

ビジネス インテリジェンス

app

WEBスクレイピング

アプリのセキュリティを第一に考える

価値あるクリックを見分ける

自動化時代におけるROIの最適化

自動化

効率性

app

不正行為

概要

アーサー・コナン・ドイルの『恐怖の谷』で、シャーロック・ホームズは現地の警部にこのように語っています。「不十分なデータから早まった理論をうちたてることはこの職業にあってはならないことです」

\$400万

配送ルートを最適化することで毎年最大\$40,000万を節約できます。



大量の情報が溢れる現在のビジネスの世界において、十分なデータにアクセスできるかどうかは問題ではありません。一般的に問題になっているのは別のこと、つまり無駄なデータです。

データと分析は、どこに投資および開発するかを決める上で役に立つツールで、その重要性はますます高まっています。これらは、現在の戦略の成果を図り、意思決定の正当な根拠を示し、成長計画を確信できる重要な手段です。顧客との関わりは大切なことで、これは一般的にクリック数で評価されます。私たちは、サイト訪問者がどこから来たのか、いくつのページにアクセスしているか、広告およびバナーをクリックしているか、および最終的にサイトまたはサービスの利用を選択するまでにどのくらい時間がかかったかを追跡しています。この情報がなければ、意思決定の根拠はありません。

私たちはビッグ データに依存して、配送物流¹や作物収量²から革新的なマーケティング技術³まであらゆることに関する実用的なビジネス インテリジェンスを提供していますが、収集する情報の価値は、それが比較される背景に限られます。情報を収集し、それを操作して、ビジネス インサイトを生み出すことは比較的簡単なことですが、収集しているデータが適切なデータでなければ、これらのインサイトの価値はありません。

¹ <http://www.cnn.com/2017/02/16/world/ups-trucks-no-left-turns/index.html>

² <https://www.forbes.com/sites/timspalapani/2017/03/23/how-big-data-and-tech-will-improve-agriculture-from-farm-to-table/#3059d9d65989>

³ <http://www.businessinsider.com/the-incredible-story-of-how-target-exposed-a-teen-girls-pregnancy-2012-2>

データが嘘を付いていたら、 どうしますか

データが実際に嘘を付くことはありませんが、その解釈の仕方によっては、データは偏った印象を与えることができます。「ガベージ イン、ガベージ アウト」(ガラクタを入れればガラクタが出てくる) という古い格言があります。この問題についての「ガベージ イン」の部分は、1つの主要因、つまり善悪両方の可能性があるボットに要約できます。

サイトまたはWebサービスに対するWebトラフィックの大部分の発信源は恐らくボットです。これらの自律プログラムは、有益なもの (Webのマッピング⁴、デジタル パーソナルアシスタントとしての行動⁵) から悪意のあるもの (Webスクレイピング⁶、不正行為⁷、DDoS⁸) まで、あらゆるアクティビティに関係しています。ボット トラフィックは正当なように見えますが、自動化されたプログラムで実行されるスキャンおよびプローブと、顧客との実際の関わりを区別することが重要です。

ボットによるクリックは、実際の人間によるクリックと同じではありません。これらの不要なクリックは、分析を歪曲し、マーケット インテリジェンスを歪め、利益を損ねます。たとえば、既存の顧客ベースのほとんどが米国本土内にあることが分かっているとき、米国外を発信源とする大量のトラフィックを確認すれば、より大規模な国際市場に展開するための重要なリソースに投資することを考えるかもしれませんが、現実には、このトラフィックのほとんどは、ページをスキャンおよびスクレイプするボットから発信されている可能性もあります。

**ボットを積極的および効果的に
管理しなければ、正確な分析は
できません。**

データに基づいて意思決定を行う場合、適切なデータを利用する必要があります。ボットだけでなく、ボットとサイトおよびサービスとの関係を積極的および効果的に管理しなければ、正確な分析はできません。自動化されたトラフィックを識別および分類して初めて、ビジネス インテリジェンスの担当者が必要とする現実の実用的な情報にたどり着くことができます。

⁴ <https://www.google.com/search/howsearchworks/crawling-indexing/>

⁵ <https://www.forbes.com/sites/blakemorgan/2017/03/21/how-chatbots-will-transform-customer-experience-an-infographic/#4d4d3c5d7fb4>

⁶ <https://www.businesscomputingworld.co.uk/web-scraping-is-eating-away-at-revenue-profit-and-ip/>

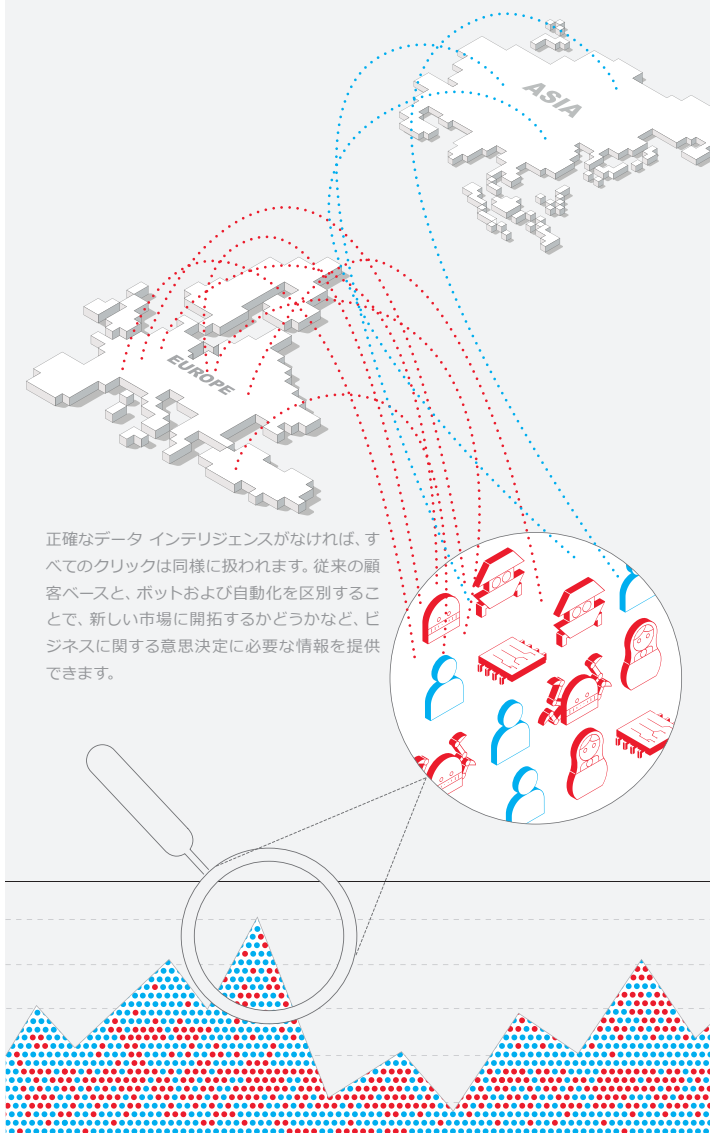
⁷ <https://f5.com/labs/articles/threat-intelligence/malware/yasuo-bot-flexible-customized-fraudulent-content-22442>

⁸ <https://f5.com/labs/articles/threat-intelligence/ddos/the-hunt-for-iot-the-rise-of-thingbots>

ガベージ イン、ガベージ アウト

ボットはデータを歪曲できる

ボットからの不要なクリックは、分析を歪曲し、マーケット インテリジェンスを歪め、利益を損ねます。



正確なデータ インテリジェンスがなければ、すべてのクリックは同様に扱われます。従来の顧客ベースと、ボットおよび自動化を区別することで、新しい市場に開拓するかどうかなど、ビジネスに関する意思決定に必要な情報を提供できます。



迷惑なだけではない ボットには余計なコストがかかる

ボットは、ビジネスの意思決定に影響を与える不正データを提供するだけでなく、収益に悪影響を及ぼすこともできます。従量課金モデルで提供されるクラウドベースのサービスがますます増加する中、自動化されたトラフィックは、ビジネス上の価値を何一つもたらすことなく、コストを押し上げます。

次のことを考えてください。ボットからサイトに送られるリクエストはすべて、帯域幅、CPU時間およびメモリ コストにより数量化でき、これらすべては毎月の費用に反映されます。ボット トラフィックが増えるほど、ますます多くのクラウドのコンピュー能力、マシン インスタンスおよびコストが必要になります。

また、悪意のあるボットは多種多様です。犯罪者は、自動化されたプログラムを使用して、価格設定を盗んで競合情報分析を強化、サービス拒否攻撃によりビジネスを妨害、およびさまざまな方法により不正取引を企み、これらすべてがビジネスおよびブランドの評判に悪影響を与えます。ビジネスを積極的に妨害しようとしているマシンのためにお金を払って、ページを表示、およびサーバ リクエストを実行していることは言うまでもありません。これらは顧客になる気はなく、ただ脆弱性をスキャンまたは知的財産を盗もうとしているだけです。

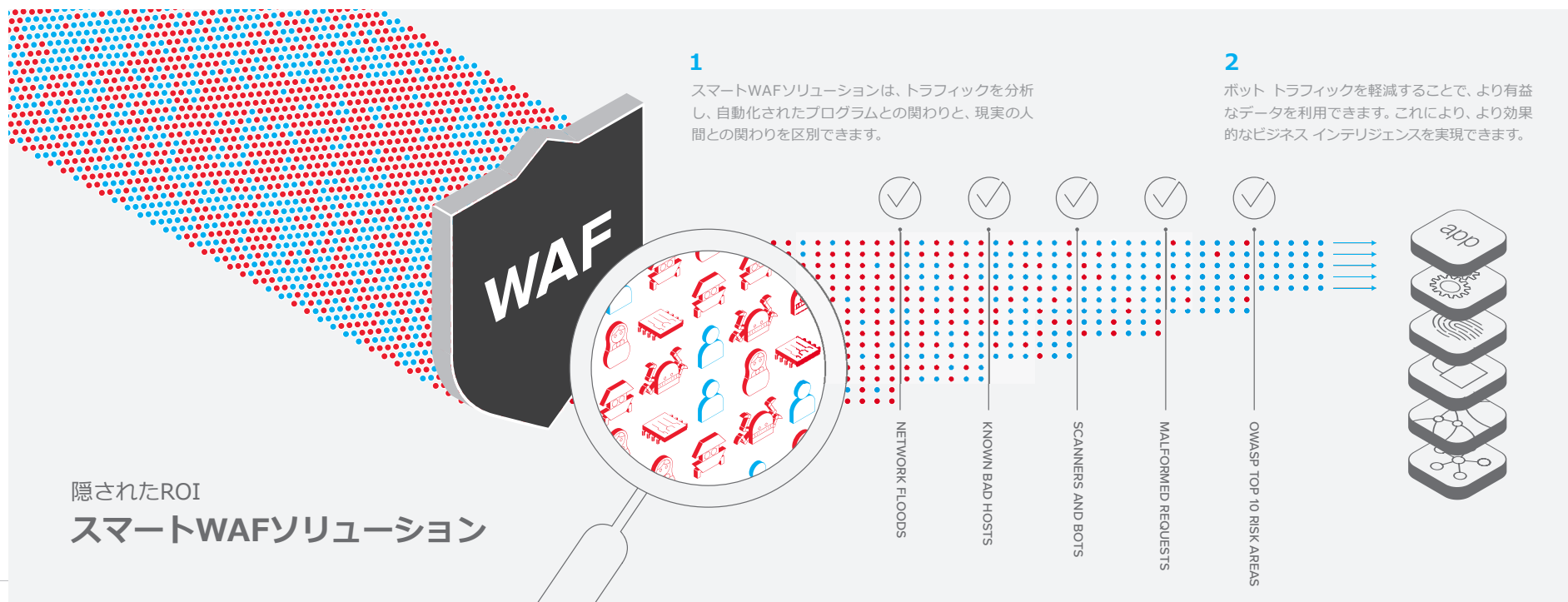
データセットを歪曲する、利用料金を高騰させる、またはマルウェアのベクトルとして行動する場合でも、ボットには余計なコストがかかります。しかし、セキュリティ コントロール（ボット トラフィックと人間のトラフィックの区別に役立つCAPTCHAなど）を過度に強化すると、顧客の我慢の限度を超え、事実上自らのサイトにDoS攻撃を仕掛けていることになり得ます。自動化されたすべてのトラフィックをサイトからブロックすることはできないので、悪意のある（または単に不要な）ボットによる損害を軽減しながら、「良い」ボットを最適にサポートするにはどうすべきかに注目する必要があります。

利益の向上 効果的なセキュリティ ソリューションの利用

従来のネットワーク アーキテクチャでは、セキュリティ アプライアンスは一般的に埋没原価と見なされました。これらが必要なことは確かですが、測定可能なROIを必ず実現するわけではありません。ファイアウォールは、攻撃された場合の防御となることを期待して購入します。しかし、実際に攻撃されるかどうかはわかりません。それでも、ビッグ データおよびクラウド コンピューティングの時代においては、セキュリティにより、ビジネスを攻撃から守るだけでなく、実際にアプリケーションおよびWebサイトを最適化し、コストを削減できます。

その仕組みについて説明します。スマートWebアプリケーション ファイアウォール (WAF) ソリューションは、サイトに送られるトラフィックを管理し、自動化されたアクセスと、実際の人間との関わりを分けてフィルタリングできます。大規模なボットトラフィックを軽減することで、ワークロードが減り、より有益なデータを利用できます。これにより、より効果的なビジネスインテリジェンスを実現できます。実用的なデータを利用することで、クリックボットの軍隊ではなく、実際の顧客を相手にしたマーケティングをより簡単に実行できます。

また、ボット管理機能を備えた効果的なWAFは、不要なトラフィックや悪意のあるトラフィックを減らすことで、Webプロパティを最適化でき、これが大幅なコスト節約につながり、現実の見込み客のみにサービスを提供することで合理化にもなります。つまり、セキュリティ ツールは、クラウドのコストを削減することで、真の価値を提供します。測定可能なROIを実現するセキュリティ ソリューションは、ビジネスが必要とするだけでなく、ビジネスが求めるツールです。



価値あるクリックを見分ける

このビッグ データと分析の時代において、虚偽的なクリックをブロックしながら、顧客からのクリックに注目することが、成功と失敗の分かれ目となります。しかし、正当なトラフィックと価値のない（または悪意のある）トラフィックを独自に区別することは困難です。このためには、専用のスタッフと、開発リソースへの多額の投資が必要であり、これらはどちらもコストを増大し、収益を減少させます。

より効果的な方法

スマート セキュリティ ソリューションは、自動化されたトラフィックの急増を管理するだけでなく、コストを削減し、全体的なセキュリティを向上できます。動的なボット管理、および変化を続ける脅威ランandscapeを学習してこれに適應できるアプリケーション保護ソリューションを組み合わせることで、人間の顧客に最適なサービスを提供し、サイトおよびサービスを最適化して、ビジネスが必要とするデータに基づいたのインサイトを手に入れることができます。

ボットの管理がビジネスにどのように役立つかの詳細については、f5.com/securityをご覧ください。

スマート セキュリティ ソリューションは、トラフィック管理、コスト削減、全体的なセキュリティの改善に役立つだけでなく、ビジネスに必要なデータに基づいたのインサイトを手に入れることができます。



アプリのセキュリティを第一に考える

常時稼働、常時接続のアプリは、ビジネスを強化および変革する一方、ファイアウォールに保護されないデータへのゲートウェイにもなり得ます。ほとんどの攻撃はアプリ レベルで発生しているため、ビジネスを推進する機能を保護することは、攻撃を受けるアプリを保護することにつながります。



F5 ネットワークスジャパン合同会社

東京本社

〒107-0052 東京都港区赤坂 4-15-1 赤坂ガーデンシティ 19 階
TEL 03-5114-3210 FAX 03-5114-3201

お問い合わせ先：<https://f5.com/jp/fc/>

西日本支社

〒530-0012 大阪府大阪市北区芝田 1-1-4 阪急ターミナルビル 16 階
TEL 06-7222-3731 FAX 06-7222-3838