

上場を機に攻撃が増えたサイトに 次世代 WAF を導入 導入の手間なく、 低コストで期待どおり攻撃を事前に遮断

食に詳しい人や好みの合う人の口コミから、自分にぴったりなお店を探ることができるRetty株式会社。同社は上場を機に増えた実名口コミグルメサービス「Retty（以下、Retty）」への不正アクセス対策の一環として、Fastly の次世代 WAF を採用。次世代WAFの基本機能として期待していた「攻撃を事前に遮断したい」、および「特定のリクエストを遮断したい」という効果を十分に発揮している。

誤検知率の低さなど、機能面、運用面を評価して Fastly 次世代 WAF を採用

月間4,000万人が利用する Retty。最大の特長は、ユーザーアカウントを実名で登録することである。飲食店の情報はすべて実名で投稿されるので、批評的な口コミは少なく、ポジティブなオススメの言葉、信頼性の高い投稿が多い。2021年11月より、特定のジャンルに詳しい人達がオススメするお店が「〇〇好きの人気店」として表示される新たな機能の提供も開始。これまで以上に好みに合った飲食店探しができるようになっている。

Software Engineer の幸田優哉氏は、「リアルな場では、自分と好みの合う人や食に詳しい人からオススメのお店を聞いて飲食店を選ぶことが多いですね。そんな体験をインターネット上に作ったのが Retty です。その中で食に詳しく、ほかの利用者がお店を選ぶときの参考になる投稿をしているユーザーを Retty TOP USER に認定しています。食に詳しいユーザー同士がつながるコミュニティが育っていることも特徴の1つです」と話す。

Retty では、2020年10月の上場をきっかけに、ウェブサイトへの攻撃と思われるリクエストが増えている。幸田氏は、「以前より攻撃があることはアクセスログなどで認識していましたが、上場以降攻撃を受ける頻度が高くなり、短時間に大量のリクエストを送信する bot によりデータベースの負荷が高くなるなど、外部からの攻撃が起因でサービスに影響が出る機会が増えてきました」と話す。

そこで他社の WAF を導入したが、細かいチューニングを行わないデフォルトのルールでは、正当なリクエストであるにも関わらず攻撃と判定される False Positive（偽陽性）と呼ばれる誤検知が大量に記録された。また誤検知を無くそうとすると、各ページやリクエストに合わせて細かく正規表現を調整するようなチューニングが必要になり、自社だけで運用するのはリソース的にもコスト的にも現実的ではなかったことから導入を断念した。

これをきっかけに別の WAF を導入するための検討を開始。採用のポイントは「細かいルールのチューニング」や「継続的なルールのアップデート」が不要なこと。いくつかの WAF を比較検討した結果、Fastly 次世代 WAF の採用を決定した。採用を決めた最大の理由は、誤検知率の低さである。次世代 WAF の存在を知ったのは、Fastly 主催のイベントである Yamagoya Traverse 2020で発表された事例だった。



社名:Retty株式会社

2010年11月に設立。「新たな『食体験』を創り上げ、人生をもっと Happy に。」という新しいビジョンに基づいて、2011年6月より実名口コミグルメサービス「Retty」を運営。2020年8月には、スマートフォンで注文できる店内モバイルオーダーサービス「RettyOrder」も提供。テクノロジーを活用することで新たな食体験を創造し、外食を楽しむユーザーはもちろん、飲食店の経営者や従業員、食材を提供する生産者など、食に関わるすべての人をハッピーにする「BESTなお店が見つかる」体験を推進する。2020年10月30日には、東京証券取引所マザーズに上場している。

住所:〒108-0073 東京都港区三田 1-4-1

住友不動産麻布十番ビル 3F

URL:<https://retty.me/>

幸田氏は、「そこで2021年1月に、次世代 WAF の機能面、運用面などの情報を Fastlyの担当者にヒアリングし、4月に PoC（概念実証）の実施に至りました。PoC では、実際のトラフィックを利用して誤検知がないか、どのような設定ができるのかなどを検証し、問題がないことが確認できたことから2021年11月に本番環境への組み込みを完了しました」と話している。

次世代 WAF の本番環境への導入では、Cloud WAF と Agent WAF の両方を採用

次世代 WAF の本番環境への導入では、エージェントの管理が不要な Cloud WAF と独自にエージェントをセットアップする Agent WAF の両方が採用されている。具体的な用途としては、転送量が少なく比較的規模の小さい店舗向けのシステムには Cloud WAF を利用し、転送量が多く比較的規模の大きいユーザー向けシステムには必要に応じて段階的、部分的に導入することもできる Agent WAF を利用している。

幸田氏は、「環境構築では、エージェントのセットアップや本番環境への導入はほとんど迷うことなく完了させることができました。Cloud WAF に至っては、DNS レコードを切り替えるだけで組み込みが完了するので非常に手軽に導入することができます。運用面でも作業の負荷はほとんどなく、Agent WAF を利用しているので SigSci Agent の更新作業が必要ですが、更新作業を自動化しているので運用コストはほぼゼロです」と話す。

また、Fastly で公式に提供されている Terraform Provider を利用することで、WAF のルールなどを Terraform で設定し、管理、運用することができる。これにより、WAF のルールの変更や追加を Git の履歴として残すことが可能。CI/CD パイプラインを整備することで、レビューのプロセスを整備することもできる。

幸田氏は、「WAF に誤ったブロックルールを適用してしまうと、通常のリクエストがブロックされるなどのインシデントにもつながります。設定をコード化し、Pull Request によるレビューのプロセスを整備することでこういったミスを防ぐことができ、また必要があれば設定のロールバックなども簡単に行うことができるので本当に便利です」と話す。

次世代 WAF の基本的な機能の効果はすべて期待どおり

WAF 導入前に期待していた「攻撃を事前に遮断したい」「特定のリクエストを遮断したい」という効果は、Fastly 次世代 WAF で十分に発揮できている。幸田氏は、「実際にリクエストをモニタリングし、デフォルトのルールでは拾いきれないブロックルールを追加したり、過剰なリクエストを送信してくる bot を遮断したりするなど、サービスは十分に守られていると感じています」と話す。

また、Web ダッシュボードが非常に分かりやすいこと、Terraform Provider が公式に提供されていること、各種 API が充実していることなど、開発者にとって便利な機能が多いことも次世代 WAF を導入した決め手になった。幸田氏は、「環境構築や管理、運用において苦労することはほとんどありませんでした。PoC 期間中に Web ダッシュボード上に正しくクライアントの IP アドレスが表示されないという不具合が発生しましたが、Fastly の担当者の迅速なサポートのおかげで、原因をすぐに特定し解決することができました」と話す。

「想定外の効果としては、想像以上にチューニングが不要なこと、誤検知が少ないことです。公式ページに、『ルールの調整や継続的なメンテナンスが不要』『90%以上の顧客が WAF でブロックモードを有効化している』といった記述がありましたが、これが文字どおりで、ルールの調整や継続的なメンテナンスはほとんど必要ありませんでした。正直、半信半疑でしたが、実際に導入してみると想像以上の精度の高さで驚きました」（幸田氏）。

さらに Fastly のサポートについて幸田氏は、次のように話す。「次世代 WAF の機能面も気に入っていますが、個人的にはサポート体制の充実も素晴らしいと感じています。PoC 実施時には、専用の Slack ワークスペースを作成してもらい、質問対応など素早いやり取りが可能で、作業が非常に進めやすかったです。本番環境への組み込み時も、リアルタイムでトラフィック状況をモニタリングしてもらえなど、非常に手厚いサポートだと感じました」

今後の取り組みについて幸田氏は、「ルールの細かいチューニングなど、よりセキュアにするためにできることは、まだまだたくさん残っているので、引き続き対応を続けていく予定です。またマイクロサービス化に伴い、本番環境で GraphQL を採用している部分も増えているので、Fastly で提供している GraphQL インспекションの利用も検討したいと思っています。Fastly には、そのためのサポートを今後も期待しています」と話している。



Software Engineer
幸田 優哉 氏

お問い合わせ



✉ japan@fastly.com

🐦 @FastlyJapan

🌐 www.fastly.com/jp

📘 @FastlyEdgeCloudJapan

fastly

Retty

© 2023 Fastly, Inc. All Rights Reserved

