資料１-４

Data Platform Consortium

第３回スーパーシティ／スマートシティにおけるデータ連携等に関する検討会　資料

# スーパーシティにおける共通サービスとしてのプライバシー保護の仕組みの実装について

2020年12月17日

一般社団法人　官民データ活用共通プラットフォーム協議会（DPC）

代表理事　奥井規晶

資料１-４

# プライバシー保護の原則とPIAについて

**スーパーシティにプライバシー保護の原則やPIAを実装するには、クラウド上に「共通サービス」として実装（API連携）するだけでなく、住民の手間を省く仕組みや住民UIの実装が重要となる。**

## 大原則：プライバシー保護の原則（森委員）

1. 当事者の原則（PF（都市OS）が当事者を仲介）
2. 同意取得の原則（オプトイン/アウト）
3. 提供制限の原則（利用者に一定の資格）
4. 再提供制限の原則（勝手に再提供できない）
5. パーソナルデータの原則（対象範囲の定義）
6. 透明性の原則（どう使われているかがわかる）
7. 本人関与の原則（開示/訂正/削除を求められる）

## サービス提供者のPIA（プライバシー影響評価）（坂下委員）

- 取得/利用/保管/廃棄プロセス
- 2017年ISO/IEC29134国際標準化
- 2021年1月JISX9251企画化予定
- サービス提供者が評価計画/PIA実施/結果の的/公表
- 国内事例マイナンバーの「情報提供等記録開示システム」
- 将来的にはアイデンティティ・プロバイダー（情報空間上の代理人）への信託
- 類似の仕組みに「情報銀行」がある

## 実装の要件

① スーパーシティの「共通サービス」としてクラウド実装、サービスや都市OSとはAPI連携、都市OSの内外は問わない

② 住民の手間を省く仕組み

③ スマホやPCを使えない住民を救うUI

## 個人にとって

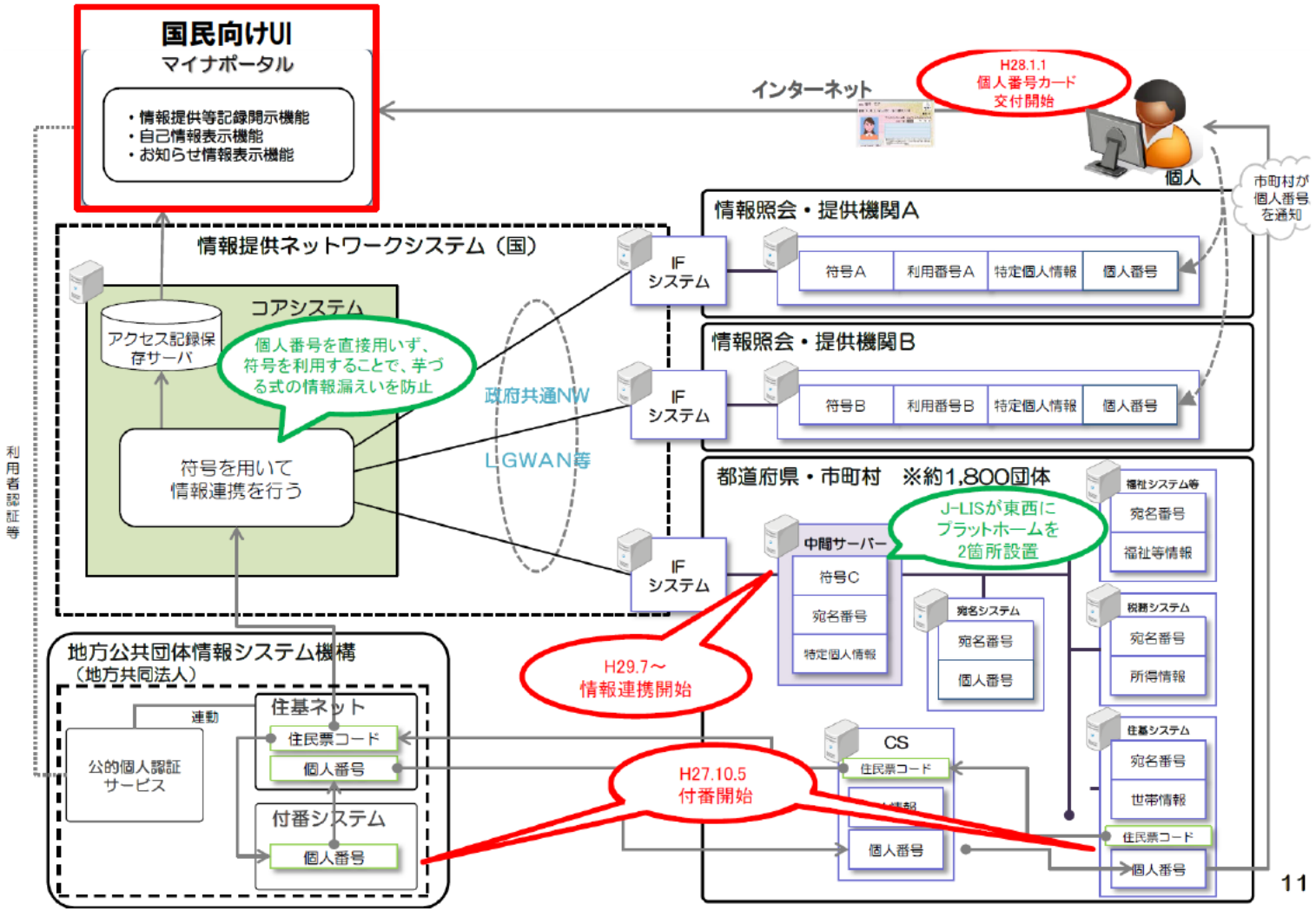
- 自分のどの情報を誰が使ってよいか、悪いかを判断できる（オプトイン/アウト、PIAや資格が参考になる）
- 自分のどの情報がどこで、どのように、どれだけ使われているか、自分で調べられる
- 自分の情報を訂正/削除できる

# ①「共通サービス」としての実装 アーキテクチャ上の位置づけ

**アイデンティティ・プロバイダーはスーパーシティの共通サービスの一部であり、住民がプライバシーに関して同意や確認等が容易にできるUIを備える。**

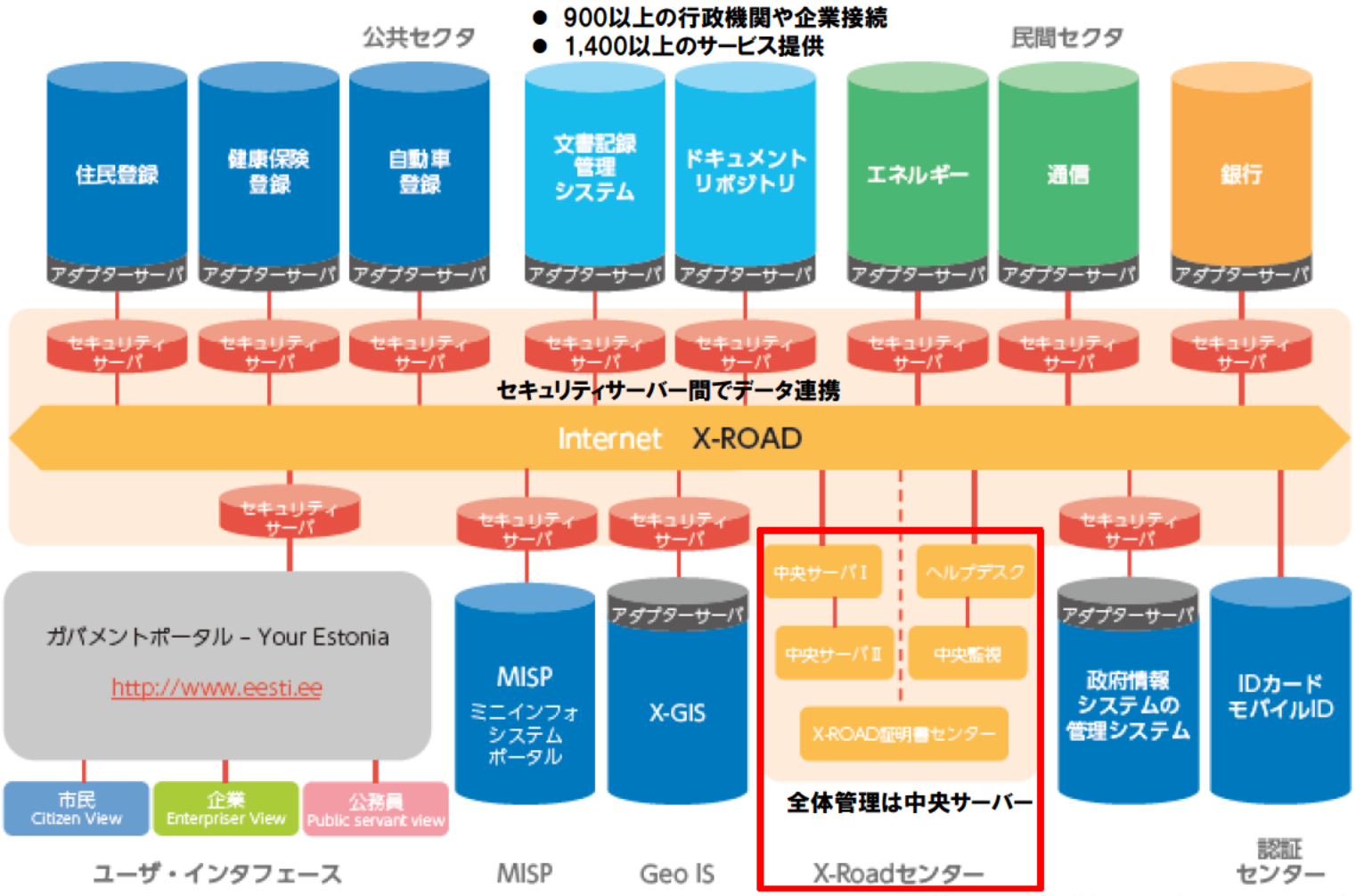
# ①「共通サービス」としての実装
# 実装例：マイナンバー情報提供等記録開示機能

**マイナンバーでは対象情報と利用システムが限定されており、自分の情報がどのように使われたかをマイナポータルで確認できる。**



# ①「共通サービス」としての実装
# 履歴確認の例：エストニアX-ROAD

**エストニアの「X-ROAD」では、全てのサービスをセキュリティサーバー経由とするアーキテクチャで、個人情報の履歴が確認できるようになっている。**




（出典）エストニア国家情報システム庁ホームページより作成

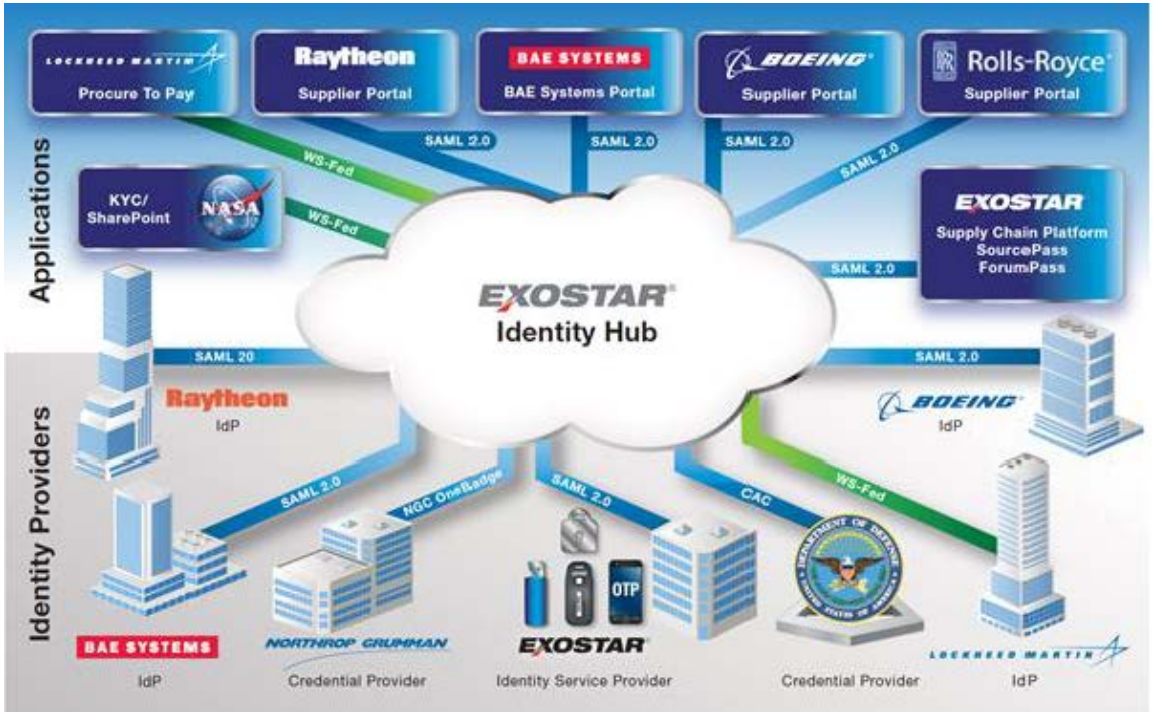
出所：平成27年情報通信白書

# ①「共通サービス」としての実装
# アイデンティティ・プロバイダーの例：米航空防衛業界EXOSTAR（機密情報）

**米国航空防衛業界では、ロッキード等主要5社が2000年に設立したEXOSTAR社がMAG（Managed Access Gateway for Aerospace and Defense）サービスを提供。業界共通の「アイデンティティ認証」を行い、各社の提供するアプリケーションへの入口をIdentity Hubによって制御。アイデンティティ・プロバイダーの概念が実装されている。**

**この他にバイオ医薬品等産業向け の SAM（Secure Access Manager）、商用航空宇宙産業向け の DAF（Digital Aviation Federation ）**

サプライチェーン内のトラストグループによるアプリケーション群




トラスグループ：特定の運用ポリシーに沿って事業を行うこと了承した上で 協業するメンバー企業から構成されたグループ

SAMLやWS-Fedのようなプロトコルを使用

**アイデンティティプロバイダー**

Identity Provider：
IDP、 MAG を介してユーザが他のウェブサイトをアクセスできる環境を提供する事業者

ISP：
Identity Service Provider、IDP以外のユーザにクレデンシャ ルを発行するIDaaSサービス事業者（Exostar社）

CP：
Credential Provider、各種クレデンシャルを発行する事業者

出所：https://www.evaaviation.com/wp/wp-content/uploads/2017/02/EW03-20150800-PKI JP USV02.pdf

# ①「共通サービス」としての実装
## ロールモデルの例：RAMI4.0/IDSのビジネス層（産業データ）

**インダストリー4.0のリファレンスアーキテクチャ（RAMI4.0）に基づくIDS（Industrial Data Space）のビジネス層は、データ所有者からデータ利用者までの流れをオブジェクト指向のモジュール構造で定義している。データ所有者/データ提供者/サービス提供者/ブローカー/データ消費者/データ利用者といったロールモデルが参考となりそう。**

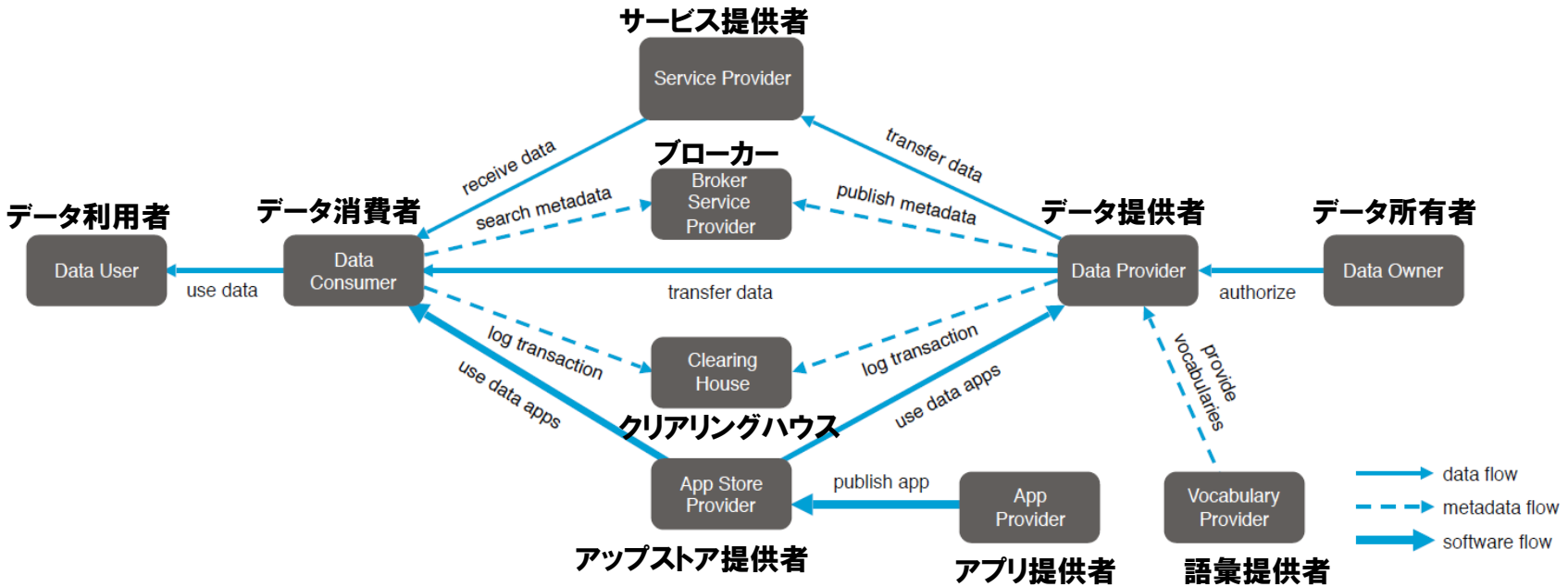
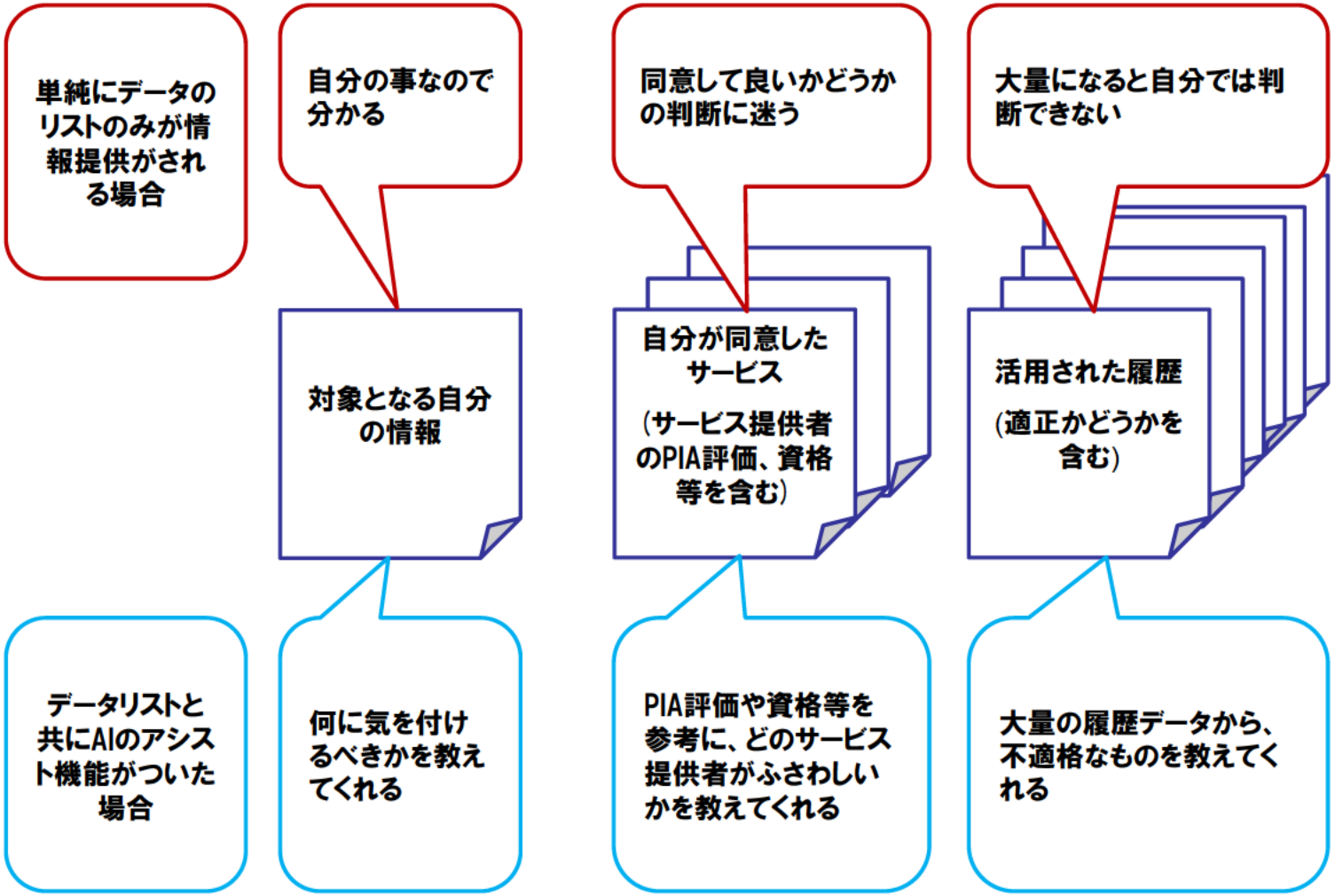



Figure 3.1: Roles and interactions in the Industrial Data Space

出所：https://www.fraunhofer.de/content/dam/zv/de/Forschungsfelder/industrial-data-space/IDS_Referenz_Architecture.pdf

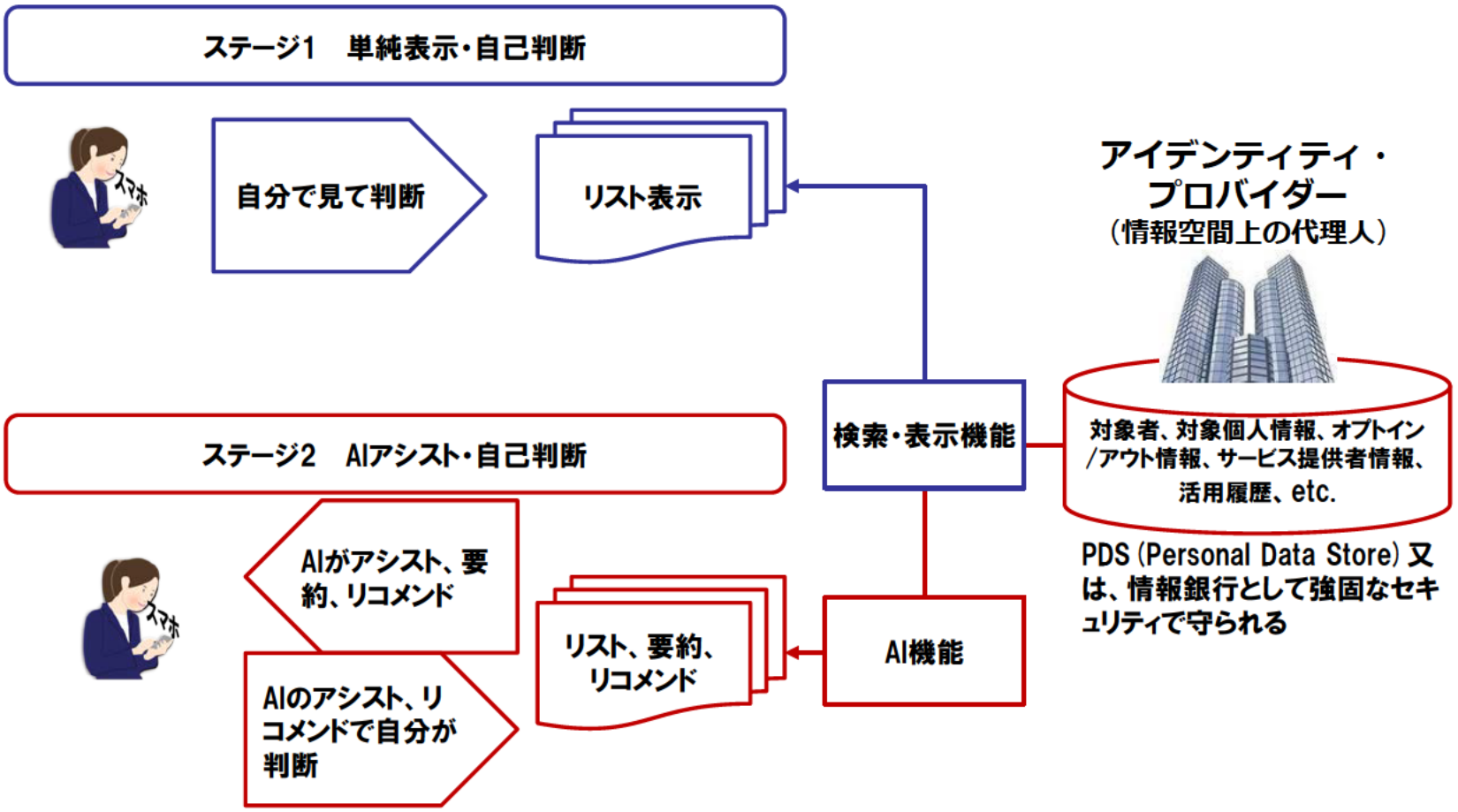
# ②住民の手間を省く仕組み
# あるべき姿

**アイデンティティ・プロバイダーを実装する場合、住民側にも膨大な手間が要求されるため、手間を軽減するためのAIが必要となる。**



# ②住民の手間を省く仕組み
# 実装イメージ

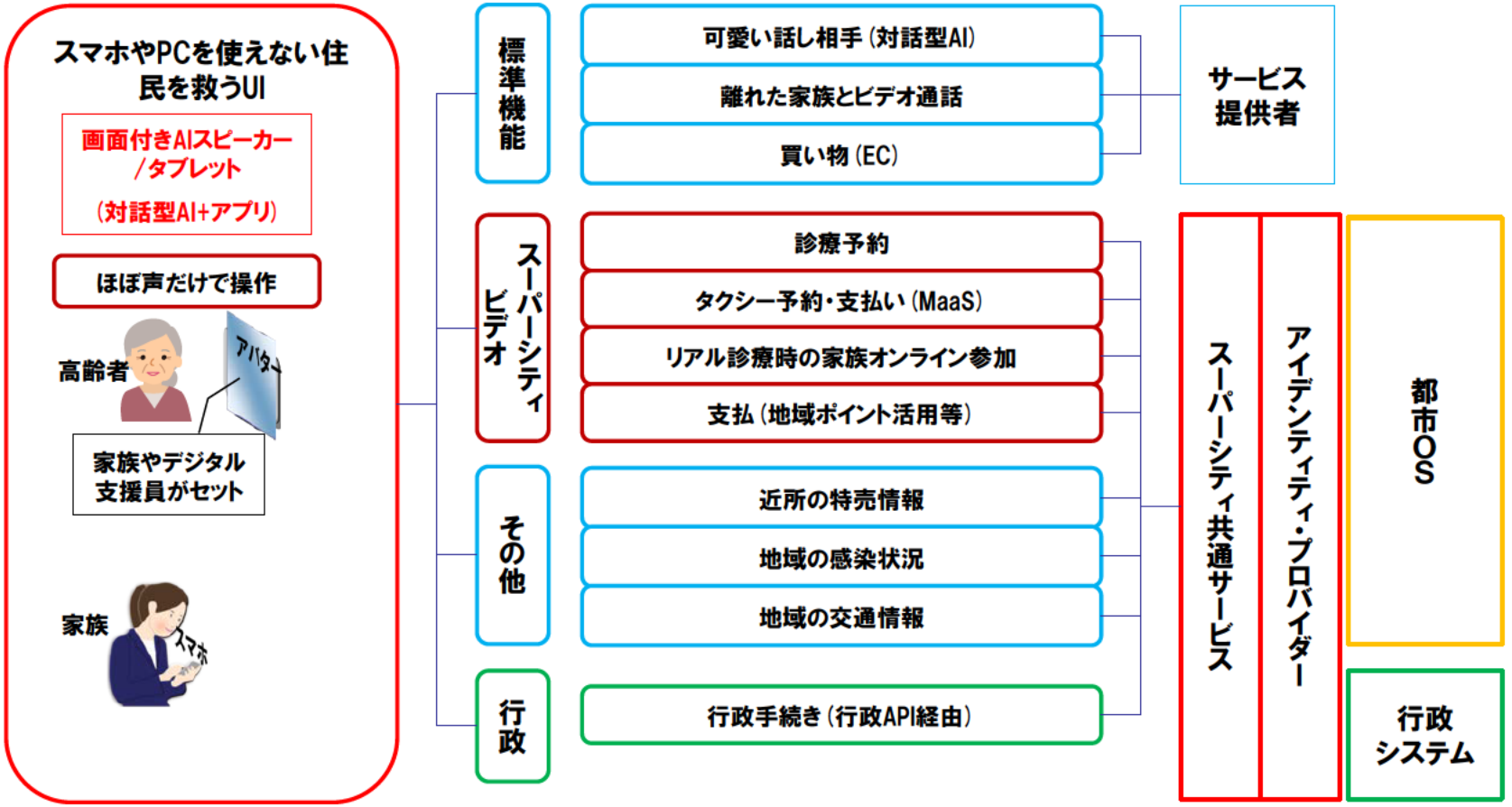
**住民側の手間を省くための機能は、強固なセキュリティに守られたアイデンティティ・プロバイダーに人工知能（AI）を適用し、単なるリスト表示に対して、要約、アシスト、リコメンドの機能を持たせることになる。**



# ③スマホやPCを使えない住民を救うUI あるべき姿

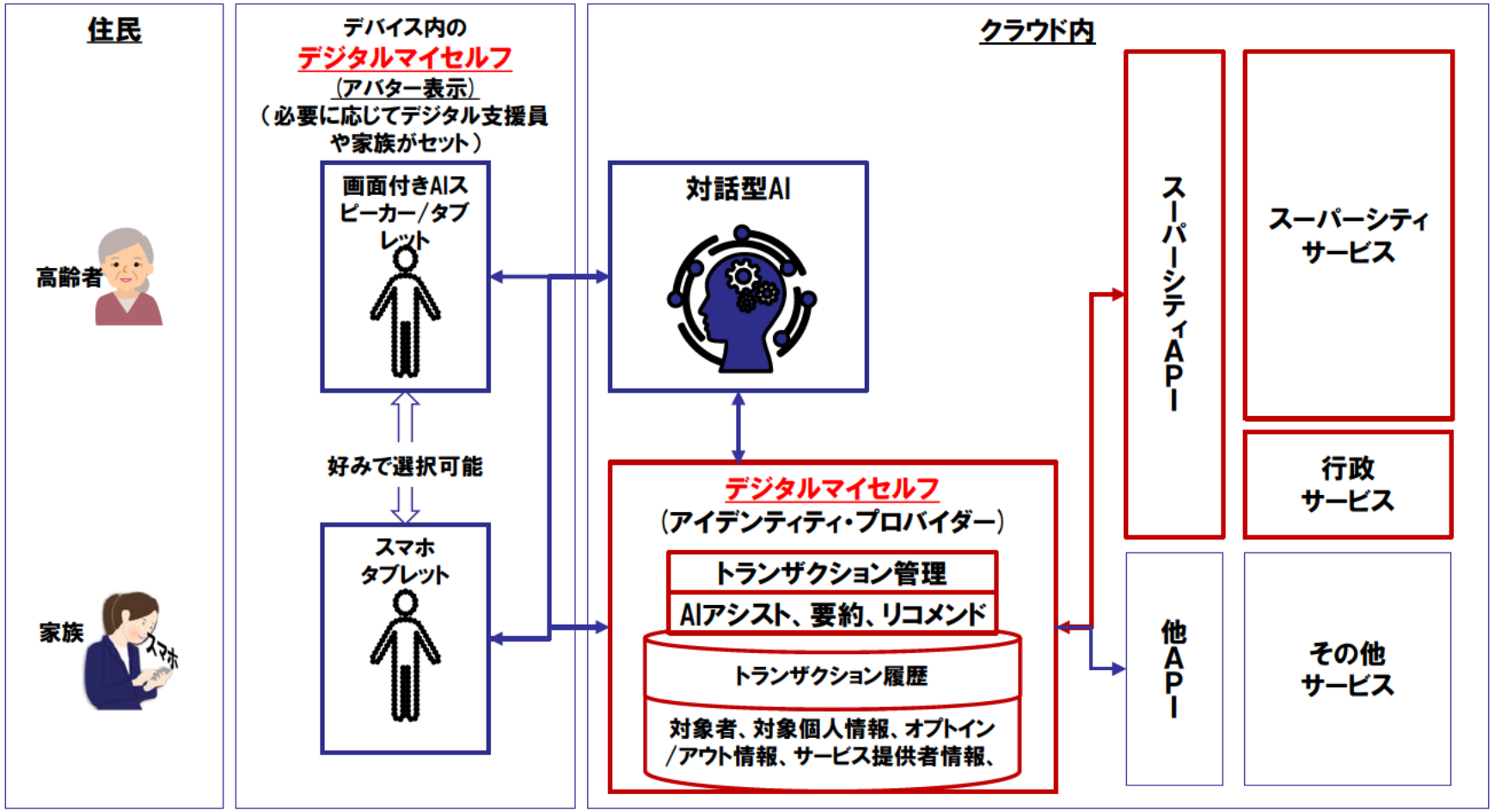
**スマホやPCを使えない住民を救うUIとして、現在最も近いのは、画面付きAIスピーカー/タブレット（対話型AI+アプリ）で、**

## 各種サービスの例



# ③スマホやPCを使えない住民を救うUI
# デジタルツインとしてのデジタルマイセルフの実装

**人工知能の進化を考えると、スマホやPCを使えない住民を救うUIは画面上のアバターとクラウド内の「デジタルマイセルフ」となっていく。デジタルマイセルフは、アイデンティティ・プロバイダーの役割を持つ。**



資料１-４

Data
Platform
Consortium

# 一般社団法人 官民データ活用共通プラットフォーム協議会

（略称:DPC）

（事務局）
〒108-0073 東京都港区三田3-12-16山光ビル
株式会社インターフュージョン・コンサルティング内
TEL03-5419-7171 Fax03-5419-0597
メール：jimukyoku@dpc-japan.org
ホームページ: https://dpc-japan.org