Akamai

ホワイトペーパー

まだ消えない DDoS に関する 11 の誤解

分散型サービス妨害（DDoS）攻撃は、ここ数年で、サイズや規模が劇的に拡大し、分散化と高度化も大きく進みました。実際、記録を塗り替えるような攻撃がいくつも発生しています。残念なことに、組織の多くは今も防御に対する古い考え方から抜け出せず、防御は十分であると思い込んでいます。それどころか、攻撃の標的になる可能性は低いと考えている組織も少なくありません。現実にこのような攻撃の被害者は、金融サービスから e コマース、ゲームまで、あらゆる主要業界に及びます。実際、ヘルスケア、エネルギー、公益事業、教育、運輸などの重要な公共インフラへの攻撃は特に懸念されています。2023 年、Akamai はアジア太平洋地域のお客様を 900 Gbps（ギガビット／秒）の大規模な攻撃から防御しました。その同じ年の後半、Akamai は 634 Gbps、5,500 万パケット／秒（Mpps）の攻撃を阻止しました。この攻撃は、米国の金融サービスの顧客に対するこれまでで最大規模の攻撃の 1 つである複雑に絡み合った攻撃ベクトルを特徴としていました。このほかに、Akamai がこれまでに緩和した最大規模の DDoS 攻撃も発生しています。これは、1.44 Tbps、385 Mpps のグローバル分散型攻撃で、2 時間近く続きました。こうしたイベントにより、サイバー犯罪者が引き続き経済の重要な柱を標的としていることは明らかです。

小規模な企業は、このように攻撃規模が大きければ、自分たちが DDoS 攻撃の標的になるリスクは低いと考えがちです。しかし、実際には、あらゆる業界のビジネスクリティカルなサービスやアプリケーションが簡単に狙われています。政治的、思想的な動機を持つハクティビストが増え、またサイバー犯罪者グループ（Killnet や Anonymous Sudan など）がサービスとしての DDoS を比較的低コストで提供していることもあり、ほぼすべての人が標的になる可能性があります。組織が懸念すべき最初の攻撃だけでなく、ネットワークやセキュリティのリソースを混乱させるための偽装手段として DDoS 攻撃が使用されるケースも増えています。この場合、攻撃者は、ランサムウェア DDoS 攻撃（RDDoS）や、三重の脅迫キャンペーンなど、その他の卑劣な攻撃を同時に試行します。さらに、洗練された高度な分散型 DDoS 攻撃を編成するために人工知能（AI）ツールの導入が増えている点にも注意が必要です。特に、一貫した可用性とパフォーマンスを確保する必要がある企業や公共機関にとっては、AI が防御上の重要課題となっています。

脅威は日々複雑化し、進化しています。しかし、残念ながら DDoS 防御については未だに誤解が多く、なかにはセキュリティベンダーが推奨しているものさえあります。DDoS 防御は、セキュリティ戦略の基本理念でなければならないため、これらの誤解がもたらす危険を理解することは、DDoS 防御にとって非常に重要です。

誤解 1

総キャパシティは、利用可能な緩和リソースの全貌を示す

総キャパシティは重要ですが、単にネットワークキャパシティを示すことで重要な詳細を省略して誤解を招くことがあります。DDoS 防御テクノロジーソリューションを評価している組織は、次の質問をする必要があります。

- 攻撃トラフィックの消費のみに使用される専用のネットワークキャパシティはどの程度あるか。
- 緩和システムのリソースのうち、攻撃阻止**専用と明記**されているものはどれだけあるか。
- そのプラットフォーム上のすべての顧客のオリジンや各ユニークテナントに対してクリーントラフィックを配信するために使用可能なネットワークリソースやシステムリソースはどれだけあるか。

これらの質問は、ネットワークの総キャパシティにコンテンツ配信などの他の要件が含まれている場合、実際の DDoS 防御能力はプロバイダーが主張している数分の 1 に過ぎない可能性があるため、極めて重要です。

DDoS 防御のキャパシティはテクノロジーだけで決まるわけではありません。ある時点で、テクノロジーが効率的に機能しなくなった場合、エスカレーション、インシデント対応、緩和の微調整を行う専任の人材はいるか。最も堅牢な緩和策は、自動化とマシンインテリジェンスを人間の専門知識と組み合わせて、徹底した保護を提供することです。

ヒント

プロバイダーのネットワークの総キャパシティとプラットフォームの安定性に不一致がないかどうかや、攻撃緩和用とクリーントラフィックの配信用にどの程度のキャパシティが用意されているかを詳しく確認する必要があります。これらは、固有の区分として捉えるべきです。たとえば、攻撃トラフィックのネットワークルーティング、攻撃トラフィックの阻止または緩和、データセンターへのクリーンなトラフィックの配信など、目的別にキャパシティを割り当てる必要があります。

誤解 2

インターネット・サービス・プロバイダーやクラウド・サービス・プロバイダーからの DDoS 防御は十分である

残念なことに、必要なのはインターネット・サービス・プロバイダー（ISP）によって提供される保護だけだと、未だに多くの組織が考えています。実際には、ISP が一般的に提供しているのは、市販されている既製の DDoS 防御を再調整したもので、帯域幅も限られています。ハードウェアは、自社のインフラと共有しているため、キャパシティや CPU サイクルが制限されています。DDoS 攻撃の規模が拡大している今、ISP のインフラはすべて過負荷状態になる可能性があります。ISP は、他の実稼働リソースへの巻き添え被害を防ぐために、顧客のトラフィックを null ルート（ブラックホール）に入れます。すべてのトラフィックがブラックホールに入れられると、企業はエンドユーザーからの正当なトラフィックを失い、サービスは停止します。つまり、実質的にビジネスをオフラインにするという目的が達成されるため、攻撃を成功させることになります。

さらに、クラウド・サービス・プロバイダー（CSP）はほとんどの場合、顧客自身が制御を設定できるようにして、顧客が CSP のクラウド環境内でのセキュリティ対策に関して主権を維持できるようにしています。しかし、ほとんどの CSP は説明責任を拒否し、不正な DDoS トラフィックのコストを最終的に顧客に請求しています。このことにより、最新 DDoS 攻撃の規模やサイズに応じて、被害者にとって大きな過剰費用が発生することがあります。

ヒント

DDoS 防御条項を詳細に検討し、ISP や CSP と交渉することをお勧めします。さらに、その ISP がオンプレミスに堅牢な DDoS 防御ハードウェアを用意し、バックアップとしてクラウドを使用しているかどうかも確認する必要があります。このような ISP であれば、小規模で高速な DDoS 攻撃はオンプレミスで緩和し、大規模なボリューム型攻撃はクラウドの DDoS 防御サービスで適切に緩和できます。

誤解 3

緩和所要時間 SLA はどれも同じようなものである

数字は、時として誤解を招く可能性があります。緩和所要時間（TTM）は、セキュリティベンダーがよく宣伝に利用する数値です。TTM は本来、正当なトラフィックやユーザーに影響を及ぼすことなく、悪性の DDoS トラフィックをどれだけ速く停止または阻止できるかを示します。しかし、これには解釈の余地がたくさんあります。たとえば、あるベンダーはトラフィックが急増しても、それが 5 分以上続かないと DDoS 攻撃とはみなしません。この場合、SLA のタイマーは、攻撃を受けてからでないと開始されない可能性があります。平均的な攻撃期間が 5 分未満の場合、これがいかに問題であるかがわかります。つまり、緩和所要時間は 10 秒と宣伝していても、実際には 5 分以上かかる可能性があるのです。

また、緩和ルールをどれだけ迅速に展開できるかを、緩和所要時間と定義しているベンダーもいます。攻撃の停止や、この制御がアクティベートされる品質または一貫性を反映するものではありません。最終的に確認すべき数値は、**正当なユーザーやサービスへの影響を最小限に抑えながら**、インターネットに面したアセットを安全に保護し、バックアップして稼働できるまでにかかる時間です。そのため、ベンダーの SLA の細則を綿密に確認することが重要になります。

ヒント

SLA に記載されている緩和時間を細かく調べて、次の式が示されていることを確認してください。実際の緩和時間 = 攻撃検知までの時間 + 緩和制御適用までの時間 + 攻撃をブロック／停止するまでの時間 + 緩和の品質／一貫性。正当なユーザーに影響を及ぼさずに DDoS 攻撃を緩和する、**真のゼロ秒 SLA** を提供しているベンダーを選んでください。

誤解 4

null ルーティング／ブラックホーリングおよびレート制限は防御策として容認できる

null ルーティング（またはブラックホーリング）は、一般的ではありますが、どちらかというと旧式な防御対応であり、一部の DDoS 緩和プロバイダーがよく使用しています。こうしたプロバイダーは、あるアセットが攻撃を受けて、他の顧客やサービスがリスクにさらされると、巻き添え被害を防ぐために、そのリソースのトラフィックを仮想のブラックホールに導き破棄します。これは本当に役に立っているのでしょうか？攻撃者から見ると、ブラックホーリングは目的が達成されたことを意味します。なぜなら、標的としたアセットは実質的にオフラインになるからです。結局、そのプロバイダーのインフラに依存している他の顧客も、オフラインになったり、パフォーマンスが低下したりする可能性があります。

多くのセキュリティプロバイダーが提供するもう 1 つの基本的な DDoS 防御対応には、共有環境内での対策として、顧客トラフィックのレート制限を適用することが含まれます。しかし、アセットやサービスが稼働しているとみなすために、正当なトラフィックの 20% ～ 40% が廃棄されるのでは、攻撃を受けている顧客にとって満足できる緩和結果とは言えません。レート制限は、レイヤー 3、4、5 で DDoS 攻撃に対処する際の第 2 または第 3 の対策として効果的です。レイヤー 7 の DDoS 攻撃に直面した場合、レート制限は最初の制御として効果的な場合もありますが、第 1 の手段として必ずシグネチャによる緩和を使用する必要があります。デジタルインフラのセキュリティを 100% 確保するためには、DDoS 攻撃から効果的に保護することが必要であり、オープンシステム相互接続モデルのどのレイヤーが影響を受けるかに関係なく、60% 以下では不十分です。

ヒント

平常時と攻撃を受けている時に、トラフィックのブラックホーリングまたはレート制限をどの程度の頻度で行っているのか、プロバイダーに確認してください。プロバイダーはいつ（どのような状況で）トラフィックをブラックホーリングするのか、そして貴社はサービスの復旧に関してどのような基準を満たす必要があるのかを把握したうえで判断してください。

誤解 5

クラウドプラットフォームをどこと共有しているかは気にしなくてよい

すべての組織がセキュリティを必要としています。ギャンブルやアダルトサイトなどのグレーマーケットのように、問題視されているビジネスも、攻撃を引き寄せやすいため、DDoS 防御のセキュリティを必要とします。犯罪活動やテロ攻撃を推進する組織でさえ、合法的なクラウドベンダーからサイバーセキュリティを購入しています。

このようなサイトは自分には関係ないと考えるのは簡単です。しかし、自社のビジネスが、不法なエンタープライズや頻繁に攻撃されているエンタープライズとクラウドプラットフォームを共有しているとしたら、巻き添え被害を受ける可能性が高くなります。ベンダーのリソースが余裕のない状態であったり、過負荷になっていたりすれば、貴組織はリスクにさらされます。

ヒント

クラウド・セキュリティ・ベンダーの利用規定をよく読み、セキュリティプラットフォームのリソースがリスクの高い標的と共有されることがないことを十分に確認してください。また、誤解 1 と誤解 2 に記載されているキャパシティと能力に関するヒントを再度参照してください。

誤解 6

DDoS 防御には、Web アプリケーションファイアウォールで十分である

Web アプリケーションおよび API 保護（WAAP）ソリューションの大規模なグループの一部であることが多い、Web アプリケーションファイアウォール（WAF）は、アプリケーションレイヤー（レイヤー 7）攻撃に対して効果的な DDoS 防御を提供します。基本的なネットワークレイヤー（レイヤー 3）またはトランスポートレイヤー（レイヤー 4）保護を提供する場合もありますが、すべての IP、ポート、およびプロトコルを包括的にカバーするだけでは不十分です。

DDoS 攻撃にはさまざまな種類と形式があり、インフラレイヤー（レイヤー 3 と 4）、HTTP（s）アプリケーションレイヤー（レイヤー 7）、DNS インフラを標的にすることができます。さらに、攻撃者は動的に攻撃を切り替えることが多く、たとえば DNS から開始し、その後他のレイヤーやプロトコルに拡大する可能性があります。真の DDoS 防御は、多層防御戦略によって実現されます。そのためには、レイヤー 3、レイヤー 4、レイヤー 7、DNS に保護を提供できるような明確な強みと機能を備えた堅牢なソリューションプラットフォームを採用する必要があります。万全を期すためには、どのようなソリューションでも 1 つだけでは十分とは言えません。攻撃に対する脆弱性が残っていたり、正当なトラフィックやサービスを過剰に緩和するリスクが高くなります。

ヒント

DDoS 防御ソリューションが、特定のタイプの DDoS 攻撃や実装設計に偏っていないことを確認します。最善の防御策は、複数の専用 DDoS 防御機能を提供し、それらの相互運用性を維持できる単一のベンダーを利用することです。また、統一的かつ迅速に対応してくれるセキュリティ・サービス・チームが実稼働リソースの保護をサポートしてくれるようなベンダーであることも重要です。これらのアセットがハイブリッドネットワークとクラウドホスティング環境に展開されると、状況は複雑になります。防御サービスは、ネットワークや導入モデルに依存しない必要があります。

誤解 7

オールインワンのセキュリティプラットフォーム = 質の高いセキュリティ体験

一部のプロバイダーは、単一のクラウドプラットフォーム上にさまざまなサービスを提供しています。これにより、短期的にはセキュリティ制御の導入と統合の技術的な複雑さが軽減されるかもしれませんが、同じバックエンドインフラとネットワークを共有する複数のサービスは、環境の他の部分が中断された場合の、プラットフォームの停止、巻き添え被害、および回復力の問題に対し、脆弱になります。多くの場合、このようなワンストップショップのベンダーは、単一プラットフォームアプローチの限界によって機能性を犠牲にしています。

特定の技術課題やセキュリティ課題の解決を目的とした専用設計の CDN、DNS、DDoS 防御プラットフォームやソリューションを、透明の網目のように張り巡らせることで、高品質の緩和と高パフォーマンスを大規模に提供し、防御対策を最適化できます。

ヒント

同じインフラを共有していなくても、セキュリティ体験の統一は可能であるということを忘れないでください。多様な防御アプローチでは、シームレスなユーザー体験とハイパフォーマンスセキュリティの緩和を実現する基盤となるアーキテクチャを使用します。

誤解 8

IPv6 には DDoS 防御は必要ない

Google によると、インターネットトラフィックの約 45% が IPv6 対応デバイスから発信されています。DDoS 攻撃に関しては、IPv6 では、巨大なアドレス空間や IPsec のような内蔵セキュリティ機能など、IPv4 と比較していくつかの改善点が導入されていますが、本質的にこの種の攻撃に対する防御機能を備えているわけではありません。

DDoS 攻撃は、大量のトラフィックでネットワークを圧倒したり、脆弱性を悪用したり、IP バージョンから独立したさまざまな攻撃ベクトルを使用したりすることで、IPv4 と IPv6 の両方のネットワークを標的にすることができます。サイバー犯罪者は、さらに大容量の DDoS 攻撃を仕掛けるために、IPv6 の大幅に拡大された IP スペースをすでに使用していました。攻撃者が、ネットワーク内のランダムなアドレスにトラフィックを送信し、物理ネットワークレイヤーでブロードキャストストームを発生させて、ルーターやネットワークリソースを使い果たしたケースもあります。

クリーンな IPv6 環境は通常想定できないため、IPv4 と IPv6 の間の現在のフラグメンテーションがさらに複雑になります。

ヒント

IPv6 の DDoS 防御には、ネットワーク監視、トラフィックフィルタリング、レート制限、特殊な DDoS 緩和サービスの採用など、IPv4 と同様の戦略とテクノロジーが必要です。

誤解 9

多層防御は必要ない

これを本当に信じている組織はほとんどないとは思いますが、これが真実であるかのような防御戦略は見かけることがあります。自宅を安全にする場合、玄関口をロックしておけば、裏口と窓に鍵を掛けなくても大丈夫という訳ではありません。真の DDoS 防御は、攻撃者が一撃で目標を達成するのを防ぐため、シームレスに連携する複数のセキュリティ層を構築することで達成されます。

ワールドクラスの DDoS 防御は、ネットワークのエッジへのファイアウォールの負荷を軽減するネットワーク・クラウド・ファイアウォールから始まります。次に、ハイブリッド DDoS 防御モデルで、オンプレミスでのハードウェア機器ベースの短時間で急激な攻撃への防御と、クラウドベースの大規模で複雑な大量攻撃への防御のフォールバックを組み合わせて、最適な対処を実現します。DNS インフラも同様の階層戦略で保護する必要があります。そのためには、ネットワークのエッジでセキュリティポリシーを動的に実装できるプロキシサービスを使用し、さらにプライマリモードまたはセカンダリモードで権威 DNS ソリューションを使用して階層化します。最後に、WAF 機能を備えた堅牢な WAAP ソリューションを使用して、すべてのアプリケーションと API を保護する必要があります。

ヒント

多様な専用機能を備えた最高レベルのテクノロジーとソリューションを階層化して、包括的な多層防御戦略を構築すれば、サイバー犯罪者が攻撃を成功させることは難しくなります。

誤解 10

すべてのセキュリティ・オペレーション・センターで同じレベルのサポートが提供される

多くのベンダーがセキュリティ・オペレーション・センター（SOC）によるサポートを宣伝しています。しかし、24 時間体制の SOC があることは最重要事項ではありません。重要なのは、アセットが攻撃された時に受けることができるサービスと専門知識のレベルです。DDoS 緩和プロバイダーを評価する際に考慮すべき重要ポイントは、

- 攻撃前、攻撃中、攻撃後にどのようなサポートと分析を受けることができるか
- 防御の継続性を確保するために、SOC スタッフがどのように配置されているか
- SOC に連絡した場合、電話の相手は実際に緩和を行うアナリストか、単なる窓口担当者か
- そのプロバイダーには、緩和に関するトレーニングを受けたセキュリティプロフェッショナルがいるか、あるいは、プロバイダーのスタッフは市販の緩和商品にトラフィックをルーティングする「交通整理役」なのか
- そのプロバイダーはカスタムランブックを提供しているか

セキュリティプロバイダーの SOC は、インシデント対応チームの拡張部門として、実際に価値を高めるために機能しなければなりません。

ヒント

サービスプロバイダーの SOC から得られるサポートの品質を予想し、評価する必要があります。攻撃の検知と緩和だけでなく、統合とテスト、インシデントのトラブルシューティング、事後分析（知見の獲得）、およびアタックサーフェスの縮小に役立つ設計サポートを提供しているかどうかも判断します。

誤解 11

DDoS 攻撃は古い攻撃手法であるため、最も安価な保護で十分である

「ただほど高いものはない」という格言は、おそらく DDoS 防御に最もよく当てはまります。低価格は魅力的に見えるかもしれませんが、目に見えないコストが生じることも少なくありません。

一部のベンダーは価格を低く設定しておいて、緩和する攻撃の数や規模を制限しています。こうしたプロバイダーは、貴社が膨大な数または規模の攻撃を受けると、攻撃を阻止する前に、より高レベルの（高価な）サービスにアップグレードするよう依頼してきます。しかも、貴社がビジネスをオンライン状態に戻そうとしている最中にです。成熟した DDoS セキュリティベンダーは、顧客が「常時オン」と「オンデマンド」の DDoS 防御を柔軟に選択し、それらをシームレスに切り替えられるようにすることで、運用コストを低く抑えながらクラス最高の保護を提供しています。ベンダーや価格を比較する際には、得失を理解し、自社の DDoS セキュリティ体制への影響を確認する必要があります。

ヒント

サインをする前に、見積もり価格に含まれているものを十分に把握してください。

DDoS セキュリティは複雑であり、急速に進化する今日の状況では、多大な時間とリソースが必要です。昨日は効果的だった方策が、今日からは機能しないという可能性もあります。エンドユーザー、顧客、従業員との接続を維持することは、ビジネス成長の根幹と言えます。エラーを許容する余地はなく、また、単独で取り組もうとして高いコストをかける必要もありません。Akamai は、最も包括的で柔軟性に優れ、信頼性の高い DDoS 防御プラットフォームを提供します。

Akamai の DDoS セキュリティソリューションの詳細はこちらをご覧ください。

Akamai のセキュリティについて

Akamai のセキュリティは、パフォーマンスや顧客体験を損なうことなく、ビジネスを推進するアプリケーションをあらゆる場面で保護します。当社のグローバルプラットフォームの規模と脅威に対する可視性を活用して、お客様と Akamai が提携し、脅威を防止、検知、緩和することで、ブランドの信頼を構築し、ビジョンを実現できます。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。公開日：2024 年 10 月。