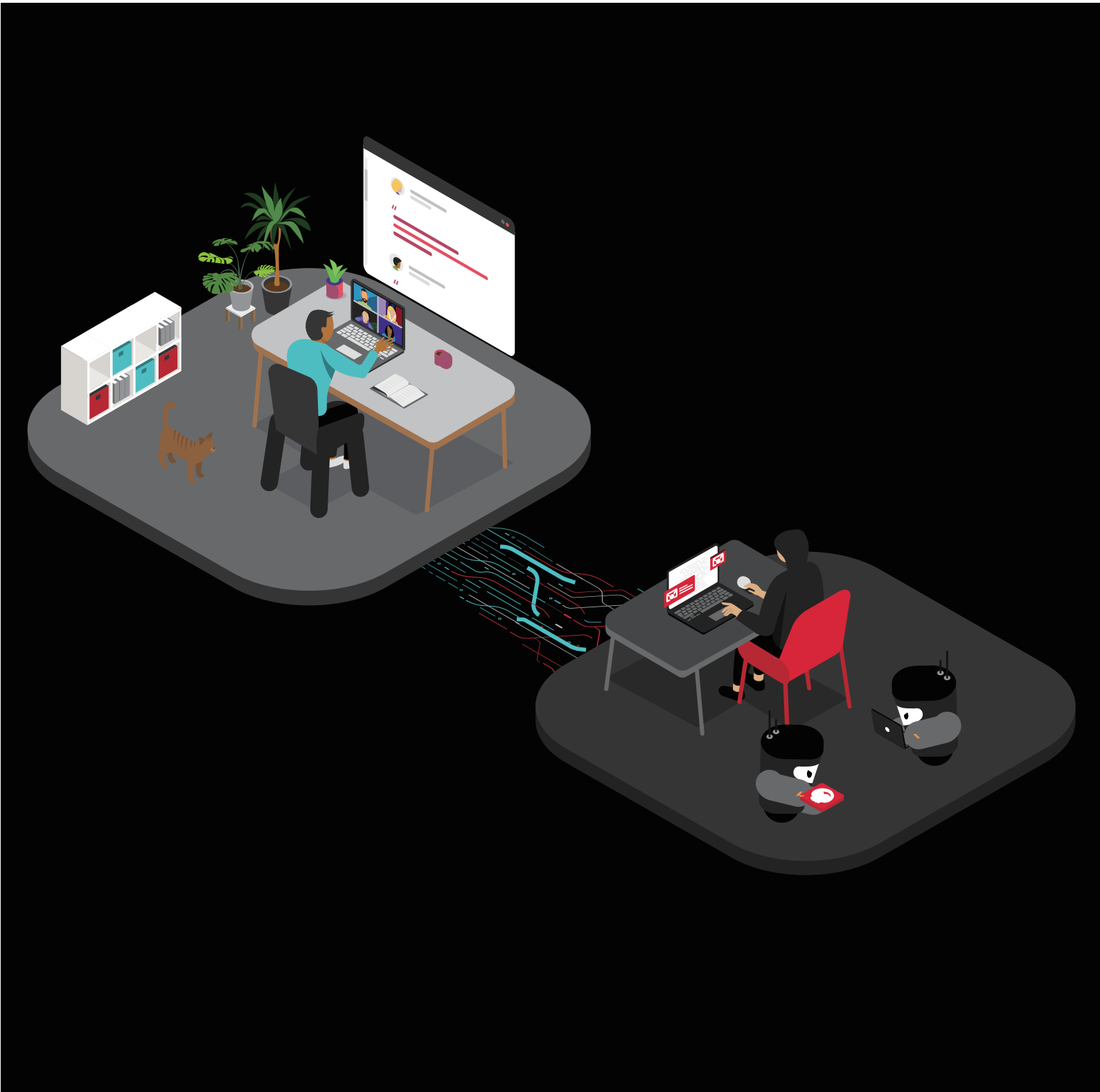
Part of F5

ログイン離脱解消で増収達成

一般的な「ログイン」がサイトの売り上げに限界をもたらしているワケ

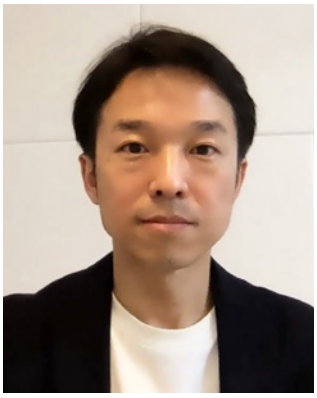


オンライン会員サイトでアクティブユーザーを増やす近道は何なのか？　実は、UI や購入フローを見直す前に、真っ先に目を向けたいことがある。それが、ログイン失敗からの離脱ユーザーをすくいあげ、カスタマーエクスペリエンスを向上させることだ。

EC サイトでログインに失敗する――これは、多くの人に共通する経験だろう。失敗しても、正しいパスワードを入れ直す、またはパスワードを再発行することでログインはできるが、当然そのまま離脱するユーザーも一定数いる。

自粛生活が続き「買い物や手続きはネットで」という人が増えている今、EC サイトをはじめとするオンライン会員サイトを集客チャンネルとして強化することは勝機になり得る。しかし、SEO 対策や広告などを駆使してサイトにアクセスしてもらっても、ログインの失敗で購入・利用者を逃してしまうのは、あまりにもったいない。

ログインに失敗するかどうかはユーザー次第であり、サイト側でコントロールできることではないように思えるが、実はそうではない。



F5 ネットワークスジャパンでクラウドソリューション営業部長を務める常川啓明氏。取材はオンラインで実施した

なぜなら、その背景にはサイト側のセキュリティ対策が大きく関係しているからだ。

セキュリティ対策の“ジョーシキ”がアダになる

通常、オンライン会員サイトはログイン後のセッション時間を定めて、一定期間アクションがなければ自動的にログアウトする仕組みになっている。セッション時間が長いほど不正アクセスによるアカウント乗っ取り、また誤操作による購入といったリスクが高まるためだ。こうした“短時間セッション”はオンライン会員サイトの標準的なセキュリティ対策といえるだろう。

しかし、ユーザー側からするとどうだろうか。「不正利用の防止を目的とした短時間の Web セッションは、カスタマーエクスペリエンス（CX）の低下を招き、利用客を減らす“機会損失”につながっています」。そう言い切るのは、F5 ネットワークスジャパン（以下 F5）でクラウドソリューション営業部長を務める常川啓明氏だ。

例えば、購入を迷っていた商品を取りあえずカートに入れて、検討した上、後日決済するという流れはよくあること。しかし、再びログインを求められ失敗したら――。F5 が日米大手である複数の EC サイト、金融事業者のオンラインサービスを対象に行った調査によると、再ログインの際、約 60%が初回の試みで成功、約 30%が複数回の試みで成功、そして約 10%は失敗してサイトを離脱していることが分かったという。

ログインに失敗して、「もういいや」。多くの人に心当たりがあるのでは？（画像はイメージ、出所：ゲッティイメージズ）

「ログインに成功している合計 90%の内、約 35%はその後の購入につながっていました。しかし、ログインに失敗した 10%はそもそもお店に入れていない状態です。より細部まで調べてみると、ログインに失敗した人のうち 20%は購入履歴がある優良ユーザーであり、収益チャンスを逃していることが判明しました」（常川氏）

短時間セッションはユーザーの安全を確保するためのものだが、それによってカスタマーエクスペリエンスを損なっているとは、なんとも悩ましい状況である。そこで、そんな“ログインにおける摩擦”を解消するソリューションとして登場したのが、F5 が提供する「Shape Recognize（シェイプ レコグナイズ）」だ。

そのログインは不正か、正当か？

Shape Recognize は、ログインというアクションを対象に、不正ユーザーか優良ユーザーかを見極める機能を持っている。もっと詳しく説明すると、「購入履歴はあるか」「怪しいふるまいはないか」といったユーザーの挙動をセンシング（観測）できる JavaScript を活用することで、ユーザーの質を判別し、サイト側へレコメンドする仕組みだ。

「クライアント一つとっても、Google Chrome や Firefox などではなく、攻撃を仕掛けてくるユーザーは特殊なブラウザやツールを利用する傾向にあります。また、ブラウザの拡張機能が作動している、一般的にはあまり使わないファンクションキーを多用している、普段と異なる場所やデバイスで利用している――といった動作も判断材料になります。こういったいくつもの情報を掛け合わせ、『今ログインしようとしているのはどういうユーザーか』をサイトに対しレコメンドするのが、Shape Recognize の役割です」（常川氏）

Shape Recognize からのレコメンドを参考に、例えばサイト側は以下のようなアクションを設定できる。

怪しいユーザー

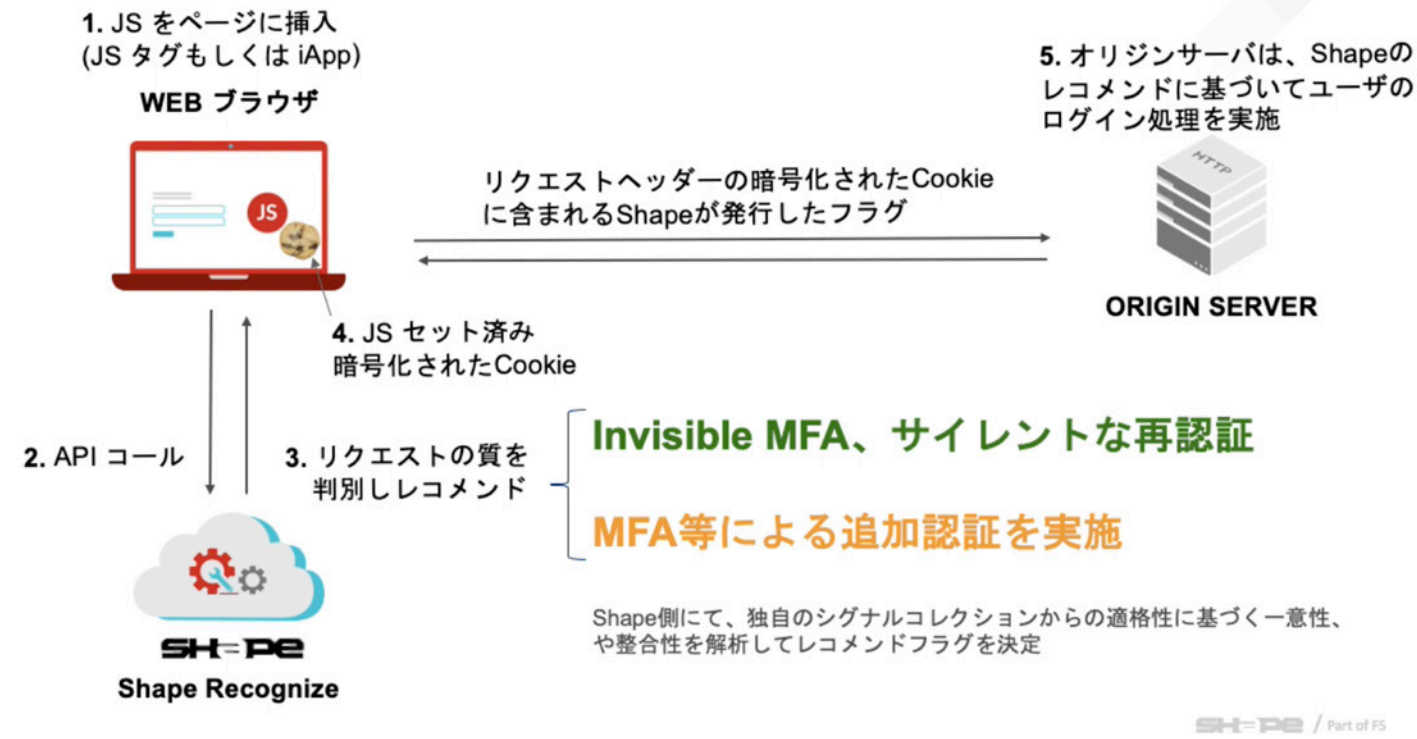
→　MFA（多要素認証）でログイン

正当性が認められるユーザー

→　短期間セッションでログイン

より優良と認められるユーザー

→　セッションを拡張しログイン



Web テクノロジーの中では必要不可欠な JavaScript 技術を使い、瞬時にユーザーの動向を捉える

ただ決められた条件に沿ってセンシングするだけではない。「サービスを導入していただく際、『こういったふるまいは危険度が高い／低い』といったデフォルトのデータセットはご提供しています。しかし、そこからサイト側の判断に基づき、われわれが細かくチューニングすることでより最適化されたルールにブラッシュアップします」（常川氏）

サイレント認証で年約20億円の増収を達成

以上の認証作業は、もちろんユーザー側からは一切見えない。「サイレントな再認証」により、画一的なセキュリティゲートを取り払い、10%の離脱ユーザーを意図せずブロックしていた現状を脱却できることになる。加えて、ユーザー全体のフラストレーション軽減にもなるため、「来店者→購入者へのコンバージョン（転換）も改善しやすくなります」と常川氏は話す。

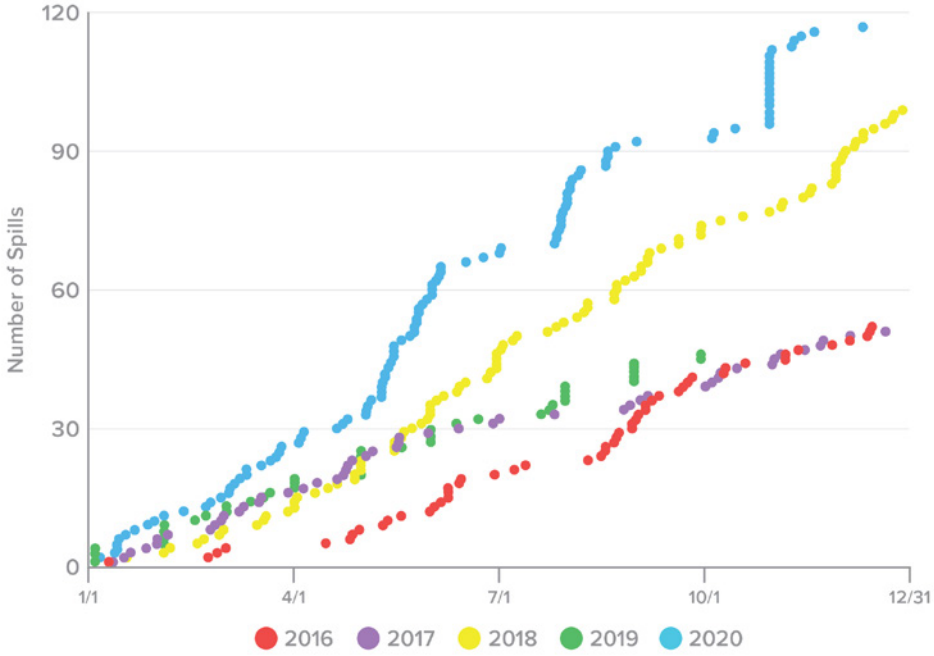
実際に、前述の日米大手 EC サイトで AB テストを実施したところ、Shape Recognize 導入後は、未導入時と比較して 40%の手動ログイン削減に成功。コンバージョンレートが 6.1%向上したことで、1 日あたりの購入客数は 750 人増加し、年間約 20 億円の売り上げ増加が見込めるという。

ユーザー訪問数が多い大手サイトであるほど、ログイン時の失敗を解消することで利幅が大きいことが分かる結果といえよう。

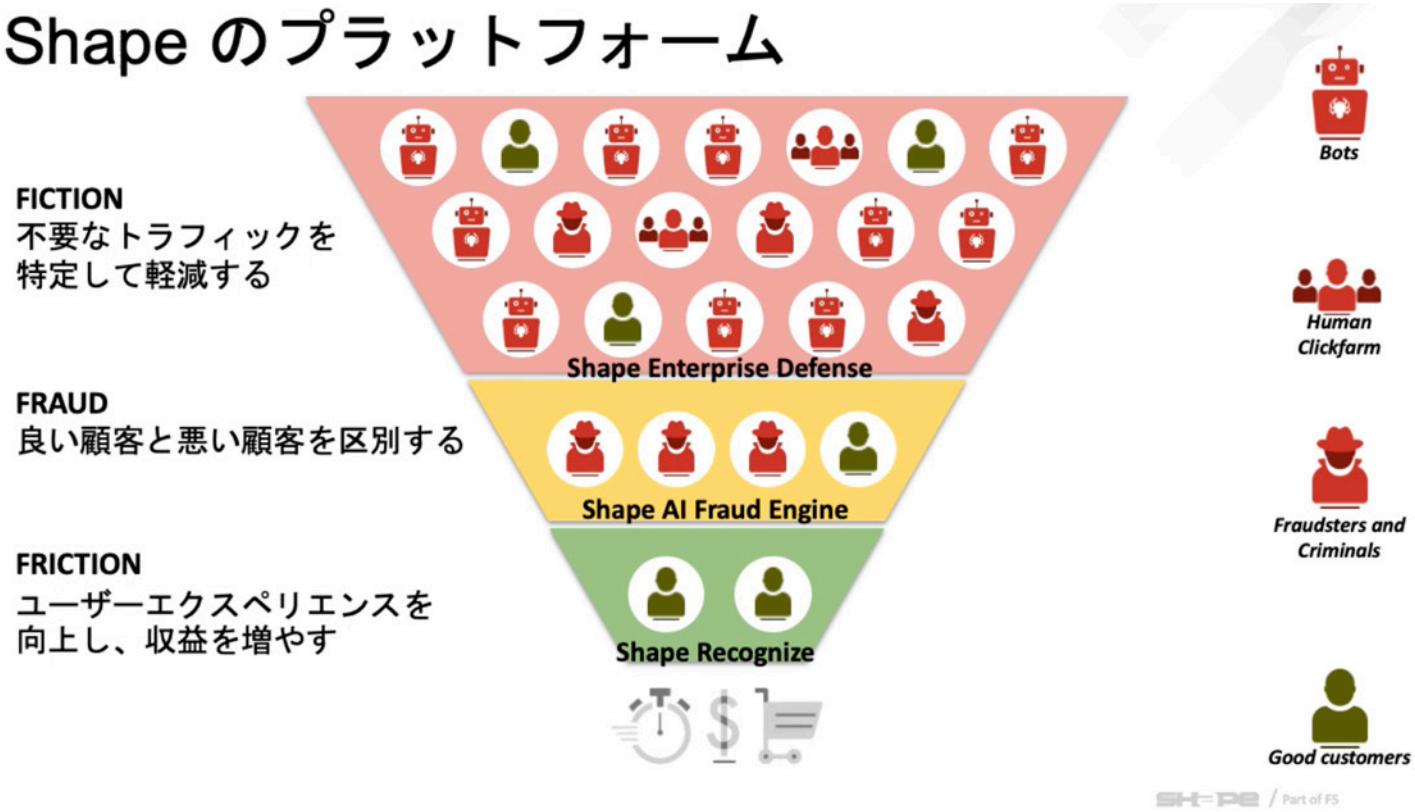
日本のサイトにとっても同様の課題、影響は大きく変わらない。「インターネットはオープンだからこそ産業としても発展していますが、それと比例して国に関係なく悪意のあるアクセスも増加しています」（常川氏）

増加するネット上の脅威、世界規模の収集データで応戦

F5 が Shape Security 社（以下 Shape）と統合し、Shape Recognize の開発に乗り出したのは、不正アクセスが急増しはじめた 2020 年だった。



ここ数年、ネット上で攻撃手法として主流だという「クレデンシャルスタッフィング（不正目的でアカウント情報などを盗む攻撃）」の増加推移を表したグラフ。20 年はコロナの影響で一気に増加した（出典：F5 Labs 2021 Credential Stuffing Report「Figure 8. Rate of credential spill incidents over each calendar year, 2016-2020.」）



Shape Recognize をはじめとする、Shape のプラットフォーム。総合的に導入することで、セキュリティ対策を強固にする

F5 は、ロードバランサー「BIG-IP」をはじめ多くのアプリケーションサービスでグローバルに市場をけん引してきた。導入企業も、大手通信事業者や銀行など多岐にわたる。一方 Shape は、米国国防総省や CIA、Google などで AI とサイバーセキュリティの一翼を担ってきたメンバーにより創業され、そして成長してきた、いわばアメリカ国家のお墨付きともいえる技術力を持つ会社だ。Shape Recognize には、そんな Shape が培ってきた技量が惜しみなく活用されている。

日々、攻撃手法が変化するインターネットの世界では、静的なセキュリティ対策はいつか突破されてしまう。Shape Recognize は、Shape が世界規模で収集した不正行為データを照合しながら、常時アップデートを重ねている。並行して、前述の通りサイトごとのチューニングも実施されるため、ダブルで最適化を行っていることになる。

「インターネット全体のアクセスで見たとき、半分以上は不正なトラフィックである」と、常川氏は話す。新しい攻撃手法とセキュリティ技術の登場は、国に関係なくいたちごっこ状態が続いていく。そんな中でサイトが収益を確保していくためには、「セキュリティ強化とカスタマーエクスペリエンスをてんびんにかけるのではなく、両立させることが重要です」（常川氏）

Shape Recognize をはじめとする最新技術により、それを可能とする土台はすでに整っているといえるだろう。

F5 では、Shape との統合により、今まで IPS や WAF※ではカバーし切れなかった、不正かどうかを見分けにくい分野でのセキュリティソリューション強化に力を注いでいる。

bot など自動化された攻撃を判別し、アプリケーションを高度に保護する「Shape Enterprise Defense（シェイプ エンタープライズ ディフェンス）」や、サイトへの不正なアクセスを見つけ出し遮断する「Shape AI Fraud Engine（シェイプ エーアイ フロードエンジン ）」など、Shape Recognize の姉妹ソリューションはすでに世界で活用されており、前者に関しては日本でも導入企業を増やしているという。

日本を含む、世界で数多くの実績と高い評価を得ている F5 のソリューション。ぜひ自社サイトの収益向上に役立ててはいかがだろうか。

※ IPS：不正侵入防止システム。OS やミドルウェアなどの脆弱性を突いた攻撃に対応する。WAF：Web アプリケーションファイアウォール。Web アプリケーションの脆弱性を突いた攻撃に対応する。

● 製品や F5 に関するお問い合わせは、以下の URL のお問い合わせフォームよりご連絡ください。
https://www.f5.com/ja_jp/ContactFormJP

※この冊子は、ITmedia ビジネスオンライン（https://www.itmedia.co.jp/business/）に 2021 年 6 月に掲載されたコンテンツを再構成したものです。
https://www.itmedia.co.jp/business/articles/2106/14/news003.html