資料３

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（案）について

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とは

- **情報が外部に漏れないように管理すること（紛失、窃視や盗難の防止）**

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
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守ること
登録室の外で部外者に個人情報を漏らさないための対策
事故や事故を誘発しかねない事象を発見した場合は速やかに報告

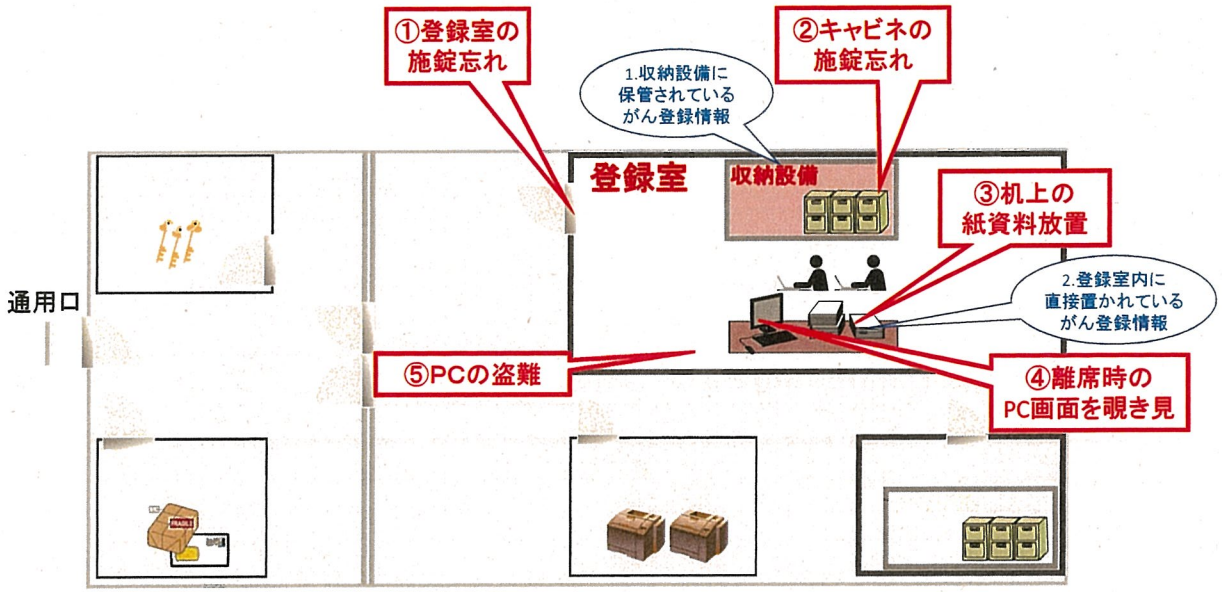
- **情報が消失することがないように管理すること（バックアップを取得し安全な場所に保管）**

登録データの復旧遅延を最小化するための対策

情報が外部に漏れないように管理する

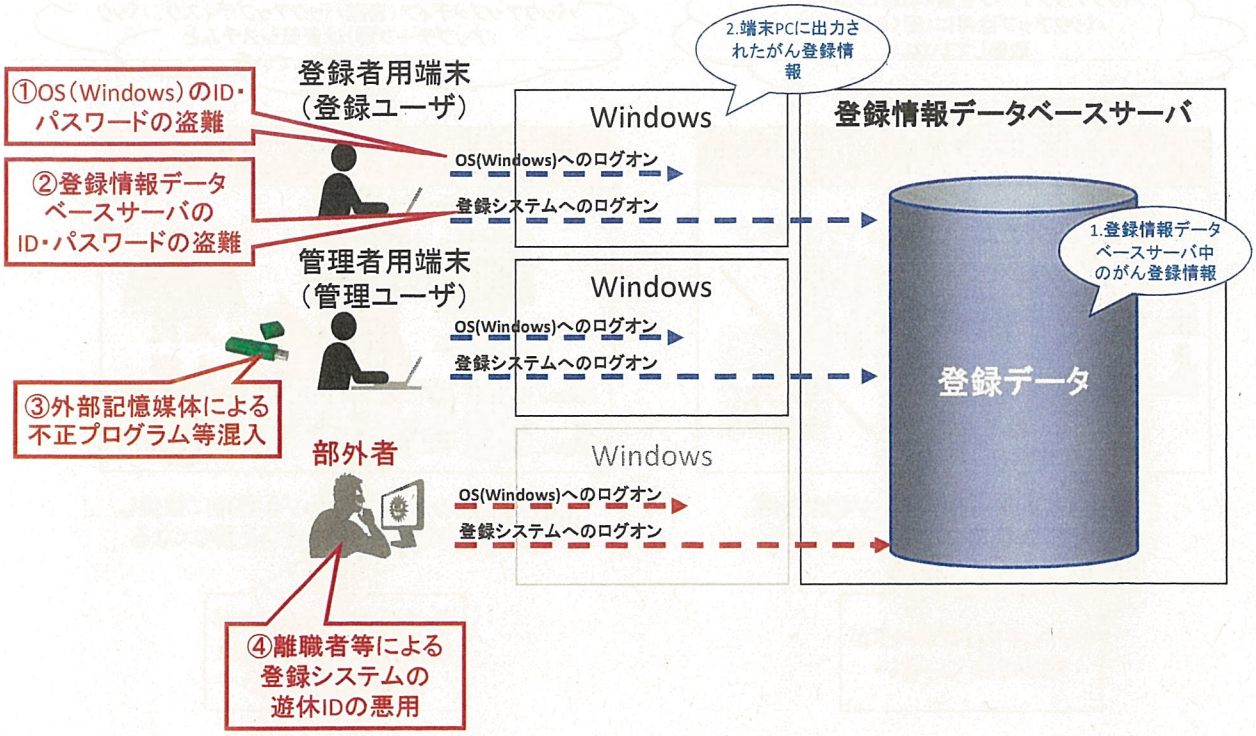
登録室内における個人情報の漏えいリスク

保護すべき情報　リスク



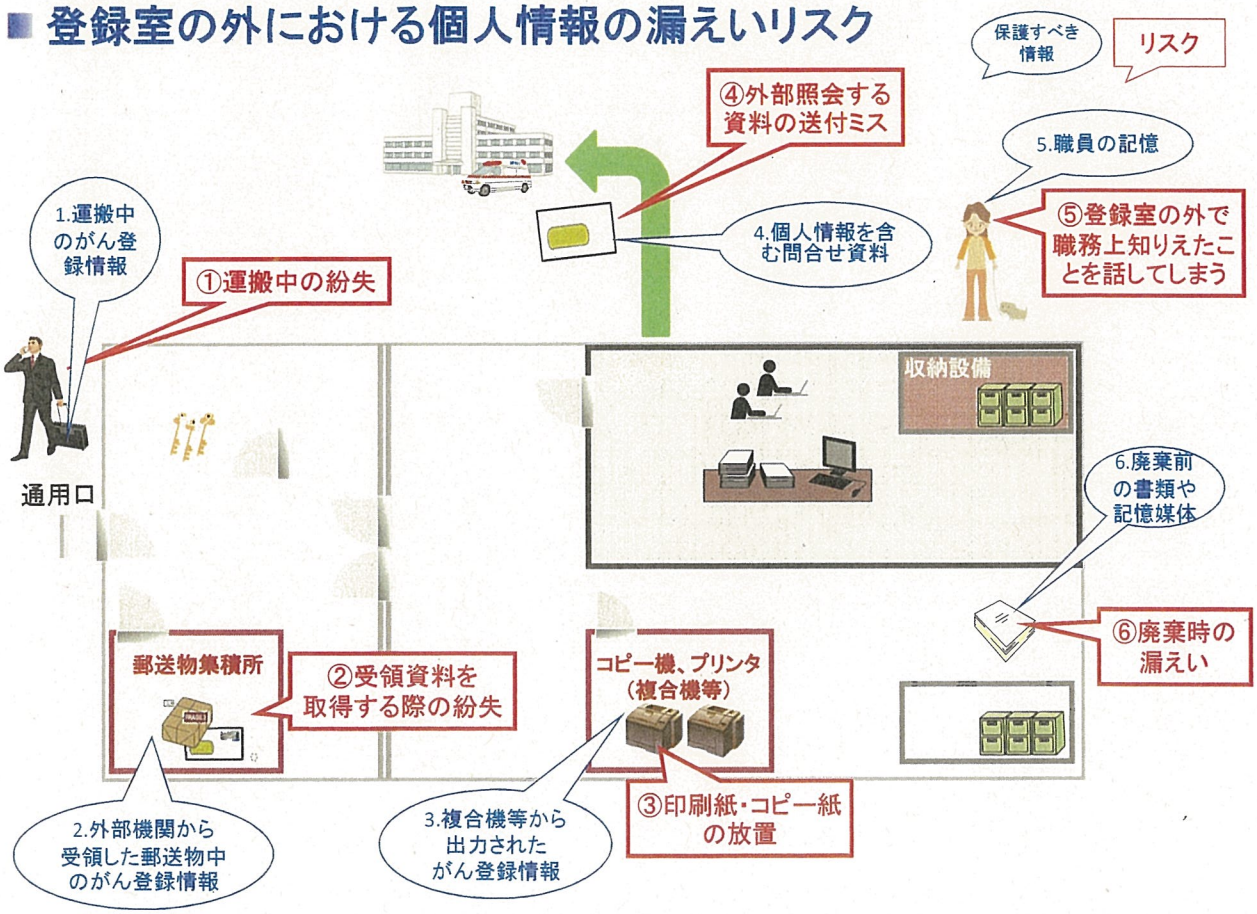
保護すべき情報　リスク

■ 登録システム中のデータの漏えいにつながる可能性があるリスク



■ 登録室の外における個人情報の漏えいリスク

保護すべき情報　リスク



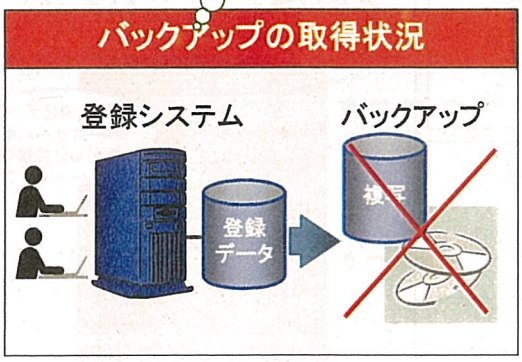
情報が消失することがないように管理する

■ 登録データの消失を防ぐ上で想定すべきリスク

現場での判断ミスの例

リスク

バックアップテープを置く場所はないので
バックアップは月に1回くらいしか
取得していない



登録システムデータベースが壊れた際、
1ヶ月前の状態にしか戻せなくなる

①バックアップデータが
取得されていない

登録室の中が一番安全なので、
バックアップメディア（自動バックアップディスク、バックアップテープ等）は登録システムと
同室内に保管している

登録システムもバックアップも同時に被災し
1から登録作業をやり直さざるを得なくなる

②バックアップデータが
登録システムと別個に
管理されていない

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　目　次

Ⅳ. 基本的な安全管理対策

1. 組織的安全管理対策

国及び都道府県がん登録室の管理責任者は、国及び都道府県がん登録室における安全管理について、登録室職員の責任と権限を明確に定め、安全管理に関する規程や手順書(以下、「規程等」と言う。)を整備運用し、その実施状況を日常の自己点検等によって確認しなければならない。組織的安全管理対策には以下の事項が含まれる。

(1) 安全管理対策を講じるための組織体制の整備
(2) 安全管理対策を定める規程等の整備と規程等に従った運用
(3) 個人情報の取扱状況を一覧できる手段の整備
(4) 国及び都道府県がん登録室の安全管理対策の評価、見直し及び改善
(5) 事故(情報の漏えい等)又は違反(従事者の運用管理規程違反等)への対処

2. 物理的安全管理対策

国及び都道府県がん登録室の業務においては、がんの診断や予後に関する情報を紙媒体、電子媒体、あるいはデータベースサーバ等の情報機器の中で保管・管理を行っている。これらの媒体や機器を管理するにあたっては、盗難、紛失、窃視等を防止する物理的な安全対策を講じなければならない。物理的安全管理対策には以下の事項が含まれる。

(1) 登録室の入退室の管理
(2) 盗難、窃視等の防止
(3) 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

事業の実施体制によっては、都道府県がん登録室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。

3. 技術的安全管理対策

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。しかし、その有効範囲を認識し適切な適用を行えば、これらは強力な手段となりうる。技術的安全管理対策には以下の事項が含まれる。

(1) 担当職員の識別及び認証
(2) 情報の区分管理とアクセス権限の管理
(3) アクセスの記録(アクセスログ)
(4) 不正ソフトウェア対策
(5) ネットワーク上からの不正アクセス対応

4. 人的安全管理対策

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、教育・訓練等を行

うことを言う。

V. 作業内容から見た安全管理対策

本項では、国及び都道府県がん登録室の作業内容に沿って、基本的な安全管理対策を踏まえて、マニュアルに記述するべき内容と対策を示す。各作業項目では、作業責任者と作業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記述する。

1. 入退室管理

可能な限り他の業務から独立した登録室を確保し、入退室の手続きを定め、権限のない者が登録室に入退室することを防ぐ。

2. 取得

国及び都道府県がん登録室で取得する個人情報には、以下のものが含まれる。電子ファイルによる取得がある場合は、紙と電子ファイルそれぞれについて整理する。

(1) 所定の届出票・遡り調査票
(2) 死亡者情報票
(3) (研究利用) 研究対象者ファイル

3. 入力

入力とは、取得した個人情報を含む資料（届出票、遡り調査票、死亡者情報票）の入力作業（電子的インポート含む）を言う。

4. 利用・加工

利用・加工には以下を含む。

(1) 電子ファイルで取得した個人情報を含む資料の入力前処理
(2) データ入力以外の登録作業
(3) 研究利用への対応

5. 保管・匿名化・消去・廃棄

ここで言う「保管」とは、一連の登録作業及び抽出・利用・加工の処理が終了した後、一定期間の保管が法第 27 条に定められている個人情報を言う。予め定めた保管期間を過ぎたもの、あるいは保管期間内であっても不要となったデータは、速やかに、安全に、廃棄する。**別紙 3「個人情報の保管及び廃棄に関する一覧」**に沿って、保管・消去・廃棄の担当者と手続きを記述する。

6. バックアップ

データベースファイルの損失や、データの保存されたコンピュータの故障に備えて、国は、登録用アプリケーションとデータベースファイルを定期的にバックアップし、適切に保存する。

7. システム管理

登録システム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、プログラムの異常などの障害対応やソフトウェア改訂がある。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がん登録資料の利用、データベースに保存されたデータを救済するためにがん登録資料へのアクセスが必要な場合がある。また、都道府県がんデータベースの整備等、これまでに使用していた地域がん登録のデータベースシステムから、新しく導入するデータベースシステムへがん登録資料を移行する場合に、外部の保守要員や開発者が管理者モードで直接がん登録資料に触れる可能性があり、安全保護対策が必要である。

8. 国がん登録室から都道府県がん登録室又は市町村等への問い合わせ、都道府県がん登録室からの病院等への問い合わせ

登録の内容に疑義が生じた場合や、登録作業において他の資料を参照することが有効な手段である場合（例：患者同定における住民票照会）に、国がん登録室から都道府県がん登録室又は市町村等への問い合わせをして、作業を進める。また、届出票の記載内容に不備がある場合、都道府県がん登録室から、病院等に問い合わせて正確な情報の収集に努めることは、全国がん登録の精度向上のみならず、当該病院等の院内がん登録などの精度向上にも重要である。

9. 外部からの問い合わせ

外部からの問い合わせは、問い合わせ者と問い合わせ内容別に対応者と手続きを定める。問い合わせ者には以下が含まれる。

(1) 国立がん研究センター、医師会、市町村、保健所、都道府県庁、他県の都道府県がん登録室、及び協力病院等

(2) 新聞、雑誌、テレビなどのマスメディア

(3) 患者、患者の家族、一般市民

10. 移送

個人情報の郵送には、配達記録が残る形のものを利用することを推奨する。個人識別情報と腫瘍情報とを分離して送付し、受け取り側で権限のある者のみが両者をリンクしうる手段も検討する。電子データでは、個人情報の暗号化と特別なキーによる解読は、分離して送付する手続きの代替となる。送付における資料の物理的な安全保護と機密保持を確実にするための注意が払われるべきである。権限のない者がデータを容易に読むことができないことを確実にするための措置に加えて、不正な、ないし損なわれたファイルをチェックする手段を用意しておかなければならない。