福崎町情報セキュリティ基本方針

平成１５年１１月１日制定・実施

令和８年３月２３日制定（改正）

（序文）

福崎町において取り扱う情報には、住民の個人情報や行政運営上重要な情報等、外部への漏えい等が発生した場合に極めて重大な影響を及ぼす情報が多数含まれており、これらの情報資産を適切に保護し、責任を持って管理するためには、情報セキュリティマネジメント（情報資産を適切に保護するための組織としての継続的かつ計画的な取り組み）が必要不可欠である。

そのため、福崎町は、情報セキュリティマネジメントの実現に関する体系的かつ具体的な対策等を「福崎町情報セキュリティ基本方針」として定めることとする。

第１章 総則

（目的）

第１条　福崎町情報セキュリティ基本方針（以下「基本方針」という。）は、福崎町（以下「本町」という。）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、本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。

（定義）

第２条　基本方針において、次の各号に掲げる用語の意義は、当該各号の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

職員等が職務上作成し、又は取得したすべての文書等のうち電磁的に記録されたもの。

（３）情報資産

情報及び情報システムの総称（教育機関で専ら教育用に使用する情報資産は含まない）。

（４）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。

（５）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。

（６）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。

（７）機密性

情報資産にアクセスすることが認められた者だけがアクセスできる状態を確保すること。

（８）完全性

情報資産が破壊、改ざん又は消去されておらず、正確及び完全である状態を確保すること。

（９）可用性

情報資産にアクセスすることが認められた者が、必要な時に中断されることなく、情報資産にアクセスできる状態を確保すること。

(10) 個人情報

福崎町個人情報保護条例（平成１３年福崎町条例第２号。）第２条第２号に規定する個人情報をいう 。

(11) 職員等

地方公務員法第３条第２項及び第３項第１号、１号の２、２号、３号、４号、第２２条の２第１項第１号、２号、第２２条の３に掲げる者をいう。

(12) 情報セキュリティに関する事案

不正アクセス、コンピュータウイルスの感染等、情報セキュリティに関する事故、事件をいう。

(13) 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。

(14) 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。）

(15) 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。

(16) 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うえで、安全が確保された通信だけ許可できるようにすることをいう。

(17) 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。

（適用範囲）

第３条　基本方針における行政機関及び情報資産の適用範囲は、以下のとおりとする。

（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、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

（対象とする脅威）

第４条　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）職員等による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

（2）職員等によらない不正アクセス、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

（3）地震、落雷、火災等の災害によるサービスおよび業務の停止等

（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２章 基本的な考え方

（職員等の責務）

第５条　本町の業務に携わる全ての職員等は、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。

（組織体制）

第６条 本町の情報資産について、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。

（情報資産の分類と管理）

第７条　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。

（情報システム全体の強靭性の向上）

第８条　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うえで、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。

（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、都道府県及び市区町村のインターネットとの通信を集約したうえで、自治体情報セキュリティクラウドの導入等を実施する。

（人的セキュリティ）

第９条　情報セキュリティに関し、職員等の責務を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（物理的セキュリティ）

第１０条　サーバ、情報システム室、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。

（技術的セキュリティ）

第１１条　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。

（外部サービスの利用）
第１２条　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。

（情報セキュリティに関する事案への対応）
第１３条　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正に対応するため、緊急時対応計画を策定する。

（準拠）
第１４条　職員等は、ポリシーに定められた条項のほか、情報資産の利用において、関連法令、本町が定める条例等を遵守し、これに従う。

（違反への対応）
第１５条　職員等がポリシーに違反した場合は、地方公務員法等に基づき、懲戒処分等の対象とする。

（評価・見直し）
第１６条　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は、適宜情報セキュリティポリシーの見直しを行う。

第３章 雑則

（情報セキュリティ対策基準の策定）
第１７条　第５条から第１５条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。

（情報セキュリティ実施手順の策定）
第１８条　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。
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。

（その他）
第１９条　基本方針に定めるもののほか、情報セキュリティに関し必要な事項については、別に定める。