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

Cisco Easy VPN クライアント

I 概　要

Cisco Easy VPN は、遠隔オフィスとテレワーカーのための仮装プライベートネットワーク（VPN）構築を簡素化します。Cisco VPN ソリューションは、すべての Cisco VPN デバイスの VPN 接続を集中管理し、VPN 展開における管理を容易にします。Cisco Easy VPN は、Cisco Easy VPN リモート、Cisco Easy VPN サーバという 2 つのコンポーネントから構成されます。Cisco Easy VPN リモート機能は、Cisco IOS ルータが Cisco Easy VPN サーバから VPN トンネル接続に関するセキュリティポリシーを受けとることにより、離れた場所でのコンフィグレーション要件を最小限にとどめることができます。特に遠く離れたオフィスでは、このような費用対効果の高い解決策は IT サポートを効率的に行うために有効です。Cisco Easy VPN サーバは、サイト間接続またはリモートアクセス VPN ゲートウェイデバイスとして機能します。リモートオフィス側（スポーク側）のルータが Cisco Easy VPN リモートの機能を果たします。

このサーバクライアント機能は、主要サイトで定義されたセキュリティポリシーをリモート VPN 装置に配信し、それぞれの VPN 接続において VPN の接続確立前に最適・最新のポリシーを適用するなど VPN ポリシー管理の簡素化に有効です。

Cisco Easy VPN サーバとして構成されたルータは、Cisco Easy VPN リモートが有効になっているリモートルータからの VPN トンネルを終端することができます。Cisco Easy VPN リモートの大きな特徴は、内部 IP アドレス、内部サブネットマスク、DNS サーバアドレス、WINS サーバアドレス、スプリット トンネリングの有無などの VPN パラメータについて、リモートデバイスへ配信することです。本社などの中核サイトに保存された構成は、エンドユーザポリシーの動的な構成をサポートし、エンドユーザとフィールドエンジニアの作業工数を最小限にとどめます。これにより、設定ミスとそのために要するさらなるサポートコストを抑えることができます。このような特徴から、セキュリティ ポリシーの集中管理を提供する Cisco Easy VPN は、迅速なユーザ対応を必要とする大規模な VPN 展開において有効なソリューションとなります。

Cisco Easy VPN は、VPN トンネルに対する接続パラメータのネゴシエーションを行い、IP Security（IPSec）トンネルを確立するための自動管理を提供します。拡張認証（Xauth）は IPSec 接続を要求するユーザを特定するさらなる認証パターンを追加します。スプリットトンネリングは、インターネット向けのトラフィックについて、リモートルータがそれらのトラフィックを暗号化されたトンネルに送らず直接インターネットへ送信することを可能にする機能です。

II 設定手順

本設定ガイドでは以下の前提条件の下、LAN to LAN での IPSec VPN 構成を想定しています。

(1) 固定 IP アドレスを持つ Cisco Easy VPN サーバ

(2) 固定または動的 IP を持つ Cisco Easy VPN リモート

(3) Cisco Easy VPN リモートは、Cisco Easy VPN サーバへ送信するトラフィックのみ暗号化

(4) リモート拠点（営業所）からのインターネット向けトラフィックは暗号化を行わず、直接送信される

(5) リモート拠点からのトラフィックはアドレス変換（NAT/PAT）が行われる

(6) ユーザレベルの認証は VPN アクセスの拡張認証によって行われる

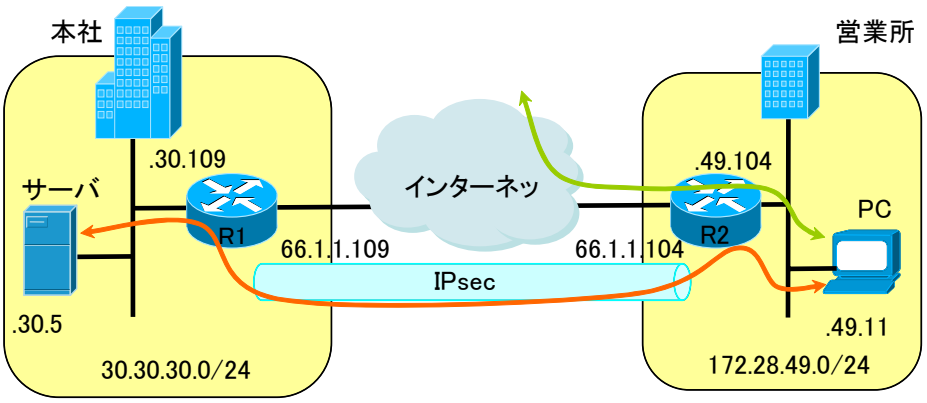

図 1：ネットワーク構成イメージ

このサンプル構成では、Cisco Easy VPN リモートをクライアントモードで使用します。クライアントモードでは、Cisco Easy VPN リモートの背後にある LAN 全体は、Cisco Easy VPN サーバによって提供される IP アドレスによってアドレス変換（NAT）されます。

Cisco Easy VPN サーバ上でスプリットトンネリングが構成されている場合、このポリシーは Cisco Easy VPN リモートへ自動的に適用されます。スプリットトンネリングは、インターネット向けのトラフィックについてリモートルータが暗号化されたトンネルを通ることなく直接送信することを可能にしています。

本例において、事前共有キーはルータを認証するのに使用され、拡張認証（Xauth）は IPSec 接続を要求するユーザを特定するための追加レベルの認証を提供します。リモートルータは、Internet Key Exchange（IKE）セキュリティアソシエーションが確立された後に「ユーザ名/パスワード」チャレンジ認証を待ち受けます。

また本構成に使用する機器は、LAN および WAN インターフェイスが設定されており、SDM が利用できる状態にあるものとしています。

1. Cisco Easy VPN リモートの作成

VPN タスクの構成モードで、「Easy VPN リモート」を選び、[Eazy VPN リモートの作成]を選択します。画面中の「Easy VPN リモートを作成する。」を選択して「選択したタスクを実行する」をクリックし、Easy VPN リモート設定ウィザードを起動します(図 2)。

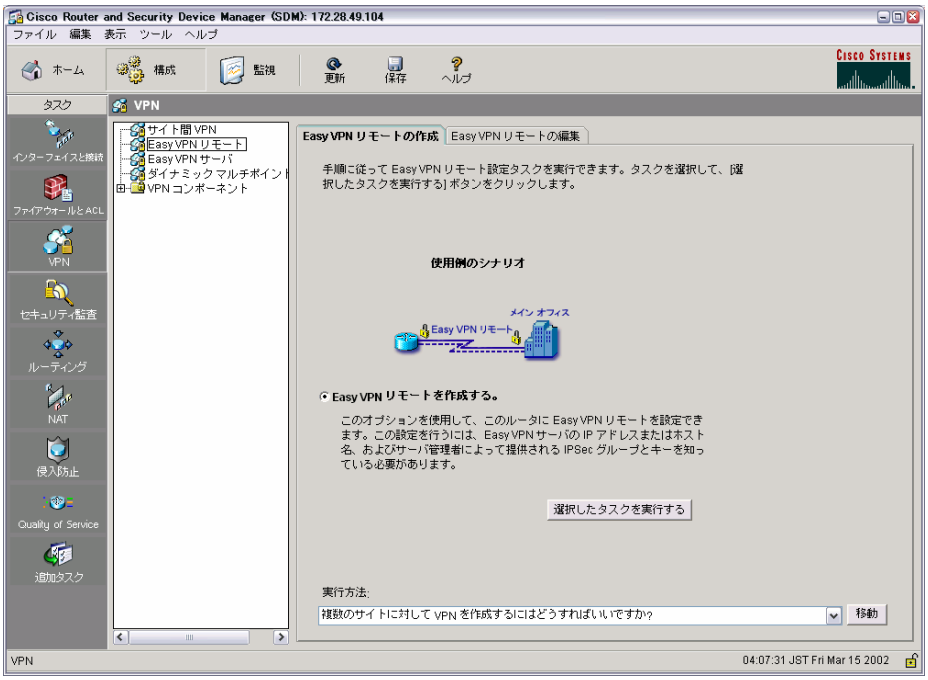

図 2:Easy VPN リモートの作成

Easy VPN リモートウィザード画面が表示(図 3)されます。「次へ」をクリックして処理を進めます。

図 3:Easy VPN リモートウィザード

Easy VPN リモートの接続情報（図 4）を以下のように構成し、「次へ」をクリックします。

Easy VPN トンネル名：ToHQ

Easy VPN サーバ

　Easy VPN　サーバ 1: 66.1.1.109

　グループ：EZVPNgroup

キー：cisco123

　　（画面上では暗号化されます）

図 4：接続情報

Easy VPN リモートにおける接続の特徴（図 5）を以下のように構成し、「次へ」をクリックします。

モード：Client

制御：Auto

図 5：接続の特徴

ユーザ認証（Xauth）設定（図 6）を以下のように構成し、「次へ」をクリックします。

画面上の「ルータ上にXauthユーザ名とパスワードを保存する」をチェック

ユーザ名：sdmuser1

パスワード：cisco123

図 6：ユーザ認証（Xauth）

ISP などに接続している外部インターフェイス及び内部インターフェイスを以下のように指定し（図 7）、「次へ」をクリックします。

外部インターフェイス：Fas tEthernet 1

内部インターフェイス：Fast Ethetnet 0

図 7：インターフェス設定

Easy VPN リモートの設定内容を確認し、「完了」をクリックします（図 8）。

図 8：Easy VPN リモート設定確認画面

Easy VPN サーバとの通信を可能にするために、デフォルトルートを追加します。SDM のルーティングタスクで、スタティックルーティングの「追加」をクリックします（図 9）。

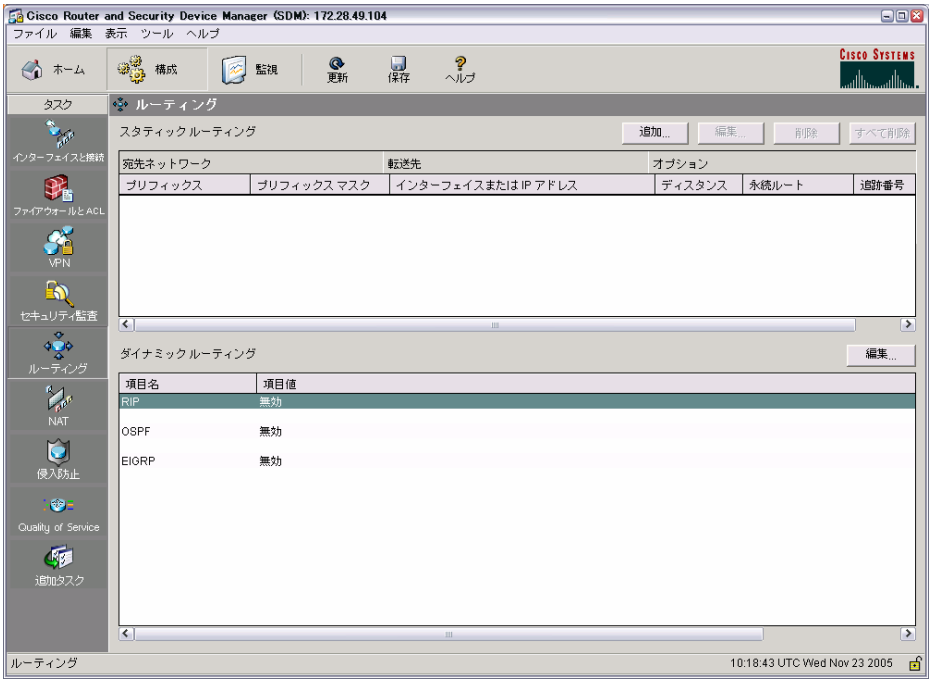

図 9：スタティックルーティングの追加

IP スタティックルートの追加画面で、「このルートをデフォルトルートにする」をチェックし、「転送（ネクストホップ）」は「インターフェイス」をチェックして、外側インターフェイスである Fast Ethetnet 1 を選択します（図 10）。

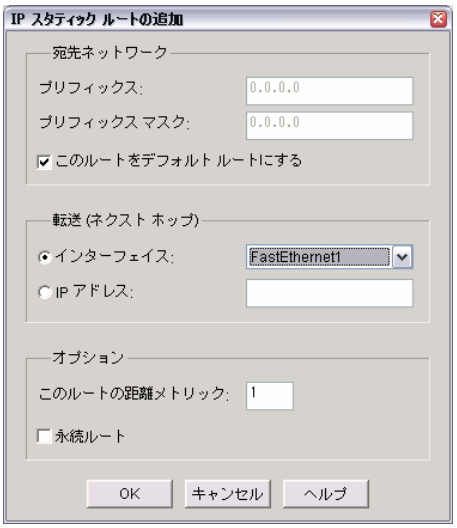

図 10：デフォルトルート設定

ルーティングタスク画面に設定したデフォルトルートが正しく反映されていることを確認します（図 11）。

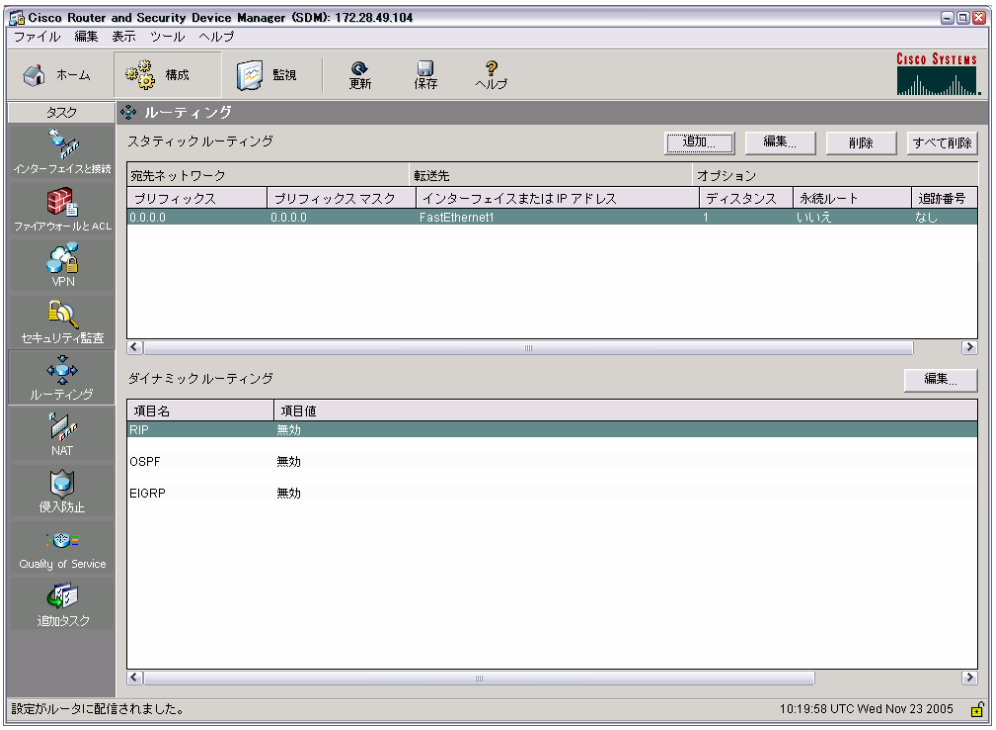

図 11：デフォルトルートの確認

2. 接続確認

Easy VPN の接続確認を行うため、[VPN]タスクの［Easy VPN リモート］の［Easy VPN リモートの編集］タブから、「トンネルのテスト」をクリックし、VPN トラブルシューティングを起動します（図 12）。

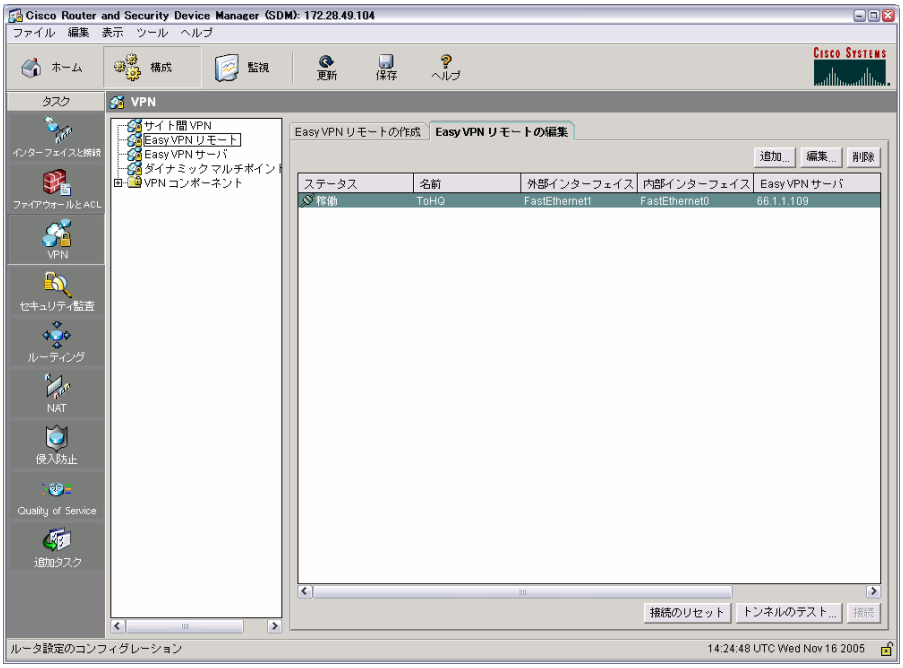

図 12：Easy VPN リモートの編集

VPN トラブルシューティング画面の「開始」をクリックし、接続テストを開始します（図 13～図 16）。

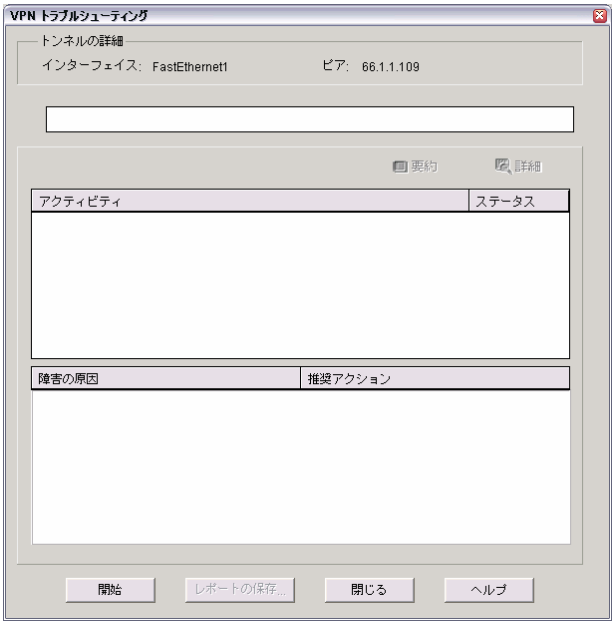

図 13：VPN 接続テスト（1）

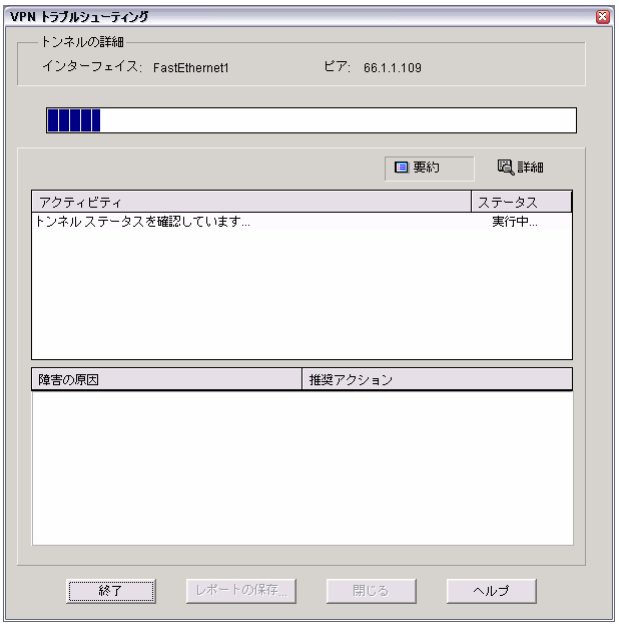

図 14:VPN 接続テスト(2)

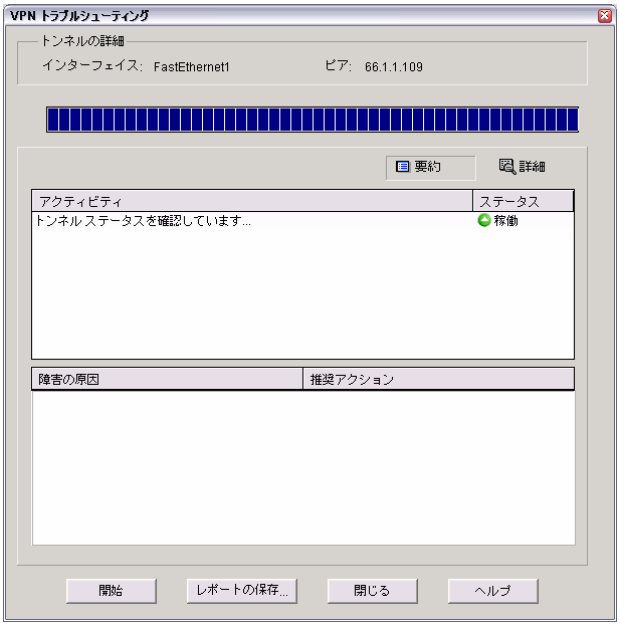

図 15:VPN 接続テスト(3)

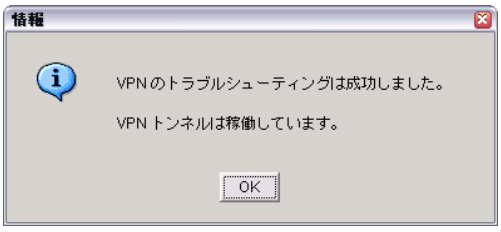

図 16:VPN 接続テスト(4)

3. VPN ステータスの確認

VPN ステータスの確認は、監視モードの VPN タスクを参照します。Easy VPN リモートのステータスを確認するには、[IPSec トンネル]タブ（図 17）と[IKE SA]タブ（図 18）を参照します。

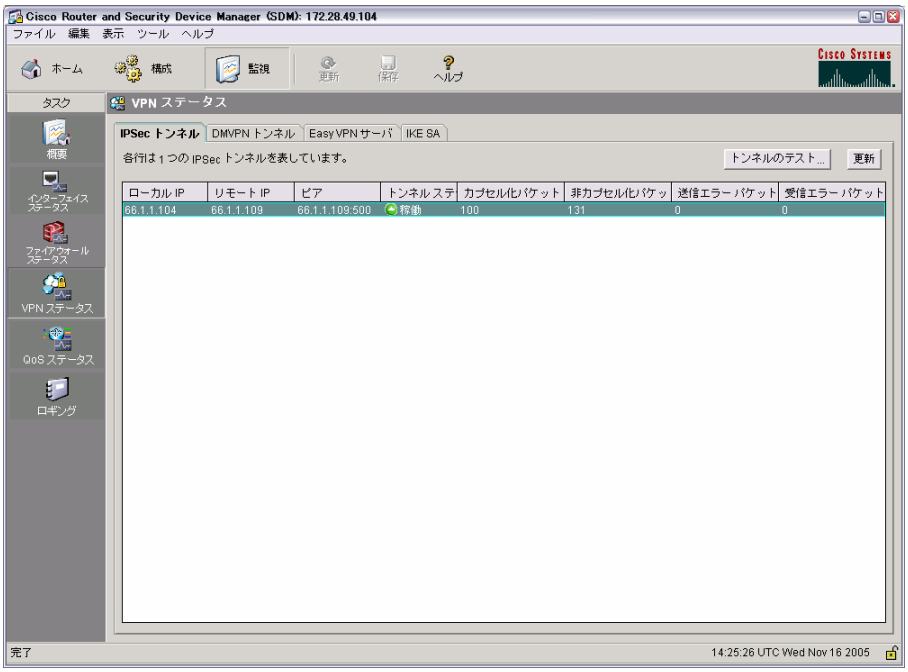

図 17：VPN ステータス/IPSec トンネル

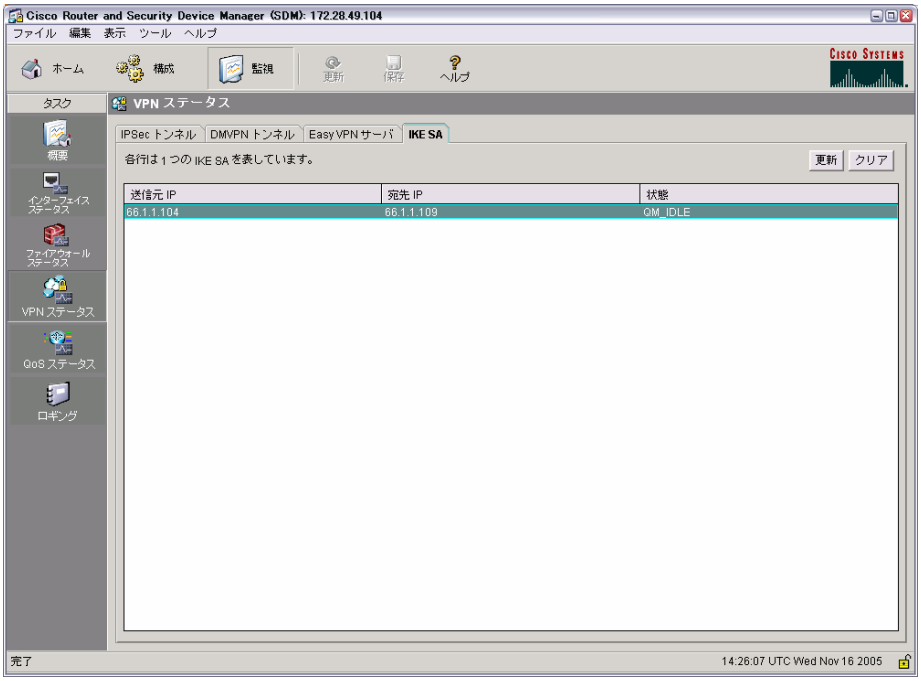

図 18：VPN ステータス/IKE SA

参考:コマンドラインでの Easy VPN クライアント構成設定例

以下の CLI コマンドは、これまで SDM で行ってきたものと同じ内容の構成を行う場合のコマンドになります。

```
The Cisco Easy VPN Remote Configuration
!
crypto isakmp enable
crypto ipsec client ezvpn ToHQ
 !Cisco Easy VPN リモートの作成:接続名「ToHQ」
connect auto
mode client
 ! NAT/PAT を使用する VPN クライアントの指定
group EZVPNgroup key cisco123
! Cisco Eazy VPN サーバに定義されたグループ「EZVPNgroup」と事前共有鍵「cisco123」の設定
peer 66.1.1.109
 # Cisco Easy VPN サーバアドレス
username sdmuser1 password cisco123 # Easy VPN サーバでパスワード保存機能が有効になっている場合、Xauth の ユーザ名/パスワードを保存する
interface FastEthernet0/0
crypto ipsec client ezvpn toHQ inside
interface FastEthernet0/1
crypto ipsec client ezvpn toHQ outside # NAT/PAT 変換用の外部インターフェイス指定
```

Cisco SDM Easy VPN ウィザードを利用することによって、ユーザは簡単かつ迅速に、クライアント/サーバ IPSec VPN 設定に関する最小限の知識で Easy VPN リモート設定を生成することができます。

```
1812J SDM config

service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no logging buffered
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
!
aaa session-id common
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
ip cef
no ip dhcp use vrf connected
!
!
ip name-server 30.30.30.5
```

```
no ip ips deny-action ips-interface
!
!
!
username cisco privilege 15 password 0 cisco
!
!
!
!
!
!
!
crypto ipsec client ezvpn ToHQ
 connect auto
 group EZVPNgroup key cisco123
 mode client
 peer 66.1.1.109
 username sdmuser1 password cisco123
 xauth userid mode local
!
!
!
!
interface Loopback0
 ip address 10.10.10.101 255.255.255.255
!
interface BRI0
 no ip address
 shutdown
!
interface FastEthernet0
 ip address 172.28.49.104 255.255.255.0
 duplex auto
 speed auto
 crypto ipsec client ezvpn ToHQ inside
!
```

```
interface FastEthernet1
 description $ETH-LAN$
 ip address 66.1.1.104 255.255.255.0
 duplex auto
 speed auto
 crypto ipsec client ezvpn ToHQ
!
interface FastEthernet2
!
interface FastEthernet3
!
interface FastEthernet4
!
interface FastEthernet5
!
interface FastEthernet6
!
interface FastEthernet7
!
interface FastEthernet8
!
interface FastEthernet9
!
interface Vlan1
 no ip address
!
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet1
!
!
ip http server
ip http authentication local
no ip http secure-server
!
!
!
```

```
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
no scheduler allocate
end
```

Cisco Security Device Manger サンプル設定ガイド
Cisco Easy VPN クライアント

発行　　2006 年 4 月　第 1 版

発行　　シスコシステムズ株式会社