知立市情報セキュリティポリシー

知　立　市

平成１５年１０月１４日　策定

令和　３年１０月１８日　改定

情報セキュリティポリシーの改定一覧

版数	改定年月日	情報セキュリティ ポリシーの改定内容	承認者	作成部署
初版	平成１５年１０月１４日	新規制定	情報資産管理会議	企画課 （情報管理係）
２版	平成２５年　3月　４日	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（平成２２年１１月版総務省改定）に準ずる	情報資産管理会議	企画政策課 （情報係）
３版	平成２９年　3月１５日	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（平成２７年３月版総務省改定）に準ずる	情報資産管理会議	企画政策課 （情報係）
４版	平成３１年　3月２９日	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（平成３０年９月版総務省改定）に準ずる	情報資産管理会議	企画政策課 （情報係）
５版	令和　3年１０月１８日	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月版総務省改定）に準ずる	情報資産管理会議	企画政策課 （DX 推進係）

（注意）

（１）本ポリシーを一部改定したときは、当該一部改定に係る部分（影響するページ）を加除方式により差し替え、最新化する。

（２）本ポリシーを全部改定したときには、改定後のポリシーに全てを差し替える。

（３）ポリシー改定の都度、改定の履歴を記載したものと差し替える。

＜目　　次＞

序　情報セキュリティポリシーの構成

情報セキュリティポリシーとは、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とりまとめたものを総称する。情報セキュリティポリシーは、本市が所掌する情報資産を取り扱う全職員に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分『基本方針』と情報資産を取り巻く状況の変化に依存する部分『対策基準』に分けて策定することとした。

具体的には、情報セキュリティポリシーを『第１章 情報セキュリティ基本方針』及び『第２章情報セキュリティ対策基準』の２階層に分け、それぞれを策定するものとする。また、情報セキュリティポリシーに基づき、情報システム毎の具体的な情報セキュリティ対策の実施手順として『情報セキュリティ実施手順』を策定することとする。

情報セキュリティの構成

文書名		内容
情報セキュリティポリシー	第１章　情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	第２章　情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための情報セキュリティ対策の基準
情報セキュリティ実施手順		情報セキュリティ対策基準に基づいた具体的な実施手順

第１章　情報セキュリティ基本方針

１　目的

この基本方針は、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に関する基本的な事項を定めることにより、行政の適正かつ円滑な運営を図り、もって市政に対する市民の信頼を確保することを目的とする。

２　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。

（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、ネットワーク及び電磁的記録媒体及びソフトウェアで構成され、情報処理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

情報資産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

情報資産が破壊、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

情報資産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（個人情報利用事務系）

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）又は戸籍事務等に関わる情報システム及びデータをいう。

（９）　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。）

（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

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。

（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、コンピュータウイルス等の不正プログラムの付着がない等、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）実施機関の範囲

この基本方針を実施する機関は、市長、議会、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及び水道事業管理者の権限を行う市長とする。

（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、次のとおりとする。

ア　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

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、再任用職員、任期付職員、会計年度任用職員（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

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ものとする。

（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行う。

（３）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 接続系においては、LGWAN と接続する業務システムと、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、無害化通信を行う。

③ インターネット接続系においては、愛知県が構築する自治体情報セキュリティクラウドに参加することで、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。

（４）物理的セキュリティ

サーバ、情報システム室、通信回線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な対策を講じる。

（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、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。

クラウドサービスを除く、約款による外部サービスを利用する場合には、機密性のあ

る情報を扱ってはならない。

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する。

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。

１１　違反に対する対応

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。