WAFの重要性と
選定ポイントを徹底解説

あなたの会社のWebアプリケーションは大丈夫?
WAFの重要性と選定ポイントを徹底解説!

ビジネス展開にWebアプリケーションが欠かせなくなるなか、WAF(Web Application Firewall)の重要性が高まっている。企業の規模や業種、展開エリアなどに関わらず導入は必須だと言ってもいい。ただWAFには「どう導入すればいいかわからない」「運用が難しい」といった課題が残るのも現状だ。そこで注目したいのが、クラウドWAFサービス「Akamai APP & API Protector (Akamai AAP)」だ。本サービスは、グローバル企業はもちろん、人手や予算などのリソース不足、スキル不足に悩む中堅企業でも利用しやすいWAFサービスとなっている。

ビジネスに欠かせないWebアプリ、求められるWAFによる保護

企業ポータルサイトやECサイト、取引先とのシステム連携など、近年のビジネス活動にはWebアプリケーションの活用が欠かせない。企業を狙ったサイバー攻撃が激しさを増すなか、そうしたWebアプリケーションのセキュリティ対策が重要になってきた。実際、サイバー攻撃の多くは、Webアプリケーションに潜む脆弱性や設定の不備を悪用して攻撃をしかけてくる。Webアプリケーションのセキュリティ対策を徹底し、サイバー攻撃の被害を最小限にすることでビジネス継続を図っていくことは、いまや企業にとって不可欠な取り組みといっていい。

Webアプリケーションのセキュリティ対策のなかでもとくに重要な取り組みとなるのがWAF(Web Application Firewall)の導入だ。WAFは従来型のファイアウォールやマルウェア対策、IPS/IDS(侵入検知・防御システム)などでは対応できないWebアプリケーションの通信(HTTPS)を保護する製品だ。サイバー攻撃者の攻撃コードを検知したり、脆弱性を悪用する攻撃をブロックしたりすることで、データの破壊や情報漏洩を防ぐことができる。

ただ、WAFの導入・運用には特有の難しさがあるのも事実。WAFの導入がなかなか進まないケースや、導入したものの運用がうまくいかないケースを紹介していこう。

よくある課題(1)「WAFをどう導入すればよいかがわからない」

企業が抱えるWAF導入の悩み

- 「ECサイトに導入するだけで十分なのか」
- 「営業拠点や製造拠点が複数あるなかで、それぞれの拠点に機器を設置するのは大変」
- 「人手不足で担当者を配置することができない」
- 「企業規模や事業規模が大きくなくてもWAFは必要なのか」

よくある課題の1つは「WAFをどう導入すればよいかがわからない」というものだ。WAFはWebサイトを保護する役割を担うが、Webサイトがあらゆるビジネスで活用されているなかで、どこにどのようにWAFを導入すればよいかが見えにくくなっているのだ。

あなたの会社のWebアプリケーションは大丈夫? WAFの重要性と選定ポイントを徹底解説!

ビジネス展開にWebアプリケーションが欠かせなくなるなか、WAF(Web Application Firewall)の重要性が高まっている。企業の規模や業種、展開エリアなどに関わらず導入は必須だと言ってもいい。ただWAFには「どう導入すればいいかわからない」「運用が難しい」といった課題が残るのも現状だ。そこで注目したいのが、クラウドWAFサービス「Akamai APP & API Protector (Akamai AAP)」だ。本サービスは、グローバル企業はもちろん、人手や予算などのリソース不足、スキル不足に悩む中堅企業でも利用しやすいWAFサービスとなっている。

ビジネスに欠かせないWebアプリ、求められるWAFによる保護

企業ポータルサイトやECサイト、取引先とのシステム連携など、近年のビジネス活動にはWebアプリケーションの活用が欠かせない。企業を狙ったサイバー攻撃が激しさを増すなか、そうしたWebアプリケーションのセキュリティ対策が重要になってきた。実際、サイバー攻撃の多くは、Webアプリケーションに潜む脆弱性や設定の不備を悪用して攻撃をしかけてくる。Webアプリケーションのセキュリティ対策を徹底し、サイバー攻撃の被害を最小限にすることでビジネス継続を図っていくことは、いまや企業にとって不可欠な取り組みといっていい。

Webアプリケーションのセキュリティ対策のなかでもとくに重要な取り組みとなるのがWAF(Web Application Firewall)の導入だ。WAFは従来型のファイアウォールやマルウェア対策、IPS/IDS(侵入検知・防御システム)などでは対応できないWebアプリケーションの通信(HTTPS)を保護する製品だ。サイバー攻撃者の攻撃コードを検知したり、脆弱性を悪用する攻撃をブロックしたりすることで、データの破壊や情報漏洩を防ぐことができる。

ただ、WAFの導入・運用には特有の難しさがあるのも事実。WAFの導入がなかなか進まないケースや、導入したものの運用がうまくいかないケースを紹介していこう。

よくある課題(1)「WAFをどう導入すればよいかがわからない」

企業が抱えるWAF導入の悩み

- 「ECサイトに導入するだけで十分なのか」
- 「営業拠点や製造拠点が複数あるなかで、それぞれの拠点に機器を設置するのは大変」
- 「人手不足で担当者を配置することができない」
- 「企業規模や事業規模が大きくなくてもWAFは必要なのか」

よくある課題の1つは「WAFをどう導入すればよいかがわからない」というものだ。WAFはWebサイトを保護する役割を担うが、Webサイトがあらゆるビジネスで活用されているなかで、どこにどのようにWAFを導入すればよいかが見えにくくなっているのだ。

実際、攻撃を受けたときの影響度や導入コストを考慮して、自社製品を販売するECサイトや重要なWebシステムだけにWAFを導入するというケースは多い。ただ、昨今のサイバー攻撃は、企業の規模や業種、事業内容など関係なく、攻撃しやすいところを狙う傾向にある。そのため、一部のECサイトやWebサイトだけを保護しても、ほかのWebサイトから侵入され、被害が拡大してしまうことも多い。

また、WebサイトがAPIサービスサイトとして稼働しているケースもある。Webサイトを保護するだけでなく、APIサービスサイトを含めてWAFで保護しなければ、Webサービス全体に攻撃の影響が及ぶこともあるのだ。

よくある課題(2)「WAFの運用には手間がかかる」

2つ目の課題は「WAFの運用には手間がかかる」というものだ。WAFは、マルウェア対策製品と同じように、攻撃を検知するためにシグネチャーを使って判定する。未知の攻撃を検知するためにはシグネチャーを適切に更新したり、検知しやすくするようカスタマイズ、チューニングしたりする必要がある。そのため、運用が企業にとって負担になることが多いのだ。

企業が抱えるWAF運用の悩み

- 「WAFを適切にカスタマイズできる担当者がいない」
- 「シグネチャーをアップデートするための作業が負担になっている」
- 「機器のメンテナンスや故障した際の対応が負担になっている」

こうした運用負担を軽減するために近年ではクラウド型のWAFサービスが主流になりつつある。ただし、クラウド型WAFサービスを導入すると、既存のオンプレミスのWAFと新たなクラウド型WAFサービスの両方を運用しなければならず、さらに負担が増えることもある。またマルチクラウド環境では、それぞれのWAFサービスを利用することでそのぶん運用管理の負担もかかってくる。「マルチクラウド環境を構築しているが、個々のWAFを運用するリソースがない」といった運用課題につながりやすいのだ。

WAF選定のために押さえておきたい3つのポイント

こうした課題やニーズに対応するためにどのようなWAFを選定すればよいのだろうか。WAF選定のポイントは、大きく3つを挙げることができるだろう。

1. **企業全体で均一のセキュリティレベルを実現できること**
   複数拠点やマルチクラウド環境に対応し、1つのサービスでECサイトやAPIサービスサイトなど、企業全体のWebアプリケーションをカバーできることが重要だ。
2. **大規模かつ高度なサイバー攻撃にも耐えられること**
   サイバー攻撃は企業規模や業種、地域など関係なく発生する。日本国内はもちろん、世界中のどこに拠点があっても対応でき、ゼロデイ攻撃のような未知の脅威も検知・ブロックできることが重要だ。
3. **簡単にカスタマイズやチューニングができ、運用も事業者や専門組織に任せられること**
   マネージドサービスとしてWAFの運用を外部に任せることで、導入コストや運用負担を低減し、人手不足の課題を解消できる。これによって本来WAFによって守りたいシステムやデータの管理といった業務に集中できることが重要だ。

こうした3つのポイントを押さえたWAFサービスとして注目したいのが、NTTコミュニケーションズ(以下、NTT Com)が販売を手がける「Akamai APP & API Protector」(以下、Akamai AAP)だ。

自動アップデートからBot可視化まで――Akamai AAPの強み

Akamai AAPは、CDN(Content Delivery Network)事業者のパイオニアとして知られるAkamaiが提供するクラウド型WAFサービスだ。複数のIT調査会社による評価でリーダーに位置するサービスであり、世界中に分散した30万台を超えるAkamaiサーバーを活用しながら、ユーザー企業が抱えるすべてのWebとAPIのトラフィックを検査し、DDoS(分散型サービス妨害)、Webアプリケーション、APIに対する攻撃からシステムやデータを保護する。

まず特長として挙げたいのは、さまざまな環境にすばやくWAFを展開できる点だ。特別な知識は不要で、数クリックで30分以内にセキュリティ設定が可能だ。また、シグネチャーなどの更新が自動で行われ、未知の脅威への対応や検知のための最新機能を常に利用することができるのもポイントだ。Akamaiのセキュリティ専門家が1日あたり290TBにも及ぶ膨大な攻撃データをもとに脅威の分析を行い、APIの最新情報の習得や機械学習などの知見を活用しながら、適切なチューニングを施していく。

さらに、AkamaiのCDNを活用することで、攻撃を受けたときに最大のパフォーマンスで対応できることも特長だ。WebサイトとAPIの脆弱性を突く攻撃だけでなく、DDoSへの対応や、DDoSに至らないが企業ネットワークに悪影響を与えるBotを可視化しブロックする仕組みも備える。

加えて、提供コストにも注目できる。市場のリーダー製品でありながら、月額十数万円からという中堅規模でも利用しやすい価格帯となっている。

NTT Comが顧客に寄り添ってWAF導入・運用をサポート

導入にあたって、NTT Comによる強力なサポートが得られることも大きな魅力だ。前述した「WAFをどう導入すればいいかわからない」「運用負担が大きい」といった課題もNTT Comのコンサルタントやエンジニアが顧客に寄り添って解決していく。

NTT Comは、Akamaiパートナーとして約20年の実績を持っている。数十名規模のAkamai有資格者を擁するAkamai最上位パートナーで、全世界数百社におよぶパートナーの中から「Akamai Partner of the Year」を日本で唯一受賞している。企業が抱えるさまざまなセキュリティ課題を理解し、24時間365日サポート体制で解決策を提示していく。

NTT ComのAkamai AAP導入実績

A 自動車メーカー

公式サイト、カーナビ向けシステム、コネクテッドカー向けAPIサービスなどを展開しており、それらを包括的に防御するためにAkamai AAPを活用している。システム管理者の異なる多岐に渡るシステムで一定のセキュリティレベルを確保しながら、大規模な攻撃に対抗し、運用管理コストを低減させた。

B アパレル企業

店舗システムとECサイトの融合といったOMO戦略を推進するなかで、Akamai AAPを活用することで、クラウドとエッジ環境のセキュリティを確保できるようになった。

あらゆるWebアプリケーションの脆弱性を突いたサイバー攻撃が日に日に増加していくなかで、WAFの重要性は高まる一方だ。しかしWAFの導入や運用にあたって悩みを抱え、足踏みしてしまっている企業も少なくない。そうした状況を脱するためにも、スピーディーな展開が可能で、包括的な保護を実現するAkamai AAPの導入を検討してみてはいかがだろうか。自社環境やリソースにあわせて適切にAkamai AAP を活用していくことで、ビジネスをさらに加速させていけるだろう。

Akamai AAPに関するお問い合わせ

NTTコミュニケーションズ株式会社

法人のお客さまお問い合わせ窓口［ドコモビジネスコンタクトセンター］

0120-003300 受付時間 9:00～17:00
※携帯電話からもご利用になれます。土・日・祝日・年末年始は休業とさせていただきます。

サイト www.ntt.com/business/services/network/cdn/cdn.html

お問い合わせメールアドレス cdn-sales@ntt.com

A1207092 2022.10