

東大和市訓令第 号

東大和市保有個人情報管理規程を次のように定める。

平成27年 月 日

東大和市長 尾崎 保夫

東大和市保有個人情報管理規程

目次

- 第1章 総則（第1条—第3条）
- 第2章 管理体制（第4条—第11条）
- 第3章 教育研修（第12条）
- 第4章 保有個人情報の取扱い（第13条—第19条）
- 第5章 情報システムにおける安全の確保等（第20条—第25条）
- 第6章 サーバ室等の安全管理（第26条）
- 第7章 事務の委託等（第27条・第28条）
- 第8章 安全確保上の問題への対応（第29条—第31条）
- 第9章 監査及び点検の実施（第32条—第34条）
- 第10章 雑則（第35条・第36条）

附則

第1章 総則

（趣旨）

第1条 この規程は、別に定めがあるものを除くほか、東大和市個人情報保護条例施行規則（平成18年規則第2号）第7条等の規定により、東大和市（以下「市」という。）における保有個人情報等の漏えい、滅失及び毀損の防止その他の適正な管理のために必要な措置について定めるものとする。

（定義）

第2条 この規程における用語の意義は、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号。以下「番号法」という。）及び東大和市個人情報保護条例（平成17年条例第33号。以下「保護条例」という。）の例による。

（職員の責務）

第3条 職員は、番号法及び保護条例の規定並びに次条に規定する最高統括責任者、第5条第1項に規定する統括管理者及び第6条第1項に規定する情報責任者の指示に従い、保有個人情報を適正に取り扱わなければならない。

第2章 管理体制

(最高統括責任者)

第4条 保有個人情報の管理に関する事務を統括するため、保有個人情報最高統括責任者（以下「最高統括責任者」という。）を置き、副市長をもって充てる。

(統括管理者)

第5条 最高統括責任者を補佐するため、保有個人情報統括管理者（以下「統括管理者」という。）を置き、総務部長をもって充てる。

2 統括管理者は、最高統括責任者の命を受けて、保有個人情報の保護について、次条第1項に規定する情報責任者、第8条第1項に規定する統括責任者、第9条第1項に規定する情報システム管理者その他の職員に対して必要な指示をするとともに、最高統括責任者に事故があるとき又は最高統括責任者が欠けたときは、その職務を代理する。

(情報責任者)

第6条 課（東大和市会計事務規則（平成22年規則第6号）第2条第2号に規定する課をいう。以下同じ。）における保有個人情報の管理に関する事務を統括するため、保有個人情報責任者（以下「情報責任者」という。）を置き、課長（同条第3号に規定する課長をいう。）をもって充てる。

2 情報責任者は、課における保有個人情報の管理に関する権限及び責任を有する。

(特定個人情報取扱者)

第7条 情報責任者は、特定個人情報を取り扱う職員（以下「特定個人情報取扱者」という。）を指定する。

2 情報責任者は、特定個人情報取扱者の担当事務及び当該事務において取り扱う特定個人情報の範囲を指定するとともに、その職務を監督する。

(統括責任者)

第8条 保有個人情報の管理に関する実務を統括するため、保有個人情報統括責任者（以下「統括責任者」という。）を置き、総務部文書課長をもって充てる。

2 統括責任者は、次に掲げる事務を担当する。

(1) 保有個人情報の管理に係る連絡調整等

(2) 特定個人情報を利用する事務を複数の課において処理する場合における各情報責任者の特定個人情報の管理に関する任務の分担の調整

(情報システム管理者)

第9条 保有個人情報を取り扱う情報システムの管理に関する実務を統括するため、保有個人情報システム管理者（以下「情報システム管理者」という。）を置き、総務部情報管理課長をもって充てる。

2 情報システム管理者は、保有個人情報を取り扱う情報システムの運用における保有個人情報の保護に必要な措置について連絡調整等を担当するものとする。

(監査責任者)

第10条 保有個人情報の管理の状況について監査するため、保有個人情報監査責任者（以下「監査責任者」という。）を置き、最高統括責任者が指名する職員をもって充てる。

2 監査責任者は、第32条の規定により、保有個人情報の適正な管理を検証するための監査を行うものとする。

(保有個人情報の管理のための会議)

第11条 最高統括責任者は、保有個人情報の管理に係る重要事項の決定、連絡調整等を行うため必要があると認めるときは、関係職員を構成員とする会議を開催することができる。

第3章 教育研修

第12条 最高統括責任者は、保有個人情報の取扱いに従事する職員に対し、保有個人情報の保護の必要性について理解を深め、保有個人情報を適正に取り扱うために必要な教育研修を実施するものとする。

2 最高統括責任者は、保有個人情報を取り扱う情報システムの管理に関する事務に従事する職員に対し、情報システムにおいて保有個人情報を適正に保護するために必要な教育研修を実施するものとする。

3 最高統括責任者は、情報責任者に対し、課における保有個人情報の適正な管理のために必要な教育研修を実施するものとする。

4 情報責任者は、第1項及び第2項の規定により最高統括責任者が実施する研修について、所属の職員が参加できるよう、十分な配慮をしなければならない。

第4章 保有個人情報の取扱い

(保有個人情報を取り扱う権限の制限)

第13条 情報責任者は、保有個人情報を取り扱う権限を有する者を、事務処理上必要最小限の職員に限らなければならない。

2 前項の権限を有する職員は、事務の目的以外の目的で保有個人情報を取り扱ってはならない。

3 第1項の権限を有しない職員は、保有個人情報を取り扱ってはならない。

(複製等の制限)

第14条 職員は、次に掲げる行為については、情報責任者の指示に従い行わなければならない。

(1) 保有個人情報の複写及び複製

(2) 保有個人情報の送信

(3) 保有個人情報が記録されている媒体（以下「記録媒体」という。）の外部への送付又は持出し

(4) その他保有個人情報の適正な管理に支障を及ぼすおそれのある行為
(誤りの訂正)

第15条 職員は、保有個人情報の内容に誤り等を発見した場合には、情報責任者の指示に従い、訂正等を行わなければならない。

(記録媒体の管理等)

第16条 職員は、情報責任者の指示に従い、記録媒体を施錠できる保管庫等で保管しなければならない。

2 職員は、記録媒体を移動させる場合には、紛失、盗難等に留意しなければならない。

(廃棄等)

第17条 情報責任者は、保有個人情報又は記録媒体（端末機及びサーバに内蔵されているものを含む。）が不要となった場合には、速やかに当該保有個人情報の復元又は判読が不可能となる方法により当該保有個人情報の消去又は当該記録媒体の廃棄を行わなければならない。

(取扱状況の把握)

第18条 情報責任者は、保有個人情報の秘匿性等その性質に応じて、当該保有個人情報の利用、保管等の取扱いの状況について把握しておかななければならない。

(特定個人情報の利用の制限等)

第19条 特定個人情報取扱者は、番号法第9条各項に定める場合を除き、個人番号を利用してはならない。

2 特定個人情報取扱者は、番号法第19条各号に定める場合を除き、特定個人情報を提供してはならない。

3 特定個人情報取扱者は、番号法第19条各号に規定する場合を除き、特定個人情報の提供を求め、並びに特定個人情報を収集し、及び保管してはならない。

4 特定個人情報取扱者は、番号法第28条に規定する場合を除き、個人番号利用事務及び個人番号関係事務を処理するために必要な範囲を超えて特定個人情報ファイルを作成してはならない。

5 情報責任者は、特定個人情報を取り扱う事務の執務をする区域及び特定個人情報ファイルを取り扱う情報システムを管理する区域を明確にし、物理的な安全管理措置を講じなければならない。

第5章 情報システムにおける安全の確保等

(情報システムにおける保護措置)

第20条 情報責任者又は情報システム管理者は、保有個人情報（情報システムで取り扱うものに限る。第21条第3号を除き、以下この章において同じ。）の秘匿性等その性質に応じて、情報システムにおける技術的及び物理的な安全管理措置とし

て次に掲げるものを講じなければならない。ただし、その性質上必要がないと認められる事項については、この限りでない。

- (1) 保有個人情報を取り扱う情報システムにおけるアクセスの制御のために行うパスワード及び認証符号を使用して権限を識別する機能を設定する等の措置並びにパスワード及び認証符号の適正な管理のために行う取扱基準の制定等の措置
- (2) 情報システムにおける適正なアクセスの維持のために行うアクセス状況についての記録、保存及び分析並びに当該記録の改ざん等の防止に関する措置並びに不適切なアクセスを警告する等のアクセス状況の監視に関する措置
- (3) 管理者権限（情報システムのプログラムに係る構成について変更等を行うことができる権限であって、当該プログラムにおいて定められたものをいう。）が不正取得された場合の影響を最小化するために行う管理者権限の範囲の制限に関する措置
- (4) 外部からの不正アクセスを防止するために行う情報システムにファイアウォールを設定する等の措置
- (5) 不正プログラムによる保有個人情報の漏えい、滅失又はき損（以下「漏えい等」という。）の防止のために行う情報システムのソフトウェアの更新等の脆弱性の解消等の措置
- (6) 保有個人情報の漏えい等の防止のために行う情報システムの端末機等に記録機能を有する機器又は媒体を接続することの制限等の措置
- (7) 保有個人情報の破損等の事故に備えるために行うバックアップを作成し、分散管理を行う等の措置
- (8) 特定個人情報の保管又は送信における安全確保のために行う特定個人情報の暗号化等の措置

（情報システムで取り扱う保有個人情報の遵守事項）

第21条 職員は、情報システムで取り扱う保有個人情報については、次に掲げる事項を遵守しなければならない。

- (1) 保有個人情報の複写又は複製をする場合は、第14条の規定による指示に従うほか、複写又は複製をする範囲を必要最小限にすること。
- (2) 複写又は複製をした保有個人情報は、事務の処理後は速やかに消去すること。
- (3) 保有個人情報を情報システムに入力する場合は、入力前後の情報について照合を行うこと。

（情報システム設計書等の管理）

第22条 情報責任者又は情報システム管理者は、保有個人情報に係る情報システムの設計書、構成図等に係る文書の保管、複製、廃棄等をしようとする場合は、漏えい等を防止するために必要な措置を講じなければならない。

(端末機の限定)

第23条 情報責任者又は情報システム管理者は、保有個人情報の秘匿性等その内容に応じて、その処理を行う端末機を限定しなければならない。

2 前項の保有個人情報を取り扱う職員は、同項の規定により使用が認められた端末機以外の端末機を使用してはならない。

(端末機の盗難防止等)

第24条 情報責任者又は情報システム管理者は、端末機の盗難又は紛失の防止のため、端末機の固定、執務室の施錠等の必要な措置を講じなければならない。

2 職員は、情報責任者又は情報システム管理者が認める場合を除き、端末機を外部に持ち出し、又は外部から持ち込んで서는ならない。

(端末機の使用における注意事項)

第25条 職員は、端末機の使用に当たっては、保有個人情報が第三者に閲覧されることがないようにしなければならない。

第6章 サーバ室等の安全管理

第26条 情報システム管理者は、保有個人情報を取り扱う基幹的なサーバ等の機器を設置する室等（以下「サーバ室等」という。）について、その安全管理のため、次に掲げるところにより管理しなければならない。

(1) 外部からの不正な侵入がないように、サーバ室等の出入口に、施錠装置、監視設備等を設置し、入退室の管理に必要な措置を講ずるとともに、入室することができる者及び記録媒体の持ち込み等を制限する等入退室における遵守事項を定めること。

(2) 災害等に備え、耐震、防火、防災、防水等に必要な措置を講ずること。

(3) サーバ等の予備電源を確保すること。

(4) その他サーバ室等の管理に必要な措置を講ずること。

2 情報システム管理者は、サーバ室等の設備を維持するため、その保守管理を確実に行わなければならない。

第7章 事務の委託等

(事務の委託等)

第27条 保護条例第9条の規定により個人情報を取り扱う事務について委託をしようとするとき、又は指定管理者に公の施設の管理を行わせようとするときは、個人情報の適正な管理を行う能力を有する者を選定しなければならない。

2 特定個人情報を取り扱う事務について委託をしようとするときは、委託を受ける者については、市が講ずる保有特定個人情報の適正な管理のために必要な措置と同等の措置を講ずることができるかどうかをあらかじめ確認しなければならない。再委託を許諾する場合も、また同様とする。

(委託契約書等の記載事項等)

第28条 保護条例第9条の規定により個人情報を取り扱う事務について委託をするとき、又は指定管理者に公の施設の管理を行わせるときは、当該委託又は管理に係る契約書、協定書等に次に掲げる事項を明記するとともに、委託を受けた者又は指定管理者に係る組織的管理体制及び事務処理の実施体制（再委託（委託を受けた者が委託を受けた事務を処理する目的で行う委託又は指定管理者が管理に係る事務のうち個人情報を取り扱うものを処理する目的で行う委託をいう。以下同じ。）に関する事項を含む。）、取り扱う個人情報の管理方法その他の必要な事項について書面を提出させて確認しなければならない。ただし、事務の性質又は目的により必要がないと認められる事項については、この限りでない。

- (1) 個人情報の秘密保持に関する事項
 - (2) 個人情報の目的外の利用及び第三者への提供の禁止に関する事項
 - (3) 再委託の禁止又は許諾に関する事項
 - (4) 個人情報の複写及び複製の禁止又は制限に関する事項
 - (5) 提供した個人情報の委託期間又は指定期間終了後における返却又は廃棄に関する事項
 - (6) 個人情報の管理方法の指定に関する事項
 - (7) 個人情報の管理状況に係る必要な調査に関する事項
 - (8) 事故発生時における報告に関する事項
 - (9) 従業者に対する教育研修に関する事項
 - (10) 義務違反の場合における契約解除等の措置及び損害賠償に関する事項
 - (11) 前各号に掲げるもののほか、当該事務の性質又は目的により市長が必要と認める個人情報の保護に関する事項
- 2 委託した事務又は指定管理者の管理する事務が再委託される場合は、当該再委託をする者又は指定管理者に前項に規定する措置を講じさせるものとする。
- 3 前項の規定は、再委託された保有個人情報の取扱いに係る事務が更に委託された場合に準用する。

第8章 安全確保上の問題への対応

(事案の報告及び再発防止措置)

第29条 職員は、保有個人情報の漏えい等安全確保の上で問題となる事案が発生した場合又は問題となる事案の発生のおそれを認識した場合は、直ちに当該保有個人情報を管理する情報責任者に報告しなければならない。

- 2 情報責任者は、前項の規定による報告を受けた場合は、被害の拡大防止及び復旧等に必要な措置を速やかに講ずるとともに、外部からの不正アクセス、不正プログラム等の感染が疑われるときは、次に掲げる措置を講じなければならない。

- (1) 直ちに当該端末機を庁内ネットワークから隔離し、使用を中止すること。
- (2) 不正アクセス、不正プログラム等の感染の証拠となる情報を保持し、情報システム管理者に調査を依頼すること。
- 3 情報責任者は、統括責任者及び情報システム管理者と連携して、事案の発生した経緯、被害状況等を調査するとともに、最高統括責任者に報告しなければならない。ただし、特に重大と認める事案が発生した場合は、直ちに最高統括責任者に当該事案の内容等について報告しなければならない。
- 4 最高統括責任者は、前項の規定による報告を受けた場合は、事案の内容等に応じて、当該事案の内容、経緯、被害状況等を、速やかに市長に報告しなければならない。
- 5 最高統括責任者は、事案の発生した原因を分析し、再発防止のために必要な措置を講じなければならない。

(公表等)

第30条 最高統括責任者は、前条第1項に規定する事案が発生した場合は、市長の指示に基づき、その内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る保有個人情報の本人への対応、関係行政機関への報告その他の必要な措置を講じなければならない。

(特定個人情報の事案における報告)

第31条 特定個人情報について第29条第1項に規定する事案が発生した場合は、統括責任者は、別に定めるところにより、関係行政機関に直ちに報告しなければならない。

第9章 監査及び点検の実施

(監査)

第32条 監査責任者は、保有個人情報の適正な管理を検証するため、各課における保有個人情報の管理の状況について、情報セキュリティポリシー（東大和市情報システムマネジメント本部設置規則（平成18年規則第63号）第1条に規定する情報セキュリティについて定める基本の方針をいう。）に基づく情報セキュリティ監査に併せて定期的に、及び必要に応じ随時に監査を行い、その結果を最高統括責任者に報告する。

(点検)

第33条 情報責任者は、課における保有個人情報の保管方法等について、定期的に、及び必要に応じ随時に点検を行い、必要があると認めるときは、その結果を最高統括責任者に報告する。

(評価及び見直し)

第34条 情報責任者は、第32条の規定による監査又は前条の規定による点検の結

果等を踏まえ、保有個人情報の適正な管理のための措置について評価を行い、必要があると認めるときは、当該措置の見直し等を行うものとする。

第10章 雑則

(死者の個人番号の取扱い)

第35条 番号法第12条の規定により市が講ずべき死者の個人番号の適切な管理のために必要な措置については、特定個人情報の適正な管理のために必要な措置の例による。

(補則)

第36条 この規程に定めるもののほか必要な事項は、市長が別に定める。

附 則

この訓令は、平成28年1月1日から施行する。