

Cisco Security Manager 3.01

Cisco® Security Manager は、エンタープライズクラス向けの優れたセキュリティ管理アプリケーションです。Cisco Security Manager を使用すると、ルータ、セキュリティ アプライアンス、およびスイッチ サービス モジュールで稼働するファイアウォール、VPN、Intrusion Prevention System (IPS; 侵入防御システム) サービスのプロビジョニングができます。

Cisco Security Manager はシスコ セキュリティ管理製品の 1 つであり、シスコの自己防衛型ネットワークにおける包括的なポリシーの管理と実施を可能にします。複数ベンダーの単機能セキュリティ製品を使用した場合、製品間の連携機能がないために脆弱性が残る可能性があります。シスコ セキュリティ管理製品を使用すれば、プロビジョニング、モニタリング、DDoS 攻撃軽減対策機能、およびアイデンティティを備えた包括的なソリューションが実現し、ネットワークの安全性と耐障害性を向上させることができ、運用もシンプルになります。シスコ セキュリティ管理製品のなかには、モニタリングと軽減対策機能を備えた Cisco Security Monitoring, Analysis, and Response System (CS-MARS) も含まれます。

Cisco Security Manager は、強力なポリシーベースの管理手法により、あらゆる規模のネットワークを効率的に管理できるアプリケーションです。わかりやすいグラフィカル ユーザー インターフェイスによって、誰にでも使いやすいツールとなっています。Cisco Security Manager は、さまざまなタスクとユーザー エクスペリエンス レベルに対応するために、アプリケーションに関する複数のビューを提供します。たとえば、デバイス視点のビュー(図 1 を参照)やマップ視点のビュー(図 2 を参照)があります。

図 1 デバイス視点のビュー: 簡易インターフェイスによる、デバイスの追加とセキュリティ ポリシーの編集および導入

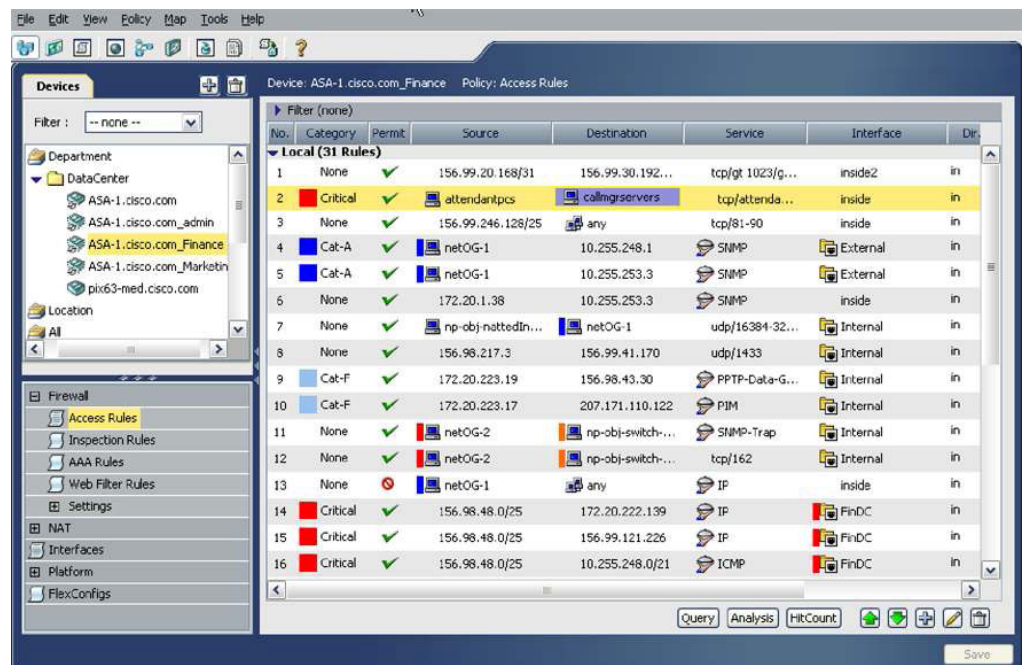
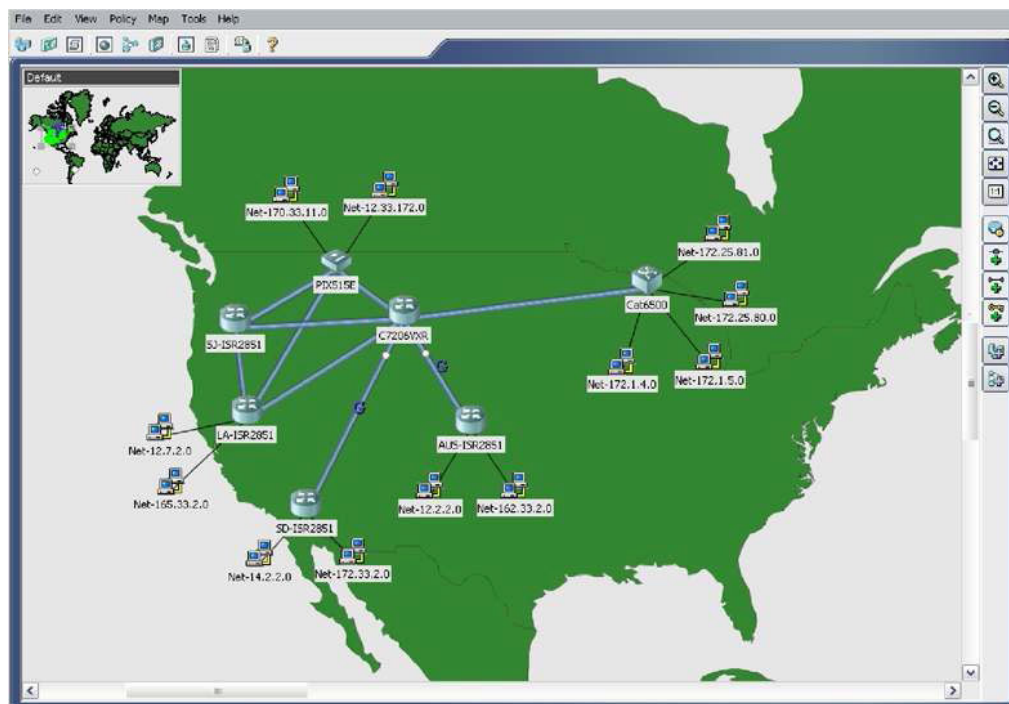
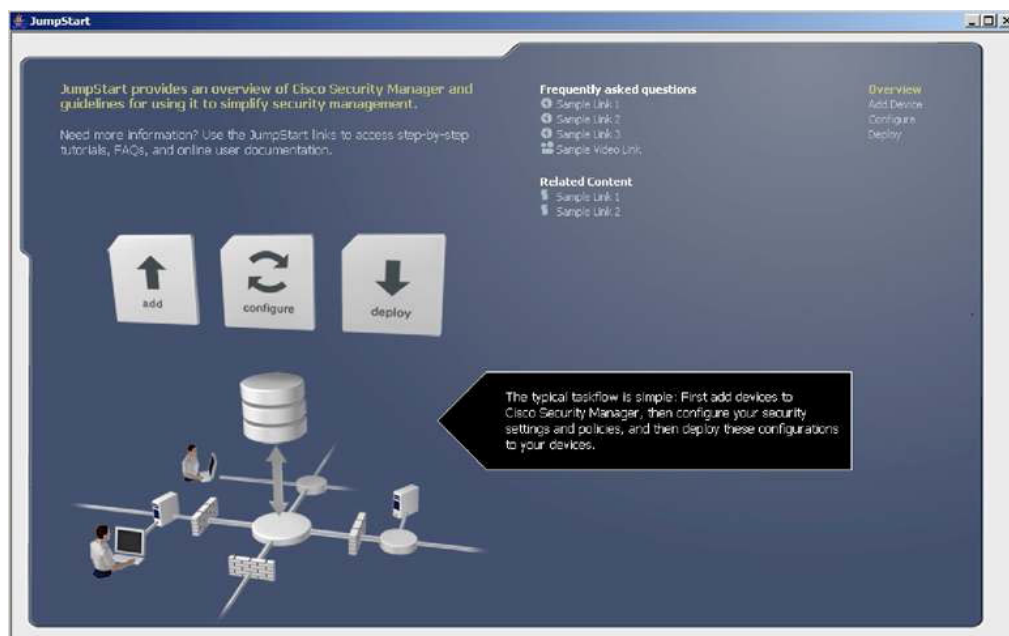


図 2 マップ視点のビュー:ポリシーとデバイスの視覚的な管理



Cisco Security Manager には、「JumpStart」と呼ばれるインタラクティブ チュートリアルも組み込まれており、新規のユーザは、Cisco Security Manager の機能と概念を短期間で習得できます(図 3 を参照)。

図 3 Cisco Security Manager の「JumpStart」インタラクティブ チュートリアル



Cisco Security Manager を使用すると、デバイス単位、デバイス グループ単位、またはグローバルにセキュリティ ポリシーを設定できます。セキュリティ ポリシーは、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 IPS 4200 シリーズ センサー、Cisco Catalyst® 6500 シリーズ サービス モジュール、および Cisco IOS® ソフトウェア セキュリティ ソフトウェア イメージを実行するシスコ ルータ プラットフォームに適用できます。

表 1 に、Cisco Security Manager 3.01 の機能と利点を示します。

表 1 Cisco Security Manager 3.01 の機能と利点

機能	利点
スケーラブルなネットワーク管理	<p>Cisco Security Manager を利用することで、少数のデバイスで構成されるネットワークから数千台のデバイスで構成されるネットワークまで、効率的な管理が可能になります。スケーラビリティは、強力なポリシーベースの管理手法により実現されます。この手法により設定を 1 回定義したあと、オプションで設定を個別のデバイス、デバイスのグループ、または企業全体に割り当てることができます。設定を変更した場合、Cisco Security Manager は、関連するすべてのネットワーク デバイスに自動的に変更を適用します。ファイアウォールまたは VPN ポリシーはプラットフォームに依存しないため、シスコ ルータ、セキュリティ アプライアンス、またはサービス モジュールなど、異なるデバイス プラットフォーム間に適用できます。Cisco Security Manager は、ポリシーの再利用と共有を行う一方で、必要に応じてデバイス固有の設定をカスタマイズすることもできる、デバイスレベルの柔軟な上書き機能も備えています。</p>
VPN プロビジョニング	<p>VPN ウィザードを使用すると、サイト間、ハブ アンド スポーク、フルメッシュ、およびエクストラネット VPN を簡単に設定できます。</p> <ul style="list-style-type: none"> • Cisco Security Manager は、ダイナミック IP と階層型認証を使用する、Dynamic Multipoint VPN (DMVPN) と Generic Routing Encapsulation (GRE; 総称ルーティング カプセル化) IP Security (IPSec) をサポートしています。 • VPN と Easy VPN サービスはリモートで設定できます。 • 安全なデバイス プロビジョニングのサポートにより、自動で展開が可能です。 • ヘッドエンド用の自動フェールオーバーとロードバランシングの設定がサポートされています。
ファイアウォール プロビジョニング	<p>Cisco Security Manager を使用すると、管理者は、Cisco ASA 5500 シリーズ アプライアンス、Cisco PIX アプライアンス、Cisco Catalyst 6500 シリーズ ファイアウォール サービス モジュール、および Cisco IOS ソフトウェア セキュリティ イメージを実行するシスコ サービス統合型ルータ プラットフォームのポリシーを設定できます。</p> <ul style="list-style-type: none"> • ソフトウェアにより、すべてのプラットフォームに 1 つのルール テーブルが提供されます。ユーザは、1 つのソリューションでこれらのデバイスを管理できます。 • ルール分析機能により、他のルールと重複または競合するファイアウォール ルールがレポートされます。 • オブジェクト グループ化機能により、特定のセキュリティ ポリシーの実装に必要なアクセス ルールの数が大幅に削減されます。オブジェクト グループ化では、類似したオブジェクトをグループ化するアルゴリズムを使用することで、1 つのアクセス ルールをグループ内のすべてのオブジェクトに適用できます。 • ソフトウェアにより、ネットワークに影響しないルールの識別と削除が可能です。 • Access Control List (ACL; アクセス コントロール リスト) ヒット カウント機能により、トラフィックが正常に送信されていることが確認されます。 • ポリシー クエリー機能により、ワイルドカードを含む、特定の送信元、宛先、およびサービス フローと一致するルールが表示されます。 • 設定を容易にするために、デバイス情報をデバイス リポジトリまたはコンフィギュレーション ファイルからインポートしたり、ソフトウェアに追加したりできます。また、デバイス自体からファイアウォール ポリシーを検出することもできます。 • インターフェイス ロールを使用すると、ユーザはインターフェイスのグループにスケーラブルな方法でルール ポリシーを適用できます。
IPS プロビジョニング	<p>Cisco Security Manager では、IPS センサーの IPS マネージャを使用して、次の機能をサポートしています。</p> <ul style="list-style-type: none"> • Cisco IPS センサー ソフトウェア — インライン型のネットワークベースのソフトウェア ソリューションで、ワーム、スパイウェアとアドウェア、ネットワーク ウイルス、およびアプリケーションの不正利用を含む不正なトラフィックを、業務の継続に影響する前に、正確に識別、分類、抑止するように設計されています。 • Cisco IOS IPS — インライン型の侵入防御機能を持つ Cisco IOS IPS は、インライン型のディープ パケット インスペクション ベースの IPS ソリューションを提供する業界初のシステムです。Cisco IOS IPS は、シスコ ルータがトラフィック フォワーディング パフォーマンスを損なうことなく、さまざまなネットワーク攻撃を効率的に軽減できるようにします。Cisco IOS IPS は、シスコの自己防衛型ネットワークの中心となるコンポーネントで、不正なトラフィックや攻撃的なトラフィックをリアルタイムに識別、分類、および抑止できます。Cisco IOS IPS は、トラフィックの廃棄、アラームの送信、または接続のリセットを行って、ルータがセキュリティの脅威に迅速に対応できるようにします。IPS マネージャは、Cisco IOS IPS の詳細な設定を行います。 • 単一インターフェイスのマルチ VLAN IPS 設定 — インライン サポートの導入により、IPS マネージャで VLAN のペアを単一インターフェイスに割り当てることができます。 • レート リミット設定 — 過度の帯域幅を使用できないようにすることで、IPS デバイスが特定のタイプのトラフィックを制限できるようにします。また、Cisco IOS ルータなどの外部デバイスにレート リミットを実行するように通知して、同じ機能を実行させることもできます。 • シグニチャ更新の自動適用 — ユーザは、Cisco.com からシグニチャ更新、マイナー リリース、およびパッチをダウンロードし、Cisco IPS センサーを自動的に更新できます。 • シグニチャのコピー ウィザード — 1 台のデバイスから複数のデバイスにシグニチャチューニングをコピーできます。 • グローバル イベント設定 — イベント アクションの上書き、イベント アクション フィルタ、およびイベント変数をすべての Cisco IPS センサーにグローバルに適用します。 • アウトオブバンド設定検出 — IPS マネージャは、他の管理コンポーネントによって行われたデバイスのアウトオブバンド設定変更を検出します。アウトオブバンド設定が検出されると、ユーザは Sensor Health and Welfare 機能を介して通知を受けることができます。

機能	利点
統合セキュリティ サービスの管理	Cisco Security Manager により、VPN の QoS(Quality of Service)、ルーティング、Network Admission Control(NAC)などを含む、統合セキュリティ サービスを管理できます。
柔軟なデバイス グループ化オプション	ユーザは、業務上の機能または配置に基づいてデバイス グループを作成および定義し、組織的な構造を正確に表すことができます。グループ内のすべてのデバイスを 1 つのデバイスを扱うように簡単に管理できます。
複数のアプリケーション ビュー	Cisco Security Manager は、さまざまな使用事例とエクスペリエンス レベルをサポートするために、アプリケーションに関する複数のビューを提供します。デバイス視点のビューは、初心者ユーザ、または単一のデバイス マネージャの使用に慣れているユーザに便利です。マップ視点のビューは、VPN のトポロジ、または Cisco Catalyst 6500 シリーズ サービス モジュールとセキュリティ コンテキスト間の抑制関係を視覚化します。ポリシー視点のビューは、非常に効率的でスケーラブルな複数デバイスの管理に優れています。
Policy Object Manager	再利用可能なオブジェクトを作成して、ネットワーク アドレス、サービス、デバイス設定、時間範囲、または VPN パラメータなどを表すことができます。オブジェクトは、1 回定義すると何回でも使用できるため、手動で値を入力する必要がありません。
Deployment Manager — 柔軟な展開オプション	Cisco Security Manager は、デバイスまたはファイルへのオンデマンドの展開と計画的な展開の両方をサポートしています。
ロールバック	Cisco Security Manager は、必要に応じて、以前の設定へのロールバックを実行できます。
ロールベースのアクセス コントロール	Cisco Security Manager を使用すると、複数の管理者に対して適切な制御を使用してアクセス権を定義できます。Cisco Security Manager には 5 つのユーザ ロールがあり、オプションの Cisco Secure ACS で追加のロールを使用することもできます。
ワークフロー	Cisco Security Manager では、ポリシーの導入時に特定のタスクを各管理者に割り当てることができ、変更管理と追跡機能も提供します。ワークフローを使用すると、スタッフの共同作業(ネットワークとセキュリティ運用間など)が改善されます。
分散型の展開方法 — Auto Update Server、Cisco Network Services Configuration Engine	Cisco Security Manager により、ダイナミック アドレスまたは NAT アドレスを持つ多数のリモート ファイアウォールの更新が簡易化されます。この機能は、リモート サイトに断続的なネットワーク リンクがあり、最小限の技術スタッフしかいないユーザに役立ちます。
運用管理	Cisco Security Manager は、ソフトウェアの配布やデバイス インベントリ レポートなどの運用機能に役立ちます。また、Device and Credentials Repository(DCR)と CiscoWorks Resource Manager Essentials(RME)と統合できます。
状態とパフォーマンスのモニタリング	Cisco Security Manager サービス契約を結んでいるユーザは、Cisco.com から CiscoWorks Monitoring Center for Performance アプリケーションをダウンロードできます。このアプリケーションは、シスコのネットワーク デバイスおよび特定のセキュリティ サービスのための、状態とパフォーマンスのモニタリング データを提供します。

Cisco Security Manager 3.01 の変更点

Cisco Security Manager 3.01 は、Cisco Security Manager 3.0 に次の機能拡張を行うマイナー ソフトウェア アップデートです。

- Cisco Catalyst 6500 シリーズ ファイアウォール サービス モジュール 3.1 のサポート
- Cisco ASA ソフトウェア 7.1 および Cisco PIX ソフトウェア 7.1 のサポート
- Cisco 7600 シリーズ/Cisco Catalyst 6500 シリーズ IPsec VPN 共有ポート アダプタ デバイスのサポート
- Cisco Catalyst 6500 シリーズ ルータの ACL の管理機能のサポート
- Cisco IOS ルータでの Network Time Protocol(NTP)および Syslog 設定機能のサポート
- CiscoWorks RME(バージョン 4.04)のアップデート
- 複数の既知のソフトウェア バグに対する修正の追加

Cisco Security Manager 3.01 ではさらに、ソフトウェアに追加できるデバイス数を制御するライセンス キーが適用されます。バージョン 3.0 の時点でライセンスの制限数を超過している場合、バージョン 3.01 にアップグレードすることで、管理ソフトウェアには新しいデバイスを追加できなくなります。オペレータは、追加のライセンス キーを購入することで、より多くのデバイスを管理できます。この場合、ソフトウェアを再インストールする必要はありません。Cisco Security Manager 管理者オプションを使用すると、新しいキーを簡単に追加できます。ライセンス購入オプションについては、次の URL にある Product Bulletin を参照してください。

http://www.cisco.com/en/US/products/ps6498/prod_bulletins_list.html

表 2 に、Cisco Security Manager の最小サーバ要件、表 3 に最小クライアント要件を示します。

表 2 サーバの要件と制限

コンポーネント	最小要件
システム ハードウェア	<ul style="list-style-type: none"> IBM PC 互換機、2 GHz 以上のプロセッサ搭載 1024 × 768 以上の解像度のカラー モニタと 16 ビット カラーに対応したビデオ カード DVD-ROM ドライブ 100BASE-T(100 Mbps)以上のネットワーク接続、単一インターフェイスのみ キーボード マウス
ファイル システム	<ul style="list-style-type: none"> NTFS
メモリ(RAM)	<ul style="list-style-type: none"> 2 GB
システム ソフトウェア	<p>次のいずれかを使用できます。</p> <ul style="list-style-type: none"> Microsoft Windows 2003 Server: <ul style="list-style-type: none"> Enterprise Edition(SP1 を適用) Standard Edition(SP1 を適用) Microsoft Windows 2000: <ul style="list-style-type: none"> Advanced Server(SP4 を適用) Server(SP4 を適用) Professional(SP4 を適用) <p>注: Cisco Security Manager は、Windows のアメリカ英語版と日本語版のみをサポートしています。サーバで Sybase データベース ファイルを使用するためには、Microsoft ODBC Driver Manager 3.510 以降も必要です。</p>
ブラウザ	<p>次のいずれかを使用できます。</p> <ul style="list-style-type: none"> Microsoft Internet Explorer 6.0(6.0.2600) Microsoft Internet Explorer 6.0(SP1 を適用) (6.0.2800) Mozilla 1.7 または 1.7.5
圧縮ソフトウェア	WinZip 9.0 または同等のソフトウェア
ハードドライブの空き容量	20 GB
IP アドレス	<p>スタティック IP アドレス × 1</p> <p>サーバに複数の IP アドレスが設定されている場合は、1 つのアドレスを除いてすべてを無効にします。ターゲット サーバでダイナミック IP アドレスが検出された場合、Cisco Security Manager インストーラに警告が表示されます。ダイナミック アドレスはサポートされていません。</p>

表 3 クライアントの要件と制限

コンポーネント	最小要件
システム ハードウェア	<ul style="list-style-type: none"> IBM PC 互換機、1 GHz 以上のプロセッサ搭載 カラー モニタと 24 ビット カラーに設定されたビデオ カード キーボード マウス
メモリ(RAM)	1 GB
仮想メモリ/スワップ領域	512 MB
ハードドライブの空き容量	10 GB
オペレーティング システム	<p>次のいずれかを使用できます。</p> <ul style="list-style-type: none"> Microsoft Windows XP Professional(SP1 以上を適用) Microsoft Windows 2003: <ul style="list-style-type: none"> Server Edition(SP1 を適用) Enterprise Edition(SP1 を適用) Microsoft Windows 2000: <ul style="list-style-type: none"> Advanced Server(SP4 を適用) Professional(SP4 を適用) <p>注: Cisco Security Manager クライアントは、Windows のアメリカ英語版と日本語版のみをサポートします。他の言語バージョンはサポートしていません。</p>
ブラウザ	<p>次のいずれかを使用できます。</p> <ul style="list-style-type: none"> Microsoft Internet Explorer 6.0(6.0.2600) Microsoft Internet Explorer 6.0(SP1 を適用) (6.0.2800) Mozilla 1.7 または 1.7.5
Java	<p>Cisco Security Manager クライアントには、完全に独立して機能する Java が組み込まれます。このバージョンの Java は、ブラウザの設定または他の Java ベースのアプリケーションには影響しません。</p> <p>IPS マネージャの起動時に必要なバージョンの Java が存在しない場合、Cisco Security Manager サーバに、必要なバージョンの Java をダウンロードおよびインストールする方法を示すメッセージが表示されます。</p>

Cisco Security Manager のハードウェアおよびソフトウェアの要件の詳細については、http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html にある『Cisco Security Manager Installation Guide』を参照してください。

表 4 に、Cisco Security Manager でサポートされるデバイス製品ファミリーの一部を示します。製品ファミリーの一覧については、http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html にある『Supported Devices and OS Versions for Cisco Security Manager』を参照してください。

表 4 Cisco Security Manager でサポートされるシスコ デバイスの概要

サポート対象デバイス
Cisco PIX セキュリティ アプライアンス
Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンス
Cisco サービス統合型ルータ
Cisco 7600 シリーズ ルータ
Cisco 7500 シリーズ ルータ
Cisco 7300 シリーズ ルータ
Cisco 7200 シリーズ ルータ
Cisco 7100 シリーズ ルータ
Cisco Catalyst 6500 シリーズ ファイアウォール サービス モジュール
Cisco Catalyst 6500 シリーズ VPN サービス モジュール
Cisco 7600 シリーズ/Catalyst 6500 シリーズ IPSec VPN 共有ポート アダプタ
Cisco Catalyst 6500 シリーズ IDSM-2
Cisco IPS 4200 シリーズ センサー
Cisco Catalyst 6500 シリーズ IPS サービス モジュール
Cisco IOS IPS ルータ センサー モジュール

オプションの CiscoWorks RME 4.04 でサポートされるデバイスの一覧については、次の URL にある互換性に関する資料を参照してください。

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

発注情報

Cisco Security Manager の Product Bulletin には、ライセンス オプションと発注の詳細が記載されています。この Product Bulletin は、<http://www.cisco.com/jp/product/hs/security/csm> にある製品資料で公開されています。

©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。(0701R)

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/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