丸森町情報セキュリティ基本方針

令和８年３月３１日　公表

丸森町

1　策定の背景及び目的

○背　景

本町が取り扱う情報資産には、町民の個人情報のみならず行政運営上重要な情報など、外部への漏洩等が発生した場合には、極めて重大な結果を招く情報が多数含まれており、これらの情報資産を様々な脅威などから防御することは、町民の財産、プライバシー等を守るためにも、また、安定的な行政運営のためにも必要不可欠となる。

また、近年の情報通信技術の進展により、電子商取引や電子自治体の構築が現実のものとなってきており、本町がさらに電子自治体を構築するためには、本町が管理しているすべての行政情報ネットワークシステムが安全性を有することが不可欠となってきている。

そのため、本町の情報資産の機密性、完全性及び可用性（注）を維持するための対策を講じるため、丸森町情報セキュリティポリシーを定めることとし、情報セキュリティの確保に最大限取り組むこととする。

このうち、情報セキュリティ基本方針については、本町の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものである。

（注）：国際標準化機構(ISO)が定めるもの（ISO7498-2：1989）

・機密性（confidentiality）：
情報にアクセスすることを許可された者だけがアクセスできることを確実にすること。

・完全性（integrity）：
情報及び処理の方法の正確さ及び完全である状態を安全防護すること。

・可用性（availability）：
許可された利用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。

○策定の目的

セキュリティポリシーは次の事項を目的として策定するものである。

①情報資産の適正な取り扱い
②セキュリティ侵害に対する適切な対応
③町の組織、役割分担及び責任の明確化
④情報セキュリティの意識並びに知識の向上

2　定　義

（1）情報

情報公開条例（平成 11 年丸森町条例第 15 号）第２条第２号に規定するものをいう。

※条例の抜粋

「情報」とは、町職員が職務上作成し、又は取得した文書、図画及び写真並びに電子計算機による処理に使用される磁気テープ、磁気ディスクその他一切の情報媒体等であって、実施機関において保有、管理しているものをいう。

（2）情報システム（「電子計算機」も同義）

ハードウェア及びソフトウェアで構成するパーソナルコンピュータ（サーバ及びクライアント）、印刷装置、接続に要する配線及び接続機器並びにその他の周辺装置をいう。

（3）行政情報

本町の行政事務の執行に関わる情報をいう。

（4）情報資産

情報システム及び行政情報をいう。

（5）情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。具体的に定義すると次に掲げる状態をいう。

①情報の利用及び閲覧（以下「利用等」という。）を行うことを許可された者だけが利用等をできること。

②情報の処理方法が正確かつ安全であること。

③許可された者が必要なときに情報の利用等をできること。

（6）ネットワーク

ネットワークとは、情報を処理するために情報システム及び通信機器等で構成するものをいう。

なお、本町が導入、管理等を行うネットワークは、次の行政情報ネットワークシステム（以下「システム」という。）をいい、下記のとおり分類される。

「行政情報ネットワークシステム」の分類及び対象システム

丸森町イントラネットシステム	各課及び各学校等の共同利用（インターネットや電子メール等、外部とのネットワークシステムに接続し情報の送受信を行う業務を含む。）に供するために設置されたネットワークシステム	文書管理、財務会計、グループウェア、行政情報提供、学校間交流、議会中継等
基幹業務系ネットワークシステム	各課における特定の業務（町民に関する直接的な業務等）及び共同利用の業務を処理するために設置されたネットワークシステム	住民情報、住基ネット、戸籍、介護保険、上下水道料金、申告支援等

（7）特定個人情報

行政手続における特定の個人を識別するための番号の利用等に関する法律（以下「番号法」という。）第２条に規定する個人番号をその内容に含む個人情報ファイルをいう。

（8）個人番号利用事務

番号法第９条第１項又は第３項の規定により個人番号を利用して処理する事務をいう。

（9）個人番号関係事務

番号法第９条第３項の規定により個人番号利用事務に関して行われる個人番号を利用して処理する事務をいう。

3　情報セキュリティポリシーの位置付けと職員等及び外部委託事業者の義務

情報セキュリティポリシーは、本町の情報資産に関する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最高位に位置するものである。

したがって、本町が所掌する情報資産に関する業務に携わる全ての職員等及び外部委託事業者は、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。

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対象範囲は、本町における情報資産及び情報資産に接する町長部局、教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会、議会、地方公営企業の職員等並びに外部委託事業者とする。

5　情報セキュリティ管理体制

本町の情報資産について、適切に情報セキュリティ対策を推進・管理するための体制を確立するものとする。

6　情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

7　情報資産への脅威

情報セキュリティポリシーを策定するうえで、情報資産を脅かす脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

（1）職員等または、外部委託事業者による機器又は情報資産の持出、誤操作、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、故意の不正アクセス又は不正行為による破壊・盗聴・改ざん・消去等、搬送中の事故等による機器又は情報資産の盗難、規定外の端末接続によるデータ漏洩等

（2）外部からの不正アクセスやコンピュータウィルス、地震、落雷、火災等の災害並びに事故、故障等による業務の停止

（3）権限外者による故意の不正アクセス又は不正操作によるデータやプログラムの持出、盗聴、改ざん、消去、機器及び記録媒体の盗難等

8　情報セキュリティ対策

上記7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ずるものとする。

（1）人的セキュリティ対策

情報セキュリティに関する権限や責任等を定め、職員等及び外部委託事業者に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるように必要な対策を講ずる。

（2）物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産の損傷・妨害等から保護するために物理的な対策を講ずる。

（3）技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、コンピュータウィルス対策等を実施する。

（4）運　用

情報セキュリティポリシーの実効性を確保するため、また、不正アクセスされること及び不正アクセスによって他のシステムに対して被害を及ぼすことを防ぐため、ネットワークの監視等、情報セキュリティポリシーの遵守状況の確認等運用面の対策を講ずる。

また、障害が発生した際に迅速な対応を可能とするため、障害時の対応を講ずる。

9　情報セキュリティ対策基準の策定

本町の情報資産について、上記８の情報セキュリティ対策を講ずるに当たっては、遵守すべき事項及び判断等の基準を統一的なレベルで定める必要がある。

そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

１０　情報セキュリティ実施手順（運用マニュアル）の策定

情報セキュリティ対策基準を遵守して、情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めておく必要がある。そのため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、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、公開することにより本町の行政運営及び行政情報ネットワークシステム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。

１１　情報セキュリティ監査の実施

情報セキュリティポリシーが遵守されていることを検証するため、監査を実施する。

１２　評価及び見直しの実施

情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価、システムの変更、新たな脅威等情報セキュリティを取り巻く状況の変化に対応するために、適宜、情報セキュリティポリシーの見直しを実施する。