吹田市特定個人情報の適正な取扱いに関する指針

制　定　　平成２７年１１月９日
改　正　　令和元年８月１５日

第１章　総論

１　目的

この指針は、市が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「番号利用法」という。）、個人情報の保護に関する法律（平成１５年法律第５７号。以下「個人情報保護法」という。）、特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）（以下「ガイドライン」という。）、吹田市個人情報保護条例（平成１４年吹田市条例第７号）、吹田市個人番号の利用等に関する条例（平成２７年吹田市条例第２４号。以下「番号利用条例」という。）及び吹田市特定個人情報の安全管理に関する基本方針に基づき、特定個人情報（個人番号をその内容に含む個人情報をいう。）の適正な取扱いを確保するために定める。

２　定義

この指針における用語の定義は、番号利用法その他関係法令等及びガイドラインの例による。

３　個人番号を取り扱う事務の範囲

（１）本市が取り扱う個人番号利用事務は、番号利用法、番号利用条例及び吹田市個人番号の利用等に関する条例施行規則（平成２７年吹田市規則第３７号。以下「番号利用規則」という。）に定めるところによる。

（２）本市が取り扱う個人番号関係事務は、次のとおりとする。

ア　給与所得等の源泉徴収票及び給与支払報告書等作成事務

イ　社会保険等の届出及び申請等の事務

ウ　その他法令等で定められた個人番号関係事務

４　特定個人情報の範囲

（１）個人番号利用事務における本市が取り扱う特定個人情報は、番号利用法、番号利用条例及び番号利用規則に定めるところによる。

（２）個人番号関係事務における本市が取り扱う特定個人情報は、以下のとおりとする。

ア　番号利用法第９条第３項に掲げる事務に必要な申告書及び申請書等

イ　番号利用法第１６条に基づく本人確認の措置を実施する際に提示を受けた本人確認書類等

ウ　行政機関等に提出するために作成した法定調書等及びその控え

エ　ウの法定調書等の作成のために提出を受けた申告書等

オ　その他個人番号と関連付けられて保存される情報

第２章　安全管理措置

第１節　組織的安全管理措置の実施

１　組織体制の整備

（１）総括責任者の設置及び責任

市に特定個人情報の適正な取扱いに係る総括責任者を置き、市長が指名する副市長をもって充てる。

総括責任者は、本市が保有する特定個人情報の保護及び適正な取扱いに関する最高責任者として、特定個人情報の適切な管理のために必要な措置を講ずるとともに保護責任者等を監督する責務を負う。

（２）保護責任者の設置及び責任

市に特定個人情報の適正な取扱いに係る保護責任者を置き、各部局の長をもって充てる。

保護責任者は、番号利用法その他関係法令等、ガイドライン及びこの指針（以下「番号利用法等」という。）を遵守し、各部局において保有する特定個人情報を適切に管理する任に当たる。また、所属の事務取扱責任者等に番号利用法等を理解させ、遵守させるよう必要な措置を講ずる責務を負う。

（３）監査責任者の設置及び責任

市に特定個人情報の管理の状況について監査するために監査責任者を置き、市長の指名する者をもって充てる。

監査責任者は、必要に応じて、総括責任者、保護責任者等に対して、報告又は資料の提出を求めることができる。

（４）事務取扱責任者の設置及び責任

市に特定個人情報の適正な取扱いに係る事務取扱責任者を置き、各室課の長をもって充てる。

事務取扱責任者は、番号利用法等を遵守し、各室課において保有する特定個人情報を適切に管理するとともに、所属の事務取扱担当者にこれを理解させ、遵守させるよう必要な措置を講ずる責務を負う。

事務取扱責任者の所管する業務は、次のとおりとする

ア　事務取扱担当者を選任するとともに、その名簿を作成し、総括責任者に提出する。

イ　事務取扱担当者に対するこの指針の周知徹底並びに特定個人情報等の適正な取扱いについての教育及び研修の実施

ウ　事務取扱担当者（特定個人情報に関する事務の委託先を含む。）が行う特定個人情報の取扱い状況の管理及び監督

エ　複数の所管で特定個人情報を取り扱う場合は、それぞれの所管における事務取扱責任者が調整の上、それぞれの事務を行うものとする。

（５）事務取扱担当者及びその役割

特定個人情報に関する事務は、事務取扱責任者がその所属の職員のうちからあらかじめ

指名する事務取扱担当者が行うものとする。

事務取扱担当者は、特定個人情報の取得、保管、利用、提供、廃棄及び開示等、特定個人情報を取り扱う業務に従事するときは、番号利用法等の規定に従い、特定個人情報を適正に取り扱わなければならない。

（６）事務取扱担当者が取り扱う特定個人情報の範囲

事務取扱責任者は、所属の事務取扱担当者が取り扱う特定個人情報の範囲を指定する。

２　この指針等に基づく運用

事務取扱責任者は、番号利用法等に基づく運用状況を確認するため、特定個人情報へのアクセス状況等を記録し、その記録を一定の期間保存し、定期に又は随時に分析するために必要な措置を講ずる。また、記録の改ざん、窃取又は不正な削除の防止のために必要な措置を講ずる。

３　取扱状況を確認する手段の整備

（１）事務取扱責任者は、特定個人情報ファイルの取扱状況を確認する手段として、次に掲げる項目を記録する。

なお、取扱状況を確認するための記録等には、特定個人情報は記載しない。

ア　特定個人情報ファイルの名称

イ　取扱部署

ウ　利用目的

エ　特定個人情報ファイルに記録される項目及び対象者

オ　特定個人情報ファイルに記録される特定個人情報の収集等の方法

ただし、これに代わる手段により特定個人情報ファイルの取扱状況を確認することができるときは、当該手段によることができるものとする。

（２）特定個人情報ファイルに記録される特定個人情報の収集、保管及び廃棄に関する手順は、事務取扱責任者が定め、保護責任者に報告するものとする。

４　情報漏えい等事案に対応する体制等の整備

（１）情報漏えい等事案に対応する体制

ア　事務取扱担当者は、特定個人情報の漏えい、滅失又は毀損による事故（以下「漏えい事案等」という。）の事実又は兆候を把握した場合は、速やかに保護責任者及び事務取扱責任者に報告する。

イ　職員は、漏えい事案等の発生又は兆候を把握した場合及び事務取扱担当者がこの指針等に違反している事実又は兆候を把握した場合は、速やかに保護責任者及び事務取扱責任者に報告しなければならない。

ウ　保護責任者及び事務取扱責任者は、漏えい事案等の事実又は兆候を把握した場合は、速やかにその旨を総括責任者に報告する。

エ　総括責任者は、「特定個人情報の漏えい事案等が発生した場合の対応について（通知）」（平成２７年９月２８日付特個第５８７号特定個人情報保護委員会事務局通知）に基づ

き、以下の措置を講じ、適切かつ迅速に対応するものとする。

(ｱ) 事実関係の調査及び原因の究明

(ｲ) 影響を受ける可能性のある本人への連絡

(ｳ) 特定個人情報保護委員会への報告

(ｴ) 再発防止策の検討及び決定

(ｵ) 事実関係及び再発防止策の公表

5　取扱状況の把握及び安全管理措置の見直し

（1）監査責任者は、特定個人情報の取扱いの状況について点検又は監査を行い、その結果を総括責任者に報告する。

（2）総括責任者は、点検又は監査の結果等を踏まえ、必要があると認めるときは、この指針等の見直し等の措置を講ずる。

第2節　人的安全管理措置の実施

1　事務取扱担当者の監督

総括責任者、保護責任者及び事務取扱責任者は、特定個人情報がこの指針等に基づき適正に取り扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行う。

2　研修による教育

総括責任者は保護責任者及び事務取扱責任者に、室課等における特定個人情報の適切な管理のために必要な教育研修を行う。

保護責任者及び事務取扱責任者は、事務取扱担当者及び所属の職員に、特定個人情報の適正な取扱いについて理解を深め、特定個人情報の保護に関する意識の高揚を図るための啓発その他必要な教育研修を定期的に行う。

また、特定個人情報を取り扱う情報システム（以下「情報システム」という。）の管理に関する事務に従事する職員に対し、特定個人情報の適切な管理のために、情報システムの管理運営及びセキュリティ対策に関して必要な教育研修を行う。

総括責任者、保護責任者及び事務取扱責任者は、特定個人情報の適切な管理のために、事務取扱担当者に教育研修への参加の機会を付与する等の必要な措置を講ずる。

3　番号利用法等違反等に対する厳正な対処

総括責任者は、番号利用法等に違反した職員に対し、法令等に基づき厳正に対処する。

第3節　物理的安全管理措置の実施

1　特定個人情報を取り扱う区域の安全管理

特定個人情報の情報漏えい等を防止するために、特定個人情報を取り扱う事務を実施する区域（以下「取扱区域」という。）及び情報システムの基幹的なサーバを設置し管理する区域（以下「管理区域」という。）を明確にし、次に掲げる物理的な安全管理措置を講ずる。

（1）取扱区域には、部外者がみだりに立ち入ることができないようにする。

（２）取扱区域に設置する窓口用端末の画面は、フィルター、間仕切り等により盗み見ができないようにする。
（３）管理区域は、情報政策室長が管理するサーバ室とし、原則として、電子錠により施錠管理する。
（４）管理区域への立ち入りは、必要最小限とし、入退室管理台帳により入退室者及びカードキーの管理を行う。
（５）管理区域において外部事業者が保守等の作業を行う際は、原則として、当該情報システム所管の職員が立ち会う。

２　管理区域以外に設置する情報システムの安全管理

管理区域以外に情報システムを設置する場合においては、原則として、前項各号の規定を考慮した安全管理措置を講ずる。

３　機器及び電子媒体等の盗難等の防止

特定個人情報を取り扱う機器、端末、電子媒体及び書類の盗難又は紛失を防止するために、次に掲げる物理的な安全管理措置を講ずる。
（１）取扱区域に設置する端末は、盗難を防止するためにワイヤーロック等で固定し、又は適切に管理される鍵により施錠できるロッカー等に保管する。
（２）特定個人情報が記録された電子媒体及び特定個人情報が記載された書類は、適切に管理される鍵により施錠できるロッカー等に保管する。

４　電子媒体等の取扱いにおける漏えい等の防止

特定個人情報が記録された電子媒体及び特定個人情報が記載された書類からの情報漏えいを防止するために、次に掲げる措置を講ずる。
（１）電子媒体へのデータの書き込みは、原則として常時禁止する。なお、業務上必要があって使用する場合は情報政策室長に申請を行い、一時的に利用するものとする。
（２）電子媒体に保存する場合は、データを暗号化するものとする。ただし、行政機関に法定調書を提出する等でデータの保存が必要な場合は、行政機関等が指定する提出方法を踏まえたデータの保存方法等を別途明確にすることとする。
（３）事務取扱責任者は、電子媒体管理台帳を作成し、情報政策室長から求められた場合は提示する。
（４）電子媒体及び書類の庁外への持ち出しは、原則として禁止する。なお、業務上必要があって持ち出す場合は、当該電子媒体及び書類を管理する保護責任者の許可を得るものとする。
（５）電子媒体又は書類を取扱区域外へ持ち出す場合は、容易に個人番号が判明しない措置の実施及び追跡可能な移送手段の利用等の安全な方策を講ずる。

５　特定個人情報の削除並びに機器及び電子媒体等の廃棄

特定個人情報ファイル、特定個人情報が記録された電子媒体及び特定個人情報が記載された書類は、法令等で定められた保存期間を経過した場合には、次のとおりできるだけ速やか

に復元できない手段により削除し、又は廃棄する。

（１）特定個人情報ファイルを削除する場合又は電子媒体若しくは書類を廃棄する場合には、削除又は廃棄した日付け等を記録し、保存する。

（２）特定個人情報ファイルの削除又は電子媒体若しくは書類の廃棄作業を委託する場合には、委託先が確実に削除し、又は廃棄したことについて、証明書等により確認する。

（３）特定個人情報ファイル又は一部の特定個人情報を削除する場合には、容易には復元不可能な手段を採る。

（４）特定個人情報が記録されたサーバ等の機器又は電子媒体を廃棄する場合には、専用のデータ削除ソフトウェアの利用又は物理的な破壊等の容易には復元不可能な手段を採る。

（５）特定個人情報が記録された書類を廃棄する場合には、焼却、溶解等の容易には復元不可能な手段を採る。

第４節　技術的安全管理措置の実施

１　情報システムの構築

情報システムは、原則としてインターネットから独立した住民情報系ネットワーク上に構築する。

２　アクセス制御の実施

事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定し、アクセス権を有する者を必要最小限とするために、次に掲げるアクセス制御を行う。

（１）情報システムを所管する室課の長は、事務取扱担当者ごとに個別のユーザーＩＤを付与する。

（２）情報システムを所管する室課の長は、ログインする者が事務取扱担当者であることを識別するために、ユーザーＩＤと生体情報又はパスワードによる認証を用いる。

（３）情報システムを所管する室課の長は、事務取扱担当者のみに特定個人情報ファイルへのアクセス権を付与する。

（４）情報システムを所管する室課の長は、個人番号と紐付けてアクセスできる情報の範囲を、権限がない者には画面表示されない等の方法で制限する。

（５）情報システムを所管する室課の長は、情報システムに導入したアクセス制御機能に脆弱性等が発見された場合には速やかに対応する。

３　不正アクセス等による被害の防止等

情報システムを外部等からの不正アクセス又は不正ソフトウェアから保護するため、次に掲げる仕組み等を導入し、適切に運用する。

なお、個人番号利用事務の実施に当たっては、情報提供ネットワークシステムの接続に係る地方公共団体情報システム機構（J-LIS）の規定等に定める安全管理措置を遵守する。

（１）情報システムには、外部ネットワーク又は庁内の他のシステムとの接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する。

（２）情報システム及び機器には、ウィルス対策ソフトウェア等のセキュリティ対策ソフトウェアを導入し、不正ソフトウェアの侵入を防止する。
（３）情報システムを所管する室課の長は、ソフトウェア等に脆弱性が発見された場合は、速やかに修正パッチを適用される仕組みを導入する。
（４）情報システムを所管する室課の長は、定期及び必要に応じログ等の分析を行い、不正アクセス等を検知する。
（５）情報システムを所管する室課の長は、不正アクセス等の被害に遭った場合の対応を別途記載し、適切に運用する。
（６）情報システムを所管する室課の長は、電子媒体の利用、機器の接続、ソフトウェアのインストール等により情報システムの構成を変更する場合には、情報政策室長の管理の下で実施する。

附　則

この指針は、平成２７年１１月９日から施行する。

附　則

この指針は、令和元年８月１５日から施行する。