Cloudflare Bot Management

CAPTCHAを必要とせずに、悪意のあるボットを阻止し、AIボットを管理します。

トラフィックにはボットが潜んでいることがあります。悪意のあるボットは、収益とUXに悪影響を与えます。

インターネット上のアプリケーショントラフィックの**30%**は自動化されたトラフィックです。最新のボットは、地理情報に基づくヒューリスティックやIPベースのヒューリスティック、CAPTCHAチャレンジといった従来の防御策を容易に回避します。それがリアルユーザーを大いに苛つかせています。

Webの約**20%**の利用状況を把握するCloudflareほど、多くのAIクローラーと検索ボットのフィンガープリンティングを行う企業はありません[2]。

Cloudflare Bot Managementは、Webアプリやモバイルアプリに入るAIクローラーとボットトラフィックをCAPTCHAを使わずに管理するのに役立ちます。検証済みのボットや規制に準拠するAIクローラーによるアプリへのアクセスを許可し、非準拠のAIボットと悪意のあるボットを阻止します。これは、当社のアプリケーションセキュリティポートフォリオにおける重要な機能です。

製品がもたらすメリット

- 詐欺、金銭的損失、ブランド毀損から保護する
- より優れたWebおよびモバイルアプリ体験を提供する
- 不要なAIクローラーや検索ボットを排除する

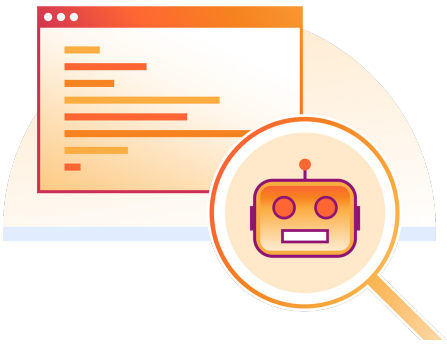

図1：Cloudflareのアプリケーションセキュリティポートフォリオに統合されたCloudflare Bot Management

出典

1. Cloudflare Radarデータ、2024年
2. W3techs、Usage statistics and market shares of reverse proxy services、2025年

Cloudflare Bot Managementの仕組み

Cloudflareは、グローバルかつアプリケーション固有の機械学習、クライアント側のJavaScript、モバイルデバイス、ヒューリスティックによる多層的な検出を組み合わせ、すべてのHTTPリクエストに対して単一のボットスコアを算出します。ボットスコアは、そのリクエストがボットから送信された可能性を示します。このボットスコアは、ブロックや許可などの標準対応や、他のCloudflare製品を介したカスタム対応ポリシーに使用されます。ボットスコア、HTTPリクエストメタデータなどを含むボット分析は、CloudflareダッシュボードUIまたはサードパーティツールのCloudflare APIから利用できます。

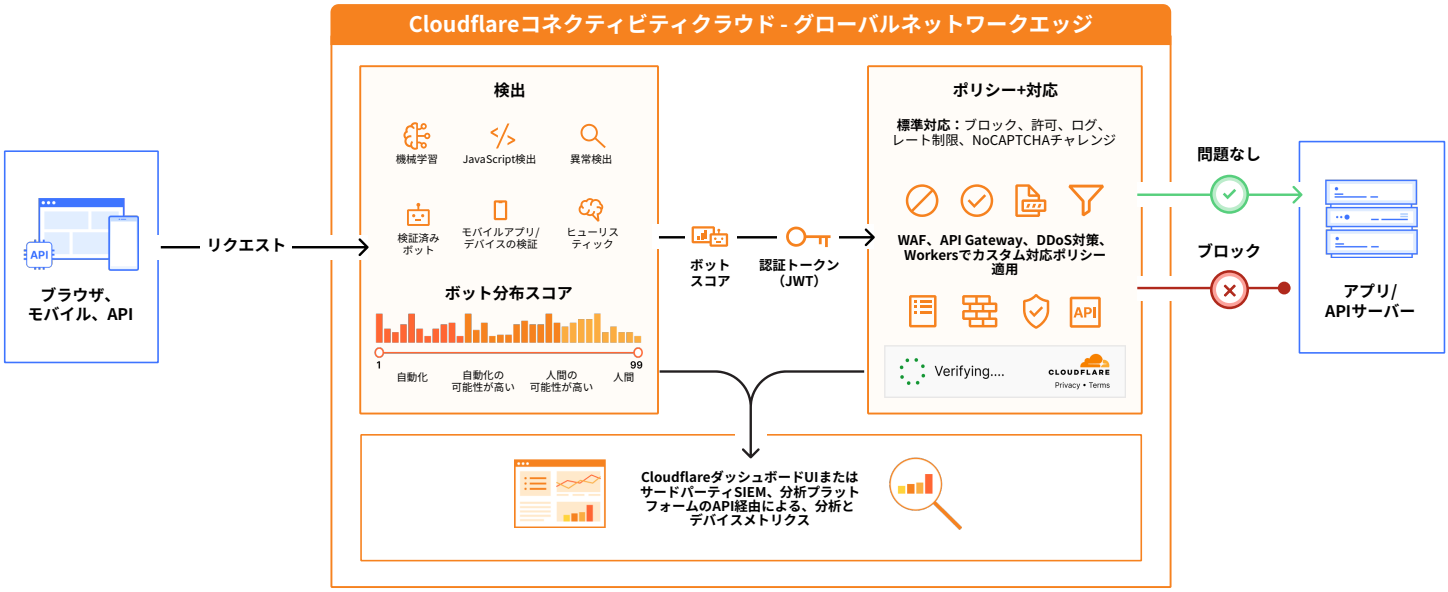

図2：Cloudflare Bot Managementを介したサンプルリクエストパス

Cloudflare Bot Managementの主な機能

アカウント乗っ取りや詐欺を阻止

公開より早く脆弱性を検出できるMLベースのモデルで、ゼロデー攻撃から保護します。記録的なDDoS攻撃から防御し、機密データを保護し、クライアント側のリスクを軽減し、Webアプリケーションのソフトウェアサプライチェーンを監視します。

ボットと詐欺から防御

ユーザーをアカウント乗っ取りから保護し、エンドユーザーエクスペリエンスに影響を与える悪質なボットを阻止します。MLモデルをクライアント、ネットワーク、脅威インテリジェンスと組み合わせることで、悪意のあるボットネット、クレデンシャルスタッフィング、カードスタッフィング、コンテンツスクレイピング、買い占めを阻止できます。

AIクローラーやボットを管理

AIクローラーをブロックする、課金する、または無限ループに閉じ込めることによって、コンテンツとコストをより強力に管理できます。リクエストパターンとrobots.txtディレクティブへの準拠状況を可視化します。Cloudflareのすべてのお客様にご利用いただけます。

主な機能	
検出エンジン	
機械学習	当社のグローバルな機械学習モデルは、毎日数十億件のリクエストをプロキシするCloudflareのグローバルネットワークの全トラフィックで訓練されており、自動トラフィックと人間によるトラフィックを識別します。これは、当社の総合的なボットスコアに含まれています。お客様は自動的に最新モデルにアップデートされます。
異常検出	当社の教師なし学習による異常挙動検出モデルは、アプリケーション固有のトラフィックパターンを基準とし、ルールしきい値を調整することで、顧客のトラフィックパターンの経時変化に対応してボットの異常挙動を特定します。これは、当社の総合的なボットスコアに含まれています。
ヒューリスティック	過去のボットトラフィックから把握した悪質なボットの挙動の既知のパターンを利用して、ボットを識別します。Cloudflareでは、すべてのお客様向けのヒューリスティックを定期的に更新しています。これは、当社の総合的なボットスコアに含まれています。
検証済みボットとAIボット	当社のボットディレクトリは、Cloudflareの検証済みボットポリシーに従って、正当な機能を果たし検証済みボットとして透明性をもって機能する既知のボットの検出IDを識別します。Cloudflareでは、robots.txtの指示を尊重しているかどうか、アプリに認識されないよう挙動隠蔽しているかどうかにかかわらず、既知のAIボット用に個別のカテゴリーを設定しています。
JavaScript検出	JavaScript検出モジュールは、リクエストのクライアント側に挿入される軽量で不可視のJavaScriptインジェクションによって、ヘッドレスブラウザやその他の悪意のあるフィンガープリントを識別します。当社は、非常に厳格なプライバシー基準を尊重し、その過程で個人を特定できる情報を一切収集しません。
ボットスコア	個々のボットIDやタイプごとにルールを作成するのではなく、ボットスコアを利用して、より少ないルールで大半のボットを捕捉します。ボットスコアは、当社の検出エンジンからの情報を統合し、リクエストがボットから送信された可能性を1～99のスコアで示します。スコア1は間違いなく自動化されたリクエストを指し、99は間違いなく人間によるリクエストを指します。
モバイルデバイスSDKを使用したデバイス検証	Android、iOS、React Native、Unityなどの主要なモバイルアプリプラットフォーム向けのSDKは、アプリの完全性を検証し、安全でない環境を検出し、APIトラフィックを認証します（自己提供またはCloudflare承認済みの暗号トークンを使用）。
ポリシーと対応	
標準対応	Cloudflareの検出エンジンによって識別されたボットトラフィックへの対応として、ブロック、許可、ログ、レート制限、またはさまざまなユーザーフレンドリーなチャレンジを設定できます。
カスタム対応ポリシー	Cloudflare WAFやDDoS ProtectionなどのCloudflare製品のポリシーにボット管理シグナルを統合し、Workersを介してカスタムアクションを記述します。
分析	
Cloudflareダッシュボード	過去30日間のボットアクティビティを確認し、ボットスコア、ボットトラフィック、およびリクエストフィルターで絞り込むことができます。ボットフィードバックループを使用してCloudflareに誤検出や検出漏れを報告し、詳細な調査を依頼することもできます。
サードパーティツール（SIEM、データレイク、分析ツールなど）	Cloudflareの統合ダッシュボードで、Cloudflare Security Analyticsを使って全アプリのボット管理シグナルを分析し、Log Explorerで追加のログデータを探し、Log Pushを介して、サードパーティのSIEMや分析プラットフォームでCloudflareデータとサードパーティデータを集約します。

さらに詳しい情報をご覧になりたいですか？
アプリケーションセキュリティのデモシリーズにご登録ください