国立大学法人高知大学における行政機関等匿名加工情報等の適切な管理に関する規則

（平成 31 年２月 27 日
規　則　第　68　号）

最終改正　令和５年３月 16 日規則第 88 号

（趣旨）

第１条　この規則は、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「法」という。）第 121 条及び第 123 条並びに国立大学法人高知大学における行政機関等匿名加工情報の提供に関する規則第 16 条第４項及び国立大学法人高知大学の保有する個人情報の適切な管理に関する規則第 13 条の２第７項の規定に基づき国立大学法人高知大学（以下「本学」という。）における行政機関等匿名加工情報等及び民間事業者等から取得した匿名加工情報（以下「加工情報等」という。）の適切な管理に関し、必要な事項を定める。

（定義）

第２条　この規則において使用する用語は、国立大学法人高知大学の保有する個人情報の適切な管理に関する規則及び国立大学法人高知大学における行政機関等匿名加工情報の提供に関する規則において使用する用語の例によるものとする。

（管理体制）

第３条　本学に、総括保護管理者を置き、理事（総務・企画・危機管理担当）をもって充てる。

２　加工情報等を取り扱う事務局各課・室に、保護管理者を置き、事務局各課長又は室長をもって充てる。

３　加工情報等を取り扱う事務局各課・室に、保護担当者を置き、前項に規定する保護管理者が指定する者をもって充てる。

４　前２項の規定にかかわらず、教員保有個人情報及び医学部附属病院が保有する医療関係情報に係る加工情報等の管理に当たっては、当該部局等の長又は当該部局等の長に準ずる者を保護管理者とし、当該部局等の教員等を保護担当者とする。

５　本学に監査責任者を置き、法人監査室長をもって充てる。

６　総括保護管理者は、本学における加工情報等の管理に関する事務を総括する。

７　保護管理者は、加工情報等の適切な管理を確保する。加工情報等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。

８　保護担当者は、保護管理者を補佐し、加工情報等の管理に関する事務を担当する。

９　監査責任者は、加工情報等の管理の状況について監査する。

（教育研修）

第４条　総括保護管理者は、加工情報等の取扱いに従事する役員及び職員等に対し、加工情報等の取扱いについて理解を深め、加工情報等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わなければならない。

２　総括保護管理者は、高知大学情報セキュリティポリシー（以下「セキュリティポリシー」という。）に定める最高情報セキュリティ責任者との協力の下に、加工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等に対し、加工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わなければならない。

３　総括保護管理者は、保護管理者及び保護担当者に対し、部局等の現場における加工情報等の適切な管理のための教育研修を実施しなければならない。

４　保護管理者は、当該部局等の職員等に対して、加工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研修への参加の機会を付与する等の必要な措置を講じなければならない。

（責務及び罰則）

第５条　役員又は職員等は、法の趣旨に則り、関連する法令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、加工情報等を取り扱わなければならない。

２　役員又は職員が次の各号に掲げる行為を行った場合は、本学の懲戒に関する定めによる処分を受けるほか、法に定める罰則が適用される。

(1)　正当な理由がないにもかかわらず、個人の秘密事項が記載された加工情報等（全部又は一部を複製し、又は加工したものを含む。）を提供した場合

(2)　業務に関して知り得た加工情報等を自己若しくは第三者の不正な利益を図る目的で提供し、又は盗用した場合

（加工情報等の取扱い）

第６条　加工情報等の取扱いに当たっては、セキュリティポリシー及び各部局において策定した情報セキュリティポリシー実施手順（以下「実施手順」という。）に準拠し、次の各号に掲げるところによらなければならない。

(1)　保護管理者は、加工情報等の秘匿性等その内容に応じて、当該加工情報等にアクセスする権限を有する職員等とその権限の内容を、当該職員等が業務を行う上で必要な最小限の範囲に限ること。

(2)　アクセス権限を有しない職員等は、加工情報等にアクセスしないこと。

(3)　職員等は、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加工情報等にアクセスしないこと。

(4)　職員等が業務上の目的で加工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、当該加工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、職員等は、保護管理者の指示に従い行うこと。

ア　加工情報等の複製

イ　加工情報等の送信

ウ　加工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

エ　その他加工情報等の適切な管理に支障を及ぼすおそれのある行為

(5)　職員等は、加工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、訂正等を行うこと。

(6)　職員等は、保護管理者の指示に従い、加工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、施錠等を行うこと。

(7)　職員等は、加工情報等又は加工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、当該加工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こと。

(8)　保護管理者は、加工情報等の秘匿性等その内容に応じて、台帳等を整備して、当該加工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こと。

（情報システムにおける安全の確保等）

第７条　情報システムにおける安全の確保等に当たっては、セキュリティポリシー及び実施手順に準拠し、次の各号に掲げる措置を講じなければならない。

(1)　保護管理者は、加工情報等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じるこ

と。

(2)　保護管理者は、前号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じること。

(3)　保護管理者は、加工情報等の秘匿性等その内容に応じて、当該加工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、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じること。

(4)　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じること。

(5)　保護管理者は、加工情報等の秘匿性等その内容及びその量に応じて、当該加工情報等への不適切なアクセスの監視のため、加工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じること。

(6)　保護管理者は、加工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じること。

(7)　保護管理者は、加工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じること。

(8)　保護管理者は、不正プログラムによる加工情報等の漏えい、滅失又は毀損（以下「漏えい等」という。）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。）を講じること。

(9)　職員等は、加工情報等について、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こと。保護管理者は、加工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こと。

(10)　保護管理者は、加工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じること。職員等は、これを踏まえ、その処理する加工情報等について、当該加工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こと。

(11)　保護管理者は、加工情報等の秘匿性等その内容に応じて、当該加工情報等の情報

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じること。

(12)　保護管理者は、加工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を限定するために必要な措置を講じること。

(13)　保護管理者は、端末の盗難又は紛失の防止のため、執務室の施錠等の必要な措置を講じること。

(14)　職員等は、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まないこと。

(15)　職員等は、端末の使用に当たっては、加工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じること。

(16)　保護管理者は、加工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じること。

(17)　保護管理者は、加工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、その保管、複製、廃棄等について必要な措置を講じること。

（情報システム室等の安全管理）

第８条　加工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。）の安全管理に当たっては、セキュリティポリシー及び実施手順に準拠し、次の各号に掲げる措置を講じなければならない。

(1)　保護管理者は、情報システム室等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並びに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並びに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じること。また、加工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、同様の措置を講じること。

(2)　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措置を講じること。

(3)　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じること。

(4)　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じること。

(5)　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じること。

（加工情報等の提供及び業務の委託等）

第９条　保護管理者は、法第 109 条第２項の規定により、法令に基づく場合を除き、利用目的以外の目的のために加工情報等を自ら利用し、又は提供してはならない。

２　保護管理者は、加工情報等の提供及び業務の委託等に当たっては、セキュリティポリシー及び実施手順に準拠し、次の各号に掲げる措置を講じなければならない。

(1)　保護管理者は、法第 109 条第１項及び第 115 条の規定（第 118 条の規定により第 115 条の規定を準用する場合を含む。）により、行政機関等匿名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。）から法第 112 条第２項第７号の規定に基づき当該契約相手方が講じた措置によってもなお行政機関等匿名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。

(2)　行政機関等匿名加工情報の作成に係る業務又は加工情報等の取扱いに係る業務を外部に委託する場合には、加工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、委託先における責任者及び業務従事者の管理並びに実施体制及び加工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、書面で確認するなどの必要な措置を講ずるとともに、契約書に次に掲げる事項を明記すること。

ア　加工情報等に関する秘密保持、目的外利用の禁止等の義務

イ　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

ウ　加工情報等の複製等の制限に関する事項

エ　加工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

オ　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

カ　違反した場合における契約解除及び損害賠償責任その他必要な事項

(3)　加工情報等の取扱いに係る業務を派遣労働者に行わせる場合には、労働者派遣契約書に秘密保持義務等、加工情報等の取扱いに関する事項を明記すること。

(4)　加工情報等の取扱いに係る業務を外部に委託する場合には、委託する加工情報等の秘匿性等その内容に応じて、委託先における加工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こと。

(5)　委託先において、行政機関等匿名加工情報の作成に係る業務又は加工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２号に規定する措置を講じさせるとともに、再委託される業務に係る加工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号に規定する措置を実施すること。加工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。

（被害の拡大防止又は復旧等のために必要な措置）

第10条　安全確保上の問題への対応に当たっては、セキュリティポリシー及び実施手順に準拠し、次の各号に掲げるところによらなければならない。

(1)　役員又は職員等は、加工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は、直ちに当該加工情報等を管理する保護管理者に報告すること。

(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ること。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（職員等に行わせることを含む。）こと。

(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の内容等について報告すること。

(4)　総括保護管理者は、前号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こと。

(5)　総括保護管理者は、事案の内容、経緯、被害状況等について、文部科学省に対し、速やかに情報提供を行うこと。

(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

ること。

(7)　学長又は総括保護管理者は、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、当該事案に係る加工情報等の本人への対応等の措置を講じること。

(8)　前号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、速やかに個人情報保護委員会事務局に情報提供を行うこと。

（監査及び点検の実施）

第 11 条　監査及び点検の実施に当たっては､セキュリティポリシー及び実施手順に準拠し、次の各号に掲げるところによらなければならない。

(1)　監査責任者は、加工情報等の適切な管理を検証するため、第３条から前条までに規定する措置の状況を含む本学における加工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。以下同じ。）を行い、その結果を総括保護管理者に報告すること。

(2)　保護管理者は、各部局等又は各課室における加工情報等の記録媒体、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こと。

(3)　総括保護管理者、保護管理者等は、前２号の監査又は点検の結果等を踏まえ、実効性等の観点から加工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じること。

（個人情報保護委員会事務局への報告）

第 12 条　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９条第２項第１号、第 10 条第３号及び第４号の報告をするとき。

(2)　第 10 条第６号及び第７号の措置を講じたとき。

(3)　契約相手方が国立大学法人高知大学における行政機関等匿名加工情報の提供に関する規則第 15 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。

（苦情処理）

第 13 条　本学は、行政機関等匿名加工情報等の取扱いに関する苦情又は意見の適切かつ迅速な処理に努めなければならない。

（雑則）

第 14 条　この規則に定めるもののほか、本学における加工情報等の適切な管理に関し、必要な事項は、別に定める。

附　則

この規則は、平成 31 年２月 27 日から施行する。

附　則（平成 31 年３月 27 日規則第 100 号）

この規則は、平成 31 年４月１日から施行する。

附　則（令和２年１月 15 日規則第 45 号）

この規則は、令和２年１月 15 日から施行する。

附　則（令和４年４月１日規則第４号）

この規則は、令和４年４月１日から施行する。

附　則（令和５年３月 16 日規則第 88 号）

この規則は、令和５年４月１日から施行する。