

多摩市情報システム  
管理運営基準  
(基本方針)

令和8年2月10日

## 目次

1	目的	2
2	定義	2
3	対象とする脅威	3
4	適用範囲	4
	(1) 行政機関の範囲	4
	(2) 情報資産の範囲	4
5	職員等の遵守義務	4
6	情報セキュリティ対策	4
	(1) 組織体制	4
	(2) 情報資産の分類と管理	4
	(3) 情報システム全体の強靱性の向上	4
	(4) 物理的セキュリティ	5
	(5) 人的セキュリティ	5
	(6) 技術的セキュリティ	5
	(7) 運用	5
	(8) 業務委託と外部サービス（クラウドサービス）の利用	5
	(9) 評価・見直し	6
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

## 1 目的

本基本方針は、多摩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、多摩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

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

市の業務を電算処理するために必要なコンピュータ、ネットワーク、ソフトウェア、電子記録媒体、業務情報等の体系で構成され、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

多摩市情報システムの管理運営に関する条例（以下、「システム条例」という。）第12条第1項の規定に基づいて策定する「多摩市情報システム管理運営基準（以下、「管理運営基準」という。）をいう。

### (5) 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。

### (6) 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。

### (7) 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。

### (8) マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務又は戸籍事務等に関わる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。

### (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。

### (11) 通信経路の分割

LGWAN接続系とインターネット接続系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無い等、安全が確保された通信をいう。

#### (13) 重要情報

「多摩市情報システムの管理運営に関する条例第3条第5号」に規定する重要情報のことで、市の行政運営上必要な情報のうち、個人情報を除くもので、その機密性又は正確性が損なわれた場合、市に著しい損害を与える恐れがあるものをいう。

#### (14) 職員等

「多摩市情報システムの管理運営に関する条例第3条第7号」に規定する職員のことで、市の実施機関に所属する全ての職員（議員、教育委員会の教育長及び委員、選挙管理委員会の委員、農業委員会の委員、固定資産評価審査委員会の委員及び監査委員含む）をいう。

#### (15) 業務情報

「実施機関ごとに定める情報システムの管理運営に関する規則(又は規程)第2条第1号」に規定する業務情報のことで、市の所掌事務を処理するために必要な情報をいう。

#### (16) 個人情報

生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。【番号法第2条第3項、個人情報保護法第2条第1項】

#### (17) 特定個人情報

個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。番号法第7条第1項及び第2項、第8条並びに第51条並びに附則第3条第1項から第3項まで及び第5項を除く。）をその内容に含む個人情報をいう。【番号法第2条第8項】

#### (18) 外部記録媒体

コンピュータシステムにおいて情報を記録する電子記録媒体のうち、USBメモリ、DVD等の取り外し可能なものをいう。

### 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、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な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) 行政機関の範囲

本基本方針が適用される行政機関は、多摩市情報システムの管理運営に関する条例第3条第6号に実施機関として定義されている市長（下水道事業の管理者の権限を行う市長を含む。）、教育委員会、監査委員、選挙管理委員会、農業委員会、固定資産評価審査委員会及び議会とする。

##### (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、電子記録媒体
- 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本管理運営基準並びに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

前記の項番3の「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

多摩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

多摩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ことを原則とする。

ア 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。

イ 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、無害化通信を行う。

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

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、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じる。

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、緊急時対応計画の策定等必要な対策を講じる。

#### (8) 業務委託と外部サービス（クラウドサービス）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（クラウドサービス）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、利用する課の

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。

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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、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必要に応じて策定する。

なお、情報セキュリティ対策基準は、公にすることにより多摩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。

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実施手順書を必要に応じて策定するものとする。

なお、実施手順書は、公にすることにより多摩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。