



ほかにはない
アンサーを。

Amazon API Gateway 導入による オリックスグループ向けAPI の提供

2022年 6月17日
オリックス・システム株式会社

オリックスグループの紹介

オリックスグループの紹介

1964年にリース事業からスタートして隣接分野に進出し、現在では法人金融、産業/ICT機器、環境エネルギー、自動車関連、不動産関連、事業投資・コンセッション、銀行、生命保険など多角的に事業を展開しています。

また、1971年の香港進出を皮切りに世界約30カ国・地域に拠点を設け、グローバルに活動しています。

オリックス・システムは、国内・海外で発展するグループの中枢を担うシステム開発・運用会社として発展してきました。

単なるシステム子会社ではなく「オリックスグループ全体（従業員約32,000名/ 2022年3月末現在）のシステム部」として位置づけられています。

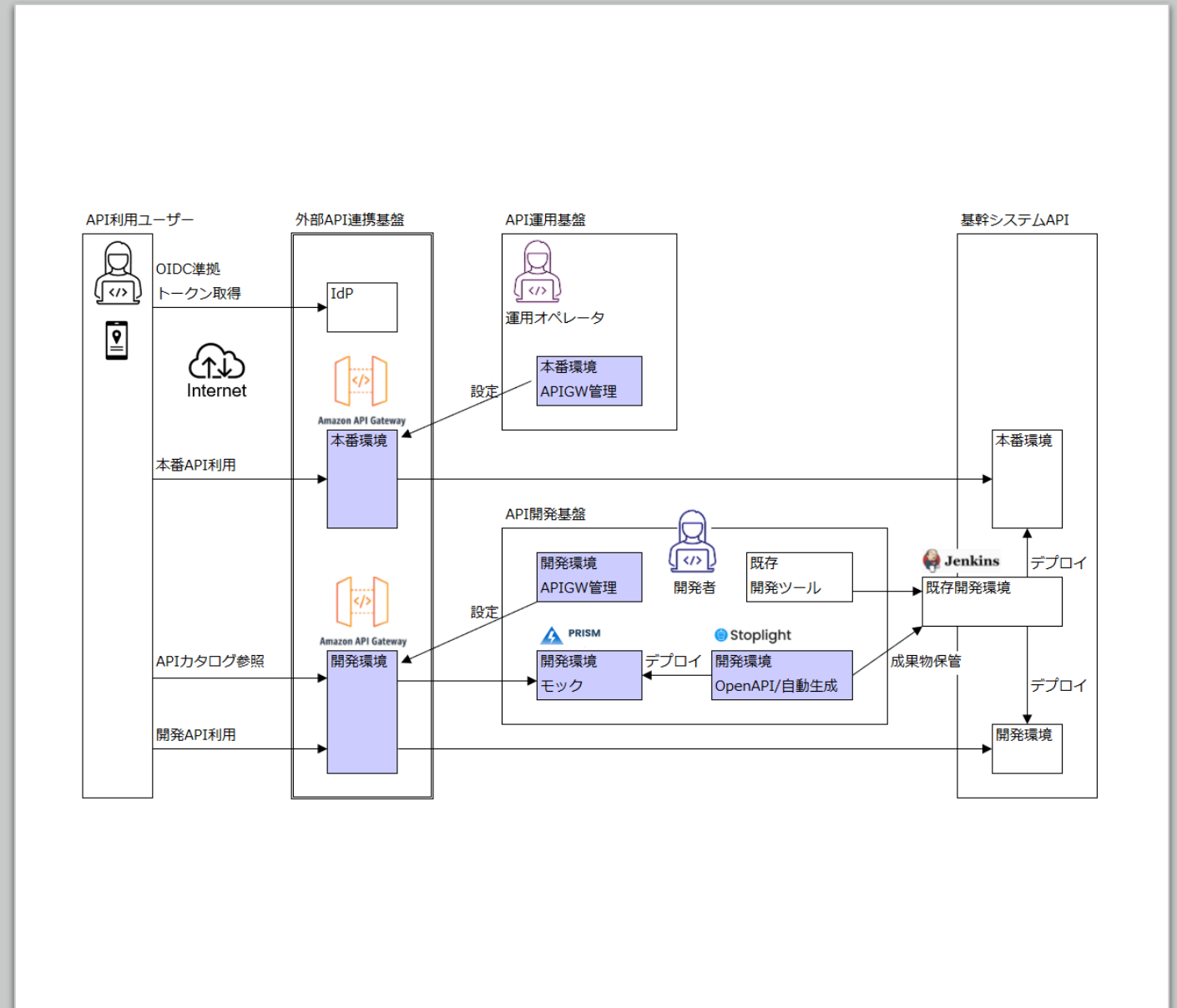
【オリックス・システムの特徴、データ】

- ・ 100%オリックスグループ向けのシステム開発で全て直請けの案件。
- ・ グループ業務のあらゆる場面で「システムの観点」から関わり、グループ全体を支えている。
- ・ 社員数：282名（2022.4現在）
- ・ 中途採用比率：56%
- ・ 女性比率：3割、男性育休取得実績有

本日、お話しするプロジェクトのキーワード

何を実現したかったのか

- ① 基幹API への安全なアクセス
(= 内部API の安全な外部公開)
- ② スモールスタート
- ③ 既存設備との疎結合な連携
- ④ 運用省力化
- ⑤ API ポータル・カタログの構築
- ⑥ API 管理のルール整備を急ぐ



プロジェクトの背景

プロジェクト規模

体制

- PJメンバー（5名）
- アプリ部門がプロマネ&AWS 設計に責任を持つ
- 新技術採用リスクに対し、外部支援体制を固めリターンを確実に
 - ・ クラスメソッド(株) AWSコンサルティングサービス
 - ・ (株)豆蔵 API デザイン方針の整備
 - ・ AWS ソリューションアーキテクトとのディスカッション

期間 約9カ月

- 他社製品含む調査およびPoC 期間（6カ月）
- 構築期間（3カ月）



サーバーレス型を選択したきっかけ、当初の期待

- 基幹システムをAPI 化し、安全に基幹データを活用できる技術を導入したい
 - ※APIゲートウェイ3製品を選定、ニュートラルな技術評価を実施
- セキュリティ、ログ、モニタリング等、API の横断的な一元管理を急ぎたい
- 複数データセンター統廃合が検討中のため、新規に自前基盤の構築は避けたい

- 必要な機能だけをスモールスタートで導入したい
- 保守運用フェーズでもメンテナンスコスト、ランニングコストを減らしたい

- 既存セキュリティポリシーとの整合性をとりつつ、「クラウドネイティブ」に

サーバーレス型を選択した決定要因と実際の効果

■ Amazon API Gateway 選定要因

- ・ スモールスタート可能な料金体系（必要な機能だけをオンデマンドで利用できる）
- ・ 強固なセキュリティ（WAF 多層境界防御、相互TLSによる身元確認、ACM 証明書発行 等）
- ・ Lambdaオーソライザー による柔軟なトークン検証（既存認証発行のJWT 検証）
- ・ サーバーレス採用による納期短縮、インフラ部門の運用、保守コストの軽減
- ・ 将来の拡張性も確保（将来のアクセス増への対応、他のAWSサービス連携の可能性）

■ 短納期（投資決裁がおりた後、3カ月で導入）により、
本当にやりたい基幹システムAPI 開発案件の増加、ニーズの喚起につながった

■ 維持保守フェーズに必要な要員リソースの削減

導入にあたってのコンセンサスづくり、関係者承認プロセスでの報告ポイント

- プロジェクト側でAWS設計に責任を持ち、関連部門の若手に参画してもらうこと
- 新技術採用に伴うリスクに対し、AWS 研修受講、外部技術支援を契約
- 既存設備と密な連携は避け、業界標準で疎結合につくる
(RESTful API、OIDCベースのトークン活用)

- サービスレベルアグリメント、可用性設計目標が要件を満たしていること
- クラウドネイティブで構築することのメリットを既存セキュリティポリシーと比較
セキュリティ部門との協力体制を構築していること

サーバーレス利用の実情

「開発体制や進め方に不安がある」「社内にエンジニアがいない」問題の軽減のために

■ トップダウンでのプロジェクト化と専任メンバー確保、外部支援を含む体制構築

・ 初期メンバーのスキルセット：

AWS経験者 1 名がPM、PoC期間にメンバーのトレーニングを実施

経験者がハンズオン手順を作成、メンバーによる手順の再現と疑問の解消、実機への投入

(サーバーレス型だと費用も押さえた反復トレーニングが可能、日本語のブログ情報も多い)

■ プロジェクトメンバーへのAWSトレーニング

・ 一括発注 (Architecting on AWS、Developing Serverless Solutions on AWS コース等)

■ 技術交流会を通じて、運用イメージ固める

サーバーレス利用プロジェクトで変わること、変わらないこと

変わること

- アプリ部門主導でAWS のコントロールが可能
- サーバー、仮想マシンのメンテナンス（セキュリティパッチ等）の負荷軽減
- スモールスタートで必要な部分のみの調達がしやすい

変わらないこと

- 開発、運用の分離（アプリ部門が本番環境を気楽にさわられるようにしない）
- 障害の基本的な運用は変わらない（障害切り分け、異常に気づける仕組みづくり）
- ドキュメントは整備する（運用部門への移管を見据えて）
- テスト自動化、CI/CD の検討（プロセスを取捨選択し、自動化対象決定）

サーバーレス利用プロジェクトで工夫が必要だったこと

- 既存資産への変更や移行を最小化
疎結合となる配置重視して、複雑なサービスの組み合わせにならないようにする
- ベンダーロックにならぬよう利用機能のドキュメントを読み込む（上手く肩に乗る）
- 製品の制約（タイムアウト値 29秒 等）の基幹システム側仕様とのすり合わせ
- API ポータル公開については、OSS 製品（Stoplight Studio/Prism）を利用

今後に向けて

今後に向けて

オリックスグループ向けAPI コミュニティの拡充

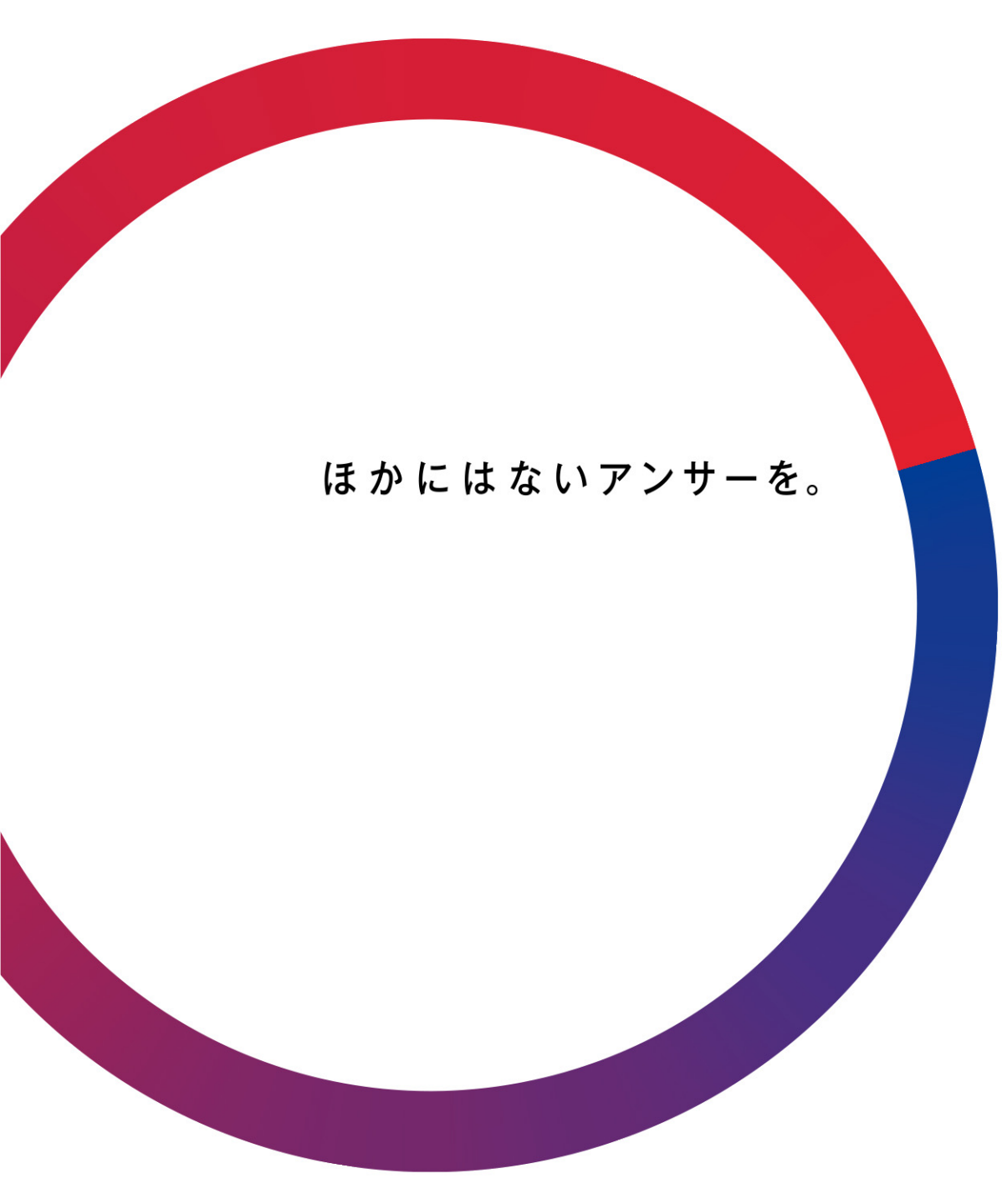
- API Gateway を経由すれば、さまざまなAPI にセキュアにアクセスできる
- オリックスだけでなく、グループ会社へのAPI 公開を推進する
- API 開発ガイドラインの整備・定着と横展開

AWS への期待

- ガートナーMQ レポートの、AWS API 製品ビジョンに関する評価が低いため、
もっと製品の将来像を語ってもいいのではないか？（実行力は高いという評価）
※今回は、ビジョンの評価の高い製品の考え方を学びつつ、それがAWS でもできることを確認する流れでもあった
- セキュリティ強化（相互TLS対応範囲拡大、API 不正利用検知、API 認証認可支援等）
- API デザイン機能提供（yaml の可読性アップ、API 定義のデプロイ支援等）

最後に

- ユーザーニーズをクラウドネイティブに実現するにあたって、サーバーレス技術はユーザーにとって強い武器になります。
- AWS コミュニティには、活発さだけでなく、法人/個人、世代をまたいだ交流があります。今後も、コミュニティへの貢献をしていきたいと思えます。
- オリックス・システムでは、一緒に働けるエンジニアを募集しています。ご興味をお持ちの方はぜひご連絡ください。
<https://www.orix.co.jp/system/recruit/>

A large, thick circular graphic on the left side of the page, composed of three segments: red at the top, blue on the right, and purple at the bottom.

ほかにはないアンサーを。

オリックス・システム株式会社

〒104-0053 東京都中央区晴海1-8-11

晴海アイランド トリトンスクエア オフィスタワーY棟

TEL:03-5144-0700 (代表)