

# RECIKA

## ブロックチェーンを利用した患者を中心とした医療データ共有の仕組み

Prepared for 第2回ブロックチェーンセキュリティワークショップ  
Oct 25<sup>th</sup>, 2022

### 企業概要

会社名	株式会社レシカ
設立	2018年12月1日
所在地	東京都千代田区大手町1丁目6番1号 大手町ビル6階 Inspired. Lab
代表	代表兼CEO：戴有造 Chris Dai UniCask共同創設者兼CEO。以前はCOO / CIO Yixing SCM（ロジスティクス・プロバイダー）複数のベンチャーを立ち上げる。Accentureのコンサルタント、BitcoinとEthereumの初期の投資家の一人。2004年にスタンフォード大学で管理科学と工学を専攻し、B.S.を取得。RIETIブロックチェーン技術の将来性に関する研究会委員
リーガルアドバイザー	増島 雅和(森・濱田松本法律事務所)

### 提供サービス/実績

提供サービス	<ul style="list-style-type: none"> <li>•<b>ブロックチェーン活用に向けたWeb3.0コンサルティング</b> <ul style="list-style-type: none"> <li>- 大手企業・独立行政法人とPoCを多数実施</li> </ul> </li> <li>•<b>ライブ配信・コンテンツ販売「livesola」開発</b> <ul style="list-style-type: none"> <li>- プラットフォームに依存しない配信が可能</li> <li>- NFTを含むコンテンツを販売</li> </ul> </li> <li>•<b>実物資産 x N F T「UniCask」開発</b></li> </ul>
弊社コンサルティング実績	<ul style="list-style-type: none"> <li>•<b>大手広告代理店</b>：ブロックチェーンを活用した分散型データプラットフォームの構築に向けて、飲食のレコメンデーションのユースケースに対して、サービス設計及びシステム構築に向けた要件を整理</li> <li>•<b>大手自動車会社</b>：ブロックチェーンを活用した、モビリティビジネスのユースケースを抽出。その中から優先度の高いユースケースに対し、サービス設計及びシステム構築に向けた要件を整理(車両履歴レポート市場を対象とした車両使用状況の監視、P2Pカーシェアリング等)</li> <li>•<b>独立行政法人(大学病院)</b>：ブロックチェーンを活用したデータ管理を目指し、アクセス申請・承認、データ参照のログをブロックチェーン上に書き込み、患者・複数の病院の医師間でセキュアにデータを共有する仕組みについて、PoCを実施</li> </ul>

# アジェンダ

- 1. なぜ医療にブロックチェーン？**
- 2. 医療×ブロックチェーンの構想**
- 3. 千葉大病院との本検証プロジェクトの概要**
- 4. ゲノムデータの将来性**

# 1. なぜ医療にブロックチェーン？

# ブロックチェーン101

## 医療分野でのデータ管理の課題

**院内システムによりスタンダードが乱立**

病院のシステムは多くのソフトウェアベンダーによって作成されており、スタンダードが乱立しており互換性がない。

**クラウドは基本信用していない**

基本的にクラウドは信頼できないという認識をもっている。

**病院間のやり取りはFAXが基本**

FAXは病院間の情報通信によく使われており、人件費が多くかかっている。

**患者の合意は紙で管理している。**

合意は基本紙で患者に署名して合意を取っており、しかし合意された内容を後で患者がチェックしたり、許可を取り下げたりはほとんどの場合できない。

## 非中央集権

- 中央管理者不在の、自立分散的なネットワーク。

## 改竄・偽造不可

- 電子署名やハッシュ関数などの暗号技術や、経済インセンティブに基づいた合意形成メカニズムを用いて、データが改竄・偽造される可能性を限りなくゼロに近づけている。

## ゼロダウンタイム

- 世界中に散らばった、マイナー（ノード）がゼロになるまでブロックチェーンは動き続ける。したがって事実上、停止することがないシステム。

# ブロックチェーンの活用

## パブリック・コンソーシアム・プライベートチェーン

	パブリックチェーン	コンソーシアムチェーン	プライベートチェーン
管理者	不在	有り(複数企業)	有り(1社のみ)
ノード参加者	誰でも参加可能	許可制	組織内のみ
トークン	有り	どちらでも可	どちらでも可
合意形成	PoW,PoS,Polなど	モデルに依る	モデルに依る
取引速度	遅い	速い	速い
スケーラビリティ	低い	高い	高い
ファイナリティ	困難	容易	容易
例	ビットコイン、イーサリアム	IBM、リブラ (Facebook)	-

## 2. 医療×ブロックチェーンの構想



# 構想1：患者主体の医療データ管理 本件でブロックチェーン技術を導入するメリット

本クライアントは、既に検診データをクラウド上で管理する仕組みを有していたことから、既存システムにブロックチェーンの層を追加する方法を採用。

これにより、既存の仕組みを活用しながら、医師や関係者の“誰”が“どの”診断情報を“いつ”参照し、アップデートしたかに関する確実な管理を実現。

## ◆ 既存の検診データ管理システムのデータ構造の変更が不要 (複数ユーザーによるクラウド上でのデータシェアを実現)

- ✓ 現状の仕組みの場合、利用する病院ごとにデータ構造やIF連携の仕様をカスタマイズする必要が生じるが、ブロックチェーンの技術導入により、病院ごとの仕様の変更は不要となる

## ◆ 二段階認証による厳重なユーザー管理の実現

- ✓ 病院・組織によるユーザー管理に加えて、患者からの権限承認の二段階でのユーザー管理を実施することにより、患者自身の個人データの参照・更新者を厳密に管理

## ◆ アクセスコントロールの容易さ

- ✓ 患者が複数病院での診断データを保持している場合、医師ごとに参照可能なデータの範囲を選択・コントロールすることが可能

## ◆ アプリや機能の追加の容易さ

- ✓ システム上に新しいアプリケーションを追加する場合、ユーザー認証データと診断データは、既存システムから継承されるため、データの確実性・安全性を担保しつつも、開発ボリュームを抑えることも可能

# 3. 千葉大病院との本検証プロジェクト の概要

## 1 まだ前例のない「DNA × ブロックチェーン」のプロジェクト

- ✓ 近年、ブロックチェーンを活用したプロジェクトは増えてつつあるものの、「DNA × ブロックチェーン」プロジェクトは日本ではまだ実践されていないため、関係者を含めた取り組みへの理解・協力を、いかに得られるかが成功へのカギ

## 2 適切な階層コントロール（セキュリティコントロール）

- ✓ 遺伝子データは非常に機密性の高い情報でもあることから、その内容によってアクセスできるユーザーを制限するなど、階層を切り分けた適切なコントロールが重要
- ✓ このアクセス制御のための階層コントロールは、特にGDPRや個人情報の保護に関する法律等にも準拠した対応が必要

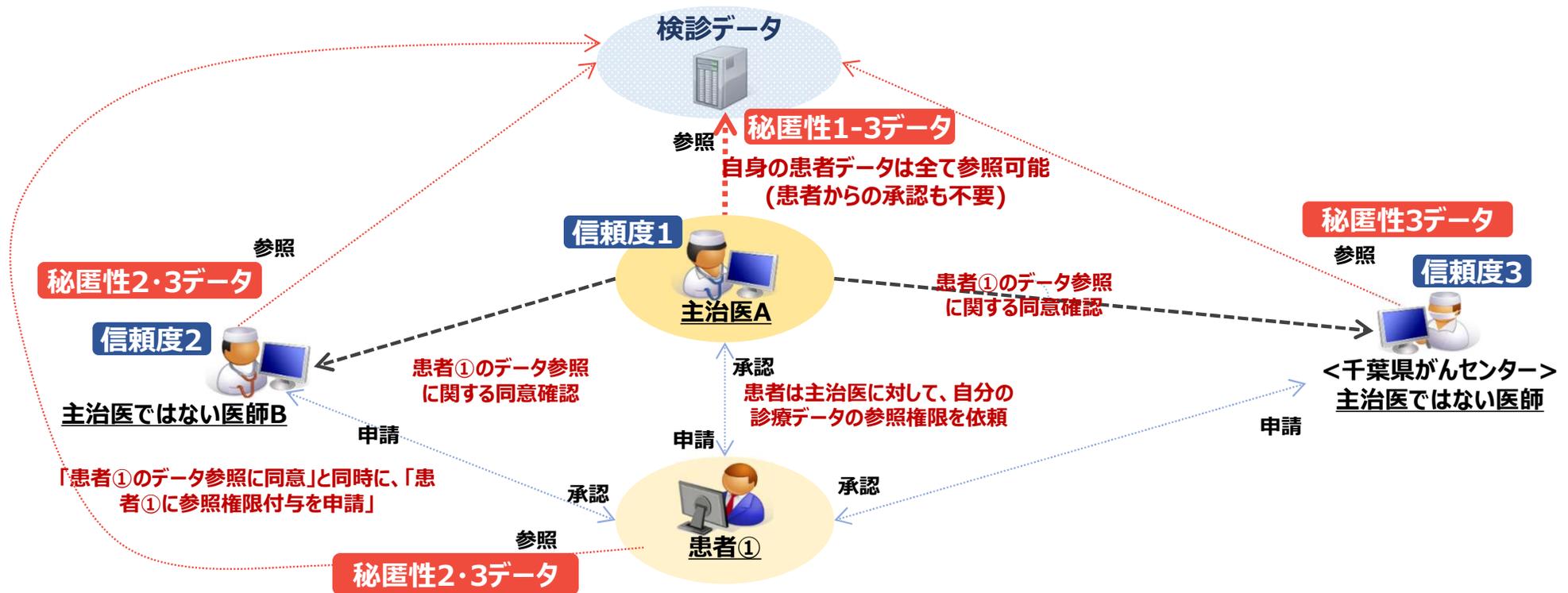
## 3 コストコントロールと費用の負担

- ✓ 本件においては、どの情報をブロックチェーンで管理するのかの範囲によってもコストボリュームが変動することから、利用時の安全なデータ管理とコストバランスを見極めた対応がポイント
- ✓ 現在は科学研究費で費用を補っていますが、将来的に費用負担がどのようにできるかが実用化のカギとなる。

## パイロット1の検証 全体像(イメージ)

パイロット1では、医師・患者などの複数ユーザーが、データを保有する患者の承認を踏まえて正しくデータ参照できるか否かを確認します。

本件において、主治医は自身の患者の全てのデータを患者からの承認無く参照することができますが、それ以外の医師は患者からの承認を踏まえて、医師自身の信頼度レベル×患者データの秘匿性レベルに応じたデータ参照が可能となります。



### アプリケーションのコンセプト

1. 患者本位の質の高い患者情報の共有方法の開発（ゲノム情報、家系図情報などを含む）。
2. 限定された使用者のネットワーク上で改ざん防止、追跡可能、記録の保存など。
3. 電子同意（本人確認含む）や患者側から医療情報の使用確認が可能（オプトアウト）。かつ医療者と患者の信頼度レベル（医療情報の質や量などレベルと主治医やセカンドオピニオンなどの取り扱い）の設定。
4. 将来的に厚労省が進めるオンライン診療（遠隔医療）の情報共有の補助ツールとして利用可能。

## パイロット1における検証のゴール

パイロット1の検証においては、患者データの秘匿性レベル1-3のデータと医師の信頼度レベル1-3を組み合わせたデータ参照の仕組みが技術的に実現できるか否かを検証すること

## パイロット1の検証方法は・・・

- 秘匿性レベル1・2・3のデータを設定するため、検証用に使うデータを1種類ずつ決定する
- 決定した秘匿性レベル1～3のデータに対して、信頼度1・2・3の医師がデータ参照する際の患者への承認依頼の有無、患者からの承認/否認の結果を踏まえた参照可否を確認する

### ■ 秘匿性レベルと信頼度レベルの組み合わせによるデータ参照の実現方法

\* 主治医は信頼度レベルに拠らず自身の持つ患者データは全て参照可能。その他の医師としてのみレベルに応じた参照可否が決まるイメージ。

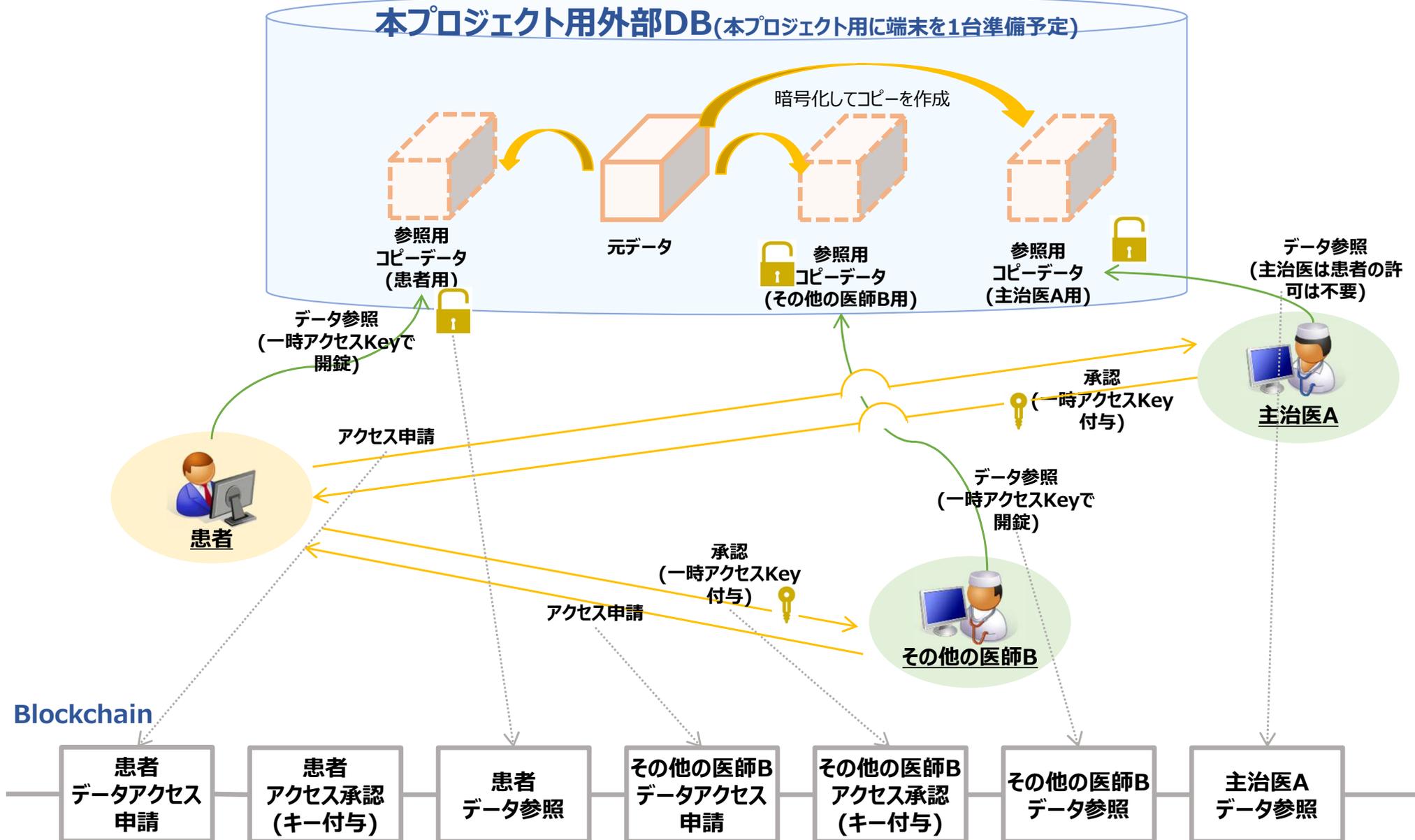
秘匿性 分類	主治医*	その他の医師としての信頼度*			患者
	1	2	3	4	
レベル1	いつでも参照可能	参照不可 ※参照の依頼もできない	参照不可 ※参照の依頼もできない	参照不可 ※参照の依頼もできない	参照不可 ※参照の依頼もできない
レベル2	いつでも参照可能	患者から承認された場合は参照可能	参照不可 ※参照の依頼もできない	参照不可 ※参照の依頼もできない	主治医から承認された場合は参照可能
レベル3	いつでも参照可能	患者から承認された場合は参照可能	患者から承認された場合は参照可能	参照不可 ※参照の依頼もできない	主治医から承認された場合は参照可能

高  
↑  
低

## パイロット1の検証

### 【参考】データアクセスによるブロックチェーン書き込みのイメージ

ブロックチェーンを活用したデータ管理においては、アクセス申請・承認、データ参照のログをブロックチェーン上に書き込み、適切に管理できているかを確認する。



## 検証項目

## 検証内容

### ユーザー 管理

- ユーザー：患者、医師
- ※患者は、病院での診察時に利用申請することで、主治医から利用権限を付与される想定だが、本検証においては、既にアプリケーション利用は可能な状態で検証を開始

### アクセス コント ロール

- 個人のプライベートキーに依存したアクセスコントロール
- 主治医、その他の医師のパターンによるアクセスコントロール
- ① **患者**は主治医からの承認があるまでデータアクセスは不可。
- ② **主治医**は自身の患者データは患者の承認は不要。いつでもアクセス可能。
- ③ **主治医以外の医者**は患者の承認を以って患者データへのアクセスが可能。
- ユーザーのトラストレベル (医師(主治医、その他の医師)、患者)と診療データの秘匿性レベルに応じたアクセスコントロール

### アクセス ログ

- Blockchainでのログ管理
  - ✓ データ参照のリクエストログ
  - ✓ データアクセスの承認ログ
  - ✓ データへのアクセス&参照ログ
  - ✓ チャット(テキストMsg)書き込み時のアクセスログ

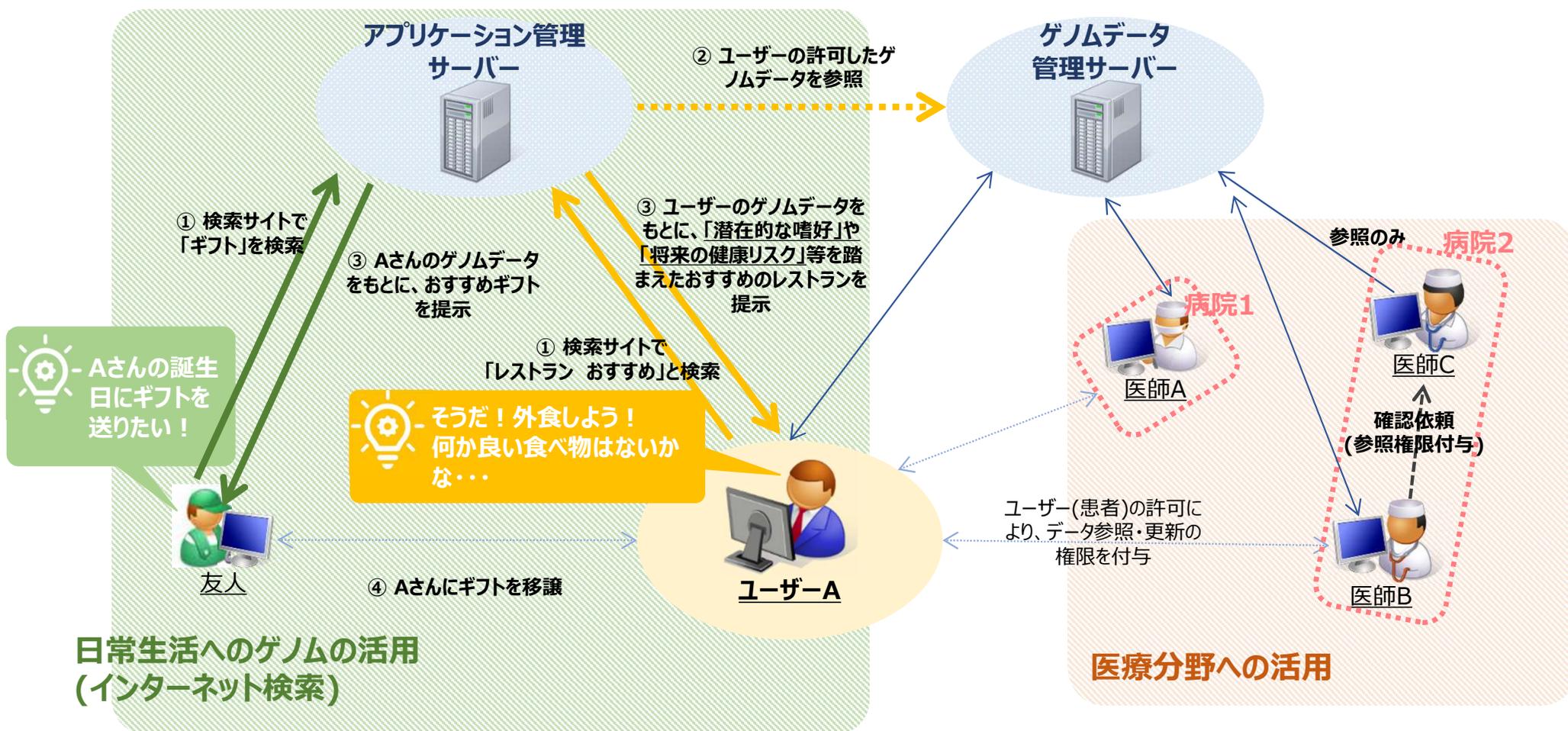
### クワイテリア

- 複数種類のユーザー間でのアクセス申請/承認・同一データの参照
- 外部からの攻撃への耐性(情報流出しない・データ改ざんされない)
- 2段階でのセキュリティコントロール  
(ユーザーパスワードを盗まれてもデータ参照されない など)

#	シナリオ	概要
0	ログイン	患者・医師がWebサービスを利用する場合に、ログインを行う
1	患者による診察データの参照	患者が自身の受けた診察結果のデータを参照するために、主治医に対して診察データの参照を申請する
2	その他の医師による患者データ参照	主治医がその他の医師に対して、患者データ参照に招待する。その他の医師の同意を踏まえ、患者にてその他の医師が患者自身のデータを参照することの承認をすると、その他の医師は当該患者のデータを参照できる。
3	患者⇔主治医とのチャット送受信	患者と医師の間で、診療に係るチャットを送受信する。
4	アクセスログ一覧	患者または医師それぞれのユーザーが、アクセスログ一覧を参照する。
5	ブロックチェーン上の情報確認	自身が参照しているデータがブロックチェーン上に記録されていることを確認する

## 4. ゲノムデータの将来性

将来的なゲノムデータの活用方法の一つとして、日常生活で欠かせない「検索」において、ユーザー自身のゲノムデータに基づいた嗜好性・身体の状態などを踏まえた、提案型の情報提供に活用することもできるようになります。



**ご清聴ありがとうございました**