# 名取市情報セキュリティポリシー

平成１６年　３月制定
令和　５年　２月改定

名取市情報セキュリティポリシー

目次

# １．情報セキュリティ基本方針

## １．１．目的

名取市の各情報システムが取り扱う情報には、市民の個人情報のみならず行政運営上重要な情報等、外部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。

したがって、これらの情報及び情報を取り扱う情報システムを様々な脅威から防御することは、市民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが名取市に対する市民の信頼の維持向上に寄与するものである。

また、近年における急速な情報化の流れや番号制度の利用拡充等により、ＩＣＴを取り巻く環境は著しく変化しており、名取市がこれらの変化に対応した電子自治体の実現を積極的に推進するためには、すべてのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

そのため、名取市の情報資産の機密性、安全性及び可用性を維持するための対策（情報セキュリティ対策）を整備するために名取市情報セキュリティポリシー（以下「本ポリシー」という。）を定めることとし、このうち、情報セキュリティ基本方針については名取市の情報セキュリティ対策の基本的な方針として、本ポリシーの対象、位置づけ等を定めるものとする。

## １．２．定義

（１）職員　次の①～⑤に該当する本市職員の身分を有する者をいう。

① 副市長
② 教育長
③ 地方公務員法（昭和 25 年法律第 261 号）第 3 条第 2 項に規定する一般職又は同条第 3 項第 3 号に規定する非常勤嘱託員
④ 任期を定めて任用される職員及び再任用職員並びに会計年度任用職員
⑤ 国、他自治体及び外郭団体より本市の組織に配属されている職員

（２）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とその構成機器（ハードウェア及びソフトウェア）をいう。本市の全てのネットワーク（各業務担当部署が独自構築したものを含む）を本ポリシーの適用対象とする。

（３）情報システム

電子計算機（ネットワーク、ハードウェア及びソフトウェア）及び記録媒体で構成され、処理を行う仕組みをいう。

（４）情報資産　次の①～③をいう。

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すべてのデータ（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）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。

（６）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。

（7）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。

（8）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。

（9）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。

（10）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、地方税若しくは防災に関する事務）又は戸籍事務等、住民情報に関わる情報システム及びデータをいう。

（11）LGWAN 接続系
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（マイナンバー利用事務系を除く。）。

（12）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。

（13）通信経路の分割
LGWAN 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。

（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。

## １．３．ポリシーの位置づけと職員等の責務

本ポリシーは、本市が所掌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、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の根幹を成すものである。

したがって、本市が所掌する情報資産に関する業務に携わる職員及び外部委託事業者（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つとともに業務の遂行に当たって本ポリシーを遵守する義務を負うものとする。

## １．４．情報セキュリティ管理体制

本市の情報資産について、その責任を明確にし、対策の実効性を保障するため、情報セキュリティ対策を推進・管理するための体制を確立するものとする。

## １．５．情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

## １．６．情報資産への脅威

本ポリシーを策定するうえで、情報資産を脅かす脅威の発生度合いや発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

（１）職員等でない者による不正アクセス又は不正操作、及びウイルス攻撃・サービス不能攻撃等のサイバー攻撃等による情報資産の持出・盗聴・改ざん・消去、並びに機器及び媒体の盗難等

（２）職員等による意図しない操作あるいは故意による、不正アクセス又は不正操作並びに無許可ソフトウェアの使用等による情報資産の持出・盗聴・改ざん・消去、及び機器や媒体の盗難、並びに規定外の端末接続による情報資産の漏えい等

（３）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、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

（４）地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止等

（５）大規模・広範囲における疾病による要員不足に伴う情報システムの機能不全等

（６）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

## １．７．情報セキュリティ対策

上記１．６で示した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ものとする。

（１）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 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、端末へ情報持ち出し不可設定や多要素認証等を導入することにより、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、自治体情報セキュリティクラウドの導入等を実施する。

（２）物理的セキュリティ対策

情報システムを設置する施設への不正な立ち入り、情報資産への損傷・妨害等か

ら保護するために物理的な対策を講じる。

（3）人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、すべての職員に本ポリシーの内容を周知徹底する等、十分な教育啓発が講じられるように必要な対策を講じる。

（4）技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、端末の管理や情報資産へのアクセス制御、不正プログラム対策やネットワーク管理等の技術的対策を講じる。

（5）運用面セキュリティ対策

情報システム及びネットワークの監視や本ポリシーの遵守状況の確認、情報システム開発等を含む業務委託を行う際のセキュリティ確保等、運用面の対策を講じる。また、緊急事態が発生した場合に迅速な対応を可能とするための、危機管理対策を講じる。

（6）業務委託と外部サービスの利用

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き措置を講じる。

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。

## １．８．情報セキュリティ対策基準の策定

本市の様々な情報資産について、上記１．７の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に定める必要がある。そのため、情報セキュリティ対策を行ううえで必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

## １．９．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を遵守して情報セキュリティ対策を実施するために、個々の情報資産の対策手順をそれぞれ定める必要がある。そのため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、各課室等の長が所掌する情報資産の情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ基本方針は公開し、積極的に情報セキュリティ対策へ取り組む姿勢を内外に示す。一方で、情報セキュリティ対策基準及び実施手順は、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恐れのある情報であることから非公開とする。

## １．10．情報セキュリティ自己点検の実施

情報セキュリティ対策が遵守されていることを検証するため、毎年度又は必要に応じて自己点検を実施する。

## １．11. 評価及び見直しの実施

情報セキュリティ自己点検の結果により、本ポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、本ポリシーの見直しを実施する。