

保有個人情報管理規程

規程第27号

平成29年5月31日

一部改正 令和元年7月12日規程第73号

最終改正 令和4年3月24日規程第121号

目次

- 第1章 総則（第1条・第2条）
- 第2章 管理体制（第3条－第10条）
- 第3章 教育研修（第11条）
- 第4章 役職員の責務（第12条）
- 第5章 保有個人情報の取扱い（第13条－第23条）
- 第6章 保有個人情報を取り扱う情報システムにおける安全の確保等（第24条－第38条）
- 第7章 情報システム室等の安全管理（第39条－第42条）
- 第8章 保有個人情報の提供及び業務の委託等（第43条－第45条）
- 第9章 安全確保上の問題への対応（第46条・第47条）
- 第10章 監査及び点検の実施（第48条－第50条）
- 第11章 主務省との連携（第51条）
- 第12章 雑則（第52条）

附則

第1章 総則

（目的）

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「個人情報保護法」という。）第66条第1項の規定に基づく「行政機関等の保有する個人情報の適切な管理のための措置に関する指針」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。）に基づき、外国人技能実習機構（以下「機構」という。）の保有する個人情報の適切な管理のために必要な措置について定め、その保有個人情報の漏えい、滅失、毀損等を防止し、適正な管理を図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、個人情報保護法第2条及び第60条並びに番号法第2条の定めるところによるほか、次の各号に掲げるとおりとする。

- (1) この規程において「本部」とは、機構本部をいい、「地方事務所等」とは、組織規程(規程第2号)第28条に規定する地方事務所及び第29条に規定する支所をいう。
- (2) 「部等」とは、組織規程第7条に規定する監査室及び第8条に規定する部をいう。
- (3) この規程において「課」とは、本部に置かれる課をいう。
- (4) 「情報システム」とは、ハードウェア、ソフトウェア、ネットワーク及び記録媒体で構成されるものであって、これら全体で事務処理を行うものをいう。

第2章 管理体制

(総括個人情報保護管理者)

第3条 機構に、総括個人情報保護管理者(以下「総括保護管理者」という。)を一人置くものとし、総務担当理事をもって充てる。

- 2 総括保護管理者は、機構の役員及び職員(契約職員(無期雇用契約職員を含む。)、パートタイム職員(無期雇用パートタイム職員を含む。))及び派遣職員を含む。以下「役職員」という。)に対する保有個人情報の管理に関する事務の指導監督等を行うとともに、機構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。

(部等個人情報保護管理者)

第4条 部等及び地方事務所等に、部等個人情報保護管理者(以下「部等保護管理者」という。)を各一人置くものとし、部等に置く部等保護管理者は部等の長、地方事務所等に置く部等保護管理者は地方事務所等の長をもって充てる。

- 2 部等保護管理者は、総括保護管理者の指示に従い、当該部等又は地方事務所等における保有個人情報の管理に関する事務の運営につき監督を行う。

(個人情報保護管理者)

第5条 監査室、課及び地方事務所等に、個人情報保護管理者(以下「保護管理者」という。)を各一人置くものとし、別表に定めるとおりとする。

- 2 保護管理者は、部等保護管理者の指示に従い、当該監査室、課又は地方事務所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。
- 3 保有個人情報を情報システムで取り扱う場合、保護管理者は、当該情報システムの管理者と連携して、その任に当たるものとする。

(個人情報保護担当者)

第6条 監査室、課及び地方事務所等に、個人情報保護担当者（以下「保護担当者」という。）を各一人又は複数人置くものとし、保護担当者は、保護管理者が指定する。

- 2 保護担当者は、保護管理者を補佐し、監査室、課又は地方事務所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。

(事務取扱担当者)

第7条 保護管理者は、特定個人情報を取り扱う職員（以下「事務取扱担当者」という。）及びその役割を指定する。

- 2 保護管理者は、各事務取扱担当者が取り扱う特定個人情報の範囲を指定する。

第8条 保護管理者は、次に掲げる組織体制を整備する。

- (1) 事務取扱担当者がこの規則等に違反している事実又は兆候を把握した場合の責任者への報告連絡体制
- (2) 特定個人情報の情報漏えい等事案の発生又は兆候を把握した場合の職員から責任者等への報告連絡体制
- (3) 特定個人情報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

(個人情報保護監査責任者)

第9条 機構に、個人情報保護監査責任者（以下「監査責任者」という。）を一人置くものとし、監査室長をもって充てる。

- 2 監査責任者は、機構における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。

(保有個人情報の適切な管理のための委員会)

第10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、関係役職員を構成員とする委員会を設け、随時に開催することができる。

第3章 教育研修

(教育研修)

- 第11条 総括保護管理者は、保有個人情報の取扱いに従事する役職員に対し、保有個人情報の取扱いについて理解を深め、個人番号その他の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、各組織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実施するものとする。
- 4 保護管理者は、当該組織の職員に対し、保有個人情報の適切な管理のために、総括保護管理者等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。
- 5 前3項の措置を講ずる場合には、保有個人情報の取扱いに従事する派遣労働者についても、職員と同様の措置を講ずるものとする。

第4章 役職員の責務

(役職員の責務)

- 第12条 役職員は、法の趣旨にのっとり、関連する法令及びこの規程の定め並びに総括保護管理者、部等保護管理者、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13条 保護管理者は、保有個人情報の秘匿性、個人識別の容易性、要配慮個人情報の有無、情報漏えい等が発生した場合に生じ得る被害の性質及び程度その他の内容（以下「秘匿性等その内容」という。）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及び権限の内容を、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ない。

(複製等の制限)

第14条 保護管理者は、保有個人情報の複製又は送信、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出等の業務について、当該保有個人情報の秘匿性等その内容に応じて、当該業務を行うことができる場合を限定するものとする。

- 2 職員は、前項の業務を行うときは、保護管理者の指示に従い、当該保有個人情報の秘匿性等その内容に応じて、必要最小限の範囲においてこれらを行うとともに、情報漏えい等が行われないよう取扱いに注意するものとする。

(誤りの訂正等)

第15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、訂正等を行うものとする。

(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、必要に応じ、耐火金庫等への保管、施錠等を行うものとする。

(誤送付等の防止)

第17条 職員は、保有個人情報を含む電磁的記録又は媒体(注)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・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。

(注) 文書の内容だけでなく、付加情報(PDFファイルの「しおり機能表示」やプロパティ情報等)に個人情報が含まれている場合があることに注意する。

(廃棄等)

第18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。

特に、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（二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19条 保護管理者は、必要に応じて保有個人情報の秘匿性等その内容に応じた台帳等を整備して、当該保有個人情報の利用、保管等の取扱状況を記録するものとする。

2 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、当該特定個人情報の利用及び保管等の取扱状況について記録するものとする。

（外的環境の把握）

第20条 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。

（※）近年、民間事業者が提供するクラウドサービスを利用する場合があります。得るところであり、こうした場合においてはクラウドサービス提供事業者が所在する外国及び個人データが保存されるサーバが所在する外国が該当する。

（個人番号の利用の制限）

第21条 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ものとする。

（特定個人情報の提供の求めの制限）

第22条 事務取扱担当者は、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、個人番号の提供を求めてはならない。

（特定個人情報ファイルの作成の制限）

第23条 事務取扱担当者は、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。

（特定個人情報の収集・保管の制限）

第24条 事務取扱担当者は、番号法第19条各号のいずれかに該当する場合を除き、他人の特定個人情報を収集又は保管してはならない。

(取扱区域)

第25条 保護管理者は、特定個人情報を取り扱う事務を実施する区域を明確にし、物理的な安全監理措置を講ずるものとする。

第6章 保有個人情報を取り扱う情報システムにおける安全の確保等

(アクセス制御)

第26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34条を除く。)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(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。
- 3 職員は、自己の利用する保有個人情報に関して認証機能が設定されている場合、その認証機能の適切な運用を行うものとする。

(アクセス記録)

第27条 保護管理者は、保有個人情報(特定個人情報を除く。)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ものとする。

- 2 保護管理者は、特定個人情報へのアクセス状況を記録し、その記録を一定の期間保存し、定期に又は随時に分析するために必要な措置を講ずるものとする。
- 3 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。

(アクセス状況の監視)

第28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、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情報システムからダウンロード

ードされた場合に警告表示がなされる機能の設定、当該機能の定期的確認等の必要な措置を講ずるものとする。

(管理者権限の設定)

第29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ものとする。

(外部からの不正アクセスの防止)

第30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ネットワーク経路制御等の必要な措置を講ずるものとする。

(不正プログラムによる漏えい等の防止)

第31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、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。

(情報システムにおける保有個人情報の処理)

第32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。

2 前項の場合において、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33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、その暗号化のために必要な措置を講ずるものとする。

2 職員は、前項の規定を踏まえ、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（適切なパスワードの選択、パスワードの漏えい防止の措置等を含む。）を行うものとする。

(入力情報の照合等)

第34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ものとする。

(バックアップ)

第35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ものとする。

(情報システム設計書等の管理)

第36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、仕様書、ネットワーク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ずるものとする。

(端末の限定)

第37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ものとする。

(端末の盗難防止等)

第38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ものとする。

2 職員は、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。ただし、保護管理者の指示に従い、業務の必要最小限の範囲において行うときはこの限りではない。

3 職員は、前項の規定に基づき、端末を外部へ持ち出したときは、紛失による情報漏えい等が行われないよう取扱いに注意するものとする。

(第三者の閲覧防止)

第39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に、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。

(記録機能を有する機器・媒体の接続制限)

第40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、滅失又は毀損の防止のため、スマートフォン、USBメモリ等の記録機能を有する機器・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ものとする。

第7章 情報システム室等の安全管理

(入退管理)

第41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。

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ものとする。

3 保護管理者は、情報システム室等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を整備（その定期又は随時の見直しを含む。）、パスワード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。

(情報システム室等の管理)

第42条 保護管理者は、外部からの不正な侵入に備え、情報システム室等への施錠装置、警報装置、監視設備等の設置等の措置を講ずるものとする。

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ものとする。

(特定個人情報等の安全管理)

第43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。）を取り扱う事務について、次の措置を講じるものとする。

- (1) 特定個人情報等を取り扱う事務を実施する区域の明確化
- (2) 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の明確化
- (3) 前項の区域における入退管理及び持ち込む機器等の制限

(執務室等に設置する場合の特例)

第44条 保護管理者は、情報システム室等について、専用の部屋を確保するのが困難である等の理由により執務室内にサーバ等を設置する場合において、必要があると認めるときは、第41条及び第42条に規定する措置に準じて、

所要の措置を講ずるものとする。

第8章 保有個人情報の提供及び業務の委託等

(保有個人情報の提供)

第45条 保護管理者は、個人情報保護法第69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（特定個人情報を除く。第2項及び第3項において同じ。）を提供する場合には、第70条の規定に基づき、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、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すものとする。

2 保護管理者は、個人情報保護法第69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、保有個人情報の提供を受ける者に対し、安全確保の措置を要求する。また、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ものとする。

3 保護管理者は、個人情報保護法第69条第2項第3号の規定に基づき行政機関及び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2項に規定する措置を講ずるものとする。

(特定個人情報の提供)

第46条 保護管理者は、番号法で限定的に明記された場合を除き、特定個人情報を提供してはならない。

(業務の委託等)

第47条 保護管理者は、保有個人情報の取扱いに係る業務を委託（注1）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、必要な措置（注2）を講ずるものとする。また、契約書に、次の各号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3号に規定する子会社をいう。以下この号において同じ。）である場合を含む。以下この号、第5項及び第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。なお、当該事項のうち再委託に際し

て再委託先に求めるものについては、再委託先が委託先の子会社である場合も、同様に求めるべきこととしなければならない。

- (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) 前各号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) その他必要な事項

(注1)「委託」とは、契約の形態・種類を問わず、機構が他の者に個人情報の取扱いを行わせることをいう。具体的には、個人情報の入力(本人からの取得を含む。)、編集、分析、出力等の処理を行うことを委託すること等が想定されるが、これらに限られない。

(注2)例えば、第49条(サイバーセキュリティの確保)に記載したサイバーセキュリティに関する対策の基準等を参考に、委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準や委託先の選定基準を整備すること等が挙げられる。

- 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、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 保護管理者は、個人番号利用事務等の全部又は一部を委託する場合には、委託先において、番号法に基づき機構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、あらかじめ確認するものとする。また、契約書に前項に掲げる事項に加え、次に掲げる事項を明記するものとする。
 - (1) 情報漏えい等事案等が発生した場合の委託先の責任に関する事項
 - (2) 事業所内からの特定個人情報の持出しの禁止に関する事項
 - (3) 特定個人情報を取扱う従業者の明確化及び従業者に対する監督・教育に関する事項
 - (4) 契約内容の遵守状況についての報告の求めに関する事項
 - (5) 必要があると認めるときに実地調査を行うことができる旨
- 4 保護管理者は、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、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並びに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ものとする。

- 5 保護管理者は、個人番号利用事務等の全部又は一部の委託をする際には、委託先において、機構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うものとする。
- 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第3項の措置を実施するものとする。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 保護管理者は、個人番号利用事務等の全部又は一部の委託先が再委託をする際には、委託をする個人番号利用事務等において取り扱う特定個人情報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ものとする。
- 8 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、労働者派遣契約を担当する職員は、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とともに、労働者派遣契約が、個人情報等の適切な取扱いを行うことに配慮されたものとしなければならない。
- 9 保護管理者は、保有個人情報を提供し、又は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、情報漏えい等による被害発生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等を考慮し、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ものとする。

第48条 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 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49条 個人情報を取扱い、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、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50条 保有個人情報の情報漏えい等の事案の発生又は兆候等を把握した場合及び事務取扱担当者が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等安全確保の上で問題となる事案又はこの問題となる事案の発生のおそれがあると認識した場合に、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しなければならない。この場合において、職員は、時間を要する事実確認を行う前にまず保護管理者に報告するものとする。

- 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、部等保護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、直ちに部等保護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 部等保護管理者は、前項の規定に基づく報告を受けた場合には、当該事案の内容、経緯、被害状況等を総括保護管理者に報告しなければならない。
- 5 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しなければならない。
- 6 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、主務省の担当部署に対し、速やかに情報提供を行うものとする。
- 7 部等保護管理者及び保護管理者は、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。

(個人情報保護法に基づく報告及び通知)

第51条 漏えい等が生じた場合であって個人情報保護法第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には、前条第1項から第7項までと並行して、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52条 個人情報保護法第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、当該事案に係る保有個人情報の本人への連絡等の措置を講ずる。

国民の不安を招きかねない事案（例えば、個人情報保護に係る内部規程に対する違反があったとき、委託先において個人情報の適切な管理に関する契約条項等に対する違反があったとき等、公表を行う必要のある漏えい等が発生したとき）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へ情報提供を行うことについて検討する。

第11章 監査及び点検の実施

(監査)

第53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9章までに規定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、定期的に及び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するものとする。

2 監査責任者は、前項の監査を行うに当たっては、部等の長及び地方事務所等の長に対し、保有個人情報の管理の状況について報告を求めることができる。

(点検)

第54条 保護管理者は、自ら管理責任を有す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、定期的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、その結果を部等保護管理者に報告する。また、部等保護管理者は、点検結果について、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55条 総括保護管理者、部等保護管理者及び保護管理者は、保有個人情報の適切な管理のため、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記録媒体、処理経路、保管方法等の評価し、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12章 主務省との連携

(主務省との連携)

第56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、主務省の担当部署と緊密に連携して、その保有する個人情報の適切な管理を行うものとする。

第13章 雑則

(細目)

第57条 この規程の部等における運用に関する細目は、総務担当理事が定めることができる。

2 この規程の地方事務所等における運用に関する細目は、当該地方事務所等の長が定めることができる。

附 則

この規程は、平成29年5月31日から施行する。

附 則

この規程は、令和元年7月12日から施行する。

附 則 (令和4年3月24日規程第121号)

この規程は、令和4年4月1日から施行する。

別表 (第5条関係)

管理の範囲		個人情報保護管理者	
部等	監査室	監査室長が指定する監査室の職員	
	総務部	総務課	総務課長
		人事課	人事課長
		会計課	会計課長
		情報システム課	情報システム課長
		企画・広報課	企画・広報課長
	国際部	国際課	国際第一課長
	指導援助部	指導課	指導課長
		援助課	援助課長
	技能実習部	認定課	認定課長
		審査課	審査課長

地方事務所等	札幌地方事務所	札幌地方事務所総務課長
	仙台地方事務所	仙台地方事務所総務課長
	東京地方事務所	東京地方事務所総務課長
	名古屋地方事務所	名古屋地方事務所総務課長
	大阪地方事務所	大阪地方事務所総務課長
	広島地方事務所	広島地方事務所総務課長
	高松地方事務所	高松地方事務所総務課長
	福岡地方事務所	福岡地方事務所総務課長
	水戸支所	水戸支所総務課長
	長野支所	長野支所総務課長
	富山支所	富山支所総務課長
	松山支所	松山支所総務課長
	熊本支所	熊本支所総務課長