個人データの集中管理と分散管理

2014-04-24 橋田浩一

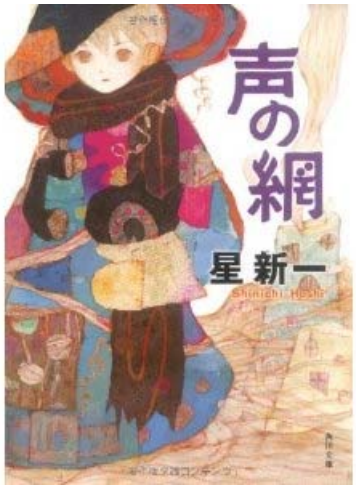
東京大学大学院情報理工学系研究科
ソーシャルICT研究センター

B2Cサービスと個人データ

- B2Cサービスは第一義的に個人に価値を提供する
  - その価値に関する競争がイノベーションの主因
  - 事業者は競争に勝つことで第二義的受益者となる
- データ共有の第一の受益者も個人
- 個人が本人のデータの主たる管理者としてデータを自由に共有し活用可能にすることが、B2Cサービスの価値向上において重要
  - 他者が個人データの主な管理者だと、データの共有・活用による価値創造が起こりにくい
- その前提で最適なサービスを構築することが必要
  - 破綻した制度に依存しない持続可能な収益事業

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?
  - Alan Mitchell (2001) Right Side Up: Building Brands in the Age of the Organized Consumer. Harper Collins Business.

集中型PDS	分散型PDS
事業者が多数の個人のデータを集中管理 ● 個別のデータ利用に本人の許可が不要	個別のデータ利用を本人(または家族等)が許可
あらゆる種類のデータを相互連携可能にするには全データの集中管理が必要だが、それは明らかに不可能	個人の判断であらゆる種類のデータを相互運用 ● 複数の集中型PDS等を統合
EHR、従来のPHR、情報銀行等	PLR (東大・アセンブローグ)、OpenPDS (MIT)

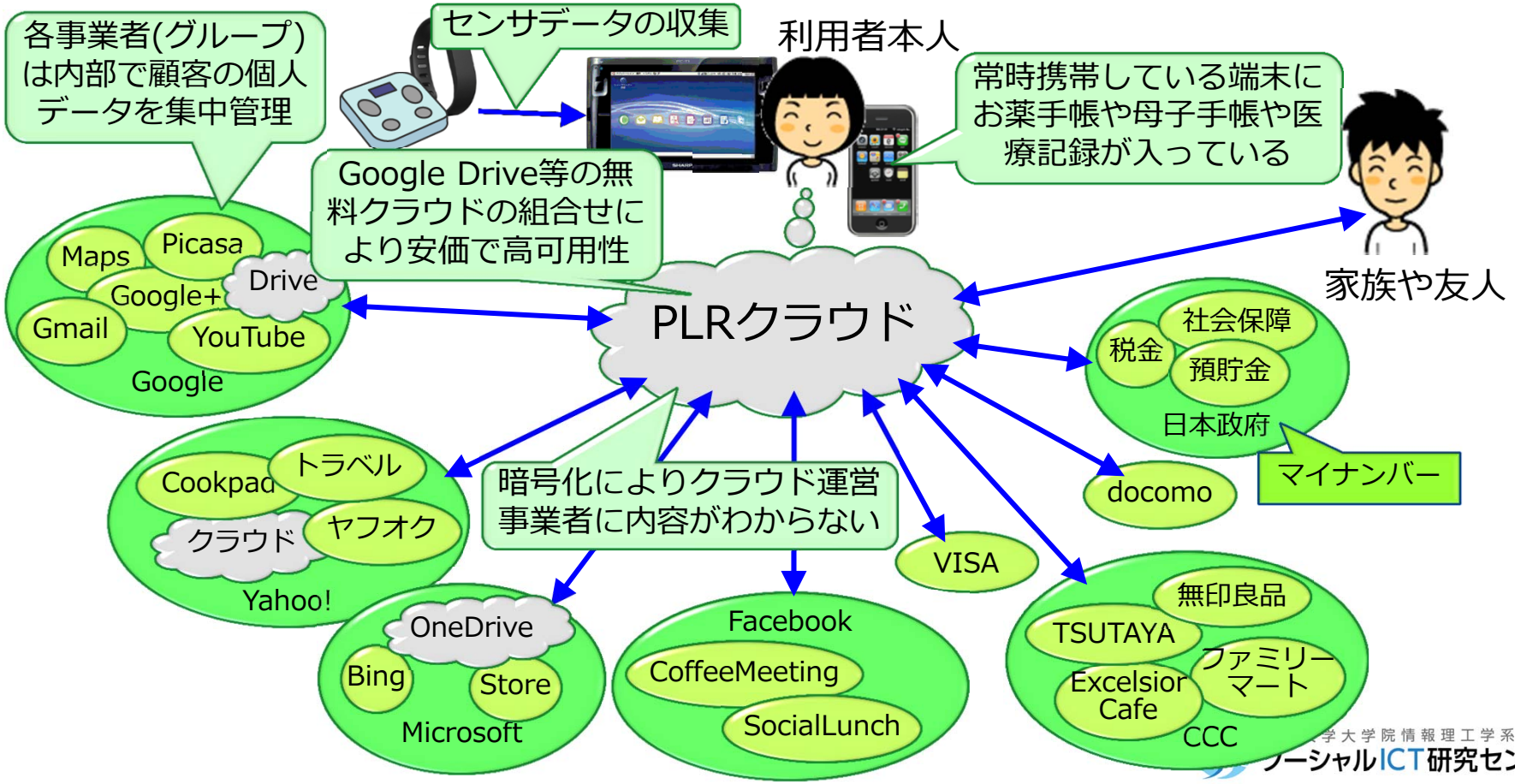
個人データ管理における安全性と利便性

- 安全性 ＝ 本人に不利益なデータ利用の防止
  - A. 管理者(利用を許可する者; 複数可)の厳格な認証
  - B. 本人(または本人の利益に即して判断する代理人)を管理者に含める … Cを含意
  - C. 1回に漏洩するデータを少なくする(分散管理)
  - ◆集中管理(Aのみ) « 個人ごとの分散管理(A+B+C)
- 利便性 ＝ 有益なデータ利用の促進
  - ◆個益 ＝ 本人に有益
  - ◆公益 ＝ 多くの人々に有益

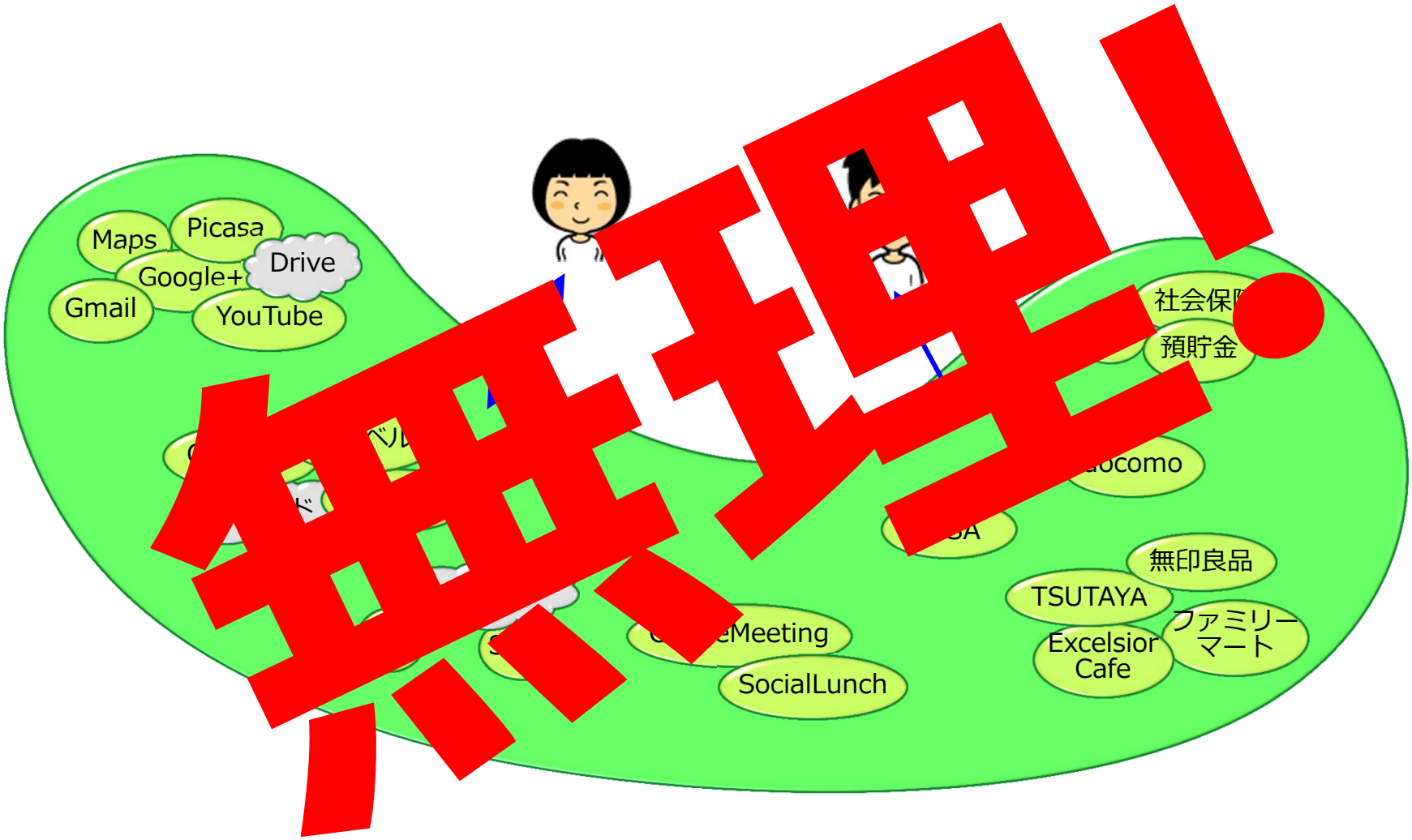
本人が毎回直接許可するのは煩雑なので、利用の条件をソフトウェアエージェントが理解できるようにしてマッチングを半自動化するのが望ましい。

PLR: Personal Life Repository

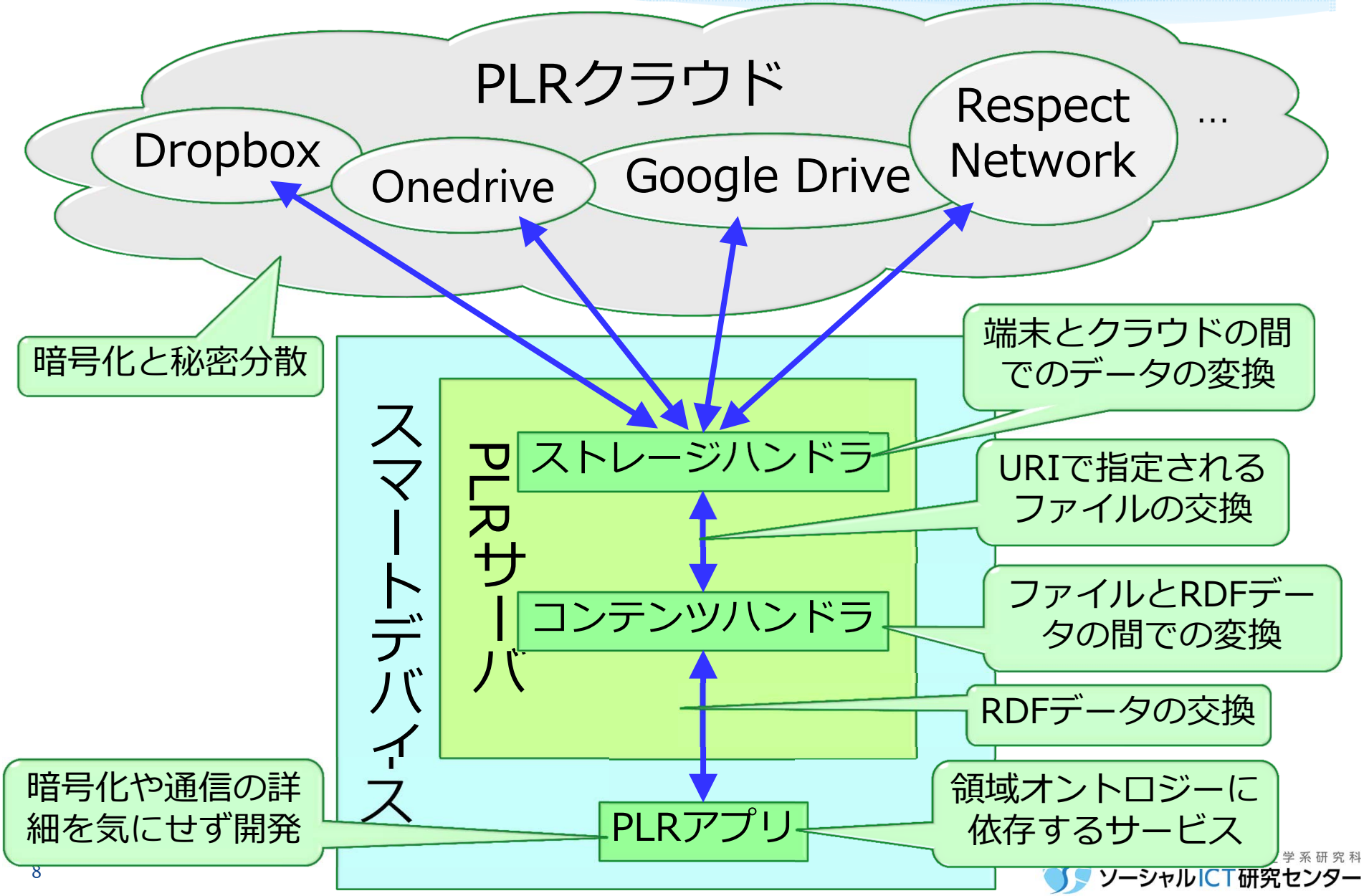
- 個人データを本人が蓄積・管理し、相手とデータの種類を自由に選んで安全に共有・活用するためのスマートフォン等のアプリ(分散PDS)
- 個人は多数のアカウント(ID)を持ち、それらをPLRで連携させる
  - 事業者が各IDの範囲で個人データを名寄せして集中管理
  - すべてのIDを事業者側で相互連携させるのは不可能



全個人データの集中管理による連携?



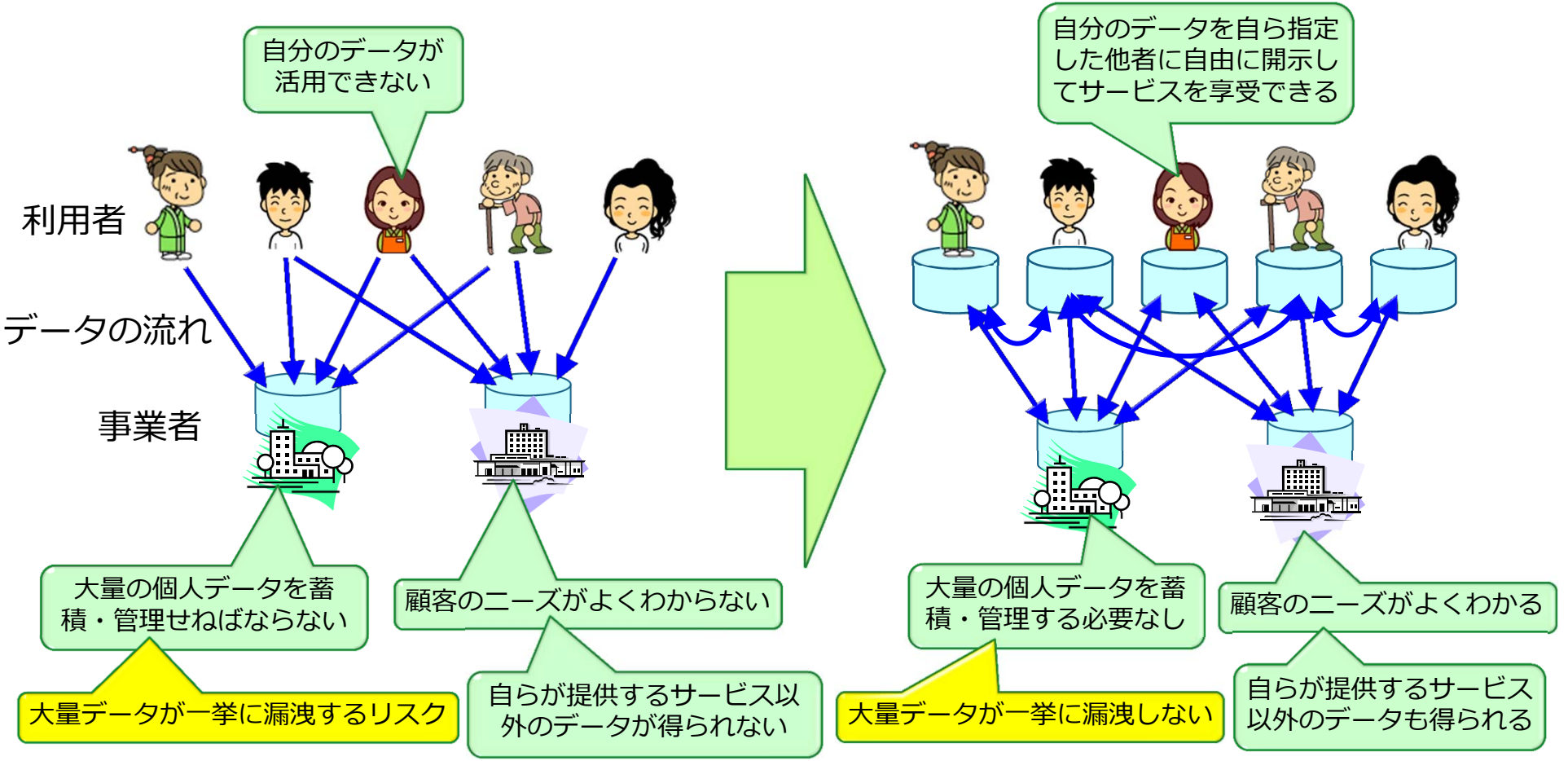
PLRクラウドの仕組み



データ管理の責任分界

- 個人は本人のデータを自らの責任において管理
  - 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
- 個人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のデータ保護指令、他

個人データの流通と活用
事業者が集中管理 → 個人が自律分散管理



- 市場の参入障壁が高い
- 既存の事業者によるロックイン

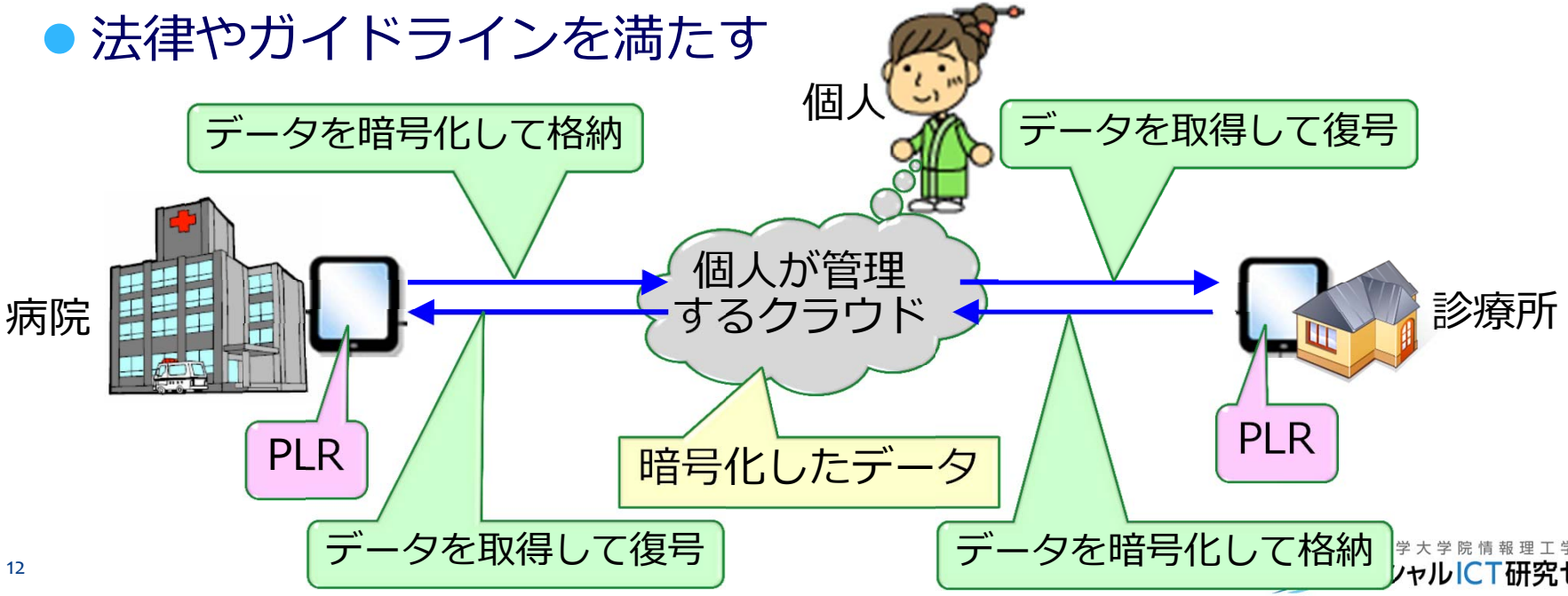
- 市場の参入障壁が低い
- サービスの質に関する自由競争

PLRによる個人データの利活用

- 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)

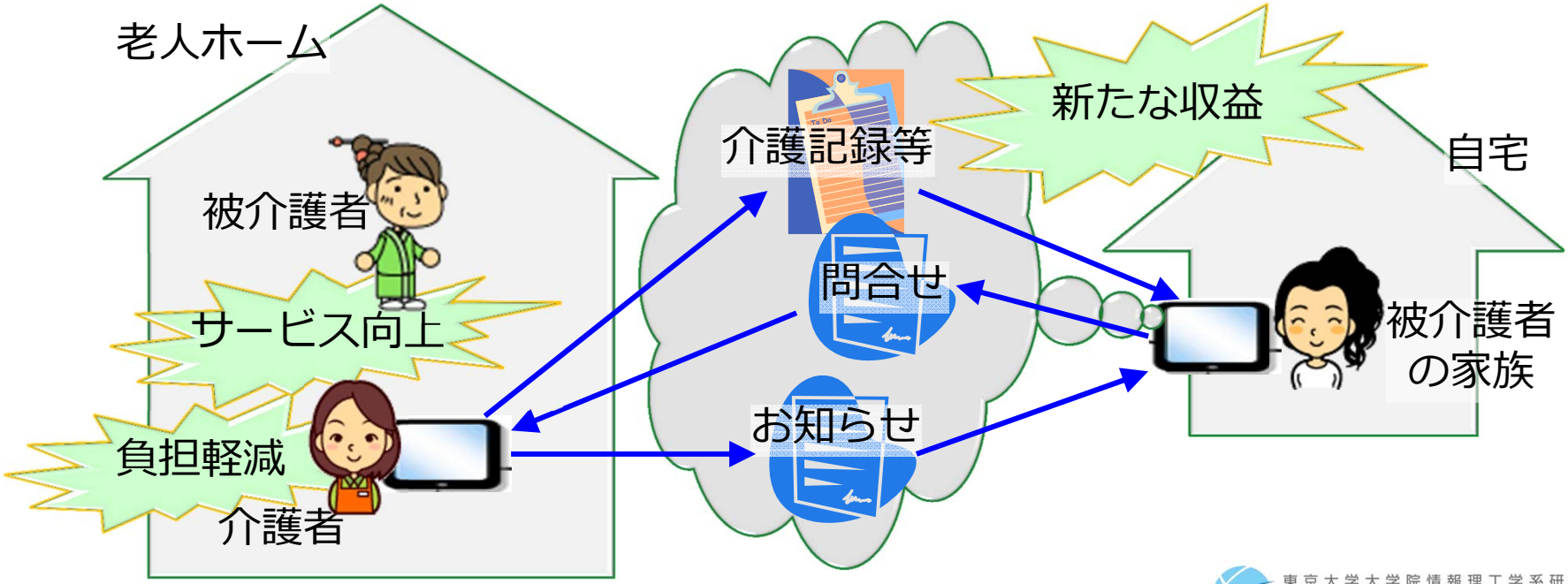
本人を介する個人データの共有

- 福島県相馬郡新地町の地域医療連携
- 個人が自分のデータをパブリッククラウドで管理
  - 相手と情報の種類を自由に選んでデータを共有
  - スマホ等は不要
  - クラウドのデータを暗号化しておけば本人からのデータ漏洩はない
- 医療機関等はデータを作成・利用するのにPLRを使う
  - データを暗号化して患者のクラウドに格納
  - 患者のクラウドからデータを取得して復号
  - 導入コストは数万円で運用コストはほぼゼロ
- 法律やガイドラインを満たす



老人ホームと入居者家族とのデータ共有

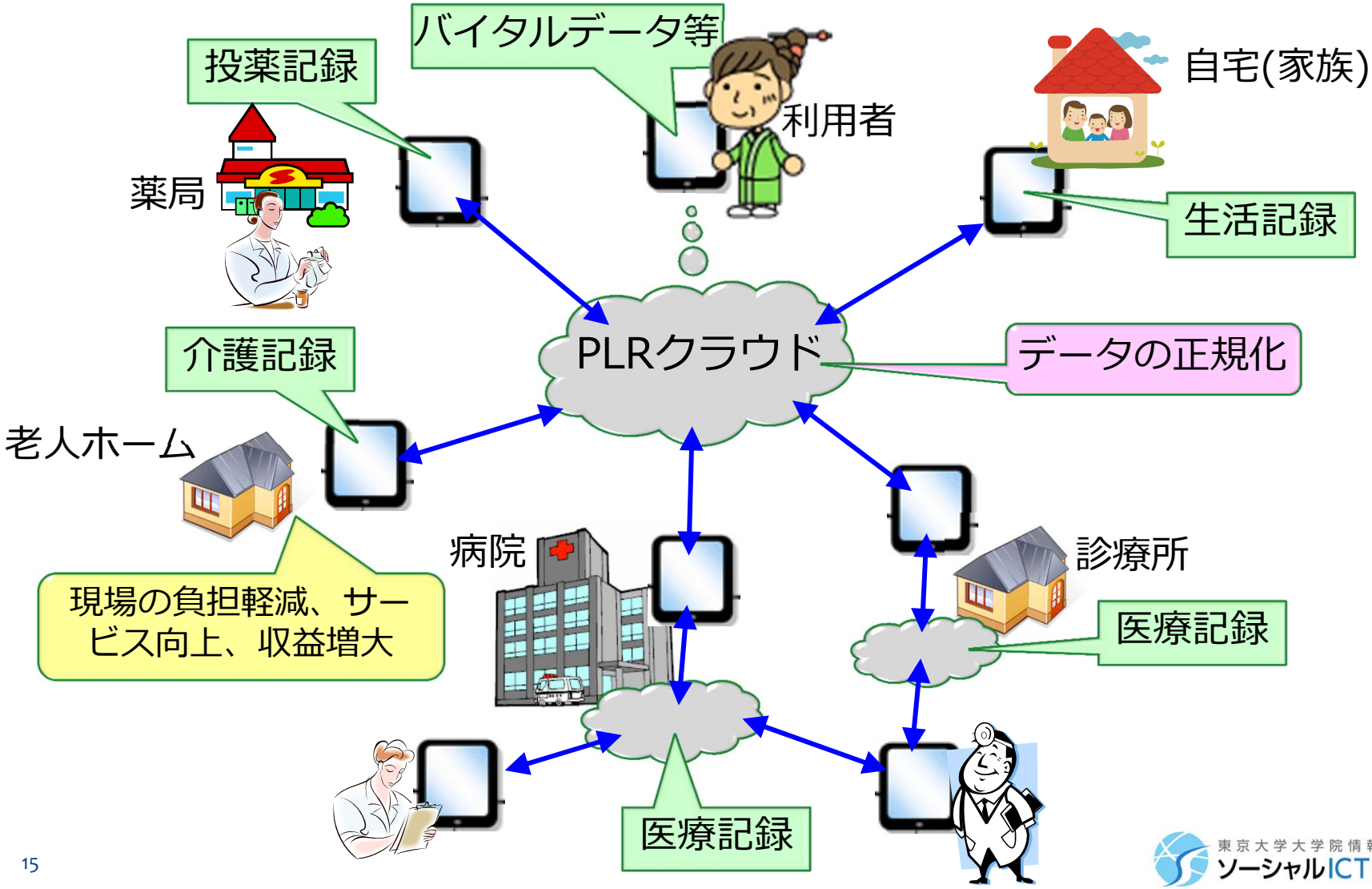
- 恵信会: 山梨県甲府市の医療・介護事業者グループ
- 被介護者の家族に対する新たな有料サービス
  - 介護記録のデータを家族が管理
    - 自宅や外出先からタブレットPCやスマートフォンで閲覧
    - 介護日誌レベルの要約も容易
  - 老人ホームと家族との通信にも活用
  - 映像等の共有や遠隔見守りも
- PLRアプリ運用費 < 新サービスの収益(5,000円/月?)




100% 13:37
山本一郎 さんの介護...
排泄確認表
2014年04月20日～2014年04月26日
04月23日 10:05 ○ 湿布 首 池本
04月23日 12:49 ◎ 便 自然 水様 少 パッド 池本
04月23日 13:16 介護者の所感 テスト 池本
04月23日 22:56 体温37.5℃ 浩一
04月23日 22:56 血圧141/65mmHg 浩一

ヘルスケアデータ連携のシナリオ(例)

老人ホーム→病院→薬局の順にPLRと連携することで全ステークホルダがデータを共有することにより全体最適化



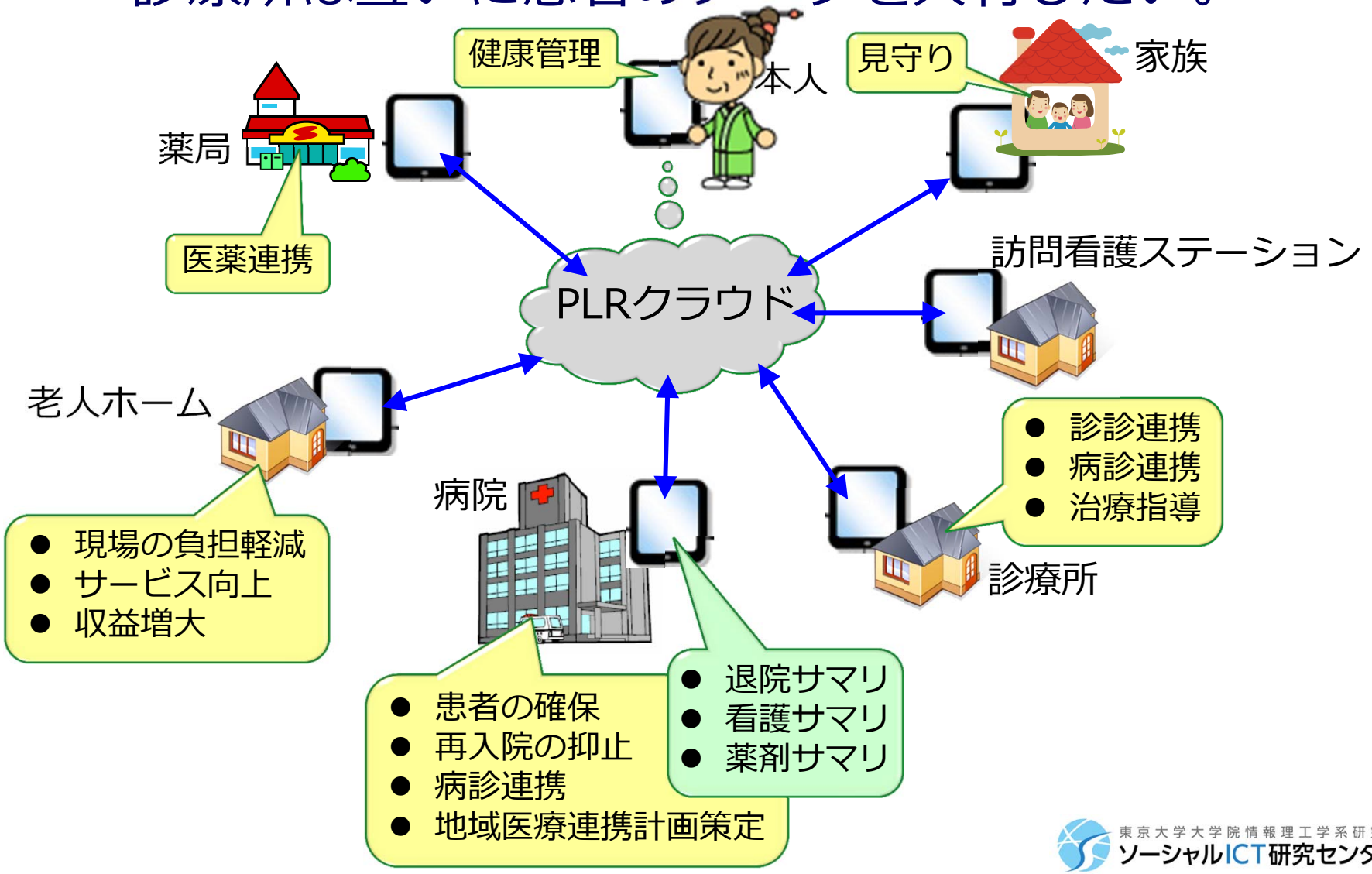
ヘルスケアデータの個人分散管理

- 今後5～10年で普及
- 医療制度改革(～2025年)
  - 異業種間でのデータ共有が必須
    - ヘルスケア事業者の間の水平分業
      - 病院を急性期、回復期、療養期等に分類
  - 診療所間のデータ共有も必須
    - 24時間365日の在宅医療対応
- 集中管理型データ共有による囲い込みは不可能
  - 分散管理の方が圧倒的に安価で便利で安全

データ共有の方法	集中型		分散型
	ID-Link	HumanBridge (SaaS型)	ＰＬＲ
導入コスト	6～180百万円	各電子カルテシステムへの接続に10百万円以上	端末購入費等 ＜ 集中型の1/10
運用コスト	2～8万円/月 ＋ サーバ運用費	10万円/月 （富士通のデータセンタ利用）	端末償却費等 ＜ 集中型の1/10
データ共有	公開機関のデータを他機関が参照	医療機関同士がデータを相互参照	患者の同意で任意の者が共有
連携サーバ	@拠点病院	@データセンタか拠点病院	パブリッククラウド
累計導入実績	2,407機関 （2013年10月）	2,000機関 （2014年末?）	3機関 (2014年前半?)

在宅医療のビジネスモデル

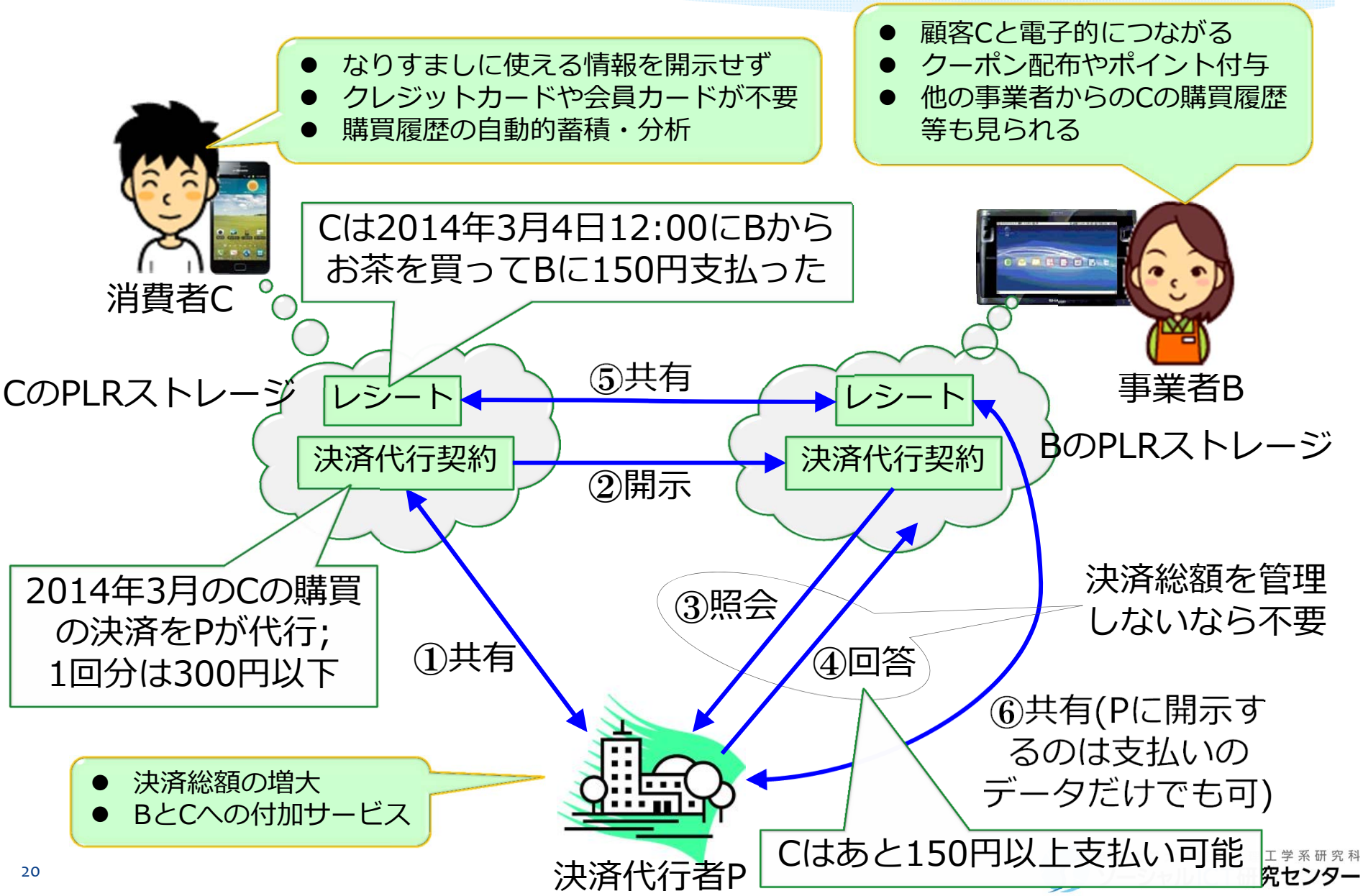
- 急性期病院は患者の手離れを良くしたい。
- 診療所は互いに患者のデータを共有したい。



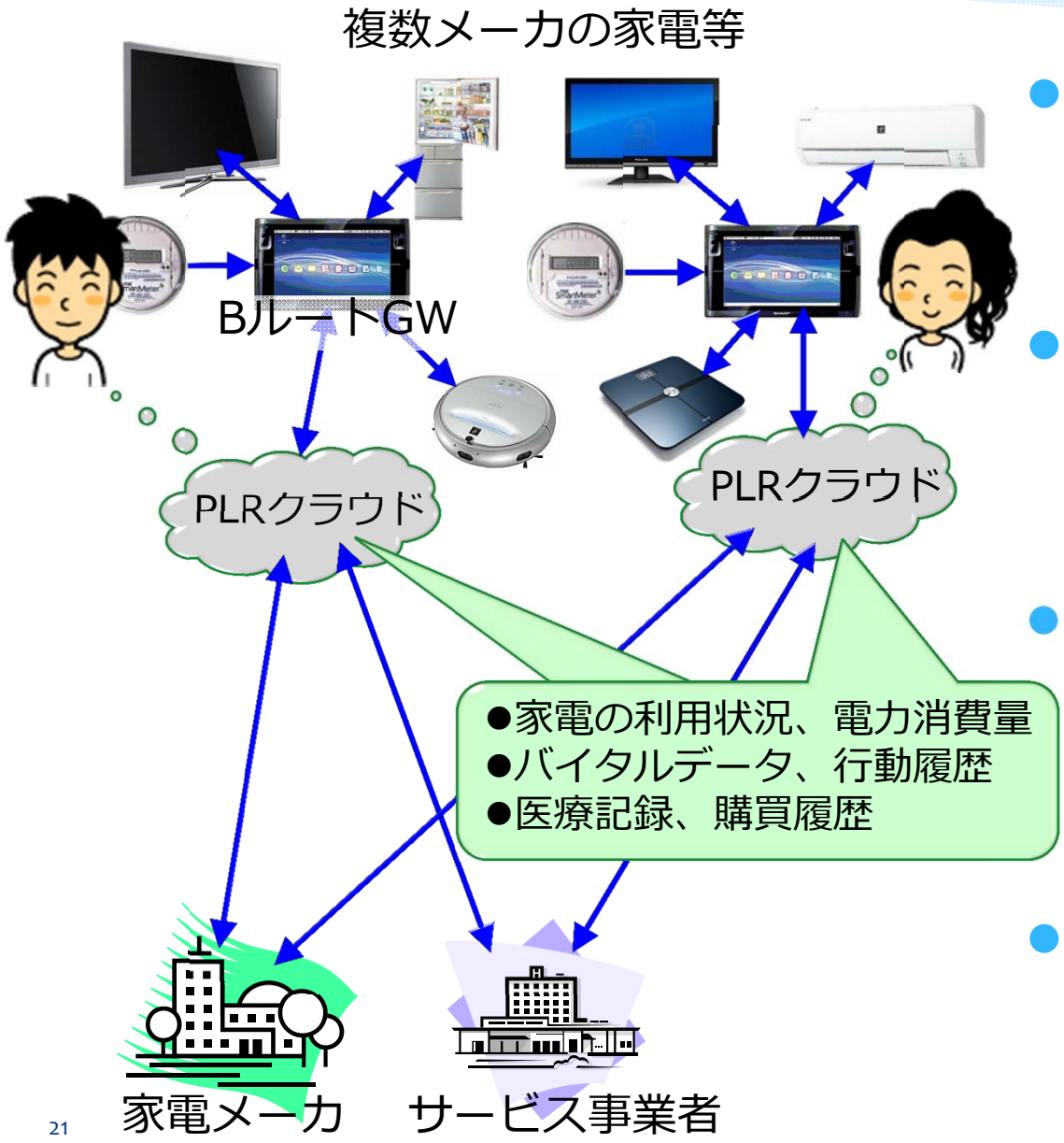
決済と履歴の利用

- 消費者Cと事業者Bと決済代行者Pがデータを共有
  cf. スマートレシート(東芝テック)
  - 購買に関する個人データをセキュアに管理し流通させる
    - CのデータがCのPLRストレージに自動的に蓄積され、Cの意思により他者と簡単かつ安全に共有可能
  - BがCのニーズを正確に把握して質の高いサービスを提供
    - Cの同意の下でBからの購買以外のCのデータも参照
  - Cが自分の購買等の行動を最適化
    - 多くの事業者からの購買等のデータをPLRアプリで分析
  - 消費者が適正な評価に基づいて事業者を選ぶことで市場が健全に機能
    - 多くの消費者がデータを共有することにより事業者を評価
- 個人用電子手形
  - クレジットカードの不正使用 ← なりすまし
    - 番号等の開示が必要
    - 他者の端末を認証に使ってパスワード等を詐取される
  - 30年の実績がある法人間の電子決済を個人用にスマホで
  - PLRによる鍵対と講買履歴の管理

個人用電子手形 + 購買データの活用

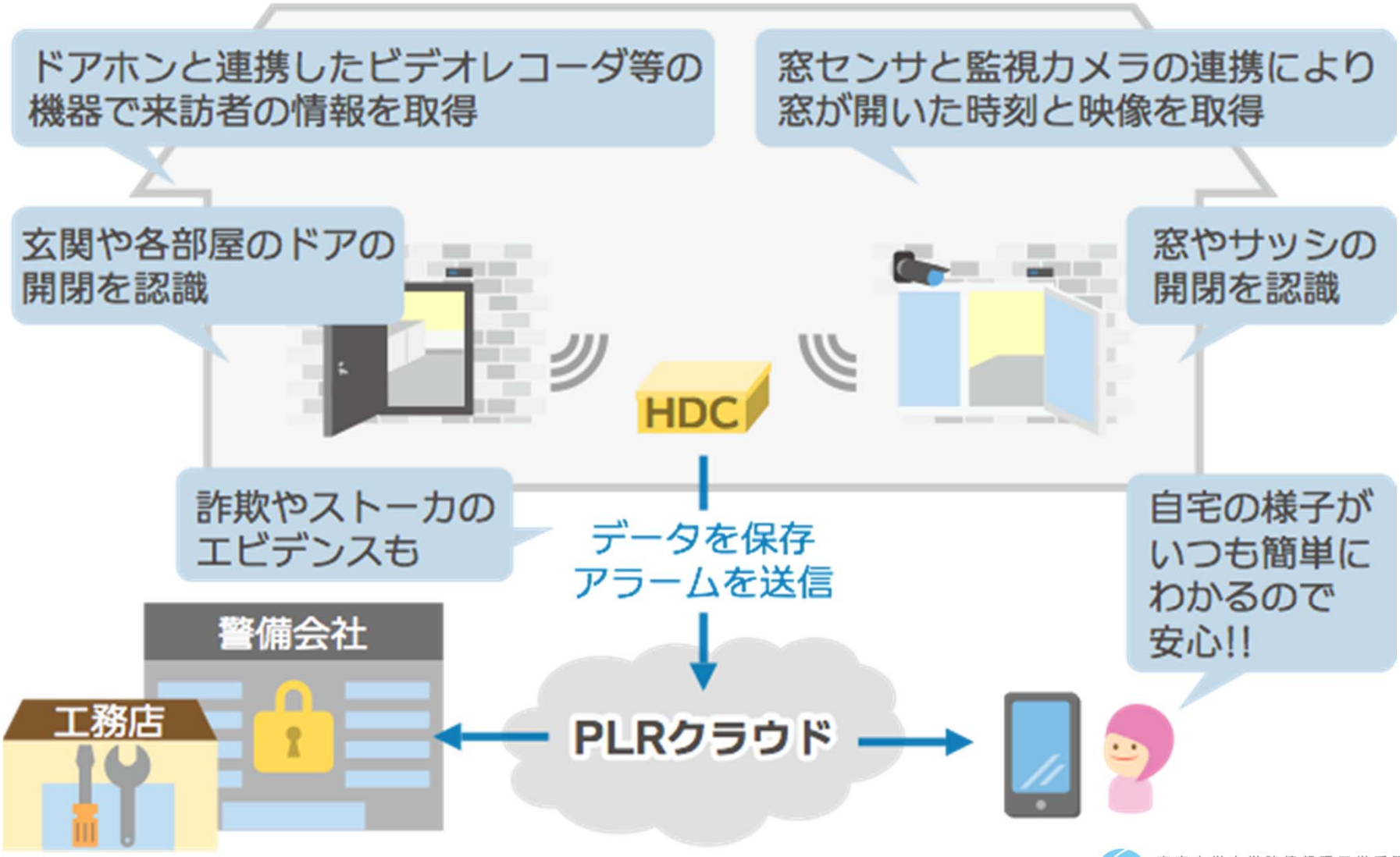


家電を活用した生活サービス



- 多数の利用者のPLRで蓄積された標準形のデータを利用者の同意の下で分析することにより、多様なサービスを低コストで提供できる。
- 家電とエネルギーの管理
  - 家電のトラブル対応
  - 漏電やガス洩れの検知
  - PVの保守と省エネ
  - 製品の改良・開発
- 見守りと健康管理
  - 行動と体調の把握
  - 緊急時のデータ開示
    - 災害、犯罪、事故等
    - コールボタン付バイタルセンサ
- セキュリティ
  - ドアや窓の開閉や来訪者のデータの蓄積と分析

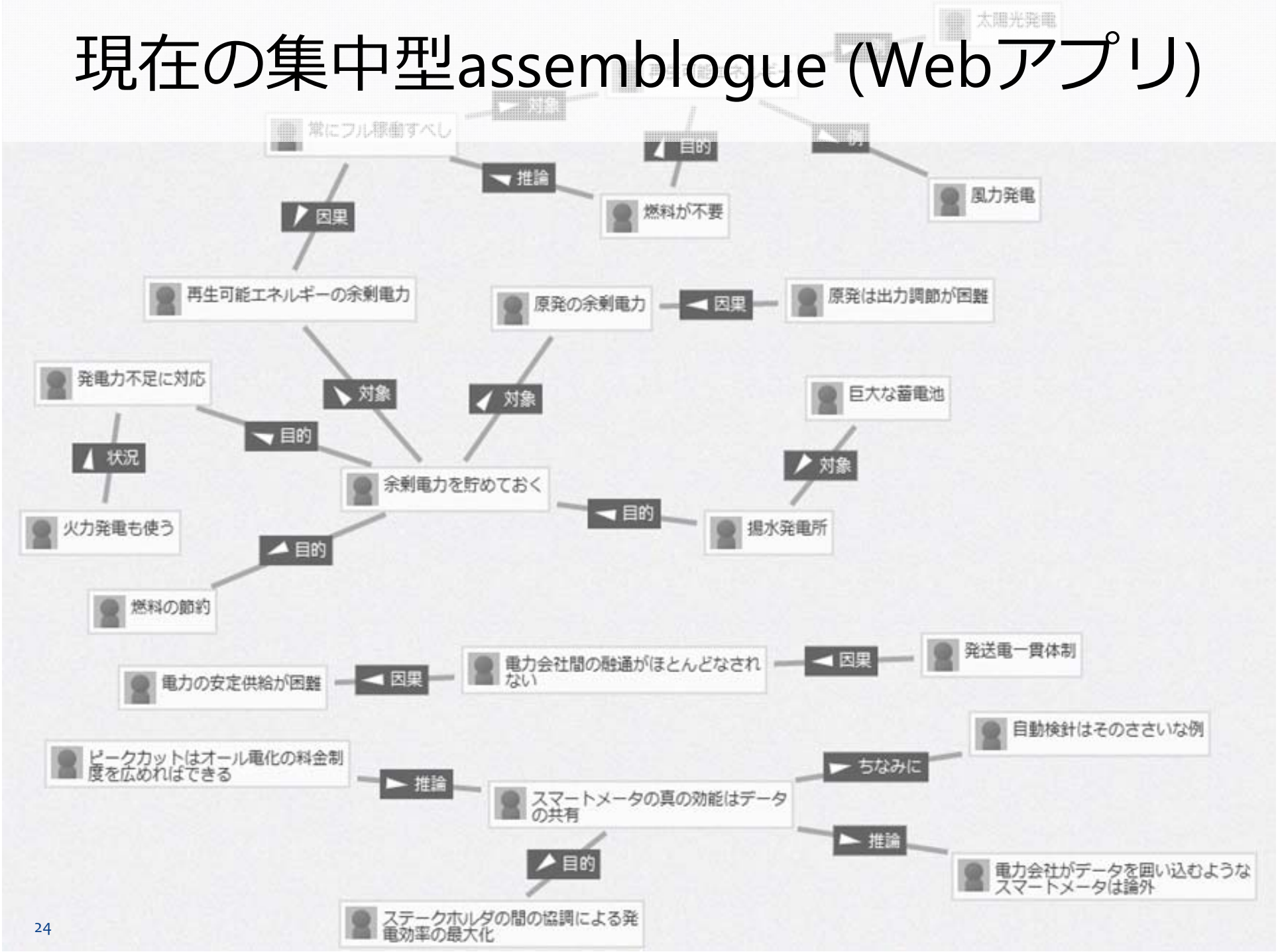
スマートホーム(セキュリティ)



assemblogue (分散SNS)

- 各利用者のコンテンツはPLRにより本人が管理
- 大規模なサーバの運用は不要
  - 低いコスト・高い持続可能性
  - 高いスケーラビリティ
  - 大規模で長期にわたる実践的研究が可能
- プライバシと言論の自由
  - 個人情報の漏洩
    - モバイル・ウェアラブルデバイスの普及
  - 検閲や言論統制
    - 中国や中東だけでなく米国や日本でも

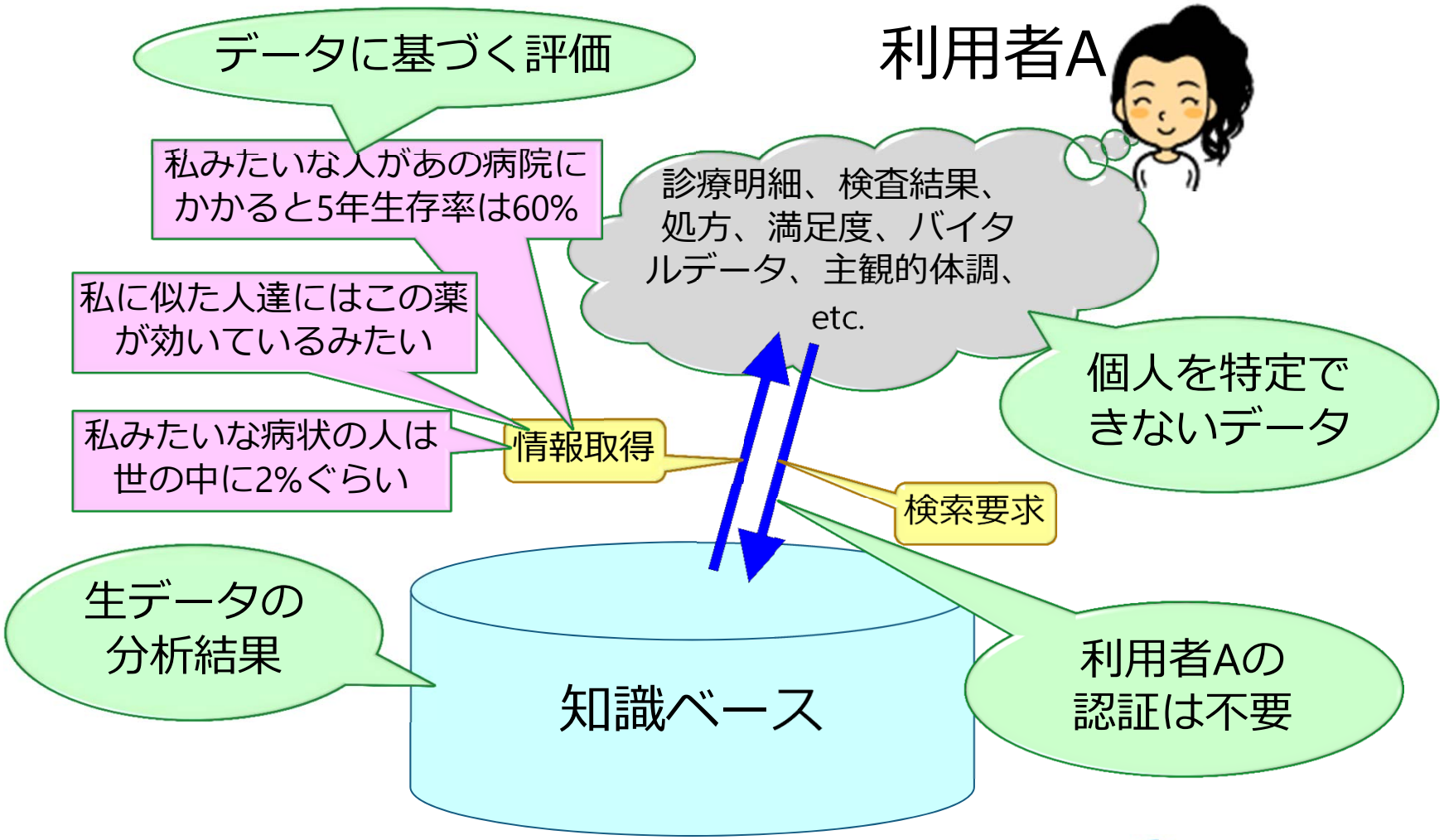
現在の集中型assemblogue (Webアプリ)



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(サービスや商品)の組み合わせ(買い方)を最適化
    - 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 … Media Lab., MITと連携
- 顧客がPLRデータを事業者に開示し、それに基づいて事業者がサービスや商品を提案
- 顧客のPLRデータを託されたソフトウェアエージェントがサービスや商品を検索

ヘルスケアにおけるVRMの例

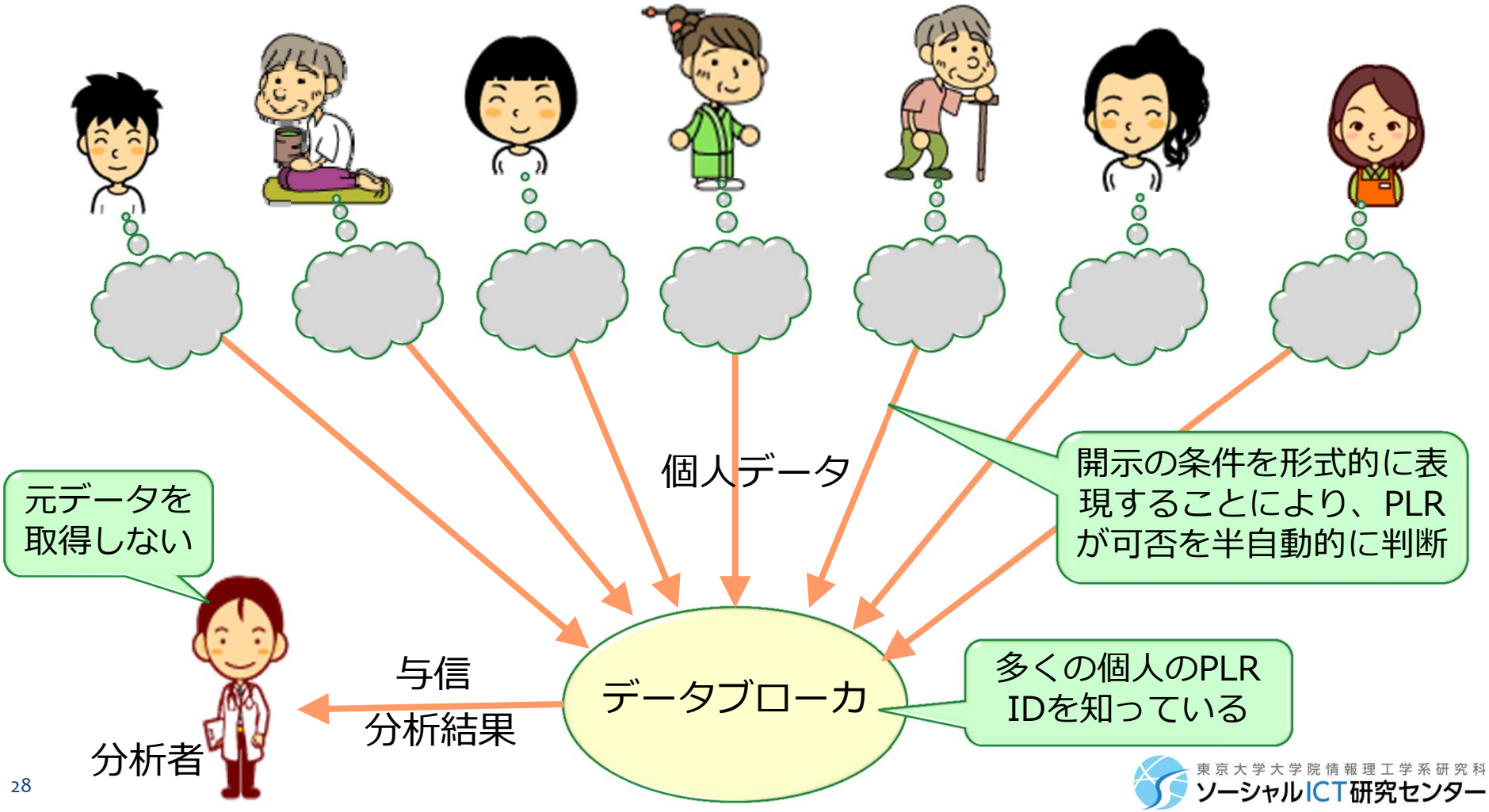


集めないビッグデータ

- 個人の全データを集められるのは本人だけ
  - たった1人の個人に関してですら、その全データを他者が集めるのは不可能・不適切
  - Googleも個人の医療データ等は集められない
- データをいきなり集めるのではなく、いつでも必要に応じて集められるようにしておく
  - 本格的に集めるのは目的と利用法が明確化してから
  - 各個人が本人のデータをPLRで統合的に蓄積・管理
  - 個人の同意の下で事業者が必要なデータを参照
    - 多数の個人のPLRアカウントを知っていれば良い
    - 生データを保管せず分析結果を残す

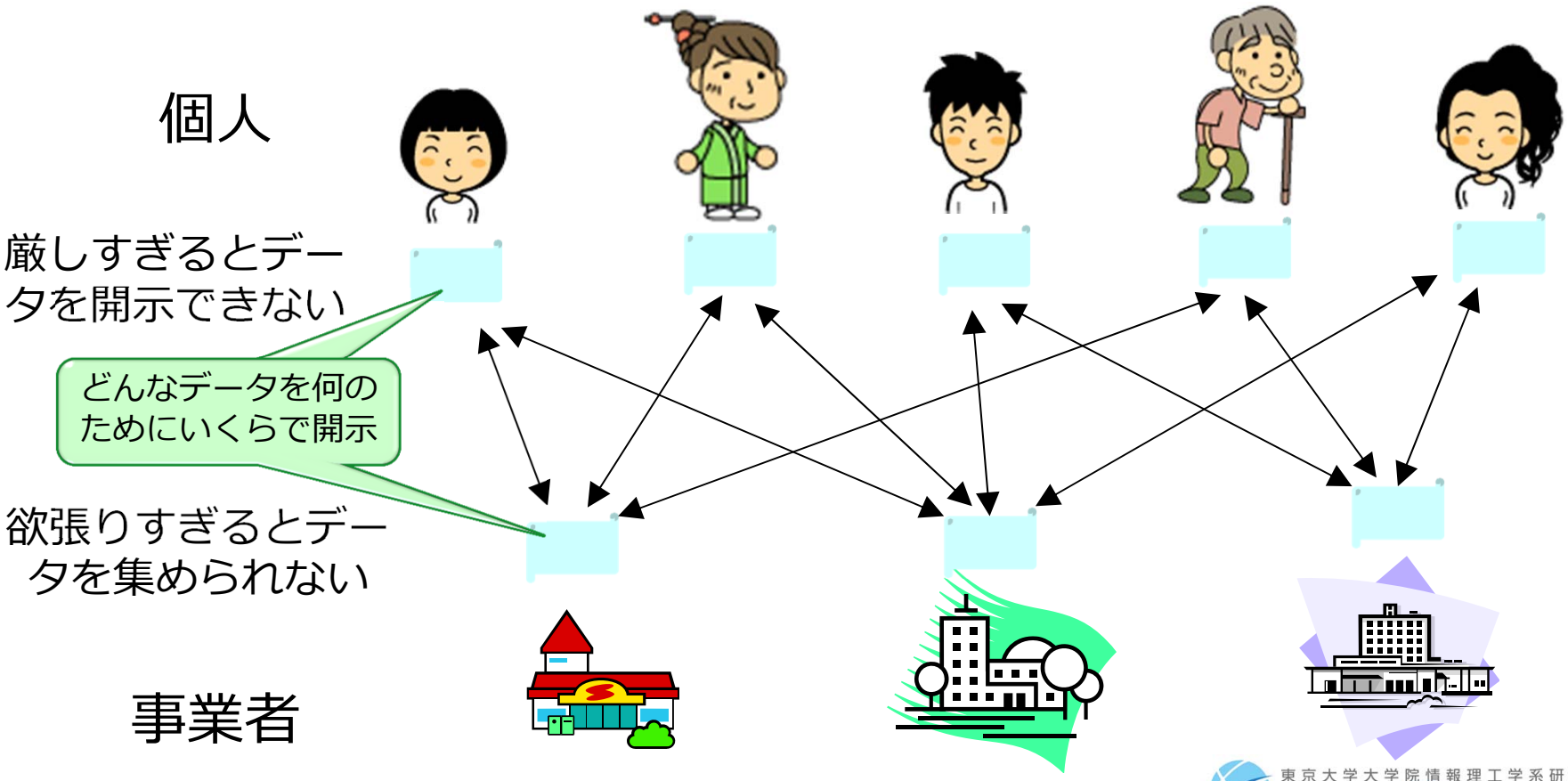
個人データのアドホックな集約と分析

- データ開示の手続きがオンラインで簡単に
- 本人の目の届く範囲で個人データが流通
  → 安心してデータを開示



個人データと開示条件(PP)の市場

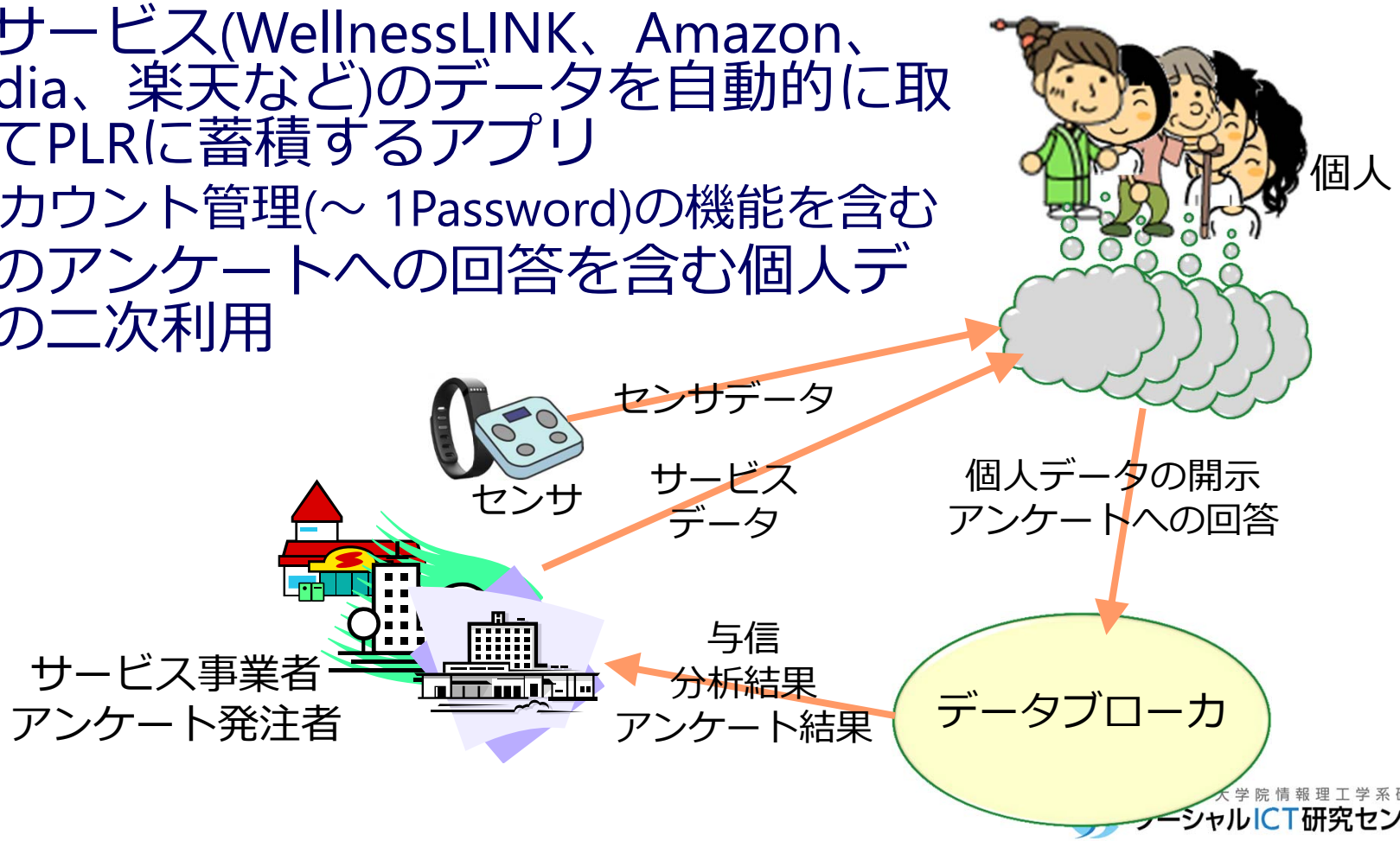
- ソフトウェアエージェントが自動照合できるように開示条件を表現
- 開示条件の相場を市場メカニズムで形成
- よくわかっていて自分に似た他者の開示条件を流用



アンケート代行 → データブローカ

アンケート代行事業

- PLRにデータが蓄積される前から可能
- アンケートへの回答を回答者のPLRに蓄積
- 他のサービス(WellnessLINK、Amazon、Expedia、楽天など)のデータを自動的に取得してPLRに蓄積するアプリ
  - アカウント管理(～ 1Password)の機能を含む
- 過去のアンケートへの回答を含む個人データの二次利用



PLRで得をするのは誰か?

- もちろん個人のメリットは大きい。
- しかし、PLRの最大の受益者は、巨大なB2Cサービス事業者:
  - Google、Amazon、Facebook、Dropbox、Apple、通信事業者、電力事業者、政府・自治体、etc.
  - Google主導の分散PDS?
    - その気になれば簡単のはずだが…
  - Amazon主導のVRM?
    - Amazonは、PLRに基づくVRMにより、個人データ管理や推薦のコストを激減させ、売り上げを増大させることが可能。
- 早い者勝ち!
  - 特にデータ仕様の集合的な標準化

PLRのグローバル展開

- パトリオット法により、米国企業は通信の秘密を完全に保証するサービスやアプリを提供できない?
  - E. Snowden氏が使っていた暗号化メールサービスLavabitの閉鎖
- 通信の秘密を完全に保証するサービスやアプリを特定の者がグローバルに提供するのは困難
- 公共財としてのPLR
  - 中長期的にはオープンソースソフトウェアとして不特定多数の人々がメンテナンスする体制を構築

32

課題: 不特定多数の一般利用者

- セキュリティ
  - PLRは社会全体のセキュリティを劇的に高める。
    - 個人データ利用に本人の許可が必要。
    - 数百万人のクレジットカード等のデータより、1人がPLRで管理するデータの方がはるかに小さい。
  - しかしもちろん完璧なセキュリティはあり得ない。
    - 不適切な開示の許諾
    - パスワード等の漏洩 → 代理人や後見人による支援
- データの質
  - センサ等の使い方
  - 問診票等の書き方

会員募集!

JEITA 知識情報処理技術専門委員会(～H25)

↓

JEITA ビッグデータ工学専門委員会(H26～)

自律分散協調社会基盤コンソーシアム?