Cisco ACE Web Application Firewall

Q. 今日の発表内容について教えてください。

A. シスコは、Cisco ACE Web Application Firewall の発売により、Application Networking Services（ANS）向けのソリューション（Cisco Application Control Engine [ACE] 製品シリーズ）の枠をさらに広げます。このソリューションの主なコンポーネントは、便利な 1 RU のフォーム ファクタで構成される ACE Web Application Firewall アプライアンスです。このアプライアンスは、HTML ベースと XML ベースの両方のアプリケーションに完全なプロキシ ファイアウォール ソリューションを提供します。ACE Web Application Firewall ソリューションには、セキュリティ ポリシーの作成とモニタリング用のセキュアな Web ベース アプリケーションである ACE Web Application Firewall Manager も含まれます。Cisco ACE 製品シリーズは、データセンター アプリケーションの可用性、アクセラレーション、および保護機能を最大化する、次世代のアプリケーション スイッチングおよび Web サービス ソリューションです。

Q. ACE Web Application Firewall のパフォーマンス特性を教えてください。

A. Cisco ACE Web Application Firewall は、業界最高レベルのスケーラビリティとスループットを提供して、Web に公開された HTML アプリケーションおよび XML アプリケーションを保護します。パフォーマンスの特性については、パフォーマンス テストの完了後に詳しくお伝えします。ACE Web Application Firewall では、高性能で並列性の高いイベント駆動型アーキテクチャを実装することで、サービスの遅延の低減、およびユーザ エクスペリエンスとサーバ利用率の向上を実現します。詳細は、ACE Web Application Firewall のデータシートに記載されています。http://www.cisco.com/jp/go/ace/ にアクセスしてください。

Q. Cisco ACE Web Application Firewall では、どのような課題を解決できますか。

A. Web アプリケーション ファイアウォールは通常、DMZ に配置されるか、または HTTP や HTTPS を経由してインターネット上のクライアント ブラウザに配信されるアプリケーションの前面に配置されます。XML サービスおよび Web サービスも、Web アプリケーション ファイアウォールで保護される同じアプリケーションによって展開および使用されます。ほとんどの場合、従来の Web アプリケーション ファイアウォールでは、XML および Web サービスの検査を実行して、悪意のあるコードの挿入や XDOS 攻撃などの脅威を検出することができませんでした。そのため、お客様からは、XML ファイアウォールと従来の Web アプリケーション ファイアウォールの両方を 1 つのシステムに統合するアプリケーション ファイアウォールへの要望が寄せられました。Cisco ACE Web Application Firewall は、Web に公開された HTML アプリケーションと XML アプリケーションを保護します。

Payment Card Industry Data Security Standard（PCI DSS; クレジット カード業界のセキュリティ基準）の第 6.5 項と 6.6 項では、クレジット カード データの保存、処理、および送信を行う企業の Web アプリケーションのセキュリティが重視されています。特に、第 6.6 項は、OWASP Top 10 攻撃（http://www.owasp.org/index.php/Top_10_2007）からアプリケーションを保護するために、2008 年 6 月 30 日までに 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、クレジット カード情報の取り扱い、処理、または保存を行う企業に義務付けています。

Cisco ACE Web Application Firewall は、詳細な Web アプリケーション分析と高性能な XML 検査および管理機能を組み合わせて、新しい Web アプリケーション サービスすべてに関連する広範な脅威に確実に対処することで、最新の PCI 要件に完全に準拠しています。

セキュアかつ高速で信頼性の高い HTML アプリケーションや XML アプリケーションでは、確実なスループット、高い並行性、低遅延、および重要な処理（セキュリティや可用性など）へのサポートを実現する能力が必要です。Cisco ACE Web Application Firewall には、これらの能力がすべて備わっています。ACE Web Application Firewall では、次の機能を提供します。

- PCI Web アプリケーション ファイアウォールのコンプライアンスに完全に準拠
- カスタム アプリケーション向けの強固なセキュリティ
- 既知の悪質なパターンに対する、シスコ検証済みの広範なシグニチャ
- Web アプリケーションを把握することで、適正なトラフィックのみをフィルタリングおよび許可
- ユーザ手動型の学習機能により、セキュリティ設定から曖昧さを排除

Q. ACE Web Application Firewall には、どのような利点がありますか。

A. Cisco ACE Web Application Firewall を使用すると、企業は次のような IT 目標を達成できます。

- ミッションクリティカルなアプリケーションに多大な被害をもたらす Web ベース攻撃からの危険を大幅に軽減
- 優れたソリューションにより、ごくわずかな時間とコストで、セキュアな Web プロジェクトを展開
- SOA および XML アプリケーションを将来の拡張に対応できるようにすることで、継続的な Web セキュリティの管理を簡素化

Q. ACE Web Application Firewall の主な機能は何ですか。

A. 主な機能は次のとおりです。

- Web アプリケーション セキュリティ
- プライバシー保護
- 暗号化と署名
- 監査とロギング
- モニタリング、統計情報、およびレポート
- ポリシーベースのプロビジョニングとバージョン管理

Q. ACE Web Application Firewall の主な機能の利点は何ですか。

A. 利点は次のとおりです。

- Web に公開されたカスタム アプリケーション向けの強固なセキュリティ
- 既知の悪質なパターンに対する、シスコ検証済みの広範なシグニチャ
- Web アプリケーションを把握することで、適正なトラフィックのみをフィルタリングおよび許可
- ユーザ手動型の学習機能により、セキュリティ設定から曖昧さを排除

Q. ACE Web Application Firewall ソリューションの主な差別化要因を教えてください。

A. ACE Web Application Firewall は、ID の盗用、データの盗用、アプリケーションの停止、不正行為、標的攻撃などの一般的な攻撃から Web アプリケーションを保護します。このような攻撃には、Cross-Site Scripting（XSS; クロスサイト スクリプティング）攻撃、SQL およびコマンド インジェクション、権限の昇格、Cross-Site Request Forgery（CSRF; クロスサイト リクエ

スト フォージェリ）、バッファ オーバーフロー、クッキーの改ざん、DoS 攻撃などがあります。主な差別化要因は次のとおりです。

- 将来に対応したアプリケーション セキュリティ — Cisco ACE Web Application Firewall に統合された XML ファイアウォール機能により、従来の HTML ベースの Web アプリケーションへの保護機能が XML 対応の最新の Web サービス アプリケーションにまで拡張されます。XML データのセキュリティには、XML スキーマ、SOAP、および XML コンテンツの検証といった XML 脅威軽減機能などが含まれており、Web アプリケーション トラフィック内のメッセージ処理ポリシーの違反をブロックします。
- スケーラビリティ — Cisco ACE Web Application Firewall は、XML アプリケーション トラフィック管理において業界で最高のスケーラビリティとスループットを提供します。1 台のアプライアンスで 10,000 TPS 以上を処理し、10,000 の同時接続が可能です。最終的なパフォーマンスの特性については、パフォーマンス テストの完了後に詳しく説明します。
- ポジティブおよびネガティブ セキュリティの適用 — Cisco ACE Web Application Firewall はポジティブおよびネガティブ セキュリティの利点を最大限に活用して、不正なトラフィック パターンを阻止し、有効なトラフィックのみを許可します。
- ユーザ手動型の学習機能 — セキュリティ ポリシーおよびプロファイルを監視モードで展開することで、自動学習環境にありがちな誤検出によるアプリケーションのダウンタイムを回避します。
- ポリシーベースのプロビジョニング — Cisco ACE Web Application Firewall は、高度なロールバックおよびバージョン管理機能により、開発者の生産性と展開の柔軟性を向上させます。

Q. Cisco ACE Web Application Firewall の Return On Investment（ROI; 投資収益率）は、どのようになっていますか。

A. お客様が Cisco ACE Web Application Firewall を展開する主な理由としては、アプリケーションの保護による業務コストの削減が挙げられます。米国連邦取引委員会の調査では、ID の盗用により、米国の企業で 2002 ～ 2003 年の間に 450 億米ドルを超える損失が発生したと見積もられています。セキュリティ侵害による間接費用は、潜在的に膨大な額になります。たとえば、次のような間接費用が発生します。

- ブランドの侵害
- 顧客の減少
- 規制違反の罰金（PCI DSS など）
- 訴訟

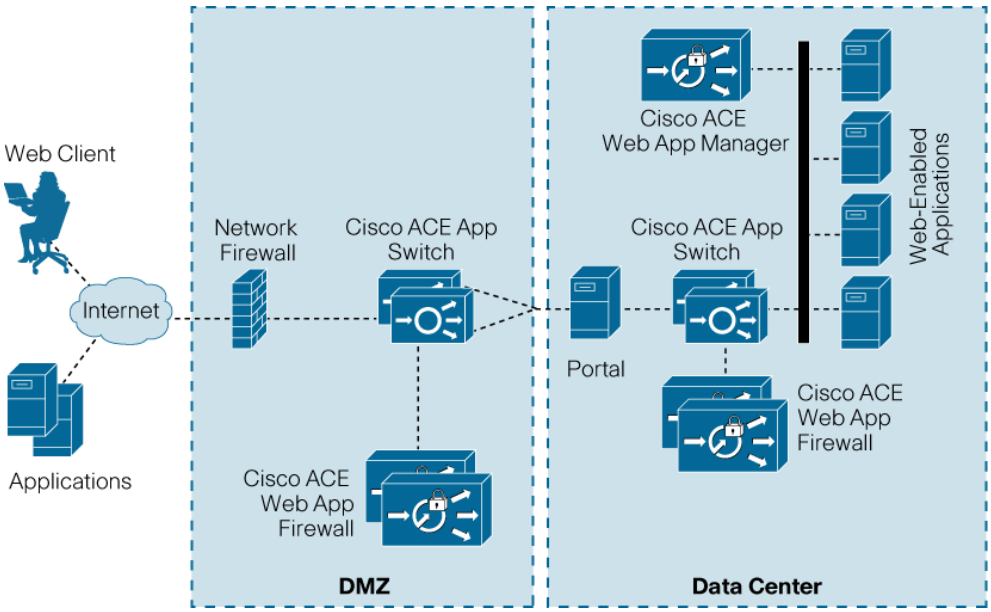
Q. ACE Web Application Firewall はどのようなユーザに役に立ちますか。

A. Cisco ACE Web Application Firewall は、Web に公開されたアプリケーションの保護を検討している企業、連邦政府機関、サービス プロバイダー、および法人顧客を対象としています。

Q. ACE Web Application Firewall は、どのように展開されるのですか。

A. ACE Web Application Firewall は通常、DMZ に配置されるか、または HTTP や HTTPS を経由してインターネット上のクライアント ブラウザに配信されるアプリケーションの前面に配置されます。

図 1　Cisco ACE Web Application Firewall の展開



Q.　ACE Web Application Firewall の主な機能と利点を教えてください。

A.

機能	利点
Web アプリケーション セキュリティ	• 監視モード展開を使用したユーザ手動型の学習機能をサポート • Web ベースの HTML および XML の脅威からアプリケーションを保護 • ID の盗用、データの盗用、コンテンツとフォーマットへの脅威、アクセスの脅威、コンプライアンス、転送、および標的攻撃（DoS 攻撃など）に対するセキュリティ保護 • カスタム ルールおよびシグニチャの作成が可能 • PCI DSS 1.1 第 6.5 項 および 6.6 項（OWASP Top 10）要件に対応するための設定済みのルールを提供
プライバシー	• アプリケーションへのアクセスとデータ プライバシーに対して、包括的かつ全社的なポリシー制御を実施
暗号化と署名	• クッキーの改ざんを防止し、ブラウザのクッキーに保存された情報の機密性を維持 • FIPS に完全に準拠。プラットフォーム ハードウェアにプライベート SSL キーを固定的に保存することで、Secure Sockets Layer（SSL）キー ハイジャックから保護
監査とロギング	• 監査機能および否認防止機能により、コンプライアンス要件に対応
モニタリング	• 高度な GUI により、Web アプリケーションの迅速なデバッグと監視が可能 • 包括的な統計情報およびレポート機能
ポリシーベースのプロビジョニングとバージョン管理	• 高度なロールバックおよびバージョン管理機能により、開発者の生産性と展開の柔軟性を向上 • ワンクリックで、特定の違反に対するファイアウォール ルールをオフにして、誤検出を迅速に解消 • Web GUI または Secure Shell（SSH）インターフェイスにより、ネットワーク上のどこからでもアクセスできる全社的な管理機能を提供 • プログラミングを行わずに、1 台の中央集中型ポリシー管理システムでセキュリティ ポリシーを設定
アクセラレーションとオフロード	• 転送セキュリティなど、コンピュータを多用する操作の負荷を軽減し、HTTP TCP セッションを再使用できるようにすることで、Web および XML アプリケーションの処理を高速化し、サーバの利用率を向上 • 新しいハードウェアを追加しなくても、将来のパフォーマンス強化に合わせてアップグレードが可能

Q. Web Application Firewall 6.0 リリースの新機能は何ですか。

A. 主な機能の利点については、すでに説明しました。次の表に、主な機能を機能カテゴリ別に示します。

項目	仕様
Web アプリケーション セキュリティ	• 完全なリバース プロキシ • 監視モード展開 • バッファ オーバーフロー • HTTP パラメータ操作、プロトコル適合性 • ヌル バイト ブロック • 入力エンコーディングの正規化 • 応答のフィルタリングおよび書き換え • 柔軟なファイアウォール処理 • クッキーおよびセッションの改ざん • Cross-Site Scripting（XSS; クロスサイト スクリプティング） • コマンド インジェクション、SQL インジェクション • 情報漏えいの防止によるプライバシー保護 • 暗号化の適用 • アプリケーションおよびサーバのエラー メッセージの非表示化 • 参照者機能の適用 • ポジティブおよびネガティブ セキュリティ モデル • カスタム ルールとシグニチャ • PCI 準拠のプロファイル
転送セキュリティ	• 設定可能な暗号スイートによる SSL v2/3 の完全なサポート • FIPS 140-2 レベル 3 プラットフォームの利用が可能
暗号化のサポート	• 使用可能な暗号化アルゴリズム： • Advanced Encryption Standard（AES; 高度暗号化規格） • Data Encryption Standard（DES; データ暗号規格） • Triple DES（3DES） • Blowfish • RSA • Diffie-Helman • Digital Signature Algorithm（DSA; デジタル署名アルゴリズム） • SHA-1（Secure Hash Algorithm 1）および MD5（Message-Digest 5）
管理性	• Web ユーザ インターフェイス • CLI（コマンドライン インターフェイス） • SSH • SNMP（簡易ネットワーク管理プロトコル） • Roles-Based Access Control（RBAC; ロールベース アクセス コントロール） • 委任された管理 • 中央集中型のポリシー管理と分散型の適用 • 設定、統計情報、およびログのインポートとエクスポート
ロギング、モニタリング、および監査	• Syslog、メッセージ、イベント ログ • トラフィックおよびサービスレベル契約（SLA）のモニタリングとレポート • モニタリング用の統計情報と各種アラートおよびトリガー • 管理操作の監査証跡

Q. ACE Web Application Firewall のハードウェアの機能を教えてください。

A. Cisco ACE Web Application Firewall は、FIPS バージョンと非 FIPS バージョンでご利用いただけます。非 FIPS バージョンには 10,000 TPS の暗号カード、FIPS バージョンには 4000 TPS の暗号カードが搭載されています。非 FIPS バージョンの方が SSL スループットが高く、低価格です。

Q. FIPS バージョンと非 FIPS バージョンの両方で、ACE Web Application Firewall がサポートしている最小ソフトウェア リリースは何ですか。

A. Web アプリケーション ファイアウォール機能を使用するには、6.0 以上のソフトウェア リリースが必要です。

Q. ACE Web Application Firewall の非 FIPS バージョンから FIPS バージョンへのアップグレードは可能ですか。

A. いいえ。暗号カードを現場交換できないため、アップグレードはできません。

Q. 非 FIPS の ACE XML Manager は、FIPS ACE Web Application Firewall を管理できますか。

A. 非 FIPS の ACE Web Application Firewall Manager で FIPS ACE Web Application Firewall を管理すること、および FIPS ACE XML Manager で 非 FIPS の ACE Web Application Firewall Manager を管理することは推奨していません。FIPS ACE Web Application Firewall がハードウェア保護キーを使用していない場合は、非 FIPS の ACE XML Manager で管理できる場合があります。同様に、FIPS ACE XML Manager はハードウェア保護キーを生成できますが、非 FIPS の ACE Web Application Firewall はそのキーを使用できないため、エラーが発生する可能性があります。

Q. ACE Web Application Firewall からフル機能の ACE XML Gateway にアップグレードすることはできますか。

A. はい。Cisco ACE Web Application Firewall を購入し、XML と Web サービスの変換および仲介機能を追加で提供する Cisco ACE XML Gateway にアップグレードする場合は、ACE XML Gateway と ACE XML Manager の両方に新しいライセンスを展開することを推奨します。詳細については、販売代理店にお問い合わせください。

Q. ACE Web Application Firewall のハード ディスクは、現場交換可能ですか。

A. はい、可能です。

Q. Cisco ACE Web Application Firewall は、Cisco IOS ソフトウェアを実行しますか。

A. いいえ。

Q. Cisco ACE Web Application Firewall と Cisco ACE Web Application Manager には、外部インターフェイスはありますか。

A. はい。どちらにも、4 GB イーサネット ポートおよび専用の完全自動管理ポートがあります。

Q. ACE Web Application Firewall で使用できるメモリ容量を教えてください。メモリをアップグレードできますか。

A. 4 GB です。メモリはアップグレードできません。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先(シスコ コンタクトセンター)
http://www.cisco.com/jp/go/contactcenter
0120-933-122(通話料無料)、03-6670-2992(携帯電話、PHS)
電話受付時間 : 平日10:00〜12:00、13:00〜17:00

お問い合せ先

08.06