CLOUDFLARE®

良質なオンライン体験を提供するインフラストラクチャの構築方法

+81 3 4510 1893 | enterprise@cloudflare.com | www.cloudflare.com/ja-jp/

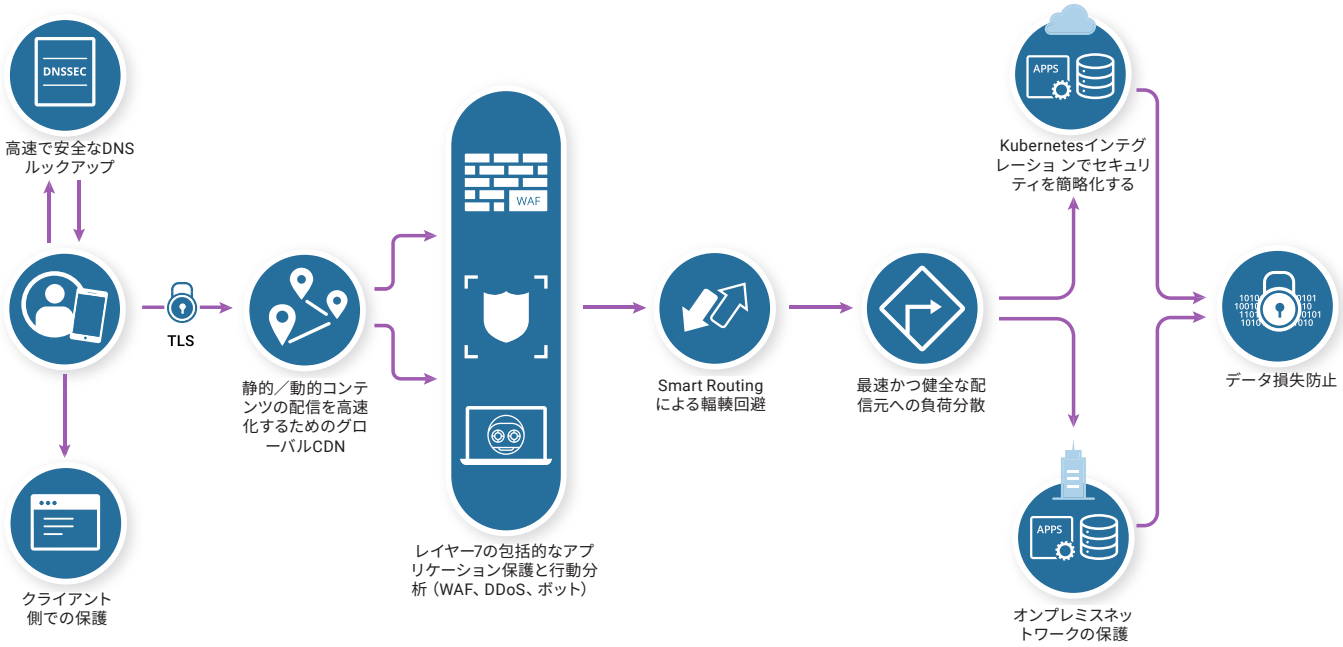
目次

はじめに

世界中のお客様に良質なオンライン体験を提供することは、必須だと言えます。Webベースのサービスとアプリケーションへの需要の高まりに合わせて、企業はWebサイトとアプリケーションを可能な限り安全で、高速で、信頼性のあるものに維持すると同時に、お客様のニーズを満たしていかなければなりません。

こうした変化により、お客様のデジタルニーズを予期してそのニーズを満たすことから、Webベースの攻撃に対する強力な防御、レイテンシー問題の克服、サイト障害の防止、ネットワークの接続性とパフォーマンスの維持まで、企業は新しい挑戦に直面しますが、成長するチャンスを得ることにもなります。

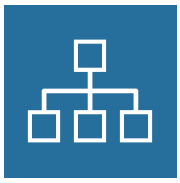
良質なオンライン体験の構築が必要とするのは、単一のツールや製品スイートだけではありません。下図が示すようにレイテンシーの短縮、ネットワークの信頼性を向上させる包括的なセキュリティに対する取り組みとパフォーマンス機能も必要とします。



本書では企業がお客様のニーズを満たし、安全でシームレスなユーザー体験を提供するために必要となる5つの重要なステップをご紹介します。

ステップ1

お客様が安全・高速・確実に接続できるようにする



DNS

DNSはインターネットベースのビジネスにとって不可欠なコンポーネントですが、問題が発生するまで見落とされる傾向があります。DNS攻撃の多発にともなって、企業は耐障害性のあるDNSの不足が、セキュリティ戦略全体の弱点となっていることに気づき始めました。アプリケーションが利用できなくなり、お客様が見つけられなくなってしまっては、Webプロパティの構築と確保に投入した何百万ドルもの費用が無駄になります。

DNSにおける課題

高いレイテンシー：Webページが複数のドメインから頻繁にアセットを読み込むと、リクエストされた各ドメインの解決に要する時間が長くなり、Webパフォーマンスの点で問題が発生することがあります。

社内DNSインフラストラクチャ：自己ホストのDNSは維持にコストがかかり、グローバルに分散した顧客ベースの場合、DNS解決が遅くなり、レイテンシーが増える可能性があります。そして、高度なDNS攻撃に対して完全な保護がありません。

小規模ネットワークDNSプロバイダー：DNSソリューションを選ぶ際に、企業は大きなネットワークを持たなかったり、すべてのデータセンターでDNSソリューションを実行できないプロバイダーを選択するという間違いをすることがよくあります。特に世界中の様々な地域のお客様にサービスを提供する企業にとって、これはパフォーマンスと信頼性を頭打ちにする可能性があります。

DNSプロバイダーに必要なこと

総合的なセキュリティソリューション：DNS脅威は多種多様なので、効果的にDNS攻撃を軽減するには、DNSSEC、DDoS攻撃軽減策、DNSファイアウォールなどを含む総合的なセキュリティ戦略が必要となります。独自にDNSインフラストラクチャを維持したいと考える大企業では、DNSファイアウォールをセカンダリDNSと組み合わせて実行することができます。このセットアップにより、オンプレミスのDNSインフラストラクチャにセキュリティレイヤーが追加されることになり、DNS冗長性全体の確保に役立ちます。

高速DNS解決：クラウドベースのマネージドDNSプロバイダーを考えている企業にとって、高速DNS解決とジオベースの動的なルーティングで、パフォーマンスと可用性を最大限に広げるプロバイダーを選択することは必要不可欠です。

冗長性：1つのプロバイダーでDNSレコードをホストすることを選んだ企業は単一障害点に依存することになり、システム停止が起きやすくなります。耐障害性を最大限にするために、複数の個別マネージドDNSプロバイダーのサポートを求めるだけでなく、こうしたプロバイダーが同じネームサーバー設備を共有していないことを確認する必要もあります。

クライアント側のセキュリティ

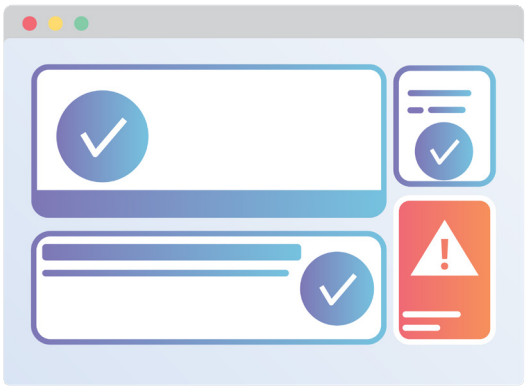
現在、ユーザーのブラウザーで実行し、レンダリングするコードの最大70%[1]が監視されていない外部のJavaScriptインテグレーションから来ています。これは、Magecart、クロスサイトスクリプティング（XSS）、クレジットカードスキミング、Webサイト改ざん（website defacement）などさらに悪質なクライアント側の攻撃に発展する新しい道を開くことになります。

サーバー側のセキュリティツールは、クライアント側の脅威に対して可視性があるとしても、それは限定的で、攻撃を防止することも脆弱性にパッチを適用することもできません。Webプレゼンスのある企業は、こうした発生頻度が高く急速に進化する脅威に対してWebサイトを守ために、専用のクライアント側保護を展開し、維持することは必須です。

クライアント側の攻撃

クロスサイトスクリプティング（XSS）：XSS攻撃は、攻撃者が正規のWebサイトに悪意のあるコードを添付または挿入したときに発生します。ユーザーログイン資格情報を盗む、他の機密情報にアクセスする、ユーザーブラウザーを乗っ取ることが目的です。

Magecart攻撃：Magecart攻撃は、「データスキミング」の一種で、攻撃者は悪意のあるコードをWebサイトに挿入し、オンライン支払い用紙から機密のユーザーデータ（クレジットカード番号、パスワードなど）をスクレイピングします。この種の攻撃は、攻撃者が害のないコード内に悪意のあるコードを隠したり、盗んだデータをエンコードしたりするため、攻撃者は検出されることなく戻ることができ、企業が検知するのがより難しくなっています。



スプーフィング：信頼されるソースになりすますことで悪意のある通信を偽装して、攻撃者が機密性の高いユーザーデータを盗んだり、DDoS攻撃を起こすようにトラフィックのルーティングを変更したり、組織のシステムやネットワークに不正アクセスをしたりすることです。

[1] Bermingham, Mark. “Redefining Client-Side Security with the Tala Security Certified Module for NGINX Plus,” NGINX, https://www.nginx.com/blog/redefining-client-side-security-tala-certified-module-nginx-plus/

クライアント側のセキュリティソリューションで必要なこと

エンドツーエンド保護：企業はクライアント側の脅威だけに的を絞るのではなく、バックエンドインフラストラクチャと同様にフロントエンドプロセスも保護する必要があります。

パフォーマンスへの影響を最小限に抑える：厳格なセキュリティプロトコルの導入と管理が多くの企業にとって最重要課題であると同時に、こうしたセキュリティ製品がWebパフォーマンスを干渉しないことも重要です。Webサイトの動作が遅くなることで潜在的顧客の興味を失わせ、直帰率が上がり、コンバージョン率が低下する恐れがあります。

TLS

機密データを保存して送信する企業は、データの漏えい、悪用、盗難を防止する方法を見つける必要があります。「SSL」と呼ばれることが多いTLSネットワークプロトコルは、パブリックネットワークでの通信を暗号化し、信頼できる相手に承認を与えるやり方で、これを遂行します。このようなプロトコルは、お客様のプライバシーを守り、サードパーティの監視や改ざんからデータを保護するのに役立ちます。

TLSの課題

SSL/TLS証明書の管理：SSL/TLS証明書は信頼できる機関の身元を確認するためにデザインされていますが、不正行為者に侵害されたり、操作されたりするかもしれません。こうした証明書は誰でも購入できるので、攻撃者が証明書を使って信頼できる当事者になりすまし、セキュリティ手順をすり抜け、機密データへのアクセス権を得ることも起きてしまいます。

最新の状態に保つ：SSL/TLSの後続バージョンは既知の脆弱性にパッチを適用し、攻撃に対するWebサイトの防御を強化しようと試みています。暗号化されたプロトコルの旧バージョン (たとえばTLS 1.1または1.2) を使うことで、企業はうっかり悪意のある者に既存の脆弱性を狙い、攻撃を実行する隙を与えてしまうことになりかねません。現在、Alexa Top 1000のWebサイトのうち、わずか22%しか最新版のTLSを使用していません。[2]

[2] Holz, Ralph, Amann, Johanna, Razaghpanah, Abbas, and Vallina-Rodriguez, Narseo. “The Era of TLS 1.3: Measuring Deployment and Use with Active and Passive Methods,” The University of Sydney, https://arxiv.org/pdf/1907.12762.pdf

規制と基準への準拠性の確保：多くの企業がEU一般データ保護規則（GDPR）とカリフォルニア州消費者プライバシー法（CCPA）のデータプライバシー基準を遵守しています。両方とも消費者データを盗難や不正利用から保護するためのガイドラインを規定しています。適切に顧客データトラフィックを暗号化しない企業は、マルウェアやデータ引き出しなど潜在的な脅威を見落とす可能性があります。

TLSソリューションで必要なこと

簡単な実装：SSL/TLSプロトコルを手動で設定する必要がある企業の場合、設定を間違えることでお客様がWebサイトにアクセスできなくなる可能性があります。SSL/TLSの実装を合理化し、（障害が発生した場合）テストとロールバックを簡単にする、そして最新の脆弱性をパッチするためにTLSプロトコルを自動で常に最新状態に保つプロバイダーを選択します。

柔軟性：企業のセキュリティニーズが徐々に進化するに従い、認証局が発行する証明書から自己署名の証明書まで、複数の証明書設定を提供するSSL/TLSプロバイダーが必要となるかもしれません。

コンプライアンスの遵守：包括的なSSL/TLSインスペクションにより、企業は暗号化されたデータトラフィックになりすます可能性がある潜在的な脅威を特定することができます。こうした脅威を迅速に特定し対処することで、GDPRとCCPAのような規則を確実に遵守しつつ、改ざんや盗難から顧客データを保護することができます。

ステップ2

ユーザー体験を加速させる

グローバルなCDN

リーチを拡大するための簡単で効果的な方法を求めているグローバル企業の場合、CDNはリモートのホスティング設備への投資の代わりとなる理論的な選択肢です。企業は広大なグローバルインフラストラクチャを構築する必要もなく、膨大で分散した消費者基盤に影響を及ぼすことができますが、コストがかかり管理も保守も難しい場合があります。

CDNの課題

セキュリティとパフォーマンスのトレードオフ：CDNがネットワーク問題に直面した際に耐障害性を発揮し、機密データの盗難や損失から保護する必要がありますが、セキュリティ機能を統合すると、追加のレイテンシーが引き起こされて、パフォーマンスのトレードオフにつながることがあります。

リアルタイム分析の欠如：リアルタイム分析は、結果を得るのが難しいか、大幅に遅れる可能性があります。これは、企業のWebプロパティのパフォーマンスに関するインサイトを取得する企業能力に影響します。

モノリシックなアーキテクチャ：従来のCDNはモノリシックアーキテクチャで構築されており、設定変更がネットワーク全体に反映されるまでに時間がかかります。
この種の遅れは、ポリシー変更を迅速に実装し、イテレーションを行いたい開発者をイラつかせることがあります。

CDNプロバイダーに必要なこと

パフォーマンスの改善：CDNを評価する場合、企業はまず主要なマーケットにおけるパフォーマンスがそれに匹敵しているかを判断するテストを実行するべきです。CDNプロバイダーの結果は、地域によって良し悪しが異なります。最初のテストに続き、企業はパフォーマンスの低下が許容範囲内なのか、とるに足らない程度かを他の地域における結果も考慮して評価する必要があります。

リアルタイム分析：Webドメインの使用状況やユーザー体験に関する情報が得られる分析結果とデータを世界中から収集するのは、簡単ですか。また、こうした情報の収集が遅れる原因は何ですか。

開発者にとっての利便性：開発者もエンジニアリングチームも自分たちのデジタルインフラストラクチャの構築でCDNが担う役割を決定します。企業はシームレスなAPIの統合を提供し、カスタム設定のために外部ベンダーの専門的サービスを必要としないプロバイダーを見つける必要があります。

より速いルーティング

グローバルな顧客基盤を持つ企業は、Webアプリケーションのパフォーマンスを維持する必要があります。面倒なセキュリティプロトコルから世界中のユーザーにとって今ひとつなネットワーク状況まで、レイテンシーを引き起こす要因は数多くあります。

Smart Routingは、ネットワーク輻輳と信頼性に基づいてルートを選択することで、こうした問題の軽減に役立ちます。優れたパフォーマンスを提供するパス（経路）を判断するために、BGPで実行され、利用可能なパスがテストされます。信頼性の低いネットワーク接続を回避することで、サービスの遅延やネットワークの中断を招く可能性が高いパケットの欠落を防ぐことができます。

ルーティングにおける課題

ネットワークの輻輳：ネットワークの輻輳は、十分なインフラストラクチャに欠ける特定の地理的領域に限って発生することもあれば、ISPネットワーク全体に影響していることもあります。祝日や世界的な大災害時などトラフィックが混雑する出来事が発生すると、通信やサービスを求めるユーザーがインターネットに集まり、さらに輻輳します。

ネットワークレイテンシーの増加：ネットワークレイテンシーの増加は、Webサイトのスピードとパフォーマンスに直接影響を与えます。これによって、ユーザー体験全体が低下し、コンバージョン率低下と収益減少につながることがあります。

法外な費用がかかるソリューション：専用回線とMPLS（マルチプロトコルラベルスイッチング）ネットワークは、ビジネス通信目的で専用アクセスルートを取得するために大手のサービスプロバイダーから購入することがあります。専用回線をリースする利点はいくつかありますが、ただ、実装に法外な費用がかかることもあり、収益性や他のビジネスに不可欠なサービス用の予算に影響を与えかねません。

最適なネットワークパス選択のためのツール選び

アセットパフォーマンスの向上：プロバイダーが適切な場合、企業は利用できる最速のリンクでWebトラフィックを提供することができるはずです。そして、アセットスピードとパフォーマンスで測定可能な増加とエンドユーザー体験の改善という結果がもたらされます。

リアルタイムのメトリクスと分析：企業はリアルタイムメトリクスと分析によって潜在的なルーティング問題を見極めることができ、ユーザーの所在地、デバイス、現在のネットワーク状況に関わらず、輻輳の回避、ルーティングの最適化、グローバルなパフォーマンス向上の測定、長い稼働時間の提供が可能にします。

ネットワークモニターツール：レイテンシーの削減とネットワーク輻輳を回避するために、企業は潜在的な輻輳ポイントを特定してトラフィックに優先順位をつけるため、ネットワークモニタリングツールを実装することがあります。これが、最も重要なデータトラフィックが、意図とする目的地に届いていることと帯域幅を過剰消費するアプリケーションが1つもないことを保証します。

モバイルの最適化

Webサイトをデスクトップで閲覧する時と同じように、モバイルユーザーもモバイルデバイスでのページ読み込み時間が3秒以下であることを期待しており、モバイルの最適化はWebベースのビジネスの成功に欠かせない要素となっています。もしユーザーの期待に応えることができず、高速でシームレスなモバイル体験が実現しないと、顧客はどこか他の場所に行ってしまうのです。

モバイル最適化における課題

粗末な画像の最適化：画像が小さなモバイル画面に合ったサイズとフォーマットになっていない場合、ページビューが歪み、Webページの移動が難しくなるため、ユーザー体験が悪化します。画像のファイルサイズが大きいほど、ダウンロードに時間がかかります。多くのデバイスは十分な画面解像度もなければ、必要な高解像度を作成するのに十分な大きさの画面も持たないため、その結果として、ページ読み込み時間が長くなります。

帯域幅使用率の向上：ファイルサイズが大きければ消費する帯域幅も大きくなり、ホスティングプロバイダーから高いデータ料金が課せられます。モバイルプロパティに適切な画像の最適化ソリューションを実装しなかった企業は、帯域幅コストから顧客の興味を損失やコンバージョン率や収益の損失まで多大なリスクを背負うことがあります。

厄介な内部開発：Webデベロッパーは、モバイルデバイス向けにアセット最適化のサポート作業を行うことがよくあります。この作業には、様々なデバイスタイプに対応する画像の複製を手動で行う処理の作成が含まれます。これは、長時間にわたる保守管理が必要となる別のシステムまたはプロセスとなるため、理想的なソリューションとは言えません。その代わりとして、画像の最適化にサードパーティの専用ソリューションを実行すると経費がかかり、機能使用率の面でROI（投資対効果）の低下につながることがあります。

モバイル最適化ソリューションで必要なこと

CDNの統合：モバイルの最適化は、既存のCDNサービスとシームレスに統合する必要があります。それによって、企業はキャッシュの利点を活かし、画像ファイルの冗長を扱うサービスへの依存度を軽くすることができます。適切なCDNは、ユーザーデバイス要件を検出したり、小さいファイルサイズ画像に「仮想化」したり、モバイルユーザーにできるだけ近くで画像をキャッシュしたりして、モバイルパフォーマンスの改善に貢献するものです。

社内保守 vs. サードパーティ保守：モバイルの最適化ソリューションを検討する際、社内で構築も管理もできるソリューションを比較し、どう言った種類の長期的保守とアップデートが必要となるのかを注意深く考える必要があります。こうした最適化ソリューションを拡張して、ドメイン外のサードパーティストレージをサポートできるかどうかも考慮に入れなければなりません。

ステップ3

インフラストラクチャのセキュリティ体制を強化する

Webアプリケーションファイアウォール

自社インフラストラクチャとデータの保護に積極的に取り組む企業であっても、特にセキュリティ上の欠陥が攻撃の機会を生み出してしまうこの世界でセキュリティ対策を実装することは運用上、極めて困難です。

WAFを導入すると、企業はゼロデイ攻撃を防止して、クロスサイトリクエストフォージェリ（CSRF）、クロスサイトスクリプティング（XSS）、SQLインジェクションといった一般的な脅威からアプリケーションを保護することができます。また、WAFにより、企業は、アプリケーションの脆弱性の保護および新たな脅威に対する防御力の強化に役立つルールを設定することで、セキュリティポリシーに対してきめ細かな制御を行うことができます。

WAFにおける課題

リソースを消費するオンボーディングと管理：優れたサイバー衛生の開発とビジネスに不可欠なアプリケーションの保護において、最新のインフラストラクチャパッチングは大切なコンポーネントです。しかし、最大規模のセキュリティチームであっても、パッチ修正の数が多く、多数のベンダーによるパッチリリースが速いため、通常、インフラストラクチャ全体をパッチすることはできません。WAFソリューションがこの問題を軽減するのに役立ちますが、オンボードや管理については時間がかかったり、リソースの消費が多かったりします。そのため、現在多くのWAFでこのプロセスを処理するために高い技術を持ったセキュリティの専門家が必要となっています。

柔軟性の欠如：アプライアンスベースのハードウェアWAFは、今、存在する脅威にはかなり時代遅れのセキュリティソリューションです。アプリケーションとデータは、主にオンプレミスインフラストラクチャとクラウド内のハイブリッド環境にあるため、クラウドベースのWAFはあらゆる企業の階層型防衛戦略にとって、重要なコンポーネントです。ハードウェアWAFアプライアンスとは異なり、クラウドベースのWAFは、アプリケーションとインフラストラクチャがどこでホストされているかに関わらず、脆弱性ベースの攻撃に対して保護できます。

機敏性（アジリティ）：アセットとデータの保護がセキュリティチームと悪質な行為者が絶え間ない競争を繰り広げる世の中において、機敏性がカギとなります。ハードウェアベースのWAFはルールを作成し、それを迅速にインフラストラクチャ全体に伝達する機敏なメカニズムの提供に失敗しました。脆弱性の存在が知らされてから、その脆弱性を悪用しようとする攻撃に対して保護するパッチを適用するまでの時間が、肝心です。

WAFソリューションで必要なこと

使いやすさ：WAFの選択、オンボーディング、管理に関しては、使いやすさが重要です。WAFのオンボーディングに数週間、または数ヶ月もかかってはいけません。その管理についても、多数の専門家の力を必要とするようではいけません。さらに、シームレスなAPI統合を提供してくれるWAFプロバイダーを考えるといいかもしれません。

リアルタイム脅威インテリジェンス：ハードウェアベースWAFの大きな欠点の1つとして、脅威と攻撃に対するリアルタイムのコンテキストがないことです。企業はハード話ベースWAFと脅威インテリジェンスのフィードを統合できるかもしれませんが、これは能動的ソリューションではなく、受動的ソリューションにすぎません。攻撃が急速に進化する現状では、リアルタイムの脅威インテリジェンスコンテキストは、最新の脅威情報を把握していたい企業にとって、必要不可欠です。WAFは、世界規模で多様な脅威についてのリアルタイムのコンテキストを含む必要があり、脅威インテリジェンスデータのセットの規模だけでなく、データの多様性にも注意を向ける必要があります。

包括的なサービス：攻撃者が、OWASPトップ10を含む一般的な脆弱性を悪用しようとすることがよくありますが、危険な脆弱性とゼロデイ脆弱性への関心が高まっています。包括的なWAFソリューションには、ゼロデイ脆弱性や他の危険な脆弱性を悪用しようと試みる攻撃を自動的に阻止するように定期的にアップデートされるマネージドルールのセットを含む必要があります。

ボット軽減策

悪意のあるボットはWebベースのビジネスに大打撃を与え、機密データを侵害して顧客体験全体を損なうだけでなく、企業の運営コストも直接影響を及ぼします。また、ボット攻撃はさらに高度になってきており、本物のユーザーか自動ボットか区別するのがもっと困難になっています。これは、企業をかつてないほどの大きなリスクにさらす可能性が大いにあります。悪意のあるボットに狙われた時、サイトは侵害されてしまいます。ボットはWebサーバーを過負荷の状態にし、分析を歪め、ユーザーがWebページにアクセスできないようにし、ユーザーデータを盗み、スパムをばらまき、ブランドの整合性を損ない、顧客維持と収益に影響を及ぼすことができるのです。

ただし、すべてのボットが有害であるわけではありません。ボット管理ソリューションを実装することで、有用なボットと有害なボットの区別がつけられ、ユーザー体験に影響しないように悪意のある行為を防止することもできます。

ボットに関する課題

高額なインフラストラクチャコスト：どんなWebトラフィックでも、ビジネスに具体的なコストを課します。なぜかと言うと、コンテンツをホストし、サーバーを展開し、ストレージとコンピューティングのために支払う必要があるからです。残念ながら、こうした経費は、Webプロパティが悪意のあるボットの標的になるにつれ、上がっていきます。良性ボットがSEO、顧客サポート、他の有用なタスクのために必要不可欠なのに対して、悪性ボットはコンテンツをスクレイピングし、サービスを中断させることで、帯域幅料金の過剰請求を引き起こす可能性があります。

ユーザー体験の低下：顧客は、悪性ボットが与えるビジネスへの影響を敏感に感じとります。アカウントから締め出されたり、不正取引で請求を受けたり、単に企業のWebサイトにまったくアクセスできなくなったりすることがあるかもしれません。ボットの活動によって過負荷になったサーバーは、高速のページ読み込みを正規のユーザーへ提供することができなくなります。そして、バーチャルな買い物かごの放棄率が上がり、直帰率が高くなり、コンバージョン率が低下し、顧客のエンゲージメント、維持、収益の全体的な損失へとつながっていきます。

歪んだ分析：ユーザー体験の低下とインフラストラクチャにかかるコストの急増に加えて、悪意のあるボットが分析を歪め、企業のWebパフォーマンスについて誤ったイメージを与えてしまうかもしれません。悪性ボットのトラフィックは質が悪い傾向があり、企業の集計分析データに（ページビューを人為的に水増しするなど）悪影響を及ぼし、トラフィックパターンとパフォーマンスメトリクスに価値あるインサイトを得るチャンスを失うことがあります。

ボット軽減ソリューションで必要なこと

正確な検出：企業が悪性ボットに対抗するために、Webプロパティ上でのボット活動を正確に特定する能力を持つ必要があります。最も正確な検出方法の中には、行動分析、フィンガープリンティング、機械学習と脅威インテリジェンスを組み合わたものもあります。企業は本物のユーザーの活動を妨げたり、ユーザー体験を損なうことなく、悪意のある行為を検出するのに役立ちます。

シームレスな統合：包括的なボット軽減戦略がレンダリングされても、長期にわたるうえに複雑な設定を必要とする場合は、役に立ちません。ボット軽減ソリューションは、テクノロジースタック、セキュリティ戦略（DDoS攻撃防止を含む）、CDNと簡単かつ迅速に統合する必要があります。そうすることで、お客様はユーザー体験において大きな影響を目にすることなく、アップグレードされた攻撃防御のメリットを享受することができます。

多様な軽減策：悪意のあるボットは年々、複雑で高度になってきており、企業は軽減戦略を適応させてボットの動きをできるだけ迅速に検出し、阻止する必要があります。たった1つで、どんな悪性ボットの動きでも予防できる作戦はありませんから、様々な検知方法および軽減方法を最低でも1つ、実装することが絶対必要です。こうした方法には、すべてのボットトラフィックをブロックする、良性ボットをホワイトリストする、疑わしいボットをCAPTCHAでチェックする、すべてのサイトトラフィックの日次ログを維持する、すべてのユーザーに追加の認証を実装する、代替コンテンツにボットをリダイレクトするといったものがあります。

DDoS攻撃軽減策

DDoS攻撃は、ターゲットデバイスとインターネット間の利用可能なすべての帯域幅を消費することにより、深刻なサービスの中断を引き起こすだけでなく、お客様がその企業のリソースにアクセスできないため、ビジネスに大きな悪影響を及ぼします。

Webサーバーを保護するために、リバースプロキシは攻撃者があなたのサーバーのIPアドレスを特定し、標的にさせないようにします。より複雑なレイヤー7 DDoS攻撃の場合、webアプリケーションファイアウォール（WAF）はリバースプロキシとして行動し、特定の種類の悪意のあるトラフィックから標的にされているサーバーを保護できます。

独自のリバースプロキシを構築している企業もありますが、これには集中的なソフトウェアリソースとエンジニアリングリソース、物理的なハードウェアへの多額の投資が必要です。リバースプロキシのメリットを享受するのに簡単で費用対効果の高い方法は、Global Server Load Balancingを提供するCDNを利用するやり方です。企業はパフォーマンスに影響することなく、ソースにより近い場所で、DDoS攻撃を軽減することができます。

言うまでもなく、Webサーバーだけを DDoS攻撃から保護しても十分ではありません。多くの場合、企業はパブリック環境またはプライベート環境のデータセンターにてホストされているオンプレミスネットワークインフラストラクチャも持っています。それらについても脅威から保護する必要があります。

DDoS対策への従来のアプローチ

スクラビング：スクラビングは悪意のあるネットワークトラフィックをその他のトラフィックから除外するか、「スクラブ（浄化）」するために、指定された地理的な場所にある集中型のスクラビングサーバーにルート変更するように要求します。すべてのトラフィックを地理的に遠距離にあるスクラビングセンターへとルート変更すると、かなりレイテンシーが追加され、大部分のアプリケーションでは許容されないことが多いです。

オンプレミスハードウェアボックス：他のDDoS対策テクニックはオンプレミスハードウェアボックスを使ってトラフィックをスキャンし、悪意のあるリクエストを除外します。スキャニングハードウェアも、スキャニング作業を完了するためにボックスを通過するルート変更されたネットワークトラフィックが集中し、ボトルネックとなるため、ネットワークレイテンシーを引き起こし、パフォーマンスの妨げになります。オンプレミスのDDoS対策アプライアンスは、デフォルトで帯域幅を制限することがあります。これは、組織のネットワーク容量とボックスのハードウェア容量の組み合わせに基づきます。

DDoS対策プロバイダーに必要なこと

軽減処理能力と軽減までの時間：企業は、サイトの機能性に影響を与えることなく、DDoS攻撃軽減に対する既存の処理能力を評価する必要があります。従来のアプローチは、DDoS攻撃によるトラフィックスパイクを吸収するタイプで、コストがかかる上に帯域幅消費型攻撃の場合に、簡単に過負荷になるオンプレミスのサーバーファームを構築する方法でした。もっと効果的なアプローチは、DDoS攻撃に対する保護能力を無制限に提供できて、ネットワークエッジでサービスをプロビジョニングできるクラウドベースの軽減ソリューションをデプロイする方法です。

常時稼働 vs. オンデマンド保護：オンデマンドの軽減サービスの場合、潜在的なDDoS攻撃が検出されると、そのトラフィックは毎回クラウド軽減サービスにルーティングされなければなりません。そして、ユーザーは必要な場合だけDDoS対策に支払います。分析が開始し、誰かが手動で軽減サービスをオンにする前に、トラフィックスパイクがある程度のThresholdsに到達しなければならないため、DDoS攻撃の阻止には時間がかかるかもしれません。

それに対して、常時稼働の軽減策は継続してルーティングを行い、すべてのサイトトラフィックをフィルタリングするので、常にクリーンなトラフィックだけがユーザーのサーバーに到達します。常時稼働軽減策はオンデマンドサービスよりも高額ではありますが、自動的かつ中断のない保護を提供し、より速い応答時間につながります。絶え間ない攻撃に直面している企業にとって、常時稼働の軽減策はオンデマンド保護よりも費用対効果が高い選択肢です。

セキュリティとパフォーマンスの統合：DDoS攻撃は停滞や停止を引き起こし、パフォーマンスを低下させるだけでなく、持続的な成長を達成する企業の力にも悪影響を与えます。そこで、企業はサイトのパフォーマンスや顧客体験に悪影響を及ぼすことなく、DDoS攻撃に対する屈強な防御が提供できるセキュリティとパフォーマンスの統合ソリューションを視野に入れるべきでしょう。

ステップ4

回復力のあるインフラストラクチャを構築することで、アプリケーションの高い稼働率を確保する

負荷分散

サーバーのリソースと効率性を最大化することは、微妙なバランスを取る必要がある場合があります。過負荷状態になるサーバーまたはエンドユーザーから地理的に離れすぎているサーバーは、レイテンシーやサーバー障害の発生につながる可能性が高く、収益の損失、顧客の信頼の失墜、ブランド力の低下を招く恐れがあるため、ビジネスに悪影響を及ぼす可能性があります。

クラウドベースのLoad Balancerは、トラフィックのスパイクを処理するために複数のサーバーを通してリクエストを分散します。負荷分散の決定は、ユーザーに近いネットワークエッジで行われます。こうすることで、応答時間を短縮し、サーバー障害のリスクを最小限に抑えつつ、インフラストラクチャの最適化を効率的に行うことができます。たとえ1つのサーバーで障害が発生しても、Load Balancerが他のサーバー間でトラフィックにリダイレクトして再分散できます。お客様が決して大きなレイテンシー悩まされることもサイトの中断を経験することもありません。Load Balancerがアクティブヘルスチェックを行うことで、企業はパフォーマンスが悪いサーバーを特定し、実際に故障する前に予防措置を講じることができます。

負荷分散における課題

アプリケーションダウンタイムとレイテンシー：わずかな遅れでも、エンゲージメント率とコンバージョン率に大きな影響を与えることがあります。レイテンシーが30ミリ秒になるとユーザーの目には顕著になり、100〜400ミリ秒ほどの短い遅れでさえも、消費者行動に悪い影響を及ぼします。[3]機能的な負荷分散ソリューションの実装に失敗した企業は、Webプロパティが必然的にパフォーマンス上の問題を抱えることになり、コンバージョン率と収益が減少する可能性があります。

高いコストと限られた柔軟性：ハードウェアのLoad Balancerは高価かつ複雑であり、企業の成長に合わせて拡張することが、本質的にできません。企業は自社Webプロパティが受けるトラフィックの量を見積もってハードウェアデバイスを事前に購入しなければなりません。つまり、未使用の容量に対して支払いをするか、使用デバイスの数が増やせるまで、最適ではない読み込み時間とWebパフォーマンスに悩まされるしかないということです。

複雑なトラフィック管理：Webパフォーマンスと信頼性を最大限にしたいと考える企業にとって、トラフィックのパターンを可視化すること、地域のトラフィックを管理すること、そして配信元サーバーの健全性を監視することは必要不可欠です。企業が可視性を持たなければ、正常に動作しない負荷分散ソリューションが問題を抱えていたり、ユーザーに大幅な遅延やダウンタイムを起こしているサーバーに誤ってトラフィックをルーティングしていたりする時に、検出できない可能性があります。

[3] Brutlag, Jake. “Speed Matters,” Google AI Blog, https://ai.googleblog.com/2009/06/speed-matters.html

Load Balancerに必要なこと

ベンダーに依存しないソリューション：Load Balancerはマルチクラウドとハイブリッドクラウドのサポートを提供して、企業がベンダーに縛られることと、複雑な設定を回避するのに役立ちます。スタンドアローンのクラウドベースソリューションは既存の負荷分散サービスに取って代わるのではなく、クラウドベンダーのネイティブLoad Balancer、または従来のハードウェアアプライアンスと統合して、柔軟性を最大限にし、不適切な設定を最小限にします。基本的に、配信元サーバーがオンプレミスでホストされているのか、マルチクラウドまたはハイブリッドクラウド環境でホストされているのかにかかわらず、企業のインフラストラクチャ全体にトラフィックを動的に分散できなければなりません。

アクティブヘルスチェックと詳細な分析：負荷分散ソリューションを選択する際、可視性は重要な要素です。それは、企業のサーバーとアプリケーションの健全性を確認するためだけでなく、潜在的なレイテンシーとダウンタイムに先手を打つためでもあります。トラフィックパターンと配信元の健全性に関する詳細な分析があれば、企業はパフォーマンスが悪いサーバーを特定し、高い可用性と稼働時間のためにインフラストラクチャを最適化することができるはずです。

CDNの統合理想的な設定では、負荷分散ソリューションがCDNと連携してレイテンシーと帯域幅消費を最小限に抑えます。ネットワークエッジで静的コンテンツをキャッシングすることで、CDNはエンドユーザーに最も近いサーバーからコンテンツを配信することができ、Webパフォーマンス全体を高め、配信元サーバーへと送信されるリクエストの総数を減少させます。

ステップ5

エッジで異常な動作を検出し、Webプロパティを保護する

データ損失防止（DLP）

クラウドコンピューティングの出現によって、データ漏えいは現代の企業にとって最も重大な脅威の1つとなりました。標的型攻撃や内部システムの不具合、単なる人的エラーの結果として、こうした侵害は機密性の高い顧客データを危険にさらし、データプライバシー規制に違反して、数百万ドルもの罰金と収益損失につながるかもしれません。

機密データの潜在的な漏えいと紛失に適切な対処をするために、サイバーセキュリティ戦略とセキュリティ製品を数多く実装する企業もあります。報漏えい防止（DLP）ソリューションも、データのプライバシーポリシーを適用し、不正使用情からユーザーデータを保護するために設計された他の規制と同様に、GDPRとCCPAを遵守する企業を支援します。

DLPの課題

複雑な配置：本質的に堅牢なレガシーDLPソリューションはセットアップが複雑で、時間がかかるかもしれません。企業はDLPポリシーを調整して、特定のユーザーグループとビジネスユースケースに合わせる必要があります。これは外部からの広範囲なサポートと管理を必要とするため、骨の折れる作業かもしれません。また、DLPルールにより、ユーザーは厳密に規定された境界を超えてデータを送信できないため、必要なデータへのアクセスが誤ってブロックされてしまい、従業員の生産性とコラボレーションを妨げることもあります。

包括的なデータ保護の欠如：DLPポリシーは、規制対象のデータ（機密と分類したままにするべき機密性の高いデータ）と規制対象外のデータ（一般的によく知られている情報。機密データが含まれることもあります）の両方をカバーする必要があります。ただし、多くのレガシーDLP製品は、規制対象外のIPデータ保護を考慮に入れていないため、データ侵害が発生した場合、企業は大きな損失を被る可能性があります。

限定的な可視性：機密データの完全保護を保証し、内部関係者の脅威を防止し、地域のプライバシー規制に遵守するために、企業は自社データへのアクセス方法と送信方法を可視化する必要があります。既存の脅威や予期される脅威に注意を向けすぎると、予期せぬ悪意のある行為に先手を打つための企業の能力を妨げることになるかもしれません。

DLPソリューションに必要なこと

合理的なデプロイと管理：ハードウェアベースのDLPシステムは、セットアップが複雑で管理が煩雑なだけでなく、進化し続ける脅威に対して常にアップデートする必要があります。クラウドベースソリューションは新しいデータ脅威に対して柔軟性を持ち、企業にデータ使用状況と管理に卓越した可視性を提供する一方で、デプロイコストを削減します。

柔軟性：企業は、実装や管理、維持が簡単でありながら、様々なユーザーグループとユースケースに対応できる柔軟性を備えたDLPソリューションを採用する必要があります。ハードウェアベースのレガシーDLPソリューションに依存するよりも、クラウドベースを代替として検討するべきです。クラウドベースにはさらに柔軟性があり、機密の企業データや顧客データを防御するために導入されるポリシーや保護方法の管理ができます。

保護 vs. 防止：レガシーDLPシステムは、主にデータ損失防止に重点を置きますが、社内機密データを外部脅威と内部脅威から保護することができません。しかし、次世代ソリューションなら、こうした脅威を軽減するだけでなく、高速でより効果的な方法でデータ漏えいから回復することができます。

エッジプログラマビリティ

エッジコンピューティングでは、企業がアプリケーション開発をネットワークエッジに移して、計算を可能な限りエンドユーザーに近づけることで、レイテンシー、サーバーリソース、帯域幅の使用量を最小限に抑えることができます。サーバーレスアーキテクチャによって、企業はインフラストラクチャ設定と管理をサードパーティに任せることができるので、開発者は、他の作業に時間を費やすことができるようになります。たとえば、アプリケーションを構築したりデプロイしたりする、既存のアプリケーションのためにカスタム設定を有効にする、アプリケーション開発とセキュリティを最適化する助けをするなどが挙げられます。

エッジプログラマビリティの課題

レイテンシーとコールドスタート ：サーバーレスコンピューティングは必要に応じて機能を実行するため、機能の起動に数秒かかることがあります。この「コールドスタート」は、望まないレイテンシーを発生させることがあります。Webパフォーマンスにおいて明らかな低下が起きないように、コールドスタートにかかる時間と頻度を最小限に抑えるための回避策を見つけるなど、企業は積極的な対策を講じる必要があります。

グローバル規模の欠如：ユーザー基盤が広く分散しているWebベースの企業の場合、アプリケーションをグローバル規模で展開しなければなりません。アプリケーションパフォーマンスと配信を向上させると同時に、アプリケーションをネットワークエッジに移動させて、より効率的にユーザーに到達することができます。

非効率なリソースアプリケーション：アプリケーションの構築とカスタムプログラミングの作成には、専用の内部リソース、中央クラウドプロバイダーによる適切なサーバー容量、テストを行う時間を必要とする作業が含まれます。この作業が不十分な場合、プロトタイピングの経費がかさみ、アプリケーションの迅速な市場投入が遅れることもあります。

エッジコンピューティングソリューションで必要なこと

拡張性の簡略化：エッジコンピューティングは、ネットワークエッジからアセットを配信することで、エンドユーザーのためにレイテンシーを最小化するために設計されているため、企業がグローバルなネットワークを持つプロバイダーを選ぶことは極めて重要です。そうすることで、企業はリーチを広げ、高速のユーザー体験を提供するだけでなく、地域ごとではなく、すべてのロケーションでお客様に到達するためにエッジでコードを実行して、デプロイに必要な作業も簡略化することができます。

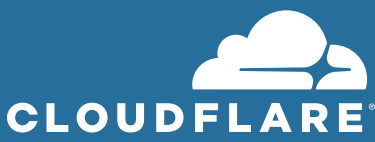
開発者体験を改善：新規アプリケーションの開発と既存のアプリケーションの拡張は、合理化された作業でなければなりません。合理化されていると、開発者はテクニカル運用チームに頼らなくても、迅速かつ簡単にコードを展開することができます。

インフラストラクチャコストの削減：サーバーレスアーキテクチャがあれば、企業は未使用のサーバースペースやCPUがアイドル状態である時間にお金を払う必要はなくなります。その代わりに、リクエストの処理をネットワークに移行して、必要なリソースにのみ料金を支払うことができるので、インフラストラクチャコストを大幅に削減できます。

Cloudflareが良質なオンライン体験を届ける仕組み

良質なオンライン体験を創出するには、適切なセキュリティ戦略とパフォーマンス戦略が必要です。そうした戦略は、企業がコンテンツ配信を加速化するだけでなく、ネットワークの信頼性を確保して各自のWebプロパティをサイトの停止、データの盗難、ネットワークの脆弱性、そのほかの重大な攻撃から保護する、ということも可能にするものでなければなりません。

世界中の95か国以上、200以上の都市に広がるネットワークをもつCloudflareは、企業がオンプレミス、クラウド、SaaSアプリケーションのセキュリティ、パフォーマンス、信頼性の強化を可能にし、拡張性のある統合グローバルクラウドプラットフォームを提供します。Cloudflareを使用してオンラインビジネスを保護する詳しい方法については、Cloudflare.comをご覧ください。



+81 3 4510 1893 | enterprise@cloudflare.com | www.cloudflare.com/ja-jp/

© 2020 Cloudflare, Inc.All rights reserved.
Cloudflareのロゴは、Cloudflareの商標です。その他の会社名および商品名はそれぞれ関連する各企業の商標です。

REV: 200525