全国がん登録における安全管理措置

愛知県がんセンター　がん情報・対策研究分野
伊藤秀美

全国がん登録の目的

- 一定地域におけるがん症例の診断、治療、予後等の情報を収集し、国や地域におけるがん対策の企画立案や評価、がん研究に役立てること

医療機関
罹患情報

- 新たにがんと診断された人の数（罹患数）
- がんが診断された時の進み具合（進行度）の分布
- がんと診断された人のその後の生存割合（生存率）

非常に機密性の高い個人情報を取り扱っている

安全管理措置

- 個人情報の漏えい（外部へ流出する）、滅失（内容が失われる）、毀損（内容が意図せず変更される）の防止等のために行われる措置のこと

- 全国がん登録では、氏名、生年月日、住所情報といった個人識別情報を含む患者の病歴というセンシティブな情報を扱うため、とりわけ入念な安全管理措置が求められる

「がん登録推進法」における安全管理措置

（国等による全国がん登録情報の適切な管理等）

第二十五条

２　　都道府県知事（略）は、第二節及び第三節の規定による事務を行うに当たっては、都道府県がん情報（略）及びその匿名を行った情報並びに死亡者情報票に記載され、又は記載された情報について、その漏えい、減出及び毀損の防止その他の適切な管理のために必要な措置を講じなければならない。

国内外の地域がん登録における安全管理措置の取り組み

- 1992年 “Guidelines on Confidentiality in the Cancer Registry”（国際がん登録協議会）
- 1996年「地域がん登録における情報保護」ガイドライン（厚生省がん研究助成金「地域がん登録の精度向上と活用に関する研究班」）
- 2004年　”Guidelines on Confidentiality for Population-based Cancer Registration” (国際がん登録協議会）
- 2005年「地域がん登録における機密保持に関するガイドライン」（地域がん登録全国協議会）
  - 情報技術の著しい進歩に対応
  - 個人情報保護法（平成17年）
  - 国際がん登録協議会のガイドライン改定
- 2006年　がん対策基本法の付帯決議「16.　（中略）がん登録精度のさらなる推進と登録精度の向上ならびに個人情報の保護を徹底するための措置について、本法成立後、検討を行い、所用の措置を講ずること」の明記

厚生労働省第三次対がん総合戦略事業「がんの実態とがん情報の発信に関する研究班」における安全管理措置向上への取り組み

- 2009年
  「地域がん登録における安全管理措置ハンドブック第1版」
- 2010年
  「地域がん登録室における安全管理措置に関するミニマムベースライン」
- 2012年
  「地域がん登録の安全管理」共通教育パッケージ
- 2014年
  「地域がん登録における安全管理措置ハンドブック第2版」
  - 厚生労働省ガイトラインと経済産業省による個人情報の保護に関する法律についての経済産業分野を対象とするガイドラインを参考にし、「地域がん登録における機密保持に関するガイドライン」に示されたがん登録における機密保持の原則と方法を詳細かつ具体的に記載

全国がん登録における安全管理の指針

- 厚労省ガイドライン
  - 医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス、医療情報システムの安全管理に関するガイドライン
- **全国がん登録における個人情報保護のための安全管理マニュアル**（第1版改定版、平成30年3月）
  - 全国がん登録事業の特性を踏まえ、がん登録推進法と厚労省ガイドラインを遵守し、業務を円滑に遂行することを促進するのに必要な対策
    - 全国がん登録の特性とは？
      - 患者の同意なく病歴を含む個人情報が収集されること
      - 都道府県またはその権限および事務に委任された機関において勤務する者は必ずしも医療従事者でないこと
      - 住民基本台帳情報や死亡者情報表に基づく死亡情報など、病院等からの届出対象情報以外の個人情報を取り扱う

全国がん登録における個人情報保護のための安全管理マニュアル

- 平成28年6月　第1版
- 平成30年3月　同改定版

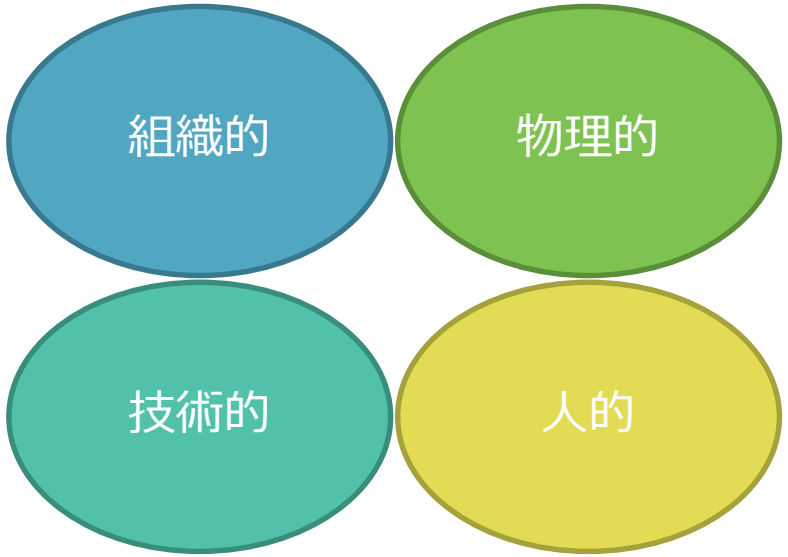
- 「地域がん登録における安全管理措置ハンドブック第２版」を基本として、全国がん登録の運用に即した内容に再編集したもの。

- 都道府県がん登録室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基本対策として、103項目を定めている。

全国がん登録における個人情報保護のための安全管理マニュアルにおける基本対策

- 情報が外部に漏れないように
  （紛失、窃視や盗難の防止）
- 情報が消失することのないように
  （バックアップを取得し安全な場所に保管）

- 作業面からみた安全管理措置
  - 入退室管理
  - 取得
  - 入力
  - データ加工
  - 保管・消去・廃棄
  - システム管理
  - 病院等または市町村等への問い合わせ
  - 外部からの問合せ
  - 移送



４つの安全管理対策

全国がん登録における安全管理措置の指針等

- 「全国がん登録における個人情報保護のための安全管理措置マニュアル」
  - 都道府県がん登録室

- 「全国がん登録届出マニュアル2016」
  - 病院等

がん登録における安全管理措置の基本的な考え方

全国がん登録における安全管理措置の基本的な考え方

- コンプライアンスの遵守（耐監査性への対応）
  - 組織面での管理措置
    （マニュアルや様式、事故時対応手順の整備、規程の教育・周知、および規程に基づいた業務実施の徹底）

- 漏えいリスクへの対応
  - 登録室内
    - 登録室内：物理的管理措置（動線管理）
    - 技術的管理措置（PC, プリンタ、サーバ等の管理）
  - 登録室外（紙媒体、電子媒体のライフサイクル管理）

- 業務の確実性への対応
  - 業務保全面での管理措置
    （規程・手順書の保管場所の周知と最新化、バックアップの取得）

コンプライアンスの遵守（耐監査性への対応）

- 各登録室における安全管理措置を含む業務内容を文書化し、文書に基づいて業務を行うことで外部からの監査に対応できるようにする

- **愛知県がん登録室で実施していること（組織的安全管理対策）**
  - 個人データの取扱に関する管理責任者の明確化
  - 従事者の作業分担と処理してよい情報の範囲を明記したリストの作成と最新化
  - 個人情報の取扱に関する要領・手順の作成
  - 個人情報取扱台帳の整備
  - 保管及び破棄に関する一覧の整備
  - 登録室職員が手順に違反している事実または聴講に気づいた場合の登録室責任者への報告
  - 安全管理措置チェックリストを用いた内部評価
  - 要領・手順の最新状態の維持
  - 外部監査の受審
  - 事故時対応手順の整備

  など

管理責任者のがん登録における安全管理措置での役割

- 安全管理措置に関する規定書や手順書の整備、具体化、運用、最新化
- 上記規定などの実施状況を日常の自己点検などにより確認

PDCAサイクルの実践

- 事故（情報漏えい）や違反（従事者の規定違反）への対応

漏洩へのリスク対応

リスク分析

1. 守るべき個人情報の洗い出し
2. 個人情報および形態や場所をリスト化
3. どのような状況において情報の漏洩及び滅失・毀損のリスクがおこりうるか
4. 予防するにはどのような対策をとるべきか
5. 残余リスクの有無の確認と対策

愛知県がん登録室において保護すべき情報

1. 収納設備に保管されているがん登録情報
2. 登録室内に直接置かれているがん登録情報
3. 登録情報データベースサーバー中のがん登録情報
4. クライアントＰＣに出力されたがん登録情報
5. 外部機関から受領した配送物中のがん登録情報
6. 移送・運搬中のがん登録情報
7. 複合機等から出力されたがん登録情報
8. 廃棄前の書類や電子媒体
9. 個人情報を含む問合せ情報
10. 職員の記憶

物理的管理措置　－多層防御の重要性

物理的防御　情報資産

すべての人物がアクセスできる階層

郵送物等の集積所

大型複合機等、登録室の外にある出力機器

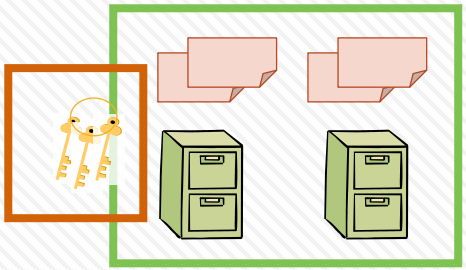
登録室

登録室の職員がアクセスできる階層

登録室に置かれた紙媒体

キャビネ等収納設備

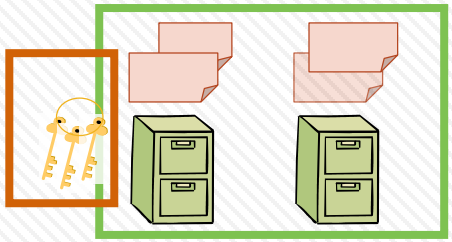
登録室に入れる者で、当該設備の鍵を持つ者がアクセスできる階層



キャビネに保管された紙媒体

保管庫

キャビネ等収納設備



キャビネに保管された紙媒体

がん登録室において保護すべき情報とリスクと対策の考え方の流れ（例）

- （保護すべき情報は何か）収納設備に保管されているがん登録情報
- →（取り扱うメディアは何か）電子媒体（USBメモリ、CD）及び紙
- →（その情報に関わる情報漏えい等のリスクは何か）
- 保管キャビネットの施錠忘れ
- →（リスクを回避するための対策は何か）
  - 主たる対策分野　物理的安全管理措置
  - 関連する登録室作業　保管・消去・廃棄
  - 対策例　個人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、鍵の使用を記録するとともに、複数の鍵をさらに鍵付きボックスに収納して、登録室責任者または作業責任者がボックスの鍵を管理する

キャビネットは、鍵のかかる登録室や保管庫に設置することで、
多重防御を担保

登録室内から個人情報を漏らさないための物理的な対策

- 鍵をかける（鍵のかけ忘れを防ぐ）
  - 個人情報が存在する登録室、保管庫、キャビネットなどは施錠する
  - 登録室の解錠者と施錠者の記録をつける
- 部外者の立ち入りやのぞき見を防ぐ
  - 机上の帳票は離席時には裏返しにするか見えない場所にしまう
  - PC画面は離席時もしくは一定時間でスクリーンセーバが作動するように設定する
  - （同線上、領域を奥に設置する、配置構成を工夫する）
- サーバ、パソコンの盗難
  - サーバを施錠したサーバラック内へ設置する、ワイヤーロックをかける

登録システムを介した情報漏えいリスクを減らすために

- IDとパスワードを守る
  - IDを共有することは避け、各個人が固有のIDを持つようにする
  - ログインパスワードに条件と有効期間を設定してパスワードは定期的に変更する
  - パスワードを記録しておく場合は保管を厳重にする
- 他人のID/パスワードは使わない
  - 登録システムへのログインは自分のID/パスワードで行う（PCを共有している場合には、自分のIDでログインしなおす）
- 外部記憶媒体を接続する前にウィルスチェック
  - ウィルス感染に伴う登録システムの破壊を未然に防ぐ

技術的管理措置　－論理的防壁の設定

物理的防御　論理的防御　情報資産

すべての人物がアクセスできる階層

登録室

登録室の職員がアクセスできる階層

キャビネ等収納設備

電子データ

可搬媒体（パスワード保護等がされたもの）

登録端末

登録室に入れる者で、かつ「登録端末」にログオンできる階層

OS（Windows）による認証

サーバ

登録室に入れる者で、かつ「登録端末」にログオンでき、かつ「登録システム」にログオンできる階層

電子データ

登録システムによる認証

技術的管理措置　ーリスクと対応策

① OS（Windows）のID・パスワードの盗難

② 登録システムのID・パスワードの盗難

- ログインパスワードの条件（利用文字、文字数、利用期間）および再入力の失敗が一定回数を超えた場合のブロック方法（入力回数制限等）を設定
- 有効期間を設定してパスワードは定期的に変更
- パスワードを記録しておく場合は厳重に保管

③ 離職者等による登録システムの（遊休）IDの悪用

- 離職者のIDは速やかに削除（もしくはパスワードを変更）する
- IDの棚卸点検を実施し、遊休のIDが無いかをチェックする
- IDを共有することはできる限り避け各個人が固有のIDを持つようにする
- 登録システムへのログインは自分のID/パスワードで行う

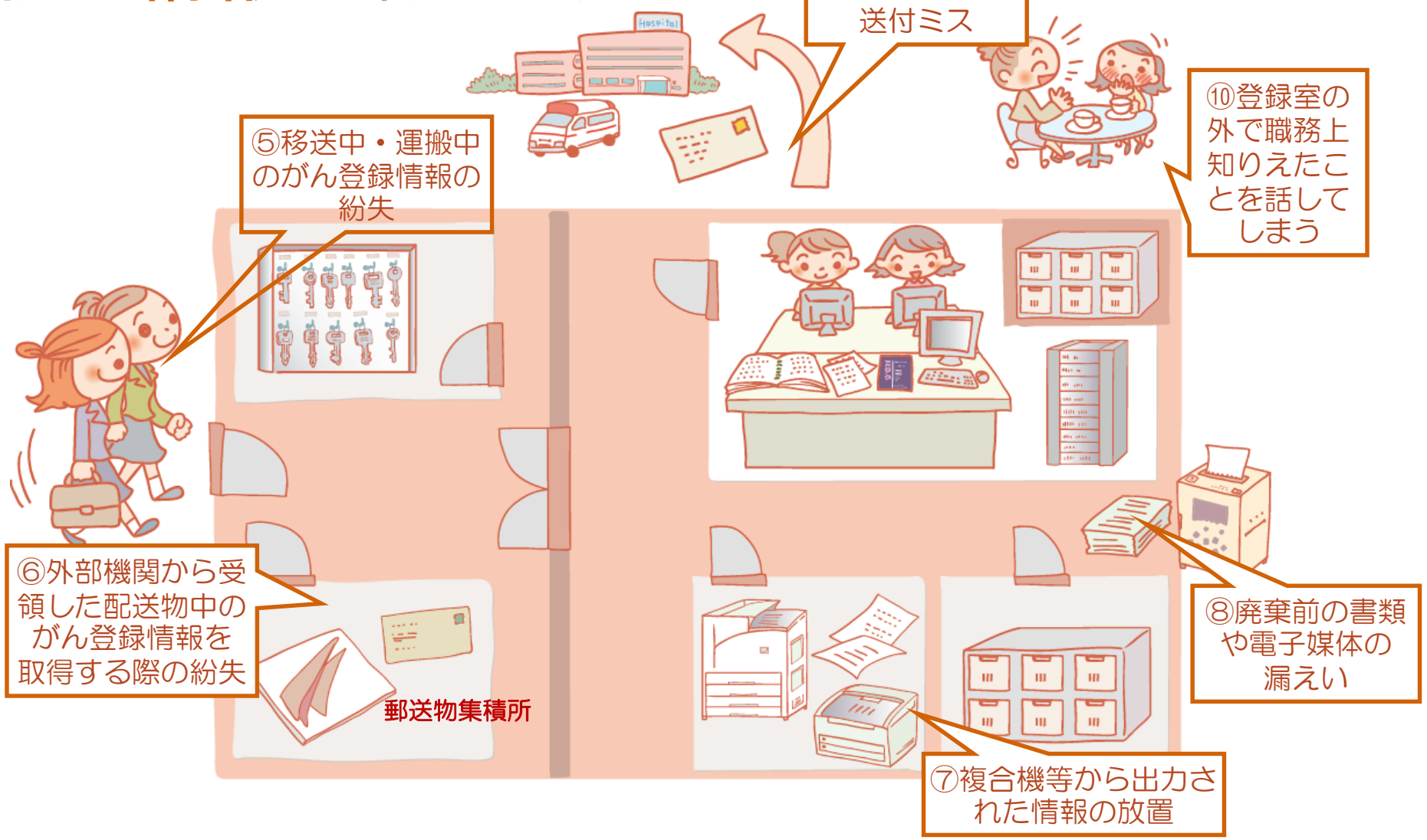
④ 委託業者による登録システムの特権ID悪用

- 委託業者のシステムアクセス時に立ち会う

⑤ 外部記憶媒体による不正プログラム等混入

- 外部記憶媒体については登録システムに接続する前にウィルスチェックを行い不正なプログラム等が混入していない事を確認する

登録室の外における個人情報の漏えいリスク



登録室外で部外者に個人情報を漏らさないための対策

⑤　移送・運搬中（登録室外）の紛失
- 移送中は常に人が付くようにする

⑥　受領資料を取得する際の紛失
- 追跡サービス付きの配送の利用
- 集配所の安全管理措置の確認

⑦　印刷紙・コピー紙の放置
- コピー機やプリンターに出力した紙を放置しない（確認の徹底）

⑧ 廃棄時の漏洩
- 消去・廃棄の作業場所を限定し、作業記録を残す

⑨ 外部照会する資料の問合せ作業、送付のミス
- 電話による照会の利用条件の限定
- 宛先の再確認もしくは複数名でのダブルチェック
- 追跡サービス付きの配送を利用

⑩ 登録室の外で職務上知り得た事を話してしまう。
- 職員に対する守秘義務教育の徹底

その他

- 外部からの問合せ
  - 個人情報に関する問合せには一切回答しない
    - 回答は作業責任者に限定
  - 医療機関からの個人情報に関する電話による問い合わせ
    - 作業責任者から必ず電話をかけ直す。
  - 個人情報の提供と関連する問合せに関して、日付、相手、内容、回答、対応者を項目に含む記録簿に記入して施錠保管する。

- 従事者への教育の実施
  - 着任者に対し。登録室責任者から規程等や役割と着任に関する説明
  - 従事者に対する最低年1回の安全管理措置の教育とテストの実施、受講記録、テスト結果の取得
  - 離職者に対する登録室責任者からの秘密保持に関する説明

事故や事故を誘発しかねない事情を発見した場合には速やかに報告

- 情報漏えいや、それにむすびついかねない事象（インシデント）が発生した場合、その事象や対応状況を速やかに管理者へ報告する

- **報告しなければならない事象**
- 情報管理やシステム運用上に関して保安上の脅威となる現象や事案
  - 個人情報の紛失や盗難
  - 鍵の紛失
  - メールや郵送物の誤送信
  - ウィルス感染
  - システム障害　など

業務の確実性への対応

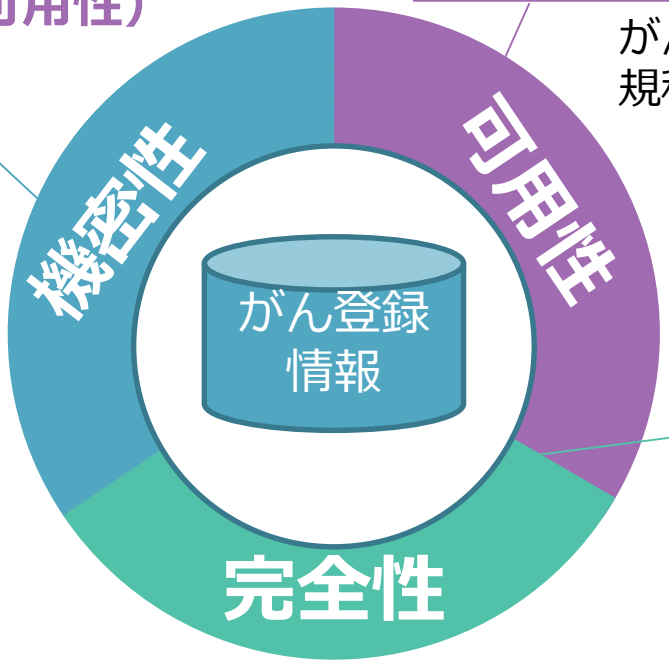
情報セキュリティ3要素からみた業務保全の考え

- 情報セキュリティの3要素とは
  1. C: Confidentiality（機密性）
  2. I: Integrity（完全性）
  3. **A: Availability（可用性）**

<u>業務保全対策</u>
障害や天災等による業務中断を防ぐため、必要なときに必要な情報資源を利用できる状態を維持すること

がん登録データのバックアップ規程や手順書の最新化

<u>情報漏えい対策</u>
情報漏えいやなりすまし等を防ぐため、アクセスを許可された者だけが情報にアクセスできることを確実にする



<u>がん登録情報保全対策</u>
情報の正確性や完全性が維持されること

がん登録業務時の入力内容確認など

登録データの消失を防ぐための基本的な考え方

- システム障害や災害等により過去の登録データがなくなってしまうことを防ぐとともに、登録データの復旧遅延を最小化する

- バックアップデータを取得する
  - 登録システムのデータベースバックアップは、登録作業後毎日作成
- バックアップデータは登録システムとは別の部屋で管理
  - 火災、地震に備え、バックアップ媒体はサーバ設置場所と分離する

愛知県がん登録においても、安全管理措置マニュアルに沿った安全管理措置を実施しています。

統括責任者
愛知県知事　大村秀章
愛知県保健医療局健康医務部健康対策課　古川大祐
登録室責任者
愛知県がんセンター がん情報対策研究分野　伊藤秀美
作業責任者
愛知県保健医療局健康医務部健康対策課　森佐代美