A10 Web Application Firewall (WAF) 導入・運用支援サービス

A10 Thunder/Lightningシリーズの WAF 導入から運用をサポート

課題：

- 保護対象のウェブサイトに適したセキュリティ保護策の導入
- ウェブセキュリティに精通した専門家の不在
- サービスの変化・脅威のトレンドに継続的に対応できる能力
- セキュリティポリシー・コンプライアンスへの対応
- ウェブサイトのパフォーマンスを考慮したセキュリティ設計

解決策：

A10 Thunder/LightningシリーズのWAF機能の導入・運用を効率且つ有効にするため、パフォーマンスの劣化の影響を最小限に考慮したセキュリティ設定を行い、WAF導入・運用を支援します。

また脆弱性診断と組み合わせたフレームワークを活用することでWAF導入・運用だけでなくセキュリティポリシー・コンプライアンス対応にも有効です。

メリット：

- ウェブセキュリティに精通した専門家によるWAF導入・運用支援
- ウェブサイトに最適なセキュリティルールを構成
- 定期的な脆弱性診断を行うことでセキュリティ強化を継続
- A10のパフォーマンスを最大限に活かしたルール構成
- お客様の運用要件に合わせて柔軟にサービス内容を調整

WAF 導入・運用支援サービスの目的

ウェブサイトを適切に保護するには開発プロセスからプログラム、ネットワークやサーバインフラの脆弱性を低減させる努力が必要になります。セキュアコーディングや定期的な脆弱性診断はセキュリティを強化するには欠かせない活動ですが、ヒューマンエラーやプロセス上の問題で発生することも考慮しなくてはなりません。ソフトウェアにクリティカルなバグが発見された場合にソフトウェア側で改修するリードタイムを考慮するとWAFで保護することは有効なリスク低減策になります。また潜在的な脆弱性が外部に露呈するリスクを抑えるためにWAFの導入は欠かせません。

しかし、WAFの効果を最大限に活用するためにはウェブサイトに最適なセキュリティ設定を適用することが不可欠になります。多くのWAF製品ではシグネチャー配信による自動処理を採用しており、これは一見運用が容易に見えますが、ウェブサイトの環境に合わせて適用するシグネチャーを選定しないと偽陽性（フォールス・ポジティブ）や偽陰性（フォールス・ネガティブ）が多く発生する結果になり運用できない状態に陥る場合があります。また対象のウェブサイトに関係ないシグネチャーを多く適用してしまいWAFのパフォーマンスに影響を与え、最終的にウェブサイトのパフォーマンスに影響を及ぼす事例もよくあります。

A10のWAF導入・運用支援はWAF運用における課題を脆弱性診断と組み合わせることで、ウェブサイトに必要なルールを見極め、最適なルールを適用します。またウェブサイトに対する脆弱性診断は企業のセキュリティポリシーやコンプライアンス遵守のため不可欠な活動になることもあります。脆弱性診断と連携したWAF導入・運用フレームワークを活用することで脆弱性診断だけではなく、有効なWAF運用を実現し、費用対効果の高いサービスを提供することができます。

A10 WAF の特徴

多くのウェブ脆弱性はSQLインジェクション、クロスサイトスクリプティングやクロスサイトリクエストフォージェリーなどOWASP TOP 10に代表される脆弱性に起因しています。この脆弱性に焦点を当てたルールを構成することで効率的にウェブサイトを保護することができます。

またシグネチャー配信は既知のパッケージ製品の脆弱性を中心に考えられていますが自組織で開発したウェブサイトのプログラムに対して潜在的な脆弱性を攻撃者から保護することは重要になります。そのために既知の脆弱性だけでなく、未知の脆弱性に対応できる万能なセキュリティ設定が可能なルールベースのアーキテクチャーを採用しています

A10 WAF 導入・運用支援サービスの概要

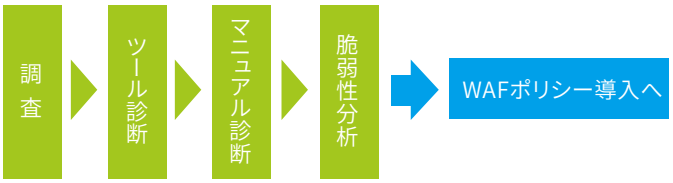
A10 WAF 導入・運用支援サービスは4つのフェーズで構成されます。

「脆弱性診断」では保護対象のウェブサイトに対して脆弱性診断を行い、潜在的な脆弱性を洗い出し、リスク判定します。「WAF ポリシー導入」では脆弱性診断で判定したリスクを低減させるために必要なルール設定をします。ルール設定後は「WAF 有効性確認」で、設定したルールが有効か脆弱性の再検査を実施しながら確認します。「脆弱性結果・WAF 適用報告」では WAF の各種状況の報告と WAF で対応効果が難しいまたは低い脆弱性について報告し、推奨対応策を助言します。

システムやセキュリティ脅威の変化に柔軟に対応するため、導入時だけでなく、毎月、四半期毎など定期的に脆弱性診断を行い、WAF ポリシーを柔軟に構成すること推奨します。

脆弱性診断アプローチ

脆弱性診断は以下の４つのフェーズで構成され、脆弱性診断後に「WAF ポリシー導入」に進みます。



「調査」ではお見積もり時に確認した費用、スケジュールに基づいて診断範囲を確定します。「ツール診断」では脆弱性診断ツールを活用して既知の脆弱性を中心に網羅的に検査します。「マニュアル診断」ではツールで検出が難しいと想定される箇所を特定し、専門家により特定した箇所を深く検査します。「脆弱性分析」では脆弱性の内容やセキュリティの脅威レベル、トレンド、システム環境を踏まえて、各脆弱性のリスクレベルを判定します。

WAF ポリシー導入アプローチ

診断項目から特定の URL に対して脆弱性が発見された場合、個別にポリシー作成して脆弱性を WAF で保護します。

https://www.xxx.co.jp/a1/に対して
クロスサイトリクエストフォージェリー対策のルールを適用した
ポリシーを作成

以下、診断項目を中心にポリシーを作成します

項目	内容
認証	ログインフォームのデータ 脆弱な認証方式
セッション管理	クッキー、セッション ID の保護 クロスサイトリクエストフォージェリー
入出データの処理	SQL、コマンドインジェクション、 クロスサイトスクリプティングなど
サイト構成の脆弱性	強制ブラウジング、ディレクトリーリスティング
システムの設定	システム情報の表示、 サーバエラーメッセージの表示

A10 Networks / A10 ネットワークス株式会社について

A10 Networks（NYSE: ATEN）はセキュアアプリケーションサービスにおけるリーディングカンパニーとして、高性能なアプリケーションネットワーキングソリューション群を提供しています。お客様のデータセンターにおいて、アプリケーションとネットワークを高速化し可用性と安全性を確保しています。A10 Networks は 2004 年に設立されました。米国カリフォルニア州サンノゼに本拠地を置き、世界各国の拠点からお客様をサポートしています。

A10 ネットワークス株式会社は A10 Networks の日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワーキングソリューションを提供することを使命としています。

詳しくはホームページをご覧ください。
www.a10networks.co.jp
Facebook：http://www.facebook.com/A10networksjapan

A10ネットワークス株式会社
www.a10networks.co.jp
a10networks.co.jp/contact

お問い合わせ：

Part Number: A10-SB_WAF Service Solution Apr 2018