地方独立行政法人北海道立総合研究機構が保有する個人情報等の適切な管理のための措置に関する基準

目　次

第１章　総則

（趣旨）

第１条　この基準は、地方独立行政法人北海道立総合研究機構北海道立総合研究機構（以下「道総研」という。）における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。）第23条に規定する個人データの安全管理のため、また、個人情報保護法第60条第１項に規定する保有個人情報及び第121条第２項に規定する行政機関等匿名加工情報等の適切な管理のために必要な措置について定めるものとする。

（定義）

第２条　この基準で使用する用語は、この基準で定めるもののほか、個人情報保護法、地方独立行政法人北海道立総合研究機構組織規程（平成22年４月１日規程第４号）等で使用する用語の例による。

第２章　管理体制

（総括保護管理者）

第３条　道総研に、総括保護管理者１人を置く。

２　総括保護管理者は、経営管理部長をもって充てる。

３　総括保護管理者は、道総研における保有個人情報の管理に関する事務を総括する。

（保護管理者）

第４条　各部等（部に相当する組織を含む。以下同じ。）に、保護管理者１人を置く。

２　保護管理者は、本部にあっては各部副部長、各研究本部又は各試験場等にあっては各部長（相当職を含む。部に所属しない課等にあっては課長等、支場にあっては支場長）

とし、地方独立行政法人北海道立総合研究機構情報セキュリティ対策基準（令和５年９月29日規程第35号。以下「対策基準」という。）別表に掲げる職にあるものとする。

３　保護管理者は、所管する所属における保有個人情報等管理に関する事務を総括する。

４　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、当該情報システムの管理者と連携して、前項の事務を行う。

（保護担当者）

第５条　各部等に、保護担当者を置く。

２　保護担当者は、保有個人情報等の管理を取り扱う事務を所管する所属の主幹（相当職を含む。）をもって充てる。

３　保護担当者は、保護管理者を補佐し、各部等における保有個人情報等の管理に関する事務を行う。

（監査責任者）

第６条　道総研に、監査責任者１人を置く。

２　監査責任者は、経営管理部副部長（総括を所管する者）をもって充てる。

３　監査責任者は、道総研における保有個人情報の管理の状況について監査する事務を総括する。

（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に対し、保有個人情報等の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研修を行わなければならない。

２　保護管理者は、各部等の職員に対し、保有個人情報等の適切な管理のため、総括保護管理者の実施する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３章　職員の責務

（職員の責務）

第８条　職員は、個人情報保護法の趣旨にのっとり、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、保有個人情報等を取り扱わなければならない。

第４章　保有個人情報等の取扱い

（複製等の制限）

第９条　保護管理者は、職員が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、次に掲げる行為については、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、職員は、保護管理者の指示に従い行うものとする。

⑴　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)　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として保護管理者が定めるもの

（誤りの訂正等）

第10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、訂正等を行うものとする。

（媒体の管理等）

第11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、当該媒体の耐火金庫への保管、保管場所への施錠等の保有個人情報等の漏えい等を防止するための措置を講ずるものとする。また、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、パスワードを設定する等の必要な措置を講ずるものとする。

第５章　情報システムにおける安全の確保等

（アクセス制御）

第12条　保護管理者は、情報システム管理者（対策基準第10条に規定する情報システム管理者をいう。以下同じ。）と連携して保有個人情報等（情報システムで取り扱うものに限る。以下第20条を除き、この章及び次章において同じ。）の秘匿性等その内容に応じて、パスワードを設定する等の当該保有個人情報等へのアクセスを制御するために必要な措置を講ずるものとする。（対策基準第86条及び第87条関係）

（アクセス記録）

第13条　保護管理者は、情報システム管理者と連携して、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、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。（対策基準第71条関係）

２　保護管理者は、情報システム管理者と連携して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。

（アクセス状況の監視）

第14条　保護管理者は、情報システム管理者と連携して、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必要な事項について、定期的な確認等の必要な措置を講ずるものとする。（対策基準第92条関係）

（管理者権限の設定）

第15条　保護管理者は、情報システム管理者と連携して、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付与されたＩＤを利用する者を必要

最小限にし、漏えい等が発生しないよう、必要な措置を講ずるものとする。（対策基準第89条関係）

（外部からの不正アクセスの防止）

第16条　保護管理者は、情報システム管理者と連携して、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。（対策基準第73条関係）

（不正プログラムによる漏えい等の防止）

第17条　保護管理者は、情報システム管理者と連携して、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を講ずるものとする。（対策基準第105条及び第109条関係）

（情報システムにおける保有個人情報等の処理）

第18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を行う場合には、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するものとする。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確認するものとする。

（暗号化）

第19条　保護管理者は、情報システム管理者と連携して、保有個人情報等の秘匿性等その内容に応じて、その暗号化のために必要な措置を講ずるものとする。職員は、これを踏まえ、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。（対策基準第18条関係）

（入力情報の照合等）

第20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21条　保護管理者は、情報システム管理者と連携して、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22条　保護管理者は、情報システム管理者と連携して、保有個人情報等に係る情報システムの仕様書及びその他の情報システムに関連する文書について業務上必要とする者以外の者が閲覧することのないよう適正に管理するとともに、当該情報システムが存続する限り保持しなければならない。（対策基準第70条関係）

（端末機器の限定）

第23条　保護管理者は、情報システム管理者と連携して、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処理を行う端末機器を限定するために必要な措置

を講ずるものとする。（対策基準第46条関係）

（端末機器の盗難防止等）

第24条　保護管理者は、情報システム管理者と連携して、端末機器の盗難又は紛失の防止のため、執務室の施錠等の必要な措置を講ずるものとする。

２　職員は、保護管理者及び情報システム管理者が必要があると認めるときを除き、端末機器を外部へ持ち出し、又は外部から持ち込んではならない。（対策基準第45条関係）

（閲覧防止）

第25条　職員は、端末機器の使用に当たっては、保有個人情報等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を徹底する等の必要な措置を講ずるものとする。（対策基準第48条関係）

（記録機能を有する機器・媒体の接続制限）

第26条　保護管理者は、情報システム管理者と連携して、外部記録媒体の紛失、盗難の防止その他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、必要な措置を講ずるものとする。（対策基準第37条関係）

（サイバーセキュリティに関する対策の基準等）

第27条　保護管理者は、情報システム管理者と連携して、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、対策基準により、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６章　情報システム室の安全管理

（情報システム室）

第28条　保護管理者は、情報システム管理者と連携して、保有個人情報等を取り扱う基幹的なサーバー等を設置する室その他の区域（以下「情報システム室」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、利用及び持出しの制限又は検査等の措置を講ずるものとする。また、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、同様の措置を講ずるものとする。（対策基準第29条及び第30条関係）

（入退室管理）

第29条　保護管理者は、情報システム管理者と連携して、情報システム室への入退室を許可された者のみに制限し、入退室管理簿の記録及びＩＣカード等による入退室管理を行わなければならない。

２　保護管理者は、情報システム管理者と連携して、情報システム室の入退の管理について必要があると認めるときは、身分証明書の提示を求めるとともに、必要の都度、その提示を求め確認しなければならない。（対策基準第31条関係）

（情報システム室の管理）

第30条　保護管理者は、情報システム管理者と連携して、外部からの不正な侵入に備え、情報システム室に制御機能、施錠装置、警報装置及び監視設備の整備等の措置を講ずるものとする。（対策基準第29条第３項及び第30条関係）

２　保護管理者は、情報システム管理者と連携して、災害等に備え、情報システム室に、耐震、防火、防煙、防水等の必要な措置を講ずるとともに、サーバー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。（対策基準第37条第４項関係）

第７章　保有個人情報等の提供及び業務の委託等

（保有個人情報等の提供）

第31条　保護管理者は、個人情報保護法第27条第５号から第７号の規定に基づき第三者に保有個人情報を提供する場合には、提供する保有個人情報の範囲を限定するなど、学術研究の目的に照らして可能な措置を講ずるものとする。

２　保護管理者は、個人情報保護法第109条第２項及び第３項の規定により、法令に基づく場合を除き、利用目的以外の目的のために行政機関等匿名加工情報及び削除情報（保有個人情報に該当するものに限る。）を自ら利用し、又は提供してはならない。

３　保護管理者は、個人情報保護法第109条第２項及び第115条の規定（第118条の規定により第115条の規定を準用する場合を含む。）により、行政機関等匿名加工情報の利用に関する契約を締結した者（以下「契約相手方」という。）から個人情報保護法第112条第２項第７号の規定に基づき当該契約相手方が講じた行政機関等匿名加工情報の適切な管理に支障を及ぼすおそれがある旨の報告を受けたときは、直ちに総括保護管理者に報告するとともに、当該契約相手方がその是正のために講じた措置を確認するものとする。

（業務の委託等）

第32条　保有個人情報若しくは行政機関等匿名加工情報等の取扱いに係る業務又は行政機関等匿名加工情報の作成に係る業務を外部に委託する場合には、当該各情報の適正な管理を行うことができる者を委託先として選定するものとする。また、契約書に、次の条文を追加し、次の（1）から（8）に掲げる事項を明記した別紙「個人情報取扱特記事項」（以下「特記事項」という。）を契約書に添付若しくは契約書本文に記載するとともに、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、個人情報又は行政機関等匿名加工情報等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十分に確認し、適切な監督を行うものとする。

　なお、契約書等の書面を作成しない契約の場合には、特記事項を契約事項として受託者に交付するものとする。

（個人情報の保護）
第〇条　乙は、この契約による業務を処理するための個人情報の取扱いについては、別記「個人情報特記事項」を遵守しなければならない。

(1)　個人情報又は行政機関等匿名加工情報等に関する秘密保持、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。本号及び第６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)　個人情報又は行政機関等匿名加工情報等の複製等の制限に関する事項
(4)　個人情報又は行政機関等匿名加工情報等の安全管理措置に関する事項
(5)　個人情報又は行政機関等匿名加工情報等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又は行政機関等匿名加工情報等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又は行政機関等匿名加工情報等の取扱状況を把握するための事項

２　保有個人情報又は行政機関等匿名加工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　委託先において、保有個人情報若しくは行政機関等匿名加工情報等の取扱いに係る業務又は行政機関等匿名加工情報の作成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ものとする。保有個人情報又は行政機関等匿名加工情報等の取扱いに係る業務若しくは行政機関等匿名加工情報の作成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。

４　保有個人情報を提供し、又は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若しくは一部を削除し、又は別の記号等に置き換える等の措置を講ずる。

第８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33条　保有個人情報等の漏えい等の事案が発生した場合等、安全管理の上で問題となる事案の発生を認識した場合に、その事案の発生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、情報システム管理者と連携して、被害の拡大防止、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端末ネットワーク遮断スクリプトの実行等によるネットワークからの遮断など、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ものとする。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、前項の規定に基づく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、被害状況等を理事長に速やかに報告するものとする。

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、総括保護管理者に当該措置を報告するものとする。

６　総括保護管理者は、同種の業務を実施している所属に前項の措置を共有するものとする。

（法に基づく報告及び通知）

第34条　漏えい等が生じた場合であって個人情報保護法第26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、前条で定める事項と並行して、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35条　個人情報保護法第26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対応等の措置を講ずるものとする。公表を行う事案については、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事務局に情報提供を行うものとする。

第９章　監査及び点検の実施

（監査）

第36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章から第８章の措置状況を含む保有個人情報の管理の状況について、必要に応じ随時に監査を行い、その結果を総括保護管理者に報告ものとする。

（点検）

第37条　保護管理者は、所管する所属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必要に応じ点検を行い、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38条　総括保護管理者及び保護管理者等は、監査又は点検の結果等を踏まえ、実行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ものとする。

第10章　補則

（個人情報保護委員会事務局への報告）

第39条　保護管理者は、行政機関等匿名加工情報等に関して、次に掲げるときは、直ちに個人情報保護委員会事務局に報告するものとする。

(1)　第29条第３項、第31条第３項及び第４項の報告をするとき

(2)　第31条第５項及び第６項、第33条の措置を講じたとき

(3)　契約相手方が個人情報保護法第120条各号に該当すると認められ、契約を解除しようとするとき及び解除したとき

（他の基準との関係）

第40条　他の基準の規定により、情報システムの管理に関する事項について、この基準と別段の定めが設けられている場合にあっては、この基準に定めるもののほか、当該基準の定めるところによる。

（細則）

第41条　この基準の施行に関し必要な事項は、別に総括保護管理者が定める。

２　保護管理者は、この基準の実施のため、又は保有個人情報等の適切な管理のため、必要があるときは、細則を定めることができる。

３　保護管理者は、前項の細則を定め、変更し、又は廃止したときは速やかに総括保護管理者に報告しなければならない。

附　則

１　この要綱は、令和６年１月５日から施行し、令和５年４月１日から適用する。

２　この基準の施行の際「地方独立行政法人北海道立総合研究機構個人情報取扱事務委託等の基準」の規定に基づいて作成されている用紙がある場合においては、この基準によるそれぞれの規定に関わらず、当分の間、必要な調整をして使用することを妨げない。

個人情報特記事項

（基本的事項）

第１　受託者及び受託者の業務に従事する職員（雇用関係のない職員を含む。以下同じ。）は、この委託業務を処理するに当たって、個人情報の保護の重要性を認識し、個人情報の保護に関する法令等を遵守し、個人の権利、利益を侵害することのないよう適正に行わなければならない。

（秘密の保持）

第２　受託者及び受託者の業務に従事する職員は、この契約による業務を処理するために知り得た個人情報の内容を他に漏らしてはならない。

２　受託者は、その使用する者が、この契約による業務を処理するために知り得た個人情報の内容を他に漏らさないようにしなければならない。

３　前２項の規定は、この契約が終了し、又は解除された後においても、また同様とする。

（適正な取得・目的外利用の禁止）

第３　受託者及び受託者の業務に従事する職員は、この契約による事務を処理するため、個人情報を収集し、又は利用するときは、受託事務の目的の範囲内で、適正かつ公正な手段により行うものとする。

２　受託者は、委託者の指示又は承諾があるときを除き、この委託業務に係る個人情報を、他の目的に利用してはならない。

（第三者への提供制限）

第４　受託者及び受託者の業務に従事する職員は、この契約による事務を処理するため委託者から提供された個人情報が記録された資料等を委託者の承諾なしに第三者に提供してはならない。

（再委託の禁止）

第５　受託者は、この委託業務を処理するに当たって、個人情報を自ら取り扱うものとし、第三者に取り扱わせてはならない。ただし、あらかじめ、委託者の書面による承諾を得た場合はこの限りでない。

２　受託者は、前項ただし書きの規定により第三者（以下「再受託者」という。）に個人情報を取り扱わせる場合は、再受託者の当該業務に関する行為について、委託者に対しすべての責任を負うものとする。

３　受託者は、個人情報を取り扱う業務を再受託者に委託し、又は請け負わせる場合には、再受託者がこの規定を遵守するために必要な事項及び委託者が指示する事項について再受託者と約定しなければならない。

４　受託者は、前項の約定において、再受託者が個人情報を第三者に取り扱わせることを例外なく禁止しなければならない。

（複写、複製の禁止）

第６　受託者及び受託者の業務に従事する職員は、この契約による業務の処理するため委託者から提供された個人情報が記録された資料等（情報記録媒体を含む。）を、委託者の承諾なしに複写し、又は複製をしてはならない。

（安全管理措置）

第７　受託者及び受託者の業務に従事する職員は、取り扱う個人情報の漏えい、滅失又はき損の防止その他の個人情報の安全管理のための必要かつ適切な措置を講じなければならない。

（漏えい等の報告等）

第８　受託者は、個人情報等の漏えい、滅失、毀損等の事案が発生した場合、また安全管理の上で問題となる事案の発生を認識した場合に、直ちに委託者に報告しなければならない。この契約が完了し、又は解除された後においても同様とする。

（提供資料等の返還等）

第９　受託者及び受託者の業務に従事する職員は、業務を処理するため委託者から提供された、又は自らが収集した個人情報が記録された資料等を、業務完了後、速やかに委託者に返還し、又は引き渡すものとする。ただし、委託者が別に指示したときは、当該方法によるものとする。

（契約解除及び損害賠償）

第 10　委託者は、次のいずれかに該当するときは受託者に対し、この契約の解除及び損害賠償の請求をすることができる。

(1)　この委託業務を処理するために受託者又は再受託者が取り扱う個人情報について、受託者又は再受託者の責に帰すべき理由による漏えいがあったとき。

(2)　前号に掲げる場合のほか、この特記事項に違反し、この委託業務の目的を達成できないと認められるとき。

（契約内容の遵守及び取扱状況の報告等）

第 11　委託者は、個人情報を保護するために必要があると認められるときは、受託者に対し、契約内容の遵守状況及び取扱状況について報告若しくは資料の提出を求めることができる。

（注）委託等の事務の実態に即して適宜必要な事項を追加し、又は不要な事項は省略して差し支えないものとする。