双葉町情報セキュリティ基本方針

第１　目的

この双葉町情報セキュリティ基本方針（以下、「基本方針」という。）は、町が所管する情報資産の重要性を認識し、その機密性、完全性及び可用性を維持するため、様々な脅威に対する抑止、予防、検知及び復旧について、町として組織的かつ計画的に取り組むための基本的な方針であり、情報セキュリティ対策（以下、「セキュリティ対策」という。）のための基本的な事項を示すことを目的とする。

第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及びその構成機器（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）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。

（４）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。

（５）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。

（６）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。

（７）情報セキュリティポリシー

本基本方針及び双葉町情報セキュリティ対策基準を総称したものをいう。

（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 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ないなど、安全が確保された通信をいう。

第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、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、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

第４　適用範囲

（１）行政機関の範囲

この対策基準が適用される行政機関は、町長部局、教育委員会、農業委員会、議会事務局、選挙管理委員会、監査委員及び固定資産評価審査委員会とする。

なお、教育のために用いるシステム等は、この対策基準の対象となるシステムと機構的に分けるものとする。

（２）情報資産の範囲

この対策基準が対象とする情報資産は、次のとおりとする。

ア　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

イ　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。）

ウ　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

第５　職員等の遵守義務

常勤職員、会計年度任用職員及び臨時的任用職員等（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つとともに、業務等の遂行に当たって、情報

セキュリティ関係法令、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。

第６　セキュリティ対策

町が所管する情報資産を、上記第３の脅威から守るために、以下の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、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。

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　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の分割を行う。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、県及び市町村のインターネットとの通信を集約する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、システム室、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など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

情報システム及びネットワークの監視、情報セキュリティポリシーの遵守状況の確認等、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。

（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。

第７　情報セキュリティ対策基準の策定

上記第６に規定する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る情報セキュリティ対策基準（以下「対策基準」という。）を定めるものとする。

第８　情報セキュリティ実施手順の策定

この基本方針及び対策基準に基づき、業務内容に応じたセキュリティ対策を具体的に実施するため、情報セキュリティ実施手順（以下「実施手順」という。）を定めるものとする。

第９　対策基準及び実施手順の非公開

対策基準及び実施手順は、公にすることにより町の行政運営に重大な支障を及ぼすおそれがあるため、これを非公開とする。

第10　情報セキュリティに関する違反への対応

情報セキュリティポリシーに違反した者については、その重大性、生じた事案の状況等に応じて関係法令に基づく処分等の対象とする。

附　則

この基本方針は、平成２９年１１月２２日から施行する。

附　則（令和７年告示第６号）

この基本方針は、令和７年４月１日から施行する。