）。

(10）インターネット接続系

インターネット、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

総合行政ネットワーク（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）情報資産

情報システムで取り扱う情報で、開発と運用に係る全ての情報をいう。

（14）委託業者

朝日町が情報システム開発、情報システム運用、データ入力、警備及び清掃等の目的で「３　適用範囲」に示す情報資産に接する業務を委託した者をいう。

３　適用範囲

（１）行政機関の範囲

基本方針が適用される行政機関の範囲は、町長部局、議会事務局、教育委員会部局、選挙管理委員会事務局、監査事務局及び農業委員会事務局とする。

（２）情報資産の範囲

基本方針が対象とする情報資産は、次のとおりである。

ア　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）及びこれらに関する設備

イ　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情報システム関連文書

（３）対象者

適用される情報資産に接する組織の職員（会計年度任用職員等を含む。以下「職員等」という）とする。

４　職員等及び委託事業者の責務

職員等及び委託事業者は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たっては情報セキュリティポリシー及び実施手順を遵守しなければならない。

５　対象とする脅威

情報資産への脅威として、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）人による脅威（故意）

不正アクセスやウイルス攻撃等のサイバー攻撃、機器の盗難、不正な操作や持ち出し等の故意による情報資産の漏えい・破壊・改ざん・消去等

（２）人による脅威（過失）

情報資産の管理不備、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、操作・設定ミス、委託管理の不備等の過失による情報資産の漏えい・破壊・破壊消去等

（３）災害による脅威

地震、落雷、火災、水害等の災害によるサービス及び業務の停止、情報資産の消失等

（４）必要資産の不足、故障等による脅威

電力及び通信等の途絶、交通機能の麻痺や大規模・広範囲にわたる疾病のまん延による要員の不足、機器の故障等によるサービス及び業務の停止、情報システム運用の機能不全等

６　情報セキュリティ管理体制

本町の情報資産について、情報セキュリティ対策を推進・管理するため、情報セキュリティ管理体制を確保する。

７　情報セキュリティ対策

前記５で示した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ものとする。

（１）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　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。

イ　総合行政ネットワーク（LGWAN）接続系においては、総合行政ネットワーク（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。

ウ　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、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（２）物理的セキュリティ

コンピュータ、ネットワーク等の管理について、物理的な対策を講じる。

（３）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。

（４）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な対策を講じる。

（５）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、業務委託を行う際の情報セキュリティの確保等の運用面の対策を講じる。

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、定期的また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

情報セキュリティ監査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、情報セキュリティポリシーを見直す。

10　情報セキュリティ対策基準の策定

情報セキュリティ対策を実施するために、具体的な遵守事項及び判断基準等を定めた「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サイバー攻撃を受けるリスクがあることから、非公開とする。

11　情報セキュリティ実施手順の策定

対策基準に基づき、情報セキュリティに関する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業務担当課において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町の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。