平内町情報セキュリティ基本方針

令和８年３月

平内町

目次

平内町情報セキュリティ基本方針

平内町情報セキュリティ基本方針

１．方針の目的

本基本方針は、当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、当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．情報セキュリティポリシーの構成と位置づけ

情報セキュリティポリシーは、当町が保有する情報資産の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、情報セキュリティに対する取組姿勢を示す「情報セキュリティ基本方針」と、この情報セキュリティ基本方針に定められた情報セキュリティを確保するために遵守すべき行為及び判断等の基準を示す「情報セキュリティ対策基準」をもって構成する。

３．用語の定義

情報セキュリティポリシーにおける用語の定義は、次に定めるところによる。

（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）データ

電子計算機処理に係る入出力帳票、磁気テープ、磁気ディスク、光ディスクその他の記録媒体に記録されている情報又は通信回線により送信される情報をいう。

（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）サーバ等

ネットワーク上で行政情報を処理し、端末機に提供するコンピュータをいう。

（１０）端末機等

ネットワークを通じてサーバに接続されたパソコン及びモバイル端末をいう。

（１１）電磁的記録媒体等

情報システムでデータ等を記録するための媒体（メディア）で、ハードディスク、フロッピーディスク、ＵＳＢメモリ等をいう。

（１２）情報資産

情報システム及びネットワーク並びにこれらで取扱われるデータ~~行政情報~~（これらを印刷した文書も含む）をいう。

（１３）無線ＬＡＮ

電波等を利用してデータの送受信を行う構内通信網システムをいう。

（１４）広域無線通信

電波等を利用してデータの送受信を行う、事業者が提供する広域向けの通信網システムをいう。

（１５）ＡＳＰ／クラウド

庁外データセンター等でプログラムやデータベースを管理し、ネットワークを介してこれを利用する仕組みや概念をいう。

（１６）職員等

職員、非常勤職員、派遣職員及び委託職員をいう。

（１７）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。

（１８）ＬＧＷＡＮ接続系

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。（マイナンバー利用事務系を除く）

（１９）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。

（２０）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。

（２１）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。

４．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、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、通信の途絶等のインフラの障害からの波及等。

５．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、町長部局、議会事務局、地方公営企業、教育委員会、選挙管理委員会事務局、農業委員会事務局、固定資産評価審査委員会事務局、消防署とする。

（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も含む。）

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．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、業務の遂行にあたって情報セキュリティポリシー及び関連法令を遵守しなければならない。

７．情報セキュリティ対策

情報資産を上記４の脅威から保護するため、次に定める情報セキュリティ対策を講ずるものとする。

（１）組織体制

情報資産を管理し、機密性、完全性及び可用性を維持するための組織体制を確立する。

（２）情報資産の分類と管理

当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。

②ＬＧＷＡＮ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、無害化通信を行う。

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行う。高度な情報セキュリティ対策として、青森県及び県内市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へ接続する。

（４）物理的セキュリティ対策

サーバ、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な対策を講じる。

（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切に対応するため、緊急時対応計画を整備する。

（８）業務委託と外部サービス（クラウドサービス）の利用

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。

約款による外部サービス（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。

８．情報セキュリティ監査及び自己点検

情報セキュリティ対策の遵守状況を検証するため、定期的及び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。

１０．情報セキュリティ対策基準の策定

上記７，８及び９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。

なお、情報セキュリティ対策基準は、公にすることにより当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。

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。

なお、情報セキュリティ実施手順は、公にすることにより当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。