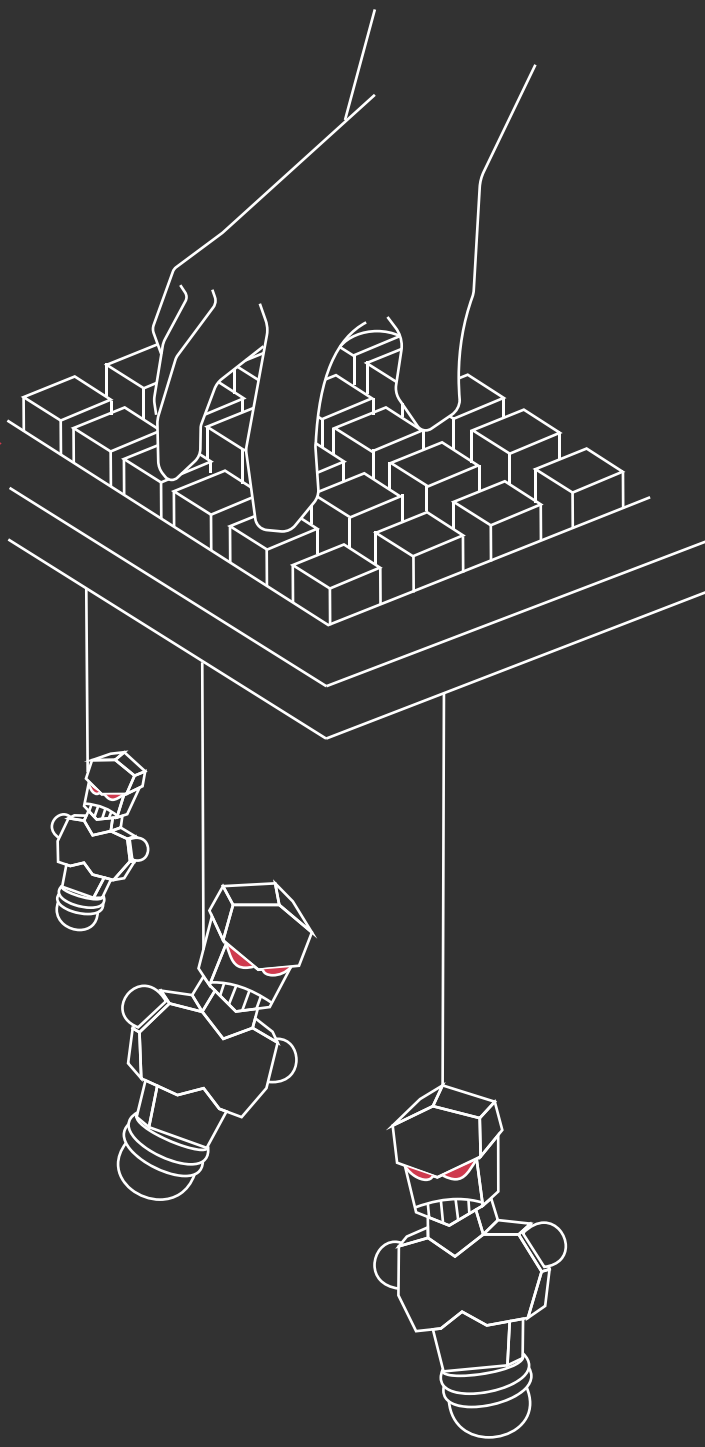
ボットの現状：
デジタル広告詐欺の実態



White Ops, Inc.
全米広告主協会（ANA：Association of National Advertisers）

※この文書は、全米広告主協会の許諾を得て Web 担当者 Forum 編集部が作成した日本語版です。

翻訳：株式会社トップスタジオ
編集：Web 担当者 Forum 編集部
http://web-tan.forum.impressrd.jp/e/2015/05/19/19944

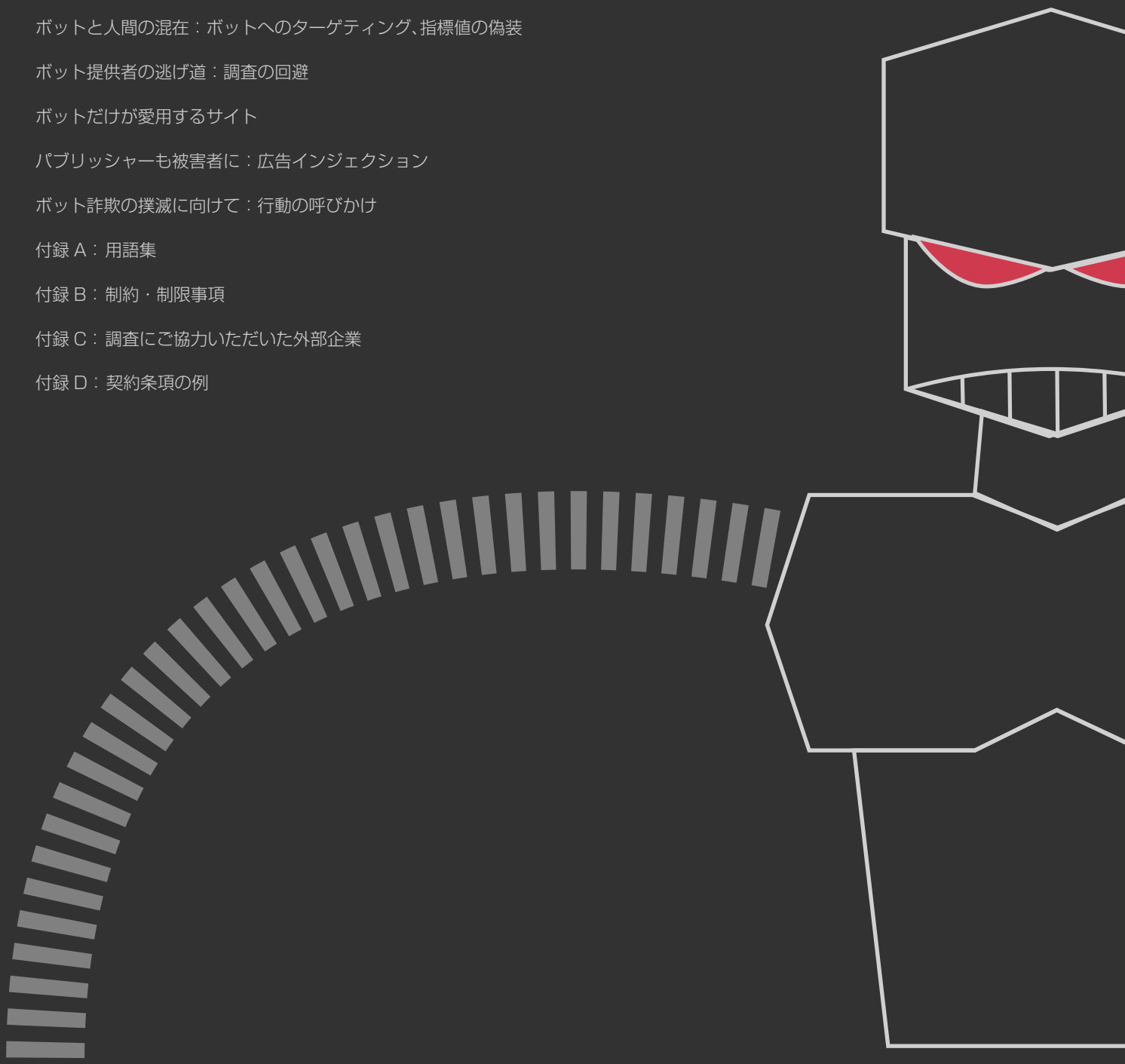
For more information please visit:
http://www.ana.net/content/show/id/botfraud

whiteops

ANA

2014 年 12 月

目次



調査にご協力いただいた ANA 会員企業

White Ops について

White Ops は、Web 上のボットやマルウェアの検出という課題に早くから取り組み、ボットによる操作と人間による操作とを区別する新たなボット検出技術の開発を手がけています。

ボット検出は、オンライン広告、パブリッシング、エンタープライズビジネスネットワーク、電子商取引、金融システムといった分野においてボットと人間の区別をするために不可欠な技術です。White Ops は、ボット詐欺からお客様を守るために、悪質なトラフィックを元から遮断し、ボットやマルウェアによる詐欺の収益性と持続性を断ち切ることに取り組んでいます。

全米広告主協会（ANA）について

全米広告主協会（ANA：Association of National Advertisers）は、マーケティングの発展と業界の未来に向けて指導的役割を果たす団体です。1910 年に設立され、現在では 640 社以上の企業が加盟しています。そのブランド数は 1 万を超え、広告宣伝費は合計 2500 億ドル以上に達します。また、ANA の下部組織として、BMA（Business Marketing Association）と BAA（Brand Activation Association）が活動しています。ANA は、マーケターの利益を発展させ、健全なマーケティングコミュニティの促進と保護に力を注いでいます。

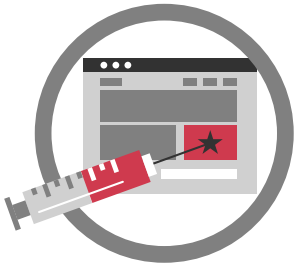
調査の概要

エグゼクティブサマリー

事前の予想では、ボット専用に構築されてボットだけがアクセスする Web サイトが見つかるものと想定していましたが、実際には、今回調査した約 300 万の Web サイトのうち、完全にボット専用のサイトは数千だけでした。大半のボットは、本物の企業が運営し、本物の人間が利用する、本物の Web サイトにアクセスしていました。こうしたボットの活動により、これらのサイトでは、広告費の支払い対象となるオーディエンスが実際よりも 5% ～ 50% 多くカウントされる結果になっていました。

ボットに対する無駄な広告費、2015 年は全世界で 63 億ドル

ボットの割合が現在の状態を維持したとすると、2015 年に広告主がボットに対して無駄に投じる広告費は、世界全体で約 63 億ドルとなる見込みです（世界全体での広告費の総額は、ディスプレイ広告が 400 億ドル、動画広告が 83 億ドルの見通し。今回の調査で見つかったボットの割合をこれらの値に当てはめて額を算出）。



一般家庭のパソコンをハッキングして広告詐欺に利用

ボットは、ごく普通のパソコンをハッキングして、Web サイトへのアクセスに利用しています。今回の調査で検出されたボットトラフィックの 67% 以上は、一般家庭の IP アドレスが発信元でした。ボット業者は、家庭のパソコンを遠隔制御することで、広告詐欺の稼ぎを得ています。ボットはブラウザーをハイジャックして本物のユーザーになりすまし、人間のトラフィックに溶け込んで、収益を増やしています。

広告ボットでターゲティングが台無しに

サイバー犯罪者は、家庭のパソコンにマルウェアを送り込んだうえで、そのパソコンを利用して実際の稼ぎを上げるために、広告ボットをインストールします。標的となるのは、実際のユーザーが利用しているコンピューターです。その人は、Gmail にログインしたり、Facebook でコンテンツをシェアしたり、Amazon で買い物したりしています。したがって、そこに入り込んだボットは、ユーザーの行動に溶け込むだけでなく、ターゲティングの対象にもなります。

ボットは、ハイジャックしたパソコンの実際のユーザーのログイン情報などの認証情報を利用します。ボットは人間のユーザーよりも多くのクリックを行います（ただし、現実味がないほど極端に多いわけではありません）。高度なボットになると、きちんとマウスを操作して、カーソルを広告の上に移動します。また、ショッピングカートに商品を入れたり、数多くのサイトを訪問したりすることで、広告主やパブリッシャーのターゲットとなるデモグラフィック属性を備えたユーザーに見えるような履歴やクッキーを生成します。

ボットは蔓延するも、割合にはばらつきが

今回の調査では、計 9 業界の多種多様なブランドを調査しました。Kantar のデータによると、これらの各ブランドの米国での年間広告予算は、1000 万ドル以下から 10 億ドル以上までさまざまです。しかし、参加企業の広告支出の規模と、検出されたボットのレベルとの間には、相関関係はありませんでした。

ボットの割合が高かった調査結果：

夜間

検出されたボットの約半数には、人間同様に昼間のみ活動するという巧妙さがありませんでした。

ディスプレイ広告

ディスプレイ広告の全インプレッションの 11% がボットによるものでした。

動画広告

動画広告の全インプレッションの 23% がボットによるものでした。

プログラマティックとリターゲティングのインベントリ

プログラマティックインベントリでは、平均 17% がボットトラフィックでした。リターゲティング広告では 19% がボットでした。

トラフィック誘導

サードパーティのトラフィック誘導は、52% がボット詐欺でした。

ドメインのカテゴリ別

金融、家庭、食品のジャンルはボットによるトラフィックの割合が高く、16% ～ 22% でした。

目的と手法

「ボット」とは、ネットワーク化されたコンピューター上で動作するソフトウェアスクリプトで、ボットネットの一部として、中央のコントローラーによって制御されています。ボットネットのコントローラーは、ボットネットを構成するコンピューターに対して、さまざまな動作や任務遂行の命令を送信します。たとえば、広告詐欺、オンラインバンキングからの金銭詐取、ID の盗み取り、分散型サービス拒否（DDoS）攻撃などです。広告詐欺を遂行する場合、ボットネットのコントローラーは、ボットネットを構成するコンピューターを制御して、広告の表示やクリックを行わせます。これにより広告主は、広告のクリック数やインプレッションに応じた費用を支払うことになります。実際には人間のユーザーは広告に接していないにもかかわらずです。

これまで広告主は、膨大な広告詐欺を検出できずにいました。今回、White Ops と全米広告主協会は、同協会に加盟する 36 社の協力のもと、2014 年 8 月 1 日から 9 月 30 日までの 60 日間にわたって、デジタル広告キャンペーンのトラフィックを分析しました。

この調査では、新たに開発した技術を利用してボットの正体を暴き、広告のインプレッションの消費元について真の姿を解き明かしました。今回の調査対象は 55 億インプレッションに及びます。デジタル広告のボットに関する調査で、実施を公表したものとしては過去最大です。

調査に参加したすべての企業に対して、White Ops が指導を行いましたが、調査の中で測定する広告トラフィックの種類については、各社の判断に委ねました。対象のトラフィックの分析点、種類、割合については統一しておらず、参加各社に義務づけた要件はありません。人間からのリクエストとボット（機械制御）のリクエストとを区別するために White Ops が利用した独自の手法が、今回の調査方法の中で唯一共通していた部分です。

White Ops は、数十億のインプレッションを評価し、数億に及ぶボットを検出しました。調査対象は、動画広告と、あらゆる種類のディスプレイ広告です。直接購入、ネットワーク、プログラマティックの各チャネルで購入したディスプレイ広告と動画広告をすべて評価しました。

今回の調査では、全米広告主協会に加盟する 36 社のトラフィックを調べました。対象の業種は次のとおりです：自動車、酒類、消費財、金融 / 保険、ホスピタリティ、製薬、レストラン、小売、IT

36社 参加企業数

181 キャンペーン数

300万 ドメイン数

55億 インプレッション

60日 期間

データの集計方法

今回の調査は、この 10 年間で浮かび上がってきた脅威であるデジタル広告詐欺について、その現状を調べたものです。

この調査では、新しいボット検出技術を利用して、広告詐欺の攻撃に関するデータを集めました。参加各社から得たデータは、White Ops の過去のデータや、外部の協力企業（Chartbeat、Ghostery、Grapeshot）が持つデータと比較対照しました。

今回の調査に参加した協会加盟企業 36 社に関して、それぞれの取得データで企業個別の影響を最小限に抑えるために、複数の種類のトラフィックや分析方法にまたがってデータを集計しました。

今回の調査は、公表のうえで実施したものであり、著名なデジタル広告ブランドに関して、1 年の中でも広告活動のペースが比較的落ち着いている時期を調べたものです。したがって、**今回の調査で確認されたボットの状況は、広告のエコシステム全体におけるボット詐欺の総合的な状況に比べて、結果が低く出ている**ことが考えられます。

このレポートでは、広告主、広告代理店、パブリッシャーの方々に向けて、ますます高まりつつあるデジタル広告詐欺の脅威に対する防御を確立するためのアドバイスを紹介していきます。

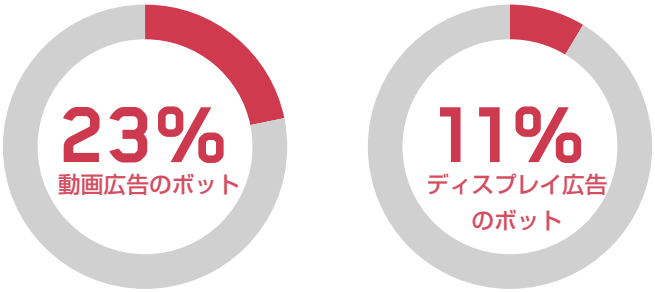
ボットが
デジタルメディアに
及ぼす影響

あらゆる種類のキャンペーンにボットが蔓延

技術的に難しいと考えられている動画インベントリも、ボットの標的になっています。一般に、動画広告の CPM はディスプレイ広告よりもはるかに高く、ボットによる詐欺の割合は、動画広告の方が 2 倍以上でした。

リターゲティングキャンペーンでのボットの検出データと、ボットのエンゲージメントの指標値を見てみると、CPM が高い媒体には高度なボットが集まる可能性があることがわかります。精鋭のボットネット運営者ともなると、CPM が高いインベントリがもたらす収益拡大のチャンスを生かせるようにボットをカスタマイズしていたようです（29 ページの「ボットはエンゲージメントと視認能力に関する測定値すべてを偽装」を参照）。

調査全体でのボットの割合



ケーススタディ

プレミアムディスプレイ広告と動画広告でボットの割合が高かった事例

10% がボット

62% がボット

11% がボット

今回の調査に参加した消費財分野の企業の事例です。この企業の広告代理店が、米国のある大手ケーブル / メディア企業が所有および運営するサイトの 12 のプレースメントに広告を出したところ、ボットの割合は 10% でした。また、オープンな取引を行っている動画 SSP（サプライサイドプラットフォーム）と、ある大手のインターネットポータルの両方で、この消費財企業が動画広告枠を購入したところ、ボットの割合は、SSP が 62%、ポータルが 11% でした。

ボット詐欺の割合はキャンペーンやプレースメントで差異

ボットの割合は、キャンペーンやプレースメントごとに異なり、予測が付きません。したがって、ボット詐欺によって生じる実際のコストを割り出したり比べたりするのは、一筋縄では行きません。うまくいく戦略の 1 つは、ボット詐欺による損失を、ブランド全体や会社全体の合計の数字で見るのではなく、プレースメントレベルで個別に見ていくことです。

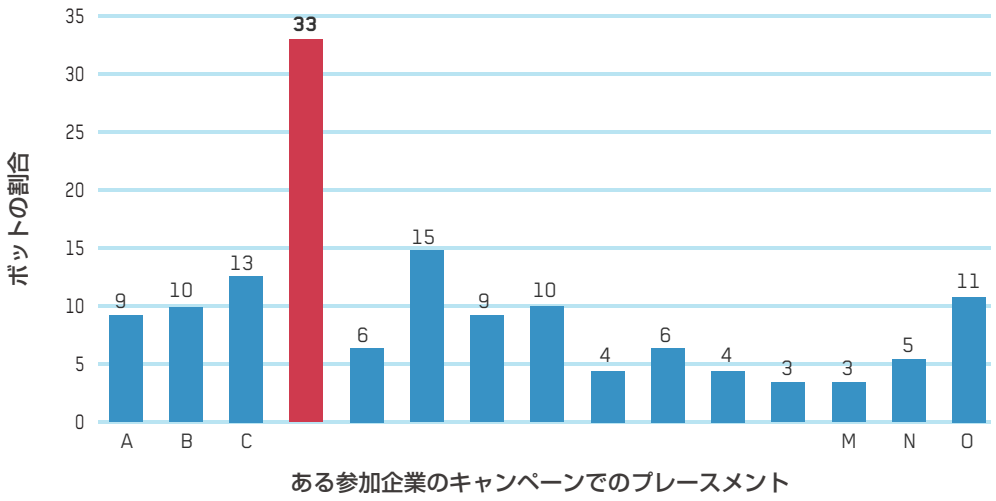
アドバイス

広告費の損失が多いプレースメントに対するトラブルシューティングを行う

情報を細分化して、たとえば「プレースメント I、K、L、M はボットの割合が平均以下だったが、プレースメント D はインプレッションの 33% をボットに奪われた」というように把握できれば、ブランド全体で見たときにボットトラフィックの水準が低かったとしても、状況をすばやく分析でき、ボットによる多額の損失を防ぐことができます。

ボット詐欺による損失を加味したうえで、ヒューマンインプレッションの実際のコストを表すのが、「CPH（Cost Per Human、人間インプレッション単価）」という指標です。CPH の数値を、プレースメントごと、キャンペーンごと、ブランドごと、トラフィックの発信元ごとに比較すれば、本物の人間のオーディエンスに到達するのにかかる実際のコストを把握したり説明したりできます。

データ



CPH
Cost Per Human
（人間インプレッション単価）

ボットトラフィックによる損失を加味したうえで、ヒューマンインプレッション 1000 件あたりの実際のコストを表す指標

図 1：同じブランド内でもボットの割合はプレースメントごとに異なる

時間帯によるボット詐欺の違い

ボットの活動は完全に平等なわけではありません。半数のボットには、人間が通常起きている時間に活動するという巧妙さがありませんでした。

データ

夜の方がボットの割合が高い

検出されたボットの数自体は日中の方が多かったのですが、トラフィック全体に対する割合は夜の方が上でした。

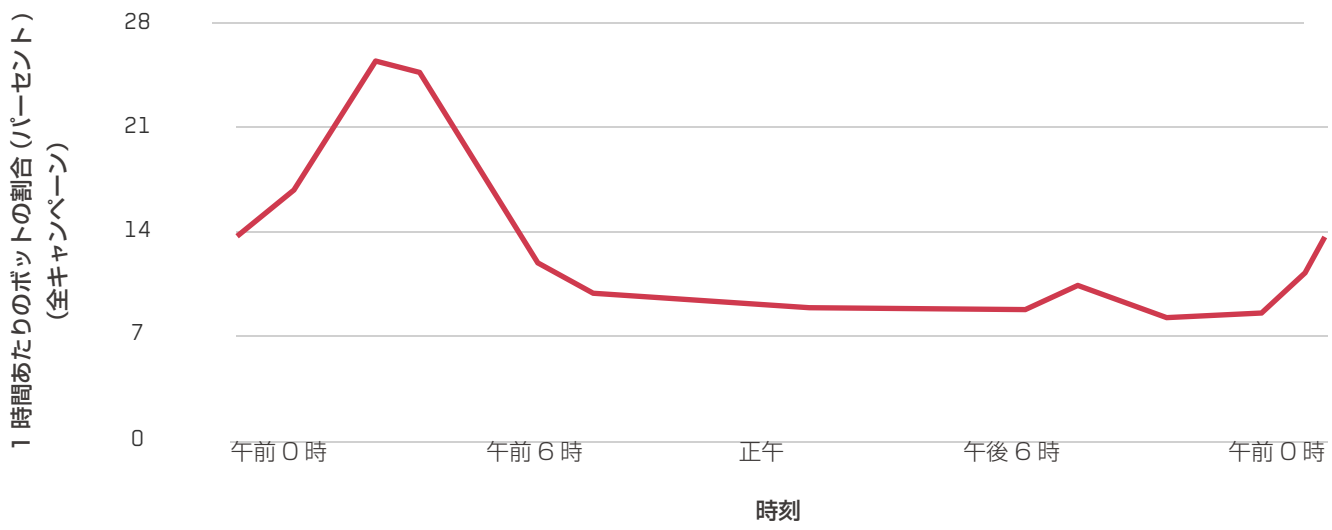


図 2：調査期間全体における、時間帯ごとのボットトラフィックの推移

現地時間の判定には、Maxmind 提供の IP ジオロケーションデータを使用

アドバイス

特定の時間にボットの割合が高まるのを抑えるために、時間帯制限出稿を検討する。

リーチを増やそうとすると ボットも増える

オンライン広告でいう「リーチ」とは、広告に接したユニークユーザー数のことです。今回の調査では、参加企業が掲出サイトを特定しない RON（Run Of Network）キャンペーンでリーチを増やそうとした場合、ボット詐欺の割合は平均 16% となり、通常の平均より高い値となりました。

週末、月末、四半期末を中心に、広告主がトラフィックの増加を求めることがあります。こうしたときに、実際にアクセス可能な人間と、広告主が求めるトラフィックとの差が、ボットによって埋まることがあります。

ボットには、特定の層の膨大なオーディエンスに簡単に到達できるかのように見せかける力があります。ボットはどんなおユーザーなりすますことができます。スポーツ好きのユーザーにも、年収 10 万ドル超のユーザーにも、車を買いたいと思っているユーザーにも、孫へのクリスマスプレゼントを探しているユーザーにも。

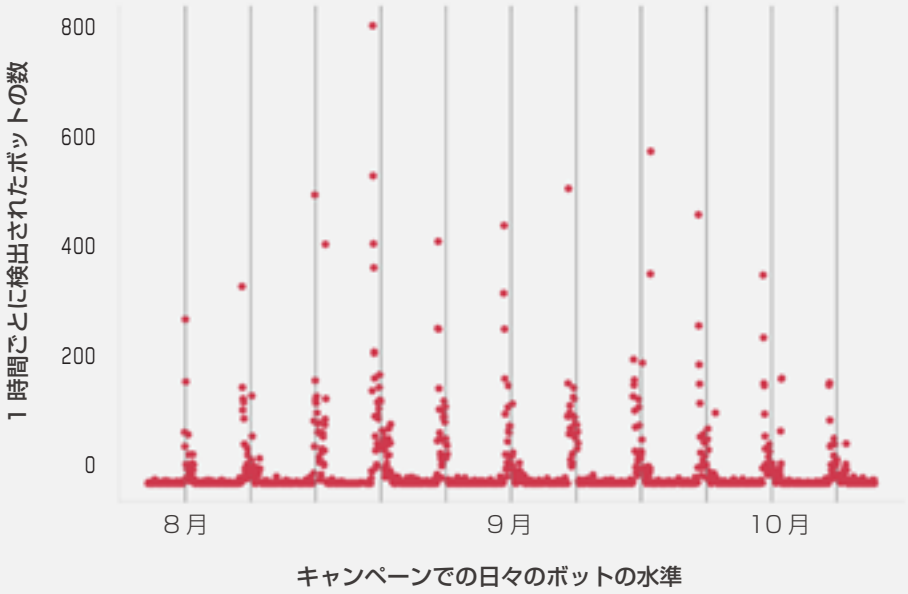
White Ops のこれまでの観測でも、商品発売、映画、テレビ番組など、特定の期限があるリリースを中心としたキャンペーンは、ボットの活動の影響を格段に受けやすくなっています。期日の枠が明確に定まっていることで、ボットの問題に拍車がかかる場合があるからです。

ケーススタディ

毎週土曜日にボットが激増

今回の調査に参加した酒類業界の企業の事例です。キャンペーンの中で、毎週末の土曜の正午（太平洋標準時）にボットのスパイク（急増）が生じ、1 時間あたりの数がゼロから 800 に増えるという変動が一様に見られました。ピークの土曜正午を過ぎると、1 時間あたりの数はゼロに戻りました。

土曜以外の曜日は、ボットはほぼゼロの水準に下がっています（右のグラフで、線の間が空いている部分がそれです）。毎週土曜に発生するボットのスパイクは、このキャンペーンでのボット詐欺全体の 95% を占めていました。



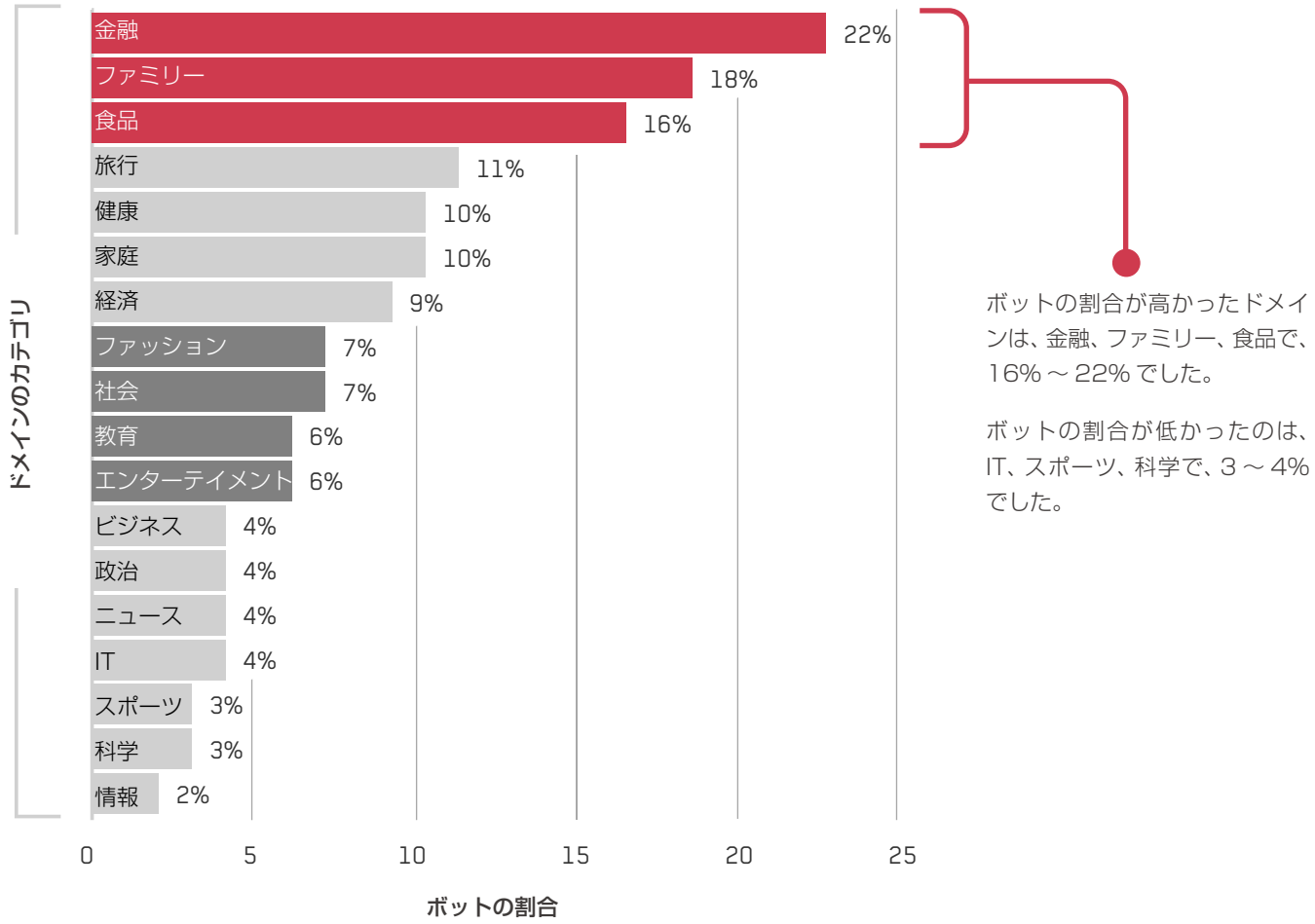
- Y 軸のそれぞれの点は、調査の中で 1 時間ごとに検出されたボットの数を表します。

図 3：このキャンペーンでは毎週土曜の正午にボットのスパイクが発生

ボットの割合は
ドメインのカテゴリごとに異なる

参加企業の業種別で見た場合、ボットトラフィックの割合に関して一定の傾向は特に見られませんでした。

しかし、今回の調査で得たボットのデータを、Grapeshot のドメインコンテンツ分析と照合して調べてみたところ、広告が表示されたドメインのカテゴリごとに、ボットトラフィックの割合に顕著な違いが見られました。



ボットの割合が高かったドメインは、金融、ファミリー、食品で、16% ～ 22% でした。

ボットの割合が低かったのは、IT、スポーツ、科学で、3 ～ 4% でした。

図 4：ボットの割合が高かったのは、金融、ファミリー、食品のドメイン

Grapeshot 提供のドメインカテゴリデータを使用

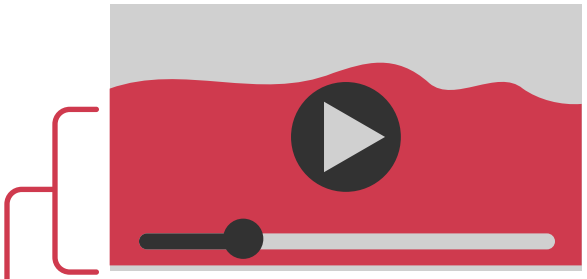
動画広告キャンペーンが大きな食い物に

データ

動画広告の全インプレッションの 23% が、ボットによるものでした。

動画のプレースメントでは、ボットトラフィックの割合は 2% ～ 100% と幅がありましたが、参加企業のキャンペーンごとで見ると、ボットトラフィックは最大 63% でした（複数のプレースメントで構成されていたキャンペーンも含みます）。参加企業の中には、複数の動画キャンペーンを展開した所もあり、1 社で動画広告のインプレッションが最高 9000 万に及んだ参加企業もありました。キャンペーンの規模とボットの割合の間に相関関係は見られませんでした。

動画広告は、ボットトラフィックだけでなく、ボット以外の広告詐欺にも狙われていました。動画広告キャンペーンで、インプレッションの規模が特に大きかったもののなかには、ボットトラフィックに加えて、動画を自動再生するアドウェアに大規模に見舞われたキャンペーンもありました（24 ページの「アドウェア：広告詐欺はロボットの仕業とは限らず」を参照）。動画自動再生のアドウェアは、ボットを導入するのではなく、人間がほとんど（あるいはまったく）操作できないアドウェアアプリケーションを利用して、広告インベントリを不正に消費していました。



最大 **63%**

参加企業の動画広告キャンペーンでのボットの割合の平均

アドバイス

広告詐欺がなければ、デジタル動画広告は大きな可能性を秘めています。広告代理店や広告主が、オンライン動画広告キャンペーンから大きな価値を引き出し、マーケティングの目標を達成するためには、品質管理のメカニズムを導入することが必要です。

そのような品質保証の手段は、プログラマティックディスプレイ広告のキャンペーンに対する広告詐欺を防ぐうえでも役立ちます。

動画広告とプログラマティックディスプレイ広告のキャンペーンで信頼性を確保するには：

- 継続的な不正監視の仕組みを導入する。
- サイトがトラフィック誘導を利用していないことをボット検出技術により確認する。
- アドウェアやボットトラフィックをはじめ、あらゆる種類の広告詐欺を監視する。

トラフィック誘導があるとボットの割合が上昇

パブリッシャーは、自らのサイトで測定されるオーディエンスのレベルを高めるために、トラフィック誘導（サードパーティを通じて閲覧者を増やす手法）を利用することがあります。

我々は、トラフィック誘導の徴候が見られるトラフィックを、調査全体でのトラフィックのボットの割合と比較してみました。ボットの割合が高いと判断できる頻度は、トラフィック誘導の徴候がある場合には、他のあらゆる挙動と比べて上でした。

トラフィック誘導の場合にボットの割合が高いという傾向は、調査期間全体にわたって一貫して見られました。個別のトラフィック誘導でのボットの割合は、完全に人間（ボットが 0%）のものから、ボットが 100% のものまで、幅がありました。この範囲のなかには、インセンティブを受けていることが明らかとなったトラフィックも含まれていました。

有名なパブリッシャーやプレミアムパブリッシャーの場合でも、トラフィック誘導ではボットの割合が高い点は、変わりませんでした。

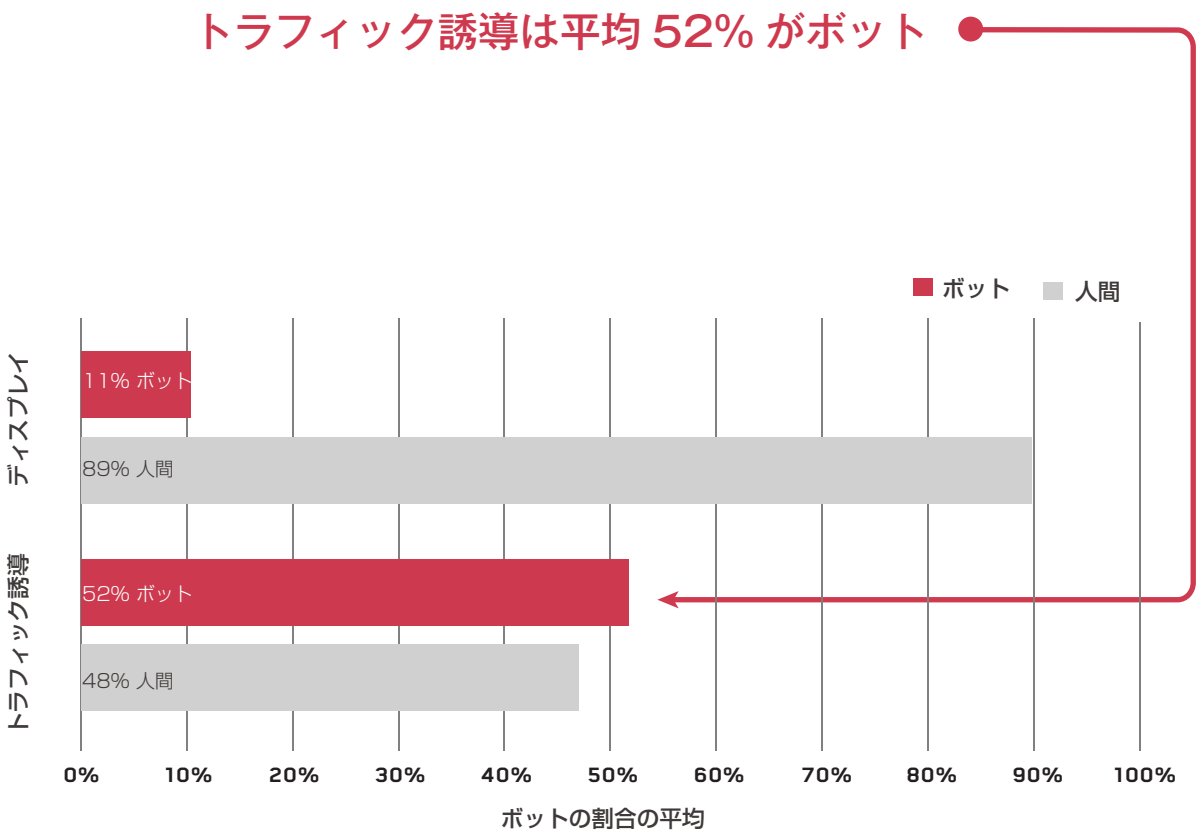


図 5：トラフィック誘導で得られるのは人間よりボットのトラフィック

思い込みは禁物：
プレミアムサイトも
ボットの餌食に

プレミアム枠の直接購入にもボットは混入

ボットの猛威は、あらゆる層、あらゆる種類のパブリッシャーに及んでいます。知名度の高いドメインでも、プレミアムの直接購入のディスプレイ広告キャンペーンで、ボットの割合が 10% 以上ということが多くありました。

プレミアムパブリッシャーのトラフィックでの広告詐欺には、ボットトラフィックによるものと、広告インジェクション（本来は認められていないサイトに広告を不正に掲載すること）によるものがありました。

「プレミアムパブリッシャーへのトラフィックにはボットは入り込まない」と広告主が思い込んでいると、意図的または偶発的なボット詐欺によって大きな被害に遭うリスクがあります。

ケーススタディ

プレミアムパブリッシャーで 19% がボット

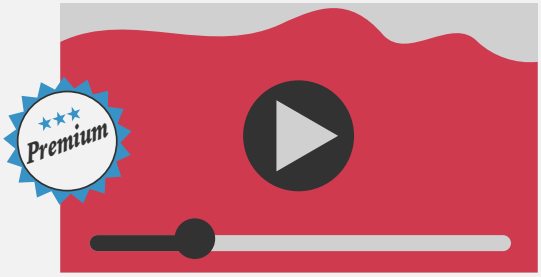
今回の調査に参加した消費財分野の企業の事例です。米国のプレミアムメディア企業から 23 万インプレッションを購入したところ、そのサイトからのトラフィックの平均 19% がボットでした。

ケーススタディ

プレミアムパブリッシャーでの直接購入の結果、動画広告キャンペーンの 98% がボット

ライフスタイル業界で有名なあるプレミアムパブリッシャーでは、Web ページのレイアウトとして、大きな動画プレーヤー 1 つをページの上部に配置したレイアウトを利用していました。自動再生動画の周囲に、ランダムな選択と見られるコンテンツを配した形のページでした。

今回の調査に参加した自動車業界の企業が、このパブリッシャーのページで動画広告を配信したところ、その 98% がボットによる消費でした。動画のインプレッションは合計で約 4000 だったものの、人間に対するインプレッションはそのうちの 100 足らずでした。



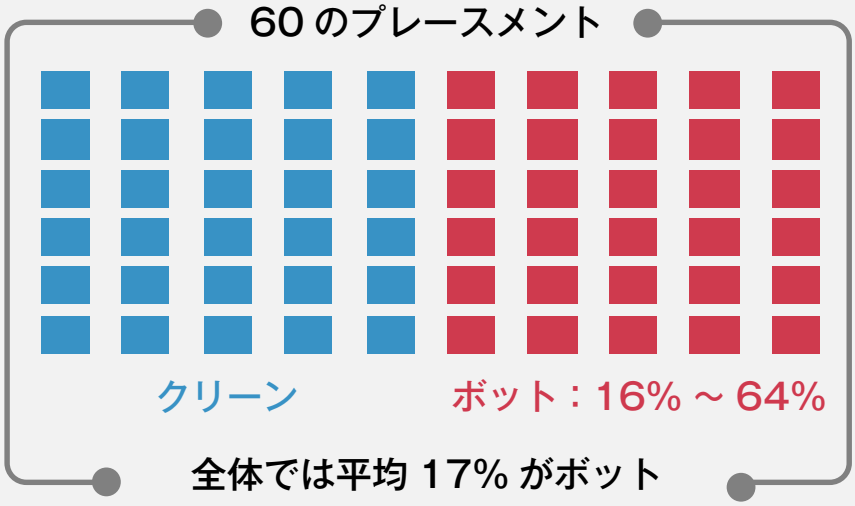
98% がボット

平均値の魔術：
クリーンなプレースメントとボットが多いプレースメントの混在で値が低下

ケーススタディ

直接購入のプレミアムキャンペーンで 16% ～ 64% がボット

今回の調査に参加した小売業界の企業の事例です。この企業の広告代理店が、米国の有名なメディア企業が所有および運営するサイトに対して直接購入を行いました。60 のプレースメント全体では、ボットの割合は平均 17% でした。約半数のプレースメントは非常にクリーンでしたが、残りの半数には 16% ～ 64% のボットが含まれていました。



プレミアムキャンペーンでボットを抑えるには思い込みからの脱却が必要

知名度の高いプレミアムパブリッシャーと言えども、その名声を確立した Web の黎明期と比べれば、質が低下している可能性があります。現在では、パブリッシャーの評判の高さは、ボットトラフィックの水準を予測するうえでの信頼に足る判断基準にはなり得ません。

アドバイス

思い込みをテクノロジで検証する

- プレミアムキャンペーンで広告費がボットに流れるのを防ぐためには、サードパーティの不正検出技術を利用して、あらゆる提供元からの広告購入について、思い込みや想定を検証したり、その誤りを明らかにしたりすることが必要です。対象がプレミアムパブリッシャー、トップクラスのパブリッシャー、信頼されている提供元であってもです。
- トラフィックの品質に先入観を抱くこと（パブリッシャーがプレミアムかどうかやティアの分類に基づいて）は避けてください。

メディアサプライチェーン全体から見たボットの発信源

デジタル広告のサプライチェーンですべてのステークホルダーを騙すのがボット

ボットのサプライチェーンに関与している関係者のなかには、トラフィックにボットが含まれていることを知らず、不正な利益を上げようという意識がない人もいれば、ボットトラフィックを積極的に呼び集めて、利益を増やそうとする人もいます。

デジタル広告のサプライチェーンですべてのステークホルダーがボット提供者に騙される：

- 広告主のマーケティングチーム
- 広告代理店のメディアプランニングチーム
- 広告代理店のメディアバイイングチーム
- 広告代理店のアドサーバー
- 広告代理店の分析 / 最適化チーム
- パブリッシャーの広告運用チーム
- パブリッシャーの営業部門
- パブリッシャーのアドサーバー
- サードパーティの広告検証サービス
- 広告主の内部監査管理

ボットによる詐取は、1 件 1 件がミリ秒単位の速さであり、被害者が検出できないことも少なくありません。ボット提供者は、こうした詐取を自動化し、1 日に何億回という規模で繰り返すことによって、きわめて大規模な詐欺を実現しています。

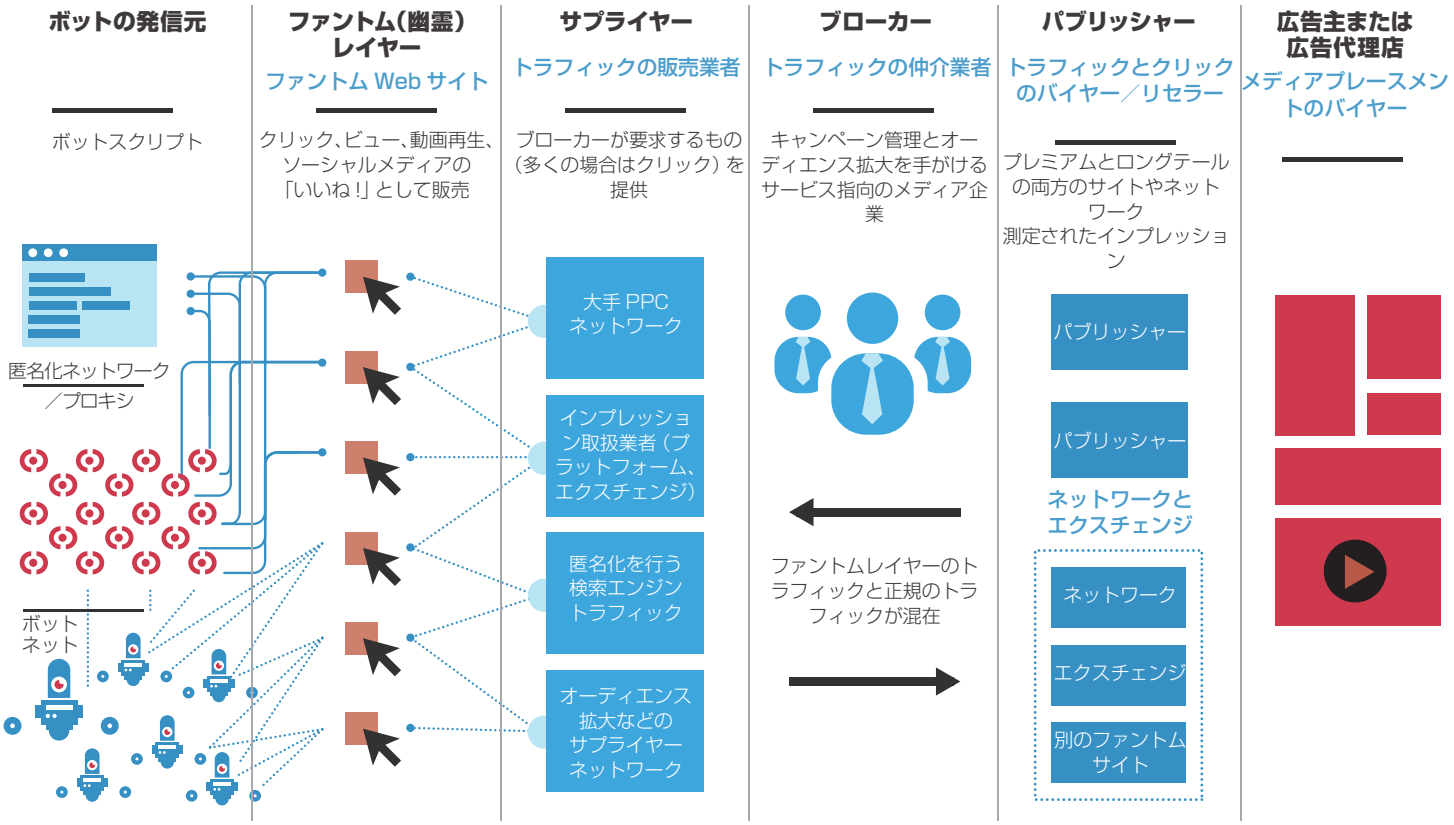


図 6：不正な Web トラフィックを生成してロンダリングするファントム（幽霊）レイヤー

ボットインプレッションは、ボット提供者が発生源です。デジタル広告のエコシステムのなかで、正規の要素とファントム（幽霊）レイヤーの要素の両方を経由しています。ファントムレイヤーを構成しているのは、広告詐欺のロンダリングのためだけに運営されている Web サイトです。

アドウェア：
広告詐欺はロボットの仕業とは限らず

「アドウェア」とは、目に見える形や見えない形でユーザーに広告を配信し、広告の消費を促すソフトウェアです。多くの場合、ユーザーのデバイスに自動でインストールされます。

今回の調査に参加したうちの数社では、アドウェアによる膨大な活動が確認され、「ボット詐欺」ではなく「広告詐欺」として分類されました。

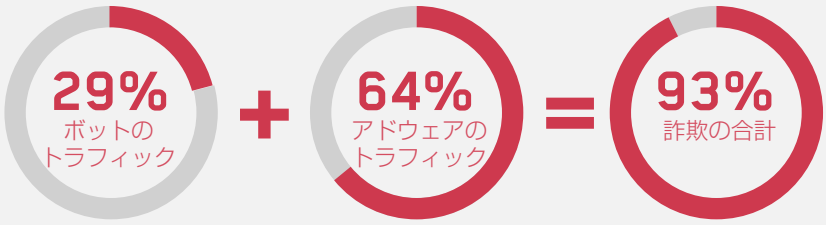
アドウェア業者は、ボットを利用して不正なインプレッションを生成したわけではありません。しかし、アドウェアの活動は正規に認められていない詐欺的なものであり、一般のコンピューターユーザーと広告主の両方に害をもたらします。アドウェアによって生まれた、広告主にとっては望ましくないインプレッションの対価として、パブリッシャーは膨大な収益を上げていました。

こうして関係者に影響をもたらすアドウェアは、ボットと非常に近いものでした。主な違いは、アドウェアはポップアンダーウィンドウを生成していたことです。ユーザーがそのウィンドウを閉じるまでは表示され続けているもので、その間は、ユーザーが知らないうちにアドウェアはバックグラウンドで動作を続けていました。

ケーススタディ

一般のパソコンユーザーを犠牲にしてデジタルメディア予算を食いつぶすアドウェア

今回の調査に参加したある企業の動画広告キャンペーンの事例です。調査開始から 1 週間足らずで、単一のアドウェア業者のアドウェアに対する配信が 1000 万インプレッションに達しました。この動画広告キャンペーンは全体で約 9000 万インプレッションでしたが、正規のヒューマンインプレッションは 7% にとどまり、93% は詐欺でした。



このアドウェアのパブリッシャーは、動画広告を収益源とするサービスを提供していました。このサービスの利用者は、アドウェアのソフトウェアをダウンロードすることが必須となっています。場合によっては、何も知らないユーザーのコンピューターにアドウェアのソフトウェアを無断でインストールすることで儲けを上げているケースも見られました。このアドウェアは、ユーザーのコンピューターのバックグラウンドで動画広告を 1 つずつ順番にひたすら再生していくというものです。ユーザーからは広告がまったく見えないケースがほとんどでした。

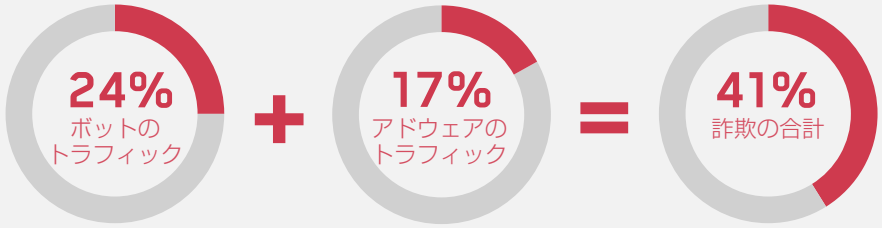
このアドウェアは、最初にポップアンダーを表示し、その中で動画広告を再生していました。音声の再生中は自らの音量をゼロに変えますが、他のソフトウェアの音量調整は変更しません。ユーザーがポップアンダーを閉じた後も、アドウェアはミュート状態で広告の再生を続けるようになっていました。ユーザーがコンピューターを再起動してログインし直した時には、アドウェアのサイトやアプリケーションを再度開かなくても、動画広告を自動再生する仕組みでした。アドウェアの自動再生機能は正規のものではなく、ユーザーは制御できないようになっていました。

アドウェア：攻撃にも程度の差

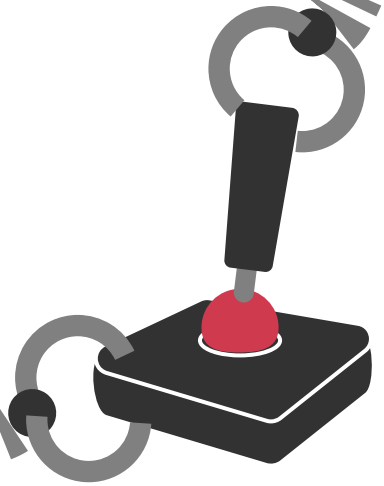
ケーススタディ

アドウェアによる不正の程度には違いあり

ある別のアドウェアサイトの場合は、動画広告を無音で自動再生するものでしたが、ユーザーが見ることができる状態のときのみ再生していました。また、ユーザーが広告のポップアップを閉じた時に、広告の再生を最後まで続ける仕組みにはなっていませんでした。その分、ユーザーによる制御性が高いと言えます。この事例では、消費財分野の参加企業の 700 万インプレッションのうち、正規のヒューマンインプレッションは 59% で、詐欺は 41% でした。



ある参考企業の動画広告キャンペーンでのトラフィックの内訳



大半のボットは一般家庭の IP アドレスが発信元

広告主のなかには、詐欺の問題を軽減するために IP アドレスブラックリストを活用しようとする所もあります。しかし、ボット提供者も、ブラックリストの作成と撃破のために使われていた指標に対抗できるよう、ボットを少しずつ進化させています。ドメイン名のブラックリスト、地理情報によるブラックリスト、ブラウザーやリターゲティングのリストなど、我々が調査したリストは、大多数のボット詐欺に対して抑止効果がありませんでした。

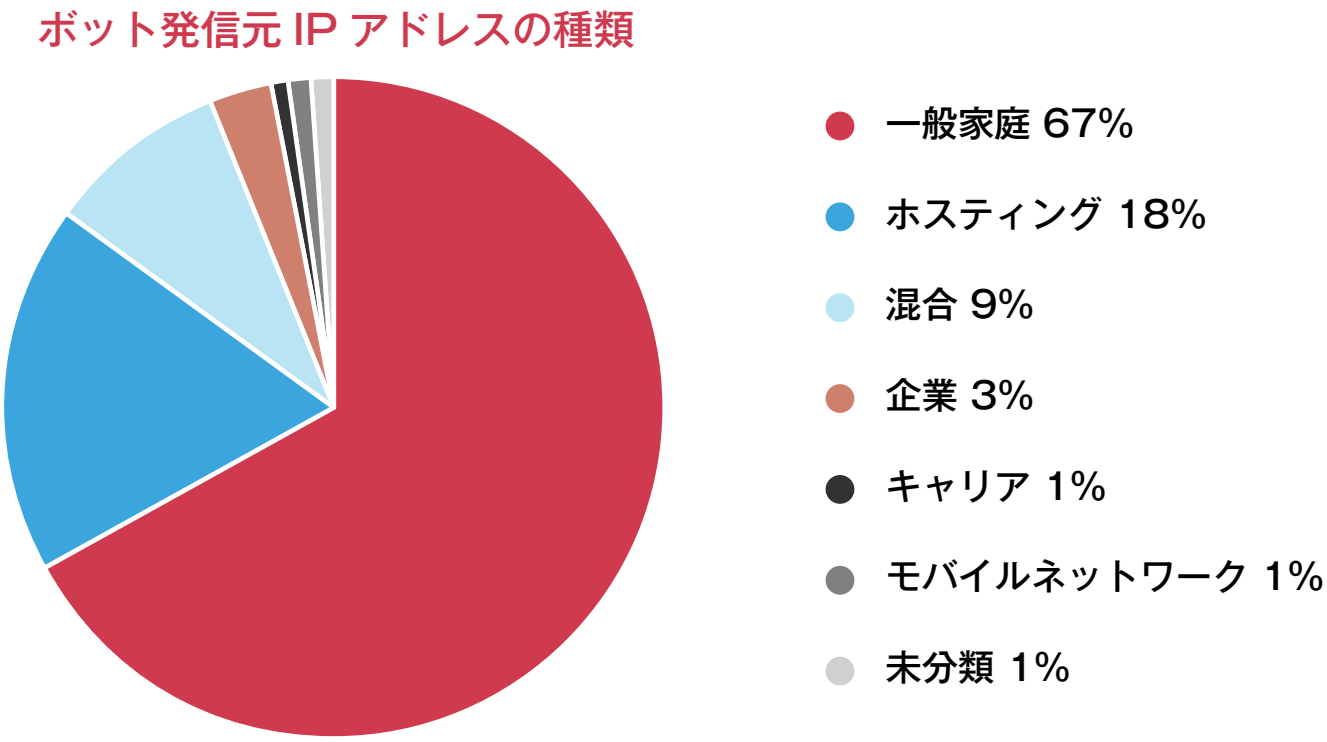


図 7：ボットネット運営者は一般ユーザーのコンピューターに侵入してボット詐欺を遠隔制御

ボットの問題に対処するために作成されたリソースのうちで、最も初期からあるものの 1 つが、「IAB/ABC International Spiders and Bots List」です。このリストは、人間ではないトラフィックを検出し、こうしたトラフィックが Web 分析でカウントされるのを防ぐためのもので、今でも存在します。人間以外によるトラフィックは、広告のインプレッションやサイトのトラフィック数の大幅な水増しにつながりかねませんが、このリストを使うことでフィルタリングが可能です。リストは毎月更新されています。広告のインプレッションやサイトのトラフィックのデータに関する透明性が高まり、正確に測定できるようになることが、このリストの最終的な効果です。ただしこのリストは、犯罪的なボットネットを追跡するためのものではありません。

ボットネットのコントローラーは一般ユーザーの身元とマシンをハイジャック

これをお読みのあなたが今お使いのコンピューターも、ボットトラフィックの発信元になっているかもしれません。今回の調査で検出されたボットトラフィックの 67% 以上は、一般家庭の IP アドレスが発信元でした。

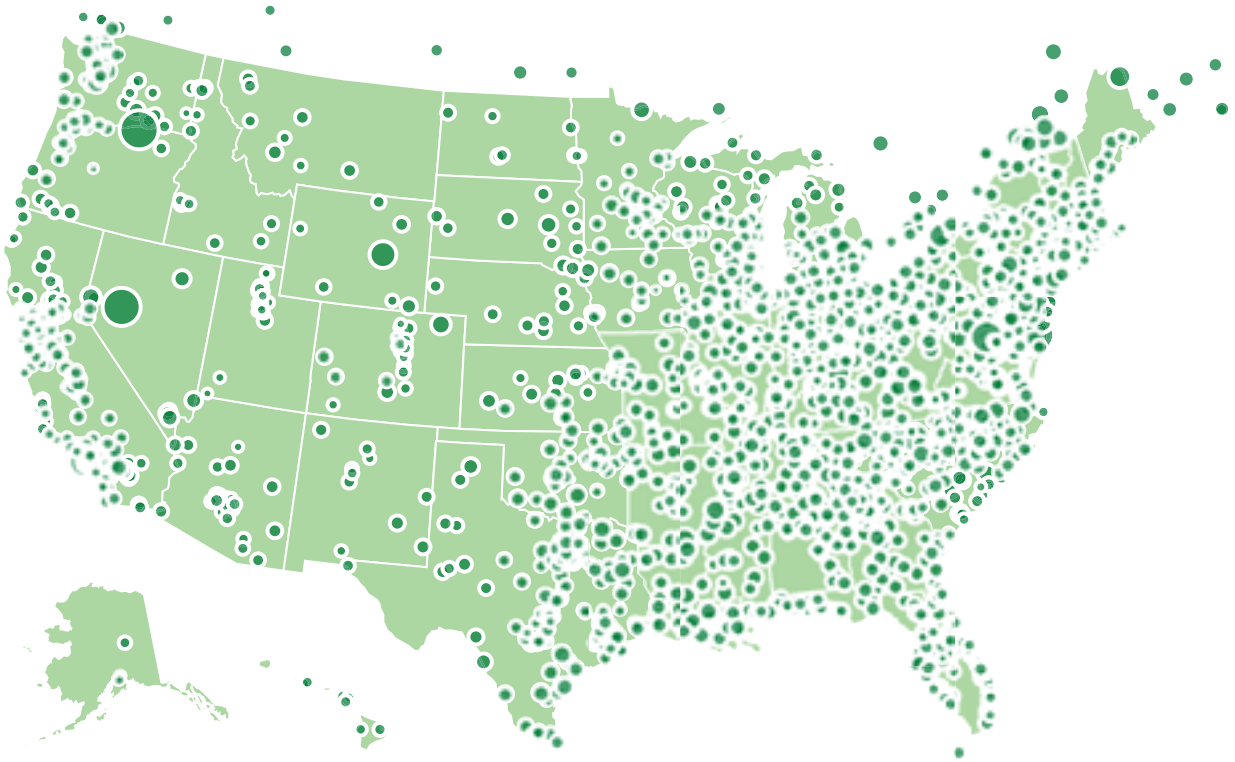


図 8：ボット詐欺の発信元となった一般家庭の IP アドレスは全米各地に分散

ボット業者は、米国の一般家庭のコンピューターをハッキングして、米国内の IP アドレスとクッキーを手中に収めています。ボットトラフィックの大半は、大規模な侵害を受けた一握りのコンピューターによって生成されています。

ボットと人間の混在：ボットへのターゲティング、指標値の偽装

ボットはエンゲージメントと視認能力に関する測定値すべてを偽装

White Ops は、Chartbeat と協力して、ボットと人間とのエンゲージメントの指標値を比較しました。

ボットの割合が高いサイトは、ボットの数は多くエンゲージメントも低い値。ボットの割合が低いサイトにおけるボットのエンゲージメントは、人間よりも上

ボットの割合が低いサイトでは、ボットの数は少なくても、そのエンゲージメントは高い値でした。こうしたサイトのボットは、ページでのエンゲージの時間が人間より 5% 長く、ページでのスクロールダウンは人間より 12% 少ない値でした。ボットの割合が高いサイトでは、ページでのエンゲージの時間は、人間の平均値と比べるとわずか 14% の長さでした。

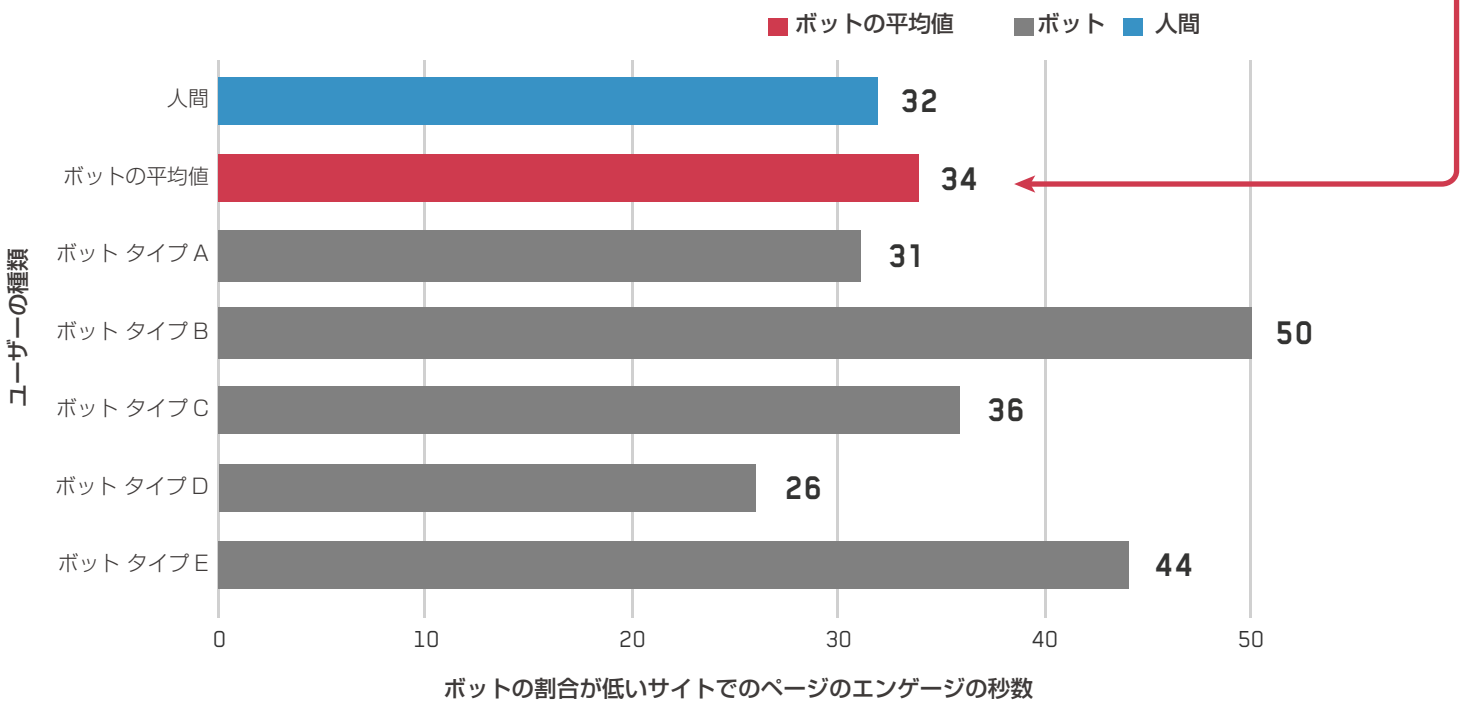
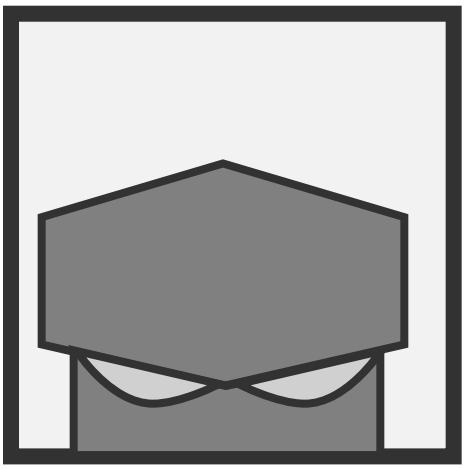


図 9：人間よりエンゲージメントが高いボット

Chartbeat 提供のエンゲージメント測定値を使用

ビューアビリティが確保されていても人間だとは限らない

ボットは Web ブラウザーを操作するように設計されています。ボットとブラウザーがメディアを消費するとき、実際には画面に表示していなくても、ブラウザーはこれを視認可能だと報告します。ボットにはこうした特性があることから、ボットのアクセスでは、広告のビューアビリティは基本的に高くなります。



主要 5 タイプのボットは、広告の消費量が人間より上

Chartbeat の協力のもと、人間の割合が高い 87 のサイトで、ボットと人間のビューアビリティを比較しました。

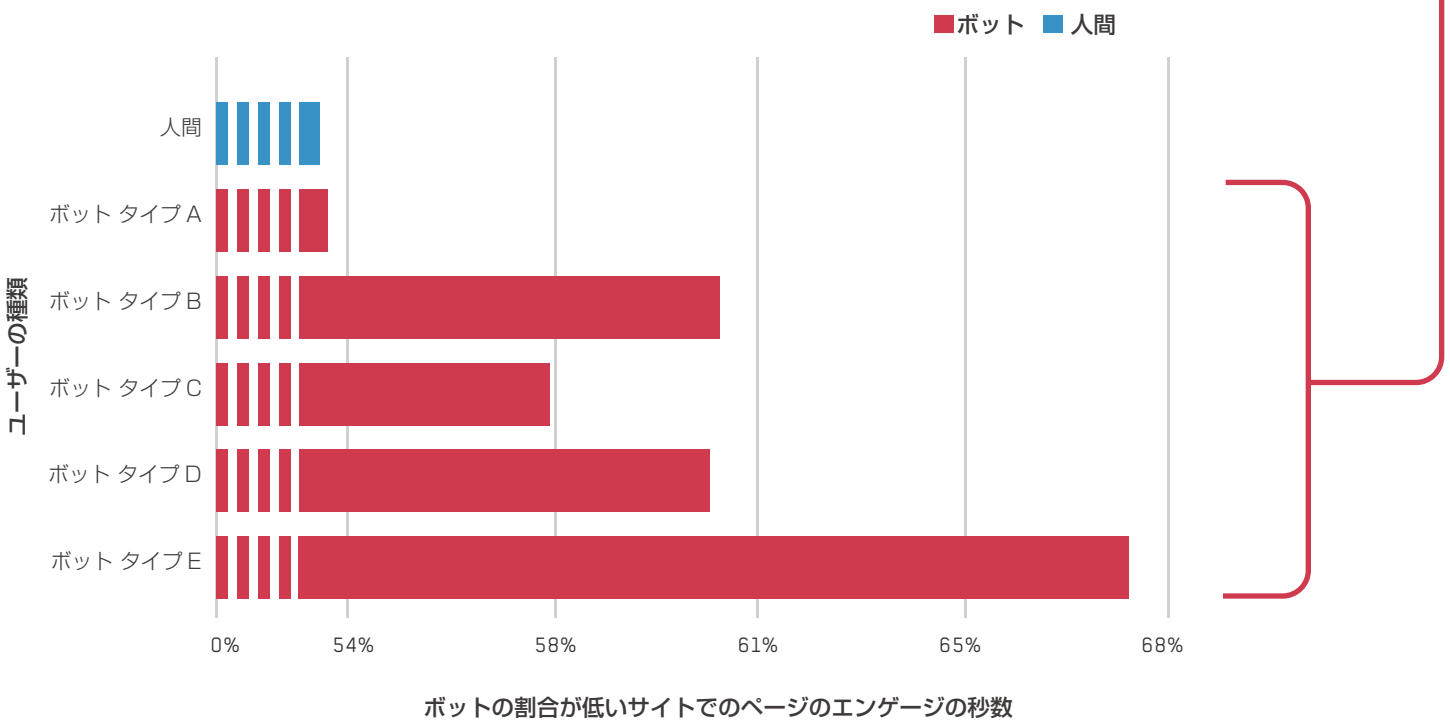


図 10：ボットのアクセスでは広告のビューアビリティは基本的に高い値を示す

Chartbeat 提供のビューアビリティの測定値を使用

ボットはターゲティングとリターゲティングの両方の対象に

一般に、ボットは人間よりも多くの Web サイトを訪れ、人間よりも多くの広告を消費します。しかし、あまりに度が過ぎる場合や、エンゲージメントの指標値に届かない場合は、ボットだとばれてしまいます。一方、広告主のターゲットとなる人間のエンゲージメントの指標値に合致したボットは、検出をまぬがれ、収益を増やすことができます。

今回の調査では、リターゲティング広告の 19% はボットが消費していました。リターゲティングとは、ユーザーがインターネット上で以前に取った行動に基づいて、特定のユーザーに広告を配信するプロセスのことです。

Web ブラウザーは、クッキーという形でトラッキングデータをエンコードしています。広告主やパブリッシャーが Web 上の訪問者を追跡したり覚えておいたりできるのは、クッキーのおかげです。ボットのブラウザーは、自らクッキーを生成したり、クッキーのプロフィールを作成したりします。より人間らしく見せるため、そして広告主にとって魅力的な存在となるためです。エンゲージメントの高い人間の行動を真似たボットは、価値の高いクッキーを持っており、広告主からターゲティングの対象となります。これによって、ボットネットの収益力が高まります。

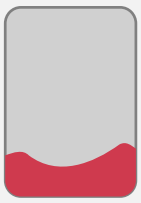
ボットが労せずしてクッキーを再利用することもできます。高度なボットネットの場合には、そのコンピューターを利用している人間の実際の行動によってブラウザーが生成したクッキーにボットが便乗することもあります。この場合、ボットがリターゲティングキャンペーンの対象として選ばれるのはさらに簡単です。

多くの場合、クッキーによってリターゲティングの対象となったボットは、消費者を細分化したセグメンテーションリストに追加されます。こうして、多数のアドテクノロジプラットフォームのオーディエンスモデルにボットが組み込まれるというサイクルが生まれます。

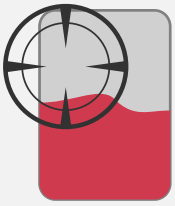
ケーススタディ

リターゲティングでのボットの割合は、全体での割合よりはるかに上

ある参加企業では、キャンペーン全体のトラフィックではボットの割合が 17% だったのに対し、リターゲティングキャンペーンでは 55% でした。

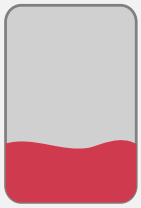


17%
ボット
ある参加企業のトラフィック全体

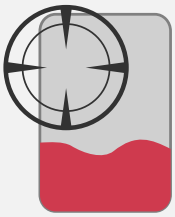


55%
ボット
ある参加企業のリターゲティングキャンペーン

別のある参加企業でも同様で、キャンペーン全体のトラフィックではボットの割合が 19% だったのに対し、リターゲティングキャンペーンでは 27% でした。



19%
ボット
ある参加企業のトラフィック全体



27%
ボット
ある参加企業のリターゲティングキャンペーン

プログラマティックインベントリは、信頼できる提供元から入手した場合でもボットトラフィックが混入

データ

知名度のあるプログラマティックアドサーバードメインを利用したときのボットの割合には大きな幅があり、ボットトラフィックのレベルを判断できる明確な特徴はありませんでした。調査に参加した 36 社のうち 18 社では、有名なプログラマティックアドエクスチェンジ 3 社を利用したプログラマティックトラフィックにおいて、ボットの割合が 90% 以上でした（右のケーススタディを参照）。

今回の調査では、プログラマティックプレースメントのボットの割合は平均 17% でした。

参加企業のプログラマティックのボットトラフィックの平均値は、3% ～ 31% と幅がありました。

アドバイス

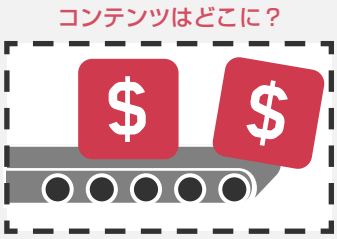
サプライヤーの評判や信頼度からは、ボットトラフィックの割合はわかりません。プログラマティックバイイングでボットを防ぐための対策には、次のようなものがあります。

ケーススタディ

参加企業の半数が DSP を通じてパブリッシャー 1 社に掲載した広告で、ボットトラフィックの割合が 90% 以上に

あるボットサイトが、DSP（デマンドサイドプラットフォーム）を通じたプログラマティックディスプレイトラフィックの発信元処理の不透明さを利用して、詐欺であることが広告主にわからないようにする体系的な隠蔽工作を行いました。

調査に参加した 36 社のうち 18 社では、それぞれの広告代理店が、信頼できる有名な DSP3 社を通じてインベントリを購入しました。ターゲットにした消費者のプロフィールやセグメントは、広告代理店ごとに別々です。これら 18 社の広告は、いずれも共通のパブリッシャーに掲載され、ボットの割合は一貫して 90% 以上でした。



プログラマティックエクスチェンジ

このサイトに広告を表示したことで、パブリッシャーに対する支払いが発生しましたが、それらは実際に人間が接した広告ではありません。このサイトは、広告主が出す費用を効率よく奪えるようにボット提供者がデザインしたもので、Web ページの高さいっぱいに、何段にもわたる広告を掲載していましたが、実際のコンテンツはありませんでした。

このサイトは、利用するボットネットのリソースを最小限に抑えながら、最大限の不正収入を得られるようにデザインされていました。

プログラマティックバイイングの監視とトラブルシューティングを継続的に行う

- 信頼できる提供元のものも含めて、すべての広告インベントリを監視する。
- トラフィックの監視を提供元自身が行うことを義務づける。
- ヒューマントラフィックの割合が一定の比率に達しないキャンペーンは、休止やトラブルシューティングを行う。

ボット提供者たちはいかにして調査を避けたのか

調査を回避したボット提供者

White Ops の見解としては、今回の調査で検出されたボットの割合は、実情より数字が低く出たものと考えています。調査の実施が公表され、事前に業界全体で広く認知されていたことによるものです。

トラフィックの監査や監視の予告を受けたときには、ボットのサプライチェーンに関与するすべての関係者が対処できます。朗報なのは、キャンペーンの監視という行為だけでも、ボットの活動をある程度抑えられることです。

ケーススタディ

公表された調査を回避するボットトラフィック

関係者に認知されていたことを受けて、我々は、9 月末までの期間を秘密の調査期間として、ボットの検出を継続して行いました。

ある参加企業の場合、8 月 2 日（公式発表した調査期間の 2 日目）の時点では、ボットの割合は全体で 41% でしたが、その 2 日後の 8 月 4 日には、4% まで激減しました。この企業では、公式に発表した調査期間である 8 月末までは、ボットの割合は低水準を維持していました。

しかし、9 月末まで秘密裏に調査を継続したところ、9 月 9 日には、この企業でのボットの割合は 38% まで戻り、公式な調査期間の平均をはるかに上回る水準を同月末まで維持しました。

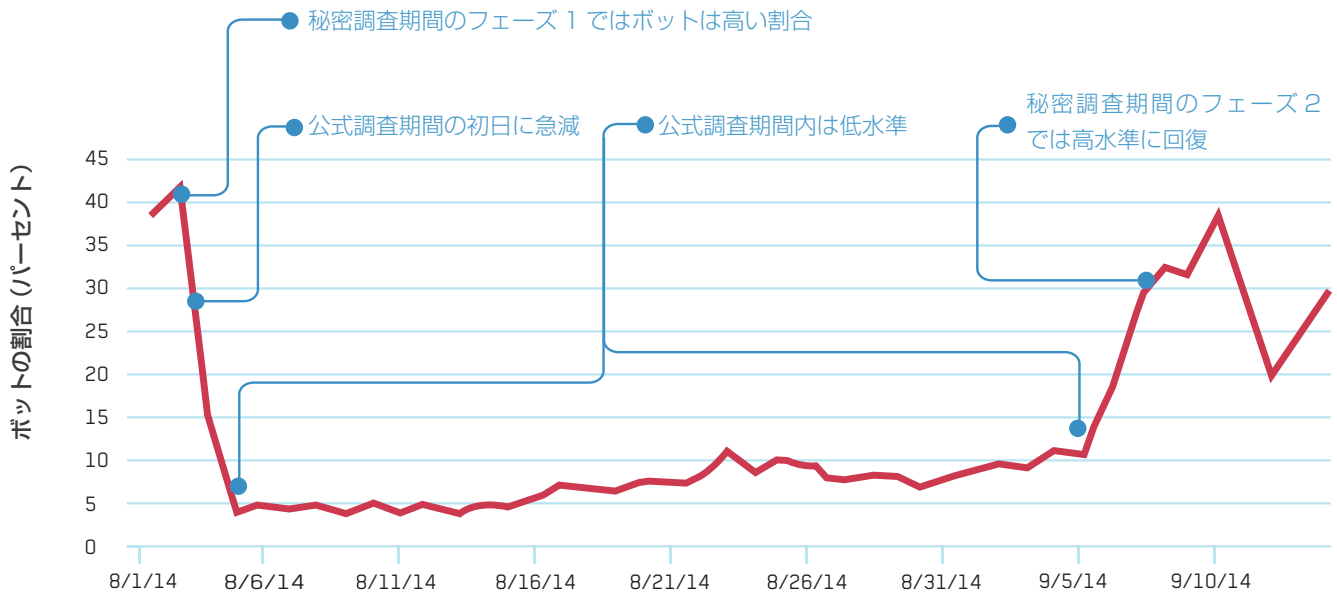


図 11：ある参加企業ではボットトラフィックが調査期間を回避

キャンペーン監視の期間中は ボットトラフィックの偽装が活発に

人間にインセンティブを与えて不正な広告インプレッションを生成する手法は、それ自体は広告費の大規模な損失にはつながらないのが普通です。ボットトラフィックとは違って、低コストで簡単に規模を拡大することができないからです。しかし、広告主が監査を実施している間に、ボット提供者がボットトラフィックのレベルを隠す目的で、こうした手法による偽のインプレッションを利用する事例も見られました。

ケーススタディ

ボット隠蔽の仕組み

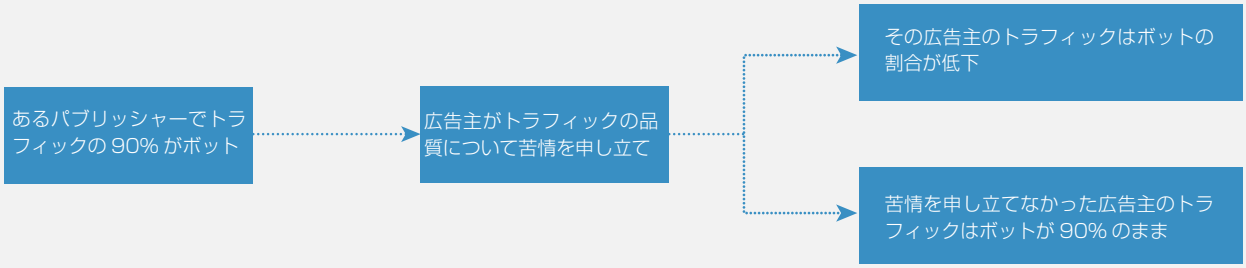


図 12：ボット業者は広告主による監査を積極的に回避

ボット提供者による隠蔽工作は、今回の調査とは別のキャンペーン監査の期間中にも見られました。キャンペーンの監視を始めた後で、ある広告主がトラフィックのサプライヤーに対し、そこからのトラフィックで検出されたボットの割合が 90% を超えていることを伝えました。その後は、このサプライヤーから当該の広告主へのトラフィックは、ボットの割合がわずか 4% に下がりました。

同じボット提供者が他のバイヤーに送り込んだトラフィックは、ボットの割合が 90% を超えた状態のままでした。今回の調査に参加したある企業もそんなバイヤーの 1 社です。同時に実施しているキャンペーン（有名な動画 SSP で広告代理店が購入したキャンペーン）において、同じボット提供者のトラフィックを利用したものがありました。

実際には、このサプライヤーから広告主へのトラフィックで詐欺の割合が本当に 4% に下がったわけではありません。このサプライヤーは、インセンティブを与えたトラフィック（人間に対価を支払って広告をクリックさせたヒューマントラフィック）を、ボットの割合が高いと伝えてきた広告主に回していたのです。

ボット提供者は、ボットトラフィックの割合が高いと伝えられた後で、監査を打破するための次のような対策を実施して、一見正当なトラフィックとなるようにしていました。

- 本物のヒューマントラフィックとボットとを自在に切り替える。
- トラフィックのボットの割合に関する苦情に応える。
- ボットと、インセンティブを与えたヒューマントラフィックの両方を、同水準のトラフィック量に維持する。

広告詐欺の抑止と検出のためには、広告主による公然 / 秘密裏の監視が必要

ボットを監視しているとボット提供者が認識しただけで、ボットトラフィックの割合が下がることがあります。広告主が購買のなかで、詐欺の排除について意識し、積極的に関与するだけでも、ボットの問題を多少は軽減できる可能性があります。

逆に言うと、ボットやボット詐欺のトラフィックパターンには、監視に応じて変化や回避が見られます。ボット業者は、本物のユーザーのなかにボットを紛れ込ませるために、あの手この手を尽くします。したがって、ボットか人間かという判断は、ボット検出技術がなくては不可能です。

金融や小売といった一部の業界が、失敗と大規模な損失の経験から学んだことがあります。監査や認証を定期的に実施するとしても、やはり継続的かつ高度なセキュリティ対策は必要だということです。

ボット業者を牽制し、偽装したボットを防ぐために、広告主に必要なことは、両面的な監視戦略の導入です。すなわち、公然と行う監視によってボット業者を牽制するとともに、秘密裏の監視によって、偽装したボットトラフィックを検出することです。

アドバイス

広告主がボット詐欺に打ち勝つためには、詐欺と戦う姿勢を対外的に打ち出すとともに、極秘の監視プログラムを続けていく必要があります。

公然の監視

- 外部のすべてのパートナーに向けて、詐欺対抗のポリシーを広く公表することによって、特定の犯罪集団や詐欺集団を一時的に抑止する。
- サプライチェーンのすべてのパートナーを対象として監査を実施する意向を表明する。

秘密裏の監視

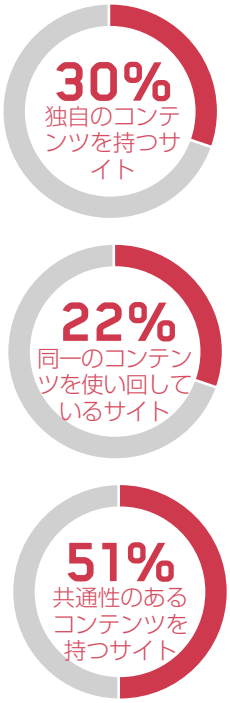
- ボット検出技術を利用して、メディアバイイングの中で、インセンティブを受けたヒューマントラフィック、ボットトラフィック、トラフィック誘導、アドウェアを暴く。
- 検出した詐欺への対処として、キャンペーンの一時休止とトラブルシューティングを行ったり、詐欺のレベルについてサプライヤーと話し合ったり、詐欺の抑止と排除に積極的なサプライヤーのトラフィックを優先的に扱ったりといった対応を行う。

ボットだけが
愛用するサイト

独創性のないボットトラフィックサイト

White Ops は、今回の調査でワーストランキングに入ったボットトラフィックサイトの内容を確認しました。ワースト 50 のサイトのうち、独自のコンテンツを持つサイトは 30%、1 つのサイト内で同じコンテンツを使い回しているサイトは 22%、共通性のあるコンテンツを持つサイト（まったく同じではないが、非常によく似たコンテンツを複数のページで表示するサイト）は 51% でした。

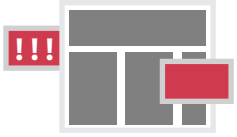
ボットサイトはコンテンツをコピー＆ペーストしている。ボットトラフィックサイトのワースト 50 での内訳：



ボットトラフィックサイトは以下の種類の広告を 6 種類以上表示：


動画の自動再生


音声の自動再生



ポップアップ／ポップアンダー

ボットトラフィックサイトは多数の広告を掲載

ボットトラフィックサイトが掲載している広告は、1 ページあたり平均 6 個でした。これに対し、Alexa のランキングで上位のサイトは、広告が平均 2 個でした。ボットトラフィックサイトの多くでは、動画の自動再生、音声の自動再生、ポップアップ、ポップアンダーのいずれかの要素が見られましたが、Alexa のランキングのトップ 50 で広告表示のあるサイトでは、これらの要素はまったく見られませんでした。

ボット提供者はユーザーを監視

ボット業者は、ボットネットやボットサイトから最大限の収益を上げるために、トラフィックを入念に測定しています。White Ops は、タグ、ピクセル、ビーコンなどのサードパーティトラッカーについて、ワーストランキングのボットトラフィックサイトと、Alexa のランキングのトップ 50 で広告表示のあるサイトとで、こうしたトラッカーが使用されている数を比較しました。

ワーストランキングのボットトラフィックサイトは使用するトラッカーが 4 倍

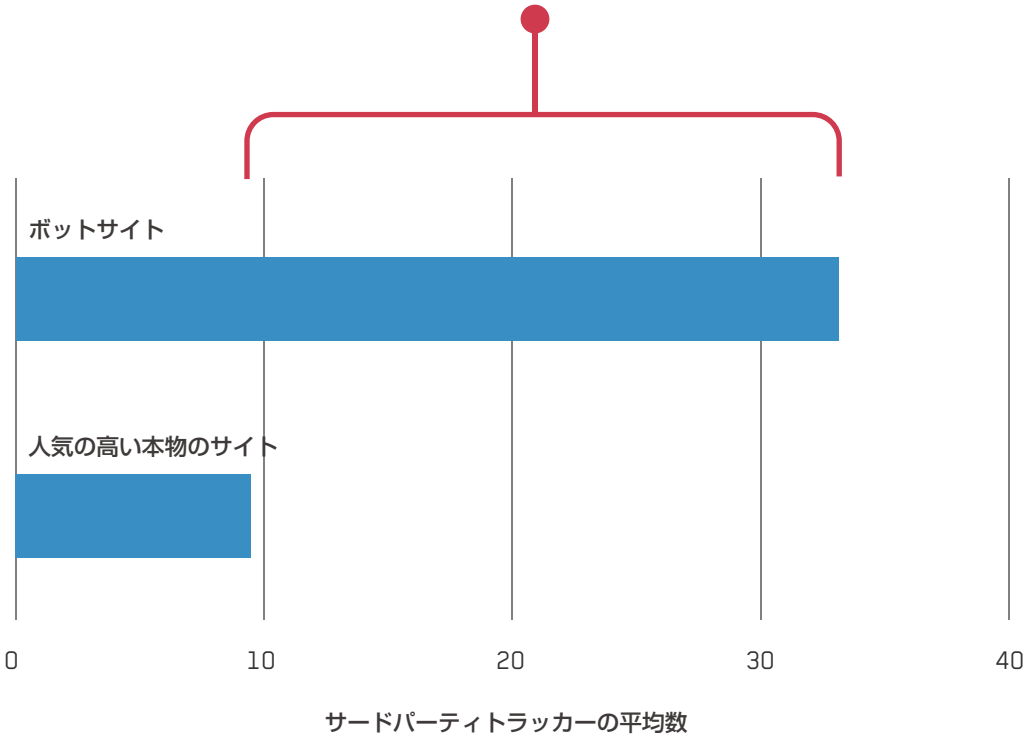


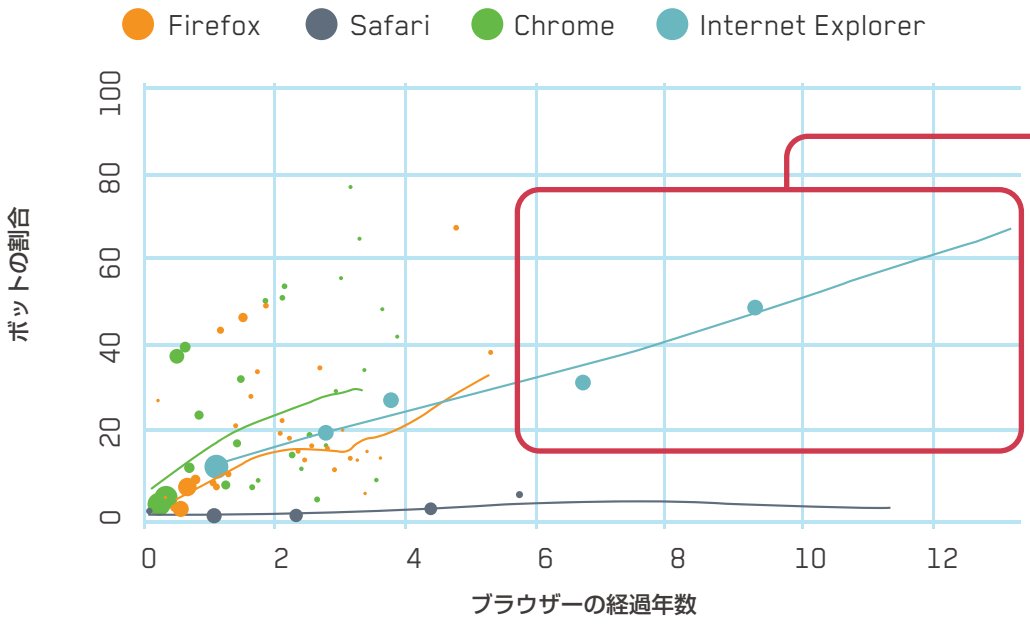
図 13：ボットサイトは収益拡大のためにトラフィックを測定

Ghostery 提供のトラッカー測定値を使用

旧式のブラウザーの方がボットは多い

旧式のブラウザーではボットの割合が上昇。
古いブラウザーに対応したサイト構築は、費用対効果の面で、もはや不合理か。

新バージョンのブラウザーで攻撃を遂行するためには、ボット業者は、それぞれの新規リリースごとに、展開、コンパイル、テストをやり直すことが必要になります。最新のブラウザー向けにメディアを最適化し、旧式のブラウザーでのインプレッションを抑えるようにすれば、ボットの防御に関して、業界全体で時間的なメリットが得られる可能性があります。



データ

IE 6 でのインプレッションの半数以上（58%）、IE 7 でのインプレッションの半数弱（46%）は、ボットによるものでした。

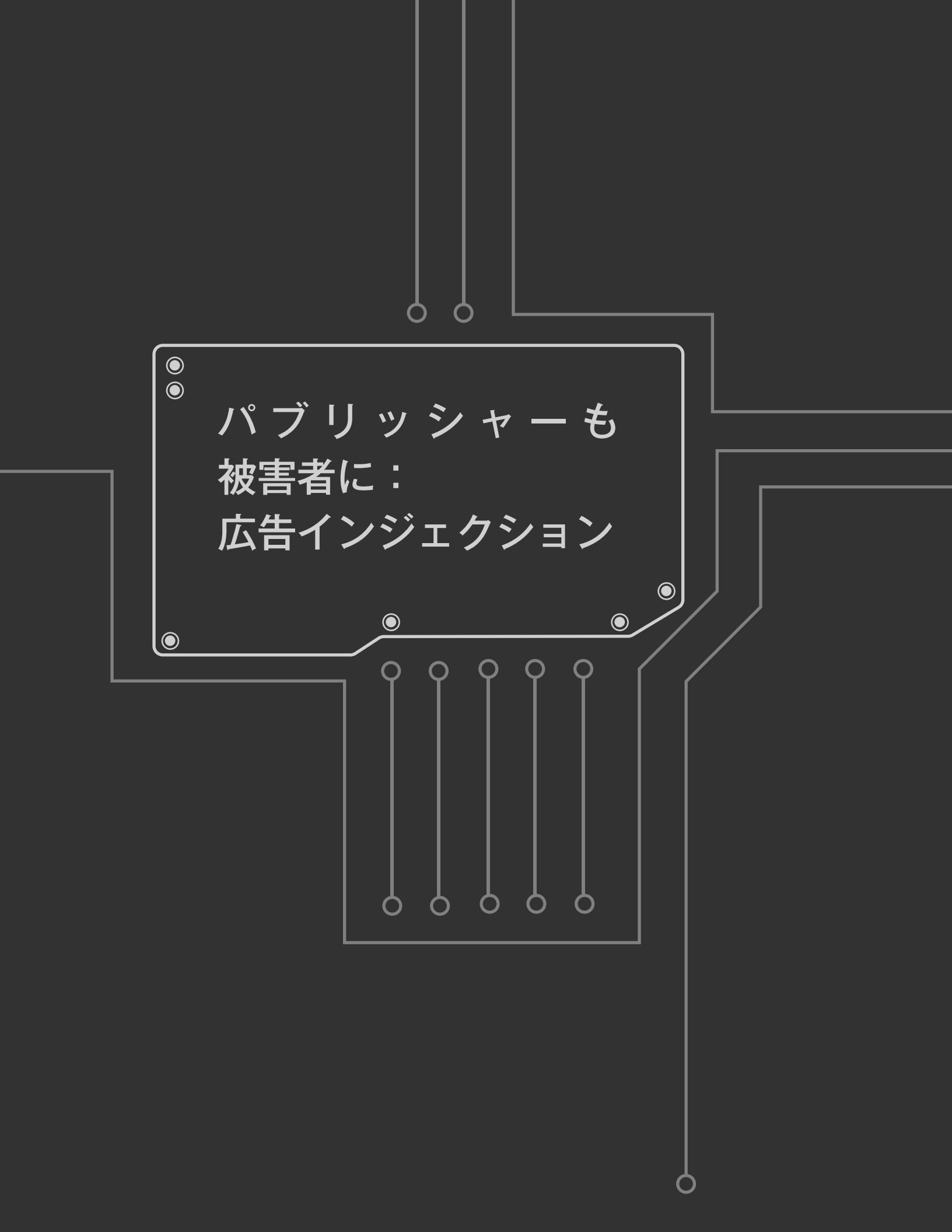
図 14：ボットは今でも IE 6 と IE 7 を利用

アドバイス

ボットのブラウザーは、人間のユーザーが広く利用しているブラウザーのようには自動更新されていないのが一般的です。メディアバイイングで、比較的新しいブラウザーをターゲットにすれば、ボットのダウンタイムとコストを高めることができ、業界がボットへの防御で先手を打つことができます。

新しいブラウザーをサポートする

- 旧式のバージョンより新しいバージョンを優先する。
- どのバージョンのブラウザーで人間よりボットの方が多いかを把握する。
- 人間のオーディエンスがあまり多くない旧式のブラウザーのサポートを縮小して、開発コストを抑える。


パブリッシャーも
被害者に：
広告インジェクション

広告インジェクションは、ユーザーとパブリッシャーを犠牲にして広告主の費用を巻き上げる

広告インジェクションの攻撃で使われる手口は、オンラインバンキングを狙ったサイバー犯罪の手口と同じです。挿入された広告インベントリに対する支払いとインプレッションデータは、広告が表示されたサイトとは縁もゆかりもないサードパーティに流れ込みます。広告を挿入するボットネットのコントローラーは、自前で構築や保守を行っているわけではないコンテンツとブランドを使って、莫大な収益を上げることができます。

広告インジェクション

パブリッシャー、広告主、ユーザーに対する MITB（Man-in-the-Browser）攻撃の一種で、Web サイト上に広告を強制的に表示する。Web ページの元々のコンテンツを置き換えたり、既存のコンテンツや広告を覆い隠したりする形で表示するものが多い。

トゥルードメイン

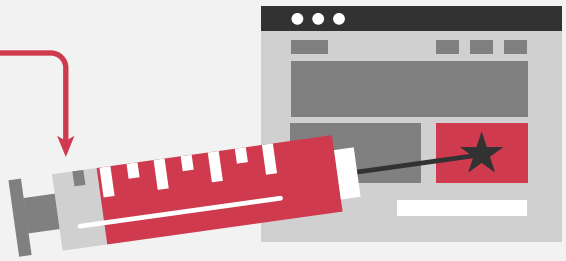
広告が表示された実際のドメインを識別する技術。アドサーバーが報告するドメインは偽装できる可能性があるが、そのドメインではなく実際のドメインがわかる。

今回の調査では、広告インジェクションの検出をもともと目指していたわけではありません。しかし、White Ops のトゥルードメイン検出技術を利用した結果、広告インジェクションの大きな証拠を見つけ出すことができました。ユーザーの寄付やサブスクリプション型により運営されていて、広告の掲載を認めていない有名なサイトのいくつかで、広告が表示されていたというものです。挿入された広告は、パブリッシャーが承認したものではなく、一般家庭のコンピューターに不正にインストールされたマルウェアによって（そのブラウザー上でだけ）表示されていました。

マルウェアによる広告インジェクションの被害者は、知らないうちに自らの個人情報を外部にさらすことになります。悪意を持つであろう何者かが、被害者のコンピューターに入り込んだ広告インジェクションのソフトウェアを通じて、閲覧履歴、興味、金融情報などの PII（個人識別可能情報）にアクセスできます。

ケーススタディ

1 日に 50 万個以上の広告を挿入されたパブリッシャー



調査終了後の分析によると、あるパブリッシャーは、調査期間全体にわたって、1 日あたり 50 万個以上の広告を挿入される被害に遭っていました。

広告インジェクションによってインターネットの質が低下

サイトに広告を挿入することは、広告主やパブリッシャーの意向によるものではありません。広告インジェクションのマルウェアの所有者が、メディアにおいて勝手に広告を掲載し広告料の支払いを受け取ります。この結果、広告主とパブリッシャーの双方の評判が損なわれたり、広告主がデジタル広告インベントリ向け予算を使い果たしたりする可能性があります。

広告インジェクションによって、そのサイトが正規に掲載している広告の価値もすべて下がります。

広告インジェクションを防ぐために、広告主とパブリッシャーが取ることのできる策としては、トラフィック誘導の利用を制限する、トラフィック誘導を継続的に監視する、挿入された広告がトラフィックに含まれていないことをサプライヤー（DSP を含む）が実証するよう義務づける、といったものがあります。

広告インジェクションによって低下するユーザーのブラウジングエクスペリエンス：

- 広告を挿入された Web サイトは読み込みに時間がかかる。
- ページ内の広告が多すぎるとユーザーは威圧感を感じる。
- 挿入される広告は、非常に押し付けがましくて目ざわりなものが多く、表示先の Web サイトが本来意図していた機能が損なわれる可能性がある。

広告インジェクションによって本来の広告インベントリが台無しに

ボット詐欺の撲滅に向けて：行動の呼びかけ

ボットネット運営者はすでに、一部の対抗策への回避策をもっている

ボット対策に有効だと広告代理店やアドテクノロジプラットフォーム側が現時点で考えているいくつかの戦術は、すでにほとんど無意味となっています。

アドベリフィケーションなどのビューアビリティを確認する技術的対策を講じても、人間かどうかは確実にはわかりません。ビューアビリティを偽装するように改良されたボットは少なくないからだ。実際に、ボットインシデントでは、非ビューアブルなインプレッションに比べ、ビューアブルなインプレッションが若干高い値に出ています。

- ブラックリストは、リアルタイムに近い更新が必要であり、ボットだけでなく、実際の人間のオーディエンスも膨大にブロックしてしまうことも多くあります。詐欺犯側の対応は、すばやいものなのです。
- 高度なエンゲージメント指標やアトリビューションモデルを用いてキャンペーンを最適化しても、ボットトラフィックを排除することはできませんでした。ボットは実在する人間になりすまし（実際の人間が行った購入だと判断されるようにし）、エンゲージメントを偽装するからです。
- トラフィック誘導（トラフィックソーシング）が広く行われていることから、購買先をプレミアムパブリッシャーのみに厳しく限定しても、ボットトラフィックは排除できませんでした。

誰が得しているのか？

ボットインプレッションによって、実際よりも多くの人が広告を目にしているかのように偽装されるため、市場全体が歪んでしまっています。多種多様かつ無限な広告インベントリの供給という幻想によって、本物のヒューマンインプレッションの価格は下がっています。この結果、誠実に事業を進めている企業が、競争で非常に大きな不利を被っており、トラフィック誘導へのプレッシャーも高まっています。

動機や誘因は、エコシステムの各部分で大きく異なっています。

- ボットネット運営者の狙い —— 詐欺のサプライチェーンの終端にあたる現金化ポイントを通じて金を手に入れること。
- アグリゲーターと中間業者の狙い —— リーチを拡大し、販売するインベントリに事欠かないようにすることと、考え得る限りのオーディエンスセグメントに対応できるよう、ボットのプロフィールを多種多様にすること。
- パブリッシャーの狙い —— 見かけ上のオーディエンスの規模を拡大させ、トラフィック獲得コストと、広告主から得る売上との差を利益として懐に入れること。

恐れが暗黙の障壁に

このレポートが扱っているエコシステムは複雑です。現在の広告詐欺には、勝者と敗者が存在します。そして、この勝負には明らかに不当な偏向が見られます。

勝者の側は何十億ドルという稼ぎを上げています。その多くは、ボットを提供する側の者によるサイバー犯罪活動の資金にもなっており、ボット提供側が行動を改める理由はありません。一方、デジタル広告をめぐる争いで大きく負けがこんでいるのは、適切な顧客に向けて優れた製品を提供したいと考えている広告主であり、自らのメディアプランで的確なターゲットへのリーチを実現したいと考えている広告代理店であり、関連性の高い広告によってサイト上のコンテンツを支えたいと考えているパブリッシャーであり、オンライン広告のための先進的なインフラとマーケットプレイスを提供したいと考えているアドテクノロジコミュニティです。

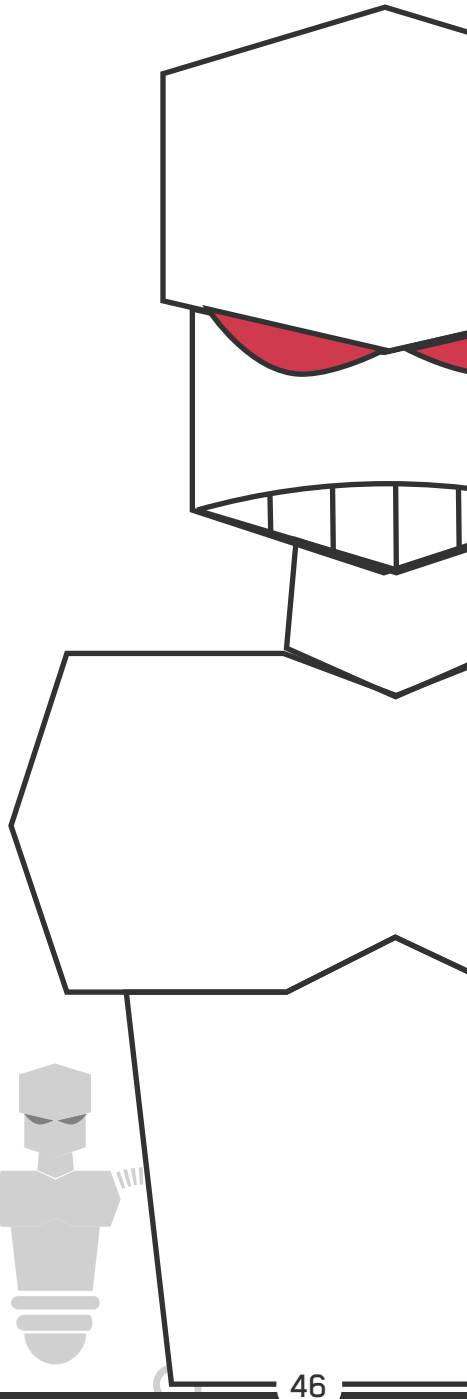
また、消費者も大きく負けている側です。デジタル広告業界が存在するのは、消費者がいるからこそです。そしてその消費者は、ボットネットの巨大なネットワークに、知らないうちに共犯者として巻き込まれているのです。

詐欺という問題に対してよくある反応は「恐れ」です。恐れは逃げの姿勢につながり、それこそが詐欺グループの求めるものです。**無自覚、悪徳、杜撰といった印象を強く与え、この種の活動を許してしまうのは、誰にとっても望ましいことではありません。**

詐欺はどこにでも存在するというのが真相です。その影響を受けない人はいません。社員やパートナーをその恐れから解放しないことには、この問題に効果的に対処するために必要な協力を得ることはできません。

ボット詐欺は、新たな種類の攻撃です。広告主、広告代理店、パブリッシャーは、ここ数年で明らかになってきたボット詐欺の脅威を理解するために、新しい概念を学び役立てる必要があります。広告主をはじめ、業界のすべての関係者にとって、行動を起こすことは可能であり、また必須です。

単独でできる行動もあれば、詐欺検出のパートナーとの協力が必要なものもあります。以下のページでは、業界内の利害関係者に向けて、デジタル広告の詐欺と戦うための行動計画を示していきます。



すべての広告関係者の行動計画

ボット詐欺との戦いでは、敵ではなく味方を作る

ボット詐欺は、広告主に達するまでの間に、デジタル広告のサプライチェーンの多数のサプライヤーに影響を及ぼします。広告主、広告代理店、サプライヤーが一丸となって、サプライチェーンでのボット詐欺の抑止と撲滅に取り組むことが必要です。ボット詐欺を大きく減らすために、業界のキープレーヤーが共同作戦と単独作戦の両方を展開するよう、我々は呼びかけます。

広告詐欺の話し合いでは感情論は排除する

自社のキャンペーンでボット詐欺が見つかったからといって、広告代理店やパブリッシャーが無能である・悪であると決めてかかってはいけません。自社にメディアを売った企業も、ボットネット運営者の被害に遭った側である可能性は大いにあり、悪徳だとは限らないという点を忘れないでください。

サードパーティトラフィックの検証テクノロジ利用を承認・許可する

今回の調査は、参加企業のすべてのプレースメントを対象として実施したわけではありません。その理由の 1 つは、広告代理店とパブリッシャーのポリシーにあります。広告代理店やパブリッシャーによっては、一部のプレースメントで監視ソフトウェアの利用を認めていない所があるからです（55 ページの「付録 B：制約・制限事項」を参照）。

広告主がメディアバイイングにおいてボットとの戦いを効果的に進めるためには、監視ツールを導入できなくてはなりません。パブリッシャーと広告代理店は、こうした監視ツールの導入を実現する必要があります。広告枠を購入する広告主がボット検出ソフトウェアやドメイン検出ソフトウェアを導入できるようなポリシーと手順を定めてください。

TAG（Trustworthy Accountability Group）をサポートする

IAB、4A's、全米広告主協会は 2014 年 11 月初め、マーケティング / メディア業界の共同プログラムとして、TAG（Trustworthy Accountability Group）の設立を発表しました。デジタル広告詐欺、マルウェア、広告に支えられた海賊行為など、デジタルコミュニケーションのサプライチェーンにおける不正の撲滅を目指すための取り組みです。TAG の品質保証ガイドラインは、すべてのベンダーが遵守する必要があります。

ボットトラフィックに対する行動と併せて、ボットについての効果的なコミュニケーションが必要

社内で、ボット詐欺の問題が正確に伝わるような表現を使う。

メディアバイイングについて社内外で話し合うときに、ボット詐欺に関する議論の時間を必ず設ける。

同盟関係を維持し、詐欺に対抗するアライアンスを構築しながら、脅威や真の敵を正確に特定できるような用語を取り入れ、利用する。

広告主（バイヤー）の行動計画

問題を認識し、積極的な姿勢をとる

広告主は、デジタル広告詐欺を認識することと、問題への対処に向けて、行動と発言の両方で積極的な姿勢をとることが欠かせません。詐欺の悪影響は、デジタルコミュニケーションのサプライチェーンのすべての関係者に及びます。特に、広告主への影響は深刻です。

したがって、プラスの変化をもたらすために、広告主には積極的な役割が求められます。

トラフィック誘導に透明性を要求する

トラフィック誘導とボットの割合の高さには、強い相関関係があります。トラフィック誘導に関しては、バイヤーがパブリッシャーに透明性を要求することをお勧めします。また、サードパーティから得るトラフィックについて、その取得元すべてをパブリッシャーが特定することを要件として定める文言を、RFP や IO に盛り込んでおくこともお勧めします。さらに、バイヤーとしては、トラフィック誘導を拒否し、パブリッシャーのオーガニックサイトトラフィックのみで広告を運用するという選択肢も持っておく必要があります。

非ヒューマントラフィックに関する文言を契約条項に加える

この調査レポートで取り上げた問題に対処するための具体的な文言を契約条項に加えることを検討してください。付録では、詐欺的なトラフィックの定義、および広告主とメディア企業との交渉のたたき台となる保護条項の一例を紹介しています（全米広告主協会の外部法務顧問である Reed Smith が作成）。各社の個別の利益に最もかなう条項の具体的な内容については、顧問弁護士に相談してください（57 ページの「付録 D：契約条項の例」を参照）。

サードパーティのツールを使って監視する

すべてのトラフィックを一貫したツールで監視してください。比較できるということがきわめて重要です。月 1 回や 3 か月に 1 回といった監視や、特定のチャネルのみの監視など、対象を限定した監視では、ボットサプライヤーがこれを回避するための策を講じようとします。サードパーティによる監視では、パブリッシャーの質や、アドテクノロジ企業のトラフィックの質について、想定の正しさや間違いを検証できます。広告への投資から最大限の価値を引き出すために、継続的な監視をお勧めします。

監視とボット検出を利用して、リターゲティングキャンペーンやオーディエンスの指標でボットの存在を明らかにすれば、こうしたボットをターゲットとしたメディアの追加購入を回避でき、キャンペーンの指標を向上できます。

広告主（バイヤー）の行動計画（続き）

可能であれば時間帯制限出稿を利用する

午前 0 時から 7 時の間は、トラフィックに占めるボット詐欺の割合が高まります。オーディエンスの人間が起きている時間に広告を集中させれば、ボットの数を抑えることができます。

ブラックリストは限定的にして、頻繁に更新する

ブロックの仕方には要注意です。ブラックリストが効果を発揮するためには、少なくとも 1 日 1 回は更新すること、対象を絞り込むこと（マイクロブラックリスト）、他の防御策と組み合わせることが必要です。

広告インジェクションを抑制する

広告インジェクション（本来は無関係なサイトに広告を許可なく表示すること）の手法を使われると、プログラマティックバイイングに高水準の詐欺が含まれることになります。広告インジェクションを抑制する方法について、DSP やアドテクノロジプラットフォームと話し合ってください。

旧式ブラウザーのインプレッション購入を減らすことを検討する

IE 6（2001 年リリース）や IE 7（2007 年リリース）を今でも使用している本物の人間は少なく、これらのブラウザーからのインプレッションの多くはボットによるものです。このような旧式ブラウザーのインプレッション購入を減らすことを検討してください。

外部の全パートナーに対し、詐欺対抗のポリシーを公表する

秘密裏の継続的な監視と併せて、明確なポリシーを示すようにします。番犬効果によって、行動の変革、詐欺の減少、周囲との共闘を促すことができます。

セキュリティに対して予算を確保する

セキュリティに対する一般的なコストは、多くの業界で 1% ～ 3% の間接費として予算化されています。クレジットカードのエコシステムでは、こうしたセキュリティ支出によって、詐欺による損失が 100 ドルあたりわずか 8 セントまで減りました。広告のボット詐欺が仮にそのレベルまで下がれば、その達成にかかったセキュリティ支出の何倍ものリターンを得られる可能性があります。

パブリッシャーの行動計画

トラフィック誘導を継続的に監視する

トラフィック誘導を常に監視してください。トラフィックの誘導元を把握し、トラフィック誘導についての透明性を維持してください。

ボットの割合が高いことが判明している誘導元は排除してください。すべてのベンダーを常時監視してください。

コンテンツの盗用や広告インジェクションに対する自衛策を施す

ドメイン検出やボット検出のサービスを利用して、コンテンツスクレイピング（他の Web サイトのコンテンツを自らのサイトに掲載し、そのコンテンツに広告を付けることで収入を得る行為）や広告インジェクションの徴候がないかどうか監視してください。ボット検出サービスを導入すると、ボットの割合が高いトラフィックでもボットの実際の数を測定できるため、ボットを広告費請求のプロセスから排除して、人間のオーディエンスのみを請求対象とすることができます。

サードパーティのトラフィック監視ツールの使用を認める

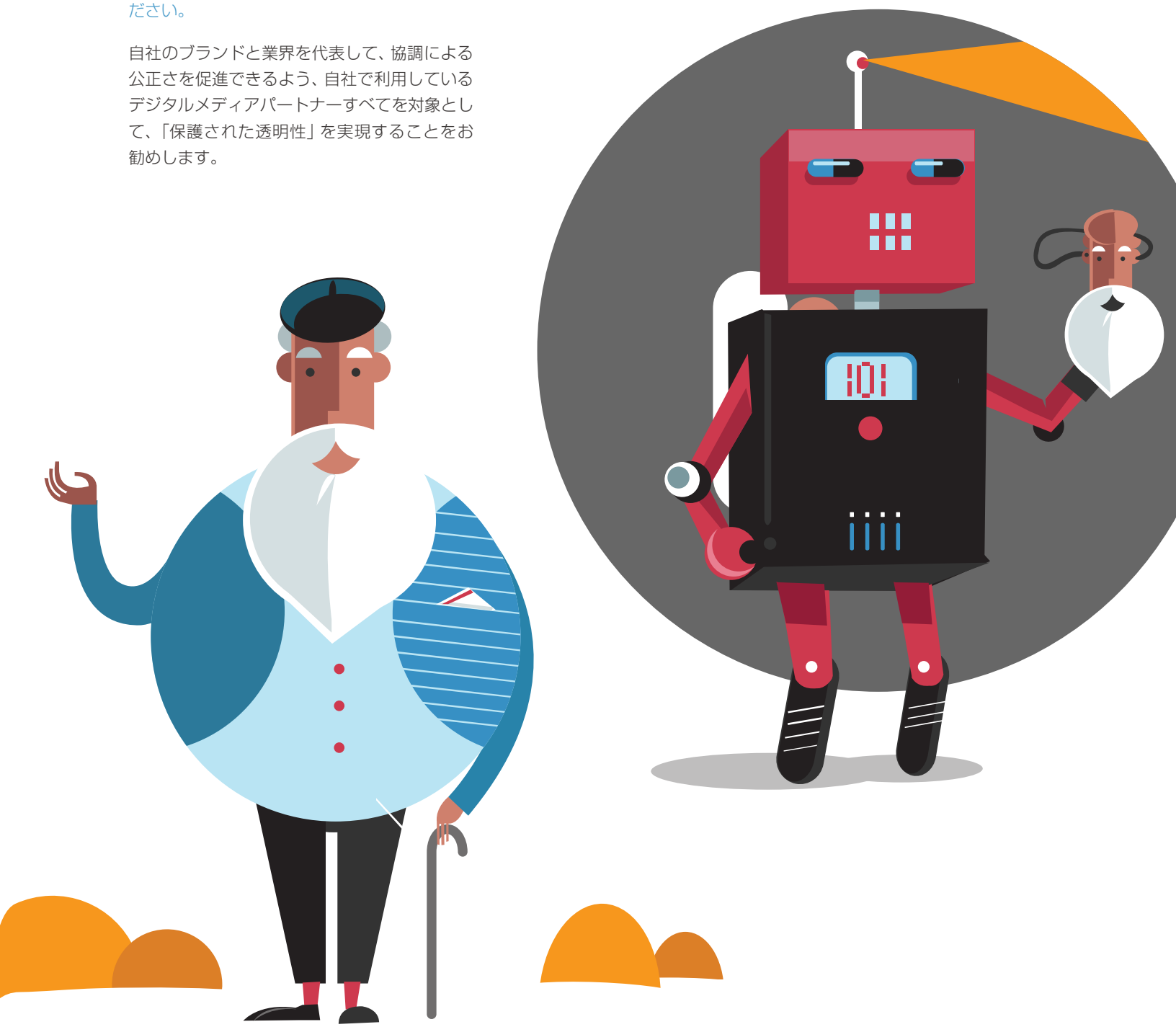
サードパーティの監視ツール（ビューアビリティ、エンゲージメント、ボット検出などの監視）やサードパーティのトラッカー測定ツールを広告主に使ってもらい、広告主がトラフィックパフォーマンスをきめ細かく把握できるようにすることも 1 つの手段です。

オーディエンスの**真の姿**は：

人間？ or ボット？

詐欺を撲滅するために、ぜひ行動を起こしてください。

自社のブランドと業界を代表して、協調による公正さを促進できるよう、自社で利用しているデジタルメディアパートナーすべてを対象として、「保護された透明性」を実現することをお勧めします。



付録 A

用語集

DSP（デマンドサイドプラットフォーム）
広告主またはその広告代理店が利用するプラットフォーム。複数のエクスチェンジのアカウントを束ねて管理し、それらにまたがった入札が可能。

HREF ドメイン
個々のインプレッション、ページビュー、その他のオンラインイベントが発生した場所を表すドメインのフルパス。広告配信に関するレポートに含まれていることが多い。

IP（IP アドレス）
インターネットに接続された特定のデバイスまたは複数のデバイスに紐付けられた一意の数値。

IP アドレスのブラックリスト化
悪質であることがわかっている IP アドレスのリストを利用して、その IP アドレスへの広告配信を回避すること。

IP ジオロケーション
インターネットにつながったデバイスが特定の時刻にどこにいたかというおおまかな場所を、デバイスの IP アドレスに関する情報、または IP アドレスから推定可能な情報を利用して判断すること。

MITB（Man-in-the-Browser）攻撃
インターネットで見られる攻撃の種類の 1 つ。ブラウザーやアプリケーションのセキュリティの脆弱性を突いて、ユーザーのオンラインでの通信に不正な操作を加え、広告、Web ページ、トランザクションのコンテンツを改変したり、別の広告、コンテンツ、トランザクションを挿入したりするもの。ユーザー本人や、ユーザーが操作しようとしたリソース側はこのことを知らず、同意もしていない。

RON（Run Of Network）
膨大な Web サイトに表示される広告またはキャンペーン。ターゲットとなるサイト、プレースメント、ドメインを個別に選択できない。

SSP（サプライサイドプラットフォーム）
パブリッシャーが利用するテクノロジプラットフォーム。広告インベントリを管理し、オンライン広告からの収益を最大化するために利用する。通常は、アドエクスチェンジとの間でやりとりを行い、自らの広告プレースメントのインベントリを、多数の購入候補者に向けて自動処理で販売できる。

アドウェア
目に見える形または見えない形でユーザーに広告を表示し、広告の消費を促すソフトウェア。多くの場合、ユーザーのデバイスに自動でインストールされる。

インセンティブによるヒューマンインプレッション
報酬やその他のインセンティブを受け取っている人間に対するインプレッション。

インプレッション
個別のオンライン広告の 1 回 1 回の配信のこと。オンライン広告の基本的な経済単位。一般には、広告主または広告代理店への課金に利用できるようにアドサーバーが記録している。

エクスチェンジ
パブリッシャー自体や、パブリッシャーどうしを束ねたネットワークなど、複数の提供元との間で、広告や関連データの売買を円滑に進めることができるテクノロジプラットフォーム。

エンゲージメント
所定の広告または Web ページに対するユーザーのインタラクションを質的に評価した指標値。きわめて明確かつ具体的に定義されているものが多い。

キャンペーン
共通のアイデアやテーマがあり、広告主の声を代弁する一連の広告。種類が異なる複数の広告で構成したり、複数のパブリッシャー、サイト、チャネルで展開したり、複数のフォーマットで展開したりといった場合もある。

キャンペーン監視
各種の広告とそのフォーマット、およびそれらを表示するパブリッシャー / サイト / チャネルを監視すること。さまざまなレベルの広告詐欺を検出することを目的とし、支出を最適化して広告詐欺を抑制できる。

クリックファーム
広告詐欺の一種で、1 か所または複数の場所にいる大勢の人に対し、きわめて少額の報酬やその他のインセンティブを与えて、広告の閲覧やクリックを行わせること。こうして不正に広告を消費させることにより、元締めのサードパーティが利潤を得ることができる。

付録 A

用語集（続き）

現金化サイト
広告を配信できる Web サイト、アプリ、その他のリソースのうち、オンライン広告のエコシステムから金を奪い取ることを目的として、広告詐欺の実行者が運営しているもの。

広告
あらゆる種類のオンライン広告。

広告インジェクション
アプリ、Web ページ、各種オンラインリソースに対し、そのリソースのパブリッシャーまたは運営者の同意を得ないままで、目に見える形または見えない形で広告を挿入すること。

広告詐欺
レポートや請求、およびその他の分析の中に、実際の人間が何らかのデバイスを普通に使用するなかで広告に接触したものとは異なるものが含まれること。

広告主
費用を支払って広告を出す企業、ブランド、個人のこと。広告主は、広告を表示するサードパーティ、または広告表示の代理店となるサードパーティに対して費用を支払う。

サイト、Web サイト
互いに関連する Web ページをひとまとまりにしたもの。単一のドメインで提供されることが多い。

サプライヤー
パブリッシャーやサイトにトラフィックを販売する業者。

自動再生
ユーザーが Web ページやその他のリソースを読み込んだときに、音や動画などの各種メディアをユーザーの操作なしで再生すること。通常こうしたメディアは広告の一部となっている。

トゥルードメイン
広告の実際の運用先のドメイン。ドメイン検出により判定される。

トラフィック
サイトやページなど、個別のオンラインリソースの閲覧のこと。また、個別の広告に関するインプレッションのこと。

トラフィック誘導
パブリッシャーがサードパーティを通じて閲覧者を増やす手法のこと。

ドメイン
Web サイトなどのインターネットリソースを一意に識別する名前。そのリソースにアクセスするときに利用できる。

ドメイン検出
アドサーバーのレポートで示されるドメインではなく、広告が実際に表示されたドメインを特定すること。

ドメインのブラックリスト化
悪質であることがわかっているドメインのリストを利用して、そのドメインへの広告配信を回避すること。

判定
個々のインプレッション、ページビュー、その他のオンラインイベントが、正当なものなのか、それとも広告詐欺によるものかを、証拠に基づいて確定的に識別すること。

パブリッシャー
単一の Web サイト、または複数の Web サイトで構成されるネットワークの運営者。それらのサイトのコンテンツの制作者や監督者でもある。オンライン広告枠やインプレッションの販売元となるが、サードパーティのトラフィックを購入することも多い。

ヒューマンインプレッション
実際の人間に向けて正当に配信され、意図的または無作為のいかなる広告詐欺にも関係していないインプレッション。

ヒューマントラフィック
Web サイトなどのオンライントラフィックや広告消費のうち、実際の人間が行った正規のもの。

ファントム（幽霊）レイヤー
広告詐欺のロンダリングのためだけに運営されている Web サイト。オンライン広告のエコシステムに投入されるインベントリとインプレッションの出所がわかりにくいようになっている。

付録 A

用語集（続き）

ブローカー
サードパーティの中間業者。サプライヤーからトラフィックを購入し、パブリッシャーに販売する。メディアエージェンシー、リターゲティングプラットフォーム、トラフィックエクステンションプラットフォームであることが多い。

ページビュー
Web サイトの中の 1 つのページを読み込む 1 回のリクエスト。

ボット
テキスト、動画、画像、音声、各種データなどのデジタルコンテンツを自動処理で消費できるエンティティ。広告の表示、動画の閲覧、ラジオ広告の聴取、視認能力の偽装、広告のクリックなどを、意図的または無作為に行う場合がある。NHT（Non-Human Traffic：人間ではないトラフィック）ともいう。

ボットインプレッション
ボットが消費したインプレッションのこと。

ボット検出
ボットトラフィックやボットインプレッションを検出し、ヒューマントラフィックやヒューマンインプレッションと区別すること。

ボット詐欺
広告詐欺のなかでも、特にボットが行ったもの。

ボットトラフィック
ボットの挙動または影響によって自動で生成された Web サイトのトラフィックや各種オンライントラフィック、または広告の消費。

ボットネット
感染したコンピューターをグループ化したもの。自動処理によるイベントを Web 上で引き起こす。さまざまな種類のボットの作成で使用されるインフラ。

ボットの割合
オンライン広告のトラフィックの所定の部分のうち、ボットが消費した分の割合。

ボットプリント
所定のインプレッション、ページビュー、Web 上のその他のイベントの中で直接確認された複数の特性を一意に組み合わせたもの。そのイベントが特定の種類のボットによって引き起こされたということを、その組み合わせにより識別できる。

ポップアップ
ユーザーが使用中のブラウザーの手前で開くウィンドウ。

ポップアンダー
ユーザーが使用中のブラウザーの背後で開くウィンドウ。ブラウザーのウィンドウを閉じると見えるようになる。

マイクロブラックリスト
更新と期限切れが頻繁に発生するブラックリスト。巧妙で適応性が高い脅威に対する実効性を高めるためのもの。

メークグッド
広告の構成、掲載、配信の誤りに対する埋め合わせとして、広告主や広告代理店に与えられる補償（またはその利用）のこと。

ユーザー
コンピューターなどのデバイスやネットワークサービスの利用者のこと。オンライン広告の世界では、ユーザーは、パブリッシャーのサイトを訪問する閲覧者であり、広告主の広告に接する消費者である。

リーチ
所定の期間内に、広告またはキャンペーンに少なくとも 1 回は接触したユーザーを重複なしで数えた総数。

リターゲティング（行動リターゲティング）
ユーザーがオンライン上で以前に取った行動に基づいて、特定のユーザーに広告を配信するプロセスのこと。

ロングテール
トラフィックの量は比較的少ないが、的を絞ったニッチなユーザー層に人気があり、広告主に価値をもたらす可能性がある Web サイト

付録 B

制約・制限事項

調査の複雑さ

今回の調査に参加した各社は、調査期間、プラットフォームの構成、対象のオーディエンス、業種、広告代理店がそれぞれ異なります。したがって、調査で得られたすべてのデータを参加企業ごとに直接比較することはできません。

Web フレームワークの制約

調査で使用したソフトウェアは、JavaScript が有効なシステムにのみ導入可能です。

実施を公表した調査に対する認知度

参加企業の多くでは、公式調査期間の段階で、管理面および技術面で導入の遅れが生じました。また、公式調査期間内は、ボットの数が意図的に減らされていた可能性があります。これらのことから、秘密の調査期間に検出されたボットの数の方が、今回の調査の枠組みに含まれない通常の広告キャンペーンの実情に近いことが考えられます。今回の調査を実施することは広く公表されていたため、正式な調査期間の月には、ボットの数が通常時より人為的に引き下げられていたものと推測されます。

季節的要因

White Ops の推定では、ボットの数は夏の終わりの時期が最も少なく、広告のニーズが最高潮に達する年末の時期が最も多いものと考えられます。今回の調査は、8 月と 9 月という時期のみを切り取ったものであり、通常月のボットの数や、広告量が多いピーク時期のボットの数をここから予測することはできません。

広告代理店との連携

調査の参加企業のなかには、キャンペーン全体に対して調査用のソフトウェアを均一に導入できなかった所もありました。法的条項、サイトポリシー、組織の複雑さといった管理上の要因によるものです。場合によっては、広告代理店に至る部分まで調査用のソフトウェアが導入されていないということを、参加企業が認識していないケースもありました。監視やデータ収集の実施期間中にこうした問題が明らかになったときには、White Ops は、参加企業やその広告代理店と連携して、問題の是正を試みました。

付録 C

調査にご協力いただいた外部企業

White Ops は、調査結果への洞察を深めるために、複数の企業から協力をいただきました。

Chartbeat

Chartbeat は、betaworks 傘下の企業で、Web サイトやブログのリアルタイム分析を提供しています。今回の調査では、ボットと人間のエンゲージメントや視認能力に関する指標値を比較するためのデータを提供し、1 億 2000 万のインプレッションと、87 のパブリッシャーに関する White Ops のデータとを照合しました。

Ghostery

Ghostery® は、インターネットの透明性や制御を実現するためのソリューションを個人向けや企業向けに提供しているグローバルテクノロジ企業です。今回の調査では、トラフィック量で上位 1 万のドメイン、ボットのワーストランキングに入ったサイト、および Alexa のランキングで上位のサイトが利用しているトラッカーについての洞察を提供しました。

Grapeshot

Grapeshot は、ケンブリッジ大学が開発した高度な情報取得技術を利用しているソフトウェアテクノロジ企業です。今回の調査では、1 万 3000 のドメインの特性データを提供しました。White Ops は、このデータを利用して、ドメインのカテゴリごとのボットの傾向を割り出しました。

付録 D

契約条項の例

この調査レポートで取り上げた問題に対処するための具体的な文言を契約条項に加えることを検討してください。ここでは、詐欺的なトラフィックの定義、および広告主とメディア企業との交渉のたたき台となる保護条項の一例を紹介します（全米広告主協会の外部法務顧問である Reed Smith が作成）。各社の個別の利益に最もかなう条項の具体的な内容については、顧問弁護士に相談してください。

契約条項

詐欺的トラフィック

(a)「詐欺的トラフィック」とは、何らかの機器を通常の手順で使用する中で実際に表示された広告を自然人が閲覧した行為以外のものを、データに計上または合算し、報告書、請求書、または本契約に伴うその他の情報および資料に対して、かかるデータを含めることをいう。これには、オンライン、モバイル、およびその他のテクノロジまたはプラットフォームを通じた閲覧が含まれるが、これに限定されない。多義性を回避するために、詐欺的トラフィックには、以下の (i)（ii)（iii)（iv) の閲覧を計上または合算することを含めるものとするが、これに限定されない。(i) かかる広告の閲覧を目的として従事している自然人による閲覧。その人間が閲覧のみを行うか、他の活動と付随して閲覧を行うかは問わない。(ii) 人間以外による訪問。(iii)（i) と (ii) のいずれかまたは両方の組み合わせによって誘導またはリダイレクトされた表示の組み合わせ。(iv) 人間の目で実際に見ることができない表示、人間の感覚で認識できない表示、または人間が知覚できない表示。

(b) メディア企業は、以下の (i)（ii)（iii) を目的として、商業的に妥当なすべてのテクノロジおよび手法を確立、導入、および利用するものとする。(i) 詐欺的トラフィックの回避。(ii) 詐欺的トラフィックが発生した場合の検出。(iii) その継続または再発を回避するための迅速な対処。メディア企業は、契約、指示、または法的拘束力のある何らかの手段により、広告の配信先、表示先、または利用先となるすべてのサードパーティについて、前述の義務をメディア企業が確実に遵守できるようなテクノロジと手法を各サードパーティが採用および導入していること（およびそれに書面により同意すること）を保証するものとする。本契約では、詐欺的トラフィックの代償となる補償、債務、またはその他の義務を広告主が負わないこと、および詐欺的トラフィックに対する請求または支払い義務を広告主が負わないことに、メディア企業は同意するものとする。詐欺的トラフィックに起因する支払いを広告主が行った場合、その範囲においてメディア企業は、かかる支払いを広告主に対して 5 日以内に返済および弁償するものとし、かかる返済または弁償の正確性を立証するための合理的に十分な文書を添えるものとする。本契約の中で他の監査条項に定めがない限り、広告主またはその指名監査人は、本契約の条項の遵守に関する判断を目的として、メディア企業の帳簿および記録を監査する権利を有するものとする。