壬生町情報セキュリティポリシー
基本方針

平成１７年３月策定
平成２７年７月全部改定
平成３１年３月一部改定
令和　３年６月一部改定
令和　７年３月一部改定

栃木県壬生町

1. 目的

壬生町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方針、位置付け等を定めることを目的とする。

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、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、記録媒体で構成され、処理を行う仕組みをいう。

（3）情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

（4）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。

（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）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

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無い等、安全が確保された通信をいう。

3. 対象とする脅威

情報資産を脅かす脅威として、認識すべきは以下のとおりである。

（1）サイバー攻撃をはじめとする部外者の侵入、不正アクセス又はウィルス攻撃、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洩・破壊・改ざん・消去・重要情報の詐取等、内部不正等

（2）情報資産の無断持出、無許可端末やソフトウェアの持込・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洩・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因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提供サービス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（水道事業管理者及び下水道事業管理者の職務を行う町長を含む）、教育委員会、選挙管理委員会事務局、監査委員事務局、固定資産評価審査委員会、農業委員会事務局及び議会事務局とする。

（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

5. 職員等の遵守義務

職員、非常勤職員及び臨時職員等当町の情報・機器・ネットワーク等を用い業務にあたるもの(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.で示した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ずるものとする。

（1）組織体制

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。

（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、完全性及び可用性を踏まえ、その重要度に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

（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。

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上で、自治体情報セキュリティクラウドの導入等を行う。

（４）物理的セキュリティ対策

サーバ、情報システム室、通信回線及び職員等のパソコンやモバイル端末の管理について、物理的な対策、例として入退館（室）の管理（業務時間帯、深夜時間帯等の時間帯別に、入室権限を管理)、 盗難や窃視等の防止、機器・装置・情報媒体等の盗難や紛失防止も含めた保護及び措置を講じる等を行う。

（５）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、職員等が遵守すべき事項を定めるとともに、セキュリティポリシーの内容を周知徹底し、十分な教育及び啓発をする。

（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、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、セキュリティ侵害が発生した際に迅速な対応を可能とするための危機管理対策・緊急時対応計画の策定、災害時等の業務継続対策・計画の策定を行う。

（８）外部サービス(クラウドサービス)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(クラウドサービス)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、適宜情報セキュリティポリシーの見直しを行う。

特に、急速な DX 化に対応できるよう適宜見直しや柔軟な対応を行うことが求められるため、職員はデジタル技術の利活用の必要性やセキュリティポリシーの重要性の理解を深めることと、評価・見直しについては十分な協議・対話を行うことを徹底すること。

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及び自己点検の実施を、最低年 1 回実施する。

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、職員からの提言や相談等により、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、情報セキュリティを取り巻く状況の変化に対応するために、新たに対策が必要となった場合には、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、リスクを検討したうえで、情報セキュリティポリシー及び運用の見直しを実施する。

9．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に基づき、情報セキュリティ対策を実施するために、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行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。