神河町個人情報等取扱規程

令和6年3月29日
規程第6号

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「法」という。）及び神河町個人情報の保護に関する法律施行条例（令和5年神河町条例第2号。以下「条例」という。）に定めるところにより、個人情報の安全管理のために必要な措置を定めるものとする。

（定義）

第2条　この規程において使用する用語は、法及び条例において使用する用語の例による。

（基本理念）

第3条　保有個人情報を取り扱うに当たっては、保有個人情報の漏えい等が生じた場合に本人が被る権利利益の侵害の大きさを考慮し、事務又は業務の規模及び性質、保有個人情報の取扱状況（取り扱う保有個人情報の性質及び量を含む。）、保有個人情報を記録した媒体の性質等に起因するリスクに応じて、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2章　管理体制

（総括保護管理者）

第4条　実施機関に、総括保護管理者を1人置くこととし、総務課長をもって充てる。

2　総括保護管理者は、実施機関の長を補佐し、各実施機関における保有個人情報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5条　保有個人情報を取り扱う課等に、保護管理者を1人置くこととし、当該課長に該当する者をもって充てる。

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を確保する任に当たる。保有個人情報を情報システムで取り扱う場合は、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6条　保有個人情報を取り扱う課等に、当該課等の保護管理者が指定する保護担当者を1人又は複数人置く。

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担当する。

（監査責任者）

第7条　実施機関に、監査責任者を1人置くこととし、総務課長をもって充てる。

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任に当たる。

（情報化推進委員会）

第8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、神河町情報セキュリティポリシー(2024年4月1日改定)に定める情報化推進委員会を、定期に又は随時に開催する。

2　総括保護管理者は、前項の委員会の開催に当たって、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。

第3章　教育研修

(教育研修の実施)

第9条　総括保護管理者及び保護管理者は、保有個人情報の取扱いに従事する職員(一般職及び特別職の職員並びに会計年度任用職員及び再任用職員をいう。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、保有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　総括保護管理者及び保護管理者は、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、保有個人情報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、課等の現場における保有個人情報の適切な管理のための教育研修を定期的に実施する。

4　保護管理者は、当該課等の職員に対し、保有個人情報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、研修計画を策定し、研修計画に基づき教育研修を実施する。

第4章　職員の責務

第10条　職員は、法及び条例の趣旨にのっとり、関連する法令及び規程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11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、当該保有個人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る。

2　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。

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12条　職員が業務上の目的で保有個人情報を取り扱う場合であっても、保護管理者は、次の行為については、当該保有個人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い行う。

(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ち出し
(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のある行為

(誤りの訂正等)

第13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、保護管理者の指示に従い、訂正等を行う。

(媒体の管理等)

第14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、必要があると認めるときは施錠等を行う。また、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。

(誤送付等の防止)

第15条　職員は、保有個人情報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16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(端末及びサーバに内蔵されているものを含む。)が、文書管理に関する規程等によって定められている保存期間を経過した場合その他不要となった場合には、保護管理者の指示に従い、できるだけ速やかに、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う。

2　保有個人情報を削除し、又は廃棄した場合には、必要に応じて、その記録を保存する。

3　保有個人情報の消去や保有個人情報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。

(保有個人情報の取扱状況の記録)

第17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。

(外的環境の把握)

第18条　保有個人情報が、外国において取り扱われる場合は、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

(アクセス制御)

第19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。

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の整備(その定期又は随時の見直しを含む。)をするとともに、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。

(アクセス記録)

第20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、当該保有個人情報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21条　保護管理者は、保有個人情報の秘匿性等その内容及びその量に応じて、当該保有個人情報への不適切なアクセスの監視のための必要な措置を講ずる。

(管理者権限の設定)

第22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、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23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24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。

(情報システムにおける保有個人情報の処理)

第25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26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、暗号化のために必要な措置を講ずる。職員は、これを踏まえ、その処理する保有個人情報について、当該保有個人情報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27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、当該保有個人情報の漏えい等の防止のため、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28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、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29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30条　職員は、端末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、使用状況に応じて情報システムからログアウト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31条　職員は、情報システムで取り扱う保有個人情報の重要度に応じて、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の内容の確認、既存の保有個人情報との照合等を行う。

(バックアップ)

第32条　保護管理者は、保有個人情報の重要度に応じて、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33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34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若しくは監視設備による監視又は外部電磁的記録媒体等の持ち込み、利用及び持ち出しの制限若しくは検査等の措置を講ずる。保有個人情報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、同様とする。

2　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。

3　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(その定期又は随時の見直しを含む。)、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。

(情報システム室等の管理)

第35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、警報装置及び監視設備を設置する等の措置を講ずる。

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　保有個人情報の提供

(保有個人情報の提供)

第36条　保護管理者は、法第69条第2項第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を提供する場合には、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。

2　保護管理者は、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を提供する場合には、法第70条の規定に基づき、安全管理の措置を講ずること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。

3　保護管理者は、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、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。

4　保有個人情報を提供する場合には、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、保有個人情報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。

第9章　個人情報の取扱いの委託等

(業務の委託等)

第37条　個人情報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、必要な措置を講ずる。また、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。

(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)　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　個人情報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　個人情報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個人情報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、定期的に、委託先からの報告書により確認し、必要に応じて実地検査により確認する。

4　委託先において、個人情報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個人情報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。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場合以降も、同様とする。

5　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。

6　個人情報の取扱いに係る業務を外部に委託する場合には、漏えい等による被害発生のリスクを低減する観点から、委託する業務の内容、個人情報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。

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　保有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、神河町情報セキュリティポリシー(2024年4月1日改定)を遵守するとともに、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39条　保有個人情報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。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。

4　総括保護管理者は、前項の規定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、被害状況等を実施機関の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）

第40条　漏えい等が生じた場合であって、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には、前条の規定に基づく措置と並行して、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。

（公表等）

第41条　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、当該事案に係る個人情報の本人への連絡、当該事案の内容、経緯、被害状況等についての個人情報保護委員会への情報提供等の措置を講ずる。

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章から前章までに記載する措置の状況を含む保有個人情報の管理の状況について、定期に、及び必要に応じ随時に監査（外部監査及び他部署等による点検を含む。以下同じ。）を行い、その結果を総括保護管理者に報告する。

2　監査責任者は、監査を行うに当たり、監査計画を立案し、総括保護管理者の承認を得る。

（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。

（評価及び見直し）

第44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。

第13章　雑則

（委任）

第45条　この規程に定めるもののほか、必要な事項は、実施機関の長が別に定める。

附　則

この規程は、令和6年4月1日から施行する。