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、安全性及び可用性を確保するため、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　情報システム

情報システムとは、コンピュータ関連機器（ネットワーク、ハードウェア機器及びソフトウェア等を含む。）及び電磁的記録媒体で構成され、電子情報の生成、運用、管理及び利用（以下、「処理」という。）を行う仕組みをいう。

２　情報資産

情報資産とは、町が所管する情報システム、ネットワーク及びこれらに関する設備、電磁的記録媒体並びにこれらにより処理、保管又は出力される全ての情報（媒体の形式、形態、材質を問わず。開発と運用に係る全てのデータを含む。）をいう。

３　ネットワーク

ネットワークとは、コンピュータ等を相互に接続、利用するための通信回線網及びその構成機器をいう。

４　電磁的記録媒体

電磁的記録媒体とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録に係る記録媒体をいう。

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　情報セキュリティ

情報セキュリティとは、情報資産の機密の保持及び正確性、完全性の維持並びに所定

の利用者が目的に応じ利用可能な状態を維持することをいう。

９　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。

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、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

第４　基本方針の適用範囲と義務

この基本方針は、町が所管する情報資産の処理に携わる下記の者（以下、「職員等」という。）に適用し、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つとともに、業務等の遂行においては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する義務を負うものとする。

（１）地方公務員法第３条に定める町の地方公務員

（２）契約により操作を認められた事業者

第５　管理体制

本町の情報資産について、統一的な情報セキュリティを確保するため、全庁的な組織体制を整備する。

第６　情報資産の分類及び管理

町の情報資産は、その資産の内容及び重要性に応じて適宜分類し、適切な管理を行うとともに、統一的な情報セキュリティを確保するための管理連絡体制を整備する。

第７　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以下の対策を講ずる。

１　物理的セキュリティ対策

情報システムを設置する施設等への不正な立入り、情報資産への損傷・利用の妨害等から保護するための物理的な対策

２　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を定め、全ての職員等に情報セキュリティポリシーの内容を周知徹底、遵守する等、十分な教育及び啓発が講じられるようにするための人的な対策

３　技術的セキュリティ対策

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、情報資産を適切に保護するための技術的対策

４　運用等における対策

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

５　緊急時におけるセキュリティ対策

情報資産に業務上の障害及び脅威となる緊急事態が生じた場合に、迅速かつ適切な対応を可能とするための危機管理対策と体制の整備

第８　情報セキュリティ対策基準の策定

この基本方針に基づき、セキュリティ対策を講ずるに当たっての遵守すべき事項及び判断等の統一的な基準として、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９　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、町が所管する情報システムについて、構成される組織の個々の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10　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11　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。

第12　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、定期的又は必要に応じて情報セキュリティ監査（以下、「監査」という。）を実施する。

第13　評価及び見直しの実施

情報セキュリティポリシーにおいて、監査により指摘された改善を要する事項及び情報セ

キュリティに含める必要性が認められる事案の発生等がある場合、また、情報セキュリティを取り巻く社会状況の変化等に対応するために、情報セキュリティポリシー等に定める事項の評価と検討を必要に応じて行い、その見直しを適時実施する。

附　則

この基本方針は、平成２９年１１月２２日から施行する。