南丹市情報セキュリティポリシー

＜基本方針＞

2023（令和5）年4月版

（第7版）

2008 年(平成 20 年)　9 月 24 日策　　定
2010 年(平成 22 年)　7 月　1 日一部改定
2013 年(平成 25 年)　4 月　1 日一部改定
2015 年(平成 27 年) 12 月 28 日一部改定
2019 年(令和 元 年)　6 月　7 日一部改定
2020 年(令和 2 年)　3 月 27 日一部改定
2023 年(令和 5 年)　4 月　3 日一部改定

第1章
情報セキュリティ基本方針

1．目的

南丹市（以下「本市」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数含まれている。

本基本方針は、本市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の基本的事項を定めることを目的とする。

2．定義

①ネットワーク

コンピューター等の情報機器を相互に接続する通信回線、通信機器及びそのソフトウェアをいう。

②情報システム

ネットワーク、記録媒体、コンピューター及び周辺機器（これらに登載するソフトウェアを含む。）で構成され、情報処理（データの収集・蓄積・加工・伝達・利用）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、又は防災に関する事務）及び戸籍事務等に関わる情報システム及びデータをいう。

⑨LGWAN接続系

人事給与、財務会計又は文書管理等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。

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

マイナンバー利用事務系、LGWAN接続系、インターネット接続系の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、コンピューター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部外者による意図的な不正アクセス、ウイルス攻撃、サイバー攻撃または不正操作によるデータやプログラムの漏えい・破壊・改ざん・消去・詐取等

②職員及び部外委託者等による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、外部委託管理の不備、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、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、火災等の災害並びに事故、故障によるサービス及び業務の停止など

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、市長部局、教育委員会、選挙管理委員会、公平委員会、監査委員、農業委員会、固定資産評価審査委員会、議会及び地方公営企業をいう。

(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、情報システム及びこれらに関する設備、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、非常勤職員及び臨時職員（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

対象とする脅威から情報資産を保護するため、以下の情報セキュリティ対策を講じる。

（1）組織体制

情報セキュリティ対策の推進と情報資産の適正な管理をするための全庁的な組織体制を確立するものとする。

（2）情報資産の管理と情報の分類

情報資産は、機密性、完全性及び可用性により管理し、必要により作成された情報は、その内容に応じて分類し、その重要度に応じた管理を行うものとする。

（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。

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、京都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

サーバ等、情報システム室等、通信回線等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

コンピューター等の管理、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)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、運用改善を行う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．情報セキュリティ対策基準の策定

本市の情報資産について、情報セキュリティ対策を講ずるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基準を明記した情報セキュリティ対策基準を策定する。

9．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の見直しが必要な場合は見直しを行う。

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市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。

１１．情報セキュリティ対策実施状況の点検

(1)年度点検計画の策定・実施手順の整備

対策推進計画に基づき、担当者等の情報セキュリティ対策実施状況の年度点検計画を策定するとともに、点検実施手順を整備する。

(2)点検の実施

年度点検計画に基づき、担当者等の情報セキュリティ対策実施状況の点検を実施する。

(3)点検結果の評価・改善

点検結果を全体として分析・評価し、点検の結果により明らかになった問題点について、必要な改善を行う。

１２．情報システムの運用継続計画

(1)情報システムの運用継続計画の整備

必要に応じ、情報システムの運用継続計画を策定する。特に、情報提供ネットワークシステムと直接接続する関係システム及びインターフェイスシステムについては、その策定について十分検討を行う。

その際、非常時における情報セキュリティに係る対策事項を検討する。

(2)情報システムの運用継続計画の整合的運用の確保

情報システムの運用継続計画の教育訓練や維持改善を行う際等に、非常時における情報セキュリティに係る対策事項が運用可能であるかを確認する。