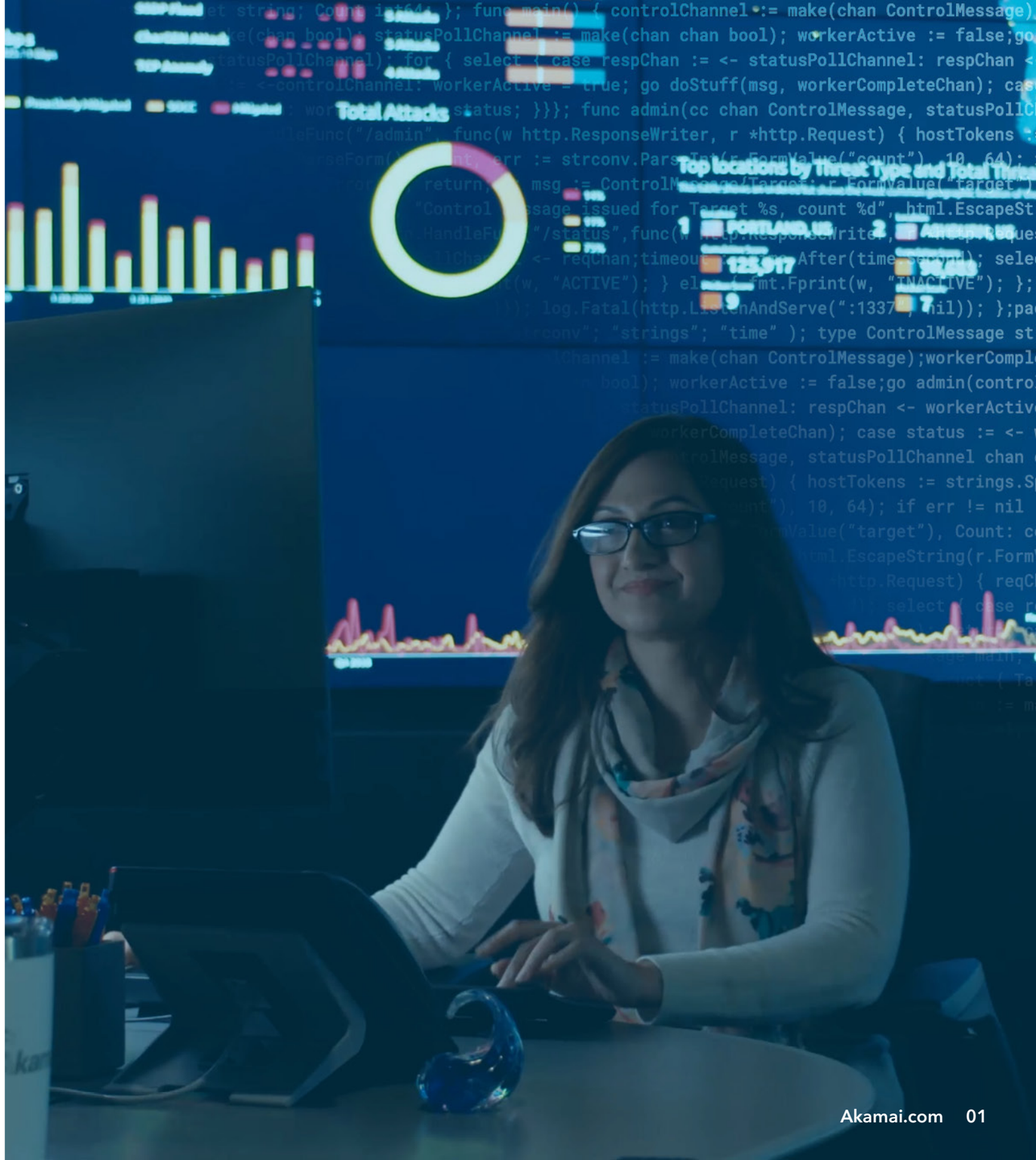
ハイブリッドクラウド環境での DDoS 防御

Eブック

ハイブリッドクラウド環境での DDoS 防御

分散型サービス妨害（DDoS）は、最も古くからあるサイバー脅威の 1 つですが、今もなお、大量破壊の手段として一般に使われ続けており、規模の大小にかかわらず、事実上あらゆる企業や組織にセキュリティリスクをもたらしています。事実、IDC によると、DDoS 攻撃は 2023 年まで CAGR ベースで 18% 拡大すると予想され、堅牢な緩和制御機能への投資を増やす時期であることを明確に示唆しています。DDoS 攻撃のターゲットになるリスクは低いと考えている組織も一部にありますが、ビジネスクリティカルなサービスやアプリケーションを強化するためにインターネット接続への依存度がますます高まることで、インフラが保護されていないと、誰もがダウンタイムの発生やパフォーマンスの低下による影響を受けやすくなっています。



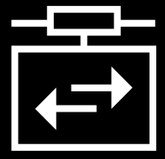
進化する脅威

DDoS 攻撃の規模は 2 年ごとに倍増しており、その複雑性も、攻撃ベクトルの発生件数と組み合わせも、かつてないほど増加しています。アプリケーションとネットワークの可用性は事業継続性に不可欠であることから、攻撃者はボリューム型や、プロトコルおよびアプリケーション層への DDoS 攻撃を仕掛けて、あらゆる潜在的な障害点（Point of Failure）を破壊することで、インターネットに接続されたリソースやアセットをエンドユーザーが利用できなくすることを攻撃の目的としています。

DDoS 攻撃者は、次のようなあらゆる潜在的な障害点をターゲットにします。

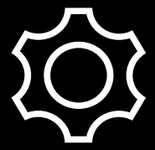
Web サイト

Web アプリケーションとその他のエンタープライズサービス



企業リソースにリモートアクセスするための VPN コンセントレーター

SD-WAN コントローラー



アプリケーション・プログラミング・インターフェース（API）

ドメイン・ネーム・システム（DNS）とオリジンサーバー

データセンターとネットワークインフラ

攻撃者は攻撃対象の環境、アプリケーション、IP空間を偵察することで、インターネットに面したサービスやオリジンホスティングインフラに及ぼす被害が最も大きくなる DDoS ベクトルを特定できます。攻撃への参入障壁は低く、攻撃者はさまざまな攻撃手法やツール（booter や DDoS を請け負う組織など）を駆使して、企業や組織の防御対策に弱点や脆弱性を見つけることができます。

攻撃者には、脅迫や金融操作など、さまざまな動機があります。Akamai では、ビジネスサービス、ゲーム、旅行＆ホテル、ハイテク、物流、小売など、金融業界以外の業界をターゲットにした脅迫キャンペーンの拡大を確認しています。

– Akamai Global Security Operations 担当
Vice President、Roger Barranco

組織が従業員の生産性と通常どおりの事業継続を確保するためにリモートアクセス機能の拡張と保護を図るのに伴って DDoS 攻撃の影響は大きくなります。

DDoS 攻撃による被害

ネットワーク（レイヤー 3）とトランスポート（レイヤー 4）レイヤー攻撃の場合、大量のプロトコルベース攻撃でインターネットパイプを満杯にし、サーバーに過剰な負荷をかけ、ステートテーブルのエントリーを使い果たして、ネットワークとサービスを利用できなくします。アプリケーションベース（レイヤー 7）攻撃では、攻撃者は Low & Slow（少しずつ時間をかけた）攻撃のようなベクトルで Web パフォーマンスとユーザー体験を混乱させるだけでなく、HTTP フラッドで収益に影響を与えるダウンタイムを発生させます。

ただし、ダウンタイムの影響は、攻撃の標的となるサービスやアプリケーションが利用できない場合のコストだけではありません。**Ponemon Institute によれば、組織が被る DDoS 攻撃の平均年間コストは 170 万ドルにのぼり**、それはテクニカルサポートや、インシデント対応リソースの消費量、社内エスカレーション、法的コスト、業務の中断、従業員の生産性喪失の増加によるものです。

影響が甚大であることは明らかで、ハイブリッド・クラウド・インフラへの移行が増えることで、さらにその影響は大きくなります。

クラウドはセキュリティ対策をさらに複雑化している

組織が従来のデータセンターを廃止し、アプリケーションをクラウドホスティングの環境に移行すると、セキュリティアーキテクチャはますます複雑になります。組織の多くは、インターネットに面したアセットをデータセンター内のアセットと同じレベルの DDoS 防御で保護しようとして苦慮しています。複雑さに加え、クラウドホスティングされた IP の多くは、企業や組織の直接制御の対象から外れてしまうことで脆弱になり、適切に保護されていないと、DDoS 攻撃の格好の標的になってしまいます。

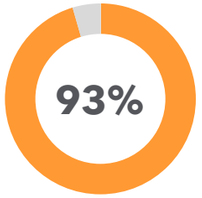
さらに、攻撃者はコロケーション施設やパブリッククラウドへの移行が加速していることを十分に認識しています。そして、一貫性のないセキュリティポリシーと要件によって策定された組織のセキュリティアーキテクチャと対策の弱点や、さまざまな断片化されたクラウドホスト型インフラ全体でのトラブルシューティングの難しさを積極的に悪用しようとします。

要点：

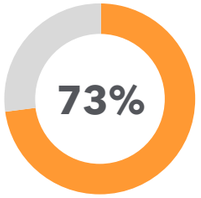
モダンな企業や組織には、Web 上のさまざまなアセットやサービスを場所に関係なく保護するための適応型防御機能が必要です。また、（従業員数が 1,000 人未満の）企業や組織の 93% 以上でマルチクラウド戦略が採用されている今こそ、インフラの複雑さに起因する防御のギャップを埋める時です。[1]

[1] https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020

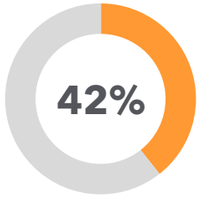
パブリッククラウド環境のセキュリティ対策はプロバイダーごとにまちまちです。そのため、多くの組織が誤った想定をしており、その結果、自社が危険に晒される可能性があります。たとえば、IBM が実施したアンケート調査では、企業や組織の 73% が、パブリック・クラウド・サービス・プロバイダー（CSP）が Software as a Service（SaaS）のセキュリティ確保に主な責任を負っていると回答しました。一方で、42% は、CSP が主にクラウド Infrastructure-as-a-Service（IaaS）のセキュリティ確保に責任があると回答しています。このように、セキュリティ制御に対する責任の所在が不明であることが侵害、つまりどの組織にとっても許容できないリスクにつながる可能性があります。



マルチクラウド戦略を採用しているエンタープライズの割合



パブリック CSP が SaaS のセキュリティ確保に責任があると回答した企業の割合



CSP がクラウド IaaS のセキュリティ確保に責任があると回答した企業の割合

Forrester の最新レポートでは、組織の多くがハイブリッド戦略アプローチを選択し、複数のパブリック・クラウド・プロバイダーを利用するだけでなく、オンプレミスワークロードもホスティングしていると指摘しています。そのため、Forrester では、アナリストファームとして、ハイブリッドアーキテクチャ全体を対象に防御できる DDoS 緩和プロバイダーの選定を推奨しています。

すべての DDoS 緩和が同じように作成されるわけではない

クラウドインフラへの投資が続く中、セキュリティチームは依然として、一貫性のある制御をハイブリッド環境全体に広げるという課題を抱えています。そして、アプリケーションが複数のバックエンド・クラウド・インフラに展開されるのに伴い、保護することはより難しくなり、多くの組織では防御を調整するための単一の制御ポイントを求めています。セキュリティのテクノロジースタックがより複雑化するのに伴い、可視性の最適化だけでなく、API を介してイベントデータ相関システムにフィードしてレポートの作成を合理化するためにも、このように一元的な制御を求める声は多くなっています。

この問題を解決するために、組織はハイブリッドクラウド移行戦略を阻害するのではなく、実現することのできるクラウドベースの DDoS セキュリティプロバイダーに注目しています。組織はエンタープライズサービスの存在する場所に関係なく、スケーラブルでレスポンシブな防御を必要としています。これは、CSP 固有の環境で DDoS 防御を統合、展開、管理する場合の運用の複雑さが増大することへの直接的な反応です。また、複数のクラウドに配置されたインターネットに面したアセットが多いと、複雑さの度合いはすぐに高くなります。

このようなプレッシャーに加え、多くの CSP の自社開発 DDoS 緩和ソリューションは、可視性、SLA、レポート作成という今日のエンタープライズ防御策の強化に欠かせない重要な領域の機能が十分とは言えません。

セキュリティチームにとって、インシデント対応と対策を最適化するためには、可視性と実践的な知見を得ることがすべてです。一部の CSP の DDoS ソリューションには、レポート作成、可視性、攻撃後の分析の点で透明性がほとんどないものもあります。CSP がアナリティクスとレポーティングのブラックボックスと呼ばれているのもうなずけます。

さらに、CSP には DDoS 緩和までの所要時間の SLA を提供せず、その代わりに影響を受けた組織にサービスクレジットを付与しているところもあります。一刻を争う対応が重要な場合、組織にはプロバイダーがパフォーマンスの低下を招くことなくアップタイムと可用性の維持を約束するという確証が必要です。

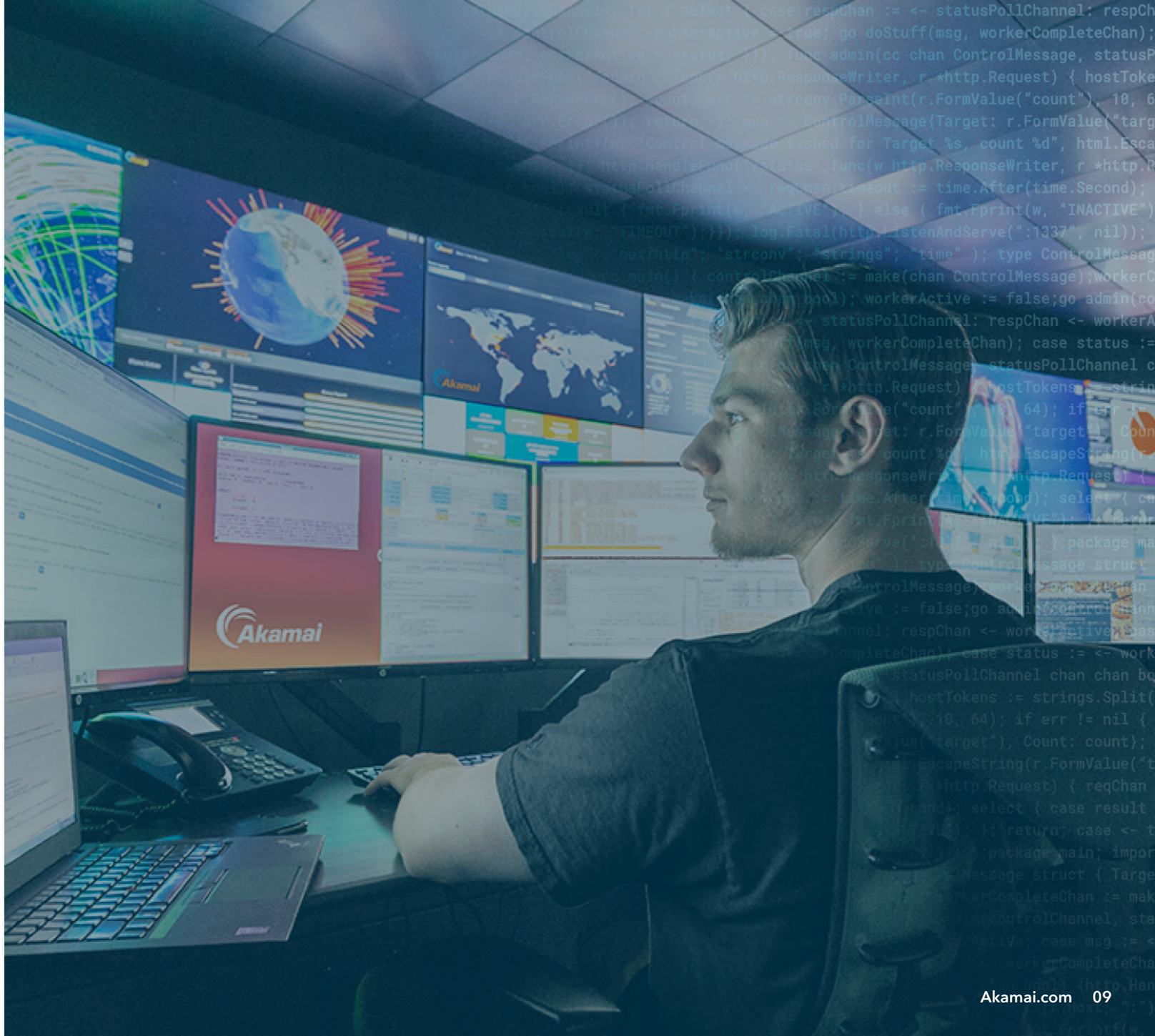
最後に、CSP の多くは、主要なクラウドベース DDoS 緩和プロバイダーでは標準仕様である攻撃前、攻撃中、攻撃後のサポートを提供していないばかりか、24 時間体制のグローバルなセキュリティ・オペレーション・センター（SOC）サポートをオンデマンドで利用できるサービスも提供していません。提供しているとしても、それはプレミアムサービスとして提供され、多くの場合、クラス最高レベルのプロバイダーが提供する専門の DDoS 緩和ソリューションより費用がかかります。フルマネージド型 DDoS 防御ソリューションの場合、サービスプロバイダーは企業や組織のインシデント対応チームの一部として機能し、DDoS イベントにすばやく対応するための専門知識を提供します。

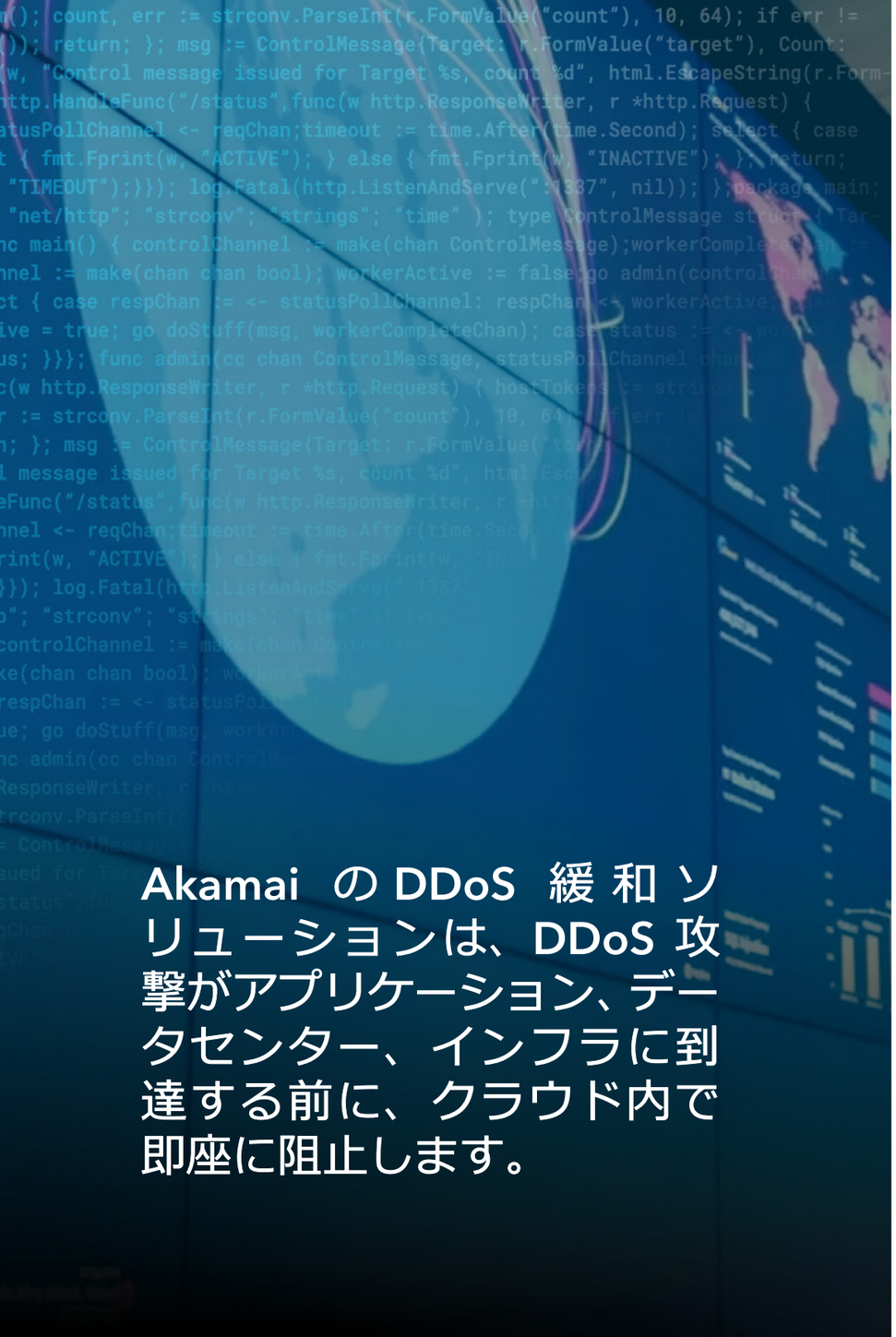
現在の脅威状況では、先進的な企業がハイブリッド環境全体で合理化されたセキュリティ体験をサポートし、アタックサーフェスの複雑さも軽減するような DDoS 緩和パートナーに注目しているのは明らかです。

DDoS 緩和パートナーには、クラウド戦略の妨害者ではなく、セキュリティに対するプレッシャーの軽減をサポートするイネーブラーになることが求められます。

Akamai による専用の DDoS 緩和

組織がエンドツーエンドのクラウド戦略を必要としているのと同様に、エンドツーエンドの DDoS 防御も検討する必要があります。Akamai は包括的なアプローチを取ることで、防御の最前線として機能し、専用のエッジ、分散 DNS、巻き添え被害や Single Points Of Failure を回避するためのクラウド緩和戦略で防御します。他のクラウド・セキュリティ・プロバイダーに見られる「オールインワン」ソリューションとして構築されたアーキテクチャとは対照的に、Akamai の専用 DDoS クラウドは増強された耐障害性、専用のスクラビング機能や高品質の緩和機能を備え、Web アプリケーションやインターネットベースのサービスに特定の要件にもきめ細かく調整できます。





Akamai の DDoS 緩和ソリューションは、DDoS 攻撃がアプリケーション、データセンター、インフラに到達する前に、クラウド内で即座に阻止します。

エッジ防御

Akamai エッジ（CDN）は、HTTP や HTTPS プロトコルを使用する Web トラフィックを配信し、高速化を図ります。すべての Akamai エッジサーバーは、リバースプロキシとして動作し、ポート 80 と 443 で正当な HTTP/S トラフィックを転送し、それ以外のすべてのトラフィックをネットワークエッジで破棄します。そのため、Akamai のすべてのお客様は、Web 配信に仕組まれたネットワーク - レイヤーへのすべての DDoS 攻撃を即座に緩和できます。

DNS 防御

同様のテクノロジーは、Akamai の権威 DNS サービスである Edge DNS にも応用され、ポート 53 以外のすべてのトラフィックは即座に破棄されます。他の DNS ソリューションとは異なり、Akamai の Edge DNS は、パフォーマンスに加えて、DDoS 攻撃に対抗する可用性と耐障害性も考慮した設計となっています。そのため、ネームサーバー、POP（Point of Presence）、ネットワーク、およびセグメント化された IP Anycast クラウドなど、多層的な冗長性を備えたアーキテクチャが採用されています。

クラウドスクラビング防御

Prolexic は、厳しくテストされたクラウド・スクラビング・サービスとして、データセンターとインターネットに面するインフラ全体を対象に、すべてのポートとプロトコルを DDoS 攻撃から守ります。正当なトラフィックと悪性トラフィックの両方を Prolexic を介してルーティングすることで、ポジティブとネガティブの両方のセキュリティモデルを構築し、DDoS 攻撃を高い精度で即座に緩和できます。Akamai Security Operations Command Center（SOCC）のエキスパートは、お客様のインシデント対応チームの一部として機能し、自動検知・対応と手作業とのバランスを取ります。

Akamai を選ぶ理由

Akamai は、世界最大の成熟したグローバル DDoS 緩和クラウドを提供しています。保護する対象が個々のアプリケーション、データセンター全体、権威 DNS のいずれであっても、Akamai は最大のキャパシティ、最強の耐障害性、最速の緩和を念頭に置いて設計された DDoS 緩和ソリューションで対応できます。

Akamai はこれまで、世界で発生した最大規模の DDoS 攻撃のいくつかを緩和しました。Akamai が提供する事前対応型の緩和制御は、文字通りのゼロ秒緩和を定めた業界をリードする SLA に対応します。また、複数のクライアント向けに複数の DDoS 攻撃を同時に阻止する DDoS 防御サービスも提供しています。

Akamai

DDoS 攻撃ベクトルは変化し続け、攻撃規模も大きくなり続けているため、プロバイダーは攻撃を検知・調整・緩和するためのツールやルールの投資・開発・展開を絶えず行う必要があります。Akamai は、攻撃が開始する前に緩和することで、脅威に先手を打つことに専念しています。

お客様の DDoS 緩和戦略は、クラウド戦略を強化するものでなければなりません。Akamai Intelligent Edge Platform は、それを実現する DDoS 防御を提供するもので、クラウドからエッジまでコア全体に防御を拡張することでリスクを最小限に抑えられるようお客様をサポートするだけでなく、クラウド戦略の将来的な進化にも対応できる柔軟性を提供します。

お客様のビジネスを保護するために Akamai がお手伝いできることについてお問い合わせください

詳細を見る

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 でご紹介しています。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：2020 年 11 月。