

Taichung Bank Securities Investment Trust が Akamai を活用してインターネットの速度と DDoS 防御を強化



「サイバー攻撃とコンピューターウイルスは日々変化しています。これに対抗して情報セキュリティの防御および早期警告システムを強化するため、Taichung Bank はここ数年大きな目標をいくつか設定してきました。」 – Taichung Bank Securities Investment Trust の Information Office Manager, Peng Zhenqian 氏

Taichung Bank Securities Investment Trust は、台湾 17 番目の国内証券投資信託会社として 1995 年に創設されました。株式ファンド、国内 MMF (マネー・マーケット・ファンド)、海外株式ファンドなどの商品を扱っています。同社は 20 年以上にわたり、堅実と信頼を戦略としてビジネスを確立してきました。安定した投資率の金融商品を慎重に開発することで、同社のファンドは業界有数の実績をあげています。現在、Taichung Bank Securities Investment Trust は、金融テクノロジーを活用し、利用しやすく革新的な投資サービスを、より多くのチャネルを通じて投資者に提供しています。

同社の Investment and Information 部門の Information Office でマネージャーを務める Peng Zhenqian 氏によると、同社はここ数年、急速に変化するサイバー攻撃やコンピューターウイルスに対抗するため、情報セキュリティ防御システムと情報セキュリティ早期警告システムの強化に関する目標をいくつか設定してきたとのことです。

第 1 の目標は社内セキュリティの改善です。社内のセキュリティが改善されれば、投資部門が毎日行う多数の調査レポートや金融情報の受信と保存が安全になり、しかも、トレーダーはリアルタイムの情報を取得して円滑かつ自由に市場にアクセスできます。第 2 の目標は外部セキュリティの改善です。外部セキュリティの改善によって、投資者は、取引プラットフォームを通じてファンドの申し込み、償還、転換などを行う際に、ハッカーによるサービス停止や個人情報の盗み取りを心配せずに済むようになります。

Taichung Bank Securities Investment Trust は、この 2 つの目標を達成するためには Web Application Firewall (WAF) サービスとコンテンツ・デリバリー・ネットワーク (CDN) サービスの導入が必要であると認識しました。これらのサービスを活用すれば、DDoS 攻撃を効果的に防御し、Web ページをスピードアップできます。入念な評価の結果、同社は Akamai ソリューションの導入を決め、2020 年 5 月に正式に導入しました。



会社名

Taichung Bank Securities Investment Trust Co., Ltd.
台北、台湾
tcbisic.com.tw

業種

金融サービス

ソリューション

- Web Application Protector および DSA
- コンテンツ・デリバリー・ネットワーク
- NetStorage
- Site Accelerator
- Kona Site Defender

主な影響

- Taichung Bank Securities Investment Trust の Web サイトの速度とパフォーマンスの向上
- DDoS 防御の強化
- ハッキング防止機能の強化

まとめ

Taichung Bank Securities Investment Trust が Akamai を活用してインターネットの速度と DDoS 防御を強化

Taichung Bank Securities Investment Trust が Akamai を活用してインターネットの速度と DDoS 防御を強化

トラフィックスクラビングの予算を削減

Peng Zhenqian 氏は、ここ数年、注目すべきランサム DDoS インシデントが多数発生していることに言及しました。特に、金融業界はハッカーの最大の標的であり、投資信託会社や信販会社も例外ではありません。Taichung Bank Securities Investment Trust は常に Web サイトのダウンタイム回避を最優先事項と考えてきました。今はほとんどの金融取引がネットワークを介して行われているためです。ファンドを償還する投資者も、情報を受信する投資調査部の従業員も、その日の市場変動に合わせてファンドを調整するファンドマネージャーも、みなインターネットを頼りにしています。ネットワークの 1 つの領域が停止するだけで、こうした作業すべてに影響が及びます。

同社は数年前、まず、このようなダウンタイムの発生を回避するために、WAF サービスと CDN サービスを導入しました。当初は社内開発による WAF ソリューションの構築を検討しましたが、メンテナンスや更新に多大な時間と資源を要することがわかり、専門ベンダーのサービスに資金を投じることにしました。ベンダーには、世界の攻撃傾向に関する知識や、自動ルール調整アルゴリズムがあり、これらを活用することで、Taichung Bank Securities Investment Trust はメンテナンスの負担を軽減できます。

DDoS 攻撃によって 100 Gbps のトラフィックが生成されても、同社が支払うのはスクラブされたトラフィックの料金だけです。これにより情報セキュリティ予算から不要な支出を除くことができます。

Peng Zhenqian 氏と情報部門のメンバーは、既存の WAF サービスも検討しました。一般的に WAF サービスの料金は攻撃ボリュームに基づいて決まります。1 Gbps のソリューションを選択していても、ある日 1 Gbps を超える攻撃トラフィックが発生するかもしれません。その場合、サービスプロバイダーは顧客に追加ボリュームを購入するよう求めます。これを断れば、防御は無いも同然です。しかし、追加ボリュームは高価であり、いったんボリュームを増やせば、その後もとに戻すことはほぼ不可能となります。たとえば、ある顧客が 1 Gbps のソリューションを購入した後で、攻撃に耐えるためにボリュームを 5 Gbps に増強したとします。その顧客はその後、5 Gbps 分の料金を支払うことになり、経済的な負担は徐々に重くなっていきます。

「DDoS は散発的に発生し、そのトラフィックは常に不規則で予測不能です」と Peng Zhenqian 氏は述べます。そのため、1 Gbps、5 Gbps、10 Gbps、それ以上と、どれだけ多くのボリュームを購入しても、安心は得られません。こうしたことから、Taichung Bank Securities Investment Trust は、それまでの WAF 契約が満期となるタイミングで、よりニーズに適したソリューションに切り替えることにしました。同社が選んだのは、Akamai の WAF、Site Shield、DSA (CDN) などのサービスです。

Akamai が選ばれたのは、エージェンシーパートナーである Sysage Technology を通じ、生成トラフィック量に対して料金を支払うプランが可能だったからです。つまり、DDoS 攻撃によって、5 Gbps、10 Gbps、あるいは 100 Gbps のトラフィックが生成されたとしても、同社が支払うのはスクラブされたトラフィック量に対する料金だけです。これにより、Taichung Bank Securities Investment Trust は、情報セキュリティ予算から不要な支出を除くことができます。

Taichung Bank Securities Investment Trust が Akamai を活用してインターネットの速度と DDoS 防御を強化

IP アドレスを隠してハッカーの攻撃を軽減

2019 年に、所轄官庁がクロスボーダーネットワーク攻撃と防御の演習を実施しました。すべての参加者のなかで、Akamai WAP プラットフォームは高いパフォーマンスを示し、3 Gbps のテスト攻撃トラフィックの処理に成功しました。これは金融業界が求めるボリュームに相当します。この結果により、Akamai ソリューションの購入に対する Taichung Bank Investment Trust の信頼感はずまます高まりました。

Akamai は世界最大規模のクラウド・インターネット・プラットフォームを維持し、毎日膨大な量の Web トラフィックを処理しています。そのため、Akamai には、ビッグデータ解析を活用してさまざまな脅威を効果的に特定する能力があります。これは、Taichung Bank Securities Investment Trust が DDoS 防御、Web セキュリティ、速度をバランスよく改善していくために役立ちます。Peng Zhenqian 氏が最も注目したのは、効率よく防御層を追加できる Akamai 独自の Site Shield サービスでした。

ほとんどの WAF サービスや CDN サービスでは、みな同様のプロキシモードの動作が採用されています。ユーザーはまず CDN サーバーに接続し、トラフィックがクリーンであることが確認された場合にのみ、アプリケーションオリジンに到達できます。しかし問題なのは、通常、ハッカーはプロキシを迂回し、IP アドレスを使用してアプリケーションオリジンに直接到達しようとする

点です。Site Shield サービスを使用すれば、Taichung Bank Securities Investment Trust は同社の IP アドレスを隠し、ハッカーの検知範囲から逃れることができるため、攻撃を受ける可能性が著しく軽減されます。

5 月の導入前に、Taichung Bank Securities Investment Trust は 2 か月間の概念実証 (POC) を行いました。この段階で、Sysage Technology がディーラーパートナーとともに Taichung Bank Investment Trust を支援し、WAF 管理ルールを調整しました。その結果、Akamai WAF は、攻撃および侵入に関するサードパーティチームの厳しいテストに合格しました。Akamai サービスの稼働後、Sysage Technology はリセラーパートナーと協力し、四半期ごとのポリシーレビューや攻撃傾向分析も提供しています。これらは同社が Web サイトのパフォーマンスと保護機能を高いレベルに維持するために役立ちます。また、Information Office 部門の不安も解消しました。

Akamai ソリューションを導入することで Taichung Bank Securities Investment Trust は Web サイトのパフォーマンスや速度を改善しながら、DDoS 防御とハッキング阻止の機能も強化しました。その結果、一般投資家、投資リサーチャー、ファンドマネージャー、社内外のその他ユーザーの体験も向上し、安心してオンライン活動を実行できるようになりました。



Akamai は世界中の企業に安全で快適なデジタル体験を提供しています。Akamai のインテリジェントなエッジプラットフォームは、企業のデータセンターからクラウドプロバイダーのデータセンターまで広範に網羅し、企業とそのビジネスを高速、スマート、そしてセキュアなものにします。マルチクラウドアーキテクチャの力を拡大させる、俊敏性に優れたソリューションを活用して競争優位を確立するため、世界中のトップブランドが Akamai を利用しています。Akamai は、意思決定、アプリケーション、体験を、ユーザーの最も近くで提供すると同時に、攻撃や脅威は遠ざけます。また、エッジセキュリティ、Web / モバイルパフォーマンス、エンタープライズアクセス、ビデオデリバリーによって構成される Akamai のソリューションポートフォリオは、比類のないカスタマーサービスと分析、365 日 / 24 時間体制のモニタリングによって支えられています。世界中のトップブランドが Akamai を信頼する理由について、www.akamai.com、blogs.akamai.com、および Twitter の [@Akamai](https://twitter.com/Akamai) でご紹介しています。全事業者の連絡先情報は、www.akamai.com/locations をご覧ください。公開日：2020 年 9 月。