# Citrix NetScaler AppFirewall

Citrix® NetScaler AppFirewall™は、Web アプリケーションまたは Web サービスアプリケーションに対する既知および未知の攻撃をブロックする ICSA 認定の総合的なアプリケーションセキュリティソリューションです。NetScaler AppFirewall はハイブリッドセキュリティモデルを実装しているため、正しいアプリケーションの動作のみを許可すると同時に、既知のアプリケーション脆弱性を効率的にスキャンして保護します。また、本ソリューションを使用して SSL 暗号化通信を含む双方向のトラフィックを分析することにより、アプリケーションを一切変更することなく、広範な種類の脅威に対する防御を実施できます。

NetScaler AppFirewall テクノロジーは、Citrix® NetScaler® MPX および VPX の Platinum Edition に含まれているほか、NetScaler Enterprise Edition を実行している NetScaler MPX アプライアンスに追加可能なオプションモジュールとしても提供されます。また、NetScaler AppFirewall は、7 台の NetScaler MPX アプライアンス上で実行するスタンドアロンソリューションとしても提供されます。スタンドアロンの NetScaler AppFirewall モデルは、ソフトウェアライセンスを通じて、完全な NetScaler Application Delivery Controller（ADC）へとアップグレードできます。

## 各種のセキュリティ上の課題に対処可能

Web アプリケーションは攻撃を受けやすいだけでなく、ハッカーにとって魅力的なターゲットとなります。これは、多くの場合、Web アプリケーションは、機密性の高い顧客情報や企業情報を含む 1 台以上のデータベースとダイレクトに接続されているためです。アプリケーションに対する脅威は、しばしばターゲットとなるアプリケーションに特化して考案されるため、ネットワークレベルのセキュリティデバイス（侵入防止システムやネットワークファイアウォールなど）による脅威の識別が不可能となります。この結果、Web アプリケーションは、数えきれないほどの既知の攻撃やゼロデイ攻撃に晒されることになります。NetScaler AppFirewall を導入すると、企業は、あらゆる Web アプリケーションおよび Web サービスに対して、中央で一元管理されるアプリケーションレイヤセキュリティを提供することが可能となります。

## ハイブリッド型のセキュリティモデル

NetScaler AppFirewall は、ポジティブセキュリティモデルおよびネガティブセキュリティモデルの両方を実装することにより、正しいアプリケーションの動作を保証します。ポジティブセキュリティモデルは、正常なアプリケーションのトラフィックを定義し、それ以外のトラフィックはすべて悪意のあるものとして取り扱うものです。ポジティブセキュリティモデルは、ゼロデイ攻撃のような未知の攻撃に対する防御を行うための唯一の実証されたアプローチです。一方、既知の攻撃に対する防御を行うには、自動的にアップデートされる数千ものシグネチャをスキャンする必要があります。

## PCI コンプライアンス要件および監査要件を満たす

NetScaler AppFirewall を使うと、企業の IT セキュリティチームは、政府機関によるプライバシー規制や業界の指令に準拠することが容易になります。例えば、クレジットカード業界のデータセキュリティ標準（PCI-DSS）要件に準拠する必要がある組織は、現時点で NetScaler AppFirewall を導入することで、PCI-DSS のセクション 6.6 に記述されている要件（適切なセキュリティレベルを維持するために、一般ユーザーの目に触れるアプリケーションの前方に Web アプリケーションファイアウォールをインストールすることを義務付けているもの）を完全に満たすことができます。また、PCI セキュリティ監査をサポートする必要がある場合、NetScaler AppFirewall を使うことで、PCI 要件に関連するアプリケーションファイアウォールポリシーに定義されているすべてのセキュリティ保護についての詳細を記述した専用のレポートを作成できます。さらに、NetScaler AppFirewall を使うと、クレジットカード番号やカスタム定義データオブジェクトのような機密性の高い情報をアプリケーションの応答から削除するか、またはアプリケーションの応答に含まれている当該コンテンツをマスクすることにより、それらの情報が不注意に漏えいすることを防止できます。

## PCI-DSS v.3.0 に準拠

- カード業界のデータセキュリティ標準に従ってクレジットカードやデビットカードのアカウント番号を保護します。
- 政府規制により顧客への通知が求められるようなデータの消失を防ぎます。
- デスクトップ管理を簡素化します。

## 各種の脅威から企業ネットワークを保護

- L7 DOS 攻撃に対処することにより Web サイトや Web サービスのアップタイムを保証します。
- アプリケーションが学習することで誤検出なしに防御を確立します。
- クロスサイトスクリプティング（XSS）やクロスサイトリクエストフォージェリ（XSRF）などの攻撃を回避することで、消費者やベンダー間の信頼関係を維持します。

## XML ベースの脅威に対処

XML ベースのアプリケーションを標的とする一般的な脅威（クロスサイトスクリプティングやコマンドインジェクションなど）を検出およびブロックする機能に加えて、NetScaler AppFirewall には、XML に特化した豊富なセキュリティ保護機能のセットが含まれています。これには、SOAP メッセージや XML ペイロードを徹底的に検証するためのスキーマ検証機能や、悪意のある実行可能ファイルやウイルスを含んでいる添付ファイルをブロックするための強力な XML 添付ファイルチェック機能などが含まれます。自動トラフィック検査方式により、アクセスの取得を目的とする URL やフォームへの XPath インジェクション攻撃をブロックできます。また、NetScaler AppFirewall を使うと、外部エンティティ参照、再帰展開、過剰なネスティング、長大なまたは多数の属性や要素を含んでいる悪意あるメッセージなどの各種の DoS 攻撃を阻止できます。

## 独自のセキュリティポリシーを作成可能

NetScaler AppFirewall には、実証済みの先進的な適合学習エンジンが組み込まれています。同エンジンは、それが Web アプリケーションにより意図された動作であったとしても、ポジティブセキュリティモデルによりブロックされる可能性のあるアプリケーションの動作の様々な側面を検出します。この例としては、HTML のフォームフィールドを合法的に変更するクライアントサイドのアプリケーションスクリプティングなどが挙げられます。いったん特定のアプリケーションの動作を学習すると、NetScaler AppFirewall は、人間が読み取り可能なポリシー推奨レポートを生成します。このレポートを参照することで、セキュリティ管理者は実際のアプリケーションの動作をより明確に理解できます。その結果、セキュリティ管理者は自社独自のセキュリティポリシーを作成した上で、同ポリシーを各アプリケーションに適用できるようになります。

## 業界トップレベルのパフォーマンスを実現

NetScaler AppFirewall は、最大規模のネットワークのニーズにも応えるために、高容量のアプリケーションセキュリティスループットを提供します。また、同ソリューションを使用すると、TCP 接続管理、SSL 暗号化、圧縮などの計算を多用するタスクを Web サーバーからオフローディングすることにより、実際のアプリケーションのパフォーマンスを改善し応答時間を短縮できます。さらに、NetScaler プラットフォーム上で利用できる内蔵型のキャッシング機能により、サーバーからのオフローディングを行うと同時に、完全なファイアウォール機能を適用できます。このような方法で貴重なサーバーリソースを解放することにより、全体的なアプリケーションエクスペリエンスを改善できます。

## 絶えず変化するビジネス要件に適用できる柔軟性を提供

NetScaler AppFirewall を使うと、Web アプリケーション保護の柔軟かつ段階的な導入が可能となります。デフォルトの Web アプリケーション保護プロファイルを使うと、最も一般的な脅威に対する防御のほか、データの窃盗やレイヤ 4～7 を標的とする DoS 攻撃に対する完全な防御を実施できます。

高度な Web アプリケーション保護プロファイルを使うと、クッキー、フォームフィールド、セッション固有の URL などの動的要素を保護するためのセッションアウェアな保護を実施できます。NetScaler により挿入される一意の ID をチェックしてクライアント-サーバー間でやり取りされる要求を検証することにより、クロスサイトリクエストフォージェリ（XSRF）のようなクライアント-サーバー間の信頼を標的とする攻撃を阻止できます。このような保護は、e コマースサイトのような、ユーザー固有のコンテンツを処理するアプリケーションにとって必須です。これらのセキュリティ手法があらゆるアプリケーションで互換性があることを保証するために、NetScaler AppFirewall は学習機能を提供しています。この機能を使うことで、管理者は、アプリケーションの意図的（合法的）な動作によってデフォルトのセキュリティポリシー違反が発生するような場合、例外や緩和を含む自社独自のセキュリティポリシーを作成できます。

| モデル | MPX 5550 | MPX 5650 | MPX 8005 | MPX 11515 |
|---|---|---|---|---|
| **構成** | | | | |
| プロセッサ | Intel E3-1225 | Intel E3-1275 | Intel E3-1275 | Intel Xeon E5645×2 |
| メモリ | 8GB | 8GB | 32GB | 48GB |
| イーサネットポート | 6x10/100/1000 BASE-T | 6x10/100/1000 BASE-T | 6x10/100/1000 BASE-T および 6x1000BASE-T SFP または 6x10/100/1000 BASE-T および 2x10G BASE-X SFP+ | 8x10G BASE-X SFP+ および 4x1000 BASE-X SFP |
| アップグレードオプション | MPX 5650 へのアップグレードオプション | | | MPX 11520/11540 へのアップグレードオプション |
| **性能** | | | | |
| 基本モードのスループット（Mbps） | 500 | 1,000 | 2,800 | 5,000 |
| SSL スループット（Mbps） | 500 | 2,000 | 4,000 | 14,000 |
| SSl トランザクション/秒 | 1,500 | 2,800 | 6,500 | 22,500 |
| **電源、環境、規制** | | | | |
| 電源装置数 | 1 | 1 | 1（オプションで+1） | 2 |
| 高さ | 1U | 1U | 1U | 2U |

| モデル | MPX 11520 | MPX 11540 | MPX 21550 |
|---|---|---|---|
| **構成** | | | |
| プロセッサ | Intel Xeon E5645×2 | Intel Xeon E5645×2 | Intel Xeon E5680×2 |
| メモリ | 48GB | 48GB | 96GB |
| イーサネットポート | 8x10G BASE-X SFP+ および 4x1000 BASE-X SFP | 8x10G BASE-X SFP+ および 4x1000 BASE-X SFP | 8x10G BASE-X SFP+ |
| ソフトウェアアップグレード | MPX 11540 へのアップグレードオプション | | |
| **性能** | | | |
| 基本モードのスループット（Mbps） | 6,500 | 8,000 | 12800 |
| SSL スループット（Mbps） | 15,000 | 19,000 | 11,000 |
| SSL トランザクション/秒 | 25,000 | 43,000 | 380,000 |
| **電源、環境、規制** | | | |
| 電源装置数 | 2 | 2 | 2 |
| 高さ | 2U | 2U | 2U |

注：上記のモデルは、スタンドアロンの NetScaler AppFirewall ソリューションとして提供されます。追加的なアプリケーションファイアウォールのサポートは、NetScaler VPX 10、200、1000、3000 の各仮想アプライアンス、およびすべての NetScaler MPX Application Delivery Controller（ADC）ハードウェアプラットフォームにおける内蔵モジュールとして提供されます。

# 技術情報

## 各種の脅威から企業ネットワークを保護

- バッファオーバーフロー
- CGI-BIN パラメータ操作
- フォーム/隠しフィールドの操作
- 強制的なブラウジング保護
- クッキーまたはセッション改ざん
- クロスサイトスクリプティング（XSS）
- クロスサイトリクエストフォージェリ（XSRF）
- コマンドインジェクション
- SQL インジェクション
- エラーに起因する機密情報の漏えい
- 暗号の非セキュアな使用
- サーバーの設定ミス
- バックドアやデバッグオプション
- レートベースのポリシー実施
- 既知のプラットフォーム脆弱性
- SOAP アレイ攻撃への防御
- コンテンツ書き換えおよび応答の制御
- コンテンツフィルタリング
- ユーザー認証、権利認証、監査
- L4-7 DoS 攻撃への防御

## 管理および開発用のユーザーインターフェイスを簡素化

- セキュアな Web ベースの GUI
- SSH ベースの CLI を通じたアクセスネットワーク管理
- SNMP
- Syslog ベースのロギング
- PCI-DSS 準拠のレポーティングツール
- Web Interface および Microsoft SharePoint 向けの AppExpert テンプレート
- AppFirewall プロファイルのインポート/エクスポート
- サードパーティ製のアプリケーション脆弱性ツールの出力を NetScaler ルールへと変換
- Common Event Format（CEF）ログを使用して新規ルールを簡単に導入

## Web サーバーや Web サービスに関する総合的なセキュリティを提供

- ディープストリームインスペクションによる双方向の分析
- HTTP/HTML ヘッダおよびペイロードの検査
- 完全な HTML 構文解析、セマンティック抽出
- セッションアウェアでありかつステートフル
- HTTP シグネチャのスキャン
  - 数千ものシグネチャをスキャン
  - 応答側のチェック
- プロトコル中立性
- HTML フォームフィールドの保護
  - 必須フィールドが戻されること、追加フィールド不可、読み取り専用フィールドおよび隠しフィールドの強制
  - ドロップダウンリストおよびラジオボタンの適合性
  - フォームフィールドの最大長の強制
- クッキーの保護：シグネチャにより改ざんを防止、クッキーの暗号化とプロキシ化
- 合法的な URL の強制：Web アプリケーションコンテンツの整合性を保証
- 完全な SSL オフローディング
  - 検査前にトラフィックを復号化し、転送後にトラフィックを暗号化する
  - バックエンドの暗号化を設定可能
  - クライアントサイド証明書をサポート
- XML データの保護
  - XML セキュリティ：XML に固有のサービス拒否（xDoS）攻撃、XML SQL インジェクション、Xpath インジェクション、クロスサイトスクリプティング（XSS）などへの防御
  - XML メッセージおよびスキーマの検証、フォーマットチェック、WS-I 基本プロファイル準拠、XML 添付ファイルのチェック
- URL 変換
- WSDL スキャンの回避により未公開の API を保護
- チャンク形式の POST リクエストをサポート

**Citrix について**

Citrix Systems, Inc.（NASDAQ:CTXS）は、新しい快適なワークスタイルを実現する仮想化、ネットワーキング、クラウドインフラストラクチャのリーディングカンパニーです。多くの企業および組織の IT 部門やサービスプロバイダーが、仮想化、モバイル化されたワークスペースの構築、管理、セキュリティ確保のために、シトリックスのソリューションを利用しています。仮想化、モバイル化されたワークスペースでは、デバイス、ユーザー、利用するネットワークやクラウドを問わず、アプリケーション、デスクトップ、データ、サービスをシームレスに利用することができます。シトリックスは今年、創設 25 周年を迎えますが、今後も革新に取り組み、モバイルワークスタイルにより IT をさらにシンプルにするとともに生産性の向上に貢献していきます。シトリックスの 2013 年度の年間売上高は 29 億ドルで、その製品は世界中の 33 万以上の企業や組織において、1 億人以上の人々に利用されています。シトリックスの詳細については www.citrix.co.jp をご覧ください。



**E1112/PDF**
**J1214/PDF** **www.citrix.co.jp**