

# 京丹波町情報セキュリティポリシー 基本方針

平成17年10月11日	策定
平成19年4月1日	一部改定
平成22年4月1日	一部改定
平成23年11月1日	全部改定
平成28年4月1日	一部改定
平成30年5月1日	一部改定
平成31年4月1日	一部改定
令和2年4月1日	一部改定
令和3年4月1日	一部改定
令和4年4月1日	一部改定
令和6年4月1日	一部改定
令和8年3月25日	一部改定

# 第1章 総則

## 1 目的

京丹波町（以下、「本町」という。）が保有する情報資産には、住民の個人情報のみならず、行政運営に必要な情報など、部外に漏えい等した場合には、極めて重大な結果を招く情報が多く含まれている。本基本方針は、本町が保有する情報資産を漏えい、事故、災害、その他の脅威から防御し、情報資産の機密性、完全性、可用性を維持するため、情報セキュリティ対策について基本的事項を定めることを目的とする。

## 2 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、他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、地方公共団体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、地方公共団体は、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、地方公共団体はL G W A N等のネットワークにより相互に接続しており、一部の団体で発生したI T障害がネットワークを介して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、すべ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事故の未然防止のみならず、事故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。

## 3 情報セキュリティの体系

情報セキュリティは、基本方針、対策基準及び実施手順で構成される。

基本方針は、情報セキュリティ対策に関する統一かつ基本的な方針を示すもので、対策基準は基本方針に基づく情報セキュリティ対策として実施すべき基準を示したものである。情報セキュリティポリシーを基本方針と対策基準として、京丹波町情報セキュリティポリシーとする。

## 第2章 情報セキュリティ基本方針

### 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。

なお、本基本方針については、地方自治法（昭和22年法律第67号）第244条の6第1項に規定するサイバーセキュリティを確保するための方針として位置付けるものとする。

### 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、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) 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) L G W A N 接続系

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 G W A N 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) 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、ウイルス攻撃、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提供サービスの障害からの波及等

### 4 適用範囲

#### (1) 機関の範囲

本対策基準は、本町の情報資産に携わる職員(会計年度任用職員を含む)及び外部委託事業者とする。なお、情報センター、病院、学校等の専門分野に特化した機関については、本対策基準に加え、各機関において別途定める対策基準を遵守しなければならない。

#### (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、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。

②L G W A N接続系においては、L G W A N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、情報資産への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。

(8) 外部サービスの利用

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。

#### 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。

#### 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になった場合には、情報セキュリティポリシーを見直す。

#### 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。

#### 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。