

## Cisco ACE Web Application Firewall

### 製品概要

Cisco® ACE Web Application Firewall(図 1)は、Cisco Application Control Engine(ACE)製品シリーズの最新コンポーネントです。

多くの企業が、新しい Web ベースのアプリケーション、Web 2.0、および SOA ソリューションの実装により、効率性や収益が向上することを期待しています。この新しい Web ベースのサービスを導入すると、顧客、従業員、およびパートナーの柔軟性と双方向性が大幅に向上します。それと同時に、金融詐欺、ID やデータの盗用、DoS 攻撃、マルウェアやリモート制御エージェント ソフトウェアなど、セキュリティが手薄になりがちな新サービスを悪用しようと、犯罪者が狙っています。

privacyrights.org によると、2005 年以降、米国だけで約 2 億 5 千万件の記録が漏えいしています。それに伴い、世界中のほぼすべての国と地域で制定された、Sarbanes-Oxley(SOX; 米国企業改革法)、Gramm-Leach Bliley(GLB; 米国金融制度改革法)、HIPAA、PCI、Basel II、EU Data Privacy Regulation、J-SOX、PIPEDA のような新しい規制要件は、顧客や従業員の個人情報や金融情報など、機密情報へのアクセス、送信、および保存の保護に重点を置いています。

特に興味深いのは、消費者の金融情報や個人情報の保護です。ID の盗用やセキュリティ侵害の増加に対応するため、主要なクレジット カード会社が協力して、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)を制定しました。このセキュリティ基準は、企業によるクレジット カード情報の保存方法とアクセス方法を合理化および標準化するための要件です。

Cisco ACE Web Application Firewall 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が、PCI DSS 要件に準拠できるように支援します。Cisco ACE Web Application Firewall は、HTML と XML のセキュリティを独自に組み合わせることで、PCI DSS バージョン 1.1 の第 6.5 項 および 6.6 項の要件を遵守しています。

特に、第 6.6 項は、OWASP Top 10 攻撃([http://www.owasp.org/index.php/Top\\_10\\_2007](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ます。Cisco 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。

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 コンテンツ検証などの

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。

Cisco ACE Web Application Firewall は、要求と応答の両方のトラフィックに対して詳細なメッセージ レベルの検査を行う完全なプロキシ セキュリティ ソリューションでもあります。この機能により、攻撃を阻止するだけでなく、Web アプリケーションをハッカーから隠すこともできます。クレジットカードなどの機密データやパスポート番号、社会保障番号などの個人識別番号の漏えいを防ぐために発信トラフィックをフィルタリングすることで、プライバシー ポリシーも適用できます。

Cisco ACE Web Application Firewall ソフトウェア ライセンスは、完全な Cisco ACE XML Gateway ソフトウェアを含むようにアップグレードできます。アップグレードすることで、XML ベースのソフトウェア アプリケーションに対応した、堅牢な XML パフォーマンス強化ツールと管理ツールのセットを使用することができるようになります。Cisco ACE XML Gateway を使用すると、セキュリティ、相互運用性、または信頼性を損なうことなく、すべての XML メッセージを処理できます。企業は、市場で最も豊富なポリシー制御およびエンドツーエンドのパフォーマンスを使用して、XML Web サービスを効率的に保護、迅速化、および統合できます。これにより、お客様は商品化までの時間を短縮し、競争上の優位性を確保できます。

図 1 Cisco ACE Web Application Firewall



セキュアで高速な信頼性の高い 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、および重要な業務（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 は次の機能により、これらの利点を提供します。

- 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

Cisco ACE Web Application Firewall を使用すると、高性能なネットワーク アプライアンスで業界最高レベルのセキュリティ処理を実行でき、開発および展開に関する要件に対処することが可能になります。概念の実証を行う場合、一部の Web 対応アプリケーションを保護する場合、または企業全体で広範な Web アプリケーションを展開する場合でも、シスコは、お客様のアプリケーションのセキュリティ、可用性、およびパフォーマンスの各要件に合わせて拡張できる、業界最高レベルの Web アプリケーション ファイアウォール ソリューションを提供します。

### 機能および利点

- 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
- SOAP アプリケーションおよび XML アプリケーションとの連携により、継続的な Web セキュリティ管理を簡素化

図 2 に、一般的な展開を示し、表 1 には、Cisco ACE Web Application Firewall の機能と利点を示します。

図 2 Cisco ACE Web Application Firewall の展開

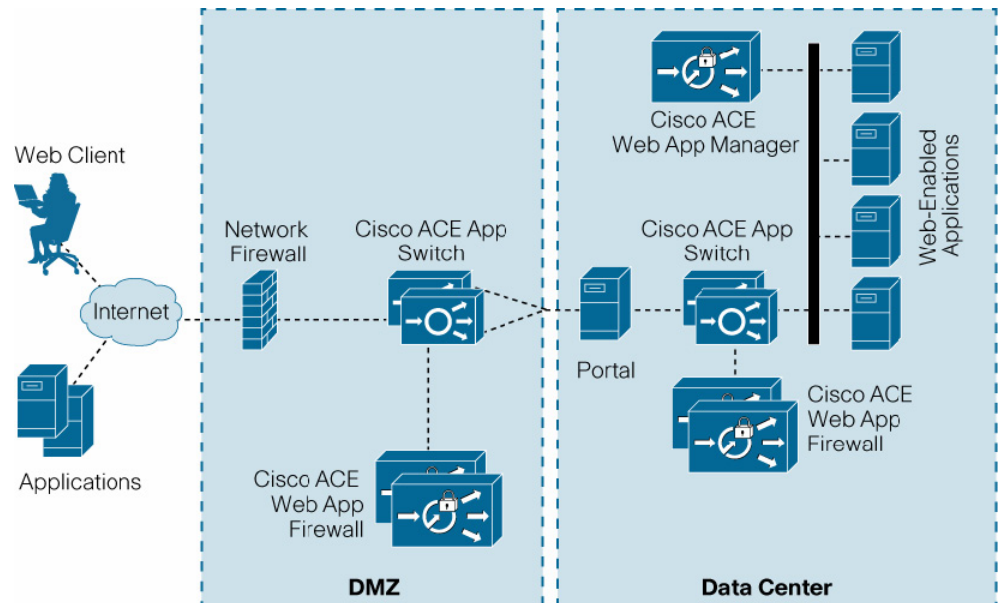


表 1 機能および利点

機能	利点
Web アプリケーション セキュリティ	<ul style="list-style-type: none"> <li>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</li> <li>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</li> <li>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</li> <li>カスタム ルールおよびシングニチャの作成が可能</li> <li>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</li> </ul>
プライバシー	<ul style="list-style-type: none"> <li>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</li> </ul>
暗号化と署名	<ul style="list-style-type: none"> <li>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</li> <li>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</li> </ul>
監査とロギング	<ul style="list-style-type: none"> <li>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</li> </ul>
モニタリング	<ul style="list-style-type: none"> <li>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</li> <li>包括的な統計情報およびレポート機能</li> </ul>
ポリシーベースのプロビジョニングとバージョン管理	<ul style="list-style-type: none"> <li>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</li> <li>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</li> <li>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</li> <li>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</li> </ul>
アクセラレーションとオフロード	<ul style="list-style-type: none"> <li>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</li> <li>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</li> </ul>

## 製品仕様

表 2 に、Cisco ACE Web Application Firewall のソフトウェア仕様、表 3 に、ハードウェア仕様を示します。

表 2 Cisco ACE Web Application Firewall の製品仕様

項目	仕様
Web アプリケーション セキュリティ	<ul style="list-style-type: none"> <li>• 完全なリバース プロキシ</li> <li>• 監視モード展開</li> <li>• バッファ オーバーフロー</li> <li>• HTTP パラメータ操作、プロトコル適合性</li> <li>• マル バイト ブロック</li> <li>• 入力エンコーディングの正規化</li> <li>• 応答のフィルタリングおよび書き換え</li> <li>• 柔軟なファイアウォール処理</li> <li>• クッキーおよびセッションの改ざん</li> <li>• Cross-Site Scripting (XSS; クロスサイト スクリプティング)</li> <li>• コマンド インジェクション、SQL インジェクション</li> <li>• 情報漏えいの防止によるプライバシー保護</li> <li>• 暗号化の適用</li> <li>• 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</li> <li>• 参照者機能の適用</li> <li>• ポジティブおよびネガティブ セキュリティ モデル</li> <li>• カスタム ルールとシグニチャ</li> <li>• PCI 準拠のプロファイル</li> </ul>
転送セキュリティ	<ul style="list-style-type: none"> <li>• 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</li> <li>• FIPS 140-2 レベル 3 プラットフォームの利用が可能</li> </ul>
暗号化のサポート	<ul style="list-style-type: none"> <li>• 使用可能な暗号化アルゴリズム: <ul style="list-style-type: none"> <li>• Advanced Encryption Standard (AES; 高度暗号化規格)</li> <li>• Data Encryption Standard (DES; データ暗号規格)</li> <li>• Triple DES (3DES)</li> <li>• Blowfish</li> <li>• RSA</li> <li>• Diffie-Helman</li> </ul> </li> <li>• Digital Signature Algorithm (DSA; デジタル署名アルゴリズム)</li> <li>• SHA-1 (Secure Hash Algorithm 1) および MD5 (Message-Digest 5)</li> </ul>
管理性	<ul style="list-style-type: none"> <li>• Web ユーザ インターフェイス</li> <li>• CLI (コマンドライン インターフェイス)</li> <li>• SSH</li> <li>• SNMP (簡易ネットワーク管理プロトコル)</li> <li>• Roles-Based Access Control (RBAC; ロールベース アクセス コントロール)</li> <li>• 委任された管理</li> <li>• 中央集中型のポリシー管理と分散型の適用</li> <li>• 設定、統計情報、およびログのインポートとエクスポート</li> </ul>
ロギング、モニタリング、および監査	<ul style="list-style-type: none"> <li>• Syslog、メッセージ、イベント ログ</li> <li>• 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</li> <li>• 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</li> <li>• 管理操作の監査証跡</li> </ul>

表 3 製品仕様: Cisco ACE Web Application Firewall のハードウェア

項目	仕様
シャーシ	外形寸法 <ul style="list-style-type: none"> <li>1 RU の標準ラックマウント: 4.32 × 42.62 × 70.49 cm (1.70 × 16.78 × 27.75 インチ)</li> </ul> 重量 <ul style="list-style-type: none"> <li>完全構成時 16.8 kg (37 ポンド) (1 ユニットあたり、輸送用資材を除く)</li> </ul>
プロセッサ	<ul style="list-style-type: none"> <li>Intel デュアルコア Xeon プロセッサ × 2</li> </ul>
ハードウェア アクセラレータ	次のいずれかを使用できます。 <ul style="list-style-type: none"> <li>FIPS 140-2 レベル 3 準拠 (4,000 SSL TPS) × 1</li> <li>非 FIPS 準拠 (14,000 SSL TPS) × 1</li> </ul>
ポート	<ul style="list-style-type: none"> <li>4 ギガビット イーサネット ポートおよび専用の完全自動管理イーサネット ポート</li> </ul>
メモリ	<ul style="list-style-type: none"> <li>4 GB の RAM (固定)</li> </ul>
ストレージ	<ul style="list-style-type: none"> <li>RAID 構成のホットスワップ対応デュアル シリアル接続 Small Computer System Interface (SCSI) ハード ディスクドライブ (SAS HDD) (20 GB 使用可能)</li> </ul>
電力	<ul style="list-style-type: none"> <li>デュアル冗長構成、700 W</li> </ul>

### シスコのサービスおよびサポート

シスコでは、サービスへのライフサイクル アプローチを採用し、パートナーとの協力により広範なセキュリティ サービスを提供しています。そのため、企業は、攻撃やサービス停止からの重要なビジネス プロセスの保護、プライバシーの保護、ポリシーと法令順守へのサポートを実現するネットワーク プラットフォームを設計、実装、運用、および最適化することが可能になります。

ネットワークへの投資を無駄にすることなく、ネットワーク運用を最適化しネットワーク インテリジェンスの強化や事業拡張を進めていただくためにシスコのサービスを是非お役立てください。シスコでは以下のサービスを提供しています。

- Cisco Security Center では、早期警告脅威/情報、脅威/脆弱性の分析、Cisco IPS シグニチャ、および脅威軽減技術をワンストップ ショッピングでご利用いただけます。Cisco Security Center ([www.cisco.com/security](http://www.cisco.com/security)) にアクセスして、ブックマークしてください。
- Cisco Security Intellishield Alert Manager Service では、カスタマイズ可能な、Web ベースの脅威および脆弱性アラート サービスを提供して、お客様が、自社環境の潜在的な脆弱性について、正確で信頼できるタイムリーな情報を簡単に入手できるようにしています。
- Cisco Security Optimization Service: ネットワーク インフラストラクチャは、迅速で適応力のあるビジネスの基盤となりつつあります。Cisco Security Optimization Service は、計画と評価、設計、パフォーマンス チューニング、およびシステム変更への継続的なサポートを提供することで、進化し続けるセキュリティ システムをサポートし、絶えず変化するセキュリティへの脅威に対処します。このサービスにより、コア ネットワーク インフラストラクチャにセキュリティが組み込まれます。
- Cisco SMARTnet Service では、シスコ エンジニア、評価の高いオンライン サポート センター、指定デバイスでのマシン間の診断、ハードウェア交換のプレミアム オプションにお客様がいつでも直接、アクセスできるようにすることで、問題の迅速な解決を図ります。
- Cisco Software Application Support Services, plus Upgrades (SASU) は、テクニカル サポート、ソフトウェア アップデート、および主要なアップグレードにいつでもアクセスできるようにすることで、CSA の可用性、機能、および信頼性を保証します。

表 4 で説明しているサービスおよびサポート プログラム (Cisco SMARTnet<sup>®</sup> Service および Software Application Support plus Upgrades [SASU]) は、Cisco ACE Web Application Firewall サービスおよびサポート ソリューションの一部としてご利用いただけます。

表 4 Cisco SMARTnet とソフトウェア アプリケーション サービスおよびサポート プログラム

サービスおよびサポート	機能	利点
シスコまたはシスコ認定パートナーから直接利用可能 <ul style="list-style-type: none"> <li>• Cisco SMARTnet Service</li> <li>• Cisco SASU</li> </ul>	<ul style="list-style-type: none"> <li>• ソフトウェア アップデートおよびアップグレードに 24 時間アクセス可能</li> <li>• Web、電話、E メールを通じて Cisco Technical Assistance Center (TAC) に 24 時間アクセス可能</li> <li>• ハードウェア部品の迅速な交換 (Cisco SMARTnet サービスのみ)</li> </ul>	<ul style="list-style-type: none"> <li>• 人的資源の補充</li> <li>• ニーズに合った機能性の確保</li> <li>• リスクの緩和</li> <li>• 問題の予防および迅速な解決</li> <li>• シスコの技術者および専門知識を活用することで TCO を削減</li> <li>• ネットワーク ダウンタイムの最小化</li> </ul>

### 発注情報

お客様は自社のニーズに対応した暗号化プロセッサに応じて、2 つのバージョンの Cisco ACE Web Application Firewall のいずれかを選択できます。4000 トランザクション/秒 (TPS) での FIPS 準拠 SSL アクセラレーションに対応したバージョンと、10,000 TPS の処理が可能で FIPS には準拠していないバージョンがあります。

表 5 に、Cisco ACE Web Application Firewall の発注情報を示します。

表 5 発注情報

製品オプション	製品名	製品番号	サポートおよびサービス
シャーシ	<ul style="list-style-type: none"> <li>• Cisco ACE Web Application Firewall アプライアンス</li> </ul>	<ul style="list-style-type: none"> <li>• ACE-XML-K9</li> </ul> または <ul style="list-style-type: none"> <li>• ACE-XML-NF-K9</li> </ul>	<ul style="list-style-type: none"> <li>• CON-SNT-ACEXK9</li> </ul> または <ul style="list-style-type: none"> <li>• CON-SNT-ACEXNK9</li> </ul>
ソフトウェア	<ul style="list-style-type: none"> <li>• Cisco ACE Web Application Firewall ソフトウェア</li> </ul>	<ul style="list-style-type: none"> <li>• ACE-XML-SW-6.0</li> </ul>	—
暗号化	<ul style="list-style-type: none"> <li>• FIPS 準拠の SSL アクセラレーション</li> </ul> または <ul style="list-style-type: none"> <li>• 非 FIPS 準拠の SSL アクセラレーション</li> </ul>	<ul style="list-style-type: none"> <li>• ACE-XML-FIPS</li> </ul> または <ul style="list-style-type: none"> <li>• ACE-XML-NONFIPS</li> </ul>	<ul style="list-style-type: none"> <li>• CON-SNT-ACEXFIPS</li> </ul> または <ul style="list-style-type: none"> <li>• CON-SNT-ACEXNFIP</li> </ul>
ライセンス	<ul style="list-style-type: none"> <li>• Cisco ACE Web Application Firewall ライセンス</li> </ul> または <ul style="list-style-type: none"> <li>• Cisco ACE Web Application Firewall Manager ライセンス</li> </ul>	<ul style="list-style-type: none"> <li>• ACE-WAF-GAT-LICFX</li> </ul> または <ul style="list-style-type: none"> <li>• ACE-WAF-MGT-LICFX</li> </ul>	<ul style="list-style-type: none"> <li>• CON-SAU-ACEWGW</li> </ul> または <ul style="list-style-type: none"> <li>• CON-SAU-ACEWMG</li> </ul>

### 関連情報

Cisco ACE Web Application Firewall の詳細については、以下の URL を参照してください。

<http://www.cisco.com/jp/go/waf/>

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0704R)  
この資料に記載された仕様は予告なく変更する場合があります。



#### 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>

0120-092-255 (通話料無料)

電話受付時間：平日10:00～12:00、13:00～17:00

#### お問い合わせ先