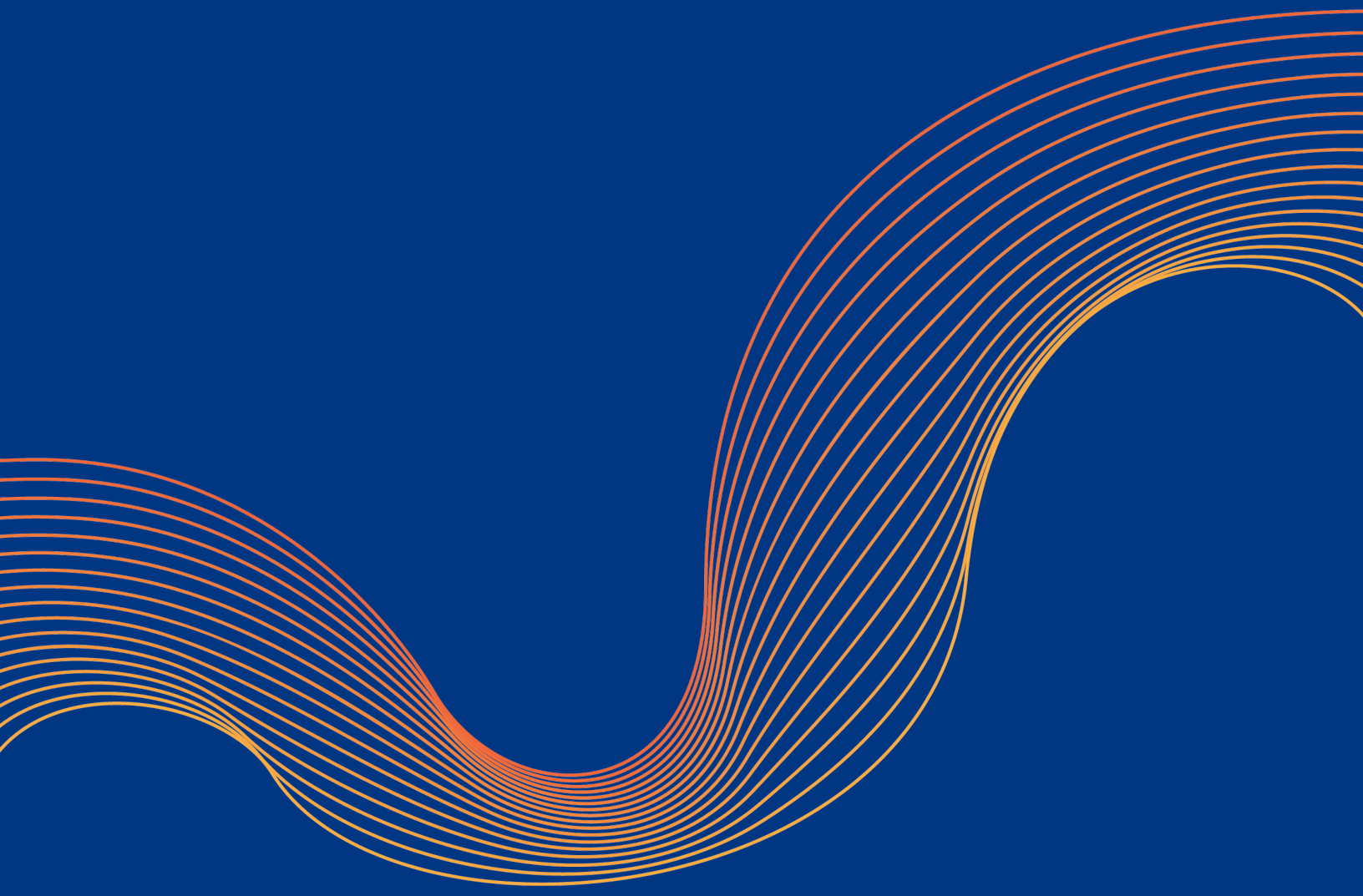
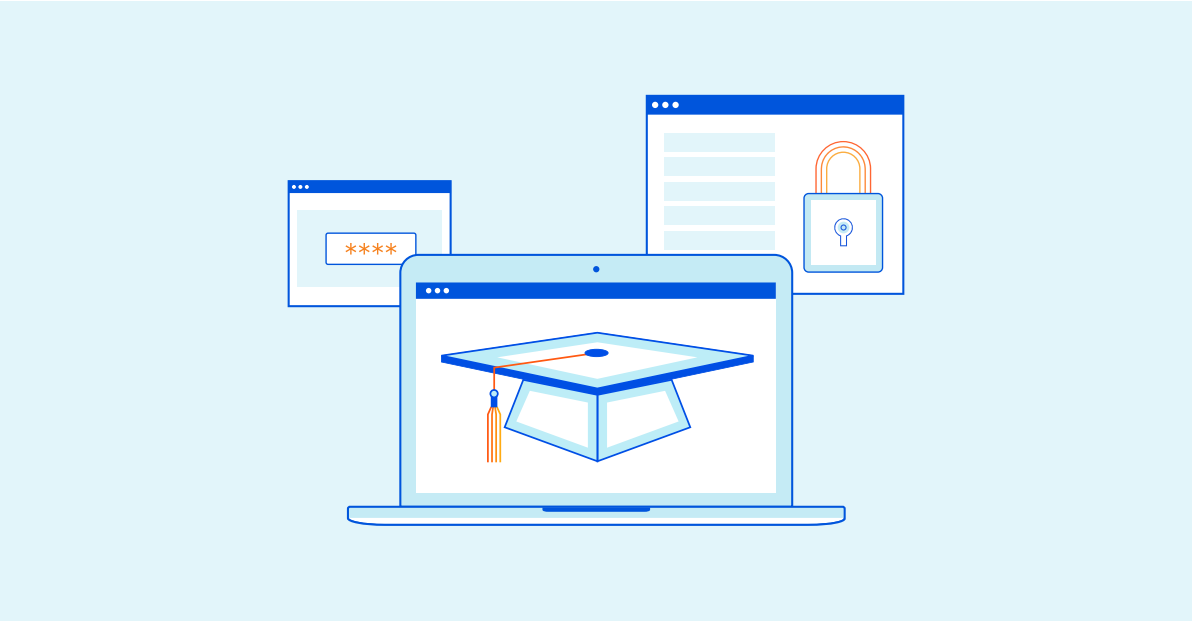
ホワイトペーパー

CLOUDFLARE

安全でスケーラブルなリモート学習インフラストラクチャを設計する



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



はじめに

近年、リモート学習はますます人気のある教育モデルとなっています。新型コロナウイルスによるパンデミックのため、多くの教育機関がウイルスから学生や教員を守るためにリモート学習へと移行せざるを得なくなりました。これが、オンライン授業と対面授業のいわゆるハイブリッドモデルと完全リモートモデルへの移行を加速化させることになりました。

リモート学習には、通常の対面型教育とは異なるアプローチが必要となります。教える側は、講義や動画、双方向型のコンテンツなどを含めて、幅広い学習スタイルや様々なコンテンツをサポートする機能を求めています。リモート学習では、授業を受ける学生全員が、迅速かつ同時に共有コンテンツにアクセスできることが不可欠です。

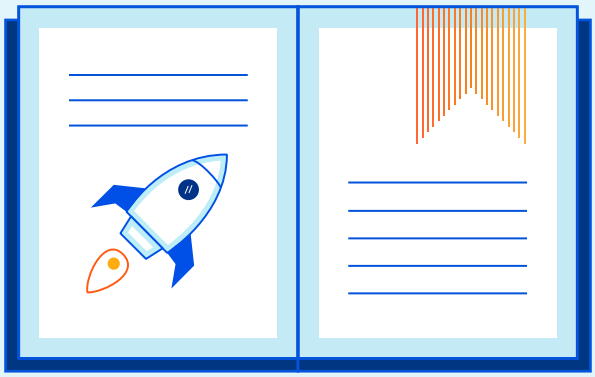
テクニカルな面では、教育機関がこの幅広い種類のコンテンツをサポートし、生徒が必要とするときにシステムが機能するよう準備を整えておく必要があります。そのため、次のようなさまざまな課題に取り組まなければなりません。

- 大規模なコンテンツの配信
- 分散サービス妨害攻撃の軽減
- アカウント乗っ取りの防止
- 悪意のあるコンテンツとマルウェアの阻止

大規模なコンテンツの配信

リモート学習を運営する上で中核を担うのは、教育機関のITインフラストラクチャです。教員は、コンテンツを多数の生徒に同時配信でき、コンテンツを送信する際の遅延を最小限にできる機能を望んでいます。

教員は、広範なコンテンツを生徒に届ける必要があります。これには、静的なWebページから、インテラクティブな学習ツールを介したストリーミング動画などの動的コンテンツまで含まれます。教育機関のITインフラストラクチャに必要なのは、リモートで学ぶ生徒達にこうしたコンテンツを効率的にスケーラブルに配信できる機能です。



静的コンテンツ

教員が生徒に配信する必要があるコンテンツの中には、静的なコンテンツもあります。ページ内の情報に変更がなく、頻繁に更新する必要がないWebページはこれに該当します。

このような種類のコンテンツに関して、ITの大きな課題となるのは拡張性と遅延です。多数の生徒が同時にひとつのコンテンツにアクセスした場合、Webサーバーは対応できるでしょうか？さらに、リモート学習にとっては、Webサーバーの場所もかなり重要になります。生徒がサーバーから遠いほど、コンテンツ配信の遅延は大きくなります。

静的コンテンツでは、ローカルにコンテンツのキャッシュを作成する機能が、こうした課題の克服に役立ちます。生徒が特定のページに頻繁にアクセスした場合、そのページのコピーがローカルに保存されて、必要な時にすぐにアクセスできるようになるためです。

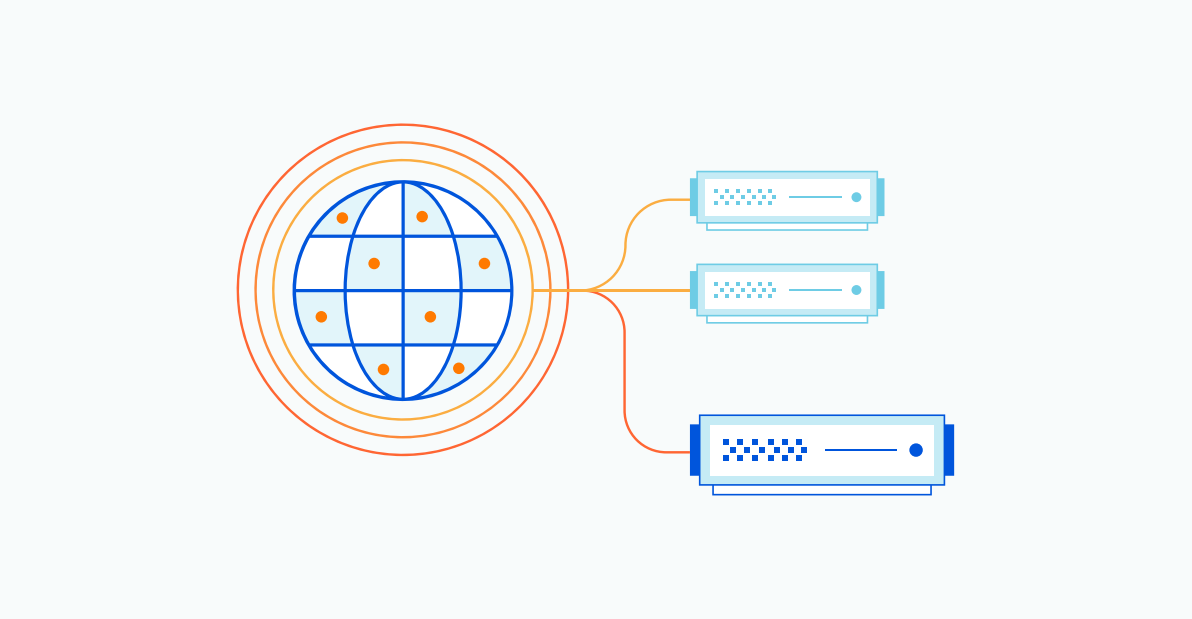
コンテンツ配信ネットワーク（CDN）を使って、キャッシングをスケールに応じて実装することもできます。CDNは、静的コンテンツのローカルコピーを保存し、更新の有無を定期的に確認するノードのネットワークで構成されています。世界的に展開するCDNでは、効果的なリモート学習に必要なスケーラビリティが提供され、遅延も少なくなります。

動的コンテンツと双方向型コンテンツ

静的コンテンツと同様に、対話型のオンライン学習とその他のコンテンツには、スケーラビリティの点で潜在的な問題があります。ところが、CDNノードのネットワークを使用しても、このタイプのコンテンツではうまく機能しません。コンテンツを頻繁に、またはひっきりなしに更新する必要がある場合、CDNノードが最新バージョンにするためにメインのWebサーバーに継続的にクエリーを実行します。これがユーザーに遅延を引き起こし、メインのWebサーバーに負荷が集中することがあるのです。

一方、動的コンテンツにおけるスケーラビリティの問題は、負荷分散によって解決できます。生徒のリクエストに対処するために、単一のサーバーを使うのではなく、複数のサーバーを使ってトラフィックを分散させます。こうすることで、1台のサーバーに負荷が集中せず、遅延を最低限に抑えることができます。

効果を上げるには、負荷分散したサーバーが完全に独立して動作できるようにするか、当該サーバーが負荷分散された他のデバイスにのみ依存するようにします。すべてのサーバーが同一のデータベースサーバーを使うように設定されている場合、そのデータベースサーバーがボトルネックとなる可能性があるため、負荷分散された追加のサーバーによるメリットは極めて限定的か、まったくありません。リモート学習ソリューションは、必要なときに必要なスケーリングが行われ、負荷分散の利点すべてを提供できるシステムが構築されるよう、慎重にデザインする必要があります。

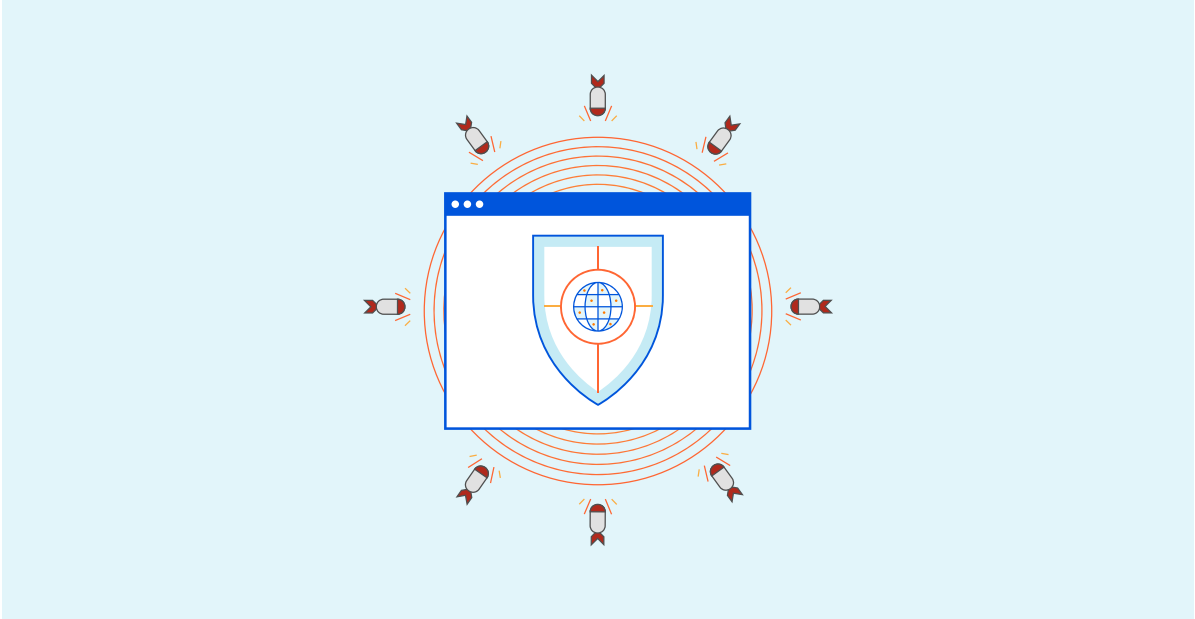


分散サービス妨害攻撃

分散サービス妨害（DDoS）攻撃はますます一般的になっています。Internet of Things（IoT）とクラウドコンピューティングの拡大にともない、攻撃者はより安価で簡単に、インターネット接続のコンピューティングパワーにアクセスできるようになりました。安全性が損なわれたデバイスは、サービスに悪意のあるトラフィックを送信するために使われてしまい、正当なリクエストに応答できなくなります。

リモート教育では、DDoS 攻撃がサービスの提供機能に重大なリスクをもたらします。2020年の上半期に多くの教育機関がリモート学習に移行した際、オンラインの教育リソースに対するDDoS 攻撃は、350%も増加しました[1]。

さらに、一部のDDoS 攻撃はランサムコンポーネントを組み込むよう進化を遂げています。攻撃者はDDoS 攻撃で企業を脅迫し、攻撃を停止するための身代金を要求することもあります。こうした脅威の多くは、根拠のないものですが、DDoS攻撃対策をしていない教育機関は、インフラストラクチャに対するリスクが大きすぎるため、無視できないと感じることもあるでしょう。

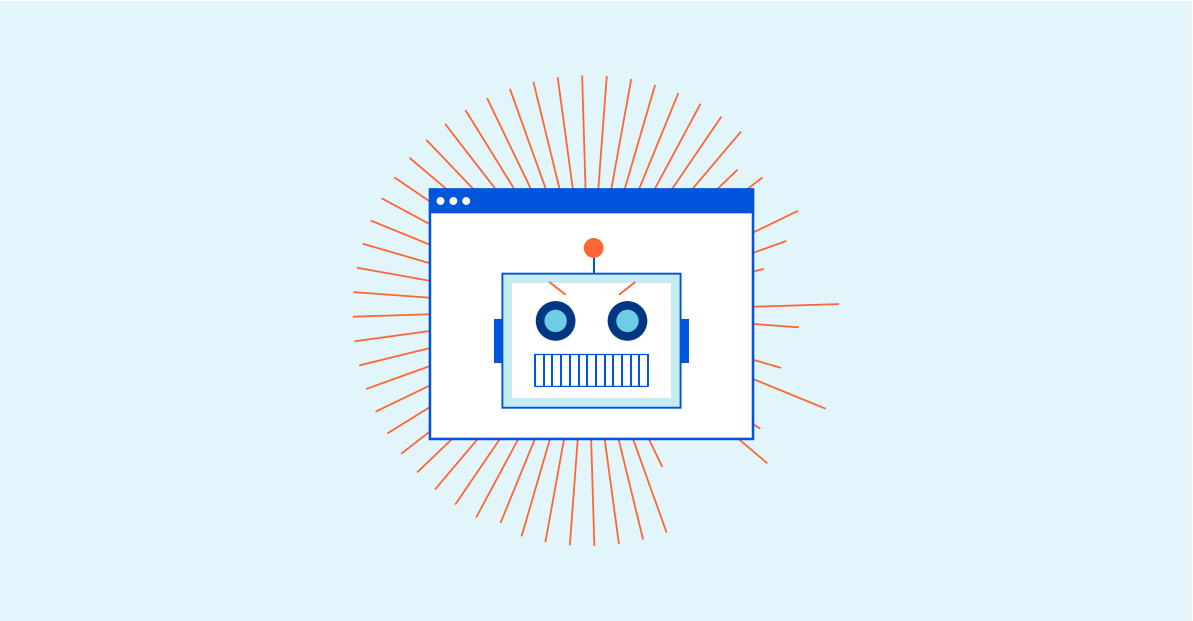


幸いなことに、比較的予算に余裕がない教育機関でも、数々の効果的なDDoS 軽減方策を利用できます。教育機関が考慮するべき点：

- 高い軽減能力：教育機関に必要と予測される攻撃対策にだけ資金を投じることは魅力的に思えるかもしれませんが、予期せぬ大規模な攻撃が発生した場合、サービスをアップグレードするのに要する時間が、余分なダウンタウンにつながる可能性があります。
- 分散型の軽減：DDoSトラフィックスクラビングは、分散化される必要があります。これは、企業のトラフィックすべてをフィルタリングするために単一の集中ポイントを通過させるルーティングは、スケーラビリティがなく、ネットワークの遅延を増長するためです。
- オンデマンド vs. 常時稼働の保護：オンデマンドのDDoS 軽減では通常、潜在的な攻撃が検出されるまで、トラフィックがパブリックインターネットから企業サーバー、またはネットワークインフラストラクチャまで流れます。徹底した検査とフィルタリングが行われるのは攻撃が検出された時点です。一方、常時稼働の軽減策は、継続的にすべてのトラフィックをフィルタリングします。常時稼働の軽減策は、オンデマンドサービスよりも高額になることもありますが、中断のない保護を提供し、サービスを手動で有効にする必要がないため、応答時間の短縮につながります。

DDDoS 軽減戦略の詳細については、Cloudflareリソースハブにある「DDoS 攻撃を軽減するための5つのベストプラクティス」をご参照ください。

[1] *https://www.infosecurity-magazine.com/news/ddos-attacks-on-virtual-education/*



アカウントの乗っ取り

多くのサイバー攻撃は、システム内の正当なユーザーアカウントの乗っ取りから始まります。アカウントの乗っ取り攻撃には、ネットワーク、アプリケーション、またはその他のシステムにある正当なユーザー資格情報の侵害も含まれます。攻撃者は、フィッシング攻撃とクレデンシャルスタッフィングを含む様々な方法でアカウント認証情報へのアクセスが可能になります。

こうした資格情報を使って、攻撃者は正当なユーザーになりすまし、ターゲットとするシステムにマルウェアを仕込んだり、データを盗んだり、他の目的を遂げたりするのです。児童オンラインプライバシー保護法（COPPA）や家族教育権とプライバシー法（FERPA）などの規制によって保護されているデータへのアクセスを攻撃者に許してしまうこともあります。また、このアクセスによって、攻撃者は学生の重要な記録を削除したり、ランサムウェアを使って身代金目的のために保持したりすることもあります。

教育機関は、疑わしい言い回しや未知の脅威を検出するために、既知の悪意のあるコンテンツと機械学習を活用し、攻撃検出能力を持つフィッシング軽減ソリューションをデプロイする必要があります。メールのスキャニングはこうした手段の一つです。もう一つの手段としては、安全なWebゲートウェイを使って、既知の悪意のあるサイトをブロックし、ユーザーに特定のタイプのファイルをダウンロードをさせないようにする方法があります。

クレデンシャルスタッフィング

その一方で、攻撃者は仮想プライベートネットワーク（VPN）、リモートデスクトッププロトコル（RDP）、Webアクセスプロトコルのように、企業の外部公開されたログインシステムを使って、ユーザー資格情報の安全性を損なうこともできます。一般的なユーザーは、13ものオンラインアカウントに同じログイン認証情報を使い[2]、弱く簡単に推測できるパスワードが使用されていることもよくあります。クレデンシャルスタッフィング攻撃では、自動化ボットを使い、こうした認証ポータルでユーザーのパスワードの推測を試みます。これに成功した場合、攻撃者は正規のログイン認証情報を把握するため、ユーザーアカウントに問題なくアクセスできてしまいます。

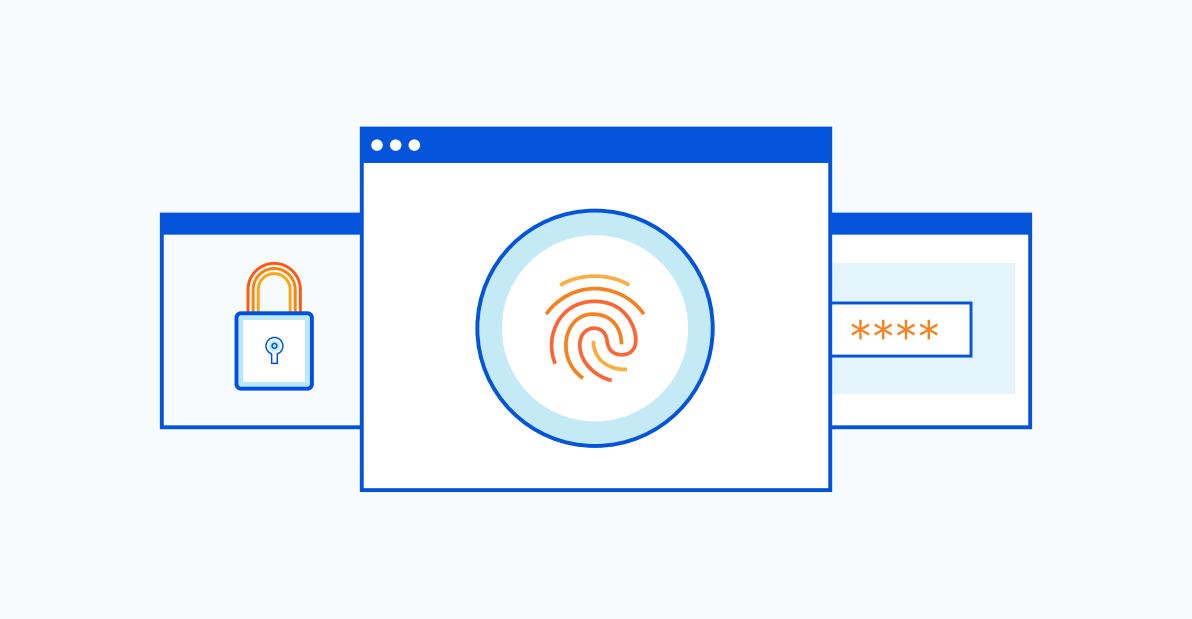
[2] *https://www.lastpass.com/state-of-the-password/global-password-security-report-2019*

クレデンシャルスタッフィング攻撃は、この自動化を利用します。このタイプの攻撃から保護するには、ボット検出ソリューションが必要になります。しかし、良性ボットと悪性ボットを識別することも重要です。

ボットは、さまざまな方法で検出／ブロックすることができます。悪意のあるボット軽減戦略の基本的な要素は次の通りです。

- **レート制限：**IP アドレスがお客様のサイト、またはネットワークにリクエストを送信できる回数を制限します。これは、単純なブルートフォースボット攻撃に最も効果的です。
- **CAPTCHAと二要素認証：**この2つによって、多くのボットがまったくログインページにアクセスできなくなりますが、これらの対策がユーザーエクスペリエンスを損なう可能性もあります。
- **ボットのブロックリストと許可リストの維持：**これは、既知の悪意のあるボット追跡を継続し、検索エンジンクローラーと他の良性ボットが引き続きタスクを実行できるようにします。

しかし、この方法は高度な特殊機能に特化したボットに対しては、効果的でないことがあります。ボット軽減については、Cloudflareリソースハブにある「悪意のあるボットのプレイブック」をご確認ください。

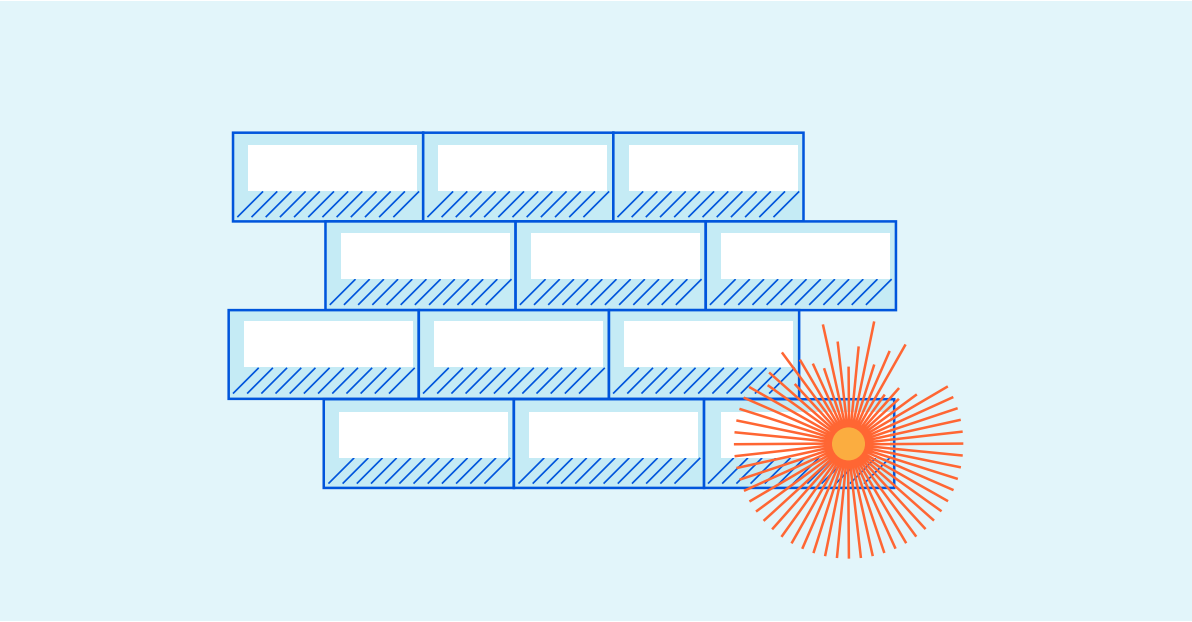


悪意のあるコンテンツとマルウェア

教員がリモート学習を利用するにつれて、パブリックインターネットにさらされるシステムの数も増えることになります。生徒がWebアプリケーションを使って、オンライン学習を活用することもあるでしょう。リモート学習では、教員も生徒もVPN、RDP、同様のソリューションを使って、リモートネットワークとPCにアクセスすることがあります。このシステムもサイバー脅威から保護する必要があります。

Webアプリケーションのセキュリティ

教育目的のWebアプリケーションが広範囲な機密データにアクセスすることもあります。米国のCOPPAやFERPA、類似の規則で守られている学生のデータは、こうしたプラットフォームに保存されることがあり、教育機関による適切な保護が不可欠です。



こうしたアプリケーションはソフトウェアなので、悪用される可能性のある脆弱性が含まれていることもあります。サイバー攻撃からこれらのアプリケーションを保護するには、ネットワークトラフィックを検査して、ソフトウェアのバグを悪用しようとする動きを検出し、ブロックする必要があります。

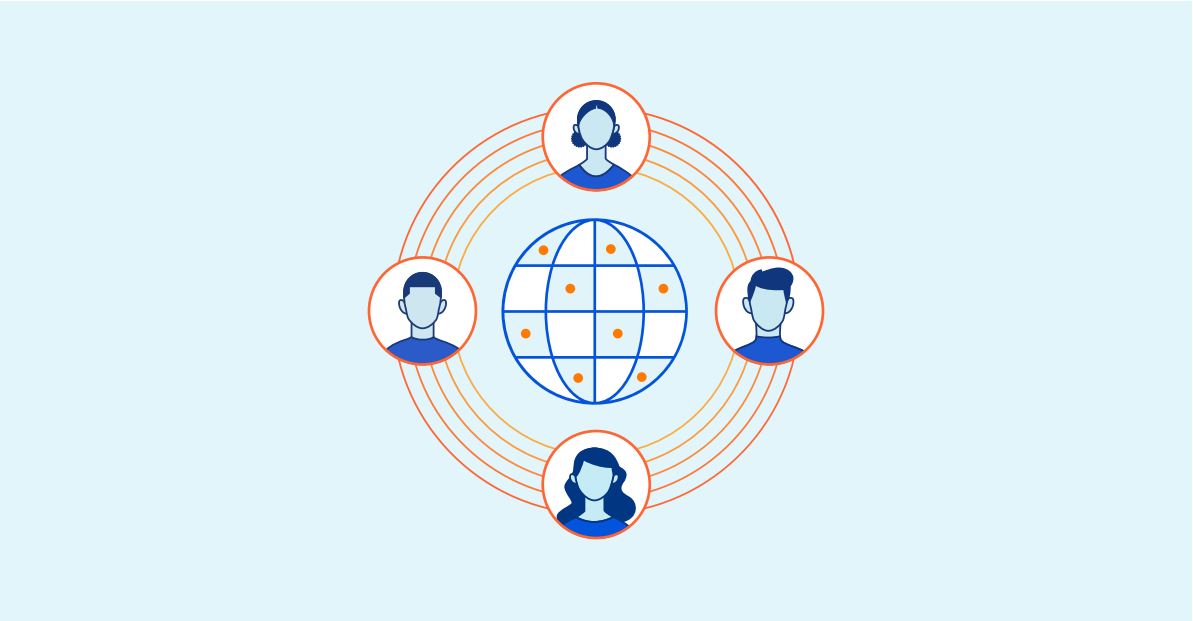
Webアプリケーションファイアウォール（WAF）は、様々な種類のWebアプリケーションの脆弱性に対する保護を提供します。シグネチャベースの検出と機械学習の組み合わせを使って、既知の攻撃と新型の攻撃を識別します。企業のWebベースのインフラストラクチャで、ゼロデイ攻撃さえも防御することができます。

ランサムウェアからの保護

ランサムウェアは、最も急成長しているマルウェアのひとつです。ランサムウェアが一度PCへのアクセスを手に入れると、そこに保管されているファイルを暗号化します。そして、アクセスを復元するために支払いを要求してきます。学校側が身代金をすぐに支払うことができるとしても、影響を受けたシステムを復元させるために多大な時間と費用がかかることがあります。

ランサムウェアは、VPNやRDPのようなリモートアクセス技術を介して、送り付けられることが増えています。正規のログイン資格情報へのアクセスを有する攻撃者は、それを使ってコンピューターにサインインし、マルウェアを仕掛けることができます。組織のネットワーク内に入ると、通常マルウェアはネットワーク上にある他のコンピューターを感染させるために拡散します。

教育機関には、すべての企業ネットワークトラフィックを検査できるファイアウォールソリューションが必要です。これで、組織のコンピューターが感染する前に、（ランサムウェアのように）悪意のあるコンテンツの流入を検出し、（学生の保護された個人データを含めた）データの流出を防ぐことができます。



Cloudflareでリモート学習の安全を確保する

新型コロナウイルスのパンデミックはやがて終息するでしょうが、リモート学習へ簡単に移行できる機能は教育機関にとって有益です。オンライン学習のリソースは、対面型学習にとっても価値のあるアセットであり、リモート学習に必要なインフラストラクチャを整備することで、悪天候や予期しない出来事で引き起こされる混乱に対する組織の回復力を高めることにつながります。

Cloudflareは、すべての教育機関が抱える最も一般的なITとセキュリティ上の課題に対応するソリューションと、統合型で使いやすいプラットフォームをご提供します。Cloudflareのように、単一で統合されたソリューションを活用することで、教育機関は不要な複雑性を回避し、予期せぬ事態に対する適応力と回復力を高めます。Cloudflareのサービス：

- グローバルなコンテンツ配信ネットワーク。世界200都市を上回るデータセンターを擁します。
- 47 TbpsのDDoS 軽減容量。ネットワーク Edgeで常時稼働の軽減策を行います。
- Webアプリケーションファイアウォール。Cloudflareネットワークにある2500万あまりのインターネットプロパティから脅威インテリジェンスを継続的に引き出します。
- 高度なボット軽減機能。機械学習とフィンガープリンティングを使って、ネットワーク全体のトラフィックパターンを分析し、最も高度なボットでも検出します。
- セキュアなWebゲートウェイ。ネットワーク Edgeで動作し、地理的に隔離されたデータセンターに送信されるトラフィックのバックホールによる遅延を短縮します。

詳細については www.cloudflare.comをご覧ください。