

# 十和田市情報セキュリティポリシー

---

## 情報セキュリティ基本方針

制定：平成31年3月

十和田市

## 目 次

1. 目的 .....	1
2. 定義 .....	1
3. 対象とする脅威 .....	2
4. 適用範囲 .....	2
5. 情報セキュリティ対策 .....	2
6. 情報セキュリティ監査及び自己点検の実施 .....	3
7. 情報セキュリティポリシーの見直し .....	3
8. 情報セキュリティ対策基準の策定 .....	3
9. 情報セキュリティ実施手順の策定 .....	3
10. 公開範囲 .....	4

## 十和田市情報セキュリティ基本方針

### 1 目的

本基本方針は、本市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、本市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。

### 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。

#### (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) 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) 情報セキュリティインシデント

情報管理やシステム運用に関して保安上の脅威(障害・事故・システム上の欠陥)となる事象をいう。

#### (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、地方税及び災害対策に関する事務)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、重要情報の詐取、内部不正等
- 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、プログラム上の欠陥、操作ミス、機器故障等の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、十和田市事務分掌条例（平成 17 年十和田市条例第 7 号）第 2 条に掲げる部、上下水道部、会計管理者、中央病院事務局、教育委員会事務局、教育機関（小学校及び中学校を除く。）、選挙管理委員会事務局、監査委員事務局、農業委員会事務局及び議会事務局とする。

なお、上下水道部、中央病院事務局及び教育機関で十和田市情報セキュリティポリシー対策基準の対象となるシステムと物理的に分けられ、個別に管理されるネットワーク及び情報システムについては、対象外とする。

### (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

### (3) 職員等の範囲

本基本方針が対象とする職員等は、次のとおりとする。

十和田市職員、臨時職員、非常勤職員、期間業務職員、パートタイマー及び派遣職員

## 5 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

本市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

本市の保有する情報資産を重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

### (3) 情報システム全体の強靱性の向上

情報システム全体に対し、次の 3 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。
- 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、青森県自治体情報セキュリティクラウドサービスを利用する。

#### (4) 物理的セキュリティ

サーバ等の情報システムを設置し、当該機器等の管理並びに運用を行うための部屋等、通信回線等及び職員等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、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切に対応するため、緊急時対応計画を策定する。

### 6 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。

### 7 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には、情報セキュリティポリシーを見直す。

### 8 情報セキュリティ対策基準の策定

上記5、6及び7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。

### 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。

## 10 公開範囲

情報セキュリティ対策基準及び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。