# パーソナルデータと時空間ビッグデータ

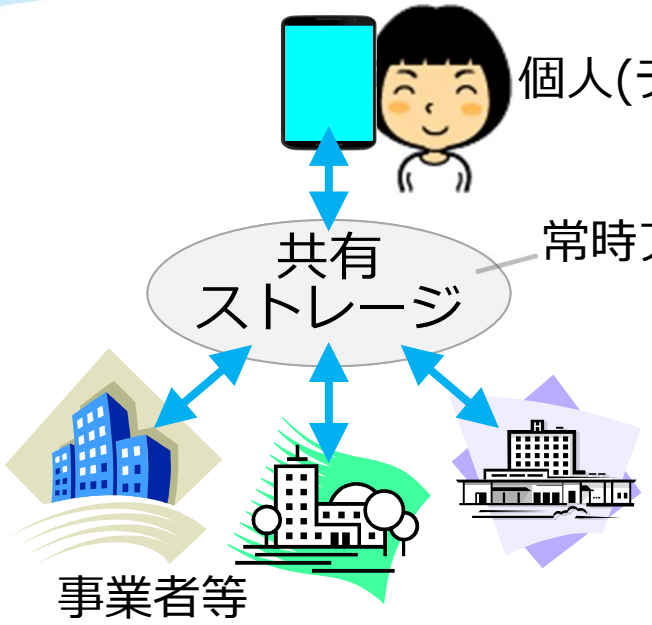
2021-01-14 橋田浩一

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

# 本人主導のパーソナルデータ(PD)活用

- **PDを本人に集約することで価値が最大化**
  - **PDが名寄せされて価値が高まる**
    - 複数事業者に共通のID等は不要
  - 1次利用: 本人へのサービスでの活用
    - **各個人がPDをフル活用**できる
  - 2次利用: 多数の人々のPDの統計分析
    - **名寄せされたPDを本人同意だけで容易に収集**できる
    - **ごく一部(たいてい1%未満)の個人のPDを集めれば十分**
      - 実際は十分多くの個人がPDを提供してくれる
        - ドナー登録やLINEのアンケートは国民の10%がオプトイン
  - PDの継続的集中管理がなければ**大規模な漏洩もない**
- 顧客の価値が最大化 → 事業者の収益も最大化
  - その価値への**貢献(PDの本人への提供など)の度合に応じた収益分配**で各事業者の収益を高める持続可能なモデル
- ただし公共等(課税など)の目的には集中管理が必須

# データ管理法の分類




下表で全部

| | 共有ストレージ | 共有関係 | 経済性 | 可用性（共有） | 機密性・完全性 | 追跡可能性アクセス制御 |
|---|---|---|---|---|---|---|
| 集中PDS、情報銀行など | 他 | ? | | ✓ | | ✓ |
| ID連携、MedRecなど | ? | 他 | ✓ | ✓ | ✓ | ✓ |
| PLR | 自 | 自 | ✓ | ✓ | ✓ | ✓ |
| digi.me、CitizenMeなど | 無 | 自 | ✓ | ✓ | ✓ | ✓ |

他者が集中管理

- 集中管理機能が単一障害点(SPoF)
- 共有ストレージがなく共有関係をブロックチェーンで管理すれば機密性・完全性は✓

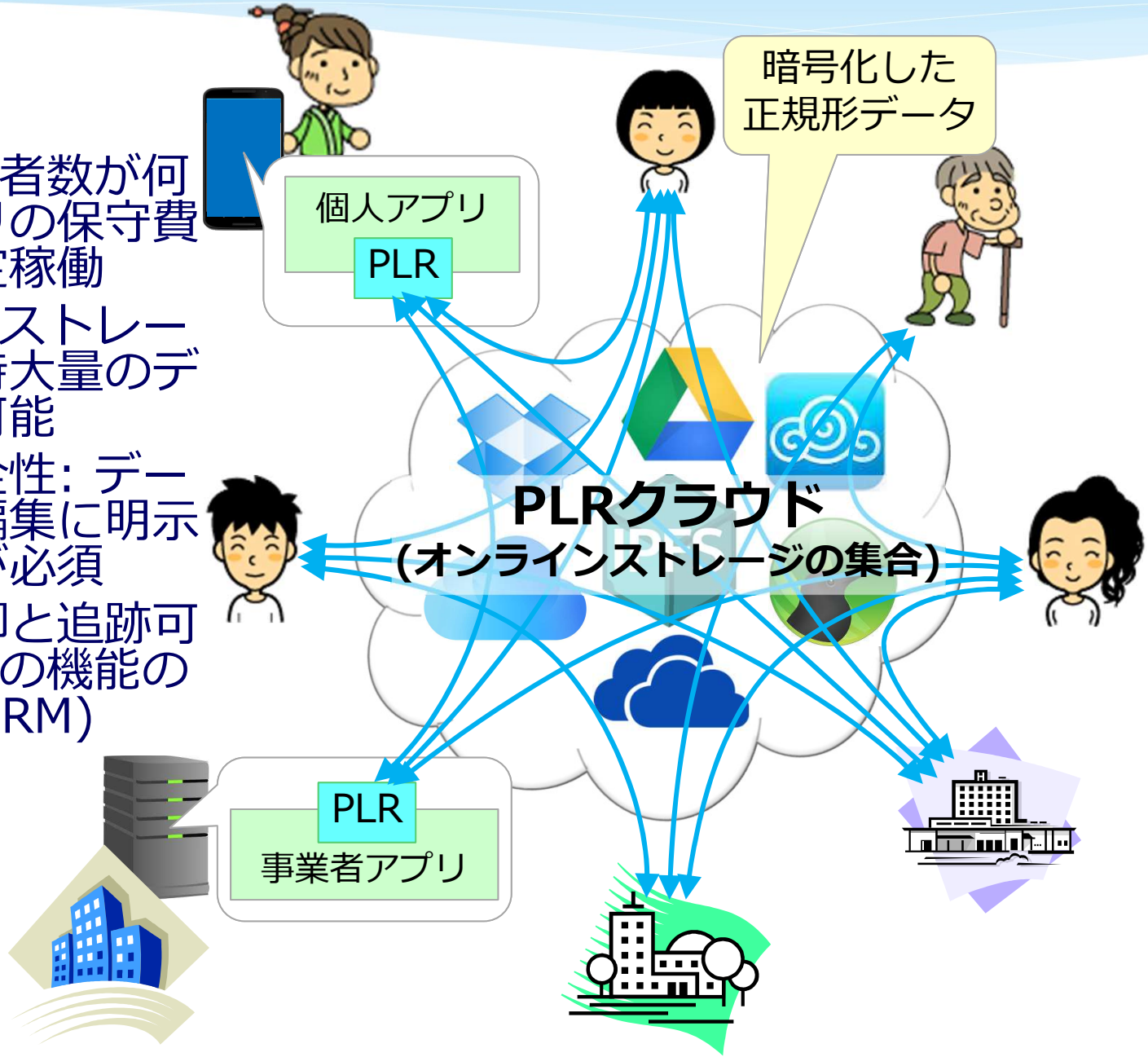
データ主体自身(またはほぼ専属の代理人)が管理

個人同士の共有や大量データの共有が困難

暗号化データへのアクセスをIRMにより制御・追跡

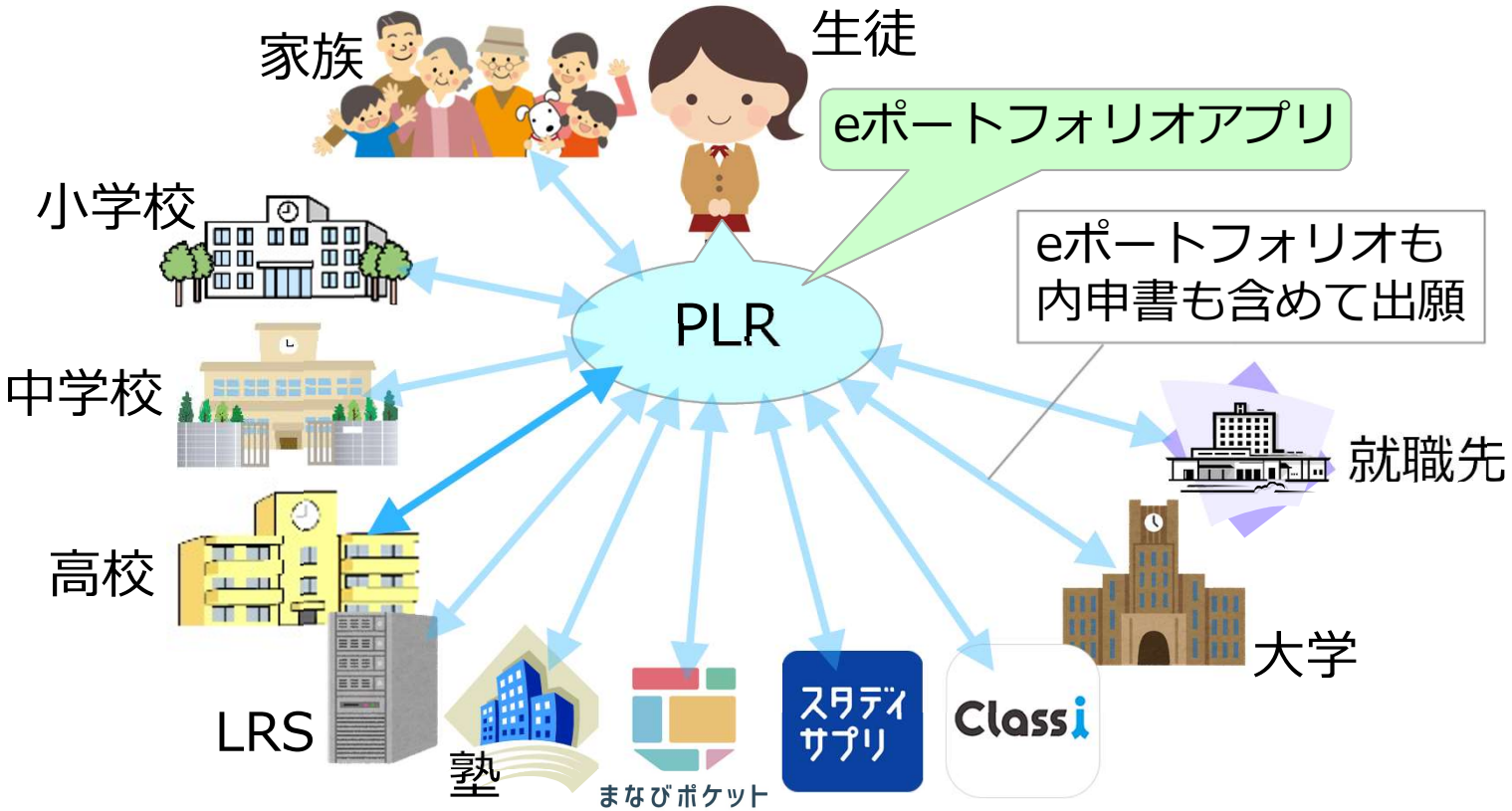
# 共有ストレージと共有関係の自己管理(PLR)

- 経済性: 利用者数が何億でもアプリの保守費用だけで安定稼働
- 可用性: 共有ストレージにより常時大量のデータ共有が可能
- 機密性・完全性: データの閲覧・編集に明示的本人同意が必須
- アクセス制御と追跡可能性: アプリの機能の限定と強制(IRM)

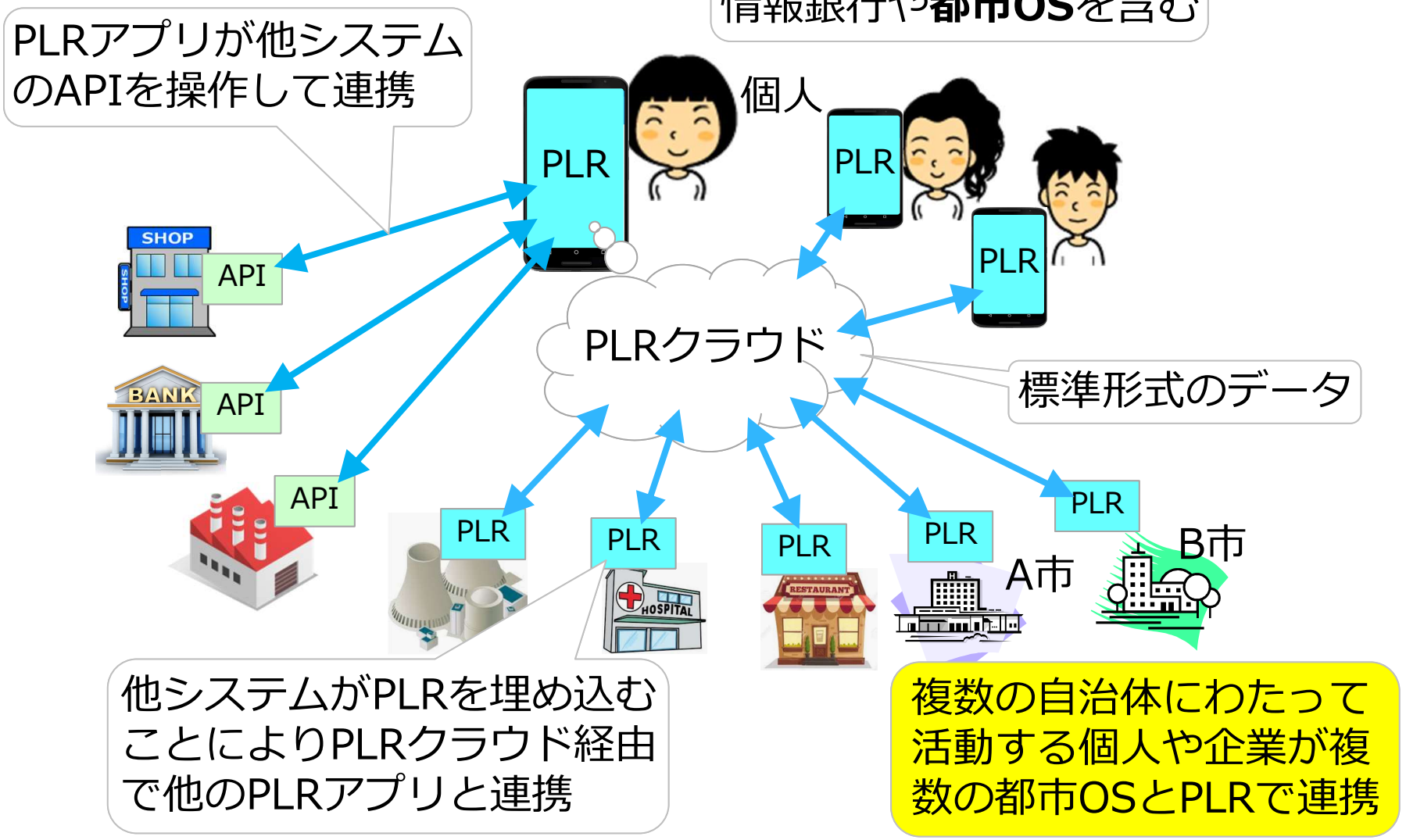


# 分散eポートフォリオ

- 調査書の電子化や生涯スタディログの基盤を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2020年度から実運用中

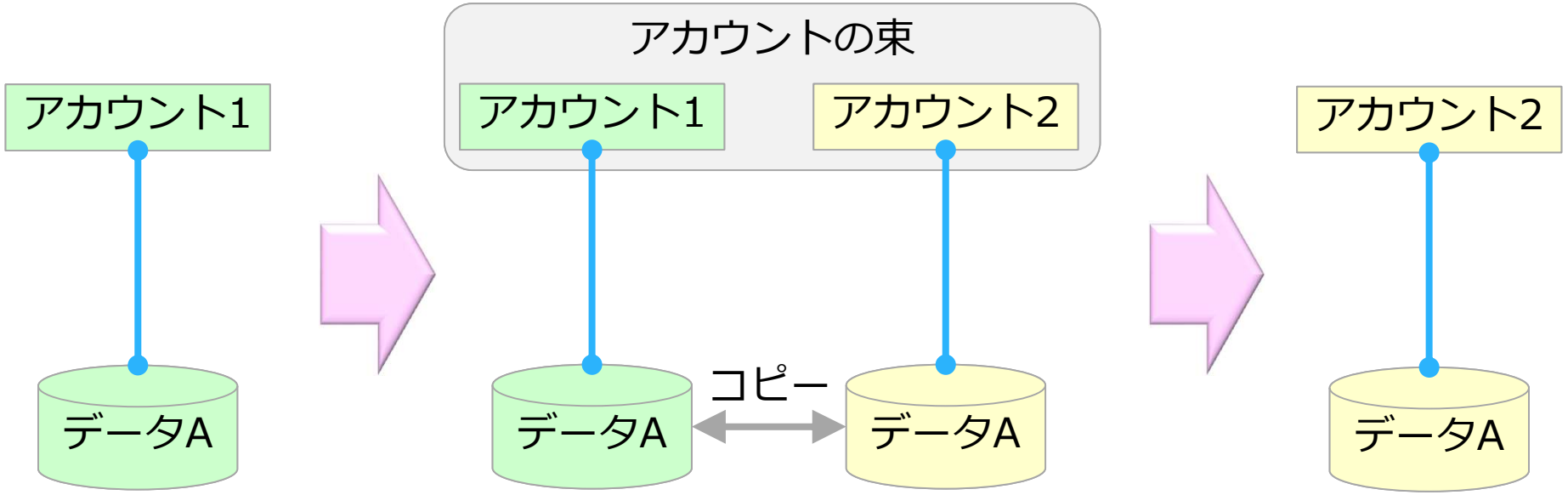


# PLRによる**異種システム**間連携



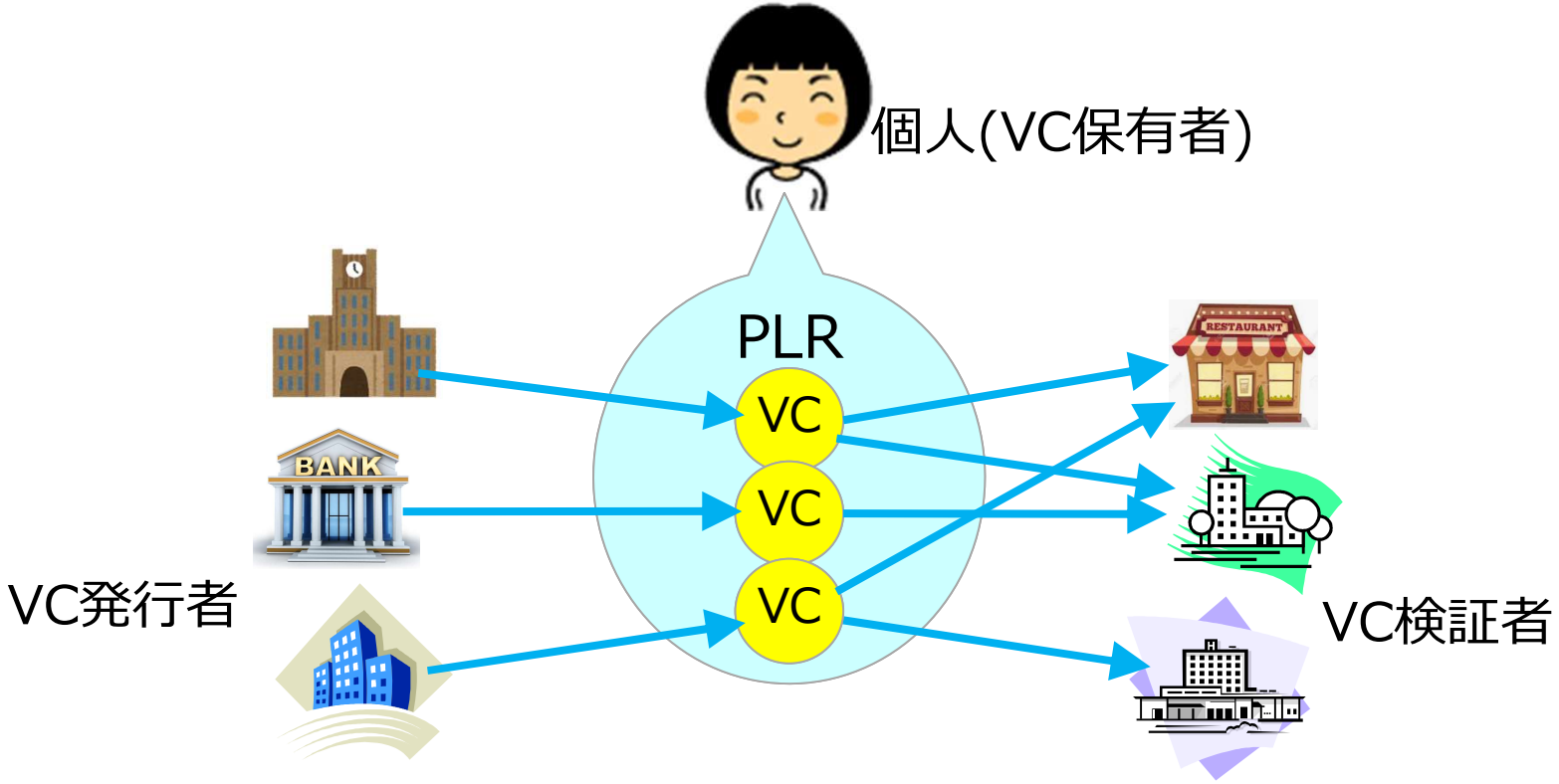
# アカウント連携

- 異種サービスにわたる複数アカウントを束ねる
  - 束の内容は利用者本人だけが把握
  - データの多重化による可用性の向上
  - 進学や転職の際のアカウントとデータの移行(下図)

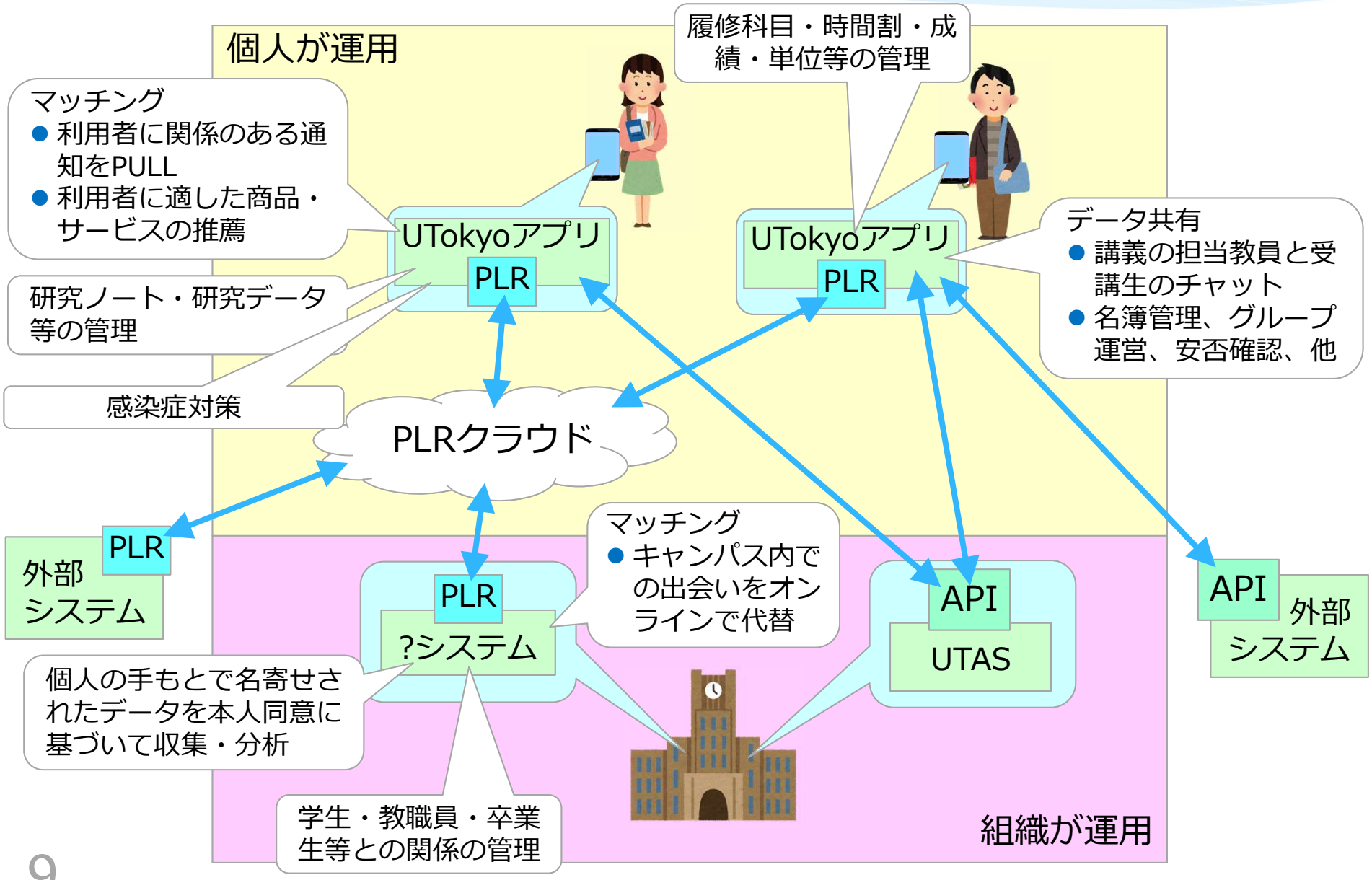


# 分散ID = PLR + VC

- 個人が検証可能資格証明(Verifiable Credentials; パーソナルデータ)を複数の発行者から取得してPLRに保管し、適宜組み合わせて検証者に開示することにより自らの属性を証明
- VCの仕組みはPLRとは一応別
  - VC発行者の公開鍵等をブロックチェーンで管理しても良い
  - そのブロックチェーンネットワークをPLRで実現することも可能

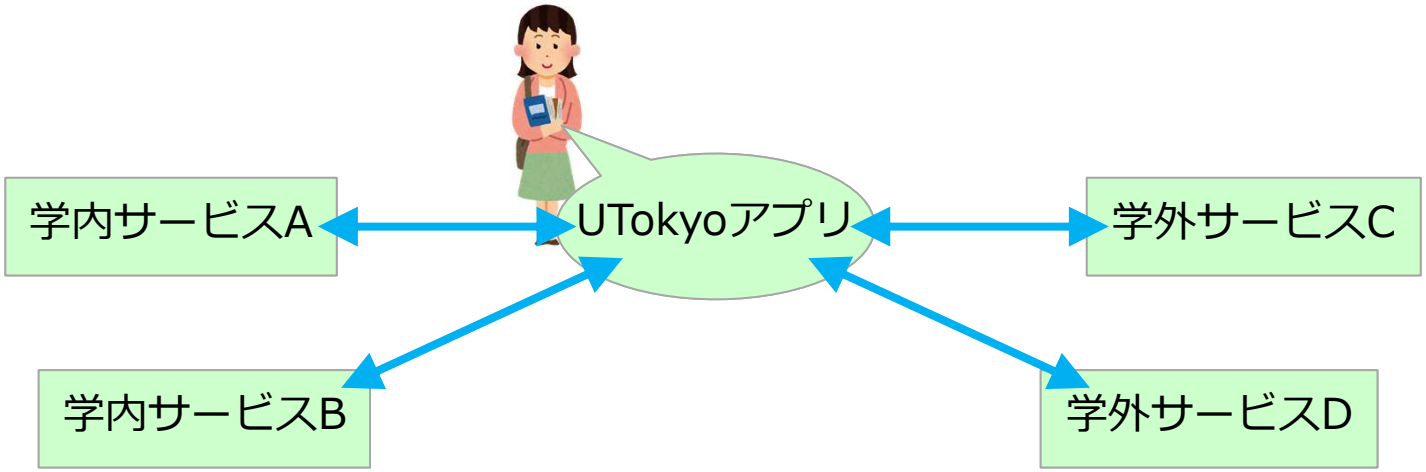


# UTokyoアプリ


個人が運用
履修科目・時間割・成績・単位等の管理
マッチング
● 利用者に関係のある通知をPULL
● 利用者に適した商品・サービスの推薦
UTokyoアプリ
PLR
UTokyoアプリ
PLR
データ共有
● 講義の担当教員と受講生のチャット
● 名簿管理、グループ運営、安否確認、他
研究ノート・研究データ等の管理
感染症対策
PLRクラウド
PLR
外部システム
マッチング
● キャンパス内での出会いをオンラインで代替
PLR
?システム
API
UTAS
API
外部システム
個人の手もとで名寄せされたデータを本人同意に基づいて収集・分析
学生・教職員・卒業生等との関係の管理
組織が運用

# 多様なサービスのハブ

- PLR利用者は、各サービスから取得した自らのデータを手もとで自由に活用でき、また原則として任意の他者に開示できる。
  - 履修科目や成績のデータを分析して進学先を選ぶ
  - あるサービスから得たデータを別のサービスに開示
    - 例: 成績証明書を就職先に開示
  - 学外サービスに対して自分の学籍を証明…分散ID




- ただし各サービスはそのデータの開示範囲を限定できる。
  - 例: シラバスの開示先はUTokyoアカウントのみ

# データのサプライチェーン