礼文町情報セキュリティポリシー基本方針

令和８年４月１日

北海道礼文町

目次

はじめに 3

基本的な考え方 3

１．目的 4

２．定義 4

３．対象とする脅威 5

４．適用範囲 5

５．職員等の遵守義務 5

６．情報セキュリティ対策 6

７．情報セキュリティ監査及び自己点検の実施 7

８．情報セキュリティポリシーの見直し 7

９．情報セキュリティ対策基準の策定 7

10．情報セキュリティ実施手順の策定 7

はじめに

　礼文町は、町民の皆さまからお預かりする情報及び行政運営に必要な情報を重要な資産として位置付ける。
　これらの情報を適切に保護することは、町民の信頼を確保し、行政サービスを安定して提供する上で不可欠である。
　本基本方針は、情報セキュリティに関する町としての基本的な考え方を示すものであり、特定の技術や運用方法を固定するものではない。
　本方針で用いる用語や区分は、制度改正、技術動向、運用実態の変化等を踏まえ、必要に応じて見直すものとする。

基本的な考え方

　町は、情報セキュリティを一部の部署だけの課題とは捉えず、組織全体で取り組むべき重要な責務として位置付け、継続的に対策を推進する。

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。

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

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。

（９） LGWAN 系

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（マイナンバー系を除く。）。

（10） インターネット系（北海道セキュリティクラウド）

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 系とインターネット系（北海道セキュリティクラウド）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。

３．対象とする脅威

（１） 不正アクセス、ウイルス攻撃、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、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

（６） 離島特性に起因する交通・物流の制約（フェリー・航空路の欠航等）による、機器・部材の搬入遅延、外部事業者による保守対応の遅延、復旧対応の長期化等

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、内部部局、行政委員会（教育委員会を含む。）、議会事務局、消防本部及び地方公営企業とする。

（２） 情報資産の範囲

本基本方針が対象とする情報資産は、町が保有し、又は管理するすべての情報資産（文書、図面、写真、音声、映像、電子データその他媒体のいかんを問わない。）及び情報システムとし、外部事業者が提供するサービスその他庁外で運用されるサービス上で取り扱う情報を含む。

① ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

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

５．職員等の遵守義務

職員、会計年度任用職員（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、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。

６．情報セキュリティ対策

（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

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、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 系においては、LGWAN と接続する業務用システムと、インターネット系（北海道セキュリティクラウド）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 インターネット系（北海道セキュリティクラウド）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。

（４） 物理的セキュリティ

サーバ室、通信回線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、業務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（クラウドサービス等）の利用

業務委託を行う場合には、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。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、定期的に情報セキュリティ監査及び自己点検を実施するとともに、必要に応じてこれらを追加で実施し、運用改善を行い、情報セキュリティの向上を図る。

また、情報セキュリティポリシーについては、定期的に見直しを行うほか、必要が生じた場合には適宜見直しを行う。

７．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、情報セキュリティ監査及び自己点検を定期的に実施するとともに、必要に応じてこれらを追加で実施する。

８．情報セキュリティポリシーの見直し

情報セキュリティポリシーは、次の各号のいずれかに該当する場合には、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並びに発生時の損失等を分析し、リスクを検討した上で、見直す。

（１） 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

（２） 情報セキュリティに関する状況の変化に対応するため、新たに対策が必要となった場合

９．情報セキュリティ対策基準の策定

上記６、７及び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。

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、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。