AKAMAI ソリューション概要

グローバル規模のプラットフォームで生成されるインテリジェンスに基づく効果的なセキュリティ

グローバル規模、可視性、インテリジェンス

システムの出力品質は、そのシステムに入力された高品質データの量によって決まります。たとえば、AI ツールの出力品質は、そのツールを駆動する複雑なアルゴリズムによって決まり、CRM システムの出力品質は、そのシステムに保存された重要データによって決まります。サイバーセキュリティでは、このような高品質データを収集することが特に重要となります。Akamai は、比類のない規模を誇るプラットフォームを通じて、業界をリードする効果的なセキュリティソリューションを提供しています。グローバル規模の Akamai プラットフォームにより、グローバルなアクティビティを可視化して、データを実用的なインテリジェンスに変換し、複雑化する脅威から組織を保護します。

グローバルなリーチと分散

Akamai のプラットフォームは、世界中の 2,000 か所に分散しており、その対象範囲は他のプロバイダーの 10～100 倍に及びます。この広範なネットワークにより、貴社および貴社の顧客に近い場所からサービスが提供されるため、ビジネスのパフォーマンスと可用性を強化できます。また、分散型サービス妨害（DDoS）攻撃などのボリューム型攻撃を受けた際には、この規模が強力な防御メカニズムとして機能します。Akamai プラットフォームでは、トラフィックを複数の場所に分散できるため、攻撃の影響を緩和して、遅延を軽減し、運用を維持できます。さらに、このプラットフォームのメリットはセキュリティだけではありません。何兆通りものルートの組み合わせとインテリジェントなトラフィックルーティングにより、ユーザー体験を強化できます。

比類のないデータインサイト

Akamai は 1 日あたり平均 788 TB のファーストパーティデータを分析しています。この膨大なデータセットと高度なヒューリスティック／機械学習モデルにより、Akamai は、複数の調査会社の評価において、グローバル・トラフィック・パターン分析、イベント追跡、および脅威検知のリーダーに選定されています。Akamai のセキュリティサービス／製品は、この規模のプラットフォームを通じて取得したリアルタイムのインテリジェンスによって強化されています。Akamai は、機械学習を活用して、9 PB のインテリジェンスを格納したデータベースを常に更新／分析し、適応型の自動保護を迅速かつ正確に提供しています。これにより、Akamai のお客様は CVE やグローバルな脅威から常に自社を保護できます。

DDoS 攻撃に対する強力な防御

DDoS 攻撃など、リソースに過負荷をかける攻撃を受けた場合、運用を維持できるか否かはプラットフォームの規模によって決まります。攻撃件数は前年比で 45% 増加しています。そこで重要となるのが、Akamai の規模と分散です。特定の場所が攻撃を受けた場合、トラフィックを近隣の他の場所に再ルーティングすることで、攻撃の影響を緩和できます。Akamai プラットフォームは最近、最大 900 GB の攻撃規模にも耐え、大規模攻撃を緩和できることを実証しました。Akamai は、レイヤー 3、レイヤー 4、レイヤー 7、および DNS に対するボリューム型攻撃を緩和することで、DDoS 攻撃に対処します。

Akamai Connected Cloud

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をサポートする、世界で最も分散したプラットフォーム

4,100 以上
のエッジ PoP
（Point of Presence）

1,200 以上
のネットワーク

130 以上
の国

750 以上
の都市

SSD 搭載
ハードウェア

Akamai

可用性を確保し、リスクを軽減する Akamai プラットフォームの特徴

DNS ベースのメリット

Akamai プラットフォームの基本的な特徴の 1 つが、DNS ベースのアーキテクチャ（Akamai 独自の DNS ネットワークなど）です。Akamai のネットワークは、DNS をインターネットへのゲートウェイとして認識することで、パフォーマンス重視の卓越したユーザー体験を提供します。また、DNS ネットワークの冗長性により、100% の可用性を保証する SLA に裏打ちされた、中断のないサービスが実現します。

効率的なトラフィック管理

Akamai プラットフォームの要となるコンテンツ・デリバリー・ネットワークは、ポート 80 とポート 443 のトラフィックのみ受け入れます。これにより、インターネットのノイズを最小限に抑制し、アタックサーフェスを大幅に縮小できます。不要なトラフィックをエッジで破棄することで、リスクを緩和できるだけでなく、不要なトラフィックにリソースを浪費する必要がなくなるため、全体的な効率性が向上します。

幅広いセキュリティ・ソリューション・ポートフォリオをサポート

グローバル規模の Akamai プラットフォームでは、広範かつ統一されたデータセットが生成されます。このデータセットを活用した機械学習に基づいて、Akamai の幅広いセキュリティ・ソリューション・ポートフォリオに推奨事項が提供されます。この推奨事項を単一のインターフェースを通じて取得することで、セキュリティ運用を効率化して、リソースを解放し、全体的なサイバーセキュリティ体制を改善できます。

結論

Akamai プラットフォームは、その優れた規模により、25 年以上にわたってリーダーとして信頼されてきました。Akamai は、比類のない規模と可視性、そして最先端のインテリジェンスを通じて、複雑な脅威環境に自信を持って対応できるよう、組織を支援しています。Akamai の包括的なセキュリティアプローチを採用することで、情報セキュリティの最高責任者（CISO）は比類のない効率性、耐障害性、インテリジェンスを通じて自社を保護できます。

Akamai プラットフォームならではのメリットを体験

Akamai のセキュリティソリューションにより、Akamai プラットフォーム独自のメリットを活用して、貴社と貴社の顧客を保護できます。貴社のニーズが拡大や変化に対応できるだけの幅広いソリューションポートフォリオを用意しています。単一のプラットフォームポータル、単一の契約、同じサポートチームの支援で、さまざまなソリューションのお試し、追加、変更ができます。

> Akamai を活用すると、セキュリティ対策はバックグラウンドで密かに効果的に行われます。
>
> **– ブリティッシュ・カウンシル、Operations and Commercial Manager**

Akamai App & API Protector

DDoS 攻撃、ボット攻撃、アプリケーションレイヤー攻撃、API 攻撃を防御

Akamai Bot Manager

巧妙な悪性ボットを検知および緩和しつつ、良性ボットを許容するように設計された、高度なボット管理

Akamai Account Protector

アカウントの乗っ取り、アカウント作成の悪用、Credential Stuffing の検知と緩和

Akamai Brand Protector

ブランドなりすまし攻撃（フィッシングや偽の Web サイトなど）の検知と緩和

Akamai Client-Side Protection & Compliance

PCI コンプライアンスを支援し、Web サイトを JavaScript 攻撃から保護

Akamai Edge DNS

DNS インフラを外部の権威 DNS サービスで強化

Akamai Prolexic

インフラを DDoS 攻撃から防御

Akamai API Security

リアルタイム分析を使用して、API アクティビティを探索、監視、監査し、脅威や悪用に対応

> WAF 内の検知はきわめて重要です。Akamai の支援により、複雑な環境でも効果的に検知できます。
>
> – Panasonic Business Support Europe、Principal IT Consultant

詳細については、アプリケーションと API のセキュリティページをご覧ください。