制定日	平成１６年１２月２７日
改定日	令和　４年　４月　１日

いなべ市情報セキュリティ基本方針
（第３版）

制定改定履歴

版 No	制改定 年月日	制改定 理由	制改定 内容	承諾	審査
１版	H16.12.27	初版制定			
２版	H31.3.5	全部改定	本基本方針は平成 31 年４月１日から施行する	H31.3.5	H31.3.5
３版	R4.4.1	総務省「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２年 12 月版）への対応	・定義（３）、(14)、(15)、(16）の追加。 ・他、表記上の軽微な修正。	R4.4.1	R4.4.1

目　　次

1　目的

本基本方針は、本市が保有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、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　定義

（1）ネットワーク（network）

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（information system）

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

（3）情報資産（information assets）

情報システム及びネットワークで取り扱われる全ての情報（電磁的に記録されている情報及び出力した媒体を含む。）をいう。なお、情報資産には紙等の有体物に出力されて情報を含むものとする。

（4）情報セキュリティ（information security）

情報資産の機密の保持並びに正確性及び完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

（5）情報セキュリティポリシー（information security policy）

本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（confidentiality）

情報にアクセスすることが許可された者だけがアクセスできる状態を確実にすること。

（7）完全性（integrity）

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。

（8）可用性（availability）

許可された利用者が必要なときに情報にアクセスできる状態を確実にすること。

（9）職員等（staff etc.）

常勤、非常勤、臨時等の雇用形態を問わず、いなべ市に勤務する者をいう。

(10) 行政接続系（administrative network segment）

個人番号利用事務（社会保障、地方税及び防災に関する事務）、戸籍事務及び内部情報事務（人事給与、財務会計、文書管理等に関する事務）の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) LGWAN（local government wide area network）

地方公共団体の組織内ネットワークを相互に接続し、地方公共団体間のコミュニケーションの円滑化及び情報の共有による情報の高度利用を図ることを目的とする

高度なセキュリティを維持した行政専用のネットワークをいう。

(12) LGWAN 接続系（lgwan network segment）

LGWAN に接続された端末及びその端末で取り扱うデータをいう。

(13) インターネット接続系（internet network segment）

インターネット上で提供される Web サービス（インターネットメール、Web コンテンツの閲覧､情報検索等)を利用する端末及びその端末で取り扱うデータをいう。

(14) 学校情報接続系（intra-school segment）

市内公立小中学校の校務支援事務及び授業支援事務の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。

(15) 通信経路の分割（division of communication path）

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。

(16) 無害化通信（detoxification communication）

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、コンピュータウィ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、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､改ざん及び消去､重要情報の詐取､内部不正

（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、設計又は開発の不備、プログラム上の欠陥、操作又は設定ミス、メンテナンス不備、内部又は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、破壊及び消去

（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

（４）大規模又は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

（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

4　適用範囲

（１）組織の範囲

本基本方針が適用される組織は、市長の内部組織（会計管理者を含む)、教育委員会事務局、農業委員会事務局、監査委員事務局及び議会事務局とする。

（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。

ア　ネットワーク、情報システム及びこれらに関する設備並びに電磁的記録媒体

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、ネットワーク図等のシステム関連文書

5　職員等の守秘義務

職員等は、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は、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に、以下の情報セキュリティ対策を講じる。

（１）組織体制

本市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

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。

（３）情報システム全体のセキュリティの向上

情報システム全体に対し、次の対策を講じる。

ア　行政接続系においては、職員等による情報資産の誤操作や不適切管理による漏えい、外部からのネットワークへの不正アクセス等を防止するため、他の領域との通信をできないようにする。また、端末からの情報持ち出し制限、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　LGWAN 接続系においては、職員等による誤操作や不適切管理による情報資産の漏えい、外部からのネットワークへの不正アクセス等を防止するため、他の領域との通信をできないようにする。

ウ　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講じる。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。

（４）物理的セキュリティ

サーバ、情報システム室、通信回線、職員等の使用する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など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、情報セキュリティポリシーの運用面の対策等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、利用に係る規程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）評価及び見直し

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。

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

上記６、７及び８に規定する情報セキュリティ対策等を実施するために、具体的な遵守事項、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。

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。