CLOUDFLARE®

時代に取り残されないために

モバイル消費者向けにEコマースサイトのパフォーマンスとセキュリティを高める

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

概要

現在、モバイルはEコマース戦略の最も重要なチャネルへと成長を遂げる転換点を迎えています。米国の上位25%の小売業者は、圧倒的な市場シェアを占有するために、どうすればモバイルのコンバージョン率を高められるかをすでに把握しており、勝者がすべてを手にするレースを優位に運んでいます。これらの小売業者は、高速で使いやすいモバイルサイトやアプリを提供することで、ユーザーを効果的につなぎ留めるとともに、幅広い層に商品をアピールしています。Cloudflareは、以下の機能を提供することで、モバイル市場で成長するための要件の達成をサポートします。

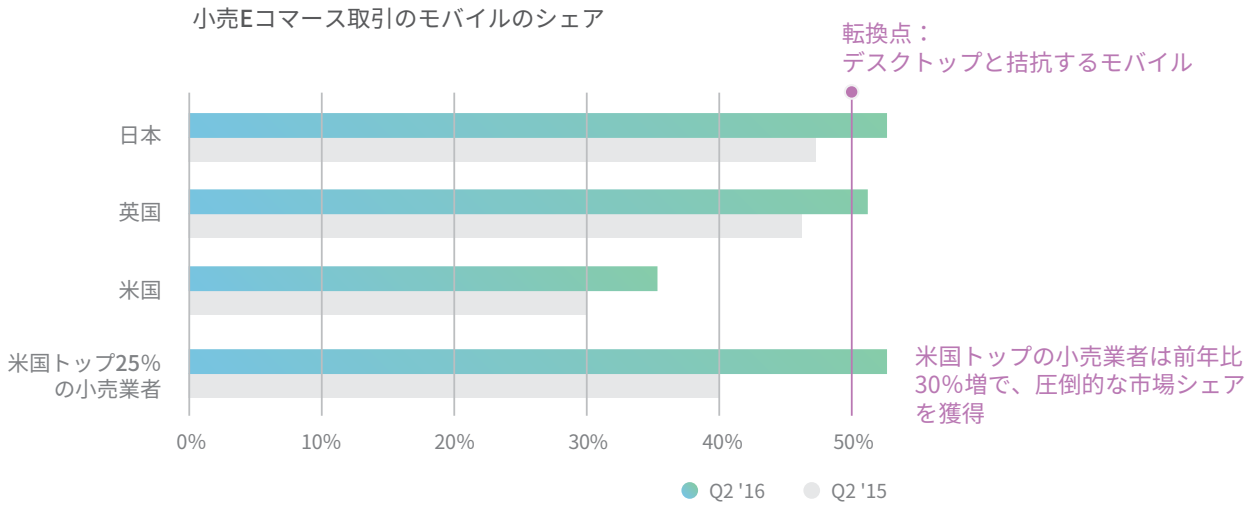
- エニーキャストルーティングに基づく世界最速レベルのコンテンツ配信ネットワークと消費者に物理的に近い場所にコンテンツをキャッシュする機能によってレイテンシーを短縮
- 予測可能な均一料金
- モバイルイメージおよびコードの最適化とIPv6のサポートによってモバイルデバイスのレイテンシーを短縮
- レイヤー3、4、7のDDoS攻撃とレイヤー7のアプリケーション脆弱性から保護して稼働時間を増大
- 適切に行われる暗号化と高いパフォーマンス

Cloudflareをセットアップしてこれらの機能を利用することは、Eコマースベンダーにとって、年間を通して高速で安全なサイトを維持することに積極的に取り組むための大きな一歩です。

転換点を迎えるモバイルコマース

Eコマースが盛り上がりを見せています。2015年には対前年比で14.6%成長し、2015年における米国の小売売上成長の実に36.2%を占めました。Eコマースの成長率は実店舗販売の成長率を大きく上回っています。それ以上の盛り上がりを見せているのがモバイルコマースです。モバイルコマースはEコマースを上回る速度で成長しており、日本と英国では、2016年第2四半期に史上初めてモバイルEコマース小売取引のシェアが50%を超え、デスクトップ取引を上回りました。米国では、Eコマース取引に占めるモバイルのシェアは対前年比17%で増加しています。米国のEコマース取引に占めるモバイルのシェアは35%と、この分野をリードする国々にまだ後れを取っていますが、これらの国々に追いつく勢いで成長しています。

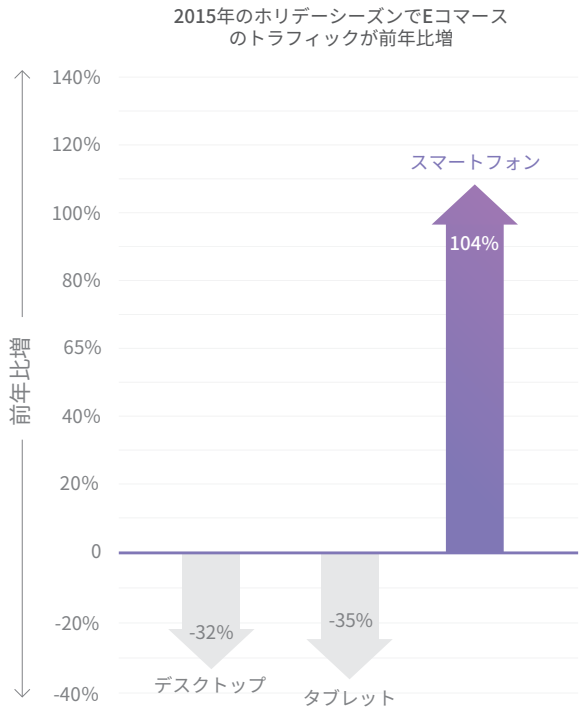
米国の上位25%の小売業者は、すでに最適なモバイルサイトやアプリを提供して、このトレンドを収益に結び付けています。これらの小売業者は、ユーザーを効果的につなぎ留めるとともに、幅広い層に商品をアピールすることで、平均的な新しい小売業者を最大90%上回るコンバージョン率を達成し、モバイル市場で過度に大きなシェアを獲得しています。モバイルはこれらの小売業者のEコマース売上の52%を占め、対前年比30%増という驚異的な速度で成長しています。

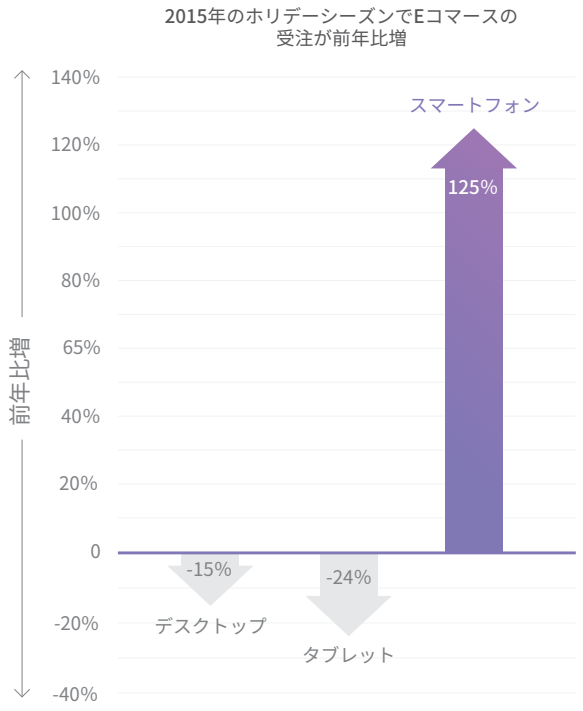


モバイルコマースが重要な販売およびマーケティングチャネルに成長したことは間違いありません。最適なモバイルサービスを提供できる小売業者が勝者になり、モバイルが利用可能な市場でこれまで以上に圧倒的なシェアを獲得し続けるでしょう。

ホリデーショッピングシーズンに欠かせないモバイル

2015年のホリデーオンラインショッピング（サイバー5）は史上最高の売上を記録し、サイバーマンデーは史上最大のオンライン支出が行われた日として米国の歴史に刻まれました。スマートフォンは非常に重要な役割を果たし、トラフィックの49%、注文の27%を占めました。スマートフォンのトラフィックと注文は驚異的な速度で増加しており、その反動でデスクトップとタブレットのトラフィックと注文が減少しています。

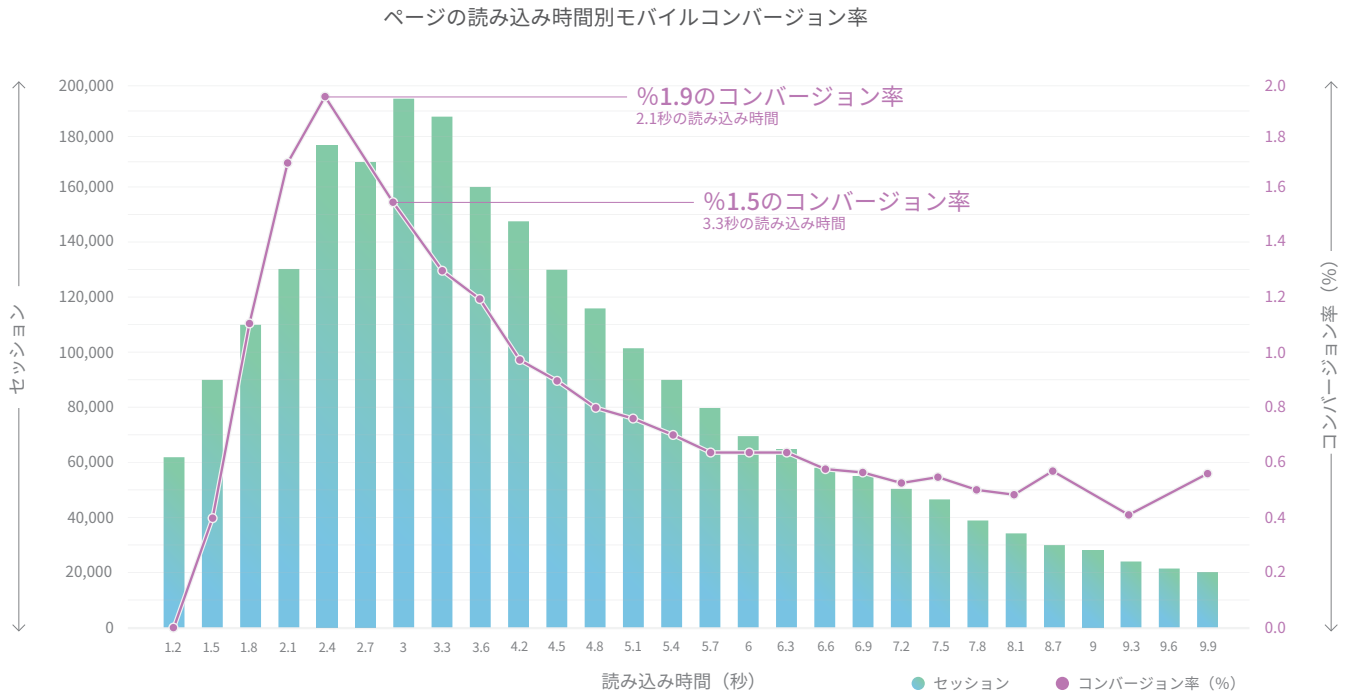




2015年のサイバー5ショッピング期間は、最適なモバイルサービスを提供する小売業者がすべてを手にすることを改めて証明しています。たとえば、Amazonは2015年のサイバー5期間に前年同期比で24.1%売上を伸ばしました。店頭販売とオンライン販売の両方を行っている小売業者では、来年のホリデーシーズンには、オンライン売上が店頭売上を上回る可能性があります。これは、モバイルショッピング環境が成長に不可欠であることを示しています。

レイテンシーと可用性がコンバージョン率に与える影響

リーダーとその他大勢を分けるものは何でしょうか。Eコマースをリードしている小売業者は、最適なモバイルサイトやアプリを提供してコンバージョン率を高めています。モバイルのコンバージョン率はまだ低水準で、モバイルサイトやアプリのパフォーマンスと可用性に直接結び付いています。たとえば、ある大手オンライン小売業者では平均ページ読み込み時間2.4秒で、コンバージョン率が最高1.9%に達しました。平均ページ読み込み時間が1秒増えて3.3秒になるだけで、コンバージョン率は27%低下します。

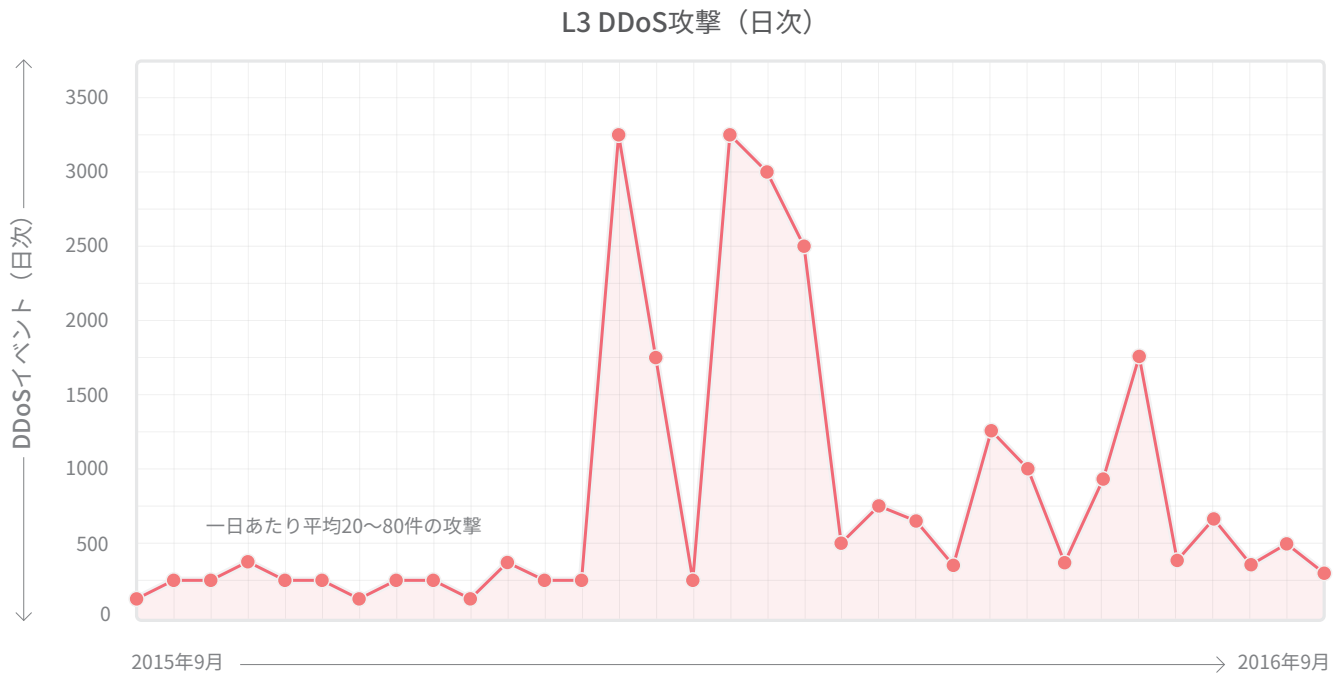


業界には、サイトのパフォーマンスとコンバージョン率の結び付きを示す例が多数あります。

- Amazonでは、サイトのレイテンシーが100ミリ秒減るごとに収益が1%ずつ増加しました。
- Yahooでは、サイトのレイテンシーが400ミリ秒減るごとにトラフィックが9%ずつ増加しました。
- Walmartでは、サイトの読み込み時間が1秒から4秒に増加したときにコンバージョン率が急落しました。

一般的には、Googleが報告しているように、100〜400ミリ秒のサイトのレイテンシーは顧客行動に目に見えるほどの影響を与え、競合他社のサイトより250ミリ秒遅いサイトはアクセス頻度が減少します。

サイトやアプリ自体のレイテンシーに加え、分散サービス拒否（DDoS）攻撃を受けると、サイト全体が利用不能になる可能性があります。Cloudflareは世界全体のインターネットトラフィックの10%近くが流れるネットワークを運用しており、攻撃をフィルタリングして正確に測定できます。Cloudflareの調査によると、この1年間に攻撃の回数と強度が増しています。1日に最大1,400回のDDoSイベントが発生しており、受信トラフィックは合計で400Gbpsにものぼり、1秒あたり2億個の攻撃パケットが送信されています。



多くの場合、攻撃は一度では終わりません。通常、被害を受ける組織は年に何度も標的にされます。Cloudflareの経験から言えば、規模の大小を問わずあらゆる組織が標的にされる可能性があります。多くの地域では、DDoS攻撃を違法とする法律を制定していますが、DDoS攻撃をサービスとして提供しているプロバイダーが存在し、月あたり5〜10ドルという低額で利用できるサービスもあります。

小売収入990億ドル（2015年）を誇る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）。Eコマースベンダーにとってのダウンタイムのコストは、ホリデーシーズン中にはこれよりもはるかに大きくなる可能性があります。Amazonでは、ビジネスの季節性により、2015年の年間収入の33%が第4四半期に生み出されたことを認めています。システムダウンタイムのその他の悪影響として、顧客満足度、検索エンジンのランキング、投資家との関係などへの影響があります。

要するに、コンバージョン率を（特にホリデーシーズン中に）高めたいと考えているEコマースベンダーにとっては、魅力的なサイトやアプリを提供し、それをDDoS攻撃から保護して稼働時間を増やすことが何よりも重要です。

高速で安全なモバイルサイトを実現するために不可欠なテクノロジー

Cloudflareを使用すれば、ハードウェアの追加や、ソフトウェアのインストール、またコードを1行と変更することなく、モバイルコマースサイトやアプリを高速化し保護できます。

最初のステップはCloudflareのコンテンツ配信ネットワーク（CDN）を使用することです。CloudflareのCDNは世界最大のネットワークの1つで、月に10兆件以上のリクエストを供給しています。これは、世界中の25億以上のインターネットユーザーによって行われるインターネットリクエスト全体のほぼ10%に相当します。Cedexisの調査によると、CloudflareのCDNは平均応答時間34ミリ秒（米国の場合）で、常に世界最速のCDNの1つにランクされています。CloudflareのCDNの主な機能は次のとおりです。

エニーキャストベースのルーティング

CloudflareのCDNはエニーキャストと呼ばれるルーティングスキームに基づいて動作しますが、現在のほとんどのインターネットはユニキャストと呼ばれるスキームに基づいて動作しています。ユニキャストでは、ネットワーク上のすべてのノードが一意のIPアドレスを取得します。ルーターは、世界中のIPアドレスのマッピングを保持し、さまざまなホップを経由して最終宛先に至るまでの最短ホップを管理します。しかし、最終宛先は大陸の反対側にある場合もあれば、世界のどこか遠い場所にある場合もあります。その場合は追加のホップが必要になり、ホップごとに遅延が発生します。Cloudflareが使用しているエニーキャストルーティングスキームでは、CDNネットワーク内の複数のマシンが同じIPアドレスを共有するため、ルーターは物理的に最も近いサーバーに直接リクエストを送信できます。これにより、レイテンシーが軽減されます。

コンテンツのキャッシング

Cloudflareのエニーキャストネットワークは、コンテンツのキャッシングと連係して動作します。エニーキャストが物理的に最も近いサーバーにリクエストをルーティングすると、このサーバーでキャッシュされたコンテンツにアクセスできるようになります。キャッシングのメリットは、オブジェクトを要求元の訪問者の近くに移動し配信速度を上げられることと、送信元Webサーバーの負荷を軽減できることです。Cloudflareは、静的コンテンツを自動的にキャッシュする機能を提供します。また、Railgunによって動的コンテンツをキャッシュするメカニズムも提供します。

Cloudflareは、CDN内のサーバーを通過するトラフィックを分析し、送信元サイトの静的部分を見つけます。次に、静的コンテンツをCDNに短期間キャッシュします。通常、Webコンテンツの66%がキャッシュ可能（「静的コンテンツの自動キャッシング」）ですが、残りの34%はキャッシュできず、送信元Webサーバーから取得する必要があります。Railgunは、Web全体が実質上キャッシュ可能になるよう、キャッシュできないコンテンツの配信を高速化するように設計されています。Railgunは、キャッシュできないWebページは急速には変化せず、CloudflareのCDNサーバーはWebページのバージョン間の非常に小さな差異を識別できるという認識に基づいて動作します。次にCloudflareは、この変更部分を最大99.6%の圧縮率で圧縮し、リンクを介して送信します。これにより、パフォーマンスが最大700%向上します。Railgunを使用する場合は、送信元サーバー側にソフトウェアコンポーネントをインストールする必要があります。

「帯域幅コストが上がり続けるなか、Cloudflareのようにエッジでイメージをユーザーに提供するCDNを利用すれば、コスト効率を高められると同時に、当社のモバイルのお客様のレイテンシーを軽減できます」

Big 5 Sporting Goods Eコマース担当責任者 Chris Smith氏

均一料金

インターネットの一角を担うCloudflareは、さまざまなプロバイダーからトランジットと呼ばれる帯域幅を購入しています。Cloudflareは、任意の月に使用する容量に基づいてトランジットを卸値で購入し、一定期間の最大使用量に応じて料金を支払っています。Cloudflareが支払う料金は世界の地域によって大きく異なりますが、Cloudflareはシンプルな料金体系を保つために、トラフィックが世界のどこで配信されているかにかかわらず、お客様への提供料金は均一にしています。ネットワークで配信されたビット単位で請求する一部のクラウドサービスとは異なり、Cloudflareの月間料金は予測可能です。Cloudflareはできる限りリーズナブルな料金で優れたサービスを提供するために、今後もトランジットコストの削減とピアリングの増大に取り組んでいきます。

イメージとコードの最適化

Cloudflareは、Polish、Mirage、Auto-Minifyの3つを組み合わせてレイテンシーを大幅に削減します。これらの機能は、帯域幅が制限されているモバイルデバイスで特に重要です。

Polishはメタデータを削除し、イメージを圧縮することによってイメージのサイズを縮小します。Polishは無損失モードで実行できます。無損失モードでは、イメージデータを削除せずに、イメージヘッダーの不要な肥大化とメタデータを削除します。ファイルサイズは平均で21%縮小されます。Polishは非可逆モードでも実行できます。非可逆モードでは、無損失モードの処理に加えて、適切なイメージに圧縮アルゴリズムを適用します。イメージは以前とまったく同じように表示され、認識可能な視覚的違いは一切ありませんが、ファイルサイズは平均で48%縮小します。イメージは、標準的なWebサイトを構成するデータの50%以上を占めます。

Mirageは、モバイルデバイスでのイメージの読み込み方法を管理します。ユーザーがサイトを操作できるように使いやすいページの外観をすばやく生成しながら、ユーザーによる操作を妨げることなく、ページの残りの部分を描画します。

- Mirageは、遅延読み込みを使用して、ビューポートにあるイメージ、つまりブラウザーに実際に表示されるイメージを優先的に読み込みます。次に、ブラウザーに表示されないその他のイメージを、それらが必要になったとき、または予備のネットワークリソースが使用可能になったときにページに読み込みます。

- モバイルデバイスは画面サイズが小さいため、小さい画像が必要です。Mirageは、サーバーにあるイメージを通常はフル解像度の画像の1%程度に縮小し、サイズを縮小したイメージを最初に送信します。サイズを縮小したイメージでページがレンダリングされた後、それらのイメージはフル解像度のイメージに置き換えられます。イメージはまず低品質で表示され、その後、明瞭に表示されます。

- Mirageは、イメージごとに新しいリクエストを開始するのではなく、1回のリクエストですべてのイメージをCloudflareのネットワークからストリーム配信します。つまり、数百個のイメージがあるページでも、わずか2回のリクエストでブラウザーでのレンダリングを開始できます。低速なモバイル接続を使用しているユーザーでも、ページの操作をすぐに開始できます。すべてのフル解像度イメージが読み込まれるまで待つ必要はありません。

Auto Minifyは、HTML、JavaScript、CSSファイルから不要な文字（ホワイトスペース）を適宜取り除き、ファイルの機能を変更せずにファイルサイズを20%縮小します。CloudflareのAuto Minifyの実装は、次に高速なアプローチよりも優に100倍以上高速です。

IPv6のサポート

FacebookおよびLinkedinによって実施されたリアルユーザーモニタリング測定によると、米国の上位4つのモバイルネットワークでは、IPv6を使用したモバイルページの読み込みがIPv4を使用した読み込みよりも優に10%以上高速であることがわかりました。IPv6の展開は何十年にもわたる活動で進展が遅いと批判されている一方で、米国の上位4つのモバイルネットワークからのAndroidリクエストの約60%、iPhoneリクエストの20%以上がデュアルスタックサイトに対してIPv6を使用していました（2016年5月4日時点）。Cloudflareは、完全なIPv6サポートだけでなく、IPv6からIPv4へのゲートウェイも2012年以降提供しています。また、お客様がこのサービスを「1回のクリックで簡単に」有効にできるようにしています。送信元サーバーがIPv6をサポートしている場合、IPv6接続を使用してアクセスした訪問者のリクエストは、IPv6によってエンドツーエンドで転送されます。送信元サーバーがIPv4しかサポートしていない場合、CloudflareはIPv6でアクセスしてきた訪問者を受け入れ、IPv4を使用してサーバーにリクエストを送信します。また、IPv4でしか動作できないアプリケーションが送信元サーバーで実行されている場合、CloudflareはPseudo IPv4を提供します。このオプションは、接続がIPv6で確立された場合は常に、「疑似」IPv4アドレスを含むHTTPヘッダーをリクエストに追加します。

レイヤー3およびレイヤー4 DDoSに対する保護 - エニーキャストネットワークの回復力と自動学習プラットフォーム

Cloudflareのコンテンツ配信ネットワーク（CDN）を利用するだけでは十分ではありません。次のステップは、稼働時間を確保するために悪意のある攻撃からサイトやアプリを保護することです。ネットワークエッジでサービスとしてプロビジョニングされるCloudflareの高度なDDoS保護は、巧妙かつ大規模な脅威に対抗できる力があり、あらゆる形態や規模のDDoS攻撃を軽減するために使用できます。Cloudflareは、400Gbps以上の攻撃を含む大規模DDoS攻撃を何度も防ぎました。

通常、レイヤー3およびレイヤー4 DDoS攻撃は、DDoS増幅、DDoSフラッド、DDoS SYNフラッドなどの帯域幅消費型攻撃です。このような攻撃は通常のユニキャストベースのネットワークを圧倒できますが、Cloudflareのエニーキャストベースのネットワークでは、100以上のCloudflare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トラフィックを分散させて攻撃対象領域を広げ、攻撃トラフィックを簡単に吸収できます。さらに、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、異常なリクエストや悪意のあるリクエスト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その攻撃タイプを自動的にブロックし始めます。

コストの観点から見ても、通常であればCloudflareは攻撃による影響を受けません。Cloudflareはかなりの量の卸売帯域幅を購入し、月あたりの平均入力（受信）と出力（送信）のいずれか量の多いほうに基づいて料金を支払っています。Cloudflareはキャッシングプロキシとして機能するため、通常の状況では、出力が常に入力を4〜5倍ほど上回っています。攻撃が発生すると、出力と入力の差が縮まりますが、Cloudflareの総帯域幅コストを押し上げるほど大規模な攻撃はめったに起こりません。Cloudflareはこのメリットをお客様に還元します。つまり、お客様は、DDoS攻撃によるネットワークトラフィックの増大分については料金を請求されません。

Cloudflareはネットワークとコミュニティを継続的に拡大しているため、Cloudflareユーザーに対して効果的なDDoS攻撃をしかけるのは今後ますます難しくなります。

レイヤー7 DDoSに対する保護 - IPレピュテーションデータベースによる速度制限

レイヤー7のサービス拒否攻撃は、レイヤー3およびレイヤー4の帯域幅消費型攻撃と同様に、大量のリクエストを使用して実際のユーザーのWebサイトへのアクセスを妨げます。レイヤー7のサービス拒否攻撃では、単一のIPアドレスから多数のリクエストを送信します。これは通常の悪意のないトラフィックのパターンに似ているため、防御するのが困難です。

CloudflareのTraffic Protector（現在はEarly Access Programで利用できます）は、各IPアドレスから送信されたリクエストの数を追跡し、1分あたりのリクエスト数が過剰なサイトを特定します。疑わしいIPアドレスが特定されると、そのIPアドレスからのトラフィックに対して割り込みページが約5秒間表示され、一連の数学的チャレンジが実行されます。リクエストがこのチャレンジに失敗した場合、Traffic ProtectorはこのIPのレピュテーションを格下げし、このアドレスからアクセスが試みられるたびにそのトラフィックに対してCAPTCHAページを表示します。

Cloudflareが悪意のあるリクエストを行っていると思われるIPアドレスを特定した場合、そのIPアドレスはCloudflareのIPレピュテーションデータベースに格納されます。リクエストは脅威スコアに応じて通過するか、CAPTCHAを返されるかのいずれかです。CAPTCHAに失敗し、IPアドレスが悪質とみなされた場合、リクエストはCloudflareのエッジでネットワーク全体に対してブロックされます。これにより、Cloudflareコミュニティ全体が恩恵を受けることができます。

レイヤー7非DDoSアプリケーション脆弱性攻撃 - Webアプリケーションファイアウォール

レイヤー7アプリケーションレイヤー攻撃は、最も複雑で最も巧妙な攻撃タイプです。アプリケーションの通常の使用方法を模倣することで、ほとんどのDDoS軽減装置や脆弱性保護サービスを通過できてしまいます。一般的な攻撃タイプであるSQLインジェクションとクロスサイトスクリプティング（XSS）では、攻撃者が顧客データやその他のアプリケーションデータにアクセスし、改ざんできる場合があります。

Cloudflareはこれらの脅威にWebアプリケーションファイアウォール（WAF）で対応します。WAFはOWASPコアルールセットを実装し、Cloudflareではすぐに使用できるルールを提供しています。また、コミュニティやお客様がカスタムルールを作成することが可能です。Cloudflareからリリースされた新しいルールは30秒以内にすべてのCloudflareサーバーノードに伝搬され、WAF自体のレイテンシーは1リクエストあたり1ミリ秒以下であるため、パフォーマンスを犠牲にせずにセキュリティを高めることができます。Cloudflareは、このようにして主要なゼロデイ脆弱性（Shellshockの脆弱性やHeartbleedのバグなど）からお客様を保護してきました。

> 「当社は、DDoS攻撃の影響を非常に深刻に受け止めています。当社のドメインがDDoS攻撃を受けたときでさえも、Cloudflareは当社のドメインを迅速に保護し、当社のお客様に通常どおりのサービスを提供できました。Cloudflareが当社にもたらす最も大きなメリットは、誰かがネットワークをモニタリングしてくれている、どんな攻撃でも軽減できる術があるという安心感です」
>
> Big 5 Sporting Goods Eコマース担当責任者 Chris Smith氏

TLS 1.3とHTTP/2（サーバープッシュ機能付き）

信頼できるショッピングサービスを提供するには暗号化が不可欠です。最新のSSL強化機能を使用すると、暗号化を適切に行うとともにパフォーマンスを高めることができます。Transport Layer Security 1.3（TLS）では、以前のバージョンのTLSの安全でない機能が削除されているうえ、プロトコルのラウンドトリップが半減されてレイテンシーが短縮されています。Cloudflareは、TLS 1.3を初めて導入したベンダーで、TLS 1.3の標準化に大きく貢献しました。TLSとのみ連携するHTTP/2を初めて導入したベンダーでもあります。HTTP/2は、パフォーマンスの向上、特にエンドユーザーがブラウザーを使用しているときに体感するレイテンシーの短縮を実現します。HTTP/2はサーバープッシュと連携して動作します。サーバープッシュとは、クライアントがまだ要求していないリソースをサーバーが送信することで、ユーザーが体感するパフォーマンスをさらに向上させる機能です。TLS 1.3とHTTP/2（サーバープッシュ機能付き）は、Cloudflareが新しいテクノロジーをネットワークに組み込むことに継続的に取り組んでいることを示すほんの2つの例に過ぎません。

要点

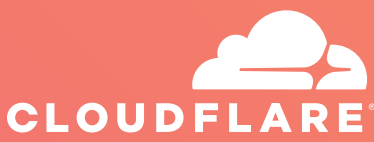
Cloudflareに登録し、モバイルサイトやアプリのパフォーマンスを高めると同時に、DDoS攻撃およびアプリケーションの脆弱性からモバイルサイトやアプリを保護しましょう。セットアップは簡単で、通常であれば5分以内に稼働させることができます。FreeからEnterpriseまで各種プランをご用意しておりますので、www.cloudflare.comでご確認ください。

Cloudflareについて詳しくは、以下にお問い合わせください。

www.cloudflare.com

enterprise@cloudflare.com

1 888 99 FLARE



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com