

利便性

自動化

クリック詐欺

アプリのセキュリティを第一に考える

DDOSからオンライン販売まで： ボットとはビジネスである

効率性

DDOS



WE MAKE APPS  SAFER

概要

割に合わない仕事や雑用をこなしてくれるクローンの軍隊が欲しいと思ったことはありませんか。少なくともインターネット上では、この夢は実現しつつあります。

実際のクローンではないかもしれませんが、ボットは大量のデジタル上の面倒な作業をこなし始めています。

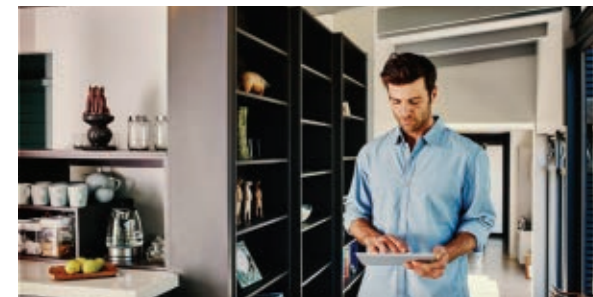
善意か悪意があるかに限らずボットとの関係を管理することは、つながる世界でビジネスをする上で不可欠なことになっています。2016年に発信されたオンライン トラフィックの半分以上が自律プログラムをその発信源としていることから、ボットが技術変化の推進力となり、定着していることは明らかです。¹

ボット技術、マシン ラーニングおよびAIが進化を続けているように、それらによる脅威も進化を続けています。ボットには善意のボットもありますが、多くは悪意のあるボットです。これらを操るサイバー犯罪者は、アプリケーションを狙っています。ボットがビジネスに与える影響に組織が対応できるように備えることは、新しいボット対応の世界に適応しながら成長できる持続的な戦略を開発する上で不可欠なことです。

¹ <https://www.recode.net/2017/5/31/15720396/internet-traffic-bots-surpass-human-2016-mary-meeker-code-conference>

51.8%

2016年のオンライン トラフィックの
51.8%はボットが発信源



朗報： ロボット イノベーションにより顧客体験が改善

現在のインターネット上での人間の定義とは何でしょうか。対話する相手が現実の人間か自律プログラムかが問題なのでしょうか。多くの状況で、ロボットは一般消費者をサポートし、そのやりたいことを消費者自身でやる場合の数分の1の時間でこなしています。

オンライン ショッピングについて考えてみます。顧客が必要な物をすでにわかっている場合、サイトをナビゲートしてそれを見つける理由はなく、代わりに便利なロボットがより効率的に注文できます。これはすでにWebの至る所で起きていることです。

ここで、iOSベースのSiriやAmazonのAlexaのような家庭内バージョンなど、ますます増加するデジタル アシスタ

ントの利用について考えてみます。これらもロボットであり、私たちの生活をより快適にすることを目的としています。人は、グラノーラ バーを切らしたときに自動的に注文できる利便性をコスト以上の価値があると判断し、これと引き換えに重要なプライバシーを犠牲にしています。² ロボットを中心とする世界の新しい現実に適応しない顧客対面の店は、この現実に適応する店にその市場シェアを奪われていることを実感しているかもしれません。

マシン ラーニングやニューラル ネットワーク技術により、ロボットがますますスマートになっているため、インターネットで増加を続けるロボット トラフィックを管理する組織戦略を設計することが不可欠です。大手の技術企

業は、これらの自律プログラムを利用して、より耐性のあるネットワークを構築し、運用を監視および維持することで、その顧客の生活をより快適にしています。しかし、ロボットは、ソフトウェアおよびビジネス プロセスの弱点を狙う攻撃者、詐欺師または競合企業の活動も快適にしています。

² <https://insights.dice.com/2017/07/14/digital-assistants-greater-us-age-adoption/>

³ <https://insights.dice.com/2017/07/14/digital-assistants-greater-us-age-adoption/>

⁴ <https://nakedsecurity.sophos.com/2017/01/27/data-privacy-day-know-the-risks-of-amazon-alexa-and-google-home/>



91%

デジタル アシスタントを利用する人の91%は、インターネット接続機器をさらに購入する可能性が高いと答えています。³

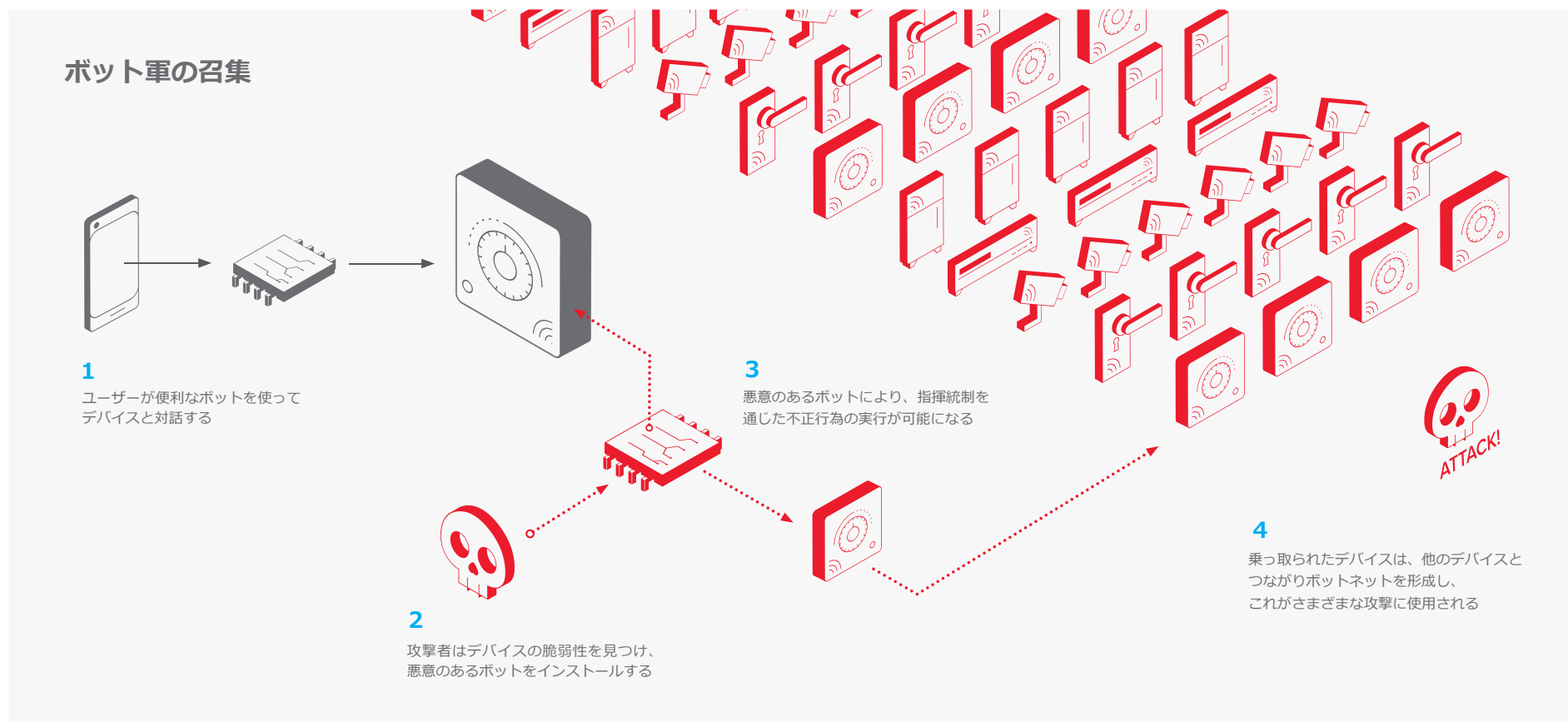
70%


ALEXAやGOOGLE HOMEなどの専用のホーム アシスタントを使用している人の70%は、その利用を始めてから1年経っていません。⁴

悲報： ボット イノベーションによりサイバー犯罪が可能に

他の便利なツールと同様に、ボットは、攻撃者の犯罪活動を最適化するために利用できます。

直面する脅威は、直接的な消費者詐欺、IP窃取、ロングテールの不当利益行為、政治的目的または些細な個人的な恨みなどの多様化する動機を背景に進化の一途をたどっていて、ボットはこれらの不正な行為に利用されています。





他の便利なツールと同様に、ボットは、攻撃者の犯罪活動を最適化するために利用できます。



DDoS攻撃

有料で使えるDDoSは、利益になり、簡単に利用できます。クラウド サービスを使用して1時間のDDoS攻撃を開始するために必要な費用はわずか4ドルです。⁵ これは、その対策に必要な費用を大きく下回ります。このようなDDoS攻撃の利用者は、攻撃を止める代わりに身代金を要求する犯罪者、または考えられる可能性としてビジネスの邪魔をして市場シェアの拡大を目論む競合会社です。MiraiなどのIoTボットネットの台頭により、犯罪者はほとんどの正当な組織の防御力を簡単に凌ぐことができます。⁶



知的財産窃取

サイバー犯罪者は、機密情報およびデータの複製にもボットを使用します。この複製を解析することで、Webコードに隠されていることがあるビデオやPDFの印刷資料、電子メール アドレスやユーザー名などの知的財産を探ることができます。また、サイバー犯罪者は、ブランド力や企業の評判が落ちるだけでなく、顧客との関係にも悪影響を及ぼす本物そっくりのフィッシング サイトの設計に役立つロゴやグラフィックも狙っています。



リソースの買いだめ (および転売)

ボットはダフ屋にとっての完璧なツールです。ダフ屋はボットを利用することで、人気イベントの大量のチケットを簡単に買い漁り、これらを異常な高値で転売します。また、限定版Yeezysの最新ペアを競って手に入れ、スニーカーマニアに異常な高値で売り付けようとする転売業者が使用するAll-in-Oneスニーカー ボットなどの自動化されたエージェントもあります。⁷



競合情報分析

航空券、ホテルの部屋、および価格が迅速に変動する旅行関連商品について、ボットは、他の業者から情報を収集し、価格を低下させ、市場における競争上の優位性を生み出すことができます。

他にもまだまだあります。マルウェア拡散からクリック詐欺まで、ボットは、サイバー犯罪者の金稼ぎに利用されています。これにより、従来の詐欺捜査員は、詐欺取引との戦いにおけるまったく新しい前線への対応にばかりきりになっています。⁸

⁵ <https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/>

⁶ <https://f5.com/labs/articles/threat-intelligence/ddos/ddoss-new-est-minions-iot-devices-v1-22426>

⁷ <https://www.cnbc.com/2017/05/13/adidas-yeezy-collectors-sneakerheads-using-bots.html>

⁸ <https://krebsonsecurity.com/tag/bot-ad-fraud/>

ボット時代におけるビジネス インテリジェンスの最適化

これらのデジタル傭兵がもたらす機会と脅威を理解した上で、組織は、サイトおよびアプリケーションを利用するボットと人間の比率をより深く掘り下げて調べ分析することが重要です。そのためには、ボットと人間のトラフィックを識別および区別するために必要なインテリジェンスを備えたツールやサービスへの投資が必要になるかもしれませんが、他のマシンからのリクエストに応えるためにどのくらいの費用を費やしているかを適切に把握できます。高度なボット管理機能を提供するウェブ アプリケーション ファイアウォール (WAF) などのツールを実装することで、ボットへのサービスに伴うコストを軽減できます。



しかし、過剰にボットを避けると、顧客がサービスを利用できる機能に悪影響を与える場合があります。人間であることを証明するために多くの時間と労力が顧客に求められれば、顧客は不満を感じ、競合会社へ乗り換えるかもしれません。

また、GoogleやBingなどのデジタル アシスタントおよび検索エンジン インデクサのような「善意」のボットをサポートできないと、見込み客がサービスを利用または認識できなくなる可能性もあります。

ここでの注意として、ボット管理に成功すると、一部のトラフィックをブロックすることになるので、サイトの統計情報（ページ ビューなど）にある程度の影響が及び、データ マイニングが、より正確にはなりませんが、ある程度異なる可能性があります。しかし、このような変化を認識してそれに備えることで、人間の顧客にサービスを提供していることを確信できます。

ボットが与える現在のセキュリティ戦略への影響

インターネット上で有害および無害の両方の自律プログラムが急増したことで、アプリケーションおよびデータを安全に保つためのこれまでの戦略の見直しが必要になることがあります。

従来のIPインテリジェンスおよびレピュテーションに基づいたフィルタリングも役に立ちますが、これらの技術は、その上を行くボットに対応できるように進化が求められる場合があります。今後、ビジネス コミュニティは、ボット検知および管理をより効果的に促進するために、暗号を使って証明できる識別子が関連付けられた長期的なレピュテーションの評価など、IPレピュテーションの代わりの方法を考える必要があります。

AI技術が進歩することで、ボットが人間と同じようにアプリケーションを使い始める可能性があり、この場合、セッションおよびワークフロー プロファイリングなどの行動特性に基づいてボットを識別しようとする努力が無駄になり得ます。いくつかのボットは、人間にも対応します。つまり、ボットには難しすぎる特殊なタスク (CAPTCHA問題を解くなど) を人間にアウトソースできます。

AI技術が進歩することで、ボットが人間と同じようにアプリケーションを使い始める可能性があります。

指揮統制システムも進化しています。サイバー犯罪者は、パブリック フォーラムやソーシャル ネットワークに投稿される画像内に隠したコマンドを伝えるため、ステガノグラフィ技術を使い始めています。これは、ボット対応マルウェア トラフィックの検知を非常に難しく、または不可能にさえするプロセスです。ハッカーがマルウェアの一部をテストし、それらのコマンドをブリットニー・スピアーズのインスタグラム アカウントのコメントに隠した、これまでにはなかった事例もあります（しかし恐らくはすでに模倣されています）。⁷

⁷ <http://gizmodo.com/russian-hackers-testing-malware-with-britney-spearss-in-1795912325>

セキュリティの現在： 多方面におけるボットとの戦い

すべてのボットをブロックできないのであれば、さまざまなボットを最適に区別し、悪意のあるボットがビジネスに損害を与えないようにブロックするにはどうすればよいでしょうか。

ボットの課題への包括的な対応を簡単にする特効薬はありませんが、インテリジェンス対応の多層防御戦略は、悪意のあるボットが組織に与える影響を軽減するだけでなく、善意のボットの促進に大いに役立ちます。以下にいくつかの手順を示します。

1. アイデンティティおよびレピュテーションを使用し、ボットと人間のトラフィックを分類して、優先順位を付けます。
2. ボットの「利用規定」を設けることで、無害なボットとの対話およびサービス提供だけでなく、それらによるサービスへの影響の管理が簡単になります。
3. ビジネス プロセスを検証し、詐欺関連の問題への対応を効率化できるようにプロセスを強化することで、組織がより安全になり、場合によっては詐欺師の注意をより弱い標的に背けることができます。
4. 実用的な脅威インテリジェンスを採用して、攻撃される可能性を判別し、その対応の優先順位を決めます。
5. 完全装備の柔軟なWAFを導入し、ボットに対する積極的な防御、ヘッドレス ブラウザの検知、フォームおよびフィールドレベルの暗号化、レイヤ7のDoS攻撃への対策、入力データの無害化、行動分析などの機能により、不要なトラフィックを軽減およびブロックします。
6. WAFなどのマシン ラーニングを採用したトラフィック管理ツールを使用し、新しい脅威や進化する脅威への対応に役立つ対策を素早く構築および実装します。

実用的な脅威インテリジェンスを採用して、攻撃される可能性を判別し、その対応の優先順位を決めます。

ボットにより、現在の通常のオンラインでの生活が変化していることは明らかです。インターネットに広がる数多くの悪意のあるボットに注目しがちですが、組織は、これらの自律プログラムがもたらす機会にも目を向ける必要があります。包括的で柔軟な戦略を開発し、ボットがビジネスに与える影響に対応することで、アプリケーションおよびデータを保護するだけでなく、組織の持続的な成長に備えることができます。

アプリケーション保護の詳細については、f5.com/securityをご覧ください。

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