第5回 エリア・データ連携基盤 技術セミナー（FIWARE Orion / Kong Gateway編）

2023年7月31日

DATA-EX
Data Society Alliance

©Data Society Alliance 2023

アジェンダ・本セミナーの位置づけ

- 前提となる技術知識 / 用語について
- エリア・データ連携基盤のシステム構成要素
- FIWARE Orionについて
- Kong Gatewayについて
- 構築デモ
- 質疑応答

非パーソナルデータを取り扱う前提で説明を行います。パーソナルデータを取り扱う必要がある場合は、先日開催した第2回 ～ 第4回 エリア/データ連携基盤 技術セミナー（パーソナルデータ連携モジュール編）の開催レポートを参照ください。
https://data-society-alliance.org/

アンケート協力のお願い
セミナー終了後、お申込み時のメールアドレス宛にアンケート依頼を送付予定です。
DSAの支援内容について率直なご意見・ご感想をぜひお聞かせください。
(匿名形式, 目安時間:数分)

©Data Society Alliance 2023

エリア・データ連携基盤の構築に関連する技術知識 / 用語

©Data Society Alliance 2023

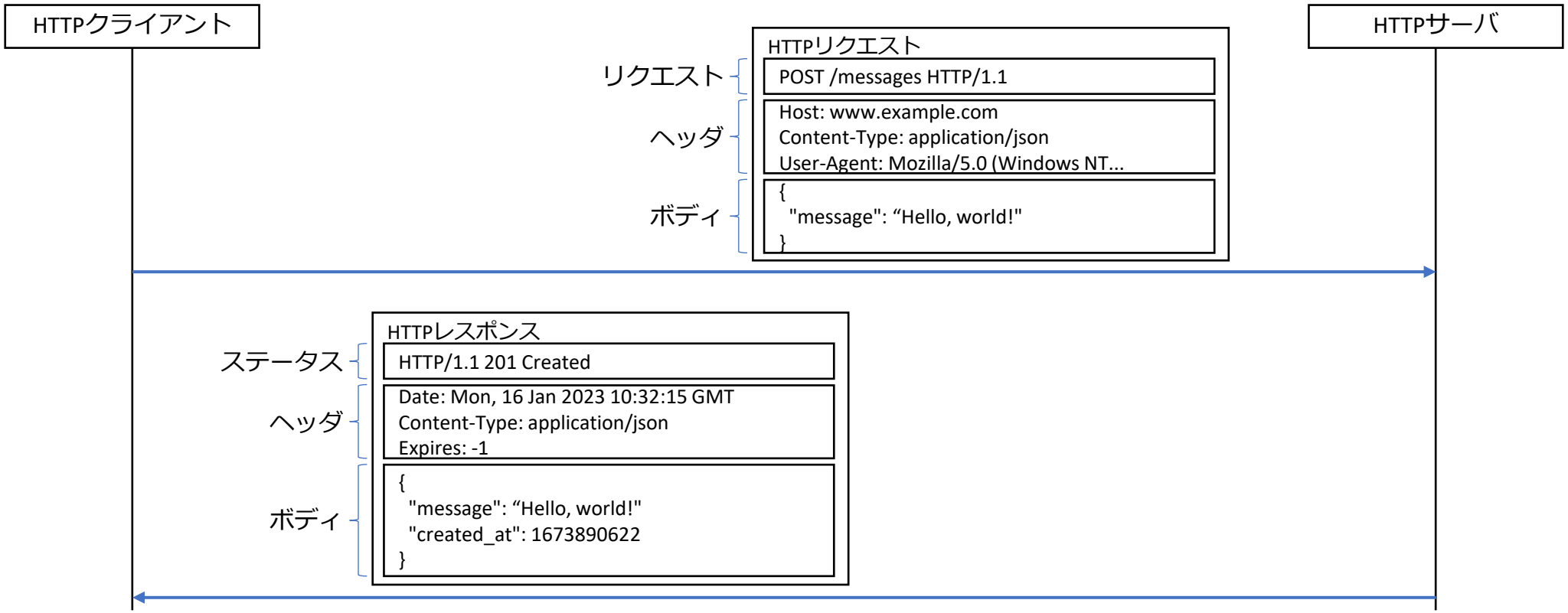
構築に必要となる技術知識 / 用語

- HTTP / HTTPS
- API / Web API / REST API / NGSIv2
- REST API
- OpenAPI仕様
- APIゲートウェイによるAPI管理

©Data Society Alliance 2023

HTTP / HTTPS

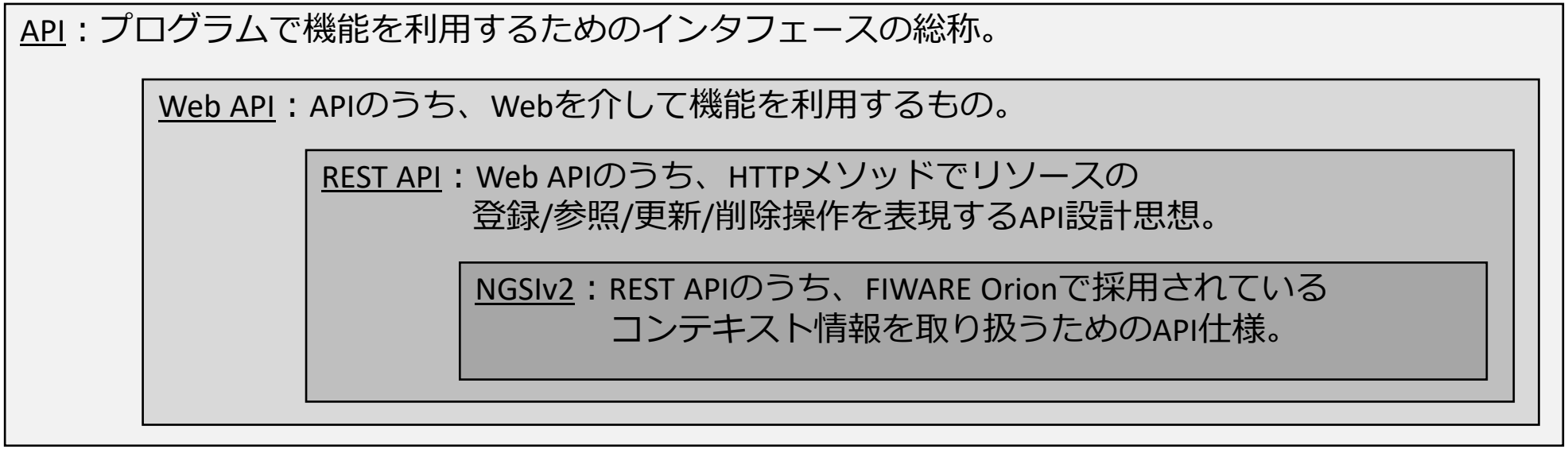
- クライアント～サーバ間のコネクション（HTTPSの場合はSSL/TLSにより暗号化されている）上でメッセージをやりとりするプロトコル。Webブラウザをはじめとして、インターネットを介した通信を行う多数のアプリケーションが採用しています。



©Data Society Alliance 2023

API / Web API / REST API / NGSIv2 の関係

- API (Application Programming Interface) とは、プログラムから機能を利用するためのインタフェースの総称。Web API、REST API、NGSIv2は下図のような包含関係にあります。
- YouTubeやFacebookなどサービスが提供するAPIは、REST APIとして設計されるのがデファクトスタンダードとなっています。



▲ API / Web API / REST API / NGSIv2 の関係

©Data Society Alliance 2023

REST APIの設計思想

- REST APIは、リソースをパスで、アクションをHTTPメソッドで表現するAPI設計思想です。近年公開されているWebサービスのAPIは、ほとんどがREST APIに準拠した設計となっています。
- GETのパラメータはURL内のクエリパラメータで、それ以外のパラメータはBodyに記載するのが一般的です。

▼ HTTPメソッドとCRUDの対応

	Method	用途
Read	GET	リソースの参照
Write	POST	リソースの登録
	PUT	リソースの更新
	PATCH	リソースの部分更新
	DELETE	リソースの削除

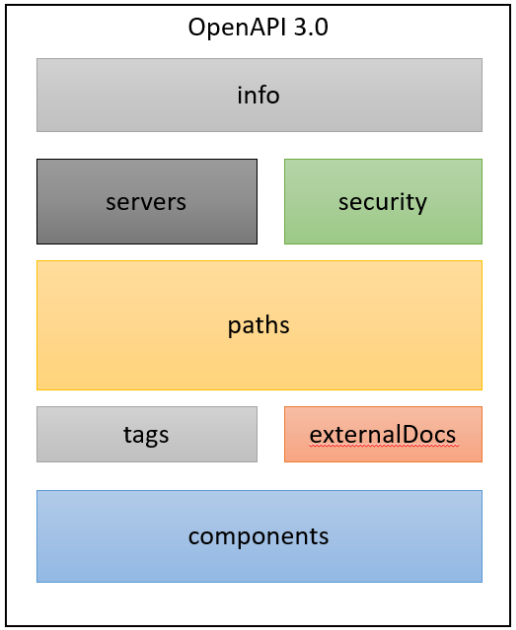
▼ 記事とコメントが管理できるサービスのAPI例

用途	Method	Path
記事一覧の取得	GET	/articles
記事の登録	POST	
記事の参照	GET	/articles/{articleId}
記事の更新	PUT	
記事の部分更新	PATCH	
記事の削除	DELETE	
コメント一覧の取得	GET	/articles/{articleId}/comments
コメントの登録	POST	
コメントの参照	GET	/articles/{articleId}/comments/{commentId}
コメントの更新	PUT	
コメントの部分更新	PATCH	
コメントの削除	DELETE	

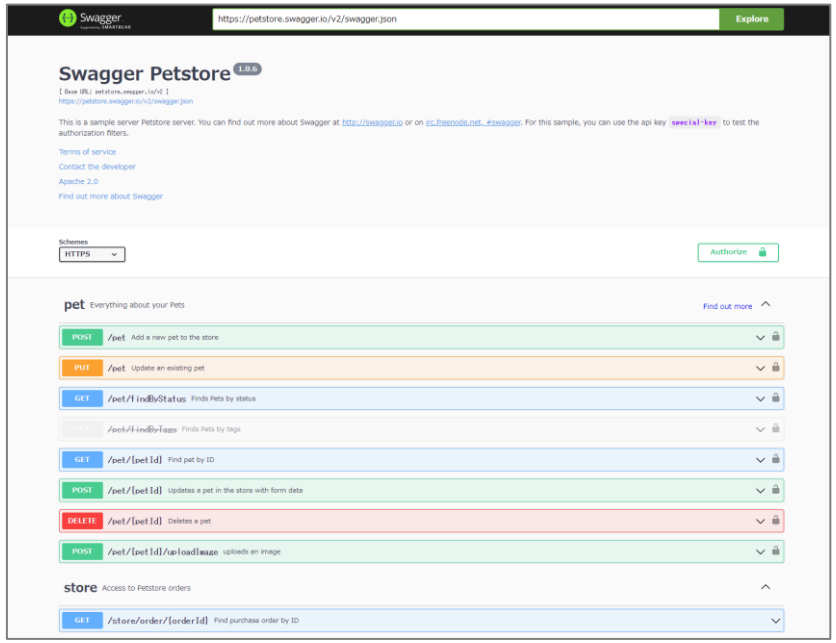
©Data Society Alliance 2023

OpenAPI仕様によるREST API設計

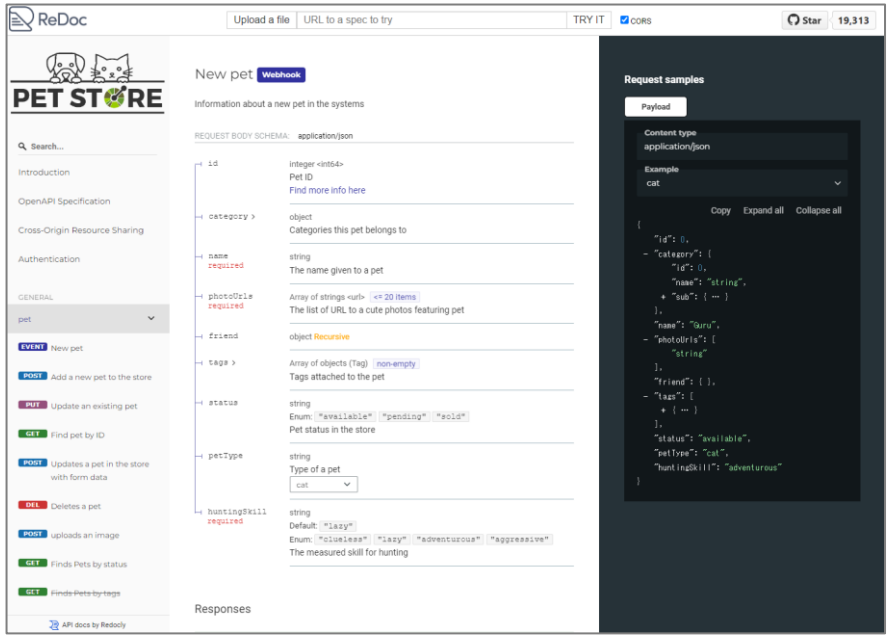
- REST APIの設計は、OpenAPI Specification（API設計書の書き方の仕様）に準拠した形で記載するのがデファクトスタンダードとなっています。
- OpenAPI Specファイルは、SwaggerUIやRedoc等の外部ツールに読み込ませることでWebブラウザで見やすく表示することができます。



▲ OpenAPI Specの構造。
実際はYAMLかJSONで記載される。



▲ SwaggerUIでAPI仕様を表示した例。

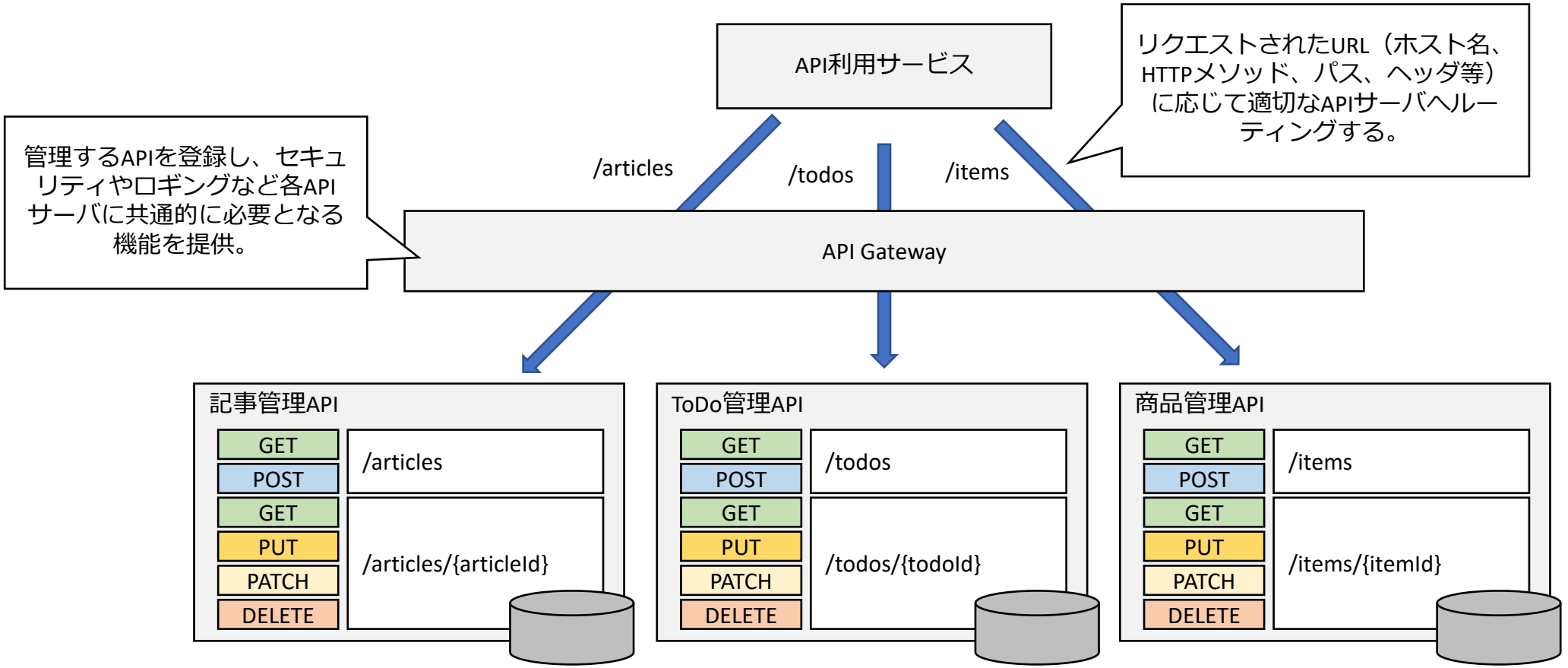


▲ RedocでAPI仕様を表示した例。

©Data Society Alliance 2023

APIゲートウェイによるAPI管理

- APIゲートウェイは、複数のAPIサーバが提供されるとき、そのリクエストの受け口をまとめるリバースプロキシです。APIサーバーとAPI管理機能が分離でき、システムの疎結合化、共通管理機能の集約化による利便性やセキュリティの向上が見込めます。



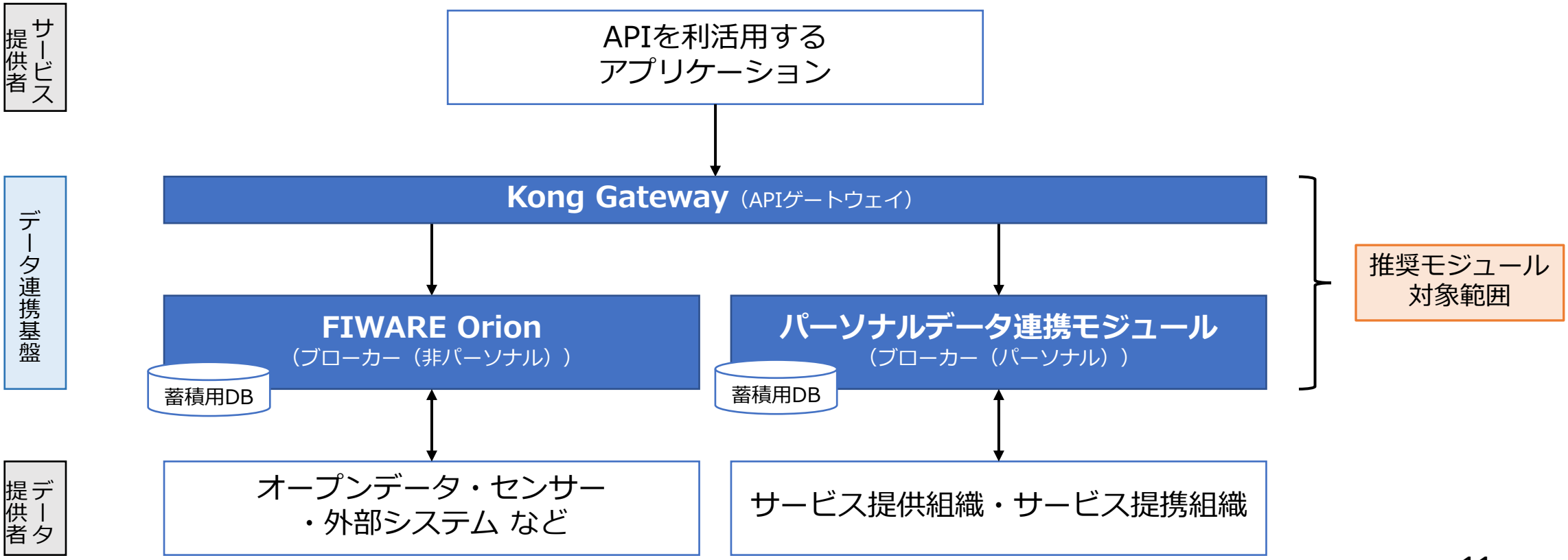
©Data Society Alliance 2023

エリア・データ連携基盤のシステム構成

©Data Society Alliance 2023

推奨モジュールを用いたエリア・データ連携基盤の構成例

- APIゲートウェイはアプリケーションからのAPIリクエストを受けつけ、ルーティング、認証・認可、ロギングなどトラフィックの制御やセキュリティの管理を担います。
- ブローカーはデータの取得・収集・配信などデータ連携やデータ管理を担います。



©Data Society Alliance 2023

更新

推奨モジュールの導入事例紹介

- 令和4年度、DSAは推奨モジュールを活用したデータ連携基盤の構築先行事例を調査いたしました。本調査研究の報告書※1は、デジタル庁Webサイトにて公開済です。
- DSAのWebサイトでも上記のサマリ記事を公開中です※2。

推奨モジュールの導入事例

アンケートにおいて推奨モジュールを利用した導入事例の公開に関するご要望がありました。そのため、先行自治体における推奨モジュール導入事例として、推奨モジュールと他機能との連携状況を図式化した≪データ連携処理概念図≫、≪事業内容≫、≪推奨モジュールの利用事例≫を以下の基準のもと、公開します。

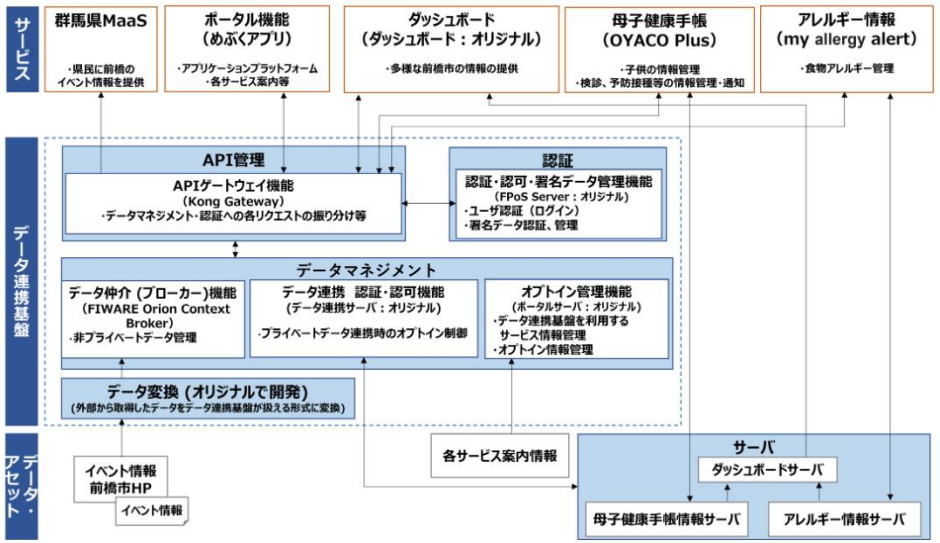
・データ連携基盤を複数の自治体で共同利用している事例
・データ連携基盤と連携しているサービスの取り組み内容に特徴がある事例

事例	取り組みの特徴
事例①群馬県/群馬県前橋市	県と市でデータ連携基盤を共同利用する取り組みを行っている。
事例②福島県会津若松市	様々なベンダーのデータを利用して、複数の分野でサービスの提供を行っている。
事例③埼玉県秩父市	市区町村で共同利用しており、災害時ドローン配送サービスのために物流分野で利用している。
事例④岡山県西粟倉村	森林植生データなどを観光サービスや森林活用斡旋サービスなどの異なったサービス分野で利用している。
事例⑤北海道江別市	健康関連の実証研究を大学と連携しながらおこなっており、健康・医療分野に特化して利用している。
事例⑥静岡県焼津市	避難情報を市民にメール・SNSで配信するために、防災分野で利用している。

■事例①群馬県/群馬県前橋市

《取り組みの特徴》
県と市でデータ連携基盤を共同利用する取り組みを行っている。

《データ連携処理概念図》



※1 “デジタル田園都市国家構想の実現に向けた生活用データ連携基盤におけるデータ仲介機能に関する機能及び運用等に係る調査研究令和4年度 調査報告書”, 2023-03-31, https://www.digital.go.jp/budget/entrustment_deliverables/ (参照:2023-07-30)
※2 “データ連携基盤における推奨モジュールの普及状況と導入事例”, https://data-society-alliance.org/area-data/survey (参照:2023-08-10)

©Data Society Alliance 2023

FIWARE Orion
（非パーソナルデータ向けのコンテキストブローカー）

©Data Society Alliance 2023

FIWARE Orionの役割

- FIWARE Orionは、データ提供者～データ利用者間のデータ授受を仲介します。
(※正確にはデータではなくContextの仲介 = Context broker)
  - 1. データの管理 (登録, 更新, 削除)
  - 2. データの提供
- データ所有者の考え方がなく、個人情報の管理には適さないため、オープンデータに代表される非パーソナルデータ向けブローカーとしての役割を担います。

©Data Society Alliance 2023

[用語] Context, Entity, Attribute, Data

- **Context**：ある対象やイベントの状態・状況を示す情報の集合体
- **Entity**：特定の物理的なオブジェクトやデータ　FIWARE Orionでの管理単位
- **Attribute**：Entityが持つ個々の特性や情報
- **Data**：Attributeの値

Context ≒ Entity(Attribute1, Attribute2, ...) ＋ タイミング/背景など

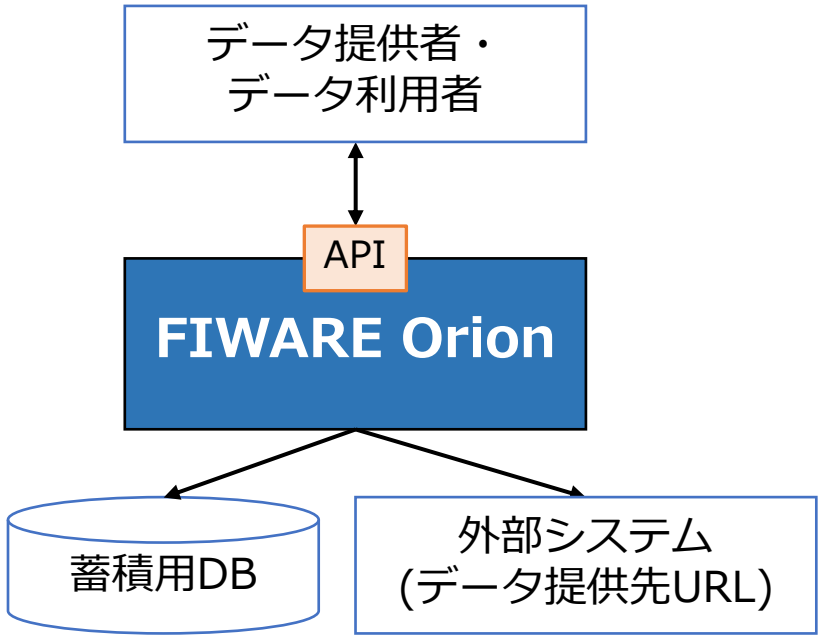
例:

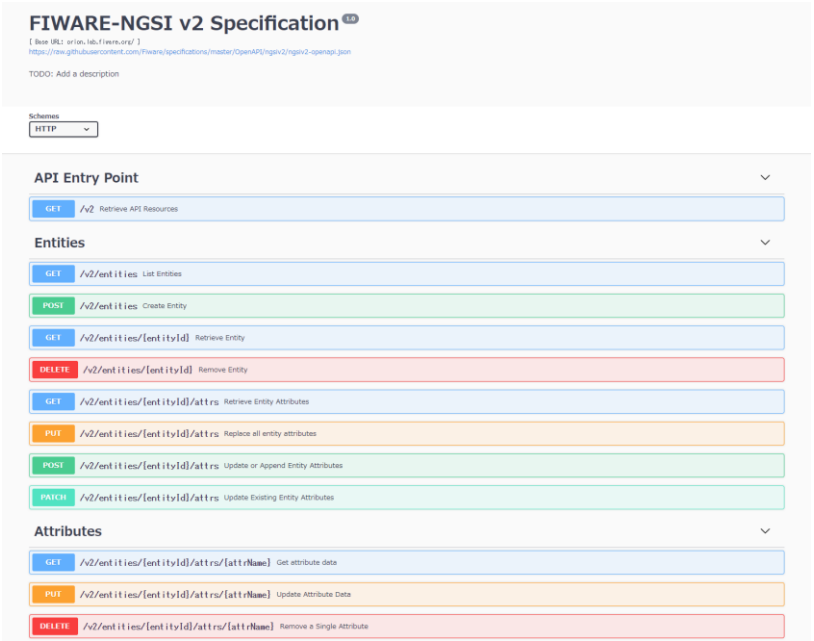
- **Context**：観測所から定期的に通知される気象センサー収集データの最新値
- **Entity**：観測所の気象センサー
- **Attribute**：センサーが収集した気温や気圧 (気温:35 ℃, 気圧:960 hPa)
- **Data**：35 ℃, 960 hPa

©Data Society Alliance 2023

FIWARE Orionの特徴

- FIWARE Orionのデータ管理/データ提供機能は、すべてAPIで操作できます。
- API仕様は予め定められていて(NGSIv2)、かつすべて公開(オープンAPI)されています。
- NGSI ＝ データ形式 ＋ 通信方法のルール





FIWARE-NGSI v2 Specification（公開されているAPI仕様ページ）
https://swagger.lab.fiware.org/

©Data Society Alliance 2023

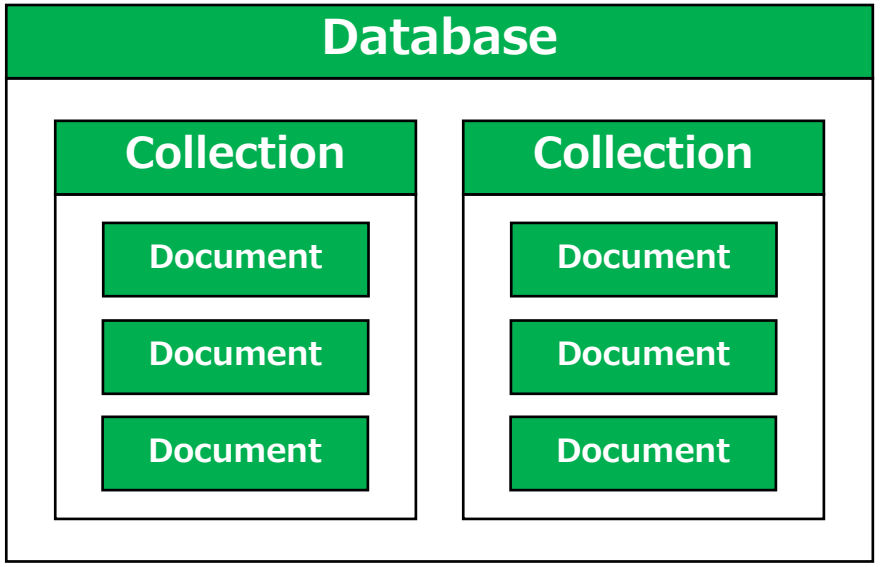
FIWARE Orionが保持する情報

- FIWARE Orionは蓄積用DBとして必ずMongoDBを利用します。
- MongoDBには大別して3種の情報を記録し、このデータ群を元に機能提供しています。
  ①データ提供者が登録したEntityデータ (**Entities**コレクション)
  ②データ提供者が登録したEntityデータ提供先情報 (**Registrations**コレクション)
  ③Entityデータ更新通知の配信先情報 (**Subscriptions**コレクション)

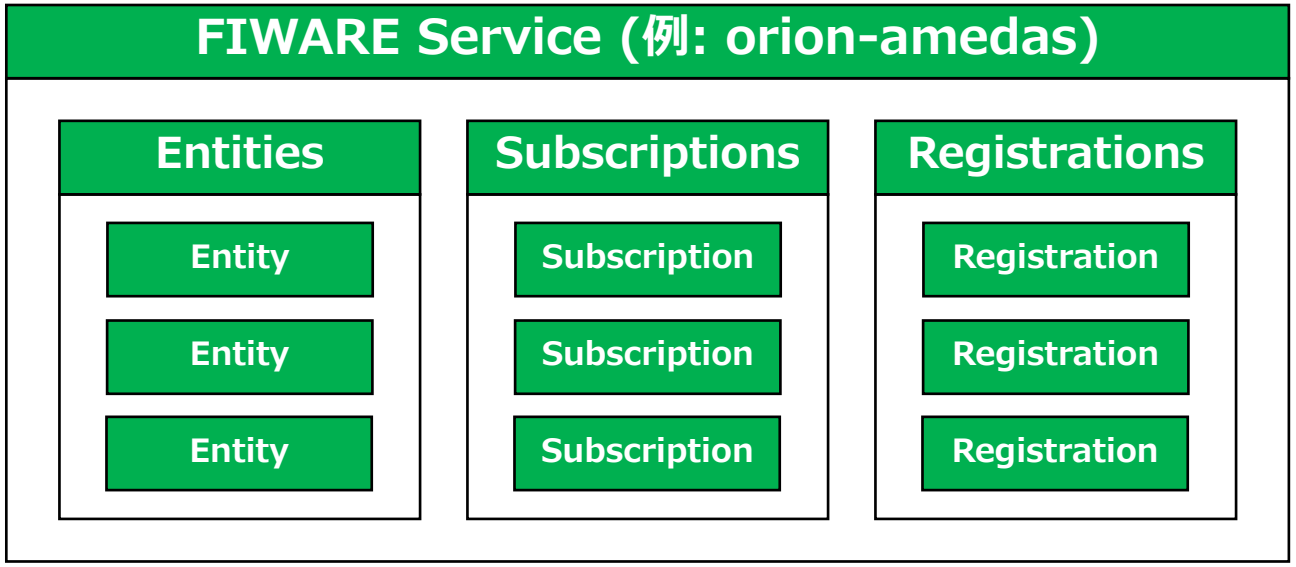
©Data Society Alliance 2023

MongoDBのデータベース構造とFIWARE Orionでの管理方法

- MongoDBではDocumentと呼ばれるJSON形式(BSON)のデータをCollection, Databaseという単位でまとめてデータを管理します。
- FIWARE Orionの3種の情報はCollection単位で管理され、1つのデータベースで情報が完結します。
- MongoDB内に複数のDatabaseを作成し、マルチテナント運用も可能です。



MongoDBのデータベース構造

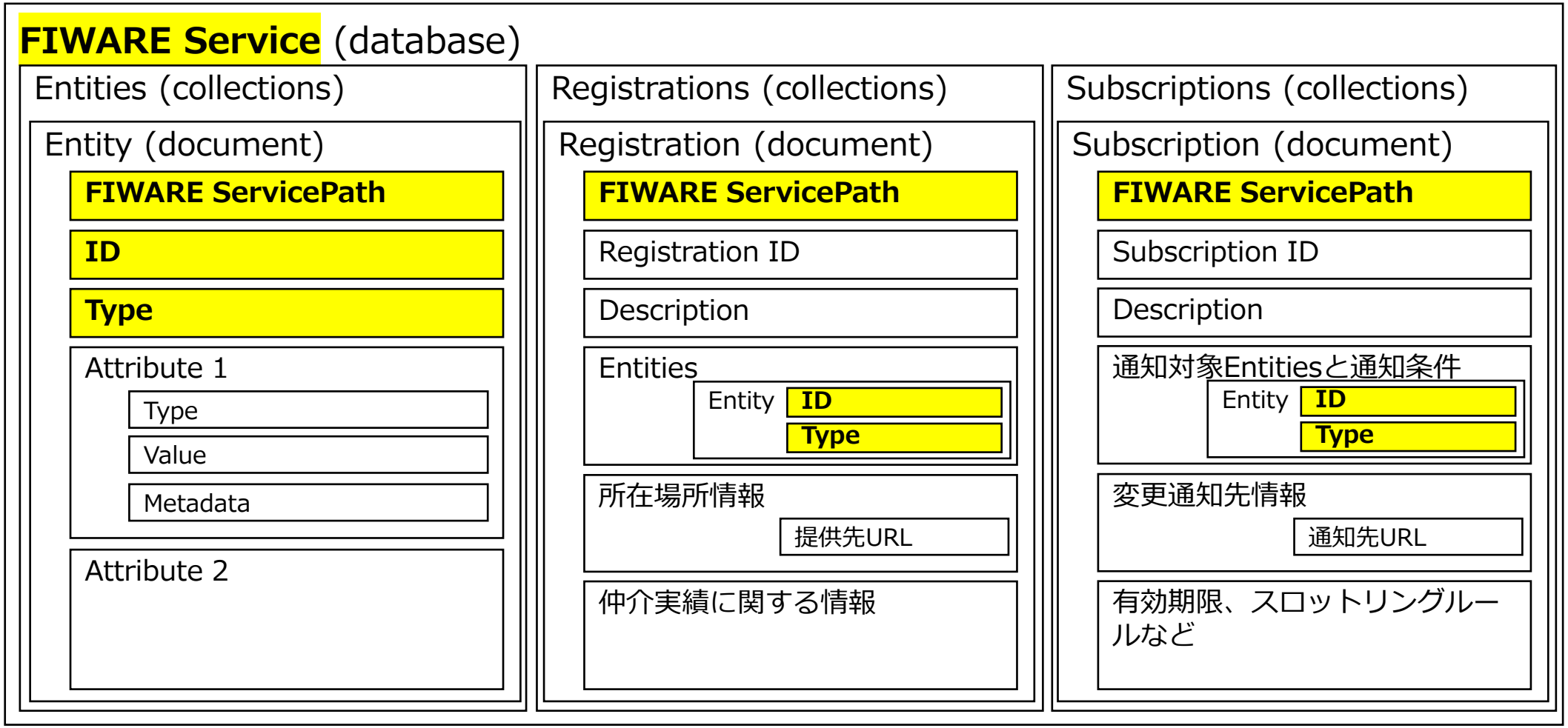


FIWARE Orionのデータ管理構造と名称

©Data Society Alliance 2023

FIWARE Orionのドキュメント構造と取得時の識別キー

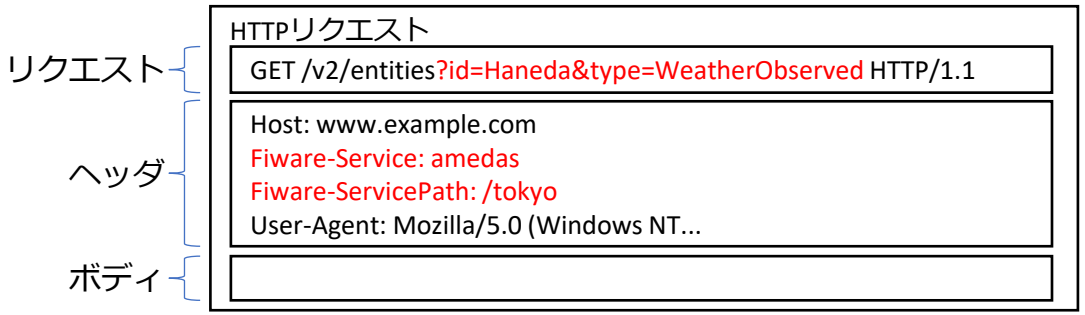
- データ利用時のクエリでは、**FIWARE Service**, **FIWARE ServicePath**, **Entity ID**, **Entity Type**の4項目の複合キーでレコードを検索し、ドキュメントを取得します。



©Data Society Alliance 2023

４種のEntity識別キーの指定方法

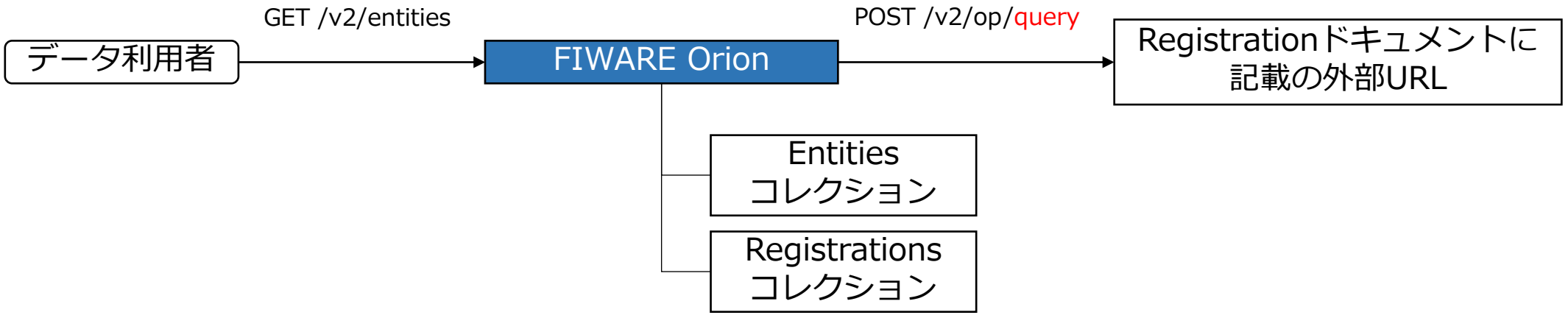
- **FIWARE Service**, **FIWARE ServicePath**はリクエストヘッダーで指定します。未指定の場合はデフォルト値を指定したとみなされます。
  - デフォルト値
    - FIWARE Service: (なし) ※データベース名: orion
    - FIWARE ServicePath: **/**
- **Entity ID**および**Entity Type**はクエリパラメータで指定します。未指定の場合、①リスト取得系の場合は検索条件から除外されます。②単一取得系の場合、取得結果が一意にならないとエラーになります。



©Data Society Alliance 2023

データの取得 (GET /v2/entities)

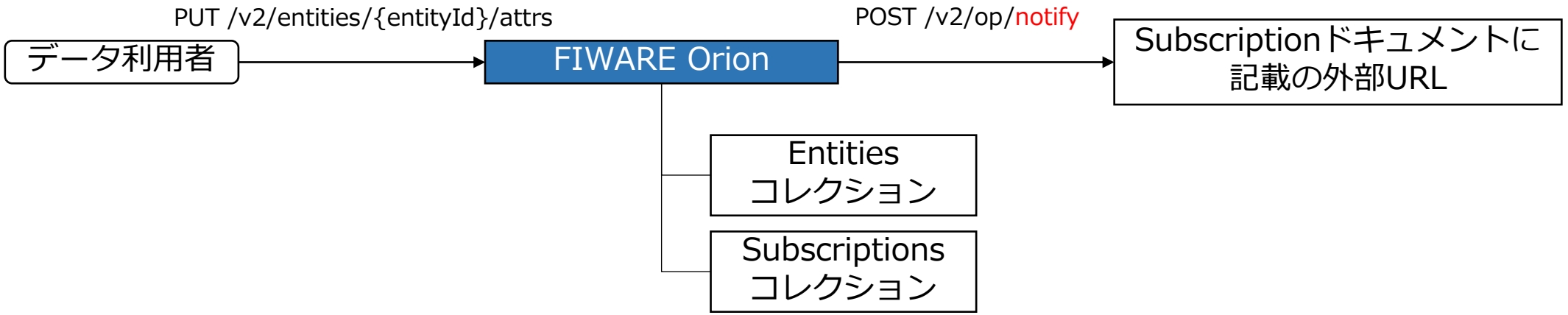
- **GET /v2/entities**はEntityのリストを返却するAPIです。
- ドキュメントの有無に関わらずEntitiesコレクションとRegistrationsコレクションの両方にクエリを実行し、FIWARE ServiceおよびFIWARE ServicePathが合致するEntityドキュメントの一覧を返却します。
- Registrationsコレクションに該当レコードありの場合、OrionからRegistrationに登録された外部URLへクエリを発行します。



©Data Society Alliance 2023

データの更新と更新通知 (例: PUT /v2/entities/{entityId}/attrs)

- **PUT /v2/entities/{entityId}/attrs**はEntityを更新するAPIです。
- ドキュメントの有無に関わらずEntitiesコレクション内でFIWARE Service、FIWARE ServicePath、およびEntity ID が合致するEntityドキュメントを検索します。
- 同様にSubscriptionsコレクション内でクエリを実行し、該当レコードあり かつSubscription記載の条件を満たす場合は、OrionからSubscriptionに登録された外部URLへクエリを発行します。



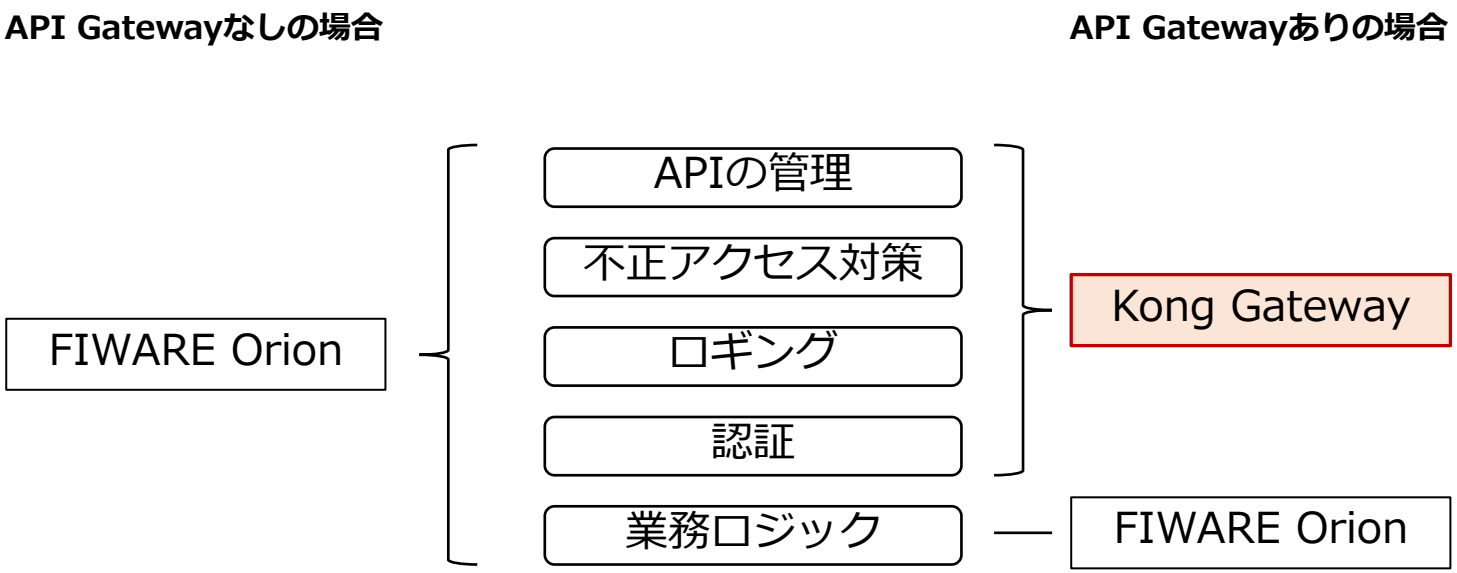
©Data Society Alliance 2023

Kong Gateway
（APIゲートウェイ）

©Data Society Alliance 2023

Kong Gatewayの役割

- APIを個別公開した場合、必ず設定しなければならないセキュリティ機能や運用管理機能等を、APIコンポーネントの代わりに提供します。
- 機能開発の作業負荷軽減だけでなく、個別実装によるセキュリティ/運用管理関連機能の品質不安定化懸念を払しょくすることで、APIの相互運用性の確保に貢献します。



©Data Society Alliance 2023

Kong Gateway：APIゲートウェイの推奨モジュール

- Kong Gatewayは、国内外で広く利用されている代表的なAPIゲートウェイです。コア機能はOSSで提供され、プラットフォームの制約なく利用することが可能です。プラグインによる機能拡張が可能な設計で、拡張性と柔軟性の高さにも優位性があります。

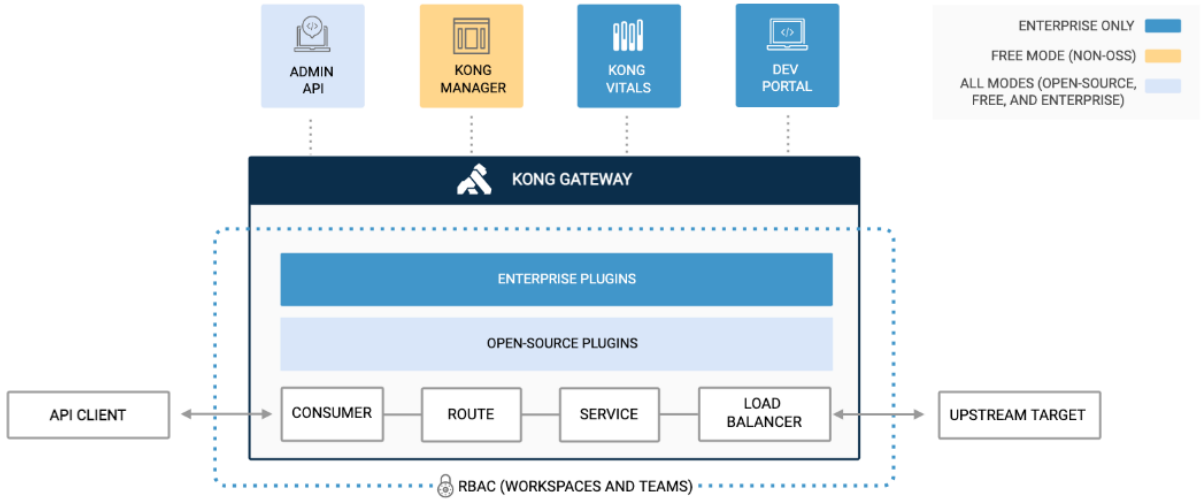
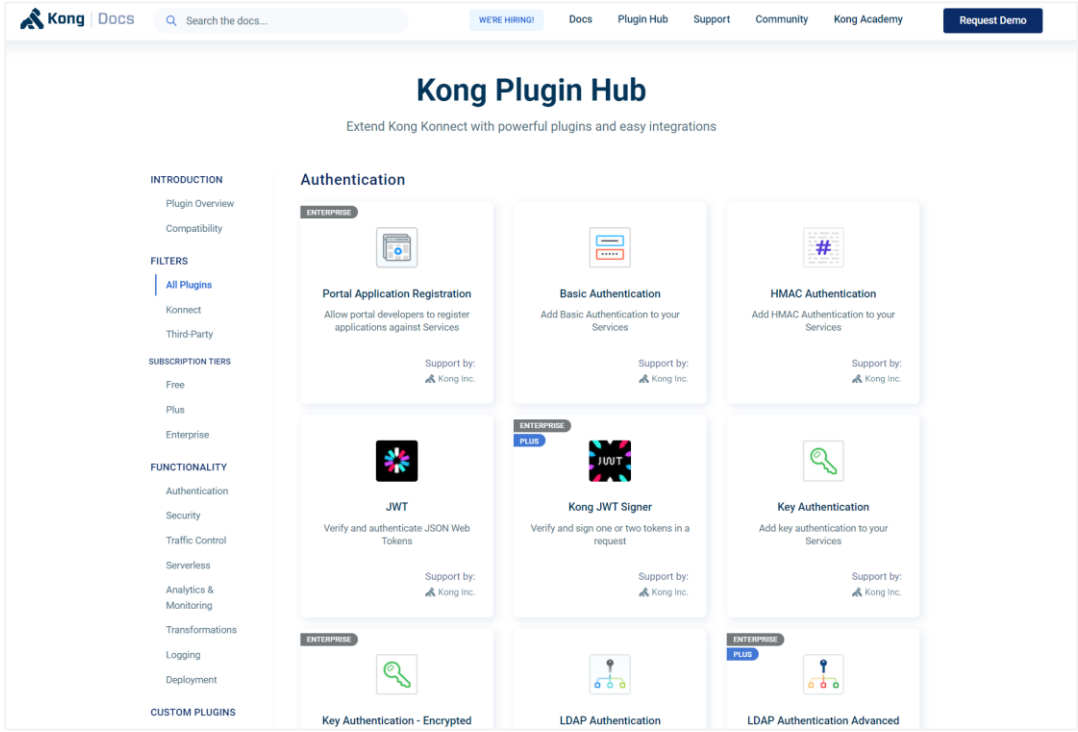


Figure 1: Diagram of Kong Gateway modules and how they relate to the foundational Gateway components. Requests flow from an API client into the Gateway, are modified and managed by the proxy based on your Gateway configuration, and forwarded to upstream services.

Kongドキュメントより引用
https://docs.konghq.com/gateway/latest/



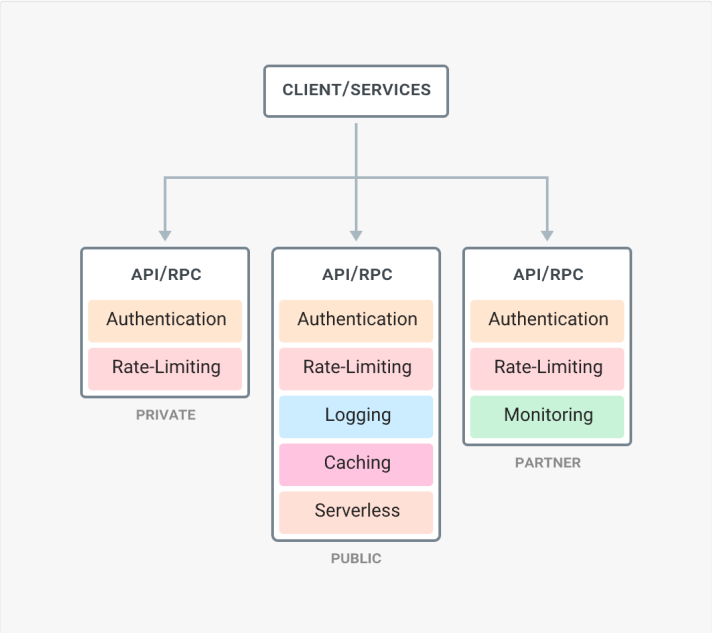
Kongプラグイン一覧ページ
https://docs.konghq.com/hub/

©Data Society Alliance 2023

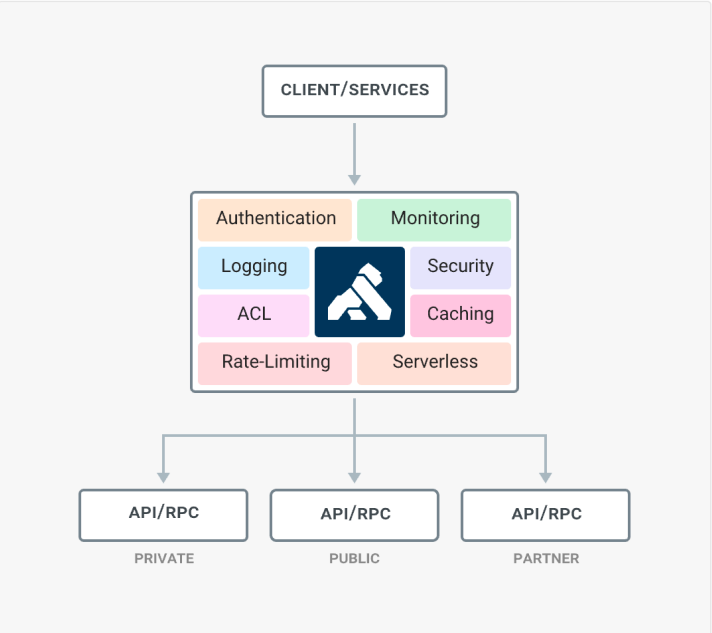
Kong Gatewayの特徴

- APIの公開時に備えるべき、セキュリティ機能、運用管理系機能をプラグイン形式で利用することが可能です。標準的なプラグインはバンドルで備わっていて、システム稼働後も柔軟に設定変更/着脱が可能なことなら、提供するAPIの均質化や、API開発コストの低減を比較的容易に実現することが可能です。

The Redundant Old Way



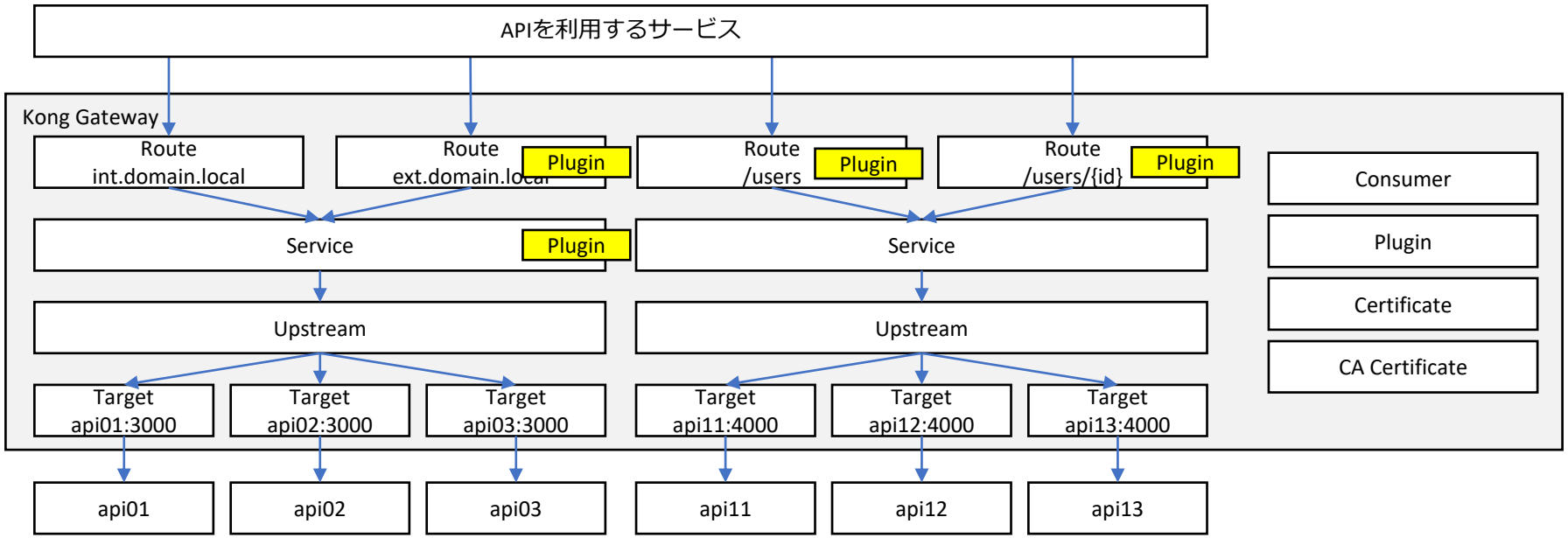
The Kong Way



©Data Society Alliance 2023

Kong Gatewayの内部構成

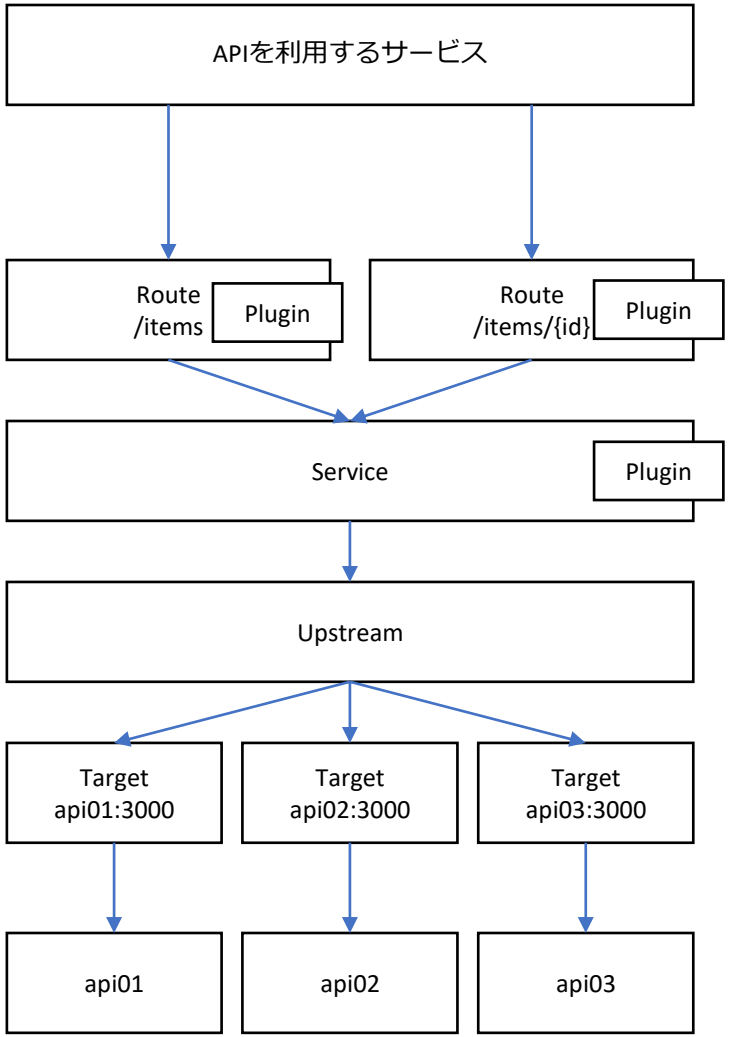
- 外部から受け付けたHTTPリクエストは、Route、Service、Upstream、Targetと内部リソースを辿りAPIサーバへルーティングされます。
- APIリクエストのプロキシ先の種類(Service)ごとに複数のAPI受付パス(Route)が設定可能です。プラグインは全てまたは任意のService、Routeなどへ自由に着脱・および有効無効化の設定が可能です。



©Data Society Alliance 2023

[用語] kong Gatewayの内部リソース

- Service　：APIサービス1つに相当
- Route　：メソッドとパスの組に相当
- Upstream　：Kongの内部ロードバランサ
- Target　：APIサーバ1つに相当
- Consumer　：API利用ユーザに相当
- Plugin　：Service、Route、Consumer、またはグローバルに動作するリクエスト / レスポンスの追加処理



©Data Society Alliance 2023

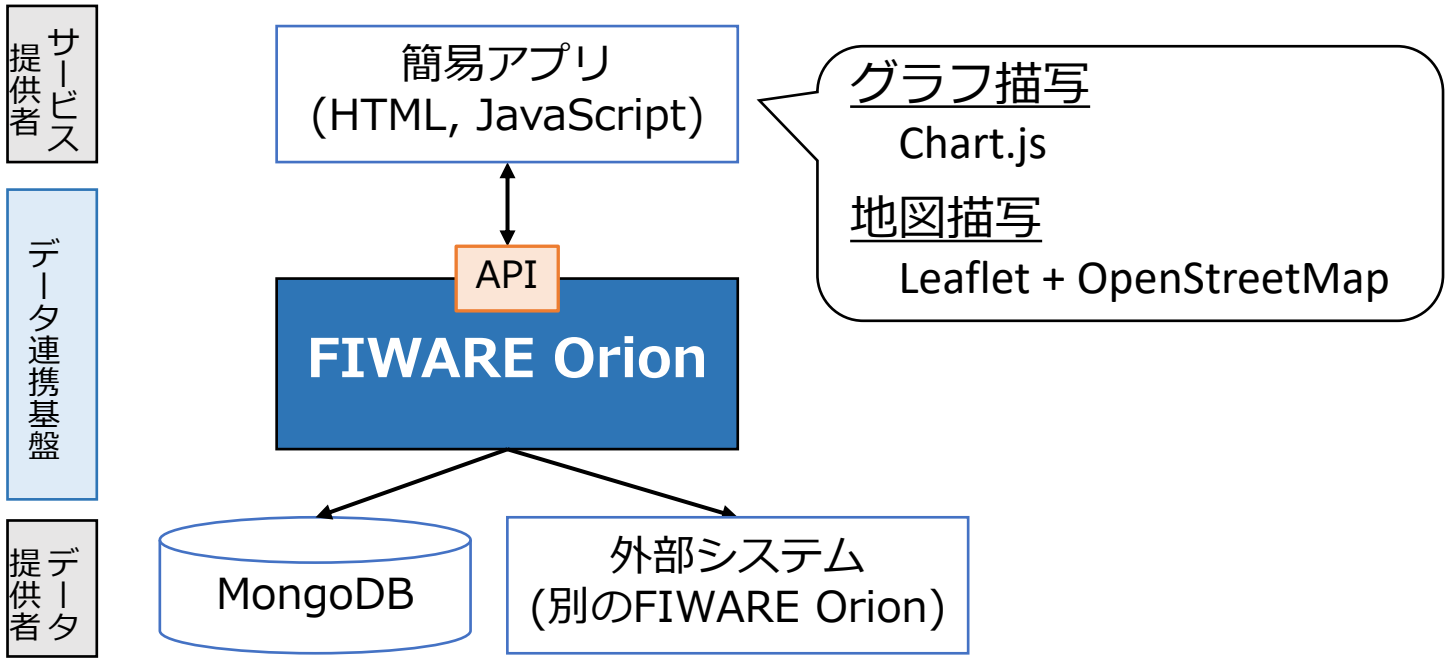
FIWARE Orionによる
データ連携のデモ

©Data Society Alliance 2023

更新

デモ

- FIWARE Orionに登録されたデータが、FIWARE OrionのAPI経由で取得され、データ利用者であるWebアプリケーションでEntityデータが利用できることを確認します。
- FIWARE Orionにデータ提供元URLだけが提供された状態でも、全項目と同様にデータ利用者であるWebアプリケーションでEntityデータが利用できることを確認します。



※当日利用したスクリプト等は「デモ資材.zip」を参照ください。本資材は開発環境での動作確認のみを想定したものです。

©Data Society Alliance 2023

質疑応答

©Data Society Alliance 2023

追加

Q. データ連携基盤の構築にあたり守るべき事項/ドキュメント

- データ連携基盤としての明確な定義や条件はありませんが、システムの構築前提や要件などに準ずる必要があります。該当する取り組みの制度要綱などを参照ください。
- 例えばデジ田交付金の”TYPE1/2/3等制度概要”の申請要件には「オープンなデータ連携基盤を活用して、複数のサービス提供事業者が異なるサービスを提供するものであること」とあり、確認方法として、データブローカー機能やデータモデルなどの条件が列挙されています。
- エリア・データ連携基盤および推奨モジュールの詳細，最新情報に関しては、DSA公式Webサイトに掲載中の「エリア・データ連携基盤に関する取り組み」を参照ください。

※デジタル田園都市国家構想交付金（デジタル実装タイプ）, https://www.chisou.go.jp/sousei/about/mirai/policy/policy1.html, (参照:2023-08-10)
※デジタル田園都市国家構想交付金 デジタル実装タイプ TYPE1/2/3等 制度概要, https://www.chisou.go.jp/sousei/about/mirai/pdf/denenkohukin_2022type123_gaiyou.pdf, (参照:2023-08-10)
※エリア・データ連携基盤に関する取り組み, https://data-society-alliance.org/area-data/, (参照:2023-08-10)

©Data Society Alliance 2023

追加

Q. WAF (Web Application Firewall)の必要性

- システムの規模、アクセス頻度、運用上の制約条件などによって要否が異なります。
  - 必要な可能性が高い事例
    - システムが重要な業務と関連していて、システム停止が重大な損失を招く場合
    - 一般利用者のアクセス数が非常に多く、悪意あるユーザーからの攻撃が懸念される場合
  - 見送られる可能性が高い事例
    - アクセス数が小規模で、Kong Gatewayのセキュリティ設定(IP制限, Bot制限など)で十分対策可能と考えられる場合
    - システムのランニングコストに制限があり、システムの大規模運用がそもそも難しい場合

- 小規模利用では、Kong Gatewayのプラグインを用いたセキュリティ対策のみで対応可能な場合もあります。システムの状況/目的/制約などを総合的に加味して、導入要否を判断することが重要です。

©Data Society Alliance 2023

追加

Q. デモにてWireCloudではなくChart.js/Leafletを用いた理由

- WireCloudはFIWARE Orionと併用されることが多いウィジェット支援ツールです。
- WireCloudを用いることで、FIWARE Orionのデータを用いた簡易的な地図ダッシュボードをGUIで作成することが可能です。
- 本セミナーは、デモの時間に限りがありましたので、htmlファイル単独で動作確認が可能な、Chart.js/Leafletを採用しました。
  WireCloudを利用した場合、WireCloud自体が内部的にどのような処理をしているのかを説明する時間を設ける必要があるなど、本筋以外の説明に時間を要すると判断し本デモでは採用を見送りました。

©Data Society Alliance 2023

まとめ

©Data Society Alliance 2023

FIWARE Orion 要旨

- FIWARE Orionはデータ利用者～データ提供者間のデータ授受を仲介します。
- FIWARE OrionはEntity単位でデータを管理することができます。
- FIWARE Orionを利用することで、APIによるEntityデータの授受が可能になります。
- FIWARE Orionでは3種のコレクションで情報を管理します。
- Entityは4種の複合キーで一意に定まります、これは3種すべてのコレクションで同様です。
- データ取得リクエストがRegistrationに登録されたEntityを要求した時、FIWARE Orionはそのの Registration Entityの提供元URLへクエリを発行し、結果を返却します。
- Subscriptionに登録されたEntityがEntitiesコレクション内で更新された時、FIWARE OrionはそのSubscription Entity通知先URLへ通知を発行します。

©Data Society Alliance 2023

Kong Gateway 要旨

- Kong GatewayはAPIが公開時に具備すべきセキュリティ系/管理系の機能を、APIの代わりに提供します。
- Kong Gatewayはプラグイン形式の機能着脱設定が可能であり、拡張性と柔軟性に優れた代表的なAPIゲートウェイです。プラグインはRoute単位、Serviceなど設定範囲も自由度高く設定することができます。
- Kong Gatewayの標準的なプラグインはバンドルで備わっていて、API品質の安定化を比較的容易に達成することができます。

©Data Society Alliance 2023

補足

©Data Society Alliance 2023

デジタル庁が指定する推奨モジュールについて

©Data Society Alliance 2023

推奨モジュールの位置付け

- デジタル庁の開発提供するブローカー機能を採用せず、同様機能を有するブローカーを活用する場合は、オープンAPIを提供するものであること又は複数地域のデータ連携基盤間のデータ連携を実現すること、などを要件としていますので、推奨モジュールを使用せず上記の要件を満たすことでも問題ありません。
- 推奨モジュールに準拠させることにより、行政事務の効率化を図るとともに、APIゲートウェイを介して各地域のデータ連携基盤とも接続し様々なサービスが展開されるメリットがあります。
- 共通的な基盤や機能を活用しながら、アプリケーションレベルにおいては複数の民間事業者による競争環境を確保して、ベンダーロックインによる弊害を回避することができ、スタートアップや地方ベンダーが自社開発したアプリケーションが全国展開できる可能性が広がるものと考えています。

©Data Society Alliance 2023

エリア・データ連携基盤の構成要素とデジタル庁の推奨モジュールの対応

- 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）のそれぞれについて、下記のソフトウェアの活用が推奨されています。

ビルディングブロック	推奨モジュール	説明
APIゲートウェイ	Kong Gateway	様々な分野でAPIゲートウェイとして広く使われており、国内外の多様なサービスで実績のあるOSS（オープンソースソフトウェア）です。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ます。
ブローカー（非パーソナル）	FIWARE Orion	データブローカーとして国内/国外のスマートシティ事業において多数の実績があるOSSです。データ蓄積とデータ分散双方の機能を具備し、提供される接続インターフェースとしてNGSIv2というオープンAPIで実装されています。
ブローカー（パーソナル）	パーソナルデータ連携モジュール	ブローカー（パーソナル）は、パーソナルデータの流通に必要な同意管理や所在管理などの機能を備えたデータ連携モジュールです。蓄積と共有で個別の同意管理が可能です。

©Data Society Alliance 2023

OSSの位置付け

©Data Society Alliance 2023

5. OSSの位置づけ
5.1. OSSの基本的な考え方

- 推奨モジュールは基本としてOSS（オープンソースソフトウェア）で提供されており、利用条件等についてはそれぞれのOSSライセンスに従います。

  - オープンソースソフトウェア（英: Open Source Software、略称: OSS）とは、利用者の目的を問わずソースコードを使用、調査、再利用、修正、拡張、再配布が可能なソフトウェアの総称

    引用元：オープンソースソフトウェア（ Wikipedia ）

  - オープンソースソフトウェアの定義（基本的な考え方）

    1. 再頒布の自由
    2. ソースコード
    3. 派生ソフトウェア
    4. 作者のソースコードの完全性(integrity)
    5. 個人やグループに対する差別の禁止
    6. 利用する分野(fields of endeavor)に対する差別の禁止
    7. ライセンスの分配(distribution)
    8. 特定製品でのみ有効なライセンスの禁止
    9. 他のソフトウェアを制限するライセンスの禁止
    10. ライセンスは技術中立的でなければならない

    引用元 : https://opensource.jp/osd/osd19plain/

（参考）一般的なOSSライセンスの種類と特徴

類型	特徴	ライセンス例	OSS例
コピーレフト型	• 改変部分のソースコードの開示が必須 • 他と組み合わせた場合、ソースコード全体の開示の義務あり	GPL	MySQL、Linux、等
		AGPL	eyeOS、Launchpad、等
準コピーレフト型	• 改変部分のソースコードの開示が必須 • 他と組み合わせた場合、他のソースコードの開示は不要	MPL	Mozilla Firefox、等
		LGPL	Cygwin、等
		EPL	Eclipse、等
非コピーレフト型	• 改変部分のソースコードの開示は不要 • 他と組み合わせた場合を含め、ソースコードの開示は不要	Python License	Python、等
		MIT License	Chainer、JQuery、等
		Apache License	Spark、Kafka、等

コピーレフト： コピーライトに対する造語。著作物の権利に関する考え方の一つで、著作物の複製・改変・再配布を認め、また、そこから派生した著作物についてこれらの行為を制限してはならないとするもの。

©Data Society Alliance 2023

5. OSSの位置づけ
5.2. 推奨モジュールのOSSライセンスの種類

- OSSには様々なライセンス形態があります。デジタル庁の推奨モジュール（Kong Gateway、FIWARE Orion）のライセンスは次のようになっています。

■Kong Gateway
（APIゲートウェイの推奨モジュール）

ライセンス名	Apache License 2.0
概要	Apache ライセンスでは公開されたプログラムを改変した場合や、自らのプログラムに組み込んだ派生的（二次的）な著作物を制作した場合でも、ソースコードを公開せずに販売・配布することが可能であり、さらに Apache ライセンスとは異なるライセンスで提供することもできます。

■FIWARE Orion
（ブローカー(非パーソナル)の推奨モジュール）

ライセンス名	AGPL v3.0
概要	AGPL ライセンスの下では、独自アプリケーションのソースコード一式を公開せずにネットワーク上で展開することはできません。独自の製品やWebベースのアプリケーションを含め、すべてのソースコードを配布する必要があります。

©Data Society Alliance 2023