

Cisco PIX セキュリティ アプライアンス ソフトウェア バージョン 7.0

バージョン 7.0 の特徴

高度なファイアウォール サービス

- HTTP、FTP、ESMTP などに対応した詳細なインスペクション ファイアウォール サービス
- インスタント メッセージング、ピアツーピア、およびトンネリング アプリケーションのブロック
- フローベースのセキュリティ ポリシーを備えたシスコのモジュラ型ポリシー フレームワーク
- 仮想ファイアウォール サービス
- レイヤ 2 トランスペアレント ファイアウォール
- 3G モバイル無線セキュリティ サービス

安定した IPSec VPN サービス

- VPN クライアントのセキュリティ ポスチャの実施
- VPN クライアント ソフトウェアの自動アップデート
- VPN トンネルでの OSPF ダイナミック ルーティング

ハイ アベイラビリティ サービス

- 非対称ルーティングをサポートするアクティブ/アクティブ フェールオーバー
- リモート アクセスおよびサイトツーサイト VPN のステートフル フェールオーバー
- ゼロダウンタイム ソフトウェア アップグレード

インテリジェント ネットワーク サービス

- PIM マルチキャスト ルーティング
- QoS
- IPv6 ネットワーキング

柔軟な管理ソリューション

- SSHv2 と SNMPv2c
- コンフィギュレーションのロールバック
- ユーザビリティの強化

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、ユーザおよびアプリケーション ポリシーの実施、マルチベクタ攻撃からの保護、およびセキュア コネクティビティ サービスを、費用効率が高く展開しやすいソリューションとして提供します。

この専用アプライアンスは、以下のようなさまざまな統合セキュリティおよび統合ネットワーク サービスを提供します。

- 高度なアプリケーション対応のファイアウォール 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
- 安定したサイト間およびリモート アクセス IP Security (IPSec) Virtual Private Network (VPN; 仮想私設網) 接続
- 評価の高い耐障害性
- インテリジェント ネットワーキング サービス
- 柔軟な管理ソリューション

SOHO 向けのコンパクトなデスクトップ アプライアンスから、大企業およびサービス プロバイダー環境向けの投資保護に優れたモジュラ型ギガビット アプライアンスまで、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で、強固なセキュリティ、パフォーマンス、および信頼性を実現します。

高度なファイアウォール サービスで企業を強力に保護し、豊富なアプリケーション制御を提供

強固なステートフル インスペクションとアプリケーション層セキュリティ

Cisco PIX セキュリティ アプライアンスは幅広く高度なファイアウォール サービスを備え、インターネットおよびビジネス ネットワーク環境での絶え間ない脅威から企業を保護します。Cisco PIX セキュリティ アプライアンスは、安全の土台として豊富なステートフル インスペクション 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、未認証のネットワーク アクセスを防止します。これらのサービスに加えて、Cisco PIX セキュリティ アプライアンスは、レイヤ 4～7 でネットワーク 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認識インスペクション エンジンによって、強力なアプリケーション層セキュリティを提供します。アプリケーション層への攻撃からネットワークを防御し、自社の環境で使用されているアプリケーションとプロトコルに対する制御を拡張するため、これらのインスペクション エンジンには幅広いアプリケーションおよびプロトコル情報が組み込まれ、各種のセキュリティ実現テクノロジーが使用されています。これには、プロトコル異常検出、アプリケーションとプロトコルの状態追跡、Network Address Translation (NAT; ネットワーク アドレス変換) サービス、およびアプリケーションと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 解読などの攻撃検出および緩和技術が含まれます。またこれらのインスペクション エンジンで、企業はインスタント メッセージング、ピアツーピアのファイル共有、およびトンネリング アプリケーションの制御が可能となるため、使用ポリシーを実施してネットワーク帯域幅を正規のビジネス アプリケーションに振り向けることができます。

マルチベクタ攻撃防御

Cisco PIX セキュリティ アプライアンスにはマルチベクタ攻撃防御サービスが組み込まれており、Denial of Service (DoS) 攻撃、フラグメント攻撃、リプレイ攻撃、および不正パケット攻撃など、多くの一般的な攻撃形態から企業を防御します。Cisco PIX セキュリティ アプライアンスは、TCP ストリームの再構築、トラフィックの正規化、DNSGuard、FloodGuard、FragGuard、MailGuard、IPVerify、および TCP インターセプトといった多数の拡張攻撃保護機能を利用して、さまざまな攻撃を識別阻止し、管理者に対してリアルタイムで警告を發します。

柔軟なアクセス制御と強力なフローベースのポリシー

管理者は、Cisco PIX セキュリティ アプライアンスが提供する柔軟なアクセス制御テクノロジーを使用して、カスタム セキュリティ ポリシーを簡単に作成できます。これには、ネットワークおよびサービス オブジェクト グループ、ユーザベースおよびグループベースのポリシー、100 以上の定義済みアプリケーションおよびプロトコルなどがあります。Cisco PIX セキュリティ アプライアンス ソフトウェア バージョン 7.0 で導入された強力なモジュラ型ポリシー フレームワークを使用すれば、管理者はフローベースおよびクラスベースのポリシーを精密に定義し、一連のカスタマイズ可能なセキュリティ サービス（インスペクション エンジン ポリシー、Quality of Service [QoS; サービス品質] ポリシー、接続タイマーなど）を、管理者が指定する各トラフィック フローまたはクラスに適用できます。Cisco PIX セキュリティ アプライアンスが提供する、これらの柔軟なアクセス制御とフロー単位またはクラス単位のセキュリティ サービス、強力なステートフル インスペクションとアプリケーション認識ファイアウォール サービス、およびマルチベクタ攻撃保護サービスを組み合わせれば、企業は包括的なセキュリティ ポリシーを実施して自社を攻撃から保護できます。

市場をリードする Voice over IP セキュリティ サービスで次世代の統合ネットワークを保護

Cisco PIX セキュリティ アプライアンスは、VoIP やその他のさまざまなマルチメディア規格に対応するトップレベルの保護機能を提供します。これによって企業は、生産性の向上、運用コストの削減、競争力の強化など、データ、音声、および映像をサポートする統合ネットワークがもたらす多くの利点を安全に活用できます。これらの統合ネットワーク規格用に、Cisco PIX セキュリティ アプライアンスが提供する高度なプロトコル インスペクション サービスと VPN および QoS を組み合わせれば、企業は音声およびマルチメディア サービスを安全に拡大し、リモート オフィス、ホーム オフィス、およびモバイル ユーザに、より大きな利益を提供できます。

Cisco PIX セキュリティ アプライアンスがサポートする VoIP とマルチメディアの規格には、H.323 バージョン 4、Session Initiation Protocol (SIP)、Cisco Skinny Client Control Protocol (SCCP)、Real-Time Streaming Protocol (RTSP)、および Media Gateway Control Protocol (MGCP) などがあり、企業が現在および次世代の、さまざまな VoIP およびマルチメディア アプリケーションを安全に展開するのに役立ちます。Cisco PIX セキュリティ アプライアンスは、Telephony Application Programming Interface (TAPI) ベースおよび Java TAPI (JTAPI) ベースのアプリケーションが、Cisco IP SoftPhone や Cisco Customer Response Solution (CRS) と同様に、ネットワーク伝送メカニズムとして Computer Telephony Interface Quick Buffer Encoding (CTIQBE) を使用している場合、それに対応したセキュリティ サービスも提供します。

安定した IPSec VPN サービスでネットワークとモバイル ユーザを低コストで接続

Cisco PIX セキュリティ アプライアンスの新しいフル装備の VPN 機能を使用すれば、企業は世界中のネットワークとモバイル ユーザを、低コストのインターネット接続で安全に接続できます。ソリューションのサポートは、Internet Key Exchange (IKE) と IPSec VPN 規格を使用した標準規格のサイト間 VPN から、Cisco PIX セキュリティ アプライアンスやその他のシスコシステムズのセキュリティ ソリューション（Cisco IOS[®] ルータや Cisco VPN 3000 シリーズ コンセントレータなど）に装備されている革新的な Cisco Easy VPN リモート アクセス機能まで、広範囲にカバーします。Cisco Easy VPN は、スケーラブルで低コストの、管理しやすい独特なリモート アクセス VPN アーキテクチャを提供します。Cisco Easy VPN を利用することで、リモート デバイスの設定のメンテナンスに伴う運用コストが不要になります。Cisco Easy VPN は、VPN クライアントのセキュリティ ポ

スチャ要件の実現や Cisco VPN クライアントの自動ソフトウェア アップデートの実行など、豊富な機能のリモート アクセス VPN サービスを提供し、企業ネットワークへの安全で管理しやすいリモート アクセスを実現します。Cisco PIX セキュリティ アプライアンスでは、56 ビットの Data Encryption Standard (DES)、168 ビットの Triple DES (3DES)、または最大 256 ビットの Advanced Encryption Standard (AES) 暗号化を使用してデータが暗号化されます。Cisco PIX セキュリティ アプライアンスの一部のモデルはハードウェア VPN アクセラレーションを搭載しているため、高度にスケーラブルでハイパフォーマンスな VPN サービスが実現できます。

評価の高い耐障害性アーキテクチャでビジネスの稼働時間を最大化

Cisco PIX セキュリティ アプライアンスの一部のモデルは、評価の高いステートフル フェールオーバー サービスを提供しており、企業のネットワーク環境で耐障害性のネットワーク保護を保証します。企業は Cisco PIX セキュリティ アプライアンスの展開に当たり、アクティブ/スタンバイ フェールオーバー設計、またはより高度なアクティブ/アクティブ フェールオーバー設計のいずれかを使用して、非対称ルーティングのサポートを必要とする複雑なネットワーク環境にも対応できます。フェールオーバー ペアは、接続状態とデバイスの設定データを常時同期させて、管理しやすいハイアベイラビリティ ソリューションを提供します。同期化は高速 LAN 接続を経由して実行できるので、企業はフェールオーバー ペアを地理的に分離して設置するという保護レイヤを実装することもできます。システムまたはネットワークに障害が発生すると、ネットワーク セッションがアプライアンス間で自動的に移行しますが、これはユーザに対して完全にトランスペアレントに実行されます。

インテリジェント ネットワーキング サービスで展開の簡略化とシームレスなネットワーク統合が可能

Cisco PIX セキュリティ アプライアンスは、ネットワーキングでの 20 年以上におよぶシスコのリーダーシップと技術革新を活用し、現在の多様なネットワーク環境へのシームレスな統合を可能にする幅広いインテリジェント ネットワーキング サービスを提供します。管理者は、ネイティブの 802.1Q ベース VLAN サポートを利用することで、Cisco PIX セキュリティ アプライアンスをスイッチド ネットワーク環境へ簡単に統合できます。Cisco IP Phone の設定では、Cisco PIX セキュリティ アプライアンスが提供する「ゼロタッチ プロビジョニング」サービスが利用できます。これによって、IP Phone を適切な Cisco CallManager で自動的に登録し、追加の設定情報やソフトウェア イメージをダウンロードできます。企業は、Cisco PIX セキュリティ アプライアンスが提供する Open Shortest Path First (OSPF) の安定したダイナミック ルーティング サービスを利用して、ネットワーク全体の耐障害性を向上させることができます。このサービスでは、ネットワークの機能停止を数秒以内に検出し、ルートを迂回させます。ミッションクリティカルなリアルタイムの企業アプリケーション、コラボレーティブ コンピューティング アプリケーション、およびストリーミング マルチメディア サービスは、Cisco PIX セキュリティ アプライアンスが提供する包括的な Protocol Independent Multicast (PIM) スパース モード v2 と、双方向の PIM ルーティングのサポートを利用することで安全に実現できます。企業は、Cisco PIX セキュリティ アプライアンスが提供する高度な IPv6 セキュリティ サービスを使用して、次世代の IPv6 ネットワークを安全に展開できます。また IPv6 インフラストラクチャへの移行期間中は、同じアプライアンスによって既存の IPv4 環境のセキュリティを確保できます。

柔軟な管理ソリューションで運用コストを削減

Cisco PIX セキュリティ アプライアンスには設定、監視、およびトラブルシューティングのオプションが多数用意されており、企業は自社のニーズに最も適した方法を柔軟に選択、利用できます。管理ソリューションは、ポリシーベースの集中管理ツールから、Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) や Syslog などのリモート監視プロトコルをサポートする統合された Web ベースの管理にまでおよびます。Cisco PIX セキュリティ アプライアンスには最大 16 レベルのカスタマイズ可能な管理ロールが用意されているので、企業は管理者と運用スタッフに対して、各アプライアンスへの適切なアクセス レベルを付与できます (監視専用アクセス、設定読み取り専用アクセス、ネットワーク設定専用アクセス、またはファイアウォール設定専用アクセスなど)。Cisco PIX セキュリティ アプライアンスにはセキュア リモート管理サービスの 1 つである安定した自動アップデート機能も備わっており、アプライアンスの設定とソフトウェア イメージを自動的に最新の状態に保つことができます。

攻撃緩和およびイベント監視ソリューション

ネットワーク ベースの攻撃は、Cisco Security Monitoring, Analysis, and Response System (CS-MARS) 製品ファミリーを使用して、事業または企業環境の内部で簡単かつ正確に特定、管理、および一掃できます。CS-MARS アプライアンスは、多数のデスクトップ、サーバ、およびネットワーク セキュリティ ソリューションからのセキュリティ イベント、Syslog、および NetFlow のデータを分析し、かつ関連させることで実際の攻撃パスを特定し、緩和オプションを提供するため、専門のセキュリティ アナリストがいない環境でも、セキュリティ攻撃に簡単に対処できます。

トップレベルのデバイス管理ソリューション

シスコの統合型 Adaptive Security Device Manager (ASDM) はトップレベルの Web ベース管理インターフェイスです。これにより単一の Cisco PIX セキュリティ アプライアンスの展開、運用中の設定、および監視を大幅に簡略化できます。管理者のコンピュータに、(標準的な Web ブラウザと Java プラグイン以外の) ソフトウェアをインストールする必要はありません。インテリジェント セットアップと VPN ウィザードであらゆるネットワーク環境に簡単に統合できる一方、情報提供監視機能 (ダッシュボードやリアルタイムの Syslog ビューアなど) でデバイスやネットワークにとっての重要な健全性とイベントをひと目で確認できます。

また、管理者は Command-Line Interface (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、監視、およびトラブルシューティングをリモートで行うこともできます。CLI へのアクセスは、Secure Shell (SSHv2) プロトコル、Telnet over IPSec、およびコンソール ポート経由のアウトバンドなど、いくつかの方法で安全に行うことができます。

Cisco PIX セキュリティ アプライアンス ソフトウェア バージョン 7.0 の新機能

Cisco PIX セキュリティ アプライアンス ソフトウェア バージョン 7.0 は、表 1 に詳しく説明されている機能をはじめ、多くの新しい機能を備えています。機能の完全なリストは、Cisco PIX セキュリティ アプライアンス ソフトウェア バージョン 7.0 のリリース ノートを参照してください。

表 1 新しい機能と利点

機能	利点
高度なファイアウォール サービス	
シスコ モジュラ型ポリシー フレームワーク	<ul style="list-style-type: none">• フローベースまたはクラスベースのポリシーを定義するために、柔軟性の高い強力なフレームワークを提供。管理者はネットワーク フローまたはクラスをさまざまな条件に基づいて識別し、カスタマイズ可能な一連のサービスを各フローまたはクラスに適用することが可能• フローまたはクラス固有のファイアウォールおよびインスペクション ポリシー、QoS ポリシー、接続制限および接続タイマーなどを備える機能を導入することで、アプリケーションの制御を拡張
拡張 Web セキュリティ サービス	<ul style="list-style-type: none">• Web トラフィックの詳細なインスペクション サービスを新たに導入。このサービスは HTTP セッションの精密な制御が可能で、Web ベースのさまざまな攻撃に対する保護を強化• 企業は、使用できる HTTP コマンドまたはメソッドをフロー単位で精密に制御できるので (たとえばインターネットからのトラフィックと、ステージング Web サーバから稼働 Web サーバへのトラフィックに異なるポリシーを適用するなど)、Web コンテンツに対する未認証の削除や変更など、Web ベースのさまざまな攻撃から自社を保護することが可能• RFC 適合性の実現、プロトコル異常検出、プロトコル状態追跡、応答の検証、MIME タイプの検証とコンテンツ制御、および Uniform Resource Identifier (URI) レングスの実現など、幅広く強力な HTTP セキュリティ サービスを追加提供

機能	利点
トンネリング アプリケーション 制御	<ul style="list-style-type: none"> • インスタント メッセージング、ピアツーピアのファイル共有、および Web アプリケーション ポート経由でトンネリングを行うその他のアプリケーションを検出し、オプションでブロックする新しいインスペクション サービスを導入 • AOL Instant Messenger、Microsoft Messenger、および Yahoo Messenger など、一般的なインスタント メッセージング アプリケーションをブロック • KaZaA や Gnutella など、ピアツーピアのファイル共有アプリケーションをブロック • GoToMyPC などのトンネリング アプリケーションをブロック
セキュリティ コンテキスト	<ul style="list-style-type: none"> • 単一の Cisco PIX セキュリティ アプライアンスに複数のセキュリティ コンテキスト（仮想ファイアウォール）を作成可能。各コンテキストには専用のセキュリティ ポリシー セット、論理インターフェイス、および管理ドメインを備えることが可能 • セキュリティ コンテキストのライセンス レベルは、5、10、20、50、および 100 の 5 つをサポート（サポートされるコンテキストの最大数は、Cisco PIX セキュリティ アプライアンスのモデルに基づいて決定） • 複数のファイアウォールを単一の物理アプライアンスまたはフェールオーバー ペアに統合。これらの仮想インスタンスはそれぞれ別々に管理可能 • サービス プロバイダーは、冗長アプライアンスのペアによって、復元力のあるマルチテナントのファイアウォール サービスを提供可能
レイヤ 2 のトランスペアレントなファイアウォール	<ul style="list-style-type: none"> • Cisco PIX セキュリティ アプライアンスを、両側の各デバイスに対しては「不可視」なまま、安全なレイヤ 2 ブリッジング モードで展開。豊富なレイヤ 2～7 ファイアウォール セキュリティ サービスを保護対象のネットワークに提供 • 企業は保護対象のネットワークにアドレスを再指定する必要がないので、Cisco PIX セキュリティ アプライアンスを既存のネットワーク環境で簡単に展開可能 • 管理者が定義する Ethertype ベースのレイヤ 2 ネットワーク トラフィック用アクセス制御ポリシーを実施することで、レイヤ 2 のセキュリティ境界を作成
FTP セッション コマンドのフィルタリング	<ul style="list-style-type: none"> • Cisco PIX セキュリティ アプライアンスが提供する従来の FTP インスペクション サービス（プロトコル異常検出、プロトコル状態追跡、NAT および Port Address Translation [PAT; ポート アドレス変換] のサポート、ポートのダイナミックなオープンとクローズなど）に加えて、多数の FTP コマンドの使用に対する管理者の制御を強化し、ユーザとグループが FTP セッション内で実行できる操作（FTP の get や put など）を規制 • サーバの難読化技術と追加的な攻撃シグニチャを導入し、攻撃に対する FTP サーバの保護を強化
Extended Simple Mail Transport Protocol (ESMTP) E メール インスペクション サービス	<ul style="list-style-type: none"> • SMTP インスペクション エンジンの機能を拡張して ESMTP をサポートし、プロトコル異常検出、プロトコル状態追跡、および ESTMP プロトコルで導入される新しいコマンド（AUTH、DATA、EHLO、ETRN、HELO、HELP、MAIL、NOOP、QUIT、RCPT、RSET、SAML、SEND、SOML、および VRFY）のサポートなどのセキュリティ サービスを提供 • 自動コマンド フィルタリングによって、悪意のある SMTP および ESTMP コマンドから企業を保護
3G モバイル ワイヤレス セキュリティ サービス	<ul style="list-style-type: none"> • 3G モバイル ワイヤレス環境向けに、General Packet Radio Service (GPRS) Tunneling Protocol (GTP) 規格を使用してパケット交換データ サービスを行う豊富なセキュリティ サービスを提供 • GTP 固有のパラメータ（International Mobile Subscriber Identity [IMSI] プレフィクスや Access Point Name [APN] 値など）に基づく強固なフィルタリング機能によって、モバイル ワイヤレス プロバイダーとローミング パートナーとの安全な通信を可能にする高度な GTP インスペクション サービスを提供 <p>注： この機能を使用するには、個別のライセンスが必要</p>

機能	利点
Sun RPC/NIS+ インспекション サービス	<ul style="list-style-type: none"> Portmapper v2 または RPCBind v3/v4 を使用する Sun RPC および NIS+ セッション トランザクション用の新しいステートフル インспекションおよび NAT サービスによって、ポートホッピングを行う UNIX アプリケーションのサポートを強化
Internet Control Message Protocol (ICMP) インспекション サービス	<ul style="list-style-type: none"> ICMP 接続の状態追跡サービスを提供し、ICMP エラー メッセージの制御を拡張することで、トラブルシューティングに ICMP を安全に使用できるようになり、ネットワークのパフォーマンスが向上
拡張 TCP セキュリティ エンジン	<ul style="list-style-type: none"> プロトコルとアプリケーション層攻撃の検出に役立つ、新しい基本機能をいくつか導入 一連のパケット全体にわたる攻撃の検出に役立つ、TCP ストリームの再構築と分析サービスを提供 TCP トラフィック正規化サービスを提供し、攻撃検出技術を追加。内容は、フラグとオプションの拡張チェック、TCP パケットのチェックサム検証、再送信パケットのデータ改ざん検出など
アウトバンド Access Control List (ACL; アクセス制御リスト)	<ul style="list-style-type: none"> (従来のインバンド ACL のほかに) アウトバンド ACL のサポートを追加することで、アクセス制御ポリシーの定義の柔軟性を拡大。ネットワーク トラフィックがインターフェイスを出入りする際のアクセス制御を実現
時間ベースの ACL	<ul style="list-style-type: none"> 選択した ACL にカスタム時間範囲を適用し、特定の ACL エントリがアクティブになるタイミングを定義することで、リソースの使用に対する管理者の制御を拡張
個々の ACL エントリの有効化と無効化	<ul style="list-style-type: none"> 管理者が ACL エントリの削除や書き換えを行うことなく、ACL のテストや微調整ができる便利なトラブルシューティング ツールを提供
Websense URL フィルタリングのパフォーマンスの向上	<ul style="list-style-type: none"> Websense Enterprise Employee Internet Management (EIM) ソリューションで、同時 URL フィルタリング ルックアップのスケラビリティを大幅に拡張
Voice over IP とマルチメディア セキュリティ サービス	
T.38 Fax Over IP (FoIP)	<ul style="list-style-type: none"> H.323 インспекション サービスを拡張し、T.38 プロトコル (FoIP のリアルタイム伝送方式を定義する ITU 規格) をサポート
Gatekeeper Routed Control Signaling (GKRCS)	<ul style="list-style-type: none"> H.323 インспекション サービスを拡張し、現在サポートされている Direct Call Signaling (DCS) 方式に加えて GKRCS をサポート H.323 ゲートキーパ間で直接交換されるコール シグナリング メッセージを、Cisco PIX セキュリティ アプライアンスでサポートすることが可能
フラグメント化/セグメント化マルチメディア ストリーム インспекション	<ul style="list-style-type: none"> フラグメント化またはセグメント化された H.323、SIP、SCCP ベースの音声およびマルチメディア ストリームのインспекションを導入
MGCP アドレス変換サービス	<ul style="list-style-type: none"> Cisco PIX セキュリティ アプライアンスが提供する豊富な MGCP セキュリティ サービスに加えて、NAT および PAT ベースのアドレス変換サービスを、メディア ゲートウェイとコール エージェントまたはメディア ゲートウェイ コントローラ間の MGCP ベース接続に追加
RTSP アドレス変換サービス	<ul style="list-style-type: none"> NAT ベースのアドレス変換サービスを RTSP メディア ストリームに提供し、さまざまなネットワーク環境でのサポートを強化
安定した IPSec VPN サービス	
VPN クライアントのセキュリティ ポスチャを実現	<ul style="list-style-type: none"> VPN 接続要求が受信された際に、VPN クライアントのセキュリティ ポスチャ チェックを実行する機能を導入。認証済みのホスト ベース セキュリティ製品 (Cisco Security Agent など) の使用を実現し、リモート ユーザに企業のネットワークへのアクセスを許可する前に、そのバージョン番号とステータスを確認
OS (オペレーティング システム) とタイプによる VPN クライアントのブロック	<ul style="list-style-type: none"> 接続を許可するさまざまなタイプの VPN クライアント (ソフトウェア クライアント、ルータ、または Cisco PIX など) を、クライアントのタイプ、インストールされている OS、および VPN クライアント ソフトウェアのバージョンに基づいて制限する機能を追加 非適合の VPN クライアントへのアクセスを制限または防止

機能	利点
VPN クライアント ソフトウェアの自動アップデート	<ul style="list-style-type: none"> • Cisco VPN クライアントの自動ソフトウェア アップデートのサポートを導入。アップデートの起動は、VPN 接続の確立時、または現在接続している VPN クライアントがオンデマンドで実行可能
非スプリット トンネリング リモート アクセス VPN 環境のサポートの強化	<ul style="list-style-type: none"> • リモート アクセス VPN 接続を、Cisco PIX セキュリティ アプライアンスの外側のインターフェイスで終端させることが可能。これにより、リモート アクセス ユーザ VPN トンネルからインターネットへ向かうトラフィックを、(ファイアウォール ルール、URL フィルタリング ポリシー、およびその他のセキュリティ チェックをオプションで適用後、) 着信時と同じインターフェイスから送出
VPN NAT のトランスペアレンシの強化	<ul style="list-style-type: none"> • NAT または PAT を実装するネットワーク環境 (空港、ホテル、ワイヤレス ホットスポット、ブロードバンド環境など) への IPSec ベースのサイト間およびリモート アクセス VPN のサポートを拡張 • NAT/PAT バウンダリを安全に通過できるように、シスコの TCP/UDP NAT トラバーサル方式のサポートを、既存の IETF UDP ラッパー メカニズムのサポート補完方式として追加
一般的なユーザ認証サービスとのネイティブ統合	<ul style="list-style-type: none"> • 一般的な認証サービスとのネイティブ統合によって、VPN ユーザを認証する便利な方法を提供。対象となる認証サービスは、Microsoft アクティブ ディレクトリ、Microsoft Windows ドメイン、Kerberos、Lightweight Directory Access Protocol (LDAP)、および RSA SecurID など (仲介役として機能する個別の RADIUS/TACACS+ サーバは不要)
VPN トンネルでの OSPF ダイナミック ルーティング	<ul style="list-style-type: none"> • 包括的な OSPF ダイナミック ルーティング サービスを拡張して IPSec VPN トンネルでのネイバをサポートし、VPN 接続されたネットワークの信頼性を向上 • OSPF リバース ルート インジェクションをサポートすることで、ネットワークのパフォーマンスと信頼性を向上
スポーク間 VPN のサポート強化	<ul style="list-style-type: none"> • Cisco PIX セキュリティ アプライアンスがハブとして機能する場合、VPN トラフィックを同じインターフェイスで送受信することで、スポーク間 VPN 通信のサポートを強化
X.509 証明書のサポート強化	<ul style="list-style-type: none"> • Public Key Cryptography Standard (PKCS) #10 形式の証明書要求をサポートすることで、X.509 認証局に手動登録する機能を導入 • PKCS #7 を使用した証明書の手動インポート、および PKCS #12 を使用したプライベート キーによる証明書のインポートをサポート • n 階層の証明書チェイニングのサポートで、マルチレベルの認証局階層を持つ環境での展開が可能 • RSA キーのサポートを最大 4096 ビットのサイズまで拡張 • キー サイズが最大 1024 ビットまでの Digital Signature Algorithm (DSA) ベースの X.509 証明書のサポートを追加
Cisco IOS ソフトウェア認証局のサポート	<ul style="list-style-type: none"> • Cisco IOS ソフトウェアでの新しい認証局へのオンライン登録のサポートを導入。この軽量の X.509 認証局によって、Public Key Infrastructure (PKI; 公開鍵インフラストラクチャ) 対応のサイト間 VPN のロールアウトが簡略化
ハイアベイラビリティ サービス	
アクティブ/アクティブ ステートフル フェールオーバー	<ul style="list-style-type: none"> • 評価の高い Cisco PIX セキュリティ アプライアンスのアクティブ/スタンバイ フェールオーバーを補完するソリューションを提供。アクティブ/アクティブ フェールオーバー ペア内の両システムがネットワーク トラフィックをアクティブに同時転送するため、フェールオーバー ペアのスループットは実質的に 2 倍になり、ネットワーク トラフィックの集中状態にも対応可能 • アクティブ/アクティブ フェールオーバー ペアのメンバー間で双方向の状態共有がサポートされているため、非対称なルーティング トポロジーを持つ高度なネットワーク環境にも対応可能。これにより、一方の Cisco PIX セキュリティ アプライアンスに着信したフローを、必要に応じて他方のアプライアンスから送出 <p>注: この機能は、無制限 (Unrestricted) およびフェールオーバー アクティブ/アクティブ モデルでのみ利用可能。アップグレード ライセンスを購入すれば、フェールオーバー モデルをフェールオーバー アクティブ/アクティブ モデルに変換可能</p>

機能	利点
VPN ステートフル フェールオーバー	<ul style="list-style-type: none"> VPN 接続用の新しいアクティブ/スタンバイ ステートフル フェールオーバーで、VPN の接続可能時間を最大限に延長 フェールオーバー ペアのメンバー間で、セキュリティ アソシエーションの状態に関する情報とセッション キー マテリアルをすべて同期させ、復元力の高い VPN ソリューションを実現 <p>注: この機能は、無制限 (Unrestricted)、フェールオーバー、およびフェールオーバーアクティブ/アクティブ モデルでのみ利用可能</p>
フェールオーバー移行時間の短縮	<ul style="list-style-type: none"> フェールオーバー パートナー間で、ハートビート/状態共有インターバルに対するより精密な制御をサポートすることで、フェールオーバーにかかる時間を大幅に短縮
ゼロダウンタイム ソフトウェア アップグレード	<ul style="list-style-type: none"> 異なる Cisco PIX セキュリティ アプライアンス ソフトウェア バージョン (バージョン 7.0(1)以上) 間での状態共有をサポートすることで、企業はネットワークの使用可能時間や接続に影響を与えることなく、Cisco PIX セキュリティ アプライアンスのフェールオーバー ペアでソフトウェアのメンテナンス リリース アップグレードを実行
インテリジェント ネットワーキング サービス	
PIM マルチキャスト ルーティング	<ul style="list-style-type: none"> PIM スパース モード v2 と双方向 PIM ルーティングを (Cisco IOS マルチキャスト テクノロジーに基づいて) 完全サポートすることで、ビデオ会議アプリケーション、コラボレーティブ コンピューティング アプリケーション、およびミッションクリティカルなリアルタイム企業アプリケーションでのマルチメディアトラフィックの配信を効率化
QoS サービス	<ul style="list-style-type: none"> Low-Latency Queuing (LLQ; 低遅延キューイング) とトラフィック ポリシングのサポートによってフロー単位、ポリシーベースの QoS サービスを提供することで、遅延の影響を受けやすいネットワークトラフィックに優先順位を付け、管理者固有のアプリケーションの使用帯域幅を制限 企業は、拡張ネットワークにエンドツーエンドの QoS ポリシーを備えることが可能
IPv6 ネットワーキング	<ul style="list-style-type: none"> デュアル スタックのサポートで、ネイティブの IPv6 ネットワーク環境と、IPv4/IPv6 混在ネットワーク環境におけるアクセス制御と詳細なインスペクション ファイアウォール サービスを提供 IPv6 対応のインスペクション サービスを HTTP、FTP、SMTP、ICMP、TCP、および UDP に基づくアプリケーション向けに提供 SSHv2、Telnet、HTTP/Secure HTTP (HTTPS)、および ICMP ベースの管理を IPv6 でサポート
複数のインターフェイスに共通のセキュリティ レベル	<ul style="list-style-type: none"> Cisco PIX セキュリティ アプライアンスのインターフェイス セキュリティ レベルの概念を拡張し、複数のインターフェイスで 1 つの共通セキュリティ レベルを共有することが可能 管理者はカスタム セキュリティ ポリシーを定義することで、自動トラフィック フローをあらかじめ許可することなく、インターフェイス間のトラフィック伝送を同じセキュリティ レベルで実行。これにより、Cisco PIX セキュリティ アプライアンスをイントラネット環境で簡単に展開
VLAN 容量の拡張	<ul style="list-style-type: none"> Cisco PIX セキュリティ アプライアンスがサポートする 802.1Q VLAN ベースの仮想インターフェイスの数が増加し、各プラットフォームのポート密度が増大 企業はネットワークをさまざまなセキュリティ ゾーンに分割することで、セキュリティを強化 Cisco PIX 515 および 515E セキュリティ アプライアンスでは最大 25 の VLAN、Cisco PIX 525 セキュリティ アプライアンスでは最大 100 の VLAN、および Cisco PIX 535 セキュリティ アプライアンスでは最大 200 の VLAN をサポート
アドレス変換サービス オプション	<ul style="list-style-type: none"> アドレス変換を必要とするホストとネットワークがアドレス変換ポリシーを設定するだけで変換できるように、Cisco PIX セキュリティ アプライアンスの展開を簡略化。ネットワークトラフィック伝送前にアドレス変換ポリシーを展開していた以前の方法は廃止

機能	利点
柔軟な管理ソリューション	
SNMP 監視の強化	<ul style="list-style-type: none"> • SNMPv2c のサポート導入で、Cisco PIX セキュリティ アプライアンスの状態をより詳細に確認 • 64 ビット カウンタなどの新しいサービス（ギガビット イーサネット インターフェイスの監視強化用）、および MIB データのバルク転送のサポートを提供 • SNMPv2 MIB (RFC 1907)、Interfaces Group MIB (RFC 1573 および 2233)、IP MIB (RFC 2011)、および Entity MIB (RFC 2737) など、多数の SNMP MIB のサポートを追加 • Cisco IPSec Flow Monitoring MIB がサポートされ、トンネル単位の詳細な統計情報（トンネルの使用可能時間、転送バイト数およびパケット数など）によって VPN 接続の状態を完全把握
SSHv2 と Secure Copy Protocol (SCP)	<ul style="list-style-type: none"> • Cisco PIX セキュリティ アプライアンスのリモート管理用に SSHv2 のサポートを追加し、サードパーティ製 SSH ツールとの互換性を向上 • コンフィギュレーション ファイルやソフトウェア イメージ ファイルなどを、Cisco PIX セキュリティ アプライアンスとの間で安全に転送するもう 1 つの方式として、SCP のサポートを導入
フラッシュ メモリに複数のコンフィギュレーションを保存	<ul style="list-style-type: none"> • 新しいフラッシュ ファイル システム、および複数のコンフィギュレーションをフラッシュに保存して使用する機能が導入されたため、管理者によるコンフィギュレーションのロールバックが実行可能
安全なアセット リカバリ	<ul style="list-style-type: none"> • アセット リカバリ/パスワード リセット手順が実行された場合、フラッシュの内容を自動的に消去することで、Cisco PIX セキュリティ アプライアンスに保存されている機密の設定データ、証明書、およびキー マテリアルに対する未認証のアクセスを防止（事前に設定されている場合）
システム リロードのスケジューリング	<ul style="list-style-type: none"> • 管理者は Cisco PIX セキュリティ アプライアンスのリロードを、ある特定の時刻、または現在時刻との差でスケジューリング可能。これにより、ネットワークのダウンタイムのスケジューリング、およびリモート アクセス VPN ユーザに対するリロード前の通知が簡略化
アウトバンド管理専用インターフェイス	<ul style="list-style-type: none"> • 企業は、特定のインターフェイスをアウトバンド管理専用指定する新しい機能によって、シスコの SAFE ブループリントに従い、Cisco PIX セキュリティ アプライアンスのアウトバンドを管理するベスト プラクティスを実装することが可能
拡張 ICMP ping サービス	<ul style="list-style-type: none"> • IPv6 アドレスの追加サポートと ICMP オプションの拡張により、新しい有効なトラブルシューティングを提供（データ パターン、df ビット、リポート カウント、データグラム サイズ、タイムアウト インターバル、詳細出力、およびサイズのスイープ範囲など）
CLI のユーザビリティの強化	<ul style="list-style-type: none"> • 多くの一般的な Cisco IOS コマンドライン サービス（コマンドの補完、コンテキスト ヘルプ、エイリアスの使用など）を組み込むことで、Cisco PIX セキュリティ アプライアンスの CLI のユーザ環境を強化
SMTP E メール アラート	<ul style="list-style-type: none"> • クリティカルなイベントが発生した場合に、管理者が定義した E メール アドレスに警告メッセージを送信することで、管理者に通知
TACACS+ 管理アカウンティング	<ul style="list-style-type: none"> • TACACS+ の Authentication, Authorization, Accounting (AAA; 認証、許可、アカウンティング) レコードを生成する機能を導入。Cisco PIX セキュリティ アプライアンスに対する管理アクセスの追跡、および管理セッション中に加えられたすべての設定変更の追跡に利用でき、Cisco PIX セキュリティ アプライアンスで従来からサポートされている管理ログ用の Syslog サポートを補完
複数のサーバに対する RADIUS アカウンティング	<ul style="list-style-type: none"> • 複数の RADIUS サーバに対するアカウンティング情報同時送信のサポートを追加

技術仕様

表 2～4 に、Cisco PIX セキュリティ アプライアンスと VPN クライアント、VPN 製品、および一部の暗号化規格間の互換性に関する情報を示します。

Cisco VPN クライアントの互換性

Cisco PIX セキュリティ アプライアンスは、表 2 に挙げるものを含めて、多数のソフトウェアおよびハードウェア ベースの Cisco VPN クライアントをサポートしています。

表 2 Cisco PIX セキュリティ アプライアンスと VPN クライアント間の互換性

Cisco VPN クライアント	サポートされるソフトウェア バージョン
ソフトウェア IPsec VPN クライアント	<ul style="list-style-type: none">• Cisco VPN Client for Windows、バージョン 3.6 以降• Cisco VPN Client for Linux、バージョン 3.6 以降• Cisco VPN Client for Solaris、バージョン 3.6 以降• Cisco VPN Client for Mac OS X、バージョン 3.6 以降
ハードウェア IPsec VPN クライアント (Cisco Easy VPN Remote)	<ul style="list-style-type: none">• Cisco VPN 3002 ハードウェア クライアント、バージョン 3.0 以上• Cisco IOS Software Easy VPN Remote、リリース 12.2(8)YJ• Cisco PIX セキュリティ アプライアンス ソフトウェア バージョン 6.2 および 6.3

シスコのサイト間 VPN との互換性

多くのサードパーティ製 VPN 製品との相互運用性の提供に加えて、Cisco PIX セキュリティ アプライアンスは次の Cisco VPN 製品との相互運用により、サイト間 VPN 接続が可能です。

表 3 Cisco PIX セキュリティ アプライアンスと VPN 製品間のサイト間 VPN の互換性

Cisco VPN 製品	サポートされるソフトウェア バージョン
Cisco IOS ルータ	Cisco IOS ソフトウェア リリース 12.1(6)T 以降
Cisco PIX 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 ソフトウェア バージョン 6.0(1)以降
Cisco VPN 3000 コンセントレータ	Cisco VPN 3000 コンセントレータ ソフトウェア バージョン 3.0 以降

サポートされる暗号化規格

Cisco PIX セキュリティ アプライアンスは、以下のような多数の暗号化規格、および関連するサードパーティ製の製品とサービスをサポートします。

表 4 Cisco PIX セキュリティ アプライアンスでサポートされる暗号化規格および製品

暗号化規格および製品	説明
非対称(パブリック キー)暗号化アルゴリズム	<ul style="list-style-type: none">• RSA パブリック/プライベート キー ペア、512 ~ 4096 ビット• DSA パブリック/プライベート キー ペア、512 ~ 1024 ビット
対称暗号化アルゴリズム	<ul style="list-style-type: none">• AES : 128、192、および 256 ビット• DES : 56 ビット• 3DES : 168 ビット• RC4 : 40、56、64、および 128 ビット
Perfect Forward Secrecy (Diffie-Hellman キー ネゴシエーション)	<ul style="list-style-type: none">• グループ 1 : 768 ビット• グループ 2 : 1024 ビット• グループ 5 : 1536 ビット• グループ 7 : 163 ビット (Elliptic Curve Diffie-Hellman)

暗号化規格および製品	説明
ハッシュ アルゴリズム	<ul style="list-style-type: none"> • MD5 : 128 ビット • SHA-1 : 160 ビット
X.509 認証局	<ul style="list-style-type: none"> • Baltimore UniCERT • Cisco IOS ソフトウェア • Entrust Authority • iPlanet/Netscape CMS • Microsoft Certificate Services • RSA KEON • VeriSign OnSite
X.509 証明書登録方式	<ul style="list-style-type: none"> • Simple Certificate Enrollment Protocol (SCEP) • 手動 (PKCS #7 および #10)

システム要件

表 5 は、Cisco PIX セキュリティ アプライアンス ソフトウェア バージョン 7.0 を実行する Cisco PIX セキュリティ アプライアンスのシステム要件一覧です。

表 5 システム要件

システム要件	説明
サポートされるプラットフォーム	<ul style="list-style-type: none"> • Cisco PIX 515 セキュリティ アプライアンス • Cisco PIX 515E セキュリティ アプライアンス • Cisco PIX 525 セキュリティ アプライアンス • Cisco PIX 535 セキュリティ アプライアンス
最小 RAM 容量	<p>Cisco PIX 515/515E セキュリティ アプライアンス</p> <ul style="list-style-type: none"> • 64 MB (制限モデルの場合) • 128 MB (無制限、フェールオーバー、およびフェールオーバー アクティブ/アクティブ モデルの場合) <p>注 : このリリースでは、Cisco PIX 515/515E セキュリティ アプライアンスで、以前のソフトウェア リリースを超えるメモリを要するため、メモリのアップグレードが必要になる場合あり</p> <p>Cisco PIX 525 セキュリティ アプライアンス</p> <ul style="list-style-type: none"> • 128 MB (制限モデルの場合) • 256 MB (無制限、フェールオーバー、およびフェールオーバー アクティブ/アクティブ モデルの場合) <p>Cisco PIX 535 セキュリティ アプライアンス</p> <ul style="list-style-type: none"> • 512 MB (制限モデルの場合) • 1024 MB (無制限、フェールオーバー、およびフェールオーバー アクティブ/アクティブ モデルの場合)
最小フラッシュ メモリ容量	<ul style="list-style-type: none"> • 16 MB
サポートされる拡張カード	<ul style="list-style-type: none"> • 1 ポート 10/100 ファスト イーサネット カード • 4 ポート 10/100 ファスト イーサネット カード • 1 ポート ギガビット イーサネット マルチモード (SX) SC カード • VPN Acceleration Card (VAC) • VPN Acceleration Card+ (VAC+)

製品の発注情報

表 6 は、Cisco PIX セキュリティ アプライアンス ソフトウェアの発注情報です。

表 6 発注情報

製品番号	説明
PIX-SW-UPGRADE=	Cisco PIX セキュリティ アプライアンス ソフトウェアのワンタイム アップグレード（現在 Cisco SMARTnet [®] サポートの契約をされていないお客様向け）

サポート サービス

サポート サービスは、シスコおよびシスコのパートナーからご利用いただけます。Cisco SMARTnet サービスではカスタマーサポートのリソースが增強され、（オンラインおよび電話による）時と場所を選ばない技術リソースへのアクセス、アップデートされたシステム ソフトウェアのダウンロード機能、およびハードウェアのアドバンス交換が提供されます。

その他の情報

詳細は、以下の URL をご覧ください。

Cisco PIX セキュリティ アプライアンス シリーズ :

<http://www.cisco.com/jp/product/hs/security/pix/>

Cisco Adaptive Security Device Manager :

<http://www.cisco.com/jp/product/hs/security/pdm/>

Cisco Secure ACS :

<http://www.cisco.com/jp/product/hs/security/acs/>

CiscoWorks VMS、Management Center for Firewalls、Auto Update Server Software、および Security Monitor :

<http://www.cisco.com/jp/product/hs/netmgt/cw2000/vpnsm/>

最新の Cisco PIX セキュリティ アプライアンス ソフトウェアと Cisco Adaptive Security Device Manager を（有効な Cisco.com ログインで）ダウンロードするには、次の URL にアクセスしてください。ただし、有効な Cisco.com User ID が必要です。

<http://www.cisco.com/pcgi-bin/tablebuild.pl/pix>

©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