Web アプリケーションと API のセキュリティ保護機能に関するチェックリスト

情報セキュリティ戦略の計画、実装、最適化をする際に、Web アプリケーションと API のセキュリティソリューションを実装することは、貴社に固有のリスクを把握し、セキュリティのギャップに的を絞り、脅威を検知することにつながります。そのためには、包括的な知見と継続的な可視性、および最も巧妙な攻撃を特定して阻止できる機能を備えた Web アプリケーションと API 保護（WAAP: Web Application and API protection）ソリューションが必要です。

このチェックリストは、ベンダーの機能の評価だけでなく、効果的な WAAP ソリューションの実装に必要な要件のリストとしても使用いただけます。

カテゴリー 1：プラットフォーム要件

あらゆる形態や規模の組織が存在し、その要件レベルも組織ごとに異なります。Web アプリケーション・セキュリティ・ソリューションは、柔軟でスケーラブル、かつ容易に管理できるものである必要があります。

- ☐ **パフォーマンスを損なわずに、トラフィック需要に応じて常に保護を提供できるスケーラビリティ**
- ☐ **地理的に分散したアプリケーションに対応できるアーキテクチャ**
- ☐ **適切に使用されていることを確認できる監査ログ機能**
- ☐ **オンプレミス、プライベート、パブリッククラウド（マルチクラウド、ハイブリッドクラウドを含む）上のオリジン Web サーバーの保護**
- ☐ **ネットワークレイヤ [L3/L4] の DDoS のゼロ秒での緩和に関する SLA（サービスレベル契約）**
- ☐ **プラットフォーム全体からの情報に基づく攻撃インテリジェンスにより攻撃者、攻撃頻度、攻撃の重大度を可視化**
- ☐ **ポート 80 とポート 443 経由の Web トラフィックのリバースプロキシ**
- ☐ **SSL／TLS 暗号化によるネットワークプライバシー保護**

Web アプリケーションと API のセキュリティ保護機能に関するチェックリスト

カテゴリー 2：適応型の Web アプリケーション保護と DDoS 防御

最も正確で信頼性の高いセキュリティを実現するためには、Web アプリケーションセキュリティは、従来のシグネチャベースの検知ではなく、より高度な適応型の Web アプリケーション保護と DDoS 防御へと進化する必要があります。

- ☐ アノーマリスコアリングやリスクベースのスコアリングによる、シグニチャベースの攻撃検知を超える検知
- ☐ 機械学習、データマイニング、ヒューリスティック分析に基づいて、急速に進化する脅威を特定
- ☐ セキュリティリサーチャーが提供する継続的なリアルタイム脅威インテリジェンスによる Web Application Firewall（WAF）ルールの自動更新
- ☐ 新規またはアップデートされた WAF ルールを本番環境に展開する前にライブトラフィックに対してテストするしくみ
- ☐ SQL インジェクション、XSS、ファイルインクルージョン、コマンドインジェクション、SSRF、SSI、XXE に対する防御（最小限）
- ☐ 顧客の要件に合わせてカスタマイズ可能な事前定義済みルール
- ☐ 再帰的なアプリケーションアクティビティにより Web サーバーに過負荷を与えるよう設計されたアプリケーションレイヤー［L7］ボリューム型 DoS 攻撃からの防御
- ☐ 継続的な設定と更新が不要な、フルマネージド型の WAF ルール
- ☐ 個々および共有の IP アドレスに対応する、クライアント・レピュテーション・スコアリングとインテリジェンス
- ☐ 特定のトラフィックパターンに対して迅速に保護を提供するカスタムルール（仮想パッチ）
- ☐ 自動化されたボットトラフィックや過度なボットトラフィックを防ぐためのリクエスト制限
- ☐ オリジンを標的にした直接攻撃からの防御
- ☐ 特定の IP、サブネット、地域からのトラフィックをブロックまたは許可する、複数のネットワークリストを介した IP／地理制御
- ☐ 脆弱性スキャンや Web 攻撃ツールなど、自動化されたクライアントからの防御

Web アプリケーションと API のセキュリティ保護機能に関するチェックリスト

カテゴリー 3：API の可視性、保護、制御

API 保護は、Web アプリケーションセキュリティの重要な要素となっています。API の脆弱性を緩和し、リスクサーフェスを縮小するためには、強力な API 検知、保護、および制御機能を備えた WAAP ソリューションが必要です。

- ☐ 未知の API や変化する API（API エンドポイント、特性、定義など）の自動検出とプロファイリング
- ☐ API ベースの攻撃を検知するための XML リクエストと JSON リクエストの自動検査
- ☐ 特定のユーザー要件を満たすカスタム API 検査ルール
- ☐ 許容できる XML と JSON オブジェクトフォーマットを事前定義し、API リクエストのサイズ、タイプ、深さを制限する機能
- ☐ リソースを枯渇させるよう設計された Low & Slow（少しずつ時間をかける）攻撃（Slow Post、Slow Get など）から、API バックエンドのインフラを保護
- ☐ API レベルでのリアルタイムのアラート、レポート、ダッシュボード
- ☐ API キーに基づく API エンドポイントのレートコントロール（スロットリング）
- ☐ IP／地域に基づく API ネットワークリスト（許可リスト／ブロックリスト）
- ☐ バージョン管理による API ライフサイクル管理
- ☐ JSON Web Token（JWT）の検証による安全な認証と認可
- ☐ 許可される API リクエストをキーごとに定義（各キーに対するクォータは個別に定義）し、消費を完全制御
- ☐ 標準 API 定義を使用した API オンボーディング（Swagger／OAS および RAML）

Web アプリケーションと API のセキュリティ保護機能に関するチェックリスト

カテゴリー 4：柔軟な管理

投資効果を最大化し、運用効率を上げるためには、シンプルで自動化されたワークフローが必要です。新しいアプリケーションや変化していくアプリケーションの保護、新しい WAF ルールの導入、API への保護の拡大。どの場合でも、プロセスはシームレスかつ直感的である必要があります。

- ☐ **セキュリティ設定タスクを CI／CD プロセスに統合するための Open API と CLI**
- ☐ **オンプレミスおよびクラウドベースのセキュリティ情報やイベント管理（SIEM）アプリケーションとの統合**
- ☐ **完全なステージング環境と変更管理を実装するしくみ**
- ☐ **トラフィックに自動的に適応する、自己調節型のセキュリティ保護**
- ☐ **リアルタイムのダッシュボード機能、レポート機能、ヒューリスティック分析に基づくアラート機能**
- ☐ **詳細な攻撃テレメトリーへのアクセスとセキュリティ事象の分析ができる、集中型ユーザーインターフェース（UI）**
- ☐ **人または／および完全に自動化された防御によって WAAP を管理できる柔軟性**
- ☐ **セキュリティ管理、監視、脅威の緩和をオフロードまたは強化できる、フルマネージド型セキュリティサービス**

Akamai Intelligent Edge Platform は、日々数百万の Web アプリケーション攻撃、数十億のボットリクエスト、数兆の API リクエストから知見を収集します。収集した知見を高度な機械学習や脅威リサーチと組み合わせることで、継続的な改善、新たな脅威の発見、革新的な機能の開発を行っています。

Akamai の Web アプリケーションと API セキュリティソリューションは、最先端の Web アプリケーション攻撃、DDoS 攻撃、API ベースの攻撃から組織を保護します。WAAP ソリューションの詳細な説明やデモをご希望の場合は、弊社までお問い合わせください。

Akamai *Intelligent Security Starts at the Edge*