独立行政法人国立文化財機構保有個人情報等取扱細則

平成１９年４月１日
国立文化財機構細則第２２号

第１章　保有個人情報等

（総則）

第１条　独立行政法人国立文化財機構保有個人情報等管理規程（平成１９年国立文化財機構規程第５９号。以下「管理規程」という。）による保有個人情報等の適切な管理のために必要な措置については，法令又は別に定める場合を除き，この細則の定めるところによる。

（定義）

第２条　この細則における用語の定義は，管理規程第１条から第７条までに規定するものをいう。

（教育研修）

第３条　総括保護管理者は，保有個人情報等を取り扱う役員及び職員（派遣労働者を含む。以下「職員等」という。）に対し，保有個人情報等の取扱いについて理解を深め，個人情報及び特定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　総括保護管理者は，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等に対し，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　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の適切な管理のための教育研修を実施する。

４　保護管理者は当該担当部課等の職員等に対し，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等の必要な措置を講ずるものとする。

（保有個人情報等の取扱い）

第４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等は，保有個人情報等にアクセスしてはならない。

３　職員等は，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等にアクセスしてはならない。

４　職員等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，保護管理者は，

次に掲げる行為については，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限定し，職員等は，保護管理者の指示に従わねばならない。

(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)　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

５　職員等は，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。

６　職員等は，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。

７　職員等は，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ものとする。

８　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。

９　保有個人情報が，外国において取り扱われる場合，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。

１０　保護管理者は，個人番号の利用に当たり，番号法があらかじめ限定的に定めた事務に限定する。

１１　個人番号利用事務又は個人番号関係事務（以下「個人番号利用事務等」という。）を処理するために必要な場合その他番号法で定める場合を除き，個人番号の提供を求めてはならない。

１２　個人番号利用事務等を処理するために必要な場合その他番号法で定める場合を除き，特定個人情報ファイルを作成してはならない。

１３　番号法第１９条各号のいずれかに該当する場合を除き，他人の個人番号を含む個人情報を収集又は保管してはならない。

１４　保護管理者は，特定個人情報ファイルの取扱状況を確認する手段を整備して，当該特定個人情報等の利用及び保管等の取扱状況について記録する。

１５　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。）を明確にし，物理的な安全措置を講ずる。

（情報システムにおける安全の確保等）

第５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。以下本条（第１６項を除く。）において同じ。）の秘匿性等その内容に応じてパスワード等（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ものとする。

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（その定期又は随時の見直しを含む。）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ものとする。

3　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ものとする。

4　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ものとする。

5　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，当該保有個人情報を取り扱うための業務システムを導入する。当該システムにおいては，当該保有個人情報への不適切なアクセスの監視のため，保有個人情報を含むか又は含むおそれがある一定量以上の情報が当該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。

6　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。

7　情報システム担当保護管理者は，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ものとする。

8　情報システム担当保護管理者は，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。）を講ずるものとする。

9　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。

10　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ものとする。

　職員等は，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。

11　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，滅失又は毀損の防止のため，第５項に規定する業務システムに接続する情報システ

ム端末等においては，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。

12　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ものとする。

13　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ものとする。

14　職員等は，保護管理者が必要があると認める場合を除き，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。

15　職員等は，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ものとする。

16　職員等は，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。

17　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ものとする。

18　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ものとする。

（情報システム室等の安全管理）

第６条　情報システム担当保護管理者は，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等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。

２　情報システム担当保護管理者は，必要があると認めるときは，情報システム室等の出入り口の特定化によるに入退の管理の容易化，所在表示の制限等の措置を講ずるものとする。

３　情報システム担当保護管理者は，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ものとする。

４　情報システム担当保護管理者は，外部からの不正な侵入に備え，必要に応じて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。

５　情報システム担当保護管理者は，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ものとする。

（保有個人情報等の提供及び業務の委託等）

第７条　保護管理者は，保有個人情報等を提供する場合には，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，利用する記録範囲内及び記録項目，利用形態等について書面を取り交わすものとする。

２　保護管理者は，保有個人情報等を提供する場合には，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，提供前に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ものとする。

３　保護管理者は，行政機関又は独立行政法人等に保有個人情報等を提供する場合において，必要があると認めるときは，前二項に規定する措置を講ずるものとする。

４　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，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。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

(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。本号及び 6 号において同じ。）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)　個人情報の漏えい等の事案の発生時における対応に関する事項

(5)　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

(6)　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

５　保有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保有個人情報の秘匿性等その内容やその量等に応じて，委託先における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。

６　委託先において，保有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４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５の措置を実施する。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場合以降も同様とする。

７　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。

８ 保有個人情報を提供又は業務委託する場合には、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、氏名を番号に置き換える等の匿名化措置を講ずる。

（安全確保上の問題への対応）

第８条　保有個人情報等の漏えい，滅失又は毀損等の事案の発生又は兆候を把握した場合及び事務取扱担当者が管理規程等に違反している事実又は兆候を把握した場合等，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場合に，その事案等を認識した職員等は，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　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や不正プログラムの感染が疑われる場合に当該端末等のＬＡＮケーブルを抜く又はシステム管理者に対応を依頼するなど，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（職員等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について報告しなければならない。

４　総括保護管理者は，第３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及び理事に速やかに報告しなければならない。

５　総括保護管理者は，事案の内容等に応じて，事案の内容，経緯，被害状況等について，独立行政法人国立文化財機構（以下「機構」という。）を所管する行政機関に対し，速やかに情報提供を行う。

６　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ものとする。

７　総括保護管理者は，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場合は，速やかに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ものとする。

８　前項による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，速やかに総務省（行政管理局）に情報提供を行う。

９　保護管理者は，次に掲げる組織体制を整備する。

(1)　事務取扱担当者が管理規程等に違反している事実又は兆候を把握した場合の保護管理者への報告連絡体制

(2)　特定個人情報等の漏えい，滅失又は毀損等（以下「情報漏えい等」という。）事案の発生又は兆候を把握した場合の職員等から保護管理者等への報告連絡体制
(3)　特定個人情報等を複数の部署で取り扱う場合の各部署の任務分担及び責任の明確化
(4)　特定個人情報等の情報漏えい等の事案の発生又は兆候を把握した場合の対応体制

（監査及び点検の実施）

第９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，管理規程の第３条から第７条及び本細則第３条から第８条に規定する措置の状況を含む機構における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。

２　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ものとする。

３　保有個人情報等の適切な管理のための措置については，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ものとする。

（個人番号を取扱う事務の範囲）

第１０条　機構が個人番号を取り扱う事務の範囲は以下のとおりとする。

対象区分	事務の内容
１．職員等に係る個人番号関係事務及び職員等の扶養者に係る個人番号関係事務	給与所得・退職所得の源泉徴収票作成事務
	雇用保険申請・届出事務
	健康保険・厚生年金保険届出事務
	国家公務員共済組合届出事務
	国民年金の第３号被保険者の届出事務
２．職員等以外の個人に係る個人番号関係事務	給与所得の源泉徴収票作成事務
	報酬・料金等の支払調書作成事務
	不動産の使用料等の支払調書作成事務
	不動産等の譲受けの対価の支払調書作成事務

２　前項の対象区分１．２に付随して行う事務（特定個人情報等取扱事務を含む。）

第２章　特定個人情報等の安全管理措置

第１１条　特定個人情報等の安全管理措置に関しては，第３条から第９条及び第４５条の規定によるほか，第１２条から第４４条までの規定によるものとする。

（総括保護管理者）

第１２条　総括保護管理者は，特定個人情報等に関する監査を除き，次に掲げる事項その他機構における特定個人情報等に関する全ての権限と責務を有するものとする。

(1)　本細則及び委託先の選定基準の策定並びに職員等への周知

(2)　本細則に基づき特定個人情報等の取扱いを管理する上で必要とされる規定の整備

(3)　特定個人情報等に関する安全対策の策定・実施

(4)　特定個人情報等の適正な取扱いの維持・推進等を目的とした諸施策の策定・実施

(5)　事故発生時の対応策の策定・実施

(6)　特定個人情報等の安全管理に関する教育・研修の企画

２　総括保護管理者は，監査責任者より監査報告を受け，必要に応じて特定個人情報等管理体制の改善を行う。

（保護管理者の責務）

第１３条　保護管理者は，本細則に定められた事項を理解し，遵守するとともに，事務取扱担当者にこれを理解させ，次に掲げる事項の権限と責務を有するものとする。

(1)　特定個人情報等が本細則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こと

(2)　特定個人情報等の届出申請の承認及び記録等の承認と管理を行うこと

(3)　特定個人情報ファイルを取り扱う情報システムを管理する区域（以下「管理区域」という。）及び取扱区域を設定すること

(4)　特定個人情報等の取扱区分及び権限についての設定及び変更の管理を行うこと

(5)　特定個人情報等の取扱状況を把握すること

(6)　委託先における特定個人情報等の取扱状況等を監督すること

(7)　特定個人情報等の安全管理に関する教育・研修を実施すること

(8)　特定個人情報等を削除・廃棄したことの確認をすること

(9)　その他機構における特定個人情報等の安全管理に関する事項について総括保護管理者の補佐をすること

２　前項に定めるほか，本部事務局総務企画課の保護管理者は第４１条に規定するユーザーＩＤを管理する。

（保護担当者の責務）

第１４条　保護担当者は，保護管理者を補佐し，保護管理者の行う特定個人情報等の安全管理措置の事務を担当する。

（事務取扱担当者の責務）

第１５条　事務取扱担当者は，特定個人情報等の「取得」，「保管」，「利用」，「提供」，「開示」，「訂正」，「利用停止」，「廃棄」又は委託処理等，特定個人情報等を取扱う業務に従事する際，番号法及び法並びにその他の関連法令，特定個人情報等の適正な取扱いに関するガイドライン(行政機関等・地方公共団体等編)（以下「ガイドライン」という。），本

細則及びその他の機構規定並びに保護管理者の指示した事項に従い，特定個人情報等の保護に十分な注意を払ってその業務を行うものとする。

２　事務取扱担当者は，特定個人情報等の漏えい等，番号法若しくは法又はその他の関連法令，ガイドライン，本細則又はその他の機構規定に違反している事実又は兆候を把握した場合，速やかに保護管理者に報告するものとする。

３　各部門において個人番号が記載された書類等の受領をする事務取扱担当者は，自己の手元に個人番号を転記したもの等を残してはならないものとする。

（監査責任者）

第１６条　監査責任者は，機構内の特定個人情報等を取り扱う業務において，関係法令，本細則等が遵守され，適法かつ適正に取り扱われているかについて，定期に又は随時に点検又は監査を行い，その結果を総括保護管理者に報告する。総括保護管理者は，点検又は監査の結果等を踏まえ，必要があると認めるときは，管理規程等の見直し等の措置を講ずる。

２　監査責任者は，特定個人情報等の取扱いに関する監査に必要な監査担当者を選任することができる。

（情報漏えい事故等への対応）

第１７条　総括保護管理者は，特定個人情報等の漏えい，滅失又は毀損による事故（以下「漏えい事案等」という。）が発生したことを知った場合又はその可能性が高いと判断した場合は，本細則に基づき，適切に対処するものとする。

２　総括保護管理者は，理事長及び保護管理者と連携して漏えい事案等に対応する。

（情報漏えい事故等の公表）

第１８条　総括保護管理者は，漏えい事案等が発生したと判断した場合は，その旨及び調査結果を理事長に報告し，当該漏えい事案等の対象となった情報主体に対して，事実関係の通知，謝意の表明，原因関係の説明等を速やかに行うものとする。

２　総括保護管理者は，漏えい事案等が発生した場合，主務官庁を通じ，特定個人情報保護委員会に必要な報告を速やかに行うものとする。

３　総括保護管理者は，漏えい事案等が発生したと判断した場合は，その事実を本人に通知するとともに，必要に応じて公表する。

（情報漏えい事故等の再発防止）

第１９条　総括保護管理者は，漏えい事案等が発生したと判断した場合は，情報漏えい等が発生した原因を分析し，再発防止に向けた対策を講じるものとする。

２　総括保護管理者は，他法人における漏えい事故等を踏まえ，類似事例の再発防止のために必要な措置の検討を行うものとする。

３　総括保護管理者は，漏えい事案等への対応状況の記録を（年に 1 回以上）の頻度にて分析するものとする。

（運用の確認，本細則に基づく運用状況の記録）

第２０条　事務取扱担当者は，本細則に基づく運用状況を確認するため，次に掲げる事項につき，システムログ及び利用実績を記録するものとする。

(1)　特定個人情報等の取得及び特定個人情報ファイルへの入力状況

(2)　特定個人情報ファイルの利用・出力状況の記録

(3)　書類・媒体等の持出しの記録

(4)　特定個人情報ファイルの削除・廃棄記録

(5)　削除・廃棄を委託した場合，これを証明する記録等

(6)　特定個人情報ファイルを情報システムで取り扱う場合，事務取扱担当者の情報システムの利用状況（ログイン実績，アクセスログ等）の記録

（取扱状況の確認手段）

第２１条　事務取扱担当者は，特定個人情報ファイルの取扱状況を確認するための手段として，特定個人情報管理台帳に次に掲げる事項を記録するものとする。なお，特定個人情報管理台帳には，特定個人情報等は記載しないものとする。

(1)　特定個人情報ファイルの種類，名称

(2)　責任者，取扱部署

(3)　利用目的

(4)　削除・廃棄状況

(5)　アクセス権を有する者

(6)　特定個人情報ファイルを取り扱う情報システムを管理する「管理区域」の場所

(7)　特定個人情報等を取り扱う事務を実施する「取扱区域」の場所

（特定個人情報等の適正な取得）

第２２条　機構は，特定個人情報等の取得を適法かつ公正な手段によって行うものとする。

（特定個人情報等の利用目的）

第２３条　機構が，職員等又は第三者から取得する特定個人情報等の利用目的は，第１０条に掲げた個人番号を取り扱う事務の範囲内とする。

（特定個人情報等の取得時の利用目的の通知等）

第２４条　機構は，特定個人情報等を取得した場合は，あらかじめその利用目的を公表している場合を除き，速やかに，その利用目的を情報主体に通知し，又は公表しなければならない。この場合において，「通知」の方法については，原則として書面（電子的方式，磁気的方式，その他人の知覚によっては認識することができない方式で作られた記録を電子機器等で表示する場合を含む。以下同じ。）によることとし，「公表」の方法については，機構の掲示版への書面の掲示・備付け，インターネット上のホームページ等での公表等適切な方法によるものとする。また，機構の職員等から特定個人情報等を取得する場合には，機構内 LAN における通知，利用目的を記載した書類の提示，就業規則への明記等の方法を用いる。

２　機構は，利用目的の変更を要する場合，当初の利用目的と相当の関連性を有すると合

理的に認められる範囲内で利用目的を変更して，本人への通知，公表又は明示を行うことにより，変更後の利用目的の範囲内で特定個人情報等を利用することができる。

（個人番号の提供の要求）

第２５条　機構は，第１０条に掲げる事務を処理するために必要がある場合に限り，本人に対して個人番号の提供を求めることができるものとする。

（個人番号の提供を求める時期）

第２６条　機構は，第１０条に定める事務を処理するために必要があるときに個人番号の提供を求めることとする。

２　前項にかかわらず，本人との法律関係等に基づき，個人番号関係事務の発生が予測される場合には，契約を締結した時点等の当該事務の発生が予想できた時点で個人番号の提供を求めることが可能であるものとする。

（特定個人情報等の提供の求めの制限）

第２７条　特定個人情報等の「提供」とは，法的な人格を超える特定個人情報等の移動を意味するものであり，同一法人の内部等の法的な人格を超えない特定個人情報等の移動は「提供」ではなく「利用」に該当し，個人番号の利用制限（第３０条）に従うものとする。

２　機構は，番号法第１９条各号のいずれかに該当し特定個人情報等の提供を受けることができる場合を除き，特定個人情報等の提供を求めてはならない。

（特定個人情報等の収集制限）

第２８条　機構は第１０条に定める事務の範囲を超えて，特定個人情報等を収集しないものとする。

（本人確認）

第２９条　機構は番号法第１６条に定める方法により，職員等又は第三者の個人番号の確認及び当該人の身元確認を行うものとする。また，代理人については，同条に定める方法により，当該代理人の身元確認，代理権の確認及び本人の個人番号の確認を行うものとする。

（個人番号の利用制限）

第３０条　機構は，第２３条に掲げる利用目的の範囲内でのみ利用するものとする。

２　機構は，人の生命，身体又は財産の保護のために必要がある場合を除き，本人の同意があったとしても，利用目的を超えて特定個人情報等を利用してはならないものとする。

（特定個人情報ファイルの作成の制限）

第３１条　機構が特定個人情報ファイルを作成する場合は，第１０条に定める事務を実施するために必要な範囲に限り，これらの場合を除き特定個人情報ファイルを作成しないものとする。

（特定個人情報等の正確性の確保）

第３２条　事務取扱担当者は，特定個人情報等を，第２３条に掲げる利用目的の範囲にお

いて，正確かつ最新の状態で管理するよう努めるものとする。

（保有個人情報等に関する事項の公表等）

第３３条　機構は，法第７８条に基づき，特定個人情報等に係る保有個人情報等に関する事項を本人の知り得る状態に置くものとする。

（特定個人情報等の保管制限）

第３４条　機構は，第１０条に定める事務の範囲を超えて，特定個人情報等を保管してはならない。

２　機構は，所管法令で定められた個人番号を記載する書類等の保存期間を経過するまでの間は，雇用保険資格取得届作成等の個人番号関係事務を行うために必要があると認められるため，当該書類だけでなく，届出書類を作成するシステム内においても保管することができる。

３　機構は，番号法上の本人確認の措置を実施する際に提示を受けた本人確認書類（個人番号カード，通知カード及び身元確認書類等）の写し，機構が行政機関等に提出する書類の控え及び当該書類を作成するうえで機構が受領する個人番号が記載された書類等を特定個人情報等として保管することができる。これらの書類については，法定調書の再作成を行うなど個人番号関係事務の一環として利用する必要があると認められるため，関連する所管法令で定められた個人番号を記載する書類等の保存期間を経過するまでの間保存することができる。

（特定個人情報等の提供制限）

第３５条　機構は，番号法第１９条各号に掲げる場合を除き，本人の同意の有無に関わらず，特定個人情報等を第三者（法的な人格を超える特定個人情報等の移動を意味し，同一法人の内部等の法的な人格を超えない特定個人情報等の移動は該当しないものとする。）に提供しないものとする。なお，本人の事前同意があっても特定個人情報等の第三者提供ができないことに留意するものとする。

（特定個人情報等の廃棄・削除）

第３６条　機構は第１０条に規定する事務を処理する必要がある範囲内に限り特定個人情報等を収集又は保管し続けるものとする。なお，書類等について所管法令によって一定期間保存が義務付けられているものについては，これらの書類等に記載された個人番号については，その期間保管するものとし，それらの事務を処理する必要がなくなった場合で，所管法令において定められている保存期間を経過した場合には，個人番号をできるだけ速やかに廃棄又は削除するものとする。

（特定個人情報等を取り扱う区域の管理）

第３７条　保護管理者は管理区域及び取扱区域を明確にし，それぞれの区域に対し，次に掲げる方法に従い以下の措置を講じる。

⑴　管理区域

入退室管理及び管理区域へ持ち込む機器及び電子媒体等の制限を行うものとする。

⑵　取扱区域

可能な限り壁又は間仕切り等の設置や，事務取扱担当者以外の者の往来が少ない場所への座席配置や，後ろから覗き見される可能性が低い場所への座席配置等をするなど座席配置を工夫するものとする。

（機器及び電子媒体等の盗難等の防止）

第３８条　保護管理者は管理区域及び取扱区域における特定個人情報等を取り扱う機器，電子媒体及び書類等の盗難又は紛失等を防止するために，次に掲げる措置を講じる。

⑴　特定個人情報等を取り扱う機器，電子媒体又は書類等については，施錠できるキャビネット・書庫等に保管する。

⑵　特定個人情報ファイルを取り扱う情報システムが機器のみで運用されている場合は，セキュリティワイヤー等により固定する。

（電子媒体等を持ち出す場合の漏えい等の防止）

第３９条　特定個人情報等が記録された電子媒体又は書類等の持出しは，次に掲げる場合を除き禁止する。なお，「持出し」とは，特定個人情報等を，管理区域又は取扱区域の外へ移動させることをいい，施設内での移動等も持出しに該当するものとする。

⑴　第１３条により保護管理者が監督する外部委託先に，委託事務を実施する上で必要と認められる範囲内でデータを提供する場合

⑵　行政機関等への届出書類の提出等，機構が実施する個人番号関係事務に関して番号法で定める個人番号利用事務実施者に対しデータ又は書類を提出する場合

２　前項により特定個人情報等が記録された電子媒体又は書類等の持出しを行う場合には，以下の安全策を講じるものとする。ただし，行政機関等に法定調書等をデータで提出するに当たっては，行政機関等が指定する提出方法に従うものとする。

⑴　特定個人情報等が記録された電子媒体を安全に持ち出す方法

イ　持出しデータの暗号化

ロ　持出しデータのパスワードによる保護

ハ　施錠できる搬送容器の使用

ニ　追跡可能な移送手段の利用

⑵　特定個人情報等が記載された書類等を安全に持ち出す方法

イ　封緘又は目隠しシールの貼付

（記録媒体等の廃棄・削除）

第４０条　特定個人情報等の廃棄・削除における記録媒体等の管理は次のとおりとする。

⑴　事務取扱担当者は，特定個人情報等が記録された書類等を廃棄する場合，シュレッダー等による記載内容が復元不能までの裁断，機構又は外部の焼却場での焼却・溶解等の復元不可能な手段を用いるものとする。

⑵　事務取扱担当者は，特定個人情報等が記録された機器及び電子媒体等を廃棄する場

合，専用データ削除ソフトウェアの利用又は物理的な破壊等により，復元不可能な手段を用いるものとする。

(3)　事務取扱担当者は，特定個人情報ファイル中の個人番号又は一部の特定個人情報等を削除する場合，容易に復元できない手段を用いるものとする。

(4)　特定個人情報等を取り扱う情報システムにおいては，当該関連する届出書類等の法定保存期間経過後速やかに個人番号を削除するよう情報システムを構築するものとする。

(5)　個人番号が記載された書類等については，当該関連する届出書類等の法定保存期間経過後速やかに廃棄をするものとする。

２　事務取扱担当者は，個人番号若しくは特定個人情報ファイルを削除した場合，又は電子媒体等を廃棄した場合には，削除又は廃棄した記録を保存するものとする。削除・廃棄の記録としては，特定個人情報ファイルの種類・名称，責任者・取扱部署，削除・廃棄状況を記録するものとし，個人番号自体は含めないものとする。

（アクセス制御）

第４１条　特定個人情報等へのアクセス制御は以下のとおりとする。

(1)　個人番号と紐付けてアクセスできる情報の範囲をアクセス制御により限定する。

(2)　特定個人情報ファイルを取り扱う情報システムを，アクセス制御により限定する。

(3)　ユーザーＩＤに付与するアクセス権により，特定個人情報ファイルを取り扱う情報システムを使用できる者を事務取扱担当者に限定する。

（アクセス者の識別と認証）

第４２条　特定個人情報等を取り扱う情報システムにおいては，ユーザーＩＤ，パスワード，磁気・ＩＣカード等の識別方法により，事務取扱担当者が正当な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ものとする。

（外部からの不正アクセス等の防止）

第４３条　次に掲げる方法により，情報システムを外部からの不正アクセス及び不正ソフトウェアから保護するものとする。

(1) 情報システムと外部ネットワークとの接続箇所に，ファイアウォール等を設置し，不正アクセスを遮断する方法

(2) 情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入する方法

(3) 導入したセキュリティ対策ソフトウェア等により，入出力データにおける不正ソフトウェアの有無を確認する方法。

(4) 機器やソフトウェア等に標準装備されている自動更新機能等の活用により，ソフトウェア等を最新状態とする方法

(5) ログ等の分析を定期的に行い，不正アクセス等を検知する方法

（情報漏えい等の防止）

第４４条　特定個人情報等をインターネット等により外部に送信する場合，次に掲げる方法により通信経路における情報漏えい等及び情報システムに保存されている特定個人情報等の情報漏えい等を防止するものとする。

(1)　通信経路における情報漏えい等の防止策

通信経路の暗号化

(2)　情報システムに保存されている特定個人情報等の情報漏えい等の防止策

データの暗号化又はパスワードによる保護

（行政機関との連携）

第４５条　機構は，「個人情報の保護に関する基本方針」（平成 16 年４月２日閣議決定）４を踏まえ，機構を所管する行政機関と緊密に連携して，その保有する個人情報の適切な管理を行う。

附　則

この細則は，平成１９年４月１日から施行する。

附　則

この細則は，平成２７年１１月３０日に改正し，同日から施行する。

附　則

この細則は，平成３０年１０月２２日に改正し，同日から施行する。

附　則

この規程は，令和４年１１月１０日に改正，同日から施行し，令和４年４月１日から適用する。