

Akamai の API Security 製品、 PCI コンプライアンスへの準拠達成、顧客が大幅に増加 2023 年の提供開始以来、顧客の需要が 200% 以上増加

※本リリースは 2024 年 4 月 23 日（現地時間）マサチューセッツ州ケンブリッジで発表されたプレスリリースの抄訳版です。

オンラインライフの力となり、守るクラウド企業、[Akamai Technologies](#)（NASDAQ : AKAM）は、API Security 製品がクレジットカード業界のセキュリティ標準である Payment Card Industry Data Security Standard（PCI DSS）の最新バージョン（PCI DSS 4.0）のコンプライアンスに準拠を達成したことを発表しました。このプロセスの一環として、API に関連する特定の要件が追加されました。

[PCI DSS](#) は、クレジットカード情報を保存、処理、伝送する組織が効果的なセキュリティ対策を整えられるように考案された一連のセキュリティ標準です。API はカード所有者の機微な情報を処理し、決済処理を容易にするために使用できるため、PCI DSS コンプライアンスにおいて重要な役割を担います。PCI DSS はグローバルスタンダードであるため、今回の準拠は同様の慣行を実施するための先例ともなります。

また、Akamai は昨年 [Neosec](#) を買収して以降、[API Security](#) 製品に対する大きな需要が生じていると発表しました。顧客からの需要は、2023 年 8 月の提供開始以後、200% 以上増加しています。この強力なトレンドは、Akamai のプラットフォームから API アクティビティデータを簡単に取り込めるネイティブコネクタ機能が追加されたことが要因である可能性があります。この機能により、本番環境への導入が数分で完了し、検知結果に基づいて API Security が [App & API Protector](#) に指示を出して脅威を即座にブロックできるようになります。また、他社の WAAP および API ゲートウェイプラットフォームで展開するための統合も可能になります。さらに、Akamai API Security は他のツール（Apiiro の ASPM サービスなど）とシームレスに連携して、組織のシフトレフトを支援します。

API セキュリティの重要性は、Akamai の[最新の「インターネットの現状」レポート](#)の調査結果で明らかになりました。それによると、Web 攻撃の約 3 件に 1 件が API を標的にしたものでした。（国内のデータを引用したブログは[こちら](#)をご覧ください）

ホテルから小売までさまざまな業界のお客様が、Akamai の API Security の有効性、直感的な使用方法、リアルタイム監視機能を高く評価し、セキュリティ運用とユーザー体験の向上において大きな役割を果たしていることを強調しています。

Clal Insurance and Finance 社は保険および貯蓄の大手企業です。Clal の CTO である Haim Inger 氏は、イノベーションを促進するために API を活用しており、パフォーマンスと使いやすさの点から Akamai API Security を選択したと述べています。「何もしなくても API アセットの状態を把握できました。弊社の API に関するトークン化されたデータをインGESTした後、Akamai ソリューションは修正すべき点とその修正方法についての知見を自動的に提供してくれました」

その他にも、Gartner® Peer Insights™ では次のようなお客様のコメントが紹介されています。

- 「Akamai はリアルタイムの監視を提供し、潜在的なセキュリティインシデントを即座に可視化して、迅速な対応を可能にします。悪用を防止し、リソースの可用性を確保するために、レート制限メカニズムを使用して API の使用を効率的に制御できます」— [Salesforce の管理者 \(IT サービス業界\)](#)
- 「Akamai API Security Platform は、先進的なアプリケーションの API のセキュリティを確保するための、堅牢で使いやすいソリューションです。総合的な一連の機能と効果的な脅威緩和機能を備えているため、API セキュリティを重視する組織にとって価値ある投資となります」— [エンジニア \(小売業界\)](#)
- 「Akamai API Security は優れた機能を備えており、全体的なパフォーマンスとセキュリティが強化されています。また、既存のシステムやワークフローと簡単に統合できます。Akamai のソリューションはスケーリングできるよう設計されており、セキュリティを損なうことなく、成長中の企業の高まるニーズに対応します。また、業界の標準や規制を遵守し、安全でコンプライアンスに準拠した API 環境を確立します」— [上級自動化テストアナリスト \(IT サービス業界\)](#)

Akamai の Application Security 担当 Vice President 兼 General Manager である Rupesh Chokshi は「エンタープライズが事業にますます多くの API を使用するようになっていくのに伴って API セキュリティの重要性が高まり続けていることは、お客様の声から明らかです。PCI DSS に準拠した Akamai の API Security は、プラットフォームやゲートウェイの種類に関係なく API のふるまいを監視する機能を提供できるので、事業が円滑かつ安全に機能していることを確認できます」と、述べています。

組織がどのように API Security を使用し、継続的な探索と監視を通じて API 資産全体を完全に可視化しているのかを示すユースケースを確認したい場合は、[HiBob](#)、[EarnIn](#) (英語版のみ)、[Dan Hotels](#) のお客様事例をご覧ください。

Gartner® および Peer Insights™ は、Gartner, Inc. または関連会社、あるいはその両方の商標です。All rights reserved. Gartner Peer Insights の内容は、個々のエンドユーザーの主観的意見を集めたものであり、事実を表現したもので、ガートナーおよびその関連会社の見解を表すものではありません。ガートナーは、本コンテンツに掲載された特定のベンダーまたは製品、サービスを推奨するものではありません。また、明示または黙示を問わず、商品性や特定目的への適合性を含め、本コンテンツの正確性または完全性について一切の保証を行うものではありません。

Akamai Technologies について :

Akamai はオンラインライフの力となり、守っています。世界中のトップ企業が Akamai を選び、安全なデジタル



体験を構築して提供することで、毎日、いつでもどこでも、世界中の人々の人生をより豊かにしています。超分散型のエッジおよびクラウドプラットフォームである [Akamai Connected Cloud](#) は、アプリと体験をユーザーに近づけ、脅威を遠ざけます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、[akamai.com](#) および [akamai.com/blog](#) をご覧いただくか、[X](#) (旧 Twitter) と [LinkedIn](#) で Akamai Technologies をフォローしてください。

※Akamai と Akamai ロゴは、Akamai Technologies Inc.の商標または登録商標です

※その他、記載されている会社名ならびに組織名、ロゴ、サービス名は、各社の商標または登録商標です

※本プレスリリースの内容は、個別の事例に基づくものであり、個々の状況により変動しうるものです