

## Cisco Catalyst<sup>®</sup> 6500 および Cisco 7600 シリーズ対応 ファイアウォール サービス モジュール

図 1 Catalyst 6500 および Cisco 7600 シリーズ用ファイアウォール サービス モジュール



Firewall Service Module (FWSM; ファイアウォール サービス モジュール) は、Cisco Catalyst<sup>®</sup> 6500 スイッチ、および Cisco 7600 シリーズ ルータ用の高速な統合型ファイアウォール モジュールで、業界最速のファイアウォール データ速度を実現します。5 Gb のスループット、100,000 CPS、および 1M 同時接続が可能です。1 シャーシにつき 最大 20 Gb のスケーラビリティを実現している単一シャーシに、最大 4 つの FWSM をインストールできます。Cisco PIX<sup>®</sup> ファイアウォール ファミリのメンバである FWSM は大企業やサービスプロバイダーに、最高のセキュリティ、信頼性、およびパフォーマンスを提供します。

FWSM を使用すると、Cisco PIX テクノロジーが活用され、Cisco PIX オペレーティング システム (OS) が実行されます。この堅牢化された埋め込み型リアルタイム システムには、セキュリティ ホールやパフォーマンスを低下させるオーバーヘッドがありません。このシステムの中核では、Adaptive Security Algorithm (ASA; アダプティブ セキュリティ アルゴリズム) をベースとした保護スキームにより、ステートフルなコネクション型ファイアウォールが提供されます。ASA を使用することにより、FWSM では、送信元アドレスと宛先アドレス、ランダム化された TCP セッション番号、ポート番号および追加の TCP フラグに基づき、セッション フロー向けに、接続テーブル エントリが作成されます。FWSM では、こうした接続テーブル エントリにセキュリティ ポリシーを適用することによって、すべての受信トラフィックと発信トラフィックが制御されます。

### FWSM の主な利点

ファイアウォールの従来の役割が変わっています。ファイアウォールの役割には、不正な外部アクセスから企業ネットワークを保護するだけではありません。ファイアウォールは、不正ユーザが企業ネットワーク内の特定のサブネット、ワークグループ、または LAN にアクセスすることも防止します。FBI の統計によると、すべてのセキュリティ問題の 70 % は、組織内部から発生しています。FBI の調査の回答者のうち 5 人に 1 人が、これまでの 1 年間で、不正ユーザが企業ネットワークへ侵入したか、侵入を試みたことがあると回答しています。またほとんどの専門家が、ネットワークへの侵入の大部分が発見されていないと認めています。

### 統合モジュール

Cisco Catalyst 6500 シリーズ スイッチ、または Cisco 7600 インターネット ルータ内にインストールされた FWSM によって、デバイス上の任意のポートが、ファイアウォール ポートとして動作可能です。また、ネットワーク インフラストラクチャに、ファイアウォール セキュリティが統合されます。ラック スペースを重視する場合、これは特に重要です。Cisco Catalyst 6500 は、ファイアウォール サービス、侵入検知、Virtual Private Networking (VPN; 仮想私設 ネットワーク)、マルチレイヤ LAN、WAN、および MAN 切り替え機能などのインテリジェント サービスを必要とするお客様にとって、まさしく最適の IP サービス スイッチとして登場しました。

### 将来の保証

FWSM では将来の要件を満たす卓越した性能が提供されるため、システムをオーバーホールしなくても、最大 5 Gb のトラフィックが処理できます。Catalyst 6500 に最大 3 つの FWSM を追加して、増大を続ける要求を満たすことができます。

## 信頼性

FWSM は Cisco PIX テクノロジーをベースに、同じく長期間にわたって実績を積んだ Cisco PIX オペレーティング システムが使用されています。これはセキュリティが確保されたリアルタイムのオペレーティング システムです。FWSM では、実績のある Cisco PIX テクノロジーをパケット検査に使用することにより、同一システム上で優れたパフォーマンスとセキュリティというユニークな組み合わせを実現します。

## 所有コストの低減

FWSM ではどのようなファイアウォールでも、最高の性能価格比が実現されます。保守コストは、Cisco Catalyst シャーシの SmartNet™ 契約に含まれています。FWSM が Cisco PIX ファイアウォールをベースにしているため、トレーニング コストと管理コストが安く、FWSM がシャーシ内に組み込まれているため、管理するボックスが少なく済みす。

## 使いやすさ

Cisco PIX Device Manager のわかりやすい Graphical User Interface (GUI; グラフィカル ユーザ インターフェイス) を使って、FWSM の管理と設定を行うことができます。FWSM は、構成とモニタリングに関して、Cisco 管理フレームワークおよび Cisco Architecture for Voice, Video and Integrated Data (AVVID) パートナーによってサポートされています。

## FWSM の機能

主要機能	利点
パフォーマンス	<ul style="list-style-type: none"><li>• 5 Gbps</li><li>• 100 万の同時接続</li><li>• 1 秒当たり、10 万を超える接続のセットアップとティアダウン</li></ul>
複数のインターフェイス	<ul style="list-style-type: none"><li>• 最大 100 個のファイアウォール VLAN をサポート — 任意の Cisco Catalyst 4000 VLAN をファイアウォール VLAN として設定可能</li><li>• 802.1q および Inter-Switch Link (ISL; スイッチ間リンク) プロトコルに対応</li></ul>
カットスルー プロキシ	VLAN 単位でセキュリティ ポリシーを実施
設定サポート	<ul style="list-style-type: none"><li>• Command-Line Interface (CLI; コマンド ライン インターフェイス) への Console</li><li>• Cisco PIX Firewall の内部インターフェイスへの Telnet</li><li>• Cisco PIX Firewall の外部インターフェイスへの Telnet over IP Security (IPsec)</li><li>• CLI への Secure Shell (SSH) プロトコル</li><li>• Cisco PIX Device Manager への Secure Sockets Layer (SSL)</li></ul>
AAA サポート	TACACS+ および RADIUS サポートを介して、広く使用されている認証、許可、アカウントリング サービスとの統合
NAT/PAT サポート	動的/静的な Network Address Translation (NAT; ネットワーク アドレス変換) および Port Address Translation (PAT) を実現
Cisco PIX Device Manager (PDM)	<ul style="list-style-type: none"><li>• シンプルでわかりやすい Web ベースの GUI によって、リモート ファイアウォール管理をサポート</li><li>• 使用傾向、パフォーマンスのベースライン、セキュリティ イベント情報など、広い範囲にわたるリアルタイム レポートと履歴レポート</li></ul>
安全なネットワーク管理	安全で Triple Data Encryption Standard (3DES; トリプルデータ暗号標準) で暗号化されたネットワーク管理アクセス
アクセス リスト	<ul style="list-style-type: none"><li>• 最大 128,000 個のアクセス リスト</li></ul>
URL フィルタリング	サーバ上で定義されたポリシーを使って、発信 URL 要求をチェックするために Websense ソフトウェアを使用

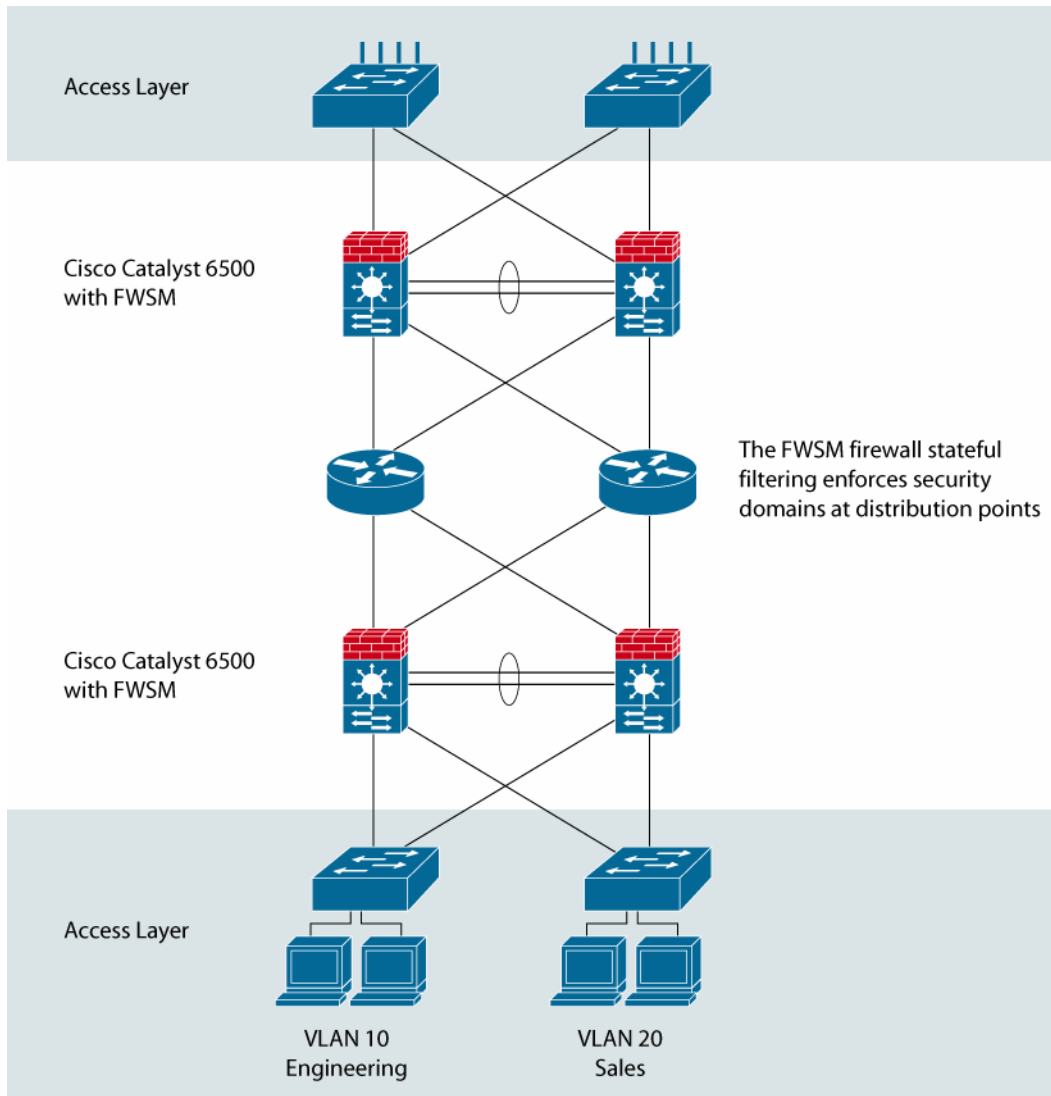
主要機能	利点
コマンド許可	特権レベルのすべての CLI への割り当て、およびこれらの特権レベルに関連するユーザ アカウントまたはログイン コンテキストの作成が可能
オブジェクトのグループ化	ネットワーク オブジェクト（ホストなど）とサービス（ftp や http など）のグループ化機能
DoS からの保護	<ul style="list-style-type: none"> <li>• DNS Guard</li> <li>• Flood Defender</li> <li>• Flood Guard</li> <li>• TCP Intercept</li> <li>• Unicast Reverse Path Forwarding</li> <li>• Mail Guard</li> <li>• FragGuard および Virtual Reassembly</li> </ul>
ルーティング	<ul style="list-style-type: none"> <li>• スタティック ルート</li> <li>• ダイナミック; Routing Interface Protocol (RIP) および Open Shortest Path First (OSPF)</li> </ul>
高いアベイラビリティ	ステートフル フェールオーバー — シャーシ内およびシャーシ間
ログイン	総合的なシステム ログギング、FTP、URL、および ACL ログギング
追加プロトコル	<ul style="list-style-type: none"> <li>• H.323 V2</li> <li>• NetBios over IP</li> <li>• RAS Version 2</li> <li>• RTSP</li> <li>• SIP</li> <li>• XDMCP</li> <li>• Skinny</li> </ul>

## FWSM の展開

FWSM は、企業のキャンパスおよびデータ センターにサービスを提供するトポロジで展開できます。

今日の企業は単なる境界セキュリティ以上のものを必要としています。企業は、ビジネス パートナーに接続し、組織内の複数のグループを対象とするキャンパス セキュリティ ドメインを提供する必要があります。FWSM では、ユーザや管理者が組織内で複数のポリシーを使ってセキュリティ ドメインを確立できるため、柔軟で費用効果の高いパフォーマンス ベースのソリューションが提供されます。図 2 に、個別の VLAN ベースのセキュリティ ドメインを確立するために、ステートフル フィルタリングを使ったキャンパス展開を示します。

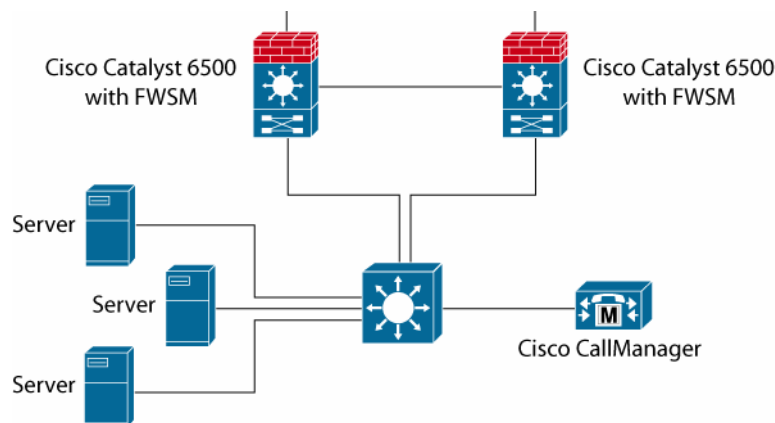
図 2 キャンパス展開



FWSM を使用すると、ユーザはさまざまな VLAN に対して適切なポリシーを設定できます。

データセンターでもデータを保護すると同時に、できる限り費用をかせげずにギガビットレベルのパフォーマンスを実現するため、ステートフルなファイアウォールセキュリティが必要です。図 3 にサーバデータを保護する冗長 FWSM を設置したデータセンターを示します。

図 3 e コマース データ センター展開



FWSM を使うと、ファイアウォールにおいて最高の価格性能比が実現されるため、資本投資が最大活用されます。またお客様はファイアウォール負荷バランシング デバイスを必要とする、コスト高の複数のファイアウォールを置き換えることができます。

### 発注情報

製品番号	説明
WS-SVC-FWM-1-K9	Cisco Catalyst 6500 対応 ファイアウォール サービス モジュール
WS-SVC-FWM-1-K9=	Cisco Catalyst 6500 対応 ファイアウォール サービス モジュール (予備)
SC-SVC-FWM-1.1-K9	Catalyst 6500 対応ファイアウォール モジュール ソフトウェア
SC-SVC-FWM-1.1-K9=	Catalyst 6500 対応ファイアウォール モジュール ソフトウェア (予備)

### ライセンス

FWSM はライセンスは不要です。

### システム要件

- Supervisor 2/Multilayer Switch Feature Card 2 (MSFC2)
- ネイティブ Cisco IOS® ソフトウェア リリース 12.1(13)E 以降
- Hybrid CatOS ソフトウェア リリース 7.5(1)以降
- Cisco Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ インターネット ルータの 1 スロットを占有
- 同一シャーシ内に最高 4 個のファイアウォール モジュール

### 認定準拠性

#### 安全性

- UL1950
- CSA-C22.2、No. 950-95
- EN60950
- EN60825-1
- TS001
- CE マーク

- IEC 60950
- AS/NZS3260

#### **EMI**

- FCC Part 15 Class A
- ICES-003 Class A
- VCCI Class B
- EN55022 Class B
- CISPR22 Class B
- CE マーク
- AS/NZS3548 Class B

#### **NEBS**

- SR-3580 - NEBS : 基準レベル (レベル 3 準拠)
- GR-63-CORE - NEBS : 物理的保護
- GR-1089-CORE - NEBS : EMC および安全性

#### **ETSI**

- ETS-300386-2 スイッチング機器

#### **テレコミュニケーション**

- ITU-T G.610
- ITU-T G.703
- ITU-T G.707
- ITU-T G.783、セクション 9 ~ 10
- ITU-T G.784
- ITU-T G.803
- ITU-T G.813
- ITU-T G.825
- ITU-T G.826
- ITU-T G.841
- ITU-T G.957 Table 3
- ITU-T G.958
- ITU-T I.361
- ITU-T I.363
- ITU I.432
- ITU-T Q.2110
- ITU-T Q.2130
- ITU-T Q.2140
- ITU-T Q.2931
- ITU-T O.151
- ITU-T O.171
- ETSI ETS 300 417-1-1
- TAS SC BISDN (1998)
- ACA TS 026 (1997)
- BAPT /TC/139 (Draft 1e)

©2006 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco ロゴは米国およびその他の国における Cisco Systems, Inc. の商標または登録商標です。  
この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。  
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。



シスコシステムズ株式会社

〒107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館  
<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/service/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