国立研究開発法人建築研究所保有個人情報等管理規程

平成２８年３月２９日
規　程　第　６７　号

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「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、国立研究開発法人建築研究所（以下「研究所」という。）が保有する個人情報及び個人番号（以下「保有個人情報等」という。）の適切な管理のために必要な措置について定めるものとする。

（用語の定義）

第２条　この規程で使用する用語は、法及び番号法で使用する用語の例による。

第２章　管理体制

（総括保護管理者）

第３条　研究所に総括保護管理者１人を置く。

２　総括保護管理者は、総務部長をもって充てる。

３　総括保護管理者は、次に掲げる事務を行うものとする。

一　研究所における保有個人情報等の管理に関する事務の総括に関すること。

二　前号に掲げる事務を行うに当たって、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委員会を設け、定期又は随時に開催すること。

（保護管理者及び情報システム保護管理者）

第４条　保有個人情報等を取り扱う各部等（国立研究開発法人建築研究所組織規程（平成２７年規程第３号。以下「組織規程」という。）に規定する部、研究グループ及びセンターをいう。ただし、総務部にあっては組織規程第２３条に定める課をいい、企画部にあっては組織規程第２７条に定める課をいう。以下同じ。）に、保護管理者１人を置く。

２　保護管理者は、各部等の長をもって充てる。

３　保護管理者は、各部等における保有個人情報等の管理に関する事務を総括する。

４　研究所における基幹的な情報システムの整備及び管理を行う部等の保護管理者を、情報システム保護管理者とする。

（保護担当者）

第５条　保有個人情報等を取り扱う各部等に、保護担当者１人（業務上必要と認められる場合にあっては複数人）を置く。

２　保護担当者は、保護管理者が指定する者をもって充てる。

３　保護担当者は、保護管理者の指示を受け、各部等における保有個人情報等の管理に関する事務を行う。

（特定個人情報等取扱者）

第６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（以下「特定個人情報等取扱者」という。）並びにその役割を指定する。
２　保護管理者は、各特定個人情報等取扱者が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　研究所に監査責任者１人を置く。
２　監査責任者は、総務課長をもって充てる。
３　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。

第３章　教育等

（教育等）
第８条　総括保護管理者は、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、保有個人情報等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啓発その他必要な教育等を行う。
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等を行う。
３　総括保護管理者は、保護管理者及び保護担当者に対し、各部等の現場における保有個人情報等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、各部等の職員に対し、保有個人情報等の適切な管理のため、総括保護管理者の実施する教育等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。

第４章　職員の責務

（職員の責務）
第９条　職員は、法及び番号法の趣旨に則り、関連する法令及び規程等の定め並びに総括保護管理者、保護管理者、情報システム保護管理者及び保護担当者の指示に従い、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１０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（情報を入手し利用する行為をいう。以下同じ。）をする権限（以下「アクセス権限」という。）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するものとする。
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をしてはならない。
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等にアクセスをしてはならない。

（複製等の制限）
第１１条　職員が、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、当該保有個人情報等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ものとする。
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１２条　職員は、保有個人情報等の内容の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１３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、当該媒体の耐火金庫への保管、保管場所への施錠等の保有個人情報等の漏えい、滅失又は毀損を防止するための措置を講ずるものとする。

（廃棄等）
第１４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（端末機器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。

（保有個人情報等の取扱状況の記録）
第１５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、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するものとする。

第６章　個人番号の利用制限等

（個人番号の利用の制限）
第１６条　保護管理者は、特定個人情報等取扱者が個人番号を利用する事務について、番号法第９条の規定する事務に限定しなければならない。

（特定個人情報等の提供の求めの制限）
第１７条　特定個人情報等取扱者は、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制限）
第１８条　特定個人情報等取扱者は、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。

（特定個人情報等の収集・保管の制限）
第１９条　特定個人情報等取扱者は、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。

第２０条　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確認するものとする。

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。）を明確にし、物理的な安全管理措置を講ずるものとする。

第７章　情報システムにおける安全の確保

（アクセス制御）

第２２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。以下この章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。

（アクセス記録）

第２３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、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２４条　情報システム保護管理者は､保有個人情報等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ものとする。

（管理者権限の設定）

第２５条　情報システム保護管理者は、保有個人情報等の秘匿性等その内容に応じて、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２６条　情報システム保護管理者は、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。

（不正プログラムによる漏えい等の防止）

第２７条　情報システム保護管理者は、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等の処理）

第２８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ものとする。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、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２９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、暗号化のために必要な措置を講ずるものとする。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、当該保有個人情報等の秘匿性等その内容に応じて、適切に暗号化を行うものとする。

（記録機能を有する機器・媒体の接続制限）
第３０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機器等への接続の制限（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。

（端末機器の限定）
第３１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、その処理を行う端末機器を限定するために必要な措置を講ずるものとする。

（端末機器の盗難防止等）
第３２条　保護管理者は、端末機器の盗難又は紛失の防止のため、端末機器の固定、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、保護管理者が必要であると認めるときを除き、端末機器を外部へ持ち出し、又は外部から持ち込んで情報システムと接続してはならない。

（第三者の閲覧防止）
第３３条　職員は、端末機器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。

（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３５条　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。

（情報システム設計書等の管理）
第３６条　保護管理者及び情報システム保護管理者は、保有個人情報等に係る情報システムの設計書、構成図等又は研究所の基幹的な情報システムに関する設計書、構成図等の文書について業務上必要となる者以外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。

第８章　情報システム室等の安全管理

（入退管理）
第３７条　情報システム保護管理者は、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、入退の記録、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を行わせるものとする。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情報システム室等の安全を管理するための措置を講ずるものとする。

3　情報システム保護管理者は、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、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。）及び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。

（情報システム室等の安全管理）

第３８条　情報システム保護管理者は、外部からの不正な侵入に備え、情報システム室等に施錠装置等の措置を講じ、必要があると認めるときは、警報装置、監視設備の設置等の措置を講ずるものとする。

2　情報システム保護管理者は、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。

第９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３９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、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、法第９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２項に規定する措置を講ずるものとする。

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

（業務の委託等）

第４０条　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（特定個人情報等を含む。以下この項において同じ。）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。

一　個人情報に関する秘密保持、目的外利用の禁止等の義務

二　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

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、損害賠償責任の措置その他必要な事項

2　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、委託する保有個人情報等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、保有個人情報等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等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する。保有個人情報等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ものとする。

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４１条　保有個人情報等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職員は、時間を要する事実確認を行う前に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するものとする。

2　保護管理者及び情報システム保護管理者は、被害の拡大防止、復旧等のために必要な措置を速やかに講ずるものとする。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機器等の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（職員に行わせることを含む。）ものとする。

3　保護管理者及び情報システム保護管理者は、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の内容等について報告するものとする。

4　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するものとする。

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、当該独立行政法人等を所管する行政機関に対し、速やかに情報提供を行うものとする。

6　保護管理者及び情報システム保護管理者は、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。

（公表等）

第４２条　研究所は、発生した事案の内容、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等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ものとする。

第１１章　監査及び点検の実施

（監査）

第４３条　監査責任者は、保有個人情報等の秘匿性等その内容及びその量に応じて、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１０章に規定する措置の状況を含む当該独立行政法人等における個人情報の管理及び取り扱いの状況について、定期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。

（点検）
第４４条　保護管理者及び情報システム保護管理者は、各部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、又は情報システムの管理方法等について、定期又は随時に点検を行い、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。

（評価及び見直し）
第４５条　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ずるものとする。

第１２章　行政機関との連携

（行政機関との連携）
第４６条　研究所は、「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、当該独立行政法人等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ものとする。

附　則（平成２８年３月２９日規程第６７号）
（施行期日）
第１条　この規程は、平成２８年３月２９日から施行する。

（独立行政法人建築研究所が保有する個人情報の適切な管理に関する規程の廃止）
第２条　独立行政法人建築研究所が保有する個人情報の適切な管理に関する規程（平成１７年３月２５日規程第３号）は、廃止する。