

独立行政法人国立公文書館の保有する法人文書に係る個人情報管理規程

平成17年3月25日規程第5号
改正 平成21年7月2日規程第9号
改正 平成23年4月1日規程第14号
改正 平成24年11月22日規程第12号
改正 平成28年2月4日規程第1号
改正 令和元年10月1日規程第11号

第1章 総則

(目的)

第1条 この規程は、独立行政法人国立公文書館（以下「館」という。）の保有する個人情報及び個人番号の適切な管理に関して必要な事項を定めることを目的とする。

(用語の定義)

第2条 この規程における用語の定義は、「独立行政法人等の保有する個人情報の保護に関する法律」（平成15年法律第59号。以下「法」という。）第2条及び「行政手続き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2条の定めるところによる。

第2章 管理体制

(総括個人情報管理者)

第3条 館に、総括個人情報管理者1人を置き、次長をもって充てる。

2 総括個人情報管理者は、館におけ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。）の管理に関する事務を総括する任に当たる。

3 総括個人情報管理者は、その指名する職員に、館における保有個人情報等の適切な管理のための企画調整に関する事務を行わせることができる。

(個人情報管理者)

第4条 各課等に個人情報管理者1人を置き、各課等の長（アジア歴史センター（以下「センター」という。）にあつてはセンター次長とする。以下、同じ。）をもって充てる。

2 個人情報管理者は、当該課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。保有個人情報等を情報システムで取り扱う場合、個人情報管理者は、当該情報システムの管理者と連携して、その任に当たる。

(個人情報取扱主任)

第5条 各課等に、個人情報取扱主任を置き、当該課等の個人情報管理者が指名する職員をもって充てる。

2 個人情報取扱主任は、個人情報管理者を補佐し、当該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。

(特定個人情報等取扱担当者)

第6条 個人情報管理者は、当該課等において、個人番号及び特定個人情報(以下「特定個人情報等」という。)を取り扱う場合には、特定個人情報等を取り扱う職員(以下「特定個人情報等取扱担当者」という。)を指名し、当該特定個人情報等取扱担当者が個人番号を取り扱う事務の範囲及び取り扱う特定個人情報等の範囲を指定する。

(監査責任者)

第7条 館に、監査責任者1人を置き、総務課長をもって充てる。

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。

(保有個人情報の適切な管理のための会議)

第8条 総括個人情報管理者は、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会議を開催することができる。

第3章 教育研修

第9条 総括個人情報管理者は、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を目的として必要な教育研修を実施する。

2 総括個人情報管理者は、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実施する。

3 総括個人情報管理者は、個人情報保護管理者及び個人情報取扱主任に対し、各課等の現場における個人情報等の適切な管理のための教育研修を定期的に実施する。

4 個人情報管理者は、当該課等の職員に対し、保有個人情報等の適切な管理のために、総括個人情報管理者の実施する教育研修への参加の機会を付与す

る。

第4章 職員の責務

第10条 職員は、法及び番号法の趣旨に則り、関連する法令及びこの規程並びに総括個人情報管理者、個人情報管理者及び個人情報取扱主任の指示に従い、保有個人情報等を取り扱わなければならない。

第5章 保有個人情報の取扱い

(アクセス制限)

第11条 個人情報管理者は、保有個人情報等の秘匿性等その内容に応じて、当該保有個人情報にアクセスする（紙等に記録されている保有個人情報に接する行為を含む。以下同じ。）権限を有する職員の範囲とその権限の内容をそれぞれの業務を行うために必要最小限の範囲に限らなければならない。

2 前項の場合において、職員の範囲と権限の内容を定めるときは、個人識別の容易性（匿名化の限度等）、要配慮個人情報の有無、漏えい等が発生した場合に生じ得る被害の性質又は程度などを考慮する。

3 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。

4 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、個人情報管理者は、次に掲げる行為については当該行為を行うことができる場合を限定し、職員は、個人情報管理者の指示に従い行わなければならない。

一 保有個人情報等の複製

二 保有個人情報等の送信

三 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ち出し

四 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

(誤りの訂正等)

第13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、個人情報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14条 職員は、個人情報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、施錠等を行わなければならない。

(廃棄等)

第15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、個人情報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わなければならない。

（個人番号の利用の制限）

第16条 職員は、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、個人番号を利用してはならない。

（個人番号の提供の求めの制限）

第17条 職員は、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、個人番号の提供を求めてはならない。

（特定個人情報等の収集・保管の制限）

第18条 職員は、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等を収集又は保管してはならない。

（特定個人情報ファイルの作成の制限）

第19条 職員は、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。

（保有個人情報等の取扱状況の記録）

第20条 個人情報管理者は、保有個人情報等の秘匿性等その内容及び必要に応じて、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しなければならない。

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21条 個人情報管理者は、保有個人情報等（情報システムで取り扱うものに限る。以下第27条を除き、この章において同じ。）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。

2 個人情報管理者が前項の措置を講じる場合には、パスワード等の管理に関する規程を定め、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。パスワード等の管理に関する規程は、必要に応じて見直しを行う。

（アクセス記録）

第22条 個人情報管理者は、保有個人情報等の秘匿性等その内容及び必要に

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なければならない。

2 個人情報管理者は、必要に応じてアクセス記録を分析するものとする。

3 個人情報管理者は、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じなければならない。

（不正アクセス行為の防止）

第23条 個人情報管理者は、保有個人情報等を取り扱う情報システムへの不正アクセス行為（不正アクセス行為の禁止等に関する法律（平成11年法律第128号）第2条第4項に規定する不正アクセス行為をいう。）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の防止）

第24条 個人情報管理者は、不正プログラムによる保有個人情報等の漏えい、滅失又はき損等の防止のため、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25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の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。個人情報管理者は、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 個人情報管理者は、保有個人情報等の秘匿性等その内容に応じて、その暗号化のために必要な措置を講じなければならない。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適切に暗号化を行う。

（入力情報の照合等）

第27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28条 個人情報管理者は、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じなければならない。

（情報システム設計書等の管理）

第29条 個人情報管理者は、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に、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。

(端末の限定)

第30条 個人情報管理者は、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しなければならない。

(端末の盗難防止等)

第31条 個人情報管理者は、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じなければならない。

2 職員は、個人情報管理者が必要が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32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にしなければならない。

第7章 コンピュータ室等の安全管理

(入退室の管理)

第33条 個人情報管理者は、保有個人情報等を取り扱う基幹的なコンピュータ等の機器を設置する室等（以下「コンピュータ室等」という。）に入室する権限を有する者を定めるとともに、必要に応じ、用件の確認、入退室の記録、部外者についての識別化、部外者が入室する場合の職員の立会い等の措置を講ずる。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、同様の措置を講じる。

2 個人情報管理者は、必要があると認めるときは、コンピュータ室等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じる。

3 個人情報管理者は、コンピュータ室等及び保管施設の入退室の管理について、必要があると認めるときは、入室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を整備（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じる。

(コンピュータ室等の管理)

第34条 個人情報管理者は、外部からの不正な侵入に備え、コンピュータ室等に施錠装置、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 個人情報管理者は、災害等に備え、コンピュータ室等に、耐震、防火、防煙、防水等の必要な措置を講ずるとともに、コンピュータ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 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35条 個人情報管理者は、法第9条第2項第3号及び第4号の規定に基づ

き行政機関及び独立行政法人等以外の者に保有個人情報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、利用する記録範囲及び記録項目、利用形態等について書面を取り交わさなければならない。

- 2 個人情報管理者は、法第9条第2項第3号及び第4号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報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、提供前又は随時に実地の調査等を行い措置状況を確認し、その結果を記録するとともに、改善要求等の措置を講じることができる。
- 3 個人情報管理者は、法第9条第2項第3号の規定に基づき行政機関又は独立行政法人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、前二項に規定する措置を講じることができる。
- 4 職員は、番号法で限定的に明記された場合を除き、特定個人情報等の提供をしてはならない。

(保有個人情報の取扱いに係る業務の委託等)

第36条 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、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にしなければならない。また、契約書に、次に掲げる事項を明記する(独立行政法人国立公文書館会計規程(平成13年4月2日規程第6号)第37条の規定により契約書の作成を省略する場合にあっては、次に掲げる事項を遵守する旨を委託先に誓約させる。次条において同じ。)とともに、委託先における責任者等の管理体制、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しなければならない。

一 個人情報に関する秘密保持等の義務

二 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。以下同じ。)の制限又は条件に関する事項

三 個人情報の複製等の制限に関する事項

四 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

五 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

六 違反した場合における契約解除の措置その他必要な事項

- 2 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、原則として実地による検査等により確認しなければならない。
- 3 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、委託先に第一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しなければならない。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。

- 4 保有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しなければならない。
- 5 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、保有個人情報等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じなければならない。

(特定個人情報等の取扱いに係る業務の委託等)

第37条 特定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、委託先において、番号法に基づき個人番号利用事務等を行う行政機関が果たすべき安全管理措置と同等の措置が講じられるか否かについて、あらかじめ書面で確認しなければならない。また、委託契約の締結については、契約書に、次に掲げる事項を明記しなければならない。

一 特定個人情報等に関する秘密保持、目的外利用の禁止等の義務

二 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。以下同じ。）の制限又は事前承認等再委託に係る条件に関する事項

三 特定個人情報等の複製等の制限に関する事項

四 特定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

五 委託終了時における特定個人情報等の消去及び媒体の返却に関する事項

六 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

七 事務所内からの特定個人情報等の持ち出しの禁止に関する事項

八 特定個人情報等の漏えい事案等が発生した場合の委託先の責任に関する事項

九 特定個人情報等を取り扱う従業者の明確化及び当該従業者に対する監督及び教育に関する事項

十 契約内容の遵守状況の報告に関する事項

十一 委託先における実地検査等に関する事項

- 2 特定個人情報等の取扱いに係る業務を外部に委託する際には、委託を受けた者において、番号法に基づき個人番号利用事務等を行う行政機関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。また、委託する業務に係る特定個人情報等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地体制や特定個人情報等の管理の状況について、少なくとも年1回以上、原則として実地による検査等により確認しなければならない。

- 3 委託先において、特定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、委託をする当該業務において取り扱う特定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託の諾否を判断する。
- 4 特定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、必要に応じて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しなければならない。

第9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38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特定個人情報等取扱担当者がこの規程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り得る事案が発生した場合に、その事実を知った職員は、直ちに当該保有個人情報を管理する個人情報管理者に報告しなければならない。

- 2 個人情報管理者は、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に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 個人情報管理者は、事案の発生した経緯、被害状況等を調査し、総括個人情報管理者に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、直ちに総括個人情報管理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 総括個人情報管理者は、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、被害状況等を館長に速やかに報告しなければならない。
- 5 統括個人情報管理者は、事案の内容、経緯、被害状況等について、内閣府に対し速やかに情報提供を行う。
- 6 個人情報管理者は、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じなければならない。

(公表等)

第39条 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、当該事案に係る本人への対応等の措置を講じる。なお、公表を行う場合は、当該事

案の内容、経緯、被害状況について、速やかに総務省行政管理局に情報提供を行う。

第10章 監査及び点検の実施

(監査)

第40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、第2章から第9章に規定する措置の状況を含む館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監査を行い、その結果を総括個人情報管理者に報告する。その際監査責任者は、その指名する職員に、監査に関する事務を行わせることができる。

(点検)

第41条 個人情報管理者は、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点検を行い、必要があると認めるときは、その結果を総括個人情報管理者に報告する。

(評価及び見直し)

第42条 保有個人情報の適切な管理のための措置については、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行う。

第11章

(行政機関との連携)

第43条 館は、「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、内閣府と緊密に連携して、その保有する個人情報の適切な管理を行う。

第12章 その他

(細則)

第44条 この規程に定めるもののほか、この規程の実施のための手続その他について必要な事項は、別に定める。

附 則

この規程は、平成17年4月1日から施行する。

附 則（平成21年7月2日規程第9号）

この規程は、平成21年7月2日から施行する。

附 則（平成23年4月1日規程第14号）
この規程は、平成23年4月1日から施行する。

附 則（平成24年11月22日規程第12号）
この規程は、平成24年11月22日から施行する。

附 則（平成28年2月4日規程第1号）
この規程は、平成28年2月4日から施行する。

附 則（令和元年10月1日規程第11号）
この規程は、令和元年10月1日から施行する。