CHAPTER 32

# ルータ プロパティ

ルータ プロパティでは、ルータの全体的な属性を定義できます。たとえば、ルータ名、ドメイン名、パスワード、簡易ネットワーク管理プロトコル（SNMP）ステータス、ドメイン ネーム システム（DNS）サーバ アドレス、ユーザ アカウント、ルータ ログの属性、仮想端末（vty）設定、SSH 設定、その他のルータ アクセス セキュリティ設定などです。

# デバイス プロパティ

［デバイス プロパティ］画面には、ルータのホスト、ドメイン、およびパスワードの情報が表示されます。

## デバイス タブ

［デバイス］タブには、次のフィールドがあります。

### ホスト

このフィールドには、ルータに付ける名前を入力します。

### ドメイン

組織のドメイン名を入力します。ドメイン名がわからない場合は、ネットワーク管理者に確認してください。

### バナーのテキストの入力

ルータ バナーのテキストを入力します。このバナーは、ルータにログインするたびに表示されます。不正アクセスの禁止を知らせるメッセージをこのバナーに記載することをお勧めします。

## パスワード タブ

［パスワード］タブには、次のフィールドがあります。

### Enable Secret パスワード

Cisco Configuration Professional（Cisco CP）では、enable secret パスワードがサポートされています。このパスワードを使用すると、このルータ上で設定コマンドを入力できるユーザを制御できます。enable secret パスワードを設定することを強くお勧めします。このパスワードは、Cisco CP の［デバイス プロパティ］ウィンドウでは読めません。また、ルータ コンフィギュレーション ファイルには暗号化されて表示されます。したがって、このパスワードを忘れてしまったときのために書き留めておいてください。

ルータで実行されている Cisco IOS リリースで enable パスワードもサポートされている場合があります。enable パスワードは enable secret パスワードに似ていますが、コンフィギュレーション ファイル内で暗号化される点が異なります。コマンドライン インターフェイス（CLI）を使用して enable パスワードを設定しても、enable secret パスワードが設定されている場合は無視されます。

### 現在のパスワード

パスワードがすでに設定されている場合は、このエリアにアスタリスク（*）が表示されます。

### 新しいパスワードの入力

このフィールドには新しい enable パスワードを入力します。

### 新しいパスワードの再入力

［新しいパスワードの入力］フィールドに入力したのと同じパスワードを再入力します。

# 日付と時刻 : 時計のプロパティ

このウィンドウでは、ルータの日付と時刻の設定を表示したり編集したりできます。

### 日付 / 時刻

Cisco CP ステータス バーの右側でルータの日付と時刻の設定を確認できます。［時計プロパティ］ウィンドウのこの部分に表示される日付と時刻の設定は更新されません。

### ルータのタイム ソース

このフィールドには、次のいずれかの値が表示されます。

- NTP — ルータは NTP サーバから時刻情報を受け取ります。
- ユーザ設定 — 日付と時刻の値は、Cisco CP または CLI を使用して手動で設定します。
- タイム ソースなし — ルータには日付または時刻が設定されていません。

### Change Settings

ルータの日付と時刻の設定を変更する場合にクリックします。

## 日付と時刻のプロパティ

このウィンドウでは、ルータの日付と時刻を設定します。Cisco CP で設定を PC と同期させることも、ユーザが手動で設定することもできます。

### ローカル PC の時計と同期をとる

ルータの日付と時刻の設定を PC の設定と同期させるように Cisco CP をセットアップする場合にオンにします。

### 同期

Cisco CP で時間設定を同期させる場合にクリックします。Cisco CP でこの方法によって日付と時刻の設定が調整されるのは、ユーザが［同期］をクリックしたときだけです。つまり、その後のセッションで設定が自動的に PC と同期されるようなことはありません。［ローカル PC の時計と同期をとる］を選択しなかった場合、このボタンは無効になります。

**（注）** ［同期］をクリックしたときに Cisco CP で正しい設定が受信されるようにするには、Cisco CP を起動する前に PC でタイム ゾーンと夏時間を設定しておく必要があります。

### 日付と時刻の編集

このエリアでは、日付と時刻を手動で設定します。年と月はドロップダウン リストから、日はカレンダーで選択できます。［時刻］エリア内のフィールドには、値を 24 時間制で入力する必要があります。グリニッジ標準時（GMT）に基づくタイム ゾーンを選択するか、またはリストからタイム ゾーン内の主要都市を選択できます。

ルータで夏時間と標準時の時刻設定が自動的に調整されるようにするには、［自動的に夏時間の調整をする］を選択します。

### 適用

［日付］、［時刻］、および［タイム ゾーン］フィールドに指定した日時の設定を適用する場合にクリックします。

## NTP

ネットワーク タイム プロトコル（NTP）を使用すると、ネットワーク上のルータの時刻の設定を NTP サーバと同期させることができます。NTP クライアントのグループで日付と時刻の情報を同一のソースから取得すると、各クライアントの時刻設定をより正確に一致させることができます。このウィンドウでは、設定されている NTP サーバ情報の表示、新しい情報の追加、および既存の情報の編集または削除を行うことができます。

（注）　ルータで NTP コマンドがサポートされていない場合、このブランチは［ルータ プロパティ］ツリーに表示されません。

### IP アドレス

NTP サーバの IP アドレスです。

組織に NTP サーバがない場合は、次の URL に記述されているような公開サーバを使用することもできます。

http://www.eecis.udel.edu/~mills/ntp/clock2a.html

### インターフェイス

ルータと NTP サーバとの通信に使用されるインターフェイスです。

### 優先する

この NTP サーバが優先 NTP サーバとして指定されている場合は、このカラムに［はい］と表示されます。ルータは、優先でないサーバよりも前に優先 NTP サーバに接続します。優先 NTP サーバは、複数存在する場合があります。

### 追加

NTP サーバ情報を追加する場合にクリックします。

### 編集

指定した NTP サーバ設定を編集する場合にクリックします。

### 削除

指定した NTP サーバ設定を削除する場合にクリックします。

## NTP サーバ詳細の追加 / 編集

このウィンドウでは、NTP サーバの情報を追加または編集します。

### IP アドレス

NTP サーバの IP アドレスを入力または編集します。

### 優先する

このサーバを優先 NTP サーバにする場合にクリックします。

### インターフェイス

NTP サーバにアクセスする際に使用するルータ インターフェイスを選択します。**show IP routes** という CLI コマンドを実行すると、この NTP サーバへのルートを持つインターフェイスを確認できます。

**（注）** ポート 123 のトラフィックに対する拡張アクセス ルールが作成され、このウィンドウで選択したインターフェイスに適用されます。このインターフェイスに対するアクセス ルールがすでに存在している場合は、Cisco CP によって、このインターフェイス上のポート 123 のトラフィックを許可するステートメントが追加されます。既存のルールが標準アクセス ルールの場合は、トラフィックのタイプと宛先を指定できるように、Cisco CP によって拡張ルールに変更されます。

### 認証キー

NTP サーバで認証キーが使用されている場合は、このボックスを選択して、必要な情報をフィールドに入力します。NTP サーバ上のキー情報と一致する情報を入力する必要があります。

#### キー番号

認証キーの番号を入力します。キー番号の範囲は 0 ～ 4294967295 です。

### キー値

NTP サーバで使用されるキーを入力します。キー値には、アルファベット A ～ Z（大文字または小文字）を使用できます。キー値の長さは 32 文字以内です。

### キー値の確認

確認のため、キー値を再入力します。

## SNTP

このウィンドウは、Cisco 830 ルータの場合に表示されます。簡易ネットワーク タイム プロトコル（SNTP）はネットワーク タイム プロトコル（NTP）の簡易版です。NTP を使用すると、ネットワーク上のルータの時刻設定を NTP サーバと同期させることができます。NTP クライアントのグループで日付と時刻の情報を同一のソースから取得すると、各クライアントの時刻設定をより正確に一致させることができます。このウィンドウでは、設定されている NTP サーバ情報の表示、新しい情報の追加、および既存の情報の編集または削除を行うことができます。

**（注）** ルータで NTP コマンドがサポートされていない場合、このブランチは［ルータ プロパティ］ツリーに表示されません。

### プロパティ

この NTP サーバのシステム定義名です。

### 値

この NTP サーバの IP アドレスです。

### 追加

NTP サーバ情報を追加する場合にクリックします。

### 編集

指定した NTP サーバ設定を編集する場合にクリックします。

### 削除

指定した NTP サーバ設定を削除する場合にクリックします。

## NTP サーバ詳細の追加

このウィンドウでは、NTP サーバの IP アドレスを入力します。

（注）　ポート 123 のトラフィックに対する拡張アクセス ルールが作成され、このウィンドウで選択したインターフェイスに適用されます。このインターフェイスに対するアクセス ルールがすでに存在する場合は、Cisco CP によって、このインターフェイス上のポート 123 のトラフィックを許可するステートメントが追加されます。既存のルールが標準アクセス ルールの場合は、トラフィックのタイプと宛先を指定できるように、Cisco CP によって拡張ルールに変更されます。

### IP アドレス

NTP サーバの IP アドレスをドット（.）で区切った 10 進表記で入力します。詳細については、「IP アドレスとサブネット マスク」を参照してください。

# ロギング

このウィンドウでは、システム メッセージのロギングを有効にしたり、ログを格納するロギング ホストを指定したりできます。送信および収集するロギング メッセージのレベルの指定、および複数のロギング ホストのホスト名または IP アドレスの入力が可能です。

### IP アドレス / ホスト名

［追加］をクリックして、ルータから送信されるロギング メッセージの格納先のネットワーク ホストの IP アドレスまたはホスト名を入力します。入力した情報を変更するには、［編集］ボタンをクリックし、エントリを削除するには、［削除］ボタンをクリックします。

ロギング ホストに送信するメッセージのタイプを指定するには、［ロギング レベル］ドロップダウン リストからロギングのレベルを選択します。詳細については、「ロギング レベル」を参照してください。

### ロギング レベル

［ロギング レベル］ドロップダウン リストから指定できるロギング レベルは次のとおりです。

- 緊急（0）
- アラート（1）
- 重大（2）
- エラー（3）
- 警告（4）
- 通知（5）
- 情報（6）
- デバッグ（7）

指定したレベル以下のすべてのメッセージがログに収集されるか、ルータにより ロギング ホストに送信されます。たとえば、通知（5）を選択すると、レベル 0 ～ 5 のメッセージが収集または送信されます。ファイアウォールのロギング メッセージのロギング レベルはデバッグ（7）、アプリケーション セキュリティのロギング メッセージのロギング レベルは情報（6）である必要があります。

### バッファへのロギング

システム メッセージのログがルータのバッファに収集されるようにするには、［編集］をクリックしたときに Cisco CP に表示されるダイアログで［ロギング バッファ］チェック ボックスを選択し、［バッファ サイズ］フィールドにバッファ サイズを入力します。バッファ サイズを大きくすると、新しいエントリ用

の領域を確保するために最も古いエントリが削除されるまでに格納できるエントリ数が多くなります。ただし、ロギングのニーズとルータのパフォーマンスのバランスをとる必要があります。

ログに収集するメッセージのタイプを指定するには、［ロギング レベル］ドロップダウン リストからロギングのレベルを選択します。詳細については、「ロギング レベル」を参照してください。

## SNMP

このウィンドウでは、SNMP の有効化、SNMP コミュニティ文字列の設定、および SNMP トラップ マネージャ情報の入力を行うことができます。

### SNMP を有効にする

SNMP のサポートを有効にする場合に選択します。SNMP のサポートを無効にする場合は選択を解除します。SNMP はデフォルトでは有効です。

### コミュニティ文字列

SNMP コミュニティ文字列は、管理情報ベース（MIB）への埋め込みパスワードです。MIB にはルータの動作に関するデータが格納され、認証されたリモートユーザだけが MIB を使用できます。コミュニティ文字列には、"public" と "private" の 2 つのタイプがあります。"public" コミュニティ文字列は、コミュニティ文字列を除く MIB 内のすべてのオブジェクトに対する読み取り専用アクセスを可能にします。一方、"private" コミュニティ文字列は、コミュニティ文字列を除く MIB 内のすべてのオブジェクトに対する読み書きアクセスを可能にします。

コミュニティ文字列の表には、設定されているすべてのコミュニティ文字列とそのタイプが表示されます。［追加］ボタンをクリックすると、［コミュニティ文字列の追加］ダイアログ ボックスが表示され、新しいコミュニティ文字列を追加できます。［編集］または［削除］ボタンをクリックすると、表で選択したコミュニティ文字列を編集または削除できます。

### トラップ レシーバ

トラップ レシーバの IP アドレス（トラップ情報の送信先アドレス）とコミュニティ文字列を入力します。これらは、通常はドメインを監視する SNMP 管理ステーションの IP アドレスです。アドレスがわからない場合は、サイト管理者に確認してください。

トラップ レシーバ情報を管理するには、[追加]、[編集]、または [削除] ボタンをクリックします。

### SNMP サーバの場所

SNMP サーバの場所を入力するためのテキスト フィールドです。これは、ルータの動作に影響を及ぼす設定パラメータではありません。

### SNMP サーバの連絡先

SNMP サーバの管理者の連絡先情報を入力するためのテキスト フィールドです。これは、ルータの動作に影響を及ぼす設定パラメータではありません。

## Netflow

このウィンドウには、Netflow が設定されているインターフェイスで、Netflow の上位トーカーを監視するためにどのようにルータが設定されているかが表示されます。表示される項目の詳細については、「Netflow トーカー」を参照してください。

Netflow のパラメータはルータ上で監視できます。また、[監視] > [インターフェイス ステータス]、および [監視] > [トラフィック ステータス] > [上位 N トラフィック フロー] で上位トーカーの統計情報を確認できます。Netflow の上位トーカーを有効化していない場合は、上位 10 のトーカーが監視されます。

### Netflow トーカー

このウィンドウでは、上位トーカーを Netflow できます。

### 上位トーカーの有効化

［上位トーカーの有効化］チェック ボックスを選択すると、Netflow が設定されているインターフェイス上で上位トーカーを監視できるようになります。

### 上位トーカー

［上位トーカー］数値ボックスには、上位トーカーの数を設定します。数値は 1 ～ 200 の範囲から選択します。Cisco CP では、設定された上位トーカーの数を上限としてデータが追跡および記録されます。

### キャッシュ タイムアウト

［キャッシュ タイムアウト］数値ボックスには、上位トーカーのキャッシュのタイムアウト値をミリ秒単位で設定します。数値は 1 ～ 3600000 の範囲から選択します。タイムアウトに到達すると、上位トーカーのキャッシュが更新されます。

### 並べ替え

［並べ替え］ドロップダウン リストからバイトまたはパケットを選択して、上位トーカーの並べ替えの基準を指定します。

# ルータ アクセス

このウィンドウには、ルータ アクセス関連機能の説明が表示されます。

## ユーザ アカウント：ルータ アクセス用のユーザ アカウントの設定

このウィンドウでは、ユーザが HTTP、Telnet、PPP、またはその他の方法でルータにログインするときに認証を受けるためのアカウントとパスワードを定義できます。

### ユーザ名

ユーザ アカウント名を入力します。

### パスワード

ユーザ アカウントのパスワードを入力します。入力したパスワードはアスタリスク（*）で表示されます。

（注）　ユーザ パスワードは、［デバイス プロパティ ― パスワード］タブで設定される enable secret パスワードとは異なるものです。指定されたユーザによるルータへのログインと限定されたコマンド セットの入力を可能にします。

### 権限レベル

ユーザの権限レベルを入力します。

### ビュー名

ユーザ アカウントに CLI ビューが関連付けられている場合は、そのビュー名がこのカラムに表示されます。ビューによって、ユーザの役割に基づく Cisco CP へのアクセス権が定義されます。詳細については、「ビューをユーザに関連付ける」を参照してください。

（注）　Cisco CP は、ユーザ定義のビューまたは変更された Cisco CP 定義のビューで起動されると、監視モードで動作します。この場合、ユーザには読み取り専用の権限が与えられます。監視可能な Cisco CP の機能は、ビューに表示されるコマンドによって決まります。すべての機能が監視に利用できるとは限りません。

### 実行する操作

| 目的： | 手順： |
|---|---|
| 新しいユーザ アカウントを追加する。 | ［追加］をクリックする。次に、［ユーザ名の追加］ウィンドウでアカウントを追加する。 |
| ユーザ アカウントを編集する。 | ユーザ アカウントを選択して［編集］をクリックする。次に、［ユーザ名の編集］ウィンドウでアカウントを編集する。 |
| ユーザ アカウントを削除する。 | ユーザ アカウントを選択して［削除］をクリックする。表示される警告ボックスで削除を確認する。 |

## ユーザ名の追加 / 編集

このウィンドウの各フィールドでは、ユーザ アカウントを追加または編集します。

### ユーザ名

このフィールドでは、ユーザ名を入力または編集します。

### パスワード

このフィールドでは、パスワードを入力または編集します。

### パスワードの確認

このフィールドにはパスワードを再入力します。パスワードと確認パスワードが一致しない場合は、［OK］をクリックするとエラー メッセージ ウィンドウが表示されます。

［OK］をクリックすると、追加または編集したアカウント情報が［Telnet のユーザ アカウントの設定］ウィンドウに表示されます。

### MD5 ハッシュ アルゴリズムを使用してパスワードを暗号化チェック ボックス

単方向の Message Digest 5（MD5）アルゴリズムを使用してパスワードを暗号化する場合に選択します。MD5 は、暗号化による強力な保護を可能にします。

**（注）** CHAP などのクリア テキスト パスワードの取得を必要とするプロトコルは、MD5 で暗号化されたパスワードと併用することはできません。MD5 の暗号化は不可逆です。したがって、パスワードをクリア テキストに戻すには、ユーザ アカウントを一度削除して、このチェック ボックスを選択しないで再作成する必要があります。

### 権限レベル

ユーザの権限レベルを入力します。CLI コマンドに権限レベルを適用すると、そのコマンドを実行できるのは、そのコマンドに対して設定された権限レベル以上の権限を持つユーザだけになります。

### ビューをユーザに関連付ける

このフィールドは、ルータ アクセスのユーザ アカウントを設定しているときに表示されます。Cisco CP の別のエリアで作業をしている場合は、表示されないことがあります。

ユーザ アクセスを特定のビューに制限する場合は、このチェック ボックスを選択します。ユーザに初めてビューを関連付ける場合は、ビュー パスワードの入力を要求されます。このオプションは、［追加タスク］ツリーの［ルータ アクセス］ノードだけで使用できます。

### ビュー名：

このユーザに関連付けるビューを次の中から選択します。

- SDM_Administrator — このビュー タイプが関連付けられたユーザは、Cisco CP への完全なアクセス権を持ち、Cisco CP でサポートされているすべての操作を実行できます。
- SDM_Monitor — このビュー タイプが関連付けられたユーザは、Cisco CP でサポートされているすべての機能を監視できます。Cisco CP を使用して設定を配信することはできません。ユーザは［インターフェイスと接続］、［ファイアウォール］、［VPN］などのさまざまな Cisco CP のエリアに移動できます。ただし、これらのエリア内のユーザ インターフェイスのコンポーネントは無効になっています。
- SDM_Firewall — このビュー タイプが関連付けられたユーザは、Cisco CP のファイアウォール機能と監視機能を使用できます。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、および ACL エディタを使用してファイアウォールと ACL を設定できます。他のエリア内のユーザ インターフェイスのコンポーネントは使用できません。
- SDM_EasyVPN_Remote — このビュー タイプが関連付けられたユーザは、Cisco CP の Easy VPN リモート機能を使用できます。Easy VPN リモート接続を作成したり、編集したりできます。他のエリア内のユーザ インターフェイスのコンポーネントは使用できません。

### 詳細

［ビューをユーザに関連付ける］エリアには、指定したビューの詳細が表示されます。指定したビューに関するさらに詳細な情報を参照するには、［詳細］ボタンをクリックします。

## ビュー パスワード

ユーザに初めてビューを関連付ける際には、Cisco CP 定義のビューに対するビュー パスワードの入力を要求されます。ビューを切り替える場合はこのパスワードを使用します。

### ビュー パスワードの入力

［ビュー パスワード］フィールドにビュー パスワードを入力します。

# vty 設定

このウィンドウには、ルータの仮想端末（vty）設定が表示されます。［プロパティ］カラムには、設定済みの回線範囲と各範囲に設定可能なプロパティが含まれます。これらのプロパティの設定は、［値］カラムに含まれます。

この表では、ルータの vty 設定が次のカラムに表示されます。

- 回線範囲 — この行の他の設定が適用される vty 接続の範囲が表示されます。
- 許可される入力プロトコル — 入力用に設定されたプロトコルが表示されます。表示される値は、Telnet、SSH、または Telnet と SSH の両方です。
- 許可される出力プロトコル — 出力用に設定されたプロトコルが表示されます。表示される値は、Telnet、SSH、または Telnet と SSH の両方です。
- EXEC タイムアウト — セッションがアイドル状態になってから終了するまでの秒数が表示されます。
- インバウンド アクセスクラス — 回線範囲のインバウンド方向に適用されるアクセス ルールの名前または番号が表示されます。
- アウトバウンド アクセスクラス — 回線範囲のアウトバウンド方向に適用されるアクセス ルールの名前または番号が表示されます。
- ACL — 設定されている場合は、vty 接続に関連付けられている ACL が表示されます。
- 認証ポリシー — この vty 回線に関連付けられている AAA 認証ポリシーです。このフィールドは、ルータに AAA が設定されている場合にだけ表示されます。
- 許可ポリシー — この vty 回線に関連付けられている AAA 許可ポリシーです。このフィールドは、ルータに AAA が設定されている場合にだけ表示されます。

**（注）** SSH を入力または出力プロトコルとして使用するには、［追加タスク］ツリーで［SSH］をクリックし、RSA キーを生成することによって SSH を有効にする必要があります。

# vty 回線の編集

このウィンドウでは、ルータの仮想端末（vty）設定を編集できます。

### 回線範囲

このウィンドウで行った設定を適用する vty 回線の範囲を入力します。

### タイムアウト

アイドル状態の接続が切断されるまでの時間を秒単位で入力します。

### 入力プロトコル

適切なチェック ボックスをクリックして入力プロトコルを選択します。

#### ［Telnet］チェック ボックス

ルータへの Telnet アクセスを可能にする場合に選択します。

#### ［SSH］チェック ボックス

SSH クライアントによるルータへのログインを可能にする場合に選択します。

### 出力プロトコル

適切なチェック ボックスをクリックして出力プロトコルを選択します。

#### ［Telnet］チェック ボックス

ルータへの Telnet アクセスを可能にする場合に選択します。

#### ［SSH］チェック ボックス

ルータと SSH クライアントの通信を可能にする場合に選択します。

### アクセス ルール

アクセス ルールを関連付けて、範囲内の vty 回線上のインバウンド トラフィックとアウトバウンド トラフィックをフィルタできます。

#### インバウンド

インバウンド トラフィックをフィルタするアクセス ルールの名前または番号を入力するか、ボタンをクリックしてアクセス ルールを参照します。

#### アウトバウンド

アウトバウンド トラフィックをフィルタするアクセス ルールの名前または番号を入力するか、ボタンをクリックしてアクセス ルールを参照します。

### 認証 / 許可

これらのフィールドは、ルータ上で AAA が有効になっている場合にだけ表示されます。AAA を有効にするには、［設定］>［セキュリティ］>［AAA］>［AAA の要約］>［AAA の有効化］の順にクリックします。

#### 認証ポリシー

この vty 回線に使用する認証ポリシーを選択します。

#### 許可ポリシー

この vty 回線に使用する許可ポリシーを選択します。

## 管理アクセス ポリシーの設定

このウィンドウでは、既存の管理アクセス ポリシーを確認したり、編集するポリシーを選択したりできます。′管理アクセス ポリシーでは、ルータのコマンドライン インターフェイスへのアクセスを許可するネットワークとホストを指定します。また、ポリシー内のホストまたはネットワークが使用できるプロトコルや管理トラフィックの伝送に使用するルータ インターフェイスも指定できます。

### ホスト / ネットワーク

ネットワーク アドレスまたはホストの IP アドレスです。ネットワーク アドレスを指定すると、ポリシーはそのネットワーク上のすべてのホストに適用されます。ホスト アドレスを指定すると、ポリシーはそのホストだけに適用されます。

ネットワーク アドレスは、次の例のように、ネットワーク番号 / ネットワーク ビットの形式で表示されます。

```
172.23.44.0/24
```

この形式および IP アドレスとサブネット マスクの使い方の詳細については、「IP アドレスとサブネット マスク」を参照してください。

### 管理インターフェイス

管理トラフィックの伝送に使用されるルータ インターフェイスです。

### 許可されるプロトコル

このカラムには、指定したホストがルータと通信するときに使用できるプロトコルが表示されます。次のプロトコルを設定できます。

- Cisco CP — 指定したホストは Cisco CP を使用できます。
- Telnet — 指定したホストは Telnet を使用してルータの CLI にアクセスできます。
- SSH — 指定したホストはセキュア シェル（SSH）を使用してルータの CLI にアクセスできます。
- HTTP — 指定したホストは Hypertext Transfer Protocol（HTTP）を使用してルータにアクセスできます。Cisco CP を指定した場合は、HTTP または HTTPS も指定する必要があります。
- HTTPS — 指定したホストは Hypertext Transfer Protocol Secure（HTTPS）を使用してルータにアクセスできます。
- RCP — 指定したホストはリモート コピー プロトコル（RCP）を使用してルータ上のファイルを管理できます。
- SNMP — 指定したホストは簡易ネットワーク管理プロトコル（SNMP）を使用してルータを管理できます。

### 追加ボタン

管理ポリシーを追加する場合にクリックし、[管理ポリシーの追加] ウィンドウでポリシーを指定します。

### 編集ボタン

管理ポリシーを編集する場合にクリックし、[管理ポリシーの編集] ウィンドウでポリシーを指定します。

### 削除ボタン

指定した管理ポリシーを削除する場合にクリックします。

### 適用ボタン

[管理ポリシーの追加 / 編集] ウィンドウでルータの設定に加えた変更を適用する場合にクリックします。

### 変更の破棄ボタン

[管理ポリシーの追加 / 編集] ウィンドウでルータの設定に加えた変更を破棄する場合にクリックします。変更は破棄され、[管理アクセス ポリシーの設定] ウィンドウから削除されます。

## 管理ポリシーの追加 / 編集

このウィンドウでは、管理ポリシーを追加または編集します。

### タイプ

ホスト アドレスとネットワーク アドレスのどちらを指定するか選択します。

### IP アドレス / サブネット マスク

［タイプ］フィールドで［ネットワーク］を選択した場合は、ホストの IP アドレスを入力するか、またはネットワーク アドレスとサブネット マスクを入力します。詳細については、「IP アドレスとサブネット マスク」を参照してください。

### インターフェイス

管理トラフィックを許可するインターフェイスを選択します。このインターフェイスは、ホストまたはネットワークからローカル ルータへの最も直接的なルートでなければなりません。

### 管理プロトコル

ホストまたはネットワークに対して許可する管理プロトコルを指定します。

#### Cisco CP を許可する

指定したホストまたはネットワークに Cisco CP へのアクセスを許可する場合に選択します。このチェック ボックスを選択すると、Telnet、SSH、HTTP、HTTPS、および RCP プロトコルが自動的に選択されます。このオプションを選択しても、他のプロトコルを許可できます。

ユーザが Cisco CP にログインするときにセキュアなプロトコルを使用するように設定するには、［セキュアなプロトコルのみ許可する］を選択します。このチェック ボックスを選択すると、SSH、HTTPS、および RCP プロトコルが自動的に選択されます。Telnet などのセキュアでないプロトコルを選択すると、Cisco CP によって［セキュアなプロトコルのみ許可する］の選択が自動的に解除されます。

#### 管理プロトコルは個別に指定可能

ホストまたはネットワークで使用可能なプロトコルを個別に指定するには、［Telnet］、［SSH］、［HTTP］、［RCP］、［SNMP］の中から該当するチェック ボックスを選択します。

［VTY］ウィンドウで Telnet と SSH が無効になっていて（選択されていない）、［SNMP プロパティ］ウィンドウで SNMP が無効になっている場合は、このウィンドウでこれらのプロトコルを選択すると、有効にすることを勧めるメッセージが表示されます。

**（注）** ルータの Cisco IOS リリースで HTTPS がサポートされていない場合は、［セキュアなプロトコルのみ許可する］および［HTTPS］オプションが無効になります。

## 管理アクセス エラー メッセージ

管理アクセス機能によって次のエラー メッセージが生成される場合があります。

### エラー メッセージ

SDM 警告：ANY は許可されていません。

**説明**　管理ポリシーの送信元または宛先ルール エントリのいずれかに「any」キーワードが含まれている場合、そのポリシーは読み取り専用です。読み取り専用のポリシーは［管理アクセス］ウィンドウで編集できません。ポリシーに「any」キーワードが含まれていると、次の理由でセキュリティ リスクが生じる可能性があります。

- 送信元に「any」が関連付けられている場合、あらゆるネットワークからのトラフィックがルータに到達できる。
- 宛先に「any」が関連付けられている場合、ルータがサポートしているネットワーク上のすべてのノードへのアクセスが許可される。

**推奨アクション**　［ルール］ウィンドウでルールを選択して［編集］をクリックすると、このメッセージの原因となったアクセス エントリを削除できます。または、［インターフェイスと接続］ウィンドウで、ルールとそのルールが適用されたインターフェイスの関連付けを解除できます。

### エラー メッセージ

SDM 警告：アクセス コントロール エントリがサポートされていません。

**説明**　管理ポリシーを適用したインターフェイスまたは vty 回線に、サポートされていないアクセス コントロール エントリ（ACE）が関連付けられている場合、管理ポリシーは読み取り専用になります。サポートされていない ACE は CLI を使用して削除できます。サポートされていない ACE とは、Cisco CP でサポートされていないキーワードまたは構文を含む ACE のことです。

### エラー メッセージ

SDM 警告：SDM は許可されていません。

**説明**　このメッセージは、このルータ上の Cisco CP へのアクセスをホストまたはネットワークに許可する管理アクセス ポリシーがまだ設定されていない場合に表示されます。

**推奨アクション**　このルータ上の Cisco CP へのアクセスを可能にするには、このようなポリシーを設定する必要があります。Cisco CP へのアクセスをホストまたはネットワークに許可する管理アクセス ポリシーが設定されていない間は、他の機能に移動することもコマンドをルータに配信することもできません。

### エラー メッセージ

SDM 警告：現在のホストは許可されていません。

**説明**　このメッセージは、このルータ上の Cisco CP へのアクセスを現在のホストまたはネットワークに許可する管理アクセス ポリシーが設定されていない場合に表示されます。

**推奨アクション**　現在のホストまたはネットワークからこのルータ上の Cisco CP にアクセスできるようにするには、このようなポリシーを作成する必要があります。作成しない場合、設定をルータに配信した時点で、ルータとの接続が切断されます。現在のホストまたはネットワークに対する管理アクセス ポリシーを今すぐ追加する場合は、[はい] をクリックします。現在のホストまたはネットワークに対する管理アクセス ポリシーを追加せずに続行する場合は、[いいえ] をクリックします。この場合、コマンドの配信中にルータとの接続が切断され、別のホストまたはネットワークを使用しないと Cisco CP にログインできなくなります。

# SSH

このルータにはセキュア シェル（SSH）サーバが実装されています。SSH サーバは、SSH クライアントが安全な暗号化された接続を確立してシスコのルータと通信できるようにします。SSH 接続では、インバウンド Telnet 接続と同様の機能が提供されますが、Cisco IOS ソフトウェア認証で使用される強力な暗号化機能も提供されます。Cisco IOS ソフトウェアの SSH サーバは、公開および商用の SSH クライアントと連携します。ルータで IPsec DES または 3DES Cisco IOS リリースが使用されていない場合、および［追加タスク］ツリーに［SSH］ブランチが表示されない場合、この機能は無効になります。

SSH では、RSA 暗号キーを使用してルータと SSH クライアント間のデータが暗号化されます。このウィンドウで RSA キーを生成すると、ルータと SSH クライアント間の SSH 通信が可能になります。

## ステータス メッセージ

**暗号キーはこのデバイスに設定されていません。**

デバイスに暗号キーが設定されていない場合に表示されます。キーが設定されていない場合は、モジュラス サイズを入力してキーを生成できます。

**RSA キーはこのルータに設定されています。**

暗号キーが生成された場合に表示されます。このルータでは SSH が有効です。

## キー モジュラス サイズ ボタン

暗号キーが生成されていない場合に表示されます。このボタンをクリックして、キーのモジュラス サイズを入力します。モジュラス値を 512 ～ 1024 の範囲内の値にする場合は、64 の倍数（整数値）を入力します。1024 より大きい値にする場合は、1536 または 2048 を入力します。512 以上の値を入力すると、キーの生成に 1 分以上かかる場合があります。

## RSA キーの生成ボタン

入力したモジュラス サイズに基づいてルータの暗号キーを生成する場合にクリックします。暗号キーが生成されている場合、このボタンは無効になります。

# DHCP 設定

このウィンドウでは、ルータの DHCP 設定を管理できます。

## DHCP プール

このウィンドウには、ルータに設定されている DHCP プールが表示されます。

### プール名

DHCP プールの名前です。

### インターフェイス

DHCP プールが設定されているインターフェイスです。このインターフェイスに接続されたクライアントは、この DHCP プールから IP アドレスを受け取ります。

### DHCP プール < *名前* > の詳細

このエリアには、< *名前* > というプールに関する次の詳細情報が表示されます。

- DHCP プール範囲 — クライアントに割り当て可能な IP アドレスの範囲。
- デフォルト ルータ IP アドレス — ルータに DHCP プールと同じサブネット内の IP アドレスが割り当てられている場合のルータのアドレス。
- DNS サーバ — ルータから DHCP クライアントに渡される DNS サーバの IP アドレス。
- WINS サーバ — ルータから DHCP クライアントに渡される WINS サーバの IP アドレス。
- ドメイン名 — ルータに設定されているドメイン名。
- リース期間 — ルータからクライアントに IP アドレスがリースされる期間。
- すべてをインポート — ルータが DHCP オプション パラメータを DHCP サーバのデータベースにインポートし、LAN 上の DHCP クライアントが IP アドレスを要求したときにこの情報を送信するかどうか。

### 追加

新しい DHCP プールを作成する場合に選択します。DHCP プール名、DHCP プールのネットワーク、DHCP プールの IP アドレス範囲、およびリース期間を指定する必要があります。オプションで、DNS サーバ、WINS サーバ、ドメイン名、およびデフォルト ルータも DHCP プールに設定できます。

### 編集

既存の DHCP プールを編集する場合に選択します。

### 削除

DHCP プールを削除する場合に選択します。

### DHCP プール ステータス

指定したプールからリースされている IP アドレスを表示するには、このボタンをクリックします。ネットワーク、IP アドレス範囲、リース期間、DNS サーバ、WINS サーバ、ドメイン名、およびデフォルト ルータ以外のパラメータが指定されている DHCP プールは、Cisco CP で読み取り専用として表示されます。また、非連続的な IP アドレス範囲が指定されている DHCP プールも読み取り専用として表示されます。

## DHCP プールの追加 / 編集

このウィンドウでは、DHCP プールを追加または編集します。Cisco CP のデフォルト プールは編集できません。

### DHCP プール名

このフィールドには、DHCP プールの名前を入力します。

### DHCP プールのネットワーク

プールの IP アドレスを取得するネットワーク（192.168.233.0 など）を入力します。個別のホストの IP アドレスは入力できません。

### サブネット マスク

サブネット マスクを入力します。255.255.255.0 と指定すると、255 個の IP アドレスを使用できるようになります。

### DHCP プール

範囲内の開始 IP アドレスと終了 IP アドレスを入力します。たとえば、ネットワークが 192.168.233.0 でサブネット マスクが 255.255.255.0 の場合、開始アドレスは 192.168.233.1、終了アドレスは 192.168.233.254 です。

### リース期間

クライアントに IP アドレスがリースされる期間を入力します。アドレスのリース期間を無期限にするか、またはリース期間を日数、時間数、および分数で指定できます。365 日、23 時間、または 59 分を超える期間は指定できません。

### DHCP オプション

DNS サーバ、WINS サーバ、ドメイン名、およびデフォルト ルータの情報を DHCP オプション フィールドに入力します。これらの値は、DHCP クライアントから IP アドレスが要求されたときに、それらのクライアントに送信されます。

#### すべての DHCP オプションを DHCP サーバ データベースにインポートする

DHCP オプション パラメータを DHCP サーバのデータベースにインポートし、LAN 上の DHCP クライアントから IP アドレスが要求されたときにこの情報も送信されるようにする場合は、このオプションをクリックします。

## DHCP バインディング

このウィンドウには、既存の手動 DHCP バインディングが表示されます。手動 DHCP バインディングでは、使用可能な DHCP プール内の IP アドレスが特定のクライアントから要求されるたびに、同じ IP アドレスを割り当てることができます。

また、新しいバインディングの追加、既存のバインディングの編集、または既存のバインディングの削除も行えます。

### バインディング名

DHCP バインディングに割り当てられた名前です。

### ホスト /IP マスク

クライアントにバインドされた IP アドレスとマスクです。

### MAC アドレス

クライアントの MAC アドレスです。

### タイプ

MAC アドレスには次のタイプがあります。

- イーサネット
  クライアントにはハードウェア アドレスが設定されています。
- IEEE802
  クライアントにはハードウェア アドレスが設定されています。
- < なし >
  クライアントにはクライアント識別子が設定されています。

### クライアント名

クライアントにオプションで割り当てられた名前です。

### 追加ボタン

新しい手動 DHCP バインディングを追加する場合にクリックします。

### 編集ボタン

指定した手動 DHCP バインディングを編集する場合にクリックします。

### 削除ボタン

指定した手動 DHCP バインディングを削除する場合にクリックします。

## DHCP バインディングの追加 / 編集

このウィンドウでは、既存の手動 DHCP バインディングを追加または編集できます。

### 名前

DHCP バインディングに設定する名前を入力します。DHCP バインディングを編集している場合、このフィールドは読み取り専用です。

### ホスト IP アドレス

クライアントにバインドする IP アドレスを入力します。クライアントが使用できる DHCP プール内のアドレスを指定する必要があります。別の DHCP バインディングで使用中のアドレスは入力しないでください。

### マスク

ホストの IP アドレスに使用されているマスクを入力します。

### 識別子

MAC アドレスが設定されたクライアントを識別する方法を、ドロップダウン リストから選択します。

### MAC アドレス

クライアントの MAC アドレスを入力します。別の DHCP バインディングで使用中のアドレスは入力しないでください。

### タイプ

［識別子］ドロップダウン メニューから［ハードウェア アドレス］を選択した場合は、［イーサネット］または IEEE802 を選択してクライアントの MAC アドレス タイプを設定します。

### クライアント名（オプション）

クライアントを識別する名前を入力します。ドメイン形式の名前ではなく、ホスト名だけを指定する必要があります。たとえば、*router* は指定できますが、*router.cisco.com* は指定できません。

# DNS プロパティ

ドメイン ネーム システム（DNS）は、インターネットのホスト名とその IP アドレスを格納したデータベースです。これらのホスト名と IP アドレスは、専用の DNS サーバに分散して格納されています。DNS を使用すると、ネットワーク ユーザは、覚えにくい IP アドレスではなく名前でホストを参照できます。このウィンドウでは、ホスト名からアドレスへの変換に DNS サーバを使用できるように設定します。

### DNS ベースのホスト名 - アドレス変換を有効にするチェック ボックス

ルータで DNS を使用できるようにする場合に選択します。DNS を使用しない場合は、選択を解除します。

### DNS IP アドレス

ルータから DNS 要求が送信される DNS サーバの IP アドレスを入力します。

DNS の IP アドレス情報を管理するには、［追加］、［編集］、または［削除］ボタンをクリックします。

# 動的 DNS 方式

このウィンドウには、動的 DNS 方式のリストが表示されます。

表示される各動的 DNS 方式では、その方式を更新したときに、［設定］>［ルータ］>［ルータ（詳細設定）］>［動的 DNS］に設定されているホスト名とドメイン名が送信されます。ただし、WAN インターフェイスの設定時に動的 DNS 方式を作成すると、［設定］>［ルータ］>［ルータ（詳細設定）］>［動的 DNS］に設定されているホスト名とドメイン名を上書きできます。この場合、指定したホスト名とドメイン名は、作成した DNS 方式にだけ適用されます。

一部の動的 DNS 方式は読み取り専用です。読み取り専用の動的 DNS 方式は CLI を使用して Cisco IOS ソフトウェアに設定されたもので、編集したり削除したりすることはできません。これらの読み取り専用方式を編集できるようにするには、CLI を使用して内部キャッシュまたはホスト グループのオプションを HTTP または IETF に変更します。

### 追加ボタン

新しい動的 DNS 方式を作成するには、［追加］ボタンをクリックします。

### 編集ボタン

動的 DNS 方式を編集するには、編集する方式を既存の動的 DNS 方式のリストから選択し、［編集］をクリックします。

### 削除ボタン

動的 DNS 方式を削除するには、削除する方式を既存の動的 DNS 方式のリストから選択し、［削除］をクリックします。

**（注）** 1 つ以上のインターフェイスに関連付けられている動的 DNS 方式を削除しようとすると、警告メッセージが表示されます。

# 動的 DNS 方式の追加 / 編集

このウィンドウでは、動的 DNS 方式を追加または編集できます。［HTTP］または［IETF］を選択して、方式のタイプを設定してください。

### HTTP

動的 DNS 方式のタイプを HTTP に設定すると、関連するインターフェイスの IP アドレスが変更されたときに、DNS サービス プロバイダが更新されます。

### サーバ

HTTP を使用する場合、DNS サービス プロバイダのドメイン アドレスをドロップダウン メニューから選択します。

### ユーザ名

HTTP を使用する場合、DNS サービス プロバイダへのアクセスに使用するユーザ名を入力します。

### パスワード

HTTP を使用する場合、DNS サービス プロバイダへのアクセスに使用するパスワードを入力します。

### IETF

動的 DNS 方式のタイプを IETF に設定すると、関連するインターフェイスの IP アドレスを変更したときに、DNS サーバが更新されます。

IETF を使用する場合、［設定］>［ルータ］>［DNS］でルータ用の DNS サーバを設定します。