

シスコの統合型ファイアウォール ソリューション

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス、Cisco PIX セキュリティ アプライアンス、Cisco IOS Firewall、および Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ向け FWSM

ビジネスにおけるネットワークの重要性は、これまでになく高いものになっています。ネットワークは主要なアプリケーションとプロセスをサポートし、データ、音声、および映像を統合するサービスに共通のインフラストラクチャを提供します。シスコでは、お客様に最高クラスのセキュリティ ソリューションを提供することで、お客様のビジネスをサポートしています。シスコは、基本的なセキュリティ機能を備えただけの製品群を提供するのではなく、ネットワークのすべての場所にセキュリティ機能を組み込んで、すべての製品にセキュリティ サービスを統合します。これにより、セキュリティの強度が向上し、トランスペアレントで拡張性が高く管理の容易なセキュリティ インフラストラクチャを実現できます。

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス、Cisco PIX[®] セキュリティ アプライアンス、Cisco IOS[®] Advanced Security フィーチャ セット、および Cisco Catalyst[®] 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ向けセキュリティ サービス モジュールは、シスコのセキュリティ理念を反映した統合型のセキュリティ ソリューションです。これらは、ファイアウォール、侵入防止、および Virtual Private Network (VPN; 仮想私設網) の幅広いテクノロジーを単体の機器に搭載した製品です。これらのソリューションでは、単体のプラットフォームにセキュリティ サービスを統合しインテリジェントに共有しているため、高度なセキュリティを実現しながら、所有コストと運用コストを削減できます。

すべてのニーズに対応する統合型ファイアウォール ソリューション

Cisco ASA 5500 シリーズ、Cisco PIX セキュリティ アプライアンス、Cisco IOS Firewall、および Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ向け Firewall Services Module (FWSM; ファイアウォール サービス モジュール) は、シスコの柔軟性の高い統合型ファイアウォール ソリューションです。これらの製品は、モジュラ型の拡張性の高いプラットフォームをベースに、さまざまなネットワーク環境のセキュリティを強化する個別のフィーチャ セットを備えています。これらのソリューションを単独で使用すると、ネットワーク インフラストラクチャの特定の部分のセキュリティを強化できます。また、これらのソリューションを組み合わせると、シスコの SAFE ブループリントに示される設計上のベスト プラクティスに準じた多層的な階層防御セキュリティを実現できます。統合型ファイアウォール ソリューションには、シスコ セキュリティ アプライアンスと Cisco IOS ソフトウェアのセキュリティ機能、組み込み型のデバイス マネージャ、スタンドアロンの管理アプリケーションなどの幅広いセキュリティ管理製品ポートフォリオが用意されているため、お客様は、現在使用しているシスコ製セキュリティ インフラストラクチャへの投資に対する管理を効果的に行うことができます。

Cisco ASA 5500 シリーズ

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスは、革新的な適応型のアーキテクチャに基づいて設計され、豊富な実績を持つセキュリティおよび VPN サービスを統合した専用アプライアンス ソリューションです。強力な多機能セキュリティ アプライアンスにより、中堅・中小企業

から大企業までネットワークを保護しながら、新たなセキュリティ機能に必要な導入コストおよび運用コストを削減します。

Cisco ASA 5500 シリーズは、Cisco PIX 500 シリーズ セキュリティ アプライアンス、Cisco IPS 4200 シリーズ侵入防御システム、および Cisco VPN 3000 シリーズ コンセントレータ用に開発されたテクノロジーを使用しています。これらのテクノロジーは Cisco ASA 5500 シリーズで統合され、さまざまな脅威を抑制するプラットフォームを提供します。Cisco ASA 5500 シリーズは、アプリケーション セキュリティ、Anti-X 防御、ネットワークでの脅威の抑制と制御、および製品間の「クリーンな」VPN 接続を実現します(図 1 を参照)。この幅広いセキュリティにより、リモート サイト、LAN で接続された内部ユーザ、リモート アクセス VPN などの一般的な脅威の経路を含む、すべてのネットワーク セグメントが保護されます。

図 1 Cisco ASA 5500 シリーズ アプライアンスのポートフォリオ

ASA 5505	ASA 5510	ASA 5520	ASA 5540	ASA 5550
小規模ブランチ	中規模ブランチ	大企業	企業エッジ	企業エッジ/本部
				

注: 図 1 は一般的なガイドラインを示しています。ネットワーク環境は、要件に基づいて拡張する必要があります。

Cisco ASA 5500 シリーズは、レイヤ 4 ~ 7 のネットワーク フローを検査するインテリジェントなアプリケーション対応インスペクション エンジンによって、強力なアプリケーション セキュリティを提供します。これにより、Web、音声、3G モバイル ワイヤレス サービスなど、より安全なネットワークが実現します。ネットワークをアプリケーション レイヤの攻撃から保護し、企業環境で使用されるアプリケーションとプロトコルを制御するために、これらのインスペクション エンジンには、アプリケーションとプロトコルに関する幅広いナレッジが組み込まれ、プロトコル異常検出、アプリケーションとプロトコルのステート トラッキングなどのセキュリティ テクノロジーが使用されています。また、アプリケーション/プロトコルのコマンド フィルタリング、コンテンツ検証、URL 非隠蔽化などの攻撃検出/緩和テクノロジーも使用されています。これらのインスペクション エンジンにより、インスタント メッセージング、ピアツーピア ファイル共有、およびトンネリング アプリケーションも制御されるため、企業ではポリシーを適用して、クリティカルなビジネス アプリケーション用のネットワーク帯域幅を解放できます。

Cisco ASA 5500 シリーズでは、ネットワーク セキュリティが向上する一方で、導入と運用に必要なコストが削減されます。Cisco ASA 5500 シリーズの幅広い VPN およびセキュリティ サービス プロファイルにより、単一のデバイスを複数の目的に使用して、プラットフォームを標準化することができます。Cisco ASA 5500 シリーズは、アクセス コントロール、アプリケーション検査、ワーム、ウイルス、およびその他のマルウェア緩和テクノロジーを利用することで、統合型の脅威対策デバイスとして中央サイトに導入できます。また、VPN 機能を利用する専用のリモート アクセス デバイスとして使用することもできます。社内ネットワークでは、部門間のアクセス制御を行い、内部ユーザがネットワークに持ち込む可能性があるワーム、ウイルス、およびその他の悪意のあるコードを阻止します。小規模オフィスおよびブランチ オフィス環境では、Cisco ASA 5500 シリーズは、包括的な脅威対策と VPN サービスを提供する「オールインワン」デバイスとして機能し、小規模での導入や運用モデルにも適合します。この適応型の「単一デバイス、多目的」のアプローチにより、導入および管理に必要なプラットフォーム数を削減しながら、すべての導入に共通する運用/管理用の環境を実現します。このアプローチにより、コンフィギュレーション、モニタリング、トラブルシューティ

ング、およびセキュリティ スタッフのトレーニングが簡素化されます。運用コストを抑えるために、Cisco ASA 5500 シリーズはネットワークにも対応し、正規のトラフィックとアプリケーションを中断することなく、ネットワークにスムーズに統合できます(表 1 を参照)。

表 1 Cisco ASA 5500 シリーズのファイアウォール処理能力

ファイアウォール処理能力
Cisco ASA 5505: 150 Mbps
Cisco ASA 5510: 300 Mbps
Cisco ASA 5520: 450 Mbps
Cisco ASA 5540: 650 Mbps
Cisco ASA 5550: 1.2 Gbps

Cisco PIX セキュリティ アプライアンス

市場をリードする Cisco PIX セキュリティ アプライアンス シリーズは、堅牢なユーザ ポリシーおよびアプリケーション ポリシーの適用、多様な攻撃からの保護、および安全な接続サービスを、費用有効で導入が容易なソリューションで提供します。この専用のアプライアンスは、高度なアプリケーション対応ファイアウォール サービス、市場をリードする Voice over IP (VoIP) およびマルチメディア セキュリティ、堅牢なサイト間およびリモート アクセス IP Security (IPSec) VPN 接続、実績のある耐障害性、インテリジェントなネットワーク サービス、柔軟な管理ソリューションなど、多様な統合型のセキュリティおよびネットワーク サービスを提供します。Cisco PIX セキュリティ アプライアンス ファミリー(図 2)には、小規模オフィスやホーム オフィス向けのコンパクトな「プラグアンドプレイ」式デスクトップ アプライアンスから、企業環境やサービス プロバイダー環境に適した投資保護効果の高いモジュラ型ギガビット アプライアンスまで、幅広い製品が用意されています。Cisco PIX セキュリティ アプライアンスは、あらゆる規模のネットワーク環境に、堅牢なセキュリティ、パフォーマンス、および耐障害性を提供します。

Cisco PIX セキュリティ アプライアンスは、幅広い高度なファイアウォール サービスを統合して、インターネットおよび企業のネットワーク環境におけるさまざまな脅威から企業を保護します(図 2 を参照)。Cisco PIX セキュリティ アプライアンスは安全な基盤として、ステートフル インспекション ファイアウォール サービスを提供し、すべてのネットワーク通信の状態を追跡して、不正なネットワーク アクセスを防止します。Cisco PIX セキュリティ アプライアンスは、このようなサービスを基盤として、レイヤ 4 ~ 7 のネットワーク フローを検査するインテリジェントなアプリケーション対応インспекション エンジンによって、強力なアプリケーションレイヤ セキュリティを提供します。ネットワークをアプリケーション レイヤの攻撃から保護し、企業環境で使用されるアプリケーションとプロトコルを制御するために、これらのインспекション エンジンには、アプリケーションとプロトコルに関する幅広いナレッジが組み込まれ、プロトコル異常検出、アプリケーションとプロトコルのステートトラッキング、Network Address Translation (NAT; ネットワーク アドレス変換) サービス、攻撃検出/緩和技術(アプリケーション/プロトコル コマンド フィルタリング、コンテンツ検証、URL 非隠蔽化など)といったセキュリティ テクノロジーが使用されています。これらのインспекション エンジンにより、インスタント メッセージング、ピアツーピア ファイル共有、およびトンネリング アプリケーションも制御されるため、企業はポリシーを適用して、適正なビジネス アプリケーション用のネットワーク帯域幅を解放できます。

図 2 Cisco PIX セキュリティ アプライアンス ポートフォリオ

Cisco PIX 501	Cisco PIX 506E	Cisco PIX 515E	Cisco PIX 525	Cisco PIX 535
在宅勤務者/SOHO (1 ~ 20 ユーザ)	小規模ブランチ (20 ~ 99 ユーザ)	中規模ブランチ (100 ~ 999 ユーザ)	中大規模ブランチ、 企業エッジ	企業本部/データ センター
				

注: 図 2 は一般的なガイドラインを示しています。ネットワーク環境は、ネットワークの規模だけでなく、アプリケーション要件に基づいて拡張する必要があります。

豊富なセキュリティ サービスを備えた専用のオペレーティング システム(OS)を搭載した Cisco PIX セキュリティ アプライアンスは、最高レベルのセキュリティを提供し、Common Criteria Evaluation Assurance Level 4 (EAL 4) や ICSA Labs Firewall and IP Security (IPSec) 認定を含む多数の業界評価や認定を取得しています。Cisco PIX セキュリティ アプライアンスは、H.323 バージョン 4、Session Initiation Protocol (SIP)、Cisco Skinny Client Control Protocol (SCCP)、Real-Time Streaming Protocol (RTSP)、Media Gateway Control Protocol (MGCP) など、その他のさまざまな VoIP マルチメディア規格に対応した市場最高レベルの保護が用意されており、企業は現在および次世代のさまざまな VoIP/マルチメディア アプリケーションを安全に導入できます。

Cisco PIX セキュリティ アプライアンスは、さまざまなコンフィギュレーション、モニタリング、およびトラブルシューティングのためのオプションを提供し、企業のニーズに適した方法を柔軟に使用できるようにします。管理ソリューションには、中央集中型のポリシーベース管理ツールや Web ベースの統合管理ツールなどがあります。これらのソリューションは、SNMP (簡易ネットワーク管理プロトコル) などのリモート モニタリング プロトコルや Syslog をサポートしています。統合型の Cisco Adaptive Security Device Manager (ASDM) は、管理者のコンピュータにソフトウェア (標準の Web ブラウザと Java プラグイン以外) をインストールしなくても、単一の Cisco PIX セキュリティ アプライアンスの導入、継続的な設定、およびモニタリングを簡素化する、優れた Web ベースの管理インターフェイスを提供します。管理者は、CLI (コマンドライン インターフェイス) を使用して、Cisco PIX セキュリティ アプライアンスの設定、モニタ、およびトラブルシューティングをリモートで実行することもできます。Secure Shell (SSHv2) プロトコル、Telnet over IPSec、コンソール ポート経由のアウトオブバンドなど、複数の方法を使用することで、CLI に安全にアクセスできます。また、セキュアな遠隔管理による自動更新機能が用意されているため、ファイアウォールのコンフィギュレーションやソフトウェア イメージを常に最新の状態に維持できます。

表 2 は、Cisco PIX セキュリティ アプライアンスの各モデルのファイアウォール処理能力を示しています。

表 2 Cisco PIX セキュリティ アプライアンスのファイアウォール処理能力

ファイアウォール処理能力
Cisco PIX 501: 60 Mbps
Cisco PIX 506E: 100 Mbps
Cisco PIX 515E: 190 Mbps
Cisco PIX 525: 330 Mbps
Cisco PIX 535: 1.7 Gbps

Cisco IOS Firewall

Cisco IOS Firewall は、シスコ ルータで使用できるステートフル インспекション ファイアウォール オプションです。Cisco IOS Firewall は、業界トップクラスの PIX Firewall テクノロジーをベースにして構築され、Cisco IOS ソフトウェアの Advanced Security フィーチャ セット(またはさらに上位のフィーチャ セット)を搭載したすべてのサービス統合型ルータでサポートされています。Cisco IOS Firewall は、ネットワークへの WAN エントリ ポイントを保護するのに適した単一の機器によるセキュリティおよびルーティング ソリューションです。Cisco IOS Firewall の主な特長として、DoS 保護機能を備えたステートフル ファイアウォール、アプリケーションを識別、検査、制御するために強化されたアプリケーション、トラフィック、およびユーザ認識、音声、ビデオ、およびその他のアプリケーションに対応する拡張プロトコル インспекション、ユーザ、インターフェイス、またはサブインターフェイスごとのセキュリティ ポリシー、ユーザごとの認証と許可を提供するために厳密に統合された識別サービス、管理の容易さなどがあります。精度の高いロールベースのアクセスにより、ネットワーク運用スタッフとセキュリティ運用スタッフの間でルータ管理を安全かつ論理的に分離できます。

Cisco IOS Firewall を利用すると、ネットワーク境界部分のシングル ポイントを保護できるだけでなく、ネットワークそのものにセキュリティ ポリシーを実施する機能を組み込むことができます。Cisco IOS Firewall は、多数の Cisco IOS ルータ上で動作するため、Quality of Service (QoS; サービス品質)、マルチプロトコル、マルチキャスト、および高度なルーティングなどの Cisco IOS ソフトウェアの機能を引き続き利用しながら、ネットワーク インフラストラクチャのセキュリティを向上しようと検討している中小・中堅企業のお客様に最適です(図 3 を参照)。

図 3 Cisco IOS Firewall ポートフォリオ

Cisco ISR 1841	Cisco ISR 2801	Cisco ISR 2811	Cisco ISR 2821	Cisco ISR 2851	Cisco ISR 3825	Cisco ISR 3845
小規模ブランチ	中規模ブランチ	中規模ブランチ	中規模ブランチ	中規模ブランチ	大規模ブランチ	大規模ブランチ
						

注: 図 3 は一般的なガイドラインを示しています。ネットワーク環境は、ネットワークの規模だけでなく、アプリケーション要件に基づいて拡張する必要があります。

統合型 Cisco IOS Firewall は、アプリケーション レベルのインテリジェンスに基づいたダイナミックなトラフィック フロー制御が可能な優れたファイアウォール エンジンを使用して、複雑なアプリケーションに対して高度なセキュリティを提供します。Cisco IOS Firewall には、Hypertext Transport Protocol (HTTP; ハイパーテキスト転送プロトコル) と E メールに対応した高度なアプリケーション インспекションおよび制御も含まれます。Cisco IOS Firewall HTTP Inspection Engine はプロトコル適合検査を実施し、ポート 80 トンネリング、不正パケット、トロイの木馬などの悪意のある不正な動作が通過するのを防ぎます。Cisco IOS Firewall で HTTP Inspection Engine を利用すると、非 HTTP トラフィックをブロックできるばかりではなく、HTTP と推定されるトラフィックが本物の Web ブラウジングであり、ファイアウォール経由でアクセスしようとするインスタント メッセージングなどではないことを確認できます。それにより、ネットワーク管理者は、ファイアウォールを通過するアプリケーションをより詳細に制御できるようになります。

シスコのサービス統合型ルータには、Cisco IDS ファミリーからのテクノロジーを利用する Intrusion Prevention System (IPS; 侵入防御システム) も含まれています。Cisco IOS IPS は、シスコ ルータがネットワーク攻撃を効果的に軽減できるようにするインライン ディープパケット インспекション

ベースのソリューションです。Cisco IOS ソフトウェア IPS はインラインのため、トラフィックを廃棄することができ、ルータはセキュリティの脅威にただちに反応してネットワークを保護します。

Cisco IOS の IPSec は、Common Criteria EAL 4 や ICASA Labs IPSec 認定などの業界認定を取得しています。Cisco IOS Firewall のその他の機能には、音声トラバーサルサポートや IPv6 のサポート、トランスパレント ファイアウォール、URL フィルタリング、VRF 環境用の個別のファイアウォール コンテキストのサポート、Cisco Network Admission Control (NAC) のサポート、フェールオーバーのサポート、Network Address Translation (NAT; ネットワーク アドレス変換) のサポート、時間ベースのアクセス リスト、Java Applet ブロッキング、ピア ルータ認証、リアルタイムのアラート、監査証跡、イベント ログイングなどがあります。また、Cisco IOS Firewall は ICASA Firewall の認定を得ています。

Cisco IOS Firewall を管理するには、Telnet、SSH、またはコンソール ポート経由のアウトバンドなどのさまざまな方法で CLI を使用します。また、Cisco IOS Firewall に組み込まれた使いやすいセキュアな Web ベースのデバイス管理ツールである Cisco Security Device Manager (SDM) を使用して、Cisco IOS Firewall の設定およびモニタリングを行うこともできます。Cisco SDM を使用すると、優れたウィザードによってデバイスやセキュリティの設定を簡素化できるため、Cisco IOS の CLI に関する十分な知識がなくても、Cisco IOS Firewall の導入、設定、およびモニタリングを容易に実行できます。また、Cisco IOS Firewall には、Cisco AutoSecure が搭載されています。AutoSecure は、Cisco IOS ソフトウェア リリース 12.3 から導入された機能で、セキュリティ機能の設定とデフォルトで有効になっているセキュアでない機能の解除を自動的に行うことにより、ルータの複雑なセキュリティ設定を簡素化します。この新たな機能を使用すると、セキュリティ プロセスを簡素化できるため、セキュリティに関するポリシーと手順を迅速に実装して、セキュアなネットワーク サービスを実装できます。Cisco IOS Firewall の設定とモニタリングには、Cisco AVVID パートナーが提供するツールを使用することもできます。

表 3 は、Cisco IOS Firewall が稼働する Cisco IOS ルータ プラットフォームのファイアウォール処理能力を示しています。性能値は、NAT とログイングの両方を有効にしてテストした場合の結果を反映しています。

表 3 Cisco IOS Firewall の処理能力

ファイアウォール処理能力
Cisco ISR 1841: 125 Mbps
Cisco ISR 2801: 127 Mbps
Cisco ISR 2811: 130 Mbps
Cisco ISR 2851: 455 Mbps
Cisco ISR 3825: 530 Mbps
Cisco ISR 3845: 855 Mbps
Cisco ISR 3845: 1.1 Gbps

Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ向け Cisco FWSM

Cisco FWSM は、Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ向けの高性能統合型ファイアウォール モジュールです。このモジュールは、業界最高レベルのファイアウォール データ レートである 5 Gbps のスループット、100,000 cps (connections per second)、および 100 万同時接続を実現します。同一のシャーシに最大 4 つの Cisco FWSM を設置できるため、シャーシ単位で 20 Gbps の優れたファイアウォール処理能力を実現できます。

FWSM は、Intrusion Detection Service Module (IDSM-2)、IPSec VPN Service Module (VPNSM)、および Network Analysis Module (NAM-1 および NAM-2) シリーズなどのシスコ製セキュリティ サービス モジュールと組み合わせて使用することもできます。各モジュールを組み合わせて使用できるため、お客様は既存のスイッチングおよびルーティング インフラストラクチャを低コストで活用しながら、業界最高レベルのパフォーマンスを実現できます。FWSM は企業とサービスプロバイダーのデータ センター、および企業のキャンパス ディストリビューション ポイントに最適なソリューションです。

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 ルータに FWSM を搭載すると、任意のポートをファイアウォール ポートとして機能させて、ネットワーク インフラストラクチャ内にステートフルなファイアウォール セキュリティを統合することができます。これは、ラック スペースが限られている場合には特に重要です。Cisco Catalyst 6500 は、マルチレイヤ型の LAN、WAN、および MAN スwitching機能だけでなく、ファイアウォール サービス、侵入検知、および VPN などのインテリジェントなサービスを必要としているお客様に適した IP サービス スイッチになっています (図 4 を参照)。

図 4 Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータの Cisco FWSM



Cisco FWSM は Cisco PIX テクノロジーに基づき、セキュアなリアルタイム OS として実績のある Cisco PIX OS を使用します。FWSM は、パケット検査で実績のある Cisco PIX テクノロジーを使用して、同一のプラットフォーム上でパフォーマンスとセキュリティを両立させます。

Cisco Catalyst 6500 シリーズ スイッチでは、CiscoView Device Manager (CVDM) が Cisco FWSM をサポートすることで、初期設定を実行し、すべてのサービスにグラフィカルな VLAN 仮想化を提供します。組み込みのマネージャである Cisco PIX Device Manager (PDM) は、詳細な設定、モニタリング、およびトラブルシューティングを行い、CVDM から起動することもできます。

シスコの統合型ファイアウォール ソリューションを利用する場合のガイドライン

Cisco ASA 5500 シリーズ、Cisco PIX セキュリティ アプライアンス、Cisco IOS Firewall、および Cisco FWSM には、いずれも最先端のファイアウォール テクノロジーが搭載されており、多数の共通の利点と機能を有していますが、これらのソリューションはいずれも、特定の環境を対象に設計されたものです。以下の表は、これらのソリューションの類似点と相違点を示しています。以下の内容は一般的なガイドラインですが、ネットワーク設計者が状況に応じて使用するソリューションを判断し、それぞれの機能を最大限に活かす方法を理解するのに役立ちます (表 4 ~ 8 を参照)。

表 4 Cisco ASA 5500 シリーズ、Cisco PIX セキュリティ アプライアンス、Cisco IOS Firewall、および Cisco FWSM に共通の機能と利点

機能	利点
ステートフル インспекション ファイアウォール	管理者定義のアクセス制御ポリシー、詳細なパケット検査、およびすべてのネットワーク通信の状態監視を行うことにより、堅牢なネットワークとアプリケーション セキュリティを実現します。

機能	利点
アプリケーション/プロトコルの検査および制御	レイヤ 4 ~ 7 のデータ ストリームを検査できる専用の検査エンジンを使用して、アプリケーションとプロトコルの高度なセキュリティを実現します。
ダイナミックなユーザ単位の認証および許可	Remote Authentication Dial-In User Service (RADIUS) および Terminal Access Controller Access Control System Plus (TACACS+) プロトコルを使用して、ハイ パフォーマンスのカットスルー プロキシ メカニズムを介して Cisco Secure Access Control Sever (ACS) と統合することにより、柔軟性の高いユーザ認証および許可を実現します。ACS は、Microsoft Active Directory、Microsoft Windows NT ドメイン、LDAP ディレクトリ、およびワンタイム パスワード システムなどのさまざまなユーザ データベースと統合できます。
ダイナミック/スタティック NAT および Port Address Translation (PAT; ポート アドレス変換)	各種 NAT アプリケーションおよびプロトコルをサポートし、内部のネットワーク アドレスを外部から保護して、セキュリティ機能を強化します。
コンテンツ フィルタリング	URL フィルタリングをサポートし、不正な Java アプレットをブロックする機能を備えたサードパーティ製 URL フィルタリング ソリューションと統合することによって、社員の生産性を向上させます。
リモート管理	コンフィギュレーション、モニタリング、およびトラブルシューティングを行うための豊富なリモート管理方式を提供します。管理ソリューションには、拡張性の高い中央集中型の管理ツールや Web ベースの統合管理ツールなどがあります。これらのソリューションは、SNMP (簡易ネットワーク管理プロトコル) などのリモート管理プロトコルや Syslog をサポートしています。
Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウントिंग) に基づいた管理アクセス制御	TACACS+ および RADIUS プロトコルによって実現される AAA サービスに基づいて、管理アクセスの詳細な制御を可能にします。この機能を使用すると、管理者は各管理ユーザまたはグループに許可されているサービスやコマンドのレベルに対してアクセス ポリシーを適用できます。
複数の DMZ サポート	共有ネットワーク (DMZ) 上にある Web、E メール、FTP、または DNS などのサーバへの保護アクセスを可能にする物理または仮想ネットワーク インターフェイスを追加できます。
各種マルチメディアのサポート (ストリーミング ビデオ、ストリーミング オーディオ、および音声アプリケーションなど)	各種 VoIP 規格やマルチメディア規格に対応する豊富なステートフル インспекション ファイアウォール サービスを提供します。この機能を使用すると、企業はデータ、音声、および映像の統合ネットワークによって実現される生産性の向上や競争力の強化などといった多数の利点を安全に利用できます。
DoS 攻撃からの保護	DoS 攻撃の阻止および軽減を行う TCP 代行受信、TCP SYN クッキー、DNS Guard、Flood Defender、Flood Guard、Mail Guard、Unicast Reverse Path Forwarding (uRPF) などのさまざまなメカニズムを提供します。
セキュアなダイナミック ルーティング	Routing Information Protocol (RIP) および Open Shortest Path First (OSPF) に対して、Message Digest Algorithm 5 (MD5) ベースのプレーン テキスト ルーティング認証をサポートし、ルート スプーフィングやさまざまなルーティングベースの DoS 攻撃を防御します。
ファイアウォールの仮想化	デバイスを複数の仮想ファイアウォール、またはセキュリティ コンテキストにパーティション化できます。組織は各仮想ファイアウォールを個別に管理し、同一の物理インフラストラクチャ上で事業部門や業務領域を分離できます。同様に、サービス プロバイダーはファイアウォール仮想化を利用して、単一の物理デバイス上で複数のカスタマーをサポートおよび分離できます。

表 5 Cisco ASA 5500 適応型セキュリティ アプライアンスの機能

お客様の要求事項	Cisco ASA 5500 セキュリティ アプライアンスの利点
専用の高性能「統合型」セキュリティ アプライアンス	Cisco ASA シリーズ デバイスは、ステートフル インспекション ファイアウォール、IPS、VPN、ワームおよびマルウェア被害の軽減、ネットワーク アンチウイルス、VPN クラスタリング、およびモジュラ型セキュリティ サービス スロットなどの最新の統合型ネットワーク セキュリティ サービスを提供します。Cisco ASA 5500 シリーズ デバイスは Cisco PIX アプライアンスと完全に互換性があり、導入時にはお客様の要求事項に応えるためにその両方を利用できます。
ヘッドエンドおよびブランチ オフィス向けの多目的の単一セキュリティ アプライアンス	アクセス コントロール、アプリケーション検査、ワーム、ウイルス、およびマルウェア緩和テクノロジーを利用することで、統合型の脅威対策デバイスとして導入できます。Cisco ASA シリーズは、IPSec および SSL VPN 機能を利用するリモート アクセス デバイスとして導入できます。社内ネットワークでは、部門間のアクセス制御に使用して、内部ユーザが無意識にネットワークに持ち込む可能性があるワーム、ウイルス、およびその他の悪意のあるコードから保護できます。いずれの場合も、Cisco ASA デバイスは最も機能豊富なシスコ ソリューションとなります。
運用コストを削減した統合型アプライアンス	「単一デバイス、多目的」のアプローチにより、導入および管理に必要なプラットフォーム数を削減しながら、すべての導入に共通する運用/管理用の環境を実現します。このアプローチにより、コンフィギュレーション、モニタリング、トラブルシューティング、およびセキュリティ スタッフトレーニングが簡素化されます。

お客様の要求事項	Cisco ASA 5500 セキュリティ アプライアンスの利点
ハイアベイラビリティ	Cisco ASA 5500 セキュリティ アプライアンスは、フェールオーバー ペアとして構成した場合、ステートフルなフェールオーバーを提供し、接続状態と機器の接続データが常に同期されます。これにより、ユーザに影響を与えることなく、ネットワーク セッションが自動的に切り替わります。

表 6 Cisco PIX セキュリティ アプライアンスの機能

お客様の要求事項	Cisco PIX セキュリティ アプライアンスの利点
専用の高性能オールインワン セキュリティ アプライアンス	Cisco PIX セキュリティ アプライアンスは、ステートフル インспекション ファイアウォール、アプリケーション検査、VPN、インライン侵入防止、およびマルチメディア/音声セキュリティなどの最新の統合型ネットワーク セキュリティ サービスを提供します。Cisco PIX セキュリティ アプライアンスは Cisco ASA 5500 シリーズ デバイスと完全に互換性があり、導入時にはお客様の要求事項に応えるためにその両方を利用できます。
企業のヘッドエンドおよびデータ センター向けの専用デバイス	Cisco PIX セキュリティ アプライアンスはセキュリティに特化した製品で、強化された組み込み型 OS を使用しているため、汎用 OS の一般的なセキュリティ ホールの影響を受けることがなく、あらゆる面で優れたセキュリティ システムを実現できます。
セキュリティ インフラストラクチャの分離	Cisco PIX セキュリティ アプライアンスは、専用のセキュリティ システムとして実装できます。Cisco PIX セキュリティ アプライアンスの高度なセキュリティ機能を使用すると、ネットワークからセキュリティ インフラストラクチャを効果的に分離できます。
ハイアベイラビリティ	Cisco ASA 5500 シリーズ アプライアンスと同様に、Cisco PIX セキュリティ アプライアンスは、フェールオーバー ペアとして構成した場合、ステートフルなフェールオーバーを提供し、接続状態と機器の接続データが常に同期されます。これにより、ユーザに影響を与えることなく、ネットワーク セッションが自動的に切り替わります。
Small Office/Home Office (SOHO; スモールオフィス、ホーム オフィス) 向けアプライアンス	Cisco PIX 501 セキュリティ アプライアンスは、コンパクトなオールインワンセキュリティソリューションで、豊富な機能を備えた統合型セキュリティ サービス、高度なネットワーク サービス、および強力なリモート管理機能を提供します。SOHO および在宅勤務者環境向けに、信頼性が高く導入が容易な専用アプライアンスを使用して、エンタープライズ クラスのセキュリティを提供します。

表 7 Cisco IOS Firewall の機能

お客様の要求事項	Cisco IOS Firewall の利点
優れたセキュリティ、QoS、マルチプロトコル ルーティング、統合型 WAN インターフェイス、および音声アプリケーションを統合したワンボックス ソリューション	Cisco IOS の Advanced Security フィーチャ セットを使用すると、ステートフル パケット フィルタリング、侵入検知、侵入防止、ユーザ単位の認証と許可、VPN 機能、各種 QoS メカニズム、マルチプロトコル ルーティング、音声アプリケーション サポート、および内蔵 WAN インターフェイスなどを備えた統合型セキュリティ ソリューションを単一の機器で実現できます。
ネットワーク インフラストラクチャを活用してセキュリティ機能を実現	Cisco IOS Firewall は既存の Cisco IOS ルータ上に搭載できるため、ネットワーク インフラストラクチャの優れた投資保護が可能です。同じハードウェアのシャーシとコンポーネントを再利用すると、所有コストだけでなく、運用コストも削減されます。これは、同じ管理インフラストラクチャを使用でき、スタッフの追加トレーニングも必要ないためです。
ファイアウォール機能と各種 VPN サポートを単一の機器に統合	Cisco IOS Firewall を Cisco IOS の暗号化機能や QoS VPN 機能と併用すると、パブリック ネットワーク経由のセキュアで安価な通信が可能になります。Cisco IOS Firewall は、Dynamic Multipoint VPN (DMVPN)、IPSec ステートフル フェールオーバー、Easy VPN Remote、Easy VPN Server、サイト間 VPN、Advanced Encryption Standard (AES)、VPN アクセラレーションカード、Voice and Video-Enabled VPN (V3PN)、および VPN QoS などの幅広い VPN 機能をサポートしています。

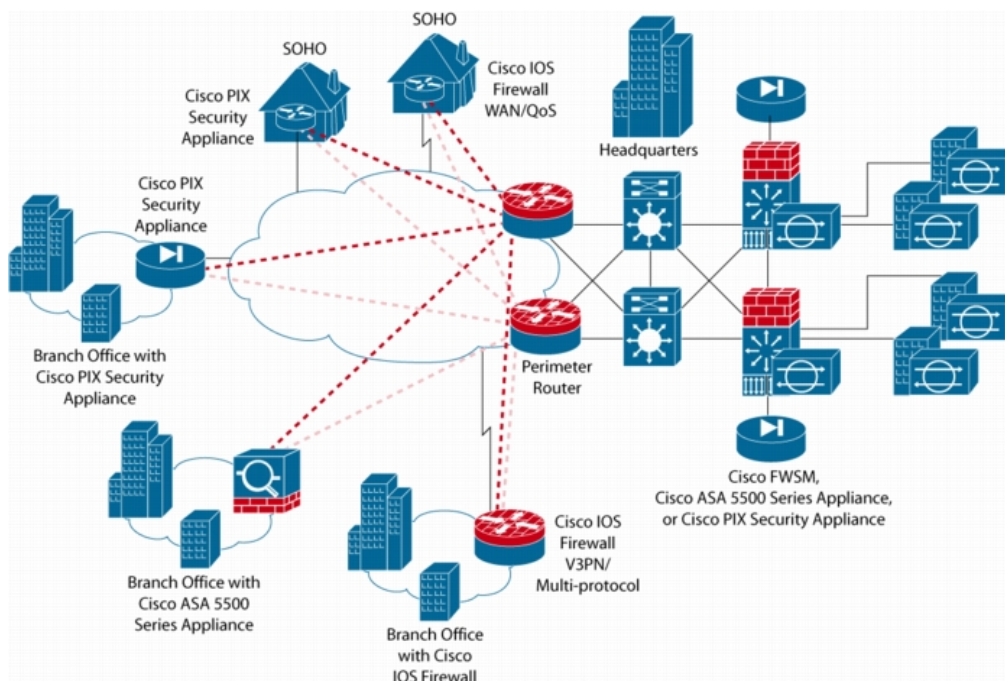
表 8 Cisco FWSM の機能

お客様の要求事項	Cisco FWSM の利点
サービス プロバイダーと大企業のヘッドエンドおよびデータセンター	Cisco FWSM のパフォーマンス、スケーラビリティ、および仮想化機能は、サービス プロバイダーと大企業のヘッドエンドおよびデータセンターでの使用に最適です。Cisco FWSM は、業界最高レベルのファイアウォール性能 (5 Gbps のスループット、100,000 cps、および 100 万同時接続) を実現します。同一のシャーシで最大 4 つの FWSM を使用できるため、全体で 20 Gbps の処理能力を実現できます。1 つの FWSM は最大 1000 の仮想インターフェイス (コンテキストごとに 256) をサポートでき、1 つのシャーシで VLAN を最大 4000 まで拡張できます。1 つの FWSM を最大 100 の仮想ファイアウォール (セキュリティ コンテキスト) にパーティション化できます。

お客様の要求事項	Cisco FWSM の利点
	FWSM Resource Manager を使用すると、組織はセキュリティ コンテキストに割り当てられるリソースをいつでも制限できるため、セキュリティ コンテキスト間で干渉が発生しないようになります。
ヘッドエンドまたはデータ センターにあるネットワークおよびスイッチング インフラストラクチャを 活用	Cisco FWSM は既存の Cisco Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータに導入できるため、優れた投資保護、および高速のスイッチングやルーティングとの統合が可能です。また、FWSM は、透過的なレイヤ 2 ブリッジング モードとレイヤ 3 ルーティング モードの両方で導入できます。透過的なレイヤ 2 ファイアウォールによりネットワーク統合が簡素化され、ルーティングを行わなくても、同じサブネット内でトラフィックをファイアウォールで制御できます。
ハイアベイラビリティ	Cisco FWSM を二重化すると、シャーン内またはシャーン間でのステートフル フェールオーバー サービスが可能になるため、最も重要性の高い環境で障害に強いネットワーク保護を実現できます。フェールオーバー モードで構成されたモジュールは、接続状態と機器の接続データを常に同期させます。障害が発生すると、モジュールは自動的にフェールオーバーして、ユーザに影響を与えることはありません。

図 5 は、シスコの統合型ファイアウォール ソリューションを組み合わせた企業ネットワークのセキュリティ対策を示しています。

図 5 シスコの統合型ファイアウォール ソリューションを組み合わせた企業ネットワークのセキュリティ対策



シスコのセキュリティ管理ソリューション

シスコでは、シスコのファイアウォール ソリューションに組み込まれたデバイス マネージャのほか、統合型のセキュリティ管理アプリケーションを用意しています。ファイアウォール ソリューションに組み込まれたデバイス マネージャは 1 ～ 5 台のデバイスを管理できるように設計されていますが、より多くのデバイスを管理する必要があるお客様には、統合型のセキュリティ管理アプリケーションが適しています。

シスコのファイアウォール ソリューションでセキュリティ管理、ポリシー管理、モニタリング、および分析を行う必要のあるお客様向けに、シスコは CiscoWorks VPN/Security Management Solution (VMS)を提供しています。CiscoWorks VMS は企業ネットワークのセキュリティを実現する Cisco SAFE ブループリントに不可欠な要素で、VPN、ファイアウォール、およびネットワーク/ホストベ

スの Intrusion Detection System (IDS; 侵入検知システム) の設定、モニタリング、およびトラブルシューティングを行う Web ベースのツールと組み合わせて使用することで企業活動を保護します。CiscoWorks VMS を使用すると、VPN の構成管理、ファイアウォール管理、監視、デバイスのインベントリ管理、およびソフトウェア バージョン管理などの機能を単一の管理コンソールから利用できます。

シスコでは、セキュリティ情報を一元的に管理できるように、Cisco Security Monitoring, Analysis and Response System (MARS) を提供しています。Cisco Security MARS は、ネットワーク デバイスとセキュリティ対策を強化するハイパフォーマンスのスケラブルな脅威抑制アプライアンスファミリです。Cisco Security MARS は、ネットワーク トポロジー インテリジェンス、さまざまなコンテキストの相関分析、分析および被害の拡散防止の自動化機能と組み合わせることで、ネットワーク攻撃を識別、管理、および排除し、セキュリティ ポリシーを維持できます。

シスコでは、大企業のお客様やサービス プロバイダー向けに、CiscoWorks Security Information Management Solution (SIMS) も提供しています。CiscoWorks SIMS を使用すると、お客様はセキュリティ スタッフを増やすことなく、拡大するマルチベンダー セキュリティ インフラストラクチャを管理できます。CiscoWorks SIMS を使用すると、お客様はセキュリティ デバイスやセキュリティ アプリケーションから毎日送信される多数のセキュリティ アラートの標準化、集約、相関処理、および視覚化を行うことができます。CiscoWorks SIMS には、大規模な構成に適した多層構造のサーバアーキテクチャを柔軟に実装できるソフトウェアのみのオプションと、Cisco 1160 ハードウェア ソリューション プラットフォームに CiscoWorks SIMS がプレインストールされたアプライアンス オプションが用意されています。

シスコのファイアウォール ソリューションをベースにしたファイアウォール マネージド サービスの提供を検討しているお客様向けに、シスコは Cisco IP Solution Center (ISC) を提供しています。Cisco ISC は、ビジネス中心のポリシーレベル管理モデルを実装しているため、お客様はハイレベルなセキュリティ ポリシーを定義できるだけでなく、特定のネットワーク デバイスに対するポリシーの適用を Cisco ISC ソフトウェアにオフロードできます。Cisco ISC セキュリティ管理モジュールは、シスコの各種セキュリティ デバイス (Cisco IOS Firewall、Cisco PIX セキュリティ アプライアンス、および Cisco VPN 3000 シリーズ コンセントレータなど) の LAN 間 VPN、リモートアクセス VPN、EZ VPN、DMVPN、ファイアウォール、NAT、および QoS のプロビジョニングと管理をフルサポートしています。

発注情報

シスコ製品の購入方法の詳細は、[「購入案内」](#)を参照してください。

関連情報

詳細は、以下のリンクをご覧ください。

Cisco ASA 5500 シリーズ セキュリティ アプライアンス: <http://www.cisco.com/jp/go/asa>

Cisco PIX セキュリティ アプライアンス シリーズ: <http://www.cisco.com/jp/go/pix>

Cisco IOS Firewall: <http://www.cisco.com/jp/product/hs/security/iosfeature>

シスコのルータ セキュリティ: <http://www.cisco.com/jp/product/hs/ios/security>

Cisco Firewall Services Module (FWSM):

<http://www.cisco.com/jp/product/hs/switches/cat6500/modules/service/fwsm>

Cisco PIX Device Manager: <http://www.cisco.com/jp/product/hs/netmgt/pdm>

Cisco Security Device Manager: <http://www.cisco.com/jp/product/hs/security/csdm>

CiscoWorks VMS: <http://www.cisco.com/jp/product/hs/netmgt/cw2000/vpnsms>

©2007 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。



シスコシステムズ株式会社

〒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