（様式２-１）

**院内がん登録全国収集データ利用に際しての安全管理措置**

以下の内容は、主に個票利用時に必要な安全管理措置についての必要事項になります。

集計値利用は、個人情報保護の観点から問題がない集計値による提供のため、基本的には特別な措置は必要ありません。

施設名利用は、1. 組織的安全管理対策、2. 物理的安全管理対策、4. 人的安全管理対策を講じてください。3. 技術的安全管理対策については、ウイルス対策ソフトの導入及び該当ソフトの定期更新を行ってください。

ただし、集計値利用や施設名利用であっても、希少がんなどの集計値で小さな値の集計値提供を希望される場合は、審査委員会の判断により個票利用時と同等の安全管理措置が求められる場合があります。

様式2-2 院内がん登録全国収集データ利用におけるデータ安全管理チェックリストの「具体的なデータ管理場所」には全ての管理場所を具体的に記載してください。（例 ●号棟■階○○室 等）

１．組織的安全管理対策

申請者は申請内容の範囲に従って、提供されたデータを取り扱う責任を負う。事務局に提出した内容に変更が生じた場合は、事務局に遅滞なく報告するとともに、変更申請を速やかに行うこと。また、事務局による監査の申し入れには協力し、指摘事項が生じた場合には速やかに是正すること。

個人情報の漏洩等の事故が発生した、もしくは発生の可能性が高いと判断した場合は、自らが帰属する組織の情報管理規定に従うとともに、事務局に直ちに報告し、その指示に従うものとする。

２．物理的安全管理対策

　申請者は物理的安全管理対策として、以下の事項を遵守すること。

* 提供データの利用場所を特定し、物理的にデータを持ち出さないこと。
* 利用場所に随時入室可能な者を特定し、監査に応じて入退室記録を提出可能とすること。
* 上記以外の者が利用場所に入室する際は、必要事項（氏名、所属部署、連絡先、入室目的、入室日時、退室日時）の記録を含む入退室管理を行うこと。
* 保存・解析を行う端末を特定すること。解析に使用する端末の中にデータを保存する場合は、施錠管理された利用場所内で、ワイヤーなどを利用して固定するか、施錠されたラックの中で管理すること。モバイル端末の中にはデータ（個票・中間生成物）を保存しないこと。外付けの記憶装置に保管する場合には、施錠管理すること。
* 情報のレベルに応じた追加的な管理を別途定めること。

３．技術的安全管理対策

解析端末は、以下の対策を講ずること。

* システム管理者によって管理されている不正侵入検知・防御システムのあるルータで接続されたネットワーク環境を構築するか、インターネットに接続しないこと。
* 情報を取り扱うパソコン及びサーバへのアクセスは、ログイン認証機能により個票利用者のみがアクセスできるよう設定を行うこと。
* IDとパスワードのみによる認証機能を用いる場合は、パスワードを8桁以上の英文字、数字、記号を含むものとし、定期的に変更すること。また他者と共有しないこと。
* 端末にはウイルス対策ソフトをインストールし、ウイルスパターン定義ファイルは少なくとも48時間毎に定期的に更新すること。

４．人的安全管理対策

申請者はすべての利用者を監督し、以下の事項の責任を負う（利用者は、院内がん登録全国収集データ提供規程で定める定義に従う）。

* データに触れる者は利用者に限られること。
* 中間生成物の共有範囲が、申請書に記載された範囲を逸脱しないようにすること
* 利用者全員が、利用終了あるいは離任等の理由により、利用者ではなくなったのちも秘密保持を徹底させること
* 作業の一部を利用者以外に委託することは許可しないこと。
* 技術的安全管理、物理的安全管理を確保すること。

（様式２-２）

**院内がん登録全国収集データ利用におけるデータ安全管理チェックリスト**

研究課題名：

以下、確認の上該当するものにチェックしてください。

**具体的なデータ管理場所：（ 　　）**

**必須基準：**

1. **データの保管は、以下の要件を満たすこと。**

　　データの保管場所は、入室者が限定されており、通常施錠下にあること。

　　データの保管媒体は、常に施錠下に管理されること。

　　パソコン内のハードディスクに保管する場合は、当該パソコンがワイヤー固定されていること。

　　外付けハードディスクその他の移動可能媒体の場合は、施錠管理できる管理場所に限定し持ち出さないこと。

1. **データを解析するパソコンは、以下の要件を満たすこと。**

　　8文字以上のパスワード(英文字・数字・記号を含む)を設定するポリシーがあり、ゲストアカウントはオフになっている。

　　ウイルス対策ソフトがインストールされている。（ソフト名：　　　　　　　　　　　）

　　OS の定期的アップデートを行っている。

　　ウィニーなどの P2P ファイル共有ソフトはインストールしていない。

　　解析端末はネットワークに接続しない。

　　国外の保管場所を利用しない(国外にサーバのあるクラウドサービスも不可)

※解析端末をネットワークに接続しない場合は、以上で確認終了

1. **解析端末をネットワークに接続する場合は、それぞれの要件を満たすこと（それぞれ以下のチェックも記入）。**

* 施設名あるいは対応キーの提供を受けない場合　→　a基準を満たすこと
* 提供を受ける場合　→　b1基準またはb2基準を満たすこと、またはISMS等の外部機関認定を得ている(c)

**a基準（施設名あるいは対応キーの提供を受けない場合）：**

　　施設名あるいは対応キー（院内がん登録連番）の提供は受けない。

　　接続するLANの管理者がいる。  
（管理者所属： 　　　氏名：　　　　　　　　　　　　）

　　セキュリティ上の問題の発生時の対応窓口／担当部署がある。  
（対応窓口／担当部署 　　）

　　データを解析するパソコンがWindowsの場合、ネットワーク探索はオフになっている。

**b1基準（解析者が全て同一の施設に属する場合）：**

　　施設内で他の個人情報つきの診療情報を扱うのと同じネットワークにのみ接続される。

　　施設における当該ネットワークの管理方針（規程）等が設けられている（規程等の複写を提出）

**b2基準（複数施設で共同解析をする場合）：**

　　データの保存管理場所は物理的に1箇所とし、VPN など通信経路を暗号化したネットワークを通じて解析者が接続する。また、その接続認証には2 要素認証が設定されている（通常のID／パスワードに加え、端末認証、クライアント証明書、ワンタイムパスワードなどのいずれかの認証が行われること）。

　　保存・解析用のサーバの設置場所は、少数の限定された者だけが入室許可され入室記録がある。

**c情報セキュリティ関連の外部認証がある場合：**

　　ISMS(情報セキュリティマネジメントシステム)の認定を得ている（認証の複写を提出）。