様式１－２

利用者氏名

所属機関名

|  |
| --- |
| 個票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組織的管理措置**   * + （ⅰ）所属機関が、個人情報保護に関する方針及び個人情報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。   + （ⅱ）所属機関が、情報セキュリティマネジメントシステムを実践していること。具体的には、情報システムで扱う情報を全てリストアップした上で、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するとともに、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）所属機関が、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）の限定を行い、その権限及び責務並びに業務について、明確化を図っていること。また、所属機関の管理者が、個人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ずるとともにその実施状況を監督すること。   + （ⅳ）所属機関が、個人情報が参照可能な場所においては、来訪者の記録・識別、入退の制限等の入退管理を定めること。   + （ⅴ）所属機関が、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。   + （ⅵ）所属機関が、情報システムに関する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及び発生時の対応の方法  ・機器を用いる場合は機器及び記録媒体の管理方法   * （ⅶ）所属機関が、個人情報保護方針の中で把握した情報種別ごとに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。   **②人的管理措置**   * + （ⅰ）個票データの適正な取扱いについての理解と関係規定の遵守の徹底が図られるよう、利用者に対して必要な教育が行われていること。   + （ⅱ）研究者、公的機関に所属する常勤の役職員又は教育責任者以外の者が利用者に含まれている場合、当該者に個票データの保管及び管理をさせないようにすること。   **③物理的管理措置**   * + （ⅰ）個票データの利用、保管及び管理場所が、申出書に記載された施錠可能な物理的な場所（日本国内）に限定されていること。   ただし、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その持ち出しに関する方針、管理方法を定めるなど、情報漏えい防止のための適切な措置を講ずること。   * + （ⅱ）個票データの利用、保管及び管理場所には、第三者の無断立入りを防ぐ対策を講じると共に、入退管理を実施すること。   + （ⅲ）個票データが保存されている端末等の重要な機器について、盗難防止用のチェーンを設置するなど、盗難防止のための措置を講ずること。   + （ⅳ)個票データが保存されている端末等の重要な機器を破棄する場合、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。   **④技術的管理措置**   * + （ⅰ）個票データは、あらかじめ申出書に記載された利用者のみが使用すること。個票データにアクセス可能な者が申出書に記載された利用者に限定されるよう、個票データを利用、保管及び管理する情報システムに識別及び主体認証、スクリーンロック等の不正操作対策を講ずること。   + （ⅱ）個票データを利用、保管及び管理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い、個票データの不正利用の有無の確認措置を講ずること。   + （ⅲ）個票データの利用、保管及び管理に際して、インターネット等の外部ネットワークに接続している場合、不正アクセス行為（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第二条第四項に規定する不正アクセス行為をいう。）を防止するため、適切な措置を講ずること。   + （ⅳ）個票データを利用、保管及び管理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、個票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措置を講ずること。 |