

Linked Personal Data

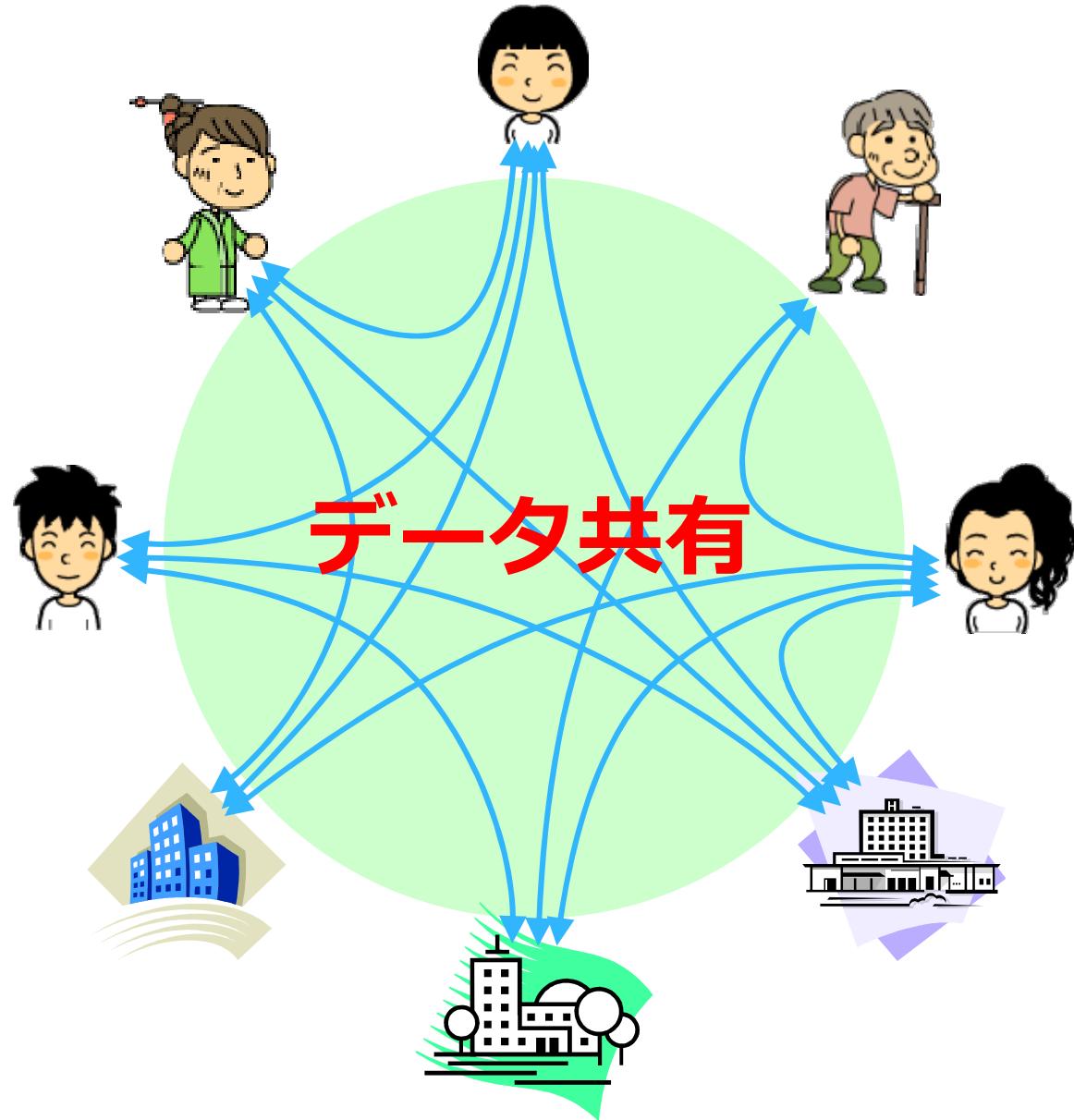
2017-03-11 橋田浩一



東京大学大学院情報理工学系研究科
ソーシャルICT研究センター

パーソナルデータの共有による1次利用

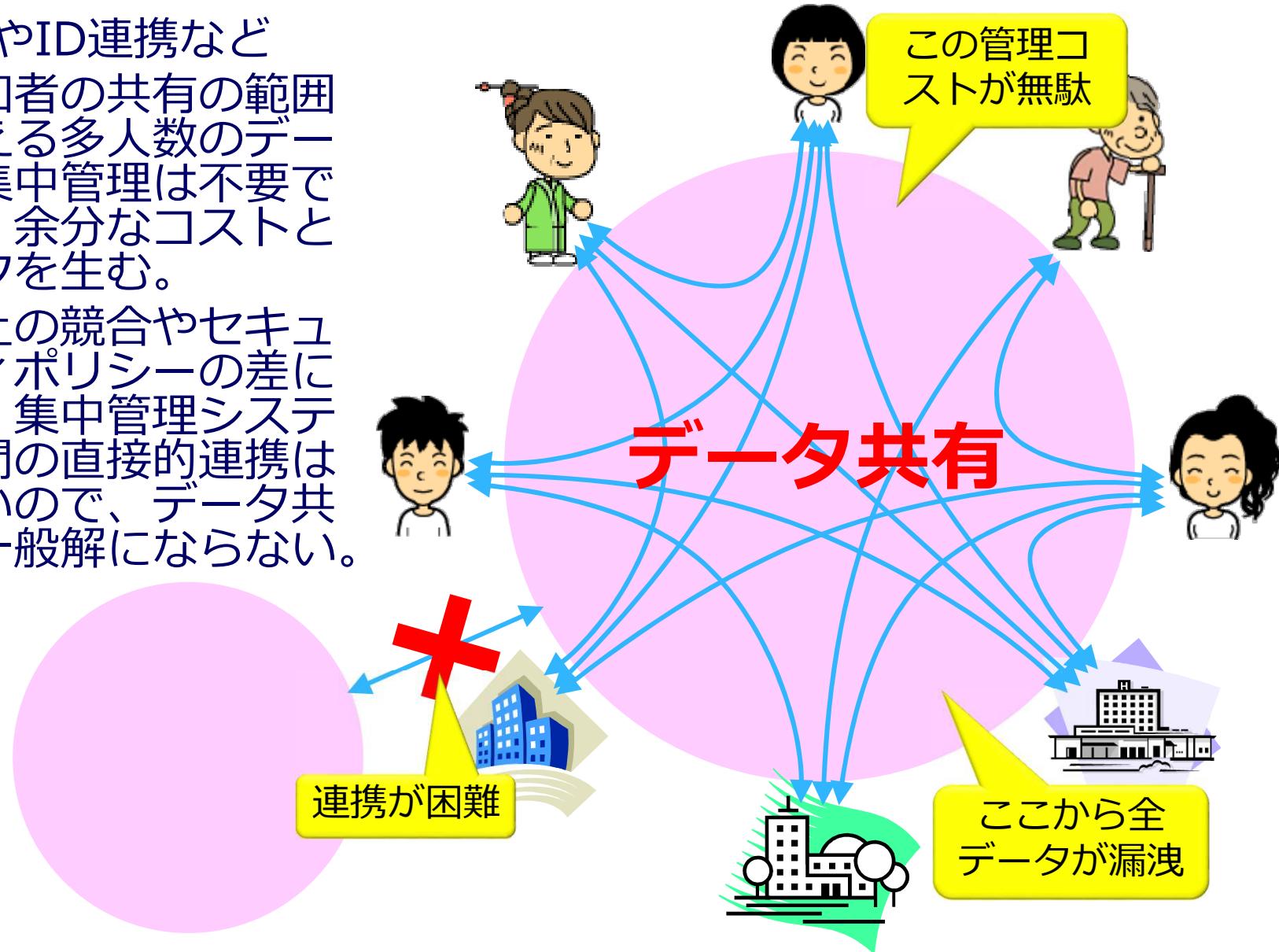
ヘルスケア、教育・学習、観光、就労など、多様なサービス各領域において、各顧客のデータを複数の事業者等が共有することにより、価値の高いサービスが提供できる。



集中管理によるデータ共有

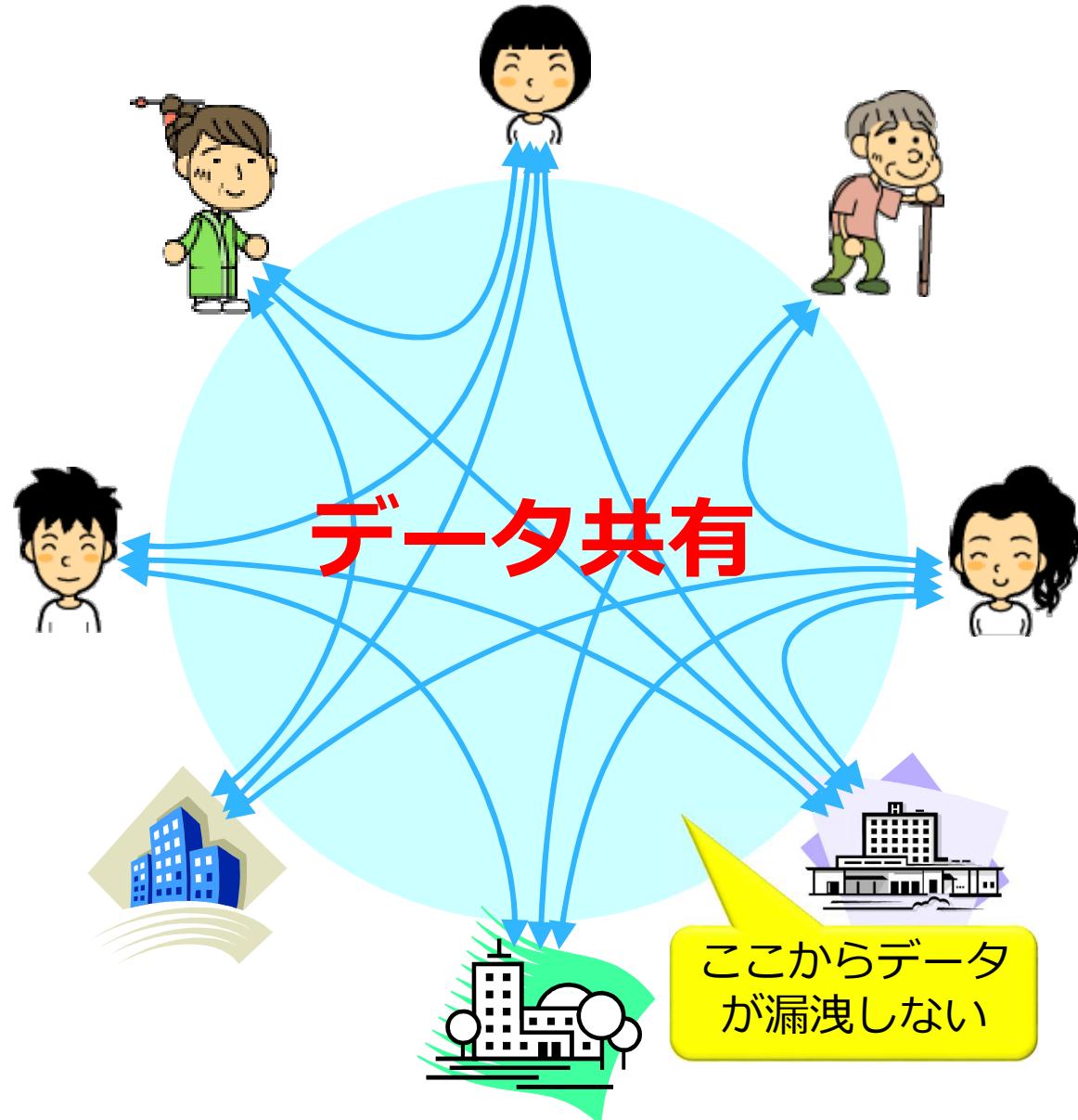
集中DBやID連携など

- 各参加者の共有の範囲を越える多大なデータの集中管理は不要であり、余分なコストとリスクを生む。
- 事業上の競合やセキュリティポリシーの差により、集中管理システムの間の直接的連携は難しいので、データ共有の一般解にならない。



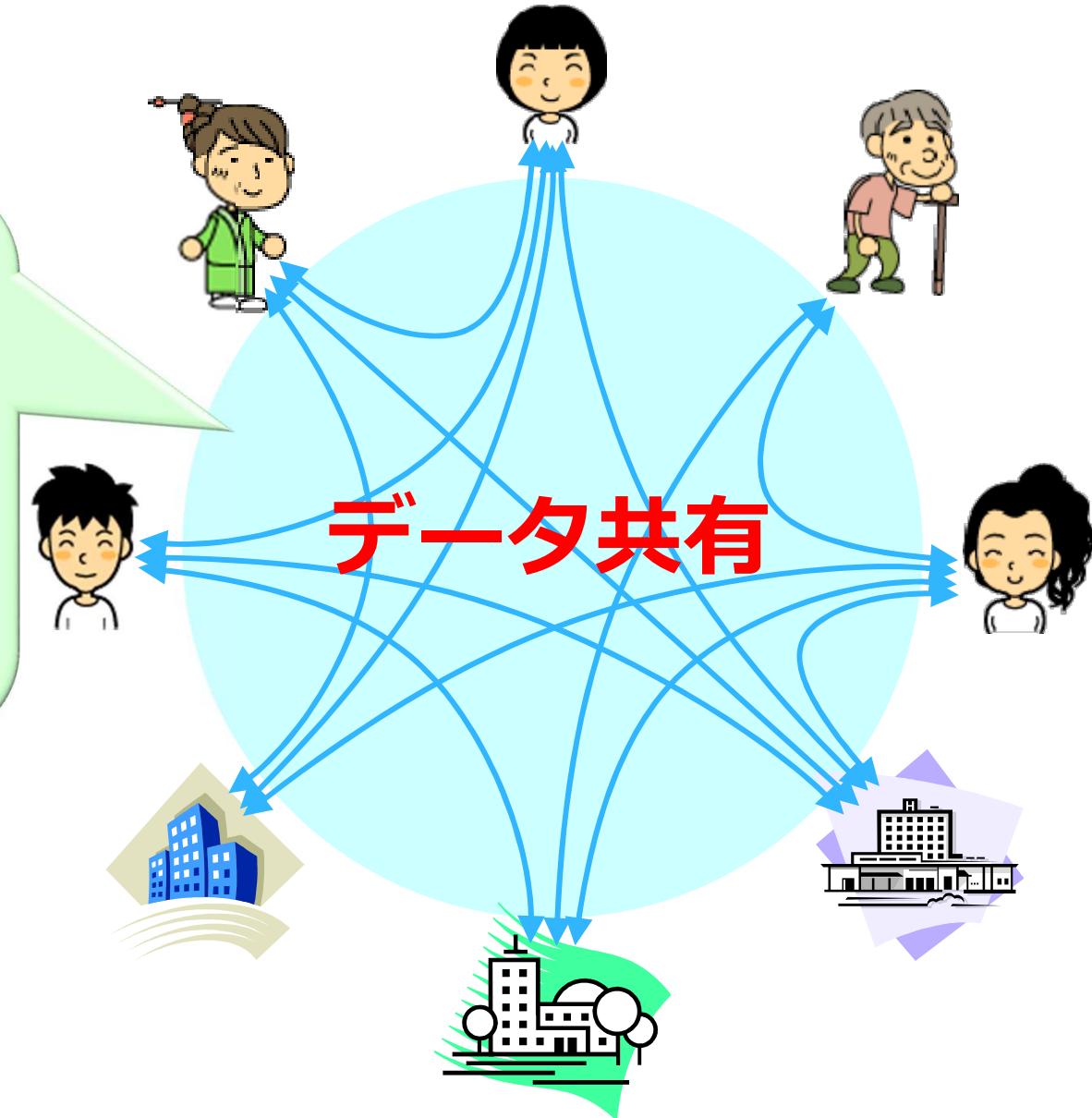
分散管理によるデータ共有

- 集中管理と異なり、参加者ごとの共有の範囲を越える規模のデータが漏洩しない。
- 誰でも簡単に参加できる仕組みなら、データ共有の一般解になる。



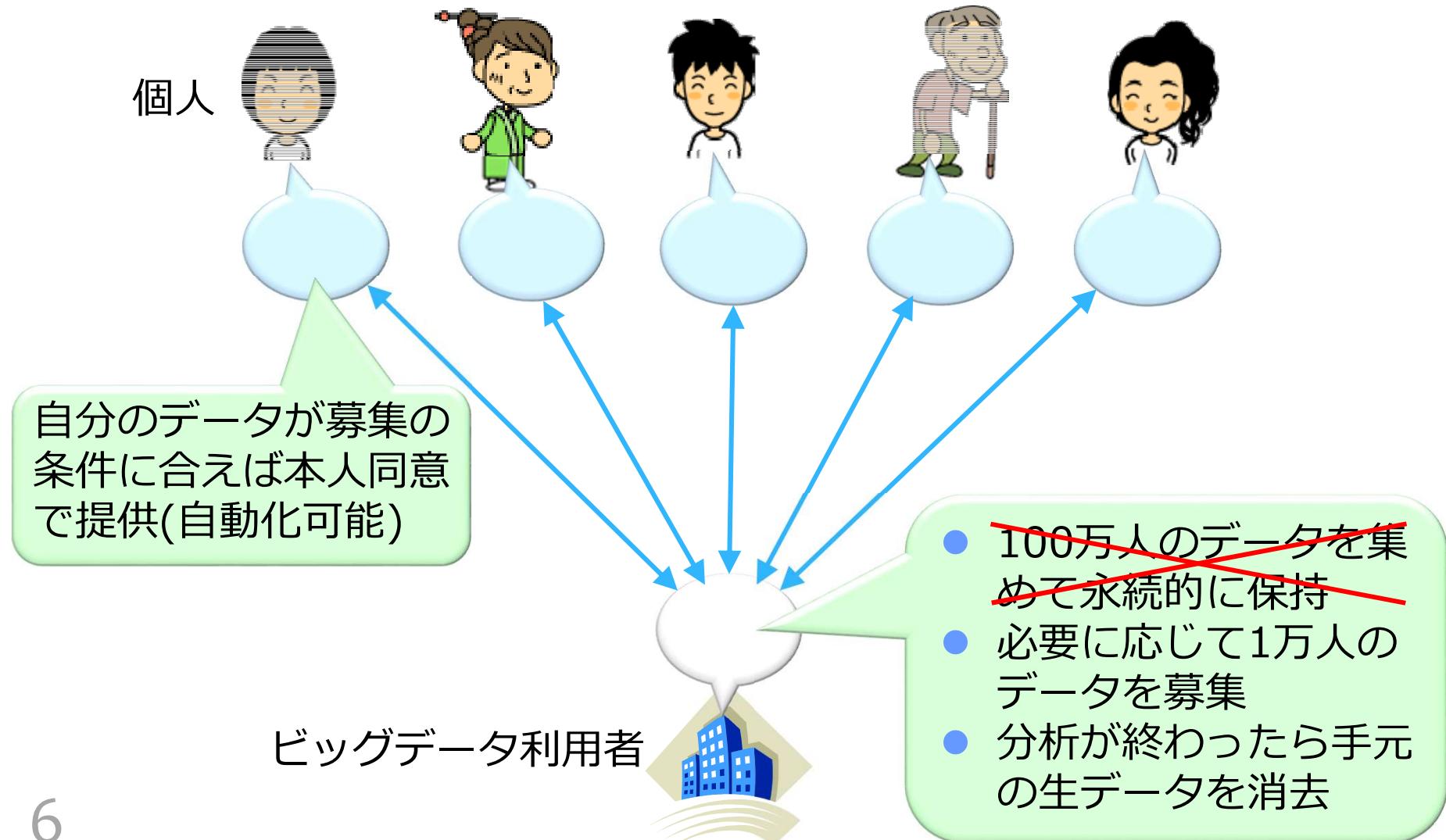
分散管理によるデータ共有のコスト

- ブロックチェーン
 - MedRecなど
 - PoWのコスト
 - ◆ 研究用データがもらえる等のインセンティブ
- 個人用ストレージ
 - PLRなど
 - ストレージのコスト
 - ◆ パブリッククラウドなら基本無料



本人管理に基づくビッグデータ活用

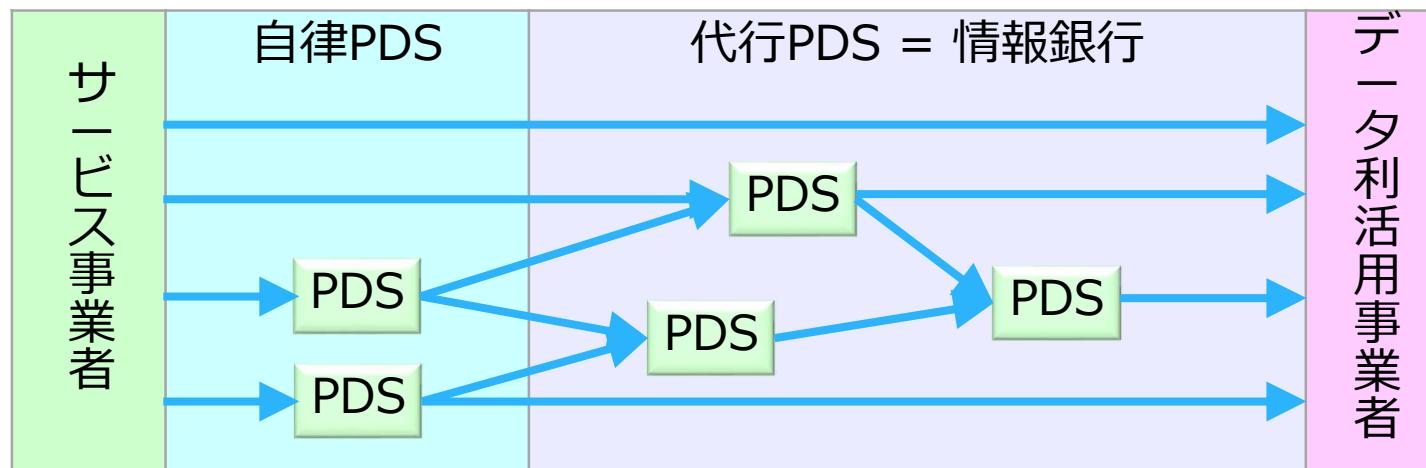
- 個人が本人のデータを管理していれば本人同意に基づくデータ収集が簡単。
- ビッグデータ利用者は多人数のデータを永続的に管理する必要がない。



PDSと情報銀行



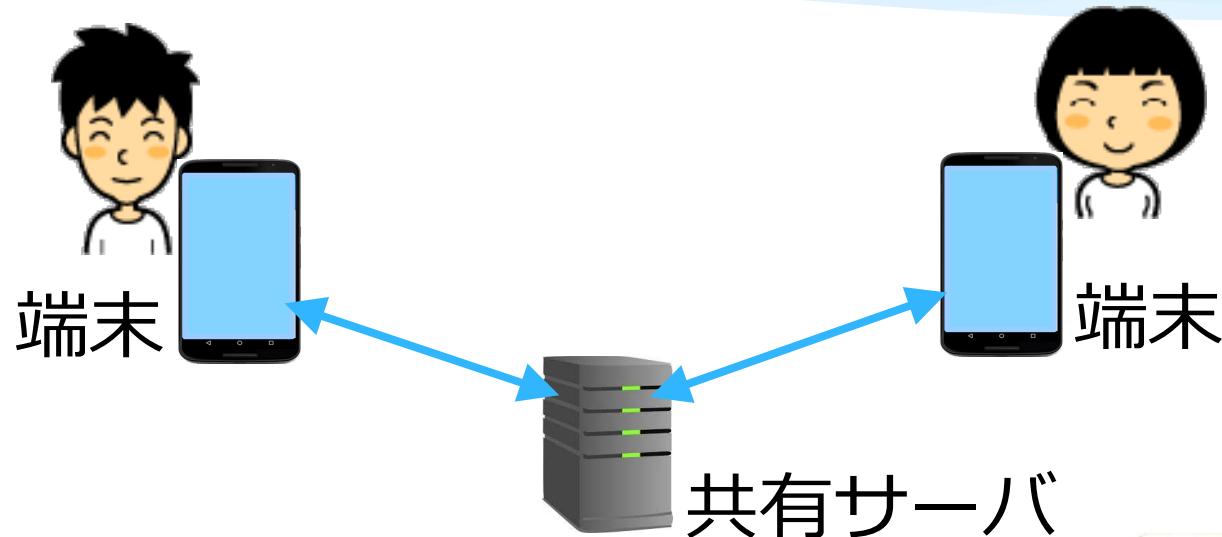
- Personal Data Store
 - ◆ パーソナルデータを本人の意思に従って運用する仕組み
 - * 運用 ~ データ開示の設定
 - * 必然的にデータポータビリティを満たす
 - ◆ 概念自体は部分的には古い: 星新一(1970) 声の網. (情報銀行)
- PDSシステムの用法
 - ◆ 自律(autonomous): 本人が自ら運用
 - * より分散的(decentralized): 少人数のデータを運用
 - ◆ 代行(surrogate): 他者が運用を代行
 - * より集中的(centralized): 多人数のデータを運用
 - ◆ 各PDSシステムはいずれの用法も可能



データの運用 = マッチング+開示の判断

- パーソナルデータとのマッチングの対象
 - ◆ 商品、サービス、求人、求職、結婚相手、他
- マッチングに応じたデータ開示
 - ◆ マッチングしたサービスの享受に必要なデータをサービス提供者に開示
 - ◆ マッチングした研究グループにデータを開示
- 運用代行が必要な場合
 - ◆ マッチングの対象に関するデータが大きすぎて個人端末に入らない
 - ◆ 本人も個人端末の中のAIもマッチングができない
- メディエータは大規模な代行PDS(情報銀行)
g

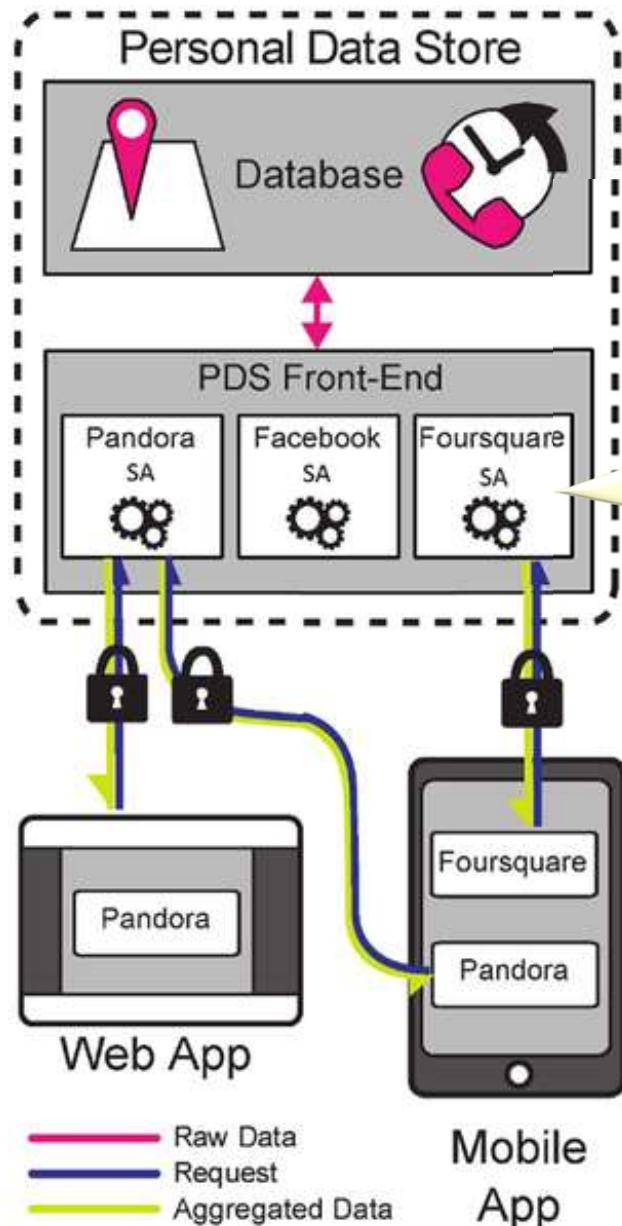
PDSシステム



サーバ 主導	Personium、OpenPDS、 Cozy、meeco、HAT、…	SafeAnswer
端末 主導	PLR、MedRec、 digi.me?、…	コンテナとマイ クロサービス ブロックチェーン

専用中継サーバの導入?

OpenPDS



SafeAnswerモジュール

- データそのものを共有するのではなく、プライバシを守りつつ質問に答える。

de Montjoye YA, Shmueli E, Wang SS, Pentland AS (2014)
openPDS: Protecting the Privacy of Metadata through
SafeAnswers. PLOS ONE 9(7): e98790.
doi:10.1371/journal.pone.0098790

<http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0098790>

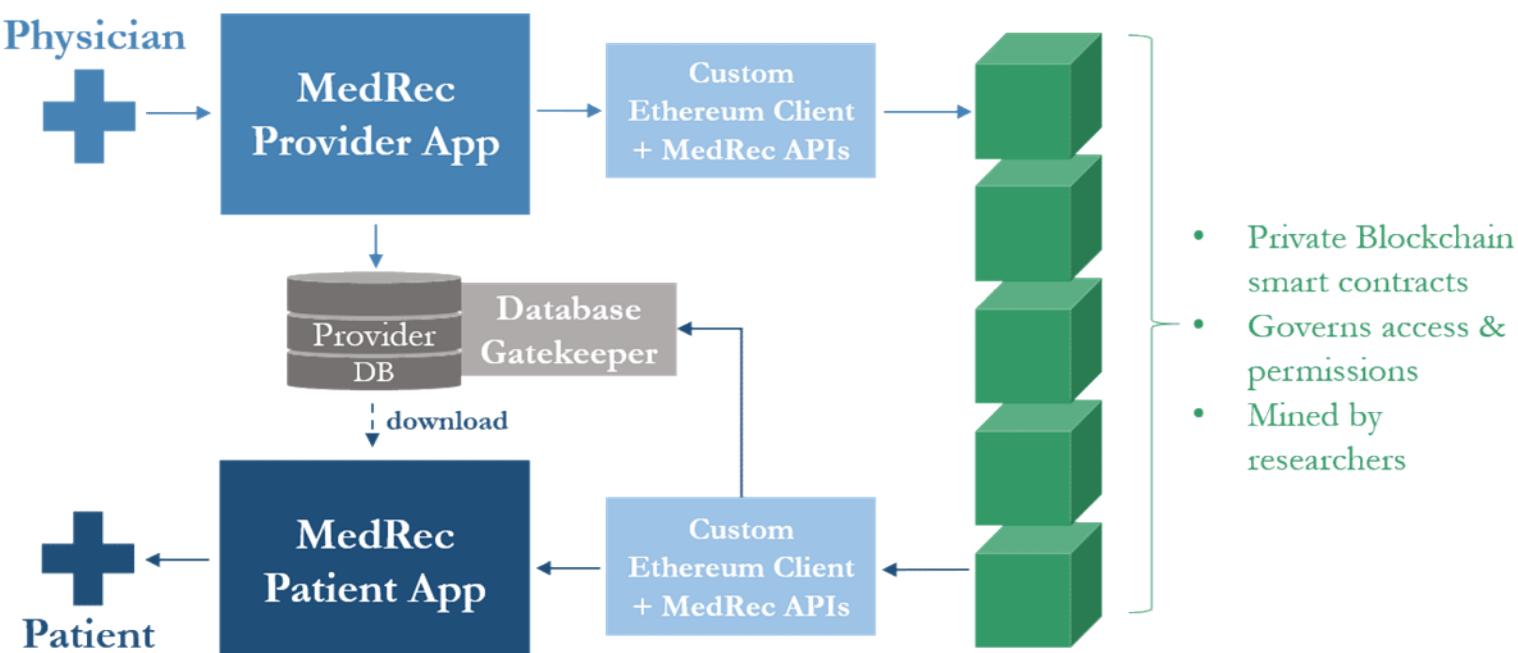
HAT: Hub-of-All-Things



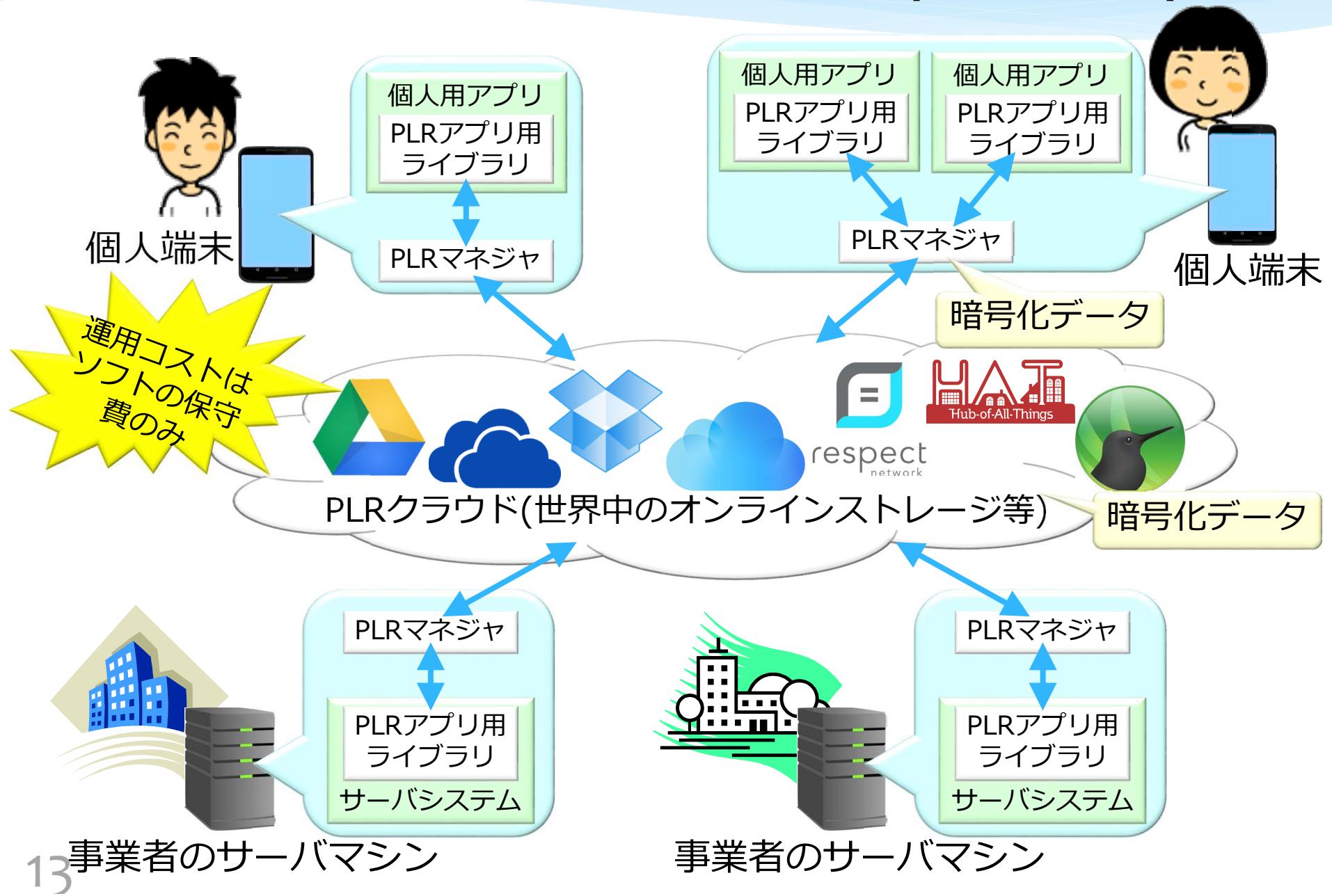
- 各利用者がパーソナルデータをクラウド(AWSなど)のコンテナに保管
- マイクロサービス
 - ◆ アクセス制御
 - ◆ OauthによるIdP → 外部サービスとの連携
- AGPL: Affero General Public License
 - ◆ 強いコピーレフト
 - * ネット越しの利用者にもソースコードを開示
 - ◆ ソースコードを改変したらHAT財団に提供
 - ◆ 商業利用可能
 - * HAT財団に使用料を支払う?

MedRec

- 参加者(患者と医療者と研究者)の間のデータ共有関係をブロックチェーンで管理
 - ◆ 医療機関がデータ開示を勝手に止めたり、研究者が患者のデータを見たりできない
 - ◆ 研究者が研究用データを得るために採掘することで運用コストを貢う



PLR: Personal Life Repository



PLRの用途

- 少人数のデータの処理は個人端末で
 - ◆ 業務システム(電力ル等を含む)、EHR、PHR、他
 - ◆ 本人に中味がわからないパーソナルデータを本人が管理して専門家等に開示するEHR的な運用も可
- 多人数のデータの処理はサーバマシンで
 - ◆ 検索、分析、マッチング、他
 - ◆ 平文データをファイルに書き出したり外部に送したりする可能性のある不正なアプリをOSが排除すれば、不正なOSのインストールを防ぐ管理だけでセキュリティを安価に担保できる。

PLRに関する役割分担

- パーソナルデータの管理運用に必要な関係者の役割は下記で全部
- 従来のように1つの事業者が全役割を担うと、権限と責任・コストとリスクが過大
- PLRはこれらの役割を3者に分散させることによりコストとリスクを低減
 - ◆ 個人がPLRを使う場合、データが洩れるよりもパスワードを忘れたりIDカードを紛失したりするリスクの方が大きいが、それはアカウント管理支援サービスで対処可能

利用者(本人または代理人)

- データの内容へのアクセス権限の設定
- PLRとストレージのアカウントの管理
- データの内容の分析や可視化(任意)

データ漏洩はここからしか生じない

契約

契約

ソフトウェア提供者

- アセンブローグ、アスクレップなど

ソフトウェアの保守拡張

- あるオンラインストレージが閉鎖するとわかったら他に乗り換える
- 量子コンピュータが現われたら暗号の代わりに秘密分散を使う

ストレージ提供者

- Google、Dropbox、Microsoft、日本政府など

データの保管

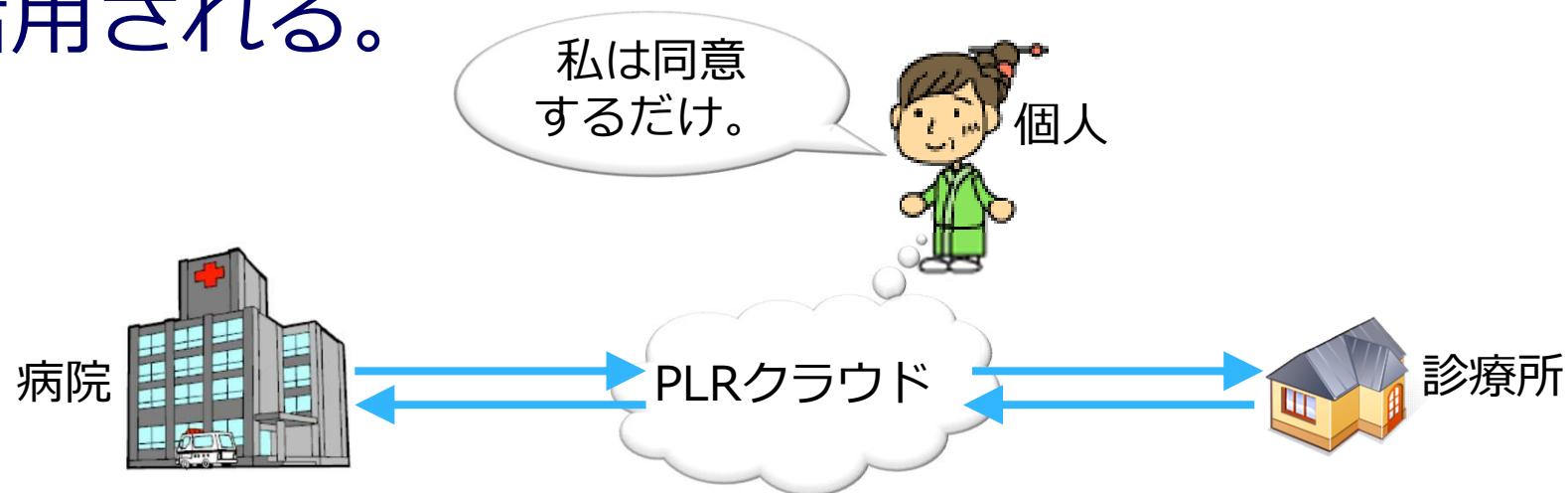
- ストレージのアカウントの管理(パスワードの再発行など)

PLRは安全

- データの集中管理が最低限
 - ◆ データの主体と利用者以外からの漏洩がない
 - ◆ データの主体と利用者からの漏洩も従来程度以下
- 多要素統合認証
 - ◆ 多要素認証
 - * クラウドのアカウント(またはAPIトークンの入った端末)
 - * PLRのパスワード
 - * 公的個人認証(予定):マイナンバーカード + パスワード
 - ◆ アカウントアグリゲーション
 - * 多数のアカウントを少数(5程度以下)にまとめることによって、人手による管理を可能にする
- DRM (デジタル権利管理): 暗号化 + アプリの機能制限
 - ◆ 平文データを書き出したり送信したりできない
 - * 本人が間違ったり騙されたりしても、他人に認証を破られても、多量の情報が一挙に洩れることがない
 - ◆ 不適切なデータ共有を防止(予定)
 - * 血液型占いのために住所を開示したりしない。

PLRは簡単

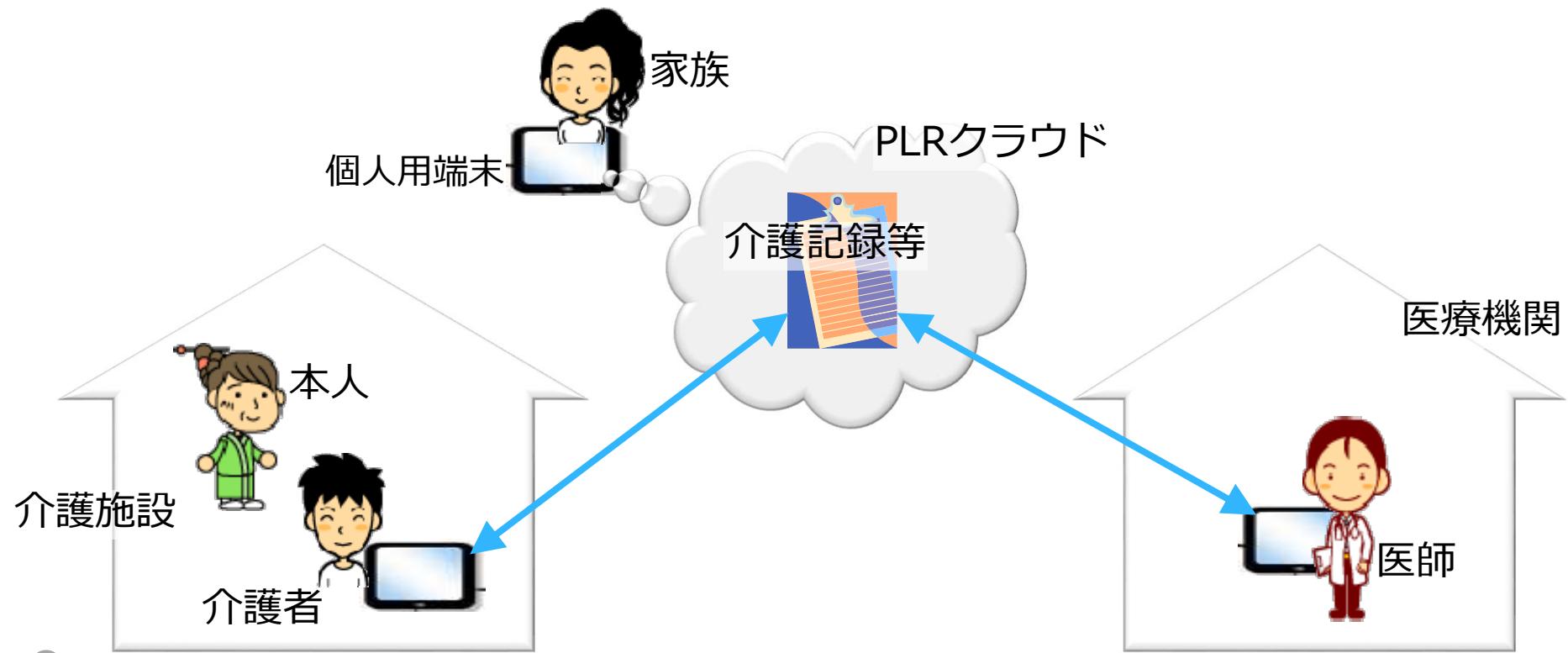
- ITリテラシは不要: データ共有を設定(委託可能)した後は、本人が端末を操作しなくても、指定された者の間でパーソナルデータが共有・活用される。



- 専門知識も不要: データのさまざまな部分の運用をPLRで他者に委託(信託)できる。

ヘルスケアデータの個人管理

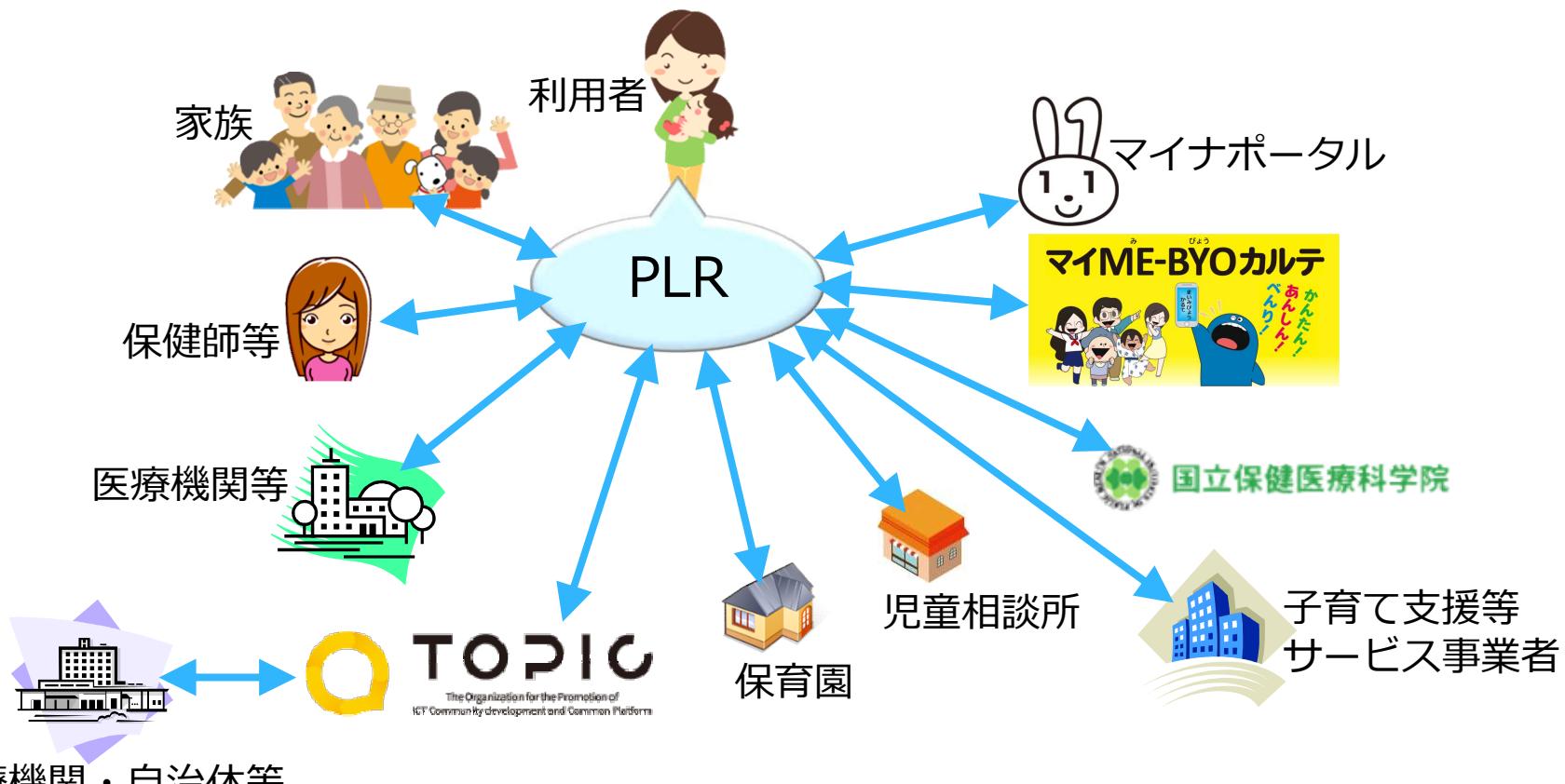
- 介護記録のデータを本人(の家族)が管理して関係者と共有可能に
- 山梨と鳥取で約70人のうち2人の高齢者について運用中
- 分散システムなのでそのまま**何億人**にでも拡張可能



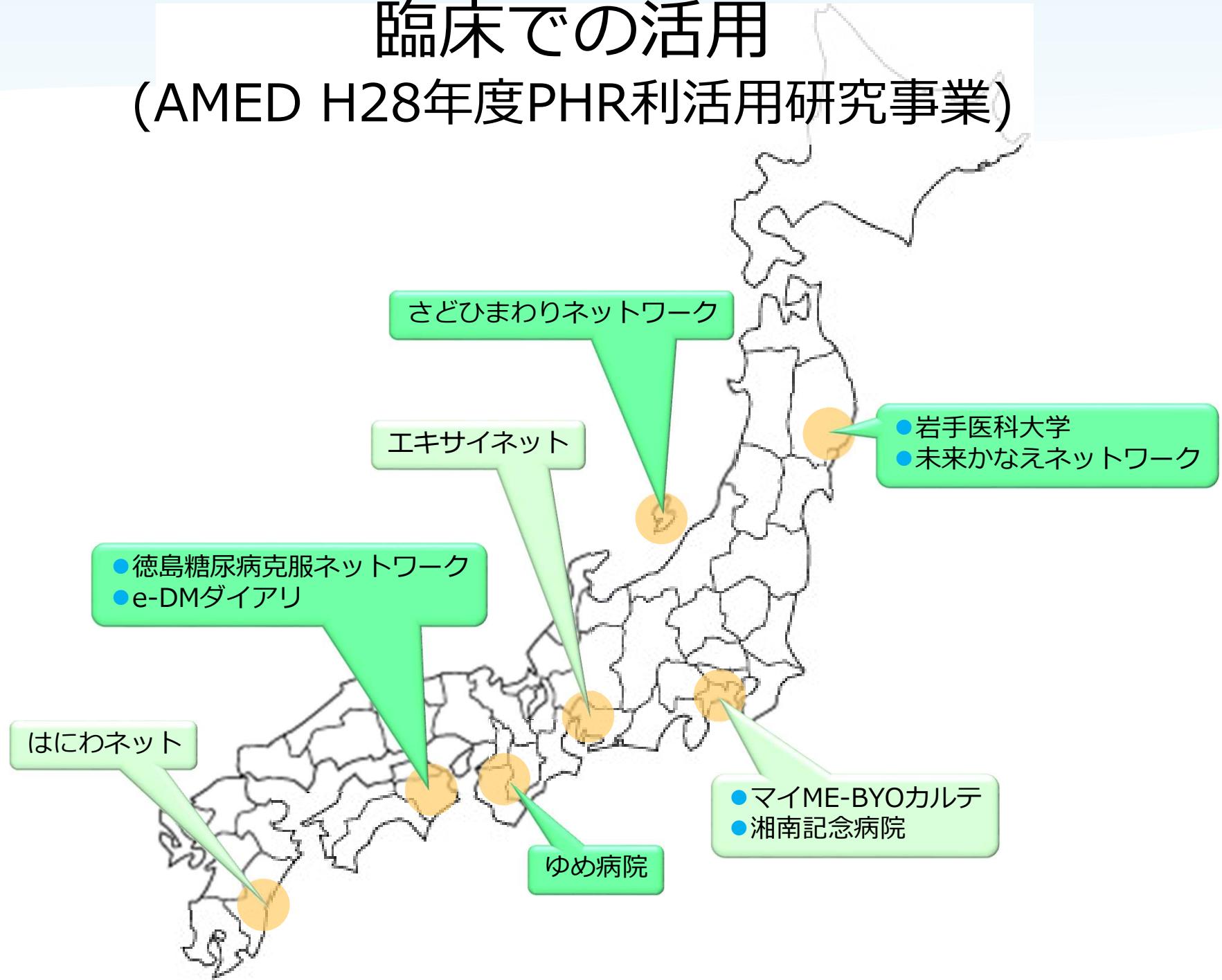
母子保健での活用

(AMEDのH28年度PHR利活用研究事業1次公募の(1))

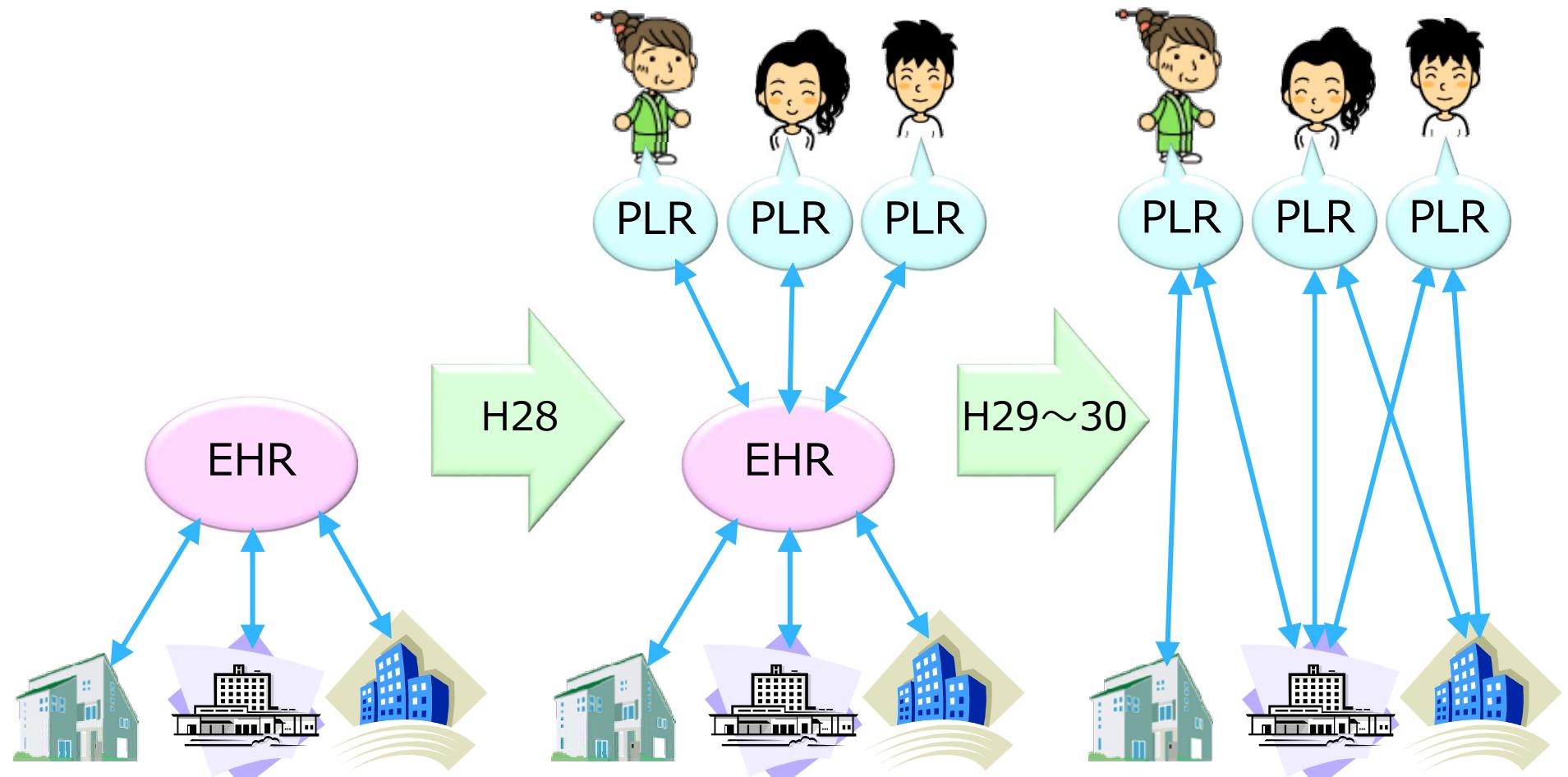
- 母親が医療機関等の事業者からデータを取得
- 保健師等の業務を電子化することにより、負担を軽減するとともに、母親とリアルタイム・双方向に情報共有



臨床での活用 (AMED H28年度PHR利活用研究事業)



集中から分散へ



保健医療分野におけるICT活用推進懇談会 提言【2016年10月19日】

ICTを活用した「次世代型保健医療システム」

2020年度からのスタートを目指す

次世代型ヘルスケアマネジメントシステム(仮称)

PeOPLe(仮称)
Person centered Open Platform for wellbeing

PLR

個人ごとのデータの集約

データ利活用プラットフォーム(仮称)

匿名化データ

多数の個人にわたるデータの集約

次世代型保健医療システム：ICTの技術革新を徹底的に取り入れ、限られた社会資源を効果的・効率的に活用し、保健医療サービスの質と、システム全体の持続可能性を高めていくことができる体制

価値不在の情報化

患者・国民の価値主導

3つのパラダイムシフトと3つのインフラ

つくる

集まるデータ

生み出すデータ

データの収集段階から、集積・分析・活用（出口）で使える
アウトカム志向のデータをつくる

<インフラ>

最新のエビデンスや診療データをAIを用いてビッグデータ解析し、
現場の最適な診療を支援するシステムを構築

つなげる

分散したデータ

データの統合

個人の健康なときから疾病・介護段階までの
基本的な保健医療データをその人中心に統合する

<インフラ>

保健医療専門職に共有され、個人自らも健康管理に役立てる
全ての患者・国民が参加できるオープンな情報基盤を整備

ひらく

たこつぼ化

安全かつ
開かれた利用

産官学のさまざまなアクターがデータにアクセスして、
保健医療データをビッグデータとして活用する

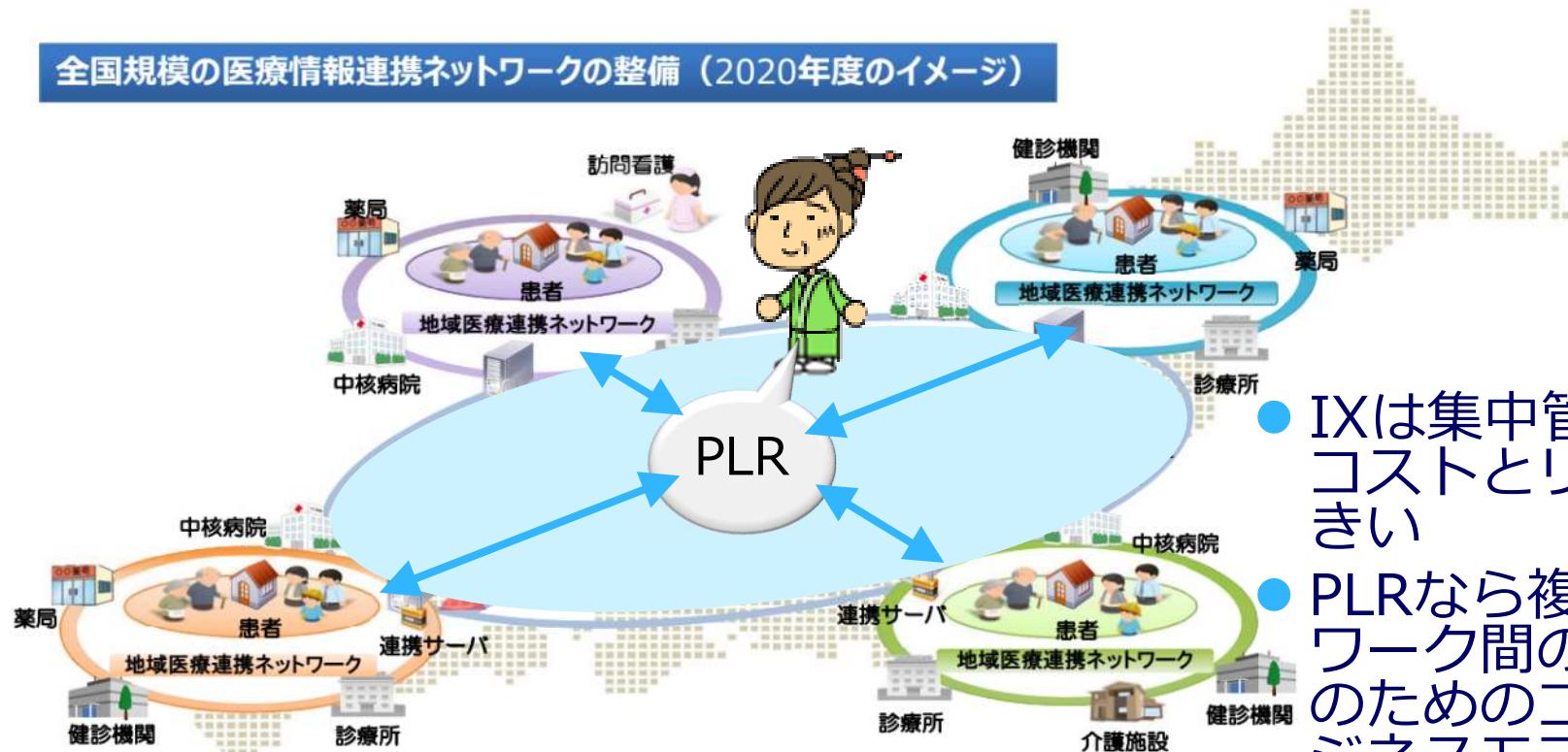
<インフラ>

産官学の多様なニーズに応じて、保健医療データを
目的別に収集・加工（匿名化等）・提供できるプラットフォームを整備

医療等分野のネットワークの相互接続について

- 日本医師会が提案する「医療等分野専用ネットワーク」は、全国の医療機関・介護施設等を網羅し、セキュリティが確保された医療情報連携の情報通信回線を構築し、医療・介護情報やレセプトオンライン請求等のサービスを接続するというもの。
- 医療保険のインフラを活用したオンライン資格確認を行うためのネットワーク(回線)が今後整備される予定。この回線を活用して、全国の保険医療機関・薬局や地域医療連携ネットワークを認証し、相互に接続する機能を持つ医療(介護)情報連携ネットワークを形成し、全国共通のユニバーサルIDとして医療等IDを活用することにより、地域の医療(介護)情報連携(EHR)を超えて、全国の医療機関等間で、患者の治療・検査・画像診断等の医療情報を共有することが可能となる。
- このような医療等分野の複数の回線の相互接続について、「IX (Internet Exchange) 接続センタ」を用いた場合の技術、運用、ビジネスモデルの検討を、厚労省において実施予定（平成28年度）。

全国規模の医療情報連携ネットワークの整備（2020年度のイメージ）



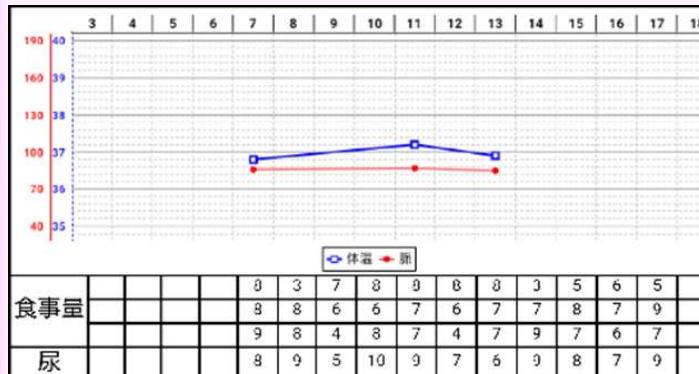
- IXは集中管理なのでコストとリスクが大きい
- PLRなら複数ネットワーク間の相互接続のためのコストやビジネスモデルは不要

PLRアプリ

- オントロジー(データの仕様)と制約(ビジネスロジック)とスタイルシート(画面と帳票の仕様)をExcelで作れる
- 生活録 → 介護記録、疾病管理手帳、健康手帳、母子手帳、他
- 問診 → 診療科の問診、フレイルチェック、アンケート、他

生活録アプリ

時系列サマリ画面



タイムライン画面

The timeline screen shows a log of events for a patient named Potter Harry from August 9 to August 15, 2015. The log includes entries for urination, defecation, meals, bathing, and blood pressure measurements.

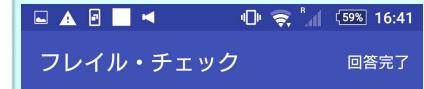
日付	時間	内容	担当者
08月09日	06:51	尿 普通 中回数3	橋田浩一
08月09日	08:00	朝食9	橋田浩一
08月09日	08:50	便 自然 軟多	橋田浩一
08月09日	10:46	髭剃り	橋田浩一
08月09日	12:00	昼食10	橋田浩一
08月09日	13:48	Sp0296%	橋田浩一
08月09日	13:55	血圧 125/63mm	橋田浩一

グループサマリ画面

The group summary screen shows meal records for multiple patients on December 30, 2015. The patients listed are 工藤進一, 辻山まや, 近藤志ずか, 佐藤C作, and 樋田徳行. The table includes columns for 朝食 (Breakfast), 昼食 (Lunch), おやつ夕食 (Snack/Dinner), レク (Recreation), 尿 (Urination), and 便 (Defecation).

日付	朝食	昼食	おやつ夕食	レク	尿	便
2015年12月30日	10	9	+	8	+	6 中1
工藤進一	10	9	+	8	+	6 中1
辻山まや	10	10	+	-	4	少3
近藤志ずか	10	9	-	9	+	5 中1 少1
佐藤C作	9	9	+	9	+	5 多1
樋田徳行	10	10	15:00	18:00	12:11	

問診アプリ



The questionnaire screen shows a list of questions for a questionnaire. The questions are: 1. 指輪っかテスト (Yes/No), 2. 囲める (Yes/No), 3. いいえ (Yes/No), 4. はい (Yes/No), and 5. はい (Yes/No). The responses are marked with blue or red circles.

オントロジーと制約の例

BP ja:血圧; blood pressure [%max]/[%min]mmHg	max=1 ja:最大;maximum	decimal>20<400
	min=1 ja:最小;minimum	decimal>10<300
MC 口腔ケア 口	¥labelが「口腔ケア」でabbrevが「口」	
BF ja:朝食;breakfast	pf=1 ja:主食; principal food ja:主;principal	integer)0(10
	of=1 ja:副食;other food ja:副;other	integer)0(10

]C pregnancy ja:妊娠;pregnancy	[Sex]	[Pregnant]
[0%value]	[1]	
[_Female]		¥女性だけが妊娠; SexとPregnantが存在す るならば、 Sex%value=_Female
	&absent	

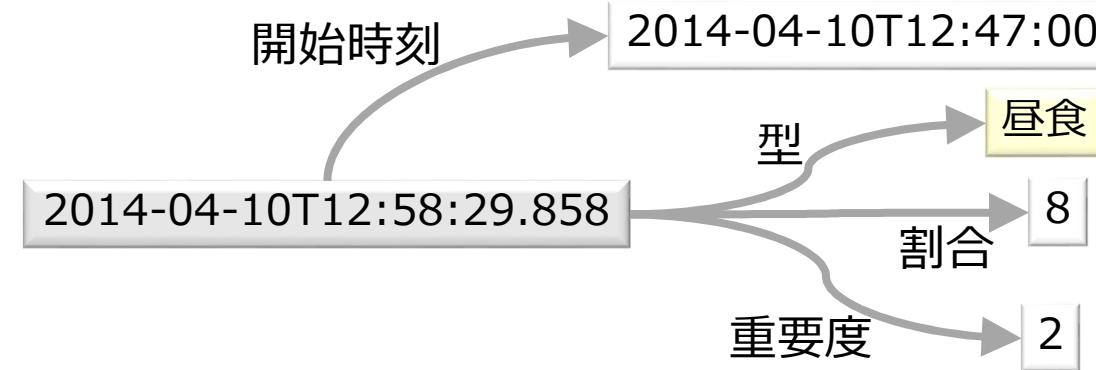
介護記録/生活録アプリ

2014年04月06日～2014年04月12日

04月07日	11:05	その他	台風	明子
04月07日	21:13	夕食9		慶子
04月08日	09:20	体温36.5°C	普通	明子
04月08日	16:05	○ 体重48kg		明子
04月10日	12:25	備考	問題なし。	
04月10日	12:47	◎ 昼食8		
04月10日	14:49	その他	読書	
04月10日	15:11	尿 濃縮 パッド		

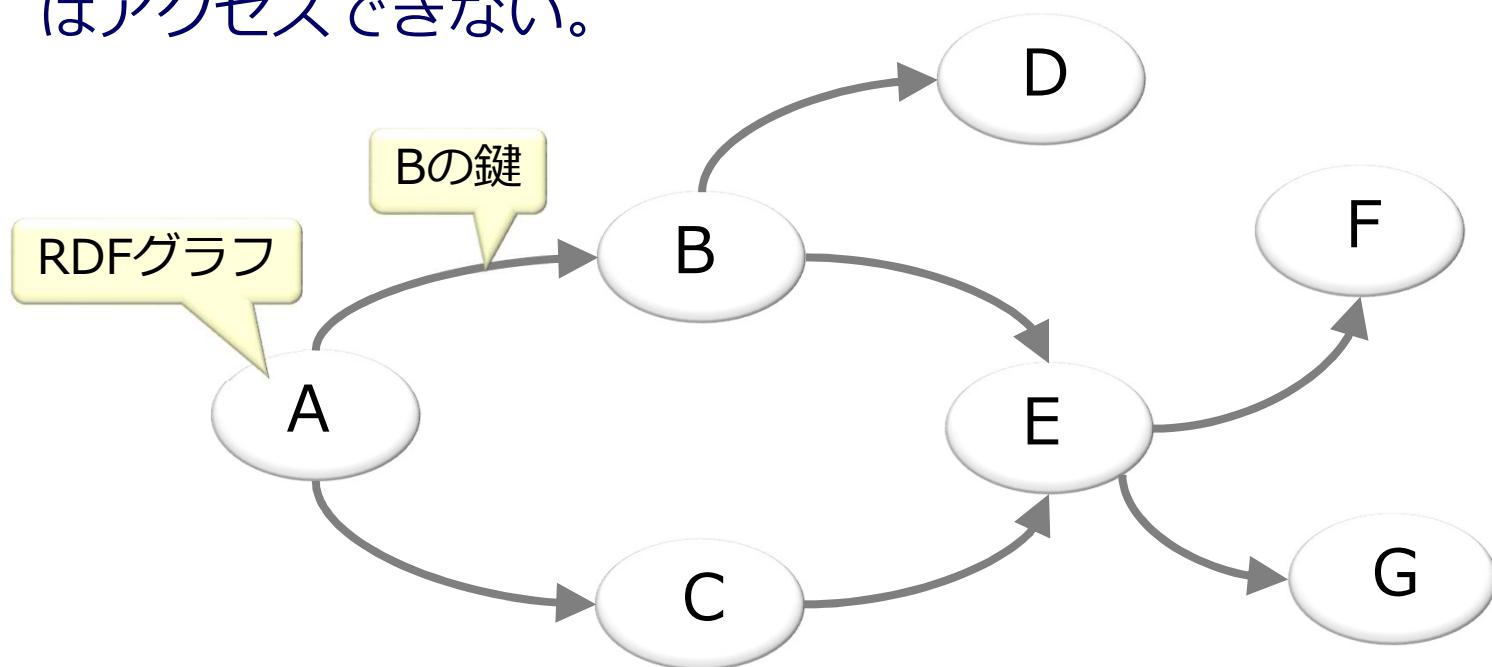


```
{  
  "creation": "2014-04-10T12:58:29.858",  
  "begin": "2014-04-10T12:47:00",  
  "@type": "LU",  
  "int10": 8,  
  "importance": 2  
}
```

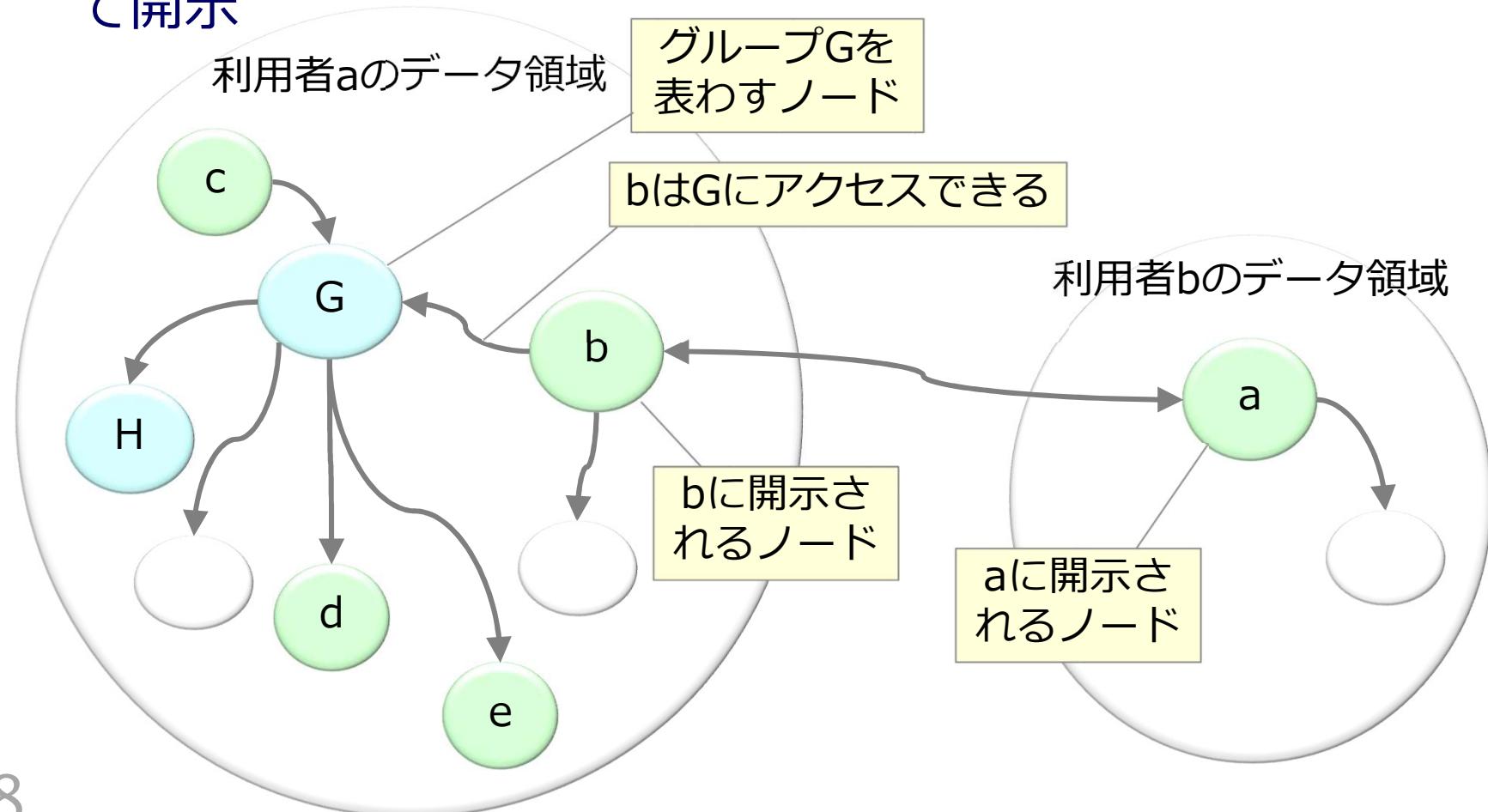


部分グラフへのアクセス

- グラフ中の各ノードはRDFグラフ
- 各ノードは固有の対称鍵で暗号化されている
 - ◆ 1個のノードの一部分だけを復号する鍵もある
- 各ノードへのリンクはそのノードの鍵を含むので、あるノードにアクセスできればその子孫にアクセスできる。
 - ◆ BにアクセスできればD、E、F、Gにアクセスできるが、AとCにはアクセスできない。

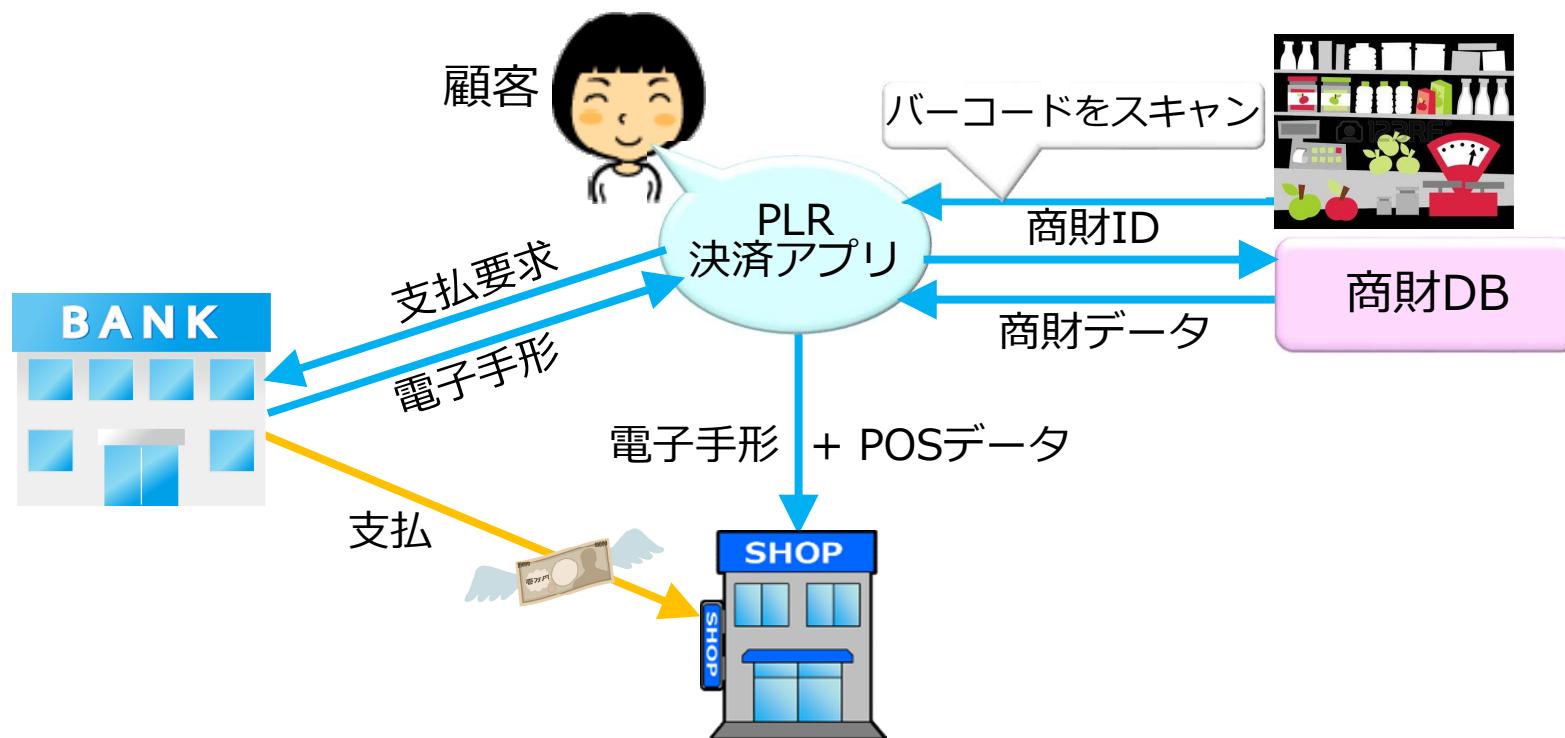


- 他の利用者aとフレンドになる
= aに開示するノードを自分の領域に作る
 - ◆ そのノードを対称鍵Kで暗号化し、Kをaの公開鍵で暗号化して開示



客のスマホがPOSレジ

- 個人(買物客)のPLR端末
 - ◆ POSデータを生成して店舗に渡す
 - ◆ 電子手形(電子小切手)を銀行から取得して店舗に渡す
 - ◆ 銀行のAPIのアカウントの情報をPLRで管理
- 店舗は電子手形を換金(銀行間決済?)
- 決済代行事業者を使うよりはるかに安全かつ安価



世界の動向

- 日本

- ◆ 2017～ 改正個人情報保護法
- ◆ 2017～ マイナポータル
- ◆ 2018～ 銀行法施行令等の一部を改正する政令等

- 欧州

- ◆ 2018～ GDPR (一般データ保護規則)
- ◆ 2018～ PSD2 (改正決済サービス指令)

- アジア

- ◆ IndiaStack

10年後はインドの時代?

- すでに11億人が公的個人認証システムAadharに登録
 - ◆ 銀行口座の開設等が容易に
- モバイル決済により2年で現金とクレジットカードをなくす
- 決済に限らない多様なサービスをAPIで相互連携



India Stack Ecosystem



インド版国民PDS

- MITのOpenPDSは仕組が複雑すぎて不採用?
- PLRのように専用サーバ不要のPDSでないと全国展開は無理?

