調査レポート | 2023

不正トラフィック
業種別の傾向と予測

CHEQ

目次

はじめに

不正トラフィックとは

インターネットは、過去40年間で大量の情報が行き交う高速道路のような存在になりました。インターネット上では、日々数十億人のアクティブユーザーが数兆件のエンゲージメントを行っており、世界中で技術革新や経済成長を促進し、人々をつなげています。

しかし、インターネットの規模が拡大し、技術が進歩する一方で、トラフィックの品質や信頼性は低下し、オートメーションツールやボット、さらに、いろいろな要因で偽ユーザーが溢れるようになりました。このようなトラフィックは不正トラフィックと言われています。

不正トラフィックとは、ボットや偽ユーザーなど実際の顧客にならないネットワーク上のやりとり、情報またはその量のことです。これには、検索エンジンのクローラーのような無害なボットも、アドフラウドを実行するボットネットのような悪質なトラフィックも含まれます。調査によるとトラフィックの40%以上※が不正であることが判明していますがそのすべてがビジネスに影響を与えるわけではありません。当ホワイトペーパーでは、企業や消費者向けの Web サイトに影響を与える不正トラフィックについて説明します。

マーケターにとって、不正トラフィックは懸念材料です。なぜなら貴重な広告費を浪費し、不正リードでファネルを汚染し、最終的にはそれがデータ分析の結果を歪めることにより、意思決定を不正確にしてしまうからです。

それにとどまらず、不正トラフィックの影響はマーケティング部門を超えて拡大し、戦略的なビジネス課題になっています。

Twitter、PayPal、Ticketmaster をはじめとした、さまざまな企業による GTM（Go-To-Market、 市場開拓）施策は気づかないうちにサイバー犯罪の標的となっており、ビジネスをリスクにさらしています。当ホワイトペーパーでは、拡大する不正トラフィックがビジネスに与える課題や影響についても解説します。

※Wired.com, 2022

はじめに

GTM 戦略への影響

不正トラフィック対策は従来、IT やセキュリティチームが担当しており、GTM 戦略への影響はほぼ見過ごされてきました。しかし、企業の経営陣が現在気づいているように、不正トラフィックは、新製品やサービスの市場導入や販売促進のための戦略立案や実行の役割を担う GTM チームが多く直面する問題であり、ビジネス全体のセキュリティを脅かす可能性があります。

売上を促進するために Web 経由のトラフィックが欠かせないマーケターや企業にとって、こうした状況は独自の課題を生み出します。不正トラフィックの拡大は、ほぼすべてのファネル、キャンペーン、オペレーションに多かれ少なかれ影響を与え、場合によって深刻な被害をもたらします。

不正トラフィックの侵入は、オーディエンスデータや、CDP（顧客データプラットフォーム）セグメント、CRM（顧客管理システム）を汚染することで、その歪められたデータによりキャンペーンを偽ユーザーに向けて最適化してしまうため、機会損失を引き起こします。また不正データがデータ分析や BI システムの分析結果を歪めるとインサイトの精度が低下し、さらに不正確な情報に基づいた意思決定をし、悪循環に陥ります。

偽リードや偽ユーザーは Web サイトやコンバージョンのファネルを妨害し、ビジネス全体に大きな損失を与えかねないため、不正トラフィックへの対策は急務です。

当調査では、不正トラフィックの脅威の拡大や被害状況に注目しています。2022年に数千件の Web サイトと、数十億件の正当および不正なアクセスから収集したデータに基づいた、不正トラフィックを構成する脅威の種類の多様化、不正トラフィックが各業界・業種、国、地域に与える影響、マーケティングチャネル毎の不正トラフィックの内訳をご確認いただけます。

また、上記のデータを利用して、2023年の不正トラフィックの傾向を予測し、マーケティングおよびセキュリティチームがこの深刻化する課題に対処するための方法についても論じていきます。

**「不正トラフィックの侵入は
オーディエンスデータや、CDP セグメント、
CRM を汚染し、キャンペーンを
偽ユーザーに向けて最適化してしまうため
機会損失を引き起こします。」**

要旨

2022年の不正トラフィック率

１万5000社以上の CHEQ 利用企業様の不正トラフィック率を調査したところ、ブロックされた不正トラフィックの量は2021年比で**167%増**と、かつてないレベルで増加していました。

11.3%
全トラフィックの不正トラフィック率

5.9%
ペイドの不正トラフィック率

5.7%
オーガニックの不正トラフィック率

22.1%
ダイレクトの不正トラフィック率

注目すべき数字

10回に１回
偽ユーザーによるサイトアクセス

50回に 1回
悪質なユーザーによるサイトアクセス

357億米ドル
// 約４兆8195億円※
損失した広告予算

1428億米ドル
// 約19兆2780億円
機会損失

※以下１米ドル＝135円にて換算（2023年５月現在）

要旨

拡大する脅威

2022年、不正トラフィックの攻撃の手法や種類は全体的に拡大しましたが、以下３種の脅威は特に目立ちました。

125%
クリックジャッキング攻撃の増加率

112%
悪質なボットによる攻撃の増加率

101%
Web スクレイパー攻撃の増加率

被害の大きい業界・業種

不正トラフィックは、Web を利用するすべての業界・業種に影響を与えますが以下３業界の被害は特に深刻でした。

49.1%
娯楽・ギャンブル

20%
IT・SaaS

17.3%
通信

調査方法

GTM セキュリティの世界的な第一人者である CHEQ は、Web 上のさまざまなダイレクトおよびオーガニックトラフィックやペイドマーケティング経由のトラフィックの挙動を頻繁に調査し、各トラフィックがボット、悪質なユーザー、または正当な関心を持つ人間のユーザーであるかどうかを判断しています。

「不正トラフィック最新情報 2023」は１万5000社以上の CHEQ の利用企業様のデータを過去１年分析した結果を利用したものです。CHEQ は、お客様が所有・運営するドメインにアクセスしたユーザーに対して、2000項目以上のセキュリティチェックをリアルタイムを行い、各アクセスの正当性を識別しました。

不正である、または悪意があると判断されたトラフィックは、お客様に悪影響を及ぼす前にブロックまたはリダイレクトしました。

トラフィックを識別した後、流入元（ダイレクト、オーガニック、ペイド）、業界・業種、地域、脅威の種類ごとに不正トラフィック率を分類しました。

当調査の目的は、インターネット上の不正トラフィックを分析し、その特徴、影響、被害の実態について、実用的な考察や指針を提供することです。

そして、これらの不正トラフィック率と外部指標を組み合わせて、マーケティングによって創出された収益に不正トラフィックが与える影響、営業業務、および BI 主導の意思決定に与える影響を算出しました。

不正トラフィック　３つの大分類

不正トラフィックの３つの脅威グループと、いくつかの具体例を見ていきましょう。

疑わしい無効アクティビティ

疑わしい無効アクティビティは、弊社の2000以上ある検知項目に１つ以上該当したトラフィックです。 不審なトラフィックは、プロキシ、VPN、および偽の個人情報を利用して身元を隠そうとしているデータセンターまたはユーザーによるものであることが多いです。 2022年には、疑わしい無効アクティビティが不正トラフィック全体の **44.3%** を占め、2021年の21.8%から２倍以上になりました。

ボットによる無効アクティビティ

Twitter ボット対イーロン・マスク氏の戦いからテイラー・スウィフトのツアーのチケット買い占め、奨学金の不正獲得を目的とした大学への「入学」に至るまで、ボットは2022年のニュースに多く取り上げられました。

ボットとは、あらかじめ定義されたタスクを自動で実行するツールやシステムのことです。ボットは人間の行動を真似て、なりすますことが可能で、分散型サービス拒否（DDoS）攻撃やアドフラウドなど、悪質な目的に使用されることがあります。2022年、ボットによる無効アクティビティは不正トラフィック全体の **38.2%**を占め、2021年の30.1%から増加しました。

悪意がある無効アクティビティ

悪質なユーザーは、犯罪目的で偽のアクティビティを作成します。 多くの場合、悪質なユーザーは、カードスキミングやアカウント乗っ取り攻撃の標的を探しています。2022年、明らかに悪意があると判定されたトラフィックは、CHEQ がブロックしたすべての不正トラフィックの**17.4%**、調査対象のトラフィック全体の2%となりました。つまり、Web サイトへのアクセスの50回に１回は、悪意がある無効アクティビティであることになります。

３つの脅威グループの内訳

44.3%
疑わしい無効アクティビティ

38.2%
ボットによる無効アクティビティ

17.5%
悪意がある無効アクティビティ

脅威のタイプ

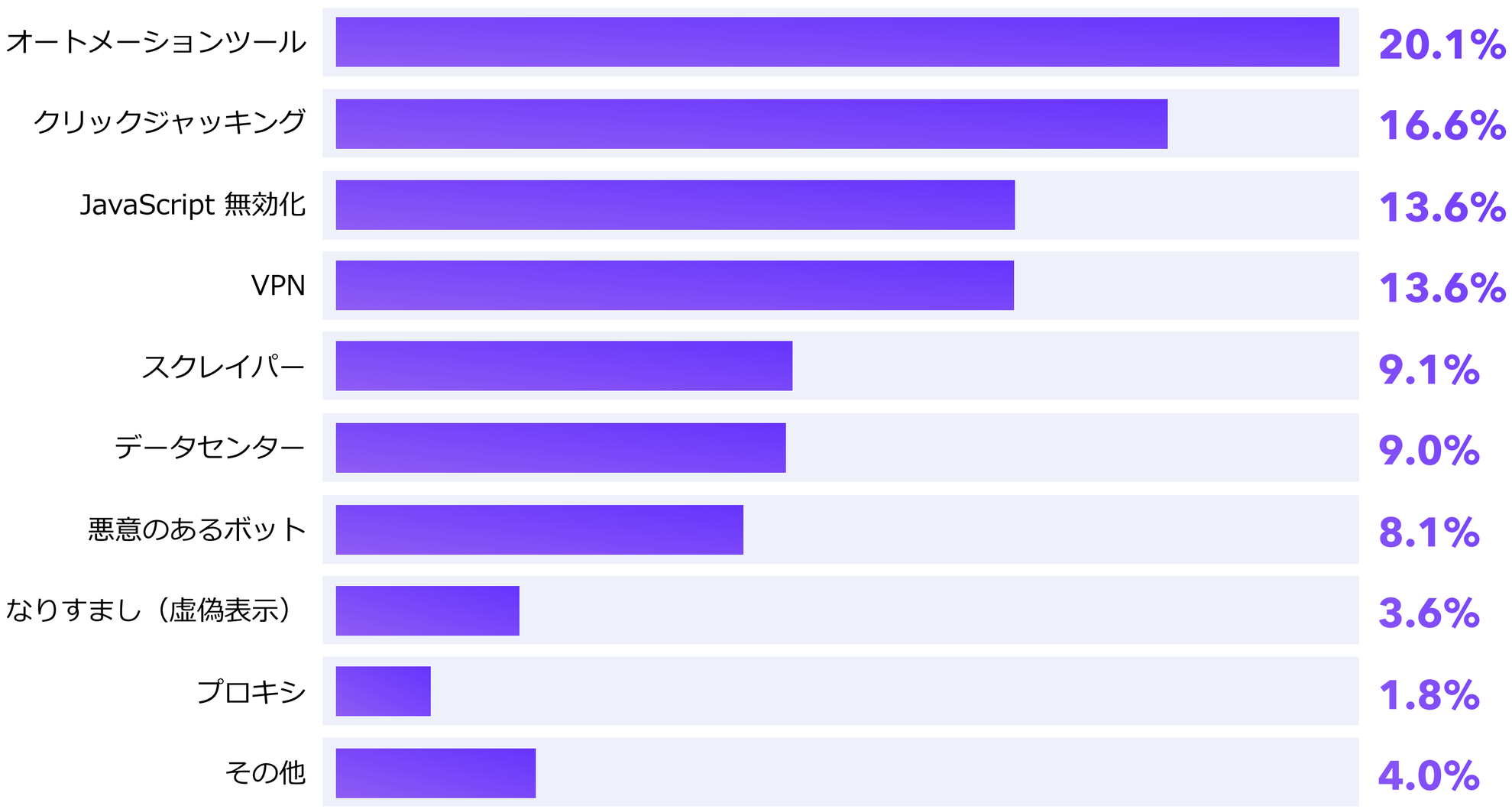
不正トラフィックの種類

脅威のタイプと種類

不正トラフィックがもたらす脅威をより深く理解するために、CHEQ は膨大な不正トラフィックを20種類以上に分類しています。以下のグラフは2022年に最も多く検知された脅威タイプのトップ10とその割合を示しています。
Web インデックス作成や SEO 評価などのルーチンタスクを実行するために使用されるボットであるオートメーションツールは、**20.1%**と最も多く占めています。

これらのツールは犯罪目的ではないことが多いですが、コンバージョンにつながらないただのプログラムであるため、マーケティングデータや分析からは除外する必要があります。2022年のデータを2021年のデータと比較したところクリックジャッキング、悪質なボット、スクレイパーの３種類の脅威が、2022年に飛躍的に増加したことが確認されました。

2022年に最も多く発見された10種類の脅威



Other is comprised of Low Quality Users, Geo Exclusions, Disabled Cookies, and other suspicious behaviors.

脅威のタイプ

拡大する脅威

クリックジャッキング攻撃

クリックジャッキング攻撃は、2022年に急増し**前年比125%増**で、不正トラフィック全体の**16.6%**を占めました。

クリックジャッキングは、リンクや広告など、一見普通に見えるが、実はマルウェアをインストールしたり、サイト訪問者をリダイレクトさせたり意図しない動作をするよう誘導させる手法です。2022年には100万回以上インストールされた Google Chrome の拡張機能にて発見されました。この拡張機能は、検索機能を乗っ取り、Web ページへのアフィリエイトリンクの挿入によりユーザー体験を混乱させ、小売業者に数千ドルもの損害を与えていたことが判明しました。

悪質なボット攻撃

悪質なボットによる攻撃は**前年比112%増**で2022年には不正トラフィック全体の**8.1%**に達しました。これらは、カードスキミング、転売ヤー、アカウント乗っ取り攻撃、アドフラウド、データ侵害などの攻撃のために特別に設計された既知のボットです。

転売ヤーとは、人間とは比べものにならない程高速で、オンラインの在庫商品を手に入れ、他の Web サイトで製品を高額で再出品するボットで年末年始のバーゲン時期に特に急増します。テイラー・スウィフトのツアーチケットをボットが買い占め、チケットマスターのサイトをダウンさせた際には、訴訟となり、米議会で公聴会が開かれることになりました。

スクレイパー

スクレイパーのブロック件数は、**前年比101%増**で、2022年の不正トラフィック全体の**9.1%**となりました。スクレイパーとは、特定の標的やデータを探して Web サイトをスキャンするボットで、競合サイトの価格をモニタリングし自社サイトで商品をわずかに安く販売することで、より多くの顧客を獲得しようとする手法で EC サイトの運営者により、頻繁に利用されます。

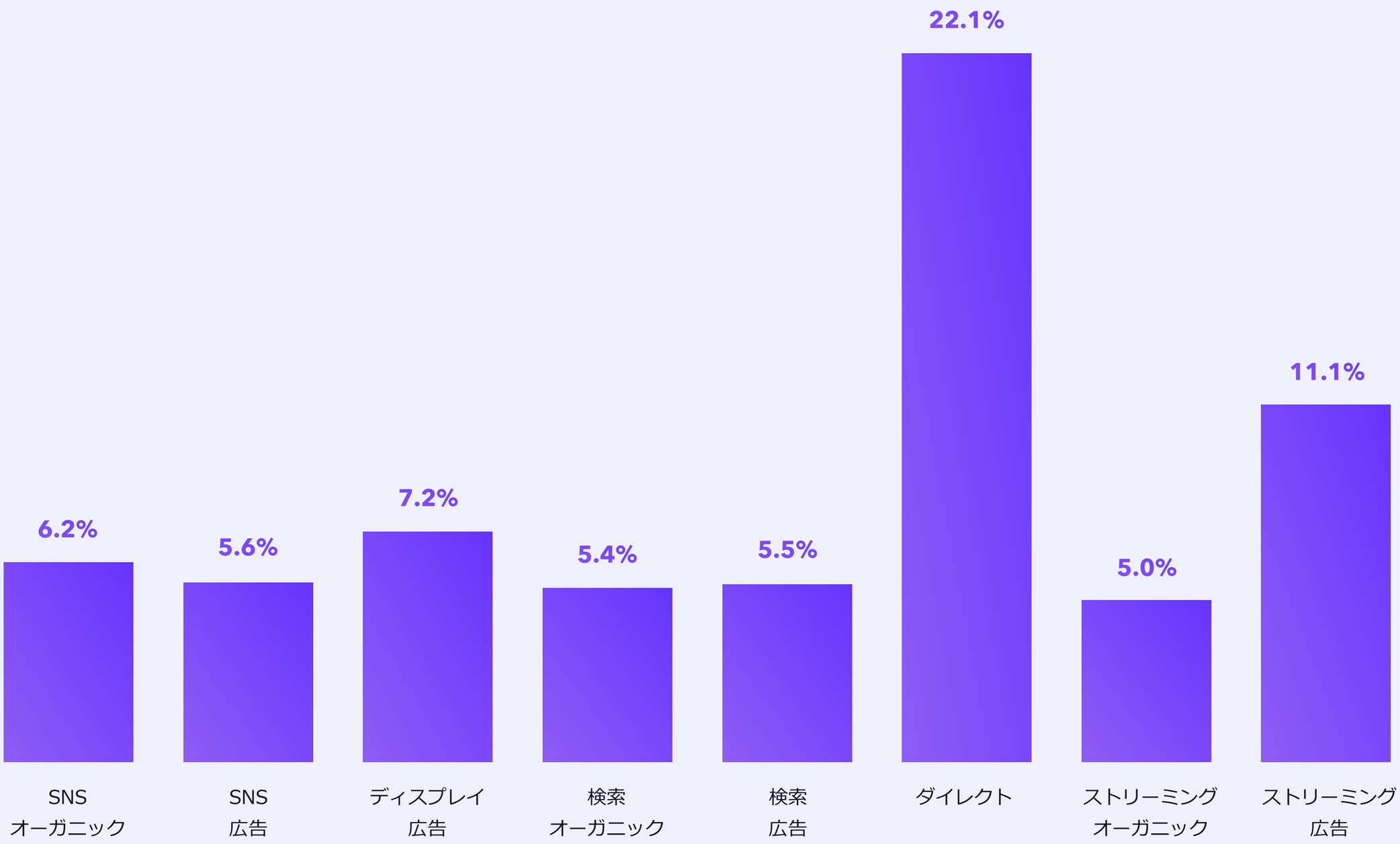
「クリックジャッキング攻撃は
2022年に急増し、前年比125%増で
不正トラフィック全体の16.6%でした。」

不正トラフィックの流入元

不正トラフィックは、デジタルマーケティングの各チャネルに影響を与え続けている脅威です。不正トラフィックに対し、適切な対策を講じずに放置すると、広告予算の浪費、最適化の歪み、キャンペーンの効果が低下、データ分析の混乱、アトリビューションの精度の低下など、業務全体に影響が発生します。検索エンジン、広告ネットワーク、および SNS プラットフォームは、専任のチームと組み込みツールにより、不正行為や改ざんを軽減しようとしていますが、不正トラフィックの各プラットフォームへの流入は続いています。

何十億件もの不正トラフィックの流入元を分析した結果、いくつかの顕著な例外を除いて、ほとんどのプラットフォームで不正トラフィックが同様のレベルであることが判明しました。調査結果について、以下のグラフにまとめました。次ページ以降の詳細データと併せて、ご確認ください。

流入元別の不正トラフィック率（2022年）



SNS の不正トラフィック率は上昇しており

ビジネス特化型 SNS にクラッカー※が集中

SNS の不正トラフィック率は、検索広告やディスプレイ広告よりも低かったもののビジネス特化型の SNS は、調査したプラットフォームの中で、圧倒的に不正トラフィック率が高くなっていました。

ビジネス特化型 SNS から流入するトラフィックの不正トラフィック率は平均**12.4%**となっており、広告経由のトラフィックの**9.7%**、オーガニックトラフィックの**15.3%**が不正であると判明しました。クラッカーにとって、ビジネス SNS のユーザーは価値の高い標的として、格好の攻撃対象になっていることが判ります。

また、アドフラウドを行う者にとって、ビジネスSNSを攻撃する動機はさらに強いです。2022年のSNS 全体のクリック単価は平均5.58米ドルで、ビジネス特化型 SNS のクリック単価は、一般的な SNS やクリック課金型広告の最大 5 倍となっています。クラッカーにとって、ビジネス SNS を攻撃する方が他の SNS に比べて 5 倍も効率的であるということになります。

Twitter：2022年最大のボットニュース

2022年の Twitter 上のボットの挙動は、他の SNS よりもニュースで取り上げられることが多くありました。しかし、広告経由とオーガニックトラフィックを加重平均した不正トラフィック率は**5.3%**で、Twitter の競合他社と比較して、特に高い数値ではありませんでした。

しかし、Twitter では、 5 月にマスク氏が偽アカウントへの懸念から買収を一時停止したこと、10 月に買収が強行されたこと、12月にマスク氏がボットや偽アカウントの取り締まり強化を発表したことなどから、 1 年を通して不正トラフィックが急増しました。

ディスプレイ広告に不正トラフィックを

侵入させるクリックジャッキング攻撃

ディスプレイ広告は、オンライン広告の最も古い形態であり、企業が幅広いオーディエンスにリーチし、ブランドの認知度を高めるために非常に効果的なツールです。しかし、ディスプレイ広告はサードパーティの Web サイトに配信されるため、クラッカーにより容易に不正操作される可能性があります。ディスプレイ広告は特にクリックジャッキング攻撃に脆弱で、2022年にはプラットフォーム全体におけるクリックジャッキングが125%増加しました。このような攻撃の拡大により、ディスプレイ広告の不正トラフィック率は2022年、**7.2%**となり、検索連動型広告の不正トラフィック率より**40%**高くなっています。

クリックジャッキング攻撃では、攻撃者は、隠しレイヤーの追加や Web ページのコードの改ざんなど、さまざまな技術を使って、サイト訪問者が気づかない間にディスプレイ広告をクリックさせ、広告主からクリック報酬を不正獲得しようとします。

クリックジャッキング攻撃は、クライアント側で発生するため、サイト訪問者のブラウザが正規のクリックとジャッキングによるクリックを区別できないことが多く、検知・防止が困難です。

※ クラッカーとは、：コンピューターやネットワークシステムなどに不正に侵入し、悪意をもって他人のデータを盗み見たり破壊したりする「クラック」（crack）あるいは「クラッキング」（cracking）を行う者。

ビューボッティングによる
ストリーミング数値の水増しと広告費の浪費

2022年、ストリーミングプラットフォームはかつてないほどのリーチを獲得しました。18～49歳のユーザー層では、最も人気のあるストリーミングサイトがテレビの総視聴数よりも多く視聴されました。これは、同時に、ストリーミングサイトで広告を多く出せば、より多くの視聴者にエンゲージでき、最終的にコンバージョンにつながる確率も高まることを意味します。

しかし、これらの広告視聴者の多くは実際の人ではなく、ボットであることがわかりました。
2022年、ストリーミングプラットフォームにおける広告経由のトラフィックの不正率は**11.1%**とあらゆる手法の中で最も高い割合となりました。あるストリーミングプラットフォームの広告収入に基づくと、**30億米ドル（約4050億円）以上の広告費が浪費**されている可能性が試算できます。

こうした不正トラフィックの多くはビューボッティングによるものです。ビューボッティングとは、自動化されたソフトウェア（ボット）を使って、ストリーミング動画やライブストリームを視聴させ、閲覧者数を水増しし閲覧数を稼ぐために手段を選ばないクリエイターのために偽のエンゲージメントと偽の広告視聴を行う、比較的新しい不正トラフィックの手法です。

ほとんどのビューボッティングは、ヘッドレスブラウザで動画を開くシンプルなスクリプトですが、高度なビューボッティングは、ログインしたユーザーになりすますための偽アカウントの作成や、チャットボット機能の組み込みによりストリームのチャットやコメント欄に書き込みをして水増しした閲覧者数があたかも実在するアカウントと見せかけることもできます。一部のビューボッティングは、広告をクリックしてクリック率を高めます。このようなボットは、月額10米ドル（約1350円）という低価格でレンタルできます。

偽ユーザーの影響は、不正クリックに限りません。最近では、多くの著名なクリエイターがメンションやインプレッションの数に対して報酬をもらっていますが、もしこれらの報酬が実際のユーザではなく、ボットによって作られた数値を元に支払われていたとしたら、広告主が投資した広告費の多くが無駄になっているということになります。

10万回のインプレッションに2000米ドル（約27万円）かかるとします。そのうちの15～20%が偽のインプレッションだとしたら、150～200米ドル（２万円～2.7万円）が無駄になってしまいます。ストリーミング広告のキャンペーンの多くが数百万インプレッションを計測していると考えると、偽のインプレッションにかかる費用は、あっという間に膨れ上がってしまいます。その上、不正トラフィックによって KPI が歪められると、意思決定がますます困難になります。

業界・業種別の不正トラフィック

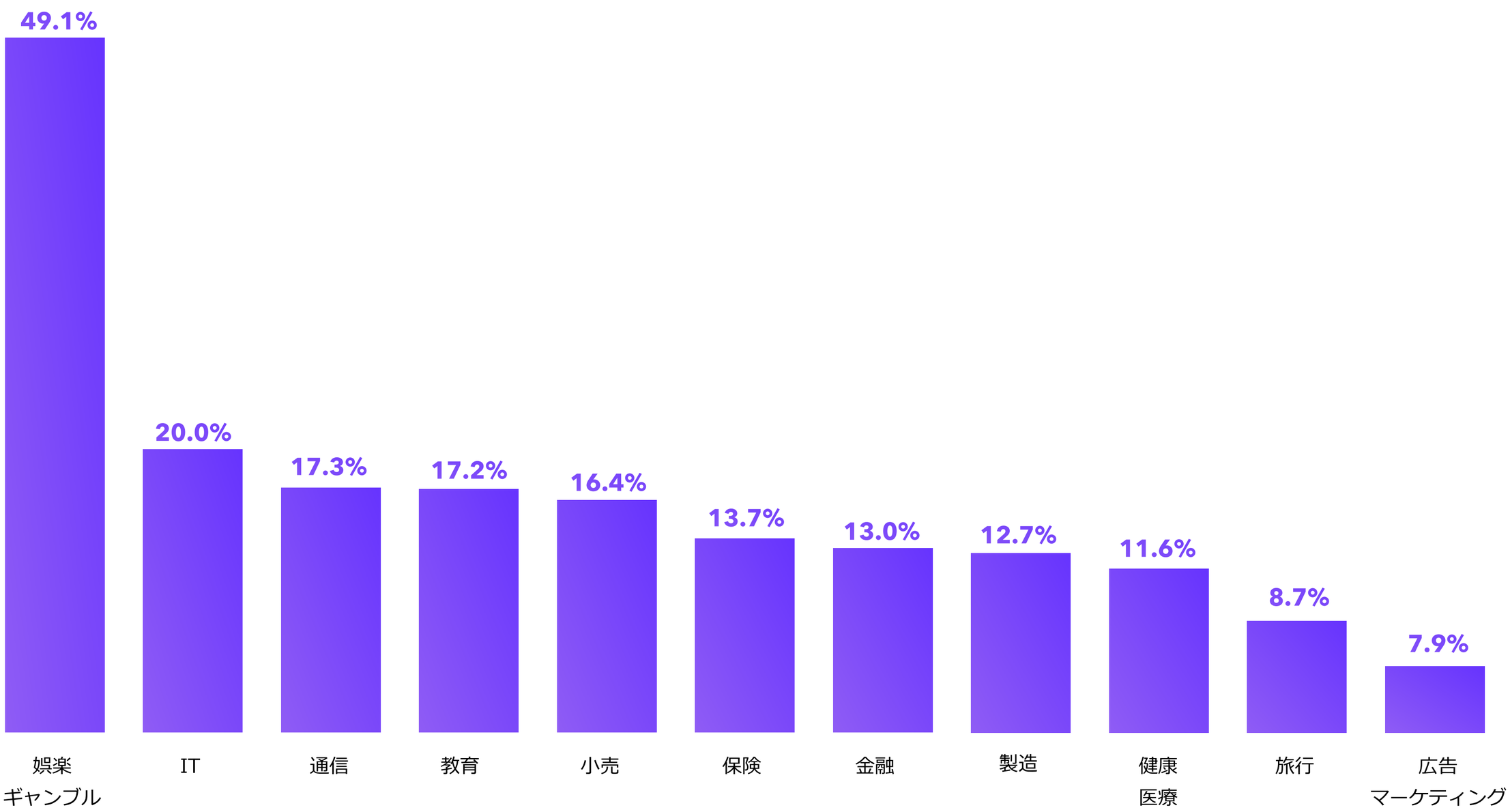
不正トラフィックは、事業の規模および業界・業種を問わず、ビジネスに影響を与え、拡大し続けています。トラフィックや広告を収益源としている業種では、アドフラウドのリスクが高くなりますが、セキュリティレベルが低い Web サイトは常にサイバー犯罪者やクラッカーに狙われています。

全ユーザー企業のデータを分析した結果、不正トラフィック率は業界・業種により大きく異なることが判明しました。

娯楽・ギャンブル業界では、2022年、クリック詐欺の割合が最も高く、トラフィック全体の**49.1%**が不正でした。

IT、教育、通信業界も、2022年に平均を上回る割合の不正トラフィック率が確認されています。次ページ以降では、脅威の種類が各業界・業種に与える影響についても検証します。

業界・業種別の不正トラフィック（2022年）



業界・業種別の不正トラフィック

広告・マーケティング

広告・マーケティング関連の Web サイトにおける不正トラフィックは、全体の7.9%に達していました。CHEQ が発見・ブロックした不正トラフィックの大半は、データセンターとオートメーションツールによるものでした。広告業界は、アドフラウドやアフィリエイト詐欺を実行しようとする際に使用されるクリックファームやボットネットの格好の標的となっています。

しかし、これらの攻撃は主に、サードパーティのプラットフォームでホストされている広告やコンテンツに集中しているため、当結果には含まれていません。つまり、想定される被害範囲はさらに広範囲と言えます。広告およびマーケティング代理店にとって、不正トラフィックは、広告収入に対する潜在的な脅威だけではなく、クライアントのキャンペーンを管理する企業の評判に対する脅威の両方を含む、二重の脅威をもたらします。

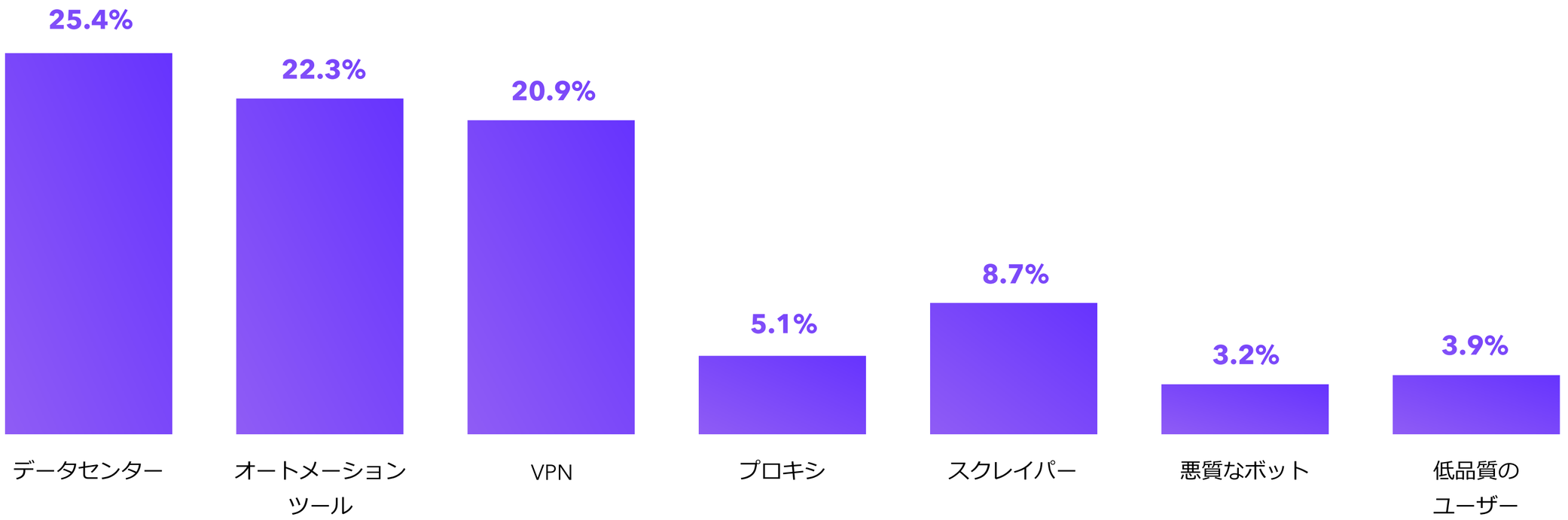
7.9%
全体

4.9%
ペイド

7.5%
ダイレクト

5.7%
オーガニック

脅威の種類および不正トラフィック全体における割合
広告・マーケティング（2022年）



業界・業種別の不正トラフィック

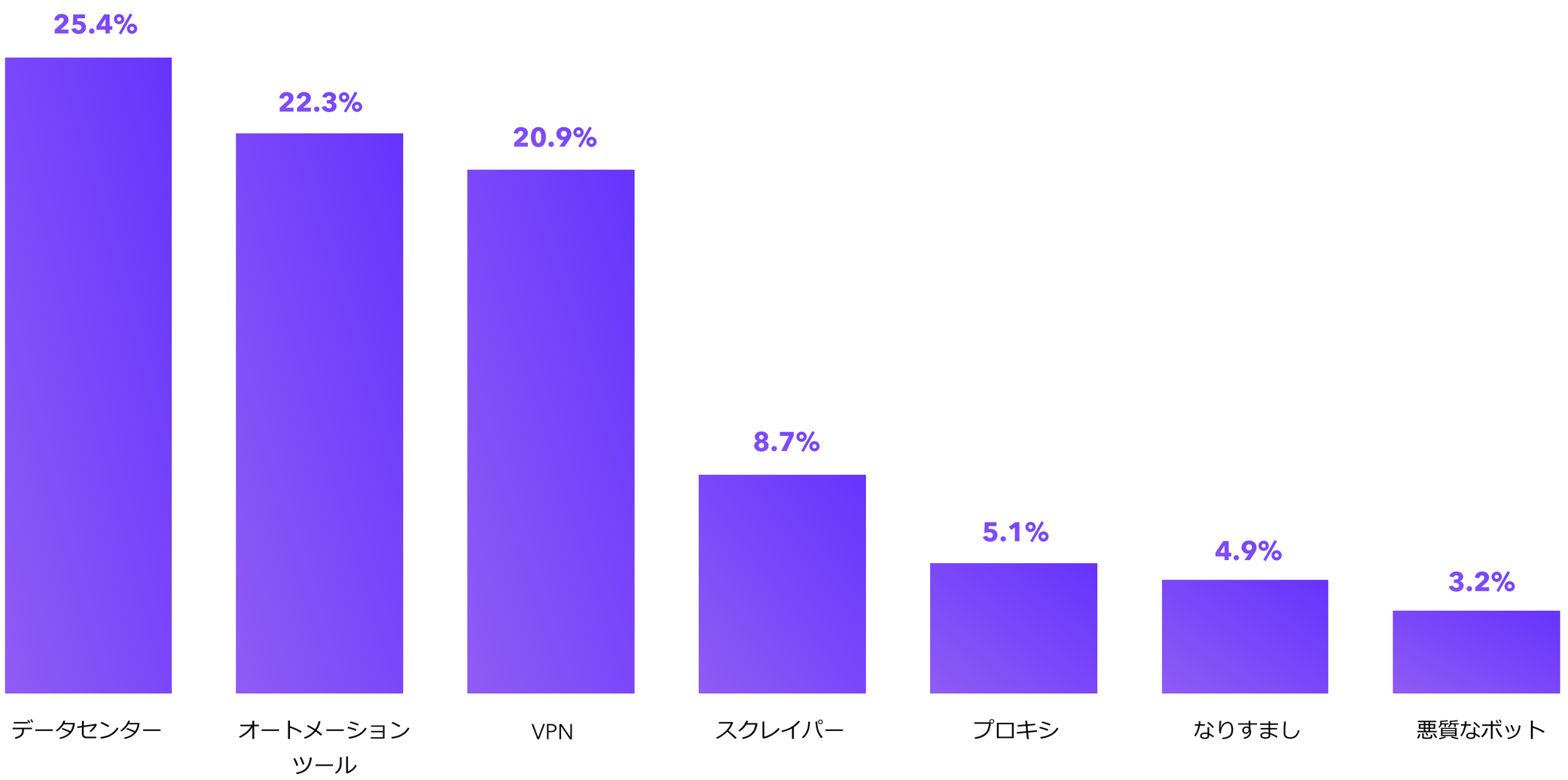
IT・SaaS

Statista 社の調査によると、SaaS（Software-as-a-Service）市場は2023年までに2000億米ドル（約27兆円）以上の規模になると予想されています。SaaS の価値は主に複雑なビジネスプロセスを簡素化し、オンラインですぐに利用できるようにする B2B ツールによって構築されており、リモートワークやコラボレーション、業務効率の向上を可能にします。

しかし、このようなビジネスモデルは SaaS ツールと運営企業をクラッカーの格好の標的にしてしまいました。ひとつの SaaS ツールに侵入することができれば、何千社ものツール利用企業の機密データにアクセスできることになります。SaaS 企業の2022年の不正トラフィック率は、ギャンブルに次ぐ**20%**でした。

20%	5.9%	23.4%	8.8%
全体	**ペイド**	**ダイレクト**	**オーガニック**

脅威の種類および不正トラフィック全体における割合
IT・SaaS（2022年）



業界・業種別の不正トラフィック

教育機関・高等教育機関

2021年、ボットや偽ユーザーが奨学金や学生特典を不正受給・利用するために、大学への出願を行い、このような犯罪行為のほとんどは成功していたことが発覚し話題になりました。高等教育機関における、ボットの問題は2022年も継続して起きているようです。

2022年に CHEQ が保護している Web サイトへのトラフィックのうち、17.2%が不正と検知され、ダイレクトトラフィックの不正率は32.9%と異常に高くなっていました。悪質なボット攻撃のブロック量は平均値を上回り、ボットやクラッカーによる激しい攻撃が続いていることが明らかです。

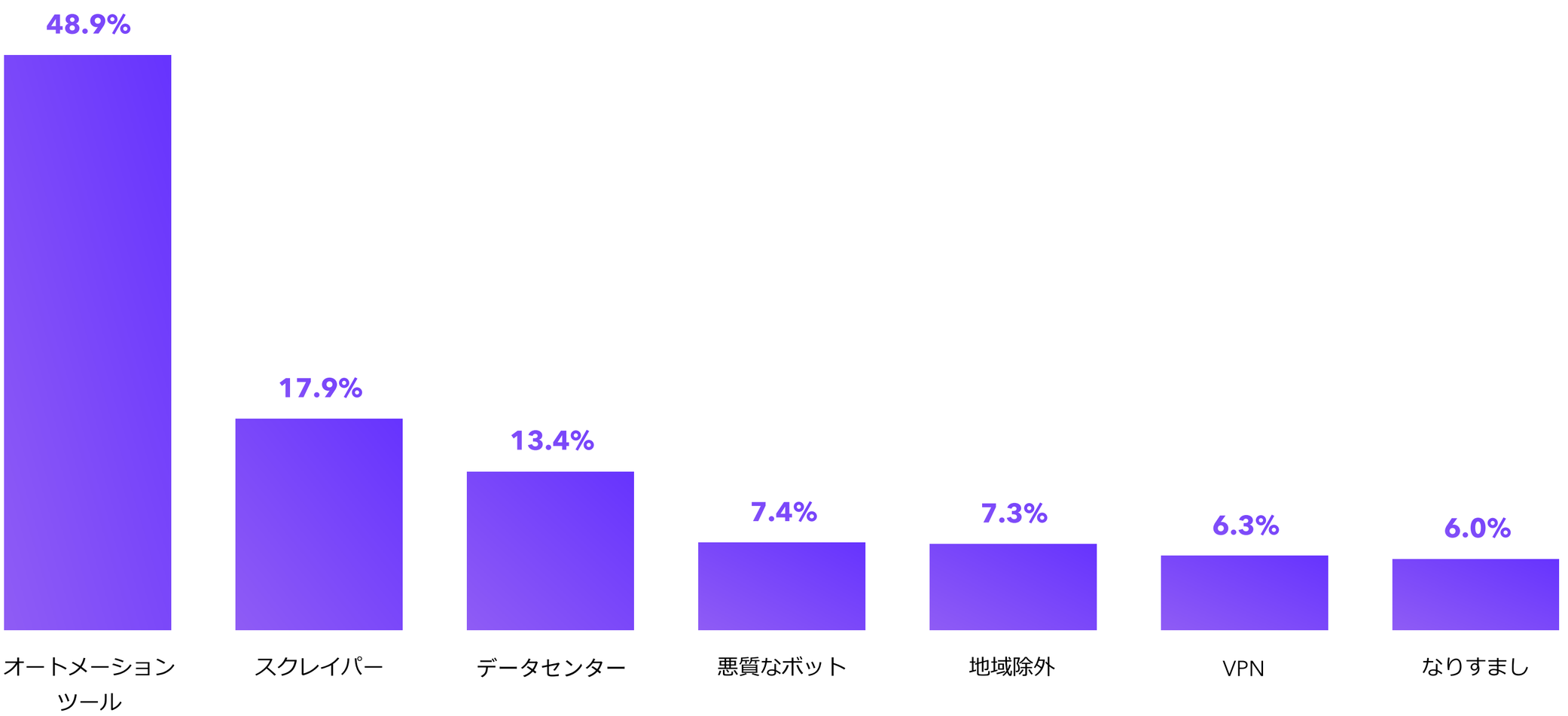
17.2%
全体

4.5%
ペイド

32.9%
ダイレクト

8.2%
オーガニック

脅威の種類および不正トラフィック全体における割合
教育機関・高等教育機関（2022年）



業界・業種別の不正トラフィック

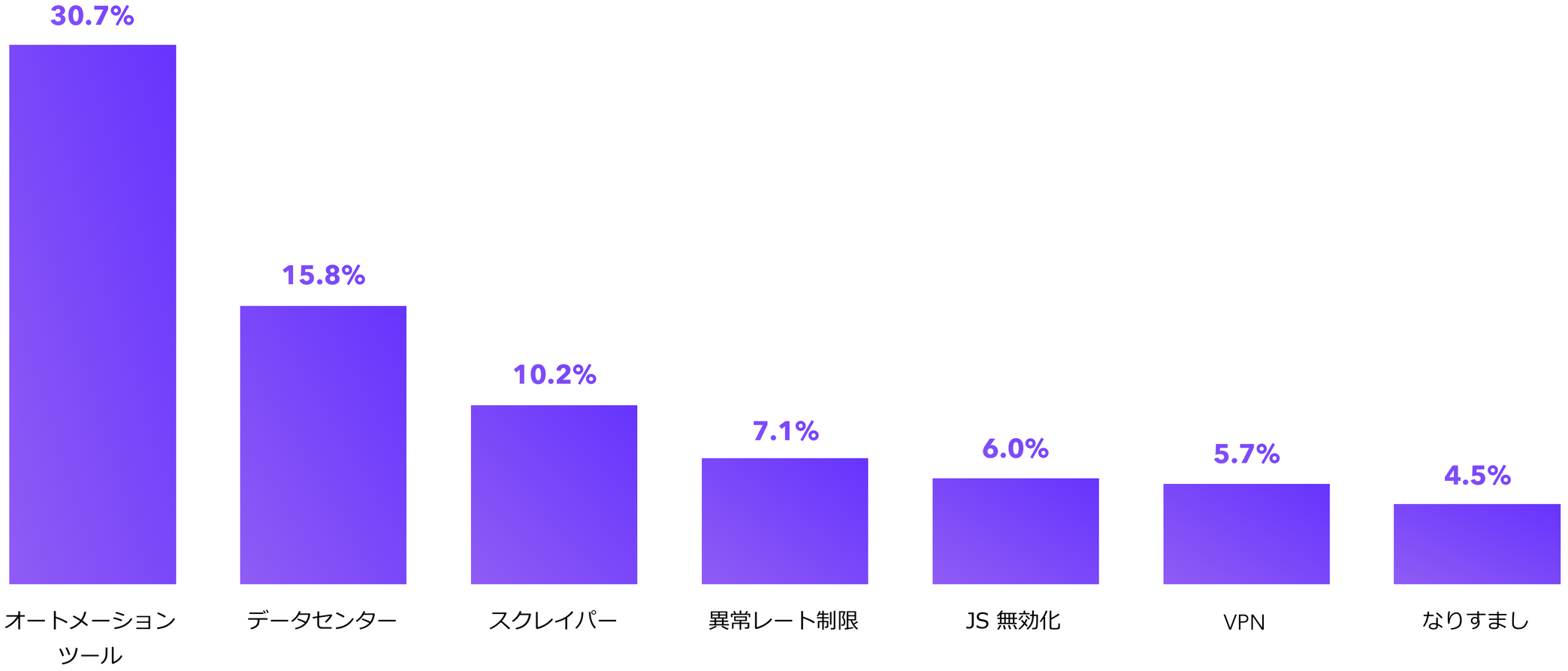
金融

2017年の Equifax データ流出事件や国内外の規制当局からの監視強化を受けて、多くの金融・フィンテック企業はサイバー攻撃へのセキュリティ対策を強化しましたがクラッカーによる攻撃は止まりません。

2022年、金融業界の不正トラフィック率は平均13%でした。CHEQ のユーザーデータでは金融業界での不正トラフィックのトップ 3 はオートメーションツール、データセンターに次いで、スクレイパーが多く検出されました。スクレイパーは金融業界の不正トラフィック全体の10.2%となっています

13%	3.1%	19.7%	4.9%
全体	**ペイド**	**ダイレクト**	**オーガニック**

脅威の種類および不正トラフィック全体における割合
金融（2022年）



業界・業種別の不正トラフィック

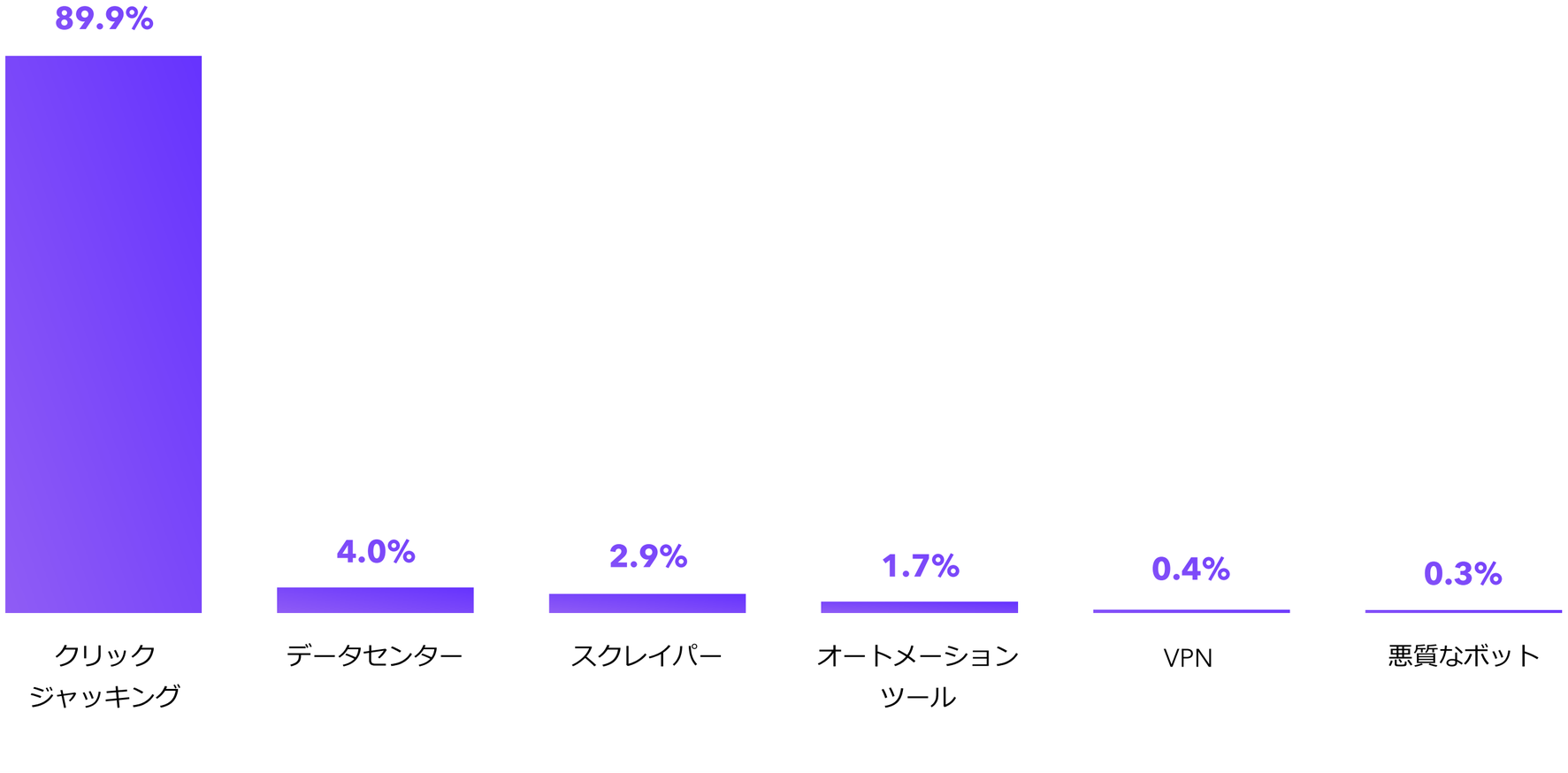
娯楽・ギャンブル

今回調査した業界の中で、不正トラフィック率が最も高かったのは**娯楽・ギャンブル業界**で不正トラフィック率は49.1%です。またオーガニックが6.1%、広告経由が5.7%であるのに対し、ダイレクトトラフィックの不正トラフィック率が55.1%と大きな比重を占めているという特徴があります。

不正トラフィックの89.9%は、クリックジャッキング攻撃によるものでした。

49.1%	5.7%	55.1%	6.1%
全体	**ペイド**	**ダイレクト**	**オーガニック**

脅威の種類および不正トラフィック全体における割合
娯楽・ギャンブル（2022年）



業界・業種別の不正トラフィック

健康・医療

米国保健福祉省の市民権局は、2022年1月1日から10月31日の間に594件のデータ侵害が発生し毎月平均60件のデータ侵害が確認されたと報告しています。クラッカーはセキュリティの脆弱な接続機器を通じてネットワークに侵入しますが、多くの場合、流入経路は標的の Web サイトです。

2022年、健康・医療業界の Web サイトの不正トラフィック率は11.6%で、悪質なトラフィックの大半は、脆弱性や侵害しやすいデータを見つけるために45.2%のスクレイパーが Web サイトを巡回しました。

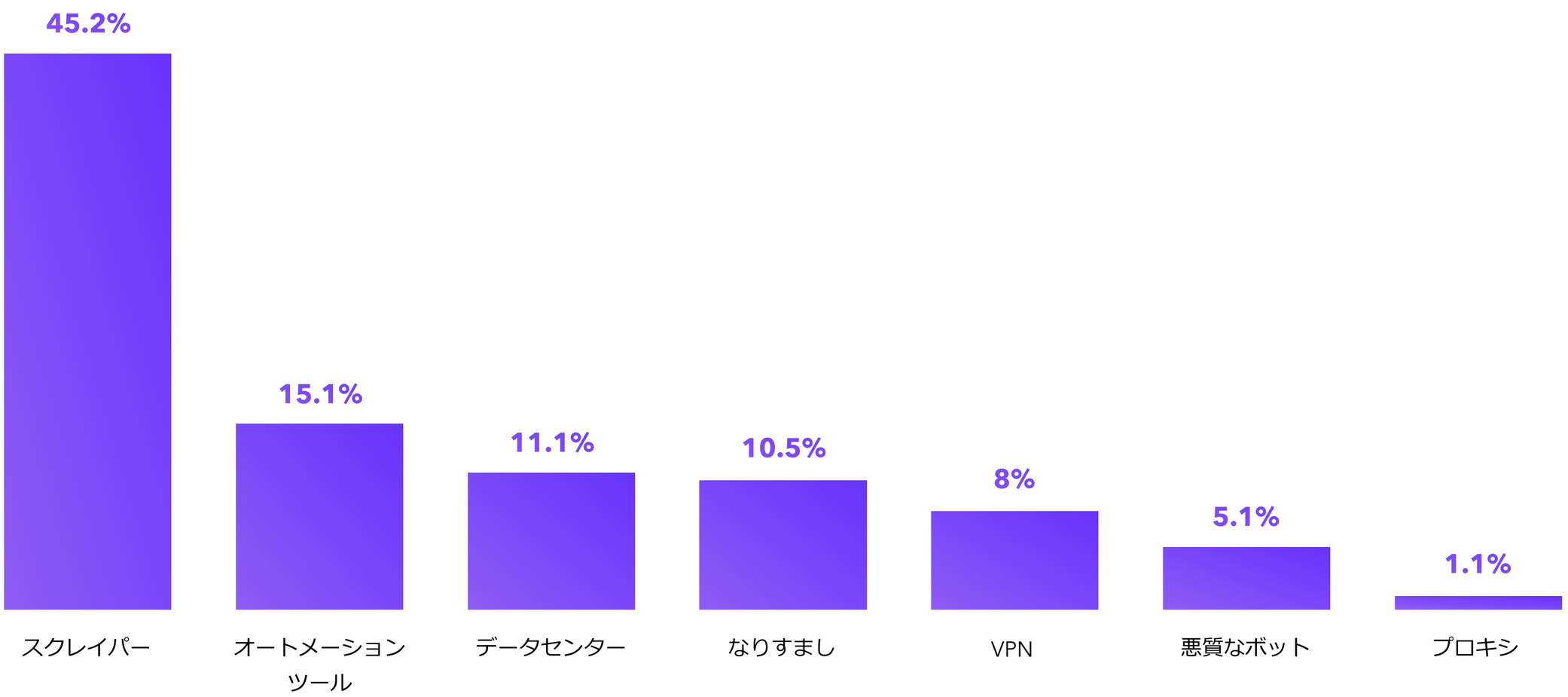
11.6%
全体

2.5%
ペイド

21%
ダイレクト

13.8%
オーガニック

脅威の種類および不正トラフィック全体における割合
健康・医療（2022年）



業界・業種別の不正トラフィック

保険

健康・医療業界と同様に、保険会社もデータ侵害があった場合、クラッカーに多くの貴重な個人情報が盗まれてしまいます。そのため、保険業も脆弱で侵害しやすいデータを探すスクレイパーの格好の標的となっています。

2022年には、保険サイトの不正トラフィック率は13.7%であり、その内の３分の２以上（67.8%）がスクレイパーでした。

13.7%	2.4%	32.2%	2.5%
全体	ペイド	ダイレクト	オーガニック

脅威の種類および不正トラフィック全体における割合
保険（2022年）

業界・業種別の不正トラフィック

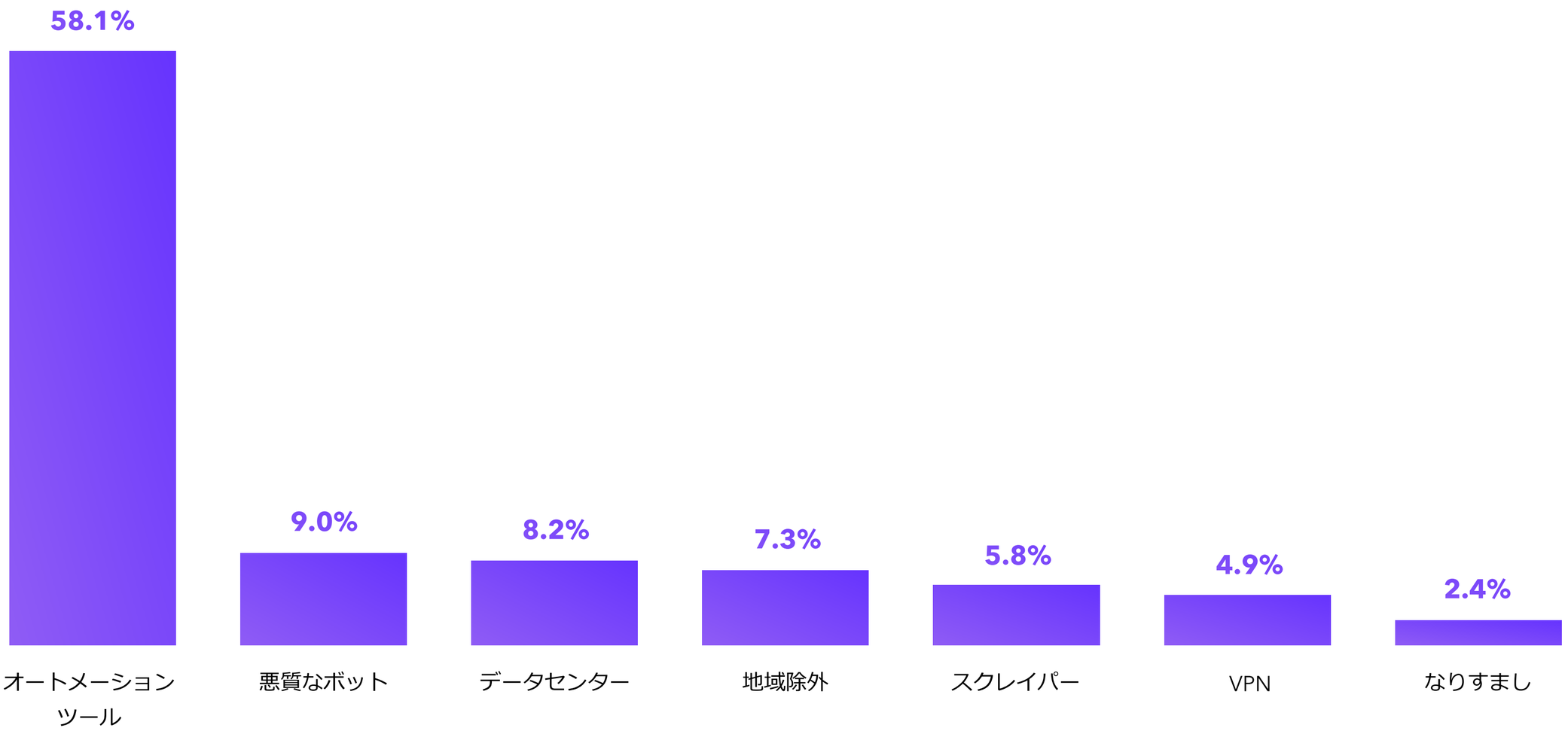
小売

価格に特化したスクレイパー、カゴ落ち、転売ヤー、カードスキミング攻撃など、小売業や EC サイトを標的にした攻撃は多種多様で、2022年に小売業の Web サイトのトラフィック全体の16.4%が不正だったことも説明がつきます。

不正トラフィックのうち、既知の悪質なボットは9%、つまりトラフィック全体の約1.5%を占めています。

16.4%	3.0%	34.5%	4.4%
全体	ペイド	ダイレクト	オーガニック

脅威の種類および不正トラフィック全体における割合
小売（2022年）



業界・業種別の不正トラフィック

通信

通信事業者は、分散型サービス拒否（DDoS）攻撃の標的となることが多くあります。DDoS攻撃では、ネットワークのインフラに負荷をかけてダウンさせるために、標的の Web サイトに大量の不正トラフィックが送り込まれます。このような攻撃は、ほとんどの場合、ボットネットによって実行されます。

ボットネットとは、ボットに感染し制御されたユーザーの端末や単純な IoT 機器を悪用した大規模ネットワーク、つまり複数のボットをネットワーク化したものを指します。2022年通信事業者とインターネットサービスプロバイダーの Web サイトにおける不正トラフィックの割合は17.3%に達しました。

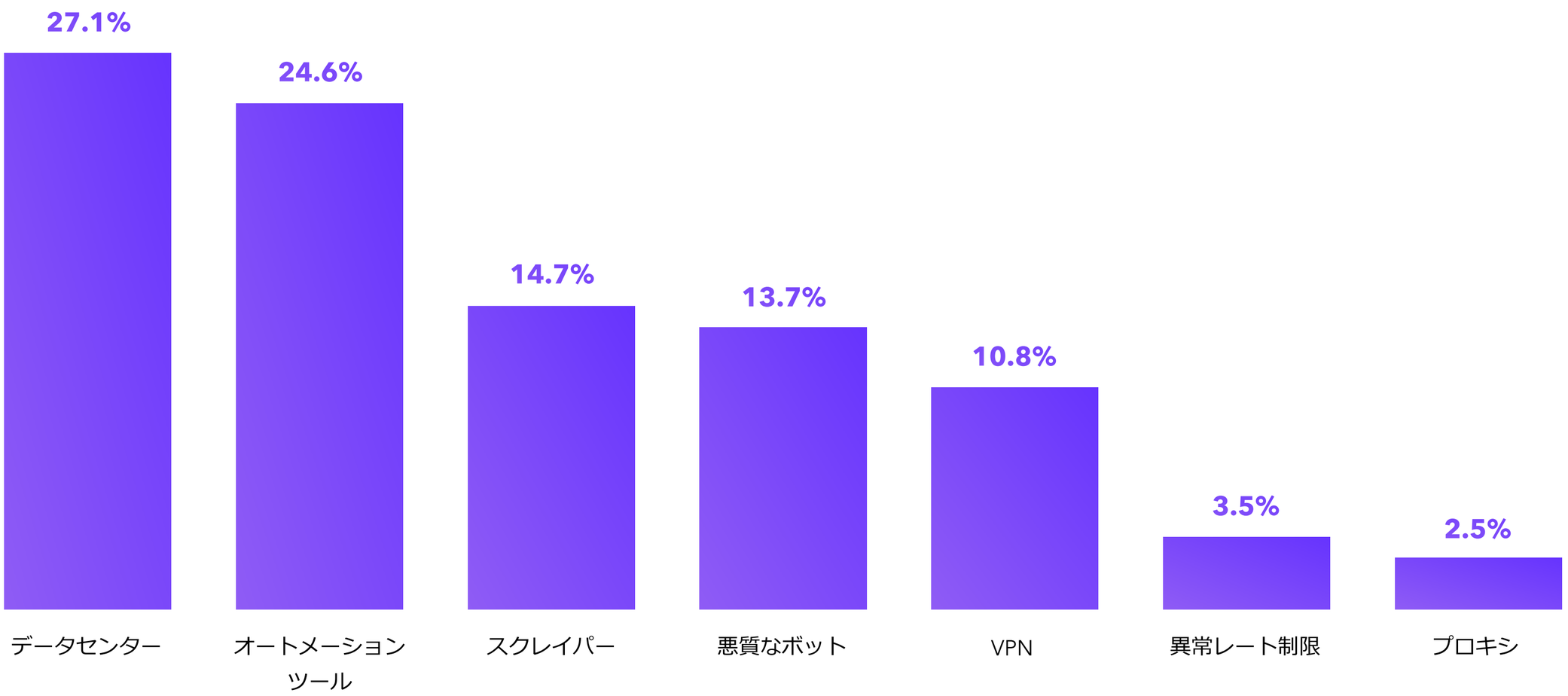
17.3%
全体

7.1%
ペイド

24.3%
ダイレクト

9.6%
オーガニック

脅威の種類および不正トラフィック全体における割合
通信（2022年）



業界・業種別の不正トラフィック

旅行・観光

旅行・観光業界は、2022年の不正トラフィック率が平均より低い8.7%でした。しかし、旅行・観光業界の Web サイトを標的にした特殊なスクレイパーが不正トラフィック全体の30%に達し、脅威が拡大しています。

スクレイパーの大部分は、競合他社や価格比較サイトによる価格スクレイパーであると思われますが、スクレイパーはメールアドレスやクレジットカード番号などの個人情報の不正取得や、スパム、なりすまし、詐欺などの犯罪に悪用されることもあります。

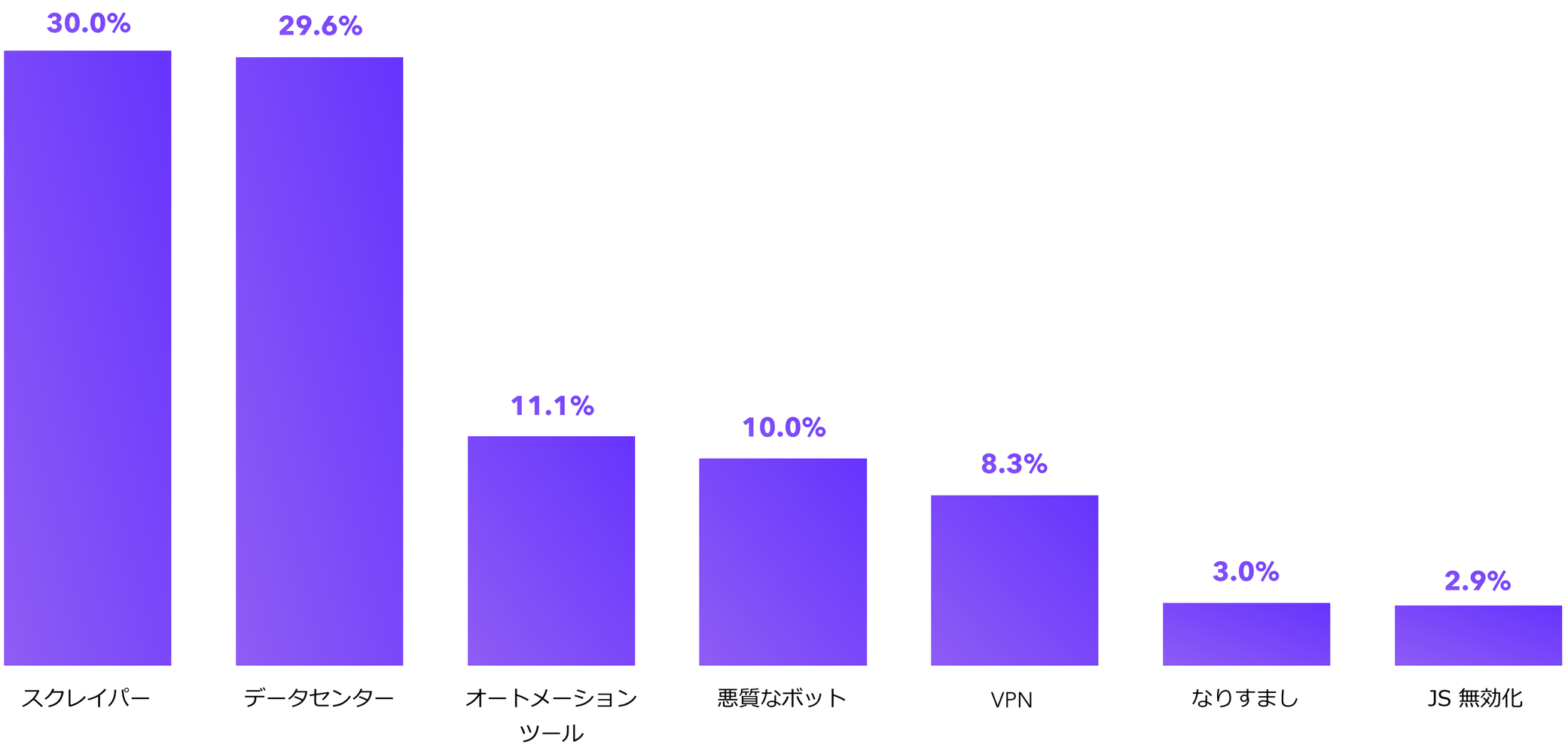
8.7%
全体

3.3%
ペイド

14.4%
ダイレクト

3.0%
オーガニック

脅威の種類および不正トラフィック全体における割合
旅行・観光（2022年）



業界・業種別の不正トラフィック

製造

製造業は、今回の調査で注目した他の業界・業種と比較すると「消費者向け」ではないため、通常、Web サイトはトラフィック量が少なく後回しにされてしまいがちです。しかし、不正トラフィックはインターネットの至る所にリスクを生じさせる可能性があり、製造業も例外ではありません。

2022年には、製造業の Web サイトに流入したトラフィックの12.7%が不正でした。この不正トラフィックの大部分はオートメーションツール、スクレイパー、JavaScript を無効化したブラウザ（ヘッドレスブラウザが多い）により構成されていました。これは、製造業のサイトにおいてデータを見つけ、流出させようとする試みが平均よりも高いことを示唆しています。

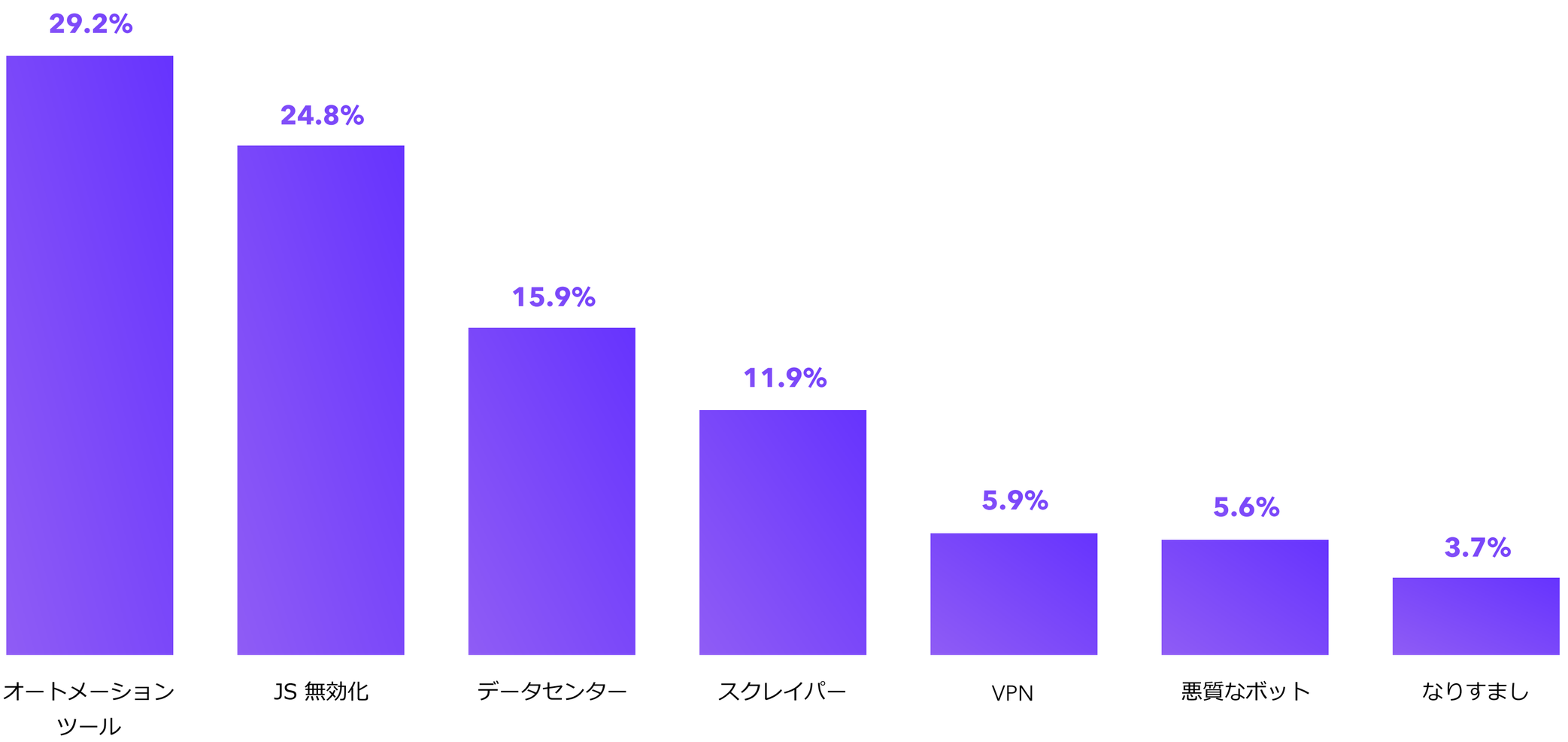
12.7%
全体

3.0%
ペイド

32.4%
ダイレクト

4.4%
オーガニック

脅威の種類および不正トラフィック全体における割合
製造（2022年）



地域別の不正トラフィック

北米、EMEA、APAC、LATAMの４地域から流入する不正トラフィックの量を調査しました。これらの地域ごとの不正トラフィック量を分析することで、各市場における不正行為の拡大状況を把握し、不正トラフィック率を高くする要因を特定することができます。これらの統計は、各地域から流入した不正トラフィックを対象としており
それらのトラフィックの流入先ではないことにご注意ください。

地域別の不正トラフィック率（2022年）

17.0%
北米

18.9%
EMEA
（ヨーロッパ・中東・アフリカ）

18.1%
APAC
（アジア太平洋）

8.7%
LATAM
（ラテンアメリカ）

地域別の不正トラフィック

北米

2022年には、北米発の全トラフィックの**17.0%**を不正トラフィックが占め、その大部分はオートメーションツールやスクレイパーなどのボットです。

北米の中でも特に世界中の IT 企業が集まっている米国の不正トラフィック率は**25.3%**です。
北米は大手 IT 企業の存在感が強く
オートメーションツールやスクレイパーを利用してデジタルマーケティングを行うデジタル広告会社やマーケターが多数存在する地域でもあります。

17.0%
不正トラフィック率

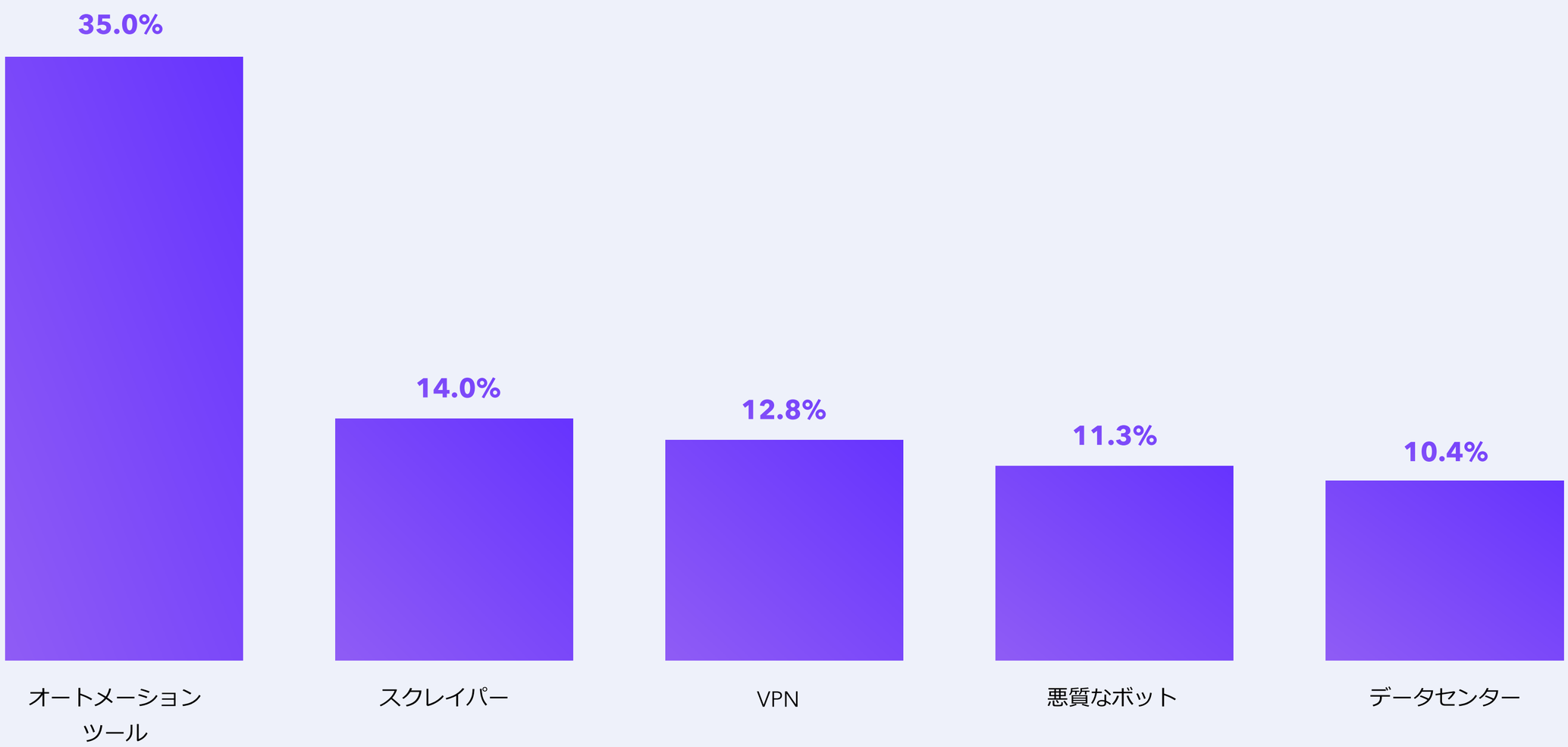
不正トラフィックの内訳
北米（2022年）

38.2%
疑わしい無効アクティビティ

8.0%
悪意がある無効アクティビティ

62.0%
ボットによる無効アクティビティ

脅威の種類および不正トラフィック全体における割合
北米（2022年）



地域別の不正トラフィック

EMEA（ヨーロッパ・中東・アフリカ）

2022年、EMEA 地域を流入元とするトラフィック全体の18.9%が不正であり、どの地域よりも高い不正トラフィック率となっています。この不正トラフィックのうち、身元を隠すため、または単に地域の閲覧制限を回避するために使用される可能性のある VPN などの不審なアクティビティが大部分を占めていました。またクリックジャッキングや悪質なボット攻撃も世界平均を大きく上回っています。EMEA には、世界でも不正トラフィックへの生成量が多い２カ国が含まれています。ナイジェリアとギリシャは、それぞれ**77.3%**と**48.5%**と高い数字となっています。

18.9%
不正トラフィック率

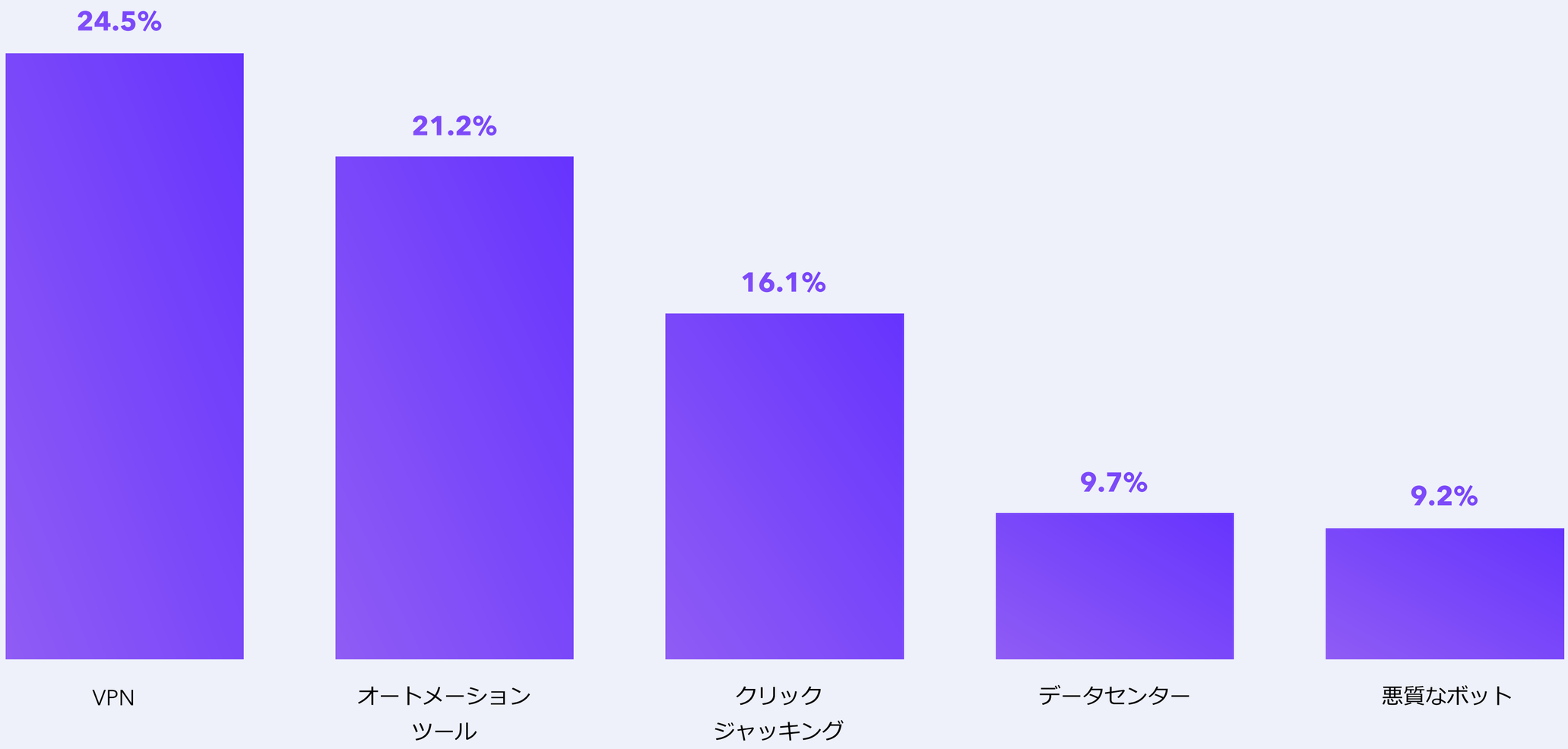
不正トラフィックの内訳
EMEA（2022年）

56.6%
疑わしい無効アクティビティ

6.3%
悪意がある無効アクティビティ

36.9%
ボットによる無効アクティビティ

脅威の種類および不正トラフィック全体における割合
EMEA（2022年）



地域別の不正トラフィック

APAC（アジア太平洋）

APAC 地域から流入した不正トラフィックは、2022年、全トラフィックの**18.1%**を占めました。注意すべき点は、不正トラフィック中の悪質な挙動の比率が**37.0%**と他のどの地域よりも大きかったということです。脅威の種類としては、JavaScript 無効化が35.4%、クリックジャッキングが31.4%で、不正トラフィック全体において高い割合となっています。APAC、特に中国、フィリピン、インドネシアは、クリックファーム事業の世界的な拠点として知られており、高額入札者に雇われた事業者が、虚偽のクリックやトラフィックにより、広告やエンゲージメントへの報酬を犯罪者が不正獲得する手助けをしています

18.1%
不正トラフィック率

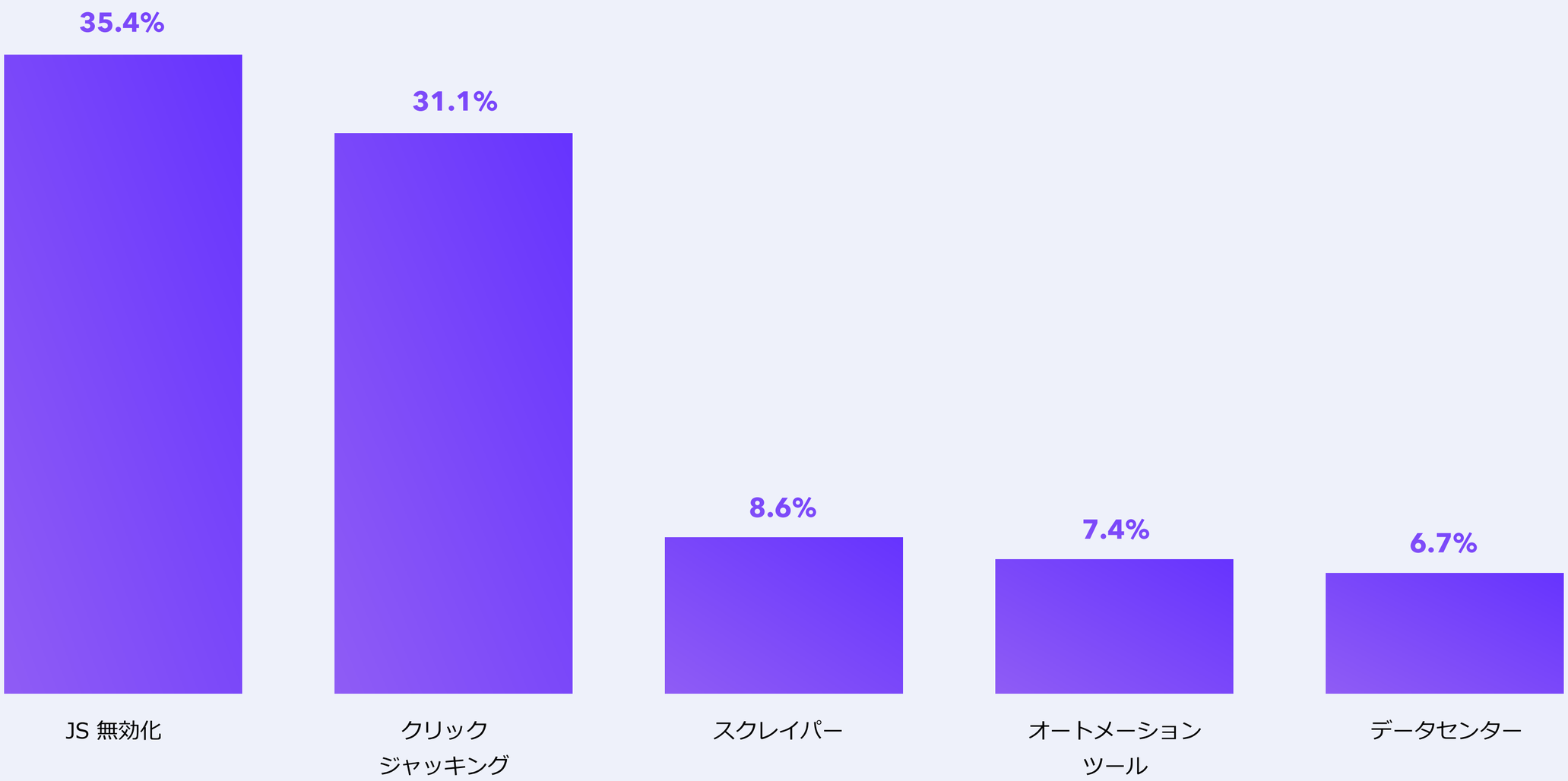
不正トラフィックの内訳
APAC（2022年）

42.1%
疑わしい無効アクティビティ

37.0%
悪意がある無効アクティビティ

20.8%
ボットによる無効アクティビティ

脅威の種類および不正トラフィック全体における割合
APAC（2022年）



地域別の不正トラフィック

LATAM（ラテンアメリカ）

LATAM 地域の不正トラフィック率は2022年、8.7%と他の地域に比べて圧倒的に低いものでした。LATAM 地域から流入した不正トラフィックの大半は、VPN とプロキシであり、合計49%となりました。これは、同地域における不正行為の兆候かもしれませんが、検閲や地域制限を回避しようとするユーザーである可能性もあります。一方、悪質なボットは13.0%で、LATAM 地域の不正トラフィックに占める割合が他のどの地域よりも大きくなっています。

8.7%
不正トラフィック率

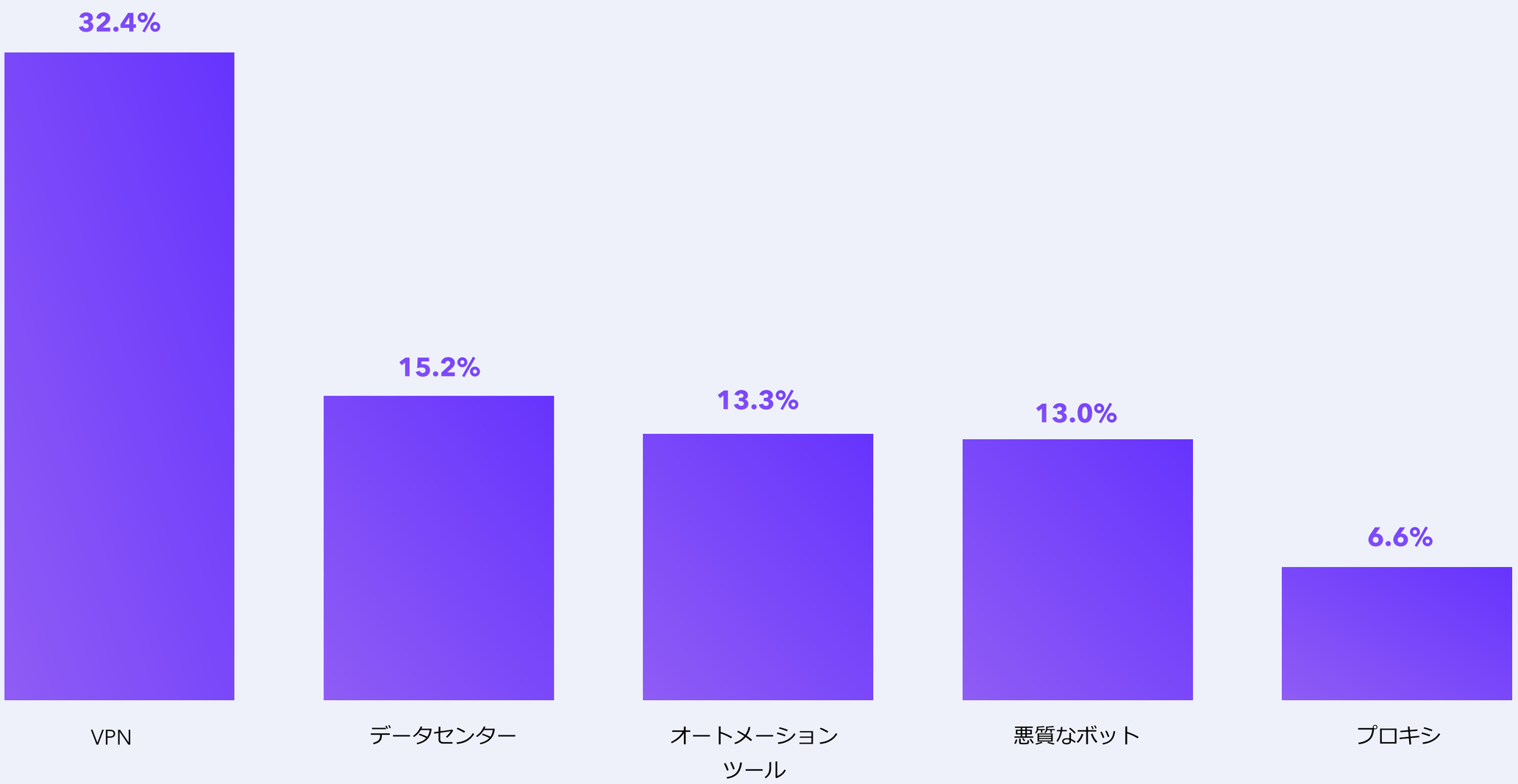
不正トラフィックの内訳
LATAM（2022年）

58.0%
疑わしい無効アクティビティ

9.0%
悪意がある無効アクティビティ

32.8%
ボットによる無効アクティビティ

脅威の種類および不正トラフィック全体における割合
LATAM（2022年）



不正トラフィックによるビジネスへの影響

ビジネスにおいては、予算の全額を有効に活用する必要があります。ボット、オートメーションツール、偽アカウント、クリックファームなどの不正トラフィックは、こうしたビジネス目標を達成する上で大きな障壁となります。

Statista.com によると、2022年、デジタル広告費は全世界で6000億米ドル（約81兆円）を超えました。CHEQ が算出したペイドトラフィックの不正率と合わせると、2022年には少なくとも約357億米ドル（約５兆625万円）の広告費が不正トラフィックにより奪われてしまったと推定することができます。

不正トラフィックは、広告予算だけでなく、潜在的な収益機会にも影響を与えています。

ROAS（Return on ad spend）とは、広告費が生み出す投資利益率（ROI）を算出することで、広告キャンペーンの効果を測定する指標です。計算式は単純で、広告費１ドル（X）に対して、企業は1.5倍、2倍、4倍のリターンを期待することができます。

Adacado 社によると、EC サイトの平均 ROAS は 4:1 です。つまり、2022年に不正トラフィックにより企業が失った潜在的な収益は1428億米ドル（約19兆2780億円）であることになります。

上記の収益機会の損失は、リマーケティングや類似オーディエンスの汚染やアルゴリズムの歪みなど、ペイドマーケティング施策が受ける追加の損害を考慮していないため、実際より被害が大きい可能性があります。

ビジネスへの影響

業務効率の低下、分析データの歪み、ブランドへの信頼の失墜

重要業績評価指標（KPI）が主導する

マーケティングが盛んになる中、業務効率が最重要視されています。

マーケターは、顧客獲得単価を改善し、広告費用対効果（ROAS）を高め、契約金額を高め、取引サイクルを短縮するため、常に試行錯誤をして、データ分析をする必要があります。 1960年代のニューヨークの広告業界を描いた、テレビドラマシリーズ「マッドメン」に登場する広告クリエイティブディレクター、ドン・ドレイパーよりも多くのデータサイエンティスト、A/Bテスト、広告メッセージの見直し、ターゲティング設定、オーディエンスのセグメンテーションは、現代のマーケターに必須です。しかし、データが不正確な場合、これらのツールはどれも問題なく動いているように見えて、歪んだデータにより、最終的なアウトプットは全く意味をなしません。このようにマーケティングファネルにボットや偽ユーザーが流入すると、デジタルマーケティングの土台が崩れてしまいます。「garbage in, garbage out（ゴミを入れたらゴミが出てくる）」という古い格言が当てはまってしまうのです。

マーケターの分析において月間200万件のユニーク訪問が示されていても、その25%が不正トラフィックであることに気付いていない場合将来予測、予算計画、A/B テスト、最適化、および測定のすべてが不正確になってしまいます。

信頼の低下

マーケティング施策は、組織内での高い信頼と透明性をいかに獲得するかで成功が決まります。マーケティングチームが質の高いリードを提供していると営業チームが信頼し、経営陣がマーケティング予測の精度を信頼し、マーケター自身が目の前の数字の精度を信頼できるときマーケティング施策は成功に近づきます。

しかし、ファネル内に不正トラフィックが流入すると、上記のすべてが損なわれます。インバウンドリードが偽ユーザーからのものである場合、営業とマーケティングチームの関係は悪化します。

ZoomInfo 社による最近の調査によると、営業およびマーケティングチームは、不正確なデータを使用することで約550時間、営業担当者１人あたり３万2000米ドル（約432万円）もの損失を出していることがわかりました。こうした損失の大半は、顧客管理システム（CRM）に侵入した偽リードによるものです。

ビジネスへの影響

Twitter や PayPal の事例に学ぶ 不正トラフィックによるブランド価値の低下

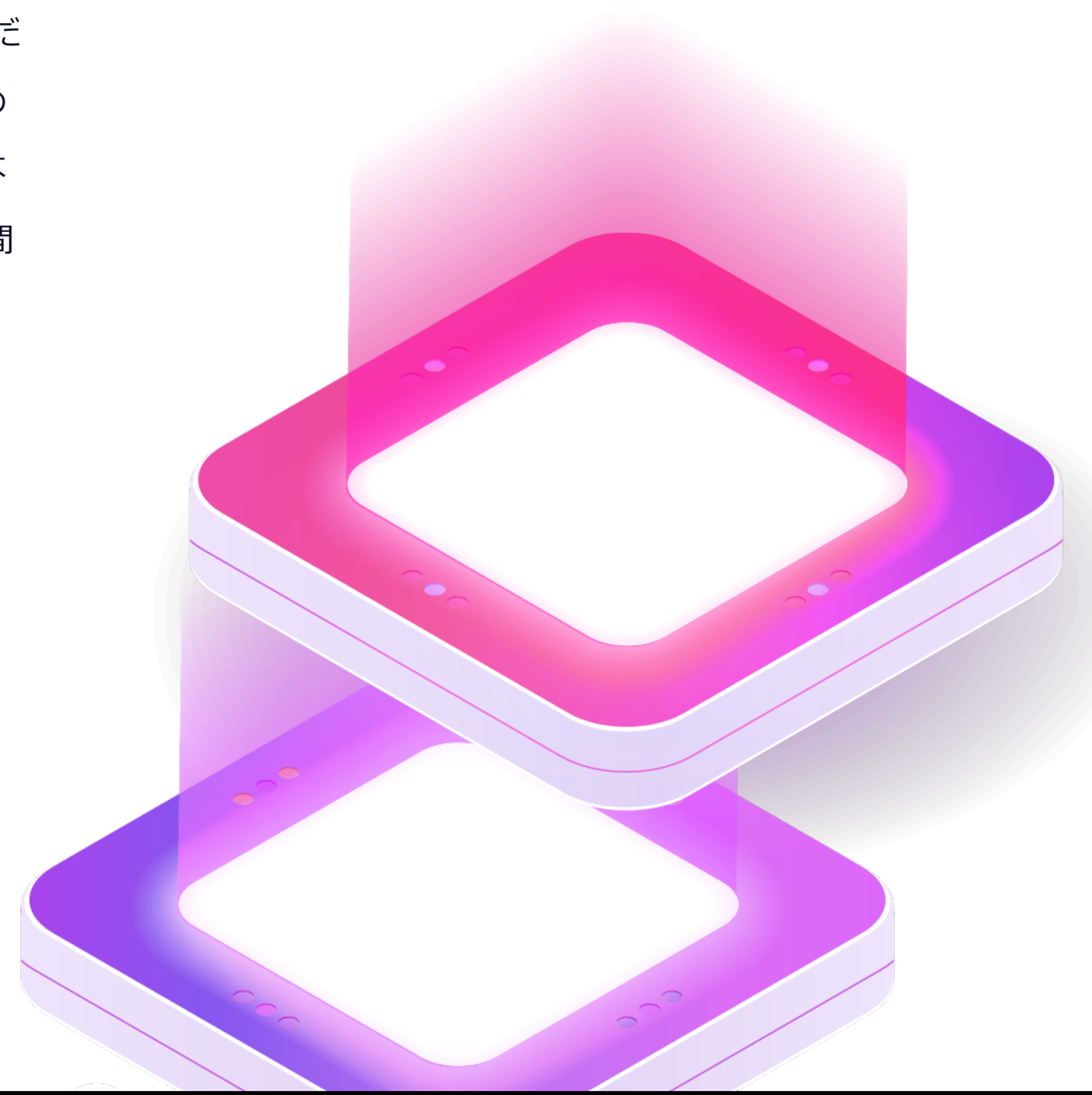
不正トラフィックは、チーム間の信頼を低下させるだけでなく、ブランドや企業の評判を大きく低下させる可能性があります。ボットが Twitter に与えた被害を考えてみましょう。悪質なボットの問題を抱えたプラットフォームで広告を出稿しようとする広告主がどれだけいるでしょうか?

不正トラフィックの被害は Twitter だけにとどまりません。2022年２月、イーロン・マスク氏も経営に関わった PayPal 社が、決済サービス プラットフォームにおいて約450万人の偽 ユーザーを発見しました。 これらの「ユーザー」は、 ５～10ドルの入会特典を提供する キャンペーンを大規模に悪用していました。

しかし、PayPal 社の被害は入会特典の不正利用だけに止まりませんでした。同社の顧客獲得戦略の失敗と、ユーザー数の増加に関するレポートの不正確性を株主が知ったとき、株価はわずか24時間で 25%と急速に下落しました。

これらの問題は単に不便・迷惑をかけたなどという単純なことではありません。 消費者と、消費者がビジネスを行うことを選択したブランドとの間の信頼が損なわれます。信頼が失われると、消費者は代わりに競合他社から商品を購入することを検討したり、同様の商品やサービスの使用を将来的に避けたりする可能性が出てきます。

不正トラフィックがなくなることは、残念ながらありません。行政や一般市民がこの問題を認識する中、2023年も同様の事件が発生することが予想されます。



2023年以降の不正トラフィック

2021年から2022年にかけて、CHEQ 利用企業の Web サイトにおけるチャットボットなど不正利用が 163%増加したことが判明しました。

2023年も、不正トラフィックが増加する傾向は続くでしょう。AI 技術の急速な発達は、ボットネットの作成を容易にし、加速させます。また悪質なボットは、功名さが増し、その精度はますます高まる可能性があります。

AI の進歩によるボットの拡大

ChatGPT などの高度な AI モデルの開発が進み、さまざまなユーザーが利用できるようになる中、個人が悪意のある目的でボットを作成して使用することも容易になりました。 これらのボットは、Web サイトのスクレイピング、フォームへの偽情報の入力、虚偽または身元を隠したトラフィックの生成に使用できます。 現在 ChatGPT は要求に応じて単純なスクレイパーボットを生成しますが、コードはあまり正確ではなく、ボットはほとんど機能しません。ただし、ChatGPT の作成者であり、基盤となっている人工知能モデルである OpenAI は、次のバージョンである GPT4 をこの夏にリリースする計画を発表しました。 GPT4 の詳細は明かされていませんが、GPT3 から 3.5 におけるバージョンアップの際の大きな飛躍を考慮すると、機能の大幅な改善が見込まれます。

ボットの精度の向上

サイバーセキュリティはいたちごっこです。防御が向上すると、ボットやクラッカーも防御を克服しようとします。しかし、無料で使用できる強力な人工知能モデルの出現は、そのパラダイムを覆し、悪意のある人物を有利に導く可能性を秘めています。

たとえば、ボットが AI を利用すると、誤解を招くレビュー、コメント、UGC（ユーザー生成コンテンツ）など本物のようなコンテンツや説得力のあるフィッシングメール、現在の機能をはるかに超える規模の偽チャットボットを作成できるようになる可能性があります。

これらのボットの精度が向上し、高機能なボットが作られた場合、我々は協力して、多面的な解決法で対策することを求められます。IP を手動でブロックし、500件に制限された Google のブロックリストを利用する古い方法は、規模の拡大に追いつきません。現代のビジネスにおいては、流入するトラフィックをモニタリングし、不正トラフィックがファネルに入る前に自動的にブロックして検出する必要があるのです。

CHEQ について

CHEQ は 世界中で 1 万5000 社以上のお客様に利用されている GTM セキュリティの第一人者として、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。

業界で評価の高いサイバーセキュリティ技術を利用した CHEQ は、脅威への対応からビジネスの持続性、ブランド価値、マーケティング効果まで、GTM 組織全体を保護するための最も幅広いソリューションスイートを提供しています。

CHEQ がどのように不正トラフィックをブロックし、不正リードや偽ユーザーからから GTM 施策を保護するのか、詳細は、セキュリティ診断の結果を踏まえてご説明させていただきます。