参考資料８

○久喜市の保有する個人情報の適切な管理のための措置に関する規程

令和５年５月２９日

訓令第１３号

目次

第１章　総則

（趣旨）

第１条　この訓令は、久喜市の保有する個人情報の適切な管理に関して必要な事項を定めるものとする。

（定義）

第２条　この訓令で使用する用語は、個人情報の保護に関する法律（平成１５年法律第５７号。以下「法」という。）第２条及び第６０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　市に、総括保護管理者を１人置き、副市長をもって充てる。

２　総括保護管理者は、市長を補佐し、保有個人情報の管理に関する事務を総括するものとする。

（保護管理者）

第４条　保有個人情報を取り扱う課等（以下「課等」という。）に、保護管理者を１人置き、課等の長をもって充てる。

２　保護管理者は、課等における保有個人情報の適切な管理に関する事務を統括するものとする。

３　保護管理者は、保有個人情報を情報システムで取り扱う場合は、当該情報システムの管理者と連携して、前項の事務を統括するものとする。

（保護担当者）

第５条　課等に、保護担当者を置き、課等の保護管理者が指名する職員をもって充てる。

２　保護担当者は、保護管理者を補佐し、課等における保有個人情報の管理に関する事務を行うものとする。

（監査責任者）

第６条　市に、監査責任者を１人置き、総務部長をもって充てる。

２　監査責任者は、保有個人情報の管理の状況について監査するものとする。

（保有個人情報の適切な管理のための会議）

第７条　総括保護管理者は、保有個人情報の管理に係る重要事項について、調整等を行う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　研修

第８条　総括保護管理者は、法第６７条に規定する保有個人情報の取扱いに従事する職員（派遣労働者を含む。以下同じ。）に対し、保有個人情報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及び研修を実施するものとする。

２　総括保護管理者は、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、情報システムの管理、運用及びセキュリティ対策のための研修を実施するものとする。

３　総括保護管理者は、保護管理者及び保護担当者に対し、課等における保有個人情報の

適切な管理のための研修を実施するものとする。

４　保護管理者は、課等の職員に対し、総括保護管理者の実施する研修への参加の機会の付与その他の必要な措置を講ずるものとする。

第４章　職員の責務

（適切な取扱いの義務）

第９条　職員は、法の趣旨に則り、関連する法令及びこの規程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、保有個人情報を取り扱わなければならない。

第５章　保有個人情報の取扱い

（アクセス制限）

第１０条　保護管理者は、保有個人情報の秘匿性又はその内容に応じて、当該保有個人情報にアクセス（情報に接する行為をいう。以下同じ。）をする権限（以下「アクセス権限」という。）を有する職員及びアクセス権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限定しなければならない。

２　保護管理者は、前項の規定により職員の範囲とアクセス権限の内容を限定するときは、個人識別の容易性の程度、要配慮個人情報の有無、漏えい等が発生した場合に生じ得る被害の性質又は程度等を考慮して、これを行わなければならない。

３　アクセス権限を有しない職員は、保有個人情報にアクセスしてはならない。

４　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にアクセスしてはならない。

（複製等の制限）

第１１条　保護管理者は、職員が行う次に掲げる行為については、当該保有個人情報の秘匿性又はその内容に応じて、当該行為を必要最小限に限定するものとし、職員は、保護管理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の外部への送付又は持出し

（４）　その他保有個人情報の適切な管理に支障を及ぼすおそれがあると保護管理者が

認める行為

（誤りの訂正等）

第１２条　職員は、保有個人情報の内容に誤り等を発見したときは、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１３条　職員は、保護管理者の指示に従い、保有個人情報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、必要に応じ、当該媒体の耐火金庫への保管、保管場所への施錠等を行わなければならない。

２　職員は、保有個人情報が記録されている媒体を外部へ送付し、又は持ち出すときは、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。）を使用してアクセス権限を識別する機能（以下「認証機能」という。）の設定その他のアクセスを制限するために必要な措置を講じなければならない。

（誤送付等の防止）

第１４条　職員は、保有個人情報を含む電磁的記録若しくは媒体の誤送信、誤送付若しくは誤交付又は保有個人情報の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又はその内容に応じ、複数の職員による確認、チェックリストの活用その他の必要な措置を講じなければならない。

（廃棄等）

第１５条　職員は、保有個人情報又は保有個人情報が記録されている媒体（端末又はサーバに内蔵されているものを含む。）が不要となったときは、保護管理者の指示に従い、当該保有個人情報の復元又は判読が不可能な方法により当該保有個人情報の消去又は当該媒体の廃棄を行わなければならない。

２　職員は、保有個人情報の消去又は保有個人情報が記録されている媒体の廃棄の委託（２以上の段階にわたる委託を含む。）をするときは、必要に応じて職員が消去及び廃棄に立ち会い、又は写真等を付した消去及び廃棄を証明する書類を受け取る方法等により、委託先において保有個人情報の消去及び保有個人情報が記録されている媒体の廃棄が確実に行われていることを確認しなければならない。

（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又はその内容により、必要に応じて台帳等を整備し、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しなければならない。

（外的環境の把握）

第１７条　保護管理者は、保有個人情報が外国（クラウドサービス提供事業者が所在する外国及び個人データが保存されるサーバが所在する外国又は日本以外の地域をいう。）において取り扱われるときは、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

（アクセス制限）

第１８条　保護管理者は、保有個人情報（情報システムで取り扱うものに限る。以下第３０条を除き、この章において同じ。）の秘匿性又はその内容に応じて、認証機能の設定その他のアクセスを制御するために必要な措置を講じなければならない。

２　保護管理者は、前項の措置を講じるときは、パスワード等の管理に関する定めを整備し、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じなければならない。

３　前項に規定する定めは、必要に応じて見直しを行うものとする。

（アクセス記録）

第１９条　保護管理者は、保有個人情報の秘匿性又はその内容に応じて、当該保有個人情報へのアクセスの状況を記録し、その記録（以下「アクセス記録」という。）を一定の期間保存し、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じなければならない。

２　保護管理者は、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じなければならない。

（アクセス状況の監視）

第２０条　保護管理者は、保有個人情報の秘匿性又はその内容及びその量に応じて、当該保有個人情報への不適切なアクセスの監視のため、保有個人情報を含み、又は含むおそ

れのある一定量以上の情報が情報システムからダウンロードされた場合に警告表示がなされる機能の設定、当該設定の定期的な確認その他の必要な措置を講じなければならない。

（管理者権限の設定）

第２１条　保護管理者は、保有個人情報の秘匿性又はその内容に応じて、情報システムの管理者としての権限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、当該権限を最小限とすることその他の必要な措置を講じなければならない。

（外部からの不正アクセスの防止）

第２２条　保護管理者は、保有個人情報を取り扱う情報システムへの外部からの不正アクセス行為（不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）第２条第４項に規定する不正アクセス行為をいう。）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じなければならない。

（不正プログラムによる漏えい等の防止）

第２３条　保護管理者は、不正プログラムによる保有個人情報の漏えい、滅失又は毀損の防止のため、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その他の必要な措置（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。）を講じなければならない。

（情報システムにおける保有個人情報の処理）

第２４条　職員は、保有個人情報について、一時的に加工等の処理を行うための複製等を行う場合は、その対象を必要最小限とし、処理終了後は不要となった情報を速やかに消去しなければならない。

２　保護管理者は、当該保有個人情報の秘匿性又はその内容に応じて、前項の規定による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２５条　保護管理者は、保有個人情報の秘匿性又はその内容に応じて、暗号化のために必要な措置を講じなければならない。

２　職員は、処理する保有個人情報の秘匿性又はその内容に応じて、適切に暗号化を行わなければならない。

（記録機能を有する機器又は媒体の接続制限）

第２６条　保護管理者は、保有個人情報の秘匿性又はその内容に応じて、当該保有個人情報の漏えい、滅失又は毀損の防止のため、記録機能を有する機器又は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。）その他の必要な措置を講じなければならない。

（端末の限定等）

第２７条　保護管理者は、保有個人情報の秘匿性又はその内容に応じて、その処理を行う端末を限定するために必要な措置を講じなければならない。

２　職員は、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。ただし、保護管理者が必要であると認めるときは、この限りでない。

（端末の盗難防止）

第２８条　保護管理者は、端末の盗難又は紛失の防止のため、端末の固定、執務室の施錠その他の必要な措置を講じなければならない。

（閲覧防止）

第２９条　職員は、端末の使用に当たっては、保有個人情報が当該職員以外の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その他の必要な措置を講じなければならない。

（入力情報の照合等）

第３０条　職員は、情報システムで取扱う保有個人情報の秘匿性又はその内容に応じて、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の内容の確認、既存の保有個人情報との照合等を行うものとする。

（バックアップ）

第３１条　保護管理者は、保有個人情報の秘匿性又はその内容に応じて、バックアップを作成し、分散保管をするために必要な措置を講じなければならない。

（情報システム設計書等の管理）

第３２条　保護管理者は、保有個人情報に係る情報システムの設計書、構成図その他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じなければならない。

第７章　情報システム室等の安全管理

（入退管理）

第３３条　保護管理者は、保有個人情報を取り扱う基幹的なサーバ等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。）に入室す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、部外者が入室す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その他の必要な措置を講じなければならない。

２　保護管理者は、保有個人情報を記録する媒体を保管するための施設（以下「保管施設」という。）を設けているときにおいても、必要があると認めるときは、同様の措置を講ずるものとする。

３　保護管理者は、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室の管理の容易化、所在表示の制限等の措置を講ずるものとする。

４　保護管理者は、情報システム室等及び保管施設の入退室の管理について、必要があると認めるときは、入室に係る認証機能を設定し、及びパスワード等の管理に関する規程を定め、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。

５　パスワード等の管理に関する前項の規定は、必要に応じて見直しを行うものとする。

（情報システム室等の管理）

第３４条　保護管理者は、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、監視設備の設置等の措置を講ずるものとする。

２　保護管理者は、災害等に備え、情報システム室等に、耐震、防火、防煙、防水その他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、配線の損傷防止その他の措置を講ずるものとする。

第８章　保有個人情報の提供

第３５条　保護管理者は、法第６９条第２項第４号の規定により行政機関等以外の者に保

有個人情報を提供する場合には、法第７０条の規定により、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書面を取り交わさなければならない。

２　保護管理者は、法第６９条第２項第４号の規定により行政機関等以外の者に保有個人情報を提供する場合には、法第７０条の規定により、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、その結果を記録するとともに、改善要求その他の措置を講ずるものとする。

３　保護管理者は、法第６９条第２項第３号の規定により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、法第７０条の規定により、前２項に規定する措置を講ずるものとする。

第９章　個人情報の取扱いの委託

（業務の委託等）

第３６条　市長は、個人情報の取扱いに係る業務を外部に委託するときは、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、必要な措置を講ずるものとする。

２　市長は、個人情報の取扱いに係る業務を外部に委託するときは、契約書に、次に掲げる事項を明記するとともに、委託先における責任者及び業務従事者の管理体制、個人情報の管理の状況についての検査に関する事項その他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、目的外利用の禁止等の義務に関する事項

（２）　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

（９）　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。）

３　市長は、保有個人情報の取扱いに係る業務を外部に委託するときは、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とする。

４　市長は、保有個人情報の取扱いに係る業務を外部に委託するときは、委託する業務に係る保有個人情報の秘匿性又は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、毎年少なくとも１回以上、原則として実地検査により確認するものとする。

５　市長は、保有個人情報の取扱いに係る業務が再委託されるときは、委託先に第１項及び第２項の対応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の秘匿性又はその内容に応じて、委託先を通じて又は市長が前項の対応を実施するものとする。保有個人情報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ときも同様とする。

６　市長は、保有個人情報の取扱いに係る業務を派遣労働者によって行わせるときは、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。

（業務の委託に関するその他の措置）

第３７条　保有個人情報を提供又は業務委託するときは、提供先の利用目的、委託する業務の内容、保有個人情報の秘匿性又はその内容を考慮し、必要に応じ、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、若しくは別の記号等に置き換えるその他の措置を講じなければならない。

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３８条　市長は、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

ときは、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号の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の性質等に照らし、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　安全確保上の問題への対応

（事案の報告及び再発防止措置）

第３９条　職員は、保有個人情報の漏えいについて安全確保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ときは、直ちに当該保有個人情報を管理する保護管理者に報告しなければならない。

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じなければならない。ただし、外部からの不正アクセス又は不正プログラムの感染が疑われる当該端末のLANケーブルを抜く等の被害拡大防止のための措置については、直ちに行う（職員に行わせるときを含む。）ものとする。

３　保護管理者は、事案の発生した経緯及び被害状況等を調査し、総括保護管理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ときは、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しなければならない。

４　総括保護管理者は、前項の規定により報告を受けたときは、事案の内容等に応じて、当該事案の内容、経緯及び被害状況等を市長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課等に再発防止措置を共有しなければならない。

（法に基づく報告及び通知）

第４０条　市長は、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ときは、前条により、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４１条　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の本人への連絡その他の措置を講じなければならない。

２　公表を行う漏えい等が発生したときは、当該事案の内容、経緯、被害状況等について、

速やかに個人情報保護委員会へ情報提供を行うものとする。

第１２章　監査及び点検の実施

（監査）

第４２条　監査責任者は、保有個人情報の適切な管理を検証するため、第２章から前章までに規定する措置の状況を含む久喜市における保有個人情報の管理の状況について、定期及び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４３条　保護管理者は、課等における保有個人情報の記録媒体、処理経路、保管方法等について、定期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４４条　総括保護管理者及び保護管理者は、監査又は点検の結果等を踏まえ、保有個人情報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、その見直しその他の措置を講ずるものとする。

第１３章　その他

第４５条　この訓令に定めるもののほか、保有する個人情報の適切な管理のための措置について、必要な事項は、市長が別に定める。

附　則

この訓令は、公布の日から施行し、令和５年４月１日から適用する。