ルータ デバイス管理

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

この章は次のトピックで構成されています。

Cisco IOS ルータにおける AAA

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、バグの修正や拡張はサポートしていません。

認証、許可、アカウンティング（AAA）ネットワーク セキュリティ サービスは、Cisco IOS ルータのアクセス コントロールを設定する際に使用する主要なフレームワークを提供します。Security Manager で AAA ポリシーを使用すると、Cisco IOS ルータ上の AAA 機能をイネーブルにしたり、デフォルトの AAA 設定を指定したりできます。このポリシーで定義したデフォルト設定は、HTTP や回線アクセス（コンソールと VTY）のポリシーなど、他のポリシーで使用できます。AAA 機能をイネーブルにすることは、NAC、SDP、802.1x などの AAA を利用するデバイス ポリシーの前提条件です。

AAA の詳細については、次を参照してください。

- サポートされる認可タイプ （3 ページ）
- サポートされるアカウンティング タイプ （3 ページ）
- 方式リストについて （4 ページ）

AAA ポリシーの設定については、次を参照してください。

- AAA サービスの定義 （5 ページ）

関連項目

- AAA サーバおよびサーバ グループ オブジェクトについて
- Cisco IOS ルータにおける回線アクセス （45 ページ）

サポートされる認可タイプ

AAA 認可を使用すると、認証済みのユーザが利用できるサービスを制限できます。Security Manager では、次のタイプの認可がサポートされます。

- ネットワーク：PPP、SLIP、ARAP などのさまざまなタイプのネットワーク接続を認可します。
- EXEC：EXEC（CLI）セッションの起動を認可します。
- コマンド：特定の権限レベルに関連付けられているすべての EXEC モード コマンドの使用を認可します。

認可を有効にすると、ルータはユーザーのプロファイルから取得した情報を使用してユーザーセッションを設定します。プロファイルは、ローカルユーザデータベースまたはセキュリティサーバにあります。ユーザに要求したサービスへのアクセス権が付与されるのは、プロファイルで許可されている場合だけです。

関連項目

- サポートされるアカウンティング タイプ （3 ページ）
- 方式リストについて （4 ページ）
- AAA サービスの定義 （5 ページ）
- Cisco IOS ルータにおける AAA （2 ページ）

サポートされるアカウンティング タイプ

AAA アカウンティングを使用すると、ユーザがアクセスしているサービスとそれらのサービスが消費しているネットワーク リソースの量を追跡できます。Security Manager では、次のアカウンティング タイプがサポートされます。

- 接続：Telnet、Local-Area Transport（LAT; ローカルエリア トランスポート）、TN3270、Packet Assembler/Disassembler（PAD; パケット アセンブラ/ディスアセンブラ）、rlogin 接続など、このデバイスから確立されたすべてのアウトバウンド接続に関する情報を記録します。

たとえば、アウトバウンド Telnet 接続の RADIUS 接続アカウンティング レコードには、Network Access Server（NAS; ネットワーク アクセス サーバ）のポートや IP アドレス、接続の開始時刻と終了時刻、ユーザの ID、セッション中に送信されたパケットの数などの情報が含まれます。

- EXEC：ユーザ名、日付、開始時刻と終了時刻、NAS の IP アドレスなど、デバイス上のユーザ EXEC（CLI）セッションに関する情報を記録します。ダイヤルインユーザの場合、レコードには、コールの発信元の電話番号が含まれます。
- コマンド：特定の権限レベルを持つユーザがデバイスで実行する EXEC コマンドに関する情報を記録します。各コマンド アカウンティング レコードには、その権限レベルに対し

て実行されたコマンドのリスト、各コマンドが実行された日時、およびそのコマンドを実行したユーザの名前が含まれます。

アカウンティング タイプごとに、アカウンティング レコードを各ユーザ セッションの開始時と終了時に生成するか、または終了時にだけ生成するかを選択できます。

AAAアカウンティングをイネーブルにすると、ルータはユーザアクティビティのアカウンティング レコードをTACACS+またはRADIUSセキュリティ サーバに送信します。各アカウンティング レコードにはアカウンティングのAttribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。このデータをあとでネットワーク管理、クライアント請求、および監査のために分析できます。

関連項目

- サポートされるアカウンティング タイプ （3 ページ）
- 方式リストについて （4 ページ）
- AAA サービスの定義 （5 ページ）
- Cisco IOS ルータにおける AAA （2 ページ）

方式リストについて

方式リストは、特定の AAA 機能を実行するために使用する方式を記述した順序付きリストです。Security Manager では、AAA サーバ グループを選択して方式リストを定義します。AAA サーバ グループは、一般に RADIUS や TACACS+ などの同じプロトコルを実行している 1 つ以上のAAAサーバを含む再利用可能なオブジェクトです。方式リストを使用すると、各AAA機能に使用するセキュリティプロトコルを1つ以上指定できるため、最初の方式が失敗した場合のバックアップ システムを確保できます。

（注） Security Managerには、イネーブルパスワードまたはローカルデータベースを使用するための定義済みの AAA サーバ グループ オブジェクトもあります。定義済みの AAA 認証サーバ グループを参照してください。

各 AAA 機能について、デバイスは最初にリストに定義されている最初の方式を使用します。その方式で応答がない場合、デバイスはリスト内の次の方式を選択します。このプロセスは、リスト内の方式との通信に成功するまで、または方式リストに定義されているすべての方式が試されるまで続行されます。

（注） デバイスは、前の方式で応答がない場合にだけリスト内の次の方式と通信しようとします。AAA サービスがこのサイクルのある時点で失敗した場合、つまり、セキュリティ サーバまたはローカル ユーザ名データベースの応答でユーザ アクセスまたはサービスが拒否された場合、プロセスは停止し、他の方式は試されません。

関連項目

- サポートされる認可タイプ （3 ページ）
- サポートされるアカウンティング タイプ （3 ページ）
- AAA サービスの定義 （5 ページ）
- Cisco IOS ルータにおける AAA （2 ページ）

AAA サービスの定義

Cisco IOS ルータで AAA サービスを定義するには、まずルータで AAA 機能をイネーブルにする必要があります。その後、デバイスで実装する機能の種類（認証、許可、アカウンティング）を定義できます。各機能の方式リスト（イネーブルにする認可およびアカウンティングのタイプごとのリストなど）を定義する必要があります。

たとえば、EXEC 認可とコマンド認可を設定する場合は、EXEC 認可用に 1 つの方式リストを定義し、コマンド認可を実行する権限レベルごとに他の方式リストを定義する必要があります。

（注） 認証に RADIUS を使用する場合は、認可にも同じ RADIUS サーバ グループを使用する必要があります。

関連項目

- 方式リストについて （4 ページ）
- Cisco IOS ルータにおける AAA （2 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [AAA]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [AAA]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[AAA] ページが表示されます。このページのフィールドの説明については、[AAA] ポリシー ページ （7 ページ）を参照してください。

ステップ 2 デバイスにアクセスするユーザに対して使用するログイン認証方式を定義します。

a) [認証（Authentication）] タブ（[AAA] ページ - [Authentication] タブ （8 ページ）を参照）で、[デバイスログイン認証の有効化（Enable Device Login Authentication）] チェックボックスをオンにします。

b) 1 つ以上の AAA サーバーグループ オブジェクト（最大 4 つ）の名前を [優先順位付けされた方式リスト（Prioritized Method List）] フィールドに入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。

（注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。

ステップ 3 （任意）[Maximum Number of Attempts] フィールドで、許可する認証試行の失敗回数の最大数を定義します。その回数を超えると、ユーザはロックアウトされます。

ステップ 4 （任意）正常に認証されたユーザに対して使用する認可方式を定義します。

a) [AAA] ページの [許可（Authorization）] タブをクリックします。このタブのフィールドの説明については、表 3 : [AAA] ページ - [Authorization] タブ （10 ページ）を参照してください。

b) 次の 1 つ以上の認可タイプの方式リストを定義します。

- ネットワーク（Network）
- EXEC
- コマンド : [追加（Add）] ボタンをクリックして、[コマンド許可（Command Authorization）] ダイアログボックス（[Command Authorization] ダイアログボックス （11 ページ）を参照）を表示します。ここから、権限レベルとそれに適用する方式リストを選択できます。

これらの認可タイプの詳細については、サポートされる認可タイプ （3 ページ）を参照してください。

（注） RADIUS では、認証と認可に同じサーバが使用されます。したがって、認証に RADIUS 方式リストを定義する場合は、認可にも同じ方式リストを定義する必要があります。

ステップ 5 （任意）ユーザによって実行されるアクティビティに対して使用するアカウンティング方式を定義します。

a) [AAA] ページの [アカウンティング（Accounting）] タブをクリックします。このタブのフィールドの説明については、表 5 : [AAA] ページ - [Accounting] タブ （13 ページ）を参照してください。

b) 次の 1 つ以上のアカウンティング タイプの方式リストを定義します。

- Connection
- EXEC
- コマンド : [追加（Add）] ボタンをクリックして、[コマンドアカウンティング（Command Accounting）] ダイアログボックス（[Command Accounting] ダイアログボックス （15 ページ）を参照）を表示します。ここから、権限レベルとそれに適用する方式リストを選択できます。

これらのアカウンティング タイプの詳細については、サポートされるアカウンティング タイプ （3 ページ）を参照してください。

c) 前の手順で定義した各アカウンティング タイプについて、[Accounting Process Notices] リストから値を選択します。これにより、アカウンティング レコードをユーザ プロセスの開始時と終了時に作成するか、または終了時にだけ作成するかを定義します。

d) 前の手順で定義した各アカウンティングタイプについて、方式リストに定義されている各 AAA サーバーグループ内の最初のサーバに同時にアカウンティング情報を送信する場合は、[複数サーバーへのブロードキャストを有効化（Enable broadcast to multiple servers）] チェックボックスをオンにします。

[AAA] ポリシー ページ

[AAA] ページでは、ルータで使用するデフォルトの認証、許可、アカウンティング方式を定義します。この定義は、使用する方式とその方式を使用する順序を定義する方式リストを設定することによって行います。

（注） このポリシーに定義された方式リストは、ルータのコンソールポートおよび VTY 回線の AAA を設定するときに、デフォルト設定として使用できます。 [Console] ポリシー ページ （53 ページ）および [VTY] ポリシー ページ （65 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]>[デバイス管理（Device Admin）] > [AAA]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [AAA]** を選択します。[AAA] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存ポリシーを選択します。

関連項目

- Cisco IOS ルータにおける AAA （2 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて
- [Console] ポリシー ページ （53 ページ）
- [VTY] ポリシー ページ （65 ページ）

フィールド リファレンス

表 1 : [AAA] ページ

要素	説明
[Authentication] タブ	使用するログイン認証方式とそれらの認証方式を使用する順序を定義します。 [AAA] ページ - [Authentication] タブ （8 ページ）を参照してください。

要素	説明
[Authorization] タブ	実行するネットワーク認可、EXEC 認可、およびコマンド認可のタイプと各タイプに使用する方式を定義します。 [AAA] ページ - [Authorization] タブ （9 ページ）を参照してください。
[Accounting] タブ	実行する接続、EXEC、およびコマンド アカウンティングのタイプと各タイプに使用する方式を定義します。 [AAA] ページ - [Accounting] タブ （12 ページ） を参照してください。

[AAA] ページ - [Authentication] タブ

[AAA] ページの [Authentication] タブでは、デバイスにアクセスするユーザの認証に使用する方式を定義します。認証方式は、LDAP、RADIUS、および TACACS+ などの使用するセキュリティ プロトコルを定義する方式リストで定義します。

（注） コンソールおよびデバイスとの通信に使用される VTY 回線でこのポリシーに定義された方式リストを使用できます。 [Console] ポリシー ページ （53 ページ）および [VTY Line] ダイアログボックス - [Authentication] タブ （70 ページ）を参照してください。

ナビゲーション パス

[AAA] ポリシー ページ （7 ページ）に移動し、[認証（Authentication）] タブをクリックします。

関連項目

- AAA サービスの定義 （5 ページ）
- 方式リストについて （4 ページ）
- [AAA Server Group] ダイアログボックス
- 定義済みの AAA 認証サーバ グループ

フィールド リファレンス

表 2 : [AAA] ページ - [Authentication] タブ

要素	説明
Enable Device Login Authentication	選択すると、デバイスへのログイン時に、方式リストに定義されている方式を使用したすべてのユーザの認証がイネーブルになります。 選択を解除すると、認証は実行されません。

要素	説明
Prioritized Method List	ユーザを認証する場合に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）]をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバグループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認証を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 サポートされる方式には、[Line]、[Local]、[Kerberos]、[LDAP]、[RADIUS]、[TACACS+]、および [None] があります。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。
Maximum Number of Attempts	認証試行の失敗回数の最大数を定義します。その回数を超えると、ユーザはロックアウトされます。この機能は、デフォルトではディセーブルになっています。有効値の範囲は 1 ～ 65535 です。 （注） ユーザから見ると、通常の認証失敗と、ロックアウトによる認証失敗に違いはありません。システム管理者は、**clear** コマンドを使用して、ロックアウトされたユーザーのステータスを明示的にクリアする必要があります。

[AAA] ページ - [Authorization] タブ

[AAA] ページの [Authorization] タブでは、デバイスに対してイネーブルにする認可サービスのタイプと各タイプで使用する方式を定義します。Security Manager では、次のタイプの認可がサポートされます。

- ネットワーク：PPP などのさまざまなタイプのネットワーク接続を認可します。
- EXEC：EXEC セッションの起動を認可します。
- コマンド：特定の権限レベルに関連付けられているすべての EXEC モード コマンドの使用を認可します。

（注） コンソールおよびデバイスの通信に使用される VTY 回線でこのポリシーに定義された方式リストを使用できます。[Console] ポリシー ページ （53 ページ）および [VTY Line] ダイアログボックス - [Authentication] タブ （70 ページ）を参照してください。

ナビゲーション パス

[AAA] ポリシー ページ （7 ページ）に移動し、 [承認（Authorization）] タブをクリックします。

関連項目

- AAA サービスの定義 （5 ページ）
- サポートされる認可タイプ （3 ページ）
- 方式リストについて （4 ページ）
- [AAA Server Group] ダイアログボックス
- テーブルのフィルタリング

フィールド リファレンス

表 3 : [AAA] ページ - [Authorization] タブ

要素	説明
[Network Authorization] 設定	
Enable Network Authorization	選択すると、方式リストに定義されている方式を使用した PPP、SLIP、ARAP 接続などのネットワーク接続の認可がイネーブルになります。 選択を解除すると、ネットワーク認可は実行されません。
Prioritized Method List	ユーザを認可する場合に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（最大 4 つ）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバー グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認可を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 サポートされる方式には、[LDAP]、[RADIUS]、[TACACS+]、[Local]、および [None] があります。 （注） RADIUS では、認証と認可に同じサーバが使用されます。したがって、認証に RADIUS 方式リストを定義する場合は、認可にも同じ方式リストを定義する必要があります。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。

要素	説明
[EXEC Authorization] 設定	
Enable CLI/EXEC Operations Authorization	選択すると、このタイプの認可は、方式リストに定義されている方式を使用して、EXEC（CLI）セッションを開くことをユーザに許可するかどうかを決定します。 選択を解除すると、EXEC 認可は実行されません。
Prioritized Method List	ユーザを認可する場合に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（最大 4 つ）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクトセレクタの上向きおよび下向き矢印を使用して、選択したサーバグループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認可を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。
[Command Authorization] 設定	
特権レベル	コマンド認可定義が適用される権限レベル。
Prioritized Method List	この権限レベルでユーザを認可するときに使用する方式リスト。
[追加（Add）] ボタン	[Command Authorization] ダイアログボックス （11 ページ）が開きます。ここから、コマンド認可定義を設定できます。
[編集（Edit）] ボタン	[Command Authorization] ダイアログボックス （11 ページ）が開きます。ここから、コマンド認可定義を編集できます。
[削除（Delete）] ボタン	選択したコマンド認可定義をテーブルから削除します。

[Command Authorization] ダイアログボックス

[Command Authorization] ダイアログボックスでは、特定の権限レベルに関連付けられている EXEC コマンドを認可するときに使用する方式を定義します。これにより、特定の権限レベル（0 ～ 15）に関連付けられているすべてのコマンドを認可できます。

ナビゲーション パス

[AAA] ページ - [Authorization] タブ （9 ページ）で、[コマンド認可（Command Authorization）] テーブルの下にある [追加（Add）] ボタンをクリックします。

関連項目

- AAA サービスの定義　（5 ページ）
- サポートされる認可タイプ　（3 ページ）
- 方式リストについて　（4 ページ）

フィールド リファレンス

表 4 : [Command Authorization] ダイアログボックス

要素	説明
Privilege Level	コマンド アカウンティング リストを定義する権限レベル。有効値の範囲は 0 ～ 15 です。
Prioritized Method List	ユーザを認可する場合に使用する方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認可を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 サポートされる方式には、[TACACS+]、[Local]、および [None] が含まれます。 （注）　方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。

[AAA] ページ - [Accounting] タブ

[AAA] ページの [Accounting] タブでは、デバイスに対してイネーブルにするアカウンティング サービスのタイプと各タイプで使用する方式を定義します。Security Manager では、次のタイプのアカウンティングがサポートされます。

- 接続：このデバイスから確立されたすべてのアウトバウンド接続に関する情報を記録します。
- EXEC：ユーザ名、日付、開始時刻と終了時刻、IP アドレスなど、デバイス上のユーザ EXEC セッションに関する情報を記録します。
- コマンド：特定の権限レベルを持つユーザがデバイスで実行する EXEC コマンドに関する情報を記録します。

さらに、[Accounting] ページでは、アカウンティング レコードをいつ生成し、それらのレコードを複数の AAA サーバにブロードキャストするかどうかを指定します。

（注） コンソールおよびデバイスの通信に使用される VTY 回線でこのポリシーに定義された方式リストを使用できます。[Console] ポリシー ページ （53 ページ）および [VTY Line] ダイアログボックス - [Authentication] タブ （70 ページ）を参照してください。

ナビゲーション パス

[AAA] ポリシー ページ （7 ページ）に移動し、[アカウンティング（Accounting）] タブをクリックします。

関連項目

- AAA サービスの定義 （5 ページ）
- サポートされるアカウンティング タイプ （3 ページ）
- 方式リストについて （4 ページ）
- [AAA Server Group] ダイアログボックス
- テーブルのフィルタリング

フィールド リファレンス

表 5 : [AAA] ページ - [Accounting] タブ

要素	説明
[Connection Accounting] 設定	
Enable Connection Accounting	選択すると、方式リストに定義されている方式を使用した、このデバイスを介して確立されたアウトバウンド接続（Telnet など）に関する情報の記録がイネーブルになります。 選択を解除すると、接続アカウンティングは実行されません。

要素	説明
Generate Accounting Records for	デバイスがアカウンティング通知をアカウンティング サーバにいつ送信するかを定義します。 • [Start and Stop]：ユーザ プロセスの開始時と終了時にアカウンティング レコードを生成します。アカウンティングサーバーが「start」アカウンティングレコードを受信するかどうかにかかわらず、ユーザープロセスが開始されます。 • [Stop Only]：ユーザ プロセスの終了時にだけアカウンティング レコードを生成します。 • [None]：このタイプのアカウンティングをディセーブルにします。
Prioritized Method List	ユーザの接続アカウンティング レコードの作成時に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（IOS 12.4(22)T+ の場合は 10 個まで、それ以外は 4 個まで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 サポートされる方式には、LDAP、RADIUS および TACACS+ が含まれます。
Enable Broadcast to Multiple Servers	選択されている場合、複数の AAA サーバへのアカウンティング レコードの送信をイネーブルにします。アカウンティング レコードは、方式リストに定義されている各 AAA サーバ グループ内の最初のサーバに同時に送信されます。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。 選択解除されている場合、アカウンティング レコードは、方式リストに定義されている最初の AAA サーバ グループ内の最初のサーバにだけ送信されます。
[EXEC Accounting] 設定	
Enable CLI/EXEC Operations Accounting	選択すると、方式リストに定義されている方式を使用したユーザEXEC セッションに関する基本情報の記録がイネーブルになります。 選択を解除すると、EXEC アカウンティングは実行されません。
Generate Accounting Records for	表 1を参照してください。

要素	説明
Prioritized Method List	ユーザの接続アカウンティング レコードの作成時に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（IOS 12.4(22)T+ の場合は 10 個まで、それ以外は 4 個まで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。
Enable Broadcast to Multiple Servers	選択されている場合、複数の AAA サーバへのアカウンティング レコードの送信をイネーブルにします。アカウンティング レコードは、方式リストに定義されている各 AAA サーバ グループ内の最初のサーバに同時に送信されます。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。
[Command Accounting] 設定	
特権レベル	コマンド認可定義が適用される権限レベル。
Generate Accounting Records for	プロセスで、デバイスがアカウンティング通知をアカウンティング サーバに送信するポイント。
Enable Broadcast	アカウンティング レコードが複数のサーバに同時にブロードキャストされるかどうか。
Prioritized Method List	この権限レベルでユーザを認可するときに使用する方式リスト。
[追加（Add）] ボタン	[Command Accounting] ダイアログボックス （15 ページ）が開きます。ここから、コマンド アカウンティング定義を設定できます。
[編集（Edit）] ボタン	[Command Accounting] ダイアログボックス （15 ページ）が開きます。ここから、コマンド アカウンティング定義を編集できます。
[削除（Delete）] ボタン	選択したコマンドアカウンティング定義をテーブルから削除します。

[Command Accounting] ダイアログボックス

[Command Accounting] ダイアログボックスでは、特定の権限レベルに対して実行される EXEC コマンドに関する情報を記録するときに使用する方式を定義します。各アカウンティング レコードには、その権限レベルに対して実行されるコマンドのリストと、各コマンドが実行された日時およびそのコマンドを実行したユーザ名が含まれます。

ナビゲーション パス

[AAA] ページ - [Accounting] タブ （12 ページ）で、[コマンドアカウンティング（Command Accounting）] テーブルの下にある [追加（Add）] ボタンをクリックします。

関連項目

- AAA サービスの定義 （5 ページ）
- サポートされるアカウンティング タイプ （3 ページ）
- 方式リストについて （4 ページ）

フィールド リファレンス

表 *6 : [Command Accounting]* ダイアログボックス

要素	説明
Privilege Level	コマンド アカウンティング リストを定義する権限レベル。有効値の範囲は 0 ～ 15 です。
Generate Accounting Records for	デバイスがアカウンティング通知をアカウンティング サーバにいつ送信するかを定義します。 • [Start and Stop]：ユーザ プロセスの開始時と終了時にアカウンティング レコードを生成します。アカウンティングサーバーが「start」アカウンティングレコードを受信するかどうかにかかわらず、ユーザープロセスが開始されます。 • [Stop Only]：ユーザ プロセスの終了時にだけアカウンティング レコードを生成します。 • [None]：アカウンティング レコードは生成されません。

要素	説明
Prioritized Method List	ユーザのアカウンティング レコードの作成時に使用する方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（IOS 12.4(22)T+ の場合は 10 個まで、それ以外は 4 個まで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してアカウンティングの実行を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 サポートされる方式は [TACACS+] だけですが、[TACACS+] が設定された複数の AAA サーバ グループを選択できます。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。
Enable Broadcast to Multiple Servers	選択されている場合、複数の AAA サーバへのアカウンティング レコードの送信をイネーブルにします。アカウンティング レコードは、方式リストに定義されている各 AAA サーバ グループ内の最初のサーバに同時に送信されます。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。 選択解除されている場合、アカウンティング レコードは、方式リストに定義されている最初の AAA サーバ グループ内の最初のサーバにだけ送信されます。

Cisco IOS ルータにおけるユーザ アカウントおよびデバイス クレデンシャル

アカウントおよびクレデンシャル ポリシーでは、各ユーザ アカウントに与えられた権限レベルなど、ルータにアクセスするための接続情報を定義します。ユーザ アカウントは、必要な数だけ設定できます。ただし、Security Manager がルータへの接続に使用するユーザ アカウントは、常に [Device Properties] ページで設定されているアカウントです。

さらに、デバイス アクセス ポリシーを使用して、特権 EXEC モードへのアクセスに必要なイネーブル パスワードまたはイネーブル シークレット パスワードを定義します。このモードは、ルータの設定変更に必要です。

（注） このポリシーを使用してパスワードを定義する場合、次の展開までは置換ポリシーを割り当てずにこのポリシーの割り当てを解除しないように注意してください。このパスワードを削除するデバイス アクセス ポリシーを展開したときに、Security Manager が認識できない別のタイプのパスワード（ライン コンソール パスワードなど）がデバイスに含まれている場合、今後このデバイスを設定できなくなります。これは、Security Manager が以前に設定したイネーブル パスワードを削除すると、デバイスによってパスワードがこの認識できないパスワードに戻されるためです。

関連項目

- アカウントおよびクレデンシャル ポリシーの定義 （18 ページ）

アカウントおよびクレデンシャル ポリシーの定義

ここでは、Cisco IOS ルータにデバイス アクセス ポリシーを定義する方法について説明します。ルータに接続するために [Device Properties] ページで設定したユーザ名（デバイス プロパティの表示または変更を参照）が、このポリシーで定義したユーザ アカウントのいずれかと一致する場合、Security Manager はポリシー定義に従ってデバイス クレデンシャルを更新します。

Security Manager がデバイスへの設定の展開に使用するデバイス プロパティで定義したユーザのパスワードを変更する場合、またはイネーブル パスワードを変更する場合は、Security Manager は、デバイス プロパティで定義された既存のクレデンシャルを使用して、デバイスにログインし、変更を展開します。展開に成功したら、デバイス プロパティは、新しい設定を使用するように変更されます。デバイス プロパティのクレデンシャルの詳細については、[Device Credentials] ページを参照してください。

（注） 暗号化されたパスワードは検出できますが、入力するパスワードはクリア テキストである必要があります。暗号化されたパスワードを検出し、そのパスワードを変更した場合、パスワードはクリア テキストで保存されます。

関連項目

- Cisco IOS ルータにおけるユーザ アカウントおよびデバイス クレデンシャル （17 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイス ビュー）デバイス ポリシー セレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [アカウントおよびログイン情報（Accounts and Credentials）]** を選択します。

- （ポリシービュー）ポリシータイプセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [アカウントおよびログイン情報（Accounts and Credentials）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Accounts and Credentials] ページが表示されます。このページのフィールドの説明については、表 7 : [Accounts and Credentials] ページ （21 ページ）を参照してください。

ステップ 2 ルータで特権 EXEC モードに切り替えるためのパスワードを入力します。

a) [パスワードの有効化（Enable Password）] または [シークレットパスワードの有効化（Enable Secret Password）] を選択します。[Enable Secret Password] オプションを選択すると、MD5 暗号化を使用してパスワードが保存されるため、[Enable Password] オプションよりもセキュリティが向上します。このオプションは、パスワードがネットワークをまたがって使用される場合、または TFTP サーバに格納される場合に役立ちます。

（注） イネーブル シークレット パスワードを設定したあとは、イネーブル シークレットがディセーブルになっている場合、または古い rxboot イメージを実行しているときなど、Cisco IOS ソフトウェアの古いバージョンが使用されている場合にだけイネーブル パスワードに切り替えることができます。

b) パスワードを入力し、[Confirm] フィールドにパスワードを再入力します。入力するパスワードはクリアテキストである必要があります。イネーブル シークレット パスワードを設定すると、パスワードは展開時に暗号化されます。

ステップ 3 （任意）[パスワード暗号化サービスを有効にする（Enable Password Encryption Service）] チェックボックスをオンにして、デバイス上のすべてのパスワードを暗号化します。たとえば、イネーブル パスワード、ユーザ名パスワード、認証キー パスワード、コンソールと VTY 回線アクセス パスワード、BGP ネイバー パスワードなどがあります。

未認可ユーザによる設定ファイル内のパスワードの表示を防ぐために、この機能を使用することを推奨します。

（注） このオプションでは、高レベルのセキュリティは確保されません。したがって、このオプションを他のネットワーク セキュリティ対策の代わりに使用しないでください。

ステップ 4 ルータの新しいユーザ アカウントを定義するには、次の手順を実行します。

a) テーブルの下にある [追加（Add）] ボタンをクリックして、[ユーザーアカウント（User Accounts）] ダイアログボックスを表示します。

b) 新規ユーザの詳細を入力します。使用可能なフィールドの説明については、表 8 : [User Account] ダイアログボックス （23 ページ）を参照してください。

c) [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義が [User Accounts] テーブルに表示されます。

（注） ユーザーアカウントを編集するには、[ユーザーアカウント（User Accounts）] テーブルからユーザーアカウントを選択し、[編集（Edit）] をクリックします。ユーザーアカウントを削除するには、そのアカウントを選択し、[削除（Delete）] をクリックします。

注意 ユーザーアカウントの削除中に Cisco Security Manager がタイムアウトになり、展開が失敗します。これを回避するには、エラーが発生してもダウンロードするように Security Manager をセットアップします。Configuration Manager の [ツール（Tools）] > [管理者（Administrator）] > [展開（Deployments）] で、[エラー時にダウンロードを許可（Allow Download on Error）] をオンにします。

[アカウントおよびログイン情報ポリシー（Accounts and Credentials Policy）] ページ

[Accounts and Credentials] ページでは、ルータに割り当てるイネーブル パスワードまたはイネーブル シークレット パスワードを定義します。さらに、ルータへのアクセスに使用できるユーザ名のリストを定義できます。

詳細については、アカウントおよびクレデンシャル ポリシーの定義 （18 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [アカウントおよびログイン情報（Accounts and Credentials）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [アカウントおよびログイン情報（Accounts and Credentials）]** を選択します。[アカウントおよびログイン情報（Accounts and Credentials）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータにおけるユーザ アカウントおよびデバイス クレデンシャル （17 ページ）
- [User Account] ダイアログボックス （22 ページ）
- テーブル カラムおよびカラム見出しの機能
- テーブルのフィルタリング

フィールド リファレンス

表 *7 : [Accounts and Credentials]* ページ

要素	説明
イネーブル シークレット パスワード（Enable Secret Password）	ルータで特権 EXEC モードを開始するためのイネーブル シークレット パスワード。このオプションを選択すると、[Enable Password] オプションを選択する場合よりもセキュリティが向上します。 イネーブル シークレット パスワードには、1 ～ 25 文字の英数字を使用できます。最初の文字は文字である必要があります。スペースは使用できますが、先頭のスペースは無視されます。疑問符も使用できます。 （注） 暗号化されたパスワードは検出できますが、入力するパスワードはクリア テキストである必要があります。暗号化されたパスワードを変更した場合、パスワードはクリア テキストで保存されます。 （注） イネーブル シークレット パスワードを設定したあとは、イネーブル シークレットがディセーブルになっている場合、または古い rxboot イメージを実行しているときなど、Cisco IOS ソフトウェアの古いバージョンが使用されている場合にだけイネーブル パスワードに切り替えることができます。
パスワードを有効にする（Enable Password）	ルータで特権EXECモードを開始するためのイネーブル パスワード。 イネーブル パスワードには、1 ～ 25 文字の英数字を使用できます。最初の文字は文字である必要があります。スペースは使用できますが、先頭のスペースは無視されます。疑問符も使用できます。 （注） パスワードはクリア テキストで入力する必要があります。
Enable Password Encryption Service	選択すると、選択しなければクリアテキストで保存されるイネーブル パスワードなど、デバイス上のすべてのパスワードが暗号化されます。 たとえば、このオプションを使用して、ユーザ名パスワード、認証キー パスワード、コンソールおよびVTY回線アクセス パスワード、およびBGPネイバーパスワードを暗号化します。このオプションは、主に未認可ユーザによる設定ファイル内のパスワードの表示を防ぐために使用します。 選択を解除すると、デバイスパスワードは暗号化されずに設定ファイルに保存されます。 （注） このオプションでは、高レベルのネットワーク セキュリティは確保されません。他のネットワーク セキュリティ対策も必要になります。

要素	説明
[User Accounts] テーブル	
ユーザー名	ルータへのアクセスに使用できるユーザ名。ユーザ名は、長さが最大64文字の1つの単語にする必要があります。スペースと引用符は使用できません。
暗号化（Encryption）	MD5 暗号化を使用してユーザのパスワード情報が暗号化されるかどうかを示します。
特権レベル	ユーザに割り当てられる権限レベル。
[追加（Add）] ボタン	[User Account] ダイアログボックス （22 ページ）が開きます。ここから、ユーザ アカウントを定義できます。
[編集（Edit）] ボタン	[User Account] ダイアログボックス （22 ページ）が開きます。ここから、選択したユーザを編集できます。
[削除（Delete）] ボタン	選択したユーザ アカウントをテーブルから削除します。

[User Account] ダイアログボックス

[User Account] ダイアログボックスでは、Security Manager でルータへのアクセスに使用できるユーザ名とパスワードの組み合わせを定義します。ユーザアカウントの権限レベルを定義することもできます。これにより、このルータ上のすべてのコマンドを設定できるか、またはそのサブセットだけを設定できるかが決まります。

（注） CLI などの他の方法を使用して、ルータに他のユーザ アカウントが定義されている場合があります。

ナビゲーション パス

[アカウントおよびログイン情報ポリシー（Accounts and Credentials Policy）] ページ （20 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- アカウントおよびクレデンシャル ポリシーの定義 （18 ページ）
- Cisco IOS ルータにおけるユーザ アカウントおよびデバイス クレデンシャル （17 ページ）
- FlexConfig ポリシーとポリシー オブジェクトについて

フィールド リファレンス

表 *8 : [User Account]* ダイアログボックス

要素	説明
[ユーザー名（Username）]	ルータにアクセスするためのユーザ名。
パスワード	このユーザ アカウントでルータにアクセスするためのパスワード。 （注） 暗号化されたパスワードは検出できますが、入力するパスワードはクリア テキストである必要があります。
確認（Confirm）	このユーザ アカウントのパスワードを確認します。
Ecrypt password using MD5	選択すると、MD5 暗号化を使用してこのユーザ アカウントのパスワードが暗号化されます。これがデフォルトです。 選択を解除すると、パスワードは暗号化されずにルータに送信されます。
特権レベル	ユーザ アカウントに割り当てられる権限レベル。有効値の範囲は 0 ～ 15 です。 • 0：**disable**、**enable**、**exit**、**help**、および **logout** の各コマンドにだけアクセス権を付与します。 • 1：ルータへの権限なしアクセスをイネーブルにします（通常の EXEC モードでは権限が使用されます）。 • 15：ルータへの権限付きアクセスをイネーブルにします（従来のイネーブル権限）。 （注） レベル 2 ～ 14 は、通常はデフォルト設定では使用されませんが、通常はレベル 15 にあるコマンドをそれよりも低いレベルに移動し、通常はレベル 1 にあるコマンドをそれよりも高いレベルに移動することで、カスタム設定を作成できます。CLI を使用するか FlexConfig を定義することにより、コマンドの権限レベルを設定できます。

Cisco IOS ルータにおけるブリッジング

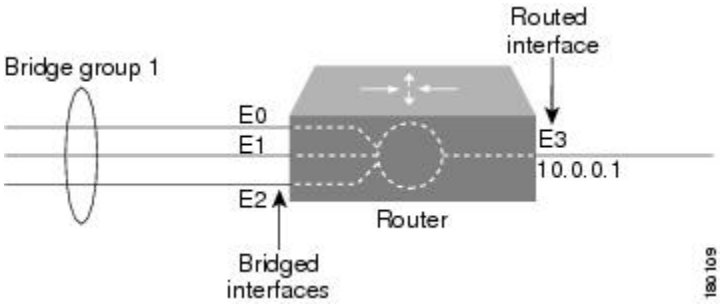
ブリッジング ポリシーを使用すると、ブリッジ グループとして機能するように設定した選択済みインターフェイスに対して、RFC 1286 で規定されているトランスペアレント ブリッジングを実行できます。Security Manager では、Integrated Routing and Bridging がサポートされます。Integrated Routing and Bridging を使用すると、ルーテッド インターフェイスとブリッジ グループ間、またはブリッジ グループ間で特定のプロトコルをルーティングできます。図 1 : トラン

スペアレント ブリッジング （24 ページ）に示すように、ローカル トラフィックやルーティング不可能なトラフィックは、同じブリッジ グループ内のブリッジド インターフェイス間でブリッジングでき、ルーティング可能なトラフィックは、他のルーテッド インターフェイスやブリッジ グループにルーティングできます。

Integrated Routing and Bridging を使用して、次の処理を実行できます。

- パケットをブリッジド インターフェイスからルーテッド インターフェイスにスイッチングする。
- パケットをルーテッド インターフェイスからブリッジド インターフェイスにスイッチングする。
- パケットを同じブリッジ グループ内でスイッチングする。

図 *1*: トランスペアレント ブリッジング



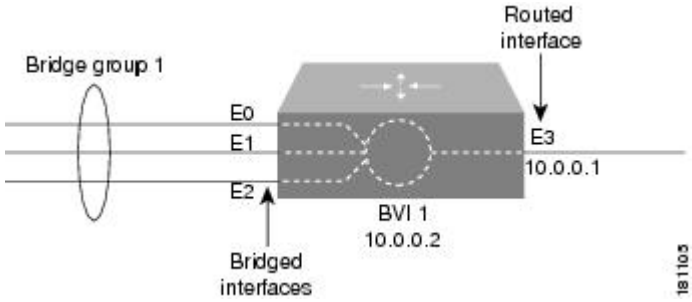
関連項目

- ブリッジ グループの定義 （25 ページ）
- ブリッジ グループ仮想インターフェイス （24 ページ）

ブリッジ グループ仮想インターフェイス

ブリッジングはデータ リンク層で実行され、ルーティングはネットワーク層で実行されるため、ブリッジングとルーティングはプロトコル コンフィギュレーション モデルが異なります。たとえば、IP では、ブリッジ グループ インターフェイスは同じネットワークに属し、共通の IP ネットワーク アドレスを持ちます。一方、各ルーテッド インターフェイスは個別のネットワークを表し、独自の IP ネットワーク アドレスを持ちます。Integrated Routing and Bridging では、Bridge-group Virtual Interface（BVI; ブリッジ グループ仮想インターフェイス）の概念を使用して、これらのインターフェイスが特定のプロトコルのパケットを交換できるようにします。図 2 : ブリッジ グループ仮想インターフェイス （25 ページ）に示すように、BVI に割り当てられたインターフェイス番号は、BVI が表すブリッジ グループに対応します。この番号は、仮想インターフェイスとブリッジ グループ間のリンクです。

図 *2:* ブリッジ グループ仮想インターフェイス



BVI 上の特定のプロトコルのルーティングをイネーブルにすると、ルーテッドインターフェイスからブリッジドドメイン内のホスト宛に送信されたパケットは、BVI にルーティングされ、対応するブリッジドインターフェイスに転送されます。BVI にルーティングされたすべてのトラフィックは、ブリッジド トラフィックとして対応するブリッジ グループに転送されます。ブリッジドインターフェイスで受信したすべてのルーティング可能なトラフィックは、BVI から直接送信されているかのように他のルーテッドインターフェイスにルーティングされます。

（注） BVI インターフェイスは、インターフェイス ポリシーを使用して設定します。基本的なルータ インターフェイス設定の定義を参照してください。BVI インターフェイスには、同じ番号を持つ、対応するブリッジ グループが必要です。このようなブリッジ グループがなければ、展開は失敗します。

（注） ブリッジ グループに 3 つ以上のインターフェイスが含まれている場合は、BVI インターフェイスをグループに追加して、セキュリティ上の問題となる可能性があるユニキャスト フラッディングを防ぎます。

関連項目

- ブリッジ グループの定義 （25 ページ）
- Cisco IOS ルータにおけるブリッジング （23 ページ）

ブリッジ グループの定義

ブリッジ グループを定義するには、ブリッジ グループに含める L3 インターフェイスを選択し、グループに番号を割り当てます。Security Manager 内のすべてのブリッジ グループは、IP トラフィックに対してだけ Integrated Routing and Bridging を実行し、標準のスパニングツリー プロトコル（IEEE 802.1D）を使用します。

（注） CLI コマンドまたは FlexConfig を使用して、AppleTalk や IPX などの他のプロトコルにブリッジングしたり、VLAN-Bridge などの他のスパニングツリー プロトコルを使用したりします。同時ルーティングおよびブリッジングはサポートされません。

関連項目

- Cisco IOS ルータにおけるブリッジング （23 ページ）
- ブリッジ グループ仮想インターフェイス （24 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ブリッジング（Bridging）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [ブリッジング（Bridging）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Bridging] ページが表示されます。このページのフィールドの説明については、表 9 : [Bridging] ページ （27 ページ）を参照してください。

ステップ 2 テーブルの下にある [追加（Add）] ボタンをクリックして、[ブリッジグループ（Bridge Group）] ダイアログボックスを表示します。このダイアログボックスのフィールドの説明については、表 10 : [Bridge Group] ダイアログボックス （28 ページ）を参照してください。ここから、ブリッジ グループを定義できます。

ステップ 3 ブリッジ グループを識別する番号を入力します。

ステップ 4 ブリッジグループに含めるインターフェイスとインターフェイスロールの名前を入力します。または [選択（Select）] をクリックしてインターフェイスロールを選択するか、新しいインターフェイスロールを作成します。詳細については、ポリシー定義中のインターフェイスの指定を参照してください。

X.25 を除くほとんどのレイヤ 3 インターフェイスと Integrated Services Digital Network（ISDN）ブリッジド インターフェイス、および特定のタイプの論理インターフェイス（ループバック、トンネル、ヌル、BVI など）を選択できます。各インターフェイスは、1 つのブリッジ グループだけに含めることができます。

親インターフェイスがスイッチ間リンク（ISL）または 802.1Q カプセル化で設定されている場合にだけ LAN サブインターフェイスを選択できます。

ステップ 5 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。ブリッジグループが [Bridging] ページのテーブルに表示されます。

（注） ブリッジグループを編集するには、[グループ（Groups）] テーブルからブリッジグループを選択し、[編集（Edit）] をクリックします。ブリッジグループを削除するには、そのグループを選択し、[削除（Delete）] をクリックします。

[Bridging] ポリシー ページ

[Bridging] ページでは、ルータに対して Integrated Routing and Bridging を実行できるブリッジ グループを定義します。詳細については、ブリッジ グループの定義 （25 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ブリッジング（Bridging）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [ブリッジング（Bridging）]** を選択します。[ブリッジング（Bridging）] を右クリックしてポリシーを作成するか、共有ポリシーセレクタから既存ポリシーを選択します。

関連項目

- Cisco IOS ルータにおけるブリッジング （23 ページ）
- テーブル カラムおよびカラム見出しの機能
- テーブルのフィルタリング

フィールド リファレンス

表 9 : [Bridging] ページ

要素	説明
グループ番号（Group Number）	ブリッジ グループを識別する番号。
Group Interfaces	ブリッジグループに含めるインターフェイスとインターフェイス ロール。
[追加（Add）] ボタン	[Bridge Group] ダイアログボックス （28 ページ）が開きます。ここから、ブリッジ グループを定義できます。
[編集（Edit）] ボタン	[Bridge Group] ダイアログボックス （28 ページ）が開きます。ここから、ブリッジ グループを編集できます。
[削除（Delete）] ボタン	選択したブリッジ グループをテーブルから削除します。

[Bridge Group] ダイアログボックス

[Bridge Group] ダイアログボックスでは、ルータ上のブリッジ グループを定義します。各ブリッジ グループには、シリアル インターフェイスなど、さまざまなタイプの複数のレイヤ 3 インターフェイスを含めることができます。

（注） すべてのブリッジ グループは、標準のスパニングツリープロトコル（IEEE 802.1D）を使用します。CLI コマンドまたは FlexConfig を使用して、AppleTalk や IPX などの他のプロトコルにブリッジングしたり、VLAN-Bridge などの他のスパニングツリー プロトコルを使用したりします。

ナビゲーション パス

[Bridging] ポリシー ページ （27 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- ブリッジ グループの定義 （25 ページ）
- Cisco IOS ルータにおけるブリッジング （23 ページ）
- インターフェイス ロール オブジェクトについて

フィールド リファレンス

表 *10 : [Bridge Group]* ダイアログボックス

要素	説明
グループ番号（Group Number）	ブリッジ グループに割り当てる番号。有効値の範囲は、1 ～ 255 です。

要素	説明
Group Interfaces	ブリッジグループに含めるインターフェイス。1つ以上のインターフェイスとインターフェイスロールの名前を入力するか、または [選択（Select）] をクリックしてそれらを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 シリアル インターフェイス（High-level Data Link Control（HDLC; ハイレベル データリンク コントロール）またはフレームリレー カプセル化が設定されている場合）などのほとんどのレイヤ 3 インターフェイスを選択できます。各インターフェイスは、1つのブリッジグループだけに属することができます。 親インターフェイスがスイッチ間リンク（ISL）または802.1Q カプセル化で設定されている場合にだけ LAN サブインターフェイスを選択できます。 （注） ループバック、トンネル、ヌル、BVI などの特定のタイプのインターフェイスはブリッジングできません。 （注） ブリッジグループにより、Security Manager とデバイスとの通信が妨害されていないことを確認してください。

Cisco IOS ルータにおけるタイム ゾーン設定

Cisco IOS ルータの現地時間は、一般に CLI で clock set コマンドを使用して設定するか、またはNTP サーバから時刻を動的に取得して設定します。これらの時刻設定を調整するには、ルータが存在するタイム ゾーンおよびそのタイム ゾーンの Daylight Saving Time（DST; 夏時間）の開始日と終了日を定義します。

関連項目

- タイム ゾーンと DST 設定の定義 （29 ページ）
- Cisco IOS ルータにおける NTP （125 ページ）

タイム ゾーンと DST 設定の定義

Security Manager では、Cisco IOS ルータが配置されているタイム ゾーンを定義できます。Daylight Saving Time（DST; 夏時間）の開始日と終了日を定義することもできます。

関連項目

- NTP サーバの定義 （125 ページ）
- Cisco IOS ルータにおけるタイム ゾーン設定 （29 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [クロック（Clock）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [クロック（Clock）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Clock] ページが表示されます。このページのフィールドの説明については、表 11 : [Clock] ページ （31 ページ）を参照してください。

ステップ 2 ルータが配置されているタイム ゾーンを選択します。タイム ゾーンは、Greenwich Mean Time（GMT; グリニッジ標準時）との時差に従ってリストに表示されます。

ステップ 3 （任意）DST の開始日と終了日を決定するための方法を選択します。

- [Set by Date]：このオプションは、DST が指定日に開始し、終了する場合に選択します。「ステップ 4 （30 ページ）」に進みます。
- [Set by Day]：このオプションは、特定の曜日（日付はその年によって異なる）に開始し、終了する場合に選択します。「ステップ 5 （30 ページ）」に進みます。
- [None]：このオプションは、DST を使用しない場合に選択します。

ステップ 4 （[Set by Date] を選択した場合）DST が開始および終了する日付を定義します。

a) [Start] の下にあるカレンダー アイコンをクリックし、適切な日付をクリックします。
b) 表示されるリストから時間と分を選択します。
c) 手順 a と b を繰り返して終了日と終了時刻を設定します。

ステップ 5 （[曜日による設定（Set by Day）] を選択した場合）米国の大部分で使用されるデフォルト以外の DST 期間を定義する場合は、[繰り返し時刻を指定（Specify Recurring Time）]チェックボックスをオンにします。

ステップ 6 （[Specify Recurring Time] を選択した場合）DST の開始と終了を指定します。

a) [Start] で、DST が開始する月を選択します。
b) 月の週を選択します（1、2、3、4、first、または last）。
c) 曜日を選択します。
d) 表示されるリストから時間と分を選択します。たとえば、DST が毎年 3 月の最後の日曜日の午前 1:00 に開始する場合は、[3月（March）]、[最後（last）]、[日曜日（Sunday）]、[1]、および [00] を選択します。
e) 手順 a ～ d を繰り返して終了日と終了時刻を設定します。

[Clock] ポリシー ページ

[Clock] ページでは、ルータが配置されているタイム ゾーンと Daylight Saving Time（DST; 夏時間）を設定します。詳細については、Cisco IOS ルータにおけるタイム ゾーン設定 （29 ページ）を参照してください。

ヒント　NTP ポリシーを定義するか、または CLI を使用して **clock set** コマンドを設定することによって、ルータの現地時間を設定できます。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]>[デバイス管理（Device Admin）] > [クロック（Clock）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [クロック（Clock）]** を選択します。[クロック（Clock）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [NTP Policy] ページ （127 ページ）

フィールド リファレンス

表 *11 : [Clock]* ページ

要素	説明
Device Time Zone	Coordinated Universal Time（UTC; 協定世界時）とも呼ばれる Greenwich Mean Time（GMT; グリニッジ標準時）との関連で表現される、ルータが配置されているタイム ゾーン。 **注意**　CLI（コマンドラインインターフェイス）を使用してルータのタイムゾーンを設定する場合は、『Cisco IOS Configuration Fundamentals Command Reference』に記載されている必要なタイムゾーンの頭字語を使用する必要があります。タイムゾーンに他の形式を使用してから、Security Manager を使用してルータを検出した場合、Security Manager はタイムゾーン CLI を検出しません。
Daylight Savings Time (Summer Time)	ルータの現地時間に適用する DST のタイプ。 • [Set by Date]：DST が開始および終了する正確な日時を定義できます。 • [Set by Day]：DST が開始および終了する相対的な繰り返し日時を定義できます。たとえば、DST が 3 月の最後の日曜日に開始し、10 月の最後の日曜日に終了する場合にこのオプションを使用できます。 • [None]：夏時間を使用しません。

要素	説明
[Set by Date] の追加フィールド	
開始（Start）	DST が開始する日時： • [Date]：カレンダーアイコンをクリックして、開始日を選択します。 • [Hour]：開始時刻（時間）を選択します。 • [Minute]：開始時刻（分）を選択します。
終了（End）	DST が終了する日時： • [Date]：カレンダーアイコンをクリックして、終了日を選択します。 • [Hour]：終了時刻（時間）を選択します。 • [Minute]：終了時刻（分）を選択します。 （注） Cisco IOS ソフトウェアでは、2035 年 12 月 31 日までの日付がサポートされます。
[Set by Day] の追加フィールド	
Specify Recurring Time	選択すると、ルータはこのポリシーで指定された日付と時刻に従って DST を実装します。 選択を解除すると、ルータは米国の大部分で使用されているスケジュールに従って DST を実装します。
開始（Start）	夏時間が開始する相対的な日時： • [Month]：月を選択します。 • [Week]：月の週を選択します（1、2、3、4、first、または last）。 • [Weekday]：曜日を選択します。 • [Hour]：時間を選択します。 • [Minute]：分を選択します。 たとえば、DST が毎年 3 月の最後の日曜日の午前 1:00 に開始する場合は、[3月（March）]、[最後（last）]、[日曜日（Sunday）]、[1]、および [00] を選択します。

要素	説明
終了（End）	夏時間が終了する相対的な日時： • [Month]：月を選択します。 • [Week]：月の週を選択します（1、2、3、4、first、または last）。 • [Weekday]：曜日を選択します。 • [Hour]：時間を選択します。 • [Minute]：分を選択します。

Cisco IOS ルータにおける CPU 使用率設定

CPU ポリシーでは、CPU 使用率に関する設定を行います。このポリシーを使用すると、CPU リソースをモニタしたり、事前に決定されているレベルの使用率を超えるプロセスを追跡したりできます。

（注） CPU ポリシーは、Cisco IOS ソフトウェア Release 12.3(14)T 以降を実行しているルータでサポートされます。

関連項目

- CPU 使用率設定の定義 （33 ページ）

CPU 使用率設定の定義

Security Manager を使用して、次のデフォルトの CPU 使用率設定を変更できます。

- CPU 履歴テーブルのサイズ
- 拡張 CPU 負荷履歴テーブルのサイズ
- 自動 CPU Hog プロファイリングをイネーブルにするかどうか

また、オプションで次の項目を定義できます。

- プロセスを履歴テーブルに含める CPU 使用率レベル。
- イネーブルにする CPU 使用率しきい値のタイプ。しきい値のタイプごとに、通知をトリガーするしきい値を指定できます。

関連項目

- CPU 使用率設定の定義 （33 ページ）

- Cisco IOS ルータにおけるロギング

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [CPU] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [CPU] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[CPU] ページが表示されます。

ステップ 2 （任意）ルータのCPU使用率設定を必要に応じて定義します。使用可能なフィールドの説明については、表 12 : [CPU] ページ （35 ページ）を参照してください。

[CPU] ポリシー ページ

[CPU] ページでは、ログ メッセージを送信するしきい値、CPU 履歴テーブルのサイズ、自動 CPU Hog プロファイリングをイネーブルにするかどうかなど、ルータの CPU 使用率に関する設定を定義します。

詳細については、CPU 使用率設定の定義 （33 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイスアクセス（Device Access）] > [CPU]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイスアクセス（Device Access）] > [CPU]** を選択します。[CPU] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [Memory] ポリシー ページ （103 ページ）
- Syslog ロギングの設定ポリシーのページ
- Syslog サーバ ポリシーのページ

フィールド リファレンス

表 *12 : [CPU]* ページ

要素	説明
CPU Utilization Statistics	CPU 使用率の統計情報の履歴テーブルに関する設定： • [History Table Entry Limit]：プロセスで使用される CPU 使用率で、この値を超えるとプロセスは履歴テーブルに格納されます。 • [History Table Size]：CPU 統計情報を履歴テーブルに格納しておく期間。有効値の範囲は 5 ～ 86400 秒（24 時間）です。デフォルトは 600 秒（10 分）です。
CPU Total Utilization	通知をトリガーする合計 CPU 使用率のしきい値。 • [Enable CPU Total Utilization]：選択されている場合、合計 CPU 使用率しきい値がイネーブルになります。選択解除されている場合、これらのしきい値はディセーブルになり、通知をトリガーしません。これがデフォルトです。 • [リソースの最大合計使用率（Maximum Total Utilization Resources）]：定義された間隔に使用状況がこのレベルを超えた場合に通知をトリガーする CPU リソースのパーセンテージ。 • [Maximum Total Utilization Violation Duration]：最大 CPU しきい値の通知をトリガーする違反間隔。有効値の範囲は 5 ～ 86400 秒（24 時間）です。 • [リソースの最小合計使用率（Minimum Total Utilization Resources）]：定義された間隔に使用状況がこのレベルを下回った場合に通知をトリガーする CPU リソースのパーセンテージ。 • [Minimum Total Utilization Violation Duration]：最小 CPU しきい値の通知をトリガーする違反間隔。有効値の範囲は 5 ～ 86400 秒（24 時間）です。

要素	説明
CPU Interrupt Utilization	通知をトリガーする合計 CPU 割り込み使用率のしきい値。 • [Enable CPU Interrupt Utilization]：選択されている場合、CPU 割り込み使用率のしきい値がイネーブルになります。選択解除されている場合、これらのしきい値はディセーブルになり、通知をトリガーしません。これがデフォルトです。 • [リソースの最大割り込み使用率（Maximum Interrupt Utilization Resources）]：定義された間隔に使用状況がこのレベルを超えた場合に通知をトリガーする CPU リソースのパーセンテージ。 • [Maximum Interrupt Utilization Violation Duration]：最大 CPU しきい値の通知をトリガーする違反間隔。有効値の範囲は 5 ～ 86400 秒（24 時間）です。 • [リソースの最小割り込み使用率（Minimum Interrupt Utilization Resources）]：定義された間隔に使用状況がこのレベルを下回った場合に通知をトリガーする CPU リソースのパーセンテージ。 • [Minimum Interrupt Utilization Violation Duration]：最小 CPU しきい値の通知をトリガーする違反間隔。有効値の範囲は 5 ～ 86400 秒（24 時間）です。
CPU Process Utilization	通知をトリガーする合計 CPU プロセス使用率のしきい値。 • [Enable CPU Process Utilization]：選択されている場合、CPU プロセス使用率のしきい値がイネーブルになります。選択解除されている場合、これらのしきい値はディセーブルになり、通知をトリガーしません。これがデフォルトです。 • [リソースの最大プロセス使用率（Maximum Process Utilization Resources）]：定義された間隔に使用状況がこのレベルを超えた場合に通知をトリガーする CPU リソースのパーセンテージ。 • [Maximum Process Utilization Violation Duration]：最大 CPU しきい値の通知をトリガーする違反間隔。有効値の範囲は 5 ～ 86400 秒（24 時間）です。 • [リソースの最小プロセス使用率（Minimum Process Utilization Resources）]：定義された間隔に使用状況がこのレベルを下回った場合に通知をトリガーする CPU リソースのパーセンテージ。 • [Minimum Process Utilization Violation Duration]：最小 CPU しきい値の通知をトリガーする違反間隔。有効値の範囲は 5 ～ 86400 秒（24 時間）です。
Extended CPU History Size	5 秒間隔で収集する拡張 CPU 負荷の履歴のサイズ。有効値の範囲は 2 ～ 720 です。デフォルトは 12 で、これは 1 分間の履歴に相当します。

要素	説明
Enable Automatic CPU Hog Profiling	選択すると、自動 CPU Hog プロファイリングがイネーブルになります。これがデフォルトです。 選択を解除すると、自動 CPU Hog プロファイリングがディセーブルになります。 この機能は、プロセスがいつ CPU を独占する可能性があるかを予測し、そのプロセスのプロファイリングを開始します。 （注） CPU Hog プロファイルデータを表示するには、CLI で **show processes cpu autoprofile hog** コマンドを使用します。

Cisco IOS ルータにおける HTTP と HTTPS

Security Manager では、Cisco IOS ルータ上の HTTP および HTTP over Secure Socket Layer（HTTP over SSL または HTTPS とも呼ぶ）サーバ機能を設定できます。この機能により、HTTP 1.1 サーバで SSL バージョン 3.0 がサポートされます。

セキュアな HTTP 接続とは、HTTP サーバとの間で送受信されるデータがインターネットを介して送信される前に暗号化されることを意味します。SSL 暗号化を使用した HTTP により、セキュアな接続が提供され、Web ブラウザからのルータの設定などの機能を実行できます。

HTTP と HTTPS は、Cisco Web ブラウザ ユーザ インターフェイスを使用したデバイスへのアクセスを提供する以外に、デバイスと通信するために Cisco Router and Security Device Manager（SDM）などのデバイス管理アプリケーションで使用されます。

関連項目

- HTTP ポリシーの定義　（37 ページ）

HTTP ポリシーの定義

HTTP ポリシーを定義すると、次の処理を実行できます。

- ルータにおける HTTP および SSL 機能のイネーブル化とディセーブル化
- 各プロトコルで使用されるポートの指定
- （任意）これらのプロトコルを使用したデバイスへのアクセスを制限する標準の番号付き ACL の定義

さらに、ユーザに対して実行する AAA 認証と認可の方式を定義できます。

HTTP ポリシーを定義するときは注意が必要です。設定が Security Manager（およびこれらのプロトコルを使用する他の管理アプリケーション）とデバイス間の通信に影響する可能性があるためです。

（注） 原則として、Security Manager は SSL を Cisco IOS ルータとの通信のデフォルト プロトコルとして使用するため、Security Manager によって検出された Cisco IOS ルータではすでに HTTPS がイネーブルになっています。Cisco IOS ルータでの SSL の設定を参照してください。

はじめる前に

- ルータで AAA サービスをイネーブルにします。 AAA サービスの定義 （5 ページ） を参照してください。

関連項目

- Cisco IOS ルータにおける HTTP と HTTPS （37 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [HTTP] を選択し、作業領域で [セットアップ（Setup）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [HTTP] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[HTTP Setup] タブが表示されます。このタブのフィールドの説明については、表 13 : [HTTP] ページ - [Setup] タブ （41 ページ）を参照してください。

ステップ 2 チェックボックスをオンにして、ルータにおける HTTP および SSL（HTTPS）機能をイネーブルにします。

（注） SSL がディセーブルになっている（または HTTP ポリシー全体が割り当てられていない）場合、デバイスから SSH へのトランスポート プロトコルを変更しないかぎり、Security Manager は展開後にそのデバイスと通信できません。この設定は、[Device Properties] にあります。デバイス通信設定および証明書の管理を参照してください。

ヒント SSL がイネーブルになっているときは HTTP をディセーブルにすることを推奨します。サーバに対してセキュアな接続だけを確立するには、これが必須です。

ステップ 3 （任意）HTTP（80）および HTTPS（443）によって使用されるデフォルト ポートを変更します。

ステップ 4 （任意）[ここからの接続を許可（Allow Connection From）] フィールドに、このデバイス上の HTTP および HTTPS を使用できるアドレスを指定する標準の番号付き ACL の名前オブジェクトを入力します。または、[選択（Select）] をクリックしてリストから ACL オブジェクトを選択するか、新しい ACL オブジェクトを作成します。このオプションは、これらのプロトコルへのアクセスを制限する場合に使用します。標準の ACL オブジェクトを作成する方法の詳細については、標準アクセス コントロール リスト オブジェクトの作成を参照してください。

（注） 選択した ACL で Security Manager サーバが許可されていることを確認してください。許可されていない場合、デバイスとの通信は失われます。

ステップ 5 （任意）[AAA] タブで、HTTP または HTTPS を使用してデバイスにアクセスしようとするユーザに対して実行する認証のデフォルト タイプを変更します。オプションには、[AAA]、[Enable Password]（デフォルト）、[Local Database]、および [TACACS] があります。

[AAA] を選択した場合はステップ 6 （39 ページ）に進みます。[AAA] 以外を選択した場合はステップ 8 （39 ページ）に進みます。

（注） [TACACS] オプションは、12.3(8) よりも前の IOS ソフトウェア バージョンを使用するデバイスにだけ適用されます。

[AAA] タブのフィールドの説明については、表 14 : [HTTP] ページ - [AAA] タブ （42 ページ）を参照してください。

ステップ 6 ユーザに対して実行する認証方式を選択します。

- デバイスの AAA ポリシー（AAA サービスの定義 （5 ページ）を参照）で定義されているデフォルトの AAA ログイン認証方式を使用する場合は、[デバイスログイン認証を有効にする（Enable Device Login Authentication）] チェックボックスをオフにしてください。「ステップ 7 （39 ページ）」に進みます。
- このポリシー用に特別に方式リストを定義する場合は、次の手順を実行します。

a) [デバイスログイン認証を有効にする（Enable Device Login Authentication）] チェックボックスをオンにします。

b) [優先方法リスト（Prioritized Method List）] で、認証に使用する AAA サーバーグループの名前を入力します。または、[選択（Select）] をクリックしてリストから AAA サーバーグループを選択するか、新しいAAAサーバーグループを作成します。セレクタの上向きおよび下向き矢印を使用して、これらの認証方式を適用する順序を定義します。

（注） Security Manager ユーザが AAA サーバで定義されていることを確認します。定義されていない場合、デバイスとの通信は失われます。

ステップ 7 HTTP または HTTPS を使用して EXEC セッションを開始するユーザに対して実行する認可方式を選択します。

- デバイスの AAA ポリシーで定義されているデフォルトの AAA 認証方式を使用する場合は、[CLI/EXEC 操作認証を有効にする（Enable CLI/EXEC Operations Authorization）] チェックボックスをオフにしてください。「ステップ 8 （39 ページ）」に進みます。
- このポリシー用に特別に方式リストを定義する場合は、[CLI/EXEC操作認証を有効にする（Enable CLI/EXEC Operations Authorization）] チェックボックスをオンにし、方式リストを定義します。

（注） このオプションを選択解除のままにした場合は、ルータの AAA ポリシーで EXEC認証が有効になっていることを確認してください。イネーブルになっていない場合は、HTTP または HTTPS（SSL）を介してデバイスに接続できません。これは、Security Manager および SDM などのその他のアプリケーションに適用されます。 AAA サービスの定義 （5 ページ）を参照してください。

ステップ 8 （任意）特定の権限レベルのコマンド認可定義を作成します。

a) [コマンド認証の上書き（Command Authorization Override）] テーブルの下の [追加（Add）] ボタンをクリックします。[Command Authorization Override] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 15 : [Command Authorization] ダイアログボックス （45 ページ）を参照してください。
b) 必要に応じてコマンド認可定義を設定します。
c) [OK] をクリックダイアログボックスが閉じ、認可方式が [Command Authorization Override] テーブルに表示されます。
d) 8.a （40 ページ）～8.c （40 ページ）を繰り返して、追加のコマンド認可定義を作成します。

[HTTP] ポリシー ページ

[HTTP] ページでは、ルータ上の HTTP および HTTPS アクセスを設定します。[HTTP] ポリシーページの次のタブから Cisco IOS ルータ上の HTTP ポリシーを設定できます。

- [HTTP] ページ - [Setup] タブ （40 ページ）
- [HTTP] ページ - [AAA] タブ （42 ページ）

詳細については、Cisco IOS ルータにおける HTTP と HTTPS （37 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [HTTP] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [HTTP] を選択します。[HTTP] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存ポリシーを選択します。

[HTTP] ページ - [Setup] タブ

[HTTP] ページの [Setup] タブでは、ルータ上の HTTP および HTTP over Secure Socket Layer（HTTP over SSL または HTTPS）をイネーブルにします。これらのプロトコルへのアクセスをアクセス コントロール リストで定義されているアドレスに制限することもできます。

（注） 原則として、Security Manager は SSL を Cisco IOS ルータとの通信のデフォルト プロトコルとして使用するため、Security Manager によって検出された Cisco IOS ルータではすでに HTTPS がイネーブルになっています。Cisco IOS ルータでの SSL の設定を参照してください。

ナビゲーション パス

[HTTP] ポリシー ページ （40 ページ）に移動し、[セットアップ（Setup）] タブをクリックします。

関連項目

- [HTTP] ページ - [AAA] タブ （42 ページ）
- Cisco IOS ルータにおける HTTP と HTTPS （37 ページ）

フィールド リファレンス

表 *13 : [HTTP]* ページ - *[Setup]* タブ

要素	説明
HTTP の有効化	選択すると、ルータで HTTP サーバがイネーブルになります。 選択を解除すると、ルータでHTTPがディセーブルになります。これは、検出されなかったデバイスのデフォルトです。
HTTP ポート（HTTP Port）	HTTP で使用するポート番号。有効値は、80 または 1024 ～ 65535 の任意の値です。デフォルトは 80 です。
SSL の有効化（Enable SSL）	選択すると、セキュアな HTTP サーバ（HTTP over SSL または HTTPS）がルータでイネーブルになります。 選択を解除すると、HTTPS がディセーブルになります。これは、検出されなかったデバイスのデフォルトです。 （注） SSL がディセーブルになっている（または HTTP ポリシー全体が割り当てられていない）場合、デバイスから SSH へのトランスポート プロトコルを変更しないかぎり、Security Manager は展開後にそのデバイスと通信できません。この設定は、[Device Properties] にあります。 （注） SSL がイネーブルになっているときは HTTP をディセーブルにすることを推奨します。サーバに対してセキュアな接続だけを確立するには、これが必須です。
SSL Port	HTTPS で使用するポート番号。有効値は、443 または 1025 ～ 65535 の任意の値です。デフォルトは 443 です。

要素	説明
Allow Connection From	このデバイス上の HTTP および HTTPS の使用を制限する標準の番号付き ACL の名前。ACL オブジェクトの名前を入力するか、[選択（Select）] をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 （注） ACL を定義する場合は、ACL に Security Manager サーバが含まれていることを確認してください。含まれていない場合、Security Manager は SSL を使用してこのデバイスと通信できません。

[HTTP] ページ - [AAA] タブ

[HTTP] ページの [AAA] タブでは、HTTP または HTTPS を使用してルータにアクセスしようとするユーザに対して実行する認証方式および認可方式を定義します。

ナビゲーション パス

[HTTP] ポリシー ページ （40 ページ）に移動し、[AAA] タブをクリックします。

関連項目

- [HTTP] ページ - [Setup] タブ （40 ページ）
- Cisco IOS ルータにおける HTTP と HTTPS （37 ページ）
- テーブルのフィルタリング

フィールド リファレンス

表 14 : [HTTP] ページ - [AAA] タブ

要素	説明
Authenticate Using	使用する認証のタイプ： • [AAA]：AAA ログイン認証を実行します。 • [Enable Password]：ルータに設定されているイネーブル パスワードを使用します。これがデフォルトです。 • [Local Database]：ルータに設定されているローカル ユーザ名データベースを使用します。 • [TACACS]：ルータに設定されている TACACS または XTACACS サーバを使用します。12.3(8) または 12.3(8)T よりも前の IOS ソフトウェア バージョンを使用するデバイスにだけ適用されます。
[Login Authentication] 設定	

要素	説明
Enable Device Login Authentication	[AAA] が認証方式として選択されている場合にだけ適用されます。 選択すると、認証は [Prioritized Method List] フィールドで定義されている方式に基づいて実行されます。 選択を解除すると、ルータの AAA ポリシーで定義されているデフォルトの認証リストが使用されます。 [AAA] ページ - [Authentication] タブ （8 ページ）を参照してください。
Prioritized Method List	[Enable Device Login Authentication] チェックボックスがオンになっている場合にだけ適用されます。 ユーザを認証する場合に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認証を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。
[EXEC Authorization] 設定	
Enable CLI/EXEC Operations Authorization	[AAA] が認証方式として選択されている場合にだけ適用されます。 選択すると、EXEC 認可は [Prioritized Method List] フィールドで定義されている方式に基づいて実行されます。このタイプの認可では、EXEC（CLI）セッションを開くことをユーザに許可するかどうかを決定します。 選択を解除すると、ルータの AAA ポリシーで定義されているデフォルトの EXEC 認可リストが使用されます。 [AAA] ページ - [Authorization] タブ（9 ページ）を参照してください。 （注） このオプションを選択解除のままにした場合は、ルータの AAA ポリシーで EXEC 認可がイネーブルになっていることを確認してください。イネーブルになっていない場合は、HTTP または HTTPS（SSL）を介してデバイスに接続できません。これは、Security Manager および SDM やデバイスの Web インターフェイスなどのその他のアプリケーションに適用されます。

要素	説明
Prioritized Method List	[Enable CLI/EXEC Operations Authorization] チェックボックスがオンになっている場合にだけ適用されます。 EXEC（CLI）セッションを開くことをユーザに許可する場合に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認可を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。
[Command Authorization] 設定	
特権レベル	コマンド認可定義が適用される権限レベル。
Prioritized Method List	この権限レベルでユーザを認可するときに使用する方式リスト。
[追加（Add）] ボタン	[Command Authorization Override] ダイアログボックス （44 ページ）が開きます。ここから、コマンド認可定義を設定できます。
[編集（Edit）] ボタン	[Command Authorization Override] ダイアログボックス （44 ページ）が開きます。ここから、コマンド認可定義を編集できます。
[削除（Delete）] ボタン	選択したコマンド認可定義をテーブルから削除します。

[Command Authorization Override] ダイアログボックス

[Command Authorization Override] ダイアログボックスでは、特定の権限に関連付けられている EXEC コマンドを認可するときに使用する方式を定義します。これにより、特定の権限レベル（0 ～ 15）に関連付けられているすべてのコマンドを認可できます。

ナビゲーション パス

[HTTP] ページ - [AAA] タブ （42 ページ）で、[コマンド許可のオーバーライド（Command Authorization Override）] テーブルの下にある [追加（Add）] ボタンをクリックします。

関連項目

- [HTTP] ポリシー ページ （40 ページ）

- [AAA] ポリシー ページ （7 ページ）

フィールド リファレンス

表 *15 : [Command Authorization]* ダイアログボックス

要素	説明
Privilege Level	コマンド アカウンティング リストを定義する権限レベル。有効値の範囲は 0 ～ 15 です。
Prioritized Method List	ユーザを認可する場合に使用する方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認可を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 サポートされる方式には、[TACACS+]、[Local]、および [None] が含まれます。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。

Cisco IOS ルータにおける回線アクセス

Security Manager では、次の方法を使用したルータへのコマンドライン アクセス（EXEC アクセスとも呼ばれる）を設定できます。

- コンソール ポート：ローカル アクセスのための標準の RS232 ケーブルによる物理接続。詳細については、以下を参照してください。
  - コンソール ポートの設定パラメータの定義 （46 ページ）
  - コンソール ポートの AAA 設定の定義 （47 ページ）
- VTY 回線：一般に Telnet、SSH、rlogin などのプロトコルを使用したリモート アクセスのための仮想端末回線。詳細については、以下を参照してください。
  - VTY 回線の設定パラメータの定義 （49 ページ）
  - VTY 回線の AAA 設定の定義 （52 ページ）

これらのポリシーを設定して展開したあと、CLI を使用した設定または診断時にこれらの回線を使用して個々のデバイスと直接通信できます。

コンソール ポートの設定パラメータの定義

ルータのコンソール ポートは、一般的にデバイスに物理的にアクセスできる管理者によってローカル システム アクセスに使用されます。デフォルトでは、コンソール ポートは次のように設定されます。

- 許可されるすべてのユーザは、すべてのコンフィギュレーション コマンド（権限レベル 15）を含む、ルータへの権限付きアクセス権を持ちます。
- 回線は、ユーザ入力がなくなってから 10 分経過後に切断されます。
- 着信接続は許可されません。
- 発信接続では Telnet だけがサポートされます。

デフォルト設定を変更する以外に、次の設定を定義することもできます。

- コンソールにアクセスするためのパスワード
- コンソール上のすべての EXEC セッションをディセーブルにするかどうか
- コンソール上で許可される接続を制限する着信 ACL と発信 ACL
- コンソール上で VRF 接続を許可するかどうか

関連項目

- Cisco IOS ルータにおける回線アクセス （45 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [コンソール（Console）] を選択し、作業領域で [セットアップ（Setup）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [コンソール（Console）]** を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[セットアップ（Setup）] タブをクリックします。

[Console Setup] タブが表示されます。このタブのフィールドの説明については、表 16 : [Console] ページ - [Setup] タブ （54 ページ）を参照してください。

ステップ 2 （任意）コンソール ポートにアクセスするためのパスワードを入力し、[Confirm] フィールドに再入力します。

ステップ 3 （任意）コンソール ポートのユーザに付与するデフォルト（15）を変更します。 [Console] ページ - [Authorization] タブ （58 ページ）を参照してください。

ステップ 4 （任意）[この回線を介したルータへの EXEC セッションをすべて無効にする（Disable all the EXEC sessions to the router via this line）] チェックボックスをオンにして、コンソールを介した着信接続を阻止します。

（注） このオプションを選択すると、コンソール ポートを介したデバイスへのすべてのアクセスがブロックされます。

ステップ 5 （任意）デフォルトのタイムアウトを変更します。この時間の経過後もユーザ入力が検出されない場合は、回線が切断されます。

（注） この値を 0 に設定するとタイムアウトがディセーブルになります。タイムアウトがディセーブルになると、ネットワークのセキュリティが低下する可能性があります。

ステップ 6 （任意）コンソール ポート上のアウトバウンド接続に使用できるプロトコルを指定します。

- [All]：サポートされるすべてのプロトコルが許可されます。
- [None]：プロトコルは許可されません。
- [Protocol]：SSH、Telnet、rlogin のプロトコルの 1 つ以上をイネーブルにします。

（注） コンソール ポートで SSH および rlogin プロトコルを許可するデバイスに AAA 認証を設定する必要があります。 コンソール ポートの AAA 設定の定義 （47 ページ）を参照してください。

ステップ 7 （任意）ACL の名前を入力して、デバイスとこれらのリスト内のアドレス間における着信接続と発信接続を制限します。または、[選択（Select）] をクリックして ACL オブジェクトを選択するか、新しい ACL オブジェクトを作成します。セレクタの最上部にある [Type] フィールドで、ACL タイプとして [Standard] または [Extended] を選択します。

ステップ 8 （任意）[AAA] タブをクリックして、コンソールポートの認証、許可、アカウンティング設定を定義します。 コンソール ポートの AAA 設定の定義 （47 ページ） を参照してください。

コンソール ポートの AAA 設定の定義

デフォルトでは、認証、許可、アカウンティングはコンソール ポートに対して実行されません。これらのアクセス コントロール オプションの 1 つ以上を設定するときに、デバイスの AAA ポリシーで定義されたデフォルトの方式リストを使用するか、1 つ以上の AAA 方式を含むカスタム方式リストを定義できます。

関連項目

- コンソール ポートの設定パラメータの定義 （46 ページ）
- Cisco IOS ルータにおける回線アクセス （45 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [コンソール（Console）]** を選択し、作業領域で [認証（Authentication）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから **[ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [コンソール（Console）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成し、[エリア（Area）] タブをクリックします。

[Console Authentication] タブが表示されます。

ステップ 2 （任意）コンソール回線にアクセスしようとするユーザに対して実行する認証方式を選択します。

[Authentication] タブのフィールドの説明については、表 17 : [Console] ページ - [Authentication] タブ （57 ページ）を参照してください。

（注） ローカル認証を選択する場合は、展開の前に設定全体をプレビューして、**aaa new-model** コマンドが、（たとえば、AAA ポリシーで方式リストを設定することにより）別のポリシーで設定されていないこと、またはそのデバイス自体にすでに設定されていることを確認します。

ステップ 3 （任意）[Authorization] タブで、コンソール回線にアクセスして EXEC セッションを開始するユーザに対して実行する認可方式を選択します。

[Authorization] タブのフィールドの説明については、表 18 : [Console] ページ - [Authorization] タブ （59 ページ）を参照してください。

（注） RADIUS では、認証と認可に同じサーバが使用されます。したがって、認証に RADIUS 方式リストを定義する場合は、認可にも同じ方式リストを定義する必要があります。

ステップ 4 （任意）特定の権限レベルのコマンド認可定義を作成します。

a) [コマンド認可（Commands Authorization）] テーブルの下の [追加（Add）] ボタンをクリックします。[Command Authorization] ダイアログボックスが表示されます。詳細については、表 26 : [Command Authorization] ダイアログボックス - [Line Access] （79 ページ）を参照してください。

b) 必要に応じてコマンド認可定義を設定します。

c) [OK] をクリックダイアログボックスが閉じ、認可方式が [Commands Authorization] テーブルに表示されます。

d) 6.a （48 ページ）～6.c （49 ページ）を繰り返して、追加のコマンド認可定義を作成します。

ステップ 5 （任意）[Accounting] タブで、コンソール回線にアクセスするユーザに対して実行する EXEC および接続アカウンティング方式を選択します。

このタブのフィールドの説明については、表 19 : [Console] ページ - [Accounting] タブ （60 ページ）を参照してください。

ステップ 6 （任意）特定の権限レベルのコマンド アカウンティング定義を作成します。

a) [コマンドアカウンティング（Commands Accounting）] テーブルの下の [追加（Add）] ボタンをクリックします。[Command Accounting] ダイアログボックス - [Line Access] （80 ページ）が表示されます。

b) 必要に応じてコマンド アカウンティング定義を設定します。

c) [OK] をクリックダイアログボックスが閉じ、アカウンティング方式が [Commands Accounting] テーブルに表示されます。
d) 6.a （48 ページ）～6.c （49 ページ）を繰り返して、追加のコマンド アカウンティング定義を作成します。

VTY 回線の設定パラメータの定義

すべての Cisco IOS ルータには、デフォルトで 5 本の VTY 回線（ラベル 0 ～ 4）が設定されており、これらの回線は次のように設定されています。

- 許可されるすべてのユーザは、すべてのコンフィギュレーション コマンド（権限レベル 15）を含む、ルータへの権限付きアクセス権を持ちます。
- VTY 回線は、ユーザ入力がなくなってから 10 分経過後に切断されます。
- 着信接続は許可されません。
- 発信接続では Telnet だけがサポートされます。

Security Manager を使用して、これらの 5 本の VTY 回線のデフォルト設定を変更したり、追加の回線（最大 16 本）を設定したりできます。さらに、各回線に次の設定を行うこともできます。

- 回線にアクセスするためのパスワード
- 回線上のすべての EXEC セッションをディセーブルにするかどうか
- 回線上で許可される接続を制限する着信 ACL と発信 ACL
- 回線上で VRF 接続を許可するかどうか

VTY 回線のグループの定義

複数の VTY 回線を連続したグループとして設定できます。これにより、1 つの手順でグループ内のすべての回線に同じ設定を定義できます。グループ内のすべての回線は、0 ～ 4 または 6 ～ 15 のどちらかの範囲内である必要があります。グループがこれらの 2 つの範囲にまたがることはできません。

VTY 回線 5 を設定するためのルールは次のとおりです。回線 5 は回線 0 ～ 4 と同じ定義に含めることができますが、回線 5 よりも上の回線が設定されていない場合にかぎります。回線 5 よりも上の回線が設定されている場合は、設定が同じでも回線 5 を回線 0 ～ 4 の定義に含めることはできません。設定が同じであれば、回線 5 を回線 5 よりも上の回線の定義に含めることができます。

たとえば、回線 0 ～ 5 のすべてがある設定を共有し、回線 6 ～ 9 の設定が異なる場合は、3 つの定義を作成する必要があります。1 つめは回線 0 ～ 4 の定義、2 つめは回線 5 の定義、3 つめは回線 6 ～ 9 の定義です。

（注） VTY 回線を設定する場合は、ユーザがデバイスに接続するときに、ユーザにランダムに回線が割り当てられることに留意してください。

（注） 定義は VTY 回線ごとに 1 つだけ作成できます。既存の定義と重複する VTY 回線の定義を作成すると、エラーが表示されます。

（注） Security Manager を使用してデフォルトの VTY 回線（0 ～ 4）を設定すると、その定義によってデバイス上のデフォルト設定が上書きされます。あとでこの定義を Security Manager から削除した場合は、入力プロトコル設定が保持され、他のデフォルト設定が復元されます。これにより、常にデバイスへのリモートアクセスに使用できる VTY 回線を確保できます。

（注） CLI または FlexConfig を使用して、16 本を超える回線がサポートされるデバイスに追加の VTY 回線を設定できます。

関連項目

- Cisco IOS ルータにおける回線アクセス （45 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）]>[デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [VTY] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）]>[デバイス管理（Device Admin）]>[デバイスアクセス（Device Access）]>[回線アクセス（Line Access）] > [VTY] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[VTY] ページが表示されます。このページのフィールドの説明については、表 20 : [VTY] 回線ページ （65 ページ）を参照してください。

ステップ 2 [回線（Lines）] テーブルの下にある [追加（Add）] ボタンをクリックするか、回線の定義を選択して [編集（Edit）] ボタンをクリックします。[VTY Lines] ダイアログボックスの [Setup] タブが表示されます。このタブのフィールドの説明については、表 21 : [VTY Line] ダイアログボックス （67 ページ）を参照してください。

ステップ 3 VTY 回線の相対回線番号を入力します。VTY 回線のグループを設定する場合は、グループの最初と最後の番号を表示されたフィールドに入力します。

ステップ 4 （任意）コンソール回線にアクセスするためのパスワードを入力し、[Confirm] フィールドに再入力します。

ステップ 5 （任意）このVTY回線（または回線のグループ）のユーザに付与するデフォルト権限（15）を変更します。

ステップ 6 （任意）[この回線を介したルータへのEXECセッションをすべて無効にする（Disable all the EXEC sessions to the router via this line）] チェックボックスをオンにして、この VTY 回線（または回線のグループ）を介した着信接続を阻止します。

ステップ 7 （任意）デフォルトのタイムアウトを変更します。この時間の経過後もユーザ入力が検出されない場合は、回線が切断されます。

（注） この値を 0 に設定するとタイムアウトがディセーブルになります。タイムアウトがディセーブルになると、放棄されたセッションにより、利用可能なVTY回線がブロックされる可能性があります。また、ネットワークのセキュリティが低下する可能性もあります。

ステップ 8 （任意）このVTY回線（または回線のグループ）上のインバウンド接続およびアウトバウンド接続に使用できるプロトコルを指定します。

- [All]：サポートされるすべてのプロトコルが許可されます。
- [None]：プロトコルは許可されません。
- [Protocol]：SSH、Telnet、rlogin のプロトコルの 1 つ以上をイネーブルにします。

注意 インバウンド接続設定を [None] に設定すると、Security Manager は展開後にデバイスに接続できなくなる可能性があります。

（注） VTY 回線で SSH および rlogin プロトコルを許可する場合は、AAA 認証を設定する必要があります。VTY 回線の AAA 設定の定義 （52 ページ）を参照してください。

ステップ 9 （任意）ACL の名前を入力して、デバイスとこれらのリスト内のアドレス間における着信接続と発信接続を制限します。または、[選択（Select）] をクリックしてリストから ACL オブジェクトを選択するか、新しい ACL オブジェクトを作成します。標準 ACL または拡張 ACL の中から選択できます。

ヒント 管理アクセスのためだけに VTY 回線を予約する場合は、インバウンド ACL を定義することを推奨します。

ステップ 10 （任意）[AAA] タブをクリックして、このVTY回線（または回線のグループ）の認証、許可、アカウンティング設定を定義します。VTY 回線の AAA 設定の定義 （52 ページ）を参照してください。

ステップ 11 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義が [Lines] テーブルに表示されます。

（注） VTY 回線の定義を削除するには、その定義を選択し、[削除（Delete）] をクリックします。IOS デバイスからVTY回線を削除した場合、後続の回線もすべて削除されます。たとえば、デバイスに回線 0 ～ 9 が含まれる場合、回線 5 を削除すると、回線 6 ～ 9 も削除されます。回線 0 ～ 4 の定義を Security Manager から削除した場合、ルータはインバウンド プロトコル定義を保持し、デバイス上のこれらの回線に対する他のデフォルト設定を復元します。これにより、5 本の VTY 回線を常に使用できるようになります。

VTY 回線の AAA 設定の定義

デフォルトでは、認証、許可、アカウンティングは VTY 回線に対して実行されません。これらのアクセス制御オプションの 1 つ以上を設定するときに、デバイスの AAA ポリシーで定義されたデフォルトの方式リストを使用するか、1 つ以上の AAA 方式を含むカスタム方式リストを定義できます。

はじめる前に

- VTY 回線または VTY 回線のグループの基本パラメータを定義します。 VTY 回線の設定パラメータの定義 （49 ページ） を参照してください。

関連項目

- VTY 回線の設定パラメータの定義 （49 ページ）
- Cisco IOS ルータにおける回線アクセス （45 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [VTY] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [VTY] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[VTY] ページが表示されます。このページのフィールドの説明については、表 20 : [VTY] 回線ページ （65 ページ）を参照してください。

ステップ 2 [回線（Lines）] テーブルで VTY 回線の定義を選択し、[編集（Edit）] ボタンをクリックして [VTY回線（VTY Line）] ダイアログボックスを表示します。次に、[認証（Authentication）] タブをクリックします。

ステップ 3 （任意）VTY 回線にアクセスしようとするユーザに対して実行する認証方式を選択します。

このタブのフィールドの説明については、表 23 : [VTY Line] ダイアログボックス - [Authentication] タブ （71 ページ）を参照してください。

（注） ローカル認証を選択する場合は、展開の前に設定全体をプレビューして、**aaa new-model** コマンドが、（たとえば、AAA ポリシーで方式リストを設定することにより）別のポリシーで設定されていないこと、またはそのデバイス自体にすでに設定されていることを確認します。

ステップ 4 （任意）[Authorization] タブで、VTY 回線にアクセスして EXEC セッションを開始するユーザに対して実行する認可方式を選択します。

[Authorization] タブのフィールドの説明については、表 24 : [VTY Line] ダイアログボックス - [Authorization] タブ （73 ページ）を参照してください。

（注） RADIUS では、認証と認可に同じサーバが使用されます。したがって、認証に RADIUS 方式リストを定義する場合は、認可にも同じ方式リストを定義する必要があります。

ステップ 5 （任意）特定の権限レベルのコマンド認可定義を作成します。

a) [コマンド認可（Commands Authorization）] テーブルの下の [追加（Add）] ボタンをクリックします。[Command Authorization Override] ダイアログボックス （44 ページ）が表示されます。

b) 必要に応じてコマンド認可定義を設定します。

c) [OK] をクリックダイアログボックスが閉じ、認可方式が [Commands Authorization] テーブルに表示されます。

d) 5.a （53 ページ）～5.c （53 ページ）を繰り返して、追加のコマンド認可定義を作成します。

ステップ 6 （任意）[Accounting] タブで、VTY 回線にアクセスしようとするユーザに対して実行する EXEC および接続アカウンティング方式を選択します。

[Accounting] タブのフィールドの説明については、表 25 : [VTY Line] ダイアログボックス - [Accounting] タブ （74 ページ）を参照してください。

ステップ 7 （任意）特定の権限レベルのコマンド アカウンティング定義を作成します。

a) [コマンドアカウンティング（Commands Accounting）] テーブルの下の [追加（Add）] ボタンをクリックします。 [Command Accounting] ダイアログボックス - [Line Access] （80 ページ）が表示されます。

b) 必要に応じてコマンド アカウンティング定義を設定します。

c) [OK] をクリックダイアログボックスが閉じ、アカウンティング方式が [Commands Accounting] テーブルに表示されます。

d) 7.a （53 ページ）～7.c （53 ページ）を繰り返して、追加のコマンド アカウンティング定義を作成します。

[Console] ポリシー ページ

[Console] ページでは、コンソール ポートを介したルータへのアクセスを設定します。[Console] ポリシー ページの次のタブから Cisco IOS ルータ上のコンソール ポリシーを設定できます。

- [Console] ページ - [Setup] タブ （54 ページ）
- [Console] ページ - [Authentication] タブ （56 ページ）
- [Console] ページ - [Authorization] タブ （58 ページ）
- [Console] ページ - [Accounting] タブ （60 ページ）

詳細については、Cisco IOS ルータにおける回線アクセス （45 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [コンソール（Console）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [コンソール（Console）]** を選択します。[コンソール

（Console）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [VTY] ポリシー ページ （65 ページ）

[Console] ページ - [Setup] タブ

[Console] ページの [Setup] タブでは、コンソール ポートの基本パラメータを定義します。これには、ポートにアクセスするためのパスワード、ユーザに割り当てる権限レベル、許可するプロトコル、アクセスを制限する ACL などがあります。

ナビゲーション パス

[Console] ポリシー ページ （53 ページ）に移動し、[セットアップ（Setup）] タブをクリックします。

関連項目

- [Console] ページ - [Authentication] タブ （56 ページ）
- [Console] ページ - [Authorization] タブ （58 ページ）
- [Console] ページ - [Accounting] タブ （60 ページ）
- [VTY Line] ダイアログボックス - [Setup] タブ （67 ページ）

フィールド リファレンス

表 16 : [Console] ページ - [Setup] タブ

要素	説明
[パスワード（Password）]	コンソール ポートにアクセスするためのパスワード。 パスワードは大文字と小文字が区別され、最大 80 文字の英数字を含むことができます。最初の文字を数値にはできません。スペースは使用できません。 [Confirm] フィールドにパスワードを再入力します。

要素	説明
特権レベル	コンソール ポートに接続するユーザに割り当てる権限レベル。有効値の範囲は 0 ～ 15 です。 • 0：**disable**、**enable**、**exit**、**help**、および **logout** の各コマンドにだけアクセス権を付与します。 • 1：ルータへの権限なしアクセスをイネーブルにします（通常の EXEC モードでは権限が使用されます）。 • 15：ルータへの権限付きアクセスをイネーブルにします（従来のイネーブル権限）。 （注） レベル 2 ～ 14 は、通常はデフォルト設定では使用されませんが、通常はレベル 15 にあるコマンドをそれよりも低いレベルに移動し、通常はレベル 1 にあるコマンドをそれよりも高いレベルに移動することで、カスタム設定を作成できます。CLI を使用するか FlexConfig を定義することにより、コマンドの権限レベルを設定できます。 （注） 値を定義しない場合は、デフォルトでレベル 1 が割り当てられます。この値はデバイス設定に表示されません。
Disable all the EXEC sessions to the router via this line	選択すると、この回線を介した EXEC セッションがディセーブルになります。このオプションは、コンソール上での発信接続だけを許可する場合に選択します。このオプションは、回線を独占する可能性がある割り込みデータがコンソール ポートに着信しないようにする場合に役立ちます。 選択を解除すると、コンソール ポートで EXEC セッションがイネーブルになります。これがデフォルトです。 （注） このオプションを選択すると、コンソール ポートを介したデバイスへのすべてのアクセスがブロックされます。
Exec Timeout	EXEC コマンド インタープリタがコンソール ポート上のユーザ入力を検出するまで待機する時間（秒数）。入力が検出されない場合は、回線が切断されます。有効値の範囲は 0 ～ 2147483 です。デフォルトは 600（10 分）です。値を 0 に設定するとタイムアウトがディセーブルになります。 （注） タイムアウトは秒単位で定義されますが、CLI には [mm ss] の形式で表示されます。

要素	説明
Output Protocols	コンソール ポート上の発信接続に使用できるプロトコル。 • [All]：サポートされるすべてのプロトコルが許可されます。サポートされるプロトコルには、LAT、MOP、NASI、PAD、rlogin、SSH、Telnet、および V.120 があります。 • [None]：プロトコルは許可されません。これにより、ポートを発信接続で使用できなくなります。 • [Protocol]：次のプロトコルの 1 つ以上をイネーブルにします。 • [SSH]：セキュア シェル プロトコル。 • [Telnet]：標準 TCP/IP 端末エミュレーション プロトコル。 • [rlogin]：UNIX rlogin プロトコル。 （注） [SSH] と [rlogin] では、AAA 認証を設定する必要があります。[Console] ページ - [Authentication] タブ （56 ページ）を参照してください。 （注） すべての IOS ソフトウェア バージョンで rlogin が出力プロトコルとしてサポートされるわけではありません。
Inbound Access List	コンソール ポート上の着信接続を制限する ACL オブジェクトの名前。ACL オブジェクトの名前を入力するか、[選択（Select）] をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。
Permit VRF Interface Connections	インバウンド ACL がコンソール ポート上で定義されている場合にだけ適用されます。 選択されている場合は、VRF に属するインターフェイスからの着信接続を受け入れます。選択解除されている場合は、VRF に属するインターフェイスからの着信接続を拒否します。
Outbound Access List	コンソール ポート上の発信接続を制限する ACL オブジェクトの名前。ACL オブジェクトの名前を入力するか、[選択（Select）] をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。

[Console] ページ - [Authentication] タブ

[Console] ページの [Authentication] タブでは、コンソール ポートにアクセスしようとするユーザに対して実行する AAA 認証方式を定義します。

ナビゲーション パス

[Console] ポリシー ページ （53 ページ）に移動し、[認証（Authentication）] タブをクリックします。

関連項目

- [Console] ページ - [Setup] タブ （54 ページ）
- [Console] ページ - [Authorization] タブ （58 ページ）
- [Console] ページ - [Accounting] タブ （60 ページ）
- [VTY Line] ダイアログボックス - [Authentication] タブ （70 ページ）

フィールド リファレンス

表 *17 : [Console]* ページ - *[Authentication]* タブ

要素	説明
Authenticate Using	コンソール ポートの認証設定： • [None]：認証は実行されません。これがデフォルトです。 • [Local Database]：ローカル ユーザ名データベースを認証に使用します。 • [AAAポリシーデフォルトリスト（AAA Policy Default List）]：デバイスの AAA ポリシーで定義されているデフォルトの認証方式リストを使用します。 [AAA] ページ - [Authentication] タブ （8 ページ）を参照してください。 • [Custom Method List]：[Authentication Method List] フィールドで指定された認証方式を使用します。 （注） ローカル認証を選択する場合は、展開の前に設定全体をプレビューして、**aaa new-model** コマンドが、（たとえば、AAA ポリシーで方式リストを設定することにより）別のポリシーで設定されていないこと、またはそのデバイス自体にすでに設定されていることを確認します。

要素	説明
Prioritized Method List	[Custom Method List] が認証方式として選択されている場合にだけ適用されます。 ユーザを認証する場合に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認証を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。

[Console] ページ - [Authorization] タブ

[Console] ページの [Authorization] タブでは、コンソール ポートにアクセスするユーザに対して実行する EXEC およびコマンド認可方式を定義します。

（注） この機能を使用するには、ルータで AAA サービスをイネーブルにする必要があります。そうしないと展開が失敗します。 AAA サービスの定義 （5 ページ）を参照してください。

ナビゲーション パス

[Console] ポリシー ページ （53 ページ）に移動し、 [承認（Authorization）] タブをクリックします。

関連項目

- [Console] ページ - [Setup] タブ （54 ページ）
- [Console] ページ - [Authentication] タブ （56 ページ）
- [Console] ページ - [Accounting] タブ （60 ページ）
- [VTY Line] ダイアログボックス - [Authorization] タブ （72 ページ）
- テーブルのフィルタリング

フィールド リファレンス

表 18 : [Console] ページ - [Authorization] タブ

要素	説明
[EXEC Authorization] 設定	
Authorize EXEC Operations Using	ユーザが EXEC セッションの実行を許可されるかどうかを決定する認可方式。 • [None]：認可は実行されません。これがデフォルトです。 • [AAAポリシーデフォルトリスト（AAA Policy Default List）]：デバイスの AAA ポリシーで定義されているデフォルトの認証方式リストを使用します。[AAA] ページ - [Authorization] タブ （9 ページ）を参照してください。 • [Custom Method List]：[EXEC Method List] フィールドで指定された認可方式を使用します。
Prioritized Method List	[Custom Method List] が EXEC 方式として選択されている場合にだけ適用されます。 ユーザを認可する場合に問い合わせる方式の順序付きリストを定義します。Enter the names of one or more AAA server group objects（up to four）, or click **Select** to select them. オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認可を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。 （注） RADIUS では、認証と認可に同じサーバが使用されます。したがって、認証に RADIUS 方式リストを定義する場合は、認可にも同じ方式リストを定義する必要があります。
[Command Authorization] 設定	
特権レベル	コマンド認可定義が適用される権限レベル。
Prioritized Method List	この権限レベルでユーザを認可するときに使用する方式リスト。
[追加（Add）] ボタン	[Command Authorization] ダイアログボックス - [Line Access] （79 ページ）が開きます。ここから、コマンド認可定義を設定できます。

要素	説明
[編集（Edit）] ボタン	[Command Authorization] ダイアログボックス - [Line Access] （79 ページ）が開きます。ここから、コマンド認可定義を編集できます。
[削除（Delete）] ボタン	選択したコマンド認可定義をテーブルから削除します。

[Console] ページ - [Accounting] タブ

[Console] ページの [Accounting] タブでは、コンソール ポートにアクセスするユーザに対して実行する EXEC、接続、およびコマンド アカウンティング方式を定義します。

（注） この機能を使用するには、ルータで AAA サービスをイネーブルにする必要があります。そうしないと展開が失敗します。 AAA サービスの定義 （5 ページ）を参照してください。

ナビゲーション パス

[Console] ポリシー ページ （53 ページ）に移動し、[アカウンティング（Accounting）] タブをクリックします。

関連項目

- [Console] ページ - [Setup] タブ （54 ページ）
- [Console] ページ - [Authentication] タブ （56 ページ）
- [Console] ページ - [Authorization] タブ （58 ページ）
- [VTY Line] ダイアログボックス - [Accounting] タブ （74 ページ）
- テーブルのフィルタリング

フィールド リファレンス

表 19 : [Console] ページ - [Accounting] タブ

要素	説明
[EXEC Accounting] 設定	

要素	説明
Perform EXEC Accounting Using	ユーザEXECセッションに関する基本情報の記録に使用するアカウンティング方式。 • [None]：アカウンティングは実行されません。これがデフォルトです。 • [AAAポリシーデフォルトリスト（AAA Policy Default List）]：デバイスの AAA ポリシーで定義されているデフォルトの EXEC アカウンティング方式リストを使用します。[AAA] ページ - [Accounting] タブ（12 ページ）を参照してください。 • [Custom Method List]：[EXEC Method List] フィールドで指定されたアカウンティング方式を使用します。 EXECアカウンティングは、ユーザ名、日付、開始および終了時刻、アクセス サーバの IP アドレスなど、EXEC セッションに関する基本的な詳細を記録します。
Generate Accounting Records for	[Custom Method List] が EXEC 方式として選択されている場合にだけ適用されます。 デバイスがアカウンティング通知をアカウンティング サーバにいつ送信するかを定義します。 • [Start and Stop]：ユーザ プロセスの開始時と終了時にアカウンティング レコードを生成します。アカウンティングサーバーが「start」アカウンティングレコードを受信するかどうかにかかわらず、ユーザープロセスが開始されます。これがデフォルトです。 • [Stop Only]：ユーザ プロセスの終了時にだけアカウンティング レコードを生成します。 • [None]：アカウンティング レコードは生成されません。

要素	説明
Prioritized Method List	[Custom Method List] が EXEC 方式として選択されている場合にだけ適用されます。 ユーザのアカウンティング方式の作成時に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してアカウンティングの実行を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。
Enable Broadcast to Multiple Servers	[Method List] が EXEC 方式として選択されている場合にだけ適用されます。 選択されている場合、複数の AAA サーバへのアカウンティング レコードの送信をイネーブルにします。アカウンティング レコードは、方式リストに定義されている各 AAA サーバ グループ内の最初のサーバに同時に送信されます。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。 選択解除されている場合、アカウンティング レコードは、方式リストに定義されている最初の AAA サーバ グループ内の最初のサーバにだけ送信されます。
[Connection Accounting] 設定	

要素	説明
Perform Connection Accounting Using	コンソール回線を介して確立されたアウトバウンド接続に関する情報を記録するために使用するアカウンティング方式。 • [None]：アカウンティングは実行されません。これがデフォルトです。 • [AAAポリシーデフォルトリスト（AAA Policy Default List）]：デバイスの AAA ポリシーで定義されているデフォルトの接続アカウンティング方式リストを使用します。 [AAA] ページ - [Accounting] タブ （12 ページ）を参照してください。 • [Custom Method List]：[Connection Method List] フィールドで指定されたアカウンティング方式を使用します。 接続アカウンティングは、Telnet 接続や rlogin 接続など、回線上の発信接続に関する詳細を記録します。
Generate Accounting Records for	[Custom Method List] が接続方式として選択されている場合にだけ適用されます。 デバイスがアカウンティング通知をアカウンティング サーバにいつ送信するかを定義します。 • [Start and Stop]：ユーザ プロセスの開始時と終了時にアカウンティング レコードを生成します。アカウンティングサーバーが「start」アカウンティングレコードを受信するかどうかにかかわらず、ユーザープロセスが開始されます。これがデフォルトです。 • [Stop Only]：ユーザ プロセスの終了時にだけアカウンティング レコードを生成します。 • [None]：アカウンティング レコードは生成されません。

要素	説明
Prioritized Method List	[Custom Method List] が接続方式として選択されている場合にだけ適用されます。 ユーザのアカウンティング方式の作成時に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してアカウンティングの実行を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。
Enable Broadcast to Multiple Servers	[Custom Method List] が接続方式として選択されている場合にだけ適用されます。 選択されている場合、複数の AAA サーバへのアカウンティング レコードの送信をイネーブルにします。アカウンティング レコードは、方式リストに定義されている各 AAA サーバ グループ内の最初のサーバに同時に送信されます。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。 選択解除されている場合、アカウンティング レコードは、方式リストに定義されている最初の AAA サーバ グループ内の最初のサーバにだけ送信されます。
[Command Accounting] 設定	
特権レベル	コマンド認可定義が適用される権限レベル。
Generate Accounting Records for	プロセスで、デバイスがアカウンティング通知をアカウンティング サーバに送信するポイント。
Enable Broadcast	アカウンティング レコードが複数のサーバに同時にブロードキャストされるかどうか。
Prioritized Method List	この権限レベルでユーザを認可するときに使用する方式リスト。
[追加（Add）] ボタン	[Command Accounting] ダイアログボックス - [Line Access] （80 ページ）が開きます。ここから、コマンドアカウンティング定義を設定できます。

要素	説明
[編集（Edit）] ボタン	[Command Accounting] ダイアログボックス - [Line Access] （80 ページ）が開きます。ここから、コマンドアカウンティング定義を編集できます。
[削除（Delete）] ボタン	選択したコマンド アカウンティング定義をテーブルから削除します。

[VTY] ポリシー ページ

[VTY] ページでは、ルータへのリモート アクセス用に最大 16 本の VTY 回線を設定します。個々の回線を設定する以外に、同じ定義を共有する回線のグループを設定できます。

詳細については、Cisco IOS ルータにおける回線アクセス （45 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [VTY] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [VTY] を選択します。[VTY] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存ポリシーを選択します。

関連項目

- [Console] ポリシー ページ （53 ページ）
- テーブル カラムおよびカラム見出しの機能
- テーブルのフィルタリング

フィールド リファレンス

表 *20 : [VTY]* 回線ページ

要素	説明
回線（Line）	VTY 回線の相対回線番号。このフィールドには、連続したグループとして設定された複数の VTY 回線を含めることもできます。
Line/Line Group Parameters	
Input Protocols	VTY 回線上の着信接続に使用できるプロトコル。
Output Protocols	VTY 回線上の発信接続に使用できるプロトコル。

要素	説明
特権レベル	ユーザに割り当てる権限レベル。
Exec Timeout	EXEC コマンド インタープリタがユーザ入力を検出するまで待機する時間。
Inbound ACL	インバウンド トラフィックの制限に使用する ACL。
Outbound ACL	アウトバウンド トラフィックの制限に使用する ACL。
認証	使用する AAA 認証のタイプ。
許可	使用する AAA 認可のタイプ。
アカウンティング	使用する AAA アカウンティングのタイプ。
[VTY] 回線ページのボタン	
[追加（Add）] ボタン	[VTY Line] ダイアログボックス （66 ページ）が開きます。ここから、VTY 回線または回線グループを定義できます。
[編集（Edit）] ボタン	[VTY Line] ダイアログボックス （66 ページ）が開きます。ここから、VTY 回線または回線グループを編集できます。
[削除（Delete）] ボタン	選択した VTY 回線をテーブルから削除します。 IOS デバイスから VTY 回線を削除した場合、後続の回線もすべて削除されます。たとえば、デバイスに回線 0 ～ 9 が含まれる場合、回線 5 を削除すると、回線 6 ～ 9 も削除されます。 （注） デバイス上のデフォルトの VTY 回線（0 ～ 4）を削除した場合は、入力プロトコル設定が保持され、他のデフォルト設定が復元されます。これにより、デバイスへのリモートアクセスが中断されるのを防止できます。

[VTY Line] ダイアログボックス

[VTY Line] ダイアログボックスでは、リモート ユーザによるルータへのアクセスを可能にする 1 つ以上の VTY 回線（最大 16 本）を設定します。VTY 回線を設定するときに、回線にアクセスするユーザに対して実行する認証および認可のタイプを定義できます。

ナビゲーション パス

[VTY] ポリシー ページ （65 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- Cisco IOS ルータにおける回線アクセス （45 ページ）
- [Console] ポリシー ページ （53 ページ）

フィールド リファレンス

表 *21 : [VTY Line]* ダイアログボックス

要素	説明
[Setup] タブ	VTY 回線または回線グループの基本設定を定義します。 [VTY Line] ダイアログボックス - [Setup] タブ （67 ページ）を参照してください。
[Authentication] タブ	VTY 回線にアクセスするユーザに対して実行する AAA 認証のタイプを定義します。 [VTY Line] ダイアログボックス - [Authentication] タブ （70 ページ）を参照してください。
[Authorization] タブ	VTY 回線にアクセスするユーザに対して実行する AAA 認可のタイプを定義します。 [VTY Line] ダイアログボックス - [Authorization] タブ （72 ページ）を参照してください。
[Accounting] タブ	VTY 回線にアクセスするユーザに対して実行する AAA アカウンティングのタイプを定義します。 [VTY Line] ダイアログボックス - [Accounting] タブ （74 ページ） を参照してください。

[VTY Line] ダイアログボックス - [Setup] タブ

[VTY Line] ダイアログボックスの [Setup] タブでは、VTY 回線の基本パラメータを定義します。これには、回線にアクセスするためのパスワード、ユーザに割り当てる権限レベル、回線上で許可するプロトコル、アクセスを制限する ACL などがあります。

ナビゲーション パス

[VTY Line] ダイアログボックス （66 ページ）に移動し、[セットアップ（Setup）] タブをクリックします。

関連項目

- VTY 回線の設定パラメータの定義 （49 ページ）
- [VTY Line] ダイアログボックス - [Authentication] タブ （70 ページ）
- [VTY Line] ダイアログボックス - [Authorization] タブ （72 ページ）
- [VTY Line] ダイアログボックス - [Accounting] タブ （74 ページ）
- [Console] ページ - [Setup] タブ （54 ページ）

フィールド リファレンス

表 *22 : [VTY Line]* ダイアログボックス - *[Setup]* タブ

要素	説明
Starting VTY Line Number	VTY 回線の相対回線番号。VTY 回線のグループを設定する場合は、グループの最初の回線の番号を入力します。有効値の範囲は 0 ～ 15 です。 （注） サポートされる VTY 回線の数（4 ～数千）はルータごとに異なりますが、Security Manager によってサポートされるデバイスあたりの回線数は最大 16 です。同じ回線番号を複数回設定することはできません。
Ending VTY Line Number	回線のグループを設定する場合にだけ適用されます。 グループ内の最後の VTY 回線の相対回線番号。 （注） 回線のグループを設定する場合、グループ内のすべての回線は 0 ～ 4 または 6 ～ 15 のどちらかの範囲内である必要があります。
パスワード	この VTY 回線にアクセスするためのパスワード。 パスワードは大文字と小文字が区別され、最大 80 文字の英数字を含むことができます。最初の文字を数値にはできません。スペースは使用できません。 [Confirm] フィールドにパスワードを再入力します。
特権レベル	この VTY 回線上のユーザに割り当てる権限レベル。有効値の範囲は 0 ～ 15 です。 • 0：**disable**、**enable**、**exit**、**help**、および **logout** の各コマンドにだけアクセス権を付与します。 • 1：ルータへの権限なしアクセスをイネーブルにします（通常の EXEC モードでは権限が使用されます）。 • 15：ルータへの権限付きアクセスをイネーブルにします（従来のイネーブル権限）。 （注） レベル 2 ～ 14 は、通常はデフォルト設定では使用されませんが、通常はレベル 15 にあるコマンドをそれよりも低いレベルに移動し、通常はレベル 1 にあるコマンドをそれよりも高いレベルに移動することで、カスタム設定を作成できます。CLI を使用するか FlexConfig を定義することにより、コマンドの権限レベルを設定できます。 （注） 値を定義しない場合は、デフォルトでレベル 1 が割り当てられます。この値はデバイス設定に表示されません。

要素	説明
Disable all the EXEC sessions to the router via this line	選択すると、この回線を介した EXEC セッションがディセーブルになります。このオプションは、この回線上の発信接続だけを許可する場合に選択します。このオプションは、回線を独占する可能性がある割り込みデータが特定の回線に着信しないようにする場合に役立ちます。 選択を解除すると、この回線を介した EXEC セッションがイネーブルになります。これがデフォルトです。
Exec Timeout	EXEC コマンドインタープリタが回線上のユーザ入力を検出するまで待機する時間（秒数）。入力が検出されない場合は、回線が切断されます。有効値の範囲は 0 ～ 2147483 です。デフォルトは 600（10 分）です。値を 0 に設定するとタイムアウトがディセーブルになります。 （注） タイムアウトは秒単位で定義されますが、CLI には [mm ss] の形式で表示されます。
Input Protocols	この回線上の着信接続に使用できるプロトコル。 • [All]：サポートされるすべてのプロトコルが許可されます。サポートされるプロトコルには、LAT、MOP、NASI、PAD、rlogin、SSH、Telnet、および V.120 があります。 • [None]：プロトコルは許可されません。これにより、ポートを SSH、Telnet、および rlogin の着信接続で使用できなくなります。 （注） 入力プロトコル設定を [None] に設定すると、Security Manager は展開後にデバイスに接続できなくなる可能性があります。HTTP ポリシーで SSL をイネーブルにすると、SSL を使用してデバイスを管理できます。 [HTTP] ページ - [Setup] タブ （40 ページ）を参照してください。 • [Protocol]：次のプロトコルの 1 つ以上をイネーブルにします。 • [SSH]：セキュア シェル プロトコル。 • [Telnet]：標準 TCP/IP 端末エミュレーション プロトコル。 • [rlogin]：UNIX rlogin プロトコル。 （注） [SSH] と [rlogin] では、AAA 認証を設定する必要があります。 [VTY Line] ダイアログボックス - [Authentication] タブ （70 ページ）を参照してください。 （注） すべての IOS ソフトウェア バージョンで rlogin が入力プロトコルとしてサポートされるわけではありません。

要素	説明
Output Protocols	この回線上の発信接続に使用できるプロトコル。 • [All]：サポートされるすべてのプロトコルが許可されます。サポートされるプロトコルには、LAT、MOP、NASI、PAD、rlogin、SSH、Telnet、および V.120 があります。 • [None]：プロトコルは許可されません。これにより、ポートを発信接続で使用できなくなります。 • [Protocol]：次のプロトコルの 1 つ以上をイネーブルにします。 • [SSH]：セキュア シェル プロトコル。 • [Telnet]：標準 TCP/IP 端末エミュレーション プロトコル。 • [rlogin]：UNIX rlogin プロトコル。 （注） [SSH] と [rlogin] では、AAA 認証を設定する必要があります。[VTY Line] ダイアログボックス - [Authentication] タブ （70 ページ）を参照してください。 （注） すべての IOS ソフトウェア バージョンで rlogin が出力プロトコルとしてサポートされるわけではありません。
Inbound Access List	この回線上の着信接続を制限する ACL オブジェクトの名前。ACL オブジェクトの名前を入力するか、[選択（Select）] をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。
Permit VRF Interface Connections	インバウンドACLがこの回線上で定義されている場合にだけ適用されます。 選択されている場合は、VRF に属するインターフェイスからの着信接続を受け入れます。選択解除されている場合は、VRF に属するインターフェイスからの着信接続を拒否します。
Outbound Access List	この回線上の発信接続を制限する ACL オブジェクトの名前。ACL オブジェクトの名前を入力するか、[選択（Select）] をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。

[VTY Line] ダイアログボックス - [Authentication] タブ

[VTY Line] ダイアログボックスの [Authentication] タブでは、選択した VTY 回線または回線グループにアクセスしようとするユーザに対して実行する認証方式を定義します。

ナビゲーション パス

[VTY Line] ダイアログボックス （66 ページ）に移動し、[認証（Authentication）] タブをクリックします。

関連項目

- VTY 回線の AAA 設定の定義 （52 ページ）
- [VTY Line] ダイアログボックス - [Setup] タブ （67 ページ）
- [VTY Line] ダイアログボックス - [Authorization] タブ （72 ページ）
- [VTY Line] ダイアログボックス - [Accounting] タブ （74 ページ）
- [Console] ページ - [Authentication] タブ （56 ページ）

フィールド リファレンス

表 23 : [VTY Line] ダイアログボックス - [Authentication] タブ

要素	説明
Authenticate Using	VTY 回線の認証設定： • [None]：認証は実行されません。これがデフォルトです。 • [Local Database]：ローカル ユーザ名データベースを認証に使用します。 • [AAAポリシーデフォルトリスト（AAA Policy Default List）]：デバイスの AAA ポリシーで定義されているデフォルトの認証方式リストを使用します。 [AAA] ページ - [Authentication] タブ （8 ページ）を参照してください。 • [Custom Method List]：[Prioritized Method List] フィールドで指定された認証方式を使用します。 （注） ローカル認証を選択する場合は、展開の前に設定全体をプレビューして、**aaa new-model** コマンドが、（たとえば、AAA ポリシーで方式リストを設定することにより）別のポリシーで設定されていないこと、またはそのデバイス自体にすでに設定されていることを確認します。

要素	説明
Prioritized Method List	[Custom Method List] が認証方式として選択されている場合にだけ適用されます。 ユーザを認証する場合に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認証を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。

[VTY Line] ダイアログボックス - [Authorization] タブ

[VTY Line] ダイアログボックスの [Authorization] タブでは、選択した VTY 回線または回線グループにアクセスするユーザに対して実行する EXEC およびコマンド認可方式を定義します。

（注） この機能を使用するには、ルータで AAA サービスをイネーブルにする必要があります。そうしないと展開が失敗します。 AAA サービスの定義 （5 ページ）を参照してください。

ナビゲーション パス

[VTY Line] ダイアログボックス （66 ページ）に移動し、 **Authorization** tab.

関連項目

- VTY 回線の AAA 設定の定義 （52 ページ）
- [VTY Line] ダイアログボックス - [Setup] タブ （67 ページ）
- [VTY Line] ダイアログボックス - [Authentication] タブ （70 ページ）
- [VTY Line] ダイアログボックス - [Accounting] タブ （74 ページ）
- [Console] ページ - [Authentication] タブ （56 ページ）
- テーブルのフィルタリング

フィールド リファレンス

表 *24 : [VTY Line]* ダイアログボックス - *[Authorization]* タブ

要素	説明
[EXEC Authorization] 設定	
Authorize EXEC Operations Using	ユーザが EXEC セッションの実行を許可されるかどうかを決定する認可方式。 • [None]：認可は実行されません。これがデフォルトです。 • [AAAポリシーデフォルトリスト（AAA Policy Default List）]：デバイスのAAAポリシーで定義されているデフォルトの認証方式リストを使用します。 [AAA] ページ - [Authorization] タブ （9 ページ）を参照してください。 • [Custom Method List]：[Prioritized Method List] フィールドで指定された認可方式を使用します。
Prioritized Method List	[Custom Method List] が EXEC 方式として選択されている場合にだけ適用されます。 ユーザを認可する場合に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）]をクリックして選択します。オブジェクトセレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）]ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認可を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として[None]を選択した場合は、リストの最後の方式として表示される必要があります。 （注） RADIUS では、認証と認可に同じサーバが使用されます。したがって、認証にRADIUS方式リストを定義する場合は、認可にも同じ方式リストを定義する必要があります。
[Command Authorization] 設定	
特権レベル	コマンド認可定義が適用される権限レベル。
Prioritized Method List	この権限レベルでユーザを認可するときに使用する方式リスト。
[追加（Add）]ボタン	[Command Authorization] ダイアログボックス - [Line Access] （79 ページ）が開きます。ここから、コマンド認可定義を設定できます。

要素	説明
[編集（Edit）] ボタン	[Command Authorization] ダイアログボックス - [Line Access] （79 ページ）が開きます。ここから、コマンド認可定義を編集できます。
[削除（Delete）] ボタン	選択したコマンド認可定義をテーブルから削除します。

[VTY Line] ダイアログボックス - [Accounting] タブ

[VTY Line] ダイアログボックスの [Accounting] タブでは、選択した VTY 回線または回線グループにアクセスするユーザに対して実行する EXEC、接続、およびコマンドアカウンティング方式を定義します。

（注） この機能を使用するには、ルータで AAA サービスをイネーブルにする必要があります。そうしないと展開が失敗します。 AAA サービスの定義 （5 ページ）を参照してください。

ナビゲーション パス

[VTY Line] ダイアログボックス （66 ページ）に移動し、[アカウンティング（Accounting）] タブをクリックします。

関連項目

- VTY 回線の AAA 設定の定義 （52 ページ）
- [VTY Line] ダイアログボックス - [Setup] タブ （67 ページ）
- [VTY Line] ダイアログボックス - [Authentication] タブ （70 ページ）
- [Console] ページ - [Accounting] タブ （60 ページ）
- テーブルのフィルタリング

フィールド リファレンス

表 *25 : [VTY Line]* ダイアログボックス - *[Accounting]* タブ

要素	説明
[EXEC Accounting] 設定	

要素	説明
Perform EXEC Accounting Using	ユーザ EXEC セッションに関する基本情報の記録に使用するアカウンティング方式。 • [None]：アカウンティングは実行されません。これがデフォルトです。 • [AAA Policy Default List]：デバイスの AAA ポリシーで定義されているデフォルトの EXEC アカウンティング方式リストを使用します。[AAA] ページ - [Accounting] タブ （12 ページ）を参照してください。 • [Custom Method List]：[Prioritized Method List] フィールドで指定されたアカウンティング方式を使用します。 EXEC アカウンティングは、ユーザ名、日付、開始および終了時刻、アクセス サーバの IP アドレスなど、EXEC セッションに関する基本的な詳細を記録します。
Generate Accounting Records for	[Custom Method List] が EXEC 方式として選択されている場合にだけ適用されます。 デバイスがアカウンティング通知をアカウンティング サーバにいつ送信するかを定義します。 • [Start and Stop]：ユーザ プロセスの開始時と終了時にアカウンティング レコードを生成します。アカウンティングサーバーが「start」アカウンティングレコードを受信するかどうかにかかわらず、ユーザープロセスが開始されます。これがデフォルトです。 • [Stop Only]：ユーザ プロセスの終了時にだけアカウンティング レコードを生成します。 • [None]：アカウンティング レコードは生成されません。

要素	説明
Prioritized Method List	[Custom Method List] が EXEC 方式として選択されている場合にだけ適用されます。 ユーザのアカウンティング方式の作成時に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）]ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してアカウンティングの実行を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。
Enable Broadcast to Multiple Servers	[Method List] が EXEC 方式として選択されている場合にだけ適用されます。 選択されている場合、複数の AAA サーバへのアカウンティング レコードの送信をイネーブルにします。アカウンティング レコードは、方式リストに定義されている各 AAA サーバ グループ内の最初のサーバに同時に送信されます。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。 選択解除されている場合、アカウンティング レコードは、方式リストに定義されている最初の AAA サーバ グループ内の最初のサーバにだけ送信されます。
[Connection Accounting] 設定	

要素	説明
Perform Connection Accounting Using	VTY 回線を介して確立されたアウトバウンド接続に関する情報を記録するために使用するアカウンティング方式。 • [None]：アカウンティングは実行されません。これがデフォルトです。 • [AAA Policy Default List]：デバイスの AAA ポリシーで定義されているデフォルトの接続アカウンティング方式リストを使用します。[AAA] ページ - [Accounting] タブ （12 ページ）を参照してください。 • [Custom Method List]：[Prioritized Method List] フィールドで指定されたアカウンティング方式を使用します。 接続アカウンティングは、Telnet 接続や rlogin 接続など、回線上の発信接続に関する詳細を記録します。
Generate Accounting Records for	[Custom Method List] が接続方式として選択されている場合にだけ適用されます。 デバイスがアカウンティング通知をアカウンティング サーバにいつ送信するかを定義します。 • [Start and Stop]：ユーザ プロセスの開始時と終了時にアカウンティング レコードを生成します。アカウンティングサーバーが「start」アカウンティングレコードを受信するかどうかにかかわらず、ユーザープロセスが開始されます。これがデフォルトです。 • [Stop Only]：ユーザ プロセスの終了時にだけアカウンティング レコードを生成します。 • [None]：アカウンティング レコードは生成されません。

要素	説明
Prioritized Method List	[Custom Method List] が接続方式として選択されている場合にだけ適用されます。 ユーザのアカウンティング方式の作成時に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）]ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してアカウンティングの実行を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。
Enable Broadcast to Multiple Servers	[Custom Method List] が接続方式として選択されている場合にだけ適用されます。 選択されている場合、複数の AAA サーバへのアカウンティング レコードの送信をイネーブルにします。アカウンティング レコードは、方式リストに定義されている各 AAA サーバ グループ内の最初のサーバに同時に送信されます。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。 選択解除されている場合、アカウンティング レコードは、方式リストに定義されている最初の AAA サーバ グループ内の最初のサーバにだけ送信されます。
[Command Accounting] 設定	
特権レベル	コマンド認可定義が適用される権限レベル。
Generate Accounting Records for	プロセスで、デバイスがアカウンティング通知をアカウンティング サーバに送信するポイント。
Enable Broadcast	アカウンティング レコードが複数のサーバに同時にブロードキャストされるかどうか。
Prioritized Method List	この権限レベルでユーザを認可するときに使用する方式リスト。
[追加（Add）] ボタン	[Command Accounting] ダイアログボックス - [Line Access] （80 ページ）が開きます。ここから、コマンドアカウンティング定義を設定できます。

要素	説明
[編集（Edit）] ボタン	[Command Accounting] ダイアログボックス - [Line Access] （80 ページ）が開きます。ここから、コマンドアカウンティング定義を編集できます。
[削除（Delete）] ボタン	選択したコマンド アカウンティング定義をテーブルから削除します。

[Command Authorization] ダイアログボックス - [Line Access]

[Command Authorization] ダイアログボックスでは、特定の権限に関連付けられている EXEC コマンドを認可するときに使用する方式を定義します。これにより、特定の権限レベル（0 ～ 15）に関連付けられているすべてのコマンドを認可できます。

ナビゲーション パス

[Console] ページ - [Authorization] タブ （58 ページ）または [VTY Line] ダイアログボックス - [Authorization] タブ （72 ページ）で、[コマンド認可（Command Authorization）] テーブルの下にある [追加（Add）] ボタンをクリックします。

関連項目

- [Console] ポリシー ページ （53 ページ）
- [VTY] ポリシー ページ （65 ページ）

フィールド リファレンス

表 26 : [Command Authorization] ダイアログボックス - [Line Access]

要素	説明
Privilege Level	コマンド認可リストを定義する権限レベル。有効値の範囲は 0 ～ 15 です。 （注） 値を定義しない場合は、デフォルトでレベル 1 が割り当てられます。この値はデバイス設定に表示されません。
AAA Policy Default List	このオプションを選択すると、デバイスの AAA ポリシーで定義されているデフォルトの認可リストがこの権限レベルに関連付けられている EXEC コマンドに適用されます。[Command Accounting] ダイアログボックス （15 ページ）を参照してください。
Custom Method List	このオプションを選択すると、この権限レベルの認可方式リストを定義できます。

要素	説明
Prioritized Method List	[Custom Method List] オプションが選択されている場合にだけ適用されます。 ユーザを認可する場合に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認可を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。

[Command Accounting] ダイアログボックス - [Line Access]

[Command Accounting] ダイアログボックスでは、特定の権限に対して実行される EXEC コマンドに関する情報を記録するときに使用する方式を定義します。各アカウンティング レコードには、その権限レベルに対して実行されるコマンドのリストと、各コマンドが実行された日時およびそのコマンドを実行したユーザ名が含まれます。

ナビゲーション パス

[Console] ページ - [Accounting] タブ （60 ページ）または [VTY Line] ダイアログボックス - [Accounting] タブ （74 ページ）で、[コマンドアカウンティング（Command Accounting）] テーブルの下にある [追加（Add）] ボタンをクリックします。

関連項目

- [Console] ポリシー ページ （53 ページ）
- [VTY] ポリシー ページ （65 ページ）

フィールド リファレンス

表 27 : [Command Accounting] ダイアログボックス - [Line Access]

要素	説明
Privilege Level	コマンドアカウンティング リストを定義する権限レベル。有効値の範囲は 0 ～ 15 です。 （注） 値を定義しない場合は、デフォルトでレベル 1 が割り当てられます。この値はデバイス設定に表示されません。

要素	説明
AAA Policy Default List	このオプションを選択すると、デバイスの AAA ポリシーで定義されているデフォルトのアカウンティングリストがこの権限レベルに対して実行される EXEC コマンドに適用されます。
Custom Method List	このオプションを選択すると、この権限レベルのアカウンティング方式リストを定義できます。
Generate Accounting Records for	[Custom Method List] が選択されている場合にだけ適用されます。 デバイスがアカウンティング通知をアカウンティング サーバにいつ送信するかを定義します。 • [Start and Stop]：ユーザ プロセスの開始時と終了時にアカウンティング レコードを生成します。アカウンティングサーバーが「start」アカウンティングレコードを受信するかどうかにかかわらず、ユーザープロセスが開始されます。これがデフォルトです。 • [Stop Only]：ユーザ プロセスの終了時にだけアカウンティング レコードを生成します。 • [None]：アカウンティング レコードは生成されません。
Prioritized Method List	[Custom Method List] オプションが選択されている場合にだけ適用されます。 ユーザのアカウンティング レコードの作成時に使用するアカウンティング方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（最大 4 つ）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクトセレクタの上向きおよび下向き矢印を使用して、選択したサーバグループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してアカウンティングの実行を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。

要素	説明
Enable Broadcast to Multiple Servers	[Custom Method List] が選択されている場合にだけ適用されます。 選択されている場合、複数の AAA サーバへのアカウンティング レコードの送信をイネーブルにします。アカウンティング レコードは、方式リストに定義されている各 AAA サーバ グループ内の最初のサーバに同時に送信されます。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。 選択解除されている場合、アカウンティング レコードは、方式リストに定義されている最初の AAA サーバ グループ内の最初のサーバにだけ送信されます。

Cisco IOS ルータにおける任意の SSH 設定

Secure Shell（SSH; セキュア シェル）はアプリケーションであり、暗号化を使用してクライアントとサーバ間のセキュアな通信を提供するプロトコルです。SSH を使用すると、リモートから VTY 回線を介して Cisco IOS ルータに接続したり、EXEC セッションを確立したりできます。セキュリティ面が懸念される環境では、Telnet や rlogin などの他のプロトコルの代わりに SSH を使用することを推奨します。

Security Manager に Cisco IOS ルータを追加するには、それらのすべてのルータに SSH が設定されている必要があります。これは、Security Manager は SSL 以外に SSH を使用してルータと通信するためです。SSH ポリシーを使用すると、選択したデフォルト設定を変更したり、選択した任意の設定を定義したりできます。

関連項目

- 任意の SSH 設定の定義　（82 ページ）
- デバイスの通信要件について
- SSH の設定

任意の SSH 設定の定義

SSH は、デフォルトでは次のように設定されます。

- SSH バージョン 1 と SSH バージョン 2 の両方がサポートされます。
- ネゴシエーション フェーズは、120 秒後に正常に完了しない場合は終了します。
- ルータは切断前に SSH クライアントの認証を 3 回試行します。

Security Manager を使用して、次のデフォルト設定を変更したり、任意で次の設定を定義したりできます。

- SSH パケットの送信元インターフェイス
- 使用する RSA キー ペアの名前
- 次の展開時にキーを生成するかどうか

はじめる前に

- ルータで SSH がイネーブルになっていることを確認します。デバイスの通信要件についてを参照してください。
- ルータ上の VTY 回線でインバウンド SSH トラフィックが許可されていることを確認します。 VTY 回線の設定パラメータの定義 （49 ページ）を参照してください。
- ルータでホスト名とドメイン名が設定されていることを確認します（別の RSA キー ペアを使用する場合を除く）。このために Security Manager で CLI またはホスト名ポリシーを使用できます。 Cisco IOS ルータにおけるホスト名とドメイン名 （100 ページ） を参照してください。

関連項目

- Cisco IOS ルータにおける任意の SSH 設定 （82 ページ）
- SSH の設定

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [Secure Shell] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [Secure Shell] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Secure Shell] ページが表示されます。このページのフィールドの説明については、 [Secure Shell] ポリシー ページ （84 ページ）を参照してください。

ステップ 2 （任意）次のデフォルト設定を変更します。

a) サポートする SSH のバージョン
b) SSH 接続のネゴシエーション フェーズを完了するためのタイムアウト
c) SSH クライアントの認証を試行する回数

ステップ 3 （任意）[送信元インターフェイス（Source Interface）] フィールドに、インターフェイスまたはインターフェイスロールの名前を入力します。これが、SSH クライアントに送信されるすべての SSH パケットの送信元インターフェイスとして使用されます。あるいは、[選択（Select）] をクリックしてリストからインターフェイス ロール オブジェクトを選択するか、新しいインターフェイス ロール オブジェクトを作成します。送信元インターフェイスには IP アドレスが必要です。

このフィールドに値を入力しない場合は、宛先に最も近いインターフェイスのアドレスが使用されます。

ステップ 4 （任意）SSH 接続に使用する RSA キー ペアの名前を入力します。このフィールドに値を入力しない場合は、ホスト名とドメイン名に基づくキー ペアが使用されます。

ヒント CLI コマンド show crypto key mypubkey rsa を使用して、デバイスに設定されている各キー ペアの名前と値を表示します。

ステップ 5 （任意）SSHに使用するRSAキーペアをルータで再生成する場合は、[展開中にキーを再生成する（Regenerate Key During Deployment）]チェックボックスをオンにします。このオプションは、キーの機密性が失われる可能性がある場合に便利です。キーの再生成に使用する係数のサイズを入力します。

（注） 展開後にこのポリシーに戻ってチェックボックスをオフにする必要があります。チェックボックスをオフにしないと、展開のたびに新しいキーが生成されます。

（注） このオプションでは、展開中にデバイスとの対話が必要です。したがって、ファイルを展開するときではなく、ライブ デバイスを展開するときにだけ使用する必要があります。

（注） キーペアは、このオプションを選択する前にデバイスにすでに存在する必要があります。そうでないと展開が失敗します（IOS ルータを Security Manager に追加するには、ルータで SSH がイネーブルになっている必要があるため、一般的にはこのような状況になります）。

[Secure Shell] ポリシー ページ

[Secure Shell] ページでは、必要に応じて、ルータ上のデフォルトの SSH 設定を変更したり、他の任意の設定を定義したりできます。

詳細については、Cisco IOS ルータにおける任意の SSH 設定 （82 ページ）を参照してください。

（注） デバイスを Security Manager に追加する前に、CLI コマンドを使用してデバイスに SSH を設定する必要があります。これは、Security Manager は SSH と SSL を使用して Cisco IOS ルータと通信するためです。詳細については、SSH の設定を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [Secure Shell] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [Secure Shell] を選択します。[Secure Shell] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- デバイスの通信要件について
- [VTY] ポリシー ページ （65 ページ）
- [Console] ポリシー ページ （53 ページ）

フィールド リファレンス

表 *28 : [Secure Shell]* ページ

要素	説明
SSH Version	ルータに接続するときに使用する SSH のバージョン。 • [1 and 2]：SSH バージョン 1 と SSH バージョン 2。これがデフォルトです。 • [1]：SSH バージョン 1 だけ。 • [2]：SSH バージョン 2 だけ。
タイムアウト（Timeout）	接続の切断前に、ルータがネゴシエーション フェーズ中に SSH クライアントの応答を待機する時間。デフォルト値（および最大値）は 120 秒です。 （注） ネゴシエーションが終了して EXEC セッションが開始されると、VTY 回線に設定されているタイムアウトが適用されます。[VTY Line] ダイアログボックス - [Setup] タブ （67 ページ）を参照してください。
Authentication Retries	ルータが SSH クライアントの認証を試行する回数有効値の範囲は 0 ～ 5 です。デフォルトは 3 です。
送信元インターフェイス（Source Interface）	SSH クライアントに送信されるすべての SSH パケットの送信元アドレス。 このフィールドで値を定義しない場合は、宛先に最も近いインターフェイス（つまり、SSH パケットの送信に使用される出力インターフェイス）のアドレスが使用されます。 インターフェイスの名前またはインターフェイスのロールを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

要素	説明
RSA キーペア	SSH 接続に使用する RSA キー ペアの名前。 値を入力しない場合は、ホスト名とドメイン名に基づいて生成された RSA キー ペアが使用されます。これがデフォルトです。 ヒント　CLI コマンド **show crypto key mypubkey rsa** を使用して、デバイスに設定されている各キーペアの名前と値を表示します。これらは、このフィールドに入力できる有効な名前です。
展開中にキーを再生成	選択すると、次回の展開時にルータで RSA キーペアを再生成します。このオプションは、キーの機密性が失われる可能性がある場合に便利です。 選択を解除すると、新しいキー ペアは生成されません。 （注）　このチェックボックスは、展開後に自動的にオフになりません。このポリシーに戻ってチェックボックスの選択を解除しないと、展開を行うたびにキーが再生成されます。 （注）　このオプションでは、展開中にデバイスとの対話が必要です。したがって、ファイルを展開するときではなく、ライブ デバイスを展開するときにだけ使用する必要があります。 （注）　キーペアは、このオプションを選択する前にデバイスにすでに存在する必要があります。そうでないと展開が失敗します（IOS ルータを Security Manager に追加するには、ルータで SSH が有効になっている必要があるため、一般的にはこのような状況になります）。
Modulus Size	[Regenerate Key] チェックボックスがオンになっている場合にだけ適用されます。 新しいキー ペアの生成に使用される係数のサイズ。係数が大きいほどセキュリティが高くなりますが、生成に時間がかかります。有効な値の範囲は 360 ～ 2048 ビットです。デフォルトは 1024 ビットです。

Cisco IOS ルータの SNMP

簡易ネットワーク管理プロトコル（SNMP）は、ネットワーク管理ステーションまたはワークステーションが、スイッチ、ルータ、ファイアウォールデバイスなどのさまざまなタイプのデバイスのヘルスとステータスをモニタするための標準的な方法を定義します。SNMP は、プロトコル、データベース構造の仕様、および一連の管理データベース オブジェクトで構成されます。各 SNMP デバイスまたはメンバはコミュニティに含まれ、コミュニティによって各デバイスのアクセス権（読み取り専用または読み取り/書き込み）が決まります。

SNMP は、管理情報ベース（MIB）を介して管理対象デバイスから情報を取得します。MIB は、MIB オブジェクトと呼ばれるコード ブロックのデータベースであり、各 MIB オブジェクトは固有の 1 つの機能を制御します。MIB オブジェクトは、MIB オブジェクト名、説明、デ

フォルト値などを定義する MIB 変数で構成されます。MIB オブジェクトは MIB ツリーという階層構造になっています。

SNMP ポリシーを使用して、ルータで実行されている SNMP エージェントの動作を設定できます。エージェントは、イベントが発生すると、未承諾の情報を SNMP ホストに送り返します。ルータ上で事前に定義された重要なイベントに応答して生成されるこれら未承諾のメッセージは、トラップと呼ばれます。

ここでは、Cisco IOS ルータ上に SNMP ポリシーを作成するために実行するタスクについて説明します。

• SNMP エージェントのプロパティの定義 （87 ページ）
• SNMP トラップの有効化 （88 ページ）

SNMP エージェントのプロパティの定義

SNMP エージェントのプロパティを定義するときに、コミュニティストリングとコミュニティストリング タイプ、およびトラップを受信する SNMP ホストのアドレスとプロパティを定義する必要があります。

SNMP コミュニティストリングは MIB に対する組み込みパスワードであり、ルータの動作に関するデータを格納して、リモートユーザーの認証に使用できます。コミュニティストリングには 2 つのタイプがあります。「パブリック」コミュニティストリングは、MIB 内のすべてのオブジェクト（コミュニティストリング自体を除く）への読み取りアクセスを提供し、「プライベート」コミュニティストリングは、MIB 内のすべてのオブジェクト（コミュニティストリングを除く）への読み書きアクセスを提供します。

SNMP ホストは、ルータによって生成されたトラップを受信します。SNMP ホストにアクセスするためのアドレス、パスワード、ポート番号、および使用する SNMP バージョンを定義する必要があります。Security Manager は、SNMP バージョン 1、バージョン 2c（「コミュニティベースの SNMP」とも呼ばれる）、およびバージョン 3（認証と暗号化を提供）をサポートしています。

関連項目

• Cisco IOS ルータの SNMP （86 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[SNMP] ページが表示されます。このページのフィールドの説明については、表 29 : [SNMP] ページ （90 ページ）を参照してください。

ステップ 2 MIB へのアクセスに必要なコミュニティ ストリングを定義します。

a) [権限（Permissions）] の下にある [追加（Add）] をクリックして、[権限（Permission）] ダイアログボックスを表示します。

b) ストリングを定義します。使用可能なフィールドの説明については、表 30 : [Permission] ダイアログボックス （92 ページ）を参照してください。

c) [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義が [Permissions] テーブルに表示されます。

（注） SNMP ホストで使用中のコミュニティ ストリングを編集または削除しようとすると、警告が表示されます。操作を続行すると、デバイスは、[トラップ受診者（Trap Receiver）] テーブルに含まれるホストの定義に一致するプライベートの読み取り専用文字列を作成します。

ステップ 3 SNMP エージェントによって生成されたトラップを受信する SNMP ホストを定義します。

a) [トラップ受信者（Trap Receiver）] の下にある [追加（Add）] をクリックして、[トラップ受信者（Trap Receiver）] ダイアログボックスを表示します。

b) ホストを定義します。使用可能なフィールドの説明については、[Trap Receiver] ダイアログボックス （92 ページ）を参照してください。

c) [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義が [Trap Receiver] テーブルに表示されます。

ステップ 4 [SNMP Server Properties] で、この SNMP ポリシーが設定されたルータを担当する管理者の場所と連絡先情報を入力します。

この定義はテキストで指定します。ルータの動作には影響を与えません。SNMP ホストのマネージャが特定のトラップを調査するときに役立つ情報を指定します。

ステップ 5 [トラップの設定（Configure Traps）] をクリックして [SNMP トラップ（SNMP Traps）] ダイアログボックスを表示します。このダイアログボックスは、ルータ上でイネーブルにするトラップを選択するために使用します。詳細については、SNMP トラップの有効化 （88 ページ）を参照してください。

SNMP トラップの有効化

定義されている条件（リンク アップ、リンク ダウン、syslog イベントなど）が発生すると、ルータはすぐに SNMP トラップとも呼ばれる通知を、指定された SNMP ホスト（管理ステーション）に送信します。

SNMP トラップをイネーブルにするには、関連する各トラップの横にあるチェックボックスをオンにします。複数の関連するトラップをアクティブにするチェックボックスもあります。

（注） イネーブルにした各トラップは、システム リソースを消費します。システム パフォーマンスへの影響を軽減するには、ネットワーク モニタリングに必要なトラップだけを選択します。

関連項目

- Cisco IOS ルータの SNMP （86 ページ）

ステップ 1 SNMP エージェントのプロパティの定義 （87 ページ）の説明に従って、Cisco IOS ルータ上の SNMP サーバ ポリシーを定義するための [SNMP] ページを開きます。

ステップ 2 [SNMP] ページで、[トラップの設定（Configure Traps）] をクリックします。[SNMP Traps] ダイアログボックスが表示されます。

ステップ 3 イネーブルにするトラップの各タイプの横にあるチェックボックスをオンにします。トラップは、次の 4 つのカテゴリに分類されます。

- 標準の SNMP トラップ（Authentication、Cold Start、Warm Start など）
- ISAKMP トラップ（IPsec プロセスのフェーズ 1 に関連するトラップ）
- IPsec トラップ（IPsec プロセスのフェーズ 2 に関連するトラップ）
- その他のトラップ（syslog メッセージ、プロトコル関連の通知、CPU 使用率の警告など）

使用可能なトラップの説明については、表 32 : [SNMP Traps] ダイアログボックス （95 ページ）を参照してください。

（注） IP マルチキャストと CPU トラップを完全に実装するには、コマンドライン インターフェイス（CLI）のコマンドを追加する必要があります。コマンドの入力に使用できる 1 つの方法として、FlexConfig を使用する方法があります。FlexConfig ポリシーとポリシー オブジェクトについてを参照してください。

ヒント [すべて選択（Select All）] をクリックしてダイアログボックスに表示されるすべてのトラップをイネーブルにするか、または [すべて選択解除（Deselect All）] をクリックしてすべてのトラップをディセーブルにします。

ステップ 4 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。

ヒント このダイアログボックスに表示されない SNMP トラップを設定するには、FlexConfig を定義します。

[SNMP] ポリシー ページ

[SNMP] ページでは、トラップをルータから指定した SNMP ホストに送信するために必要なパラメータを設定します。これらのトラップは、SNMP ホストにルータで発生している重要なイベントを通知する割り込みメッセージです。

詳細については、 SNMP エージェントのプロパティの定義 （87 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択します。[SNMP] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータの SNMP （86 ページ）
- テーブル カラムおよびカラム見出しの機能
- テーブルのフィルタリング

フィールド リファレンス

表 *29 : [SNMP]* ページ

要素	説明
[Permissions] テーブル	
コミュニティ ストリング（Community String）	ルータの MIB へのアクセスに使用するコミュニティストリング。
タイプ（Type）	コミュニティ ストリング タイプ（[read-only] または [read-write]）。
ACL	ルータの MIB へのアクセスが許可される IP アドレスを定義する標準の ACL。
[追加（Add）] ボタン	[Permission] ダイアログボックス （91 ページ）が開きます。ここから、トラップの生成に必要なコミュニティ ストリングとタイプを入力できます。
[編集（Edit）] ボタン	[Permission] ダイアログボックス （91 ページ）が開きます。ここから、選択した権限プロファイルを編集できます。
[削除（Delete）] ボタン	選択した権限プロファイルをテーブルから削除します。
[Trap Receiver] テーブル	
ホスト IP アドレス	ルータによって生成されたトラップを受信する SNMP ホストの IP アドレス。

要素	説明
SNMP バージョン（SNMP Version）	ルータによって使用される SNMP バージョン。
UDP ポート（UDP Port）	SNMP ホストによって使用される UDP ポート。
[追加（Add）] ボタン	[Trap Receiver] ダイアログボックス （92 ページ）が開きます。ここから、ルータによって生成されたトラップを受信する SNMP ホストを定義できます。
[編集（Edit）] ボタン	[Trap Receiver] ダイアログボックス （92 ページ） を開きます。ここから、選択した SNMP ホストを編集できます。
[削除（Delete）] ボタン	選択した SNMP ホストをテーブルから削除します。
その他のフィールドおよびボタン	
SNMP Server Properties	SNMP サーバ/エージェント（つまりルータ）を担当するシステム管理者の名前と連絡先情報。SNMP ホストを管理する担当者は、異常なイベントの発生元を追跡するときにこの情報を使用できます。 これらの各プロパティの最大長は、スペースを含めて 255 文字です。 （注） これらのフィールドに入力した値はすべてテキストであり、ルータの動作に影響しません。
[Configure Traps] ボタン	ルータが生成する SNMP トラップを選択するためのダイアログボックスを開きます。 [SNMP Traps] ダイアログボックス （94 ページ） を参照してください。

[Permission] ダイアログボックス

[Permission] ダイアログボックスでは、SNMP ポリシーに必要なコミュニティ ストリングとストリング タイプを定義します。コミュニティ ストリングは、ルータに関する動作データが格納されている管理情報ベース（MIB）にアクセスするための、組み込みパスワードです。

ナビゲーション パス

[SNMP] ポリシー ページ （89 ページ）に移動し、[権限（Permissions）] テーブルの下にある [追加（Add）] ボタンまたは [編集（Edit）] ボタンをクリックします。

関連項目

- [SNMP] ポリシー ページ （89 ページ）
- [Trap Receiver] ダイアログボックス （92 ページ）

- [SNMP Traps] ダイアログボックス （94 ページ）
- SNMP エージェントのプロパティの定義 （87 ページ）
- Cisco IOS ルータの SNMP （86 ページ）

フィールド リファレンス

表 *30 : [Permission]* ダイアログボックス

要素	説明
コミュニティ ストリング（Community String）	ルータの MIB にアクセスするためのコミュニティストリング。文字列の長さの範囲は 1 ～ 128 文字です。
アクセス コントロール リスト	Cisco IOS ソフトウェア Release 12.3(2)T 以上（T トレイン）または 12.4 バージョンを実行しているルータだけに適用されます。 ルータの MIB にアクセスできる IP アドレスを含む標準の ACL。ACL を定義すると、コミュニティ ストリングを使用できる送信元アドレスを制限することによって、セキュリティを強化できます。 標準の ACL オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。
Read-Write	このコミュニティ ストリング タイプを選択すると、MIB 内のすべてのオブジェクト（コミュニティ ストリングを除く）への読み書きアクセスが提供されます。
読み取り専用	このコミュニティ ストリング タイプを選択すると、MIB 内のすべてのオブジェクト（コミュニティ ストリングを除く）への読み取り専用アクセスが提供されます。これがデフォルトです。

[Trap Receiver] ダイアログボックス

[Trap Receiver] ダイアログボックスでは、ルータによって生成されたトラップを受信する SNMP ホストを定義します。これには、使用する SNMP のバージョンの定義が含まれます。

ナビゲーション パス

[SNMP] ポリシー ページ （89 ページ）に移動してから、[トラップの受信者（Trap Receiver）] テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- [SNMP] ポリシー ページ （89 ページ）

- [Permission] ダイアログボックス （91 ページ）
- [SNMP Traps] ダイアログボックス （94 ページ）
- SNMP エージェントのプロパティの定義 （87 ページ）
- Cisco IOS ルータの SNMP （86 ページ）

フィールド リファレンス

表 *31 : [Trap Receiver]* ダイアログボックス

要素	説明
[ホストIPアドレス（Host IP Address）]	ルータによって生成されたトラップを受信する SNMP ホストの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
SNMP バージョン（SNMP Version）	使用する SNMP のバージョン（バージョン 1、バージョン 2c、またはバージョン 3）。
コミュニティ ストリング（Community String）	バージョン 1 またはバージョン 2c が選択されている場合にだけ適用されます。 SNMP ホストへのアクセスに必要なパスワード。[Confirm] フィールドに文字列をもう一度入力します。 （注） SNMP ホストへのパスワードとして [Permissions] テーブルで定義されている文字列の 1 つを使用することを推奨します。ただし、別のパスワードも入力できます。文字列の長さの範囲は 1 ～ 128 文字です。入力した内容は [Permissions] テーブルに表示されず、読み取り専用です。
ユーザー名	バージョン 3 が選択されている場合にだけ適用されます。 SNMP ホストへのアクセスに必要なパスワード。[Confirm] フィールドに文字列をもう一度入力します。 （注） SNMP ホストへのパスワードとして [Permissions] テーブルで定義されている文字列の 1 つを使用することを推奨します。ただし、別のパスワードも入力できます。文字列の長さの範囲は 1 ～ 128 文字です。入力した内容は [Permissions] テーブルに表示されず、読み取り専用です。

要素	説明
SNMPv3 セキュリティ	バージョン 3 が選択されている場合にだけ適用されます。 SNMP トラフィックに適用するセキュリティのレベル： • [No MD5, No DES]：パケット認証なし。 • [MD5 (auth)]：MD5 認証あり、暗号化なし。 • [DES (priv)]：MD5 認証あり、DES 暗号化あり。
UDP ポート（UDP Port）	SNMPホストのポート番号。デフォルトは162です。有効な値の範囲は 0 ～ 65535 です。

[SNMP Traps] ダイアログボックス

[SNMP Traps] ダイアログボックスでは、SNMP トラップを生成するルータにおけるイベントを選択します。システム パフォーマンスが低下する可能性を軽減するには、ネットワーク モニタリングに必要なトラップだけを選択します。

ヒント　このダイアログボックスに表示されない SNMP トラップを設定するには、FlexConfig を定義します。詳細については、FlexConfig ポリシーとポリシー オブジェクトについてを参照してください。

ナビゲーション パス

[SNMP] ポリシー ページ （89 ページ）に移動してから、[トラップの設定（Configure Traps）] をクリックします。

関連項目

- [SNMP] ポリシー ページ （89 ページ）
- [Permission] ダイアログボックス （91 ページ）
- [Trap Receiver] ダイアログボックス （92 ページ）
- SNMP トラップの有効化 （88 ページ）
- Cisco IOS ルータの SNMP （86 ページ）

フィールド リファレンス

表 *32 : [SNMP Traps]* ダイアログボックス

要素	説明
[標準SNMPトラップ（Standard SNMP Traps）]	標準 SNMP トラップをイネーブルまたはディセーブルにします。次のオプションがあります。 • [Cold start]：SNMP エージェント（または、その他いずれかのトラップ受信エンティティ）の設定が変化する可能性がある方法でルータが再初期化する場合に、トラップを送信します。 • [Warm start]：SNMP エージェント（または、その他いずれかのトラップ受信エンティティ）の設定が変化しない方法でルータが再初期化する場合に、トラップを送信します。 • [Authentication]：コミュニティ ストリングが無効であるため、SNMP ホストからの SNMP 要求が失敗した場合に、トラップを送信します。
IPsec Traps	個々の IPsec 関連のトラップをイネーブルまたはディセーブルにします。次のオプションがあります。 • [クリプトマップ（Cryptomap）]：デバイスのクリプトマップセットに対してクリプトマップエントリが追加または削除されるときに、トラップを送信します。さらに、クリプト マップ セットがアクティブ インターフェイスに対して適用または適用解除されたときに、トラップを送信します。 • [Too Many SAs]：デバイス上のメモリが不足しているときに Security Association（SA; セキュリティ アソシエーション）の作成が試行された場合に、トラップを送信します。 • [Tunnel]：IPsec フェーズ 2 トンネルがアクティブまたは非アクティブになったときに、トラップを送信します。 詳細については、サイト間 VPN の IPsec プロポーザルについてを参照してください。
[ISAKMPトラップ（ISAKMP Traps）]	個々の Internet Security Association and Key Exchange Protocol（ISAKMP）トラップをイネーブルまたはディセーブルにします。次のオプションがあります。 • [ポリシー（Policy）]：ISAKMP ポリシーが作成または削除されたときにトラップを送信します。 • [Tunnel]：フェーズ 1 IKE トンネルがアクティブまたは非アクティブになったときに、トラップを送信します。 詳細については、IKE についてを参照してください。

要素	説明
Other Traps	その他の SNMP トラップをイネーブルまたはディセーブルにします。次のオプションがあります。 • [Syslog]：syslog メッセージを SNMP ホストに送信します。 • [TTY]：伝送制御プロトコル（TCP）接続が閉じたときに、シスコ固有の通知を送信します。 • [BGP]：ボーダーゲートウェイプロトコル（BGP）の状態変化が発生したときに、通知を送信します。Cisco IOS ルータにおける BGP ルーティングを参照してください。 • [IP Multicast]：（マルチキャスト ルータにのみ適用可能）ルータが、定義された期間中に定義された数のハートビート パケットをハートビート ソースから受け取ることができなかった場合に、トラップを送信します。 [IPマルチキャスト（IP Multicast）] を選択した場合は、デバイスで **ip multicast heartbeat** コマンドを手動で設定して、マルチキャストアドレスとハートビート制限も設定する必要があります。FlexConfig を使用してこれを行います。 • [CPU]：CPU 使用率が上昇して上限しきい値を超えたままになるか、低下して下限しきい値を下回ったままになった場合にトラップを送信します。 CPU を選択した場合は、デバイスで **process cpu threshold type** コマンドを手動で設定して、しきい値を設定する必要もあります。FlexConfig を使用してこれを行います。 • [HSRP]：Hot Standby Routing Protocol（HSRP）通知を送信します。
[Select All] ボタン	ダイアログボックスに表示されるすべての SNMP トラップを有効にします。
[Deselect All] ボタン	ダイアログボックスに表示されるすべての SNMP トラップを無効にします。

Cisco IOS ルータにおける DNS

ドメイン ネーム システム（DNS）は、DNS サーバから DNS プロトコルを使用してホスト名を IP アドレスにマッピングできる分散データベースです。一意の各 IP アドレスにホスト名を関連付けることができます。DNS を使用すると、ホストの 32 ビットの IP アドレスがわからない場合でも、そのホストに接続できます。DNS サーバーは、指定されたホスト名を取得して、適切な IP アドレスに変換します。

リモート DNS サーバによって変換が行われる以外に、ホストから IP アドレスへのスタティック マッピングを含むローカル ホスト テーブルを Cisco IOS ルータに設定できます。connect、telnet、ping などのコマンドを使用すると、ルータはこのホスト テーブルを確認してから DNS サーバに問い合わせます。これにより、変換プロセスが速くなります。

デフォルトでは、DNS 機能はすべての Cisco IOS ルータで有効になっています。

関連項目

- DNS ポリシーの定義　（97 ページ）

DNS ポリシーの定義

Security Manager で DNS ポリシーを定義すると、ルータによってホスト名とアドレス間の変換に使用されるリモート DNS サーバを指定できます。さらに、このデバイスによって排他的に使用されるローカル変換を含む静的ホストテーブルを定義できます。このタイプのキャッシュでアドレスを選択すると、DNS サーバーにクエリを実行する必要がなくなるため、変換プロセスを高速化できます。

関連項目

- Cisco IOS ルータにおける DNS　（96 ページ）

ステップ 1　次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [DNS]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [DNS]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[DNS] ページが表示されます。このページのフィールドの説明については、表 33 : [DNS] ページ　（99 ページ）を参照してください。

ステップ 2　[サーバー（Servers）] フィールドに、ルータのホスト名からアドレスへの変換を実行できる DNS サーバー（最大 6）のアドレスを入力します。アドレスとネットワーク/ホストオブジェクトの組み合わせを使用するか、[選択（Select）] をクリックしてセレクタを表示できます。詳細については、ポリシー定義中の IP アドレスの指定を参照してください。

ヒント　必要なネットワークがセレクタに表示されていない場合は、セレクタで [作成（Create）] ボタンまたは [編集（Edit）] ボタンをクリックして、[Add Network/Host]/[Edit Network/Host] ダイアログボックスを表示します。ここから、ポリシーで使用するネットワーク/ホストオブジェクトを作成できます。

ステップ 3　（任意）[ホスト（Hosts）] フィールドに、ルータのホストテーブルに定義する静的ホストマッピングを入力します。

a) [追加（Add）] をクリックして、 [IP Host] ダイアログボックス （99 ページ）を表示します。
b) 変換するホスト名を入力します。
c) アドレスまたはネットワーク/ホストオブジェクトを最大 3 つまで入力し、[選択（Select）] をクリックしてセレクタを表示します。これらはホスト名の変換先のアドレスです。
d) [OK] をクリックマッピングが [DNS] ページの [Hosts] フィールドに表示されます。
e) 3.a （98 ページ） から 3.d （98 ページ） を繰り返すと、さらに多くのホストをホスト テーブルに追加できます。

（注） ホストマッピングを編集するには、[ホスト（Hosts）] フィールドから定義を選択し、[編集（Edit）] をクリックします。ホストマッピングを削除するには、そのマッピングを選択し、[削除（Delete）] をクリックします。

ステップ 4 （任意）[ドメインルックアップ（Domain Lookup）] チェックボックスをオフにして、ルータの DNS 機能を無効にします。

[DNS] ポリシー ページ

[DNS] ポリシー ページでは、ルータがホスト名を IP アドレスに変換するために使用するローカル IP ホスト テーブルとドメイン ネーム システム（DNS）サーバを定義します。DNS 機能をディセーブルにして、ルータが DNS ルックアップを実行できないようにすることもできます。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]>[デバイス管理（Device Admin）] > [DNS]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [DNS]** を選択します。[DNS] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータにおける DNS （96 ページ）

フィールド リファレンス

表 *33 : [DNS]* ページ

要素	説明
サーバー	DNS ルックアップを実行するためにルータによって使用される DNS サーバーです。1 つ以上のアドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。最大 6 個の DNS サーバーを定義することができます。
ホスト（Hosts）	ルータに設定するローカル ホスト テーブル。ユーザがホスト名を入力すると、ルータはまずこのテーブルを確認してから [Servers] フィールドに定義されている DNS サーバに問い合わせます。 [追加（Add）] をクリックして、[IP Host] ダイアログボックス （99 ページ）を表示します。ここから、ホスト名とそのホスト名に関連付ける IP アドレスを定義できます。 （注） ホストテーブルのエントリを編集するには、エントリを選択して [編集（Edit）] をクリックします。エントリを削除するには、そのエントリを選択し、[削除（Delete）] をクリックします。
ドメイン検索（Domain Lookup）	選択すると、ルータは定義済みの DNS サーバ上で検索を実行します。これがデフォルトです。 選択を解除すると、リモート DNS サーバ上での検索はディセーブルになります。

[IP Host] ダイアログボックス

[IP ホスト（IP Host）] ダイアログボックスを使用して、ルータのホストテーブルを設定します。これは、ルータがホスト名を IP アドレスに変換するために使用するスタティックなローカルマッピングのテーブルです。ルータは、ホストテーブルで必要なエントリを見つけられない場合、[DNS] ページで定義されている DNS サーバーにクエリを実行します。

ナビゲーション パス

[DNS] ポリシー ページ （98 ページ）に移動し、[ホスト（Hosts）] の下にある [追加（Add）] をクリックします。

関連項目

- Cisco IOS ルータにおける DNS （96 ページ）

フィールド リファレンス

表 *34 : [IP Host]* ダイアログボックス

要素	説明
ホスト名	ルータのローカルホストテーブルに含めるホスト名。
アドレス	ホスト名に関連付けるアドレス。1つ以上のアドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択（Select）]をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。ホスト名ごとに最大 3 つのアドレスを定義できます。

Cisco IOS ルータにおけるホスト名とドメイン名

ホスト名ポリシーでは、選択したルータのホスト名とドメイン名を設定します。このポリシーを展開すると、ホスト名とドメイン名に対する変更が [Device Properties] ページに反映されます（デバイス プロパティの表示または変更を参照）。

関連項目

- ホスト名ポリシーの定義　（100 ページ）

ホスト名ポリシーの定義

ホスト名ポリシーを定義すると、Security Manager は展開後に [Device Properties] ダイアログボックスのホスト名とドメイン名のフィールドを更新します。デバイスプロパティの表示または変更 を参照してください。

関連項目

- Cisco IOS ルータにおけるホスト名とドメイン名　（100 ページ）

ステップ 1　次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ホスト名（Hostname）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [ホスト名（Hostname）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Hostname] ページが表示されます。このページのフィールドの説明については、表 35 : [Hostname] ページ（101 ページ）を参照してください。

ステップ 2 ルータのホスト名を入力します。名前は文字で始まり、文字または数字で終了し、文字、数字、およびハイフンだけから構成される必要があります。最大で 63 文字です。

ステップ 3 ルータのドメイン名を入力します。ルータは、RSA キーを生成するときにこのドメイン名を使用します。また、完全修飾ドメイン名を入力しなかった場合に、ポリシーでこのドメイン名を使用します。

[Hostname] ポリシー ページ

[Hostname] ページでは、ルータに割り当てるホスト名とドメイン名を定義します。詳細については、ホスト名ポリシーの定義 （100 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]>[デバイス管理（Device Admin）] > [ホスト名（Hostname）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータプラットフォーム（Router Platform）]>[デバイス管理（Device Admin）]>[ホスト名（Hostname）]** を選択します。[ホスト名（Hostname）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータにおけるホスト名とドメイン名 （100 ページ）

フィールド リファレンス

表 35 : [Hostname] ページ

要素	説明
ホスト名	ルータのホスト名。 名前は文字で始まり、文字または数字で終了し、文字、数字、およびハイフンだけから構成される必要があります。最大で 63 文字です。
ドメイン名	ルータのデフォルトのドメイン名。最大で 63 文字です。 ルータは、RSA キーを生成するときにこのドメイン名を使用します。また、Fully-Qualified Domain Name（FQDN; 完全修飾ドメイン名）を入力しなかった場合に、ポリシーでこのドメイン名を使用します。

Cisco IOS ルータにおけるメモリ設定

メモリ ポリシーでは、ルータのメモリに関する設定を定義します。このポリシーは、使用可能なメモリが定義済みのしきい値を下回った場合に通知メッセージを生成する機能など、メモリ使用量をモニタするための手段を提供します。

（注） メモリ ポリシーは、Cisco IOS ソフトウェア Release 12.3(14)T 以降を実行しているルータでサポートされます。

関連項目

- ルータのメモリ設定の定義 （102 ページ）

ルータのメモリ設定の定義

Security Manager を使用して、次のデフォルトのメモリ設定を変更できます。

- ルータがメモリ使用量のログを保持する時間数
- Memory Allocation Lite 機能をイネーブルにするかどうか
- 重要なシステム ログ メッセージ用に予約するメモリ容量

さらに、次の項目を定義できます。

- プロセッサおよび I/O メモリの下限しきい値。使用可能なメモリがこれらのしきい値を下回ると、ログ メッセージが送信されます。
- 実行する健全性チェックのタイプ。

関連項目

- Cisco IOS ルータにおけるメモリ設定 （102 ページ）
- Cisco IOS ルータにおけるロギング

ステップ 1 次のいずれかを実行します。

- （デバイス ビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [メモリ（Memory）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）]>[メモリ（Memory）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Memory] ページが表示されます。

ステップ 2 （任意）必要に応じて、ルータのメモリ設定を定義します。使用可能なフィールドの説明については、表 36 : [Memory] ページ （104 ページ）を参照してください。

[Memory] ポリシー ページ

[Memory] ページでは、ルータのメモリに関する次の設定を定義します。

- メモリ ログを保持する時間
- 使用可能なプロセッサおよび I/O メモリのしきい値
- 重要なログ メッセージ用に予約するメモリ容量
- バッファおよびキューで健全性チェックを実行するかどうか
- 「memory-allocation lite」機能をイネーブルにするかどうか

詳細については、ルータのメモリ設定の定義 （102 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]>[デバイス管理（Device Admin）] > [メモリ（Memory）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [メモリ（Memory）]** を選択します。[メモリ（Memory）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存ポリシーを選択します。

関連項目

- Cisco IOS ルータにおけるメモリ設定 （102 ページ）
- [CPU] ポリシー ページ （34 ページ）
- Syslog ロギングの設定ポリシーのページ
- Syslog サーバ ポリシーのページ

フィールド リファレンス

表 *36 : [Memory]* ページ

要素	説明
Maintain Memory Log	ルータがデバイス上のメモリ使用量の履歴が格納されたログを保持する時間数。有効値の範囲は 12 ～ 72 時間です。デフォルトは 24（1 日）です。 （注） メモリ ログはデフォルトでイネーブルになっており、ディセーブルにすることはできません。
Processor Threshold	プロセッサのメモリしきい値（KB 単位）。使用可能なプロセッサ メモリがこのしきい値を下回った場合は、通知メッセージがトリガーされます。有効値の範囲は 1 ～ 4294967295 KB（4096 GB）です。 （注） 使用可能な空きメモリがしきい値を 5% 上回ると、別の通知メッセージが生成されます。
I/O Threshold	I/O メモリのしきい値（KB 単位）。使用可能なプロセッサ メモリがこのしきい値を下回った場合は、通知メッセージがトリガーされます。有効値の範囲は 1 ～ 4294967295 KB（4096 GB）です。 （注） 使用可能な空きメモリがしきい値を 5% 上回ると、別の通知メッセージが生成されます。
Memory Allocation Lite	選択すると、ルータ上の「memory-allocation lite」（malloc_lite）機能がイネーブルになります。この機能により、128 バイト以上のメモリが必要ではない状況で、過剰なメモリ割り当てによるオーバーヘッドを防ぐことができます。これがデフォルトです。 選択を解除すると、「memory-allocation lite」機能がディセーブルになります。 （注） この機能は、プロセッサ メモリ プールだけでサポートされます。
Memory Region For Critical Notifications	重要なシステムログメッセージ用に予約するメモリ容量（キロバイト）有効値の範囲は 1 ～ 4294967295 KB（4096 GB）ですが、メモリ合計の 25% を超える値を指定することはできません。 このオプションは、システムリソースが過負荷になっている場合でも、ルータが重要なシステムログメッセージを発行できるように、ルータにメモリ領域を予約します。

要素	説明
Perform Sanity Checks	実行する健全性チェックのタイプ： • [Buffer]：すべてのバッファに対して健全性チェックを実行します。健全性チェックは、パケットバッファが割り当てられるとき、およびパケットバッファがバッファ プールに戻されるときに実行されます。 • [Queue]：すべてのキューに対して健全性チェックを実行します。 • [All]：すべてのバッファとキューに対して健全性チェックを実行します。 （注） これらのオプションのいずれかをイネーブルにすると、ルータパフォーマンスが多少低下する可能性があります。

Cisco IOS ルータにおけるセキュア デバイス プロビジョニング

Secure Device Provisioning（SDP; セキュア デバイス プロビジョニング）は、VPN およびネットワーク セキュリティの展開を効率化するための統合ソリューションを提供します。SDP（以前の Easy Secure Device Deployment（EzSDD））を使用すると、リモートサイト ユーザは使いやすい Web インターフェイスで VPN デバイスを安全にブートストラップできます。これにより、展開の負担やコストが軽減され、ネットワーク開発サイクルが短縮されます。たとえば、在宅勤務者や小規模のブランチ オフィス ユーザは、新しいデバイスを出荷パッケージから取り出して接続し、簡単な Web 管理インターフェイスを開いて VPN 接続を確立できます。これらのすべての作業をほんの数分間で行うことができます。

SDP の詳細については、Cisco IOS セキュリティ コンフィギュレーション ガイド、リリース 12.4T [英語] の「Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI」を参照してください。

（注） SDP を使用するには、Cisco IOS ソフトウェア Release 12.3(8)T 以降が必要です。これよりも前のバージョンが実行されているルータにこのポリシーを展開しようとすると、展開が失敗する可能性があります。また、NO-VPN ルータ モデル（3845 NOVPN など、VPN 設定ができないモデル）ではポリシーを設定できません。

Trusted Transitive Introduction（TTI）は、SDP を実装するための主なメカニズムとして機能するプロトコルです。図 3 : Secure Device Provisioning（Secure Device Provisioning） （106 ページ）に示すように、TTI は次の 3 つのエンティティで構成されています。

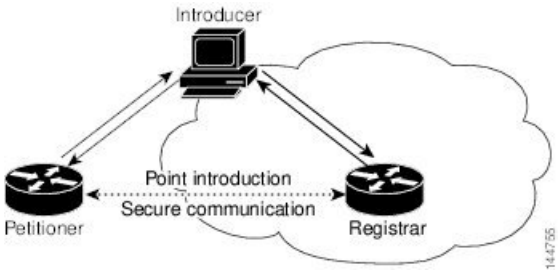
- イントロデューサ：ペティショナをレジストラに紹介する、相互に信頼できるデバイス。イントロデューサは、SDP を使用して自分に関連付けられた VPN デバイスを PKI ネットワークに配置するエンド ユーザ、または SDP を使用して多くの VPN デバイスを PKI ネッ

トワークに配置する管理者/管理システムのいずれかです。後者のイントロデューサは、管理イントロデューサと呼ばれます。詳細については、管理イントロデューサの AAA サーバ グループの設定 （109 ページ）を参照してください。

- ペティショナ：セキュア ドメインに参加しているリモートサイト デバイス。ペティショナは、イントロデューサに Web ページを提供し、イントロデューサの Web ブラウザからブートストラップ設定を受信します。ペティショナコンポーネントは、すべての Cisco IOS デバイスでデフォルトで有効になっています。
- レジストラ：認証、許可、アカウンティング（AAA）サーバと直接通信してユーザ クレデンシャルの確認、登録の許可または拒否、およびユーザ固有の設定情報の取得を行うことによって、ペティショナを認可するサーバ。

ルータをレジストラとして設定するには、Security Manager で SDP ポリシーを使用します。

図 *3 : Secure Device Provisioning*（*Secure Device Provisioning*）



Secure Device Provisioning の詳細については、次を参照してください。

- ブートストラップ設定の内容 （106 ページ）
- セキュア デバイス プロビジョニングのワークフロー （107 ページ）
- セキュア デバイス プロビジョニング ポリシーの定義 （107 ページ）

ブートストラップ設定の内容

SDP によって提供されるブートストラップ設定では、一般に次のことを行います。

- ペティショナのホスト名の設定
- ペティショナのシステムクロックとレジストラとの同期
- ペティショナのトラストポイントの設定
- ペティショナの認証および許可メカニズムの設定
- CA 証明書のプッシュ
- PKI サーバへのペティショナの登録
- 管理トンネルの確立に必要な設定など、他の VPN 設定の定義

- Cisco Networking Services（CNS）の設定
- ペティショナの DHCP プールの設定

関連項目

- セキュア デバイス プロビジョニングのワークフロー （107 ページ）
- Cisco IOS ルータにおけるセキュア デバイス プロビジョニング （105 ページ）

セキュア デバイス プロビジョニングのワークフロー

ここでは、SDP を使用してリモートサイト デバイスをセキュア ネットワークに登録するために必要な手順を示します。

1. ルータを開梱し、電源、LAN、および WAN ケーブルを接続します。
2. ルータ上の DHCP サーバから IP アドレスが割り当てられているコンピュータ（イントロデューサ）に電源を投入し、Web ブラウザを開いてルータ上のペティショナの URL（http://device/ezsdd/welcome）に移動します。ルータから登録ページ（ローカル ログイン ダイアログボックスとも呼ばれる）が返されます。
3. ユーザー名とパスワードを入力し、[OK] をクリックします。初期ページでレジストラの URL を入力します。次が実行されます。
   1. ブラウザは、中央サイトのレジストラとのセッションを開きます。このセッションは HTTPS で保護されます。レジストラは、AAA サーバを使用してユーザ名を検証し、適切なブートストラップ設定をブラウザに返します。
   2. ブラウザは、ブートストラップ設定をリモートサイトのルータに提供し、PKI トラストポイントの登録と IPsec VPN 接続の設定およびシステム属性やその他の情報のプロビジョニングを行います。
   3. ブートストラップ設定の完了が通知されます。

関連項目

- ブートストラップ設定の内容 （106 ページ）
- Cisco IOS ルータにおけるセキュア デバイス プロビジョニング （105 ページ）

セキュア デバイス プロビジョニング ポリシーの定義

ペティショナ コンポーネントは、すべての Cisco IOS ルータで自動的にイネーブルになります。Security Manager の SDP ポリシーにより、レジストラが有効になります。SDP ポリシーを定義するには、以下を定義する必要があります。

- レジストラがイントロデューサの認証と認可に使用する AAA サーバが含まれている AAA サーバ グループ

- ブートストラップ プロセス中にペティショナの登録先となる CA サーバ
- 認可の実行後に表示される初期ページの場所
- ペティショナに提供されるブートストラップ設定の場所

関連項目

- セキュア デバイス プロビジョニングのワークフロー （107 ページ）
- 管理イントロデューサの AAA サーバ グループの設定 （109 ページ）
- Cisco IOS ルータにおけるセキュア デバイス プロビジョニング （105 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [セキュアデバイスプロビジョニング（Secure Device Provisioning）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [セキュアデバイスプロビジョニング（Secure Device Provisioning）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[セキュアデバイスプロビジョニング（Secure Device Provisioning）] ページが表示されます。このページのフィールドの説明については、表 37 : [Secure Device Provisioning] ページ （111 ページ）を参照してください。

ステップ 2 [Introducer Authentication] で、関連する AAA サーバーが含まれている AAA サーバーグループの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。

選択した AAA サーバによって、イントロデューサが指定したユーザ名とパスワードが認可されたユーザを表すかどうかが判断されます。AAA サーバは TACACS+ や RADIUS を使用するか、またはローカルである必要があります。

（注） 選択したグループの各 AAA サーバは、ルータ上に存在するインターフェイスと通信するように設定する必要があります。そうしないと、検証が失敗します。管理イントロデューサの認証と認可に別の AAA サーバ グループを設定する場合は、 管理イントロデューサの AAA サーバ グループの設定 （109 ページ）を参照してください。

ステップ 3 [Petitioner Authentication] で、次のいずれかの手順を実行して、ペティショナの ID を認証する CA サーバを定義します。

- [ローカルCAサーバー（Local CA Server）] を選択し、表示されるフィールドにローカル CA の名前を入力します。レジストラ上で CA サーバをすでにローカルに設定している場合は、トラストポイントが自動的に生成されます。

（注） ルータを CA サーバーとして設定していない場合は、CLI または FlexConfig を使用してコマンド **Crypto pki server [name]** を入力します。このコマンドは、ローカル CA サーバで設定された SDP ポリシーを展開する場合は必須です。

- [リモートCAサーバー（Remote CA Server）] を選択し、PKI 登録オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。

PKI 登録オブジェクトでは、SDP ポリシーで使用される外部 CA サーバを定義します。

ステップ 4 レジストラへのログイン後に表示される初期ページの場所を選択します。初期ページには、認可が正常に完了したかどうかが表示され、ブートストラップ設定の取得プロセスを完了するためのボタンが表示されます。

デフォルトの初期ページを選択しない場合は、他の場所に準備した別の初期ページにアクセスするために必要な URL を入力する必要があります。

ステップ 5 ペティショナに提供するブートストラップ設定の場所を選択して、その最初の設定を実装します。

- ブートストラップ設定の場所が Security Manager 以外の URL である場合は、その URL を入力します。必要に応じて、その URL にアクセスするためのユーザ名とパスワードも入力します。
- 設定ファイルの場所が Security Manager の URL である場合：
  - FlexConfig の名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。FlexConfig には、適切なブートストラップ設定の取得に必要なデバイス コマンドが含まれています。詳細については、[Add FlexConfig]/[Edit FlexConfig] ダイアログボックスを参照してください。
  - FlexConfig が、イントロデューサによって送信されたユーザ名に基づいて、ペティショナのデバイス名を設定するために必要なデバイス名の式を入力します（通常、2 つの名前の関連付けは変更されません）。デフォルトの式は$nで、イントロデューサ名を使用してデバイス名を決定します。

デバイス名によって、ペティショナが受信するブートストラップ設定が決まります。生成される URL には、選択した FlexConfig の名前および定義したパラメータと式が含まれます。

- FlexConfig が含まれている Security Manager サーバにアクセスするためのユーザ名とパスワードを入力します。パスワードには、英数字を使用できますが、単一の数字だけでは構成できません。

管理イントロデューサの AAA サーバ グループの設定

管理イントロデューサは、多くのデバイスを PKI ネットワークに導入する管理者または管理システムです。次の FlexConfig をルータの設定に追加することによって、管理イントロデューサを認証および認可するための AAA サーバ グループを設定できます。

```
aaa new-model
radius-server host 1.2.3.4 auth-port 1645 acct-port 1646 key key
aaa group server radius default-radius-group2
server 1.2.3.4 auth-port 1645 acct-port 1646
exit
aaa authentication login CSM_SDP2 group default-radius-group2
crypto provisioning registrar
```

```
administrator authentication list CSM_SDP2
administrator authorization list CSM_SDP2
exit
```

この FlexConfig は、2 つの機能を提供します。使用する AAA サーバ グループを設定し、このサーバ グループを SDP 暗号に関連付けます。

管理イントロデューサの詳細については、次の URL にある Cisco.com の『Administrative Secure Device Provisioning Introducer』を参照してください。
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtadintr.html

関連項目

- Cisco IOS ルータにおけるセキュア デバイス プロビジョニング （105 ページ）
- セキュア デバイス プロビジョニング ポリシーの定義 （107 ページ）
- FlexConfig ポリシーとポリシー オブジェクトについて

[Secure Device Provisioning] ポリシー ページ

Secure Device Provisioning（SDP）のポリシー（以前の Easy Secure Device Deployment（EzSDD））を使用すると、Cisco IOS ルータをレジストラとして設定できます。これは、ペティショナのブートストラップ設定を取得する SDP コンポーネントです。ペティショナは、ネットワークセキュリティインフラストラクチャに登録されるリモートサイトデバイスです。これらのデバイスは、初回の設定のためにブートストラップ設定を使用します。レジストラは、ペティショナをレジストラに紹介するユーザであるイントロデューサの ID の検証も行います。

詳細については、セキュア デバイス プロビジョニング ポリシーの定義 （107 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]>[デバイス管理（Device Admin）]>[セキュアデバイスプロビジョニング（Secure Device Provisioning）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）]>[デバイス管理（Device Admin）]>[セキュアデバイスプロビジョニング（Secure Device Provisioning）]** を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。

関連項目

- Cisco IOS ルータにおけるセキュア デバイス プロビジョニング （105 ページ）
- セキュア デバイス プロビジョニングのワークフロー （107 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて

- FlexConfig ポリシーとポリシー オブジェクトについて

フィールド リファレンス

表 37 : [Secure Device Provisioning] ページ

要素	説明
Introducer Authentication (AAA)	イントロデューサによって指定されたユーザ名とパスワードを認証する AAA サーバ グループ。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。 （注） 管理イントロデューサの認証に別の AAA サーバ グループを設定する場合は、管理イントロデューサの AAA サーバ グループの設定 （109 ページ）を参照してください。
Petitioner Authentication	ペティショナの ID を認証する CA サーバ。 • ローカル CA サーバー：ルータ自体が CA サーバーとして機能するようにすでに設定されている場合は、このオプションを選択します。表示されるフィールドにローカル CA の名前を入力します。 （注） ルータを CA サーバーとして設定していない場合は、CLI または FlexConfig を使用してコマンド **Crypto pki server [name]** を入力します。このコマンドは、ローカル CA サーバで設定された SDP ポリシーを展開する場合は必須です。 • [Remote CA Server]：外部 CA サーバを使用する場合は、このオプションを選択します。PKI 登録オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。PKI 登録オブジェクトの詳細については、[PKI Enrollment] ダイアログボックスを参照してください。
Introduction Page	認可の実行後にイントロデューサに表示する初期ページの場所： • [デフォルトの初期ページを使用（Use default introduction page）]：Security Manager で提供されるデフォルトのページを使用します。 • [Specify introduction page URL]：[URL] フィールドに指定された初期ページを使用します。サポートされるプロトコルには、FTP、HTTP、HTTPS、null、NVRAM、RCP、SCP、system、TFTP、Webflash、および XMODEM があります。

要素	説明
Bootstrap Configuration	初回の設定用にペティショナに提供するブートストラップ設定の場所 • [Non-Security Manager URL]：ブートストラップ設定が Security Manager の外部にある場合に使用します。その場所を [URL] フィールドに入力します。 必要に応じて、ブートストラップ設定を含むサーバにアクセスするためのユーザ名とパスワードを入力します。 • [Security Manager URL]：Security Manager によってブートストラップ設定が提供される場合に使用します。次のフィールドに情報を入力します。 • [FlexConfig]：ブートストラップ設定の作成に必要な基本 CLI 構造が含まれている FlexConfig。FlexConfig オブジェクトの名前を入力するか、[選択（Select）] をクリックしてセレクタを表示します。 FlexConfig の選択後、FlexConfig が格納されている Security Manager サーバにアクセスするためのユーザ名とパスワードを入力する必要があります。 • [Device name formula]：Security Manager が、イントロデューサが指定したユーザ名に基づいて、ペティショナのデバイス名を決定するために必要な式。 通常、ユーザ名とデバイス名の間には一定の関係があるため、このような式を設定できます。デフォルトの式は $n で、イントロデューサ名を使用してデバイス名を決定します。ペティショナが受信する設定ファイルを特定するには、デバイス名が必要です。 必要に応じて、ブートストラップ設定を含むサーバにアクセスするためのユーザ名とパスワードを入力します。パスワードには、英数字を使用できますが、単一の数字だけでは構成できません。

Cisco IOS ルータにおける DHCP

Security Manager では、Easy VPN や 802.1x などの特定のセキュリティ機能を使用するときに、Dynamic Host Configuration Protocol（DHCP）のクライアント/サーバ設定が必要となります。DHCP は、中央のサーバーからホスト IP アドレスを動的に割り当てるために LAN 環境で広く使用されており、それによって IP アドレス管理のオーバーヘッドが大幅に軽減されます。

DHCP サーバは、ルータ内の指定したアドレス プールから DHCP クライアントに IP アドレスを割り当てて管理します。DHCP サーバーが自身のデータベースで DHCP 要求を実行できない場合、この要求をネットワーク管理者が定義した 1 つまたは複数のセカンダリ DHCP サーバーに転送できます。

Security Manager を使用すると、デバイスの内部インターフェイスに接続されているクライアント（ホスト）の DHCP サーバーとして Cisco IOS デバイスを設定できます。DHCP サーバを

設定する場合は、IP プール（DHCP サーバ用に予約された IP アドレスの範囲）を使用します。選択した IP プールによって、サーバが使用できる IP アドレスの範囲が決まります。これらのアドレスは、リースと呼ばれる定義済みの期間、クライアントデバイスに提供されます。このリースの期限が切れると、アドレスがアドレスプールに返され、DHCP サーバはそのアドレスを別のデバイスに割り当てることができるようになります。

DHCP の詳細については、次を参照してください。

- DHCP データベース エージェントについて （113 ページ）
- DHCP リレーエージェントについて （114 ページ）
- DHCP Option 82 について （114 ページ）
- Secured ARP について （115 ページ）

DHCP ポリシーの設定については、次を参照してください。

- DHCP ポリシーの定義 （116 ページ）
- DHCP アドレス プールの定義 （117 ページ）

DHCP データベース エージェントについて

DHCP データベース エージェントは、DHCP バインディング データベースが格納されている外部ホスト（FTP、TFTP、RCP サーバなど）です。各 DHCP ポリシーに 1 つ以上の DHCP データベースエージェントを含めたり、エージェントのデータベース更新の間隔を設定したりできます。

（注） 外部 DHCP データベース エージェントを設定する場合、IP アドレス プールの定義は必須ではありませんが、必要に応じて定義することもできます。IP アドレス プールの詳細については、 DHCP アドレス プールの定義 （117 ページ）を参照してください。

関連項目

- DHCP リレーエージェントについて （114 ページ）
- DHCP Option 82 について （114 ページ）
- Secured ARP について （115 ページ）
- DHCP ポリシーの定義 （116 ページ）
- Cisco IOS ルータにおける DHCP （112 ページ）

DHCP リレーエージェントについて

DHCP リレーエージェントは、クライアントとサーバが同じ物理サブネット上に存在しない場合に、それらのクライアントとサーバの間で DHCP パケットを転送するホストです。リレーエージェントは DHCP メッセージを受信し、別のインターフェイス上で送信する新しい DHCP メッセージを生成します。転送メッセージにすでにリレー情報が含まれている場合の DHCP リレーエージェントによる処理方法を決定する、情報再転送ポリシーを設定できます。

Security Manager には次の DHCP リレー オプションがあります。

- [Drop]：Option 82 情報も存在する場合、リレーエージェントは、既存のリレー情報を含むメッセージを廃棄します。
- [Keep]：リレー エージェントは、既存のリレー情報を保持します。
- [Replace]：リレー エージェントは、既存の情報を独自のリレー情報で上書きします。

たとえば、転送されたメッセージを DHCP リレー エージェントで新しいリレー メッセージに置き換えることができます。さらに、転送された BOOTREPLY メッセージ内に含まれているリレー情報の有効性をリレー エージェントで確認するかどうかを選択できます。

関連項目

- DHCP データベース エージェントについて （113 ページ）
- DHCP Option 82 について （114 ページ）
- Secured ARP について （115 ページ）
- DHCP ポリシーの定義 （116 ページ）
- Cisco IOS ルータにおける DHCP （112 ページ）

DHCP Option 82 について

DHCP Option 82 を使用すると、DHCP リレー エージェントは、DHCP クライアントからの要求を DHCP サーバに転送するときに、エージェント自体に関する情報と、接続されているクライアントに関する情報を含めることができます。DHCP サーバは、この情報を使用して IP アドレスを割り当てたり、アクセス コントロールを実行したり、各サブスクライバの Quality of Service（QoS）やセキュリティ ポリシーを設定したりできます。DHCP Option 82 機能がイネーブルになっている場合、サブスクライバは、MAC アドレスではなく、ネットワークへの接続に使用しているスイッチ ポートによって識別されます。サブスクライバ LAN 上の複数のホストをアクセス スイッチの同じポートに接続できます。これらのホストは一意に識別されます。また、Option 82 を使用すると、ユーザの IP アドレスを使用してユーザが接続されているポートを特定できるため、アクセススイッチ上のセキュリティを強化できます。

関連項目

- DHCP データベース エージェントについて （113 ページ）

• DHCP リレーエージェントについて （114 ページ）
• Secured ARP について （115 ページ）
• DHCP ポリシーの定義 （116 ページ）
• Cisco IOS ルータにおける DHCP （112 ページ）

Secured ARP について

DHCP セキュア IP アドレス割り当て機能（DHCP 認可 ARP とも呼ばれる）を使用すると、DHCP データベース内の DHCP リースに対するアドレス解決プロトコル（ARP）テーブルのエントリを保護できます。この機能では、クライアントの MAC アドレスを DHCP バインディングに保護して同期させることで、無許可のクライアントまたはハッカーが DHCP サーバーをスプーフィングして、許可されたクライアントの DHCP リースを横取りすることを防ぎます。

この機能をイネーブルにすると、DHCP サーバは IP アドレスを DHCP クライアントに割り当ててから、クライアントの割り当て済み IP アドレスと MAC アドレスを持つ ARP テーブルに、セキュアな ARP エントリを追加します。これらの ARP エントリは、他の動的な ARP パケットによって更新することはできず、リースがアクティブであるかぎり ARP テーブルに存在します。

セキュアな ARP エントリは、DHCP クライアントからの明示的な終了メッセージによって削除されるか、またはバインディングの期限が切れたときに DHCP サーバによって削除されます。クライアントのログアウトを検出するために、Secured ARP は、認可ユーザだけが応答できる ARP メッセージを定期的に送信します。未認可応答は DHCP サーバでブロックされるため、セキュリティが強化されます。

（注） Secured ARP により、インターフェイスにおける動的な ARP 学習がディセーブルになります。

関連項目

• DHCP データベース エージェントについて （113 ページ）
• DHCP リレーエージェントについて （114 ページ）
• DHCP Option 82 について （114 ページ）
• DHCP ポリシーの定義 （116 ページ）
• Cisco IOS ルータにおける DHCP （112 ページ）

DHCP ポリシーの定義

DHCP ポリシーを設定する場合、サーバが DHCP クライアントにアドレスを提供するために使用する IP アドレス プールを定義する必要があります。さらに、任意で次を定義できます。

- 外部の DHCP データベース エージェント
- DHCP から除外する IP 範囲
- DHCP リレーパラメータ

（注） Cisco IOS ルータで DHCP を設定する場合は、ルータに Bootstrap Protocol（BootP; ブートストラップ プロトコル）トラフィックを拒否するアクセス ルールが含まれていないことを確認してください。このようなルールが設定されていると、DHCP トラフィックはブロックされます。

関連項目

- Cisco IOS ルータにおける DHCP （112 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DHCP] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DHCP] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[DHCP] ポリシー ページが表示されます。このページのフィールドの説明については、表 38 : [DHCP] ポリシー ページ （119 ページ）を参照してください。

ステップ 2 （任意）[データベース（Databases）] で、[追加（Add）] ボタンをクリックして [DHCP Database] ダイアログボックス （121 ページ）を表示します。ここから、外部の DHCP データベース エージェントを定義できます。詳細については、DHCP データベース エージェントについて （113 ページ）を参照してください。

ステップ 3 （任意）[Excluded IPs] で、DHCP クライアントで使用できないようにする DHCP アドレス プール内の IP アドレスまたはアドレス範囲を入力します。アドレスとネットワーク/ホストオブジェクトの組み合わせを使用するか、[選択（Select）] をクリックしてセレクタを表示できます。詳細については、ポリシー定義中の IP アドレスの指定を参照してください。

ヒント 必要なネットワークがセレクタに表示されていない場合は、[作成（Create）] ボタンをクリックして、[Add Network/Host]/[Edit Network/Host] ダイアログボックスを表示します。ここから、ネットワーク/ホスト オブジェクトを作成できます。

ステップ 4 [IP プール（IP Pools）] で、[追加（Add）] ボタンをクリックして [IP Pool] ダイアログボックス （122 ページ）を表示します。ここから、DHCP サーバによって使用されるアドレス プールを定義できます。詳細については、 DHCP アドレス プールの定義 （117 ページ）を参照してください。

ステップ 5 （任意）リレーエージェントを使用して、DHCP サーバーとは異なるサブネットにある DHCP クライアントからの要求を管理する場合は、次の DHCP リレーオプションを定義します。

a) リレーエージェント情報再転送ポリシー（[Drop]、[Keep]、または [Replace]）を選択します。DHCP リレー エージェントは、すでにリレー情報が含まれているメッセージを受信すると、このポリシーを実装します。

b) リレーエージェントが DHCP サーバーに転送する要求に Option 82 データを挿入できるようにするには、[オプション（Option）] チェックボックスをオンにします。

c) [チェック（Check）] チェックボックスをオンにして、DHCP サーバーによって送信された DHCP Option 82 リレーパケットを検証します。

このオプションをイネーブルにすると、無効なメッセージはドロップされます。有効なメッセージは、DHCP クライアントに転送される前に option-82 フィールドが削除されます。このオプションをディセーブルにすると、先に有効性が確認されることなく option-82 フィールドはパケットから削除されます。

詳細については、 DHCP リレーエージェントについて （114 ページ）を参照してください。

DHCP アドレス プールの定義

外部データベース エージェントを含まない DHCP ポリシーを設定する場合は、少なくとも 1 つの IP アドレス プールを定義する必要があります。DHCP サーバは、このプールに含まれているアドレスを DHCP クライアントに動的に割り当てることができます。さらに、次の IP プール固有のオプションを定義できます。

- DHCP クライアントで使用するデフォルト ルータ、DNS サーバ、WINS サーバ、およびドメイン
- Secured ARP 機能を使用するかどうか
- IP プール オプションに関する情報を中央の DHCP サーバからインポートするかどうか
- リースの期間
- IP テレフォニー デバイスがこのプールのアドレスを使用するために必要な TFTP サーバの場所

関連項目

- DHCP ポリシーの定義 （116 ページ）
- Cisco IOS ルータにおける DHCP （112 ページ）

ステップ 1 [DHCP] ページで、[IPプール（IP Pools）] の下にある [作成（Create）] ボタンをクリックします。[IP Pool] ダイアログボックスが表示されます。

ステップ 2 アドレス プールを定義します。使用可能なフィールドの説明については、表 40 : [IP Pool] ダイアログボックス （123 ページ）を参照してください。

ステップ 3 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。IP プールが [DHCP] ページの [IP Pools] の下にあるテーブルに表示されます。

ステップ 4 必要に応じてステップ 1 （118 ページ）～ステップ 3 （118 ページ）を繰り返して、他のアドレス プールを定義します。

（注） IP プールを編集するには、テーブルからプールを選択し、[編集（Edit）] ボタンをクリックします。IP プールを削除するには、テーブルからプールを選択し、[削除（Delete）] ボタンをクリックします。アドレスが DHCP クライアントに割り当てられているプールを削除することはできません。

[DHCP] ポリシー ページ

[DHCP] ポリシー ページでは、選択したルータ上の DHCP サーバ ポリシーを定義します。たとえば、要求側クライアントへのアドレスの割り当て時に DHCP サーバで使用するアドレス プールを指定します。

詳細については、DHCP ポリシーの定義 （116 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DHCP] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DHCP] を選択します。[DHCP] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータにおける DHCP （112 ページ）
- テーブル カラムおよびカラム見出しの機能
- テーブルのフィルタリング

フィールド リファレンス

表 *38 : [DHCP]* ポリシー ページ

要素	説明
[データベーステーブル（Database Table）]	
Database URL	外部の DHCP データベース エージェントの URL。
タイムアウト（Timeout）	データベース転送を中断するまでに外部の DHCP データベースエージェントからの応答を待機する時間（秒単位）。
Write Delay	外部の DHCP データベース エージェントに送信される DHCP 割り当て更新の間隔（秒数）。
[追加（Add）] ボタン	[DHCP Database] ダイアログボックス （121 ページ）が開きます。ここから、DHCP データベース エージェントを定義できます。
[編集（Edit）] ボタン	[DHCP Database] ダイアログボックス （121 ページ）が開きます。ここから、選択した DHCP データベース エージェントを編集できます。
[削除（Delete）] ボタン	選択した DHCP データベース エージェントを削除します。
Excluded IPs	
[除外 IP または IP 範囲（Excluded IPs or IP Ranges）]	DHCP から除外する IP アドレスまたはアドレス範囲。これらのアドレスは、DHCP サーバによって、アドレスを要求している DHCP クライアントに割り当てられません。 1 つ以上のネットワークアドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 詳細については、ポリシー定義中の IP アドレスの指定を参照してください。
[IP Pools] テーブル	
名前	IP プールの名前。
ネットワーク（Network）	IP プールの IP アドレスおよびサブネットマスク。
デフォルト ルータ	DHCP クライアントで使用するデフォルト ルータの IP アドレス。
DNS サーバー	DHCP クライアントで使用する DNS サーバの IP アドレス。

要素	説明
[NetBIOS（WINS）サーバー（NetBIOS (WINS) Server）]	Microsoft DHCP クライアントで使用する Windows インターネット ネーム サービス（WINS）サーバーの IP アドレス。
ドメイン名	DHCP クライアントのドメイン名。
Import All	リモート DHCP サーバが特定の DHCP オプションを中央の DHCP サーバからインポートするかどうかを示します。
Secured ARP	Secured ARP がこの IP プールでイネーブルになっているかどうかを示します。この機能を使用すると、未認可ユーザによる IP スプーフィングを防止できます。
Lease	この IP プールから DHCP サーバーによって割り当てられた各 IP アドレスのリース期間。
オプション 150	DHCP option 150 を使用して定義された、IP 電話での設定に必要な TFTP サーバの IP アドレス。
Option 66	DHCP option 66 を使用して定義された、IP 電話での設定に必要な TFTP サーバの IP アドレス。
[追加（Add）] ボタン	[IP Pool] ダイアログボックス （122 ページ）が開きます。ここから、DHCP IP アドレス プールを定義できます。
[編集（Edit）] ボタン	[IP Pool] ダイアログボックス （122 ページ）が開きます。ここから、選択した IP プールを編集できます。
[削除（Delete）] ボタン	選択した IP プールを削除します。
Relay parameters	
ポリシー	DHCP リレーエージェントがすでにリレー情報が含まれているメッセージを受信するときに実装するポリシー。 • [Drop]：Option 82 情報も存在する場合、リレー エージェントは、既存のリレー情報を含むメッセージを廃棄します。 • [Keep]：リレーエージェントは、既存のリレー情報を保持します。 • [Replace]：リレーエージェントは、既存の情報を独自のリレー情報で上書きします。

要素	説明
オプション	選択すると、DHCP クライアントからサーバに転送されたメッセージ要求への DHCP Option 82 データの挿入がイネーブルになります。DHCP Option 82 は、DHCP サーバに要求側クライアントのスイッチおよびポート ID の両方を提供します。このオプションにより、ユーザーがネットワークに物理的に接続している場所を特定し、スプーフィングを防ぐことができます。 DHCP リレーエージェントについて （114 ページ）を参照してください。 選択を解除すると、DHCP Option 82 がディセーブルになります。
Check	選択すると、DHCP サーバーから受信される DHCP Option 82 応答パケットが検証されます。無効なメッセージはドロップされます。有効なメッセージは、DHCP クライアントに転送される前に option-82 フィールドが削除されます。 選択を解除すると、先に有効性が確認されることなく option-82 フィールドはパケットから削除されます。

[DHCP Database] ダイアログボックス

[DHCP Database] ダイアログボックスを使用して、自動バインディングが含まれている外部の DHCP データベースを定義します。定義する各データベース URL は一意である必要があります。

詳細については、 DHCP データベース エージェントについて （113 ページ）を参照してください。

ナビゲーション パス

[DHCP] ポリシー ページ （118 ページ）に移動してから、データベーステーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- DHCP ポリシーの定義 （116 ページ）
- Cisco IOS ルータにおける DHCP （112 ページ）
- [IP Pool] ダイアログボックス （122 ページ）

フィールド リファレンス

表 *39 : [DHCP Database]* ダイアログボックス

要素	説明
Database URL	自動バインディングが含まれている外部の DHCP データベース エージェントの URL。URL は、HTTP、FTP、TFTP、または RCP 形式で入力できます。 （注） URL を定義する場合、IP アドレス プールを定義する必要はありません。ただし、定義することもできます。
タイムアウト（Timeout）	DHCP サーバがデータベース転送を中断するまで外部の DHCP データベース エージェントからの応答を待機する時間（秒数）。デフォルトは 300 秒（5 分）です。 （注） 値を 0 に設定するとタイムアウトがディセーブルになります。
Write Delay	DHCP サーバから外部の DHCP データベース エージェントに送信される更新の間隔（秒数）。最小遅延は 60 秒です。デフォルトは 300 秒（5 分）です。

[IP Pool] ダイアログボックス

[IP Pool] ダイアログボックスでは、DHCP サーバがダイナミック アドレスを DHCP クライアントに割り当てるために使用するアドレス プールを 1 つ以上定義します。外部の DHCP データベース エージェントが定義されている場合を除き、少なくとも 1 つのアドレス プールを定義する必要があります。

ナビゲーション パス

[DHCP] ポリシー ページ （118 ページ）に移動してから、[IPプール（IP Pools）] テーブルの下にある [追加（Add）] ボタンまたは [編集（Edit）] ボタンをクリックします。

関連項目

- DHCP アドレス プールの定義 （117 ページ）
- DHCP データベース エージェントについて （113 ページ）
- [DHCP Database] ダイアログボックス （121 ページ）
- Cisco IOS ルータにおける DHCP （112 ページ）

フィールド リファレンス

表 *40 : [IP Pool]* ダイアログボックス

要素	説明
プール名（Pool Name）	IP プールの名前。
ネットワーク（Network）	IP プールの IP アドレスおよびサブネットマスク。このサブネットには、DHCP サーバがクライアントへの割り当てに使用できる IP アドレスの範囲が含まれます。 ネットワーク/ホストオブジェクトのアドレスとマスク、または名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 **ヒント** 範囲内の特定のアドレスを [Excluded IPs] フィールドで定義して、それらのアドレスを除外できます。[DHCP] ポリシー ページ （118 ページ）を参照してください。
Default Router Addresses	この IP プールを使用している DHCP クライアントのデフォルトルータの IP アドレス。DHCP クライアントが起動した後、このルータへのパケットの送信が開始されます。ルータは、クライアントとして同じサブネット上に存在する必要があります。 最大 8 つのアドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
DNS Server Addresses	この IP プールを使用する DHCP クライアントがホスト名を IP アドレスに関連付ける必要があるときに問い合わせる DNS サーバの IP アドレス。 最大 8 つのアドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
NetBIOS (WINS) Server Addresses	Microsoft DHCP クライアントでホスト名を一般的なネットワーク グループ内の IP アドレスに関連付けるために使用する Windows Internet Naming Service（WINS）サーバの IP アドレス。 最大 8 つのアドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
ドメイン名	この IP プールを使用している DHCP クライアントのドメイン名。この名前を指定すると、これらのクライアントはドメインを構成する一般的なネットワーク グループ内に配置されます。

要素	説明
Import All	選択すると、リモート DHCP サーバは中央のサーバから特定の DHCP オプション（DNS サーバなど）をインポートできます。このオプションは、設定情報を自動的に更新できるようにする場合に使用します。 選択を解除すると、すべての DHCP オプションがこの特定のサーバに対してローカルになります。
Secured ARP	選択すると、DHCP 認可 ARP 機能がイネーブルになり、認可されたモバイル ユーザへの IP アドレスのリースが制限されます。この機能は、権限のないユーザーによる IP スプーフィングの防止に役立ちます。 Secured ARP について （115 ページ）を参照してください。 選択を解除すると、DHCP 認可 ARP 機能はディセーブルになります。 （注） この機能を使用すると、インターフェイスにおける動的な ARP 学習がディセーブルになります。
Lease Never Expires	選択すると、DHCP サーバは IP アドレスをクライアントに永続的に割り当てます。 選択を解除すると、アドレスは、[Time Length] フィールドに定義された期間だけリースされます。
Time Length (DD:HH:MM)	[Lease Never Expires] チェックボックスがオフになっている場合にだけ適用されます。 この IP プールから割り当てられた各 IP アドレスに対して指定するリース期間（DD:HH:MM の形式）。リース期間が終了すると、割り当てられた IP アドレスが無効になり、プールに返されます。
[オプション66（Option 66）]（IP アドレス）	IP 電話に設定ファイルを提供するために使用される TFTP サーバの IP アドレス。これらの設定ファイルでは、Cisco CallManager に接続するために IP 電話で必要とされるパラメータを定義します。 最大 8 つのアドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 （注） このオプションは、機能的には [Option 150] と似ています。一方または両方のオプションを使用できます。

要素	説明
Option 150 (IP Addresses)	IP 電話に設定ファイルを提供するために使用される TFTP サーバの IP アドレス。これらの設定ファイルでは、Cisco CallManager に接続するために IP 電話で必要とされるパラメータを定義します。 最大 8 つのアドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 （注） このオプションは、機能的には [Option 66] と似ています。一方または両方のオプションを使用できます。

Cisco IOS ルータにおける NTP

ネットワーク タイム プロトコル（NTP）は、ネットワーク デバイス間の時間同期の標準です。時間の同期により、syslog およびその他のデバッグ出力を特定のイベントに関連付けることができます。これは、トラブルシューティング、障害分析、およびセキュリティ インシデントの追跡に必要です。時間の比較は、ネットワーク内で発生するロギング、管理、および AAA 機能の間で正確な時間の同期がない限り、実行できません。

NTP では、ストラタムの概念を利用して、マシンが信頼できる時刻源からどれだけ離れているかを示します。たとえば、ストラタム 1 タイム サーバは、ラジオ クロックまたはアトミック クロックに直接接続されています。NTP は、この信頼できる時刻源の時刻をネットワーク全体に配信します。ストラタム 2 タイムサーバーは、ストラタム 1 タイムサーバーと同期します。ストラタム 3 タイムサーバーは、ストラタム 2 タイムサーバーと同期します。以降、同様に続きます。1 分あたり 1 つの NTP トランザクションを実行するだけで、2 台のマシンを 1 ミリ秒以内に同期できます。

NTP はポート 123 を使用し、ユーザ データグラム プロトコル（UDP）で動作します。Security Manager では、RFC 1305 で規定されている NTP バージョン 3 がサポートされます。

関連項目

- NTP サーバの定義 （125 ページ）

NTP サーバの定義

ここでは、ルータが時間の同期に使用する NTP サーバを定義する方法について説明します。NTP ポリシーの展開後、ルータは、遅延、分散、ジッタなどの要素に基づくアルゴリズムを使用して、最も正確な NTP サーバを特定し、そのサーバと同期をとります。

グローバル レベルでは、MD5 認証をイネーブルにし、ルータから送信されたすべての NTP パケットに対して使用する送信元アドレスを指定します。

ポリシーへの NTP サーバーの追加は、その IP アドレスを入力するだけで完了します。さらに、任意で認証パラメータを定義したり、精度が同程度の他の NTP サーバよりも特定のサーバを優先するかどうかを指定したりできます。

関連項目

- NTP サーバの定義 （125 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [NTP]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [NTP]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[NTP] ページが表示されます。このページのフィールドの説明については、表 41 : [NTP] ページ （128 ページ）を参照してください。

ステップ 2 （任意）[ソースインターフェイス（Source Interface）] フィールドに、インターフェイスまたはインターフェイスロールの名前を入力します。このインターフェイスまたはインターフェイスロールのアドレスが、ルータから送信されるすべての NTP パケットの送信元インターフェイスとして使用されます。または、[選択（Select）] をクリックしてリストからインターフェイスロールを選択するか、新しいインターフェイスロールを作成します。送信元インターフェイスには IP アドレスが必要です。

このオプションは、NTP サーバが（たとえばファイアウォールが原因で）接続元のアドレスに到達できない場合に役立ちます。このフィールドに値を入力しない場合は、発信インターフェイスのアドレスが使用されます。

（注） ステップ 5 （126 ページ）の手順に従って、個々の NTP サーバについてこのグローバル設定を上書きできます。

ステップ 3 （任意）[NTP認証の有効化（Enable NTP Authentication）] チェックボックスをオンにして、このルータとこのポリシーで定義する NTP サーバー間のすべてのアソシエーションを認証します。

ステップ 4 [サーバー（Servers）] テーブルの下にある [追加（Add）] ボタンをクリックして、[NTPサーバー（NTP Server）] ダイアログボックスを表示します。ここから、NTP サーバを定義できます。

ステップ 5 NTP サーバを定義します。使用可能なフィールドの説明については、表 42 : [NTP Server] ダイアログボックス （129 ページ）を参照してください。

ステップ 6 （任意）この NTP サーバの認証パラメータを定義します。

（注） 前に定義した認証キーの値を変更すると、変更はこのキーを共有するすべての NTP サーバに反映されます。

（注） Security Manager で認証キーを定義すると、CLI コマンドの最後に値 0 が自動的に付加されます。この値は、デフォルトの認証キー暗号化タイプを表し、CLI を使用して変更できます。

ステップ 7 ステップ 5 （126 ページ）～ステップ 6 （126 ページ）を繰り返して、他の NTP サーバを定義します。

ステップ 8 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義が [Servers] テーブルに表示されます。

（注） NTP サーバーを編集するには、[サーバー（Servers）] テーブルからサーバーを選択し、[編集（Edit）] をクリックします。NTP サーバーを削除するには、そのサーバーを選択し、[削除（Delete）] をクリックします。削除するサーバに定義されているキーが別の NTP サーバに定義されていない場合は、キーも削除されます。

[NTP Policy] ページ

[NTP] ページでは、ルータが時間の同期に使用できる NTP サーバを 1 つ以上定義します。たとえば、必要に応じて認証をイネーブルにしたり、これらのサーバに送信されるすべてのトラフィックのグローバル送信元インターフェイスを定義したりします。

詳細については、NTP サーバの定義 （125 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]>[デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [NTP]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [NTP]** を選択します。[NTP] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータにおける NTP （125 ページ）
- インターフェイス ロール オブジェクトについて
- テーブル カラムおよびカラム見出しの機能
- テーブルのフィルタリング

フィールド リファレンス

表 *41 : [NTP]* ページ

要素	説明
送信元インターフェイス（Source Interface）	NTP サーバに送信されるすべてのパケットの送信元アドレス。この設定は、NTP サーバが（たとえばファイアウォールが原因で）パケットの送信元のアドレスに応答できない場合に必要になることがあります。送信元インターフェイスには IP アドレスが必要です。 このフィールドで値を定義しない場合、発信インターフェイスのアドレスが使用されます。 インターフェイスの名前またはインターフェイスのロールを入力します。または、[選択（Select）]をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。 （注） このフィールドで定義した送信元インターフェイスは、個々の NTP サーバに対して上書きできるグローバル設定です。詳細については、[NTP Server] ダイアログボックス（129 ページ）を参照してください。
Enable NTP Authentication	選択すると、NTP サーバに接続するときに MD5 を使用した認証がイネーブルになります。 選択を解除すると、認証がディセーブルになります。
[Servers] テーブル	
IPアドレス	NTP サーバの IP アドレス。
送信元インターフェイス（Source Interface）	この NTP サーバに送信されるすべてのパケットの送信元アドレス。この設定は、ページの上部で定義されたグローバル設定を上書きします。
優先（Preferred）	精度が同程度の他の NTP サーバーよりもこの NTP サーバーが優先されるかどうかを示します。 （注） デフォルトでは、優先サーバがテーブルの最初に表示されます。
Key Number	この NTP サーバによる認証に使用されるキーの ID 番号。
信頼できる	この NTP サーバ用に定義された認証キーが trusted key であるかどうかを示します。
[追加（Add）] ボタン	[NTP Server] ダイアログボックス （129 ページ）が開きます。ここから、NTP サーバを定義できます。

要素	説明
[編集（Edit）] ボタン	[NTP Server] ダイアログボックス （129 ページ）が開きます。ここから、選択した NTP サーバを編集できます。
[削除（Delete）] ボタン	選択した NTP サーバをテーブルから削除します。 削除するサーバに定義されているキーが別の NTP サーバに定義されていない場合は、キーも削除されます。

[NTP Server] ダイアログボックス

[NTP Server] ダイアログボックスでは、ルータが時間の同時を実行するために使用できる NTP サーバのアドレスを定義します。さらに、このダイアログボックスを使用して、このサーバに送信される NTP パケットのデフォルトの送信元インターフェイスと認証パラメータを定義できます。

ナビゲーション パス

[NTP Policy] ページ （127 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- NTP サーバの定義 （125 ページ）
- Cisco IOS ルータにおける NTP （125 ページ）
- インターフェイス ロール オブジェクトについて

フィールド リファレンス

表 *42 : [NTP Server]* ダイアログボックス

要素	説明
IPアドレス	NTP サーバの IP アドレス。ネットワーク/ホストオブジェクトのアドレスまたは名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

要素	説明
送信元インターフェイス（Source Interface）	この NTP サーバに送信されるすべてのパケットの送信元アドレス。この設定は、NTP サーバが（たとえばファイアウォールが原因で）パケットの送信元のアドレスに応答できない場合に必要になることがあります。送信元インターフェイスには IP アドレスが必要です。 このフィールドで値を定義せず、グローバル設定がない場合は、発信インターフェイスのアドレスが使用されます。 （注） この設定は、[NTP Policy] ページ（127 ページ）で定義したグローバル設定を上書きします。 インターフェイスの名前またはインターフェイスのロールを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
優先（Preferred）	選択すると、精度が同程度の他の NTP サーバよりもこの NTP サーバが優先されます。このサーバが同期に使用される場合、ローカルクロックの修正に使用される時間オフセットは、このサーバだけに基づいて計算されます。 （注） 別の NTP サーバが優先サーバよりも著しく正確な場合（たとえば、ストラタム 2 対ストラタム 3）、ルータはより正確なサーバと同期をとります。 選択を解除すると、この NTP サーバは、精度が同程度の他の NTP サーバよりも優先されません。ローカルクロックの修正に使用される時間オフセットは、すべての NTP サーバのオフセットを組み合わせて計算されます。 複数のサーバのストラタムが同じであり、優先サーバの精度を信頼できる場合にだけ、特定の NTP サーバを優先サーバとして設定することを推奨します。
認証キー（Authentication Key）	NTP サーバによるアソシエーションの認証に使用される MD5 キー。 • [Key Number]：認証キーの ID 番号。キー番号を入力するか、またはリストから定義済みの番号を選択します。 • [Key Value]：認証キーを定義する最大 32 文字の文字列。[Confirm] フィールドに文字列をもう一度入力します。 • [Trusted]：選択すると、このキーはこのサーバと同期しようとしているシステムの ID を認証します。選択を解除すると、このキーは認証に使用されません。 リストからキー番号を選択してキー値を変更する場合は、この変更を保存すると同じ認証キーを使用する他の NTP サーバに影響する、という内容の警告が表示されます。 （注） 認証を使用するには、[NTP Policy] ページ（127 ページ）で認証をイネーブルにする必要があります。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。