

八千代市情報セキュリティポリシー

第8版

令和8年4月1日

目 次

序章	セキュリティポリシーの構成	1
第1章	情報セキュリティ基本方針	2
1	目的	2
2	定義	2
3	対象とする脅威	3
4	適用範囲	4
5	職員等の遵守義務	4
6	情報セキュリティ対策	5
7	情報セキュリティ監査及び自己点検の実施	6
8	情報セキュリティポリシーの見直し	6
9	情報セキュリティ対策基準の策定	6
10	情報セキュリティ実施手順の策定	6

序章 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、八千代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を総称する。情報セキュリティポリシーは、八千代市が所掌する情報資産に関する業務に携わる常勤職員、非常勤職員等（以下、「職員等」という。）並びに委託事業者に浸透、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、①情報セキュリティ基本方針、②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こととする。また、情報セキュリティポリシーに基づき、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に規定するセキュリティ対策を実施するために定めた具体的な遵守事項及び判断基準等
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

今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。一方で、個人情報の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん・システム障害等が後を絶たない。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。

八千代市は、市民の個人情報や行政運営上の情報などの極めて重要な情報を多数取り扱っている。また、ICT化が進み、多くの業務が情報システムやネットワークに依存している。したがって、これらの情報資産を様々な脅威から防御することは、市民の権利、利益を守るため、また、安定的、継続的な行政運営のためにも必要不可欠である。

これらの状況に鑑み、本基本方針は八千代市の情報資産の機密性、完全性、可用性を維持するため、八千代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

八千代市における市長部局、行政委員会、議会事務局、消防本部及び消防署、上下水道局及び教育委員会に設置された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で構成され、情報処理を行う仕組みをいう。

(3) 情報資産

本市のネットワーク及び情報システムそのもの並びにこれらに関する設備・機器、これらで取り扱う情報等をいう。

(4) 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。

(5) 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。

- (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、必要な時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、重要情報の搾取、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，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因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) 対象機関の範囲

本基本方針が適用される行政機関は，市長部局，行政委員会，議会事務局，消防本部及び消防署，上下水道局及び教育委員会とする。

(2) 情報資産の範囲

本対策基準が対象とする情報資産は，次のとおりとする。ただし，教育ネットワーク，教育情報システムに関するものは除く。

- ① 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
- ② 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。）
- 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

情報資産の種類	情報資産の例
ネットワーク	通信回線，ルータ等の通信機器等
情報システム	サーバ，パソコン，モバイル端末，プリンタ，ソフトウェア等
これらに関する施設・設備	マシン室，通信分電盤，配電盤，電源ケーブル，通信ケーブル等
電磁的記録媒体	各種機器に内蔵される電磁的記録媒体，USBフラッシュメモリ，DVD-R，外付ハードディスク等の外部電磁的記録媒体等
ネットワーク及び情報システムで取り扱う情報	ネットワーク，情報システムで取り扱うデータ，これらを印刷した文書等
システム関連文書	システム設計書，プログラム仕様書，ネットワーク構成図等

5 職員等の遵守義務

常勤職員，非常勤職員等（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) 組織体制

八千代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ものとする。

(3) 情報システム全体の強靱性の向上

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。

(4) 物理的セキュリティ対策

サーバ、情報システム室、通信回線等及び職員等のパソコン等の管理について、物理的な対策を講ずる。

(5) 人的セキュリティ対策

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対策

コンピュータ等の管理、ネットワーク管理、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、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ずる。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。

(8) 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。

(9) 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。情報セキュリティポリシーの見直しが必要な場合は、適宜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が職員等により遵守されていることを検証するため、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な対策が必要となった場合には、情報セキュリティポリシーの見直しを行う。

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、情報セキュリティ対策基準及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おそれがあることから原則非公開とする。