WAF による Web アプリケーションの保護

WAF (Web Application Firewall)

- 脆弱性を悪用したサイバー攻撃から Web アプリケーションを保護
- インターネット上にあるサーバや Web サイトを攻撃から守ることに特化
- HTML を解釈して、不正な攻撃を遮断
- HTTP 通信を検査し、検査結果に基づき通信を遮断し、処理結果をログ出力

Webアプリケーション層への攻撃

SQL インジェクション
クロスサイトスクリプティング
ブルートフォースアタック
ディレクトリトラバーサル …etc

企業間のやりとりやホームページを活用した問合せや商品販売など、多くの企業が Web アプリケーションを利用していますが、インターネット上でアプリケーションを実行するということは、サイバー攻撃などのリスクが高まります。
こうした状況の中、Web アプリケーションの脆弱性を悪用した攻撃から Web アプリケーションを保護するセキュリティ対策の一つに、「WAF（ワフ：Web Application Firewall）」があります。
WAF は、ネットワークレベルのセキュリティ対策である「ファイアウォール」や、OS やミドルウェアなどプラットフォームレベルでの「IPS（侵入防止検知システム）」、「IDS（不正侵入検知システム）」などとは異なり、通信の中身までチェックするためにアプリケーションレベルにおいて、シグネチャに対してパターンマッチングをすることで攻撃を検知、あるいは防御を行います。
Web アプリケーションの脆弱性を突いた攻撃の例としては、「SQL インジェクション」や、「クロスサイトスクリプティング」などがあります。
SQL インジェクションは、Web アプリケーションに対して、作成者が想定していないデータベースを操作する命令の SQL 文を実行させることにより、データベースシステムを不正に操作する攻撃方法のことで、情報漏洩やデータの悪用につながり、過去には多くの企業でクレジットカード情報を含む個人情報の漏洩 や、Web サイトの不正改ざんの被害に会っています。
クロスサイトスクリプティングは、脆弱性のある標的サイトにおいて、攻撃者が作成した悪意のあるスクリプトをそのサイトの閲覧者のブラウザで実行させる攻撃方法で、cookie などが盗まれるような被害が多く、過去には YouTube のコメント欄の脆弱性を悪用してコメント表示できなくなったり、悪趣味な別サイトにリダイレクトされるなどの被害の例などがありました。また、悪意のあるスクリプトにより、パスワードやクレジットカード番号を入力するフォームを Web ページに追加し情報を盗むフィッシング 詐欺や、ユーザ端末を乗っ取るような被害もありました。
こうした Web アプリケーションへの攻撃に対処するために WAF は有効な手段なのですが、設定や日々のシグネチャの適用など、運用担当者の煩雑な作業を軽減するために、クラウド型の WAF のサービスの人気が高まっています。