患者さんの「たいせつな情報」の旅

医療や介護の現場で働くIT担当者のための、個人情報保護のはじめの一歩。

この資料では、患者さんの大切な情報が、どのように生まれ、使われ、
そして守られるべきなのか、その「旅」を一緒にたどっていきます。

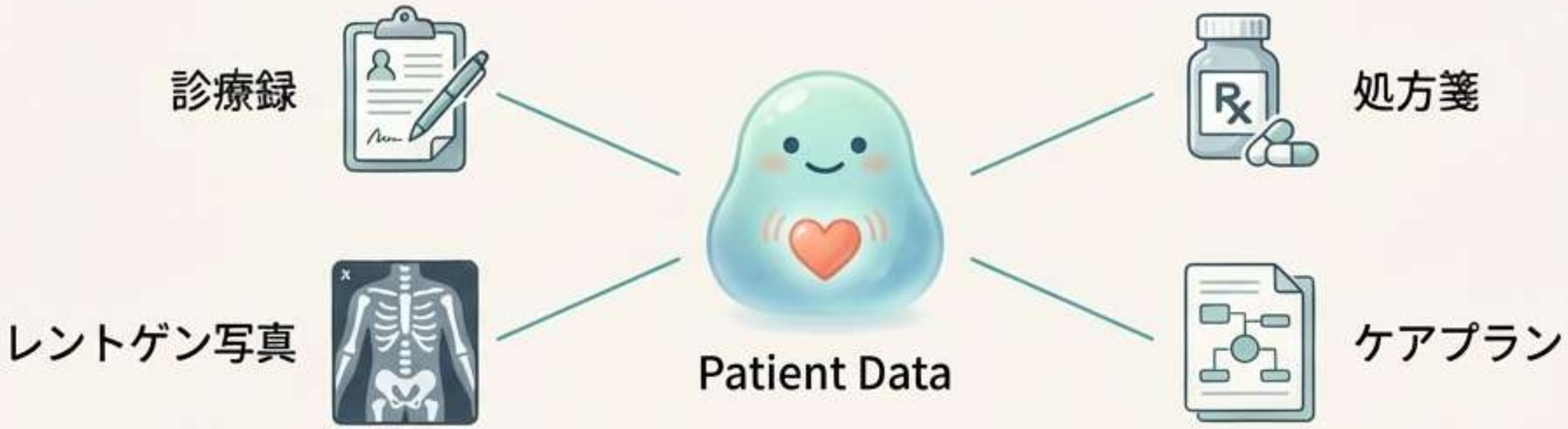
なぜ、この情報が「たいせつ」なのか？

- 医療・介護サービスの基本は、患者さん・利用者さんとの「信頼関係」です。
- 病歴や健康状態といった情報は、最もプライベートでデリケートなもの。
- この情報を適切に扱うことが、安心できる医療の提供と、その信頼を守るための基盤となります。
- 「ルールだから守る」のではなく、「信頼を守るために」ルールがあるのです。

旅のはじまり：そもそも「個人情報」って何？

「個人情報」とは、生きている個人に関する情報で、特定の個人を識別できるすべてのものを指します。(法第2条第1項)

これらすべてが個人情報です:



- 氏名、生年月日、住所、顔写真など

医療・介護の現場では、例えば…

- 診療録、処方箋、手術記録
- 検査所見記録、エックス線写真
- ケアプラン、介護サービスの提供記録

(出典: 別表 1 記録例)

特にデリケートな「要配慮個人情報」

個人情報の中でも、特に不当な差別や偏見が生じないよう、**取り扱いに特別な配慮が必要な情報を「要配慮個人情報」**と呼びます。（法第2条第3項）

- 本人の同意なく取得することは、原則として禁止されています。

具体例：

- **病歴**：これまでの病気や治療の記録
- **心身の障害**：身体障害、知的障害、精神障害など
- **健康診断の結果**：検査の数値や医師の所見
- **診療や調剤の情報**：医師による指導や、処方された薬の情報

（出典：II 3. 要配慮個人情報）

旅の目的：情報は「何のために」使うのか？

- 個人情報を取り扱う際は、あらかじめ**「何のために使うのか（利用目的）」を具体的に決める**必要があります。（法第17条）
- そして、**決めた目的の範囲を超えて、勝手に情報を使ってはいけません。**（法第18条）これを**「目的外利用の禁止」**といいます。
- 利用目的は、院内掲示やホームページなどで、患者さん・利用者さんに分かりやすく**公表**する必要があります。

医療・介護の現場で想定される「利用目的」

院内・事業所内での利用

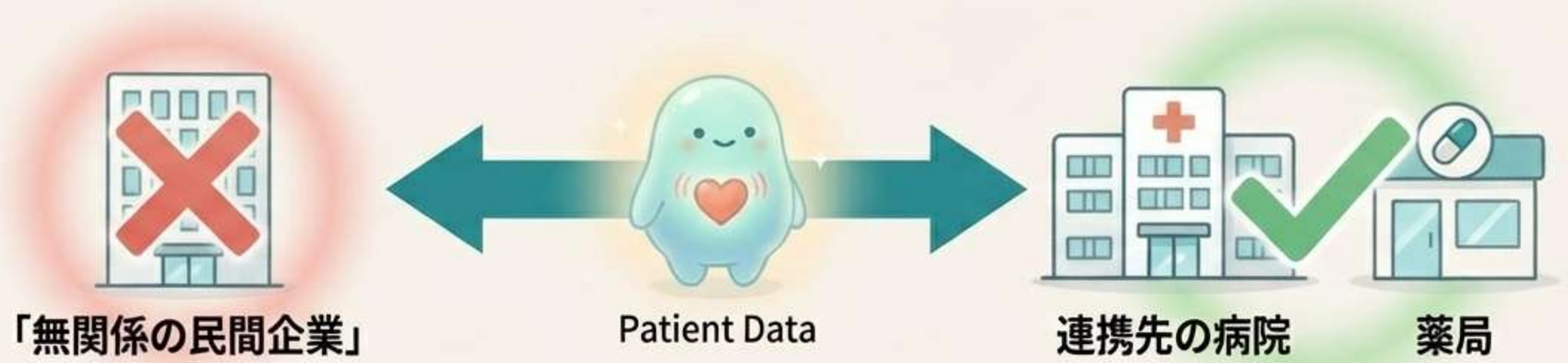
- 患者さんへの医療サービスの提供
- 医療保険事務（レセプト作成など）
- 入退院の病棟管理、会計・経理
- 医療サービスの質の向上、院内での研究や実習

他の事業者等への情報提供

- 他の病院、診療所、薬局などとの連携
- 他の医療機関からの照会への回答
- 外部の医師への意見・助言の依頼
- 検体検査業務などの外部委託
- 家族等への病状説明
- 審査支払機関へのレセプト提出

（出典：別表２ 利用目的例）

旅の仲間：情報は「誰と」共有できる？



個人データを他の事業者などの「第三者」に提供するには、原則としてあらかじめ本人の同意**が必要です。**（法第27条）

同意が必要な例：

- 民間保険会社からの照会への回答
- 職場や学校からの問い合わせへの回答
- マーケティング会社からの照会への回答

たとえ相手が誰であっても、「本人の同意」が基本ルールです。

「本人の同意」の考え方

原則は「明確な同意」ですが、例外もあります。

- **黙示の同意**：
  - 患者さんへの医療提供に必要な目的（他の病院との連携など）を院内に掲示し、患者さんから特に反対の意思表示がない場合、同意が得られているものと見なせます。（Ⅳ 9.(3)）
  - この場合でも、患者さんはいつでも同意を撤回できます。
- **同意が不要な場合**：
  - 法令に基づく場合（例：感染症の届出）
  - 人の生命や身体を守るために必要で、本人の同意取得が困難な場合（例：意識不明の患者の家族への説明）

（出典：Ⅳ 9.(2) 第三者提供の例外, Ⅳ 9.(3) 本人の同意が得られていると考えられる場合）

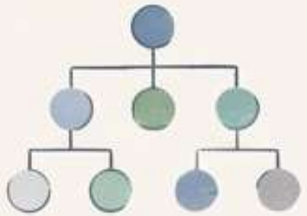
旅の守り人：どうやって情報を守るのか？

個人データを安全に管理するため、法律は事業者に「安全管理措置」を講じることを義務付けています。（法第23条）
これは、情報漏えい、紛失、改ざんなどを防ぐための具体的な取り組みです。
安全管理措置は、大きく４つのカテゴリーに分けられます。

1. 組織的安全管理措置：ルールと体制づくり
2. 人的安全管理措置：スタッフへの教育と監督
3. 物理的安全管理措置：モノや場所の管理
4. 技術的安全管理措置：ITシステムによる防御

4つの安全対策①：組織と人による守り

組織的安全管理措置



「個人情報保護委員会」

- 個人情報保護に関する院内規程の整備
- 責任者の設置や、推進のための委員会を組織
- 漏えい事故などが発生した際の報告連絡体制の構築
- 定期的な自己評価と見直し

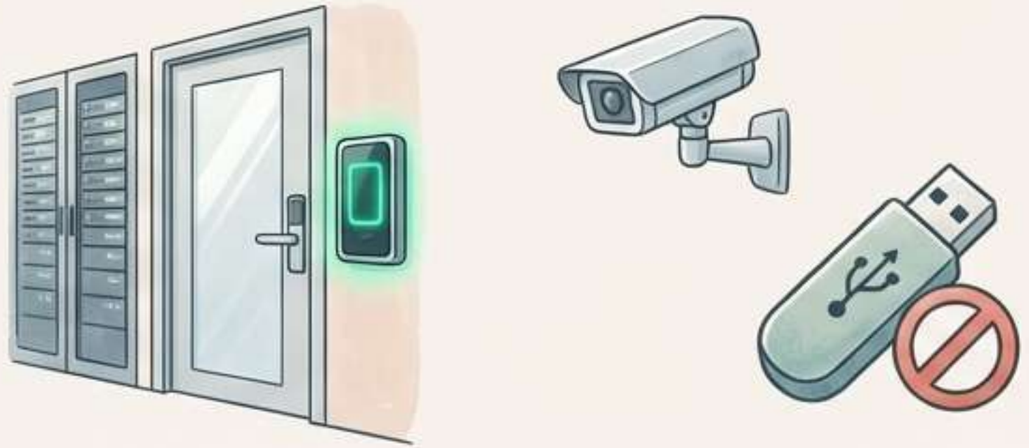
人的安全管理措置

- 全従業者（派遣・委託含む）との守秘義務契約
- 従業者に対する定期的な教育・研修の実施
- 個人データへのアクセス権限の適切な管理・監督

（出典：Ⅳ 7.(2) ②, ③, ④, ⑤）

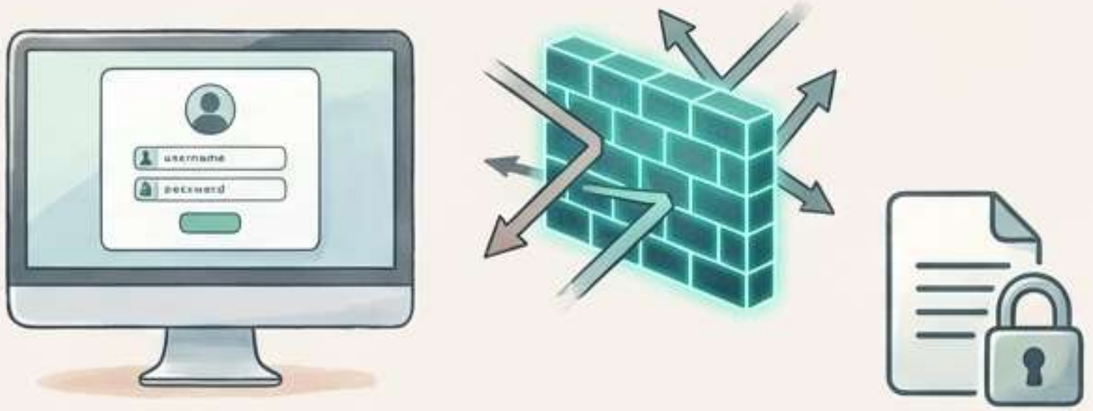
4つの安全対策②：物理的・技術的な守り

物理的安全管理措置



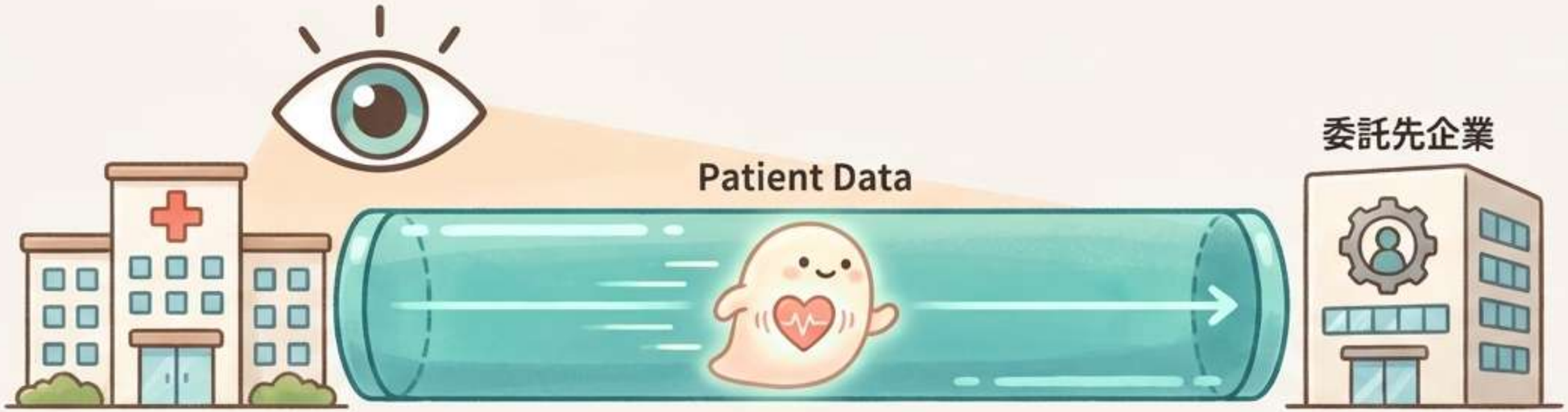
- 重要な情報システムを管理する部屋への入退室管理
- PCやサーバーラックの盗難防止措置（ワイヤーロックなど）
- 個人データを含む書類や媒体の施錠保管
- 不要になったデータの確実な廃棄・消去（物理破壊、データ消去ソフト）

技術的安全管理措置



- アクセス制御（ID・パスワード、二要素認証の導入）
- アクセス記録（ログ）の保存と定期的な確認
- 外部からの不正アクセス対策（ファイアウォールの設置）
- ソフトウェアの脆弱性対策（セキュリティパッチの適用）

（出典: Ⅳ 7.(2



外部のパートナーも旅の仲間：委託先の監督

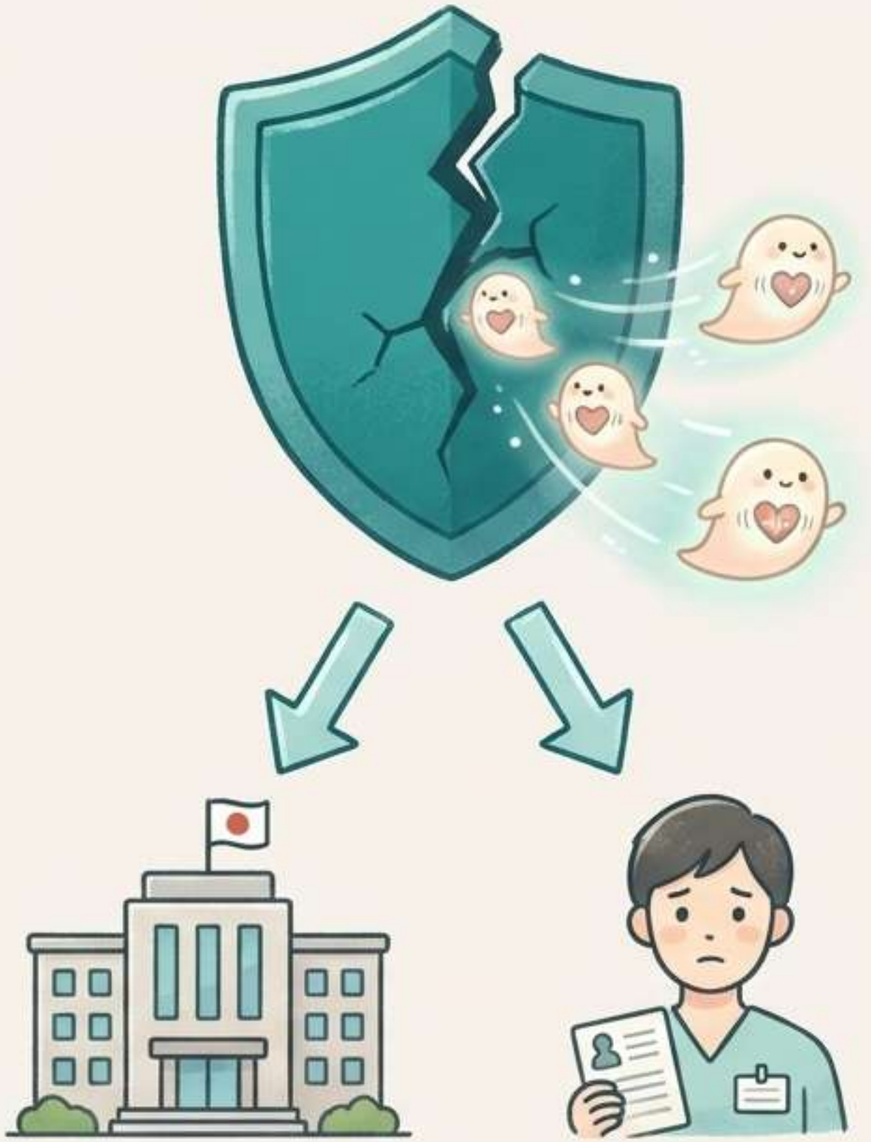
検査業務やシステムの保守など、個人データの取扱いを外部に委託することはよくあります。

- この場合、委託した側（医療・介護事業者）は、委託先がデータを安全に管理しているか**必要かつ適切に監督する義務**を負います。（法第25条）

****監督のポイント**：**

1. **選定**：適切な安全管理体制を持つ事業者を委託先に選ぶ。
2. **契約**：契約書で、データの取扱いに関するルール（再委託の可否など）を明確にする。
3. **確認**：委託先が適切に業務を行っているか、定期的に状況を確認する。

万が一、委託先で問題が起きれば、委託元の責任も問われます。



もしもの時：情報が漏えいしてしまったら

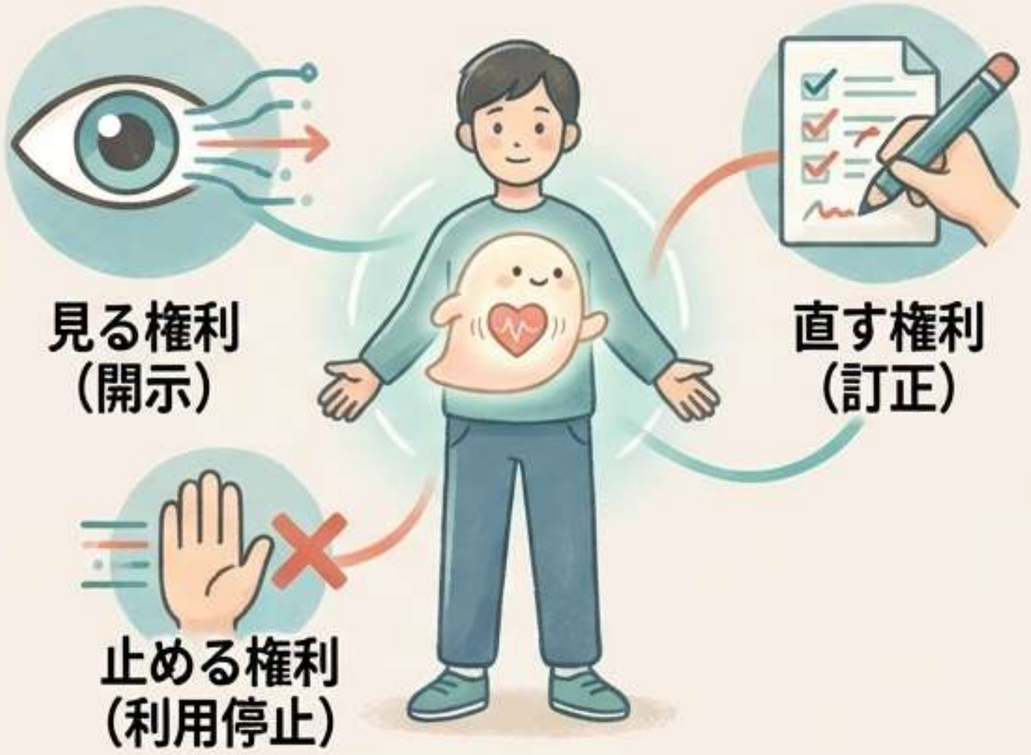
- 個人データの漏えい、滅失、毀損などが発生した場合、法律に基づく対応が必要です。（法第26条）
- 特に、個人の権利利益を害するおそれが大きい事態では、**個人情報保護委員会への報告**と、**本人への通知**が義務付付けられています。
- **報告・通知が義務となる主なケース：**
  1. **要配慮個人情報**（病歴など）が含まれるデータの漏えい
  2. 不正利用により財産的被害が生じるおそれがある漏えい（クレジットカード情報など）
  3. 不正な目的による、サイバー攻撃などの漏えい
  4. **1,000人分を超える**個人データの漏えい
- 「発生したおそれ」がある段階でも、迅速な報告・通知が必要です。

（出典: Ⅳ 8. 漏えい等の報告等, 対

旅の主役は患者さん：本人の「権利」

個人情報は、患者さん・利用者さん本人のものです。
そのため、本人には自身の情報に対して以下の権利が認められています。

- **開示請求権（法第33条）**
  - 自分の情報がどのように記録されているか、開示を求める権利。



- **訂正・追加・削除請求権（法第34条）**
  - 情報の内容が事実と異なる場合に、訂正などを求める権利。

- **利用停止・消去・第三者提供の停止請求権（法第35条）**
  - 情報がルール違反で取り扱われている場合に、利用停止などを求める権利。

これらの請求には、定められた手続きに従い、遅滞なく対応する必要があります。

「たいせつな情報」を守ることは、患者さんの「信頼」を守ること

- 患者さんの個人情報の旅は、
  一つひとつのデータを個人情報の旅は、日々の業務の中にあります。
  それが、医療・介護の現場で最も重要な「信頼」を築き、守り続けることに繋がります。
- IT担当者として、私たちはこの旅の最も重要な「守り人」の一員です。