FUJITSU
Hybrid IT Service
Digital Application Platform
「API Management Service」
ご紹介資料

富士通株式会社

2024年10月

Version 1.2

Agenda(1/2)

- Web APIの活用動向
  - はじめに　～WebAPIとは～
  - 利用シーン
  - 世の中のWebAPI活用イメージ
  - 動向　コンシューマビジネスでの利用活発化
  - デジタル・エコシステム（APIエコノミー）
  - エンタープライズ領域の動向
- API Management Serviceご紹介
  - API Management Serviceとは
  - 機能概要
  - API公開のための機能
  - プロコトル／データ形式変換機能とは
  - 認証機能とは（例：OAuth 2.0）
  - サーバーレスAPI, APIマッシュアップ機能とは
  - API開発の流れ
- API Management Serviceご紹介（続き）
  - API Proxy機能
  - API Proxy機能 - Policy
  - API Proxy機能 - Flow
  - 開発機能 - デプロイ機能
  - 開発機能 - トレース機能
  - Publish機能
  - 解析＆モニタリング機能 - 解析
  - 解析＆モニタリング機能 - Custom Report
  - 解析＆モニタリング機能 - ダッシュボード
  - ゲートウェイ拡張機能（独自ドメインでのAPI公開）
  - ゲートウェイ拡張機能 (公開APIの接続制限)
  - ゲートウェイ拡張機能（Java機能）
  - バックエンドセキュア接続機能（Digital enhanced EXchange）
  - バックエンドセキュア接続機能（IPsec VPN接続）
  - バックエンドセキュア接続機能（ネットワークRBAC接続）
  - DNS機能

Agenda(2/2)

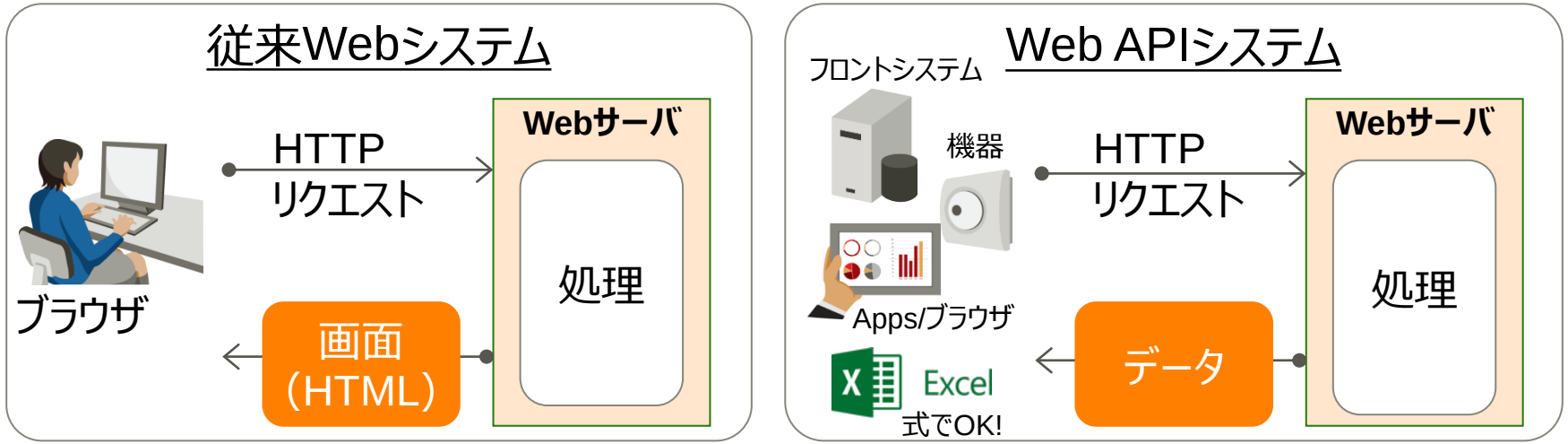
- API Management Serviceご紹介（続き）
  - フルアナリティクス機能
  - WebAPI
  - マルチリージョン
  - サービスアカウントと環境
  - API Management Serviceサービスメニュー
  - 課金の考え方について
  - プラン変更の可否
  - プラン変更方法
  - プラン変更時の注意事項
  - バックエンドセキュア接続の利用について
  - 制限事項・注意事項
- 要素技術
  - 要素技術：従来のWebシステムとの違い
  - 要素技術：リクエスト・レスポンス形式
  - 要素技術：認証
  - 要素技術：セション管理
  - 要素技術：REST関連
- 参考情報
  - 【参考】Policy - トラフィック管理
  - 【参考】Policy - データ加工
  - 【参考】Policy - セキュリティ
  - 【参考】Policy - 拡張機能
  - 【参考】解析一覧

Web APIの活用動向

はじめに ～Web APIとは～

- Web APIとは、組織が持つデータや機能をAPI形式で提供したもの
  - API利用者が独自に様々なAPIを組み合わせて利用することが可能です。
    利用者起点での付加価値創造、新たなサービス創出に繋がる例が出始めています。

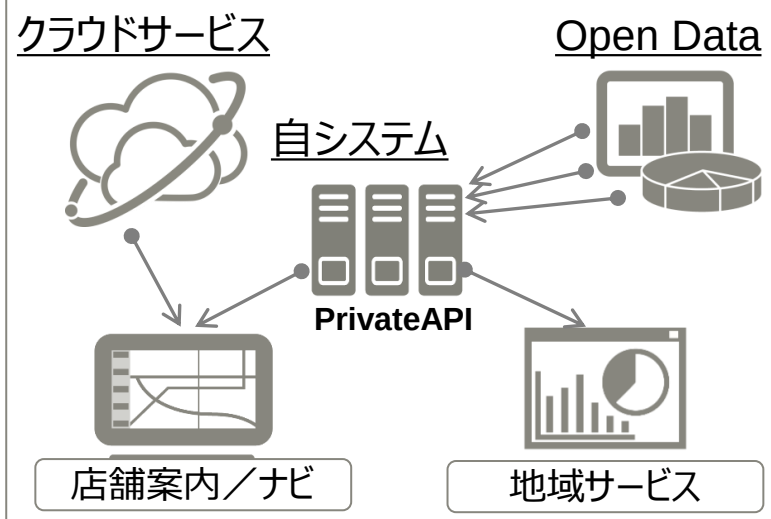
- 従来のWebシステムとの違い
  - 従来のWebシステムは、データや機能を画面（HTML）で提供。
  - Web APIでは、データのみやりとりされます。様々なクライアントから利用されます。



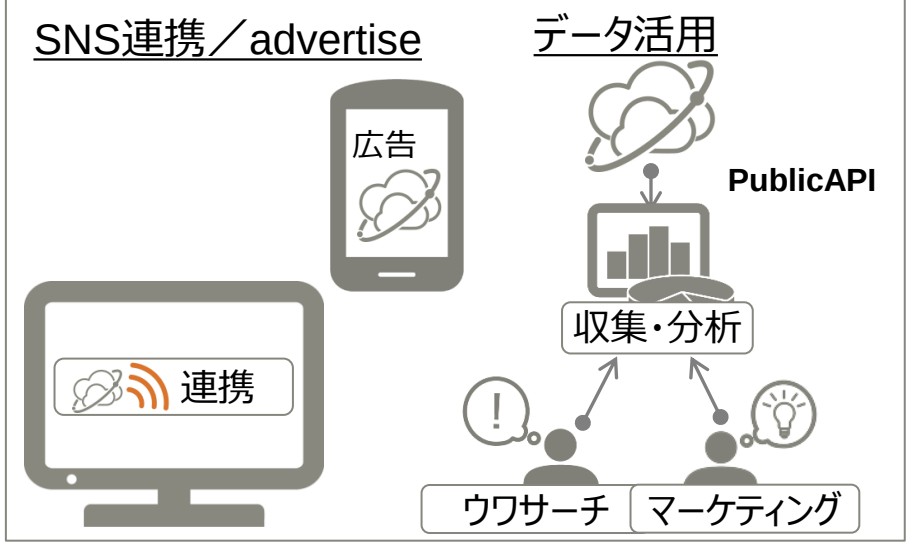
従来の複雑なプロトコルとは異なり、HTTPとテキストのみのシンプルさ・利用しやすさが特徴

（参考）世の中のWeb API活用イメージ

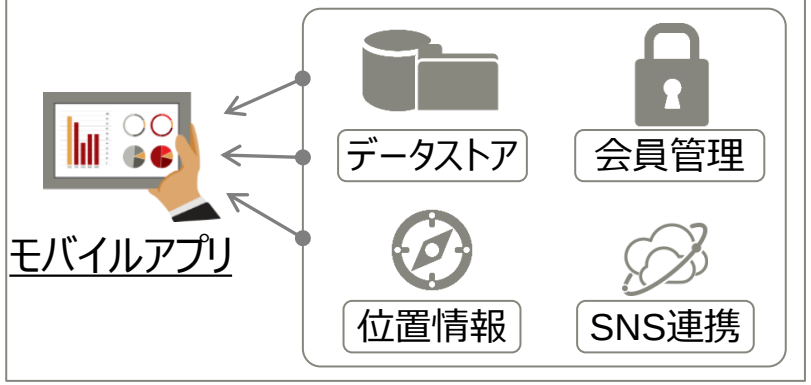
サービスマッシュアップ



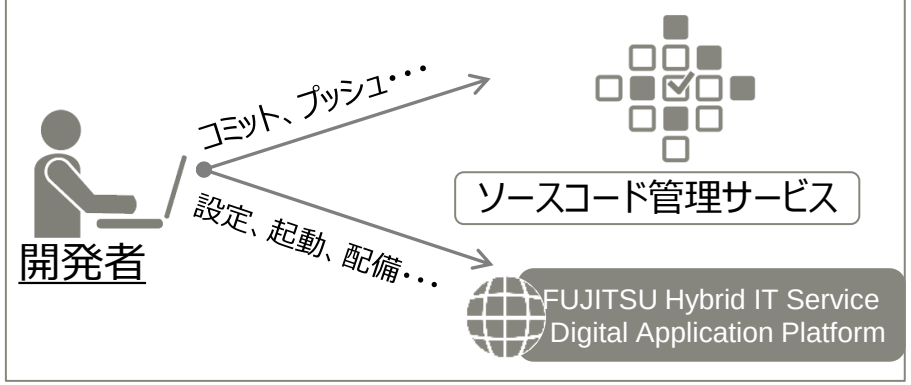
ソーシャル活用



モバイルバックエンド（MBaaS）



クラウド基盤／開発環境



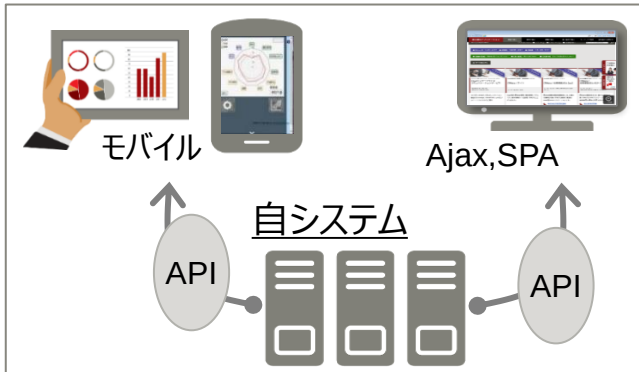
動向　コンシューマビジネスでの利用活発化

○ ネット上での活用を経て、新規ビジネス創出のコアテクノロジへ

ネット／ソーシャル活用

Web API提供が既に当たり前

Webフロント／モバイルアプリ



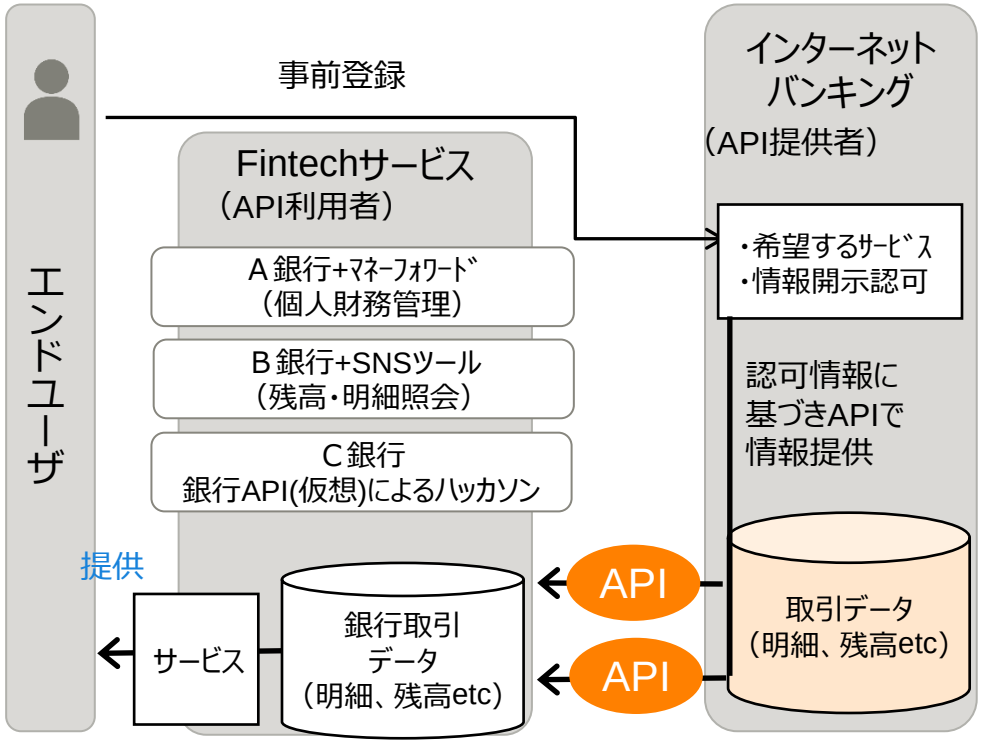
技術的な面での活用容易性から、
デファクト技術へ

新たなビジネス価値創造（Fintech例）

API公開→第三者サービス提供の容易化

優良第三者サービスによる利用者増

APIエコノミー

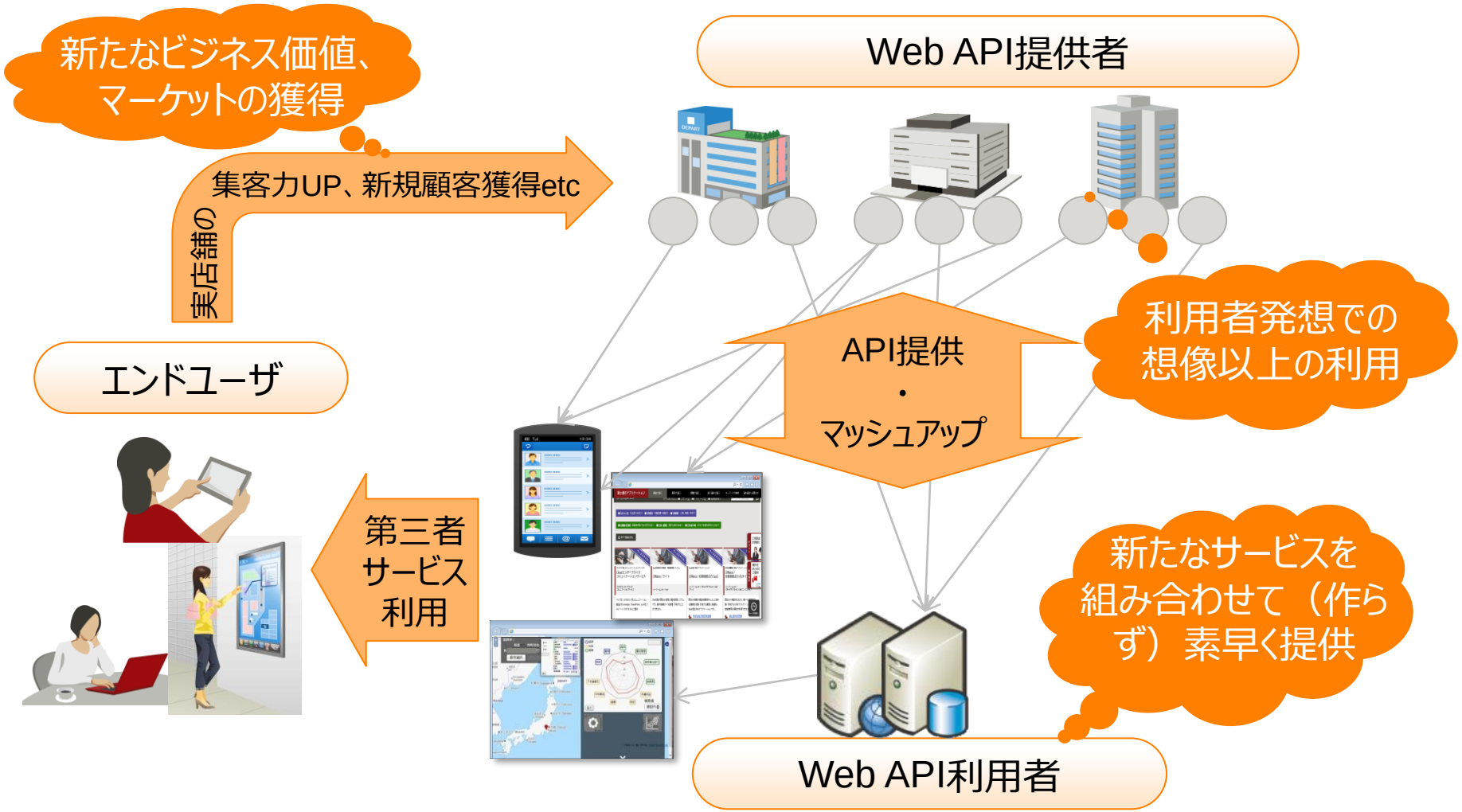


まずはAPI公開　⇒　利用者視点での新たな価値

デジタル・エコシステム（APIエコノミー）

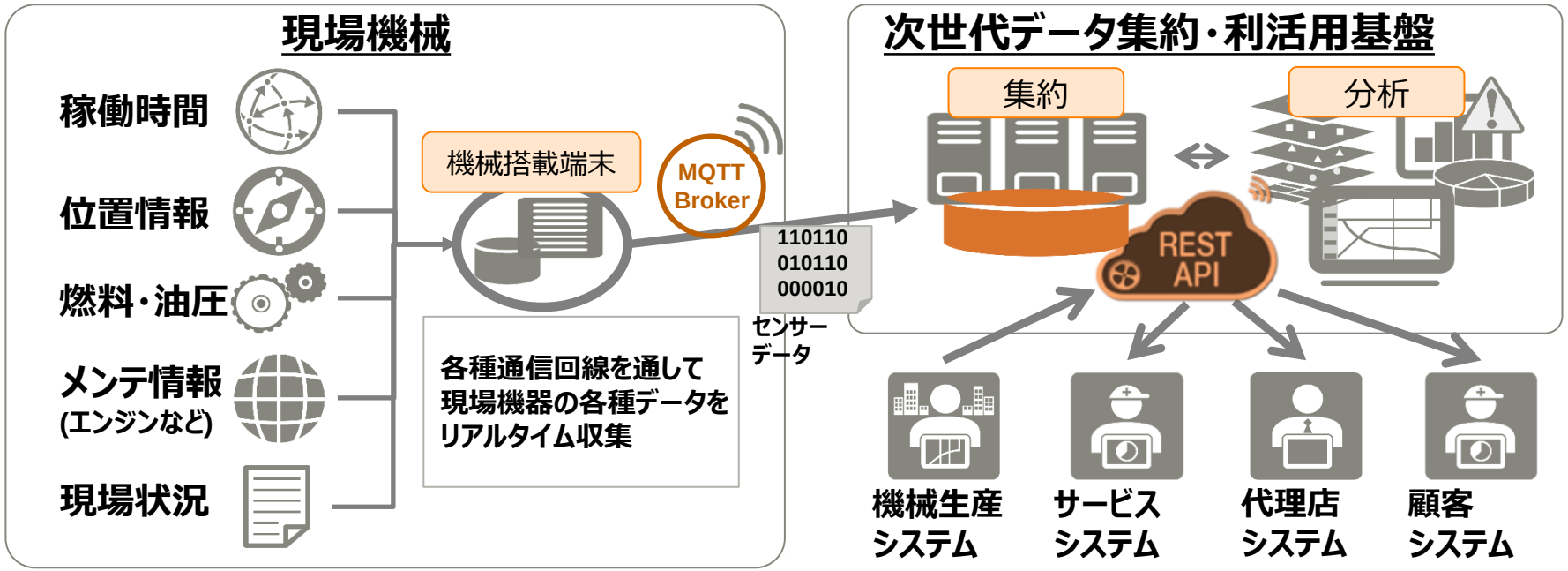
FUJITSU

○ Web APIを活用したサービス提供を通して、新たなビジネス価値やマーケット創出に繋がる例が出始めている。



エンタープライズ領域の動向

- コンシューマ領域の成功例に対する期待感から、活用例が増加
  - データ集約を行い、**利活用I/FとしてWebAPIを活用**、フロント業務システムへ解放
  - 社内／社外（代理店、業界各社 etc）でのビジネススピード向上を狙う
- 弊社SI案件での一例（機械製造販売業）
  - 現行はWeb画面による情報公開。代理店・サービス業務側主体の素早い新サービス提供のために、Web APIによるデータ収集・利活用基盤を構築する。



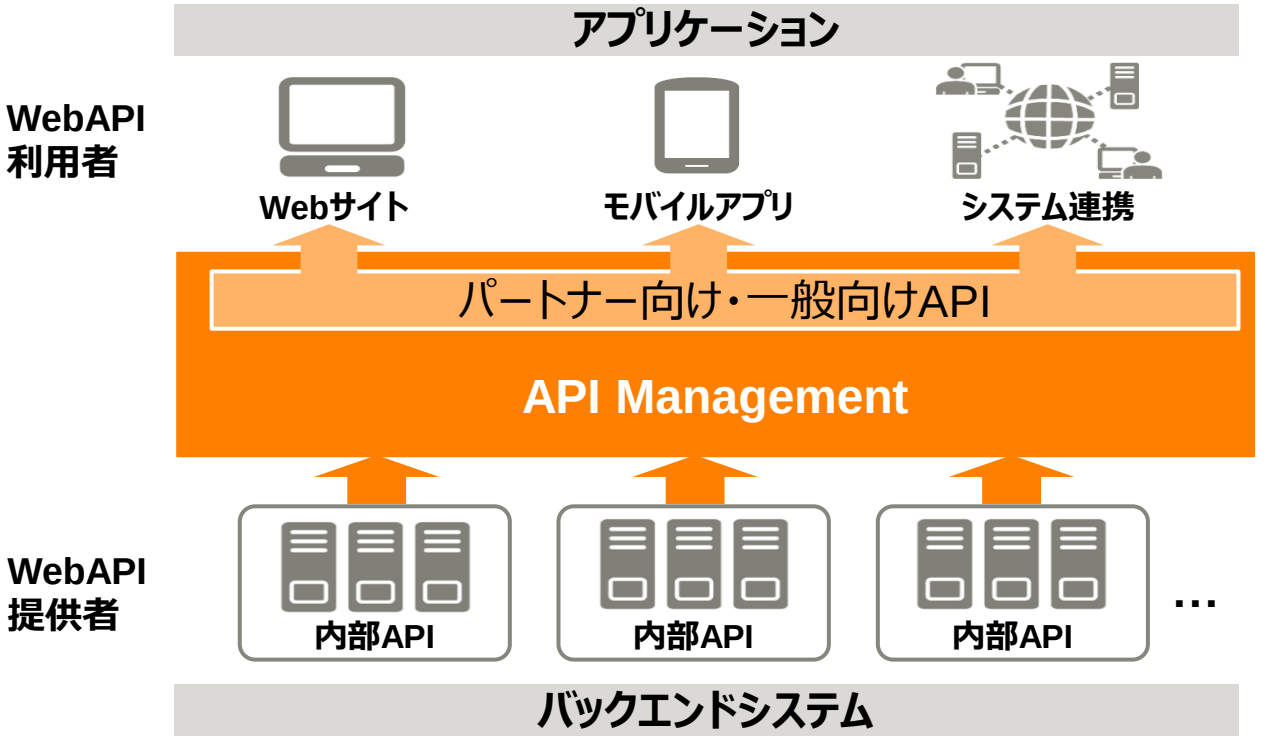
API Management Service ご紹介

- API Management Service
- APIの開発・公開・運用を支援する機能の提供

API Management Serviceとは（1/2）

APIプログラムの作成、拡張、保守に役立つ機能を提供し、ビジネスの継続的な成長に寄与するサービス

①アクセス制御機能・データの形式変換機能により、APIの開発期間を短縮
②認証、トラフィック制御により、安全にAPIを公開
③解析・モニタリング機能により、拡張や保守情報を提供



提供機能

①安全なアクセス
- 認証・認可
- セキュリティチェック
- トラフィック制御

②利便性の向上
- 呼出方式の統一・変換
- サービスのマッシュアップ
- APIバージョン管理
- キャッシュによる性能向上
- プログラマブル

③利用状況の把握
- ダッシュボードによる監視
- グラフによる視覚化
- カスタムレポート

API Management Serviceとは（2/2）

FUJITSU

- 安全なアクセス
  - 認証・認可
    - OAuth, APIキー, SAMLなどAPIの認証・認可を行うための機能を提供します。
  - トラフィック制御
    - 流量制限などバックエンドのリソースを保護するための機能を提供します。
- 利便性の向上
  - 外部仕様の統一
    - APIの外部仕様を統一するリクエスト／レスポンス変換機能を提供します。統一されたIFは利用者拡大の必須要件となります。
  - API開発支援機能の提供
    - マッシュアップ、アドオンプログラムなどAPI開発を支援する機能を提供します。
- 利用状況の把握
  - 利用されているAPIの把握
    - APIの本数が増えてきた場合、どのようなAPIが存在し、誰が利用しているか、など把握が難しくなってきます。API Management ServiceはAPIの利用把握を支援するユーザーインターフェースを提供します。
  - APIのコール数の把握
    - API毎に時系列でコール数の確認ができ、APLサーバーのリソース管理など運用面に加え、売れるAPIの発掘などビジネス面でも重要な情報の見える化を実現します。

機能概要

FUJITSU

○API Management Serviceが提供する機能

- ○ 共通機能　Private API向け機能
- ○ Public API向け機能

共通機能 PrivateAPI向け機能

互換・接続	最適化	セキュリティ	API開発
• メッセージからデータの抽出 • XSL変換 • SOAP→REST変換 • リクエスト編集 • レスポンス編集	• レスポンスキャッシュ • Key Value Store • 同時接続数の制限 • トラフィックスパイクの抑止 • トラフィック制限	• OAuth 2.0 • Basic認証 • SAML対応 • LDAP連携	• アドオンプログラム • 開発/本番環境 • 無停止デプロイ • マルチバージョン管理 • Policy/Flowエディタ • 監視(API性能、エラー)

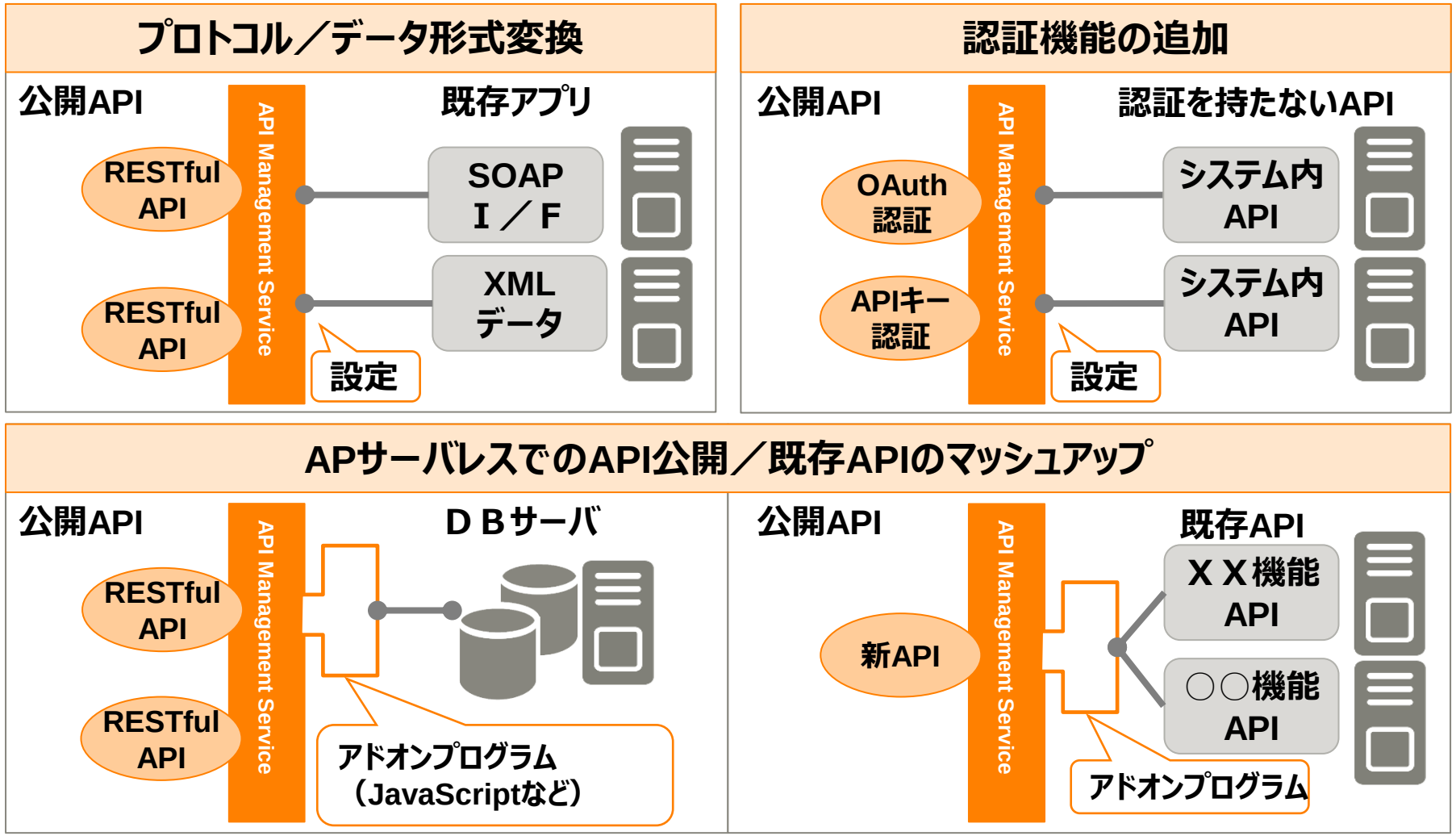
PublicAPI向け機能

公開	解析
• APIのパッケージング • ACL設定(更新/参照) • トラフィック制限 • 利用キー(APIキー)払出	• 運用管理者用統計 • API開発者の利用統計 • アプリ統計 • ビジネス統計機能 • レポートのカスタマイズ

API公開のための機能

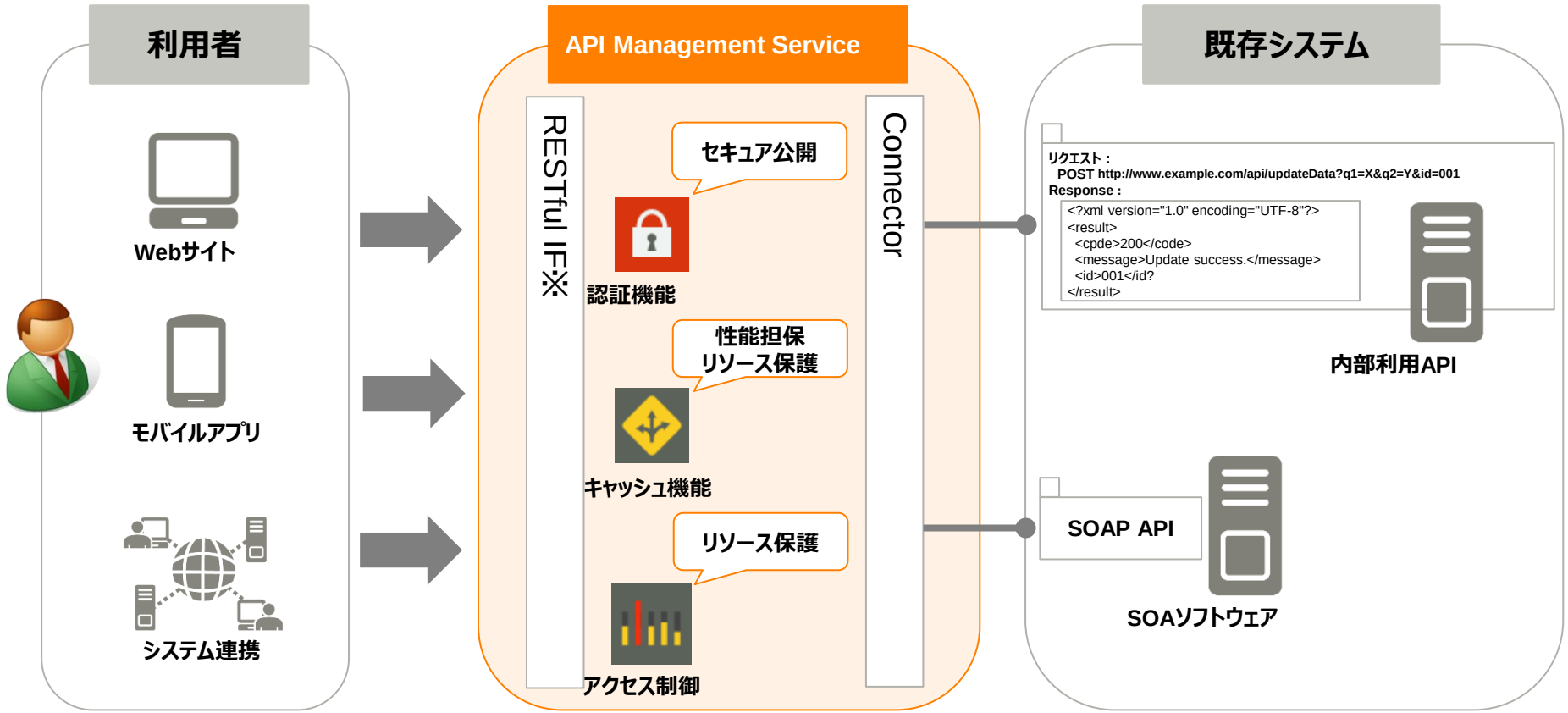
FUJITSU

○ API公開を簡単にするための機能を提供します（以下、機能の一部）



プロトコル／データ形式変換機能とは

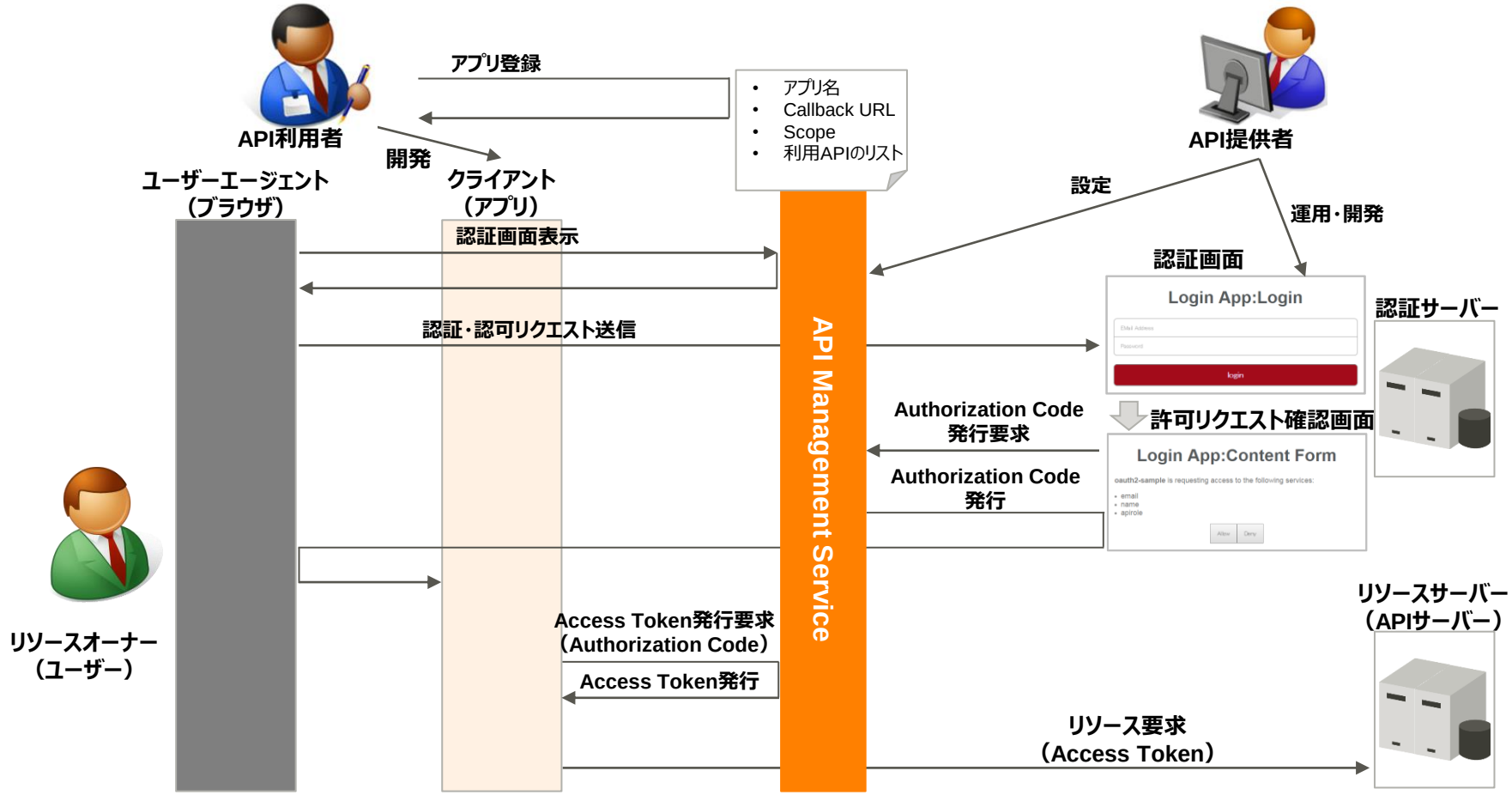
レガシーなシステムを性能を担保し、バックエンドのリソースを保護したうえでセキュアに公開できます。



※ 要素技術：リクエスト・レスポンス形式を参照のこと

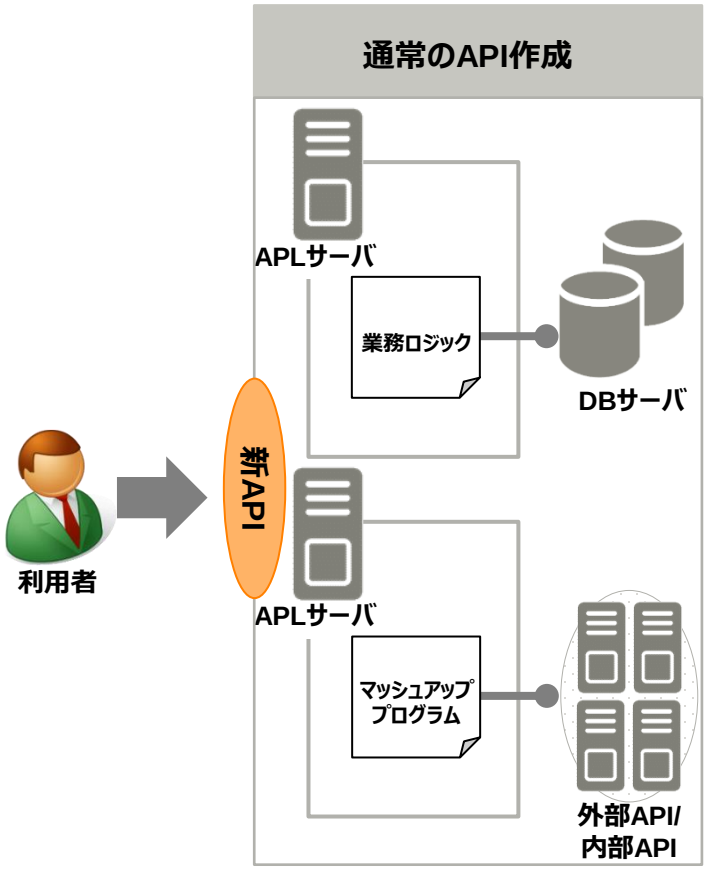
認証機能とは（例：OAuth 2.0）

インフラなど環境を含めた認証機能がAPI Management Serviceから提供され、APIに対する認証の組み込みを容易に実施できます。

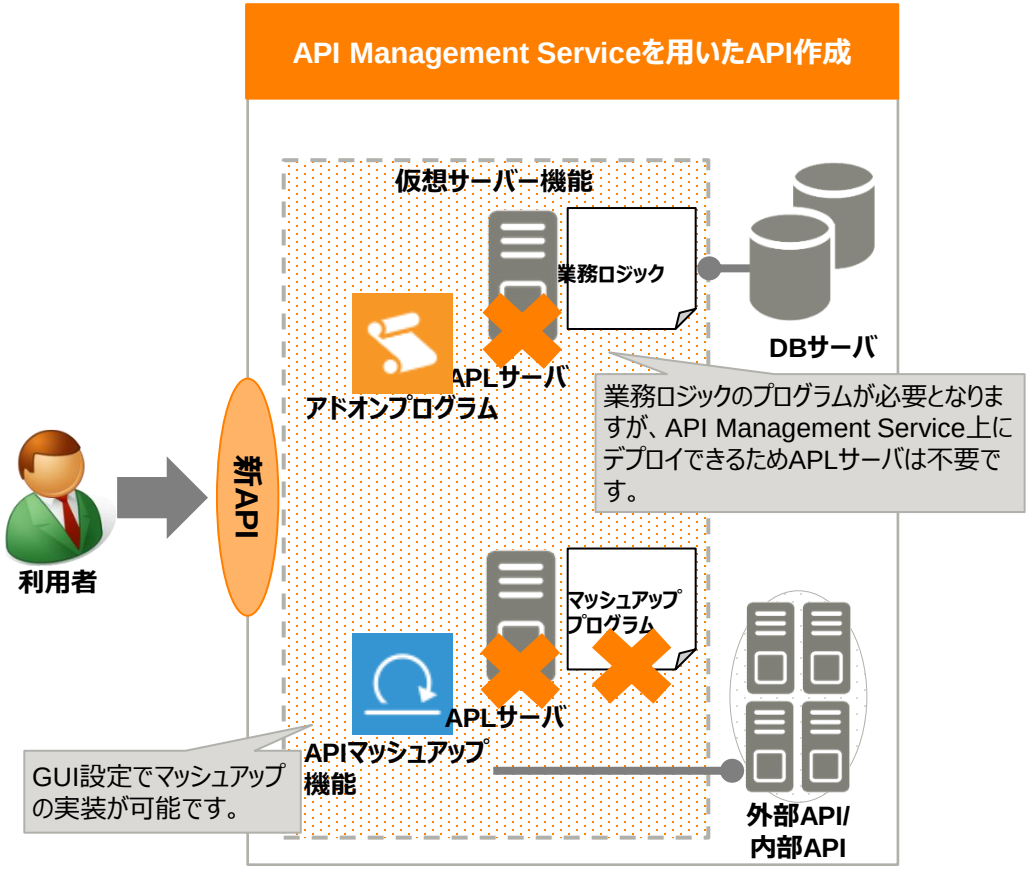


サーバーレスAPI, APIマッシュアップ機能とは

API Management Serviceを利用することでAPLサーバを構築せず、業務ロジックの実装のみでAPIを公開することができます。
（サーバレスAPI公開）
短期間での開発や改修が多いAPIを作成するのに適した機能です。
また、プログラムを書くことなく、外部API/内部APIをマッシュアップして新規APIを公開できます。



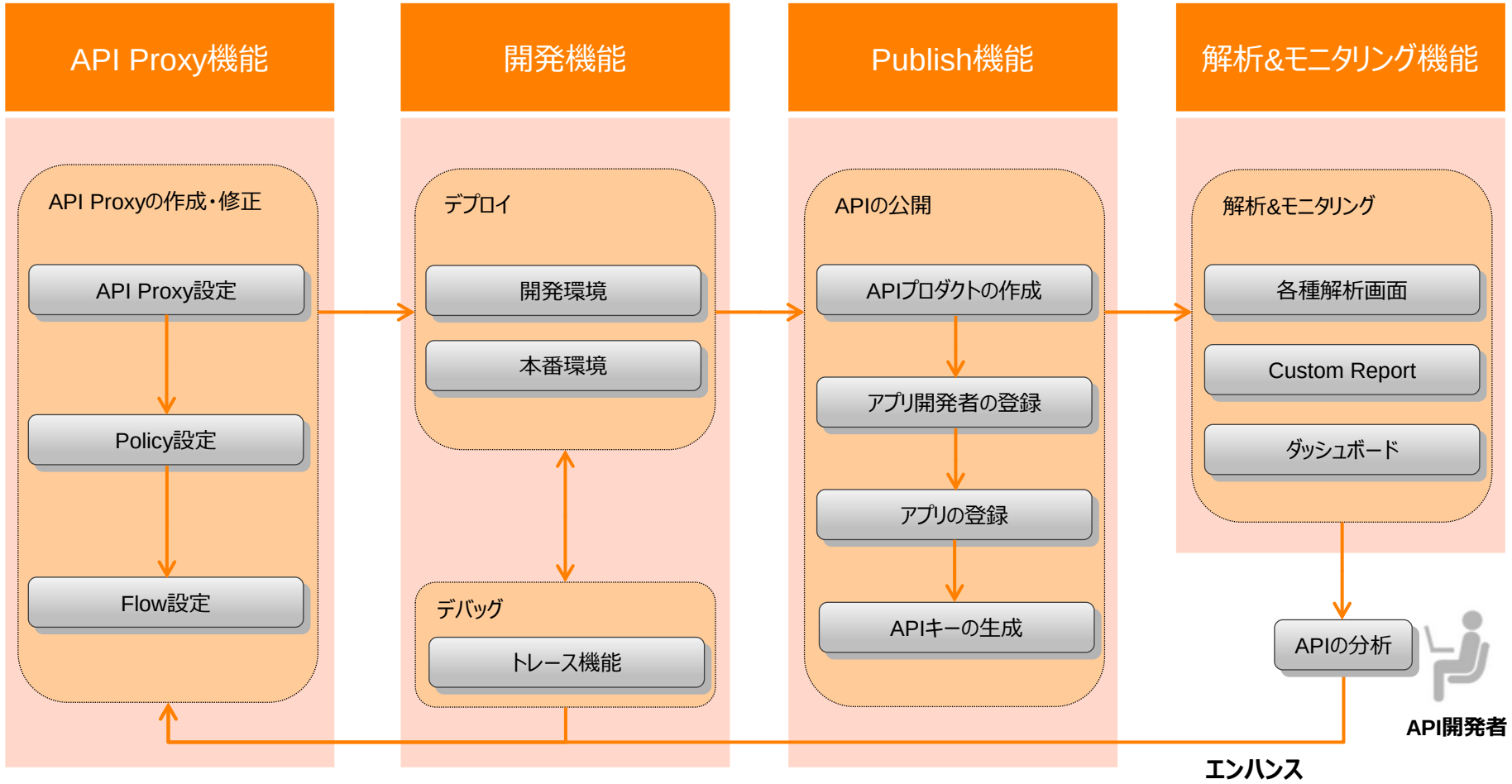
APLサーバを構築し、プログラムをデプロイする必要があります。



API Management Serviceが仮想サーバとして機能するためAPLサーバは不要です

API開発の流れ

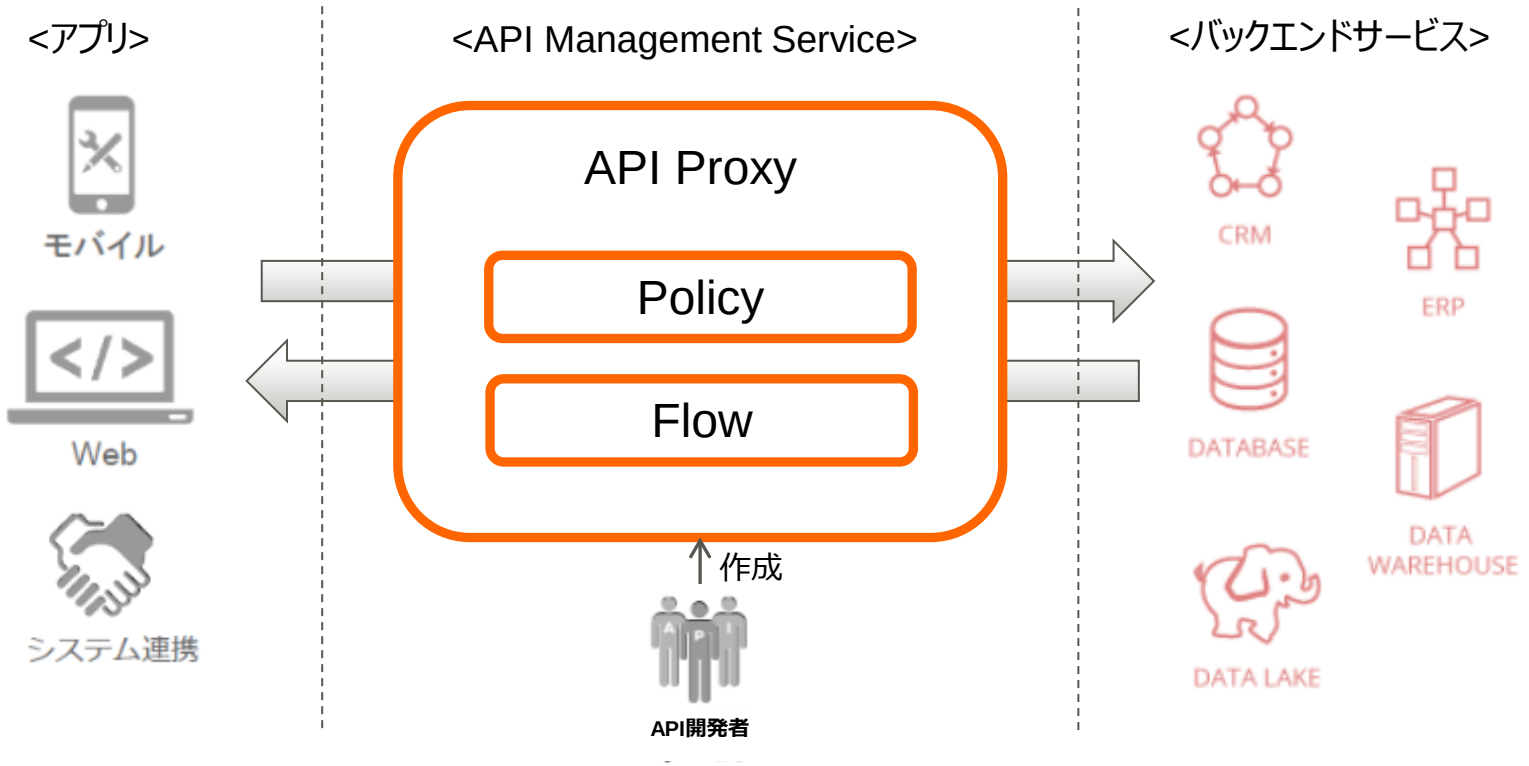
API Management ServiceでAPIを開発する際の流れを示します。



API Proxy 機能

API ProxyはAPI Management Serviceのコアコンポーネントであり
ゲートウェイとして働きます。API Proxyに下記を設定することで、APIの振る舞いをコーディングなしで
プログラムできます。

- Policy（バックエンドサービスへの付加機能）
- Flow（追加した付加機能の処理シーケンスの制御）



API Proxy 機能 - Policy

コーディングなしでAPIに機能（Policy）を追加できます。 開発工数を大幅削減

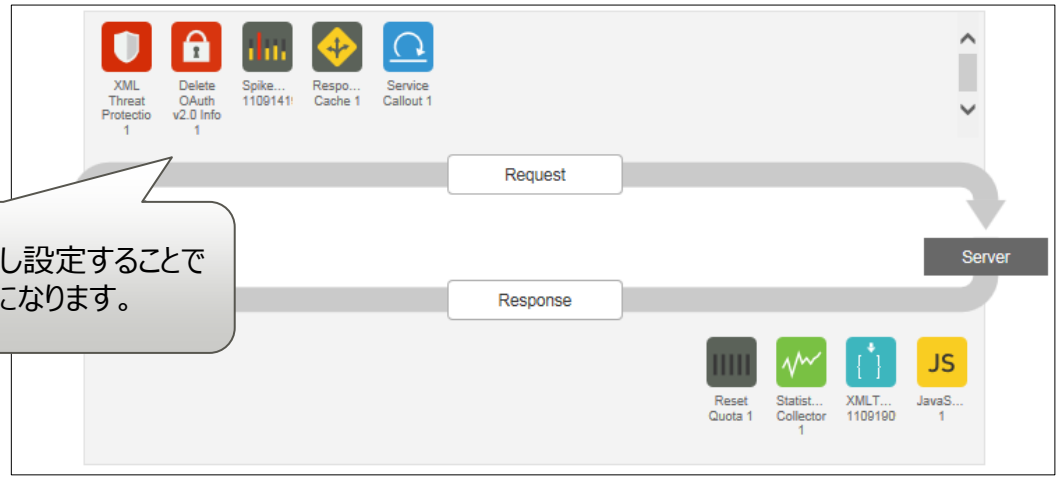
30を超える機能を設定のみ（コーディングなし）で追加可能

- 認証／セキュリティ
- リクエスト・レスポンス情報の加工
- キャッシュ
- トラフィック制限
- データ形式変換
- ロギング

スクリプトで独自機能を追加可能

- JavaScript
- Java
- Python

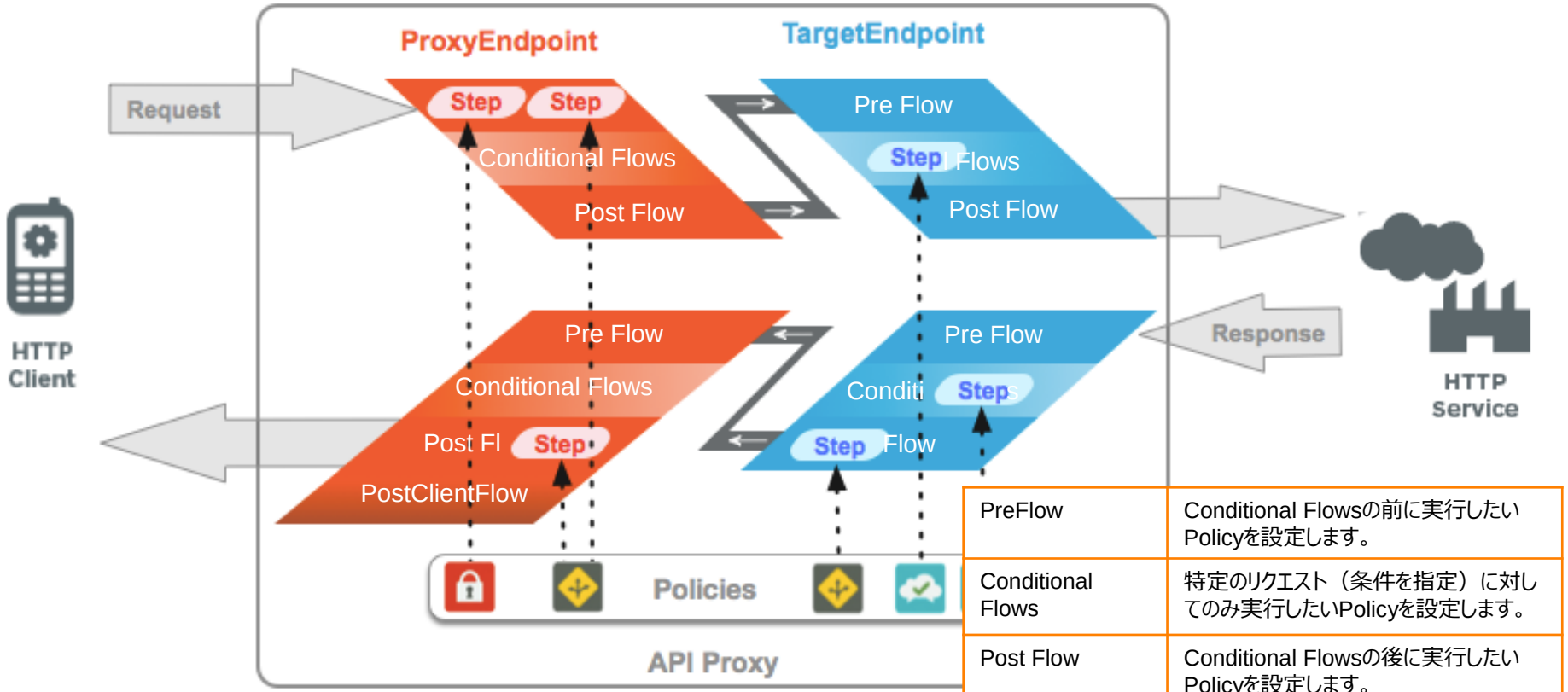
※全機能については【参考資料】Policyをご参照ください



API Proxy 機能 - Flow

Policyの実行タイミングや実行条件を設定することによりAPIの振る舞いを計画できます。

GUIベースでフローにPolicyのアイコンを配置するだけでAPIの振る舞いをプログラム可能



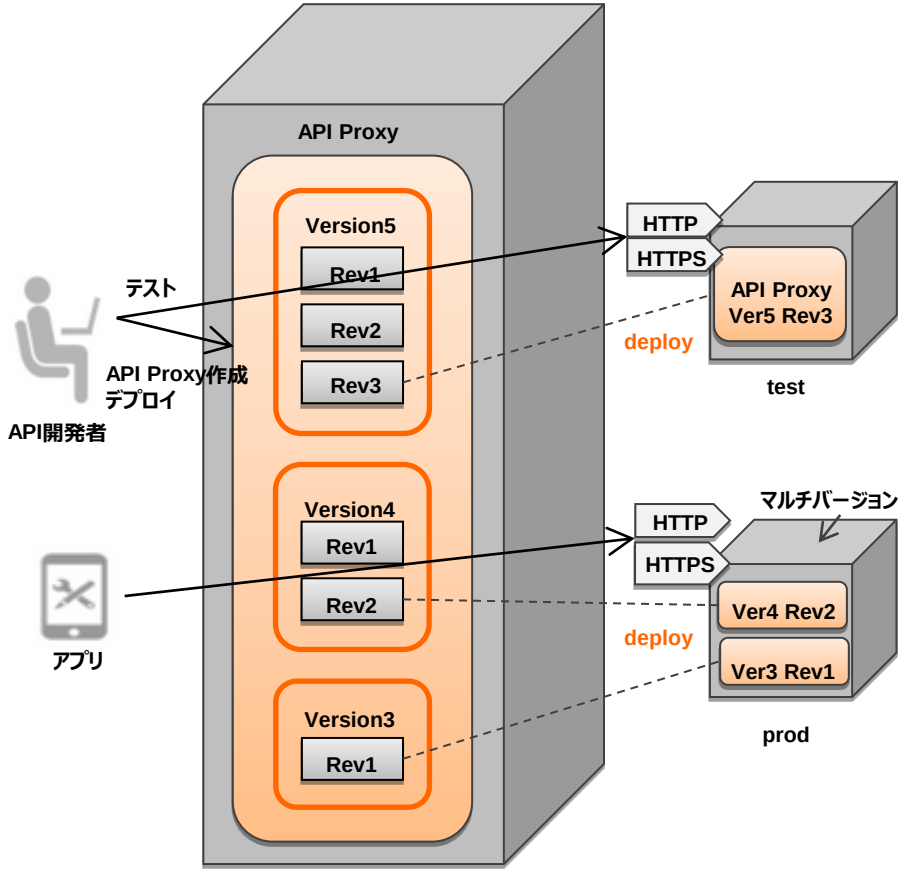
PreFlow	Conditional Flowsの前に実行したいPolicyを設定します。
Conditional Flows	特定のリクエスト（条件を指定）に対してのみ実行したいPolicyを設定します。
Post Flow	Conditional Flowsの後に実行したいPolicyを設定します。
PostClientFlow	アプリにレスポンスを送信した後に実行したいPolicyを設定します。

開発機能 - デプロイ機能

デプロイ、バージョン管理、環境機能により効率的なAPI Proxy開発を実現できます。

アジャイル開発を支援

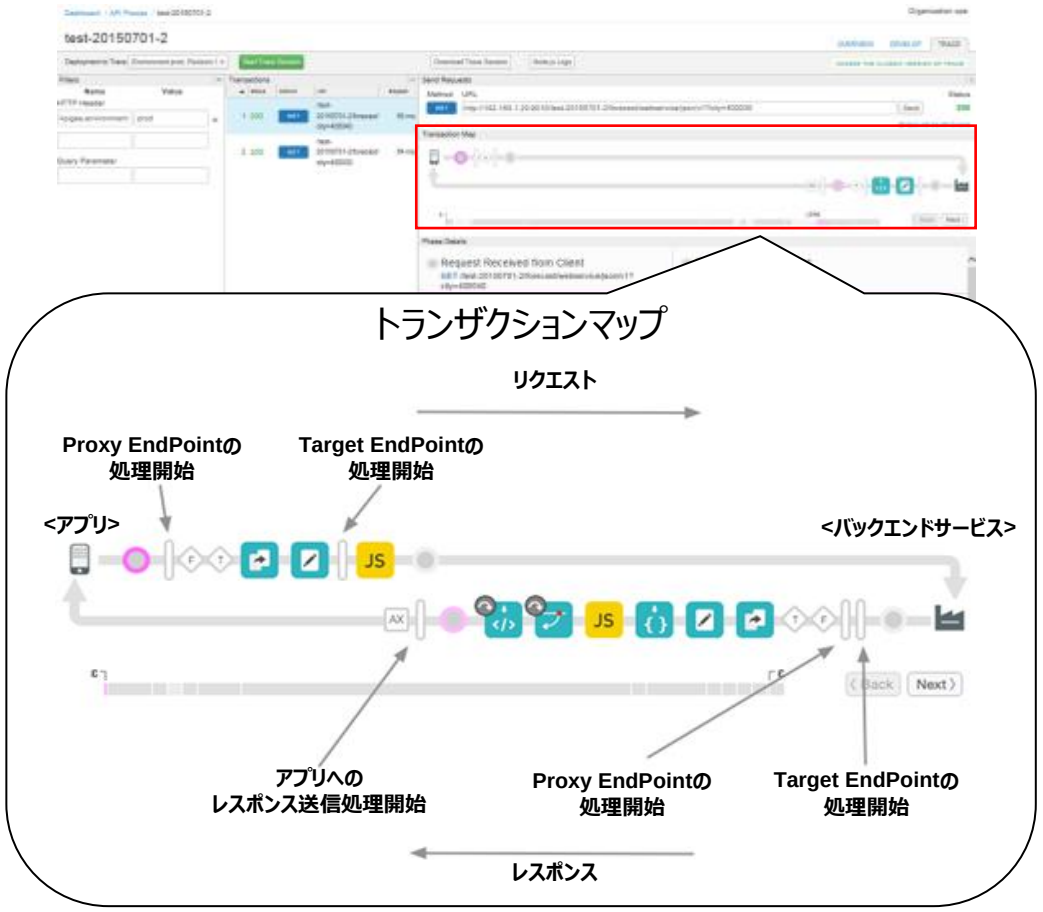
機能	機能項目	説明
デプロイ	シームレスなデプロイ	アプリへの影響を最小限に抑えながらデプロイ可能です。
	マルチバージョンデプロイ	バージョンの異なるAPI Proxyを同一環境に複数デプロイ可能なため、マルチバージョン環境を実現できます。
バージョン管理	バージョン	API Proxyをバージョン管理できます。
	リビジョン	バージョンより細かい改訂単位であるリビジョンでの管理が可能です。
環境	フェーズ毎の環境	開発環境と本番環境の2環境が利用できます。
	HTTP／HTTPS	HTTPとHTTPSの２つのエンドポイントが利用できます。



開発機能 - トレース機能

API Proxyのトランザクションを視覚化し、各処理ステップの詳細表示を利用することで、
効率良くAPI Proxyをデバッグできます。

効率的なトラブルシュート



トランザクションマップ

- トランザクションの各ステップをアイコンで表示します。
- アイコンをクリックすると詳細情報を表示します。
- 詳細情報に表示される機密情報はマスキングできます。
- トランザクションのトレースは、ブラウザ、curlなど
  任意のツールを利用することができます。

フィルター

- トランザクションは、トレースする際、下記条件で
  フィルタリングすることができます。
  - HTTPヘッダー
  - クエリパラメーター

オフライントレース

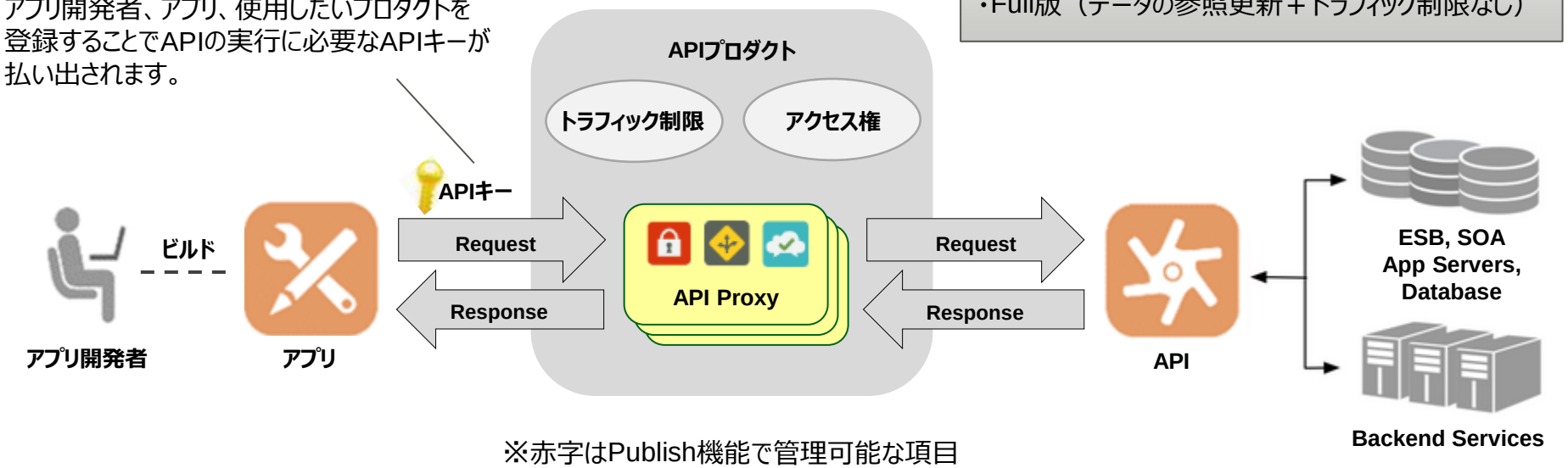
- トレース結果はエクスポートすることが可能で、
  オフライントレース画面で読み込むことができます。

Publish機能

作成したAPI（API Proxy）をアプリ開発者に公開する機能です。
API Proxyをプロダクトとしてパッケージ化し、アクセス権やトラフィック制限を設定することで、用途に応じてAPIを公開できます。

ビジネス要求に応じた
柔軟な製品提供を支援

プロダクト例
・Free版（データの参照＋トラフィック制限あり）
・Lite版（データの参照更新＋トラフィック制限あり）
・Full版（データの参照更新＋トラフィック制限なし）



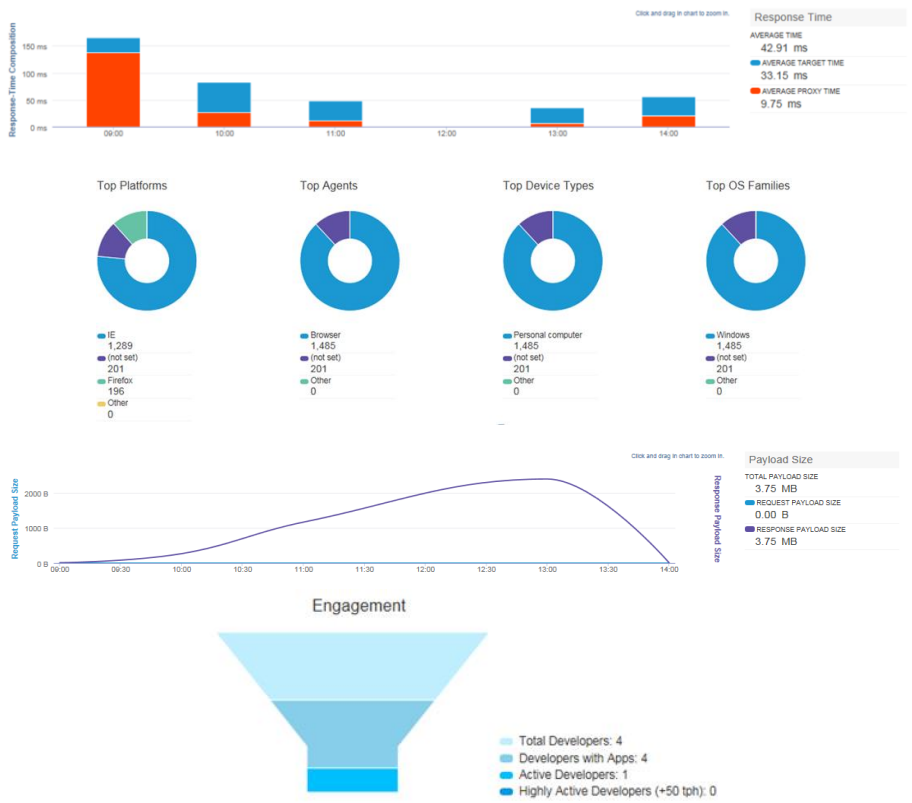
※赤字はPublish機能で管理可能な項目

解析＆モニタリング機能 - 解析

APIトラフィックの情報を集計・可視化することで、APIや開発者の利用状況やパフォーマンスなどをリアルタイムに解析できます。

・利用状況の把握
・問題の早期発見
・パフォーマンス監視

APIトラフィックの集計例



解析画面

以下の8つの画面で集計した情報を、モニタリングできます。

- Proxy Performance
- Target Performance
- Cache Performance　(*)
- Latency Analysis
- Error Analysis
- Developer Engagement　(*)
- Traffic Composition
- Devices

* Proまたは後述のフルアナリティクスプランのみ利用可能

※東日本リージョン1でサービスをご利用の場合の例です。
各リージョンごとの仕様はサービス仕様書にてご確認ください。

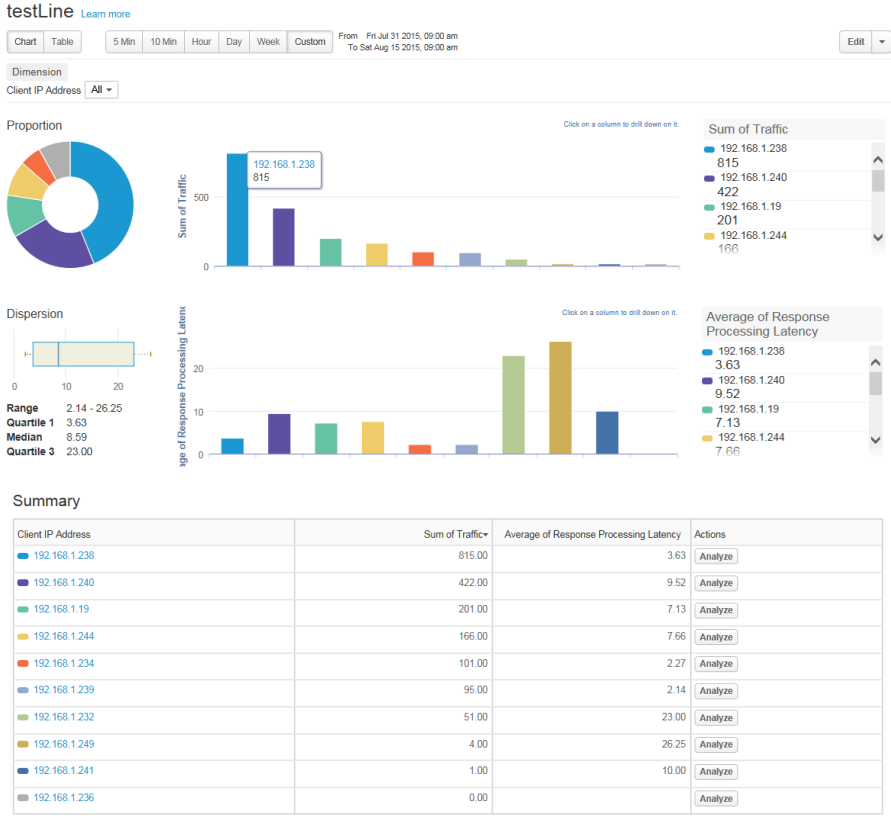
※各画面の説明につきましては、【参考資料】解析一覧をご参照ください。

解析＆モニタリング機能 - Custom Report

Custom Reportでは、横軸（Dimensions)と縦軸（Metrics）に表示する項目を選択して、自由にグラフを作成することができます。

独自レポートの作成

Custom Reportの作成例



Dimensions

・クライアントのIPアドレスやOSの種別など、トラフィックに含まれる様々な情報を指定できます。

・複数選択することで、集計結果を絞り込んでいくドリルダウン解析ができます。

ドリルダウン例

OS＋IPアドレス ・・・ Windows利用者をIPアドレス別に分析したい場合など

Metrics

・リクエスト数やエラー数、応答時間などAPIの利用状況に関する情報を指定できます。

・選択した数だけ、解析画面にグラフを表示します。

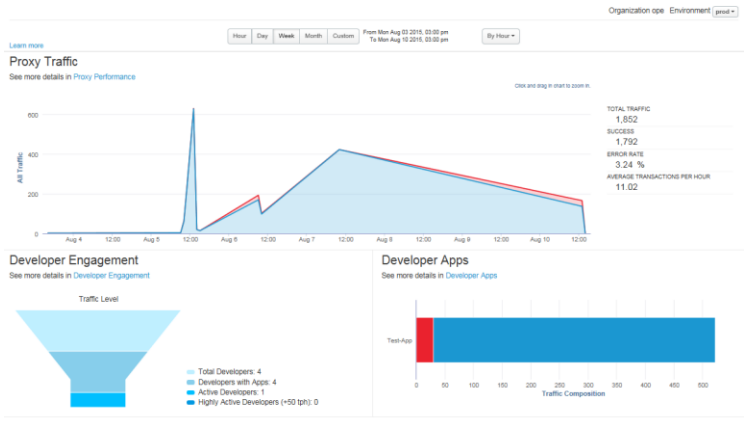
フィルター

・DimensionsやMetricsの値を選択して、集計結果をフィルタリングすることができます。

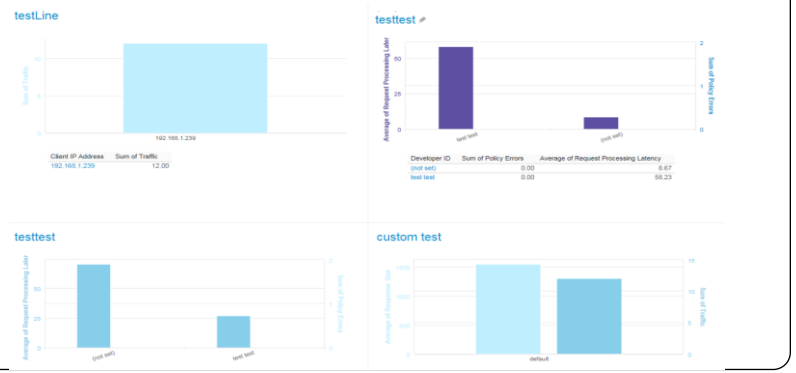
解析＆モニタリング機能 - ダッシュボード

APIの利用状況を、すばやく把握することができます。

ダッシュボード画面の表示例



Custom Reportのダッシュボード画面の表示例



画面説明

ダッシュボード機能は、大きくわけて左記の２画面が用意されています。

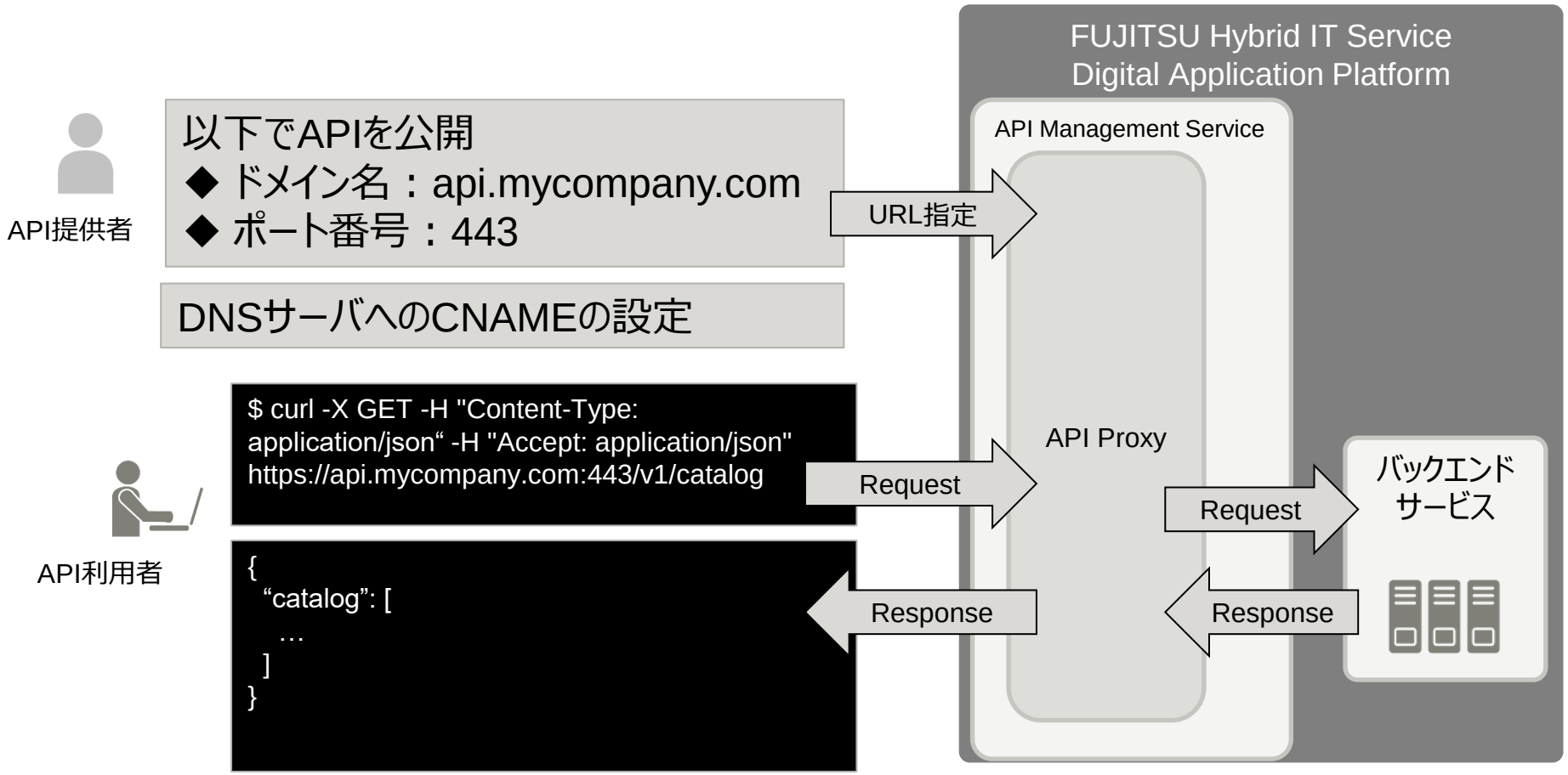
- ダッシュボード画面について
  API Proxy全体のトラフィック量、アプリ開発者の利用状況、アプリ毎のエラー割合を1画面で確認することができます。

- Custom Reportのダッシュボード画面について
  作成したCustom Reportを、最大４つまで選択して1画面に表示させることができます。

※グラフの詳細を確認したい場合は、グラフ名のリンクをワンクリックするだけで表示されます。

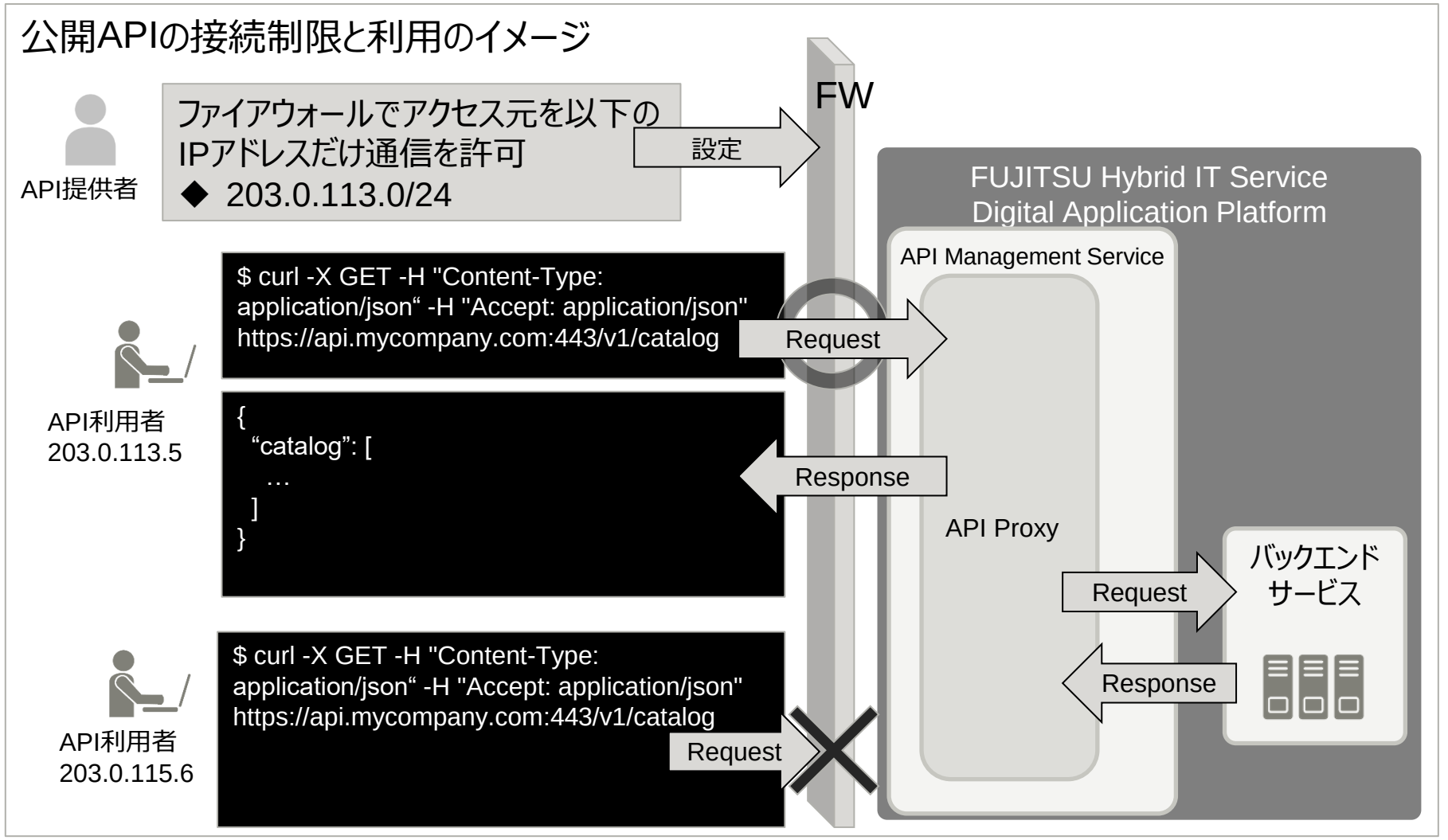
ゲートウェイ拡張機能（独自ドメインでのAPI公開）

当社から提供するドメインではなく、お客様独自のドメイン名を利用できます（URLを変更することなくAPIを利用できます）。
独自ドメインでAPIを公開できます（DNSサーバへのCNAMEの設定が必要です）。



ゲートウェイ拡張機能（公開APIの接続制限）

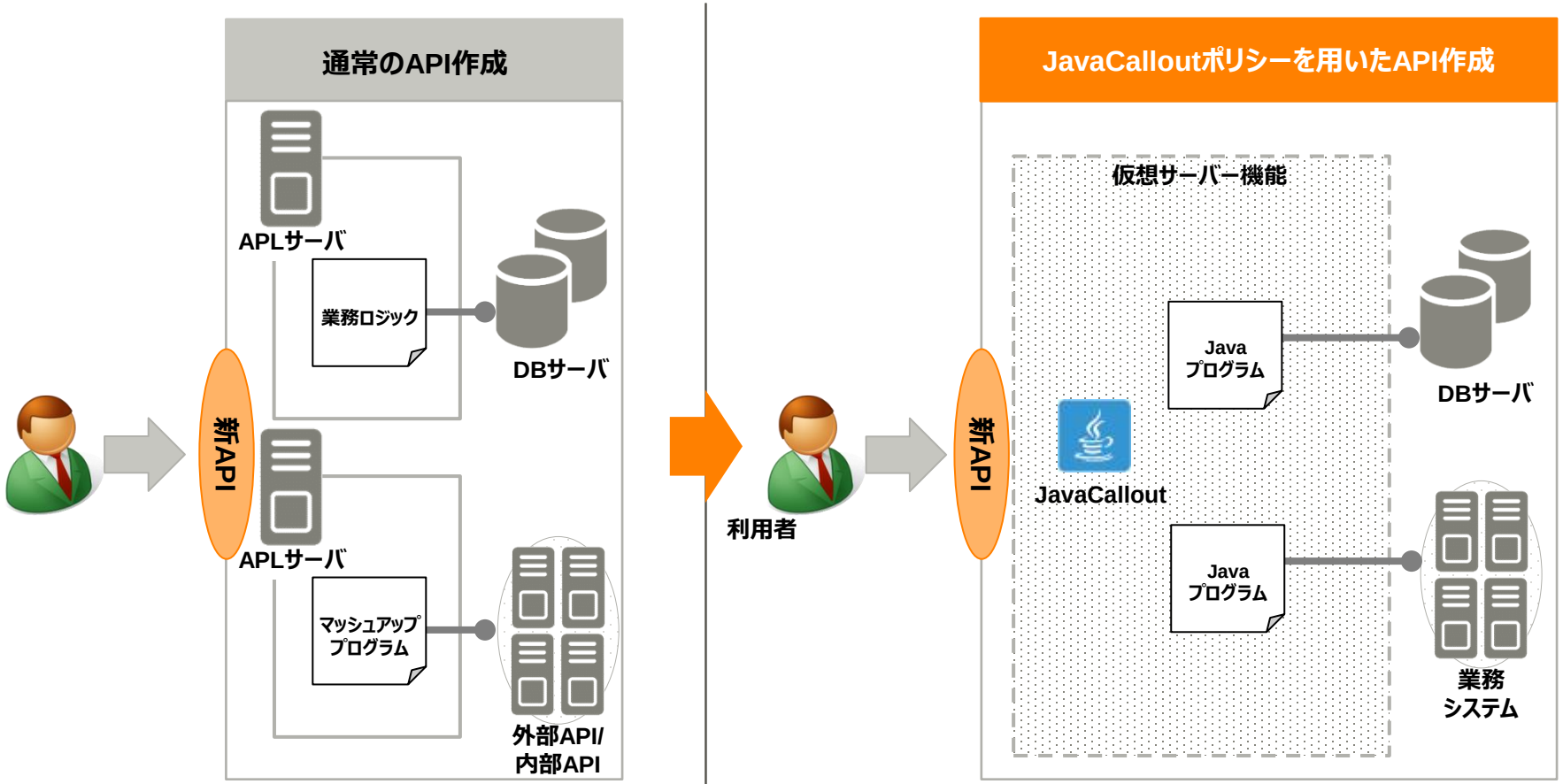
公開APIに対してアクセス元IPアドレスを制限することができます。



ゲートウェイ拡張機能（Java機能）

Javaプログラムにより、業務システムやDBサーバと連携することができ、
APIの機能を拡張することができます。

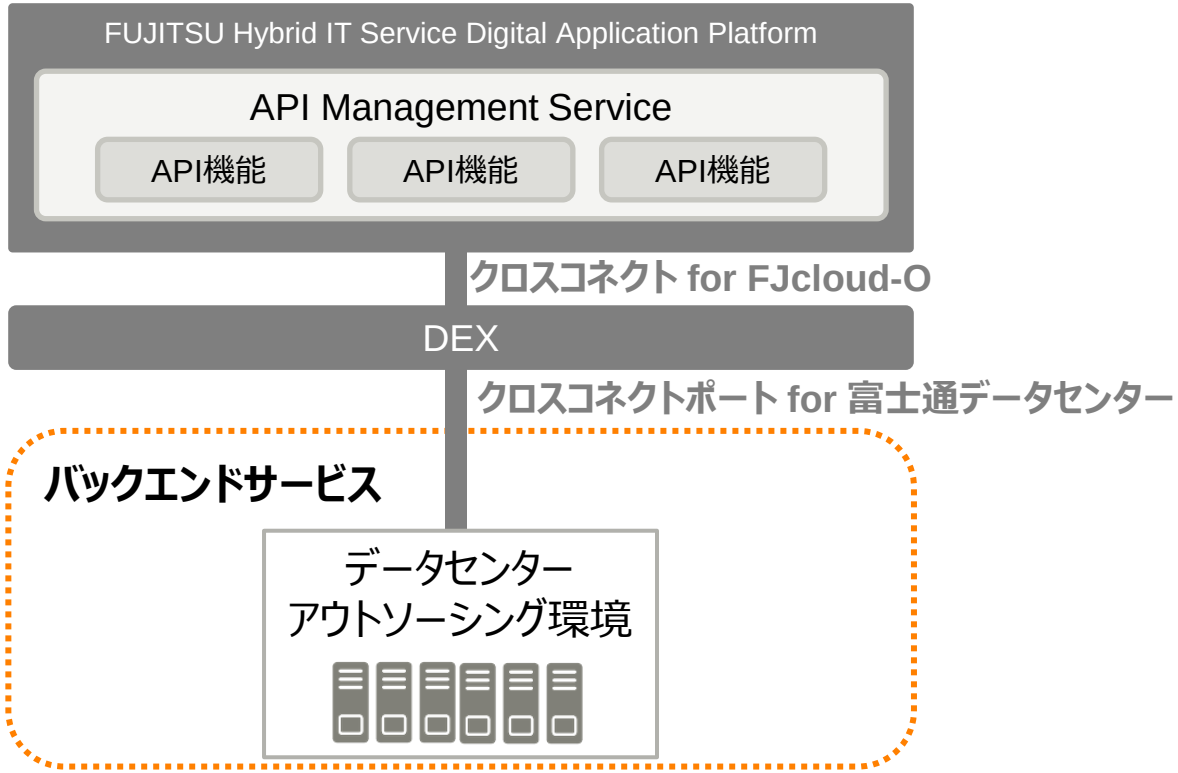
Javaプログラムの活用



バックエンドセキュア接続機能（Digital enhanced EXchange）

FUJITSU Hybrid IT Service FJcloud Digital enhanced EXchange（以下、DEX※）を利用して、データセンターアウトソーシング環境に構築されたバックエンドサービスにセキュアに接続できます。
DMZに配備できないバックエンドサービスのデータソースにアクセスできます。なお、ゲートウェイ拡張の機能も使用できます。

※別途、DEXの申込が必要です。
詳細は以下のページをご参照ください。
https://jp.fujitsu.com/solutions/cloud/fjcloud/-o/function/paas/private-connect/



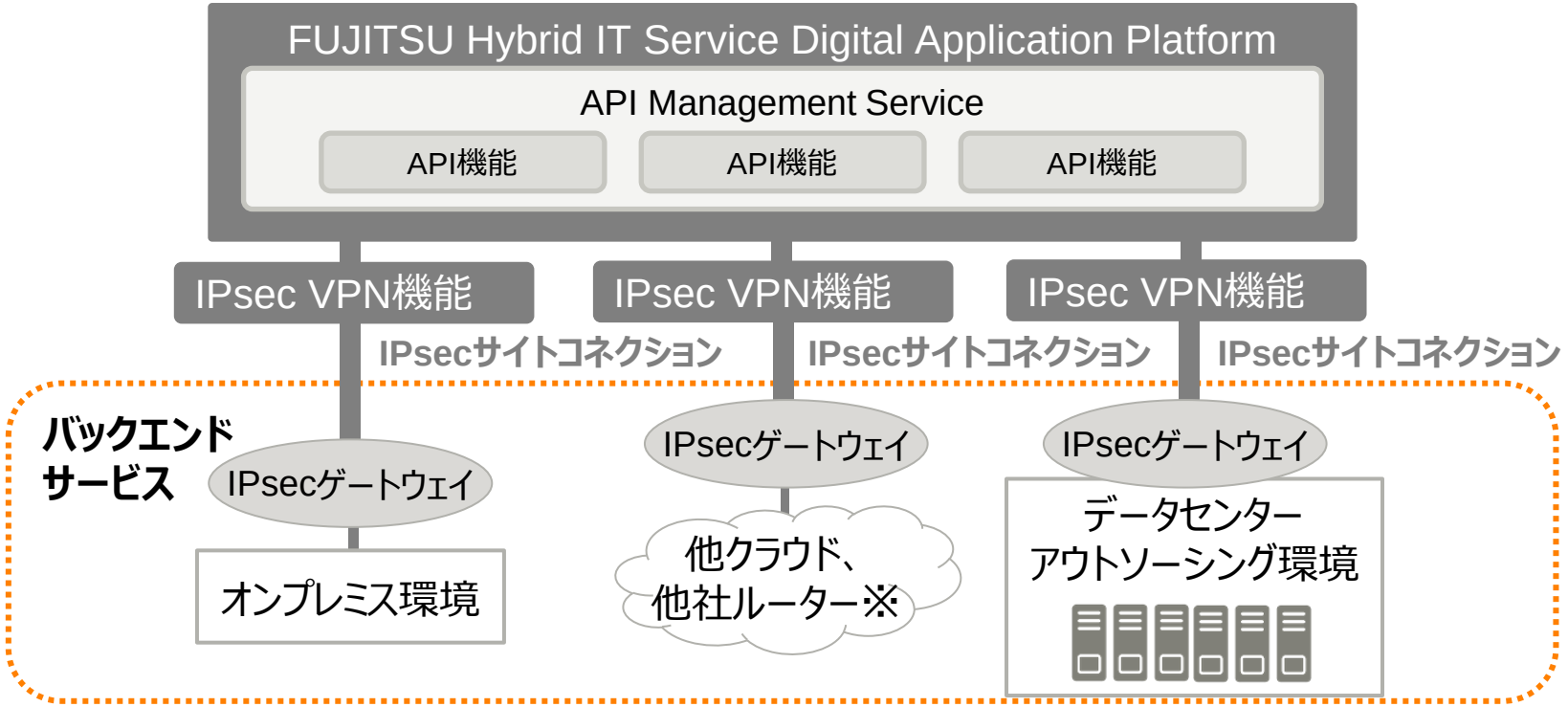
DEX提供メニューのうち、以下に対応しています。
a.クロスコネクト for FJcloud-O
（100Mbpsベストエフォートのみ）
（100Mbps帯域確保のみ）
b.クロスコネクトポート for 富士通データセンター
データセンターアウトソーシングサービスの中で提供されるメニューとなり、DEXのご契約に加え、データセンターアウトソーシングサービスの契約が必要となります。

※その他の接続形態（WANコネクト for FENICS、クラウドコネクトなど）をご希望の際はヘルプデスクまでお問合せください。

バックエンドセキュア接続機能（IPsec VPN接続）

IPsec VPN機能（※）を利用して、各種クラウドやオンプレミス環境などに構築されたバックエンドサービスにセキュアに接続できます。DMZに配備できないバックエンドサービスのデータソースにアクセスできます。
なお、ゲートウェイ拡張の機能も使用できます。

※IPsec VPN機能の詳細については、以下をご参照ください。
https://doc.cloud.global.fujitsu.com/lib/iaas/jp/function-manual/index.html

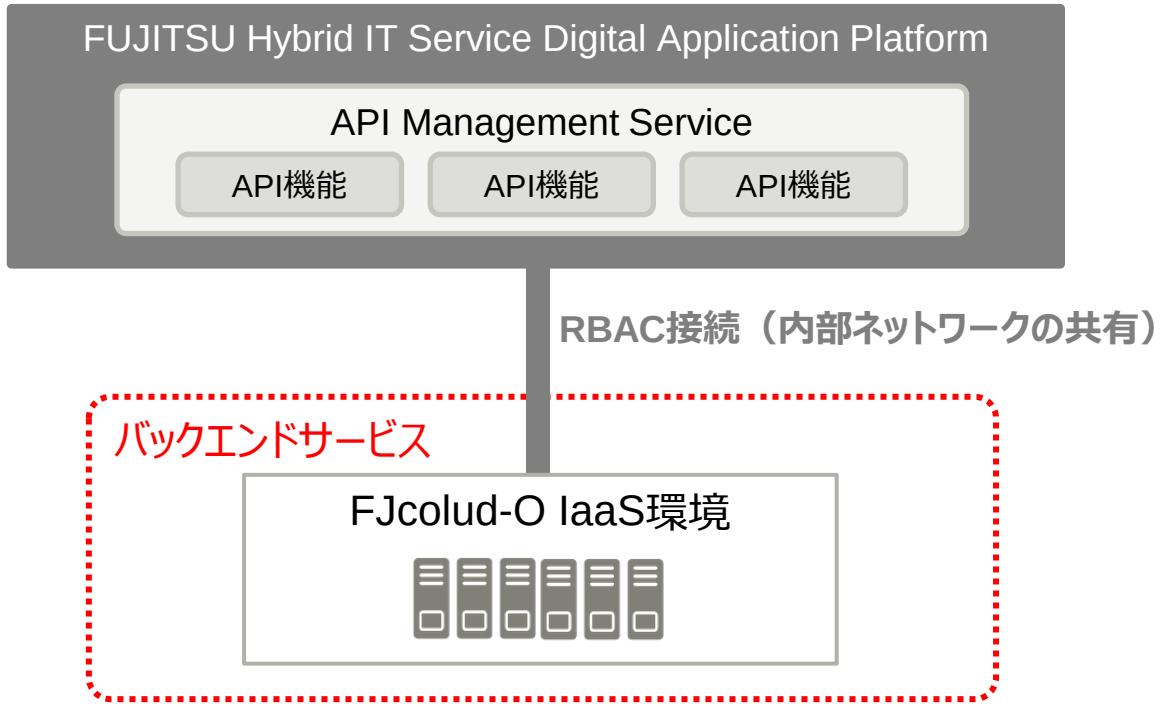


※他クラウド、他社ルーターと接続する場合、IPsecVPNがサポートされていても接続できない場合があります

バックエンドセキュア接続機能（ネットワークRBAC接続）

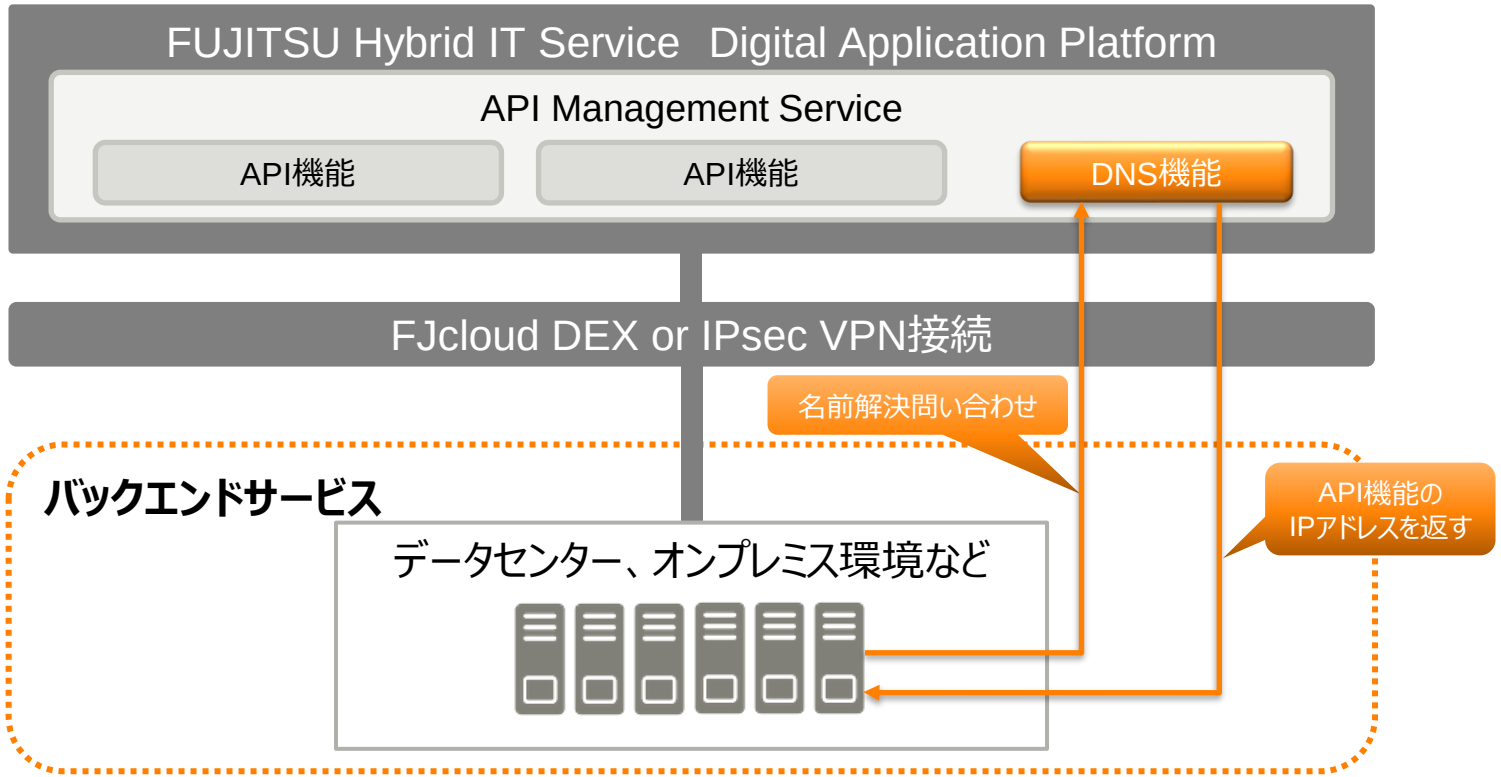
FUJITSU Hybrid IT Service FJcloud-O IaaSのネットワークRBAC機能（※）を利用して、FJcloud-O IaaSに構築されたバックエンドサービスにセキュアに接続できます。
DMZに配備できないバックエンドサービスのデータソースにアクセスできます。なお、ゲートウェイ拡張の機能も使用できます。（東日本リージョン３、西日本リージョン３、マルチリージョンのみ）

※ネットワークRBAC機能の詳細については、以下をご参照ください。
https://doc.cloud.global.fujitsu.com/lib/iaas/jp/function-manual/index.html



DNS機能

バックエンドセキュア接続では、接続したネットワーク環境に対してAPIを公開することが可能です。
DNSオプションでは、API公開時に必要となるFQDNの名前解決を行うことができます。
本機能はバックエンドセキュア接続のオプションとして提供します。



DNSに設定するドメイン名は、お客様のドメインのサブドメインや、ローカルドメインが使用できます。

フルアナリティクス機能

- 各3M/10M/20Mのプランでは、以下の解析パターンを利用できる「フルアナリティクスオプション」を選択できます。（東日本リージョン３、西日本リージョン３、マルチリージョンのみ）
  - Target Performance
  - Cache Performance
  - Error Analysis
  - Developer Engagement
  - 上記の解析パターンで生成される詳細データを保持する期間（「アナリティクスデータ保持期間」）は「3か月」となります。
    - 保持期間を過ぎた詳細データは削除されます。
  - プラン変更により、アナリティクスデータ保持期間とAPIコール数を変更できます。
- WebAPIを利用した分析
  - 統計情報関連のWebAPIを使用して詳細データを取得することで効率的な分析が可能です。

WebAPI

- WebAPI
  - HTTPクライアントを使用してAPIサービスにHTTPSでアクセスできるREST APIです。
  - 以下の操作をAPIで実行できるようにWebAPIを公開します。
    - SSL証明書の一覧取得、アップロード、エクスポート（ゲートウェイ拡張機能およびバックエンドセキュア接続機能）
      - 一覧取得はGUIでも可能です。
    - アナリティクスサービスのデータの取得（API、開発者、開発者アプリに関する統計情報の取得）
      - GUIで参照は可能ですが、WebAPIを使用することで効率的な分析が可能です。
  - 使用可能なWebAPIについては、以下をご確認ください。
    FUJITSU Hybrid IT Service ポータル＞ドキュメント＞マニュアル＞API Management Service＞「WebAPIリファレンス」

マルチリージョン

- 東日本リージョン3／西日本リージョン3
  - 各リージョンでの利用に加えて、マルチリージョン（東日本リージョン3／西日本リージョン3）にて本サービスを利用することができます。
  - マルチリージョンにてサービスを利用することにより、東日本リージョン3または西日本リージョン3のいずれかのサービスが停止するなどの大規模障害が発生した場合でもサービスを継続して利用することができます。
  - 基本構成、ゲートウェイ拡張構成、バックエンドセキュア接続構成のいずれの構成でも利用することができます。

サービスアカウントと環境

- ID, パスワード
  - 管理者権限を有するIDおよびパスワードを設定し、担当者に通知します。担当者は、管理者権限をもつアカウントを利用することにより、アカウントを追加することができます。
  - 追加するアカウントに設定できる権限は、Organization Administrator, Operations Administrator, Business User, Userの４種類となります。
- 組織、環境
  - １契約に対して１つのOrganization（組織）を利用することができます。
  - Organization（組織）は、API Management Serviceの管理単位です。
  - １組織に対して、テスト向け、本番向けの２つのEnvironment（環境）を利用することができます。

API Management Serviceサービスメニュー（1/5）

FUJITSU

○ サービスメニュー（東日本リージョン1）

メニュー	課金単位	備考
基本構成		【Pro】 API呼出回数(※3か月ごとに集計) 固定(固定メニュー)+従量(超過オプション) ・固定:2500万コール/3か月 ・超過オプション:250万コール毎 【Standard】 API呼出回数(※1か月ごとに集計) 固定(固定メニュー)+従量(オプション) ・固定(3M):300万コール/1か月 ・固定(10M):1000万コール/1か月 ・固定(20M):2000万コール/1か月 ・超過オプション:100万コール毎
Pro		
固定メニュー(Pro)	月	
Standard		
固定メニュー(3M)	月	
固定メニュー(10M)		
固定メニュー(20M)		
ゲートウェイ拡張構成		
Pro		
固定メニュー(Pro)	月	
Standard		
固定メニュー(3M)	月	
固定メニュー(10M)		
固定メニュー(20M)		

（次ページへ続く）

API Management Serviceサービスメニュー（2/5）

FUJITSU

○ サービスメニュー(東日本リージョン1 続き)

メニュー	課金単位	備考
バックエンドセキュア接続構成		【Pro】 API呼出回数(※3か月ごとに集計) 固定(固定メニュー)+従量(超過オプション) ・固定:2500万コール/3か月 ・超過オプション:250万コール毎 【Standard】 API呼出回数(※1か月ごとに集計) 固定(固定メニュー)+従量(オプション) ・固定(3M):300万コール/1か月 ・固定(10M):1000万コール/1か月 ・固定(20M):2000万コール/1か月 ・超過オプション:100万コール毎
Pro		
固定メニュー(Pro)	月	
Standard		
固定メニュー(3M)	月	
固定メニュー(10M)		
固定メニュー(20M)		
オプション		
超過オプション		
超過オプション(Pro)	250万コール毎	
超過オプション(Standard)	100万コール毎	
DNSオプション		
DNSオプション	月	バックエンドセキュア接続プランをご利用の方が利用可能なオプションです。

API Management Serviceサービスメニュー（3/5）

○ Pro／Standardで利用できる機能(東日本リージョン1)

○: 利用可能
—: 利用不可

機能				Pro	Standard 3M/10M/20M
ゲートウェイサービス（API Proxyの設定～公開の機能）				○	○
アナリティクスサービス (解析&モニタリング機能)	ダッシュボード			○	○
	解析画面	Proxy Performance	API Proxyのトラフィック量と平均応答時間を グラフ化	○	○
		Target Performance	全バックエンドサービスへのトラフィック量とリクエス トの成功・失敗件数、応答時間、レスポンスの 成功・失敗件数、ペイロードサイズをグラフ化	○	○
		Cache Performance	トラフィック制御ポリシーを通じて処理された キャッシュヒット率や件数、応答時間をグラフ化	○	—
		Latency Analysis	API Proxyの応答時間や、バックエンドサービス の応答時間をグラフ化	○	○
		Error Analysis	API Proxyが処理するリクエストおよびレスポン スで発生したエラーの情報（件数やステータス コード等）をグラフ化	○	○
		Developer Engagement	Developerの人数やアクセス状況、トラフィック 量、エラー率をグラフ化	○	—
		Traffic Composition	API Proxy、API Product、Developer、アプリケーションのトラフィック量Top10をグラフ化	○	○
		Devices	API Proxyに対するアクセス元のデバイス情報 （プラットフォーム、エージェント、デバイスタイプ、OS種別等）をグラフ化	○	○
	Custom Reports			○	—

※各リージョンごとの仕様はサービス仕様書にてご確認ください。

API Management Serviceサービスメニュー（4/5）

FUJITSU

○ サービスメニュー（東日本リージョン3、西日本リージョン3、マルチリージョン）

メニュー	課金単位	備考
基本構成		【Standard】 API呼出回数(※1か月ごとに集計) 固定(固定メニュー)+従量(オプション) ・固定(3M):300万コール/1か月 ・固定(10M):1000万コール/1か月 ・固定(20M):2000万コール/1か月 ・超過オプション:100万コール毎
Standard		
固定メニュー(3M)	月	
固定メニュー(10M)		
固定メニュー(20M)		
固定メニュー(3M)フルアナリティクスオプション		
固定メニュー(10M)フルアナリティクスオプション		
固定メニュー(20M)フルアナリティクスオプション		
ゲートウェイ拡張構成		
Standard		
固定メニュー(3M)	月	
固定メニュー(10M)		
固定メニュー(20M)		
固定メニュー(3M)フルアナリティクスオプション		
固定メニュー(10M)フルアナリティクスオプション		
固定メニュー(20M)フルアナリティクスオプション		
バックエンドセキュア接続構成		
Standard		
固定メニュー(3M)	月	
固定メニュー(10M)		
固定メニュー(20M)		
固定メニュー(3M)フルアナリティクスオプション		
固定メニュー(10M)フルアナリティクスオプション		
固定メニュー(20M)フルアナリティクスオプション		
オプション		
超過オプション		
超過オプション(Standard)	100万コール毎	
DNSオプション		
DNSオプション	月	バックエンドセキュア接続プランをご利用の方が利用可能なオプションです

API Management Serviceサービスメニュー（5/5）

FUJITSU

○ Standardで利用できる機能

（東日本リージョン3、西日本リージョン3、マルチリージョン）

○: 利用可能
△ : フルアナリティクスオプションで利用可能
—: 利用不可

機能				Standard 3M/10M/20M
ゲートウェイサービス（API Proxyの設定～公開の機能）				○
アナリティクスサービス (解析&モニタリング機能)	ダッシュボード			○
	解析画面	Proxy Performance	API Proxyのトラフィック量と平均応答時間を グラフ化	○
		Target Performance	全バックエンドサービスへのトラフィック量とリクエス トの成功・失敗件数、応答時間、レスポンスの成功・失敗件数、ペイロードサイズをグラフ化	○
		Cache Performance	トラフィック制御ポリシーを通じて処理された キャッシュヒット率や件数、応答時間をグラフ化	△
		Latency Analysis	API Proxyの応答時間や、バックエンドサービス の応答時間をグラフ化	○
		Error Analysis	API Proxyが処理するリクエストおよびレスポン スで発生したエラーの情報（件数やステータスコード等）をグラフ化	○
		Developer Engagement	Developerの人数やアクセス状況、トラフィック 量、エラー率をグラフ化	△
		Traffic Composition	API Proxy、API Product、Developer、アプリケーションのトラフィック量Top10をグラフ化	○
		Devices	API Proxyに対するアクセス元のデバイス情報 （プラットフォーム、エージェント、デバイスタイプ、OS種別等）をグラフ化	○
	Custom Reports			△

各リージョンごとの仕様はサービス仕様書にてご確認ください。

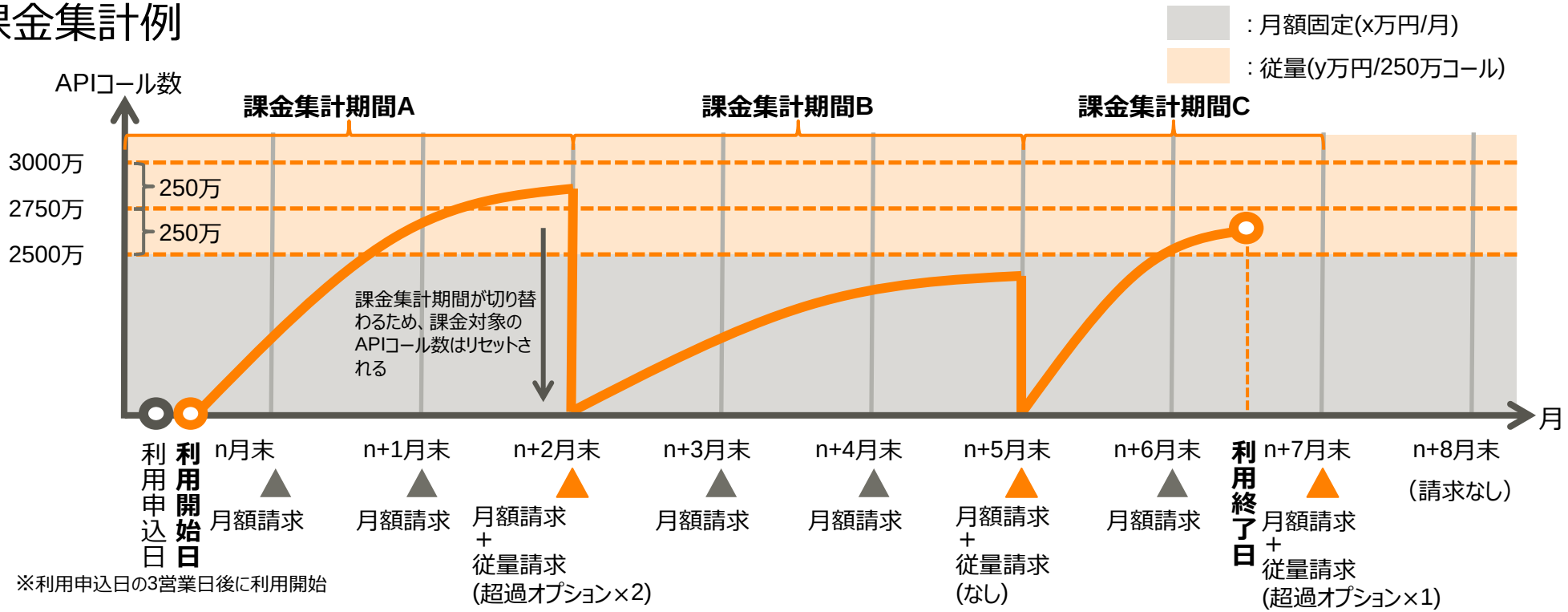
課金の考え方について（1/3）

- 課金の考え方（Pro）（東日本リージョン1のみ）
  - 月額固定＋従量課金
    - 本サービスに登録したAPIのコール数に応じて月額固定＋従量(超過オプション)で課金。
    - 月額固定：固定料金/月
      ※利用可能なAPIコール数：2500万コール/3か月
    - 従量(超過オプション)：250万コール毎
      ※1 3か月の合計APIコール数が2500万コールを超えた場合に発生します。
      ※2 3か月毎に課金・請求されます。
      ただし、利用終了時は利用終了月に課金・請求されます。
    - 利用開始日、利用終了日について
      - 利用開始日は、利用申込日(FUJITSU Hybrid IT Service ポータルよりお申込みいただいた日)の3営業日後となります。
      - 利用開始日の月から利用終了日の月まで料金が発生します。
      - 利用終了日は、利用終了申込日となります。

Proの場合の課金集計の例は次ページをご参照ください。

課金の考え方について（2/3）

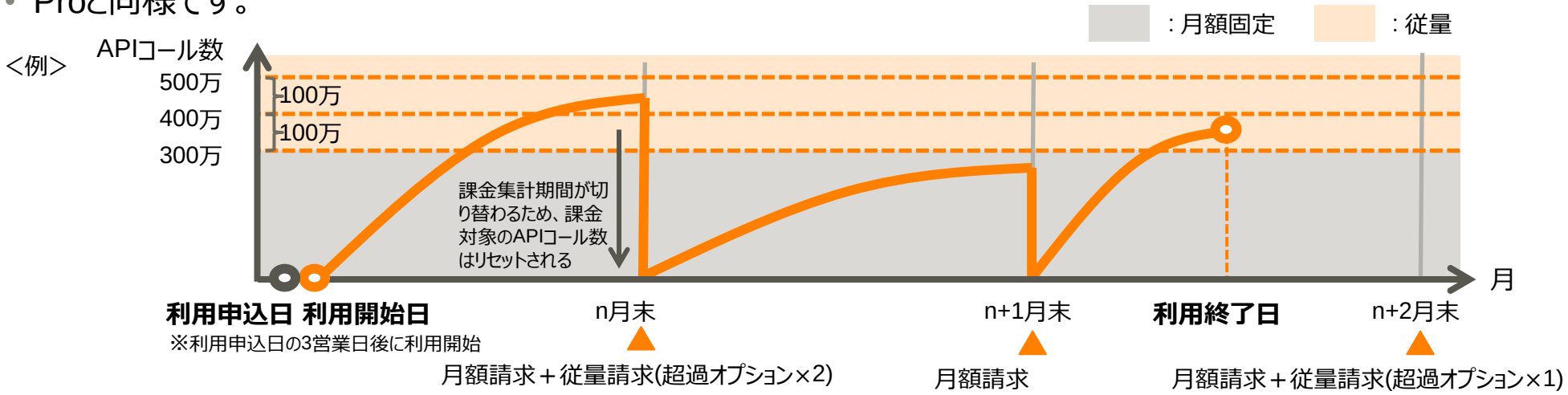
○ 課金集計例



- **課金集計期間A：月中利用開始／従量あり**
  - 利用開始月を含む3か月で集計。2か月目(n+1月)で月額固定の2500万コールを超えているが、従量の請求は3か月毎のため3か月目(n+2月)で請求。2750万 <コール数≦3000万のため、n+2月の請求は(x+2y)万円。　※月額＋従量超過オプション×2
- **課金集計期間B：継続利用中／従量なし**
  - 3か月の総APIコール数が2500万以下のため、従量請求はなし。n+5月の請求はx万円。
- **課金集計期間C：課金集計期間が3か月に満たない解約**
  - 集計期間の2か月目(n+7月)に利用終了。従量請求は利用終了月末に行われる。n+7月の請求は(x+y)万円。

課金の考え方について（3/3）

- 課金の考え方（Standard）
  - 月額固定＋従量課金
    - 本サービスに登録したAPIのコール数に応じて月額固定＋従量(超過オプション)で課金。
    - 月額固定：固定料金/月
      ※利用可能なAPIコール数：(選択したプランによる)/1か月
    - 従量(超過オプション)：100万コール毎
      ※1 料金月内のAPIコール数が各プランのコール数を超えた場合に発生します。
      ※2 1か月毎に課金・請求されます。
    - 利用開始日、利用終了日について
      - Proと同様です。



プラン変更の可否（1/4）

- プラン変更のお取り扱いは以下となります。（東日本リージョン1）
  - プラン変更後もプラン変更前のOrganization（組織）、Environment（環境）および登録したAPI Proxyは引き続きご利用いただけます。
  - プラン変更に伴うサービス停止時間（サービスにログイン不可能な時間）はございません。

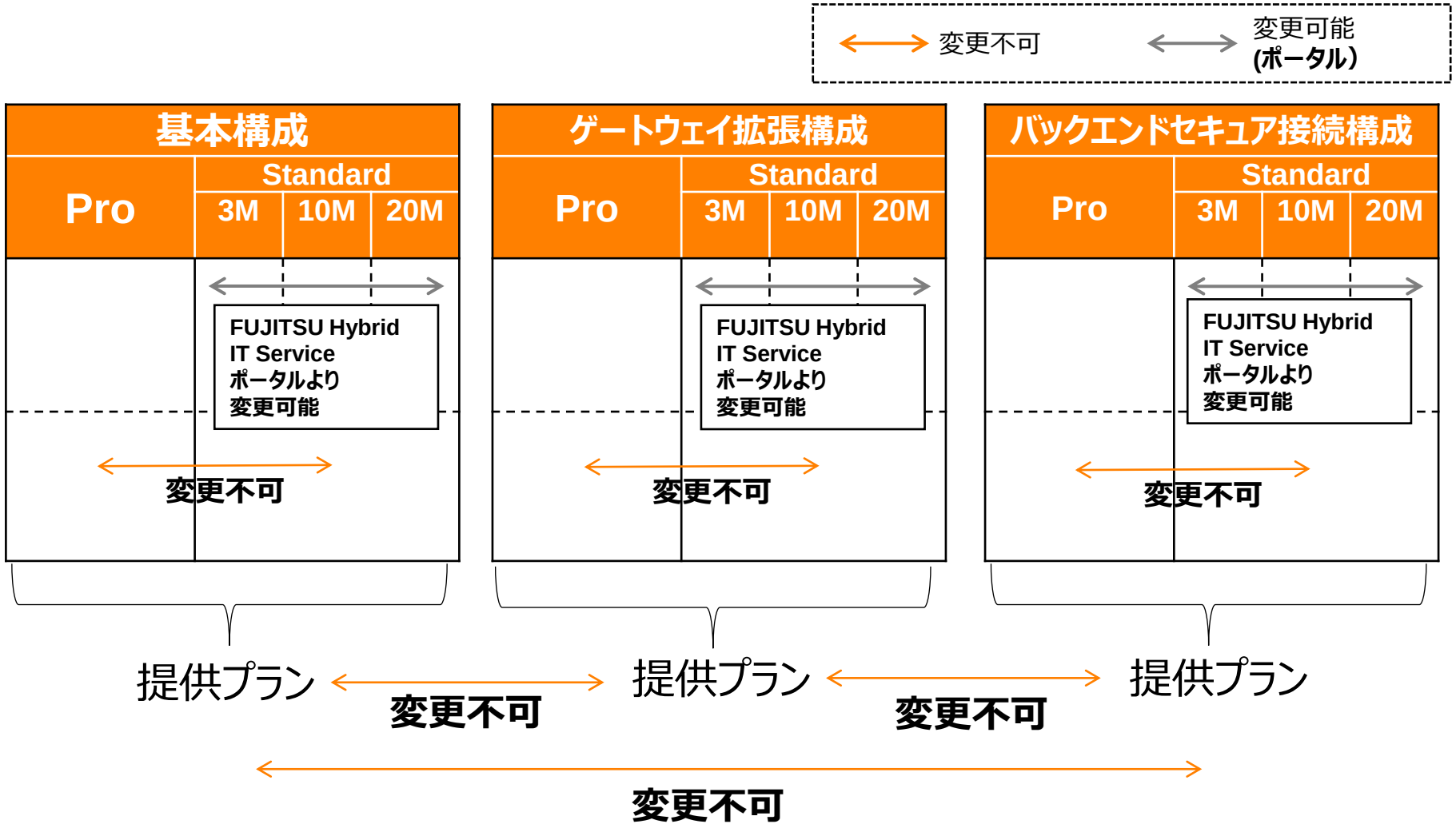
●：変更可能
FUJITSU Hybrid IT Service ポータルから変更の申し込みが可能です。

×：変更不可
プラン変更はできません。

利用中のサービス ＼ 変更するサービス	基本構成 Pro	基本構成 3M	基本構成 10M	基本構成 20M	ゲートウェイ拡張構成 Pro	ゲートウェイ拡張構成 3M	ゲートウェイ拡張構成 10M	ゲートウェイ拡張構成 20M	バックエンドセキュア接続構成 Pro	バックエンドセキュア接続構成 3M	バックエンドセキュア接続構成 10M	バックエンドセキュア接続構成 20M
基本構成 Pro		×	×	×	×	×	×	×	×	×	×	×
基本構成 3M	×		●	●	×	×	×	×	×	×	×	×
基本構成 10M	×	●		●	×	×	×	×	×	×	×	×
基本構成 20M	×	●	●		×	×	×	×	×	×	×	×
ゲートウェイ拡張構成 Pro	×	×	×	×		×	×	×	×	×	×	×
ゲートウェイ拡張構成 3M	×	×	×	×	×		●	●	×	×	×	×
ゲートウェイ拡張構成 10M	×	×	×	×	×	●		●	×	×	×	×
ゲートウェイ拡張構成 20M	×	×	×	×	×	●	●		×	×	×	×
バックエンドセキュア接続構成 Pro	×	×	×	×	×	×	×	×		×	×	×
バックエンドセキュア接続構成 3M	×	×	×	×	×	×	×	×	×		●	●
バックエンドセキュア接続構成 10M	×	×	×	×	×	×	×	×	×	●		●
バックエンドセキュア接続構成 20M	×	×	×	×	×	×	×	×	×	●	●	

プラン変更の可否（2/4）

○ プラン変更のお取り扱いは以下となります。（東日本リージョン1）



プラン変更の可否（3/4）

- プラン変更のお取り扱いは以下となります。
  （東日本リージョン3、西日本リージョン3、マルチリージョン）
  - プラン変更後もプラン変更前のOrganization（組織）、Environment（環境）および登録したAPI Proxyは引き続きご利用いただけます。
  - プラン変更に伴うサービス停止時間（サービスにログイン不可能な時間）はございません。

○: 変更可能（要お問合せ）
ヘルプデスクへのお問合せが必要です。

×: 変更不可
プラン変更はできません。
解約、新規申込となります。

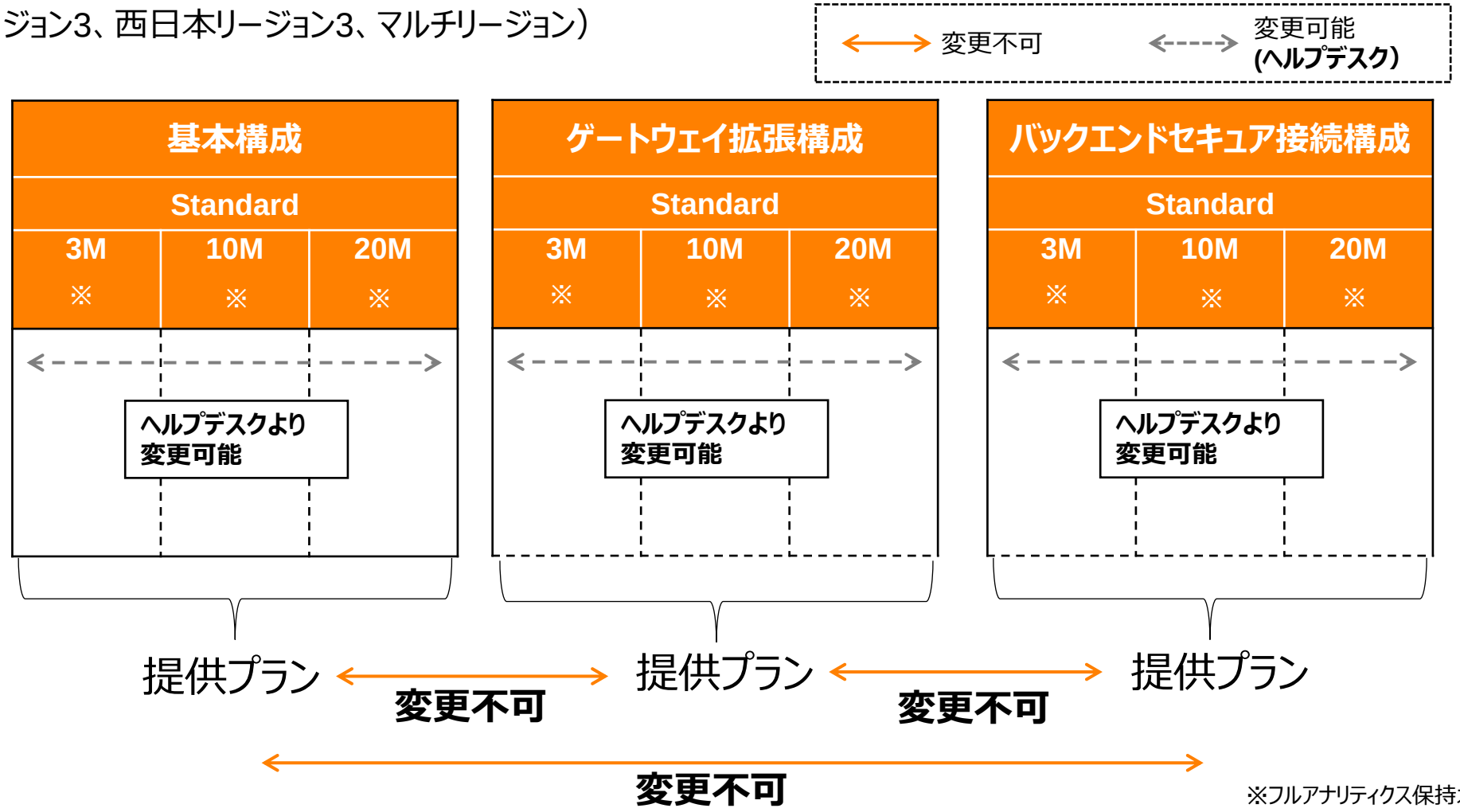
※フルアナリティクス保持オプションの有無を問いません。

利用中のサービス ＼ 変更するサービス	基本構成 3M※	基本構成 10M※	基本構成 20M※	ゲートウェイ拡張構成 3M※	ゲートウェイ拡張構成 10M※	ゲートウェイ拡張構成 20M※	バックエンドセキュア接続構成 3M※	バックエンドセキュア接続構成 10M※	バックエンドセキュア接続構成 20M※
基本構成 3M※		○	○	×	×	×	×	×	×
基本構成 10M※	○		○	×	×	×	×	×	×
基本構成 20M※	○	○		×	×	×	×	×	×
ゲートウェイ拡張構成 3M※	×	×	×		○	○	×	×	×
ゲートウェイ拡張構成 10M※	×	×	×	○		○	×	×	×
ゲートウェイ拡張構成 20M※	×	×	×	○	○		×	×	×
バックエンドセキュア接続構成 3M※	×	×	×	×	×	×		○	○
バックエンドセキュア接続構成 10M※	×	×	×	×	×	×	○		○
バックエンドセキュア接続構成 20M※	×	×	×	×	×	×	○	○	

プラン変更の可否（4/4）

○ プラン変更のお取り扱いは以下となります。

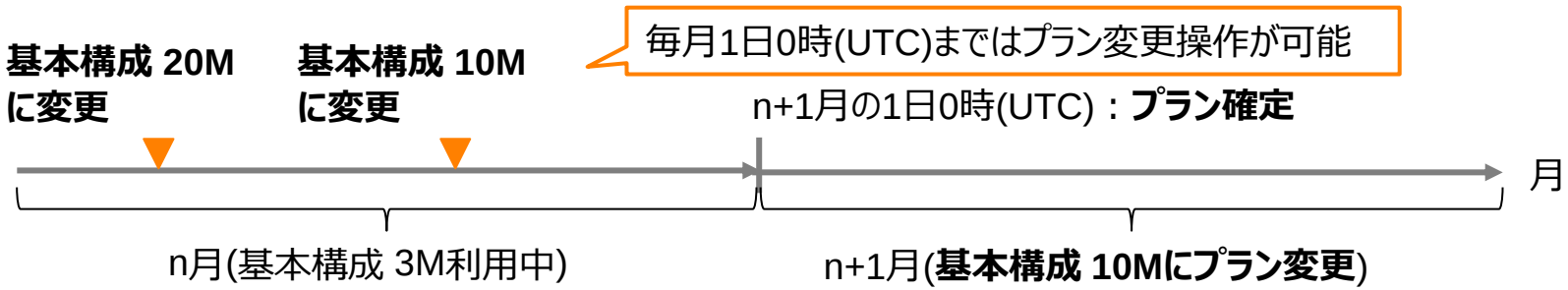
（東日本リージョン3、西日本リージョン3、マルチリージョン）



※フルアナリティクス保持オプションの有無を問いません。

プラン変更方法

- Standard間の変更方法
  - FUJITSU Hybrid IT Serviceポータルの「ご利用サービス管理」画面より変更が可能です。
  - 毎月1日0時(UTC)時点で選択されているプランで該当月のプランが確定し、課金が行われます。



プラン変更時の注意事項（東日本リージョン3、西日本リージョン3、マルチリージョン）

- 解析機能（アナリティクスサービス）のデータ保持について
  - アナリティクスサービスで使用するデータには「サマリデータ」と「詳細データ」があります。
    - サマリデータ：すべてのプランにて保持されるデータ
    - 詳細データ：フルアナリティクスオプションのみで保持されるデータ
      - 対象プランを利用開始すると詳細データの保持が開始されます。
      - 詳細データを保持しないプランに変更した場合は詳細データは削除されます。

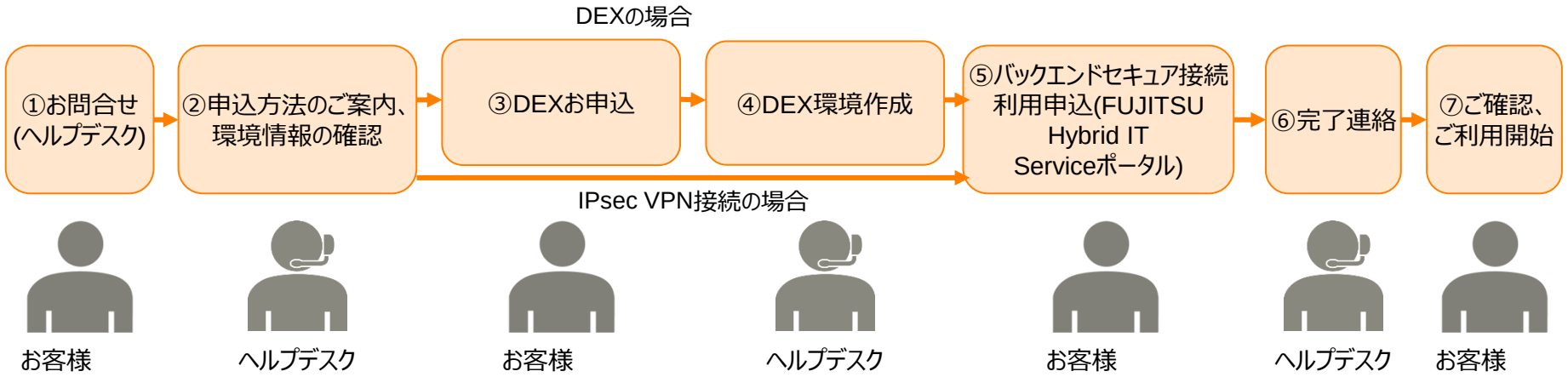
アナリティクスサービスの機能と使用するデータ

機能	使用データ
Proxy Performance	サマリデータ
Target Performance	サマリデータ、詳細データ
Cache Performance	サマリデータ、詳細データ
Latency Analysis	サマリデータ
Error Analysis	サマリデータ
Developer Engagement	サマリデータ、詳細データ
Traffic Composition	サマリデータ
Devices	サマリデータ
Custom Reports	サマリデータ、詳細データ

仕様はサービス仕様書にてご確認ください。

バックエンドセキュア接続の利用について

- FUJITSU Hybrid IT Service FJcloud Digital enhanced EXchangeを利用して接続する場合
  - 別途、DEXの申込が必要です。
  - DEXの申し込みには、本サービスとの接続のための情報が必要となりますので、ヘルプデスクよりお問合せください。
    詳細は、公開ホームページのFAQをご確認ください。
- FUJITSU Hybrid IT Service FJcloud-O IaaSのIPsec VPN機能を利用して接続する場合
  - 本サービスとの接続には対向IPsecVPNゲートウェイとの接続設定が必要となりますので、ヘルプデスクよりお問合せください。
    詳細はFUJITSU Hybrid IT Service 公開ホームページのFAQをご確認ください。
- FUJITSU Hybrid IT Service FJcloud-O IaaSのネットワークRBAC機能を利用して接続する場合
  - 本サービスとの接続には設定情報が必要となりますので、ヘルプデスクよりお問合せください。
    詳細はFUJITSU Hybrid IT Service 公開ホームページのFAQをご確認ください。
- ご利用開始までの流れは以下のとおりです。



制限事項・注意事項

- 本サービスの提供リージョンについては、FUJITSU Hybrid IT Service Digital Application Platform 公開ホームページのサービス仕様書をご参照ください。
- お申込から利用開始までにかかる期間は以下のとおりです。
  - 基本構成 Standard プランの場合
    FUJITSU Hybrid IT Serviceポータルのサービス利用設定申込画面から利用申込をしていただいてから約3営業日で環境の配備が完了します。
  - ゲートウェイ拡張構成 Standard プランの場合
    FUJITSU Hybrid IT Serviceポータルのサービス利用設定申込画面から利用申込をしていただいてから約10営業日で環境の配備が完了します。
  - バックエンドセキュア接続構成 Standard プランの場合
    バックエンドと接続する回線情報確認のため、お申込み前にヘルプデスクにお問い合わせください。
    DEXの場合、回線開通確認後、約10営業日でご利用いただけます。
    - DNSオプションをご利用になる場合、バックエンドセキュア接続構成プランの利用開始日以降に本オプションをFUJITSU Hybrid IT Serviceポータルのサービス利用設定申込画面から利用申込いただく必要があります。
      利用申込後、約10営業日で本オプションが利用可能になります。

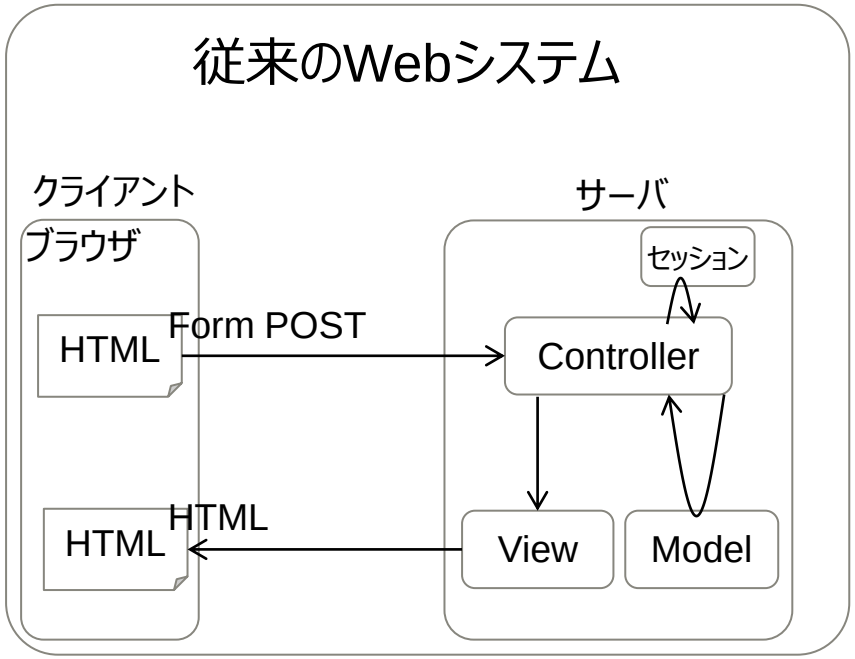
要素技術

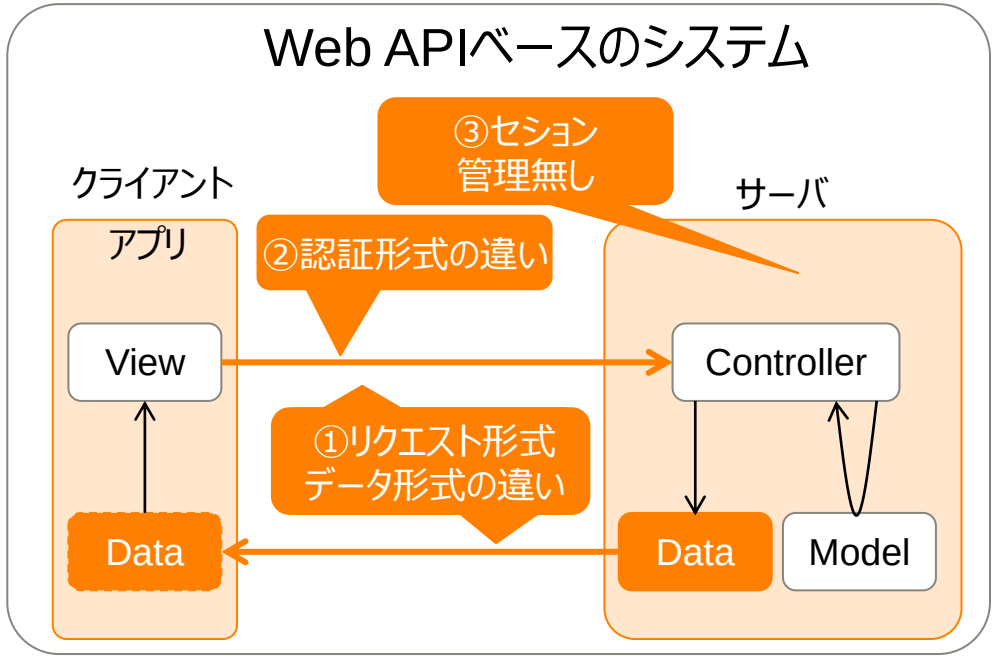
要素技術：従来のWebシステムとの違い

FUJITSU

○ アプリのアーキテクチャ面での、３つの大きな違い

①	リクエスト・レスポンス形式 （データ形式）	RESTスタイル / JSON形式
②	認証	認証するのは利用者だけではない （認証・認可）
③	セション管理	サーバ側では（原則）ステートレス





要素技術：リクエスト･レスポンス形式

FUJITSU

- アーキテクチャスタイル：REST
  - 「**Not 規約**」、緩いルール。４つの原則がある（RESTful）

HTTPメソッド（参照：GET, 登録：POST, 更新：PUT, 削除：DELETE）による操作

リソースをURIで表す | JSONやXMLを利用する | ステートレス

【例】Twitter API　指定したユーザーのフォロワー一覧を、ユーザーIDで取得する

リクエスト　GET　https://api.twitter.com/1.1/followers/ids.json?user_id=99999

操作：GET = 取得する

リソース：followers/idsから

条件：ユーザIDが99999の時

レスポンス（JSON）

```
{
  “ids” :[xxxxxx,xxxxx,xxxxx,xxxxx,xxxxx,・・・・],
  “next_cursor": 0,
   以下略
}
```

フォロワーのユーザIDが列挙される

JSON形式（JavaScript Object Notation）データ。
RFC/ECMAで規格化。JavaScriptで利用するデータ形式そのもの

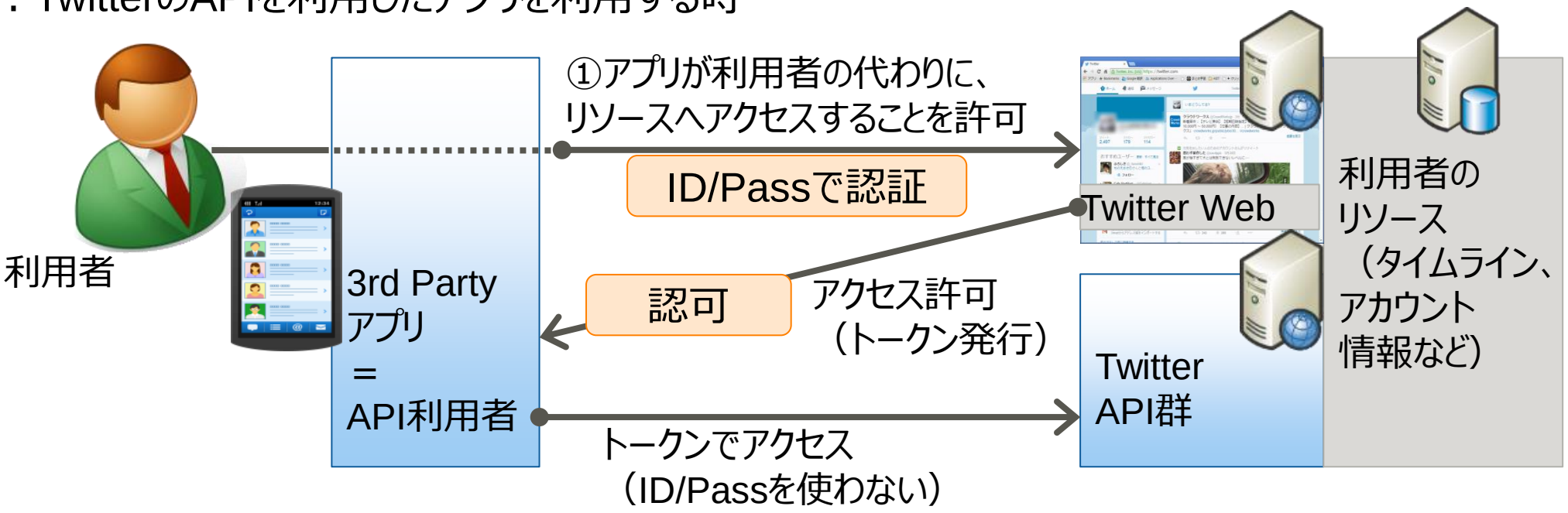
Webで使いやすい技術（JS親和性、データ量、パース性能etc）

要素技術：認証

- 認証するのは利用者だけではない
  - 従来のWebシステム：利用者を認証する（ID/Pass等）
  - WebAPI：クライアントは何らかのプログラム。
    利用形態によって、認証するものが異なる。

認証：本人確認　　認可：リソースへのアクセス権限委譲

  - 例：TwitterのAPIを利用したアプリを利用する時



要素技術：認証技術選択

- 先の例では、**API提供者-API利用者-アプリ利用者の3者間**
  - 2者間の場合（例えばクラウドの基盤管理API等）もある。
  - 登場者間の関係と、クレデンシャル（認証情報）の扱いの関係で選択する

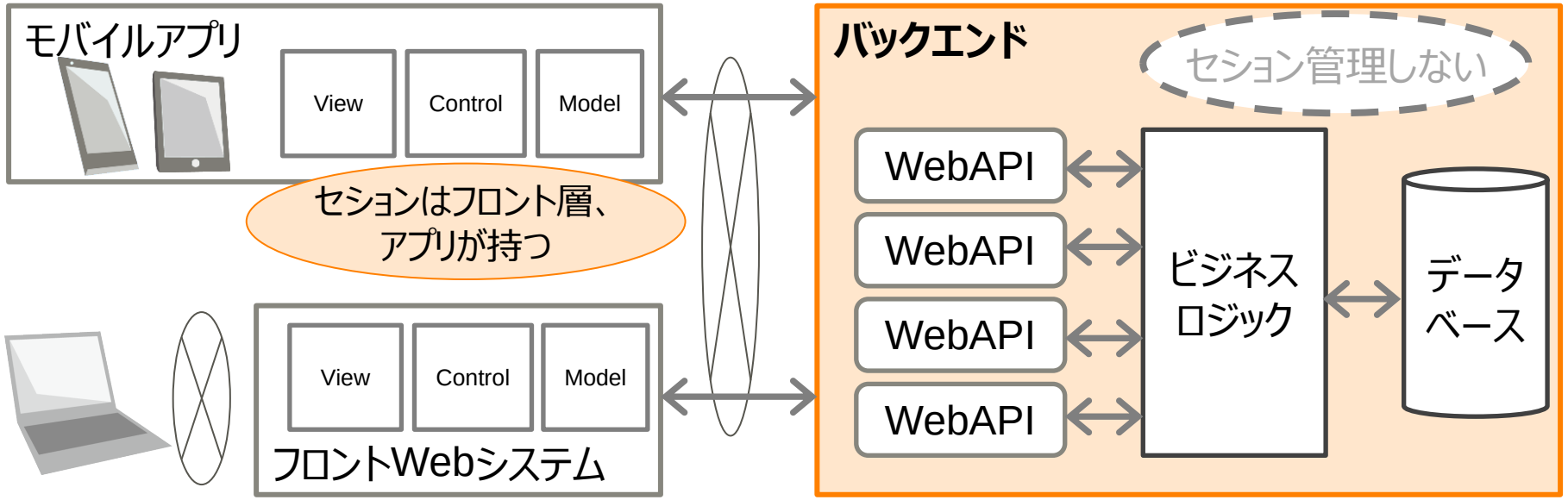
主な認証・認可方式	概要
APIキー	アプリ利用者を識別するIDを利用する
Digest認証	アプリ利用者とパスワードをMD5でハッシュ化。
WSSE	パスワードと日時とセキュリティトークンをSHA1でハッシュ化
SAML	異なるドメイン間でのシングルサインオン
OAuth1.0、2.0	APIへのアクセス権限をAPI利用アプリに委譲するプロトコル。 2.0は、HTTPSを必須としてプロトコルを簡易化。
OpenID Connect	OAuth2.0をベースにアイデンティティ層を拡張したOpenIDの次期仕様

【基本的な使い分けの考え方】

- データ公開範囲が無制限、人の認証不要　：APIキー
- アプリ利用者のクレデンシャルをアプリに渡してもよい　：Digest認証
- アプリ利用者のクレデンシャルをアプリに渡さない　：OAuth、OpenID Connect
- 利用者と提供者の信頼関係が構築済（B2Bなど）　：SAML

要素技術：セション管理

- バックエンドはステートレス構造に
  - ロジックが（再び）フロント層に移動、セションはフロント層で担う

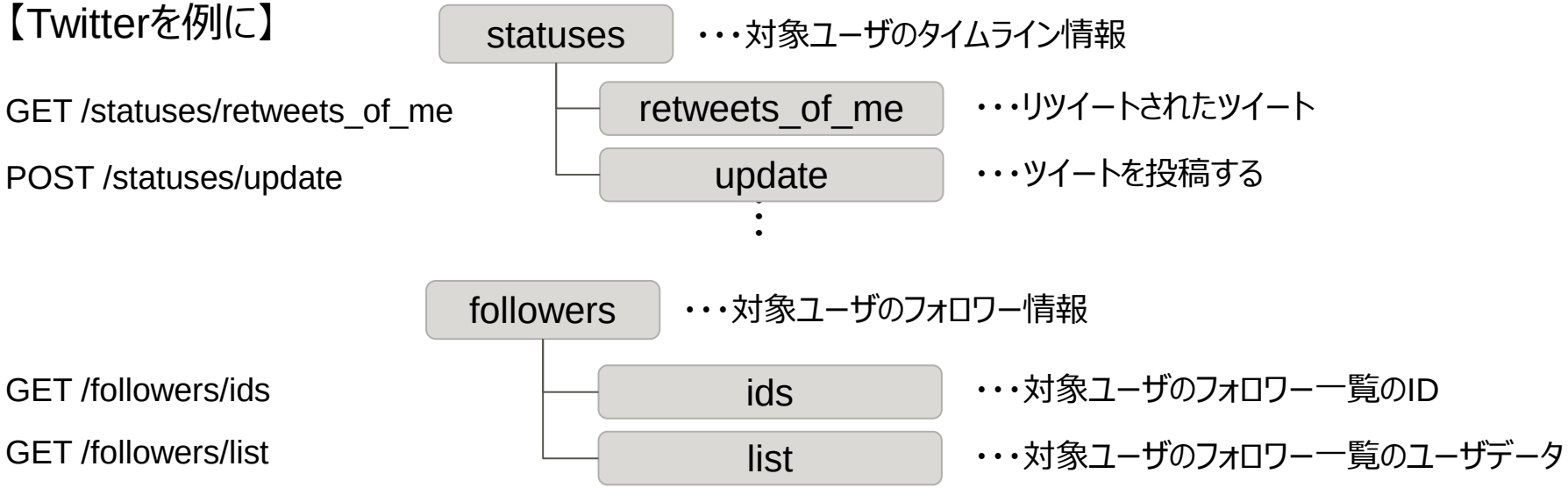


- スケーラビリティ・運用性の向上に効果（運用・基盤観点）
  - スティッキーセションからの解放 ⇒ ロードバランサネック回避
  - スケールアップ性の向上（特に、大規模サイトのオートスケールなど）
  - メンテナンス時運用のシンプル化、利用者影響の極小化

要素技術：REST関連

- HTTPメソッドによる操作　・・・　CRUDに割り当て可能
  - GET：get/list/findなど・・・情報参照、取得
  - PUT：update/replaceなど・・・更新
  - DELETE：delete/remove・・・削除
  - POST：create/generate・・・新規作成、（上記以外の）何らかの処理依頼
- リソース
  - ≒APIが提供するデータ構造（DB構造を基本に考えるとイメージしやすい）

【Twitterを例に】



要素技術：言語バインディング

FUJITSU

○ JAX-RS（Java EEのRESTアプリ用FW）の例

GET　https://api.twitter.com/1.1/followers/ids.json?user_id=99999

HTTPメソッドで
メソッドに割り当て

リソース（上位パス）
をクラスに割り当て

下位のパスを
メソッドに割り当て

パラメタを
引数に
割り当て

【Javaコードイメージ】

```
package jp.fujitsu.com.services;

@Path(“/followers”)
public class FollowerResources{

  @GET
  @Path(“/ids.json”)
  String getFollowerIDs(@PathParam(“user_id”)){
    //処理・・・・・
  }
```

こういう割り当てを
JAX-RSの
フレームワークが担う

要素技術：SOAP vs REST

- 仕様が規定されており相互接続性が高いため、企業間での利用にはSOAPもまだ多く利用されている
- 重厚な規約がなく、サービスの利用／作成の負荷が低いため、コンシューマー向けにはRESTが向いている

	SOAP	REST
仕様の明確さ	○ W3C、WS-Iで規定	× 仕様の規定なし
相互接続性	○ 規約により標準化されてる	△ 利用者が提供者の仕様に 合わせて利用する
サービス開発のしやすさ	○ 規約に沿ったツール多数	△ 発展途上
サービスの利用しやすさ	△ 専用ライブラリやMWが必要	○ 比較的容易に利用できる
性能	△ パース処理が必要 RESTに比べメッセージサイズ大	○ SOAPに比べ早い

IKB-開発技術 アプリ方式 Webサービス選択ガイド ～SOAPとRESTはどう違う～（2011年）

参考情報

【参考】Policy - トラフィック管理

APIのトラフィックに関する処理（流量制限、キャッシュなど）ができます。

Policy	説明
 Quota	時間の単位（月、日、時、分、秒）と件数を指定し、リクエスト件数を制限します。
 Spike Arrest	秒間あたりのリクエスト件数を指定して制限します。 例）毎分３０件（３０pm）許可する設定にした場合、２秒毎に１件許可します。２秒以内に２件来た場合、２件目は処理されません。
 Concurrent Rate Limit	バックエンドサービスへの同時接続数を制限します。
 Response Cache	バックエンドサービスからのレスポンスをキャッシュします。
 Lookup Cache	Populate Cacheでキャッシュしたデータを取得します。
 Populate Cache	セッションIDや認証情報等、任意のデータをキャッシュします。
 Invalidate Cache	条件を指定してPopulate Cacheでキャッシュしたデータを削除します。
 Reset Quota	Quotaでカウントしたリクエスト件数を指定した値でリセットします。

【参考】Policy - データ加工

APIのデータ加工（形式変換、メッセージ修正など）ができます。

Policy	説明
JSON to XML	JSON形式をXML形式に変換します。
XML to JSON	XML形式をJSON形式に変換します。
Raise Fault	ステータスコードに応じてカスタムメッセージを出力します。
XSL Transform	XML 形式をHTML やプレーンテキスト等の別フォーマットに変換します。
SOAP Message Validation	受信したSOAPメッセージが、XSDスキーマまたはWSDLに準拠していない場合は拒否します。
Assign Message	HTTP Request またはResponse メッセージを作成・修正します。
Extract Variables	リクエストまたはレスポンス情報の値を取り出して、変数に値を設定します
Access Entity	Delvelopers、apps、API Product、Developer などの属性を取り出して、変数に値を設定します。
Key Value Map Operations	PUT、GET、DELETE メソッドでKey/Value のペアを保存・検索・削除します。

【参考】Policy - セキュリティ（1/2）

APIのセキュリティに関する制御（認証、脆弱性対策など）ができます。

Policy	説明
Basic Authentication	Basic 認証（Base64 のエンコードまたはデコード）の設定をします。
XML Threat Protection	XML の脆弱性に対する攻撃を防ぐ設定をします。
JSON Threat Protection	JSON の脆弱性に対する攻撃を防ぐ設定をします。
Regular Expression Protection	正規表現でリクエストを拒否します。
OAuth v2.0	OAuth2.0 のエンドポイントに対する設定（アクセストークンの生成やチェック等）をします。
Get OAuth v2.0 Info	OAuth2.0 のアクセストークンや認証コード等の情報を取得します。
Set OAuth v2.0 Info	OAuth2.0 のアクセストークンに関連付けられたカスタム属性を追加・更新します。

【参考】Policy - セキュリティ（2/2）

APIのセキュリティに関する制御（認証、脆弱性対策など）ができます。

Policy	説明
OAuth v1.0a	OAuth1.0a のエンドポイントに対する設定（アクセストークンの生成やチェック等）をします。
Get OAuth v1.0a Info	OAuth1.0a のアクセストークンや認証コード等の情報を取得します。
Verify API Key	アクセスを許可するAPI Key を設定をします。
Access Control	IP アドレスによるアクセス許可・拒否設定をします。
LDAP	LDAP 認証の設定をします。
Generate SAML Assetion	送信するXML Request にSAML Assertion を追加します。
Validate SAML Assertion	受信したSOAP Request に添付されているSAML Assertionをチェックし、無効なメッセージの場合は拒否します。

【参考】Policy - 拡張機能

スクリプトの実行、メッセージ内データ収集、ログ記録などができます。

Policy	説明
JavaScript	JavaScript を実行します。
Service Callout	外部サービスを呼び出します。
Statistics Collector	Analytics 用にメッセージ内のデータ（Product ID、価格、ターゲットURL等）を収集します。
Message Logging	syslog サーバにメッセージログを記録します。

【参考】解析一覧

FUJITSU

トラフィック量、応答時間、エラー数などを可視化できます。

解析パターン	説明
Proxy Performance	APIのトラフィック量と平均応答時間をグラフ化します。
Target Performance	バックエンドサービスへのトラフィック量とリクエストの成功・失敗件数、応答時間、レスポンスの成功・失敗件数、Payload Sizeをグラフ化します。
Cache Performance	Response Cache Policyのキャッシュヒット率や件数、応答時間をグラフ化します。
Latency Analysis	APIの応答時間や、バックエンドサービスの応答時間をグラフ化します。
Error Analysis	APIが処理するリクエストおよびレスポンスで発生したエラーの情報（件数やステータスコード等）をグラフ化します。
Developer Engagement	アプリ開発者の人数やアクセス状況、トラフィック量、エラー率をグラフ化します。
Traffic Composition	API、プロダクト、アプリ開発者、アプリのトラフィック量Top10をグラフ化します。
Devices	APIに対するアクセス元のデバイス情報（プラットフォーム、エージェント、デバイスタイプ、OS種別など）をグラフ化します。
Reports	縦軸(Metrics)および横軸(Dimensions)または時間を自由に選択して、情報をグラフ化します。

※東日本リージョン1でサービスをご利用の場合の例です。各リージョンごとの仕様はサービス仕様書にてご確認ください。

Thank you