# 奈良市情報セキュリティ基本方針

＜ 目　　次 ＞

## １　目的

この基本方針は、本市が保有する個人情報をはじめとする行政運営上必要な情報資産の機密性、完全性及び可用性を維持するため、情報セキュリティ対策にかかる基本的な事項を定めることを目的とする。

## ２　用語の定義

(1)　情報

本市が保有するコンピュータに記録されたデータ及び記録されたデータが処理され出力されたものすべてをいう。

(2)　情報システム

本市が管理するすべてのコンピュータ（ハードウェア、ソフトウェア及びネットワーク）及び電磁的記録媒体で構成され、処理を行う仕組みをいう。

(3)　情報資産

情報及び情報システムをいう。

(4)　情報セキュリティ

脅威から情報資産を保護し、情報資産の「機密性」、「完全性」及び「可用性」を確保することをいう。

(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)　情報セキュリティ対策

情報資産の情報セキュリティを維持するための管理策をいう。

(9)　個人番号利用事務系

個人番号利用や住民票発行をはじめとする基幹業務に関わる情報資産をいう。

(10)　ＬＧＷＡＮ接続系

地方公共団体を相互に接続する行政専用のネットワーク（ＬＧＷＡＮ）に接続された情報資産をいう（個人番号利用事務系を除く）。

(11)　インターネット系

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資産をいう。

(12)　通信経路の分割

ＬＧＷＡＮ接続系とインターネット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無い等、安全が確保された通信をいう。

## ３　情報資産への脅威

情報資産への脅威は、次のとおりとする。

(1)　悪意を持つ者による脅威

悪意を持つアクセス権のない者による行為と、悪意を持つアクセス権のある者による行為を物理的側面及び論理的側面の両面から洗い出し定義した脅威

(2)　あらゆる事故による脅威

情報システムの故障や不具合、不確実な廃棄、委託先倒産等による脅威

(3)　自然災害による脅威
　　地震、落雷、火事等の災害による脅威
(4)　人的ミスによる脅威
　　誤操作、紛失等による脅威

4　適用範囲
(1)　行政機関の範囲
　　市長部局、消防局、教育委員会事務局、選挙管理委員会事務局、公平委員会事務局、監査委員事務局、農業委員会事務局及び議会事務局が保有する情報資産及びこの情報資産に接する職員（会計年度任用職員等を含む。以下同じ。）及び委託事業者等に適用する。
(2)　情報資産の範囲
　　この基本方針が対象とする情報資産は、次のとおりとする。
　①　情報システム及びこれらに関する設備
　②　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　職員の責務等
(1)　職員は、この基本方針を遵守し、情報セキュリティ対策を有効に機能させる責務を負うとともに、職務上知り得た秘密を漏らしてはならない。その職を退いた後も同様とする。
(2)　職員は、職務遂行において、関連法令等に従わなければならない。
(3)　委託事業者に対しては、契約等を通じて、この基本方針を遵守させるための必要な措置を講じるものとする。

6　情報セキュリティ対策
　上記３の脅威から情報資産を守るため、次の情報セキュリティ対策を講じるものとする。
(1)　情報セキュリティの管理体制
　　情報セキュリティの保持のために、全庁的な管理体制を確立する。
(2)　情報資産の分類と管理
　　情報資産は、その内容及び重要性に応じて分類し、それらに応じた適正な対策を講じる。
(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　個人番号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)　物理的なセキュリティ対策
　　情報システムを設置する施設への不正な立入り等による情報資産の損傷、妨害等から保護するため、物理的な対策を講じる。
(5)　人的なセキュリティ対策
　　職員に対して情報セキュリティの重要性を認識させるために情報セキュリティに関する教育及び啓発に努め、職員それぞれの立場における情報セキュリティに関する権限及び責任、情報セキュリティインシデント発生時の対応等を明確にする等、必要な対策を講じる。
(6)　技術的なセキュリティ対策
　　ネットワーク管理、サーバ管理、端末管理、アクセス制御、情報システムの導入、開発、保守、コンピュータウイルス対策等の技術面での対策を講じる。

(7)　運用面におけるセキュリティ対策

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等、運用面の対策を講じる。

また、情報資産への侵害が発生した場合等に迅速かつ適正に対応しなければならない。

(8)　業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、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いた措置を講じる。

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。

## 7　情報セキュリティ監査及び自己点検の実施

この基本方針及び「奈良市情報セキュリティ対策基準」の遵守状況を確認するため、情報セキュリティ監査及び自己点検を実施する。

## 8　評価及び見直し

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、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。

## 9　情報セキュリティ対策基準

本市における情報セキュリティ対策の統一基準となる「奈良市情報セキュリティ対策基準」を定める。

なお、奈良市情報セキュリティ対策基準は、公にすることにより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。

## １０　情報セキュリティ実施手順

この基本方針及び「奈良市情報セキュリティ対策基準」に基づき、情報システムや業務に関する運用管理手順、設計書、マニュアル、ガイドライン等必要となる情報セキュリティ実施手順を作成又は更新するものとする。

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。