報道関係各位

2025年5月7日
株式会社ビットフォレスト

アクセスログに潜む“見えないボット”の存在を可視化
Web攻撃ログ分析ツールLoggol（ロゴル）
2025年5月7日、新機能「ボット検知機能」をリリース

株式会社ビットフォレスト(所在地：東京都千代田区　代表取締役：高尾 都季一　以下、ビットフォレスト)は、Web攻撃ログ分析ツールLoggol(ロゴル)の新機能「ボット検知機能」を2025年5月7日にリリースいたしました。本機能の追加により、Webサイトに対するボットのアクセス状況を可視化し、悪意あるボットや不要なクローラーによるアクセスの実態を把握・特定することが可能となり、ユーザのセキュリティ対策の強化や、アクセスログ調査の効率化、さらには不要なシステム負荷の回避といった運用コストの最適化にもつながります。「ボット検知機能」はプラスプランおよびフルサポートプランをご契約のお客様がご利用いただけます。

複数のWebサイトの実データに基づくボットアクセスの可視化と傾向分析

「ボット検知機能」の実装に先立ち、Loggolでは複数のWebサイトを対象にアクセスログを分析し、ボットによるアクセスの実態を調査しました。その結果、ボットのアクセスが想定以上に多いケースが複数確認されました。今回の分析では、計22サイトのアクセスログをもとに、ログ行数からボットの割合を算出しています。

図1は、各サイトにおける総アクセス数に対して、どの程度ボットが占めているかを示したものです。最も割合が高かった「Site15」では、**全アクセスの87%がボットによるもの**という結果になりました。また、**ボットのアクセスが全体の50%を超えたサイトも全体の約4分の1（6サイト）**に上るなど、**特定のWebサイトにおいては、通常のユーザアクセスを上回るボットの存在が確認**されました。

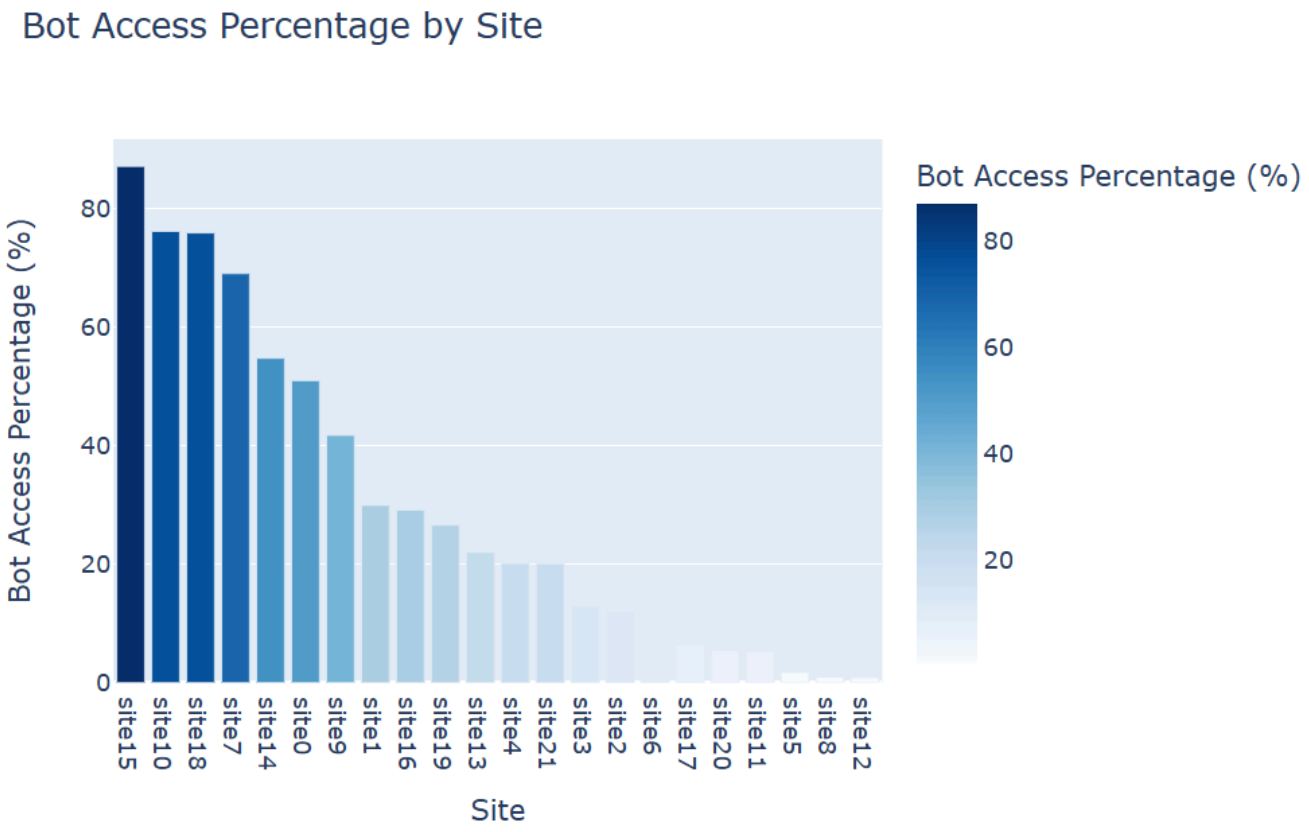

図1:サイト別 ボットアクセスの割合

続く図2では、縦軸にログ行数ベースのボット割合、横軸にIPアドレス単位でのボット割合を示しています。横軸は、全IPアドレスのうち、どの程度がボットによるものかを表しています。

最も右にプロットされている「Site10」では、**アクセスが行われた全IPアドレスのうち半数以上がボットのIPアドレス**であることになります。

また、図2の中央上部には、図1で「87%のアクセスがボットだった」とされた「Site15」がプロットされています。こちらはIPアドレス単位で捉えた場合は全体の23%がボットであることになります。つまりそれぞれのボットはボット以外のクライアントに比べ多くのアクセスを行う傾向がありそうだと推測できます。あるいは、一部のボットが非常に多くのアクセスをしているかもしれません。

このようにボットのアクセスが非常に多いサイトがあることがわかります。一方で、一部のサイトではボットのアクセスは数%程度の低い割合であり、サイトによって状況が大きく異なることがわかります。

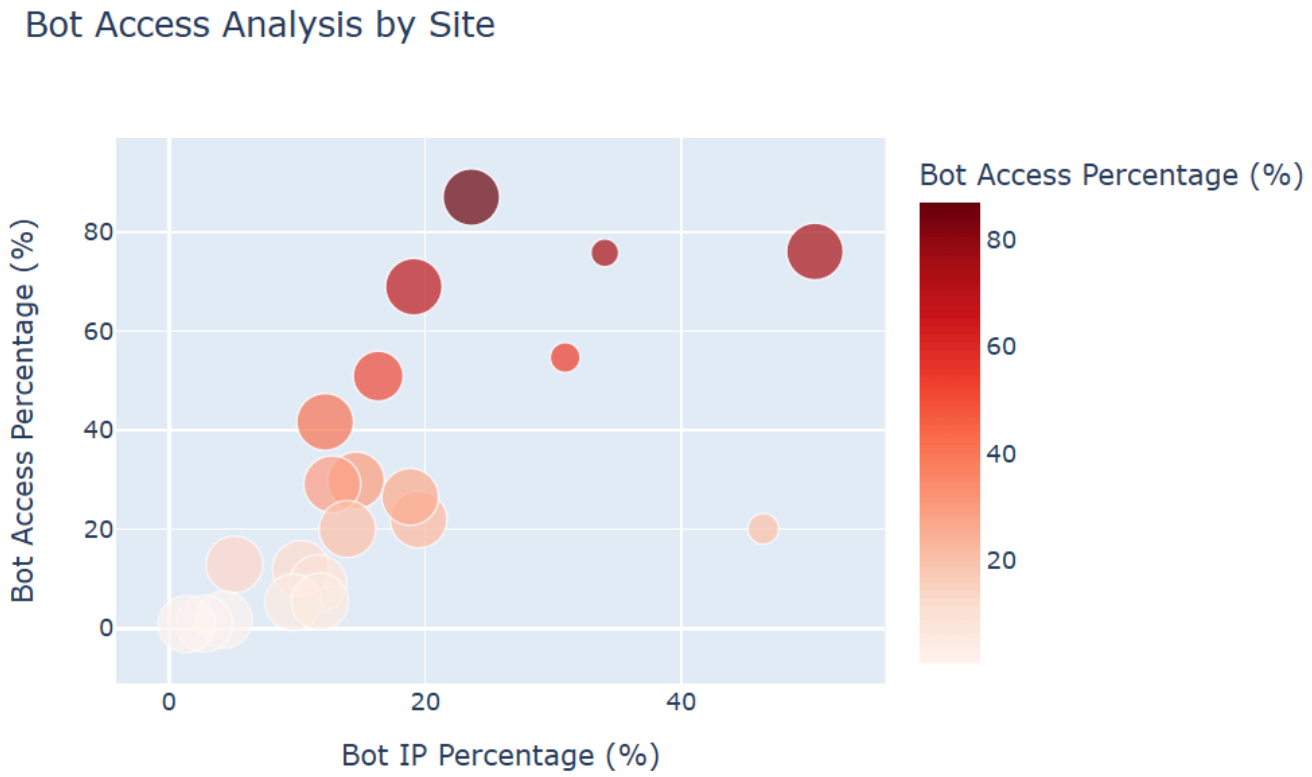

図2：IPアドレス単位でのボット割合

ボットによるアクセスがもたらす運用上の課題

ボットによるアクセスは、その目的や規模によってWebサイトに与える影響が大きく異なります。とくにクラウド環境における従量課金制のインフラを利用している場合、意図しないボットによるアクセス——たとえば競合他社による情報収集や、国外からのクローラーのような存在が頻繁に発生すると、それだけで通信量や処理コストが発生し、ビジネスに対する直接的なコスト増加につながる可能性があります。

また、小規模なWebシステムやテスト環境など、アクセス数をあまり想定していない環境では、想定外のボットアクセスが原因でサーバが不安定になるといった事例も少なくありません。

さらに、情報収集型のボットは静的な画像やCSSといったファイルよりもウェブサイトのコンテンツ自体にアクセスすることが多く、システムの負荷に直結しやすいという点でも注意が必要です。

不要なボットによるアクセスは、IPアドレス単位でのブロックやファイアウォール設定によって制限することが望ましい対策の一つです。Loggolでは、ボット判定されたIPアドレスを特定できるため、例えば海外の特定地域やISPに紐づくアドレスを除外対象とするなど、運用に即した制御が可能になります。

ボットは少量であれば問題にならないケースもあるものの、規模や頻度によっては事業コストやユーザ体験に影響を及ぼしかねない存在です。まずはその存在と動向を正確に把握することが、持続的なWeb運用における第一歩となります。

Loggolなら現行環境に影響を与えずにボットを把握

Loggolの「ボット検知機能」は、**アクセスログをアップロードするだけで、Webサイトに対するボットの動向をシンプルに可視化**できる仕組みです。従来のLoggolと同様、特別な設定やスクリプトの追加は不要で、ログをアップロードし、分析ボタンを押すだけで利用できます。

分析の結果、ボットと判定されたIPアドレスや、それぞれのIPから実際に行われたアクセス内容の一部を自動的に抽出・表示。全件出力ではなく代表的な例をピックアップすることで、実務に即した見やすさと扱いやすさを両立しています。

また、Loggolは稼働中のWebサーバやアプリケーションに変更を加えることなく、**ログファイルのみで独立して動作する点も大きな特長**です。これにより、**既存のシステムに一切の影響を与えることなく、安全かつ気軽に導入・活用することが可能**です。

「自社サイトに、どの程度のボットがアクセスしているのか？」という疑問に対し、最小限の作業で確かな可視化を実現できるのが、Loggolの「ボット検知機能」です。

無料トライアルを実施中

Loggolは14日間の無料トライアルがお試しいただけます。ご利用の際は下記URLからサインアップをお願いします。

無料トライアル：https://www.loggol.jp/trial.html

※無料トライアル・ベーシックプランでは「ボット検知機能」はご利用いただけません。

Loggolブログ

新機能「ボット検知機能」についてはLoggolブログにて詳しく解説しています。

ぜひ、Loggolブログも合わせてご確認ください。

ビットフォレスト製品について

Loggol公式Webサイト：https://www.loggol.jp/

VAddy公式Webサイト ： https://vaddy.net/ja/

Scutum公式Webサイト： https://www.scutum.jp/（販売元：株式会社セキュアスカイ・テクノロジー）

株式会社ビットフォレストについて

【会社概要】

社名：株式会社ビットフォレスト

所在地：

東京本社

〒101-0054
東京都千代田区神田錦町1-17-5 Daiwa神田橋ビル 8F
福岡オフィス
〒810-0001
福岡県福岡市中央区天神4-6-28 天神ファーストビル 6F
代表取締役：高尾 都季一
事業内容： Webアプリケーションセキュリティ製品の開発、販売
設立： 2002年2月
URL：https://www.bitforest.jp/

【本件に関する報道関係者からのお問合せ先】
株式会社ビットフォレスト 広報担当：Loggolサポートチーム
電話：03-5577-2032 メールアドレス：loggol@bitforest.jp