（別紙様式３）利活用申出書Ⅳ

|  |
| --- |
| 【利活用情報の管理方法】以下、括弧内の単位ごとに（１）から（５）について記載すること（複数の場合は、利活用申出の単位ごとに分けて別紙としてそれぞれ添付すること）（１）基本的な事項（１利活用申出の単位ごと）（２）利活用者の所属する組織が一般的に具備すべき条件（利活用申出書に記載された利活用者の１組織単位ごと）（３）オンサイトセンターに設置された専用端末の利用に当たって具備すべき条件（利活用申出書に記載された利活用者の１組織単位ごと）（４）MID-NET接続環境において分析用データセット等を取り扱う際に具備すべき条件（５）データセンターから移動した統計情報の利活用に当たって具備すべき条件（利活用申出書に記載された利活用者の１組織単位ごと）※　１組織単位ごとについて、利活用の一部を委託する場合は、委託先の運用・管理体制の状況も含めて１組織単位として記載するものとする |
| [ ] 　下記の（１）～（５）の内容について遵守する。ただし、各項目のうち該当しない（措置を講じる必要がない）、又は各項目に記載のとおり対応できない場合には、同等以上の代替措置を講じる。 |
| ※　各項目のうち該当しない（措置を講じる必要がない）、又は対応できていない項目は、□を■に変更し、その内容（変更した項目の理由、その他の備考）を各項目の右欄に明記すること。 |
| **（１）基本的な事項** |
| [ ] 　ⅰ)　データセンターから外部へ移動させた統計情報は、利活用契約者の責任の下、利活用契約者、MID-NET利活用者及び統計情報利活用者のみが利用することとし、その他の者へ譲渡、貸与又は他の情報との交換等を行わないこと。 |  |
| [ ] 　ⅱ)　データセンターから移動した統計情報の取扱いについて、「医療情報システムの安全管理に関するガイドライン」の「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、次の（２）及び（５）（MID-NET接続環境において分析用データセット等を取り扱う場合には④も含む）に規定する情報の安全管理と同等の措置が講じられていること。なお、利活用者は、ここに規定されている事項以外についても上記ガイドラインの趣旨を十分に理解した上で、適切なセキュリティ対策を講じるよう努めなければならない。 |  |
| ⅲ)　 データセンターを利用する、又はデータセンターから移動した統計情報を取り扱うMID-NET利活用者及び統計情報利活用者について、次の人的安全対策を講じなければならない。 |  |
| [ ] 　a) 利活用契約者は、安全管理に関する措置が適切に実施されるようにするとともに、その実施状況を監督する必要があり、次に掲げる措置を講じること。・ MID-NET利活用者及び統計情報利活用者について、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。・ MID-NET利活用者及び統計情報利活用者に対して、定期的に個人情報等の安全管理に関する教育訓練を行うこと。・ MID-NET利活用者及び統計情報利活用者について、退職後の守秘・非開示及び個人情報保護に関する規程を定めること。 |  |
| [ ] 　b) 利活用契約者は、利活用の一部を外部の事業者に委託する場合は、適切な情報管理が行われるように、次に掲げる措置を講じること。・ 受託事業者における包括的な罰則を定めた就業規則等で守秘契約が裏付けられることを確認した上で、守秘契約を締結すること。・ 情報を取り扱うシステムに直接アクセスする作業に当たっては、作業者、作業内容及び作業結果の確認を行うこと。・ 清掃作業等の情報を取り扱うシステムに直接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て、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。 |  |
| **（２）利活用者の所属する組織が一般的に具備すべき条件（必ずしも組織全体で具備する必要はなく、部、課又は研究室等、利活用者の状況を勘案して適切な単位で対応すること。）** |
| ⅰ)　個人情報保護に関する方針の策定・公開 |
| [ ] 　a) 個人情報保護に関する方針を策定し、かつ公開していること。 |  |
| [ ] 　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。 |  |
| 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は求めない。） |
| [ ] 　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について、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) 上記a) のリストは、情報システム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) 当該分析により得られた脅威に対して、利活用情報の管理方法に規定する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。 |  |
| [ ] 　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) 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) データセンターから移動した統計情報の取扱いを外部委託する場合、委託契約において安全管理に関する情報を含めること。 |  |
| [ ] 　e) 運用管理規程等において、次に掲げる内容を定めること。・ 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・ 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)　運用管理 |
| [ ] 　 データセンターから移動した統計情報の取扱いについて、利活用情報の管理方法において規定された内容のうち、利活用契約者が対応を行うこととした事項が適切に運用管理規程等に含められていること。 |  |
| **（３）オンサイトセンターに設置された専用端末の利用に当たって具備すべき条件** |
| ⅰ)　技術的安全対策 |
| [ ] 　a) 機構のシステム管理者から発行されたMID-NETのシステムの利用に必要なユーザID及びパスワードについて、ユーザID及びパスワード並びにそれらの組合せを本人しか知り得ない状態に保つよう対策を行うこと。 |  |
| [ ] 　b) 機構のシステム管理者から発行されたMID-NETのシステムの利用に必要なユーザID及びパスワードについて、MID-NET利活用者は次の事項に留意すること。・ パスワードは機構の定める規程に基づき、定期的に変更すること。・ 類推しやすいパスワードを使用しないこと。 |  |
| **（４）MID-NET接続環境において分析用データセット等を取り扱う際に具備すべき条件****※ NCDAデータを利用する利活用については、MID-NET接続環境をご利用いただけません。** |
| ⅰ)　 物理的安全対策 |
| [ ] 　a) 製造販売後調査又はこの他製造販売業者等が機構と相談して実施している調査（以下、「対象調査」という。）を実施する医薬品の製造販売業者の役職員又は対象調査の実施に関する業務の委託を受けた者の役職員のみが入室できる施錠管理した領域内でデータセンターへのアクセスを行うこと。 |  |
| ☐　b) データセンターにアクセスする端末について、覗き見防止の対策を実施すること。 |  |
| ⅱ)　 技術的安全対策 |  |
| [ ] 　a) 機構のシステム管理者から発行されたデータセンターの利用に必要なユーザID及びパスワードについて、ユーザID及びパスワード並びにそれらの組合せを本人しか知り得ない状態に保つよう対策を行うこと。 |  |
| [ ] 　b) 機構のシステム管理者から発行されたデータセンターの利用に必要なユーザID及びパスワードについて、MID-NET利活用者は次の事項に留意すること。* パスワードは機構の定める規程に基づき、定期的に変更すること。
* 類推しやすいパスワードを使用しないこと。
 |  |
| ⅲ)　 人的安全対策の措置 |
| [ ] 　a) 利活用が行われている時間帯に入室できる者は、緊急時を除き、対象調査を実施する医薬品の製造販売業者の担当役職員、対象調査の実施に関する業務の委託を受けた者の担当役職員に限定すること。 |  |
| [ ] 　b) 緊急時を除き、（４）ⅲ）a）以外の役職員が入室する必要がある場合には、（４）ⅲ）a）に示す担当役職員が同席すること。 |  |
| [ ] 　c) 緊急時を除き、データセンターにアクセスできる者は、ユーザID等を付与したものに限定すること。 |  |
| [ ] 　d) MID-NETの利活用者は、データセンターにアクセスしている画面は、携帯電話、デジタルカメラ等の電子機器類による撮影及び録画を行わないとともに、画面の覗き見防止等情報管理を徹底すること。また、利活用契約者は、MID-NETの利活用者に対して、その旨教育訓練を実施すること。 |  |
| **（５）データセンターから移動した統計情報の利活用に当たって具備すべき条件（必ずしも組織全体で具備する必要はなく、部、課又は研究室等、利活用者の状況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 |
| [ ] 　a) データセンターから移動した統計情報を利活用者自らが適切に管理する機器（利活用者が所属する組織が管理する場合を含む）に保存する場合には、当該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。クラウドサービスを利用する場合には、あらかじめ盗難や紛失防止も含めた物理的な保護及び措置が講じられていることを確認したうえで、統計情報を保存すること。 |  |
| [ ] 　b) データセンターから移動した統計情報を取り扱う又は閲覧可能な端末が設置されている区画について、業務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が立ち入ることができない対策を講じること。ただし、以下の例のように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にはこの限りではない。・ 業務時間帯以外に端末を施錠できる場所に保管する。・ 盗難防止対策と盗難・紛失時におけるセキュリティ対策を講じる。・ 業務時間帯以外に端末を第三者が触れないように保管する。 |  |
| [ ] 　c) データセンターから移動した統計情報を利活用者自らが管理する機器（利活用者が所属する組織が管理する場合を含む）に物理的保存を行う場合、当該機器が設置されている区画への入退管理を実施すること。クラウドサービスを利用する場合には、a)における確認を実施したうえで統計情報を保存すること。 |  |
| [ ] 　d) データセンターから移動した統計情報が存在する端末等の重要な機器に対して、盗難防止用チェーンを設置すること。統計情報を取り扱う又は閲覧する端末に可搬型端末を用いる場合には、盗難防止用チェーンの設置に代えて、端末を操作しない間は端末を施錠できる場所に保管する、又は、端末に統計情報を保存しないことでも良い。 |  |
| [ ] 　e) データセンターから移動した統計情報を閲覧可能な端末について、覗き見防止の対策を実施すること。 |  |
| ⅱ)　技術的安全対策 |
| [ ] 　a) データセンターから移動した統計情報を取り扱うシステムについて、当該システムへのアクセスにおける利活用者の識別及び認証を行うこと。 |  |
| [ ] 　b) 上記a) の利活用者の識別又は認証に対して、ユーザID及びパスワードの組合せを用いる場合には、ユーザID及びパスワード並びにそれらの組合せ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) 利活用者がデータセンターから移動した統計情報を取り扱うシステムの端末から長時間、離席する際に、あらかじめ認められた利活用者以外の者が閲覧又は操作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) データセンターから移動した統計情報を取り扱うシステムについて、動作確認等には当該統計情報を用いないこと。 |  |
| [ ] 　e) データセンターから移動した統計情報について、利用者に応じたアクセス権限の管理を行うこと。また、運用管理規程において、当該アクセス権限の見直しを適切に行うことを規定すること。 |  |
| [ ] 　f) データセンターから移動した統計情報を取り扱うシステムについて、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活用者のログイン時刻及びアクセス時間並びにログイン中に操作した利活用者が特定できること。 |  |
| [ ] 　g) データセンターから移動した統計情報を取り扱うシステムについて、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、改ざん及び追加等の行為を防止する対策を講じること。 |  |
| [ ] 　h) 上記g) 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。 |  |
| [ ] 　i) 原則として、データセンターから移動した統計情報を取り扱うシステムには、適切に管理されていないメディアを接続しないこと。ただし、システム構築時、やむをえず適切に管理されていないメディアを使用する場合、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認すること。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には、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講じること。また、その対策の有効性・安全性の確認・維持を行うこと。 |  |
| [ ] 　j） データセンターから移動した統計情報を取り扱うシステムについて、パスワードを利活用者の識別に用いる場合には、当該システムの管理者は次に掲げる事項に留意すること。・ 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（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にて定めること。）。・ 利活用者がパスワードを忘れたり、盗用されたりするおそれがある場合に、システム管理者がパスワードを変更する場合は、利活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、本人以外が知り得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、利活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の状況は許容されない）。 |  |
| [ ] 　k) データセンターから移動した統計情報を取り扱うシステムについて、パスワードを利活用者の識別に用いる場合には、利活用者は次に掲げる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か月以内。ただし、２要素認証又は端末操作を行う区画への入場時・端末利用時を含め２要素以上の認証を採用している場合を除く）、英字（大文字）、英字（小文字）、数字、記号から３種以上を混在させた８文字以上の文字列とすること。・ 類推しやすいパスワードを使用しないこと、かつ類似のパスワードを繰り返し使用しないこと。 |  |
| [ ] 　l) データセンターから移動した統計情報を取り扱うシステムにおいて、無線LANを利用する場合には、システム管理者は次に掲げる事項に留意すること。・ 当該システムの利用者以外に無線LANの利用を特定されないようにすること。・ 不正アクセスの対策を施すこと（少なくともSSIDやMACアドレスによるアクセス制限を行うこと）。・ 不正な情報の取得を防止すること。・ 無線LANの適用に関しては、総務省発行の「一般利用者が安心して無線LANを利用するために」や「企業等が安心して無線LAN を導入・運用するために」を参考にすること。 |  |
| [ ] 　m) テレワークを実施する場合には、端末の作業環境内に仮想的に安全管理された環境をVPN 技術と組み合わせて実現する仮想デスクトップのような技術を用いるとともに、外部からのアクセスに用いる機器の安全管理の運用管理規程を設定すること。なお、外部媒体への記録やアプリケーションのインストールなどが制限された、利活用者が所属する組織が管理する端末をVPN 技術と組み合わせて使用することに加え、運用管理規程の整備及び必要な教育訓練の実施により当該端末への統計情報の保存が行われないよう運用することにより、仮想デスクトップ技術の使用に代えることも可能とする。 |  |
| ⅲ)　人的安全対策の措置 |
| [ ] 　a) データセンターから移動した統計情報を取り扱う情報システムについて、プログラムの異常等により保存データを救済する必要があるとき等のやむを得ない事情で、外部の保守要員が当該統計情報にアクセスする場合は、罰則のある受託事業者の就業規則等で裏付けられた守秘契約を行う等の秘密保持の対策を行うこと。 |  |
| ⅳ)　情報の破棄の手順等の設定 |
| [ ] 　a) データセンターから移動した統計情報を破棄する手順を定めること。当該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及び具体的な破棄の方法を含めること。 |  |
| [ ] 　b) データセンターから移動した統計情報が保存された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すること。 |  |
| [ ] 　c) 委託した事業者にデータセンターから移動した統計情報の破棄を委託した場合は、「医療情報システムの安全管理に関するガイドライン」の「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」に準じた対応を行うとともに、利活用契約者の責任の下で、確実に情報の破棄が行われたことを確認すること。 |  |
| ⅴ)　情報システムの改造と保守 |
| [ ] 　a) データセンターから移動した統計情報を取り扱うシステムの動作確認等には用いないこと。 |  |
| [ ] 　b) 保守会社の作業員がデータセンターから移動した統計情報を取り扱うシステムのメンテナンスにおいて、当該システムに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、当該統計情報へのアクセスの有無、及びアクセスした場合は当該統計情報を含む作業記録を残すこと。 |  |
| [ ] 　c) データセンターから移動した統計情報を取り扱うシステムについて、保守会社の作業員がシステムにアクセスするためのアカウント情報の適切な管理を当該保守会社に要求すること。 |  |
| [ ] 　d) データセンターから移動した統計情報を取り扱うシステムについて、保守会社の作業員の離職や担当替え等に対してシステムの保守用アカウントを速やかに削除できるよう、当該保守会社からの報告を義務付けるとともに、それに応じるアカウント管理体制を整えておくこと。 |  |
| [ ] 　e) データセンターから移動した統計情報を取り扱うシステムについて、保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を要求するとともに、それらの書類を当該システムの管理者が逐一承認すること。 |  |
| [ ] 　f) データセンターから移動した統計情報を取り扱うシステムについて、保守会社が当該統計情報を利活用者又は当該利活用者が業務を委託した者の組織の外に持ち出さないこと。 |  |
| [ ] 　g) データセンターから移動した統計情報を取り扱うシステムについて、リモートメンテナンスによるシステムの改造や保守が行われる場合には、必ずアクセスログを収集するとともに、当該作業の終了後速やかに作業内容を当該システムの責任者が確認すること。 |  |
| ⅵ)　情報及び情報機器の持ち出しについて |
| [ ] 　データセンターから移動した統計情報の取扱い及び保管については、利活用契約者の責任の下、決められた場所でのみ行うこととし、原則として外部への持ち出しは行わないこと。ただし、外部委託や共同研究の場合等、利活用契約者の責任の下で利活用者の間で最小限の範囲で中間生成物等の受け渡し等の移動を行う場合には、次のa)からi)に掲げる措置を講じていること。 |  |
| [ ] 　a) 組織としてリスク分析を実施し、データセンターから移動した統計情報及び当該情報を保存した可搬媒体又は情報機器の持ち出しに関する方針を運用管理規程で定めること。 |  |
| [ ] 　b) 運用管理規程には、データセンターから移動した統計情報及び当該情報を保存した可搬媒体又は情報機器の持ち出しの方法を定めること。 |  |
| [ ] 　c) 運用管理規程には、データセンターから移動した統計情報及び当該情報を保存した可搬媒体又は情報機器の盗難、紛失時の対応を定めること。 |  |
| [ ] 　d) 上記a)からc) で定めた対応について、利活用者等に周知徹底し、教育を行うこと。 |  |
| [ ] 　e) データセンターから移動した統計情報及び当該情報を保存した可搬媒体又は情報機器の所在について、台帳を用いる等して把握すること。 |  |
| [ ] 　f) データセンターから移動した統計情報の移動に用いる可搬媒体又は情報機器に対して、起動パスワードを設定すること。設定に当たっては、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講じること。 |  |
| [ ] 　g) 盗難、置き忘れ等に対応する措置として、データセンターから移動した統計情報の暗号化又は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) データセンターから移動した統計情報及び当該情報を保存した可搬媒体又は情報機器を、他の外部媒体等と接続する場合は、コンピュータウイルス対策ソフトの導入を行う等して、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) データセンターから移動した統計情報の移動について個人保有の情報機器（PC等）を使用する場合であっても、上記のf）、g）、h）と同様の要件を遵守させること。 |  |
| ⅶ)　外部とデータを交換する場合の安全管理 |
| [ ] 　a) データセンターから移動した統計情報について、ネットワークを経由して交換する場合は、次に掲げる措置を講じていること。・ ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策を行うこと。・ 施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策を行うこと。・ セッション乗っ取り、IPアドレス詐称等のなりすましを防止する対策を行うこと。 |  |
| [ ] 　b) データセンターから移動した統計情報について、ネットワークを経由して交換する場合は、採用する通信方式や運用管理規程により、採用する認証手段を決めること。 |  |
| [ ] 　c) データセンターから移動した統計情報について、ネットワークを経由して交換する場合は、次に掲げる措置を講じていること。・ ルータ等のネットワーク機器に安全性が確認できる機器を利用すること。・ 施設内のルータを経由して異なる施設間を結ぶVPNの間で送受信ができないように経路設定されていること。 |  |
| [ ] 　d) データセンターから移動した統計情報について、ネットワークを経由して交換する場合は、送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。 |  |

【留意事項】

記載内容が多くなる場合には、必要に応じて、様式には簡潔にその概要を記載するとともに詳細は別紙参照の旨を記載し、詳細を記載した資料を添付することとして差し支えない。