千曲市訓令第７号

本　　庁
出先機関

千曲市保有個人情報等の取扱いに関する管理規程を次のように定める。

令和８年１１月２０日

千曲市長　小　川　修　一

千曲市保有個人情報等の取扱いに関する管理規程

目次

第１章　総則（第１条・第２条）
第２章　管理体制（第３条―第９条）
第３章　教育研修（第 10 条）
第４章　職員の責務（第 11 条）
第５章　安全管理措置（第 12 条―第 20 条）
第６章　情報システムにおける安全の確保等（第 21 条―第 36 条）
第７章　情報システム室等の安全管理（第 37 条・第 38 条）
第８章　業務の委託等（第 39 条―第 41 条）
第９章　安全管理上の問題への対応等（第 42 条―第 44 条）
第10章　補則（第 45 条）
附則

第１章　総則

（趣旨）

第１条　この規程は、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。）及び千曲市個人情報保護法施行条例（令和４年千曲市条例第 22 号）に定めるところにより、保有個人情報及び個人番号（以下「保有個人情報等」という。）の取扱いに関し必要な事項を定めるものとする。

（定義）

第２条　この規程における用語の意義は、個人情報保護法第２条及び番号法第２条に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　総括保護管理者を１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、市長を補佐し、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）

第４条　保有個人情報等を取り扱う課室等に、保護管理者を１人置くこととし、当該課室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、各課室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　保有個人情報等を情報システムで取り扱う場合、保護管理者は、当該情報システムの管理者と連携して、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室等に、当該各課室等の保護管理者が指定する保護担当者を１人又は複数名置く。

２　保護担当者は、保護管理者を補佐し、各課室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１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。

（委員会）

第７条　総括保護管理者は、保有個人情報等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委員会を設け、定期又は随時に開催する。

２　委員会には、必要に応じて情報セキュリティ等について専門的な知識及び経験を有する者等の参加を求めることとする。

（事務取扱担当者の指定等）

第８条　保護管理者は、個人番号及び特定個人情報（以下「特定個人情報等」という。）を取り扱う職員（以下「事務取扱担当者」という。）及びその役割を明確化し、事務取扱担当者を事務取扱担当者一覧（個人単位）（様式第１号）により指定する。

２　保護管理者は、事務取扱担当者が取り扱う特定個人情報等の範囲を明確化する。

（事務取扱担当者の監督）

第９条　総括保護管理者及び保護管理者は、特定個人情報等が本規定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。

第３章　教育研修

第10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。以下同じ。）に対し、保有個人情報等の適切な取扱いについて理解を深め、保有個人情報等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　総括保護管理者は、保護管理者及び保護担当者に対し、課室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行う。

４　保護管理者は、当該課室等の職員に対し、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とともに、研修未受講者に対して再受講の機会を付与する等の必要な措置を講ずる。

５　総括保護管理者は、教育研修を行うに当たり、個人情報等に関する研修計画（様式第２号）を策定し、研修計画に基づき教育研修を実施する。

６　総括保護管理者及び保護管理者は特定個人情報ファイルを取り扱う事務に従事する者に対し、番号法第 29 条の２に定めるサイバーセキュリティの確保に関する事項その他の事項に関する研修を行う。

第４章　職員の責務

（職員の責務）

第11条　職員は、個人情報保護法及び番号法の趣旨に則り、関連する法令及び規定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　安全管理措置

（取扱区域）

第12条　特定個人情報等を取り扱う事務を実施する区域においては、事務取扱担当者等以外の者が特定個人情報等を容易に閲覧できないように留意するほか、書類等の盗難又は紛失等を防止するために施錠可能な場所への保管等の物理的な安全管理措置を講ずる。

（アクセス制限）

第13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、当該情報にアクセスする権限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。

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、アクセスする場合も、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14条　職員が業務上の目的で保有個人情報等を取り扱う場合、保護管理者は、次の各号の行為については、当該情報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、職員は、保護管理者の指示に従わなければならない。

(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出し

(4)　前３号に掲げるもののほか、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15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、訂正等を行う。

（媒体の管理等）

第16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、キャビネットへの保管、施錠等を行う。

２　職員は、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、ＩＣカード、生体情報等（以下「パスワード等」

という。）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。

（誤送付等の防止）

第17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・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やチェックリストの活用等の必要な措置を講ずる。

（廃棄等）

第18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。

2　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。）には、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など、委託先において消去及び廃棄が確実に行われていることを確認する。

3　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。）には、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など、委託先において消去及び廃棄が確実に行われていることを確認する。

4　保有個人情報等を削除又は廃棄した場合には、その記録を保存する。

（保有個人情報等の取扱状況の記録）

第19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、台帳等を整備して、当該保有個人情報等の利用及び保管等の取扱いの状況について記録する。

（事務の流れの整理）

第20条　個人番号利用事務等の範囲等を明確にした上で、特定個人情報等の取扱いに関する事務マニュアル（様式第３号）により個人番号利用事務等の流れを整理し、管理段階ごとに安全管理措置を織り込む。

第６章　情報システムにおける安全の確保等

（情報資産）

第21条　個人番号利用事務の実施に当たり接続する情報提供ネットワークシステム等の接続規定等が示す安全管理措置を遵守する。

2　個人番号利用事務において使用する情報システムについて、インターネットから独立する等の高いセキュリティ対策を踏まえたシステム構築や運用体制整備を行う。

3　その他の情報資産の取扱いについては、千曲市情報セキュリティポリシーの例による。

（アクセス制御）

第22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。以下本章において同じ（第34条を除く。）。）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。

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。

3　前項の定めは、定期又は随時に見直しを行う。

（アクセス記録）

第23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。

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ずる。

（アクセス状況の監視）

第24条　保護管理者は、保有個人情報等の秘匿性等その内容及びその量に応じて、当該保有個人情報等への不適切なアクセスの監視のため、保有個人情報等を含む又は含むおそれが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、当該設定の定期的確認等の必要な措置を講ずる。

（管理者権限の設定）

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、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。

（外部からの不正アクセスの防止）

第26条　保護管理者は、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。

（不正プログラムによる漏えい等の防止）

第27条　保護管理者は、不正プログラムによる保有個人情報等の漏えい、滅失又は毀損（以下「漏えい等」という。）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。

（情報システムにおける保有個人情報等の処理）

第28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。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。

（暗号化）

第29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、暗号化のため

に必要な措置を講ずる。

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。

（記録機能を有する機器・媒体の接続制限）

第30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・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。

（端末の限定）

第31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、その処理を行う端末を限定するために必要な措置を講ずる。

（端末の盗難防止等）

第32条　保護管理者は、端末の盗難又は紛失防止のため、端末の固定、執務室の施錠等の必要な措置を講ずる。

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33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。

（入力情報の照合等）

第34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。

（バックアップ）

第35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。

（情報システム設計書等の管理）

第36条　保護管理者は、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。

第７章　情報システム室等の安全管理

（入退管理）

第37条　保護管理者は、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。）に立ち入る権限を有するものを定める。

2　保護管理者は、要件の確認、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。
3　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、前項と同様の措置を講ずる。
4　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の管理の容易化、所在表示の制限等の措置を講ずる。
5　保護管理者は、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し、及びパスワード等の管理に関する定めの整備、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。
6　前項の定めは定期又は随時に見直しを行う。

（情報システム室等の管理）

第38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措置及び監視設備の設置等の措置を講ずる。
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。

第８章　業務の委託等

（業務の委託等）

第39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、保有個人情報等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。なお、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。
2　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、あらかじめ書面で確認する。
3　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、少なくとも年１回以上、原則として実地検査により確認する。
4　委託先との契約書に、次の事項を明記する。
(1)　個人情報に関する秘密保持、利用目的外の目的のための利用の禁止等の義務
(2)　再委託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)　個人情報等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)　契約内容の順守状況についての定期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

(9)　事務所棟内からの特定個人情報等の持出しの禁止に関する事項
(10)　特定個人情報等を取り扱う従事者の明確化並びに当該従事者の監督及び教育に関する事項
5　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２項及び第４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第３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。
6　委託先が特定個人情報等の取扱いに係る業務を再委託しようとする場合は、番号法第10条に基づき、事前に許諾を行う。
7　前項の許諾を行う場合、委託をする個人番号利用事務等において取り扱う特定個人情報の適切な安全管理が図られていることを確認する。また、委託先が再委託先に対して必要かつ適切な監督を行うかを監督するものとし、特定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も同様とする。
8　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。
9　保有個人情報等を提供し、又は保有個人情報等の取扱いに係る業務を委託する場合には、漏えい等による被害発生のリスクを低減させるため、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。

（外的環境の把握）

第40条　外国において保有個人情報等を取り扱う場合には、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、保有個人情報等の安全管理のために必要かつ適切な措置を講ずる。

（サイバーセキュリティの確保）

第41条　保有個人情報等を取り扱い、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。

第９章　安全管理上の問題への対応等

（漏えい等事案の報告及び再発防止措置）

第42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恐れを認識した場合に、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。
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。
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。

4　総括保護管理者は、前項による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、被害状況等を市長に速やかに報告する。

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部局等に再発防止措置を共有する。

（法に基づく報告及び通知等）

第43条　保有個人情報等の漏えい等が生じた場合であって、個人情報保護法又は番号法の規定による個人情報保護委員会への報告及び本人への通知を要する場合には、前条の措置と並行して、速やかに所定の手続きを行うとともに、個人情報保護委員会による事案の把握等に協力する。

2　個人情報保護法又は番号法の規定による個人情報保護委員会への報告及び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。

（監査及び点検の実施）

第44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、本要領に記載する措置の状況を含む本市における保有個人情報等の管理状況について、定期に及び必要に応じ監査（外部監査を含む。）を行い、その結果を総括保護管理者に報告する。

2　監査責任者は、監査を行うに当たり、保有個人情報等に関する監査計画（様式第４号）を立案し、総括保護管理者の承認を得る。

3　保護管理者は、各課室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、その結果を総括保護管理者に報告する。

4　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。

附　則

（施行期日）

1　この訓令は、令和８年11月20日から施行する。

（千曲市特定個人情報の取扱いに関する管理規程の廃止）

2　千曲市特定個人情報等の取扱いに関する管理規程（令和５年千曲市訓令第５号）は、廃止する。

様式第１号（第８条関係）

年　　月　　日

事務取扱担当者一覧（個人単位）

	部	課	係	氏名	役職	事務	備考
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

注：適宜、行を追加すること。また、変更が生じた場合、速やかに反映させること。

様式第２号（第10条関係）

年　　月　　日

部

課

年度　個人情報等に関する研修計画

	実施時期	研修名	対象者	実施方法	備考
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

注：適宜、行を追加すること。

様式第３号（第20条関係）

年　　月　　日

部

課

特定個人情報等の取扱いに関する事務マニュアル

（　　に関する事務）

各事務手続の実施にあたっては、保有個人情報等の取扱いに関する管理規程を遵守する。

区　分	概　要（主な留意点）	担当（係）

注：適宜、行を追加すること

様式第４号（第44条関係）

年　　月　　日

部

課

年　保有個人情報等に関する監査計画

１．監査計画

1	監査目的	
2	監査範囲	
3	被監査部門	
4	監査方法	
5	監査実施日程	
6	監査実施体制	
7	適用基準	

２．監査結果のフォローアップ

総括保護管理者は、監査の結果等を踏まえ、必要があると認めるときは、取扱規程等の見直し等の措置を講ずることとする。

以　上