奈良県
情報セキュリティ基本方針

平成３１年３月改定

目次

１　目的

この基本方針は、高度情報通信ネットワーク社会の到来に伴い増大する情報への脅威に的確に対応するとともに、個人情報等の県が管理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、必要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、電磁的記録媒体等で構成され、情報処理を行う仕組みをいう。

（３）　全庁共通基盤

情報システムのうち、情報の共有化及び業務の効率化を図るため、全庁で統一的に利用する次の機器及び情報システムをいう。

ア　ファイルサーバ
イ　共通端末
ウ　共通複合機
エ　電子メールシステム
オ　職員認証システム
カ　全庁ネットワークに係るウイルス対策システム
キ　その他アからカに付随する機器及び情報システム

（４）　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。

（５）　情報セキュリティポリシー

この基本方針及び情報セキュリティ対策基準をいう。

（６）　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。

（７）　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。

（８） 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。

（９）番号ネット系

行政手続における特定の個人を識別するための番号の利用等に関する法律に定められた情報提供ネットワークシステムに接続された、同法律に定められた特定個人情報を取り扱う情報システム、データをいう。

（１０）行政ネット系

地方公共団体を相互に接続した行政専用のネットワークである総合行政ネットワーク（以下「ＬＧＷＡＮ」という。）に接続された行政事務で使用する情報システム、データをいう。

（１１）インターネット系

インターネットに接続された情報システム、データをいう。

（１２）通信経路の分割

行政ネット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などにより、コンピュータウイルス等の不正プログラム付着が無い等、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） 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

４ 適用範囲

（１） 組織の範囲

この基本方針が適用される組織は、知事部局、教育委員会、水道局、議会事務局、人事委員会事務局、監査委員事務局、警察本部、労働委員会事務局、選挙管理委員会事務局、収用委員会事務局、及び内水面漁場管理委員会（以下「県」という。）とする。

なお、教育委員会及び警察本部については、知事部局が設置し、かつ管理運用する情報システムを利用する課、室、出先機関（以下「課室等」という。）のみとする。

（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、県が管理するもので、次のものをいう。

ア 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

イ 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。）

ウ 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

職員及び地方公務員法における臨時的に任用される職員、その他の法律により任期を定めて任用される職員（以下「職員等」という。） は、情報資産の取扱いに当たっては、地方公務員法（昭和２５年法律第２６１号）第３４条に規定する秘密を守る義務、奈良県個人情報保護条例（平成１２年３月奈良県条例第３２号）第９条に規定する職員等の義務等関係法規の規定、情報セキュリティポリシー並びに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

県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

情報資産について、機密性、完全性及び可用性を踏まえ、被害を受けた場合に想定される影響の大きさをもとに分類し、当該分類に応じた情報セキュリティ対策を講じる。

（３） 情報システム全体の強靭性の向上

情報システム全体に対し、次の三段階の対策を講じる。

ア　番号ネット系においては、原則として、他の領域との通信をできないようにしたうえで、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。

イ　行政ネット系においては、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、無害化通信を行う。

ウ　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行う。高度な情報セキュリティ対策として、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を行う。

（４） 物理的セキュリティ

情報資産を有する場所への不正な立入りの禁止等、情報資産を損傷、妨害等から保護するために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

情報システム等の情報資産を不正アクセス等から保護するため、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、事故対応手順を策定する。

（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順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。情報セキュリティポリシーの見直しが必要な場合は、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

この基本方針に基づき、情報セキュリティ対策を実施するにあたっての具体的な基準を（遵守事項及び判断基準等）統一的に定めるため、情報セキュリティ対策基準（以下「対策基準」という。）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（以下「実施手順」という。）又は事務マニュアル等を策定するものとする。

なお、実施手順は、公にすることにより情報セキュリティ対策に支障を及ぼすおそれがあるため、非公開とする。

附則

この基本方針は平成１５年４月１日より施行する。

附則

この基本方針は平成２３年４月１日より施行する。

附則

この基本方針は平成２７年１０月５日より施行する。

附則

この基本方針は平成２９年４月１日より施行する。

附則

この基本方針は平成３１年４月１日より施行する。