国立大学法人東京外国語大学個人情報の管理に関する細則

［令和５年３月22日
規　　則　第55号］

東京外国語大学個人情報の管理に関する細則（平成２６年１１月１１日制定）の全部を改正する。

第１章　総則

（目的）

第１条　この細則は、国立大学法人東京外国語大学個人情報保護規程(令和４年規則第13号。以下「規程」という。)第10条及び第12条に基づき、国立大学法人東京外国語大学（以下「本学」という。)における個人データの適切な管理のために必要な事項を定め、もって個人情報の適正な取扱いの確保に資することを目的とする。

（定義）

第２条　この細則において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1) 情報システム　本学の業務に係る情報を収集・蓄積・処理・伝達・利用するためのコンピュータのハードウェア及びソフトウェア、データベース、通信・伝送装置、保管・蓄積装置、記録媒体など（仮想基盤上に構築された仮想システム及びハウジングサービス、レンタルサーバ、オンラインストレージサービス、クラウドサービス等も含むものとする。）をいう。

(2) 端末　パソコン、タブレット、スマートフォンなどの情報機器（仮想デスクトップやリモートデスクトップを含むものとする。）をいう。

(3) 職員　常勤職員のほか、非常勤職員、派遣労働者等を含むものとする。

第２章　安全管理措置

第１節　組織的安全管理措置

（事案発生時の報告連絡体制及び再発防止措置）

第３条　個人データの漏えい等の事案の発生又は兆候を把握した場合及び個人情報の取扱いに係る規律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問題となる事案の発生のおそれを認識した役員又は職員（以下「職員等」という。）は、直ちに当該個人データ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、発生した事案による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場合は、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を直ちに行う（職員等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、総括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。

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、被害状況等を学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、規程第１３条に定める報告を速やかに行うものとする。

６　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じなければならない。

７　保護管理者は、総括保護管理者の指示に従い、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、当該事案に係る個人データの本人への対応等の措置を講ずるものとする。

（運用状況の確認）

第４条　保護管理者は、本細則に基づく個人情報管理の運用状況を確認するため、次の各号に定める項目について利用状況等を記録し、その記録を一定期間保存し、分析するための体制を整備するものとする。

(1) 個人情報データベース等の利用・出力状況の記録

(2) 個人データが記載又は記録された書類・媒体等の持ち運び等の状況

(3) 個人情報データベース等の削除・廃棄記録

(4) 削除・廃棄を委託した場合、これを証明する記録等

(5) 個人情報データベース等を情報システムで取り扱う場合、職員等の情報システムの利用状況（ログイン実績、アクセスログ等）

（端末の限定）

第５条　保護管理者は、個人データ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。

（クラウドサービス等の利用）

第６条　個人データを取扱う情報システムとしてハウジングサービス、レンタルサーバ、オンラインストレージサービス、クラウドサービスなど（以下「クラウドサービス等」という。を利用する場合には、クラウドサービス等のレベルに応じた適切な情報セキュリティ管理を行う能力を有する者であることを慎重に確認した上で選定しなければならない。

２　前項の規定によりクラウドサービス等を利用する場合において契約の締結等を行うときは、個人データを取扱う情報システムが該当するこの細則の規定に相当する事項を契約書等に明記するものとする。

（取扱状況の確認）

第７条　保護管理者は、個人データの取扱状況を把握するため、個人情報管理台帳を作成し、以下の事項を記録するものとする。なお、個人情報管理台帳には、個人データ自体は記載しないものとする。

(1) 個人情報データベース等の種類、名称

(2) 個人データの項目

(3) 責任者

(4) 取扱部署

(5) 利用目的

(6) アクセス権を有する者

２　規程２３条に定める個人情報ファイル簿を作成する場合には、前項の規定を適用しない。

（監査）

第８条　監査責任者は、個人データの適切な管理を検証するため、本学における個人データ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。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９条　保護管理者は、各部局等における個人データの記録媒体、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１０条　総括保護管理者及び保護管理者は、第８条に規定する監査又は前条に規定する点検の結果等を踏まえ、実効性等の観点から個人データの適切な管理のための措置について評価を行うものとする。

２　総括保護管理者及び保護管理者は、前項の評価の結果を踏まえ、必要があると認めるときは、その見直しの措置を講ずるものとする。

（文部科学省との連携）

第１１条　本学は、「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）を踏まえ、文部科学省と緊密に連携して、本学が保有する個人情報の適切な管理を行うものとする。

第２節　人的安全管理措置

（職員等の研修）

第１２条　総括保護管理者は、個人データの取扱いに従事する職員等に対し、個人データの取扱いについて理解を深め、個人データの保護に関する意識の啓発その他を図るための必要な教育研修を行うものとする。

２　総括保護管理者は、個人データ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等に対し、個人データ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　保護管理者は、その所属する組織の職員等に対し、個人データ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ものとする。

４　総括保護管理者は、保護管理者及び保護担当者に対し、各部局等の現場における個人データの適切な管理のための教育研修を実施するものとする。

５　個人データを取り扱う職員等は、個人データ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に参加しなければならない。

（職員等の責務）

第１３条　職員等は、法の趣旨に則り、関連する法令等及び規則等の定め並びに総括保護管理者、保護管理者及び保護担当者の指示に従い、個人データを取り扱わなければならない。

２　職員等は、その業務に関して知り得た個人データの内容をみだりに他人に知らせ、又は不当な目的に利用してはならない。その職を退いた後においても同様とする。

３　職員等は、アクセス権限を有しない個人データにアクセスしてはならない。

４　職員等は、取り扱う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個人データを取り扱

ってはならない。

５　職員等は、業務上の目的でアクセス権限を有する個人データにアクセスする場合であっても、情報セキュリティ対策が実施されていることが確認できないネットワークや端末を使用して個人データにアクセスしてはならない。

第３節　物理的安全管理措置

（個人データを取り扱う区域の管理）

第１４条　保護管理者は、個人情報データベース等を取り扱うサーバ等の重要な情報システムを管理する区域（以下「管理区域」という。）及びその他の個人データ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、それぞれの区域に対し、物理的安全管理のための適切な措置を講じるものとする。

（管理区域の入退管理）

第１５条　保護管理者は、管理区域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等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、個人データを記録する媒体を保管するための施設（以下「保管施設」という。）を設けている場合において、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　保護管理者は、必要があると認めるときは、管理区域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。

４　保護管理者は、管理区域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、及び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を行うために必要な措置を講ずるものとする。

（管理区域の管理）

第１６条　保護管理者は、外部からの不正な侵入に備え、管理区域に施錠装置、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　保護管理者は、災害等に備え、管理区域に、耐震、防火、防煙、防水等の必要な措置を講ずるとともに、停電時におけるサーバ等の機器の確保予備電源の確保、配線の損傷防止等の措置を講ずるものとする。

（取扱区域の管理）

第１７条　保護管理者は、取扱区域に可能な限り壁又は間仕切り等を設置し、又は当該取扱区域において個人データを取り扱う職員等以外の者の往来が少ない場所への座席配置や、後ろから覗き見される可能性が低い場所への座席配置等をするなど座席配置の工夫等をすることにより、権限を有しない者による個人データの閲覧等を防止するものとする。

（第三者の閲覧防止）

第１８条　職員等は、端末の使用に当たっては、個人データ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じなければならない。

（端末の盗難防止等）

第１９条　保護管理者は、管理区域及び取扱区域における個人データを取り扱う機器、電子媒体及び書

類等の盗難又は紛失等を防止するために、次の各号に掲げる措置のいずれかを講じるものとする。

(1) 個人データを取り扱う機器、電子媒体又は書籍等を、施錠できるキャビネット・書庫等に保管する。

(2) 個人データを取り扱う情報システムが機器のみで運用されている場合は、セキュリティワイヤー等により固定する。

(3) 前２号により難い場合は、これらに準ずる措置。

２　職員等は、保護管理者が必要と認めるときを除き、端末及び記憶装置を外部へ持ち出し、又は外部から持ち込んではならない。

３　保護管理者は、台帳等を整備して、端末及び記憶装置の学外持ち出し状況を記録するものとする。

４　保護管理者は、学外に持ち出した端末及び記憶装置の盗難あるいは紛失の防止のために必要な措置を講ずるものとする。

５　保護管理者は、端末及び記憶装置の取扱いに関する定めを整備（その定期又は随時の見直しを含む。）するものとする。

（記録機能を有する機器・媒体の接続制限）

第２０条　保護管理者は、個人データの秘匿性等その内容に応じて、当該個人データの情報漏えい等の防止のため、スマートフォン、ＵＳＢメモリ等の記録機能を有する機器・媒体のサーバ及び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。

（媒体の管理等）

第２１条　職員等は、保護管理者の指示に従い、個人データ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、施錠等を行うものとする。

（電子媒体等を持ち運ぶ場合の漏えい等の防止）

第２２条　本学は、個人データが記録された電子媒体又は書類等の持ち運び（個人データを管理区域又は取扱区域の外へ移動させることをいう。）は、次に掲げる場合を除き禁止する。

(1) 個人データに係る外部委託先に、委託事務を実施する上で必要と認められる範囲内でデータを提供する場合

(2) 利用目的の範囲で個人データを利用する場合

２　前項により個人データが記録された電子媒体又は書類等の持ち運びを行う場合には、以下の安全策を講じるものとする。

(1) 個人データが記録された電子媒体を安全に持ち運ぶ方法

ア　持ち運びデータの暗号化

イ　持ち運びデータのパスワードによる保護

ウ　施錠できる搬送容器の使用

エ　追跡可能な移送手段の利用

(2) 個人データが記載された書類等を安全に持ち運ぶ方法

ア　封緘、目隠しシールの貼付

（個人データの削除及び機器、電子媒体等の廃棄）

第２３条　職員等は、個人データ又は個人データ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、次の各号に掲げる場合ご

とに、適切な措置を講じるものとする。

(1) 個人データが記録された書類等を廃棄する場合、焼却、溶解、シュレッダー、マスキング等の復元不可能な手段を用いるものとする。

(2) 個人データが記録された機器及び電子媒体等を廃棄する場合、専用データ削除ソフトウェアの利用又は物理的な破壊等により、復元不可能な手段を用いるものとする。

(3) 情報システム中の個人データを削除する場合、容易に復元できない手段を用いるものとする。

２　保護管理者は、個人データの削除、又は電子媒体等の廃棄を委託した場合には、委託先が確実に削除又は廃棄したことについて、証明書等により確認するものとする。

３　職員等は、個人データの記録に利用している媒体（端末及びサーバに内蔵されているものを含む。）を他の目的で再利用する場合には、保護管理者の指示に従い、当該個人データの復元又は判読を不可能にする方法により当該情報の消去を行った後に再利用するものとする。

４　職員等は、個人データを記録している媒体あるいは媒体を内蔵する装置を修理する場合には、保護管理者の指示に従い、媒体を取り外す又は修理業者と機密情報の取扱いについて書面を取り交わした上で修理を依頼しなければならない。

第４節　技術的安全管理措置

（アクセス制御）

第２４条　保護管理者は、個人データ（情報システムで取り扱うものに限る。以下本節において同じ。）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、情報システムにアクセスする者の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。

（外部からの不正アクセス等の防止）

第２５条　保護管理者は、次の各号に掲げる方法により、情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用するものとする。

(1) 情報システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する。

(2) 情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入し、不正ソフトウェアの有無を確認する。

(3) 機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。

(4) ログ等の分析を定期に及び随時に行い、不正アクセス等を検知する。

(5) 不正アクセス等の被害に遭った場合であっても、被害を最小化する仕組み（ネットワークの遮断等）を導入し、適切に運用する。

(6) 情報システムの不正な構成変更（許可されていない電子媒体及び機器の接続、ソフトウェアのインストール等）を防止するために必要な措置を講じる。

（アクセス記録）

第２６条　保護管理者は、個人データ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、定期に又は随時に分析するために必要な措置を講ずる。

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２７条　保護管理者は、個人データの秘匿性等その内容及びその量に応じて、当該個人データへの不適切なアクセスの監視のため、個人データ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２８条　保護管理者は、秘匿性等その内容に応じて、個人データを取り扱う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。

（不正プログラムによる漏えい等の防止）

第２９条　保護管理者は、ソフトウェアの脆弱性や不正プログラムによる個人データの漏えい、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。

（情報システムの安全性の確保）

第３０条　保護管理者は、情報システムの設計時に安全性を確保し、継続的に見直す（情報システムのぜい弱性を突いた攻撃への対策を講じることも含む。）ものとする。

（情報システムにおける個人データの処理）

第３１条　職員等は、個人データについて、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、前項処理による個人データ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。

３　在宅勤務用の端末機器の貸出については、返却時に情報企画室において初期化を行うものとする。

（情報漏えい等の防止）

第３２条　保護管理者は、個人データをインターネット等により外部に送信する場合及び情報システム内に保存する場合、次の各号に掲げる方法等により、通信経路における情報漏えい、情報システム内に保存されている個人情報の情報漏えい等を防止するものとする。

(1) 通信経路における情報漏えい等を防止するため、通信データの暗号化。

(2) 情報システムに保存されている個人情報の情報漏えい等を防止するため、データの暗号化又はパスワードによる保護。

２　保護管理者は、前項に規定する措置を講ずる場合には、暗号化及び複合化に必要な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を行うた

めに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　職員等は、情報システムで取り扱う個人データの重要度に応じて、入力原票と入力内容との照合、処理前後の個人データの内容の確認、既存の個人データとの照合等を行うものとする。

２　職員等は、個人データ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。

（バックアップ）

第３４条　保護管理者は、個人データの重要度に応じて、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３５条　保護管理者は、個人データに係る情報システムに関する文書（設計図、構成図等）が外部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５節　外的環境の把握

（外国におけるデータの取扱い）

第３６条　保護管理者は、職員等が外国において個人データを取り扱う場合、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、個人データ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。

第３章　個人データの委託の取扱い

（委託先における安全管理措置）

第３７条　総括保護管理者及び保護管理者は、個人データの全部又は一部の取扱いを委託する場合には、本学自らが果たすべき安全管理措置と同等の措置が委託先において適切に講じられるよう、必要かつ適切な監督を行うものとする。

２　前項の「必要かつ適切な監督」には次に掲げる事項が含まれる。

(1) 委託先の適切な選定

(2) 委託先に安全管理措置を遵守させるために必要な契約の締結

(3) 委託先における個人データの取扱状況の把握

３　前項第１号の委託先の適切な選定に当たっては、委託先の安全管理措置が、本学における安全管理措置と同等であることを確認するため、規程及び本細則に定める各項目が、委託する業務内容に沿って、確実に実施されることについて、あらかじめ確認しなければならない。

４　前項の規定より業務を外部に委託する場合において契約を締結するときは、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（再委託先が委託元の子会社（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

(3) 個人データの複製等の制限に関する事項

(4) 個人データ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データ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
(7) 情報セキュリティ対策の状況

5　個人データの取扱いに係る業務を外部に委託する場合には、委託する業務による個人データ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データ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。

6　委託先において、個人データ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個人データ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項の措置を実施する。個人データ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、前項の派遣労働者に個人データの取扱いに係る業務を行わせる場合は、当該派遣労働者に関係法令及び規程等を遵守させるための指導及び監督を行うものとする。

8　個人データ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、個人データ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ずるものとする。

第４章　雑則

（苦情処理）

第３８条　総括保護管理者は、本学における個人情報の取扱いに関し苦情があった場合には、その内容に応じて、適切かつ迅速な処理に努めるものとする。

（雑則）

第３９条　この細則に定めるもののほか、個人情報の管理に関し必要な事項は、総括保護管理者が定める。

附　則

この細則は、令和５年４月１日から施行する。