様式11

|  |  |
| --- | --- |
| ＯＲＩＯＮデータの管理状況報告書    　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　令和　　年　　月　　日  大阪府知事　○　○　○　○　　様  申請者　　所属機関名  役職名  氏名　　　　　 　　　　 　　印  （連絡先住所等）  〒    　　　　　　　　　　　　　　　　　　　　　　　　　 電話番号  E-mail  令和　年　月　日付で提供を受けたＯＲＩＯＮデータについて、その管理状況を下記のとおり検査しましたので、その旨報告いたします。  記 | |
| ＯＲＩＯＮデータを用いて行う研究の名称 |  |
| 検査年月日 | 令和　　年　　月　　日 |
| 検査実施者 |  |
| 検査場所 |  |
| 検査状況 | １　利用者の範囲は適正か。  ２　管理方法は適正か。（※別紙の該当するものにチェックする。）  □　その他（　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　） |
| 検査結果(所見) |  |

備考

用紙の大きさは、日本工業規格Ａ４とすること。

様式11（別紙）

|  |
| --- |
| 【管理方法等（当てはまるものに✔を入れること。）】　＊添付書類が必要なもの　☆添付写真が必要なもの　※提出を求める可能性のあるもの  ①基本的な事項  □ⅰ）ＯＲＩＯＮデータの利用場所は国内であること。  □ⅱ）ＯＲＩＯＮデータを複写したＰＣ等を利用、管理及び保管する場所は、あらかじめ☆申請のあった施錠可能な物理的な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。  □ⅲ）ＯＲＩＯＮデータを複写したＰＣ等は、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。  □ⅳ）提供されたＯＲＩＯＮデータは、あらかじめ申請のあった利用者のみが利用し、その他の者への譲渡、貸与又は他の情報との交換等を行わないこと。  □ⅴ）提供するＯＲＩＯＮデータは全体として個人情報に準じた取り扱いを徹底する観点から、ＯＲＩＯＮデータの利用、保護及び管理について、ガイドライン「６　情報システムの基本的な安全管理」等に定められた措置に準じた措置として、以下②及び③に規定する当該ガイドライン中に示された個人情報を含む、情報の安全管理と同等の措置が講じられていること。    ②ＯＲＩＯＮデータの利用に限らず所属機関が一般的に具備すべき条件（必ずしも所属機関全体で具備する必要はなく、部又は課等、申請者の利用形態を勘案して適切な単位で対応すること）。  ⅰ）個人情報保護方針の策定・公開  □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ＰＣ等の安全管理に関する方針を策定していること。  □c）提供されるＯＲＩＯＮデータについても当該方針に従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（ＩＳＭＳ）の実践（必ずしもＩＳＭＳ適合性評価制度における認証の取得を求めるものではない。）  □a）ＰＣ等で扱う情報をすべ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）このリストはＰＣ等の安全管理者が必要に応じて速やかに確認できる状態で管理していること。  □d）リストアップした情報に対してリスク分析を実施していること。  □e）この分析の結果から得られた脅威に対して、申請書に記載した「ＯＲＩＯＮデータの利用場所、保管場所及び管理方法」において対策を行っていること。  ⅲ）組織的安全管理対策（体制、運用管理規程）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。ただし所属機関が小規模な場合において役割が自明の場合は、明確な規程等を定めなくとも良い。  □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、入退を制限する等の入退管理を定めること。  □c）ＰＣ等へのアクセス制限、記録、点検等を定めた＊アクセス管理規程等を作成すること。  □d）個人情報の取り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）運用管理規程等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（役割分担を明記）  ・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  ・個人情報の記録媒体の管理（保管・授受等）の方法  ・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、その実施状況を検査する必要があり、以下の措置を行うこと。  ・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あたっては、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＊個人情報保護規程等を定めること。  □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契約を締結すること。  ・保守作業等でＰＣ等に直接アクセスする作業の際には、作業者・作業内容・作業結果の確認し、記録を残すこと。  ・清掃等で直接ＰＣ等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い、記録を残すこと。  ・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や、やむをえ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）ＰＣ等を破棄する場合、必ず専門的な知識を有するものが行うこととし、残存し、読み出し可能な情報がないことを確認し、記録を残すこと。  □c）外部保存を受託する機関に破棄を委託した場合はガイドライン「６．６人的安全対策 （2）事務取扱委託業者の監督及び守秘義務契約」に準じ、さらに委託する所属機関等が確実に情報の破棄が行われたことを確認し、記録を残すこと。  ⅵ）運用管理について  □ＯＲＩＯＮデータを含めた個人情報の取り扱いについて、申請書に記載した「ＯＲＩＯＮデータの利用場所、保管場所及び管理方法」に規定された内容のうち申請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まれていること。  ③ＯＲＩＯＮデータの利用に際し具備すべき条件（必ずしも所属機関全体で具備する必要はなく、部又は課等、申請者の利用形態を勘案して適切な単位で対応すること）。  ⅰ）物理的安全対策  　　　ＯＲＩＯＮデータが保存されているＰＣ等及びその設置・保存場所に、以下の安全対策を講じること。ただし、本対策項目と同等レベルの他の取り得る手段がある場合はこの限りではない。  □a）ＯＲＩＯＮデータが保存されているＰＣ等  　　ｱ）☆盗難防止チェーンを設置すること。  　　ｲ）窃視防止の対策を実施すること。  □b）ＯＲＩＯＮデータが保存されているＰＣ等の設置・保存場所  　ｱ）施錠を行うこと。  　ｲ）業務時間帯以外は施錠等、運用管理規程等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。  ｳ）入退管理を実施することに加え、以下のことも実施すること。  ・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。  ⅱ）技術的安全対策  □a）ＯＲＩＯＮデータを利用するＰＣ等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 とパスワードの組み合わ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ＯＲＩＯＮデータを利用するＰＣ等の端末から長時間、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恐れがある場合には、クリアスクリーン等の防止策を講じること。  □d）ＯＲＩＯＮデータを利用するＰＣ等への※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、並びにログイン中に操作した利用者が特定できること。なお、ＯＲＩＯＮデータを利用するＰＣ等にアクセス記録機能がない場合は※業務日誌等で操作の記録（操作者及び操作内容）を必ず行い、かつ、記録を残すこと。  □e）ＯＲＩＯＮデータを利用するＰＣ等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。  □f）上記e）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。  □g）ＯＲＩＯＮデータを利用するＰＣ等には、適切に管理されているメディア（例：過去数ヶ月以内にウイルスチェックが行われていること、推定しにくいパスワードによって暗号化されていること）を接続すること。適切に管理されていないと考えられるメディアを使用する際は、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持を行うこと。  □h）パスワードを利用者識別に使用する場合  システム管理者は以下の事項に留意すること。  ・ＯＲＩＯＮデータが複写されたＰＣ等が複数の者によって利用される場合にあっては、ＰＣ等のパスワードファイルでパスワードは必ず暗号化(可能なら不可逆変換が望ましい。)され、適切な手法で管理及び運用が行われること(利用者識別にＩＣカード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理規程等にて定めること)。  ・利用者がパスワードを忘れたり、盗用されたりする恐れがある場合で、システム管理者がパスワードを変更する場合には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載(本人確認を行った書類等のコピーを添付)し、本人しか知りえない方法で再登録を実施すること。  ・システム管理者であっても、利用者のパスワードを推定できる手段を防止すること。(設定ファイルにパスワードが記載される等があってはならない。)  また、利用者は以下の事項に留意すること。  ・パスワードは定期的に変更し（最長でも2 ヶ月以内）、極端に短い文字列を使用しないこと。英数字、記号を混在させた8 文字以上の文字列が望ましい。  ・類推しやすいパスワードを使用しないこと。  □i）ＯＲＩＯＮ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ＰＣ等を使用しないこと。  □j) ＯＲＩＯＮデータの消去後に当該ＰＣ等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ーウイルス等の有害ソフトウェアが無いか検索し、ファイアウォールを導入するなど、安全対策に十分配意すること。  ⅲ）情報及びＰＣ等の持ち出しについて  提供されたＯＲＩＯＮデータの利用、管理及び保管は、事前に申請した場所でのみ行うこととし、外部への持ち出しは行わないこと。ただし、共同研究の場合など、やむをえず、あらかじめ申請した利用者の間で、最小限の範囲で中間生成物等の受け渡しを行う場合には、利用者が以下の措置を講じており、ＯＲＩＯＮデータの受け渡し方法に準用していること。  □a）組織としてリスク分析を実施し、情報及びＰＣ等の持ち出しに関する方針を＊運用管理規程等で定めること。  □b）運用管理規程等には、持ち出した情報及びＰＣ等の管理方法を定めること。  □c）情報を格納したＰＣ等の盗難、紛失時の対応を運用管理規程等に定めること。  □d）あらかじめ運用管理規程等で定めたＯＲＩＯＮデータの盗難、紛失時の対応を利用者等に周知徹底し、教育を行うこと。  □e）利用者は、ＯＲＩＯＮデータが格納されたＰＣ等の所在を、台帳等を用いて把握すること。  □f）ＯＲＩＯＮデータの持ち出しに利用するＰＣ等に対して起動パスワードを設定すること。設定にあたっては推定しやすいパスワード等の利用を避け、定期的にパスワードを変更する等の措置を行うこと。  □g）盗難、置き忘れ等に対応する措置として、ＯＲＩＯＮデータに対して暗号化や、アクセスパスワードを設定する等、容易に内容を読み取られないようにすること。  □h）ＯＲＩＯＮデータが保存されたＰＣ等を、他のＰＣ等と接続する場合は、コンピューターウイルス対策ソフトの導入等を行い、情報漏えい、改ざん等の対象にならないような対策を施すこと。  □i）ＯＲＩＯＮデータの持ち出しについて個人保有のＰＣ等を使用する場合にあっても、上記のf）、g）、h）と同様の要件を遵守させること。 |