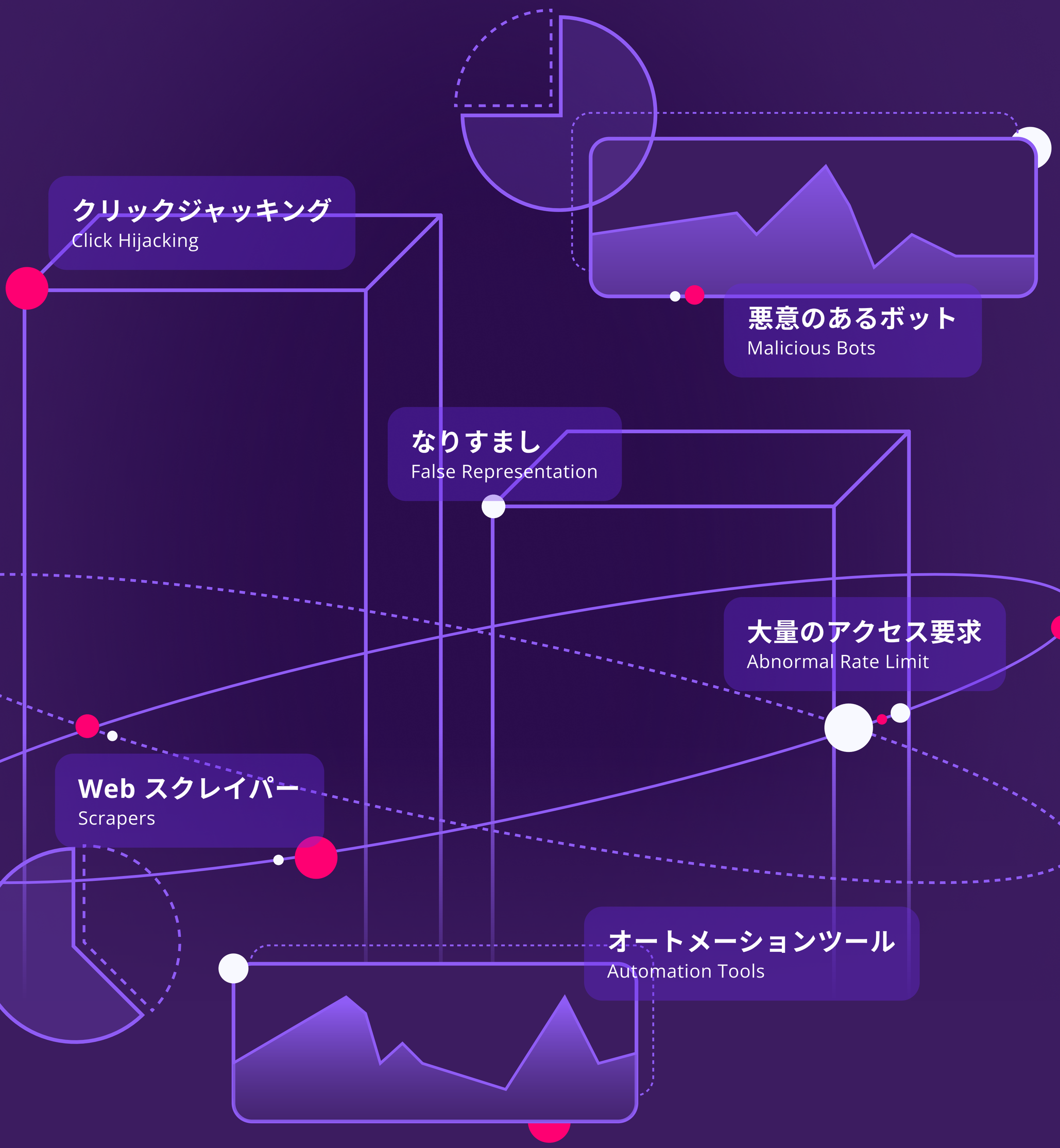
The State of Fake Traffic 2024

ボットと偽アカウントがもたらす
ビジネスへの深刻な影響



CHEQ

目次

はじめに

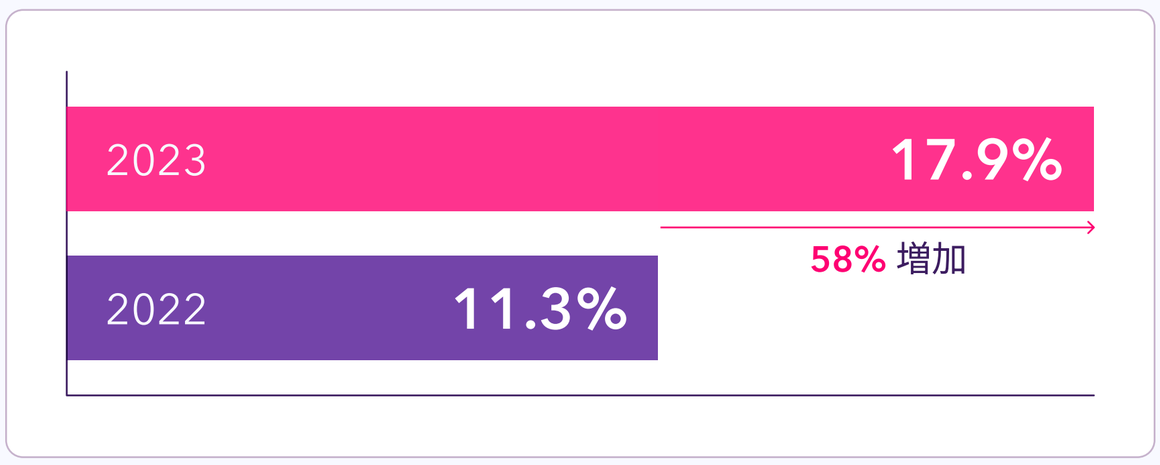
> **想像してみてください。目に見えない無数の手がインターネットを操り、オンライン体験を操作し、デジタルエコシステムを混乱させている世界を。しかも、彼らは本物のユーザーになりすまして、その正体を隠しているのです。**

これは SF 小説のような話ではありません。2024 年の現在、サイバー犯罪者や詐欺師は、単純なボットやクリックファームではなく、高度なボットを駆使して巧妙な犯罪を行っています。これらのボットは、人間のような行動を模倣し、検知を逃れ、様々な悪意のある活動を実行することが可能です。具体的には、許可なくデータを収集したり、エンゲージメント指標を不正に操作したり、詐欺行為を行ったり、ウェブサイト、モバイルアプリ、API のセキュリティと整合性を侵害したりします。

これは、善良であれ悪意あるものであれ、真の意図を持たない無数のユーザーと共存する世界。これが「偽トラフィック」と呼ばれる現象であり、その問題は深刻化しています。

この現象を私たちは「偽トラフィック」と呼んでおり、問題はますます拡大しています。今年で 2 回目になる「The State of Fake Traffic 2024」における分析では、2023 年に観測されたトラフィックの 17.9 %が自動化されているか無効であることが明らかになり、2022 年の 11.3 %から 58 %増加しました。

2023 年に監視された
全トラフィックの 17.9 %が
偽トラフィックでした。



偽トラフィックは単なる厄介者ではありません。それは戦略的なビジネス上の問題なのです。その影響は、広告効果の低下や分析の歪みから、業務の中断、不正なデータアクセス、顧客基盤の浸食など、より広範な懸念にまで及びます。これらの問題は総合的に、株主価値の低下、評判の低下、さらには市場シェアの喪失にもつながりかねないのです。

今年は、偽トラフィックの特徴を深く理解するために、業界の範囲を広げ、ボットをなりすましているブラウザやオペレーティングシステム、デバイスタイプによって分類する新しい指標を含める分析を拡大しました。

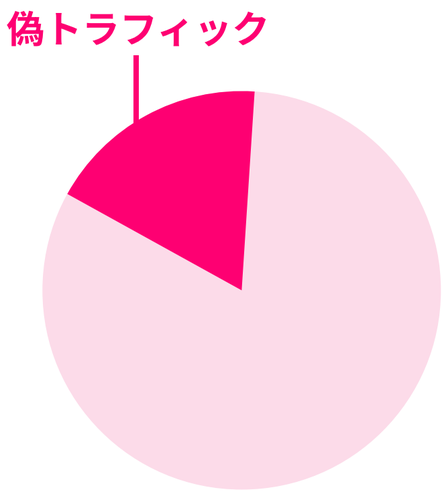
さらに、Chromedriver や Puppeteer などのボットを作成するために使用されるオートメーションツールを調査し、偽トラフィックの背後にある技術とそれがデジタル環境に与える影響について、より細かな理解を得ることができました。

概要

「The State of Fake Traffic 2024」では、自動化システム、クリックファーム、悪意のあるボットなど、デジタル環境全体で高まる脅威について重要な分析を提供しています。このレポートでは主要なトレンド、ツール、そして様々な業界への影響について取り上げています。

2023 年の状況

ボットトラフィックの増加が続いています



全トラフィックのうち

17.9 %

が偽トラフィック

58 % YoY

偽トラフィックの増加

28 % YoY

ボットの増加

特定の脅威が急増

- **悪意のあるボット**のインスタンスは前年比で 32% 増加しました。
- **自動化ツール**を使用して検出されたボットは前年比で 20% 増加しました。

偽トラフィックの影響を大きく受けている主な業界

金融・保険

17.3 % が偽トラフィック

小売・E コマース

15.8 % が偽トラフィック

ソフトウェア

14.1 % が偽トラフィック

悪意のあるユーザーにはデスクトップのユーザーエージェントが多用されています

偽トラフィック全体を見ると、71 % がデスクトップ、
29 % がモバイルから発生しています。

71 %
デスクトップ

29 %
モバイル

リサーチ手法

CHEQ は、2,000 以上のリアルタイムのサイバーセキュリティチャレンジを実施することで、各訪問の信頼性を評価しました。

このレポートのデータは、2023 年を通じて観察された 340 億のデータポイントのプールに基づいており、これらは CHEQ の数百のエンタープライズレベルのクライアントから得られました。

これらのデータポイントは、CHEQ によって保護されたクライアントのウェブサイト、アプリケーション、またはインフラストラクチャデバイスと、スマートフォン、タブレット、デスクトップコンピューター、IoT デバイス、組み込みシステムを含むさまざまなエンドポイントデバイスとの間のユニークなインタラクションを表しています。

デバイスが CHEQ によって保護されたドメインとインタラクションするたびに、2,000 以上のリアルタイムのサイバーセキュリティチャレンジにさらされ、訪問の有効性が判断されました。

CHEQ と統合技術により、偽トラフィックを即座に検知し、クライアントへ通知します。徹底的な属性分析に基づいて、トラフィックを分類します。具体的には、本物と偽りのトラフィック源を調査し、デバイスの種類、オペレーティングシステム、ブラウザ（またはボットによって自己報告されたもの）、ボット作成に使用されたツールやライブラリを特定します。

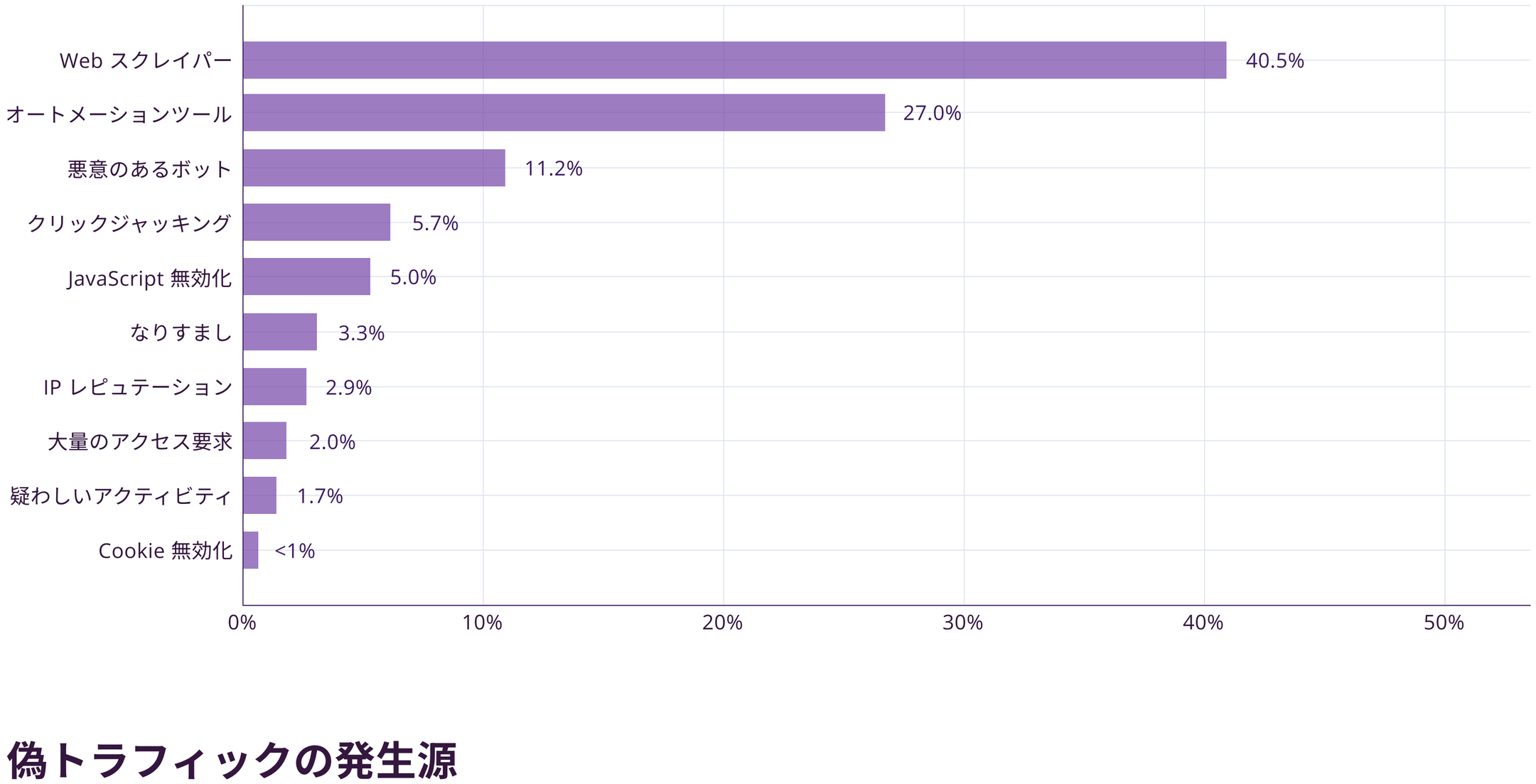
本研究では、企業における不正トラフィックについて包括的な分析を行いました。それにより、不正トラフィックの特徴、影響、脅威に関する実用的な知見と指針を導き出しました。

このレポートで提示されるデータは、最も極端なイベントを除外して正常化のプロセスを経ており、このレポートで表されるトレンドが珍しいまたは例外的な発生によって影響を受けないようにしています。

偽トラフィックの脅威の種類と流入元

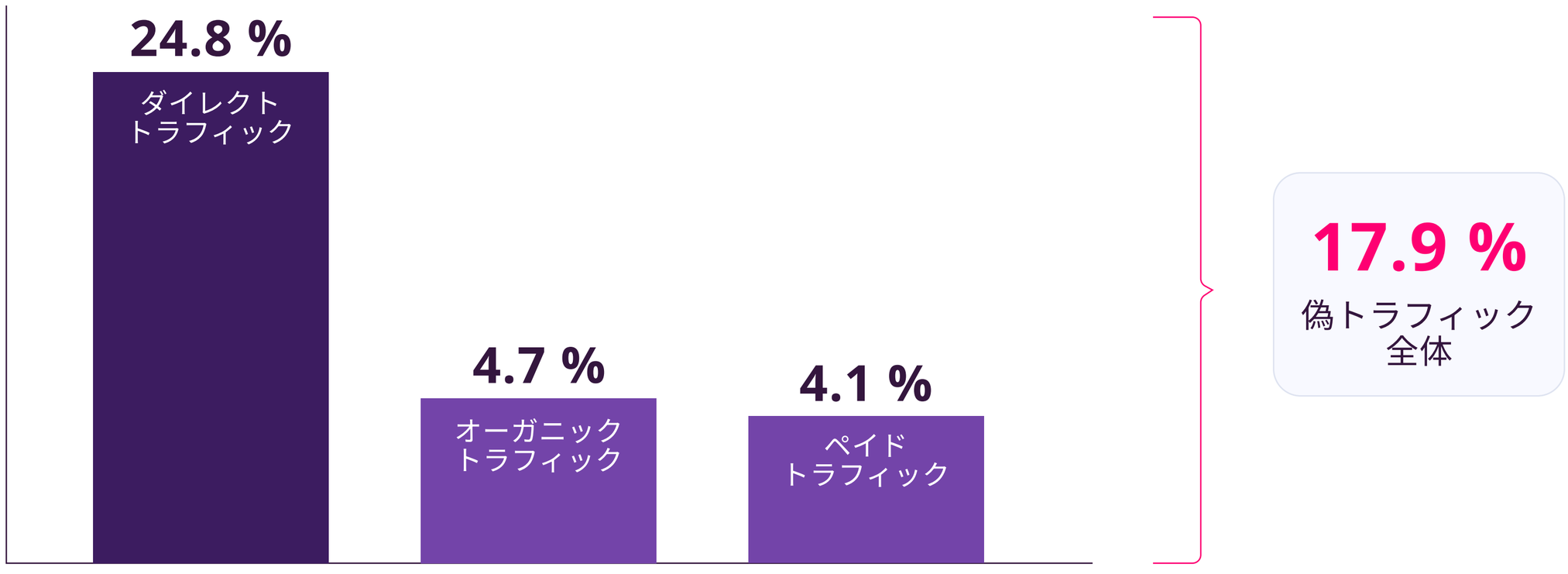
偽トラフィックの脅威のトップ 10

2023 年の業界全体における脅威のトップ 10 には、Web スクレイパー、自動化ツール、悪意のあるボットが含まれています。生成 AI の台頭と並行して、ユーザーがボットを簡単かつアクセスしやすく作成できるようになっていることに起因しています。



偽トラフィックの発生源

偽トラフィックの発生源を分析したところ、ダイレクトトラフィックが最も高い割合を占めていました。24.8 %という数字は、前年の 22.1 %から増加しています。ダイレクトトラフィックは正規のユーザーからの高い関心を示す場合もありますが、悪意のあるボットやユーザーが攻撃対象とするサイトに迅速にアクセスするためによく使用される方法でもあります。



業界別　偽トラフィック

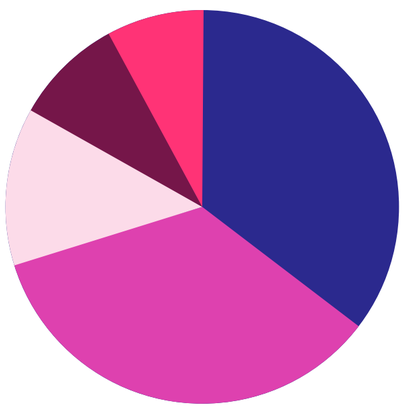
近年、様々な規模の企業が、ニセの閲覧者によるアクセス増加という問題に悩まされています。特に、オンライントラフィックや広告収入に依存する業界は、不正行為の影響を受けやすい傾向があります。当社が世界各地の様々なクライアントから得たデータ分析によると、企業の業種はニセの閲覧者によるアクセス増加に大きく影響を与えることが明らかになりました。

小売・EC、ソフトウェア、金融・保険、高等教育などの主要な業界では、偽トラフィックの割合がそれぞれ 15.8 %、14.1 %、17.3 %、15.7 %に達しました。

以下のグラフは、業界ごとの平均偽トラフィック率、5 つの主要な脅威の種類、偽トラフィックのトップソースを詳細に示しています。

金融・保険

金融サービス、銀行、保険



脅威の 5 つのタイプの内訳

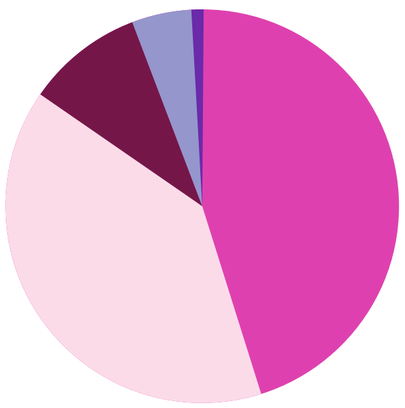
IP レピュテーション	35.5 %
オートメーションツール	35.0 %
Web スクレイパー	12.2 %
悪意のあるボット	9.1 %
JavaScript 無効化	8.0 %

偽トラフィック率合計：17.3 %

ダイレクト　：18.9 %
オーガニック　：13.2 %
ペイド　：10.3 %

ヘルスケアとライフサイエンス

医療サービス、製薬、バイオテクノロジー



脅威の 5 つのタイプの内訳

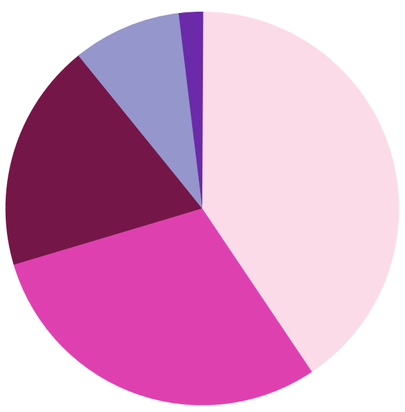
オートメーションツール	48.8 %
Web スクレイパー	39.7 %
悪意のあるボット	9.0 %
なりすまし	4.6 %
クリックジャッキング	1.0 %

偽トラフィック率合計：9.5 %

ダイレクト　：17.0 %
オーガニック　：3.4 %
ペイド　：2.8 %

高等教育

非営利大学や営利大学



脅威の 5 つのタイプの内訳

Web スクレイパー	41.4 %
オートメーションツール	29.5 %
悪意のあるボット	18.7 %
なりすまし	8.9 %
大量のアクセス要求	1.3 %

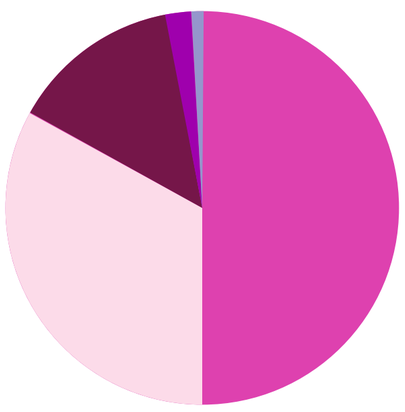
偽トラフィック率合計：15.7 %

ダイレクト　：29.4 %
オーガニック　：4.5 %
ペイド　：9.0 %

業界別　偽トラフィック

製造

建設、住宅リフォーム、インフラ整備



脅威の 5 つのタイプの内訳

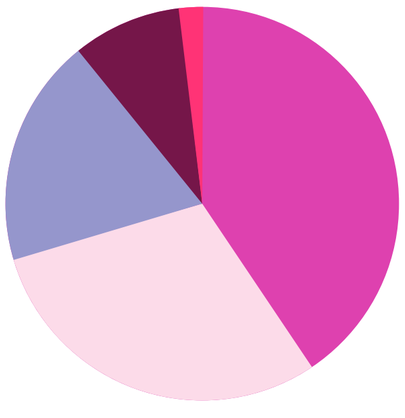
オートメーションツール	50.4 %
Web スクレイパー	33.7 %
悪意のあるボット	14.0 %
Cookie 無効化	<1 %
なりすまし	<1 %

偽トラフィック率合計：16.8 %

ダイレクト　：30.9 %
オーガニック　：3.2 %
ペイド　：6.0 %

広告・マーケティング

広告・マーケティングサービスと代理店



脅威の 5 つのタイプの内訳

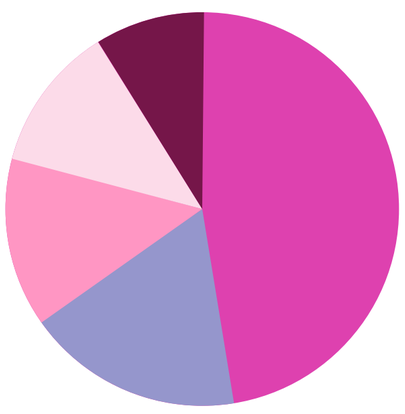
オートメーションツール	41.4 %
Web スクレイパー	29.5 %
なりすまし	18.7 %
悪意のあるボット	8.9 %
JavaScript 無効化	1.3 %

偽トラフィック率合計：17.4 %

ダイレクト　：29.5 %
オーガニック　：13.6 %
ペイド　：6.3 %

メディア・出版

伝統的なニュース出版社とデジタルニュース出版社



脅威の 5 つのタイプの内訳

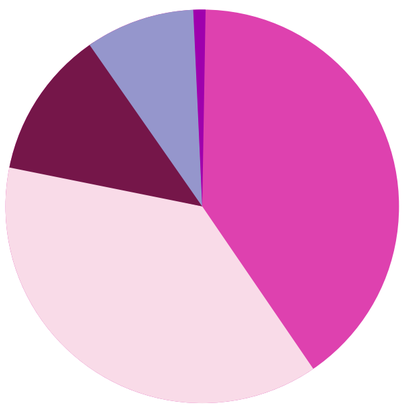
オートメーションツール	47.8 %
なりすまし	17.6 %
疑わしいアクティビティ	14.2 %
Web スクレイパー	11.7 %
悪意のあるボット	8.4 %

偽トラフィック率合計：10.4 %

ダイレクト　：10.3 %
オーガニック　：11.8 %
ペイド　：3.0 %

不動産

不動産開発、賃貸、および販売



脅威の 5 つのタイプの内訳

オートメーションツール	47.8 %
Web スクレイパー	37.8 %
悪意のあるボット	12.2 %
なりすまし	9.1 %
Cookie 無効化	<1 %

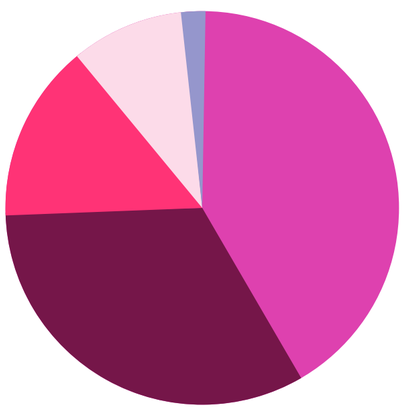
偽トラフィック率合計：10.6 %

ダイレクト　：34.4 %
オーガニック　：3.1 %
ペイド　：3.4 %

業界別　偽トラフィック

小売・EC

店舗型、オンライン型、D2C



脅威の 5 つのタイプの内訳

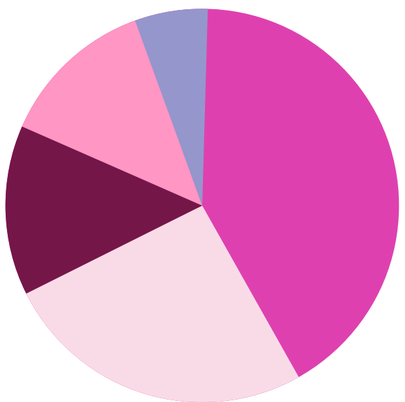
オートメーションツール	41.8 %
悪意のあるボット	32.7 %
JavaScript 無効化	14.5 %
Web スクレイパー	9.0 %
なりすまし	1.8 %

偽トラフィック率合計：15.8 %

ダイレクト	：32.6 %
オーガニック	：3.75 %
ペイド	：3.3 %

ソフトウェア

エンタープライズ向けとコンシューマー向けのソフトウェア開発企業



脅威の 5 つのタイプの内訳

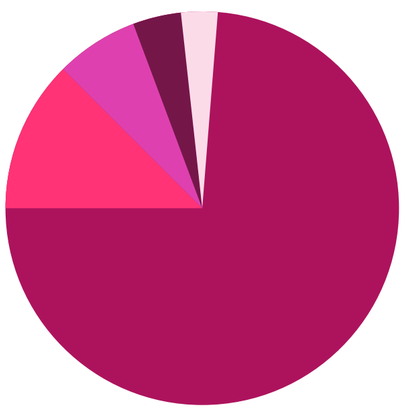
オートメーションツール	42.1 %
Web スクレイパー	25.8 %
悪意のあるボット	13.5 %
疑わしいアクティビティ	13.1 %
なりすまし	5.2 %

偽トラフィック率合計：14.1 %

ダイレクト	：22.5 %
オーガニック	：4.5 %
ペイド	：2.7 %

旅行・レジャー

旅行・ホスピタリティ・エンターテインメント・サービス



脅威の 5 つのタイプの内訳

クリックジャッキング	75.5 %
JavaScript 無効化	11.8 %
オートメーションツール	6.1 %
悪意のあるボット	3.7 %
Web スクレイパー	2.7 %

偽トラフィック率合計：11.9 %

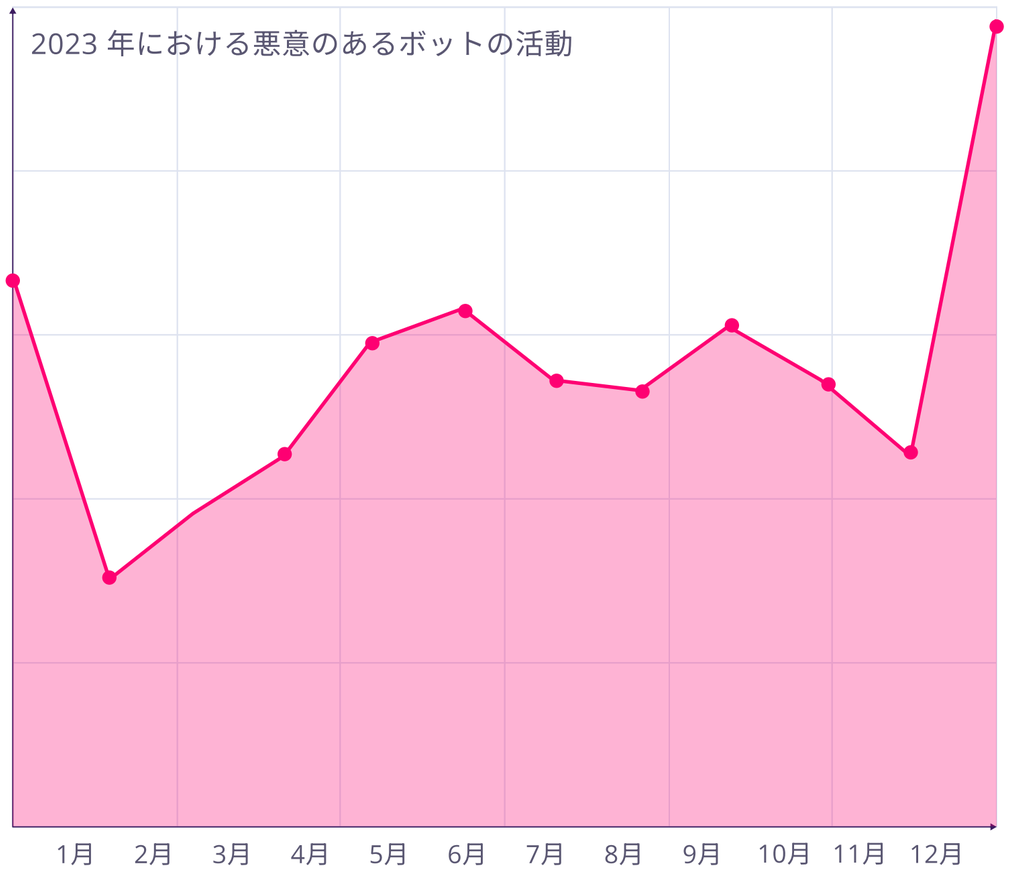
ダイレクト	：13.4 %
オーガニック	：3.1 %
ペイド	：2.4 %

2023 年のトレンド：ホリデーシーズンに急増

年末年始、悪意のある活動が急増！

2023 年 12 月のホリデーシーズンには、悪意のあるトラフィックが急増しました。特に、小売業と旅行業を標的としたボットによる活動が顕著でした。

この急増は、ボットを人間のトラフィックに偽装することを目的としたオートメーションツールの使用が特徴的でした。特に 12 月は、これらのボットの能力が大幅に向上し、リソースの枯渇から在庫枯渇攻撃まで、深刻な脅威をもたらしました。



実例：BaaS（Bots-as-a-Service）の台頭

2023 年末に悪意のあるトラフィックが急増した要因の一つは、BaaS（Bots-as-a-Service）プラットフォームの台頭です。これらのプラットフォームは、高度な自動化ツールを提供しており、技術的なスキルがなくても簡単に利用することができます。この利便性とアクセシビリティの向上により、潜在的な攻撃者の範囲が広がり、わずかな労力で広範囲にわたる攻撃を仕掛けることが可能になりました。

具体的な例としては、12 月に旅行業界のドメインに対して行われた標的型攻撃があります。よく知られている BaaS プラットフォームが、Google 検索広告経由の不正なクリックスルーを 14 倍に増加させたことを検知しました。これは、重要な販売期間中にターゲット企業の PPC 予算を意図的に枯渇させるための攻撃とみられます。

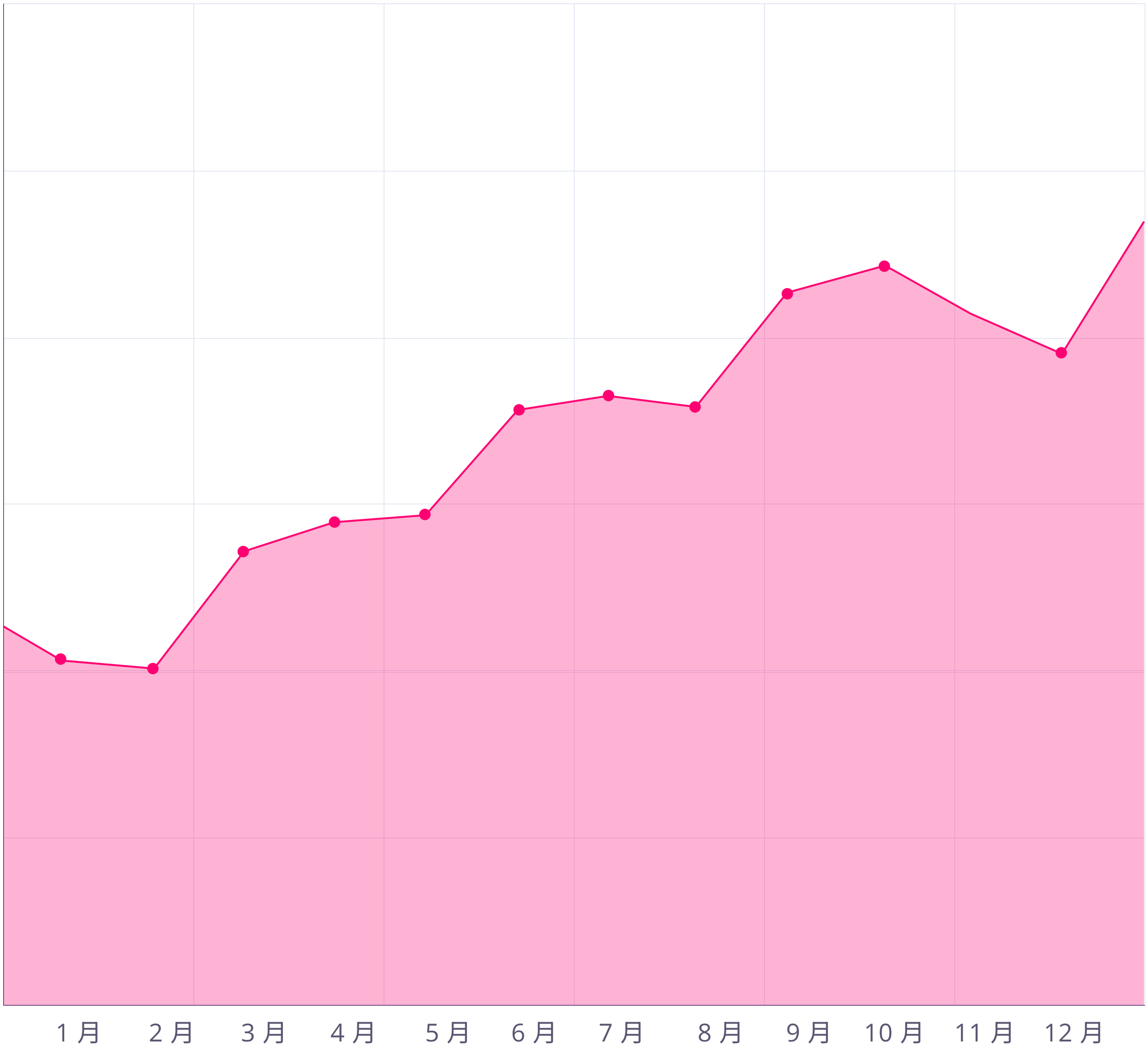
2023 年のトレンド：自動化ツールの台頭

オートメーションツールによる偽トラフィック、2023 年には 24 %に到達

2023 年、オートメーションツールによる偽トラフィックは全体の 24.0 %に達しました。特に小売業や EC 業界で被害が顕著であり、これらツールがスクレイピングや悪用目的で広く使用されていることを示唆しています。

検知されたオートメーションツールの中で最も多かったのは、オープンソースのブラウザオートメーションフレームワークとして知られる Selenium と、Mozilla の Firefox Web ブラウザを制御・操作するためのオートメーションドライバーである Marionette でした。

2023 年におけるオートメーションツールの活動



2023 年のトレンド：高度な回避策で対抗

増える検知困難な Chrome Driver と Puppeteer-extra-plugin-stealth の使用を追跡

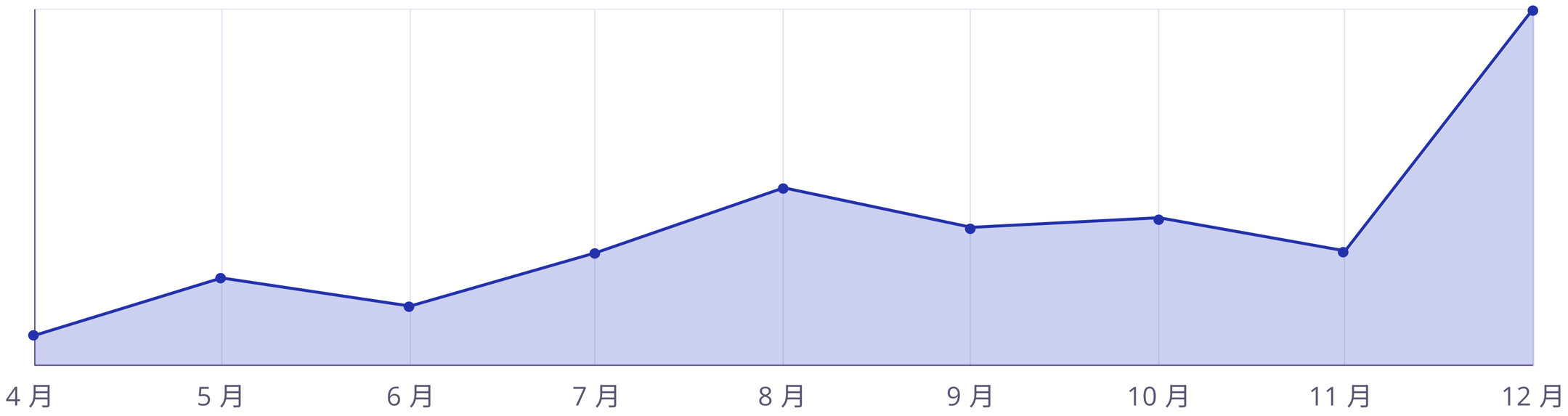
近年、自動テストを実行する開発者だけでなく、悪意のあるWebトラフィックを自動化するボット作成者にとっても、Headless Chromeは非常に有用なツールとなっています。しかし、Headless Chromeを用いた自動化は、「navigator.webdriver」などの特定のプロパティやフィンガープリントを通じて容易に検知されてしまうという課題がありました。

この対策として、ボット作成者は高度なツールに目を向け始めています。無検知のChromeDriverとPuppeteer-extra-stealth-pluginは、自動化の痕跡を隠し、より人間的な操作を模倣するように設計されています。これらのツールは、アンチボットシステムがチェックするブラウザ属性を改変し、自動化されたブラウザを通常のユーザーブラウザとして見せかけるのです。

当社のデータは、これらの検出回避ツールの利用拡大と潜在的な影響を裏付けています。2023 年第 2 四半期から第 4 四半期にかけて、Undetected ChromeDriver の利用は急増し、2023 年を通して検出された事例は 650 %増加しました。同様に、より一般的なツールである Puppeteer-extra-plugin-stealth の導入数は、ピーク時には 414 %増加しました。

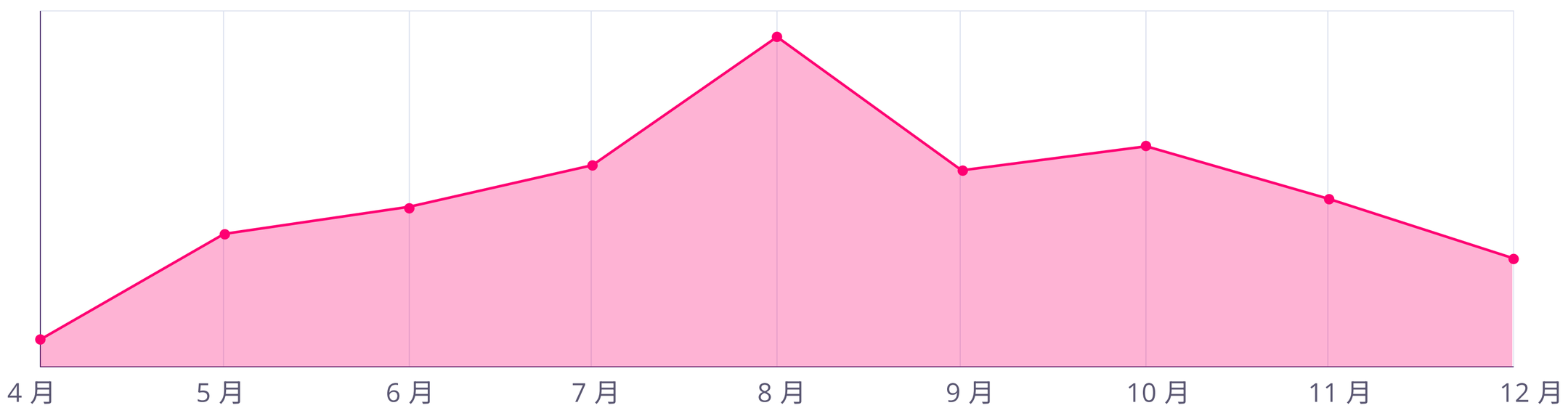
Undetected ChromeDriver を使用したボット

2023 年 第 2 四半期から第 4 四半期



Puppeteer-extra-plugin-stealth

2023 年 第 2 四半期から第 4 四半期



2023 年のトレンド：ユーザー環境別

ユーザー環境別の偽トラフィック

ユーザー環境の分類による偽クトラフィックの分析から、デスクトップ プラットフォームでは 32.6 %という高い無効率が明らかになりました。この背景には、デスクトップ環境が広く普及し、ビジネスや企業活動においても主力として利用されている点が挙げられます。加えて、攻撃者にとってデスクトップ環境は使い慣れた環境であり、攻撃手法も確立されていることから、不正行為の標的となりやすいと考えられます。

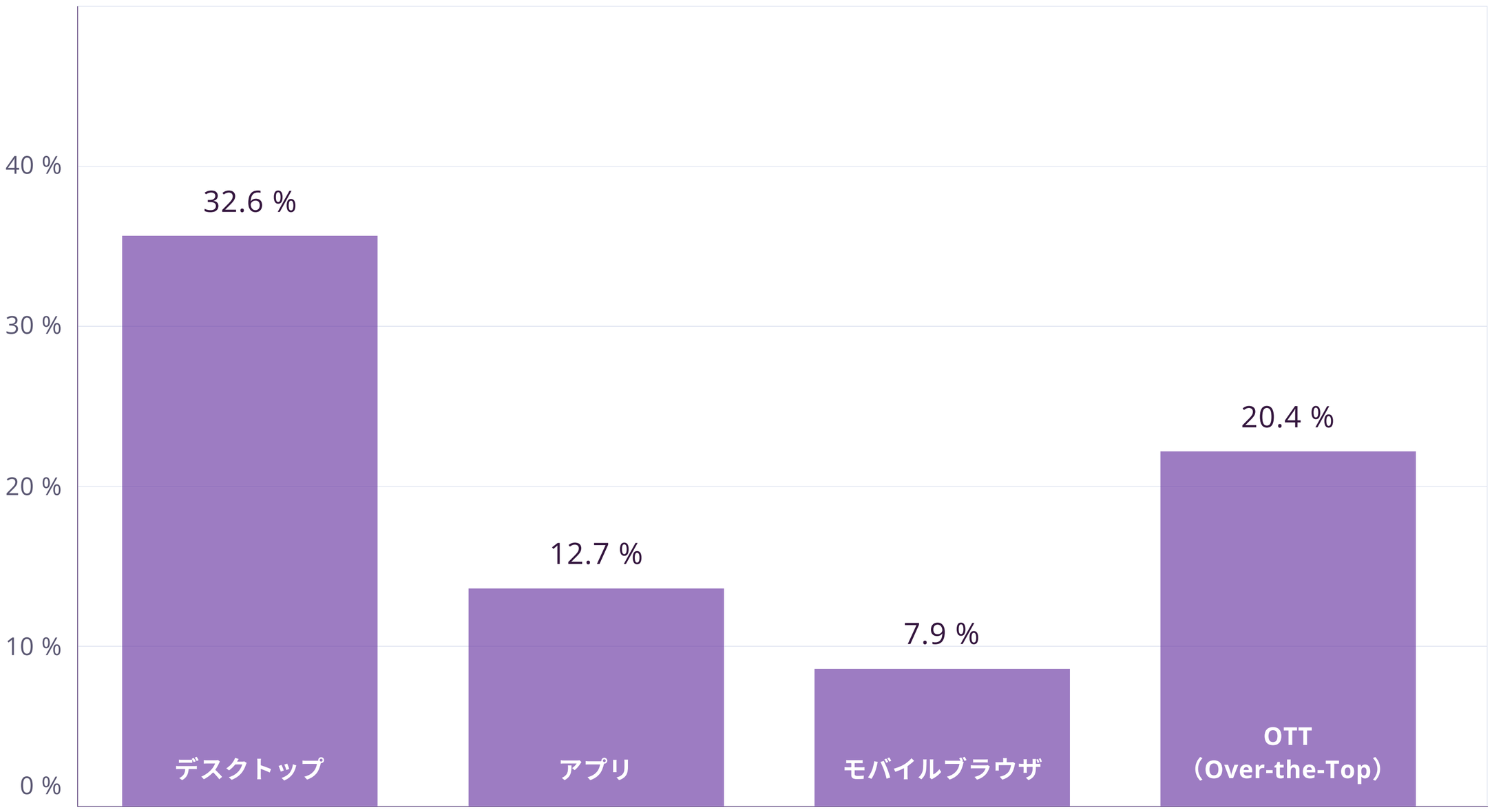
インターネットに接続されたデバイスを介してストリーミング コンテンツを配信する技術である OTT（Over-the-Top）環境では、偽トラフィック率が 20.4 %と、他の環境と比べて非常に高いことが明らかになっています。これは、OTT 広告の広告単価が高いこと（平均 3,700 円から 6,000 円の CPM）と、OTT 広告配信の複雑さの両方によって引き起こされています。

* 1 米ドル＝ 149.75 円にて換算

近年、動画配信において注目を集めているのが「サーバーサイド広告挿入（SSAI）」です。SSAI は、広告主にとって柔軟かつ効率的な広告配信を可能にする一方で、クライアントサイドの広告検証ツールが広告の正当性を評価できなくなったり、ユーザーデータを隠蔽したり、広告の積み重ねやドメインスプーフィングを可能にしたりすることで、意図せずに広告詐欺の扉を開けてしまう可能性もあります。

一方で、モバイル Web では偽トラフィックの割合が 7.9 % と著しく低くなっています。これは、デスクトップや OTT プラットフォームと比較して、収益性が低いと認識されているため、攻撃者からの関心も低くなっています。

ユーザー環境別の偽トラフィック



2023 年のトレンド：オペレーティングシステム別

オペレーティングシステム別の偽トラフィック

2023 年の当社の分析では、デバイスごとの偽トラフィックの蔓延状況について驚きの結果が明らかになりました。この分析結果から、悪意ある行為者の間で新たに浮上している手口を解き明かすことができます。

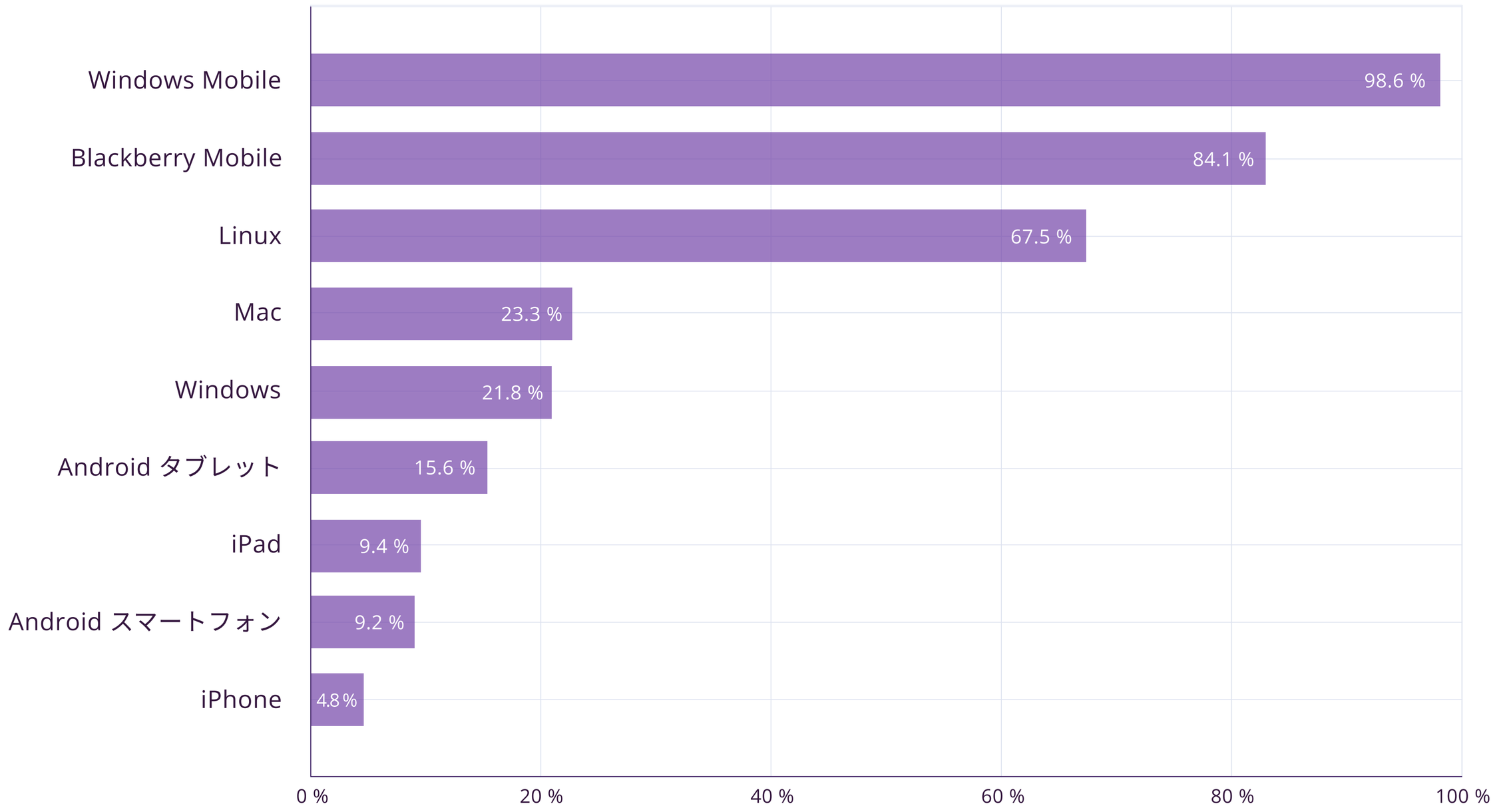
デスクトップとモバイルの偽トラフィック率を比較すると、興味深い現象が見られます。利用者がほとんどいない古い携帯 OS である Windows Mobile や Blackberry からのトラフィックは、他のどのモバイル OS よりも偽トラフィックの割合が圧倒的に高かったのです。

これは、攻撃者が古い端末を使用しているわけではなく、何年も更新されていない古いボットが原因である可能性が高いと考えられます。また、攻撃者が気付かれないように、ニッチなプラットフォームを装っている可能性もわずかにあります。

これらの調査結果は、トラフィックソースを厳しく監視し、堅牢な検証メカニズムを導入して、不正行為の影響を軽減することが重要であることを強調しています。

さらに、主要なデスクトップデバイスで観測された偽トラフィックの割合は、主要なモバイルデバイスよりも高かったことから、デスクトッププラットフォームが攻撃者にとって魅力的なターゲットであることがわかります。デスクトップ上でボット攻撃を仕掛けるのは比較的容易であり、マーケターにとって大きな課題となっています。なぜなら、このような攻撃はパフォーマンス指標を歪め、デジタル広告チャネルへの信頼を損なうからです。

オペレーティングシステム別の偽トラフィック率



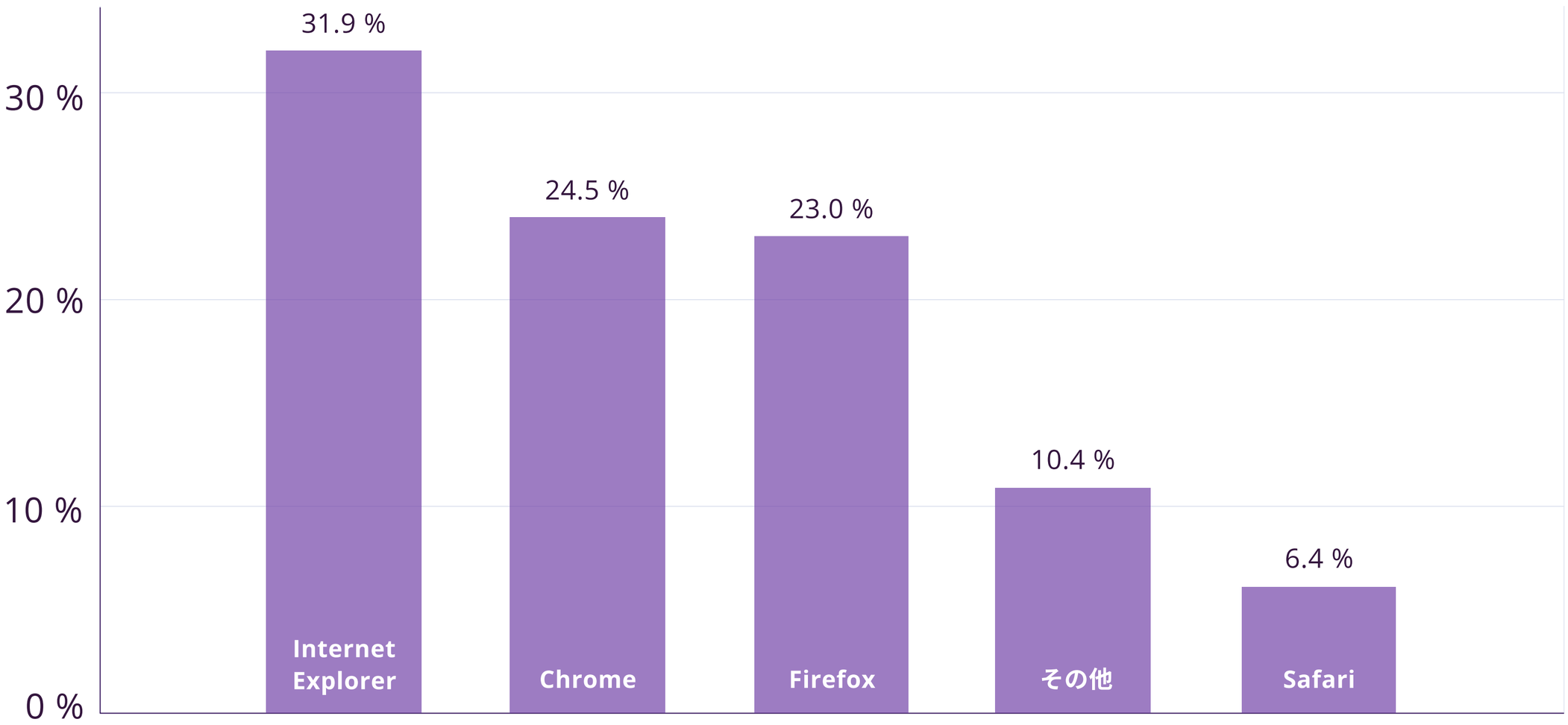
2023 年のトレンド：ブラウザ別

ブラウザ別の偽トラフィック

ユーザーエージェントから抽出されたブラウザ情報は、偽トラフィックの動向を分析するもう一つの手がかりとなります。特に、偽トラフィックは本物のユーザーと混ざり込むために、様々なブラウザ情報偽装を行う点が特徴です。

インターネットエクスプローラー（IE）は、利用率が低くなったとはいえ、偽トラフィック率は 31.9 %と高止まりしています。これは、悪意のある行為者が、古いブラウザや更新頻度の低いブラウザを悪用しやすいことを示しています。

ブラウザ別の偽トラフィック率



まとめ

ボットや偽造トラフィックによる脅威は、常に変化しているため、あらゆる業界の企業は積極的で適応性のある対策を行う必要があります。

2023 年は、生成 AI の導入が飛躍的に進んだ年でしたが、同時に、この脅威に新たな側面をもたらしました。生成 AI 技術は、ボットの作成を民主化し、誤情報を急速に拡散し、言語学習モデルのスクレイピングによる著作権侵害の可能性など、企業にとって新たなリスクを生み出す可能性を秘めています。この容易さは、デジタルプラットフォームに新たなボットの流入をもたらし、偽トラフィックや自動攻撃に関連するリスクを拡大する可能性があります。

現代のサイバー空間は、絶えず変化し、新たな脅威が次々と出現しています。悪意のあるボットや偽トラフィックは、企業にとって深刻な被害をもたらす可能性があります。顧客情報の漏洩、ブランドイメージの毀損、収益の減少など、さまざまなリスクが潜んでいます。

このような脅威からビジネスを守るためには、常に警戒を怠らず、防御体制を強化し続けることが重要です。人工知能（AI）技術の進歩に対応した積極的な対策を講じることで、新たな脅威を先取りし、安全なデジタルプレゼンスを維持することができます。

CHEQ について

CHEQ は GTM セキュリティの第一人者として、新興ブランドから Fortune 50 まで、世界中 1 万 5000 社以上のお客様に利用されています。インターネット上の悪質なトラフィックからデータ分析、マーケティング活動、およびお客様情報を保護しています。

CHEQ は、独自の状況に応じた検出エンジンを搭載し、ビジネスの継続性、ブランドの評判、プライバシーコンプライアンス、マーケティングの効果を脅かす脅威から Go-to-Market のオペレーションを保護するための、最も包括的なソリューションセットを提供しています。そのため、CISO は CHEQ を信頼し、マーケターは CHEQ を愛用し、より多くの企業が CHEQ を選択しているのです。

悪質なボットや偽トラフィックが、あなたの Go-to-Market 活動をどのように妨害しているのか、今すぐ確認しましょう。

無料診断も行なっているので、ぜひご連絡ください。

SaaS レビューサイトで高評価を獲得

Leader 2024

Easiest To Do Business With 2024

Best Support 2024

Momentum Leader 2024