

Cisco 806 ブロードバンドゲートウェイルータ

スモールオフィスと在宅ワーカーにCisco IOSテクノロジーのパワーによるセキュア共有ブロードバンドアクセスを提供

Cisco 806 ブロードバンドゲートウェイルータは、スモールオフィスと在宅ワーカーのために、ブロードバンドアクセスおよびビジネスクラスの機能を提供します。Cisco 806 は Cisco IOS® テクノロジーのパワーにより、ビジネスクラスのセキュリティ、リモート管理機能、そして QoS (Quality of Service) 機能が提供されます。こうした付加価値機能は、実績ある信頼性を備えた Cisco IOS テクノロジーによってもたらされ、今日のビジネスに必要とされるミッションクリティカルなネットワーキングを実現します。

固定構成でビジネスクラスのデュアルイーサネットルータであるCisco 806ブロードバンドゲートウェイルータは、実績あるCisco 800シリーズの最新ラインナップです。このプラットフォームの機能はソフトウェアによるアップグレードが可能で、境界セキュリティを提供するステートフルインスペクションファイアウォー

ルやVPN (仮想プライベートネットワーク) を実現するデータ暗号化などのビジネスクラスのセキュリティ機能を提供し、単一のブロードバンド接続上でマルチユーザーアクセスをサポートします。

Cisco 806ルータは、以下のようなミッションクリティカルなビジネスニーズに応え、スモールビジネスや企業の在宅ワーカーに理想的なソリューションとなります。

- マルチユーザーアクセス
- ビジネスクラスのセキュリティ
- Cisco IOSソフトウェアの管理性と信頼性
- QoS (Quality of Service) によるビデオ、音声、およびトラフィック管理

Cisco 806はイーサネットポートによってブロードバンドモデムに接続するため、ブロードバンドサービスがDSL、ケーブル、イーサネット、またはLRE (Long Reach Ethernet) テクノロジーのいずれを使用している場合でも、セキュアで管理しやすい標準デバイスとして各サイトに配備して、従業員を企業ネットワークに接続させることができます。セキュアなデバイスを標準化しておくことで、初期の展開と日常の管理を簡素化し、時間とコストを削減することができます。

図1: Cisco 806ブロードバンドゲートウェイルータは、ビジネスクラスのデュアルイーサネットルータです。小規模オフィスや企業の在宅勤務者向けに開発された製品で、Cisco IOSファイアウォールやVPNソフトウェアによってセキュアで信頼性の高いインターネットあるいは企業ネットワークへのアクセスを可能にします。





マルチユーザーブロードバンドアクセス

ブロードバンドモデムではひとりのユーザーしか利用することができません。しかしCisco 806を利用すれば、ブロードバンド接続を利用してマルチユーザーアクセスを実現できます。NAT (Network Address Translation) は、インターネットサービスプロバイダーが提供する単一のパブリックIPアドレスを使用して、LAN上のユーザーに複数のプライベートIPアドレスを提供します。Cisco 806をブロードバンドモデムに接続することで、オフィスのLANにアクセスする全ユーザーが単一のブロードバンド接続を共有することが可能になります。

ビジネスクラスのセキュリティ

インターネットベースの通信とe-コマースによるビジネスチャンスを活用するには、プライベートな情報のセキュリティを保護する必要があります。Cisco IOSセキュリティサービスは、それぞれに必要なセキュリティソリューションを構築するための多数のテクノロジーを提供します。このなかには、標準および拡張アクセス制御リスト (ACL)、ロック&キー (動的ACL)、ルータおよびルート認証、GRE (Generic Routing Encapsulation) トンネリング、およびNATなどがあります。境界セキュリティ機能は、プライベートネットワーク、イントラネット、エクストラネット、およびインターネット間のトラフィックを制御します。

Cisco 806はCisco IOSソフトウェアの基本的なセキュリティ機能のほかに、ステートフルインスペクションファイアウォールやデータ暗号化といった先進的なセキュリティ機能もサポートしています。ステートフルインスペクションファイアウォールは、シンプルなパケットフィルタリングよりもインテリジェントな境界セキュリティを提供します。そして、セッションの状況に基づいてWANトラフィックを拒否または許可するため、ファイアウォール背後のユーザーのリクエストを受信しながら不正なアクセスを阻止することができます。

VPNは、インターネットのようなパブリックインフラストラクチャを利用しながらセキュアな通信を可能にします。ファイアウォールは特定のサイトに境界ネットワークセキュリティを提供しますが、VPNはブランチオフィスから本社へ送信されるデータなど、あるサイトから別のサイトに送信されるデータを保護します。VPNはデータ暗号化とセキュアトンネルを使用して、パブリック接続上を伝送されるデータの完全性を保護します。Cisco 806は、最もセキュアなデータ暗号化方式であるIPSec 3DES暗号化をサポートしており、ハッカーが企業情報にアクセスするのを阻止します。

すでにPC VPNクライアントを使ったVPNを構築している場合には、Cisco 806を導入することで、ステートフルファイアウォールおよびリモート管理機能を提供できるようになります。従業員や代理店をかかえる小規模オフィスでは、Cisco 806が、ステートフルファイアウォールやリモートアクセスの監視/管理といった境界セキュリティのための中央制御ポイントとなります。こうしたサイトにステートフルファイアウォール機能を備えたCisco 806ルータを追加することで、企業は境界セキュリティを強化できます。

Cisco 806ルータは、IPSecパストスルーもサポートします。この機能は、ルータをパストスルーしてIPSecトンネルをPCにまで到達させます。これによって、ユーザーがVPNソフトウェアクライアントを利用できると同時に、ファイアウォールやマルチユーザーアクセスを可能にするというルータの機能が活用できます。

企業はビジネスクラスのセキュリティ機能によって通信のセキュリティを保護し、通常に普及しているブロードバンドサービスを利用することが可能になります。また、サービスプロバイダーやリセラーはこうした機能を使用して、付加価値ある管理型ファイアウォール、VPN、およびリモート管理サービスを提供することが可能になります。

Cisco IOSソフトウェアの管理性と信頼性

Cisco 806はCisco IOSテクノロジーをベースとしているため、サービスプロバイダーやリセラーは、Cisco IOSソフトウェアに対するこれまでのトレーニングや投資を活用することができ、事業運営費全体を削減しながら顧客を増やしていくことができます。サービスプロバイダーやリセラーは、以下のような優れた管理/トラブルシューティング機能を利用でき、顧客サイトに導入したCisco 806ルータをリモートで管理することができます。

- インタラクティブな診断/デバッグ機能を含むCisco IOSの管理性
- Cisco IOS CLI (コマンドラインインタフェース)
- 実績ある信頼性

Cisco 806ルータはSNMP (Simple Network Management Protocol) とTelnetによる中央での集中管理/運用機能、およびルータのコンソールポートによるローカル管理機能をサポートします。サービスプロバイダーはCisco IOSソフトウェアが提供する多数のデバッグ機能を使って、ネットワークの問題をリモートで診断することができます。また、Cisco VPN Solutions CenterやCisco Security Policy ManagerといったCiscoネットワーク管理ソフトウェアをCisco 806ルータのサポートに使用することもできます。

多くのエンタープライズ、リセラー、およびサービスプロバイダーは、すでにCisco IOSソフトウェアを使って大規模ネットワークを運営しており、スモールオフィスおよび在宅ワーカーのアプリケーションにCisco IOS CLI (コマンドラインインタフェース) の知識を活用することができます。

Cisco 800シリーズルータは、インターネットを構成するルータで標準的に使用されている実績あるCisco IOSテクノロジーをベースとしています。Cisco IOSソフトウェアはミッションクリティカルな企業ネットワークのための業界標準アプリケーションであるため、スモールビジネスのユーザーや在宅ワーカーもCisco 806ルータを信頼して使うことができます。

簡単なセットアップとインストール

Cisco 806ルータには、インストールとセットアップを簡素化するWebベースの設定ツールCisco Router Web Setupツールが装備されています。ユーザーはWebブラウザを使ってルータのIPアドレスにアクセスすれば、いくつかの簡単な手順に従うだけで製品を設定して使い始めることができ



ます。このツールにより、テクニカルスタッフが出向がなくても、エンドユーザーが簡単にインストールできます。ユーザーはこのセットアップツールを使って、パケットフィルタリングなどのIPフィーチャセットの基本的なセキュリティに加え、オプションのCisco IOSソフトウェア Firewallフィーチャセットも設定することができます。

Cisco IOS ソフトウェアによる管理型ネットワークサービス

サービスプロバイダーとシステムインテグレーターは、Cisco 806ルータを使ってネットワークアップタイムのSLA (サービスレベルアグリーメント) やネットワークトラブルシューティングの迅速な応答といった管理型ネットワークサービスとインターネットアクセスをスモールビジネスや在宅ワーカーに提供することができます。Cisco IOS ソフトウェアは、ネットワーク接続の監視機能だけでなく、パフォーマンスや構成上の問題をすばやく判断するためのトラブルシューティングおよびデバッグツールも提供します。

表1:製品の主な機能と利点

主な機能	利点
マルチユーザーアクセス	
NAT/PAT	<ul style="list-style-type: none"> 複数のプライベート IP アドレスを単一のパブリック IP アドレスに割り当て可能作成 複数ユーザーが単一のブロードバンド接続を共有可能
PPPoE	<ul style="list-style-type: none"> PPP over Ethernetカプセル化により、既存ネットワークとの互換性を保証
ビジネスクラスのセキュリティ	
Cisco IOSソフトウェアによる基本セキュリティ (ACL, NAT/PAT, Lock & Key, 動的ACL, ルータ/ルート認証)	<ul style="list-style-type: none"> 境界ネットワークセキュリティによって不正なネットワークアクセスを阻止
ステートフルインスペクションファイアウォール (Cisco IOS Firewallフィーチャセット)	<ul style="list-style-type: none"> 境界上の全トラフィックに対するセキュアなアプリケーションごとの動的アクセス制御機能 (ステートフルインスペクション) を内部ユーザーに提供 サービス拒否 (DoS) 攻撃からルータリソースを保護 パケットヘッダをチェックして、不審なパケットをドロップ 身元不明の悪意あるJavaアプレットからの保護 アプリケーションごと、機能ごとにトランザクションの詳細をレポート
IPSec 3DES/DES暗号化	<ul style="list-style-type: none"> 標準化された暗号化方式を使用して、機密データの完全性と発信元の真正性を保証 個々のPCを設定することなくLAN上の全ユーザーにWAN暗号化を提供
マルチユーザ IPSec パススルー	<ul style="list-style-type: none"> VPN PC ソフトウェア クライアントからの要求に応じて、ルータが IPSec トンネルをパススルー PC 主導での PPTPトンネル、暗号化、あるいは復号化をサポート
拡張管理機能	
Cisco IOS管理機能	<ul style="list-style-type: none"> SNMP, Telnet, または HTTP によるリモート管理 / 監視機能、およびコンソールポートによるローカル管理機能を提供
Cisco IOSインタラクティブデバッグ機能	<ul style="list-style-type: none"> サービスプロバイダーやシステム管理者はネットワークの問題をリモートまたはローカルで詳細に診断することが可能 (たとえば、Telnetによってルータを診断)
Cisco IOS CLI	<ul style="list-style-type: none"> これまでのCisco IOS CLIの知識を活用でき、あらためてトレーニングをしなくても簡単にインストールおよび管理することが可能
Cisco IOSテクノロジー	<ul style="list-style-type: none"> インターネットバックボーンおよび多くの企業ネットワークで使用されているテクノロジーを提供
Cisco Router Web Setupツール	<ul style="list-style-type: none"> テクニカルスタッフ以外のユーザーもブラウザを使ってルータにアクセスし、ユーザー情報を入力するだけでインストールを完了することが可能
Easy VPN*	<ul style="list-style-type: none"> 自動 IPSec トンネル開設およびポリシー承認のプッシュにより、VPN 接続の展開および管理が容易
* 2002年第1四半期に提供予定	

QoSによるビデオ、音声、およびトラフィック管理

Cisco 806ルータはIP QoS (Quality of Service) 機能により、音声/ビデオトラフィックをWebサーフィンなどの優先度の低いアプリケーションよりも優先させることができます。この機能を使って帯域幅の割り当てを効率的に行うことで、IP電話などの音声/ビデオ通信が可能になります。またLLQ (Low-Latency Queuing) を使用すれば、サービスプロバイダーやリセラーはアプリケーションあるいはユーザーのデータ別に帯域幅を保証/差別化することができます。たとえば、マーケティング部門のデータよりカスタマーサービス部門のデータを優先させるといったことができます。サービスプロバイダーやリセラーは特定アプリケーションやユーザーの帯域幅を制限するCisco 806の機能によって、アプリケーションやユーザーの要求に応じてトラフィックを管理することが可能になります。

* QoS機能は2002年第1四半期に対応予定です。



主な機能	利点
Cisco VPN Solution CenterおよびCisco Secure Policy Managerによるサポート	• セキュリティポリシーのスケラブルな展開を実現するセキュリティ管理ツール
SSH(Secure Shell) プロトコル	• インパウンドの telnet セッションと同様のセキュアな暗号化接続をルータに対して提供
トラフィック管理	
IPマルチキャストテクノロジー	• 冗長トラフィックを削減して帯域幅を節約。企業内通信、遠隔学習、ソフトウェアの配布、在庫照会、ニュースアプリケーションを実現
IP QoS --- LLQ(Low-Latency Queuing)、WRED(Weighted Random Early Detection)、CAR(Committed Access Rate) * 2002年第1四半期に提供予定	<ul style="list-style-type: none"> • 帯域幅をインテリジェントに割り当てることで、複数アプリケーションに一貫した応答時間を保証 • アプリケーションの分類を可能にして、最も重要なアプリケーションが WAN 回線を優先して使用できるように保証 • 優先度に応じて特定TCPセッションに減速させて輻輳を回避

表2:ハードウェア仕様
ハードウェア仕様Cisco 806

プロセッサ	MPC 855T RISC
プロセッサ速度	50 MHz
デフォルトDRAMメモリ	16 MB
最大DRAMメモリ	32 MB
デフォルトフラッシュメモリ	8MB
最大フラッシュメモリ	8MB
イーサネット(1ポートWAN、4ポートLAN)	10 Mbps
コンソール	RJ-45
LED	10
クロスオーバーハブスイッチ	あり
電源	ユニバーサル100~240 VAC

表3:Cisco 806のメモリ要件とCisco IOSソフトウェアフィチャーセット

Cisco 806 IOS ソフトウェアイメージ	フラッシュ	DRAM
デフォルトメモリ構成	8MB	16 MB
IP	8MB	16 MB
IP Plus	8MB	16 MB
IP Firewall	8MB	16 MB
IP/Firewall Plus IPSec 3DES	8MB	20 MB

表4:Cisco 806ソフトウェアフィチャーセット

Cisco 806 ソフトウェアフィチャーセットがサポートする IP プロトコルとフィチャー (基本プロトコル/フィチャー)	IP Plus	IP Firewall	IP/Firewall Plus IPSec 3DES
ルーティング/ブリッジング			
PPPoE			
トランスパレントブリッジング			
IP			
ルーティングプロトコル			
IP Enhanced IGRP			
RIP、RIPv2			
セキュリティ			
ルートおよびルータ認証			
PAP、CHAP、ローカルパスワード			
GREトンネリング			
IP基本および拡張アクセスリスト			
ステートフルインスペクションファイアウォール			
IPSec 56ビット暗号化			
IPSec 3DES暗号化			
マルチユーザ IPSecパススルー(TCP&アンカプセル化)			
マルチユーザ PPTP パススルー			
RADIUS			
TACACS +			
QoS			
LLQ(2002年第1四半期に提供予定)			
IPポリシールーティング			
NetMeetingサポートV.2.10/1, 3.01			
CAR (Committed Access Rate)			
クラスベース トラフィック シェーピング (2002年第1四半期に提供予定)			

Cisco 806 ソフトウェアフィチャセットがサポートする IP プロトコルとフィチャ (基本プロトコル/フィチャ)	IP Plus	IP Firewall	IP/Firewall Plus IPSec 3DES
帯域幅最適化&管理			
IPマルチキャスト			
ファースト スイッチング			(IPSec時は不可)
STAC圧縮			
容易な使用と展開			
Cisco Router Web Setupツール 管理			
SNMP, Telnet, コンソールポート Syslog			
NTPクライアントおよびサーバ			
TFTPクライアントおよびサーバ			
DHCPクライアントおよびサーバ			
DHCPリレー			
アドレス節約			
NAT(PAT)			
NAT(マルチNAT)			
IPCPアドレスネゴシエーション			
DHCPクライアントアドレスネゴシエーション			

適合基準 / 規格

この製品は以下の要件に準拠しています。

EMC

- EN 55022, 1998 class B
- CISPR22, 1997 class B
- CFR47, Part 15, Subpart B, 1995, class B
- EN61000-3-3
- CISPR24, 1997
- EN 55024:1998

安全性

- CSA/NRTL & C認可:UL 1950, 3rd ed./CSA 22.2 No. 950-95, 3rd ed.(USA, カナダ)
- ACA/A2LA認可:TS001-1997, AS/NZS 3260(オーストラリア/ニュージーランド)
- CB Cert./Report CSA ~ IEC 60950
- CCIB認可:GB4943-9(中国)

物理仕様

寸法と重量

- 寸法 (H x W x D): 5.1 x 24.6 x 21.6 cm
(2.0 x 9.7 x 8.5インチ)
- 重量: 0.67/0.68 kg (1.48/1.5ポンド)

動作環境

- 非動作時温度: - 20 ~ 65 (- 4 ~ 149 ° F)
- 非動作時湿度: 5 ~ 95%、相対湿度(結露しないこと)
- 動作温度: 0 ~ 40 (32 ~ 104 ° F)
- 動作湿度: 10 ~ 85%、相対湿度(結露しないこと)

ルータ電源

- AC入力電圧: 100 ~ 250 VAC, 50 ~ 60 Hz
- 消費電力: 6 ~ 10W(アイドル時 ~ 最大消費電力)
- 電源装置定格: 15W

©2002 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。その他、記載されている会社名、製品名は各社の商標、登録商標または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: 03-6670-2992

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

お問い合わせ先