東近江市保有個人情報等取扱規程

目次

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。）第66条第１項及び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。）第12条の規定により、市長が保有する保有個人情報及び個人番号（以下「保有個人情報等」という。）の漏えい、滅失又は毀損（以下「漏えい等」という。）の防止その他の保有個人情報等の安全管理のために必要な措置等について定めるものとする。

（定義）

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

第２章　管理体制

（総括責任者）

第３条　実施機関に総括責任者を１人置くこととし、副市長をもって充てる。

２　総括責任者は、保有個人情報等の管理を総括する任に当たる。

（総括保護管理者）

第４条　保有個人情報等を取り扱う部に総括保護管理者を１人置くこととし、当該部の長をもって充てる。

２　総括保護管理者は、総括責任者を補佐し、当該部における保有個人情報等を適切

に管理する任に当たる。

（保護管理者）

第５条　保有個人情報等を取り扱う課等に保護管理者を１人置くこととし、当該課等の長をもって充てる。

２　保護管理者は、当該課等における保有個人情報等を適切に管理する任に当たる。

（情報システム管理者）

第６条　保有個人情報等を取り扱う情報システムを管理する実施機関に情報システム管理者を１人置くこととし、情報セキュリティに関する事務を分掌する課等の長をもって充てる。

２　情報システム管理者は、保有個人情報等を情報システムで取り扱う場合、保護管理者と連携して保有個人情報等を適切に管理する任に当たる。

（保護担当者）

第７条　保有個人情報等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、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８条　保有個人情報等を取り扱う実施機関に監査責任者を１人置くこととし、個人情報の保護に関する事務を分掌する課等の長（以下「個人情報保護担当課長」という。）をもって充てる。

２　監査責任者は、保有個人情報等の管理状況について監査する任に当たる。

（特定個人情報等の適切な管理のための組織体制）

第９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（派遣労働者を含む。以下「事務取扱担当者」という。）を指定する。

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及び個人番号を取り扱う事務の範囲を指定する。

３　前項の規定による指定を行う場合において、保護管理者は、その特定個人情報等の利用目的を達成するために必要最小限の範囲としなければならない。

４　保護管理者は、第１項及び第２項の規定により指定した内容を記載した事務取扱担当者等整理票（様式第１号）を作成するものとする。

５　前各項の規定は、番号法第27条第１項の規定により特定個人情報保護評価を実施した事務については、適用しない。

６　保護管理者は、特定個人情報等を複数の課等で取り扱う場合の各課等の任務分担

及び責任について明確にしなければならない。

（保有個人情報等取扱検討会議）

第10条　保有個人情報等の取扱いに係る重要事項の決定、連絡、調整等を行うため、保有個人情報等取扱検討会議（以下「会議」という。）を設置する。

２　会議は、会長、副会長及び委員をもって組織する。

３　会長は、個人情報の保護に関する事務を分掌する部の長（以下「個人情報保護担当部長」という。）をもって充てる。

４　副会長は、個人情報保護担当課長をもって充てる。

５　副会長は、会長を補佐し、会長に事故があるとき又は会長が欠けたときは、その職務を代理する。

６　委員は、個人情報の保護に関する事務を分掌する課等の職員その他保有個人情報等の取扱いに関する課等の職員をもって充てる。

７　会議は、必要に応じて会長が招集し、会長が議長となる。

８　会長は、会議における審議の結果について必要と認める事項を総括責任者に報告するものとする。

第３章　教育研修

（教育研修）

第11条　個人情報保護担当部長は、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ものとする。

２　情報セキュリティに関する事務を分掌する部の長(以下「情報システム担当部長」という。）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ものとする。

３　個人情報保護担当部長は、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等の適切な管理のために必要な教育研修を行うものとする。

４　総括保護管理者及び保護管理者（以下「総括保護管理者等」という。）は、当該部及び課等の職員に対し、保有個人情報等の適切な管理のために、個人情報保護担当部長及び情報システム担当部長の実施する教育研修への参加の機会を付与する等必要な措置を講じなければならない。

第４章　職員の責務

（職員の責務）

第12条　職員は、法及び番号法の趣旨にのっとり、関連する法令、規程等の定め及び

総括責任者、総括保護管理者等の指示に従い、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、当該保有個人情報等にアクセスする権限を有する職員をその利用目的を達成するために必要最小限に限るものとする。

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　アクセス権限を有する職員であっても、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ない。

（複製等の制限）

第14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、次に掲げる行為については、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、訂正等を行わなければならない。

（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、耐火金庫への保管、施錠等を行うものとする。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じなければならない。

（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ぐため、事務において取り扱う保有個人情報等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じなければならない。

（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で、東近江市文書管理規程（令和３年東近江市訓令第１号）第22条第１項に規定する公文書保存期間基準による保存期間が満了したときは、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保有個人情報等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、前項に規定する場合において、保有個人情報等に個人番号が含まれている場合は、保護管理者の指示に従い、前項に規定する方法により確実かつ速やかに当該個人番号の消去又は当該個人番号が記録されている媒体の廃棄を行わなければならない。

３　職員は、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職員以外の第三者に行わせる場合は、保護管理者の指示に従い、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、第三者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ものとする。

（取扱状況の記録）

第19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、当該保有個人情報等の利用、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20条　保有個人情報等が外国において取り扱われる場合、保護管理者は、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じなければならない。

（取扱区域における配慮）

第21条　保護管理者は、特定個人情報等を取り扱う事務を実施する区域（以下「取扱区域」という。）について、事務取扱担当者以外の者が特定個人情報等を容易に閲覧することができないよう配慮するものとする。

（取扱区域からの持ち出し）

第22条　職員は、特定個人情報等が記録された電子媒体又は書類等を取扱区域からその区域外へ持ち運ぶ必要がある場合は、容易に個人番号が判明しないよう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23条　情報システム管理者及び保護管理者（以下「システム管理者等」という。）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をするために必要な措置を講じなければならない。

２　システム管理者等は、特定個人情報等を取り扱う情報システムにおいて、事務取扱担当者がアクセス権を有する者であることを識別した結果に基づき認証するために必要な措置を講じなければならない。

３　システム管理者等は、前２項の措置を講ずる場合において、パスワード等の管理に関する定めの整備（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じなければならない。

（アクセス記録）

第24条　システム管理者等は、次に掲げる措置を講じなければならない。

(1) 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

(2) 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

（アクセス状況の監視）

第25条　システム管理者等は､保有個人情報等の秘匿性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じなければならない。

（管理者権限の設定）

第26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、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じなければならない。

（外部からの不正アクセスの防止）

第27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28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等の処理）

第29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とし、処理の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、当該保有個人情報等の秘匿性等その内容に応じて、随時、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30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じなければならない。

２　職員は、前項の規定による措置を踏まえ、保有個人情報等の秘匿性等その内容に応じて、適切に暗号化を行わなければならない。

（記録機能を有する機器及び媒体の接続制限）

第31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、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。）等必要な措置を講じなければならない。

（端末の限定）

第32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、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。

（端末の盗難防止等）

第33条　保護管理者は、端末の盗難又は紛失の防止のため、執務室の施錠等必要な措置を講じなければならない。

２　職員は、端末を施錠できる机等で保管する等端末の盗難又は紛失の防止のために必要な措置を講じなければならない。

３　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34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じなければならない。

（入力情報の照合等）

第35条　職員は、情報システムへの入力により保有個人情報等の処理を行うに当たっ

ては、保有個人情報等の重要度に応じて、当該処理に係る入力原票と入力内容との照合、当該処理の前後における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わなければならない。

（バックアップ）

第36条　システム管理者等は、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じなければならない。

（情報システム設計書等の管理）

第37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じなければならない。

第７章　電算室の安全管理

（入退室の管理）

第38条　システム管理者は、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「電算室」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、入退室の記録、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じなければならない。また、保護管理者は、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、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。

２　システム管理者は、必要があると認めるときは、電算室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。

３　システム管理者は、電算室の入退室の管理について、必要があると認めるときは、立入りに係る認証機能の設定、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ものとする。

（電算室の管理）

第39条　システム管理者は、外部からの不正な侵入に備え、電算室に施錠装置、警報装置、監視設備の設置等の措置を講じなければならない。

２　システム管理者は、災害等に備え、電算室に耐震、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じなければならない。

第８章　情報システムのセキュリティ確保の対策

（情報システムのセキュリティ確保の対策）

第40条　保有個人情報等を取り扱う情報システムのセキュリティ確保の対策は、市長

が別に定める。

第９章　保有個人情報等の提供及び業務の委任等

（保有個人情報の提供）

第41条　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は、法第70条の規定により原則として、保有個人情報の提供を受ける者と提供先における利用目的、利用する業務の根拠法令（条例を含む。）、利用する記録範囲及び記録項目、利用形態等について利用目的以外の目的のために保有個人情報を提供する場合における確認書（様式第２号）により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３号及び第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は、法第70条の規定により保有個人情報の提供を受ける者に対し、当該保有個人情報の安全を確保する措置を要求するとともに、必要があると認めるときは、当該保有個人情報の提供前又は随時に実地の調査等を行い、当該措置の状況を確認し、その結果を記録するとともに、改善の要求等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ものとする。

（個人情報等の取扱いの委任等）

第42条　保護管理者は、個人情報及び個人番号（以下「個人情報等」という。）を取り扱う業務を第三者に行わせる場合（事務の委託及び業務の指定管理を含む。以下「委任」という。）は、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にしなければならない。この場合においては、契約書、協定書等に次に掲げる事項を明記するとともに、委任先における責任者、従事者の管理及び実施体制、個人情報等を取り扱う作業場所並びに個人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確認しなければならない。

(1) 個人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) 再委任（個人情報等を取り扱う業務の委任を受けた第三者（以下「受任者」という。）が別の第三者（受任者の子会社（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。）である場合を含む。以下「再受任者」という。）に個人情報等を取り扱う業務を委任することをいう。以下同じ。）の制限又は事前承認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) 個人情報等の安全管理措置に関する事項
(5) 個人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) 契約、協定等の終了時における個人情報等の消去及び媒体の返却に関する事項
(7) 契約、協定等に違反した場合における契約、協定等の解除、損害賠償責任その他必要な事項
(8) 契約、協定等の遵守状況についての報告に関する事項及び委任された個人情報等の取扱いの状況を把握するための監査等に関する事項（再受任者の監査等に関する事項を含む。）
(9) 前各号に掲げるもののほか、個人情報等の安全管理のために必要と認める事項

2　前項の規定による委任先における責任者、従事者の管理及び実施体制並びに個人情報等を取り扱う作業場所の確認は、個人情報等管理体制報告書（様式第３号）により行うものとする。

3　受任者に委任する場合において、保護管理者は、取り扱わせる個人情報等の範囲を委任する業務の内容に照らして必要最小限としなければならない。

4　受任者に委任する場合において、保護管理者は、委任する業務に係る個人情報等の秘匿性等その内容、量等に応じて、作業の管理体制及び実施体制並びに個人情報等の管理の状況について、実地検査により確認するものとする。

5　受任者が再委任をする場合において、保護管理者は、受任者に第１項及び第２項に規定する措置を講じさせるとともに、再委任される業務に係る個人情報等の秘匿性等その内容に応じて、受任者に前項に規定する措置を講じさせなければならない。個人情報等の取扱いに係る業務が更に委任される場合も同様とする。

6　委任を行い、及び再委任が行われる場合において、保護管理者は、受任者及び再受任者において市長が果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行わなければならない。

7　受任者が再委任をしようとする場合において、保護管理者は、再受任者において個人情報等の適切な安全管理が図られることを確認した上で再委任の諾否を判断しなければならない。

（提供及び委任における措置）

第43条　保有個人情報等を提供し、又は委任する場合には、保護管理者は、保有個人情報等の漏えい等による被害の発生の危険性を低減するため、提供先の利用目的、委任する業務の内容、保有個人情報等の秘匿性等その内容等を考慮し、必要に応じて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。

（派遣労働者における取扱いに係る措置）

第44条　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は、保護管理者は、労働者派遣契約書に秘密保持義務等の個人情報等の取扱いに関する事項を明記しなければならない。

第10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45条　保有個人情報等の漏えい等の事案の発生又は兆候を把握した場合及び職員が法、番号法、この規程等に違反している事実又は兆候を把握した場合その他保有個人情報等の安全を確保する上で問題となる事案（以下「事案」という。）が発生した場合に、その事実を知った職員は、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しなければならない。

２　前項の規定による事案の報告を受けた保護管理者は、事案が発生したと認めるときは、次に掲げる措置等を速やかに講じなければならない。この場合において、事案に係る保有個人情報等を情報システムで取り扱っている場合には、保護管理者は、情報システム管理者と連携し対応するものとする。

(1) 被害の拡大防止又は復旧等のために必要な措置。ただし、外部からの不正アクセス、不正プログラムの感染等が疑われる端末等の隔離等、直ちに行い得る措置については、直ちに行うものとする。

(2) 報告を受けた事案に係る状況の整理並びに総括保護管理者及び個人情報保護担当課長への報告

３　総括保護管理者等は、事案の発生した経緯、被害状況等を調査し、当該事案の内容等に応じて、総括責任者に当該事案の内容、経緯、被害状況等について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場合には、直ちに総括責任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　総括責任者は、前項の規定による報告を受けた場合は、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しなければならない。

５　総括保護管理者等は、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、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等）

第46条　保有個人情報（特定個人情報ファイルに記録された特定個人情報を除く。）の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（以下「委員会」という。）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は、総括保護管理者等は、個人情報保護担当課長と協議し、前条の規定による措置と並行して、速やかに個人情報の保護に関する法律施行規則（平成28

年個人情報保護委員会規則第３号）第44条及び第45条の規定による手続を行うとともに、委員会による事案の把握等に協力しなければならない。

２　特定個人情報ファイルに記録された特定個人情報の漏えい等が生じた場合であって、番号法第29条の４第１項の規定による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は、総括保護管理者等は、個人情報保護担当課長と協議し、前条の規定による措置と並行して、速やかに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第29条の４第１項及び第２項に基づく特定個人情報の漏えい等に関する報告等に関する規則（平成27年特定個人情報保護委員会規則第５号）第３条及び第５条の規定による手続を行うとともに、委員会による事案の把握等に協力しなければならない。

３　前２項に規定する場合以外であって、漏えい等が発生し公表したとき、この規程等に対する違反があったとき、受任者又は再受任者において個人情報の適切な管理に係る契約条項等に対する違反があったときその他の市民等の不安を招きかねない事案が発生したときは、総括保護管理者等は、個人情報保護担当課長と協議し、前条の規定による措置と並行して、当該事案の内容、経緯、被害状況等について、必要に応じて速やかに委員会へ情報提供を行うものとする。

４　前２項に規定する場合以外であって、前項の規定による情報提供を行った場合その他事案が発生したときは、総括保護管理者等は、個人情報保護担当課長と協議し、前条の規定による措置と並行して、本人に対し、事案の内容、影響等に応じて、本人の権利利益を保護するために必要な範囲において、事案の概要、保有個人情報等の項目、漏えい等の原因、二次被害又はそのおそれの有無及びその内容並びにその他参考となる事項を必要に応じて通知するものとする。

（公表等）

第47条　前条第１項又は第２項に規定する場合その他事案が発生した場合において、総括保護管理者等は、個人情報保護担当課長と協議し、事案の内容、影響等に応じて、事実関係、再発防止策等について速やかに公表するものとする。

第11章　監査及び点検の実施

（監査）

第48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、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、定期に及び必要に応じて随時に監査（外部監査を含む。以下同じ。）を行い、その結果を総括責任者及び総括保護管理者に報告しなければならない。

（点検）

第49条　保護管理者は、自ら管理責任を有す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て随時に点検を行い、必要があると認めるときは、その結果を総括責任者及び総括保護管理者に報告しなければならない。

（評価及び見直し）

第50条　総括責任者及び総括保護管理者等は、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じなければならない。

（特定個人情報保護評価）

第51条　システム管理者等は、特定個人情報の漏えいその他の事態を発生させる危険性を軽減するための措置として、評価書（番号法第28条第１項に規定する評価書をいう。）に記載した全ての措置を講じなければならない。

附　則

この訓令は、令和５年４月１日から施行する。