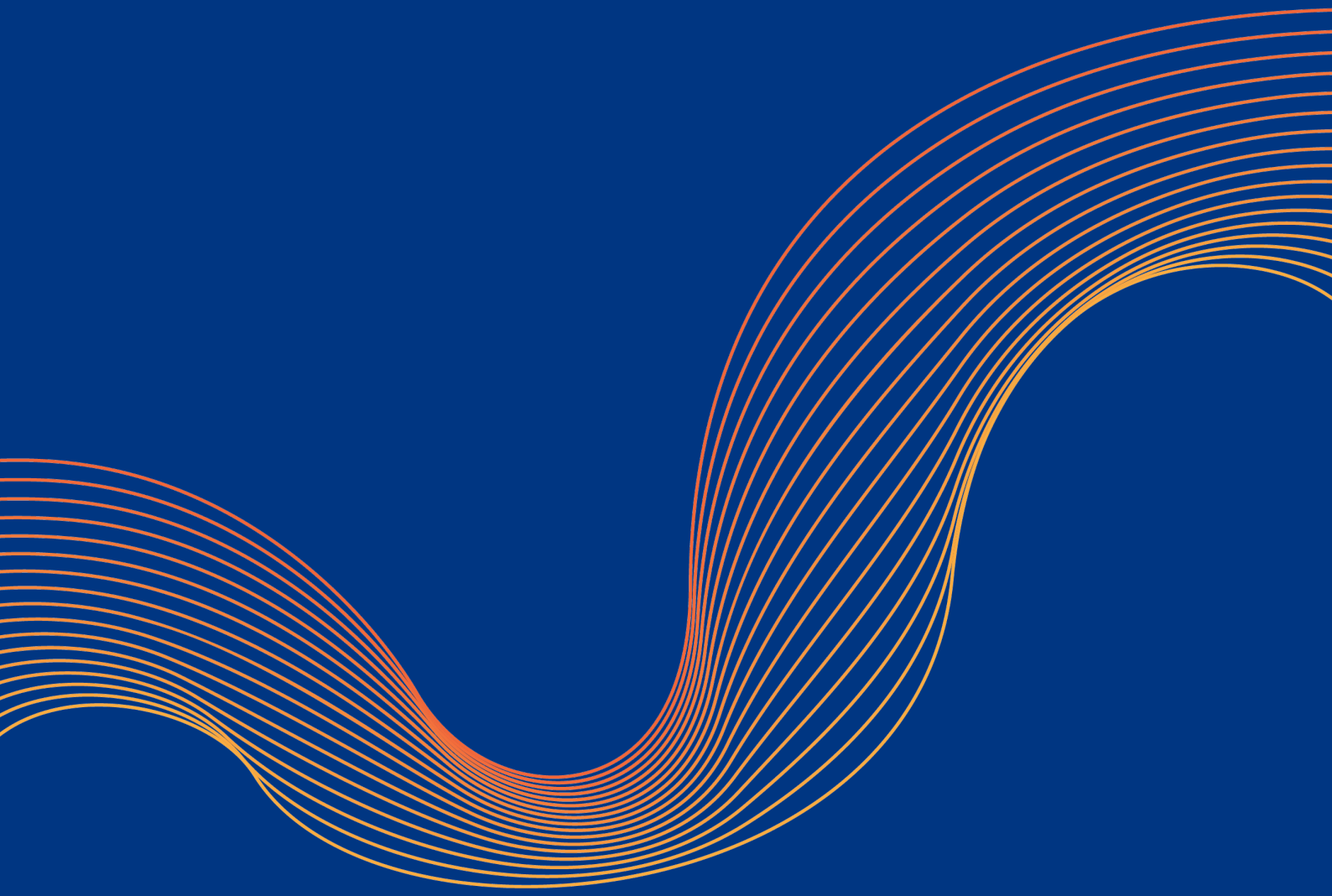
CLOUDFLARE

ホワイトペーパー

Cloudflareのネットワークがデータプライバシーを維持する方法



03-4510-1893 | enterprise@cloudflare.com | www.cloudflare.com/ja-jp/

目次

はじめに

Cloudflareのネットワークとビジネスのすべてが、お客様の信頼の上に成り立っています。当社は、このシステム上でお客様とエンドユーザーのデータ管理方法の指針となるプライバシー第一主義のポリシーと手順だけでなく、当社の製品とサービスにプライバシー保護を構築することで、その信頼を獲得し続け、維持することを目指しています。このような理由から、このシステムのセキュリティを継続的に向上させ、保存データも転送中のデータも暗号化しています。そして、世界中にある様々なロケーションでトラフィックがどのように検査されるかをお客様が決定できるようにします。

このホワイトペーパーでは、データがCloudflareのネットワークを移動する際や、ネットワークからメタデータを分析する際に、どのようにセキュリティ対策を使ってデータを保護するかについて詳細に説明します。

パート1では、データセンターのグローバルエッジネットワークをデータがどのように横断するか、プライバシーを保証するためにどのように暗号化をネットワークに組み込むかについて説明します。

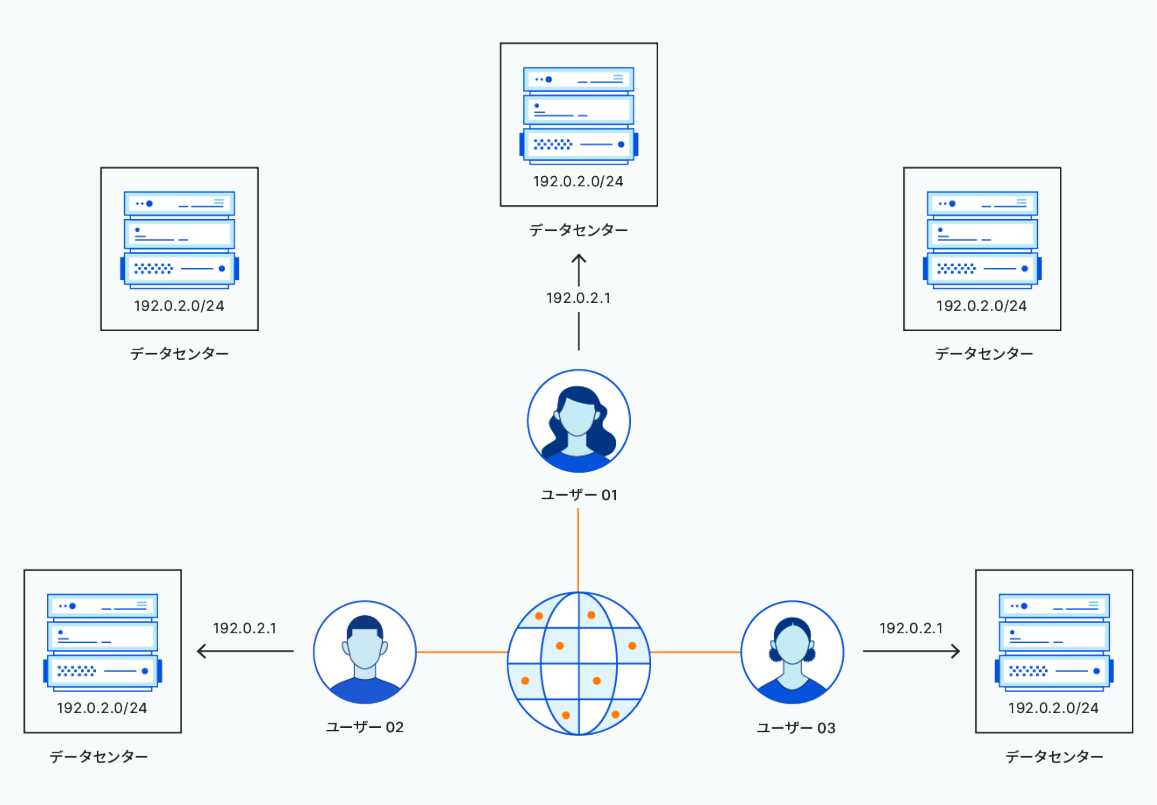
パート2では、Cloudflareがエッジネットワークから収集したメタデータを保護するためにどのように暗号化を使用するかについて説明します。

パート3では、暗号が解読されないための暗号化キーの保護について触れています。

パート1：CLOUDFLAREネットワーク内でのデータの動き

Cloudflareネットワークには、世界100か国200都市以上に広がるデータセンターがあります。優れたレジリアンスと高速パフォーマンスのために、エニーキャストネットワークとして構築されています。つまり、どのロケーションでもすべてのCloudflare IP アドレスをアナウンスします。この構造により、Cloudflareネットワーク上のWebサイトまたはアプリケーションにリクエストするユーザーは、常に最も近い場所にあるデータセンターへと送られます。

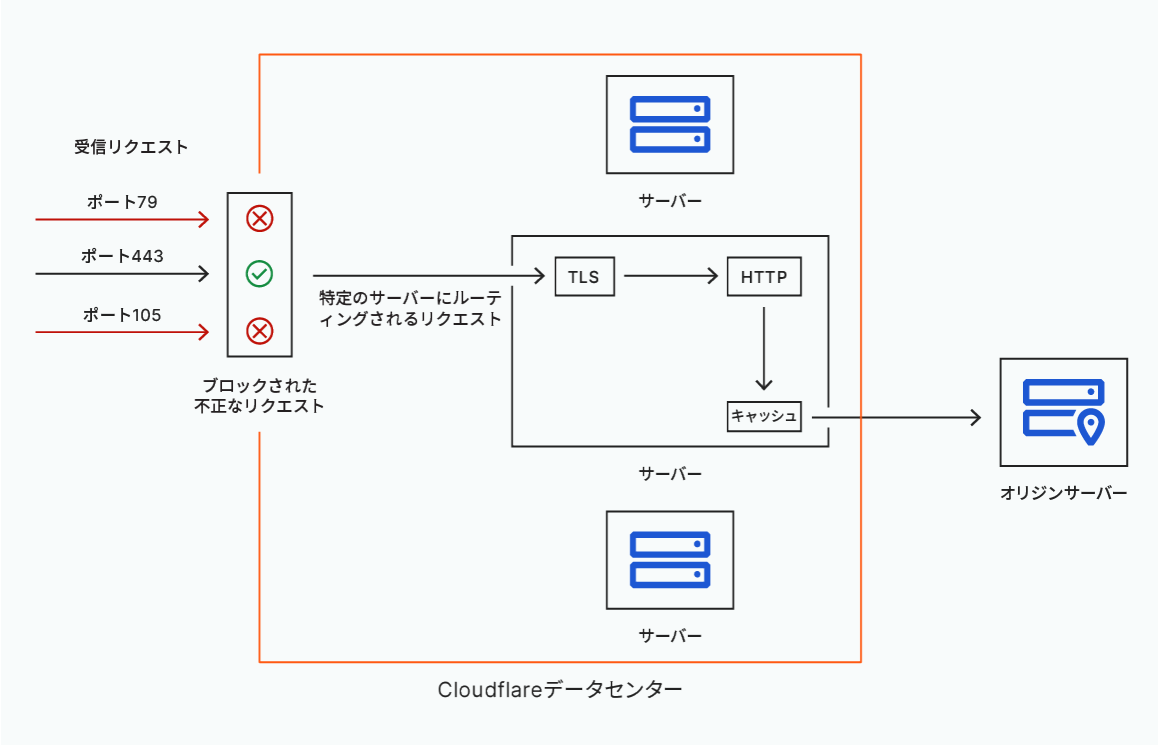
ドイツのケルンにいるカテリーナがCloudflareネットワーク上にあるWebサイトを読み込むとしましょう。カテリーナのWebサイトへのリクエストは、ドイツのデュッセルドルフにあるCloudflareデータセンターに送られます。これはわずか45キロ（ほど）の位置にあります。それでは、次の日にカテリーナはフランクフルトにドライブに行き、そこで同じWebサイトを読み込むとしましょう。フランクフルトにあるCloudflareデータセンターがデュッセルドルフにあるデータセンターと同じIPアドレスをアナウンスするため、カテリーナからのリクエストはフランクフルトのデータセンターに送られます。



パート1：CLOUDFLAREネットワーク内でのデータの動き

カテリーナのようなユーザーのデバイスが一度Cloudflareデータセンター（どのセンターかに関係なく）に接続されると、そのリクエストは次のように処理されます。

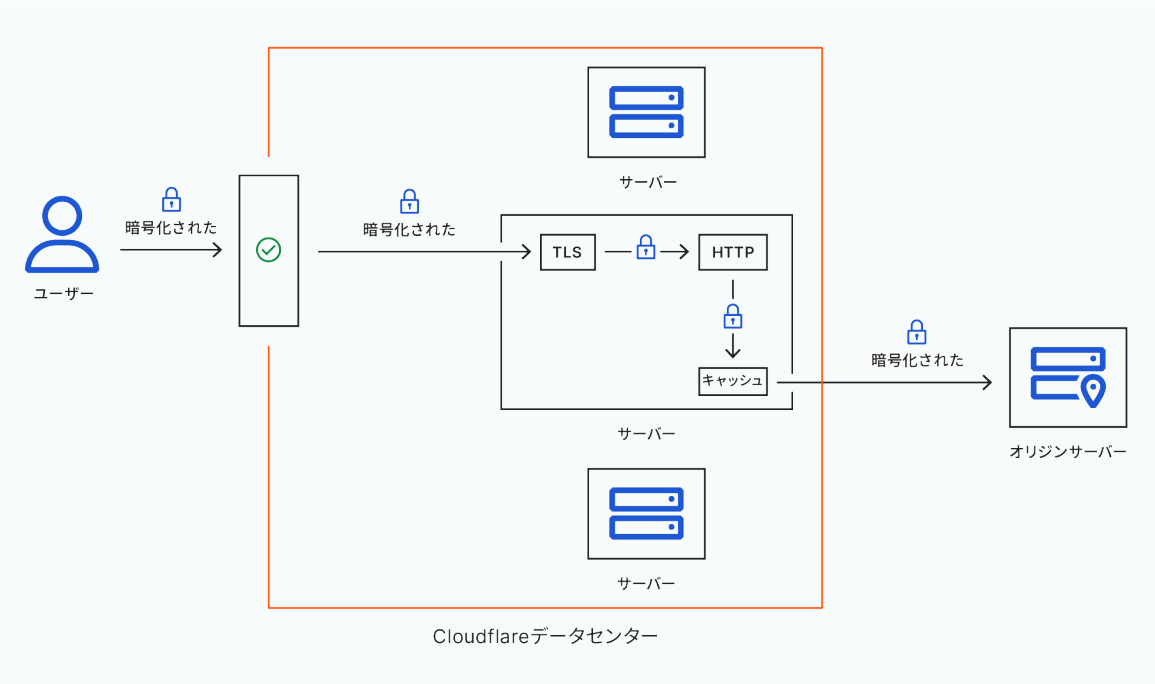
- サイバー攻撃に使われる可能性があるデータを要求する特定のリクエストはアドレス情報に基づき、すぐに削除されます。
- 次にリクエストは、お客様にリクエストされたビジネスロジック（ページルール、ファイアウォールール、レート制限など）を使って検査されます。これにより、レイヤー7DDoS攻撃、自動化されたボットトラフィック、クレデンシャルスタッフィング、SQLインジェクションなど種々多様なサイバー攻撃と悪意のあるトラフィックの検出や防止が可能になります。
- その後で、リクエストはキャッシュに渡されます。キャッシュがコンテンツのキャッシュされたコピーでリクエストを実行できる場合は、それを実行します。そうでない場合は、インターネット上でお客様のオリジンサーバーにリクエストを転送します。お客様側でCloudflareサーバーとオリジンサーバー間のトラフィックの暗号化を有効にしている場合は、トラフィックが暗号化されます。
- レスポンスの発信元がお客様のオリジンサーバーである場合、静的コンテンツはすべて暗号化されたディスクにキャッシュされます。それから、チェーンを通してインターネット上でユーザーに送信されます。



パート1：CLOUDFLAREネットワーク内でのデータの動き

HTTPリクエストのプライバシー

Cloudflareはお客様のご指示に従い、エンドユーザーとCloudflareデータセンター間で転送中の全データにTLS暗号化の使用を強制します。データの移動のみに関わる中間ネットワークであっても、悪意ある攻撃者であっても、中間にあるサードパーティが暗号化されたデータを表示することは不可能なので、機密性と安全性を確保できます。



データセンター内やデータセンター間、Cloudflareネットワークとお客様のオリジン間のトラフィックも暗号化されます。さらに、Cloudflareデータセンター内のすべてのリクエストとレスポンス処理はメモリ内で行われます。キャッシュされた静的コンテンツ以外ディスクには何も書き込まれません。そして、すべてのキャッシュディスクは暗号化されます。

Cloudflareの地域サービスを使用してデータが移動する仕組み

多くのCloudflareのお客様から、データ処理の場所と方法に対するきめ細かな制御に関心があるという声が寄せられています。

Cloudflareの地域サービスを利用することで、Cloudflareのお客様はデータの検査場所を指定できます。地域サービスをアクティブにしているお客様のために、Cloudflareネットワークはリクエストも上記と同様の方法で処理します。リクエストは特定の地域内にあるデータセンターに到着した時にのみ、サイバーセキュリティのリスクを検査され、キャッシュされるという点が大きな違いです。

エンドユーザーのリクエストが（ネットワークホップの数で測定される「直近」の）データセンターに移動する点も変わりません。データセンターが特定地域外にある場合は、リクエストはビジネスロジックが適用される前に指定された地域内のデータセンターに転送されます。地域サービスのお客様には専用IPアドレスが割り当てられ、この地域固有の処理が使用可能となります。それと同時にグローバルなDDoS攻撃対策のメリットも受けられます。

パート2：データ収集とプライバシー

Cloudflareがエッジから収集するデータとは？

Cloudflareのビジネスがユーザーの追跡や広告販売に関連して構築されたことは一度もなく、個人データの収集は最小限に抑えられています。Cloudflareがネットワークの円滑な運営を維持し、サービスを最適化するためにデータセンターのグローバルエッジネットワークから収集するメタデータは、本質的に技術的なものです。メタデータには極めて限定された個人データが含まれますが、ほとんどの場合、IPアドレスの形式です。収集されたデータは、処理のために米国のコアデータセンターに送信されます。

Cloudflareが収集したメタデータは次の3つのメインカテゴリーに分類されます。

1. **システムメトリクスとデータのデバッグ**
2. **Cloudflareのデータ分析製品のためのデータ収集**
3. **CloudflareのネットワークをHTTPリクエストメタデータ**

詳細は、以下のとおりです。

1. システムメトリクスとデータのデバッグ

Cloudflareは、特定のデータセンターが受信した1分あたりのリクエスト数やデータセンター間のラウンドトリップ時間（RTT）など、サーバーとネットワークパフォーマンスに関する様々なメトリクスを収集し、処理します。これらのメトリクスは、前後関係を取り除き、集約された統計情報として収集されます。個人データを含まれない、これらの集約統計情報は、処理のために当社のコアデータセンターに送信され、エッジからコアに送信された全データは、転送中にTLSで暗号化されます。

Cloudflareはエッジネットワーク上で動作するソフトウェアすべてから、通常のメンテナンスのためにデバッグ情報も収集します。

このデータ収集はいずれも、CloudflareネットワークとCloudflareサービスを正常に運用するためにのみ必要なものです。データの転送中にTLSで暗号化されるだけでなく、データのすべてがハードディスク暗号化によってコアデータセンターで保存中も暗号化されます。

2. Cloudflareデータ分析製品

Cloudflareは、Cloudflareのサービスと Cloudflareをより効果的に活用する方法を理解していただくために、顧客データ製品を提供しています。当社のデータ製品はお客様が自社のオリジンサーバーをより適切に保護してサービスを構成し、ビジネスとシステムの動作を理解するのに役立ちます。

当社のデータ製品はすべて、エッジのデータセンターで動作するソフトウェアに関するメタデータから生じています。たとえば、CloudflareではHTTPリクエストにURL、Cloudflare機能の何が使用されたかという情報、タイミング情報、キャッシュ情報、一部のHTTPリクエストとレスポンスヘッダーを組み込みます。同様に、 CloudflareはDNSリクエスト、TCPフロー、Accessログイン、Stream動画ビュー、当社の全製品に関するメタデータを収集します。また、プライバシー第一のWeb分析サービスをお客様に提供し、ユーザーがお客様のWebサイトをどのように閲覧しているかを知るきっかけとなっています。

お客様がCloudflareのログを有効にしている場合、この機能によりすべてのイベントに関する詳細情報がお客様に提供されます。このデータは転送中に暗号化されて、エッジネットワークからコアデータセンターに送り返され、お客様にプッシュされます。お客様は、コアデータセンターで暗号化されたログデータを最長7日間保存することもできます。

分析とログはどちらもエッジネットワーク間とお客様同士の間で送受信されるデータを暗号化します。

パート2：データ収集とプライバシー

3. ランダムサンプリングされたHTTPトラフィックデータのCloudflareでの使用

CloudflareではCloudflareのネットワークを通過した全HTTPトラフィックの単純無作為サンプルを保存します。このデータは匿名化され、インターネットプロパティ全体で個々のユーザーを追跡するために使われることはありません。Cloudflareには、いずれかのIPアドレスを自然人に結び付ける手段はありません。収集されたすべてのサンプルデータは、暗号化された接続を介して転送され、安全なハードディスク暗号化を使用して保存され、限られた期間（最大12か月）保持されます。Cloudflareではサンプルデータを使用して、悪意のあるアクティビティを診断し、お客様のインシデントを調査し、セキュリティ製品の全体的な有効性を向上させます。Cloudflareのすべてのお客様は、ネットワーク全体でサンプリングされたデータの累積インテリジェンスの恩恵を受けます。

パート3：暗号化キーの保護

暗号化は、お客様のコンテンツとメタデータがネットワーク上を移動するうえで、その機密性を保護するために使う技術的な対策の根幹を成すものです。ネットワーク上の暗号化されたデータが、サードパーティによって解読されることはありません。これは機密性という点において、重要な意味を持ちます。暗号化キーの安全性が守られれば、暗号で保護されるコンテンツのプライバシーは守られます。

セキュリティ企業として、Cloudflareは暗号化キーの保護を最重要視しています。暗号化キーのセキュリティを確保するために、Cloudflareでは厳格な物理的セキュリティ基準とアクセス制御を整備しています。Cloudflareでは長年、透明性レポートに明記しているように、Cloudflareの暗号化や認証キー、お客様の暗号化、認証キーにアクセスを試みようとする政府機関とは断固闘うことを宣言してきました。

暗号化キーの秘密を守り、保護することがどれだけ重要であるかを考えると、堅牢なアクセス制御システムを構築するだけでなく、お客様が独自の暗号化キーに対してきめ細かな制御ができるオプションを持てるようにすることが不可欠だと考えています。データセンターのきめ細かな制御とともに、キーが保存される地理的な地域を限定したいお客様には、Geo Key Managerをご利用いただけます。当社のSSLサービスを引き続き使いながら、プライベートキーをオンプレミスで管理したいとお考えのお客様には、Keyless SSLをご利用いただけます。

まとめ

Cloudflareの使命はより良いインターネット構築をお手伝いすることであり、データプライバシーは、その中核であると信じています。この10年間、お客様とインターネット全体のプライバシーとセキュリティを確保するための新しい方法を見つけるために努力を重ねてきました。そして、その姿勢はこれからも変わりません。

CLOUDFLARE

ホワイトペーパー