

○三鷹市情報セキュリティ基本方針

平成15年10月16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、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。

第3 対象となる情報の範囲

この基本方針の対象は、市が電子データ及び書類として保有するすべての情報

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 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。
- 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。

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、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。

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。

第10 業務委託契約

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。

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

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。

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 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実施しなければならない。

第16 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17 関連法規等の遵守

- 1 職員等は、情報セキュリティに係る法令、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18 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19 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20 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21 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。

附 則

この基本方針は、平成15年10月16日から施行する。

附 則（平成16年4月1日施行）

この基本方針は、平成16年4月1日から施行する。

附 則（平成19年4月1日施行）

この基本方針は、平成19年4月1日から施行する。

附 則（平成20年5月16日施行）

この基本方針は、平成20年5月16日から施行し、平成20年4月1日から適用する。

附 則（平成20年10月1日施行）

この基本方針は、平成20年10月1日から施行する。

附 則（平成22年4月28日22三企情第146号）

この基本方針は、平成22年4月28日から施行し、平成22年4月1日から適用する。

附 則（令和2年4月1日制定）

この基本方針は、令和2年4月1日から施行する。