2006 年 4 月（第 1 版）

Cisco Security Device Manager サンプル設定ガイド

SDM 2.1.2 2005/09 リリース版

ロールベースアクセス制御

I 概　要

Cisco IOS ロールベース CLI アクセスは、ネットワーク管理者が Cisco IOS EXEC またはコンフィグレーション（config）モードコマンドに対して、選択的あるいは部分的なアクセス制御を提供する「ビュー」を定義する機能です。

ビューは、Cisco IOS コマンドライン インターフェイス（CLI）へのユーザクセスと構成情報を制限します。ビューはユーザに対してどんなコマンドを許可するか、そしてどんな構成情報を表示可能であるかを定義することができ、この機能によって、ネットワーク管理者は Cisco ネットワークデバイスへのアクセスについて厳密なアクセス制御を行うことができます。

シスコルータとセキュリティ デバイス マネージャ（SDM；Security Device Manager）は、SDM ユーザアクセスのために事前に定義された 4 つのビュー（SDM_Administrator（root）、SDM_Monitor、SDM_Firewall、SDM_Easy VPN_Remote）の作成/削除を行うことができます。

（1） SDM_Administrator（root）

このビュータイプに関連づけられたユーザは、Cisco SDM に完全なアクセスを持って、Cisco SDM によってサポートされたすべての操作を実行することができます。

（2） SDM_Monitor

このビュータイプに関連づけられたユーザは、Cisco SDM によってサポートされたすべての機能について監視することができますが、構成変更を行うことができません。このユーザは Cisco SDM のインターフェイスと接続、ファイアウォールと ACL、VPN 機能など様々な領域にアクセスすることができます。しかしながら、これらの領域のユーザ インターフェイス コンポーネントは監視のみが許可され、設定はできないよう無効になっています。

（3） SDM_Firewall

このビュータイプに関連づけられたユーザは、SDM のファイアウォールと ACL 及びモニター監視機能を使用することができます。このユーザは、ファイアウォール ウィザード（ファイアウォール ポリシービュー）、インスペクトルール エディタ、およびアクセスリスト エディタを使用することでファイアウォールとアクセスコントロールリストを設定することができます。ユーザは、「インターフェイスと接続」構成画面からアクセスリストとインスペクトルールを関連づけたり、または解除したりすることができます。他の領域のユーザインターフェイスコンポーネントは、設定/変更ができないよう無効にされています。

（4）SDM_EasyVPN_リモート:

このビュータイプに関連づけられたユーザは Cisco SDM Easy VPN リモートの機能を使用することができます。ユーザは、Easy VPN リモート接続を作成して、それらを編集することができます。他の領域のユーザ

インターフェイス コンポーネントは無効にされています。

ユーザ定義されたビューが Cisco SDM によって必要とされている最小量のコマンドを含む場合、ユーザ定義されたビュー（あるいはシスコ SDM が事前に定義している「none」と呼ばれるビュー）に関連づけられたユーザがシスコ SDM を呼び出すことができます。Cisco SDM はユーザ定義されたビューを SDM_Monitor ビューにマップし、そして Cisco SDM は読込み専用モードとして起動されます。

II 設定手順

ここでは、ファイアウォールと監視機能をもつセキュリティオペレータの作成を行います。

設定を始める前に、以下の前提条件が満たされているのを確認してください。

(1) イネーブルパスワードが設定されていることが必要です。

(2) Cisco IOS 12.3(11)T 以前のバージョンの場合、認証・承認・課金の依存関係の点から AA 機能を有効化し、認証と承認を適切に行う必要があります。

(3) ビューを構成するために、ユーザは root ビューにアクセスしなければなりません。(特権レベル 15 のユーザのみアクセス可能)

サンプル構成はセキュリティオペレータと新しいユーザ(secOP)作成のためのビュー(ビューセキュリティ)の構成を含んでいます。前提条件を構成する方法についてはこのサンプル構成でカバーされていません。CLI によるビュー構成は、アクセスルール、インスペクトルール、および show コマンドによって表示されるファイアウォールルール、ファイアウォールステータス、ルータ構成、およびルータステータスを構成するのに使用されるシスコ IOS CLIs に関する広範囲にわたる知識を必要とします。

1. Cisco SDM ロールベースアクセス

Cisco SDM は、事前に定義された 4 つのビューを提供することによって、ロールベースのアクセスを容易にします。各ビューがその主な操作コマンドと構成コマンドのセットに基づいて名づけられているので、ビューへのユーザの関連づけを容易に行うことができます。このドキュメントでは、ユーザとビューの関連付けをどのように構成するか、またビューに関連づけられたユーザをどのように編集するかを解説します。ビューに関連付けられた 2 つのユーザが設定されており、sdmadmin は特権レベル 1 で SDM_Administrator(root)に定義され、sdmvpn は特権レベル 15 で SDM_EasyVPN_Remote に定義されています。このシナリオでは、新しいユーザカウント sdmOP を特権レベル 1 で SDM_Firewall に定義し、既存の sdmvpn を特権レベル 1 に変更します。

2. ユーザカウントと関連付けたビューの設定

ユーザカウントの変更を行うために、特権レベル 15 のユーザまたは SDM_Administraitor(root)ビューに定義されたユーザで SDM にログオンします。この例では、「sdmadmin」でログオンします。追加タスクの構成画面で[ルータアクセス]フォルダを展開し、[ユーザカウント/表示]を選択します(図 1)。

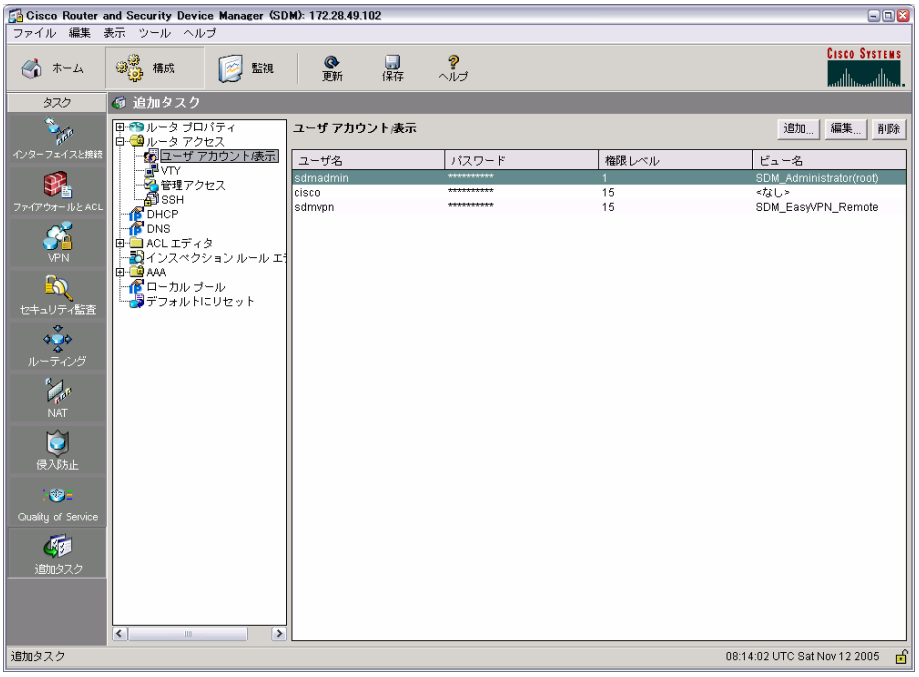
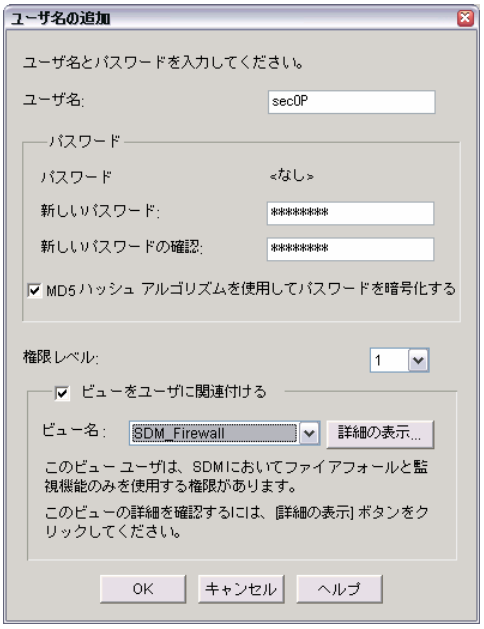


図 1:追加タスクーユーザカウント/表示

ユーザカウント/表示の「追加」をクリックし、ユーザ名の追加画面を表示させます（図 2）。以下の情報を入力し、「OK」をクリックします。



ユーザ名：secOP

パスワード：secOP123

MD5 ハッシュアルゴリズム：チェック（有効化）

特権レベル：1

ビューをユーザに関連付け：チェック（有効化）

ビュー名：SDM_Firewall

図 2：ユーザ名の追加

これまでに SDM_Administrator（root）以外のビューに関連付けられるユーザを初めて定義する場合には、ビューパスワードの入力を求められます（図 3）。このシナリオでは、security123 というビューパスワードを使用します。

図 3：ビューパスワード設定

ユーザの追加が完了すると、図 4 のようにユーザカウント/表示画面にユーザ「secOP」が追加されます。

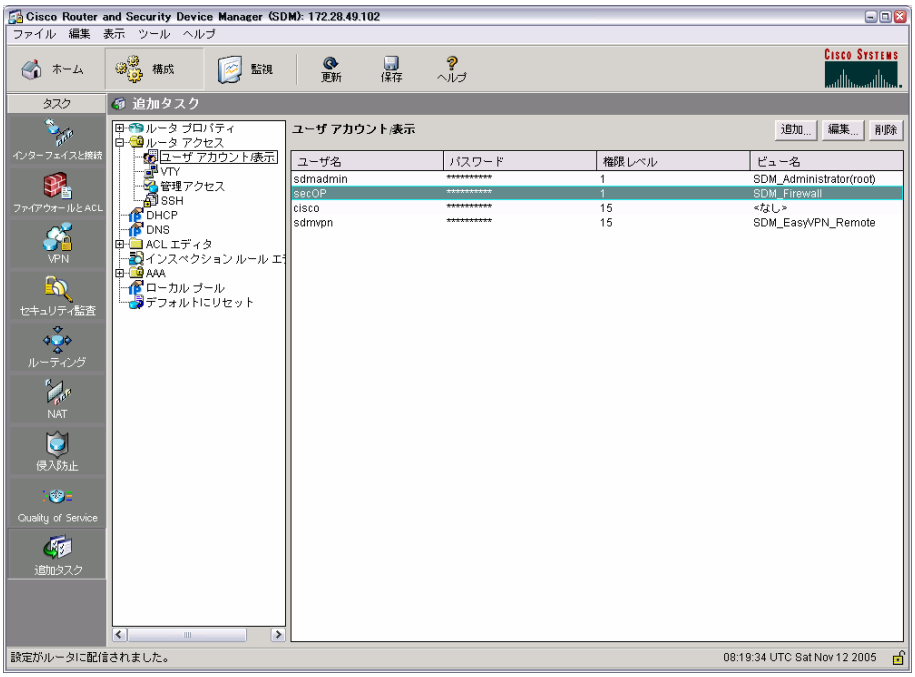


図 4：ユーザ「secOP」登録完了

続いて、ユーザ「sdmvpn」の編集を行います。ユーザ「sdmvpn」を選択し、「編集」をクリックします（図 5）。

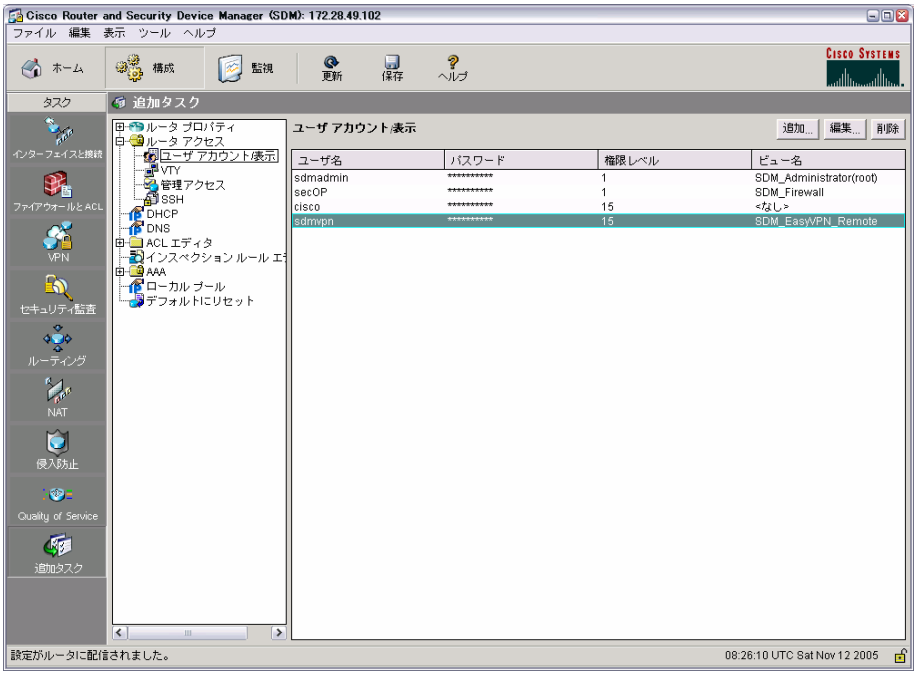


図 5：ユーザ「sdmvpn」の編集

ユーザ「sdmvpn」のパスワードを「likesdm」に、特権モードを 15 から 1 に変更し「OK」をクリックします（図 6）。

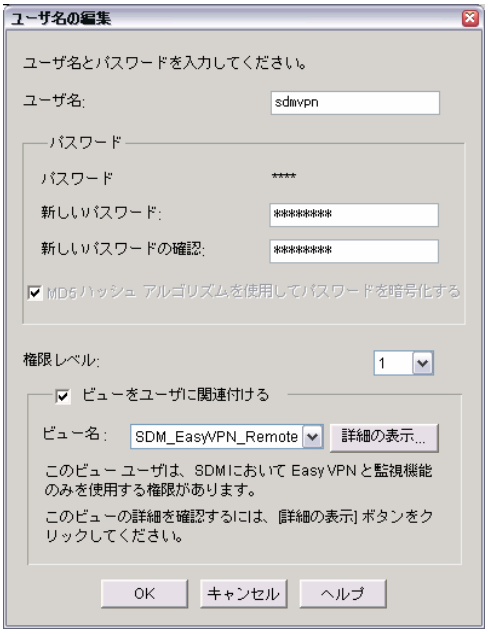


図 6:ユーザ名の編集

登録ユーザの内容を変更する場合、図 7 の警告が表示されます。現在ログオンしている管理権限のあるアカウントを削除すると、以後 SDM にアクセスできなくなることへの警告メッセージです。このシナリオでは問題がありませんので、「はい」をクリックして処理を進めます。

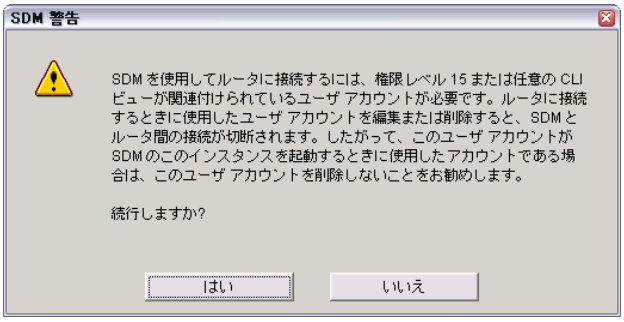


図 7:ユーザ名変更警告

ユーザ「sdmvpn」の編集が反映され、特権レベルが 1 に変更されていることを確認します（図 8）。

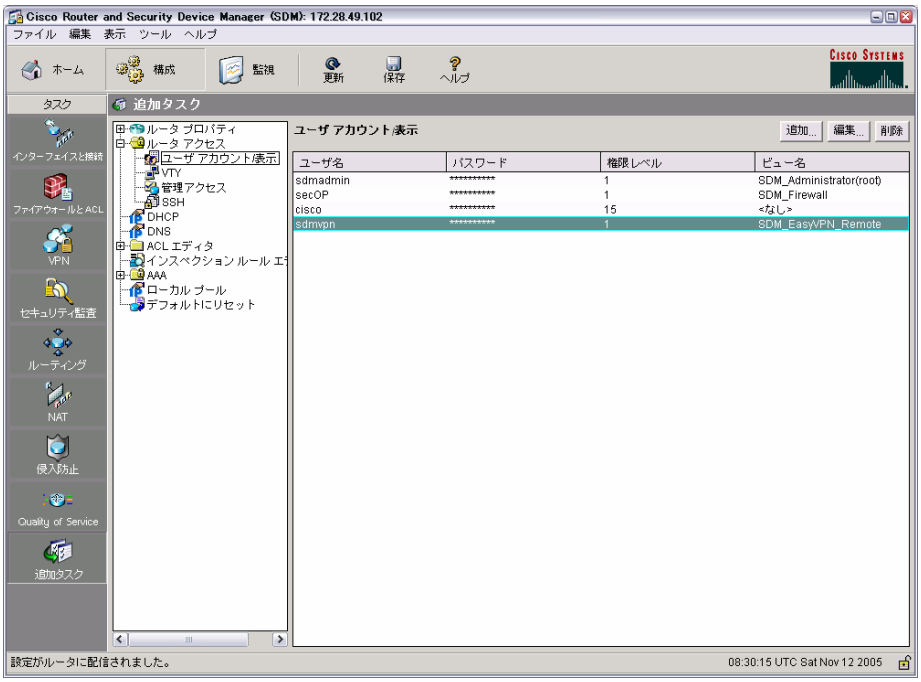


図 8:ユーザ変更の確認

3. 設定の確認

設定したユーザでログオンし、ロールベースのアクセス制限が正しく機能していることを確認します。一旦 SDM からログオフし、再度ユーザ「secOP」でログオンします。ユーザ secOP は SDM_Firewall ビューに属しているため、ファイアウォールと ACL の確認/変更を行うことができます。図 9/図 10 では、ユーザ secOP がファイアウォールと ACL 画面の構成項目をすべて設定できる状態であることがわかります。また図 11/図 12 のインターフェイス/接続画面では、そのほとんどがグレーアウトして設定を行うことができなくなっています。

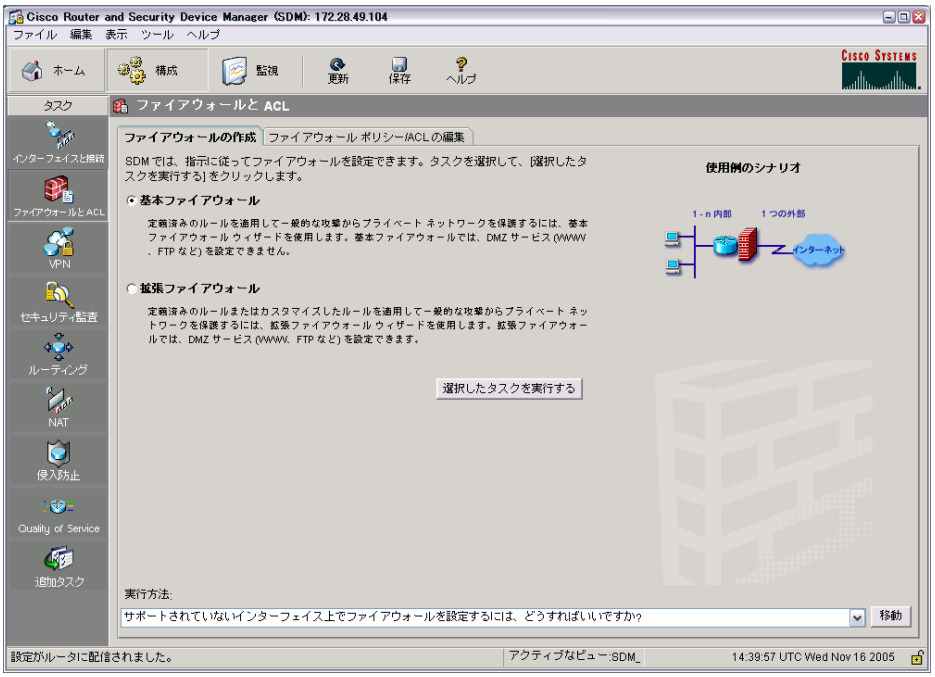


図 9：ユーザ「secOP」によるファイアウォールと ACL（1）

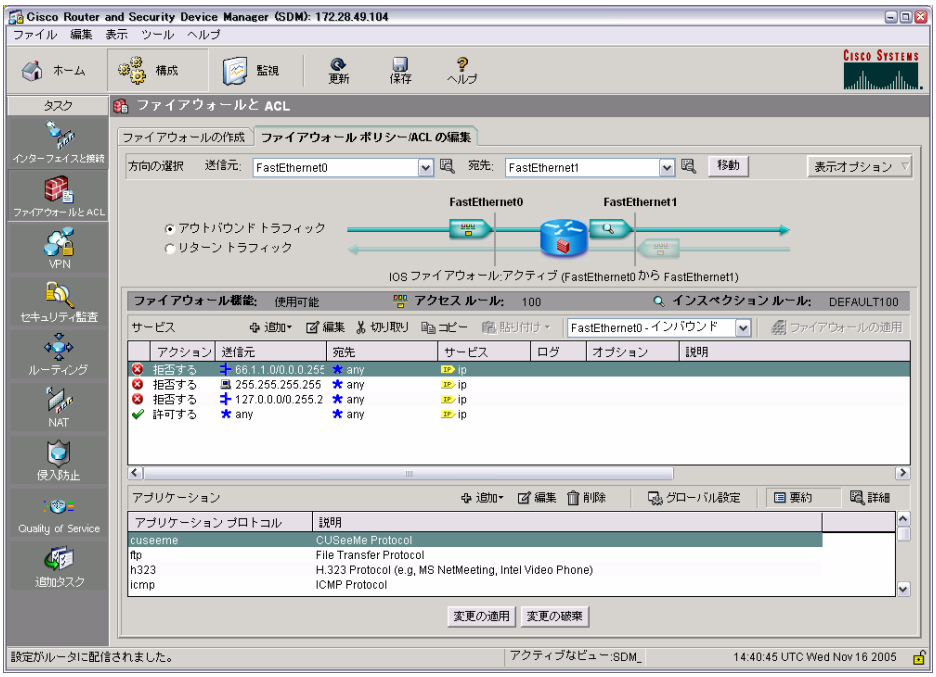


図　10：ユーザ「secOP」によるファイアウォールと ACL（2）

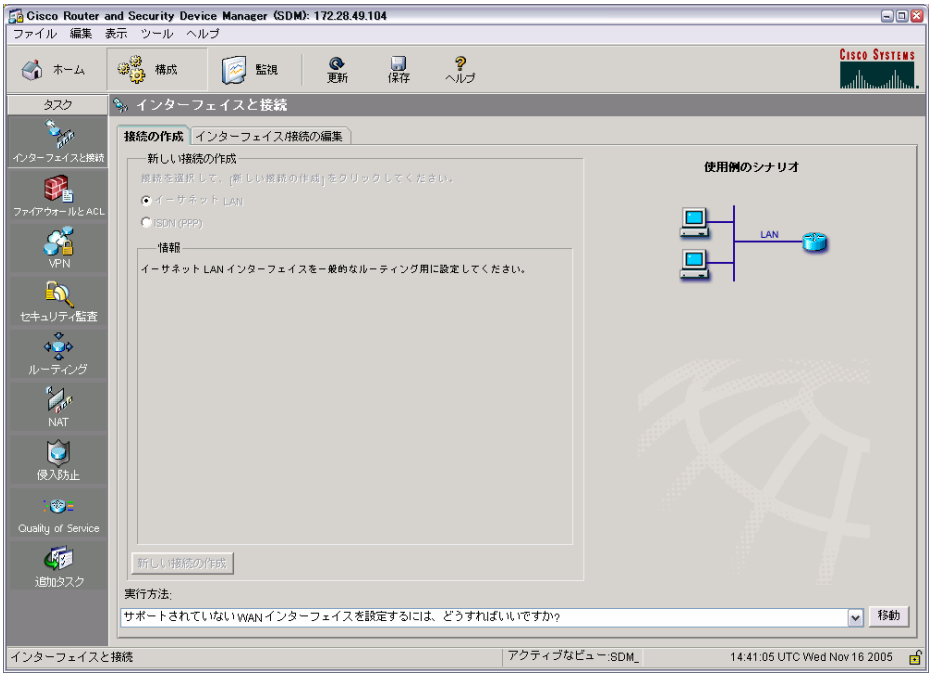


図　11：ユーザ「secOP」によるインターフェイスと接続画面（1）

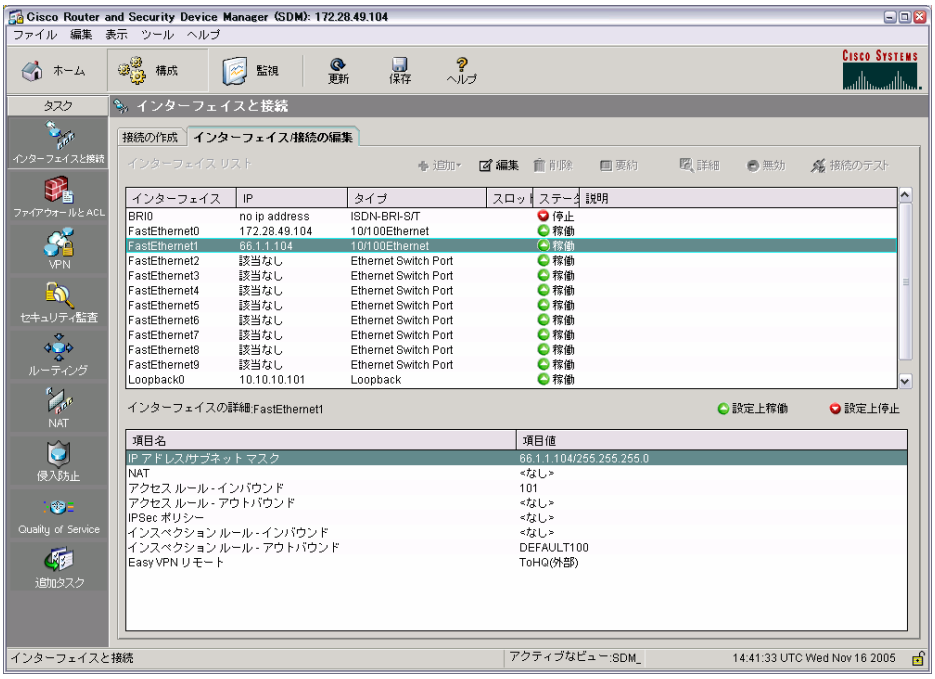


図 12：ユーザ「secOP」によるインターフェイスと接続画面（2）

またインターフェイス/接続の編集画面でインターフェイスの編集をクリックしインターフェイス機能編集ダイアログを表示させると、図 13 のようにセキュリティ関係の設定項目については secOP（SDM_Fireall）で設定可能な状態にあることがわかります。

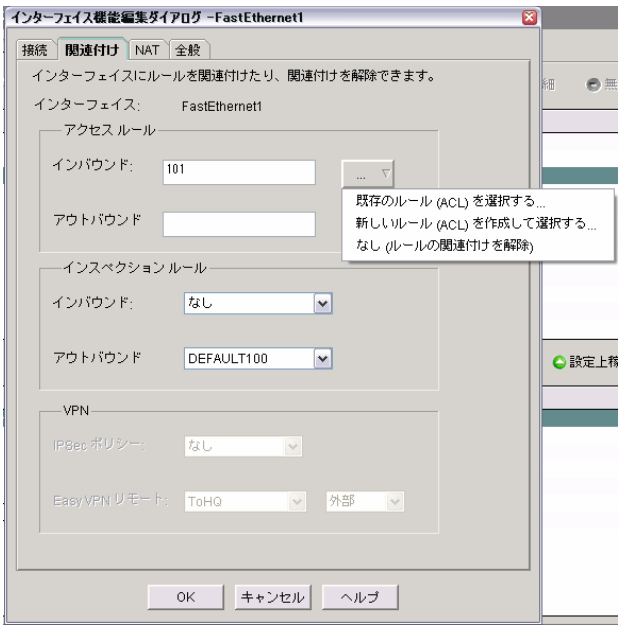


図 13：インターフェイス機能編集ダイアログ

Cisco Security Device Manger サンプル設定ガイド
ロールベースアクセス制御

発行　　2006 年 4 月　第 1 版

発行　　シスコシステムズ株式会社