

# Akamai と Apiiro による コードからランタイムまでのセキュリティ

API は最新のアプリケーションを強化し、イノベーションを推進し、シームレスなデジタル体験を実現します。しかし、API によって攻撃ベクトルも増加しており、API が適切に保護されていないければ組織は重大なリスクにさらされます。Akamai と Apiiro は、Akamai API Security と Apiiro のアプリケーション・セキュリティ・ポスチャ管理 (ASPM) プラットフォームを統合することで、この課題に対処するために協力してきました。この共同ソリューションは、コードからランタイムまで API を保護し、リスクを低減し、修復をシンプル化し、セキュリティを損なうことなくイノベーションを加速します。

API ベースのリスクを効果的に管理するには、可視性が不可欠です。重要なのは、脆弱性を迅速に特定して対応することです。つまり、問題が検知されたら、セキュリティチームは開発者と協力して、リスクの高い脆弱性をできるだけ早く修復する必要があります。しかし、ほとんどのソリューションは特定されたリスクをコード内のソースに結び付けることができず、セキュリティチームと開発者チームが奔走することになります。Akamai と Apiiro の統合により、エンドツーエンドでの可視性やコンテキストが提供され、こうした分断を克服できます。

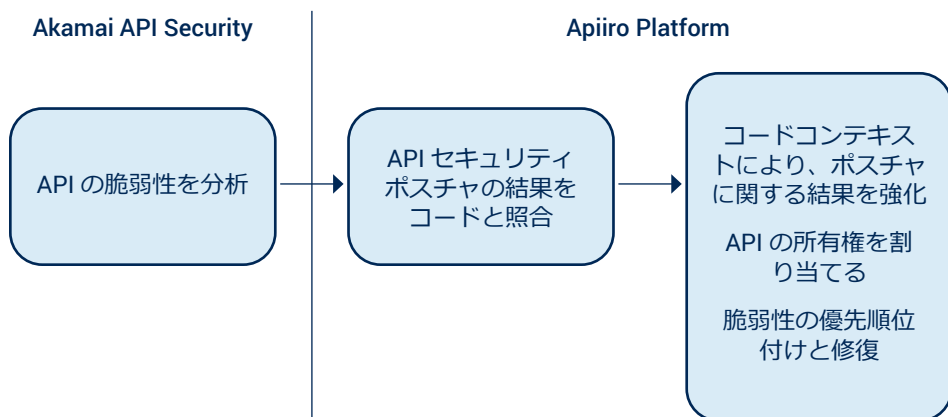
Akamai API Security は、トラフィックの API を検出し、攻撃につながる可能性のある設定ミスや脆弱性がないか API を分析します。それぞれの脆弱性について、開発者には、発生した原因、リスクの理由、問題の再現方法など、詳細な解説を提供します。この実用的な情報は Apiiro プラットフォームに渡されます。そのため、コードの詳細な分析を使用して、探索された API の包括的なインベントリが維持されます。Apiiro のプラットフォームは、Akamai が識別した API と脆弱性を既存の API ライブラリーと自動的に照合し、それぞれの脆弱性を、関連するリポジトリ、特定のコード行、責任あるコード所有者にマッピングします。

Akamai API Security が検知した API リスクに対し、このシームレスな統合技術を活用して、根本的な原因まで動的に追跡することができます。開発者は、脆弱性を迅速に修復するために必要なすべての情報を入手できるため、解決プロセスの速度と効率が共に向上します。さらに、このアプローチはセキュリティチームと開発チーム間のより良いコミュニケーションとコラボレーションを促進し、API セキュリティワークフローにおける重要なギャップを埋めます。

## ビジネス上のメリット

-  **可視性の向上**  
API 脆弱性コンテキストでコード分析を強化します。
-  **修復までの時間を短縮**  
API の脆弱性をソースコードに自動的にマッピングし、開発チームの所有者を割り当てます。
-  **リスクプロファイルの削減**  
API トラフィックをコードに関連付けることで脆弱性調査を合理化し、潜在的な影響に基づいて脆弱性に優先順位を付けます。

## 仕組み



## 主要なユースケース

- 自動化されたリスク評価：API と関連コードを継続的かつ包括的に分析し、リスクを特定します。
- リスク緩和の促進：API の脆弱性に優先順位を付け、それらをソースコードにマッピングし、所有者を割り当てて平均解決時間（MTTR）を短縮します。
- 稼働前のガードレール：セキュリティ対策を開発ワークフローに統合して、API の変更をプロアクティブに監視および管理します。

## 結論

Akamai と Apiiro の統合により、エンドツーエンドの可視性と実用的な知見を提供し、API セキュリティに対する独自のアプローチを提供します。この統合により、Apiiro をご利用のお客様は、コードからランタイムまで保護の範囲を拡大し、包括的な API セキュリティを確保することができます。Akamai のお客様は、コード内での API リスクの起源を特定し、適切なチームに割り当てることで、修復効率を高めることができます。Akamai と Apiiro は、複雑化する API 環境において、企業が安全かつ自信を持って革新を進められるよう支援します。

