○三鷹市情報セキュリティ基本方針

令和８年４月１日制定

三鷹市(以下「市」という。) が保有する情報は、市民全体の共有財産であり、市は、市民の信託によりこれを管理し、利用している。市は、これらの情報を安全に管理し、利用するため、情報セキュリティの管理を行う。

第１ 目的

この基本方針は、情報の漏えい、改ざん、盗難等を防止することにより、業務の中断及び社会的信用の失墜を防止するとともに、すべての職員等が情報セキュリティの必要性及び責任について理解を深め、情報の適切な管理を継続する体制を整備することを目的とする。

第２ 定義

１ この基本方針において「機密性」とは、アクセスを認可された者のみが、情報にアクセスできることをいう。

２ この基本方針において「完全性」とは、情報及びその処理方法が正確かつ完全であることをいう。

３ この基本方針において「可用性」とは、情報を必要とするときにアクセスを認可された者が、情報にアクセスできることをいう。

４ この基本方針において「情報セキュリティ」とは、情報の機密性、完全性及び可用性を維持することをいう。

５ この基本方針において「リスク評価」とは、個々の情報の重要性及び情報セキュリティに対する脅威の発生の可能性を評価することをいう。

６ この基本方針において「職員等」とは、一般職の職員、特別職の職員、議員、会計年度任用職員、市と業務委託契約を締結した事業者、市に派遣された作業員等情報を業務上利用するすべての者をいう。

７ この基本方針において「情報システム」とは、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。

８ この基本方針において「情報セキュリティポリシー」とは、この基本方針及び情報セキュリティ対策基準をいう。

９ この基本方針において「マイナンバー利用事務系」とは、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 この基本方針において「LGWAN 接続系」とは、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 この基本方針において「インターネット接続系」とは、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 この基本方針において「通信経路の分割」とは、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 この基本方針において「無害化通信」とは、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。

第 3 対象となる情報の範囲

この基本方針の対象は、市、行政委員会及び市議会が業務上取り扱うすべての情報（電子データ、書類として保有する情報。ただし、議員又は会派が保有する議員活動又は会派活動に関する情報等を除く。）とする。

第 4 情報セキュリティの管理の基本的なあり方

情報及び情報を作成するために使用するソフトウェア並びに当該情報の作成、保管及び利用をするために使用する機器及び媒体を市が保有する他の資産と同様に、自治体経営に欠くべからざる重要な資産と位置付け、継続的に管理することを基本的なあり方とする。

第 5 基本方針の位置付け

1 この基本方針は、市の情報セキュリティに関する最上位の基準とする。

2 市の情報セキュリティに関するガイドライン、取扱要領等は、この基本方針に基づき、策定されなければならない。

3 この基本方針に定める事項の具体的な対策基準及び手順については、総務省が定める「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」を参考にするものとする。

4 法令、条例等に定めのある事項については、その定めるところによる。

第 6 職員等の責務

職員等は、情報の漏えい、改ざん、盗難等を防止するため、この基本方針に基づき、適切な情報セキュリティの管理を継続的に行わなければならない。

第 7 情報セキュリティの管理体制

1 情報セキュリティの管理を適切に行うため、情報セキュリティ統括責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報セキュリティ担当者、情報システム責任者、情報システム管理者、庁舎・文書責任者、庁舎管理者及び文書管理者並びに情報セキュリティ監査担当を置く。

2 情報セキュリティに関する重要事項の検討、承認等を行うため、情報セキュリティ運営委員会を置き、別に定める者をもって構成する。

3 情報セキュリティ統括責任者は、市長の指示を受け、市におけるすべての情報セキュリティを統括するものとし、企画部に関する事務を分担する副市長をもって充てる。また、情報セキュリティインシデントに対処するための体制（CSIRT：Computer Security Incident Response Team、以下「CSIRT」という。）を整備し、役割を明確化する。

4 情報セキュリティ責任者は、各部における情報セキュリティの管理を行うものとし、各部の長（行政委

員会事務局及び議会事務局においてはその長）をもって充てる。
5　情報セキュリティ管理者は、情報セキュリティ責任者の下で各課における情報セキュリティの管理を行うものとし、各課の長（行政委員会事務局及び議会事務局においてはその長の指名する職員）をもって充てる。
6　情報セキュリティ担当者は、情報セキュリティ管理者の下で各課における情報セキュリティの運用を行うものとし、情報セキュリティ管理者の指名する職員をもって充てる。
7　情報システム責任者は、市における情報システムに関する統括的な権限及び責任を有するものとし、企画部長をもって充てる。
8　情報システム管理者は、情報システム責任者の下で市における情報システムの管理を行うものとし、企画部情報推進課長をもって充てる。
9　庁舎・文書責任者は、庁舎における物理的セキュリティ(部外者の侵入、事故、災害等による障害から情報を保護することをいう。）の管理及び文書の管理を行うものとし、市長部局及び教育委員会を除く行政委員会においては総務部長をもって充て、教育委員会においては教育委員会事務局教育部長をもって充て、市議会においては議会事務局長をもって充てる。
10　庁舎管理者は、庁舎・文書責任者の下で庁舎における物理的セキュリティの管理を行うものとし、市長部局及び教育委員会を除く行政委員会においては総務部契約管理課長をもって充て、教育委員会においては教育委員会事務局教育部総務課長をもって充て、市議会においては議会事務局次長をもって充てる。
11　文書管理者は、庁舎・文書責任者の下で文書の管理を行うものとし、市長部局及び教育委員会を除く行政委員会においては総務部政策法務課長をもって充て、教育委員会においては教育委員会事務局教育部総務課長をもって充て、市議会においては議会事務局次長をもって充てる。
12　情報セキュリティ監査担当は、情報セキュリティの管理の状況を監査することとし、情報セキュリティ統括責任者が指名する職員をもって充てる。
13　CSIRT は、情報セキュリティ統括責任者の指揮の下、インシデントの検知、分析、影響評価、封じ込め、復旧及び再発防止策の検討を行うものとし、情報システム管理者が指名する職員をもって充てる。

第 8　情報の管理及びリスク評価
1　情報セキュリティ責任者は、担当する部で扱うすべての情報について、機密性、完全性及び可用性の観点から定期的に評価を行い、その重要度に応じて分類し、総務省が定める「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」等を参考に、適切に管理しなければならない。
2　情報セキュリティ責任者は、担当する部で扱うすべての情報について、情報セキュリティ管理者を明確にしたうえで、リスク評価に応じて管理しなければならない。
3　情報セキュリティ責任者は、情報資産の分類に応じ、その作成、入手、利用、保管、運搬、提供及び廃棄に至るまでのライフサイクル全般にわたり、適切な物理的、人的及び技術的セキュリティ対策が確保されるよう配慮するものとする。
4　情報システム責任者及び情報システム管理者は、情報システム全体に対し、マイナンバー利用事務

系、LGWAN 接続系、インターネット接続系の三層の対策を講じるものとし、LGWAN 接続系とインターネット接続系との通信は、無害化通信等の措置により安全を確保しなければならない。

第 9　情報の取扱い

1　情報セキュリティ管理者は、取扱う情報について、業務上必要な者に必要最小限の権限を与えて、利用するものとし、利用者 ID 及びパスワード等の認証情報を厳重に管理しなければならない。特に、特権 ID（システム管理者権限）は利用者を限定し、利用記録を保持する等、適切な管理策を講じるものとする。

2　情報セキュリティ管理者は、業務上必要な情報を適時に利用できるようにするため、適切な管理体制を構築するものとする。

3　職員等は、業務以外の目的で情報資産（端末、ネットワーク、電子メールアドレス等）の利用を行ってはならない。

4　職員等は、情報セキュリティ管理者の許可なく、支給された端末のセキュリティ設定を変更してはならない。また、庁内ネットワーク及び情報システムへの不正アクセスを試みてはならない。

第 10　業務委託契約及び外部サービス

1　第三者との業務委託契約の締結に際して、市の情報を確実に保護するため、必要な機密保護に関する対策及び情報セキュリティに関する障害等が発生した場合の責任について定めなければならない。

2　情報システム責任者は、外部サービス（クラウドサービスを含む。）を利用する場合、その特性と責任分界点を明確にし、取り扱う情報の分類に応じて、利用の可否及びセキュリティ対策の基準を定めなければならない。

第 11　監視

情報セキュリティ責任者は、各部においてこの基本方針が適切に運用されているかどうか継続的に監視しなければならない。

第 12　監査

1　情報セキュリティ監査担当は、この基準の運用について定期的に監査し、その結果を情報セキュリティ統括責任者に報告しなければならない。

2　監査は、被監査部門から独立した者に対して実施を依頼し、その客観性を確保しなければならない。また、業務委託事業者（再委託事業者を含む。）に対しても、情報セキュリティポリシーの遵守について定期的に監査を行わなければならない。

第 13　報告

職員等は、情報セキュリティに関する障害等を発見した場合は、別に定める方法により、市長、情報セキュリティ統括責任者、情報セキュリティ責任者又は情報セキュリティ管理者に報告しなければならない。

第 14　事業継続管理

1　市の事業の継続性を確保するため、災害又は重大な障害等による市の業務の中断を防止し、迅速な復旧を図るための対応策等をあらかじめ定めなければならない。

2　市の業務に多大な影響のある災害又は重大な障害等が発生した場合には、業務への影響を減少させ、迅速な復旧を図るため、一時的な業務の中断を含む対応策をあらかじめ定めなければならない。

第 15　物理的セキュリティ対策

1　情報システム管理者は、サーバ等の機器を設置する際には、火災、水害、埃、振動、温度、湿度等の外的要因の影響を可能な限り排除した安全な場所に設置し、容易に取り外しができないよう適切に固定する等、必要な措置を講じなければならない。

2　重要情報を格納するサーバ、セキュリティサーバ、住民サービスに関するサーバ及びその他の基幹サーバについては、冗長化を行い、同一データを保持することが推奨される。また、メインサーバに障害が発生した場合には、速やかにセカンダリサーバを起動することで、システムの運用停止時間を最小限に抑えることが推奨される。

3　情報システム管理者は、情報セキュリティ統括責任者及び庁舎管理者と連携し、サーバ等の機器の電源について、停電等の電源供給停止に備え、機器が適正に停止するまで十分な電力を供給できる容量の予備電源を備え付けなければならない。また、落雷等による過電流に対しても、サーバ等の機器を保護するための適切な措置を講じなければならない。

4　情報セキュリティ統括責任者及び情報システム管理者は、庁舎管理者と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために配線収納管の使用など必要な措置を講じることが求められる。主要箇所のケーブルについて損傷等の報告があった場合は、速やかに連携して対応しなければならない。さらに、ネットワーク接続口（ハブのポート等）は他者が容易に接続できない場所に設置し、適正に管理することが重要である。配線の変更や追加については、情報システム担当者や契約事業者以外の者が行えないよう、必要な措置を実施しなければならない。

5　情報システム管理者は、サーバ等の機器について定期的な保守を実施しなければならない。また、電磁的記録媒体を内蔵する機器を事業者に修理させる際には、内容を消去した状態で行わせ、内容の消去が困難な場合は、守秘義務契約の締結や秘密保持体制の確認等を徹底しなければならない。

6　統括情報セキュリティ責任者及び情報システム管理者が庁外にサーバ等の機器を設置する場合は、CISO の承認を得るとともに、定期的に当該機器への情報セキュリティ対策状況を確認しなければならない。

7　機器の廃棄、リース返却等を行う際には、情報システム管理者は機器内部の記憶装置からすべての情報を消去し、復元不可能な状態にする措置を徹底しなければならない。

第 16　職員研修

情報セキュリティ責任者は、その所管する職員等に対して、職務に応じて必要な情報セキュリティに関する職員研修を定期的に実施しなければならない。

第 17　情報システム全体の強靭性の向上

1　情報システム責任者及び情報システム管理者は、業務の効率性・利便性を考慮しつつ、情報システム全体に対し、マイナンバー利用事務系、LGWAN 接続系、インターネット接続系の三層の対策を講じることを原則とする。

2　LGWAN 接続系とインターネット接続系の通信経路を論理的又は物理的に分離しなければならない。両環境間で通信を行う際は、インターネットメールの本文テキスト化、端末への画面転送等により無害化通信を図るか、その他の適切な措置により安全を確保しなければならない。

3　マイナンバー利用事務系は、原則として他の領域との通信をできないようにし、端末からの情報持ち出し不可設定や多要素認証の導入等により、住民情報の流出を防止しなければならない。

第 18　技術的セキュリティ対策

1　すべての情報システム及び端末に対し、不正プログラム対策ソフトウェア（アンチウイルスソフト）を導入し、常に最新の状態に維持しなければならない。また、外部から入手するファイル、特に電子メールの添付ファイルについては、適切な無害化処理及び確認を経るものとする。

2　情報システムへのアクセスは、情報セキュリティ管理者が定めたアクセス権限に基づき行われなければならない。パスワードは推測されにくいものを設定し、定期的に変更することを義務付ける等、識別・認証に関する厳格な基準を設けなければならない。

3　情報システム責任者及び情報システム管理者は、情報システムの運用において、各種ログ（アクセス、操作等）の取得及び定期的な監視を常時実施し、システムのセキュリティ機能が適切に運用されるよう維持しなければならない。また、使用するソフトウェアの脆弱性対策を計画的に実施しなければならない。

4　ネットワーク及びサーバに対して、不正アクセス検知システム（IDS/IPS）の導入や、使用されていないポートの閉鎖、不要なサービスの停止等により、外部からの不正な侵入を防御する対策を講じなければならない。

第 19　保険

情報セキュリティに関する損害を軽減させるために、必要に応じて保険に加入しなければならない。

第 20　関連法規等の遵守

1　職員等は、情報セキュリティに関係する法令、条例等を遵守しなければならない。
2　情報セキュリティ責任者は、情報の保護及び取扱いに関する法令、条例等を識別し、それに応じた情報の管理の方法を定めなければならない。
3　市は、業務委託契約に定める事項を遵守しなければならない。

第 21　違反行為に対する処分

この基本方針に違反する行為を行った職員等に対しては、法令、条例、契約書等に定めるところにより処分するものとする。

第 22　特例

技術、経費等の理由により、この基本方針に定める事項を達成することが困難であると認められる場合は、情報セキュリティ運営委員会の承認を受け、別に定めるところにより情報セキュリティの管理を行うことができる。

第 23　基本方針の見直し

情報セキュリティ統括責任者は、情報の種別及び構成並びに当該情報の作成、保管及び利用など、リスク評価の基礎事項に影響を及ぼす変化に対応して、別に定める手続に従い、この基本方針の見直しを行わなければならない。

第 24　基本方針の改廃

この基本方針を改正し、又は廃止をするときは、情報セキュリティ運営委員会の承認を得なければならない。

第 25　他のセキュリティ管理体制との関係

この基本方針及びこの基本方針に定める情報セキュリティ対策は、市における情報セキュリティ対策の最低限の基準を定めるものである。情報セキュリティマネジメントシステム（ISMS）等の本ポリシーを上回るセキュリティ水準を定めた管理体制を既に導入している部局においては、当該管理体制を優先して適用することができる。ただし、当該管理体制は、この基本方針の目的及び要求事項を確実に満たすものでなければならない。