

Cisco Router And Security Device Manager (SDM)

このデータシートでは、Cisco® Router and Security Device Manager (SDM) の機能と利点について説明します。

製品概要

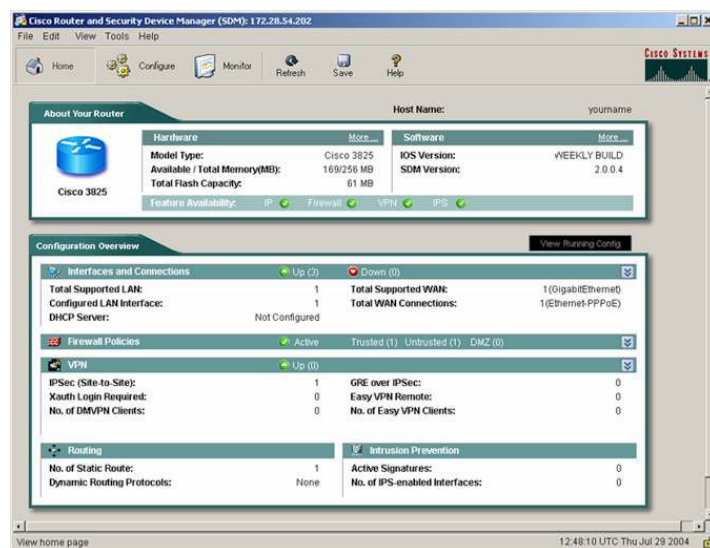
Cisco SDM は、Cisco IOS® ソフトウェアを搭載したルータのための Web ベースのデバイス管理ツールです。Cisco SDM では、スマート ウィザードによってルータおよびセキュリティを容易に設定でき、CLI (コマンドライン インターフェイス) の知識のないユーザでも、シスコのルータを短時間で簡単に配置、設定、および監視することができます。Cisco SDM は、さまざまな Cisco ルータおよび Cisco IOS ソフトウェア リリースでサポートされています。Cisco SDM でサポートされる特定のモデル番号については、表 3 を参照してください。

使いやすさとインテリジェントなアプリケーション

Cisco SDM を使用すると、ルーティング、スイッチング、セキュリティ、および Quality of Service (QoS; サービス品質) の各サービスを Cisco ルータに簡単に設定できます。また、パフォーマンスモニタリングによって予防的な管理も可能になります (図 1)。Cisco SDM ユーザは、Cisco IOS ソフトウェア CLI を使用しなくても、Cisco ルータをリモートで設定および監視できます。Cisco SDM には日本語 GUI (グラフィカル ユーザ インターフェイス) が装備されているので、Cisco IOS ソフトウェアの初心者ユーザでも、日常業務をこなすことができます。また、使いやすいスマート ウィザード、自動化されたルータ セキュリティ管理、および広範な日本語オンライン ヘルプとチュートリアルも用意されています。

* 日本語表示は Ver.2.1.2 より対応

図 1 Cisco SDM ホームページ



ユーザは、Cisco SDM のスマート ウィザードを使用して、ルータ設定およびセキュリティ設定のワークフローに従い、LAN、Wireless LAN (WLAN; 無線 LAN)、および WAN インターフェイス、ファイアウォール、Intrusion Prevention System (IPS; 侵入防御システム)、IP Security (IPSec) VPN を体系的に設定できます。Cisco SDM のスマート ウィザードには、適切ではないセキュリティ設定をインテリジェントに検出し、修正方法を提示する機能があります。たとえば、WAN インターフェイスのアドレスに Dynamic Host Configuration Protocol (DHCP; ダイナミック ホスト コンフィギュレーション プロトコル) によるアドレス指定が設定されていれば、DHCP トラフィックがファイアウォールを通過できるように設定します。Cisco SDM に組み込まれたオンライン ヘルプには、設定のための基礎知識や、ユーザが Cisco SDM に正しいデータを入力するための段階的な手順が記載されています。また、ユーザがよく目にするネットワーク関連およびセキュリティ関連の用語と定義を載せたオンライン用語集もあります。

Cisco SDM では、Cisco IOS ソフトウェアとそのセキュリティ機能に習熟したネットワークの専門家向けに、ルータのセキュリティ機能を迅速に設定および微調整するための詳細設定ツールが用意されています。この機能を使用すると、ルータに設定変更を適用する前に、Cisco SDM によって生成されたコマンドを確認できます。

管理者は Cisco SDM を使用することで、Secure Sockets Layer (SSL) 接続と Secure Shell (SSHv2) プロトコル接続経由でリモートからルータを設定して監視できるようになります (図 2)。SSL および SSHv2 プロトコルは、ユーザのブラウザとルータ間でのインターネット経由の安全な接続を可能にするテクノロジーです。Cisco SDM 対応のルータをブランチ オフィスに導入すれば、そのルータを本社から設定および監視できるため、熟練のネットワーク管理者がブランチ オフィスに出向く必要がなくなります。

図 2 Cisco SDM 対応ルータへの SSL による安全なリモート接続

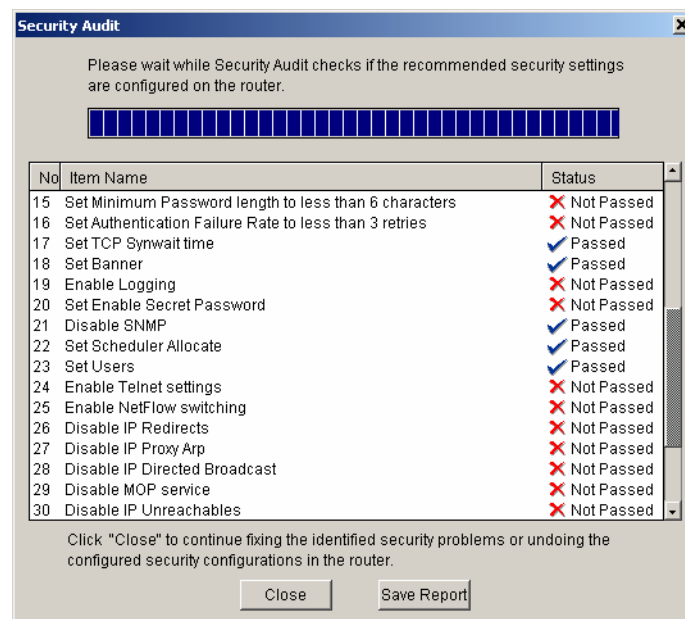


Remote User Configuring
Router Using Cisco SDM

統合されたセキュリティ設定

新しいルータを導入するときに Cisco SDM を使用すると、International Computer Security Association (ICSA) および Cisco Technical Assistance Center (TAC) によって推奨されたベストプラクティスに従って、Cisco IOS ファイアウォールを迅速に設定できます。Cisco SDM により、最も強力な VPN デフォルト設定が構成され、セキュリティ監査も自動的に実行されます (図 3)。また、ファイアウォールのルータ ロックダウン機能や、安全なサイト間接続 VPN の設定も一度の操作で実行できます。SDM にバンドルされた IPS シグニチャのシスコ推奨リストに基づき、ワーム、ウイルス、およびプロトコルの不正利用措置も迅速に展開できます。

図3 ルータのセキュリティ監査



設定済みのルータで Cisco SDM を起動すると、セキュリティ監査を 1 度の操作で実行し、一般的なセキュリティの脆弱性と比較しながらルータ設定の利点と弱点を評価することができます。管理者は、それぞれのビジネス ニーズに合わせて、既存のルータ セキュリティ設定を微調整します。Cisco SDM は、モニタリング、障害管理、およびトラブルシューティングなどの日常業務にも利用できます。

ルータ設定

Cisco SDM を使用すると、セキュリティ設定以外のルータ サービスの設定 (LAN、WLAN、および WAN のインターフェイス設定、ダイナミック ルーティング、DHCP サーバ、QoS ポリシーなど) を迅速かつ簡単に実行できます。

LAN 設定ウィザードを使用すると、ユーザはイーサネット インターフェイスに IP アドレスとサブネットマスクを割り当て、DHCP サーバを有効または無効にすることができます。WAN 設定ウィザードでは、WAN およびインターネットにアクセスできるように、xDSL、T1/E1、イーサネット、および ISDN インターフェイスの設定が行えます。シリアル接続の場合は、フレームリレー、PPP (ポイントツーポイント プロトコル)、High-Level Data Link Control (HDLC; ハイレベル データリンク制御) のカプセル化を実装することができます。また、スタティック ルーティングや、Open Shortest Path First (OSPF)、Routing Information Protocol (RIP) Version 2、Enhanced Interior Gateway Routing Protocol (EIGRP) などの一般的なダイナミック ルーティング プロトコルの設定も可能です。

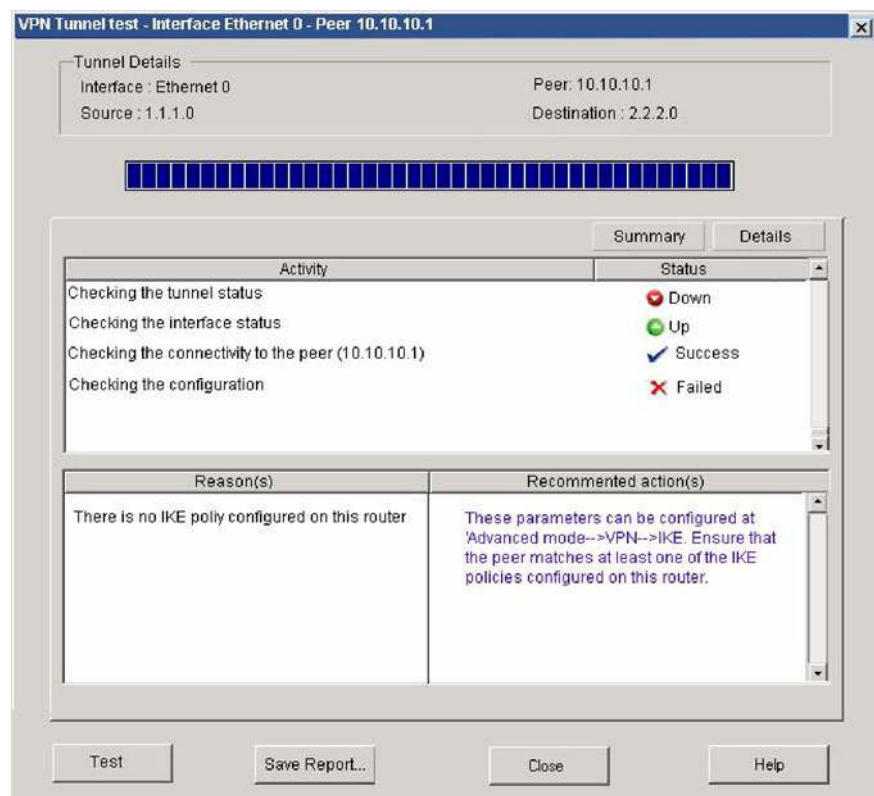
QoS ポリシーも、Cisco SDM の使用により、任意の WAN または VPN トンネル インターフェイスに簡単に適用できます。QoS ポリシー ウィザードは、QoS ポリシーに関するシスコのアーキテクチャ ガイドラインを自動的に実行し、リアルタイム アプリケーション (音声またはビデオ)、ビジネスクリティカルなアプリケーション (Structured Query Language [SQL]、Oracle、Citrix、ルーティング プロトコルなど)、およびその他のネットワーク トラフィック (Web、電子メールなど) に対して、効率的にトラフィックの優先順位を決定します。Cisco SDM の Network-Based Application Recognition (NBAR) ベースのモニタリングにより、ユーザは、アプリケーション層トラフィックの状

況をリアルタイムで視覚的に把握し、さまざまなクラスのアプリケーション トラフィックに対する QoS ポリシーの効果を確認できます。

モニタリングとトラブルシューティング

Cisco SDM のモニタ モードでは、インターフェイスの状態(アップまたはダウン)、CPU、メモリの使用状況などのルータの主要リソースとパフォーマンス測定値がすばやくグラフィカルに表示されます。ワイヤレス モデルでは、Cisco SDM では、802.11 a/b/g インターフェイスのリアルタイム統計情報がサポートされています。また、Cisco SDM は、ルータに統合されたルーティング機能とセキュリティ機能を利用して、WAN および VPN 接続を綿密に診断し、トラブルシューティングを行います。たとえば、障害のある VPN 接続のトラブルシューティングを行いながら、ルータの設定、および WAN インターフェイス レイヤと IPSec クリプト マップ レイヤ間の接続を検証することが可能です。また、各レイヤの設定とリモート ピア接続のテストを行いながら、診断結果(合格またはエラー)、考えられる障害の原因、Cisco TAC 推奨の対処方法を表示します。

図 4 VPN のトラブルシューティングとリカバリ



Cisco SDM モニタ モードには、Cisco IOS ファイアウォールによって拒否されたネットワーク アクセスの試行数を表示したり、ファイアウォール ログに簡単にアクセスしたりする機能もあります。さらに、IPSec トンネルで暗号化または暗号解除されたパケット数など、VPN の詳細な状態や、Easy VPN クライアント セッションの詳細も監視できます。

表 1 Cisco SDMv2.1.1 の機能

機能	利点
新しいハードウェアのサポート <ul style="list-style-type: none"> Cisco 850 シリーズ、Cisco 870 シリーズ、Cisco 1812J HWIC-AP-G-X、HWIC-AP-AG-X 	新しいハードウェアを認識、設定、および監視する機能を提供 注：現バージョンの SDM では、CISCO1812W-AG-P/K9 をサポートしていません。将来のバージョンでサポートする計画ですが、時期は未定です。
多言語でのローカライズ <ul style="list-style-type: none"> Cisco SDM ユーザ インターフェイスとオンライン ヘルプは、簡体字中国語、フランス語、ドイツ語、スペイン語、およびイタリア語に翻訳(2005 年 6 月から利用可能)。日本語は 2005 年下半期 Ver.2.1.1 より対応予定 上記の言語の MS Windows OS をサポート(現在利用可能) 	多言語ユーザのルータ管理を簡素化
統合された無線管理 <ul style="list-style-type: none"> Express Setup ウィザードを使用した無線インターフェイスの初回設定を簡素化 Web ベースの設定およびモニタリングの操作性を向上 	<ul style="list-style-type: none"> 無線インターフェイス構築に要する時間および人員が減少 サイトごとの要件に応じ、ワイヤレス環境の設定やセキュリティを柔軟にカスタマイズ可能
IPS プロビジョニングの改良	ルータ モデルごとに個別の IPS シグニチャを迅速に適用可能

コストの削減

Cisco SDM は、デバイスの配置コストおよびネットワーク管理コストをかけることができず、専任の経験豊富な技術者がいないブランチ オフィスや中小企業に最適です。Cisco SDM を使用すると、シスコの販売代理店や企業は、ルータのセキュリティやネットワークの設定を容易に実行できます。Cisco SDM によって生成される Cisco IOS ソフトウェア コンフィギュレーションは、Cisco TAC 推奨設定です。Cisco SDM に組み込まれている設定チェック機能、上級者向けの設定エディタ、便利なデフォルト設定を使用することにより、ネットワークおよびセキュリティ管理者の生産性が向上します。このような Cisco SDM の各種機能により、設定エラーの頻度が減少し、ネットワークのオペラビリティが改善されます。

大規模ネットワークを維持している企業は、Cisco SDM と Cisco CNS コンフィギュレーション エンジン統合することで、非常にスケーラブルなルータの配置を実現できます。Cisco SDM が生成した Cisco IOS ソフトウェア設定を Cisco CNS コンフィギュレーション エンジンにインポートして、数千台の Cisco ルータに同じ設定を展開することができます。

マネージド CPE サービス

サービス プロバイダーにとって Cisco SDM は、Cisco ルータ サービス(ファイアウォール、IPSec VPN、侵入防御、WAN アクセス、QoS など)をグラフィカルに表示する、費用対効果に優れたソリューションとなります。これにより、付加価値の高い Customer Premises Equipment(CPE; 顧客宅内機器)サービスを短時間でプロビジョニングできます。エンド カスタマーにビューを提供するために、複雑な Operations Support System(OSS; オペレーションズ サポート システム)ソフトウェアに投資する必要はありません。

さらに、このソリューションは、サービス プロバイダーのエンド カスタマー向けに、CPE 関連の問題を迅速に解決するためのローカル ツールを提供します。これは、ネットワーク ヘルプ デスクのサポート業務の負担軽減につながります。

シスコのリセラーは、Cisco SDM を利用して、付加価値の高いセキュリティ、トラフィック シェーピング、またはマネージド CPE サービスを、Cisco アクセス ルータの既存のお客様、そして新たに導入されるお客様に提供できます。

Cisco SDM とその他の管理アプリケーション

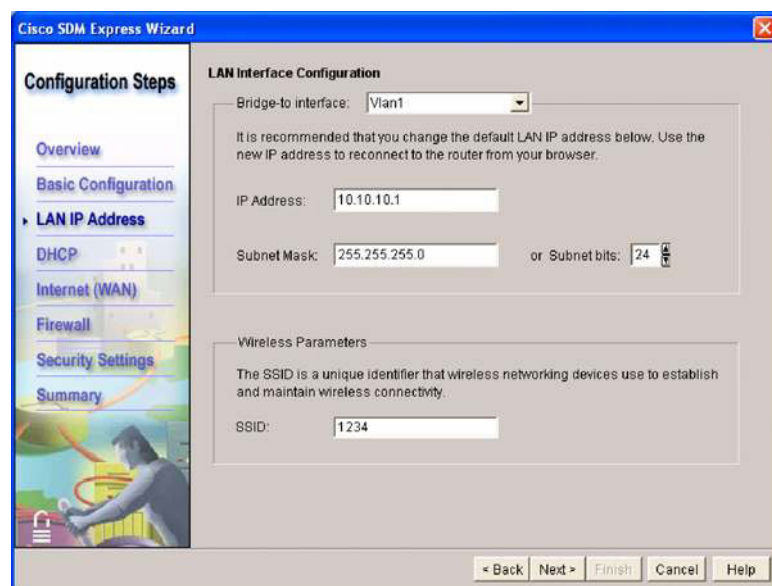
シスコでは、Cisco SDM と組み合わせて使用できるデバイス管理アプリケーションやネットワーク管理アプリケーションを提供しています。CiscoView は Web ベースの管理アプリケーションで、CiscoWorks 専用サーバにインストールして、シスコ製デバイスの物理構成図を表示したり、監視に使用したりします。Cisco SDM と CiscoView のクライアント インターフェイスは同じワークステーションにインストールして使用できます。Cisco SDM は主に、ルータ設定とセキュリティ機能の設定に使用され、CiscoView はルータの物理的な状態のリアルタイム表示や、SNMP (簡易ネットワーク管理プロトコル) ベースのデバイス モニタリングに使用されます。

アプリケーション

Cisco ルータの初期展開

Cisco SDM を使用すると、シスコ製品の販売代理店やお客様は、Cisco SDM Express とその他のタスクベースのスマート ウィザードで、Cisco ルータをすばやく安全に展開できます。たった 1 つの操作でルータをロックダウンできる機能があるので、Cisco ルータを一般のインターネットや WAN に接続する前に、Cisco IOS ソフトウェア内の不要なサービスを確実に停止させることができます。

図 5 Cisco SDM Express



Cisco ルータの大規模展開

Cisco SDM には Cisco CNS 2100 シリーズ インテリジェント エンジンが組み込まれており、Cisco CNS 2100 シリーズとの連携により出荷時初期設定の Cisco ルータを短時間で大規模展開できます。サービス プロバイダーや大企業は、ステー징段階で Cisco SDM と Cisco CNS 2100 シリーズを統合して使用することができ、経験の浅いオンサイト管理者しかいなくても、Cisco IOS CLI を使用せずに Cisco IOS ソフトウェアの最終的な設定をダウンロードすることができます。

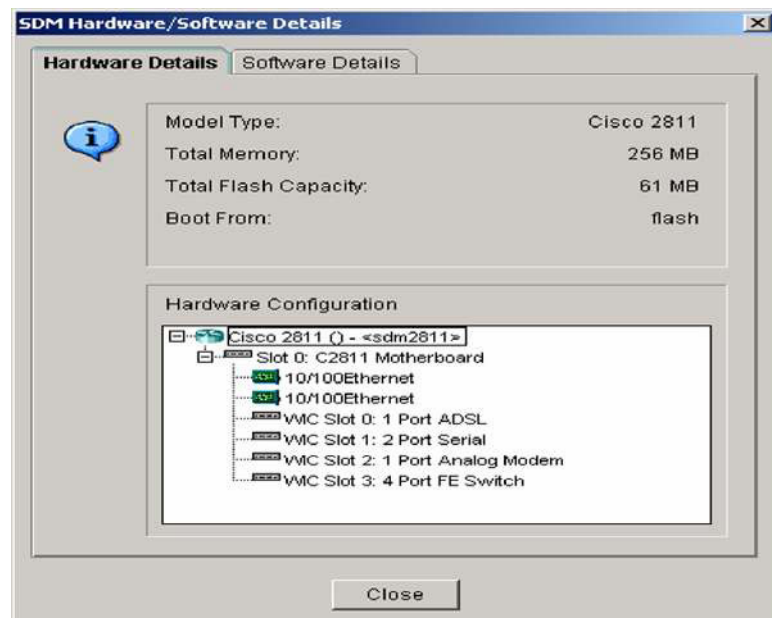
Cisco ルータのセキュリティ管理

Cisco SDM を使用すると、シスコ製品の販売代理店やお客様は、Network Address Translation (NAT; ネットワーク アドレス変換)、ACL、ファイアウォール、IPS、IPSec VPN などの Cisco IOS ソフトウェアのセキュリティ機能を容易に展開し、既存のルータ設定やネットワーク アーキテクチャに統合することができます。Cisco SDM のスマート ウィザードは、ルーティング機能とセキュリティ機能の相互関係を認識し、Cisco TAC によって検証済みの推奨設定を提示します。上級ユーザであれば、Cisco SDM の CLI プレビュー モードを使って、ルータに配布する前の最終的な設定を確認することもできます。

Cisco ルータの動作管理

Cisco SDM を使用すると、シスコ製品の販売代理店やお客様は、SSL および SSH により、ルータのクリティカルな動作のすべてを安全かつリモートに管理できます。このような重要な側面には、ハードウェアとソフトウェアのインベントリ状況、インターフェイスの状態、ファイアウォールおよび ACL のログ、VPN トンネルの状態、最新の Syslog メッセージなどが挙げられます。

図 6 Cisco ルータのハードウェアとソフトウェアのインベントリ



まとめ

Cisco SDM は、ネットワークおよびセキュリティ管理者にとって便利な生産性向上ツールです。シスコ製品の販売代理店は、Cisco SDM を使用して、WAN アクセス機能とネットワーク セキュリティ機能を兼ね備えた Cisco ルータを短時間で展開できるようになります。

Cisco SDM が生成する設定は、シスコのエンジニアによってテスト済みであり、Cisco TAC にも推奨されています。したがって、お客様は、Cisco SDM を採用し、この設定を利用することで、Cisco ルータの総所有コストを削減できます。また、Cisco SDM に組み込まれている設定チェック機能により、設定エラーの頻度も減らせます。

製品仕様

表 2 Cisco SDM の主な機能と利点

機能	利点
組み込みの Web ベース管理ツール	<ul style="list-style-type: none"> 独自の管理ツールによって、ルータがセキュリティおよびリモートアクセスの統合ソリューションを提供 専用の管理ステーションが不要 デスクトップまたはラップトップからリモート管理が可能
SSL および SSHv2 ベースの安全なリモート アクセス	WAN 全体にわたって安全な管理を提供
ルータの状態の一覧表示	ルータのハードウェア、ソフトウェア、および VPN、ファイアウォール、QoS などの主要なルータ サービスの一覧をグラフィカルに表示する
ルータのセキュリティ監査	<ul style="list-style-type: none"> 既存ルータの脆弱性を判定 (Cisco TAC、ICSA によって推奨された) ベスト プラクティスに基づくルータのセキュリティポリシーをすばやく適用
簡単操作によるルータのロックダウン	セキュリティや Cisco IOS ソフトウェアに関する専門知識がなくても、ファイアウォールと Cisco IOS ソフトウェアを簡単に設定できる
頻度の高いルータ設定作業とセキュリティ設定作業を支援するスマート ウィザード	<ul style="list-style-type: none"> Cisco TAC 推奨の設定を生成 ルーティングとセキュリティに関する知識を組み込むことで設定エラーを防止 Cisco IOS ソフトウェアの新しいセキュリティ機能は、ネットワーク管理者の研修に時間をかけなくても、簡単に習得できる 既存のネットワーク インフラストラクチャを低コストで容易にセキュリティ保護できる
ポリシー ベースのファイアウォールおよび ACL 管理 (ファイアウォール ポリシー)	セキュリティ管理者は、グラフィカルで見やすいポリシー テーブルを使用して、Access Control List (ACL; アクセス制御リスト) とパケット インスペクション ルールを簡単に管理できる
IPS	<ul style="list-style-type: none"> 入カトラフィックと出カトラフィックに対し、シスコがチューニングを施した高度な攻撃シグニチャを、任意のルータ インターフェイスに設定できる 稼働中のルータの基本動作に影響することなく、新しい IPS シグニチャをいつでも更新できる 新たなワームやウイルスの変種に即座に対処するために、GUI を使って IPS シグニチャをカスタマイズできる シグニチャのフィルタリングと選択したシグニチャの一括設定変更 (処理ベースまたは危険度ベース) が可能 IPS エンジンからリアルタイムのステータスおよびエラー メッセージを表示
Cisco Easy VPN サーバ	<ul style="list-style-type: none"> ウィザードベースの設定を行うことができ、リモートアクセス VPN ユーザをリアルタイムでモニタリングできる ルータ上またはリモート Authentication, Authorization, Accounting (AAA; 認証、許可、アカウンティング) サーバとの統合
ロールベースのアクセス	<ul style="list-style-type: none"> ルータ管理者とユーザとでルータを論理的に分離 管理者のプロファイルごとに、Cisco SDM ユーザ インターフェイスおよび Telnet インターフェイスへの安全なアクセスを提供 高付加価値を提供するシスコのリセラーとサービス プロバイダーが、CPE サービスを表示するためのグラフィカルなビューをエンド カスタマーに提供できるようにする 出荷時にデフォルトで設定されているプロファイル: <ul style="list-style-type: none"> 管理者 ファイアウォール管理者 Easy VPN クライアント ユーザ 読み取り専用ユーザ
WAN および VPN のトラブルシューティング	<ul style="list-style-type: none"> ルーティング、LAN、WAN、セキュリティの各機能をルータ上に統合することで、詳細なトラブルシューティングが可能になり、平均修復時間 (MTTR) を短縮 ルーティング、LAN、WAN、セキュリティの各機能がルータに統合されているため、IPSec VPN や WAN リンクを詳細にトラブルシューティングできる Cisco TAC ナレッジ ベースのリカバリ アクションにレイヤ 2 以上のトラブルシューティングを統合
QoS ポリシー	<ul style="list-style-type: none"> WAN および VPN の帯域幅とアプリケーション パフォーマンスをさまざまなビジネスニーズ (音声とビデオ、エンタープライズ アプリケーション、Web など) に合わせて効率よく簡単に最適化 事前定義されている 3 つのカテゴリ: リアルタイム、ビジネス クリティカル、およびベストエフォート

機能	利点
NBAR	<ul style="list-style-type: none"> 事前に定義されたサービス ポリシーと比較しながら、WAN および VPN 帯域幅のアプリケーションによる使用状況をリアルタイムで確認できる トラフィック パフォーマンス モニタリングを提供
SSHv2	<ul style="list-style-type: none"> PC と Cisco ルータ間を安全に接続することで、リモート管理が可能 Cisco SDM とルータ間のすべての暗号化通信に SSHv2 を自動的に使用
リアルタイムなモニタリングとロギング	管理者は、ルータのリソースとセキュリティを予防的に管理して、ネットワーク上のミッションクリティカルなアプリケーションに影響を及ぼす前に対処可能
デジタル証明書	<ul style="list-style-type: none"> 事前共有鍵よりはるかにスケーラブルで安全なソリューションを提供 Cisco SDM、Cisco IOS 認証局サーバ、および Easy Secure Device Deployment (EzSDD) と組み合わせて簡単に使用、展開できる
リアルタイムなネットワークおよびルータのリソース モニタリング	<ul style="list-style-type: none"> ルータ リソースとネットワーク リソースの使用状況を迅速に分析 LAN および WAN のトラフィックと帯域幅の使用状況をグラフィカルに表示
タスクベースの Cisco SDM ユーザ インターフェイス	<ul style="list-style-type: none"> IPSec VPN、ファイアウォール、ACL、IPS などのセキュリティ設定をより迅速かつ簡単に設定 ホームページのダッシュボード ビューによりルータ サービス設定のクイック スナップショットを提供
Cisco SDM Express ウィザードベースのルータの導入	<ul style="list-style-type: none"> 基本的な WAN アクセス設定に合わせてルータを迅速かつ簡単に導入 上級以外のユーザに最適なルータ導入ツール
PC ベースの SDM ルータのフラッシュ メモリではなく Windows ベースの PC にインストールされる Cisco SDM	<ul style="list-style-type: none"> SDM 用の余分なフラッシュ メモリ容量が不要 Cisco ルータの導入ベースの管理に適したツール

表 3 Cisco SDM の製品仕様 (サポートされる Cisco IOS バージョンの最少要件)

機能	説明
サポートされるプラットフォーム	<ul style="list-style-type: none"> Cisco 831 イーサネット ブロードバンド ルータ: <ul style="list-style-type: none"> Cisco IOS ソフトウェア リリース 12.2(13)ZH または 12.3(2)T Cisco 851、Cisco 871 ルータ: <ul style="list-style-type: none"> Cisco IOS ソフトウェア リリース 12.3(8)YI Cisco 1812J ルータ <p>注: 現バージョンの SDM では、CISCO1812W-AG-P/K9 をサポートしていません。将来のバージョンでサポートする計画ですが、時期は未定です。</p> <ul style="list-style-type: none"> Cisco IOS ソフトウェア リリース 12.3(8)YI Cisco ISR 1841: <ul style="list-style-type: none"> Cisco IOS ソフトウェア リリース 12.3(8)T4 Cisco 2610XM、Cisco 2611XM、Cisco 2620XM、Cisco 2621XM、Cisco 2650XM、Cisco 2651XM、および Cisco 2691 マルチサービス ルータ: <ul style="list-style-type: none"> Cisco IOS ソフトウェア リリース 12.2(15)ZJ3、12.2(11)T6、または 12.3(1)M Cisco ISR 2801、Cisco ISR 2811、Cisco ISR 2821、および Cisco ISR 2851: <ul style="list-style-type: none"> Cisco IOS ソフトウェア リリース 12.3(8)T4 Cisco 3620、Cisco 3640、Cisco 3661 マルチサービス プラットフォーム、および Cisco 3662 Telco Versatile DCN アクセス プラットフォーム: <ul style="list-style-type: none"> Cisco IOS ソフトウェア リリース 12.2(15)ZJ3、12.2(11)T6、または 12.3(1)M Cisco 3725 および Cisco 3745 マルチサービス アクセス ルータ: <ul style="list-style-type: none"> Cisco IOS ソフトウェア リリース 12.2(15)ZJ3、12.2(11)T6、または 12.3(1)M Cisco ISR 3825 および Cisco ISR 3845: <ul style="list-style-type: none"> Cisco IOS ソフトウェア リリース 12.3(11)T Cisco 7204VXR、Cisco 7206VXR、および Cisco 7301ルータ: <ul style="list-style-type: none"> Cisco IOS ソフトウェアリリース 12.3(2)T または 12.3(3)M。B、E、S シリーズはサポートしていません
ソフトウェアの互換性	上記の Cisco SDM がサポートする Cisco IOS ソフトウェア リリース対応の Cisco IOS ソフトウェア フィーチャ セットのすべてと互換性があります
接続性	HTTP および HTTPS、Telnet、SSH、および SSHv2

機能	説明
基本的なルータ設定パラメータ	<ul style="list-style-type: none"> • 様々なアクセス プロファイルを持つユーザ • Domain Name System (DNS; ドメイン ネーム システム) • DHCP サーバおよびクライアント • SNMP • Telnet、SSH、SSHv2、および vty • 日付と時刻、Network Time Protocol (NTP) • Syslog • 出荷時設定へのリセット • ホスト名、ドメイン名、およびバナー
高度なルータ設定パラメータ	<ul style="list-style-type: none"> • ルーティング プロトコル (スタティック、RIP Version 1 および 2、OSPF、EIGRP) • NAT (スタティックおよびダイナミック) • ACL • QoS ポリシー、NBAR • Cisco EtherSwitch® ポート上の VLAN • IP プロキシ Address Resolution Protocol (ARP)、Internet Control Message Protocol (ICMP) リダイレクト、ICMP 到達不能、ICMP マスク リプレイ、および有向ブロードキャスト • AAA のローカル設定またはリモート設定
設定可能なルータインターフェイス	<ul style="list-style-type: none"> • イーサネット (10、10/100、および 10/100/1000 Mbps) • 802.11 a、802.11 b/g • xDSL (非同期 DSL [ADSL] および G.SHDSL) • T1/E1 (シリアル) • ISDN BRI (基本インターフェイス) (マルチレベルの優先順位と優先使用が可能) • アナログ モデム
サポートされる WAN カプセル化	<ul style="list-style-type: none"> • フレームリレー • PPP • PPP over Ethernet (PPPoE) • PPP over ATM (PPPoA) • RFC 1483 ルーティング • HDLC • ADSL 自動検出
設定可能な VPN パラメータ	<ul style="list-style-type: none"> • Internet Key Exchange (IKE)、デジタル証明書、データ暗号化規格 (DES)、Triple DES (3DES)、Advanced Encryption Standard (AES)、および圧縮 • IPSec サイトツーサイト • Cisco Easy VPN サーバ • Cisco Easy VPN リモート • Generic-Routing-Encapsulation (GRE; 総称ルーティング カプセル化) トンネル • Dynamic Multipoint VPN (DMVPN; ダイナミック マルチポイント VPN、ハブとスポークの両方)、冗長ハブを備えたダイナミック スポークツースポークを含む
サポートされるファイアウォールパラメータ	Context-Based Access Control (CBAC; コンテキストベースのアクセス制御)、DMZ、ファイアウォール ログ、ファイアウォールおよび ACL ポリシーのビュー、安全な管理アクセス
サポートされる IPS 機能	入力または出カトラフィックを検査するための IPS 規則、シグニチャの微調整、シグニチャのカスタマイズ、Security-Device-Event-Exchange (SDEE) エラー メッセージの表示
CiscoView との互換性	Cisco SDM と併用可能
Cisco CallManager Express (CME) との互換性	Cisco SDM と併用可能
パフォーマンス	Cisco SDM がルータ DRAM や CPU に及ぼす影響はごくわずか

システム要件

表 4 に、Cisco SDM のシステム要件を示します。

表 4 システム要件

機能	要件
ルータのフラッシュ メモリ	<ul style="list-style-type: none"> • Cisco SDM ファイル用に、ルータ上に最小 6 MBの空きフラッシュ メモリ • Cisco SDM Express 用に、ルータ上に最小 2 MBの空きフラッシュ メモリ。無線管理ファイルには、さらに 1.7 MB のメモリが必要。その他の SDM ファイルは PC のハード ディスクにインストール可能
PC ハードウェア	Pentium III シリーズ以上のプロセッサ
PC オペレーティングシステム	<ul style="list-style-type: none"> • Windows XP Professional • Windows 2003 Server (Standard Edition) • Windows 2000 Professional • Windows NT 4.0 Workstation (サービス パック 4) • Windows ME • 簡体字中国語、フランス語、ドイツ語、スペイン語、イタリア語、日本語の OS をサポート <ul style="list-style-type: none"> ◦ Windows XP Professional ◦ Windows 2000 Professional
ブラウザ ソフトウェア	<ul style="list-style-type: none"> • Microsoft Internet Explorer 5.5 以上 • Netscape Navigator 7.1 および 7.2 • Firefox 1.0.2
Java ソフトウェア	<ul style="list-style-type: none"> • Java Virtual Machine (JVM) 内蔵ブラウザが必須 • Java プラグイン (Java Runtime Environment Version 1.4.2_05 以上)

発注情報

Cisco SDM の出荷オプションには、次の種類があります。

- **ROUTER-SDM**: Cisco SDM ソフトウェアが、ルータのフラッシュ メモリにプレインストールされます。
- **ROUTER-SDM-CD**: Cisco SDM Express がルータのフラッシュ メモリにプレインストールされ、Cisco SDM CD がルータに付属されます。
- **ROUTER-SDM-NOCF**: Cisco IOS の Auto-Install 機能を使用する場合の製品番号です。この製品番号を選択した場合は、工場にて SDM ソフトウェアがルータのフラッシュメモリに搭載されますが、ルータの NVRAM にデフォルト スタートアップ コンフィギュレーションはロードされません。
- **ROUTER-SDM-CD-NOCF**: SDM Express がルータのフラッシュ メモリにプレインストールされ、Cisco SDM CD がルータに付属されますが、NVRAM にデフォルト スタートアップ コンフィギュレーションはロードされません。

表 5 に、Cisco SDM の発注オプションおよび出荷オプションを示します。

表 5 Cisco SDM の発注オプションおよび出荷オプション

製品	出荷オプション
Cisco 831-SDM-64、Cisco 851、Cisco 871	<ul style="list-style-type: none"> ROUTER-SDM-CD をデフォルトで付属 ROUTER-SDM-CD-NOCF も選択可能
Cisco 1700 および Cisco 2600XM	<ul style="list-style-type: none"> セキュリティバンドル(K9)には ROUTER-SDM-CD をデフォルトで付属。ROUTER-SDM-CD-NOCF 選択も可能 その他の製品では、ROUTER-SDM-CD もしくは ROUTER-SDM-CD-NOCF を選択可能(デフォルト搭載ではない)
Cisco 1812J、Cisco ISR 1800 シリーズ、Cisco ISR 2800 シリーズ、および Cisco ISR 3800 シリーズ	<ul style="list-style-type: none"> ROUTER-SDM をデフォルト搭載 ROUTER-SDM-NOCF 選択も可能
Cisco 2691 および Cisco 3700 シリーズ	<ul style="list-style-type: none"> セキュリティバンドル(K9)には ROUTER-SDM をデフォルトで付属。ROUTER-SDM-NOCF 選択も可能 その他の製品では、ROUTER-SDM もしくは ROUTER-SDM-NOCF を選択可能(デフォルト搭載ではない)
Cisco 7204VXR、Cisco 7206VXR、および Cisco 7301	<ul style="list-style-type: none"> セキュリティバンドル(K9)には ROUTER-SDM をデフォルトで付属。ROUTER-SDM-NOCF 選択も可能 その他の製品では、ROUTER-SDM もしくは ROUTER-SDM-NOCF を選択可能(デフォルト搭載ではない)

シスコ製品の購入方法の詳細は、「[購入案内](#)」を参照してください。

ソフトウェアのダウンロード方法

ルータのフラッシュメモリまたは PC にインストール可能な最新の Cisco SDM ソフトウェアをダウンロードするには、[ソフトウェアセンター](#)にアクセスしてください。

サービスおよびサポート

シスコは、お客様の成功を支援するため、さまざまな新しいサービスプログラムを用意しています。これらのサービスは、スタッフ、プロセス、ツール、パートナーをそれぞれに組み合わせて提供され、お客様から高い評価を受けています。ネットワークへの投資を無駄にすることなく、ネットワーク運用を最適化しネットワークインテリジェンスの強化や事業拡張を進めていただくためにシスコのサービスをぜひお役立てください。サービスについての詳細は、以下の URL を参照してください。

テクニカル サポート サービス

<http://www.cisco.com/jp/go/tac/>

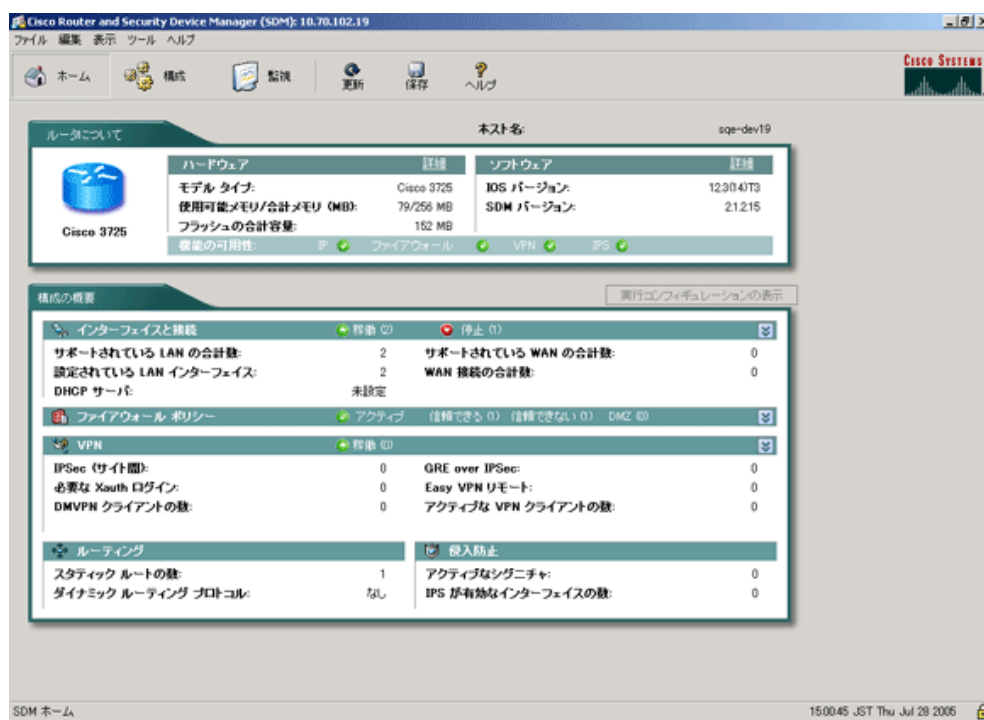
サービス プログラム

<http://www.cisco.com/jp/services/>

参考情報

Cisco Router and Security Device Manager (SDM) Ver.2.1.2 より、日本語*GUI(グラフィカル ユーザ インターフェイス)が装備され、日本語*オンライン ヘルプとチュートリアルも用意されています。

図 7 Cisco SDM 日本語画面



©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

お問い合わせ先