

ギフトカード

映画チケット

アプリのセキュリティを第一に考える

不正行為

標的は銀行だけではない

カプチーノ

配送料金

銀行の暗証番号

自宅住所

概要

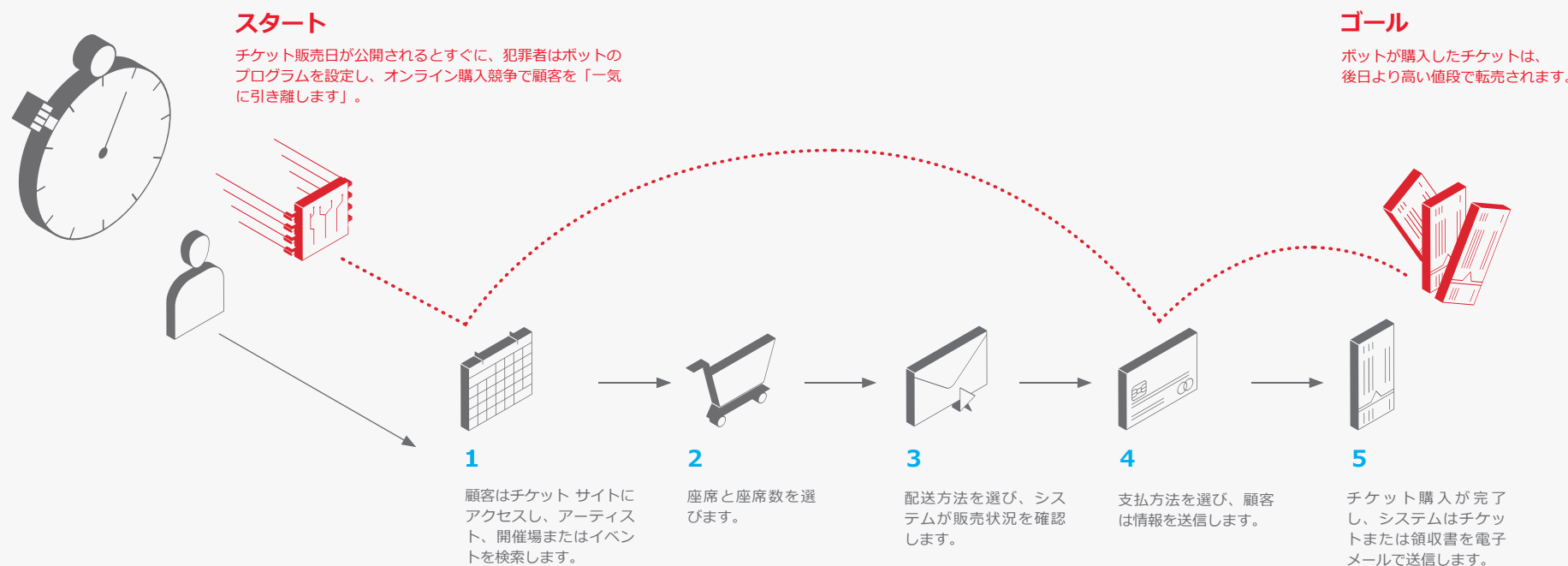
デジタル イノベーションはすべてを変えた：お金はどこにでもあるので、すべてのビジネスが不正行為の標的になる可能性があります。

銀行と金融機関は、不正行為の主な標的でした。なぜ銀行が標的になるのでしょうか。アメリカの悪名高い銀行強盗Willie Suttonの言葉を引用すれば「そこにお金があるから」です。銀行は依然として詐欺師の標的とされていますが、デジタル ビジネス イノベーションの大きな流れによりすべてが変わりました。

た。お金はどこにでもあるので、すべてのビジネスが不正行為の標的になる可能性があります。私たちが航空券、コンサートシート、または大人気のエア・ジョーダンの最安価格を見つけるときに利用できるテクノロジーは、犯罪者も利用できます。詐欺師は、自動化された顔のないボットを利用して、儲けの機会になる

ビジネス アプリを物色します。また、詐欺師は、ソフトウェアの脆弱性だけでなく、ビジネス プロセスの弱点も標的とするので、不正行為に気付かない場合もあります。

オンライン チケットを巡る競争 人間VSボット



敵を知る 不正行為のさまざまな側面

不正行為とそれを促す戦略を理解することが、効果的な検知および対策における重要な第一歩です。不正行為を特定および防止できるかどうかは、犯罪者がアプリやプロセスが脆弱かどうか評価し、そうである場合にこれを悪用できる創造的かつ複雑で、隠密に実行されるツールや戦略により、これからも永久的に試されます。



ビジネス ロジック攻撃

これらの攻撃では、コードの欠陥だけでなく、アプリケーションの動作やビジネスの仕組みが利用されます。たとえば、Webアプリで少額の購入（ピザの注文など）を行うときに、盗まれたクレジットカード番号を認証する、あるいは、毎日無料の「バーズデー コーヒー」をもらうために、コーヒー ショップのポイントプログラムに365回登録する、などです。



ダフ屋

これらのボットは、コンサート チケットや人気のスニーカーなど、一般的に限定販売される商品やサービスを買占めて転売します。ダフ屋はできるだけ多くの商品を買占め、これらの商品を後で転売して大儲けします。このような行動を認める、または見過ごしていると、正当な顧客が直接購入できないサービス拒否攻撃のような状態になり、信頼できるソースとしての評価が下がり、実際の顧客ベースを失います。



サービス拒否攻撃

サービス拒否はビジネスの拒否です。これらの攻撃は、アプリまたはサイトにその処理能力以上のリクエストを送り付け、リソースを浪費させ、実際の顧客への対応を困難（または不可能）にします。サービス拒否攻撃は、犯罪者が他の標的型攻撃を仕掛けるときの陽動作戦としても利用されます。



ヘッドレス ブラウザ

これらのツールは、乗っ取られたコンピュータのボットネットに利用されると、人間の行動を模倣して、アカウントの登録や広告のクリック（広告収入を不正に増やす）など、さまざまな目的の達成を促します。この種のツールでより高度なものでは、従来のJavaScript対応ワークフローを無効にして、ロボットやその他の自律エージェントが人間を装うプロセスを疑うことができます。



知的財産の盗難

ダフ屋は、デジタル財産を物色して、価格情報や公開されている記事、およびその他の資産などのコンテンツを盗み、別の目的に利用します。詐欺師は、この盗んだコンテンツを利用して、より安い価格を設定、潜在的な訪問者を横取り、または顧客情報を収集できます。

ボット、ボット、ボット!

現在、ボットが発信するインターネット トラフィックは、人間が発信するトラフィックを超えています。¹ その1つの理由として、通常のユーザが正当なボットにますます多くの有用性を見出していることが挙げられます。正当なボットは、インターネットのインデックス作成および検索を推進し、最適な旅行商品を見つけ、関連するコンテンツをお気に入りのWebサイトに表示します。Siri、AlexaおよびGoogleが、人間の命令に応えるパーソナル アシスタントとしてボットを利用しているように、ボットは、ビジネスと消費者の両方にとって重要なツールになっています。

しかし、ボットは詐欺師の良きパートナーでもあります。ボットは効率的かつ効果的で、質問もしないので、悪意のある行為を実施する上で欠かせない存在です。一般的に、私たちのお気に入りのアプリに利用される同じテクノロジーが、ボットを介した不正行為を可能にしています。

一部のボットは人間のフリをするように設計されています。詐欺師は、これらのソーシャル ボットを使用し、ソーシャルメディア、ディスカッション グループ、製品レビューやパブリック フォーラムを介して、製品やサービスをプロモート、さらに世論を操ろうとします。²

また、「クリック ボット」により、広告ネットワークを悪用して、多額の利益を挙げています。この巧妙で創造的な手口では、フェイク ドメインを登録して、自動化広告アルゴリズムを騙して広告を詐欺サイトに提示させます。その後、犯罪者は、「ボット ファーム」を使用してフェイク サイトにアクセスし、広告をクリックします。これ

により、世界中で1日数百万ドルを稼ぎ、企業のマーケティング予算を浪費にします。³

すべてのボットが詐欺に利用されるわけではありません。一部の自律プログラムは、インターネットをクロールして、悪用するためのWebアプリケーションの脆弱性を物色します。一般的に狙われるのは、アップデートやパッチが正しく適用されていないWebアプリケーションで、未対応の情報リークにより、これらのIDを簡単に作成できます。このようなアプリが特定されると、詐欺師は不正行為を計画できます。

一部のボットは、マルウェアの配信および伝播を可能にします。たとえば、TrickBotは、従来のボットというよりはむしろトロイの木馬を可能にするワームであり、金融業界への不正行為に幅広く利用されています。⁴これらのボットは、ソーシャル エンジニアリング、フィッシングまたはマルウェアが潜む広告を使用し、ユーザを騙してそのシステムに悪意のあるプログラムをインストールさせようとします。インストールされたマルウェアは、機密情報を収集できる金融機関の偽の複製サイトに犠牲者を送ります。

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

² <https://www.theguardian.com/technology/2017/jun/19/social-media-proganda-manipulating-public-opinion-bots-accounts-facebook-twitter>

³ <http://www.ana.net/content/show/id/botfraud-2017>

⁴ <https://f5.com/labs/articles/threat-intelligence/malware/trickbot-expands-global-targets-beyond-banks-and-payment-processors-to-crms>

⁵ <http://www.ana.net/content/show/id/botfraud-2017>

65 億

デジタル広告での不正行為による
損失は2017年で\$65億に到達すると
予想されます。⁵



A photograph of five men in dark suits and ties standing in a row against a white wall with horizontal black lines and height markings (4, 5, 6, 7). Each man is holding a laptop computer in front of his face, completely obscuring it. The laptops are silver and appear to be from the early 2000s. The scene is dimly lit, with the background wall being the primary light source.

終わりのないモグラたたきのようなゲーム： 不正行為への対抗

不正行為との戦いは、終わりのないモグラたたきゲームのようなものです。詐欺師の手口は実に巧妙で、1つの解決策や技術で包括的に防ぐことはできません。しかし、攻撃から完全に守られる環境を実現することは不可能ですが、アプリケーションをより手強い標的にする防御を実装することで、犯罪者が関心や行動を他に移す可能性が大幅に高くなります。

最適な防御は、フルプロキシ機能を備えたWebアプリケーション ファイアウォール (WAF) などのセキュリティ デバイスまたはサービスです。これは、着信と発信の両方のトラフィックを検査し、悪意のあるボット、フィッシング、サービス拒否攻撃、サイト特有の標的型攻撃に対して適切に防御

する、インターネットとアプリの間の緩衝装置として機能します。

また、レピュテーションおよびID検査を介したWeb不正行為対策、およびグローバル ボット活動を学習しこれに対応できるリスクベースの対策を提供できます。アプリケーション トラフィックを可視化することは、防御戦略を有効にするために重要です。そのため、プロキシをネットワークの中央に置くことで、不正行為に対する一連の防御を導入できるようにします。

最適な防御は、フルプロキシ機能を備えたWEBアプリケーション
ファイアウォールなどのセキュリティ デバイスまたはサービスです。



WEBアプリケーション ファイアウォール

悪意のあるスクリプトおよびインジェクションをブロックすることで、WAFは、重要な不正行為対策を構成します。既知の攻撃をブロックするほか、WAFは、「通過を許可する」既知のアプリケーション入力を定義（たとえば、入力フィールドのアルファベット以外の文字をブロック）できる「ポジティブ セキュリティ モデル」を使用します。WAFのポジティブ セキュリティ モデルは、アプリケーション自体での効果的な実行が非常に難しい、アプリケーションによる包括的な入力検証の不足を補うので、開発者は機能および機能性に集中できます。

WAFはアプリを保護するだけでなく、アプリケーション トラフィックの重要な可視化、ログ機能および統計分析を提供できます。これは、ビジネス インテリジェンス、トラフィック予測、または必要な場合はフォレンジック分析にも利用できます。



プログラマビリティ

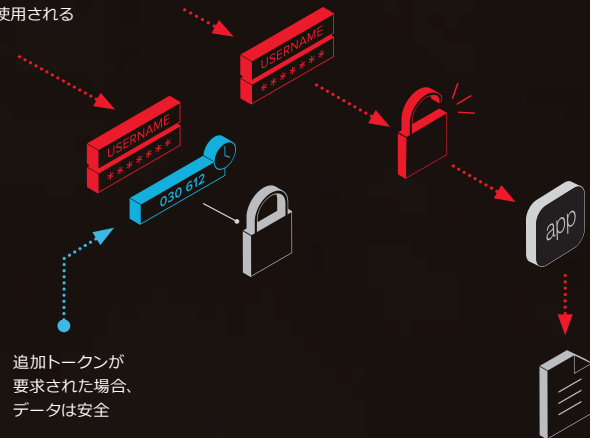
攻撃者は新しいコントロールおよび市場状況に適応するため、ポットおよび不正行為戦略は常に変化します。これらの変化の速さに適応できるツールを使用することは、効果的な防御を維持する上で有効な手段です。これは特に、個々の企業を標的としてそれに合わせた戦略を用いる不正行為キャンペーンに対応する場合に重要です。

高度なプログラマビリティ機能を備えたWAFは、個々のサービスを標的とした攻撃も防御できます。たとえば、悪意のあるエンドポイントまたは既知の正当なエンドポイントのいずれかのフィンガープリントを収集することで、さらなる課題に対応または回避するか、不正行為に関与していると判断されるエンドポイントをブロックできます。

WAFはアプリを守るだけでなく、
アプリ トラフィックの重要な
可視化、ログ機能および
統計分析も提供できます。

多要素認証はアプリ ユーザの認証要件をステップアップできます。

盗まれた認証情報は
アカウントへのアクセスに
使用される



追加トークンが
要求された場合、
データは安全

追加認証ステップがない場合、
アカウントが漏洩し、
データが流出する恐れがある



IPインテリジェンス

IPインテリジェンスは、アプリとの接続のソース ネットワークおよび地理的位置情報を検証し、そのレピュテーションベースのコンテキストを提供できます。既知の悪質な/悪意のあるアドレスまたは不適切な場所からの接続はネットワーク レベルでドロップできます。これにより、リスクを軽減するだけでなく、価値あるシステム リソースの完全性と可用性を保持でき、最終的に運用コストの節約にもなります。



アンチフィッシング

フィッシングは、詐欺師が主に利用するツールであり、実際のWebサイトおよびアプリの複製が関与します。アプリケーション プロキシは、サイト リソース（たとえばイメージ）が悪意のあるサイトから呼び出されているか検知できます。プロキシは、コンテンツをブロックし、管理者に警告できるので、悪意のあるWebサイトを特定および切り離すことができます。さらに、アンチスクレイピング テクノロジーを利用することで、プログラムによる偽造サイト複製をほぼ不可能にし、これらの偽造サイトが設立される可能性自体を軽減できます。

アプリケーション プロキシはクレデンシャル スタッフィングを検知し、これを防ぐことができます。



IDおよびアクセス コントロール

詐欺師は、盗まれた認証情報のリストを手に入れたら、一般的には、これらを他のサイトで使用して、他のアプリケーションへのアクセスを取得しようとします。ボットは、このプロセスを一括で自動化できます。この戦略は通常「クレデンシャル スタッフィング」と呼ばれます。アプリケーション プロキシは、このクレデンシャル スタッフィングを検知し、防ぐことができます。また、この同じテクノロジーで、詐欺師がボット生成パスワードを使用して継続的にアカウント認証情報を不正取得しようとする総当たり攻撃を防御できます。アプリケーション プロキシは、コンテキストベースの適応多要素認証も実装できます。これは、地理的位置情報またはアプリケーション アクションの感度などの特定の条件に基づいて、アプリ ユーザの認証要件をステップアップできます。



コンテンツ インスペクションおよび保護

発信データの検査も不正行為対策を強化できます。アプリケーション プロキシは、予期せぬ、または悪意のある情報漏洩を軽減し、それに従いポリシーを実施する取り組みにおいて、発信アプリケーション トラフィックを分析できます。たとえば、支払またはアカウント情報などの機密データが密かに抽出された場合、そのデータが詐欺師の手に渡る前に、プロキシでデータをブロックまたは文字列をスクリプトコードとして意味を持たないように無害化することができます。このようなデータには、脆弱性が検出および公開されたときに悪用される可能性があるソフトウェアIDおよびバージョンなどの一見無害に見えるデータも含まれる場合があります。




自動化ブラウジング対策

不正行為の大部分は、サイト ナビゲーションおよびブラウジングが可能な自動化ソフトウェアにより促進されます。人間以外のトラフィックをプロキシ レベルで検査することで、不正行為のリスクを軽減できます。これは、行動分析（「人間のように動作しているかどうか」）、およびセッションやIP情報が変わった場合でも人間以外のブラウザを識別および分類できるデバイス/ブラウザ フィンガープリントなどの検査を組み合わせることで実現できます。

不正行為：最適な防御は全体論的な防御

不正行為に対処するには、戦略とテクノロジーをうまく組み合わせ、継続的に努力する必要があります。不正行為を簡単に軽減することはできませんが、インターネットとアプリ間の緩衝装置としてアプリケーション プロキシを使用することが最適な防御です。アプリケーション プロキシを使用することで、適切な保護を必要な場所、つまりアプリケーションの前に適用できます。

アプリ保護、ネットワーク セキュリティ アクセス コントロール、脅威インテリジェンスおよびエンドポイント インスペクションを組み合わせることで、ビジネスに大打撃を与える前に不正行為を防ぐためのツールを手にすることができます。



不正行為に対処するには、戦略とテクノロジーをうまく組み合わせ、継続的に努力する必要があります。

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