

独立行政法人空港周辺整備機構の保有する個人情報の管理に関する規程

平成17年3月30日規程第8号
改正 平成19年10月1日規程第5号
平成22年3月24日規程第3号
平成22年3月24日規程第7号
平成23年3月24日規程第3号
平成24年3月26日規程第1号
平成24年3月26日規程第5号
最終改正 平成28年3月24日規程第17号

目次

- 第1章 総則（第1条－第4条）
- 第2章 管理体制（第5条－第8条）
- 第3章 教育研修（第9条）
- 第4章 機構における個人情報の取扱い（第10条－第15条）
- 第5章 情報システムにおける安全性の確保等（第16条－第25条の2）
- 第6章 情報システム室等の安全管理（第26条）
- 第7章 保有個人情報の提供及び業務の委託等（第27条・第28条）
- 第8章 安全確保上の問題への対応（第29条・第30条）
- 第9章 監査及び点検の実施（第31条－第33条）
- 第10章 行政との連携（第34条）
- 附則

第1章 総則

（目的）

第1条 この規程は、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。）及び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施行令（平成15年政令第549号）その他関係法令に定めるもののほか、独立行政法人空港周辺整備機構（以下「機構」という。）の保有する個人情報の取扱いに関して必要な事項について定めることにより、事務及び事業の適正な運営を図るとともに、個人の権利利益を保護することを目的とする。

（適用範囲）

第2条 この規程の適用を受ける者は、業務上機構の保有する個人情報を取り扱う役員及び職員（独立行政法人空港周辺整備機構就業規則（平成15年規程第5号）第2条に規定する職員のほか、招聘職員、嘱託職員、非常勤職員及び派遣労働者を含む。以下同じ。）とする。

（定義）

第3条 この規程において使用する「個人情報」、「保有個人情報」、「個人情報ファイル」及び「個人情報ファイル簿」の各用語の意義は、それぞれ法第2条第2項、第3項、第4項、法第11条第1項に定めるところによる。

（役職員の責務）

第4条 役員及び職員（以下「役職員」という。）は、法の趣旨に則り、関連する法令及び本規程の定めに従い、保有個人情報を取り扱わなければならない。

第2章 管理体制

(総括保護管理者)

第5条 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ため総括保護管理者を置くこととし、理事をもって充てる。

(保護管理者)

第6条 各課における保有個人情報を適切に管理するため保護管理者を置くこととし、課長をもって充てる。

2 保護管理者は、各課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。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(注)。

(注) 例えば、第5章、第6章、第29条第3項、第32条、第33条その他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、情報システムの管理者と連携して、それぞれの措置を講ずる。

3 保有個人情報の管理上の措置として、役員及び審議役については総務課所属として位置付ける。

(保護担当者)

第7条 保有個人情報を取り扱う各課に、保護管理者が指定する保護担当者を一人置く。

2 保護担当者は、保護管理者を補佐し、各課における保有個人情報の管理に関する事務を担当する。

(監査責任者)

第8条 保有個人情報の管理の状況についての監査を実施するため、監査責任者を置くこととし、審議役をもって充てる。

第3章 教育研修

第9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、個人情報の保護に関する意識の高揚を図るための教育研修等を必要に応じて行う。

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措置を講ずる。

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、当該課の職員に対し、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。

第4章 機構における個人情報の取扱い

(アクセス制限)

第10条 保護管理者は、保有個人情報の秘匿性等の程度及びその利用目的を考慮した上、当該保有個人情報にアクセスする権限を有する職員とその権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限定しなければならない。

2 アクセス権限を有しない役職員は、保有個人情報にアクセスしてはならない。

3 役職員は、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11条 役職員が 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、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、職員は、保護管理者の指示に従い行う。

- (1) 保有個人情報の複製
- (2) 保有個人情報の送信
- (3) 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し
- (4) その他保有個人情報の適切な管理に支障を及ぼすおそれのある行為

2 前項第1号、2号及び3号に定める行為のうち、通常業務の中で必要となる事務処理の過程で行われるものであって、個人情報の漏洩に繋がる、又は個人の権利利益を損なう等の不適切なものではないことが明らかな行為については、同項の適用を受けないものとする。

(誤りの訂正等)

第12条 役職員は、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。

(個人情報ファイルの管理)

第13条 役職員は、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個人情報ファイル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。

(廃棄等)

第14条 役職員は、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。

(保有個人情報の取扱状況の記録)

第15条 保護管理者は、個人情報ファイルのうち、秘匿性が特に高く取扱いに注意を要するものについては、個人情報管理台帳を整備した上、当該個人情報ファイルの利用及び保管等の状況について記録する。

第5章 情報システムにおける安全性の確保等

(システム管理)

第16条 理事長は、独立行政法人空港周辺整備機構ネットワークシステム（以下「機構ネットワークシステム」という。）を適正に管理するために機構ネットワークシステム管理者を置く。

2 機構ネットワークシステムの管理運用については、別に定める。

3 機構ネットワークシステム以外の保有個人情報を有する情報システムの管理は、当該システムを有する課の長がこれを行なう。

(アクセス制御)

第17条 機構ネットワークシステム管理者及び保有個人情報を有する情報システムを管理する課長（以下「システム管理者」という。）は、保有個人情報（情報システムで取り扱うものに限る。以下本章において同じ。）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カード等をいう。以下同じ。）を使用して権限の有無を識別する機能を設定する等アクセス制御のために必要な措置を講ずる。

(注) アクセス制御の措置内容は、第10条により設定した必要最小限のアクセス権限

を具体化するものである必要がある。

(アクセス記録)

第18条 システム管理者は、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。）を一定の期間保存するとともに、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。

(アクセス状況の監視)

第18条の2 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。

(管理者権限の設定)

第18条の3 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。

(外部からの不正アクセスの防止)

第19条 システム管理者は、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経路制御等の必要な措置を講ずる。

(不正プログラムによる漏えい等の防止)

第20条 システム管理者は、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。

(情報システムにおける保有個人情報の処理)

第20条の2 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。

(暗号化)

第20条の3 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、暗号化のために必要な措置を講ずる。職員（注）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。

（注）職員が行う暗号化には、適切なパスワードの選択、その漏えい防止の措置等が含まれる。

(記録機能を有する機器・媒体の接続制限)

第20条の4 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。

(バックアップ)

第21条 システム管理者は、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。

(情報システム設計書等の管理)

第22条 システム管理者は、保有個人情報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ずる。

(端末の限定)

第23条 システム管理者は、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。

(端末の盗難防止等)

第24条 システム管理者は、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。

2 役職員は、保護管理者が必要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25条 役職員は、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、端末の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。

(入力情報の照合等)

第25条の2 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。

第6章 情報システム室等の安全管理

(情報システム室等の安全管理)

第26条 総括保護管理者は、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（以下「情報システム室」という。）について、入退室管理等の安全管理措置を講ずる。

2 前項に定める入退室管理等の安全管理措置については別に定める。

第7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27条 保護管理者は、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す。

2 保護管理者は、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。

3 保護管理者は、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場合は、前2項に規定する措置を講ずる。

(業務の委託等)

第28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、必要な措置を講ずる。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。

- (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
- 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、委託する保有個人情報の秘匿性等その内容に応じて、委託先における個人情報の管理の状況について、年1回以上の定期的検査等により確認する。
 - 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。
 - 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する。

第8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29条 保有個人情報の漏えい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役職員は、直ちに当該保有個人情報を管理する保護管理者に報告する。

(注) 役職員は、当該事案の発生(事案発生のおそれを含む。)を認識した場合、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。

- 2 総括保護管理者は、前項に規定する報告の手順をあらかじめ定めるものとする。
- 3 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ずる。

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LANケーブルを抜くなど、被害拡大防止のため直ちに行いうる措置については、直ちに行う(職員に行わせることを含む。)ものとする。

- 4 保護管理者は、事案の発生した経緯、被害状況等を調査し、速やかに総括保護管理者に報告する。
- 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、当該事案の内容、経緯、被害状況等を速やかに理事長に報告する。
- 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、国土交通省に対し、速やかに情報提供を行う。
- 7 総括保護管理者は、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。

(公表等)

第30条 総括保護管理者は、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。

- 2 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。

第9章 監査及び点検の実施

(監査)

第31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5条から第30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、定期的に又は随時に監査（外部監査を含む。以下同じ。）（注）を行い、その結果を総括保護管理者に報告する。

（注）保有個人情報の秘匿性等その内容及びその量に応じて、実地監査を含めた重点的な監査として行うものとする。

2 監査の実施については別に定める。

(点検)

第32条 保護管理者は、各課における 保有個人情報の記録媒体、処理経路、保管方法等について、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、その結果を総括保護管理者に報告する。

(評価及び見直し)

第33条 総括保護管理者は、監査又は点検の結果等を踏まえ、本規程を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。

第10章 行政との連携

(行政機関との連携)

第34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、国土交通省と緊密に連携して、その保有する個人情報の適切な管理を行う。

附 則

この規程は、平成17年4月1日から施行する。

附 則（平成19年10月1日規程第5号）

この規程は、平成19年10月1日から施行する。

附 則（平成22年3月24日規程第3号）

この規程は、平成22年4月1日から施行する。

附 則（平成22年3月24日規程第7号）

この規程は、平成22年4月1日から施行する。

附 則（平成23年3月24日規程第3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3月26日規程第1号）

この規程は、平成24年4月1日から施行する。

附 則（平成24年3月26日規程第5号）

この規程は、平成24年7月1日から施行する。

附 則（平成28年3月24日規程第17号）

この規程は、平成28年3月24日から施行する。