取扱厳重注意

# 四街道市情報セキュリティポリシー

平成１６年２月　４日　策定
平成１８年２月２４日　改定
平成２８年９月３０日　改定
令和　４年２月１７日　改定
令和　８年３月２５日　改定

＜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、四街道市（以下「本市」という。）の情報資産に関する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を総称する。

また、情報セキュリティポリシーは、本市の情報資産に関する業務に携わる全職員、非常勤職員、会計年度任用職員等（以下、「職員等」という。）及び外部委託事業者に浸透、普及、定着させるものであり、安定的な規範であるものとする。

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。

さらに、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。

したがって、情報セキュリティポリシーの構成は下表のとおりとなる。

情報セキュリティポリシーの構成

| 文　書　名 | | 内　　容 |
|---|---|---|
| 情報セキュリティポリシー | 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 |
| | 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全てのネットワーク及び情報システムに共通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 | | ネットワーク及び情報システム毎に定める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　四街道市情報セキュリティ基本方針

### １　目的

本市が目指す電子自治体を実現するためには、本市の所有するあらゆる情報資産を様々な脅威から保護する統一的な対策を確立することが必要不可欠なことである。

このため、基本方針は、情報セキュリティ対策の普遍的な規範として基本的事項を定めることを目的として策定する。

### ２　定義

（１）パソコン等

複雑な計算を自動的に行う電子計算機類であるパソコン、タブレット、サーバ、シンクライアント、プリンタ等をいう。

（２）ネットワーク

電子計算機を相互に接続するための通信網をいう。

（３）情報システム

電子計算機を用いて特定の業務を処理するための仕組みをいう。

（４）情報資産

ネットワーク及び情報システムで取り扱う全ての情報をいう。

（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）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。

（７）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。

（８）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。

（９）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）又は戸籍事務等に関わる情報システム及びデータをいう。

（10）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）。

（11）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。
（12）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。
（13）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　対象範囲

（1）実施機関
この情報セキュリティ基本方針が対象とする範囲は、市長部局、行政委員会、議会、消防及び地方公営企業とする。
（2）情報資産
本基本方針は、本市が保有する全ての情報資産を対象とする。

## 4　職員等の義務

本市が所掌する情報資産に関する業務に携わる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もつとともに、本基本方針及び情報セキュリティ対策に関する基準、手順等を遵守しなければならない。

## 5　情報セキュリティ管理体制

本市の情報資産について、情報セキュリティ対策を推進・管理するための体制を確立する。

## 6　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。

## 7　情報資産への脅威

情報資産を脅かす脅威の発生度合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）部外者の侵入による機器又は情報資産の破壊・盗難、故意の不正アクセス又は不正操作による機器又は情報資産の破壊・改ざん・消去等

（２）職員等又は外部委託事業者による機器又は情報資産の持出、誤操作、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、故意の不正アクセス又は不正行為による盗聴・破壊・改ざん・消去等（以下「盗聴等」という。）事故等による機器又は情報資産の盗聴、規定外の端末接続による情報資産の、搬送中の漏えい等

（３）コンピュータウィルス、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

（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

## ８　情報セキュリティ対策

上記７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ずるものとする。

（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ずる。

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、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（２）物理的セキュリティ対策

情報システムのうち重要な機器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ずる。

（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、職員等及び外部委託事業者に情報対策の内容を周知徹底する等、十分な教育及び啓発が講じられるように必要な対策を講ずる。

（４）技術及び運用におけるセキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産の

アクセス制御、ネットワーク管理等の技術面の対策、また、システム開発等の外部委託、ネットワークの監視、情報セキュリティ対策の遵守状況の確認等の運用面の対策を講ずる。
また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

（５）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ずる。
また、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、対策を講ずる。
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　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８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。

## 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等をそれぞれ定めていく必要がある。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、課等の長等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。

## １１　非公開の原則

情報セキュリティ対策基準および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恐れがあることから非公開とする。

## １２　情報セキュリティ監査の実施

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、定期的に監査を実施する。

## １３　評価及び見直しの実施

情報セキュリティ監査の結果等により、情報セキュリティ対策の評価を実施するとともに、見直しを実施する。