資料２

全国がん登録　利用者の安全管理措置（仮称）

目　次

I. はじめに

がん医療及びがん予防活動を評価し、その向上を進めていく上で、がん登録は欠くことができない。がん登録から得られる罹患率や生存率の統計が正確で高い信頼性を持つためには、1 つの同じ腫瘍を誤って複数の腫瘍として登録することを避けなければならないため、氏名、生年月日、住所といった個人情報を収集することが必要である。従って、がん登録事業に携わる者は患者の病歴を含む機微な個人情報を扱うこととなるため、データ収集、管理、利用及び提供の各段階に必要とされる安全管理措置を講ずることが求められる。

平成 25 年 12 月 6 日に成立した、がん登録等の推進に関する法律（平成 25 年法律第 111 号。以下「法」という。）に規定されている秘密保持義務は、国又は国立がん研究センターにおいて全国がん登録情報等の取扱いの事務に従事する職員や、都道府県がん情報等の取扱いの事務に従事する都道府県職員に規定されているのと同様に、法第 33 条では、全国がん登録情報若しくは都道府県がん情報の提供を受けた者にも秘密保持義務が課せられることが規定されている。また、全国がん登録情報及び都道府県がん情報の機微性や、事業自体の重要性から、法第 6 章において、こうした規定に反して秘密を漏らした者は、厳格に処罰されることが規定されている。

厚生労働省と国立がん研究センターは、本書を作成し、全ての利用者が、法及び厚労省ガイドライン等を遵守し、全国がん登録情報の積極的かつ安全な活用を促進するために必要な対策を一定程度具体的に記載することとした。

本書では、利用者において実施可能と考えられ、かつ確実に実現すべきことを「対策」とした。、更に、非匿名化情報を取り扱う利用者においては必須とし、匿名化情報を取り扱う利用者でも実現可能で推奨される対策に、「*」を付した。利用者が、本書に基づき安全管理措置体制を自ら評価し、実態に即した適切な対策を作り上げる上で役立つことを期待するものである。

II. 用語の定義

本書において使用する用語は、法及び情報の提供マニュアルにおいて使用する用語の例のほか、次の定義に従うものとする。

(1) 情報

本書において「情報」とは、全国がん登録情報及びその匿名化が行われた情報並びに都道府県がん情報及びその匿名化が行われた情報の総称をいう。(匿名化が行われた情報とは、特定匿名化情報、及び提供依頼申出者が求める範囲の情報を提供の際に匿名化を行い提供する情報のことをいう。)

(2) 資料

本書において「資料」とは、情報及び情報を加工した中間生成物を含む電子媒体、紙資料等のことをいう。

(3) 個人情報

利用者が収集した情報及び利用者に提供された情報の内、個々の患者を特定しうる情報をいう。

(4) 利用者・利用責任者・統括利用責任者

本書において「利用者」とは、情報の提供を受け、これらを利用する者をいう。利用者の内、各利用場所において当該情報の取扱いを統括し、情報の安全管理の責任を担うものを利用責任者という。さらに、これらの利用責任者を統括し、調査研究全体の安全管理の責任を担うものを統括利用責任者という。

(5) 利用場所

本書で取り扱う「利用場所」とは、情報の提供を受け、集計、分析、保管を行う物理的スペースをいう。

(6) 情報を取り扱う PC 等

利用者において、情報を含むデータを入力・処理するシステムをいう。サーバ、クライアント PC、プリンタ、スキャナ、アプリケーションを含む。

(7) 窓口組織

情報の提供依頼申出者に対する一元的窓口機能を果たし、かつ、申請を取りまとめた上で、それぞれの情報について厚生労働大臣、国立がん研究センター、都道府県知事が行った提供の決定に基づき、情報の提供を行う調整機能を果たす組織を窓口組織という。

III. 基本的な安全管理対策と推奨される安全管理対策

リスクに対し、安全管理措置として、組織的、物理的、技術的、人的な対策をとるべきである。

1.　組織的安全管理対策

本節では組織的安全管理対策について述べる。組織的安全管理対策とは、統括利用責任者が、利用場所における安全管理について、自らの責任とすべての利用者の権限を明確に定め、その実施状況を日常の自己点検等によって確認することをいう。組織的安全管理対策には以下の事項が含まれる。

ア．安全管理対策を講じるための組織体制の整備
イ．個人情報の取扱状況を一覧できる手段（個人情報取扱台帳）の整備
ウ．利用者の安全管理対策の評価方法の整備とその見直し及び改善
エ．事故（情報の漏洩等）又は違反（従事者の運用管理規程違反等）への対処方法の整備

【対策】

(1)　統括利用責任者は、各利用場所に、情報の利用責任者を置き、体制を整備する。
(2)　利用責任者は、利用場所ごとに、利用者のリストを作成し、それぞれの作業分担と処理してよい情報の範囲とを明記する。このリストは、常に最新のものに更新する。
(3)　統括利用責任者は、取り扱う情報の種類ごとに、保管及び廃棄に関する一覧を整備する。一覧には、以下の項目を含む。
　1)　保管期限
　2)　保管方法
　3)　保管場所
　4)　廃棄方法
(4)　利用者は、定められた担当範囲と手続きに従い、情報を適切に取り扱う。利用責任者は、利用者が、万一、担当範囲や手続きに違反している事実又は兆候に気付いた場合は、速やかに是正する。
(5)　統括利用責任者は、厚生労働大臣又は都道府県知事より、報告の要請、助言、勧告及び命令があった場合には、外部監査の受け入れを含め、現状を把握し、対策を実施し、結果を取りまとめ、窓口組織に報告する。（法第 36 条、第 37 条、第 38 条）

（報告の徴収）
第三十六条　厚生労働大臣及び都道府県知事は、この節の規定の施行に必要な限度において、第三節の規定により全国がん登録情報若しくは都道府県がん情報の提供を受けた者（都道府県知事及び市町村長を除く。次条において同じ。）又は当該提供を受けた者からこれらの情報の取扱いに関する事務若しくは業務の委託を受けた者に対し、これらの情報の取扱いに関し報告をさせることができる。

（助言）
第三十七条　厚生労働大臣及び都道府県知事は、この節の規定の施行に必要な限度において、第三節の規定により全国がん登録情報又は都道府県がん情報の提供を受けた者に対し、これらの情報の取扱いに関し必要な助言をすることができる。

（勧告及び命令）
第三十八条　厚生労働大臣及び都道府県知事は、前条に規定する者が第三十条第一項、第三十一条第一項又は第三十二条の規定に違反した場合において個人の権利利益を保護するため必要があると認めるときは、当該者に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を勧告することができる。
２　厚生労働大臣及び都道府県知事は、前項の規定による勧告を受けた者が正当な理由がなくてその勧告に係る措置をとらなかった場合において個人の権利利益が不当に害されるおそれがあると認めるときは、当該者に対し、その勧告に係る措置をとるべきことを命ずることができる。
３　厚生労働大臣及び都道府県知事は、前二項の規定にかかわらず、第三十六条に規定する者が第三十条、第三十一条又は第三十二条の規定に違反した場合において個人の重大な権利利益を害する事実があるため緊急に措置をとる必要があると認めるときは、当該者に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべきことを命ずることができる。

* (6)　統括利用責任者は、個人情報の漏洩等（漏洩、滅失又はき損）の事故が発生した場合、若しくは発生の可能性が高いと判断した場合の対応の手順を、整備する。事故時対応手順には、以下の項目を含む。
    1)　発見者から統括利用責任者への報告
    2)　発見者から報告を受けた利用責任者から統括利用責任者への報告
    3)　統括利用責任者から窓口組織への報告
    4)　報告先の連絡方法（休日・夜間、連絡がつかない場合の対応を含む）
    5)　事実確認、原因究明、漏洩停止措置
    6)　影響範囲の特定
    7)　再発防止策の検討・実施
    8)　不正アクセス行為の禁止等に関する法律等の法令に定めるところによる対処

2.　物理的安全管理対策

本節では物理的安全管理対策について述べる。利用者の作業においては、情報及び中間生成物を電子媒体、PC 等の情報機器の中、あるいは紙媒体で保管・管理を行っている。物理的安全管理対策とは、これらの媒体や情報を取り扱う PC 等を管理するに当たって、盗難、紛失、窃視等を防止することである。物理的安全管理対策には以下の事項が含まれる。

ア．利用場所の入退室の管理

イ．盗難、窃視等の防止

ウ．機器・装置・情報媒体等の盗難や紛失防止も含めた物理的な保護及び措置

利用の体制によっては、利用者として独立した空間の確保が困難な場合がある。その場合は、他の物理的、技術的、人的安全管理対策を強固にする。

【対策】

(1)　情報を含む電子媒体及び紙媒体は、鍵付きキャビネット等に施錠保管し、利用者は施錠されていることを、作業終了時に確認する。

*(2)　情報を含む電子媒体及び紙媒体が保管されている鍵付きキャビネット等の鍵の使用を記録すると共に、複数の鍵を更に鍵付きボックスに収納して、利用者がボックスの鍵を管理する。

(3)　USB 等の可搬電子媒体に情報を保存し保管している場合、現物の確認ができるように保管対象の電子媒体リスト（提供を受けた日や廃棄日を含める）を作成する。

(4)　キャビネット等の鍵は、作業終了時には定位置に戻し、利用者が鍵を確認する。

(5)　情報が保存されているロッカー、キャビネットは、施錠可能な利用場所（保管庫を含む）に設置する。

(6)　利用場所（保管庫を含む）が無人のときは施錠する。

*(7)　利用場所（保管庫を含む）が独立していない場合には、利用場所エリアへの出入口となる場所を限定し、そのポイントについては利用者が正対して座るように座席を調整する等、動線についても管理する。

*(8)　利用責任者は、利用場所の設置状況に応じて、利用場所あるいは利用場所を含む執務室への入室を許可する者の範囲を明らかにする。

*(9)　利用責任者は、利用場所の設置状況に応じて、入退室時（夜間・休日を含む)の手続きを明らかにする。

*(10)　個人情報の利用を行う利用場所並びに個人情報の物理的保存を行っている区画は、他の業務から独立した部屋として確保する。

*(11)　利用場所に必要な機器類（プリンタ、コピー機、シュレッダなど）は、他の業務と共用せず、利用場所内に設置する。

*(12)　個人情報の物理的保存を行っている区画の施錠は鍵を二重にする。

*(13)　利用者以外が、保守作業等により情報を取り扱う PC 等に直接アクセスする作業の際は、利用者が、作業者・作業内容・作業結果等の確認を行う。

（14） 情報を取り扱う PC 及びサーバに盗難防止策を講じる（セキュリティチェーン等による固定、施錠したサーバラック内への設置、など）。

（15） 情報を取り扱う PC 等は、安全管理上の脅威（盗難、破壊、破損）のみならず、環境上の脅威（漏水、火災、停電）からの物理的な保護にも配慮する。

3.　技術的安全管理対策

本節では技術的安全管理対策について述べる。技術的安全管理措置とは、情報及びそれを取り扱う PC 等へのアクセス制御、不正ソフトウェア対策、監視等をいう。技術的な対策のみで全ての脅威に対抗できる保証はなく、一般的には運用による対策との併用は必須である。技術的安全管理対策には以下の事項が含まれる。

ア．利用者の識別及び認証

イ．情報の区分管理とアクセス権限の管理

ウ．アクセスの記録（アクセスログ）

エ．不正ソフトウェア対策

オ．ネットワーク上からの不正アクセス対策

【対策】

*（1） 情報を取り扱う PC 等は、物理的又は論理的に外部ネットワークから独立した有線の環境であること。

（2） システム管理者によって管理されている不正侵入検知・防御システム及びウイルス対策機能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。

（3）情報を取り扱う PC 及びサーバは、OS（Windows など）のサインインパスワードの設定を行う。

*（4）個人情報を取り扱う PC 及びサーバは、生体計測＋ID・パスワード等の 2 要素認証とする。

（5） OS（Windows など）のログインのためのパスワードを 8 桁以上のものに設定し、第三者が容易に推測できるものは避ける。

（6） OS（Windows など）のログインのためのパスワードを定期的に変更し、以前設定したものの使い回しは避ける。

（7） パスワードを第三者の目につくところにメモしたり、貼付したりしない。

（8） 外部ネットワークと接続する電子媒体（USB メモリ、CD-R など）を情報を取り扱う PC 等に接続する場合は、ウイルス等の不正なソフトウェアの混入がないか、最新のウイルス定義パターンファイルを用いて確認する。

4.　人的安全管理対策

本節では人的安全管理対策について述べる。人的安全管理措置とは、秘密保持義務と違反時の罰則に関する規程について、統括利用責任者及び利用責任者は自ら学習し、利用者に、教育・訓練等を行うことをいう。

【対策】

(1)　統括利用責任者及び利用責任者は、情報に関する規程等及び各利用者の役割並びに責任について、自ら学習し、すべての利用者に説明を行う。下記内容を含む。

1)　情報に関する規程等

- 法に規定される秘密保持義務　（法第 33 条及び第 34 条）

（受領者等に係る全国がん登録情報の取扱いの事務等に従事する者等の秘密保持義務）
第三十三条　第三節の規定により全国がん登録情報若しくは都道府県がん情報の提供を受けた場合におけるこれらの情報の取扱いの事務若しくは業務に従事する者若しくは従事していた者又は当該提供を受けた者からこれらの情報の取扱いに関する事務若しくは業務の委託があった場合における当該委託に係る業務に従事する者若しくは従事していた者は、それぞれその事務又は業務に関して知り得たこれらの情報に関するがんの罹患等の秘密を漏らしてはならない。

（受領者等に係る全国がん登録情報の取扱いの事務等に従事する者等のその他の義務）
第三十四条　第三節の規定により全国がん登録情報若しくは都道府県がん情報若しくはこれらの情報の匿名化が行われた情報の提供を受けた場合におけるこれらの情報の取扱いの事務若しくは業務に従事する者若しくは従事していた者又は当該提供を受けた者からこれらの情報の取扱いに関する事務若しくは業務の委託があった場合における当該委託に係る業務に従事する者若しくは従事していた者は、それぞれその事務又は業務に関して知り得たこれらの情報をみだりに他人に知らせ、又は不当な目的に使用してはならない。

- 本書
- その他

2)　各利用者の役割及び責任

3)　業務離任後の秘密保持

(2) 利用責任者は、利用者が追加された場合は、当該利用者に対し情報に関する規程等、各利用者の役割及び責任について説明を行う。

(3) 利用責任者は、利用者が業務を離れるときには、当該利用者に対し離任後の秘密保持に関して説明を行う。

(4)　利用責任者は、情報を取り扱う PC 等の保守作業やネットワーク環境構築及び維持保守を外部に委託する場合の手続きを明らかにする。契約が、利用者単独の契約でない場合、秘密保持義務契約の内容を確認し、必要な対策を講じる。

Ⅳ. 作業内容から見た安全管理対策

本章では、利用者の作業内容に沿って、基本的な安全管理対策と推奨される安全管理対策を踏まえて、手順に明らかにするべき具体的な内容と対策を示す。各作業項目では、担当者を明らかにし、個人情報の取扱いに関する具体的な手続きを明らかにする。

1.　入退室管理

他の業務から独立した利用場所を確保し、入退室の手続きを定め、権限のない者が利用場所に入退室することを防ぐ。

【対策】

* (1)　利用責任者は、利用場所の設置状況に応じて、利用場所あるいは利用場所を含む執務室への入室を許可する者の範囲を記述し、入退室管理簿を確認する作業管理者と、入退室管理簿の更新や保管を実施する担当者を明らかにする。
* (2)　利用責任者は、利用場所の設置状況に応じて、入退室時（夜間・休日を含む）の手続きを明らかにする。
* (3)　利用場所（保管庫を含む）が独立している場合には、最初の入室者による開錠と、最終退出者による施錠について入退出者名や時刻の記録をとり保管する。
* (4)　利用場所（保管庫を含む）が独立している場合には、個人情報の物理的保存を行っている区画に入退した者については入退室管理簿に記録の上、利用責任者が定期的に記録の確認を行う。

(5)　清掃業者等が立ち入る際には利用者が作業に立ち会う等、部外者の入退室における対応を行う。

* (6)　利用責任者は、利用場所あるいは利用場所を含む執務室の施錠の手続き（鍵の管理方法を含む）を明らかにする。

2.　移送

情報の移送には、配達記録が残る手段を利用する。電子媒体については、未使用品を使用することとする。

個人情報を取り扱う場合は、個人情報とその他の情報とを分離し、暗号化して送付した後、受け取り側で権限のある者のみが両者を復号し、結合する。この運用が可能となるよう、両者に同一のキー項目を設定するなど、結合を可能とする手段を提供する。個人情報とその他の情報の分離をしない場合、個人情報の暗号化と特別なキーによる復号を、代替手段とすることができる。また、不正なファイルやファイルの破損をチェックする手段を用意しておかなければならない。

【対策】

(1)　統括利用責任者は、移送の担当者を明確にする。
(2)　統括利用責任者は、移送先と情報を含む資料の種類（形態）に応じて、移送の手続きを明らかにする。
*(3)　個人情報を含む資料の移送には、予め受け取り側が準備する受け取り側の住所と、赤字で「親展」、「取扱注意」が記載された封筒を用いる。
*(4)　個人情報を含む資料を移送する場合には、追跡サービス付きの手段（レターパック、書留、特定記録郵便、ゆうパックなど）を利用する。
*(5)　移送する電子ファイルには、強固な暗号化方法を採用する。
*(6)　統括利用責任者は、利用者が自ら資料を持ち運ぶ場合の手続きを明らかにする。
*(7)　利用者が自ら資料を運搬する場合、移送中は当該資料に対して、常に人を付ける。
*(8)　利用者が紙の資料を運搬する場合、鞄や紙袋に入れる等、外部の人間が資料を直接見ることができないようにする。
(9)　統括利用責任者は、移送に関する記録の手続きを明らかにする。
*(10) 利用者と窓口組織を結ぶネットワークとして、厚生労働省が安全性を確認したものを除き、個人情報を含む資料を、インターネットを介して移送すること（電子メールへの添付など）を禁ずる。

3.　情報処理

情報処理とは、提供された情報の集計・統計分析に係る作業をいう。

【対策】
(1)　統括利用責任者は、情報処理の担当者を明確にする。
(2)　統括利用責任者は、各利用者が担当する情報処理の範囲と情報処理の手続き、方法を明らかにする。
(3)　利用責任者は、情報処理作業開始時、途中離席時、終了時について、情報を取り扱う PC 等と資料の取扱手続きを明確にする。
(4)　利用責任者は、情報処理に用いる PC と作業場所を限定する。

4.　保管・廃棄

資料は、応諾された利用期間内に申出た方法で保管する。応諾された利用期間を過ぎたもの、あるいは利用期間内であっても不要となった資料は、迅速かつ安全に廃棄する。

【対策】
(1)　統括利用責任者は、保管の担当者を明確にする。
(2)　利用責任者は、各利用者が保管してよい資料の種類と保管の手続き、方法を明らかにする。
(3)　資料の利用場所（保管庫を含む）以外への持ち出しを禁止する。

(4)　電子ファイルの保存には、ファイル及び電子媒体それぞれのパスワードや個人認証による保護等、複数の技術的・物理的安全管理措置を講じる。
(5)　統括利用責任者は、廃棄の担当者を明確にする。
(6)　利用責任者は、各利用者が廃棄してよい資料の種類と廃棄の手続き、方法を明らかにする。
*(7)　個人情報を含む紙資料はシュレッダ等、復旧ができないような方法で廃棄する。
*(8)　個人情報を含む資料の廃棄の作業場所は、利用者以外の者が余り出入りしないような部屋や、動線上、第三者が通る必要のない場所や、廊下の端等に限定する。
*(9)　個人情報が印刷された紙資料を利用者が利用場所外部で廃棄するような場合、利用者本人が、複数名で実施する。
(10)　紙資料、PC やメディアの廃棄を外部に委託することを禁止する。
*(11)　統括利用責任者は、情報を取り扱った PC 及びサーバ、記録・保管している電子媒体を廃棄する手続きを明らかにする。
(12)　PC や電子媒体の廃棄に当たっては、内部データ消去の専用ソフトウェアを利用するか、若しくはデータ記憶領域を物理的に破壊して再利用不可能な状態にする。
(13)　利用責任者は、廃棄の作業記録を残す。

【補足：廃棄の方法について】
*(1)　個人情報が記録・保管された電子媒体・PC 及びサーバ
- CD 等は、メディアシュレッダやはさみによる切断などにより物理的に破壊する。USB メモリも、物理的破壊が必要である。
- PC 及びサーバは、データの複数回上書き、消去用ソフトの利用で処理する。

*(2)　個人情報が記録された紙
- 裁断：ペーパーシュレッダは幅 1mm 以下、かつ面積 10mm2 以下のものの単体処理、又は幅 2mm 以下、かつ裁断面積が 30mm2 以下のクロスカット式又はマイクロクロスカット式のものと溶解・焼却等の併用処理とする。
- 溶解・焼却

5.　PC 管理

情報を取り扱う PC 等を維持するためには、定期的な保守が必要である。保守作業には、PC に障害を来さないためのソフトウェア更新等の対策、障害発生時に被害を最小限にとどめるための PC 異常の早期発見や迅速な応急処置等の対策、障害を是正し通常業務に戻るために行う復旧作業がある。障害対応時において、原因特定や解析のために障害発生時の情報の利用、利用中の情報を救済するために情報へのアクセスが必要な場合がある。

【対策】
(1)　統括利用責任者は、情報を取り扱う PC 等を管理する担当者を明確にする。

(2)　統括利用責任者は、情報を取り扱う PC 等の構成と設置場所を明らかにする。
(3)　利用場所内での業務に用いる PC の外部持ち出しは禁止する。
(4)　管理者用パスワードは不測の場合に対応できる管理方法をとる。
(5)　情報を取り扱う PC 等へのユーザ登録は、利用者が実施する。
(6)　利用者の追加が発生した場合、情報を取り扱う PC 等のユーザ ID とその利用者を紐付けて確認する作業を実施する。
(7)　統括利用責任者は、利用者が担当する情報処理の範囲に応じてアクセス可能範囲を定める。

6.　利用者からの窓口組織への問合せ

情報の内容に疑義が生じた場合、利用者は、窓口組織に問合せをして疑義照会を行う。
問い合わせ内容は記録する。

【対策】

(1)　統括利用責任者は、窓口組織への問合せを行う担当者を明確にする。担当者は原則として統括利用責任者とする。
(2)　統括利用責任者は、情報に関わる問合せについて、予め窓口組織と相談の上、問合せの手続きを明らかにする。
(3)　文書による照会の場合、依頼状、返信用封筒ともに、「**7. 移送**」に定めた手段を用いる。
*(4)　電話による、提供された情報に関する照会は、原則禁止する。やむを得ず電話を利用する場合は、機密保持の違反を容易に引き起こしうることを念頭に置き、利用条件を限定する。利用条件の例を以下にあげる。
　1)　電話の相手が窓口組織の担当者であることを間違いなく特定できる場合
　2)　具体的な質問事項を電話により誤解なく説明できる場合
*(5)　一般回線の FAX による照会は、原則禁止する。やむを得ず FAX を利用する場合は、誤送信と、権限のない者が送受信時に個人情報を目にすることとを防止するための具体的手続きを予め窓口組織と相談して定め、その条件を満たすことが確認できた場合に限る。
*(6)　利用者と窓口組織を結ぶ回線については、厚生労働省が安全性を確認したものを除き、インターネットを利用した電子メール等による照会は禁止する。
(7)　利用者の、患者や患者家族への直接接触は禁止する。
(8)　情報に関する、利用者及び窓口組織以外の外部からの問合せには、回答しない。外部からの問合せ者には以下が想定される。
　ア．病院等、医師会、市町村、保健所、都道府県庁等
　イ．学術団体等
　ウ．新聞、雑誌、テレビなどのマスメディア等
　エ．患者、患者家族、医師、一般市民等