オープンソースPDS Personium とその応用

Personium
An open source Personal Data Store

2018-05-25

下野　暁生 (SHIMONO, Akio)

Personium Project Lead
Open Knowledge Japan 会員
富士通株式会社クラウドサービス事業本部クラウドプロモーション統括部マネージャ

紹介動画

2:43

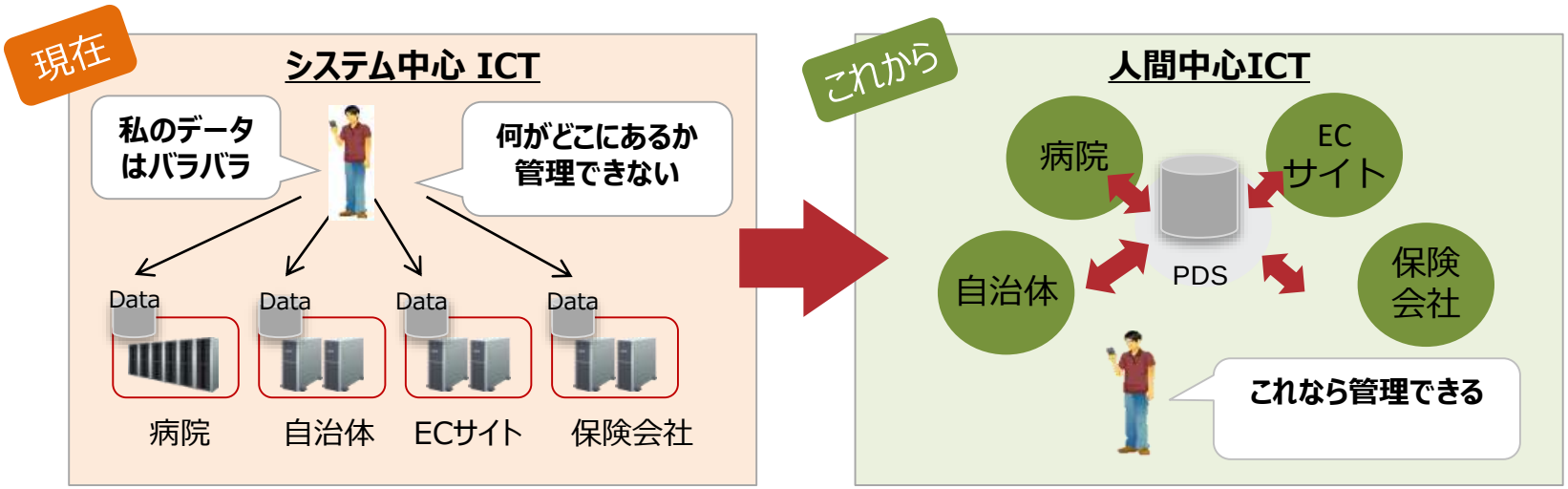
Personium
An open source Personal Data Store

https://youtu.be/uBFfsCIwGq4

PDS (Personal Data Store)

Personium
An open source Personal Data Store

パーソナルデータストア ＝ 人間中心ICTを実現するための個人用データストア



システムは課題解決等
関心事に作られる
結果、利用者データは
バラバラのサイロの中

皆が**自分のデータ置き場**をもち
サービスがここに読み書き
自身の意思でサービスの垣根
を超えてデータを自由に活用

ICTの人間社会との関係を根底から変えようという野心的取り組みでもある

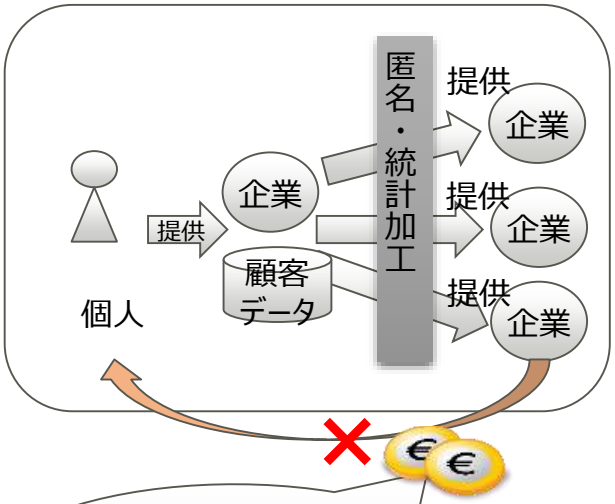
なぜPDS？：企業の視点から

Personium
An open source Personal Data Store

従来のデータ流通の限界

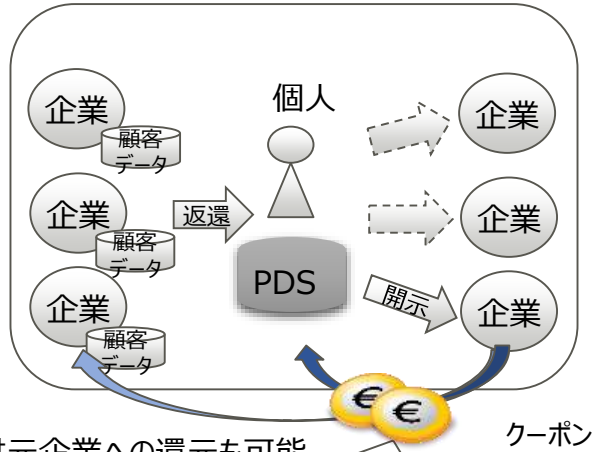
従来のデータ流通方法では匿名化が必須であり、利用者に直接対価を還元できない。
個人情報を個人の意思で開示するPDSであれば、実名のままでの流通が可能となり、
直接対価を還元することができます。

従来：BigData型のデータ利活用



匿名であるため
データ提供した個人に提供対価を
直接還元できない

PDS型のデータ利活用



情報提供の**制御を個人に返す**ことで
ユーザの**自己意思で個人を特定して**提供できる
⇒個人への**直接還元**が可能

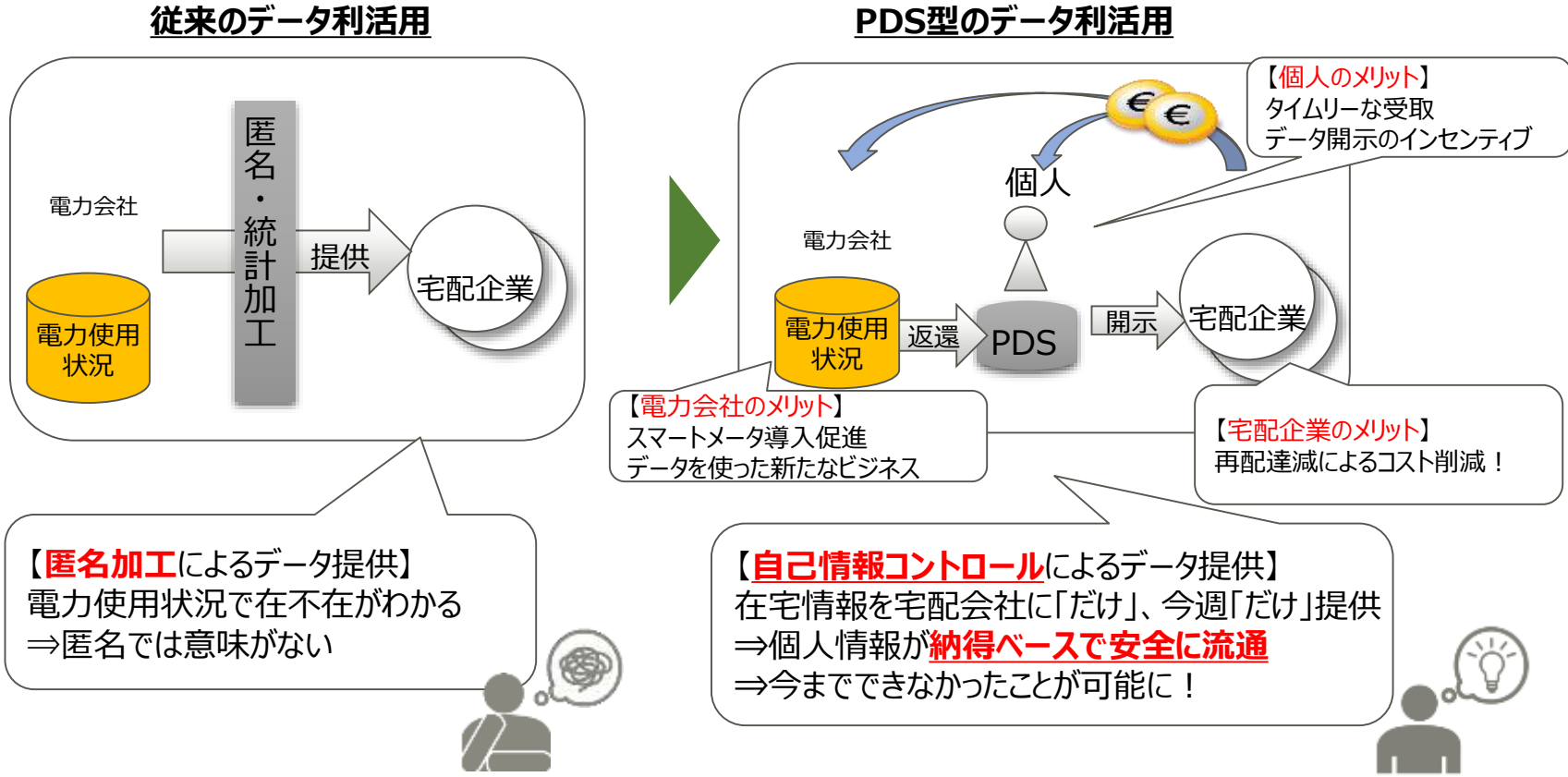
本質：個人同意のもと多くの企業間でデータ流通するためのハブ

PDSがつなげるサービス連携の例

Personium
An open source Personal Data Store

■ 例：在宅情報の活用

宅配業者が荷物の配送前に、配送先の在宅状況を確認したい。

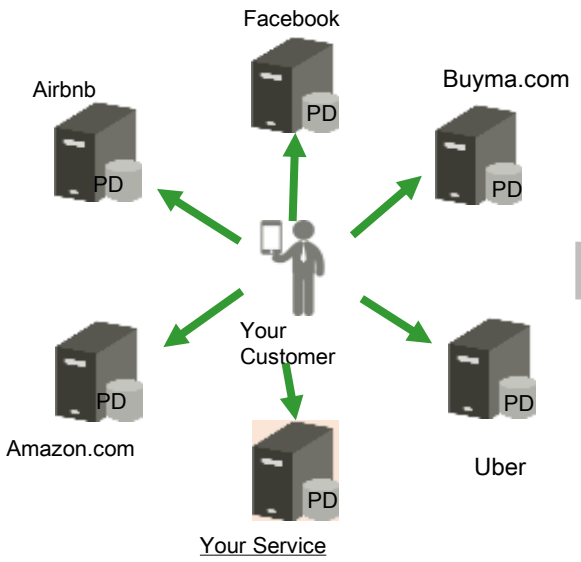


このような業種をまたがったデータ連携ニーズはあらゆる分野に

データポータビリティという追い風

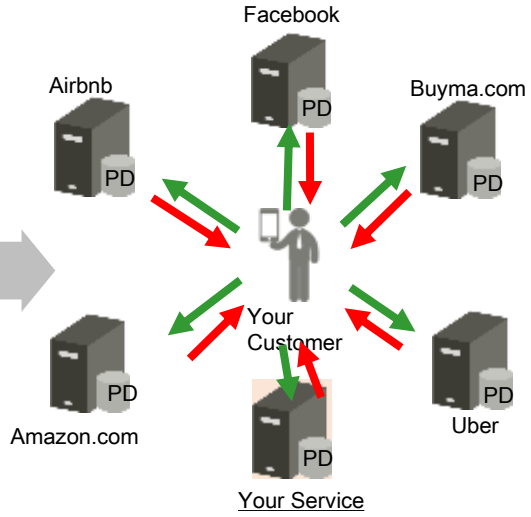
Personium
An open source Personal Data Store

Data Portabilityなし



利用者データは各サービスに**囲い込まれた**まま

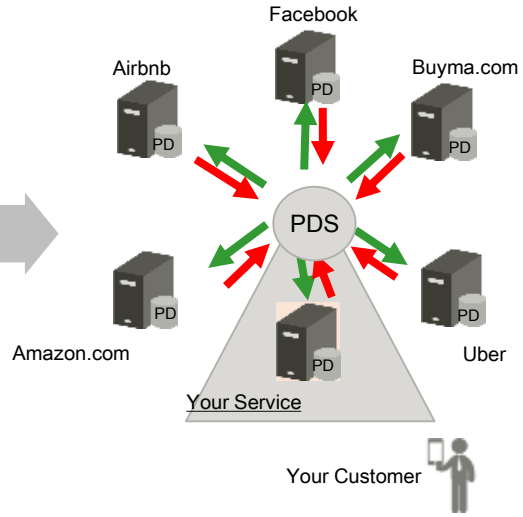
Data Portabilityのみ



利用者が使う**すべてのサービス**のデータは **機械可読なかたちで**利用者には**返ってくる**。

ただし、人間は機械ではないので、それだけでは何も起こらない。

PDSを使うと・・・



PDSを置くことで、様々なサービスから戻ってくるパーソナルデータを個人が**自ら集約して、統合活用**することができる。

まずは動いているところをご覧ください

Personium
An open source Personal Data Store

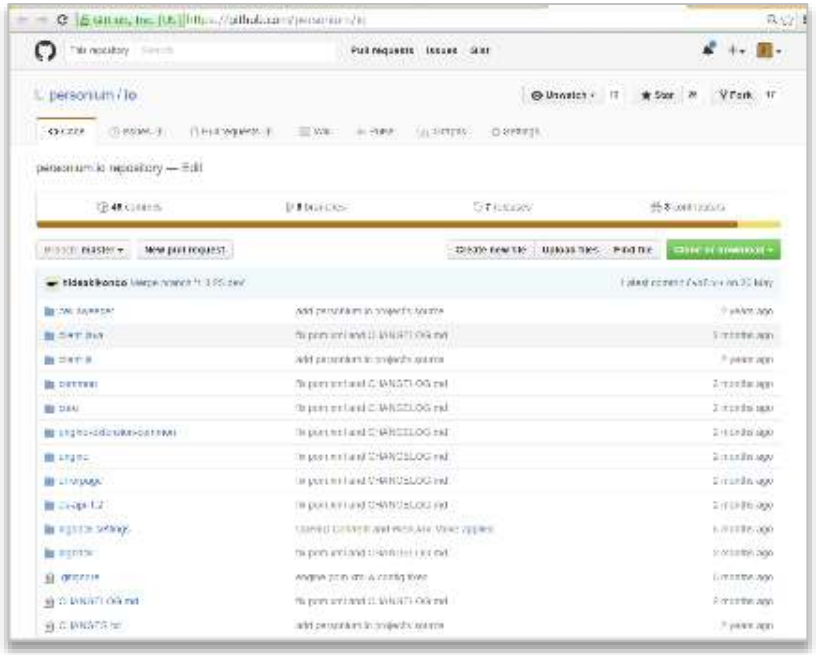
Personiumとは

Personium
An open source Personal Data Store

オープンソースの分散(Decentralized) PDSサーバです。

https://personium.io/

現在富士通を中心に開発、公開、順次改版リリース中。ただし、中立かつオープンなプロジェクト運営を目指しています。



https://github.com/personium/

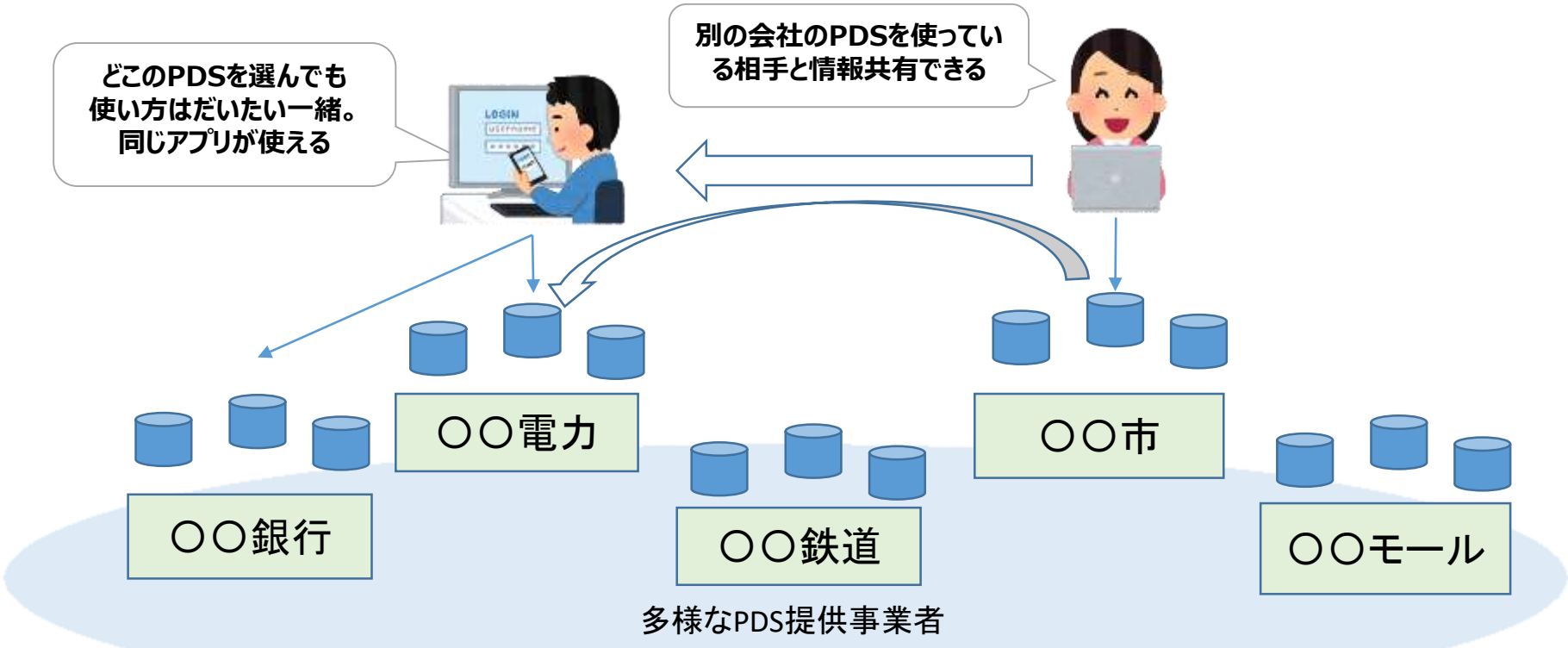
- ✓ Githubにて公開中
- ✓ ライセンスはApache License 2.0
- ✓ GUI・ツール・サンプルアプリ群等も併せて開発公開

Linux OSのマシンにインストールするとPDSサーバになります。
立てたPDSサーバ上には好きなだけPDSを作成してホストすることができます。

目指す世界：だれもがどこかにPDSを持つ

Personium
An open source Personal Data Store

■様々なPDS提供事業者（情報銀行）が共存共栄できる世界
- ＝消費者が選択できる世界
- 相互接続性のある世界

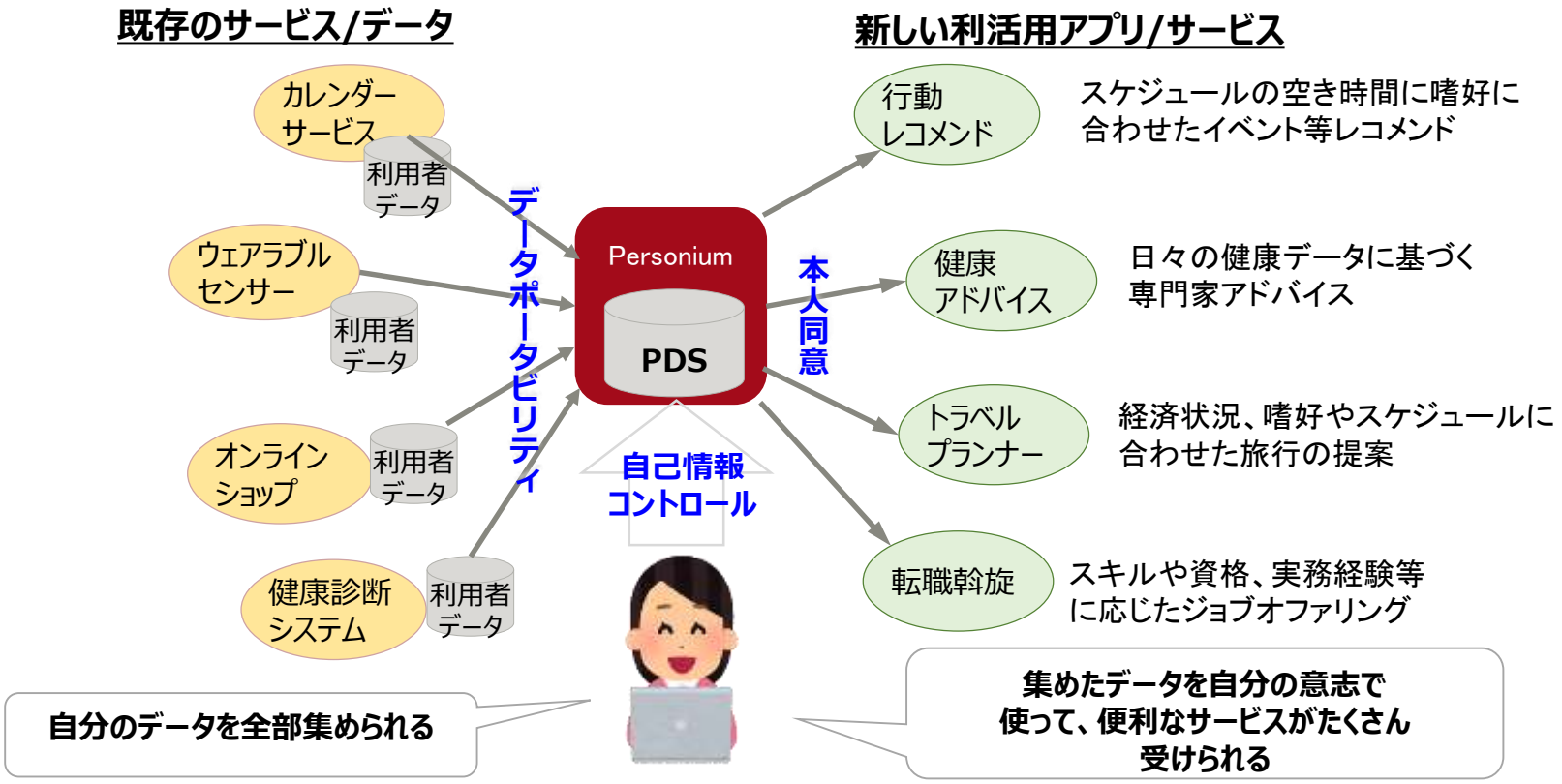


Personiumや互換性のあるPDSソフトを使った事業者同士はすぐに相互接続

目指す世界：無数のアプリ/サービスがアクセス

Personium
An open source Personal Data Store

- **多様なパーソナルデータ**がPDSに入り、**多様な組み合わせ活用**ができることがPDSの価値
- 様々な既存サービスとの**アダプタ**や、パーソナルデータ**利活用アプリ**の**充実度**が利用者の感じる価値に直結



必要なもの：

様々なプレーヤが参画できる**アプリエコシステム**

それを実現するための**プラットフォーム**としてのPDS

Personiumの技術ポイント

Personium
An open source Personal Data Store

- オープンな分散性とセキュリティ
  - 特定国家の一企業が運営する**単一システム**上に実現するモデルは**社会受容**されない

  →ユーザ、アプリの認証状態を、サーバインフラを超えて連携

  →**悪意あるアプリやPDS運用主体**なども想定したうえでの**全体としてのセキュリティ**を実現

- 柔軟かつセキュアなデータ管理
  - 利用者が**内容を意識するデータ**とそうでないデータ（ドキュメントデータ/アプリデータ）に両対応する

  →ファイル/テーブル状のデータどちらにも対応する

  - プラットフォーム**中立性**（様々な機器、OS,言語から扱えること）

  → UIを完全分離して**全機能Web API**で提供

- 自己情報コントロール
  - 柔軟なコントロール単位定義実現への対応
  - コントロール単位定義主体とコントロール主体のねじれ
  - 分散環境下での第三者アクセスの認証・制御

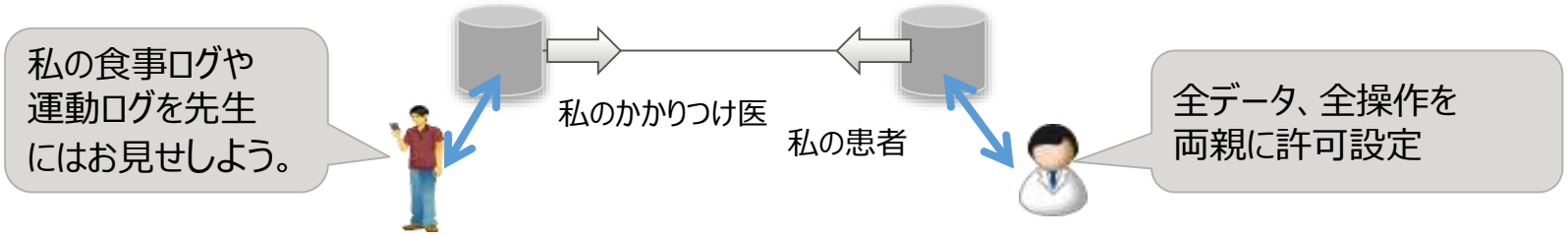
  →**ユーザ・アプリがともにロールを定義**可能なロールベースアクセス制御

  →任意の格納データを**加工**して出力する**ロジック実行環境**

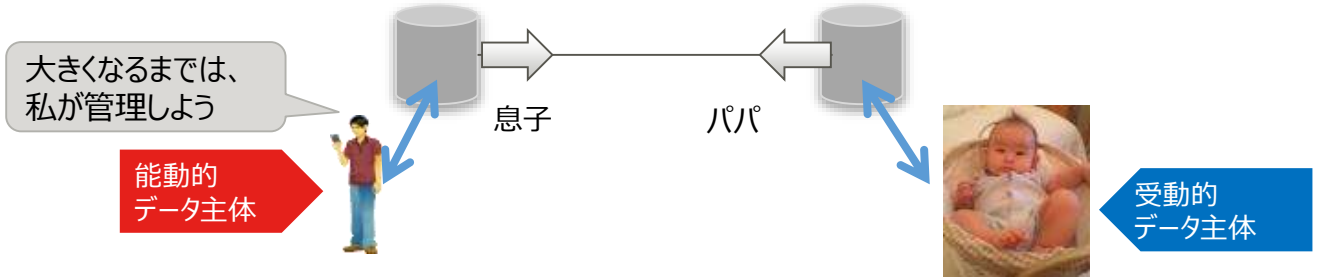
Personiumの特長(1/2)

- **誰でもPDSサーバを立てられる**
  - オープンソースソフトウェアであるため、事業者/自治体/政府/個人等**誰でもPDSプロバイダに**なれる。
- **全機能がREST API**
  - HTTPはどんなプラットフォーム（OS, 開発言語）扱えるため、クライアントの**プラットフォームを選ばない**。

- **データ開示・共有設定は相手PDSのURLを指定**
  - PersoniumのPDSにはみなURLが与えられる。
  - 他者(例： 妻、かかりつけ医、勤務先 etc.)へのデータ開示・共有は相手PDSのURLを指定して行う。
    他者PDSアクセスには電子署名技術を利用しており、**相手は別サーバであってもよい**。



  - **受動的データ主体**：幼児・高齢者などは、親族等に全データの全権限を許可することでPDSの運用移譲が可能



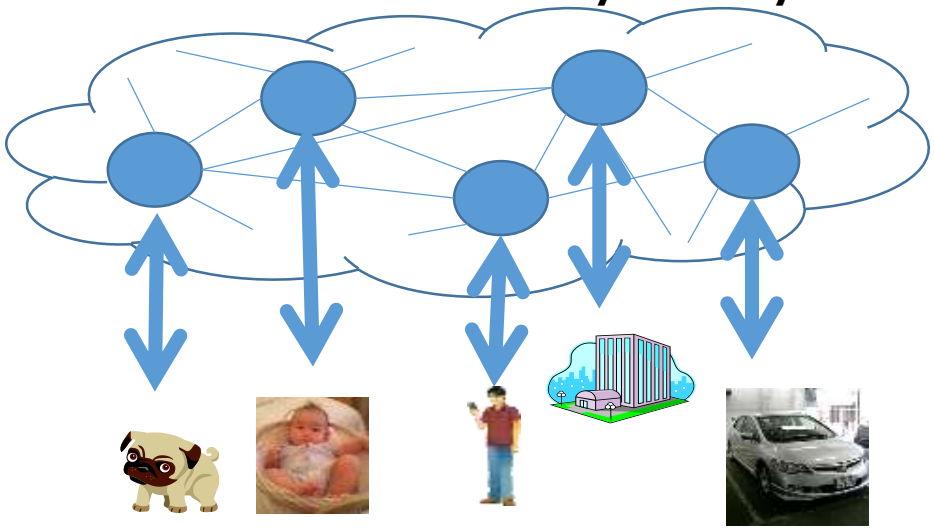
Personiumの特長(2/2)

■ Web of PDSを構成可能

- データ開示・被開示という関係で結ばれたPDS群は、特定の事業者が胴元（⇒ 一人勝ち）になるのではない中心を持たない**Decentralizedなネットワーク**を構成　（分散ソーシャルグラフ）
- バラバラにたてられたWebサーバにホストされたWebサイトがリンクしあってWWWができたように、バラバラに立てられたPDSがリンクし合った**巨大なWeb of PDSを形成可能**。
- オープンなエコシステム形成に必要となるセキュリティも実装

■ データ主体（⇒PDSオーナ）を人に限らず、モノ・組織などに拡張可能

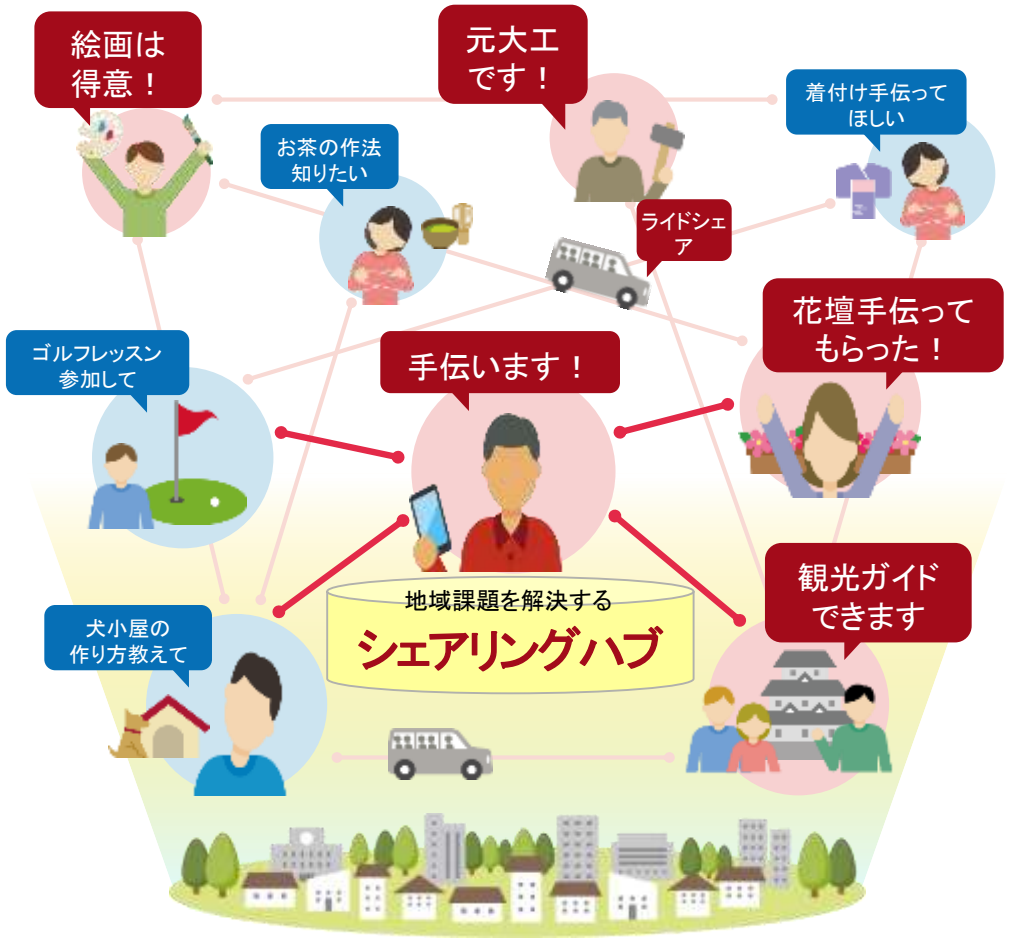
- 受動的データ主体を扱う要領で**データ主体をモノや組織などにも拡張可能**（例、家族/犬のポチのデータストア）
- **IoM, IoT, IoE を統合的に扱うモデルを標榜（Cyber-Physical）**



データ利活用イメージ：シェアリングハブ

Personium
An open source Personal Data Store

地域の新たな担い手となるアクティブシニアが地域課題を解決



地域のアクティブシニアが
豊富な知識や経験を活かし
地域の課題を解決

パーソナルデータを
自身がコントロール

シェアリングハブに開示することで
スケジュールの開いているところに
最適なレコメンドを提案

データ利活用イメージ：シェアリングハブ

Personium
An open source Personal Data Store

地域の新たな担い手となるアクティブシニアが地域課題を解決

坂東　陽子さん
（元建築士）

趣味特技

- 絵画や製図が得意
- お茶が趣味
- 着付けが得意

動画

坂東さん専用の
スマホアプリ画面

データ利活用イメージ：シェアリングハブ

Personium
An open source Personal Data Store

地域の新たな担い手となるアクティブシニアが地域課題を解決

伊藤　太郎さん
（元ゼネコンのサラリーマン）

趣味特技

- プレゼン、喋りがうまい
- ゴルフのセミプロ
- ドバイ駐在経験あり

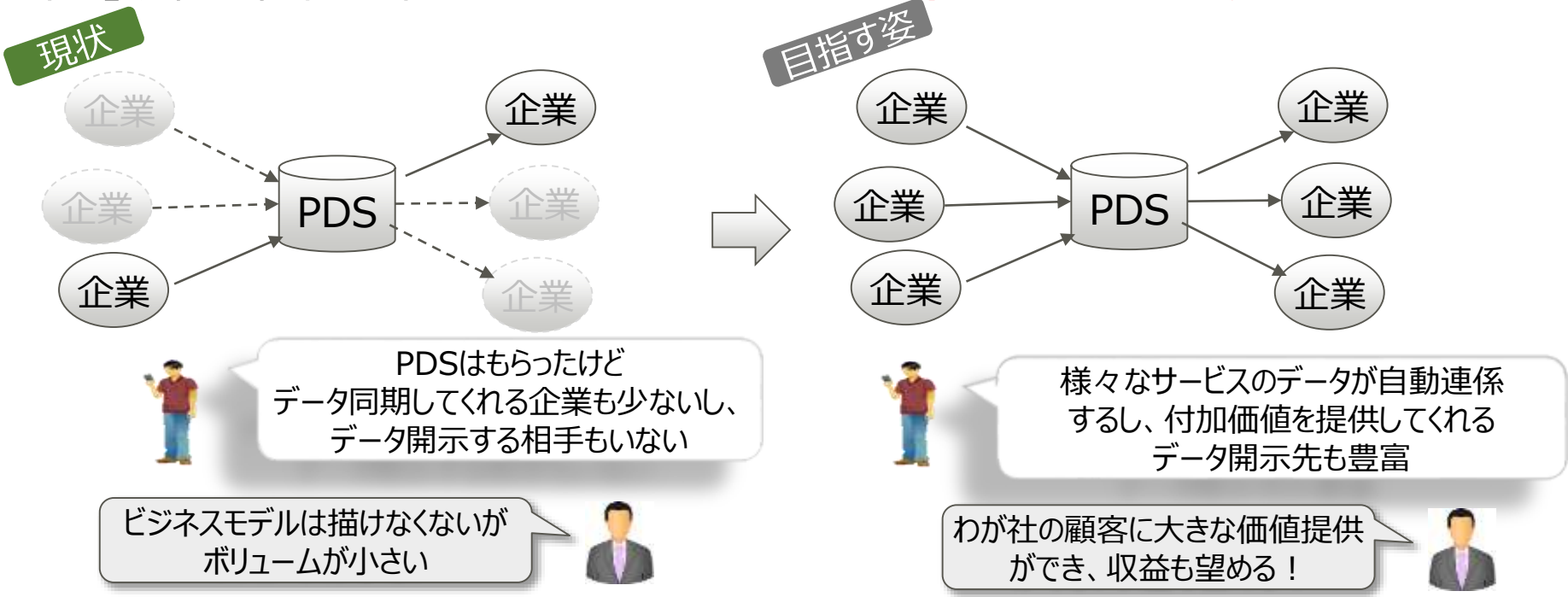
動画

伊藤さん専用の
スマホアプリ画面

課題：「繋ぐ」技術の価値訴求

Personium
An open source Personal Data Store

「繋ぐ」技術の価値は繋がる**相手の数で決まる**ため**最初は価値訴求が難しい**



ネットワーク外部性 (メトカーフの法則)

ネットワークの通信の価値は、接続されているシステムのユーザ数の二乗（n2）に比例する

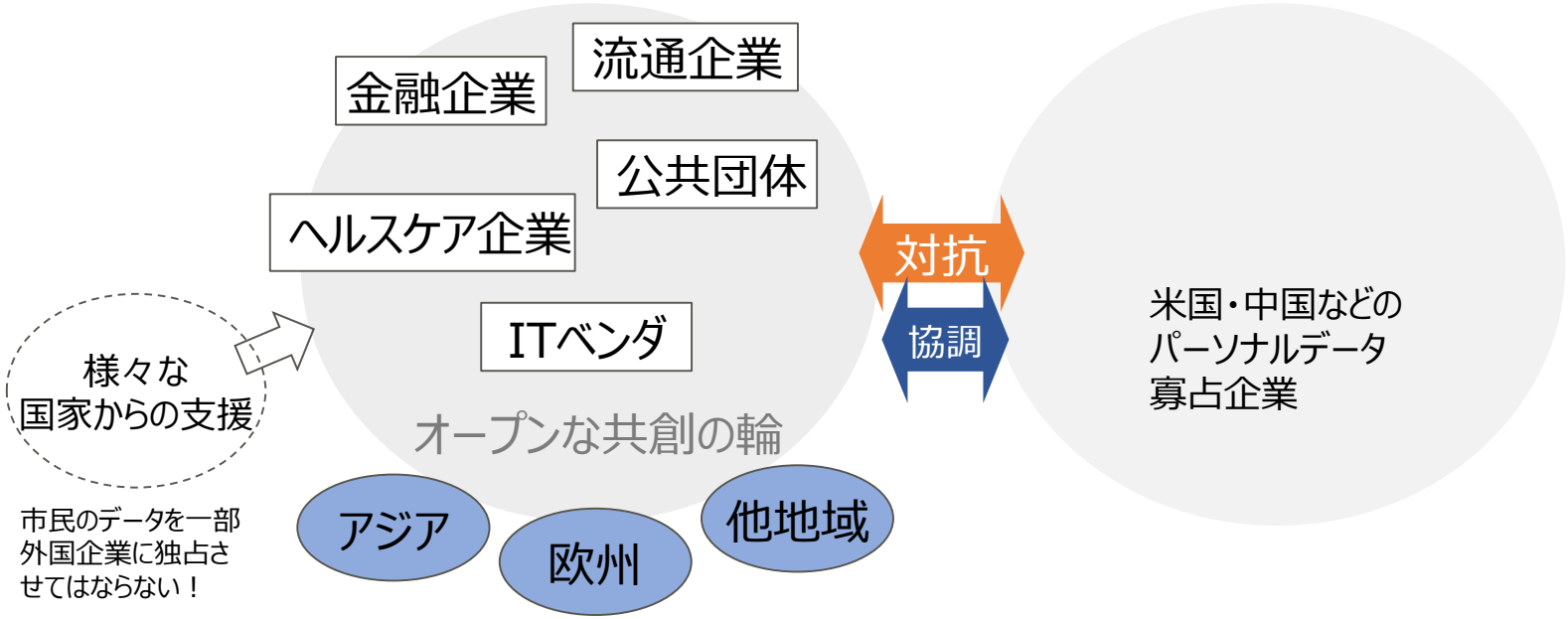
現状では、地域・領域などを絞って狭く濃く価値を出すしかなく、バラバラの小さな取り組みになりがち。

しかし個別の小さなPJをいくらやっても、点の確保にしかならず右図のような面的価値提供には至らない。

解決の方向性：オープンな企業連合体形成

Personium
An open source Personal Data Store

- Open Personal Data Exchange Alliance（仮称）
  - Personium推進のための国際コンソーシアム（案）
  - 様々な業種・地域のPersoniumベースPDS提供事業者の連合体
  - 業種横断の連合体として**<u>ネットワーク効果の初期値を得る</u>**



「一部企業によるパーソナルデータ寡占を脅威と感じる」みなで連合体をつくり、
<u>ユーザベースとアプリエコシステムを共有</u>
ネットワーク効果の「初期値」を獲得（最初から1000万人ぐらいとつながるPDSの世界を作る）

Personium コミュニティ

Personium
An open source Personal Data Store

コミュニティ概要

- Slack 上で日本語/英語でPersoniumに関する様々な情報交換をします。
- ある程度の人数が集まり、要望があればオフラインのイベント(Personium Meeting)も企画します。
- 参加者を広く募集しています。

http://personium.io
https://personium-io.slack.com

公開チャンネル - 議論テーマ

デフォルトのチャンネル

- #general, #random – 全参加者共通チャンネル。randomは雑談用。
- #hello_ja – 参加者自己紹介。参加したいチャンネルのリクエストはこちらで。
- #github – Personium開発状況のリアルタイム通知

テーマ別チャンネル

- #general – PDS関連の技術・制度動向など、共通の話題。
- #infra_ja – Personiumサーバー環境の構築、導入上の相互支援
- #docs_ja - Personiumドキュメンテーション
- #appdev_ja - Personiumのアプリ開発

随時、追加チャンネルの要望を承ります！！

参加フォームはこちら↓

https://goo.gl/forms/ODgVX6eMkRDtReLg1

ぜひお気軽にご参加ください！

宣伝：富士通 K5 Personium サービス

Personium
An open source Personal Data Store

もしご関心ありましたら富士通のクラウドサービスをぜひお使いください！

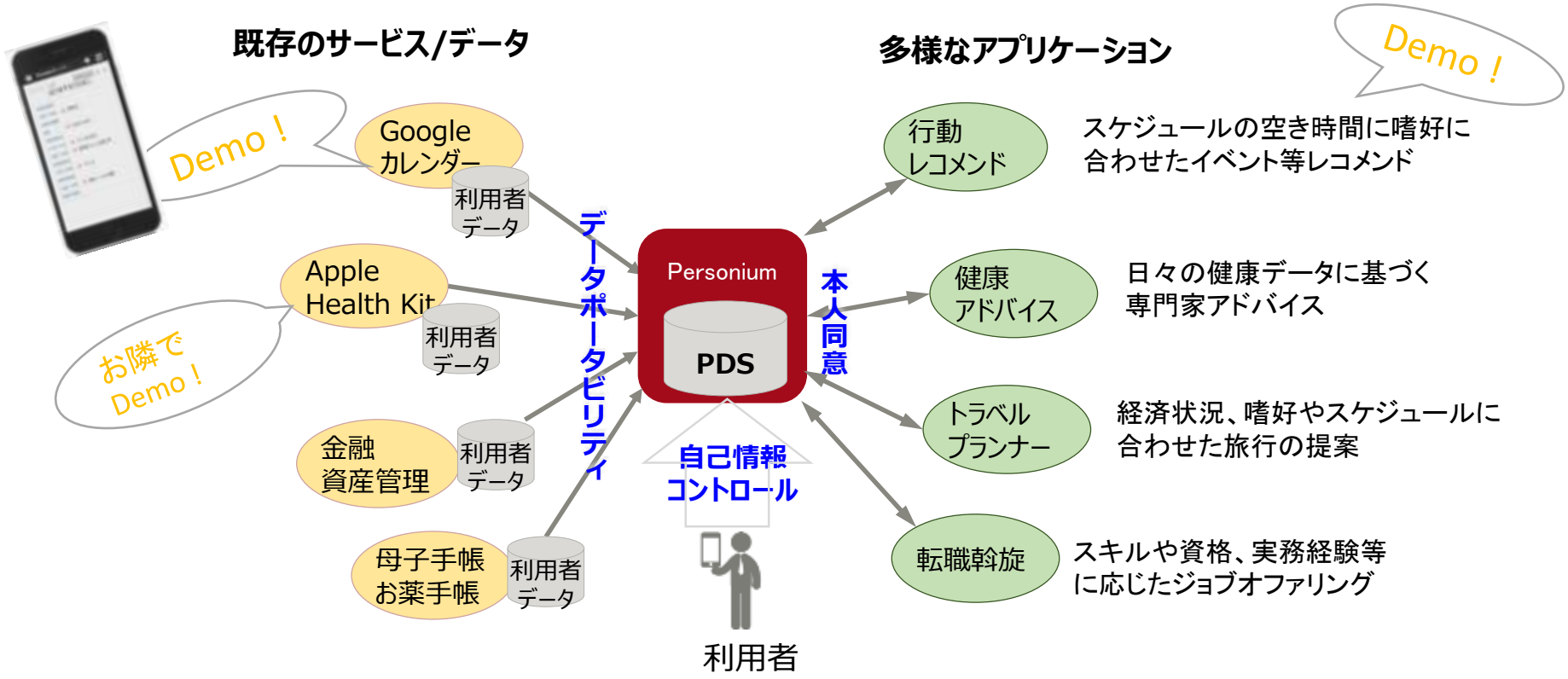
Sサイズユニット月額約10万円
300GBのデータ領域と
24/365運用ついてます。
（だいたい1000名程度の実証実験等に
お使いいただく想定。）

ISO27001/27017取得済
PCI-DSS対応予定（年内）

外でブースを出しています！

Personium
An open source Personal Data Store

- 今お見せしたデモを実際に見て、さわっていただけます。
- （弊社別部署から）ドライブレコーダと連携したデモなども出しています。
- 会津大学さんのPersoniumを使った研究のブースも是非ご覧ください！

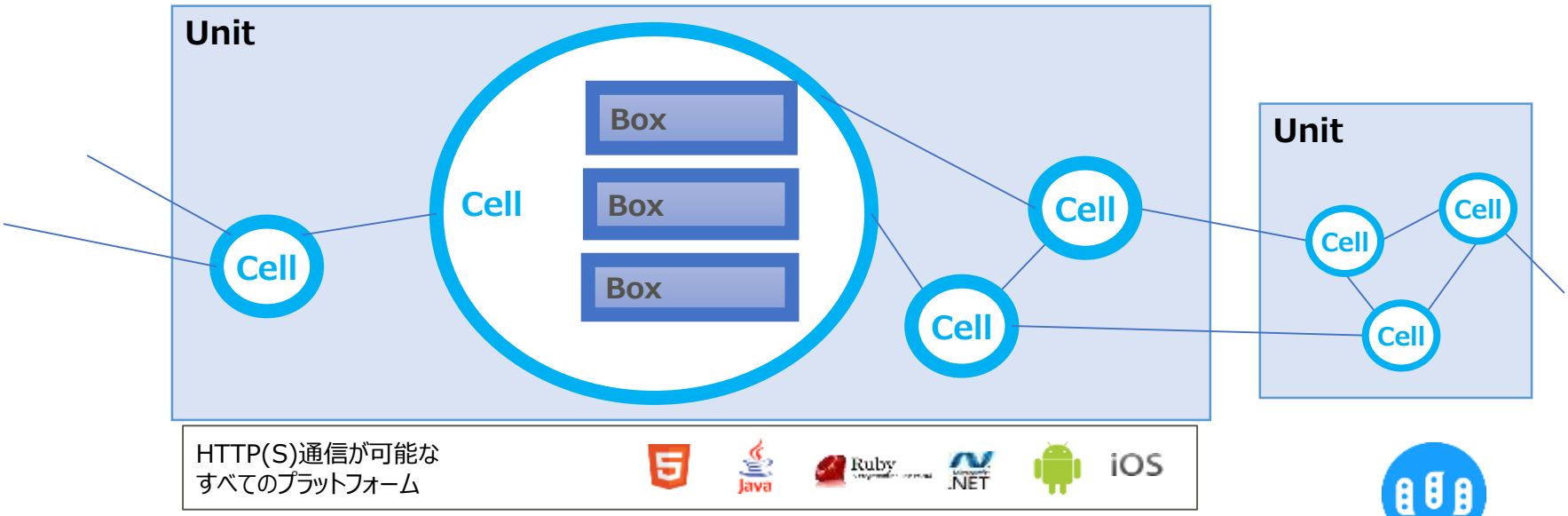


Personium

An open source Personal Data Store

3レイヤーのモデル：Unit/Cell/Box

名称	説明	Typical URL
Unit	Cell群をホストするサーバ。インストールで得られるもの。	https://pds.example/
Cell	PDS。人・モノ・組織のためのデータストア	https://pds.example/akio.shimono/
Box	Cell内のアプリ毎の空間	https://pds.example/akio.shimono/schedule/

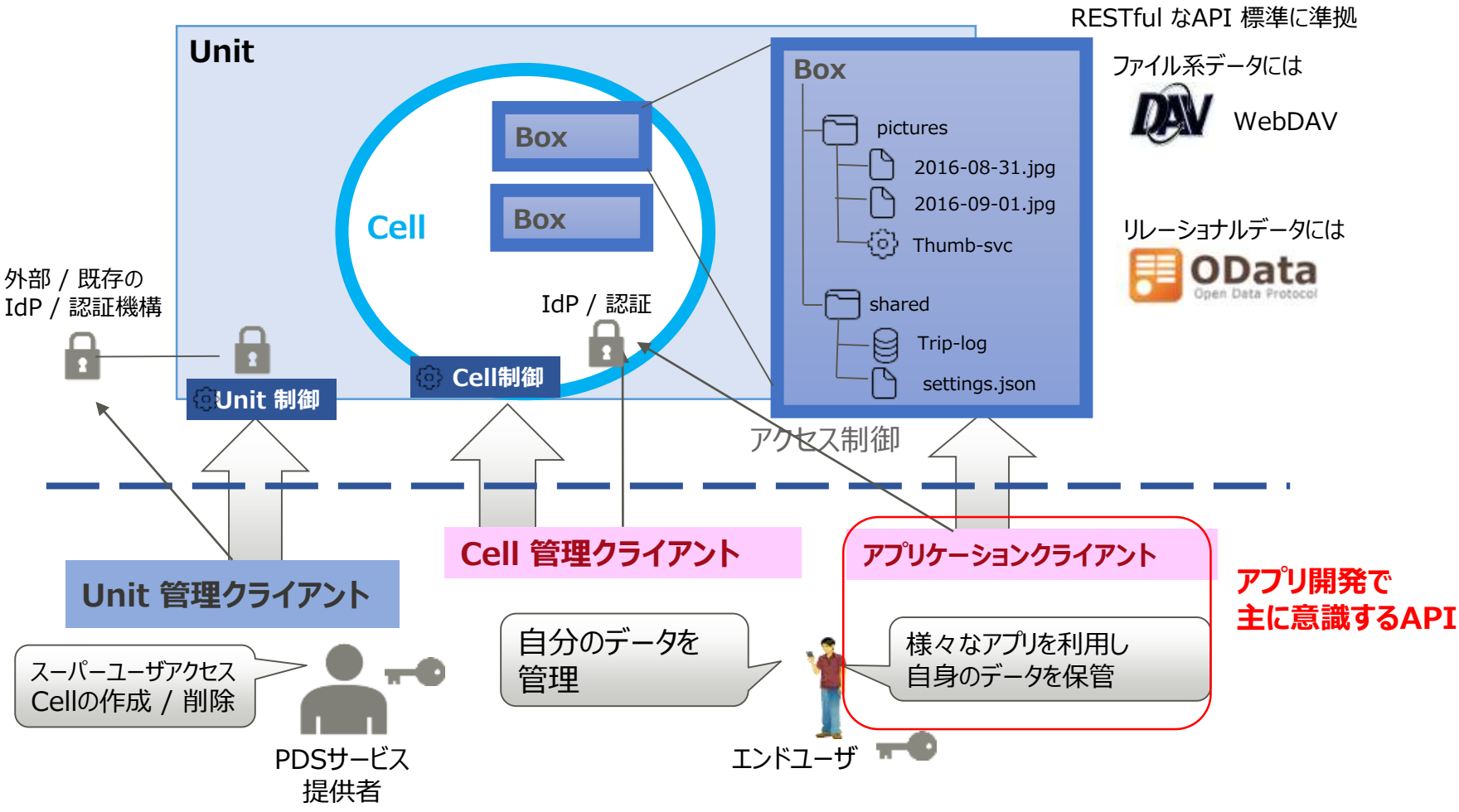


- 全機能をREST APIの形式で提供
- **Cell群はUnitを超えてネットワーク可能．（信頼するUnitとの相互連携）**
- **Box** はそれぞれのアプリのための専用の隔離された領域を提供

Mastodonみたいな感じです

レベル別APIとその用途

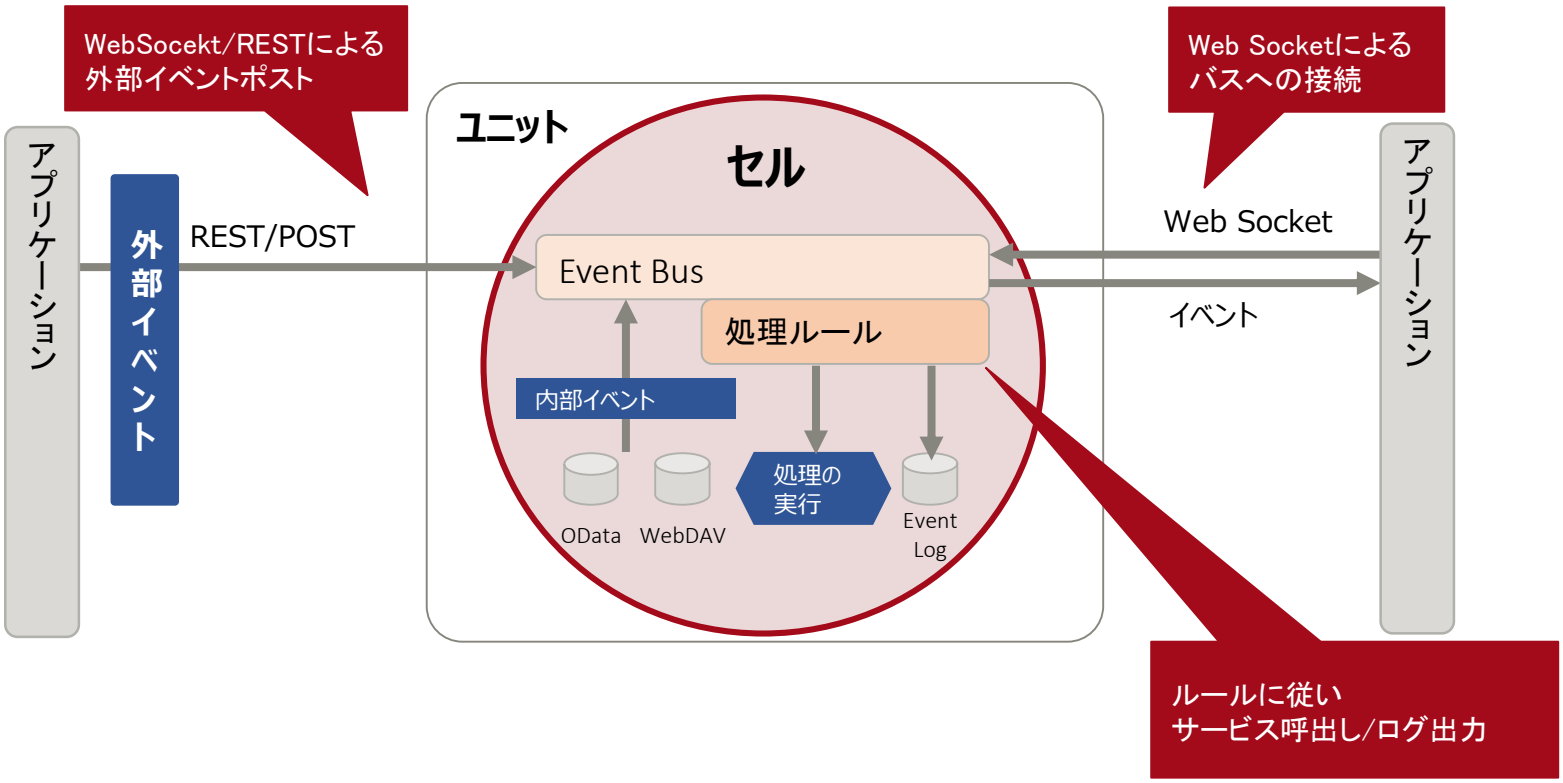
- 全通信はSSLで暗号化。認証・認可・アクセス制御でデータを保護
- 3種類のクライアントがそれぞれ対応する**レベル**のAPIを呼び出す想定



イベント制御（v1.6.xからの新機能）

イベント処理ルールを設定することで、セルに発生する様々なイベントに応じて処理を起動したりログ出力を行うことができます。

- データ操作を始めとする、セルに対するあらゆるAPI呼出は内部イベントとして捕捉可能です。
- クライアント等から外部イベントをポストすることもできます。
- イベントの発生状況をWebSocketで連続的に監視することもできます。



データポータビリティの受け止め方類型

Personium
An open source Personal Data Store

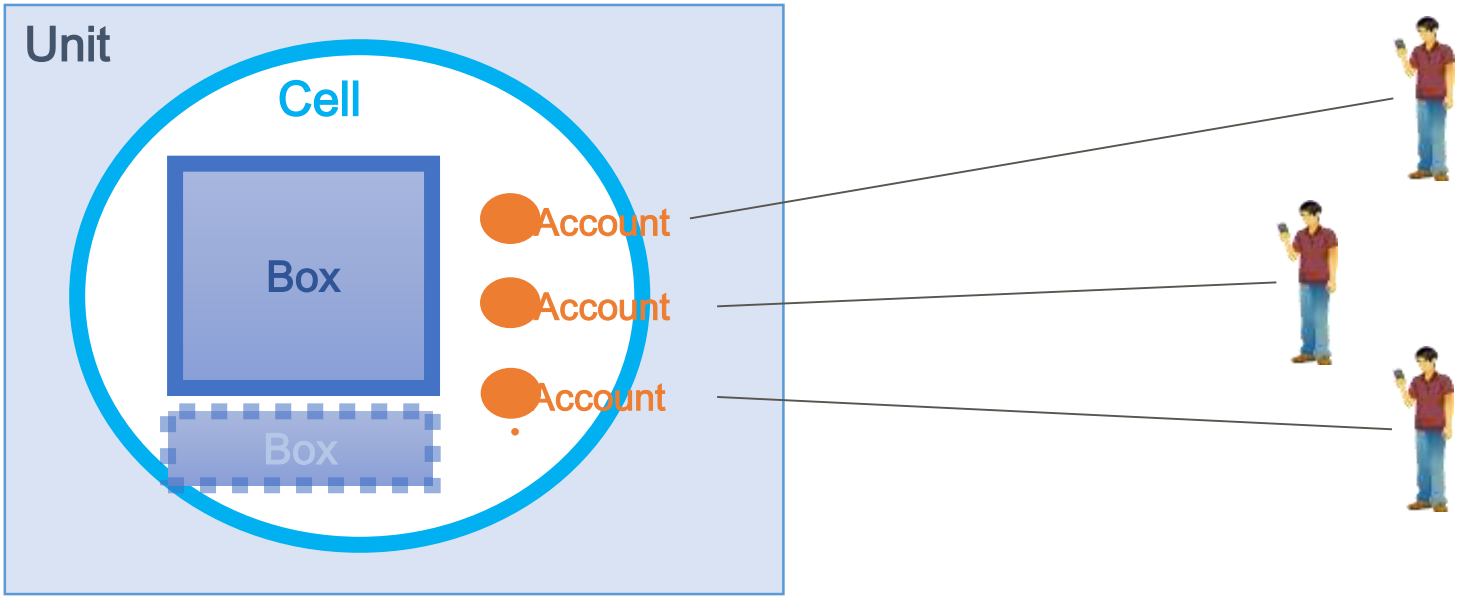
項番	方式	説明	備考
1	OAuth方式	データ連携元のシステムとデータ連携先のシステム間で、OAuth 2.0の プロトコルを用いて、認可を行う仕組み。 セキュリティ：◎ 導入コスト：△	・GitHub ・Google Cloud ・Twitter ・Facebook
2	パーソナルアクセストークン方式	利用者がデータ連携元のシステムで個人のアクセストークンを発行し、 発行したアクセストークンをデータ連携先のシステムに登録することで 認可を行う仕組み。 セキュリティ：〇 導入コスト：〇	・GitHub ・LINE
3	代理認証方式	データ連携先のシステムに対して、利用者の代わりにIDとパスワードを 送信し、認証を行う仕組み。 セキュリティ：△ 導入コスト：△	・Salesforce

Personiumの利用モデル

- 以下、様々な典型的Personium利用モデルをご紹介します。
  - シングルセル
  - 個人向けPDSプロバイダ
  - 簡易情報銀行
  - PDSアプリホスティング
  - コミュニティでのデータ共有
  - スマートシティ：　モノ・コトへの拡張
- Personium利用のパターンは上記モデルのみには閉じませんが、Personiumの使い方を考えていただく一助にしていただくべく、典型的な利用例をお示ししております。

1.シングルセル

■一つのCell、一つのBoxだけを使ってPersoniumを使うモデルです。

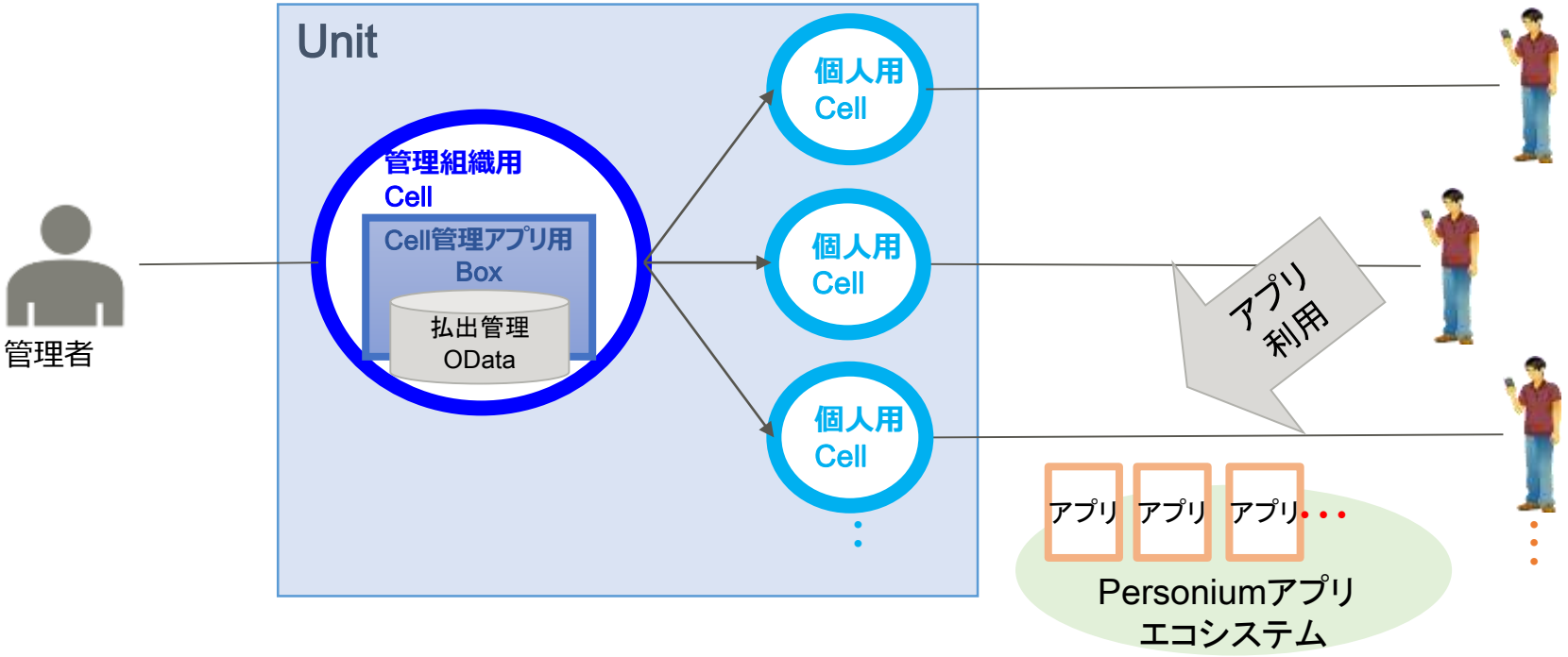


- PersoniumをPDSとしてではなくBaaS(Backend as a Service)として使うモデルです。
- アプリケーションをホストするのであればBoxも一つで問題ありません。
- サーバ側は設定をするのみで開発せずにデータ操作や認証のAPIが利用でき、クライアント側の開発だけで済むため、アプリケーション開発コストを大幅に下げることができます。
- 以降でご紹介するPDSとしての使い方と比べて構成がシンプルであるため、Personiumを使ったアプリ開発に取り組む方は、まずこのモデルを試してみていただくのをお勧めします。

2.個人向け純粋PDSプロバイダ

Personium
An open source Personal Data Store

■ 純粋なPDSプロバイダとして個人用セルを個人に払出して管理するモデル

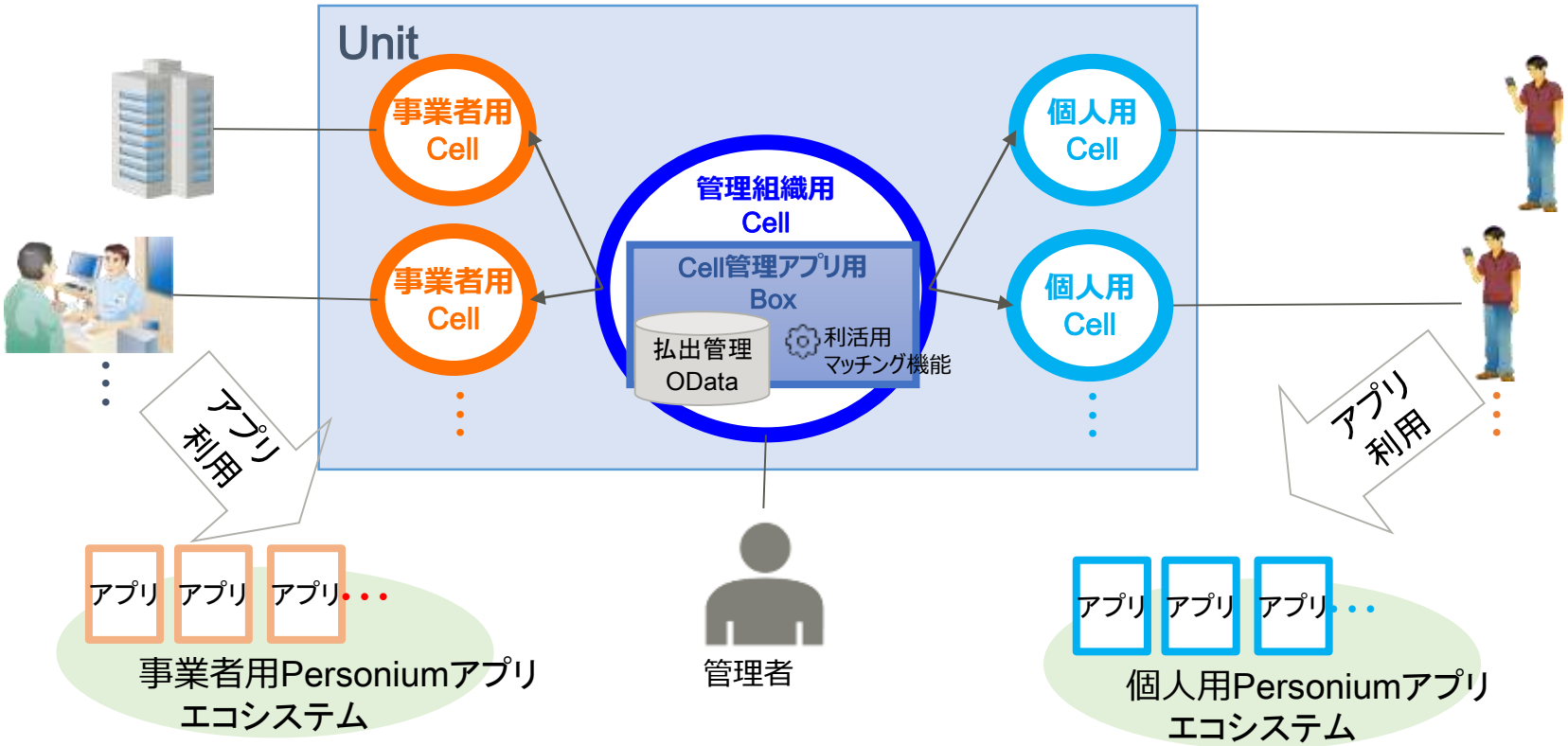


- PDS(個人用Cell)を払出して管理するというPDSプロバイダとしての最低限の業務を行うためのモデルです。
- PDSにデータを読み書きするアプリをどう提供するかという観点はこのモデルには含まれていません。
  - 利用者にオープンエコシステムを案内するか、後述モデルと組み合わせて用意する必要があります。
- 管理者は管理組織用Cellのアカウントで管理組織用Cellにログインして、Cell管理アプリを使ってCell管理業務を行います。
  - Cell管理アプリの作り方次第で様々な要件に対応可能です。
    - 新規利用者からの申込みをWeb画面で受け付けて次々にPDS(個人用Cell)を払い出す
    - 既存顧客管理DBと連携して自動でPDSを払い出す
    - 管理者が手動でPDSを払い出す。
  - Cell管理アプリのサンプルはオープンソース公開されていますので、これをそのまま使ったりカスタマイズして使うことができます。

3.簡易情報銀行

Personium
An open source Personal Data Store

■ PDSに加えて事業者用にもCellを払出して管理するモデル

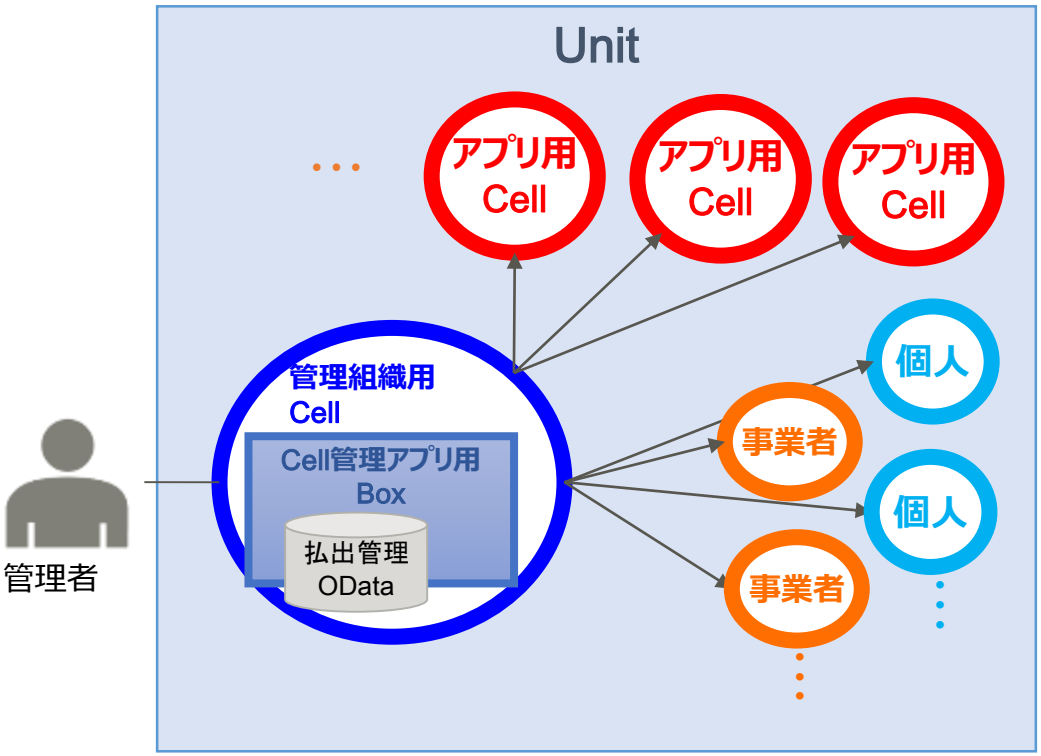


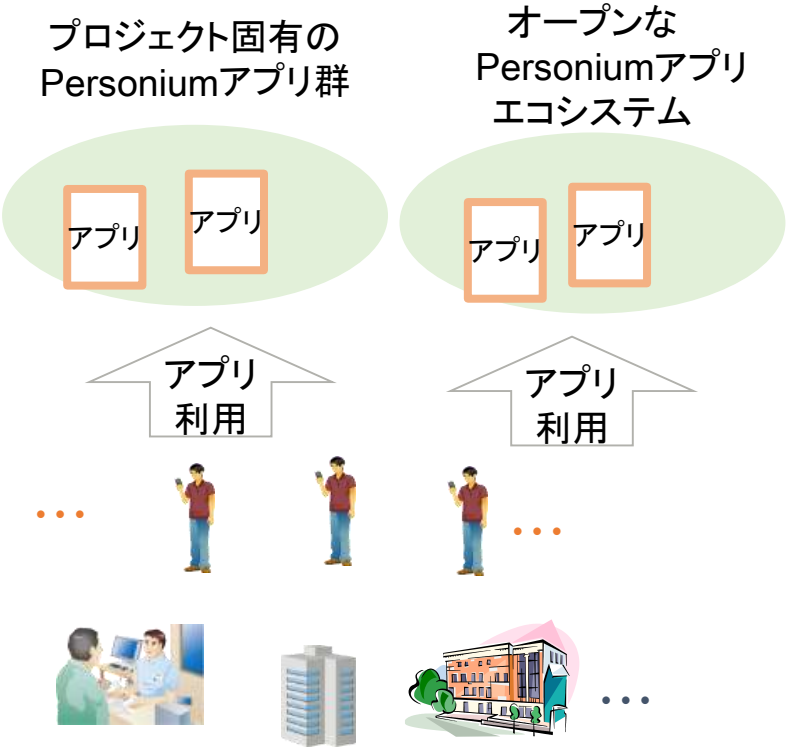
- PDS(個人用Cell)に加えて事業者用Cellも払出して管理するというPDSプロバイダとしての業務を行うためのモデルです。
- アプリをどう提供するかという観点はこのモデルには含まれていません。
  - 個人が使う個人向けのアプリケーション
  - 事業者が使う事業者向けのアプリケーション

  ⇒ アプリのオープンエコシステムを案内するか、後述モデルと組み合わせて用意する必要があります。
- 組織管理用Cellでデータを持つ個人とそれを利活用したい事業者のマッチング機構は含まれていません。
  - オープンエコシステムを案内するか、後述モデルと組み合わせて用意する必要があります。

4.アプリ提供

■ アプリ開発事業者用にもCellを払出して管理する。





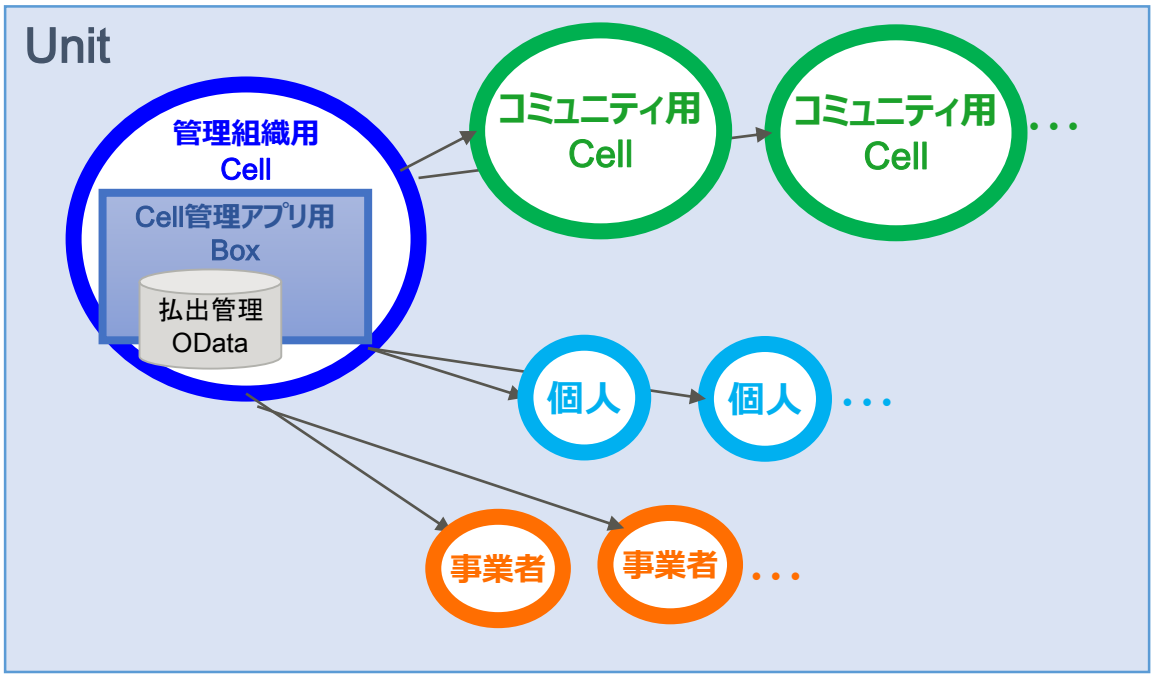
■ さらにアプリ開発者（事業者）に向けてアプリ用Cellも払出して管理するモデルです。

■ 様々なアプリの形態を実現可能です。

- 既存システムのデータをPDSに連携
- ウェアラブルセンサーのデータをPDSに格納

5.コミュニティ

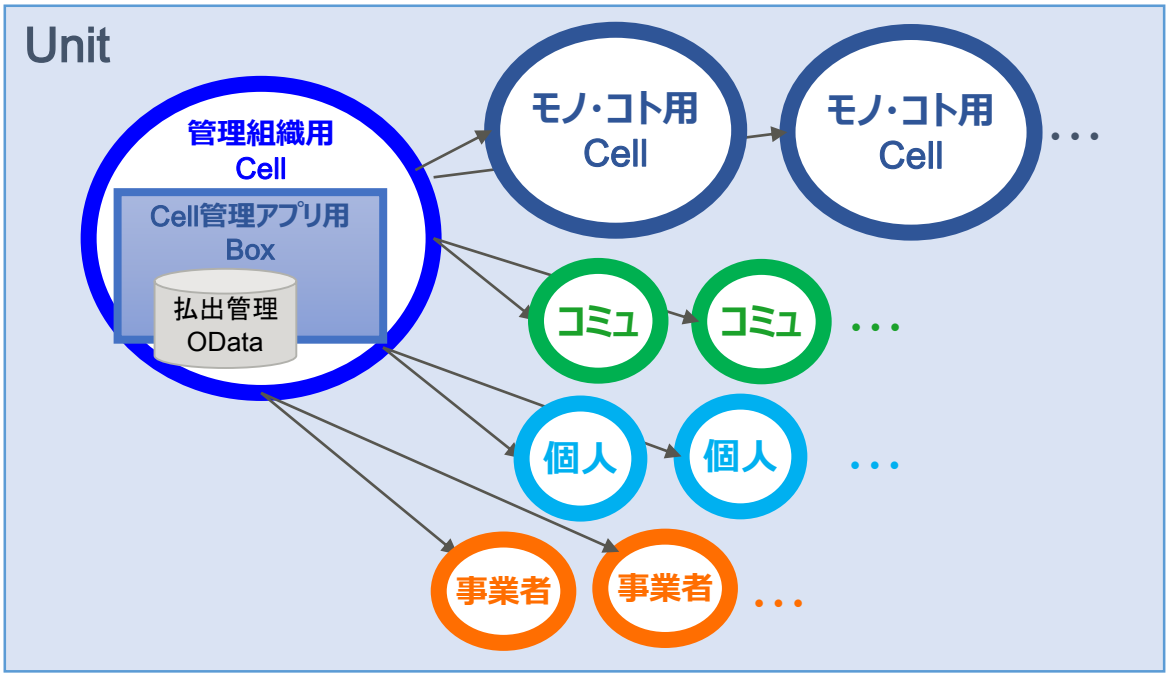
■ 利用者（個人・事業者）からの依頼に基づき自発的コミュニティにもCellを払出す。



- 家族、趣味の集まり、技術コミュニティ、オープンイノベーションプロジェクトなど、データの共有保持を行いたいコミュニティはなにも事業者に限られません。
- これら任意コミュニティに対してもCellを発行して個人や事業者と「参加」という関係で結ぶことで、例えば以下のような使い方が可能です。
  - コミュニティ参加者の中でのプライベートなデータ共有、
  - 書き込みはメンバにのみ許可しつつ成果データはオープンデータとして全公開

6.スマートシティ

■ 利用者（個人・事業者）からの依頼に基づきモノや場所・コト等にもCellを払出す。



- 個人・事業者・コミュニティに加えて、さらにモノやコトに対してもCellを作ってゆくモデルです。
- モノのCellはコミュニティや個人と所有・管理や利用といった関係で接続します。
- むやみにすべてのモノにCellを割り当てると扱いづらいことがあります。
  - 例えばウェアラブル機器など明らかに個人に従属する機器は個人セルにデータを格納するほうがよいでしょう。
  - 複数の個人やコミュニティで共有的に使われるモノであり、そのモノを主体とするデータが生成され管理したいケースで有効です。

ご参考：特許状況

Personium
An open source Personal Data Store

Personium サーバ本体機能に関する私たちからの特許出願状況 (2018年5月現在)

登録/公開番号	名称	概要	出願日	日本	米国	欧州	中国	実装状況
PDS系技術								
特許5445692	情報処理装置およびプログラム	PDSにアクセスするときに、アプリが自アプリ用領域を取得する方法	20101210	登録	登録	出願	登録	実装済
特許5799855	サービス提供方法、プログラム、および情報処理装置	他者が自PDSにアクセスする際に、関係に基づきロールを発行	20120302	登録	登録	出願		実装済
特許5845973	サービス利用管理方法、プログラム、および情報処理装置	間接的関係しか持たない他者が自PDSにアクセスする際、関係距離に基づいてアクセス制御を行う方式	20120301	登録	登録	出願		
特許6065903	保存領域管理方法及びサーバ装置	PHRにおいて、システムに登録済みかどうかの検索を行わず登録を実施し、同じユーザであると申告があってからデータの名寄せを実施する仕組み。	20120319	登録	出願			
特許6044299	データ参照システムおよびアプリケーション認証方法	PDSのアプリ用領域にアクセスするためアプリ認証を行う際、悪意のあるPDS運用者に鍵を渡さない方式	20121126	登録	出願			実装済
特許6311214	アプリケーション認証プログラム、認証サーバ、端末およびアプリケーション認証方法	PDSにアプリが初めてアクセスする際などに用いるOAuth2等による動的な認可取得時の方法	20130130	登録	出願		登録	実装済
特許6103069	アプリデータ記憶領域生成方法，アプリデータ記憶領域生成装置，及びアプリデータ記憶領域生成プログラム	アプリ用データ領域生成時にアプリ定義ロールとアクセス制御情報も合わせて定義体で配布する方法。	20130926	登録	出願			実装済
特許6288241	サービス提供方法、サービス提供装置、及び、サービス提供プログラム	アクセスを許可された他者PDSの領域をあたかも自分の領域のように使えるよう方式。マウント的機能	20140224	登録	出願			
特開2016-0359846	サービス提供方法、サービス要求方法、情報処理装置、及び、クライアント装置	保護されたVIDEOやAUDIOなどをブラウザアプリで扱う場合Cookieでのアクセス制御が便利だが、クロスオリジン的なアクセスが前提になるPDSアプリではCSRFの脅威がある。この問題を解決する方法。	20140217	出願	出願			実装済
BaaS系技術								
特許6136694	データ管理プログラム、データ管理装置およびデータ管理方法	テーブル上データで、スキーマレス項目を扱うさい、のちにデータ移行を伴わずに正式にスキーマ定義項目に昇格させる方法。	20130719	登録	出願		出願	実装済

えっ！
使って大丈夫なの？

もちろんです！

Personium はApacheライセンス v2.0なので、
利用にあたってこれら特許は自動的にライセンスされます

Personium