CloudflareのDDoS攻撃対策

最近のDDoS攻撃の進化

2016年
1Tbps
IoTボットネットによるレイヤー7への攻撃

Mirai IoTボットネットを使った、史上最大のレイヤー7攻撃。攻撃は大容量なだけでなく、サーバーリソースを活用。

2014年
400Gbps
NTP増幅攻撃

攻撃者は4,529のNTPサーバーを使い、たった87Mbpsのソースサーバーからの攻撃を増幅。

2013年
120Gbps
レイヤー3や4へのDDoS攻撃

Spamhausへの攻撃は当時の最大規模の攻撃だったと言われており、「インターネットを破壊しかけた攻撃」と呼ばれる。

分散サービス妨害（DDoS）攻撃はその数を増やしており、複雑で対抗するのが難しいセキュリティ上の問題になっています。DDoS攻撃は新しい攻撃方法ではありませんが、このような攻撃を実施し、それを巧妙に隠すために利用できる手段やリソースは劇的に進化しています。DDoS攻撃の進化の歴史で1つの転機となったのは、Miraiボットネットの出現です。このボットネットは30万を超えるIoTデバイスをハッキングし、現在わかっている中で最大のDDoS攻撃を実行するのに使用されました。この攻撃のピーク時のトラフィックは、1Tbpsを超えるスループットになりました。このような規模の攻撃は新たな標準になりつつあります。

多くの場合、DDoS攻撃は一度で終わらず、被害を受ける組織は年に何回も標的にされます。Cloudflareの経験から言えば、組織の大小を問わず、どこでも標的にされる可能性があります。多くの法域でDDoS攻撃を違法とする法律ができていますが、DDoS攻撃をサービスとして提供するプロバイダーがあり、中には月額わずか5〜10ドルで利用できるサービスもあります。

この種の攻撃がWebサイトやビジネスに与える脅威は数多くありますが、その1つは収益の低下です。小売収入990億ドル（2015年）をほこるAmazonのWebサイトでさえ、過去に原因不明のサービス停止が何度も起こっています。たとえば、2013年にAmazon.comでは推定15〜45分間サービスが停止し、180〜530万ドルの売上が失われました（同社の毎分11万7,882ドルという平均売上高をもとに算出）。さらに、サイトにアクセスできないことなどにより、ブランド力や顧客満足度の低下といった数値化しにくい損失も発生します。

スケーラブルで的確なDDoSソリューション

Cloudflareが提供するグローバルなAnycast™ネットワークは、史上最大のDDoS攻撃の10倍となる10Tbpsのスループットをほこり、最近の大規模なDDoS攻撃を受けても、Cloudflareのネットワークにあるすべてのインターネットアセットが持ちこたえられるようになっています。Cloudflareは、レイヤー3、4、7に対するDDoS攻撃への対策として、ネットワークエッジ向けのサービスを提供しています。最近の脅威の規模に対応しており、あらゆる規模や形態のDDoS攻撃を軽減するのに利用できます。Rate LimitingはCloudflareのDDoS攻撃対策を補完するものであり、アプリケーションレイヤーに対する最も高度な攻撃を的確に軽減できます。

レイヤー3と4に対するDDoS攻撃への対策

レイヤー3やレイヤー4に対するDDoS攻撃は通常、DDoS増幅攻撃、DDoSフラッド攻撃、DDoS SYNフラッド攻撃といった大容量の攻撃です。一般的なユニキャストベースのネットワークではこのような攻撃に圧倒されてしまいますが、Cloudflareのエニーキャストベースのネットワークなら、102か所を超えるCloudflareのデータセンターや他のネットワークとのさまざまな高帯域相互接続に攻撃のトラフィックを分散させることにより、処理量を本質的に増やし、攻撃のトラフィックを緩和できます。

DDoS攻撃対策の特徴

- レイヤー3、4、7へのDDoS攻撃に対する保護
- DNS攻撃に対する保護
- Rate Limitingによる微細な脅威のブロック
- IPレピュテーションデータベースを使った予測型セキュリティ

「APIやゲートウェイサーバーへのDDoS攻撃を心配しなくてよいため、製品の向上や改善に専念できます」

- Discord、ソフトウェアエンジニア、Jake Heinz氏

Cloudflareのネットワーク

- 102か所以上のデータセンターからなる、グローバルなAnycast™ネットワーク
- 10Tbpsのスループットで大容量の攻撃も緩和
- 600万のインターネット資産
- 帯域幅によらない一律の価格設定

「Cloudflareを導入した理由は、セキュリティ機能が優れており、CDNのパフォーマンスが高く、またこれらのソリューションが1つのパッケージになっていて便利だからです。おかげで管理業務が簡単になり、本業に専念できます」

- Zendesk、オンライン事業部部長、Amanda Kleha氏

レイヤー7アプリケーション脆弱性に対する保護

レイヤー7への攻撃でよくあるタイプは、SQLインジェクションやクロスサイトスクリプティング（XSS）などです。これらの攻撃では、攻撃者がお客様や何らかのアプリケーションデータにアクセスし、改ざんできる場合もあります。CloudflareはWebアプリケーションファイアウォール（WAF）によってこれらの脅威に対処します。WAFは、OWASPのトップ10のルールセット、Cloudflareのアプリケーションルールセット、およびコミュニティやお客様が作成したカスタムルールに定義されている脅威を自動的にブロックします。Cloudflareは、シェルショック脆弱性やハートブリードバグといった主要なゼロデイ脆弱性からお客様を守ることに成功しています。

RATE LIMITING

Rate Limitingを有効にすると、CloudflareのDDoS攻撃対策やWebアプリケーションファイアウォール（WAF）サービスを補完する微細なトラフィック管理を実施できます。Rate Limitingは、DoS攻撃、ブルートフォース攻撃、アプリケーションレイヤーを標的にしたその他の不正行為に対する保護ソリューションです。要求のしきい値を設定する、チャレンジやCAPTCHAといった軽減アクションや応答コードなどのカスタム応答を定義する、自社のWebサイト、アプリケーション、APIのエンドポイントに関する分析結果を得るなどができます。

予測型セキュリティ

Cloudflareはネットワークトラフィックをリアルタイムで分析し、特異的なまたは悪意のある要求を特定する、自動学習プラットフォームを提供しています。新しい攻撃が特定されると、Cloudflareは、特定のWebサイトとコミュニティ全体の両方で、同じ攻撃タイプを自動的にブロックするようになります。Cloudflareのネットワークとコミュニティが広がるにつれて、Cloudflareユーザーに対して効果のあるDDoS攻撃をしかけるのが難しくなるしくみです。

帯域幅によらない一律の価格設定

Cloudflareは、無制限のエンタープライズグレードのDDoS攻撃対策を、一律の月額で提供しています。DDoS攻撃によるネットワークトラフィックの急増に対し、お客様がペナルティを課せられるべきではないと考えるからです。CloudflareのDDoS攻撃対策を導入すれば、Webサイトがサービス停止に陥ることはなく、毎月の請求額も予測できるためご安心いただけます。

Cloudflareに登録

Cloudflareに登録し、Rate Limitingを有効にして、Webサイト、アプリケーション、APIをDDoS攻撃から守りましょう。また、レイテンシーを軽減したり、最新のWebテクノロジーを利用することもできます。設定は簡単です。実装にかかる時間は通常5分以内です。無料プランからエンタープライズグレードまで、さまざまなプランをご用意しています。詳しくはwww.cloudflare.comをご覧ください。