ホワイトペーパー

CLOUDFLARE

Webサイトの中国でのパフォーマンスとセキュリティを最適化する

中国の巨大で複雑、かつ急成長しているインターネット経済に進出するための戦略

03-4510-1893 | enterprise@cloudflare.com | www.cloudflare.com

概要

中国は世界最大のインターネット人口を擁しています。しかしながら、この市場に参入することは、悪意のある攻撃、およびインターネットインフラストラクチャ上の課題によって難しい場合があります。こうしたハードルを越え、顧客の中国におけるWebサイトの最適化のプロセスを効率化するお手伝いができるよう、Cloudflareはそのグローバルパフォーマンスとセキュリティネットワークサービスを中国にシームレスに拡大しています。

オンラインビジネスの中国進出における課題

中国の広大で急成長するオンライン経済は、さまざまな企業にとって魅力的な市場となっています。中国は世界最大規模の10億人を超えるインターネット人口を擁しており、8億1200万人以上が2021年上半期にネット上で何かを購入しています。この期間のオンライン上の全体的な消費額は、前年に比べてやや減少しましたが、これは主に新型コロナウイルス感染症のパンデミックによる広範な経済不安によるものです。しかし中国経済はコロナ後も2桁の成長を続け、2020年の電子商取引市場は12.5%の伸びを示しています。

他の地域市場と同様に、中国で事業を展開するグローバル企業は、現地の期待に応えるために、サービスとオンライン体験を適応させる必要があります。残念ながら、中国のインターネット規制、基盤となるインフラストラクチャ、脅威の状況によってもたらされるさまざまな固有の課題により、グローバル企業が同じ顧客体験を現地の消費者に提供することは困難になっています。これらの課題は次のとおりです。

- 断片化されたネットワークと、不十分なローカルピアリングによって引き起こされる遅延
- モバイルWebサイトのパフォーマンスの妥協点
- 中国国内での持続的なサイバー攻撃

このホワイトペーパーでは、これらの課題の具体的な例、それらを克服するための戦略と、Cloudflareがどのように役立つかについて説明します。

インターネットのボトルネックと不十分なローカルピアリングによって引き起こされる遅延

多くの消費者と同様に、中国のユーザーもオンライン体験に大きな期待を寄せています。HSBCの報告書によると、中国は世界の電子商取引市場をリードし、支配しています。また、business.comの分析から、国別で世界最大の電子商取引市場であることが確認されています。

残念ながら、中国のユーザーがアクセスできる、ほとんどの組織のWebサイトのパフォーマンスは遅く、リライアビリティに欠けるものです。

1つの理由は、ネットワークのボトルネックです。中国を出入りするすべてのインターネットトラフィックは、北京、上海、広州の3つのインターネットエクスチェンジポイント（IXP）のいずれかを通過しなければなりません。使用率の高い時期では、これらのIXPは混雑し、中国国外でホストされているWebサイトの読み込み時間が大幅に増加する可能性があります。一連のテストでは、TEDのWebサイトが上海で読み込まれるのに8〜38秒かかりましたが、ニューヨークでは5〜8秒しかかかりませんでした。

これらのボトルネックを回避するために、一部のグローバル企業は、中国の3つのIXPのいずれかに近いデータセンターでWebサイトをホストしています。例：広州IXPに近い香港にホストするか、中国の国境内のサーバー上にホストするかです。ただし、これらのアプローチは、依然としてピアリングが不十分なローカルインターネットサービスプロバイダー（ISP）の数が限られているという、別の主要なネットワークの課題によるリスクにさらされています。

中国のインターネット情勢に精通している企業は、中国電信、中国移動通信、中国聯合通信の3つの国営ISPが市場を支配していることをすでに知っているかもしれません。これらのISPはそれぞれ、国の異なる地域を支配していますが、IXP同士で別々のネットワークを接続するという「ピアリング」をあまり行っていません。2017年のMlyticsの調査によると、中国で最もピアリングされているネットワークは2つのIXPにのみ接続されていましたが、北米では66、ヨーロッパでは71でした。

つまり、中国国内のインターネットトラフィックであっても、物理的に短い距離がネットワーク距離的に遠い場合が珍しくなく、エンドユーザーが体験する遅延をさらに悪化させる原因になります。

ボトルネックと貧弱なローカルピアリングを克服する方法

このようなウェブパフォーマンスの課題に直面し、中国でビジネスを展開している多くのグローバル組織は、コンテンツ配信ネットワーク（CDN）を使用して、エンドユーザーに近いデータセンターに静的（またはユーザー固有でない）Webサイトコンテンツをキャッシュし、リクエストがオリジンサーバーまで戻る必要をなくします。企業が採用すべきCDNの特徴：

- **大規模でよくピアリングされたネットワークを持っていること。**CDNのデータセンターの数が多いほど、エンドユーザーに近くなります。中国の三大ISPのカバー率が高ければ高いほど、エンドユーザーのリクエストにかかるネットワークホップは少なくなります。
- **中国国内でDNSクエリを解決できること。**DNS解決プロセス(ドメイン名をIPアドレスに変換するプロセス)は、他のサイトコンテンツがローカルにキャッシュされている場合でも、トラフィックが中国を出入りする必要がある場合に、遅延を発生させる可能性があります。
- **WebサイトのHTML、CSS、およびJavascriptコードを最小限に抑えていること。**これらのコードは、ほとんどのWebサイトの構成要素であり、エンドユーザーのブラウザがWebサイトの表示させるために使用します。「縮小」とは、コードから不要な文字を削除し、全体のサイズを縮小することで、ネットワークを通過するときの帯域幅を少なくするプロセスです。帯域幅が少なくなると、サイトのロード時間が短くなります。
- **ネットワークエッジでサーバーレスコードを使用して、リクエストに応答するためのカスタムルールを作成していること。**サーバーレスコードは、開発者が制御する特定のサーバーに限定されないコードです。サーバーレスコードは、ネットワークエッジ上で実行すると、大規模なデータセンターのネットワーク全体に拡散されます。これは、コードが特定のエンドユーザートラフィックに特別なルールを簡単かつ迅速に適用できることを意味します。たとえば、モバイルユーザー、低速のインターネット接続、およびその他のユースケースに合わせて特別なルールを適用するサーバーレスコードを中国ベースのネットワークに書き込むことができます。

CloudflareとJD Cloudとのネットワークパートナーシップは、グローバルパフォーマンスサービスとともに、トラフィックのボトルネックと不十分なピアリングの両方を克服するのに役立ちます。このホワイトペーパーの次のセクションに移動して、その方法を確認してください。

中国国内での持続的なサイバー攻撃

他の地域と同様に、中国で運営されているWebサイトもさまざまなセキュリティの脅威にさらされています。

このような脅威の1つは、分散型サービス拒否(DDoS)攻撃です。DDoS攻撃は、サーバーやネットワークインフラストラクチャを迷惑トラフィックで過負荷状態にし、正当なリクエストに応答できなくすることです。Talos Intelligenceの2017年のレポートによると中国では、サイバー攻撃に詳しくないユーザーでもサイバー攻撃を依頼できる「雇われDDoS」が急速に増えています。「雇われDDoS」は、感染されたデバイスで構成された既存のボットネットを利用してサイバー攻撃を行います。

それ以来、中国の法執行機関は、2019年に20万台以上のデバイスを感染させ、200 Gbps以上の攻撃を開始したものを含む、いくつかの主要なDDoSボットネットをシャットダウンしています。しかし、DoubleGunsなどの他のボットネットはまだ健在で、そのオペレータは、この論文の出版時点でまだ捕まっておりません。

中国で展開しているWebサイトはまた、プライベートデータや開発環境にアクセスしようとする試みを防ぐ必要があります。2018年、サイバー攻撃者は人気のPHPフレームワークの脆弱性を悪用し、45,000を超える中国のWebサイトのサーバーにアクセスしようとしました。フレームワークへの攻撃は、脆弱性が公開されてから24時間以内に開始されました。同様に、2020年に中国を拠点とする2人のサイバー攻撃者が、Webアプリケーションのさまざまな脆弱性を利用して、10年間にわたって数百の企業のプライベートネットワークに不正にアクセスしたとして起訴されました。

さらに、中国で個人データを保護したい組織は、他国で使用している手段が使えない可能性があります。中国のネットワークは、TLS1.3やEncrypted Server Name Identification（ESNI）などの最新の暗号化標準がないため、トラフィックが権限のないオブザーバーに傍受されるリスクが高くなります。

中国国内の持続的なサイバー攻撃に対抗する方法

世界中でDDoS攻撃が増加しているため、DDoS軽減サービス（およびWebアプリケーションファイアウォール（WAF）などの他のアプリケーションセキュリティツール）は、アクティブなWebサイトにとっての最低限のセキュリティ要件になりました。中国も例外ではありません。この地域でそのような保護を求む組織は、以下を採用を検討してください：

- **限りのある「スクラビングセンター」ではなく、ネットワークエッジで実施するDDoS軽減策。**ほとんどすべての最新のDDoS軽減サービスはクラウドで動作しますが、悪意のあるトラフィックをフィルタリングまたは「スクラブ」するために限られた数のデータセンターに依存している場合も少なくありません。検証のためにこれらの「スクラビングセンター」までトラフィックを迂回させると、追加のネットワークホップが必要になり、ネットワークの制限がある中国では特に、遅延とユーザーの混乱を引き起こす可能性があります。中国でのインターネットパフォーマンスに影響を与えることなくDDoS軽減を提供するには、余分なネットワークホップが発生しないように、すべてのエッジデータセンターでDDoSを提供するクラウドサービスを検討すべきです。
- **不正使用を阻止するためのレート制限。**トラフィックスパイクによる予想外のコストを回避しながら、高精度のレイヤー7 DDoS攻撃の軽減、APIの不正使用の阻止による可用性の確保、ブルートログイン攻撃からの機密性の高い顧客情報の保護、オリジンサーバーのリソース枯渇からの保護など、きめ細かな制御が不可欠です。

- **自動的かつ迅速に更新されるWAF。**中国国内のサイバー攻撃者が、新しいWebアプリケーションの脆弱性をすばやく悪用できることは証明されています。組織は、独自のWAFルールを作成したくても、独自の脅威インテリジェンスと更新機能だけに頼るべきではありません。観察された脅威の幅広いプールに基づいて自動的に更新されるWebアプリケーションファイアウォールを検討すべきです。また、組織が独自のルール更新を行う際には、それらの変更が迅速に伝達されることを確信しなければなりません。
- **カスタマイズ可能な暗号化の手段。**TLS 1.3とESNIがない状態で転送中のデータを保護するために、組織は、カスタマイズ可能な暗号化方式を幅広く提供するセキュリティサービスを検討すべきです。

当社のチャイナネットワークの一部として利用できるCloudflareのセキュリティサービスは、遅延のないDDoS軽減と、グローバルな脅威インテリジェンスを利用した迅速に更新可能なWAFを提供します。詳細については、このペーパーの次のセクションに移動してください。

Cloudflareが中国で運営されているグローバルWebサイトをどのようにサポートしているか

Cloudflareは、100か国の200のグローバル都市にまたがるデータセンターのネットワークを運営しています。中国では、2022年3月現在、38都市に45のデータセンターが展開されています。各データセンターは、コンテンツ配信、DNS解決、DDoS軽減、WAF施行、サーバーレスコードの実行など、幅広いセキュリティ、パフォーマンス、リライアビリティのサービスを実行できます。各サービスはすべてのデータセンターで動作するため、エンドユーザーの近くで機能することが可能です。これにより、遅延が短縮され、ネットワークは最新の脅威とネットワークの状態に関する詳細を把握することができます。しかも、組織はこれらすべてのサービスを1つのダッシュボードから管理できます。

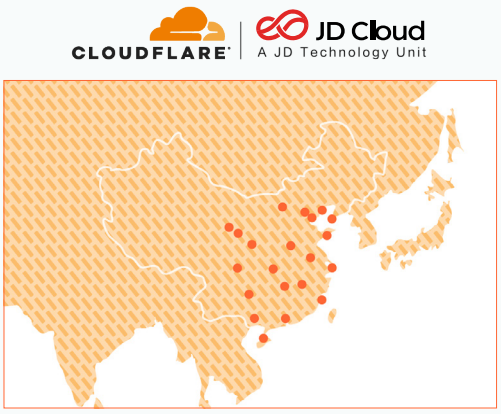
Cloudflareは、2015年から組織のお客様が中国在住の訪問者に対してセキュアで高速、安定したインターネット体験を提供できるように尽力してきました。そのサービスを改善するために、当社は中国インターネット大手JD.com（京東商城）のクラウド＆インテリジェントテクノロジー部門であるJD Cloudとのパートナーシップを締結しました。

このネットワークが、組織が前のセクションで取り上げた課題を克服するのにどのように役立つかを次に示します。

Cloudflareがレイテンシーの克服にどのように役立つか

Cloudflareと中国でのJDクラウドのネットワークは、次のものを提供しています：

- **Argo Smart Routing:**クライアントからオリジンへの往復のデータ転送は、遅延を発生させることがあります。キャッシュの使用により、静的コンテンツはネットワークの混雑を避けることができますが、動的コンテンツはインターネットの可用性、信頼性、パフォーマンスに依存します。その結果、ロードタイムの遅延、タイムアウト、接続の切断、エンドユーザーエクスペリエンスの低下を招く可能性があります。**Argo Smart Routing**は、**リアルタイムで混雑を検知し、webトラフィックを最も高速で信頼性の高いネットワークパスにルーティング**する独自の機能を備えています。Cloudflareのお客様とそのユーザーからのCloudflareのネットワークへのリクエストは、インターネットのさまざまな部分が特定の時点でどのように機能しているかを理解するのに役立ちます。Argo Smart Routingは、Cloudflareが収集したタイミングデータを使用して、**トラフィックをオリジンに戻る最速のパスに動的にルーティングし**、パフォーマンスを向上させることができます。平均すると、ArgoはWebアセットのパフォーマンスを約30%向上させます。そして、これは結果的にお客様の売上や維持率の向上につながります。
- **中国国内の多くのデータセンターからの静的コンテンツのキャッシュと提供により**、エンドユーザーの配置場所に関係なく、レイテンシーが短縮され、ページのロード時間が短縮されます。当社のネットワークは、すべての中国のISPと密接に相互接続されており、トラフィックに必要なネットワークホップの数を減らしています。



中国本土のデータセンター

- **中国国内でのDNS解決（オプション）が可能になり**、応答時間が短縮されます。
- 効率的なルーティングとパケット処理を可能にする**インターネットプロトコルバージョン6(IPv6)を使用する**機能。
- Cloudflareダッシュボードのボックスをチェックすることで簡単に有効化できるAuto Minify機能を使用して、**ウェブサイトコードを最小限に抑える**ことができます。
- 当社の中国ネットワークのすべてのデータセンターで動作するCloudflare Workersサービスを介した**サーバーレスコンピューティング。**これにより、カスタマイズ可能な方法で特定のリクエストに応答し、既存のアプリケーションを強化することができます。また、インフラストラクチャを構成または保守することなく、まったく新しいものを作成することさえ可能になります。

Cloudflareが中国国内の持続的なサイバー攻撃に対抗する方法

当社の中国ネットワークに統合されたセキュリティサービスにより、組織は以下のことが可能になります。

- **DDoS攻撃を軽減します。**中国にある当社のデータセンターはすべて、攻撃を軽減でき、正当なリクエストを逃すことなく、世界中のCloudflareデータセンターに依存することなく、最大級の攻撃を受けられる巨大な容量をネットワークに提供します。トラフィック検証はエンドユーザーの近くで行われるため、そのリクエストは遠くの「スクラビングセンター」に迂回されずに済みます。また、中国のネットワーク課題への対処法として、Cloudflareは攻撃トラフィックの自動ルーティングを可能にする独自の自動トラフィックエンジニアリング機能を提供しています。これらの機能はすべて、中国内外の正規なトラフィックに対するパフォーマンスの低下を防ぎます。
- Cloudflare WAFで**Webアプリケーションの脆弱性を保護します。**WAFは、管理されたルールセット（OWASPやCloudflare独自のルールの実装など）により既知の攻撃ベクトルを阻止するだけでなく、ネットワーク全体から継続的に得られる脅威インテリジェンスを利用して、最新の脅威を自動的に阻止できます。さらに、組織は独自のルールを簡単に作成し、数分でネットワーク全体に伝達させることができます。2021年に行われた改善により、WAFはより迅速にデプロイされ、より多くのトラフィックをカバーするために容易に拡張できるようになりました。また、WAFのルールセットも更新され、ルールのステータスとアクションを分離した、より優れた制御を提供します。ユーザーは、高度なフィルタリング、一括編集、ルールタグなどを使用して、より適切なルールブラウジングが可能になりました。
- **レート制限**は、当社のWAFカスタムルールと統合されており、DDoS攻撃、ブルートフォースログイン試行、オリジンサーバーの過負荷、APIやアプリケーションを標的としたその他のタイプの不正行為から保護します。ユーザーは、しきい値の設定、トラフィックの定義、応答のカスタマイズを行い、Webサイト、アプリケーション、またはAPIエンドポイントの特定のURLに関する貴重な洞察を得ることができます。
- **TLS 1.2を使用してデータを暗号化し**、Cloudflareダッシュボードから独自の認定を簡単に管理できます。

詳細

Cloudflareのチャイナネットワークサービスは、Cloudflare Enterpriseのすべてのお客様がご利用になれます。また、中国の法規制に完全に準拠しており、有効なインターネットコンテンツプロバイダー（ICP）ライセンスがチャイナネットワークへの接続の必須要件となっています。

中国のインターネット経済が成長し続けるにつれ、セキュリティとパフォーマンスの新たな課題が必然的に現れます。Cloudflareの中国での継続的な成長計画は、当社のネットワーク上の企業がこれらの課題に迅速に対応できるようにし、シームレスなユーザーエクスペリエンスの水準を引き上げ続けます。

今すぐCloudflareにご連絡ください。中国でのWebプレゼンスの最適化を今すぐ始めましょう！

Cloudflareチャイナネットワークの詳細については、cloudflare.com/network/china/またはCloudflare担当者までご連絡ください。