

APIのパフォーマンス、信頼性、セキュリティの課題を解決する



APIがモバイルアプリケーション、ウェブサイト、シングルページアプリケーション、データ共有のために利用される事例はますます増えています。APIはビジネスとテクノロジーの境界を超えた接続を可能にします。つまり、すべての企業にとってAPIを開発、提供、使用すべき十分な理由があるということです。APIによりハードウェアとソフトウェアの新たな組み合わせが可能になり、それによって製品とサービスの提供方法が一変することもあります。このようにAPIの利用は急増しているため、インフラストラクチャの拡張に対する要求、ユーザー体験、セキュリティ、信頼性、レイテンシーなどを適切に考慮せずAPIが作成されている場合、企業は波及する影響に対処せざるを得なくなっています。

既存のAPIや将来のAPIを見直す際に、企業はどのように自問すべきでしょうか。

APIのレイテンシーの問題の影響を定量化したか？

多くのウェブサイト、あらゆるネイティブアプリ、一部のシングルページアプリでAPIコールが利用されています。ユーザー、特にモバイルユーザーが高いパフォーマンスを期待していることは分かっています。しかし、エンドユーザーがリクエストする情報の収集に100以上のAPIコールが使用されることは珍しくなく、ネットワークのレイテンシーによってこれらのうち1つでも遅れると、コンテンツが読み込まれないことになりかねません。

幸いなことに、以下のようなウェブサイトのパフォーマンスに関する課題を解決するために長年利用されている様々な手法がAPIのために役立ちます。

- **キャッシュ:** APIは、通常はキャッシュ可能なコンテンツとキャッシュできないコンテンツが混在するXMLデータまたはJSONデータを送信します。キャッシュは「軽量」トラフィックとみなされることが多いためAPIの開発プロセスでは見落とされがちですが、実際のところ、コンテンツをキャッシュすると、応答速度の向上とAPIオリジンでのトラフィックのオフロードに役立ち、ユーザー体験が向上します。
- **圧縮:** LMA圧縮をJSONやXMLのペイロードに適用すると、必要となるバイト数が大幅に減少する場合があります。バイト数が少なくなれば、特に帯域幅が限られている場合にはAPIのセキュリティとパフォーマンスが向上します。
- **エッジにおけるTLSターミネーション:** コンテンツがセキュアであれば、APIオリジンではなくインターネットのエッジにおいてTLSハンドシェイクをネゴシエートすることが可能であり、これにより必要なラウンドトリップ数が減ります。

APIの利用対象:

- ネイティブ・モバイル・アプリ
- APIコールによってコアページを繰り返し取得するシングルページアプリ
- ウェブサイトの検索ボックスでの先行入力による検索結果表示
- 製品の消費を促進するベンダーAPI
- ウェブサイトでの検索結果表示
- 価格または在庫の検索
- 製品詳細のフェッチ
- サプライヤー、パートナー、顧客のB2B統合
- API自体が製品である場合
- 政府のオープンデータ共有
- IoT製品
- リアルタイムコンテンツ/データのシンジケートと配信

APIを常時利用できないことはビジネスにとって何を意味するのか？

APIは、収益を生み出す重要なアプリケーションにおいて、リソース間の橋渡し役を果たします。オンデマンド交通モバイルアプリ、リアルタイム・ナビゲーション・システム、サプライ・チェーン・ソフトウェアで利用されるAPIを考えてみてください。これらは、リアルタイムでの輸送の最適化や空港の大きなボードでフライト出発時刻の更新を行っています。このような情報のフローは途切れることがあってはならず、APIは常時利用可能であることが不可欠です。

多くの企業は、一定しない可用性への対処を目的として、多様な地域に存在するデータセンターやクラウドプロバイダーを利用し、そのAPIインフラストラクチャ、冗長ネットワークアーキテクチャやコンポーネントをホスティングしています。ただし、従来のハードウェアによるロードバランシングアプライアンスだけでは不十分です。また、データセンターやクラウドベンダーでは想定外のダウンタイムイベントが発生することがあり、エンドユーザーがアプリケーションにアクセスできないという悪影響が生じる可能性があります。可用性を保証するためにできることは以下のとおりです。

- サードパーティをAPIの供給元とし、分散した保護階層として活用する
- APIリクエストをAPIオリジンのインフラストラクチャからオフロードする
- サードパーティサービスを利用して、可用性、パフォーマンス、地理的な場所などに基づいて複数のAPIオリジン(自社のデータセンターまたはクラウドプロバイダーのいずれか)にルーティングして、エラーやメンテナンス時における配信を管理する

自社のAPIインフラストラクチャはトラフィック急増に対してどのような準備を行っているか？

あらゆるオリジンと同様に、APIサーバーは提供するデータのピーク需要に対応できるように構築されていなければなりません。多くのAPIでは、ウェブトラフィックと同じように急増が発生することがあり、予測できないトラフィックのパターンにさらされます。予想されるピ

ーク需要に合わせてオーバードプロビジョニングすることはコストのかかる方法です。これは、パブリック・クラウド・インフラストラクチャを使用したとしても同様です。APIデータを利用するためにパートナーやサードパーティが想定外の新規チャンネルを開くため、APIトラフィックの予測は特に難しくなっています。サーバーがAPIリクエストにより過負荷状態になると、応答に遅延が発生するか、応答がすべて失われます。

企業は、このようなAPIの課題を克服するため、ピークトラフィックに対応できるよう自動的に拡張し、セキュリティ上の脅威を検出して回避するソリューションを求めています。

使用しているAPIに対応するセキュリティスタックをどのように設計すべきか？

Webサーバーとまったく同様に、APIエンドポイントはハッカーやボットの攻撃のリスクにさらされています。悪意のある攻撃に加えて、パブリッシャーが作成する際に想定していた使用事例に当てはまらないコードにより偶発的にAPIが誤用され、意図しないDDoS攻撃を発生させてしまうこともあります。

APIの脆弱性を理解することは、解決策の第一歩に過ぎません。APIのセキュリティ管理方法には様々なアプローチがありますが、多くの企業が包括的な戦略を持たないことによって自社を危険にさらしています。

したがって、真の多層防御戦略を導入すべきなのです。すなわち、APIの利用方法を定義するポジティブ・セキュリティ・モデル、APIエンドポイントをレイヤー7のウェブアプリケーションの脆弱性から保護するネガティブ・セキュリティ・モデル、API固有のレポートイングによるエンドユーザーと利用可能なAPIとの間のインタラクションの可視化の向上です。

このような戦略を導入すれば、パフォーマンスに影響を与えることなく、データの安全性とAPIインフラストラクチャの過負荷防止を実現できます。

API に関する課題の克服

コンテンツ・デリバリー・ネットワーク (CDN) がウェブサイトやウェブアプリケーションの場合と同様に API の配信でもいかに役立つかを考慮している企業はほとんどありませんでした。Akamai はコンテンツ・デリバリー・ネットワーク (CDN) サービスのグローバルリーダーとして、最も浸透し高度に分散した CDN プラットフォームを展開しており、世界の 120 以上の国、1,500 以上のネットワークで数十万台のサーバーが稼働しています。これは、Akamai をご利用いただければ、以下のことが可能だということです。

- リアルタイムのインテリジェンスに基づく適応インターネットルーティングを用いて API のレイテンシーに対処する
- キャッシュサービスを使用することでパフォーマンスを向上させ、オリジンの負荷を軽減し、他のどの CDN よりも API の応答をエンドユーザーに近づけるとともに、クライアントの近くで TLS のターミネーションを行う
- 正当なトラフィック (コントロール対象)、またはセキュリティ上の問題 (ブロック対象) のいずれに關しても、トラフィックの急増時における API レート制限の問題を解決する
- WAF レート制限を活用することにより DDoS 攻撃をブロックする
- エラー時またはメンテナンス時にはデータセンターを瞬時かつ自動的に切り替える。また、可用性、パフォーマンス、地理的な場所に基づいてクラウドプロバイダーの複数のデータセンターにルーティングする (Application Load Balancer Cloudlet を使用すればこれ以上の対応が可能)

- API Prioritization Cloudlet の使用により、API 需要のピーク時の管理とオーバーフロー時のリクエストの管理を支援する
- China CDN を利用してコンテンツを中国内の Akamai のネットワークから配信することにより、中国から発着信するコールの遅延を緩和し、レイテンシーを大幅に低減する
- Akamai の Bot Manager を利用することにより、ボットに関連する高トラフィックの API アクティビティを抑制する
- Akamai の Access Control Cloudlet を使用して、地域、デバイスの種類、その他多数のベクトルに基づいてリクエストを制限する

API の使用を継続的に拡大してデジタル企業を運営する場合には、多くの企業が経験してきた可用性、ユーザー体験、セキュリティ、レイテンシー、拡張性の問題が API プロジェクトに影響する前に対応してください。

Akamai による API に関する問題解決の支援の詳細については、[Akamai の API に関するページ](#)を参照してください。



コンテンツ・デリバリー・ネットワーク (CDN) サービスのグローバルリーダーとして、Akamai は、インターネットを高速、安全、信頼できるものとしてお客様がご利用いただけるようにします。Akamai の先進的なウェブパフォーマンス、モバイルパフォーマンス、クラウドセキュリティおよびメディアデリバリーの各ソリューションは、デバイスと場所を問わず、コンシューマー体験、エンタープライズ体験、およびエンターテインメント体験を企業が最適化する方法を大きく変化させています。Akamai のソリューションとそのインターネット専門家チームが、企業のより速い進歩にいかに関与しているかについて、www.akamai.com/jp/ja/ または blogs.akamai.com/jp/ および Twitter の [@Akamai_jp](https://twitter.com/Akamai_jp) で詳細をご紹介します。

Akamai は、米国マサチューセッツ州ケンブリッジを本拠地として、世界中に 57 を超える拠点を展開しています。Akamai のサービスや質の高いカスタマーケアは、世界中のお客様に比類のないインターネット体験を提供する企業を支援することを目的としています。全事業所の住所、電話番号、および連絡先情報は、<https://www.akamai.com/jp/ja/locations.jsp> に記載されています。