Akamai

ホワイトペーパー

DDoS 防御に関する 9 つの迷信

過去 2 年間に、分散型サービス妨害（DDoS）攻撃は規模が 2 倍に拡大し、攻撃ベクトルの数や組み合わせが著しく増えました。2020 年には、ある組織が 8 億 900 万パケット／秒（Mpps）の攻撃を受けました。これは 1 秒あたりの攻撃パケット数の最大記録です。DDoS 攻撃の標的になるリスクは低いと考えている組織もありますが、ビジネスクリティカルなサービスやアプリケーションは業界を問わず標的となっています。インフラが保護されていない企業は、ダウンタイムやパフォーマンス低下のリスクにさらされています。

DDoS 防御はセキュリティ戦略全体の要です。DDoS 防御対策を確立するためには、よく耳にするものの実は間違っている話、つまり迷信に惑わされないようにすることが重要です。

DDoS 防御には多くの迷信があり、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。

迷信 1：総キャパシティは利用可能な緩和リソースを示している

単純なネットワークキャパシティの数値では重要なことはわかりません。知る必要があるのは、1）攻撃トラフィックのみに使われる専用のネットワークキャパシティ、2）攻撃阻止専用の緩和システムのリソース数、3）そのプラットフォーム上に置かれている顧客のオリジンすべてにクリーントラフィックを配信するために利用可能なネットワークリソースとシステムリソースの数です。また、キャパシティはテクノロジーによって決まるわけではありません。テクノロジーが効果的に機能していない場合や、緩和のために最適化されていない場合は、専任のスタッフがいても、そのキャパシティをエスカレーションやインシデント対応、および緩和の微調整に活用できません。

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、攻撃緩和に使用できるキャパシティ、およびクリーントラフィックの配信への利用率を区別し、詳しく確認してください。

迷信 2：緩和所要時間 SLA はどれも同じようなものである

緩和所要時間とは、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、悪性のトラフィックをどれだけ迅速に阻止またはブロックできるかを意味します。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の急増が 5 分以上続かないと DDoS 攻撃とはみなしません。この場合、5 分間攻撃を受けてからでないと、SLA のタイマーは開始されません。つまり、10 秒で緩和すると宣伝していても、実際には緩和までに 5 分以上かかる可能性があります。また、緩和ルールをどれだけ迅速に展開できるかを緩和時間と定義しているベンダーもいます。最終的に重要なのは、インターネットに接続されているアセットが再稼働するまでの時間です。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。攻撃を検知するまでの時間 + 緩和制御を適用するまでの時間 + 攻撃をブロックするまでの時間 + 緩和の品質 = 実際に攻撃を停止するまでにかかる時間。

迷信 3：ブラックホーリングとレート制限は容認できる防御策である

一部の DDoS 緩和プロバイダーの間では、ブラックホーリングが一般的な防御対策となっています。こうしたプロバイダーは、あるアセットが攻撃を受けて、他の顧客がリスクにさらされた場合、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廃棄して巻き添え被害を防ごうとします。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。また、対抗策として共有環境内の顧客のトラフィックにレート制限を適用するプロバイダーも少なくありません。しかし、正当なトラフィックの 20% ～ 40% が失われているのに、アセットやサービスが稼働しているとみなすのでは、攻撃を受けている顧客にとって満足できる結果とは言えません。

ヒント：平常時または攻撃を受けている時にどの程度の頻度で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行っているかプロバイダーに尋ねてください。プロバイダーは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を復旧するために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する必要があります。

迷信 4：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もよい

すべての組織がセキュリティを必要としています。ギャンブルやポルノ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は攻撃を引き寄せやすく、やはりセキュリティ保護を必要とします。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。自分にとって重要では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・セキュリティ・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にすでに余裕がなかったり、過負荷になっていたりすれば、あなたの組織はリスクにさらされます。

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・セキュリティ・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。

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。

迷信 5：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

単一のクラウドプラットフォームにさまざまなサービスをスタックして提供しているプロバイダーもいます。こうすることで、短期的には、セキュリティ制御の展開や統合に伴う技術的な複雑さが軽減されるかもしれません。しかし、同じバックエンドインフラやネットワークを複数のサービスが共有していると、その環境内の他の部分が停止した場合に、プラットフォームの停止、巻き添え被害、耐障害性の問題が生じやすくなります。1 か所ですべてをまかなうベンダーは、多くの場合、シングルプラットフォーム設計の制約により、機能を犠牲にせざるを得なくなります。特定の技術課題やセキュリティの課題を解決する目的で設計された専用の CDN、DNS、DDoS スクラビングクラウドは、見えない網目を張り巡らせることで、より高い緩和品質とパフォーマンスを大規模に提供して防御対策を最適化します。

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。多様な基盤アーキテクチャを使用することで、シームレスなユーザー体験と、高パフォーマンスの緩和の両方を提供できます。

迷信 6：オンプレミスソリューションの方が多くのことを制御できる

オンプレミスのソリューションでは、自分でノブを回してレバーを引くことができます。しかし、それで制御できるというのは錯覚である可能性があります。オンプレミスソリューションは、多くの場合、インターネットリンクの規模が弱点となります。DDoS 攻撃は規模が拡大し、複雑化（マルチベクトル化）しつつあります。4 Gbps に満たない典型的な攻撃でも、インターネットリンクが飽和状態になり、最高レベルのオンプレミスハードウェアが設置されたデータセンターでさえ、サービス拒否が発生する可能性があります。オンプレミスの場合、深刻な攻撃の緩和をクラウドに移行するために時間を買うことになります。セキュリティの人材が不足していたり、過負荷状態になっている場合は、DDoS 緩和をクラウドベースのプラットフォームに外注するか、組織内で DDoS 緩和の専門技能を育成しなければなりません。

ヒント：ネットワーク、IT、インシデント対応のスタッフに負荷がかかりすぎていれば、制御は不可能です。DDoS は、緩和のエキスパートが処理すべき攻撃ベクトルです。社内でできることを強化し、できないことはエキスパートにアウトソースしてください。

迷信 7：多層防御は必要ない

この迷信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、時々、これがいかにも本当であるかのような防御戦略を構築している例を見かけます。たとえば、ハイブリッドアプローチを考えてみましょう。オンプレミスのセキュリティソリューションを強化したいと考えている組織が、同じベンダーのクラウドベースソリューションを追加することでアップグレードする場合があります。1 か所ですべてに対応できれば便利ですが、多層防御が提供されるとは限りません。複数の防御層が同じ基盤テクノロジーで構築されている場合、それらには共通の隙間や弱点があるため、リスクは軽減されません。

ヒント：異なる長所と短所を持つ最高水準のテクノロジーを層状に重ねることで、1 つの防御層の隙間を別の防御層で埋めることができます。

迷信 8：SOC はどこも同レベルのサポートを提供している

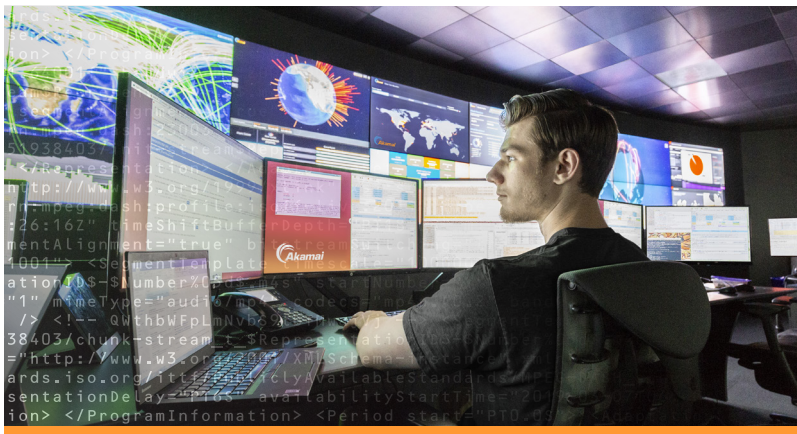
多くのベンダーがデータシートに Security Operations Center（SOC）によるサポートを記載しています。しかし、24 時間体制の SOC があることは最重要事項ではありません。重要なのは、アセットが攻撃された時に受けることができるサービスと専門知識のレベルです。DDoS 緩和プロバイダーを評価する際に考慮すべき重要ポイントは、1）攻撃前、攻撃中、攻撃後にどのようなサポートと分析を受けることができるか、2）防御の継続性を確保するために、SOC スタッフはどのように配置されているか、3）SOC に連絡した場合、電話の相手が実際に緩和を行うアナリストか、または単なる窓口担当者か、4）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、またはそ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、5）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、です。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。

迷信 9：DDoS 防御は包括的なサービスである

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発生することもあります。一部のベンダーは低価格ですが、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。ベンダーや価格を比較する際には、得失を理解し、リスクへの影響を確認することが重要です。

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。



一部のベン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。

DDoS セキュリティは複雑で時間がかかり、常に変化しています。クライアント、顧客、従業員との接続を維持することは、ビジネスの根幹と言えます。エラーを許容する余地はなく、また、高いコストをかけて独力で実施する必要もありません。Web セキュリティに対応した最大かつ最も信頼できるクラウド・デリバリー・プラットフォームを提供している Akamai がお手伝いいたします。詳細については、www.akamai.com/secureapps をご覧ください。

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、Web ／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：2020 年 12 月。