永平寺町情報セキュリティポリシー　基本方針

（目的）

第１条　永平寺町情報セキュリティポリシー基本方針（以下「基本方針」という。）は、永平寺町（以下「町」という。）が保有する情報資産に関し、適切な情報セキュリティ水準を保つため、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。

（用語の定義）

第２条　この基本方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

（１）部局等

町長部局、行政委員会、議会事務局及び消防本部をいう。

（２）職員等

部局等の業務に従事する職員その他これに準ずる者および受託事業者ならびに部局等が受け入れる研修者をいう。

（３）コンピュータ

中央処理装置および周辺装置から構成され、電気信号を用いて情報の演算、記憶、制御、通信および入出力の各機能を有する装置および機器をいう。

（４）情報システム

ハードウェア、ソフトウェア、記録媒体等で構成され、これらで業務処理を行うものをいう。

（５）ネットワーク

コンピュータを相互に接続するための通信網およびその構成機器をいう。

（６）アクセス

コンピュータ、情報システムおよびネットワークを通じて情報の参照、変更等を行うことをいう。

（７）情報

電磁的に記録されたデータで、特定のプログラム等により内容を判断、識別できるものをいう。

（８）コンピュータ組織

情報を管理するためのコンピュータ、情報システム、ネットワーク等による仕組みおよびそれらの運用・管理のために必要な資料等をいう。

（９）記録媒体

情報を電磁的に記録するためのもので、ハードディスク、フロッピーディスク、CD、MO、DVD、USB メモリ、メモリカード、磁気テープ等をいう。

（１０）情報資産

情報および情報を格納した記録媒体ならびにコンピュータ組織の総称をいう。

（１１）情報セキュリティポリシー

本基本方針および別に定める永平寺町情報セキュリティポリシー対策基準（以下「対策基準」という。）の総称をいう。

（１２）情報セキュリティ

情報資産の機密性、完全性および可用性を維持することをいう。

（１３）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。

（１４）完全性

情報が破壊、改ざんまたは消去されていない状態を確保することをいう。

（１５）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。

（１６）実施要領等

情報システムまたはネットワークの運用・管理および情報セキュリティ対策を具体的に実施するために必要な事項を定めた要綱、要領等をいう。

（１７） 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。

（１８） 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。

（１９） 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。

（２０） 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。

（２１）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。

（対象範囲）

第３条　情報セキュリティポリシーは、部局等が所管する情報資産および職員等に適用する。

（情報資産の取扱い）

第４条　町が保有する情報資産の取扱いについては、別に定めのあるもののほか、情報セ

キュリティポリシーの定めるところによる。

２　職員等は、情報セキュリティの重要性についての共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシーを遵守しなければならない。

（情報資産への想定する脅威）

第５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）　職員等および部外者による不正アクセスや部外者による侵入、サービス不能攻撃等の意図的な要因による情報資産の漏えい、破壊、改ざん、消去等

（２）　プログラム上の欠陥・操作ミス・故障等のほか、職員等による情報資産の誤った取扱いにおける非意図的な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

（情報セキュリティ対策）

第６条　前条の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じる。

（１）組織体制

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。

（２）情報資産の分類と管理

町の保有する情報資産を重要度に応じて分類し、当該分類を考慮した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。

②LGWAN 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を実施する。高度な情報セキュリティ対策として、県と町のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（４）物理的セキュリティ

サーバ等、サーバ室等、ネットワークおよび職員等が使用する端末機等の管理につ

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。

（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

情報システムの監視、外部委託を行う際の情報セキュリティ確保、脅威発生時の対応等、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。

（８）外部サービスの利用

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。

約款による外部サービスを利用する場合には、利用にかか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には、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は、情報セキュリティポリシーの見直しを行う。

（監査および自己点検の実施）

第７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、定期的または必要に応じて情報セキュリティ監査（以下「監査」という。）および自己点検を実施する。

なお、監査および自己点検の実施に関し必要な事項は、別に定める。

（情報セキュリティポリシーの見直し）

第８条　情報セキュリティポリシーは、監査や自己点検の結果により不備な対策が発見された場合、あるいは情報セキュリティに関する状況の変化により新たな対策が必要になった場合には、必要に応じて見直しを図る。

（対策基準の策定）

第９条　上記６，７及び８規定する情報セキュリティ対策を実施するために、具体的な判断基準、措置事項および遵守事項を定めた対策基準を策定する。

（実施要領等の策定）

第 10 条　対策基準に基づき、各情報システム等が実施する情報セキュリティ対策の具体的

な手順を定めた実施要領等を策定する。

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市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　この方針は、平成 29 年 4 月 1 日から施行する。

附則　この方針は、令和元年 9 月 1 日から施行する。