（別紙１）

|  |  |
| --- | --- |
| 申出者氏名 |  |
| 所属機関 |  |
| 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. 個票データの利用場所  * 個票データの利用場所は国内であること。 * 保管・管理する場所は、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おり、原則として持ち出されないこと。  1. 個票データの利用方法  * 個票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. 個票データの利用者  * 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利用すること。  1. 個票データの安全管理  * 個票データについては、個人情報を含む情報の安全管理と同等の措置が講じられていること。   ⑤所属機関が具備すべき条件  (ⅰ)個人情報の保護   * (a)個人情報保護に関する方針を策定し、公開していること。 * (b)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。 * (c)貸与される個票データについても、当該方針に沿った対応を行うこと。   (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)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。   * + (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)個人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  ・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、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   う措置するとともにその実施状況を監督する必要があり、以下の措置をとること。  ・法令上の守秘義務のある者以外を事務職員等として採用するに当たっては、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。  ・定期的に従業者に対し個人情報の安全管理に関する教育訓練を行うこと。  ・従業者の退職後の個人情報保護規程を定めること。   * (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   部における適切な個人情報保護が行われるように、以下の措置を行うこと。  ・受託する事業者に対する包括的な罰則を定めた就業規則等で裏付けられた守秘・非開示契約等を締結すること。  ・保守作業等の情報システムに直接アクセスする際には、作業者・作業内容・作業結果の確認を行うこと。  ・清掃等の直接情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。  ・委託事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託事業者と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること。   * (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   の保守要員が個人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)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。   * (b)個票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情報の破   棄が行われたことを確認すること。  (ⅵ)運用管理   * ガイドライン第6の2（4）で示す個人情報の取扱いについて、申出者が対応を行っていると申し出た事項が適切に運用管理規程等に含められていること。   ⑥個票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)個票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)個票データを参照できる区画には、利用者以外の者の無断立入りを防ぐ対策を講じること。   また、個票データを参照できる端末が設置されている区画は、施錠等、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)個票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)個票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)個票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)利用者が個票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)個票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)個票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)個票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、個票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、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を行うこと。   * + (i)個票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)個票データの保存・利用に際しては、インターネット等の外部ネットワークに接続した情報   システムを使用しないこと。   * + (k)個票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個票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   * + 貸与された個票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。 | |