

統合型セキュリティ アプライアンスと専用セキュリティ アプライアンスの比較

Cisco ASA 5500 シリーズ、Cisco PIX セキュリティ アプライアンス、Cisco IPS 4200 シリーズ、および Cisco VPN 3000 シリーズ コンセントレータの使い分け

シスコでは、利用環境の要件に合わせてカスタマイズ可能なセキュリティ ソリューションを提供します。Cisco ASA 5500 シリーズは、単一のプラットフォームにさまざまな機能を持つ統合されたセキュリティ/VPN サービスを実現するためのアプライアンスです。ファイアウォール、Intrusion Prevention System (IPS; 侵入防御システム)、およびネットワーク ウイルス対策サービス プロファイルが統合された Cisco ASA 5500 シリーズを使うと、お客様は幅広い適応型の攻撃防御サービスを利用できます。VPN サービスの場合、Cisco ASA 5500 シリーズが持つ柔軟性の高いテクノロジーを利用すると、リモートアクセスおよびサイト間接続の要件に適したソリューションを実現できます。

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 プロファイルを利用すると、単体でさまざまな用途に使用できます。Cisco ASA 5500 シリーズを統合型の攻撃防御デバイスとして中央サイトに導入する場合は、アクセス制御、アプリケーション検査、およびワーム/ウイルス/マルウェア対策などのテクノロジーを使用します。また、専用のリモートアクセス デバイスとして使用する場合は、IP Security (IPSec)/Secure Socket Layer (SSL) VPN の機能を利用します。部門間のアクセス制御を行う場合や、ユーザが知らないうちにネットワーク内に持ち込んでしまうワーム、ウイルス、およびその他の不正コードを防御する場合は、Cisco ASA 5500 シリーズをネットワークの内部に移動します。小規模企業やブランチ オフィス環境の場合、Cisco ASA 5500 は「オールインワン」デバイスとして使用できます。Cisco ASA 5500 シリーズは、幅広い攻撃防御や VPN サービスを備えているだけでなく、予算および運用面でも小規模企業やブランチ オフィス環境での利用に適しています。

Cisco ASA 5500 などの多機能型デバイス、または従来の「専用」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 IPS 4200 シリーズ センサ 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) のいずれを使用するか判断するには、いくつかの考慮事項を検討する必要があります。この資料では、専用アプライアンスの代わりに多機能型セキュリティ アプライアンスを導入する場合の考慮事項を、機能、運用、およびコスト面から説明します。セキュリティ/VPN アプライアンスと Cisco ルータの導入に関する考慮事項の比較はこの資料の対象外です。

シスコのセキュリティ アプライアンス製品ファミリ

シスコは、アプライアンスベースのセキュリティ製品を利用してセキュリティ システムを構成するお客様向けに、Cisco PIX セキュリティ アプライアンス、Cisco IPS 4200 シリーズ アプライアンス、Cisco VPN 3000 シリーズ コンセントレータ、および Cisco ASA 5500 シリーズ セキュリティ アプライアンスを提供しています。これらの製品はいずれも、小規模オフィスから本社拠点および小規模企業から大企業に至る幅広い構成や規模に適したソリューションを提供します。Cisco PIX セキュリティ アプライアンスには、SOHO 環境向けのソリューションも用意されています。以下に、各製品の機能と構成例の概要を示します。

Cisco PIX セキュリティ アプライアンス

優れた評価を得ている Cisco PIX セキュリティ アプライアンスは、アプリケーション アウェアな安定性の高いファイアウォール サービスと VPN 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、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、およびサイト間のセキュア コネクティビティ サービスを、費用対効果の高い導入の容易なソリューションとして提供します。

Cisco IPS 4200 シリーズ センサ アプライアンス

Cisco IPS 4200 シリーズ センサは、悪意のある攻撃、ワーム、およびウイルスからネットワークを保護して、企業のデータやリソースが被害を受けるのを未然に防ぎます。Cisco IPS センサは、ワーム、スパイウェア/アドウェア、ネットワーク ウイルス、およびアプリケーションの不正使用といった脅威を検出、分類、および防止することによって、ネットワークを強力に保護します。

Cisco VPN 3000 シリーズ コンセントレータ

Cisco VPN 3000 シリーズ コンセントレータは、SSL VPN 接続と IPSec VPN 接続の両方を提供するクラス最高レベルのリモートアクセス VPN ソリューションです。Cisco VPN 3000 シリーズ コンセントレータでは、リモート アクセス VPN のインストール、設定、監視を簡単に行うことができる管理システムに加えて、標準ベースの使いやすい VPN クライアントとスケーラブルな VPN トンネル 終端デバイスも利用できます。

Cisco ASA 5500 シリーズ セキュリティ アプライアンス

Cisco ASA 5500 シリーズは、最先端のセキュリティ テクノロジーを統合することによって、シスコの導入実績豊富なファイアウォール、侵入防御、ネットワーク ウイルス対策、および VPN サービスを 1 台のアプライアンスで提供します。Cisco ASA 5500 シリーズは、統合型の管理パッケージを備えており、優れたパフォーマンスにも対応しています。そのため、大企業および中堅・中小企業のアプリケーション管理を簡素化すると同時に、複数のサービスを並行して処理できる強力なパフォーマンスを提供できます。

機能の比較

Cisco ASA 5500 シリーズは、Cisco PIX、Cisco IPS 4200、および Cisco VPN 3000 プラットフォームの導入実績豊富なフィーチャ セットとトレンドマイクロ社のネットワーク ウイルス対策機能を、単一のデバイスと管理フレームワークで提供します。これらの機能を統合することにより、リモートアクセス VPN 接続のワーム/ウイルス/マルウェアからの保護、ネットワーク境界における幅広いワーム/ウイルス/マルウェア対策、および内部ネットワークでのアプリケーションの高度な検査や制御といった、新たな機能が可能になります。Cisco ASA 5500 シリーズは、高度に統合された相互に連携するサービス プロファイルにより、専用のシスコ製セキュリティ アプライアンスや VPN アプライアンスが提供する機能の多くを単体で提供します。

また、Cisco ASA 5500 シリーズは単体で幅広い攻撃を防御できるため、リモート オフィス、本社の DMZ、およびネットワーク内部といったさまざまな場所の防御機能を強化できます。これにより、これまで予算や運用上の問題で高度なセキュリティ機能を導入できなかったリモート サイトやネットワーク内部といったネットワークの無視された場所でも、ワーム/ウイルス/マルウェア対策やアプリケーション セキュリティの実施が可能になります。このように、Cisco ASA 5500 シリーズはネットワークの全体的なセキュリティ状態を向上させることによって、ネットワーク全体のセキュリティ チェーンを強化します。

Cisco ASA 5500 シリーズは、既存のすべての Cisco PIX、Cisco IPS 4200、および Cisco VPN 3000 との完全な互換性を持っているため、既存構成と統合して利用できます。前述のように、これらのアプライアンスはすべて導入実績の豊富な共通のテクノロジーを搭載しています。そのため、Cisco ASA 5500 シリーズと専用製品との機能上の違いはほとんどありません。また、セキュリティスタッフは、ASA 5500 シリーズを導入する際に、Cisco PIX、Cisco IPS 4200、および Cisco VPN 3000 アプライアンスを通じて得た経験や知識を活用できます。

表 1 に、各プラットフォームのアプリケーション環境と機能の概要を示します。

表 1 機能の比較

	用途	ASA に追加されているサービス
Cisco ASA 5500 と Cisco PIX	<ul style="list-style-type: none"> Cisco ASA 5500 は一般的な Cisco PIX 515E/525 環境を対象としている 小規模企業やホーム オフィス、大企業の本社では PIX 501、506E、および 535 の方が適している 	<ul style="list-style-type: none"> すべての IPS サービス ワームおよびマルウェア対策 ネットワーク ウイルス対策 強化されたアプリケーション検査 VPN クラスタリング モジュラ サービス スロット
Cisco ASA 5500 と IPS 4200	<ul style="list-style-type: none"> Cisco ASA 5500 は統合されたファイアウォールと IPS に焦点を置いている IPS のみを使用する場合は、Cisco IPS 4200 が最適で価格的にも優れている 	<ul style="list-style-type: none"> すべてのファイアウォール サービス すべての VPN サービス モジュラ サービス スロット
Cisco ASA 5500 と Cisco VPN 3000	<ul style="list-style-type: none"> Cisco ASA 5500 はすべてのサイトでの IPsec リモート アクセスおよびサイト間 VPN サービスを対象としている Cisco ASA 5500 は既存の Cisco VPN 3000 クラスタと相互運用可能 Cisco VPN 3000 は SSL VPN 中心の構成に最適 	<ul style="list-style-type: none"> スループットが 3 倍優れている VPN のステートフル フェールオーバー サイト間 VPN の QoS、OSPF ワーム/マルウェア/ウイルス対策を備えた VPN

セキュリティアーキテクチャおよび IT 組織に関する考慮事項

セキュリティおよび VPN プラットフォームは、ネットワークの規模、運用モデル、およびセグメントを考慮して判断します。単一のデバイス上に複数のセキュリティ/VPN 機能を統合するのが適している場合と、特定機能向けの専用デバイスの方が適している場合があります。

規模の観点から見ると、通常、トラフィック量が多く複雑な大規模ネットワークでは、専用デバイスの利用が多くなります。特定の機能(または単一の機能)を実行するデバイスを使用して構築されたセキュリティおよび VPN インフラストラクチャを利用すると、最適なスケラビリティ、ソフトウェアバージョンの選択/アップグレード サイクルの簡素化、およびコンフィギュレーションの綿密なチューニングとネットワーク セグメンテーションの強化が可能になります。運用上の観点から見た場合、専用デバイスを利用することによって、異なる IT チーム間でのネットワーク セキュリティの責任分担を明確にすることもできます。

専用のセキュリティ デバイスや VPN デバイスを必要とする機能分割の一般的な例は、次のような場合です。

- 専用のリモートアクセス VPN デバイスを使用する場合
- セキュリティ ポリシー監査やコンプライアンス対策として、または IT 部門の役割分担に合わせて専用の IPS デバイスを使用する場合
- Web サーバ ファームやアプリケーション サーバの保護に特化してデータセンターで高速処理を行う場合
- ネットワークエッジで耐障害性、高速トラフィック検査、およびアクセス制御に対応したファイアウォールを使用する場合

小規模なネットワークや組織の場合は、これとは逆の傾向があります。小規模ネットワーク(小規模企業やリモート オフィスなど)や小規模な IT 組織では、できるだけ少ないデバイス上にできるだけ多くのセキュリティ機能や VPN 機能を統合しようとし、使用するデバイスが少なければ、ネットワークの複雑さが軽減されます。また、数多くの個別プラットフォームで構成されるネットワークの運用には幅広い知識が必要ですが、使用するデバイスが少なければ、その負担も軽減されます。基本的に、設置場所の IT スタッフが少なく、その多くがセキュリティの専門家ではない場合、デバイスを統合することによって設置場所の運用が簡素化されます。

Cisco ASA 5500 シリーズは柔軟性に優れているため、さまざまな専用機能構成や統合機能構成で使用できます。Cisco ASA 5500 シリーズは幅広い VPN およびセキュリティ サービス プロファイルを備えているため、単体でさまざまな用途に使用できます。Cisco ASA 5500 シリーズ アプリアンスを統合型の攻撃防御デバイスとして中央サイトに導入する場合は、アクセス制御、アプリケーション検査、およびワーム/ウイルス/マルウェア対策などのテクノロジーを利用します。従来型のファイアウォールとしてネットワーク エッジに配置する場合や、専用のリモートアクセス デバイスとして使用する場合は、VPN 機能を利用します。小規模企業やブランチ オフィス環境の場合、Cisco ASA 5500 シリーズは「オールインワン」デバイスとして使用できます。Cisco ASA 5500 シリーズは、幅広い攻撃防御や VPN サービスを備えているだけでなく、予算および運用面でも小規模企業やブランチ オフィス環境での利用に適しています。

IPS 機能のみを使用する場合(セキュリティ ポリシー監査やコンプライアンス対策として IPS を使用する場合は)、Cisco IPS 4200 シリーズの方が適しています。この監査用インフラストラクチャは、「チェックアンドバランス」の手法を利用してネットワーク状態の保護と検証を行うと同時に、ポリシーを実施するデバイスの上部で、攻撃、ワーム、ウイルス、およびスパイウェア/アドウェアの防御も行います。さらに、多くの場合、IPS と他のセキュリティ機能(ファイアウォールなど)は異なる IT 管理チームによって管理されています。そのため、IPS インフラストラクチャを管理する部門は、通常、IPS サービス専用のデバイスを使用したいと考えます。

SSL VPN では、Cisco VPN 3000 シリーズ コンセントレータが最も高度な機能(Cisco Secure Desktop によるエンドポイント セキュリティ、クライアントレス Citrix、および SSL VPN トンネリングによるフル ネットワーク/アプリケーション アクセスなど)を備えています。主に SSL VPN を使用する環境では、Cisco VPN 3000 コンセントレータの方が適しています。

プラットフォームと運用コストに関する考慮事項

プラットフォーム コスト

多くの場合、Cisco ASA 5500 シリーズに統合されている機能のコストは、専用の機能に特化した Cisco PIX や Cisco VPN 3000 製品の類似モデルのコストと同等かそれ以下です。そのため、デバイスのコストは統合型の Cisco ASA 5500 と専用の Cisco PIX/VPN 3000 デバイスのいずれが適しているかを判断する要素にはなりません。この判断を行う際には、製品の機能、セキュリティアーキテクチャ、および組織の運用モデルを比較する必要があります(前記を参照)。

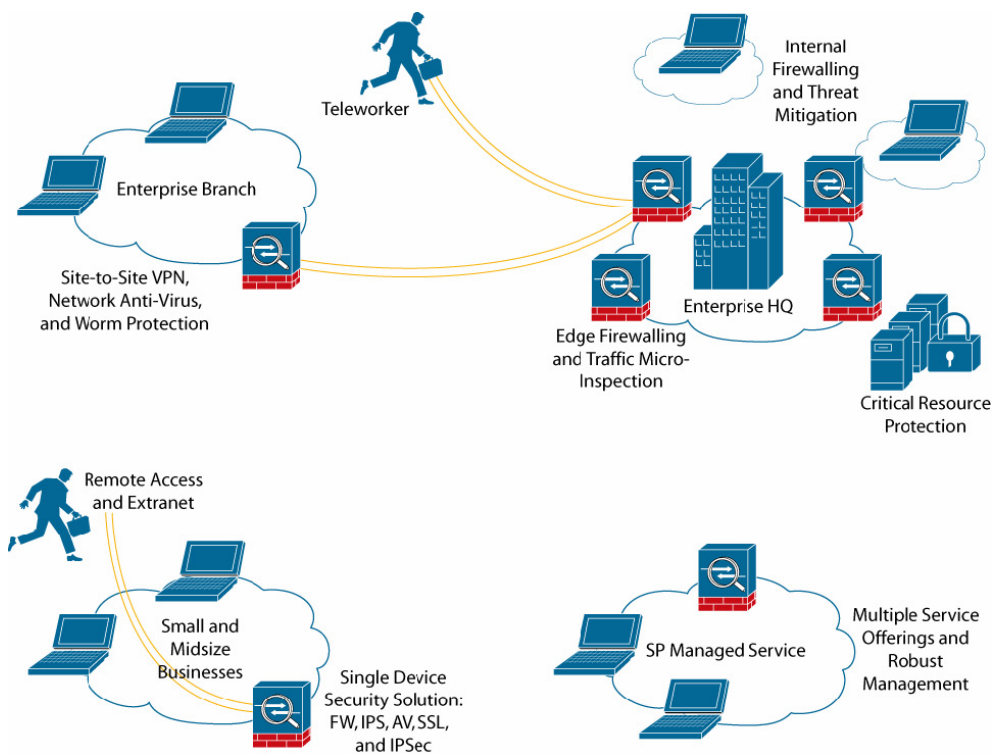
IPS のみを使用する場合は、Cisco IPS 4200 シリーズが Cisco ASA 5500 シリーズよりも価格および性能の点で有利です。Cisco ASA 5500 シリーズは、ファイアウォール、IPS、およびネットワーク ウイルス対策機能の統合によって実現される幅広い脅威の防御とアプリケーション セキュリティを必要とする環境に適しています。一方、Cisco IPS 4200 シリーズは IPS に特化した環境に適しています。

小規模企業やホーム オフィス、または大企業の本社でファイアウォールやサイト間 VPN を使用する場合は、Cisco PIX 501、PIX 506E、および PIX 535 セキュリティ アプライアンスが最も費用対効果の高いプラットフォームになります。Cisco ASA 5500 シリーズは、比較的小規模なサイトで複数のサービス アプリケーションを集約するのに適しています。一部の攻撃防御機能や VPN 機能のみを使用する場合は、Cisco PIX 501 および PIX 506E アプライアンスが SOHO 拠点向けの最も費用対効果の高い製品になります。1.7 Gbps の卓越したパフォーマンスを提供するハイエンドの Cisco PIX 535 セキュリティ アプライアンスは、価格および性能面で Cisco ASA 5500 シリーズを補完する製品です。また、前述のように、Cisco ASA 5500 および Cisco PIX 製品の機能は完全な互換性を持っているため、ネットワーク アーキテクチャの要件に応じて組み合わせて使用できます。

運用コスト

Cisco ASA 5500 シリーズは単体で幅広い用途に対応できるため、セキュリティおよび VPN の運用コストを大幅に改善できます(図 1)。Cisco ASA 5500 シリーズが提供する幅広いサービス(ファイアウォール、IPS、VPN、およびネットワーク ウイルス対策など)を利用すると、機能要件の異なるさまざまな環境にプラットフォームを導入できます。これらのサービスはすべて、シスコの導入実績豊富なセキュリティ アプライアンスや VPN アプライアンスから派生したものです。そのため、Cisco ASA 5500 シリーズを使用しても、機能、パフォーマンス、または管理性が損なわれることはありません。Cisco ASA 5500 シリーズを共通のプラットフォームとして使用すると、導入および管理が必要なプラットフォームの数を削減できます。また、すべての構成で共通の運用および管理環境が利用できるため、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 スタッフの教育を簡素化できます。

図 1 単体で幅広い用途に対応



次に、Cisco ASA 5500 シリーズを共通のプラットフォームとして使用できる一般的な構成例を示します。

- ネットワーク エッジまたは DMZ におけるアクセス制御、トラフィックとアプリケーションの検査、およびワーム/ウイルス/マルウェア対策の統合
- ネットワーク内部におけるアクセス制御、トラフィックとアプリケーションの検査、およびワーム/ウイルス/マルウェア対策の統合
- ネットワーク エッジまたは DMZ における従来型ファイアウォールとアプリケーション検査の利用
- ネットワーク内部における従来型ファイアウォールとアプリケーション検査の利用
- トラフィックとアプリケーションの検査およびワーム/ウイルス/マルウェア対策が統合されたリモートアクセス VPN
- 従来型の単体でのリモート アクセス VPN 終端
- サイト間 VPN サービス
- 任意の拠点におけるオールインワン型のアクセス制御、トラフィックとアプリケーションの検査、ワーム/ウイルス/マルウェア対策、リモートアクセス VPN、およびサイト間 VPN

まとめ

統合型のセキュリティ/VPN 構成および専用のセキュリティ/VPN 構成はいずれも、今日のネットワーク保護において一定の役割を担っています。いずれの構成を使用するかは、主にネットワークの規模、ネットワーク アーキテクチャ、ネットワーク内の場所、および IT サポート モデルなどで判断します。幅広いサービスに対応した Cisco ASA 5500 シリーズは柔軟性に優れているため、統合型のセキュリティ/VPN 構成または専用のセキュリティ/VPN 構成のどちらにも適応できます。

Cisco ASA 5500 シリーズを共通のプラットフォームとしてネットワーク内のさまざまな構成やセキュリティ機能に使用すると、ネットワーク アーキテクチャが簡素化されるため、導入および運用コストが削減されます。Cisco ASA 5500 シリーズは、Cisco PIX 515E および PIX 525 セキュリティ アプライアンスを使用する構成や、IPSec VPN サービスを提供する Cisco VPN 3000 シリーズ コンセントレータの代わりに使用するのに適しています。ただし、Cisco ASA 5500 シリーズは Cisco PIX および Cisco VPN 3000 シリーズのテクノロジーを使用するため、これらの既存の構成と機能的に完全な互換性を持っています。単体で IPS および SSL VPN を使用する場合は、Cisco IPS 4200 シリーズや Cisco VPN 3000 シリーズ コンセントレータがこれらの機能を実現する最適なプラットフォームになります。小規模企業やホーム オフィス、または大企業の本社で従来型のファイアウォールやサイト間 VPN を使用する場合は、Cisco PIX 501、PIX 506E、および PIX 535 セキュリティ アプライアンスが最も費用対効果の高いプラットフォームになります。これらは、マルチサイトに導入された Cisco ASA 5500 シリーズを補完して使用できます。

©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>

0120-933-122(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

お問い合わせ先