

七飯町サイバーセキュリティを確保するための方針

第1版
七飯町

七飯町サイバーセキュリティを確保するための方針

1 目的

本方針は、総務省が示す地方公共団体におけるサイバーセキュリティ確保の指針を踏まえ、七飯町（以下「本町」という。）の保有する情報資産の機密性、完全性及び可用性を確保し、サイバー攻撃その他の脅威から住民情報及び行政情報を保護することを目的とする。

2 定義

本方針における用語の定義は、次のとおりとする。

(1) ネットワーク

ハードウェア（コンピュータを構成している電子回路、周辺機器等の物理的実体をいう。以下同じ。）を相互に接続するための通信網をいう。

(2) 情報システム

ハードウェア、ソフトウェア（コンピュータを動作させる手順及び命令をコンピュータが理解できる形式で記述したものをいう。以下同じ。）及びネットワークにより業務処理を行う仕組みをいう。

(3) 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

(4) 機密性

情報にアクセスすることを認められたものだけが、情報にアクセスできる状態を確保することをいう。

(5) 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。

(6) 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。

(7) 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、地方税もしくは防災に関する事務）または戸籍事務等に係る情報システム及びデータをいう。

(8) 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。

(9) インターネット接続系

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。

(10) 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を許可できるようにすることをいう。

(11) 無害化通信

インターネットを利用したメールや外部ネットワークへのアクセス等を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影響がないよう、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、サイバー攻撃等の意図的な要因による情報資産漏洩・破壊・改ざん等
- (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的要因等
- (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) 電力供給や通信の途絶等のインフラ障害からの波及等

4 適用範囲

本方針は、町長部局、教育委員会部局、選挙管理委員会、監査委員、議会事務局、農業委員会事務局、固定評価資産評価審査委員会、地方公営企業の全ての職員（特別職を含む。以下同じ。）に適用する。

5 職員等の遵守義務

職員及び会計年度任用職員（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に、以下の情報セキュリティ対策を講じる

- (1) 組織体制
本町の情報資産について、情報セキュリティ対策を精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、当該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靱性の向上

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。

- ア) 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。
- イ) 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、両システム間で接続する場合には、無害化通信を実施する。
- ウ) 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、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実施する。

(4) 物理的セキュリティ

サーバ、情報システム室、通信回線、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、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に迅速かつ適正に対応する。

(8) 業務委託と外部サービスの利用

業務委託を行う場合には、委託業者を選定し、情報セキュリティ要件を明記した契約を締結し、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。

外部サービスを利用する場合には、利用するサービスに応じ対策と責任者を定める。

(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事故点検を実施し、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。