（別紙２）

|  |  |
| --- | --- |
| 申出者氏名 |  |
| 所属機関 |  |
| 匿名データの管理方法等（当てはまるものにチェックを入れること） | |
| 1. 匿名データの利用場所  * 匿名データの利用場所は国内であること。 * 保管する場所は、あらかじめ申出書に記載された施錠可能な物理的スペースに限定されていること。  1. 匿名データの利用方法  * 匿名データを複写した情報システムは、インターネット等の外部ネットワークに接続しないこと。  1. 匿名データの利用者  * 匿名データはあらかじめ申出書に記載された利用者のみが利用すること。  1. 匿名データの安全管理  * 貸与される匿名データに加え、作業等によって生成される匿名データを含む中間生成物及び廃棄物についても、漏えい等の事故を防止するために適正な管理が行われること。  1. 匿名データの管理者  * ガイドライン第3の1の規定に基づき行われる高等教育の発展に資することを目的として利用する場合、匿名データは教員（教育責任者）が保管・管理し、利用者たる学生には保管・管理させないこと。また、教育責任者は、利用者たる学生に対し、あらかじめ利用に必要な教育（制度、遵守事項、不適切利用への措置等）を行うこと   ⑥ 所属機関が具備すべき条件  (ⅰ)情報の安全管理   * (a)匿名データを取り扱う情報システムの安全管理に関する方針を策定していること。 * (b)貸与される匿名データについても、適正な管理を行うことができること。   (ⅱ)情報セキュリティマネジメントシステムの実践   * (a)情報システムで扱う情報を全てリストアップしていること。 * (b)リストアップした情報を、安全管理上の重要度に応じて分類を行い、常に最新の状態を維持   　していること。   * (c)情報システムの安全管理者は、上記のリストを必要に応じて速やかに確認できる状態で管理   　しておくこと。   * (d)リストアップした情報を、リスク分析し、その結果得られた脅威に対して適切な対策を行っ   　ていること。  (ⅲ)組織的安全管理対策の実施   * (a)情報システム運用責任者の設置及び担当者（システム管理者を含む）の限定を行うこと。   + (b)匿名データを参照可能な場所においては、来訪者の入退管理を適切に行うこと。   + (c)情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。   + (d)匿名データに係る情報の取扱いを委託する場合、委託契約において安全管理に関する条項を   　含めること。   * + (e)運用管理規程において次の内容を定めること。   ・理念（基本方針と管理目的の表明）  ・利用者等の体制  ・契約書・マニュアル等の文書の管理  ・リスクに対する予防、発生時の対応の方法  ・機器を用いる場合は機器の管理  ・匿名データと同程度の安全管理が必要な情報の記録媒体の管理方法  ・監査  ・苦情・質問の受付窓口  (ⅳ)人的安全対策の措置   * + (a)利用者が所属する組織の管理者は、匿名データに係る情報の安全管理に関する施策が適切に   　実施されるよう必要な措置を講じるとともに、その実施状況を監督すること。   * (b)利用者が所属する組織の事務、運用等を外部の事業者に委託する場合は、これらの機関の内   　部における適切な情報の安全管理が行われるよう、罰則のある就業規則等で裏付けられた守  　秘・非開示契約の締結その他必要な措置を行うこと。   * (c)プログラムの異常等で、保存データを救済する必要があるとき等、やむを得ない事情で外部   　の保守要員が匿名データに係る情報にアクセスする場合は、罰則のある就業規則等で裏付けら  れた守秘・非開示契約等の締結その他の秘密保持の対策を行うこと。  (ⅴ)情報の破棄の手順等の設定   * (a)匿名データに係る情報の破棄の手順を定めること。手順には破棄を行う条件、破棄を行うこ   とができる従業者の特定、具体的な破棄の方法を含めること。   * (b)匿名データを利用又は保存する情報処理機器自体を破棄する場合、必ず専門的な知識を有す   　る者が行うこととし、残存し、読み出し可能な情報がないことを確認すること。   * (c)外部保存を受託する機関に破棄を委託した場合は、更に委託する利用者等が確実に匿名デー   タに係る情報の破棄が行われたことを確認すること。  ⑦ 匿名データの利用に際し具備すべき条件  (ⅰ)物理的安全対策   * + (a)匿名データが保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。   + (b)匿名データを参照できる端末が設置されている区画は、利用時間帯以外は施錠する等、運用   管理規程に基づき許可された者以外立ち入ることができない対策を講じること。   * + (c)匿名データの物理的保存を行っている区画への入退管理を実施すること。例えば、以下のこ   とを実施すること。  ・入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録す  る。  ・入退者の記録を定期的にチェックし、妥当性を確認する。   * (d)匿名データが保存されている端末等の重要な機器に盗難防止用チェーンを設置すること。 * (e)窃視防止の対策を実施すること。   (ⅱ)技術的安全対策   * + (a)匿名データを利用する情報システムへのアクセスにおける利用者の識別と認証を行うこと。   + (b)上記(a)の利用者の識別・認証にユーザＩＤとパスワードの組合せを用いる場合には、それら   の情報を、本人しか知り得ない状態に保つよう対策を行うこと。   * + (c)利用者が匿名データを利用する情報システム端末から長時間、離席する際に、あらかじめ認   められた利用者以外の者が利用するおそれがある場合には、クリアスクリーン等の防止策を講  じること。   * + (d)匿名データを利用する情報システムへのアクセスの記録及び定期的なログの確認を行うこ   と。アクセスの記録は少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作  した利用者が特定できること。   * + (e)匿名データを利用する情報システムには、アクセス記録機能を備えること。（アクセス記録機   能を備えていない場合には、業務日誌等で操作の記録（操作者及び操作内容）を行うこと。）   * + (f)匿名データを利用する情報システムにアクセスログへのアクセス制限を行い、アクセスログ   の不当な削除、改ざん、追加等を防止する対策を講じること。   * + (g)上記(f)のアクセスの記録に用いる時刻情報は信頼できるものであること。   + (h)原則として、匿名データを利用する情報システムには、適切に管理されていないメディアを   接続しないこと。また、匿名データを利用する情報システムにメディアを接続する場合には、  ウイルスチェック等の検疫を行うこと。   * + (i)匿名データが複写された情報システムが複数の者によって利用され、パスワードを利用者識   別に使用する場合には、当該システム内のパスワードファイルでパスワードは必ず暗号化さ  れ、適切な手法で管理及び運用が行われること。   * + (j)匿名データが複写された情報システムが複数の者によって利用され、パスワードを利用者識   別に使用する場合には、当該システム内のパスワードファイルでパスワードは必ず暗号化さ  れ、適切な手法で管理及び運用が行われること。   * + (k)匿名データの利用の終了後には、情報システム内に記録された匿名データに関する情報及び   中間生成物を消去することに加え、消去後に当該機器を外部ネットワークに接続する際にはあ  らかじめコンピュータウイルス等の有害ソフトウェアがないか検索し、ファイアーウォールを  導入し、適切なアクセス制御を実施するなど、安全対策に十分配慮すること。  (ⅲ)情報及び情報機器の持ち出しについて   * 貸与された匿名データの情報の利用、管理及び保管は、申出書に記載された場所でのみ行うこと。ただし、外部委託や共同研究の場合など、やむを得ず、利用者間で最小限の範囲で中間生成物等の受渡しを行う場合には、運用管理規程において情報及び情報機器の持ち出しに関する方針、管理方法を定めるなど、情報漏えいを防止するための適切な措置を講じること。 | |