

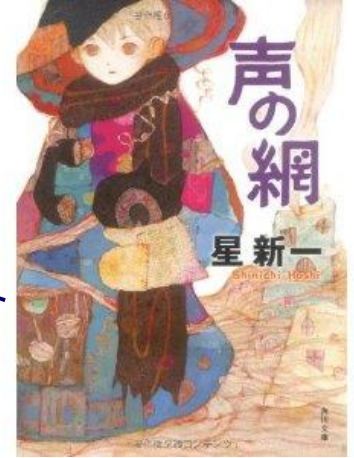
臨床および臨床研究のための 分散PDSの応用

2017-05-19 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

PDSと情報銀行

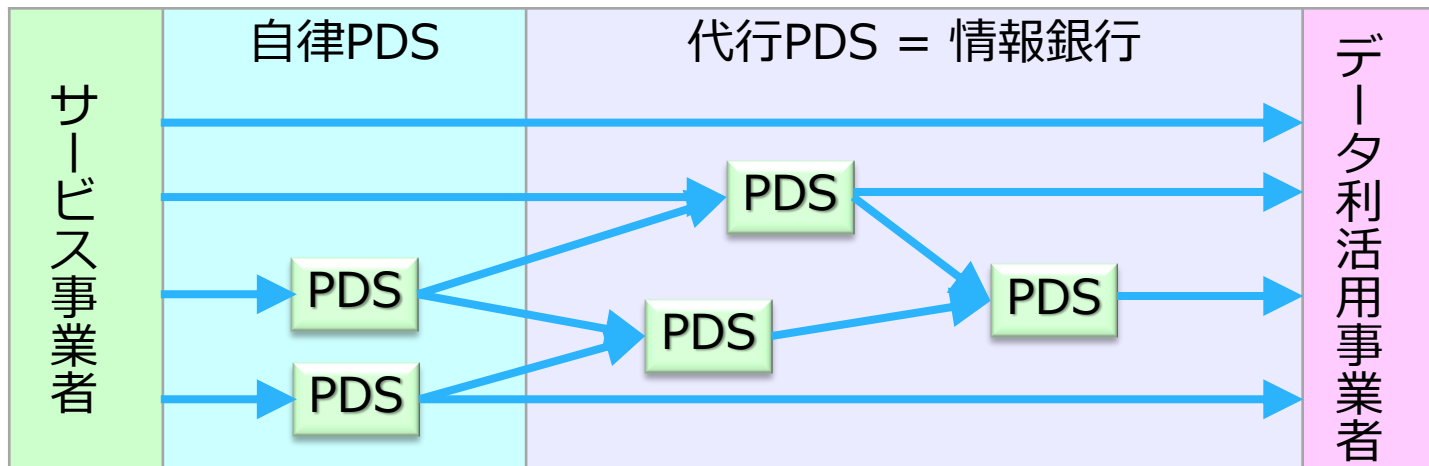


- Personal Data Store

- ◆ 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



AIの基盤としてのBPR

- AIの**研究開発**よりもむしろ**実運用**のために、構造化されたデータが容易に取得できる必要あり
 - ◆ 研究開発のコストはほとんどデータ整備にかかる
 - ◆ AIによるサービスの相手(多くは個人)に関するリッチなデータが必要
- AIの普及にはBPRによるデータ循環社会の構築が必須

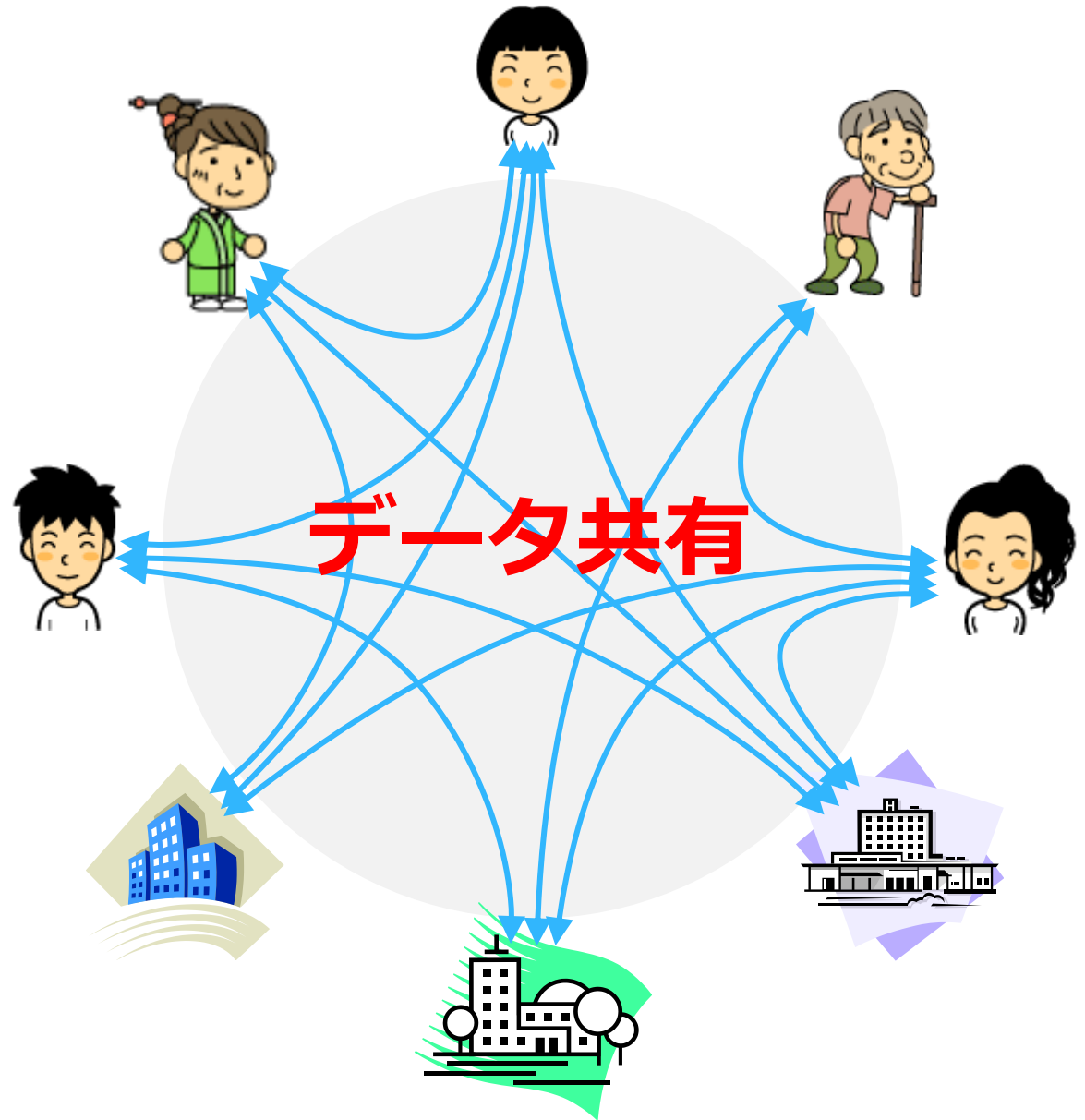
業務改革: business process reengineering

- 一般の人々の日常の生活や業務のあらゆる場面において意味構造化されたデータが生成され循環する社会の構築
- 標準スキーマに基づくデータ構造化によるデータ・サービス連携
- データ主体(ほとんどは個人)の意思によるデータの流通
 - GDPの60%が個人消費

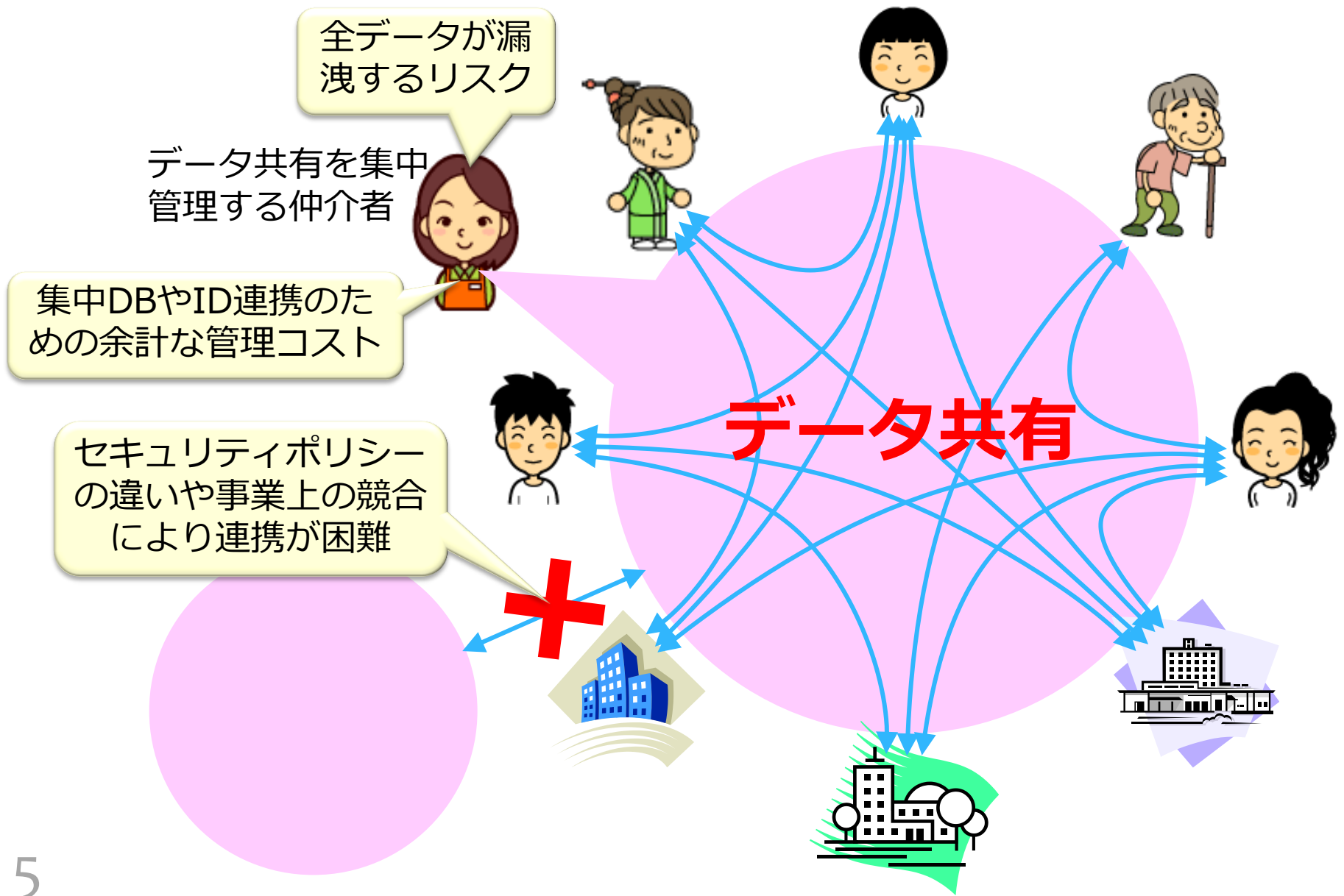
スキーマの標準化や書式変換には意味理解が必要だが、AIは意味を理解しないので、**AIによるBPRの自動化は不可能**

パーソナルデータの共有による1次利用

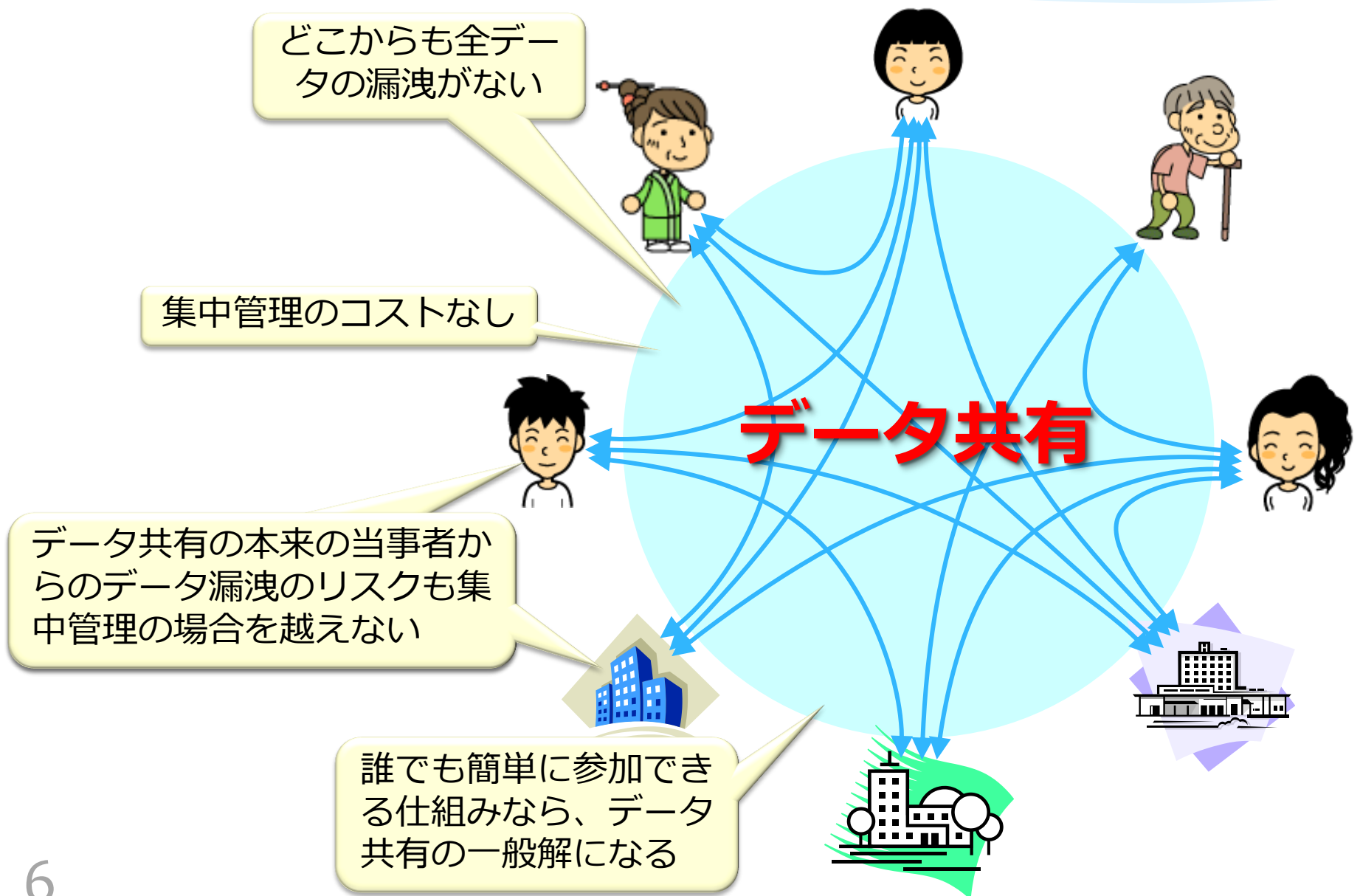
ヘルスケア、教育・学習、観光、就労など、多様なサービスの領域において、各顧客のデータを複数の事業者等が共有することにより、価値の高いサービスが提供できる。



集中管理によるデータ共有



分散管理によるデータ共有



分散管理に基づくビッグデータ活用

自分のデータが募集の条件に合えば本人同意で提供(自動化可能)

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。

- ~~多人数分のデータを~~
~~集めて永続的に保持~~
- 必要に応じてデータを募集・収集
- 分析が終わったら手元の生データを消去

データ共有

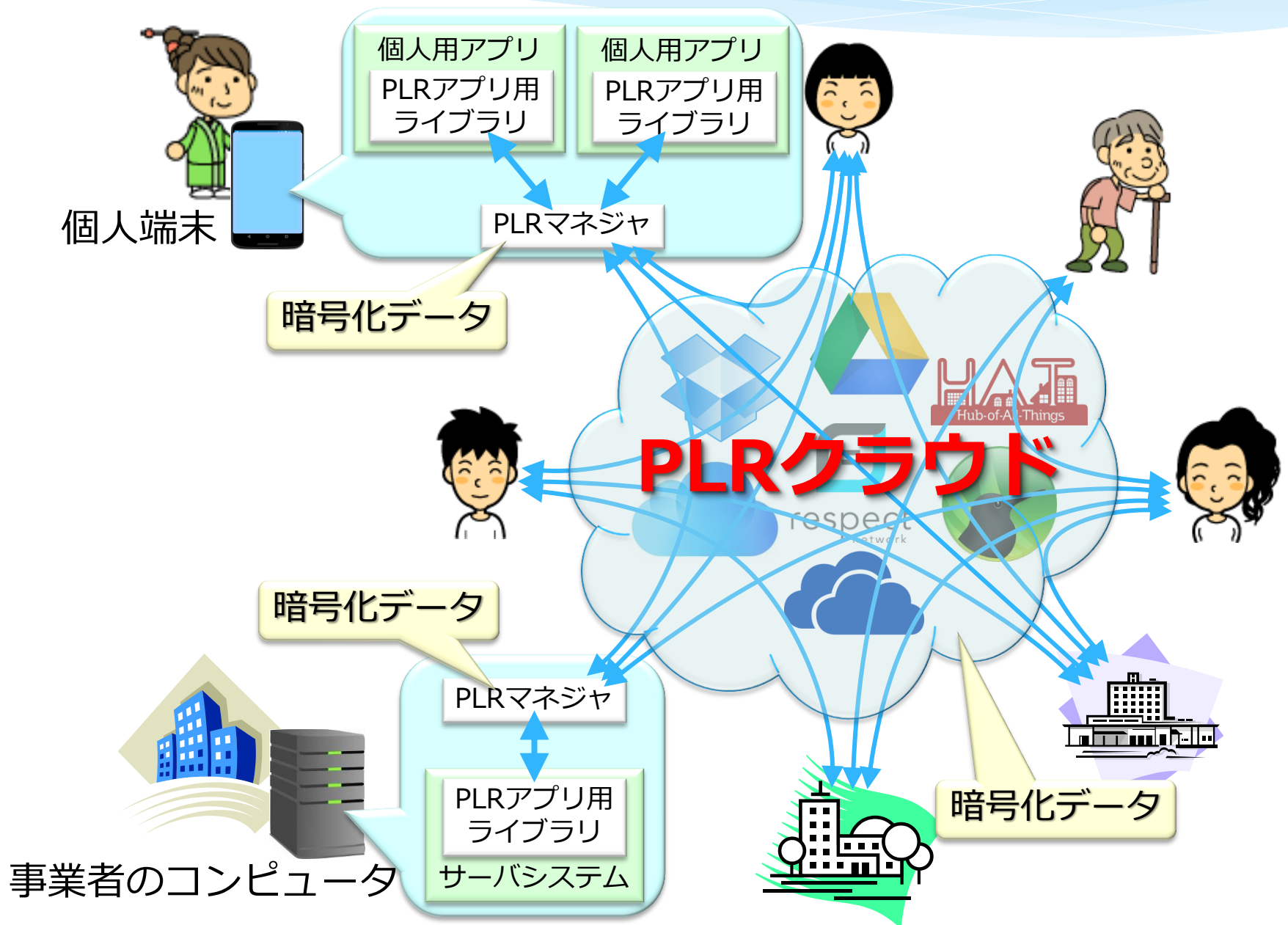


ビッグデータ利用者

パーソナルデータの流通

- 1 次利用: 分散型(仲介者なし)のデータ共有
 - ◆ 集中型はわざわざコストをかけてリスクを高める
- 2 次利用(検索や分析): 同意によるデータ収集
 - ◆ データの管理運用が本人(代理人)に分散されていれば本人同意に基づくデータ収集が容易

PLR: Personal Life Repository



PLRは安価

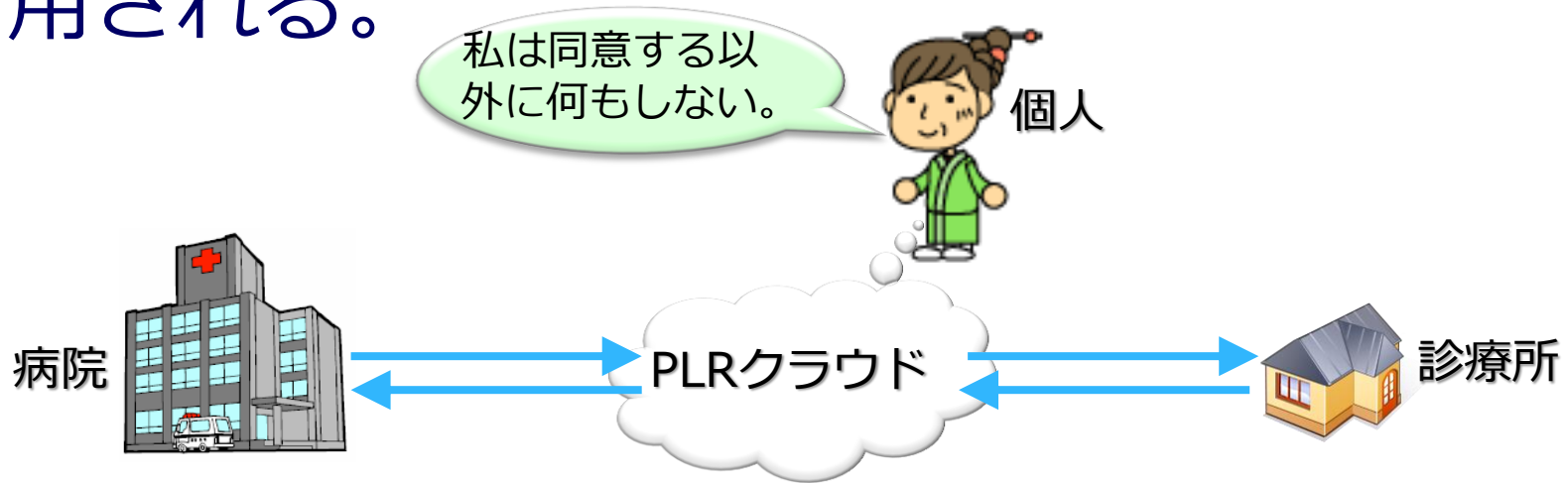
- 分散型(仲介者なし)のデータ共有
 - ◆専用サーバもVPNもDBMSも不要
 - ◆基本無料のパブリックストレージサービスで十分
- 個人端末も必須ではない
 - ◆データ共有の設定には代理人の端末を使えば良い
- 運用コストも低い
 - ◆自分の端末を自力で操作できる利用者へのサポートは不要

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。

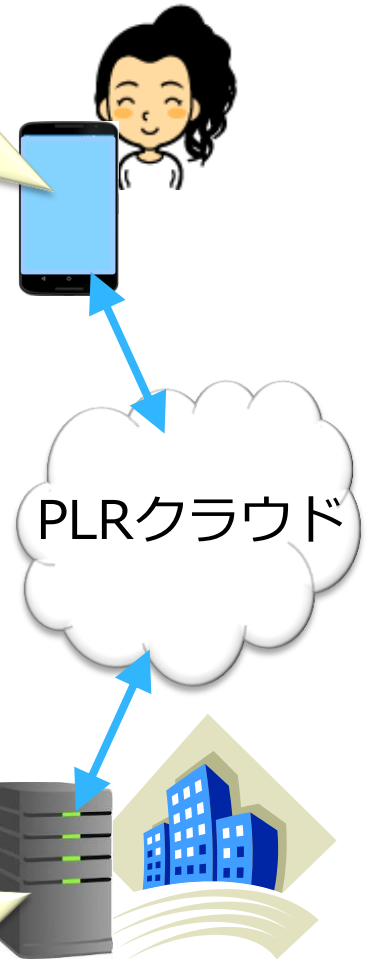
PLRは多用途

多人数のデータを集める必要のないサービスは個人端末で

- 電カル、EHR、PHR、通常の業務システム等のほとんどの処理(個票デーの入出力)
- 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の開示するEHR的な運用も可

多人数のデータを集める必要のあるサービス(検索や分析)はサーバマシンで

- 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**必要な役割は下記で全部**
- 1つの事業者が全役割を担うと、権限・責任とコスト・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
- EHRやPHRをPLRで実現する場合、運営事業者は下記の代理人となるが、利用者の役割の多くは本人が担い、またアクセス権限の設定が簡単なので、**運営コストが小さい**

利用者(本人または代理人)

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

契約

ソフトウェア提供者

- アセンブログ、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

契約

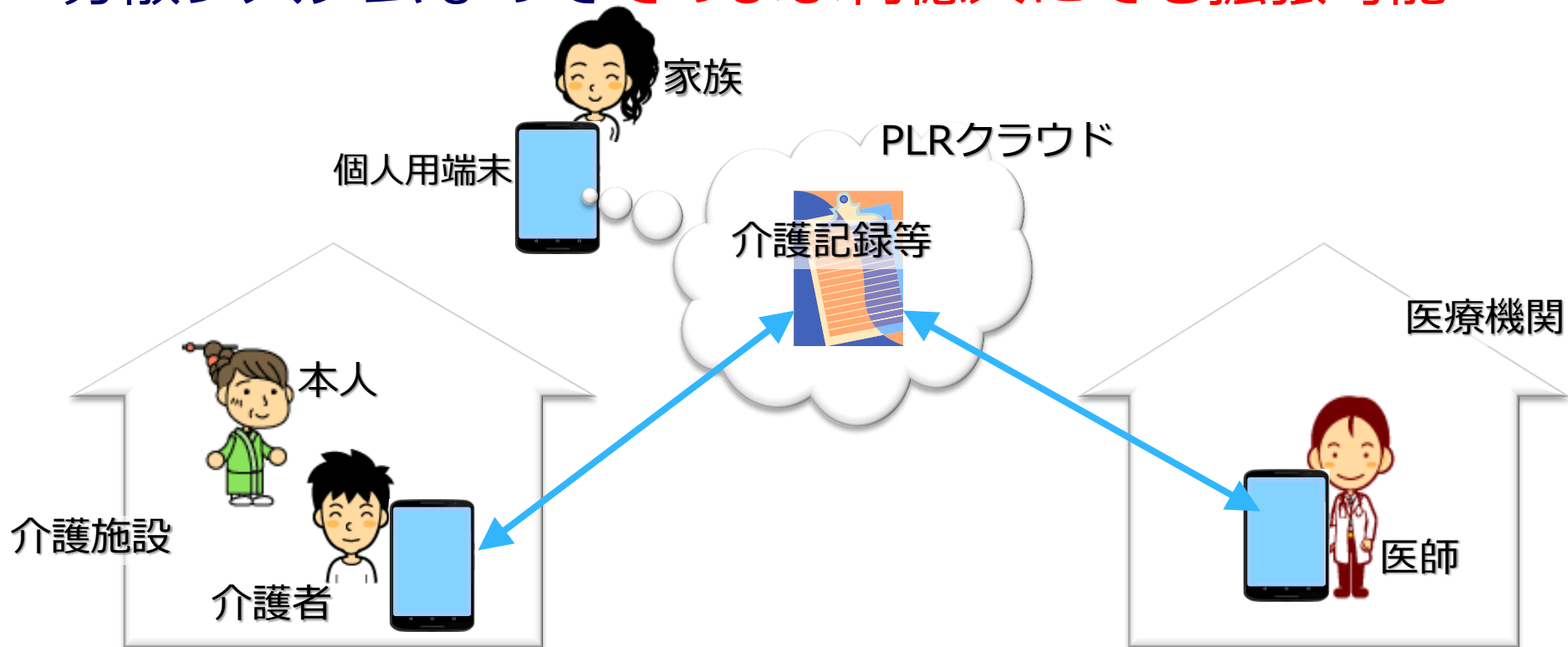
ストレージ提供者

- 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の実運用

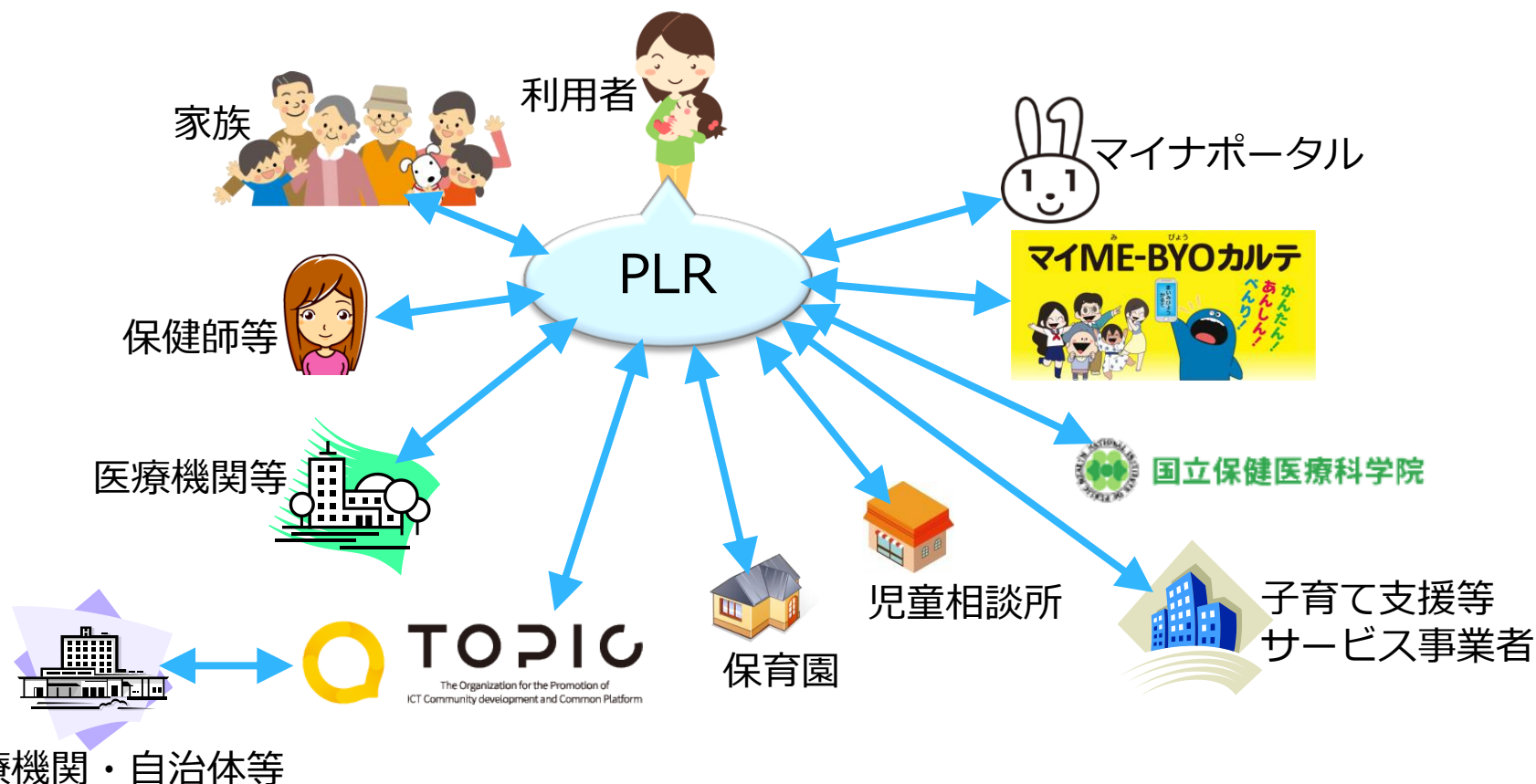
- 介護記録のデータを本人(の家族)が管理して関係者と共有可能に
- 山梨と鳥取で2人の高齢者について運用中
 - ◆ PLR介護記録の対象者は70人以上
- 分散システムなので**そのまま何億人にでも拡張可能**



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))

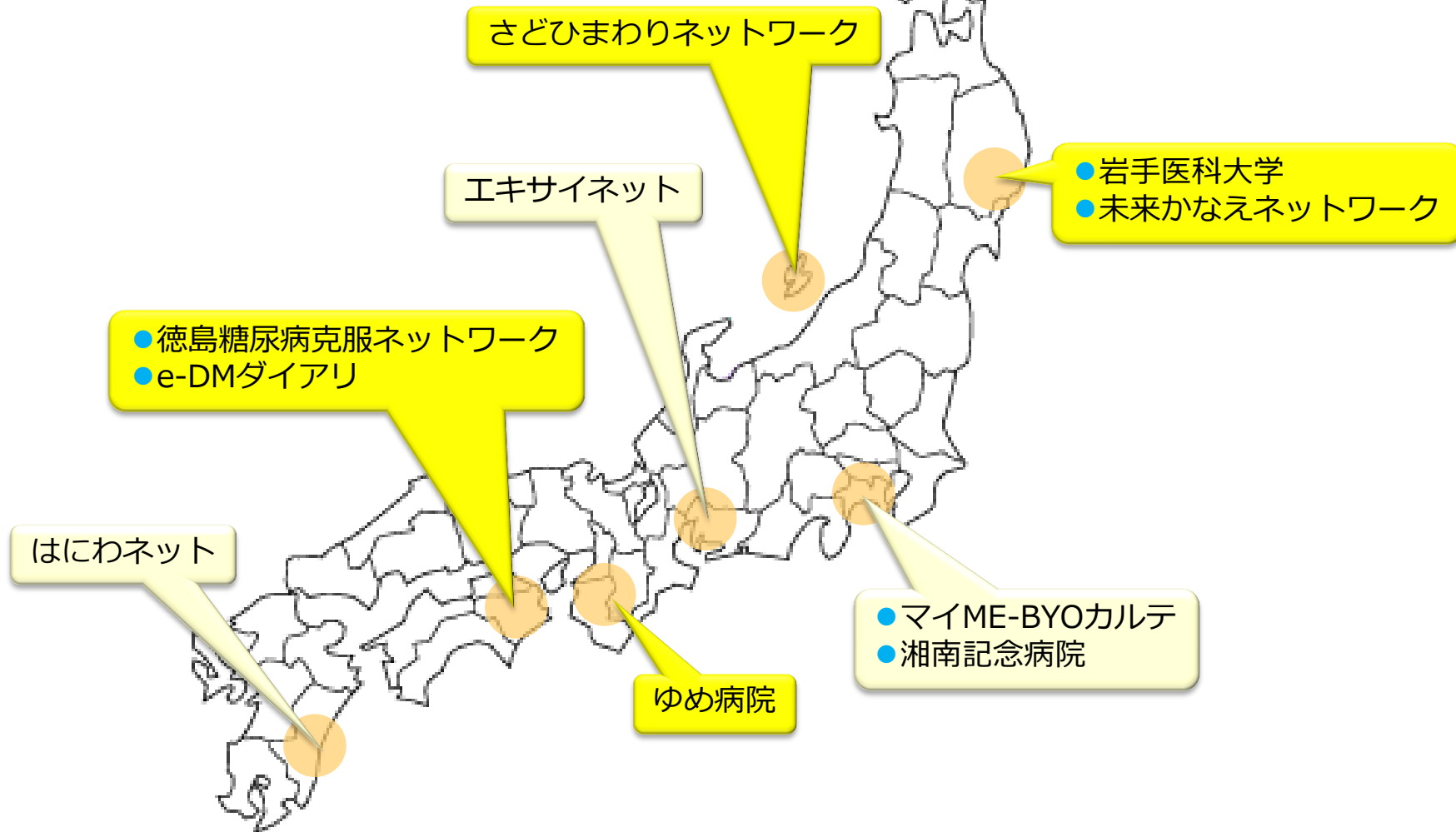
- 母親が医療機関等の事業者からデータを取得
- 保健師等の業務を電子化することにより、負担を軽減するとともに、母親とリアルタイム・双方向に情報共有



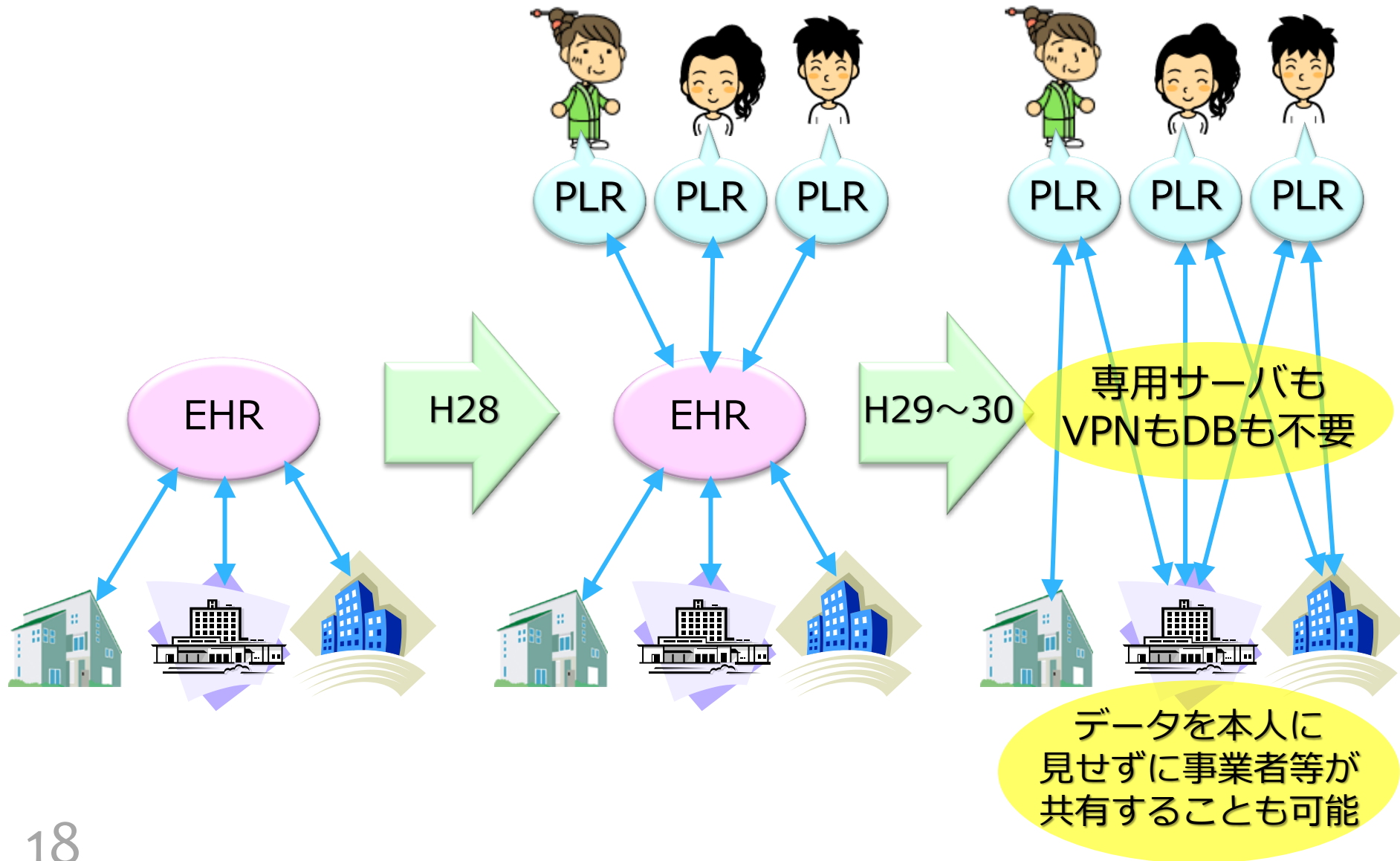
臨床での活用

(AMEDのH28年度PHR利活用研究事業2次公募の(2))

- 各実証フィールドにおいて既存の地域医療連携システム等とPLRとを連携



集中から分散へ



PLR統合アプリ

- マルチプラットフォーム
 - ◆ Android版: 2017年9月
 - ◆ iOS版・Java版: 2018年2月
- PLR基本機能
 - ◆ 認証、暗号化/復号、通信
- データ共有
 - ◆ フレンド、グループ、同意
- データ作成・活用
 - ◆ 生活録と問診(アンケート)
 - ◆ 自分/フレンド/グループのデータ
 - ◆ 画面と帳票のカスタマイズが容易



世界の動向

●日本

- ◆ 2016年～ マイナンバーの運用
- ◆ 2016年～ 官民データ活用推進基本法
 - * 第十二条 本人関与の下でのパーソナルデータの流通
- ◆ 2017年～ マイナポータルの運用と改正個人情報保護法の施行
- ◆ 2018年～ 銀行のオープンAPI

●ヨーロッパ

- ◆ 2018年～ 一般データ保護規則(GDPR)の施行
 - * 消去の権利とデータポータビリティの権利
- ◆ 2018年～ PSD2の施行: 銀行のオープンAPI

●途上国

- ◆ IndiaStack、カンボジアの暗号通貨、他

IndiaStackプロジェクト

- 公的個人認証システムAadhaarに11億人が登録済
 - ◆ 銀行口座が簡単に作れる
- 2年で現金とクレジットカードを廃止
- 銀行だけでなく他の民間企業や公的機関もサービスをAPIで公開
 - ◆ 個人がPOSデータ等を蓄積し活用しつつサービスを連携させて利用

India Stack Ecosystem



インド版国営PDS

- MITのOpenPDSはSafeAnswers等の仕組みが複雑すぎて高コスト
- 12億人分の運用にはPLRのような安価で安定したPDSが必要

COMMERCE
(GSTn)

CREDIT
(RBI)

INVESTMENTS
(SEBI)

SKILLS

HERS

CONSENT LAYER

Provides a modern privacy data sharing framework

Open Personal Data Store

CASHLESS LAYER

Game changing electronic payment systems and transition to cashless economy

IMPS, AEPS, APB, and UPI

PAPERLESS LAYER

Rapidly growing base of paperless systems with billions of artifacts

Aadhaar e-KYC, E-sign, Digital Locker

PRESENCE-LESS LAYER

Unique digital biometric identity with open access of nearly a Billion users

Aadhaar Authentication

JAM

Jan Dhan, Aadhaar, Mobile

Cambodia taps Japanese blockchain tech for payment system

Central bank eyes easily accessible means of remittance for people



Electronic funds transfer systems are not widely available in Cambodia.

TOKYO -- The National Bank of Cambodia will develop a blockchain-based payment system with help from a Japanese financial technology startup to offer people a secure, low-cost way of sending and receiving money.

おわりに

- スマートソサエティの基盤
 - データ主体の意思によるリッチデータの循環
 - ◆ 個人認証
 - ◆ オープンAPI
 - * モバイル決済、スマートディスクロージャ、etc.
 - ◆ 分散PDS
 - ◆ 意味構造化データ
- インド等の途上国が10年後には欧米や日本を生産性で上回っている？