（別紙様式３の４）利活用申出書４

|  |  |
| --- | --- |
| **【利活用情報の管理方法】** | |
| 該当するものを■へ変更すること  　以下の各項目を遵守する。  　以下の各項目を遵守する。ただし、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項目があるため、各項目の右欄の該当項目を■で示し、その内容（変更した項目の理由、その他の備考）及び同等以上の代替措置について記載する。  ※　「２（３）データセンターから外部へ移動した統計情報の取扱いについて」については、該当する利活用以外の項目について記載する必要はない。  ※　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。  （業務を委託する場合は以下も選択すること）  　業務委託先に対して、以下の各項目を遵守させる。  　業務委託先に対して、以下の各項目を遵守させる。ただし、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項目があるため、各項目の右欄の該当項目を■で示し、その内容（変更した項目の理由、その他の備考）及び同等以上の代替措置について記載する。  ※　利活用契約者の所属する法人における管理状況と、委託先における管理状況を区別して記載すること | |
| **１　利活用者の所属する組織が一般的に具備すべき条件** | |
| 個人情報保護に関する方針を策定し、公開していること。 |  |
| ＭＩＤ－ＮＥＴ利活用全般に関し適切な安全管理に関する措置が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るため、ＭＩＤ－ＮＥＴ利活用者及び統計情報利活用者に対して、次の人的安全対策を講じられていること。   * 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。 * 定期的に個人情報等の安全管理に関する教育訓練を行うこと。 * 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。 |  |
| 利活用の一部の作業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、次の人的安全対策を講じられていること。   * 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あたっては、作業者、作業内容及び作業結果の確認を行うこと。 * 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　利活用にあたり遵守する事項** | |
| 次の（１）から（３）に掲げる事項を遵守させるとともに、これらの内容について教育訓練を実施する |  |
| オンサイトセンターの利用及びデータセンターへの接続について | |
| 1. ＭＩＤ－ＮＥＴ利活用者は、携帯電話、デジタルカメラ等の電子機器類によるデータセンターにリモートアクセスしている画面の撮影及び録画の防止、画面の覗き見防止等の情報管理を徹底すること。 |  |
| 1. ＭＩＤ－ＮＥＴ利活用者は、機構から発行されたデータセンターの利用に必要となるユーザＩＤ及びパスワードを、本人しか知り得ない状態に保つこと。また、パスワードについては次の事項に留意し管理すること  * パスワードは定期的に変更すること。 * 類推しやすいパスワードは使用しないこと。 |  |
| ＭＩＤ－ＮＥＴ接続環境の利用について **※接続環境の利用有無によらず、対応可否について記載すること** | |
| 物理的安全対策 |  |
| 1. データセンターへのリモートアクセスは、ＭＩＤ－ＮＥＴを利活用する調査を実施する者の役職員又は当該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から行わせること。ただし、機構の許可を受け、機構内でＭＩＤ－ＮＥＴ接続環境を利用する場合を除く。 |  |
| 1. ＭＩＤ－ＮＥＴ接続環境として用いる専用端末は、機構から許可された場合を除き、上記ａ）の領域から外部に移動させないこと。 |  |
| 1. ＭＩＤ－ＮＥＴ接続環境として用いる専用端末に対して、盗難防止のために、常時、盗難防止用セキュリティワイヤーを設置するか、或いは、端末を使用しない間はロッカー等に施錠して保管すること。 |  |
| 1. ＭＩＤ－ＮＥＴ接続環境として用いる専用端末について、データセンターへリモートアクセスする際、覗き見防止の対策を実施すること。 |  |
| 技術的安全対策 |  |
| 1. ＭＩＤ－ＮＥＴ接続環境として用いる専用端末は、機構より貸与された端末又はデータセンターへリモートアクセスすることを機構より許可された端末に限定すること。 |  |
| 人的安全対策の措置 |  |
| 1. ＭＩＤ－ＮＥＴ接続環境として用いる専用端末を利用する者は、機構よりユーザＩＤ及びパスワードが発行されたものに限定すること。 |  |
| その他 |  |
| 1. 機構内でＭＩＤ－ＮＥＴ接続環境を利用する場合は、機構の指示を遵守させること。 |  |
| データセンターから外部へ移動した統計情報の取扱いについて | |
| 【全ての利活用区分における共通事項】 | |
| データセンターから外部へ移動した統計情報は、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。 |  |
| データセンターから外部へ移動した統計情報について、台帳等によりリストアップし、所在を把握すること。 |  |
| データセンターから外部へ移動した統計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（個人保有の情報機器（パソコン等）を含む。）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。 |  |
| **（３） データセンターから外部へ移動した統計情報の取扱いについて**  **※利活用の種類に応じて選択すること** | |
| 【製造販売業者等が行う製造販売後調査その他法令に基づき実施する調査のための利活用】 | |
| ＧＰＳＰ省令または、ＧＶＰ省令に則り作成された手順書等に基づき、統計情報を適切に保存及び管理し、情報漏えいを防ぐこと。 |  |
| 【行政利活用】 | |
| 機構法に基づく秘密保持義務に従って、統計情報を適切に保存及び管理し、情報漏えいを防ぐこと。 |  |

行政利活用又は製造販売業者等が行う製造販売後調査その他法令に基づき実施する調査のための利活用に該当する場合、次項以降は記載する必要はない。

|  |  |
| --- | --- |
| **（３） データセンターから外部へ移動した統計情報の取扱いについて** | |
| 【その他の利活用】 | |
| 組織的安全管理対策（体制、運用管理規程）の実施 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 1. 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 |  |
| 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、この別紙の項目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。 |  |
| 物理的安全対策 |  |
| 1. 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、当該機器の設置場所及び記録媒体の保存場所を施錠すること。クラウドサービスを利用する場合は、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上で、統計情報を保存すること。 |  |
| 1. 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、次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。 |  |
| 1. 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上で統計情報を保存すること。 |  |
| 1. 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、盗難防止用セキュリティワイヤーを設置すること。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、盗難防止用セキュリティワイヤーの設置に代えて、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。 |  |
| 1. 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。 |  |
| 技術的安全対策 |  |
| 1. 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。 |  |
| 1. 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及びパスワードを本人しか知り得ない状態に保つよう対策を行うこと。 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 1. 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、やむを得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。 |  |
| 1. 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）。 |  |
| 1. 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。 |  |
| 1. 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、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。 |  |
| 人的安全対策の措置 |  |
| 1. 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。 |  |
| 情報の破棄の手順等の設定 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 1. 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、情報セキュリティ対策を踏まえた教育訓練、守秘・非開示に関する内容を委託契約に含める等の「医療情報システムの安全管理に関するガイドライン」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。 |  |
| 情報システムの改造と保守 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 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、次に掲げる措置を講じていること。 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 1. 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講じること。 |  |
| 1. 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。 |  |
| 1. 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（パソコン等）を使用する場合であっても、上記のf）及びg）と同様の要件を遵守させること。 |  |
| 外部とデータを交換する場合の安全管理 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 1. 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。 |  |
| 1. 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。 |  |