ASP・CP サービスへの WAF 対策が進まない 3 つの課題と解決策！

Web アプリケーションの脆弱性を狙った攻撃による大規模な情報漏えい被害が相次いでいます。このようなサイバー攻撃を防ぐ WAF は、もはや必須セキュリティ対策の一つです。しかし、ASP・CP サービスのような大規模なトラフィックが発生する Web サービスにおいては、そのサービス特性から WAF 対策が進まない現状があります。
本資料では、ASP・CP サービスへの WAF 対策における課題と、その解決策をご紹介します。

▶情報漏えいを防ぐ必須セキュリティ”WAF”

あらゆるサービスがインターネット上で手軽に利用できるようになり、生活における Web サービスの利用シーンは年々増えています。

そうしたなか、Web アプリケーションの脆弱性を狙った攻撃により、企業の大切な資産である個人情報が数十万件の規模で漏えいする事件が相次いでいます。情報漏えいは、経営問題に直結する信用失落、利益損失につながるため、セキュリティ対策が急務となっています。ASP（ASP: Application Service Provider）・CP（CP: Contents Provider ニュース配信や動画配信、音楽配信サービスなど）サービスのような大規模なトラフィックが発生する Web サービスを提供する企業にとって、ユーザーへ安全な Web サービスを提供するためには、WAF（WAF: Web Application Firewall）は必須セキュリティ対策の１つです。

しかし、WAF 導入によるシステムへの影響確認や高額な費用など、導入ハードルは決して低くありません。現在も多くの ASP・CP サービスは WAF 対策が施されないままとなっています。

▶ASP・CP サービスへ WAF 対策が進まない 3 つの課題

このように、いつサイバー攻撃にあってもおかしくない状況下の ASP・CP サービスにおいて、WAF 対策が進まない３つの課題を紹介します。

①サービス稼働への影響

ASP・CP サービスを提供する企業にとって、ユーザーへのスムーズなサービス提供は、利用者増加や売上増加につながる重要な要素です。

WAF の導入により、ユーザーレスポンスに影響が発生し、スムーズなサービス提供が出来なくなり、機会損失に繋がるという課題があります。また、万が一 WAF 自体に障害が発生した場合は、WAF 導入サービスの稼働にも影響が及ぶというリスクもあります。

つまり、WAF 導入には、サービス稼働に影響を与えない製品を選定する事が重要です。

②WAF 運用のリソース

WAF の運用に、多くのリソースを割く必要があることも課題の一つです。自社サービスが成長するにつれて、サーバ台数は数十台から数百台規模へと増加していきます。複数のデータセンターに分けて運用するケースも少なくありません。データセンターごとに WAF を管理するのは、技術者の確保や工数の増加という膨大なリソースが必要となるため、現実的ではありません。

そうした理由から、WAF を選定する際は保守や運用を任せることが出来るクラウド型 WAF が主流となっています。運用・保守はメーカーが行い、ユーザーは本業に専念出来るため、クラウド型の WAF は有力な選択肢の一つです。

③WAF 導入費用

WAF には様々なタイプがありますが、初期費用や運用費用はタイプによって大きく異なります。

最近では、初期費用、運用費用が高額なアプライアンス型、ホスト型に比べ、比較的低価格で導入出来る DNS 切り替え型（クラウド型）が人気です。しかし、DNS 切り替え型は導入するサービスのトラフィック量に比例して費用が高額になるという課題があります。ASP・CP サービスへの WAF 導入は、トラフィック量の増加に伴い費用が増

加しない定額制のクラウド型 WAF が最適です。

『ASP・CP サービスにおける WAF 導入の課題』

確認ポイント		ホスト型（ソフトウェアインストール型）	アプライアンス型	クラウド型
サービスへの影響	ユーザーレスポンス遅延	影響あり	影響あり	影響あり
	WAF障害発生時	導入サービスの稼働に影響あり	導入サービスの稼働に影響あり	導入サービスの稼働に影響あり
運用リソース	技術者	必要	必要	不要
	自社でのシグネチャカスタマイズ	必要	必要	不要
費用	運用・保守費用	高額	高額	不要
	費用の増加	ライセンス数に比例して、費用が増加	不要	トラフィック量に比例して、費用が増加

▶従来の WAF とは異なる、クラウド連動エージェント型「攻撃遮断くん」

ASP・CP サービスのような大規模 Web サービスを提供する企業にご紹介したいのが、先ほど挙げた 3 つの課題を解決するクラウド型 WAF「攻撃遮断くん」です。

「攻撃遮断くん」は、従来の Web サーバに直接ソフトウェアをインストールするホスト型の WAF にはない革新的な仕組みであるクラウド連動エージェント型を採用することで、ASP･CP サービスにも対応できる仕組みの WAF です。

①ユーザーレスポンス・サービス稼働に影響なし

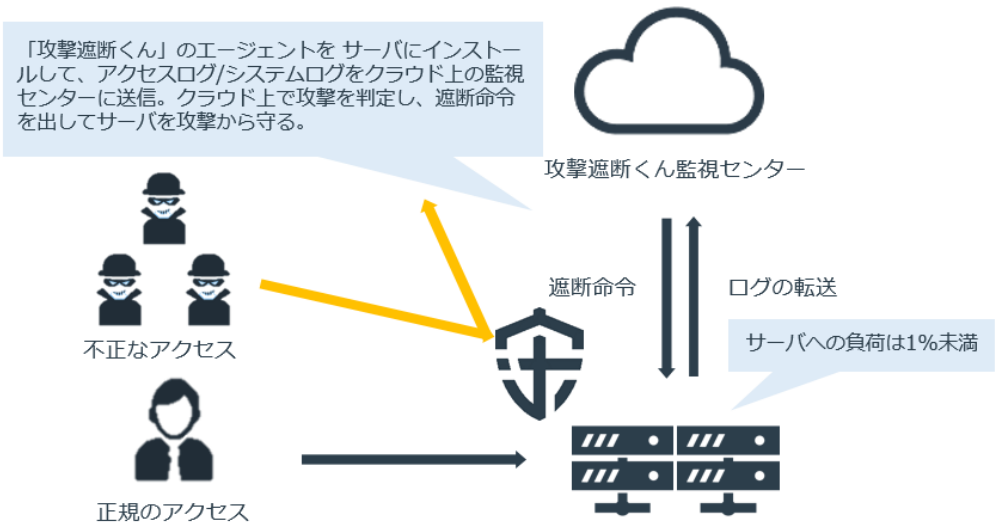
サーバへインストールした「攻撃遮断くん」エージェントからクラウド上の監視センターへログを送信し、監視センターにて攻撃検知、遮断命令の処理を行うため、サイバー攻撃の検知・遮断の最中でもサーバ負荷は 1%を超えません。この仕組みにより、WAF の導入によるユーザーレスポンスには、ほぼ影響がありません。また、万が一「攻撃遮断くん」監視センターに障害が起こった場合でも、従来型の WAF のように導入サービスの稼働が止まってしまうといったリスクがありません。

②数百台の Web サーバに 1 契約で対策可能

たとえデータセンターが複数に分かれていても、サーバが何百台あっても、「攻撃遮断くん」使い放題プランでは、1 契約で全てのサーバ、Web サイトへの対策が可能です。事業の成長に伴い、サーバ台数、トラフィックがどれだけ増加しようとも「使い放題プラン」1 契約で対策できるため、プランアップや新しい製品を導入する必要はありません。

「攻撃遮断くん」はクラウド型のため、最新の攻撃に自動で対応し、運用には一切の手間が掛かりません。また、ユーザー毎に、シグネチャを個別カスタマイズすることが可能なため、誤検知の心配もありません。万が一のトラブル時も、24 時間 365 日体制のサポートセンターで対応しています。「攻撃遮断くん」の仕組みなら、従来のクラウド型のメリットをそのままに、ユーザーへ安全な Web サービスの提供を実現することが可能になります。

『攻撃遮断くんのサービス仕組み図』



③クラウド型 WAF 唯一の定額制プランを提供

「攻撃遮断くん」使い放題プランは、サービス契約者ごとに専用の監視センターを立ち上げ、攻撃を検知・遮断するサービスです。専用の監視センターを立ち上げることで、サーバ台数が数百台あり、トラフィック量が膨大な Web サービスでも定額で対策することができます。

例えば、広告キャンペーンを打ったときにサービスのトラフィック量が急増してしまった場合でも、トラフィック量に応じて費用が増えることはありません。トラフィック量が膨大なため、見積もりが高額となり WAF の導入を諦めていたケースも、「攻撃遮断くん」であれば定額制のため安心して導入することできます。

なお、「使い放題プラン」は、初期費用 50 万円、月額 80 万円でご提供しています。

ASP・CP サービスを提供する企業にとって、サービス稼働に影響がなく、リソース不要かつ定額で導入できる「攻撃遮断くん」は有力な選択肢になるのではないでしょうか。

▶大規模な動画配信サービスへの導入事例

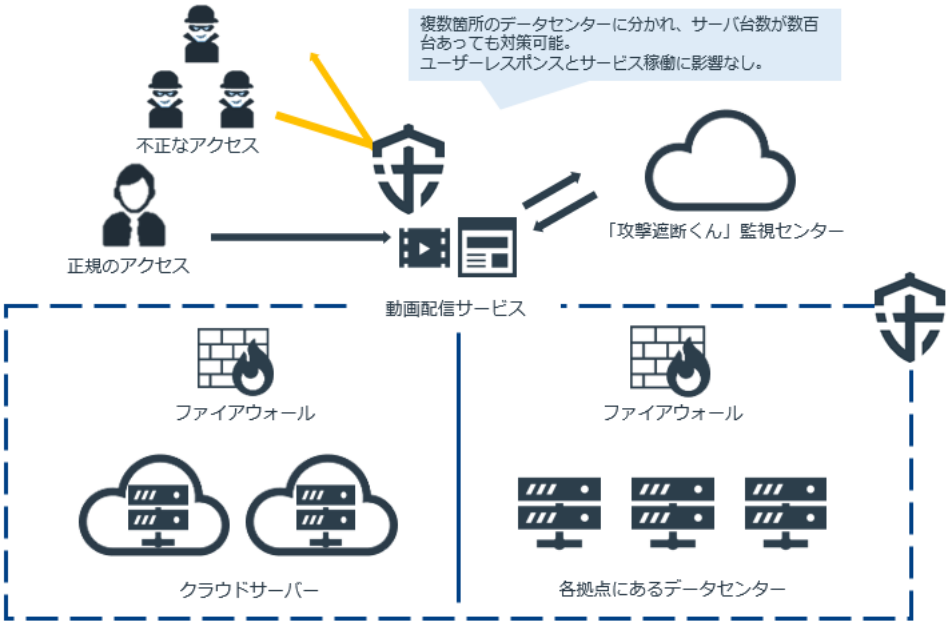
WAF 導入に課題を抱えていた大規模な動画配信サービスが、「攻撃遮断くん」使い放題プランを採用した事例をご紹介します。

サービス利用者が増加するなか、データセンターが複数箇所に別れており、さらにサーバが数百台ある環境のため WAF 対策を行えない状況でした。また、従来のアプライアンス型やホスト型といった WAF では、それぞれのデータセンターごとに対策する必要があるため、導入コスト、運用リソースが膨大となり、導入・運用が現実的ではありませんでした。

こうした課題に対して、クラウド連動エージェント型「攻撃遮断くん」を導入したことで、1 契約のみで WAF 対策を実現しました。また、最新の攻撃に自動で対応するため、データセンターごとに WAF を管理するという運用の負担も軽減しました。

DNS 切り替え型のクラウド型 WAF では、ユーザーレスポンスへ影響が出るほか、万が一 WAF 自体に障害が発生した場合、WAF 導入サービスの稼働にも影響が及びますが、「攻撃遮断くん」にはこうしたリスクがないことから、大規模な動画配信サービスへの導入が可能となりました。

『複数に点在するデータセンターへの「攻撃遮断くん」使い放題プラン導入イメージ図』



▶自社サービスの特性にあった WAF 対策

セキュリティ対策は、売上獲得のためのプロモーションに比べて、取り組みが後回しになってしまうケースがあります。しかし、ASP・CP サービスのような Web サービスがサイバー攻撃によってサービスの提供が滞ってしまうと、利益損失に直結する問題となります。Web アプリケーションの脆弱性を狙った攻撃がなくなることはなく、新たな攻撃手法は次々と生み出されています。

WAF 対策を施すことは、提供するサービス、ひいてはそのサービスを利用するユーザーの保護につながります。前述した WAF 対策における 3 つの大きな課題と、それぞれの WAF の特徴を確認し、自社サービスに最適な WAF 対策を施して行くことが大切です。

お問い合わせ先
〒150-0002 東京都渋谷区渋谷 2-3-8 倉島渋谷ビル 6 階
株式会社サイバーセキュリティクラウド
Web セキュリティ事業部
電話番号: 03-6696-6298
サービスページ : https://www.shadan-kun.com

CSC
CYBER SECURITY CLOUD