独立行政法人勤労者退職金共済機構個人情報管理規程

（平成１７年　４月　１日）
改正　平成２７年　４月　１日
改正　平成２７年１２月２５日

独立行政法人勤労者退職金共済機構個人情報管理規程を次のように定める。

目次

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）に基づき、独立行政法人勤労者退職金共済機構（以下「機構」という。）の保有する個人情報の取扱いについて必要な事項を定めることを目的とする。

（定義）

第２条　この規程における用語の意義は、法第２条及び次に定めるところによる。

（１）この規程において「職員」とは、独立行政法人勤労者退職金共済機構が定める就業規則、労働条件の達等の適用を受ける者をいう。

（２）この規程において「部」とは、独立行政法人勤労者退職金共済機構組織規程（以下「組織規程」という。）の第９条の規定により機構に置かれる部をいい、「部長」とはこれらの長をいう。
（３）この規程において「課室」とは、組織規程第９条の規定により機構に置かれる課及び室をいい、「課室長」とはこれらの長をいう。
（４）この規程において「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、これら全体で保有個人情報に係る業務処理を行うものをいう。

第２章　管理体制

（総括保護管理者）
第３条　総務担当理事をもって総括保護管理者として、機構における保有個人情報の管理に関する規程類の整備、個人情報ファイル簿の整備、保有個人情報の管理に関する事務の指導監督、研修等の実施その他の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ものとする。

（副総括保護管理者）
第４条　総務部長をもって副総括保護管理者とし、機構における保有個人情報の管理に関する事務について総括保護管理者を補佐又は代理するものとする。

（情報システム保護管理者）
第５条　情報システムを保有する部の部長をもって情報システム保護管理者とし、部における情報システムを適切に管理するものとする。

（保護管理者）
第６条　保有個人情報を取り扱う課室の課室長をもって保護管理者とし、課室における保有個人情報の適切な管理を確保するものとする。
２　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、情報システム保護管理者と連携して適切な管理を確保するものとする。

（保護担当者）
第７条　保有個人情報を取扱う課室の文書管理担当者をもって保護担当者とし、保護管理者の命を受けて、当該保護管理者の事務を補佐するものとする。

（監査責任者）

第８条　監事をもって、監査責任者とし、保有個人情報の管理の状況について監査するものとする。

（総合窓口）

第９条　総務課に総合窓口を置き、開示、訂正、利用停止、個人情報保護制度の案内、苦情の相談等を受け付けるものとする。

（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、機構における保有個人情報の管理に係る重要事項の決定、連絡・調整等を行うために必要があると認めるときは、関係する役員及び職員（以下「役職員」という。）を構成員とする委員会を設け、定期に又は随時に開催するものとする。

２　委員会の要綱については、別に定める。

（個人情報ファイル簿）

第１１条　総務課に法第１１条に規定する個人情報ファイル簿（様式１）を備えるものとする。

２　副総括保護管理者は、保有個人情報について個人情報ファイル簿を整備し、一般の閲覧に供するものとする。

第３章　教育研修

（教育研修）

第１２条　副総括保護管理者は、保有個人情報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　副総括保護管理者は、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ものとする。

３　副総括保護管理者は、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に必要な教育研修を行うものとする。

４　保護管理者は、当該部課室の職員に対し、保有個人情報の適切な管理のために、副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。

第４章　役職員の責務

（役職員の責務）

第１３条　役職員は、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、副総括保護管理者、情報システム保護管理者、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。

２　役職員又は役職員であった者は、その業務に関して知り得た個人情報の内容をみだりに他人に知らせ、又は不当な目的に使用してはならない。

第５章　個人情報の取得

（個人情報の取得）

第１４条　保護管理者は、個人情報を含む情報の収集をする際には事前に、副総括保護管理者の許可を得なければならない。

第６章　保有個人情報の取扱い

（アクセス制限）

第１５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た上で、当該保有個人情報ごとその名簿を副総括保護管理者に届け出なければならない。

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　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１６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、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。このうち、保護管理者は、定例的な行為について予めその方法等を指定することができる。また、予め指定した以外の行為については、当該保有個人情報の名称、記録項目、記録範囲、提供先、目的等を示した上で保護管理者の許可を得るものとする。

（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

（誤りの訂正等）

第１７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、保護管理者が指示する方法により、訂正等を行うものとする。

（媒体の管理等）

第１８条　保護管理者は、アクセス権限を有する職員以外の者が保有個人情報の記録されている媒体にアクセスすることがないよう、媒体ごとに適切な保管場所を定めた上で、副総括保護管理者に届け出なければならない。

２　職員は、保有個人情報が記録されている媒体を前項で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。

３　保管場所に係る鍵の所在については、アクセス権限を有しない職員が把握できないよう、原則として保護管理者が管理するものとする。

（廃棄等）

第１９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。）が不要になった場合には、保護管理者が指示する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。

２　職員は、前項により廃棄した場合には、保護管理者に報告しなければならない。

（保有個人情報の取扱状況の記録）

第２０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、個人情報管理簿（様式２）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状況について記録するものとする。ただし、情報システムについては、情報システム保護管理者において、別途記録（第１８条に係るものを除く。）を保持することとする。

第７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　情報システム保護管理者は、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２６条を除く。）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　情報システム保護管理者は、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の措置を講ずるものとする。

（アクセス記録）

第２２条　情報システム保護管理者は、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　情報システム保護管理者は、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２３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、当該保有個人情報へのアクセス状況を監視する機能を設定するとともに、当該機能の定期的確認を行う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２４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防止）

第２５条　情報システム保護管理者は、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の防止）

第２６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の漏えい、滅失また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２７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

消去するものとする。

２　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ものとする。

（暗号化）

第２８条　情報システム保護管理者は、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ものとする。

２　職員は、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ものとする。

（記録機能を有する機器・媒体の接続制限）

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、当該保有個人情報の漏えい、減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。

（端末の限定）

第３０条　情報システム保護管理者は、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じなければならない。

（端末の盗難防止等）

第３１条　保護管理者は、端末の盗難又は紛失の防止のため、必要に応じて端末の固定を行うとともに部又は課室の出入口の施錠を徹底するものとする。

２　職員は、保護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。

（第三者の閲覧禁止）

第３２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、スクリーンセーバーのパスワード管理や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３３条　職員は、事務処理マニュアルに基づき、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情報の内容の確認、既存の保有個人情報との照合を行うものとする。

（バックアップ）

第３４条　情報システム保護管理者は、保有個人情報の重要度に応じて、バックアップを作成し、原本と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３５条　情報システム保護管理者は、保有個人情報に係る情報システムの設計書、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、鍵付き書庫に保管するとともに、その複製等については、第１６条の規定を準用する。

第８章　情報システム室等の安全管理

（入退安全管理）

第３６条　情報システム保護管理者は、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限定するとともに、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徹底を行うものとする。

２　情報システム保護管理者は、保有個人情報を記録する媒体を保管するための施設（第４項において「保管施設」という。）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、前項と同様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、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、所在表示の制限の措置を講ずるものとする。

４　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の設定、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の措置を講ずるものとする。

（情報システムの管理）

第３７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、警報装置、監視設備を設置のうちいずれか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、必要に応じて情報システム室等に耐震、防火、防煙、防水等の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　保有個人情報の提供及び業務の委託等

（保有個人情報の提供）

第３８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、改善要求をするものとする。

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２項に規定する措置を講ずるものとする。

（業務の委託等）

第３９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ものを選定することがないよう、プライバシーマーク取得（予定を含む。）企業（組合等を含む。）、又は機構と同等以上の個人情報の保護に関する措置を講じているなど理事長が適当と認める企業（組合等を含む。）に限定することとする。

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、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した上で契約を締結しなければならない。

（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

３　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。

４　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、必要に応じ定期的検査等を行い、確認することとする。

５　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２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、必要に応じ委託先を通じて又は委託元自らが４の措置を実施することができる。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。

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４０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（役職員に行わせることを含む。）ものとする。

３　保護管理者は、発生した事案の内容、経緯、被害状況等を調査し、副総括保護管理者に報告しなければならない。副総括保護管理者は、発生した事案が特に重大であると認める場合には、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、前項の規定に基づく報告を受けた場合には、発生した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　第１項から前項までの規定にかかわらず、保護管理者が不明である場合、保護管理者が不在である等緊急の対応が必要な場合、発生した事案が特に重大であると考えられる場合等にあっては、役職員は直ちに理事長、総括保護管理者又は副総括保護管理者に当該事案について報告するものとする。この場合、報告を受けた者は直ちに副総括保護管理者に通知するとともに、副総括保護管理者は当該保有個人情報を管理する保護管理者に対し、報告された事項に関する第２項及び第３項の措置を行うよう指示するものとする。

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、厚生労働省に対し、速やかに情報提供を行うものとする。

７　保護管理者は、発生した事案の原因を分析し、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４１条　総括保護管理者は、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の本人への対応等の措置を講じなければならない。

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）に情報提供を行うものとする。

第１１章　監査及び点検の実施

（監査）

第４２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章から前章まで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。）を行い、その結果を理事長及び総括保護管理者に報告するものとする。

（点検）

第４３条　保護管理者は、各課室等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。

（評価及び見直し）

第４４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、その見直しを行うものとする。

第１２章　厚生労働省との連携

第４５条　機構は、個人情報の保護に関する基本方針の４を踏まえ、厚生労働省と緊密に連携して、保有個人情報の適切な管理を行うものとする。

第１３章　雑則

（その他の必要事項）

第４６条　この規程に定めるもののほか、機構の保有個人情報の管理に必要な事項につい

ては理事長が別に定める。

附　則

（施行期日）

１　この規程は、平成１７年４月１日から実施する。

（規程の廃止）

２　独立行政法人勤労者退職金共済機構中小企業退職金共済事業本部電子計算機処理データ保護管理規程（平成１５年１０月１日施行）及び独立行政法人勤労者退職金共済機構特定業種退職金共済事業における電子計算機処理データ保護管理規程（平成１５年１０月１日施行）は、廃止する。

附　則

この規程は、平成２７年４月１日から実施する。なお、特別な事情により同日から実施することが困難なものについては、できるだけ早期に必要な措置を講ずるものとする。

附　則

この規程は、平成２７年１２月２５日から実施する。