上尾市保有個人情報等の適切な管理に関する要領（案）

　　　　　　　　　　　　　　　　　　　　　　 　令和５年　　月　　日

　　　　　　 　市長決裁

# 第１章　総則

　（趣旨）

第１条　この要領は、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。）、行政手続における特定の個人を識別する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。）、上尾市情報セキュリティ基本方針（平成２１年２月２７日市長決裁。以下「セキュリティ基本方針」という。）及び上尾市情報セキュリティ対策基準（平成２１年２月２７日市長決裁。以下「セキュリティ対策基準」という。）に基づき、保有個人情報及び個人番号（以下「保有個人情報等」という。）の適切な管理に関する必要な措置について定めるものとする。

　（定義）

第２条　用語の意義は、個人情報保護法第２条、番号法第２条、上尾市個人情報の保護に関する法律施行条例第２条第１項、及びセキュリティ基本方針第２条の定めるところによる。

# 第２章　管理体制

　（総括保護管理者）

第３条　法第６６条第１項の規定に基づき総括保護管理者を一人置くこととし、副市長をもって充てる。

２　総括保護管理者は、法第６６条第１項の規定に基づき各実施機関における保有個人情報等の管理に関する事務を総括する任に当たる。

　（保護管理者）

保護管理者は、次に掲げる職にある者とする。

第４条　保有個人情報等を取り扱う各課等（上尾市組織規則（昭和５９年上尾市規則第１１号）第３条各号に定める課及び同規則第５条の表に掲げる出先機関の組織（子育て支援センター、子ども家庭総合支援センター、発達支援相談センター、消費生活センター及び西貝塚環境センターに限る。）並びに上尾市会計管理者の補助組織設置規則（昭和６０年上尾市規則第１４号）第１条に定める出納室をいう。以下同じ。）に、保護管理者を一人置くこととし、当該各課等の長又はこれに代わる者をもって充てる。

２　保護管理者は、各課等における保有個人情報等の適切な管理を確保する任に当たる。

３　保護管理者は、保有個人情報等を情報システムで取り扱う場合、システム管理者（総務部ＩＴ推進課長の職にあるものをいう。以下同じ。）と連携して、その任に当たる。

　（保護担当者）

第５条　保有個人情報等を取り扱う各課等に、当該各課等の保護管理者が指定する保護担当者を一人以上置く。

２　保護担当者は、保護管理者を補佐し、当該各課等における保有個人情報等の管理に関する事務を担当する。

　（監査責任者）

第６条　監査責任者を一人置くこととし、総務部長をもって充てる。

２　監査責任者は、保有個人情報等の管理の状況について監査する任に当たる。

# 第３章　教育研修

　（教育研修）

第７条　総括保護管理者は、保有個人情報等の取扱いに従事する職員（派遣労働者を含む。）に対し、保有個人情報等の取扱いについて理解を深め、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行う。

２　総括保護管理者は、保有個人情報等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（派遣労働者を含む。）に対し、保有個人情報等の適切な管理のために、情報システムの管理、運用及びセキュリティ対策に関して必要な教育研修を行う。

３　前２項に規定する教育研修は、セキュリティ対策基準第４３条により、行うことができる。

４　総括保護管理者は、保護管理者及び保護担当者に対し、各課等の現場における保有個人情報等の適切な管理のための教育研修を定期的に実施する。

５　保護管理者は、当該各課等の職員（派遣労働者を含む。）に対し、保有個人情報等の適切な管理のために、総括保護管理者の実施する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。

# 第４章　職員の責務

　（職員の責務）

第８条　職員は、個人情報保護法、番号法、セキュリティ基本方針の趣旨にのっとり、関連する法令等の定め並びに総括保護管理者、保護管理者及び保護担当者の指示に従い、保有個人情報等を取り扱わなければならない。

# 第５章　保有個人情報等の取扱い

　（アクセス制限）

第９条　保護管理者は、保有個人情報等の秘匿性等その内容に応じて、当該保有個人情報等にアクセスする権限（以下「アクセス権限」という。）を有する職員の範囲と権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限定するものとする。

２　アクセス権限を有しない職員は、保有個人情報等にアクセスしてはならない。

３　職員は、アクセス権限を有する場合であっても、業務上の目的以外の目的で保有個人情報等にアクセスしてはならず、アクセスは必要最小限としなければならない。

　（複製等の制限）

第１０条　職員は、業務上の目的で保有個人情報等を取り扱う場合であっても、次の行為については、当該保有個人情報等の秘匿性等その内容に応じて、当該行為を行うことができる場合を必要最小限に限定し、保護管理者の指示に従い行うものとする。

　(1)　保有個人情報等の複製

　(2)　保有個人情報等の送信

　(3)　保有個人情報等が記録されている媒体の外部への送付又は持ち出し

　(4)　その他保有個人情報等の適切な管理に支障を及ぼすおそれのある行為

　（誤りの訂正等）

第１１条　職員は、保有個人情報等の内容に誤り等を発見した場合には、保護管理者の指示に従い、訂正等を行わなければならない。

　（媒体の管理等）

第１２条　職員は、保護管理者の指示に従い、保有個人情報等が記録されている媒体を定められた場所に保管するとともに、必要があると認めるときは、耐火金庫への保管、施錠等を行うものとする。

２　保有個人情報等が記録されている媒体を外部へ送付し、又は持ち出す場合には、原則として、パスワード等（パスワード、ＩＣカード、生体情報等をいう。以下同じ。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講ずるものとする。

　（誤送付等の防止）

第１３条　職員は、保有個人情報等を含む電磁的記録又は媒体の誤送信、誤送付、誤交付、又はウェブサイト等への誤掲載を防止するため、個別の事務又は事業において取り扱う個人情報の秘匿性等その内容に応じ、複数の職員による確認、チェックリストの活用等の必要な措置を講ずるものとする。

　（廃棄等）

第１４条　職員は、保有個人情報等又は保有個人情報等が記録されている媒体（端末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、保護管理者の指示に従い、当該保有個人情報等の復元又は判読が不可能な方法により当該情報の消去又は当該媒体の廃棄を行うものとする。

　（廃棄等の委託）

第１５条　保有個人情報等の消去又は保有個人情報等が記録されている媒体の廃棄を委託する場合（２以上の段階にわたる委託を含む。）は、必要に応じて職員が消去若しくは廃棄に立ち会い、又は写真等を付した消去若しくは廃棄を証明する書類を受け取るなど、委託先において消去若しくは廃棄が確実に行われていることを確認することとする。

　（保有個人情報の取扱状況の記録）

第１６条　保護管理者は、保有個人情報の秘匿性等その内容に応じて、台帳等を整備して、当該保有個人情報の利用及び保管等の取扱いの状況について記録するものとする。

　（外的環境の把握）

第１７条　保有個人情報が、外国において取り扱われる場合、当該外国の個人情報の保護に関する制度等を把握した上で、保有個人情報の安全管理のために必要かつ適切な措置を講じなければならない。

# 第６章　情報システムにおける安全の確保等

　（アクセス制御）

第１８条　保護管理者は、保有個人情報等（情報システムで取り扱うものに限る。以下この章（第３１条を除く。）において同じ。）の秘匿性等その内容に応じて、認証機能を設定する等のアクセス制御のために必要な措置を講ずるものとする。

２　保護管理者は、前項の措置を講ずる場合には、パスワード等の管理に関する定めを整備（その定期又は随時の見直しを含む。）するとともに、パスワード等の読取防止等を行うために必要な措置を講ずるものとする。

　（アクセス記録）

第１９条　システム管理者並びに保護管理者（情報システム（当該システムにおいて保有個人情報等へのアクセス状況を記録し、その記録（以下「アクセス記録」という。）を管理するものに限る。以下この章において同じ。）を取り扱うものに限る。）（以下これらの者を総称して「システム管理者等」という。）は、保有個人情報等の秘匿性等その内容に応じて、アクセス記録を一定の期間保存し、及びアクセス記録を定期的に分析するために必要な措置を講ずるものとする。

２　システム管理者等は、アクセス記録の改ざん、窃取又は不正な消去の防止のために必要な措置を講ずるものとする。

　（管理者権限の設定）

第２０条　保護管理者は、保有個人情報等の秘匿性等その内容に応じて、情報システムの管理者権限の特権を不正に窃取された際の被害の最小化及び内部からの不正操作等の防止のため、当該特権を最小限とする等の必要な措置を講ずるものとする。

　（外部からの不正アクセスの防止）

第２１条　システム管理者等は、保有個人情報等を取り扱う情報システムへの外部からの不正アクセスを防止するため、ファイアウォールの設定による経路制御等の必要な措置を講ずるものとする。

　（不正プログラムによる漏えい等の防止）

第２２条　システム管理者等は、不正プログラムによる保有個人情報等の漏えい等の防止のため、ソフトウェアに関する公開された脆弱性の解消、把握された不正プログラムの感染防止等に必要な措置（導入したソフトウェアを常に最新の状態に保つことを含む。）を講ずるものとする。

　（情報システムにおける保有個人情報等の処理）

第２３条　職員は、保有個人情報等について、一時的に加工等の処理を行うため複製等を行う場合には、その対象を必要最小限に限り、処理終了後は不要となった情報を速やかに消去するものとする。

２　保護管理者は、当該保有個人情報等の秘匿性等その内容に応じて、随時、消去等の実施状況を重点的に確認するものとする。

　（暗号化）

第２４条　システム管理者等は、保有個人情報等の秘匿性等その内容に応じて、暗号化のために必要な措置を講ずるものとする。

２　職員は、前項の措置を踏まえ、その処理する保有個人情報等について、当該保有個人情報等の秘匿性等その内容に応じて、適切に暗号化を行うものとする。

　（記録機能を有する機器・媒体の接続制限）

第２５条　保護管理者は、保有個人情報等の秘匿性等その内容に応じて、当該保有個人情報等の漏えい等の防止のため、スマートフォン、ＵＳＢメモリ等の記録機能を有する機器及び媒体の情報システム端末等への接続の制限（当該機器の更新への対応を含む。）等の必要な措置を講ずるものとする。

　（端末の盗難防止等）

第２６条　保護管理者は、端末の盗難又は紛失の防止のため、適切な措置を講ずるものとする。

２　職員は、保護管理者が必要であると認めるときを除き、端末を外部へ持ち出し、又は外部から持ち込んではならない。

　（第三者の閲覧防止）

第２７条　職員は、端末の使用に当たっては、保有個人情報等が第三者に閲覧されることがないよう、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講ずるものとする。

　（入力情報の照合等）

第２８条　職員は、情報システムで取り扱う保有個人情報等の重要度に応じて、入力原票と入力内容との照合、処理前後の当該保有個人情報等の内容の確認、既存の保有個人情報等との照合等を行うものとする。

　（バックアップ）

第２９条　保護管理者は、保有個人情報等の重要度に応じて、バックアップを作成し、分散保管するために必要な措置を講ずるものとする。

　（情報システム設計書等の管理）

第３０条　システム管理者等は、保有個人情報等に係る情報システムの設計書、構成図等の文書について外部に知られることがないよう、その保管、複製、廃棄等について必要な措置を講ずるものとする。

# 第７章　情報システム室等の安全管理

　（入退管理）

第３１条　システム管理者等は、保有個人情報等を取り扱う基幹的なサーバ等の機器を設置する室その他の区域（以下「情報システム室等」という。）の入退出に立ち入る権限を有する者を定めるとともに、用件の確認、入退の記録、部外者についての識別化、部外者が立ち入る場合の職員の立会い又は監視設備による監視、外部電磁的記録媒体等の持込み、利用及び持ち出しの制限又は検査等の措置を講ずるものとする。

２　システム管理者等は、保有個人情報等を記録する媒体を保管するための施設を設けている場合においても、必要があると認めるときは、前項に規定する措置と同様の措置を講ずるものとする。

３　システム管理者は、必要があると認めるときは、情報システム室等の出入口の特定化による入退の管理の容易化、所在表示の制限等の措置を講ずるものとする。

４　システム管理者等は、情報システム室等及び保管施設の入退の管理について、必要があると認めるときは、立入りに係る認証機能を設定する等の措置を講ずるものとする。

　（情報システム室等の管理）

第３２条　システム管理者等及び統括情報セキュリティ責任者（セキュリティ対策基準第３条第６項に規定する統括情報セキュリティ責任者という。次項において同じ。）は、外部からの不正な侵入に備え、情報システム室等に施錠装置、警報装置及び監視設備の設置等の措置を講ずるものとする。

２　システム管理者等及び統括情報セキュリティ責任者は、災害等に備え、情報システム室等に、耐震、防火、防煙、防水等の必要な措置を講ずるとともに、サーバ等の機器の予備電源の確保、配線の損傷防止等の措置を講ずるものとする。

# 第８章　保有個人情報等の提供

　（保有個人情報等の提供）

第３３条　保護管理者は、個人情報保護法第６９条第２項第３号及び第４号の規定に基づき他の行政機関、独立行政法人等、地方公共団体の機関又は地方独立行政法人（以下「他の行政機関等という」。）以外の者に保有個人情報等を提供する場合に、同法第７０条の規定に基づき、原則として、提供先における利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について提供先との間で書面（電磁的記録を含む。）を取り交わすものとする。

２　保護管理者は、個人情報保護法第６９条第２項第３号及び第４号の規定に基づき他の行政機関等以外の者に保有個人情報等を提供する場合には、同法第７０条の規定に基づき、安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地の調査等を行い、措置状況を確認してその結果を記録するとともに、改善要求等の措置を講ずるものとする。

３　保護管理者は、個人情報保護法第６９条第２項第３号の規定に基づき他の行政機関等に保有個人情報を提供する場合において、必要があると認めるときは、同法第７０条の規定に基づき、前２項に規定する措置を講ずるものとする。

# 第９章　個人情報の取扱いに係る業務の委託

　（業務の委託等）

第３４条　保有個人情報等の取扱いに係る業務を外部に委託する場合には、個人情報の適切な管理を行う能力を有しない者を選定することがないよう、必要な措置を講じ、契約書に、次の各号に掲げる事項を明示するとともに、委託先における責任者及び業務従事者の管理体制及び実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認するものとする。

　(1)　 個人情報に関する秘密保持、利用目的以外の目的のための利用の禁止 等の義務

　(2)　 個人情報の取扱いに係る業務の再委託（再委託先が委託先の子会社（会社法（平成１７年法律第８６号）第２条第１項第３号に規定する子会社をいう。）である場合も含む。以下この項及び第４項において同じ。）の制限又は事前承認等再委託に係る条件に関する事項

　(3)　個人情報の複製等の制限に関する事項

　(4)　個人情報の安全管理措置に関する事項

　(5)　個人情報の漏えい等の事案の発生時における対応に関する事項

　(6)　委託終了時における個人情報の消去及び媒体の返却に関する事項

　(7)　法令及び契約に違反した場合における契約解除、損害賠償責任その他必要な事項

　(8)　契約内容の遵守状況についての定期的報告に関する事項及び委託先における委託された個人情報の取扱状況を把握するための監査等に関する事項（再委託先の監査等に関する事項を含む。）

２　保有個人情報等の取扱いに係る業務を外部に委託する場合には、取扱いを委託する個人情報の範囲は、委託する業務内容に照らして必要最小限でなければならない。

３　保有個人情報等の取扱いに係る業務を外部に委託する場合には、委託する業務に係る保有個人情報等の秘匿性等その内容やその量等に応じて、作業の管理体制及び実施体制や個人情報の管理の状況について、年１回以上、原則として実地検査又は入室が困難な場合は他の検査により確認するものとする。

４　委託先において、保有個人情報等の取扱いに係る業務が再委託される場合には、委託先に第１項の措置を講じさせるとともに、再委託される業務に係る保有個人情報等の秘匿性等その内容に応じて、委託先を通じて又は委託元自らが前項の措置を実施する。保有個人情報等の取扱いに係る業務について再委託先が再々委託を行う場合以降も同様とする。

５　保有個人情報等の取扱いに係る業務を派遣労働者によって行わせる場合には、労働者派遣契約書に秘密保持義務等個人情報の取扱いに関する事項を明記するものとする。

第３５条　保有個人情報等を提供し、又は業務委託する場合には、漏えい等による被害発生のリスクを低減する観点から、提供先の利用目的、委託する業務の内容、保有個人情報等の秘匿性等その内容などを考慮し、必要に応じ、特定の個人を識別することができる記載の全部又は一部を削除し、又は別の記号等に置き換える等の措置を講ずるものとする。

# 第１０章　サイバーセキュリティの確保

　（サイバーセキュリティに関する対策の基準等）

第３６条　個人情報を取り扱い、又は情報システムを構築し、若しくは利用するに当たっては、サイバーセキュリティ基本法（平成２６年法律第１０４号）第２６条第１項第２号に掲げられたサイバーセキュリティに関する対策の基準等を参考として、取り扱う保有個人情報等の性質等に照らして適正なサイバーセキュリティの水準を確保するものとする。

# 第１１章　安全管理上の問題への対応

　（事案の報告及び再発防止措置）

第３７条　保有個人情報等の漏えい等安全管理の上で問題となる事案又は問題となる事案の発生のおそれを認識した場合は、その事案等を認識した職員は、直ちに当該保有個人情報等を管理する保護管理者に報告するものとする。

２　保護管理者は、被害の拡大防止又は復旧等のために必要な措置を速やかに講ずるものとする。ただし、外部からの不正アクセスや不正プログラムの感染が疑われる当該端末等のＬＡＮケーブルを抜くなど、被害拡大防止のため直ちに行い得る措置については、直ちに行う（職員に行わせることを含む。）ものとする。

３　保護管理者は、事案の発生した経緯、被害状況等を調査し、総括保護管理者に報告する。ただし、特に重大と認める事案が発生した場合には、直ちに総括保護管理者に当該事案の内容等について報告するものとする。

４　総括保護管理者は、前項の報告を受けた場合には、事案の内容等に応じて、当該事案の内容、経緯、被害状況等を実施機関に速やかに報告しなければならない。

５　保護管理者は、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ずるとともに、同種の業務を実施している各課等に再発防止措置を共有するものとする。

　（法に基づく報告及び通知）

第３８条　保有個人情報等の漏えい等が生じた場合であって個人情報保護法第６８条第１項の規定による個人情報保護委員会への報告及び同条第２項の規定による本人への通知を要する場合には、前条と並行して、速やかに所定の手続を行うとともに、個人情報保護委員会による事案の把握等に協力するものとする。

　（公表等）

第３９条　実施機関は、個人情報保護法第６８条第１項の規定による個人情報保護委員会への報告及び同条第２項の規定による本人への通知を要しない場合であっても、事案の内容、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等の本人への連絡等の措置を講ずるものとする。

第１２章　監査及び点検の実施

　（監査）

第４０条　監査責任者は、保有個人情報等の適切な管理を検証するため、第２章から第４章までに記載する措置の状況を含む当該実施機関における保有個人情報等の管理の状況について、定期又は必要に応じ随時に監査（外部監査を含む。以下同じ。）を行い、その結果を総括保護管理者に報告するものとする。

　（点検）

第４１条　保護管理者は、各課等における保有個人情報等の記録媒体、処理経路、保管方法等について、定期又は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、その結果を総括保護管理者に報告するものとする。

　（評価及び見直し）

第４２条　総括保護管理者、保護管理者等は、監査又は点検の結果等を踏まえ、実効性等の観点から保有個人情報等の適切な管理のための措置について評価し、必要があると認めるときは、その見直し等の措置を講ずるものとする。

　　附　則

この要領は、令和５年　月　日から施行する。