越前町情報セキュリティ基本方針

令和８年３月

１　目的

本基本方針は、情報セキュリティポリシーの体系及び本町における情報セキュリティ対策の基本的な方針を示すことをその目的としている。

２　用語の定義

（１）　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

（２）　情報資産

情報システム及びネットワークで取り扱われる全ての情報（電磁的に記録されている情報及び出力した媒体を含む）

（３）　情報システム

電子計算機及び記録媒体で構成され、情報を処理するための仕組み

（４）　ネットワーク

情報システムを相互に接続するための通信網、構成機器及び記憶媒体で構成され、処理を行う仕組み

（５）　装置

情報システムに関わる装置

（６）　端末

職員等が、個別に情報システムの情報を処理する装置

（７）　職員等

常勤、非常勤等の雇用形態を問わず、本町に勤務する者（以下「職員等」という。）

（８）　第三者

職員等に該当しない者

（９）　情報処理施設

装置（ホスト、サーバ等）が設置されている建物

（１０）　コンピュータルーム

重要な情報資産を保護する目的で設置された、高いセキュリティが保たれた部屋

（１１）　情報セキュリティインシデント

情報資産の正常な運営や維持が、セキュリティ上の問題や不正な攻撃等によって妨げられる事象

（１２）　脅威

情報資産の価値を失わせる事象（不正アクセス等の意図的脅威、入力ミス等の偶発的脅威、災害等の環境的脅威等）

（１３）　機密性

許可された者のみが、情報にアクセスできることを確実にすること

（１４）　完全性

情報及び処理方法が、正確であること及び完全であることを保護すること

（１５）　可用性

許可された者が、必要なときに情報にアクセスできることを確実にすること

（１６）　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）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。

（１７）　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。

（１８）　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。

（１９）　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。

（２０）　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。

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、ウィルス攻撃、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、外部委託管理の不備、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　情報セキュリティポリシーの文書体系

情報セキュリティポリシー及び関連する規則の文書体系を下記に定め、各々を明文化するものとする。

（１）　情報セキュリティポリシー

①　情報セキュリティ基本方針

本町の情報セキュリティ対策に関する基本的な方針。（本基本方針）

② 情報セキュリティ対策基準

情報セキュリティ基本方針に基づき情報セキュリティ対策を実施する上での統一的な対策基準。

（２） 関連規則

① 情報セキュリティ実施手順

情報セキュリティ対策を実施するため、用途、対象者、情報システム等に分類して、適宜定める情報セキュリティ対策基準に基づいた具体的な実施手順書。

② 緊急時対応計画

情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するための具体的な対処手順書

5 適用範囲

（１） 本基本方針が適用される行政機関は、内部部局、教育委員会、議会事務局及びその他関係機関とする。

（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

6 情報セキュリティの推進体制

情報セキュリティポリシーに基づき、情報セキュリティ対策を推進するため、副町長を最高責任者とする組織横断的なセキュリティ推進体制を確立するものとする。

7 職員等の遵守義務

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持ち、業務の遂行に当たって情報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。

８　情報資産の取扱い

情報資産を適正に取り扱うため、情報資産の分類を行い、分類レベルに応じた管理方法及び管理責任者を定めるものとする。

９　情報セキュリティ対策の実施

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

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３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　サーバ等、情報システム室等、通信回

線等及び職員等のパソコン等の管理について、物理的な対策を講じる。

（５）　人的セキュリティ　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、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、情報資産に対するセキュリティ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）　業務委託と外部サービス（クラウドサービス）の利用　業務委託する場合には、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（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。また、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、適宜情報セキュリティポリシーの見直しを行う。

１０　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。

１１　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、情報セキュリティポリシーを見直す。

１２　情報セキュリティ対策基準の策定

上記９、１０及び１１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。

１３　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。

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。