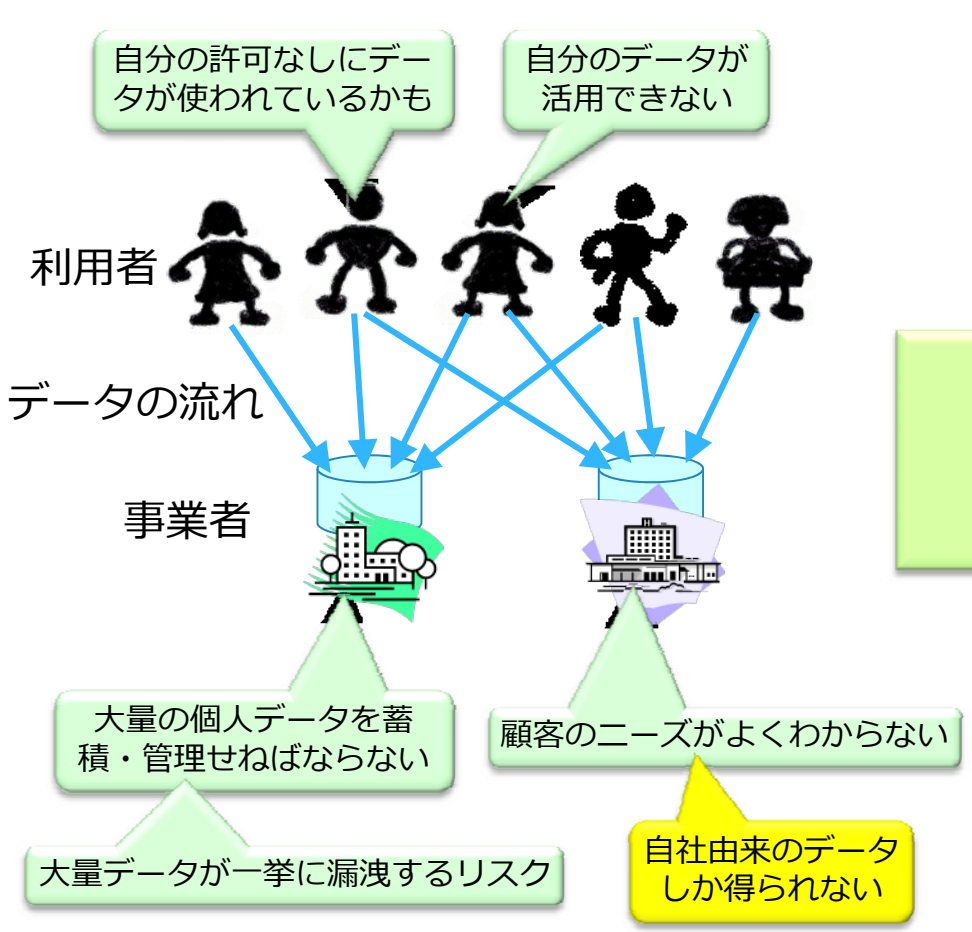
分散PDS

2015-10-05 橋田浩一

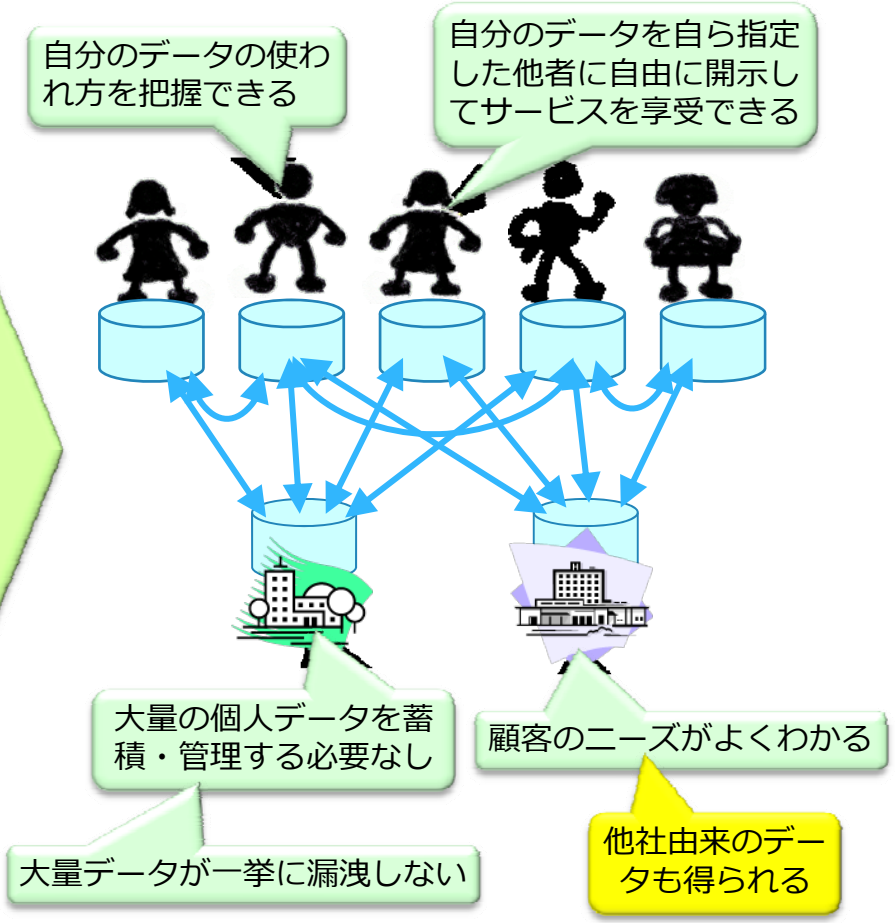
東京大学大学院情報理工学系研究科
ソーシャルICT研究センター

パーソナルデータの管理(1)

事業者に集中



＋ 個人に分散



パーソナルデータの管理(2)

物理的集中・分散ではなく管理権限の集中・分散

- 集中管理
  - 管理者の意思または過失により多数の個人のデータが利用または漏洩可能
    - ベネッセや年金機構の個人情報漏洩事件
  - 本人に直接メリットのないデータ利用(～二次利用)に適する
  - 顧客の連絡先や契約書の集中管理は事業者にとって必須
- 分散管理
  - 管理者(本人または代理人)の意思または過失により高々1人分のデータが利用または漏洩可能
    - データを盗むコスト > メリット
  - 本人に直接メリットのあるデータ利用(～一次利用)に適する
  - 多数のアカウントをシングルサインオンでまとめることにより個人ごとのセキュリティも向上

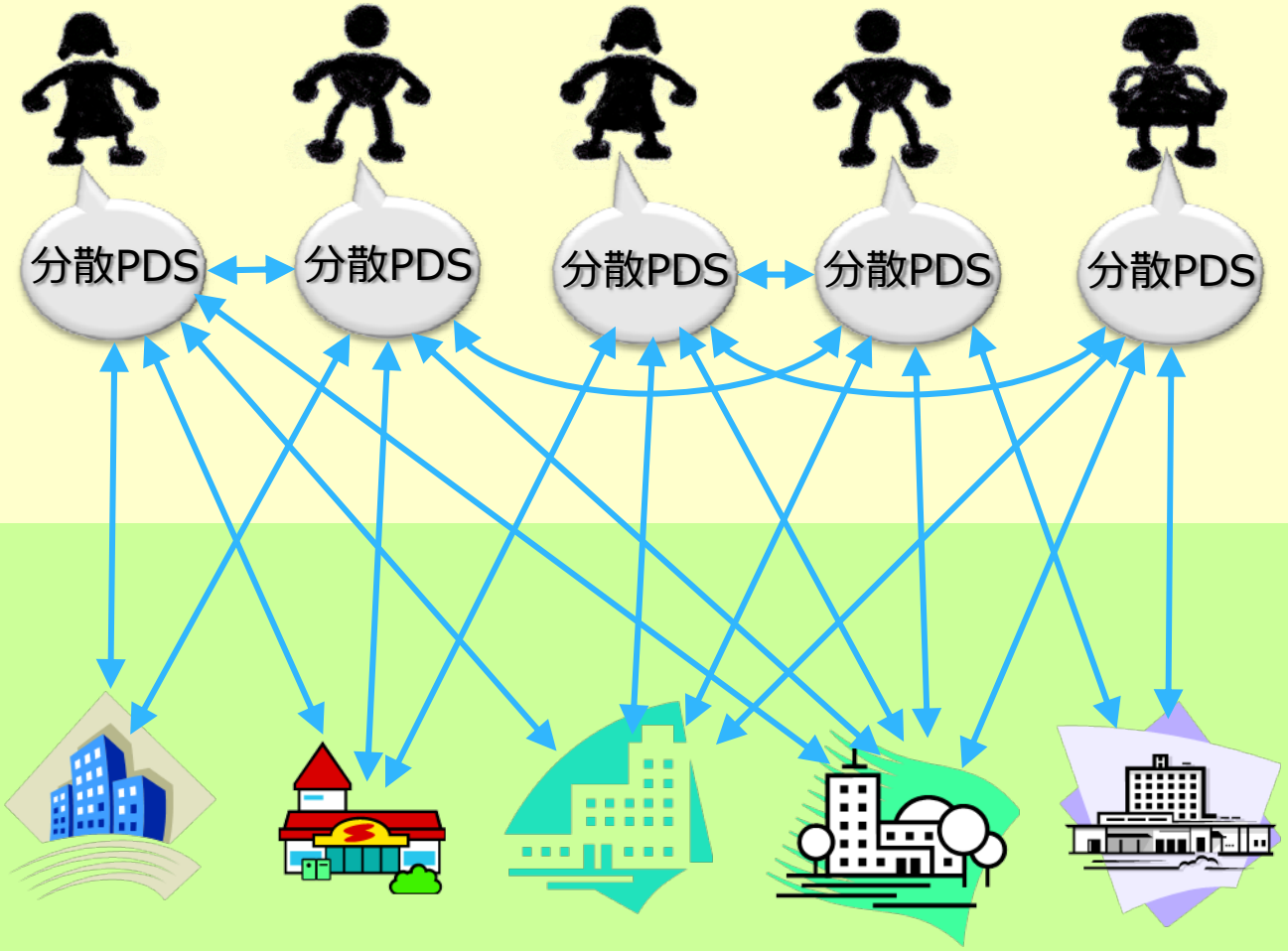
集中管理はスケールしない

- 単一の集中型サービスが市場を独占するのは不可能
  - 単一の医療介護SNSが全国に広がったり病院のデータをすべて取り込んだりすることはあり得ない
- 複数の集中型サービスを統合するのも無理
  - 技術的に高コスト
  - 競合する事業者同士は連携しない
- 特定事業者(病院等)がデータを抱え込んでいると顧客のメリットが高まらない
  - EHRの利用者は対象地域の人口の2%以下
    - 上野 智明(2014) ITを利用した全国地域医療連携の概況 (日医総研ワーキングペーパー No.321)

集めないビッグデータ

- パーソナルデータの集中管理(集めるビッグデータ)は必要だが問題が多い。
  - 自己情報コントロールが困難
  - 情報漏洩のリスク
  - 産業振興の阻害
    - 事業者による囲い込み
    - 本人の利益が最大化されない
- 個人に分散した管理(集めないビッグデータ)との組み合わせでこれらの問題を解決したい。

データ管理を個人に分散(集めないビッグデータ)



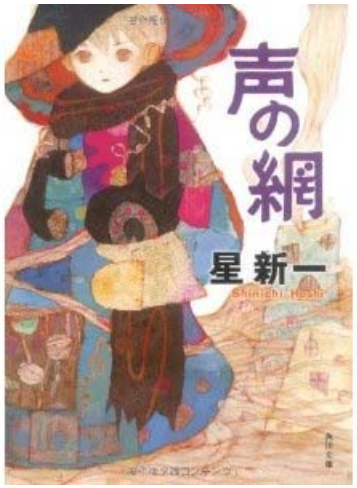
少数(1,000程度以下?)主体のデータの処理

多数主体のデータの処理(検索、情報抽出、統計分析、マッチングなど)

データ管理を事業者に集中(集めるビッグデータ)

PDS: Personal Data Store

個人が本人のデータを自ら蓄積・管理し、他者と自由に共有して活用する仕組み



- 星新一(1970) 声の網.
  - 情報銀行…東大・慶大・JIPDEC
- 2,000年ごろに提案された?
  - Gordon Bell (2001) A Personal Digital Store. *Communications of the ACM*, 44: 86–91.

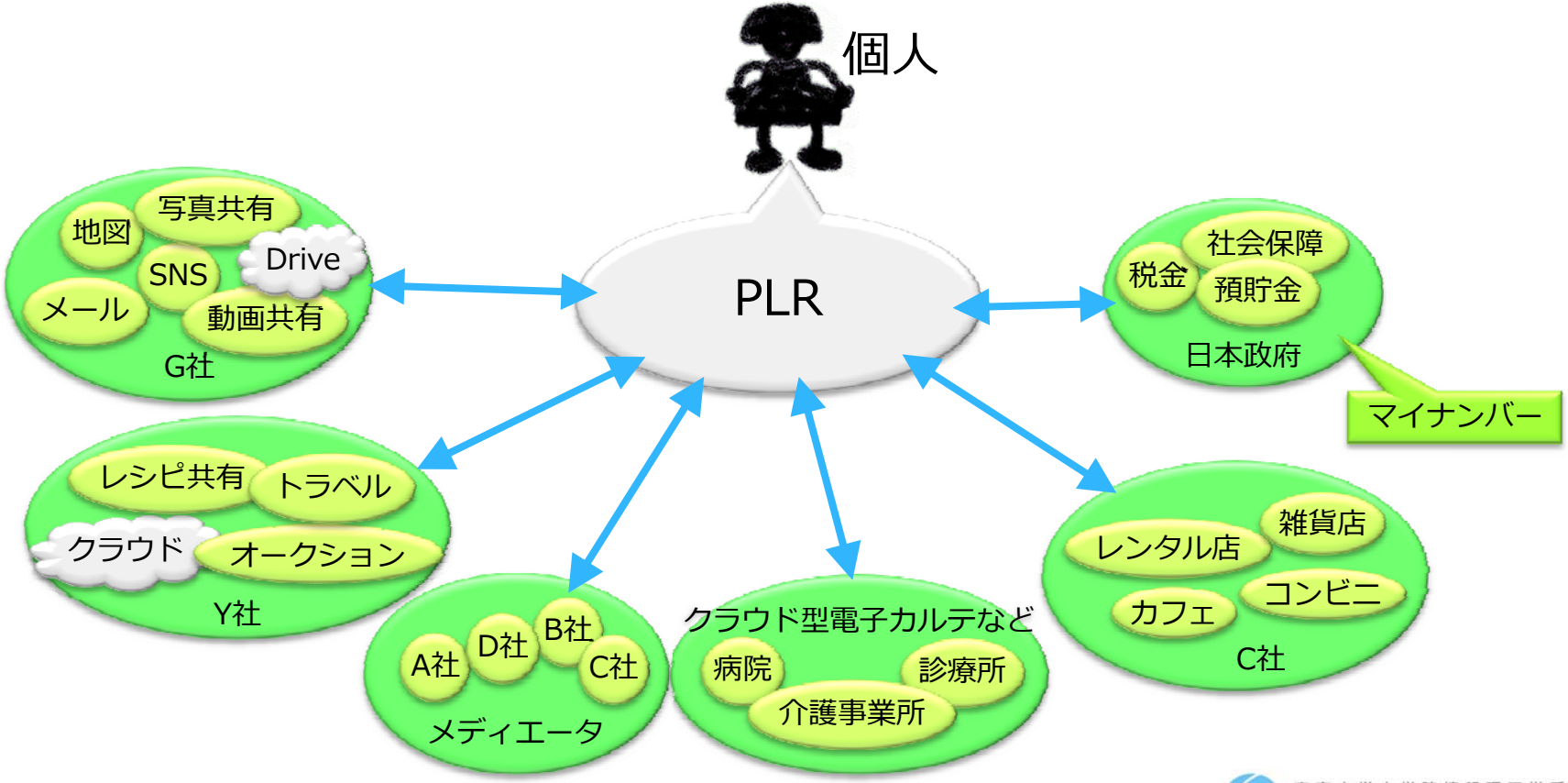
PDSの分類

- 集中PDS ～ メディエータ(後述)
  - EHR、従来のPHR、情報銀行、代理機関、…
- 分散PDS
  - P2P方式: 個人端末間のP2P通信でデータ共有
    - Personal Server
  - 中継方式: サーバを介してデータ共有
    - サーバ主導: サーバが特別な機能を持つ
      - Persona、VIS、PDV、PrPl、openPDS、RespectNetwork、…
    - 端末主導: 端末もサーバも既存のコモディティ
      - PLR (個人生活録; personal life repository)

分散PDSとしてのPLR

個人が特定事業者に依存せず本人のデータを管理して他者と安全に共有

- 1つの集中型サービス（緑の楕円）であらゆる個人データを管理するのは不可能かつ不適切。
- 複数の集中型サービスにわたる多種の個人データを組合せて活用するには、本人がPLRでそれらのデータを名寄せすることが必須。



PLRの構成

個人

PLRアプリ

暗号化や通信の詳細を気にせず開発

個人端末

PLRサーバ

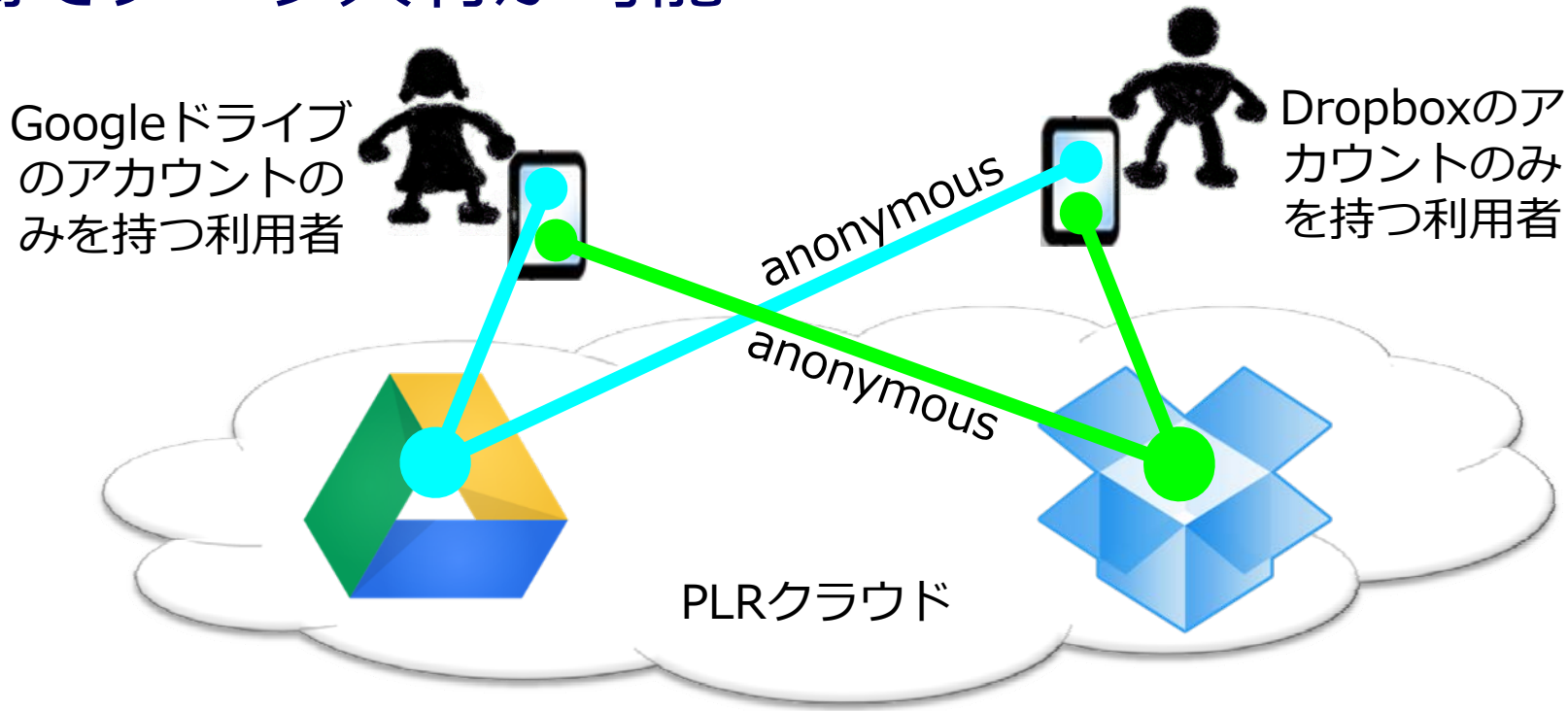
暗号化されたデータ

…

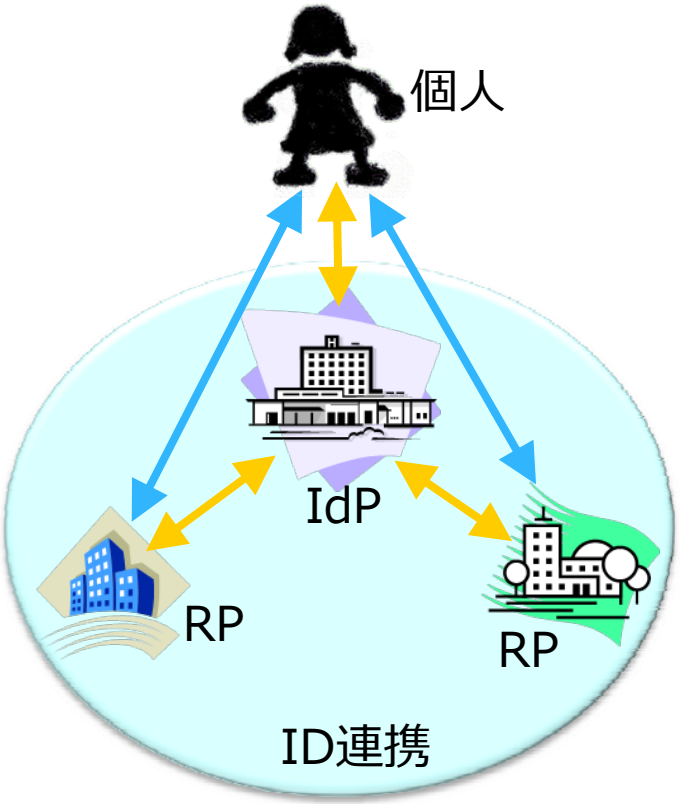
PLRクラウド

複数サーバの連携

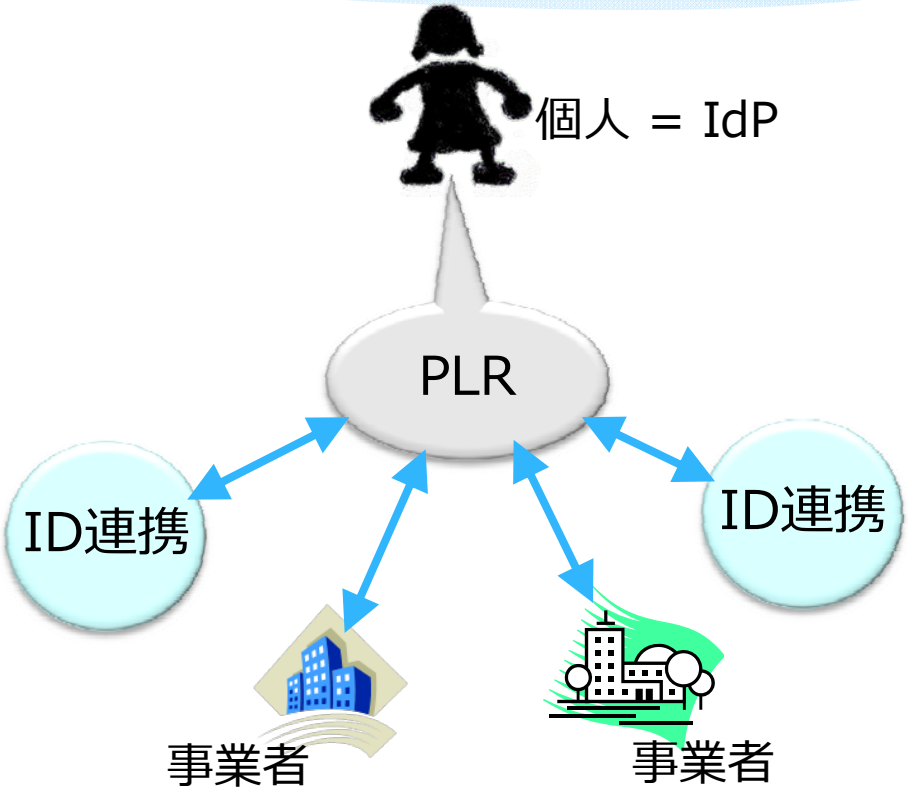
- PLRクラウドは複数のサーバ(Googleドライブ、Dropbox等)からなり得る
- 各利用者は自分がアカウントを持たないサーバにもanonymousでアクセスできるので、全利用者の間でデータ共有が可能



ID連携との比較



- 個人には本人のデータの流れがわかることが望ましい
- IdPにはデータの内容がわからないことが望ましい
- RPは他のどのRPにどんなデータを提供したかがわからないことが望ましい



- 個人には本人のデータの流れがわかる
- 事業者は個人経由で他の事業者にどんなデータを提供したかがわからない
- 複数のID連携の仕組みを統合可能
- 本人認証は外部のIdPによる

PLRのセキュリティ

データの不正使用を防止し、共有・活用を促進

1. 集めない: データの管理を個人に分散
   - 1人分のデータを盗むコスト > メリット
   - たとえ集めても処理が終わったらすぐ消去
2. 個人主導のDRM (digital rights management)
   - 自分のデータ提供条件を厳格に適用
     * 個票データを人間が見ない、平文でファイルに書き出したり外部に送信したりしない、など

   ① 暗号化
     * 暗号化されたデータの鍵をデータ共有相手の公開鍵で暗号化して渡す

   ② データにアクセスするアプリの限定

   現状: PLRアプリが少ない

   予定: 暗号化されたデータとその鍵にアクセスするハードウェアとソフトウェアを認証

サービスの間のデータ連携

- サービス自動化の前提
- サービス(センサ)の出力データを他のサービスで活用
- データの仕様の標準は利用者主導で普及

データ管理の責任分界

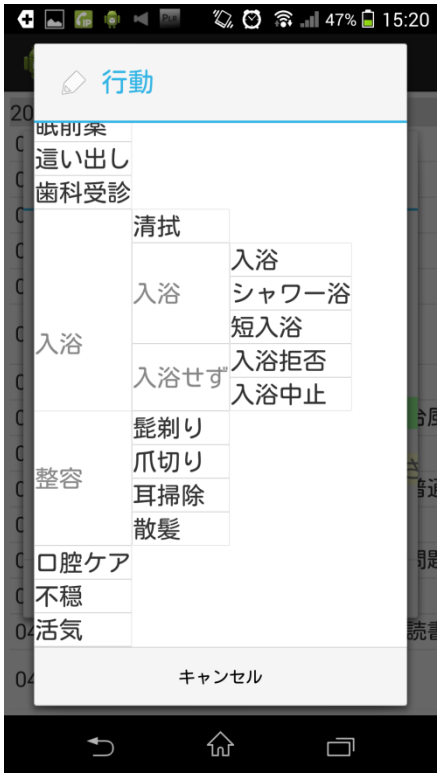
- 個人は本人のデータを自らの権限と責任で管理
  - 他の個人や事業者とのデータ共有を自由に設定・解除
  - PLRによってデータを自ら作成・利用
- 事業者は個人が管理するデータに責任を負わない
  - 顧客の連絡先や契約書やその他法律等で定められたデータだけを保管すれば良いので低コストかつ低リスク
- パーソナルデータに関する法令等を満たす
  - 個人情報保護法、医療情報システムの安全管理に関するガイドライン(厚労省)、EUのデータ保護規令則など

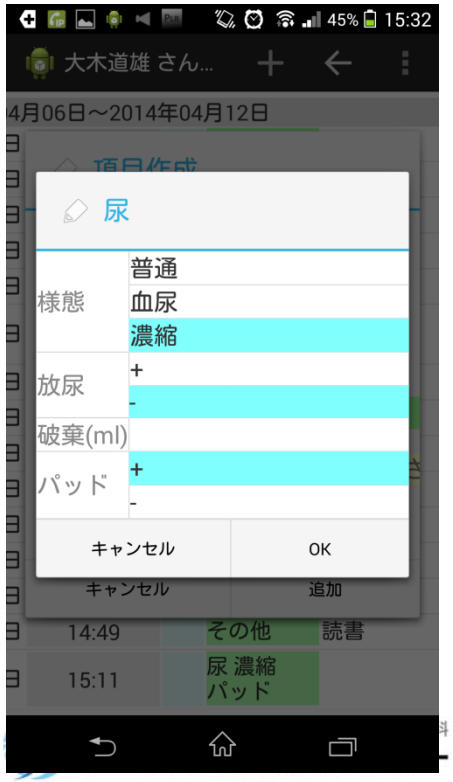
PLRによるパーソナルデータの利活用

- 自律分散協調エネルギー管理
  - 太陽光発電システム等の保守
  - スマートグリッド … 配電系統の安定化
- 自律分散協調ヘルスケア
  - 医療・健康データの自己管理
  - 医療機関や介護施設が個人を介してデータ連携
- 自律分散協調学習
  - 学習者の興味や進度に応じたアドバイスと協調学習
- 自律分散協調資産管理
  - 金融資産や不動産の管理・相続等
  - データに基づく住宅・建物保守
- 自律分散協調マーケティング
  - 購買等のデータを顧客が蓄積・管理 → 収集・分析
  - 事業者が売り方を最適化(CRM)
  - 顧客が買い方を最適化(VRM)

PLR介護記録アプリ

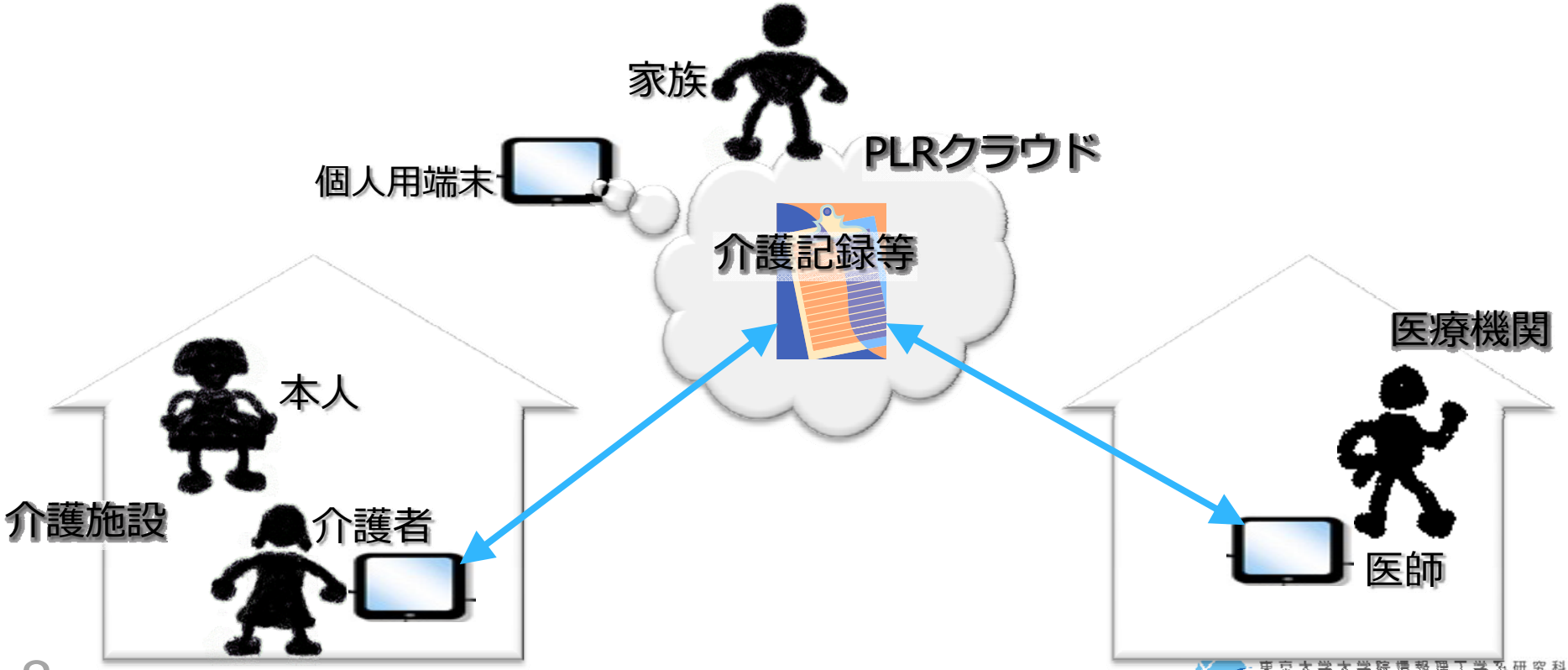
- 恵信福祉会(山梨県の介護事業者)で被介護者70名以上を対象に運用中
- 他の介護施設や病院にも展開する予定
- オントロジー(データのスキーマ)の変更が容易
  - 訪問医療や訪問看護用のカスタマイズ
  - がん連携手帳やお薬手帳の実装
  - 電子カルテシステムの簡易版も





パーソナルデータの本人(代理人)管理

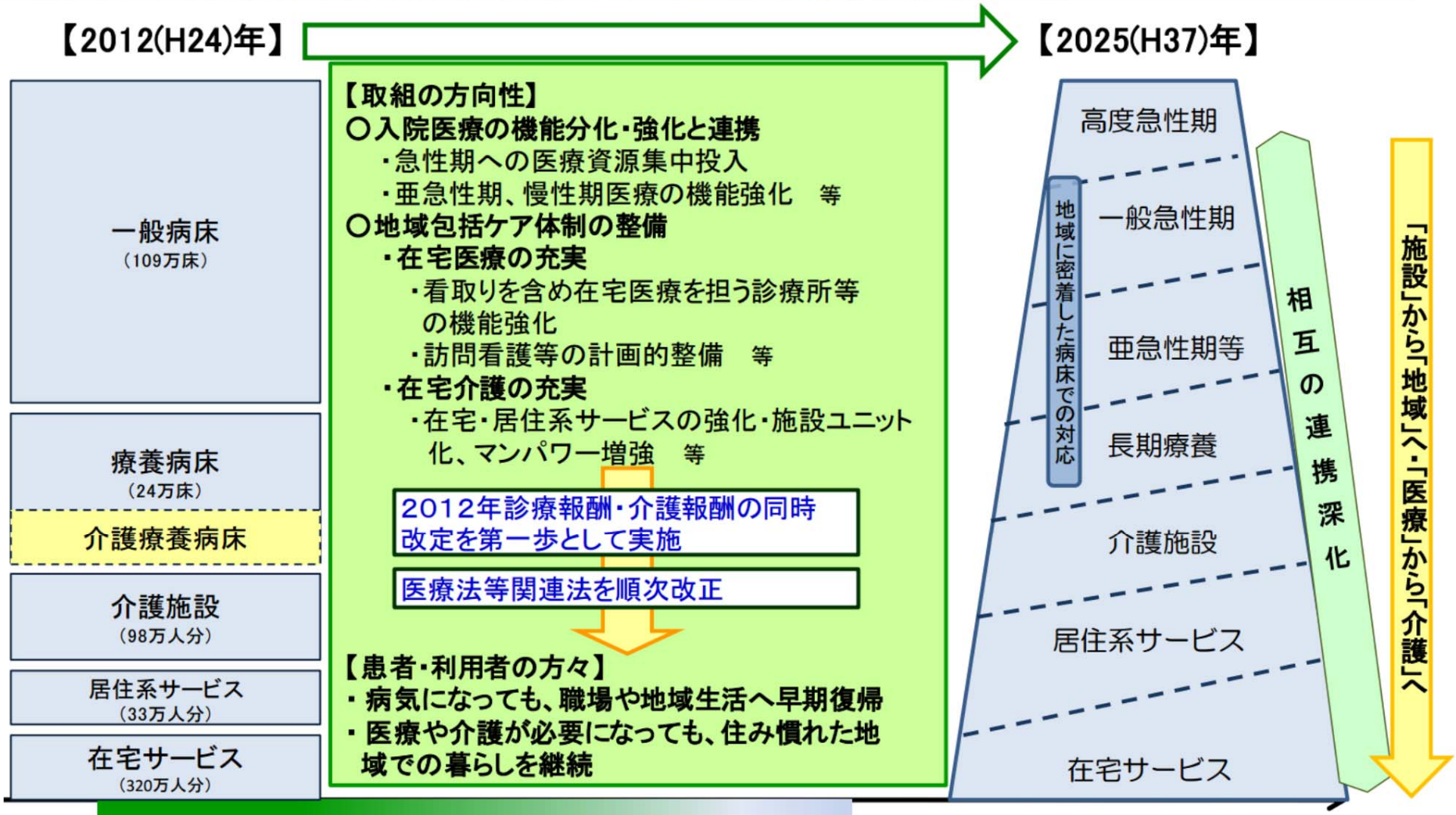
- 介護記録のデータを本人(の家族)が管理して複数の事業者等と共有
- 恵信福祉会で2015年8月14日から運用中



医療制度改革

医療・介護機能の再編（将来像）

患者ニーズに応じた病院・病床機能の役割分担や、医療機関間、医療と介護の間の連携強化を通じて、より効果的・効率的な医療・介護サービス提供体制を構築します。



医療・介護の基盤整備・再編のための集中的・計画的な投資

医療制度改革(続)

- 医療機関等の間でのデータ共有が必須に
  - before: データを共有しても儲からない。
  - after: データを共有しないと経営が成り立たない。
- 病院(病床)の機能分類を2018年から運用
  - 高度急性期、急性期、回復期、療養期、診療所
- 異種病院間のデータ共有
  - 急性期病院は、退院患者の再入院を防ぐため、受入先の回復期病院や診療所に患者のデータを渡さねばならない。
  - 回復期病院や診療所は、急性期病院等からの退院患者を多く受け入れるため、患者のデータを受け取って治療の成績を高める必要がある。
- 診療所同士のデータ共有
  - 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せねばならない。

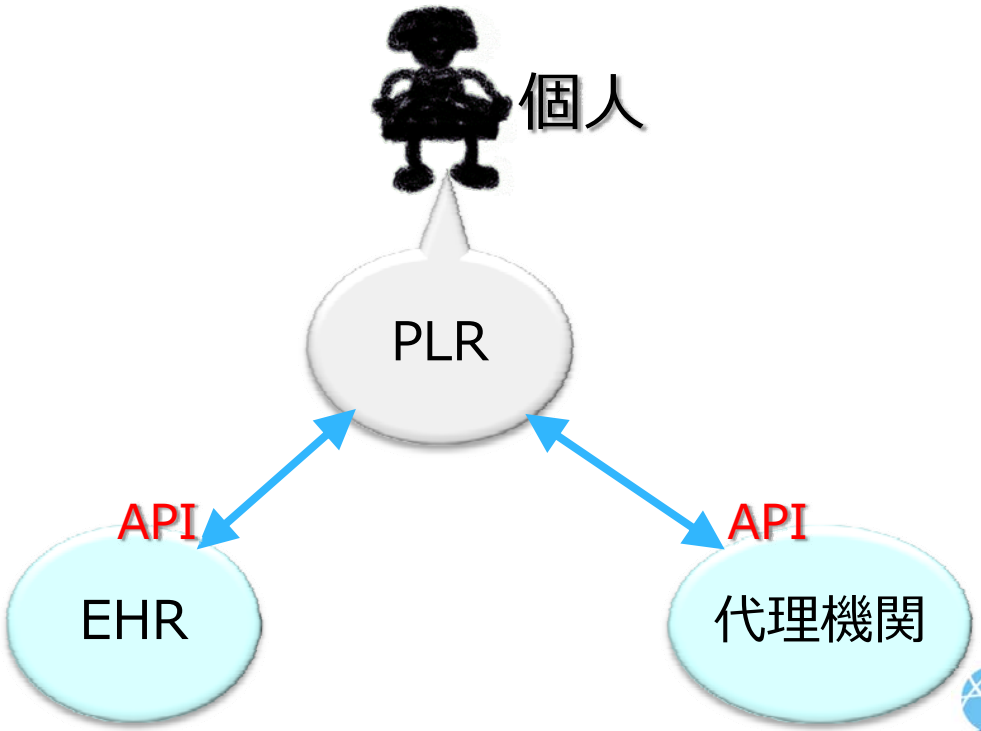
データ共有の方法	集中(EHRなど)	分散(PLRなど)
内容	事業者が多数の個人のデータを集中管理	個人のデータを本人(代理人)が管理
費用	集中管理システムなので高価	既存の安価な端末やストレージを用いるので安価
拡張性	集中管理システム同士の直接連携は一般には不可能	集中管理システム同士の連携を仲介
普及可能性	対象地域の人口の2%未満	100%

自律分散協調ヘルスケア

- 地域包括ケアや地域医療連携を実現するために、
- 事業者同士が直接データ共有するのは無理な場合が多いので、
- 現実的には、個人(患者や被介護者や家族)が中心になって多数のヘルスケア関連事業者を連携させる(下図)しかない。

メタ連携

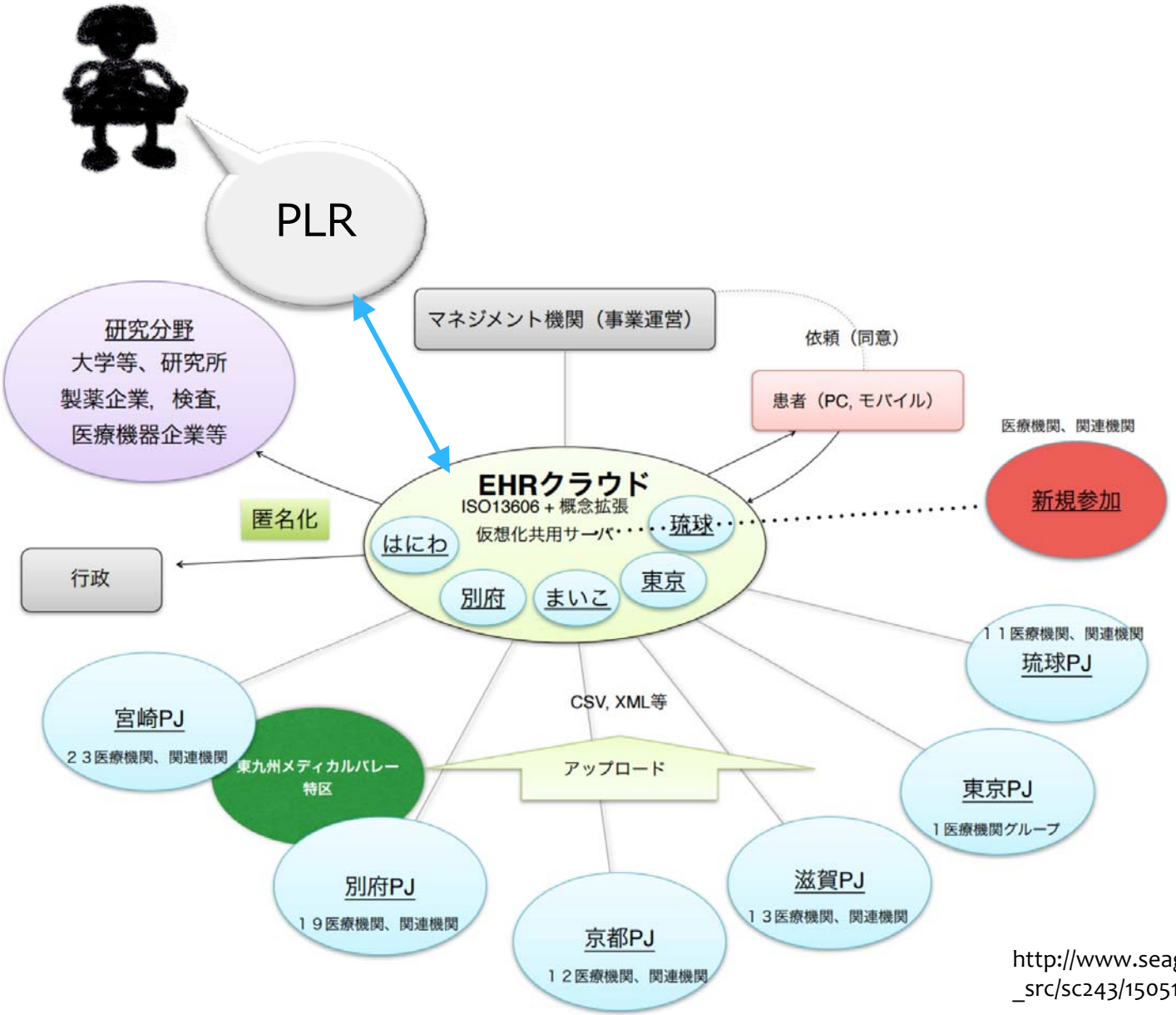
- 集中PDS(EHRや医療介護SNSや代理機関)同士の直接的連携は困難
  - 技術的に高コスト、事業者同士の競合など
  - 例: 京都のまいこネットとポケットカルテ
- 集中PDS(事業者)と分散PDS(個人)との連携は容易
  - ⇒ 集中PDS同士の間接的連携
  - ⇒ 自己情報コントロールに基づくパーソナルデータの流通



自律分散協調ヘルスケアプロジェクト

- 宮崎
  - はにわネットのPLRによる拡張
  - 他のサービスへの展開 … 大学の同窓会など
- 山梨
  - 恵信グループ(社会福祉法人恵信福祉会・ 医療法人恵信会)の介護施設にPLR介護記録アプリを導入済
    - 2015年8月からデータの本人(家族)管理を運用
  - さらに同グループ内の療養型病院や地域の他のヘルスケア事業者をPLRで結ぶ
- 愛知
  - 藤田保健衛生大学・名古屋大学等との共同研究
  - まずは医療法人陽明会の診療所と介護施設をPLRで結ぶ
- 米子、東京、湯河原、春日井、他

千年カルテプロジェクトとの連携



http://www.seagaia.org/~sg2015/_src/sc243/150516yoshihara.pdf

ITベンダと医療ビッグデータ

- 医療ビッグデータ事業の構築が必須。
  - 電子カルテシステムやEHRの事業が大きく成長することはあり得ない。
- だが、医療データは医療機関が管理しており、ITベンダはアクセスできない。
- 医療データを個人に渡せば、ITベンダも個人から直接データを取得できる。
  - 電子カルやEHRの事業もそのまま継続可能。
  - 医療機関も他の医療機関に由来するデータを個人から取得できる。

VRM: 業者関係管理

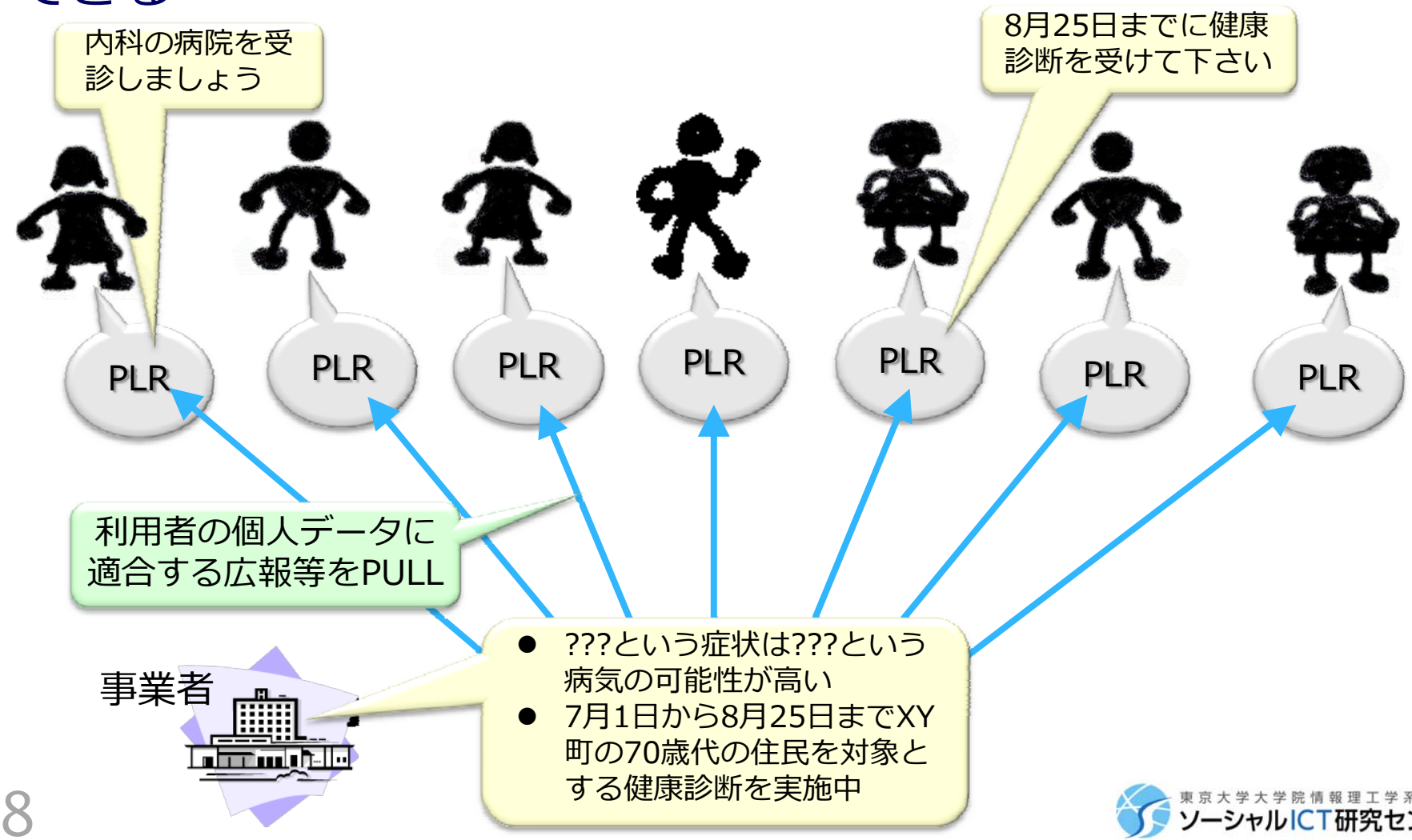
Vender Relationship Management

- CRM (顧客関係管理; customer relationship management)の逆
- 顧客が自らの意思とデータに基づいて業者からのサービスや商品の買い方を最適化
  - 顧客のソフトウェアエージェントが当人のデータに適合するサービスや商品を選択
- 広告や推薦よりはるかに高精度で安価
- Berkman Center for Internet and Society, Harvard Univ.の研究プロジェクト

27

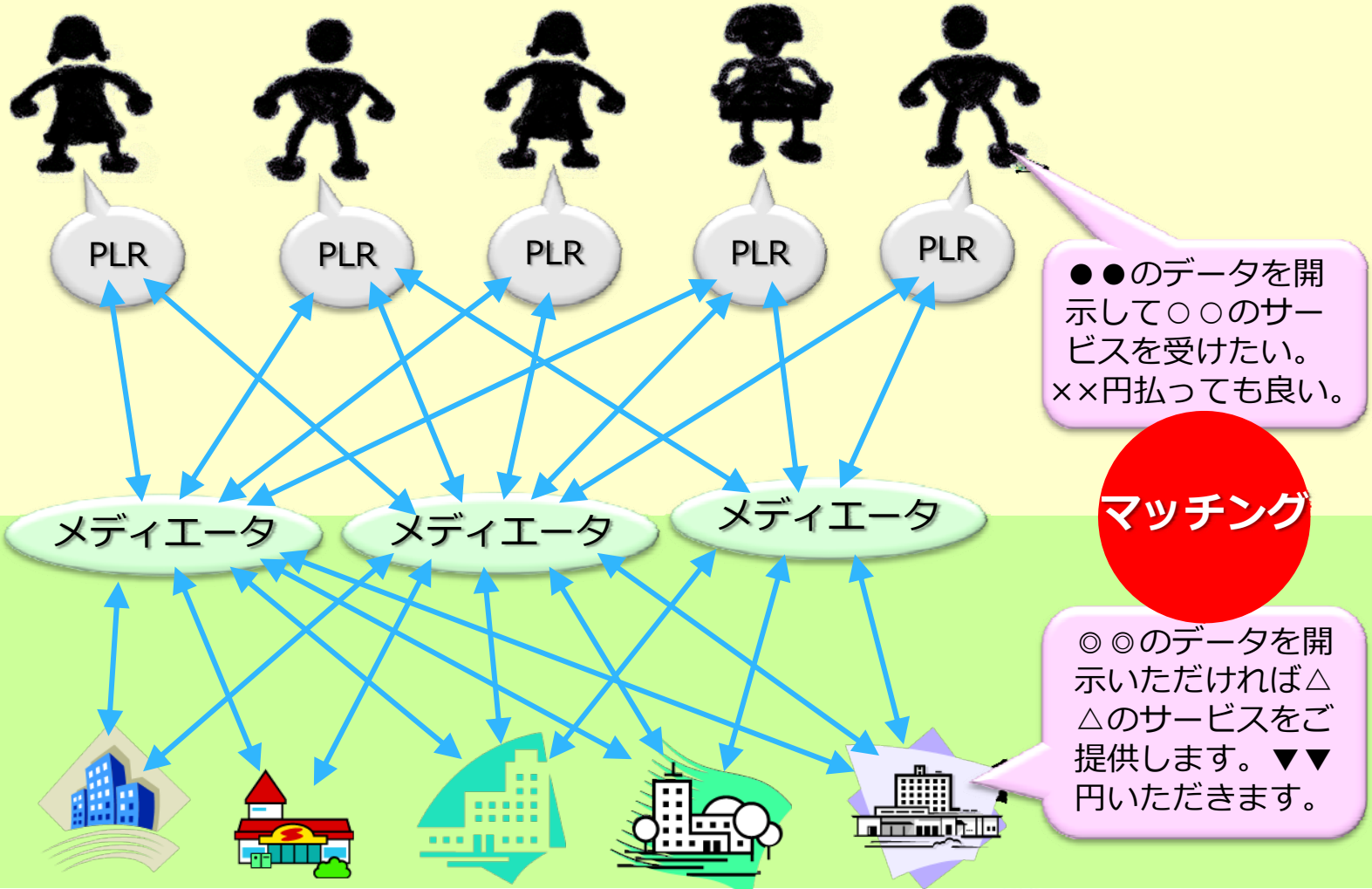
VRMの基本形

- 利用者の個人データに適合する広報等を分散PDSがPULL
- 事業者は個人情報を見ずに行動ターゲティング以上のことができる



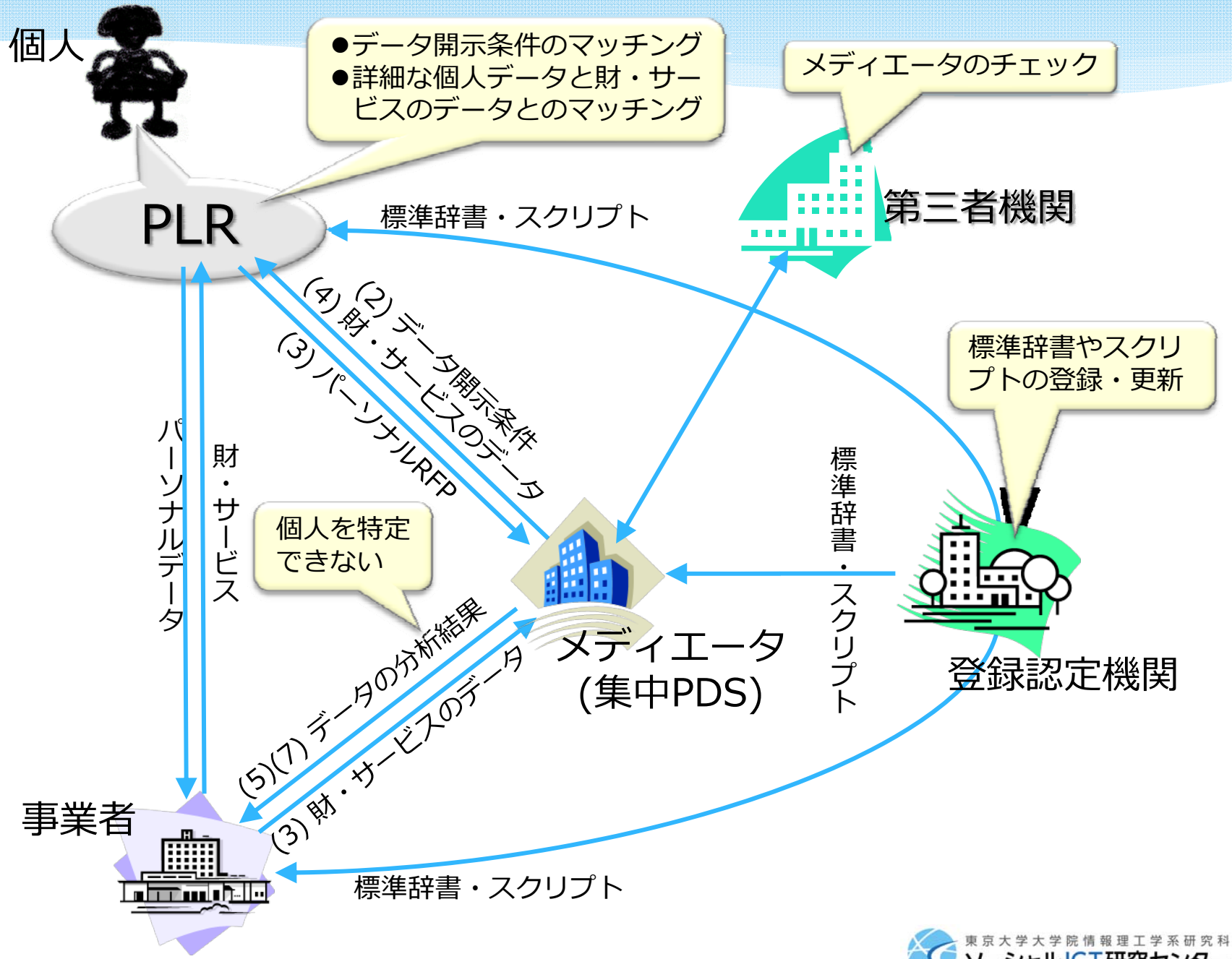
メディエータ(個人と事業者との仲介)

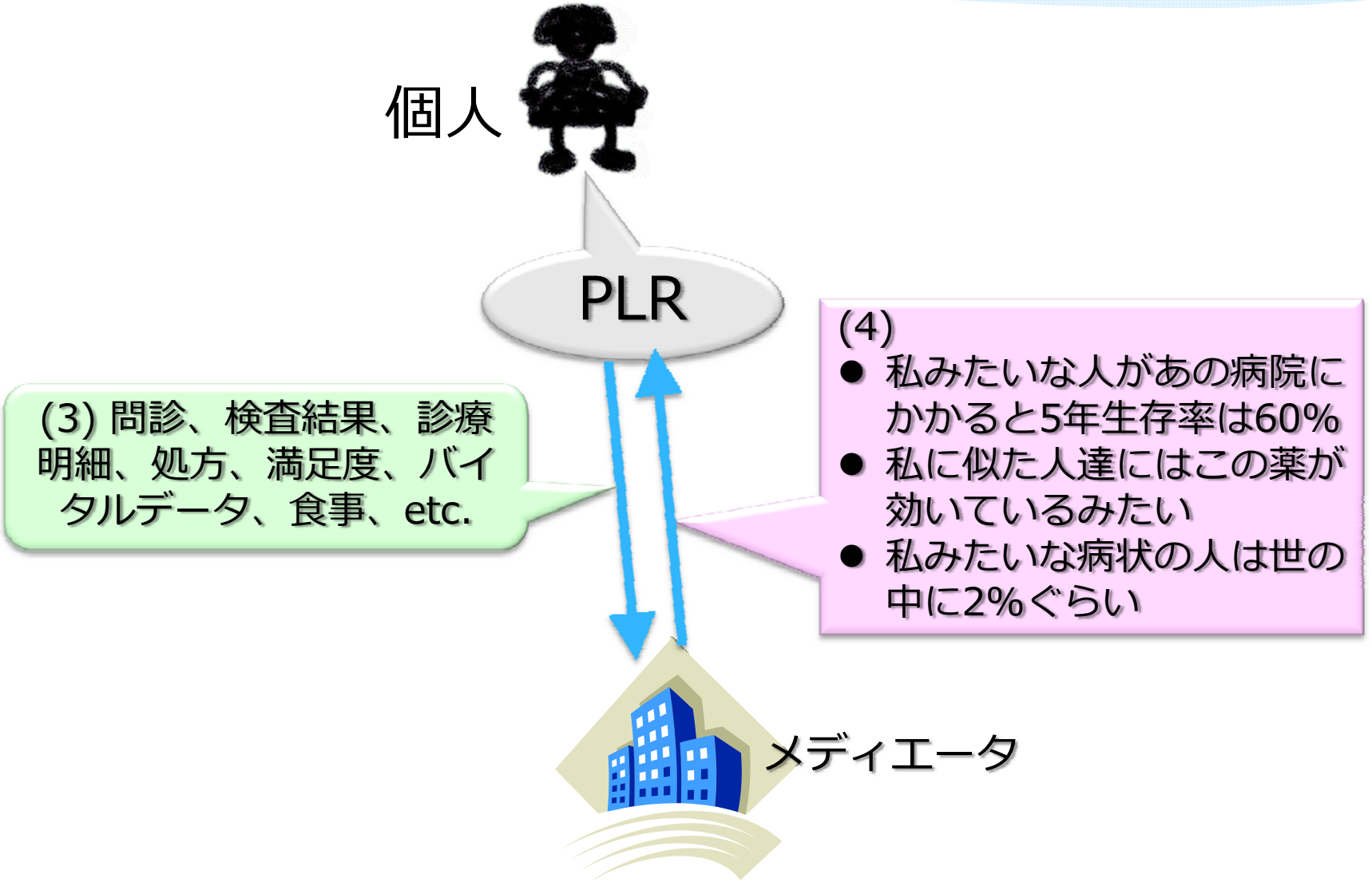
- 双方の取引条件を構造化することでマッチングを自動化(人工知能)
- マッチングの結果を個人に開示
- 市場のニーズ等を事業者に開示



メディエータ(一般化)

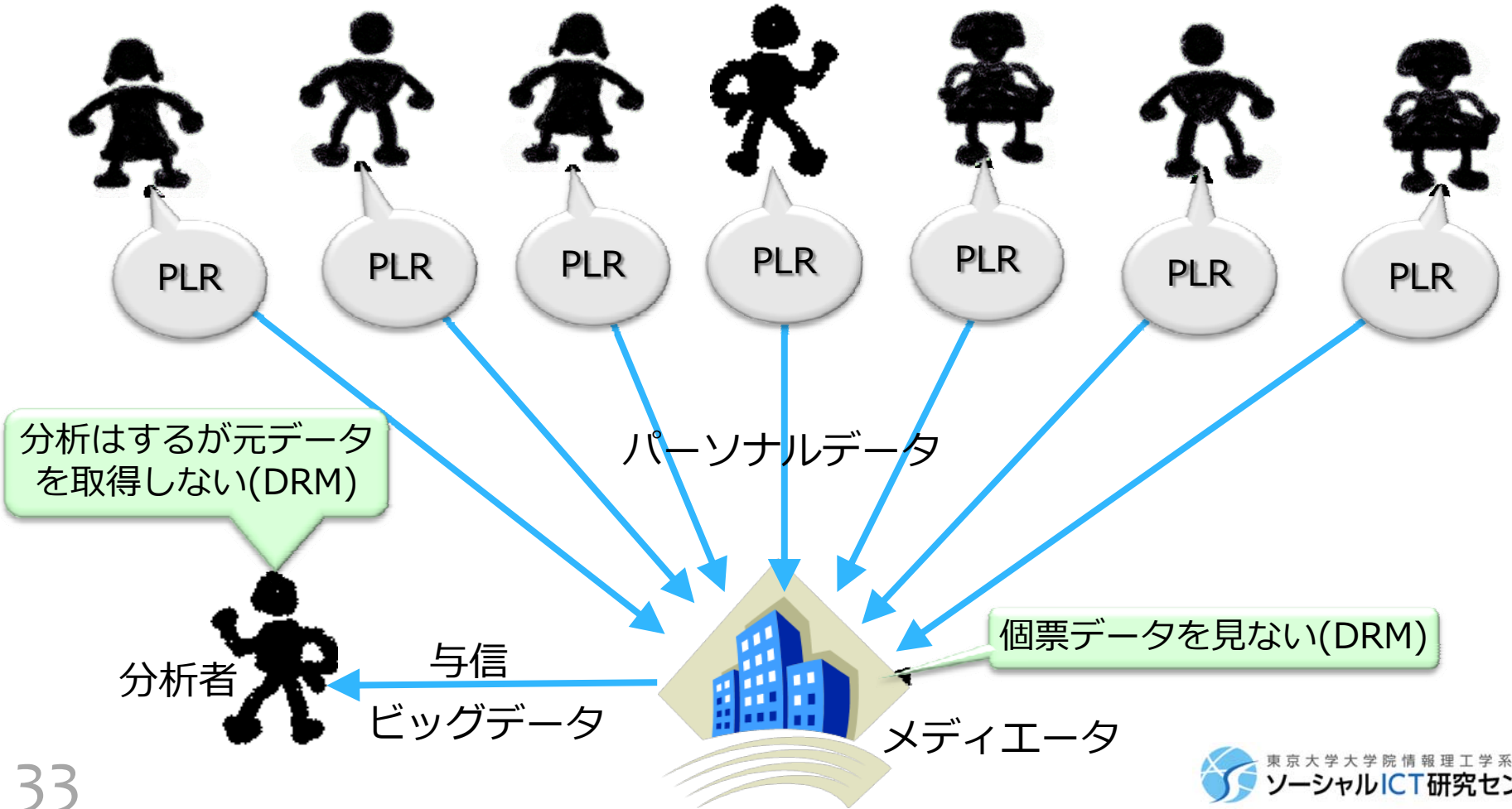
- 多数の主体(個人と事業者)からデータを集めて共通する処理を代行
  - マッチング(前頁)
  - 分析(前頁)
  - 検索…分析結果と個票との照合も
  - ブローカ…匿名化して第三者提供
- 集中PDS?
  - 個人の自己情報コントロールを担保
  - EHR、従来のPHR、情報銀行、代理機関、他

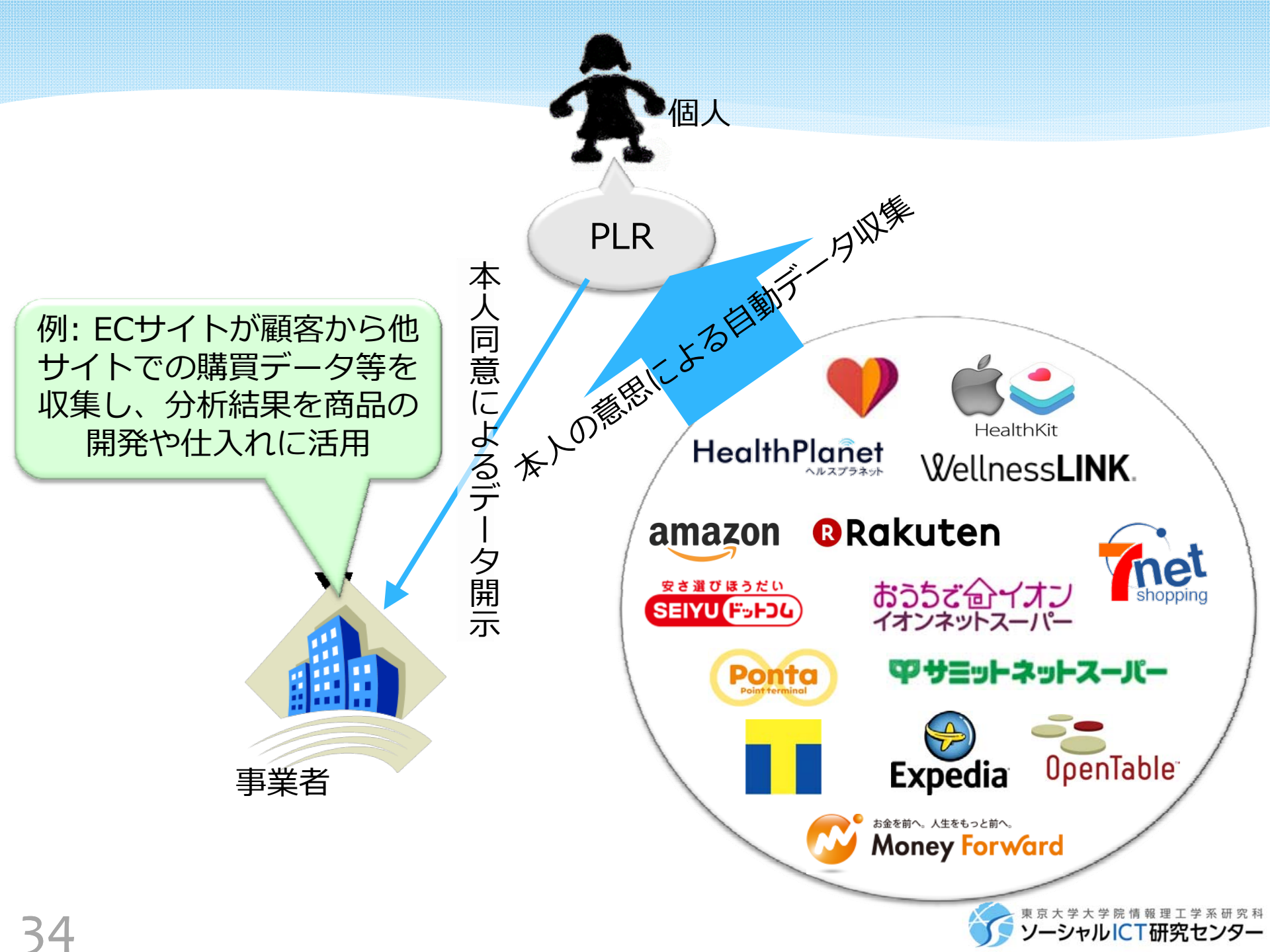

個人
●データ開示条件のマッチング
●詳細な個人データと財・サービスのデータとのマッチング
メディエータのチェック
PLR
標準辞書・スクリプト
第三者機関
(4) 財・サービスのデータ
(2) データ開示条件
(3) パーソナルRFP
パーソナルデータ
財・サービス
標準辞書やスクリプトの登録・更新
個人を特定できない
標準辞書・スクリプト
メディエータ
(集中PDS)
登録認定機関
(5)(7) データの分析結果
(3) 財・サービスのデータ
事業者
標準辞書・スクリプト


個人
PLR
(3) 問診、検査結果、診療明細、処方、満足度、バイタルデータ、食事、etc.
(4)
● 私みたいな人があの病院にかかると5年生存率は60%
● 私に似た人達にはこの薬が効いているみたい
● 私みたいな病状の人は世の中に2%ぐらい
メディエータ

ビッグパーソナルデータ

- データ提供の手続きがオンラインで簡単に
- 本人の条件を遵守しつつデータが流通
  → 安心してデータを提供




個人
PLR
本人同意によるデータ開示
本人の意思による自動データ収集
例: ECサイトが顧客から他サイトでの購買データ等を収集し、分析結果を商品の開発や仕入れに活用
事業者
HealthPlanet
ヘルスプラネット
HealthKit
WellnessLINK
amazon
Rakuten
7net shopping
安さ選びほうだい
SEIYU ドットコム
おうちでイオン
イオンネットスーパー
Ponta
Point terminal
サミットネットスーパー
Expedia
OpenTable
お金を前へ。人生をもっと前へ。
Money Forward

ビジネスモデル

- ヘルスケア
  - 介護アプリは低価格ゆえに代理店による拡販が困難なので、付加サービスによる単価の向上が望ましい
  - 分散PDSに基づく診療所用電子カルテは、医療制度改革に伴うデータ共有へのニーズが顕在化すれば拡販可能?
  - 患者や家族へのデータの還元には保険を適用?
- 他の産業領域
  - 事業者間で購買データ等を直接共有するのは困難
  - 消費者に購買データ等を電子的に提供するのもコストがかかる
  - 個人のエンパワメント
    - 個人が保有するデータの活用

地域包括ケア付加サービス?

- 複数のカメラの映像を一覧(下図)
- カメラ等のセンサデータから検出されたイベントの通知
  - 宅内での人やペットの動き、来訪者など
- 宅内の家族や来訪者と宅外から映像通話
- センサデータ(ライブまたは録画の映像など)への一時的なアクセス権限を他のPLR利用者に安全に付与
  - 家族、近隣住民、警察、自治体など

名簿(1)

友人		
阿部 正	090-8722-4473	abe0925@foo.ne.jp
井上 浩子	070-4327-3276	inoueh@ab-c.co.jp
加藤 和美	03-3471-8759	
佐々 ウメ	080-8922-3216	h.sasaki@t.u-tokyo.ac.jp
鈴木 典子	050-5482-3981	noriko-s@puppy.org
田中 光	047-651-4489	h347891@sloppy.com
中村 綾	0898-49-3276	yuichi@jcss.gr.jp
開示		
自宅住所、自宅電話番号、メールアドレス		

PLR利用者なので本人が情報を管理

PLR利用者ではないので私が情報を管理

自分がグループメンバーに開示している情報

名簿(2)

地域包括ケア			
新浦CLINIC	新浦安クリニック	047-211-4411	gp@shinurayasuclinic.co.jp
YVC	山田訪問介護	043-412-1237	info@yamadacare.com
	浦安病院	047-311-4862	rec@urayasuh.co.jp
開示			
医療記録、介護記録、投薬記録、生活行動記録、宅内カメラ			

追記可能な開示は別途

制度に関する課題(1)

- 運用ルールの策定と実効性の担保
  - 運用ルール
    - 事業者が取得したデータの消去に関わる時期や条件
    - 事業者間でのデータ共有の制限
    - メディエータが事業者に提供しうる情報の範囲
  - トラストフレームワーク
    - 同意取得手続の標準化
    - ルールの実効性を担保する手段
      - 個人主導DRMなど
  - 個人情報保護委員会等の関与?
- 同意取得のあり方と事業者間共有
  - 分散PDSは本人同意に基づいてパーソナルデータを活用
    - 機微性の高いデータの流通も容易
  - 個人のデータはすべて本人が管理しているので第三者提供が不要
    - DRMを使えば第三者提供も可?
    - 匿名加工情報等の事業者間共有?

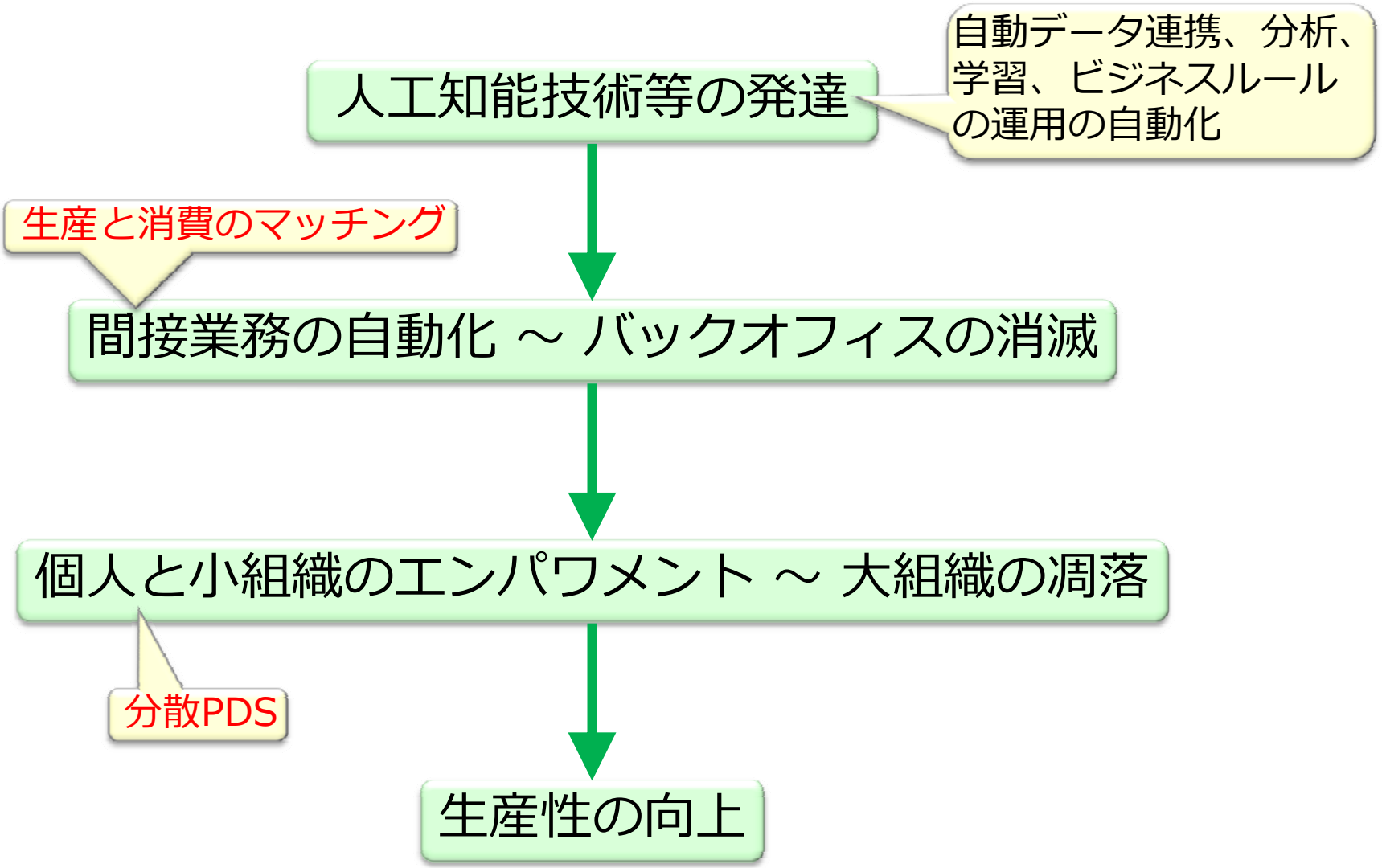
制度に関する課題(2)

- 個人の認知限界の緩和
  - 分散PDSにおけるデータの管理 ＝ 使用許可の判断
  - 個人の認知限界
    - 事業者からのデータ提供要請が頻繁
    - 使用条件の記述が複雑
  - わかりやすい標準的インタフェースと手続
  - メディエータが顧客の意思決定を支援
    - 個人と事業者とのマッチング等
    - 実質的な本人意思に基づくデータ流通
      - 明示的な本人同意なしで本人の意思に基づくデータ活用
    - データ管理の委託・信託の可能性
- 顧客へのデータ還元に関わる制度枠組
  - 分散PDSの普及には、個人が自分のデータを電子的に活用可能な形で保有することが必要
  - スマートディスクロージャ：機械判読可能な標準形式でのデータ還元
    - 英国のmidata、EUのデータ保護規則など
    - エネルギーやヘルスケアなど公共性の高い分野から?

個人と事業者とのデータ共有の動向

- 個人に由来するデータを本人が蓄積して自ら利用するようになる。
  - ウェアラブルセンサ、IoT、人工知能の普及等により、個人のエンパワメントが進む。
- 事業者は個人からそのデータを取得したい。
- それには、個人のエンパワメントを促進して個人由来のデータの質と量を向上させ、さらにそのような個人と信頼関係を築く必要がある。
- 信頼関係の構築にはデータの一方的な取得ではなく共有が必須。

展望


人工知能技術等の発達
自動データ連携、分析、学習、ビジネスルールの運用の自動化
生産と消費のマッチング
間接業務の自動化 ～ バックオフィスの消滅
個人と小組織のエンパワメント ～ 大組織の凋落
分散PDS
生産性の向上

おわりに

- 分散PDSは自己情報コントロールに基づくパーソナルデータの流通を促進する。
- 分散PDSの普及につれて、多数主体(個人と事業者)のデータの処理(検索、分析、マッチング)を担うメディエータ(集中PDS)が必要になる。
  - 集中PDS同士を連携させるために分散PDSが必要
- 分散・集中PDSの処理を自動化する人工知能技術により社会全体の生産性が高まる。
  - 人工知能にはPDSによるデータの流通が必要