

○国立大学法人筑波技術大学保有個人情報管理規程

〔平成17年10月3日〕
規程第37号

最終改正 平成30年2月28日規程第7号

国立大学法人筑波技術大学保有個人情報管理規程

目次

- 第1章 総則（第1条，第2条）
- 第2章 管理体制（第3条－第7条）
- 第3章 教育研修（第8条）
- 第4章 職員の責務（第9条）
- 第5章 保有個人情報等の取扱い（第10条－第15条）
- 第6章 情報システムにおける安全の確保等（第16条－第30条）
- 第7章 情報処理室等の安全管理（第31条，第32条）
- 第8章 保有個人情報等の提供及び業務の委託等（第33条－第34条）
- 第9章 安全確保上の問題への対応（第35条，第36条）
- 第10章 監査及び点検の実施（第37条－第39条）
- 第11章 補則（第40条－第41条）

附則

第1章 総則

（趣旨）

第1条 この規程は、国立大学法人筑波技術大学個人情報保護規則（平成17年規則第3号。以下「規則」という。）第48条の規定に基づき、国立大学法人筑波技術大学（以下「本学」という。）の保有する個人情報（法第44条の15に規定する独立行政法人等非識別加工情報，独立行政法人等非識別加工情報の作成に用いた保有個人情報から削除した記述等及び個人識別符号並びに別に定める方法により行った加工の方法に関する情報（以下「独立行政法人等非識別加工情報等」という）を含む。次項及び第41条において同じ。）の適切な管理に関し必要な事項を定めるものとする。

2 本学の保有する個人情報の管理については、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。）その他の法令等に別段の定めがあるもののほか、この規程の定めるところによる。

（定義）

第2条 この規程における用語の定義は、規則第2条のほか、次の各号に定めるところによる。

- (1) 部局等 国立大学法人筑波技術大学組織及び管理運営に関する規則第13条第1項第1号及び第2号，第13条の2第1項，第14条第1項，第15条第1項，第16条第1項，第17条第1項並びに第18条第1項に定める組織をいう。

第2章 管理体制

(総括保護管理者)

第3条 本学に、総括保護管理者を一人置き、学長が指名する理事をもって充てる。

2 総括保護管理者は、学長を補佐し、本学における保有個人情報及び独立行政法人等非識別加工情報等（以下「保有個人情報等」という。）の管理に関する事務を総括する任に当たる。

(保護管理者)

第4条 保有個人情報等を取り扱う部局等（規則第2条第14項に規定する組織をいう。以下同じ。）に、当該保有個人情報等の適切な管理を確保する任に当たる保護管理者を置き、当該部局等の長又はそれに代わる者として学長が指名するものをもって充てる。

2 保護管理者は、保有個人情報等を情報システムで取り扱う場合は、当該情報システムの管理者と連携して、その任に当たる。

(保護担当者)

第5条 部局等に、保護担当者1人又は複数人を置き、当該部局等の保護管理者が指定する職員をもって充てる。

2 保護担当者は、保護管理者を補佐し、部局等における各組織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。

(監査責任者)

第6条 本学に、監査責任者1人を置き、学長が指名する監事をもって充てる。

2 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。

(個人情報管理委員会)

第7条 本学における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、個人情報管理委員会（以下「委員会」という。）を置く。

2 委員会は、総括保護管理者及び保護管理者をもって組織し、総括保護管理者が定期に又は随時に開催する。

3 委員会に関する必要な事項は、別に定める。

第3章 教育研修

(教育研修)

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研修を行う。

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等の適切な管理のための教育研修を定期的実施する。

4 保護管理者は、当該課・学科等の職員に対し、保有個人情報等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 職員の責務

(職員の責務)

第9条 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、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してはならない。

(複製等の制限)

第11条 保護管理者は、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、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。

(1) 保有個人情報等の複製

(2) 保有個人情報等の送信

(3) 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

(4) 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。

(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、耐火金庫への保管、施錠等を行う。

(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保有個人情報等の消去又は当該媒体の廃棄を行う。

2 保護管理者は、レンタル及びリース契約端末からの保有個人情報等の漏えいを防ぐため、契約業者に対して当該端末返却時における端末に内蔵される記録媒体の完全な初期化を義務づけるものとする。

(保有個人情報等の取扱い状況の記録)

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、台帳等を整備して、当該保有個人情報等の利用及び保管等の取扱いの状況について記録する。

第6章 情報システムにおける安全の確保等

(アクセス制御)

第16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。以下本章（第24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。

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。

(アクセス記録)

第17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。

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。

(アクセス状況の監視)

第18条 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。

(管理者権限の設定)

第19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、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20条 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。

(不正プログラムによる漏えい等の防止)

第21条 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等の処理)

第22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。

2 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。

(暗号化)

第 2 3 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、その暗号化のために必要な措置を講ずる。

2 職員は、前項を踏まえ、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。

(入力情報の照合等)

第 2 4 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との照合等を行う。

(バックアップ)

第 2 5 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。

(情報システム設計書等の管理)

第 2 6 条 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。

(端末機器の限定)

第 2 7 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。

(端末機器の盗難防止等)

第 2 8 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。

2 職員は、保護管理者が必要があると認めるときを除き、端末機器を外部へ持ち出し、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 2 9 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。

(記録機能を有する機器・媒体の接続制限)

第 3 0 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。

第 7 章 情報システム室等の安全管理

(入退管理)

第 3 1 条 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、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。

2 保護管理者は、保有個人情報等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。

3 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の安全を管理するための措置を講ずる。

4 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、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。）、パスワード等の読取防止等を行うために必要な措置を講ずる。

（情報システム室等の管理）

第32条 保護管理者は、外部からの不正な侵入に備え、情報システム室等に施錠装置、警報装置、監視設備の設置等の措置を講ずる。

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。

第8章 保有個人情報等の提供及び業務の委託等

（保有個人情報の提供）

第33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ときは、前2項に規定する措置を講ずる。

（独立行政法人等非識別加工情報の提供）

第33条の2 保護管理者は、規則第44条の2及び国立大学法人筑波技術大学独立行政法人等非識別加工情報の提供に関する取扱規程（以下「取扱規程」という。）第8条（取扱規程第11条第2項の規定により取扱規程第8条の規定を準用する場合を含む。）により、独立行政法人等非識別加工情報の利用に関する契約を締結した者（以下「契約相手方」という。）から法44条の5第2項第7号の規定に基づき当該契約相手方が講じた独立行政法人等非識別加工情報の適切な管理に支障を及ぼすおそれがある旨の報告を受けたときは、直ちに総括保護管理者に報告するとともに、当該契約相手方がその是正のために講じた措置を確認しなければならない。

（業務の委託等）

第34条 独立行政法人等非識別加工情報の作成に係る業務又は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、保有個人情報等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、必要な措置を講じなければならない。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、保有個人情報等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) 保有個人情報等に関する秘密保持、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) 保有個人情報等の複製等の制限に関する事項
 - (4) 保有個人情報等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保有個人情報等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、委託先における保有個人情報等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保有個人情報等の取扱いに関する事項を明記する。

第9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35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、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。

- 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、総括保護管理者に報告する。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。
- 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。
- 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文部科学省等に対し、速やかに情報提供を行う。
- 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ずる。

(公表等)

第36条 本学は、前条の事案が発生したときは、事案の内容、影響等に応じて、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とともに、速やかに事実関係及び再発防止策等を公表するものとする。

2 前項の規定により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）及び個人情報保護委員会に情報提供を行う。

第10章 監査及び点検の実施

（監査）

第37条 監査責任者は、保有個人情報等の適切な管理を検証するため、第3条から第36条に規定する措置の状況を含む本学における保有個人情報等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、その結果を総括保護管理者に報告する。

（点検）

第38条 保護管理者は、各組織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39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11章 補則

（行政機関との連携）

第40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）4を踏まえ、文部科学省と緊密に連携して、保有個人情報等の適切な管理を行う。

（個人情報保護委員会事務局への報告）

第40条の2 総括保護管理者は、次に掲げるときは、直ちに個人情報保護委員会事務局に報告しなければならない。

- (1) 第33条の2、第35条第3項及び第4項の報告とするとき
- (2) 第35条第6項及び第36条第1項の措置を講じたとき
- (3) 契約相手方が取扱規定第13条各号に該当すると認められ契約を解除しようとするとき及び解除したとき

第41条 この規程に定めるもののほか、本学が保有する個人情報の管理について必要な事項は、別に定めるところによる。

附 則

この規程は、平成17年10月3日から施行し、同年10月1日から適用する。

附 則

この規程は、平成22年4月1日から施行する。

附 則

この規程は、平成27年3月18日から施行する。

附 則

この規程は、平成28年1月27日から施行する。

附 則

この規程は、平成30年2月28日から施行し、同年2月23日から適用する。