

# 由布市情報セキュリティ基本方針

## 1-1 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。

## 1-2 定義

### (1) ネットワーク

電子計算機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

電子計算機等及びネットワークをいう。

### (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) 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

人事給与、財務会計及び文書管理等 L G W A N 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**

L GWAN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。

#### **(13) クラウドサービス**

ソーシャルメディアサービス、生成AIサービス、その他のクラウドサービスをいう。

### **1-3 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、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の障害からの波及等

### **1-4 適用範囲**

#### **(1) 実施機関の範囲**

本基本方針が適用される実施機関は、市長部局、行政委員会、議会、消防本部、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

## 1-5 職員等及び議員の遵守義務

(1) 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つとともに、情報資産の利用にあたっては情報セキュリティポリシー及び情報セキュリティポリシー実施手順を遵守するものとする。

(2) 市議会議員(以下、「議員」という。)は、公務において本市の情報資産を取り扱う際、本基本方針の趣旨に則り、適切な管理に努めるものとする。

## 1-6 情報セキュリティ対策

市の情報資産を上記1-3の脅威から保護するため、以下の情報セキュリティ対策を講ずる。

### (1) 組織体制

本市の情報資産について、適切に情報セキュリティ対策を推進するための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行う。

### (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。

- 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、都道府県及び市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対策**

電算機器、電算室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講ずる。

#### **(5) 人的セキュリティ対策**

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対策**

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。

#### **(8) 業務委託とクラウドサービスの利用**

- ①委託する場合には、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、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。
- ②クラウドサービスを利用する場合には、利用に係る規定を整備し対策を講じる。
- ③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。

## 1-7 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。

## 1-8 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、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。

## 1-9 情報セキュリティ対策基準の策定

上記1-6、7及び8に規定する対策等を実施するために、基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。(第2章に記述)なお、議員が遵守すべき事項については、議会が別途定める。

## 1-10 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。

なお、情報セキュリティ実施手順は、公開することにより当市の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。