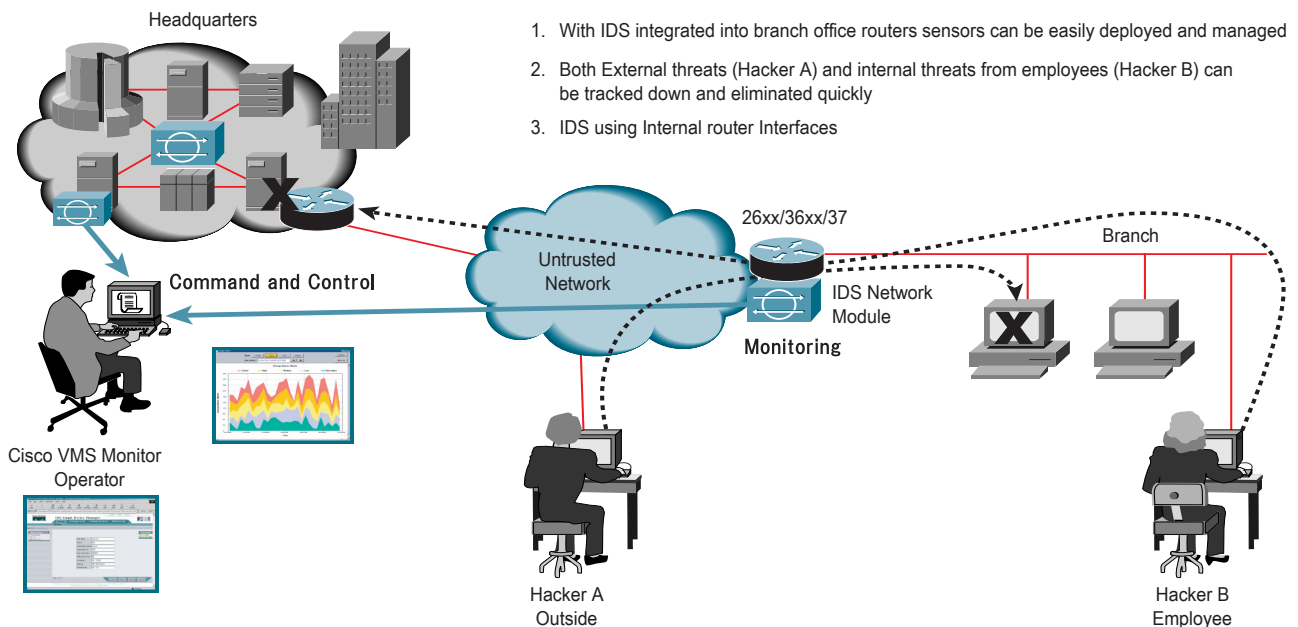


# Cisco 2600/3600/3700 シリーズ ルータ用 Cisco IDS ネットワーク モジュール

Cisco® IDS ネットワーク モジュールは、シスコによる Intrusion Detection System (IDS) ネットワーク セキュリティ ソリューションの1つで、企業資産を保護し、運用コストを削減します。

Cisco 2600/3600/3700 シリーズ ルータ用 Cisco IDS ネットワーク モジュールは、Cisco IDS センサ製品のひとつであり、シスコの侵入防御システム (IPS) の構成要素です。これらの IDS センサは、データおよび情報インフラストラクチャを保護するために、Cisco IDS 管理コンソール、CiscoWorks VPN (仮想私設網) / セキュリティ管理ソリューション (VMS)、Cisco IDS Device Manager など、ほかの IDS コンポーネントと連携して動作します (図 1 を参照)。セキュリティに対する脅威が複雑化しつつある今日、高度な保護性能を維持するには、効果的なネットワーク侵入セキュリティ ソリューションが不可欠です。厳重な侵入防御機能によって、ビジネスの継続性を確保し、侵入による損害を未然に防ぐことができます。シスコの侵入防御システムに関する詳細については、<http://www.cisco.com/go/ids> (英語) を参照してください。

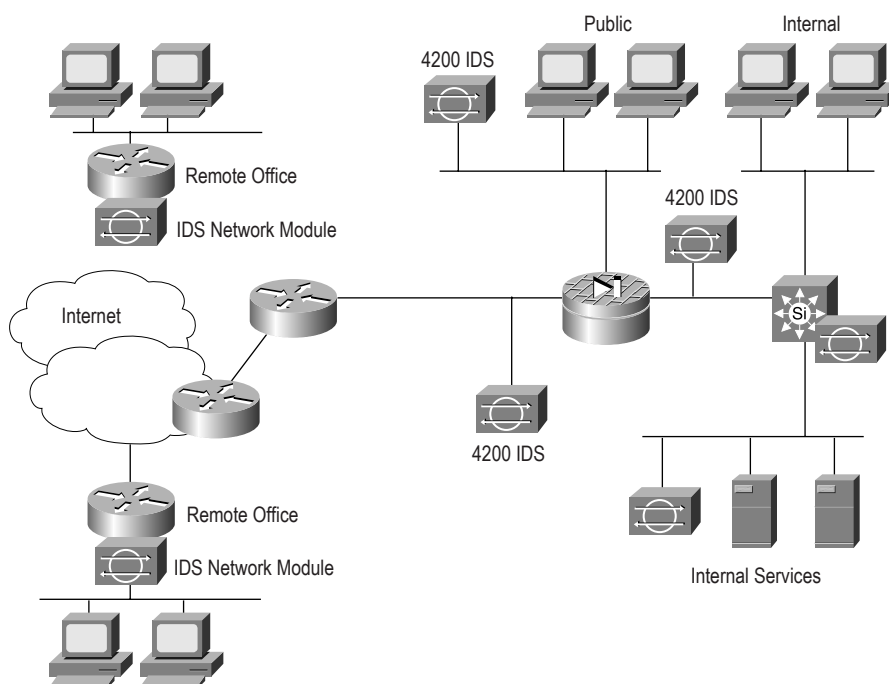
図 1 Cisco 2600、3600、または 3700 上の Cisco IDS ネットワーク モジュール センサの配置





この IDS ソリューションでは、ネットワーク アーキテクチャ上の必要な場所に IDS センサを配置することが可能です (図 2 を参照)。Cisco IDS 4200 シリーズ センサには、Cisco IDS 4215、IDS 4235、IDS 4250、および IDS 4250-XL というタイプがあります。ルーティングおよびスイッチング プラットフォーム上で使用できる Cisco IDS ソリューションとしては、Cisco Catalyst® 6500 シリーズ IDS サービス モジュール (IDSM-2)、および Cisco 2600XM、3660、3700 シリーズ ルータ用の Cisco IDS ネットワーク モジュールがあります。シスコの IDS 製品には、エンタープライズ環境からサービス プロバイダー環境まで、さまざまな環境に簡単に組み込むことのできる広範囲のソリューションが用意されています。各センサはルータごとに異なる帯域要件に対応しています (Cisco 2600XM は最大 10 Mbps、Cisco 3700 シリーズは最大 45 Mbps)。アプライアンス製品では、80 Mbps ~ 1 Gbps がサポートされます。Cisco Catalyst IDSM-2 では、600 Mbps がサポートされます。シスコの侵入防御 (IPS) 製品ファミリーに関する詳細については、<http://www.cisco.com/go/ids> (英語) を参照してください。

図 2 Cisco IDS ファミリー : Cisco 4200 ファミリーと Cisco IDS ネットワーク モジュール



### Cisco 2600/3600/3700 シリーズ ルータ用 Cisco IDS ネットワーク モジュール : IDS とブランチ オフィス ルーティングの統合

ブランチ オフィス ルーティングに IDS を統合することによって、WAN リンクの保護をより容易にするとともに、運用コストを削減できます。ブランチ オフィス ルータに IDS を統合した場合、次の多くの重要なメリットを実現します。

- **物理的なスペースの節約**— Cisco IDS ネットワーク モジュールは、Cisco 2600XM シリーズ、Cisco 3660、または Cisco 3700 シリーズ ブランチ オフィス ルータのネットワーク モジュール スロットに 1 つ搭載できます。
- **電源管理およびケーブル管理の簡易性**— Cisco IDS ネットワーク モジュールでは、ルータの電源オプション (DC 電源および冗長電源) を利用できます。

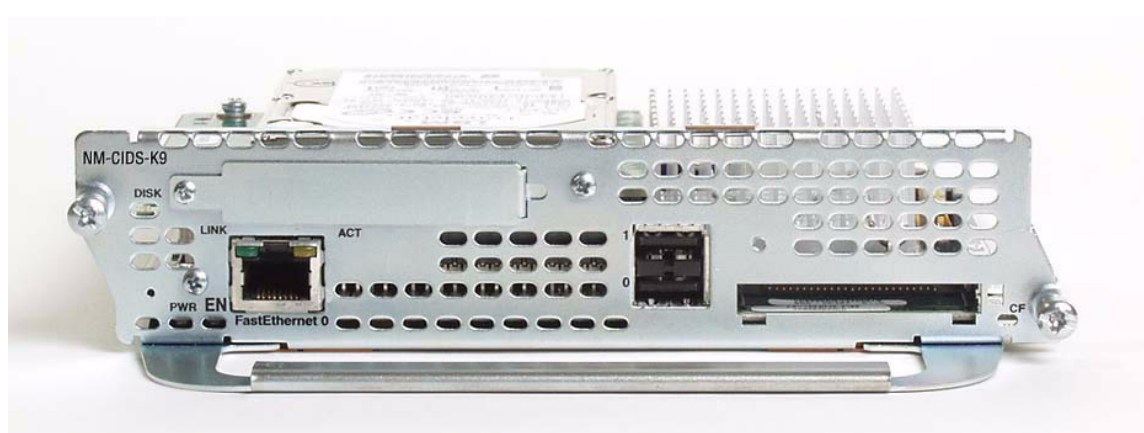


- **共通の管理インターフェイス**—IDS ネットワーク モジュールの設定および管理は、Cisco IOS® の CLI (コマンドライン インターフェイス) を使用して行うことができます。Cisco IDS 4200 シリーズでサポートされる CiscoWorks Management Center for IDS Sensors に対応しているため、アプライアンスおよびルータ IDS センサの両方を、1つの管理システムで集中的に管理できます。
- **ネットワーク コマンドおよび制御インターフェイス** — コマンド投入と制御には外部ファスト イーサネット ポートを使用するため、Cisco IDS ネットワーク モジュールのルータ内部インターフェイスは、IDS エンジンで処理するパケットのキャプチャリング専用インターフェイスとして使用することが可能です。
- **Cisco IDS ネットワーク モジュールの専用プロセッサによるパフォーマンスの向上** — ネットワーク モジュール自体に専用の CPU が搭載されているため、ルータの CPU には IDS 関連タスクの負荷が掛かりません。
- **運用コストの削減**— Cisco IDS ネットワーク モジュールは、ルータと同時に保守を行うことができるため、ネットワーク運用コストを節約できます。

Cisco IDS ネットワーク モジュールは最大 45 Mbps のトラフィックをモニタすることができ、T1/E1 環境および T3 環境に適しています。この IDS ネットワーク モジュールを搭載したルータは、一般的な Cisco IOS 機能のほかに、VPN、ファイアウォール、Multiprotocol Label Switching (MPLS)、Network Address Translation (NAT; ネットワークアドレス変換)、Web Cache Control Protocol (WCCP) など、その他の Cisco IOS セキュリティ機能もサポートしています。

Cisco IDS ネットワーク モジュールは、Cisco 2600XM シリーズ、Cisco 3660、および Cisco 3700 シリーズプラットフォーム上の1つのネットワーク モジュール スロットに搭載します。イベントのログおよびストレージには、20 GB のハード ディスクを使用できます。コマンドおよび制御には外部イーサネット ポートが使用され、管理用の発信ポートの安全性を確保します。この構成では、セキュリティ処理とネットワーク動作にそれぞれ専用のコマンドおよび制御インターフェイスを使用することもできます。

図 3 Cisco IDS ネットワーク モジュール





## シスコの侵入防御システム（IPS）の特長

### 効果的な侵入防御

効果的な侵入防御システムは、次の4つの要素によって実現します。

- **脅威の正確な検知**— 環境を保護するための第一段階として、Cisco IDS Sensor ソフトウェア バージョン 4.1 が、すべての潜在的な脅威を総合的に検出します。
- **脅威のインテリジェントな検証**— シスコの Threat Response テクノロジーによって誤ったアラームが実質的に排除され、侵入を防ぐために直ちに対処する必要のある脅威が自動的に判別されます。
- **管理の簡易性**— ブラウザ ベースの各種ツールによる簡単な対話形式と、強力な解析ツールで脅威に対し迅速かつ効果的に対処できます。
- **柔軟性のある構成オプション**— 高い可用性を持つ幅広い種類のデバイスをバックボーンとして、安全かつ効果的な侵入防御システムをフレキシブルに構成できます。

安全性と効率性に優れた、これら4つの総合的な侵入防御ソリューションの要素について、さらに詳しい情報をお求めの場合は、次の URL をご参照ください。

<http://www.cisco.com/en/US/products/sw/secursw/ps21113/> (英語サイト)

<http://www.cisco.com/japanese/warp/public/3/jp/solution/netsol/security/> (シスコ セキュリティ ソリューション日本語サイト)

### 柔軟性のある構成オプション

シスコでは、お客様の環境に適したコスト効率の高い侵入防御ソリューションをご利用いただけるよう、広範囲にわたるネットワーク IDS 構成オプションを提供しています。どのソリューションもハイ アベイラビリティを前提に設計されており、シスコの充実したスタマー サポートの対象となります。ネットワーク IDS ソリューションは、10 ~ 45 Mbps (Cisco IDS ネットワーク モジュールの場合) から 45 Mbps ~ 1 Gbps (Cisco Catalyst 製品ライン) まで、さまざまなパフォーマンス レベルでご使用いただけます。

Cisco IDS 4200 シリーズ センサの詳細については、次の URL を参照してください。

<http://www.cisco.com/japanese/warp/public/3/jp/product/hs/security/ids4200/> (日本語)

Cisco Catalyst 6500 シリーズ IDSM-2 サービス モジュールの詳細については、次の URL を参照してください。

<http://www.cisco.com/japanese/warp/public/3/jp/product/hs/switches/cat6500/modules/service/idsm2/> (日本語)

### 簡単なインストール

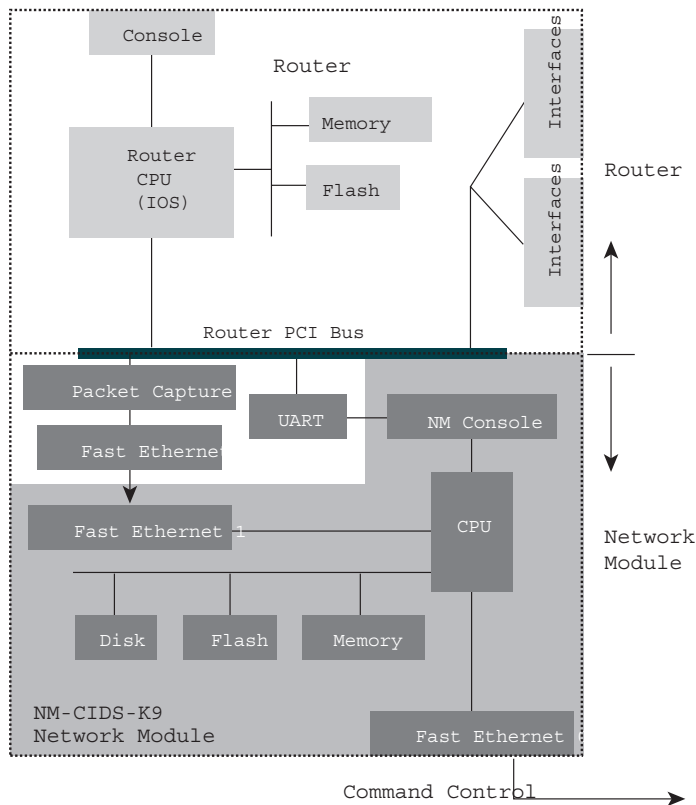
Cisco IDS ネットワーク モジュールは簡単にインストールできます。シャーシの空いているスロットにモジュールを取り付け、モジュールの初期化パラメータを設定し、ルータがモジュールを認識してトラフィックを送信するように設定するだけです。IDS ネットワーク モジュールが初期化され動作を開始したあとは、任意の管理コンソールからコンフィギュレーションを変更してモジュールに適用することができます。

### ハードウェア アーキテクチャ

Cisco IDS Sensor 4.1 ソフトウェアは、ネットワーク モジュール上の専用のプロセッサで動作し、ログ保存用に 20 ギガビットのハードディスク ドライブを使用します。ルータは内部ファスト イーサネット インターフェイスを通じて、検証のためネットワーク モジュールにパケットをコピーします。ネットワーク管理ステーションとネットワーク モジュールの通信には、外部ファスト イーサネット インターフェイスが使用されます。



図 4 CiscoWorks VPN/セキュリティ管理ソリューション (VMS) 2.1 を使用する統合型 Cisco IDS ネットワーク モジュールのアーキテクチャ



### 主な管理機能

- *CiscoWorks Management Center for IDS Sensors* — ネットワークおよびスイッチの IDS センサの設定に使用します。グループプロファイルを使用して複数のセンサを同時に設定できる、拡張性の高い管理機能です。
- *CiscoWorks Monitoring Center for Security* — ネットワーク IDS、スイッチ IDS、ホスト IDS、ファイアウォール、およびルータからのイベントのキャプチャ、保管、表示、関連づけ、およびレポート生成を実行する統合型のモニタリング機能です。

詳細については、次の URL を参照してください。 <http://www.cisco.com/japanese/warp/public/3/jp/product/hs/netmgt/cw2000/vpnsms/> (日本語)

### Cisco IDS ネットワーク モジュール製品概要

#### ネットワーク モジュール

表 1 に、Cisco IDS ネットワーク モジュールの製品番号および製品名を示します。発注の際にご利用ください。

表 1 Cisco ID ネットワーク モジュールの製品番号

製品番号	説明
NM-CIDS-K9	Cisco IDS ネットワーク モジュール、20 GB IDE ハード ディスク



## 必要なソフトウェア ライセンス

Cisco IDS ネットワーク モジュールは、Cisco IOS ソフトウェア Release 12.2(15)ZJ 以上で提供される Cisco IOS ファームウェアまたは IDS フィーチャ ライセンスで使用できます。表 2 に、Cisco 2600/3600/3700 ルータで使用可能な Cisco IOS IDS ソフトウェア イメージの一覧を示します。

表 2 Cisco 2600/3600/3700 ルータで使用可能な Cisco IOS IDS ソフトウェア イメージ

製品
IOS IP/FW/IDS
IOS IP/FW/IDS PLUS IPSEC 56
IOS IP/FW/IDS PLUS IPSEC 3DES
IOS IP/IPX/AT/DEC/FW/IDS PLUS
IOS ENTERPRISE/FW/IDS PLUS IPSEC 56
IOS ENTERPRISE/FW/IDS PLUS IPSEC 3DES

## サポート対象のルータ

1 台のルータで使用できる Cisco IDS ネットワーク モジュールは 1 枚です。表 3 に、Cisco IDS ネットワーク モジュールに対応するルーティング プラットフォームの一覧を示します。

表 3 Cisco IDS ネットワーク モジュールをサポートするプラットフォーム

ルータ	NM-CIDS-K9
Cisco 2600 シリーズ	不可
Cisco 2600XM シリーズ	可
Cisco 2691	可
Cisco 3620	不可
Cisco 3631	不可
Cisco 3640、Cisco 3640A	不可
Cisco 3660	可
Cisco 3725	可
Cisco 3745	可



## ハードウェア仕様

表 4 に、Cisco IDS ネットワーク モジュールのハードウェア仕様を示します。

表 4 Cisco IDS ネットワーク モジュールのハードウェア仕様

項目	NM-CIDS-K9
<b>ハードウェア機能</b>	
プロセッサ	500 MHz Intel Mobile Pentium III
デフォルトの SDRAM	256 MB
最大 SDRAM	512 MB
内部ディスク ストレージ	Cisco IDS ネットワーク モジュール 20 GB IDE
ネットワーク インターフェイス	内部 10/100 Mbps イーサネット ポート × 1 (ルータのバックプレーンまで) および 外部 10/100 Mbps イーサネット ポート × 1
フラッシュ メモリ	内蔵 16 MB フラッシュ メモリとオプションの外部コンパクト フラッシュ メモリ
<b>物理仕様</b>	
寸法 (高さ×幅×奥行)	3.9 × 18.0 × 18.3 cm 1.55 × 7.10 × 7.2 インチ
重量	最大 0.7 kg 最大 1.5 ポンド
動作湿度	5 ~ 95% (結露しないこと)
動作温度	0 ~ 40°C 32 ~ 104°F
保管温度	-40 ~ 85°C -40 ~ 185°F
動作高度	0 ~ 3000 m 0 ~ 10,000 フィート
安全性	UL 1950、CSA-C22.2 No. 950、EN 60950、IEC 60950
EMC (電磁適合性)	FCC Part 15 Class A、EN55022 Class B、AS/NZS 3548 Class A、CISPR22 Class B、 VCCI Class B、EN55024、EN61000-3-2、EN61000-3-3



## 製品仕様

表 5 に、Cisco IDS ネットワーク モジュールの製品仕様を示します。

表 5 Cisco IDS ネットワーク モジュールの仕様

項目	NM-CIDS-K9
ハードウェア機能	
Cisco IDS ネットワーク モジュールを Cisco 2600XM シリーズ ルータに搭載した場合のパフォーマンス	最大 10 Mbps
Cisco IDS ネットワーク モジュールを Cisco 3700 シリーズ ルータに搭載した場合のパフォーマンス	最大 45 Mbps
標準のモニタリング インターフェイス	ルータの内部バス
標準のコマンドおよび制御インターフェイス	ネットワーク モジュールの外部 10/1010/100BASE-T
オプションのインターフェイス	なし
パフォーマンスの拡張	不可
ステートフル パターンの認識	可
学習的検出 (Heuristic detection)	可
異常の検出 (Anomaly detection)	可
スウィープまたはフラッド	可
DoS の軽減	可
ワームまたはウイルス	可
Common Gateway Interface (CGI) または WWW アタック	可
バッファ オーバーフローの防止	可
Remote-Procedure Call (RPC) アタックの検知	可
IP フラグメンテーション アタック	可
Internet Control Message Protocol (ICMP) アタック	可
Simple Message Transfer Protocol (SMTP)、sendmail、Internet Message Access Protocol (IMAP)、または Post Office Protocol (POP) アタック	可
FTP (ファイル転送プロトコル)、Secure Shell Protocol (SSH)、Telnet、rlogin アタック	可
Domain Name System (DNS; ドメイン ネーム システム) アタック	可
TCP ハイジャック	可
Windows または NetBIO アタック	可
TCP アプリケーションの保護	可
Back Orifice アタック	可
Network Timing Protocol (NTP) アタック	可
Signature Micro-Engine 技術によるシグニチャのカスタマイズ	可



表 5 Cisco IDS ネットワーク モジュールの仕様 (続き)

項目	NM-CIDS-K9
シグニチャの自動更新	可
アラーム集約	可
802.1Q トラフィックのサポート	可
センサと管理コンソール間の IP Security (IPSec) または Secure Sockets Layer (SSL)	可
シグニチャ パッケージの暗号化	可
SSH によるリモート管理	可
安全なファイル転送のための Serial Control Protocol (SCP) サポート	可
IP フラグメンテーション再アセンブリ	可
TCP ストリームの再アセンブリ	可
Unicode の復号化	可
ルータ ACL (アクセス制御リスト) の変更	可
ファイアウォール ポリシーの変更	可
スイッチ ACL の変更	可
TCP リセットによるセッション終了	可
IP セッションのロギングまたはセッションのリプレイ	可
アラーム表示	可
E メールによるアラート	可
E ポケベルによるアラート	可
スクリプト実行のカスタマイズ	可
複数のアラーム送信先	可
サードパーティ製ツールの統合	可
IDS アクティブ アップデート告知	可
Web ユーザ インターフェイス (HTTPS)	可
CLI (コンソール)	可
CLI (Telnet または SSH)	可
CiscoWorks VPN セキュリティ管理 (VMS) ソリューションのサポート	可
冗長電源装置	可 (Cisco 3745 のみ)
リンク障害の検出	可
通信障害の検出	可
サービス障害の検出	可

表 5 Cisco IDS ネットワーク モジュールの仕様 (続き)

項目	NM-CIDS-K9
デバイス障害の検出	可

注 :

Cisco IDS ネットワーク モジュールの 10 ~ 45 Mbps というパフォーマンスは、次の条件を前提とした値です。

- 1 秒ごとに 500 の新しい TCP 接続
- 1 秒ごとに 500 の HTTP トランザクション
- 平均パケット サイズは 445 バイト
- Cisco IDS 4.1 Sensor ソフトウェアを実行
- Cisco 2600XM で最大 10 Mbps
- Cisco 3745 で最大 45 Mbps

©2004 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

URL: <http://www.cisco.com/jp/>  
問合せ URL: <http://www.cisco.com/jp/service/contactcenter/>

〒 107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館  
TEL: 03-6655-4433

電話でのお問合せは、以下の時間帯で受付けております。  
平日 10:00 ~ 12:00 および 13:00 ~ 17:00

お問合せ先