パンフレット

Akamai エッジ・セキュリティ・ソリューション

Web での販売、世界各地のクラウド・データ・センターの運用、外出先での従業員の支援など、ビジネスのつながりが必要となるさまざまな場面で、インターネットは必要不可欠です。このようなつながりを保護することは、セキュリティの脅威が進化し、ビジネス要件が変化している世界ではきわめて重要です。

モバイル。クラウド。DevOps。そこで役立つのが Akamai のソリューションです。Akamai はインターネットを熟知し、インターネットを利用してビジネスを推進する方法を知っています。攻撃者がどのような方法でインフラ全体の脆弱性を発見して悪用するのか、それによってどのような悪影響や損害が生じるのかも把握できます。だからこそ、インターネットに接続しているインフラのさまざまな側面を、増大するリスクから守るために役立つ、堅牢で柔軟なプラットフォームを提供できるのです。

アタックサーフェスを狭めるための 7 つの重要事項

お客様の保護

ビジネスは、お客様の信頼があってこそ成長できます。そのためには、お客様の、個人を特定できる情報（PII）、口座残高、取引の詳細情報を自分自身の情報と同じレベルで保護することが必要です。

WEB アプリケーションの保護

Web サイトがビジネスの中心である場合、攻撃によってビジネスが多大な影響をこうむる可能性があります。Web サイトと Web アプリケーションを、サービス妨害攻撃、Web アプリケーション攻撃、ボット攻撃から保護することは不可欠です。

API の保護

企業はモバイルアプリ、パートナー、クライアントにデータを提供するために API に移行しています。しかし、API エンドポイントにより、新たな方法でアタックサーフェスが拡大します。API も Web サイトと同じ脅威から保護します。

データセンターの保護

データセンター内の IT 資産は、ビジネスのあらゆる側面をサポートします。ネットワーク帯域幅、アプリケーション、サーバー、IoT（モノのインターネット）デバイスなどのインターネットに接続された資産を、サービス妨害攻撃やマルウェアから保護する必要があります。

DNS サービスの保護

ユーザーが Web サイトやアプリケーションを見つけることができるよう、ドメイン・ネーム・システム（DNS）サービスを常に利用でき、高速で信頼性の高いものにしておく必要があります。DNS をサービス妨害攻撃、偽装、改ざんから保護します。

従業員の保護

最大の損害を与えるセキュリティ侵害は、自社従業員によって始まっている場合が多々あります。マルウェア、ランサムウェア、フィッシング攻撃によって、悪性ファイルを騙されてダウンロードする可能性があるのです。

エンタープライズのアプリケーションとデータの保護

セキュリティ境界が消滅していく中、エンタープライズアプリケーションへの安全なアクセスを提供すると同時に、エンドユーザーを高度な脅威から保護し、データが DNS を介して盗まれないようにする必要があります。

グローバル・セキュリティ・プラットフォームでのビジネス構築

Akamai エッジ・セキュリティ・ソリューションは、アプリケーションやインフラからユーザーにまで広がるグローバルプラットフォームに展開されます。Akamai はお客様と潜在的な攻撃者との間に位置し、ネットワークエッジの攻撃者により近い場所で、アプリケーションやインフラが危険にさらされる前に、クラウド内で攻撃を阻止します。

巨大規模

Akamai の比類ない規模とグローバルな分散により、最大規模の直接攻撃を阻止するとともに、他のお客様に対する攻撃からの巻き添え被害も防ぐことができます。

グローバルな保護

データセンター、パブリッククラウド、さらには世界中のマルチクラウド環境でも、アプリケーションを展開しているビジネスをサポートします。

リアルタイムのサポート

グローバルに統合された Akamai の Security Operations Center（SOC）では、さまざまな脅威に対して、攻撃に関する単一の専用窓口によるサポートと、リアルタイムインシデント対応を活用できます。攻撃後は、攻撃の概要をダッシュボードで確認できるだけでなく、攻撃後のフォレンジック調査および根本原因の分析も詳細に可視化できます。

ソリューションの統合

すべてを単一のインタフェースで管理し連携するよう設計されたソリューションにより、緩和の改善と、セキュリティのシンプル化を実現します。

攻撃可視化の向上

Akamai の Web ベースポータルで複数のソリューションを一元管理し、攻撃とポリシー制御を可視化します。ダッシュボードで概要を確認してから、さまざまな問題領域を細かく分析できます。既存のセキュリティ情報およびイベント管理（SIEM）ツールと統合することで、すべてのセキュリティソリューションについて全体的な認識が高まります。

簡単な管理

マネージド型セキュリティサービスにより、物理的な機器やソフトウェアソリューションを展開する必要がなくなります。適応型脅威防御により、絶えず変化する脅威に対応します。アプリケーション開発ライフサイクルを管理 API に統合することで、Akamai ソリューションの設定への変更を自動化します。

将来のリスク緩和

将来の脅威にも対応できるようなセキュリティインフラを構築します。アプリケーションのインフラを中断することなく、新しいセキュリティ機能やソリューションが利用可能になるとすぐに、シームレスに展開します。

Akamai エッジ・セキュリティ・ソリューション

DDoS 防御

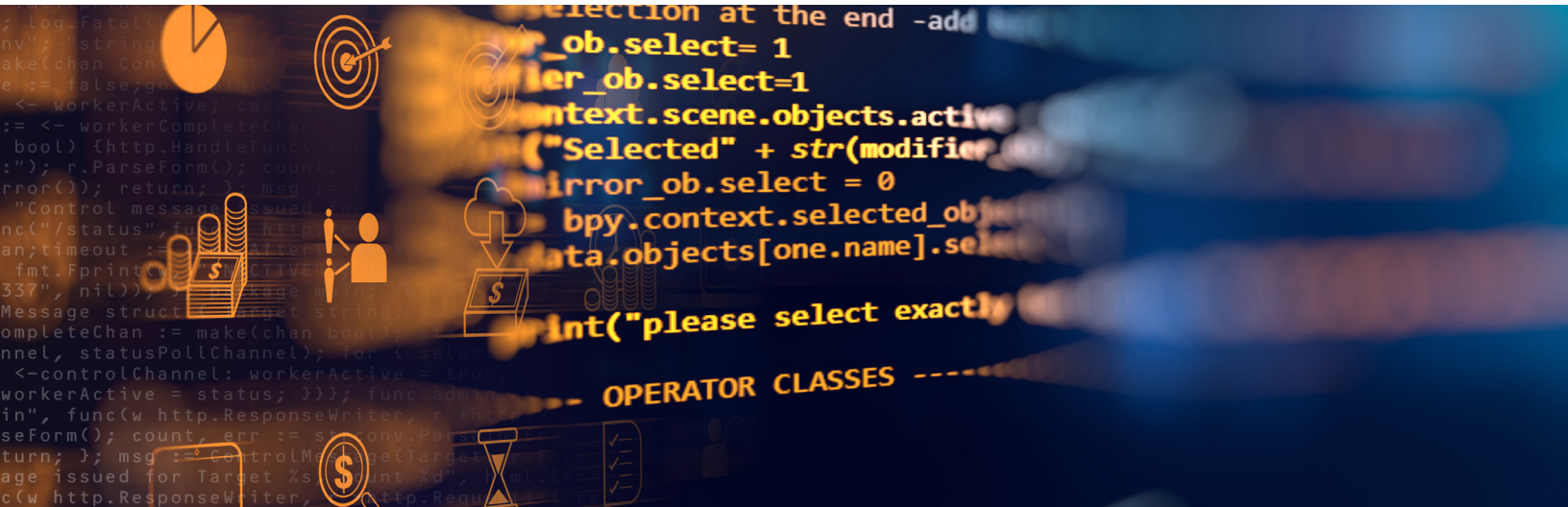
Web サイト、インフラ、DNS を保護する Akamai のクラウドベース DDoS 防御ソリューションにより、最大規模の攻撃が発生しても、アプリケーションおよび IT サービスの可用性を維持できます。毎月、何千件もの攻撃を緩和している Akamai SOC では、誰よりも早く新たな攻撃ベクトルを発見し、経験から得た教訓を体系化して、より迅速に攻撃を阻止します。

合計 175 Tbps 以上のキャパシティを備えた最大規模の DDoS 緩和プラットフォーム	業界をリードする緩和所要時間 SLA による迅速な緩和	100% アップタイム保証および巻き添え被害最小化のために設計された、高い耐障害性
24 時間／ 365 日体制でいつでも攻撃に対応できるグローバル SOC	毎月、数千件の攻撃を効果的に阻止している実績	2003 年以来クラウドの DDoS 攻撃を阻止してきた実績

WEB APPLICATION FIREWALL

Web サイトおよび Web アプリケーションはますます複雑化しリスクも高まっており、毎日のように、新たな脆弱性が発見されています。市場で初めて発表されたクラウド WAF として、また Gartner 社による「Magic Quadrant for Web Application Firewalls」の「リーダー」として評価された、業界をリードする Akamai の WAF ソリューションにより、Web サイトおよび Web アプリケーションを保護します。Akamai は、お客様に対する攻撃の可視化と、新たに明らかになった脆弱性に基づいて、WAF ルールを継続的に更新しています。

世界中に広く分散された 34 万台以上のサーバー	最新の脅威に対応するための適応型 WAF ルール	Akamai の脅威リサーチによって裏打ちされた高い精度
パフォーマンスへの影響をゼロにする保証	数百万のクライアントに対する最新の悪性「ふるまい」を可視化	PCI DSS に準拠



ボット管理

パフォーマンスの低下から顧客の喪失や詐欺行為にいたるまで、さまざまな影響を及ぼすボットは、Web サイトトラフィックの 30 ～ 70% を占めている可能性があります。Akamai のサポートで、より効果的なボット戦略を実装し、スクレイパーを制御し、Credential Stuffing を緩和できます。Akamai はボット状況の変化に対応するために、ボットと Akamai のお客様数千社とのやり取りを可視化した情報に基づいて、ボット検知機能を継続的に調整しています。

他のどのベンダーより多くのボットトラフィックを可視化	高度なボット検知機能で最も巧妙なボットも阻止	高度な管理アクションによる応答のカスタマイズ
Web サイトとモバイル専用アプリの両方を悪性ボットから保護	ボットトラフィックを詳細に分析して理解するためのボット中心のレポート	証明の負担をユーザーではなくボットに課すインビジブルチャレンジ

ブラウザー内の脅威に対する防御

Web ページのスクリプト依存が拡大するに伴い、機微な顧客情報を盗もうとする新たな攻撃ベクトルが出現しています。Web スキミング、フォームジャッキング、Magecart 攻撃を受ければ、データ漏えいが生じ、ブランドの価値が傷つき、制裁金が科せられる可能性もあります。Akamai はこれらの攻撃の検知と緩和でお客様をサポートできます。

クライアント側の攻撃に対する防御	巧妙なスクリプト攻撃に対する比類ない可視性	直感的なダッシュボードで詳細を一目で確認
管理のシンプル化とクリックひとつでの緩和	スクリプトのふるまいと望ましくないデータ抽出を管理するポリシーの作成	Akamai プラットフォーム以外の Web サイトを含め、あらゆる Web サイトを防御

IDENTITY CLOUD

現代のデジタルサイトにとって必要となる基本的な前提条件は、顧客のデジタルアイデンティティとそれに関連するプロファイルデータです。それらは、顧客の「ふるまい」やカスタマージャーニー（最初のコンタクトから購入決定まで、さらにその後の長期間のブランドロイヤルティ）を分析し、理解し、予測するための基礎となるものです。完全な SaaS ベースのソリューションである Akamai Identity Cloud により、貴社の顧客は任意のデバイスで個人アカウントを作成し、共有するデータを自身で制御および選択できるとともに、顧客と貴社ビジネスの両方をリスクから保護できるようになります。

個人アカウントの作成、使用、管理においてフリクションの少ないユーザー体験をお客様に提供	アカウントを管理および監視（顧客のプロファイルデータの保存、分析、レポート）	最大数億人ものユーザーによる複雑な消費者向けのユースケースを処理
GDPR、CCPA、PIPEDA、APPI、APA など、世界中の規制要件に準拠	エンタープライズのテクノロジー環境全体におけるアイデンティティ・データ・フローを制御、不良なデータの無秩序な拡大を防止	OAuth、OpenID、Connect、SAML などの業界のオープンスタンダードをサポート

ゼロトラスト・ネットワーク・アクセス（ZTNA）

エンタープライズのデジタルエコシステム、クラウドアプリケーション、ユーザーの分散など、ビジネスモデルは変化しています。IT には俊敏性が求められ、ユーザーはアクセス権を必要とします。Akamai は、IT チームにとって使いやすくシンプルで安全なリモートアクセス管理を提供し、セキュリティの本質的な向上と卓越したユーザー体験を提供します。

最小権限アクセスを提供	ネットワークからユーザーをセグメント化	多要素認証の有効化
オンプレミス、クラウド、SaaS のどこにあるかに関係なく、すべてのアプリケーションに SSO 機能を提供	従来のハードウェア／ソフトウェアスタックを単一の Web サービスに移行	シンプルで安全な高速のアプリケーションアクセス

DNS

権威 DNS サービスを保護し、ユーザーや従業員の接続を維持します。パフォーマンスおよび可用性の確保を目的として設計された Akamai のソリューションによって、最大規模の DDoS 攻撃が発生しても、DNS 体験の速度と可用性が維持され、さらに DNS の偽装や改ざんも防止できます。

世界各地に配置された 1,000 台規模の DNS サーバーと数百の POP が、悪性ドメインへのアクセスをあらゆる場所から特定してブロック	Fast DNS 解決により、ユーザー体験を向上	DNSSEC サポート
DDoS 攻撃からの巻き添え被害を最小限に抑える 20 以上の個別の DNS クラウド	100% アップタイム SLA による耐障害性と可用性の確保	最大規模の DDoS 攻撃も阻止できる大容量

セキュア WEB ゲートウェイ（SWG）

Akamai の高度な脅威防御ソリューションは、クラウドベースの SWG です。既存のネットワーク防御を容易に統合できるだけでなく、セキュリティ、制御、可視性を提供します。毎日 2 兆件を超える DNS リクエストを処理する Akamai の他に類のないグローバルな可視性と、複数のマルウェア検知エンジンに基づく多層防御により、ユーザーはどこから接続しているか、どのデバイスを使用しているかにかかわらず、プロアクティブに保護されます。

マルウェア、ランサムウェア、フィッシング攻撃をあらゆる場所で事前にブロック	シャドー IT を特定して制御し、アプリケーション機能を制限	すべての Web および DNS トラフィックを可視化
AUP の適用および不適切なコンテンツへのアクセス防止	PII、PCI DSS、または HIPAA のデータが含まれたコンテンツのアップロードをブロックまたは監視	SIEM などの他のセキュリティシステムと Akamai の API を通じて統合

多要素認証

多要素認証（MFA）において最も安全な業界標準である FIDO2 ベースの MFA により、フィッシング攻撃、盗難された認証情報、Credential Stuffing を利用した、従業員アカウントの乗っ取りを防ぎます。この高度なセキュリティ認証方法では、スマートフォンのプッシュ通知のフリクションレスな（手間をかけない）ユーザー体験と組み合わせることで、コストと手間のかかるハードウェアのセキュリティキーが不要になります。Akamai の MFA サービスは、Akamai Intelligent Edge Platform 上に展開され、そのスケール、耐障害性、パフォーマンスに定評があります。Akamai の ZTNA と SWG ソリューションと統合することで、ゼロトラスト・セキュリティの基盤を提供します。

- フィッシング対抗の FIDO2 ベースの MFA による、他に類を見ない従業員認証セキュリティ
- 自動化されたユーザープロビジョニングによる迅速な導入と管理
- スマートフォンアプリのプッシュ通知による、フリクションレスなユーザー体験
- パスワードレスのログインをサポートする FIDO2 ベースの認証による、将来性のある MFA 投資

マネージド型セキュリティサービス

戦略的セキュリティパートナーとして、Akamai はセキュリティ対策を容易にします。Akamai のマネージド型セキュリティサービスは、日々のセキュリティ運用で培われた Akamai の専門知識やリソースに深く根付いており、ビジネスリスクを軽減してビジネスを保護します。お客様の戦略と Akamai の人材、プロセス、テクノロジーを合わせることで、24 時間／ 365 日体制で最新型の攻撃からビジネスを保護します。

- 高度なトレーニングを受けた経験豊富な Akamai スタッフによる攻撃への対応
- 脅威状況の変化に対応し続けることで、ビジネスのリスクを軽減
- 専任スタッフとグローバル SOCC による対応で、オーバーヘッドを削減
- 24 時間／ 365 日の事前監視とインシデント対応
- お客様のセキュリティ対策をパーソナライズされた方法で継続的に評価
- 攻撃への対応準備および効果的な緩和の確かな実績

Akamai は今日のセキュリティリスクだけでなく、将来出現する新たな脅威も緩和できるように準備しています

Akamai には 20 年を超えて培われたセキュリティ経験があり、優秀なセキュリティ専門家、脅威インテリジェンス、セキュリティテクノロジーが 1 か所に集約されています。ユーザーの居場所やデバイスの種類に関係なく、最も安全なデジタル体験をお客様が簡単に提供できるように、絶えず取り組んでいます。

- **保護とパフォーマンス** — オンラインで業務を行う場合、セキュリティによる保護がなければパフォーマンスの確保はあり得ません。
- **セキュリティイノベーションの歴史** — Akamai は設立当初からお客様の保護を続けています。これまでに当社が緩和した中で最大規模の 1.3 テラバイト／秒（Tbps）の攻撃をはじめ、クラウドベースの WAF と DDoS 防御サービスを他社に先駆けて構築しました。
- **セキュリティへの継続的な投資** — Akamai は増え続けるセキュリティのニーズや脅威状況の変化にお客様が適切に対応できるようサポートします
- **最も信頼された最大のクラウド・デリバリー・プラットフォーム** — 主要なコマースサイトの 100%、世界の大手銀行の 80%、世界の大手航空会社の 70% など、Akamai は多くの企業から信頼されています

Akamai は世界中の企業に安全で快適なデジタル体験を提供しています。Akamai のインテリジェントなエッジプラットフォームは、企業のデータセンターからクラウドプロバイダーのデータセンターまで広範に網羅し、企業とそのビジネスを高速、スマート、そしてセキュアなものにします。マルチクラウドアーキテクチャの力を拡大させる、俊敏性に優れたソリューションを活用して競争優位を確立するため、世界中のトップブランドが Akamai を利用しています。Akamai は、意思決定、アプリケーション、体験を、ユーザーの最も近くで提供すると同時に、攻撃や脅威は遠ざけます。また、エッジセキュリティ、ウェブ／モバイルパフォーマンス、エンタープライズアクセス、ビデオデリバリーによって構成される Akamai のソリューションポートフォリオは、比類のないカスタマーサービスと分析、365 日／ 24 時間体制のモニタリングによって支えられています。世界中のトップブランドが Akamai を信頼する理由について、www.akamai.com、blogs.akamai.com および Twitter の @Akamai で紹介しています。全事業所の連絡先情報は、www.akamai.com/locations をご覧ください。公開日：2021 年 5 月。