鳥取市
情報セキュリティ基本方針

制定　平成１６年４月

改定　令和６年４月

改定履歴

版	改定日	施行日	改定箇所	改定内容
初	平成１６年４月１日	平成１６年４月１日	全章	初版発行
２	平成２８年１月１日	平成２８年１月１日	全章	社会保障・税番号制度導入等に伴う改正
３	令和元年１２月２５日	令和元年１２月２５日	全章	本庁舎移転及びガイドライン改定等に伴う改定
４	令和６年３月３１日	令和６年４月１日	全章	地方公共団体における情報セキュリティポリシーに関するガイドライン(令和５年３月版)に伴う改定など

目　次

１　目的

鳥取市（以下「本市」という。）は、市民の個人情報や行政運営情報など、外部への漏えいやデータの改ざん等の被害を受けた場合に極めて重大な結果を招く情報資産を多数保有している。

したがって、本市が取り扱うこれらの情報資産を盗難や不正アクセスなどの様々な脅威から守ることは、市民の財産やプライバシーを保護するとともに、行政サービスの安定的な運営を図るために必要不可欠である。

本基本方針は、本市が保有する情報資産の機密性・完全性・可用性を維持する対策として、本市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　用語の定義

この基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

⑴　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。

⑵　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。

⑶　記録媒体　磁気式、光学式、半導体メモリ等、電子データとして情報を記録する媒体（ハードディスク、ソリッドステートドライブ、ＵＳＢメモリ、ＳＤカード、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ等）をいう。

⑷　職員等　本市が保有する情報資産に関する業務に携わる全ての職員をいう。

⑸　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。

⑹　情報セキュリティポリシー　本基本方針及び鳥取市情報セキュリティ対策基準をいう。

⑺　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。

⑻　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。

⑼　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。

⑽　住民情報系ネットワーク　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ネットワークをいう。

⑾　ＬＧＷＡＮ系ネットワーク　ＬＧＷＡＮに接続されたネットワークをいう。

⑿　インターネット系ネットワーク　インターネットに接続されたネットワークをいう。

⒀　個別ネットワーク　住民情報系、ＬＧＷＡＮ系及びインターネット系ネットワーク以外のネットワークをいう。

⑭　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　情報セキュリティポリシーの位置付け及び構成

情報セキュリティポリシーは、本市が保有する情報資産に関する情報セキュリティ対策について総合的かつ体系的に取りまとめた情報セキュリティ対策の基本となるものであり、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から構成される。

情報セキュリティ対策基準は、情報セキュリティ基本方針に基づき、情報セキュリティ対策等を実施するために最低限必要な水準として、職員等が遵守すべき事項及び判断基準をまとめたものである。本市では、組織等の状況に合わせた情報セキュリティ対策基準を策定する。

４　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。

⑴　不正アクセス、ウィルス攻撃、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機器又は情報資産の漏えい・破壊・改ざん・消去等、重要情報の詐取、内部不正等

⑵　機器又は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、設定・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、監査機能の不備、業務委託管理の不備、マネジメントの欠陥、機器故障や規定外パソコン接続等の非意図的要因による情報漏えい・破壊・消去等、アクセスのための認証情報又はパスワードの不適切管理

⑶　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

⑷　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

⑸　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

⑴　行政機関の範囲

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が適用される行政機関は、市長事務部局が管理する情報システムを利用する市長事務部局、教育委員会事務局、選挙管理委員会事務局、議会事務局、農業委員会事務局、監査委員事務局、水道局、市立病院、公民館及び他組織等とする。

ただし、学校、保育園、公民館における個別の業務については、セキュリテ

ィ対策基準及び情報セキュリティ実施手順は別途策定し適用範囲外とする。

⑵　情報資産の範囲

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、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（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

職員等及び業務委託者は、情報セキュリティの重要性について共通の認識を持つとともに、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、以下のセキュリティ対策を実施するものとする。

⑴　組織体制

情報セキュリティにおける責任者を明確にし、その責任者に情報セキュリティに関する全ての権限を与える。また、専門組織を設置すると共に、組織横断的なセキュリティ推進体制を確立し、技術的対策のみならず、情報資産を取り扱う職員への教育やセキュリティ事故発生時の対応等の情報セキュリティ対策を円滑に推進・管理する。

⑵　情報資産の分類と管理

本市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。

⑶　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　住民情報系ネットワークにおいては、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系ネットワークにおいては、ＬＧＷＡＮと接続する業務用システムと、インターネット系ネットワーク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　インターネット系ネットワークにおいては、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実施する。

⑷　物理的セキュリティ

サーバ等、サーバ室等、通信回線等及び職員等の端末等の管理について、物

理的な対策を講じる。

⑸　**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。

⑹　**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。

⑺　**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。

⑻　**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、利用に係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。

⑼　**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など、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、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。