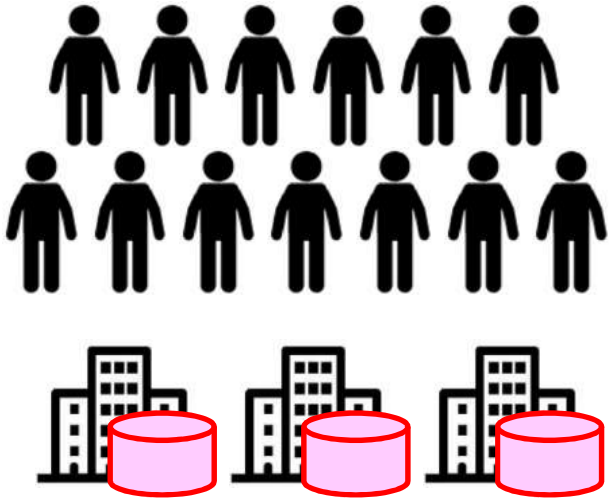
GDPRとパーソナルデータの利活用

2018-11-28 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管理運用

- 事業者にデータを集約
  - 管理が集中するので危険
  - 本人同意だけでデータが使えないので不便
  - データが散在して価値が低い



MyData

- 本人にデータを集約
  - 管理が分散するので安全
  - 本人同意だけでデータが使えるので便利
  - データが名寄せされて価値が高い

MyData: 本人主導のパーソナルデータ活用

- 個人向けサービスの価値向上にMyDataが必要
  - パーソナルデータの使用は原則本人同意で
  - 無数の個別サービスにおけるデータの共有・活用の管理は現場に分散させるしかない
  - サービス受容者にとっての価値を高めるようにデータを運用
- 価値のほとんどが個人向けサービスに由来
  - 国内で600兆円/年
    - 生活者向けサービス(家計消費) 300兆円
    - 勤労者向けサービス 200兆円?
    - 家事や育児などの無償サービス 100～140兆円

AIの基盤としてのMyData

- AIの運用に必須
  - AIによるサービスの相手はほとんどが個人
  - AIが良質のサービスを提供するには、その個人に関するリッチな(構造化された潤沢で詳細で正確な)データが活用できる必要がある
- AIの開発を容易に
  - 多数の個人から本人同意でデータを収集して分析

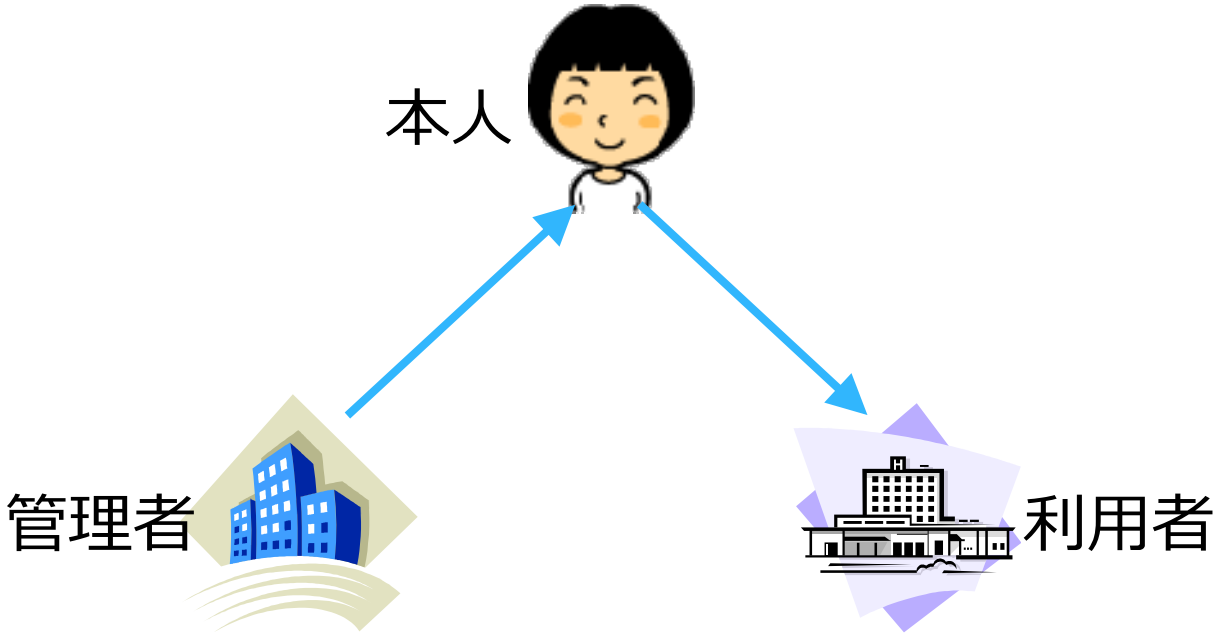
GDPR: General Data Protection Regulation

- パーソナルデータに関連する人権の保護
- EEA (EU含む31ケ国)域内の個人のデータが対象
  - **域外の事業者にも適用**
  - 英国も同様の法制
- 2018年5月25日施行
- 第7条: データ処理に関する同意
  - 同意の取消は随時可能で同意と同程度に容易
- 第17～19条: 訂正・消去・処理制限の権利
  - パーソナルデータの管理者は本人の請求に応じてデータを訂正・消去・処理制限
    - 子供のころSNSに載せた情報など
  - 管理者は当該データの開示先にもその旨を通知
- 第20条: **データポータビリティ**の権利
  - データ管理者に提供した自分のデータを、構造化され一般に利用されている機械可読な形で受け取り、当該管理者の妨害なしにそのデータを他の管理者に移転することができる
  - cf. 日本の個人情報保護法第25条(情報開示)は電子的開示を求めていない
- 第22条: 自動的決定(プロファイリング等)に従わない権利
- 第45条: データの域外移転には移転先での十分なデータ保護が必要
  - 顧客や従業員のデータ
  - 日本はGDPR施行前に十分性認定を受けられる?
- 第83条: 罰金
  - 2,000万ユーロと年間全世界売上の4%の高い方

EEA加盟国以外の国民も

データポータビリティ

- MyDataの必要条件
- パーソナルデータの利用者を本人が自由に選ぶ
  - パーソナルデータの管理者がそのデータを扱いやすい形式で電子的に本人に提供
  - 本人が自らの意思でデータを他者に開示



中国のデータ戦略

- 网络安全法(サイバーセキュリティ法)
  - ネットワーク運営者の監視、データローカリゼーション、他
- 中国人民銀行による網聯と暗号通貨
  - 国内の全キャッシュフローを政府が把握
- 信息安全技术 个人信息安全规范(個人情報セキュリティ規準)
  - **GDPRと同様のデータポータビリティ等を規定**
    - **EUと同様の事業環境で企業を育成**
  - 個別サービスを政府が集中管理するのは無理なので、パーソナルデータの活用を本人に委ねる
  - 政府は市場でのデータ流通を促進し、全データを検閲可能
    - 国としてはEUの十分性認定を求めず
    - 各グローバル企業が個別にEU等に対応

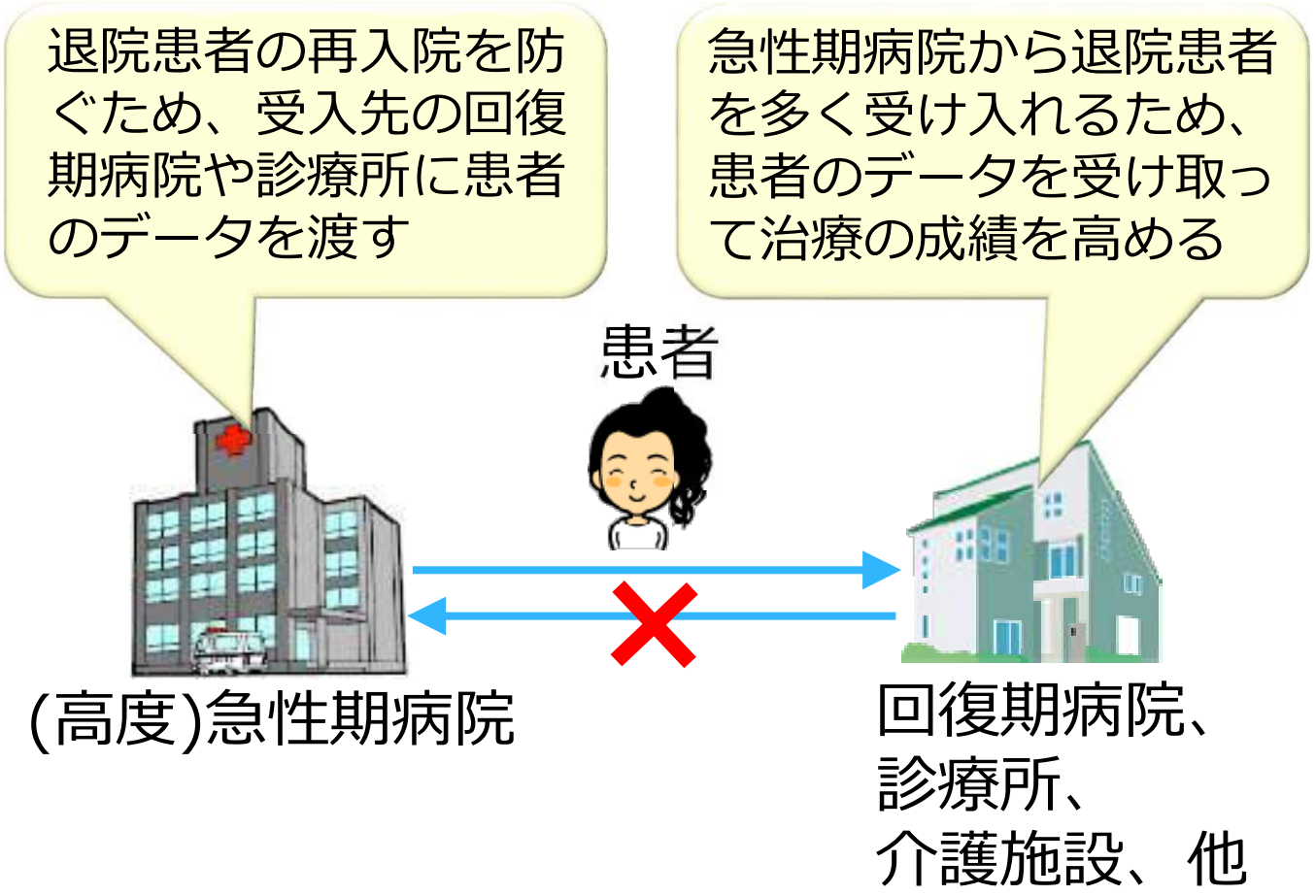
ターゲティング広告の終焉

- アドブロックの普及
  - Adobe社と広告ブロック対抗サービスを展開するPageFair社は、アドブロックによって失われた2015年の広告収入が218億ドル(ネット広告全体の14%)に上ると推計(2015年8月10日)。
- 2018カリフォルニア消費者プライバシー州法
  - 一定規模以上の企業は、州民からの要望に応じて、収集した個人情報(本人が提供した情報に限らず)の電子的開示、削除、販売停止等の義務を負う。罰則規定あり。2020年施行予定。
- eプライバシー規則(クッキー法)
  - 利用者のサービス使用記録を追跡したり会話からデータを収集したりするには本人同意が必要。利用者がデータ収集に同意しているか否かによらず同じサービスを提供せねばならない。GDPRと同じ罰則。2019年施行予定。
  - 米CITIグループは、欧州全体でディスプレイ広告売上の70%が失われデジタル広告予算が33%減ると予測。

日本でも進むMyData

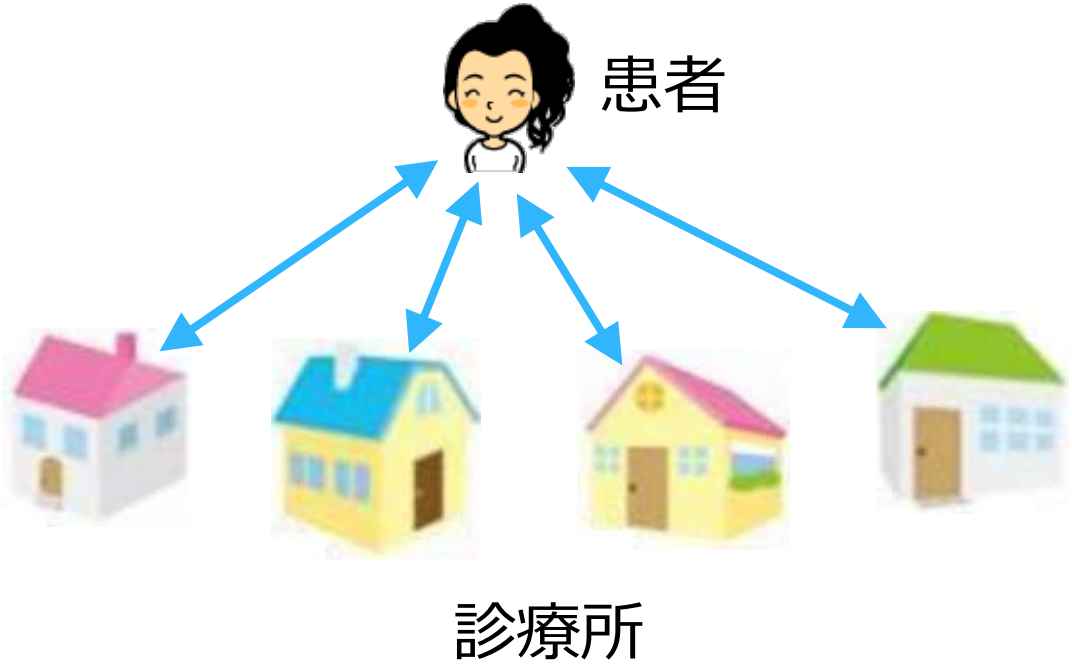
- 2005～2025年: 医療制度改革等
  ⇨ **ヘルスケアデータのポータビリティ**
  - 医療機関や介護施設の間でのデータ共有が必須に
  - 2020年から薬剤情報や特定健診等のデータをマイナポータルで本人に提供
- 2018年春: 改正銀行法施行 ⇨ **購買データのポータビリティ**
  - API公開を銀行に事実上義務付け
  - キャッシュレス化+電子レシート
- 2019年: 情報銀行・情報信託サービスの開始
  - 三菱東京UFJ信託銀行、三井住友銀行、電通、…
- 2021年: 大学入試改革 ⇨ **教育データのポータビリティ**
  - eポートフォリオ(電子学習記録)を生徒本人が管理運用
  - eポートフォリオを生涯に拡張: スタディ・ログ
- 2020～2021年: 個人情報保護法再改正
  ⇨ **一般的データポータビリティ**

医療制度改革：異種事業者間のデータ共有



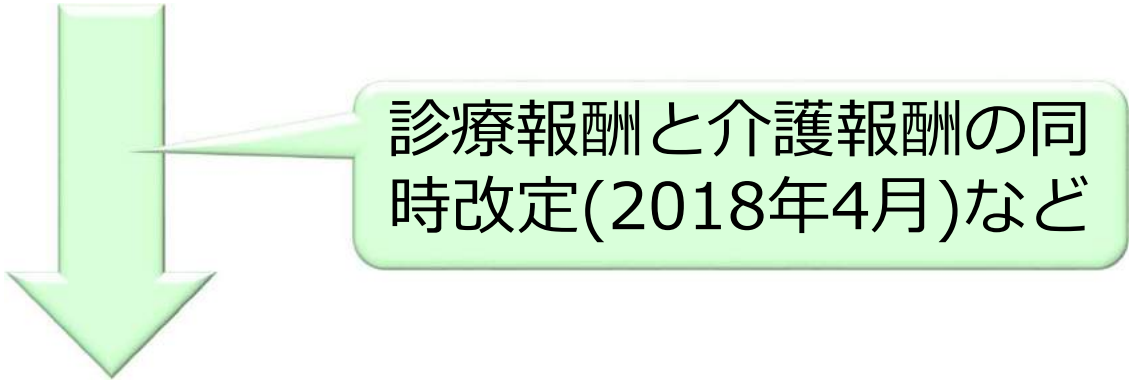
医療制度改革：診療所間のデータ共有

各患者に24時間365日の在宅医療を提供するため、複数の診療所(各々はほとんどが医師1人)がグループを組んで患者のデータを共有



医療データのポータビリティ

- データを共有すれば良い医療ができるが、そんなことをしても儲からない



- データを共有しないと経営が成り立たない
  - ◆厚労省の方針: 各患者に本人のデータを集約

マイナポータルの本格運用
(未来投資戦略2018)

- PHR (Personal Health Record): 本人等にデータを提供
  - 2017年度～予防接種歴
  - 2020年度～特定健診、乳幼児健診等の健診データ
  - 2021年度～薬剤情報等の医療データ
- API開放等により本人の許諾を受けた民間サービス事業者もデータ活用可能に
- 民間サービスの創意工夫を促進
  - 介護サービスの提供状況等の本人・家族等へのフィードバック、電子版お薬手帳との連携など

個人情報保護法制2,000個問題

- 個人情報保護法以外に自治体等の個人情報保護条例と個人情報保護審査会がある。
- 徳島市個人情報保護条例

第12条　実施機関は，保有個人情報の電子計算機による処理を行うに当たって，**実施機関以外の者との間で電気通信回線により電子計算機その他の機器との結合を行ってはならない。**ただし，次の各号のいずれかに該当するときは，この限りでない。

(1)法令等の規定に基づくとき。

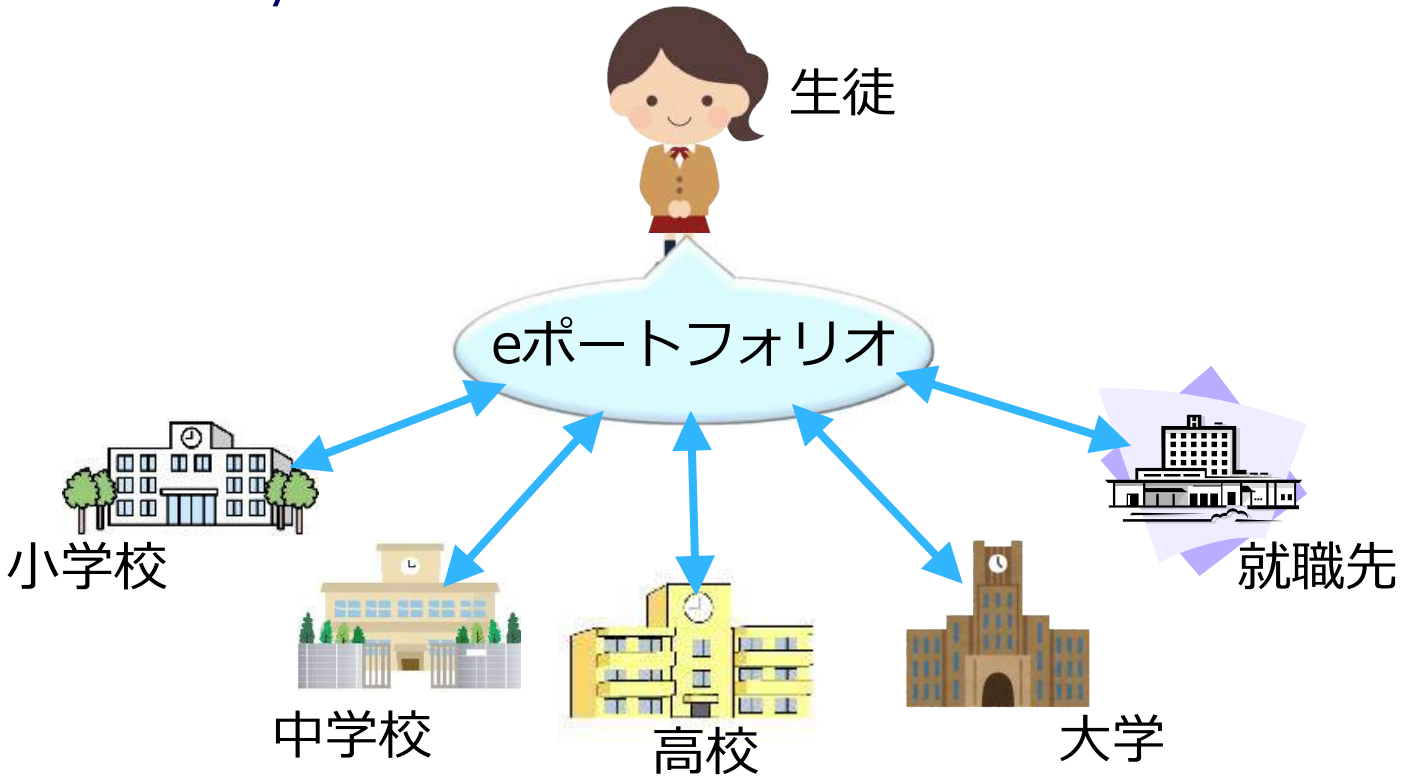
(2)当該結合が公益上必要であり，かつ，実施機関があらかじめ徳島市情報公開・個人情報保護審査会の意見を聴いて定める電子計算機の結合に関する基準を満たすとき。

購買データのポータビリティ

- 銀行サービスのオープンAPI
  - 改正銀行法 … cf. EUのPSD2
- モバイル決済
  - Amazon Pay、楽天ペイ、AliPay、他
- 電子レシート
  - 経産省の実証、CCCのカッテミル、ローソンスマホペイ、他

教育・学習データのポータビリティ

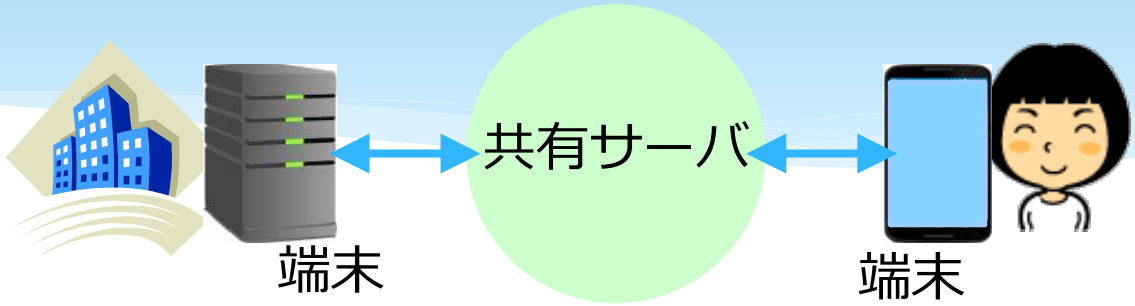
- 2020年度からの新制度の大学入試
  - 入試の成績だけでなく高校3年間の学業や課外活動のデータも考慮して合否を決定
  - 受験生はその電子データをeポートフォリオで作成して出願の際に大学に提出
- 各個人が一生にわたりeポートフォリオ(スタディログ)を運用
  - 文科省「Society 5.0に向けた人材育成」



PDS: Personal Data Store

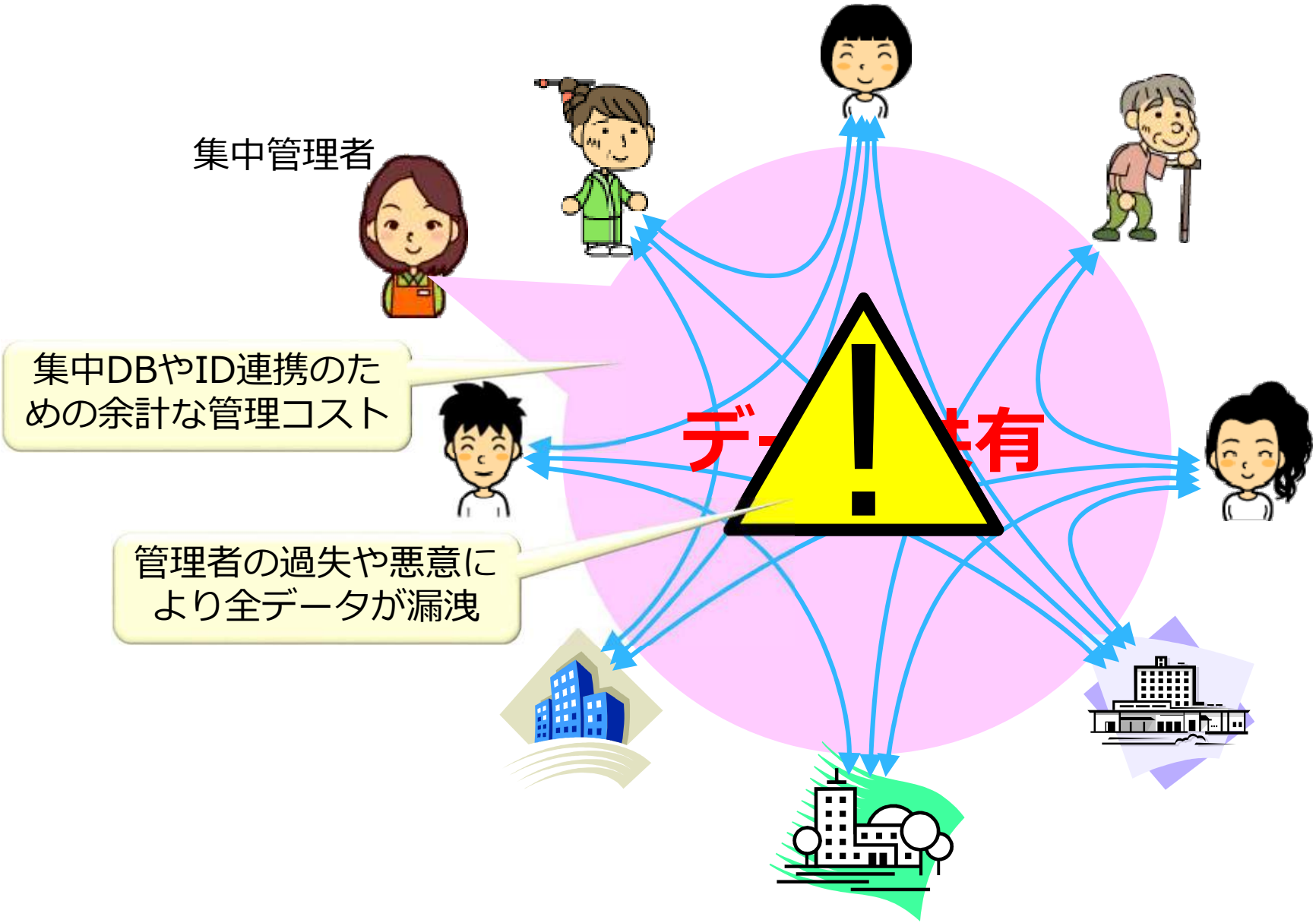
- パーソナルデータを本人の意思で共有・活用する仕組み
- MyDataの必要条件
- 概念そのものは部分的には古い:
  - 星新一(1970) 声の網. (情報銀行)
- 主な機能
  - データの**管理**(アクセス権限の設定)
  - データの**保管**
  - アクセス権限を持つ者によるデータの**活用**(取得、名寄せ、分析、可視化など)
  - アクセス権限を持たない者からのデータの**秘匿**

PDSの分類



共有サーバ	例	備考
専用	Personium、Cozy、OpenPDS、HAT、Meeco、Solid	**専用サーバの導入・運用コスト**がかかる。 専用サーバの管理者が全データにアクセスできるため、**全データ漏洩のリスク**が生じ、データ漏洩を防ぐための**管理コスト**がかかる。 顧客のデータを預る情報銀行等もこのタイプ。
専用(ブロックチェーン)	MedRec、MyDee	ブロックチェーンの導入・運用にコストがかかる。 **ブロックチェーンの機能はデータの管理だけ**なので、保管と活用と秘匿に他の仕組みが必要。 データを保管する共有サーバがなければ**個人同士のデータ共有が不可能**。
非専用	**PLR**	端末アプリ(と既存の非専用サーバ)でデータの管理と保管と活用と秘匿が可能。
なし	digi.me、CitizenMe	**個人同士のデータ共有が不可能**。 個人端末が稼働していないとデータ共有できない。 **大量データの共有が困難**。

データの集中管理



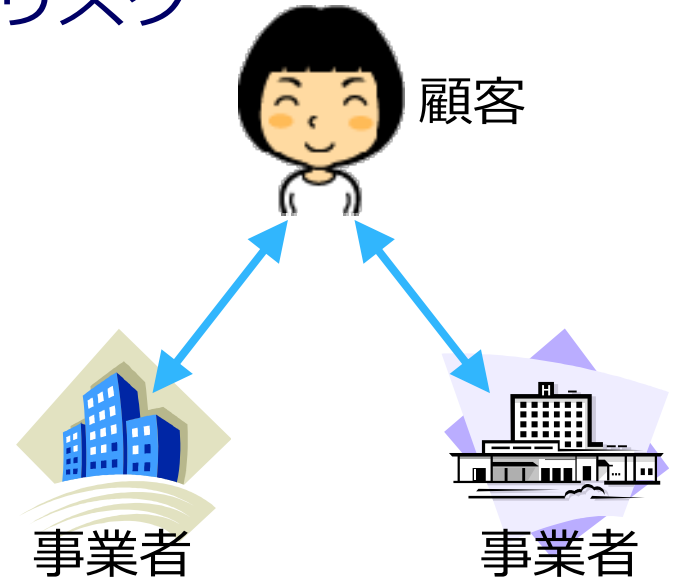
事業者間のパーソナルデータ共有

集中管理による共有は困難

- セキュリティ規準等の差違や事業上の競合により直接的共有は困難
- 全事業者のシステムを包摂する大規模なシステムは高コスト・高リスク

顧客が分散的に共有を仲介する方がはるかに容易・安価・安全

- どの事業者も顧客とは連携しやすい
- 顧客が運用する小規模なシステムは低コスト・低リスク

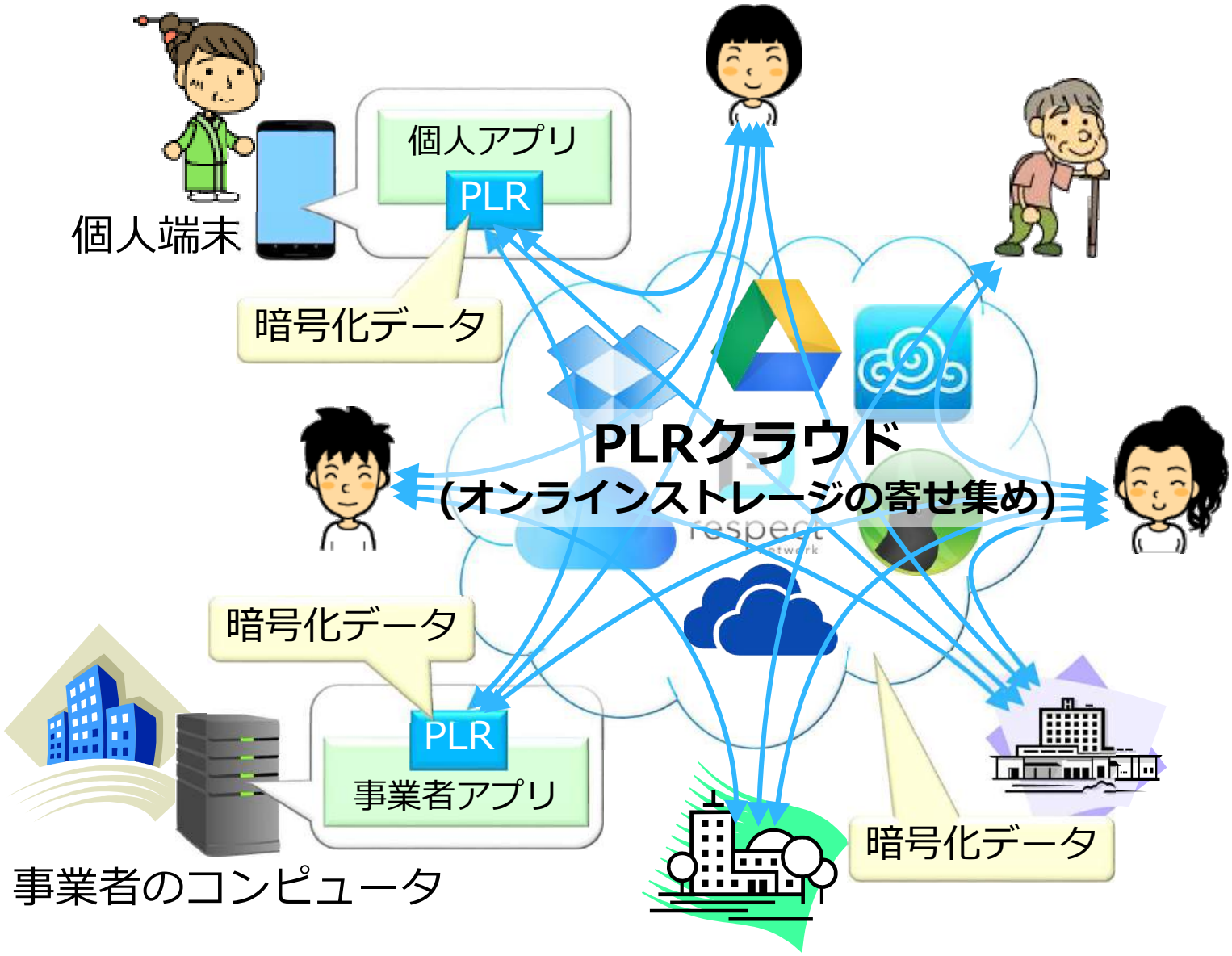


分散管理の必然性

データの管理者はデータ主体本人のみ

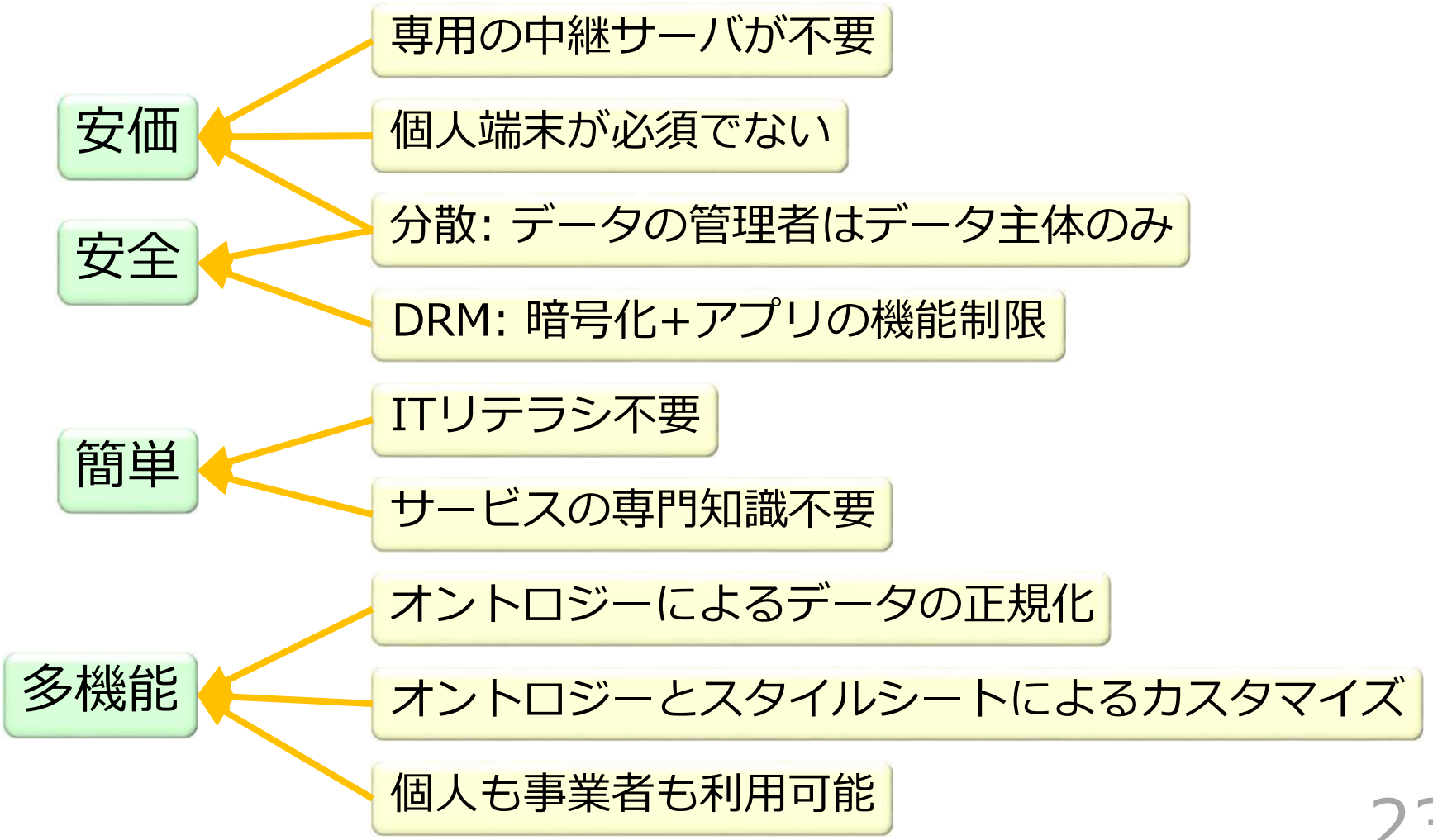
- 特定事業者等による全体の集中管理は不可能
  - データ主体とデータの種類が多いほど集中管理のリスクとコストが大きい
  - 複数のサービスを連携させる集中管理サービスはそれらのサービスよりデータ管理が大規模
- 個人が事業者等に開示したくない秘密の情報等は本人が管理するしかない
- 複数の集中管理サービスの間を個人が**分散PDS**でつなぐのが唯一の現実解

PLR: Personal Life Repository



PLRのメリット

- 下記の特長をすべて有する唯一のPDS
- 簡単で多機能な唯一の分散PDS



PLRは安全

- 分散管理: データの管理者はデータ主体本人のみ
  - 本人同意がなければデータへのアクセスが技術的に不可能
  - **集中管理者の過失等による全データの漏洩があり得ない**
- DRM (デジタル権利管理)
  - 暗号化 + アプリの機能制限
  - **過失による情報漏洩があり得ない**
    - 個人: PLRアプリは平文データを保存・送信できない
    - 事業者: 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通常の管理でセキュリティを安価に担保できる
- 紙やCDでデータを受け渡すより安全
  - 端末が他人の手に渡ってもデータを取り出されない
  - データの開示先を制限できる

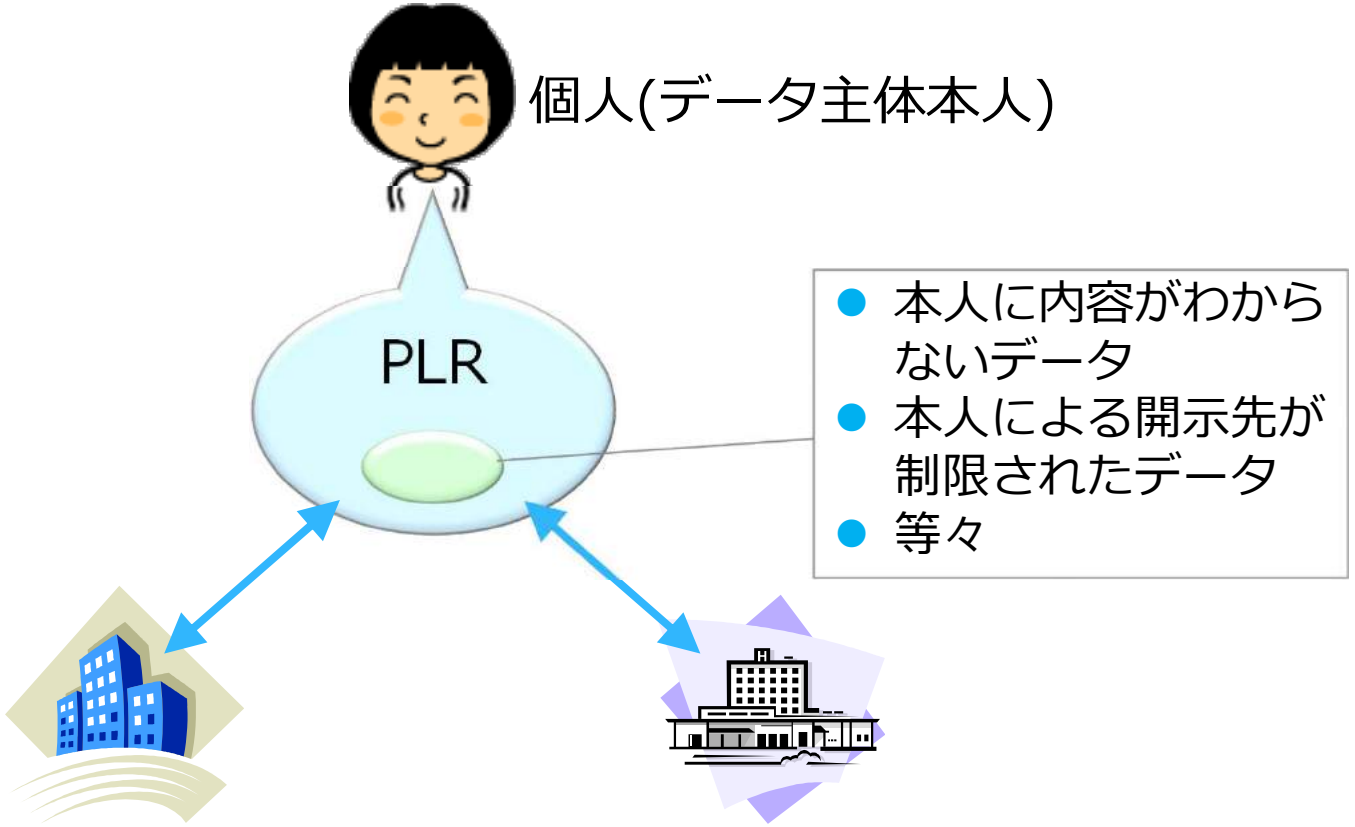
PLRは簡単

- 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**他の個人に委託**できる。

DRMによるアクセス制御

- データ作成者はデータ主体等によるアクセスを制限可能
  例1: 内申書を生徒に開示せずに高校から大学に渡す
  例2: 医師が患者に渡したデータを患者が開示できる先を限定



マッチング

- 個人のニーズに適合するサービスの選定
- ニーズ = 取引条件 + サービスの評価 + …
  - 取引条件: 取引(サービスの提供と受容)に同意する条件
- CRM (customer relationship management)
  - 事業者がマッチング
- VRM (vendor relationship management)
  - 顧客がマッチング

マッチングアルゴリズム

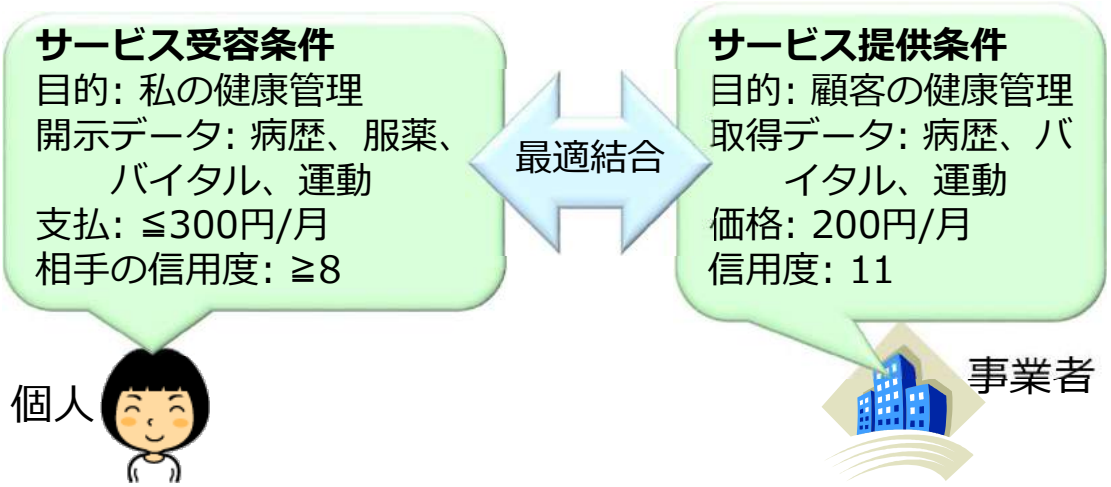
下記の2種類の処理を統合して個人端末で実行

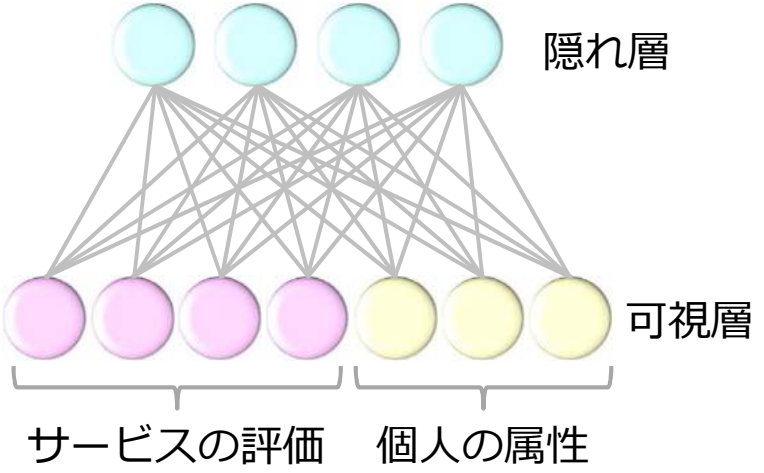
サービス参加者の取引条件を組合せて利得を全体最適化

- ゲームの求解?

サービス評価と個人属性のうち既知のものを入力して未知のサービス評価を推定

- 制限ボルツマンマシン?

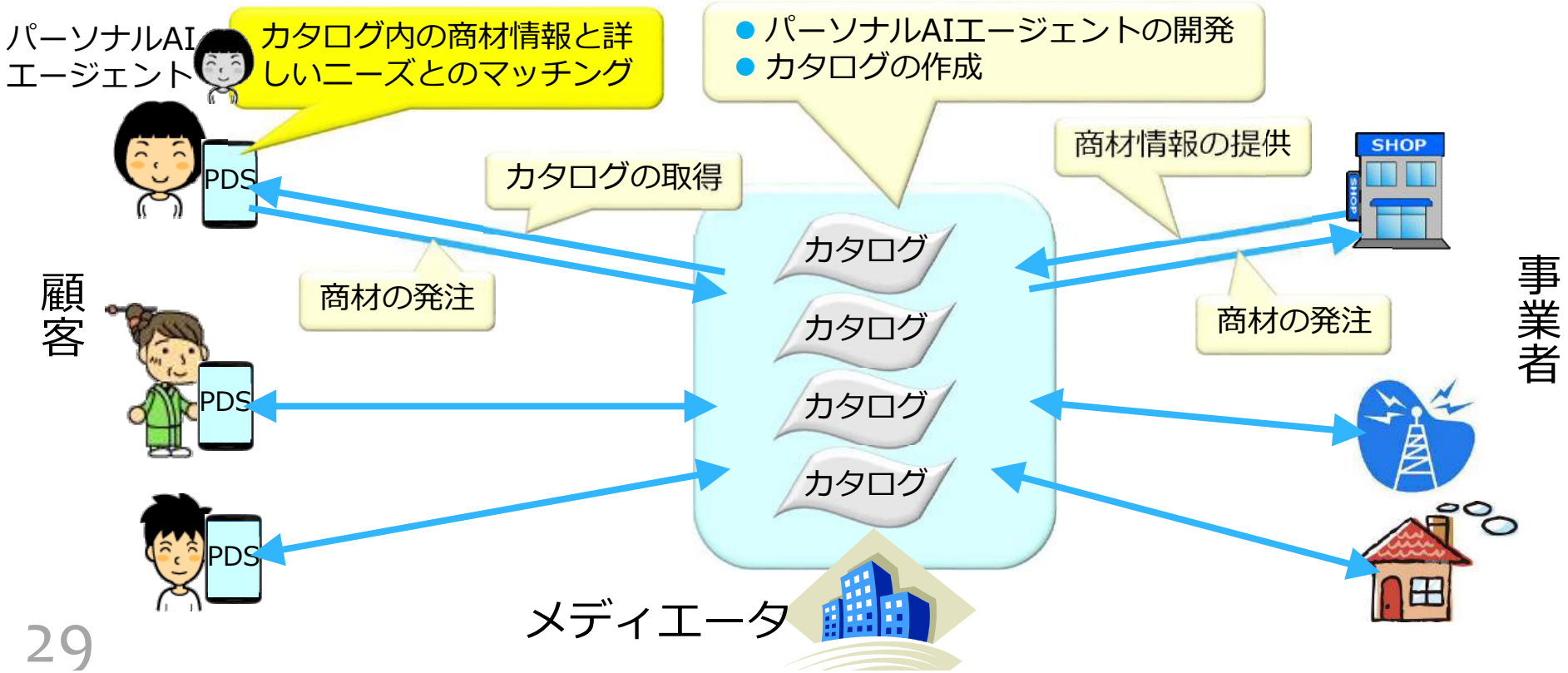




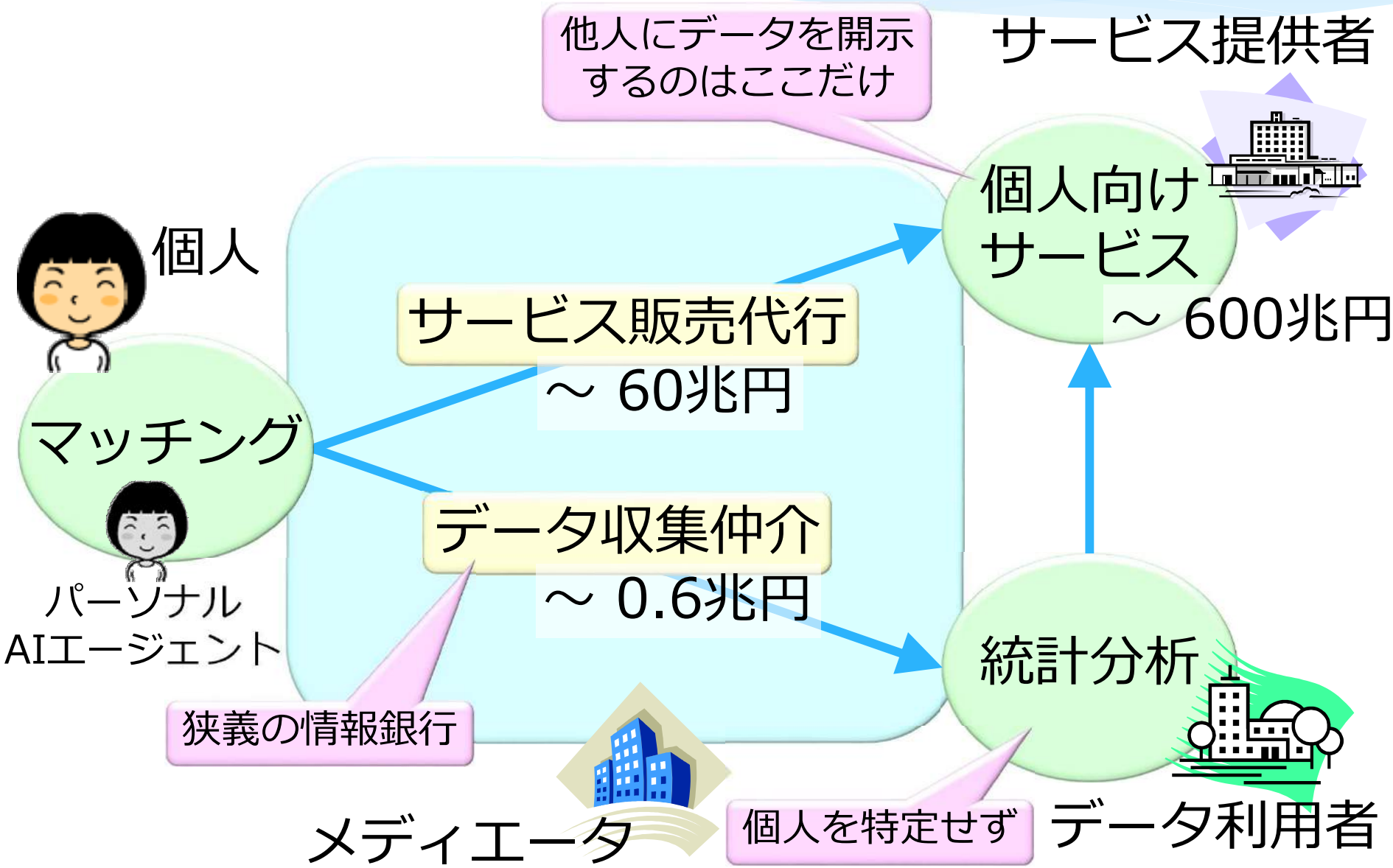
分散VRM

各個人のアプリが商材カタログを個人端末にダウンロードして詳しいニーズと商材の情報をマッチングした結果に従ってメデエータ経由で商材を購入

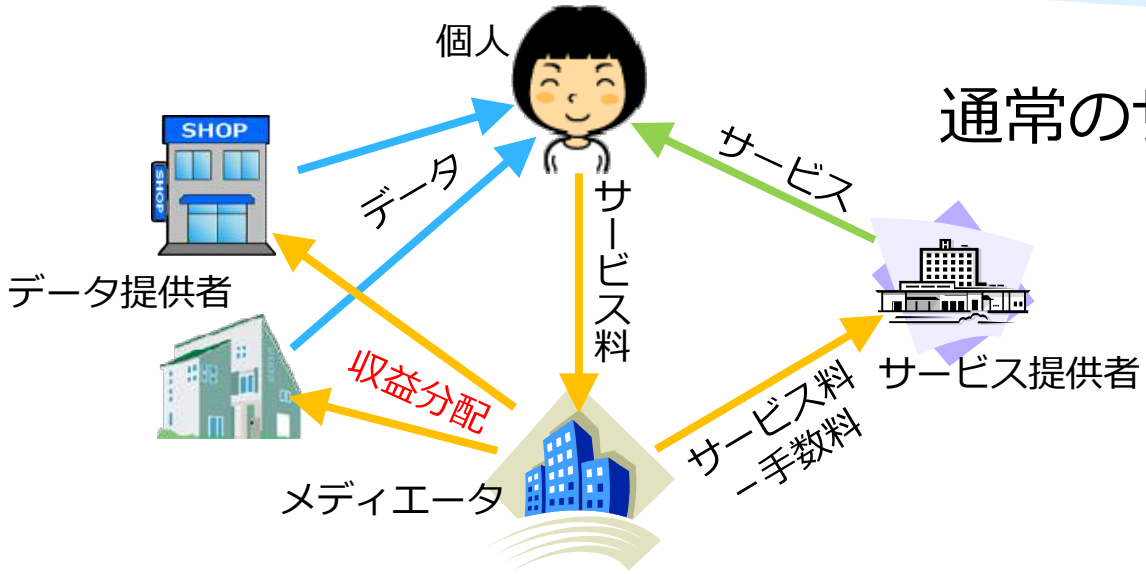
- 詳しいパーソナルデータを本人だけが使うので高精度かつ個人にとっても事業者にとっても安全
- メディエータにパーソナルデータを開示せずにメディエータのサーバでマッチングすることも可能



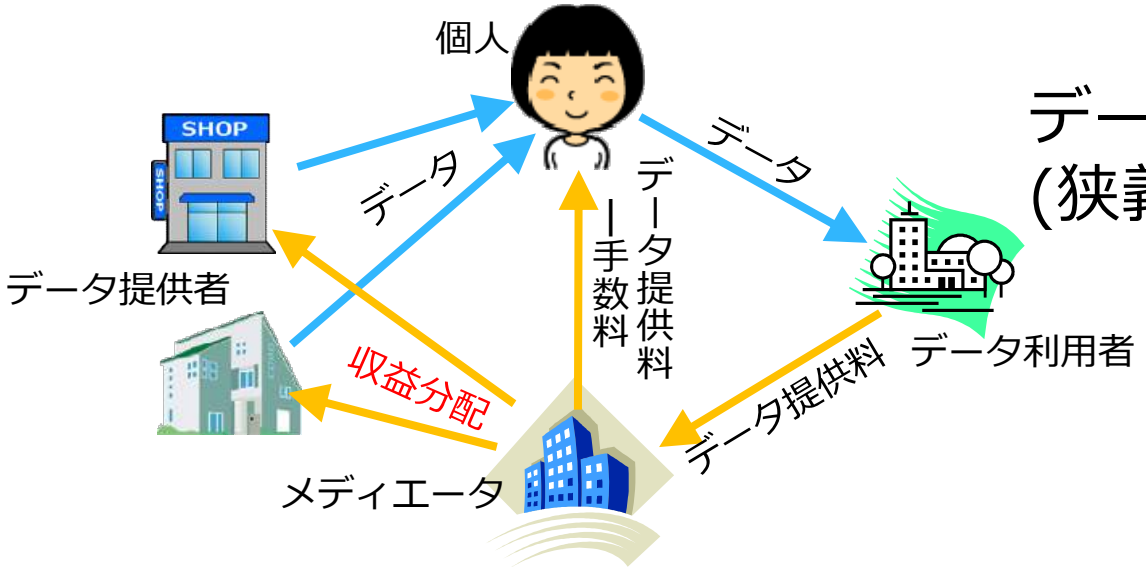
パーソナルデータの活用と価値



データポータビリティと収益分配

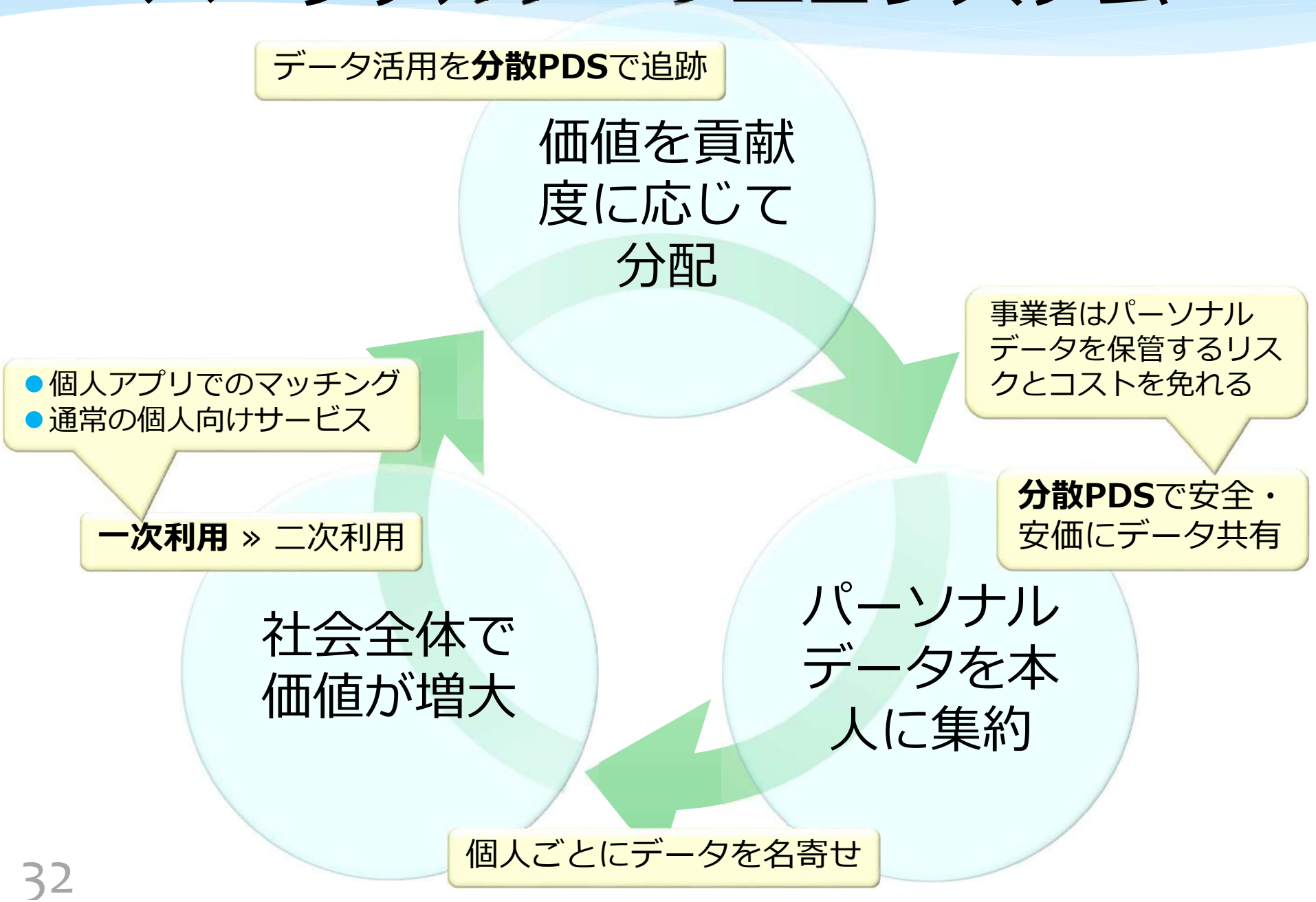


通常のサービスの販売代行



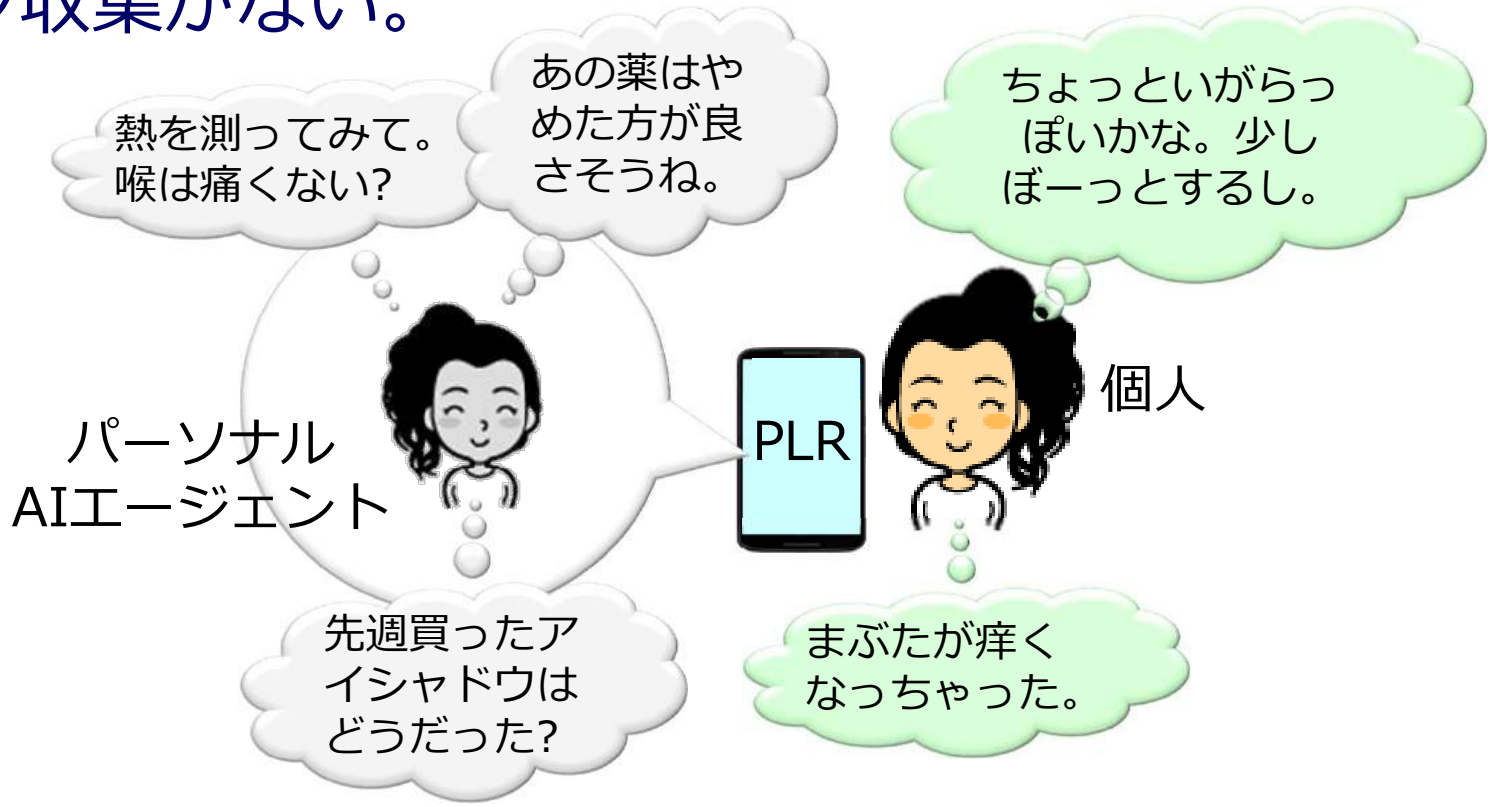
データ収集の仲介
(狭義の情報銀行)

パーソナルデータエコシステム



パーソナルAIエージェント

- PLRに付随し個人に属するパーソナルAIエージェントが本人から情報(商材の評価や本人の属性)を得てPLRに蓄積してマッチング(本人に適した商材等の選定)に活用。
- Amazon EchoやGoogle Homeと違って事業者によるデータ収集がない。

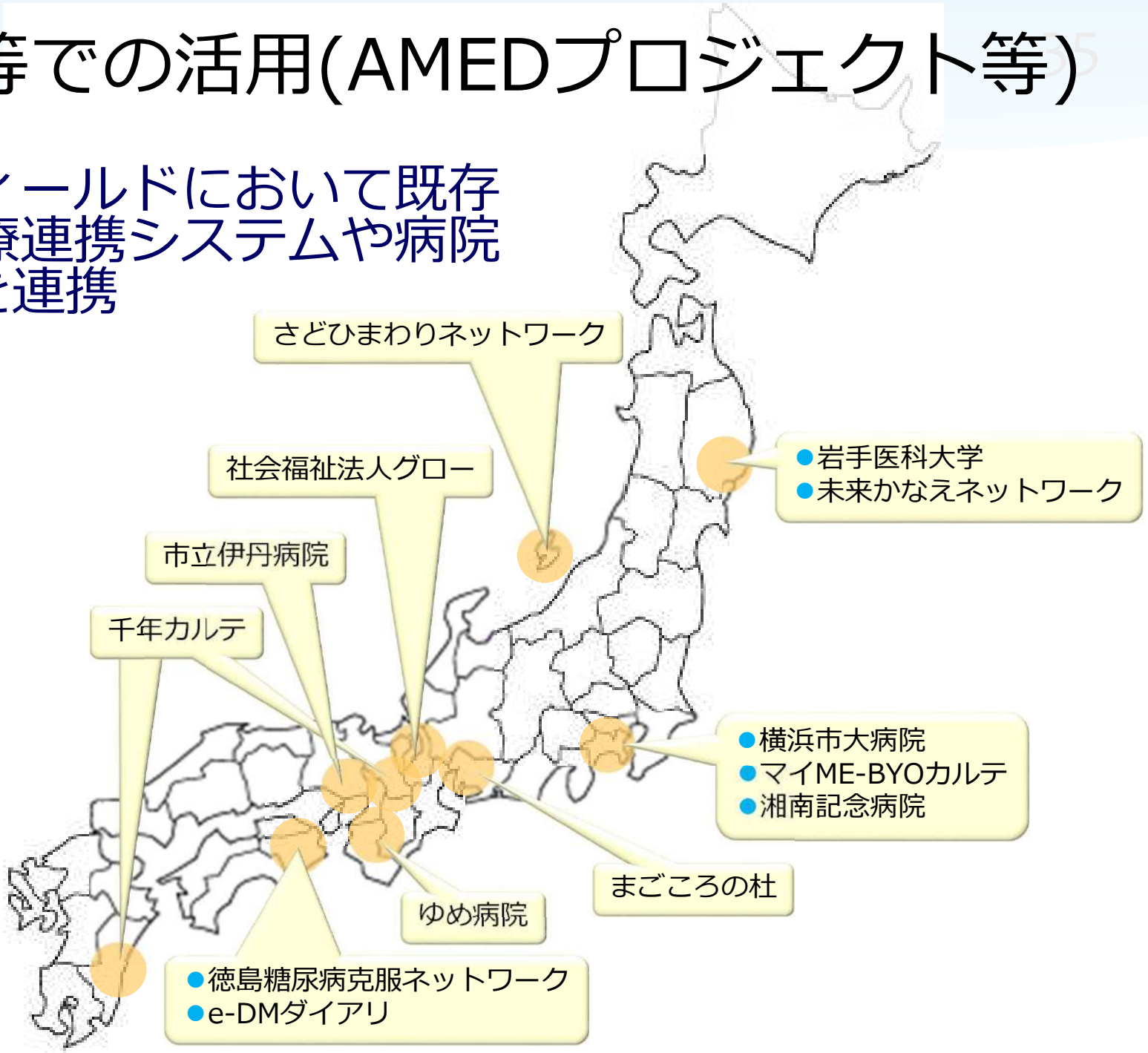


PLR第2版統合アプリ(Personary)

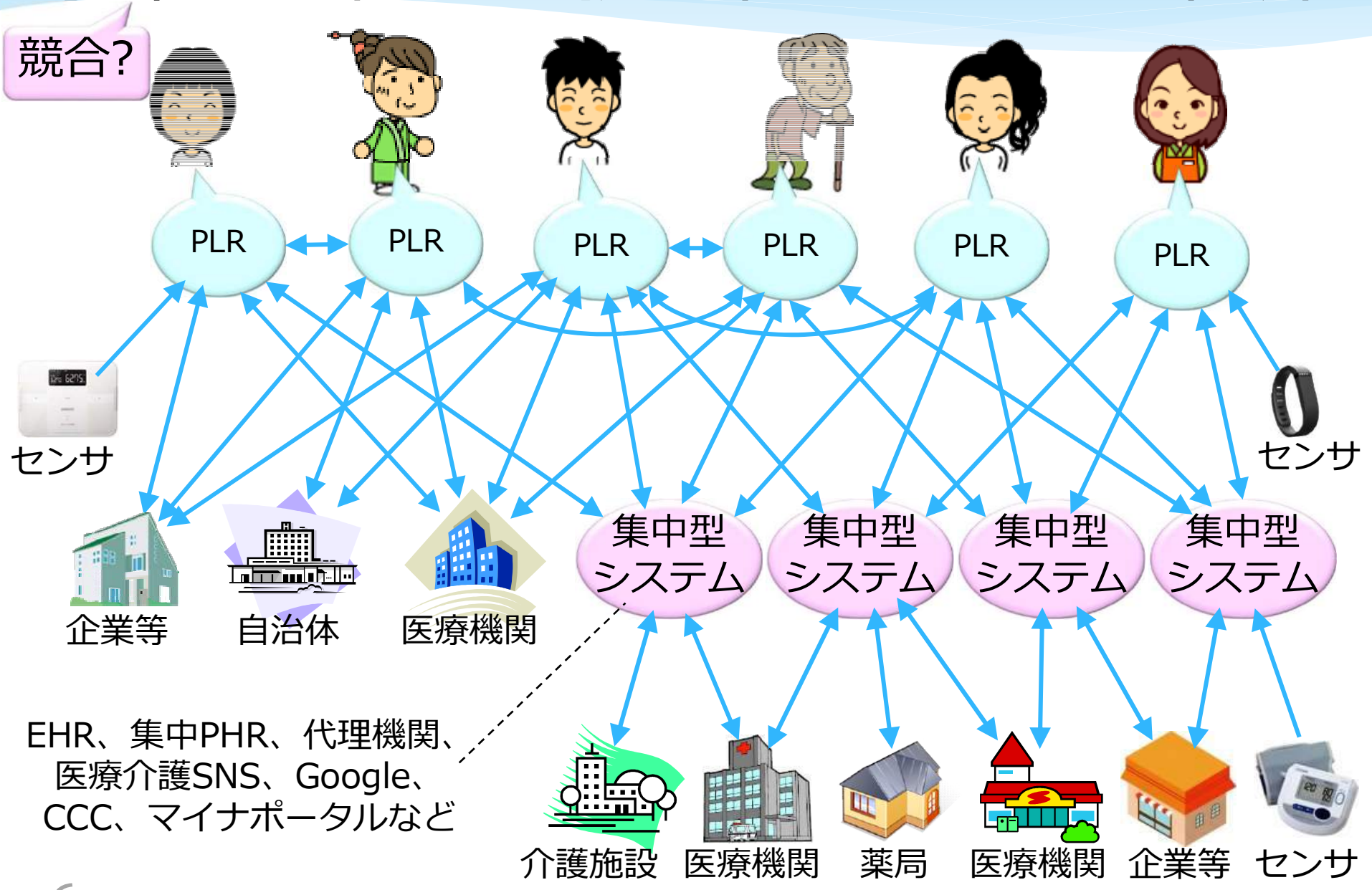
- マルチプラットフォーム
  - Android、iOS、Java
- 2018年～ 無料一般公開
- PLRの基本機能
  - 認証、暗号化/復号、通信
- データ共有
  - フレンド、グループ、同意の管理
- データ作成・活用
  - 生活録と問診(アンケート)
  - 自分/フレンド/グループのデータ
- カスタマイズが容易
  - データのスキーマ(オントロジー)
  - 画面と帳票のスタイル

医療等での活用(AMEDプロジェクト等)

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や病院とPLRとを連携

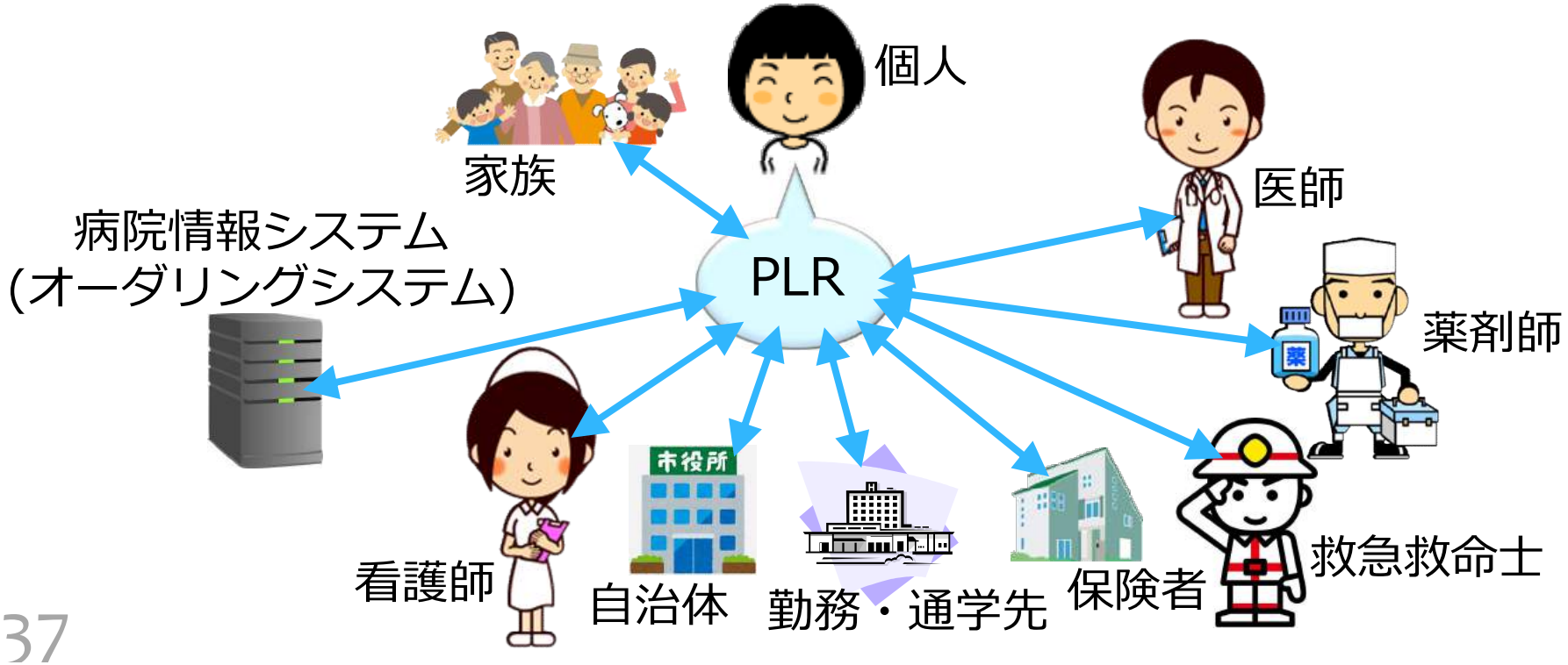


事業者の間の連携を個人がPLRで仲介



個人中心の情報システム

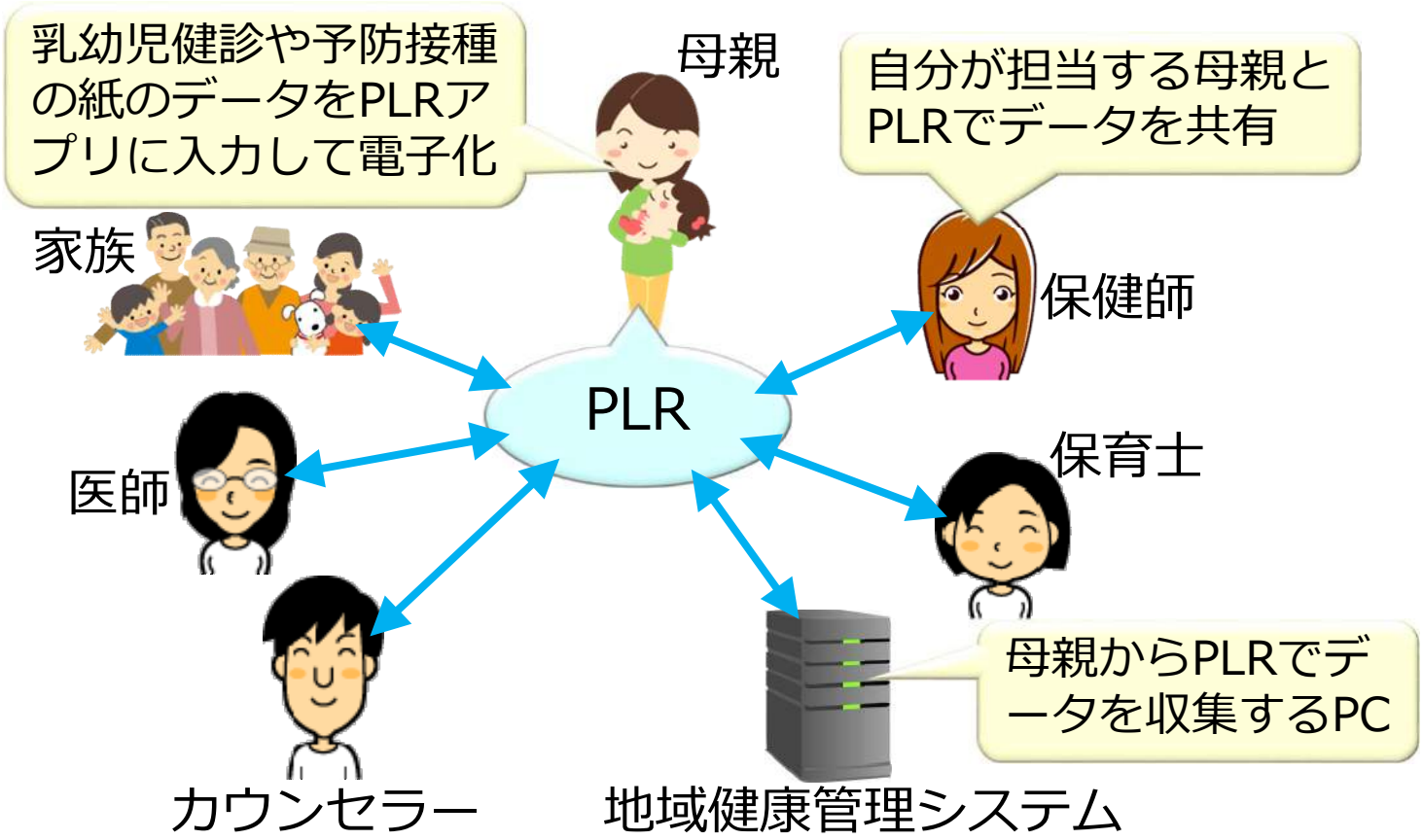
- 個人(代理人)が本人のデータを管理運用して多事業者・多職種と共有
- **本人の個票データの処理を集約**
  - 部門システムやPACSの機能を含む
  - 病院情報システムの機能はオーダリングや医事会計のみ



地域保健事業の電子化

人口3万人程度以下の市町村

- 紙の書類による保健業務を低コストで電子化
- 保健業務の効率向上
- 住民とデータを共有してサービスの質を向上
- 生涯健康手帳や地域包括ケアへの拡張



フレイル予防

PLRカード

個人

フレイルチェック

● 地域データ解析
● 健康づくり・介護予防政策の立案

個人アプリ PLR

市区町村

PLR 地域健康管理システム等

PLRクラウド

中継アプリ PLR

中継事業者

介護施設

PLR 介護アプリ

PLR 分析アプリ

PLR 事業者アプリ

PLR 電カル等

分析事業者

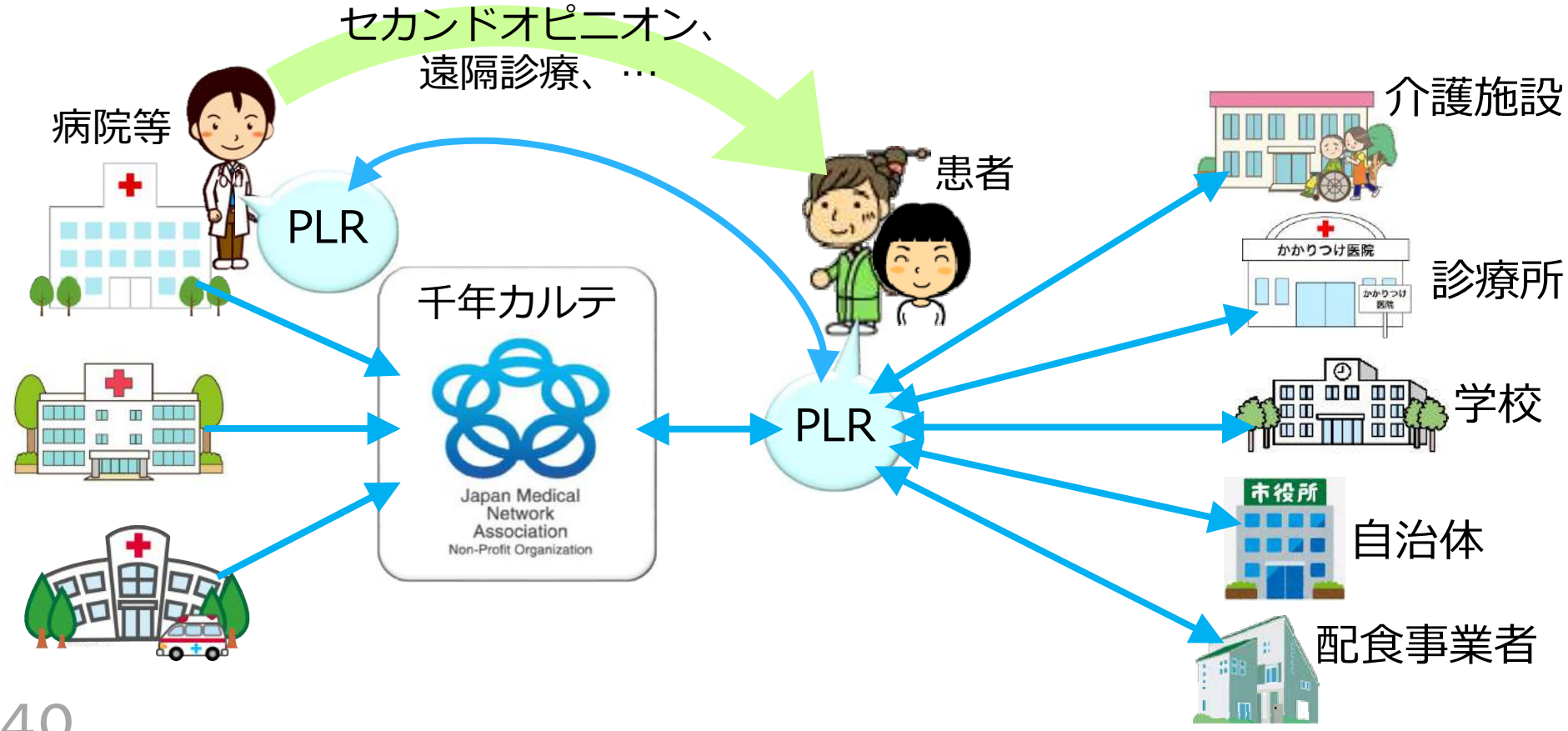
顧客別サービス、商品開発、事業戦略立案、他

企業等

医療機関

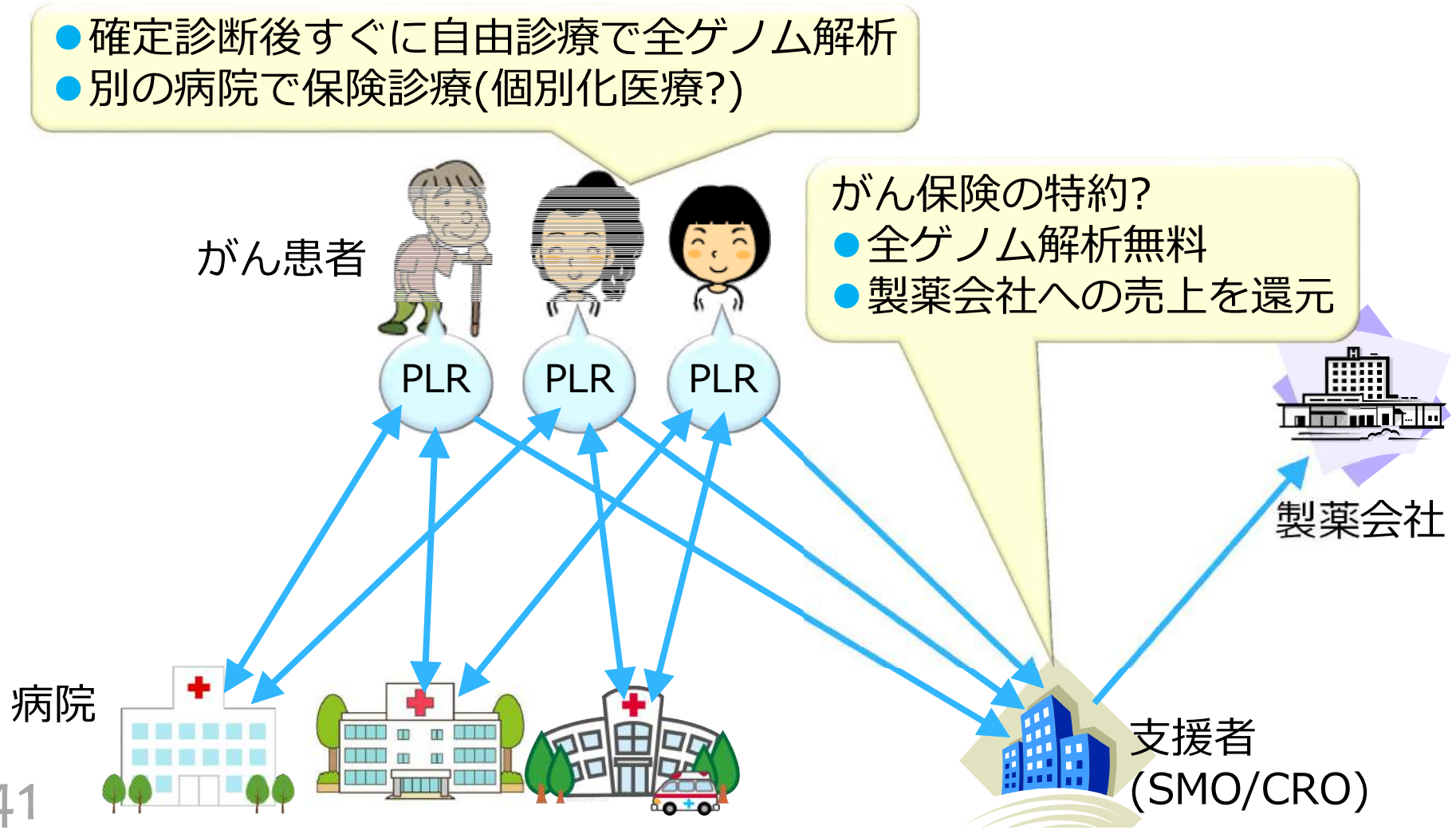
千年カルテとの連携

- 次世代医療基盤法に基づく医療情報匿名加工・提供機関が病院等から医療データを収集
- そのうちデータポータビリティに対応する千年カルテと連携することにより、遠隔診療や多職種間連携を実現



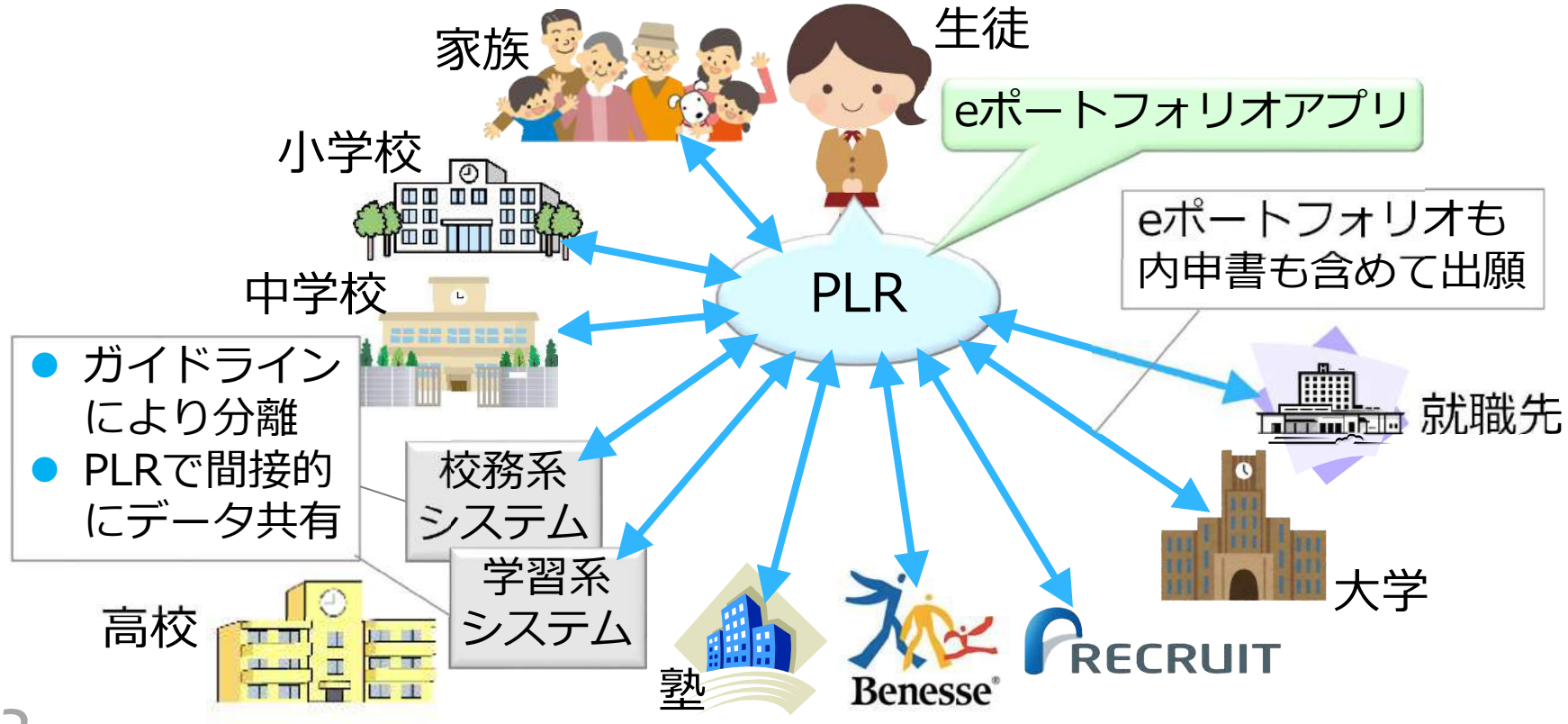
がんの全ゲノム解析

- 保険診療でのゲノム解析は手遅れになりがちで部分的
- なるべく早期の全ゲノム解析が望ましい



生徒本人主導のeポートフォリオ

- 2020年度からの新制度の大学入試で運用されるeポートフォリオ(電子学習記録)をPLRで実装
  - ◆ データポータビリティとセキュリティを確保
- データ活用の促進によるEdTech等の振興
- 埼玉県教育局が2019年度から実運用の予定



PLRによるeポートフォリオの運用

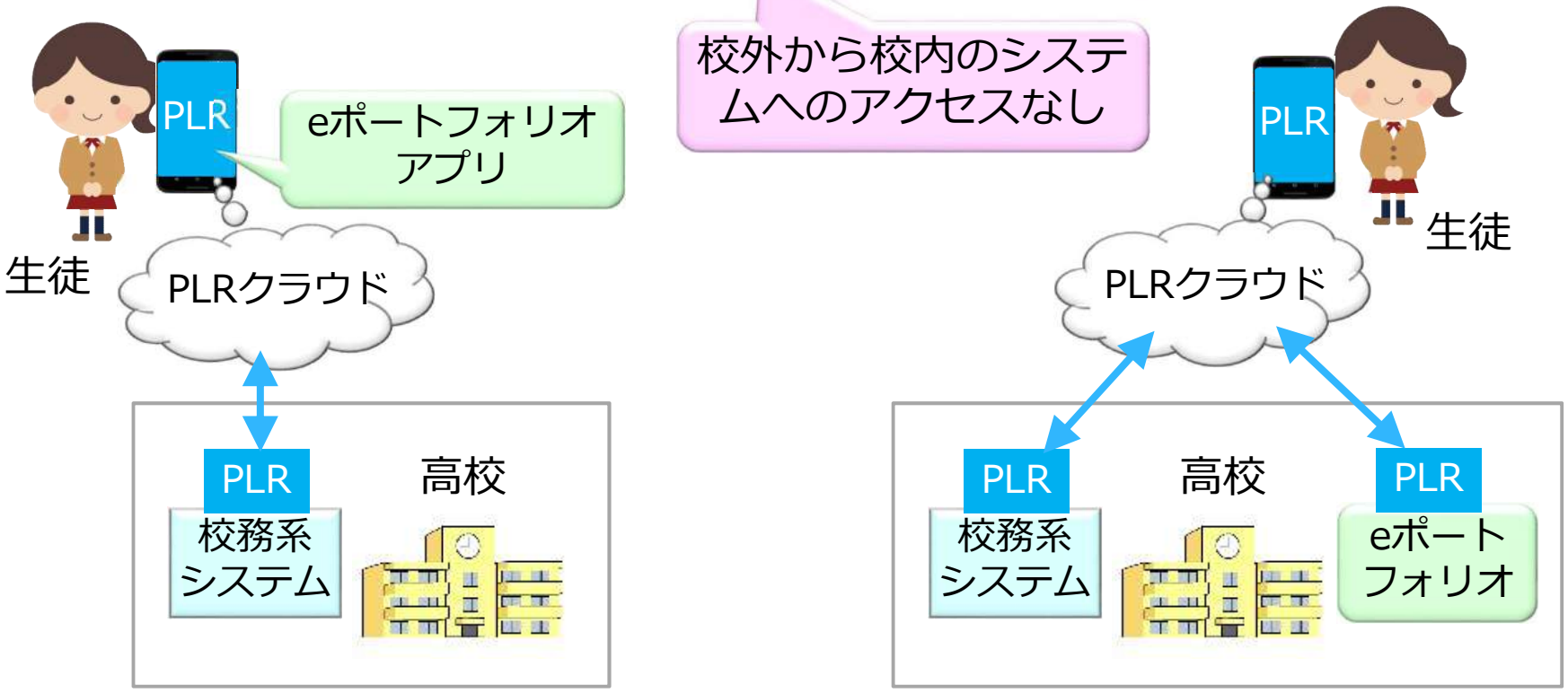
下記をすべて明確に満たす方法のうち最も安全で最も安価

1) **データポータビリティ**
2) 校務系システムとeポートフォリオとの連携
3) 生徒による校務システムへの不正アクセス防止
4) 校外から校内のシステムへの不正アクセス防止

PLRクラウド経由

生徒が見ても良いデータだけをPLRクラウドに

校外から校内のシステムへのアクセスなし



eポートフォリオが校外にある場合

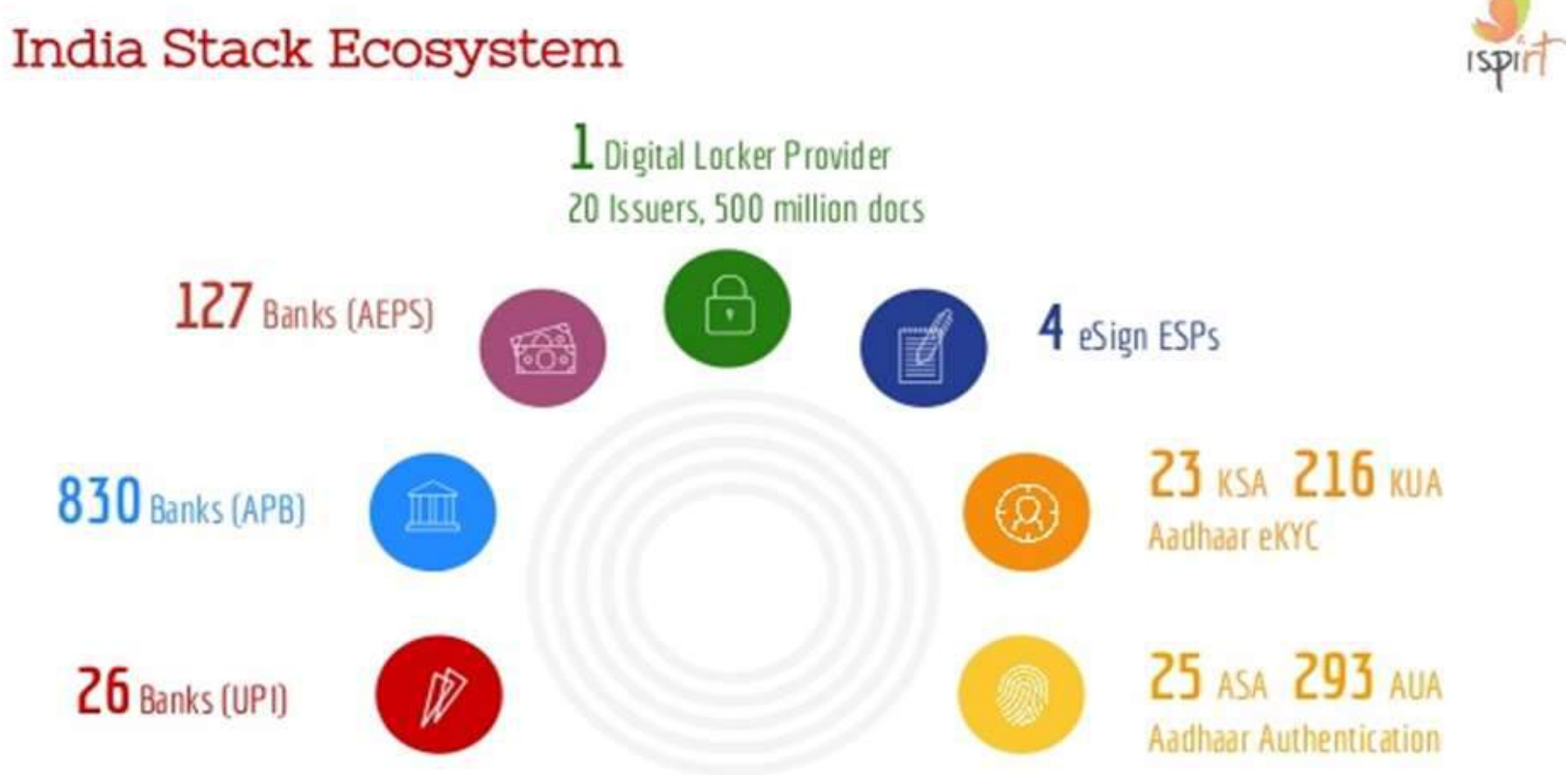
eポートフォリオが校内にある場合

スマートソサエティ：AIと融合した社会

- リッチなデータを活用するためのインフラ
  - データ流通
    - オープンデータ
      - 誰でも自由に使える
    - パーソナルデータ/企業データ
      - MyData: データ主体(個人/組織)がPDSにより自らの意思で自由に使える
      - データポータビリティ
  - デジタル通貨
    - コストや不正の抑制
    - 購買データの活用
  - 個人認証…マイナンバーカード等
    - サービスの利用: 銀行口座、税、教育、就労、他
  - オープンAPI
    - サービス連携、モバイル決済、データ共有
  - データの意味構造の標準化
- これらのインフラは安価なので、抵抗勢力の弱い国の方が有利
  - 途上国が先進国を10年後に1人当たりGDPで越える?

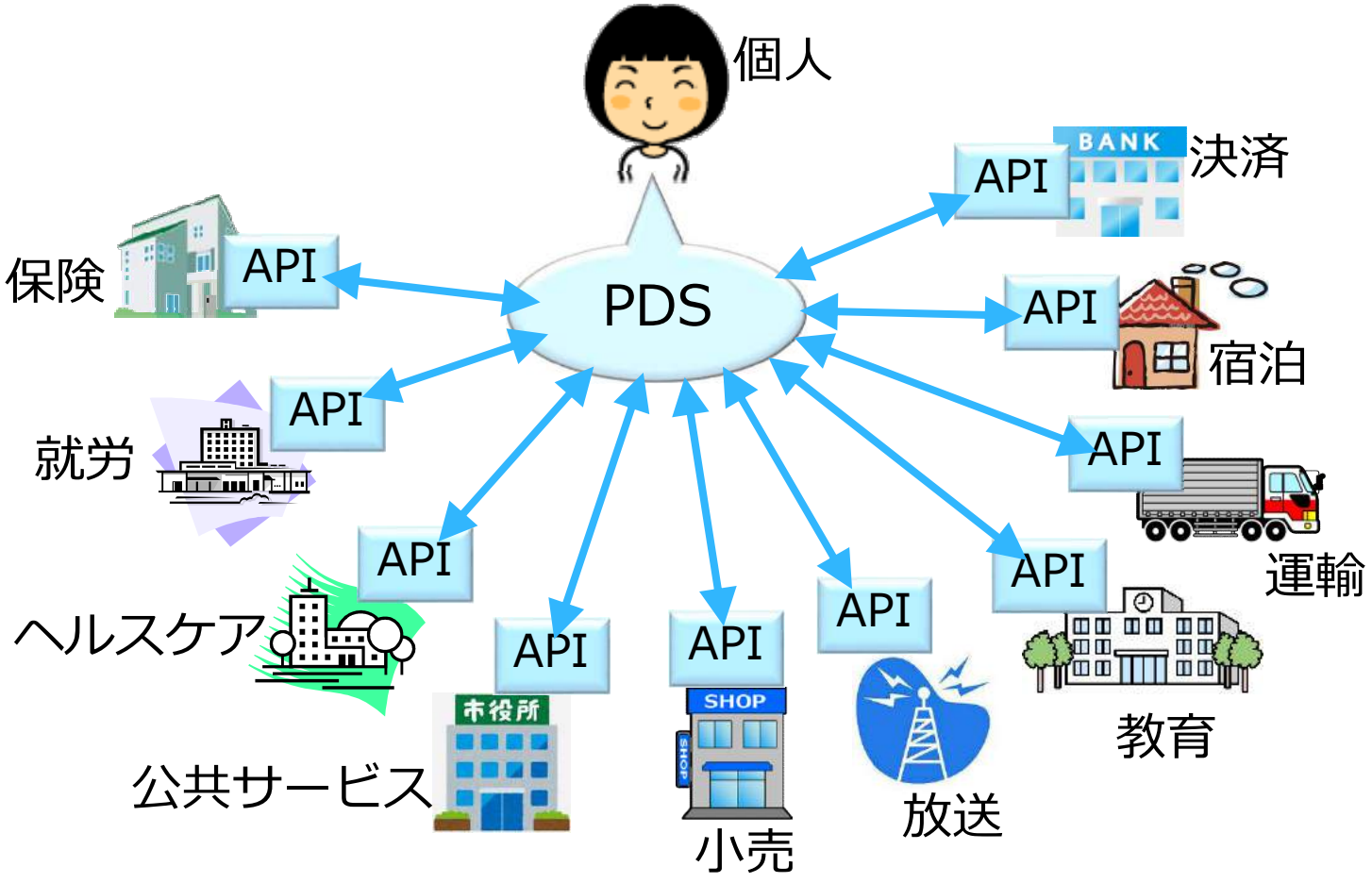
インドのオープンAPIとPDS

- 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
- 2016年末に高額紙幣の交換を停止
  - 現金とクレジットカードも廃止の予定?
- 銀行以外の民間企業や公的機関もサービスをAPIで公開
  - 個人がパーソナルデータを蓄積しサービスを連携させて利用



多数のサービスを個人が組合せて利用

- 個人向けサービスを本人が中心となって最適化
  - 情報共有等の間接業務を個人用AIが自動化
    - 大きな組織は不要



中国のスマートソサエティ

- モバイル決済
  - 購買、小遣い、割勘、施し、…
- 個人の信用スコア
  - 芝麻信用
  - データに基づいて個人を評価
  - 評価が高いと有利
- デジタルレーニン主義
  - 人間による計画経済は無理
  - AIによる計画経済は可能?
    - ビッグデータ独裁
- 全国の個別サービスを集中管理するのは無理なので、パーソナルデータの活用を本人に委ねること(PDS)が必要

まとめ: MyData

パーソナルデータを本人に集約することにより社会全体で価値が増大

- 必然性
  - 価値のほとんどを生む個人向けサービスの質を高める
  - 世界標準としてのGDPR
- 日本での普及
  - 医療制度改革等 ⇨ ヘルスケアデータのポータビリティ
  - キャッシュレス化 ⇨ 購買データのポータビリティ
  - eポートフォリオ ⇨ 学習データのポータビリティ
  - 個人情報保護法 ⇨ 一般的データポータビリティ
- 事業者のメリット
  - コスト・リスクの解消
  - データ活用
  - 収益分配
- メディエータ
  - 販売代行と収益分配
  - 国内市場規模>60兆円/年
  - 個人を中心に多数の事業者が連携 → 利便性と収益の増大