Akamai パートナー事例

Akamai とサイオステクノロジーとのパートナーシップで実現するAPIエコノミー時代のDX推進支援

APIプラットフォームを熟知したソリューションプロバイダーが Akamai API Security を活用して、APIエコノミー拡大に伴いより高度化、複雑化したセキュリティ課題の解消を後押し

信頼できるパートナーの獲得

エンタープライズサービスが求めるサポート

AIで異常を検知し攻撃や悪用を即座に阻止

APIの前線で10年にわたり知見を蓄積

サイオステクノロジー株式会社は、オープンソースソフトウェアを活用したシステム開発を原点とし、自社開発ソフトウェアおよびSaaSの販売とサービス、システムインテグレーションを行っている企業です。Web API（以下 API）についてはプラットフォームの設計、開発、運用、それに付随する周辺ソリューションを含めて、ワンストップで提供するサービスを展開しています。これまで約10年にわたり、金融、情報通信、製造業といった業界を中心に、大規模なAPIプラットフォーム開発を手がけてきました。

サイオステクノロジー　執行役員　APIソリューションSLヘッドの二瓶司氏は、「APIソリューション事業を開始した10年前、APIはあまり認知されていませんでした。しかし現在では、日本のシステム開発・運用において非常に一般的になりました。数年前まで数百本のAPIを並べることが大規模とされていましたが、現在では数千本クラスの実装が当たり前になっています」と振り返ります。その上で、APIエコノミーの拡大背景について、需要（サービス利用者）サイドと供給サイドの両面から次のように分析しています。

「いま日本では、シェアリングエコノミーやIoT、AI利活用に代表されるコネクテッドサービスのニーズが増大しています。アプリケーションを、スクラッチで全て自社開発するという思想の企業は少なくなり、APIというシステムやデータの連結器ありきのサービス開発が

SIOS

所在地

日本
api-ecosystem.sios.jp/

業種

Software and SaaS

ソリューション

- API Security

Akamai

大前提となっています。また、XaaS（Everything as a Service）型サービスの急増に伴い、サービス同士を連携させる必要性が高まっています」（二瓶氏）

APIでサービスを繋ぐことで、昨日までの競合が今日のパートナーになるなど、競争環境は劇的に変化します。API連携は容易に付加価値を生み出せるため、この流れに乗り遅れることは即座にビジネス上のリスクに繋がります。また、サービス開発のあり方も変化しました。かつてのように百発百中を狙うのではなく、多くのサービスを生み出し、市場の反応を見ながら取捨選択していく「多産多死型」の開発スタイルが主流となり、その俊敏性を支える技術としてAPIが不可欠になっています。

APIによってセキュリティ課題が複雑化

APIエコノミーの拡大に伴い複雑化した課題を、二瓶氏は3つの観点で整理します。

「まず、ネットワーク上に幾何級数的に結節点が増えることでセキュリティの脆弱なポイントが増加します。次に、マイクロサービス化によりデータの流れの可視化が困難になります。そして、情報とお金の流れが複雑化することでマネタイゼーションの管理が難しくなります」（二瓶氏）

特に深刻だと指摘するのが、リテラシーの異なるさまざまなプレーヤーがAPIエコノミーに参加することによるセキュリティの低下です。「レベルの低いプレーヤーが参加すると、どうしてもそこが狙われやすくなり、非常に脆弱なネットワークができてしまいます。これが『蟻の一穴』となって、そこからデータを抜かれたり、ハッカーを中心とした悪意のあるプレーヤーが入ってきたりするのです」と二瓶氏は警鐘を鳴らします。

さらに、今日のAPIの実装では、従来のセキュリティサービスや認証・認可の基盤サービスを、世界共通で1つ組み込むだけでは対応しきれません。地域間の差分（GDPRなど）とユースケースの多様化により、APIセキュリティに求められる要件は複雑化の一途をたどっています。

包括的なセキュリティ実現する Akamai API Security

こうした背景から、サイオステクノロジーは Akamai API Security を自社の取り扱うソリューションポートフォリオに加えました。二瓶氏は、Akamai がユースケースに応じて細かくレベル設定できる権限管理機能を備えている点を、エンタープライズクラスサービスにおいて重要だと説明しています。さらに、24時間365日のエンタープライズサポート体制はミッションクリティカルな仕組みの構築に不可欠であり、名ばかりのサポートも多い中で、Akamai　の体制は金融機関を主要顧客に持つ立場から見ても非常に信頼できると述べています。

Akamai API Security は、APIの開発・運用・更新のライフサイクル全体を通じて包括的な保護を提供します。その機能の一例を挙げると、APIエンドポイントの探索機能により、設定やタイプ（RESTful、SOAPなど）を問わず、すべてのAPIを発見してインベントリを作成し、休眠APIやゾンビAPIも検知します。テスト機能では、OWASP API Security Top 10 に挙げられた脅威をシミュレートする200以上のテストを自動実行し、APIの本番環境への展開前に脆弱性を発見することもできます。検知・レスポンス（対処）機能では、AI（機械学習）をベースにした　APIごとの特性のプロファイルによる実装上の欠陥や考慮不足による潜在リスクを検出。AI によって APIごとに正規化されたアクセスから外れた異常なアクセスを検知すること、データ改ざん・漏えい、ポリシー違反、脆弱性を探り、データを連続的に読み出そうとする不審な行動などAPIに対して実際に行われている攻撃をリアルタイムで監視し、攻撃や悪用を即座に阻止することもできます。

> Akamai API Security をポートフォリオに加えたのは、ユースケースに応じて細かくレベル設定ができる権限管理機能を有しているからです。これは、エンタープライズサービスで非常に重視される点です。また、Akamai の24時間365日のエンタープライズサポート体制は、ミッションクリティカルな仕組みを構築する上で不可欠です。

– 二瓶 司 氏
サイオステクノロジー
執行役員
APIソリューションSLヘッド

これらの機能の価値について二瓶氏は、「API攻撃による被害は、データ損失のような直接的なものだけでなく、セキュリティを懸念するあまりAPIを活用した新たなビジネス上のチャレンジに躊躇してしまうことによって起きる機会損失、さらには広報・法務など間接部門を巻き込んだレピュテーション被害まで多岐にわたります。Akamai API Security によって、こうした被害を未然に防ぐことができます」と説明します。

「APIは単にデータや情報をつなぐだけでなく、APIというツールを媒介としたビジネスアライアンス、ビジネスパートナーシップそのものです。それを支えるインフラを Akamai と共に提供していきます」（二瓶氏）

SIOS

サイオステクノロジーは、Linuxに代表されるオープンソースソフトウェアを活用したシステムインテグレーションを原点とし、自社開発ソフトウェアおよびSaaSの販売とサービスを行っています。直近では、クラウドをはじめとするDXの技術領域に注力し、AIの活用支援や次世代を支える製品とサービスを提供しています。これからも革新的なソフトウェア技術を追求し、世界のIT産業に影響力のある存在となって価値を創造し、社会の発展に貢献してまいります。
詳細情報は、https://sios.jp をご覧ください。

Akamai

Akamai はオンラインビジネスの力となり、守るサイバーセキュリティおよびクラウドコンピューティング企業です。市場をリードするセキュリティソリューション、優れた脅威インテリジェンス、世界中の運用チームが、あらゆる場所で企業のデータとアプリケーションを多層防御により保護します。Akamai のフルスタック・クラウド・コンピューティング・ソリューションは、世界で最も分散化されたプラットフォームで優れたコストパフォーマンスを実現しています。安心してビジネスを展開できる業界トップクラスの信頼性、スケール、専門知識の提供により、Akamai は、グローバル企業の信頼を獲得しています。詳細については、akamai.com および akamai.com/blog をご覧いただくか、X や LinkedIn で Akamai Technologies をフォローしてください。

Akamai