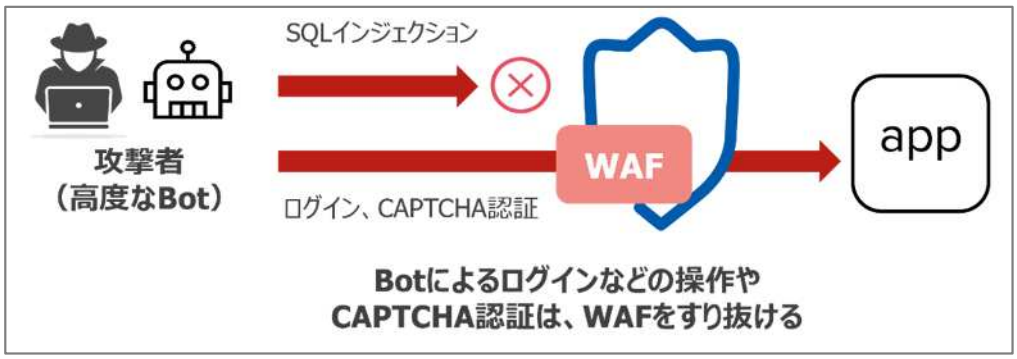
Distributed Cloud Services

買い占め・アカウント乗っ取り・クレカ不正 AI時代のBot対策ソリューション

WAFでは防げない！？近年のBot攻撃

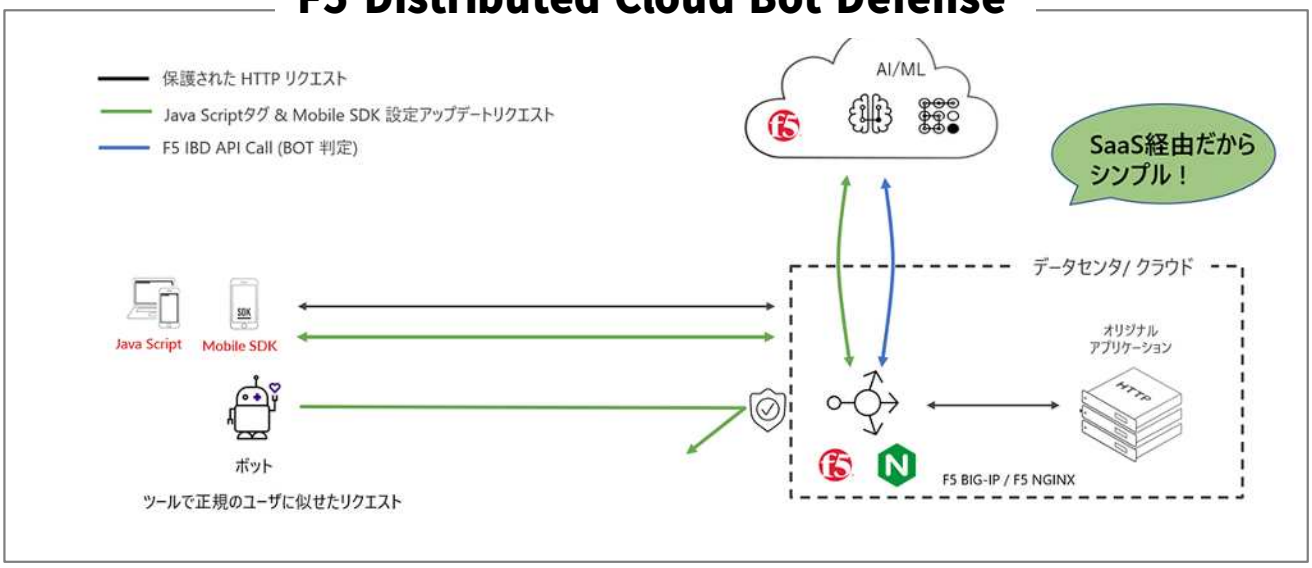
Botの通信は「ログインする」、「カート投入する」、「購入する」などの一見正常なリクエストになるため、WAFをすり抜けてしまいます。
また、一部のWAFには、CAPTCHA認証などの機能でBot対策をとることもできますが、最近のボットは人間のように巧妙に振る舞い、CAPTCHA認証すらも、すり抜けてしまいます。



AI/MLにより、高度なBotの攻撃を可視化・防御

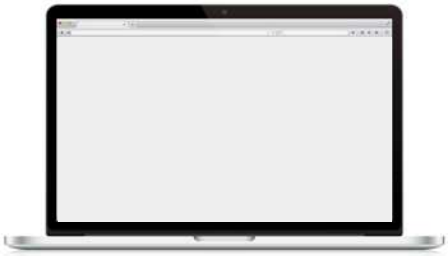
「F5 Distributed Cloud Bot Defense」 は、進化するBot攻撃に対抗する次世代のセキュリティソリューションです。
ECサイトでの商品買い占め、リスト型攻撃による不正ログイン、フェイクアカウント登録、カーディングなど、巧妙化するBotによる脅威に対し、ユーザーの行動・環境・意図を多面的に分析し、高精度にBotを識別・遮断します。

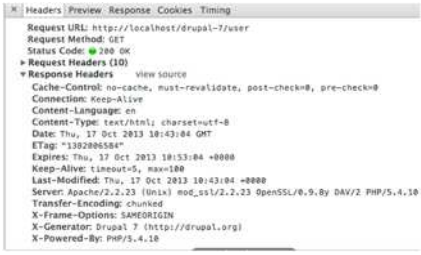
F5 Distributed Cloud Bot Defense



東京エレクトロン デバイス

AI/MLにより、3つの情報を複合的に分析
「人間か？Botか？」を判断





環境情報 (Environment)
誰が？

振る舞い情報 (Behavior)
どのように？

ネットワーク情報 (Network)
どこから？

JS

これらのシグナル情報をJavaScriptで収集・取得

Bot Defenseで防げる攻撃一例

攻撃名	概要
クレジットマスター攻撃	実在するクレジットカード番号を総当たりで自動生成・試行して特定する攻撃手法。見つけたカードは不正購入や転売に悪用される。
クレデンシャルスタッフィング	盗まれたユーザー名とパスワードのペアを用いて大量のログインを試行する攻撃。他のサービスから流出したIDとパスワードの組み合わせを使い回して、不正ログインを試みる攻撃。
ギフトカードクラッキング	攻撃者が有効なギフトカード番号とPINコードを不正に取得して使用する行為。攻撃者は、有効なカード番号を特定し、正規顧客がギフトカードを使用する前に、そのギフトカードを使用または販売する。
スクレイピング	攻撃者は自動化ツールを使用して、ターゲット アプリケーションから大量のデータを収集し、そのデータを他の場所で再利用する。
フェイクアカウント	不正に作成されたアカウントを通じて、ポイントやクーポン不正に取得、報酬制度の悪用やマネーロンダリングなどの金銭的犯罪が行う。サービスの健全性やブランドの信頼性にも深刻な影響を与える可能性がある。
Credit Application Fraud（クレジット申込詐欺）	攻撃者は盗んだ個人識別情報 (PII) を使用して、他人の名前でアカウントを開設。他人になりすましたり、虚偽の情報を用いてクレジットカードやローンなどの信用取引の申請を行い、不正に信用枠や融資を得ようとする詐欺行為。

メーカーマニュアルリンク：保護できる攻撃一例
https://docs.cloud.f5.com/docs-v2/bot-defense/plan-bot-advanced/concepts#types-of-attacks

本紙に記載された会社名、ロゴ、ブランド名、製品名、サービス名は各社の商標または登録商標です。
その他全ての商標および登録商標はそれぞれの所有者に帰属します。

東京エレクトロン デバイス株式会社
CN BU
https://cn.teldevice.co.jp/
本社：〒150-6234 東京都渋谷区桜丘町１番１号
渋谷サクラステージ SHIBUYAタワー35階

名古屋：〒451-0045 愛知県名古屋市西区名駅2-27-8
名古屋プライムセントラルタワー8階

大阪:〒530-0001
大阪市北区梅田3-2-123イノゲート大阪 17階