情報セキュリティ基本方針

１．目的

多古町の各情報システムが取り扱う情報資産には、町民の個人情報を始めとして行政運営上重要な情報等、部外に漏洩した場合、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情報ネットワークに係る犯罪、不正行為、災害等から防御することは、町民の財産、プライバシーを守るためにも、また、継続的かつ安全・安定的な行政サービスの提供を確保するためにも必要不可欠である。

このため、多古町の情報資産の機密性、完全性及び可用性を維持するための施策として情報セキュリティ基本方針及び情報セキュリティ対策基準を制定し、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、多古町の情報セキュリティ対策を実践するに当たっての基本的な考え方、情報セキュリティ対策の意義、対象等を定めることとする。

２．定義

① 情報資産

情報の所在や媒体に関係なく、多古町の行政サービス運営のために必要かつ重要な全てのデータをいう。

② 情報システム

コンピュータ（ハードウェア及びソフトウェアを含む）、ネットワーク及びその他記録媒体で構成され、情報処理を行う仕組みをいう。

③ 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とその構成機器（ハードウェア及びソフトウェアを含む）及びその記録媒体で構成された情報通信基盤をいう。

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、必要時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 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。

⑩ ＬＧＷＡＮ接続系

人事給与、財務会計及び文書管理等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。

⑪ 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。

⑫ 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。

⑬ 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等、安全が確保された通信をいう。

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、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・情報資産の搾取、内部不正等

② 情報資産の無断持出し、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、紙媒体等の紛失・盗難、機器故障等の非意図的要因による情報の漏えい・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

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、町長部局、教育委員会、その他行政委員会、議会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、次のとおりとする。

（1）ネットワーク、情報システム及びこれらに関する設備、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、非常勤職員並びに契約の如何に関わらず庁内で業務を遂行する者（以下職員等及び外部委託事業者等）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

上記３の脅威から情報資産を保護するため、以下の情報セキュリティ対策を講じる。

① 組織体制

本町の情報資産を保護するため、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、該当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連絡経路を分割する。なお、両システム間で通信する場合、無害化通信を実施する。

（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として、千葉県と市町村のインターネット接続口を集約した上で、自治体セキュリティクラウド等を活用した対策を実施する。

④ 物理的セキュリティ

サーバ、サーバ室、通信回線及び職員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、アクセス制限、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）の利用

業務委託する場合、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。また、約款による外部サービスを利用する場合、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、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。情報セキュリティポリシーの見直しが必要な場合、情報セキュリティポリシーの見直しを行う。

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、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となった場合、情報セキュリティポリシーを見直す。

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、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及び法令等に基づき、運用を行うものとする。また、システムごとに必要に応じて情報セキュリティ対策を実施するための具体的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。

附　則

この情報セキュリティ基本方針は、平成１５年９月１日から施行する。

附　則

この情報セキュリティ基本方針は、令和６年７月１日から施行する。

附　則

この情報セキュリティ基本方針は、令和８年４月１日から施行する。