# 八百津町
# 情報セキュリティ
# ポリシー

（令和８年３月版）

# 目次

**2-７．情報セキュリティ監査及び自己点検の実施**

**2-８．情報セキュリティポリシーの見直し**

**2-９．情報セキュリティ対策基準の策定**

**2-10．情報セキュリティ実施手順の策定**

# 総則

## 第1章 総則

### 1-1. 本町における情報セキュリティの考え方

本町は、法令等に基づき、住民の個人情報や企業の経営情報等の重要情報を多数保有するとともに、ほかに代替することができない行政サービスを提供している。また、本町の業務の多くが情報システムやネットワークに依存していることから、住民生活や地域の社会経済活動を保護するため、本町は、情報セキュリティ対策を講じて、その保有する情報を守り、業務を継続することが必要となっている。

今後、各種手続のオンライン利用の本格化や情報システムの高度化等、電子自治体が進展することにより、情報システムの停止等が発生した場合、広範囲の業務が継続できなくなり、住民生活や地域の経済社会活動に重大な支障が生じる可能性も高まる。また、本町はLGWAN等のネットワークにより他団体と相互に接続しており、一部の団体で発生したIT障害がネットワークを介して本町を含む他の団体に連鎖的に拡大する可能性は否定できない。

これらの事情から、本町のみならず全ての地方公共団体において、情報セキュリティ対策の実効性を高めるとともに対策レベルを一層強化していくことが必要となっている。また、情報セキュリティの確保に絶対安全ということはないことから、情報セキュリティに関する障害・事故及びシステム上の欠陥（以下、「情報セキュリティインシデント」という。）の未然防止のみならず、情報セキュリティインシデントが発生した場合の拡大防止・迅速な復旧や再発防止の対策を講じていくことが必要である。

なお、情報セキュリティ対策は、個人情報保護対策と内容的に重なる部分も多い。ま

た、自然災害時や大規模・広範囲にわたる疾病における対応という意味では防災対策とも重なる。情報セキュリティを対策する部署とこれらを担当する部署は、相互に連携をとって、それぞれの対策に取り組むことが求められる。

また、地方公共団体は、自らの情報セキュリティを確保するとともに、地域全体の情報セキュリティの基盤を強化するため、地域における広報啓発や注意喚起、官民の連携・協力等に積極的に貢献することが望まれる。例えば、住民等への広報による啓発、IT講習等による住民等への情報セキュリティに関する研修の実施、業務面で関係する団体に対する情報セキュリティポリシーの策定の働きかけなどの取組を行うことが考えられる。

## 1-2. 情報セキュリティポリシーの必要性と構成

本町においては、情報セキュリティ対策を徹底するには、対策を組織的に統一して推進することが必要であり、そのためには組織として意思統一し、明文化された文書として、情報セキュリティポリシーを定めなければならない。

なお、「サイバーセキュリティ基本法」第5条では、地方公共団体においてサイバーセキュリティに関する自主的な施策の策定と実施が責務規定として法定化された。これにより、情報セキュリティポリシーの未策定団体においては策定が必須となり、策定済み団体においても、適時適正な見直しとそれを遵守することが重要となっている。

また、番号制度等の最新の制度に係るセキュリティ対策、例えば、情報提供ネットワークシステム等の技術的基準、「特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）」（令和3年8月改正 個人情報保護委員会）が示す安全管理措置等についても遵守しなければならない。

本町の情報セキュリティ対策における基本的な考え方を定めるものが、「基本方針」である。この基本方針に基づき、全ての情報システムに共通の情報セキュリティ対策の基準を定めるのが「対策基準」である。この「基本方針」と「対策基準」を総称して「情報セキュリティポリシー」という。この「対策基準」を、具体的なシステムや手順、手続に展開して個別の実施事項を定めるものが「実施手順」である。

このように、情報セキュリティポリシーは、情報セキュリティ対策の頂点に位置するものであることから、町長をはじめ、職員、会計年度任用職員等（以下、「職員等」という。）及び外部委託事業者は、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する義務を負う。

## 1-3. 情報セキュリティ対策の実施サイクル

情報セキュリティ対策の実施プロセスは、策定･導入（Plan）、運用（Do）、評価（Check）、見直し（Action）の4段階に分けることができ、この実施サイクルを繰り返すことによって情報セキュリティは確保される。この実施サイクルは、それぞれの項目の頭文字をとって、PDCAサイクルとも呼ばれる。

情報セキュリティを取り巻く脅威や対策は常に変化しており、以上のPDCAサイクルは、一度限りではなく、これを定期的に繰り返すことで、環境の変化に対応しつつ、情報セキュリティ対策の水準の向上を図らなければならない。

## 1-4. 策定及び導入

情報セキュリティポリシーの策定及び導入は、まず、①策定のための組織体制を確立し、その組織体制の下で、②地方公共団体の基本方針を策定する。次に、③リスク分析を実施し、その結果に基づき、④対策基準の策定を行い、⑤情報セキュリティポリシーを正式に決定する。この後、情報セキュリティポリシーに基づき、⑥実施手順を策定し、⑦ポリシー・実施手順の周知を行うというプロセスになる。

## 1-5. 組織体制の確立

（１）組織体制の確立

情報セキュリティポリシーの策定には、幹部職員の関与が不可欠である。また、情報セキュリティポリシーは、組織内の様々な部局の情報資産に係る問題を取り扱うことから、責任の所在を明確にするため、全ての部局の長、情報システムを所管する課室長及び情報セキュリティに関する専門的知識を有する者などで構成する組織又はこれに代わる組織（以下、本章において、「情報セキュリティ委員会」という。）が行う。

（２）情報セキュリティポリシー策定チームの編成

情報セキュリティ委員会は、情報セキュリティポリシーの策定作業の一部を下部の組織（情報セキュリティポリシー策定チーム等）に行わせることができる。

策定チームには、全ての部、課等の関係者が関与することが望ましいが、主たる関係部署に絞って構成する場合もある。

| 担当課・室・係 | 選定の理由 |
| --- | --- |
| 総務課 企画行政係 | 庁内業務の情報政策の主管<br>庁内の情報システムの主管<br>個人情報保護条例の主管<br>文書管理規程、文書管理システムの主管<br>報道機関への対応の主管 |
| 総務課 財政係 | 庁内の施設管理の主管 |
| 防災安全室 | 災害等の危機管理の主管 |

図表1 情報セキュリティポリシー策定チームの編成例

## 1-6. 情報セキュリティ基本方針の策定

情報セキュリティ基本方針においては、情報セキュリティ対策の目的、体系等、本町の情報セキュリティに対する基本的な考え方を示す。

## 1-7. リスク分析の実施

リスク分析とは、本町が保有する情報資産を明らかにし、それらに対するリスクを評価することである。

具体的なリスク分析・評価方法については「地方公共団体における情報資産のリスク分析・評価に関する手引き」（平成21年3月 総務省）、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」（平成28年10月7日 サイバーセキュリティ対策推進会議）及び「高度サイバー攻撃対処のためのリスク評価等のガイドライン付属書」（平成28年10月7日 内閣官房内閣サイバーセキュリティセンター）を参照する。

進め方として、まずは、利用している情報資産に関わらない組織全体としての情報セキュリティ対策の現状に対するリスク分析・評価を行い、次のステップとして、情報資産に関わる情報セキュリティ対策の現状に対するリスク分析・評価を行う。

第１ステップ

庁内の情報セキュリティ規程・規則等の策定状況、組織体制の確立状況について、マネジメント体制の観点（組織的対策、人的対策）からリスク分析・評価を行う。

第２ステップ

保有する情報資産における情報セキュリティリスクを分析・評価する。具体的には以下の作業を行う。

（１）本町の保有する情報資産を調査の上、重要性の分類を行い、この結果に基づき、要求されるセキュリティの水準を定める。

（２）本町の情報資産を取り巻く脅威及び脆弱性を調査し、リスクを特定する。リスクの発生可能性及び発生した際の被害の大きさからリスクの大きさを求める。

なお、一般的に両者の積をリスクの大きさとしている。

（３）リスクの大きさがセキュリティ要求水準を下回るよう対策基準を策定し、適正なリスク管理を行う。

なお、スマートデバイス等の新しいモバイル端末、クラウドサービス等の新しい技術の導入や新たな脅威の発生等の情報セキュリティに関する環境変化により、情報資産や情報資産に対するリスクに大きな変化が生じたときには、関係する情報資産についてリスク分析を再度行い、その結果、情報セキュリティポリシーの見直しが必要と判断される場合にはその見直しを行う。また、定期的な情報セキュリティポリシーの評価・見直しの際にもリスク分析から再検討することが必要である。

リスク分析に関する資料は、情報セキュリティポリシー策定の基礎資料として保管する必要があるが、当該資料には情報資産の脆弱性に関する事項が記載されているため、厳重な管理が必要である。

## 1-8. 情報セキュリティ対策基準の策定

リスク分析の結果得られる情報セキュリティ要求水準に対して、それを実現するための遵守事項や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。情報セキュリティ対策基準は、想定される情報リスクに十分に対処し、情報セキュリティ要求水準を満たすものでなければならない。

## 1-9. 情報セキュリティポリシーの決定

情報セキュリティ委員会が策定した情報セキュリティ基本方針及び情報セキュリティ対策基準について、副町長の決裁により、本町における情報セキュリティポリシーとして正

式に決定する。

### 1-10. 実施手順の策定

実施手順は、職員等関係者が、各々の扱うネットワーク及び情報システムや携わる業務において、どのような手順で情報セキュリティポリシーに記述された内容を実行していくかを定めるマニュアルに該当する。このマニュアルには、主要な情報資産に対するセキュリティ対策実施手順も含まれる。

実施手順は、個別の目的のために作成し、見直し等を柔軟に行っていくため、業務担当課において情報システムや情報資産を管理する者等が策定する。

### 1-11. 情報セキュリティポリシー及び実施手順の周知

情報セキュリティ対策を最終的に実施するのは職員等であるため、実効性を確保するため情報セキュリティポリシーの配布や説明会などにより、情報セキュリティポリシーを職員等に十分に周知する。また、実施手順については、各課部局の責任者が当該手順を実行する者に周知する。

### 1-12. 運用

情報セキュリティポリシーを確実に運用していくため、情報システムの監視や情報セキュリティポリシーに従って対策が適正に遵守されているか否かを確認し、情報資産に対するセキュリティ侵害や情報セキュリティポリシー違反に対し、適正に対応しなければならない。このため、緊急時対応計画の策定、同計画に基づく訓練、同計画の評価・見直し等を実施する。

### 1-13. 評価・見直し

情報セキュリティポリシーの実効性を確保するとともに、情報資産や情報システム等の変化、情報セキュリティに関する脅威や対策等の変化に対応していくためには、情報セキュリティポリシーの評価・見直しを行い、前述のPDCAサイクルを繰り返すとともに、PDCAサイクルの有効性の確認のために監査・自己点検を活用し、情報セキュリティ対策を不断に強化し続けることが不可欠である。

### 1-14. 監査・自己点検

地方公共団体において情報セキュリティ対策の実効性を確保するには、情報セキュリティ対策の実施状況を検証し、情報セキュリティポリシーの見直しに反映させることが必要である。このため、独立かつ専門的知識を有する専門家（部内者であっても監査対象から独立した監査担当者等が行う場合を含む。）による検証である情報セキュリティ監査や情報システム等を運用する者自らによる検証である自己点検を行う。なお、自己点検にあたっては、「地方公共団体における情報セキュリティ監査に関するガイドライン」（令和2年12月 総務省）の「第2章 情報セキュリティ監査手順」を参照する。

### 1-15. 情報セキュリティポリシーの見直し

情報セキュリティポリシーの見直し作業は、情報セキュリティ委員会の下で、情報セキュリティポリシーの策定手順（1-4. 策定及び導入参照）に準じて実施する。

# 基本方針

## 第2章 情報セキュリティ基本方針

### 2-1. 目的

本基本方針は、本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事項を定めることを目的とする。

### 2-2. 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）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。

## 2-３．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、外部委託管理の不備、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

## 2-４．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、内部部局、行政委員会、議会事務局及び地方公共企業とする。

（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

| 情報資産の種類 | 情報資産の例 |
|---|---|
| ①ネットワーク | 通信回線、ルータ等の通信機器等 |
| ②情報システム | サーバ、パソコン、モバイル端末、汎用機、複合機、オペレーティングシステム、ソフトウェア等 |
| ③①・②に関する施設・設備 | コンピュータ室（電算室）、通信分岐盤、配電盤、電源ケーブル、通信ケーブル等 |
| ④電磁的記録媒体 | 内蔵電磁的記録媒体（サーバ装置、端末、通信回線装置等に内蔵される記録媒体）、及び、外部電磁的記録媒体（USBメモリ、外付けハードディスクドライブ、DVD-R、磁気テープ等） |
| ⑤ネットワーク及び情報システムで取り扱う情報 | ネットワーク、情報システムで取り扱うデータ等（これらを印刷した文書を含む。） |
| ⑥システム関連文書 | システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等 |

図表 情報資産の種類と例

なお、システム関連文書以外の文書は、本基本方針の対象としないが、文書管理規程等により適正に管理しなければならない。

## 2-５．職員等の遵守義務

職員等は、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。

## 2-６．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、岐阜県及び県内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

サーバ、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等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

（8）業務委託と外部サービス（クラウドサービス）の利用

業務委託する場合には、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。

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。

## 2-7．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。

## 2-8．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内部、外部の環境の変化に対応するため、新たに対策が必要になった場合には、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を見直す。

## 2-９．情報セキュリティ対策基準の策定

上記６、７及び８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。

## 2-１０．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本町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。