

# 生活用データ連携に関する機能等に係る調査研究

## 調査報告書

2022年3月31日  
日本電気株式会社

### [概要]

プロジェクト名称	生活用データ連携に関する機能等に係る調査研究
実施事項	欧州におけるインターオペラビリティを実現したデータ交換基盤の調査 ステップ 1. 技術基準の定義 ステップ 2. 公認モジュールの決定 ステップ 3. モジュールの継続的な運用の定義

# 目次

1. 業務概要	3
1-1. 生活用データ連携に関する機能等に係る調査研究の概要	3
1-2. 生活用データ連携基盤の位置づけ	4
1-3. 参考文献	8
2. 業務実施結果 ステップ1：技術基準の定義	9
2-1. データ連携基盤の機能群の定義	9
2-1-1. ビルディングブロックの必要性	9
2-1-2. ユースケースから見る生活用データ連携基盤に必要なビルディングブロック	9
2-1-3. 基盤の定義	14
2-2. 相互運用性を確保するための基準	15
2-2-1. APIの公開	15
2-2-2. API利用規約	17
2-2-3. データモデル	19
3. 業務実施結果 ステップ2：公認モジュールの決定	21
3-1. APIゲートウェイが満たすべき要件	21
3-2. ブローカー（非パーソナル）が満たすべき要件	22
3-3. ブローカー（パーソナル）が満たすべき要件	23
3-3-1. ステークホルダーリスト	23
3-3-2. トラスト関係	24
3-3-3. ユースケース整理	24
3-3-4. パーソナルデータ流通に必要な要件	30
3-3-5. 妥当性検証	41
3-4. 各ビルディングブロックの調査	46
3-4-1. 調査方針	46
3-4-2. 各ブロックの調査結果	46
3-5. 公開方法	58
4. 業務実施結果 ステップ3：モジュールの継続的な運用の定義	59
4-1. サポートサービスの定義	59
4-1-1. 先進事例の調査結果	59
4-1-2. サービス内容の定義	65
4-1-3. 運用方法の具体化	67
4-2. 組織体制の定義	70
4-2-1. 実行体制の定義	70
4-2-2. 事業計画の定義	71
5. まとめ	74

## 1. 業務概要

### 1-1. 生活用データ連携に関する機能等に係る調査研究の概要

#### (1) 生活用データ連携に関する機能等に係る調査研究の背景

DX（デジタル・トランスフォーメーション）の取組みの進展に伴い、データは「21 世紀の石油」とも呼ばれるようになり、ビジネスにおいて極めて重要なものと位置づけられている。近年は、第 4 次産業革命と呼ばれる AI 及びビッグデータを活用し、社会の在り方を根本から変えられるような都市設計の動きが急速に進展している。我が国においても、国民がデジタルを活用したより良いサービスを楽しみ、成長を実感できるためには、国を構成する「国民」「社会」「産業」「自治体」「政府」といった主体・分野にまたがる本質的な構造改革が必要となる。その早期実現のため「デジタル田園都市国家構想実現会議」等が開催され、革新的な暮らしやすさを実現するデジタル田園都市国家構想の実現に向けた方針が提示された。政府は、その実現に向け、国・地方が一体となった包括的な設計を具現化した「デジタル基盤」として、「サービス・アプローチ」「公共サービス基盤」「デジタル・インフラ」の整備を進めるとしている。このうち、いわゆる競争領域に属する「サービス・アプローチ」と、公共インフラとしての性格を持つ「デジタル・インフラ」の間に位置付けられる「公共サービス基盤」については、いわゆるシェアードエコノミーを実現するような協調領域として位置づけられているが、このレイヤーに関する技術要件や整備・運用の主体について、今後政府が、「部品やアーキテクチャを提供する」<sup>1</sup>ことが提言されている点に基づき各地域に実装を進める必要がある。

#### (2) 生活用データ連携に関する機能等に係る調査研究の目的

政府が行う「デジタル基盤の整備」を「ソフトウェアモジュール群の公開と継続的な運用」と定義する。具体的には、「公共サービス基盤」として定義される機能について、共通の機能とするモジュールはオープンな形式で公開、「政府公認のモジュール（以下、公認モジュールとする）」とし、これを各地域が共通的に活用できる運用とすることを本調査研究の基本方針・目的とする。なお、「公共サービス基盤」の位置づけについては、「1-2. 生活用データ連携基盤の位置づけ」にて述べる。

#### (3) 課題と調査内容の全体像

現在、公共サービス基盤の共通の機能として、必要となる機能群（以下、ビルディングブロックとする）の選定と各ビルディングブロックが有すべき技術基準は存在しておらず、相互運用性の担保がない公共サービス基盤の乱立を招く可能性がある。このため、ステップ 1 として技術基準の定義を行う。特に相互運用性の確保に向けては、データを API（Application Programming Interface の略称であり、あるサービスやアプリケーションにおいて、その機能や管理するデータ等を他のサービスやアプリケーションから呼び出して利用するための接続仕様等）を通じて相互にやり取りするための API の公開及び API の利用規約についての基準と、静的及び動的を含む様々なデータを扱うためのデータモデルを設計するにあたって順守すべきルールが必要と考えられるため、その内容を述べる。

ステップ 1 で定義した技術基準の定義に沿った形で「共通の機能とするモジュールはオープンな形式で公開」するにあたり、ステップ 2 では公認モジュールが満たすべき要件の検討と公認モジュールの決定、公開方法を述べる。加えて、当該公認モジュールの利用を促進する一助として、モジュールの取り扱いについての説明等を述べる。

また、当該モジュールが継続的に運用されていくためには、モジュールの管理やインセンティブ等、利

---

<sup>1</sup>「デジタル田園都市国家構想関連施策の全体像」令和 3 年 12 月 28 日デジタル田園都市国家構想担当 若宮 健嗣大臣資料 ([https://www.cas.go.jp/jp/seisaku/digital\\_denen/dai2/siryoul-2.pdf](https://www.cas.go.jp/jp/seisaku/digital_denen/dai2/siryoul-2.pdf))

用されるうえで考慮すべき点がある。ステップ3では、CEF Digital<sup>2</sup>やFIWARE Foundation<sup>3</sup>等の取り組みなど、先進事例の調査をもとに、モジュールのサポートサービスの定義、それを支える組織体制について述べる。これらを踏まえた、本調査事業の実施内容の全体像は以下とする（図 1-1-1）。

「生活用データ連携に関する機能等に係る調査研究」実施内容の全体像

本事業の前提となる「国が実施するデジタル基盤の整備」を「ソフトウェアモジュール群の公開と継続的な運用」と定義。本事業ではその整備内容を具現化するため、以下の3ステップで調査を実施。



図 1-1-1 「生活用データ連携に関する機能等に係る調査研究」の実施内容の全体像

## 1-2. 生活用データ連携基盤の位置づけ

本調査事業における生活用データ連携基盤の位置づけについて、デジタル田園都市国家構想実現会議（第1回）の牧島大臣資料<sup>4</sup>からデータ連携基盤の種類と合わせて整理する。

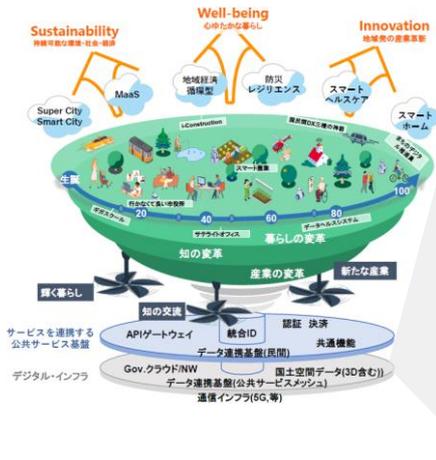
デジタル田園都市国家構想の取組イメージ（図 1-2-1 の左側の図）において、サービスを連携する公共サービス基盤の中にデータ連携基盤（民間）がある。また、サービスを連携する公共サービス基盤と共に協調領域にてデジタル田園都市国家構想を支えるデジタル・インフラとの関連性を確認するため、各デジタル・インフラの概要を図 1-2-1 の右側の表に整理した。

<sup>2</sup> EU が 2011 年に Connecting Europe Facility (CEF) を政策パッケージとして発表。エネルギー・交通・通信のプロジェクト支援が目的。通信分野はその後 Digital 分野も範囲に入れ、補助金やツール・サービスの提供を行っている。

<sup>3</sup> EU の次世代インターネット官民連携プログラム (FI-PPP) で開発・実装された基盤ソフトウェアである「FIWARE」の普及を民間主導で推進する非営利団体。

<sup>4</sup> [https://www.cas.go.jp/jp/seisaku/digital\\_denen/dail/siryoushi.pdf](https://www.cas.go.jp/jp/seisaku/digital_denen/dail/siryoushi.pdf)

データ連携基盤(民間)と関連性のあるデジタル・インフラ



デジタル・インフラ	概要
Gov.クラウド/NW	<ul style="list-style-type: none"> <li>政府の情報システムについて、共通的な基盤・機能を提供する複数のクラウドサービス( IaaS、PaaS、SaaS )の利用環境</li> <li>政府共通の標準的な業務実施環境(パーソナルコンピュータやネットワーク環境)の提供、国の組織を中心として、地方公共団体や民間を含めて統合、相互接続することで、幅広い範囲でサービスを提供</li> </ul>
国土交通データ(3D含む)	<ul style="list-style-type: none"> <li>国土交通データプラットフォームにて、国土に関するデータ、経済活動に関するデータ及び自然現象に関するデータを検索、表示、ダウンロードが可能</li> <li>今後、各種データをAPI連携可能とし、データ連携を順次拡大の予定</li> </ul>
データ連携基盤(公共サービスメッシュ)	<ul style="list-style-type: none"> <li>公共サービスメッシュとは、国や自治体利用する行政ネットワークにて、国税庁やハローワークといった政府機関と地方自治体の情報システムをつなぐ、ガバメントクラウド上に構築されるデータ連携基盤</li> </ul>
通信インフラ(5G等)	<ul style="list-style-type: none"> <li>「第5世代移動通信システム」のことで、「高速大容量」「高信頼・低遅延通信」「多数同時接続」という3つの特徴</li> <li>日本では2020年春から商用サービスがスタート</li> </ul>

図 1-2-1 デジタル田園都市国家構想におけるデータ連携基盤の位置づけ

図 1-2-1 からデータ連携基盤(民間)と関連性のある仕組みとしては、相互にデータ流通することが想定される「データ連携基盤(公共サービスメッシュ)」(以下、公共サービスメッシュと示す)が該当する。

デジタル田園都市国家構想実現会議(第4回)の牧島大臣資料<sup>5</sup>に掲載されている図 1-2-2「公共サービスメッシュの整備(イメージ)」から公共サービスメッシュは、行政ネットワークにて稼働するデータ連携基盤であり、エリア・データ連携基盤がつながることで相互にデータ流通する仕組みである。これを踏まえると、前述した図 1-2-1 に出てきた「データ連携基盤(民間)」が図 1-2-2 における「エリア・データ連携基盤」にあたるものと想定する。

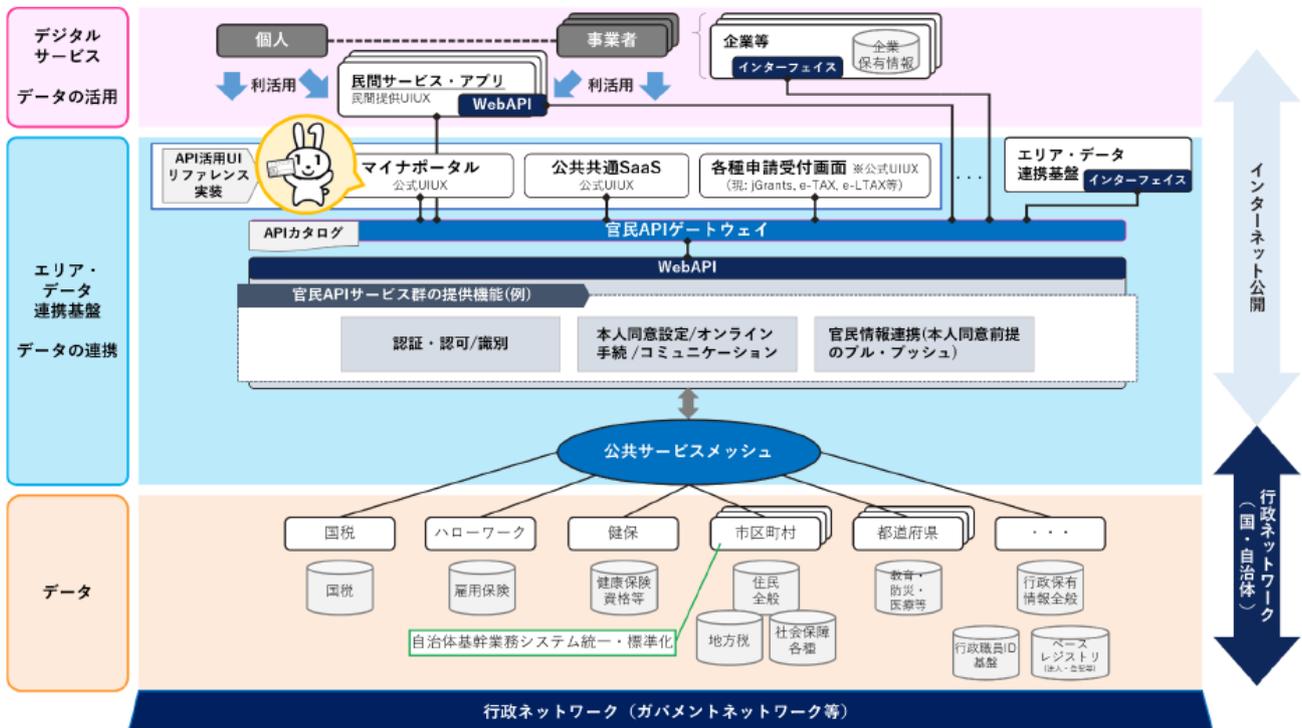


図 1-2-2 公共サービスメッシュの整備(イメージ)

<sup>5</sup> [https://www.cas.go.jp/jp/seisaku/digital\\_denen/dai4/siryous8.pdf](https://www.cas.go.jp/jp/seisaku/digital_denen/dai4/siryous8.pdf)

次に、同じくデジタル田園都市国家構想実現会議（第4回）の牧島大臣資料にて提示された図 1-2-3 「公共サービスメッシュとエリア・データ連携基盤の関係」を見ると、両者の関係を理解することができる。

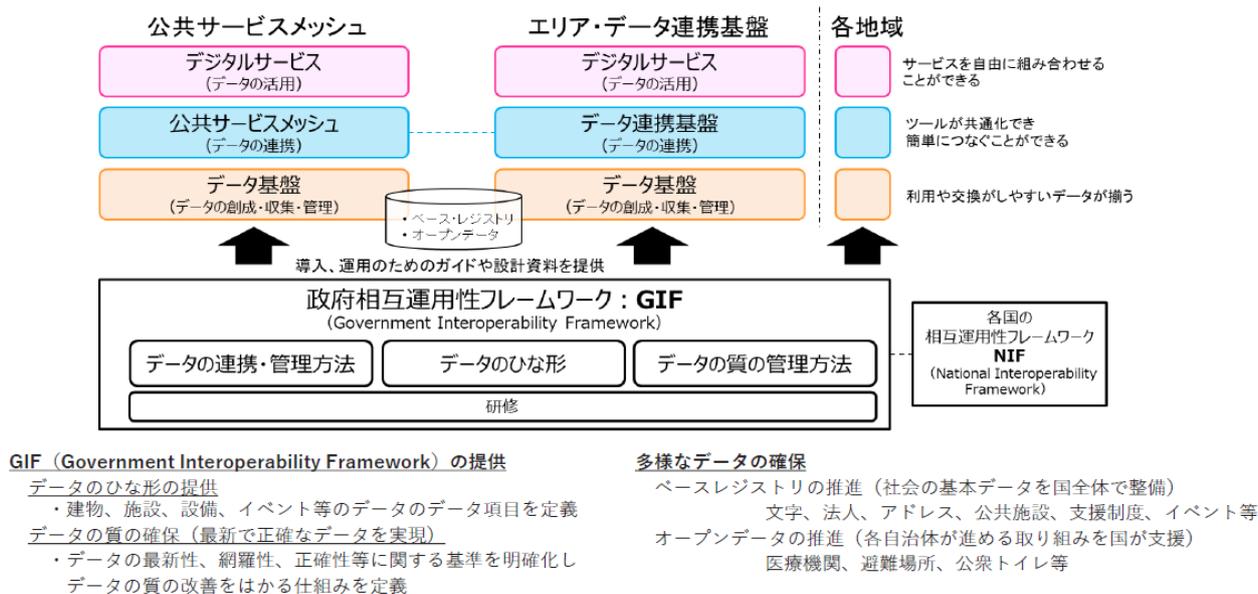


図 1-2-3 公共サービスメッシュとデータ連携基盤の関係

図 1-2-2 と図 1-2-3 から公共サービスメッシュは、ベースレジストリといった国や地方自治体で整備し、保有するデータを取り扱うものと想定される。これに対して、エリア・データ連携基盤は、地方自治体が保有するオープンデータ（例：医療機関、避難場所、公衆トイレ等）や事業者が保有しているデータを取り扱うものと想定される。なお、エリア・データ連携基盤にて取り扱うデータは、内閣府「2020年度 データ連携基盤技術報告書 スーパーシティのデータ連携基盤に関する調査業務 2021年 3月 第1版」に記載された「4-3-3. ブローカーにて取り扱うデータ種別」を基にして整理すると表 1-2-1 「ブローカーにて取り扱うデータ種別」のようになる。

表 1-2-1 ブローカーにて取り扱うデータ種別

	メタデータ	データ本体						
		静的				動的		
静的/動的	—							
データ形式	—	テキスト	地理空間	バイナリ	パーソナル	テキスト	動画(ストリーム)	パーソナル
代表的なデータ例	所有者情報	避難所情報	地形図	観光地写真	健康診断結果	水位センサー情報	河川監視画像	行動履歴
データ分散方式	対象外(※1)	必須	対象外(※2)	必須	必須	必須	対象外(※3)	必須
データ蓄積方式	対象外(※1)	原則不可(※4)	対象外(※2)	原則不可(※4)	原則不可(※4)	原則不可(※4)	対象外(※3)	原則不可(※4)

必須 : スーパーシティのブローカー機能として取り扱い必須

原則不可 : 原則として取り扱い不可ではあるが、特定の条件下でのみ取り扱い可であるもの

対象外 : ブローカー機能の対象外

- (※1) : データカタログ等の専用機能で管理されるため、ブローカー機能の対象外
- (※2) : GIS<sup>6</sup>等の専用機能で管理されるため、ブローカー機能の対象外バイナリデータとしてデータファイル自体を取り扱うことは可能
- (※3) : VMS<sup>7</sup>等の専用機能で管理されるため、ブローカー機能の対象外
- (※4) : データ分散方式を原則とするが、データ連携基盤運営者が保持するデータであればデータ蓄積方式も可能とする

図 1-2-3 と表 1-2-1 からエリア・データ連携基盤が取り扱うデータのうち、地方自治体が保有するオープンデータや事業者が保有している表 1-2-1 のデータを取り扱うデータ連携基盤が「生活用データ連携基盤」である。

公共サービスメッシュと生活用データ連携基盤の関係については、取り扱うデータ種別を考慮し、民間サービス・アプリがデータ利用する観点で図示すると、図 1-2-4 のようになる。

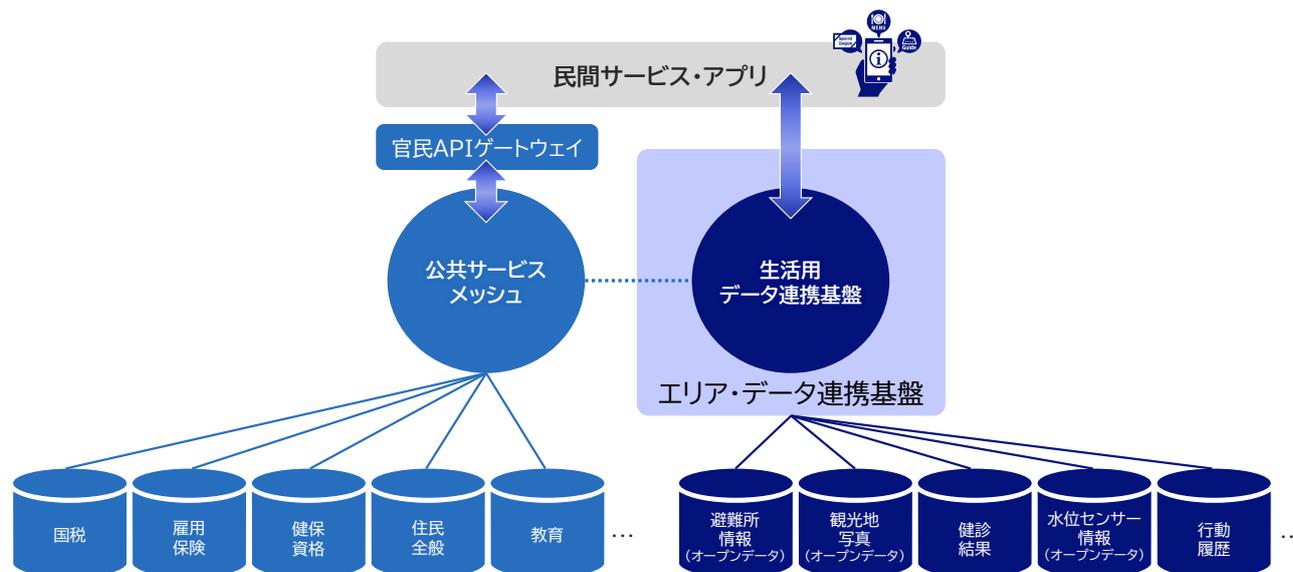


図 1-2-4 公共サービスメッシュと生活用データ連携基盤の関係

図 1-2-4 から民間サービス・アプリが公共データとオープンデータを取得する場合には、公共サービスメッシュまたは生活用データ連携基盤のどちらか一方を介することで実現できると想定される。しかし、公共サービスメッシュはアーキテクチャ設計が進められているところであり、現時点では民間サービス・アプリが生活用データ連携基盤のみにつながることで、公共サービスメッシュを介したデータ連携が可能になるのかは判断できない。引き続き、公共サービスメッシュのアーキテクチャ設計の状況を鑑み、生活用データ連携基盤とのデータ連携方式を決定することになる。

<sup>6</sup> 地理情報システム (Geographic Information System) のことで、地理的位置を手がかりに、位置に関する情報を持ったデータ (空間データ) を総合的に管理・加工し、視覚的に表示し、高度な分析や迅速な判断を可能にする技術

<sup>7</sup> Video Management Software/System の略で、映像管理システムやビデオ管理ソフトウェアを指し、防犯カメラや監視カメラで撮影した映像を記憶装置に保存及び管理するもの

### 1-3. 参考文献

本報告書における主な参考文献を以下表 1-3-1 に示す。

表 1-3-1 主な参考文献

No	文書名	本報告書における略称	参照先
1	内閣府/デジタル庁/内閣官房 「デジタル田園都市国家構想 推進交付金<デジタル実装 TYPE1>参考事例集」	デジタル実装 TYPE1 参考 事例集	<a href="https://www.chisou.go.jp/sousei/about/mirai/pdf/denenkouhukin_jissou_type1_jirei.pdf">https://www.chisou.go.jp/sousei/about/mirai/pdf/denenkouhukin_jissou_type1_jirei.pdf</a>
2	内閣府「2020年度 データ 連携基盤技術報告書 スーパー シティのデータ連携基盤に 関する調査業務 2021年 3月 第1版」	データ連携基盤技術報告 書	<a href="https://www.chisou.go.jp/tiiki/kokusentoc/supercity/pdf/20211221_DataLinkage_honsi.pdf">https://www.chisou.go.jp/tiiki/kokusentoc/supercity/pdf/20211221_DataLinkage_honsi.pdf</a>
3	内閣府「スーパーシティ/スマ ートシティの相互運用性の確 保等に関する検討会 最終報 告書」	相互運用性の確保等に関 する検討最終報告書	<a href="https://www.chisou.go.jp/tiiki/kokusentoc/supercity/pdf/sogowg_houkokusyo.pdf">https://www.chisou.go.jp/tiiki/kokusentoc/supercity/pdf/sogowg_houkokusyo.pdf</a>

## 2. 業務実施結果 ステップ1：技術基準の定義

### 2-1. データ連携基盤の機能群の定義

#### 2-1-1. ビルディングブロックの必要性

「相互運用性の確保等に関する検討最終報告書」において、データ連携基盤は、ビルディングブロック方式を用いて構成され、公開された API を通じてデータの集積や配信を行う機能と示されている。このビルディングブロック方式とは、機能群の中から必要な機能を取捨選択し組み合わせることであり、これにより、デジタル田園都市国家構想に係る国・地方にとって最適かつ疎結合なシステムを構築することが可能となり、データ流通における相互運用性の確保や、段階的な機能拡張、保守性の向上など、持続的な運用にも寄与するものである。ビルディングブロック方式による機能拡張例については、図 2-1-1-1 に示すとおり、「データ連携基盤技術報告書 9-2-3. 時代の変化に応じて柔軟にシステムを拡張する仕組み」においても報告されているため、参照いただきたい。

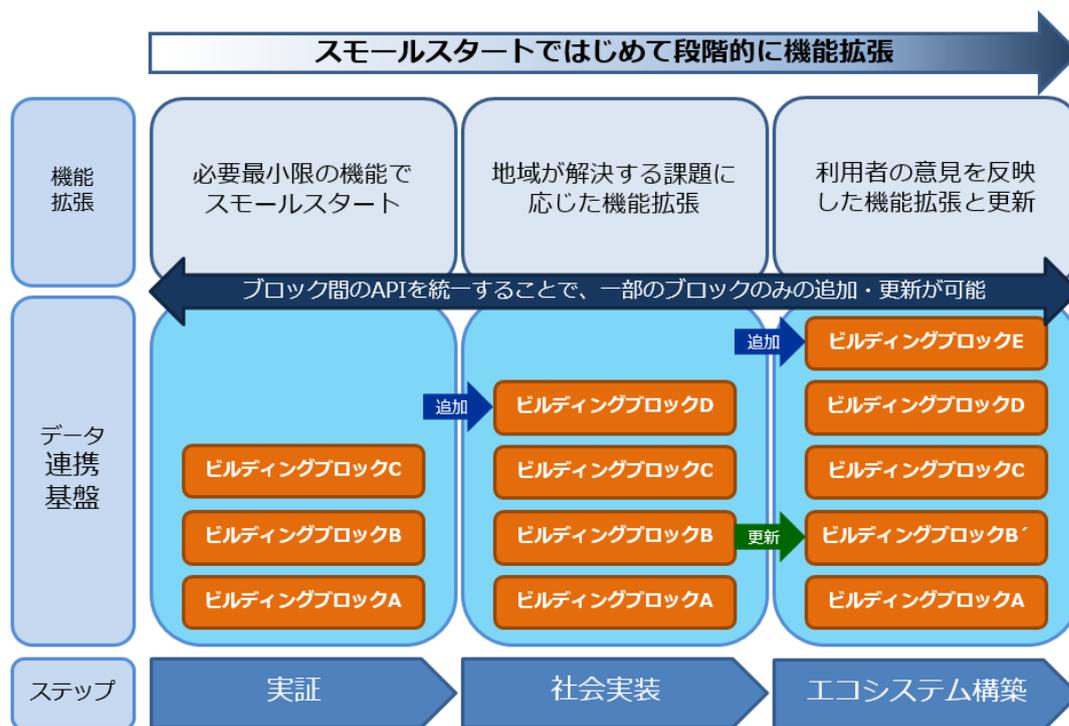


図 2-1-1-1 ビルディングブロック方式による機能拡張例

(データ連携基盤技術報告書 図 9-2-3-1 より抜粋)

このようなビルディングブロック方式は、例えば、欧州における CEF Digital での国境を越えたデジタル公共サービスの迅速な提供や、FIWARE Foundation での自治体や企業などの業種を越えたデータ活用やサービス連携の促進など、国境や分野を横断した相互運用性の確保等を目的として、国外の事例としても広く採用されるものである。

次項より、ユースケースや相互運用性の観点から、デジタル田園都市国家構想における、生活用データ連携基盤に必要なビルディングブロックを定義する。

#### 2-1-2. ユースケースから見る生活用データ連携基盤に必要なビルディングブロック

##### (1) ユースケースから見る生活用データ連携基盤に必要なビルディングブロックの調査概要

各地域固有の実情を踏まえた上で、業種間・都市間を横断してデータやサービスを共有するためには、相互運用性が確保できる最低限必要な機能を定義する必要がある。こうすることで、過大な機能を実装す

ることなく、各地域固有の実情に合わせ、必要なサービスを適用しやすくなり、オープンな技術要件に基づき開発されたサービスが多く都市にて利用できることにつながる。

「データ連携基盤技術報告書 3-2-3.」においては、データ連携基盤に最低限必要となる機能として、データを蓄積または分散管理してデータ流通を制御する「ブローカー」、そのブローカー等を API として利用するために接続仕様を外部公開する「オープン API」、そして利用者向けに API 関連情報をまとめた API カタログ等を実装する「開発者ポータルサイト」の3つが提案されている。

まず、ブローカーにおいて扱うデータは、1-2. で述べたように多種多様であるが、大別すると、例えば避難所情報やセンサーデータのような非パーソナルデータと、個人の健康診断結果や行動履歴のようなパーソナルデータに分けられる。パーソナルデータを扱う場合には、同意管理・匿名化等のプライバシー保護に関する機能が必要であり、要件が異なることから、非パーソナルとパーソナルそれぞれの要件に対応したブローカーを用意することが望ましい。

次に、オープン API については 2-2-1. で後述するが、API を個別に公開せず、一元的に管理・公開する API 管理機能 (API ゲートウェイ) は、相互運用性を確保するために具備することが望ましい。

開発者ポータルサイトについては、本調査によって公認モジュールとなる OSS 製品 (3-4-1. で後述) の開発コミュニティが利用しているものを活用する可能性があること、開発者ポータルが提供すべき想定機能はデータ連携基盤技術報告書で公開されていることから、本調査の対象外とする。

以上のことから、公認モジュールにおける共通性の高い機能候補として、「ブローカー (非パーソナル)」、「ブローカー (パーソナル)」、「API ゲートウェイ」の3つを選定した。

ここでは、デジタル田園都市国家構想推進交付金におけるデジタル実装 TYPE1 参考事例集を参照し、これらビルディングブロックの共通的な機能の必要性を基に、選定したビルディングブロックの妥当性を確認する。各ビルディングブロックの概要は以下のとおりである。

#### (ア) ブロック 1 : API ゲートウェイ

サービスから受け取ったリクエストをデータ連携基盤を構成する個々のサービスヘルパーティングする機能を有する。本機能を利用することにより、API 利用に必要な認証、ログ取得、不正アクセス対策等の機能をまとめて管理することで、API 実装コストを削減し、安定した品質で API を提供することが可能となる。

#### (イ) ブロック 2 : ブローカー (非パーソナル)

個人に紐づかないデータを蓄積、分散管理し、データの提供元組織の許諾に基づき、サービス間の非パーソナルデータの流通を制御する機能を有する。なお、1-2. でも述べたが、地理空間データや動画 (ストリーム) データといった、専用機能 (GIS や VMS) で管理するデータについては、本機能では扱わないものとする。

#### (ウ) ブロック 3 : ブローカー (パーソナル)

個人に紐づくデータを蓄積、分散管理し、データの提供元組織の許諾及び本人同意 (オプトイン) に基づき、サービス間のパーソナルデータの流通を制御する機能を有する。

なお、デジタル実装 TYPE1 参考事例集には、生活用データ連携基盤活用の有無にかかわらず、デジタルを活用した地域の課題解決や魅力向上の実現に向けて、他の地域等で既に確立されているサービスを活用し、迅速な横展開を図る事業 (デジタル実装タイプ TYPE1) について、活用が期待されるサービスが 104 事例掲載されている。生活用データ連携基盤の活用が想定される TYPE2 及び TYPE3 と違い、TYPE1 の事例集であるため、生活用データ連携基盤の活用について明記されていない事例が大半を占めているが、相互運用性の確保に向けた取組・工夫点を含めると、現在もしくは将来的に生活用データ連携基盤の活用が想定されるパターンが約 3 割あり、調査対象として適切であると判断した。

## (2) 調査方法

本項での調査フローを図 2-1-2-1 に示す。まずはデジタル実装 TYPE1 参考事例集に掲載されている 104 事例のうち、生活用データ連携基盤の活用について調査し、生活用データ連携基盤が必要とされる事例を抽出した。次に、それら生活用データ連携基盤が必要と判断した事例を対象に、2-1-2. (1) で選定した機能の活用が想定されているかを検証し、最終的にビルディングブロックとして必要なものを定義する。

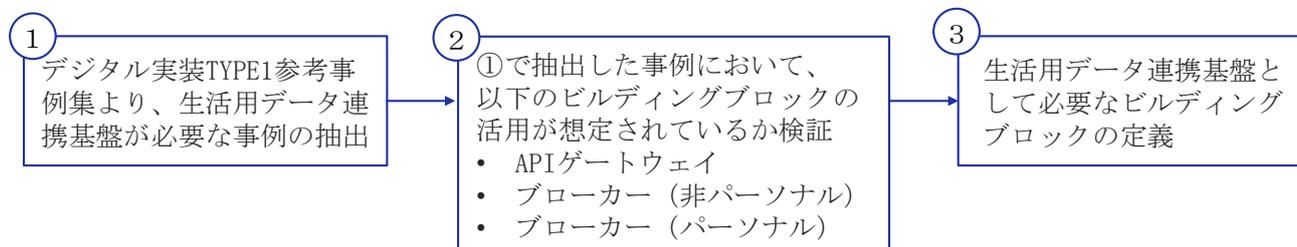


図 2-1-2-1 参考事例調査フロー

各事例における生活用データ連携基盤の活用について、図 2-1-2-2 に示すフローに沿って、表 2-1-2-1 に示す◎、○、△及び×へと分類した。個人とサービス提供組織の2者間で完結するサービスは、本来は生活用データ連携基盤は不要であるが、流通するデータが第三者のデータと連携することで効用が増大すると判断される場合には△と判定した。例えば、個人の日々の体調情報を健康アプリに提供して最適な生活習慣のアドバイスが貰えるサービスがあった場合、本来はバイタルデータが個人とサービス提供会社の2者で閉じているため生活用データ連携基盤は不要だが、そこに周辺の飲食店データを連携させることで、健康状態に合わせた最適な外食メニューの提案が可能になると想定される場合は△とした。

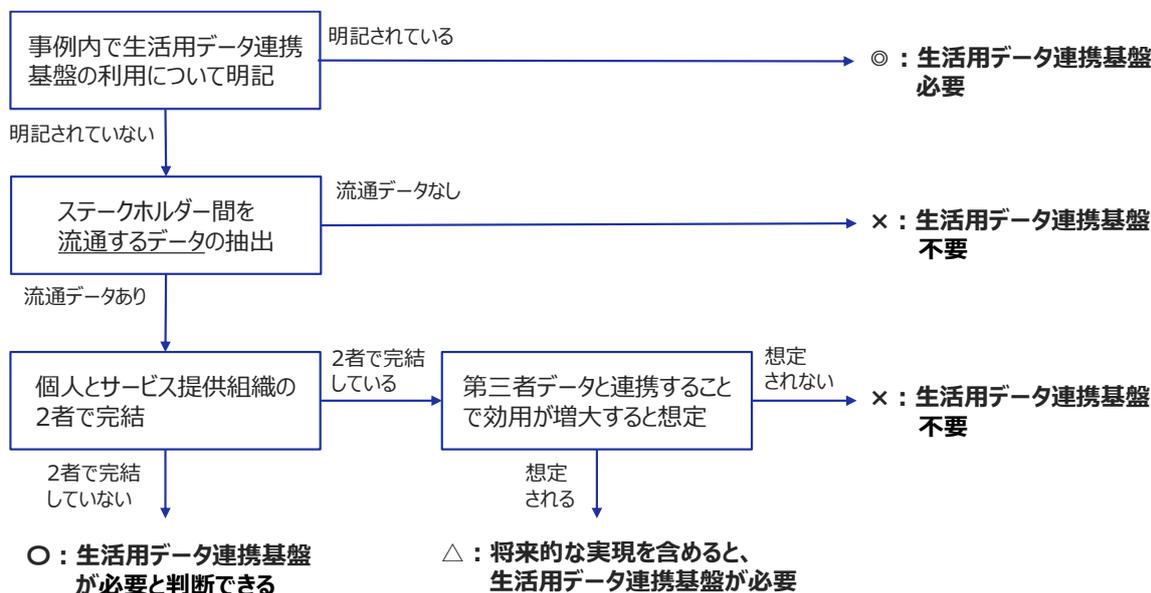


図 2-1-2-2 生活用データ連携基盤の活用判断フロー

表 2-1-2-1 生活用データ連携基盤活用の判断基準

◎	将来的な実現も含め、生活用データ連携基盤の活用がデジタル実装 TYPE1 参考事例集内に記載されている
○	複数のステークホルダー間でデータが流通しているため、生活用データ連携基盤が必要と判断できる
△	将来的な実現も含め、生活用データ連携基盤を活用することで効用が増大すると判断できる
×	生活用データ連携基盤が不要と判断できる

(3) 調査結果

(a) 生活用データ連携基盤についての調査結果

デジタル実装 TYPE1 参考事例集に掲載されている 104 事例のうち、現時点で生活用データ連携基盤が必要と判断した◎及び○の合計は 27 事例であった。分野別の集計結果を表 2-1-2-2 に示す。

表 2-1-2-2 生活用データ連携基盤の活用について

分野	総事例数	生活用データ連携基盤 必要		生活用データ連携基盤 不要	
		◎	○	△	×
インフラ・防災	7	1	2	1	3
金融・決済	1	0	0	0	1
しごと	6	0	0	0	6
文化	2	0	0	0	2
環境・エネルギー	5	0	2	1	2
観光	5	0	3	0	2
教育	5	0	0	0	5
健康・医療	16	0	9	3	4
交通	13	0	4	3	6
行政サービス	4	1	0	0	3
住民サービス	3	0	1	0	2
物流	6	1	0	3	2
農林水産	31	0	3	4	24
合計	104	3	24	15	62


  
生活用データ連携基盤必要：27

また、扱うデータを非パーソナル及びパーソナルの分類別に整理した結果を表 2-1-2-3 に示す。非パーソナルデータを扱う事例は 12 事例であり、農林水産及びインフラ/防災の分野半数を占めた。これらの分野は、IoT 機器の設置によりデータを取得する事例が多いため、生活用データ連携基盤を活用するケースが多いと考えられる。例えば、複数の自治体で取得する河川水位データを連携させることで、広域防災に役立てる事例が挙げられる。

パーソナルデータを扱う事例は 15 事例であり、生活用データ連携基盤が必要と判断した事例の半数以上であった。さらに、パーソナルデータを扱う事例の半数以上が健康・医療分野であり、要配慮

個人情報を扱うものは 8 事例であった。なお、パーソナルデータ及び非パーソナルデータの両方を扱う事例については、データ取り扱い上で考慮する事項の多いパーソナルへと分類した。

表 2-1-2-3 パーソナル/非パーソナルでの分類

データ分類	該当事例数 (計 27)	活用分野	具体例
非パーソナル	12	農林水産 : 3 インフラ/防災 : 3 交通/物流 : 2 環境/エネルギー : 2 その他 : 2	A) 気象、センサー、時刻表、車両位置、交通量、発電・蓄電量 等 : 12
パーソナル	15	健康/医療 : 9 交通 : 3 その他 : 3	B) 特定個人情報 (マイナンバー) : 2
パーソナルのみ	5		C) 要配慮個人情報 : 8
非パーソナル/ パーソナル両方	10		D) 一般 (住所・氏名・年齢・性別等) : 5 その他 (生体、購買、行動履歴等)

(b) ビルディングブロックへの分類結果

2-1-2. (3) (a)において生活用データ連携基盤が必要と判断された 27 事例において、活用が想定される 3 つのビルディングブロックに分類した結果を表 2-1-2-4 に示す。

表 2-1-2-4 ビルディングブロック分類

ビルディングブロック	該当事例数 (計 27)	分類説明
API ゲートウェイ	27	生活用データ連携基盤の活用が必要と判断した全ての事例において、複数のデータ流通が見込まれており、API を通じてそれらを相互にやりとりするためには、安定した品質の API 管理が望まれる。そのため、全ての事例で API ゲートウェイは必要と判断した。
ブローカー	27	生活用データ連携基盤の活用が必要と判断した全ての事例において、必要なデータの相互連携もしくは共有が求められており、そのためには適切なデータ集約及び処理が望まれる。そのため、全ての事例においてブローカーは必要と判断した。
非パーソナル	22	非パーソナルデータを扱う事例において使用されるため、表 2-1-2-3 より 22 事例で必要と判断した。逆に不要となるのは、パーソナルデータのみを扱う場合である。例えば、住民の健康データを複数企業で分析してビッグデータとして活用すると同時に住民へ最適な健康アドバイスを提示する事例が挙げられる。
パーソナル	15	パーソナルデータを扱う事例において必要となる。逆に不要となるのは、非パーソナルデータのみを扱う場合である。例えば、災害時に複数の交通事業者を繋いで物資を避難所に届ける事例が挙げられる。

以上のことから、サービス提供組織が生活用データ連携基盤上を流通するデータを利用してサー

ビスを提供する場合、API ゲートウェイは全ての事例で必要となり、流通するデータが非パーソナル、パーソナルの場合は、それぞれブローカー（非パーソナル）、ブローカー（パーソナル）が必要となることがわかった。

### 2-1-3. 基盤の定義

生活用データ連携基盤に必要なビルディングブロックとして、ユースケースから見る基盤に必要なブロックから、「API ゲートウェイ」「ブローカー（非パーソナル）」「ブローカー（パーソナル）」の3つが最低限必要であると導出された。これらのブロックを、各地域が共通的に活用できる公認モジュールに選定し、「データ連携基盤技術報告書 3-2. データ連携基盤の全体像」を基に、生活用データ連携基盤の全体像及び、公認モジュールとして公開する範囲を図 2-1-3-1 に示す。

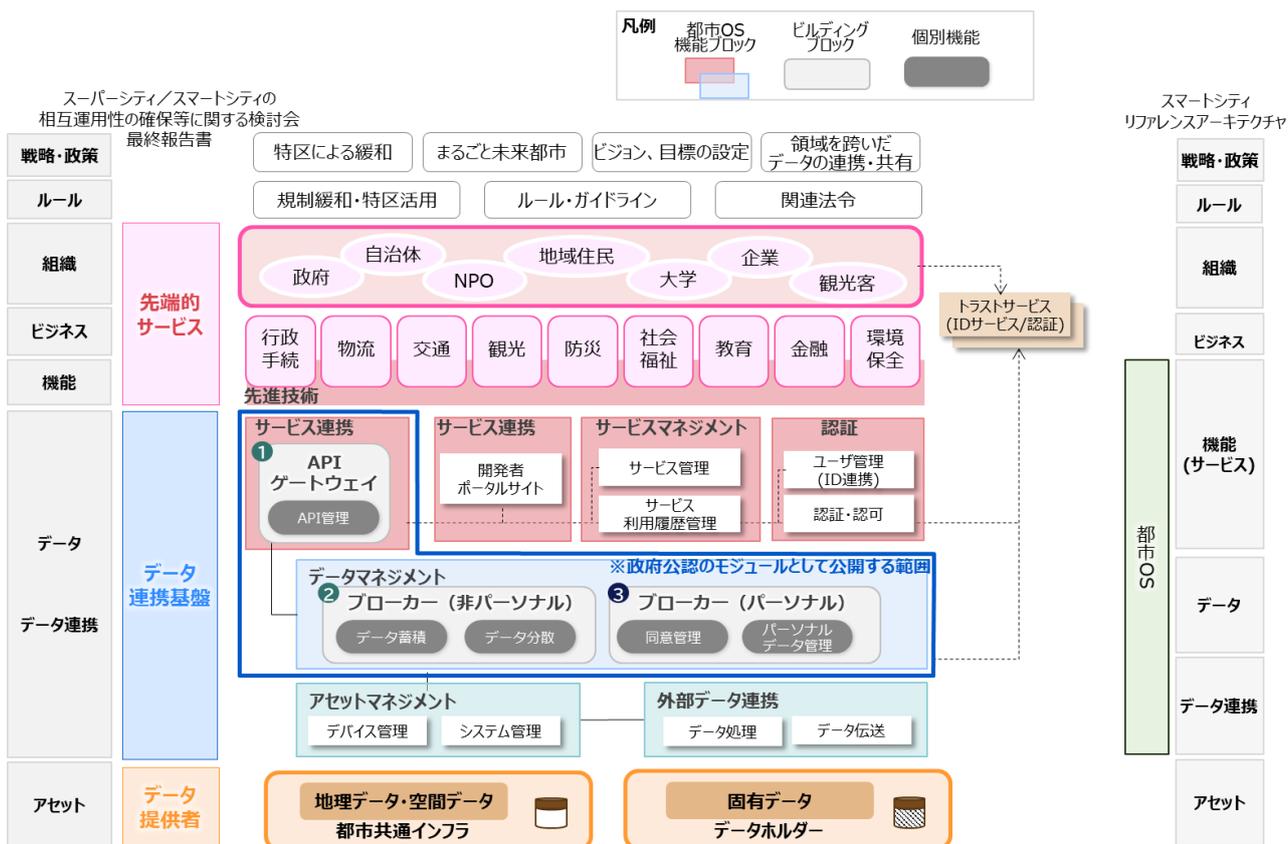


図 2-1-3-1 生活用データ連携基盤における公認モジュールとして公開する範囲

これら公認モジュールを活用することで、エリア内外のデータを連携させ、API を通じた外部公開が可能となり、最低限の相互運用性を確保することとなる。

地域のデータ連携基盤整備事業者は、公認モジュールを中心に、解決する課題や目指すべき将来像など、ユースケースに応じてビルディングブロックを組み合わせ、生活用データ連携基盤を整備・強化することとなる。この際、公認モジュール以外のビルディングブロックについては、既に各地域で稼働するサービスや、利便性やセキュリティ強度を高めるために必要な機能群など、競争領域に位置するビルディングブロックも併用することで、付加価値をつけた地域特有の取り組みとなり、地域産業の高度化にもつながるものである。

なお、生活用データ連携基盤の整備においては、スマートシティリファレンスアーキテクチャ<sup>8</sup>で公開

<sup>8</sup> <https://www8.cao.go.jp/cstp/stmain/20200318siparchitecture.html>

される都市 OS の要件一覧や、データ連携基盤技術報告書で公開されている開発者ポータルサイトの想定機能についても参照いただきたい。

## 2-2. 相互運用性を確保するための基準

相互運用性の確保は、相互運用性の確保等に関する検討最終報告書においてその技術的事項が検討されているほか、デジタル庁のデジタル臨時行政調査会における「デジタル社会の実現に向けた 5 つの原則<sup>9</sup>」にも「相互運用性確保原則」として含まれおり、デジタル社会の実現に向けた重要な概念である。以下、ここでは、相互運用性について上記の文献を参照し検討を行う。

相互運用性の確保等に関する検討最終報告書では、データ連携基盤の相互運用性を「中長期にわたって、静的及び動的なデータを API などを通じて相互にやりとりしながら、特定の施策を運用できること」と定義している。こうした相互運用性を確保することにより、データを利用した多様なサービスを生み出すとともに、より多くのサービス提供者の参入を促すことで、品質の高いサービスを住民に提供することやサービス提供の持続性を向上させることなどが可能になる。

相互運用性の確保等に関する検討最終報告書では、「広く官民を超えて、常にオープンな連携を可能にするための API の設計と、そこでやりとりされるデータモデルの策定をどのように進めていくかが、重要な要素」(1.1. 抜粋) になるとしている。これを踏まえ、データ連携基盤技術報告書では、API の共通ルール設計、公開に際する共通ルールの調査とデータモデルの方針に関する検討について、「5. 調査結果 (イ) ① API 共通ルール 標準仕様」と「7. 調査業務 (ウ) データモデルの方針」にて実施している。このことから、相互運用性の確保に向けては、最低限、データを API を通じて相互にやりとりするための API の公開及び API の利用規約についての基準と、静的及び動的を含む様々なデータを扱うためのデータモデルを設計するにあたって順守すべきルールが必要と考えられる。次項から、相互運用性の確保等に関する検討最終報告書ならびにデータ連携基盤技術報告書を踏まえ、API の公開、API の利用規約、データモデルについて説明する。

### 2-2-1. API の公開

前述のとおり、API とは、あるサービスの機能や管理するデータ等を他のサービスやアプリケーションから呼び出して利用するための接続仕様等を指す。相互運用性の確保等に関する検討最終報告書においては、API の中でも厳格な要件や契約などを必要とせず、外部から誰でもアクセス可能な API のことを「オープン API」と呼称する。API が公開され利用されることにより、データを活用する多様な主体が有機的に連結され、住民の生活に面的かつ多様なドメインをまたがった便益を提供することが可能となる。

相互運用性の確保等に関する検討最終報告書において、図 2-2-1-1 に示すように、API を開放度（誰がデータを利用可能か）の観点で分類している。

---

<sup>9</sup> <https://www.psrn.jp/topics/detail.php?id=19955>



図 2-2-1-1 オープン API の類型  
(相互運用性の確保等に関する検討最終報告書より抜粋)

相互運用性を確保するための必要となる基準について相互運用性の確保等に関する検討最終報告書から一部引用して以下のように記述されている。以下にはデータモデルに関する内容も一部含まれているが、データモデルの詳細については 2-2-3. を参照いただきたい。

○ API の開放性設計指針

- ・ API の接続先が、同じ管理主体の内部や、同じ事業者が展開するサービスとの API データ連携である場合を除き、可能な限り狭義のオープン API とする。
- ・ ユーザーの適切な識別や権限付与、悪意ある攻撃への対処等を目的に、必要に応じて API アクセストークン（アプリケーションの認証済みユーザーを識別する情報）を実装する。

・

○ API カタログの実装

- ・ API に関するデータに関する付帯情報が記載されたデータ（以降、メタデータ）や開発者ポータルサイトの情報をまとめたカタログサイトを実装する。
- ・ API に関するメタデータ等を記載する設定ファイルの配布や、それらの情報を提供する API を実装する。

○ データモデル及び API に関する情報の公開方法

- ・ データの公開主体の明確化：適切な単位を基に API 及びデータの公開主体を定める。
- ・ API 及び静的データの公開場所：開発者ポータルサイトを作成し、API に関する情報を、技術者に分かりやすい場所と形式で公開する。
- ・ API に関する情報へのアクセス：オープン API のうち Public API については特に、API に関連する情報を広く一般に公開する。
- ・ 公開するメタデータ：API に関するメタデータとして、最低限、以下の情報を公開する。
  - API エンドポイント（API にアクセスするための識別子（URI (Uniform Resource Identifier) )), あるいは静的データの配布 URL

- API あるいはデータの利用条件

なお、メタデータの伝送においては、原則、設計様式として REST (Representational State Transfer、分散システム向けソフトウェア連携に適した方式)、データ形式として JSON (JavaScript Object Notation、構造化データを表現する標準化されたテキスト形式) を利用する。

- フィードバック体制の構築：利用者からのフィードバックを基に、API 及びその付帯情報を見直す体制を構築する。

## 2-2-2. API 利用規約

API を公開するにあたり、API の提供者と利用者の中で合意されるべき API の利用条件は、API 利用規約に明示される必要がある。公開された API が広く利活用され、データ連携基盤の相互運用性が維持されるためには、API 利用規約テンプレートが必要である。相互運用性の確保等に関する検討最終報告書 3.1. では、「データ連携基盤で活用する API は、可能な限り狭義のオープン API として設置」とある。ここで「狭義のオープン API」とは、同書にて、誰でもアクセス可能な API (Public)、または一定の規約や契約が必要なものの、誰でもアクセス可能な API (Acquaintance) と定義される。しかしながら、同書では API の共通ルールや標準仕様までは規定されておらず、「全国自治体のスマートシティの取組においては、API がエリアの独自ルール・仕様で設計／開発・公開・運用され、エリア内外での相互運用性・互換性が向上しないリスクがあると想定される (データ連携基盤技術報告書 2-3-1.)」。

以上のことから、データ連携基盤技術報告書では、エリア内外で一定の統制をとることを目標に、API 運用者向けの設計/開発・公開・運用プロセスと API 利用規約 (テンプレート)、API 設計・開発者向けの標準仕様案を検討した。このうち API 利用規約テンプレートは、図 2-2-2-1 に示すとおり、「データ連携基盤整備事業者から、データ連携基盤が提供する API を利用して先端的サービスを開発する先端的サービス事業者や、API を利用して新たな API を開発する別のデータ連携基盤整備事業者」に提供される API 利用規約を対象 (データ連携基盤技術報告書 5-2-1.)」として検討された。API 利用規約テンプレートの検討に当たっては、政府標準利用規約 (第 2.0 版) と国・自治体及び民間事業者にて提供されている API の利用規約が調査・分析された。

検討の結果、得られた API 利用規約テンプレート案の項目を表 2-2-2-1 に示す。データ連携基盤の相互運用性を確保するための基準として、データ連携基盤 (民間) ごとに、表 2-2-2-1 の項目を満たす API 利用規約テンプレートを整備することが望ましい。各項目の詳細や解説は、データ連携基盤技術報告書 5-2-2. を参照されたい。

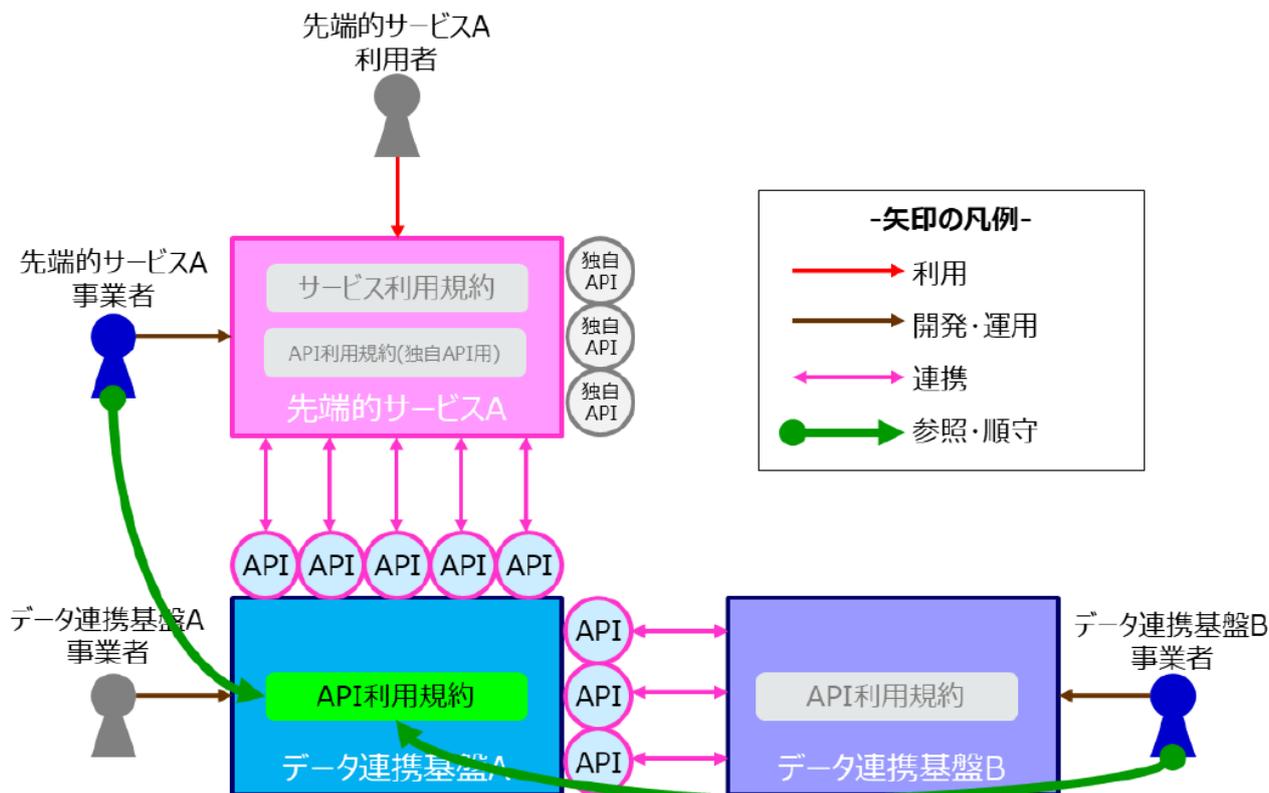


図 2-2-2-1 API 利用規約テンプレートの位置づけ  
 (※データ連携基盤技術報告書 図 5-2-1-1 より抜粋)

表 2-2-2-1 API 利用規約テンプレート案 項目  
 (※データ連携基盤技術報告書 5-2-2 章より整理)

項目	名称	概要
第1条	目的	利用規約の目的と適用範囲を明らかにする。
第2条	定義	利用規約において繰り返し登場する用語を定義する。
第3条	登録	API の利用にあたって利用規約を必要とする場合に、その登録手順について定める。
第4条	API 認証情報の発行及び管理	登録が完了した API 利用者に対して個別の API 認証情報を発行する場合に、その手続及び管理の在り方について定める。
第5条	本 API の提供条件	API をどのような条件・仕様のもとで提供するかについて定める。
第6条	料金	API 利用者による API の利用を有償とする場合に、その料金について定める。
第7条	API 利用者の義務・責任	API 利用者が API 利用アプリケーションをエンドユーザーに提供してサービスを行うにあたって、API 提供者との関係で負う義務と責任について定める。
第8条	禁止事項	API 利用者が行ってはならない行為について定める。

項目	名称	概要
第 9 条	利用解除	API 提供者が本利用規約に違反した場合における、利用の停止または解除について定める。
第 10 条	権利の帰属・利用	API に関する知的財産の帰属等を定める。
第 11 条	免責	API 提供者の免責について定める。
第 12 条	補償／賠償	API の利用に伴う賠償責任の範囲について定める。
第 13 条	反社会的勢力の排除	反社会的勢力の排除条項を定める。
第 14 条	秘密保持	API 利用者の秘密保持義務を定める。
第 15 条	個人情報取扱	API 提供者が、API の提供に関して個人情報を取り扱う場合、プライバシーポリシーを策定し、それに則り適切に取り扱う旨を宣明する。
第 16 条	規約の変更	利用規約を変更する際の手続きを定める。
第 17 条	提供の終了	API の提供を終了する場合について定める。
第 18 条	連絡／通知	API 提供者と API 利用者との連絡の方法について定める。
第 19 条	権利義務等の譲渡禁止	API 利用者が、本契約上の地位及び本契約によって生じる権利義務を、事前の承諾なく、第三者に譲渡、承継または担保提供することを禁止する。
第 20 条	分離可能性	利用規約の一部の条項が何らかの法令違反などによって無効または執行不能であるとされた場合であっても、当該無効な条項のみを分離し、他の条項は有効のまま存続させ、利用規約の大枠は引き続き維持することを定める。
第 21 条	準拠法及び管轄裁判所	利用規約の準拠法及び裁判直轄について定める。

### 2-2-3. データモデル

データモデルとは、データの項目や形式を構造化して記述したものである。データ連携基盤の相互運用性を確保するために、相互運用性の確保等に関する検討最終報告書では、データモデルの「互換性」及び「公開」を挙げている。「互換性」は、「やりとりされるデータの持つ意味について、データの提供者と利用者間で共通の理解を持ち、機械が正しくデータの持つ意味を解釈する、すなわち互換性を担保する必要がある（相互運用性の確保等に関する検討最終報告書 1.4.）」ことであり、「その都市やサービスを運用する主体が様々なレイヤーにおいて、互換性を保つことに同意し、共通理解を構築し、環境を整える必要がある（同書 1.4.）」ことを指す。また、「公開」は、「既存のデータモデルの洗い出しとそれらの関係整理を行い、各モデルの持つ意味を明確化し、可能な限り公開する（同書 2.3.）」こと、ならびに「新しくデータモデルを構築する必要がある場合は、既存のオープンな標準を可能な限り利用し、（中略）策定した結果を公開する（同書 2.3.）」ことを意図する。

これを踏まえ、データ連携基盤技術報告書では、スーパーシティ間及びスーパーシティ外でも汎用的に使用されていくデータモデルの仕様、規格等の整理を目的に、既存データモデルの調査結果を基に、データモデルの標準化についての方針が検討されている。

当該検討において、データモデルの相互運用性は図 2-2-3-1 のとおり整理されており、このうち幅広い分野にまたがる相互運用での現実解を「③参照モデルを共有する」手法であるとしている。これは

「各システムのデータモデル定義はそのままに、参照モデルとの違いや共通点を明らかにすることでデータの相互運用性を確保しようとする（データ連携基盤技術報告書 7-2-3.）」ことを意図する。加えて、データ連携基盤技術報告書では参照モデルとなりえる推奨データモデルの整理原則として、既存データモデルの活用、スモールスタートと成果の可視化、グローバル標準との整合性、イノベーションのための成長の仕組み、多様な用途に長く使える仕組みの考慮が必要としている。詳細はデータ連携基盤技術報告書 7-3-2. を参照されたい。

以上のことから、データモデルにおけるデータ連携基盤の相互運用性を確保するために、「互換性」があること及び「公開」されていることがあげられる。互換性の現実解としては、図 2-2-3-1 の③に示されるとおり、参照モデルを共有する手法が望ましい。参照モデルの検討に当たっては、データ連携基盤技術報告書 7-3-2. 推奨データモデルの整備原則を参照していただきたい。

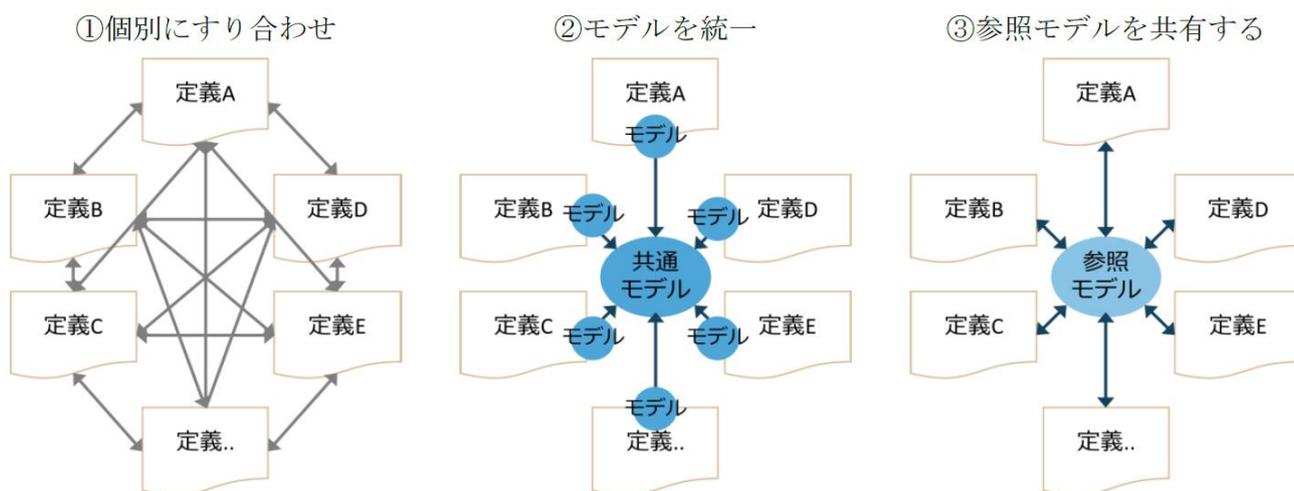


図 2-2-3-1 相互運用性の考え方  
 (※データ連携基盤技術報告書 図 7-2-3-1 より抜粋)

### 3. 業務実施結果 ステップ2：公認モジュールの決定

#### 3-1. API ゲートウェイが満たすべき要件

本節では、広く使われている API ゲートウェイを調査・分析することで API ゲートウェイが具備すべき要件を定義する。昨今ではクラウドサービス上でのシステム構築が主流となっており、API ゲートウェイもクラウドサービスが提供する機能を利用するケースが主流と想定される。日本国内においても様々な分野で使われているクラウドサービスである、Amazon Web Services（以下、AWS）、Google Cloud Platform（以下、GCP）、Microsoft Azure（以下、Azure）が提供する API ゲートウェイサービスを調査し、API ゲートウェイが満たすべき要件を抽出する。

各 API ゲートウェイサービスの調査結果を表 3-1-1 に示す。

表 3-1-1 API ゲートウェイ調査結果

分類	機能	説明	AWS <sup>10</sup>	GCP <sup>11</sup>	Azure <sup>12</sup>
基本機能	認証	API キー等により API を実行したユーザーの正当性を確認する機能	○	○	○
	ルーティング	受け付けた要求をバックエンドのマイクロサービスへ転送する機能	○	○	○
	ライフサイクル管理	API ゲートウェイで管理する API を登録/参照/変更/削除する機能	○	○	○
	バージョン管理	バージョンの異なるマイクロサービスの API を管理する機能	○	○	○
セキュリティ	アクセス制限	アクセス可能な API やデータに制限をかける機能	○	○	○
	レート制限	単位時間あたりの API 実行回数に制限をかける機能	○	○	○
利用可能 API	REST API	REST API を管理・公開する機能	○	○	○
	Websocket API	Websocket API を管理・公開する機能	○	×	○
分析・モニタリング	アクセス分析	API アクセス数を分析し、統計情報を可視化する機能	○	○	○
	アラート監視	API で発生したアラートを検出する機能	○	○	○
収益化	料金計算	API 実行回数等により、ユーザーへ請求する金額を計算する機能	× (※1)	○	× (※2)
	決済連携	決済サービス等と連携し、ユーザーへ API 利用料を請求する機能	× (※1)	×	× (※2)

(※1) AWS Market Place と連携することで実現可能<sup>13</sup>

(※2) Adyen や Stripe と連携することで実現可能<sup>14</sup>

<sup>10</sup> <https://aws.amazon.com/jp/api-gateway/>

<sup>11</sup> <https://cloud.google.com/api-gateway/>

<sup>12</sup> <https://azure.microsoft.com/ja-jp/services/api-management/>

<sup>13</sup> [https://docs.aws.amazon.com/ja\\_jp/apigateway/latest/developerguide/sell-api-as-saas-on-aws-marketplace.html](https://docs.aws.amazon.com/ja_jp/apigateway/latest/developerguide/sell-api-as-saas-on-aws-marketplace.html)

<sup>14</sup> <https://docs.microsoft.com/ja-jp/azure/api-management/monetization-support>

表 3-1-1 の調査結果から、API ゲートウェイには認証・ルーティング・ライフサイクル管理のような基本機能のみではなく、各 API ゲートウェイサービスで様々な機能が実装されていることがわかる。本調査で抽出した機能群から、以下の観点で API ゲートウェイ要件を定義する。

【必須】 ※下記の項目全てに該当するもの

- ・ データ連携基盤技術報告書における API 標準仕様書の必須要件の実現に必要な機能
- ・ 他コンポーネントで本機能を補うことが難しく、API ゲートウェイへの実装が必要な機能

【推奨】

- ・ 必須条件を満たしていないが、機能を具備することで API 利用者・管理者にとって有益である機能

【対象外】

- ・ 必須または推奨の条件に該当せず、表 3-1-1 において、いずれかのクラウドサービスで非対応の機能

上記に基づき定義した API ゲートウェイ要件を表 3-1-2 に示す。

表 3-1-2 API ゲートウェイ要件

分類	機能	要件	必須	推奨
基本機能	認証	API キー等により API を実行したユーザーの正当性を確認できること	●	
	ルーティング	受け付けた要求をバックエンドのマイクロサービスへ転送できること	●	
	ライフサイクル管理	API ゲートウェイで管理する API を登録/参照/変更/削除できること	●	
	バージョン管理	バージョンの異なるマイクロサービスの API を管理できること	●	
セキュリティ	アクセス制限	アクセス可能な API やデータを制限できること		●
	レート制限	単位時間あたりの API 実行回数を制限できること		●
利用可能 API	REST API	REST API を管理・公開できること	●	
分析・モニタリング	アクセス分析	API アクセス数を分析し、統計情報を可視化できること		●
	アラート監視	API で発生したアラートを検出できること		●

### 3-2. ブローカー（非パーソナル）が満たすべき要件

本項ではブローカー（非パーソナル）が満たすべき要件について記載する。データ連携基盤技術報告書においてブローカー要件が既に定義されているため、本調査におけるブローカー（非パーソナル）の要件もこれと同様と定義する。

表 3-2-1 ブローカー要件（非パーソナル）

データ連携目的	分類	機能	要件	必須	推奨
データ利活用	データ参照	データ分散	データ参照の要求を受け付け、外部サービスが保持するデータを返却可能なこと	●	
			データ利用者に対してデータの所在を隠蔽することができること		●

データ連携目的	分類	機能	要件	必須	推奨
		データ蓄積	データ参照の要求を受け付け、データストア機能に蓄積されたデータを返却可能なこと		●
	サービス呼び出し	イベント処理	サービス呼び出しの要求を受け付け、外部サービスの処理を実行し結果を返却可能なこと (例：交通サービスでタクシーを予約)		●
	API 仕様	API 仕様	データ利活用の利便性を考慮し、標準ルールに沿った API (REST 等) を提供可能なこと	●	
	データ変換	データ変換	外部サービスへの接続時、接続先サービスのインターフェースに合わせたデータ変換が可能なこと		●
データ収集	データ更新	イベント処理	データ提供者からデータを受け付け、必要なサービスへデータを送信できること		●
			データ送信時、リアルタイムにデータの分析・変換・加工処理等が可能なこと		●
		データ蓄積	データ提供者からデータを受け付け、データストア機能に蓄積可能なこと		●
	API 仕様	API 仕様	多種多様なアセットからのデータ収集を想定し、標準 API に限らず様々な接続方式に対応可能なこと (MQTT 等)		●

### 3-3. ブローカー（パーソナル）が満たすべき要件

個々の住民に寄り添ったサービスを展開し課題解決に資するためには、パーソナルデータの活用が重要となる。パーソナルデータ活用に際しては、個人情報保護を考慮しながらそのデータの価値を有効活用するため、オプトイン・オプトアウト、セキュリティ担保への対応が必要となる。データ連携基盤技術報告書においては、パーソナルデータを扱うブローカーは調査対象外としていたため、本調査で改めてブローカー（パーソナル）に必要な要件を、ステークホルダーリスト、トラスト関係及びユースケースを基に整理する。

#### 3-3-1. ステークホルダーリスト

要件を整備するにあたり、生活用データ連携基盤に関連するステークホルダーを表 3-3-1-1 に整理する。非パーソナルデータのみを扱う場合に加え、個人、代理人及び被代理人が関与することになる。代理人と被代理人をステークホルダーとしているのは、例えば高齢者や責任能力のない未成年でも安心してパーソナルデータを活用したサービスを楽しむことができるようにするためである。

表 3-3-1-1 ステークホルダーリスト

名称	説明
個人	生活用データ連携基盤及び先端的サービス <sup>15</sup> を利用する個人
代理人	生活用データ連携基盤及び先端的サービスの設定権限を個人から委任されている個人
被代理人	生活用データ連携基盤及び先端的サービスの設定権限を代理人に委任している個人

<sup>15</sup> 複数のサービスアセットを連携させることで価値提供を行う高度なサービス

名称	説明
サービス提供組織	先端的サービスを提供する生活用データ連携基盤接続組織
サービス提携組織	サービス提供組織と提携し、サービスアセット <sup>16</sup> を提供する生活用データ連携基盤接続組織
サービス提携組織(アプリ)	先端的サービスへ個人アプリ <sup>17</sup> をサービスアセットとして提供するサービス提携組織
サービス提携組織(ワークフロー)	先端的サービスへワークフロー <sup>18</sup> をサービスアセットとして提供するサービス提携組織
サービス提携組織(データ保有)	先端的サービスが利用するパーソナルデータを蓄積するサービス提携組織
サービス提携組織(データ利用)	先端的サービスを提供するために蓄積されたパーソナルデータを利用するサービス提携組織

### 3-3-2. トラスト関係

パーソナルデータ流通には、組織や個人間において、利用規約や接続規約の同意のもとでデータが流通する必要がある。パーソナルデータ流通に関するトラスト関係を図 3-3-2-1 のように整理する。図の左側に個人及び代理人が入るため、各種利用規約を設定し、同意を得る必要がある。

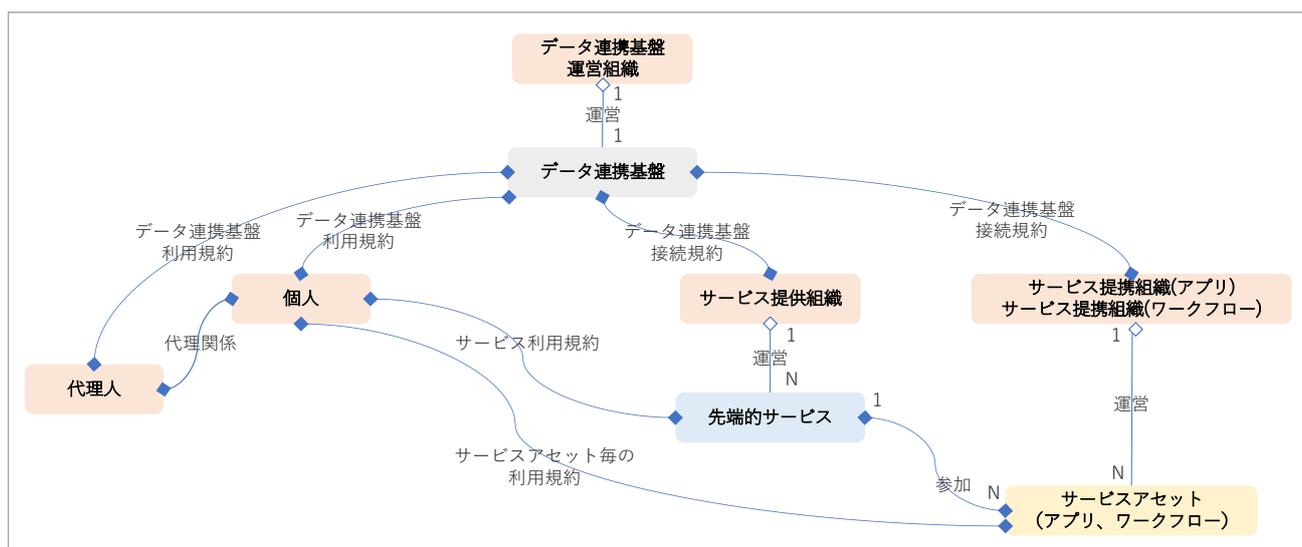


図 3-3-2-1 トラスト関係の整理

### 3-3-3. ユースケース整理

ブローカー (パーソナル) に必要となる要件を整備するにあたり、パーソナルデータ流通のユースケースについて整理する。ユースケースパターンを整理するためのフォーマットを図 3-3-3-1 に示す。

<sup>16</sup> 先端的サービスの一部の機能を提供するサービス

<sup>17</sup> 個人が利用するアプリケーション (個人が利用可能な個人認証システムを保有する)

<sup>18</sup> 個人が利用する個人アプリ以外のサービス (個人が利用可能な個人認証システムを保有しない)

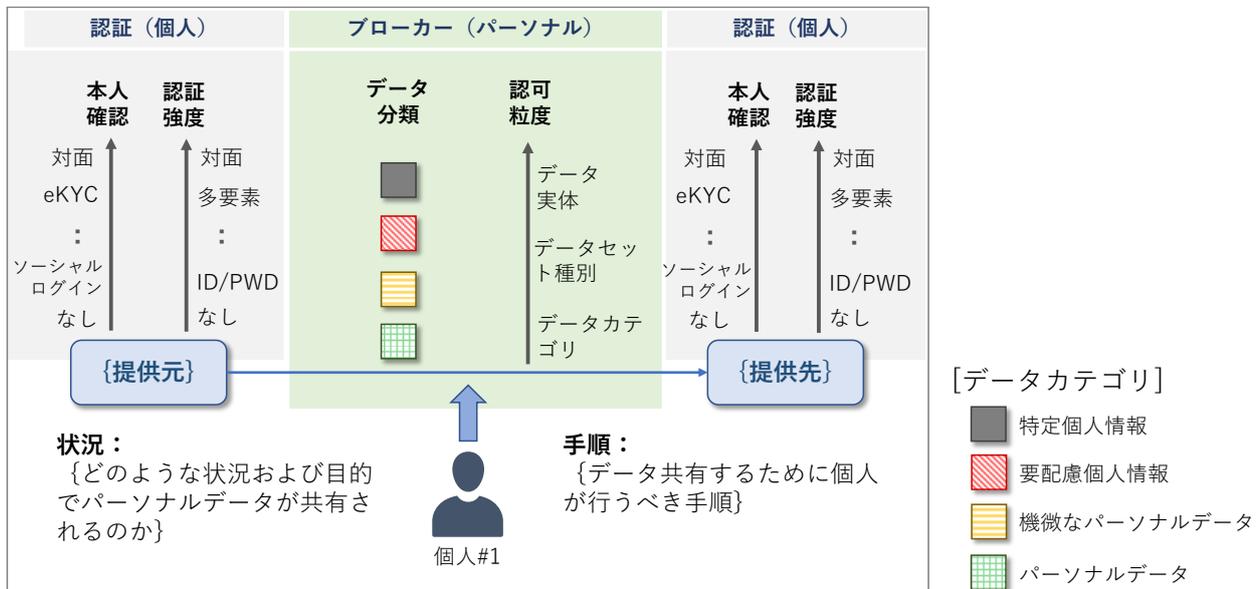


図 3-3-3-1 ユースケース整理の考え方

既にパーソナルデータを提供してサービス A（提供元）を利用している個人#1 が、別のサービス B（提供先）を利用するにあたり、サービス A からサービス B にパーソナルデータを連携させるパターンを基本として考える。この際に必要となる機能は「認証（個人）」及び「ブローカー（パーソナル）」である。

まず、認証（個人）は、サービス提供組織において個人が間違いなく本人であることを確認・証明する機能であり、その過程で個人に ID が付与されるが、ID 付与のルールは各地域で稼働するサービスにより異なるため、公認モジュールとして画一的に技術要件を決定することは望ましくない。また、認証（個人）がブローカー（パーソナル）と連携するためには、流通するデータ種別によって本人確認レベル及び認証強度を使い分けることになるが、そこで用いられる eKYC や各種認証システムはセキュリティの観点から競争領域として整備することが望ましい。そのため、認証（個人）は本調査で選定するビルディングブロックから除外している。

次に、ブローカー（パーソナル）では、連携させるデータの分類及び認可粒度を設定する必要がある。

データ分類は、①マイナンバーを含む「特定個人情報」、②連携させる際に事前の本人同意が法的に定められている「要配慮個人情報」、③確かな定義は定まっていないが、テクノロジーの進化や世論の判断等により、取り扱う上でレピュテーションリスク<sup>19</sup>が発生する「機微なパーソナルデータ」、④その他一般の「パーソナルデータ」の 4 つに分類した。

認可粒度とは、個人がパーソナルデータのどこまで把握及び認可したいかを定める尺度であり、データ実体、データセット及びデータカテゴリの 3 つに図 3-3-3-2 のように分類した。例えば、個人の健康診断データであれば、特定の健診日の心電図データのみ等、具体的なデータ中身まで指定して共有する場合は「データ実体」、全ての健診日の心電図データ一式を共有する場合は「データセット」、③心電図データ以外の健診データも共有する場合は「データカテゴリ」となる。

<sup>19</sup> ステークホルダーのネガティブな評判（＝レピュテーション）が広がることにより、様々な影響を受ける危険性のこと

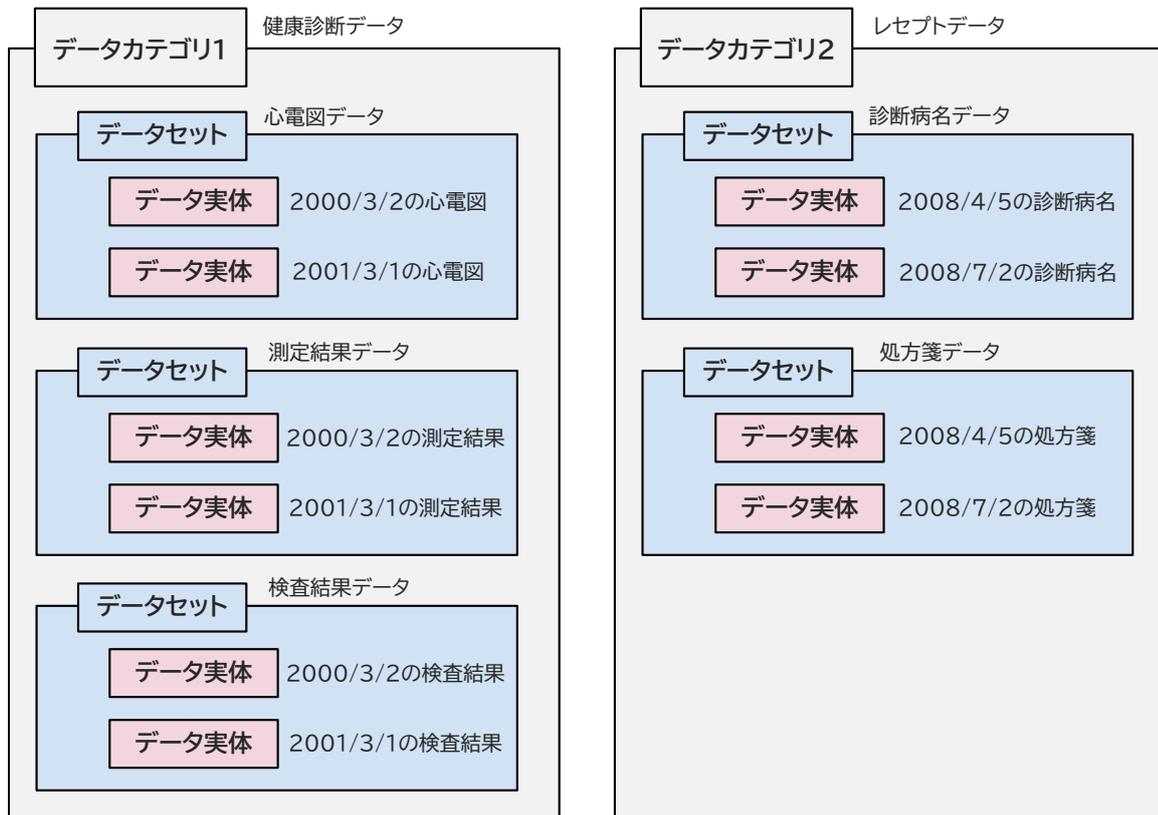


図 3-3-3-2 認可粒度（医療関連データの場合）

また、データ分類と認可粒度に加え、「データ管理の透明性」も考慮する必要がある。なぜなら、実際に個人がサービスを利用するにあたり、自らのパーソナルデータがどのような状況及び目的で共有されるのか、そして個人がデータ共有するために行うべき手順が明らかになっていないと、データ流通の同意が取れないからである。

ここで、データ管理の透明性を考慮する上で必要となる「蓄積」、「蓄積同意」、「共有」、「共有同意」について表 3-3-3-1 のように定義する。

表 3-3-3-1 データ管理に関する用語一覧

用語	説明
蓄積	サービス提携組織が保有するパーソナルデータの一部または全てを共有同意に基づく共有が可能な状態にすること
蓄積同意	個人がサービス提携組織に対して、自身のパーソナルデータを蓄積することを許可すること
共有	サービス提携組織が他組織が蓄積したパーソナルデータを利用すること
共有同意	個人がサービス提携組織に対して、蓄積された自身のパーソナルデータを共有することを許可すること

以上のことから、代表的なユースケースパターンを5つに分けて整理する。

(1) サービス間のパーソナルデータ共有 (1対1)

都市 OS 導入当初に必要なシンプルなユースケースであり、個人が状況を理解することは容易である。

(図 3-3-3-3)

例えば、個人#1 の氏名、住所及び生年月日を登録して利用する地域のポイントカードアプリ A に蓄積された個人#1 の購買データを、別のアプリ Z に共有することで個人#1 はパーソナライズされたオススメ観光情報が受け取れる場合に該当する。

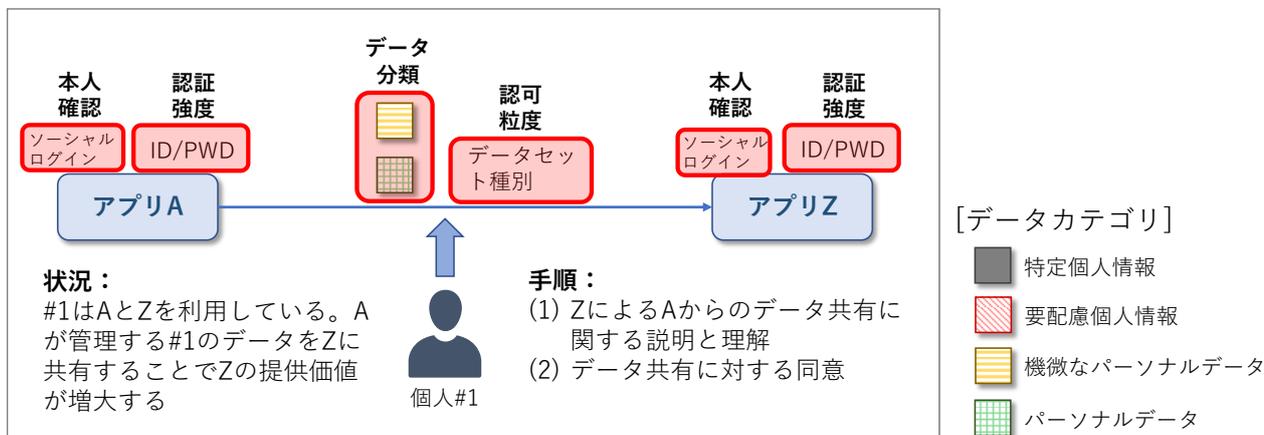


図 3-3-3-3 サービス間のパーソナルデータ共有 (1対1)

(2) サービス間の要配慮個人情報共有 (1対1)

先端的サービスの高度化に伴い必要となるユースケースであるが、個人が状況を理解することは容易である。(図 3-3-3-4)

例えば、個人#1 が自治体 A において子育てに関する要配慮個人情報を含むデータ（予防接種歴や健康診断スケジュール等）を管理するアプリ A を使っていたが、別の自治体 B に転居することになり、アプリ A で管理していたデータを別のアプリ B に引き継ぐ場合に該当する。ここでは、共有するデータ実体の内容を確認することで、個人#1 は安心して要配慮個人情報を含むデータを共有することが可能となる。

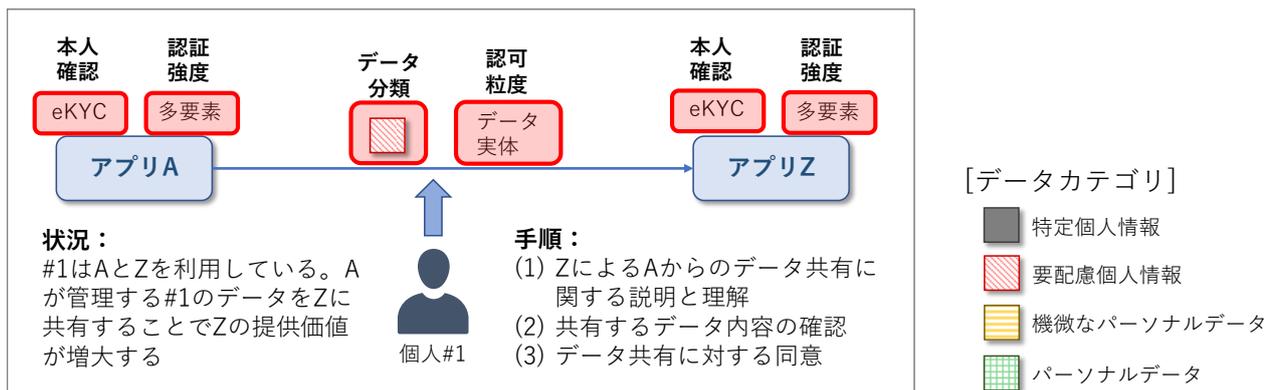


図 3-3-3-4 サービス間の要配慮個人情報共有 (1対1)

(3) 複数サービスからのパーソナルデータ共有 (N 対 1、要配慮個人情報を含まない)

都市 OS 導入から数年が経過し、個人が利用するサービスが増加してくると必要になるユースケースであり、個人が状況を理解することが難しくなる。(図 3-3-3-5)

例えば、ネットスーパーアプリ A の持つ商品購買履歴と、銀行アプリ B の持つ口座データを家計簿アプリ Z に共有することで、Z において個人#1 の消費及び資産の変動が把握可能になる場合が該当する。

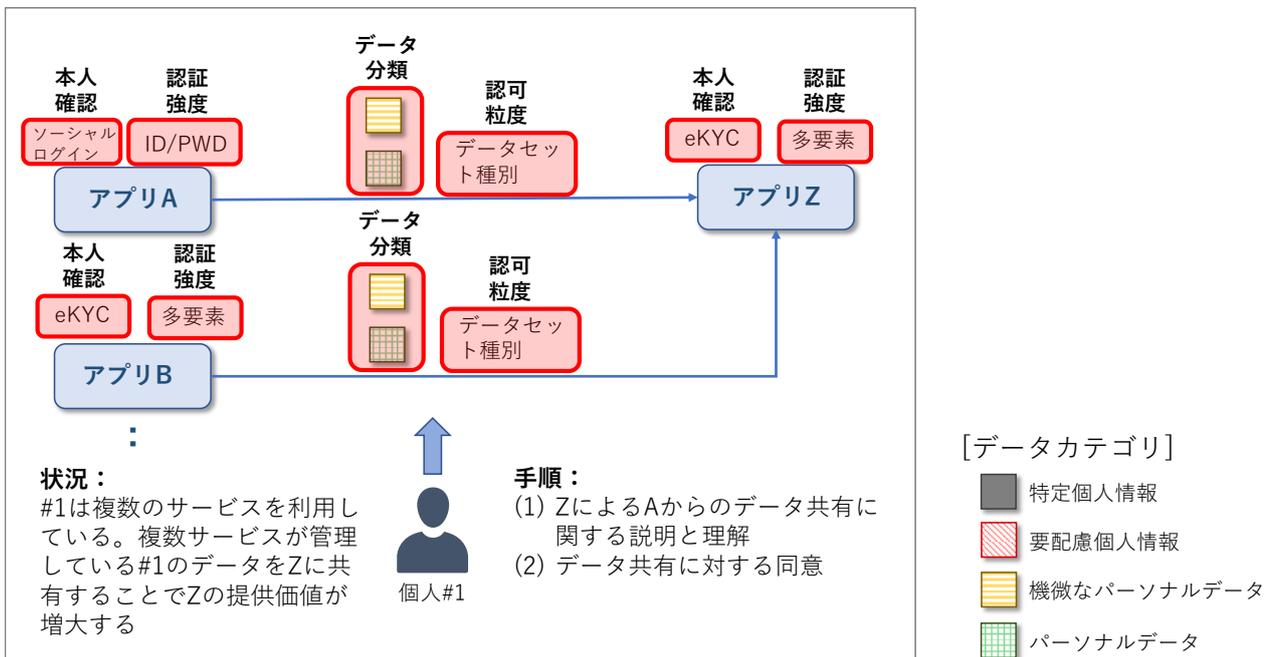


図 3-3-3-5 複数サービスからのパーソナルデータ共有 (N 対 1、要配慮個人情報を含まない)

(4) 複数サービスからのパーソナルデータ共有 (N 対 1、要配慮個人情報を含む)

こちらも都市 OS 導入から数年が経過し、個人が利用するサービスが増加してくると必要になるユースケースであり、個人が状況を理解することが難しくなる。(図 3-3-3-6)

例えば、個人#1 の日々の食事情報を記録するアプリ A の持つ食事履歴データと、病院 B の持つ個人#1 の健康診断結果データを医療サービス Z に共有することで、Z からパーソナライズされた運動や食事の提案が受けられる場合が該当する。要配慮個人情報を含むため、プライバシー保護対策が重要となる。

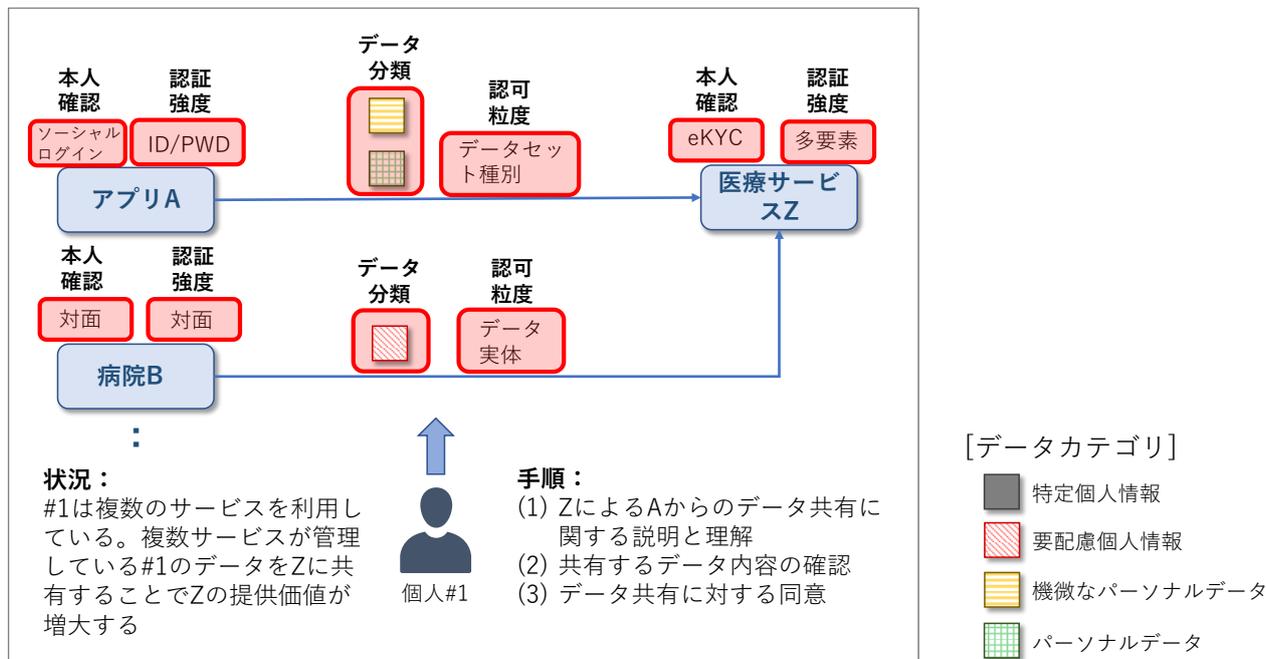


図 3-3-3-6 複数サービスからのパーソナルデータ共有 (N 対 1、要配慮個人情報を含む)

(5) 代理人によるパーソナルデータ共有 (1 対 1、要配慮個人情報を含む) ※N 対 1 も必要

責任能力のない未成年や高齢者が安心してサービスを利用するために必要なユースケース。(図 3-3-3-7)

例えば、親#2 の管理下で子#1 が利用している健康管理アプリ A のデータを睡眠管理アプリ Z に共有することで、子#1 はパーソナライズされた睡眠習慣の提案を受ける場合が該当する。ここでは、代理関係の構築、解消、代理操作のトレース等、透明性を考慮した機能及び運用が重要となる。

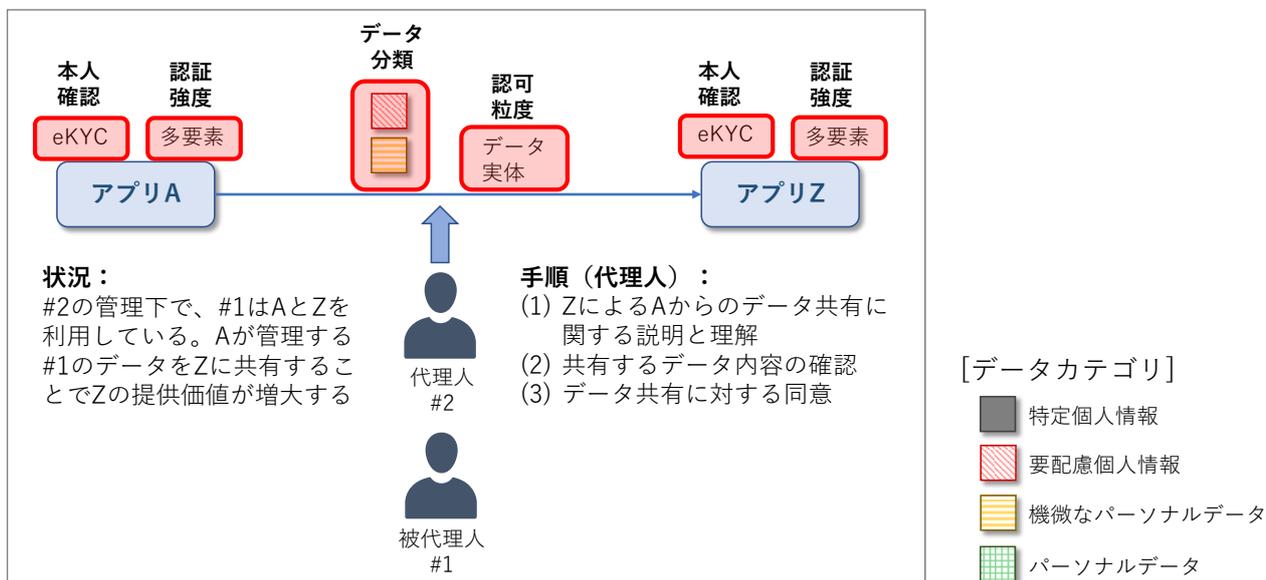


図 3-3-3-7 代理人によるパーソナルデータ共有 (1 対 1、要配慮個人情報を含む)

### 3-3-4. パーソナルデータ流通に必要な要件

3-3-3. を踏まえて、パーソナルデータの流通を担うブローカー（パーソナル）に必要な要件を、ステークホルダー別に抽出する。

なお、本調査では、パーソナルデータのうち要配慮個人情報及び特定個人情報の流通に係る機能は検討対象外とした。理由として、本調査は、3-4-1. にて後述のとおり、データ連携基盤において OSS として公開する範囲のビルディングブロックの要件を整理するものであり、要配慮個人情報及び特定個人情報のような機微性の高い情報を OSS のみで取り扱うことは、情報管理の観点でリスクを否めないためである。加えて、個人による要配慮個人情報及び特定個人情報の提供に関する手順や合意プロセスは、現時点において利用可能な OSS で標準化されていない。以上のことから、要配慮個人情報及び特定個人情報のデータ流通を OSS のみで実現することは現時点では難しく、要件の検討対象外と整理した。

初めに、3-3-3. で整理したユースケースから、パーソナルデータ流通への要求事項を整理する。各ユースケースにおいて、パーソナルデータの流通に対し個人に課される手順の一覧を表 3-3-4-1 に示す。下記表によると、いずれのユースケースにおいても、パーソナルデータの流通には手順(1)「データ蓄積に関する説明と理解」、手順(2)「データ共有に関する説明と理解」、手順(3)「データ蓄積に対する同意」、及び手順(5)「データ共有に対する同意」が求められる。加えて、要配慮個人情報の流通には、手順(4)「共有するデータ内容の確認」が必要となる。ここで、前述のとおり本調査では要配慮個人情報の流通は検討対象外とするが、手順(4)は、要配慮個人情報以外のパーソナルデータの流通においても、データ流通の透明性を示しレピュテーションリスクを下げるため、かつ利用者が安心してパーソナルデータを流通させるために必要である。よって、利用者がデータの内容確認を行う手段として提供されることが望ましい。以上のことから、手順(4)に係る機能は、要配慮個人情報の流通に限定されるものではないと整理し、本調査の検討対象とした。

表 3-3-4-1 パーソナルデータ流通の各ユースケースで求められる手順

(○：必要、△：ある方が望ましい)

手順 ユース ケース 番号	1	2	3	4	5
	サービス間のパーソナルデータ共有 (1対1)	サービス間の要配慮個人情報共有 (1対1)	複数サービスからのパーソナルデータ共有 (N対1、要配慮個人情報を含まない)	複数サービスからのパーソナルデータ共有 (N対1、要配慮個人情報を含む)	代理人によるパーソナルデータ共有 (1対1、要配慮個人情報を含む)
(1) データ蓄積に関する説明と理解	○	○	○	○	○
(2) データ共有に関する説明と理解	○	○	○	○	○
(3) データ蓄積に対する同意	○	○	○	○	○
(4) 共有するデータ内容の確認	△	○	△	○	○
(5) データ共有に対する同意	○	○	○	○	○

表 3-3-4-1 ならびに 3-3-3. を踏まえて、各手順を実現するためにパーソナルデータ流通全体へ要求される事項を以下のとおり整理した。これらの要求事項を実現する機能は、パーソナルデータを提供する個人がより安心感を得ることを考慮し、データ提供元やデータ提供先のいずれでもなく、中立的なプラットフォーム運営組織により提供されることが望ましい。なお、ステークホルダーに関する用語は表 3-3-1-1 表 3-3-3-1 に準ずる。パーソナルデータの蓄積、共有に関連する用語は表 3-3-3-1 のとおり定義される。

- ・個人が、パーソナルデータの共有及び蓄積に関する説明を事前に得られ、内容を理解できること  
データ管理の透明性を確保するため、あるサービスやサービスアセットに対してパーソナルデータの蓄積や共有を求めるとき、サービス提供組織またはサービス提携組織は、当該データが蓄積または共有される前に、個人に対して当該サービスやサービスアセットの内容を説明する先端的サービス管理手段及びサービスアセット管理手段を持つこと。この要求事項は、サービス提供組織及びサービス提携組織に必要とされる。
- ・個人が、共有するパーソナルデータの内容を確認できること  
データ管理の透明性を確保するため、パーソナルデータが蓄積または共有されるとき、個人は対象となるパーソナルデータのデータセット種別、件数、蓄積元または共有元のサービス提携組織、共有先のサービス提携組織、蓄積を行ったサービスアセット、共有された時刻、利用目的について確認できる、パーソナルデータ管理手段を持つこと。パーソナルデータのデータ実体については、機微なパーソナルデータが共有されるとき、個人がその内容を確認できる手段を持つことが望ましい。この要求事項は、個人に必要とされる。
- ・個人が、パーソナルデータの共有及び蓄積に対する同意を自ら管理できること  
個人がパーソナルデータの共有及び蓄積に関する同意状態を、自ら管理できる同意管理手段を持つこと。同意状態の管理は、オプトイン、オプトアウトの両方を含むこと。加えて、同意管理手段は、データの分類及び認可粒度に応じて提供されること。この要求事項は、個人に必要とされる。

上記を基に、パーソナルデータ流通のために、ブローカー（パーソナル）に対して個人、サービス提供組織、サービス提携組織が必要とする要件を下記に示す。

#### (1) 個人に必要な要件

##### (a) 同意管理

##### (ア) 蓄積同意機能

本機能の要件は、個人が、サービス提携組織（アプリ）に対して、自身のパーソナルデータの蓄積を許可（同意）する、または許可しない（非同意）とき、その同意の状態を管理するためのものである。同意の状態には、オプトインとオプトアウトの両方を含むこと。蓄積同意管理では、個人が以下について理解した上で、蓄積同意の状態を決定できることが求められる。

- ・先端的サービスとサービスアセットの関係
- ・サービスアセットが提供する機能の内容
- ・サービスアセットが蓄積を行う目的と対象となるパーソナルデータのデータセット種別

ここで「データセット種別」は、図 3-3-3-2 の分類を参照のこと。本調査における「蓄積」では、パーソナルデータは「共同利用」の位置づけであり「第三者提供」は行われないため、対象となるデータの蓄積同意において、個人によるデータ実体単位の認可は必須ではない。よって、

透明性のあるパーソナルデータの流通を担保しつつ、個人の手続きが煩雑になりすぎないように、蓄積同意機能では、データセット種別単位の認可粒度を設定することが望ましい。

#### (イ) 共有同意機能

本機能の要件は、個人が、サービス提携組織（アプリ）に対して、蓄積された自身のパーソナルデータを共有することを許可（同意）する、または許可しない（非同意）とき、その同意の状態を管理するためのものである。同意の状態には、オプトインとオプトアウトの両方を含むこと。共有同意管理では、個人が以下について理解した上で、共有同意の状態を決定できることが求められる。共有同意機能においても、蓄積同意機能と同様に、データセット種別単位の認可粒度を設定することが望ましい。

- ・先端的サービスの内容
- ・先端的サービスとサービスアセットの関係
- ・サービスアセットが提供する機能の内容
- ・サービスアセットが共有を求める目的と対象となるパーソナルデータのデータセット種別

加えて、サービスアセットが機微なパーソナルデータの共有を個人に求める場合、共有同意機能は以下を提供できることが推奨される。

- ・個人がパーソナルデータの共有に対する同意状態をデータ実体単位で管理できること

#### (b) パーソナルデータ管理

##### (ア) パーソナルデータ所在管理機能

本機能の要件は、個人が蓄積された自身のパーソナルデータの所在を把握するためのものである。パーソナルデータ所在管理機能では、個人が以下について把握できることが求められる。

- ・蓄積を行ったサービス提携組織（データ保有）
- ・蓄積を行ったサービスアセット
- ・蓄積されたデータセット種別
- ・蓄積されたデータの件数

加えて、個人がデータ実体単位でパーソナルデータの共有に対する同意状態を管理する必要がある場合は、以下の機能を提供することが望ましい。

- ・個人が蓄積された自身のパーソナルデータの内容を確認できること

##### (イ) アクセスログ機能

本機能の要件は、個人が、蓄積された自身のパーソナルデータのサービス提携組織における共有状態を把握するためのものである。アクセスログ機能では、個人が以下について把握できることが求められる。

- ・共有元のサービス提携組織（データ保有）
- ・共有先のサービス提携組織（データ利用）
- ・共有された時刻
- ・共有されたデータのデータセット種別
- ・共有されたデータの件数

以上のことから、個人には同意管理及びパーソナルデータ管理に関する機能が必要となる。これらに加え、将来的な機能拡張として、「再同意」ならびに「代理人によるパーソナルデータ共有」が想定される。

「再同意」は、複数のパーソナルデータを取得する場合の取得項目の変更など、パーソナルデータの取得条件に変更が生じた際に、改めて個人同意を得るための機能である（データ連携基盤技術報告書 表 9-3-2-1 項番 3）。将来、数多くのパーソナルデータが広く流通される場面では、同意管理において再同意機能も考慮すべきである点に留意されたい。

また、「代理人によるパーソナルデータ共有」は、責任能力のない未成年や高齢者が代理人を通してパーソナルデータ提供に関する同意管理を行うための機能である（3-3-3(5)）が、適切な代理人の認証手続きなど、ブローカー（パーソナル）のみでなく、トラストサービスへの連携も想定される。そこで、代理人によるパーソナルデータの共有プロセスを図式化すると、以下の図 3-3-4-1 のようになる。「フェーズ 1：本人確認」にて本人性の証明と、トラストサービス上での本人確認、個人登録を実施した後、「フェーズ 2：代理関係の構築」にて代理人と被代理人の間の代理関係を登録する。ここで、「本人性の証明」とは、免許証やマイナンバーカード等によってサービス利用者本人であることを証明する行為を指す。代理人が、被代理人のパーソナルデータ共有に関して代理操作を行う場合は、「フェーズ 3：代理操作（データ共有）」のフローに則りブローカー（パーソナル）の「個人認証連携」や「データ共有処理」と適切なインタラクションを行う必要がある。代理関係が解消される際は、「フェーズ 4：代理関係の解消」のフローに従い処理が行われる。

代理人によるパーソナルデータ共有プロセス

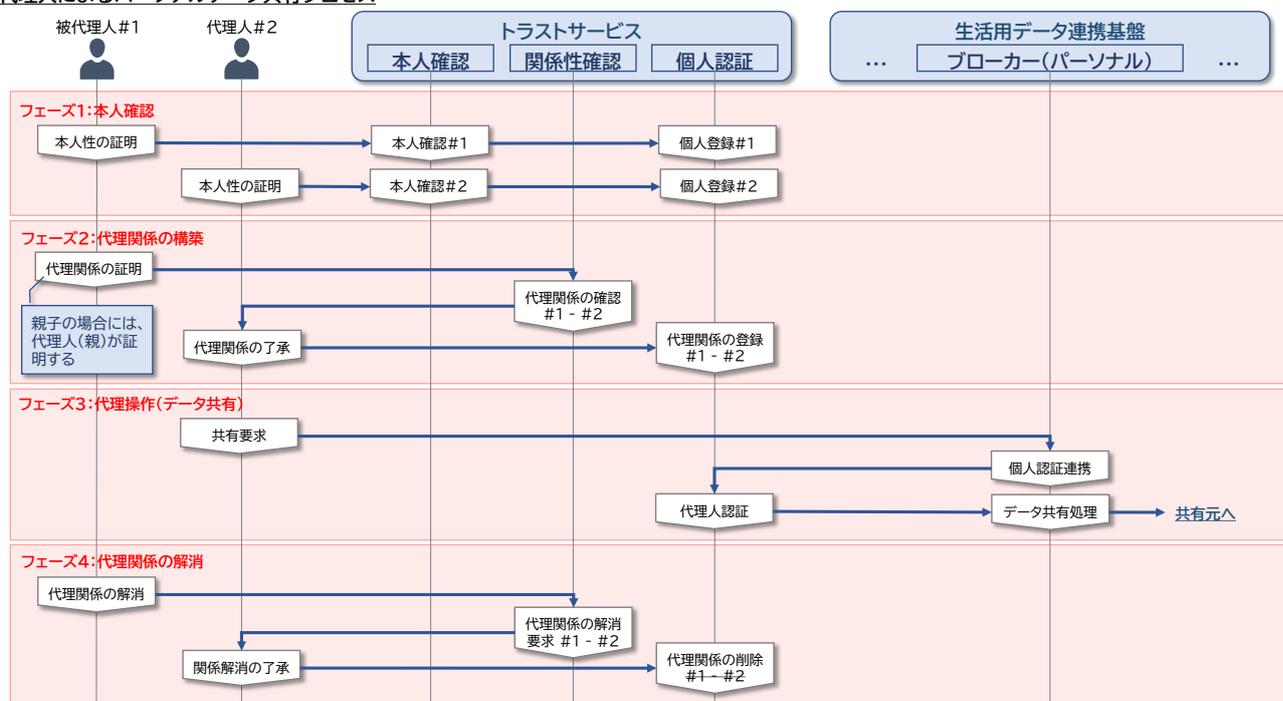


図 3-3-4-1 代理人によるパーソナルデータの共有プロセス

図 3-3-4-1 から、代理人によるパーソナルデータの共有プロセスには、トラストサービスにおける「本人確認、関係性確認、個人認証」の機能が必要になり、それらに応じたブローカー（パーソナル）の機能として、「個人認証連携」「データ共有処理」が必要となることがわかる。ただし、ブローカー（パーソナル）に要求されるこれらの機能は、トラストサービスの「本人確認、関係性確認、個人認証」に応じて詳細が定まるものであるため、詳細検討は将来的な課題とし、本調査の対象外と整理した。

## (2) サービス提供組織に必要な要件

### (a) ブローカー（非パーソナル）と同等の機能

ブローカー（パーソナル）がデータ参照の要求に応えるために、ブローカー（非パーソナル）と同等の以下の要件が必要となる。

#### (ア) API 仕様

REST 等の標準ルールに沿った API を提供可能であること。（表 3-2-1 ブローカー要件（非パーソナル）表 3-2-1 に掲載）

#### (イ) データ分散

データ利用者からデータ参照の要求を受け付け、外部サービスが保持するデータを返却可能なこと。（表 3-2-1 ブローカー要件（非パーソナル）表 3-2-1 に掲載）

#### (ウ) データ蓄積

データ提供者からデータを受け付け、データストア機能に当該データを蓄積可能なこと。また、データ利用者からデータ参照の要求を受け付け、データストア機能に蓄積されたデータを返却可能なこと。（表 3-2-1 ブローカー要件（非パーソナル）表 3-2-1 に掲載）

なお、ブローカー（非パーソナル）の要件であるイベント処理及びデータ変換は、パーソナルデータの取り扱いにおいて必須ではないため、ブローカー（パーソナル）においては必要に応じて実装することとする。

### (b) 先端的サービス管理

#### (ア) 先端的サービス定義機能

本機能の要件は、サービス提供組織が、自らが提供する先端的サービスを定義するためのものである。サービス提供組織は、以下を実施できることが求められる。

- ・先端的サービスの内容に関する個人向けの説明を定義できること
- ・先端的サービス定義に提携するサービスアセットを追加できること

## (3) サービス提携組織に必要な要件

### (a) サービスアセット定義機能

本機能の要件は、サービス提携組織が、自らが提供するサービスアセットを定義するためのものである。サービス提携組織は、以下を実施できることが求められる。

- ・サービスアセットの内容に関する個人向けの説明を定義できること
- ・サービスアセットが蓄積可能なデータセット種別を定義できること
- ・サービスアセットが共有を求めるデータセット種別を定義できること

以上のことから、ブローカー（パーソナル）の要件は、個人、サービス連携機能、サービス連携組織毎に、表 3-3-4-2 のように整理される。なお、ブローカー（パーソナル）は、一部ブローカー（非パーソナル）と同様の要件を必要とし、加えて、パーソナルデータ流通に特化した追加要件が必要となる。ブローカー（非パーソナル）の要件は表 3-2-1 に準ずることとし、以下では、本章で抽出されたブローカー（パーソナル）に要求される要件を示す。

表 3-3-4-2 ステークホルダー別ブローカー要件（パーソナル）

ステークホルダー	分類	機能	要件	必須	推奨
個人	同意管理	蓄積同意	個人が「サービス提携組織（アプリ）による蓄積」に対する自身の同意状態を、「データセット種別」の認可粒度で管理できる。	○	
		共有同意	個人が「サービス提携組織（アプリ）による共有」に対する自身の同意状態を、「データセット種別」の認可粒度で管理できる。	○	
			個人が「サービス提携組織（アプリ）による共有」に対する自身の同意状態を、「データ実体」の認可粒度で管理できる。		○
	パーソナルデータ管理	パーソナルデータ	個人が蓄積された自身のパーソナルデータの所在を把握できる。	○	
		所在管理	個人が蓄積された自身のパーソナルデータの内容をデータ実体単位で確認できる。		○
		アクセスログ	個人が蓄積された自身のパーソナルデータの共有状況を把握できる。	○	
サービス提供組織	ブローカー（非パーソナル） 同等機能	API仕様	表 3-2-1 に準ずる。	○	
		データ分散	表 3-2-1 に準ずる。	○	
		データ蓄積	表 3-2-1 に準ずる。	○	
	先端的サービス管理	先端的サービス定義	サービス提供組織が先端的サービスを定義できる。	○	
サービス提携組織	サービスアセット管理	サービスアセット定義	サービス提携組織がサービスアセットを定義できる。	○	

既存検討との整合を確認するため、表 3-3-4-2 のとおり整理したブローカー（パーソナル）の機能と、データ連携基盤技術報告書で検討された、透明性を重視したパーソナルデータ管理に必要な機能概要案（データ連携基盤技術報告書 表 9-3-1-1）、ならびに継続的なパーソナルデータの品質管理のために必要な機能概要案（データ連携基盤技術報告書 表 9-3-2-1）との対応関係を、表 3-3-4-3 と表 3-3-4-4 にそれぞれ示す。

表 3-3-4-3 及び表 3-3-4-4 より、データ連携基盤技術報告書で検討された機能概要案は、パーソナルデータの管理に必要なブローカー（パーソナル）以外の機能により提供されることが望ましい機能（開示請求や認証（組織）、データカタログ、トラストサービス等）を除き、本調査で抽出したブローカー（パーソナル）の機能に包含されることがわかる（表 3-3-4-4 項番 3 の「再同意」に係る機能は、前述のとおり、同意管理の将来課題として整理している）。以上のことから、表 3-3-4-2 のとおり整理したブローカー（パーソナル）の機能は、データ連携基盤技術報告書で整理されたパーソナルデータの管理に必要な機能概要案と整合することがわかる。

表 3-3-4-3 透明性を重視したパーソナルデータ管理に必要となる機能概要案と  
ブローカー（パーソナル）機能の対応

透明性を重視したパーソナルデータ管理に必要となる機能概要案 (データ連携基盤技術報告書 表 9-3-1-1)					ブローカー (パーソナル) 機能
項 番	発生タイミング	ステーク ホルダー	課題	機能概要案	
1	サービス利用 申込時	サービス利用者	サービス利用者が、自身のパーソナルデータの利用に関する同意を先端的サービス事業者ごとに実施できること	先端的サービス事業者が、サービス利用者のオプトイン・オプトアウトの状態を把握できること	<ul style="list-style-type: none"> <li>蓄積同意</li> <li>共有同意</li> </ul>
				サービス利用者が、自身のパーソナルデータの利用に関する同意を先端的サービス事業者ごとに実施できること	<ul style="list-style-type: none"> <li>蓄積同意</li> <li>共有同意</li> </ul>
2	サービス利用中	サービス利用者	サービス利用者が、自身のパーソナルデータに対するアクセス記録を先端的サービス事業者ごとに、いつでも、簡単に確認できること	先端的サービス事業者が、パーソナルデータの利用履歴をサービスごとに取得できること	<ul style="list-style-type: none"> <li>パーソナルデータ所在管理</li> <li>アクセスログ</li> </ul>
				サービス利用者が、自身のパーソナルデータに対するアクセス履歴を先端的サービス事業者ごとに確認できること	<ul style="list-style-type: none"> <li>パーソナルデータ所在管理</li> <li>アクセスログ</li> </ul>
3	サービス利用中	サービス利用者	サービス利用者が、自身のサービス利用記録をサービスごとに確認できること	先端的サービス事業者が、サービス利用記録を管理できること	対象外 (サービス マネジメント)
				サービス利用者が、自身のサービス利用記録を先端的サービス事業者ごとに確認できること	対象外 (サービス マネジメント)

透明性を重視したパーソナルデータ管理に必要となる機能概要案 (データ連携基盤技術報告書 表 9-3-1-1)					ブローカー (パーソナル) 機能
項番	発生タイミング	ステークホルダー	課題	機能概要案	
4	サービス利用中	サービス利用者	サービス利用者が、自身の機微なパーソナルデータの利用及び利用タイミングに関する同意を先端的サービス事業者職員の役割ごとに実施できること	先端的サービス事業者が、職員が利用する機微なパーソナルデータとその利用タイミングに関する利用権限を職員の役割ごとに管理できること	対象外 (認証(組織)、 トラストサービス)
				サービス利用者が、自身の機微なパーソナルデータ利用及び利用タイミングに関する同意を先端的サービス事業者職員の役割ごとに実施できること	対象外 (認証(組織)、 トラストサービス)
5	サービス利用中	先端的サービス事業者	サービス利用者が、自身のパーソナルデータに関する開示請求を先端的サービス事業者に対してできること	先端的サービス事業者が、サービス利用者からのパーソナルデータに関する開示請求を受け付けられること	対象外 (開示請求)
				サービス利用者が、自身のパーソナルデータに関する開示請求を先端的サービス事業者ごとに実施できること	対象外 (開示請求)
6	サービス利用解約時	サービス利用者	サービス利用者による利用解約時に、サービス利用規約に基づき自身のパーソナルデータが正しく処理(返却・削除など)されたこと	先端的サービス事業者が、サービスの利用解約を受け付けられること	・蓄積同意 ・共有同意
				サービス利用者が、サービスの利用解約を実施できること	・蓄積同意 ・共有同意

透明性を重視したパーソナルデータ管理に必要な機能概要案 (データ連携基盤技術報告書 表 9-3-1-1)					ブローカー (パーソナル) 機能
項番	発生タイミング	ステークホルダー	課題	機能概要案	
			とを確認できること	サービス利用者が、サービスの利用解約時にサービス利用規約に基づき自身のパーソナルデータの返却を受けられること	<ul style="list-style-type: none"> <li>・パーソナルデータ所在管理</li> <li>・アクセスログ</li> </ul>
				サービス利用者が、サービスの利用解約時にサービス利用規約に基づき自身のパーソナルデータが削除されたことを確認できること	<ul style="list-style-type: none"> <li>・パーソナルデータ所在管理</li> <li>・アクセスログ</li> </ul>
7	サービス利用解約時	サービス利用者	サービス利用者による利用解約後に、先端的サービス事業者間で自身のパーソナルデータが連携されていないことを確認できること	サービス利用者が、解約済みの先端的サービス事業者間で自身のパーソナルデータの連携が停止していることを確認できること	<ul style="list-style-type: none"> <li>・パーソナルデータ所在管理</li> <li>・アクセスログ</li> </ul>

表 3-3-4-4 継続的なパーソナルデータの品質管理のため必要となる機能概要案とブローカー (パーソナル) 要件の対応

継続的なパーソナルデータの品質管理のために必要となる機能概要案 (データ連携基盤技術報告書 表 9-3-2-1)					ブローカー (パーソナル) 要件
項番	発生タイミング	ステークホルダー	課題	機能概要案	
1	サービス利用受付時	先端的サービス事業者	サービス利用者によるサービス利用申込時に、先端的サービス事業者ごとに管理している既存の個人 ID の紐づけが正しく実施されること	サービス利用申込時に、先端的サービス事業者が、先端的サービス事業者間で保有する既存の個人 ID 同士の紐づけを実施できること	対象外 (トラストサービス)

継続的なパーソナルデータの品質管理のために必要となる機能概要案 (データ連携基盤技術報告書 表 9-3-2-1)					ブローカー (パーソナル) 要件
項番	発生タイミング	ステークホルダー	課題	機能概要案	
				先端的サービス事業者が保有する既存の個人 ID の本人特定は、先端的サービス事業者が行うこと	対象外 (トラストサービス)
				サービス利用申込時に、先端的サービス事業者が、誤った個人 ID の紐づけを実施した場合に訂正できること	対象外 (トラストサービス)
				サービス利用申込時に、先端的サービス事業者が、個人 ID の紐づけを実施できなかった場合にサービス利用者に通知できること	対象外 (トラストサービス)
2	サービス利用中	先端的サービス事業者	不正なパーソナルデータ（精度の不正、連携条件の違反）が収集及び連携されることを防止できること	サービス利用者のパーソナルデータ品質を上げるために、サービス利用者の手入力を極力減らし、信頼性の高いデバイス等を使用したデータ収集ができること	対象外 (データカタログ)
3	サービス利用中	先端的サービス事業者	定性的・定量的評価に基づくデータモデルの改善を継続的に行うことができること	パーソナルデータ品質を向上させるために、データセットを定期的に分析評価してデータセットをバージョンアップできること	対象外 (データカタログ)

継続的なパーソナルデータの品質管理のために必要となる機能概要案 (データ連携基盤技術報告書 表 9-3-2-1)					ブローカー (パーソナル) 要件
項番	発生タイミング	ステークホルダー	課題	機能概要案	
				先端的サービス事業者が、データモデルのバージョン管理を行うことができること	対象外 (データカタログ)
				サービス利用者が、追加の個人情報に係る項目が必要になった際には、再同意できること	将来課題 (蓄積同意、共有同意)
				先端的サービス事業者が、個人情報に紐づくデータ項目を含むデータモデルのバージョンアップ後に、サービス利用者が再同意したか否かの状態を把握できること	将来課題 (蓄積同意、共有同意)
				先端的サービス事業者が、新しいバージョンのデータモデルに対して、サービス利用者への追加同意を要求できること	将来課題 (蓄積同意、共有同意)
				サービス利用者が、自身のパーソナルデータの利用に関する同意を行う際、対象となるデータモデルのバージョンを確認できること	対象外 (データカタログ)

なお、パーソナルデータ流通では、個人がデータを流通するプロセスにおいて、個人の本人確認や統合ID発行、個人認証（SSO 含む）といったトラストサービス機能との連携が必要であるが、これらの機能はブローカー（パーソナル）ではなくトラスト関連サービスを担う他の機能群で実現されるものであり、ま

た、2-1-2. (3)で抽出したデータ連携基盤に最低限必要なビルディングブロックに含まれないことから、本調査の対象外とした。同様に、パーソナルデータの流通に関連するが、ブローカー（パーソナル）以外の機能により提供されることが望ましい、開示請求機能、変更請求機能、監査機能についても、本調査の対象外とした。

### 3-3-5. 妥当性検証

前項で整理したブローカー（パーソナル）の要件の妥当性を検証するため、欧州を中心とするスマートシティの国際団体である Open & Agile Smart Cities（以下、OASC とする）が提唱する最小限の相互運用性メカニズム（Minimal Interoperability Mechanisms（以下、MIMs とする））を参照し、このうちパーソナルデータ管理について定めた MIM4-Trust（以下、MIM4 とする）に提案されている要求事項と、ブローカー（パーソナル）の要件の整合性を確認する。

MIM4 は、都市間でパーソナルデータが共有される際の、パーソナルデータの保護、透明性、トラストに関するパーソナルデータ管理のメカニズムを検討することを目的に、2020年1月の Connected Smart City Conference 2020 にて設立されたワーキンググループである。なお、本調査事業の実施時点（2022年3月時点）では、MIM4 の標準仕様は確定しておらず、ステータスとして Capability（要求事項の整理）の段階であることに留意いただきたい。加えて、パーソナルデータ管理に必要な機能への要求事項のうち、データ仲介のためのオープン API については MIM1-Context に、標準データモデルについては MIM2-Data Models にそれぞれ準拠することが求められている。

OASC MIMs のウェブサイトで開催されている Personal Data Management MIM4 Introduction and Specifications では、パーソナルデータ管理の方針として、MyData Global からの提案内容を踏襲している。以下、同書を「パーソナルデータ管理提案書<sup>20</sup>」とする。

MyData Global は非営利団体であり、「パーソナルデータに関する自己決定権を改善することで、個人をエンパワーメントする（<https://mydata.org/about/>）」ことを目的に、人を中心にデザインされたパーソナルデータ管理のアプローチとして、「MyData」を提唱している。MyData では、パーソナルデータ管理の概念として図 3-3-5-1 を掲げている。図 3-3-5-1 のステークホルダーと各々が担う役割を下記に示す。

- Person（個人）：デジタル的に表現されるデータ主体の役割を担う。自身の目的のために、自身のパーソナルデータの使用を管理し、他の個人、サービス、または組織との関係を維持する。
- Operator：パーソナルデータ流通において、システム運用と個人へのツール提供の役割を担う。オペレータは、個人が自身のパーソナルデータに安全にアクセスし、管理し、利用できるようにし、データソースとデータ利用サービス内及びデータソース間のパーソナルデータの流れを制御する。
- Data Source：個人、事業者、データ利用サービスがアクセス及び利用を希望するパーソナルデータの収集、保管、管理に責任を負う役割を担う。パーソナルデータ管理提案書では、データ提供者と同義である。

<sup>20</sup> <http://www.mydatashare.com/oasc-mim4-specification>

- Data Using Service : サービスを提供するために、1 つまたは複数のデータソースからパーソナルデータを処理する責任を負う役割を担う。パーソナルデータ管理提案書では、データ消費者と同義である。

以上のことから、MyData が掲げるパーソナルデータ管理の概念においても、パーソナルデータの流通に際して個人が自身のパーソナルデータの使用を管理することと、図 3-3-5-1 のステークホルダーにおいては、Operator が個人へパーソナルデータのアクセス、管理、利用のための機能を提供していることがわかる。Operator が担う機能は、ブローカー（パーソナル）の要件である同意管理と整合する。

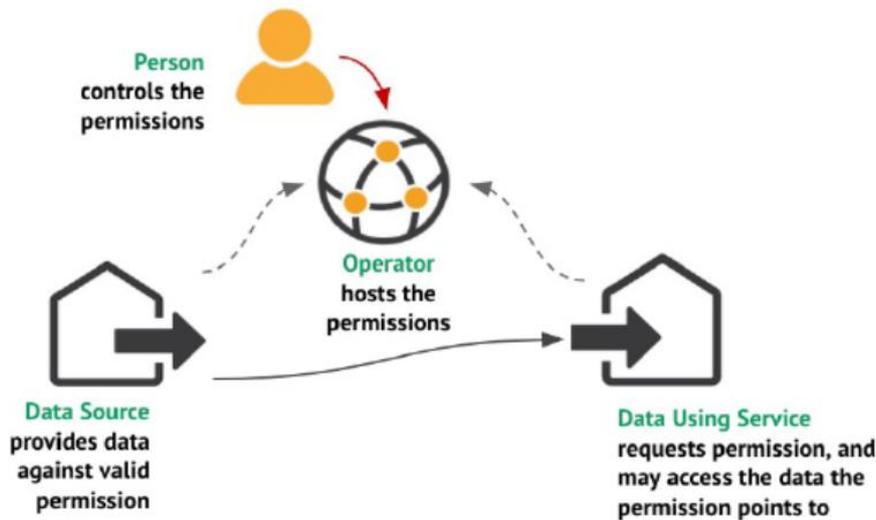


図 3-3-5-1 MyData によるパーソナルデータ管理概念図  
(パーソナルデータ管理提案書 Figure 2 抜粋)

MyData による提案と相互運用性要求を踏まえ、パーソナルデータ管理提案書では、パーソナルデータ管理を次の 4 つのレイヤーで定義している。

- レイヤー1 「Identity and trust network」  
個人デジタル ID、データ選択、データ共有合意と関連づける市民プロフィールやアカウント
- レイヤー2 「Management of data sharing agreements」  
データ共有契約の管理
- レイヤー3 「Personal Data platform」  
パーソナルクラウド、API
- レイヤー4 「Personal data models」  
共有されるパーソナルデータモデル、または異なるモデルの相互マッピング手法

パーソナルデータ管理提案書では、このうちレイヤー2 及びレイヤー3 への要求事項を整理すべく、「Pillar 1 : Connectivity specification for data transfer」と「Pillar 2 : Legal framework for

trust rulebook」の2つのアプローチで調査検討を進めている（図 3-3-5-2）。各アプローチの検討状況と、ブローカー（パーソナル）の機能との対応を以下に示す。

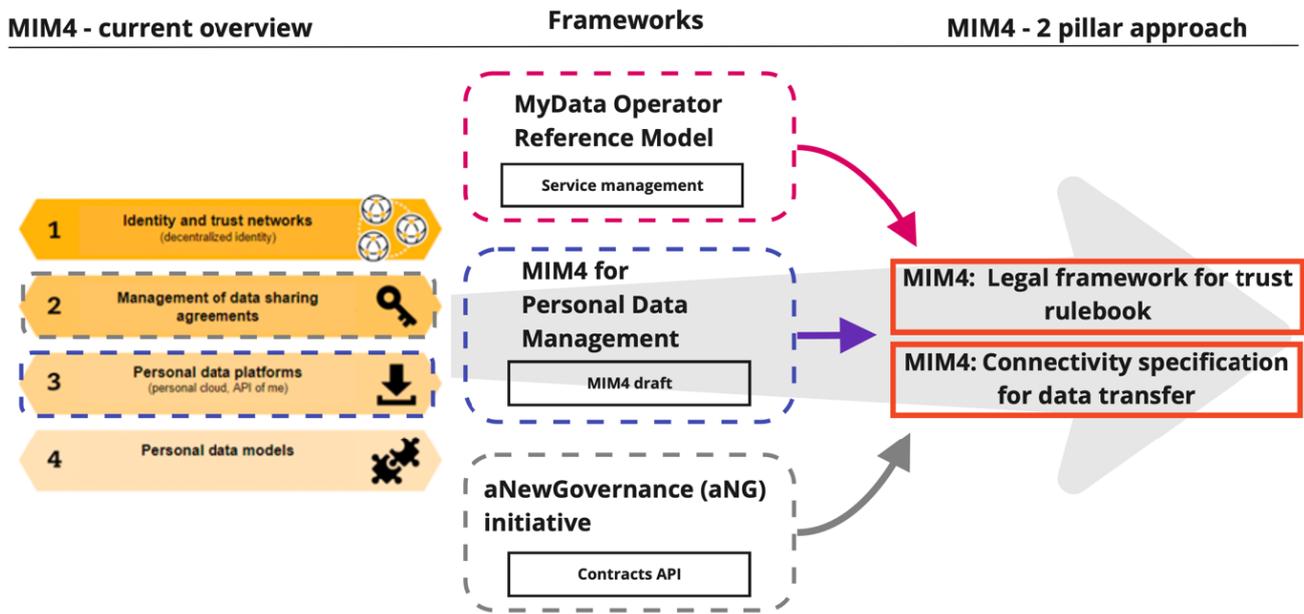


図 3-3-5-2 MIM4 レイヤーと検討アプローチ  
 (パーソナルデータ管理提案書 Figure 17 抜粋)

(1) Pillar 1: Conectivity specification for data transfer

Pillar 1は、将来的に、複数都市間でのパーソナルデータの管理と流通を実現することを目的とし、1つのデータソース（既存のAPIまたはパーソナルデータストレージ）が、複数のOperatorへ同時にデータを提供できるよう、図 3-3-5-3 に示すアーキテクチャを提唱している。図 3-3-5-3 において、MyData Operator は前述のOperatorを指し、ブローカー（パーソナル）の機能における同意管理に整合する。また、図 3-3-5-3 においてConnector（以下、コネクタとする）は、MIM4の接続性要求を備え、複数のOperatorが同じデータソースを使用できるように実装された、オープンソースの代理アクセス機能要素（プロキシコンポーネント）である。コネクタを使用すると、元のデータソースに技術的な変更を加えることなく、単一のData Sourceが複数のOperatorにより参照される。この「コネクタによりData SourceがOperatorにより参照される」という点は、ブローカー（パーソナル）の機能のうち、API仕様、データ分散、データ蓄積と整合する。加えて、パーソナルデータ管理提案書 Part2 4.2.1によると、Data Sourceとの接続においては、全てのパーソナルデータへのアクセスに関するローカルな監査証跡を残す必要がある。これは、ブローカー（パーソナル）の機能であるアクセスログと整合する。

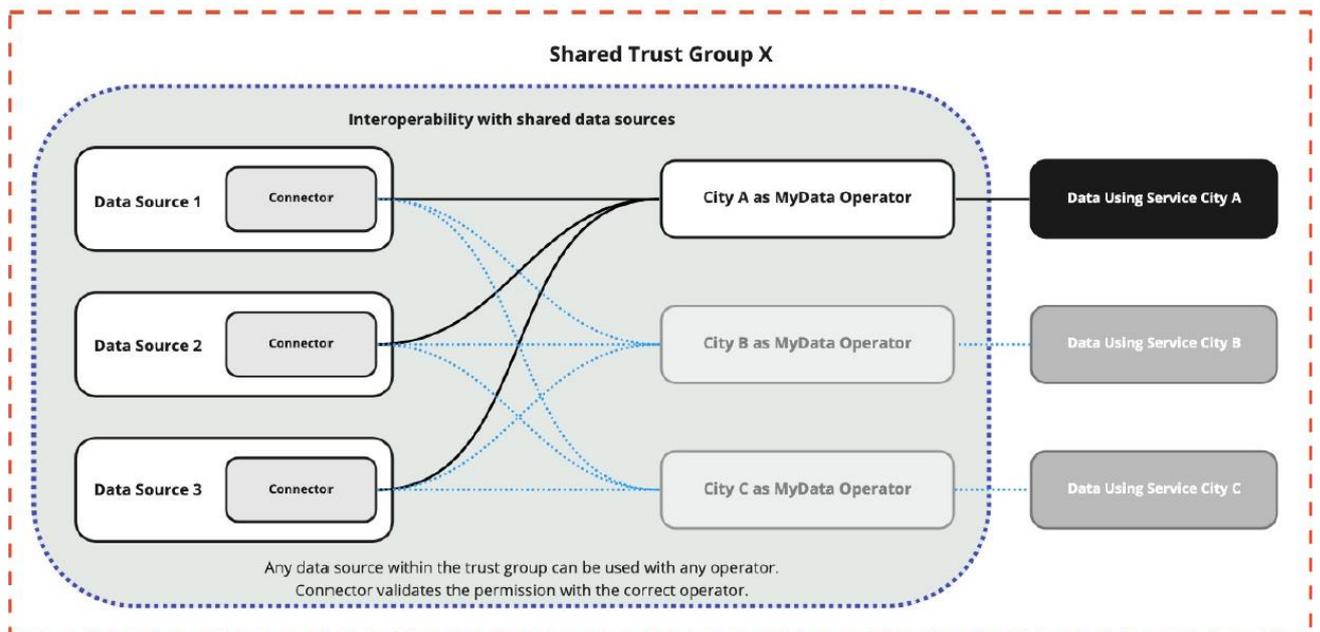


図 3-3-5-3 複数都市間パーソナルデータ流通の論理コンポーネント  
(パーソナルデータ管理提案書 Figure 19 抜粋)

以上のことから、図 3-3-5-3 をブローカー（パーソナル）の機能と比較すると、コネクタはアクセスログ、ブローカー（非パーソナル）同等機能（API 仕様、データ分散、データ蓄積）に、MyData Operator は同意管理に相当する。したが、ブローカー（パーソナル）の機能は、図 3-3-5-3 のコネクタと MyData Operator の統合として捉えることができる。ここで、図 3-3-5-3 には、MyData Operator とコネクタの都市間連携が描かれているが、都市間連携への拡張は、MIM4 においても将来課題として整理されている点に留意いただきたい（パーソナルデータ管理提案書 Part3 1.1（2021 年 5 月版））。

## (2) Pillar 2 Legal Framework for trust rulebook

Pillar 2 は、パーソナルデータを信頼性を確保して流通させるために必要なルールを定めた、法律に基づくフレームワーク（以下、トラストフレームワークとする）を定めることを目的としている。Operator、利用者、データ仲介者が互いに信頼関係を維持しながらデータを共有するためには、データ送信が相互に合意したルールに則して行われていることが保証されることが望ましい。ここでルールとはデータ共有契約等を指し、その内容は、データ共有が行われる国や地域の個人情報保護に係る法律や規制、医療や金融といった産業分野固有の規則等に則る必要がある。加えて、将来、パーソナルデータが複数都市間で効率よく流通されるには、データ共有契約の相互運用性を考慮すべきであり、共通的に参照可能なフレームワークが求められる。MIM4 に則したトラストフレームワークの検討は、Sitra Fair Data Economy Rulebook model や aNewGovernance (aNG) 等で検討が進められている。

トラストフレームワークによるデータ共有契約そのものはブローカー（パーソナル）の要件の対象外であるが、データ共有・蓄積のルールは、サービス提供者やサービス提携者によるパーソナルデータ流通の透明性を確保するために、個人との間で明確にすべきである。ブローカー（パーソナル）への要件としては、同意管理で個人がサービス提供者やサービス提携者から提供されるべき情報や同意状態の管理レベル（データ実態単位、データ種別単位等）の事前合意、パーソナルデータ管理で個人が把握できる情報の事前合意、先端的サービス管理やサービスアセット管理でサービス提携組織やサービス提供組織が個人へ提供できる情報の事前合意をしておくことに相当する。

図 3-3-5-4 に、複数都市間でパーソナルデータが流通するケースでの、トラストフレームワークの適

応範囲（図 3-3-5-4 右側の「Rulebook」で囲まれる範囲）を示す。将来、都市間でパーソナルデータを連携する場合は、相互運用性を考慮し、対象となる都市の Operator やコネクタが共通して参照するトラストフレームワークを整備することが望ましい。加えて、個人がより安心して自身のパーソナルデータを流通させるには、データ流通に係るプラットフォームは、データ提供元やデータ提携先とは独立の、中立的なプラットフォーム運営組織により提供されることが望ましい。これは、Operator やコネクタが Data Source と独立している 図 3-3-5-4 のアーキテクチャとも整合する。ただし、パーソナルデータ流通の都市間連携への拡張は、MIM4 において将来課題として整理されている点に留意いただきたい（パーソナルデータ管理提案書 Part3 1.1（2021年5月版））。

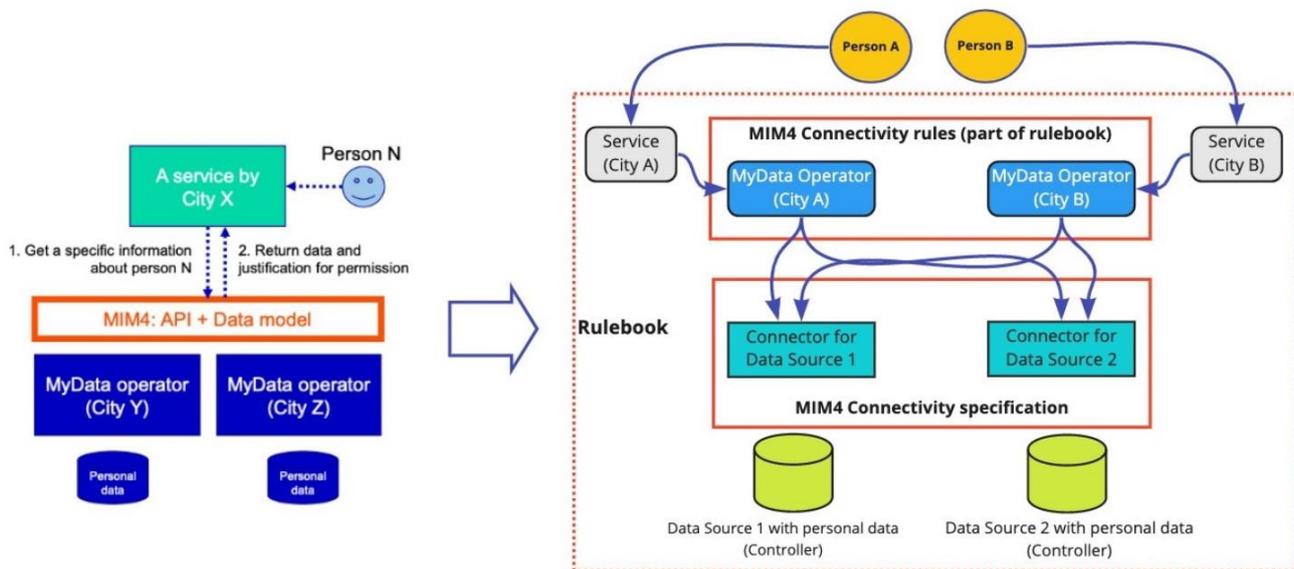


図 3-3-5-4 MIM4 パーソナルデータ流通アーキテクチャ

(Vastuu Group MyDataShare MIM4 Introduction より抜粋)

[https://www.vastuugroup.fi/hubfs/MyData/MIM4-intro-28-5-](https://www.vastuugroup.fi/hubfs/MyData/MIM4-intro-28-5-2021.pdf?utm_referrer=https%3A%2F%2Fwww.mydatashare.com%2Foasc-mim4-specification)

[2021.pdf?utm\\_referrer=https%3A%2F%2Fwww.mydatashare.com%2Foasc-mim4-specification\)](https://www.vastuugroup.fi/hubfs/MyData/MIM4-intro-28-5-2021.pdf?utm_referrer=https%3A%2F%2Fwww.mydatashare.com%2Foasc-mim4-specification)

最後に、パーソナルデータ管理提案書におけるパーソナルデータ管理への要求事項と、とブローカー（パーソナル）の機能との対比を、表 3-3-5-1 に示す。以上のことから、パーソナルデータ管理提案書で検討されているパーソナルデータ管理基準と、本調査におけるブローカー（パーソナル）機能の整合性を確認した。

表 3-3-5-1 ブローカー（パーソナル）機能とパーソナルデータ管理提案書の対比

ステークホルダー	分類	機能	MIM4 パーソナルデータ管理 要求事項
個人	同意管理	蓄積同意	Operator の役割に相当
		共有同意	Operator の役割に相当
			Operator の役割に相当
	パーソナルデータ管理	パーソナルデータ 所在管理	トラストフレームワークにより 事前合意すべき内容に相当
		アクセスログ	コネクタの役割に相当

ステークホルダー	分類	機能	MIM4 パーソナルデータ管理 要求事項
サービス提供組織	ブローカー (非パーソナル) 同等機能	API 仕様	コネクタの役割に相当
		データ分散	コネクタの役割に相当
		データ蓄積	コネクタの役割に相当
	先端的サービス管理	先端的サービス定義	トラストフレームワークにより 事前合意すべき内容に相当
サービス提携組織	サービスアセット管理	サービスアセット定義	トラストフレームワークにより 事前合意すべき内容に相当

### 3-4. 各ビルディングブロックの調査

#### 3-4-1. 調査方針

本節では、オープンソース・ソフトウェア（OSS）として公開されている「API ゲートウェイ、ブローカー（非パーソナル）、ブローカー（パーソナル）」について、3-1 にて定義した各ビルディングブロックが満たすべき要件との適合性や OSS の成熟度を考慮し、データ連携基盤として推奨されるモジュールを調査する。

#### 3-4-2. 各ブロックの調査結果

##### (1) API ゲートウェイの調査結果

本項では、オープンソース・ソフトウェア（OSS）として公開されている API ゲートウェイを調査し、3-1 で定義した要件との適合性や OSS の成熟度から、データ連携基盤として推奨されるモジュールを決定する。

調査対象とする OSS は、国内外での実績等を加味し、表 3-4-2-1 のとおり選定した。

表 3-4-2-1 API ゲートウェイの OSS 選定

No.	OSS 名	開発元	ライセンス	選定理由
1	Kong Gateway <sup>21</sup>	Kong Inc. (USA)	Apache License 2.0	様々な分野で API ゲートウェイとして広く使われており、欧米企業等を中心に大規模サービスでも実績のある OSS であること、Web 上にも豊富な情報があることから、データ連携基盤事業者が活用しやすいと考えられるため
2	WSO2 API Manager <sup>22</sup>	WSO2 Inc. (USA)	Apache License 2.0	高松市や加古川市など、国内に実装されたデータ連携基盤の API ゲートウェイとして複数の実績があるため
3	API Umbrella <sup>23</sup>	NREL (USA)	MIT License	欧州を中心に世界各国でデータ連携基盤として実績のある FIWARE GE であり、FIWARE の他コンポーネントとの親和性が期待できるため

<sup>21</sup> <https://github.com/Kong/kong>

<sup>22</sup> <https://github.com/wso2/product-apim>

<sup>23</sup> <https://github.com/umbrella-project/umbrella>

また、選定した OSS の要件との適合性を表 3-4-2-2、各 OSS の成熟度を表 3-4-2-3 に示す。

表 3-4-2-2 要件との適合性

要件				OSS		
分類	機能	必須	推奨	Kong Gateway	WSO2 API Manager	API Umbrella
基本機能	認証	●		○	○	○
	ルーティング	●		○	○	○
	ライフサイクル管理	●		○	○	○
	バージョン管理	●		○	○	○
セキュリティ	アクセス制限		●	○	○	○
	レート制限		●	○	○	○
利用可能 API	REST API	●		○	○	○
分析・モニタリング	アクセス分析		●	○	○	○
	アラート監視		●	○	○	×

表 3-4-2-3 OSS の成熟度

分類	指標	Kong Gateway	WSO2 API Manager	API Umbrella
開発活性度 (※1)	コントリビューター数	○ (281 人)	○ (178 人)	△ (13 人)
	最終リリース	○ (2022/3/2)	△ 2021/4/20	×
	リリース数 (※2)	○ (29 回)	△ (3 回)	×
利用者コミュニティ	公式コミュニティ (英語)	○ (あり)	○ (あり)	×
	国内コミュニティ	×	×	×
情報の検索性	公式マニュアル (英語)	○ (あり)	○ (あり)	○ (あり)
	日本語マニュアル	○ (xlsoft が公開)	×	×
	インターネット上の日本語記事数	○ (多数あり)	△ (少ない)	△ (少ない)

(※1) 2022/3 時点での github の情報を基に集計

(※2) 2020/1 以降のリリースが対象 (β リリース等の正式リリースでないものは除外)

今回調査した各 OSS は一般的に API ゲートウェイに期待される機能をほぼ具備していたことが表 3-4-2-2 よりわかる。各 OSS 毎に特徴や得意領域が異なることは想定されるが、実績のある OSS であれば API ゲートウェイとして期待される基本機能 (必須要件) はどの OSS も具備していると想定できる。

表 3-4-2-3 では、OSS の成熟度を評価するために開発活性度、利用者コミュニティ、情報の検索性の観点で比較分析した。どの項目においても Kong Gateway が優れた結果となっており、API ゲートウェイの OSS の中では安定性、利便性、今後の発展など様々な面で期待できる。

本調査結果より、Kong Gateway が API ゲートウェイの公認モジュールに相応しいと判断する。

ただし、表 3-4-2-2 が示すように各 OSS が全て必須要件を満たしていること、また API ゲートウェイが提供する機能は API やデータモデルの仕様には直接影響しないことから、どの OSS を用いても相互運用性が損なわれることは無いと考えられる。API ゲートウェイ製品の選定は公認モジュールに限定せず、開発者や運用者が使い慣れた製品を採用することを推奨する。

#### (2) ブローカー（非パーソナル）の調査結果

本項では、オープンソース・ソフトウェア（OSS）として公開されているブローカー（非パーソナル）を調査し、3-2. で定義した要件との適合性や OSS の活性度から、データ連携基盤として推奨されるモジュールを決定する。

調査対象とする OSS は、データ連携基盤報告書の調査対象である FIWARE Orion（以下、Orion）、Apache Kafka（以下、Kafka）、X-Road に加え、欧州電気通信標準化機構（ETSI）により標準化された FIWARE 次期標準インターフェース仕様である NGSI-LD を実装した Scorpio を対象とする。

調査対象の OSS を表 3-4-2-4 に示す。

表 3-4-2-4 ブローカー（非パーソナル）の OSS 選定

No.	API 名/OSS 名		開発元	ライセンス	選定理由
1	NGSI v2	FIWARE Orion	Telefonica	AGPL v3.0	データブローカーとして国外/国外のスマートシティ案で多数の実績があるため
2	Apache Kafka		Apache	Apache License 2.0	メッセージブローカーとして、国内で多くのユーザーにサービスを提供している海外企業等で実績があるため
3	X-Road		NIIS	MIT License	電子行政分野（エストニア等）で実績のあるデータ交換プラットフォームであり、国内でも活用検討が始まっているため
4	NGSI-LD	Scorpio	NEC	BSD 3-Clause	FIWARE の次期インターフェース仕様である NGSI-LD を実装した FIWARE GE であるため
		Orion-LD	FIWARE Foundation	AGPL v3.0	
		Stellio	ETSI	Apache License 2.0	

また、選定した OSS の要件との適合を表 3-4-2-5、OSS の成熟度を表 3-4-2-6 に示す。

表 3-4-2-5 要件との適合性

		要件				OSS			
分類	機能	説明	必須	推奨	Orion	Kafka	X-Road	NGSI-LD(※)	
データ利活用	データ参照	データ分散	データ参照の要求を受け付け、外部サービスが保持するデータを返却可能なこと	●		○	○	○	○
			データ利用者に対してデータの所在を隠蔽することができること		●	○	○	×	○
		データ蓄積	データ参照の要求を受け付け、データストア機能に蓄積されたデータを返却可能なこと		●	○	×	×	○
	サービス呼び出し	イベント処理	サービス呼び出しの要求を受け付け、外部サービスの処理を実行し結果を返却可能なこと (例：交通サービスでタクシーを予約)		●	○	×	×	○
	API仕様	API仕様	データ利活用の利便性を考慮し、標準ルールに沿ったAPI (REST 等) を提供可能なこと	●		○	○	○	○
	データ変換	データ変換	外部サービスへの接続時、接続先サービスのインターフェースに合わせたデータ変換が可能なこと		●	×	×	×	×
データ収集	データ更新	イベント処理	データ提供者からデータを受け付け、必要なサービスへデータを送信できること		●	○	○	×	○
			データ送信時、リアルタイムにデータの分析・変換・加工処理等が可能なこと		●	×	×	×	×
	データ蓄積	データ提供者からデータを受け付け、データストア機能に蓄積可能なこと		●	○	×		○	
	API仕様	API仕様	多種多様なアセットからのデータ収集を想定し、標準APIに限らず様々な接続方式に対応可能なこと (MQTT 等)		●	×	×	×	×

(※) 3 ブローカーとも類似した傾向があるため、まとめて表現

表 3-4-2-6 OSS の成熟度

分類	指標	Orion	Kafka	X-Road	NGSI-LD (※3)
開発活性度 (※1)	コントリビューター数	○ (61)	○ (880)	△ (29)	△
	最終リリース	○ (2022/3/2)	○ (2022/1/21)	○ (2022/2/11)	○
	リリース回数 (※2)	○ (17)	○ (15)	○ (10)	○
利用者コミュニティ	公式コミュニティ (英語)	○ (あり)	○ (あり)	○ (あり)	○
	国内コミュニティ	× (発見できず)	○ (kafka. apache. jp)	× (発見できず)	×
情報の検索性	公式マニュアル (英語)	○ (あり)	○ (あり)	○ (あり)	○
	日本語マニュアル	○ (github)	× (発見できず)	× (発見できず)	×
	インターネット上の日 本語技術情報 (Qiita 等)	△ (少ない)	○ (多数あり)	× (殆ど無い)	×

(※1) 2022/3 時点での github の情報を基に集計

(※2) 2020/1 以降のリリースが対象 (β リリース等の正式リリースでないものは除外)

(※3) 3 ブローカーとも類似した傾向があるため、まとめて表現

表 3-4-2-5 では、全ての OSS がブローカー機能の必須要件は満たしているが、最もブローカー要件への適合性が高い OSS は Orion または NGSI-LD ブローカーであることがわかる。Orion と NGSI-LD ブローカーはともに FIWARE のコンテキストブローカーに位置づけられるが、FIWARE が採用するインターフェース規格である NGSI が Pull 型と Push 型の両方のデータ仲介方式に対応しているため要件への適合性が高く、幅広いユースケースでの活用が期待できる。

表 3-4-2-6 では、Orion と NGSI-LD ブローカーともに活発に開発が行われていることが確認できるが、Orion のほうがコントリビューター数やリリース回数が多く、また日本での情報検索においても優位である。NGSI-LD ブローカーは FIWARE の次期インターフェース仕様である NGSI-LD を実装したコンテキストブローカーであるが、NGSI-LD はまだ事例も少なく安定した技術と言える状態にはない。一方 Orion が採用する NGSI は国内外で多数の活用事例がある。地域への社会実装として用いる OSS としては安定性が重要であり、現段階では Orion のほうが適していると考えられる。

本調査結果より、Orion がブローカー (非パーソナル) の公認モジュールに相応しいと判断する。

### (3) ブローカー (パーソナル) の調査結果

本項では、OSS として公開されているブローカー (パーソナル) を調査し、3-3-4. で定義した要件との適合性から、生活用データ連携基盤として推奨できるモジュールの決定を目的とする。

ブローカー (パーソナル) には先のブローカー (非パーソナル) の要件に加え 3-3-4. で述べたとおり「同意管理」、「パーソナルデータ管理」、「先端的サービス管理」及び「サービスアセット管理」が機能

として必要となる。欧州においては、パーソナルデータの処理と移転を定めた「GDPR（EU 一般データ保護規則）<sup>24</sup>」やパーソナルデータに対する認証技術に法的拘束力を持たせた「eIDAS 規則<sup>25</sup>」が制定されるなど、個人情報保護管理に先進的であることから、パーソナルデータを活用した自治体主導のプロジェクトも複数報告されている。そのため、欧州における事例を幅広く調査することで、上記機能に適合する OSS として公開されているブローカー（パーソナル）が発見可能であると考えた。

以上のことから、本調査では欧州におけるパーソナルデータを活用した先端的サービス展開事例を中心に広く調査対象とした。

#### (a) 調査対象事例

本調査における調査対象事例を表 3-4-2-7 に示す。表中の各事例はパーソナルデータのみを扱うわけではなく、利用データには IoT デバイスで取得するセンサーデータ等も含まれる。さらに、利用するパーソナルデータは大別すると、個人所有の IoT デバイスで取得するデータと行政が保持するデータの二つに分けられる。

表 3-4-2-7 調査対象事例

プロジェクト	実施エリア	実現しているサービス例	利用データ
EUBra-BIGSEA <sup>26</sup>	クリチバ（ブラジル） ※EU との共同実施	非効率な人流を可視化し、都市開発に係る人に提供	人流データ、バスの乗降履歴+バスの GPS 情報の紐づけ等
Snap4City <sup>27</sup>	ヘルシンキ（フィンランド） アントワープ（ベルギー） トスカーナ（イタリア）等	自身の過去の位置情報履歴を参照したり、ヘルスケアデバイスのデータを家族のみで共有可能	スマートフォンやヘルスケアデバイス等の個人所有 IoT データ
MiMurcia <sup>28</sup>	ムルシア（スペイン）	ビルのエネルギープランの効率化	スマートメーターのエネルギー消費データ、気温やパーキング利用状況等のセンサーデータ
E-Estonia <sup>29</sup>	エストニア	一度住所変更の届け出をすれば全ての行政サービスの登録が更新	居住地情報、医療・健康情報等の様々な行政データ (センサーデータは含まない)
UOP <sup>30</sup>	タリン（エストニア） ヘルシンキ（フィンランド）	<ul style="list-style-type: none"> <li>ユーザーが「同意」するのみで、必要時に年収証明やキャリア情報を第三者に提出可能</li> <li>スマートメーターデータの分析による省エネ</li> </ul>	行政データ+一部センサーデータ

<sup>24</sup> <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

<sup>25</sup> [http://data-trading.org/wp-content/uploads/2020/05/ReferenceArchitecture\\_body\\_rev11a.pdf](http://data-trading.org/wp-content/uploads/2020/05/ReferenceArchitecture_body_rev11a.pdf)

6.4.1

<sup>26</sup> An Integrated Big and Fast Data Analytics Platform for Smart Urban Transportation Management (2019)

<sup>27</sup> Smart City IoT Platform Respecting GDPR Privacy and Security Aspects (2020)

<sup>28</sup> A user-centric Internet of Things platform to empower users for managing security and privacy concerns in the Internet of Energy (2017)

<sup>29</sup> Digital Government Factsheet 2019 Estonia

<sup>30</sup> Urban Open Platform for Borderless Smart Cities (2022)

(b) 各事例でのパーソナルデータ取り扱い

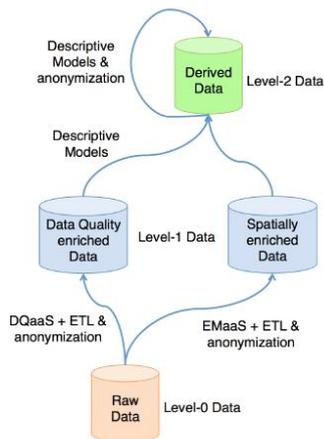
各事例でのパーソナルデータの扱いを以下に示す。

(ア) EUBra-BIGSEA

EUBra-BIGSEA は、EU とクリチバ（ブラジル）の共同プロジェクトであり、人流データ、バスの乗降履歴及び GPS 情報をビッグデータ解析することで非効率な人流を可視化し、スマートな都市交通の実現を目標の一つとしている。

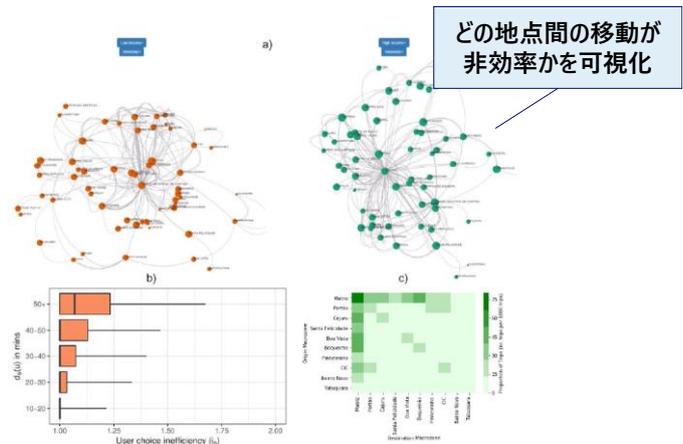
パーソナルデータの取り扱いとしては、元データとして個人情報扱いしつつ、完全匿名化して統計的に使用している。そのため、パーソナルデータは流通しているが個人に紐づく活用（パーソナライズした提案等）には使用できない。（図 3-4-2-1）

複数段工程の匿名化



加工過程で「一意に特定できる人」が出ることもあるため、加工後も匿名化をかけて個人情報に最大限配慮

匿名情報分析のアウトプット



最終的なアウトプットは統計的な傾向。個人に紐づくデータは提供しない

図 3-4-2-1 EUBra-BIGSEA でのパーソナルデータの取り扱い

(An Integrated Big and Fast Data Analytics Platform for Smart Urban Transportation Management<sup>31</sup>より抜粋)

<sup>31</sup> <https://ieeexplore.ieee.org/document/8809689>

(イ) Snap4City

Snap4City は、ヘルシンキ（フィンランド）、アントワープ（ベルギー）及びトスカーナ（イタリア）等で活用されている、異分野データ分析や IoT サービスを提供するプラットフォームである。

パーソナルデータの取り扱いとしては、匿名化はしないが、重要な個人情報とは分離し、後から紐づけ可能なようにキーを付与(=仮名化)している。そのため、ブローカー（パーソナル）を経由して扱うパーソナルデータは仮名化データである。（図 3-4-2-2）

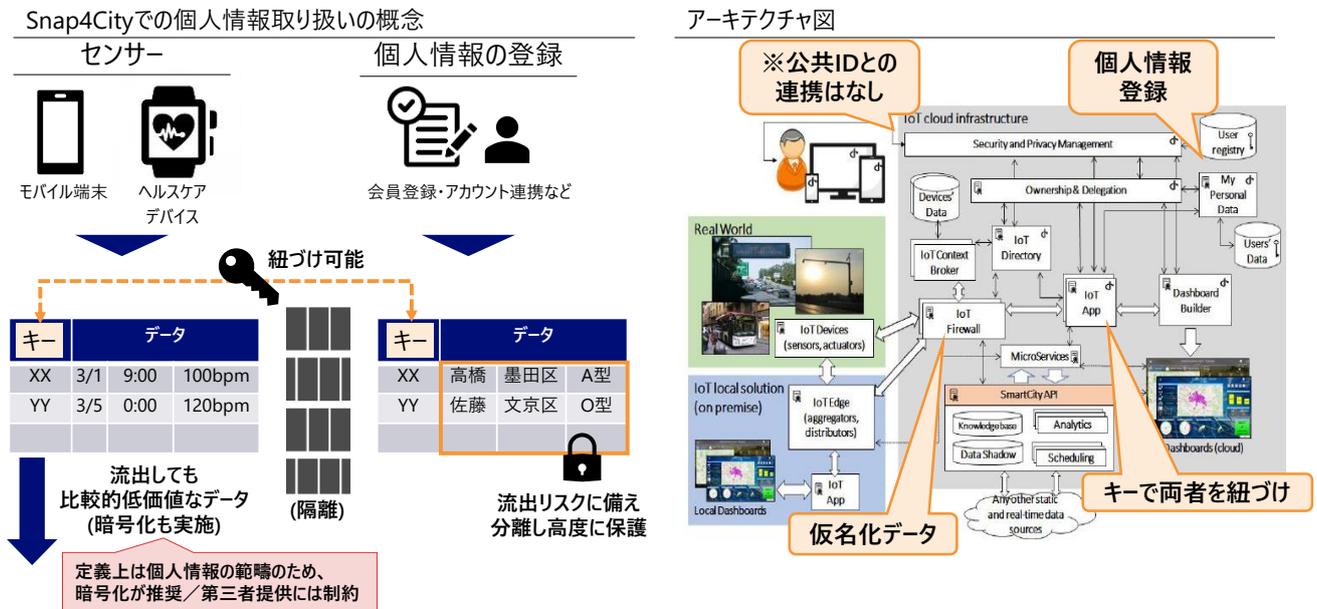


図 3-4-2-2 Snap4City でのパーソナルデータの取り扱い

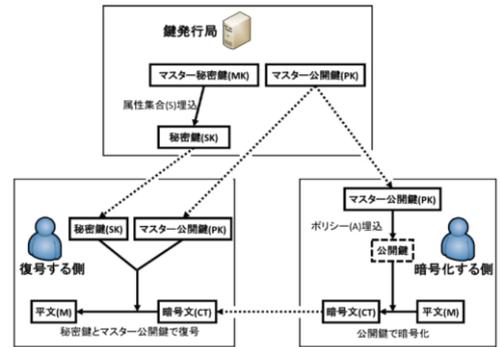
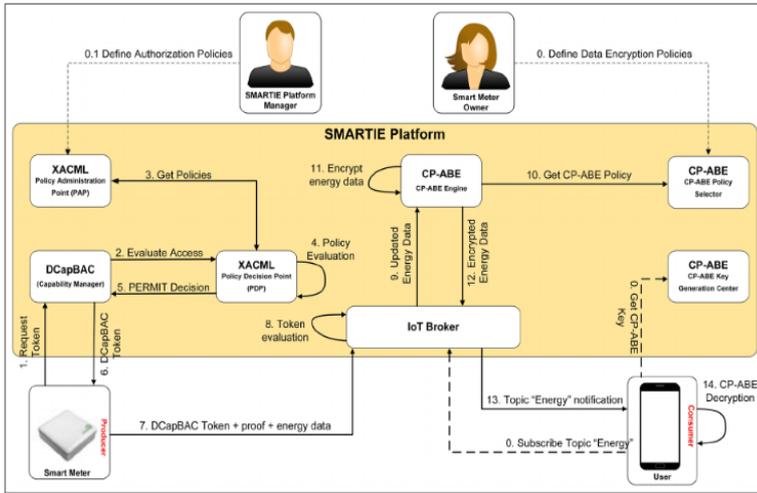
(Smart City IoT Platform Respecting GDPR Privacy and Security Aspects<sup>32</sup>より抜粋)

(ウ) MiMurcia

MiMurcia は、ムルシア（スペイン）におけるスマートシティプロジェクトであり資源（エネルギー、水、公共交通等）の最適化を目標に掲げている。住民の日常生活のデータも収集することで、効率的な省エネ戦略を展開している。

パーソナルデータの取り扱いとしては、CP-ABE による暗号化を実施して個人情報を保護すると同時に、同意管理ダッシュボードにより、ユーザーによるデータコントロール容易性を強化している。同意管理ダッシュボードでは、CaPe という同意管理ツールを活用している。（図 3-4-2-3）

<sup>32</sup> <https://ieeexplore.ieee.org/document/8966344>



認証鍵にポリシーと属性情報を埋め込むことで、属性に応じた認証を可能にする  
(例: レンタサイクルのユーザ⇔サービス間のみでデータを交換)

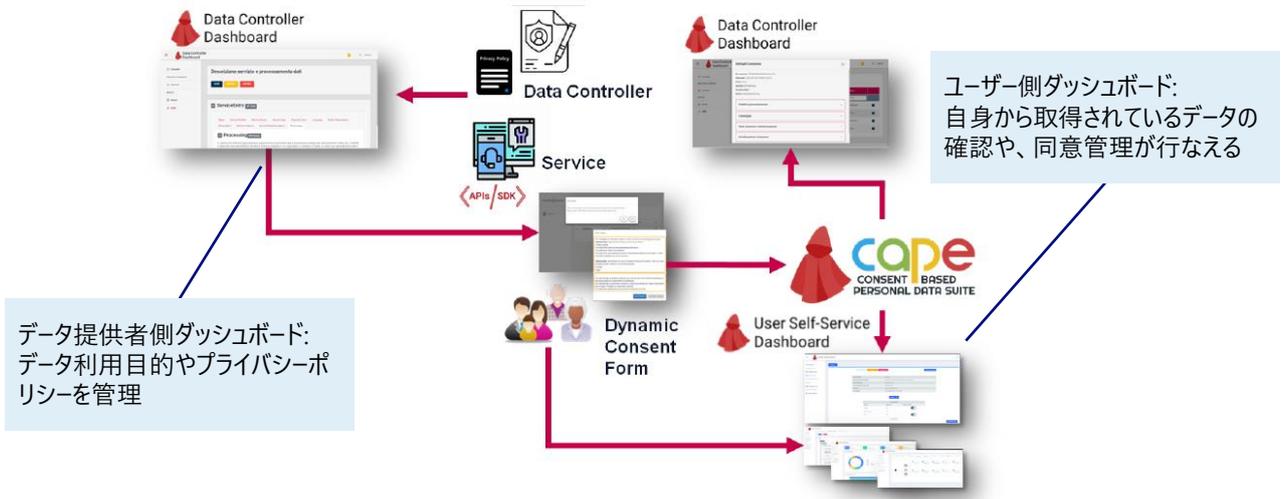


図 3-4-2-3 MiMurcia でのパーソナルデータの取り扱い

(A user-centric Internet of Things platform to empower users for managing security and privacy concerns in the Internet of Energy<sup>33</sup>, CP-ABE を用いた VDI の使用権限委譲機構の開発<sup>34</sup>, Data Protection by Design in the Context of Smart Cities<sup>35</sup>より抜粋)

<sup>33</sup> <https://journals.sagepub.com/doi/10.1177/1550147717727974>

<sup>34</sup> [https://jglobal.jst.go.jp/detail?JGLOBAL\\_ID=201902224887705023](https://jglobal.jst.go.jp/detail?JGLOBAL_ID=201902224887705023)

<sup>35</sup> <https://www.mdpi.com/1424-8220/21/21/7154>

(エ)E-Estonia

E-Estonia は、エストニアの電子政府サービスであり、住所変更の届け出により全ての行政サービスの登録が更新されるサービス等に活用されている。また、公共 ID を介し、行政サービス間及び一部民間企業とのデータ連携が高度に発達している。

パーソナルデータの取り扱いとしては、行政サービス間の重要な個人情報の連携は、X-Road によるセキュアな P2P 通信で実現している。なお、E-Estonia では行政データのみを扱い、IoT データは扱っていない。(図 3-4-2-4)

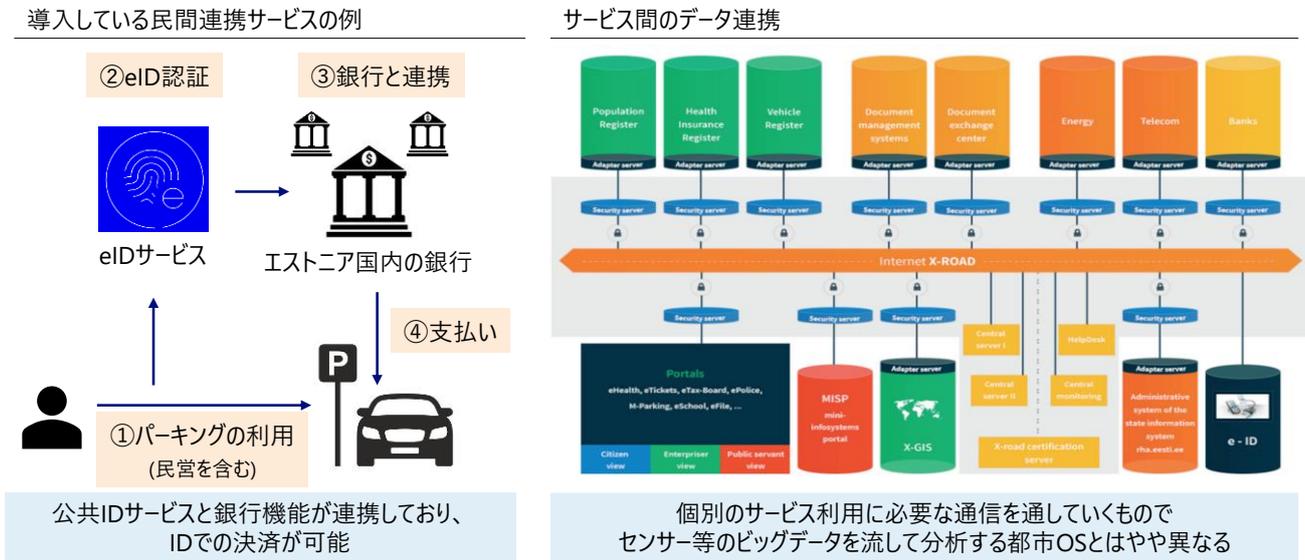


図 3-4-2-4 E-Estonia でのパーソナルデータの取り扱い  
(Digital Government Factsheet 2019 Estonia<sup>36</sup>、X-ROAD FACTSHEET<sup>37</sup>より抜粋)

(オ)UOP

UOP (Urban Open Platform) は、ともにスマートシティ先進都市のタリン(エストニア)及びヘルシンキで開発された、2都市間共通のデータプラットフォームであり、あらゆる先端的サービスのデータを一元管理し、データ利活用することでサービスレベル向上を目指している。サービス例としては、ユーザーが「同意」をするのみで、必要時に年収証明やキャリア情報を第三者に提出できる仕組み等が挙げられる。

パーソナルデータの取り扱いについては、行政データと IoT データの統合を目指しているが、現状ではほぼ未着手である。エストニアの Estfeed というプラットフォームにおいて、両データを取り扱っているが、連携させるところまでは至っていないと想定される。(図 3-4-2-5)

<sup>36</sup> [https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital\\_Government\\_Factsheets\\_Estonia\\_2019.pdf](https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Estonia_2019.pdf)

<sup>37</sup> <https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/x-road-factsheet-2014.pdf>

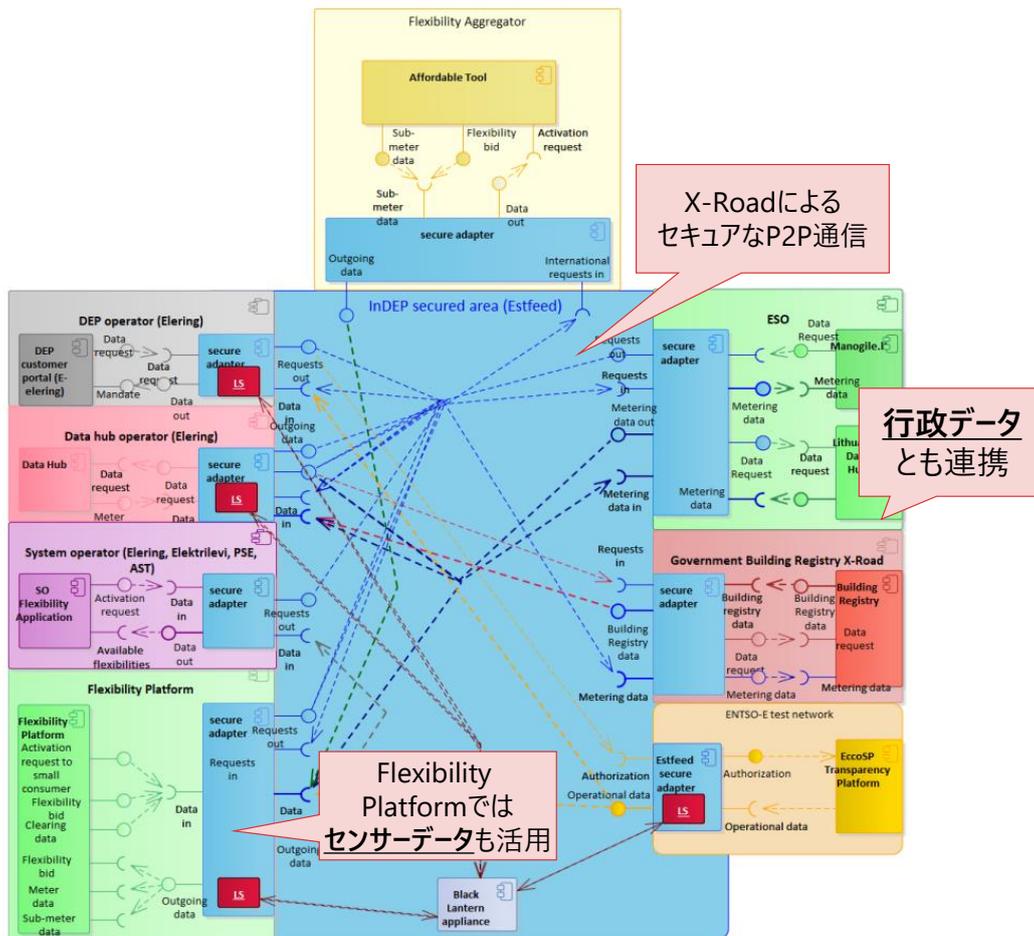


図 3-4-2-5 UOP でのパーソナルデータの取り扱い (Estfeed の概要)

(Data security and privacy guidelines and feasible cyber security methods for data exchange platforms (2021)<sup>38</sup>より抜粋)

(c) パーソナルデータ取り扱いまとめ

欧州の先進的サービス展開事例でのパーソナルデータの取り扱いを表 3-4-2-8 にまとめる。表の左部には、参考としてパーソナルデータを使用していないバルセロナの事例も掲載した。

まず、EUBra-BIGSEA、Snap4City 及び MiMurcia では匿名化もしくは仮名化したパーソナルデータを取り扱っているが、匿名化機能及び仮名化機能は公認モジュールとしてのブローカー（パーソナル）に必要な機能に含まれていないため、本調査の対象外となる。また、MiMurcia で開発された同意管理ダッシュボードでは、CaPe という同意管理ツールが活用されており、GitHub で OSS として公開されている<sup>39</sup>。しかし、この CaPe の GitHub を参照すると、2022 年 3 月時点でコントリビューター数が 3 人、最終リリースが 2021 年 6 月 5 日、リリース数が 2 回となっていることから、OSS としての開発活性度が低く、広く普及しているとは言い難い。

E-Estonia 及び UOP については、行政データとしての個人情報を取扱っているが、P2P 通信でデータを共有しているため、ブローカー（パーソナル）は活用していない。

<sup>38</sup> [https://eu-sysflex.com/wp-content/uploads/2021/06/EU-SysFlex-D5.4-Data-security-and-privacy-guidelines-and-feasible-cyber-security-methods-for-data-exchange-platforms\\_FINAL.pdf](https://eu-sysflex.com/wp-content/uploads/2021/06/EU-SysFlex-D5.4-Data-security-and-privacy-guidelines-and-feasible-cyber-security-methods-for-data-exchange-platforms_FINAL.pdf)

<sup>39</sup> <https://github.com/OPSILab/CaPe>

以上のことから、本調査の範囲において、パーソナルデータを流通させる機能を満たすブローカーが広く OSS として公開されている事例はなかった。

表 3-4-2-8 欧州の先端的サービス展開事例におけるパーソナルデータ取り扱い

		「個人情報」としてのデータ利用度			
		センサーデータ		行政データ	
個人情報 利用パターン		不使用	匿名化して使用	仮名化して使用	個人情報のまま 使用
ケース		(バルセロナなど)	EUBra-BIGSEA	Snap4City MiMurcia	E-Estonia UOP(Estfeedを除く)
概要		マシンデータのみ取扱 (ごみ箱センサー設置による 収集効率化等)	統計分析結果を サービスに活用	個人を識別したうえで サービス提供	行政サービスを 利用可能 (センサーデータは不使用)
構成		ブローカー		ブローカー + 仮名化キー紐づけ	P2P通信

(d)OSS として公開されているブローカー（パーソナル）の調査結果

本調査では「同意管理」、「パーソナルデータ管理」、「先端的サービス管理」及び「サービスアセット管理」といった機能の要件を満たした OSS として公開されているブローカー（パーソナル）について、欧州の先端的サービス活用事例を基に調査を行ったが、現実的に活用が進んでいるものは見つからなかった。ただし、本調査で対象とした事例では日々新たなプロジェクトが検討されており、その中でブローカー（パーソナル）について言及される可能性があることには留意されたい。

### 3-5. 公開方法

公認モジュールとなる OSS 製品を利用するにあたり、必要となるソースコードや取扱説明書といった資源を表 3-5-1 に示す。なお、公開方法は決定次第、別途、公表される予定である。

表 3-5-1 公認モジュールに関する公開予定の資源一覧表

項番	ビルディングブロック	公認モジュール	資源名	内容
1	API ゲートウェイ	Kong Gateway	ソースコード	ソースコードは GitHub にて無償で公開 <a href="https://github.com/Kong/kong">https://github.com/Kong/kong</a>
2			Kong ビルド手順書	開発コミュニティの公開資料を基に Kong をビルドする手順を記載
3			Kong 構築手順書	開発コミュニティの公開資料を基に Kong を構築する手順を記載
4			Kong 利用手順書	開発コミュニティの公開資料の例示を基に Kong を利用する手順を記載
5	ブローカー (非パーソナル)	Orion Context Broker	ソースコード	ソースコードは GitHub にて無償で公開 <a href="https://github.com/telefonicaid/fiware-orion">https://github.com/telefonicaid/fiware-orion</a>
6			Orion ビルド手順書	開発コミュニティの公開資料を基に Orion をビルドする手順を記載
7			Orion 構築手順書	開発コミュニティの公開資料を基に Orion を構築する手順を記載
8			Orion 利用手順書	開発コミュニティの公開資料の例示を基に Orion を利用する手順を記載
9	全ブロックのまとめ		Kong_Orion 連携手順書	Kong から Orion をサービス登録して連携できるようにする手順を記載

表 3-5-1 に記載した公開予定の公認モジュールの範囲は、API ゲートウェイ、ブローカー（非パーソナル）となるが、将来的にデジタル庁から「ブローカー（パーソナル）の同意管理、パーソナルデータ管理」の機能も提供予定である。

## 4. 業務実施結果 ステップ3：モジュールの継続的な運用の定義

本章では、3章で決定したモジュールをオープンな形式で公開し、各地域の生活用データ連携基盤構築の迅速化及び生活用データ連携基盤での高度化サービスの創出の支援に向けて、公認モジュールを普及・管理するために必要なサポートサービスの内容及びサービスの継続的な運用を実現するための組織体制について、グローバルでの先進事例での取組内容を参考に定義していく。

### 4-1. サポートサービスの定義

#### 4-1-1. 先進事例の調査結果

##### (1) 調査概要

公認モジュールの継続的な運用には、ソフトウェアアップデートや新たな脅威への対応、バグ取り等、安心安全でかつ利便性のある部品として品質を管理していくことが必要となる。特に OSS においては、開発元であるオープンソースコミュニティとの相互扶助的な連携による品質管理体制が作られてこそ機能する。また、公認モジュールの普及には、自治体や事業者に対して公認モジュールの積極的な利用を促すためのインセンティブを考慮する必要がある。

普及管理団体<sup>40</sup>が提供するサポートサービスの検討にあたって、先進事例における取組内容及び普及・管理を担う組織の実行体制を調査する。

##### (2) 調査方法

公認モジュールの管理方法の検討にあたって、FIWARE Foundation での取組内容を調査する。FIWARE Foundation は、欧州で公共サービスを提供する自治体や企業などの業種を越えたデータ利活用やサービス連携を促すために開発・実装されたプラットフォーム「FIWARE」の普及を推進するために設立された非営利団体であり、オープンソースソフトウェアを「Generic Enabler(以下、GE)」として認定し、プラットフォームを構成するためのソフトウェアとして維持・管理をおこなっている。

公認モジュールの利用促進方法の検討にあたっては、欧州委員会の CEF Digital 等の組織における取組内容を調査する。CEF Digital は、欧州においてエネルギー・交通・テレコミュニケーションの3分野のインフラ・プロジェクトを支援する取組「Connecting Europe Facility (CEF)」のうち、国境を越えたデジタル公共サービスをより迅速に提供し、規制を遵守し、デジタル・シングル・マーケットを実現するための活動である。なお、CEF Digital は現在フェーズ2としてネットワーク領域に注力した活動に移行しているが、本調査では2014～2020年のフェーズ1でのプラットフォームの整備プログラムにおける取組内容を対象とする。

##### (3) 調査結果

サポートサービスの調査にあたって、オープンソースの管理・普及を担う組織がどのような体制や事業モデルのもとで運営をおこなっているのかを整理する必要がある。大きくは3つの組織形態に分類される。1つ目は、プラットフォームにおけるオープンソース開発を主導し、当該オープンソースを組み込んだ製品やサービスを提供する Red Hat などのような営利民間法人。2つ目は、オープンソースの開発や組織運営により業界標準の策定を推進する FIWARE Foundation のような非営利民間法人。3つ目は、共通機能の提供によって公共サービスの高度化や効率化、規制の統一等を目的に政府主導のもとで設立された CEF Digital のような公的機関である。それぞれの組織形態の概要を以下に記載する。

---

<sup>40</sup> 政府が認定した公認モジュールを管理し、導入支援や普及活動を担う非営利民間法人

主体	民間法人 (営利企業)	民間法人 (非営利団体)	公的機関
ケース	Red Hat Quansight	FIWARE Foundation Linux Foundation Eclipse Foundation	CEF Digital 各国政府
概要	民間企業が営利目的で オープンソフトウェアに関する サポートサービスを提供	企業や個人からの支援を受け オープンソースソフトウェアの開発や 組織を運営	政府やEUなど公的機関の 職員が運営
資金源	サービス利用料	企業や個人からの年会費や寄付	国や公的機関の予算
受益者	エンドユーザー (企業・開発者)	オープンソースを利用する 企業・個人	政府・ 企業(サービス提供者・開発者)

表 4-1-1-1 オープンソースを管理運営する団体・組織の形態

(a) 民間法人 (営利企業)

Linux の有償ディストリビューション企業である Red Hat はオープンソースの OS である Red Hat Enterprise Linux を中心としたクラウド向け製品やデータサービス等の販売に加えて、Fedora プロジェクトなどの代表的なオープンソースプロジェクトを支援している<sup>41</sup>。プロジェクトやコミュニティに Red Hat のエンジニアが参加して、オープンソースプラットフォームの開発をおこなっている。

オープンソースの利用者に対して、ソリューション実装のコンサルティングや、トレーニング、テクニカルアドバイス等のサポートサービスをサブスクリプションモデル有償で提供している。

(b) 民間法人 (非営利団体)

FIWARE Foundation が取り扱う FIWARE は、EU で 2011 年から 5 年にかけておこなわれた ICT 研究開発プログラム「Future Internet Public-Private Partnership (FI-PPP)」のもと、本プログラムの中核となる基盤ソフトウェアとして EU からの出資により開発及び各種ユースケースが実証されたものである。本プログラムでの成果を引き継ぎ、FIWARE の普及を推進するために設立された非営利団体が FIWARE Foundation である。

FIWARE Foundation は、組織ミッションや活動内容に共感する企業、学術機関、新興企業、個人をメンバーとして募り、メンバーからの会費や公的プロジェクト参画による収益を主な運営資金として活動している。運営資金を基に、会員に向けて各種ウェビナーや deep dive セッション・ハッカソン、マーケティング・技術支援などのサポートサービスを基本的には無償で提供している。

非営利団体として他には、オープンソースの Eclipse プロジェクトを運営し、オープンソースコミュニティと関連製品やサービスの発展を支援する Eclipse Foundation があり、FIWARE Foundation と同様に運営資金は WG のメンバーとして参加する企業からの年会費と推察される。メンバーは 4 つのタイプに分かれており、また、メンバー企業の中から Eclipse Foundation の理事会会員が選出される。

<sup>41</sup> <https://www.redhat.com/ja/about/open-source>

表 4-1-1-2 Eclipse Foundation のメンバー種別と役割

	役割	会費	企業例
Strategic Members (最低2つのプロジェクトにフルタイムでコミットする必要あり)	<ul style="list-style-type: none"> <li>理事会の代表者を指名する権利を有する</li> <li>運営組織の担当に立候補もしくは推薦する資格を有する</li> <li>WGにメンバーとして参加</li> </ul>	要	IBM、Microsoft、Oracle、Red Hat、Bosch、SAP SE他
Contributing Members (上記条件を満たせない企業)	<ul style="list-style-type: none"> <li>理事会の代表者になる権利を有する</li> <li>運営組織の担当に立候補もしくは推薦する資格を有する</li> <li>WGにメンバーとして参加</li> </ul>	要	Adobe、AIRBUS、Ericsson AB、Goldman Sachs、Intel他
Committer Members	<ul style="list-style-type: none"> <li>理事会の代表者になる権利を有する</li> <li>運営組織の担当に立候補もしくは推薦する資格を有する</li> <li>条件を満たすWGに参加可能</li> </ul>	不要	- (非公表)
Associate Members	<ul style="list-style-type: none"> <li>条件を満たすWGにゲストとして参加可能</li> </ul>	要	O'REILLY他

上述した FIWARE Foundation や Eclipse Foundation などの非営利民間法人はコミュニティに参加する企業等からの会費を運営資金に充てており、参加企業はオープンソースの普及に伴う自社製品とのインテグレーションを見据えた技術動向の把握や、コミュニティでの発言権の獲得による市場での競争優位性を得るためにコミュニティを支援している。

(c) 公的機関

CEF Digital は、重要インフラ領域でのプロジェクト支援を目的に欧州委員会が運営する公的機関であり、運営資金は INEA (Innovation and Networks Executive Agency) に割り当てられた EU 予算が資金源となっている。組織は 3 つのレイヤーで構成されており、各ビルディングブロックの運営は実行レイヤーの Operational Management Board (OMB) が担っており、欧州委員会の部局が担当している。

CEF Digitalのガバナンス体制

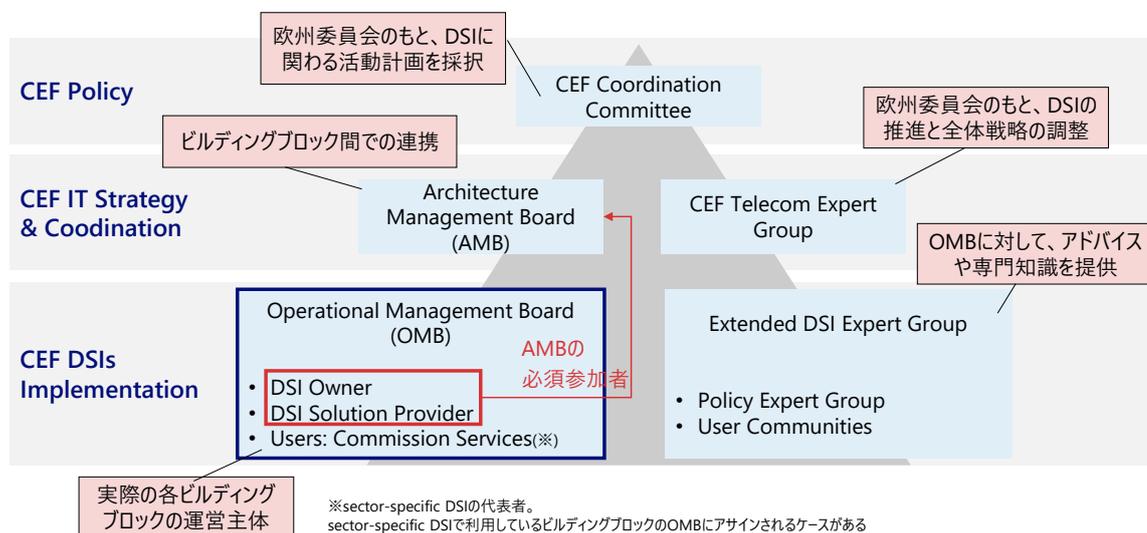


図 4-1-1-1 CEF Digital のガバナンス体制<sup>42</sup>

また、電子施策を推進するアメリカ政府においては、デジタルサービス関連技術やテーマに関するリソースの共有や協働を目的としたコミュニティの形成及びデジタルサービス構築のガイダンス機能「Digital.gov」を共通役務庁（General Services Administration:GSA）内の Technology

<sup>42</sup> EUROPEAN COMMISSION 「Non-paper on the IT Governance of the CEF Building Block Digital Service Infrastructures (DSIs)」

Transformation Services が担っている<sup>43</sup>。コミュニティにはオープンソースソフトウェアに関するコミュニティもあり、各コミュニティのマネージャーを GSA 職員が担当しているため、組織の運営資金は国の予算から捻出されていることが推察される。

公認モジュールの普及管理団体が提供するサポートサービスの検討にあたって、上記の民間法人（非営利団体）と公的機関の組織における取組内容を調査した。なお、民間法人（営利企業）においては、組織が提供するオープンソース利用者へのサポートは営利を前提としたサービスであるため、本調査事業におけるサポートサービス調査の対象外とする。

### ① モジュールの管理

FIWARE Foundation では FIWARE プラットフォームの技術的方向性と FIWARE オープンソースコミュニティの活動を統括する Technical Steering Committee<sup>44</sup>（以下、TSC）を設置している。TSC が担う主な役割は以下の 3 機能である。

#### (ア) 全体の開発ロードマップとリリース計画の策定

FIWARE では、FIWARE プラットフォームを構成する主要機能を「チャプター」として定義しており、各 GE は現在 12 種類あるチャプターのいずれかに属している。TSC には会員投票で選出された代表者がチャプターごとに 2 名おり、代表者はチャプター内の GE の開発コミュニティの活動をリードして、GE の品質管理や機能拡張に貢献する。

代表者はチャプター内での開発状況やロードマップを定期的に報告することが求められており、各チャプターの情報を取りまとめた上で TSC 議長が理事会（BOD）に報告。BOD から TSC に対して GE の機能改善や新仕様への対応等を依頼することもあるが、実際に対応するかどうかは各チャプターの代表者に一任されている。

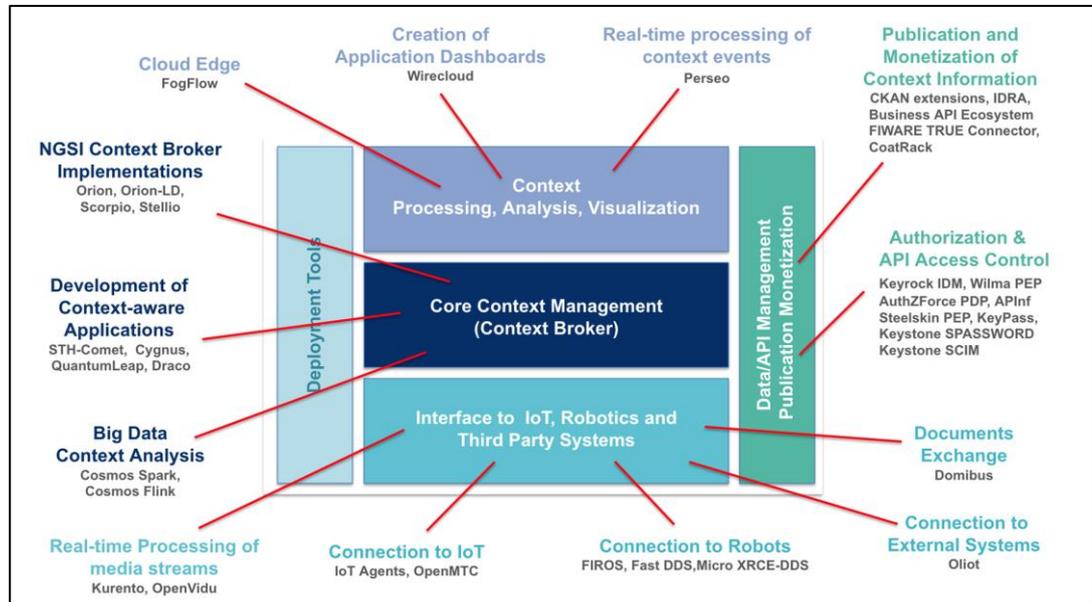


図 4-1-1-4 FIWARE Foundation の GE 構成<sup>45</sup>

<sup>43</sup> <https://www.gsa.gov/about-us/organization/federal-acquisition-service/technology-transformation-services/tts-solutions>

<sup>44</sup> <https://www.fiware.org/foundation/technical-steering-committee/>

<sup>45</sup> <https://github.com/Fiware/catalogue>

## (イ)GE の認定

### ● フル GE として満たすべき要件の策定

TSC では 2 種類の GE を管理している。1 つは、FIWARE プラットフォームのフレームワーク内においてフル GE ステータスを付与することが認められた「フル GE」。もう 1 つは、FIWARE プラットフォームに有益となる機能や将来必要と考えられる機能などを保持し、フル GE 候補である「インキュベーション GE」。

ソフトウェアがフル GE ステータスを取得するために満たすべき要件を TSC で策定しており、過去にコンテキスト情報を処理するフル GE に対して NGSI-LD サポートの要件を追加するなど要件は随時更新される。

要件は 3 種類あり、全てのフル GE が準拠を必須とする MUST 要件、必須ではないが成熟した開発プロセスが必要な場合に推奨される SHOULD 要件、現状は好ましい程度だが将来の開発プロセスの改善に向けて推奨される MAY 要件がある<sup>46</sup>。

MUST 要件に準拠していないフル GE には書面による警告をおこない、当該 GE の開発者は所定期間内に準拠させる必要があり、怠った場合はフル GE リストから削除される。

### ● GE の認定判断

ソフトウェアがフル GE として認定されるまでには、以下プロセスによって認定判断がおこなわれる。

1. 最小限の要件を満たしているかどうかを確認し、問題がなければインキュベーション GE として認定
2. MUST 要件全てに準拠しているかを確認。準拠していない場合、インキュベーション期間である 8 週間以内に対応させる必要がある。また、SHOULD 要件・MAY 要件の適用度をガイドラインリストに照らして評価する。
3. 評価の結果、フル GE ステータスの付与に望ましいことが確認できたらフル GE として認定する

## (ウ)GE の維持・改善・ライセンス関連のマネジメント

フル GE として認定されたソフトウェアの品質は当該 GE の開発元がコミュニティ等で管理しており、バグ等への対応やソフトウェアアップデートもおこなっている。TSC から GE の品質改善や機能拡張などの要望が出されるが、対応するかどうかは開発元に一任している。

フル GE が適切な品質、信頼性、最適なパフォーマンスレベルで動作していることを保証するために、ドキュメントや機能の検証、作業負荷の検証によって GE の品質をテストするプログラムを現在はリソース不足により実施していないが過去におこなっていた。

GE のソフトウェアライセンスにおいては、MUST 要件でライセンス規定について定義しており、フル GE ステータスの取得後も MUST 要件を遵守しているかを定期的に監視して管理している。

## ② モジュールの利用促進

モジュールを管理する組織が利用を促進させるために提供しているサポートサービスは、各組織ともおおよそ共通的な取組をおこなっている。代表例として欧州委員会が運営する CEF Digital が提供しているサポートサービスの内容について記載する。CEF Digital は、ヨーロッパで一般的かつ共通的な機能をビルディングブロックとして定義してオープンで再利用可能なモジュールを公開している<sup>47</sup>。モジュールの周知や利用促進を目的に提供しているサポートサービスは以下のと

<sup>46</sup> <https://github.com/FIWARE/contribution-requirements>

<sup>47</sup> <https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/CEF+Digital+Home>

おり。

#### (ア) モジュールの導入支援

モジュール情報の HP 等での公開に加えて、利用者のモジュールに関するナレッジの獲得や強化を目的とした利用開始方法の案内や研修等のサービス、問合せへの対応サービスを提供しており、導入時に生じる技術的な問題や負担を軽減させている。

- ソフトウェアやツールキットの公開・提供
- モジュールの利用開始方法のガイダンス
- オンボーディングトレーニングや研修の実施
- ビルディングブロック別のヘルプデスクの設置

#### (イ) モジュールの普及展開

ビルディングブロックに関する更新情報や活用事例等は無償で定期的に提供するとともに、導入状況を可視化させることで利用者及び利用検討者の関心を集めるようにしている。また、プロジェクト提案を募集し補助金の形式で支援することでビルディングブロックの普及を進めている。また、ビルディングブロックを活用したプロジェクトに対して、欧州委員会の担当部局から財政支援をおこなっている。

- ビルディングブロックやプロジェクトに関する情報のメルマガ等での発信
- ビルディングブロックでのプロジェクト数やドメイン別の統計による利用状況の可視化
- プロジェクトのナレッジ共有を目的としたイベント開催

上述した CEF Digital と同様のサポートサービスをモジュールを普及させる取組として非営利民間法人も提供している。本調査で公開情報から確認できた各組織の対応状況は以下のとおり。

表 4-1-1-5 各組織のサポートサービス対応状況

カテゴリ	サービス	公的機関	民間法人（非営利団体）		
		CEF Digital <sup>48</sup>	FIWARE Foundation <sup>49</sup>	Linux Foundation <sup>50</sup>	Eclipse Foundation <sup>51</sup>
導入支援	ソフトウェア情報の公開	○	○	○	○
	ガイダンスの提供	○	○	○	○
	トレーニングや研修	○	○	○	○
	ヘルプデスクの設置	○	○	○	○
普及展開	ニュースの配信	○	○	○	○
	利用状況公開	○	○	○	N/A
	イベントでのナレッジ共有	○	○	○	○

#### (4) 調査結果からの考察

調査結果から、公認モジュールの普及展開に向けて実施すべき内容は以下方針に基づき検討することが望ましいと考えられる。

##### ① モジュールの管理

<sup>48</sup> <https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/CEF+Digital+Home>

<sup>49</sup> <https://www.fiware.org/foundation/>

<sup>50</sup> <https://www.linuxfoundation.jp/>

<sup>51</sup> <https://www.eclipse.org/>

公認モジュールとして認定した各ソフトウェアの品質を普及管理団体が直接管理するのはローカル環境での修正を推奨としないオープンソースとしての仕組みの観点的にも適しておらず、管理工数負荷も増大である点から、品質向上や機能拡張を含む公認モジュールの品質管理は各ソフトウェアの開発元で実施することが現実的であると考え。その場合、候補モジュールが策定した要件に沿って選定されることで公認モジュールとしての一定の品質が担保されていることが前提となる。また、公認モジュールの品質管理を開発元に委ねることで品質低下やバグが発生した場合に問題が放置されるリスクは残存するが、バグ報告等で開発コミュニティと連携することやコントリビューターとしてコミュニティに参画するなどして可能な範囲で品質管理に貢献する仕組みを整備することが望ましいと考える。

## ② モジュールの利用促進

各地域が構築する生活用データ連携基盤に公認モジュールを導入する際に生じる負担を軽減させるための支援をおこなうサービスを提供する必要がある。普及促進にあたっては利用者及び利用希望者の行動変容を起こすための仕掛けが必要と考える。

また、組織体制の定義にあたっては、今後普及が開始される公認モジュールが一般化して普及管理団体が十分な運営資金を確保できるようになるまでに時間を要することが予想されるため、設立当初は公認モジュールを普及させるために普及管理団体として担うべき最小限の必要機能を精査した上で組織設計をすることが望ましいと考えられる。

### 4-1-2. サービス内容の定義

#### (1) 組織が提供すべきサービス内容

前項「4-1-1. 先進事例の調査結果」から、各地域での生活用データ連携基盤の構築・サービス発展に寄与する公認モジュールの利用活性化と継続的な運用には、大きく 2 種類のサービスが必要ということが判明した。1 つ目は、公認モジュールのラインアップの充足や品質管理等をおこなう「モジュールの管理」サービスであり、2 つ目は公認モジュールの周知や普及展開等をおこなう「モジュールの利用促進」サービスである。公認モジュールの普及・管理にあたって提供すべきサービス内容を以下に定義する。

#### ● モジュールの管理

多くの地域に公認モジュールを利用してもらうには、生活用データ連携基盤の構築にあたって利便性が高く共通利用が可能な機能を備え、安心安全で使い勝手のよい部品を提供する必要がある。また、提供する公認モジュールのラインアップは一度決めて固定化されるものではなく、変化する時代に合わせて柔軟に更新することが求められる。

#### ① モジュール戦略の策定

生活用データ連携基盤に必要なモジュールの在り方定義、ロードマップ立案、生活用データ連携基盤の拡張に向けた必要機能・公認モジュール導入方針の策定、ビルディングブロックの構成策定・変更

#### ② モジュールの認定判断

公認モジュール認定基準の策定、候補モジュールの選定・検証・認定

#### ③ 公認モジュールの管理

公認モジュールの一覧管理（追加・削除対応）、継続的な収集監視・対応による品質管理（ソフトウェア更新や脆弱性の監視・検証・更新、通達）、ライセンス管理<sup>52</sup>

#### ● モジュールの利用促進

<sup>52</sup> 公認モジュールのライセンス主体は当該ソフトウェアの開発者、もしくは開発コミュニティである。そのため、ここでは当該ソフトウェアを各地域が利用する上で問題がないライセンスかどうかを管理するという意味合いである。

生活用データ連携基盤を構成する公認モジュールを管理するのみでは、各地域での利用は進まず、陳腐化してしまうことから、モジュール導入時の障壁を軽減させるための支援や、各地域が自発的に利用を推進させるための納得度の高い情報の提供や行動変容を促すサービスの提供が必要となる。

④ 公認モジュールの導入支援

公認モジュールの利活用プロセス・ドキュメントの整備、自治体等への案内、技術的な問合せ対応

⑤ 公認モジュールの普及展開

公認モジュールの利用に関する情報発信、公認モジュールの普及・利用活性化に向けた各種施策の実行（セミナー開催等）、導入状況の調査

以上が公認モジュールを各地域に普及させる上で提供すべきサービス内容である。これらのサービスは公認モジュールを既存のオープンソースソフトウェアから選定することを想定して提供されるものであるが、将来的には共通機能として提供すべきだが既存のオープンソースソフトウェアに公認モジュールとしての条件を満たすものがない場合は当該機能を有するオープンソースソフトウェアの新規開発を政府が主導し、ソフトウェアの維持管理をおこなうケースも生じる可能性がある。その際は以下のようなサービスの提供が必要になることも考えられるが、公認モジュールは「定義した技術基準に適合する OSS を幅広く調査し、政府として公認」<sup>53</sup>される前提であるため、本調査では定義対象外とする。

- モジュールの新規開発  
新規ソフトウェアの開発判断、開発元の選定、開発（手配）
- 公認モジュールの機能拡張  
公認モジュールの品質向上や機能拡張に資する開発コミュニティの運営

(2) ステークホルダーとの関係性

公認モジュールは、生活用データ連携基盤の共通機能として自治体や事業者に対して政府が利用を推奨し、オープンな形式で公開・利用されるという公的な要素が強い。そのため、公平性を持った判断が必要となるモジュール戦略の策定やモジュールの認定判断などの方針策定や活動計画の採択は政府主導で実施することが望ましい。普及管理団体は、モジュールの運営やユーザーのサポートを主な活動として、政府に対して方針策定に必要な情報を提供するなどの役割を担うことが考えられる。公認モジュールの普及管理を推進する上での機能と役割のイメージを整理したのが下図である。



図 4-1-2-1 公認モジュールの普及管理を推進する上での機能と役割

<sup>53</sup> デジタル庁「生活用データ連携に関する機能等に係る調査研究 調達仕様書」

また、公認モジュールの部品整備や公開、導入に必要な情報の提供は普及管理団体が担うが、各地域で構築される生活用データ連携基盤への公認モジュールの実装は地域自身がパートナーベンダー等とおこなうことを想定している。各サービスでの検討主体者と役割を以下表に示す。

表 4-1-2-1 サービス別主体者と役割内容

カテゴリ	no.	サービス	政府(デジタル庁)		普及管理団体		OSS開発者・開発者コミュニティ		自治体・事業者	
			関与	役割	関与	役割	関与	役割	関与	役割
モジュールの管理	①	モジュール戦略の策定	◎	生活用データ連携基盤に必要なモジュールに関する方針策定、ロードマップ立案	○	方針策定に際しての情報提供(自治体等から挙げた意見の収集・報告)	-	-	-	-
	②	モジュールの認定判断	◎	公認モジュール認定基準の策定、候補モジュールの認定	○	(公認モジュール認定基準に沿った)候補モジュールの選定・検証	-	-	-	-
	③	公認モジュールの管理	○	公認モジュールの一覧管理(追加・削除判断)	◎	ソフトウェア更新や脆弱性の監視・検証・更新、通達	◎	ソフトウェアの品質管理、ソフトウェア更新、脆弱性の監視、通達	-	-
モジュールの利用促進	④	公認モジュールの導入支援	○	公認モジュールの利活用プロセス・ドキュメントの承認、自治体等への周知	◎	公認モジュールの利活用プロセス・ドキュメントの整備・公開、技術的な問合せ対応	○	ソフトウェアの情報公開、技術的な問合せ対応	-	-
	⑤	公認モジュールの普及展開	○	利用活性化施策・普及活動の支援	◎	公認モジュールの普及に向けた各種施策の実行、導入状況の調査	-	-	○	利用者としての情報提供
	-	データ連携基盤の構築	-	-	-	-	-	-	◎	公認モジュールの導入、データ連携基盤の構築
(将来的に発生する可能性のある領域)	-	モジュールの新規開発	◎	新規ソフトウェアの開発判断、開発(手配)	○	必要機能に関する情報提供、調達仕様の策定支援、開発元の選定支援	◎	新規ソフトウェアの開発、ライセンス条文の作成	-	-
	-	公認モジュールの機能拡張	○	開発者コミュニティの活動支援(経済支援含む)	○	開発者コミュニティの活動支援	◎	開発者コミュニティの運営、ソフトウェアの機能強化、参加者管理	○	開発者コミュニティへの参加

### 4-1-3. 運用方法の具体化

前項「4-1-2. サービス内容の定義」で定義したサービス内容のうち、普及管理団体が担うべきサービスについて、先端事例での取組内容等を参考に具体的な運用方法を以下に示す。

#### (1) モジュールの管理

##### ① モジュール戦略の策定

政府によって定められた生活用データ連携基盤の拡張に向けた必要機能・公認モジュール導入方針の策定、ビルディングブロックの構成策定・変更方針に基づき、普及管理団体は方針策定に際しての情報収集・提供を行う。例えば公認モジュールを利用する各地域から挙げられた意見や、生活用データ連携基盤構築事業者からの技術情報等である。

##### ② モジュールの認定判断

本調査事業で決定した公認モジュールに加えて、今後、生活用データ連携基盤の共通機能として各地域が実装すべき機能が将来生じた際に、当該機能を有するソフトウェアを調査・選定の上で認定し、公認モジュールのラインアップに追加する可能性がある。公認モジュールの認定基準の策定や認定判断は政府で実施することを想定している。

なお、共通機能として公認モジュール化する際の基本思想は以下と考える。

- 相互運用性の実現に必要な共通化すべき機能の提供  
各地域が構築する生活用データ連携基盤を相互運用可能(インターオペラブル)な仕組みにするために必要で共通化すべき機能を時代の状況に合わせて認定する。相互運用するための機能の最小範囲を政府にて判断して、都度設定する想定である。
- 相互運用性を担保するためのコスト低減への貢献(コストミニマム)  
生活用データ連携基盤に必要な機能を政府が無償で提供することにより、各地域における生

活用データ連携基盤の構築費用を最小限に抑えつつ、相互運用性を担保する。

- 協調領域と競争領域の境界線の設定

各地域に共通的に提供することで相互運用性の担保や各地域の負担軽減が期待できる協調領域とすべき機能か、各地域が独自に開発することで各地域の独自性や強みの発揮が期待できる競争領域の機能かの境界性を設定する。

共通機能として公認モジュールを各地域に提供すべきと判断された機能が生じた場合の候補モジュールの認定プロセスを以下に示す。

(ア) 候補モジュールの検証

モジュール戦略のもと、共通機能として公認モジュールに追加すべき機能を有するソフトウェアを調査して、公認モジュール認定基準のチェックリストを基に候補モジュールの適合性を検証する。認定基準としては以下のような観点で設定することを想定。

- 機能性 : 必要機能の要件を満たしているかどうか
- 信頼性 : 脆弱性やセキュリティに問題がないか
- ライセンス : 各地域が生活用データ連携基盤に実装するのに問題がないライセンスか
- サポート体制 : コミュニティが機能しているかどうか
- ドキュメント : 機能どおりの内容や利用方法がきちんと整備されているかどうか

(イ) 認定処理

検証の結果、公認モジュールとしての適合性が確認されたら、政府が認定を判断。認定された後、普及管理団体がソースコードや導入方法に関する情報を整備した上でHP等で公開する。

③ 公認モジュールの管理

公認モジュールとして認定したソフトウェアの品質管理は当該ソフトウェアの開発者や開発コミュニティでおこなわれるが、政府は各地域に当該ソフトウェアの利用を推奨した責任を有する。そのため公認モジュールとして相応の品質を維持する必要があるため、普及管理団体はソフトウェア更新や脆弱性情報を継続的に収集・監視して品質管理をおこなう。その結果、品質上のリスクが認められたソフトウェアに対して、普及管理団体はソフトウェアの開発元にバグや不具合の報告することで品質維持をおこなう。ただ、その場合、挙がってきた報告への対応義務は開発元、もしくは開発コミュニティにはないため、不具合が修正されない可能性がある。そのため、普及管理団体も当該ソフトウェアの開発コミュニティに参画し、普及管理団体自身が不具合箇所を追加・修正してソフトウェア本体への反映を依頼するなど、メンテナンスや機能拡張に向けた活動が必要となる。問題が解決されずにリスクの解消見込みが立たない場合は、公認モジュールとしての適合性を判断の上、公認モジュールの一覧から当該ソフトウェアを削除し、代替えの候補モジュールの選定と認定を行うなど、普及管理団体としての対応策詳細を考慮しておく必要がある。

また、公認モジュールは各地域がライセンスフリー無償で利用可能なライセンスを有するソフトウェアの中から選定するが、各ソフトウェアのライセンスを保有し管理する権限があるのは当該ソフトウェアの開発者、もしくは開発コミュニティである。そのため、政府はライセンスに対していかなる権限も保有していないが、自治体等が当該ソフトウェアを生活用データ連携基盤のモジュールとして利用する上で問題がないライセンスかどうかを管理する義務がある。そのため、普及管理団体は当該ソフトウェアのライセンス情報を継続的に監視することが必要となる。ライセンスの管理にあたっては、ライセンスの権限が各ソフトウェアの開発者、もしくは開発コミュニティにある以上、将来的にライセンス変更によって有償化される可能性もあり、詳細な対応方法を政府と普及管理団体が実運用の中で定義する必要がある。

## (2) 公認モジュールの利用促進

各地域の生活用データ連携基盤への公認モジュールの実装を目的に、普及管理団体は各地域に対して公認モジュールの導入に必要な情報の提供や支援、普及活動を担う。必要な支援内容は以下と考える。

### ④ 公認モジュールの導入支援

#### (ア) 公認モジュールの利活用プロセス・ドキュメントの整備

公認モジュールとして認定したソフトウェアの開発コミュニティ側の GitHub 等の URL 等の情報とともに、生活用データ連携基盤における公認モジュールの構築手順を整備した上で取扱説明として普及管理団体が管理運営する HP 等で各地域に対して公開する。

#### (イ) 各地域への案内

HP 等での情報提供に加えて、生活用データ連携基盤の構築を検討している各地域に対して、官民協議会等との連携によって作成する構築事業者リストの提供や、自治体向けセミナー等の開催によって、公認モジュールの導入に向けた実用性が高い情報を提供する。

また、各地域から事業者に公示する生活用データ連携基盤構築に関する委託仕様書において、各地域の仕様書内容検討に掛かる負荷を軽減するために、公認モジュールに関する構築手順や考え方などの標準的な内容を雛形として提供する。なお、雛形に記載する内容の検討にあたっては、政府や各地域、事業者及び有識者による検討会等を経て取りまとめる必要がある。

#### (ウ) 技術的な問合せ対応

公認モジュールに関する情報は協調領域として共通的に公開されるものであり、各地域と生活用データ連携基盤の構築事業者は公開情報を基に自力で実装をすることが前提である。とはいえ、生活用データ連携基盤の構築段階において各地域から委託を受けた事業者から技術的な問合せ要望が来ることが想定され、各地域への公認モジュールの導入には一定のサポートが必要であり、普及管理団体では問合せに対するヘルプデスクの設置を想定している。ヘルプデスクが提供するサポートレベルの検討にあたっては以下図を参照にする。

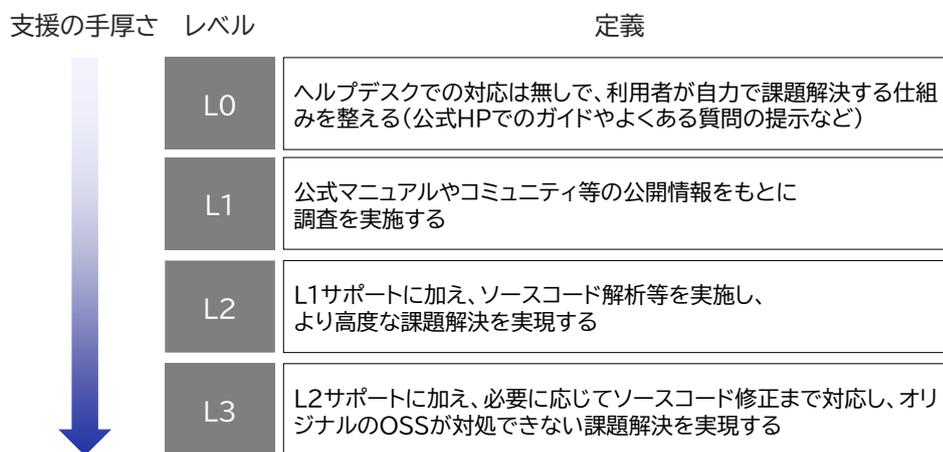


図 4-1-3-1 サポートレベルに関する考え方

先述したとおり、生活用データ連携基盤への公認モジュールの導入で生じた課題は各地域が構築事業者とともに公開情報から自力で解決することが前提であるが、図のサポートレベル L2 までの範囲においては公認モジュールの普及を組織ミッションとする普及管理団体として公認モジュールに関する詳細情報を提供することにより課題解決に貢献できる可能性がある。また、L3 においても、公認モジュール自体の問題で起因する課題である場合は、ソフトウェアの修正等をソフトウェア開発元や開発コミュニティへの報告等をするなどして普及管理団体としても解決に向けた活動が必要となる。どこまでのレベルでヘルプデスクが各地域をサポートするか

は、サポートに掛かる体制整備や運用の費用、各地域や事業者からの実需を懸案した上で策定することが望ましいと考える。

#### ⑤ 公認モジュールの普及展開

公認モジュールの導入・利用活性化に向けた普及活動である。普及管理団体においては、主に公認モジュールの利用に関する情報の発信、公認モジュールの普及・利用活性化に向けたセミナーや勉強会の開催、導入状況の調査をおこなう。政府においては、普及管理団体におけるモジュール利用活性化施策や普及活動を支援する。普及管理団体の具体的な業務は以下を想定している。

##### (エ) 公認モジュールの利用に関する情報の発信

公認モジュールの導入方法に関するガイダンスや各地域における活用事例、公認モジュールの更新情報やセミナー開催情報などを普及管理団体が管理する HP やメルマガ等で発信

##### (オ) セミナーや勉強会の開催

公認モジュールの導入方法をレクチャーする勉強会や、各地域における公認モジュールの活用事例を紹介するセミナー等を開催

##### (カ) 公認モジュールの導入状況の可視化

各地域の生活用データ連携基盤への公認モジュールの利用実態の調査し、導入状況を HP 等で公開

## 4-2. 組織体制の定義

### 4-2-1. 実行体制の定義

普及管理団体の構築にあたって、前節「4-1. サービス内容の定義」で定めたサービス内容を実行する上で必要な組織要件を整理する。普及管理団体は各地域が構築する生活用データ連携基盤における必要な機能を提供し協調領域での相互運用性を担保することで、各地域における競争領域での発展を支援する役割を担う。また、普及管理団体は政府が認定する公認モジュールを普及させるという役割を担うため、組織体制及び活動内容の透明性が求められることも組織構築にあたっては考慮する必要がある。

#### (1) 体制

##### (ア) 活動の統括管理を担う部門

普及管理団体を取り扱う公認モジュールの統括管理および活動全体の統括とともに、政府が主導するモジュールの戦略策定や認定等の検討支援を担う。

##### ① モジュール戦略の策定

生活用データ連携基盤に必要なコア機能の検討やロードマップ策定、認定基準の策定等に関する情報の提供及び支援

##### ② モジュールの認定判断

候補モジュールの調査や選定に関わる情報提供及び支援

##### (イ) 公認モジュールの管理を担う部門

公認モジュールに認定されたソフトウェアの脆弱性やアップデート情報等を定期的に監視することによって公認モジュールとして望ましい品質を維持できているかを管理するとともに、開発元もしくは開発コミュニティと連携して、バグ修正や品質向上に向けた活動を担う。

##### ③ 公認モジュールの管理

一覧管理、定常的な監視、不具合等の対応（既存 OSS 開発コミュニティとの連携）

##### (ウ) 公認モジュールの利用促進を担う部門

公認モジュールの認知を拡大するための普及展開活動及び導入支援のための利用者コミュニティの運営、技術的支援を担う。

- ④ 公認モジュールの導入支援  
公認モジュールに関する情報の公開、問合せ対応
- ⑤ 公認モジュールの普及展開  
公認モジュールの普及・利用活性化に向けた各種施策の実行、公認モジュールの利用状況の調査

## (2) 会議体

公認モジュールの普及・管理に際しての各種意思決定や審議、協議等を実施するためには以下のような会議体の設計が必要と考える。

### ① 生活用データ連携基盤普及戦略会議

政府、普及管理団体、自治体（一部）、生活用データ連携基盤構築事業者、その他関連団体及び有識者によって生活用データ連携基盤における協調領域と競争領域の境界や共通機能としての在り方を検討し、公認モジュールを普及・促進していくための会議体である。主にモジュール戦略の策定やモジュールの認定判断の基準の策定、モジュールの新規開発の要否判断等を行う。

### ② モジュール認定委員会

政府によって実施される公認モジュールの候補ソフトウェアの選定やリスク検証、認定判断を支援する委員会である。モジュールのライセンス内容の検証、脆弱性情報などのセキュリティリスクの検証、サポート有無の検証、ソースコード上のリスク検出を行い、モジュールの公認判定の参考になる情報をとりまとめ、生活用データ連携基盤普及戦略会議に上申する。また、公認モジュールの調達仕様書の雛形を検討する。

## (3) 人材スキル

普及管理団体が担う業務の遂行に必要な人材のスキルイメージは以下を想定している。

### (ア) 活動の統括管理を担う部門

- 公認モジュールの方針策定に関する提言や取組状況の共有などの政府との渉外
- 「生活用データ連携基盤普及戦略会議」での戦略検討、「モジュール認定委員会」での認定基準検討や公認モジュール認定判断に資する関係者意見の取りまとめ及び情報の提供
- 普及管理団体の活動計画の策定及び活動統括

### (イ) 公認モジュールの管理を担う部門

- ソフトウェアの脆弱性監視及び脆弱性への対応
- 公認モジュールの更新情報の発信
- OSS 開発支援

### (ウ) 公認モジュールの利用促進を担う部門

- 公認モジュールの公開に関する情報整備および環境構築（ソースコード整備や利活用プロセスの策定、案内 Web サイトの開設・運用、情報発信）
- 各地域への導入支援対応（技術的な問合せ対応、生活用データ連携基盤開発事業者リストの作成、情報提供、公認モジュールの調達仕様書（雛形）作成）
- セミナー企画・開催
- 公認モジュールの利用実態の調査

## 4-2-2. 事業計画の定義

上記で述べた組織体制を形成し、全国各地での生活用データ連携基盤の構築と安定的な維持運用に向けた事業の運営方法及びロードマップについて検討する。

## (1) 事業の運営方法

公認モジュールの普及管理団体において、関係するステークホルダーにどのような価値を提供し、その活動に必要な財源をどのような手段で確保するかについて検討した。事業の全体像は下図の内容を想定している。

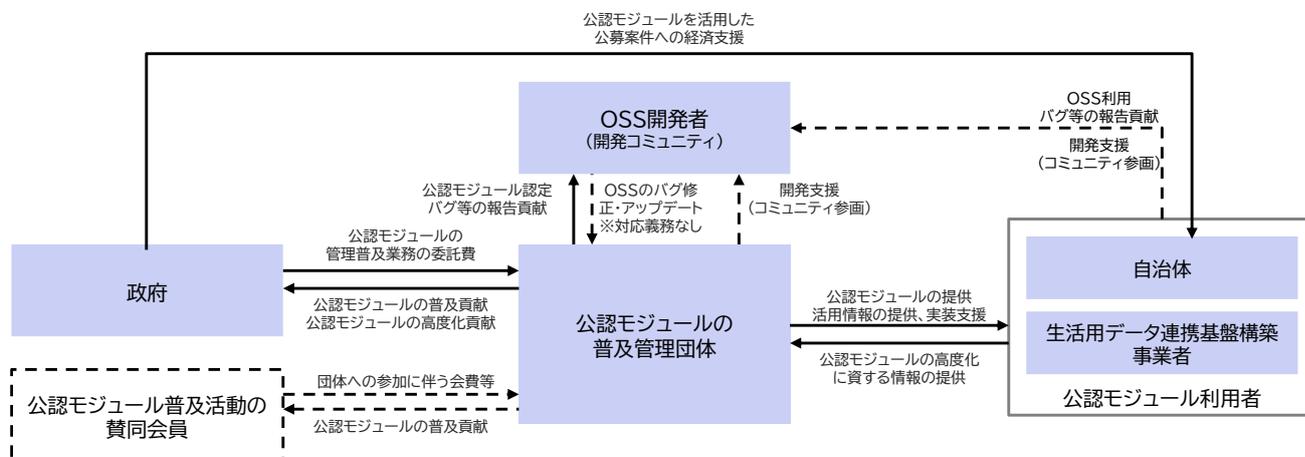


図 4-2-2-1 ステークホルダーとの価値関係図

### ① 公認モジュール利用者との関係

公認モジュールの利用者である自治体や生活用データ連会基盤構築事業者に対しては、公認モジュールに関する情報の提供や問合せ対応など、協調領域の範囲内で必要な支援を実施する。それに対して、公認モジュール利用者からは、公認モジュールの高度化に資する利用実態等の情報提供を求める。協調領域を超えて、利用者にて公認モジュールを実装する際に生じる問題や機能拡張要望等があれば自力による解決やOSS開発コミュニティとの連携を期待する。

### ② 公認モジュール普及活動の賛同会員との関係

公認モジュール普及活動に賛同する方を募り、経済補助を含む活動支援を受けることを目指す。賛同者としては、生活用データ連携基盤構築を行うことでメリットを享受する事業者や公的団体を想定する。

### ③ 政府との関係

普及管理団体の運営維持において賛同者からの支援が確保できるかが不可欠であるが、安定的な維持運営ができるようになるまでに、政府からの経済補助を含む活動支援を受けることが適当であると考え。普及管理団体として、公認モジュールの普及及び高度化に貢献することで政府の方針に資することを想定する。

### ④ OSS開発者（開発コミュニティ）との関係

公認モジュールとして認定されたソフトウェアを管理するOSS開発コミュニティに対しては、OSSのバグ報告や開発支援に参画することでOSSの普及や機能向上に貢献する。一方で、OSS開発コミュニティから提供されるバグ修正・アップデート情報を監視することで、公認モジュールとして望ましい品質が維持されているかどうかを管理する。

## (2) 公認モジュールの普及に向けた組織構築ステップ

普及管理団体の初期の活動においては、政府によって認定された公認モジュールを管理すること及び各地域に対して公認モジュールを周知し、構築する生活用データ連携基盤に導入してもらうための支援や普及展開などの活動を着実に遂行するための体制整備が必要であると考え。

各地域での公認モジュールの導入が進んだ段階で、利用の公認モジュールの導入状況や活用方法等の

事例を収集し、協調領域における共通機能としての公認モジュールの戦略検討や、必要機能の拡充に向けた公認モジュールの追加を実現する体制を拡大していくことが望ましいと考える。

## 5. まとめ

以下に各ステップ毎のまとめを述し、本調査研究報告書のまとめとする。

### (1) ステップ 1：技術基準の定義

生活用データ連携基盤に必要なビルディングブロックとして、「API ゲートウェイ」「ブローカー（非パーソナル）」「ブローカー（パーソナル）」の3つが最低限必要であると導出された。

また、相互運用性の確保はデジタル社会の実現に向けた重要な概念であり、最低限、データを API を通じて相互にやり取りするための API の公開及び API の利用規約についての基準と、静的及び動的を含む様々なデータを扱うためのデータモデルの基準が必要と考えられる。

### (2) ステップ 2：公認モジュールの決定

API ゲートウェイが満たすべき要件につき、様々なクラウドサービスで使われている AWS、GCP、Azure から要件を抽出。要件に当てはまる OSS を調査した結果、Kong Gateway が API ゲートウェイの公認モジュールに相応しいと判断する。ただし、必須要件を満たしていることや、API ゲートウェイが提供する機能は API やデータモデルの仕様には直接影響しないことを踏まえれば、API ゲートウェイ製品の選定は公認モジュールに限定せず、開発者や運用者が使い慣れた製品を採用することを推奨する。

ブローカー（非パーソナル）が満たすべき要件は、データ連携基盤技術報告書にて定義済みの要件とする。要件に当てはまる OSS を調査した結果、最もブローカー要件への適合性が高く、かつ OSS の成熟度の観点から FIWARE Orion が公認モジュールに相応しいと判断する。

ブローカー（パーソナル）が満たすべき要件は、パーソナルデータ活用に向けて、個人情報保護を考慮しながらそのデータの価値を有効活用するため、オプトイン・オプトアウト、セキュリティ担保への対応が必要となる事を踏まえ本調査業務にて整理を行った。要件に当てはまる OSS につき欧州のデジタルサービス活用事例を基に調査を行ったが、本検討で調査した範囲において、パーソナルデータを流通させる機能を満たすブローカーが OSS として公開されている事例はなかった。ただし、本検討で調査対象とした事例では日々新たなプロジェクトが検討されており、その中でブローカー（パーソナル）について言及される可能性があることには留意されたい。

これらの検討により、生活用データ連携基盤に必要な機能群、各ビルディングブロックが有すべき技術基準が定まったことで、相互運用性の担保に向けた一助となると考える。

### (3) ステップ 3：モジュールの継続的な運用の定義

公認モジュールの継続的な運用には、普及・管理団体による品質の管理やモジュールが利用されるようなインセンティブの検討が必要である。各地域での生活用データ連携基盤の構築・サービス発展に寄与する公認モジュールの利用活性化と継続的な運用には、公認モジュールのラインアップの充足や品質管理等をおこなう「モジュールの管理」サービス、公認モジュールの周知や普及展開等をおこなう「モジュールの利用促進」サービスの2点が必要であると考えられる。なお、組織体制の定義にあたっては、今後普及が開始される公認モジュールが一般化して普及管理団体が十分な運営資金を確保できるようになるまでに時間を要することが予想されるため、設立当初は公認モジュールを普及させるために普及管理団体として担うべき最小限の必要機能を精査した上で組織設計をすることが望ましいと考えられる。サービス提供における政府、普及・管理団体、自治体の役割については表 4-1-2-2 を参照されたい。

また、公認モジュールの普及・管理団体を含めたステークホルダーとの価値関係図は図 4-2-2-1 を参照されたい。普及・管理団体は、公認モジュールの利用者である自治体や生活用データ連会基盤構築事業者に対して、公認モジュールに関する情報の提供や問い合わせ対応など、協調領域の範囲内で必要な支援を実施する。それに対して、公認モジュール利用者からは、公認モジュールの高度化に資する利用実態等の情報提供を求める。協調領域を超えて、利用者にて公認モジュールを実装する際に生じる問題や機能拡張要望等があれば自力による解決や OSS 開発コミュニティとの連携を期待する。また、普及管

理団体内に構築する開発コミュニティにおいては、公認モジュールのメンテ・機能拡張に関する貢献も期待する。

普及・管理団体の初期の活動においては、政府によって認定された公認モジュールを管理すること、および各地域に対して公認モジュールを周知し、構築する生活用データ連携基盤に導入してもらうための支援や普及展開などの活動を着実に遂行するための体制整備が必要であると考ええる。

これらの検討結果が、公認モジュールが継続的に運用されていくための考え方の一助となると考える。