UNDERSTANDING INVENTORY QUALITY

インベントリの品質を理解する

ボットの上手を行く

インベントリの品質を理解する
ボットの上手を行く

広告予算に占めるデジタルの割合が増えるにつれて、ブランド企業はデジタル広告サプライチェーンのさらなる透明性を追求し、品質の定義は変化しました。業界は、独力で広告詐欺の上手を行かなければなりません。

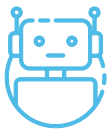
デジタル広告はマーケターに、ほかの媒体では難しい高精度のターゲティングと包括的な分析をもたらします。だからこそデジタル広告は2020年までに全世界の媒体広告費の約半分を占めると予想されており、こうしたインデマンド広告インプレッションへのアクセス手段としてプログラマティックの人気が高まっているのです。しかし同時に、デジタルオートメーションを浸透させたその仕組みが、既存媒体には存在しない難題をバイヤーにもたらしました。

10年前にプログラマティックが誕生して以来、インベントリ品質（IQ）という概念は広告詐欺との戦いと密接に結びついています。ボットや人間によらないトラフィックが収益化の過程から一掃されたとき、インベントリは本領を発揮するというのが前提条件でした。2016年には、不正なインプレッションによって広告主から1日当たり数百万ドルをだまし取る「Methbot」広告詐欺が発覚し、こうした高度な広告詐欺がデジタルエコシステムの品質上の課題を浮き彫りにしました。そして、世界最大級の広告主たちはクリーンなサプライチェーンを求めるようになりました。

すべての条件が同じだと仮定した場合、人間によらないトラフィックより人間によるトラフィックが望ましいのは事実ですが、業界は単なる広告詐欺との戦いではない新たなIQに目を向けています。また、今後は広告を消費する訪問者の価値をより的確に判断することが求められるため、サイト運営者がトラフィックを操作し、広告費を増やそうとする行為もIQの対象にしなければなりません。

このホワイトペーパーでは、バイヤーとパブリッシャーの両者に、プログラマティックが新しい未来を迎えたとき、成功を収めるために知っておくべきことをお伝えします。広告キャンペーンのROIを改善したいマーケターにとっては、ブランドの安全性とビューアビリティがとても重要ですが、このホワイトペーパーでは、IQに関わる広告詐欺、対応策に焦点を当てたいと思います。

このホワイトペーパーの目標は、以下のトピックを検証し変化しつつあるIQの定義を明確化することです。



人以外による トラフィック

コンピューターによって作られた活動で、本質的に、不正な広告インプレッションを供給します。

人による低価値の トラフィック

人間による広告インプレッションですが、価値の低いコンテンツが閲覧されたか、広告主にとって価値の低い状況で閲覧されたものです。

欺いたり混乱させたり する行為

ドメインスプーフィング、広告インジェクションなど、バイヤーに本物のトラフィック活動だと思わせ、広告収入を増やすための行為です。人および人以外、どちらの場合もありえます。

モバイルアプリ内広告 のIQ

次なるIQ革新が期待される未知の領域。

未来像

IQに関する業界の方向性であり、バイヤーとセラーが自分の身を守るためにしなければならないことです。

人以外によるトラフィック

デジタル広告業界ではしばしば、IQは人以外によるトラフィックと関連があります。

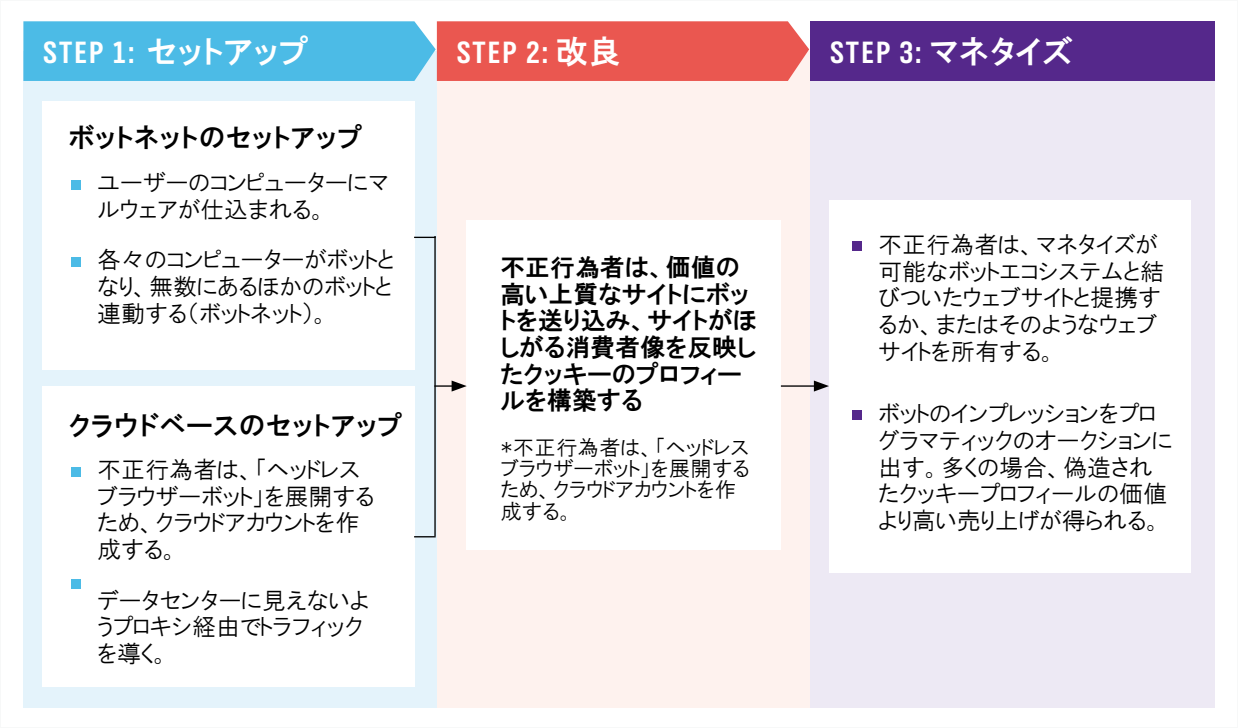
広告詐欺対策技術ベンダーが進出する以前、人によらないトラフィック（ボット詐欺など）がまん延し、不正行為者たちが懐を肥やしました。デジタルエコシステム全体で、人によらないトラフィックを特定および阻止するための投資が行われてきたにもかかわらず、全米広告主協会（ANA）とWhite Opsは、デジタル広告詐欺による経済的損失が2017年は65億ドルに達したという調査結果を発表しています。ボット詐欺の根絶という業界目標を達成するには、人によらないトラフィックの実態と仕組みについて、広告主とパブリッシャー双方が基本的な知識を身につけることが重要です。

人によらないトラフィックとは？

人によらないトラフィックは無効なトラフィック(IVT)とも呼ばれ、本人を介さずに生成されるあらゆるウェブサイトのトラフィックを指します。悪意あるボットのような不正トラフィック、消費者の不自然な閲覧行動によって生じたトラフィックなどがそれに含まれます。

	MRCによる定義[3]	例
一般的な無効トラフィック(GIVT)	GIVTは「リストの適用など、標準的なパラメーターチェックを伴う通常のフィルタリングで識別可能なトラフィック	■ 既知のデータセンターのトラフィック ■ 正体がわかっているボットやクローラー ■ 未知のブラウザー ■ ブラウザーに事前レンダリングされたトラフィック
高度な無効トラフィック(SIVT)	SIVT は「高度な分析や多点のコラボレーション／コーディネーション、人間による大幅な介入なしでは検出の難しいトラフィック	■ 本物のユーザーになりすましたボット ■ 乗っ取られたデバイス ■ 隠された／重ねられた広告配信 ■ アドウェアやマルウェア

SIVTの仕組み



身を守る方法

業界の目標は、ボット詐欺を阻止する方法を見つけ出すことですが、現実的には、回避と緩和によって無駄を最小限に抑えた方が賢明です。

1 回避

回避は通常、パブリッシャーの広告リクエストがオークションにかけられる前、または広告インプレッションが購入、供給される前に、広告詐欺対策技術ベンダーが詐欺に関する決断を下すことで発生します。いったん不正と判断されたインプレッションは廃棄が可能になります。

2 緩和

緩和は広告が配信された後、報告によって広告詐欺の割合や分布が明らかになることで発生します。この時点でのバイヤーの最善策はサプライヤーへの返金請求で、以前より一般的になっています。PubMaticもデマンドパートナー向けに広告詐欺防止プログラムを発表し、詐欺が検出された際は、バイヤーは代金を支払う必要がなくなりました。さらに、不正なドメインやアプリ、サプライヤーをメディア支出の対象外にすることをおすすめします。

人による低価値のトラフィック

現在のデジタルエコシステムでは、「詐欺でない」だけでは十分ではありません。コンテンツだけでなくオーディエンスの質を追求することが不可欠です。

広告詐欺という意味では、品質は白黒がはっきりしています。それは、広告インプレッションとは、人によって消費されるか、されないかのどちらかです。しかし、この5年間、年平均成長率（CAGR）28%のペースで拡大しており、2018年には、700億ドル規模に達する見込みであるプログラマティック業界では、健全性を欠く活動が入り込む余地が生まれているのです。

理論的には、あからさまな広告詐欺は別として、広告投資はオリジナルのコンテンツと忠実なオーディエンスを持つウェブサイトに集中させるべきです。しかし、デジタルエコシステムに流れ込んでいる金額を考えると、インセンティブのシステムはすでに壊れており、「自然の秩序」に逆らうことは可能だと皆が気づいているはずです。

広告を売るウェブサイトは無数にあります。魅力的なオリジナルコンテンツを提供するサイトの多くはすでに、広告収入に頼るビジネスモデルから脱却しています。低品質のコンテンツやユーザー体験を提供しながら、表面上は合法的なパブリッシャーに見えるサイトもあります。

サイトがどのように作られ、デザインされ、運営されているかを理解すれば、IQポリシーを決定する際、賢い判断を下す助けになります。

人による低価値のトラフィックとは？

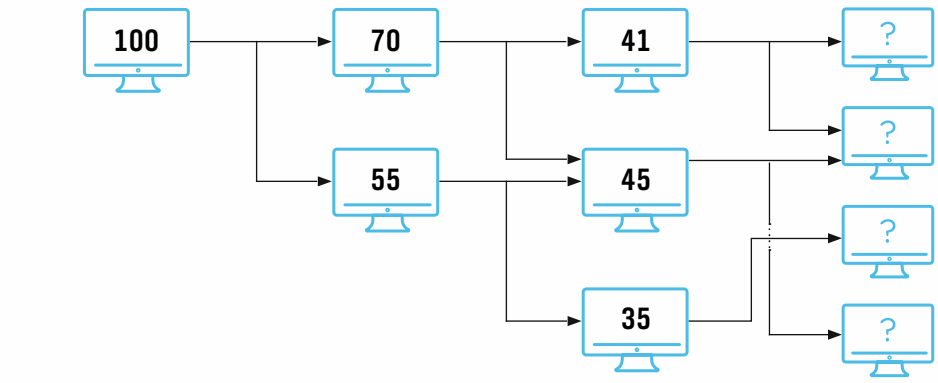
価値の低い、あるいは望ましくない人によるトラフィックとは、ユーザーが自分の意思でサイトを訪問したわけではない状況といえます。よくあるのは広告の内容に引かれてクリックした結果、コンテンツが思ったより魅力的でないというケースです。こうしたサイトは広告販売のためだけに存在します。ユーザーの同意なしにリダイレクトされるケースもあります。そのような場合、ユーザーはすぐサイトを去り、二度と戻ってきません。

ブランド広告費はデジタルメディアに投下され続けているため、この問題の重要性は増す一方です。ダイレクトレスポンス広告であれば、消費行動（売上、インストール、サインアップなど）によってキャンペーンの成功度を測定できます。しかし多くの場合、ブランド広告はこれほどわかりやすい評価基準を持たないため、不正行為の影響を受けやすいのです。

ケーススタディ

バックリンクで望ましくないオーディエンス、コンテンツを特定

特定サイトへのバックリンクをすべて分析すれば、オーディエンスの意図をより深く理解できます。リンクしてくれているサイトの密度や影響力を計算することで、ドメインの品質を測ることが可能です。下記のイラストで示しているように、リンクの流れは上流にある信頼性の高いサイトから始まり、リンクされたサイトは信頼性を獲得します。被リンクサイトの信頼性が高いほど、リンクされたサイトのスコアも高くなります。



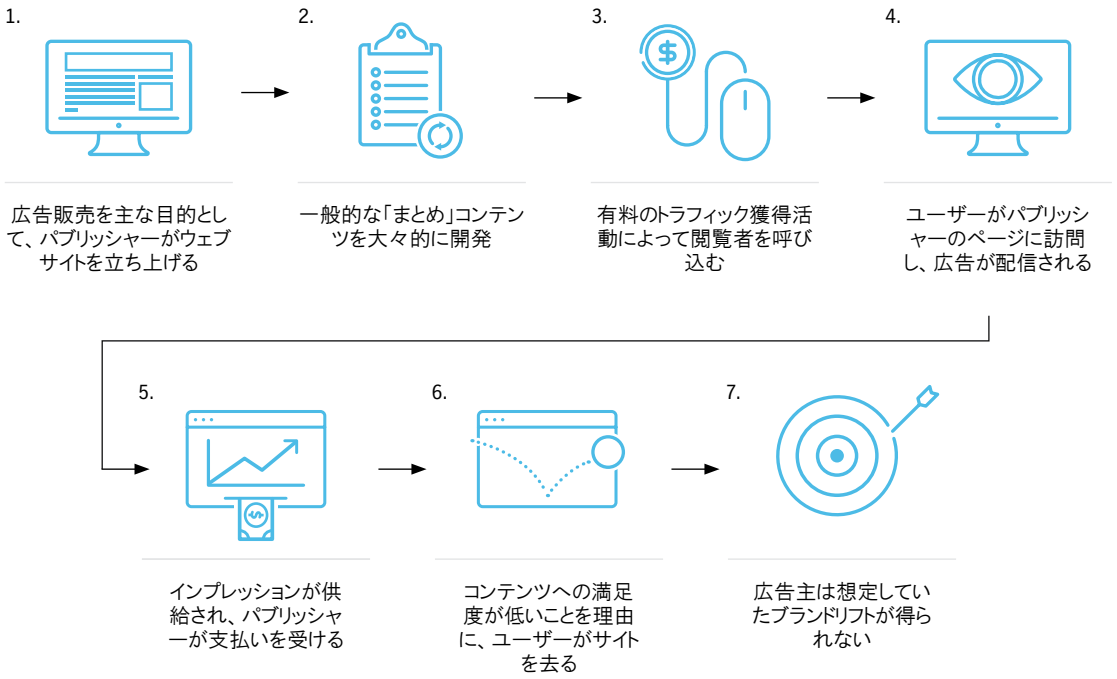
これらのスコアはトラフィックではなく評判に基づいています。低い点数は「ゴーストサイト」と強い相関があります。ゴーストサイトとは、広告収入を生み出すためだけにつくられたサイトのことです。あるウェブサイトがオーガニックで忠実なオーディエンスを構築していたら、その一部がリンクを貼って宣伝してくれるため、サイトの点数は高くなります。

低い点数は、コンテンツやオーディエンスの質が低いサイトを知るための優れた指標になるだけでなく、不正操作の影響を受ける心配がありません。バックリンクは信頼性の高いサイト（多くの場合、尊重されているニュースサイトやメディアサイト）から「流れる」ためです。もしバックリンクが信頼性の高い環境に根差していなければ、質より量だと軽視されるでしょう。

IQに関するプロのアドバイス

トラフィックの指標は、サイトの品質を評価する際に考慮すべき指標の1つにすぎません。バックリンクを分析することで、オーディエンスの意図をより正確に理解できます。大規模な分析が可能なサードパーティーのツールについて知りたい場合は、SSPパートナーにお問い合わせください。

人による価値の低いトラフィックの仕組み



身を守る方法

こうした活動は最近まで野放し状態でしたが、状況は変化しています。業界全体がサプライチェーンの効率を重視し始めたこと、透明性が求められていること、欧州連合（EU）の一般データ保護規則（GDPR）のようなプライバシーに関連する規制が施行されたこと、個人をターゲットにするというやり方が仮説通りにはいかないとわかってきたことなどが要因です。

メディアバイヤーが問題のあるサイトを見極めるには、こうした望ましくないパブリッシャーたちが用いる戦術を知っておかなければなりません。そのためにも、コンテンツやオーディエンスの質を徹底的に調べ、バイヤーを守ることに熱心なプログラマティックパートナーと連携することが重要です。

人による低価値のトラフィックに共通するシグナル：

1 コンテンツの作者が実在しない

広告の掲載場所を確保するためだけにコンテンツが作られている場合、ストック写真がライターの写真として使用されることがあります。似たような特徴を持つさまざまなゴーストサイトに、同じライターが登場することもあります。

2 トラフィックのパターンに一貫性がない

奇妙なトラフィックの急増は、トラフィック獲得活動の増加を示唆する場合があります。トラフィックの急増が不正検出技術に引っかからなければ、パブリッシャーは広告収入を得るため、サイト訪問者の水増しを続けるでしょう。

3 「企業紹介」ページが一般的な内容

ゴーストサイトは収入を生み出すことが目的で、基本原則が存在しないため、多くの場合、「企業紹介」ページや「お問い合わせ」ページが一般的な内容になっています。担当者の名前が書いてあることはほとんどないでしょう。

4 ドメイン登録が隠されている

通常、プライバシー保護されたドメインを使用しているため、サイトの背後にいる人物を特定することは困難です。米国の法執行機関が捜査できないパナマのような国でドメイン登録されている場合もあります。

欺いたり混乱させたりする行為

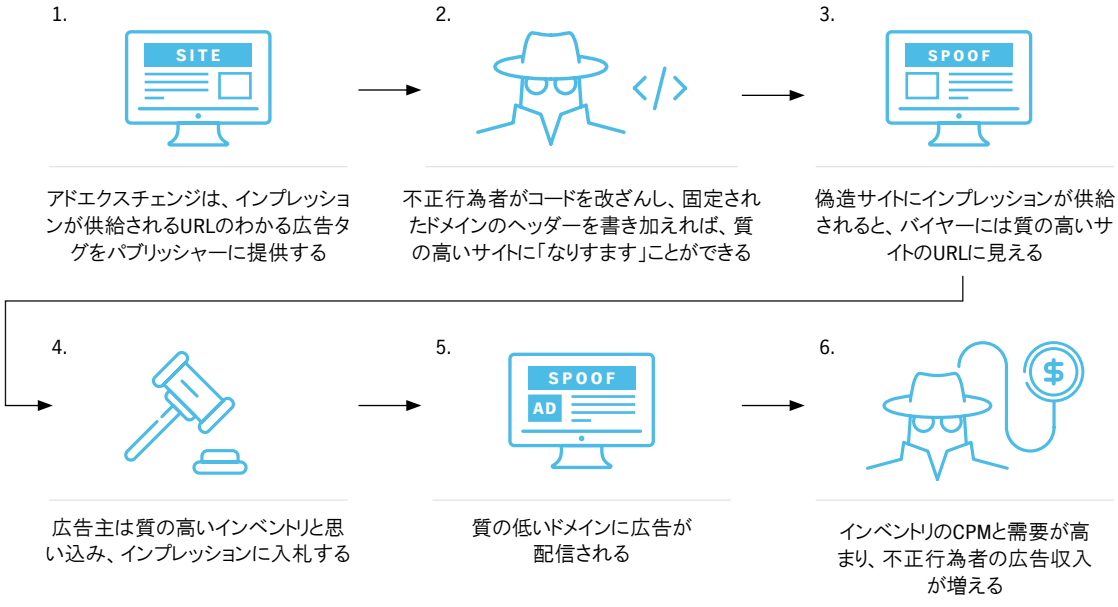
広告詐欺への対応はされていますが、インプレッションの出どころや価値を隠したり、あいまいにしたり、合法的に見せたりする方法はいくつもあります。

プログラマティック業界はエコシステムの現実に気づき、透明性と質の高いデジタルサプライチェーンの実現を目指しています。これに対し、不正を働く人々はシステムを出し抜くため、すべての時間と労力、資金を投じています。おそらく最も話題になっているのはドメインスプーフィングですが、インベントリの売り手が不正行為を疑わしくないものに見せかけ、それによってインプレッションを魅力的で価値あるものに見せる方法はいくつもあります。

ドメインスプーフィングとは？

ドメインスプーフィングとはトラフィックを隠し、入札リクエストを価値あるものに見せる手法です。たとえば、ゴーストサイトからのトラフィックを「偽造」し、質の高いドメインからのインベントリに見せることも可能です。その結果、バイヤーはインベントリを過大評価し、その品質を信頼してしまいます。

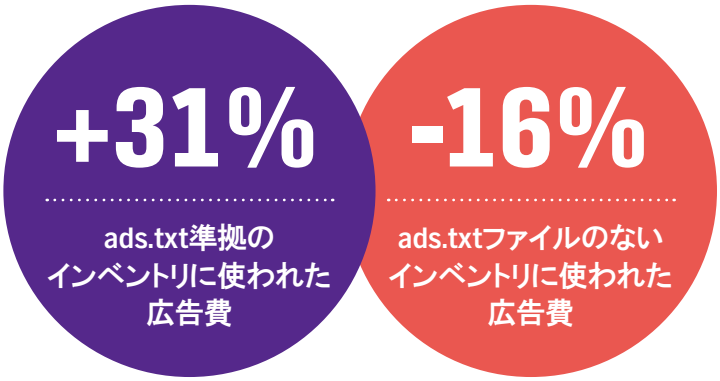
ドメインスプーフィングの仕組み



身を守る方法

ドメインスプーフィングは絶滅の運命にあるデジタル不正行為です。その大きな理由は、Interactive Advertising Bureau（IAB）が提唱する「ads.txt」の導入が急速に進んでいることです。インベントリ販売の権限を持つすべての企業をパブリッシャーが公表するというシンプルなソリューションです。

バイヤーは入札リクエストが本物かどうかを素早く容易に確認できます。プロパティーにads.txtを実装するパブリッシャー側もサプライチェーンの合法性を確保できます。PubMaticが2018年に入って実施した分析では、マーケターはads.txt準拠のインベントリに広告費を使い続けていると判明しました。4カ月にわたる分析の結果は以下の通りです：



PubMaticを含む多くのテクノロジープロバイダーが、パブリッシャーはads.txtファイルによって認証されたインベントリのみから広告収入を得られるという方針を発表しました。

- ドメインスプーフィングの拡大が続くモバイルアプリのインベントリは対象外。
- ファイル内で広告フォーマットを区別できないため、（ビデオ広告を除外した）ディスプレイ広告のみの承認をリセラーに与えられない。
- 特にスペルミスなど、人的エラーのリスクがあり、合法的なセラーの減少につながっている。
- 一部の悪質なリセラーがソーシャルエンジニアリングによって、パブリッシャーのads.txtファイルに入り込もうとしている。

ケーススタディ

ADS.TXTファイルの改ざん

Tesseractと広く呼ばれているPubMaticのサプライパートナーが、ある質の高いプロパティーで、インベントリの裁定取引をしていたことが判明しました。パブリッシャーと直接的な関係、つまり、リセラーとしての関係を築くのではなく、サードパーティーからインベントリを購入していたのです。この取引はもうしばらくは発覚しない可能性もありました。パブリッシャーのads.txtにTesseractのサプライヤーIDが掲載されているためです。しかし、私たちは検証中にいくつかの問題点を発見しました。

#Syndicated Videoというヘッダーの付いたセクションに、以下のような記述がありました：

ポーランドのメディア企業XYZ PolandとイスラエルのTesseractにどのような関係があるのでしょうか？

出来高が最も多い日のURLデータを抜き出してみたところ、ユニークURLの半分近くが同じパブリッシャーからのものでした。その日の出来高の実に97%を占めていました（広告リクエストは5億回以上）。ユニークURLはすべてポーランドと無関係で、広告リクエストの95%が米国のデータセンターを経由していました。コンテンツが広告リクエストの多さを正当化できると示唆するものは何もありませんでした。

調査の結果、Tesseractとパブリッシャーは直接的な関係がないとわかりました。TesseractはXYZ Polandが持つパブリッシャーへの影響力を利用し、パブリッシャーのads.txtファイルに掲載してもらうことで、裁定取引（ディスプレイ広告枠にカルーセル形式のビデオ広告を配信するなど）を正当化していたのです。PubMaticは直ちに契約解除の手続きを開始しました。

IQに関するプロのアドバイス

ads.txtはドメインスプーフィングや詐欺に対する防御の最前線と見なすべきです。悪意ある活動や疑わしい活動に目を光らせているベンダーと連携することが重要です。テクノロジーパートナーに問い合わせ、どのような対策を講じているかを尋ねてみましょう。

そのほかの欺いたり、混乱させたりする行為

1 ページレベルのスクリプティング

オーガニックなオーディエンスを構築するのではなく、コウコク詐欺的な手法で人間によるトラフィックを獲得しているサイトは、1ユーザー当たりの広告収入を増やすため、サイトの構造を操作していることもよくあります。この種の活動には、大きさが0×0ピクセルの目に見えないインラインフレームや広告のサイジングといった不正行為があります。前者はサイトに閲覧可能な広告を表示することなく、インプレッションを増やしていくことが可能で、後者は1ユーザー当たりのインプレッションを桁違いに増やせます。

ページレベルのスクリプティングは特に、アプリ内広告のインベントリにまん延しています。測定ツールのベンダーがモバイルアプリに独自のSDKを組み込んでいなければ、意思決定に利用できるシグナルが限られるため、インベントリの操作を突き止め、警告を発する確率が下がります。IABのOpen Measurement（OM）SDKを導入すれば、アプリに複数のSDK（ベンダーごとに1つずつ）組み込む必要がなくなります。OM-SDKの詳細については、アプリ内広告のIQセクションをご参照ください。

2 広告インジェクションとアドウェア

ツールバー、ソフトウェアのインストール、悪意あるコードが埋め込まれた広告など、さまざまな形でもたらされるマルウェアは、サイトと無関係なインベントリの販売を可能にします。多くの場合、広告インジェクションがそうであるように、不正な広告が既存の広告を完全に覆い隠すか、もともと広告のないページに不正な広告が表示されます。その結果、パブリッシャーから広告収入を奪い、サイトの知名度を利用できるのです。こうしたインベントリはしばしばドメインスプーフィングによって隠され、広告ネットワークやアグリゲーターなどからエコシステムに入り込みます。

IABのads.certはRTB 3.0を必要としますが、こうした問題を解決するための取り組みです。安全なデジタル署名を使用し、オリジナルの広告とバイヤーを切れない鎖でつなぐことによって、ads.txt以上の保護を実現します。このデジタル署名はいわゆる「認証キー」の役割を果たし、不正行為者が合法的なドメインに隠れて入札リクエストを出すのを阻止します。広告インジェクションに使用されるマルウェアの不正を阻止するということです。

3 質の低い ユーザーエクスペリエンス

このような「乗っ取り」には、パブリッシャーが広告収入を増やすため、あらゆる手段でユーザー体験の質を低下させる行為も含まれます：

- さまざまなサイズの広告をページにちりばめる。
- 広告インプレッションを増やすため、スライドショーをクリックさせる。
- 自動再生ビデオ広告の多用。音声付きが多い。

こうした手法はいずれも広告詐欺と見なすことはできませんし、見なすべきではありません。透明性と可視性が確保されているためです。

ただし、品質の問題が2つあります。1つ目は、消費者が過剰な広告にいら立ち、巻き込まれたブランドが汚名を着せられること。2つ目は、メッセージの集中砲火によって、一つひとつのインパクトや価値が下がることです。大多数のエクスチェンジやプラットフォームと同様、PubMaticはポリシーを整備し、こうした状況の回避に努めています。

モバイルアプリ内広告のIQ

タグベースの検出が不可能なため、モバイルアプリは、IQの未開発領域です。詐欺の特定は非常に難しく、コンテンツの検証も困難です。

すでにオンライン広告が成熟しているデスクトップ環境と異なり、モバイルアプリ広告のインベントリは測定や不正の検出において、いくつもの課題を抱えています。

デスクトップ環境では追跡にクッキーを使用しますが、モバイルアプリはデバイスIDで追跡します。IPアドレスはインターネットに接続された個々のコンピューターやサーバーを表しますが、モバイル環境では基地局に割り当てられており、無数のデバイスが接続します。モバイル環境ではシグナルセットも大きく異なり、人間以外によって行われた不正を同じように検出することは不可能です。シグナルはアプリ内にあり、アクセスすら困難です。「トンネル」からアプリに入り、不正（やビューアビリティ）を検出するためのデータにアクセスするには、SDKを使用する必要があります。

さらに、デバイスの環境を考えると、アプリのコンテンツやユーザー体験を評価するのも困難です。ウェブページをロードし、コンテンツを品質チェックするのは容易ですが、アプリはデバイス上でロードしなければならないため、まとめて監視するのは難しいでしょう。

アプリ内広告のIQに関する課題

アプリ内の品質シグナルや情報にアクセスしにくい現状を考えると、アプリ環境は偽造データのやりとりを助長しているとも言えます。偽造行為にはさまざまなタイプがありますが、いずれも目的は広告収入を増やすことで、広告インベントリやオーディエンスの機会を実際より大きく、価値あるものに見せるという方法がとられます。

偽造行為にはさまざまな種類があり、人間によらないトラフィック、品質の低下、指標の過大評価といった結果を招きます。

デバイススプーフィング

倫理に反する悪質なアプリが、入札リクエストに含まれるデバイス情報を偽造します。デバイスID（IMEIなど）、IPアドレス、ハードウェアのメーカーやモデルに関する幅広いデータを挿入することで、多様なユーザーから入札リクエストが来ているように見せかけることが可能です。

アプリスプーフィング

デスクトップ環境では、ads.txtがドメインスプーフィングを解決しましたが、アプリスプーフィングはドメインスプーフィングとよく似ており、アプリを魅力的に見せかけるため、有名アプリのIDを挿入します。しかし実際は、不正を働いているアプリに広告が配信されます。

ロケーションスプーフィング

悪質なアプリが偽造された座標データを入札リクエストに挿入します。ジオターゲティングが行われている場合、入札リクエストの価値が上がります（マリのトンブクトゥから来た入札リクエストをニューヨークから来たように偽造するなど）。検出を回避するため、別のスプーフィングと併用されることもあります（英国からの入札リクエストに見せかけ、スリランカの倉庫に並べられたプログラム済みのデバイスが発信元であることを隠すなど）。

身を守る方法

2017年、IAB Tech LabがOpen Measurement（OM）構想を発表し、その目玉としてOM-SDKを公開しました。OM-SDKは「ユニバーサルトランスレーター」の役割を果たし、検証ツールや測定ツールのプロバイダーがSDKを1つ実装するだけで、アプリから発信されているシグナルを「聞き」、集めることができます。もし広く導入されれば、アプリ内広告のインベントリを測定し、不正を検出したり、ビューアビリティを評価したりするための標準になるでしょう。

さらに、IABは2018年6月、モバイルアプリ版ads.txtをつくるという構想を発表しました。こちらも導入が進めば、ads.txtがウェブ上でドメインスプーフィングを一掃しているように、モバイル環境でもアプリスプーフィングの大部分を阻止できるでしょう。

これらの業界標準が浸透するまでは、モバイルアプリのインベントリに関する不正を検出するのは難しいでしょう。ただし、テクノロジープロバイダーがバイヤーを正しい方向に導くことは可能です。それ自体が悪質なアプリ、不正行為の隠れみのとして評判が利用されているアプリに目を光らせればよいのです。

1 サードパーティーの不正検出サービスを利用

モバイルアプリの不正検出はデスクトップほど確実ではありませんが、サードパーティーが防御の最前線に立ち、詳細な調査が必要なアプリやブロックすべきアプリに関するレポートを提供しています。

2 ユーザーがコンテンツ消費しているアプリを選択

懐中電灯アプリやウイルス対策アプリなど、ユーザーがコンテンツに接する時間の少ないユーティリティアプリは避けましょう。この種のアプリはしばしば、ユーザーが関わらない場所の入札リクエストを大量生成するために利用されています。

3 ANDROID/IOSのストアでアプリを選択

これらのストアはアプリを評価する際、広告詐欺を考慮に入れているわけではありませんが、ほかのストアにはない基本的な要件を設定しています。

4 人気ランキング1000位以内のアプリを選ぶ

AndroidアプリとiOSアプリの人気ランキングを利用すれば、ユーザー基盤がしっかりした優良アプリのリストを作成できます。おそらく悪質なアプリはサプライチェーンの隅で、広告エコシステムのオープンオークション構造から利益を得ようと身を潜めています。

未来像

指を鳴らせば、たちまち広告詐欺が消え去る。このような未来が訪れたらどうでしょう？

デジタル広告エコシステムの長期的な健全性を実現することはもちろん不可欠ですが、現在は広告詐欺の一掃に力が注がれており、業界にとって重要なほかの問題がおそろかになっています。ads.txt、ads.certのような業界全体を巻き込む新しい取り組みは、前進するための強固な土台となるでしょう。私たちはプログラマティックのプロとして、IQの向上を持続させるため、次に資源を投じるべき領域を見極めなければなりません。

ターゲティングの衰退

クッキーによってオーディエンスやセグメントに分類され、（広告技術によって）マーケティングメッセージのターゲットにされることに対して、消費者の不満の声はますます大きくなっています。そして、EUのGDPRをはじめとする規制が作られ、クッキーやオーディエンスターゲティングの障害になっています。その結果、質の高いコンテンツとコンテンツ連動型広告の重要性が増しています。

品質はコンテンツから始まる

サードパーティーの不正検出ツールベンダーは、ツールを導入すれば、広告主は不正トラフィックを阻止できると訴えています。人間によらないトラフィックを特定、除去することは確かに重要ですが、私たちはそれが唯一無二の解決策と思い込まされているのではないでしょうか。信頼できる合法的な発信源を持つ質の高いコンテンツは、それ自体が新たなフィルターになります。

品質向上のためのベストプラクティス

デジタルメディアのバイヤーとセラーはどちらも、デジタル業界に前向きな変化をもたらすことが可能です。これまでの経験から導き出したベストプラクティスを紹介しましょう:

バイヤー

1 リスク軽減のため、認証ベンダーと連携する

JIC-WEBSや米国のTrustworthy Accountability Group（TAG）は犯罪活動を根絶し、デジタル広告業界の信頼を回復するための認証プログラムです。パブリッシャーやテクノロジーパートナーに問い合わせ、あらゆるフォーマットとプラットフォームでブランド安全性のチェックやインベントリの審査を行うため、どのIQベンダーを使っているか尋ねてみることをおすすめします。

2 コンテンツとオーディエンスの重要性を意識する

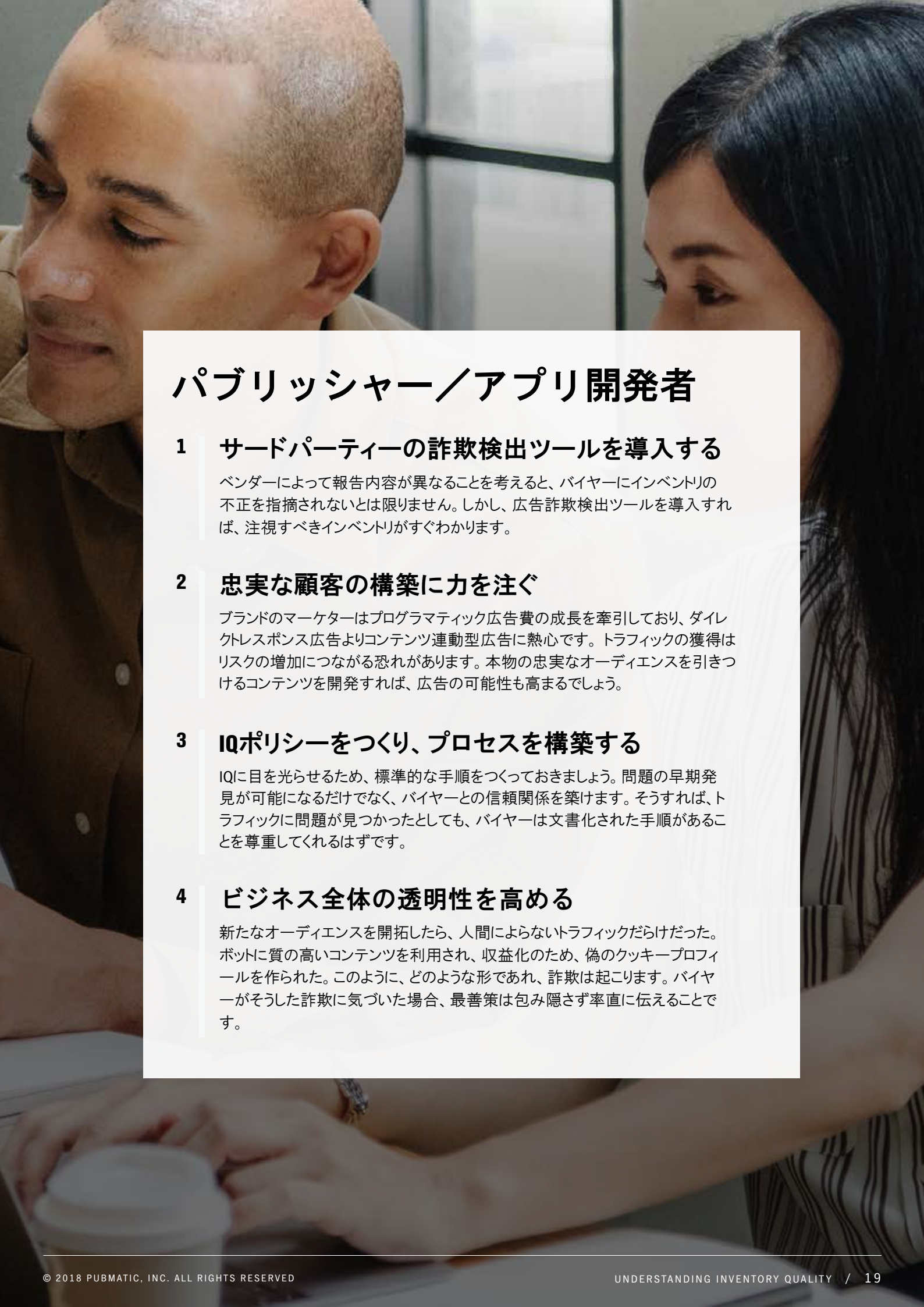
ドメインやアプリを評価する際は、IVTのレベルだけでなく、オーディエンスの価値やコンテンツのオリジナリティーを基準にすることが重要です。例えば、本物の忠実なオーディエンスは、ほかの発信源から獲得した消費者より望ましいオーディエンスです。広告インプレッションを売るためだけに存在するコンテンツファームや類似サイトも避けましょう。

3 広告が配信される場所を知る

ads.txtの登場によって、ドメインスプーフィング対策は大きく前進しましたが、ほかのタイプの詐欺やIQに対する懸念が解消されたわけではありません。広告を配信するドメインを慎重に選んだり、優良ドメインのみを対象にしたりすることで、多くの品質問題は回避可能です。

4 広告詐欺に手を貸さない

広告詐欺を防ぐエコシステムの構築に熱心で、必要なときは大胆な行動に出るパートナーと連携しましょう。テクノロジーパートナーに問い合わせ、不正行為が発覚したら返金されるかどうかを尋ねてみましょう。PubMaticの場合は、広告詐欺防止プログラムを用意しています。



パブリッシャー／アプリ開発者

1 サードパーティーの詐欺検出ツールを導入する

ベンダーによって報告内容が異なることを考えると、バイヤーにインベントリの不正を指摘されないとは限りません。しかし、広告詐欺検出ツールを導入すれば、注視すべきインベントリがすぐわかります。

2 忠実な顧客の構築に力を注ぐ

ブランドのマーケターはプログラマティック広告費の成長を牽引しており、ダイレクトレスポンス広告よりコンテンツ連動型広告に熱心です。トラフィックの獲得はリスクの増加につながる恐れがあります。本物の忠実なオーディエンスを引きつけるコンテンツを開発すれば、広告の可能性も高まるでしょう。

3 IQポリシーをつくり、プロセスを構築する

IQに目を光らせるため、標準的な手順をつくっておきましょう。問題の早期発見が可能になるだけでなく、バイヤーとの信頼関係を築けます。そうすれば、トラフィックに問題が見つかったとしても、バイヤーは文書化された手順があることを尊重してくれるはずです。

4 ビジネス全体の透明性を高める

新たなオーディエンスを開拓したら、人間によらないトラフィックだらけだった。ボットに質の高いコンテンツを利用され、収益化のため、偽のクッキープロフィールを作られた。このように、どのような形であれ、詐欺は起こります。バイヤーがそうした詐欺に気づいた場合、最善策は包み隠さず率直に伝えることです。

NOTES

[1] “Global Ad Spending: The eMarketer Forecast for 2018,” eMarketer, May 2018
[2] “Bot Baseline 2016-2017,” ANA and WhiteOps, May 2017
[3] “Invalid Traffic Detection and Filtration Guidelines Addendum,” Media Ratings Council, Inc. (MRC), October 2015
[4] “Programmatic Ad Spending Worldwide, 2012-2019,” eMarketer, November 2017

PubMatic(パブマティック)について

PubMaticは、オープンなデジタルメディアの未来のために、パブリッシャー重視のSSPを提供する企業です。
パブリッシャー向けの優れたオムニチャネル収益管理プラットフォームと、メディアバイヤーのためのエンタープライズクラスのプログラマティックツールを特色とするPubMaticのパブリッシャーファーストのアプローチにより、広告主は大規模なプレミア在庫へアクセスすることができます。
PubMaticは毎月12兆以上の広告主からの入札を処理しており、パブリッシャーの収益化を促進し広告在庫を管理するためのグローバルなインフラストラクチャを構築しました。 2006年以来、PubMaticはデータと技術革新に焦点を当てプログラム産業全体の台頭を促進してきました。カリフォルニア州レッドウッドシティーに本社を置くPubMaticは、世界13のオフィスと6つのデータセンターを運営しています。

お問い合わせ先

パブマティック株式会社
〒 107-0062
東京都港区南青山 4-11-6 YM テラス　B 棟
Email: jp@pubmatic.com
TEL: 03-6804-1143

PubMatic