WHITE PAPER | 2016 年 12 月

企業ユーザにとって最適な API 管理ソリューションの選択

ca technologies

API のビジネス・チャンス

アプリケーション・プログラミング・インタフェース（API）の概念自体は新しいものではありませんが、モバイルやクラウドへの対応のために情報アセットを社外開発者に公開する企業が増える中、APIも変革に直面しています。API を通じて開発者にデータを公開することで、eBay、Expedia、Salesforce などの企業は新しい市場でのセールスを成功させています。ProgrammableWeb.com によると、インターネット上で公開されているオープン API の数は、2005 年にはわずか 32 件でしたが、現在では 16,000 件を超えています。[1]

外部の開発者に API を公開すれば、公開した企業の中核となるデータやアプリケーション・リソースに関係する開発者コミュニティが成長し、テクノロジの新規事業の基盤になります。これは、新しい市場（Twitter の急成長など）、収益（Salesforce.com の AppExchange など）、またはエンドユーザの維持（Facebook など）にもつながります。

API を使用して社外開発者と情報や機能を共有しているのは、テクノロジの新規事業だけではありません。クラウド、モバイル、パートナーとの統合のイニシアチブにより、さらに多くの企業が API を使用して開発者エコシステムを実現しています。また、それにより、情報アセットに関連した新しい市場と収益源の開拓、およびエンドユーザの維持を推進しています。ただし、多くの新規事業とは異なり、大手企業は評判や規制を含め、多くのリスクにさらされ、顧客、パートナー、社員、株主のそれぞれのニーズへの対応も求められるため、API の公開には十分注意する必要があります。

企業における API 管理の課題

企業が社外開発者コミュニティに API を公開すると、公開先がパートナーの場合でも一般の場合でも、さまざまな課題やリスクに直面します。公開する情報資産を不正使用や攻撃からどのように保護するか、どうすれば API ユーザに影響を及ぼすようなダウンタイムのない、信頼性の高いサービスとして API を提供できるか、どうすればポリシーに基づいた一貫した方法で API のアクセスや使用を管理できるか、API でどのように収益を得るか、開発者が API を検出して各自のアクセスを管理できるようにするにはどうするかなど、こうした課題は新興企業にも既存の大手企業にも共通するものですが、大手企業の IT 組織では深刻度や緊急度がより高くなります。API 管理戦略を急いだために信用を失ってしまうことになれば、大手企業にとって大きな痛手になります。また、大手企業は計画的な IT プロセスと保護の維持も求められます。

そのため、公開する API のタイプに関係なく、大手企業には以下のような基本機能に対応できる API 管理ソリューションが必要です。

- **API のセキュリティ** — API で公開した情報とアプリケーション・リソースの悪用や不正使用を防止します。
- **API のライフサイクル管理** — API のアップグレード時やバージョン更新時、または環境、場所、データセンタ、クラウドなどの移行時に API の更新が中断しないようにします。
- **API のガバナンス** — 測定、SLA、可用性、性能などのポリシーを利用して、さまざまなパートナーや開発者に API を公開する多様な運用特性を制御および追跡します。
- **デプロイの柔軟性** — API 管理ソリューションを企業の既存のインフラストラクチャに統合します。
- **開発者のイネーブルメントとコミュニティの構築** — 開発者の関与を促し、公開した API を開発者が最大限に活用するよう管理および支援します。
- **API の収益化** — API を公開するだけでは十分でない企業もあります。API は新たな収益の機会ももたらし、さまざまな API 管理ソリューションによってさまざまなレベルの収益化が可能になります。

企業にとって、これらの機能要件に対応することは不可欠です。また、これらの機能要件に加え、API 管理ソリューションによって、独自の IT エクスペリエンスに必要な運用特性が提供されることも重要です。

- **ソリューションのセキュリティ** — API 管理ソリューションを「DMZ（非武装地帯）」にデプロイする場合、侵入に対する保護から PCI コンプライアンス、FIPS、HSM 対応に至るまで、API キーの幅広いセキュリティ要件を満たす、強力な IT クラスの API ソリューションも必要です。
- **ソリューションの管理性** — 企業は異なる地域やデータセンタ、クラウドに開発環境、テスト環境および本番環境を構築しています。そのため、API 管理ソリューションはそれぞれに固有の開発スタイルやプロセスに適応する必要があります。
- **ソリューションの信頼性** —API をビジネスとして公開している企業は、稼働時間が 99.999% になることを期待し、停止することは受け入れられません。可用性に優れた堅牢なソリューションには、どのような特徴があるでしょうか。

このホワイト・ペーパーでは、これらのさまざまな機能要件と運用要件について説明し、API 管理ソリューションを選択する上で重要な情報を IT マネージャ、Web 管理者、企業のアーキテクトに提供します。

API 管理ソリューションの機能要件

API のセキュリティ

API 管理ソリューションのデプロイを検討している企業は、セキュリティ機能を最も重視します。特に、SOAP、REST、JSON などの標準に依存しない API で重要な情報を公開する場合、この傾向は顕著です。API のセキュリティでは、まず、アクセス制御を考慮する必要があります。つまり、API を社外に公開するためには、以下の機能を備えている必要があります。

- 認証におけるさまざまな種類のクレデンシャルの使用
- 開発者に対するさまざまな種類のクレデンシャルの発行
- OAuth、OpenID Connect、SAML などの連携型のスキームを含め、さまざまなリソース権限認証スキームのサポート

企業にとっては既存のアイデンティティ・インフラストラクチャと統合する必要があることから、この課題はさらに複雑になっています。そのため、柔軟性と統合の両方を達成することが最重要目標です。まず、ポリシーでさまざまな種類のアクセス・トークンをサポートし、コードを修正せずに、開発者の API キーを別の API キーに移行できるようにします。また、ソリューションは、モバイル・セキュリティと API の標準である OAuth のさまざまなスキームをサポートするだけでなく、HMAC（メッセージ認証のための鍵付ハッシング）などのさまざまな OAuth 形式や、SAML（セキュリティ・アサーション・マークアップ・ランゲージ）などの企業標準との組み合わせにも対応する必要があります。もちろん、API 管理ソリューションが CA、IBM、Oracle、RSA などの企業の既存のアイデンティティ投資と連携して動作することも必要になります。

API のセキュリティはアクセス制御だけではありません。API ではデータを表示するプログラムのウィンドウが提供されます。そのため、企業レベルの API 管理ソリューションでは、どのデータを公開するのか、情報の機密性をどのように維持するのか、また、インターセプトや改ざんから転送をどのように保護するのかを、企業のアーキテクトやセキュリティ管理者がきめ細かく制御できる必要があります。

また、API のセキュリティは、API と API で公開するデータ / 機能の両方の完全性に依存するため、攻撃、DoS または不正使用による API の侵害を防止することも重要です。優れた API 管理ソリューションは、API の可用性と忠実性、および API が実現するコミュニケーションを保証するため、さまざまな脅威保護制御の機能を備えています。

API のライフサイクル管理

API はすぐに構築できるものではありません。アプリケーションの機能と同様に、設計からコーディング、テスト、デプロイに至るまで、API にも独自の開発ライフサイクルが必要です。そのためには、開発プロセスで使用する手法がウォーターフォールであってもアジャイルであっても、その開発ライフサイクル全体で API の変更を追跡する必要があります。このようなことから、すべての API 管理ソリューションには、以下の目的で完全に機能するワークフローが必要になります。

- 業界標準を使用した API の計画と設計
- エンドツーエンドの API の統合とセキュリティ
- バージョニングとロールバックのテスト、展開および対応
- レポートと分析を含む API の利用の管理と監視

完全な機能を備えた API 管理ソリューションなら、本番環境内で複数のバージョンに同時に対応したり、旧バージョンのクライアントに対応できるほか、SOAP（Simple Object Access Protocol ）、REST（Representational State Transfer）、JSON（JavaScript® Object Notification）などのさまざまなアクセス・テクノロジにも対応できます。ローカライズ型の開発にのみ対応したライフサイクル管理フレームワークでは、最先端企業のニーズに応えることはできません。パブリック・クラウドとプライベート・クラウドは、いずれもますます重要になっています。そのため、API 管理ソリューションにはテストと本番の両方のクラウドに対応する機能に加え、ネットワークの独自性やトポロジの予測しない変更から API 開発者を隔離する機能も必要です。

API のガバナンス

ガバナンスは管理、プロセス、および可視性の幅広い要件を含む広範な用語で、API をコンシューマに公開するときの条件を定義します。ガバナンスにはセキュリティの概念とライフサイクルの概念が含まれますが、SLA、監視、およびレポートのさまざまな要件も明確に示されます。さらに、API 管理ソリューションの場合、ガバナンスはより広範な規則に相当し、アイデンティティ、機能、サブスクリプション・レベル、またはポリシーで定義可能な他のトランザクション・コンテキストに基づいて、API のデータと機能を共有するための差別化された条件がさまざまなコンシューマに適用されます。

効果的な API ガバナンスで一番重要なものは柔軟性です。API の共有方法を制御するテクノロジは、企業の優先事項やプロセスに対応させるのであって、その逆であってはなりません。そのためには、ポリシーを使用して、SLA、セキュリティ、ログ、またはその他の制御を構成できる API 管理ソリューションが必要です。ポリシーは柔軟性の要であり、実装間での一貫性を確保します。完全なポリシー IDE が提供されないために、管理者がおおまかな制御しかできない API 管理ソリューションでは、管理対象と管理方法も限られてしまいます。

デプロイの柔軟性

多くの企業には、ビジネスを補完するために設計された既存のインフラストラクチャがあります。API 管理ソリューションに移行する前に、既存の環境で使用するソリューションを評価する必要があります。アーキテクチャ・チームは、別の環境としてではなく、インフラストラクチャの延長としてこのソリューションを管理します。このレベルの統合の詳細については、ソリューションの概要を説明した「An Architect’s Guide for Extending Your ESB/SOA Environment to Mobile, Cloud, and IoT」をご覧ください。

開発者のイネーブルメントとコミュニティの構築

API を管理すると、発行元の企業には一貫性のある制御が保証されますが、外部開発者が API を簡単に検出して使用できなければ、使用されないリスクがあります。そのため、最新の API 管理ソリューションでは、セキュリティ、ライフサイクル、ガバナンスなどの制御機能だけでなく、発行元の企業が API に関する情報を社外開発者に公開するのに役立つ機能も提供されます。この機能は多くの場合、開発者ポータルを使用して提供されます。このポータルによって、開発者はアカウントの登録、API アクセス・キーの要求、使用可能な API の検出、サンプル・コードの参照などの操作を一か所で行うことができます。

企業の使用を重視した API 開発者ポータルでは、以下に対応している必要があります。

- 容易に使用できるモバイル API の提供（OAuth と OpenID Connect を含む）
- オペレーター向けのレポート作成と分析機能の提供
- ビジネス関係管理の簡略化

API を公開する際の操作性や優先順位は企業によって異なるため、すべてに対応できる API ポータル・アプローチは、すべてに対応できる API セキュリティ・ライフサイクルやガバナンス・フレームワークと同様に、それほど魅力的なものではありません。そのため、多くの企業は、区分け利用可能な API ポータルを検討します。これには、特定の開発者エンゲージメント戦略に合わせてカスタマイズできるホワイトレーベルのポータル、または、既存のエンタープライズ開発者ポータルで別のコンポーネントとして使用する API ポータルなどがあります。ここでも、柔軟性が非常に重要となります。

API の収益化

収益化の考え方は、開発者のイネーブルメントの考え方に関係します。多くの企業は、Web API とモバイル API に自由にアクセスできるようにすることで、利用を促進したいと考えていますが、さらに高レベルのアクセスを実現する、従量課金オプションを提供したいと考えている企業もあります。収益化の課題に対処する方法は 1 つだけではありません。以下のような方法もあります。

- データ転送やクライアント要求が一定のしきい値を下回る場合は使用が無償になる、「フリーミアム」モデルを提供する
- 一定レベルのサービス保証を行ったり無償ユーザよりも優先することで課金する
- 無償ユーザには提供されない、特別な情報や機能を提供する

選択するアプローチに関係なく、企業が柔軟に収益基準を設定できるよう、API 管理ソリューションが十分に高度なものである必要があります。また、以下も重要です。

- 幅広い使用統計情報を取得して、使用量を測定するための基礎を構築する
- 高度な SLA 機能と Class of Service 機能を提供し、トラフィックに優先順位を設定する
- 支払いを行う顧客向けに単独利用することが可能で、いかなるコーディングも必要としない支払い専用 API を作成する

API 管理ソリューションの運用要件

ソリューションのセキュリティ

API 管理ソリューションは通常、企業の API を社外から分離するテクノロジの一部に過ぎないため、ソリューションが API に提供するセキュリティのレベルはソリューション自体のセキュリティと同程度の強度でしかありません。ソリューションのセキュリティが侵害されると、API に提供されているセキュリティも侵害されます。そのため、API 管理ソリューションを検討する企業では、ソリューションのセキュリティを重点的に考慮する必要があります。

これらのソリューションは社外と社内 API の仲介として機能するため、通常はまず、ソリューション自体のセキュリティが侵害される可能性がないかを評価します。これは、ソリューションに対してどのような侵入テストが行われているのか、ソリューションへのアクセスがどの程度制限されるのか、および主な脆弱性検出に対応しているかどうかに基づきます。STIG（セキュリティ技術実装ガイド）テスト・ソリューション、クレジット・カード情報の受け渡しを行うソリューション向けの PCI DSS（PCI データ・セキュリティ・スタンダード）認定、およびさらに高度な政府セキュリティ標準への対応が必要なソリューション向けの FIPS（連邦情報処理標準）準拠と Common Criteria 認定を考慮する必要があります。

実用的な目的で、社内 API に対する社外要求を仲介するプロキシベースの API 管理ソリューションについて検討する企業もあります。仲介ベースの API ゲートウェイには、制御と分離のインライン・ポイントが明確になるという利点があり、セキュリティの認定と管理がさらに簡略化（ネットワークのファイアウォールと同様）されます。また、API キーを暗号化するために、オンボード HSM（ハードウェア・セキュリティ・モジュール）をサポートするソリューションもあります。多くのシナリオでは、API キーは不正使用を防ぐ主要な認証機能であるため、暗号化を使用して API キーを盗取から保護することは的鉄な戦略です。

ソリューションの管理性

単一の Amazon インスタンスや小規模なホスティング・プロバイダを利用して本番の Web サイトを運営している典型的な新興企業と異なり、通常、大手企業には以下のようなさまざまな開発環境と本番環境があります。

- 地理的に分散された開発者チーム
- 世界各地のデータセンタにまたがる本番環境
- クラウドベースの災害復旧システム

そのため、選択の意思決定を行う上で管理性は重要です。API ゲートウェイのクラスタを管理する方法、地理的に離れた状態で負荷分散を実行する方法、完全自動のデータセンタ環境を運用する方法、ピーク負荷を処理する方法などは、他の機能よりも優先して考慮します。すべての API 管理ソリューションが特定の企業ニーズに対応するように設計されているわけではないため、特定のソリューションを導入する前に、それぞれのソリューションがクラスタ管理、フェイルオーバ、負荷分散、災害復旧、その他の運用管理機能にどのように対応しているのかを慎重に評価する必要があります。

ソリューションの信頼性

API 公開プログラムの実施を決定した企業は、API 利用者に対して事実上サービス・プロバイダとなるため、API 利用者の信頼と継続的なアップタイムに対する期待に応える必要があります。そのため、API 管理ソリューションを選択する際には信頼性が極めて重要になります。そのような企業には、冗長性を備え、ダウンタイムのリスクがゼロではないとしても極めて低いソリューションが必要です。API 管理ソリューションを検討する際には、以下を確認します。

- オンプレミス、クラウド、またはハイブリッド・ソリューション（オンプレミスの API ゲートウェイ、クラウドの開発者ポータル）でのデプロイに対応している
- デプロイ・モデルに関係なく完全な冗長性が提供される
- 既存のセキュリティインフラストラクチャと統合できる
- セキュリティ要件に対応している

まとめ

企業によってニーズや環境は異なるため、1 つの API 管理ソリューションですべてに対応することはできません。ただし、どの企業でも、優れた機能と運用に対するニーズは共通しています。API の社外公開の準備を進めている多くの企業の場合、電話局クラスのサービス・プロバイダの厳しい本番環境に対応できる柔軟性の高い、ポリシーベースの API 管理ソリューションが必要です。そのような API 管理ソリューションは、機能面では、さまざまなセキュリティの前提条件と共通の開発ライフサイクルに対応し、ポリシー管理、開発者のオンボーディングおよび開発者エンゲージメントを可能にし、収益化のオプションをサポートする必要があります。運用面では、優れたセキュリティ、管理性、信頼性を備えている必要があります。

独立した調査を活用した API 管理ソリューションの選択

大手分析会社の中には、API 管理技術を調査して、企業がデジタル戦略に最適なソリューションを選択するのに役立つベンダーの比較レポートを発行している会社があります。また、IT Central Station などの IT レビュー・サイトは、ベンダー比較や顧客レビューの優れた情報源になります。

大手分析会社が提供している無料の比較レポートで、CA API Management に対する顧客の意見をご覧ください。Web サイト：**https://www.ca.com/jp/products/api-management.html**

CA Technologies の連絡先

CA Technologies では、質問やコメント、一般的なフィードバックを歓迎しています。

詳細については、**ca.com/jp/api** をご覧ください。

ca.com/jp/でCA Technologiesにアクセスしてください

CA Technologies（NASDAQ：CA）は、企業の変革を推進するソフトウェアを作成し、アプリケーション・エコノミーにおいて企業がビジネス・チャンスを獲得できるよう支援します。ソフトウェアはあらゆる業界であらゆるビジネスの中核を担っています。プランニングから開発、管理、セキュリティまで、CA は世界中の企業と協力し、モバイル、プライベート・クラウドやパブリック・クラウド、分散環境、メインフレーム環境にわたって、人々の生活やビジネス、コミュニケーションの方法に変化をもたらしています。詳細については **ca.com/jp** をご覧ください。

1 ProgrammableWeb API Directory、2016 年 12 月、www.programmableweb.com/apis/directory

CS200-241661_1216