

## ○国立大学法人香川大学の保有する個人情報の管理に関する規程

### (趣旨)

第1条 この規程は、国立大学法人香川大学の保有する個人情報の保護に関する規則第26条の規定に基づき、国立大学法人香川大学（以下「大学法人」という。）が保有する個人情報（以下「保有個人情報」という。）を取り扱うに当たって、漏えい、滅失又はき損の防止その他の保有個人情報の適切な管理のために必要な事項を定める。

### (定義)

第2条 この規程における用語の意義は、国立大学法人香川大学の保有する個人情報の保護に関する規則（以下「規則」という。）第2条各号に規定するもののほか、次の各号の掲げるところによる。

- (1) 情報システム 大学法人が行う事業に係る情報を蓄積・処理・伝送するサーバシステム、メインフレームシステム又はネットワーク機器（コンピュータ、これに付随するハードウェア、必要なソフトウェア及びこれらに付随する開発、運用及び保守に係る情報）をいう。
- (2) 情報セキュリティ 保有個人情報の機密性（情報にアクセスすることを許可された者だけがアクセスできることを確実にすること。）、完全性（情報システムが取り扱う情報（情報システムのシステム情報を含む。）、その入出力情報（印字された紙及び磁気的方式等で記録された媒体を含む。）及びこれらが複製された情報処理方法が、正確であること及び完全であることを保護すること。）及び可用性（許可された利用者が、必要なときに情報及び関連財産にアクセスできることを確実にすること。）を維持することをいう。

### (管理体制)

第3条 大学法人に、保有個人情報の適正な管理を行うため、総括保護管理者、保護管理責任者、保護管理者、保護担当者及び監査責任者を置く。

- 2 総括保護管理者は、学長が指名する理事をもって充て、大学法人における保有個人情報の管理に関する業務を総轄する任に当たる。
- 3 保護管理責任者は、別表第1のとおりとし、所掌する組織における保有個人情報の管理に関する業務を統括する任に当たる。
- 4 保護管理者は、別表第2のとおりとし、所掌する組織における保有個人情報の適切な管理を確保する任に当たる。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、

当該情報システムの管理者と連携して、その任に当たる。

- 5 保護担当者は、保護管理者の下にそれぞれ1人又は複数人を置くこととし、保護管理者が当該管理責任を有する範囲内の職員を指名する。指名された保護担当者は、保護管理者を補佐し、保護管理者の保有個人情報の管理に関する事務を担当する。この場合において、教育研究に係る保護管理者は、保護担当者を兼ねることができる。
- 6 監査責任者は、常勤監事をもって充て、大学法人における保有個人情報の管理の状況について監査する任に当たる。

(教育研修)

第4条 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、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、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、情報システムの管理、運用及び情報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、保護管理責任者、保護管理者及び保護担当者に対し、所掌する組織における保有個人情報の適切な管理のための教育研修を実施すること。
- 4 保護管理責任者は、管理責任を有する範囲内の職員に対し、保有個人情報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必要な措置を講じなければならない。

(職員の責務)

第5条 職員は、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）の趣旨に則り、関係法令、規則、この規程等の定め並びに総括保護管理者、保護管理責任者、保護管理者及び保護担当者の指示に従い、保有個人情報を適正かつ適切に管理しなければならない。

(保有個人情報の取扱い)

第6条 保有個人情報の取扱いに当たっては、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、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るものとし、その利用者、利用範囲及び保管場所を明確にすること。
- (2) アクセス権限を有しない職員は、保有個人情報にアクセスしてはならない。また、

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。

- (3) 職員が業務上の目的で保有個人情報を取り扱う場合にあっては、保護管理者は、保有個人情報を複製し、送信し、又は送付する行為、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と。
- (4) 保有個人情報が記録されている媒体の学外への配布及び持出しは、原則として禁止する。ただし、保護管理者の許可を得た場合は、この限りでない。
- (5) 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、保護管理者の指示に従い、訂正、利用の停止、消去等を行うこと。
- (6) 職員は、保護管理者の指示に従い、保有個人情報が記録されている媒体（端末機器及びサーバ機器に内蔵されているものを含む。）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施錠可能で入退室管理ができる保護管理者が管理する区域内のサーバ等記録媒体に保存すること。
- (7) 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が不要となった場合には、保護管理者の指示に従い、媒体の破碎又は当該個人情報の復元及び判読が極めて困難な方法により当該情報を消去し、廃棄を行うこと。
- (8) 保護管理責任者は、保有個人情報の秘匿性等その内容の重要度に応じて個人情報ファイル取扱台帳を作成し、当該保有個人情報の利用及び保管等の取扱いの状況について記録して適切に管理を行うこと。

(情報システムにおける安全性の確保等)

第7条 情報システムにおける保有個人情報（情報システムで取り扱うものに限る。以下この条において同じ。）の安全性の確保等に当たっては、次の各号に掲げる措置等を講じなければならない。

- (1) 保護管理責任者は、保有個人情報の秘匿性等その内容に応じて、パスワード、ICカード、生体情報等（以下「パスワード等」という。）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) 保護管理責任者は、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こと。

- (3) 保護管理責任者は、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こと。
- (4) 保護管理責任者は、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。
- (5) 保護管理責任者は、保有個人情報の秘匿性等その内容及びその量に応じて、当該保有個人情報への不適切なアクセスの監視のため、保有個人情報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こと。
- (6) 保護管理責任者は、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こと。
- (7) 保護管理責任者は、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、ネットワークセキュリティ機器等（ファイアーウォール、ルータ等をいう。）の設定による経路制御等の必要な措置を講ずること。
- (8) 保護管理責任者は、不正プログラムによる保有個人情報の漏えい、滅失又はき損防止のため、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。）を講ずること。
- (9) 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。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こと。
- (10) 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、持出し又は配送するときは、暗号化のために必要な措置を講ずること。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こと。
- (11) 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、滅失又はき損の防止のため、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。

- (12) 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ること。
- (13) 保護管理者は、端末機器の盗難又は紛失防止のため、端末機器の固定又は端末機器設置部屋の施錠等必要な措置を講じること。
- (14) 職員は、保護管理者が必要があると認めるときを除き、保有個人情報が記録された端末機器を外部へ持ち出さないこと。また、外部から持ち込む場合は、情報システムで利用する前にウイルスの有無等を確認すること。
- (15) 職員は、端末機器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じること。
- (16) 職員は、保有個人情報の重要度に応じて、原本との妥当性を確認すること。
- (17) 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すること。
- (18) 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秘匿性等その内容に応じて、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 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。)の安全管理に当たっては、次の各号に掲げる措置を講じなければならない。

- (1) 保護管理責任者は、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及び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じること。また、保有個人情報を記録する媒体を保管するための室がある場合においても、必要があると認めるときは、同様の措置を講じること。
- (2) 保護管理責任者は、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) 保護管理責任者は、情報システム室等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する等、必要な措置を講じること。
- (4) 保護管理責任者は、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の設置等必要な措置を講じること。

- (5) 保護管理責任者は、地震、火災等の災害に備え、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、サーバ等機器の予備電源の確保及び配線の損傷防止等の措置を講じること。

(保有個人情報の学生等の利用)

第9条 学生等（学生、研究生その他大学法人が定める規則等に基づき、大学法人が受け入れる者をいう。以下この条において同じ。）が、保有個人情報を教育、研究、研修、実習、共同研究等（以下「教育研究等」という。）において利用するに当たっては、次の各号に掲げる措置等を講じなければならない。

- (1) 学生、研究生等を指導し、又は共同研究等を行う職員は、当該学生等に保有個人情報を利用させるときは、保護管理者に届け出て、保護管理責任者の許可を得た上でなければ利用させてはならない。
- (2) 保護管理責任者は、保有個人情報を学生等に利用させることを許可するに当たっては、利用する学生等を特定し、当該保有個人情報の利用がその取り扱う業務の目的以内で、大学法人の内部において利用する場合でなければ許可してはならない。
- (3) 第1号に規定する職員は、学生等に保有個人情報を利用させるときは、当該個人情報の不正な利用、複製、提供、漏洩、滅失又はき損に注意をはらい、保護管理者の指示に従い、適切に管理すること。

(保有個人情報の提供及び業務の委託等)

第10条 保有個人情報を外部のものに提供し、又は保有個人情報の取扱いに係る業務（情報システムの保守業務を含む。以下この条において同じ。）を外部のものに委託するに当たっては、次の各号に掲げる措置等を講じなければならない。

- (1) 職員は、保護管理責任者の指示によらなければ保有個人情報を外部のものに提供し、又は学長の指示によらなければ個人情報の取扱業務を外部のものに委託してはならない。
- (2) 保護管理責任者は、保有個人情報を外部のものに提供するときは、提供先における利用目的、利用する業務の根拠法令、利用する記録項目（規則第12条第1項第4号に規定するものをいう。）、記録範囲（規則第12条第1項第5号に規定するものをいう。）、利用形態等及び当該保有個人情報を管理する上において必要とする事項について、書面を取り交わすこと。
- (3) 保護管理責任者は、国の機関、他の独立行政法人等及び地方公共団体（以下「学外機関」という。）に保有個人情報を提供する場合には、必要があると認めるときは、前

号に規定する措置を講じること。

(4) 保護管理責任者は、学外機関以外のものに保有個人情報を提供する場合には、第2号に掲げるもののほか、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、提供前及び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じること。

(5) 学長は、保有個人情報の取扱いに係る業務を外部のもの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者を選定してはならない。また、選定したときは、業務委託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、保有個人情報の取扱いに関する必要な事項を書面で確認すること。

イ 個人情報に関する秘密保持、目的外利用の禁止等の義務

ロ 再委託の制限又は事前承認等委託に係る条件に関する事項

ハ 個人情報の複製等の制限に関する事項

ニ 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

ホ 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

へ 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

(6) 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、年1回以上の定期的検査等により確認すること。

(7) 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、委託先に第5号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、委託先を通じて又は大学法人自らが前号の措置を実施する。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こと。

(8) 学長は、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すること。

(安全確保上の問題への対応)

第11条 保有個人情報の安全確保上の問題への対応に当たっては、次の各号に掲げるところによらなければならない。

(1) 職員は、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

に報告すること。

- (2) 保護管理者は、前号の報告を受けたときは保護管理責任者に報告するとともに、保護管理責任者の指示のもと、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、直ちに行うこと。（職員に行わせることを含む。）
- (3) 保護管理者は、前号に規定する措置とともに事案の発生した経緯、被害状況等を調査し、保護管理責任者に報告すること。ただし、特に重大と認める事案が発生した場合には、保護管理者は直ちに保護管理責任者を通じ、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) 保護管理責任者は、前号の事案が保護管理責任者で処理できないと判断するときは、総括保護管理者に報告すること。
- (5) 総括保護管理者は、前2号の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、経緯及び被害状況等を学長に速やかに報告するとともに、文部科学省に対し、速やかに情報提供を行うこと。学長は、その事案に対して調査が必要と認めるときは、香川大学個人情報保護委員会による調査を命じ、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。
- (6) 総括保護管理者は、第1号の事案が発生し第3号若しくは第4号による報告を受けたとき、又は前号に基づき学長から指示を受けたときは、事案の内容や影響等に応じて、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必要な措置を講じること。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）に情報提供を行うこと。

（監査及び点検の実施）

第12条 保有個人情報の管理の状況についての監査及び点検の実施に当たっては、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、保有個人情報の適切な管理を検証するため、措置の状況を含む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、所掌する組織における自ら管理責任を有する保有個人情報の記録媒体、処理経路、管理方法等について、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、その結果を保護管理責任者を通じ、総括保護管理者に報告するこ

と。

(3) 保護管理責任者及び保護管理者は、第1号に掲げる監査責任者が行う監査に協力すること。

(4) 総括保護管理者、保護管理者等は、監査、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、改善等の措置を講じること。

(文部科学省との連携)

第12条の2 大学法人は、「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、その保有する個人情報の適切な管理を行うこと。

(雑則)

第13条 この規程の実施に関し必要な事項は、部局等の長が別に定める。

2 保護管理責任者は、この規程の実施に関し、必要に応じ所掌する組織内における保有個人情報の管理のための措置を講じなければならない。

3 役員は、保有個人情報を管理するに当たっては、この規程を準用するものとする。

附 則

この規程は、平成17年4月1日から施行する。

附 則(平成18年5月24日)

この規程は、平成18年5月24日から施行する。

ただし、改正後の別表第2は平成17年6月1日から、改正後の第3条は平成17年10月1日から適用する。

附 則(平成19年4月1日)

この規程は、平成19年4月1日から施行する。

附 則(平成20年4月1日)

この規程は、平成20年4月1日から施行する。

附 則(平成23年6月1日)

この規程は、平成23年6月1日から施行し、平成23年4月1日から適用する。

附 則(平成24年4月1日)

この規程は、平成24年4月1日から施行する。

附 則(平成27年4月1日)

この規程は、平成27年4月1日から施行する。

附 則（平成27年9月28日）

この規程は、平成27年9月28日から施行する。

附 則（平成28年4月1日）

この規程は、平成28年4月1日から施行する。

附 則（平成28年9月16日）

この規程は、平成28年9月16日から施行する。

別表第1

部局等	保護管理責任者
部局等（法人本部、医学部、医学部附属病院及び監査室を除く。）	部局等の長
法人本部（国際グループを除く。）	部長
国際グループ	国立大学法人香川大学の業務組織に関する規程第7条に定める担当理事等
創造工学部（仮称）設置準備事務室	総務部長
医学部	医学部長 事務部長
医学部附属病院	附属病院長
監査室	常勤監事

別表第2

部局等	保護管理者	
部局等（法人本部、監査室、医学部、図書館、博物館、各機構、微細構造デバイス統合研究センター、医学部附属病院、学部附属教育研究施設及び教育学部附属学校を除く。）	教育研究 事務	部局等の長が指名する者 リーダー、事務課長
法人本部	事務	リーダー
創造工学部（仮称）設置準備事務室	事務	室長
監査室	事務	室長
医学部	教育研究 事務	医学部長が指名する者 課長、室長
医学部附属病院	教育研究、診療	附属病院長が指名する者
図書館、博物館	教育研究、事務	情報図書グループリーダー
各機構	教育研究、事務	研究協力グループリーダー
微細構造デバイス統合研究センター	教育研究、事務	研究協力グループリーダー

学部附属教育研究施設	教育研究	学部附属教育研究施設の長
	事務	事務課長
教育学部附属学校	教育研究	校長、園長
	事務	事務課長

※広報室の事務にあつては、副室長とする。