セキュリティ コンフィギュレーション ガイド：ユーザ サービスのセキュリティ保護

Security Configuration Guide: Securing User Services

Cisco IOS Release 15.1S

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

ユーザ サービスのセキュリティ保護の概要

『ユーザ サービスのセキュリティ保護の概要』では、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）プロトコルを使用したユーザの識別、リモート デバイスへのユーザ アクセスの制御、およびセキュリティ サーバ情報を使用した Cisco IOS ネットワーキング デバイスでのサービスの追跡について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、この概要モジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

- 「Kerberos」（P.7）
- 「Lawful Intercept（合法的傍受）」（P.7）

AutoSecure

AutoSecure 機能で、ルータのセキュリティ設定が簡単になり、ネットワーク攻撃に利用できる共通 IP サービスルータ設定を無効にしてルータ設定を強化し、ネットワーク攻撃下では、ネットワーク防御に役立つ IP サービスと機能を有効にします。

AutoSecure では、次の方法で、マネジメント プレーンおよびフォワーディング プレーンの両方でセキュリティ保護します。

- マネジメント プレーンのセキュリティ保護は、潜在的にセキュリティ攻撃に利用される可能性がある特定のグローバルおよびインターフェイス サービスをオフにし、攻撃の脅威を軽減できるグローバル サービスをオンにすることで行います。また、セキュリティ保護されたアクセスとロギングもルータに設定できます。
- フォワーディング プレーンのセキュリティ保護は、Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）またはルータの distributed CEF（dCEF; 分散 CEF）を可能な限りイネーブルにすることで行います。トラフィックが新たな宛先に到着し始めたときにキャッシュ エントリを作成する必要がないため、大量のトラフィックが多数の宛先に送信される場合でも、CEF は他のモードよりも予測しやすい方法で動作します。このため、CEF 用に設定されているルータは、SYN 攻撃下において、従来のキャッシュ方法を採用しているルータと比較して高い性能を発揮します。

認証、認可、アカウンティング（AAA）

シスコの Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）パラダイムは、3 つの独立したセキュリティ機能をまとめて一貫性のあるモジュラ形式で設定するためのアーキテクチャ フレームワークです。AAA は、ユーザを認証する主な方法（TACACS+ サーバに格納されている username/password データベースなど）提供し、さらにバックアップ方法を指定します（ローカルに格納された username/password データベースなど）。このバックアップ方法は、主な方式のデータベースがネットワーキング デバイスからアクセスできない場合に使用されます。AAA を設定するには、「認証、認可、アカウンティング（AAA）」の章を参照してください。最大 4 つの順次バックアップ方法を設定できます。

（注） バックアップ方法が設定されていない場合は、username/password データベースになんらかの理由でアクセスできない場合にデバイスへのアクセスが拒否されます。

次のセクションで、AAA セキュリティ機能についてさらに詳細に説明します。

- 「認証」（P.3）
- 「認可」（P.3）
- 「アカウンティング」（P.3）
- 「認証プロキシ」（P.3）
- 「802.1x 認証サービス」（P.4）
- 「ネットワーク アドミッション コントロール」（P.4）

認証

認証で、ログイン/パスワード ダイアログ、チャレンジ/レスポンス、メッセージング サポート、および選択したセキュリティ プロトコルによっては暗号化などによるユーザの識別方法を提供します。認証は、ユーザに対してネットワークとネットワーク サービスへのアクセスを許可する前に、ユーザの識別を行う方法です。AAA 認証は、まず認証方式の名前付きリストを定義し、次に各種インターフェイスにそのリストを適用して設定します。

認可

認可で、ワンタイム許可またはサービスごとの許可、ユーザ単位のアカウント リストとプロファイル、ユーザ グループ サポート、および IP、Internetwork Packet Exchange（IPX）、AppleTalk Remote Access（ARA）、Telnet のサポートなど、リモート アクセスの制御方法を提供します。

RADIUS や TACACS+ などのリモート セキュリティ サーバでは、権限が定義されたアトリビュート値（AV）のペアを、対象のユーザに関連付けることで、ユーザに対して特定の権限を認可します。AAA 認可は、ユーザが認可された操作を示す一連のアトリビュートを組み合せて実行します。これらのアトリビュートとデータベースに格納されているユーザの情報とが比較され、その結果が AAA に返されてユーザの実際の権限と制限事項が決定されます。

アカウンティング

アカウンティングで、ユーザ識別、開始時刻と終了時刻、実行コマンド（PPP など）、パケット数、バイト数などといったセキュリティ サーバ情報の収集と送信を行い、課金、監査、およびレポートに使用する手段を提供します。アカウンティングを使用することで、ユーザがアクセスしているサービスや、ユーザが消費しているネットワーク リソース量を追跡できます。

（注） 認証は AAA と別個に設定することができます。ただし RADIUS、TACACS+、または Kerberos を使用する場合や、バックアップの認証方式を設定する場合は、AAA を設定する必要があります。

認証プロキシ

Cisco IOS ファイアウォール認証プロキシ機能は、ユーザごとのダイナミックな認証と認可のセキュリティ ポリシーを適用するためにネットワーク管理者が使用します。セキュリティ ポリシーは、業界標準の TACACS+ および RADIUS 認証プロトコルとともにユーザを認証します。ユーザごとに認証と認可を組み合わせることで、ユーザをユーザ単位のポリシーに基づいて識別し認証できるため、ネットワーク攻撃に対し、堅牢な保護を実現します。

認証プロキシ機能を実装すると、ユーザはネットワークにログインしたり HTTP 経由でインターネットにアクセスでき、ユーザ固有のアクセス プロファイルが CiscoSecure ACS やその他の RADIUS または TACACS+ 認証サーバから自動的に取得され、適用されます。ユーザ プロファイルは、認証されたユーザからのアクティブ トラフィックが存在するときにのみ、アクティブになります。

認証プロキシは、Network Address Translation（NAT; ネットワーク アドレス変換）、Context-Based Access Control（CBAC; コンテキストベース アクセス コントロール）、IP security（IPsec; IP セキュリティ）暗号化、および Cisco Secure VPN Client（VPN クライアント）ソフトウェアなどの、他の Cisco IOS セキュリティ機能と互換性があります。

802.1x 認証サービス

802.1x 認証サービス機能は、IEEE 802.1X プロトコル フレームワーク経由の Cisco サービス統合型ルータ（ISR）での、ローカル 802.1x ポートベースの認証および Virtual Private Network（VPN; バーチャル プライベート ネットワーク）アクセスの設定に使用されます。IEEE 802.1x 認証により、無許可のデバイス（サプリカント）にネットワークへアクセスされないようにします。

Cisco ISR は固定設定またはインストールされているモジュールに基づいて、ルータ、スイッチ、およびアクセス ポイントの機能を組み合わせることができます。スイッチ機能は、組み込みスイッチ ポートまたはスイッチ ポート付きプラグイン モジュールのいずれかにより提供されます。

IEEE 802.1x 規格には、クライアント / サーバベースのアクセス コントロールと認証プロトコルが定義されています。この認証プロトコルによって、無許可のクライアントは、適切に認証されない限り、公にアクセス可能なポートを使用して LAN に接続できません。認証サーバは、ポートに接続する各クライアントを認証してから、装置またはネットワークが提供するサービスの使用を許可します。

クライアントが認証されるまで、IEEE 802.1x アクセス コントロールでは、クライアントの接続先であるポートを介して、Extensible Authentication Protocol over LAN（EAPOL）、Cisco Discovery Protocol（CDP; シスコ検出プロトコル）、および Spanning Tree Protocol（STP; スパニング ツリー プロトコル）トラフィックだけが許可されます。認証に成功すると、通常のトラフィックをポート経由で送受信することができます。

ネットワーク アドミッション コントロール

Cisco Network Admission Control（NAC; ネットワーク アドミッション コントロール）機能で、増加するワームやウィルスが業務ネットワークに与える脅威や影響を解決します。この機能は、顧客がセキュリティの脅威を認識して防御し、適合するのに役立つ Cisco Self-Defending Network Initiative（自己防衛型ネットワーク構想）の一部です。

NAC を使用して、エンドポイントがネットワークに接続しようとしたときに、アクセス権限を Cisco ルータに強制できます。このアクセス権限は、アンチウィルス ソフトウェアのバージョン、ウィルス定義、スキャン エンジンのバージョンといった現在のアンチウィルスの状態などの、エンドポイント デバイスの情報に基づいて決定されます。

NAC により、適合しないデバイスはアクセスを拒否し、検疫領域に格納するか、コンピューティング リソースへのアクセス制限を与えることができ、非セキュアなノードをネットワーク感染から保護します。NAC の主要なコンポーネントは Cisco Trust Agent（CTA）で、エンドポイント システムに常駐しており、ネットワークの Cisco ルータと通信します。CTA は、使用しているアンチウィルス ソフトウェアなどのセキュリティ状態情報を収集し、この情報を Cisco ルータに伝達します。次に、この情報は、Cisco Secure Access Control Server（ACS）にリレーされ、そこでアクセス コントロールが決定されます。ACS は、Cisco ルータに、エンドポイントに対し強制を実施するよう指示します。

セキュリティ サーバ プロトコル

AAA セキュリティ プロトコルは、セキュリティ機能を管理するルータまたはネットワーク アクセス サーバで使用されます。AAA は、ネットワーク アクセス サーバと シスコがサポートしている RADIUS または TACACS+ セキュリティ サーバ プロトコルとの間の通信を確立する手段に使用されます。

セキュリティ サーバ上のデータベースを使用してログイン ユーザ名とパスワードのペアを保存する場合は、該当するプロトコルをサポートするようルータまたはアクセス サーバを設定する必要があります。また、サポートされているほとんどのセキュリティ プロトコルは、AAA セキュリティ サービスを使用して管理する必要があるため、AAA をイネーブルにする必要があります。

次のセクションで、RADIUS および TACACS+ セキュリティ サーバについてさらに詳細に説明します。

- 「RADIUS」（P.5）
- 「TACACS+」（P.5）

RADIUS

RADIUS 分散型クライアント/サーバ システムは AAA を使用して実装されます。RADIUS はネットワークを不正アクセスから保護します。シスコの実装では RADIUS クライアントは Cisco ルータ上で稼動します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

TACACS+

TACACS+ セキュリティ アプリケーションは、AAA を使用して実装され、ルータまたはネットワーク アクセス サーバにアクセスしようとするユーザの検証を集中的に行います。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で動作する TACACS+ デーモンのデータベースで管理されます。TACACS+ は独立したモジュール型の認証、認可、およびアカウンティング機能を備えています。

このプロトコルはネットワークの規模の拡大に合わせて拡張し、新しいセキュリティ技術を適用するために設計されました。TACACS+ プロトコルの基礎となるアーキテクチャは個別 AAA アーキテクチャを補完します。

RADIUS および TACACS+ アトリビュート

RADIUS および TACACS+ RFC にはさまざまなベンダー インタープリテーションがあります。ベンダーごとに他の RFC との準拠性がある場合もありますが、相互運用性は保証されません。相互運用性は、RADIUS および TACACS+ で標準 RFC が使用されている場合にのみ保証されます。

非標準の RADIUS および TACACS+ RFC が使用されている場合、それぞれのデバイスで相互運用できるようベンダーがアトリビュートを開発し実装する必要があります。

次のセクションで、RADIUS および TACACS+ アトリビュートについてさらに詳細に説明します。

- 「RADIUS アトリビュート」（P.5）
- 「TACACS+ アトリビュート」（P.5）

RADIUS アトリビュート

RADIUS アトリビュートは、RADIUS デーモンに格納されているユーザ プロファイルの特定の AAA 要素を定義するために使用されます。

TACACS+ アトリビュート

TACACS+ アトリビュートと値のペアが、ユーザ プロファイルの特定の要素の定義に使用され、TACACS+ デーモンに格納されます。

セキュア シェル（SSH）

Secure Shell（SSH; セキュア シェル）機能は、rsh、rlogin、rc などの UNIX r-commands スイートに安全に置換するアプリケーションおよびプロトコルです（Cisco IOS は rlogin をサポートします）。このプロトコルは標準の暗号メカニズムを使用してセッションの安全を確保します。アプリケーションは Berkeley の rexec および rsh ツールと同様に使用できます。現在、2 つのバージョンの SSH（SSH バージョン 1 と SSH バージョン 2）を使用できます。

Cisco IOS ログイン機能拡張

Cisco IOS Login Enhancements（Login Block）機能により、ユーザはサービス拒絶（DoS）攻撃と思われる攻撃が検出された場合、ログイン試行を自動的にブロックするオプションを設定して、ルータのセキュリティを強化できます。

この機能により導入された Login Block オプションおよび Login Delay オプションで、Telnet または SSH 仮想接続を設定できます。この機能をイネーブルにすると、接続試行の失敗が複数回検出された場合に、「待機時間」を強制して「辞書攻撃」をスローダウンし、ルーティング デバイスを DoS 攻撃から保護できます。

Cisco IOS Resilient 設定

Cisco IOS Resilient Configuration 機能で、実行中のイメージおよび設定のワーキング コピーを保護し維持することができます。これにより、イメージや設定ファイルが永続ストレージ（NVRAM やフラッシュ）の内容を消去する不正な攻撃に耐えることができます。

イメージ確認

イメージ確認機能で、Cisco IOS イメージの整合性を自動的に確認できます。そのため、ユーザは、イメージが偶発的な破壊から保護されていることを確認できます。破壊は、シスコによってファイルが作成された瞬間からユーザに届くまで、輸送中にいつでも起きる可能性があります。

IP Source Tracker

IP Source Tracker 機能で、攻撃下にあると考えられるホストへのトラフィックに関する情報を収集できます。また、この機能で、ネットワークへの入り口への攻撃を簡単にトレースできます。

ロールベースの CLI アクセス

ロールベースの CLI アクセス機能を使用すれば、ネットワーク管理者は「ビュー」を定義できます。ビューは、Cisco IOS EXEC コマンドおよびコンフィギュレーション（config）モード コマンドへのアクセスを精選したり部分的に制限する、操作コマンドと設定機能のセットです。ビューで、ユーザの Cisco IOS Command-Line Interface（CLI; コマンドライン インターフェイス）や設定情報へのアクセスを制限します。つまり、ビューで、使用するコマンドや表示する設定情報を定義できます。したがって、ネットワーク管理者はシスコ ネットワーキング デバイスへのアクセスを柔軟に管理できます。

パスワード、権限、ログインユーザ名を使用した、ネットワーキング デバイスでの CLI セッションでのセキュリティ

ネットワーキング デバイスがネットワークに、セキュリティ オプションを設定せずにインストールされている状態や、ネットワーキング デバイスがインストールされており、セキュリティのベースラインが、ネットワーキング デバイスで実行している Cisco IOS CLI オペレーティング システム セッションでどのように実装されているか知るための手助けが必要な場合があります。

このマニュアルでは、次の基本セキュリティの内容を説明しています。

- CLI セッションでの異なる認証レベルを区別して、ネットワーキング デバイスのステータス対デバイスのモニタに使用されるコマンドを変更できるコマンドへのアクセスを制御する
- パスワードは CLI セッションに割り当てられる
- ユーザはネットワーキング デバイスにユーザ名を使用してログインできる
- コマンドの権限レベルを変更して CLI セッションでの新しい承認レベルを作成する

Kerberos

Kerberos 機能は、暗号化と認証に Data Encryption Standard（DES; データ暗号規格）暗号化アルゴリズムを使用した AAA を使用して実装されるシークレットキー ネットワーク認証プロトコルです。Kerberos はネットワーク リソースの要求を認証するために設計され、ユーザおよびサービスの安全な検証を実行する信頼のあるサードパーティのコンセプトに基づいています。これは主に、ユーザとユーザが使用しているネットワーク サービスが本当に要求されているものであるかを確認するために使用されます。この検証を行うには、信頼できる Kerberos サーバでユーザのクレデンシャル キャッシュに格納して標準のユーザ名およびパスワード認証メカニズムの代わりに使用できる期限付きのチケットを発行します。

Lawful Intercept（合法的傍受）

Lawful Intercept（LI; 合法的傍受）機能は、法執行機関の要件に適合するサービス プロバイダーをサポートし、Voice over IP（VoIP）またはエッジ ルータを通るデータ トラフィックを代行受信する機能を提供します。Lawful Intercept（LI; 合法的傍受）アーキテクチャには、Cisco Service Independent Intercept アーキテクチャと PacketCable The Lawful Lawful Intercept アーキテクチャが含まれています。

Lawful Intercept（合法的傍受）

AutoSecure

AutoSecure 機能では、1 つの CLI コマンドによって、ネットワーク攻撃に悪用されるおそれのある一般的な IP サービスを無効にしたり、攻撃を受けたときにネットワークを防御するのに役立つ IP サービスや機能を有効にしたりできます。また、ルータのセキュリティ設定を簡素化しつつ機能を堅牢にすることができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「AutoSecure の機能情報」（P.15）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

AutoSecure の制約事項

AutoSecure 機能は、実稼動ネットワークではなく、テスト環境で使用する必要があります。

AutoSecure について

AutoSecure を設定するために、次の概念を理解しておく必要があります。

- 「AutoSecure の利点」（P.2）
- 「マネジメント プレーンのセキュリティ保護」（P.3）
- 「フォワーディング プレーンのセキュリティ保護」（P.6）

AutoSecure の利点

ルータのセキュリティ設定の簡素化

AutoSecure を使用すると、すべての Cisco IOS 機能を詳しく把握していなくても、ネットワークをすばやくセキュリティ保護できるため、AutoSecure は、特別なセキュリティ操作アプリケーションを持っていない顧客にとって役に立つ機能です。

これにより、セキュリティ機能の設定を自動化したり、デフォルトで有効になり、セキュリティ ホールとして悪用されることのある特定の機能を無効化したりする CLI を作成してルータをセキュリティ保護する複雑な作業が不要になります。

強化されたパスワード セキュリティ

AutoSecure の次のメカニズムにより、ルータへのアクセスの安全性が向上しています。

- パスワードに必要な最小長を設定することができます。これにより、「lab」や「cisco」など、ほとんどのネットワークで広く使用されているありふれたパスワードを排除できます。

  パスワードの最小長を設定するコマンドは **security passwords min-length** です。

- 正常に実行できなかった回数が、設定したしきい値を超えると、syslog メッセージが生成されます。

  許容できるログイン失敗回数（しきい値）を設定するコマンドは、**security passwords min-length** です。

ロールバックおよびシステム ロギング メッセージのサポート

Cisco IOS Release 12.3(8)T では、AutoSecure 設定のロールバックがサポートされています。ロールバックを有効にすると、AutoSecure 設定に失敗しても、ルータを前の設定状態に戻すことができます。

（注） Cisco IOS Release 12.3(8)T よりも前のリリースでは、AutoSecure 設定をロールバックすることはできません。このため、AutoSecure を設定する前に、現行の設定を常に保存する必要があります。

システム ロギング メッセージは、現行の設定に適用されている AutoSecure 設定の変更または改ざんを捕捉します。つまり、AutoSecure を実行しているときに詳細な監査証跡情報が得られます。

マネジメント プレーンのセキュリティ保護

マネジメント プレーンのセキュリティ保護は、AutoSecure 機能の中心となる 2 つの分野の 1 つです（もう一方の中心分野は次の「フォワーディング プレーンのセキュリティ保護」で説明します）。マネジメント プレーンのセキュリティ保護は、セキュリティ攻撃のために悪用される可能性のあるいくつかのグローバル サービスとインターフェイス サービスをディセーブルにし、攻撃の脅威を軽減する効果のあるグローバル サービスをイネーブルにすることによって行われます。また、セキュリティ保護されたアクセスとロギングもルータに設定できます。

注意 デバイスが Network Management（NM; ネットワーク管理）アプリケーションで管理されている場合、マネジメント プレーンのセキュリティ保護によって、HTTP サーバなどのいくつかのサービスがディセーブル化され、NM アプリケーションのサポートが妨げられることがあります。

ここでは、AutoSecure がマネジメント プレーンのセキュリティ保護にどのように役立つかを説明します。

- 「グローバル サービスのディセーブル化」（P.3）
- 「サービスのインターフェイス単位のディセーブル化」（P.4）
- 「グローバル サービスのイネーブル化」（P.4）
- 「ルータへのセキュリティ保護されたアクセス」（P.4）
- 「セキュリティを確保するためのロギング」（P.5）

グローバル サービスのディセーブル化

AutoSecure 機能を（**auto secure** コマンドで）イネーブルにすると、ルータで次のグローバル サービスが自動的にディセーブルになります。

- Finger：攻撃の前のシステムの情報を収集（探査）します。イネーブルになっている場合、この情報により、デバイスが攻撃に対して脆弱なままになることがあります。
- PAD：すべての Packet Assembler and Disassembler（PAD; パケット アセンブラ/ディスアセンブラ）コマンドと、PAD デバイスとアクセス サーバとの接続をイネーブルにします。イネーブルになっている場合、このサービスにより、デバイスが攻撃に対して脆弱なままになることがあります。
- スモール サーバ：TCP および User Datagram Protocol（UDP; ユーザ データグラム プロトコル）の診断ポート攻撃の原因となります。この攻撃では、送信者がルータの UDP 診断サービスに偽の要求を大量に送信し、CPU リソースを使い果たします。
- BOOTP サーバ：BOOTP は安全ではないプロトコルで、攻撃に悪用される可能性があります。
- HTTP サーバ：Secure HTTP が使用されていないか、ACL を関連付けて HTTP サーバに組み込まれる認証が使用されていない場合、HTTP サーバは安全ではなく、攻撃に悪用されることがあります（HTTP サーバをイネーブルにする必要がある場合は、適切な認証またはアクセス リストの指定を求めるメッセージが表示されます）。

（注） Cisco Configuration Professional を使用している場合は、**ip http server** コマンドを使用して HTTP サーバを手動でイネーブルにする必要があります。

- 識別サービス：RFC 1413 で定義されている安全ではないプロトコルです。TCP ポートで ID を照会することが可能です。攻撃者は、ID サーバでユーザに関する個人的な情報にアクセスできます。
- CDP：大量の Cisco Discovery Protocol（CDP; シスコ検出プロトコル）パケットがルータに送信されると、ルータの使用可能なメモリが消費され、ルータがクラッシュすることがあります。

注意 CDP を使用してネットワーク トポロジを検出する NM アプリケーションは、検出を実行できなくなります。

- NTP：認証またはアクセス制御が行われないと、Network Time Protocol（NTP; ネットワーク タイム プロトコル）は安全ではありません。攻撃者はこのプロトコルを使用して NTP パケットを送信し、ルータをクラッシュさせたり、過負荷状態にしたりすることが可能です（NTP を有効にする場合は、Message Digest 5（MD5; メッセージ ダイジェスト 5）および **ntp access-group** コマンドを使用して NTP 認証を設定する必要があります。NTP がグローバルにイネーブルになっている場合は、NTP が不要なすべてのインターフェイスでディセーブルにしてください）。
- 送信元ルーティング：デバッグ作業でのみ使用するため、それ以外の場合はディセーブルにする必要があります。そうしないと、アクセス制御メカニズムを通過すべきパケットが、一部のアクセス制御メカニズムを回避する可能性があります。

サービスのインターフェイス単位のディセーブル化

AutoSecure 機能をイネーブルにすると、次のインターフェイス単位のサービスが自動的にルータでディセーブルになります。

- ICMP リダイレクト：すべてのインターフェイスでディセーブルになります。このサービスは、正しく設定されたネットワークにとっては有益な機能ではなく、セキュリティ ホールを悪用するために攻撃者によって使用される可能性があります。
- ICMP 到達不能：すべてのインターフェイスでディセーブルになります。Internet Control Management Protocol（ICMP;インターネット制御マネジメント プロトコル）到達不能は、ICMP ベースの Denial of Service（DoS; サービス拒否攻撃）の原因として知られています。
- ICMP マスク応答メッセージ：すべてのインターフェイスでディセーブルになります。ICMP マスク応答メッセージにより、攻撃者はインターネットワークの特定のサブネットワークのサブネットマスクを入手できます。
- プロキシ Arp：すべてのインターフェイスでディセーブルになります。プロキシ Arp 要求は、DoS 攻撃の原因として知られています。これは、攻撃者が何度も送信した要求に応答しようとしてルータの使用可能な帯域幅とリソースが消費されることがあるためです。
- ダイレクト ブロードキャスト：すべてのインターフェイスでディセーブルになります。DoS を生じさせるための SMURF 攻撃の原因となる可能性があります。
- Maintenance Operations Protocol（MOP; メンテナンス オペレーション プロトコル）サービス：すべてのインターフェイスでディセーブルになります。

グローバル サービスのイネーブル化

AutoSecure 機能をイネーブルにすると、次のグローバル サービスが自動的にルータでイネーブルになります。

- **service password-encryption** コマンド：パスワードが設定で表示されなくなります。
- **service tcp-keepalives-in** コマンドと **service tcp-keepalives-out** コマンド：異常終了した TCP セッションが確実に削除されます。

ルータへのセキュリティ保護されたアクセス

注意 デバイスが NM アプリケーションによって管理されている場合に、ルータへのアクセスをセキュリティ保護すると、重要なサービスが無効化されたり、NM アプリケーションのサポートが妨げられたりすることがあります。

AutoSecure 機能をイネーブルにすると、ルータへのアクセスをセキュリティ保護する次のオプションをユーザが使用できるようになります。

- テキスト バナーがない場合は、バナーの追加を求めるメッセージが表示されます。AutoSecure 機能には次のサンプル バナーが用意されています。

```
Authorized access only
    This system is the property of ABC Enterprise
    Disconnect IMMEDIATELY if you are not an authorized user!
    Contact abc@xyz.com +99 876 543210 for help.
```

- ログインおよびパスワード（サポートされている場合はシークレット パスワードを推奨）は、コンソール、AUX、TTY の各回線で設定されます。**transport input** コマンドおよび **transport** output コマンドも、これらのすべての回線で設定されます（Telnet および Secure Shell（SSH; セキュア シェル）だけが有効な転送方法です）。**exec-timeout** コマンドは、コンソールと AUX の各回線で 10 に設定されます。
- デバイスのイメージが暗号化イメージである場合、AutoSecure はルータに対するアクセスとファイル転送に SSH と Secure Copy（SCP; セキュア コピー）をイネーブルにします。**ip ssh** コマンドの **timeout** *seconds* および **authentication-retries** *integer* の各オプションは最小数に設定されます（Telnet および FTP は、この操作の影響を受けず、引き続き動作します）。
- AutoSecure ユーザが、デバイスで Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を使用しないと指定した場合は、次のいずれかの状態になります。
  - インタラクティブ モードでは、コミュニティ ストリングの値に関係なく SNMP をディセーブルにするかどうかを尋ねるメッセージがユーザに表示されます。コミュニティ ストリングは、パスワードと同じように機能し、ルータのエージェントへのアクセスを規制します。
  - 非インタラクティブ モードでは、コミュニティ ストリングが「public」または「private」である場合に SNMP がディセーブルになります。

（注） AutoSecure がイネーブルになると、SNMP を使用してデバイスをモニタおよび設定するツールが SNMP を介してデバイスと通信することができなくなります。

- Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）が設定されていない場合は、ローカル AAA を設定します。ユーザは、ローカルのユーザ名とそのパスワードをルータで設定するように AutoSecure から要求されます。

セキュリティを確保するためのロギング

AutoSecure 機能をイネーブルにすると、セキュリティ インシデントを識別して対応することができる次のロギング オプションが使用できます。

- すべてのデバッグ メッセージおよびログ メッセージのシーケンス番号とタイム スタンプ。このオプションは、ロギング メッセージを監査するときに役立ちます。
- ログイン関連イベントのロギング メッセージの生成。たとえば、ログイン攻撃が検出され、ルータが「待機モード」になると、「Blocking Period when Login Attack Detected」というメッセージが表示されます（待機モードでは、ルータは Telnet、HTTP、SSH によるログインをすべて許可しません）。

  ログイン関連のシステム メッセージの詳細については、『Cisco IOS Release 12.3(4)T feature module *Cisco IOS Login Enhancements*』を参照してください。
- **logging console critical** コマンド。これにより、システム ロギング（syslog）メッセージがすべての使用可能な TTY 回線に送信され、重大度に応じてメッセージが制限されます。
- **logging buffered** コマンド。これにより、ロギング メッセージが内部バッファにコピーされ、バッファに記録されるメッセージが重大度に応じて制限されます。

- **logging trap debugging** コマンド。これにより、デバッグよりも重大度の高いコマンドをすべてロギング サーバに送信できます。

フォワーディング プレーンのセキュリティ保護

ルータのフォワード プレーンでの攻撃の危険を最小限にするために、AutoSecure には次の機能が用意されています。

- Cisco Express Forwarding（CEF; Cisco エクスプレス フォワーディング）: AutoSecure は、可能であれば CEF または distributed CEF（dCEF; 分散 CEF）をルータでイネーブルにします。トラフィックが新たな宛先に到着し始めたときにキャッシュ エントリを作成する必要がないため、大量のトラフィックが多数の宛先に送信される場合でも、CEF は他のモードよりも予測しやすい方法で動作します。このため、CEF 用に設定されているルータは、SYN 攻撃下において、従来のキャッシュ方法を採用しているルータと比較して高い性能を発揮します。

（注） CEF は従来のキャッシュよりもメモリを多く消費します。

- TCP インターセプト機能が使用可能な場合、この機能をルータで接続タイムアウト用に設定することができます。
- 厳密な Unicast Reverse Path Forwarding（uRPF; ユニキャスト リバース パス転送）が使用可能である場合、偽造（詐称）された送信元 IP アドレスが入ってくることによって発生する問題を軽減できるようにするために、この uRPF をルータで設定できます。uRPF では、検証可能な送信元 IP アドレスがない IP パケットが破棄されます。
- ルータは、ファイアウォールとして使用されている場合、インターネットに繋がっているパブリック インターフェイスで Context-Based Access Control（CBAC; コンテキストベース アクセス制御）用に設定することができます。

（注） AutoSecure ダイアログの冒頭では、パブリック インターフェイスのリストの指定を求めるメッセージが表示されます。

AutoSecure の設定方法

ここでは、次の各手順について説明します。

- 「AutoSecure の設定」（P.6）（必須）
- 「その他のセキュリティ設定」（P.8）（必須）
- 「AutoSecure の確認」（P.8）（任意）

AutoSecure の設定

AutoSecure を設定するために、次の作業を行う必要があります。

auto secure コマンド

auto secure コマンドを実行すると、マネジメント プレーンとフォワーディング プレーンをセキュリティ保護するための半インタラクティブなセッション（AutoSecure ダイアログ）を行うことができます。このコマンドには、マネジメント プレーンとフォワーディング プレーンのどちらかだけをセキュリティ保護するオプションがあります。どちらのオプションも選択しない場合は、両方のプレーンを設定することを確認するメッセージがダイアログに表示されます。

また、ダイアログの非インタラクティブな部分の設定をすべて行ってから、インタラクティブな部分の設定を行うことも可能です。ダイアログの非インタラクティブな部分のイネーブル化は、オプションの **no-interact** キーワードを選択して行います。

注意 **auto secure** コマンドでルータのセキュリティ保護を行うことはできますが、ルータが完全にセキュリティ保護されるという保証はありません。

制約事項

AutoSecure の設定は、実行時またはセットアップ時に行います。AutoSecure をイネーブルにした後に、関連する設定を変更した場合は、AutoSecure の設定が完全に有効にならないことがあります。

手順の概要

1. **enable**
2. **auto secure** [**management** | **forwarding**] [**no-interact** | **full**] [**ntp** | **login** | **ssh** | **firewall** | **tcp-intercept**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 プロンプトが表示されたら、パスワードを入力します。

ステップ 2	`auto secure [management | forwarding] [no-interact | full] [ntp | login | ssh | firewall | tcp-intercept]`
	
	例：
	`Router# auto secure`
		ルータのマネジメント プレーンおよびフォワーディング プレーンをセキュリティ保護します。
		• **management**：マネジメント プレーンのみがセキュリティ保護されます。
		• **forwarding**：フォワーディング プレーンのみがセキュリティ保護されます。
		• **no-interact**：インタラクティブな設定を行うためのメッセージがまったく表示されません。
		• **full**：インタラクティブな質問メッセージがすべて表示されます。これがデフォルトです。

その他のセキュリティ設定

次の作業を行って、ルータへのアクセスのセキュリティ保護を強化します。

手順の概要

1. **enable**
2. **configure terminal**
3. **security passwords min-length** *length*
4. **enable password** {*password* | [*encryption-type*] *encrypted-password*}
5. **security authentication failure rate** *threshold-rate* **log**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**security passwords min-length** *length* 例： `Router(config)# security passwords min-length 6`	設定される各パスワードが、指定した長さ以上になるようにします。 • *length*：設定されるパスワードの最小長です。
ステップ 4	**enable password** {*password* | [*encryption-type*] *encrypted-password*} 例： `Router(config)# enable password elephant`	さまざまな権限レベルへのアクセスを制御するローカル パスワードを設定します。
ステップ 5	**security authentication failure rate** *threshold-rate* **log** 例： `Router(config)# security authentication failure rate 10 log`	許容されるログイン失敗回数を設定します。 • *threshold-rate*：許容されるログイン失敗回数。 • **log**：回数がしきい値を超えた場合、syslog 認証は失敗します。

AutoSecure の確認

AutoSecure の機能が正しく実行されていることを確認するには、次の手順を行います。

手順の概要

1. **enable**
2. **show auto secure config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show auto secure config** 例： Router# show auto secure config	（任意）AutoSecure の設定の過程で追加されたコンフィギュレーション コマンドをすべて表示します。

AutoSecure の設定例

ここでは、次の設定例について説明します。

- 「AutoSecure の設定ダイアログの例」（P.9）

AutoSecure の設定ダイアログの例

AutoSecure ダイアログの例を次に示します。**auto secure** コマンドを実行すると、下記のようなダイアログが自動的に表示されます。ただし、**no-interact** キーワードを指定した場合を除きます（ディセーブルになっているサービスと、イネーブルになっている機能については、このマニュアルの「マネジメント プレーンのセキュリティ保護」および「フォワーディング プレーンのセキュリティ保護」を参照してください）。

```
Router# auto secure
                --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of the router but it will not make
router absolutely secure from all security attacks ***

All the configuration done as part of AutoSecure will be shown here. For more details of
why and how this configuration is useful, and any possible side effects, please refer to
Cisco documentation of AutoSecure.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]:y
Enter the number of interfaces facing internet [1]:
Interface                  IP-Address OK? Method Status
Protocol
FastEthernet0/1            10.1.1.1  YES NVRAM  up down

FastEthernet1/0            10.2.2.2  YES NVRAM  up down

FastEthernet1/1            10.0.0.1  YES NVRAM  up up

Loopback0                  unassigned YES NVRAM  up up

FastEthernet0/0            10.0.0.2  YES NVRAM  up down
```

```
Enter the interface name that is facing internet:FastEthernet0/0

Securing Management plane services..

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp
Enable secret is either not configured or is same as enable password
Enter the new enable secret:abc123
Configuring aaa local authentication
Configuring console, Aux and vty lines for
local authentication, exec-timeout, transport

Configure SSH server? [yes]:
Enter the domain-name:example.com

Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:

 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces

Securing Forwarding plane services..

Enabling CEF (it might have more memory requirements on some low end
platforms)

Enabling unicast rpf on all interfaces connected to internet

Configure CBAC Firewall feature? [yes/no]:yes

This is the configuration generated:

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$CZ6G$GkGOnHdNJCO3CjNHHyTUA.
```

```
aaa new-model
aaa authentication login local_auth local
line console 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
ip domain-name example.com
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
 transport input ssh telnet
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
int FastEthernet0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int FastEthernet1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int FastEthernet1/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int FastEthernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
ip cef

interface FastEthernet0/0
 ip verify unicast reverse-path
ip inspect audit-trail
ip inspect dns-timeout 7
ip inspect tcp idle-time 14400
ip inspect udp idle-time 1800
ip inspect name autosec_inspect cuseeme timeout 3600
ip inspect name autosec_inspect ftp timeout 3600
```

```
ip inspect name autosec_inspect http timeout 3600
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout 3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15
ip inspect name autosec_inspect tcp timeout 3600
access-list 100 deny ip any any
interface FastEthernet0/0
 ip inspect autosec_inspect out
 ip access-group 100 in
!
end


Apply this configuration to running-config? [yes]:yes

Applying the config generated to running-config
The name for the keys will be:ios210.example.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys ...[OK]
Router#
```

その他の参考資料

ここでは、AutoSecure の機能の関連資料について説明します。

関連資料

内容	参照先
ログイン機能（ログイン遅延やログイン ブロッキング期間など）	「Cisco IOS Login Enhancements」フィーチャ モジュール
ルータの設定に関するその他の情報	『*Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.4T』
その他のルータ コンフィギュレーション コマンド	『*Cisco IOS Configuration Fundamentals Command Reference Guide*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1918	「Address Allocation for Private Internets」
RFC 2267	「*Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/public/support/tac/home.shtml

AutoSecure の機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　AutoSecure の機能情報

機能名	リリース	機能情報
AutoSecure	12.3(1) 12.2(18)S 12.3(8)T 12.2(27)SBC	AutoSecure 機能では、1 つの CLI コマンドによって、ネットワーク攻撃に悪用されるおそれのある一般的な IP サービスを無効にしたり、攻撃を受けたときにネットワークを防御するのに役立つ IP サービスや機能を有効にしたりできます。また、ルータのセキュリティ設定を簡素化しつつ機能を堅牢にすることができます。 この機能は、Cisco IOS Release 12.3(1)S で導入されました。 この機能は、Cisco IOS Release 12.2(18)S に統合されました。 Cisco IOS Release 12.3(8)T では、ロールバック機能とシステム ロギング メッセージがサポートされました。 この機能は、Cisco IOS Release 12(27)SBC に統合されました。 次のコマンドが導入または変更されました。**auto secure**、**security passwords min-length**、**show auto secure config**

認証、認可、アカウンティング（AAA）

認証

認証の設定

認証は、ログイン/パスワード ダイアログ、チャレンジ/レスポンス、メッセージング サポート、および選択したセキュリティ プロトコルによっては暗号化などによるユーザの識別方法を提供します。認証は、ユーザに対してネットワークとネットワーク サービスへのアクセスを許可する前に、ユーザの識別を行う方法です。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「認証の設定に関する機能情報」（P.61）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

認証の設定に関する前提条件

認証の Cisco IOS ソフトウェア実装は、AAA 認証方式と非認証方式に分かれています。シスコでは、可能であれば AAA セキュリティ サービスを試用して認証を実装することを推奨します。

認証の設定に関する制約事項

- Cisco IOS Release 12.3 では、設定できる AAA 方式リストの数が 250 になりました。
- 非標準のオプションを使用して RADIUS サーバを設定し、非標準のオプションを使用せずに別の RADIUS サーバを設定すると、非標準のオプションを使用する RADIUS サーバ ホストでは事前定義されたホストが受け入れられません。**acct-port** キーワードを使用してアカウンティング要求の異なる UDP 宛先ポートに同じ RADIUS サーバ ホスト IP アドレスを設定し、**auth-port** キーワードを使用して認証要求の UDP 宛先ポートを設定する場合、認証要求に非標準オプションを使用したかどうかに関係なく、RADIUS サーバでは非標準オプションが受け入れられません。

認証設定について

ここでは、認証方式の名前付きリストを定義し、そのリストを多様なインターフェイスに適用して AAA 認証を定義する方法と、RADIUS Change of Authorization（CoA; 認可変更）を使用して AAA 認証を処理する方法について説明します。

- 「認証の名前付き方式リスト」（P.2）
- 「RADIUS Change of Authorization」（P.5）

認証の名前付き方式リスト

まず認証方式の名前付きリストを定義して AAA 認証を設定し、その名前付きリストを多様なインターフェイスに適用します。方式リストには、実行する認証の種類と、実行するシーケンスを定義します。方式リストは特定のインターフェイスに適用され、定義済みの認証方式のいずれかが実行されます。唯一の例外は、デフォルトの方式リスト（「default」という名前が指定されています）です。デフォルトの方式リストは、名前付きの方式リストが明示的に定義されているインターフェイスを除き、すべてのインターフェイスに自動的に適用されます。デフォルトの方式リストは、定義された方式リストによって上書きされます。

方式リストとは、ユーザ認証のために照会される認証方式を記載したシーケンシャル リストです。方式リストを使用すると、認証に使用するセキュリティ プロトコルを 1 つまたは複数指定できるため、最初の方式が失敗した場合に備えて認証のバックアップ システムを確保できます。Cisco IOS ソフトウェアは、ユーザを認証するため、リストに掲載されている最初の方式が使用されます。その方式で応答に失敗した場合、Cisco IOS ソフトウェアは、方式リストに掲載されている次の認証方式を選択します。このプロセスは、方式リストのいずれかの認証方式と通信に成功するか、定義されているすべての方式が試行されるまで継続されます。

Cisco IOS ソフトウェアでは、前の方式からの応答がない場合にだけ、リストの次の認証方式で認証が試行される、という点が重要です。このサイクルの任意の時点で認証が失敗した場合（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からユーザ アクセスの拒否応答が返される場合）、認証プロセスは停止し、その他の認証方式は試行されません。

この項目は次のサブ項目から構成されます。

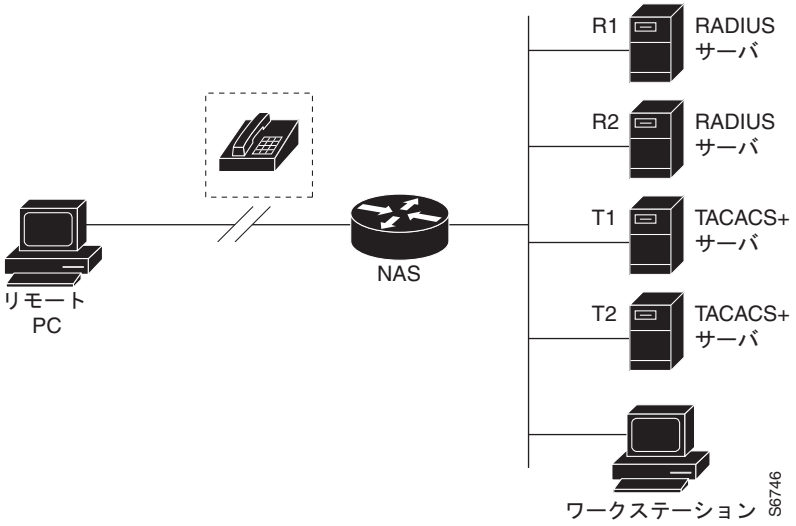
- 「方式リストとサーバ グループ」（P.3）

- 「方式リストの例」（P.4）
- 「AAA 認証の一般的な設定手順」（P.5）

方式リストとサーバ グループ

サーバ グループは、方式リストに使用する既存の Lightweight Directory Access Protocol（LDAP）、RADIUS、または TACACS+ サーバ ホストをグループ化する方法の 1 つです。図 1 に、4 台のセキュリティ サーバ（R1 と R2 は RADIUS サーバ、T1 と T2 は TACACS+ サーバ）が設置された一般的な AAA ネットワーク設定を示します。R1 と R2 で RADIUS サーバのグループを構成します。T1 と T2 で TACACS+ サーバのグループを構成します。

図 1　一般的な AAA ネットワーク設定



サーバ グループを使用して、設定したサーバ ホストのサブセットを指定し、特定のサービスに使用します。たとえば、サーバ グループを使用すると、R1 および R2 を 1 つのサーバ グループとして定義し、T1 および T2 を別のサーバ グループとして定義できます。また、認証ログインの方式リストに R1 および T1 を指定し、PPP 認証の方式リストに R2 および T2 を指定することもできます。

サーバ グループには、1 台のサーバに対して複数のホスト エントリを含めることができます。エントリごとに固有の識別情報を設定します。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。つまり、この固有識別情報を使用して、ある IP アドレスに位置する 1 台のサーバ上に複数の UDP ポートが存在する場合、それぞれの UDP ポートに対して RADIUS 要求を送信できます。1 台の RADIUS サーバ上にある異なる 2 つのホスト エントリが 1 つのサービス（認証など）に設定されている場合、設定されている 2 番めのホスト エントリは最初のホスト エントリのフェールオーバー バックアップとして動作します。この例の場合、最初のホスト エントリがアカウンティング サービスの提供に失敗すると、同じデバイスに設定されている 2 番めのホスト エントリを使用してアカウンティング サービスを提供するように、ネットワーク アクセス サーバが試行します（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

サーバ グループ設定の詳細、および Dialed Number Identification Service（DNIS）番号に基づくサーバ グループの設定については、「Configuring LDAP」、「Configuring RADIUS」、または「Configuring TACACS+」の各フィーチャ モジュールを参照してください。

方式リストの例

たとえば、システム管理者が、すべてのインターフェイスに同じ認証方式を使用して PPP 接続を認証する、というセキュリティ ソリューションを決定したとします。RADIUS グループでは、まず認証情報のために R1 に接続し、応答がない場合、R2 に接続します。R2 が応答しない場合、TACACS+ グループの T1 に接続し、T1 が応答しない場合、T2 に接続します。すべての指定したサーバが応答しなかった場合、認証はアクセス サーバ自体のローカル ユーザ名データベースで行われます。このソリューションを実装するには、システム管理者が次のコマンドを入力してデフォルトの方式リストを作成します。

```
aaa authentication ppp default group radius group tacacs+ local
```

この例では、「default」が方式リストの名前です。この方式リストにプロトコルを含める場合、名前の後に、照会される順で指定します。デフォルトのリストは、すべてのインターフェイスに自動的に適用されます。

リモート ユーザがネットワークにダイヤルインしようとすると、ネットワーク アクセス サーバは、まず R1 に認証情報を照会します。ユーザが R1 から認証されると、R1 からネットワーク アクセス サーバに対して PASS 応答が発行され、ユーザはネットワークにアクセスできるようになります。R1 から FAIL 応答が返されると、ユーザはアクセスを拒否され、セッションは終了します。R1 が応答しない場合、ネットワーク アクセス サーバでは ERROR として処理され、認証情報について R2 に照会されます。このパターンは、ユーザが認証または拒否されるか、セッションが終了するまで、残りの指定した方式について続行されます。

FAIL 応答は ERROR とまったく異なる点に注意してください。FAIL とは、適用可能な認証データベースに含まれる、認証の成功に必要な基準をユーザが満たしていないことを示します。認証は FAIL 応答で終了します。ERROR とは、認証の照会に対してサーバが応答しなかったことを示します。そのため、認証は試行されません。ERROR が検出された場合にだけ、認証方式リストに定義されている次の認証方式が AAA によって選択されます。

たとえば、システム管理者が、1 つのインターフェイス、または一部のインターフェイスにだけ方式リストを適用するとします。この場合、システム管理者は名前付き方式リストを作成し、その名前付きリストを対象のインターフェイスに適用します。次に、システム管理者が、インターフェイス 3 にだけ適用する認証方式を実装する場合の例を示します。

```
aaa authentication ppp default group radius group tacacs+ local
aaa authentication ppp apple group radius group tacacs+ local none
 interface async 3
 ppp authentication chap apple
```

この例では、「apple」が方式リストの名前です。また、この方式リストに含まれるプロトコルは、名前の後に、実行する順で指定されています。方式リストを作成すると、該当するインターフェイスに適用されます。AAA および PPP 認証コマンド両方の方式リスト名（apple）は一致する必要があります。

次の例では、システム管理者がサーバ グループを使用し、PPP 認証の場合は R2 および T2 だけが有効であることを指定します。この場合、管理者は、メンバがそれぞれ R2（172.16.2.7）と T2（172.16.2.77）であるサーバ グループを定義する必要があります。この例では、RADIUS サーバ グループ「rad2only」は **aaa group server** コマンドを使用して次のように定義されます。

```
aaa group server radius rad2only
 server 172.16.2.7
```

TACACS+ サーバ グループ「tac2only」は、**aaa group server** コマンドを使用して次のように定義されます。

```
aaa group server tacacs+ tac2only
 server 172.16.2.77
```

次に、管理者はサーバ グループを使用して PPP 認証を適用します。この例では、PPP 認証のデフォルト方式リストは、**group rad2only**、**group tac2only**、および **local** の順です。

```
aaa authentication ppp default group rad2only group tac2only local
```

AAA 認証の一般的な設定手順

AAA 認証を設定するには、次のタスクを実行します。

1. グローバル コンフィギュレーション モードで **aaa new-model** コマンドを使用して AAA をイネーブルにします。
2. セキュリティ サーバを使用している場合、RADIUS、TACACS+、Kerberos など、セキュリティ プロトコル パラメータを設定します。詳細については、それぞれ「Configuring RADIUS」、「Configuring TACACS+」、および「Configuring Kerberos」を参照してください。
3. 認証の方式リストを定義するには、AAA 認証コマンドを使用します。
4. 必要に応じて、方式リストを特定のインターフェイスまたは回線に適用します。

RADIUS Change of Authorization

標準 RADIUS インターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、クエリーが送信されたサーバが応答するプル モデルで使用されます。Cisco IOS スイッチは、RFC 5176 で定義された RADIUS Change of Authorization（CoA; 認可変更）拡張をサポートします。RFC 5176 は通常、プッシュ モデルで使用され、外部の Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）またはポリシー サーバからのセッションの動的な再設定を可能にします。

Cisco IOS Release 12.2(5) SXI 以降、次のセッションごとの CoA 要求がサポートされます。

- セッションの再認証
- セッションの終了
- ポートをシャットダウンするセッションの終了
- ポート バウンスを伴うセッションの終了
- セキュリティとパスワード：詳細については、「Configuring Security with Passwords, Privilege Levels, and Login Usernames for CLI Sessions on Networking Devices」フィーチャ モジュールを参照してください。
- アカウンティング：詳細については、「Configuring Accounting」フィーチャ モジュールを参照してください。

ここでは、RADIUS CoA メッセージングの機能について説明します。

- 「Change-of-Authorization 要求」（P.5）
- 「CoA 要求の応答コード」（P.7）
- 「CoA 要求コマンド」（P.8）
- 「セッションの再認証」（P.8）

Change-of-Authorization 要求

Change of Authorization（CoA; 認可変更）要求は、RFC 5176 で説明されているようにプッシュ モデルで使用され、セッションの識別、ホストの再認証、およびセッションの終了を可能にします。モデルは、1 つの要求（CoA-Request）および次の使用可能な 2 つの応答コードで構成されています。

- CoA 確認応答（ACK）[CoA-ACK]

- CoA 否定確認応答（NAK）[CoA-NAK]

要求は CoA クライアント（通常は RADIUS またはポリシー サーバ）から開始され、リスナーとして動作するルータに転送されます。

RFC 5176 準拠

Disconnect Request メッセージ（Packet of Disconnect（POD; パケット オブ ディスコネクト）とも呼ばれる）は、セッションの終了のためにルータでサポートされています。

表 1 に、この機能でサポートされる IETF アトリビュートを示します。

表 1　サポートされる IETF アトリビュート

アトリビュート番号	アトリビュート名
24	State
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

表 2 に、Error-Cause アトリビュートの値を示します。

表 2　Error-Cause 値

値	説明
201	残りのセッションのコンテキストが削除されました
202	EAP パケットが無効です（無視）
401	サポートされていないアトリビュート
402	存在しないアトリビュート
403	NAS ID の不一致
404	無効な要求
405	サポートされていないサービス
406	サポートされていない拡張子
407	無効なアトリビュート値
501	管理的に禁止されています
502	要求はルート不可能です（プロキシ）
503	セッション コンテキストが見つかりません
504	セッション コンテキストを削除できません
505	他のプロキシの処理エラー
506	使用できないリソース
507	要件が開始されました
508	複数セッションの選択はサポートされていません

CoA 要求の応答コード

CoA 要求の応答コードは、ルータへコマンドを発行するために使用されます。表 3（P.8）に、サポートされているコマンドが記載されています。

セッション ID

特定のセッションに対する接続解除および CoA 要求の場合、ルータは次の 1 つまたは複数のアトリビュートに基づいてセッションを検出します。

- Calling-Station-Id（ホストの MAC アドレスを含む IETF アトリビュート 31 番）
- Audit-Session-Id（Cisco VSA）
- Acct-Session-Id（IETF アトリビュート 44 番）

CoA メッセージに含まれるすべてのセッション ID アトリビュートがそのセッションと一致しないかぎり、ルータは「Invalid Attribute Value」エラーコード アトリビュートを含む Disconnect-NAK または CoA-NAK を返します。

特定のセッションに対する接続解除または CoA 要求の場合、次のいずれかのセッション ID を使用できます。

- Calling-Station-ID（MAC アドレスを含む IETF アトリビュート 31 番）
- Audit-Session-ID（シスコのベンダー固有のアトリビュート）
- Accounting-Session-ID（IETF アトリビュート 44 番）

メッセージに複数のセッション ID アトリビュートが含まれる場合、すべてのアトリビュートがセッションと一致する必要があります。一致しない場合は、ルータが「Invalid Attribute Value」エラーコードを含む Disconnect-Negative Acknowledgement（NAK; 否定確認応答）または CoA-NAK を返します。

CoA ACK 応答コード

許可ステートが正常に変更された場合、肯定確認応答（ACK）が送信されます。CoA ACK 内で返されたアトリビュートは CoA 要求によって異なります。それらについては個々の CoA コマンドで説明します。

RFC 5176 の定義に従って CoA 要求コードのパケット形式は Type:Length:Value（TLV）フォーマットで、コード、ID、長さ、オーセンティケータ、およびアトリビュートのフィールドで構成されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     コード     |       ID      |             長さ              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                         オーセンティケータ                    |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  アトリビュート ...
+-+-+-+-+-+-+-+-+-+-+-+-+-
```

アトリビュート フィールドは Cisco VSA を伝送するために使用されます。

CoA NAK 応答コード

否定確認応答（NAK）は、許可ステートの変更が失敗したことを示し、失敗の理由を示すアトリビュートが含まれます。

CoA 要求コマンド

ここでは、次の内容について説明します。

- 「セッションの再認証」
- 「セッションの終了」
- 「CoA 要求：Disable Host Port」
- 「CoA 要求：Bounce-Port」

ルータは表 3 に示すコマンドをサポートします。

表 3　ルータでサポートされる CoA コマンド

コマンド[1]	Cisco VSA
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	VSA を必要としない標準の接続解除要求です
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"

1. すべての CoA コマンドでは、ルータと CoA クライアント間のセッション ID を指定する必要があります。

セッションの再認証

セッションの認証を開始するには、AAA サーバが次の形式でシスコ ベンダー固有のアトリビュート（VSA）を含む標準の CoA-Request メッセージを送信します。
Cisco:Avpair="subscriber:command=reauthenticate" および 1 つまたは複数のセッション ID アトリビュート

次のシナリオでは、現在のセッション状態によって、メッセージに対するルータの応答が決まります。

- セッションが現在、IEEE 802.1x によって認証されている場合、ルータは EAPoL[1] -RequestId メッセージ（下記の脚注 1 を参照）をサーバに送信することで応答します。
- セッションが現在 MAC 認証バイパス（MAB）によって認証されている場合、ルータはアクセス要求をサーバに送信し、最初に成功した認証で使用したのと同じ ID アトリビュートを渡します。
- ルータがコマンドを受信する際にセッションの認証が行われている場合、ルータはプロセスを終了し、認証シーケンスを再起動して、最初に試行されるように設定された方式を開始します。

セッションの終了

CoA Disconnect-Request コマンドは、ホスト ポートをディセーブルにせずにセッションを終了します。このコマンドによって、指定したホストのオーセンティケータ ステート マシンが再初期化されますが、ホストからネットワークに対するアクセスは制限されません。セッションを検出できない場合、ルータは「Session Context Not Found」エラー コード アトリビュートを含む Disconnect-NAK メッセージを返します。セッションが検出された場合、ルータはセッションを終了します。セッションが完全に削除された後、ルータは Disconnect-ACK を返します。

1. Extensible Authentication Protocol over LAN

ホストのネットワークへのアクセスを制限するには、Cisco:Avpair="subscriber:command=disable-host-port" VSA を含む CoA 要求を使用します。このコマンドは、ホストがネットワーク上で問題を起こしていることを把握し、ホストのネットワーク アクセスを即座にブロックする必要がある場合に便利です。ポート上のネットワーク アクセスを復元する場合は、RADIUS 以外のメカニズムを使用して再度イネーブルにします。

CoA 要求：Disable Host Port

RADIUS サーバの CoA disable port コマンドを実行すると、セッションをホストしている認証ポートが管理的にシャットダウンされます。その結果、セッションは終了します。このコマンドは、次の新しい VSA を含む標準の CoA-Request メッセージで伝達されます。

Cisco:Avpair="subscriber:command=disable-host-port"

このコマンドはセッションに対して実行するため、「セッション ID」（P.7）に記載されているセッション ID アトリビュートを 1 つまたは複数使用する必要があります。ルータを検出できない場合、「Session Context Not Found」エラー コード アトリビュートを含む CoA-NAK メッセージを返します。ルータがセッションを特定すると、ホスティング ポートをディセーブルにし、CoA-ACK メッセージを返します。

CoA-ACK がクライアントに返される前にルータに障害が発生した場合、クライアントからの要求が再送信されると、新しいアクティブ スイッチでプロセスが繰り返されます。CoA-ACK メッセージがクライアントに返された後、動作が完了する前にルータに障害が発生した場合、新しいアクティブ ルータで動作が繰り返されます。

RADIUS サーバの CoA disable port コマンドを無視する必要がある場合、詳細については「bounce および disable RADIUS CoA 要求を無視するためのルータの設定」（P.36）を参照してください。

CoA 要求：Bounce-Port

RADIUS サーバの CoA bounce port コマンドが RADIUS サーバから送信されると、認証ポートでリンクのフラップが発生します。その結果、このポートに接続している 1 つまたは複数のホストから、DHCP の再ネゴシエーションが開始されます。この状況は、VLAN の変更があり、この認証ポートに関する変化を検出するメカニズムがないデバイス（プリンタなど）がエンドポイントの場合に発生する可能性があります。CoA bounce port コマンドは、次の新しい VSA を含む標準の CoA-Request メッセージで伝達されます。

Cisco:Avpair="subscriber:command=bounce-host-port"

このコマンドはセッションに対して実行するため、「セッション ID」（P.7）に記載されているセッション ID アトリビュートを 1 つまたは複数使用する必要があります。セッションを検出できない場合、ルータは「Session Context Not Found」エラー コード アトリビュートを含む CoA-NAK メッセージを返します。セッションが検出された場合、ルータはホスト ポートを 10 秒間ディセーブルにし、ポートバウンスを再度イネーブルにして CoA-ACK を返します。

RADIUS サーバの CoA bounce port コマンドを無視する必要がある場合、詳細については「bounce および disable RADIUS CoA 要求を無視するためのルータの設定」（P.36）を参照してください。

AAA 認証方式を設定する方法

ここでは、次の AAA 認証方式について説明します。

（注） **aaa new-model** コマンドを発行して AAA をグローバルにイネーブルにするまで、AAA 機能は使用できません。

AAA を使用したログイン認証の設定

AAA セキュリティ サービスにより、さまざまなログイン認証方式を容易に実行できるようになります。使用するように指定したサポート対象のログイン認証方式には関係なく AAA 認証をイネーブルにするには、**aaa authentication login** コマンドを使用します。**aaa authentication login** コマンドを使用すると、ログイン時に試行する認証方式リストを 1 つ以上作成できます。これらのリストは、**login authentication line** コマンドによって適用されます。

AAA を使用してログイン認証を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# aaa new-model`	AAA をグローバルにイネーブルにします。
ステップ 2	`Router(config)# aaa authentication login {default | list-name} method1 [method2...]`	ローカルな認証リストを作成します。
ステップ 3	`Router(config)# line [aux | console | tty | vty] line-number [ending-line-number]`	認証リストを適用する回線について、ライン コンフィギュレーション モードを開始します。
ステップ 4	`Router(config-line)# login authentication {default | list-name}`	1 つの回線または複数回線に認証リストを適用します。

list-name は、作成するリストを指定するときに使用される名前で、文字列を使用できます。method 引数は、認証アルゴリズムが試行する実際の方式を指します。追加の認証方式は、直前の方式で（失敗した場合ではなく）エラーが返された場合にだけ使用されます。すべての方式でエラーが返されても引き続き認証を行うように指定するには、コマンドラインの最後の方式として **none** を指定します。

たとえば、（この例では）LDAP サーバでエラーが返されても引き続き認証を行うように指定するには、次のコマンドを入力します。

```
aaa authentication login default group ldap none
```

たとえば、（この例では）TACACS+ サーバでエラーが返されても引き続き認証を行うように指定するには、次のコマンドを入力します。

```
aaa authentication login default group tacacs+ none
```

（注） **none** キーワードを指定すると、*すべてのユーザ*がログイン認証に成功するため、認証のバックアップ方式としてだけ使用してください。

名前付きリストが **login authentication** コマンドで指定されて*いない*場合に使用するデフォルト リストを作成するには、**default** キーワードの後に、デフォルトの状況で使用する方式を指定します。デフォルトの方式リストは、すべてのインターフェイスに自動的に適用されます。

たとえば、ログイン時のユーザ認証のデフォルト方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa authentication login default group radius
```

表 4 に、サポートされるログイン認証方式を示します。

表 4　AAA 認証ログイン方式

キーワード	説明
`enable`	認証にイネーブル パスワードを使用します。
`krb5`	認証に Kerberos 5 を使用します。
`krb5-telnet`	ルータへの接続に Telnet を使用する場合、Kerberos 5 Telnet 認証プロトコルを使用します。このキーワードを選択する場合、方式リストの最初の方式としてこのキーワードを指定する必要があります。
`line`	認証にライン パスワードを使用します。
`local`	認証にローカルなユーザ名データベースを使用します。
`local-case`	認証に大文字と小文字が区別されるローカルなユーザ名を使用します。
`none`	認証を使用しません。
`group ldap`	認証にすべての LDAP サーバのリストを使用します。
`group radius`	認証にすべての RADIUS サーバのリストを使用します。
`group tacacs+`	認証にすべての TACACS+ サーバのリストを使用します。
`group` *`group-name`*	認証に **aaa group server radius** コマンドまたは **aaa group server tacacs+** コマンドで定義された RADIUS サーバまたは TACACS+ サーバのサブセットを使用します。

（注） **login** コマンドではユーザ名と特権レベルが変更されるだけで、シェルは実行されません。そのため、autocommand は実行されません。この状況で autocommand を実行するには、Telnet セッションをルータに復帰（ループバック）させる必要があります。この方法で autocommand 機能を実装する場合は、ルータがセキュアな Telnet セッションを使用するように設定されていることを確認してください。

ここでは、次の内容について説明します。

- 「期限切れのユーザ名が指定されたアクセス要求が RADIUS サーバに送信されないようにする」（P.12）
- 「イネーブル パスワードによるログイン認証」（P.13）
- 「Kerberos によるログイン認証」（P.13）

- 「ライン パスワードによるログイン認証」（P.14）
- 「ローカル パスワードによるログイン認証」（P.14）
- 「group LDAP によるログイン認証」（P.14）
- 「group RADIUS によるログイン認証」（P.14）
- 「group tacacs+ によるログイン認証」（P.15）
- 「group group-name によるログイン認証」（P.15）

期限切れのユーザ名が指定されたアクセス要求が RADIUS サーバに送信されないようにする

次のタスクを使用して、期限切れのユーザ名が指定されたアクセス要求が RADIUS サーバに送信されないようにします。RADIUS サーバから Easy VPN クライアントに対して、パスワードが期限切れになったことが通知されます。パスワードの期限切れ機能は、ユーザがパスワードを変更する一般的な方法としても利用できます。

（注） パスワードの期限切れ機能を有効にするには、**radius-server vsa send authentication** コマンドを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** {**default** | *list-name*} **passwd-expiry** *method1* [*method2...*]
5. **radius-server vsa send authentication**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	`enable`
	
	例：
	`Router> enable`
		特権 EXEC モードをイネーブルにします。
		• プロンプトが表示されたら、パスワードを入力します。

ステップ 2	`configure terminal`
	
	例：
	`Router# configure terminal`
		グローバル コンフィギュレーション モードを開始します。

ステップ 3	`aaa new-model`
	
	例：
	`Router(config)# aaa new-model`
		AAA をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**aaa authentication login** {**default** | *list-name*} **passwd-expiry** *method1* [*method2...*] 例： `Router(config)# aaa authentication login userauthen passwd-expiry group radius`	**default** キーワードでは、ユーザがログインするときのデフォルトの方式リストとして、このキーワードに続くリストの認証方式が使用されます。 *list-name* 引数は、ユーザがログインするときにアクティブ化される認証方式リストに、名前を付けるときに使用する文字列です。 **password-expiry** キーワードを指定すると、ローカル認証リストでパスワードのエージング処理がイネーブルになります。 *method* 引数には、そのシーケンスで認証アルゴリズムが試行する方式リストを指定します。1 つ以上の方式を入力する必要があります。また最高 4 つの方式を入力できます。 この例では、クリプト クライアントで AAA を使用して、パスワードのエージングを設定しています。
ステップ 5	**radius-server vsa send authentication** 例： `Router(config)# radius-server vsa send authentication`	アクセス要求でのベンダー固有アトリビュートの送信

イネーブル パスワードによるログイン認証

ログイン認証方式としてイネーブル パスワードを指定するには、**enable** キーワードを指定して **aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式としてイネーブル パスワードを指定するには、次のコマンドを入力します。

```
aaa authentication login default enable
```

ログイン認証方式としてイネーブル パスワードを使用するには、イネーブル パスワードを定義しておく必要があります。イネーブル パスワードの定義の詳細については、「Configuring Passwords and Privileges」を参照してください。

Kerberos によるログイン認証

Kerberos による認証は、他のほとんどの認証方式とは異なり、ユーザのパスワードはリモート アクセス サーバに送信されません。ネットワークにログインするリモート ユーザは、ユーザ名の指定を求められます。Key Distribution Center（KDC; キー発行局）にそのユーザのエントリがある場合、そのユーザのパスワードを含む暗号化された Ticket Granting Ticket（TGT; チケット認可チケット）が作成され、ルータに返送されます。次に、ユーザにパスワードの入力が求められ、ルータではそのパスワードを含む TGT の復号化が試行されます。復号化に成功すると、ユーザは認証され、ルータ上にあるユーザのクレデンシャル キャッシュに TGT が保存されます。

krb5 は KINIT プログラムを使用しませんが、ルータに対して認証するために、ユーザが KINIT プログラムを実行して TGT を取得する必要はありません。これは、Cisco IOS の Kerberos 実装のログイン手順に KINIT が統合されているためです。

ログイン認証方式として Kerberos を指定するには、**krb5** キーワードを指定して **aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式として Kerberos を指定するには、次のコマンドを入力します。

```
aaa authentication login default krb5
```

ログイン認証方式として Kerberos を使用するには、Kerberos セキュリティ サーバとの通信をイネーブルにしておく必要があります。Kerberos サーバとの通信を確立する方法の詳細については、「Configuring Kerberos」を参照してください。

ライン パスワードによるログイン認証

ログイン認証方式としてライン パスワードを指定するには、**line** キーワードを指定して **aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式としてライン パスワードを指定するには、次のコマンドを入力します。

```
aaa authentication login default line
```

ログイン認証方式としてライン パスワードを使用するには、ライン パスワードを定義しておく必要があります。ライン パスワードの定義の詳細については、「ライン パスワード保護の設定」（P.37）を参照してください。

ローカル パスワードによるログイン認証

Cisco ルータまたはアクセス サーバが認証にローカル ユーザ名データベースを使用するように指定するには、**local** キーワードを指定して **aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式としてローカル ユーザ名データベースを指定するには、次のコマンドを入力します。

```
aaa authentication login default local
```

ユーザをローカルなユーザ名データベースに追加する方法の詳細については、「ユーザ名認証の確立」（P.38）を参照してください。

group LDAP によるログイン認証

ログイン認証方式として ldap を指定するには、**group ldap** 方式を指定して **aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式として ldap を指定するには、次のコマンドを入力します。

```
aaa authentication login default group ldap
```

group RADIUS によるログイン認証

ログイン認証方式として RADIUS を指定するには、**group radius** 方式を指定して **aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa authentication login default group radius
```

ログイン認証方式として RADIUS を使用するには、RADIUS セキュリティ サーバとの通信をイネーブルにしておく必要があります。RADIUS サーバとの通信を確立する方法の詳細については、「Configuring RADIUS」を参照してください。

アクセス要求での RADIUS アトリビュート 8 の設定

aaa authentication login コマンドを使用して RADIUS を指定し、NAS から IP アドレスを要求するようにログイン ホストを設定すると、グローバル コンフィギュレーション モードで **radius-server attribute 8 include-in-access-req** コマンドを使用して、access-request パケットでアトリビュート 8

（Framed-IP-Address）を送信できます。このコマンドによって、ユーザ認証の前に、NAS から RADIUS サーバに対してユーザ IP アドレスのヒントを提供できます。アトリビュート 8 の詳細については、巻末の付録「RADIUS アトリビュート」を参照してください。

group tacacs+ によるログイン認証

ログイン認証方式として TACACS+ を指定するには、**group tacacs+** 方式を指定して **aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式として TACACS+ を指定するには、次のコマンドを入力します。

```
aaa authentication login default group tacacs+
```

ログイン認証方式として TACACS+ を使用するには、TACACS+ セキュリティ サーバとの通信をイネーブルにしておく必要があります。TACACS+ サーバとの通信を確立する方法の詳細については、「Configuring TACACS+」を参照してください。

group group-name によるログイン認証

ログイン認証方式として使用する LDAP、RADIUS、または TACACS+ サーバのサブセットを指定するには、**group** *group-name* 方式を指定して **aaa authentication login** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**loginrad** というグループ（**group**）のメンバを最初に定義します。

```
aaa group server radius loginrad
 server 172.16.2.3
 server 172.16.2 17
 server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバがグループ *loginrad* のメンバとして指定されます。

他の方式リストが定義されていない場合にログイン時のユーザ認証方式として **group loginrad** を指定するには、次のコマンドを入力します。

```
aaa authentication login default group loginrad
```

ログイン認証方式としてグループ名を使用するには、RADIUS または TACACS+ セキュリティ サーバとの通信をイネーブルにしておく必要があります。RADIUS サーバとの通信を確立する方法の詳細については、「Configuring RADIUS」を参照してください。TACACS+ サーバとの通信を確立する方法の詳細については、「Configuring TACACS+」を参照してください。

AAA を使用した ppp 認証の設定

多くのユーザは、async または ISDN を介したダイヤルアップでネットワーク アクセス サーバにアクセスします。async または ISDN を介したダイヤルアップは、CLI を完全にバイパスします。その代わり、接続が確立するとすぐにネットワーク プロトコル（PPP や ARA など）が開始されます。

AAA セキュリティ サービスにより、PPP を実行するシリアル インターフェイスに使用できるさまざまな認証方式の実行が容易になります。使用するように指定したサポート対象の PPP 認証方式には関係なく AAA 認証をイネーブルにするには、**aaa authentication ppp** コマンドを使用します。

PPP を使用してシリアル回線に AAA 認証方式を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router(config)# **aaa new-model**	AAA をグローバルにイネーブルにします。
ステップ 2	Router(config)# **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]	ローカルな認証リストを作成します。
ステップ 3	Router(config)# **interface** *interface-type interface-number*	認証リストを適用するインターフェイスについて、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	Router(config-if)# **ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] {**default** | *list-name*} [**callin**][**one-time**][**optional**]	1 つの回線または複数回線に認証リストを適用します。このコマンドの *protocol1* と *protocol2* は、CHAP、MS-CHAP、および PAP のプロトコルを示します。PPP 認証は、まず *protocol1* に指定された最初の認証方式を使用して試行されます。認証に *protocol1* を使用できない場合は、次に設定されているプロトコルを使用して認証のネゴシエーションを行います。

aaa authentication ppp コマンドを使用して、PPP を介して認証を試行するときに使用する認証方式のリストを 1 つまたは複数作成します。これらのリストは、**ppp authentication** ライン コンフィギュレーション コマンドによって適用されます。

名前付きリストが **ppp authentication** コマンドで指定されて*いない*場合に使用するデフォルト リストを作成するには、**default** キーワードの後に、デフォルトの状況で使用する方式を指定します。

たとえば、ユーザ認証のデフォルト方式としてローカル ユーザ名データベースを指定するには、次のコマンドを入力します。

```
aaa authentication ppp default local
```

list-name は、作成するリストを指定するときに使用される名前で、任意の文字列を使用できます。method 引数は、認証アルゴリズムが試行する実際の方式を指します。追加の認証方式は、直前の方式で（失敗した場合ではなく）エラーが返された場合にだけ使用されます。すべての方式でエラーが返されても引き続き認証を行うように指定するには、コマンドラインの最後の方式として **none** を指定します。

たとえば、（この例では）TACACS+ サーバでエラーが返されても引き続き認証を行うように指定するには、次のコマンドを入力します。

```
aaa authentication ppp default group tacacs+ none
```

（注） **none** を指定するとすべてのユーザが認証に成功してログインできるようになるため、認証のバックアップ方式として使用する必要があります。

表 5 に、サポートされるログイン認証方式を示します。

表 5　AAA 認証 PPP 方式

キーワード	説明
if-needed	ユーザが TTY 回線で認証済みの場合、認証しません。
krb5	認証に Kerberos 5 を使用します（PAP 認証にだけ使用できます）。
local	認証にローカルなユーザ名データベースを使用します。
local-case	認証に大文字と小文字が区別されるローカルなユーザ名を使用します。
none	認証を使用しません。

表 5　AAA 認証 PPP 方式（続き）

キーワード	説明
group radius	認証にすべての RADIUS サーバのリストを使用します。
group tacacs+	認証にすべての TACACS+ サーバのリストを使用します。
group *group-name*	認証に **aaa group server radius** コマンドまたは **aaa group server tacacs+** コマンドで定義された RADIUS サーバまたは TACACS+ サーバのサブセットを使用します。

ここでは、次の内容について説明します。

- 「Kerberos による PPP 認証」（P.17）
- 「ローカル パスワードによる PPP 認証」（P.17）
- 「group RADIUS による PPP 認証」（P.17）
- 「group TACACS+ による PPP 認証」（P.18）
- 「group group-name による PPP 認証」（P.18）

Kerberos による PPP 認証

PPP を実行するインターフェイスで使用する認証方式として Kerberos を指定するには、**krb5** *method* キーワードを指定して **aaa authentication ppp** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にユーザ認証方式として Kerberos を指定するには、次のコマンドを入力します。

```
aaa authentication ppp default krb5
```

PPP 認証方式として Kerberos を使用するには、Kerberos セキュリティ サーバとの通信をイネーブルにしておく必要があります。Kerberos サーバとの通信を確立する方法の詳細については、「Configuring Kerberos」を参照してください。

（注）　Kerberos ログイン認証は、PPP PAP 認証とだけ連携します。

ローカル パスワードによる PPP 認証

Cisco ルータまたはアクセス サーバが認証にローカル ユーザ名データベースを使用するように指定するには、*method* キーワード **local** を指定して **aaa authentication ppp** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、PPP を実行する回線に使用するユーザ認証方式としてローカル ユーザ名データベースを指定するには、次のコマンドを入力します。

```
aaa authentication ppp default local
```

ユーザをローカルなユーザ名データベースに追加する方法の詳細については、「ユーザ名認証の確立」（P.38）を参照してください。

group RADIUS による PPP 認証

ログイン認証方式として RADIUS を指定するには、**group radius** *method* を指定して **aaa authentication ppp** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa authentication ppp default group radius
```

PPP 認証方式として RADIUS を使用するには、RADIUS セキュリティ サーバとの通信をイネーブルにしておく必要があります。RADIUS サーバとの通信を確立する方法の詳細については、「Configuring RADIUS」を参照してください。

アクセス要求での RADIUS アトリビュート 44 の設定

group radius *method* を指定して **aaa authentication ppp** コマンドを使用し、ログイン認証方式として RADIUS を使用すると、グローバル コンフィギュレーション モードで **radius-server attribute 44 include-in-access-req** コマンドを使用して access-request パケットでアトリビュート 44（Acct-Session-ID）を送信するようにルータを設定できます。このコマンドによって、RADIUS デーモンはコールの開始から終了までコールを追跡できます。アトリビュート 44 の詳細については、巻末の付録「RADIUS アトリビュート」を参照してください。

group TACACS+ による PPP 認証

ログイン認証方式として TACACS+ を指定するには、**group tacacs+** *method* を指定して **aaa authentication ppp** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式として TACACS+ を指定するには、次のコマンドを入力します。

```
aaa authentication ppp default group tacacs+
```

PPP 認証方式として TACACS+ を使用するには、TACACS+ セキュリティ サーバとの通信をイネーブルにしておく必要があります。TACACS+ サーバとの通信を確立する方法の詳細については、「Configuring TACACS+」を参照してください。

group group-name による PPP 認証

ログイン認証方式として使用する RADIUS または TACACS+ サーバのサブセットを指定するには、**group** *group-name* 方式を指定して **aaa authentication ppp** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**ppprad** というグループ（**group**）のメンバを最初に定義します。

```
aaa group server radius ppprad
 server 172.16.2.3
 server 172.16.2 17
 server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバがグループ *ppprad* のメンバとして指定されます。

他の方式リストが定義されていない場合にログイン時のユーザ認証方式として **group ppprad** を指定するには、次のコマンドを入力します。

```
aaa authentication ppp default group ppprad
```

PPP 認証方式としてグループ名を使用するには、RADIUS または TACACS+ セキュリティ サーバとの通信をイネーブルにしておく必要があります。RADIUS サーバとの通信を確立する方法の詳細については、「Configuring RADIUS」を参照してください。TACACS+ サーバとの通信を確立する方法の詳細については、「Configuring TACACS+」を参照してください。

PPP 要求に対する AAA スケーラビリティの設定

Network Access Server（NAS; ネットワーク アクセス サーバ）の PPP マネージャによって割り当てられた複数のバックグラウンド プロセスを設定およびモニタして、AAA 認証要求と認可要求に対応できます。以前の Cisco IOS リリースでは、PPP に対するすべての AAA 要求を処理するために、1 つのバックグラウンド プロセスだけが割り当てられていました。つまり、AAA サーバの並行処理は、完全には使用できませんでした。AAA スケーラビリティ機能によって、PPP に対する AAA 要求を処理するために使用される複数のプロセスを設定できるようになります。つまり、同時に認証または認可できるユーザ数が増えます。

PPP に対する AAA 要求を処理するために、特定の数のバックグラウンド プロセスを割り当てるには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# aaa processes number`	PPP に対する AAA 認証要求および認可要求を処理するために、特定の数のバックグラウンド プロセスを割り当てます。

引数 *number* には、PPP に対する AAA 認証要求と認可要求を処理するために確保するバックグラウンド プロセス数を定義します。また、1 ～ 2147483647 の任意の値を設定できます。PPP マネージャが PPP に対する要求を処理する方法のため、この引数には、同時に認証できる新規ユーザの数も定義します。この引数は、いつでも増減できます。

（注） 追加バックグラウンド プロセスの割り当ては、コストが高くなる可能性があります。PPP に対する AAA 要求を処理できるバックグラウンド プロセスの最小数を設定してください。

AAA を使用した ARAP 認証の設定

aaa authentication arap コマンドを使用して、AppleTalk Remote Access Protocol（ARAP）ユーザがルータにログインを試行するときに使用する認証方式のリストを 1 つまたは複数作成します。これらのリストは、**arap authentication** ライン コンフィギュレーション コマンドで使用されます。

グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# aaa new-model`	AAA をグローバルにイネーブルにします。
ステップ 2	`Router(config)# aaa authentication arap {default | list-name} method1 [method2...]`	ARAP ユーザに対する認証をイネーブルにします。
ステップ 3	`Router(config)# line number`	（任意）ライン コンフィギュレーション モードに変更します。
ステップ 4	`Router(config-line)# autoselect arap`	（任意）ARAP の自動選択をイネーブルにします。
ステップ 5	`Router(config-line)# autoselect during-login`	（任意）ユーザ ログイン時に ARAP セッションを自動的に開始します。
ステップ 6	`Router(config-line)# arap authentication list-name`	（任意 : **default** が **aaa authentication arap** コマンドに使用されている場合は不要）回線上の ARAP に対する TACACS+ 認証をイネーブルにします。

list-name は、作成するリストを指定するときに使用される名前で、任意の文字列を使用できます。方式の引数は、認証アルゴリズムが試行する方式の実際のリストを指します。試行は入力されている順序で行われます。

名前付きリストが **arap authentication** コマンドで指定されて*いない*場合に使用するデフォルト リストを作成するには、**default** キーワードの後に、デフォルトの状況で使用する方式を指定します。

追加の認証方式は、直前の方式で（失敗した場合ではなく）エラーが返された場合にだけ使用されます。すべての方式でエラーが返されても引き続き認証を行うように指定するには、コマンドラインの最後の方式として **none** を指定します。

（注） **none** を指定するとすべてのユーザが認証に成功してログインできるようになるため、認証のバックアップ方式として使用する必要があります。

表 6 に、サポートされるログイン認証方式を示します。

表 6　AAA 認証 ARAP 方式

キーワード	説明
auth-guest	ユーザが EXEC にログイン済みの場合にだけ、ゲスト ログインを許可します。
guest	ゲスト ログインを許可します。
line	認証にライン パスワードを使用します。
local	認証にローカルなユーザ名データベースを使用します。
local-case	認証に大文字と小文字が区別されるローカルなユーザ名を使用します。
group radius	認証にすべての RADIUS サーバのリストを使用します。
group tacacs+	認証にすべての TACACS+ サーバのリストを使用します。
group *group-name*	認証に **aaa group server radius** コマンドまたは **aaa group server tacacs+** コマンドで定義された RADIUS サーバまたは TACACS+ サーバのサブセットを使用します。

たとえば、ARAP とともに使用するデフォルトの AAA 認証方式リストを作成するには、次のコマンドを入力します。

```
aaa authentication arap default if-needed none
```

ARAP に同じ認証方式リストを作成し、リストに *MIS-access と名前を付けるには*、次のコマンドを入力します。

```
aaa authentication arap MIS-access if-needed none
```

ここでは、次の内容について説明します。

- 「認可済みゲスト ログインを許可する ARAP 認証」（P.21）
- 「ゲスト ログインを許可する ARAP 認証」（P.21）
- 「ライン パスワードによる ARAP 認証」（P.21）
- 「ローカル パスワードによる ARAP 認証」（P.21）
- 「group RADIUS による ARAP 認証」（P.22）
- 「group TACACS+ による ARAP 認証」（P.22）
- 「group group-name による ARAP 認証」（P.22）

認可済みゲスト ログインを許可する ARAP 認証

ユーザが EXEC にログイン済みの場合にだけ、ゲスト ログインを許可するには、**auth-guest** キーワードを指定して **aaa authentication arap** コマンドを使用します。この方式は ARAP 認証方式リストの先頭に指定する必要がありますが、この方式が成功しなかった場合は引き続き他の方式を試行できます。たとえば、認証のデフォルト方式として、すべての認可済みゲスト ログイン（つまり、EXEC にログイン済みのユーザによるログイン）を許可し、その方式が失敗した場合にだけ RADIUS を使用するには、次のコマンドを入力します。

```
aaa authentication arap default auth-guest group radius
```

ARAP の認可済みゲスト ログインの詳細については、『*Cisco IOS AppleTalk and Novell IPX Configuration Guide*』の「Configuring AppleTalk」の章を参照してください。

（注） AAA を初期化すると、デフォルトで ARAP によるゲスト ログインはディセーブルになります。ゲスト ログインを許可するには、**guest** キーワードまたは **auth-guest** キーワードを指定して **aaa authentication arap** コマンドを使用する必要があります。

ゲスト ログインを許可する ARAP 認証

ゲスト ログインを許可するには、**guest** キーワードを指定して **aaa authentication arap** コマンドを使用します。この方式は ARAP 認証方式リストの先頭に指定する必要がありますが、この方式が成功しなかった場合は引き続き他の方式を試行できます。たとえば、認証のデフォルト方式としてすべてのゲスト ログインを許可し、その方式が失敗した場合にだけ RADIUS を使用するには、次のコマンドを入力します。

```
aaa authentication arap default guest group radius
```

ARAP のゲスト ログインの詳細については、『*Cisco* IOS AppleTalk and Novell IPX Configuration Guide』の「Configuring AppleTalk」の章を参照してください。

ライン パスワードによる ARAP 認証

認証方式としてライン パスワードを指定するには、*method* キーワード **line** を指定して **aaa authentication arap** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、ARAP ユーザ認証方式としてライン パスワードを指定するには、次のコマンドを入力します。

```
aaa authentication arap default line
```

ARAP 認証方式としてライン パスワードを使用するには、ライン パスワードを定義しておく必要があります。ライン パスワードの定義の詳細については、「ライン パスワード保護の設定」（P.37）を参照してください。

ローカル パスワードによる ARAP 認証

Cisco ルータまたはアクセス サーバが認証にローカル ユーザ名データベースを使用するように指定するには、*method* キーワード **local** を指定して **aaa authentication arap** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、ARAP ユーザ認証方式としてローカル ユーザ名データベースを指定するには、次のコマンドを入力します。

```
aaa authentication arap default local
```

ローカル ユーザ名データベースにユーザを追加する方法については、「ユーザ名認証の確立」（P.38）を参照してください。

group RADIUS による ARAP 認証

ARAP 認証方式として RADIUS を指定するには、**group radius** *method* を指定して **aaa authentication arap** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa authentication arap default group radius
```

ARAP 認証方式として RADIUS を使用するには、RADIUS セキュリティ サーバとの通信をイネーブルにしておく必要があります。

group TACACS+ による ARAP 認証

ARAP 認証方式として TACACS+ を指定するには、**group** *tacacs+* method を指定して **aaa authentication arap** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式として TACACS+ を指定するには、次のコマンドを入力します。

```
aaa authentication arap default group tacacs+
```

ARAP 認証方式として TACACS+ を使用するには、TACACS+ セキュリティ サーバとの通信をイネーブルにしておく必要があります。TACACS+ サーバとの通信を確立する方法の詳細については、「Configuring TACACS+」を参照してください。

group group-name による ARAP 認証

ARAP 認証方式として使用する RADIUS または TACACS+ サーバのサブセットを指定するには、**group** *group-name* 方式を指定して **aaa authentication arap** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**araprad** というグループ（**group**）のメンバを最初に定義します。

```
aaa group server radius araprad
 server 172.16.2.3
 server 172.16.2 17
 server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバがグループ *araprad* のメンバとして指定されます。

他の方式リストが定義されていない場合にログイン時のユーザ認証方式として **group araprad** を指定するには、次のコマンドを入力します。

```
aaa authentication arap default group araprad
```

ARAP 認証方式としてグループ名を使用するには、RADIUS または TACACS+ セキュリティ サーバとの通信をイネーブルにしておく必要があります。RADIUS サーバとの通信を確立する方法の詳細については、「Configuring RADIUS」を参照してください。TACACS+ サーバとの通信を確立する方法の詳細については、「Configuring TACACS+」を参照してください。

AAA を使用した NASI 認証の設定

aaa authentication nasi コマンドを使用して、NetWare Asynchronous Services Interface（NASI）ユーザがルータにログインを試行するときに使用する認証方式のリストを 1 つまたは複数作成します。これらのリストは、**nasi authentication** ライン コンフィギュレーション コマンドで使用されます。

AAA を使用して NASI 認証を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# aaa new-model`	AAA をグローバルにイネーブルにします。
ステップ 2	`Router(config)# aaa authentication nasi {default | list-name} method1 [method2...]`	NASI ユーザに対する認証をイネーブルにします。
ステップ 3	`Router(config)# line number`	（任意：**default** が **aaa authentication nasi** コマンドに使用されている場合は不要）ライン コンフィギュレーション モードを開始します。
ステップ 4	`Router(config-line)# nasi authentication list-name`	（任意：**default** が **aaa authentication nasi** コマンドに使用されている場合は不要）回線上の NASI に対する認証をイネーブルにします。

list-name は、作成するリストを指定するときに使用される名前で、任意の文字列を使用できます。方式の引数は、認証アルゴリズムが試行する方式の実際のリストを指します。試行は入力されている順序で行われます。

名前付きリストが **aaa authentication nasi** コマンドで指定されていない場合に使用するデフォルト リストを作成するには、**default** キーワードの後に、デフォルトの状況で使用する方式を指定します。

追加の認証方式は、直前の方式で（失敗した場合ではなく）エラーが返された場合にだけ使用されます。すべての方式でエラーが返されても引き続き認証を行うように指定するには、コマンドラインの最後の方式として **none** を指定します。

（注） **none** を指定するとすべてのユーザが認証に成功してログインできるようになるため、認証のバックアップ方式として使用する必要があります。

表 7 に、サポートされる NASI 認証方式を示します。

表 7　AAA 認証 NASI 方式

キーワード	説明
enable	認証にイネーブル パスワードを使用します。
line	認証にライン パスワードを使用します。
local	認証にローカルなユーザ名データベースを使用します。
local-case	認証に大文字と小文字が区別されるローカルなユーザ名を使用します。
none	認証を使用しません。
group radius	認証にすべての RADIUS サーバのリストを使用します。
group tacacs+	認証にすべての TACACS+ サーバのリストを使用します。
group *group-name*	認証に **aaa group server radius** コマンドまたは **aaa group server tacacs+** コマンドで定義された RADIUS サーバまたは TACACS+ サーバのサブセットを使用します。

ここでは、次の内容について説明します。

- 「イネーブル パスワードによる NASI 認証」（P.24）
- 「ライン パスワードによる NASI 認証」（P.24）

- 「ローカル パスワードによる NASI 認証」（P.24）
- 「group RADIUS による NASI 認証」（P.24）
- 「group TACACS+ による NASI 認証」（P.25）
- 「group group-name による NASI 認証」（P.25）

イネーブル パスワードによる NASI 認証

認証方式としてイネーブル パスワードを指定するには、*method* キーワード **enable** を指定して **aaa authentication nasi** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、NASI ユーザ認証方式としてイネーブル パスワードを指定するには、次のコマンドを入力します。

```
aaa authentication nasi default enable
```

認証方式としてイネーブル パスワードを使用するには、イネーブル パスワードを定義しておく必要があります。イネーブル パスワードの定義の詳細については、「Configuring Passwords and Privileges」を参照してください。

ライン パスワードによる NASI 認証

認証方式としてライン パスワードを指定するには、*method* キーワード **line** を指定して **aaa authentication nasi** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、NASI ユーザ認証方式としてライン パスワードを指定するには、次のコマンドを入力します。

```
aaa authentication nasi default line
```

NASI 認証方式としてライン パスワードを使用するには、ライン パスワードを定義しておく必要があります。ライン パスワードの定義の詳細については、「ライン パスワード保護の設定」（P.37）を参照してください。

ローカル パスワードによる NASI 認証

Cisco ルータまたはアクセス サーバが認証情報にローカル ユーザ名データベースを使用するように指定するには、*method* キーワード **local** を指定して **aaa authentication nasi** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、NASI ユーザ認証方式としてローカル ユーザ名データベースを指定するには、次のコマンドを入力します。

```
aaa authentication nasi default local
```

ローカル ユーザ名データベースにユーザを追加する方法については、「ユーザ名認証の確立」（P.38）を参照してください。

group RADIUS による NASI 認証

NASI 認証方式として RADIUS を指定するには、**group radius** *method* を指定して **aaa authentication nasi** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、NASI ユーザ認証方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa authentication nasi default group radius
```

NASI 認証方式として RADIUS を使用するには、RADIUS セキュリティ サーバとの通信をイネーブルにしておく必要があります。RADIUS サーバとの通信を確立する方法の詳細については、「Configuring RADIUS」を参照してください。

group TACACS+ による NASI 認証

NASI 認証方式として TACACS+ を指定するには、**group tacacs+** *method* キーワードを指定して **aaa authentication nasi** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、NASI ユーザ認証方式として TACACS+ を指定するには、次のコマンドを入力します。

```
aaa authentication nasi default group tacacs+
```

認証方式として TACACS+ を使用するには、TACACS+ セキュリティ サーバとの通信をイネーブルにしておく必要があります。TACACS+ サーバとの通信を確立する方法の詳細については、「Configuring TACACS+」を参照してください。

group group-name による NASI 認証

NASI 認証方式として使用する RADIUS または TACACS+ サーバのサブセットを指定するには、**group** *group-name* 方式を指定して **aaa authentication nasi** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**nasirad** というグループ（**group**）のメンバを最初に定義します。

```
aaa group server radius nasirad
 server 172.16.2.3
 server 172.16.2 17
 server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバがグループ *nasirad* のメンバとして指定されます。

他の方式リストが定義されていない場合にログイン時のユーザ認証方式として **group nasirad** を指定するには、次のコマンドを入力します。

```
aaa authentication nasi default group nasirad
```

NASI 認証方式としてグループ名を使用するには、RADIUS または TACACS+ セキュリティ サーバとの通信をイネーブルにしておく必要があります。RADIUS サーバとの通信を確立する方法の詳細については、「Configuring RADIUS」を参照してください。TACACS+ サーバとの通信を確立する方法の詳細については、「Configuring TACACS+」を参照してください。

ログイン入力にかける時間の指定

timeout login response コマンドを使用すると、ログイン入力（ユーザ名やパスワードなど）がタイムアウトするまでの待機時間を指定できます。デフォルトのログイン値は 30 秒です。**timeout login response** コマンドを使用して、1 ～ 300 秒のタイムアウト値を指定します。30 秒というデフォルトのログイン タイムアウト値を変更するには、ライン コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-line)# timeout login response seconds`	タイムアウトまでログイン情報を待機する時間を指定します。

特権レベルでのパスワード保護のイネーブル化

ユーザが特権 EXEC コマンド レベルにアクセスできるかどうかを判断するときに使用する一連の認証方式を作成するには、**aaa authentication enable default** コマンドを使用します。最大 4 つの認証方式を指定できます。追加の認証方式は、直前の方式で（失敗した場合ではなく）エラーが返された場合にだけ使用されます。すべての方式でエラーが返されても引き続き認証を行うように指定するには、コマンドラインの最後の方式として **none** を指定します。

グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# aaa authentication enable default method1 [method2...]`	特権 EXEC レベルを要求するユーザに対して、ユーザ ID とパスワードのチェックをイネーブルにします。 （注） ルータから RADIUS サーバに送信されるすべての **aaa authentication enable default** 要求には、「$enab15$」というユーザ名が含まれます。TACACS+ サーバに送信される要求には、ログイン認証のために入力されるユーザ名が含まれます。

方式の引数は、認証アルゴリズムが試行する方式の実際のリストを指します。試行は入力されている順序で行われます。表 8 に、サポートされるイネーブル認証方式を示します。

表 8　AAA 認証イネーブル デフォルト方式

キーワード	説明
enable	認証にイネーブル パスワードを使用します。
line	認証にライン パスワードを使用します。
none	認証を使用しません。
group radius	認証にすべての RADIUS ホストのリストを使用します。 （注） RADIUS 方式は、ユーザ名別では機能しません。
group tacacs+	認証にすべての TACACS+ ホストのリストを使用します。
group *group-name*	認証に **aaa group server radius** コマンドまたは **aaa group server tacacs+** コマンドで定義された RADIUS サーバまたは TACACS+ サーバのサブセットを使用します。

パスワード プロンプトに表示するテキストの変更

Cisco IOS ソフトウェアからユーザに対してパスワードの入力を求めるときに表示されるデフォルト テキストを変更するには、**aaa authentication password-prompt** コマンドを使用します。このコマンドによって、イネーブル パスワードと、リモート セキュリティ サーバから提供されていないログイン パスワードのパスワード プロンプトが変更されます。このコマンドの **no** 形式を使用すると、パスワード プロンプトが次のデフォルト値に戻ります。

```
Password:
```

aaa authentication password-prompt コマンドでは、リモートの TACACS+ サーバまたは RADIUS サーバから提供されるダイアログは変更されません。

aaa authentication password-prompt コマンドは、RADIUS をログイン方式として使用するときに機能します。RADIUS サーバに到達不能の場合でも、コマンドで定義されたパスワード プロンプトが表示されます。**aaa authentication password-prompt** コマンドは、TACACS+ と併用できません。TACACS+ は、NAS に対して、ユーザに表示するパスワード プロンプトを提供します。TACACS+ サーバが到達可能な場合、NAS はそのサーバからパスワード プロンプトを受け取り、**aaa authentication password-prompt** コマンドで定義したプロンプトではなく、受け取ったプロンプトを使用します。TACACS+ サーバが到達不能の場合、**aaa authentication password-prompt** コマンドで定義したパスワード プロンプトが使用される可能性があります。

グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# aaa authentication password-prompt text-string`	ユーザにパスワードの入力を求めるときに表示するデフォルトテキストを変更します。

ユーザ名が空のアクセス要求が RADIUS サーバに送信されないようにする

次の設定手順では、ユーザ名が空のアクセス要求が RADIUS サーバに送信されないようにする方法について説明します。この機能により、RADIUS サーバとの不要なやりとりを回避でき、RADIUS ログの量を少なくすることができます。

（注） **aaa authentication suppress null-username** コマンドを使用できるのは、Cisco IOS XE Release 2.4 および Cisco IOS Release 12.2(33)SRD だけです。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication suppress null-username**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** **例：** `Router(config)# configure terminal`	AAA をグローバルにイネーブルにします。
ステップ 4	**aaa authentication suppress null-username** **例：** `Router(config)# aaa authentication suppress null-username`	ユーザ名が空のアクセス要求が RADIUS サーバに送信されないようにします。

AAA 認証のメッセージ バナーの設定

AAA は、設定可能でパーソナライズされたログインおよび失敗したログインのバナーの使用をサポートします。ユーザが AAA を使用して認証を受けるシステムにログインする場合、および何らかの理由で認証が失敗した場合に表示されるメッセージ バナーを設定できます。

ここでは、次の内容について説明します。

- 「ログイン バナーの設定」（P.28）
- 「Failed-Login バナーの設定」（P.29）

ログイン バナーの設定

ログイン バナーを作成するには、デリミタを設定する必要があります。デリミタはシステムに通知され、デリミタに続くテキスト ストリングはバナーとして表示され、テキスト ストリング自体が表示されます。デリミタは、バナーの末尾を示すために、テキスト ストリングの末尾で繰り返されます。デリミタには、拡張 ASCII 文字セットの任意の 1 文字を使用できます。ただし、デリミタとして定義した文字は、バナーを構成するテキスト ストリングには使用できません。

（ログインのデフォルト メッセージを置換して）ユーザがログインするたびに表示されるバナーを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)#` **aaa new-model**	AAA をイネーブルにします。
ステップ 2	`Router(config)#` **aaa authentication banner** *delimiter string delimiter*	パーソナライズされたログイン バナーを作成します。

ログイン バナーに表示できる最大の文字数は、2996 文字です。

Failed-Login バナーの設定

failed-login バナーを作成するには、デリミタを設定する必要があります。デリミタはシステムに通知され、デリミタに続くテキスト ストリングはバナーとして表示され、テキスト ストリング自体が表示されます。デリミタは、failed-login バナーの末尾を示すために、テキスト ストリングの末尾で繰り返されます。デリミタには、拡張 ASCII 文字セットの任意の 1 文字を使用できます。ただし、デリミタとして定義した文字は、バナーを構成するテキスト ストリングには使用できません。

（失敗したログインのデフォルト メッセージを置換して）ユーザがログインに失敗するたびに表示されるメッセージを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router(config)# **aaa new-model**	AAA をイネーブルにします。
ステップ 2	Router(config)# **aaa authentication fail-message** *delimiter string delimiter*	ユーザがログインに失敗したときに表示されるメッセージを作成します。

failed-login バナーに表示できる最大の文字数は、2996 文字です。

AAA パケット オブ ディスコネクトの設定

特定のセッション アトリビュートが指定された場合、接続解除パケット（POD）によってネットワーク アクセス サーバ（NAS）の接続が終了されます。UNIX ワークステーション上にある POD クライアントでは、AAA から取得したセッション情報を使用して、ネットワーク アクセス サーバで実行されている POD サーバに接続解除パケットを送信します。NAS では、1 つまたは複数の一致するキー アトリビュートを含む任意の着信ユーザ セッションを終了します。必要なフィールドがない場合、または完全一致が見つからない場合、要求は拒否されます。

POD を設定するには、グローバル コンフィギュレーション モードで次のタスクを使用します。

	コマンド	目的
ステップ 1	Router(config)# **aaa accounting network default** start-stop radius	AAA アカウンティング レコードをイネーブルにします。
ステップ 2	Router(config)# **aaa accounting delay-start**	（任意）POD パケットで使用できるように、Framed-IP-Address が割り当てられるまで、開始アカウンティング レコードの生成を遅延します。
ステップ 3	Router(config)# **aaa pod server server-key** *string*	POD の受信イネーブルにします。
ステップ 4	Router(config)# **radius-server host** *IP address* **non-standard**	RADIUS のベンダー固有バージョンを使用する RADIUS ホストを宣言します。

二重認証のイネーブル化

以前のバージョンで PPP セッションを認証するには、PAP または CHAP の単一の認証方法を使用する必要がありました。二重認証方式の場合、ネットワーク アクセス権を得るには、CHAP または PAP 認証後に、リモート ユーザが認証の第 2 段階に合格する必要があります。

この第 2 段階（「二重」）の認証には、ユーザがパスワードを知っている必要がありますが、ユーザのリモート ホストにパスワードは保存されません。そのため、第 2 段階の認証は、ホストではなくユーザに固有です。その結果、リモート ホストから情報が盗まれた場合でも有効な、追加のセキュリティ レベルが実現します。さらに、ユーザ別にネットワーク特権をカスタマイズできるため、柔軟性も高くなります。

第 2 段階の認証には、CHAP ではサポートされないトークン カードなど、ワンタイム パスワードを使用できます。ワンタイム パスワードを使用している場合、ユーザ パスワードが盗まれても盗用者の役に立ちません。

この項の内容は、次のとおりです。

- 「二重認証の機能」（P.30）
- 「二重認証の設定」（P.31）
- 「二重認証後のユーザ プロファイルへのアクセス」（P.32）

二重認証の機能

二重認証を使用する場合、2 つの認証/認可段階があります。この 2 つの段階は、リモート ユーザがダイヤルインした後、および PPP セッションが開始された後に発生します。

第 1 段階では、ユーザがリモート ホスト名を使用してログインして CHAP（または PAP）がリモート ホストを認証し、次に PPP が AAA とネゴシエートしてリモート ホストを認可します。このプロセスで、リモート ホストに関連付けられたネットワーク アクセス特権は、そのユーザに関連付けられます。

（注） ローカル ホストに対して Telnet 接続だけを許可するように、この第 1 段階ではネットワーク管理者が認可を制限することを推奨します。

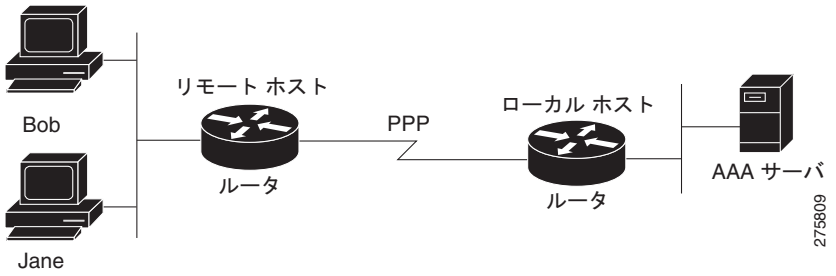
第 2 段階では、リモート ユーザが、認証を受けるネットワーク アクセス サーバに対して Telnet を送信する必要があります。リモート ユーザがログインする場合、AAA ログイン認証を使用してユーザを認証する必要があります。次に、AAA を使用して最認可を受けるために、**access-profile** コマンドを入力する必要があります。この認可が完了すると、ユーザは二重に認証され、ユーザ別のネットワーク特権に従ってネットワークにアクセスできるようになります。

システム管理者は、セキュリティ サーバで適切なパラメータを設定することで、各認証段階の後にリモート ユーザが保持するネットワーク特権を決定します。二重認証を使用するには、**access-profile** コマンドを発行してアクティブ化する必要があります。

注意 複数のホストがネットワーク アクセス サーバに対して PPP 接続を共有する場合、二重認証によって望ましくない状況が発生することがあります（図 2 を参照）。

まず、ユーザ Bob が PPP セッションを開始し、ネットワーク アクセス サーバで二重認証をアクティブにした場合（図 2 を参照）、Bob の PPP セッションが期限切れになるまで、他のすべてのユーザは Bob と同じネットワーク特権を持つことになります。この問題が発生するのは、PPP セッション時に Bob の認可プロファイルがネットワーク アクセス サーバのインターフェイスに適用され、他のユーザからの PPP トラフィックに Bob が確立した PPP セッションが使用されるためです。第 2 に、Bob が PPP セッションを開始して二重認証をアクティブにし、（Bob の PPP セッションが期限切れになる前に）別のユーザ Jane が **access-profile** コマンドを実行する場合（または、Jane がネットワーク アクセス サーバに Telnet を送信し、**autocommand access-profile** が実行された場合）、再認可が発生し、Jane の認可プロファイルがインターフェイスに適用され、Bob のプロファイルは置換されます。その結果、Bob の PPP トラフィックの不通や中止が発生することや、Bob が本来は持っていないレベルの特権が Bob に付与されることがあります。

図 2　危険性を伴うトポロジ : 複数のホストがネットワーク アクセス サーバに対する PPP 接続を共有



二重認証の設定

二重認証を設定するには、次の手順を実行します。

1. **aaa-new model** グローバル コンフィギュレーション コマンドを使用して、AAA をイネーブルにします。AAA をイネーブルにする方法の詳細については、「AAA Overview」を参照してください。
2. **aaa authentication** コマンドを使用して、ログインおよび ppp 認証方式リストを使用するようにネットワーク アクセス サーバを設定します。次に、これらの方式リストを適切な回線やインターフェイスに適用します。
3. **aaa authorization** コマンドを使用して、ログイン時の AAA ネットワーク認可を設定します。ネットワーク認可の設定の詳細については、「認可の設定」の章を参照してください。
4. セキュリティ プロトコル パラメータ（たとえば、RADIUS または TACACS+）を設定します。RADIUS の詳細については、「Configuring RADIUS」を参照してください。TACACS+ の詳細については、「Configuring TACACS+」を参照してください。
5. セキュリティ サーバで、ユーザがローカル ホストに接続できるアクセス コントロール リストの AV ペアを使用するには、Telnet 接続を確立する必要があります。
6. （任意）autocommand として **access-profile** コマンドを設定します。autocommand を設定すると、リモート ユーザは、個人のユーザ プロファイルに関連付けられた権限にアクセスするために、手動で **access-profile** コマンドを入力する必要はなくなります。autocommand の設定方法については、『*Cisco IOS Dial Technologies Command Reference: Network Services*』の **autocommand** コマンドを参照してください。

（注）　**access-profile** コマンドが autocommand として設定されている場合でも、二重認証を完了するには、ユーザがローカル ホストに Telnet を送信し、ログインする必要があります。

ユーザ固有の認可ステートメントを作成する場合、次の規則に従います（これらの規則は、**access-profile** コマンドのデフォルトの動作に関連します）。

- セキュリティ サーバでアクセス コントロール リストの AV ペアを設定する場合、有効な AV ペアを使用します。有効な AV ペアのリストについては、『*Cisco IOS Security Command Reference*』の「Authentication Commands」の章を参照してください。
- リモート ユーザがインターフェイスの既存の認可（第 2 段階の認証 / 認可の前に存在する認可）を使用し、異なるアクセス コントロール リスト（ACL）を持つようにするには、ユーザ固有の認可定義で ACL AV ペア*だけ*を指定します。この方法は、デフォルトの認可プロファイルを設定してリモート ホストに適用し、ACL はユーザ別に適用する場合などに有効です。

- これらのユーザ固有の認可ステートメントを後でインターフェイスに適用すると、ユーザの認可に使用する **access-profile** コマンドの実行方法によって、既存のインターフェイス設定に*追加*することや、既存のインターフェイス設定を*置き換える*ことができます。認可ステートメントを設定する前に、**access-profile** コマンドの機能について理解する必要があります。
- ISDN または Multilink PPP を使用する予定がある場合、ローカル ホストで仮想テンプレートも設定する必要があります。

二重認証に関する問題を解決するには、**debug aaa per-user** デバッグ コマンドを使用します。このコマンドの詳細については、『*Cisco IOS Debug Command Reference*』を参照してください。

二重認証後のユーザ プロファイルへのアクセス

二重認証で、リモート ユーザがローカル ホスト名を使用してローカル ホストに対する PPP リンクを確立すると、リモート ホストは CHAP（または PAP）認証されます。CHAP（または PAP）認証後、PPP は AAA とネゴシエートして、リモート ホストに関連付けられたネットワーク アクセス特権をユーザに割り当てます（この段階の特権では、ユーザがローカル ホストに接続するには Telnet 接続を必須にするという制限を付けることを推奨します）。

ユーザが二重認証の第 2 段階を開始する必要があり、ローカル ホストに対して Telnet 接続を確立する場合、ユーザは個人のユーザ名とパスワード（CHAP または PAP のユーザ名とパスワードとは異なります）を入力します。この処理の結果、個人のユーザ名 / パスワードに従って AAA 認証が発生します。ただし、ローカル ホストに関連付けられた初期の権限が有効です。ローカル ホストに関連付けられた権限は、**access-profile** コマンドを使用して、ユーザ プロファイルのユーザ用に定義されている権限で置き換えられるか、結合されます。

二重認証後にユーザ プロファイルにアクセスするには、EXEC コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router> access-profile [merge | replace] [ignore-sanity-checks]`	二重認証後に、ユーザに関連付けられた権限にアクセスします。

autocommand として実行するように **access-profile** コマンドを設定した場合、リモート ユーザのログイン後に自動的に実行されます。

自動二重認証のイネーブル化

自動二重認証を実装することで、ユーザにとって二重認証プロセスが容易になります。自動二重認証は、二重認証が持つセキュリティ上の利点をすべて備えていますが、リモート ユーザにとってよりシンプルでユーザフレンドリなインターフェイスです。二重認証の場合、ユーザ認証の第 2 レベルは、ユーザがネットワーク アクセス サーバまたはルータに Telnet に送信し、ユーザ名とパスワードを入力したときに完了します。自動二重認証の場合、ユーザがネットワーク アクセス サーバに Telnet を送信する必要はありません。その代わり、ユーザ名とパスワードまたは Personal Identification Number（PIN）の入力を求めるダイアログ ボックスが表示されます。自動二重認証機能を使用するには、リモート ユーザ ホストでコンパニオン クライアント アプリケーションが実行されている必要があります。Cisco IOS Release 12.0 以降、唯一の使用できるクライアント アプリケーション ソリューションは、PC 用の Glacier Bay アプリケーション サーバ ソフトウェアです。

（注） 自動二重認証は、既存の二重認証機能と同様に、Multilink PPP ISDN 接続専用です。自動二重認証は、X.25 や SLIP など他のプロトコルとは併用できません。

自動二重認証は、既存の二重認証機能の強化です。自動二重認証を設定するには、まず次の手順を実行して二重認証を設定する必要があります。

1. **aaa-new model** グローバル コンフィギュレーション コマンドを使用して、AAA をイネーブルにします。AAA をイネーブルにする方法の詳細については、「AAA Overview」を参照してください。
2. **aaa authentication** コマンドを使用して、ログインおよび ppp 認証方式リストを使用するようにネットワーク アクセス サーバを設定します。次に、これらの方式リストを適切な回線やインターフェイスに適用します。
3. **aaa authorization** コマンドを使用して、ログイン時の AAA ネットワーク認可を設定します。ネットワーク認可の設定の詳細については、「認可の設定」の章を参照してください。
4. セキュリティ プロトコル パラメータ（たとえば、RADIUS または TACACS+）を設定します。RADIUS の詳細については、「Configuring RADIUS」を参照してください。TACACS+ の詳細については、「Configuring TACACS+」を参照してください。
5. セキュリティ サーバで、ユーザがローカル ホストに接続できるアクセス コントロール リストの AV ペアを使用するには、Telnet 接続を確立する必要があります。
6. autocommand として **access-profile** コマンドを設定します。autocommand を設定すると、リモート ユーザは、個人のユーザ プロファイルに関連付けられた権限にアクセスするために、手動で **access-profile** コマンドを入力する必要はなくなります。autocommand の設定方法については、『*Cisco IOS Dial Technologies Command Reference*』の **autocommand** コマンドを参照してください。

（注） **access-profile** コマンドが autocommand として設定されている場合でも、二重認証を完了するには、ユーザがローカル ホストに Telnet を送信し、ログインする必要があります。

ユーザ固有の認可ステートメントを作成する場合、次の規則に従います（これらの規則は、**access-profile** コマンドのデフォルトの動作に関連します）。

- セキュリティ サーバでアクセス コントロール リストの AV ペアを設定する場合、有効な AV ペアを使用します。有効な AV ペアのリストについては、『*Cisco IOS Security Command Reference*』の「Authentication, Authorization, and Accounting (AAA)」を参照してください。
- リモート ユーザがインターフェイスの既存の認可（第 2 段階の認証/認可の前に存在する認可）を使用し、異なるアクセス コントロール リスト（ACL）を持つようにするには、ユーザ固有の認可定義で ACL AV ペア*だけ*を指定します。この方法は、デフォルトの認可プロファイルを設定してリモート ホストに適用し、ACL はユーザ別に適用する場合などに有効です。
- これらのユーザ固有の認可ステートメントを後でインターフェイスに適用すると、ユーザの認可に使用する **access-profile** コマンドの実行方法によって、既存のインターフェイス設定に*追加*することや、既存のインターフェイス設定を*置き換える*ことができます。認可ステートメントを設定する前に、**access-profile** コマンドの機能について理解する必要があります。
- ISDN または Multilink PPP を使用する予定がある場合、ローカル ホストで仮想テンプレートも設定する必要があります。

二重認証に関する問題を解決するには、**debug aaa per-user** デバッグ コマンドを使用します。このコマンドの詳細については、『*Cisco IOS Debug Command Reference*』を参照してください。

二重認証を設定したら、自動機能を追加できます。

自動二重認証を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# ip trigger-authentication [timeout seconds] [port number]`	二重認証の自動化をイネーブルにします。

ステップ 2	`Router(config)# interface bri number`
	または
	`Router(config)# interface serial number:23`
		ISDN BRI または ISDN PRI インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	`Router(config-if)# ip trigger-authentication`	自動二重認証をインターフェイスに適用します。

自動二重認証の問題を解決するには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router# show ip trigger-authentication`	自動二重認証が試行され、成功または失敗したリモート ホストのリストが表示されます。
ステップ 2	`Router# clear ip trigger-authentication`	自動二重認証が試行されたリモート ホストのリストをクリアします この操作で、**show ip trigger-authentication** コマンドで表示された表がクリアされます。
ステップ 3	`Router# debug ip trigger-authentication`	自動二重認証に関する **debug** の出力が表示されます。

RADIUS CoA 用の動的認可サービスの設定

次の手順を使用して、動的認可サービスの Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）サーバとしてのルータが、入力方向と出力方向でポリシー マップをプッシュする CoA 機能をサポートできるようにします。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip_addr* | *hostname*} [**server-key** [**0** | **7**] *string*]
6. **domain** {**delimiter** *character* | **stripping** [**right-to-left**]}
7. **port** {*port-num*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** **例：** `Router(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**aaa server radius dynamic-author** **例：** `Router(config)# aaa server radius dynamic-author`	ローカル AAA サーバを動的認可サービス用にセットアップして、動的認可ローカル サーバ コンフィギュレーション モードに入ります。このサービスは、ポリシー マップを入力方向と出力方向にプッシュする CoA 機能をサポートするように有効にする必要があります。このモードでは、RADIUS アプリケーション コマンドが設定されます。
ステップ 5	**client** {*ip_addr* | *hostname*} [**server-key** [**0** | **7**] *string*] **例：** AAA サーバ上の設定例を次に示します。 `Router(config-locsvr-da-radius)#client 192.168.0.5 server-key cisco1`	AAA サーバ クライアントの IP アドレスまたはホスト名を設定します。オプションの **server-key** キーワードと *string* 引数を使用して、「クライアント」レベルでサーバ キーを設定します。 **（注）** クライアント レベルでサーバ キーを設定すると、グローバル レベルで設定されたサーバ キーが上書きされます。

ステップ 6	**domain** {**delimiter** *character* | **stripping** [**right-to-left**]}
	
	例：
	`Router(config-locsvr-da-radius)# domain stripping right-to-left`
	`Router(config-locsvr-da-radius)# domain delimiter @`
		（任意）RADIUS アプリケーションについてユーザ名のドメイン オプションを設定します。
		• **delimiter** キーワードで、ドメイン デリミタを指定します。*character* 引数には、**@**、/、**$**、**%**、\、**#**、または **-** のオプションを指定できます。
		• **stripping** キーワードは、着信のユーザ名と、**@** ドメイン デリミタの左側にある名前を比較します。
		• **right-to-left** キーワードは、右から左方向に見て最初のデリミタで文字列を終了します。

ステップ 7	**port** {*port-num*} **例：** `Router(config-locsvr-da-radius)# port 3799`	CoA 要求に UDP ポート 3799 を設定します。

bounce および disable RADIUS CoA 要求を無視するためのルータの設定

次の手順を使用して、bounce port コマンドまたは disable port コマンドの形式で RADIUS サーバ CoA 要求を無視するようにルータを設定します。

複数のホストを使用して認証ポートを認証していて、このポートで 1 つのホストに対してフラップする CoA 要求があるか、このポートで終了するホスト セッションがある場合、このポート上のその他のホストにも影響があります。その結果、フラップの場合には 1 つまたは複数のホストから DHCP の再ネゴシエーションがトリガーされます。または、1 つまたは複数のホストについて、セッションをホストする認証ポートが管理的にシャットダウンされます。これは望ましくない問題になる可能性があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **authentication command bounce-port ignore**
5. **authentication command disable-port ignore**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： Router(config)# aaa new-model	AAA をイネーブルにします。
ステップ 4	**authentication command bounce-port ignore** 例： Router(config)# **authentication command bounce-port ignore**	（任意）RADIUS サーバの bounce port コマンドを無視するようにルータを設定します。無視しない場合、認証ポート上でホストがフラップをリンクし、結果として、そのポートに接続する 1 つまたは複数のホストから DHCP 再ネゴシエーションが発生します。
ステップ 5	**authentication command disable-port ignore** 例： Router(config)# **authentication command disable-port ignore**	（任意）RADIUS サーバの CoA disable port コマンドを無視するようにルータを設定します。無視しない場合、1 または複数のホスト セッションをホストする認証ポートが管理的にシャットダウンされます。ポートがシャットダウンされると、セッションも終了します。

非 AAA 認証方式

ここでは、次の非 AAA 認証タスクについて説明します。

- 「ライン パスワード保護の設定」
- 「ユーザ名認証の確立」
- 「CHAP 認証または PAP 認証のイネーブル化」
- 「MS-CHAP の使用」

ライン パスワード保護の設定

このタスクは、パスワードを入力し、パスワード チェック処理を確立することで、端末回線にアクセス コントロールを提供するために使用します。

（注） ライン パスワード保護を設定し、TACACS または拡張 TACACS を設定する場合、TACACS のユーザ名とパスワードの方が、ライン パスワードよりも優先されます。まだセキュリティ ポリシーを実装していない場合、AAA を使用することを推奨します。

手順の概要

1. **enable**
2. **configure terminal**
3. **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
4. **password** *password*
5. **login**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	`enable`
	
	例：
	`Router> enable`
		特権 EXEC モードをイネーブルにします。
		• プロンプトが表示されたら、パスワードを入力します。

ステップ 2	`configure terminal`
	
	例：
	`Router# configure terminal`
		グローバル コンフィギュレーション モードを開始します。

ステップ 3	`line [aux | console | tty | vty] line-number [ending-line-number]`
	
	例：
	`Router(config)# line console 0`
		ライン コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**password** *password* 例： Router(config-line)# secret word	回線上の端末または他のデバイスにパスワードを割り当てます。パスワードは大文字と小文字が区別されます。またスペースを含めることができます。たとえば、「Secret」というパスワードは「secret」というパスワードとは異なり、「two words」も使用できるパスワードです。
ステップ 5	**login** 例： Router(config-line)# login	ログイン時のパスワード チェックをイネーブルにします。 回線パスワードの確認をディセーブルにするには、このコマンドの **no** バージョンを使用します。 （注） **login** コマンドを実行すると、ユーザ名と特権レベルのみが変更されます。シェルは実行されません。そのため、autocommand は実行されません。この状況で autocommand を実行するには、ルータに対して Telnet セッションを確立する必要があります。autocommand をこの方法で実装する場合、セキュア Telnet セッションのためにルータを設定します。

ユーザ名認証の確立

ユーザ名ベースの認証システムを作成できます。これは、次のような場合に役立ちます。

- TACACS をサポートしないネットワークに、TACACS のようなユーザ名と暗号化されたパスワード認証システムを提供する場合
- 特殊なケース（たとえば、アクセス リストの確認、パスワードの確認なし、ログイン時の autocommand の実行、「エスケープなし」の状況など）に備えたログインを提供する場合

ユーザ名の認証を確立するには、システム設定の必要に応じて、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	**Router(config)# username** *name* [**nopassword** | **password** *password* | **password** *encryption-type encrypted password*] または **Router(config)# username** *name* [**access-class** *number*]	暗号化されたパスワードを使用してユーザ名認証を確立します。 または （任意）アクセス リストによるユーザ名認証を確立します。
ステップ 2	**Router(config)# username** *name* [**privilege** *level*]	（任意）ユーザの特権レベルを設定します。
ステップ 3	**Router(config)# username** *name* [**autocommand** *command*]	（任意）自動実行されるコマンドを指定します。
ステップ 4	**Router(config)# username** *name* [**noescape**] [**nohangup**]	（任意）「エスケープなし」のログイン環境を設定します。

キーワード **noescape** を指定すると、ユーザは接続先のホストでエスケープ文字を使用できなくなります。**nohangup** 機能を使用すると、autocommand の使用後に接続が解除されません。

注意 **service password-encryption** コマンドをイネーブルにしない限り、設定のパスワードはクリア テキストで表示されます。**service password-encryption** コマンドの詳細については、『*Cisco IOS Security Command Reference*』の「Passwords and Privileges Commands」の章を参照してください。

CHAP 認証または PAP 認証のイネーブル化

Internet Service Provider（ISP; インターネット サービス プロバイダー）のダイヤル ソリューションに使用されている最も一般的なトランスポート プロトコルの 1 つは、Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）です。従来、リモート ユーザはアクセス サーバにダイヤルインして、PPP セッションを開始していました。PPP のネゴシエート後は、リモート ユーザは ISP ネットワークに接続され、そしてインターネットに接続されます。

ISP はアクセス サーバへの接続を顧客に限定したいため、リモート ユーザはアクセス サーバに対して認証を受けてから、PPP セッションを開始する必要があります。通常、リモート ユーザは、アクセス サーバからのプロンプトに応じてユーザ名とパスワードを入力して、認証を受けます。これは実行可能なソリューションですが、管理が困難で、リモート ユーザにとっても面倒です。

よりよいソリューションは、PPP に組み込まれた認証プロトコルを使用することです。この場合、リモート ユーザはアクセス サーバにダイヤルインし、アクセス サーバと PPP の最小サブセットを開始します。この操作で、ISP のネットワークに対するアクセス権はリモート ユーザに付与されません。単に、アクセス サーバがリモート デバイスと通話できるだけです。

現在、PPP は 2 つの認証プロトコルをサポートします。Password Authentication Protocol（PAP; パスワード認証プロトコル）および Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）の 2 つです。いずれも RFC 1334 で規定され、同期インターフェイスと非同期インターフェイスでサポートされます。PAP または CHAP を介する認証は、サーバからのプロンプトを受けてユーザ名とパスワードを入力する方法と同等です。CHAP の場合、接続の間にリモート ユーザのパスワードは送信されないため、より安全性が高いと考えられます。

（PAP 認証または CHAP 認証の有無に関係なく）PPP はダイヤルアウト ソリューションでもサポートされます。アクセス サーバがダイヤルアウト機能を使用するのは、アクセス サーバからリモート デバイスに対してコールを開始し、PPP などのトランスポート プロトコルを起動しようとするときです。

CHAP および PAP の詳細については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』の「Configuring Interfaces」を参照してください。

（注） CHAP または PAP を使用するには、PPP カプセル化を実行する必要があります。

インターフェイスで CHAP をイネーブルにし、リモート デバイスがそのインターフェイスに接続しようとすると、アクセス サーバからリモート デバイスに CHAP パケットが送信されます。CHAP パケットは、リモート デバイスに応答するように要求または「チャレンジ」します。チャレンジ パケットは、ローカル ルータの ID、ランダム番号、およびホスト名から構成されます。

リモート デバイスは、チャレンジ パケットを受信すると、ID、リモート デバイスのパスワード、およびランダム番号を連結し、リモート デバイスのパスワードを使用してすべてを暗号化します。リモート デバイスは、その結果を、暗号化プロセスで使用されたパスワードに関連付けられた名前とともにアクセス サーバに返信します。

アクセス サーバがその応答を受信すると、受信した名前を使用して、ユーザ データベースに保存されているパスワードを取得します。取得したパスワードは、暗号化プロセスで使用されたリモート デバイスと同じパスワードです。アクセス サーバは、新しく取得したパスワードを使用して、連結された情報を暗号化します。その結果が応答パケットで送信された結果と一致する場合、認証は成功です。

CHAP 認証を使用する利点は、リモート デバイスのパスワードがクリア テキストで送信されないことです。結果として、他のデバイスによるパスワード盗用や、ISP ネットワークに対する不正アクセスの取得を回避できます。

CHAP トランザクションが発生するのは、リンクが確立したときだけです。アクセス サーバは、以降のコール中にパスワードを要求しません（ただし、ローカル デバイスは、コール中に他のデバイスからこのような要求があった場合、応答する可能性があります）。

PAP をイネーブルにすると、アクセス サーバに接続しようとするリモート ルータは、認証要求を送信する必要があります。認証要求に指定されているユーザ名とパスワードが受け入れられた場合、Cisco IOS ソフトウェアから認証の確認応答が送信されます。

CHAP または PAP をイネーブルにすると、アクセス サーバは、ダイヤルインするリモート デバイスからの認証を必須にするようになります。イネーブルにしたプロトコルをリモート デバイスがサポートしていない場合、コールはドロップされます。

CHAP または PAP を使用するには、次のタスクを実行する必要があります。

1. PPP カプセル化をイネーブルにします。
2. インターフェイスで CHAP または PAP をイネーブルにします。
3. CHAP の場合、認証が必須の各リモート システムについて、ホスト名の認証および秘密（パスワード）を設定します。

ここでは、次の内容について説明します。

PPP カプセル化のイネーブル化

PPP カプセル化をイネーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)# encapsulation ppp`	インターフェイスで PPP をイネーブルにします。

PAP または CHAP のイネーブル化

PPP カプセル化として設定されているインターフェイスで、CHAP 認証または PAP 認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config-if)# ppp authentication {*protocol1* [*protocol2...*]} [**if-needed**] {**default** | *list-name*} [**callin**] [**one-time**]	サポートされる認証プロトコルと、使用順序を定義します。このコマンドの *protocol1* と protocol2 は、CHAP、MS-CHAP、および PAP のプロトコルを示します。PPP 認証は、まず *protocol1* に指定された最初の認証方式を使用して試行されます。認証に *protocol1* を使用できない場合は、次に設定されているプロトコルを使用して認証のネゴシエーションを行います。

インターフェイスで **ppp authentication chap** を設定する場合、そのインターフェイスで PPP 接続を開始するすべての受信コールは、CHAP を使用して認証される必要があります。同様に、**ppp authentication pap** を設定する場合、PPP 接続を開始するすべての受信コールは、PAP を使用して認証される必要があります。**ppp authentication chap pap** を設定する場合、アクセス サーバは、CHAP を使用して PPP セッションを開始するすべての受信を認証しようとします。リモート デバイスが CHAP をサポートしない場合、アクセス サーバは PAP を使用してコールを認証しようとします。リモート デバイスが CHAP も PAP もサポートしない場合、認証は失敗し、コールはドロップされます。**ppp authentication pap chap** を設定する場合、アクセス サーバは、PAP を使用して PPP セッションを開始するすべての受信を認証しようとします。リモート デバイスが PAP をサポートしない場合、アクセス サーバは CHAP を使用してコールを認証しようとします。リモート デバイスがいずれのプロトコルもサポートしない場合、認証は失敗し、コールはドロップされます。**callin** キーワードを指定して **ppp authentication** コマンドを設定すると、アクセス サーバは、リモート デバイスがコールを開始した場合にだけ、リモート デバイスの認証を行います。

認証方式リストと **one-time** キーワードを使用できるのは、AAA をイネーブルにした場合だけです。TACACS または拡張 TACACS をイネーブルにしている場合は、使用できません。**ppp authentication** コマンドを使用して認証方式リストの名前を指定すると、PPP は、指定した方式リストに定義されている方式を使用して、接続を認証しようとします。AAA をイネーブルにし、名前で定義されている方式リストがない場合、PPP は、デフォルトに定義されている方式を使用して接続を認証しようとします。**one-time** キーワードを指定して **ppp authentication** コマンドを使用すると、認証中にワンタイム パスワードをサポートできます。

if-needed キーワードを使用できるのは、TACACS または拡張 TACACS を使用している場合だけです。**if-needed** キーワードを指定して **ppp authentication** コマンドを使用することは、現在のコール期間中にリモート デバイスがまだ認証されていない場合にだけ、PPP が PAP または CHAP を介してリモート デバイスを認証することを示します。リモート デバイスが、標準のログイン手順で認証を受け、EXEC プロンプトから PPP を開始した場合、**ppp authentication chap if-needed** がインターフェイスで設定されていれば、PPP は CHAP を介して認証しません。

注意 **aaa authentication ppp** コマンドを使用して設定されていない *list-name* を使用する場合、その回線で PPP はディセーブルです。

ローカル ルータまたはアクセス サーバが認証を必須とする各リモート システムについて、**username** エントリを追加する方法については、「ユーザ名認証の確立」（P.38）を参照してください。

着信認証と発信認証

PPP は双方向の認証をサポートしています。通常、リモート デバイスがアクセス サーバにダイヤルインするときは、それが許可されているアクセスであることをリモート デバイスが証明するように、アクセス サーバから要求されます。これは着信認証と呼ばれます。同時に、リモート デバイスは、身元を証明するようにアクセス サーバに要求することもできます。これは発信認証と呼ばれます。また、アクセス サーバは、リモート デバイスに対してコールを開始するときにも、発信認証を実行します。

発信 PAP 認証のイネーブル化

発信 PAP 認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)# ppp pap sent-username` *`username`* `password` *`password`*	発信 PAP 認証をイネーブルにします。

アクセス サーバからリモート デバイスに対してコールを開始する場合は常に、または発信認証のためにリモート デバイスの要求に応答する必要がある場合は、**ppp pap sent-username** コマンドをで指定されたユーザ名とパスワードを使用して自身を認証します。

PAP 認証要求の拒否

ピアからの PAP 認証要求を拒否するには（つまり、すべてのコールで PAP 認証をディセーブルにするには）、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)# ppp pap refuse`	PAP 認証を要求するピアからの PAP 認証を拒否します。

refuse キーワードが使用されない場合、ルータはピアから受信した PAP 認証チャレンジを拒否しません。

共通 CHAP パスワードの作成

リモート CHAP 認証だけの場合、不明なピアからのチャレンジに対して使用する共通 CHAP シークレット パスワードを作成するように、ルータを設定できます。たとえば、ルータが、新しい（つまり不明な）ルータが追加された、ルータのロータリー（別ベンダー製のルータ、または古いバージョンの Cisco IOS ソフトウェアを実行するルータ）に発信する場合などです。**ppp chap password** コマンドを使用すると、任意のダイヤラ インターフェイスまたは非同期グループ インターフェイスで、複数のユーザ名およびパスワード コンフィギュレーション コマンドをこのコマンドの単一のコピーで置換できます。

ルータのコレクションに発信するルータが、共通の CHAP シークレット パスワードを設定できるようにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)# ppp chap password` *`secret`*	ルータのコレクションに発信するルータが、共通の CHAP シークレット パスワードを設定できるようにします。

CHAP 認証要求の拒否

ピアからの CHAP 認証要求を拒否するには（つまり、すべてのコールで CHAP 認証をディセーブルにするには）、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)# ppp chap refuse [callin]`	CHAP 認証を要求するピアからの CHAP 認証を拒否します。

callin キーワードが使用されると、ルータは、ピアから受信した CHAP 認証チャレンジへの応答を拒否します。ただし、ルータが送信する CHAP チャレンジに対しては、ピアが応答することを必須とします。

（**ppp pap sent-username** コマンドを使用して）発信 PAP がイネーブルの場合、拒否パケットの認証方式として、PAP が提案されます。

ピアが認証されるまで CHAP 認証を遅延する

ピアがルータから認証を受けるまで、CHAP 認証を要求するピアに対してルータを認証しないように指定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)# ppp chap wait` *secret*	ピアがルータから認証を受けるまで、CHAP 認証を遅延するようにルータを設定します。

このコマンド（デフォルト）により、CHAP 認証を要求するピアがルータの認証を受けてから、ルータがピアの認証を受けるように指定します。**no ppp chap wait** コマンドにより、ルータが認証チャレンジに対して即時に応答するように指定します。

MS-CHAP の使用

Microsoft Challenge Handshake Authentication Protocol（MS-CHAP; マイクロソフト チャレンジ ハンドシェーク認証プロトコル）は、Microsoft バージョンの CHAP であり、RFC 1994 の拡張です。標準バージョンの CHAP と同様に、MS-CHAP は PPP 認証に使用されます。この場合、Microsoft Windows NT または Microsoft Windows 95 を使用する PC と、ネットワーク アクセス サーバとして動作する Cisco ルータまたはアクセス サーバとの間に認証が発生します。

MS-CHAP と標準の CHAP の違いは次のとおりです。

- MS-CHAP をイネーブルにするには、LCP オプション 3 の Authentication Protocol で、CHAP Algorithm 0x80 をネゴシエートします。
- MS-CHAP 応答パケットは、Microsoft Windows NT 3.5 および 3.51、Microsoft Windows 95、および Microsoft LAN Manager 2.*x* と互換性を持つように設計されたフォーマットです。このフォーマットを使用する場合、オーセンティケータは、クリア パスワードまたは可逆的に暗号化されたパスワードを保存する必要はありません。
- MS-CHAP には、オーセンティケータが制御する認証リトライ メカニズムがあります。
- MS-CHAP には、オーセンティケータが制御するチャレンジ パスワード メカニズムがあります。
- MS-CHAP には、Failure パケット メッセージ フィールドで返される「reason-for failure」コードセットが定義されています。

実装したセキュリティ プロトコルに応じて、AAA セキュリティ サービスの有無にかかわらず、MS-CHAP による PPP 認証を使用できます。AAA をイネーブルにしている場合、MS-CHAP を使用する PPP 認証は、TACACS+ および RADIUS の両方と併用できます。表 9 に、RADIUS が MS-CHAP をサポートできるベンダー固有 RADIUS アトリビュート（IETF Attribute 26）を示します。

表 9　MS-CHAP 用のベンダー固有 RADIUS アトリビュート

ベンダー ID 番号	ベンダー タイプ 番号	ベンダー固有アトリビュート	説明
311	11	MSCHAP-Challenge	ネットワーク アクセス サーバが MS-CHAP ユーザに送信するチャレンジが含まれます。Access-Request パケットと Access-Challenge パケットの両方に使用できます。
211	11	MSCHAP-Response	PPP MS-CHAP ユーザがチャレンジに対する応答で提供するレスポンス値が含まれます。Access-Request パケットでのみ使用されます。このアトリビュートは、PPP CHAP ID と同じです。

MS-CHAP を使用して PPP 認証を定義するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config-if)# encapsulation ppp`	PPP カプセル化をイネーブルにします。
ステップ 2	`Router(config-if)# ppp authentication ms-chap` [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**]	MS-CHAP を使用して PPP 認証を定義します。

あるインターフェイスで **ppp authentication ms-chap** を設定する場合、PPP 接続を開始するそのインターフェイスに着信するすべてのコールは、MS-CHAP を使用して認証する必要があります。**callin** キーワードを指定して **ppp authentication** コマンドを設定すると、アクセス サーバは、リモート デバイスがコールを開始した場合にだけ、リモート デバイスの認証を行います。

認証方式リストと **one-time** キーワードを使用できるのは、AAA をイネーブルにした場合だけです。TACACS または拡張 TACACS をイネーブルにしている場合は、使用できません。**ppp authentication** コマンドを使用して認証方式リストの名前を指定すると、PPP は、指定した方式リストに定義されている方式を使用して、接続を認証しようとします。AAA をイネーブルにし、名前で定義されている方式リストがない場合、PPP は、デフォルトに定義されている方式を使用して接続を認証しようとします。**one-time** キーワードを指定して **ppp authentication** コマンドを使用すると、認証中にワンタイム パスワードをサポートできます。

if-needed キーワードを使用できるのは、TACACS または拡張 TACACS を使用している場合だけです。**if-needed** キーワードを指定して **ppp authentication** コマンドを使用することは、現在のコール期間中にリモート デバイスがまだ認証されていない場合にだけ、PPP が MS-CHAP を介してリモート デバイスを認証することを示します。リモート デバイスが、標準のログイン手順で認証を受け、EXEC プロンプトから PPP を開始した場合、**ppp authentication chap if-needed** が設定されていれば、PPP は MS-CHAP を介して認証しません。

（注）　MS-CHAP を使用する PPP 認証と、ユーザ名認証を併用する場合、ローカル ユーザ名 / パスワード データベースに MS-CHAP シークレットを含める必要があります。ユーザ名認証の詳細については、「ユーザ名認証の確立」の項を参照してください。

認証の例

ここでは、認証設定の例を紹介します。

RADIUS 認証の例

ここでは、RADIUS を使用する 2 つの設定例を紹介します。

次に、RADIUS を使用して認証および認可を行うようにルータを設定する例を示します。

```
aaa authentication login radius-login group radius local
aaa authentication ppp radius-ppp if-needed group radius
aaa authorization exec default group radius if-authenticated
aaa authorization network default group radius
line 3
login authentication radius-login
interface serial 0
ppp authentication radius-ppp
```

この RADIUS 認証および認可設定のサンプル行は、次のように定義されます。

- **aaa authentication login radius-login group radius local** コマンドを実行すると、ルータは、ログイン プロンプトで認証に RADIUS を使用するように設定されます。RADIUS がエラーを返すと、ユーザはローカル データベースを使用して認証されます。
- **aaa authentication ppp radius-ppp if-needed group radius** コマンドを実行すると、ユーザがまだログインしていない場合、Cisco IOS ソフトウェアは CHAP または PAP による PPP 認証を使用するように設定されます。EXEC ファシリティによってユーザが認証済みの場合、PPP 認証は実行されません。
- **aaa authorization exec default group radius if-authenticated** コマンドを実行すると、autocommand や特権レベルなど、EXEC 認可時に使用される情報について、RADIUS データベースに照会されます。ただし、ユーザの認証が成功した場合にだけ、権限が付与されます。
- **aaa authorization network default group radius** コマンドを実行すると、ネットワーク認可、アドレス割り当て、および他のアクセス リストについて RADIUS に照会されます。
- **login authentication radius-login** コマンドを使用すると、ライン 3 について radius-login 方式リストがイネーブルになります。
- **ppp authentication radius-ppp** コマンドを使用すると、シリアル インターフェイス 0 について radius-ppp 方式リストがイネーブルになります。

次に、ユーザ名とパスワードの入力を求め、その内容を確認し、ユーザの EXEC レベルを認可し、特権レベル 2 の認可方式として指定するように、ルータを設定する例を示します。この例では、ユーザ名プロンプトにローカル ユーザ名を入力すると、そのユーザ名が認証に使用されます。

ローカル データベースを使用してユーザが認証されると、RADIUS 認証からのデータは保存されないため、RADIUS を使用する EXEC 認可は失敗します。また、この方式リストではローカル データベースを使用して autocommand を検索します。autocommand がない場合、ユーザは EXEC ユーザになります。次に、ユーザが特権レベル 2 に設定されているコマンドを発行しようとすると、TACACS+ を使用してコマンドの認可が試行されます。

```
aaa authentication login default group radius local
aaa authorization exec default group radius local
aaa authorization command 2 default group tacacs+ if-authenticated
radius-server host 172.16.71.146 auth-port 1645 acct-port 1646
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-req
```

この RADIUS 認証および認可設定のサンプル行は、次のように定義されます。

- **aaa authentication login default group radius local** コマンドにより、RADIUS（RADIUS が応答しない場合はルータのローカル ユーザ データベース）がユーザ名およびパスワードを確認するように指定します。
- **aaa authorization exec default group radius local** コマンドにより、RADIUS を使用してユーザが認証される場合、ユーザの EXEC レベルの設定に RADIUS 認証情報を使用するように指定します。RADIUS 情報が使用されない場合、このコマンドにより、EXEC 認可にローカル ユーザ データベースが使用されるように指定します。
- **aaa authorization command 2 default group tacacs+ if-authenticated** コマンドにより、すでにユーザの認証が成功している場合、特権レベル 2 に設定されているコマンドに TACACS+ 認可を指定します。
- **radius-server host 172.16.71.146 auth-port 1645 acct-port 1646** コマンドにより、RADIUS サーバ ホストの IP アドレス、認証要求の UDP 宛先ポート、およびアカウンティング要求の UDP 宛先ポートを指定します。
- **radius-server attribute 44 include-in-access-req** コマンドにより、access-request パケットで RADIUS アトリビュート 44（Acct-Session-ID）を送信します。
- **radius-server attribute 8 include-in-access-req** コマンドにより、access-request パケットで RADIUS アトリビュート 8（Framed-IP-Address）を送信します。

TACACS+ 認証の例

次に、PPP 認証に使用するセキュリティ プロトコルとして TACACS+ を設定する例を示します。

```
aaa new-model
aaa authentication ppp test group tacacs+ local
interface serial 0
ppp authentication chap pap test
tacacs-server host 10.1.2.3
tacacs-server key goaway
```

この TACACS+ 認証設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。

- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「test」を定義します。キーワード **group tacacs+** は、TACACS+ を介して認証を実行することを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。
- **interface** コマンドにより、回線を選択します。
- **ppp authentication** コマンドにより、この回線に test 方式リストを適用します。
- **tacacs-server host** コマンドにより、TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。
- **tacacs-server key** コマンドにより、共有暗号化キーを「goaway」に定義します。

次に、PPP に AAA 認証を設定する例を示します。

```
aaa authentication ppp default if-needed group tacacs+ local
```

この例のキーワード **default** は、デフォルトですべてのインターフェイスに PPP 認証が適用されることを示します。**if-needed** キーワードは、ユーザが ASCII ログイン手順を介してすでに認証済みの場合、PPP は不要なので、スキップできることを示します。認証が必要な場合、キーワード **group tacacs+** は、認証が TACACS+ を介して実行されることを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。

次に、PAP に同じ認証アルゴリズムを作成し、「default」ではなく「MIS-access」の方式リストを呼び出す例を示します。

```
aaa authentication ppp MIS-access if-needed group tacacs+ local
interface serial 0
ppp authentication pap MIS-access
```

この例では、リストはどのインターフェイスにも適用されないため（自動的にすべてのインターフェイスに適用されるデフォルト リストとは異なります）、管理者は **interface** コマンドを使用して、この認証スキームを適用するインターフェイスを選択する必要があります。次に、管理者は **ppp authentication** コマンドを使用して、選択したインターフェイスにこの方式リストを適用する必要があります。

Kerberos 認証の例

ログイン認証方式として Kerberos を指定するには、次のコマンドを使用します。

```
aaa authentication login default krb5
```

PPP に Kerberos 認証を指定するには、次のコマンドを使用します。

```
aaa authentication ppp default krb5
```

AAA スケーラビリティの例

次に、セキュリティ プロトコルとして RADIUS による AAA を使用する一般的なセキュリティ設定例を示します。この例では、ネットワーク アクセス サーバは、16 バックアップ プロセスを割り当てて PPP に対する AAA 要求を処理するように設定されています。

```
aaa new-model
radius-server host alcatraz
radius-server key myRaDiUSpassWoRd
radius-server configure-nas
```

```
username root password ALongPassword
aaa authentication ppp dialins group radius local
aaa authentication login admins local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa processes 16
line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin
interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication pap dialins
```

この RADIUS AAA 設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは、AAA ネットワーク セキュリティ サービスをイネーブルにします。
- **radius-server host** コマンドは RADIUS サーバ ホストの名前を定義します。
- **radius-server key** コマンドはネットワーク アクセス サーバと RADIUS サーバ ホスト間の共有秘密テキスト ストリングを定義します。
- **radius-server configure-nas** コマンドは、デバイスが最初に起動したときに、Cisco ルータまたはアクセス サーバがスタティック ルートと IP プール定義について RADIUS サーバに照会するように定義します。
- **username** コマンドはユーザ名とパスワードを定義します。これらの情報は、PPP Password Authentication Protocol（PAP; パスワード認証プロトコル）認証での発信元の身元確認に使用されます。
- **aaa authentication ppp dialins group radius local** コマンドで、RADIUS 認証を示す認証方式リスト「dialins」を定義します。次に、（RADIUS サーバが応答しない場合）PPP を使用するシリアル回線にはローカル認証が使用されます。
- **aaa authentication login admins local** コマンドは、ログイン認証の別の方式リスト「admins」を定義します。
- **aaa authorization network default group radius local** コマンドは、アドレスと他のネットワークパラメータを RADIUS ユーザに割り当てるために使用されます。
- **aaa accounting network default start-stop group radius** コマンドで、PPP の使用状況を追跡します。
- **aaa processes** コマンドにより、PPP に対する AAA 要求を処理するために 16 バックグラウンド プロセスを割り当てます。
- **line** コマンドはコンフィギュレーション モードをグローバル コンフィギュレーションからラインコンフィギュレーションに切り替え、設定対象の回線を指定します。
- **autoselect ppp** コマンドは、選択した回線上で PPP セッションを自動的に開始できるように Cisco IOS ソフトウェアを設定します。
- **autoselect during-login** コマンドを使用して、Return キー押さずにユーザ名およびパスワードのプロンプトを表示します。ユーザがログインすると、autoselect 機能（この場合は PPP）が開始します。
- **login authentication admins** コマンドは、ログイン認証の「admins」方式リストを適用します。
- **modem dialin** コマンドは選択した回線に接続されているモデムを設定し、着信コールだけを受け入れるようにします。
- **interface group-async** コマンドは非同期インターフェイス グループを選択して定義します。

- **group-range** コマンドはインターフェイス グループのメンバの非同期インターフェイスを定義します。
- **encapsulation ppp** コマンドは指定のインターフェイスに使用される PPP をカプセル化方式として設定します。
- **ppp authentication pap dialins** コマンドは「dialins」方式リストを指定したインターフェイスに適用します。

ログイン バナーと失敗バナーの例

次に、ユーザがシステムにログインするときに表示されるログイン バナー（この場合、「Unauthorized Access Prohibited」というフレーズ）を設定する例を示します。アスタリスク（*）はデリミタとして使用されます（RADIUS はデフォルト ログイン認証方式として指定されます）。

```
aaa new-model
aaa authentication banner *Unauthorized Access Prohibited*
aaa authentication login default group radius
```

この設定によって、次のログイン バナーが生成されます。

```
Unauthorized Access Prohibited
Username:
```

次に、ユーザかシステムにログイン使用として失敗したときに表示される、失敗ログイン バナー（この場合、「Failed login.Try again.」というフレーズ）を追加で設定する例を示します。アスタリスク（*）はデリミタとして使用されます（RADIUS はデフォルト ログイン認証方式として指定されます）。

```
aaa new-model
aaa authentication banner *Unauthorized Access Prohibited*
aaa authentication fail-message *Failed login. Try again.*
aaa authentication login default group radius
```

この設定で、次のログイン バナーと失敗ログイン バナーが生成されます。

```
Unauthorized Access Prohibited
Username:
Password:
Failed login. Try again.
```

AAA パケット オブ ディスコネクト サーバ キーの例

次に、Packet of Disconnect（POD; パケット オブ ディスコネクト）を設定する例を示します。その結果、特定のセッション アトリビュートが指定されると、ネットワーク アクセス サーバ（NAS）の接続が終了します。

```
aaa new-model
aaa authentication ppp default radius
aaa accounting network default start-stop radius
aaa accounting delay-start
aaa pod server server-key xyz123
radius-server host 172.16.0.0 non-standard
radius-server key rad123
```

二重認証の例

ここでは、二重認証に使用できる設定例を示します。実際のネットワークおよびセキュリティ要件によっては、この例とは大幅に異なる可能性があります。

ここでは、次の設定例について説明します。

- 「二重認証による AAA のローカル ホストの設定例」（P.50）
- 「第 1 段階の（PPP）認証と認可に関する AAA サーバの設定例」（P.50）
- 「第 2 段階の（Per-User）認証と認可に関する AAA サーバの設定例」（P.51）
- 「TACACS+ による設定完了の例」（P.52）

（注） 設定例には、特定の IP アドレスと他の特定の情報が含まれます。この情報は説明のための例であり、実際の設定には異なる IP アドレス、異なるユーザ名とパスワード、異なる認可ステートメントを使用します。

二重認証による AAA のローカル ホストの設定例

次の 2 つの例では、PPP とログイン認証、およびネットワークと EXEC 認可に AAA を使用するようにローカル ホストを設定する方法を示します。一方の例は RADIUS、もう一方は TACACS+ の例です。

いずれの例でも、先頭の 3 行で AAA を設定し、特定のサーバを AAA サーバとして設定しています。続く 2 行で PPP およびログイン認証に AAA を設定し、最後の 2 行でネットワークおよび EXEC 認可を設定します。最後の行が必要なのは、**access-profile** コマンドを autocommand として実行する場合だけです。

次に、RADIUS AAA サーバを使用するルータ設定の例を示します。

```
aaa new-model
radius-server host secureserver
radius-server key myradiuskey
aaa authentication ppp default group radius
aaa authentication login default group radius
aaa authorization network default group radius
aaa authorization exec default group radius
```

次に、TACACS+ サーバを使用するルータ設定の例を示します。

```
aaa new-model
tacacs-server host security
tacacs-server key mytacacskey
aaa authentication ppp default group tacacs+
aaa authentication login default group tacacs+
aaa authorization network default group tacacs+
aaa authorization exec default group tacacs+
```

第 1 段階の（PPP）認証と認可に関する AAA サーバの設定例

次に、AAA サーバでの設定例を示します。また、RADIUS 用の AAA 設定例の一部を示します。

TACACS+ サーバも同様に設定できます。詳細については、「TACACS+ による設定完了の例」（P.52）を参照してください。

この例では、二重認証の第 1 段階で CHAP によって認証される「host」というリモート ホストに関する認証/認可を定義します。ACL AV ペアは、リモート ホストによる Telnet 接続をローカル ホストに制限しています。ローカル ホストの IP アドレスは 10.0.0.2 です。

次に、RADIUS 用の AAA サーバの設定例を一部示します。

```
hostx   Password = "welcome"
        User-Service-Type = Framed-User,
        Framed-Protocol = PPP,
        cisco-avpair = "lcp:interface-config=ip unnumbered ethernet 0",
        cisco-avpair = "ip:inacl#3=permit tcp any 172.21.114.0 0.0.0.255 eq telnet",
        cisco-avpair = "ip:inacl#4=deny icmp any any",
        cisco-avpair = "ip:route#5=10.0.0.0 255.0.0.0",
        cisco-avpair = "ip:route#6=10.10.0.0 255.0.0.0",
        cisco-avpair = "ipx:inacl#3=deny any"
```

第 2 段階の（Per-User）認証と認可に関する AAA サーバの設定例

ここでは、RADIUS サーバでの AAA 設定例の一部を示します。これらの設定では、ユーザ名が「patuser」のユーザ（Pat）の認証と認可を定義します。このユーザは、二重認証の第 2 段階でユーザ認証されます。

TACACS+ サーバも同様に設定できます。詳細については、「TACACS+ による設定完了の例」（P.52）を参照してください。

3 つの例は、**access-profile** コマンドの 3 つの各形式で使用できる RADIUS AAA 設定の例を示します。

最初の例は、**access-profile** コマンドのデフォルト フォーム（キーワードなし）で機能する AAA 設定例の一部を示します。1 つの ACL AV ペアのみが定義されます。また、この例では autocommand として **access-profile** コマンドも設定します。

```
patuser   Password = "welcome"
          User-Service-Type = Shell-User,
          cisco-avpair = "shell:autocmd=access-profile"
          User-Service-Type = Framed-User,
          Framed-Protocol = PPP,
          cisco-avpair = "ip:inacl#3=permit tcp any host 10.0.0.2 eq telnet",
          cisco-avpair = "ip:inacl#4=deny icmp any any"
```

2 番めの例は、**access-profile** コマンドの **access-profile merge** 形式で機能する AAA 設定例の一部を示します。また、この例では autocommand として **access-profile merge** コマンドも設定します。

```
patuser   Password = "welcome"
          User-Service-Type = Shell-User,
          cisco-avpair = "shell:autocmd=access-profile merge"
          User-Service-Type = Framed-User,
          Framed-Protocol = PPP,
          cisco-avpair = "ip:inacl#3=permit tcp any any"
          cisco-avpair = "ip:route=10.0.0.0 255.255.0.0",
          cisco-avpair = "ip:route=10.1.0.0 255.255.0.0",
          cisco-avpair = "ip:route=10.2.0.0 255.255.0.0"
```

3 番めの例は、**access-profile** コマンドの **access-profile replace** 形式で機能する AAA 設定例の一部を示します。また、この例では autocommand として **access-profile replace** コマンドも設定します。

```
patuser   Password = "welcome"
          User-Service-Type = Shell-User,
          cisco-avpair = "shell:autocmd=access-profile replace"
          User-Service-Type = Framed-User,
          Framed-Protocol = PPP,
          cisco-avpair = "ip:inacl#3=permit tcp any any",
          cisco-avpair = "ip:inacl#4=permit icmp any any",
          cisco-avpair = "ip:route=10.10.0.0 255.255.0.0",
```

```
cisco-avpair = "ip:route=10.11.0.0 255.255.0.0",
cisco-avpair = "ip:route=10.12.0.0 255.255.0.0"
```

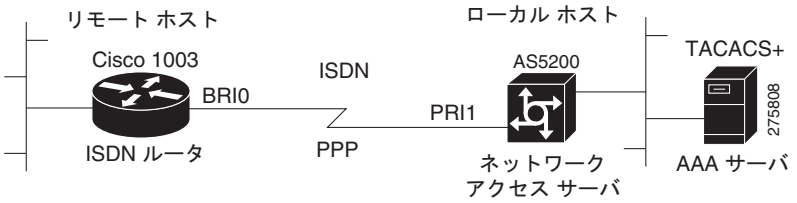
TACACS+ による設定完了の例

この例では、リモート ホスト（二重認証の第 1 段階で使用）および特定のユーザ（二重認証の第 2 段階でしよう）の両方向けの、TACACS+ 認可プロファイルの設定を示します。この TACACS+ の例には、前の RADIUS の例とほぼ同じ設定情報が使用されます。

この設定例は、リモート ホスト「host」および 3 ユーザ（ユーザ名が「pat_default」、「pat_merge」、および「pat_replace」）の TACACS+ サーバ上にある認証/認可プロファイルを示します。これら 3 つのユーザ名の設定は、**access-profile** コマンドの 3 種類のフォームに対応する異なる設定を示しています。また、3 つのユーザ設定は、**access-profile** コマンドの各形式について autocommand の設定方法も示しています。

図 3 にトポロジを示します。図の後に、TACACS+ 設定ファイルの例を示します。

図 3　　二重認証のトポロジ例



この設定例は、リモート ホスト「host」および 3 ユーザ（ユーザ名が「pat_default」、「pat_merge」、および「pat_replace」）の TACACS+ サーバ上にある認証/認可プロファイルを示します。

```
key = "mytacacskey"

default authorization = permit


#----------------------------Remote Host (BRI)------------------------
#
# This allows the remote host to be authenticated by the local host
# during fist-stage authentication, and provides the remote host
# authorization profile.
#
#---------------------------------------------------------------------

user = hostx
{
    login = cleartext "welcome"
    chap = cleartext "welcome"


    service = ppp protocol = lcp {
                interface-config="ip unnumbered ethernet 0"
    }

    service = ppp protocol = ip {
            # It is important to have the hash sign and some string after
            # it. This indicates to the NAS that you have a per-user
            # config.

            inacl#3="permit tcp any 172.21.114.0 0.0.0.255 eq telnet"
            inacl#4="deny icmp any any"
```

```
            route#5="10.0.0.0 255.0.0.0"
            route#6="10.10.0.0 255.0.0.0"
    }

    service = ppp protocol = ipx {
            # see previous comment about the hash sign and string, in protocol = ip
            inacl#3="deny any"
    }


}


#------------------- "access-profile" default user "only acls" ------------------
#
# Without arguments, access-profile removes any access-lists it can find
# in the old configuration (both per-user and per-interface), and makes sure
# that the new profile contains ONLY access-list definitions.
#
#-------------------------------------------------------------------------------

user = pat_default
{
        login = cleartext "welcome"
        chap = cleartext "welcome"

        service = exec

        {
                # This is the autocommand that executes when pat_default logs in.
                autocmd = "access-profile"
        }

        service = ppp protocol = ip {
                # Put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IP
                # access-lists (not even the ones installed prior to
                # this)!

                inacl#3="permit tcp any host 10.0.0.2 eq telnet"
                inacl#4="deny icmp any any"
        }


        service = ppp protocol = ipx {
                # Put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IPX
                # access-lists (not even the ones installed prior to
                # this)!
        }


}


#-------------------- "access-profile merge" user --------------------------
#
# With the 'merge' option, first all old access-lists are removed (as before),
# but then (almost) all AV pairs are uploaded and installed. This will allow
# for uploading any custom static routes, sap-filters, and so on, that the user
# may need in his or her profile. This needs to be used with care, as it leaves
```

```
# open the possibility of conflicting configurations.
#
#-----------------------------------------------------------------------------

user = pat_merge
{
        login = cleartext "welcome"
        chap = cleartext "welcome"


        service = exec
        {
                # This is the autocommand that executes when pat_merge logs in.
                autocmd = "access-profile merge"
        }

        service = ppp protocol = ip
        {
                # Put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IP
                # access-lists (not even the ones installed prior to
                # this)!

                inacl#3="permit tcp any any"
                route#2="10.0.0.0 255.255.0.0"
                route#3="10.1.0.0 255.255.0.0"
                route#4="10.2.0.0 255.255.0.0"

        }

        service = ppp protocol = ipx
        {
                # Put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IPX
                # access-lists (not even the ones installed prior to
                # this)!

        }

}


#--------------------- "access-profile replace" user ----------------------------
#
# With the 'replace' option, ALL old configuration is removed and ALL new
# configuration is installed.
#
# One caveat: access-profile checks the new configuration for address-pool and
# address AV pairs. As addresses cannot be renegotiated at this point, the
# command will fail (and complain) when it encounters such an AV pair.
# Such AV pairs are considered to be "invalid" for this context.
#-------------------------------------------------------------------------------


user = pat_replace
{
        login = cleartext "welcome"
        chap = cleartext "welcome"


        service = exec
        {
```

```
                # This is the autocommand that executes when pat_replace logs in.
                autocmd = "access-profile replace"
        }

        service = ppp protocol = ip
        {
                # Put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IP
                # access-lists (not even the ones installed prior to
                # this)!

                inacl#3="permit tcp any any"
                inacl#4="permit icmp any any"


                route#2="10.10.0.0 255.255.0.0"
                route#3="10.11.0.0 255.255.0.0"
                route#4="10.12.0.0 255.255.0.0"
        }

        service = ppp protocol = ipx
        {
                # put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IPX
                # access-lists (not even the ones installed prior to
                # this)!
        }

}
```

自動二重認証の例

次に、自動二重認証が設定された Cisco 2509 ルータの設定ファイル全体の例を示します。自動二重認証に適用されるコンフィギュレーション コマンドは、2 つのアスタリスク（**）を使用した記述よりも優先されます。

```
Current configuration:
!
version 11.3
no service password-encryption
!
hostname myrouter
!
!
! **The following AAA commands are used to configure double authentication:
!
! **The following command enables AAA:
aaa new-model
! **The following command enables user authentication via the TACACS+ AAA server:
aaa authentication login default group tacacs+
aaa authentication login console none
! **The following command enables device authentication via the TACACS+ AAA server:
aaa authentication ppp default group tacacs+
! **The following command causes the remote user's authorization profile to be
! downloaded from the AAA server to the Cisco 2509 router when required:
aaa authorization exec default group tacacs+
! **The following command causes the remote device's authorization profile to be
! downloaded from the AAA server to the Cisco 2509 router when required:
aaa authorization network default group tacacs+
```

```
enable password mypassword
!
ip host blue 172.21.127.226
ip host green 172.21.127.218
ip host red 172.21.127.114
ip domain-name example.com
ip name-server 172.16.2.75
! **The following command globally enables automated double authentication:
ip trigger-authentication timeout 60 port 7500
isdn switch-type basic-5ess
!
!
interface Ethernet0
 ip address 172.21.127.186 255.255.255.248
 no ip route-cache
 no ip mroute-cache
 no keepalive
 ntp disable
 no cdp enable
!
interface Virtual-Template1
 ip unnumbered Ethernet0
 no ip route-cache
 no ip mroute-cache
!
interface Serial0
 ip address 172.21.127.105 255.255.255.248
 encapsulation ppp
 no ip mroute-cache
 no keepalive
 shutdown
 clockrate 2000000
 no cdp enable
!
interface Serial1
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 no cdp enable
!
! **Automated double authentication occurs via the ISDN BRI interface BRI0:
interface BRI0
 ip unnumbered Ethernet0
! **The following command turns on automated double authentication at this interface:
 ip trigger-authentication
! **PPP encapsulation is required:
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 dialer idle-timeout 500
 dialer map ip 172.21.127.113 name myrouter 60074
 dialer-group 1
 no cdp enable
```

```
! **The following command specifies that device authentication occurs via PPP CHAP:
 ppp authentication chap
!
router eigrp 109
 network 172.21.0.0
 no auto-summary
!
ip default-gateway 172.21.127.185
no ip classless
ip route 172.21.127.114 255.255.255.255 172.21.127.113
! **Virtual profiles are required for double authentication to work:
virtual-profile virtual-template 1
dialer-list 1 protocol ip permit
no cdp run
! **The following command defines where the TACACS+ AAA server is:
tacacs-server host 171.69.57.35 port 1049
tacacs-server timeout 90
! **The following command defines the key to use with TACACS+ traffic (required):
tacacs-server key mytacacskey
snmp-server community public RO
!
line con 0
 exec-timeout 0 0
 login authentication console
line aux 0
 transport input all
line vty 0 4
 exec-timeout 0 0
 password lab
!
end
```

MS-CHAP の例

次に、MS-CHAP を使用する PPP 認証に Cisco AS5200 Universal Access Server（AAA および RADIUS セキュリティ サーバとの通信で有効）を設定する例を示します。

```
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins group radius local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius

username root password ALongPassword

radius-server host alcatraz
radius-server key myRaDiUSpassWoRd

interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication ms-chap dialins

line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin
```

この RADIUS AAA 設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは、AAA ネットワーク セキュリティ サービスをイネーブルにします。
- **aaa authentication login admins local** コマンドは、ログイン認証の別の方式リスト「admins」を定義します。
- **aaa authentication ppp dialins group radius local** コマンドで、RADIUS 認証を示す認証方式リスト「dialins」を定義します。次に、（RADIUS サーバが応答しない場合）PPP を使用するシリアル回線にはローカル認証が使用されます。
- **aaa authorization network default group radius local** コマンドは、アドレスと他のネットワークパラメータを RADIUS ユーザに割り当てるために使用されます。
- **aaa accounting network default start-stop group radius** コマンドで、PPP の使用状況を追跡します。
- **username** コマンドはユーザ名とパスワードを定義します。これらの情報は、PPP Password Authentication Protocol（PAP; パスワード認証プロトコル）認証での発信元の身元確認に使用されます。
- **radius-server host** コマンドは RADIUS サーバ ホストの名前を定義します。
- **radius-server key** コマンドはネットワーク アクセス サーバと RADIUS サーバ ホスト間の共有秘密テキスト ストリングを定義します。
- **interface group-async** コマンドは非同期インターフェイス グループを選択して定義します。
- **group-range** コマンドはインターフェイス グループのメンバの非同期インターフェイスを定義します。
- **encapsulation ppp** コマンドは指定のインターフェイスに使用される PPP をカプセル化方式として設定します。
- **ppp authentication ms-chap dialins** コマンドは ppp 認証方式として MS-CHAP を選択し、特定のインターフェイスに「ダイヤルイン」方式リストを適用します。
- **line** コマンドはコンフィギュレーション モードをグローバル コンフィギュレーションからラインコンフィギュレーションに切り替え、設定対象の回線を指定します。
- **autoselect ppp** コマンドは、選択した回線上で PPP セッションを自動的に開始できるように Cisco IOS ソフトウェアを設定します。
- **autoselect during-login** コマンドを使用して、Return キー押さずにユーザ名およびパスワードのプロンプトを表示します。ユーザがログインすると、autoselect 機能（この場合は PPP）が開始します。
- **login authentication admins** コマンドは、ログイン認証の「admins」方式リストを適用します。
- **modem dialin** コマンドは選択した回線に接続されているモデムを設定し、着信コールだけを受け入れるようにします。

その他の参考資料

ここでは、認証の設定機能に関する関連資料について説明します。

関連資料

内容	参照先
認可	「Configuring Authorization」モジュール
アカウンティング	「Configuring Accounting」モジュール
RADIUS サーバ	「Configuring RADIUS」モジュール
TACACS+ サーバ	「Configuring TACACS+」モジュール
Kerberos	「Configuring Kerberos」モジュール

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2903	「Generic AAA Architecture」
RFC 2904	「AAA Authorization Framework」
RFC 2906	「AAA Authorization Requirements」
RFC 2989	「Criteria for Evaluating AAA Protocols for Network Access」
RFC 5176	「Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

認証の設定に関する機能情報

表 10 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。この表には、Cisco IOS Release 12.2(1) または 12.0(3) 以降のリリースで導入または変更された機能のみを示しています。

ここに記載されていないこのテクノロジーの機能情報については、「*Select Your Product*」ページを参照し、お使いの Cisco IOS リリースの製品マニュアルに関するサポート ページを検索してください。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 10 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 10　認証の設定に関する機能情報

機能名	リリース	機能情報
認証	12.0 XE 2.1	この機能は、Cisco IOS Release 12.0 ソフトウェアで導入されました。 この機能は、Cisco IOS Release XE 2.1 ソフトウェアで導入されました。
AAA のユーザ別スケーラビリティ	12.2(27)SB 12.2(33)SR 15.0(1)M	この機能は、Cisco IOS Release 12.2(27)SB で導入されました。 この機能は、Cisco IOS Release 12.2(33)SR に統合されました。 この機能は、Cisco IOS Release 15.0(1)M に統合されました。
RADIUS：ユーザ名が空のアクセス要求を送信しないようにする CLI	12.2(33)SRD Cisco IOS XE Release 2.4	この認証機能によって、ユーザ名が空のアクセス要求が RADIUS サーバに送信されないようにします。この機能により、RADIUS サーバとの不要なやりとりを回避でき、RADIUS ログの量を少なくすることができます。 この機能に関する詳細については、次の項を参照してください。 • 「ユーザ名が空のアクセス要求が RADIUS サーバに送信されないようにする」（P.27） 次のコマンドが導入されました：**aaa authentication suppress null-username**。

表 10　認証の設定に関する機能情報（続き）

機能名	リリース	機能情報
LDAP の Active Directory との統合	15.1(1)T	この機能は、AAA の認証および認可のサポートを提供します。LDAP はディレクトリへのアクセスに使用される標準ベースのプロトコルです。RADIUS に類似したクライアント サーバ モデルをベースとしています。LDAP はシスコ デバイス上で稼動し、ユーザ認証およびネットワーク サービス アクセスに関するすべての情報を保持する中央の LDAP サーバへ認証要求を送信します。 コマンド **aaa authentication login default group ldap** が導入されました。
Change of Authorization（COA; 認可変更）	12.2(33)SXI4	Cisco IOS Release 12.2(33)SXI4 以降、Cisco IOS は RFC 5176 に定義されている RADIUS Change of Authorization（CoA; 認可変更）拡張機能をサポートします。COA 拡張機能は、一般的にプッシュ モデルに使用され、外部の Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）サーバまたはポリシー サーバからのセッションの動的再設定を考慮しています。 導入されたコマンド : **aaa server radius dynamic author**、**authentication command bounce-port ignore**、**authentication command disable-port ignore**。

認可の設定

AAA 認可機能を使用して、ユーザができることとできないことを定義します。AAA 認可をイネーブルにすると、ネットワーク アクセス サーバはユーザのプロファイルから取得した情報を使用して、ユーザの設定を設定します。このプロファイルは、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。認可が完了すると、ユーザ プロファイルの情報で許可されているサービスであれば、ユーザは要求したサービスに対するアクセス権を付与されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「認可の設定に関する機能情報」（P.16）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

前提条件

名前付き方式リストを使用して認可を設定する前に、次のタスクを実行する必要があります。

- ネットワーク アクセス サーバで AAA をイネーブルにします。
- AAA 認証を設定します。一般的に、認可は認証後に実行し、認証が適切に動作することに依存します。
- RADIUS または TACACS+ の認可が発行された場合、シスコ ネットワーク アクセス サーバが RADIUS または TACACS+ セキュリティ サーバと通信できるように、Lightweight Directory Access Protocol（LDAP）、RADIUS、または TACACS+ セキュリティ サーバの特性を定義します。
- ローカル認可が発行された場合、**username** コマンドを使用して、特定のユーザに関連付けられている権限を定義します。
- これらの前提条件に関連するマニュアルの詳細については、「関連資料」（P.14）を参照してください。

認可の設定の概要

ここでは、認可機能を設定する方法について説明します。

認可の名前付き方式リスト

認可の方式リストでは、認可の実行方法と、その方式を実行する順序を定義します。方式リストは、シーケンスで照会される認可方式（LDAP、RADIUS、TACACS+ など）を説明する単なる名前付きリストです。方式リストを使用すると、1 つまたは複数のセキュリティ プロトコルを認可に使用できるため、最初の方式が失敗した場合に備えて認可のバックアップ システムを確保できます。Cisco IOS ソフトウェアでは、特定のネットワーク サービスについてユーザを認可するために最初の方式が使用されます。その方式が応答しない場合、方式リストの次の方式が選択されます。このプロセスは、リストのいずれかの認可方式と通信に成功するか、定義されているすべての方式が試行されるまで継続されます。

（注） Cisco IOS ソフトウェアでは、前の方式からの応答がない場合にのみ、リストの次の認可方式が試行されます。このサイクルの任意の時点で認可が失敗した場合（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からユーザ サービスの拒否応答が返される場合）、認可プロセスは停止し、その他の認可方式は試行されません。

方式リストは、要求した認可タイプに固有です。

- **Auth-proxy**：ユーザ別に特定のセキュリティ ポリシーを適用します。認証プロキシのコンフィギュレーション マニュアルの詳細については、「関連資料」（P.14）を参照してください。

- **Commands**：ユーザが発行する EXEC モード コマンドに適用します。コマンドの認可は、特定の特権レベルに関連付けられた、グローバル コンフィギュレーション コマンドなどのすべての EXEC モード コマンドについて、認可を試行します。
- **EXEC**：ユーザ EXEC ターミナル セッションに関連付けられたアトリビュートに適用します。
- **Network**：ネットワーク接続に適用します。これには、PPP、SLIP、または ARAP 接続が含まれます。
- **Reverse Access**：リバース Telnet セッションに適用されます。

名前付き方式リストが作成されると、指定した認可タイプに固有の認可方式のリストが定義されます。

定義されると、方式リストを特定の回線またはインターフェイスに適用してから、定義済み方式のいずれかを実行する必要があります。唯一の例外は、デフォルトの方式リスト（「default」という名前が指定されています）です。特定の認可タイプ用の **aaa authorization** コマンドが、名前付き方式リストを指定せずに発行されると、デフォルトの方式リストは、名前付き方式リストが明示的に定義されている場合を除き、すべてのインターフェイスまたは回線へ自動的に適用されます（定義した方式リストは、デフォルトの方式リストよりも優先されます）。デフォルトの方式リストが定義されていない場合、デフォルトで認可は実行されません。

AAA 認可方式

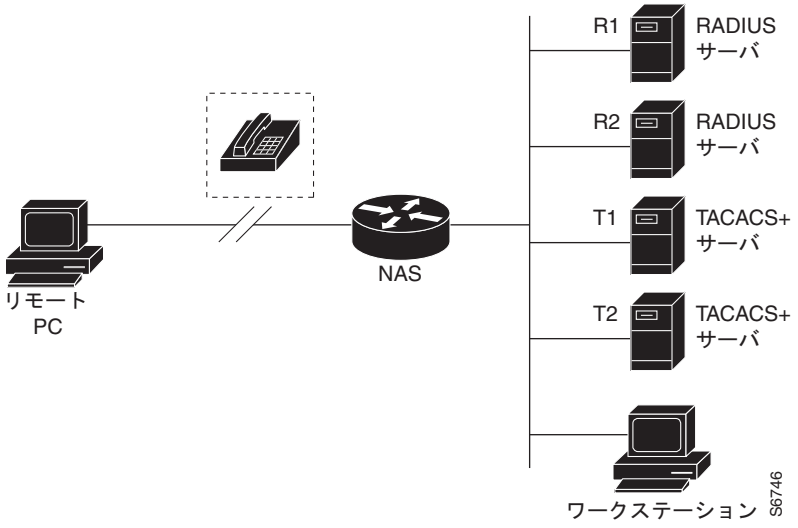
AAA は 5 種類の認可方式をサポートしています。

- TACACS+：ネットワーク アクセス サーバは、TACACS+ セキュリティ デーモンと認可情報を交換します。TACACS+ 認可は、アトリビュート値ペアを関連付けることでユーザに特定の権限を定義します。アトリビュートペアは適切なユーザとともに TACACS+ セキュリティ サーバのデータベースに保存されます。
- If-Authenticated：ユーザが認証に成功した場合、ユーザは要求した機能にアクセスできます。
- **None**：ネットワーク アクセス サーバは、認可情報を要求しません。認可は、この回線/インターフェイスで実行されません。
- Local：ルータまたはアクセス サーバは、**username** コマンドの定義に従って、ローカル データベースに問い合わせて、たとえばユーザに固有の権限を認可します。ローカル データベースでは制御できるのは、一部の機能だけです。
- LDAP：ネットワーク アクセス サーバは RADIUS セキュリティ サーバからの認可情報を要求します。LDAP 認可では、アトリビュートを関連付けることでユーザに固有の権限を定義します。アトリビュートは適切なユーザとともに LDAP サーバ上のデータベースに保存されます。
- RADIUS：ネットワーク アクセス サーバは RADIUS セキュリティ サーバからの認可情報を要求します。RADIUS 認可では、アトリビュートを関連付けることでユーザに固有の権限を定義します。アトリビュートは適切なユーザとともに RADIUS サーバ上のデータベースに保存されます。

方式リストとサーバ グループ

サーバ グループは、方式リストに使用する既存の LDAP、RADIUS、または TACACS+ サーバ ホストをグループ化する方法の 1 つです。図 1 に、4 台のセキュリティ サーバ（R1 と R2 は RADIUS サーバ、T1 と T2 は TACACS+ サーバ）が設置された一般的な AAA ネットワーク設定を示します。R1 と R2 で RADIUS サーバのグループを構成します。T1 と T2 で TACACS+ サーバのグループを構成します。

図 1　一般的な AAA ネットワーク設定



サーバ グループを使用して、設定したサーバ ホストのサブセットを指定し、特定のサービスに使用します。たとえば、サーバ グループを使用すると、R1 および R2 を 1 つのサーバ グループとして定義し、T1 および T2 を別のサーバ グループとして定義できます。R1 と T1 を方式リストに指定することや、R2 と T2 を方式リストに指定することができます。そのため、RADIUS および TACACS+ のリソースを割り当てる場合の柔軟性が高くなります。

サーバ グループには、1 台のサーバに対して複数のホスト エントリを含めることができます。エントリごとに固有の識別情報を設定します。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。つまり、この固有識別情報を使用して、ある IP アドレスに位置する 1 台のサーバ上に複数の UDP ポートが存在する場合、それぞれの UDP ポートに対して RADIUS 要求を送信できます。1 台の RADIUS サーバ上にある異なる 2 つのホスト エントリが 1 つのサービス（認可など）に設定されている場合、設定されている 2 番めのホスト エントリは最初のホスト エントリのフェールオーバー バックアップとして動作します。この例の場合、最初のホスト エントリがアカウンティング サービスの提供に失敗すると、同じデバイスに設定されている 2 番めのホスト エントリを使用してアカウンティング サービスを提供するように、ネットワーク アクセス サーバが試行します（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

サーバ グループの設定および DNIS 番号に基づくサーバ グループの設定の詳細については、「Configuring LDAP」、「Configuring RADIUS」、または「Configuring TACACS+」の各フィーチャ モジュールを参照してください。

AAA 認可タイプ

Cisco IOS ソフトウェアは、5 種類の認可をサポートしています。

- **Auth-proxy**：ユーザ別に特定のセキュリティ ポリシーを適用します。認証プロキシのコンフィギュレーション マニュアルの詳細については、「関連資料」（P.14）を参照してください。
- **Commands**：ユーザが発行する EXEC モード コマンドに適用します。コマンドの認可は、特定の特権レベルに関連付けられた、グローバル コンフィギュレーション コマンドなどのすべての EXEC モード コマンドについて、認可を試行します。
- **EXEC**：ユーザ EXEC ターミナル セッションに関連付けられたアトリビュートに適用します。

- **Network**：ネットワーク接続に適用します。これには、PPP、SLIP、または ARAP 接続が含まれます。
- **Reverse Access**：リバース Telnet セッションに適用されます。
- Configuration：AAA サーバからのコンフィギュレーションのダウンロードに適用されます。
- IP Mobile：IP モバイル サービスの認可に適用されます。

認可のアトリビュート値ペア

RADIUS および TACACS+ の認可はいずれも、セキュリティ サーバのデータベースに保存されているアトリビュートを処理することで、ユーザに固有の権限を定義します。RADIUS と TACACS+ のいずれも、アトリビュートはセキュリティ サーバに定義され、ユーザに関連付けられ、ユーザの接続に適用されるネットワーク アクセス サーバに送信されます。

サポートされる RADIUS アトリビュートと TACACS+ アトリビュート値のペアの詳細については、「関連資料」（P.14）を参照してください。

認可の設定方法

ここでは、次の設定手順について説明します。

- 「名前付き方式リストによる AAA 認可の設定」
- 「グローバル コンフィギュレーション コマンドの認可のディセーブル化」
- 「リバース Telnet の認可の設定」

詳細については、「認可設定の例」（P.8）を参照してください。

名前付き方式リストによる AAA 認可の設定

名前付き方式リストを使用して AAA 認可を設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authorization** {**auth-proxy** | **network** | **exec** | **commands** *level* | **reverse-access** | **configuration** | **ipmobile**} {**default** | *list-name*} [*method1* [*method2...*]]
4. **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
5. **authorization** {**arap** | **commands** *level* | **exec** | **reverse-access**} {**default** | *list-name*}

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	Router(config)# **aaa authorization** {**auth-proxy** | **network** | **exec** | **commands** *level* | **reverse-access** | **configuration** | **ipmobile**} {**default** | *list-name*} [*method1* [*method2...*]]	特定の認可タイプの認可方式リストを作成し、認可をイネーブルにします。
ステップ 4	Router(config)# **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*] または Router(config)# interface interface-type interface-number	認可方式リストを適用する回線について、ライン コンフィギュレーション モードを開始します。 または、認可方式リストを適用するインターフェイスについて、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	Router(config-line)# **authorization** {**arap** | **commands** *level* | **exec** | **reverse-access**} {**default** | *list-name*} または Router(config-line)# **ppp authorization** {**default** | *list-name*}	1 つの回線または複数回線に認可リストを適用します。 または、1 つのインターフェイスまたは複数インターフェイスに認可リストを適用します。

ここでは、次の内容について説明します。

- 「認可タイプ」
- 「認可方式」

認可タイプ

名前付き認可方式リストは、指定される認可の種類によって変わります。

ユーザ別に固有のセキュリティ ポリシーを適用する認可をイネーブルにする方式リストを作成するには、**auth-proxy** キーワードを使用します。認証プロキシのコンフィギュレーション マニュアルの詳細については、「関連資料」（P.14）を参照してください。

すべてのネットワーク関連サービス要求（SLIP、PPP、PPP NCP、ARAP などのプロトコル）について認可をイネーブルにする方式リストを作成するには、**network** キーワードを使用します。

ユーザが EXEC シェルを実行できるかどうかを認可で決定できるように方式リストを作成するには、**exec** キーワードを使用します。

特定の特権レベルに関連付けられた個々の EXEC コマンドについて認可をイネーブルにする方式リストを作成するには、**commands** キーワードを使用します（これによって、0 ～ 15 の指定したコマンドレベルに関連付けられたすべてのコマンドを認可できます）。

リバース Telnet 機能について認可をイネーブルにする方式リストを作成するには、**reverse-access** キーワードを使用します。

認可方式

ネットワーク アクセス サーバから TACACS+ セキュリティ サーバを介して認可情報を要求するには、**group tacacs+** *method* キーワードを指定して **aaa authorization** コマンドを使用します。TACACS+ セキュリティ サーバを使用して認可を設定する詳細な方法については、「Configuring TACACS+」フィーチャ モジュールを参照してください。TACACS+ サーバが、PPP や ARA などのネットワーク サービスの使用を認可できるようにする例については、「TACACS+ 認可：例」（P.10）を参照してください。

ユーザが認証済みであれば、要求した機能へのアクセスを許可するには、**if-authenticated** *method* キーワードを指定して **aaa authorization** コマンドを使用します。この方式を選択する場合、すべての要求した機能は、認証済みユーザに自動的に許可されます。

特定のインターフェイスまたは回線から認可を実行しない方がよい場合があります。指定した回線またはインターフェイスで認可動作を停止するには、**none** *method* キーワードを使用します。この方式を選択すると、すべてのアクションについて認可はディセーブルになります。

ローカル認可を選択するには（つまり、ルータまたはアクセス サーバがローカル ユーザ データベースに問い合わせて、ユーザが使用可能な機能を決定する場合）、**local** *method* キーワードを指定して **aaa authorization** コマンドを使用します。ローカル認可に関連する機能は、**username** グローバル コンフィギュレーション コマンドを使用して定義します。許可されている機能のリストについては、「Configuring Authentication」を参照してください。

ネットワーク アクセス サーバから LDAP セキュリティ サーバを介して認可を要求するには、**ldap** *method* キーワードを使用します。RADIUS セキュリティ サーバを使用して認可を設定する詳細な方法については、「Configuring RADIUS」フィーチャ モジュールを参照してください。

ネットワーク アクセス サーバから RADIUS セキュリティ サーバを介して認可を要求するには、**radius** *method* キーワードを使用します。RADIUS セキュリティ サーバを使用して認可を設定する詳細な方法については、「Configuring RADIUS」フィーチャ モジュールを参照してください。

ネットワーク アクセス サーバから RADIUS セキュリティ サーバを介して認可情報を要求するには、**group** *radius* method キーワードを指定して **aaa authorization** コマンドを使用します。RADIUS セキュリティ サーバを使用して認可を設定する詳細な方法については、「Configuring RADIUS」フィーチャ モジュールを参照してください。RADIUS サーバがサービスを認可できるようにする例については、「RADIUS 認可：例」（P.11）を参照してください。

（注） SLIP の認可方式リストは、関連インターフェイスで PPP に設定されているすべての方式に従います。特定のインターフェイスに定義および適用されるリストがない場合（または PPP 設定が指定されていない場合）、認可のデフォルト設定が適用されます。

グローバル コンフィギュレーション コマンドの認可のディセーブル化

commands キーワードを指定して **aaa authorization** コマンドを使用すると、その特権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（グローバル コンフィギュレーション コマンドを含む）に対して認可が試行されます。一部の EXEC レベル コマンドと同じコンフィギュレーション コマンドもあるため、認可プロセスが混乱する可能性があります。**no aaa authorization config-commands** を使用すると、ネットワーク アクセス サーバがコンフィギュレーション コマンド認可の試行を停止します。

すべてのグローバル コンフィギュレーション コマンドについて AAA 認可をディセーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# **no aaa authorization config-commands**	すべてのグローバル コンフィギュレーション コマンドについて認可をディセーブルにします。

リバース Telnet の認可の設定

Telnet は、リモート ターミナル接続に使用される標準ターミナル エミュレーション プロトコルです。通常、ネットワーク アクセス サーバにログインし、そのネットワーク アクセス サーバから Telnet を使用して他のネットワーク デバイスにアクセスします。ただし、場合によっては、リバース Telnet セッションを確立する必要があります。リバース Telnet セッションでは、反対方向の Telnet 接続（つまり、ネットワーク内部から、ネットワーク周辺にあるネットワーク アクセス サーバに対する接続）が確立されます。その接続によって、ネットワーク アクセス サーバに接続しているモデムや他のデバイスへのアクセスを取得します。リバース Telnet は、ユーザがネットワーク アクセス サーバに接続されているモデム ポートに Telnet を送信できるようにすることで、ユーザにダイヤルアウト機能を提供します。

リバース Telnet を介してアクセスできるポートのアクセス権を制御することが重要です。適切に制御しないと、たとえば、不正ユーザがモデムに自由にアクセスし、着信コールをトラップして迂回させたり、不正な宛先にコールを送信したりする可能性があります。

リバース Telnet 時の認証は、Telnet 用の標準の AAA ログイン手順を介して実行されます。通常、Telnet またはリバース Telnet セッションを確立するには、ユーザはユーザ名とパスワードを指定する必要があります。リバース Telnet 認可は、認証に加えて認可を必須にすることで、追加（オプション）レベルのセキュリティを提供します。リバース Telnet 認可をイネーブルにすることで、標準の Telnet ログイン手順を介してユーザ認証を完了した後に、RADIUS または TACACS+ を使用して、そのユーザが非同期ポートにリバース Telnet アクセスを実行できるかどうかを認可できます。

リバース Telnet 認可には次の利点があります。

- リバース Telnet アクティビティを実行しているユーザに、リバース Telnet を使用して特定の非同期ポートにアクセスする権限を付与することで、追加レベルの保護を実現しています。
- リバース Telnet 認可を管理できる（アクセス リスト以外の）代替方式があります。

ネットワーク アクセス サーバが TACACS+ または RADIUS サーバからの認可情報を要求するように設定してから、ユーザによるリバース Telnet セッションの確立を許可するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# **aaa authorization reverse-access** *method1* [*method2* ...]	ネットワーク アクセス サーバが認可情報を要求するように設定してから、ユーザによるリバース Telnet セッションの確立を許可します。

この機能によって、ネットワーク アクセス サーバは、セキュリティ サーバ（RADIUS または TACACS+）からリバース Telnet 認可情報を要求できます。セキュリティ サーバ上のユーザに固有のリバース Telnet 特権を設定する必要があります。

認可設定の例

ここでは、認可設定の例を紹介します。

名前付き方式リストの設定：例

次に、RADIUS サーバから AAA サービスを提供するために Cisco AS5300（AAA および RADIUS セキュリティ サーバとの通信で有効）を設定する例を示します。RADIUS サーバが応答に失敗すると、認証情報と認可情報についてローカル データベースへの照会が行われ、アカウンティング サービスは TACACS+ サーバによって処理されます。

```
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins group radius local
aaa authorization network scoobee group radius local
aaa accounting network charley start-stop group radius

username root password ALongPassword

radius-server host alcatraz
radius-server key myRaDiUSpassWoRd

interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication chap dialins
 ppp authorization scoobee
 ppp accounting charley

line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin
```

この RADIUS AAA 設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは、AAA ネットワーク セキュリティ サービスをイネーブルにします。
- **aaa authentication login admins local** コマンドは、ログイン認証の方式リスト「admins」を定義します。
- **aaa authentication ppp dialins group radius local** コマンドで、RADIUS 認証を示す認証方式リスト「dialins」を定義します。次に、（RADIUS サーバが応答しない場合）PPP を使用するシリアル回線にはローカル認証が使用されます。
- **aaa authorization network scoobee group radius local** コマンドで、「scoobee」というネットワーク認可方式リストを定義します。その際、PPP を使用するシリアル回線に RADIUS 認可を使用するように指定します。RADIUS サーバが応答に失敗すると、ローカル ネットワークの認可が実行されます。
- **aaa accounting network charley start-stop group radius** コマンドで、charley というネットワーク アカウンティング方式リストを定義します。その際、PPP を使用するシリアル回線に RADIUS アカウンティング サービス（この場合、特定のイベントに対する開始レコードと終了イベント）を使用するように指定します。

- **username** コマンドはユーザ名とパスワードを定義します。これらの情報は、PPP Password Authentication Protocol（PAP; パスワード認証プロトコル）認証での発信元の身元確認に使用されます。
- **radius-server host** コマンドは RADIUS サーバ ホストの名前を定義します。
- **radius-server key** コマンドはネットワーク アクセス サーバと RADIUS サーバ ホスト間の共有秘密テキスト ストリングを定義します。
- **interface group-async** コマンドは非同期インターフェイス グループを選択して定義します。
- **group-range** コマンドはインターフェイス グループのメンバの非同期インターフェイスを定義します。
- **encapsulation ppp** コマンドは指定のインターフェイスに使用される PPP をカプセル化方式として設定します。
- **ppp authentication chap dialins** コマンドは ppp 認証方式として Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）を選択し、特定のインターフェイスに「ダイヤルイン」方式リストを適用します。
- **ppp authorization scoobee** コマンドによって、scoobee ネットワーク認可方式リストは指定したインターフェイスに適用されます。
- **ppp accounting charley** コマンドによって、charley ネットワーク アカウンティング方式リストは指定したインターフェイスに適用されます。
- **line** コマンドはコンフィギュレーション モードをグローバル コンフィギュレーションからライン コンフィギュレーションに切り替え、設定対象の回線を指定します。
- **autoselect ppp** コマンドは、選択した回線上で PPP セッションを自動的に開始できるように Cisco IOS ソフトウェアを設定します。
- **autoselect during-login** コマンドを使用して、Return キー押さずにユーザ名およびパスワードのプロンプトを表示します。ユーザがログインすると、autoselect 機能（この場合は PPP）が開始します。
- **login authentication admins** コマンドは、ログイン認証の admins 方式リストを適用します。
- **modem dialin** コマンドは選択した回線に接続されているモデムを設定し、着信コールだけを受け入れるようにします。

TACACS+ 認可：例

次に、TACACS+ サーバを使用して、PPP や ARA などのネットワーク サービスの使用を認可する例を示します。TACACS+ サーバが使用不能の場合、または認可プロセス中にエラーが発生した場合、フォールバック方式（none）はすべての認可要求を許可することです。

```
aaa authorization network default group tacacs+ none
```

次に、TACACS+ を使用してネットワークの認可を許可する例を示します。

```
aaa authorization network default group tacacs+
```

次に、同じ認可を提供し、mci と att というアドレス プールも作成する例を示します。

```
aaa authorization network default group tacacs+
ip address-pool local
ip local-pool mci 172.16.0.1 172.16.0.255
ip local-pool att 172.17.0.1 172.17.0.255
```

これらのアドレス プールは、TACACS デーモンによって選択できます。デーモンの設定例を次に示します。

```
user = mci_customer1 {
    login = cleartext “some password”
    service = ppp protocol = ip {
        addr-pool=mci
    }
}

user = att_customer1 {
    login = cleartext “some other password”
    service = ppp protocol = ip {
        addr-pool=att
     }
```

RADIUS 認可：例

次に、RADIUS を使用して認可を行うようにルータを設定する方法の例を示します。

```
aaa new-model
aaa authorization exec default group radius if-authenticated
aaa authorization network default group radius
radius-server host ip
radius-server key
```

この RADIUS 認可設定のサンプル行は、次のように定義されます。

- **aaa authorization exec default group radius if-authenticated** コマンドで、ネットワーク アクセス サーバが RADIUS サーバに接続して、ユーザのログイン時にユーザが EXEC シェルを起動する権限があるかどうかを決定するように設定します。ユーザが適切に認証されていて、ネットワーク アクセス サーバが RADIUS サーバに接続するときにエラーが発生する場合、フォールバック方式は CLI の起動を許可することです。

  返される RADIUS 情報を使用して、その接続に適用される autocommand または接続アクセス リストを指定できます。

- **aaa authorization network default group radius** コマンドで、RADIUS を回するネットワーク認可を設定します。この操作は、アドレス割り当ての管理、アクセス リストのアプリケーション、および他の多様なユーザ別の数量に使用できます。

（注） この例ではフォールバック方式を指定していないため、何らかの理由で認可に失敗すると、RADIUS サーバからの応答はありません。

LDAP 認可：例

次に、LDAP を使用して認可を行うようにルータを設定する方法の例を示します。

```
aaa new-model
aaa authorization exec default group ldap if-authenticated
aaa authorization network default group ldap
```

この RADIUS 認可設定のサンプル行は、次のように定義されます。

- **aaa authorization exec default group ldap if-authenticated** コマンドで、ネットワーク アクセス サーバが LDAP サーバに接続して、ユーザのログイン時にユーザが EXEC シェルを起動する権限があるかどうかを決定するように設定します。ユーザが適切に認証されていて、ネットワーク アクセス サーバが LDAP サーバに接続するときにエラーが発生する場合、フォールバック方式は CLI の起動を許可することです。

返される LDAP 情報を使用して、その接続に適用される autocommand または接続アクセス リストを指定できます。

aaa authorization network default group ldap コマンドで、LDAP を回するネットワーク認可を設定します。このコマンドは、アドレス割り当ての管理、アクセス リストのアプリケーション、および他の多様なユーザ別の数量に使用できます。

リバース Telnet 認可：例

次に、ネットワーク アクセス サーバが TACACS+ セキュリティ サーバから認可情報を要求してから、ユーザによるリバース Telnet セッションの確立を許可する例を示します。

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization reverse-access default group tacacs+
!
tacacs-server host 172.31.255.0
tacacs-server timeout 90
tacacs-server key goaway
```

この TACACS+ リバース Telnet 認可設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは AAA をイネーブルにします。
- **aaa authentication login default group tacacs+** コマンドで、ログイン時のユーザ認証のデフォルト方式として TACACS+ を指定します。
- リバース Telnet セッションを確立しようとしているときに、**aaa authorization reverse-access default group tacacs+** コマンドで、ユーザ認可の方式として TACACS+ を指定します。
- **tacacs-server host** コマンドで、TACACS+ サーバを指定します。
- **tacacs-server timeout** コマンドで、ネットワーク アクセス サーバが TACACS+ サーバの応答を待機する期間を設定します。
- **tacacs-server key** コマンドで、ネットワーク アクセス サーバと TACACS+ デーモン間のすべての TACACS+ 通信に使用される暗号化キーを定義します。

次に、ネットワーク アクセス サーバ「maple」上のポート tty2、およびネットワーク アクセス サーバ「oak」上のポート tty5 に対するリバース Telnet アクセス権をユーザ pat に付与する汎用の TACACS+ サーバを設定する例を示します。

```
user = pat
  login = cleartext lab
  service = raccess {
    port#1 = maple/tty2
    port#2 = oak/tty5
```

（注） この例では、「maple」と「oak」には、DNS 名またはエイリアスではなく、ネットワーク アクセス サーバのホスト名が設定されています。

次に、TACACS+ サーバ（CiscoSecure）を設定して、ユーザ pat にリバース Telnet アクセス権を付与する例を示します。

```
user = pat
profile_id = 90
profile_cycle = 1
member = Tacacs_Users
service=shell {
default cmd=permit
}
```

```
service=raccess {
allow "c2511e0" "tty1" ".*"
refuse ".*" ".*" ".*"
password = clear "goaway"
```

（注） CiscoSecure は、バージョン 2.1（*x*）～ バージョン 2.2（1）のコマンドライン インターフェイスを使用して、リバース Telnet だけをサポートしています。

空の「service=raccess {}」句は、リバース Telnet のネットワーク アクセス サーバ ポートに対して無条件のアクセス権をユーザに許可しています。「service=raccess」句が存在しない場合、ユーザはリバース Telnet のすべてのポートに対してアクセスを拒否されます。

次に、ネットワーク アクセス サーバが RADIUS セキュリティ サーバから認可を要求してから、ユーザによるリバース Telnet セッションの確立を許可する例を示します。

```
aaa new-model
aaa authentication login default group radius
aaa authorization reverse-access default group radius
!
radius-server host 172.31.255.0
radius-server key go away
auth-port 1645 acct-port 1646
```

この RADIUS リバース Telnet 認可設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは AAA をイネーブルにします。
- **aaa authentication login default group radius** コマンドで、ログイン時のユーザ認証のデフォルト方式として RADIUS を指定します。
- リバース Telnet セッションを確立しようとしているときに、**aaa authorization reverse-access default group radius** コマンドで、ユーザ認可の方式として RADIUS を指定します。
- **radius-server host** コマンドで、RADIUS サーバを指定します。
- **radius-server key** コマンドで、ネットワーク アクセス サーバと RADIUS デーモン間のすべての RADIUS 通信に使用される暗号化キーを定義します。

次に、ネットワーク アクセス サーバ「maple」上のポート tty2 で、ユーザ「pat」にリバース Telnet アクセス権を付与する RADIUS サーバに要求を送信する例を示します。

```
Username = "pat"
Password = "goaway"
User-Service-Type = Shell-User
cisco-avpair = "raccess:port#1=maple/tty2"
```

構文「raccess:port=any/any」で、リバース Telnet のネットワーク アクセス サーバ ポートに対して無条件のアクセス権をユーザに許可します。「raccess:port={*nasname*}/{*tty number*}」句がユーザ プロファイルにない場合、ユーザはすべてのポートでリバース Telnet へのアクセスを拒否されます。

その他の参考資料

ここでは、認可機能に関する関連資料について説明します。

関連資料

内容	参照先
認可コマンド	『*Cisco IOS Security Command Reference*』
RADIUS	「Configuring RADIUS」フィーチャ モジュール
LDAP	「Configuring RADIUS」フィーチャ モジュール
RADIUS アトリビュート	「RADIUS Attributes Overview and RADIUS IETF Attributes」フィーチャ モジュール
TACACS+	「Configuring TACACS+」フィーチャ モジュール
TACACS+ アトリビュート値ペア	「TACACS+ Attribute-Value Pairs」フィーチャ モジュール
認証	「Configuring Authentication」フィーチャ モジュール
認証プロキシ	「Configuring Authentication Proxy」フィーチャ モジュール

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によってサポートされる新しい RFC や変更された RFC はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

認可の設定に関する機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　認可の設定に関する機能情報

機能名	リリース	機能情報
認可の設定	10.0 Cisco IOS XE Release 2.1	AAA 認可機能を使用して、ユーザができることとできないことを定義します。AAA 認可をイネーブルにすると、ネットワーク アクセス サーバはユーザのプロファイルから取得した情報を使用して、ユーザの設定を設定します。このプロファイルは、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。認可が完了すると、ユーザ プロファイルの情報で許可されているサービスであれば、ユーザは要求したサービスに対するアクセス権を付与されます。 この機能は、Cisco IOS Release 10.0 で導入されました。 この機能は、Cisco ASR 1000 シリーズ ルータで導入されました。
LDAP の Active Directory との統合	15.1(1)T	LDAP はディレクトリへのアクセスに使用される標準ベースのプロトコルです。RADIUS に類似したクライアント サーバ モデルをベースとしています。LDAP はシスコ デバイス上で稼動し、ユーザ認証およびネットワーク サービス アクセスに関するすべての情報を保持する中央の LDAP サーバへ認証要求を送信します。 この機能は、AAA の認証および認可のサポートを提供します。 コマンド **aaa authorization** が変更されました。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

認可の設定に関する機能情報

Standalone MAB Support

Standalone MAC Authentication Bypass（MAB; MAC 認証バイパス）は、802.1x 機能またはクレデンシャルにかかわらず、特定の MAC アドレスへのネットワーク アクセスを許可する認証方式です。このため、レジ、ファクス機、プリンタなどのデバイスをすぐに認証し、認証ポリシーに基づくネットワーク機能を使用可能にできます。

Standalone MAB Support が使用可能になるまで、MAB は、802.1x 認証のためのフェールオーバー方式として設定することしかできませんでした。Standalone MAB は、802.1x 認証とは独立しています。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「Standalone MAB Support の機能情報」（P.10）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

Standalone MAB Support の前提条件

IEEE 802.1x：ポートベースのネットワーク アクセス コントロール

ポートベースのネットワーク アクセス コントロールの概念とシスコのプラットフォーム上のポートベースのネットワーク アクセス コントロールの設定方法を理解しておく必要があります。詳細については、『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 15.0』を参照してください。

RADIUS および ACL

RADIUS プロトコルの概念と Access Control List（ACL; アクセス コントロール リスト）の作成および適用方法を理解しておく必要があります。詳細については、シスコのプラットフォームのマニュアル、および『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 15.0』を参照してください。

スイッチが RADIUS 設定されていて、Cisco Secure Access Control Server（ACS; アクセス コントロール サーバ）に接続されている必要があります。詳細については、『*User Guide for Secure ACS Appliance 3.2*』を参照してください。

Standalone MAB Support について

Standalone MAB をセットアップするには、次の概念を理解しておく必要があります。

- 「Cisco IOS Auth Manager の概要」（P.2）
- 「Standalone MAB」（P.3）

Cisco IOS Auth Manager の概要

指定されたネットワークに接続するデバイスの機能は異なっている可能性があるため、ネットワークはさまざまな認証方式および認証ポリシーをサポートする必要があります。Cisco IOS Auth Manager は、認証方法に関係なく、ネットワーク認証要求を処理し、認証ポリシーを強制します。Auth Manager は、すべてのポートベースのネットワーク接続試行、認証、認可、および接続解除に対する運用データを維持することで、セッション マネージャとして機能します。

Auth Manager セッションには、次のような状態が考えられます。

- Idle：idle 状態では、認証セッションは初期化されていますが、実行されている方式はありません。これは中間の状態です。
- Running：現在、方式が実行されています。これは中間の状態です。
- Authc Success：認証方式の実行に成功しました。これは中間の状態です。
- Authc Failed：認証方式が失敗しました。これは中間の状態です。
- Authz Success：このセッションに対するすべての機能の適用に成功しました。これは最終的な状態です。
- Authz Failed：このセッションに対して、少なくとも 1 つの機能の適用に失敗しました。これは最終的な状態です。
- No methods：このセッションに結果を提供する方式がありません。これは最終的な状態です。

Standalone MAB

MAB はネットワーク アクセスの許可または拒否に、接続デバイスの MAC アドレスを使用します。MAB をサポートするため、RADIUS 認証サーバは、ネットワークへのアクセスを必要とするデバイスの MAC アドレスのデータベースを維持します。MAB は、Calling-Station-Id（アトリビュート 31）で MAC アドレスを使用し、Service-Type（アトリビュート 6）で値 10 を使用して、RADIUS 要求を生成します。認証に成功すると、Auth Manager は、ACL 割り当ておよび VLAN 割り当てなど認証ポリシーによって指定されたさまざまな認証機能をイネーブルにします。

Standalone MAB の設定方法

ここでは、次の作業について説明します。

- 「Standalone MAB のイネーブル化」（P.3）
- 「ポート上の再認証のイネーブル化」（P.5）
- 「セキュリティ違反モードの指定」（P.6）

Standalone MAB のイネーブル化

Standalone MAB 機能でイネーブルにされたポートは、ネットワーク アクセスの許可または拒否に接続デバイスの MAC アドレスを使用できます。個別ポートで、Standalone MAB をイネーブルにするには、この項で説明する手順を実行します。

前提条件

Standalone MAB を設定する前に、スイッチを Cisco Secure ACS サーバに接続し、RADIUS Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）を設定する必要があります。

制約事項

Standalone MAB は、スイッチド ポート上でのみ設定できます。ルーテッド ポートでは設定できません。

（注） MAB または MAB EAP がスイッチド ポート上でイネーブルにされているかディセーブルにされているかわからない場合は、インターフェイス コンフィギュレーション モードで、**default mab** または **default mab eap** コマンドを使用して、MAB または MAB EAP をデフォルトに設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **switchport**
5. **switchport mode access**

6. **authentication port-control auto**
7. **mab** [**eap**]
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Switch> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type slot*/*port* 例： Switch(config)# interface FastEthernet2/1	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport** 例： Switch(config-if)# switchport	レイヤ 2 スイッチド モードでインターフェイスを配置します。
ステップ 5	**switchport mode access** 例： Switch(config-if)# switchport mode access	非トランキング、非タグ付き、シングル VLAN レイヤ 2 インターフェイスを設定します。
ステップ 6	**authentication port-control auto** 例： Switch(config-if)# authentication port-control auto	ポートの認証ステートを設定します。
ステップ 7	**mab** [**eap**] 例： Switch(config-if)# mab	MAB をイネーブルにします。
ステップ 8	**end** 例： Switch(config-if)# end	グローバル コンフィギュレーション モードに戻ります。

トラブルシューティングのヒント

次のコマンドは、Standalone MAB のトラブルシューティングに役立ちます。

- **debug authentication**
- **debug mab all**
- **show authentication registrations**

- **show authentication sessions**
- **show mab**

ポート上の再認証のイネーブル化

デフォルトでは、ポートは自動的に再認証されません。自動再認証をイネーブルにし、再認証の頻度を指定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **switchport**
5. **switchport mode access**
6. **authentication port-control auto**
7. **mab** [**eap**]
8. **authentication periodic**
9. **authentication timer reauthenticate** {*seconds* | **server**}
10. **end**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	`enable`
	
	例：
	`Switch> enable`
		特権 EXEC モードをイネーブルにします。
		• プロンプトが表示されたら、パスワードを入力します。

ステップ 2	`configure terminal`
	
	例：
	`Switch# configure terminal`
		グローバル コンフィギュレーション モードを開始します。

ステップ 3	`interface` *`type slot/port`* 例： `Switch(config)# interface FastEthernet2/1`	インターフェイス コンフィギュレーション モードを開始します。

ステップ 4	`switchport`
	
	例：
	`Switch(config-if)# switchport`
		レイヤ 2 スイッチド モードでインターフェイスを配置します。

ステップ 5	`switchport mode access`
	
	例：
	`Switch(config-if)# switchport mode access`
		非トランキング、非タグ付き、シングル VLAN レイヤ 2 インターフェイスを設定します。

	コマンドまたはアクション	目的
ステップ 6	**authentication port-control auto** 例： `Switch(config-if)# authentication port-control auto`	ポートの認証ステートを設定します。
ステップ 7	**mab** [**eap**] 例： `Switch(config-if)# mab`	MAB をイネーブルにします。
ステップ 8	**authentication periodic** 例： `Switch(config-if)# authentication periodic`	再認証をイネーブルにします。
ステップ 9	**authentication timer reauthenticate** {*seconds* | **server**} 例： `Switch(config-if)# authentication timer reauthenticate 900`	再認証の間隔（秒単位）を設定します。
ステップ 10	**end** 例： `Switch(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。

セキュリティ違反モードの指定

ポート上でセキュリティ違反がある場合、ポートをシャットダウンするか、トラフィックを制限できます。デフォルトでは、ポートはシャットダウンされます。ポートをシャットダウンする一定の時間を設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **switchport**
5. **switchport mode access**
6. **authentication port-control auto**
7. **mab** [**eap**]
8. **authentication violation** {**restrict** | **shutdown**}
9. **authentication timer restart** *seconds*
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Switch> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type slot/port* **例：** `Switch(config)# interface FastEthernet2/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport** **例：** `Switch(config-if)# switchport`	レイヤ 2 スイッチド モードでインターフェイスを配置します。
ステップ 5	**switchport mode access** **例：** `Switch(config-if)# switchport mode access`	非トランキング、非タグ付き、シングル VLAN レイヤ 2 インターフェイスを設定します。
ステップ 6	**authentication port-control auto** **例：** `Switch(config-if)# authentication port-control auto`	ポートの認証ステートを設定します。
ステップ 7	**mab** [**eap**] **例：** `Switch(config-if)# mab`	MAB をイネーブルにします。
ステップ 8	**authentication violation** {**restrict** | **shutdown**} **例：** `Switch(config-if)# authentication violation shutdown`	ポート上でセキュリティ違反が生じた場合に取るアクションを設定します。
ステップ 9	**authentication timer restart** *seconds* **例：** `Switch(config-if)# authentication timer restart 30`	未認証のポートの認証の間隔（秒単位）を設定します。
ステップ 10	**end** **例：** `Switch(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。

Standalone MAB の設定例

ここでは、次の例について説明します。

- 「Standalone MAB の設定：例」（P.8）

Standalone MAB の設定：例

次に、ポート上で Standalone MAB を設定する方法の例を示します。この例で、クライアントは 1200 秒ごとに再認証され、接続は 600 秒の非アクティビティでドロップされます。

```
enable
 configure terminal
  interface GigabitEthernet2/1
   switchport
   switchport mode access
   switchport access vlan 2
   authentication port-control auto
   mab
   authentication violation shutdown
   authentication timer restart 30
   authentication periodic
   authentication timer reauthenticate 1200
   authentication timer inactivity 600
```

その他の参考資料

ここでは、Standalone MAB 機能に関する関連資料について説明します。

関連資料

内容	参照先
認証コマンド	『*Cisco IOS Security Command Reference*』
IEEE 802.1x：フレキシブルな認証	『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 15.0』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
• CISCO-AUTH-FRAMEWORK-MIB • CISCO-MAC-AUTH-BYPASS-MIB • CISCO-PAE-MIB • IEEE8021-PAE-MIB	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 3580	「*IEEE 802.1x Remote Authentication Dial In User Service (RADIUS)*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

Standalone MAB Support の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　Standalone MAB Support の機能情報

機能名	リリース	機能情報
Standalone MAB Support	12.2(33)SXI	この機能は、802.1x 機能またはクレデンシャルにかかわらず、MAC アドレスに基づいてデバイスへのネットワーク アクセスを許可します。 この機能により、次のコマンドが導入または変更されました。**authentication periodic**、**authentication port-control**、**authentication timer inactivity**、**authentication timer reauthenticate**、**authentication timer restart**、**authentication violation**、**debug authentication**、**mab**、**show authentication interface**、**show mab**、**show authentication registrations**、**show authentication sessions**

アカウンティングの設定

AAA アカウンティング機能を使用すると、ユーザがアクセスするサービス、およびユーザが消費するネットワーク リソース量を追跡できます。AAA アカウンティングをイネーブルにすると、ネットワーク アクセス サーバから TACACS+ または RADIUS セキュリティ サーバ（実装しているセキュリティ手法によって異なります）に対して、アカウンティング レコードの形式でユーザ アクティビティがレポートされます。アカウンティング レコードにはアカウンティング AV のペアが含まれ、セキュリティ サーバに保存されます。このデータを分析して、ネットワーク管理、クライアント課金、および監査に利用できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「アカウンティングの設定の機能情報」（P.35）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

アカウンティングの設定の前提条件

次のタスクを実行してから、名前付き方式リストを使用してアカウンティングを設定します。

- ネットワーク アクセス サーバで AAA をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa new-model** コマンドを使用します。
- RADIUS または TACACS+ 認可が発行されている場合、RADIUS または TACACS+ セキュリティ サーバの特性を定義します。Cisco ネットワーク アクセス サーバを設定して RADIUS セキュリティ サーバと通信する方法の詳細については、「Configuring RADIUS」モジュールを参照してください。Cisco ネットワーク アクセス サーバを設定して TACACS+ セキュリティ サーバと通信する方法の詳細については、「Configuring TACACS+」モジュールを参照してください。

アカウンティングの設定の制約事項

- アカウンティング情報は、最大 4 台の AAA サーバにのみ同時送信できます。
- Service Selection Gateway（SSG）システムの場合、**aaa accounting network broadcast** コマンドを実行すると、**start-stop** アカウンティング レコードのみがブロードキャストされます。**ssg accounting interval** コマンドを使用して中間アカウンティング レコードを設定する場合、中間アカウンティング レコードは、設定したデフォルト RADIUS サーバにのみ送信されます。

アカウンティングの設定について

- 「アカウンティングの名前付き方式リスト」（P.2）
- 「AAA アカウンティング タイプ」（P.6）
- 「AAA アカウンティングの強化」（P.16）
- 「アカウンティング アトリビュートと値のペア」（P.18）

アカウンティングの名前付き方式リスト

認証および認可方式リストと同様に、アカウンティングの方式リストには、アカウンティングの実行方法とその方式を実行するシーケンスが定義されています。

アカウンティングの名前付き方式リストには、特定のセキュリティ プロトコルを指定し、アカウンティング サービスの特定の行またはインターフェイスに使用できます。唯一の例外は、デフォルトの方式リスト（「default」という名前が指定されています）です。デフォルトの方式リストは、名前付きの方式リストが明示的に定義されているインターフェイスを除き、すべてのインターフェイスに自動的に適用されます。デフォルトの方式リストは、定義された方式リストによって上書きされます。

方式リストは、シーケンスで照会されるアカウンティング方式（RADIUS、TACACS+ など）を説明する単なる名前付きリストです。方式リストでは、アカウンティングに 1 つまたは複数のセキュリティ プロトコルを指定できます。そのため、最初の方式が失敗した場合に備えてアカウンティングのバックアップ システムを確保できます。Cisco IOS ソフトウェアでは、方式リストのうち、アカウンティングをサポートする最初の方式が使用されます。その方式が応答しない場合、方式リストの次のアカウンティング方式が選択されます。このプロセスは、リストのいずれかのアカウンティング方式と通信に成功するか、定義されているすべての方式が試行されるまで継続されます。

（注） Cisco IOS ソフトウェアでは、前の方式からの応答がない場合にのみ、リストの次のアカウンティング方式でアカウンティングが試行されます。このサイクルの任意の時点でアカウンティングが失敗した場合（つまり、セキュリティ サーバからユーザ アクセスの拒否応答が返される場合）、アカウンティング プロセスは停止し、その他のアカウンティング方式は試行されません。

アカウンティング方式リストは、要求されるアカウンティングの種類によって変わります。AAA は、次の 7 種類のアカウンティングをサポートしています。

- **ネットワーク**：パケットやバイト カウントなど、すべての PPP、SLIP、または ARAP セッションに関する情報を提供します。
- **EXEC**：ネットワーク アクセス サーバのユーザ EXEC ターミナル セッションに関する情報を提供します。
- **コマンド**：ユーザが発行する EXEC モード コマンドに関する情報を提供します。コマンド アカウンティングは、特定の特権レベルに関連付けられた、グローバル コンフィギュレーション コマンドなどのすべての EXEC モード コマンドについて、アカウンティング レコードを生成します。
- **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）、rlogin など、ネットワーク アクセス サーバからの発信接続すべてに関する情報を提供します。
- **システム**：システムレベルのイベントに関する情報を提供します。
- **リソース**：ユーザ認証に成功したコールの「開始」および「終了」レコードを提供します。また、認証に失敗したコールの「終了」レコードを提供します。
- **VRRS**：Virtual Router Redundancy Service（VRRS）に関する情報を提供します。

（注） システム アカウンティングは、名前付きアカウンティング リストを使用しません。システム アカウンティングのデフォルト リストだけを定義できます。

この場合も、名前付き方式リストが作成されると、指定したアカウンティング タイプのアカウンティング方式のリストが定義されます。

アカウンティング方式リストを特定の回線またはインターフェイスに適用してから、定義済み方式のいずれかを実行する必要があります。唯一の例外は、デフォルトの方式リスト（「default」という名前が指定されています）です。名前付き方式リストを指定せずに、特定のアカウンティング タイプに対して **aaa accounting** コマンドを発行すると、明示的に名前付き方式リストが定義されている場合を除き、すべてのインターフェイスまたは回線にデフォルトの方式リストが自動的に適用されます（定義した方式リストは、デフォルトの方式リストよりも優先されます）。デフォルトの方式リストが定義されていない場合、アカウンティングは実行されません。

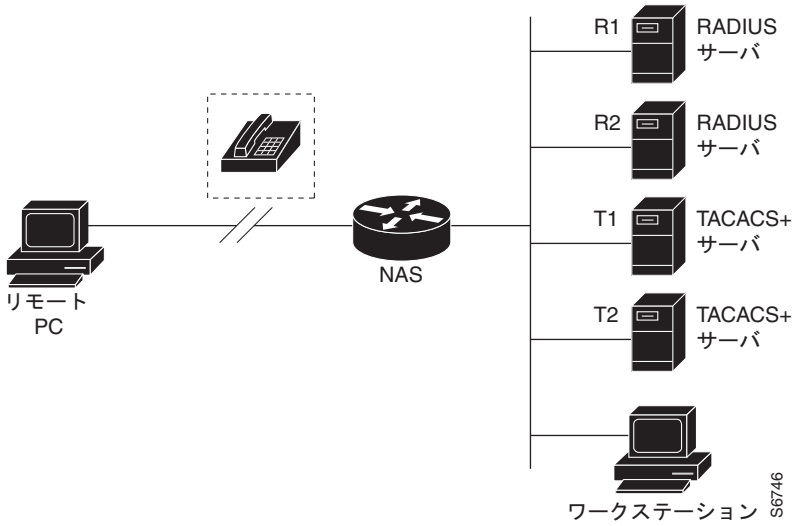
この項の内容は、次のとおりです。

- 「方式リストとサーバ グループ」（P.4）
- 「AAA アカウンティング方式」（P.5）
- 「アカウンティング レコードの種類」（P.5）
- 「アカウンティング方式」（P.5）

方式リストとサーバ グループ

サーバ グループは、方式リストに使用する既存の RADIUS または TACACS+ サーバ ホストをグループ化する方法の 1 つです。図 1 に、4 台のセキュリティ サーバ（R1 と R2 は RADIUS サーバ、T1 と T2 は TACACS+ サーバ）が設置された一般的な AAA ネットワーク設定を示します。R1 と R2 は RADIUS サーバのグループから構成されます。T1 と T2 は TACACS+ サーバのグループから構成されます。

図 1　一般的な AAA ネットワーク設定



Cisco IOS ソフトウェア、RADIUS サーバ、および TACACS+ サーバの設定はグローバルです。サーバ グループを使用して、設定済みのサーバ ホストのサブセットを指定できます。このようなサーバ グループは、特定のサービスに使用できます。たとえば、サーバ グループを使用すると、R1 と R2 を個別のサーバ グループ（SG1 と SG2）として定義し、T1 と T2 を個別のサーバ グループ（SG3 と SG4）として定義できます。つまり、R1 と T1（SG1 と SG3）または R2 と T2（SG2 と SG4）を方式リストに指定することができます。そのため、RADIUS および TACACS+ のリソースを割り当てる場合の柔軟性が高くなります。

サーバ グループには、1 台のサーバに対して複数のホスト エントリを含めることができます。エントリごとに固有の識別情報を設定します。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。つまり、この固有識別情報を使用して、1 台のサーバ上に複数の UDP ポートが存在する場合、同じ IP アドレスからそれぞれの UDP ポートに対して RADIUS 要求を送信できます。1 台の RADIUS サーバ上にある異なる 2 つのホスト エントリが 1 つのサービス（アカウンティングなど）に設定されている場合、設定されている 2 番めのホスト エントリは最初のホスト エントリのフェールオーバー バックアップとして動作します。この例を使用して、最初のホスト エントリがアカウンティング サービスの提供に失敗した場合、ネットワーク アクセス サーバは、同じデバイスに設定されている 2 番めのホスト エントリに対してアカウンティング サービスを試行します（RADIUS ホスト エントリは、設定順に試行されます）。

Dialed Number Identification Service（DNIS; 着信番号識別サービス）番号に基づくサーバ グループの設定およびサーバ グループの設定の詳細については、『*Cisco IOS Security Configuration Guide: Securing User Services*』の「Configuring RADIUS」または「Configuring TACACS+」を参照してください。

AAA アカウンティング方式

Cisco IOS ソフトウェアはアカウンティングについて次の 2 つの方式をサポートします。

- TACACS+：ネットワーク アクセス サーバは、アカウンティング レコードの形式で TACACS+ セキュリティ サーバに対してユーザ アクティビティを報告します。アカウンティング レコードにはアカウンティング AV のペアが含まれ、セキュリティ サーバに保存されます。
- RADIUS：ネットワーク アクセス サーバは、アカウンティング レコードの形式で RADIUS セキュリティ サーバに対してユーザ アクティビティを報告します。アカウンティング レコードにはアカウンティング AV のペアが含まれ、セキュリティ サーバに保存されます。

アカウンティング レコードの種類

最小限のアカウンティングの場合、**stop-only** キーワードを使用します。このキーワードによって、要求されたユーザ プロセスの終了時に、終了レコード アカウンティング通知を送信するように、指定した方式（**RADIUS** または **TACACS+**）に指示します。詳細なアカウンティング情報が必要な場合、**start-stop** キーワードを使用して、要求されたイベントの開始時には開始アカウンティング通知、そのイベントの終了時には修理用アカウンティング通知を送信します。この回線またはインターフェイスですべてのアカウンティング アクティビティを終了するには、**none** キーワードを使用します。

アカウンティング方式

表 1 に、サポートされるアカウンティング方式を示します。

表 1　　AAA アカウンティング方式

キーワード	説明
group radius	アカウンティングにすべての RADIUS サーバのリストを使用します。
group tacacs+	アカウンティングにすべての TACACS+ サーバのリストを使用します。
group *group-name*	サーバ グループ *group-name* の定義に従って、アカウンティングに RADIUS または TACACS+ サーバのサブセットを使用します。

method 引数は、認証アルゴリズムが試行する実際の方式を指します。追加の認証方式は、直前の方式で（失敗した場合ではなく）エラーが返された場合にのみ使用されます。他のすべての方式がエラーを返しても、認証に成功したことを指定するには、コマンドで追加の方式を指定します。たとえば、TACACS+ 認証がエラーを返す場合に認証のバックアップ方式として RADIUS を指定する acct_tac1 という方式リストを作成するには、次のコマンドを入力します。

```
aaa accounting network acct_tac1 stop-only group tacacs+ group radius
```

名前付きリストが **aaa accounting** コマンドで指定されていない場合に使用するデフォルト リストを作成するには、default キーワードの後に、デフォルトの状況で使用する方式を指定します。デフォルトの方式リストは、すべてのインターフェイスに自動的に適用されます。

たとえば、ログイン時のユーザ認証のデフォルト方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa accounting network default stop-only group radius
```

AAA アカウンティングは、次の方式をサポートします。

- **group tacacs**：ネットワーク アクセス サーバからアカウンティング情報を TACACS+ セキュリティ サーバに送信するようにするには、**group tacacs+** *method* キーワードを使用します。

- **group radius**：ネットワーク アクセス サーバからアカウンティング情報を RADIUS セキュリティ サーバに送信するようにするには、**group radius** *method* キーワードを使用します。

（注） SLIP のアカウンティング方式リストは、関連インターフェイスで PPP に設定されているすべての方式に従います。特定のインターフェイスに定義および適用されるリストがない場合（または PPP 設定が指定されていない場合）、アカウンティングのデフォルト設定が適用されます。

- **group** *group-name* : RADIUS または TACACS+ サーバのサブセットを指定して、アカウンティング方式として使用するには、**group** *group-name* 方式を指定して **aaa accounting** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**loginrad** というグループ（**group**）のメンバを最初に定義します。

```
aaa group server radius loginrad
 server 172.16.2.3
 server 172.16.2 17
 server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバがグループ **loginrad** のメンバとして指定されます。

他の方式リストが定義されていない場合、ネットワーク アカウンティングの方式として **group loginrad** を指定するには、次のコマンドを入力します。

```
aaa accounting network default start-stop group loginrad
```

アカウンティング方式としてグループ名を使用するには、事前に RADIUS または TACACS+ セキュリティ サーバとの通信をイネーブルにする必要があります。

AAA アカウンティング タイプ

AAA は次の 7 種類のアカウンティング タイプをサポートします。

- 「ネットワーク アカウンティング」（P.6）
- 「システム アカウンティング」（P.12）
- 「リソース アカウンティング」（P.13）
- 「接続アカウンティング」（P.11）
- 「システム アカウンティング」（P.12）
- 「リソース アカウンティング」（P.13）
- 「VRRS アカウンティング」（P.15）

ネットワーク アカウンティング

ネットワーク アカウンティングは、パケットやバイト カウントなど、すべての PPP、SLIP、または ARAP セッションに関する情報を提供します。

次に、EXEC セッションを介して着信する PPP ユーザの RADIUS ネットワーク アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:44:45 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 5
        User-Name = "username1"
```

```
        Client-Port-DNIS = "4327528"
        Caller-ID = "562"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "0000000D"
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:45:00 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 5
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "562"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = "0000000E"
        Framed-IP-Address = "10.1.1.2"
        Framed-Protocol = PPP
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:47:46 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 5
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "562"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = "0000000E"
        Framed-IP-Address = "10.1.1.2"
        Framed-Protocol = PPP
        Acct-Input-Octets = 3075
        Acct-Output-Octets = 167
        Acct-Input-Packets = 39
        Acct-Output-Packets = 9
        Acct-Session-Time = 171
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:48:45 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 5
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "408"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "0000000D"
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

次に、最初に EXEC セッションを開始した PPP ユーザの TACACS+ ネットワーク アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:00:35 2001 172.16.25.15    username1   tty4    562/4327528
starttask_id=28      service=shell
Wed Jun 27 04:00:46 2001 172.16.25.15    username1   tty4 562/4327528     starttask_id=30
addr=10.1.1.1   service=ppp
Wed Jun 27 04:00:49 2001 172.16.25.15    username1   tty4    408/4327528     update
task_id=30      addr=10.1.1.1   service=ppp     protocol=ip     addr=10.1.1.1
Wed Jun 27 04:01:31 2001 172.16.25.15    username1   tty4    562/4327528
stoptask_id=30       addr=10.1.1.1   service=ppp     protocol=ip     addr=10.1.1.1
bytes_in=2844        bytes_out=1682  paks_in=36      paks_out=24     elapsed_time=51
Wed Jun 27 04:01:32 2001 172.16.25.15    username1   tty4    562/4327528
stoptask_id=28       service=shell   elapsed_time=57
```

（注） アカウンティング パケット レコードの正確なフォーマットは、セキュリティ サーバ デーモンに応じて変わります。

次に、autoselect を介して着信する PPP ユーザの RADIUS ネットワーク アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:30:52 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 3
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "562"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = "0000000B"
        Framed-Protocol = PPP
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:36:49 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 3
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "562"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = "0000000B"
        Framed-Protocol = PPP
        Framed-IP-Address = "10.1.1.1"
        Acct-Input-Octets = 8630
        Acct-Output-Octets = 5722
        Acct-Input-Packets = 94
        Acct-Output-Packets = 64
        Acct-Session-Time = 357
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

次に、autoselect を介して着信する PPP ユーザの TACACS+ ネットワーク アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:02:19 2001 172.16.25.15    username1   Async5  562/4327528
starttask_id=35      service=ppp
Wed Jun 27 04:02:25 2001 172.16.25.15    username1   Async5  562/4327528     update
task_id=35      service=ppp     protocol=ip     addr=10.1.1.2
Wed Jun 27 04:05:03 2001 172.16.25.15    username1   Async5  562/4327528
stoptask_id=35       service=ppp     protocol=ip     addr=10.1.1.2   bytes_in=3366
bytes_out=2149       paks_in=42      paks_out=28     elapsed_time=164
```

EXEC アカウンティング

EXEC アカウンティングは、ネットワーク アクセス サーバ上にあるユーザ EXEC ターミナル セッション（ユーザ シェル）に関する情報を提供します。たとえば、ユーザ名、日付、開始時刻と終了時刻、アクセス サーバの IP アドレス、および（ダイヤルイン ユーザの場合）発信元の電話番号などです。

次に、ダイヤルイン ユーザの RADIUS EXEC アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:26:23 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 1
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329483"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "00000006"
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:27:25 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 1
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329483"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "00000006"
        Acct-Session-Time = 62
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

次に、ダイヤルイン ユーザの TACACS+ EXEC アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:46:21 2001        172.16.25.15    username1   tty3    5622329430/4327528
start    task_id=2       service=shell
Wed Jun 27 04:08:55 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=2       service=shell   elapsed_time=1354
```

次に、Telnet ユーザの RADIUS EXEC アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:48:32 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 26
        User-Name = "username1"
        Caller-ID = "10.68.202.158"
        Acct-Status-Type = Start
```

```
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "00000010"
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:48:46 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 26
        User-Name = "username1"
        Caller-ID = "10.68.202.158"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "00000010"
        Acct-Session-Time = 14
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

次に、Telnet ユーザの TACACS+ EXEC アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:06:53 2001        172.16.25.15    username1   tty26   10.68.202.158
starttask_id=41      service=shell
Wed Jun 27 04:07:02 2001        172.16.25.15    username1   tty26   10.68.202.158
stoptask_id=41       service=shell   elapsed_time=9
```

コマンド アカウンティング

コマンド アカウンティングは、ネットワーク アクセス サーバで実行される各特権レベルの EXEC シェル コマンドに関する情報を提供します。各コマンド アカウンティング レコードには、その特権レベルで実行されるコマンド、各コマンドが実行された日時、および実行したユーザのリストが含まれます。

次に、特権レベル 1 の TACACS+ コマンド アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:46:47 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=3       service=shell   priv-lvl=1      cmd=show version <cr>
Wed Jun 27 03:46:58 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=4       service=shell   priv-lvl=1      cmd=show interfaces Ethernet 0
<cr>
Wed Jun 27 03:47:03 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=5       service=shell   priv-lvl=1      cmd=show ip route <cr>
```

次に、特権レベル 15 の TACACS+ コマンド アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:47:17 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=6       service=shell   priv-lvl=15     cmd=configure terminal <cr>
Wed Jun 27 03:47:21 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=7       service=shell   priv-lvl=15     cmd=interface Serial 0 <cr>
Wed Jun 27 03:47:29 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=8       service=shell   priv-lvl=15     cmd=ip address 10.1.1.1
255.255.255.0 <cr>
```

（注） Cisco の RADIUS 実装は、コマンド アカウンティングをサポートしていません。

接続アカウンティング

接続アカウンティングは、Telnet、LAT、TN3270、PAD、rlogin などのネットワーク アクセス サーバから行われるすべての発信接続に関する情報を提供します。

次に、発信 Telnet 接続の RADIUS 接続アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:28:00 2001
        NAS-IP-Address = ”172.16.25.15”
        NAS-Port = 2
        User-Name = ”username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = ”5622329477”
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = ”00000008”
        Login-Service = Telnet
        Login-IP-Host = ”10.68.202.158”
        Acct-Delay-Time = 0
        User-Id = ”username1”
        NAS-Identifier = ”172.16.25.15”

Wed Jun 27 04:28:39 2001
        NAS-IP-Address = ”172.16.25.15”
        NAS-Port = 2
        User-Name = ”username1”
        Client-Port-DNIS = ”4327528”
        Caller-ID = ”5622329477”
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = ”00000008”
        Login-Service = Telnet
        Login-IP-Host = ”10.68.202.158”
        Acct-Input-Octets = 10774
        Acct-Output-Octets = 112
        Acct-Input-Packets = 91
        Acct-Output-Packets = 99
        Acct-Session-Time = 39
        Acct-Delay-Time = 0
        User-Id = ”username1”
        NAS-Identifier = ”172.16.25.15”
```

次に、発信 Telnet 接続の TACACS+ 接続アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:47:43 2001        172.16.25.15    username1   tty3    5622329430/4327528
start    task_id=10      service=connection      protocol=telnet addr=10.68.202.158
cmd=telnet username1-sun
Wed Jun 27 03:48:38 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=10      service=connection      protocol=telnet addr=10.68.202.158
cmd=telnet username1-sun     bytes_in=4467   bytes_out=96    paks_in=61      paks_out=72
elapsed_time=55
```

次に、発信 rlogin 接続の RADIUS 接続アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:29:48 2001
        NAS-IP-Address = ”172.16.25.15”
        NAS-Port = 2
        User-Name = ”username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = ”5622329477”
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
```

```
        Service-Type = Login
        Acct-Session-Id = "0000000A"
        Login-Service = Rlogin
        Login-IP-Host = "10.68.202.158"
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:30:09 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 2
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329477"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = "0000000A"
        Login-Service = Rlogin
        Login-IP-Host = "10.68.202.158"
        Acct-Input-Octets = 18686
        Acct-Output-Octets = 86
        Acct-Input-Packets = 90
        Acct-Output-Packets = 68
        Acct-Session-Time = 22
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

次に、発信 rlogin 接続の TACACS+ 接続アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:48:46 2001        172.16.25.15    username1   tty3    5622329430/4327528
start    task_id=12      service=connection      protocol=rlogin addr=10.68.202.158
cmd=rlogin username1-sun /user username1
Wed Jun 27 03:51:37 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=12      service=connection      protocol=rlogin addr=10.68.202.158
cmd=rlogin username1-sun /user username1 bytes_in=659926 bytes_out=138   paks_in=2378
paks_
out=1251        elapsed_time=171
```

次に、発信 LAT 接続の TACACS+ 接続アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:53:06 2001        172.16.25.15    username1   tty3    5622329430/4327528
start    task_id=18      service=connection      protocol=lat    addr=VAX        cmd=lat
VAX
Wed Jun 27 03:54:15 2001        172.16.25.15    username1   tty3    5622329430/4327528
stop     task_id=18      service=connection      protocol=lat    addr=VAX        cmd=lat
VAX  bytes_in=0      bytes_out=0     paks_in=0      paks_out=0      elapsed_time=6
```

システム アカウンティング

システム アカウンティングは、すべてのシステムレベル イベント（たとえば、システムのリブート時やアカウンティングのオン/オフ時）に関する情報を提供します。

次のアカウンティング レコードは、AAA アカウンティングがオフになったことを示す一般的な TACACS+ システム アカウンティング レコード サーバを示します。

```
Wed Jun 27 03:55:32 2001        172.16.25.15    unknown unknown unknown start   task_id=25
service=system  event=sys_acct  reason=reconfigure
```

（注） アカウンティング パケット レコードの正確なフォーマットは、TACACS+ デーモンに応じて変わります。

次のアカウンティング レコードは、AAA アカウンティングがオンになったことを示す TACACS+ システム アカウンティング レコードを示します。

```
Wed Jun 27 03:55:22 2001        172.16.25.15    unknown unknown unknown stop    task_id=23
service=system  event=sys_acct  reason=reconfigure
```

システム リソースを測定する追加のタスクについては、他の Cisco IOS ソフトウェア コンフィギュレーション ガイドを参照してください。たとえば、IP アカウンティング タスクについては、『*Cisco IOS Application Services Configuration Guide*』の「Configuring IP Services」を参照してください。

リソース アカウンティング

シスコが採用している AAA アカウンティングでは、ユーザ認証を通過したコールに対する「開始」レコードと「終了」レコードがサポートされます。ユーザ認証の一部として認証に失敗したコールの「終了」レコードを生成する追加機能もサポートされます。このようなレコードは、ネットワークを管理およびモニタするアカウンティング レコードを採用する場合に必要です。

この項の内容は、次のとおりです。

- 「AAA リソース失敗終了アカウンティング」（P.13）
- 「開始 - 終了レコードの AAA リソース アカウンティング」（P.15）

AAA リソース失敗終了アカウンティング

AAA リソース失敗終了アカウンティングの前には、コール設定シーケンスのユーザ認証段階に到達できなかったコールについて、アカウンティング レコードを提供する方式がありませんでした。このようなレコードは、ネットワークおよびその卸売りの顧客を管理およびモニタするアカウンティング レコードを採用する場合に必要です。

この機能によって、ユーザ認証に到達しなかったコールの「終了」アカウンティング レコードが生成されます。「終了」レコードは、コール設定の時点から生成されます。ユーザ認証に成功したすべてのコールは、従来と同様に動作します。つまり、追加のアカウンティング レコードは確認されません。

図 2 に、通常のコール フローで、AAA リソース失敗終了アカウンティングをイネーブルにしていないコール シーケンスを示します。

図 2　通常のフローで AAA リソース失敗終了アカウンティングをイネーブルにしていないモデム ダイヤルイン コール設定シーケンス

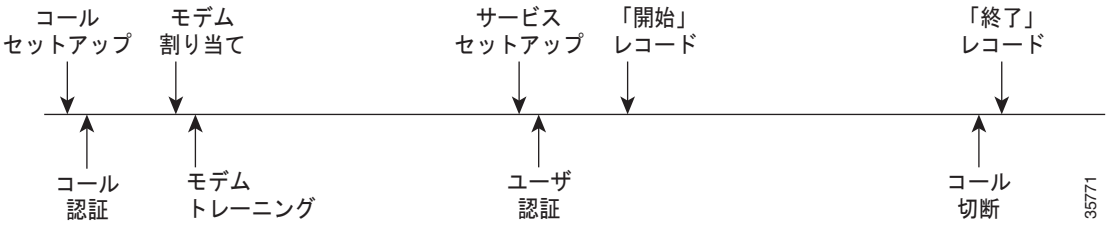


図 3 に、通常のコール フローで、AAA リソース失敗終了アカウンティングをイネーブルにしたコール シーケンスを示します。

図 3　通常のフローで AAA リソース失敗終了アカウンティングをイネーブルにしたモデム ダイヤルイン コール設定シーケンス

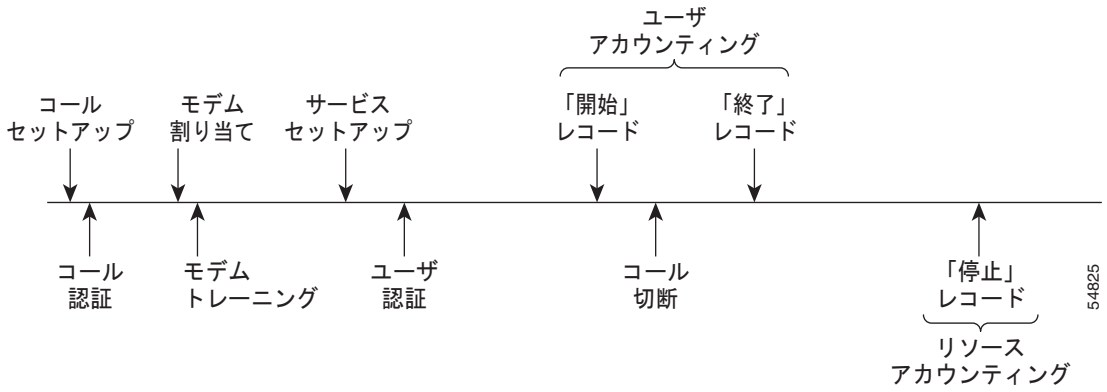
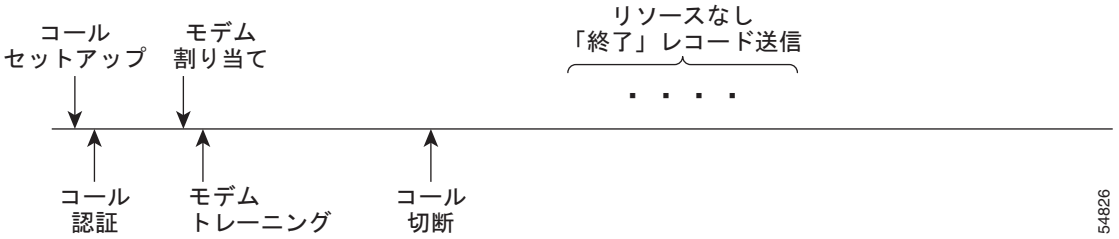


図 4 に、ユーザ認証前にコールの接続解除が発生し、AAA リソース失敗終了アカウンティングをイネーブルにしたコール設定シーケンスを示します。

図 4　ユーザ認証前にコールの接続解除が発生し、AAA リソース失敗終了アカウンティングをイネーブルにしたモデム ダイヤルイン コール設定シーケンス

図 5 に、ユーザ認証前にコールの接続解除が発生し、AAA リソース失敗終了アカウンティングをイネーブルにしないコール設定シーケンスを示します。

図 5　ユーザ認証前にコールの接続解除が発生し、AAA リソース失敗終了アカウンティングをイネーブルにしていないモデム ダイヤルイン コール設定シーケンス



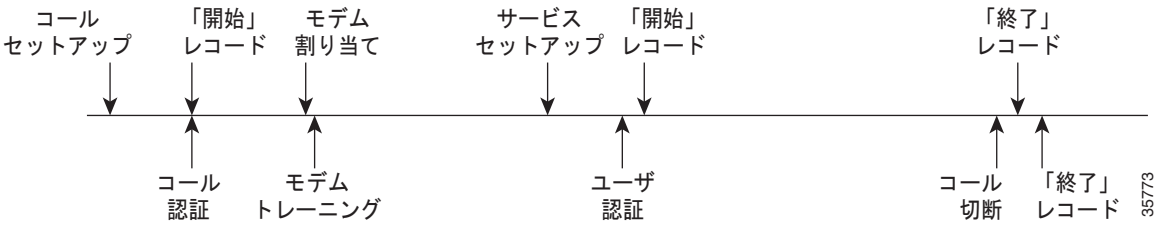
開始 - 終了レコードの AAA リソース アカウンティング

開始 - 終了レコードの AAA リソース アカウンティングは、各コール設定時に「開始」レコードを送信し、コールの接続解除時に対応する「終了」レコードを送信する機能をサポートしています。この機能は、アカウンティング レコードなどを報告するデータの発信元の 1 つから、卸売りの顧客を管理およびモニタするために使用できます。

この機能を使用すると、コール設定およびコールの接続解除の「開始 - 終了」アカウンティング レコードは、デバイスに対するリソース接続の進行状況を追跡します。個別のユーザ認証「開始 - 終了」アカウンティング レコードが、ユーザ管理の進行状況を追跡します。これら 2 セットのアカウンティング レコードは、そのコールで固有のセッション ID を使用して相互リンクされます。

図 6 は、AAA リソース 開始 - 終了アカウンティングをイネーブルにしたコール設定シーケンスを示します。

図 6　リソース開始 - 終了アカウンティングをイネーブルにしたモデム ダイヤルイン コール設定シーケンス



VRRS アカウンティング

Virtual Router Redundancy Service（VRRS）はマルチクライアント情報の抽象化機能を備え、First Hop Redundancy Protocol（FHRP）と登録済みクライアント間に管理サービスを提供しています。VRRS マルチクライアント サービスは、複数の FHRP を抽象化し、FHRP の状態の理想的なビューを提供することで、FHRP プロトコルとの一貫したインターフェイスを提供します。VRRS はデータの更新を管理しています。また、関連するクライアントを 1 か所で登録し、名前付きの FHRP グループまたはすべての登録済み FHRP グループに関する更新を受信できます。

Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）は、FHRP ステータス情報をすべての登録済み VRRS クライアントにプッシュするサーバとして動作する FHRP です。クライアントは、FHRP から提供された重要情報に関するステータスを取得します。たとえば、現在と以前の冗

長状態、アクティブ状態と非アクティブ状態の L3 および L2 アドレス、さらに場合によってはネットワーク内の他の冗長ゲートウェイに関する情報などです。クライアントはこの情報を使用して、ステートレスおよびステートフル冗長情報をクライアントとプロトコルに提供できます。

VRRS アカウンティング プラグイン

VRRS アカウンティング プラグインには、VRRS グループの状態が遷移したときに RADIUS サーバに更新情報を提供する、設定可能な AAA 方式リスト メカニズムが用意されています。VRRS アカウンティング プラグインは、既存の AAA システム アカウンティング メッセージの拡張です。VRRS アカウンティング プラグインには、accounting-on および accounting-off メッセージと、RADIUS アカウンティング メッセージで設定済みの VRRS 名を送信する追加の Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）が用意されています。VRRS 名を設定するには、インターフェイス コンフィギュレーション モードで **vrrp name** コマンドを使用します。

VRRS アカウンティング プラグインには、VRRS グループの状態が遷移したときに RADIUS サーバに更新情報を提供する、設定可能な AAA 方式リスト メカニズムが用意されています。

VRRS アカウンティング プラグインは、既存の AAA システム アカウンティング メッセージの拡張です。VRRS アカウンティング プラグインには、accounting-on および accounting-off メッセージと、RADIUS アカウンティング メッセージで設定済みの VRRS 名を送信する追加の Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）が用意されています。VRRS 名を設定するには、インターフェイス コンフィギュレーション モードで **vrrp name** コマンドを使用します。VRRS グループがマスター状態に遷移すると、VRRS アカウンティング プラグインは accounting-on メッセージを RADIUS に送信します。また、VRRS グループがマスター状態から遷移すると、accounting-off メッセージを送信します。

次の RADIUS アトリビュートは、デフォルトで VRRS アカウンティング メッセージに含まれます。

- アトリビュート 4（NAS-IP-Address）
- アトリビュート 26（Cisco VSA Type 1、VRRS Name）
- アトリビュート 40（Acct-Status-Type）
- アトリビュート 41（Acct-Delay-Time）
- アトリビュート 44（Acct-Session-Id）

VRRS がマスター状態から遷移した場合のアカウンティング メッセージは、すべての PPPoE アカウンティングがその VRRS の一部であるセッションに関するメッセージを停止した後に送信されます。

AAA アカウンティングの強化

- 「AAA ブロードキャスト アカウンティング」（P.16）
- 「AAA セッション MIB」（P.17）

AAA ブロードキャスト アカウンティング

AAA ブロードキャスト アカウンティングを使用すると、複数の AAA サーバに対してアカウンティング情報を同時送信できます。つまり、1 つまたは複数の AAA サーバに対してアカウンティング情報を同時にブロードキャストできます。この機能を使用すると、サービス プロバイダーは自社使用のプライベート AAA サーバやエンド ユーザの AAA サーバにアカウンティング情報を送信できるようになります。この機能では、音声アプリケーションによる課金情報も提供されます。

ブロードキャストは、RADIUS または TACACS+ サーバのグループに使用できます。また、各サーバグループは、他のグループとは関係なく、フェールオーバーの場合のバックアップ サーバを定義できます。

したがって、サービス プロバイダーとそのエンド ユーザは、アカウンティング サーバに異なるプロトコル（RADIUS または TACACS+）を使用できます。また、サービス プロバイダーとそのエンド ユーザは、それぞれ単独でバックアップ サーバを指定することもできます。音声アプリケーションについては、独自のフェールオーバー シーケンスを持つ個別のグループを介して、冗長的なアカウンティング情報を単独で管理できます。

AAA セッション MIB

ユーザが AAA セッション MIB 機能を使用すると、Simple Network Management Protocol（SNMP）を使用して自身の認証済みクライアント接続をモニタおよび終了できます。そのクライアントのデータが提示されるため、RADIUS または TACACS+ サーバから報告される AAA アカウンティング情報に直接関連付けることができます。AAA セッション MIB は、次の情報を提供します。

- 各 AAA 機能の統計情報（**show radius statistics** コマンドと併用する場合）
- AAA 機能を提供するサーバのステータス
- 外部 AAA サーバの ID
- （アイドル時間などの）リアルタイム情報（アクティブ コールを終了するかどうかを評価する SNMP ネットワークが使用する追加基準を提供します）

（注） このコマンドがサポートされるのは、Cisco AS5300 および Cisco AS5800 ユニバーサル アクセス サーバ プラットフォームだけです。

表 2 に、認証済みクライアントと AAA セッション MIB 機能との接続をモニタおよび終了するために使用できる SNMP ユーザエンド データ オブジェクトを示します。

表 2　SNMP エンドユーザ データ オブジェクト

SessionId	AAA アカウンティング プロトコルに使用されるセッション ID（RADIUS アトリビュート 44（Acct-Session-ID）から報告される値と同じ）
UserId	ユーザ ログイン ID または（ログインが使用できない場合）長さがゼロの文字列
IpAddr	セッションの IP アドレスまたは（IP アドレスが適用されない場合、または使用できない場合）0.0.0.0
IdleTime	セッションがアイドルになってからの経過時間
Disconnect	そのクライアントとの接続を解除するために使用されるセッション終了オブジェクト
CallId	コール トラッカー レコードが保存した、このアカウンティング セッションに対応するエントリ インデックス

表 3 に、システム別に SNMP を使用する AAA セッション MIB 機能から提供される AAA の概要情報を示します。

表 3　SNMP AAA セッションの概要

ActiveTableEntries	現在アクティブなセッションの数
ActiveTableHighWaterMark	システムが最後に再インストールされてからの同時接続セッションの最大数
TotalSessions	システムが最後に再インストールされてからのセッションの合計数
DisconnectedSessions	システムが最後に再インストールされてから接続解除されたセッションの合計数

アカウンティング アトリビュートと値のペア

ネットワーク アクセス サーバは、TACACS+ AV のペアまたは RADIUS アトリビュート（実装しているセキュリティ方式によって異なります）に定義されたアカウンティング機能をモニタします。

AAA アカウンティングの設定方法

名前付き方式リストによる AAA アカウンティングの設定

名前付き方式リストを使用して AAA アカウンティングを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa accounting {system | network | exec | connection | commands *level*} {default | *list-name*} {start-stop | stop-only | none} [*method1* [*method2...*]]**
4. **line [aux | console | tty | vty] *line-number* [*ending-line-number*]**
5. **accounting {arap | commands *level* | connection | exec} {default | *list-name*}**
6. **end**

（注） システム アカウンティングは、名前付き方式リストを使用しません。システム アカウンティングの場合、デフォルトの方式リストだけを定義します。

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	Router(config)# **aaa accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [*method1* [*method2...*]] **例：** Router(config)# aaa accounting system default start-stop	アカウンティング方式リストを作成し、アカウンティングをイネーブルにします。引数 *list-name* は、作成したリストに名前を付けるときに使用される文字列です。
ステップ 4	Router(config)# **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*] または Router(config)# **interface** *interface-type interface-number* **例：** Router(config)# line aux line1	アカウンティング方式リストを適用する回線について、ライン コンフィギュレーション モードを開始します。 または アカウンティング方式リストを適用するインターフェイスについて、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	Router(config-line)# **accounting** {**arap** | **commands** *level* | **connection** | **exec**} {**default** | *list-name*} または Router(config-if)# **ppp accounting** {**default** | *list-name*} **例：** Router(config-line)# accounting arap default	1 つの回線または複数回線にアカウンティング方式リストを適用します。 または 1 つのインターフェイスまたは複数インターフェイスにアカウンティング方式リストを適用します。
ステップ 6	Router(config-line)# **end** **例：** Router(config-line)# end	（任意）ライン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

ここでは、次の内容について説明します。

- 「RADIUS システム アカウンティングの設定」（P.20）

RADIUS システム アカウンティングの設定

このタスクを実行して、グローバル RADIUS サーバで RADIUS システム アカウンティングを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server accounting system host-config**
5. **aaa group server radius** ***server-name***
6. **server-private {*host-name* | *ip-address*} key {[0 *server-key* | 7 *server-key*] *server-key***
7. **accounting system host-config**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： Router(config)# aaa new-model	AAA ネットワーク セキュリティ サービスをイネーブルにします。
ステップ 4	**radius-server accounting system host-config** 例： Router(config)# radius-server accounting system host-config	RADIUS サーバの追加および削除の際に、ルータからシステム アカウンティング レコードを送信できるようにします。
ステップ 5	**aaa group server radius** *server-name* 例： Router(config)# aaa group server radius radgroup1	RADIUS サーバを追加し、server-group コンフィギュレーション モードを開始します。 • *server-name* 引数には、RADIUS サーバ グループ名を指定します。

	コマンドまたはアクション	目的
ステップ 6	**server-private** {*host-name* | *ip-address*} **key** {[**0** *server-key* | **7** *server-key*] *server-key* 例： Router(config-sg-radius)# server-private 172.16.1.11 key cisco	RADIUS サーのホスト名または IP アドレスと、非表示のサーバ キーを入力します。 • （任意）**0** と *server-key* 引数は、暗号化されていない（クリアテキストの）非表示のサーバ キーが続くことを示します。 • （任意）**7** と *server-key* 引数は、暗号化されていない（クリアテキストの）非表示のサーバ キーが続くことを示します。 • *server-key* 引数には、非表示のサーバ キーを指定します。*server-key* 引数の前に **0** も **7** も付いていない場合、サーバキーは暗号化されません。 （注） **server-private** コマンドが設定されると、RADIUS システム アカウンティングはイネーブルになります。
ステップ 7	**accounting system host-config** 例： Router(config-sg-radius)# accounting system host-config	プライベート サーバ ホストの追加または削除時に、システム アカウンティング レコードの生成をイネーブルにします。
ステップ 8	**end** 例： Router(config-sg-radius)# end	server-group（config-sg-radius）コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

ヌル ユーザ名セッション時のアカウンティング レコード生成の抑制

AAA アカウンティングをアクティブにすると、Cisco IOS ソフトウェアは、システム上にあるすべてのユーザにアカウンティング レコードを発行します。このとき、プロトコル変換のためにユーザ名文字列がヌルのユーザも含まれます。この例では、**aaa authentication login** *method-list* **none** コマンドが適用される回線で着信するユーザです。関連付けられているユーザ名がないセッションについて、アカウンティング レコードが生成されないようにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# **aaa accounting suppress null-username**	ユーザ名文字列がヌルのユーザについて、アカウンティング レコードが生成されないようにします。

中間アカウンティング レコードの生成

アカウンティング サーバに定期的な中間アカウンティング レコードを送信できるようにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# **aaa accounting update** [**newinfo**] [**periodic**] *number*	アカウンティング サーバに送信される定期的中間アカウンティング レコードをイネーブルにします。

aaa accounting update コマンドをアクティブにすると、Cisco IOS ソフトウェアは、システム上のすべてのユーザに中間アカウンティング レコードを発行します。キーワード **newinfo** を使用すると、報告する新しいアカウンティング情報が発生するたびに、中間アカウンティング レコードがアクセス サーバに送信されます。たとえば、IPCP がリモート ピアとの間で IP アドレスのネゴシエーションを完了したときなどです。中間アカウンティング レコードには、リモート ピアに使用されるネゴシエート済み IP アドレスが含まれます。

キーワード **periodic** とともに使用すると、*number* 引数の定義に従って、中間アカウンティング レコードが定期的に送信されます。中間アカウンティング レコードには、中間アカウンティング レコードが送信される時間までに、そのユーザについて記録されたすべてのアカウンティング情報が含まれます。

注意 多数のユーザがネットワークにログインしている場合、**aaa accounting update periodic** コマンドを使用すると、重度の輻輳が発生する可能性があります。

失敗したログインまたはセッションに対するアカウンティング レコードの生成

AAA アカウンティングをアクティブにすると、Cisco IOS ソフトウェアは、ログイン認証に失敗したシステム ユーザ、またはログイン認証には成功しても何らかの理由で PPP ネゴシエーションに失敗したユーザのアカウンティング レコードを生成しません。

ログイン時またはセッション ネゴシエーション中の認証に失敗したユーザについて、アカウンティング終了レコードを生成するように指定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# **aaa accounting send stop-record authentication failure**	ログイン時またはセッション ネゴシエーション中の認証に失敗したユーザについて、「終了」レコードを生成します。
Router(config)# **aaa accounting send stop-record always**	開始レコードが送信済みかどうかに関係なく、Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）終了レコードを送信します。

EXEC-Stop レコードよりも前のアカウンティング NETWORK-Stop レコードの指定

PPP ユーザが EXEC ターミナル セッションを開始する場合、EXEC 終了レコードの前に生成する NETWORK レコードを指定できます。特定のサービスについて顧客に課金する場合など、状況によっては、ネットワークの開始レコードと終了レコードを一緒に保持する方が望ましいことがあります。その際、基本的に、EXEC の開始メッセージと終了メッセージのフレームワーク内に「ネスト」にします。たとえば、PPP を使用するユーザ ダイヤルインによって、EXEC-start、NETWORK-start、

EXEC-stop、NETWORK-stop というレコードを作成できます。アカウンティング レコードをネストにすることで、NETWORK-stop レコードは NETWORK-start メッセージ（EXEC-start、NETWORK-start、NETWORK-stop、EXEC-stop）に従います。

ユーザ セッションのアカウンティング レコードをネストするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# aaa accounting nested`	ネットワーク アカウンティング レコードをネストします。

AAA リソース失敗終了アカウンティングの設定

リソース失敗終了アカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# aaa accounting resource` *`method-list`* `stop-failure group` *`server-group`*	ユーザ認証に到達しないコールについて、「終了」レコードを生成します。 **（注）** この機能を設定する前に、「アカウンティングの設定の前提条件」に記載されている作業を実行し、ネットワーク アクセス サーバ上で SNMP をイネーブルにしてください。Cisco ルータまたはアクセス サーバ上で SNMP をイネーブルにする方法の詳細については、『*Cisco IOS Network Management Configuration Guide*』の「Configuring SNMP Support」を参照してください。

開始 - 終了レコードの AAA リソース アカウンティングの設定

開始 - 終了レコードのフル リソース アカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# aaa accounting resource` *`method-list`* `start-stop group` *`server-group`*	各コール設定時に「開始」レコードを送信する機能をサポートします。コールの接続解除時に対応する「終了」レコードが続きます。 **（注）** この機能を設定する前に、「アカウンティングの設定の前提条件」に記載されている作業を実行し、ネットワーク アクセス サーバ上で SNMP をイネーブルにしてください。Cisco ルータまたはアクセス サーバ上で SNMP をイネーブルにする方法の詳細については、『*Cisco IOS Network Management Configuration Guide*』の「Configuring SNMP Support」を参照してください。 **（注）**

AAA ブロードキャスト アカウンティングの設定

AAA ブロードキャスト アカウンティングを設定するには、グローバル コンフィギュレーション モードで aaa accounting コマンドを使用します。

コマンド	目的
Router(config)# **aaa accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [**broadcast**] *method1* [*method2...*]	複数の AAA サーバに対するアカウンティング レコードの送信をイネーブルにします。各グループの最初のサーバに対し、アカウンティング レコードを同時に送信します。最初のサーバを利用できない場合は、該当のグループ内で定義されたバックアップ サーバを使用したフェールオーバーが発生します。

DNIS による AAA ブロードキャスト アカウンティングの設定

DNIS による AAA ブロードキャスト アカウンティングを設定するには、グローバル コンフィギュレーション モードで **aaa dnis map accounting network** コマンドを使用します。

コマンド	目的
Router(config)# **aaa dnis map** *dnis-number* **accounting network** [**start-stop** | **stop-only** | **none**] [**broadcast**] *method1* [*method2...*]	DNIS によるアカウンティングの設定を許可します。このコマンドは、グローバルの **aaa accounting** コマンドよりも優先されます。 複数の AAA サーバに対するアカウンティング レコードの送信をイネーブルにします。各グループの最初のサーバに対し、アカウンティング レコードを同時に送信します。最初のサーバを利用できない場合は、該当のグループ内で定義されたバックアップ サーバを使用したフェールオーバーが発生します。

AAA セッション MIB の設定

次のタスクは、次の AAA セッション MIB 機能の設定よりも前に実行する必要があります。

- SNMP を設定します。SNMP については、『*Cisco IOS Network Management Configuration Guide*』の「Configuring SNMP Support」の章を参照してください。
- AAA を設定します。
- RADIUS または TACACS+ サーバの特性を定義します。

（注） SNMP を多用すると、全体のシステム パフォーマンスに影響が出る可能性があります。そのため、この機能を使用するときに、通常のネットワーク管理パフォーマンスを考慮する必要があります。

AAA セッション MIB を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# aaa session-mib disconnect`	SNMP を使用して、認証済みクライアント接続をモニタおよび終了します。 コールを終了するには、**disconnect** キーワードを使用する必要があります。

VRRS アカウンティングの設定

次のタスクを実行して、AAA アカウンティング メッセージを AAA サーバに送信するように Virtual Router Redundancy Service（VRRS）を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa accounting vrrs {default | *list-name*} start-stop *method1* [*method2...*]**
4. **aaa attribute list *list-name***
5. **attribute type *name value* [service *service*] [protocol *protocol*] [mandatory] [tag *tag-value*]**
6. **exit**
7. **vrrs *vrrs-group-name***
8. **accounting delay *seconds***
9. **accounting method {default | *accounting-method-list*}**
10. **exit**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa accounting vrrs** {**default** | *list-name*} **start-stop** *method1* [*method2...*] 例： `Router(config)# aaa accounting vrrs default start-stop`	VRRS の AAA アカウンティングをイネーブルにします。
ステップ 4	**aaa attribute list** *list-name* 例： `Router(config)# aaa attribute list list1`	ルータ上で AAA アトリビュート リストをローカルに定義し、アトリビュート リスト コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 5	**attribute type** *name value* [**service** *service*] [**protocol** *protocol*][**mandatory**][**tag** *tag-value*] 例： Router(config-attr-list)# attribute type example 1	AAA アトリビュート リストへ追加されるアトリビュート タイプをルータ上でローカルに定義します。
ステップ 6	**exit** 例： Router(config-attr-list)# exit	アトリビュート リスト コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**vrrs** *vrrs-group-name* 例： Router(config)# vrrs vrrs1	（任意）VRRS グループを定義し、VRRS グループのパラメータを設定し、VRRS コンフィギュレーション モードを開始します。
ステップ 8	**accounting delay** *seconds* 例： Router(config-vrrs)# accounting delay 10	（任意）accounting-off メッセージを VRRS に送信する際の遅延時間を指定します。
ステップ 9	**accounting method** {**default** | *accounting-method-list*} 例： Router(config-vrrs)# accounting method default	（任意）VRRS グループの VRRS アカウンティングをイネーブルにします。
ステップ 10	**exit** 例： Router(config-vrrs)# exit	VRRS コンフィギュレーション モードを終了します。

AAA サーバが到達不能時のルータとのセッション確立

AAA サーバが到達不能の場合に、ルータとの間にコンソールまたは Telnet セッションを確立するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# **no aaa accounting system guarantee-first**	**aaa accounting system guarantee-first** コマンドは、最初のレコードとしてシステム アカウンティングを保証します（これがデフォルトの条件です）。 状況によっては、システムの再ロードが完了するまで（3 分よりも長くかかる可能性があります）、ユーザがコンソールまたは Telnet 接続でセッションを開始できない可能性があります。この問題を解決するには、**no aaa accounting system guarantee-first** コマンドを使用できます。

（注） **no aaa accounting system guarantee-first** コマンドの入力は、コンソールまたは Telnet セッションを開始できる唯一の条件ではありません。たとえば、特権 EXEC セッションが TACACS+ によって認証され、TACACS+ サーバが到達不能の場合、セッションは開始できません。

アカウンティングのモニタリング

RADIUS または TACACS+ アカウンティングの場合、特定の **show** コマンドは存在しません。現在ログインしているユーザに関する情報を表示するアカウンティング レコードを取得するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# show accounting`	ネットワークでアクティブなアカウント可能なイベントの表示を許可し、アカウンティング サーバでデータが損失した場合に情報を収集できます。

アカウンティングのトラブルシューティング

アカウンティング情報の問題を解決するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# debug aaa accounting`	説明の義務があるイベントが発生したときに、その情報を表示します。

AAA アカウンティングの設定例

例：名前付き方式リストの設定

次に、RADIUS サーバから AAA サービスを提供するために Cisco AS5200（AAA および RADIUS セキュリティ サーバとの通信で有効）を設定する例を示します。RADIUS サーバが応答に失敗すると、認証情報と認可情報についてローカル データベースへの照会が行われ、アカウンティング サービスは TACACS+ サーバによって処理されます。

```
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins group radius local
aaa authorization network blue1 group radius local
aaa accounting network red1 start-stop group radius group tacacs+

username root password ALongPassword

tacacs-server host 172.31.255.0
```

```
tacacs-server key goaway

radius-server host 172.16.2.7
radius-server key myRaDiUSpassWoRd

interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication chap dialins
 ppp authorization blue1
 ppp accounting red1

line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin
```

この RADIUS AAA 設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは、AAA ネットワーク セキュリティ サービスをイネーブルにします。
- **aaa authentication login admins local** コマンドは、ログイン認証の方式リスト「admins」を定義します。
- **aaa authentication ppp dialins group radius local** コマンドで、まず RADIUS 認証を示す認証方式リスト「dialins」を定義します。次に、（RADIUS サーバが応答しない場合）PPP を使用するシリアル回線にはローカル認証が使用されます。
- **aaa authorization network blue1 group radius local** コマンドで、「blue1」というネットワーク認可方式リストを定義します。その際、PPP を使用するシリアル回線に RADIUS 認可を使用するように指定します。RADIUS サーバが応答に失敗すると、ローカル ネットワークの認可が実行されます。
- **aaa accounting network red1 start-stop group radius group tacacs+** コマンドで、red1 というネットワーク アカウンティング方式リストを定義します。その際、PPP を使用するシリアル回線に RADIUS アカウンティング サービス（この場合、特定のイベントに対する開始レコードと終了イベント）を使用するように指定します。RADIUS サーバが応答に失敗すると、アカウンティングサービスは TACACS+ サーバによって処理されます。
- **username** コマンドはユーザ名とパスワードを定義します。これらの情報は、PPP Password Authentication Protocol（PAP; パスワード認証プロトコル）認証での発信元の身元確認に使用されます。
- **tacacs-server host** コマンドは TACACS+ サーバ ホストの名前を定義します。
- **tacacs-server key** コマンドはネットワーク アクセス サーバと TACACS+ サーバ ホスト間の共有秘密テキスト ストリングを定義します。
- **radius-server host** コマンドは RADIUS サーバ ホストの名前を定義します。
- **radius-server key** コマンドはネットワーク アクセス サーバと RADIUS サーバ ホスト間の共有秘密テキスト ストリングを定義します。
- **interface group-async** コマンドは非同期インターフェイス グループを選択して定義します。
- **group-range** コマンドはインターフェイス グループのメンバの非同期インターフェイスを定義します。
- **encapsulation ppp** コマンドは指定のインターフェイスに使用される PPP をカプセル化方式として設定します。

- **ppp authentication chap dialins** コマンドは ppp 認証方式として Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）を選択し、特定のインターフェイスに「ダイヤルイン」方式リストを適用します。
- **ppp authorization blue1** コマンドによって、blue1 ネットワーク認可方式リストは指定したインターフェイスに適用されます。
- **ppp accounting red1** コマンドによって、red1 ネットワーク アカウンティング方式リストは指定したインターフェイスに適用されます。
- **line** コマンドはコンフィギュレーション モードをグローバル コンフィギュレーションからラインコンフィギュレーションに切り替え、設定対象の回線を指定します。
- **autoselect ppp** コマンドは、選択した回線上で PPP セッションを自動的に開始できるように Cisco IOS ソフトウェアを設定します。
- **autoselect during-login** コマンドを使用して、Return キー押さずにユーザ名およびパスワードのプロンプトを表示します。ユーザがログインすると、autoselect 機能（この場合は PPP）が開始します。
- **login authentication admins** コマンドは、ログイン認証の admins 方式リストを適用します。
- **modem dialin** コマンドは選択した回線に接続されているモデムを設定し、着信コールだけを受け入れるようにします。

show accounting コマンドを使用すると、前述の設定に関する出力が次のように生成されます。

```
Active Accounted actions on tty1, User username2 Priv 1
 Task ID 5, Network Accounting record, 00:00:52 Elapsed
 task_id=5 service=ppp protocol=ip address=10.0.0.98
```

表 4 に、前述の出力に含まれるフィールドを示します。

表 4　show accounting のフィールドの説明

フィールド	説明
Active Accounted actions on	ユーザがログインに使用する端末回線またはインターフェイス名
User	ユーザの ID
Priv	ユーザの特権レベル
Task ID	各アカウンティング セッションの固有識別情報
Accounting record	アカウンティング セッション タイプ
Elapsed	このセッション タイプの期間（hh:mm:ss）
attribute=value	このアカウンティング セッションに関連付けられている AV ペア

例：AAA リソース アカウンティングの設定

次に、リソース失敗終了アカウンティング、および 開始 - 終了レコード機能のリソース アカウンティングを設定する例を示します。

```
!Enable AAA on your network access server.
aaa new-model
!Enable authentication at login and list the AOL string name to use for login
authentication.
aaa authentication login AOL group radius local
!Enable authentication for ppp and list the default method to use for PPP authentication.
aaa authentication ppp default group radius local
!Enable authorization for all exec sessions and list the AOL string name to use for
authorization.
```

```
aaa authorization exec AOL group radius if-authenticated
!Enable authorization for all network-related service requests and list the default method
to use for all network-related authorizations.
aaa authorization network default group radius if-authenticated
!Enable accounting for all exec sessions and list the default method to use for all
start-stop accounting services.
aaa accounting exec default start-stop group radius
!Enable accounting for all network-related service requests and list the default method to
use for all start-stop accounting services.
aaa accounting network default start-stop group radius
!Enable failure stop accounting.
aaa accounting resource default stop-failure group radius
!Enable resource accounting for start-stop records.
aaa accounting resource default start-stop group radius
```

例：AAA ブロードキャスト アカウンティングの設定

次に、グローバル **aaa accounting** コマンドを使用して、ブロードキャスト アカウンティングを有効にする例を示します。

```
aaa group server radius isp
 server 10.0.0.1
 server 10.0.0.2

aaa group server tacacs+ isp_customer
 server 172.0.0.1

aaa accounting network default start-stop broadcast group isp group isp_customer

radius-server host 10.0.0.1
radius-server host 10.0.0.2
radius-server key key1
tacacs-server host 172.0.0.1 key key2
```

broadcast キーワードによって、ネットワーク接続に関する「開始」および「終了」アカウンティングレコードが、グループ isp ではサーバ 10.0.0.1 に、グループ isp_customer ではサーバ 172.0.0.1 に同時送信されます。サーバ 10.0.0.1 が使用できなくなると、サーバ 10.0.0.2 へのフェールオーバーが行われます。サーバ 172.0.0.1 が使用できなくなっても、グループ isp_customer にはバックアップ サーバが設定されていないため、フェールオーバーは行われません。

例：DNIS による AAA ブロードキャスト アカウンティングの設定

次に、グローバル **aaa dnis map accounting network** コマンドを使用して、DNIS によるブロードキャスト アカウンティングを有効にする例を示します。

```
aaa group server radius isp
 server 10.0.0.1
 server 10.0.0.2

aaa group server tacacs+ isp_customer
 server 172.0.0.1

aaa dnis map enable
aaa dnis map 7777 accounting network start-stop broadcast group isp group isp_customer

radius-server host 10.0.0.1
radius-server host 10.0.0.2
radius-server key key_1
tacacs-server host 172.0.0.1 key key_2
```

broadcast キーワードによって、DNIS 番号 7777 のネットワーク接続コールに関する「開始」および「終了」アカウンティング レコードが、グループ isp ではサーバ 10.0.0.1 に、グループ isp_customer ではサーバ 172.0.0.1 に同時送信されます。サーバ 10.0.0.1 が使用できなくなると、サーバ 10.0.0.2 へのフェールオーバーが行われます。サーバ 172.0.0.1 が使用できなくなっても、グループ isp_customer にはバックアップ サーバが設定されていないため、フェールオーバーは行われません。

例：AAA セッション MIB

次に、AAA セッション MIB 機能を設定して、PPP ユーザの認証済みクライアント接続を解除する例を示します。

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
aaa session-mib disconnect
```

例：VRRS アカウンティングの設定

次に、AAA アカウンティング メッセージを AAA に送信するように VRRS を設定する例を示します。

```
Router# configure terminal
Router(config)# aaa accounting vrrs vrrp-mlist-1 start-stop group radius
Router(config)# aaa attribute list vrrp-1-attr
Router(config-attr-list)# attribute type account-delay 10
Router(config-attr-list)# exit
Router(config)# vrrs vrrp-group-1
Router(config-vrrs)# accounting delay 10
Router(config-vrrs)# accounting method vrrp-mlist-1
Router(config-vrrs)# exit
```

その他の参考資料

関連資料

内容	参照先
認可	「Configuring Authorization」モジュール
認証	「Configuring Authentication」モジュール
アカウンティング コマンド	『*Cisco IOS Security Command Reference*』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2903	「*Generic AAA Architecture*」
RFC 2904	「*AAA Authorization Framework*」
RFC 2906	「*AAA Authorization Requirements*」
RFC 2989	「*Criteria for Evaluating AAA Protocols for Network Access*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

アカウンティングの設定の機能情報

表 5 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 5 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 5　アカウンティングの設定の機能情報

機能名	リリース	機能情報
AAA ブロードキャスト アカウンティング	12.2 12.2S 12.2SB 12.2SX 12.4T	AAA ブロードキャスト アカウンティングを使用すると、複数の AAA サーバに対してアカウンティング情報を同時送信できます。つまり、1 つまたは複数の AAA サーバに対してアカウンティング情報を同時にブロードキャストできます。 この機能に関する詳細については、次の各項を参照してください。 • 「AAA ブロードキャスト アカウンティング」（P.16） • 「AAA ブロードキャスト アカウンティングの設定」（P.25）
開始 - 終了レコードの AAA リソース アカウンティング	12.2 12.4T 12.2S 12.2SB 12.2SX	開始 - 終了レコードの AAA リソース アカウンティングは、各コール設定時に「開始」レコードを送信し、コールの接続解除時に対応する「終了」レコードを送信する機能をサポートしています。この機能は、アカウンティング レコードなどを報告するデータの発信元の 1 つから、卸売りの顧客を管理およびモニタするために使用できます。 この機能に関する詳細については、次の各項を参照してください。 • 「開始 - 終了レコードの AAA リソース アカウンティング」（P.15） • 「開始 - 終了レコードの AAA リソース アカウンティングの設定」（P.24）

表 5　アカウンティングの設定の機能情報（続き）

機能名	リリース	機能情報
AAA セッション MIB	12.2 12.4T 12.2S 12.2SB 12.2SX	ユーザが AAA セッション MIB 機能を使用すると、SNMP を使用して自身の認証済みクライアント接続をモニタおよび終了できます。そのクライアントのデータが提示されるため、RADIUS または TACACS+ サーバから報告される AAA アカウンティング情報に直接関連付けることができます。 この機能に関する詳細については、次の各項を参照してください。 • 「AAA セッション MIB」（P.17） • 「AAA セッション MIB の設定」（P.25）
AAA：IPv6 アカウンティングの遅延の強化	15.1(1)S	VRRS はマルチクライアント情報の抽象化機能を備え、First Hop Redundancy Protocol（FHRP）と登録済みクライアント間に管理サービスを提供しています。 この機能に関する詳細については、次の各項を参照してください。 • 「VRRS アカウンティング」（P.15） • 「VRRS アカウンティングの設定」（P.26）

認証プロキシ

認証プロキシの設定

Cisco IOS Firewall 認証プロキシ機能では、動的かつユーザごとの認証と認可、業界標準の TACACS+ および RADIUS 認証プロトコルを使用したユーザの認証が可能です。ユーザによる接続の認証と認可により、ネットワーク攻撃に対するより強力な保護が可能になります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「認証プロキシの機能情報」（P.35）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

認証プロキシを設定するための前提条件

認証プロキシを設定する前に、次のことを確認してください。

- 認証プロキシが正しく機能するためには、クライアント ホストで次のブラウザ ソフトウェアが動作している必要があります。
  - Microsoft Internet Explorer 3.0 以降
  - Netscape Navigator 3.0 以降
- 認証プロキシには、標準のアクセス リストを使用するオプションがあります。認証プロキシを設定する前に、アクセス リストを使用してトラフィックをフィルタする方法について確実に理解する必要があります。アクセス リストを Cisco IOS Firewall とともに使用する方法の概要については、「Access Control Lists: Overview and Guidelines」の章を参照してください。
- 認証プロキシは、シスコの Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）の枠組みで実装されているユーザ認証と認可を使用します。認証プロキシを設定する前に、AAA ユーザ認証、認可、およびアカウンティングの設定方法について理解する必要があります。ユーザ認証、認可、およびアカウンティングについては、「Authentication, Authorization, and Accounting (AAA)」の章を参照してください。
- Cisco IOS Firewall とともに認証プロキシを正常に実行するには、ファイアウォール上で CBAC を設定します。CBAC 機能の詳細については、「Configuring Context-Based Access Control」の章を参照してください。

認証プロキシを設定するための制約事項

- 認証プロキシは、HTTP 接続だけを開始します。
- HTTP サービスは、標準的な（ウェルノウン）ポートで動作している必要があります。HTTP の場合はポート 80 です。
- セキュアな認証のために、クライアント ブラウザで JavaScript がイネーブルになっている必要があります。
- 認証プロキシ アクセス リストは、ルータを通過するトラフィックに適用されます。ルータ宛のトラフィックは、Cisco IOS ソフトウェアで提供される既存の認証方式によって認証されます。
- 認証プロキシでは、同時使用がサポートされていません。つまり、2 人のユーザが同じホストから同時にログインしようとした場合、認証と認可は、最初に有効なユーザ名とパスワードを送信したユーザだけに適用されます。
- 複数の AAA サーバまたは異なる AAA サーバを使用したロード バランシングはサポートされていません。

認証プロキシの設定に関する情報

Cisco IOS Firewall 認証プロキシ機能を使用すると、ネットワーク管理者は、詳細なセキュリティ ポリシーをユーザごとに適用できます。以前は、ユーザの身元と関連する認可済みアクセスをユーザの IP アドレスに関連付けるか、1 つのセキュリティ ポリシーをユーザ グループまたはサブネットワーク全体に適用する必要がありました。現在では、ユーザごとのポリシーに基づいてユーザを特定し認可することができます。複数のユーザに一般的なポリシーを適用するのではなく、個人に対してアクセス権を調整できます。

認証プロキシ機能を使用すると、ユーザは、ネットワークにログインしたり、HTTP 経由でインターネットにアクセスでき、ユーザ固有のアクセス プロファイルが、CiscoSecure ACS または他の RADIUS または TACACS+ 認証サーバから自動的に取得されて適用されます。ユーザ プロファイルは、認証されたユーザからのアクティブ トラフィックが存在するときにのみ、アクティブになります。

認証プロキシは、Network Address Translation（NAT; ネットワーク アドレス変換）、Context-based Access Control（CBAC; コンテキストベース アクセス コントロール）、IP Security（IPSec）暗号化、Cisco Secure VPN Client（VPN クライアント）ソフトウェアなど、他の Cisco IOS セキュリティ機能と互換性があります。

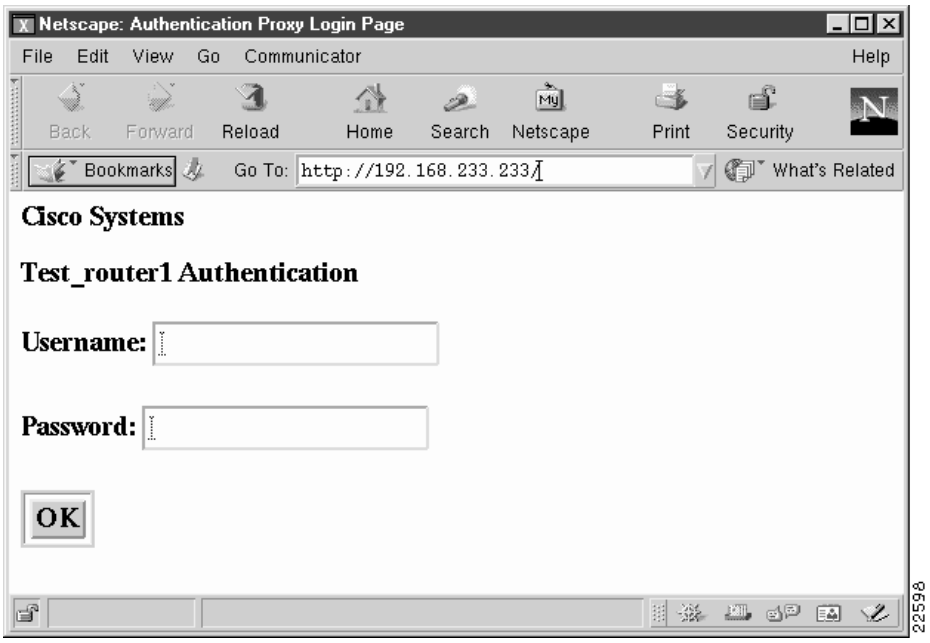
ここでは、次の各手順について説明します。

認証プロキシの仕組み

ユーザがファイアウォールを通じて HTTP セッションを開始すると、認証プロキシが起動されます。認証プロキシは、まずユーザが認証済みかどうかを確認します。ユーザの有効な認証エントリが存在する場合、認証プロキシによるそれ以上の介入なしに接続が完了します。エントリが存在しない場合、認証プロキシは HTTP 接続要求に対し、ユーザ名とパスワードの入力をユーザに求める応答を返します。

図 1 に、認証プロキシの HTML ログイン ページを示します。

図 1　　認証プロキシの HTML ログイン ページ



ユーザは、有効なユーザ名とパスワードを入力することで、認証サーバで正常に認証される必要があります。

認証が成功すると、ユーザの認可プロファイルが AAA サーバから取得されます。認証プロキシは、このプロファイル内の情報を使用して、動的な Access Control Entry（ACE; アクセス コントロール エントリ）を作成し、入力インターフェイスのインバウンド（入力）Access Control List（ACL; アクセス コントロール リスト）と、出力インターフェイスのアウトバウンド（出力）ACL に追加します（出力 ACL がインターフェイスに存在する場合）。この処理により、ファイアウォールは、認証済みユーザに、認可プロファイルで許可されたネットワークへのアクセスを許可します。たとえば、Telnet がユーザのプロファイルで許可されている場合、ユーザはファイアウォールを通じた Telnet 接続を開始できます。

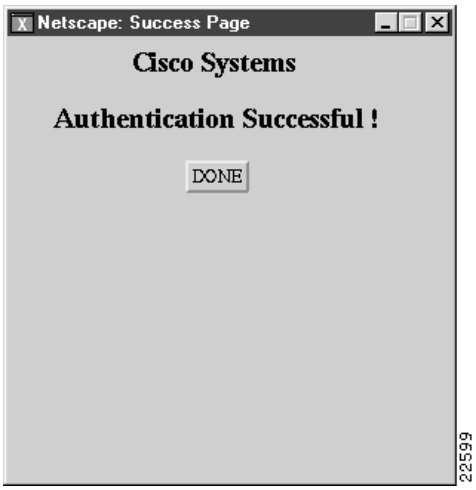
認証が失敗した場合、認証プロキシは、ユーザに失敗したことを報告し、何度か再試行するかどうかを訪ねます。5 回続けて認証に失敗した場合、2 分間待ってから、認証プロキシを起動するために別の HTTP セッションを開始する必要があります。

ログイン ページは、ユーザが Web サーバの情報にアクセスするための要求を行うたびに更新されます。

認証プロキシは、ダウンロードしたアクセス リスト中の送信元 IP アドレスを認証済みホストの送信元 IP アドレスで置き換えることで、ユーザ プロファイルの各アクセス リスト エントリをカスタマイズします。

認証プロキシは、動的な ACE をインターフェイス設定に追加するのと同時に、ログインが成功したことを確認するメッセージをユーザに送信します。図 2 に、HTML ページのログイン ステータスを示します。

図 2　認証プロキシのログイン ステータス メッセージ



認証プロキシは、各ユーザ プロファイルに対し非アクティビティ（アイドル）タイマーを設定します。ファイアウォール経由のアクティビティがある限り、ユーザのホストから送信された新しいトラフィックによって認証プロキシは起動されず、認可済みのユーザ トラフィックに対してファイアウォールを通じたアクセスが許可されます。

アイドル タイマーが満了した場合、認証プロキシはユーザのプロファイル情報と動的なアクセス リスト エントリを削除します。この処理が実行されると、クライアントからのトラフィックはブロックされます。ユーザは、別の HTTP 接続を開始し、認証プロキシを起動する必要があります。

セキュアな認証

認証プロキシでは、JavaScript を使用して、クライアント ブラウザを使用したセキュアな認証が実現されます。セキュアな認証は、クライアントが、誤って認証プロキシ ルータ以外のネットワーク Web サーバにユーザ名とパスワードを送ることを防ぎます。

ここでは、次の各手順について説明します。

- 「JavaScript を使用した操作」
- 「JavaScript を使用しない場合の操作」

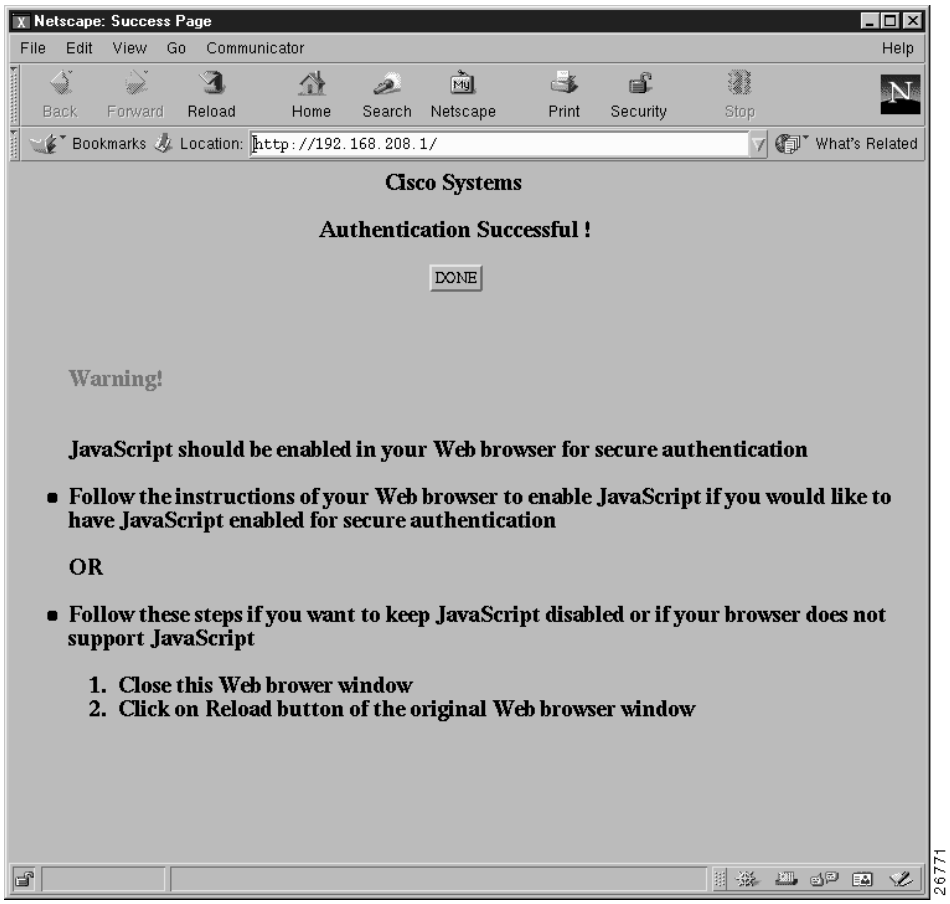
JavaScript を使用した操作

ユーザは、HTTP 接続を開始する前に、ブラウザ上で JavaScript をイネーブルにする必要があります。ブラウザで JavaScript がイネーブルになっている状態で、セキュアな認証が自動的に実行され、図 2 に示す認証メッセージが表示されます。ユーザの HTTP 接続は自動的に完了します。

JavaScript を使用しない場合の操作

クライアント ブラウザが JavaScript をサポートしていない場合や、サイトのセキュリティ ポリシーでユーザが JavaScript をイネーブルにすることが禁止されている場合、ログインしようとするとポップアップ ウィンドウに手動で接続を完了するための手順が表示されます。図 3 に、ブラウザで JavaScript がディセーブルになっている場合の認証プロキシのログイン ステータス メッセージを示します。

図 3　JavaScript がディセーブルになっている場合の認証プロキシのログイン ステータス メッセージ



このウィンドウを閉じるには、ブラウザの [File] メニューの [Close] をクリックします。

ポップアップ ウィンドウを閉じた後、認証ログイン ページが表示されているブラウザ ウィンドウの [Reload]（Internet Explorer の場合は [Refresh]）をクリックする必要があります。ユーザの最後の認証の試みが成功した場合、[Reload] をクリックすると、ユーザが取得しようとしている Web ページが表示されます。ユーザの最後の試みが失敗した場合、[Reload] をクリックすると、認証プロキシがクライアントの HTTP トラフィックを再度代行受信し、ユーザ名とパスワードの入力を求める別のログイン ページが表示されます。

JavaScript がイネーブルになっていない場合、サイト管理者は、「JavaScript を使用しないユーザ接続の確立」で説明するように、ポップアップ ウィンドウを閉じるための正しい手順を実行するよう、ユーザに忠告することを推奨します。

認証プロキシの使用

ユーザに対して透過的に動作する Cisco IOS Firewall のいくつかの機能と異なり、認証プロキシ機能では、クライアント ホスト上でいくつかの対話が必要です。表 1 で、認証プロキシとクライアント ホストの対話について説明します。

表 1　認証プロキシとクライアント ホストの対話

認証プロキシのクライアントとの動作	説明
HTTP 接続の開始	ユーザが現在ファイアウォール ルータで認証済みでない場合、ユーザが HTTP 接続を開始すると認証プロキシが起動されます。ユーザがすでに認証済みの場合、認証プロキシはユーザに対して透過的です。
ログイン ページを使用したログイン	認証プロキシを起動すると、HTML ベースのログイン ページが生成されます。ユーザは、AAA サーバで認証されるために、ユーザ名とパスワードを入力する必要があります。図 1 に、認証プロキシのログイン ページを示します。
クライアントでのユーザの認証	ログインの試行の後の認証プロキシの動作は、ブラウザで JavaScript がイネーブルになっているかどうかで変わります。JavaScript がイネーブルになっており、認証が成功した場合、認証プロキシは、図 2 に示すように、認証のステータスを示すメッセージを表示します。認証ステータスが表示された後、プロキシは自動的に HTTP 接続を完了します。 JavaScript がディセーブルになっており、認証が成功した場合、認証プロキシは、接続を完了するための追加の手順を表示したポップアップ ウィンドウを生成します。図 3 を参照してください。 いずれの場合も、認証が成功しなかった場合は、ユーザはログイン ページから再度ログインする必要があります。

認証プロキシを使用すべき場合

認証プロキシを使用するのが望ましい状況は次のとおりです。

- ホストの IP アドレスやグローバル アクセス ポリシーに基づいてアクセス コントロールを設定するのではなく、認証サーバによって提供されているサービスを使用して、個人ごと（ユーザごと）にアクセス権を管理する場合。任意のホスト IP アドレスからのユーザを認証および認可することにより、ネットワーク管理者は、DHCP を使用してホスト IP アドレスを設定できるようにもなります。
- ファイアウォールを通じたイントラネットやインターネット サービスまたはホストへのアクセスを許可する前に、ローカル ユーザを認証および認可する場合。
- ファイアウォールを通じたローカル サービスまたはホストへのアクセスを許可する前に、リモート ユーザを認証および認可する場合。
- 特定のエクストラネット ユーザに対するアクセスを制御する場合。たとえば、企業パートナーの財務責任者を、あるアクセス権のセットを使用して認証および認可し、同じパートナーの技術責任者を、別のアクセス権のセットを使用するように認可することができます。
- 認証プロキシを VPN クライアント ソフトウェアとともに使用して、ユーザを検証し、特定のアクセス権を割り当てる場合。
- 認証プロキシを AAA アカウンティングとともに使用して、課金、セキュリティ、またはリソース割り当てのために使用可能な「開始」および「停止」アカウンティング レコードを生成することで、ユーザが認証済みホストからのトラフィックを追跡できるようにする場合。

認証プロキシの適用

認証プロキシは、ユーザごとの認証と認可を行うルータの任意のインターフェイスで、インバウンド方向に適用します。認証プロキシをインターフェイスでインバウンド方向に適用することで、ユーザの初期接続要求は、ファイアウォールによる他の処理に渡される前に、認証プロキシによって代行受信されます。ユーザが AAA サーバによる認証に失敗すると、接続要求はドロップされます。

認証プロキシの適用方法は、セキュリティ ポリシーに依存します。たとえば、インターフェイスを通過するすべてのトラフィックをブロックし、認証プロキシ機能をイネーブルにして、ユーザが開始したすべての HTTP 接続に対して認証と認可を義務付けることができます。ユーザは、AAA サーバで正常に認証されない限り、サービスの利用が認可されません。

認証プロキシ機能では、標準のアクセス リストを使用し、どのホストまたはホスト グループからの初期 HTTP トラフィックに対してプロキシを起動するかを指定できます。

図 4 に示す認証プロキシは、LAN インターフェイスに適用されており、すべてのネットワーク ユーザは、初期接続時に認証される必要があります（すべてのトラフィックは各インターフェイスでブロックされます）。

図 4　ローカル インターフェイスでの認証プロキシの適用

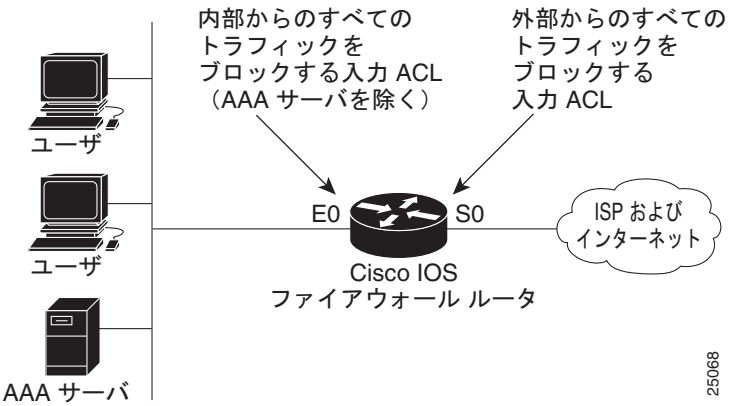
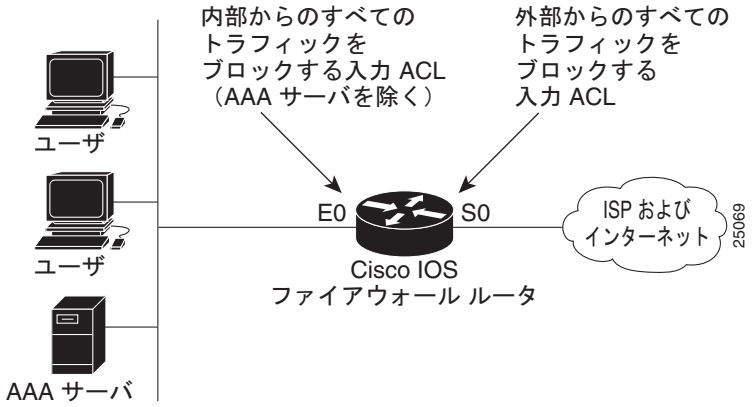


図 5 に示す認証プロキシは、ダイヤルイン インターフェイスに適用され、すべてのネットワーク トラフィックが各インターフェイスでブロックされます。

図 5　外部インターフェイスでの認証プロキシの適用



ワンタイム パスワード（OTP）を使用した動作

One-Time Password（OTP; ワンタイム パスワード）を使用する場合、ユーザはユーザ名とワンタイム パスワードを HTML のログイン ページに通常どおり入力します。

ユーザは、最初の 3 回の試行の間に正しいトークン パスワードを入力する必要があります。入力を 3 回間違えた場合、2 つの有効なトークン パスワードを続けて入力しないと、AAA サーバでの認証が許可されません。

他のセキュリティ機能との互換性

この認証プロキシは、次に示す Cisco IOS ソフトウェアおよび Cisco IOS のセキュリティ機能と互換性があります。

- Cisco IOS Firewall Intrusion Detection System（IDS）
- NAT
- CBAC
- IPSec 暗号化
- VPN クライアント ソフトウェア

認証プロキシは、Cisco IOS Firewall IDS および IPSec 暗号化機能と透過的に連動します。次のセクションでは、NAT、CBAC、および VPN クライアント ソフトウェアの各機能と認証プロキシの関係について説明します。

- 「NAT の互換性」
- 「CBAC との互換性」
- 「VPN クライアントの互換性」

NAT の互換性

認証プロキシ機能は、ACL と認証が NAT 変換の前に完了している場合にだけ、NAT と互換性があります。NAT は認証プロキシ機能と互換性がありますが、認証プロキシを使用するうえで NAT は必須ではありません。

CBAC との互換性

認証プロキシは、CBAC セキュリティ機能と互換性がありますが、認証プロキシ機能を使用するために CBAC は必須ではありません。

認証プロキシの認可は、手動で作成された ACL の先頭に動的に追加されるアクセス コントロール エントリ（ACE）を返します。それ以降、ACL を「保護された側」のインバウンドインターフェイスに適用し、認可されたユーザの送信元 IP アドレスのリモート ネットワークへのアクセスを許可または禁止します。

VPN クライアントの互換性

ネットワーク管理者は、認証プロキシを使用して、VPN クライアント トラフィックに対し、追加のセキュリティ レイヤとアクセス コントロールを適用できます。VPN クライアントが HTTP 接続を開始した場合、認証プロキシはまず既存のクライアント認証を確認します。クライアントが認証済みの場合、認可されたトラフィックは許可されます。クライアントが認証済みでない場合、HTTP 要求によって認証プロキシが起動され、ユーザに対しユーザ名とパスワードの入力が求められます。

ユーザ認証が成功した場合、認証プロキシは AAA サーバからユーザ プロファイルを取得します。ユーザ プロファイル エントリ内の送信元アドレスは、復号化されたパケット内の、認証済み VPN クライアントの IP アドレスで置き換えられます。

AAA アカウンティングとの互換性

認証プロキシを使用して、課金やセキュリティ監査で使用するために十分な情報を含む「開始」および「停止」アカウンティング レコードを生成できます。そうすることで、認証プロキシ サービスを使用する認証済みホストの動作をモニタできます。

認証プロキシのキャッシュと関連付けられている動的アクセス コントロール リストが作成されると、認証プロキシは認証済みホストからのトラフィックの追跡を開始します。アカウンティングでは、このイベントに関するデータが、他のユーザのデータとともにデータ構造に保存されます。アカウンティング開始オプションがイネーブルになっている場合、この時点でアカウンティング レコード（「開始」レコード）を生成できます。認証済みホストからの以降のトラフィックは、認証プロキシによって作成された動的な ACL がパケットを受信すると記録されます。

認証プロキシのキャッシュが満了して削除されると、経過時間などの追加のデータがアカウンティング情報に追加され、「停止」レコードがサーバに送信されます。この時点で、情報がデータ構造から削除されます。

認証プロキシ ユーザ セッションに対するアカウンティング レコードは、キャッシュおよび動的 ACL の使用に関連付けられます。

（注） アカウンティング レコードは、RADIUS と TACACS+ の両方に対し、RADIUS アトリビュート 42、46、および 47 を含んでいる必要があります。

RADIUS アトリビュートの詳細については、付録「RADIUS アトリビュート」を参照してください。

DoS 攻撃（サービス拒絶攻撃）からの保護

認証プロキシは、受信 HTTP 要求のレベルをモニタします。各要求に対し、認証プロキシはユーザのログイン クレデンシャルの入力を求めます。オープン要求が多い場合、ルータが DoS 攻撃を受けていることを示している可能性があります。認証プロキシは、オープン要求のレベルを制限し、オープン要求の数が 40 未満になるまで、追加の要求をドロップします。

ファイアウォールが、認証が必要な大量の接続要求を受信している場合、正規のネットワーク ユーザが接続を行うときに遅延が発生したり、接続が拒否されて接続の再試行が必要になることがあります。

認証プロキシでのスプーフィングの危険性

認証プロキシが起動されると、ユーザ アクセス権を持つインターフェイスを一時的に再設定することで、ファイアウォール中に動的な開口が作成されます。この開口が存在する間に、別のホストが認証済みユーザのアドレスを偽装し、ファイアウォールの背後へのアクセスを獲得する可能性があります。認証プロキシは、アドレス スプーフィングの問題を起こしません。この問題は、ユーザの関心事としてここに明記しています。スプーフィングは、すべてのアクセス リストにつきまとう問題であり、認証プロキシは特にこの問題に対処していません。

Lock-and-Key 機能との比較

Lock-and-Key は、認証とダイナミック アクセス リストを使用して、ファイアウォールを通じたユーザ アクセスを可能にする、Cisco IOS Firewall のもう 1 つの機能です。表 2 に、認証プロキシと Lock-and-Key 機能の比較を示します。

表 2　認証プロキシ機能と Lock-and-Key 機能の比較

Lock-and-Key	認証プロキシ
Telnet 接続要求により起動	HTTP 接続要求により起動
TACACS+、RADIUS、またはローカル認証	TACACS+ または RADIUS 認証および認可
アクセス リストはルータだけで設定	アクセス リストは必ず AAA サーバから取得
アクセス権は、ユーザのホスト IP アドレスに基づいて許可	アクセス権は、ユーザごとおよびホスト IP アドレスごとに許可
アクセス リストは、各ホスト IP アドレスに対し 1 つに制限	アクセス リストは、AAA サーバ上のユーザ プロファイルによって定義された複数のエントリを持つことが可能
固定の IP アドレスを特定のユーザに関連付け。ユーザは、その IP アドレスを持つホストからログインする必要あり。	DHCP ベースのホストの AP アドレスを許可。つまり、ユーザは、任意のホストからログインし、認証と認可を受けることが可能。

認証プロキシは、ユーザごとのセキュリティ ポリシーを提供する任意のネットワーク環境で使用します。Lock-and-Key は、ローカル認証と、ホスト アドレスに基づく限定的な数のルータベースのアクセス コントロール ポリシーの恩恵を受けるネットワーク環境で使用します。Lock-and-Key は、Cisco Secure Integrated Software を使用しない環境で使用します。

認証プロキシの設定方法

認証プロキシ機能を設定するには、次の手順を実行します。

- 「AAA の設定」（必須）
- 「認証プロキシ用の HTTP サーバの設定」（必須）
- 「認証プロキシの設定」（必須）
- 「認証プロキシの確認」（任意）

この章に示すコマンドを使用した認証プロキシの設定例については、この章の最後にある「認証プロキシの設定例」のセクションを参照してください。

AAA の設定

AAA サービス用に認証プロキシを設定する必要があります。認可をイネーブルにし認可方式を定義するには、次のコマンドをグローバル コンフィギュレーション モードで使用します。

	コマンド	目的
ステップ 1	router(config)# **aaa new-model**	ルータで AAA 機能をイネーブルにします。
ステップ 2	router(config)# **aaa authentication login default** *TACACS+ RADIUS*	ログイン時の認証方式リストを定義します。
ステップ 3	router(config)# **aaa authorization auth-proxy default** [*method1* [*method2*...]]	**auth-proxy** キーワードを使用して、AAA 方式に対する認証プロキシをイネーブルにします。
ステップ 4	router(config)# **aaa accounting auth-proxy default start-stop group tacacs+**	**auth-proxy** キーワードを使用して、認可ポリシーを、ダウンロード可能なダイナミック ACL として設定します。このコマンドは、認証プロキシのアカウンティングをアクティブ化します。
ステップ 5	router(config)# **tacacs-server host** *hostname*	AAA サーバを指定します。RADIUS サーバの場合は、**radius server host** コマンドを使用します。
ステップ 6	router(config)# **tacacs-server key** *key*	ルータと AAA サーバとの間の通信用の認証および暗号化キーを設定します。RADIUS サーバの場合、**radius server key** コマンドを使用します。
ステップ 7	router(config)# **access-list** *access-list-number* **permit tcp host** *source* **eq** *tacacs* **host** *destination*	AAA サーバがトラフィックをファイアウォールに返すのを許可する ACL エントリを作成します。送信元アドレスは AAA サーバの IP アドレスで、宛先は AAA サーバが存在するルータ インターフェイスの IP アドレスです。

認証プロキシでは、ファイアウォール ルータで AAA を設定するのに加えて、ユーザごとのアクセス プロファイル設定が AAA サーバ上に必要です。認証プロキシをサポートするために、ここに示す概要に従い、AAA 認可サービス **auth-proxy** を AAA サーバ上で設定します。

- **auth-proxy** キーワードに対する個別の認可セクションを定義して、ダウンロード可能なユーザ プロファイルを指定します。このキーワードは、EXEC などの他の種類のサービスと干渉しません。次に、TACACS サーバ上のユーザ プロファイルの例を示します。

```
default authorization = permit
key = cisco
user = newuser1 {
login = cleartext cisco
```

```
service = auth-proxy
{
priv-lvl=15
proxyacl#1="permit tcp any any eq 26"
proxyacl#2="permit icmp any host 60.0.0.2"
proxyacl#3="permit tcp any any eq ftp"
proxyacl#4="permit tcp any any eq ftp-data"
proxyacl#5="permit tcp any any eq smtp"
proxyacl#6="permit tcp any any eq telnet"
}
}
```

- AAA サーバのユーザ設定でサポートされる唯一のアトリビュートは、proxyacl#n です。プロファイル中のアクセス リストを設定する際には、proxyacl#n アトリビュートを使用します。アトリビュート proxyacl#n は、RADIUS と TACACS+ の両方の attribute-value（AV）のペア用です。
- すべてのユーザの特権レベルは 15 に設定する必要があります。
- AAA サーバ上のユーザ プロファイル内のアクセス リストには、**permit** キーワードだけを含むアクセス コマンドが必要です。
- 各ユーザ プロファイル アクセス リスト エントリの **any** キーワードに、送信元アドレスを設定します。ユーザ プロファイルがファイアウォールにダウンロードされるとき、アクセス リスト中の送信元アドレスは、認証プロキシ要求を行うホストの送信元アドレスで置き換えられます。
- サポートされる AAA サーバは次のとおりです。
  - CiscoSecure ACS 2.1.x for Windows NT
  - CiscoSecure ACS 2.3 for Windows NT
  - CiscoSecure ACS 2.2.4 for UNIX
  - CiscoSecure ACS 2.3 for UNIX
  - TACACS+ サーバ（vF4.02.alpha）
  - Ascend RADIUS サーバ radius-980618（必須のアトリビュートと値のペアのパッチ）
  - Livingston RADIUS サーバ（v1.16）

AAA サーバの設定例については、「AAA サーバのユーザ プロファイル例」のセクションを参照してください。

認証プロキシ用の HTTP サーバの設定

この作業は、ファイアウォール上で HTTP サーバをイネーブルにし、認証プロキシ用に HTTP サーバの AAA 認証方式を設定するために使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **ip http access-class** *access-list-number*

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip http server** **例：** Router# ip http server	ルータ上で HTTP サーバをイネーブルにします。認証プロキシは HTTP サーバを使用してクライアントと通信し、ユーザ認証を行います。
ステップ 4	**ip http access-class** *access-list-number* **例：** router(config)# configure terminal	HTTP サーバのアクセス リストを指定します。「インターフェイスの設定例」のセクションで設定する標準のアクセス リスト番号を使用します。

認証プロキシの設定

認証プロキシを設定するには次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip auth-proxy auth-cache-time** *min*
4. **ip auth-proxy auth-proxy-banner**
5. **ip auth-proxy name** *auth-proxy-name* **http** [**auth-cache-time** *min*] [**list** {*acl* | *acl-name*}]
6. **interface** *type*
7. **ip auth-proxy** *auth-proxy-name*

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** Router# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**ip auth-proxy auth-cache-time** *min* **例：** `Router(config)# ip auth-proxy auth-cache-time 5`	（任意）グローバル認証プロキシ アイドル タイムアウト値を分単位で設定します。タイムアウトが発生すると、ユーザ認証エントリと、関連付けられているダイナミック アクセス リストがすべて削除されます。デフォルト値は 60 分です。 **（注）** このオプションは、任意の認証プロキシ ルールに対して使用し、任意の CBAC 検査ルールのアイドル タイムアウト値よりも大きな値に設定します。認証プロキシが認証キャッシュとそれに関連付けられているダイナミック ユーザ ACL を削除するとき、CBAC によってモニタされているいくつかのアイドル接続が存在する可能性があり、ユーザ固有の ACL を削除すると、これらのアイドル接続がハングするおそれがあります。CBAC のアイドル タイムアウトが短ければ、アイドル タイムアウトが発生したとき（つまり、認証プロキシがユーザ プロファイルを削除する前）に CBAC はこれらの接続をリセットします。
ステップ 4	**ip auth-proxy auth-proxy-banner** **例：** `Router(config)# configure terminal`	（任意）認証プロキシのログイン ページにファイアウォール ルータの名前を表示します。デフォルトではバナーはディセーブルになっています。

	コマンド	目的
ステップ 5	**ip auth-proxy name** *auth-proxy-name* **http** [**auth-cache-time** *min*] [**list** {*acl* |*acl-name*}] 例： Router(config)# ip auth-proxy name HQ_users http	認証プロキシ ルールを作成します。ルールは、認証プロキシの適用方法を定義します。このコマンドは、HTTP プロトコル トラフィックを開始する接続を、認証プロキシ名に関連付けます。名前付きのルールをアクセス コントロール リスト（ACL）に関連付け、どのホストが認証プロキシ機能を使用するかを制御できます。標準のアクセス リストが定義されていない場合、名前付き認証プロキシ ルールが、接続開始パケットが設定済みのインターフェイスで受信されるすべてのホストからの HTTP トラフィックを代行受信します。 （任意）**auth-cache-time** オプションは、グローバル認証プロキシ キャッシュ タイマーを上書きします。このオプションにより、特定の認証プロキシ ルールに対し、タイムアウト値をより詳細に制御できます。値を指定しない場合、プロキシ ルールは、**ip auth-proxy auth-cache-time** コマンドで設定された値を使用します。 （任意）**list** オプションを使用すると、標準のアクセス リスト、拡張（1 ～ 199）アクセス リスト、または名前付きアクセス リストを、名前付き認証プロキシ ルールに適用できます。アクセス リスト中のホストによって開始された HTTP 接続は、認証プロキシによって代行受信されます。
ステップ 6	**interface** *type* 例： Router(config)# interface Ethernet0/0	認証プロキシを適用するインターフェイス タイプを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip auth-proxy** *auth-proxy-name* 例： Router(config-if)# ip auth-proxy HQ_users http	インターフェイス コンフィギュレーション モードで、名前付き認証プロキシのルールをインターフェイスに適用します。このコマンドにより、指定の名前を持つ認証プロキシのルールがイネーブルになります。

認証プロキシの確認

認証プロキシの設定の確認には、次のいくつかの項目が含まれます。

- 「認証プロキシの設定の確認」（任意）
- 「JavaScript を使用したユーザ接続の確立」（任意）
- 「JavaScript を使用しないユーザ接続の確立」（任意）

認証プロキシの設定の確認

現在の認証プロキシの設定を確認するには、特権 EXEC モードで **show ip auth-proxy configuration** コマンドを使用します。

コマンド	目的
`router# show ip auth-proxy configuration`	認証プロキシの設定を表示します。

次の例で、グローバル認証プロキシ アイドル タイムアウト値は 60 分に設定され、名前付き認証プロキシ ルールは「pxy」であり、この名前付きルールのアイドル タイムアウト値は 1 分です。表示内容は、ホスト リストが指定されていないことを示しています。つまり、そのインターフェイスでのすべての接続開始 HTTP トラフィックに認証プロキシ ルールが適用されます。

```
router# show ip auth-proxy configuration
Authentication cache time is 60 minutes
Authentication Proxy Rule Configuration
Auth-proxy name pxy
http list not specified auth-cache-time 1 minutes
```

認証プロキシがルータで正常に設定されていることを確認するには、ルータを通じて HTTP 接続を開始するようユーザに依頼します。そのユーザに対し、AAA サーバで認証と認可が設定されている必要があります。ユーザ認証が成功した場合、ファイアウォールはそのユーザの HTTP 接続を完了します。認証が成功しなかった場合は、アクセス リストと AAA サーバの設定を確認します。

特権 EXEC モードで **show ip auth-proxy cache** コマンドを使用し、ユーザ認証エントリを表示します。

コマンド	目的
`router# show ip auth-proxy cache`	ユーザ認証エントリのリストを表示します。

認証プロキシ キャッシュにより、ホストの IP アドレス、送信元ポート番号、認証プロキシのタイムアウト値、接続の状態が一覧表示されます。認証プロキシの状態が HTTP_ESTAB の場合、ユーザ認証が成功したことを示します。

```
router# show ip auth-proxy cache
Authentication Proxy Cache
 Client IP 192.168.25.215 Port 57882, timeout 1, state HTTP_ESTAB
```

1 分間（この名前付きルールのタイムアウト値）待ち、ユーザに再度接続を試みるよう依頼します。1 分後、ユーザの接続は拒否されます。これは、認証プロキシにより、ユーザの認証エントリと、関連付けられているすべてのダイナミック ACL が削除されたためです。ユーザに対し新しい認証ログインページが表示され、ファイアウォールを通じてアクセスするには再度ログインする必要があります。

JavaScript を使用したユーザ接続の確立

クライアント ブラウザで JavaScript をイネーブルにした状態で認証プロキシを使用したクライアント接続を確認するには次の手順を実行します。

ステップ 1 クライアント ホストから、ファイアウォールを通じて HTTP 接続を開始します。これにより、認証プロキシのログイン ページが生成されます。

ステップ 2 認証プロキシのログイン ページで、ユーザ名とパスワードを入力します。

ステップ 3 [OK] をクリックしてユーザ名とパスワードを AAA サーバに送信します。

ログインが成功したか失敗したかを示すポップアップ ウィンドウが表示されます。認証に成功した場合、接続が自動的に完了します。認証が失敗した場合、認証プロキシは、ユーザに失敗したことを報告し、何度か再試行するかどうかを訪ねます。

（注） 認証に 5 回失敗した場合、ユーザは 2 分間待ってから、認証プロキシを起動する別の HTTP セッションを開始する必要があります。

JavaScript を使用しないユーザ接続の確立

セキュアな認証を行うために、認証プロキシの設計では JavaScript が必要です。ブラウザで JavaScript をイネーブルにせずに認証プロキシを使用することもできますが、ユーザがネットワーク接続を正しく確立しなかった場合にセキュリティ リスクが生じます。次に、JavaScript をディセーブルにした状態で接続を確立するための正しい手順を示します。ネットワーク管理者は、このセクションの手順を使用して、接続を適切に確立する方法をユーザに指示することを強く推奨します。

（注） この手順に従わないと、ユーザのクレデンシャルが認証プロキシ以外のネットワーク Web サーバに渡されたり、認証プロキシによってログインが拒否されるおそれがあります。

クライアント ブラウザで JavaScript がイネーブルでないときに認証プロキシを使用したクライアント接続を確認するには、次の手順を実行します。

ステップ 1 ファイアウォールを通じて HTTP 接続を開始します。

これにより、認証プロキシのログイン ページが生成されます。

ステップ 2 クライアントで、認証プロキシのログイン ページから、ユーザ名とパスワードを入力します。

ステップ 3 [OK] をクリックしてユーザ名とパスワードを AAA サーバに送信します。

ログインが成功したか失敗したかを示すポップアップ ウィンドウが表示されます。ポップアップ ウィンドウに認証が成功したことが表示される場合は、ステップ 7 に進みます。

ステップ 4 ポップアップ ウィンドウに、認証失敗のメッセージが表示される場合は、ブラウザの [File] メニューの [Close] をクリックします。

（注） ポップアップ ウィンドウを閉じるために、[Reload]（Internet Explorer の場合は [Refresh]）をクリックしないでください。

ステップ 5 元の認証ログイン ページで、ブラウザ ツールバーの [Reload]（Internet Explorer の場合は [Refresh]）クリックします。ユーザのログイン クレデンシャルがフォームからクリアされます。

（注） [OK] をクリックしないでください。再度ログインする前に、ユーザ名とパスワードをクリアし、フォームをリロードするには、[Reload] または [Refresh] をクリックする必要があります。

ステップ 6 ユーザ名とパスワードを再度入力します。

認証に成功した場合、ウィンドウが開き、認証成功を示すメッセージが表示されます。認証失敗のメッセージがウィンドウに表示される場合は、ステップ 4 に進みます。

ステップ 7 ブラウザの [File] メニューで [Close] をクリックします。

ステップ 8 元の認証プロキシのログイン ページで、[Reload]（Internet Explorer の場合は [Refresh]）クリックします。

認証プロキシは、Web サーバとの認証済みの接続を完了します。

認証プロキシのモニタおよびメンテナンス

ここでは、ダイナミック アクセス リスト エントリを表示する方法と、認証エントリを手動で削除する方法について説明します。ここでは、次の各手順について説明します。

- 「ダイナミック ACL エントリの表示」
- 「認証プロキシのキャッシュ エントリの削除」

ダイナミック ACL エントリの表示

ダイナミック アクセス リスト エントリは、使用中に表示できます。管理者またはアイドル タイムアウト パラメータによって認証プロキシ エントリがクリアされた後は、表示できなくなります。表示される一致の数は、アクセス リスト エントリがヒットした回数を示します。

認証プロキシによって現在確立されているダイナミック アクセス リスト エントリと一時的なアクセス リスト エントリを表示するには、特権 EXEC モードで **show ip access-lists** コマンドを使用します。

コマンド	目的
`router# show ip access-lists`	ダイナミック ACL エントリを含め、ファイアウォールで設定済みの標準アクセス リストおよび拡張アクセス リストを表示します。

次の例では、ACL 105 が、認証プロキシを設定する入力インターフェイスでインバウンド方向に適用されています。最初の表示は、認証前の ACL の内容を示しています。2 番めの表示は、AAA サーバによるユーザ認証後の同じ表示を示しています。

（注） NAT が設定されている場合、**show ip access list** コマンドにより、ダイナミック ACL エントリの変換後のホスト IP アドレスか、接続を開始したホストの IP アドレスが表示される場合があります。NAT の外部インターフェイスに対して ACL が適用される場合、変換後のアドレスが表示されます。ACL が NAT の内部インターフェイスに適用される場合、接続を開始するホストの IP アドレスが表示されます。**show ip auth-proxy cache** コマンドで、常に接続を開始したホストの IP アドレスが表示されます。

たとえば、次に示すのは、認証プロキシの前の ACL エントリのリストです。

```
Router# show ip access-lists
     .
     .
     .
Extended IP access list 105
 deny tcp any any eq telnet
 deny udp any any
 permit tcp any any (28 matches)
 permit ip any any
```

次の出力例は、ユーザ認証後の ACL エントリのリストを示しています。

```
Router# show ip access-lists
     .
     .
     .
Extended IP access list 105
! The ACL entries following user authentication are shown below.
 permit tcp host 192.168.25.215 any eq 26
 permit icmp host 192.168.25.215 host 60.0.0.2
 permit tcp host 192.168.25.215 any eq telnet
 permit tcp host 192.168.25.215 any eq ftp
 permit tcp host 192.168.25.215 any eq ftp-data
 permit tcp host 192.168.25.215 any eq smtp
 deny tcp any any eq telnet
 deny udp any any
 permit tcp any any (76 matches)
 permit ip any any
```

認証プロキシのキャッシュ エントリの削除

認証プロキシを使用中の場合、ダイナミック アクセス リストは、認証エントリの追加および削除に伴って動的に増減します。認証エントリのリストを表示するには、**show ip auth-proxy cache** コマンドを使用します。認証エントリを手動で削除するには、特権 EXEC モードで **clear ip auth-proxy cache** コマンドを使用します。

コマンド	目的
router# **clear ip auth-proxy cache** {* | *host ip address*}	タイムアウト前にファイアウォールから認証プロキシ エントリを削除します。すべての認証キャッシュ エントリを削除するにはアスタリスクを使用します。単一のホストのエントリを削除するには、特定の IP アドレスを入力します。

認証プロキシの設定例

認証プロキシ機能を設定するには、ルータと AAA サーバの両方の設定を変更する必要があります。以降のセクションでは、認証プロキシの設定例について説明します。

- 「認証プロキシの設定例」
- 「認証プロキシ、IPSec、および CBAC の設定例」
- 「認証プロキシ、IPSec、NAT、および CBAC の設定例」
- 「AAA サーバのユーザ プロファイル例」

これらの例全体で、感嘆符（!）はコメント行を示します。コメント行は、説明している設定エントリの前に記載されています。

認証プロキシの設定例

以降の例では、特定の認証プロキシの設定エントリを取り上げています。これらの例は、完全なルータ設定を表すものではありません。認証プロキシを使用した完全なルータの設定は、この章の後のセクションに含まれています。

ここでは、次の例について説明します。

- 「AAA の設定例」
- 「HTTP サーバの設定例」
- 「認証プロキシの設定例」
- 「インターフェイスの設定例」

AAA の設定例

```
aaa new-model
aaa authentication login default group tacacs group radius
! Set up the aaa new model to use the authentication proxy.
aaa authorization auth-proxy default group tacacs group radius
! Define the AAA servers used by the router.
aaa accounting auth-proxy default start-stop group tacacs+
! Set up authentication proxy with accounting.
tacacs-server host 172.31.54.143
tacacs-server key cisco
radius-server host 172.31.54.143
radius-server key cisco
```

HTTP サーバの設定例

```
! Enable the HTTP server on the router.
ip http server
! Set the HTTP server authentication method to AAA.
ip http authentication aaa
! Define standard access list 61 to deny any host.
access-list 61 deny any
! Use ACL 61 to deny connections from any host to the HTTP server.
ip http access-class 61
```

認証プロキシの設定例

```
! Set the global authentication proxy timeout value.
ip auth-proxy auth-cache-time 60
! Apply a name to the authentication proxy configuration rule.
ip auth-proxy name HQ_users http
```

インターフェイスの設定例

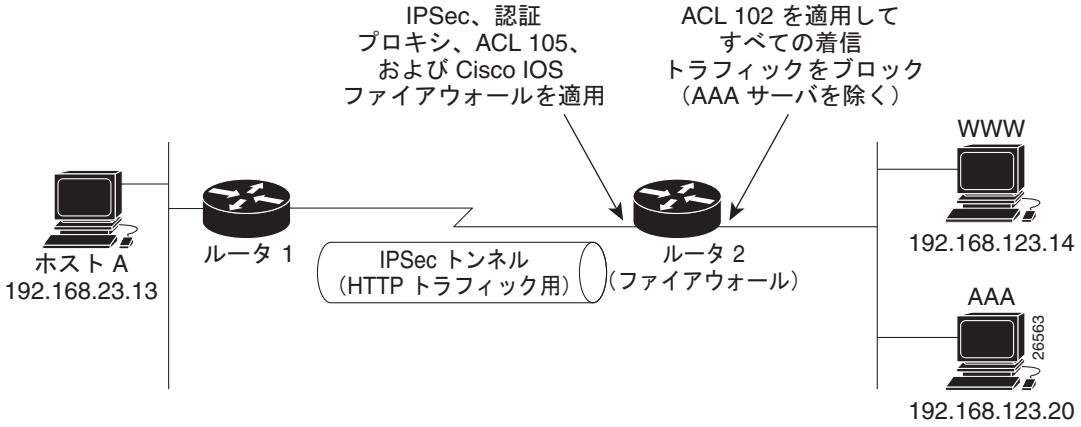
```
! Apply the authentication proxy rule at an interface.
interface e0
    ip address 10.1.1.210 255.255.255.0
    ip auth-proxy HQ_users
```

認証プロキシ、IPSec、および CBAC の設定例

次の例は、認証プロキシ、IPSec および CBAC 機能を使用するルータ設定を示します。図 6 に、設定を示します。

（注） 本機能を Cisco IOS ソフトウェア リリース 12.3(8)T 以降で使用する場合は、『Crypto Access Check on Clear-Text Packets』を参照してください。

図 6　　認証プロキシ、IPSec、および CBAC の設定例



この例では、ホスト A が Web サーバ（WWW）との HTTP 接続を開始します。ルータ 1 とルータ 2 間の HTTP トラフィックは、IPSec を使用して暗号化されます。認証プロキシ、IPSec、および CBAC は、ルータ 2 上のインターフェイス Serial0 で設定され、ファイアウォールとして機能しています。ACL 105 は、インターフェイス Serial0 ですべてのトラフィックをブロックします。ACL 102 は、ルータ 2 上のインターフェイス Ethernet0 に適用され、AAA サーバからのトラフィックを除くそのインターフェイス上のすべてのトラフィックをブロックします。

ホスト A が Web サーバとの HTTP 接続を開始すると、認証プロキシはホスト A でユーザ名とパスワードを入力するようユーザに要求します。これらのクレデンシャルは、認証および許可のために AAA サーバで検証されます。認証が正常に行われると、ユーザごとの ACL がファイアウォールにダウンロードされ、サービスが許可されます。

次の例では、完全を期すためにルータ 1 とルータ 2 の両方の設定を示します。

- 「ルータ 1 の設定例」
- 「ルータ 2 の設定例」

ルータ 1 の設定例

```
! Configure Router 1 for IPSec.
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router1
!
logging buffered 4096 debugging
no logging console
enable secret 5 $1$E0OB$AQF1vFZM3fLr3LQAOsudL/
enable password junk
!
username Router2 password 0 welcome
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco1234 address 10.0.0.2
!
crypto ipsec transform-set rule_1 ah-sha-hmac esp-des esp-sha-hmac
!
!
 crypto map testtag 10 ipsec-isakmp
 set peer 10.0.0.2
 set transform-set rule_1
 match address 155
!
interface Ethernet0/0
 ip address 192.168.23.2 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Serial3/1
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 encapsulation PPP
 ip route-cache
 no ip mroute-cache
 no keepalive
 no fair-queue
 clockrate 56000
 crypto map testtag
!
!
ip classless
ip route 192.168.123.0 255.255.255.0 10.0.0.2
! Identify the IPSec specific traffic.
access-list 155 permit tcp host 192.168.23.13 host 192.168.123.14 eq www
access-list 155 permit tcp host 192.168.23.13 eq www host 192.168.123.14
```

ルータ 2 の設定例

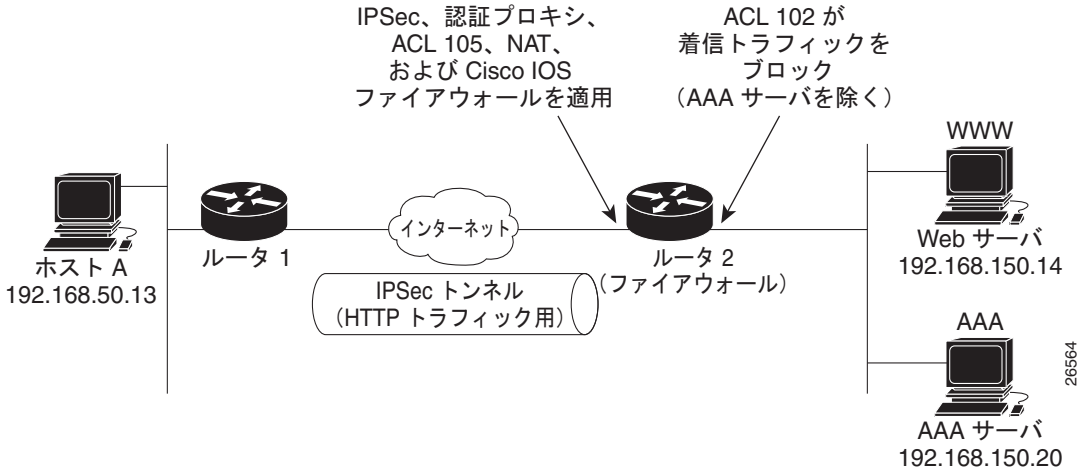
```
! Configure Router 2 as the firewall, using the authentication proxy, IPSec, and CBAC.
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router2
!
logging buffered 4096 debugging
aaa new-model
aaa authentication login default group tacacs
aaa authentication login console_line none
aaa authentication login special none
aaa authentication ppp default group tacacs
aaa authorization exec default group tacacs
! Configure AAA for the authentication proxy.
aaa authorization auth-proxy default group tacacs+
enable password junk
!
! Create the CBAC inspection rule HTTP_TEST.
ip inspect name rule22 http
ip inspect name rule22 tcp
ip inspect name rule22 ftp
ip inspect name rule22 smtp
!
! Create the authentication proxy rule PXY.
ip auth-proxy name pxy http
! Turn on display of the router name in the authentication proxy login page.
ip auth-proxy auth-proxy-banner
ip audit notify log
ip audit po max-events 100
!
! Configure IPSec.
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco1234 address 10.0.0.1
!
crypto ipsec transform-set rule_1 ah-sha-hmac esp-des esp-sha-hmac
!
 crypto map testtag 10 ipsec-isakmp
 set peer 10.0.0.1
 set transform-set rule_1
 match address 155
!
! Apply the CBAC inspection rule and the authentication proxy rule at interface
! Serial0/0.
interface Serial0/0
 ip address 10.0.0.2 255.0.0.0
 ip access-group 105 in
 no ip directed-broadcast
 ip inspect rule22 in
 ip auth-proxy pxy
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 no keepalive
 no fair-queue
crypto map testtag
!
interface Ethernet0/1
 ip address 192.168.123.2 255.255.255.0
```

```
 ip access-group 102 in
 no ip directed-broadcast
 ip route-cache
 no ip mroute-cache
!
no ip classless
ip route 192.168.23.0 255.255.255.0 10.0.0.1
ip route 192.168.50.0 255.255.255.0 16.0.0.1
! Configure the HTTP server.
ip http server
ip http access-class 15
ip http authentication aaa
!
! Create ACL 15 to block all traffic for the http server.
access-list 15 deny any
! Create ACL 102 to block all traffic inbound on interface Ethernet0/1 except for
! traffic from the AAA server.
access-list 102 permit tcp host 192.168.123.20 eq tacacs host 192.168.123.2
access-list 102 deny   tcp any any
access-list 102 deny   udp any any
access-list 102 permit ip any any
! Create ACL 105 to block all traffic inbound on interface Serial0/0. Permit only IP
! protocol traffic.
access-list 105 deny   tcp any any
access-list 105 deny   udp any any
access-list 105 permit ip any any
! Identify the IPSec specific traffic.
access-list 155 permit tcp host 192.168.123.14 host 192.168.23.13 eq www
access-list 155 permit tcp host 192.168.123.14 eq www host 192.168.23.13
!
! Define the AAA server host and encryption key.
tacacs-server host 192.168.123.14
tacacs-server key cisco
!
line con 0
 exec-timeout 0 0
 login authentication special
 transport input none
line aux 0
 transport input all
 speed 38400
 flowcontrol hardware
line vty 0 4
 password lab
```

認証プロキシ、IPSec、NAT、および CBAC の設定例

次の例は、認証プロキシ、IPSec、NAT および CBAC 機能を使用するルータ設定を示します。図 7 に、設定を示します。

図 7　認証プロキシ、IPSec、および CBAC の設定例



この例では、ホスト A が Web サーバ（WWW）との HTTP 接続を開始します。ルータ 1（インターフェイス BRI0）とルータ 2（インターフェイス Serial2）の間の HTTP トラフィックは、IPSec を使用して暗号化されます。認証プロキシは、ファイアウォールとして動作するルータ 2 で設定されます。認証プロキシ、NAT、および CBAC は、インターフェイス Serial2 で設定され、ファイアウォールとして機能しています。ACL 105 は、インターフェイス Serial2 ですべてのトラフィックをブロックします。ACL 102 は、ルータ 2 上のインターフェイス Ethernet0 に適用され、AAA サーバからのトラフィックを除くそのインターフェイス上のすべてのトラフィックをブロックします。この例で、認証プロキシは標準の ACL 10 を使用して、認証プロキシ機能を使用するホストを指定しています。

ACL 10 内のいずれかのホストが Web サーバとの HTTP 接続を開始すると、認証プロキシは、そのホストのユーザに対し、ユーザ名とパスワードの入力を求めます。これらのクレデンシャルは、認証および許可のために AAA サーバで検証されます。認証が正常に行われると、ユーザごとの ACL がファイアウォールにダウンロードされ、サービスが許可されます。

次の例では、完全を期すためにルータ 1 とルータ 2 の両方の設定を示します。

- 「ルータ 1 の設定例」
- 「ルータ 2 の設定例」

ルータ 1 の設定例

```
! Configure router 1 for IPSec.
version 12.0
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname Router1
 !
 logging buffered 4096 debugging
 no logging console
```

```
 !
isdn switch-type basic-5ess
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco1234 address 16.0.0.2
 crypto ipsec transform-set rule_1 ah-sha-hmac esp-des esp-sha-hmac
 !
  !
  crypto map testtag 10 ipsec-isakmp
  set peer 16.0.0.2
  set transform-set rule_1
  match address 155
 !
 !
 process-max-time 200
 !
 interface BRI0
  ip address 16.0.0.1 255.0.0.0
  no ip directed-broadcast
  encapsulation ppp
  dialer idle-timeout 5000
  dialer map ip 16.0.0.2 name router2 broadcast 50006
  dialer-group 1
  isdn switch-type basic-5ess
  crypto map testtag
 !
 interface FastEthernet0
  ip address 192.168.50.2 255.255.255.0
  no ip directed-broadcast
 !
 ip classless
 ip route 192.168.150.0 255.255.255.0 16.0.0.2
 no ip http server
! Identify the IPSec specific traffic.
 access-list 155 permit tcp host 192.168.50.13 host 192.168.150.100 eq www
 access-list 155 permit tcp host 192.168.50.13 eq www host 192.168.150.100
 dialer-list 1 protocol ip permit
 !
 line con 0
  exec-timeout 0 0
  transport input none
 line aux 0
 line vty 0 4
  password lab
  login
```

ルータ 2 の設定例

```
! Configure router 2 as the firewall, using the authentication proxy, IPSec, NAT, and
! CBAC.
 version 12.0
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname router2
 !
 logging buffered 4096 debugging
 aaa new-model
 aaa authentication login default group tacacs+
 aaa authentication login console_line none
```

```
 aaa authorization exec default group tacacs+
 ! Configure AAA for the authentication proxy.
 aaa authorization auth-proxy default group tacacs+
!
 ! Create the CBAC inspection rule “rule44.”
 ip inspect name rule44 http java-list 5
 ip inspect name rule44 tcp
 ip inspect name rule44 ftp
 ip inspect name rule44 smtp
 !
 ! Create the authentication proxy rule “pxy.” Set the timeout value for rule
 ! pxy to three minutes. Standard ACL 10 is applied to the rule.
 ip auth-proxy name pxy http list 10 auth-cache-time 3
 isdn switch-type primary-5ess
 !
 ! Configure IPSec.
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco1234 address 16.0.0.1
 !
 !
 crypto ipsec transform-set rule_1 ah-sha-hmac esp-des esp-sha-hmac
 !
  !
  crypto map testtag 10 ipsec-isakmp
  set peer 16.0.0.1
  set transform-set rule_1
  match address 155
!
 controller T1 2/0
  framing esf
  linecode b8zs
  pri-group timeslots 1-24
!
! Apply ACL 102 inbound at interface Ethernet0/1 and configure NAT.
interface Ethernet0/1
 ip address 192.168.150.2 255.255.255.0
 ip access-group 102 in
 no ip directed-broadcast
 ip nat inside
 no ip mroute-cache
!
! Apply the authentication proxy rule PXY, CBAC inspection rule HTTP_TEST, NAT, and
! and ACL 105 at interface Serial2/0:23.
interface Serial2/0:23
 ip address 16.0.0.2 255.0.0.0
 ip access-group 105 in
 no ip directed-broadcast
 ip nat outside
 ip inspect rule44 in
 ip auth-proxy pxy
 encapsulation ppp
 ip mroute-cache
 dialer idle-timeout 5000
 dialer map ip 16.0.0.1 name router1 broadcast 71011
 dialer-group 1
 isdn switch-type primary-5ess
 fair-queue 64 256 0
 crypto map testtag
!
! Use NAT to translate the Web server address.
ip nat inside source static 192.168.150.14 192.168.150.100
ip classless
ip route 192.168.50.0 255.255.255.0 16.0.0.1
```

```
! Configure the HTTP server.
ip http server
ip http access-class 15
ip http authentication aaa
!
! Create standard ACL 5 to specify the list of hosts from which to accept java applets.
! ACL 5 is used to block Java applets in the CBAC inspection rule named “rule44,” which
! is applied at interface Serial2/0:23.
access-list 5 permit any
! Create standard ACL 10 to specify the hosts using the authentication proxy. This ACL
! used in the authentication proxy rule named “PXY”, which is applied at interface
! Serial2/0:23.
access-list 10 permit any
! Create ACL 15 to block all traffic for the http server.
access-list 15 deny any
! Create extended ACL 102 to block all traffic inbound on interface Ethernet0/1
! except for traffic from the AAA server.
access-list 102 permit tcp host 192.168.150.20 eq tacacs 192.168.150.2
access-list 102 deny   tcp any any
access-list 102 deny   udp any any
access-list 102 permit ip any any
! Create extended ACL 105 to block all TCP and UDP traffic inbound on interface
! Serial2/0:23.
access-list 105 deny   tcp any any
access-list 105 deny   udp any any
access-list 105 permit ip any any
! Identify the IPSec specific traffic.
access-list 155 permit tcp host 192.168.150.100 host 192.168.50.13 eq www
access-list 155 permit tcp host 192.168.150.100 eq www host 192.168.50.13
dialer-list 1 protocol ip permit
! Define the AAA server host and encryption key.
tacacs-server host 192.168.126.14
tacacs-server key cisco
!
line con 0
 exec-timeout 0 0
! Define the AAA server host and encryption key.
 login authentication console_line
 transport input none
 line aux 0
 line vty 0 4
 password lab
!
!
 end
```

AAA サーバのユーザ プロファイル例

ここでは、AAA サーバでの認証プロキシのユーザ プロファイル エントリの例を示します。「proxyacl」エントリを使用して、ユーザのアクセス権限を定義します。ユーザが認証プロキシを使用してログインに成功すると、これらのエントリはファイアウォール ルータに転送されます。プロファイル内の各エントリにはサービスまたはアプリケーションの「permit」アクセスを指定する必要があります。各エントリの送信元アドレスは、「any」に設定します。アドレスは、プロファイルがファイアウォールにダウンロードされるときに認証ホストの IP アドレスに置換されます。すべての AAA ユーザの特権レベルは 15 に設定する必要があります。

ここでは、次の各手順について説明します。

- 「CiscoSecure ACS 2.3 for Windows NT」

- 「CiscoSecure ACS 2.3 for UNIX」
- 「TACACS+ Server」
- 「Livingston Radius Server」
- 「Ascend Radius Server」

CiscoSecure ACS 2.3 for Windows NT

ここでは、CiscoSecure ACS 2.3 for Windows NT 上で認証プロキシを設定する方法について説明します。CiscoSecure ACS の詳細については、該当する製品のマニュアルを参照してください。

次の設定例は、CiscoSecure ACS for Windows NT の TACACS+ サービス用の設定です。

ステップ 1 [Interface Configuration] アイコンをクリックし、[TACACS+ (Cisco)] をクリックします。

a. 下にスクロールして [New Services] を表示します。

b. 新しいサービス「auth-proxy」を [Service] フィールドに追加します。[Protocol] フィールドは空のままにします。

c. 新しいサービスに対して [User] チェックボックスと [Group] チェックボックスをオンにします。

d. 下にスクロールして [Advance Configuration Options] を表示し、[Per-user Advance TACACS+] 機能をオンにします。

e. [Submit] をクリックします。

ステップ 2 [Network Configuration] アイコンをクリックします。

a. [Network Access Servers] の [Add Entry] アイコンをクリックし、[Network Access Server Hostname]、IP アドレス、キー（ルータで設定したキー）のフィールドに情報を入力します。

b. [Authenticate Using] オプションに対して [TACACS+ (Cisco)] を選択します。

c. [Submit + Restart] アイコンをクリックします。

ステップ 3 [Group Setup] アイコンをクリックします。

a. ドロップダウン メニューからユーザ グループを選択します。

b. [Users in Group] チェックボックスをオンにします。

c. ユーザ リストからユーザを選択します。

d. [User Setup] リストで下にスクロールし、[TACACS+ Settings] を表示して、「auth-proxy」チェックボックスをオンにします。

e. [Custom Attributes] チェックボックスをオンにします。

f. プロファイル エントリを追加し（エントリは単一引用符または二重引用符で囲みません）、特権レベルを 15 に設定します。

```
priv-lvl=15
proxyacl#1=permit tcp any any eq 26
proxyacl#2=permit icmp any host 60.0.0.2
proxyacl#3=permit tcp any any eq ftp
proxyacl#4=permit tcp any any eq ftp-data
proxyacl#5=permit tcp any any eq smtp
proxyacl#6=permit tcp any any eq telnet
```

g. [Submit] をクリックします。

ステップ 4 [User Setup] アイコンをクリックします。

a. [List All Users] をクリックします。

b. ユーザ名を追加します。

c. 下にスクロールして [User Setup Password Authentication] を表示します。

d. [Password Authentication] ドロップダウン メニューから [Select SDI SecurID Token Card] を選択します。

e. 以前設定したユーザ グループ 1 を選択します。

f. [Submit] をクリックします。

ステップ 5 再度 [Group Setup] アイコンをクリックします。

a. ユーザ グループ 1 を選択します。

b. [Users in Group] をクリックします。

c. [Edit Settings] をクリックします。

d. [Submit + Restart] アイコンをクリックして、最新の設定を更新し、AAA サーバに送信します。

CiscoSecure ACS 2.3 for UNIX

ここでは、CiscoSecure ACS 2.3 for UNIX 上で認証プロキシを設定する方法について説明します。CiscoSecure ACS の詳細については、該当する製品のマニュアルを参照してください。

Administrator プログラムを使用して CiscoSecure ACS を管理するには、Java と JavaScript をサポートする Web ブラウザが必要です。ブラウザ アプリケーションで Java をイネーブルにする必要があります。Java ベースの CiscoSecure Administrator の詳細設定プログラムは、CiscoSecure ACS Administrator のどの Web ページからでも起動できます。

次に、CiscoSecure ACS 2.3 for UNIX の TACACS+ サービスの設定手順の例を示します。

ステップ 1 CiscoSecure ACS Web インターフェイスの CiscoSecure ACS Web メニュー バーで、[Advanced] をクリックし、再度 [Advanced] をクリックします。

Java ベースの CiscoSecure Administrator 詳細設定プログラムが表示されます。ロードに数分かかることがあります。

ステップ 2 CiscoSecure Administrator 詳細設定プログラムで、タブ化された [Members] ページの [Navigator] ペインで [Browse] をオフにします。

これにより [Create New Profile] アイコンが表示されます。

ステップ 3 [Navigator] ペインで、次のいずれかを実行します。

- ユーザを追加するグループを探してクリックします。
- ユーザをグループに追加しない場合は、[Root] フォルダ アイコンをクリックします。

ステップ 4 [Create Profile] をクリックして、[New Profile] ダイアログ ボックスを表示します。

ステップ 5 [Group] チェックボックスがオフになっていることを確認します。

ステップ 6 作成するユーザの名前を入力し、[OK] をクリックします。新しいユーザがツリーに表示されます。

ステップ 7 タブ化された [Members] ページの [Navigator] ペインに表示されるツリー内の、グループ プロファイルまたはユーザ プロファイルのアイコンをクリックします。

ステップ 8 必要に応じて、[Profile] ペインで [Profile] アイコンをクリックしてペインを展開します。

選択したプロファイルまたはサービスに該当するアトリビュートが含まれるリストまたはダイアログ ボックスが、画面右下のウィンドウに表示されます。このウィンドウの情報は、[Profile] ペインで選択した内容に応じて変化します。

ステップ 9 [Service-String] をクリックします。

ステップ 10 [string] をクリックし、テキスト フィールドに「**auth-proxy**」と入力し、[Apply] をクリックします。

ステップ 11 [Option] メニューを選択します。

ステップ 12 [Option] メニューで、[Default Attributes] をクリックします。

ステップ 13 アトリビュートを [Deny] から [Permit] に変更します。

ステップ 14 [Apply] をクリックします。

ステップ 15 [Option] メニューで、[Attribute] をクリックし、テキスト フィールドに特権レベルを入力します。

```
priv-lvl=15
```

ステップ 16 [Option] メニューで、[Attribute] をクリックし、テキスト フィールドに [proxyacl] エントリを入力します。

```
proxyacl#1=”permit tcp any any eq 26”
```

追加する各サービスまたはプロトコルに対してこのステップを繰り返します。

```
proxyacl#2=”permit icmp any host 60.0.0.2”
proxyacl#3=”permit tcp any any eq ftp”
proxyacl#4=”permit tcp any any eq ftp-data”
proxyacl#5=”permit tcp any any eq smtp”
proxyacl#6=”permit tcp any any eq telnet”
```

ステップ 17 すべての変更を終えたら、[Submit] をクリックします。

TACACS+ Server

```
default authorization = permit
key = cisco
user = Brian {
login = cleartext cisco
service = auth-proxy
 {
  priv-lvl=15
  proxyacl#1="permit tcp any any eq 26"
  proxyacl#2="permit icmp any host 60.0.0.2"
  proxyacl#3="permit tcp any any eq ftp"
  proxyacl#4="permit tcp any any eq ftp-data"
  proxyacl#5="permit tcp any any eq smtp"
  proxyacl#6="permit tcp any any eq telnet"
 }
}
```

Livingston Radius Server

```
Bob Password = "cisco" User-Service-Type=Outbound-User
cisco-avpair = "auth-proxy:priv-lvl=15",
cisco-avpair = "auth-proxy:proxyacl#1=permit tcp any any eq 26",
cisco-avpair = "auth-proxy:proxyacl#2=permit icmp any host 60.0.0.2",
cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq ftp",
cisco-avpair = "auth-proxy:proxyacl#4=permit tcp any any eq ftp-data",
cisco-avpair = "auth-proxy:proxyacl#5=permit tcp any any eq smtp",
cisco-avpair = "auth-proxy:proxyacl#6=permit tcp any any eq telnet"
```

Ascend Radius Server

```
Alice Password = "cisco" User-Service = Dialout-Framed-User
cisco-avpair = "auth-proxy:priv-lvl=15",
cisco-avpair = "auth-proxy:proxyacl#1=permit tcp any any eq 26",
cisco-avpair = "auth-proxy:proxyacl#2=permit icmp any host 60.0.0.2",
cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq ftp",
cisco-avpair = "auth-proxy:proxyacl#4=permit tcp any any eq ftp-data",
cisco-avpair = "auth-proxy:proxyacl#5=permit tcp any any eq smtp",
cisco-avpair = "auth-proxy:proxyacl#6=permit tcp any any eq telnet"
```

その他の参考資料

ここでは、認証プロキシ機能に関する関連資料について説明します。

関連資料

内容	参照先
認可	「Configuring Authorization」
認証	「Configuring Authentication」
アカウンティング	「Configuring Accounting」
RADIUS	「Configuring RADIUS」
TACACS+	「Configuring TACACS+」

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によってサポートされる新しい RFC や変更された RFC はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

認証プロキシの機能情報

表 3 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 3 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 3　認証を設定するための機能情報

機能名	リリース	機能情報
認証プロキシ	12.1(5)T	Cisco IOS Firewall 認証プロキシ機能では、動的かつユーザごとの認証と認可、業界標準の TACACS+ および RADIUS 認証プロトコルを使用したユーザの認証が可能です。ユーザによる接続の認証と認可により、ネットワーク攻撃に対するより強力な保護が可能になります。 この機能は、12.1(5)T で Cisco IOS に導入されました。

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

802.1X 認証サービス

IEEE 802.1x-Flexible Authentication

IEEE 802.1x-Flexible Authentication 機能には、ポートに認証方式を割り当て、認証の試行が失敗したときに方式を実行する順序を指定する手段が用意されています。この機能を使用すると、各ポートでどの認証方式を使用するかを制御できます。また、そのポートの方式についてフェールオーバー順も制御できます。

機能情報の確認

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「IEEE 802.1.x-Flexible Authentication の機能情報」（P.10）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

目次

IEEE 802.1x-Flexible Authentication の前提条件

IEEE 802.1x：ポートベースのネットワーク アクセス コントロール

ポートベースのネットワーク アクセス コントロールの概念とシスコのプラットフォーム上のポートベースのネットワーク アクセス コントロールの設定方法を理解しておく必要があります。詳細については、シスコのプラットフォームのマニュアル、および『*Cisco IOS Security Configuration Guide: Securing User Services*』を参照してください。

RADIUS および ACL

RADIUS プロトコルの概念と Access Control List（ACL; アクセス コントロール リスト）の作成および適用方法を理解しておく必要があります。詳細については、シスコのプラットフォームのマニュアル、および『*Cisco IOS Security Configuration Guide: Securing User Services*』を参照してください。

スイッチが RADIUS 設定されていて、Cisco Secure Access Control Server（ACS; アクセス コントロール サーバ）に接続されている必要があります。詳細については、『*Configuration Guide for CISCO Secure ACS*』を参照してください。

IEEE 802.1x-Flexible Authentication の制約事項

Cisco IOS Release 12.2(33)SXI では、Web 認証方式から 802.1x または MAB 認証方式にフェールオーバーすることはできません。そのため、認証順を設定するときは、Web 認証の後にその他の認証方式を指定しないでください。

IEEE 802.1x-Flexible Authentication に関する情報

IEEE 802.1x-Flexible Authentication 認証をセットアップするには、次の概念を理解しておく必要があります。

- 「Cisco IOS Auth Manager の概要」（P.2）
- 「認証方式」（P.3）
- 「ホスト モード認証」（P.3）
- 「認証順序と認証の優先順位」（P.3）

Cisco IOS Auth Manager の概要

指定されたネットワークに接続するデバイスの機能は異なっている可能性があるため、ネットワークはさまざまな認証方式および認証ポリシーをサポートする必要があります。Cisco IOS Auth Manager は、認証方法に関係なく、ネットワーク認証要求を処理し、認証ポリシーを強制します。Auth Manager は、すべてのポートベースのネットワーク接続試行、認証、認可、および接続解除に対する運用データを維持することで、セッション マネージャとして機能します。

Auth Manager セッションには、次のような状態が考えられます。

- Idle：idle 状態では、認証セッションは初期化されていますが、実行されている方式はありません。これは中間の状態です。
- Running：現在、方式が実行されています。これは中間の状態です。
- Authc Success：認証方式の実行に成功しました。これは中間の状態です。

- Authc Failed：認証方式が失敗しました。これは中間の状態です。
- Authz Success：このセッションに対するすべての機能の適用に成功しました。これは最終的な状態です。
- Authz Failed：このセッションに対して、少なくとも 1 つの機能の適用に失敗しました。これは最終的な状態です。
- No methods：このセッションに結果を提供する方式がありません。これは最終的な状態です。

認証方式

IEEE 802.1x-Flexible Authentication 機能は、次の 3 つの認証方式をサポートしています。

- **dot1x**：IEEE 802.1x 認証はレイヤ 2 の認証方式です。
- **mab**：MAC 認証バイパスはレイヤ 2 の認証方式です。
- **webauth**：Web 認証はレイヤ 3 の認証方式です。

ホスト モード認証

IEEE 802.1x-Flexible Authentication 機能は、次の 2 つの新しいホスト モードをサポートしています。

- **multi-auth :** マルチ認証では、音声 VLAN に 1 つの認証、データ VLAN に複数の認証を使用できます。
- **multi-domain**：マルチドメイン認証では、音声 VLAN に 1 つ、データ VLAN に 1 ついう 2 つの認証を使用できます。

また、IEEE 802.1x-Flexible Authentication 機能は、シングルホスト認証とマルチホスト認証もサポートしています。

認証順序と認証の優先順位

IEEE 802.1x-Flexible Authentication 機能を使用すると、認証順序と認証の優先順位を指定できます。**authentication order** コマンドでは、デフォルトの認証の優先順位を設定します。**authentication priority** コマンドを使用すると、デフォルトの認証の優先順位よりも優先されます。たとえば、MAB、802.1x という認証順序を指定するとします。ただし、認可後に後続の 802.1x ハンドシェークを無視したくない場合があります。このような場合、802.1x 認証方式に MAB 方式よりも高い優先順位を与えます。

IEEE 802.1x-Flexible Authentication の設定方法

ここでは、次の作業について説明します。

- 「認証順序の設定」（P.4）
- 「認証の優先順位の設定」（P.6）

認証順序の設定

認証順序は個々のポートで設定し、各ポートがどの認証方式を使用するかを制御します。ここで説明する手順に従って認証順序を設定してください。

前提条件

IEEE 802.1x-Flexible Authentication 機能を使用するには、スイッチを Cisco Secure ACS に接続し、RADIUS Authentication, Authorization, and Accounting (AAA; 認証、認可、およびアカウンティング) を Web 認証用に設定しておく必要があります。また、必要に応じて、ACL ダウンロードを有効にします。

認証順序に 802.1x ポート認証方式を含める場合、スイッチで IEEE 802.1x 認証をイネーブルにする必要があります。

認証順序に Web 認証を含める場合、スイッチとインターフェイスで Web 認証を可能にするフォールバック プロファイルを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **dot1x system-auth-control**
4. **interface** *type slot/port*
5. **switchport**
6. **switchport mode access**
7. **switchport access vlan** *vlan-id*
8. **mab** [**eap**]
9. **authentication port-control** {**auto** | **force-authorized** | **fort unauthorized**}
10. **authentication fallback** *profile*
11. **authentication order** {**dot1x** [**mab** | **webauth**] [**webauth**] | **mab** [**dot1x** | **webauth**] [**webauth**] | **webauth**}
12. **dot1x pae authenticator**
13. **end**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	`enable`
	
	例 :
	`Switch> enable`
		特権 EXEC モードをイネーブルにします。
		• プロンプトが表示されたら、パスワードを入力します。

ステップ 2	`configure terminal`
	
	例 :
	`Switch# configure terminal`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**dot1x system-auth-control** **例：** `Switch(config)# dot1x system-auth-control`	（任意）スイッチで IEEE 802.1x 認証をグローバルにイネーブルにします。 認証順序に **dot1x** 認証方式を含める場合、IEEE 802.1x 認証をイネーブルにします。
ステップ 4	**interface type** *slot*/*port* **例：** `Switch(config)# interface FastEthernet2/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**switchport** **例：** `Switch(config-if)# switchport`	レイヤ 2 スイッチド モードでインターフェイスを配置します。
ステップ 6	**switchport mode access** **例：** `Switch(config-if)# switchport mode access`	非トランキング、非タグ付き、シングル VLAN レイヤ 2 インターフェイスを設定します。
ステップ 7	**switchport access vlan** *vlan-id* **例：** `Switch(config-if)# switchport access vlan 2`	ポートに VLAN を設定します。
ステップ 8	**mab** [**eap**] **例：** `Switch(config-if)# mab`	（任意）MAB をイネーブルにします。 認証順序に **mab** キーワード（ステップ 11）を含める場合、MAB をイネーブルにします。
ステップ 9	**authentication port-control** {**auto** | **force-authorized** | **fort unauthorized**} **例：** `Switch(config-if)# authentication port-control auto`	ポートの認証ステートを設定します。
ステップ 10	**authentication fallback** *profile* **例：** `Switch(config-if)# authentication fallback web-profile`	（任意）Web 認証をイネーブルにします。 認証順序に **webauth** キーワード（ステップ 11）を含める場合、Web 認証をイネーブルにします。
ステップ 11	**authentication order** {**dot1x** [**mab** | **webauth**] [**webauth**] | **mab** [**dot1x** | **webauth**] [**webauth**] | **webauth**} **例：** `Switch(config-if)# authentication order mab dot1x webauth`	認証順序を設定します。

	コマンドまたはアクション	目的

ステップ 12	`dot1x pae authenticator`
	
	例：
	`Switch(config)# dot1x pae authenticator`
		IEEE 802.1x オーセンティケータ向けのメッセージに対して、ポートが応答できるようにします。

ステップ 13	`end`
	
	例：
	`Switch(config-if)# end`
		グローバル コンフィギュレーション モードに戻ります。

トラブルシューティングのヒント

次のコマンドは、Flexible Authentication 機能のトラブルシューティングに役立ちます。

- **debug authentication**
- **show authentication registrations**
- **show authentication sessions**
- **show dot1x**
- **show mab**

認証の優先順位の設定

認証の優先順位は、個々のポートの方式についてフェールオーバー順を制御するために設定します。ここで説明する手順に従って認証の優先順位を設定してください。

前提条件

認証の優先順位を設定するには、「認証順序の設定」（P.4）の説明に従って認証順序を設定しておく必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **authentication priority** {**dot1x** [**mab** | **webauth**] [**webauth**] | **mab** [**dot1x** | **webauth**] [**webauth**] | **webauth**}
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Switch> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type slot/port* **例：** `Switch(config)# interface FastEthernet2/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**authentication priority** {**dot1x** [**mab** | **webauth**] [**webauth**] | **mab** [**dot1x** | **webauth**] [**webauth**] | **webauth**} **例：** `Switch(config-if)# authentication priotiry dot1x mab webauth`	認証の優先順位を設定します。
ステップ 5	**end** **例：** `Switch(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。

IEEE 802.1x-Flexible Authentication の設定例

ここでは、次の設定例について説明します。

「Flexible Authentication：例」（P.7）

Flexible Authentication：例

次の例では、マルチ認証ホスト モードでポートを設定します。認証順序は、802.11x が最初で、次に MAB、最後が Web 認証です。

```
enable
configure terminal
dot1x system-auth-control

aaa new-model
aaa authentication login default group radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa session-id common
ip http server

ip admission name webauth-rule proxy http
fallback profile webauth-profile
 ip access-group webauthlist in
```

```
 ip admission webauth-rule


interface GigabitEthernet2/1
 switchport
 switchport mode access
 switchport access vlan 125
 switchport voice vlan 127
 mab
 authentication port-control auto
 authentication fallback webauth-profile
 authentication host-mode multi-auth
 authentication order dot1x mab webauth
 dot1x pae authenticator
```

その他の参考資料

次の項で、IEEE 802.1.x-Flexible Authentication 機能に関する参考資料を紹介します。

関連資料

内容	参照先
認証コマンド	『*Cisco IOS Security Command Reference*』
Standalone MAB Support	Standalone MAB Support

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
• CISCO-AUTH-FRAMEWORK-MIB • CISCO-MAC-AUTH-BYPASS-MIB • CISCO-PAE-MIB • IEEE8021-PAE-MIB	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 3580	「*IEEE 802.1x Remote Authentication Dial In User Service (RADIUS)*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IEEE 802.1.x-Flexible Authentication の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、Cisco IOS、Catalyst OS、Cisco IOS XE ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　IEEE 802.1.x-Flexible Authentication の機能情報

機能名	リリース	機能情報
IEEE 802.1x-Flexible Authentication	12.2(33)SXI	この機能には、ポートに 1 つまたは複数の認証方式を設定し、各認証方式を試行する順序を指定する手段が用意されています。 導入または変更されたコマンド：**authentication fallback**、**authentication host-mode**、**authentication order**、**authentication port-control**、**authentication priority**、**authentication timer restart**、**debug authentication**、**mab**、**show authentication interface**、**show authentication registrations**、**show authentication sessions**、**show mab** 削除または廃止されたコマンド：**dot1x fallback**、**dot1x host-mode**、**dot1x port control**

ネットワーク アドミッション コントロール（NAC）

ネットワーク アドミッション コントロール

ネットワーク アドミッション コントロール機能は、増大するワームやウイルスがビジネスのネットワークに与える脅威や影響に対応します。この機能は、顧客がセキュリティの脅威を認識して防御し、適合するのに役立つ Cisco Self-Defending Network Initiative（自己防衛型ネットワーク構想）の一部です。

Cisco Network Admission Control（NAC; ネットワーク アドミッション コントロール）機能は、その初期段階で、エンドポイントがネットワークに接続しようとしたときに Cisco ルータがアクセス権限を制限できるようにします。このアクセスの決定は、現在のアンチウイルスの状態などのエンドポイント装置の情報に基づいて行うことができます。アンチウイルスの状態には、アンチウイルス ソフトウェアのバージョン、ウイルス定義、およびスキャン エンジンのバージョンなどの情報が含まれます。

ネットワーク アドミッション コントロール システムにより、非準拠デバイスのアクセスの拒否、検疫エリアへの配置、またはコンピューティング リソースへの制限付きアクセスの許可が可能になり、非セキュアなノードからネットワークに感染するのを防ぐことができます。

Cisco NAC プログラムの主要なコンポーネントは Cisco Trust Agent です。このコンポーネントはエンドポイント システムに常駐して、ネットワーク上の Cisco ルータと通信します。Cisco Trust Agent は、使用されているアンチウイルス ソフトウェアなどのセキュリティ状態の情報を収集し、この情報を Cisco ルータに送信します。次に、この情報は、Cisco Secure Access Control Server（ACS）にリレーされ、そこでアクセス コントロールが決定されます。ACS は、Cisco ルータに、エンドポイントに対し強制を実施するよう指示します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「ネットワーク アドミッション コントロールの機能情報」（P.29）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

ネットワーク アドミッション コントロールの前提条件

- Cisco IOS ルータでは、Cisco IOS ソフトウェア リリース 12.3(8)T 以降を実行する必要があります。
- エンドポイント装置（PC や ラップトップなど）には Cisco Trust Agent をインストールする必要があります。
- Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）には Cisco Secure ACS が必要です。
- Access Control List（ACL; アクセス コントロール リスト）および AAA の設定に関する豊富な知識と技術が必要です。

ネットワーク アドミッション コントロールの制約事項

- この機能は、Cisco IOS ファイアウォール フィーチャ セットのみで使用できます。

ネットワーク アドミッション コントロールの概要

ネットワーク アドミッション コントロール機能を設定する前に、次の概念を理解しておく必要があります。

ウイルスの感染とネットワークへの影響

ウイルスの感染は、ネットワークに対する重大なセキュリティ違反のうち、単独では最大の原因であり、経済的に多大な損失をもたらすことが少なくありません。ウイルス感染源は非セキュアなエンドポイント（PC、ラップトップ、およびサーバなど）にあります。エンドポイントにアンチウイルス ソフトウェアがインストールされている場合でも、そのソフトウェアがディセーブルになっている場合がよくあります。ソフトウェアがイネーブルになっていても、エンドポイントに最新のウイルス定義やスキャン エンジンがない場合もあります。セキュリティのリスクを拡大するのは、アンチウイルス ソフトウェアをインストールしていない装置です。現在のアンチウイルス ベンダーは、アンチウイルス ソフトウェアを簡単にディセーブルにできないようにしていますが、古いウイルス定義やスキャン エンジンのリスクには対応していません。

ネットワーク アドミッション コントロールのしくみ

通常、エンドポイント システムまたはクライアントは、PC、ラップトップ、ワークステーション、およびサーバなどのネットワーク上のホストになっています。エンドポイント システムは潜在的なウイルス感染源であるため、ネットワーク アクセスを許可する前に、これらのアンチウイルスの状態を検証する必要があります。エンドポイントがアップストリームのシスコ ネットワーク アクセス装置（通常は Cisco IOS ルータ）を介してネットワークに IP 接続しようとすると、ルータはエンドポイントにアンチウイルスの状態を要求します。エンドポイント システムは Cisco Trust Agent と呼ばれるクライアントを実行して、エンド デバイスからアンチウイルスの状態に関する情報を収集し、その情報をシスコのネットワーク アクセス装置に転送します。次に、この情報は Cisco Secure ACS に送信されます。ACS では、エンドポイントのアンチウイルスの状態を検証し、アクセス コントロールを決定して、シスコ ネットワーク アクセス装置に返します。ネットワーク デバイスでは、エンド デバイスの許可、拒否、または検疫が行われます。Cisco Secure ACS では、エンドポイントのアンチウイルスの状態を評価する際に、バックエンドのアンチウイルス ベンダー固有のサーバを順に使用することもできます。

図 1 に、Cisco Network Admission Control の動作を示します。

図 1　Cisco IOS Network Admission Control システム

ネットワーク アクセス装置

通常、Network Access Device（NAD; ネットワーク アクセス装置）は、Cisco IOS ルータ（レイヤ 3 Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）アクセス ポイント）であり、インターネットやリモートの企業ネットワークなどの外部ネットワークに接続しています。Cisco Network Admission Control 機能にはインターセプト ACL がある場合があります。インターセプト ACL は、ネットワーク アドミッション用に代行受信される接続を決定します。アクセス リストと一致するエンドポイントからの接続はネットワーク アドミッション コントロールによって代行受信され、ネットワーク アクセスを許可する前に、レイヤ 3 アソシエーションに対してアンチウイルスの状態が要求されます。

Cisco Trust Agent

Cisco Trust Agent は、エンドポイント システムで実行される専門のソフトウェアです。Cisco Trust Agent は、エンドポイント システムのアンチウイルスの状態に関するルータからの要求に応答します。エンドポイント システムが Cisco Trust Agent を実行していない場合、ネットワーク アクセス装置（ルータ）はそのエンドポイント システムを「クライアントレス」として分類します。ネットワーク アクセス装置は EOU clientless ユーザ名と EOU clientless パスワードを使用します。これは、Cisco Secure ACS での検証のためにエンドポイント システムのクレデンシャルとしてネットワーク アクセス装置に設定されます。このユーザ名に関連付けられるポリシー アトリビュートは、エンドポイント システムに対して実行されます。

Cisco Secure ACS

Cisco Secure ACS は、業界標準の RADIUS 認証プロトコルを使用して、ネットワーク アドミッション コントロールに認証、認可、およびアカウンティング サービスを提供します。Cisco Secure ACS は、エンドポイント システムのアンチウイルスのクレデンシャルに基づいて、ネットワーク アクセス装置にアクセス コントロールの決定を返します。

RADIUS の cisco_av_pair Vendor-Specific Attributes（VSA; ベンダー固有アトリビュート）を使用して、Cisco Secure ACS に次の Attribute-Value ペア（AV ペア）を設定できます。AV ペアは、他のアクセス コントロール アトリビュートと一緒にネットワーク アクセス装置に送信されます。

- url-redirect : AAA クライアントが HTTP 要求を代行受信し、それを新しい URL にリダイレクトできるようにします。このリダイレクションは、ポスチャ検証の結果、ネットワーク アクセス コントロールのエンドポイントが修復 Web サーバで利用可能なアップデートまたはパッチが必要となる場合に特に便利です。たとえば、新しいウイルスの Directory Administration Tool（DAT）ファイルまたはオペレーティング システムのパッチをダウンロードして適用する場合に、修復 Web サーバにユーザをリダイレクトすることができます（次の例を参照してください）。

  ```
  url-redirect=http://10.1.1.1
  ```

- posture-token : Cisco Secure ACS が、ポスチャ確認で取得した System Posture Token（SPT）のテキスト バージョンを送信できるようにします。SPT は常に数値形式で送信されます。posture-token AV ペアを使用すると、AAA クライアントでポスチャ検証要求の結果を簡単に表示できます（次の例を参照してください）。

  ```
  posture-token=Healthy
  ```

  有効な SPT は次のとおりです（最善のものから順に示します）。

  - Healthy
  - Checkup

  - Quarantine
  - Infected
  - Unknown

- status-query-timeout：AAA クライアントの status-query のデフォルト値をユーザが指定した値（秒）で上書きします（次の例を参照してください）。

  ```
  status-query-timeout=150
  ```

Cisco IOS ソフトウェアがサポートする AV ペアの詳細については、ご使用の AAA クライアントに実装されている Cisco IOS ソフトウェア リリースのマニュアルを参照してください。

修復

ネットワーク アドミッション コントロールは、任意の HTTP 要求をエンドポイント装置から指定されたリダイレクト アドレスにリダイレクトする HTTP リダイレクションをサポートします。このサポート メカニズムにより、すべての HTTP 要求は発信元から指定された Web ページ（URL）にリダイレクトされ、そこで最新のアンチウイルス ファイルをダウンロードできます。HTTP リダイレクションが機能するには、ACS で「url-redirect」VSA の値を設定し、それに応じてエンドポイント システムのアクセスを許可するダウンロード可能な ACL のアクセス コントロール エントリをリダイレクト URL アドレスに関連付ける必要があります。url-redirect VSA の値が設定され、アクセス コントロール エントリが関連付けられたら、IP アドミッション インターセプト ACL に一致する HTTP 要求は、指定されたリダイレクト URL アドレスにリダイレクトされます。

ネットワーク アドミッション コントロールと認証プロキシ

ネットワーク アドミッション コントロールと認証プロキシを、特定のインターフェイスの同じホストセットに設定することができます。それぞれのケースで、IP アドミッションの EAPoUDP と認証プロキシのインターセプト ACL が同じである必要があります。プロキシ認証を使用する IP アドミッション プロキシを最初に設定し、その後で IP アドミッション コントロールを設定する必要があります。

NAC MIB

NAC MIB 機能は、NAC サブシステムに Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）のサポートを追加します。管理者は、SNMP コマンド（get および set 操作）を使用して、NAD の NAC セッションをモニタおよび制御することができます。

SNMP の get および set 操作の詳細については、「その他の参考資料」の「関連資料」を参照してください。

SNMP Get 操作および Set 操作と Cisco CLI の相互関係

NAC MIB（CISCO-NAC-NAD-MIB.my）のオブジェクト テーブルにあるほとんどのオブジェクトは、NAD のセットアップに適用できるさまざまな EAPoUDP およびセッション パラメータを表しています。SNMP のさまざまな get 操作および set 操作を実行することによって、これらのプロパティを表示したり変更できます。また、対応する Command-Line Interface（CLI; コマンドライン インターフェイス）をルータに設定することで、多くのテーブル オブジェクトの値を表示したり変更することもできます。たとえば、SNMP get 操作を cnnEOUGlobalObjectsGroup テーブルで実行したり、**show eou** コ

マンドをルータに設定したりすることができます。SNMP get 操作で取得されるパラメータ情報は、**show eou** コマンドの出力と同じです。同様に、SNMP get 操作を cnnEouIfConfigTable で実行すると、**show eou** コマンドの出力にも表示可能なインターフェイス固有のパラメータが提供されます。

SNMP set 操作は、対応する CLI コマンドがあるテーブル オブジェクトに使用できます。これを使用してテーブル オブジェクトの値を変更できます。たとえば、cnnEouHostValidateAction MIB テーブルの cnnEouHostValidateAction オブジェクトの値の範囲を 2 に変更するには、SNMP set 操作を実行するか、ルータに **eou initialize all** コマンドを設定します。

NAC MIB の出力例については、「ネットワーク アドミッション コントロールの設定例」の「NAC MIB の出力：例」を参照してください。

セッションの初期化と再検証

NAC を使用すると、管理者は次の CLI コマンドを使用してセッションの初期化と再検証を実行できます。

- **eou initialize all**
- **eou initialize authentication clientless**
- **eou initialize authentication eap**
- **eou initialize authentication static**
- **eou initialize ip** {*ip-address*}
- **eou initialize mac** {*mac-address*}
- **eou initialize posturetoken** {*string*}
- **eou revalidate all**
- **eou revalidate authentication clientless**
- **eou revalidate authentication eap**
- **eou revalidate authentication static**
- **eou revalidate ip** {*ip-address*}
- **eou revalidate mac** {*mac-address*}
- **eou revalidate posturetoken** {*string*}

また、cnnEouHostValidateAction テーブルのオブジェクトに SNMP set 操作を実行することで、初期化と再検証のアクションを実行することもできます。セッションの初期化と再検証の詳細については、「cnnEouHostValidateAction テーブル オブジェクトに関連する CLI コマンド」を参照してください。

cnnEouHostValidateAction テーブル オブジェクトに対して実行可能な変更に関連する CLI コマンドの例については、「ネットワーク アドミッション コントロールの設定例」の「NAC MIB の出力：例」を参照してください。

Session-Specific 情報

NAC MIB では、cnnEouHostQueryTable と cnnEouHostResultTable を使用して session-specific の詳細を表示する方法を用意しています。クエリーを作成するには、cnnEouHostQueryTable を使用します。クエリーは、**show eou ip** {*ip-address*} コマンドと同じ形式です（つまり、IP アドレスは **show eou ip** コマンドの場合と同様（例：10.1.1.1）に表示されます）。管理者は、cnnEouHostQueryTable のオブジェクトに対して SNMP set 操作を使用して、クエリーを作成する必要があります。クエリーの結果は cnnEouHostResultTable の行として保存されます。session-specific の詳細の表示については、「MIB クエリーの結果の表示」を参照してください。

show コマンドを使用した MIB オブジェクト情報の表示

CLI コマンド **show eou**、**show eou all**、**show eou authentication**、**show eou initialize**、**show eou ip**、**show eou mac**、**show eou posturetoken**、**show eou revalidate**、および **show ip device tracking all** を使用すると、SNMP get 操作を使用した場合の CISCO-NAC-NAD-MIB テーブルと同じ出力情報が得られます。

MIB オブジェクト テーブルでも表示可能な **show** コマンドの出力情報の例については、「ネットワーク アドミッション コントロールの設定例」の「NAC MIB の出力：例」を参照してください。

ネットワーク アドミッション コントロールの設定方法

ここでは、次の各手順について説明します。

ACL およびアドミッション コントロールの設定

ネットワーク アドミッション コントロールは、すべてのインターフェイスの着信方向に適用されます。ネットワーク アドミッション コントロールをインターフェイスの着信に適用すると、ネットワーク アドミッション コントロールはルータを介してインターセプト エンド システムの最初の IP 接続を代行受信します。

図 1 に、LAN インターフェイスで適用される IP アドミッション コントロールを示します。ルータを介して最初の IP 接続が行われるときに、すべてのネットワーク装置でアンチウイルスの状態を検証する必要があります。それまでは、エンドポイント システムからのすべてのトラフィック（EAPoUDP および Cisco Secure ACS のトラフィックを除く）はインターフェイスでブロックされます。

次に、エンドポイント システムには、EAPoUDP アソシエーションのアンチウイルスの状態が要求されます。Cisco Secure ACS によって評価されたときに、エンドポイント システムがネットワーク アドミッション コントロール ポリシーに準拠していれば、エンドポイント システムはネットワークにアクセスすることができます。エンドポイント システムが準拠していなかった場合、その装置はアクセスを拒否されるか、検疫されます。

インターセプト ACL を設定するには、次の手順の詳細を実行します。

この設定では、インターセプト ACL は「101」として定義され、インターセプト ACL は IP アドミッション コントロール ルール「greentree」に関連付けられます。192.50.0.0 のネットワークを宛先とするすべての IP トラフィックが検証の対象となります。また、ステップ 5 以降では、インターセプト ACL はネットワーク アドミッション コントロールに関連付けられたインターフェイスに対する着信に適用されます。通常、この ACL は、エンドポイント システムが検証されるまでエンドポイント システムへのアクセスをブロックします。この ACL はデフォルト アクセス リストと呼ばれます。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**permit** | **deny**} *protocol source destination*
4. **ip admission name** *admission-name* [**eapoudp** | **proxy** {**ftp** | **http** | **telnet**}] [**list** {*acl* | *acl-name*}]
5. **interface** *type slot/port*
6. **ip address** *ip-address mask*
7. **ip admission** *admission-name*
8. **exit**
9. **access-list** *access-list-number* {**permit** | **deny**} *protocol source destination*
10. **ip access-group** {*access-list-number* | *access-list-name*} **in**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list** *access-list-number* {**permit** | **deny**} *protocol source destination* 例： `Router (config)# access-list 101 permit ip any 192.50.0.0 0.0.0.255`	番号付きのアクセス リストを定義します。

	コマンドまたはアクション	目的
ステップ 4	**ip admission name** *admission-name* [**eapoudp** | **proxy** {**ftp** | **http** | **telnet**}] [**list** {*acl* | *acl-name*}] **例：** `Router (config)# ip admission name greentree eapoudp list 101`	IP ネットワーク アドミッション コントロール ルールを作成します。このルールは、アドミッション コントロールを適用する方法を定義します。次のルールがあります。 • **eapoudp**：EAPoUDP を使用して IP ネットワーク アドミッション コントロールを指定します。 • **proxy ftp**：認証プロキシを起動する FTP を指定します。 • **proxy http**：認証プロキシを起動する HTTP を指定します。 • **proxy telnet**：認証プロキシを起動する Telnet を指定します。 名前付きのルールを ACL と関連付けて、アドミッション コントロール機能を使用するホストを制御できます。標準のアクセス リストが定義されていない場合、設定されたインターフェイスで接続開始パケットを受信するすべてのホストからの IP トラフィックを、名前付きのアドミッション ルールが代行受信します。 list オプションを使用すると、標準、拡張（1 ～ 199）、または名前付きのアクセス リストを名前付きのアドミッション コントロール ルールに適用できます。アクセス リストにあるホストによって開始された IP 接続は、アドミッション コントロール機能によって代行受信されます。
ステップ 5	**interface** *type slot/port* **例：** `Router (config)# interface ethernet 2/1`	インターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ip address** *ip-address mask* **例：** `Router (config-if)# ip address 192.0.0.1 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 7	**ip admission** *admission-name* **例：** `Router (config-if)# ip admission greentree`	名前付きのアドミッション コントロール ルールをインターフェイスに適用します。
ステップ 8	**exit** **例：** `Router (config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的

ステップ 9	**access-list** *access-list-number* {**permit** | **deny**} *protocol source destination*
	
	例：
	`Router (config)# access-list 105 permit udp any any`
	
	または
	
	`Router (config)# access-list 105 permit ip host 192.168.0.2 any`
	
	または
	
	`Router (config)# access-list 105 deny ip any any`
		番号付きのアクセス リストを定義します。
		
		（注） 「コマンドまたはアクション」の最初の 2 つの例では、ACL 「105」が UDP および 192.168.0.2（Cisco Secure ACS）へのアクセスを除くすべての IP トラフィックを拒否します。
		
		（注） 「コマンドまたはアクション」の 3 番めの例では、ACL「105」はネットワーク アドミッション コントロールに設定されたインターフェイスに適用され、EAPoUDP トラフィックおよび Cisco Secure ACS へのアクセス（この例では 192.168.0.2）を除くエンドポイント システムへのアクセスは、アンチウイルスの状態が検証されるまでブロックされます。この ACL（「105」）は「インターフェイス ACL」と呼ばれます。

ステップ 10	**ip access-group** {*access-list-number* | *access-list-name*} **in** **例：** `Router (config)# ip access-group 105 in`	インターフェイスへのアクセスを制御します。

グローバルな EAPoUDP の値の設定

グローバルな EAPoUDP の値を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **eou {allow | clientless | default | initialize | logging | max-retry | port | rate-limit | revalidate | timeout}**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**eou** {**allow** | **clientless** | **default** | **initialize** | **logging** | **max-retry** | **port** | **rate-limit** | **revalidate** | **timeout**} 例： Router (config)# eou initialize	EAPoUDP の値を指定します。 • **eou** コマンドで使用可能なキーワードと引数の詳細については、次のコマンドを参照してください。 – **eou allow** – **eou clientless** – **eou default** – **eou initialize** – **eou logging** – **eou max-retry** – **eou port** – **eou rate-limit** – **eou revalidate** – **eou timeout**

インターフェイス固有の EAPoUDP アソシエーションの設定

ネットワーク アドミッション コントロールに関連付けられた特定のインターフェイスに変更またはカスタマイズ可能な EAPoUDP アソシエーションを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot*/*port*
4. **eou** [**default** | **max-retry** | **revalidate** | **timeout**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type slot*/*port* 例： `Router (config)# interface ethernet 2/1`	インターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**eou** [**default** | **max-retry** | **revalidate** | **timeout**] 例： `Router (config-if)# eou revalidate`	特定のインターフェイスの EAPoUDP アソシエーションをイネーブルにします。 • **eou** コマンドで使用可能なキーワードと引数の詳細については、次のコマンドを参照してください。 – **eou default** – **eou max-retry** – **eou revalidate** – **eou timeout**

EAPoUDP の AAA の設定

EAPoUDP の AAA を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication eou default enable group radius**
5. **aaa authorization network default group radius**
6. **radius-server host** {*hostname* | *ip-address*}
7. **radius-server key** {**0** *string* | **7** *string* | *string*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： Router (config)# aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
ステップ 4	**aaa authentication eou default enable group radius** 例： Router (config)# aaa authentication eou default enable group radius	EAPoUDP アソシエーションの認証リストを設定します。
ステップ 5	**aaa authorization network default group radius** 例： Router (config)# aaa authorization network default group radius	認証にすべての RADIUS サーバのリストを使用します。
ステップ 6	**radius-server host** {*hostname* | *ip-address*} 例： Router (config)# radius-server host 192.0.0.40	RADIUS サーバ ホストを指定します。
ステップ 7	**radius-server key** {**0** *string* | **7** *string* | *string*} 例： Router (config)# radius-server key cisco	ルータと RADIUS デーモンとの間におけるすべての RADIUS 通信用の認証および暗号化キーを設置得します。

アイデンティティ プロファイルとポリシーの設定

アイデンティティとは、ローカル プロファイルとポリシーの設定の指定に使用される共通のインフラストラクチャです。アイデンティティ プロファイルを使用すると、IP アドレス、MAC アドレス、またはデバイス タイプに基づいて、個々のデバイスをスタティックに認可または検証できます。スタティックに認証されたそれぞれのデバイスを、ネットワーク アクセス コントロール アトリビュートを指定したローカル ポリシーと関連付けることができます。**identity profile** コマンドを使用してホストを「例外リスト」に追加し、**identity policy** コマンドを使用して対応するポリシーをそのホストに関連付けます。

クライアントがアイデンティティに含まれる（つまり、クライアントが例外リストに記載されている）場合、そのクライアントのステータスはアイデンティティの設定に基づいて設定されます。クライアントではポスチャ検証処理を実行する必要はありません。また、関連するアイデンティティ ポリシーがそのクライアントに適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **identity profile eapoudp**
4. **device** {**authorize** {**ip address** *ip-address* {**policy** *policy-name*} | **mac-address** *mac-address* | **type** {**cisco** | **ip** | **phone**}} | **not-authorize**}
5. **exit**
6. **identity policy** *policy-name* [**access-group** *group-name* | **description** *line-of-description* | **redirect** *url* | **template** [**virtual-template** *interface-name*]]
7. **access-group** *group-name*
8. **exit**
9. **exit**
10. **ip access-list extended** *access-list-name*
11. {**permit** | **deny**} *source source-wildcard destination destination-wildcard*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**identity profile eapoudp** 例： `Router (config)# identity profile eapoudp`	アイデンティティ プロファイルを作成し、アイデンティティ プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**device** {**authorize** {**ip address** *ip-address* {**policy** *policy-name*} | **mac-address** *mac-address* | **type** {**cisco** | **ip** | **phone**}} | **not-authorize**} 例： `Router (config-identity-prof)# device authorize ip address 10.10.142.25 policy policyname1`	IP デバイス をスタティックに認可し、そのデバイスに関連するポリシーを適用します。
ステップ 5	**exit** 例： `Router (config-identity-prof)# exit`	アイデンティティ プロファイル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 6	**identity policy** *policy-name* [**access-group** *group-name* | **description** *line-of-description* | **redirect** *url* | **template** [**virtual-template** *interface-name*]] **例：** `Router (config-identity-prof)# identity policy policyname1`	アイデンティティ ポリシーを作成し、アイデンティティ ポリシー コンフィギュレーション モードを開始します。
ステップ 7	**access-group** *group-name* **例：** `Router (config-identity-policy)# access-group exempt-acl`	アイデンティティ ポリシーのネットワーク アクセス アトリビュートを定義します。
ステップ 8	**exit** **例：** `Router (config-identity-policy)# exit`	アイデンティティ ポリシー コンフィギュレーション モードを終了します。
ステップ 9	**exit** **例：** `Router (config-identity-prof)# exit`	アイデンティティ プロファイル コンフィギュレーション モードを終了します。
ステップ 10	**ip access-list extended** *access-list-name* **例：** `Router (config)# ip access-list extended exempt-acl`	スタティックに認証されたデバイスのアクセス コントロールを定義します（また、ネットワーク アクセス コントロール コンフィギュレーション モードを開始します）。
ステップ 11	{**permit** | **deny**} *source source-wildcard destination destination-wildcard* **例：** `Router (config-ext-nacl)# permit ip any 192.50.0.0. 0.0.0.255`	パケットが名前付きの IP アクセス リストを渡すことができる条件を設定します。

インターフェイスに関連付けられた EAPoUDP セッションのクリア

特定のインターフェイスに関連付けられた EAPoUDP セッション、または NAD の EAPoUDP セッションをクリアするには、次の手順を実行します。

手順の概要

1. **enable**
2. **clear eou all**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**clear eou all** 例： Router# clear eou all	NAD の EAPoUDP セッションをすべてクリアします。

ネットワーク アドミッション コントロールの確認

EAP および EAPoUDP のメッセージまたはセッションを確認するには、次の手順を実行します。**show** コマンドは、他の **show** コマンドには依存せず、どんな順番でも使用できます。

手順の概要

1. **enable**
2. **show eou all**
3. **show ip admission eapoudp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show eou all** 例： Router# show eou all	ネットワーク アクセス装置の EAPoUDP セッションに関する情報を表示します。
ステップ 3	**show ip admission eapoudp** 例： Router# show ip admission eapoudp	ネットワーク アドミッション コントロールの設定、またはネットワーク アドミッションのキャッシュ エントリを表示します。

ネットワーク アドミッション コントロールのトラブルシューティング

次のコマンドを使用して、EAP および EAPoUDP のメッセージまたはセッションに関する情報を表示できます。**debug** コマンドは、他の **debug** コマンドには依存せず、どんな順番でも使用できます。

手順の概要

1. **enable**
2. **debug eap** {**all** | **errors** | **packets** | **sm**}

3. **debug eou {all | eap | errors | packets | sm}**
4. **debug ip admission eapoudp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**debug eap {all | errors | packets | sm}** **例：** Router# debug eap all	EAP メッセージに関する情報を表示します。
ステップ 3	**debug eou {all | eap | errors | packets | sm}** **例：** Router# debug eou all	EAPoUDP メッセージに関する情報を表示します。
ステップ 4	**debug ip admission eapoudp** **例：** Router# debug ip admission eapoudp	IP アドミッション イベントに関する情報を表示します。

CISCO-NAC-NAD-MIB を使用した NAC のモニタおよび制御

ここでは、次の作業について説明します。

- 「cnnEouHostValidateAction テーブル オブジェクトに関連する CLI コマンド」（P.18）
- 「cnnEouIfConfigTable オブジェクトに関連する CLI コマンド」（P.18）
- 「cnnEouHostValidateAction テーブル オブジェクトに関連する CLI コマンド」（P.18）
- 「MIB クエリー テーブルの作成」（P.19）
- 「MIB クエリーの結果の表示」（P.22）

cnnEouGlobalObjectsGroup テーブル オブジェクトに関連する CLI コマンド

SNMP get または set 操作を実行して、cnnEouGlobalObjectsGroup テーブルにあるオブジェクトの値の範囲に関する情報を取得または変更できます。同じ情報は、**show eou** コマンドの出力でも表示できます。表 1 に、一部のグローバル設定オブジェクトと、その値を取得または変更するのに必要な SNMP get および set 操作の例を示します。

show eou コマンドの出力例については、「show eou」（P.25）を参照してください。

表 1　SNMP Get および Set 操作を使用したグローバル設定値の取得および変更

グローバル設定オブジェクト	SNMP の操作
EAPoUDP のバージョン	cnnEouVersion オブジェクトに対して get 操作を実行します（オブジェクトの値は「1」です）。

表 1　SNMP Get および Set 操作を使用したグローバル設定値の取得および変更（続き）

グローバル設定オブジェクト	SNMP の操作
EAPoUDP ポート	cnnEouPort オブジェクトに対して get 操作を実行します。
ロギングのイネーブル化（EOU ロギングのイネーブル化）	cnnEouLoggingEnable オブジェクトを設定します（オブジェクトの値は「true」です）。

cnnEouIfConfigTable オブジェクトに関連する CLI コマンド

cnnEouIfConfigTable にあるオブジェクトの値の範囲に関する情報を取得するには、SNMP get 操作を実行します。同じ情報は、**show eou** コマンドの出力でも表示できます。表 2 に、一部のインターフェイス固有の設定オブジェクトと、その値を取得するのに必要な SNMP get 操作の例を示します。

表 2　SNMP Get 操作を使用したインターフェイス固有の設定値の取得

インターフェイス固有のオブジェクト	SNMP の操作
AAA タイムアウト	cnnEouIfTimeoutAAA オブジェクトに対して get 操作を実行します。 • 形式 : GET cnnEouIfTimeoutAAA.IfIndex • 特定のインターフェイスの対応するインデックス番号を指定する必要があります。
最大リトライ回数	cnnEouIfMaxRetry オブジェクトに対して get 操作を実行します。 • 形式 : GET cnnEouIfMaxRetry.IfIndex

cnnEouHostValidateAction テーブル オブジェクトに関連する CLI コマンド

CLI を実行するか、cnnEouHostValidateAction テーブルに対して SNMP set 操作を使用すると、EOU セッションを初期化または再検証できます。

次に、MIB オブジェクトに関連する一部の例（CLI コマンドの一覧）を示します。

eou initialize all

すべてのセッションの EOU の初期化を実行するには、**eou initialize all** コマンドを使用するか、cnnEouHostValidateAction オブジェクトに対して SNMP set 操作を使用します。このオブジェクトには数値 2 を設定する必要があります。

eou initialize authentication clientless

認証タイプが「クライアントレス」のセッションの EOU の初期化を実行するには、**eou initialize authentication clientless** コマンドを使用するか、cnnEouHostValidateAction オブジェクトに対して SNMP set 操作を使用します。このオブジェクトには数値 3 を設定する必要があります。

eou initialize ip

特定のセッションの EOU の初期化を実行するには、**eou initialize ip** {*ip-address*} コマンドを使用します。

SNMP 操作を使用して同じ結果を得るには、cnnEouHostValidateAction MIB テーブルに次の 3 つのオブジェクトを設定する必要があります。

- cnnEouHostValidateAction : 値の範囲を設定する必要があります。

- cnnEouHostValidateIpAddrType：IP アドレスのタイプを設定する必要があります。現在 NAC でサポートされているアドレス タイプは IPv4 のみであるため、この値を Ipv4 に設定する必要があります（この値は、cnnEouHostValidateIPAddr オブジェクトに設定されるアドレス タイプです）。
- cnnEouHostValidateIPAddr：IP アドレスを設定する必要があります。

（注） この 3 つの MIB オブジェクトは 1 回の SNMP set 操作で設定する必要があります。

eou initialize posturetoken

eou initialize posturetoken {*string*} コマンドを使用すると、特定の posturetoken を持つすべてのセッションを初期化できます。このコマンドのデフォルト値の範囲は 8 です。

SNMP set 操作を使用して同じ結果を得るには、次のオブジェクトを設定する必要があります。

- cnnEouHostValidateAction：この値を 8 に設定します。
- cnnEouHostValidatePostureTokenStr：文字列の値を設定します。

（注） この 2 つの MIB オブジェクトは 1 回の SNMP set 操作で設定する必要があります。

MIB クエリー テーブルの作成

MIB テーブル cnnEouHostQueryTable は、MIB クエリーの作成または構築に使用されます。

show eou all CLI コマンドに関連する MIB クエリー

show eou all コマンドを使用した場合と同じ結果が得られるクエリーを構築するには、次の SNMP get 操作を実行します。

cnnEouHostQueryTable テーブルの cnnEouHostQueryMask オブジェクトは、クエリーの種類を表しています。**show eou all** コマンドの出力に対応する cnnEouHostQueryMask オブジェクトの値は 8（整数値）です。

手順の概要

1. cnnEouHostQueryStatus オブジェクトに createandgo を設定します。
2. cnnEouHostQueryMask オブジェクトに 8 を設定します。
3. cnnEouHostQueryStatus オブジェクトをアクティブに設定して、クエリーの作成が完了したことを示します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	cnnEouHostQueryStatus オブジェクトに createandgo を設定します。	クエリーの行を作成します。
ステップ 2	cnnEouHostQueryMask オブジェクトに 8 を設定します。	**show eou all** コマンドの値に対応します。
ステップ 3	cnnEouHostQueryStatus オブジェクトをアクティブに設定します。	クエリーの構築が終了したことを示します。

（注） 前の表では例を示していません。これは、使用しているソフトウェアによって形式が異なるためです。

この次の手順

結果を表示します。「show eou all コマンドに関連する MIB クエリーの結果の表示」の項を参照してください。

show eou all コマンドに関連する MIB クエリーの結果の表示

MIB クエリーを構築し、「アクティブ」ステータスで終了したことを示したら、結果を表示できます。cnnEouHostQueryTable のクエリーは行で表されます。行番号はクエリー インデックスになります。同様に、cnnEouHostResultTable は結果の行で構成されます。cnnEouHostResultTable の各行は、クエリー インデックスと結果インデックスの組み合わせによって一意に識別されます。cnnEouHostQueryTable の結果のインデックスと cnnEouHostResultTable は一致する必要があります。クエリー テーブル内の 1 行を、結果テーブル内の複数行の 1 つに一致させます。たとえば、**show** コマンドに対応するクエリーの結果が 10 個のセッションになった場合、結果テーブルには 10 行存在し、各行が特定のセッションに対応します。結果テーブルの 1 番めの行は R1.1 です。2 番めの行は R1.2 となり、R1.10 まで続きます。クエリー テーブルに別のクエリーが作成され、その結果が 5 個のセッションになった場合、結果テーブルには 5 行作成されます（R2.1、R2.2、R2.3、R2.4、R2.5）。

表 3 に、クエリー テーブルのセッションが結果テーブルの行にマップされる方法を示します。

表 3　クエリー テーブルと結果テーブルのマッピング

クエリー テーブル	結果テーブルの行
Q1（10 セッション）	R1.1、R1.2、R1.3、R1.4、R1.5、R1.6、R1.7、R1.8、R1.9、R1.10
Q2（5 セッション）	R2.1、R2.2、R2.3、R2.4、R2.5

SNMP クエリーの作成

show eou ip {*ip-address*} コマンドの出力と同じ情報を得られる SNMP クエリーを作成するには、次の手順を実行します。

手順の概要

1. cnnEouHostQueryStatus に createandgo を設定します。
2. cnnEouHostQueryIpAddrType に IPv4 および IP アドレス（たとえば 10.2.3.4）を設定します。
3. cnnEouHostQueryStatus をアクティブに設定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	cnnEouHostQueryStatus に createandgo を設定します。	クエリーの行を作成します。
ステップ 2	cnnEouHostQueryIpAddrType に IPv4 および IP アドレス（たとえば 10.2.3.4）を設定します。	アドレス タイプを設定します。 • 現在 NAC でサポートされているアドレス タイプは IPv4 のみです。
ステップ 3	cnnEouHostQueryStatus をアクティブに設定します。	クエリーの構築が終了したことを示します。

（注） 前の表では例を示していません。これは、使用しているソフトウェアによって形式が異なるためです。

結果の表示

cnnEouHostResultTable の結果を表示するには、次の手順を実行します。

手順の概要

1. cnnEouHostQueryRows に対して get 操作を実行します。
2. resultTableObjectName.QueryIndex.ResultIndex の形式で、cnnEouHostResultTable オブジェクトに対して get 操作を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	cnnEouHostQueryRows に対して get 操作を実行します。	特定のクエリーで結果テーブルに作成された行数を検索します。 • クエリーの行がマイナスの数字である場合、そのクエリーはまだ処理中です。
ステップ 2	resultTableObjectName.QueryIndex.ResultIndex の形式で、cnnEouHostResultTable オブジェクトに対して get 操作を実行します。	結果テーブルで特定のクエリーに一致する特定のオブジェクトの値を検索します。 • 1 つのクエリーに対して結果テーブルに複数行がある場合、ResultIndex の範囲は 1 から cnnEouHostQueryRows の値までになります。

（注） 前述の表では例を示していません。これは、使用しているソフトウェアによって形式が異なるためです。

show eou ip コマンドに関連する MIB クエリー

show eou ip {*ip-address*} コマンドと同じ結果が得られる MIB クエリーを構築するには、次の SNMP get 操作を実行します。

手順の概要

1. cnnEouHostQueryStatus オブジェクトに createandgo を設定します。
2. cnnEouHostQueryIpAddrType オブジェクトに「IPv4」を設定します。
3. cnnEouHostQueryIpAddr オブジェクトに IP アドレス（たとえば 10.2.3.4）を設定します。
4. cnnEouHostQueryStatus オブジェクトをアクティブに設定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	cnnEouHostQueryStatus オブジェクトに createandgo を設定します。	クエリーのステータスを設定します。
ステップ 2	cnnEouHostQueryIpAddrType オブジェクトに「IPv4」を設定します。	アドレス タイプを設定します。 （注） 現在 NAC でサポートされているアドレス タイプは IPv4 のみです。
ステップ 3	cnnEouHostQueryIpAddr オブジェクトに IP アドレス（たとえば 10.2.3.4）を設定します。	IP アドレスを設定します。
ステップ 4	cnnEouHostQueryStatus オブジェクトをアクティブに設定します。	クエリーの構築が終了したことを示します。

（注） 前の表では例を示していません。これは、使用しているソフトウェアによって形式が異なるためです。

MIB クエリーの結果の表示

MIB クエリーを構築したら、cnnEouHostResultTable の結果を表示できます。結果の確認方法の詳細については、「show eou all コマンドに関連する MIB クエリーの結果の表示」（P.20）を参照してください。

クエリーのサブクエリーへの分割

show eou all コマンドに関連する MIB クエリーを実行すると、2,000 もの行が出力される場合があります。MIB クエリーのすべての情報を確実に表示できるようにするために、そのクエリーをサブクエリーに分割することができます。たとえば、クエリーの出力が 2,000 行になる場合、クエリーを 4 つのサブクエリーに分割して、結果を 1 ページずつの形式で表示できます。1 番めのサブクエリーには 1 ～ 500 行め（最初の 500 セッション）が含まれ、2 番めのサブクエリーには 501 ～ 1,000 行め、3 番めのサブクエリーには 1,001 ～ 1,500 行め、4 番めのサブクエリーには 1,501 ～ 2,000 行めまでが含まれるようにします。

（注） cnnEouHostQueryTotalHosts オブジェクトは、クエリーの条件に一致するホストの合計数（行数）を提供します。この数字を調べると、必要なサブクエリーの数を判断できます。ただし、最初のクエリーを構築するまでは、cnnEouHostQueryTotalHosts オブジェクトの数字を取得できません。

クエリーを構築するには次の手順を実行します。

手順の概要

1. cnnEouHostQueryStatus オブジェクトに createandgo を設定します。
2. cnnEouHostQueryMask オブジェクトに 8 を設定します。
3. cnnEouHostQueryRows に 500 を設定します。
4. cnnEouHostQuerySkipNHosts に 0 を設定します。
5. cnnEouHostQueryStatus オブジェクトをアクティブに設定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	cnnEouHostQueryStatus オブジェクトに createandgo を設定します。	クエリーのステータスを設定します。
ステップ 2	cnnEouHostQueryMask オブジェクトに 8 を設定します。	**show eou all** コマンドのデフォルトに関連付けます。
ステップ 3	cnnEouHostQueryRows に 500 を設定します。	このクエリーで結果テーブルに構築される最大行数を識別します。
ステップ 4	cnnEouHostQuerySkipNHosts に 0 を設定します。	作成される結果の行に対応します。
ステップ 5	cnnEouHostQueryStatus オブジェクトをアクティブに設定します。	クエリーの構築が終了したことを示します。

（注） 前の表では例を示していません。これは、使用しているソフトウェアによって形式が異なるためです。この表は、2,000 セッション（行）を返すクエリーに基づいています。

この次の手順

前述のタスクを実行したら、最初の 500 ホスト（行）の情報のクエリーが実行されます。次の 500 ホスト（行）のクエリー情報を表示するには同じ 5 つの手順を実行しますが、ステップ 4 の cnnEouHostQuerySkipNHosts オブジェクトの値を 500 に変更します。このタスクによって、501 ～ 1000 行めのクエリー情報を取得できます。同じ方法で、残りのホスト（2000 まで）のクエリー情報を取得するには、もう一度同じ 5 つの手順を実行し、ステップ 4 の cnnEouHostQuerySkipNHosts オブジェクトの値をそれぞれ 1000 と 1500 に変更します。

ネットワーク アドミッション コントロールの設定例

ここでは、次の例について説明します。

- 「ネットワーク アドミッション コントロール：例」（P.24）
- 「NAC MIB の出力：例」（P.25）

ネットワーク アドミッション コントロール：例

次の出力例では、IP アドミッション コントロールが Cisco IOS ルータに設定されています。

```
Router# show running-config

Building configuration...

Current configuration: 1240 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
aaa new-model
!
!
aaa authentication eou default group radius
aaa session-id common
ip subnet-zero
ip cef
!
! The following line creates a network admission rule. A list is not specified; therefore,
! the rule intercepts all traffic on the applied interface.
ip admission name avrule eapoudp
!
eou logging
!
!
interface FastEthernet0/0
 ip address 10.13.11.106 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.0.0.1 255.255.255.0
 ip access-group 102 in
! The following line configures an IP admission control interface.
 ip admission avrule
 duplex auto
 speed auto
!
ip http server
no ip http secure-server
ip classless
!
!
```

```
! The following lines configure an interface access list that allows EAPoUDP traffic
! and blocks the rest of the traffic until it is validated.
access-list 102 permit udp any any eq 21862
access-list 102 deny   ip any any
!
!
! The following line configures RADIUS.
radius-server host 10.13.11.105 auth-port 1645 acct-port 1646 key cisco
!
control-plane
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
!
end
```

NAC MIB の出力：例

次に、MIB オブジェクト情報を表示する **show** コマンドの出力例を示します。

show eou

show eou コマンドは、さまざまな CISCO-NAC-NAD-MIB テーブルでも表示可能な情報を出力します。**show eou** コマンドを実行した結果の情報は cnnEouGlobalObjectsGroup テーブルにもあり、**show eou all** コマンドを実行した結果の情報は cnnEouIfConfigTable にもあります。

```
Router# show eou

Global EAPoUDP Configuration
----------------------------
EAPoUDP Version     = 1
EAPoUDP Port        = 0x5566
Clientless Hosts    = Enabled
IP Station ID       = Disabled
Revalidation        = Enabled
Revalidation Period = 36000 Seconds
ReTransmit Period   = 3 Seconds
StatusQuery Period  = 300 Seconds
Hold Period         = 30 Seconds
AAA Timeout         = 60 Seconds
Max Retries         = 3
EAP Rate Limit      = 20
EAPoUDP Logging     = Enabled
Clientless Host Username = clientless
Clientless Host Password = clientless

Router# show eou all

Interface Specific EAPoUDP Configurations
-----------------------------------------
Interface Vlan333
AAA Timeout         = 60 Seconds
Max Retries         = 3
eou initialize interface {interface-name}
```

```
eou revalidate interface {interface-name}
```

show ip device tracking all

show ip device tracking all コマンドは、cnnIpDeviceTrackingObjectsGroup MIB テーブルでも表示可能な情報を出力します。次に、その **show** コマンドの出力例を示します。

```
Router# show ip device tracking all

IP Device Tracking = Enabled
Probe Count: 2
Probe Interval: 10
```

その他の参考資料

ここでは、ネットワーク アドミッション コントロールに関する関連資料について説明します。

関連資料

内容	参照先
ACL の設定	「IP Access List Overview」フィーチャ モジュール
認証、認可、およびアカウンティング	『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 12.4T』の「Authentication, Authorization, and Accounting」
インターフェイス、設定	『*Cisco IOS Configuration Fundamentals Configuration Guide,* Release 12.4T』
SNMP、および SNMP get 操作と set 操作	

規格

規格	タイトル
この機能によってサポートされる新しい規格や変更された規格はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によってサポートされる新しい RFC や変更された RFC はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

ネットワーク アドミッション コントロールの機能情報

表 4 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 4 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 4　ネットワーク アドミッション コントロールの機能情報

機能名	リリース	機能情報
ネットワーク アドミッション コントロール	12.3(8)T	ネットワーク アドミッション コントロール機能は、増大するワームやウイルスがネットワーク化されたビジネスに与える脅威や影響に対応します。この機能は、顧客がセキュリティの脅威を認識して防御し、適合するのに役立つ Cisco Self-Defending Network Initiative（自己防衛型ネットワーク構想）の一部です。 Cisco Network Admission Control 機能は、その初期段階で、エンドポイントがネットワークに接続しようとしたときに Cisco ルータがアクセス権限を制限できるようにします。 この機能に関する詳細については、次の各項を参照してください。 • 「ネットワーク アドミッション コントロールの前提条件」（P.2） • 「ネットワーク アドミッション コントロールの制約事項」（P.2） • 「ネットワーク アドミッション コントロールの概要」（P.2） • 「ネットワーク アドミッション コントロールの設定方法」（P.7） • 「ネットワーク アドミッション コントロールの設定例」（P.24） この機能により、次のコマンドが導入または変更されました。**aaa authentication eou default enable group radius**、**access-group**（アイデンティティ ポリシー）、**auth-type**、**clear eou**、**clear ip admission cache**、**debug eap**、**debug eou**、**debug ip admission eapoudp**、**description**（アイデンティティ ポリシー）、**description**（アイデンティティ プロファイル）、**device**（アイデンティティ プロファイル）、**eou allow**、**eou clientless**、**eou default**、**eou initialize**、**eou logging**、**eou max-retry**、**eou port**、**eou rate-limit**、**eou revalidate**、**eou timeout**、**identity policy**、**identity profile eapoudp**、**ip admission**、**ip admission name**、**redirect**（アイデンティティ ポリシー）、**show eou**、**show ip admission**、**template**（アイデンティティ ポリシー）

表 4　ネットワーク アドミッション コントロールの機能情報（続き）

機能名	リリース	機能情報
NAC MIB	12.4(15)T	CISCO-NAC-NAD-MIB のサポートが追加されました。この MIB モジュールは、Cisco NAC システムの NAD のモニタおよび設定に使用されます。 この機能に関する詳細については、次の各項を参照してください。 • 「NAC MIB」（P.5） • 「CISCO-NAC-NAD-MIB を使用した NAC のモニタおよび制御」（P.17） この機能により、次のコマンドが導入または変更されました。**show ip device tracking**。
	12.2(33)SXI	この機能は、Cisco IOS Release 12.2(33)SXI に統合されました。

用語集

EAPoUDP : Extensible Authentication Protocol over User Datagram Protocol の略です。EAP は、PPP で複数の任意の認証メカニズムをサポートするフレームワークで、クリアテキスト パスワード、チャレンジとレスポンス、任意のダイアログ シーケンスなどがあります。UDP は、TCP/IP プロトコル スタックのコネクションレス トランスポート レイヤ プロトコルです。UDP は、確認応答または保証された配信を使用せずにデータグラムを交換するシンプルなプロトコルで、他のプロトコルでエラー処理や再送信を実行する必要があります。UDP は RFC 768 で定義されています。

IP アドミッション ルール : IP アドミッション コントロールを適用する方法を定義した名前付きのルールです。IP アドミッション ルールはインターセプト ACL に関連付けられ、IP アドミッション機能を使用できるホストを制御します。IP アドミッション コントロール ルールを作成するには、ip admission name コマンドを使用します。

デフォルト アクセス ポリシー : AAA サーバがクレデンシャルを検証するまで、クライアント デバイスに適用される ACL を設定します。

ポスチャ トークン : ポスチャ クレデンシャルの評価結果の伝達に使用されるステータスです。AAA サーバは、ポスチャ トークン（ステータスには Healthy、Checkup、Quarantine、Infected、または Unknown を使用できます）を、クライアントが到達するピアのネットワーク アクセス ポリシー（ACL、URL、リダイレクト、またはステータス クエリー タイマー）にマップします。

セキュリティ サーバ プロトコル

RADIUS

RADIUS の設定

Remote Authentication Dial-In User Service（RADIUS ）セキュリティ システムは、不正アクセスに対してネットワーク保護する分散クライアント/サーバ システムです。シスコの実装では RADIUS クライアントは Cisco ルータ上で稼動します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。RADIUS は完全にオープンなプロトコルであり、ソース コード形式で配布されているため、現在使用できる任意のセキュリティ システムと連携するように変更できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「RADIUS の設定に関する機能情報」（P.45）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

RADIUS の概要

シスコは、AAA セキュリティ パラダイムの下で RADIUS をサポートしています。RADIUS は、TACACS+、Kerberos、ローカル ユーザ名の検索など、他の AAA セキュリティ プロトコルと併用できます。RADIUS はすべてのシスコ プラットフォームでサポートされていますが、一部の RADIUS 対応機能は特定のプラットフォームでだけ動作します。

RADIUS は、リモート ユーザのネットワーク アクセスを維持すると同時に高度なレベルのセキュリティを必要とするさまざまなネットワーク環境に実装されています。

RADIUS は、アクセスのセキュリティが必要な次のネットワーク環境で使用できます。

- 複数のベンダーのアクセス サーバで構成され、それぞれが RADIUS をサポートするネットワーク。たとえば複数のベンダーのアクセス サーバが、1 つの RADIUS サーバベースのセキュリティ データベースを使用します。複数ベンダーのアクセス サーバがある IP ベースのネットワークの場合、Kerberos セキュリティ システムと連携するようにカスタマイズされた RADIUS サーバを介して、ダイヤルイン ユーザが認証されます。
- Turnkey ネットワーク セキュリティ環境。「スマート カード」コントロール システムを使用するアクセス環境など、アプリケーションが RADIUS プロトコルをサポートする環境です。ある事例では、RADIUS と Enigma のセキュリティ カードを併用してユーザを検証し、ネットワーク リソースに対するアクセス権を付与しています。
- すでに RADIUS を使用しているネットワーク。RADIUS 機能を持つ Cisco ルータをネットワークに追加できます。Terminal Access Controller Access Control System Plus（TACACS+）サーバに移行する場合、これが最初の手順となります。
- ユーザが単一のサービスにだけアクセスする必要があるネットワーク。RADIUS を使用すると、単一ホスト、単一ユーティリティ（Telnet など）、または単一プロトコル（Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル））に対するユーザ アクセスを制御できます。たとえば、ユーザがログインすると、RADIUS は、IP アドレス 10.2.3.4 を使用してそのユーザが PPP を実行する権限を持っていることを識別し、定義済みのアクセス リストが開始されます。
- リソースのアカウンティングが必要なネットワーク。RADIUS アカウンティングは、RADIUS 認証や認可と無関係に使用できます。RADIUS アカウンティング機能を使用すると、サービスの開始と終了の時点にデータを送信し、そのセッション中に使用されたリソース（時間、パケット、バイトなど）の量を示すことができます。Internet service provider（ISP; インターネット サービス プロバイダー）は、RADIUS アクセス制御およびアカウンティング ソフトウェアのフリーウェア バージョンを使用して、セキュリティおよび課金の独自ニーズを満たすこともできます。
- 事前認証のサポートを希望するネットワーク。ネットワークに RADIUS サーバを導入すると、AAA 事前認証を設定し、事前認証のプロファイルを設定できます。サービス プロバイダーが事前認証を使用すると、既存の RADIUS ソリューションを使用するポートの管理性が向上し、共有リソースを効率的に管理して、各種のサービスレベル 契約を提供できるようになります。

RADIUS は次のネットワーク セキュリティ状況には適していません。

- マルチプロトコル アクセス環境。RADIUS は次のプロトコルをサポートしていません。
  - AppleTalk Remote Access（ARA）
  - NetBIOS Frame Control Protocol（NBFCP）
  - NetWare Asynchronous Services Interface（NASI）
  - X.25 PAD 接続
- ルータ間で接続している環境。RADIUS には双方向認証機能がありません。非 Cisco ルータが RADIUS 認証を必要としている場合、一方のルータから非 Cisco ルータへの接続を認証するために、RADIUS を使用できます。

- 多様なサービスを使用するネットワーク。通常、RADIUS は 1 人のユーザを 1 つのサービス モデルにバインドします。

RADIUS の動作

ユーザがログインを試行し、RADIUS を使用してアクセス サーバから認証を受ける場合、次の手順が発生します。

1. プロンプトが表示され、ユーザはユーザ名およびパスワードを入力します。
2. ユーザ名と暗号化されたパスワードがネットワーク経由で RADIUS サーバに送信されます。
3. ユーザは、RADIUS サーバから次のいずれかの応答を受信します。
   a. ACCEPT：ユーザが認証されたことを表します。
   b. REJECT：ユーザの認証が失敗し、ユーザ名およびパスワードの再入力を要求されるか、またはアクセスが拒否されます。
   c. CHALLENGE：RADIUS サーバによりチャレンジが送信されます。チャレンジによってユーザから追加データが収集されます。
   d. CHANGE PASSWORD：ユーザは新しいパスワードを選択するように RADIUS サーバから要求が送信されます。

ACCEPT または REJECT 応答には、EXEC またはネットワーク許可に使用される追加データが含まれています。ユーザは RADIUS 認証が完了しないうちは RADIUS 許可を使用できません。ACCEPT または REJECT パケットに含まれる追加データには、次のものがあります。

- Telnet、rlogin、または Local-Area Transport（LAT; ローカルエリア トランスポート）、および PPP、Serial Line Internet Protocol（SLIP）、または EXEC サービスなどといった、ユーザがアクセスできるサービス。
- ホストまたはクライアントの IP アドレス、アクセス リスト、ユーザ タイムアウトなどの接続パラメータ。

RADIUS アトリビュート

ネットワーク アクセス サーバは、各ユーザ プロファイルで RADIUS アトリビュートで定義されている RADIUS 認可機能およびアカウンティング機能をモニタします。サポートされる RADIUS アトリビュートのリストの詳細については、「関連資料」（P.43）を参照してください。

ここでは、次の内容について説明します。

- 「ベンダー固有 RADIUS アトリビュート」（P.3）
- 「RADIUS トンネル アトリビュート」（P.4）

ベンダー固有 RADIUS アトリビュート

RADIUS の Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）ドラフト規格には、ネットワーク アクセス サーバと RADIUS サーバ間でベンダー固有情報を通信する際の方式が規定されています。さらに、一部のベンダーが固有の方法で RADIUS アトリビュートを拡張しています。Cisco IOS ソフトウェアは、RADIUS のベンダー固有アトリビュートの一部をサポートしています。詳細については、「関連資料」（P.43）を参照してください。

RADIUS トンネル アトリビュート

RADIUS は、元は Livingston, Inc. が開発した セキュリティ サーバの Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）プロトコルです。RADIUS は Attribute Value（AV; アトリビュート値）ペアを使用して、セキュリティ サーバとネットワーク アクセス サーバ間で情報を通信します。RFC 2138 と RFC 2139 では、RADIUS の基本機能と、AAA 情報の送信に使用されるインターネット技術特別調査委員会（IETF）規格の AV ペアの初期セットについて説明しています。2 つのドラフト IETF 規格「RADIUS Attributes for Tunnel Protocol Support」と「RADIUS Accounting Modifications for Tunnel Protocol Support」は、IETF が定義した AV ペアを拡張して、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）に固有のアトリビュートを追加しました。これらのアトリビュートは、RADIUS サーバとトンネル イニシエータ間のトンネリング情報を伝送するために使用されます。RFC 2865 と RFC 2868 は IETF が定義した AV ペア セットを拡張して、VPN の強制トンネリングに固有のアトリビュートを追加しています。このアトリビュートを使用して、ユーザはネットワーク アクセス サーバおよび RADIUS サーバの認証名を指定できます。

Cisco ルータとアクセス サーバは、新しい RADIUS IETF 規格の VPDN トンネル アトリビュートにサポートしています。詳細については、「関連資料」（P.43）を参照してください。

また、次の設定例も参照してください。

- 「例：RADIUS トンネリング アトリビュートを指定した RADIUS ユーザ プロファイル」（P.38）
- 「例：L2TP アクセス コンセントレータ」（P.39）
- 「例：L2TP ネットワーク サーバ」（P.40）

L2F、L2TP、VPN、または VPDN の詳細については、「関連資料」（P.43）を参照してください。

RADIUS の設定方法

Cisco ルータまたはアクセス サーバで RADIUS を設定するには、次のタスクを実行する必要があります。

- **aaa new-model** グローバル コンフィギュレーション コマンドを使用して、AAA をイネーブルにします。RADIUS を使用する予定がある場合、AAA を設定する必要があります。
- **aaa authentication** グローバル コンフィギュレーション コマンドを使用して、RADIUS 認証の方式リストを定義します。**aaa authentication** コマンドの詳細な使用方法については、「Configuring Authentication」モジュールを参照してください。
- **line** および **interface** コマンドを使用して、使用する定義済みの方式リストをイネーブルにします。詳細については、「Configuring Authentication」モジュールを参照してください。

次の設定タスクは任意です。

- **aaa group server** コマンドを使用して、特定のサービスのために、選択した RADIUS ホストをグループ化できます。**aaa group server** コマンドの詳細な使用方法については、「AAA サーバ グループの設定」（P.14）を参照してください。
- **aaa dnis map** コマンドを使用して、DNIS 番号に基づいて RADIUS サーバ グループを選択できます。このコマンドを使用するには、**aaa group server** コマンドを使用して RADIUS サーバ グループを定義する必要があります。**aaa dnis map** コマンドの詳細な使用方法については、「DNIS に基づく AAA サーバ グループの選択の設定」（P.18）を参照してください。
- **aaa authorization** グローバル コマンドを使用して、特定のユーザ機能を認可できます。**aaa authorization** コマンドの詳細な使用方法については、「Configuring Authorization」モジュールを参照してください。

- **aaa accounting** コマンドを使用して RADIUS 接続のアカウンティングをイネーブルにできます。**aaa accounting** コマンドの詳細な使用方法については、「Configuring Accounting」モジュールを参照してください。
- **dialer aaa** インターフェイス コンフィギュレーション コマンドを使用して、AAA サーバでの発信アトリビュートを含むリモート サイト プロファイルを作成できます。**dialer aaa** コマンドの詳細な使用方法については、「RADIUS アクセス要求のサフィックスとパスワードの設定」（P.30）を参照してください。

ここでは、ネットワークでの認証、認可、およびアカウンティングについて RADIUS を設定する方法について説明します。内容は次のとおりです。

- 「RADIUS サーバと通信するためのルータの設定」（P.5）（必須）
- 「RADIUS のベンダー固有アトリビュートを使用するためのルータの設定」（P.8）（任意）
- 「ベンダー固有の RADIUS サーバ通信のためのルータの設定」（P.10）（任意）
- 「RADIUS サーバのスタティック ルートと IP アドレスを照会するためのルータの設定」（P.11）（任意）
- 「ネットワーク アクセス サーバのポート情報を拡張するためのルータの設定」（P.12）（任意）
- 「AAA サーバ グループの設定」（P.14）（任意）
- 「デッドタイムによる AAA サーバ グループの設定」（P.15）（任意）
- 「AAA DNIS 認証の設定」（P.17）
- 「DNIS に基づく AAA サーバ グループの選択の設定」（P.18）（任意）
- 「AAA 事前認証の設定」（P.20）
- 「ガード タイマーの設定」（P.27）
- 「RADIUS 認証の指定」（P.28）
- 「RADIUS 認可の指定」（P.29）（任意）
- 「RADIUS アカウンティングの指定」（P.29）（任意）
- 「RADIUS Login-IP-Host の設定」（P.29）（任意）
- 「RADIUS プロンプトの設定」（P.29）（任意）
- 「RADIUS アクセス要求のサフィックスとパスワードの設定」（P.30）（任意）

このモジュールのコマンドを使用した RADIUS の設定例については、「RADIUS の設定例」（P.32）を参照してください。

RADIUS サーバと通信するためのルータの設定

通常、RADIUS ホストは、シスコ（CiscoSecure ACS）、Livingston、Merit、Microsoft、または他のソフトウェア プロバイダーの RADIUS サーバ ソフトウェアを実行するマルチユーザ システムです。RADIUS サーバとの通信のためにルータを設定するには、次のような要素があります。

- ホスト名または IP アドレス
- 認証の宛先ポート
- アカウンティングの宛先ポート
- タイムアウト時間
- 再送信値
- キー ストリング

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスおよび特定の UDP ポート番号に基づいて識別されます。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。つまり、この固有識別情報を使用して、ある IP アドレスに位置する 1 台のサーバ上に複数の UDP ポートが存在する場合、それぞれの UDP ポートに対して RADIUS 要求を送信できます。1 台の RADIUS サーバ上にある異なる 2 つのホスト エントリが 1 つのサービス（アカウンティングなど）に設定されている場合、設定されている 2 番めのホスト エントリは最初のホスト エントリのフェールオーバー バックアップとして動作します。この例の場合、最初のホスト エントリがアカウンティング サービスの提供に失敗すると、同じデバイスに設定されている 2 番めのホスト エントリを使用してアカウンティング サービスを提供するように、ネットワーク アクセス サーバが試行します（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

RADIUS サーバと Cisco ルータは、共有秘密テキスト ストリングを使用してパスワードを暗号化し、応答を交換します。RADIUS を設定して AAA セキュリティ コマンドを使用するには、RADIUS サーバ デーモンを実行するホストと、ルータと共有する秘密テキスト（キー）ストリングを指定する必要があります。

タイムアウト値、再送信値、および暗号化キー値には、すべての RADIUS サーバを対象にしたグローバル設定、サーバ別設定、またはグローバル設定とサーバ別設定の組み合わせを使用できます。すべての RADIUS サーバとルータとの通信にこのようなグローバル設定を適用するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** という 3 つの固有なグローバル コマンドを使用します。特定の RADIUS サーバにこれらの値を適用するには、**radius-server host** コマンドを使用します。

（注） 同じシスコ製ネットワーク アクセス サーバで、タイムアウト、再送信、およびキー値のコマンドを同時に設定（グローバル設定およびサーバ別設定）できます。ルータにグローバル機能とサーバ別機能の両方を設定する場合、サーバ別のタイマー、再送信、およびキー値のコマンドの方が、グローバルのタイマー、再送信、およびキー値のコマンドよりも優先されます。

サーバごとに RADIUS サーバ通信を設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}]
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] 例： `Router(config)# radius-server host 10.45.1.2`	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定し、認証とアカウンティングの宛先ポート番号を割り当てます。**auth-port** *port-number* オプションを使用して、認証専用の RADIUS サーバに固有の UDP ポートを設定します。**acct-port** *port-number* オプションを使用して、アカウンティング専用の RADIUS サーバに固有の UDP ポートを設定します。**alias** キーワードを使用して、RADIUS サーバを参照するときに使用する IP アドレス（最大 8 個）を設定します。 単一の IP アドレスに関連付けられた複数のホスト エントリを認識するようにネットワーク アクセス サーバを設定するには、必要な回数、このコマンドを繰り返すだけです。その際、各 UDP を固有の値にします。特定の RADIUS ホストで使用するタイムアウト、再送信、暗号化キーを設定します。 タイムアウトを設定しない場合、グローバル値が使用されます。設定する場合、値の範囲は 1 ～ 1000 です。再送信値を設定しない場合、グローバル値が使用されます。設定する場合、値の範囲は 1 ～ 1000 です。キーストリングを指定しない場合、グローバル値が使用されます。 **（注）** キーはテキスト ストリングで、RADIUS サーバで使用される暗号化キーと一致する必要があります。キーの先頭にあるスペースは無視されますが、キー内のスペースとキー末尾のスペースは使用されるため、キーは常に **radius-server host** コマンド構文の最後のアイテムとして設定してください。キーにスペースを使用する場合、引用符をキーに含める場合を除き、引用符でキーを囲まないでください。
ステップ 4	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。

ルータと RADIUS サーバ間のグローバル通信設定を指定するには、次の **radius-server** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server key** {**0** *string* | **7** *string* | *string*}
4. **radius-server retransmit** *retries*
5. **radius-server timeout** *seconds*
6. **radius-server deadtime** *minutes*

7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server key** {**0** *string* | **7** *string* | *string*} 例： `Router(config)# radius-server key myRaDIUSpassword`	ルータと RADIUS サーバ間に使用する共有秘密テキスト ストリングを指定します。**0** *line* オプションを使用して、暗号化されていない共有秘密を設定します。**7** *line* オプションを使用して、暗号化された共有秘密を設定します。
ステップ 4	**radius-server retransmit** *retries* 例： `Router(config)# radius-server retransmit retries`	ルータからサーバに対して、各 RADIUS 要求を送信する回数の上限を指定します（デフォルトは 3 です）。
ステップ 5	**radius-server timeout** *seconds* 例： `Router(config)# radius-server timeout 6`	ルータが RADIUS 要求に対する応答を待機して、再送信するまでの時間（秒数）を指定します。
ステップ 6	**radius-server deadtime** *minutes* 例： `Router(config)# radius-server deadtime 5`	RADIUS 認証要求に応答しない RADIUS サーバが、認証要求の期限切れになるまでの時間（分数）を指定します。
ステップ 7	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。

RADIUS のベンダー固有アトリビュートを使用するためのルータの設定

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）ドラフト標準には、ネットワーク アクセス サーバと RADIUS サーバの間で VSA（Vendor-Specific Attribute; ベンダー固有アトリビュート）（アトリビュート 26）を使用してベンダー固有の情報を伝達する方法が規定されています。ベンダーは、ベンダー固有アトリビュート（VSA）を使用して、汎用ではない拡張のベンダー固有アトリビュートをサポートしています。シスコの RADIUS 実装では、IETF 仕様で推奨される形式を使用したベンダー固有オプションを 1 つサポートしています。シスコのベンダー ID は 9 で、サポートするオプションはベンダー タイプ 1、名前は「cisco-av-pair」です。値は次の形式のストリングです。

```
protocol : attribute sep value *
```

「Protocol」は、特定の認可タイプを表すシスコの「protocol」アトリビュートです。使用可能なプロトコルには、IP、IPX、VPDN、VOIP、SHELL、RSVP、SIP、AIRNET、OUTBOUND があります。「Attribute」と「value」は、シスコの TACACS+ 仕様に定義されている適切なアトリビュート値

（AV）ペアで、「sep」は必須アトリビュートの場合には「=」、オプションのアトリビュートの場合に「*」を使用します。これにより、TACACS+ 認可で使用できるすべての機能を RADIUS にも使用できるようになります。

たとえば、次の AV ペアにより、IP を認可している間（PPP の IPCP アドレス割り当てを行っている間）、シスコの「指定された複数の IP アドレス プール」をアクティブにすることができます。

```
cisco-avpair= ”ip:addr-pool=first”
```

「*」を挿入すると、AV ペア「ip:addr-pool=first」はオプションになります。AV ペアはオプションにできることに注意してください。

```
cisco-avpair= ”ip:addr-pool*first”
```

次に、ネットワーク アクセス サーバからユーザがログインしたときに、すぐに EXEC コマンドを実行する方法の例を示します。

```
cisco-avpair= ”shell:priv-lvl=15”
```

他のベンダーには、そのベンダー固有のベンダー ID、オプション、および関連する VSA があります。ベンダー ID と VSA の詳細については、「RFC」（P.43）を参照してください。

VSA を認識および使用するようにネットワーク アクセス サーバを設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server vsa send** [**accounting** | **authentication**]
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server vsa send** [**accounting** | **authentication**] 例： Router(config)# radius-server vsa send	RADIUS IETF アトリビュート 26 の定義に従って、ネットワーク アクセス サーバが VSA を認識および使用できるようにします。
ステップ 4	**exit** 例： Router(config)# exit	特権 EXEC モードに戻ります。

RADIUS アトリビュートの詳細な一覧やベンダー固有アトリビュート 26 の詳細については、「関連資料」（P.43）を参照してください。

ベンダー固有の RADIUS サーバ通信のためのルータの設定

RADIUS のインターネット技術特別調査委員会（IETF）ドラフト規格では、ネットワーク アクセス サーバと RADIUS サーバ間でベンダー固有情報を通信するための方式を規定していますが、一部のベンダーは独自の方法で RADIUS アトリビュートを拡張しています。Cisco IOS ソフトウェアは、RADIUS のベンダー固有アトリビュートの一部をサポートしています。

前述のように、（ベンダー固有か IETF ドラフト準拠かに関係なく）RADIUS を設定するには、RADIUS サーバ デーモンを実行するホストと、シスコ デバイスと共有する秘密テキスト ストリングを指定する必要があります。RADIUS ホストと秘密テキスト ストリングを指定するには、**radius-server** コマンドを使用します。RADIUS サーバが RADIUS のベンダー固有実装を使用していることを示すには、**radius-server host non-standard** コマンドを使用します。**radius-server host non-standard** コマンドを使用しないと、ベンダー固有アトリビュートはサポートされません。

ベンダー固有の RADIUS サーバ ホストと共有秘密テキスト ストリングを指定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} **non-standard**
4. **radius-server key** {**0** *string* | **7** *string* | *string*}
5. **exit**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server host** {*hostname* | *ip-address*} **non-standard** 例： `Router(config)# radius-server host alcatraz non-standard`	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定し、RADIUS のベンダー固有実装を使用することを指定します。

	コマンド	目的
ステップ 4	**radius-server key** {**0** *string* | **7** *string* | *string*} 例： Router(config)# radius-server key myRaDIUSpassword	ルータとベンダー固有 RADIUS サーバ間に使用する共有秘密テキスト ストリングを指定します。ルータと RADIUS サーバはこのテキスト ストリングを使用してパスワードを暗号化し、応答を交換します。
ステップ 5	**exit** 例： Router(config)# exit	特権 EXEC モードに戻ります。

RADIUS サーバのスタティック ルートと IP アドレスを照会するためのルータの設定

RADIUS のベンダー固有実装の一部では、ネットワーク内にある個々のネットワーク アクセス サーバの代わりに、ユーザが RADIUS サーバのスタティック ルートおよび IP プールを定義できます。各ネットワーク アクセス サーバは、スタティック ルートと IP プール情報について RADIUS サーバに照会します。

Cisco ルータまたはアクセス サーバが最初に起動したときに、そのデバイスがスタティック ルートと IP プール定義について RADIUS サーバに照会するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server configuration-nas**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server configure-nas** 例： Router(config)# radius-server configure-nas	Cisco ルータまたはアクセス サーバが、そのドメイン内で使用するスタティック ルートと IP プール定義について RADIUS サーバに照会するように指定します。
ステップ 4	**exit** 例： Router(config)# exit	特権 EXEC モードに戻ります。

（注） **radius-server configure-nas** コマンドは Cisco ルータの起動時に実行するため、**copy system:running config nvram:startup-config** コマンドを発行するまで有効になりません。

ネットワーク アクセス サーバのポート情報を拡張するためのルータの設定

PPP またはログイン認証が、コールが着信したインターフェイスとは異なるインターフェイスで発生する場合があります。たとえば、V.120 ISDN コールの場合、ログインまたは PPP 認証は仮想非同期インターフェイス「ttt」で発生しますが、コール自体は、ISDN インターフェイスのチャネルの 1 つで発生します。

radius-server attribute nas-port extended コマンドは、RADIUS を設定して NAS-Port アトリビュート（RADIUS IETF アトリビュート 5）フィールドのサイズを 32 ビットに拡張します。NAS-Port アトリビュートの上位 16 ビットは、制御インターフェイスの種類と番号を示します。下位 16 ビットは、インターフェイスで実行中の認証を示します。

NAS-Port アトリビュート フィールドの拡張インターフェイス情報を表示するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server attribute nas-port format**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server attribute nas-port format** 例： `Router(config)# radius-server attribute nas-port format`	NAS-Port アトリビュートのサイズを 16 ビットから 32 ビットに拡張して、拡張インターフェイス情報を表示できるようにします。
ステップ 4	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。

（注） このコマンドで **radius-server extended-portnames** コマンドと **radius-server attribute nas-port extended** コマンドが置換されます。

各スロットに複数のインターフェイス（ポート）があるプラットフォームの場合、シスコ RADIUS 実装では、インターフェイスを区別できる固有の NAS-Port アトリビュートを提供しません。たとえば、デュアル PRI インターフェイスがスロット 1 にある場合、Serial1/0:1 および Serial1/1:1 のいずれも NAS-Port = 20101 と表示されます。

繰り返しになりますが、これは、RADIUS IETF の NAS-Port アトリビュートには 16 ビットのフィールド サイズ制限があるためです。この場合の解決策は、ベンダー固有アトリビュート（RADIUS IETF アトリビュート 26）で NAS-Port アトリビュートを置換することです。シスコのベンダー ID は 9 であり、Cisco-NAS-Port アトリビュートはサブタイプ 2 です。ベンダー固有アトリビュート（VSA）を有効にするには、**radius-server vsa send** コマンドを入力します。ベンダー固有アトリビュートのポート情報を提供および設定するには、**aaa nas port extended** コマンドを使用します。

NAS-Port アトリビュートを RADIUS IETF アトリビュート 26 で置換し、拡張フィールド情報を表示するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server vsa send** [**accounting** | **authentication**]
4. **aaa nas port extended**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server vsa send** [**accounting** | **authentication**] 例： `Router(config)# radius-server vsa send`	RADIUS IETF アトリビュート 26 の定義に従って、ネットワーク アクセス サーバがベンダー固有アトリビュートを認識および使用できるようにします。
ステップ 4	**aaa nas port extended** 例： `Router(config)# aaa nas port extended`	VSA NAS-Port フィールドのサイズを 16 ビットから 32 ビットに拡張して、拡張インターフェイス情報を表示できるようにします。
ステップ 5	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。

標準の NAS-Port アトリビュート（RADIUS IETF アトリビュート 5）は以降も送信されます。この情報を送信しない場合、**no radius-server attribute nas-port** コマンドを使用して停止できます。このコマンドを設定すると、標準の NAS-Port アトリビュートは送信されなくなります。

PPP の RADIUS アトリビュートと RADIUS ポートの識別については、「関連資料」（P.43）を参照してください。

AAA サーバ グループの設定

AAA サーバ グループを使用するようにルータを設定すると、既存のサーバ ホストをグループ化できます。これによって、設定したサーバ ホストのサブセットを選択し、それを特定のサービスに使用できます。サーバ グループは、グローバル サーバ ホスト リストと併せて使用されます。サーバ グループには、選択したサーバ ホストの IP アドレスが一覧表示されます。

サーバ グループには、1 台のサーバに対して複数のホスト エントリを含めることができます。エントリごとに固有の識別情報を設定します。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。つまり、この固有識別情報を使用して、ある IP アドレスに位置する 1 台のサーバ上に複数の UDP ポートが存在する場合、それぞれの UDP ポートに対して RADIUS 要求を送信できます。1 台の RADIUS サーバ上にある異なる 2 つのホスト エントリが 1 つのサービス（アカウンティングなど）に設定されている場合、設定されている 2 番めのホスト エントリは最初のホスト エントリのフェールオーバー バックアップとして動作します。この例の場合、最初のホスト エントリがアカウンティング サービスの提供に失敗すると、同じデバイスに設定されている 2 番めのホスト エントリを使用してアカウンティング サービスを提供するように、ネットワーク アクセス サーバが試行します（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

サーバ グループ名を使用してサーバ ホストを定義するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。一覧のサーバは、グローバル コンフィギュレーション モードに存在します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}]
4. **aaa group server** {**radius** | **tacacs+**} *group-name*
5. **server ip-address** [**auth-port** *port-number*] [**acct-port** *port-number*]
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] **例：** `Router(config)# radius-server host 10.45.1.2`	サーバ ホストの IP アドレスを指定および定義してから、AAA サーバ グループを設定します。**radius-server host** コマンドの詳細については、「RADIUS サーバと通信するためのルータの設定」（P.5）を参照してください。
ステップ 4	**aaa group server** {**radius** | **tacacs+**} *group-name* **例：** `Router(config-if)# aaa group server radius group1`	グループ名を使用して、AAA サーバ グループを定義します。グループのすべてのメンバは、タイプを同じにする必要があります。つまり、RADIUS または TACACS+ です。このコマンドでは、サーバ グループのサブコンフィギュレーション モードにルータを配置します。
ステップ 5	**server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] **例：** `Router(config-sg)# server 172.16.1.1 acct-port 1616`	特定の RADIUS サーバを定義済みのサーバ グループと関連付けます。セキュリティ サーバは、IP アドレスと UDP ポート番号で識別されます。 AAA サーバ グループの各 RADIUS サーバについて、この手順を繰り返します。 **（注）** グループの各サーバは、**radius-server host** コマンドを使用して事前に定義する必要があります。
ステップ 6	**end** **例：** `Router(config-sg)# end`	サーバ グループ コンフィギュレーション モードを終了します。

デッドタイムによる AAA サーバ グループの設定

サーバ名を指定してサーバ ホストを設定したら、**deadtime** コマンドを使用して、サーバ グループごとに各サーバを設定します。サーバ グループ内でデッドタイムを設定することで、AAA トラフィックを、異なる動作特性を持つ別のサーバ グループに送信できます。

デッドタイムの設定は、グローバル コンフィギュレーションに限定されなくなりました。すべてのサーバ グループの各サーバ ホストには、個別のタイマーがあります。そのため、サーバが応答せず、再送信とタイムアウトが何度も発生する場合、そのサーバは動作していない（デッド状態）と見なされます。すべてのサーバ グループの各サーバ ホストに付属するタイマーが開始されます。基本的に、タイマーがチェックされ、サーバに対する以降の要求は（デッド状態と見なされた場合）、（設定されてい

れば）代替タイマーに送信されます。ネットワーク アクセス サーバがサーバからの応答を受信すると、すべてのサーバ グループのそのサーバに関するすべての設定済みタイマー（実行中の場合）が停止されます。

タイマーが期限切れになると、タイマーが付属しているサーバだけが応答可能（アライブ状態）と見なされます。このサーバは、タイマーが属するサーバ グループを使用して後で AAA 要求のために試行できる唯一のサーバになります。

（注） 1 つのサーバが複数のタイマーを持ち、異なるデッドタイム値がサーバ グループに設定されることがあるため、同時刻の同じサーバでも複数の状態（デッドとアライブ）になる可能性があります。

（注） サーバの状態を変更するには、すべてのサーバ グループですべての設定済みタイマーを起動および終了する必要があります。

新しいタイマーと deadtime アトリビュートが追加されるため、サーバ グループのサイズはやや増えます。構造の全体的な影響は、サーバ グループの数と規模、およびその設定でサーバ グループ内でサーバを共有する方法によって変わります。

サーバ グループ内のデッドタイムを設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *group*
4. **deadtime** *minutes*
5. **end**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 1	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 1	**aaa group server radius** *group* 例： `Router(config)# aaa group server radius group1`	RADIUS タイプ サーバ グループを定義します。

	コマンド	目的
ステップ 2	**deadtime** *minutes* 例： `Router(config-sg)# deadtime 1`	デッドタイム値（分）を設定および定義します。 （注） ローカル サーバ グループのデッドタイムは、グローバル コンフィギュレーションよりも優先されます。ローカル サーバ グループ コンフィギュレーションで省略すると、値はマスター リストから継承されます。
ステップ 3	**end** 例： `Router(config-sg)# end`	サーバ グループ コンフィギュレーション モードを終了します。

AAA DNIS 認証の設定

DNIS 事前認証を使用すると、着信番号に基づいてコール設定時に事前認証を実行できます。DNIS 番号は、コールの着信時にセキュリティ サーバに直接送信されます。AAA によって認証されると、コールは許可されます。

DNIS 認証を設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa preauthorization**
4. **group** {**radius** | **tacacs+** | ***server-group***}
5. **dnis** [**password** ***string***]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa preauthorization** 例： `Router(config)# aaa preauth`	AAA 事前認証モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**group** {**radius** | **tacacs+** | *server-group*} 例： `Router(config-preauth)# group radius`	（任意）AAA 事前認証要求に使用するセキュリティ サーバを選択します。デフォルトは RADIUS です。
ステップ 5	**dnis** [**password** *string*] 例： `Router(config-preauth)# dnis password dnispass`	DNIS を使用して事前認証をイネーブルにし、必要に応じて Access-Request パケットに使用するパスワードを指定します。
ステップ 6	**end** 例： `Router(config-preauth)# end`	事前認証コンフィギュレーション モードを終了します。

DNIS に基づく AAA サーバ グループの選択の設定

Cisco IOS ソフトウェアを使用すると、Dialed Number Identification Service（DNIS; 着信番号識別サービス）番号を特定の AAA サーバ グループに割り当てることができます。これによって、サーバ グループは、その DNIS を使用して、ネットワークにダイヤルインするユーザの認証、認可、およびアカウンティングの要求を処理できます。すべての電話回線（通常の自宅電話または商用の T1/PRI 回線）を、複数の電話番号と関連付けることができます。DNIS 番号は、ユーザ宛てに発信された番号を示します。

たとえば、複数の顧客で同じ電話番号を共有する場合に、電話を受ける前に発信元を知りたいことがあります。DNIS を使用すると、応答するときに発信元の顧客がわかるため、電話に応答する方法をカスタマイズできます。

ISDN または内部モデムと接続する Cisco ルータは、DNIS 番号を受信できます。この機能を使用すると、顧客ごとに異なる RADIUS サーバ グループを割り当て可能です（つまり、DNIS 番号ごとに異なる RADIUS サーバ）。さらに、サーバ グループを使用して、複数の AAA サービスに同じサーバ グループを指定できます。また、各 AAA サービスに個別のサーバ グループを指定できます。

Cisco IOS ソフトウェアには、認証サービスとアカウンティング サービスを複数の方法で実装できる柔軟性があります。

- グローバル：AAA サービスは、グローバル コンフィギュレーション アクセス リスト コマンドを使用して定義され、特定のネットワーク アクセス サーバ上のすべてのインターフェイスに、全般的に適用されます。
- インターフェイス別：AAA サービスは、インターフェイス コンフィギュレーション コマンドを使用して定義され、特定のネットワーク アクセス サーバに設定されているインターフェイスにだけ適用されます。
- DNIS マッピング：DNIS を使用して、AAA サーバが AAA サービスを提供するように指定します。

このような複数の AAA コンフィギュレーション方式を同時に設定できるため、シスコでは、AAA サービスを提供するサーバまたはサーバ グループを決定するために、優先順位を設定しました。優先順位は次のとおりです。

- DNIS 別：DNIS を使用し、AAA サービスを提供するサーバ グループを指定/決定するようにネットワーク アクセス サーバを設定している場合、この方式の方がその他の AAA 選択方式よりも優先されます。

- インターフェイス別：サーバから AAA サービスを提供する方法を決定するために、インターフェイス別にネットワーク アクセス サーバを設定してアクセス リストを使用する場合、この方式は、他のグローバル コンフィギュレーション AAA アクセス リストよりも優先されます。
- グローバル：セキュリティ サーバが AAA サービスを提供する方法を決定するために、グローバル AAA アクセス リストを使用してネットワーク アクセス サーバを設定する場合、この方式には最も低い優先度が使用されます。

（注） DNIS に基づく AAA サーバ グループの選択を設定する前に、RADIUS サーバ ホストのリストを設定し、AAA サーバ グループを設定する必要があります。「RADIUS サーバと通信するためのルータの設定」（P.5）および「AAA サーバ グループの設定」（P.14）を参照してください。

サーバ グループの DNIS に基づいて、特定の AAA サーバ グループを選択するようにルータを設定するには、DNIS マッピングを設定します。DNIS 番号を使用して、サーバ グループをグループ名とマッピングするには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name*
4. **aaa dnis map** *dnis-number* **authorization network group** *server-group-name*
5. **aaa dnis map** ***dnis-number*** **accounting network [none | start-stop | stop-only] group** ***server-group-name***
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa dnis map enable** 例： Router(config)# aaa dnis map enable	DNIS マッピングをイネーブルにします。
ステップ 4	**aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name* 例： Router(config)# **a**aa dnis map 7777 authentication ppp group sg1	DNIS 番号を定義済みの AAA サーバ グループにマッピングします。このサーバ グループのサーバは、認証に使用されます。

	コマンドまたはアクション	目的
ステップ 5	**aaa dnis map** *dnis-number* **authorization network group** *server-group-name* 例： `Router(config)# aaa dnis map 7777 authorization network group sg1`	DNIS 番号を定義済みの AAA サーバ グループにマッピングします。このサーバ グループのサーバは、認可に使用されます。
ステップ 6	**aaa dnis map** *dnis-number* **accounting network** [**none** | **start-stop** | **stop-only**] **group** *server-group-name* 例： `Router(config)# aaa dnis map 8888 accounting network stop-only group sg2`	DNIS 番号を定義済みの AAA サーバ グループにマッピングします。このサーバ グループのサーバは、アカウンティングに使用されます。
ステップ 7	**exit** 例： `Router(config)# exit`	コンフィギュレーション モードを終了します。

AAA 事前認証の設定

サービス プロバイダーが ISDN PRI または Channel-Associated Signalling（CAS）による AAA 事前認証を使用すると、既存の RADIUS ソリューションを使用するポートの管理性が向上し、共有リソースを効率的に管理して、各種のサービスレベル 契約を提供できるようになります。ISDN PRI または CAS によって、着信コールに関する情報を Network Access Server（NAS; ネットワーク アクセス サーバ）で使用してから、コールを接続できます。使用できるコール情報は次のとおりです。

- 着信番号識別サービス（DNIS）番号（着信番号とも呼ばれます）
- Calling Line Identification（CLID; 発呼回線 ID）番号（発番号とも呼ばれます）
- コール タイプ（ベアラ機能とも呼ばれます）

この機能を使用すると、Cisco NAS は、DNIS 番号、CLID 番号、またはコール タイプに基づいて、着信コールを接続するかどうかを決定します（ISDN PRI を使用する場合、ユーザの認証と認可を行ってから、コールに応答できます。CAS を使用する場合、コールに応答する必要はありますが、事前認証に失敗した場合、コールをドロップできます）。

パブリック ネットワーク スイッチからコールを着信し、まだ接続前の場合、AAA 事前認証によって、NAS から DNIS 番号、CLID 番号、およびコール タイプを RADIUS サーバに送信し、認可を受けることができます。サーバがコールを認可すると、NAS はコールを許可します。サーバがコールを認可しない場合、NAS からパブリック ネットワーク スイッチに接続解除メッセージが送信され、コールが拒否されます。

RADIUS サーバ アプリケーションが使用不能になった場合、または応答が遅くなった場合、NAS でガード タイマーを設定できます。タイマーが期限切れになると、NAS は設定可能なパラメータを使用して、認可されなかった着信コールを許可または拒否します。

この機能は、事前認証動作を指定するために、RADIUS サーバ アプリケーションによるアトリビュート 44 の使用、および RADIUS 事前認証プロファイルに設定されている RADIUS アトリビュートの使用をサポートしています。また、これらのアトリビュートは、たとえば、以降の認証を実行するかどうか、また実行する場合、どの認証方式を使用するかを指定するためにも使用できます。

ISDN PRI および CAS による AAA 事前認証には、次の制約事項が適用されます。

- アトリビュート 44 は、事前認証またはリソース プーリングをイネーブルにした CAS コールにだけ使用できます。

- ISDN PRI では MMP を使用できません。
- AAA 事前認証を使用できるのは、Cisco AS5300、Cisco AS5400、および Cisco AS5800 プラットフォームだけです。

（注） AAA 事前認証を設定する前に、**aaa new-model** コマンドをイネーブルにし、サポートする事前認証アプリケーションが使用ネットワークの RADIUS サーバで実行されている必要があります。

AAA 事前認証を設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa preauthorization**
4. **clid** [**if-avail** | **required**] [**accept-stop**] [**password** ***string***]
5. **ctype** [**if-avail** | **required**] [**accept-stop**] [**password** ***string***]
6. **dnis** [**if-avail** | **required**] [**accept-stop**] [**password** ***string***]
7. **dnis bypass** {***dnis-group-name***}
8. **exit**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa preauthorization** 例： Router(config)# aaa preauth	AAA 事前認証コンフィギュレーション モードを開始します。
ステップ 4	**group** *server-group* 例： Router(config-preauth)# group sg2	事前認証に使用する AAA RADIUS サーバ グループを指定します。
ステップ 5	**clid** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] 例： Router(config-preauth)# clid required	CLID 番号に基づいて、コールを事前認証します。

	コマンド	目的
ステップ 6	**ctype** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] 例： Router(config-preauth)# ctype required	コール タイプに基づいて、コールを事前認証します。
ステップ 7	**dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] 例： Router(config-preauth)# dnis required	DNIS 番号に基づいて、コールを事前認証します。
ステップ 8	**dnis bypass** {*dnis-group-name*} 例： Router(config-preauth)# dnis bypass hawaii	事前認証をバイパスする DNIS 番号のグループを指定します。
ステップ 9	**end** 例： Router(config-preauth)# end	事前認証コンフィギュレーション モードを終了します。

DNIS 事前認証を設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa preauthorization**
4. **group** {**radius** | **tacacs+** | ***server-group***}
5. **dnis** [**password** ***string***]
6. **end**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa preauthorization** 例： Router(config)# aaa preauth	AAA 事前認証モードを開始します。

	コマンド	目的
ステップ 4	**group** {**radius** | **tacacs+** | *server-group*} 例： `Router(config-preauth)# group radius`	（任意）AAA 事前認証要求に使用するセキュリティ サーバを選択します。デフォルトは RADIUS です。
ステップ 5	**dnis** [**password** *string*] 例： `Router(config-preauth)# dnis password dnispass`	DNIS を使用して事前認証をイネーブルにし、必要に応じて Access-Request パケットに使用するパスワードを指定します。
ステップ 6	**end** 例： `Router(config-preauth)# end`	事前認証コンフィギュレーション モードを終了します。

Cisco ルータで事前認証を設定するだけでなく、RADIUS サーバでも事前認証プロファイルを設定する必要があります。事前認証プロファイルの設定については、次の項を参照してください。

- 「DNIS または CLID 事前認証の RADIUS プロファイルの設定」（P.23）
- 「コール タイプ事前認証の RADIUS プロファイルの設定」（P.23）
- 「コールバックのために事前認証を強化する RADIUS プロファイルの設定」（P.24）
- 「大規模なダイヤルアウトに使用されるリモート ホスト名の RADIUS プロファイルの設定」（P.24）
- 「モデム管理のための RADIUS プロファイルの設定」（P.25）
- 「後続の認証のための RADIUS の設定」（P.25）
- 「後続の認証タイプのための RADIUS の設定」（P.26）
- 「ユーザ名を含めるための RADIUS プロファイルの設定」（P.26）
- 「双方向認証のための RADIUS プロファイルの設定」（P.26）
- 「認可をサポートするための RADIUS プロファイルの設定」（P.27）

DNIS または CLID 事前認証の RADIUS プロファイルの設定

RADIUS 事前認証プロファイルを設定するには、DNIS または CLID 番号をユーザ名として使用し、**dnis** または **clid** コマンドで定義したパスワードをパスワードとして使用します。

（注） 事前認証プロファイルのサービス タイプは必ず「outbound」です。これは、パスワードが NAS で事前定義されているためです。この方法で事前認証プロファイルを設定することで、DNIS 番号、CLID 番号、またはコール タイプのユーザ名と、わかりやすいパスワードを使用してユーザが NAS にログインする操作を回避できます。「outbound」サービス タイプは、RADIUS サーバに送信される access-request パケットにも含まれます。

コール タイプ事前認証の RADIUS プロファイルの設定

RADIUS 事前認証プロファイルを設定するには、コール タイプ ストリングをユーザ名として使用し、**ctype** コマンドで定義したパスワードをパスワードとして使用します。次の表に、事前認証プロファイルで使用できるコール タイプ ストリングを示します。

コール タイプ ストリング	ISDN ベアラ機能
digital	無制限のデジタル、制限付きのデジタル。
speech	音声、3.1 kHz オーディオ、7 kHz オーディオ。 （注） これは CAS にだけ使用できるコール タイプです。
v.110	V.110 ユーザ情報レイヤがある任意のコール。
v.120	V.120 ユーザ情報レイヤがある任意のコール。

（注） 事前認証プロファイルのサービス タイプは必ず「outbound」です。これは、パスワードが NAS で事前定義されているためです。この方法で事前認証プロファイルを設定することで、DNIS 番号、CLID 番号、またはコール タイプのユーザ名と、わかりやすいパスワードを使用してユーザが NAS にログインする操作を回避できます。「outbound」サービス タイプは、RADIUS サーバに送信された access-request パケットにも含まれます。また、RADIUS サーバがチェックイン アイテムをサポートする場合、チェックイン アイテムにする必要があります。

コールバックのために事前認証を強化する RADIUS プロファイルの設定

在宅勤務者などのリモート ネットワーク ユーザは、コールバックを使用すると課金を受けずに NAS にダイヤルインできます。コールバックが必要な場合、NAS は現在のコールを終了し、発信元にコールバックします。NAS がコールバックを実行すると、発信接続の情報だけが適用されます。事前認証の access-accept メッセージのその他のアトリビュートは破棄されます。

（注） RADIUS サーバからのコールバックに宛先の IP アドレスは必要ありません。

次に、コールバック番号が 555-1111 でサービス タイプが outbound に設定された RADIUS プロファイル設定の例を示します。cisco-avpair = "preauth:send-name=<string>" は文字列 "andy" を使用し、cisco-avpair = "preauth:send-secret=<string>" はパスワード "cisco" を使用します。

```
5551111 password = ”cisco”, Service-Type = Outbound
    Service-Type = Callback-Framed
    Framed-Protocol = PPP,
    Dialback-No = ”5551212”
    Class = ”ISP12”
    cisco-avpair = ”preauth:send-name=andy”
    cisco-avpair = ”preauth:send-secret=cisco”
```

大規模なダイヤルアウトに使用されるリモート ホスト名の RADIUS プロファイルの設定

次に、前の例に処理を追加して、発信先の番号は有効でもアクセス先のルータが間違っている発信を回避するために、リモートの名前を提供する例を示します。この例は大規模なダイヤルアウトに適しています。

```
5551111 password = "cisco", Service-Type = Outbound
       Service-Type = Callback-Framed
       Framed-Protocol = PPP,
       Dialback-No = "5551212"
       Class = "ISP12"
```

```
cisco-avpair = "preauth:send-name=andy"
cisco-avpair = "preauth:send-secret=cisco"
cisco-avpair = "preauth:remote-name=Router2"
```

モデム管理のための RADIUS プロファイルの設定

DNIS、CLID、またはコール タイプの事前認証を使用する場合、NAS の RADIUS サーバからの肯定応答には、ベンダー固有アトリビュート（VSA）26 を介して、モデム管理のモデム ストリングを含めることができます。モデム管理 VSA の構文は次のとおりです。

```
cisco-avpair = "preauth:modem-service=modem min-speed <x> max-speed <y>
modulation <z> error-correction <a> compression <b>"
```

VSA のモデム管理ストリングには、次の内容を含めることができます。

コマンド	引数
min-speed	<300 ～ 56000>、any
max-speed	<300 ～ 56000>、any
modulation	K56Flex、v22bis、v32bis、v34、v90、any
error-correction	lapm、mnp4
compression	mnp5、v42bis

VSA の形式で RADIUS からモデム管理ストリングを受信すると、その情報は Cisco IOS ソフトウェアに渡され、コールごとに適用されます。Modem ISDN Channel Aggregation（MICA）モデムには、コール設定時にメッセージを送信できるコントロール チャネルがあります。そのため、このモデム管理機能をサポートするのは、MICA モデムや新しいテクノロジーだけです。この機能は Microcom モデムではサポートされません。

モデム管理の詳細については、「関連資料」（P.43）を参照してください。

後続の認証のための RADIUS の設定

事前認証に成功すると、事前認証の RADIUS ベンダー固有アトリビュート 201（Require-Auth）を使用して、後続の認証を実行するかどうかを決定できます。access-accept メッセージで返されるアトリビュート 201 の値が 0 の場合、後続の認証は実行されません。アトリビュート 201 の値が 1 の場合、後続の認証は通常どおり実行されます。

アトリビュート 201 の構文は次のとおりです。

```
cisco-avpair = "preauth:auth-required=<n>"
```

この <*n*> は、アトリビュート 201（つまり 0 または 1）と同じ値の範囲です。

事前認証プロファイルにアトリビュート 201 が含まれない場合、値 1 と仮定され、後続の認証が実行されます。

（注） 後続の認証を実行するには、事前認証プロファイルに加え、通常のユーザ プロファイルを設定する必要があります。

後続の認証タイプのための RADIUS の設定

事前認証プロファイルに後続の認証を指定した場合、後続の認証に使用する認証タイプも指定する必要があります。後続の認証で使用できる認証タイプを指定するには、次の VSA を使用します。

```
cisco-avpair = ”preauth:auth-type=<string>”
```

この *<string>* には、次のいずれかを指定できます。

ストリング	説明
chap	PPP 認証の CHAP のユーザ名とパスワードが必要です。
ms-chap	PPP 認証の MS-CHAP のユーザ名とパスワードが必要です。
pap	PPP 認証の PAP のユーザ名とパスワードが必要です。

複数の認証タイプを許可するように指定するには、事前認証プロファイルでこの VSA の複数インスタンスを設定できます。事前認証プロファイルに指定する認証タイプ VSA の順序は、PPP ネゴシエーションに使用する認証タイプの順序にもなるため、重要です。

この VSA はユーザ別のアトリビュートであり、**ppp authentication** インターフェイス コマンドで指定した認証タイプ リストは置換されます。

（注） これは後続の認証用の認証タイプを指定する VSA なので、後続の認証が必要な場合にだけ使用してください。

ユーザ名を含めるための RADIUS プロファイルの設定

コールの認証に事前認証のみを使用する場合、発信するときに NAS がユーザ名を見つけられない可能性があります。RADIUS は、NAS が RADIUS アトリビュート 1（User-Name）または access-accept パケットで返される VSA を介して使用できるユーザ名を提供します。ユーザ名を指定する VSA の構文は次のとおりです。

```
cisco-avpair = ”preauth:username=<string>”
```

ユーザ名を指定しない場合、DNIS 番号、CLID 番号、またはコール タイプが使用されます。これは、設定した最後の事前認証コマンドによって変わります（たとえば、**clid** が最後に設定された事前認証コマンドの場合、CLID 番号がユーザ名として使用されます）。

後続の認証を使用してコールを認証する場合、2 つのユーザ名が存在する可能性があります。RADIUS から提供されたユーザ名と、ユーザが指定したユーザ名です。この場合、ユーザが指定したユーザ名の方が、RADIUS 事前認証プロファイルに含まれるユーザ名よりも優先されます。ユーザが指定したユーザ名は、認証とアカウンティングの両方に使用されます。

双方向認証のための RADIUS プロファイルの設定

双方向認証の場合、発信側ネットワーク デバイスが NAS を認証する必要があります。Password Authentication Protocol（PAP; パスワード認証プロトコル）のユーザ名とパスワード、または Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）のユーザ名とパスワードを NAS のローカルで設定する必要はありません。代わりに、事前認証の access-accept メッセージにユーザ名とパスワードを含めることができます。

（注） **ppp authentication** コマンドを **radius** 方式とともに設定する必要があります。

PAP に適用する場合は、インターフェイス上で **ppp pap sent-name password** コマンドを設定しないでください。Vendor-Specific Attributes（VSA; ベンダー固有アトリビュート）の場合は、アウトバウンド認証の PAP ユーザ名および PAP パスワードとして、「preauth:send-name」および「preauth:send-secret」が使用されます。

CHAP の場合、「preauth:send-name」はアウトバウンド認証だけでなく、インバウンド認証にも使用されます。CHAP インバウンドの場合、NAS は、発信側ネットワーキング デバイスに対するチャレンジ パケットで「preauth:send-name」に定義されている名前を使用します。CHAP アウトバウンドの場合、「preauth:send-name」と「preauth:send-secret」の両方が応答パケットに使用されます。

次に、双方向認証を指定する設定の例を示します。

```
5551111 password = "cisco", Service-Type = Outbound
    Service-Type = Framed-User
    cisco-avpair = "preauth:auth-required=1"
    cisco-avpair = "preauth:auth-type=pap"
    cisco-avpair = "preauth:send-name=andy"
    cisco-avpair = "preauth:send-secret=cisco"
    class = "<some class>"
```

（注） リソース プーリングをイネーブルにする場合、双方向認証は機能しません。

認可をサポートするための RADIUS プロファイルの設定

事前認証だけを設定する場合、後続の認証はバイパスされます。ユーザ名とパスワードを使用できないため、認可もバイパスされます。ただし、事前認証プロファイルに authorization アトリビュートを含めてユーザ別のアトリビュートを適用することで、認可のために後で RADIUS に処理を戻す必要がなくなります。認可プロセスを開始するには、NAS で **aaa authorization network** コマンドも設定する必要があります。

事前認証プロファイルに authorization アトリビュートを設定できますが、service-type アトリビュート（アトリビュート 6）という 1 つの例外があります。service-type アトリビュートは、事前認証プロファイルで VSA に変換する必要があります。この VSA の構文は次のとおりです。

```
cisco-avpair = "preauth:service-type=<n>"
```

この <*n*> は、アトリビュート 6 に関する標準の RFC 2865 値の 1 つです。使用できる Service-Type 値については、「関連資料」（P.43）を参照してください。

（注） 後続の認証が必要な場合、事前認証プロファイルの authorization アトリビュートは適用されません。

ガード タイマーの設定

事前認証要求および認可要求の応答時間はさまざまなので、ガード タイマーを使用してコールの処理を制御できます。ガード タイマーは、DNIS が RADIUS サーバに送信されると開始されます。ガード タイマーが期限切れになる前に NAS が AAA から応答を受信しない場合、タイマーの設定に基づいてコールを許可または拒否します。

RADIUS サーバが認証要求または事前認証要求に応答できなかった場合にコールを許可または拒否できるガード タイマーを設定するには、次のコマンドのいずれかを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **isdn guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}]
5. **call guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}]
6. **end**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface serial1/0/0:23`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**isdn guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}] 例： `Router(config-if)# isdn guard-timer 8000 on-expiry reject`	RADIUS サーバが事前認証要求に応答できなかった場合にコールを許可または拒否できる ISDN ガード タイマーを設定します。
ステップ 5	**call guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}] 例： `Router(config-if)# call guard-timer 2000 on-expiry accept`	RADIUS サーバが事前認証要求に応答できなかった場合にコールを許可または拒否できる CAS ガード タイマーを設定します。
ステップ 6	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了します。

RADIUS 認証の指定

RADIUS サーバを指定し、RADIUS 認証キーを定義した後は、RADIUS 認証の方式リストを定義する必要があります。AAA によって RADIUS 認証が容易になるため、**aaa authentication** コマンドを入力し、認証方式として RADIUS を指定する必要があります。詳細については、「関連資料」（P.43）を参照してください。

RADIUS 認可の指定

AAA 認可を使用すると、ユーザのアクセスをそのネットワークに制限するパラメータを設定できます。RADIUS を使用する認可は、ワンタイム認可やサービスごとの認可を含むリモート アクセス コントロール用の方式が 1 つ、ユーザ別のアカウント リストおよびプロファイル、ユーザ グループのサポート、IP、IPX、ARA、および Telnet のサポートを備えています。AAA によって RADIUS 認可は容易になるため、認証方式として RADIUS を指定して、**aaa authorization** コマンドを発行する必要があります。詳細については、「認可の設定」の章を参照してください。

RADIUS アカウンティングの指定

AAA アカウンティング機能を使用すると、ユーザがアクセスしているサービスや、ユーザが消費しているネットワーク リソース量を追跡できます。AAA によって RADIUS アカウンティングは容易になるため、アカウンティング方式として RADIUS を指定して、**aaa accounting** コマンドを発行する必要があります。詳細については、「アカウンティングの設定」の章を参照してください。

RADIUS Login-IP-Host の設定

ネットワーク アクセス サーバが、ダイヤルイン ユーザに対する接続を試行するときに複数のログインホストを試行できるようにするには、RADIUS サーバのユーザ プロファイルに 3 つの Login-IP-Host エントリを入力できます。次に、ユーザ *joeuser* 用に 3 つの Login-IP-Host インスタンスを設定し、接続に TCP-Clear を使用する例を示します。

```
joeuser       Password = xyz
        Service-Type = Login,
        Login-Service = TCP-Clear,
        Login-IP-Host = 10.0.0.0,
        Login-IP-Host = 10.2.2.2,
        Login-IP-Host = 10.255.255.255,
        Login-TCP-Port = 23
```

ホストの入力順は、試行される順序になります。**ip tcp synwait-time** コマンドを使用して、ネットワーク アクセス サーバがリストの次ホストに対して接続を試行するまで待機する秒数を設定します。デフォルトは 30 秒です。

使用している RADIUS サーバが 4 つ以上の Login-IP-Host エントリを許可していても、ネットワーク アクセス サーバが access-accept パケットでサポートするのは 3 ホストだけです。

RADIUS プロンプトの設定

access-challenge パケットに対するユーザの応答を画面にエコーするかどうかを制御するには、RADIUS サーバのユーザ プロファイルで Prompt アトリビュートを設定します。このアトリビュートは、access-challenge パケットにだけ含まれます。次に、No-Echo に設定された Prompt アトリビュートの例を示します。この設定で、ユーザの応答はエコーされません。

```
joeuser Password = xyz
Service-Type = Login,
Login-Service = Telnet,
Prompt = No-Echo,
Login-IP-Host = 172.31.255.255
```

ユーザの応答をエコーするには、このアトリビュートを Echo に設定します。Prompt アトリビュートをユーザ プロファイルに含めない場合、デフォルトで応答はエコーされま。

このアトリビュートは、アクセス サーバに設定されている **radius-server challenge-noecho** コマンドの動作よりも優先されます。たとえば、アクセス サーバがエコーを表示しないように設定され、個人のユーザ プロファイルではエコーを許可している場合、ユーザ応答はエコーされます。

（注） Prompt アトリビュートを使用するには、access-challenge パケットをサポートするように RADIUS サーバを設定します。

RADIUS アクセス要求のサフィックスとパスワードの設定

大規模なダイヤルアウトでは、すべての宛先の各 NAS でダイヤラ マップを設定する必要はありません。代わりに、AAA サーバで、発信コール アトリビュートを含むリモート サイト プロファイルを作成できます。パケット トラフィックによって、コールをリモート サイトに配置する必要がある場合、NAS によって プロファイルがダウンロードされます。

RADIUS に対する access-request メッセージでユーザ名を設定できます。「-out」というユーザ名のデフォルトのサフィックスが、ユーザ名に付加されます。ユーザ名アトリビュートを構成する形式は、IP アドレスと設定したサフィックスです。

大規模なダイヤルアウトの場合にユーザ名の設定機能を提供するには、**dialer aaa** コマンドを新しい **suffix** および **password** キーワードを指定して実装します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa route download** *min*
5. **aaa authorization configuration default**
6. **interface dialer** *number*
7. **dialer aaa**
8. **dialer aaa suffix** *suffix* **password** *password*
9. **exit**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**aaa new-model** 例： `Router(config)# aaa new-model`	AAA アクセス コントロール モデルをイネーブルにします。
ステップ 4	**aaa route download** *min* 例： `Router(config)# aaa route download 450`	ダウンロードのスタティック ルート機能をイネーブルにし、ダウンロードの間隔を設定します。
ステップ 5	**aaa authorization configuration default** 例： `Router(config)# aaa authorization configuration default`	TACACS+ または RADIUS を使用して AAA サーバからスタティック ルート設定情報をダウンロードします。
ステップ 6	**interface dialer** *number* 例： `Router(config)# interface dialer 1`	ダイヤラ ロータリー グループを定義します。
ステップ 7	**dialer aaa** 例： `Router(config-if)# dialer aaa`	ダイヤラがダイヤル情報のために AAA サーバにアクセスすることを許可します。
ステップ 8	**dialer aaa suffix** *suffix* **password** *password* 例： `Router(config-if)# dialer aaa suffix @samp password password12`	ダイヤラがダイヤル情報のために AAA サーバにアクセスすることを許可し、認証に使用するサフィックスとデフォルト以外のパスワードを指定します。
ステップ 9	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

RADIUS のモニタリングとメンテナンス

RADIUS をモニタおよび保守するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **debug radius**
3. **show radius statistics**
4. **exit**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**debug radius** **例：** `Router# debug radius`	RADIUS 関連の情報を表示します。
ステップ 3	**show radius statistics** **例：** `Router# show radius statistics`	アカウンティング パケットと認証パケットについての RADIUS 統計情報を示します。
ステップ 4	**exit** **例：** `Router# exit`	ルータ セッションを終了します。

RADIUS の設定例

ここでは、RADIUS 設定の例を紹介します。

例：RADIUS の認証と認可

次に、RADIUS を使用して認証および認可を行うようにルータを設定する例を示します。

```
aaa authentication login use-radius group radius local
aaa authentication ppp user-radius if-needed group radius
```

```
aaa authorization exec default group radius
aaa authorization network default group radius
```

この RADIUS 認証および認可設定のサンプル行は、次のように定義されます。

- **aaa authentication login use-radius group radius local** コマンドを実行すると、ルータは、ログイン プロンプトで認証に RADIUS を使用するように設定されます。RADIUS がエラーを返すと、ユーザはローカル データベースを使用して認証されます。この例では、**use-radius** は方式リストの名前であり、RADIUS を指定し、ローカル認証を指定します。
- **aaa authentication ppp user-radius if-needed group radius** コマンドで、ユーザがまだ認可されていない場合に、CHAP または PAP による PPP を使用する回線に RADIUS 認証を使用するように、Cisco IOS ソフトウェアを設定します。EXEC ファシリティによってユーザが認証済みの場合、RADIUS 認証は実行されません。この例では、**user-radius** は、if-needed 認証方式として RADIUS を定義する方式リストの名前です。
- **aaa authorization exec default group radius** コマンドで、EXEC 認可、autocommand、およびアクセス リストに使用する RADIUS 情報を設定します。
- **aaa authorization network default group radius** コマンドを実行すると、ネットワーク認可、アドレス割り当て、および他のアクセス リストについて RADIUS が設定されます。

例：RADIUS 認証、認可、およびアカウンティング

次に、AAA コマンドを設定して RADIUS を使用する一般的な設定例を示します。

```
radius-server host 10.45.1.2
radius-server key myRaDiUSpassWoRd
username root password ALongPassword
aaa authentication ppp dialins group radius local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa authentication login admins local
aaa authorization exec default local
line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem ri-is-cd
interface group-async 1
 encaps ppp
 ppp authentication pap dialins
```

この例の RADIUS 認証、認可、およびアカウンティングの回線は、次のように定義されます。

- **radius-server host** コマンドは RADIUS サーバ ホストの IP アドレスを定義します。
- **radius-server key** コマンドはネットワーク アクセス サーバと RADIUS サーバ ホスト間の共有秘密テキスト ストリングを定義します。
- **aaa authentication ppp dialins group radius local** コマンドで、RADIUS 認証を示す認証方式リスト「dialins」を定義します。次に、（RADIUS サーバが応答しない場合）PPP を使用するシリアル回線にはローカル認証が使用されます。
- **ppp authentication pap dialins** コマンドは「dialins」方式リストを指定した回線に適用します。
- **aaa authorization network default group radius local** コマンドは、アドレスと他のネットワークパラメータを RADIUS ユーザに割り当てるために使用されます。
- **aaa accounting network default start-stop group radius** コマンドで、PPP の使用状況を追跡します。

- **aaa authentication login admins local** コマンドは、ログイン認証の別の方式リスト「admins」を定義します。
- **login authentication admins** コマンドは、ログイン認証の「admins」方式リストを適用します。

例：ベンダー固有の RADIUS 設定

次に、AAA コマンドを設定してベンダー固有の RADIUS を使用する一般的な設定例を示します。

```
radius-server host alcatraz non-standard
radius-server key myRaDiUSpassWoRd
radius-server configure-nas
username root password ALongPassword
aaa authentication ppp dialins group radius local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa authentication login admins local
aaa authorization exec default local
line 1 16
autoselect ppp
autoselect during-login
login authentication admins
modem ri-is-cd
interface group-async 1
encaps ppp
ppp authentication pap dialins
```

この例の RADIUS 認証、認可、およびアカウンティングの回線は、次のように定義されます。

- **radius-server host non-standard** コマンドで、RADIUS サーバ ホストの名前を定義し、この RADIUS ホストがベンダー固有バージョンの RADIUS を使用することを指定します。
- **radius-server key** コマンドはネットワーク アクセス サーバと RADIUS サーバ ホスト間の共有秘密テキスト ストリングを定義します。
- **radius-server configure-nas** コマンドは、デバイスが最初に起動したときに、Cisco ルータまたはアクセス サーバがスタティック ルートと IP プール定義について RADIUS サーバに照会するように定義します。
- **aaa authentication ppp dialins group radius local** コマンドで、RADIUS 認証を示す認証方式リスト「dialins」を定義します。次に、（RADIUS サーバが応答しない場合）PPP を使用するシリアル回線にはローカル認証が使用されます。
- **ppp authentication pap dialins** コマンドは「dialins」方式リストを指定した回線に適用します。
- **aaa authorization network default group radius local** コマンドは、アドレスと他のネットワークパラメータを RADIUS ユーザに割り当てるために使用されます。
- **aaa accounting network default start-stop group radius** コマンドで、PPP の使用状況を追跡します。
- **aaa authentication login admins local** コマンドは、ログイン認証の別の方式リスト「admins」を定義します。
- **login authentication admins** コマンドは、ログイン認証の「admins」方式リストを適用します。

例：サーバ固有の値を指定した RADIUS サーバ

次に、172.31.39.46 という IP アドレスの RADIUS サーバについて、サーバ固有のタイムアウト、再送信、およびキー値を設定する例を示します。

```
radius-server host 172.31.39.46 timeout 6 retransmit 5 key rad123
```

例：グローバル値とサーバ固有の値を指定した複数の RADIUS サーバ

次に、固有のタイムアウト、再送信、およびキー値を指定した 2 つの RADIUS サーバを設定する例を示します。この例では、**aaa new-model** コマンドを使用してルータ上の AAA サービスをイネーブルにし、特定の AAA コマンドで AAA サービスを定義します。**radius-server retransmit** コマンドで、すべての RADIUS サーバについて、グローバル再送信値を 4 に変更します。**radius-server host** コマンドで、IP アドレスが 172.16.1.1 と 172.29.39.46 の RADIUS サーバ ホストについて、特定のタイムアウト、再送信、およびキー値を設定します。

```
! Enable AAA services on the router and define those services.
aaa new-model
aaa authentication login default group radius
aaa authentication login console-login none
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
enable password tryit1
!
! Change the global retransmission value for all RADIUS servers.
radius-server retransmit 4
!
! Configure per-server specific timeout, retransmission, and key values.
! Change the default auth-port and acct-port values.
radius-server host 172.16.1.1 auth-port 1612 acct-port 1616 timeout 3 retransmit 3 key
radkey
!
! Configure per-server specific timeout and key values. This server uses the global
! retransmission value.
radius-server host 172.29.39.46 timeout 6 key rad123
```

例：同じサーバ IP アドレスを持つ複数の RADIUS サーバ エントリ

次に、同じ IP アドレスを持つ複数の RADIUS ホスト エントリを認識するように、ネットワーク アクセス サーバを設定する例を示します。同じ RADIUS サーバ上にある 2 つのホスト エントリは、同じサービス（認証とアカウンティング）のために設定されています。設定されている 2 番めのホスト エントリは、1 番めのエントリのフェールオーバー バックアップとして動作します（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group radius
! The next set of commands configures multiple host entries for the same IP address.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 2000 acct-port 2000
```

例：RADIUS サーバ グループ

次に、3 つの RADIUS サーバ メンバを持ち、各メンバがデフォルトの認証ポート（1645）とアカウンティング ポート（1646）を使用するサーバ グループ *radgroup1* を作成する例を示します。

```
aaa group server radius radgroup1
 server 172.16.1.11
```

```
 server 172.17.1.21
 server 172.18.1.31
```

次に、3 つの RADIUS サーバ メンバを持ち、各メンバは IP アドレスは同じでも認証ポートとアカウンティング ポートはそれぞれ異なるサーバ グループ *radgroup2* を作成する例を示します。

```
aaa group server radius radgroup2
 server 172.16.1.1 auth-port 1000 acct-port 1001
 server 172.16.1.1 auth-port 2000 acct-port 2001
 server 172.16.1.1 auth-port 3000 acct-port 3001
```

例：AAA サーバ グループを使用する複数の RADIUS サーバ エントリ

次に、2 つの RADIUS サーバ グループを認識するようにネットワーク アクセス サーバを設定する例を示します。一方のグループである group1 には、同じ RADIUS サーバ上に同じサービス用に設定された 2 つのホスト エントリがあります。設定されている 2 番めのホスト エントリは、1 番めのエントリのフェールオーバー バックアップとして動作します 各グループのデッドタイムは個々に設定されています。group 1 のデッドタイムは 1 分で、group 2 のデッドタイムは 2 分です。

（注） グローバル コマンドとサーバ コマンドの両方を使用する場合、サーバ コマンドの方がグローバル コマンドよりも優先されます。

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group group1
! The following commands define the group1 RADIUS server group and associate servers
! with it and configures a deadtime of one minute.
aaa group server radius group1
 server 10.1.1.1 auth-port 1645 acct-port 1646
 server 10.2.2.2 auth-port 2000 acct-port 2001
 deadtime 1
! The following commands define the group2 RADIUS server group and associate servers
! with it and configures a deadtime of two minutes.
aaa group server radius group2
 server 10.2.2.2 auth-port 2000 acct-port 2001
 server 10.3.3.3 auth-port 1645 acct-port 1646
 deadtime 2
! The following set of commands configures the RADIUS attributes for each host entry
! associated with one of the defined server groups.
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server host 10.2.2.2 auth-port 2000 acct-port 2001
radius-server host 10.3.3.3 auth-port 1645 acct-port 1646
```

例：DNIS に基づく AAA サーバ グループの選択

次に、特定の AAA サービスを提供するために、DNIS に基づいて RADIUS サーバ グループを選択する例を示します。

```
! This command enables AAA.
aaa new-model
!
! The following set of commands configures the RADIUS attributes for each server
! that will be associated with one of the defined server groups.
radius-server host 172.16.0.1 auth-port 1645 acct-port 1646 key cisco1
radius-server host 172.17.0.1 auth-port 1645 acct-port 1646 key cisco2
radius-server host 172.18.0.1 auth-port 1645 acct-port 1646 key cisco3
```

```
radius-server host 172.19.0.1 auth-port 1645 acct-port 1646 key cisco4
radius-server host 172.20.0.1 auth-port 1645 acct-port 1646 key cisco5

! The following commands define the sg1 RADIUS server group and associate servers
! with it.
aaa group server radius sg1
  server 172.16.0.1
  server 172.17.0.1
! The following commands define the sg2 RADIUS server group and associate a server
! with it.
aaa group server radius sg2
  server 172.18.0.1
! The following commands define the sg3 RADIUS server group and associate a server
! with it.
aaa group server radius sg3
  server 172.19.0.1
! The following commands define the default-group RADIUS server group and associate
! a server with it.
aaa group server radius default-group
  server 172.20.0.1

! The next set of commands configures default-group RADIUS server group parameters.
aaa authentication ppp default group default-group
aaa accounting network default start-stop group default-group
!
! The next set of commands enables DNIS mapping and maps DNIS numbers to the defined
! RADIUS server groups. In this configuration, all PPP connection requests using
! DNIS 7777 are sent to the sg1 server group. The accounting records for these
! connections (specifically, start-stop records) are handled by the sg2 server group.
! Calls with a DNIS of 8888 use server group sg3 for authentication and server group
! default-group for accounting. Calls with a DNIS of 9999 use server group
! default-group for authentication and server group sg3 for accounting records
! (stop records only). All other calls with DNIS other than the ones defined use the
! server group default-group for both authentication and stop-start accounting records.
aaa dnis map enable
aaa dnis map 7777 authentication ppp group sg1
aaa dnis map 7777 accounting network start-stop group sg2
aaa dnis map 8888 authentication ppp group sg3
aaa dnis map 9999 accounting network stop-only group sg3
```

例：AAA 事前認証

次に、事前認証に DNIS 番号を指定するという単純な設定の例を示します。

```
aaa preauth
 group radius
 dnis required
```

次に、事前認証に DNIS 番号と CLID 番号の両方を使用する設定の例を示します。DNIS 事前認証が先に実行され、次に CLID 事前認証が実行されます。

```
aaa preauth
 group radius
 dnis required
 clid required
```

次に、「hawaii」という DNIS グループに指定されている 2 つの DNIS 番号を除き、すべての DNIS 番号について事前認証を実行することを指定する例を示します。

```
aaa preauth
 group radius
 dnis required
```

```
 dnis bypass hawaii

dialer dnis group hawaii
 number 12345
 number 12346
```

次に、DNIS 事前認証を使用する AAA 設定の例を示します。

```
aaa new-model
aaa authentication login CONSOLE none
aaa authentication login RADIUS_LIST group radius
aaa authentication login TAC_PLUS group tacacs+ enable
aaa authentication login V.120 none
aaa authentication enable default enable group tacacs+
aaa authentication ppp RADIUS_LIST if-needed group radius
aaa authorization exec RADIUS_LIST group radius if-authenticated
aaa authorization exec V.120 none
aaa authorization network default group radius if-authenticated
aaa authorization network RADIUS_LIST if-authenticated group radius
aaa authorization network V.120 group radius if-authenticated
aaa accounting suppress null-username
aaa accounting exec default start-stop group radius
aaa accounting commands 0 default start-stop group radius
aaa accounting network default start-stop group radius
aaa accounting connection default start-stop group radius
aaa accounting system default start-stop group radius
aaa preauth
 dnis password Cisco-DNIS
aaa nas port extended
!
radius-server configure-nas
radius-server host 10.0.0.0 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.255.255.255 auth-port 1645 acct-port 1646 non-standard
radius-server retransmit 2
radius-server deadtime 1
radius-server attribute nas-port format c
radius-server unique-ident 18
radius-server key MyKey
```

（注） 事前認証を設定するには、RADIUS サーバでも事前認証プロファイルを設定する必要があります。

例：RADIUS トンネリング アトリビュートを指定した RADIUS ユーザ プロファイル

次に、RADIUS トンネリング アトリビュートを含む RADIUS ユーザ プロファイル（Merit Daemon 形式）の例を示します。このエントリは 2 つのトンネルをサポートします。1 つは L2F 用、もう 1 つは L2TP 用です。:1 が指定されたタグ エントリは L2F トンネルをサポートし、:2 が指定されたタグ エントリは L2TP トンネルをサポートします。

```
cisco.com Password = "cisco", Service-Type = Outbound
    Service-Type = Outbound,
    Tunnel-Type = :1:L2F,
    Tunnel-Medium-Type = :1:IP,
    Tunnel-Client-Endpoint = :1:"10.0.0.2",
    Tunnel-Server-Endpoint = :1:"10.0.0.3",
    Tunnel-Client-Auth-Id = :1:"l2f-cli-auth-id",
    Tunnel-Server-Auth-Id = :1:"l2f-svr-auth-id",
    Tunnel-Assignment-Id = :1:"l2f-assignment-id",
```

```
Cisco-Avpair = "vpdn:nas-password=l2f-cli-pass",
Cisco-Avpair = "vpdn:gw-password=l2f-svr-pass",
Tunnel-Preference = :1:1,
Tunnel-Type = :2:L2TP,
Tunnel-Medium-Type = :2:IP,
Tunnel-Client-Endpoint = :2:"10.0.0.2",
Tunnel-Server-Endpoint = :2:"10.0.0.3",
Tunnel-Client-Auth-Id = :2:"l2tp-cli-auth-id",
Tunnel-Server-Auth-Id = :2:"l2tp-svr-auth-id",
Tunnel-Assignment-Id = :2:"l2tp-assignment-id",
Cisco-Avpair = "vpdn:l2tp-tunnel-password=l2tp-tnl-pass",
Tunnel-Preference = :2:2
```

例：ガード タイマー

次に、8,000 ミリ秒に設定された ISDN ガード タイマーの例を示します。事前認証要求に対して RADIUS サーバが応答しないまま、タイマーが期限切れになった場合、コールは拒否されます。

```
interface serial1/0/0:23
 isdn guard-timer 8000 on-expiry reject

aaa preauth
 group radius
 dnis required
```

次に、20,000 ミリ秒に設定された CAS ガード タイマーの例を示します。事前認証要求に対して RADIUS サーバが応答しないまま、タイマーが期限切れになった場合、コールは許可されます。

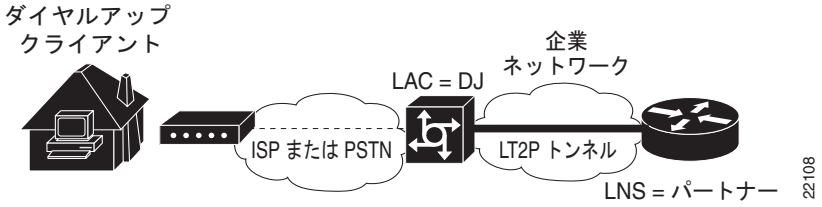
```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
 cas-custom 0
 call guard-timer 20000 on-expiry accept

aaa preauth
group radius
dnis required
```

例：L2TP アクセス コンセントレータ

次に、図 1 に示すトポロジの基本的な L2TP Access Concentrator（LAC; L2TP アクセス コンセントレータ）を設定する例を示します。ローカル名は定義されていないため、使用されるホスト名はローカル名です。L2TP トンネル パスワードは定義されていないため、ユーザ名パスワードが使用されます。この例では、VPDN が LAC のローカルで設定されます。VPDN は新しい RADIUS トンネル アトリビュートを利用しません。

図 1　設定例のトポロジ




```
! Enable AAA globally.
aaa new-model
! Enable AAA authentication for PPP and list the default method to use for PPP
! authentication.
aaa authentication ppp default local
! Define the username as ”DJ.”
username DJ password 7 030C5E070A00781B
! Enable VPDN.
vpdn enable
! Define VPDN group number 1.
vpdn-group 1
! Allow the LAC to respond to dialin requests using L2TP from IP address 172.21.9.13
! domain ”cisco.com.”
 request dialin
  protocol l2tp
  domain cisco.com
 initiate-ip to 172.21.9.13
 local name nas-1
```

次に、RADIUS トンネル アトリビュートがサポートされる場合、LAC を設定する例を示します。この例では、LAC にローカルの VPDN 設定がありません。代わりに、LAC は、リモート RADIUS セキュリティ サーバを照会するように設定されています。

```
! Enable global AAA securities services.
aaa new-model
! Enable AAA authentication for PPP and list RADIUS as the default method to use
! for PPP authentication.
aaa authentication ppp default group radius local
! Enable AAA (network) authorization and list RADIUS as the default method to use for
! authorization.
aaa authorization network default group radius
! Define the username as ”DJ.”
username DJ password 7 030C5E070A00781B
! Enable VPDN.
vpdn enable
! Configure the LAC to interface with the remote RADIUS security server.
radius host 171.19.1.1 auth-port 1645 acct-port 1646
radius-server key cisco
```

例：L2TP ネットワーク サーバ

次に、図 1 に示すトポロジの L2TP ネットワーク サーバ（LNS）で基本的な L2TP を設定する例と対応するコメントを示します。

```
! Enable AAA globally.
aaa new-model
! Enable AAA authentication for PPP and list the default method to use for PPP
! authentication.
aaa authentication ppp default local
! Define the username as ”partner.”
```

```
username partner password 7 030C5E070A00781B
! Create virtual-template 1 and assign all values for virtual access interfaces.
interface Virtual-Template1
! Borrow the IP address from interface ethernet 1.
 ip unnumbered Ethernet0
! Disable multicast fast switching.
 no ip mroute-cache
! Use CHAP to authenticate PPP.
 ppp authentication chap
! Enable VPDN.
vpdn enable
! Create vpdn-group number 1.
vpdn-group 1
! Accept all dialin l2tp tunnels from virtual-template 1 from remote peer DJ.
 accept dialin l2tp virtual-template 1 remote DJ
  protocol any
  virtual-template 1
 terminate-from hostname nas1
local name hgw1
```

次に、RADIUS トンネリング アトリビュートを使用して、基本的な L2F と L2TP 設定で LNS を設定する例を示します。

```
aaa new-model
aaa authentication login default none
aaa authentication login console none
aaa authentication ppp default local group radius
aaa authorization network default group radius if-authenticated
!
username l2f-cli-auth-id password 0 l2f-cli-pass
username l2f-svr-auth-id password 0 l2f-svr-pass
username l2tp-svr-auth-id password 0 l2tp-tnl-pass
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
accept-dialin
protocol l2f
virtual-template 1
terminate-from hostname l2f-cli-auth-id
local name l2f-svr-auth-id
!
vpdn-group 2
accept-dialin
protocol l2tp
virtual-template 2
terminate-from hostname l2tp-cli-auth-id
local name l2tp-svr-auth-id
!
interface Ethernet1/0
ip address 10.0.0.3 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface Virtual-Template1
ip unnumbered Ethernet1/0
ppp authentication pap
!
interface Virtual-Template2
ip unnumbered Ethernet1/0
ppp authentication pap
!
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
```

```
radius-server key <deleted>
```

その他の参考資料

ここでは、RADIUS の設定に関する関連資料について説明します。

関連資料

内容	参照先
RADIUS アトリビュート	「RADIUS Attributes Overview and RADIUS IETF Attributes」モジュール
AAA	「Configuring Authentication」モジュール
	「Configuring Authorization」モジュール
	「Configuring Accounting」モジュール
L2F、L2TP、VPN、または VPDN	『*Cisco IOS Dial Technologies Configuration Guide*』および『*Cisco IOS VPDN Configuration Guide*, Release 15.0』
モデムの設定と管理	『*Cisco IOS Dial Technologies Configuration Guide*, Release 15.0』
PPP の RADIUS ポートの識別	『*Cisco IOS Wide-Area Networking Configuration Guide*, Release 15.0』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2139	「*RADIUS Accounting*」
RFC 2865	「*Remote Authentication Dial-In User Service (RADIUS)*」
RFC 2868	「*RADIUS Attributes for Tunnel Protocol Support*」
RFC 2867	「*RADIUS Accounting Modifications for Tunnel Protocol Support*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

RADIUS の設定に関する機能情報

表 1 に、この機能のリリース履歴を示します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　RADIUS の設定に関する機能情報

機能名	リリース	機能情報
RADIUS の設定	11.1 Cisco IOS XE 3.1.0SG	Remote Authentication Dial-In User Service（RADIUS ）セキュリティ システムは、不正アクセスに対してネットワーク保護する分散クライアント/サーバ システムです。シスコの実装では RADIUS クライアントは Cisco ルータ上で稼動します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。RADIUS は完全にオープンなプロトコルであり、ソース コード形式で配布されているため、現在使用できる任意のセキュリティ システムと連携するように変更できます。 この機能は、Cisco IOS Release 11.1 で導入されました。
SNMP を介する RADIUS 統計情報	15.1(1)S	この機能は、RADIUS トラフィックおよびプライベート RADIUS サーバに関連する統計情報を提供します。 この機能については、次の項に説明があります。 「RADIUS のモニタリングとメンテナンス」（P.31） 変更されたコマンド：**show radius statistics**

AAA Dead-Server Detection

AAA Dead-Server Detection 機能を使用すると、RADIUS サーバをデッド状態と指定するための条件を設定できます。条件が明示的に設定されていない場合は、条件は未処理のトランザクションの数に基づいて動的に計算されます。この機能を使用すると、デッドタイムが短くなり、パケット処理が高速になります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「AAA Dead-Server Detection の機能情報」（P.9）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

AAA Dead-Server Detection の前提条件

- RADIUS サーバにアクセスできる必要があります。
- RADIUS サーバの設定方法を十分理解していることが必要です。
- Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）の設定方法を十分理解していることが必要です。
- あるサーバをデッド状態と指定するためには、まず **radius-server deadtime** コマンドを設定する必要があります。このコマンドを設定していない場合は、サーバをデッド状態と指定するための条件に適合していても、サーバは「アップ」状態になります。

AAA Dead-Server Detection の制約事項

- サーバがデッド状態と指定されるまでにルータで発生する必要がある連続タイムアウト回数には、最初の転送は含まれません。つまり、再転送の回数のみがカウントされます。

AAA Dead-Server Detection について

AAA Dead-Server Detection 機能を設定するために、次の概念を理解しておく必要があります。

- 「RADIUS サーバをデッド状態と指定するための条件」（P.2）

RADIUS サーバをデッド状態と指定するための条件

AAA Dead-Server Detection 機能を使用すると、RADIUS サーバをデッド状態と指定するための条件を決定できます。つまり、ルータが RADIUS サーバから有効なパケットを最後に受け取ってから RADIUS サーバがデッド状態と指定されるまでに経過する必要がある最低時間を秒単位で設定することができます。ルータの起動後にパケットを受信せずにタイムアウトになった場合は、この時間の条件は満たされたものとして処理されます。

さらに、RADIUS サーバがデッド状態と指定されるまでにルータで発生する必要がある連続タイムアウト回数を設定することもできます。サーバが認証とアカウンティングの両方を実行する場合、両方の種類のパケットがこの回数に含まれます。正しく作成されていないパケットは、タイムアウトになっているものとしてカウントされます。カウントされるのは再転送だけで、最初の転送はカウントされません（タイムアウトになるたびに再転送が 1 回行われることになります）。

（注） 時間の条件と試行回数の条件の両方を満たしていないと、サーバはデッド状態と指定されません。

RADIUS Dead-Server Detection を設定すると、応答を停止している RADIUS サーバが即時検出されます。また、サーバが「動きが鈍い」（応答が遅い）状態になっているときに誤ってデッド状態と指定されなくなるほか、デッド状態からライブ状態になってすぐにまたデッド状態になる現象を回避できます。この未応答 RADIUS サーバの即時検出、動きが鈍いサーバの誤検出の回避、デッド状態とライブ状態を繰り返す現象の回避が有効になると、デッドタイムが短くなり、パケット処理が高速になります。

AAA Dead-Server Detection の設定方法

ここでは、次の各手順について説明します。

- 「AAA Dead-Server Detection の設定」（P.3）（必須）
- 「AAA Dead-Server Detection の確認」（P.4）（任意）

AAA Dead-Server Detection の設定

AAA Dead-Server Detection を設定する手順は、次のとおりです。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server deadtime** *minutes*
5. **radius-server dead-criteria** [**time** *seconds*] [**tries** *number-of-tries*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： Router (config)# aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
ステップ 4	**radius-server deadtime** *minutes* 例： Router (config)# radius-server deadtime 5	いくつかのサーバが使用不能になったときの RADIUS サーバの応答時間を短くし、使用不能になったサーバがすぐにスキップされるようにします。
ステップ 5	**radius-server dead-criteria** [**time** *seconds*] [**tries** *number-of-tries*] 例： Router (config)# radius-server dead-criteria time 5 tries 4	RADIUS サーバをデッド状態と指定するための条件のいずれかまたは両方を、指定した定数で適用します。

トラブルシューティングのヒント

AAA Dead-Server Detection を設定したら、**show running-config** コマンドを使用して、その設定を確認してください。この確認が特に重要になるのは、**no** 形式の **radius-server dead-criteria** コマンドを使用している場合です。**show running-config** コマンドの出力は、**radius-server dead-criteria** コマンドを使用して設定した「Dead Criteria Details」フィールドと同じ値を示している必要があります。

AAA Dead-Server Detection の確認

AAA Dead-Server Detection の設定を確認する手順は、次のとおりです。**show** コマンドと **debug** コマンドは、どの順序で使用してもかまいません。

手順の概要

1. **enable**
2. **debug aaa dead-criteria transactions**
3. **show aaa dead-criteria**
4. **show aaa servers**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**debug aaa dead-criteria transactions** **例：** Router# debug aaa dead-criteria transactions	デッド条件の AAA トランザクションの値を表示します。
ステップ 3	**show aaa dead-criteria** **例：** Router# show aaa dead-criteria	AAA サーバのデッド条件に関する情報を表示します。
ステップ 4	**show aaa servers** [**private** | **public**] **例：** Router# show aaa server private	パブリックおよびプライベートのすべての Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）RADIUS サーバとの間で送受信されたパケットのステータスと数を表示します。 • **private** キーワードを付けると、プライベート AAA サーバのみについて表示されます。 • **public** キーワードを付けると、パブリック AAA サーバのみについて表示されます。

AAA Dead-Server Detection の設定例

ここでは、次の設定例について説明します。

- 「AAA Dead-Server Detection の設定の例」（P.5）
- 「aaa dead-criteria transactions コマンドのデバッグの例」（P.6）
- 「show aaa dead-criteria コマンドの例」（P.6）

AAA Dead-Server Detection の設定の例

次の例では、5 秒後および 4 回の試行後にルータがデッド状態と見なされます。

```
Router (config)# aaa new-model
Router (config)# radius-server deadtime 5
Router (config)# radius-server dead-criteria time 5 tries 4
```

aaa dead-criteria transactions コマンドのデバッグの例

次の出力例は、特定のサーバ グループのデッド条件のトランザクションに関する情報を示しています。

```
Router# debug aaa dead-criteria transactions

AAA Transaction debugs debugging is on

*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Computed Retransmit Tries: 22, Current Max Tries: 22
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Computed Dead Detect Interval: 25s, Current Max
Interval: 25s
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Estimated Outstanding Transactions: 6, Current Max
Transactions: 6
```

show aaa dead-criteria コマンドの例

次の出力例は、IP アドレス 172.19.192.80 の RADIUS サーバに対してデッド サーバ検出に関する情報が要求されたことを示しています。

```
Router# show aaa dead-criteria radius 172.19.192.80 radius

RADIUS Server Dead Criteria:
============================
Server Details:
    Address : 172.19.192.80
    Auth Port : 1645
    Acct Port : 1646
Server Group : radius
Dead Criteria Details:
    Configured Retransmits : 62
    Configured Timeout : 27
    Estimated Outstanding Transactions: 5
    Dead Detect Time : 25s
    Computed Retransmit Tries: 22
    Statistics Gathered Since Last Successful Transaction
=====================================================
Max Computed Outstanding Transactions: 5
Max Computed Dead Detect Time: 25s
Max Computed Retransmits : 22
```

その他の参考資料

ここでは、AAA Dead-Server Detection 機能の関連資料について説明します。

関連資料

内容	参照先
RADIUS の設定	「Configuring RADIUS」フィーチャ モジュール
AAA の設定	「Configuring Authentication」
	「Configuring Authorization」
	「Configuring Accounting」
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2865	「*Remote Authentication Dial In User Service (RADIUS)*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

AAA Dead-Server Detection の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator により、どの Cisco IOS、Catalyst OS、および Cisco IOS XE ソフトウェア イメージが特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　AAA Dead-Server Detection の機能情報

機能名	リリース	機能情報
AAA Dead-Server Detection	12.3(6) 12.3(7)T Cisco IOS XE Release 2.1 Cisco IOS XE 3.1.0SG	RADIUS サーバをデッド状態と指定するための条件を設定できます。 次のコマンドが導入または変更されました。**debug aaa dead-criteria transactions**、**radius-server dead-criteria**、**show aaa dead-criteria**、**show aaa servers**

AAA Dead-Server Detection の機能情報

AAA-SERVER-MIB Set Operation

AAA-SERVER-MIB Set Operation 機能により、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバ設定を拡張できます。CISCO-AAA-SERVER-MIB を使用して、新規 AAA サーバの作成や追加、CISCO-AAA-SERVER-MIB でのキーの変更、AAA サーバ設定の削除などを実行できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「AAA-SERVER-MIB Set Operation の機能情報」（P.8）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

AAA-SERVER-MIB Set Operation の前提条件

AAA がルータで有効になっている必要があります。つまり、**aaa new-model** コマンドが設定されている必要があります。この設定が行われていない場合、SET 操作は失敗します。

AAA-SERVER-MIB Set Operation の制約事項

現時点では、CISCO SNMP SET 操作は RADIUS プロトコルに対してのみサポートされています。このため、追加、修正、削除できるのはグローバル コンフィギュレーション モードの RADIUS サーバだけです。

AAA-SERVER-MIB Set Operation について

AAA-SERVER-MIB Set Operation 機能を使用する前に、次の概念を理解しておく必要があります。

- 「CISCO-AAA-SERVER-MIB」（P.2）
- 「CISCO-AAA-SERVER-MIB Set Operation」（P.2）

CISCO-AAA-SERVER-MIB

CISCO-AAA-SERVER-MIB により、サーバ自体と AAA サーバの動作、および外部サーバとの AAA 通信の両方の状態が統計情報に反映されます。CISCO-AAA-SERVER-MIB からは次の情報が得られます。

- 各 AAA 動作の統計情報
- AAA 機能を使用できるようになっているサーバのステータス
- 外部 AAA サーバの ID

CISCO-AAA-SERVER-MIB Set Operation

Cisco IOS Release 12.4(4)T よりも前は、CISCO-AAA-SERVER-MIB は「GET」操作のみをサポートしていました。このリリースでは、CISCO-AAA-SERVER-MIB は SET 操作をサポートしています。SET 操作を使用すると、次の作業を行うことができます。

- 新しい AAA サーバを作成または追加する。
- CISCO-AAA-SERVER-MIB で KEY を修正する。この「秘密キー」は、Network Access Server（NAS; ネットワーク アクセス サーバ）および AAA サーバに存在する AAA サーバへの接続をセキュリティ保護するために使用されます。
- AAA サーバの設定を削除する。

Configure AAA-SERVER-MIB Set Operation の設定方法

ここでは、次の作業について説明します。

- 「AAA-SERVER-MIB Set Operation の設定」（P.3）

- 「SNMP 値の確認」（P.3）

AAA-SERVER-MIB Set Operation の設定

この機能を使用するに当たって、特別な設定は必要ありません。Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）フレームワークを使用して MIB を管理できます。SNMP の設定については、「その他の参考資料」を参照してください。

SNMP 値の確認

SNMP 値は次の手順で確認できます。

手順の概要

1. **enable**
2. **show running-config | include radius-server host**
3. **show aaa servers**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show running-config | include radius-server host** 例： `Router# show running-config | include radius-server host`	グローバル コンフィギュレーション モードで設定されている RADIUS サーバをすべて表示します。
ステップ 3	**show aaa servers** 例： `Router# show aaa servers`	Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバとの間で送受信された要求の数に関するデータを表示します。

AAA-SERVER-MIB Set Operation の設定例

ここでは、次の例について説明します。

- 「RADIUS サーバの設定およびサーバの統計情報の例」（P.4）

RADIUS サーバの設定およびサーバの統計情報の例

次の出力例は、SET 操作の前と後の RADIUS サーバの設定およびサーバの統計情報を示しています。

SET 操作の前

```
Router# show running-config | include radius-server host

! The following line is for server 1.
radius-server host 172.19.192.238 auth-port 2095 acct-port 2096 key cisco2
! The following line is for server 2.
radius-server host 172.19.192.238 auth-port 1645 acct-port 1646
```

サーバの統計情報

```
Router# show aaa servers

RADIUS: id 2, priority 1, host 172.19.192.238, auth-port 2095, acct-port 2096
State: current UP, duration 25s, previous duration 0s
     Dead: total time 0s, count 7
Authen: request 8, timeouts 8
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 2
Author: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Account: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Elapsed time since counters last cleared: 5m

RADIUS: id 3, priority 2, host 172.19.192.238, auth-port 1645, acct-port 1646
State: current UP, duration 5s, previous duration 0s
     Dead: total time 0s, count 2
Authen: request 8, timeouts 8
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 4
Author: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Account: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Elapsed time since counters last cleared: 3m
```

RADIUS サーバの設定と統計情報をチェックする SNMP GET 操作

```
aaa-server5:/users/smetri> getmany 10.0.1.42 casConfigTable
casAddress.2.2 = 172.19.192.238
casAddress.2.3 = 172.19.192.238
casAuthenPort.2.2 = 2095
casAuthenPort.2.3 = 1645
casAcctPort.2.2 = 2096
casAcctPort.2.3 = 1646
casKey.2.2 =
casKey.2.3 =
! The following line shows priority for server 1.
casPriority.2.2 = 1
! The following line shows priority for server 2.
casPriority.2.3 = 2
casConfigRowStatus.2.2 = active(1)
casConfigRowStatus.2.3 = active(1)
aaa-server5:/users/smetri>
```

SNMP SET 操作

RADIUS サーバのキーが変更されています。また、インデックス「1」が使用されています。このインデックスは、エントリの追加、削除、修正に使用されるワイルドカードとして機能します。

```
Change the key for server 1:=>

aaa-server5:/users/smetri>  setany -v2c 10.0.1.42 public casAddress.2.1 -a 172.19.192.238
casAuthenPort.2.1 -i 2095 casAcctPort.2.1 -i 2096 casKey.2.1 -o king
casAddress.2.1 = 172.19.192.238
casAuthenPort.2.1 = 2095
casAcctPort.2.1 = 2096
casKey.2.1 = king
aaa-server5:/users/smetri>
```

SET 操作の後

上記の SNMP SET 操作後、ルータの設定が変更されます。SET 操作後の出力を次に示します。

```
Router# show running-config | include radius-server host

radius-server host 172.19.192.238 auth-port 1645 acct-port 1646
! The following line shows a change in the key value to ”king.”
radius-server host 172.19.192.238 auth-port 2095 acct-port 2096 key king


Router# show aaa servers

RADIUS: id 3, priority 1, host 172.19.192.238, auth-port 1645, acct-port 1646
State: current UP, duration 189s, previous duration 0s
     Dead: total time 0s, count 2
Authen: request 8, timeouts 8
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 4
Author: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Account: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Elapsed time since counters last cleared: 6m

! The following line shows a new server with new statistics.
RADIUS: id 4, priority 2, host 172.19.192.238, auth-port 2095, acct-port 2096
State: current UP, duration 209s, previous duration 0s
     Dead: total time 0s, count 7
Authen: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Author: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Account: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
```

その他の参考資料

ここでは、AAA-SERVER-MIB Set Operation 機能の関連資料について説明します。

関連資料

内容	参照先
SNMP の設定	『*Cisco IOS Network Management Configuration Guide*』の「Configuring SNMP Support」

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能がサポートする新規 RFC または改訂 RFC はありません。また、この機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

AAA-SERVER-MIB Set Operation の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　AAA-SERVER-MIB Set Operation の機能情報

機能名	リリース	機能情報
AAA-SERVER-MIB Set Operation	12.4(4)T 12.3(11)T 12.2(33)SRE	AAA-SERVER-MIB Set Operation 機能により、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバ設定を拡張できます。CISCO-AAA-SERVER-MIB を使用して、新規 AAA サーバの作成や追加、CISCO-AAA-SERVER-MIB でのキーの変更、AAA サーバ設定の削除などを実行できます。 この機能は、Cisco IOS Release 12.4(4)T で導入されました。 この機能に関する詳細については、次の各項を参照してください。 • 「CISCO-AAA-SERVER-MIB Set Operation」（P.2） • 「AAA-SERVER-MIB Set Operation の設定例」（P.3） 導入または変更されたコマンドは、**show aaa servers**、**show running-config**、**show running-config vrf** です。

AAA-SERVER-MIB Set Operation の機能情報

ACL Default Direction

ACL Default Direction 機能を使用すると、フィルタの方向が指定されていないサーバ上で、インバウンド パケット（ネットワークに着信するパケット）だけになるようにフィルタの方向を変更できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「ACL Default Direction の機能情報」（P.8）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

ACL Default Direction の前提条件

RADIUS からデフォルトのフィルタの方向を変更するためには、次の作業を行う必要があります。

- Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）用に Network Access Server（NAS; ネットワーク アクセス サーバ）を設定し、着信コールを受け付けるように設定します。

  詳細については、『*Cisco IOS Security Configuration Guide: Securing User Services,* Release 12.4T』および『*Cisco IOS Dial Technologies Configuration Guide,* Release 12.4T』の AAA に関する章を参照してください。

- NAS でフィルタを作成します。

  詳細については、『*Cisco IOS IP Addressing Services Configuration Guide*, Release 12.4T』を参照してください。

- RADIUS ユーザのフィルタ定義（Filter-Id = "myfilter" など）を追加します。

ACL Default Direction について

RADIUS から Access Control List（ACL; アクセス コントロール リスト）のフィルタのデフォルトの方向を変更するためには、次の概念を理解しておく必要があります。

- 「radius-server attribute 11 direction default コマンド」（P.2）
- 「ACL Default Direction の利点」（P.2）

radius-server attribute 11 direction default コマンド

radius-server attribute 11 direction default コマンドを使用すると、RADIUS から ACL のフィルタのデフォルトの方向を変更することができます（RADIUS アトリビュート 11（Filter-Id）はユーザのフィルタ リストの名前を示しています）。このコマンドをイネーブルにすると、トラフィックがネットワークを出るときにのみフィルタ処理が発生するデフォルトのアウトバウンド方向を維持するのではなく、トラフィックがルータに入るのを阻止し、リソースの消費を少なくするインバウンド方向にフィルタの方向を変更することができます。

ACL Default Direction の利点

ACL Default Direction 機能により、**radius-server attribute 11 direction default** コマンドを使用して ACL のフィルタのデフォルトの方向（アウトバウンド）をインバウンドに変更することができます。

ACL Default Direction の設定方法

ここでは、次の各手順について説明します。

- 「アトリビュート 11（Filter-Id）による RADIUS からの ACL のデフォルト方向の設定」（P.3）（必須）
- 「アトリビュート 11（Filter-Id）による RADIUS からの ACL のデフォルト方向の確認」（P.3）（任意）

アトリビュート 11（Filter-Id）による RADIUS からの ACL のデフォルト方向の設定

次の作業を行って、アトリビュート 11 を使用して RADIUS からフィルタのデフォルトの方向を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server attribute 11 direction default** [**inbound** | **outbound**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server attribute 11 direction default** [**inbound** | **outbound**] 例： `Router(config)# radius-server attribute 11 direction default inbound`	RADIUS からフィルタのデフォルトの方向をインバウンドまたはアウトバウンドに指定します。

アトリビュート 11（Filter-Id）による RADIUS からの ACL のデフォルト方向の確認

次の作業を行って、RADIUS からフィルタのデフォルトの方向を確認したり、アクセス受け入れ要求で RADIUS アトリビュート 11 が送信されていることを確認したりします。

手順の概要

1. **enable**
2. **more system:running-config**
3. **debug radius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**more system:running-config** **例：** `Router# more system:running-config`	現在実行されているコンフィギュレーション ファイルの内容を表示します。
ステップ 3	**debug radius** **例：** `Router# debug radius`	RADIUS 関連の情報を表示します。このコマンドの出力は、アクセス受け入れ要求でアトリビュート 11 が送信されているかどうかを示しています。

ACL Default Direction の設定例

ここでは、次の設定例について説明します。

- 「RADIUS アトリビュート 11（Filter-Id）によるフィルタのデフォルトの方向の例」（P.4）
- 「Filter-Id のある RADIUS ユーザ プロファイルの例」（P.5）

RADIUS アトリビュート 11（Filter-Id）によるフィルタのデフォルトの方向の例

次の例は、RADIUS アトリビュート 11 を設定してフィルタのデフォルトの方向を変更する方法を示しています。この例では、フィルタ処理はインバウンド パケットのみに適用されます。

radius-server attribute 11 direction default inbound

Filter-Id のある RADIUS ユーザ プロファイルの例

次に、RADIUS アトリビュート 11（Filter-Id）を含む RADIUS ユーザ プロファイル（Merit Daemon 形式）の例を示します。

```
client Password = "password1"
        Service-Type = Framed,
        Framed-Protocol = PPP,
        Filter-Id = "myfilter.out"
```

この例に示されている RADIUS ユーザ プロファイルにより、NAS から次の応答が生成されます。

```
RADIUS: Send to unknown id 79 10.51.13.4:1645, Access-Request, len 85
RADIUS: authenticator 84 D3 B5 7D C2 5B 70 AD - 1E 5C 56 E8 3A 91 D0 6E
RADIUS: User-Name           [1]   8  "client"
RADIUS: CHAP-Password       [3]   19  *
RADIUS: NAS-Port            [5]   6   20030
RADIUS: NAS-Port-Type       [61]  6   ISDN                      [2]
RADIUS: Called-Station-Id   [30]  6   "4321"
RADIUS: Calling-Station-Id  [31]  6   "1234"
RADIUS: Service-Type        [6]   6   Framed                    [2]
RADIUS: NAS-IP-Address      [4]   6   10.1.73.74

RADIUS: Received from id 79 10.51.13.4:1645, Access-Accept, len 46
RADIUS: authenticator 9C 6C 66 E2 F1 42 D6 4B - C1 7D D4 5E 9D 09 BB A1
RADIUS: Service-Type        [6]   6   Framed                    [2]
RADIUS: Framed-Protocol     [7]   6   PPP                       [1]
RADIUS: Filter-Id           [11]  14
RADIUS: 6D 79 66 69 6C 74 65 72 2E 6F 75 74          [myfilter.out]
```

その他の参考資料

ここでは、ACL Default Direction 機能の関連資料について説明します。

関連資料

内容	参照先
『Cisco IOS Dial Technologies Configuration Guide』	『*Cisco IOS Dial Technologies Configuration Guide,* Release 12.4T』
Cisco IOS セキュリティの設定	『*Cisco IOS Security Configuration Guide: Securing User Services,* Release 12.4T』
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
IP サービスの設定	『*Cisco IOS IP Addressing Services Configuration Guide*, Release 12.4T』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2865	「*Remote Authentication Dial-In User Service (RADIUS)*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

ACL Default Direction の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　ACL Default Direction の機能情報

機能名	リリース	機能情報
ACL Default Direction	12.2(4)T 12.2(28)SB 12.2(31)SB3	ACL Default Direction 機能を使用すると、フィルタの方向が指定されていないサーバ上で、インバウンド パケット（ネットワークに着信するパケット）だけになるようにフィルタの方向を変更できます。 この機能は、Cisco IOS Release 12.2(4)T で導入されました。 この機能は、Cisco IOS Release 12.2(28)SB で導入されました。 この機能は、Cisco IOS Release 12.2(31)SB3 で導入されました。 コマンド **radius-server attribute 11 direction default** が導入されました。

ACL Default Direction の機能情報

アクセス要求のアトリビュート スクリーニング

アクセス要求のアトリビュート スクリーニング機能を使用すると、認証用または認可用に RADIUS サーバへのアウトバウンドのアクセス要求のアトリビュートをフィルタ処理するように Network Access Server（NAS; ネットワーク アクセス サーバ）を設定することができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「アクセス要求のアトリビュート スクリーニングの機能情報」（P.9）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

アクセス要求のアトリビュート スクリーニングの前提条件

- アトリビュート リストの設定を十分理解していることが必要です。

アクセス要求のアトリビュート スクリーニングの制約事項

- アトリビュート 1（Username）、アトリビュート 2（User-Password）、アトリビュート 3（Chap-Password）をフィルタ処理することはできません。

アクセス要求のアトリビュート スクリーニングについて

アクセス要求のアトリビュート スクリーニング機能を設定するために、次の概念を理解しておく必要があります。

- 「アウトバウンドのアクセス要求のアトリビュートをフィルタ処理する NAS の設定」（P.2）

アウトバウンドのアクセス要求のアトリビュートをフィルタ処理する NAS の設定

アクセス要求のアトリビュート スクリーニング機能を使用すると、認証用または認可用に RADIUS サーバへのアウトバウンドのアクセス要求のアトリビュートをフィルタ処理するように NAS を設定することができます。フィルタの設定は、NAS で行ったり、ダウンロード可能な Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）によって Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバからダウンロードしたりすることができます。

次に、ダウンロード可能な VSA の例をいくつか示します。

```
Cisco:Cisco-Avpair=”ppp-authen-type=chap”
Cisco:Cisco-Avpair=”ppp-authen-list=group 1”
Cisco:Cisco-Avpair=”ppp-author-list=group 1”
Cisco:Cisco-Avpair=”vpdn:tunnel-id=B53”
Cisco:Cisco-Avpair=”vpdn:ip-addresses=10.0.58.35”
```

（注） フィルタ処理するアトリビュートがわかっている必要があります。ある一定の主要アトリビュートをフィルタ処理すると、認証に失敗することがあります（たとえば、アトリビュート 60 はフィルタ処理すべきではありません）。

アクセス要求のアトリビュート スクリーニングの設定方法

ここでは、次の各手順について説明します。

- 「アクセス要求のアトリビュート スクリーニングの設定」（P.3）
- 「ダウンロード可能なフィルタをサポートするためのルータの設定」（P.4）
- 「Attribute Filtering for Access Requests のモニタリングとメンテナンス」（P.5）

アクセス要求のアトリビュート スクリーニングの設定

アクセス要求のアトリビュート スクリーニングを設定する手順は、次のとおりです。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server attribute list** *listname*
4. **attribute** *value1* **[***value2* **[***value3...***]]**
5. **aaa group server radius** *group-name*
6. **authorization** [**request** | **reply**] [**accept** | **reject]** *listname*

   または

   accounting [**request** | **reply**] **[accept | reject]** *listname*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server attribute list** *listname* 例： `Router (config)# radius-server attribute list attrlist`	アトリビュート リストを定義します。
ステップ 4	**attribute** *value1* **[***value2***[***value3...***]]** 例： `Router (config)# attribute 6-10, 12`	許可リストまたは拒否リストにアトリビュートを追加します。
ステップ 5	**aaa group server radius** *group-name* 例： `Router (config)# aaa group server radius rad1`	アトリビュート リストを AAA サーバ グループに適用し、server-group コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 6	**authorization** [**request** | **reply**][**accept** | **reject**] *listname*
	
	または
	accounting [**request** | **reply**] [**accept** | **reject**] *listname*
	
	例：
	`Router (config-sg-radius)# authorization request accept attrlist`
	
	または
	
	例：
	`Router (config-sg-radius)# accounting request accept attrlist`
		認証用または認可用に RADIUS サーバへのアウトバウンドの Access Request のアトリビュートをフィルタ処理します。
		• **request** キーワードでは、認可の発信 Access Request に使用するフィルタを定義します。
		• **reply** キーワードでは、認可の着信 Accept パケットと着信 Reject パケットのフィルタと、発信アカウンティング要求のフィルタを定義します。

ダウンロード可能なフィルタをサポートするためのルータの設定

次の作業を行って、ダウンロード可能なフィルタをサポートするようにルータを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authorization template**
4. **aaa authorization network default group radius**
5. **radius-server attribute list** *list-name*
6. **attribute** *value1* [*value2* [*value3...*]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa authorization template** **例：** `Router (config)# aaa authorization template`	Virtual Private Network（VPN; バーチャル プライベート ネットワーク）Routing and Forwarding（VRF; VPN ルーティングおよび転送）に基づいて、ローカルまたはリモートのカスタマー テンプレートの使用をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**aaa authorization network default group radius** 例： `Router (config)# aaa authorization network default group radius`	ネットワークへのユーザ アクセスを制限するパラメータを設定します。
ステップ 5	**radius-server attribute list** *list-name* 例： `Router (config)# radius-server attribute list attlist`	許可リストまたは拒否リストの名前を定義します。
ステップ 6	**attribute** *value1* [*value2* [*value3*...]] 例： `Router (config)# attribute 10-14, 24`	許可リストまたは拒否リストにアトリビュートを追加します。

トラブルシューティングのヒント

アトリビュートのフィルタ処理が機能しない場合は、アトリビュート リストが正しく定義されているかどうかを確認します。

Attribute Filtering for Access Requests のモニタリングとメンテナンス

アトリビュートのフィルタ処理をモニタリングおよびメンテナンスするために、**debug radius** コマンドを使用できます。

手順の概要

1. **enable**
2. **debug radius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**debug radius** 例： `Router# debug radius`	RADIUS の情報（フィルタ処理の情報など）を表示します。

Attribute Filtering for Access Requests の設定例

ここでは、次の設定例について説明します。

Attribute Filtering for Access Requests の例

次の例は、「all-attr」で定義されているアトリビュート 30-31 がアウトバウンドのすべての Access Request メッセージで拒否されることを示しています。

```
aaa group server radius ras
 server 172.19.192.238 auth-port 1745 acct-port 1746
 authorization request reject all-attr
!
.
.
.
radius-server attribute list all-attr
 attribute 30-31
!
.
.
.
```

ユーザ プロファイルのアトリビュート フィルタ処理の例

次の例は、Access Request のアトリビュート フィルタ処理を設定した後のユーザ プロファイルです。

```
cisco.com Password = "cisco"
Service-Type = Framed,
Framed-Protocol = PPP,
Cisco:Cisco-Avpair = :1:"rad-serv=172.19.192.87 key rad123",
Cisco:Cisco-Avpair = :1:"rad-serv-filter=authorization request reject range1",
Cisco:Cisco-Avpair = :1:"rad-serv-filter=accounting request reject range1",
Cisco:Cisco-Avpair = "ppp-authen-type=chap"
Cisco:Cisco-Avpair = "ppp-authen-list=group 1",
Cisco:Cisco-Avpair = "ppp-author-list=group 1",
Cisco:Cisco-Avpair = "ppp-acct-list=start-stop group 1",
Cisco:Cisco-Avpair = "vpdn:tunnel-id=B53",
Cisco:Cisco-Avpair = "vpdn:tunnel-type=l2tp",
Cisco:Cisco-Avpair = "vpdn:ip-addresses=10.0.58.35",
Cisco:Cisco-Avpair = "vpdn:l2tp-tunnel-password=cisco"


user2@cisco.com
Service-Type = Outbound,
Cisco:Cisco-Avpair = "vpdn:tunnel-id=B53",
Cisco:Cisco-Avpair = "vpdn:tunnel-type=l2tp",
Cisco:Cisco-Avpair = "vpdn:ip-addresses=10.0.58.35",
Cisco:Cisco-Avpair = "vpdn:l2tp-tunnel-password=cisco"
```

aaa authorization template コマンドが設定されているため、上記のように user2@cisco.com のセッションが Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）Network Server（LNS; ネットワーク サーバ）で「確立」されると、RADIUS 要求が Cisco.com のサーバに送信されます。その後、Cisco.com のサーバは、認証が成功すれば、Cisco.com のプロファイルの一部として設定されている VSA とともに、Access Accept メッセージを送信します。Cisco.com のプロファイルの一部としてフィルタが設定されている場合は、それらのフィルタが解析され、user2@cisco.com の RADIUS 要求に適用されます。

上記のプロファイルの例では、フィルタ range1 が認可要求およびアカウンティング要求に適用されます。

debug radius コマンドの例

フィルタ処理しようとしているアトリビュートが拒否される場合、次のような **debug radius** の出力ステートメントが表示されます。

```
RADIUS: attribute 31 rejected
```

フィルタ処理できないアトリビュートをフィルタ処理すると、次のような出力ステートメントが表示されます。

```
RADIUS: attribute 1 cannot be rejected
```

その他の参考資料

ここでは、Attribute Filtering for Access Requests の関連資料について説明します。

関連資料

内容	参照先
RADIUS の設定	『Configuring RADIUS』機能マニュアル
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
RADIUS アトリビュート リスト	『RADIUS Attribute Screening』機能マニュアル

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

アクセス要求のアトリビュート スクリーニングの機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　アクセス要求のアトリビュート スクリーニングの機能情報

機能名	リリース	機能情報
アクセス要求のアトリビュート スクリーニング	12.3(3)B 12.3(7)T 12.2(28)SB 12.2(33)SRC	アクセス要求のアトリビュート スクリーニング機能を使用すると、認証用または認可用に RADIUS サーバへのアウトバウンドのアクセス要求のアトリビュートをフィルタ処理するように Network Access Server（NAS; ネットワーク アクセス サーバ）を設定することができます。 この機能は、12.3(3)B で導入されました。 この機能は、Cisco IOS Release 12.3(7)T に統合されました。 この機能は、Cisco IOS Release 12.2(28)SB に統合されました。 この機能は、Cisco IOS Release 12.2(33)SRC に統合されました。 この機能によって導入または変更されたコマンドは、**authorization (server-group)** です。

事前認証ユーザに対する RADIUS を使用したマルチリンク PPP のイネーブル化

事前認証ユーザに対する RADIUS を使用したマルチリンク PPP のイネーブル化機能を使用すると、管理者は、事前認証プロファイルに対して RADIUS Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）の preauth:ppp-multilink=1 を使用して、異なるユーザの Multilink PPP（MLP; マルチリンク PPP）ネゴシエーションを選択的にイネーブルまたはディセーブルにすることができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「事前認証ユーザに対する RADIUS を使用したマルチリンク PPP のイネーブル化の機能情報」（P.8）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

事前認証ユーザに対する RADIUS を使用したマルチリンク PPP のイネーブル化の前提条件

RADIUS の VSA preauth:ppp-multilink=1 を使用して MLP をイネーブルにする前に、次のタスクを実行する必要があります。

- Network Access Server（NAS; ネットワーク アクセス サーバ）をイネーブルにし、**radius-server vsa send** コマンドを使用して、RADIUS IETF アトリビュート 26 に定義されたように VSA を認識して使用します。

  VSA の使用の詳細については、「Configuring RADIUS」フィーチャ モジュールの「Configuring Router to Use Vendor-Specific RADIUS Attributes」を参照してください。

- 事前認証をイネーブルにします。

  事前認証の詳細と設定については、「Configuring RADIUS」フィーチャ モジュールの「Configuring AAA Preauthentication」を参照してください。

事前認証ユーザに対する RADIUS を使用したマルチリンク PPP のイネーブル化機能の概要

事前認証ユーザに対して RADIUS を使用してマルチリンク PPP 機能をイネーブルにするには、インターフェイスで **ppp multilink** コマンドを実行します。ただし、このコマンドは、そのインターフェイスのすべての接続とユーザの MLP ネゴシエーションをイネーブルにします。つまり、インターフェイスの特定の接続やユーザの MLP ネゴシエーションを選択的にイネーブルまたはディセーブルにすることはできません。

（注） この機能を有効にする場合、インターフェイスに **ppp multilink** コマンドを設定しないでください。このコマンドはデフォルトで MLP をディセーブルにします。すでにそのインターフェイスに **ppp multilink** コマンドが設定されている場合、このコマンドはアトリビュート「preauth:ppp-multilink=1」によって上書きされません。

RADIUS を使用した MLP の機能

MLP のパラメータは Link Control Protocol（LCP; リンク コントロール プロトコル）ネゴシエーションのときにネゴシエートされるため、RADIUS の VSA preauth:ppp-multilink=1 は事前認証ユーザの認可のみに含める必要があります。MLP をイネーブルにするには、この VSA をユーザの事前認証プロファイルに追加する必要があります。そうすることで、MLP は、プロファイルにこの VSA を含む事前認証ユーザに対してのみイネーブルになり、他のすべてのユーザにはディセーブルになります。事前認証ユーザの認可とは対照的に、PPP のユーザの認可時に MLP の VSA を受信した場合、MLP とネゴシエートするには遅すぎるため、MLP はイネーブルになりません。

事前認証ユーザの認可時にこの VSA を受信すると、そのユーザの MLP ネゴシエーションがイネーブルになります。MLP は VSA の値が 1 のときにイネーブルになります。1 以外のすべてのアトリビュート値は無視されます。

L2TP アクセス サーバと L2TP ネットワーク サーバのロール

この機能を使用すると、事前認証ユーザの認可時に、L2TP Access Server（LAC; L2TP アクセス サーバ）のインターフェイスにある MLP を設定する必要はありません。LAC は、preauth:ppp-multilink=1 を受信した事前認証ユーザの MLP を選択的にイネーブルにします。L2TP Network Server（LNS; L2TP ネットワーク サーバ）では、PPP ユーザの認可時に RADIUS の VSA multilink:max-links=n を送信することによって、マルチリンク バンドルで使用可能な最大リンク数を制御できます。

新しいベンダー固有アトリビュート

この機能では、次の新しい VSA を導入しています。

- Cisco-AVpair = preauth:ppp-multilink=1

  インターフェイスで MLP をオンにして、事前認証プロファイルに適用します。
- Cisco-AVpair = multilink:max-links=n

  ユーザがマルチリンク バンドルで使用できる最大リンク数を制限します。service=ppp アトリビュートと一緒に使用します。「n」の範囲は 1 ～ 255 です。
- Cisco-AVpair = multilink:min-links=1

  MLP に対するリンクの最小数を設定します。「n」の範囲は 0 ～ 255 です。
- Cisco-AVpair = multilink:load-threshold=n

  マルチリンク バンドルに対して他のリンクを追加または削除する発信元の負荷のしきい値を設定します。負荷が指定された値を超えた場合はリンクが追加され、負荷が指定された値を下回った場合はリンクが削除されます。このアトリビュートは service=ppp アトリビュートと一緒に使用します。「n」の範囲は 1 ～ 255 です。

（注） RADIUS の VSA multilink:max-links、multilink:min-links、および multilink:load-threshold は、TACACS+ のユーザ単位アトリビュート max-links、min-links、および load-threshold とそれぞれ同じ目的で機能します。

事前認証での RADIUS を使用した MLP ネゴシエーションの確認

MLP バンドルのバンドル情報を表示するには、**show ppp multilink** EXEC コマンドを使用します。

```
Router# show ppp multilink

Virtual-Access1, bundle name is mlpuser
  Bundle up for 00:00:15
  Dialer interface is Serial0:23
  0 lost fragments, 0 reordered, 0 unassigned
  0 discarded, 0 lost received, 1/255 load
  0x0 received sequence, 0x0 sent sequence
  Member links: 1 (max 7, min 1)
    Serial0:22, since 00:00:15, no frags rcvd
```

表 1 に、MLP がイネーブルである場合に表示される重要なフィールドについて説明します。

表 1　show ppp multilink のフィールドの説明

フィールド	説明
Virtual-Access1	マルチリンク バンドルの仮想インターフェイス。
Bundle	マルチリンク バンドルに設定された名前。
Dialer Interface is Serial0:23	コールをダイヤルするインターフェイス名。
1/255 load	リンクの負荷。範囲は 1/255 ～ 255/255（255/255 は 100% の負荷を表す）。
Member links: 1	子インターフェイスの数。

事前認証ユーザに対する RADIUS を使用したマルチリンク PPP のイネーブル化の設定例

ここでは、Cisco VSA ppp-multilink を使用したダイヤルイン VPDN の設定について説明します。

- 「MLP の LAC の設定：例」
- 「事前認証用の LAC RADIUS プロファイル：例」
- 「MLP の LNS の設定：例」
- 「LNS RADIUS プロファイル：例」

MLP の LAC の設定：例

次に、RADIUS を使用して MLP 用の LAC の設定に使用できる設定の例を示します。

```
! Enable preauthentication
aaa preauth
  group radius
  dnis required

!Enable VPDN
vpdn enable
!
vpdn-group 1
  request-dialin
  protocol l2tp
  dnis 56118
  initiate-to ip 10.0.1.22
  local name lac-router

! Don't need to configure multilink on the interface
! Multilink will be enabled by "ppp-multilink" attribute
interface Serial0:23
  ip address 15.0.1.7 255.0.0.0
  encapsulation ppp
  dialer-group 1
  isdn switch-type primary-5ess
  isdn calling-number 56118
  peer default ip address pool pool1
  no cdp enable
  ppp authentication chap
```

事前認証用の LAC RADIUS プロファイル：例

次に、preauth:ppp-multilink=1 という VSA を適用した事前認証ユーザの LAC RADIUS プロファイルの例を示します。

```
56118   Password = ”cisco”
        Service-Type = Outbound,
        Framed-Protocol = PPP,
        Framed-MTU = 1500,
        Cisco-Avpair = "preauth:auth-required=1",
        Cisco-Avpair = "preauth:auth-type=chap",
        Cisco-Avpair = "preauth:username=dnis:56118",
        Cisco-Avpair = "preauth:ppp-multilink=1"
```

MLP の LNS の設定：例

次に、MLP バンドルのリンク数を制限するための LNS の設定に使用できる設定例を示します。

```
! Enable VPDN
vpdn enable
!
vpdn-group 1
 accept-dialin
 protocol any
 virtual-template 1
 terminate-from hostname lac-router
 local name lns-router
!
! Configure multilink on interface
interface Virtual-Template 1
 ip unnumbered Ethernet 0/0
 ppp authentication chap
 ppp multilink
```

LNS RADIUS プロファイル：例

次に、マルチリンク バンドルの最大リンク数を指定する場合の LNS RADIUS プロファイルの例を示します。次のマルチリンク VSA は PPP ユーザの認可時に指定する必要があります。

```
mascot  password = "cisco"
        Service-Type = Framed,
        Framed-Protocol = PPP,
        Cisco-Avpair = "multilink:max-links=7"
        Cisco-Avpair = "multilink:min-links=1"
        Cisco-Avpair = "multilink:load-threshold=128"
```

その他の参考資料

ここでは、事前認証ユーザに対する RADIUS を使用したマルチリンク PPP のイネーブル化機能の関連資料について説明します。

関連資料

内容	参照先
RADIUS	「Configuring RADIUS」フィーチャ モジュール
ダイヤル テクノロジー	『*Cisco IOS Dial Technologies Configuration Guide*, Release 12.4T』
RADIUS アトリビュート	「RADIUS Attributes Overview and RADIUS IETF Attributes」フィーチャ モジュール
TACACS+ アトリビュート	「TACACS+ Attribute-Value Pairs」フィーチャ モジュール

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
サポートされる新しい RFC や変更された RFC はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

事前認証ユーザに対する RADIUS を使用したマルチリンク PPP のイネーブル化の機能情報

表 2 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 2 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 2　事前認証ユーザに対する RADIUS を使用したマルチリンク PPP のイネーブル化の機能情報

機能名	リリース	機能情報
事前認証ユーザに対する RADIUS を使用したマルチリンク PPP のイネーブル化	12.2(11)T	事前認証ユーザに対する RADIUS を使用したマルチリンク PPP のイネーブル化機能を使用すると、管理者は、事前認証プロファイルに対して RADIUS Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）の preauth:ppp-multilink=1 を使用して、異なるユーザの Multilink PPP（MLP; マルチリンク PPP）ネゴシエーションを選択的にイネーブルまたはディセーブルにすることができます。 この機能は、Cisco IOS Release 12.2(11)T で導入されました。

用語集

AAA : Authentication, Authorization, and Accounting（認証、認可、およびアカウンティング）。Cisco ルータまたはアクセス サーバにアクセス コントロールを設定できる主要なフレームワークを提供する一連のネットワーク セキュリティ サービスです。

L2F : Layer 2 Forwarding（レイヤ 2 フォワーディング）。インターネットでのセキュアなバーチャル プライベート ダイヤルアップ ネットワークの作成をサポートするプロトコルです。

L2TP : Layer 2 Tunnel Protocol（レイヤ 2 トンネル プロトコル）。レイヤ 2 トンネル プロトコルを使用すると、ISP などのアクセス サービスが仮想トンネルを作成し、顧客のリモート サイトやリモート ユーザを企業のホーム ネットワークにリンクさせることができます。具体的には、ISP Point of Presence（POP; アクセス ポイント）にある Network Access Server（NAS; ネットワーク アクセス サーバ）がリモート ユーザと PPP メッセージを交換し、L2F または L2TP の要求や応答を使用して顧客のトンネル サーバと通信し、トンネルのセットアップを行います。

LAC：L2TP Access Concentrator（L2TP アクセス コンセントレータ）。クライアントが直接接続し、PPP フレームが L2TP Network Server（LNS; L2TP ネットワーク サーバ）にトンネリングされる Network Access Server（NAS; ネットワーク アクセス サーバ）です。LAC は、L2TP が 1 つまたは複数の LNS にトラフィックを渡すために操作するメディアのみを実装します。LAC は PPP 内で伝送されるすべてのプロトコルをトンネルすることができます。また、LAC は着信コールを開始して、発信コールを受け取ります。LAC は L2F ネットワーク アクセス サーバに似ています。

LNS：L2TP Network Server（L2TP ネットワーク サーバ）。L2TP トンネルの終端ポイントです。また、PPP フレームを処理して上の階層のプロトコルに渡す場合のアクセス ポイントでもあります。LNS は PPP を終端させる任意のプラットフォーム上で動作できます。LNS はサーバ側の L2TP プロトコルを処理します。L2TP は、L2TP のトンネルが到達する 1 つのメディアにのみ依存します。LNS は発信コールを開始して、着信コールを受け取ります。LNS は L2F テクノロジーのホーム ゲートウェイに似ています。

MLP：Multilink PPP（マルチリンク PPP）。MLP を使用すると、パケットをフラグメント化し、そのフラグメントを同じリモート アドレスへの複数のポイントツーポイント リンクに同時に送信できます。定義されたダイヤラの負荷のしきい値に応じて、複数のリンクが作成されます。指定されたサイト間のトラフィックの必要に応じて、着信トラフィック、発信トラフィック、またはその両方の負荷が計算されます。MLP はオンデマンド帯域幅を提供し、WAN リンク間の伝送の遅延を削減します。

MLP は、ダイヤルオンデマンド ロータリー グループと PPP のカプセル化の両方をサポートするように設定された 1 つまたは複数のインターフェイスの同期シリアルまたは非同期シリアル、および BRI または PRI タイプに対して機能するように設計されています。

RADIUS：Remote Authentication Dial-In User Service。RADIUS は、不正アクセスからネットワークを保護する分散型クライアント / サーバ システムです。シスコの実装では RADIUS クライアントは Cisco ルータ上で稼動します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

VSA：Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）。VSA は、1 つの IETF アトリビュート（ベンダー固有、アトリビュート 26）から派生しています。アトリビュート 26 を使用すれば、ベンダーは、追加の 255 個のアトリビュートを作成して実装できます。つまり、ベンダーは IETF のアトリビュートのデータとは一致しないアトリビュートを作成し、それをアトリビュート 26 の裏側でカプセル化することができます。基本的には、Vendor-Specific = "protocol:attribute=value" の形式を使用します。

アトリビュート：RADIUS Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）アトリビュートは、255 の標準アトリビュートで構成されるオリジナルのセットで、クライアントとサーバ間での AAA 情報の伝達に使用されます。IETF アトリビュートは標準であるため、アトリビュート データは事前定義されてその内容も認識されています。このため、IETF アトリビュートを介して AAA 情報を交換するすべてのクライアントとサーバは、アトリビュートの厳密な意味や各アトリビュート値の一般的な限界など、アトリビュート データに一致させる必要があります。

拡張テスト コマンド

拡張テスト コマンド機能を使用すると、Calling Line ID（CLID; 発呼回線 ID）または Dialed Number Identification Service（DNIS; 着信番号識別サービス）アトリビュート値を持つ名前付きユーザ プロファイルを作成できます。RADIUS サーバがすべての着信コールの CLID または DNIS アトリビュート情報にアクセスできるように、CLID または DNIS アトリビュート値を、ユーザ プロファイルとともに送信される RADIUS レコードに関連付けることができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「拡張テスト コマンドの機能情報」（P.6）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

拡張テスト コマンドの制約事項

test aaa group コマンドは、TACACS+ では機能しません。

拡張テスト コマンドの設定方法

以降のセクションでは、拡張テスト コマンド機能を設定する方法について説明します。

- 「ユーザ プロファイルの設定と RADIUS レコードへの関連付け」（P.2）
- 「拡張テスト コマンドの設定の確認」（P.3）

ユーザ プロファイルの設定と RADIUS レコードへの関連付け

ここでは、CLID または DNIS アトリビュート値を持つ名前付きユーザ プロファイルを作成し、RADIUS レコードに関連付ける方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa user profile** *profile-name*
4. **aaa attribute** {**dnis** | **clid**} *attribute-value*
5. **exit**
6. **test aaa group** {*group-name* | **radius**} *username password* **new-code** [**profile** *profile-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa user profile** *profile-name* 例： `Router(config)# aaa user profile profilename1`	ユーザ プロファイルを作成します。
ステップ 4	**aaa attribute** {**dnis** | **clid**} 例： `Router# configure terminal`	DNIS または CLID アトリビュート値をユーザ プロファイルに追加し、AAA ユーザ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 6	Router# **test aaa group** {*group-name* | **radius**} *username password* **new-code** [**profile** *profile-name*] **例：** Router# test aaa group radius secret new-code profile profilename1	DNIS または CLID の名前付きユーザ プロファイルを、RADIUS サーバに送信するレコードに関連付けます。 **（注）** *profile-name* は、**aaa user profile** コマンドで指定する *profile-name* に一致する必要があります。

拡張テスト コマンドの設定の確認

拡張テスト コマンドの設定を確認するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **debug radius**	RADIUS 関連の情報を表示します。
Router# **more system:running-config**	現在実行されているコンフィギュレーション ファイルの内容を表示します（**show running-config** コマンドが **more system:running-config** に置き換えられていることに注意してください）。

拡張テスト コマンドの設定例

ここでは、次の設定例について説明します。

- 「test aaa group コマンドに関連付けるユーザ プロファイルの例」（P.3）

test aaa group コマンドに関連付けるユーザ プロファイルの例

次に、dnis = dnisvalue ユーザ プロファイル「prfl1」を設定し、**test aaa group** コマンドを使用して関連付ける例を示します。この例で、**debug radius** コマンドがイネーブルにされ、設定の後に出力が続いています。

```
aaa user profile prfl1
  aaa attribute dnis
  aaa attribute dnis dnisvalue
  no aaa attribute clid
! Attribute not found.
  aaa attribute clid clidvalue
  no aaa attribute clid
  exit
!
! Associate the dnis user profile with the test aaa group command.
test aaa group radius user1 pass new-code profile profl1
!
!
!
! debug radius output, which shows that the dnis value has been passed to the radius
! server.
*Dec 31 16:35:48: RADIUS: Sending packet for Unique id = 0
```

```
 *Dec 31 16:35:48: RADIUS: Initial Transmit unknown id 8 172.22.71.21:1645,
Access-Request, len 68
 *Dec 31 16:35:48: RADIUS: code=Access-Request id=08 len=0068
        authenticator=1E CA 13 F2 E2 81 57 4C - 02 EA AF 9D 30 D9 97 90
        T=User-Password[2]                L=12 V=*
        T=User-Name[1]                    L=07 V="test"
        T=Called-Station-Id[30]           L=0B V="dnisvalue"
        T=Service-Type[6]                 L=06 V=Login                     [1]
        T=NAS-IP-Address[4]               L=06 V=10.0.1.81

 *Dec 31 16:35:48: RADIUS: Received from id 8 172.22.71.21:1645, Access-Accept, len 38
 *Dec 31 16:35:48: RADIUS: code=Access-Accept id=08 len=0038
```

その他の参考資料

ここでは、拡張テスト コマンドに関する関連資料について説明します。

関連資料

内容	参照先
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

拡張テスト コマンドの機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　拡張テスト コマンドの機能情報

機能名	リリース	機能情報
拡張テスト コマンド	12.2(4)T 12.2(28)SB 12.2(33)SRC	拡張テスト コマンド機能を使用すると、Calling Line ID（CLID; 発呼回線 ID）または Dialed Number Identification Service（DNIS; 着信番号識別サービス）アトリビュート値を持つ名前付きユーザ プロファイルを作成できます。RADIUS サーバがすべての着信コールの CLID または DNIS アトリビュート情報にアクセスできるように、CLID または DNIS アトリビュート値を、ユーザ プロファイルとともに送信される RADIUS レコードに関連付けることができます。 この機能は、Cisco IOS Release 12.2(4)T で導入されました。 この機能は、Cisco IOS Release 12.2(28)SB に統合されました。 この機能は、Cisco IOS Release 12.2(33)SRC に統合されました。 この機能により、次のコマンドが導入または変更されました。**aaa attribute**、**aaa user profile**、**test aaa group**

用語集

CLID：発呼回線 ID。CLID は、コールの発信元の番号を示します。

DNIS：着信番号識別サービス。DNIS は、ダイヤル先の番号を示します。

アトリビュート：RADIUS Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）アトリビュートは、255 の標準アトリビュートで構成されるオリジナルのセットで、クライアントとサーバ間での AAA 情報の伝達に使用されます。IETF アトリビュートは標準であるため、アトリビュート データは事前定義されてその内容も認識されています。このため、IETF アトリビュートを介して AAA 情報を交換するすべてのクライアントとサーバは、アトリビュートの厳密な意味や各アトリビュート値の一般的な限界など、アトリビュート データに一致させる必要があります。

RADIUS アカウンティング内の Framed-Route

RADIUS アカウンティング内の Framed-Route 機能は、RADIUS Accounting-Request アカウンティング レコードに Framed-Route（RADIUS アトリビュート 22）情報を挿入します。Framed-Route 情報は、Accounting-Request パケットで RADIUS サーバに返されます。Framed-Route 情報を使用すれば、ユーザ単位ルートが Network Access Server (NAS; ネットワーク アクセス サーバ) 上の特定の静的 IP 顧客に適用されているかどうかを確認できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「RADIUS アカウンティング内の Framed-Route の機能情報」（P.7）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

RADIUS アカウンティング内の Framed-Route の前提条件

Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）、RADIUS サーバ、および RADIUS アトリビュート スクリーニングの設定に精通している必要があります。

RADIUS アカウンティング内の Framed-Route に関する情報

この項では、次の概念について説明します。

- 「Framed-Route、アトリビュート 22」（P.2）
- 「RADIUS アカウンティング パケット内の Framed-Route」（P.2）

Framed-Route、アトリビュート 22

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）標準の RFC 2865 でアトリビュート 22 として定義されている Framed-Route は、NAS 上のユーザに対して設定すべきルーティング情報を提供します。通常、Framed-Route アトリビュート情報は、Access-Accept パケットで RADIUS サーバから NAS に送信されます。このアトリビュートは複数挿入できます。

RADIUS アカウンティング パケット内の Framed-Route

RADIUS アカウンティング パケット内の Framed-Route アトリビュート情報は、NAS 上の特定の静的 IP 顧客に適用されたユーザ単位ルートを表します。現在は、Framed-Route アトリビュート情報が Access-Accept パケットで送信されます。Cisco IOS Release 12.3(4)T で有効な Framed-Route アトリビュート情報は、Access-Accept パケットに挿入され、正常に適用されていれば、Accounting-Request パケットでも送信されます。Accounting-Request パケットには、0 個以上の Framed-Route アトリビュートを挿入できます。

（注） Access-Accept パケット内に複数の Framed-Route アトリビュートが存在する場合は、Accounting-Request 内にも複数の Framed-Route アトリビュートを挿入できます。

Framed-Route 情報は、accounting Delay-Start の設定時に、Stop および Interim アカウンティング レコードと Start アカウンティング レコードで返されます。

Frame-Route アトリビュート情報を RADIUS アカウンティング パケットで返すための設定は不要です。

RADIUS アカウンティング内の Framed-Route のモニタ方法

debug radius コマンドを使用して、Framed-Route（アトリビュート 22）情報が RADIUS Accounting-Request パケットで送信されているかどうかをモニタします。

例

この項では、次の例について説明します。

- 「debug radius コマンド出力：例」（P.3）

debug radius コマンド出力：例

次の例では、**debug radius** コマンドを使用して、Framed-Route（アトリビュート 22）情報が Accounting-Request パケットで送信されているかどうかを確認します（00:06:23: RADIUS: Framed-Route [22] 26 "10.80.0.1 255.255.255.255 10.60.0.1 100" の行を参照）。

```
Router# debug radius

00:06:23: RADIUS:  Send to unknown id 0 10.1.0.2:1645, Access-Request, len 126
00:06:23: RADIUS:  authenticator 40 28 A8 BC 76 D4 AA 88 - 5A E9 C5 55 0E 50 84 37
00:06:23: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
00:06:23: RADIUS:  User-Name           [1]   14  "nari@trw1001"
00:06:23: RADIUS:  CHAP-Password       [3]   19  *
00:06:23: RADIUS:  NAS-Port            [5]   6   1
00:06:23: RADIUS:  Vendor, Cisco       [26]  33
00:06:23: RADIUS:  Cisco AVpair        [1]   27  "interface=Virtual-Access1"
00:06:23: RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
00:06:23: RADIUS:  Service-Type        [6]   6   Framed                    [2]
00:06:23: RADIUS:  NAS-IP-Address      [4]   6   12.1.0.1
00:06:23: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
00:06:23: RADIUS:  Received from id 0 10.1.0.2:1645, Access-Accept, len 103
00:06:23: RADIUS:  authenticator 5D 2D 9F 25 11 15 45 B2 - 54 BB 7F EB CE 79 20 3B
00:06:23: RADIUS:  Vendor, Cisco       [26]  33
00:06:23: RADIUS:  Cisco AVpair        [1]   27  "interface=Virtual-Access1"
00:06:23: RADIUS:  Service-Type        [6]   6   Framed                    [2]
00:06:23: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
00:06:23: RADIUS:  Framed-IP-Netmask   [9]   6   255.255.255.255
00:06:23: RADIUS:  Framed-IP-Address   [8]   6   10.60.0.1
00:06:23: RADIUS:  Framed-Route        [22]  26  "10.80.0.1 255.255.255.255 10.60.0.1 100"
<=======
00:06:23: RADIUS:  Received from id 2
00:06:24: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state
to up
00:06:25: AAA/AUTHOR:  Processing PerUser AV route
00:06:25: Vi1 AAA/PERUSER/ROUTE: route string: IP route  10.80.0.1 255.255.255.255
10.60.0.1 100

00:06:25: RADIUS/ENCODE(00000002): Unsupported AAA attribute timezone
00:06:25: RADIUS(00000002): sending
00:06:25: RADIUS:  Send to unknown id 1 10.1.0.2:1646, Accounting-Request, len 278
00:06:25: RADIUS:  authenticator E0 CC 99 EB 49 18 B9 78 - 4A 09 60 0F 4E 92 24 C6
00:06:25: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
00:06:25: RADIUS:  Tunnel-Server-Endpoi[67]  12  00:"10.1.1.1"
00:06:25: RADIUS:  Tunnel-Client-Endpoi[66]  12  00:"10.1.1.2"
00:06:25: RADIUS:  Tunnel-Assignment-Id[82]  15  00:"from_isdn101"
00:06:25: RADIUS:  Tunnel-Type         [64]  6   00:L2TP                   [3]
00:06:25: RADIUS:  Acct-Tunnel-Connecti[68]  12  "2056100083"
00:06:25: RADIUS:  Tunnel-Client-Auth-I[90]  10  00:"isdn101"
00:06:25: RADIUS:  Tunnel-Server-Auth-I[91]  6   00:"lns"
00:06:25: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
00:06:25: RADIUS:  Framed-Route        [22]  39  "10.80.0.1 255.255.255.255 10.60.0.1 100"
<========
00:06:25: RADIUS:  Framed-IP-Address   [8]   6   10.60.0.1
00:06:25: RADIUS:  Vendor, Cisco       [26]  35
00:06:25: RADIUS:  Cisco AVpair        [1]   29  "connect-progress=LAN Ses Up"
```

```
00:06:25: RADIUS:  Authentic           [45]  6   RADIUS                    [1]
00:06:25: RADIUS:  User-Name           [1]   14  "username1@example.com"
00:06:25: RADIUS:  Acct-Status-Type    [40]  6   Start                     [1]
00:06:25: RADIUS:  NAS-Port            [5]   6   1
00:06:25: RADIUS:  Vendor, Cisco       [26]  33
00:06:25: RADIUS:  Cisco AVpair        [1]   27  "interface=Virtual-Access1"
00:06:25: RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
00:06:25: RADIUS:  Service-Type        [6]   6   Framed                    [2]
00:06:25: RADIUS:  NAS-IP-Address      [4]   6   10.1.0.1
00:06:25: RADIUS:  Acct-Delay-Time     [41]  6   0
```

その他の参考資料

次の項で、RADIUS アカウンティング内の Framed-Route 機能に関する参考資料を紹介します。

関連資料

内容	参照先
RADIUS	「Configuring RADIUS」モジュール

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2865	「*Remote Authentication Dial In User Service (RADIUS)*」
RFC 3575	「*IANA Considerations for RADIUS (Remote Authentication Dial In User Service)*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

RADIUS アカウンティング内の Framed-Route の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　RADIUS アカウンティング内の Framed-Route の機能情報

機能名	リリース	機能情報
RADIUS アカウンティング内の Framed-Route	12.3(4)T 12.2(28)SB 12.2(33)SRC	RADIUS アカウンティング内の Framed-Route 機能は、RADIUS Accounting-Request アカウンティング レコードに Framed-Route（RADIUS アトリビュート 22）情報を挿入します。 この機能は、Cisco IOS Release 12.3(4)T で導入されました。 この機能は、Cisco IOS Release 12.2(28)SB に統合されました。 この機能は、Cisco IOS Release 12.2(33)SRC に統合されました。

RADIUS アカウンティング内の Framed-Route の機能情報

Offload Server Accounting Enhancement

Offload Server Accounting Enhancement 機能により、ユーザは Network Access Server（NAS; ネットワーク アクセス サーバ）とオフロード サーバとの間の認証情報とアカウンティング情報を維持できます。

NAS でもオフロード サーバと情報を同期することはできますが、この機能は一意のセッション ID を含むように拡張されており、NAS によって収集される既存のセッション ID（NAS-IP-Address）および Class（アトリビュート 25）情報の前に Acct-Session-Id（アトリビュート 44）を追加します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「Offload Server Accounting Enhancement の機能情報」（P.7）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

前提条件

Offload Server Accounting Enhancement を設定する前に、次の作業を実行する必要があります。

- AAA をイネーブルにします。詳細については、「Configuring Authentication」フィーチャ モジュールを参照してください。
- VPN をイネーブルにします。詳細については、『*Cisco IOS Security Configuration Guide: Secure Connectivity*』リリース 12.4T を参照してください。

Offload Server Accounting Enhancement について

Offload Server Accounting Enhancement 機能により、ユーザは認証およびアカウンティング情報（NAS-IP-Address（アトリビュート 4）および Class（アトリビュート 25）がオフロード サーバと同期するように Network Access Server（NAS; ネットワーク アクセス サーバ）を設定できます。

オフロード サーバは、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）経由で NAS と相互作用して、コールに必要な Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）ネゴシエーションを実行します。NAS はコールの事前認証を実行し、オフロード サーバはユーザ認証を実行します。この機能を使用すると、次のように NAS の認証データとアカウンティング データをオフロード サーバと同期できます。

- 事前認証中、NAS は一意のセッション ID を生成し、既存のセッション ID（NAS-IP-Address）の前に Acct-Session-Id（アトリビュート 44）を追加して、Class アトリビュートを取得します。新しいセッション ID は事前認証要求とリソース アカウンティング要求で送信され、Class アトリビュートはリソース アカウンティング要求で送信されます。

（注） 複数の NAS が 1 台のオフロード サーバによって処理される場合は、一意のセッション ID が必要です。

- NAS-IP-Address、Acct-Session-Id、および Class アトリビュートは、Layer 2 Forwarding（L2F; レイヤ 2 フォワーディング）オプションによってオフロード サーバに送信されます。
- オフロード サーバのユーザ アクセス要求、およびユーザ セッション アカウンティング要求には、新しい、一意のセッション ID が含まれます。NAS から渡される Class アトリビュートは、ユーザ アクセス要求に含まれますが、新しい Class アトリビュートは、ユーザ アクセスへの返信で受信します。この新しい Class アトリビュートはユーザ セッション アカウンティング要求に含まれている必要があります。

Offload Server Accounting Enhancement の設定方法

Offload Server Accounting Enhancement の設定作業については、次の項を参照してください。一覧内の各作業は、必須と任意に分けています。

- 「一意のセッション ID の設定」（P.3）（必須）
- 「NAS クライアントとオフロード サーバとの同期の設定」（P.3）（必須）
- 「オフロード サーバ アカウンティングの確認」（P.3）（任意）

一意のセッション ID の設定

NAS 間で一意のセッション ID を維持するには、次のグローバル コンフィギュレーション コマンドを使用します。複数の NAS が 1 台のオフロード サーバによって処理される場合は、すべての NAS およびオフロード サーバでこの機能をイネーブルにし、共通のセッション ID と一意のセッション ID を確認する必要があります。

コマンド	目的
Router(config)# **radius-server attribute 44 extend-with-addr**	既存の AAA セッション ID の前にアカウンティング IP アドレスを追加します。 **（注）** 一意のセッション ID は、既存のセッション ID（NAS-IP-Address）の前に Acct-Session-Id（アトリビュート 44）を追加するため、他の NAS セッション ID とは異なります。

NAS クライアントとオフロード サーバとの同期の設定

アカウンティング セッション情報を NAS クライアントと同期するようにオフロード サーバを設定するには、次のグローバル コンフィギュレーション コマンドを使用します。

コマンド	目的
Router(config)# **radius-server attribute 44 sync-with-client**	アカウンティング セッション情報を NAS クライアントと同期するようにオフロード サーバを設定します。

オフロード サーバ アカウンティングの確認

NAS がオフロード サーバと認証データおよびアカウンティング データを同期しているかを確認するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **more system:running-config**	現在実行されているコンフィギュレーション ファイルの内容を表示します（**show running-config** コマンドが **more system:running-config** に置き換えられていることに注意してください）。
Router(config)# **debug radius**	RADIUS 関連の情報を表示します。このコマンドの出力は、アトリビュート 44 がアクセス要求で送信されているかどうかを示します。ただし、出力にアトリビュート 44 の値全体が示されるわけではありません。アトリビュート 44 の値全体を表示するには、RADIUS サーバ ログを参照してください。

Offload Server Accounting Enhancement の設定例

ここでは、次の設定例について説明します。

- 「一意のセッション ID の設定：例」（P.4）
- 「NAS クライアントとオフロード サーバとの同期：例」（P.4）

一意のセッション ID の設定：例

次に、NAS 間で一意のセッション ID を設定する方法の例を示します。

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 include-in-access-req
radius-server attribute 44 extend-with-addr
```

NAS クライアントとオフロード サーバとの同期：例

次に、NAS クライアントとアカウンティング セッション情報を同期するようにオフロード サーバを設定する方法の例を示します。

```
radius-server attribute 44 sync-with-client
```

その他の参考資料

ここでは、Offload Server Accounting Enhancement に関する関連資料について説明します。

関連資料

内容	参照先
VPN のイネーブル化	『*Cisco IOS Security Configuration Guide: Secure Connectivity*, Release 12.4T』
AAA のイネーブル化	「Configuring Authentication」モジュール

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに対する MIB を特定してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

Offload Server Accounting Enhancement の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　Offload Server Accounting Enhancement の機能情報

機能名	リリース	機能情報
Offload Server Accounting Enhancement	12.2(4)T 12.2(28)SB 12.2(33)SRC	Offload Server Accounting Enhancement 機能により、ユーザは Network Access Server（NAS; ネットワーク アクセス サーバ）とオフロード サーバとの間の認証情報とアカウンティング情報を維持できます。 この機能は、Cisco IOS Release 12.2(4)T で導入されました。 この機能は、Cisco IOS Release 12.2(28)SB に統合されました。 この機能は、Cisco IOS Release 12.2(33)SRC に統合されました。 この機能により、次のコマンドが導入または変更されました。**radius-server attribute 44 extend-with-addr**、**radius-server attribute 44 sync-with-client**

用語集

AAA：Authentication, Authorization, and Accounting（認証、認可、およびアカウンティング）。Cisco ルータまたはアクセス サーバにアクセス コントロールを設定できる主要なフレームワークを提供する一連のネットワーク セキュリティ サービスです。

Acct-Session-ID（アトリビュート 44）：ログ ファイル内の開始レコードと終了レコードのマッチングを容易にする一意のアカウンティング ID。Acct-Session ID の番号は、ルータの電源を入れ直したり、ソフトウェアをリロードするたびに、1 から再開します。

Class（アトリビュート 25）：アカウンティング アトリビュート。アトリビュートが RADIUS サーバによって提供されている場合、ネットワーク アクセス サーバがすべてのアカウンティング パケットに含める任意の値。

L2F：レイヤ 2 フォワーディング。レイヤ 2 トンネル プロトコルを使用すると、ISP などのアクセス サービスが仮想トンネルを作成し、顧客のリモート サイトやリモート ユーザを企業のホーム ネットワークにリンクさせることができます。具体的には、ISP Point of Presence（POP; アクセス ポイント）にある Network Access Server（NAS; ネットワーク アクセス サーバ）がリモート ユーザと PPP メッセージを交換し、L2F または L2TP の要求や応答を使用して顧客のトンネル サーバと通信し、トンネルのセットアップを行います。

NAS：Network Access Server（NAS; ネットワーク アクセス サーバ）パケットの世界（インターネットなど）と回線の世界（公衆電話交換網など）をインターフェイスするシスコ プラットフォーム（または AccessPath システムなどのプラットフォームの集合）。

NAS-IP Address（アトリビュート 4）：認証を要求するネットワーク アクセス サーバの IP アドレスを指定します。デフォルト値は 0.0.0.0/0 です。

PPP：Point-to-Point Protocol（ポイントツーポイント プロトコル）。同期回線と非同期回線上でルータ間接続とホスト / ネットワーク間接続を提供する SLIP の代替プロトコル。SLIP は IP と連動するように設計されているのに対して、PPP は IP、IPX、ARA などの複数のネットワーク レイヤ プロトコルと連動するように設計されています。PPP には、CHAP および PAP などの組み込みのセキュリティ メカニズムもあります。PPP は LCP と NCP の 2 つのプロトコルに依存します。

RADIUS：Remote Authentication Dial-In User Service。RADIUS は、不正アクセスからネットワークを保護する分散型クライアント / サーバ システムです。シスコの実装では RADIUS クライアントは Cisco ルータ上で稼動します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

VPN：リモートでダイヤルイン ネットワークをホーム ネットワークに存在させ、あたかも直接接続されているかのように見せるシステム。VPN は、L2TP および L2F を使用し、LAC ではなく、LNS でレイヤ 2 およびより高次のネットワーク接続を終了させます。

Per VRF AAA

Per VRF AAA 機能により、ISP は、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サービスを Virtual Private Network（VPN; バーチャル プライベート ネットワーク）Routing and Forwarding（VRF; VPN ルーティングおよび転送）インスタンスに基づいて区分して、カスタマーに独自の AAA サービスの一部を制御させることができます。

サーバ グループのサーバ リストは、グローバル コンフィギュレーションでのホストへの参照に加えて、プライベート サーバの定義を含めるために拡張されています。このため、カスタマー サーバとグローバル サービス プロバイダーのサーバに同時にアクセスできます。

Cisco IOS Release 12.2(15)T 以降のリリースでは、ローカルまたはリモートで保存したカスタマー テンプレートを使用し、カスタマー テンプレートに保存された情報に基づいて、AAA サービスを実行できます。この機能は、Dynamic Per VRF AAA 機能とも呼ばれていました。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「Per VRF AAA の機能情報」（P.33）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

Per VRF AAA の前提条件

Per VRF AAA 機能を設定する前に、AAA をイネーブルにする必要があります。詳細については、「Per VRF AAA の設定方法」（P.6）を参照してください。

Per VRF AAA の制約事項

- この機能は、RADIUS サーバについてのみサポートされています。
- すべての機能について、Network Access Server（NAS; ネットワーク アクセス サーバ）と AAA サーバとの間で一貫性が必要なため、サーバ グループごとの設定ではなく、Per VRF を設定したら、動作パラメータを定義する必要があります。
- ローカルまたはリモートでカスタマー テンプレートを設定する機能は、Cisco IOS Release 12.2(15)T 以降のリリースでのみ使用できます。

Per VRF AAA について

Per VRF AAA 機能を使用する場合、AAA サービスを VRF インスタンスに基づいたものにできます。この機能により、Provider Edge（PE; プロバイダー エッジ）または Virtual Home Gateway（VHG; 仮想ホーム ゲートウェイ）で、カスタマーの Virtual Private Network（VPN; バーチャル プライベート ネットワーク）に関連付けられたカスタマーの RADIUS サーバと RADIUS プロキシを経由せずに直接通信できます。RADIUS プロキシを使用する必要がないため、ISP は、VPN による提供サービスをより効率的に拡張でき、カスタマーにさらに柔軟性を提供できます。

Per VRF AAA の機能

カスタマーごとに AAA をサポートするには、一部の AAA 機能をで VRF を認識させる必要があります。つまり、ISP は、AAA サーバ グループ、方式リスト、システム アカウンティング、およびプロトコル固有のパラメータなどの動作パラメータを定義し、これらのパラメータを特定の VRF インスタンスにバインドできる必要があります。動作パラメータの定義とバインディングには、次の 1 つ以上の方式が使用できます。

- Virtual Private Dial-up Network（VPDN; バーチャル プライベート ダイヤルアップ ネットワーク）：特定のカスタマーに設定されたに仮想テンプレートまたはダイヤラ インターフェイス。

- ローカルで定義されたカスタマー テンプレート：カスタマーの定義による Per VPN。カスタマー テンプレートは、ローカルで VHG に保存されます。この方式は、ドメイン名または Dialed Number Identification Service（DNIS; 着信番号識別サービス）に基づいて、リモート ユーザを特定の VPN に関連付け、カスタマーの AAA サーバに対する仮想アクセス インターフェイスおよびすべての動作パラメータに VPN 固有の設定を提供する場合に使用できます。
- リモートで定義されたカスタマー テンプレート：RADIUS プロファイルでサービス プロバイダーの AAA サーバに保存された、カスタマーの定義による Per VPN。この方式は、ドメイン名または DNIS に基づいて、リモート ユーザを特定の VPN に関連付け、カスタマーの AAA サーバに対する仮想アクセス インターフェイスおよびすべての動作パラメータに VPN 固有の設定を提供する場合に使用できます。

（注） ローカルまたはリモートで定義されたカスタマー テンプレートを設定する機能は、Cisco IOS Release 12.2(15)T 以降のリリースでのみ使用できます。

AAA アカウンティング レコード

シスコが採用している AAA アカウンティングでは、ユーザ認証を通過したコールに対する「開始」レコードと「終了」レコードがサポートされます。開始レコードと終了レコードは、ユーザがアカウンティング レコードを使用してネットワークを管理およびモニタするために必要です。

新しいベンダー固有アトリビュート

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）ドラフト標準には、ネットワーク アクセス サーバと RADIUS サーバの間で Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）アトリビュート 26 を使用してベンダー固有の情報を伝達する方法が規定されています。アトリビュート 26 は VSA をカプセル化します。このため、ベンダーは一般的な用途に適さない独自の拡張アトリビュートをサポートできます。

シスコの RADIUS 実装では、IETF 仕様で推奨される形式を使用したベンダー固有オプションを 1 つサポートしています。シスコのベンダー ID は 9 で、サポートするオプションはベンダー タイプ 1、名前は「cisco-av-pair」です。値は次の形式のストリングです。

```
protocol : attribute sep value *
```

「Protocol」は、特定の認可タイプを表すシスコの「protocol」アトリビュートです。「Attribute」と「value」は、シスコの TACACS+ 仕様に定義されている適切なアトリビュート値（AV）ペアで、「sep」は必須アトリビュートの場合には「=」、オプションのアトリビュートの場合に「*」を使用します。これにより、TACACS+ 認可で使用できるすべての機能を RADIUS にも使用できるようになります。

表 1 に、現在 Per VRF AAA でサポートされている VSA の概要を示します。

表 1　Per VRF AAA でサポートされる VSA

VSA 名	値の種類	説明
（注）　別の拡張子が明示的に記述されている場合を除き、各 VSA には VSA 名の前に拡張子「template:」が必要です。		
account-delay	string	この VSA は「on」にする必要があります。この VSA の機能は、カスタマー テンプレートの **aaa accounting delay-start** コマンドと同じです。
account-send-stop	string	この VSA は「on」にする必要があります。この VSA の機能は、**failure** キーワードを指定した **aaa accounting send stop-record authentication** コマンドと同じです。
account-send-success-remote	string	この VSA は「on」にする必要があります。この VSA の機能は、**success** キーワードを指定した **aaa accounting send stop-record authentication** コマンドと同じです。
attr-44	string	この VSA は「access-req」にする必要があります。この VSA の機能は、**radius-server attribute 44 include-in-access-req** コマンドと同じです。
ip-addr	string	この VSA は、IP アドレスを指定します。その後に、ルータが独自の IP アドレスを示すために使用するマスク、およびクライアントとのネゴシエーションのマスクが続きます。例：ip-addr=192.168.202.169 255.255.255.255。
ip-unnumbered	string	この VSA は、ルータ上のインターフェイスの名前を指定します。この VSA の機能は、「Loopback 0」などのインターフェイス名を指定する **ip unnumbered** コマンドと同じです。
ip-vrf	string	この VSA は､エンド ユーザのパケットに使用する VRF を指定します。この VRF 名は、**ip vrf forwarding** コマンドを使用してルータに使用する名前に一致させる必要があります。
peer-ip-pool	string	この VSA は、ピアに割り当てられるアドレスの IP アドレス プールの名前を指定します。このプールは、**ip local pool** コマンドを使用して設定するか、RADIUS 経由で自動的にダウンロード可能にする必要があります。

VSA 名	値の種類	説明
ppp-acct-list	string	この VSA は、PPP セッションに使用するアカウンティング方式リストを定義します。 VSA 構文は次のとおりです。「ppp-acct-list=[start-stop | stop-only | none] group X [group Y] [broadcast]」これは、**aaa accounting network mylist** コマンド機能と等しくなります。 ユーザは、start-stop、stop-only、または none オプションを少なくとも 1 つ指定する必要があります。start-stop または stop-only を指定した場合、ユーザは少なくとも 1 つ、ただし 4 つ以内のグループ引数を指定する必要があります。各グループ名は、整数で構成する必要があります。グループ内のサーバは、VSA「rad-serv」を経由して、access-accept で識別されている必要があります。各グループが指定されると、ユーザはブロードキャストオプションを指定できます。
ppp-authen-list	string	この VSA は、PPP セッションで使用する認証方式リスト、および複数の方式が指定されている場合は、方式を使用する順序を定義します。 VSA 構文は次のとおりです。「ppp-authen-list=[groupX | local | local-case | none | if-needed]」これは、**aaa authentication ppp mylist** コマンド機能と等しくなります。 ユーザは少なくとも 1 つ、ただし 4 つ以内の認証方式を指定する必要があります。サーバ グループが指定されている場合、グループ名は整数である必要があります。グループ内のサーバは、VSA「rad-serv」を経由して、access-accept で識別されている必要があります。
ppp-authen-type	string	この VSA を使用すると、エンド ユーザは、pap、chap、eap、ms-chap、ms-chap-v2、any のいずれかの認証タイプ、または使用可能なタイプをスペースで区切って、少なくとも 1 つの認証タイプを指定できます。 エンド ユーザは、この VSA で指定された方式のみを使用して、ログインが許可されます。 PPP はアトリビュートで提示された順序で、これらの認証方式を試行します。
ppp-author-list	string	この VSA は、PPP セッションに使用する認可方式リストを定義します。使用する方式と順序を示します。 VSA 構文は次のとおりです。「ppp-author-list=[groupX] [local] [if-authenticated] [none]」これは、**aaa authorization network mylist** コマンド機能に等しくなります。 ユーザは少なくとも 1 つ、ただし 4 つ以内の認可方式を指定する必要があります。サーバ グループが指定されている場合、グループ名は整数である必要があります。グループ内のサーバは、VSA「rad-serv」を経由して、access-accept で識別されている必要があります。

VSA 名	値の種類	説明
（注） RADIUS VSAs—rad-serv、rad-server-filter、rad-serv-source-if、および rad-serv-vrf : VSA 名の前に拡張子「aaa:」が必要です。		
rad-serv	string	この VSA は、サーバのグループとともに、IP アドレス、キー、タイムアウト、およびサーバの再送信回数を示します。 VSA 構文は次のとおりです。「rad-serv=a.b.c.d [key SomeKey] [auth-port X] [acct-port Y] [retransmit V] [timeout W]」IP アドレス以外、すべてのパラメータはオプションで、任意の順序で発行できます。オプションのパラメータが指定されていない場合、デフォルト値が使用されます。 キーにスペースを含めることはできません。「retransmit V」では「V」は、1 ～ 100 の範囲、「timeout W」では「W」は、1 ～ 1000 の範囲で指定できます。
rad-serv-filter	string	VSA 構文は次のとおりです。 「rad-serv-filter=authorization | accounting-request | reply-accept | reject-filtername」フィルタ名は、**radius-server attribute list filtername** コマンドを使用して定義する必要があります。
rad-serv-source-if	string	この VSA は、RADIUS パケットの送信に使用するインターフェイスの名前を指定します。指定されたインターフェイスは、ルータ上に設定されたインターフェイスと一致する必要があります。
rad-serv-vrf	string	この VSA は、RADIUS パケットの送信に使用する VRF の名前を指定します。VRF 名は、**ip vrf forwarding** コマンドを使用して指定された名前と一致する必要があります。

Per VRF AAA の設定方法

ここでは、Per VRF AAA 機能を使用して考えられる導入シナリオに関する手順について説明します。

- 「Per VRF AAA の設定」（P.6）（必須）
- 「ローカル カスタマー テンプレートを使用した Per VRF AAA の設定」（P.13）（任意）
- 「リモート カスタマー テンプレートを使用した Per VRF AAA の設定」（P.17）（任意）
- 「VRF ルーティングの設定確認」（P.20）（任意）
- 「Per VRF AAA 設定のトラブルシューティング」（P.21）（任意）

Per VRF AAA の設定

ここでは、次の各手順について説明します。

- 「AAA の設定」（P.7）
- 「サーバ グループの設定」（P.7）
- 「Per VRF AAA の認証、認可、およびアカウンティングの設定」（P.8）

- 「Per VRF AAA の RADIUS 固有のコマンドの設定」（P.11）
- 「Per VRF AAA のインターフェイス固有のコマンドの設定」（P.12）

AAA の設定

AAA をイネーブルにするには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **ip vrf default**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： Router(config)# aaa new-model	AAA をグローバルにイネーブルにします。
ステップ 4	**ip vrf default** 例： Router(config)# ip vrf default	デフォルトの VRF 名が設定されるまで、デフォルトの VRF 名がヌル値になるように、このコマンドは、**radius-server domain-stripping** コマンドなどの VRF 関連の AAA コマンドを設定する前に設定する必要があります。

サーバ グループの設定

サーバ グループを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius** *groupname*
5. **server-private** *ip-address* [**auth-port port-number** | **acct-port port-number**] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Router(config)# aaa new-model`	AAA をグローバルにイネーブルにします。
ステップ 4	**aaa group server radius** *groupname* 例： `Router(config)# aaa group server radius v2.44.com`	複数の RADIUS サーバ ホストを別々のリストと別々の方式にグループ分けします。server-group コンフィギュレーション モードを開始します。
ステップ 5	**server-private** *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] 例： `Router(config-sg-radius)# server-private 10.10.130.2 auth-port 1600 key ww`	グループ サーバに対するプライベート RADIUS サーバの IP アドレスを設定します。 （注） プライベート サーバ パラメータが指定されていない場合、グローバル コンフィギュレーションが使用されます。グローバル コンフィギュレーションが指定されていない場合、デフォルト値が使用されます。
ステップ 6	**exit** 例： `Router(config-sg-radius)# exit`	server-group コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

Per VRF AAA の認証、認可、およびアカウンティングの設定

Per VRF AAA の認証、認可、およびアカウンティングを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
5. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} *method1* [*method2...*]
6. **aaa accounting system default** [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname*

7. **aaa accounting delay-start** [**vrf** *vrf-name*]
8. **aaa accounting send stop-record authentication** {**failure** | **success remote-server**} [**vrf** *vrf-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Router(config)# aaa new-model`	AAA をグローバルにイネーブルにします。
ステップ 4	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*] 例： `Router(config)# aaa authentication ppp method_list_v2.44.com group v2.44.com`	PPP を実行するシリアル インターフェイス上で使用する 1 つ以上の AAA 認証方式を指定します。
ステップ 5	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} *method1* [*method2...*] 例： `Router(config)# aaa authorization network method_list_v2.44.com group v2.44.com`	ネットワークへのユーザ アクセスを制限するパラメータを設定します。
ステップ 6	**aaa accounting system default** [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname* 例： `Router(config)# aaa accounting system default vrf v2.44.com start-stop group v2.44.com`	課金、または RADIUS を使用する際のセキュリティのために、要求されたサービスの AAA アカウンティングをイネーブルにします。 （注） **stop-only** キーワードは、Cisco IOS Release 12.4(24)T 以降のリリースでは使用できません。

	コマンドまたはアクション	目的
ステップ 7	**aaa accounting delay-start** [**vrf** *vrf-name*] 例： `Router(config)# aaa acounting delay-start vrf v2.44.com`	ユーザの IP アドレスが確立されるまで、アカウンティング開始レコードの生成を表示します。
ステップ 8	**aaa accounting send stop-record authentication** {**failure** | **success remote-server**} [**vrf** *vrf-name*] 例： `Router(config)# aaa accounting send stop-record authentication failure vrf v2.44.com`	アカウンティング終了レコードを生成します。 **failure** キーワードを使用すると、認証中に拒否されたコールに対する「終了」レコードが送信されます。 **success** キーワードを使用すると、次のいずれかの基準を満たすコールに対して、「終了」レコードが送信されます。 • コールが終了したときに、リモート AAA サーバによって認証されるコール。 • リモート AAA サーバによって認証されず、開始レコードが送信されたコール。 • 正常に確立され、「stop-only」**aaa accounting** 設定で終了したコール。 （注） **success** および **remote-server** キーワードは、Cisco IOS Release 12.4(2)T 以降のリリースで使用できます。 （注） **success** および **remote-server** キーワードは、Cisco IOS Release 12.2SX では使用できません。

Per VRF AAA の RADIUS 固有のコマンドの設定

Per VRF AAA の RADIUS 固有のコマンドを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip radius source-interface** *subinterface-name* [**vrf** *vrf-name*]
4. **radius-server attribute 44 include-in-access-req** [**vrf** *vrf-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip radius source-interface** *subinterface-name* [**vrf** *vrf-name*] 例： `Router(config)# ip radius source-interface loopback55`	すべての発信 RADIUS パケットに対して、RADIUS に指定されたインターフェイスの IP アドレスを強制的に使用させ、Per VRF に基づいて仕様をイネーブルにします。
ステップ 4	**radius-server attribute 44 include-in-access-req** [**vrf** *vrf-name*] 例： `Router(config)# radius-server attribute 44 include-in-access-req vrf v2.44.com`	ユーザ認証前に、アクセス要求パケットで、RADIUS アトリビュート 44 を送信し、Per VRF に基づいて仕様を有効にします。

Per VRF AAA のインターフェイス固有のコマンドの設定

Per VRF AAA でインターフェイス固有のコマンドを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip vrf forwarding** *vrf-name*
5. **ppp authentication** {*protocol1* [*protocol2...*]} *listname*
6. **ppp authorization** *list-name*
7. **ppp accounting default**
8. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* [*name-tag*] **例：** `Router(config)# interface loopback11`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip vrf forwarding** *vrf-name* **例：** `Router(config-if)# ip vrf forwarding v2.44.com`	インターフェイスと VRF を関連付けます。
ステップ 5	**ppp authentication** {*protocol1* [*protocol2*...]} *listname* **例：** `Router(config-if)# ppp authentication chap callin V2_44_com`	Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）および Password Authentication Protocol（PAP; パスワード認証プロトコル）または両方をイネーブルにし、インターフェイス上で、CHAP または PAP 認証が選択される順序を指定します。
ステップ 6	**ppp authorization** *list-name* **例：** `Router(config-if)# ppp authorization V2_44_com`	選択したインターフェイスで、AAA 認可をイネーブルにします。
ステップ 7	**ppp accounting default** **例：** `Router(config-if)# ppp accounting default`	選択したインターフェイスで、AAA アカウンティング サービスをイネーブルにします。
ステップ 8	**exit** **例：** `Router(config)# exit`	インターフェイス コンフィギュレーション モードを終了します。

ローカル カスタマー テンプレートを使用した Per VRF AAA の設定

ここでは、次の各手順について説明します。

- 「ローカル カスタマー テンプレートを使用した AAA の設定」（P.14）
- 「ローカル カスタマー テンプレートを使用したサーバ グループの設定」（P.14）
- 「ローカル カスタマー テンプレートを使用した Per VRF AAA の認証、認可、およびアカウンティングの設定」（P.14）
- 「ローカル カスタマー テンプレートを使用した Per VRF AAA の認可の設定」（P.14）
- 「ローカル カスタマー テンプレートの設定」（P.14）

ローカル カスタマー テンプレートを使用した AAA の設定

「AAA の設定」（P.7）で説明する作業を実行します。

ローカル カスタマー テンプレートを使用したサーバ グループの設定

「サーバ グループの設定」（P.7）で説明する作業を実行します。

ローカル カスタマー テンプレートを使用した Per VRF AAA の認証、認可、およびアカウンティングの設定

「Per VRF AAA の認証、認可、およびアカウンティングの設定」（P.8）で説明する作業を実行します。

ローカル カスタマー テンプレートを使用した Per VRF AAA の認可の設定

ローカル テンプレートを使用して Per VRF AAA の認可を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authorization template**
4. **aaa authorization network default local**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa authorization template** 例： `Router(config)# aaa authorization template`	ローカルまたはリモート テンプレートの使用をイネーブルにします。
ステップ 4	**aaa authorization network default local** 例： `Router(config)# aaa authorization network default local`	ローカルを認可のデフォルト方式として指定します。

ローカル カスタマー テンプレートの設定

ローカル カスタマー テンプレートを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **vpdn search-order domain**
4. **template** *name* [**default** | **exit** | **multilink** | **no** | **peer** | **ppp**]
5. **peer default ip address pool** *pool-name*
6. **ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**]
7. **ppp authorization** [**default** | *list-name*]
8. **aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname*
9. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn search-order domain** 例： `Router (config)# vpdn search-order domain`	ドメインに基づいてプロファイルを検索します。
ステップ 4	**template** *name* [**default** | **exit** | **multilink** | **no** | **peer** | **ppp**] 例： `Router (config)# template v2.44.com`	カスタマー プロファイル テンプレートを作成し、受信先のカスタマーに関連する一意の名前を割り当てます。 テンプレート コンフィギュレーション モードを開始します。 **（注）** ステップ 5、6、および 7 はオプションです。カスタマー アプリケーション要件に適した **multilink**、**peer**、および **ppp** キーワードを入力します。
ステップ 5	**peer default ip address pool** *pool-name* 例： `Router(config-template)# peer default ip address pool v2_44_com_pool`	（任意）このテンプレートの添付先のカスタマー プロファイルが、指定した名前のローカル IP アドレス プールを使用するように指定します。
ステップ 6	**ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] 例： `Router(config-template)# ppp authentication chap`	（任意）PPP リンク認証方式を設定します。
ステップ 7	**ppp authorization** [**default** | *list-name*] 例： `Router(config-template)# ppp authorization v2_44_com`	（任意）PPP リンク認可方式を設定します。

	コマンドまたはアクション	目的
ステップ 8	**aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname* **例：** `Router(config-template)# aaa accounting v2_44_com`	（任意）指定したカスタマー プロファイルで、AAA 動作パラメータをイネーブルにします。
ステップ 9	**exit** **例：** `Router(config-template)# exit`	テンプレート コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

リモート カスタマー テンプレートを使用した Per VRF AAA の設定

ここでは、次の各手順について説明します。

- 「リモート カスタマー テンプレートを使用した AAA の設定」（P.18）
- 「サーバ グループの設定」（P.18）

- 「リモート カスタマー テンプレートを使用した Per VRF AAA の認証の設定」（P.18）
- 「リモート カスタマー テンプレートを使用した Per VRF AAA の認可の設定」（P.19）
- 「SP RADIUS サーバ上の RADIUS プロファイルの設定」（P.20）

リモート カスタマー テンプレートを使用した AAA の設定

「AAA の設定」（P.7）で説明する作業を実行します。

サーバ グループの設定

「サーバ グループの設定」（P.7）で説明する作業を実行します。

リモート カスタマー テンプレートを使用した Per VRF AAA の認証の設定

リモート カスタマー テンプレートを使用して Per VRF AAA の認証を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
4. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2...*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2*...] 例： Router(config)# ppp authentication ppp default group radius	PPP を実行するシリアル インターフェイス上で使用する 1 つ以上の Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）認証方式を指定します。
ステップ 4	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2*...] 例： Router(config)# aaa authorization network default group sp	ネットワークへのユーザ アクセスを制限するパラメータを設定します。

リモート カスタマー テンプレートを使用した Per VRF AAA の認可の設定

リモート カスタマー テンプレートを使用して Per VRF AAA の認可を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authorization template**
4. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2*...]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa authorization template** **例：** `Router(config)# aaa authorization template`	ローカルまたはリモート テンプレートの使用をイネーブルにします。
ステップ 4	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2...*] **例：** `Router(config)# aaa authorization network default sp`	認可のデフォルト方式として指定されたサーバ グループを指定します。

SP RADIUS サーバ上の RADIUS プロファイルの設定

RADIUS プロファイルのアップデート方法の例については、「リモート RADIUS カスタマー テンプレートを使用した Per VRF AAA：例」（P.23）を参照してください。

VRF ルーティングの設定確認

VRF ルーティングの設定確認には、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **show ip route vrf** *vrf-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**show ip route vrf** *vrf-name* 例： Router(config)# show ip route vrf northvrf	VRF に関連付けられた IP ルーティング テーブルを表示します。

Per VRF AAA 設定のトラブルシューティング

Per VRF AAA 機能のトラブルシューティングを行う場合は、EXEC モードで次のコマンドを少なくとも 1 つ使用します。

コマンド	目的
Router# **debug aaa accounting**	説明の義務があるイベントが発生したときに、その情報を表示します。
Router# **debug aaa authentication**	AAA 認証に関する情報を表示します。
Router# **debug aaa authorization**	AAA 認証に関する情報を表示します。
Router# **debug ppp negotiation**	PPP を実装するインターネットワークでのトラフィックおよび交換に関する情報を表示します。
Router# **debug radius**	RADIUS 関連の情報を表示します。
Router# **debug vpdn event**	VPN の通常のトンネルの確立、またはシャットダウンの一部である Layer 2 Transport Protocol（L2TP; レイヤ 2 プロトコル）のエラーおよびイベントを表示します。
Router# **debug vpdn error**	VPN のデバッグ トレースを表示します。

Per VRF AAA の設定例

ここでは、次の設定例について説明します。

- 「Per VRF の設定：例」（P.22）
- 「カスタマー テンプレート：例」（P.23）
- 「AAA アカウンティング終了レコード：例」（P.25）

Per VRF の設定：例

ここでは、次の設定例について説明します。

- 「Per VRF AAA：例」（P.22）
- 「ローカルで定義されたカスタマー テンプレートを使用した Per VRF AAA：例」（P.22）
- 「リモート RADIUS カスタマー テンプレートを使用した Per VRF AAA：例」（P.23）

Per VRF AAA：例

次に、関連付けられたプライベート サーバで AAA サーバ グループを使用して Per VRF AAA 機能を設定する方法の例を示します。

```
aaa new-model

aaa authentication ppp method_list_v1.55.com group v1.55.com
aaa authorization network method_list_v1.55.com group v1.55.com
aaa accounting network method_list_v1.55.com start-stop group v1.55.com
aaa accounting system default vrf v1.55.com start-stop group v1.55.com
aaa accounting delay-start vrf v1.55.com
aaa accounting send stop-record authentication failure vrf v1.55.com

aaa group server radius v1.55.com
    server-private 10.10.132.4 auth-port 1645 acct-port 1646 key ww
    ip vrf forwarding v1.55.com

ip radius source-interface loopback55
radius-server attribute 44 include-in-access-req vrf v1.55.com
```

ローカルで定義されたカスタマー テンプレートを使用した Per VRF AAA：例

次に、関連付けられたプライベート サーバのある AAA サーバ グループで、ローカルで定義されたカスタマー テンプレートを使用して Per VRF AAA 機能を設定する方法の例を示します。

```
aaa new-model
aaa authentication ppp method_list_v1.55.com group v1.55.com
aaa authorization network method_list_v1.55.com group v1.55.com
aaa authorization network default local
aaa authorization template
aaa accounting network method_list_v1.55.com start-stop group v1.55.com
aaa accounting system default vrf v1.55.com start-stop group v1.55.com

aaa group server radius V1_55_com
  server-private 10.10.132.4 auth-port 1645 acct-port 1646 key ww
  ip vrf forwarding V1.55.com

template V1.55.com
  peer default ip address pool V1_55_com_pool
  ppp authentication chap callin V1_55_com
  ppp authorization V1_55_com
  ppp accounting V1_55_com
  aaa accounting delay-start
  aaa accounting send stop-record authentication failure
  radius-server attribute 44 include-in-access-req
  ip vrf forwarding v1.55.com
  ip radius source-interface Loopback55
```

リモート RADIUS カスタマー テンプレートを使用した Per VRF AAA：例

次に、関連付けられたプライベート サーバのある AAA サーバ グループで、SP RADIUS サーバ上にリモートで定義したカスタマー テンプレートを使用して Per VRF AAA 機能を設定する方法の例を示します。

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization template
aaa authorization network default group sp

aaa group server radius sp
   server 10.3.3.3

radius-server host 10.3.3.3 auth-port 1645 acct-port 1646 key sp_key
```

次の RADIUS サーバ プロファイルは、SP RADIUS サーバ上で設定されます。

```
cisco-avpair = "aaa:rad-serv#1=10.10.132.4 key ww"
cisco-avpair = "aaa:rad-serv-vrf#1=V1.55.com"
cisco-avpair = "aaa:rad-serv-source-if#1=Loopback 55"
cisco-avpair = "template:ppp-authen-list=group 1"
cisco-avpair = "template:ppp-author-list=group 1"
cisco-avpair = "template:ppp-acct-list= start-stop group 1"
cisco-avpair = "template:account-delay=on"
cisco-avpair = "template:account-send-stop=on"
cisco-avpair = "template:rad-attr44=access-req"
cisco-avpair = "template:peer-ip-pool=V1.55-pool"
cisco-avpair = "template:ip-vrf=V1.55.com"
cisco-avpair = "template:ip-unnumbered=Loopback 55"
framed-protocol = ppp
service-type = framed
```

カスタマー テンプレート：例

ここでは、次の設定例について説明します。

- 「RADIUS Attribute Screening およびブロードキャスト アカウンティングを使用してローカルで設定されたカスタマー テンプレート：例」（P.23）
- 「RADIUS Attribute Screening およびブロードキャスト アカウンティングを使用してリモートで設定されたカスタマー テンプレート：例」（P.24）

RADIUS Attribute Screening およびブロードキャスト アカウンティングを使用してローカルで設定されたカスタマー テンプレート：例

次に、RADIUS Attribute Screening およびブロードキャスト アカウンティングを含む追加機能を設定する、単一のカスタマー向けにローカルで設定されたテンプレートを作成する方法の例を示します。

```
aaa authentication ppp default local group radius
aaa authentication ppp V1_55_com group V1_55_com
aaa authorization template
aaa authorization network default local group radius
aaa authorization network V1_55_com group V1_55_com
aaa accounting network V1_55_com start-stop broadcast group V1_55_com group SP_AAA_server

aaa group server radius SP_AAA_server
 server 10.10.100.7 auth-port 1645 acct-port 1646
```

```
aaa group server radius V1_55_com
 server-private 10.10.132.4 auth-port 1645 acct-port 1646
 authorization accept min-author
 accounting accept usage-only
 ip vrf forwarding V1.55.com

ip vrf V1.55.com
 rd 1:55
 route-target export 1:55
 route-target import 1:55

template V1.55.com
 peer default ip address pool V1.55-pool
 ppp authentication chap callin V1_55_com
 ppp authorization V1_55_com
 ppp accounting V1_55_com
 aaa accounting delay-start
 aaa accounting send stop-record authentication failure
 radius-server attribute 44 include-in-access-req

vpdn-group V1.55
 accept-dialin
  protocol l2tp
  virtual-template 13
 terminate-from hostname lac-lb-V1.55
 source-ip 10.10.104.12
 lcp renegotiation always
 l2tp tunnel password 7 060506324F41

interface Virtual-Template13
 ip vrf forwarding V1.55.com
 ip unnumbered Loopback55
 ppp authentication chap callin
 ppp multilink

ip local pool V1.55-pool 10.1.55.10 10.1.55.19 group V1.55-group

ip radius source-interface Loopback0
ip radius source-interface Loopback55 vrf V1.55.com

radius-server attribute list min-author
 attribute 6-7,22,27-28,242
radius-server attribute list usage-only
 attribute 1,40,42-43,46

radius-server host 10.10.100.7 auth-port 1645 acct-port 1646 key ww
radius-server host 10.10.132.4 auth-port 1645 acct-port 1646 key ww
```

RADIUS Attribute Screening およびブロードキャスト アカウンティングを使用してリモートで設定されたカスタマー テンプレート：例

次に、RADIUS Attribute Screening およびブロードキャスト アカウンティングを含む追加機能を設定する、単一のカスタマー向けにリモートで設定されたテンプレートを作成する方法の例を示します。

```
aaa authentication ppp default local group radius
aaa authorization template
aaa authorization network default local group radius

ip vrf V1.55.com
 rd 1:55
 route-target export 1:55
 route-target import 1:55
```

```
vpdn-group V1.55
 accept-dialin
  protocol l2tp
  virtual-template 13
 terminate-from hostname lac-lb-V1.55
 source-ip 10.10.104.12
 lcp renegotiation always
 l2tp tunnel password 7 060506324F41

interface Virtual-Template13
 no ip address
 ppp authentication chap callin
 ppp multilink

ip local pool V1.55-pool 10.1.55.10 10.1.55.19 group V1.55-group

radius-server attribute list min-author
 attribute 6-7,22,27-28,242
radius-server attribute list usage-only
 attribute 1,40,42-43,46
```

カスタマー テンプレートは、v1.55.com の RADIUS サーバ プロファイルとして保存されます。

```
cisco-avpair = "aaa:rad-serv#1=10.10.132.4 key ww"
cisco-avpair = "aaa:rad-serv-vrf#1=V1.55.com"
cisco-avpair = "aaa:rad-serv-source-if#1=Loopback 55"
cisco-avpair = "aaa:rad-serv#2=10.10.100.7 key ww"
cisco-avpair = "aaa:rad-serv-source-if#2=Loopback 0"
cisco-avpair = "template:ppp-authen-list=group 1"
cisco-avpair = "template:ppp-author-list=group 1"
cisco-avpair = "template:ppp-acct-list= start-stop group 1 group 2 broadcast"
cisco-avpair = "template:account-delay=on"
cisco-avpair = "template:account-send-stop=on"
cisco-avpair = "template:rad-attr44=access-req"
cisco-avpair = "aaa:rad-serv-filter#1=authorization accept min-author"
cisco-avpair = "aaa:rad-serv-filter#1=accounting accept usage-only"
cisco-avpair = "template:peer-ip-pool=V1.55-pool"
cisco-avpair = "template:ip-vrf=V1.55.com"
cisco-avpair = "template:ip-unnumbered=Loopback 55"
framed-protocol = ppp
service-type = framed
```

AAA アカウンティング終了レコード：例

次に、**start-stop** または **stop-only** キーワードを指定して **aaa accounting** コマンドを発行したときに、「終了」レコードの生成を制御する **aaa accounting send stop-record authentication** コマンドを設定する方法を示す、AAA アカウンティング終了レコードの例を示します。

（注） **success** および **remote-server** キーワードは、Cisco IOS Release 12.4(2)T 以降のリリースで使用できます。

ここでは、次の設定例について説明します。

- 「AAA アカウンティング終了レコードと成功したコール：例」（P.26）
- 「AAA アカウンティング終了レコードと拒否されたコール：例」（P.28）

AAA アカウンティング終了レコードと成功したコール：例

次に、**aaa accounting send stop-record authentication** コマンドを **failure** キーワードを指定して発行した場合に、成功したコールに関する「開始」および「終了」レコードが送信されている例を示します。

```
Router# show running-config | include aaa
.
.
.
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting send stop-record authentication failure
aaa accounting network default start-stop group radius
.
.
.
*Jul  7 03:28:31.543: AAA/BIND(00000018): Bind i/f Virtual-Template2
*Jul  7 03:28:31.547: ppp14 AAA/AUTHOR/LCP: Authorization succeeds trivially
*Jul  7 03:28:33.555: AAA/AUTHOR (0x18): Pick method list 'default'
*Jul  7 03:28:33.555: AAA/BIND(00000019): Bind i/f
*Jul  7 03:28:33.555:  Tnl 5192 L2TP: O SCCRQ
*Jul  7 03:28:33.555:  Tnl 5192 L2TP: O SCCRQ, flg TLS, ver 2, len 141, tnl 0,
ns 0, nr 0
         C8 02 00 8D 00 00 00 00 00 00 00 00 80 08 00 00
         00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
         00 06 11 30 80 10 00 00 00 07 4C 41 43 2D 74 75
         6E 6E 65 6C 00 19 00 00 00 08 43 69 73 63 6F 20
         53 79 73 74 65 6D 73 ...
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 0, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse SCCRP
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 2, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Protocol Ver 256
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 3, len 10, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Framing Cap 0x0
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 4, len 10, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Bearer Cap 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 6, len 8, flag 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Firmware Ver 0x1120
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 7, len 16, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Hostname LNS-tunnel
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 8, len 25, flag 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Vendor Name Cisco Systems, Inc.
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 9, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Assigned Tunnel ID 6897
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 10, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Rx Window Size 20050
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 11, len 22, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Chlng
         81 13 03 F6 A8 E4 1D DD 25 18 25 6E 67 8C 7C 39
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 13, len 22, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Chlng Resp
         4D 52 91 DC 1A 43 B3 31 B4 F5 B8 E1 88 22 4F 41
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: No missing AVPs in SCCRP
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: I SCCRP, flg TLS, ver 2, len 157, tnl
5192, ns 0, nr 1
contiguous pak, size 157
         C8 02 00 9D 14 48 00 00 00 00 00 01 80 08 00 00
         00 00 00 02 80 08 00 00 00 02 01 00 80 0A 00 00
         00 03 00 00 00 00 80 0A 00 00 00 04 00 00 00 00
         00 08 00 00 00 06 11 20 80 10 00 00 00 07 4C 4E
         53 2D 74 75 6E 6E 65 6C ...
```

```
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: I SCCRP from LNS-tunnel
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: O SCCCN  to LNS-tunnel tnlid 6897
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: O SCCCN, flg TLS, ver 2, len 42, tnl
6897, ns 1, nr 1
         C8 02 00 2A 1A F1 00 00 00 01 00 01 80 08 00 00
         00 00 00 03 80 16 00 00 00 0D 32 24 17 BC 6A 19
         B1 79 F3 F9 A9 D4 67 7D 9A DB
*Jul  7 03:28:33.571: uid:14 Tnl/Sn 5192/11 L2TP: O ICRQ to LNS-tunnel 6897/0
*Jul  7 03:28:33.571: uid:14 Tnl/Sn 5192/11 L2TP: O ICRQ, flg TLS, ver 2, len
63, tnl 6897, lsid 11, rsid 0, ns 2, nr 1
         C8 02 00 3F 1A F1 00 00 00 02 00 01 80 08 00 00
         00 00 00 0A 80 0A 00 00 00 0F C8 14 B4 03 80 08
         00 00 00 0E 00 0B 80 0A 00 00 00 12 00 00 00 00
         00 0F 00 09 00 64 0F 10 09 02 02 00 1B 00 00
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse  AVP 0, len 8, flag
0x8000 (M)
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse ICRP
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse  AVP 14, len 8, flag
0x8000 (M)
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Assigned Call ID 5
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: No missing AVPs in ICRP
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: I ICRP, flg TLS, ver 2, len
28, tnl 5192, lsid 11, rsid 0, ns 1, nr 3
contiguous pak, size 28
         C8 02 00 1C 14 48 00 0B 00 01 00 03 80 08 00 00
         00 00 00 0B 80 08 00 00 00 0E 00 05
*Jul  7 03:28:33.579: uid:14 Tnl/Sn 5192/11 L2TP: O ICCN to LNS-tunnel 6897/5
*Jul  7 03:28:33.579: uid:14 Tnl/Sn 5192/11 L2TP: O ICCN, flg TLS, ver 2, len
167, tnl 6897, lsid 11, rsid 5, ns 3, nr 2
         C8 02 00 A7 1A F1 00 05 00 03 00 02 80 08 00 00
         00 00 00 0C 80 0A 00 00 00 18 06 1A 80 00 00 0A
         00 00 00 26 06 1A 80 00 80 0A 00 00 00 13 00 00
         00 01 00 15 00 00 00 1B 01 04 05 D4 03 05 C2 23
         05 05 06 0A 0B E2 7A ...
*Jul  7 03:28:33.579: RADIUS/ENCODE(00000018):Orig. component type = PPoE
*Jul  7 03:28:33.579: RADIUS(00000018): Config NAS IP: 10.0.0.0
*Jul  7 03:28:33.579: RADIUS(00000018): sending
*Jul  7 03:28:33.579: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
Radius-Server 172.19.192.238
*Jul  7 03:28:33.579: RADIUS(00000018): Send Accounting-Request to
172.19.192.238:2196 id 1646/23, len 176
*Jul  7 03:28:33.579: RADIUS:  authenticator 3C 81 D6 C5 2B 6D 21 8E - 19 FF
43 B5 41 86 A8 A5
*Jul  7 03:28:33.579: RADIUS:  Acct-Session-Id     [44]  10  "00000023"
*Jul  7 03:28:33.579: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:28:33.579: RADIUS:  Tunnel-Medium-Type  [65]  6
00:IPv4                   [1]
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Client-Endpoi[66]  10  "10.0.0.1"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Server-Endpoi[67]  10  "10.0.0.2"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Assignment-Id[82]  5   "lac"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Type         [64]  6
00:L2TP                   [3]
*Jul  7 03:28:33.583: RADIUS:  Acct-Tunnel-Connecti[68]  12  "3356800003"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Client-Auth-I[90]  12  "LAC-tunnel"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Server-Auth-I[91]  12  "LNS-tunnel"
*Jul  7 03:28:33.583: RADIUS:  User-Name           [1]   16  "user@example.com"
*Jul  7 03:28:33.583: RADIUS:  Acct-Authentic      [45]  6
Local                     [2]
*Jul  7 03:28:33.583: RADIUS:  Acct-Status-Type    [40]  6
Start                     [1]
*Jul  7 03:28:33.583: RADIUS:  NAS-Port-Type       [61]  6
Virtual                   [5]
*Jul  7 03:28:33.583: RADIUS:  NAS-Port            [5]   6
```

```
0
*Jul  7 03:28:33.583: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:28:33.583: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:28:33.583: RADIUS:  NAS-IP-Address      [4]   6
10.0.1.123
*Jul  7 03:28:33.583: RADIUS:  Acct-Delay-Time     [41]  6
0
*Jul  7 03:28:33.683: RADIUS: Received from id 1646/23 172.19.192.238:2196,
Accounting-response, len 20
*Jul  7 03:28:33.683: RADIUS:  authenticator 1C E9 53 42 A2 8A 58 9A - C3 CC
1D 79 9F A4 6F 3A
```

AAA アカウンティング終了レコードと拒否されたコール：例

次に、**aaa accounting send stop-record authentication** コマンドを **success** キーワードを指定して発行した場合に、認証中に拒否されたコールに関する「終了」レコードが送信されている例を示します。

```
Router# show running-config | include aaa
.
.
.
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting send stop-record authentication success remote-server
aaa accounting network default start-stop group radius

Router#

*Jul  7 03:39:40.199: AAA/BIND(00000026): Bind i/f Virtual-Template2
*Jul  7 03:39:40.199: ppp21 AAA/AUTHOR/LCP: Authorization succeeds trivially
*Jul  7 03:39:42.199: RADIUS/ENCODE(00000026):Orig. component type = PPoE
*Jul  7 03:39:42.199: RADIUS:  AAA Unsupported     [156] 7
*Jul  7 03:39:42.199: RADIUS:   30 2F 30 2F
30                                  [0/0/0]
*Jul  7 03:39:42.199: RADIUS(00000026): Config NAS IP: 10.0.0.0
*Jul  7 03:39:42.199: RADIUS/ENCODE(00000026): acct_session_id: 55
*Jul  7 03:39:42.199: RADIUS(00000026): sending
*Jul  7 03:39:42.199: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
Radius-Server 172.19.192.238
*Jul  7 03:39:42.199: RADIUS(00000026): Send Access-Request to
172.19.192.238:2195 id 1645/14, len 94
*Jul  7 03:39:42.199: RADIUS:  authenticator A6 D1 6B A4 76 9D 52 CF - 33 5D
16 BE AC 7E 5F A6
*Jul  7 03:39:42.199: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:39:42.199: RADIUS:  User-Name           [1]   16  "user@example.com"
*Jul  7 03:39:42.199: RADIUS:  CHAP-Password       [3]   19  *
*Jul  7 03:39:42.199: RADIUS:  NAS-Port-Type       [61]  6
Virtual                   [5]
*Jul  7 03:39:42.199: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:39:42.199: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:39:42.199: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:39:42.199: RADIUS:  NAS-IP-Address      [4]   6
10.0.1.123
*Jul  7 03:39:42.271: RADIUS: Received from id 1645/14 172.19.192.238:2195,
Access-Accept, len 194
*Jul  7 03:39:42.271: RADIUS:  authenticator 30 AD FF 8E 59 0C E4 6C - BA 11
23 63 81 DE 6F D7
```

```
*Jul  7 03:39:42.271: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:39:42.275: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  26
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   20  "vpdn:tunnel-
id=lac"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  29
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   23  "vpdn:tunnel-
type=l2tp"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  30
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   24  "vpdn:gw-
password=cisco"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  31
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   25  "vpdn:nas-
password=cisco"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  34
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   28  "vpdn:ip-
addresses=10.0.0.2"
*Jul  7 03:39:42.275: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:39:42.275: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:39:42.275: RADIUS(00000026): Received from id 1645/14
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: Framed-Protocol
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: service-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: tunnel-id
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: tunnel-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: gw-password
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: nas-password
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: ip-addresses
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: service-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: Framed-Protocol
*Jul  7 03:39:42.279: AAA/BIND(00000027): Bind i/f
*Jul  7 03:39:42.279:  Tnl 21407 L2TP: O SCCRQ
*Jul  7 03:39:42.279:  Tnl 21407 L2TP: O SCCRQ, flg TLS, ver 2, len 134, tnl
0, ns 0, nr 0
         C8 02 00 86 00 00 00 00 00 00 00 00 80 08 00 00
         00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
         00 06 11 30 80 09 00 00 00 07 6C 61 63 00 19 00
         00 00 08 43 69 73 63 6F 20 53 79 73 74 65 6D 73
         2C 20 49 6E 63 2E 80 ...
*Jul  7 03:39:49.279:  Tnl 21407 L2TP: O StopCCN
*Jul  7 03:39:49.279:  Tnl 21407 L2TP: O StopCCN, flg TLS, ver 2, len 66, tnl
0, ns 1, nr 0
         C8 02 00 42 00 00 00 00 00 01 00 00 80 08 00 00
         00 00 00 04 80 1E 00 00 00 01 00 02 00 06 54 6F
         6F 20 6D 61 6E 79 20 72 65 74 72 61 6E 73 6D 69
         74 73 00 08 00 09 00 69 00 01 80 08 00 00 00 09
         53 9F
*Jul  7 03:39:49.279: RADIUS/ENCODE(00000026):Orig. component type = PPoE
*Jul  7 03:39:49.279: RADIUS(00000026): Config NAS IP: 10.0.0.0
*Jul  7 03:39:49.279: RADIUS(00000026): sending
*Jul  7 03:39:49.279: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
Radius-Server 172.19.192.238
*Jul  7 03:39:49.279: RADIUS(00000026): Send Accounting-Request to
172.19.192.238:2196 id 1646/32, len 179
*Jul  7 03:39:49.279: RADIUS:  authenticator 0A 85 2F F0 65 6F 25 E1 - 97 54
CC BF EA F7 62 89
*Jul  7 03:39:49.279: RADIUS:  Acct-Session-Id     [44]  10  "00000037"
*Jul  7 03:39:49.279: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Medium-Type  [65]  6
00:IPv4                   [1]
```

```
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Client-Endpoi[66]  10  "10.0.0.1"
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Server-Endpoi[67]  10  "10.0.0.2"
*Jul  7 03:39:49.283: RADIUS:  Tunnel-Type         [64]  6
00:L2TP                    [3]
*Jul  7 03:39:49.283: RADIUS:  Acct-Tunnel-Connecti[68]  3   "0"
*Jul  7 03:39:49.283: RADIUS:  Tunnel-Client-Auth-I[90]  5   "lac"
*Jul  7 03:39:49.283: RADIUS:  User-Name           [1]   16  "user@example.com"
*Jul  7 03:39:49.283: RADIUS:  Acct-Authentic      [45]  6
RADIUS                     [1]
*Jul  7 03:39:49.283: RADIUS:  Acct-Session-Time   [46]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Input-Octets   [42]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Output-Octets  [43]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Input-Packets  [47]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Output-Packets [48]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Terminate-Cause[49]  6   nas-
error                 [9]
*Jul  7 03:39:49.283: RADIUS:  Acct-Status-Type    [40]  6
Stop                       [2]
*Jul  7 03:39:49.283: RADIUS:  NAS-Port-Type       [61]  6
Virtual                    [5]
*Jul  7 03:39:49.283: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:39:49.283: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:39:49.283: RADIUS:  Service-Type        [6]   6
Framed                     [2]
*Jul  7 03:39:49.283: RADIUS:  NAS-IP-Address      [4]   6
10.0.1.123
*Jul  7 03:39:49.283: RADIUS:  Acct-Delay-Time     [41]  6
0
*Jul  7 03:39:49.335: RADIUS: Received from id 1646/32 172.19.192.238:2196,
Accounting-response, len 20
*Jul  7 03:39:49.335: RADIUS:  authenticator C8 C4 61 AF 4D 9F 78 07 - 94 2B
44 44 17 56 EC 03
```

その他の参考資料

ここでは、Per VRF AAA に関する関連資料について説明します。

関連資料

内容	参照先
AAA：サーバ グループの設定	『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 12.4T』
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
Cisco IOS Switching Services コマンド	『*Cisco IOS IP Switching Command Reference*』
Multiprotocol Label Switching の設定	『*Cisco IOS Multiprotocol Label Switching Configuration Guide*, Release 12.4T』
仮想テンプレートの設定	『*Cisco IOS Dial Technologies Configuration Guide*, Release 12.4T』の「Virtual Templates, Profiles, and Networks」

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によってサポートされる新しい RFC や変更された RFC はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

Per VRF AAA の機能情報

表 2 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 2 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 2　Per VRF AAA の機能情報

機能名	リリース	機能情報
Per VRF AAA Dynamic Per VRF AAA Attribute Filtering Per-Domain and VRF Aware Framed-Routes RADIUS Per-VRF サーバ グループ	12.2(1)DX 12.2(2)DD 12.2(4)B 12.2(13)T 12.2(15)T 12.4(2)T 12.2(28)SB 12.2(33)SR 12.2(33)SXI 12.2(33)SXH4	Per VRF AAA 機能により、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）Routing and Forwarding（VRF; VPN ルーティングおよび転送）インスタンスに基づいた、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）が行えます。Cisco IOS Release 12.2(15)T 以降のリリースでは、ローカルまたはリモートで保存したカスタマー テンプレートを使用し、カスタマー テンプレートに保存された情報に基づいて、AAA サービスを実行できます。 12.2(1)DX には、Cisco 7200 シリーズおよび Cisco 7401ASR に Per VRF AAA 機能が導入されています。 12.2(2)DD には、**ip vrf forwarding（server-group）**および **radius-server domain-stripping** コマンドが追加されています。 Per VRF AAA、Dynamic Per VRF AAA、および Attribute Filtering Per-Domain and VRF Aware Framed-Routes 機能は、Cisco IOS Release 12.2(15)T に導入されています。このリリースには、**aaa authorization template** コマンドも追加されています。 12.4(2)T では、**aaa accounting send stop-record authentication** コマンドが AAA アカウンティング終了レコードへの追加サポートでアップデートされました。 12.2(33)SRC には、RADIUS Per-VRF Server Group 機能が追加されました。 Cisco IOS Release 12.2(33)SXI には、これらの機能が導入されました。 Cisco IOS Release 12.2(33)SXH4 には、これらの機能が導入されました。 この機能により、次のコマンドが導入または変更されました。**aaa accounting**、**aaa accounting delay-start**、**ip radius source-interface**、**radius-server attribute 44 include-in-access-req**、**server-private（RADIUS）**

用語集

AAA：Authentication, Authorization, and Accounting（認証、認可、およびアカウンティング）。セキュリティ サービスのフレームワークであり、ユーザの身元確認（認証）、リモート アクセス コントロール（認可）、課金、監査、およびレポートに使用するセキュリティ サーバ情報の収集と送信（アカウンティング）の方式を定めています。

L2TP：Layer 2 Tunnel Protocol（レイヤ 2 トンネル プロトコル）。レイヤ 2 トンネル プロトコルを使用すると、ISP などのアクセス サービスが仮想トンネルを作成し、顧客のリモート サイトやリモート ユーザを企業のホーム ネットワークにリンクさせることができます。具体的には、ISP Point of Presence（POP; アクセス ポイント）にある Network Access Server（NAS; ネットワーク アクセス サーバ）がリモート ユーザと PPP メッセージを交換し、L2F または L2TP の要求や応答を使用して顧客のトンネル サーバと通信し、トンネルのセットアップを行います。

PE：プロバイダー エッジ。サービス プロバイダー ネットワークのエッジ上のネットワーキング デバイス。

RADIUS：Remote Authentication Dial-In User Service。RADIUS は、不正アクセスからネットワークを保護する分散型クライアント / サーバ システムです。シスコの実装では RADIUS クライアントは Cisco ルータ上で稼動します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

VPN：Virtual Private Network（VPN; バーチャル プライベート ネットワーク）。リモートでダイヤルイン ネットワークをホーム ネットワークに存在させ、あたかも直接接続されているかのように見せるシステム。VPN は、L2TP および L2F を使用し、LAC ではなく、LNS でレイヤ 2 およびより高次のネットワーク接続を終了させます。

VRF：Virtual Route Forwarding。最初は、ルータにグローバルのデフォルト ルーティング / フォワーディング テーブルは 1 つしかありません。VRF は、複数の分離されたルーティング / フォワーディング テーブルとして表示でき、ユーザのルートには別のユーザのルートとの相互関係はありません。

RFC-2867 RADIUS トンネル アカウンティング

RFC-2867 RADIUS トンネル アカウンティングは、6 つの新しい RADIUS アカウンティング タイプを導入しています。これらのタイプは、アカウンティング要求がユーザ サービスの始まり（開始）と終わり（終了）のどちらを表しているかを示す、RADIUS アカウンティング アトリビュートの Acct-Status-Type（アトリビュート 40）と一緒に使用されます。

また、この機能は、ユーザによる VPDN セッション イベントのトラブルシューティングを支援する 2 つの Virtual Private Dialup Network（VPDN; バーチャル プライベート ダイヤルアップ ネットワーク）コマンドを導入しています。

ユーザが tunnel-link ステータスの変化を判断できるようにするネットワーク アカウンティングを使用した VPDN では、RADIUS トンネル アカウンティングがサポートされていないため、使用可能なすべてのアトリビュートがアカウンティング レコード ファイルに書き込まれませんでした。現在は使用可能なすべてのアトリビュートを表示できるため、ユーザはアカウンティング レコードを Internet Service Provider（ISP; インターネット サービス プロバイダー）に確認しやすくなりました。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「RFC-2867 RADIUS トンネル アカウンティングの機能情報」（P.15）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

RFC-2867 RADIUS トンネル アカウンティングの制限事項

RADIUS トンネル アカウンティングは、L2TP トンネル サポートがなければ動作しません。

RFC-2867 RADIUS トンネル アカウンティングに関する情報

RADIUS トンネル アトリビュートとコマンドを使用するには、次の概念を理解しておく必要があります。

- 「RADIUS トンネル アカウンティングのための RADIUS アトリビュート サポート」（P.2）

RADIUS トンネル アカウンティングのための RADIUS アトリビュート サポート

表 1 に、ダイヤルアップ ネットワーク内の強制的トンネリングのプロビジョンをサポートするように設計された新しい RADIUS アカウンティング タイプの概要を示します。このアトリビュート タイプを使用すれば、トンネル ステータスの変化をより適切に追跡できます。

（注） アカウンティング タイプは 2 つのトンネル タイプに分けられるため、ユーザは、トンネル タイプが必要なのか、tunnel-link タイプが必要なのか、両方のアカウンティング タイプが必要なのかを判断できます。

表 1　Acct-Status-Type アトリビュート用の RADIUS アカウンティング タイプ

タイプ名	番号	説明	追加アトリビュート[1]
Tunnel-Start	9	別のノードとのトンネル セットアップの始まりを示します。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • Acct-Delay-Time（41）：AAA から • Event-Timestamp（55）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから
Tunnel-Stop	10	別のノードへの、または別のノードからのトンネル接続の終わりを示します。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • Acct-Delay-Time（41）：AAA から • Acct-Input-Octets（42）：AAA から • Acct-Output-Octets（43）：AAA から • Acct-Session-Id（44）：AAA から • Acct-Session-Time（46）：AAA から • Acct-Input-Packets（47）：AAA から • Acct-Output-Packets（48）：AAA から • Acct-Terminate-Cause（49）：AAA から • Acct-Multi-Session-Id（51）：AAA から • Event-Timestamp（55）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから • Acct-Tunnel-Packets-Lost（86）：クライアントから

表 1　Acct-Status-Type アトリビュート用の RADIUS アカウンティング タイプ（続き）

タイプ名	番号	説明	追加アトリビュート[1]
Tunnel-Reject	11	別のノードとのトンネル セットアップの拒否を示します。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • Acct-Delay-Time（41）：AAA から • Acct-Terminate-Cause（49）：クライアントから • Event-Timestamp（55）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから
Tunnel-Link-Start	12	トンネル リンクの構築を示します。一部のトンネル タイプ（Layer 2 Transport Protocol（L2TP; レイヤ 2 トランスポート プロトコル）しか、トンネル当たりの複数リンクをサポートしていません。この値は、トンネル当たりの複数リンクをサポートしているトンネル タイプのアカウンティング パケット以外には含めないでください。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • NAS-Port（5）：AAA から • Acct-Delay-Time（41）：AAA から • Event-Timestamp（55）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから

表 1　Acct-Status-Type アトリビュート用の RADIUS アカウンティング タイプ（続き）

タイプ名	番号	説明	追加アトリビュート[1]
Tunnel-Link-Stop	13	トンネル リンクの終わりを示します。一部のトンネル タイプ（L2TP）しか、トンネル当たりの複数リンクをサポートしていません。この値は、トンネル当たりの複数リンクをサポートしているトンネル タイプのアカウンティング パケット以外には含めないでください。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • NAS-Port（5）：AAA から • Acct-Delay-Time（41）：AAA から • Acct-Input-Octets（42）：AAA から • Acct-Output-Octets（43）：AAA から • Acct-Session-Id（44）：AAA から • Acct-Session-Time（46）：AAA から • Acct-Input-Packets（47）：AAA から • Acct-Output-Packets（48）：AAA から • Acct-Terminate-Cause（49）：AAA から • Acct-Multi-Session-Id（51）：AAA から • Event-Timestamp（55）：AAA から • NAS-Port-Type（61）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから • Acct-Tunnel-Packets-Lost（86）：クライアントから

表 1　Acct-Status-Type アトリビュート用の RADIUS アカウンティング タイプ（続き）

タイプ名	番号	説明	追加アトリビュート[1]
Tunnel-Link-Reject	14	既存のトンネル内の新しいリンクに対するトンネル セットアップの拒否を示します。一部のトンネル タイプ（L2TP）しか、トンネル当たりの複数リンクをサポートしていません。この値は、トンネル当たりの複数リンクをサポートしているトンネル タイプのアカウンティング パケット以外には含めないでください。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • Acct-Delay-Time（41）：AAA から • Acct-Terminate-Cause（49）：AAA から • Event-Timestamp（55）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから

1. 指定されたトンネル タイプが使用されている場合は、これらのアトリビュートもアカウンティング要求パケットに含める必要があります。

RADIUS トンネル アカウンティングの設定方法

ここでは、次の各手順について説明します。

- 「トンネル タイプ アカウンティング レコードの有効化」（P.6）
- 「RADIUS トンネル アカウンティングの確認」（P.8）

トンネル タイプ アカウンティング レコードの有効化

このタスクを使用して、トンネル レコードと tunnel-link アカウンティング レコードを RADIUS サーバに送信するように LAC を設定します。

VPDN トンネル イベント

2 つの新しい Command Line Interface（CLI; コマンドライン インターフェイス）の vpdn セッション アカウンティング ネットワーク（tunnel-link-type records）と vpdn トンネル アカウンティング ネットワーク（tunnel-type records）が次のイベントの特定を支援するためにサポートされています。

- VPDN トンネルが構築または破壊された。
- VPDN トンネルの作成要求が拒否された。
- VPDN トンネル内のユーザ セッションが起動または停止された。
- ユーザ セッション作成要求が拒否された。

（注） 最初の 2 つのイベントは、tunnel-type アカウンティング レコードです。Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）が、Tunnel-Start、Tunnel-Stop、または Tunnel-Reject アカウンティング レコードを RADIUS サーバに送信します。次の 2 つのイベントは、tunnel-link-type アカウンティング レコードです。AAA が、Tunnel-Link-Start、Tunnel-Link-Stop、または Tunnel-Link-Reject アカウンティング レコードを RADIUS サーバに送信します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa accounting network** {**default** | *list-name*} {**start-stop** | **stop-only** | **wait-start** | none} **group** *groupname*
4. **vpdn enable**
5. **vpdn tunnel accounting network** *list-name*
6. **vpdn session accounting network** *list-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	Router(config)# **aaa accounting network** {**default** | *list-name*} {**start-stop** | **stop-only** | **wait-start** | **none**} **group** *groupname*	ネットワーク アカウンティングを有効にします。 • **default**：デフォルト ネットワーク アカウンティングの method-list が設定され、インターフェイス上でどの追加のアカウンティング設定も有効になっていない場合は、デフォルトで、ネットワーク アカウンティングが有効になります。 **vpdn session accounting network** コマンドと **vpdn tunnel accounting network** コマンドのどちらかがデフォルトの method-list にリンクされている場合は、すべてのトンネル レコードと tunnel-link アカウンティング レコードがそれらのセッションに対して有効になります。 • *list-name*：**aaa accounting** コマンドで定義した *list-name* は、VPDN コマンドで定義した *list-name* と同じにする必要があります。そうでない場合は、アカウンティングが実行されません。

	コマンドまたはアクション	目的
ステップ 4	`Router(config)# vpdn enable`	ルータ上のバーチャル プライベート ダイヤルアップ ネットワーキングを有効にして、ルータにローカル データベースとリモート認可サーバ（該当する場合）上でトンネル定義を検索するように指示します。
ステップ 5	`Router(config)# vpdn tunnel accounting network` *`list-name`*	Tunnel-Start、Tunnel-Stop、および Tunnel-Reject アカウンティング レコードを有効にします。 • *list-name* : *list-name* は **aaa accounting** コマンドで定義された *list-name* と一致する必要があります。そうでない場合は、ネットワーク アカウンティングが実行されません。
ステップ 6	`Router(config)# vpdn session accounting network` *`list-name`*	Tunnel-Link-Start、Tunnel-Link-Stop、および Tunnel-Link-Reject アカウンティング レコードを有効にします。 • *list-name* : *list-name* は **aaa accounting** コマンドで定義された *list-name* と一致する必要があります。そうでない場合は、ネットワーク アカウンティングが実行されません。

この次の手順

RADIUS トンネル アカウンティングを有効にしたら、次のオプション タスクの「RADIUS トンネル アカウンティングの確認」（P.8）を通して設定を確認できます。

RADIUS トンネル アカウンティングの確認

次のオプション手順のどちらかまたは両方を使用して、RADIUS トンネル アカウンティング設定を確認します。

手順の概要

1. **enable**
2. **show accounting**
3. **show vpdn** [**session** | **tunnel**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	Router# **show accounting**	ネットワーク上でアクティブなアカウント可能イベントを表示して、アカウンティング サーバ上でのデータ消失イベント時の情報収集を支援します。
ステップ 3	Router# **show vpdn** [**session**] [**tunnel**]	VPDN 内のアクティブな L2TP トンネルとメッセージ識別子に関する情報を表示します。 • **session**：すべてのアクティブなトンネルのステータス サマリーを表示します。 • **tunnel**：すべてのアクティブな L2TP トンネルに関する情報をサマリー形式で表示します。

RADIUS トンネル アカウンティングの設定例

ここでは、次の設定例について説明します。

- 「LAC 上での RADIUS トンネル アカウンティングの設定：例」（P.9）
- 「LNS 上での RADIUS トンネル アカウンティングの設定：例」（P.11）

LAC 上での RADIUS トンネル アカウンティングの設定：例

次の例は、トンネル レコードと tunnel-link アカウンティング レコードを RADIUS サーバに送信するように L2TP Access Concentrator（LAC; L2TP アクセス コンセントレータ）を設定する方法を示しています。

```
aaa new-model
!
!
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
aaa session-id common
enable secret 5 $1$IDjH$iL7puCja1RMlyOM.JAeuf/
enable password lab
!
username ISP_LAC password 0 tunnelpass
!
!
resource-pool disable
!
!
ip subnet-zero
ip cef
no ip domain-lookup
ip host dirt 171.69.1.129
!
```

```
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
vpdn search-order domain dnis
!
vpdn-group 1
 request-dialin
  protocol l2tp
  domain cisco.com
 initiate-to ip 10.1.26.71
 local name ISP_LAC
!
isdn switch-type primary-5ess
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
controller T1 7/4
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
!
!
interface FastEthernet0/0
 ip address 10.1.27.74 255.255.255.0
 no ip mroute-cache
 duplex half
 speed auto
 no cdp enable
!
interface FastEthernet0/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
interface Serial7/4:23
 ip address 60.0.0.2 255.255.255.0
 encapsulation ppp
 dialer string 2000
 dialer-group 1
 isdn switch-type primary-5ess
 ppp authentication chap
!
interface Group-Async0
 no ip address
 shutdown
 group-range 1/00 3/107
!
ip default-gateway 10.1.27.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.27.254
no ip http server
ip pim bidir-enable
!
!
dialer-list 1 protocol ip permit
no cdp run
!
!
```

```
radius-server host 172.19.192.26 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
call rsvp-sync
!
```

LNS 上での RADIUS トンネル アカウンティングの設定：例

次の例は、トンネル レコードと tunnel-link アカウンティング レコードを RADIUS サーバに送信するように L2TP Network Server（LNS; L2TP ネットワーク サーバ）を設定する方法を示しています。

```
aaa new-model
!
!
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
aaa session-id common
enable secret 5 $1$ftf.$wE6Q5Yv6hmQiwL9pizPCg1
!
username ENT_LNS password 0 tunnelpass
username user1@cisco.com password 0 lab
username user2@cisco.com password 0 lab
spe 1/0 1/7
 firmware location system:/ucode/mica_port_firmware
spe 2/0 2/9
 firmware location system:/ucode/mica_port_firmware
!
!
resource-pool disable
clock timezone est 2
!
ip subnet-zero
no ip domain-lookup
ip host CALLGEN-SECURITY-V2 64.24.80.28 3.47.0.0
ip host dirt 171.69.1.129
!
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
!
vpdn-group 1
accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname ISP_LAC
 local name ENT_LNS
!
isdn switch-type primary-5ess
!
!
!
!
!
!
!
fax interface-type modem
mta receive maximum-recipients 0
!
interface Loopback0
 ip address 70.0.0.101 255.255.255.0
!
interface Loopback1
 ip address 80.0.0.101 255.255.255.0
```

```
!
interface Ethernet0
 ip address 10.1.26.71 255.255.255.0
 no ip mroute-cache
 no cdp enable
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool vpdn-pool1
 ppp authentication chap
!
interface Virtual-Template2
 ip unnumbered Loopback1
 peer default ip address pool vpdn-pool2
 ppp authentication chap
!
interface FastEthernet0
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
speed auto
 no cdp enable
!
ip local pool vpdn-pool1 70.0.0.1 70.0.0.100
ip local pool vpdn-pool2 80.0.0.1 80.0.0.100
ip default-gateway 10.1.26.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.26.254
ip route 90.1.1.2 255.255.255.255 10.1.26.254
no ip http server
ip pim bidir-enable
!
!
dialer-list 1 protocol ip permit
no cdp run
!
!
radius-server host 172.19.192.80 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
call rsvp-sync
```

その他の参考資料

次の項で、RFC-2867 RADIUS トンネル アカウンティングに関する参考資料を紹介します。

関連資料

内容	参照先
RADIUS アトリビュート	「RADIUS Attributes」フィーチャ モジュール
VPDN	『*Cisco IOS VPDN Configuration Guide, Release 12.4T*』
ネットワーク アカウンティング	「Configuring Accounting」フィーチャ モジュール

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2867	「*RADIUS Accounting Modifications for Tunnel Protocol Support*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

RFC-2867 RADIUS トンネル アカウンティングの機能情報

表 2 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 2 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 2　RFC-2867 RADIUS トンネル アカウンティングの機能情報

機能名	リリース	機能情報
RFC-2867 RADIUS トンネル アカウンティング	12.2(15)B 12.3(4)T	RFC-2867 RADIUS トンネル アカウンティングは、6 つの新しい RADIUS アカウンティング タイプを導入しています。これらのタイプは、アカウンティング要求がユーザ サービスの始まり（開始）と終わり（終了）のどちらを表しているかを示す、RADIUS アカウンティング アトリビュートの Acct-Status-Type（アトリビュート 40）と一緒に使用されます。 また、この機能は、ユーザによる VPDN セッション イベントのトラブルシューティングを支援する 2 つの Virtual Private Dialup Network（VPDN; バーチャル プライベート ダイヤルアップ ネットワーク）コマンドを導入しています。 12.2(15)B で、この機能が Cisco 6400 シリーズ、Cisco 7200 シリーズ、および Cisco 7400 シリーズのルータに導入されました。 この機能は、Cisco IOS Release 12.3(4)T に統合されました。 **aaa accounting**、**vpdn session accounting network**、および **vpdn tunnel accounting network** の各コマンドが導入または変更されました。

RADIUS アトリビュート スクリーニング

RADIUS アトリビュート スクリーニング機能を使用すれば、認可やアカウンティングなどの目的で Network Access Server（NAS; ネットワーク アクセス サーバ）上の「許可」または「拒否」RADIUS アトリビュートのリストを設定できます。

NAS が Access-Accept パケットで受信したすべての RADIUS アトリビュートを受け入れて処理する場合は、不必要なアトリビュートを処理する可能性があり、顧客の Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）サーバを制御しないホールセール プロバイダーの場合に問題が発生します。たとえば、顧客が加入していないサービスを指定するアトリビュートが存在したり、他のホールセール ダイヤル ユーザ向けのサービスを低下させるアトリビュートが存在したりする場合です。そのため、特定のアトリビュートの使用を制限するように NAS を設定できることが、多くのユーザの要件になります。

RADIUS アトリビュート スクリーニング機能を実装するには、次の方法のいずれかを使用する必要があります。

- NAS が、特定の目的で、設定された拒否リストに登録されたものを除く、すべての標準 RADIUS アトリビュートを受け入れて、処理できるようにする
- NAS が、特定の目的で、設定された許可リストに登録されたものを除く、すべての標準 RADIUS アトリビュートを拒否（除外）できるようにする

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「RADIUS アトリビュート スクリーニングの機能情報」（P.10）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

RADIUS アトリビュート スクリーニングの前提条件

RADIUS 許可リストまたは拒否リストを設定する前に、グローバル コンフィギュレーション モードで **aaa new-model** コマンドを使用して AAA を有効にする必要があります。

RADIUS アトリビュート スクリーニングの制約事項

NAS の要件

この機能を有効にするには、RADIUS グループを使用して認可するように NAS を設定する必要があります。

許可リストまたは拒否リストの制約事項

許可リストまたは拒否リストの設定に使用される 2 つのフィルタは相互排他的です。そのため、ユーザはサーバ グループの目的ごとに、1 つのアクセス リストか、1 つの拒否リストしか設定できません。

ベンダー固有アトリビュート

この機能は、Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）スクリーニングをサポートしていません。ただし、ユーザは、すべての VSA を許可または拒否する許可リストまたは拒否リスト内でアトリビュート 26（Vendor-Specific）を指定できます。

必須アトリビュート スクリーニングの推奨事項

次の必須アトリビュートは、拒否しないことを推奨します。

- 認可用：
  - 6（Service-Type）
  - 7（Framed-Protocol）
- アカウンティング用：
  - 4（NAS-IP-Address）
  - 40（Acct-Status-Type）
  - 41（Acct-Delay-Time）
  - 44（Acct-Session-ID）

アトリビュートが必須の場合は、拒否が無視され、アトリビュートのパススルーが許可されます。

（注） 必須アトリビュートの拒否リストを設定してもエラーにはなりません。これは、リストでは目的（認可またはアカウンティング）が指定されないためです。サーバが、アトリビュートの使用目的を認識したときに、そのアトリビュートが必須かどうかを判断します。

RADIUS アトリビュート スクリーニングに関する情報

RADIUS アトリビュート スクリーニング機能は、次のようなメリットを提供します。

- ユーザは、NAS 上で特定の目的のアトリビュートを選択して許可リストまたは拒否リストを設定できるため、不必要なアトリビュートが受け入れられ、処理されることがなくなります。
- 関連するアカウンティング アトリビュートだけの許可リストを設定することによって、不必要なトラフィックを削減し、アカウンティング データのカスタマイズを可能にすることができます。

RADIUS アトリビュートのスクリーン方法

次の項で、RADIUS アトリビュートをスクリーンして、確認する方法について説明します。

- 「RADIUS アトリビュート スクリーニングの設定」
- 「RADIUS アトリビュート スクリーニングの確認」

RADIUS アトリビュート スクリーニングの設定

RADIUS アトリビュートの許可リストまたは拒否リストを認可またはアカウンティング用に設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authentication ppp default group** *group-name*
4. **aaa authorization network default group** *group-name*
5. **aaa group server radius** *group-name*
6. **server** *ip-address*
7. **authorization** [**accept** | **reject**] *listname* または **accounting** [**accept** | **reject**] *listname*
8. **exit**
9. **radius-server host** {***hostname*** | ***ip-address***} [**key** ***string***]
10. **radius-server attribute list** ***listname***
11. **attribute** ***number*** [***number*** [***number...***]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa authentication ppp default group** *group-name* 例： `Router(config)# aaa authentication ppp default group radius-sg`	PPP を実行しているシリアル インターフェイス上で使用する 1 つまたは複数の AAA 認証方式を指定します。
ステップ 4	**aaa authorization network default group** *group-name* 例： `Router(config)# aaa authorization network default group radius-sg`	ユーザのネットワーク アクセスを制限するパラメータを設定します。
ステップ 5	**aaa group server radius** *group-name* 例： `Router(config)# aaa group server radius radius-sg`	複数の RADIUS サーバ ホストを別々のリストと別々の方式にグループ分けします。

	コマンドまたはアクション	目的
ステップ 6	**server** *ip-address* 例： Router(config-sg-radius)# server 10.1.1.1	グループ サーバ用の RADIUS サーバの IP アドレスを設定します。
ステップ 7	**authorization** [**accept** | **reject**] *listname* および / または **accounting** [**accept** | **reject**] *listname* 例： Router(config-sg-radius)# authorization accept min-author	RADIUS サーバから Access-Accept パケット内で返すアトリビュート用のフィルタを指定します。 および / または アカウンティング要求内で RADIUS サーバに送信すべきアトリビュート用のフィルタを指定します。 （注） **accept** キーワードは、*listname* で指定されたアトリビュートを除く、すべてのアトリビュートが拒否されることを意味します。**reject** キーワードは、*listname* で指定されたアトリビュートとすべての標準アトリビュートを除く、すべてのアトリビュートが許可されることを意味します。
ステップ 8	Router(config-sg-radius)# **exit**	server-group コンフィギュレーション モードを終了します。
ステップ 9	**radius-server host** {*hostname* | *ip-address*} [**key** *string*] 例： Router(config)# radius-server host 10.1.1.1 key mykey1	RADIUS サーバ ホストを指定します。
ステップ 10	**radius-server attribute list** *listname* 例： Router(config)# radius-server attribute list min-author	**attribute** コマンドで定義されたアトリビュートのセットに付けるリスト名を定義し、server-group コンフィギュレーション モードに入ります。 （注） *listname* はステップ 5 で定義した *listname* と同じにする必要があります。
ステップ 11	**attribute** *number* [*number* [*number...*]] 例： Router(config-sg-radius)# attribute 6-7	設定した許可リストまたは拒否リストに RADIUS アトリビュートを追加します。詳細については、「RADIUS Attributes Overview and RADIUS IETF Attributes」フィーチャ モジュールを参照してください。 （注） このコマンドは、許可リストまたは拒否リストにアトリビュートを追加するために何回も使用できます。 （注） user-password（RADIUS アトリビュート 2）アトリビュートと nas-ip（RADIUS アトリビュート 4）アトリビュートは、フィルタ対象として設定されている場合に、アクセス要求内でまとめてフィルタすることができます。アクセス要求には、ユーザ パスワード、CHAP パスワード、状態のいずれかを含める必要があります。また、NAS IP アドレスと NAS 識別子のどちらかを RADIUS アカウンティング要求に含める必要があります。

RADIUS アトリビュート スクリーニングの確認

許可リストまたは拒否リストを確認するには、特権 EXEC モードで次のコマンドのいずれかを使用します。

コマンド	目的
Router# **debug aaa accounting**	説明の義務があるイベントが発生したときに、その情報を表示します。
Router# **debug aaa authentication**	AAA 認証に関する情報を表示します。
Router# **show radius statistics**	アカウンティング パケットと認証パケットについての RADIUS 統計情報を示します。

RADIUS アトリビュート スクリーニングの設定例

ここでは、次の設定例について説明します。

- 「認可許可：例」
- 「アカウンティング拒否：例」
- 「認可拒否とアカウンティング許可：例」
- 「必須アトリビュートの拒否：例」

認可許可：例

次の例は、アトリビュート 6（Service-Type）とアトリビュート 7（Framed-Protocol）用の許可リストの設定方法を示しています。他のすべてのアトリビュート（VSA を含む）は RADIUS 認可に対して拒否されます。

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
    server 10.1.1.1
    authorization accept min-author
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list min-author
    attribute 6-7
```

アカウンティング拒否：例

次の例は、アトリビュート 66（Tunnel-Client-Endpoint）とアトリビュート 67（Tunnel-Server-Endpoint）用の拒否リストの設定方法を示しています。他のすべてのアトリビュート（VSA を含む）は RADIUS アカウンティングに対して受け入れられます。

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
    server 10.1.1.1
```

```
    accounting reject tnl-x-endpoint
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list tnl-x-endpoint
    attribute 66-67
```

認可拒否とアカウンティング許可：例

次の例は、RADIUS 認可用の拒否リストと RADIUS アカウンティング用の許可リストの設定方法を示しています。認可またはアカウンティングのサーバ グループごとに複数の許可リストまたは拒否リストを設定できませんが、サーバ グループごとに認可用のリストとアカウンティング用のリストを 1 つずつ設定できます。

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
    server 10.1.1.1
    authorization reject bad-author
    accounting accept usage-only
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list usage-only
    attribute 1,40,42-43,46
!
radius-server attribute list bad-author
    attribute 22,27-28,56-59
```

必須アトリビュートの拒否：例

次の例は、**debug aaa accounting** コマンドのデバッグ出力を示しています。この例では、必須アトリビュートの 44、40、および 41 が拒否リストの「standard」に追加されています。

```
Router# debug aaa authorization

AAA/ACCT(6): Accounting method=radius-sg (radius)
RADIUS: attribute 44 cannot be rejected
RADIUS: attribute 61 rejected
RADIUS: attribute 31 rejected
RADIUS: attribute 40 cannot be rejected
RADIUS: attribute 41 cannot be rejected
```

その他の参考資料

次の項で、RADIUS アトリビュート スクリーニング機能に関する参考資料を紹介します。

関連資料

内容	参照先
IOS AAA セキュリティ機能	『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 12.4T』
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
RADIUS	「Configuring RADIUS」モジュール

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
このリリースによってサポートされる新しい RFC や変更された RFC はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

RADIUS アトリビュート スクリーニングの機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　RADIUS アトリビュート スクリーニングの機能情報

機能名	リリース	機能情報
RADIUS アトリビュート スクリーニング	12.2(1)DX 12.2(2)DD 12.2(4)B 12.2(4)T 12.2(13)T 12.2(33)SRC	RADIUS アトリビュート スクリーニング機能を使用すれば、認可やアカウンティングなどの目的で Network Access Server（NAS; ネットワーク アクセス サーバ）上の「許可」または「拒否」RADIUS アトリビュートのリストを設定できます。 この機能は、12.2(1)DX で導入されました。 この機能は、Cisco IOS Release 12.2(2)DD に統合されました。 この機能は、Cisco IOS Release 12.2(4)B に統合されました。 この機能は、12.2(4)T に統合されました。 この機能は、Cisco IOS Release 12.2(33)SRC に統合されました。 プラットフォーム サポートが Cisco 7401 ASR ルータ用に追加されました。 Cisco 7200 シリーズ プラットフォームは、Cisco IOS Release 12.2(1)DX、12.2(2)DD、12.2(4)B、12.2(4)T、および 12.2(13)T に適用されます。 Cisco 7401 ASR プラットフォームは、Cisco IOS Release 12.2(13)T にのみ適用されます。 **accounting**（**server-group** コンフィギュレーション）、**authorization**（**server-group** コンフィギュレーション）、**attribute**（**server-group** コンフィギュレーション）、および **radius-server attribute list** の各コマンドが、この機能で導入または変更されました。

用語集

AAA：Authentication, Authorization, and Accounting（認証、認可、およびアカウンティング）。Cisco ルータまたはアクセス サーバにアクセス コントロールを設定できる主要なフレームワークを提供する一連のネットワーク セキュリティ サービスです。

NAS：Network Access Server（NAS; ネットワーク アクセス サーバ）パケットの世界（インターネットなど）と回線の世界（公衆電話交換網など）をインターフェイスするシスコ プラットフォーム（または AccessPath システムなどのプラットフォームの集合）。

RADIUS：Remote Authentication Dial-In User Service（リモート認証ダイヤルイン ユーザ サービス）。RADIUS は、不正アクセスからネットワークを保護する分散型クライアント / サーバ システムです。シスコの実装では RADIUS クライアントは Cisco ルータ上で稼動します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

VSA：Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）。VSA は、1 つの IETF アトリビュート（Vendor-Specific（アトリビュート 26））から抽出されます。アトリビュート 26 を使用すれば、ベンダーは、追加の 255 個のアトリビュートを作成して実装できます。つまり、ベンダーは、どの IETF アトリビュートとも一致しないアトリビュートを作成して、それをアトリビュート 26 の背後にカプセル化することができます。具体的には、Vendor-Specific ="protocol:attribute=value" と指定します。

アトリビュート：RADIUS Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）アトリビュートは、255 の標準アトリビュートで構成されるオリジナルのセットで、クライアントとサーバ間での AAA 情報の伝達に使用されます。IETF アトリビュートは標準であるため、アトリビュート データは事前定義されてその内容も認識されています。このため、IETF アトリビュートを介して AAA 情報を交換するすべてのクライアントとサーバは、アトリビュートの厳密な意味や各アトリビュート値の一般的な限界など、アトリビュート データに一致させる必要があります。

RADIUS 集中型フィルタ管理

RADIUS 集中型フィルタ管理機能は、ACL の設定と管理を容易にするフィルタ サーバを導入しています。このフィルタ サーバは、集中型 RADIUS リポジトリおよび管理ポイントとして機能します。ユーザは、Access Control List（ACL; アクセス コントロール リスト）フィルタを集中的に管理および設定できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「RADIUS 集中型フィルタ管理の機能情報」（P.10）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

RADIUS 集中型フィルタ管理の前提条件

- 新しい RADIUS VSA をサポートしていないサーバにディレクトリ ファイルを追加しなければならない場合があります。サンプル ディレクトリとベンダー ファイルについては、このマニュアルの「RADIUS 辞書とベンダー ファイル：例」を参照してください。

  ディレクトリ ファイルを追加する必要がある場合は、RADIUS サーバが非標準であり、新しく導入された VSA を送信可能であること確認してください。

- リモート ユーザがダイヤルインして IP 接続を確立できるように、RADIUS ネットワーク認証をセットアップすることができます。

RADIUS 集中型フィルタ管理の制約事項

この機能では複数の方式リストがサポートされていません。単一のグローバル フィルタ方式リストが設定できるだけです。

RADIUS 集中型フィルタ管理に関する情報

RADIUS 集中型フィルタ管理機能以前は、ホールセール プロバイダー（ACL などの顧客サービスに対して特別料金を課している）が、顧客の網羅的な ACL の適用を阻止できました。この行為は、ルータの性能や他の顧客に影響を与える可能性があります。この機能は、ACL 管理用の集中型管理ポイント（フィルタ サーバ）を導入しています。フィルタ サーバは、ACL 設定用の集中型 RADIUS リポジトリとして機能します。

フィルタ サーバとして使用されている RADIUS サーバがアクセス認証に使用されているサーバと同じかどうかに関係なく、Network Access Server（NAS; ネットワーク アクセス サーバ）はフィルタ サーバに対して別のアクセス要求を開始します。設定されていれば、NAS は、認証ユーザ名と 2 つめのアクセス要求用のフィルタ サーバ パスワードとして、フィルタ ID 名を使用します。RADIUS サーバは、フィルタ ID 名を認証して、access-accept 応答内に必要なフィルタリング設定を返そうとします。

ACL のダウンロードには時間がかかるため、NAS 上でローカル キャッシュが維持されます。ローカル キャッシュ上に ACL 名が存在する場合は、フィルタ サーバに問い合わせることなくその設定が使用されます。

（注） キャッシュが適切に設定されていれば、遅延は最小限に抑えられるはずです。ただし、フィルタが必要な最初のダイヤルイン ユーザは必ず待たされることになります。これは、初めての場合は、ACL 設定が読み込まれるためです。

キャッシュ管理

グローバル フィルタ キャッシュは最後に ACL をダウンロードした NAS 上で維持されます。そのため、ユーザは、過負荷状態の RADIUS サーバに対して同じ ACL 設定情報を何度も要求する必要がありません。ユーザは、次の基準が満たされている場合にキャッシュをフラッシュする必要があります。

- エントリが新しいアクティブ コールに関連付けられた後に、そのエントリに関連付けられたアイドル タイマーがリセットされる（そのように設定されている場合）。
- アイドル時間スタンプの期限が切れたエントリが削除される。

- グローバル キャッシュのエントリが指定された最大数に到達した後に、アイドル タイマーがアイドル時間限界に最も近いエントリが削除される。

1 つのタイマーがすべてのキャッシュ エントリの管理に使用されます。このタイマーは、最初のキャッシュ エントリの作成時に開始され、リブートされるまで定期的に実行されます。タイマーの期間は、キャッシュ アイドル タイマーの設定時に指定された最小粒度に対応し、毎分期限切れになります。タイマーが 1 つしかないことによって、ユーザは、キャッシュ エントリごとに別々のタイマーを管理する必要がありません。

（注） 単一のタイマーは、タイマーの期限切れの精度に欠けます。約 50% のタイマー粒度に平均誤差が含まれています。タイマー粒度を下げると平均誤差も下がりますが、性能が低下する可能性があります。キャッシュ管理には正確なタイミングが必要ないため、誤差遅延を受け入れる必要があります。

新しいベンダー固有アトリビュートのサポート

この機能は、次の 2 つのカテゴリに分類可能な 3 つの新しい Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）のサポートを導入しています。

- ユーザ プロファイルの拡張
  - Filter-Required（50）：指定されたフィルタが見つからなかった場合にコールを許可するかどうかを指定します。存在する場合は、このアトリビュートが、すべての Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）フィルタ方式リストの後に適用されます。
- 疑似ユーザ プロファイルの拡張
  - Cache-Refresh（56）：エントリが新しいセッションから参照されるたびにキャッシュ エントリをリフレッシュするかどうかを指定します。このアトリビュートは、**cache refresh** コマンドに対応します。
  - Cache-Time（57）：キャッシュ エントリのアイドル タイムアウトを分単位で指定します。このアトリビュートは、**cache clear age** コマンドに対応します。

（注） すべての RADIUS アトリビュートが、すべての Command-Line Interface（CLI; コマンドライン インターフェイス）設定よりも優先されます。

RADIUS 用の集中型フィルタ管理の設定方法

次の項を使用して、集中型フィルタ管理機能を設定します。

- 「RADIUS ACL フィルタ サーバの設定」
- 「フィルタ キャッシュの設定」
- 「フィルタ キャッシュの確認」

RADIUS ACL フィルタ サーバの設定

RADIUS ACL フィルタ サーバを有効にするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# **aas authorization cache filterserver default** *methodlist[methodlist2...]*	AAA 認可キャッシュと、RADIUS フィルタ サーバからの ACL 設定のダウンロードを有効にします。 • **default**：デフォルト認可リスト • *methodlist* [*methodlist2...*]：**password** コマンド ページに列挙されたキーワードの 1 つ。

フィルタ キャッシュの設定

この項の次の手順に従って、AAA フィルタ キャッシュを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa cache filter**
4. **password** {**0** | **7**} *password*
5. **cache disable**
6. **cache clear age** *minutes*
7. **cache refresh**
8. **cache max** *number*

	コマンド	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	Router(config)# **aaa cache filter**	フィルタ キャッシュ設定を有効にして、AAA フィルタ コンフィギュレーション モードに入ります。

	コマンド	目的
ステップ 4	`Router(config-aaa-filter)# **password** {**0** | **7**} *password*`	（任意）フィルタ サーバ認証要求に使用されるオプション パスワードを指定します。 **0**：暗号化されていないパスワードが後に続くことを示します。 **7**：非表示パスワードが後に続くことを示します。 *password*：暗号化されていない（クリア テキスト）パスワード。 **（注）** パスワードが指定されなかった場合は、デフォルト パスワード（「cisco」）が有効になります。
ステップ 5	`Router(config-aaa-filter)# **cache disable**`	（任意）キャッシュを無効にします。
ステップ 6	`Router(config-aaa-filter)# **cache clear age** *minutes*`	（任意）キャッシュ エントリの期限が切れ、キャッシュがクリアされるタイミングを分単位で指定します。 *minutes*：0 ～ 4294967295 の任意の値。 **（注）** 時間が指定されなかった場合は、デフォルト（1400 分（1 日））が有効になります。
ステップ 7	`Router(config-aaa-filter)# **cache refresh**`	（任意）新しいセッションの開始時点でキャッシュ エントリをリフレッシュします。このコマンドは、デフォルトで有効になっています。この機能を無効にするには、**no cache refresh** コマンドを使用します。
ステップ 8	`Router(config-aaa-filter)# **cache max** *number*`	（任意）キャッシュで特定のサーバ用に維持できるエントリの絶対数を制限します。 *number*：キャッシュに含めることが可能なエントリの最大数。0 ～ 4294967295 の任意の値。 **（注）** 数値が指定されなかった場合は、デフォルト（100 エントリ）が有効になります。

フィルタ キャッシュの確認

キャッシュ ステータスを表示するには、**show aaa cache filterserver** EXEC コマンドを使用します。**show aaa cache filterserver** コマンドの出力サンプルを次に示します。

```
Router# show aaa cache filterserver

Filter     Server          Age Expires Refresh Access-Control-Lists
-------------------------------------------------------------------------------
aol        10.2.3.4          0    1440     100 ip in icmp drop
                                                ip out icmp drop
                                                ip out forward tcp dstip 1.2.3...
msn        10.3.3.4         N/A   Never      2 ip in tcp drop
msn2       10.4.3.4         N/A   Never      2 ip in tcp drop
vone       10.5.3.4         N/A   Never      0 ip in tcp drop
```

（注） **show aaa cache filterserver** コマンドは、特定のフィルタが参照またはリフレッシュされた回数を表示します。この機能は、実際に使用されるフィルタを決定するために管理者が使用します。

トラブルシューティングのヒント

フィルタ キャッシュ設定のトラブルシューティングを支援するために、**debug aaa cache filterserver** 特権 EXEC コマンドを使用します。**debug aaa cache filterserver** コマンドのサンプル出力を確認するには、このマニュアルの「デバッグ出力：例」を参照してください。

フィルタ キャッシュのモニタリングと維持

フィルタ キャッシュをモニタおよび維持するには、次の EXEC コマンドの少なくとも 1 つを使用します。

コマンド	目的
Router# **clear aaa cache filterserver acl** [*filter-name*]	特定のフィルタまたはすべてのフィルタのキャッシュ ステータスをクリアします。
Router# **show aaa cache filterserver**	キャッシュ ステータスを表示します。

RADIUS 集中型フィルタ管理の設定例

ここでは、次の設定例について説明します。

- 「NAS の設定：例」（P.6）
- 「RADIUS サーバの設定：例」（P.7）
- 「RADIUS 辞書とベンダー ファイル：例」（P.7）
- 「デバッグ出力：例」（P.7）

NAS の設定：例

次の例は、キャッシュ フィルタリング用の NAS の設定方法を示しています。この例では、最初に、サーバ グループの「mygroup」に接続されます。応答がない場合は、デフォルト RADIUS サーバに接続されます。それでも応答がない場合は、ローカル フィルタ ケアに接続されます。最終的に、フィルタが解決できなければ、コールが受け入れられます。

```
aaa authorization cache filterserver group mygroup group radius local none
!
aaa group server radius mygroup
 server 10.2.3.4
 server 10.2.3.5
!
radius-server host 10.1.3.4
!
aaa cache filter
 password mycisco
 no cache refresh
 cache max 100
!
```

RADIUS サーバの設定：例

次の例は、NAS にダイヤルしているリモート ユーザの「user1」のサンプル RADIUS 設定です。

```
myfilter Password = "cisco"
        Service-Type = Outbound,
        Ascend:Ascend-Call-Filter = "ip in drop srcip 10.0.0.1/32 dstip 10.0.0.10/32
        icmp",
        Ascend:Ascend-Call-Filter = "ip in drop srcip 10.0.0.1/32 dstip 10.0.0.10/32 tcp
        dstport = telnet",
        Ascend:Ascend-Cache-Refresh = Refresh-No,
        Ascend:Ascend-Cache-Time = 15

user1 Password = "cisco"
        Service-Type = Framed,
        Filter-Id = "myfilter",
        Ascend:Ascend-Filter-Required = Filter-Required-Yes,
```

RADIUS 辞書とベンダー ファイル：例

次の例は、新しい VSA 用のサンプル RADIUS 辞書ファイルです。この例では、辞書ファイルが Merit サーバ用です。

```
dictionary file:
Ascend.attr Ascend-Filter-Required 50 integer (*, 0, NOENCAPS)
Ascend.attr Ascend-Cache-Refresh   56 integer (*, 0, NOENCAPS)
Ascend.attr Ascend-Cache-Time      57 integer (*, 0, NOENCAPS)

Ascend.value Ascend-Cache-Refresh Refresh-No  0
Ascend.value Ascend-Cache-Refresh Refresh-Yes 1

Ascend.value Ascend-Filter-Required  Filter-Required-No  0
Ascend.value Ascend-Filter-Required  Filter-Required-Yes 1

vendors file:
50     50
56     56
57     57
```

デバッグ出力：例

debug aaa cache filterserver コマンドのサンプル出力を次に示します。

```
Router# debug aaa cache filterserver

AAA/FLTSV: need "myfilter" (fetch), call 0x612DAC64
AAA/FLTSV: send req, call 0x612DAC50
AAA/FLTSV: method SERVER_GROUP myradius
AAA/FLTSV: recv reply, call 0x612DAC50 (PASS)
AAA/FLTSV: create cache
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: skip attr "filter-cache-refresh"
AAA/FLTSV: skip attr "filter-cache-time"
AAA/CACHE: set "AAA filtserv cache" entry "myfilter" refresh? no
AAA/CACHE: set "AAA filtserv cache" entry "myfilter" cachetime 15
```

```
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: PASS call 0x612DAC64
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (0 entries)
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (1 entry)
AAA/CACHE: destroy "AAA filtserv cache" entry "myfilter"
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (0 entries)
```

その他の参考資料

次の項で、RADIUS 集中型フィルタ管理に関する参考資料を紹介します。

関連資料

内容	参照先
認可の設定	「Configuring Authorization」フィーチャ モジュール
RADIUS の設定	「Configuring RADIUS」フィーチャ モジュール
認可コマンド	『*Cisco IOS Security Command Reference*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

RADIUS 集中型フィルタ管理の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　RADIUS 集中型フィルタ管理の機能情報

機能名	リリース	機能情報
RADIUS 集中型フィルタ管理	12.2(13)T 12.2(28)SB 12.2(33)SRC 1	RADIUS 集中型フィルタ管理機能は、ACL の設定と管理を容易にするフィルタ サーバを導入しています。このフィルタ サーバは、集中型 RADIUS リポジトリおよび管理ポイントとして機能します。ユーザは、Access Control List（ACL; アクセス コントロール リスト）フィルタを集中的に管理および設定できます。 この機能は、Cisco IOS Release 12.2(13)T で導入されました。 この機能は、Cisco IOS Release 12.2(28)SB に統合されました。 この機能は、Cisco IOS Release 12.2(33)SRC に統合されました。 **aaa authorization cache filterserver**、**aaa cache filter**、**cache clear age**、**cache disable**、**cache refresh**、**clear aaa cache filterserver acl**、**debug aaa cache filterserver**、**password**、および **show aaa cache filterserver** の各コマンドが、この機能で導入または変更されました。

RADIUS デバッグ拡張

このマニュアルでは、Remote Authentication Dial-In User Services（RADIUS; リモート認証ダイヤルイン ユーザ サービス）デバッグ拡張機能について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「RADIUS デバッグ拡張の機能情報」（P.8）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

RADIUS デバッグ拡張の前提条件

- 作業 IP ネットワークを構築します。IP の設定方法については、「Configuring IPv4 Addresses」モジュールを参照してください。
- ゲートウェイを RADIUS クライアントとして設定します。『*CDR Accounting for Cisco IOS Voice Gateways*』の「Configuring the Voice Gateway as a RADIUS Client」を参照してください。
- IETF RFC 2138 に精通している必要があります。

RADIUS デバッグ拡張の制約事項

音声アプリケーションで使用されている Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）アトリビュートと Cisco Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）のみがサポートされます。未サポートのアトリビュートは、「undebuggable」と表示されます。

RADIUS デバッグ拡張に関する情報

RADIUS デバッグ パラメータを有効にするには、次の概念を理解しておく必要があります。

- RADIUS の概要（P. 2）
- RADIUS デバッグ拡張のメリット（P. 3）

RADIUS の概要

RADIUS は、次の機能を提供する分散型クライアント / サーバ システムです。

- 不正アクセスからネットワークを保護します。
- 特定のサービス限界の認可を有効にします。
- サービスが課金できるようにアカウンティング情報を提供します。

シスコの実装では RADIUS クライアントは Cisco ルータ上で稼動します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

RADIUS デバッグ拡張のメリット

debug radius コマンドは、RADIUS の関連情報を表示します。RADIUS デバッグ拡張機能以前は、**debug radius** 出力が、解釈と分析が困難な拡張された 16 進文字列形式でしか使用できませんでした。さらに、アトリビュート値の表示が、特に、VSA の場合に途中で切れてしまいました。

この機能は、次のような高度な RADIUS 表示を提供します。

- 以前より読みやすく、使いやすい ASCII 形式でのパケット ダンプ
- 途中で切れないアトリビュート値の表示
- 簡易 RADIUS デバッグ出力表示も選択できる
- 通信量の多い運用環境に適した小型のデバッギング出力オプションを許可する

RADIUS デバッグ パラメータの有効化方法

ここでは、次の各手順について説明します。

- 「RADIUS デバッグ パラメータの有効化」（P.3）（任意）
- 「RADIUS デバッグ パラメータの確認」（任意）

RADIUS デバッグ パラメータの有効化

このタスクを実行して、RADIUS デバッグ パラメータを有効にします。デフォルトで、イベント ロギングが有効になっています。

（注） Cisco IOS Release 12.2(11)T 以前の **debug radius** コマンドは、ASCII ではなく、16 進表記の途中までのデバッギング出力を可能にしていました。

手順の概要

1. **enable**
2. **debug radius** [**accounting** | **authentication** | **brief** | **elog** | **failover** | **retransmit** | **verbose**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**debug radius** [**accounting** | **authentication** | **brief** | **elog** | **failover** | **retransmit** | **verbose**] 例： Router# debug radius accounting	RADIUS 設定に関連付けられた特定のパラメータに対してデバッギングを有効にします。

RADIUS デバッグ パラメータの確認

このタスクを実行して、RADIUS デバッグ パラメータを確認します。

手順の概要

1. **enable**
2. **show debug**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show debug** **例：** `Router# show debug`	デバッグ情報を表示します。

RADIUS デバッグ拡張の設定例

ここでは、次の設定例について説明します。

- 「RADIUS デバッグ パラメータの有効化：例」（P.4）
- 「RADIUS デバッグ パラメータの確認：例」（P.4）

RADIUS デバッグ パラメータの有効化：例

次の例は、RADIUS アカウンティング収集のデバッギングを可能にする方法を示しています。

```
Router> enable
Router# debug radius accounting

Radius protocol debugging is on
Radius protocol brief debugging is off
Radius protocol verbose debugging is off
Radius packet hex dump debugging is off
Radius packet protocol (authentication) debugging is off
Radius packet protocol (accounting) debugging is on
Radius packet retransmission debugging is off
Radius server fail-over debugging is off
Radius elog debugging is off
```

（注） 上のサンプル出力は、RADIUS プロトコル メッセージ内で見つかった情報を示しています。RADIUS プロトコル メッセージの詳細については、IETF RFC 2138 を参照してください。

RADIUS デバッグ パラメータの確認：例

次の例は、RADIUS デバッグ パラメータの確認方法を示しています。

```
Router> enable
Router# show debug

00:02:50: RADIUS: ustruct sharecount=3
00:02:50: Radius: radius_port_info() success=0 radius_nas_port=1
00:02:50: RADIUS: Initial Transmit ISDN 0:D:23 id 0 10.0.0.0:1824, Accounting-Request, len
358
00:02:50: RADIUS: NAS-IP-Address [4] 6 10.0.0.1
00:02:50: RADIUS: Vendor, Cisco [26] 19 VT=02 TL=13 ISDN 0:D:23
```

```
00:02:50: RADIUS: NAS-Port-Type [61] 6 Async
00:02:50: RADIUS: User-Name [1] 12 "4085274206"
00:02:50: RADIUS: Called-Station-Id [30] 7 "52981"
00:02:50: RADIUS: Calling-Station-Id [31] 12 "4085554206"
00:02:50: RADIUS: Acct-Status-Type [40] 6 Start
00:02:50: RADIUS: Service-Type [6] 6 Login
00:02:50: RADIUS: Vendor, Cisco [26] 27 VT=33 TL=21 h323-gw-id=5300_43.
00:02:50: RADIUS: Vendor, Cisco [26] 55 VT=01 TL=49 h323-incoming-conf-id=8F3A3163
B4980003 0 29BD0
00:02:50: RADIUS: Vendor, Cisco [26] 31 VT=26 TL=25 h323-call-origin=answer
00:02:50: RADIUS: Vendor, Cisco [26] 32 VT=27 TL=26 h323-call-type=Telephony
00:02:50: RADIUS: Vendor, Cisco [26] 57 VT=25 TL=51 h323-setup-time=*16:02:48.681 PST Fri
Dec 31 1999
00:02:50: RADIUS: Vendor, Cisco [26] 46 VT=24 TL=40 h323-conf-id=8F3A3163 B4980003 029BD0
00:02:50: RADIUS: Acct-Session-Id [44] 10 "00000002"
00:02:50: RADIUS: Delay-Time [41] 6 0
00:02:51: RADIUS: Received from id 0 10.0.0.0:1824, Accounting-response, len 20
00:02:51: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 4085554206
00:03:01: RADIUS: ustruct sharecount=3
00:03:01: Radius: radius_port_info() success=0 radius_nas_port=1
00:03:01: RADIUS: Initial Transmit ISDN 0:D:23 id 1 1.7.157.1:1823, Access-Request, len
171
00:03:01: RADIUS: NAS-IP-Address [4] 6 10.0.0.1
00:03:01: RADIUS: Vendor, Cisco [26] 19 VT=02 TL=13 ISDN 0:D:23
00:03:01: RADIUS: NAS-Port-Type [61] 6 Async
00:03:01: RADIUS: User-Name [1] 8 "123456"
00:03:01: RADIUS: Vendor, Cisco [26] 46 VT=24 TL=40 h323-conf-id=8F3A3163 B4980003 0 29BD0
00:03:01: RADIUS: Calling-Station-Id [31] 12 "4085274206"
00:03:01: RADIUS: User-Password [2] 18 *
00:03:01: RADIUS: Vendor, Cisco [26] 36 VT=01 TL=30 h323-ivr-out=transactionID:0
00:03:01: RADIUS: Received from id 1 1.7.157.1:1823, Access-Accept, len 115
00:03:01: RADIUS: Service-Type [6] 6 Login
00:03:01: RADIUS: Vendor, Cisco [26] 29 VT=101 TL=23 h323-credit-amount=45
00:03:01: RADIUS: Vendor, Cisco [26] 27 VT=102 TL=21 h323-credit-time=33
00:03:01: RADIUS: Vendor, Cisco [26] 26 VT=103 TL=20 h323-return-code=0
00:03:01: RADIUS: Class [25] 7 6C6F63616C
00:03:01: RADIUS: saved authorization data for user 62321E14 at 6233D258
00:03:13: %ISDN-6-DISCONNECT: Interface Serial0:22 disconnected from 4085274206, call
lasted 22 seconds
00:03:13: RADIUS: ustruct sharecount=2
00:03:13: Radius: radius_port_info() success=0 radius_nas_port=1
00:03:13: RADIUS: Sent class "local" at 6233D2C4 from user 62321E14
00:03:13: RADIUS: Initial Transmit ISDN 0:D:23 id 2 10.0.0.0:1824, Accounting-Request, len
775
00:03:13: RADIUS: NAS-IP-Address [4] 6 10.0.0.1
00:03:13: RADIUS: Vendor, Cisco [26] 19 VT=02 TL=13 ISDN 0:D:23
00:03:13: RADIUS: NAS-Port-Type [61] 6 Async
00:03:13: RADIUS: User-Name [1] 8 "123456"
00:03:13: RADIUS: Called-Station-Id [30] 7 "52981"
00:03:13: RADIUS: Calling-Station-Id [31] 12 "4085554206"
00:03:13: RADIUS: Acct-Status-Type [40] 6 Stop
00:03:13: RADIUS: Class [25] 7 6C6F63616C
00:03:13: RADIUS: Undebuggable [45] 6 00000001
00:03:13: RADIUS: Service-Type [6] 6 Login
00:03:13: RADIUS: Vendor, Cisco [26] 27 VT=33 TL=21 h323-gw-id=5300_43.
00:03:13: RADIUS: Vendor, Cisco [26] 55 VT=01 TL=49 h323-incoming-conf-id=8F3A3163
B4980003 0 29BD0
00:03:13: RADIUS: Vendor, Cisco [26] 31 VT=26 TL=25 h323-call-origin=answer
00:03:13: RADIUS: Vendor, Cisco [26] 32 VT=27 TL=26 h323-call-type=Telephony
00:03:13: RADIUS: Vendor, Cisco [26] 57 VT=25 TL=51 h323-setup-time=*16:02:48.681 PST Fri
Dec 31 1999
00:03:13: RADIUS: Vendor, Cisco [26] 59 VT=28 TL=53 h323-connect-time=*16:02:48.946
PST Fri Dec 31 1999
00:03:13: RADIUS: Vendor, Cisco [26] 62 VT=29 TL=56 h323-disconnect-time=*16:03:11.306
```

```
PST Fri Dec 31 1999
00:03:13: RADIUS: Vendor, Cisco [26] 32 VT=30 TL=26 h323-disconnect-cause=10
00:03:13: RADIUS: Vendor, Cisco [26] 28 VT=31 TL=22 h323-voice-quality=0
00:03:13: RADIUS: Vendor, Cisco [26] 46 VT=24 TL=40 h323-conf-id=8F3A3163 B4980003 0 29BD0
00:03:13: RADIUS: Acct-Session-Id [44] 10 "00000002"
00:03:13: RADIUS: Acct-Input-Octets [42] 6 0
00:03:13: RADIUS: Acct-Output-Octets [43] 6 88000
00:03:13: RADIUS: Acct-Input-Packets [47] 6 0
00:03:13: RADIUS: Acct-Output-Packets [48] 6 550
00:03:13: RADIUS: Acct-Session-Time [46] 6 22
00:03:13: RADIUS: Vendor, Cisco [26] 30 VT=01 TL=24 subscriber=RegularLine
00:03:13: RADIUS: Vendor, Cisco [26] 35 VT=01 TL=29 h323-ivr-out=Tariff:Unknown
00:03:13: RADIUS: Vendor, Cisco [26] 22 VT=01 TL=16 pre-bytes-in=0
00:03:13: RADIUS: Vendor, Cisco [26] 23 VT=01 TL=17 pre-bytes-out=0
00:03:13: RADIUS: Vendor, Cisco [26] 21 VT=01 TL=15 pre-paks-in=0
00:03:13: RADIUS: Vendor, Cisco [26] 22 VT=01 TL=16 pre-paks-out=0
00:03:13: RADIUS: Vendor, Cisco [26] 22 VT=01 TL=16 nas-rx-speed=0
00:03:13: RADIUS: Vendor, Cisco [26] 22 VT=01 TL=16 nas-tx-speed=0
00:03:13: RADIUS: Delay-Time [41] 6 0
00:03:13: RADIUS: Received from id 2 10.0.0.0:1824, Accounting-response, len 20
```

その他の参考資料

次の項で、RADIUS デバッグ拡張機能に関する参考資料を紹介します。

関連資料

内容	参照先
RADIUS の設定	「Configuring RADIUS」モジュール
デバッグ コマンド：完全なコマンド構文、デフォルト、コマンド モード、コマンド履歴、使用上のガイドライン、および例	『*Cisco IOS Debug Command Reference*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2138	「Remote Authentication Dial In User Service (RADIUS)」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

RADIUS デバッグ拡張の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　RADIUS デバッグ拡張の機能情報

機能名	リリース	機能情報
RADIUS デバッグ拡張	12.2(11)T	この機能は、既存の RADIUS デバッグ パラメータの機能に対する拡張を提供します。 この機能に関する詳細については、次の各項を参照してください。 • 「RADIUS デバッグ拡張に関する情報」（P.2） **debug radius** コマンドと **show debug** コマンドが導入または変更されました。

用語集

AAA：Authentication, Authorization, and Accounting（認証、認可、およびアカウンティング）。「トリプル エー」と発音します。

ASCII：American Standard Code for Information Interchange。文字を表現するための 8 ビット コード（7 ビット + パリティ）。

IETF：Internet Engineering Task Force（インターネット技術特別調査委員会）。インターネット標準の開発を担当する 80 を超えるワーキング グループで構成された調査委員会。IETF は ISOC の下部組織です。

RADIUS：Remote Authentication Dial-In User Service（リモート認証ダイヤルイン ユーザ サービス）。モデム接続と ISDN 接続を認証し、接続時間を追跡するためのデータベース。

VoIP：Voice over IP。POTS と同様の機能、信頼性、および音声品質を備えた、IP ベースのインターネット上で通常のテレフォニー スタイルの音声を伝送する機能。VoIP を使用すれば、ルータから IP ネットワーク上で音声トラフィック（通話や FAX など）を伝送できます。VoIP では、DSP が音声信号をフレームに分割します。その後、フレームは、2 つずつ連結され、音声パケットに保存されます。これらの音声パケットは、ITU-T 仕様の H.323 に従って、IP を使用して送信されます。

VSA：Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）。特定のベンダーによって実装されたアトリビュート。Vendor-Specific アトリビュートが使用された結果、AV ペアがカプセル化されます。基本的は、Vendor-Specific = プロトコル :attribute = 値となります。

アトリビュート：X.500 ディレクトリ サービスから提供される情報項目の形式。ディレクトリ情報ベースは、1 つ以上のアトリビュートを含むエントリで構成されます。各アトリビュートは、タイプ識別子と 1 つ以上の値で構成されます。

RADIUS 論理回線 ID

Logical Line Identification（LLID; 論理回線 ID）ブロッキング機能としても知られる RADIUS 論理回線 ID 機能を使用すれば、管理者は、顧客コールが発信された物理回線に基づいて顧客を追跡できます。管理者は、顧客が物理回線を移動しても変化しない仮想ポートを使用します。この仮想ポートは、管理者の顧客プロファイル データベースのメンテナンスを容易にし、管理者が顧客に対して追加のセキュリティ チェックを実施できるようにします。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「RADIUS 論理回線 ID の機能情報」（P.9）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

RADIUS 論理回線 ID の前提条件

この機能は任意の RADIUS サーバと一緒に使用できますが、RADIUS サーバによっては、Access-Accept メッセージで Calling-Station-ID アトリビュートを返せるようにディレクトリ ファイルを変更する必要があります。たとえば、「ATTRIBUTE　Calling-Station-Id　31　string (*, *)」のようにディレクトリを変更しなければ、Merit RADIUS サーバで LLID ダウンロードをサポートできません。

RADIUS 論理回線 ID の制約事項

RADIUS 論理回線 ID 機能は RADIUS のみをサポートしています。TACACS+ はサポートしていません。

この機能は、PPP over Ethernet over ATM（PPPoEoATM）コールと PPP over Ethernet over VLAN（PPPoEoVLAN）（Dot1Q）コールにしか適用できません。ISDN などのその他のコールは使用できません。

RADIUS 論理回線 ID に関する情報

LLID は、加入者線の論理識別を表す英数字文字列です（1 ～ 253 文字にする必要があります）。また、LLID は、RADIUS サーバ上の顧客プロファイル データベース上に保存されます。顧客プロファイル データベースがアクセス ルータから事前認可要求を受け取ると、RADIUS サーバが LLID を Calling-Station-ID アトリビュート（アトリビュート 31）としてルータに送信します。

Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）Access Concentrator（LAC; L2TP アクセス コンセントレータ）が、事前認可用に設定されている場合に、事前認可要求を顧客プロファイル データベースに送信します。**subscriber access** コマンドを使用して、LAC を事前認可用に設定します。

（注）　LLID のダウンロードは「事前認可」と呼ばれています。これは、サービス（ドメイン）認可またはユーザ認証および認可の前に実施されるためです。

RADIUS サーバ上の顧客プロファイル データベースは、ルータに接続された物理 Network Access Server（NAS; ネットワーク アクセス サーバ）ごとのユーザ プロファイルで構成されています。各ユーザ プロファイルには、ルータ上の物理ポートを表すユーザ名（アトリビュート 1）と一致したプロファイルが格納されています。ルータは、事前認可用に設定されている場合に、接続先の物理 NAS ポートの代表ユーザ名を使用して顧客プロファイル データベースに問い合わせます。顧客プロファイル データベース内で一致するものが見つかると、顧客プロファイル データベースが、ユーザ プロファイル内の LLID を含む Access-Accept メッセージを返します。LLID は、Calling-Station-ID アトリビュートとして Access-Accept レコード内に定義されています。

事前認可プロセスは、認証に使用される実際のユーザ名を RADIUS サーバに提供することもできます。物理 NAS ポート情報がユーザ名（アトリビュート 1）として使用されるため、RADIUS アトリビュート 77（Connect-Info）を認証ユーザ名を含めるように設定できます。この設定によって、RADIUS サーバは、LLID をルータに返す前に、選択した認可要求に対して追加の検証（プライバシー ルールに対するユーザ名の分析など）を実施できます。

RADIUS 論理回線 ID の設定方法

RADIUS 論理回線 ID 機能の設定タスクについては、次の各項を参照してください。一覧内の各作業は、必須と任意に分けています。

- 「事前認可の設定」（P.3）（必須）
- 「RADIUS ユーザ プロファイル内の LLID の設定」（P.4）（必須）
- 「論理回線 ID の確認」（P.4）（任意）

事前認可の設定

LLID をダウンロードして、LAC を事前認可用に設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip radius source-interface** *interface-name*
4. **subscriber access** {**pppoe** | **pppoa**} **pre-authorize nas-port-id** [**default** | *list-name*][**send username**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip radius source-interface** *interface-name* **例：** `Router (config)# ip radius source-interface Loopback1`	事前認可要求用のユーザ名の IP アドレス部分を指定します。
ステップ 4	**subscriber access** {**pppoe** | **pppoa**} **pre-authorize nas-port-id** [**default** | *list-name*][**send username**] **例：** `Router (config)# subscriber access pppoe pre-authorize nas-port-id mlist_llid send username`	LLID のダウンロードを可能にして、ルータを事前認可用に設定できるようにします。 **send username** オプションは、Access-Request メッセージ内の Connect-Info（アトリビュート 77）にセッションの認証ユーザ名を含めるように指定します。

RADIUS ユーザ プロファイル内の LLID の設定

ユーザ プロファイルを事前認可用に設定するには、顧客プロファイル データベースに NAS ポート ユーザを追加して、ユーザ プロファイルに RADIUS Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）アトリビュート 31（Calling-Station-ID）を追加します。

手順の概要

1. UserName=nas_port: ip-address:slot/module/port/vpi.vci
2. UserName=nas-port: ip-address:slot/module/port/vlan-id
3. Calling-Station-Id = "string (*,*)"

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	`UserName=nas_port: ip-address:slot/module/port/vpi.vci`	（任意）PPPoE over ATM NAS ポート ユーザを追加します。
ステップ 2	`User-Name=nas-port: ip-address:slot/module/port/vlan-id`	（任意）PPPoE over VLAN NAS ポート ユーザを追加します。
ステップ 3	`Calling-Station-Id = “string (*,*)”`	ユーザ プロファイルにアトリビュート 31 を追加します。 • String : ユーザがかけてきた電話番号を含む 1 つ以上のオクテット

論理回線 ID の確認

機能を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **debug radius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**`enable`** **例 :** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**`debug radius`** **例 :** `Router# debug radius`	RADIUS アトリビュート 31 が、LAC 上の Accounting-Request と、LNS 上の Access-Request および Accounting-Request 内の LLID であることを確認します。

RADIUS 論理回線 ID の設定例

ここでは、次の設定例について説明します。

- 「事前認可用の LAC 設定：例」（P.5）
- 「LLID 用の RADIUS ユーザ プロファイル：例」（P.6）

事前認可用の LAC 設定：例

次の例は、LLID をダウンロードすることによって、LAC を事前認可用に設定する方法を示しています。

```
aaa new-model
aaa group server radius sg_llid
 server 172.31.164.106 auth-port 1645 acct-port 1646
aaa group server radius sg_water
 server 172.31.164.106 auth-port 1645 acct-port 1646
aaa authentication ppp default group radius
aaa authorization confg-commands
aaa authorization network default group sg_water
aaa authorization network mlist_llid group sg_llid
aaa session-id common
!
username s7200_2 password 0 lab
username s5300 password 0 lab
username sg_water password 0 lab
vpdn enable
!
vpdn-group 2
 request-dialin
 protocol l2tp
 domain water.com
 domain water.com#184
 initiate-to ip 10.1.1.1
 local name s7200_2
 l2tp attribute clid mask-method right * 255 match #184
!
vpdn-group 3
 accept dialin
  procotol pppoe
  virtual-template 1
!
! Enable the LLID to be downloaded.
subscriber access pppoe pre-authorize nas-port-id mlist_llid send username
!
interface Loopback0
 ip address 10.1.1.2 255.255.255.0
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet1/0
 ip address 10.1.1.8 255.255.255.0 secondary
 ip address 10.0.58.111 255.255.255.0
 no cdp enable
!
interface ATM4/0
 no ip address
 no atm ilmi-keepalive
!
```

```
interface ATM4/0.1 point-to-point
 pvc 1/100
  encapsulation aa15snap
  protocol pppoe
!
interface virtual-template1
 no ip unnumbered Loopback0
 no peer default ip address
 ppp authentication chap
!
radius-server host 172.31.164.120 auth-port 1645 acct-port 1646 key rad123
radius-server host 172.31.164.106 auth-port 1645 acct-port 1646 key rad123
ip radius source-interface Loopback1
```

LLID 用の RADIUS ユーザ プロファイル：例

次の例は、ユーザ プロファイルを PPPoEoVLAN および PPPoEoATM に対する LLID 問い合わせ用に設定する方法とアトリビュート 31 の追加方法を示しています。

```
pppoeovlan
----------
nas-port:10.1.0.3:6/0/0/0    Password = "cisco",
    Service-Type = Outbound,
    Calling-Station-ID = "cat-example"

pppoeoa
--------
nas-port:10.1.0.3:6/0/0/1.100    Password = "cisco",
    Service-Type = Outbound,
    Calling-Station-ID = "cat-example"
```

その他の参考資料

次の項で、RADIUS 論理回線 ID に関する参考資料を紹介します。

関連資料

内容	参照先
AAA 認証	「Configuring RADIUS」モジュールの「Configuring AAA Preauthentication」の項
アクセス要求のアトリビュート スクリーニング	「Configuring RADIUS」モジュールの「RADIUS Attribute Screening」の項
ブロードバンド アクセス：PPP とルーテッド ブリッジ エンカプセレーション	『*Cisco IOS Broadband Access Aggregation and DSL Configuration Guide*, Release 12.4T』
ダイヤル テクノロジー	『*Cisco IOS Dial Technologies Configuration Guide*, Release 12.4T』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

RADIUS 論理回線 ID の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　RADIUS 論理回線 ID の機能情報

機能名	リリース	機能情報
RADIUS 論理回線 ID	12.2(13)T 12.2(15)B 12.3(14)YM1 12.4(2)T 12.3(14)YM2 12.2(28)SB 12.2(31)SB2 12.2(33)SRC	Logical Line Identification（LLID; 論理回線 ID）ブロッキング機能としても知られる RADIUS 論理回線 ID 機能を使用すれば、管理者は、顧客コールが発信された物理回線に基づいて顧客を追跡できます。 この機能は、Cisco IOS Release 12.2(13)T で導入されました。 この機能は、Cisco IOS Release 12.2(15)B に統合されました。 この機能は、Cisco IOS Release 12.3(14)YM1 に統合され、**subscriber access** コマンドに **send username** キーワードが追加されました。 この機能は、Cisco IOS Release 12.4(2)T に統合されました。 この機能は、Cisco IOS Release 12.3(14)YM2 に統合されました。 この機能は、Cisco IOS Release 12.2(28)SB に統合されました。 この機能は、Cisco IOS Release 12.2(31)SB2 に統合されました。 この機能は、Cisco IOS Release 12.2(33)SRC に統合されました。 この機能により、**subscriber access** コマンドが導入されました。

用語集

LLID ブロッキング：管理者が、顧客のコールが発信された物理回線に基づいて顧客を追跡できるようにする機能。RADIUS 論理回線 ID としても知られています。

RADIUS 論理回線 ID：管理者が、顧客のコールが発信された物理回線に基づいて顧客を追跡できるようにする機能。LLID ブロッキングとしても知られています。

RADIUS NAS-IP-Address アトリビュート設定可能性

RADIUS NAS-IP-Address アトリビュート設定可能性機能を使用すれば、RADIUS パケットの IP ヘッダー内の発信元 IP アドレスを変更せずに、任意の IP アドレスを設定して RADIUS アトリビュート 4（NAS-IP-Address）として使用できます。この機能は、サービス プロバイダーが、スケーラビリティを向上させるために、小規模な Network Access Server（NAS; ネットワーク アクセス サーバ）のクラスタを使用して大規模な NAS をシミュレートしている場合にも使用できます。この機能を使用すれば、NAS を RADIUS サーバから見て、単一の RADIUS クライアントとして機能させることができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「RADIUS NAS-IP-Address アトリビュート設定可能性の機能情報」（P.8）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

- 「RADIUS NAS-IP-Address アトリビュート設定可能性の機能情報」（P.8）

RADIUS NAS-IP-Address アトリビュート設定可能性の前提条件

この機能を設定する前に、次の要件を満たす必要があります。

- IP セキュリティ（IPSec）の使用経験と、RADIUS サーバと Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）の両方の設定経験が必要です。
- RADIUS サーバと AAA リストを設定する必要があります。

RADIUS NAS-IP-Address アトリビュート設定可能性の制約事項

スケーラビリティを向上させるために、RADIUS クライアントのクラスタを単一の RADIUS クライアントのシミュレーションに使用している場合に、次の制約事項が適用されます。制約事項に対する解決策または次善策についても説明します。

- RADIUS アトリビュート 44（Acct-Session-Id）は、複数の NAS からのセッション間で重複する可能性があります。

  2 つの解決策があります。NAS ルータ上で **radius-server attribute 44 extend-with-addr** コマンドと **radius-server unique-ident** コマンドのどちらかを使用して、NAS ルータごとに異なる先頭の番号を指定できます。

- RADIUS サーバベースの IP アドレス プールを NAS ごとに管理する必要があります。

  この解決策は、RADIUS サーバ上で NAS ごとに異なる IP アドレス プール プロファイルを設定することです。NAS ごとに異なるプール ユーザ名を使用してそれらを取得します。

- セッション内の RADIUS 要求メッセージは NAS ごとに識別される必要があります。

  この解決策の 1 つは、NAS 上で **radius-server attribute 32 include-in-access-req** コマンドを使用して、NAS ごとに異なる RADIUS アトリビュート 32（NAS-Identifier）用の形式文字列を設定することです。

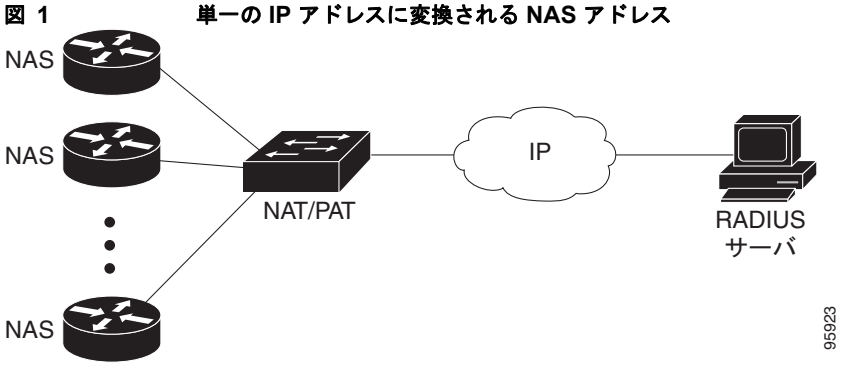
RADIUS NAS-IP-Address アトリビュート設定可能性に関する情報

図 1 に示すように、小規模な NAS RADIUS クライアントを使用して大規模な NAS RADIUS クライアントをシミュレートする場合は、Network Address Translation（NAT; ネットワーク アドレス変換）デバイスまたは Port Address Translation（PAT; ポート アドレス変換）デバイスがネットワークに挿入されます。このデバイスは、NAS のクライアントと、RADIUS サーバに接続された IP クラウドの間に配置されます。複数の NAS からの RADIUS トラフィックが NAT または PAT デバイスを通過するときに、RADIUS パケットの発信元 IP アドレスが単一の IP アドレスに変換されます。ほとんどの場合、この IP アドレスは、NAT または PAT デバイスのループバック インターフェイス上の IP アドレスです。NAS ごとに異なる User Datagram Protocol（UDP; ユーザ データグラム プロトコル）発信元プー

ルが RADIUS パケットに割り当てられます。サーバから RADIUS 応答が返されると、NAT または PAT デバイスがそれを受信して、宛先 UDP ポートを使用して宛先 IP アドレスを NAS の IP アドレスに変換し、対応する NAS に転送します。

図 1 は、複数の NAS の発信元 IP アドレスが、IP クラウドへの途中で NAT または PAT デバイスを通過するときに、どのように単一の IP アドレスに変換されるかを示しています。

図 1　単一の IP アドレスに変換される NAS アドレス



通常は、RADIUS サーバが RADIUS パケットの IP ヘッダー内の発信元 IP アドレスをチェックして、RADIUS 要求の発信元を追跡し、セキュリティを確保します。NAT または PAT による解決策は、RADIUS パケットが複数の NAS ルータから送られてきても単一の発信元 IP アドレスが使用されるため、これらの要件を満たします。

ただし、RADIUS データベースからアカウンティング レコードを取得するときに、課金システムによっては、アカウンティング レコード内で RADIUS アトリビュート 4（NAS-IP-Address）が使用される場合があります。このアトリビュートの値は、独自の IP アドレスとして NAS ルータ上に記録されます。NAS ルータは、RADIUS サーバとの間で動作している NAT または PAT を認識しません。そのため、NAS ルータごとに異なる RADIUS アトリビュート 4 アドレスがユーザのアカウンティング レコードに記録されます。最終的に、これらのアドレスは、複数の NAS ルータを RADIUS サーバと対応する課金システムに公開することになります。

RADIUS NAS-IP-Address アトリビュート設定可能性機能の使用方法

RADIUS NAS-IP-Address アトリビュート設定可能性機能を使用すれば、任意の IP アドレスを RADIUS NAS-IP-Address（RADIUS アトリビュート 4）として設定できます。すべてのルータに対して同じ IP アドレス（ほとんどの場合、NAT または PAT デバイスのループバック インターフェイス上の IP アドレス）を手動で設定することによって、NAS ルータのクラスタを NAT または PAT デバイスの後ろに隠して、RADIUS から見えないようにすることができます。

RADIUS NAS-IP-Address アトリビュート設定可能性の設定方法

ここでは、次の各手順について説明します。

- 「RADIUS NAS-IP-Address アトリビュート設定可能性の設定」（P.4）
- 「RADIUS NAS-IP-Address アトリビュート設定可能性のモニタリングとメンテナンス」（P.4）

RADIUS NAS-IP-Address アトリビュート設定可能性の設定

RADIUS NAS-IP-Address アトリビュート設定可能性機能を設定する前に、RADIUS サーバまたはサーバ グループと AAA 方式リストを設定しておく必要があります。

RADIUS NAS-IP-Address アトリビュート設定可能性機能を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server attribute 4** *ip-address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server attribute 4** *ip-address* 例： `Router (config)# radius-server attribute 4 10.2.1.1`	RADIUS NAS-IP-Address（アトリビュート 4）として使用する IP アドレスを設定します。

RADIUS NAS-IP-Address アトリビュート設定可能性のモニタリングとメンテナンス

RADIUS パケット内で使用されている RADIUS アトリビュート 4 アドレスをモニタするには、**debug radius** コマンドを使用します。

手順の概要

1. **enable**
2. **debug radius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**debug radius** 例： Router# debug radius	RADIUS 関連の情報を表示します。

例

次のサンプル出力は、**debug radius** コマンドの出力です。

```
Router# debug radius

RADIUS/ENCODE(0000001C): acct_session_id: 29
RADIUS(0000001C): sending
RADIUS(0000001C): Send Access-Request to 10.0.0.10:1645 id 21645/17, len 81
RADIUS:  authenticator D0 27 34 C0 F0 C4 1C 1B - 3C 47 08 A2 7E E1 63 2F
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  User-Name           [1]   18  "shashi@pepsi.com"
RADIUS:  CHAP-Password       [3]   19  *
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.0.0.21
UDP: sent src=10.1.1.1(21645), dst=10.0.0.10(1645), length=109
UDP: rcvd src=10.0.0.10(1645), dst=10.1.1.1(21645), length=40
RADIUS: Received from id 21645/17 10.0.0.10:1645, Access-Accept, len 32
RADIUS:  authenticator C6 99 EC 1A 47 0A 5F F2 - B8 30 4A 4C FF 4B 1D F0
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS(0000001C): Received from id 21645/17
```

RADIUS NAS-IP-Address アトリビュート設定可能性の設定例

ここでは、次の設定例について説明します。

- 「RADIUS NAS-IP-Address アトリビュート設定可能性の設定：例」（P.5）

RADIUS NAS-IP-Address アトリビュート設定可能性の設定：例

次の例は、IP アドレス 10.0.0.21 が RADIUS NAS-IP-Address アトリビュートとして設定されていることを示しています。

```
radius-server attribute 4 10.0.0.21
radius-server host 10.0.0.10 auth-port 1645 acct-port 1646 key cisco
```

その他の参考資料

次の項で、RADIUS NAS-IP-Address アトリビュート設定可能性に関する参考資料を紹介します。

関連資料

内容	参照先
AAA の設定	『*Cisco IOS Security Configuration Guide: Securing User Services*』の「Authentication, Authorization, and Accounting (AAA)」の項
RADIUS の設定	「Configuring RADIUS」モジュール
RADIUS コマンド	『*Cisco IOS Security Command Reference*』

規格

規格	タイトル
この機能によってサポートされる新しい規格や変更された規格はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によってサポートされる新しい RFC や変更された RFC はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

RADIUS NAS-IP-Address アトリビュート設定可能性の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　RADIUS NAS-IP-Address アトリビュート設定可能性の機能情報

機能名	リリース	機能情報
RADIUS NAS-IP-Address アトリビュート設定可能性	12.3(3)B 12.3(7)T 12.2(28)SB 12.2(33)SRC	この機能を使用すれば、RADIUS パケットの IP ヘッダー内の発信元 IP アドレスを変更せずに、任意の IP アドレスを設定して RADIUS アトリビュート 4（NAS-IP-Address）として使用できます。 この機能は、Cisco IOS Release 12.3(3)B で導入されました。 この機能は、Cisco IOS Release 12.3(7)T に統合されました。 この機能は、Cisco IOS Release 12.2(28)SB に統合されました。 この機能は、Cisco IOS Release 12.2(33)SRC に統合されました。 **radius-server attribute 4** コマンドがこの機能で導入されました。

RADIUS NAS-IP-Address アトリビュート設定可能性の機能情報

RADIUS ルート ダウンロード

RADIUS ルート ダウンロード機能を使用すれば、RADIUS 認可を転送するように Network Access Server（NAS; ネットワーク アクセス サーバ）を設定できます。ユーザは、NAS から Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）に送信される静的ルート ダウンロード要求用として、もう一つの名前付き方式リスト（デフォルトの方式リストに加えて）を設定できます。

この機能以前は、静的ルート ダウンロード要求用の RADIUS 認可が、デフォルトの方式リストで指定された AAA サーバにのみ送信されていました。

この機能では、AAA サーバへの静的ルート ダウンロード要求の転送に使用される方式リストの名前を指定できるように **aaa route download** コマンドの機能が拡張されています。**aaa route download** コマンドは、静的ルートをダウンロードするためのもう一つの方式リストを指定するために使用できます。この方式リストは、**aaa authorization configuration** コマンドを使用して追加できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「RADIUS ルート ダウンロードの機能情報」（P.6）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

前提条件

この機能でタスクを実行する前に、AAA ネットワーク セキュリティを有効にする必要があります。

設定作業

次の項を使用して、RADIUS ルート ダウンロード機能を設定します。

- 「RADIUS ルート ダウンロードの設定」
- 「RADIUS ルート ダウンロードの確認」

RADIUS ルート ダウンロードの設定

名前付き方式リストで指定されたサーバに静的ルート ダウンロード要求を送信するように NAS を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router(config)# **aas authorization configuration** *method-name* **[radius | tacacs+ | group** *group-name***]**	RADIUS を使用して AAA サーバから静的ルート設定情報をダウンロードします。
ステップ 2	Router(config)# **aaa route download** [*time*] [**authorization** *method-list*]	静的ルート ダウンロード機能を有効にします。**authorization** *method-list* アトリビュートを使用して、静的ルート ダウンロード用の RADIUS 認可要求が送信される名前付き方式リストを指定します。

RADIUS ルート ダウンロードの確認

インストールされているルートを確認するには、EXEC モードで **show ip route** コマンドを使用します。

RADIUS に関連付けられた情報を表示するには、特権 EXEC モードで **debug radius** コマンドを使用します。

設定例

ここでは、次の設定例について説明します。

- 「RADIUS ルート ダウンロード設定：例」

RADIUS ルート ダウンロード設定：例

次の例は、静的ルート ダウンロード要求を「list1」という名前の方式リストで指定されたサーバに送信するように NAS を設定する方法を示しています。

```
aaa new-model
aaa group server radius rad1
    server 10.2.2.2 auth-port 1645 acct-port 1646
!
aaa group server tacacs+ tac1
    server 172.17.3.3
!
aaa authorization configuration default group radius
aaa authorization configuration list1 group rad1 group tac1
aaa route download 1 authorization list1

tacacs-server host 172.17.3.3
tacacs-server key cisco
tacacs-server administration
!
radius-server host 10.2.2.2 auth-port 1645 acct-port 1646
radius-server key cisco
```

その他の参考資料

次の項で、RADIUS ルート ダウンロードに関する参考資料を紹介します。

関連資料

内容	参照先
Large-Scale Dial-Out の設定	『*Cisco IOS Dial Technologies Command Reference*』
Cisco IOS Dial Technologies	

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

RADIUS ルート ダウンロードの機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　RADIUS ルート ダウンロードの機能情報

機能名	リリース	機能情報
RADIUS ルート ダウンロード	12.2(8)T 12.2(28)SB 12.2(33)SRC	RADIUS ルート ダウンロード機能を使用すれば、RADIUS 認可を転送するように Network Access Server（NAS; ネットワーク アクセス サーバ）を設定できます。ユーザは、NAS から Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）に送信される静的ルート ダウンロード要求用として、もう一つの名前付き方式リスト（デフォルトの方式リストに加えて）を設定できます。 **aaa route download** コマンドがこの機能で導入されました。

RADIUS サーバ ロード バランシング

RADIUS サーバ ロード バランシング機能は、Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）の認証トランザクションとアカウンティング トランザクションをサーバ グループ内のサーバに分配します。これらのサーバは、トランザクションの負荷を分担し、空いているサーバを効率的に使用して着信要求に対するより迅速な応答を実現します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「RADIUS サーバ ロード バランシングの機能情報」（P.20）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

RADIUS サーバ ロード バランシングの前提条件

- RADIUS サーバ上で AAA を設定する必要があります。
- 認証、アカウンティング、スタティック ルート ダウンロードなどの機能用に RADIUS を設定する必要があります。
- AAA RADIUS サーバ グループを設定する必要があります。

RADIUS サーバ ロード バランシングの制約事項

- プロキシ RADIUS サーバ上でロード バランシングはサポートされていません。
- Packet of Disconnect（POD; パケット オブ ディスコネクト）要求などの着信 RADIUS 要求はサポートされていません。
- プライベート サーバ グループのロード バランシングはサポートされていません。

RADIUS サーバ ロード バランシングについて

RADIUS サーバ ロード バランシング機能を設定するには、次の概念を理解しておく必要があります。

- 「RADIUS サーバ ロード バランシングの機能」（P.2）
- 「RADIUS サーバ グループ全体でトランザクションを負荷分散する方法」（P.3）
- 「RADIUS サーバ ステータスと自動テスト」（P.3）

RADIUS サーバ ロード バランシングの機能

ロード バランシングは、トランザクションのバッチをサーバ グループ内のサーバに分配します。トランザクションの各バッチは、キュー内の未処理トランザクションの最小番号を使用して、サーバに割り当てられます。トランザクションのバッチの割り当てプロセスは次のとおりです。

- 最初のトランザクションが新しいバッチとして受信されます。
- すべてのサーバ トランザクション キューがチェックされます。
- 最小番号の未処理トランザクションを持つサーバが特定されます。
- 特定されたサーバが、トランザクションの次のバッチに割り当てられます。

バッチ サイズはユーザ設定パラメータです。バッチ サイズを変更すると、CPU の負荷やネットワークのスループットに影響する可能性があります。バッチ サイズが大きくなるほど、CPU の負荷が減少し、ネットワークのスループットが増加します。ただし、バッチ サイズが大きくても、使用可能なすべてのサーバ リソースが使い果たされることはありません。バッチ サイズが小さくなるほど、CPU の負荷が増加し、ネットワークのスループットが減少します。デフォルト バッチ サイズの 25 の使用を推奨します。これは、CPU の負荷に悪影響を及ぼさない、高スループットに最適化されているためです。

（注） 大きなバッチ サイズまたは小さなバッチ サイズに関する設定数はありません。目安として、50 を超えるバッチ サイズは大きいと見なされ、25 未満のバッチ サイズは小さいと見なされます。

（注） サーバ グループ内に 10 以上のサーバが存在する場合は、CPU の負荷を軽減するために、高いバッチサイズの設定を推奨します。

RADIUS サーバ グループ全体でトランザクションを負荷分散する方法

名前付き RADIUS サーバ グループごと、またはグローバル RADIUS サーバ グループに対してロードバランシングを設定できます。このサーバ グループは、AAA 方式リストで「radius」として参照する必要があります。このサーバ グループに属しているすべてのパブリック サーバが負荷分散の対象になります。

認証とアカウンティングは、同じサーバを使用するようにも、別々のサーバを使用するようにも設定できます。1 つのサーバをセッションの事前認証、認証、またはアカウンティング トランザクションに使用することもできます。内部設定であり、デフォルトとして設定される優先サーバが、AAA に、サーバ コストに関係なく、セッションの開始レコードと終了レコードに対して同じサーバを使用するように指示します。優先サーバ設定を使用する場合は、初期トランザクション（認証など）に使用されるサーバが、以降のトランザクション（アカウンティングなど）に使用される他のサーバ グループにも属している必要があります。

優先サーバは、次のいずれかの状態が真でない場合に使用されます。

- **ignore-preferred-server** キーワードが使用されている。
- 優先サーバが停止中である。
- 優先サーバが隔離中である。
- 必要サーバ フラグがセットされている場合は、優先サーバ設定が無効になります。

必要サーバ フラグの内部設定は、サーバ コストに関係なく、マルチステージ トランザクションのすべてのステージに対して同じサーバを使用する必要がある場合に、使用されます。必要サーバが使用できない場合は、トランザクションが失敗します。

次の設定の場合は、**ignore-preferred-server** キーワードを使用できます。

- 専用の認証サーバと別の専用のアカウンティング サーバ
- 開始レコードと終了レコードを含む、すべてのコール レコード統計情報とコール レコード詳細、および別々のサーバに保存されたレコードを追跡可能なネットワーク

また、認証サーバをアカウンティング サーバのスーパーセットとして設定している場合は、優先サーバが使用されません。

RADIUS サーバ ステータスと自動テスト

RADIUS サーバ ロード バランシング機能は、バッチを割り当てるときにサーバ ステータスを考慮します。動作中であることが確認されたサーバにだけ、トランザクション バッチが送信されます。あまり使用されていないサーバ（バックアップ サーバなど）を含む、すべての RADIUS ロード バランシング サーバのステータスをテストすることを推奨します。

停止中としてマークされたサーバにはトランザクションが送信されません。隔離されたサーバは、タイマーが切れるまで停止中としてマークされます。RADIUS 自動テスタ機能によって動作中であることが確認されるまでサーバは隔離中になります。

RADIUS 自動テスタは、次の手順を使用して、サーバが動作中でトランザクションを処理できるかどうかを判断します。

- 定期的に要求がテスト ユーザ ID としてサーバに送信されます。

- Access-Reject メッセージがサーバから返された場合、サーバは動作中です。
- メッセージがサーバから返されなかった場合、サーバは動作中ではありません。つまり、停止中か隔離中のどちらかです。

トランザクションが、応答しないサーバに送信された場合は、サーバが停止中としてマークされる前に、トランザクションが次の使用可能なサーバにフェールオーバーされます。失敗したトランザクションに対して再試行順序変更モードの使用を推奨します。

RADIUS 自動テスタを使用している場合は、Network Access Server（NAS; ネットワーク アクセス サーバ）から AAA サーバに送信されたテスト パケットに対して応答が返されることを確認します。サーバが正しく設定されていない場合は、パケットが破棄され、サーバが誤って停止中としてマークされる可能性があります。

注意 RADIUS サーバ上で定義されていないテスト ユーザを RADIUS サーバ自動テストに使用して、テスト ユーザが正しく設定されていない場合に発生するセキュリティ上の問題を解決することを推奨します。

（注） 特定の時点でトランザクションのロード バランシングをチェックしたい場合は、**test aaa group** コマンドを使用できます。

RADIUS サーバ ロード バランシング の設定方法

この項では、ロード バランシングを設定するための次の手順について説明します。

- 「名前付き RADIUS サーバ グループのロード バランシングの有効化」（P.4）
- 「グローバル RADIUS サーバ グループのロード バランシングの有効化」（P.5）
- 「RADIUS サーバ ロード バランシングのトラブルシューティング」（P.7）

名前付き RADIUS サーバ グループのロード バランシングの有効化

次のタスクを使用して、名前付きサーバ グループに対して RADIUS サーバ ロード バランシングを有効にします。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**idle-time** *seconds*]
4. **aaa group server radius** *group-name*
5. **load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**idle-time** *seconds*] 例： Router(config)# radius-server host 192.0.2.1 test username test1 idle-time 1	RADIUS 自動テストを有効にします。 • **test username** キーワードは、*user-name* 引数の値の前に使用して、RADIUS 自動テストを有効にする必要があります。 • デフォルトで、**auth-port** はポート 1645 を使用してテストされます。 • **ignore-auth-port** を使用して、認証ポートのテストをオフにします。 • デフォルトで、**acct-port** はポート 1645 を使用してテストされます。 • **ignore-auth-port** を使用して、アカウンティングポートのテストをオフにします。 • デフォルトで、**idle-time** は 3600 秒です。範囲は 1 ～ 35791 です。
ステップ 4	**aaa group server radius** *group-name* 例： Router(config)# aaa group server radius rad-sg	サーバ グループ コンフィギュレーション モードに入ります。
ステップ 5	**load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**] 例： Router(config-sg)# load-balance method least-outstanding batch-size 30	サーバ グループに対して最小未処理ロード バランシングを有効にします。 • デフォルトで、**batch-size** は 25 に設定されます。1 ～ 2147483647 の範囲を使用できます。 • デフォルトで、優先サーバは有効になっています。 • 優先サーバ設定を無効にする場合は、キーワード **ignore-preferred-server** を使用します。

グローバル RADIUS サーバ グループのロード バランシングの有効化

次のタスクを使用して、グローバル RADIUS サーバ グループに対して RADIUS サーバ ロード バランシングを有効にします。このグループは、AAA 方式リスト内で「radius」として参照されます。

手順の概要

1. **enable**

2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**idle-time** *seconds*]
4. **radius-server load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**]
5. **load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**idle-time** *seconds*] 例： `Router(config)# radius-server host 192.0.2.1 test username test1 idle-time 1`	RADIUS 自動テストを有効にします。 • **test username** キーワードは、*user-name* 引数の値の前に使用して、RADIUS 自動テストを有効にする必要があります。 • デフォルトで、**auth-port** はポート 1645 を使用してテストされます。 • **ignore-auth-port** を使用して、認証ポートのテストをオフにします。 • デフォルトで、**acct-port** はポート 1645 を使用してテストされます。 • **ignore-auth-port** を使用して、アカウンティングポートのテストをオフにします。 • デフォルトで、**idle-time** は 3600 秒です。範囲は 1 ～ 35791 です。

	コマンドまたはアクション	目的
ステップ 4	**radius-server load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**] 例： `Router(config)# radius-server load-balance method least-outstanding`	グローバル RADIUS サーバ グループに対して最小未処理ロード バランシングを有効にし、サーバ グループ コンフィギュレーション モードに入ります。 • デフォルトで、**batch-size** は 25 に設定されます。1 ～ 2147483647 の範囲を使用できます。 （注） バッチ サイズがスループットと CPU の負荷に影響する場合があります。デフォルト バッチ サイズの 25 の使用を推奨します。これは、CPU の負荷に悪影響を及ぼさない、高スループットに最適化されているためです。 • デフォルトで、優先サーバは有効になっています。 • 優先サーバ設定を無効にする場合は、**ignore-preferred-server** キーワードを使用します。
ステップ 5	**load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**] 例： `load-balance method least-outstanding batch-size 5`	名前付き RADIUS サーバ グループに対して RADIUS サーバ ロード バランシングを有効にします。 • デフォルトで、**batch-size** は 25 に設定されます。1 ～ 2147483647 の範囲を使用できます。 • デフォルトで、優先サーバは有効になっています。 • 優先サーバ設定を無効にする場合は、**ignore-preferred-server** キーワードを使用します。

RADIUS サーバ ロード バランシングのトラブルシューティング

RADIUS サーバ ロード バランシング機能を設定したら、アイドル タイマー、デッド タイマー、ロード バランシング サーバの選択をモニタしたり、手動テスト コマンドを発行してサーバ ステータスを確認したりすることができます。

必要に応じて、次のコマンドを使用してRADIUS サーバ ロード バランシング機能をトラブルシューティングします。

- **debug aaa test** コマンドは、アイドル タイマーまたはデッド タイマーが切れた時点、テスト パケットが送信された時点、およびサーバのステータスを判断したり、サーバの状態を確認したりするために使用できます。
- **debug aaa sg-server selection** コマンドは、ロード バランシング用に選択されたサーバを調査するために使用できます。
- **test aaa group** コマンドは、手動で RADIUS ロード バランシング サーバのステータスを確認するために使用できます。

手順の概要

1. **debug aaa test**
2. **debug aaa sg-server selection**
3. **test aaa group** *group-name username password* **new-code**

手順の詳細

ステップ 1 アイドル タイマーは、サーバ ステータスのチェックに使用され、着信要求の有無に関係なく更新されます。このタイマーは、アイドル タイマーをモニタして無応答サーバが存在するかどうかを判断したり、RADIUS サーバのステータスを最新状態に維持して使用可能なリソースを効率的に使用したりするときに役立ちます。たとえば、アイドル タイマーが更新されていれば、着信要求が動作中のサーバに送信されていることが簡単に確認できます。

デッド タイマーは、サーバが停止中であることを特定したり、停止中のサーバのステータスを適切に更新したりするために使用します。

サーバ選択のモニタリングは、サーバ選択の変更頻度の特定に役立つ可能性があります。これは、ボトルネック、つまり、キュー内の大量のアップ要求が存在するかどうかや、特定のサーバだけが着信要求を処理しているかどうかの分析に有効です。

たとえば、次のデバッグ出力は、アイドル タイマーが切れた時点を表しています。

```
Router# debug aaa test

Jul 16 00:07:01: AAA/SG/TEST: Server (192.0.2.245:1700,1701) quarantined.
Jul 16 00:07:01: AAA/SG/TEST: Sending test request(s) to server (192.0.2.245:1700,1701)
Jul 16 00:07:01: AAA/SG/TEST: Sending 1 Access-Requests, 1 Accounting-Requests in current
batch.
Jul 16 00:07:01: AAA/SG/TEST(Req#: 1): Sending test AAA Access-Request.
Jul 16 00:07:01: AAA/SG/TEST(Req#: 1): Sending test AAA Accounting-Request.
Jul 16 00:07:01: AAA/SG/TEST: Obtained Test response from server (192.0.2.245:1700,1701)
Jul 16 00:07:01: AAA/SG/TEST: Obtained Test response from server (192.0.2.245:1700,1701)
Jul 16 00:07:01: AAA/SG/TEST: Necessary responses received from server
(192.0.2.245:1700,1701)
Jul 16 00:07:01: AAA/SG/TEST: Server (192.0.2.245:1700,1701) marked ALIVE. Idle timer set
for 60 sec(s).
Jul 16 00:07:01: AAA/SG/TEST: Server (192.0.2.245:1700,1701) removed from quarantine.
```

ステップ 2 たとえば、次のデバッグ出力は、バッチ サイズが 3 のサーバ グループに 5 つのアクセス要求が送信されたことを示しています。

```
Router# debug aaa sg-server selection

Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [3] transactions remaining in batch. Reusing
server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [2] transactions remaining in batch. Reusing
server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [1] transactions remaining in batch. Reusing
server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: No more transactions in batch. Obtaining a new
server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining a new least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Server[0] load: 3
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Server[1] load: 0
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Server[2] load: 0
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Selected Server[1] with load 0
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [3] transactions remaining in batch.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [2] transactions remaining in batch. Reusing
server.
```

ステップ 3 次の例は、ユーザ名の「test」がユーザ プロファイルと一致しない場合の動作中の RADIUS ロード バランシング サーバからの応答を示しています。サーバは、**test aaa group** コマンドで生成された AAA パケットに対する Access-Reject 応答を発行した時点で動作中であることが確認されます。

```
Router# test aaa group SG1 test lab new-code

00:06:07: RADIUS/ENCODE(00000000):Orig. component type = INVALID
00:06:07: RADIUS/ENCODE(00000000): dropping service type, "radius-server attribute 6
on-for-login-auth" is off
00:06:07: RADIUS(00000000): Config NAS IP: 192.0.2.4
00:06:07: RADIUS(00000000): sending
00:06:07: RADIUS/ENCODE: Best Local IP-Address 192.0.2.141 for Radius-Server 192.0.2.176
00:06:07: RADIUS(00000000): Send Access-Request to 192.0.2.176:1645 id 1645/1, len 50
00:06:07: RADIUS:  authenticator CA DB F4 9B 7B 66 C8 A9 - D1 99 4E 8E A4 46 99 B4
00:06:07: RADIUS:  User-Password       [2]   18  *
00:06:07: RADIUS:  User-Name           [1]   6   "test"
00:06:07: RADIUS:  NAS-IP-Address      [4]   6   192.0.2.141
00:06:07: RADIUS: Received from id 1645/1 192.0.2.176:1645, Access-Reject, len 44
00:06:07: RADIUS:  authenticator 2F 69 84 3E F0 4E F1 62 - AB B8 75 5B 38 82 49 C3
00:06:07: RADIUS:  Reply-Message       [18]  24
00:06:07: RADIUS:   41 75 74 68 65 6E 74 69 63 61 74 69 6F 6E 20 66  [Authentication f]
00:06:07: RADIUS:   61 69 6C 75 72 65                               [failure]
00:06:07: RADIUS(00000000): Received from id 1645/1
00:06:07: RADIUS/DECODE: Reply-Message fragments, 22, total 22 bytes
Router#
```

RADIUS サーバ ロード バランシングの設定例

この項では、次の RADIUS サーバ ロード バランシング機能の設定例について説明します。

- 「グローバル RADIUS サーバ グループ：例」（P.9）
- 「名前付き RADIUS サーバ グループ：例」（P.12）
- 「アイドル タイマー モニタリング：例」（P.14）
- 「認証サーバと認可サーバが同じ優先サーバ：例」（P.15）
- 「認証サーバと認可サーバが別々の優先サーバ：例」（P.15）
- 「認証サーバと認可サーバが重複している優先サーバ：例」（P.16）
- 「認証サーバが認可サーバのサブセットである優先サーバ：例」（P.16）
- 「認証サーバが認可サーバのスーパーセットである優先サーバ：例」（P.16）

グローバル RADIUS サーバ グループ：例

次の例は、グローバル RADIUS サーバ グループに対してロード バランシングを有効にする方法を示しています。この例は、RADIUS コマンド出力の現在の設定、デバッグ出力、および AAA サーバ ステータス情報の 3 つの部分からなります。デリミタを使用して関連する設定部分だけを表示できます。

サーバ設定とグローバル RADIUS サーバ グループに対するロード バランシングの有効化：例

次の例は、関連する RADIUS 設定を示しています。

```
Router# show running-config | include radius

aaa authentication ppp default group radius
aaa accounting network default start-stop group radius
radius-server host 192.0.2.238 auth-port 2095 acct-port 2096 key cisco
radius-server host 192.0.2.238 auth-port 2015 acct-port 2016 key cisco
radius-server load-balance method least-outstanding batch-size 5
```

上記 RADIUS コマンド出力の現行設定内の行は、次のように定義されています。

- **aaa authentication ppp** コマンドは、RADIUS を使用してすべての PPP ユーザを認証します。
- **aaa accounting** コマンドは、クライアント認証後の AAA サーバに対するすべてのアカウンティング要求の送信と、**start-stop** キーワードを使用した切断を有効にします。
- **radius-server host** コマンドは、指定された認可ポートおよびアカウンティング ポートと、特定された認証および暗号キーを使用して、RADIUS サーバ ホストの IP アドレスを定義します。
- **radius-server load-balance** コマンドは、バッチ サイズが指定されたグローバル RADIUS サーバ グループに対してロード バランシングを有効にします。

グローバル RADIUS サーバ グループのデバッグ出力：例

下のデバッグ出力は、上の設定に関する優先サーバの選択と要求の処理を示しています。

```
Router# show debug

General OS:
  AAA server group server selection debugging is on
#
<sending 10 pppoe requests>
Router#
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
```

```
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):Server (192.0.2.238:2015,2016) now
being used as preferred server.
```

グローバル RADIUS サーバ グループのサーバ ステータス情報：例

下の出力は、グローバル RADIUS サーバ グループ設定例の AAA サーバ ステータスを示しています。

```
Router# show aaa server

RADIUS:id 4, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
             Response:unexpected 1, server error 0, incorrect 0, time 1841ms
             Transaction:success 5, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 5, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 3303ms
             Transaction:success 5, failure 0
     Elapsed time since counters last cleared:2m

RADIUS:id 5, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
             Response:unexpected 1, server error 0, incorrect 0, time 1955ms
             Transaction:success 5, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 5, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 3247ms
             Transaction:success 5, failure 0
     Elapsed time since counters last cleared:2m
```

この出力は、2 つの RADIUS サーバのステータスを示しています。いずれもサーバが動作中であり、最後の 2 分間で、次の処理に成功しています。

- 6 つの認証要求のうち 5 つ
- 5 つのアカウンティング要求のうち 5 つ

名前付き RADIUS サーバ グループ：例

次の例は、名前付き RADIUS サーバ グループに対して有効にされたロード バランシングを示しています。この例は、RADIUS コマンド出力の現在の設定、デバッグ出力、および AAA サーバ ステータス情報の 3 つの部分からなります。

サーバ設定と名前付き RADIUS サーバ グループに対するロード バランシングの有効化：例

次の例は、関連する RADIUS 設定を示しています。

```
Router# show running-config
.
.
.
aaa group server radius server-group1
 server 192.0.2.238 auth-port 2095 acct-port 2096
 server 192.0.2.238 auth-port 2015 acct-port 2016
 load-balance method least-outstanding batch-size 5
!
aaa authentication ppp default group server-group1
aaa accounting network default start-stop group server-group1
.
.
.
```

上記 RADIUS コマンド出力の現行設定内の行は、次のように定義されています。

- **aaa group server radius** コマンドは、2 つのメンバー サーバからなるサーバ グループの設定を表示します。
- **load-balance** コマンドは、バッチ サイズが指定されたグローバル RADIUS サーバ グループに対してロード バランシングを有効にします。
- **aaa authentication ppp** コマンドは、RADIUS を使用してすべての PPP ユーザを認証します。
- **aaa accounting** コマンドは、クライアントが認証された時点と **start-stop** キーワードを使用した切断後に、AAA サーバに対するすべてのアカウンティング要求の送信を有効にします。

名前付き RADIUS サーバ グループのデバッグ出力：例

下のデバッグ出力は、上の設定に関する優先サーバの選択と要求の処理を示しています。

```
Router#

*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
```

```
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):Server (192.0.2.238:2015,2016) now
being used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000032):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
.
.
.
```

名前付き RADIUS サーバ グループのサーバ ステータス情報：例

下の出力は、名前付き RADIUS サーバ グループ設定例の AAA サーバ ステータスを示しています。

```
Router# show aaa servers

RADIUS:id 8, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
```

```
     Elapsed time since counters last cleared:0m

RADIUS:id 9, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
```

この出力は、2 つの RADIUS サーバのステータスを示しています。両方のサーバが動作中ですが、カウンタが 0 分前にクリアされて以降は、どの要求も処理されていません。

アイドル タイマー モニタリング：例

次の例は、名前付き RADIUS サーバ グループに対して有効にされたロード バランシングに関するアイドル タイマーと関連するサーバ状態を示しています。この例は、RADIUS コマンド出力の現在の設定とデバッグ出力の 2 つの部分からなります。

サーバ設定とアイドル タイマー モニタリングに対するロード バランシングの有効化：例

次の例は、関連する RADIUS 設定を示しています。

```
Router# show running-config | include radius

aaa group server radius server-group1
radius-server host 192.0.2.238 auth-port 2095 acct-port 2096 test username junk1 idle-time
1 key cisco
radius-server host 192.0.2.238 auth-port 2015 acct-port 2016 test username junk1 idle-time
1 key cisco
radius-server load-balance method least-outstanding batch-size 5
```

上記 RADIUS コマンド出力の現行設定内の行は、次のように定義されています。

- **aaa group server radius** コマンドは、サーバ グループの設定を表示します。
- **radius-server host** コマンドは、指定された認可ポートおよびアカウンティング ポートと、特定された認証および暗号キーを使用して、RADIUS サーバ ホストの IP アドレスを定義します。
- **radius-server load-balance** コマンドは、バッチ サイズが指定されたグローバル RADIUS サーバに対してロード バランシングを有効にします。

アイドル タイマー モニタリングのデバッグ出力：例

下のデバッグ出力は、サーバに送信されるテスト要求を示しています。サーバに送信されたテスト要求に対する応答が受信され、必要に応じて、隔離からサーバが除外され、動作中としてマークされてから、アイドル タイマーがリセットされます。

```
Router#

*Feb 28 13:52:20.835:AAA/SG/TEST:Server (192.0.2.238:2015,2016) quarantined.
*Feb 28 13:52:20.835:AAA/SG/TEST:Sending test request(s) to server (192.0.2.238:2015,2016)
*Feb 28 13:52:20.835:AAA/SG/TEST:Sending 1 Access-Requests, 1 Accounting-Requests in
current batch.
*Feb 28 13:52:20.835:AAA/SG/TEST(Req#:1):Sending test AAA Access-Request.
*Feb 28 13:52:20.835:AAA/SG/TEST(Req#:1):Sending test AAA Accounting-Request.
*Feb 28 13:52:21.087:AAA/SG/TEST:Obtained Test response from server
(192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Obtained Test response from server
(192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Necessary responses received from server
(192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Server (192.0.2.238:2015,2016) marked ALIVE. Idle timer
set for 60 secs(s).
*Feb 28 13:52:22.651:AAA/SG/TEST:Server (192.0.2.238:2015,2016) removed from quarantine.
.
.
.
```

認証サーバと認可サーバが同じ優先サーバ：例

次の例は､サーバの 209.165.200.225 と 209.165.200.226 を共有する認証サーバ グループと認可サーバ グループを示しています。両方のサーバ グループで優先サーバ フラグが有効になっています。

```
aaa group server radius authentication-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2

aaa group server radius accounting-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
```

あるセッションで優先サーバが選択されると、そのセッションのすべてのトランザクションでオリジナルの優先サーバの使用が継続されます。サーバの 209.165.200.225 と 209.165.200.226 は、トランザクションではなく、セッションに基づいて負荷分散されます。

認証サーバと認可サーバが別々の優先サーバ：例

次の例は、サーバの 209.165.200.225 と 209.165.200.226 を使用する認証サーバ グループとサーバの 209.165.201.1 と 209.165.201.2 を使用する認可サーバ グループを示しています。両方のサーバ グループで優先サーバ フラグが有効になっています。

```
aaa group server radius authentication-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2

aaa group server radius accounting-group
   server 209.165.201.1 key radkey3
   server 209.165.201.2 key radkey4
```

認証サーバ グループとアカウンティング サーバ グループはどの共通サーバも共有しません。アカウンティング トランザクション用の優先サーバが見つかることはないため、認証サーバと認可サーバがトランザクションに基づいて負荷分散されます。1 つのセッションで開始レコードと終了レコードが同じサーバに送信されます。

認証サーバと認可サーバが重複している優先サーバ：例

次の例は、サーバの 209.165.200.225、209.165.200.226、および 209.165.201.1 を使用する認証サーバ グループとサーバの 209.165.201.1 と 209.165.201.2 を使用する認可サーバ グループを示しています。両方のサーバ グループで優先サーバ フラグが有効になっています。

```
aaa group server radius authentication-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
   server 209.165.201.1 key radkey3

aaa group server radius accounting-group
   server 209.165.201.1 key radkey3
   server 209.165.201.2 key radkey4
```

すべてのサーバのトランザクション処理機能が同じ場合は、すべての認証トランザクションの 1/3 がサーバの 209.165.201.1 に転送されます。そのため、すべてのアカウンティング トランザクションの 1/3 もサーバの 209.165.201.1 に転送されます。残りの 2/3 のアカウンティング トランザクションは、サーバの 209.165.201.1 と 209.165.201.2 の間で均等に負荷分散されます。サーバの 209.165.201.1 は、サーバの 209.165.201.1 で未処理アカウンティング トランザクションが発生すると、受信する認証トランザクションが減ります。

認証サーバが認可サーバのサブセットである優先サーバ：例

次の例は、サーバの 209.165.200.225 と 209.165.200.226 を使用する認証サーバ グループと、サーバの 209.165.200.225、209.165.200.226、および 209.165.201.1 を使用する認可サーバ グループを示しています。両方のサーバ グループで優先サーバ フラグが有効になっています。

```
aaa group server radius authentication-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2

aaa group server radius accounting-group
  server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
   server 209.165.201.1 key radkey3
```

すべての認証トランザクションの半分がサーバの 209.165.200.225 に送信され、残りの半分がサーバの 209.165.200.226 に送信されます。サーバの 209.165.200.225 と 209.165.200.226 は、認証および認可用の優先サーバになるため、サーバの 209.165.200.225 と 209.165.200.226 の間で認証トランザクションとアカウンティング トランザクションが均等に分散されます。サーバの 209.165.201.1 はあまり使用されません。

認証サーバが認可サーバのスーパーセットである優先サーバ：例

次の例は、サーバの 209.165.200.225、209.165.200.226、および 209.165.201.1 を使用する認証サーバ グループとサーバの 209.165.200.225 と 209.165.200.226 を使用する認可サーバ グループを示しています。両方のサーバ グループで優先サーバ フラグが有効になっています。

```
aaa group server radius authentication-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
   server 209.165.201.1 key radkey3

aaa group server radius accounting-group
```

```
server 209.165.200.225 key radkey1
 server 209.165.200.226 key radkey2
```

最初に、1/3 の認証トランザクションが認可サーバ グループ内の各サーバに割り当てられます。アカウンティング トランザクションはセッションごとに生成されますが、優先サーバ フラグがオンになっているサーバの 209.165.200.225 と 209.165.200.226 にしか送信されません。サーバの 209.165.200.225 と 209.165.200.226 がトランザクションの処理を開始しますが、認証トランザクションはサーバの 209.165.201.1 に送信されます。サーバの 209.165.201.1 で認証されたトランザクション要求は、どの優先サーバ設定も含まず、サーバの 209.165.200.225 と 209.165.200.226 に分配されるため、優先サーバ フラグの使用が無効になります。この設定は慎重に使用する必要があります。

その他の参考資料

ここでは、RADIUS サーバ ロード バランシング機能に関する関連資料について説明します。

関連資料

内容	参照先
AAA および RADIUS	『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 12.4T』
AAA サーバ グループと RADIUS 設定	「Configuring RADIUS」モジュール
フェールオーバー再試行順序変更モード	「RADIUS Server Reorder on Failure」モジュール

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によってサポートされる新しい RFC や変更された RFC はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

RADIUS サーバ ロード バランシングの機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　RADIUS サーバ ロード バランシングの機能情報

機能名	リリース	機能情報
RADIUS サーバ ロード バランシング	12.2(28)SB 12.4(11)T 12.2(33)SRC	RADIUS サーバ ロード バランシング機能は、Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）の認証トランザクションとアカウンティング トランザクションをサーバ グループ内のサーバに分配します。これらのサーバは、トランザクションの負荷を分担し、空いているサーバを効率的に使用して着信要求に対するより迅速な応答を実現します。 この機能は、Cisco IOS Release 12.2(28)SB に統合されました。 この機能は、Cisco IOS Release 12.4(11)T に統合されました。 この機能は、Cisco IOS Release 12.2(33)SRC に統合されました。 **debug aaa sg-server selection**、**debug aaa test**、**load-balance (server-group)**、**radius-server host**、**radius-server load-balance**、および **test aaa group** の各コマンドが導入または変更されました。
RADIUS サーバ ロード バランシング ポーティング	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータで導入されました。

56 ビット アカウンティング セッション ID の RADIUS サポート

56 ビット アカウンティング セッション ID の RADIUS サポート機能は、新しい 32 ビット Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）変数の acct-session-id-count を導入しています。acct-session-id-count 変数の最初の 8 ビットは、リロード間で保存されるアカウンティング セッションに割り当てられた一意の番号である一意識別子変数として予約されています。acct-session-id-count 変数は、既存の 32 ビット acct-session-id 変数の RADIUS アトリビュート 44 に加えて使用されます。これによって、全部で 56 ビットで実際のアカウンティング セッション ID が表されます。この機能のメリットを次に示します。

- 8 ビットの一意識別子変数で、リロードが発生した場合のアカウンティング セッション ID を識別できます。
- acct-session-id-count 変数によって提供される追加のスペースによって、音声電話通話などの大容量トラフィックが発生した場合の acct-session-id ラッピングを追跡できます。acct-session-id 変数がラップするごとにインクリメントすることによって、acct-session-id-count 変数にアカウンティング情報が保存されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「56 ビット アカウンティング セッション ID の RADIUS サポートの機能情報」（P.6）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

56 ビット アカウンティング セッション ID の RADIUS サポートの前提条件

AAA アカウンティングを設定する必要があります。AAA アカウンティングの設定方法については、『*Cisco IOS Security Configuration Guide*』の「Configuring Accounting」を参照してください。

56 ビット アカウンティング セッション ID の RADIUS サポートに関する情報

56 ビット アカウンティング セッション ID の RADIUS サポート機能を設定するには、次の概念を理解しておく必要があります。

- 「Acct-Session-Id アトリビュート」（P.2）
- 「Acct-Session-Id-Count アトリビュート」（P.2）

Acct-Session-Id アトリビュート

RADIUS アトリビュート 44 のアカウンティング セッション ID は、ログ ファイル内の開始レコードと終了レコードの照合を容易にする一意のアカウンティング識別子です。アカウンティング セッション ID 番号は、ルータの電源を入れ直すか、ソフトウェアをリロードするたびに 1 にリセットされます。RADIUS アトリビュート 44 は、AAA アカウンティングの設定時に自動的に有効になります。

acct-session-id 変数は、00000000 ～ FFFFFFFF の値を取ることが可能な 32 ビット変数です。

Acct-Session-Id-Count アトリビュート

新しい acct-session-id-count 変数は 32 ビット変数です。この変数の最初の 8 ビットは、リロードが発生した場合に RADIUS サーバでアカウンティング セッションを特定可能にする一意識別子変数として予約されています。acct-session-id-count 変数の残りの 24 ビットはカウンタ変数として機能します。最初の acct-session-id 変数が割り当てられたときに、このカウンタ変数が 1 に設定されます。この変数は、acct-session-id 変数がラップするたびに 1 ずつインクリメントされ、アカウンティング情報の欠落を防止します。

acct-session-id-count 変数は ##000000 ～ ##FFFFFF の値を取ることができます。ここで、## は一意識別子変数として予約されている 8 ビットを表します。

acct-session-id-count 変数と acct-session-id 変数は、RADIUS サーバに送信される前に連結され、次のような acct-session 変数を表します。

##000000 00000000 ～ ##FFFFFF FFFFFFFF

これによって、全部で 56 ビットを acct-session-id 空間として使用できるようになります。

56 ビット アカウンティング セッション ID の RADIUS サポートの設定方法

ここでは、次の手順について説明します。

- 「56 ビット アカウンティング セッション ID の RADIUS サポートの設定」（P.3）

56 ビット アカウンティング セッション ID の RADIUS サポートの設定

このタスクでは、一意識別子変数を含む acct-session-id-count 変数を有効にします。

手順の概要

1. **enable**
2. **radius-server unique-ident** *id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**radius-server unique-ident** *id* 例： Router(config)# radius-server unique-ident 5	一意識別子変数を含む acct-session-id-count 変数を有効にします。 • *id* 引数は、acct-session-id-count 変数の先頭の 8 ビットで表わされる一意の識別子を指定します。有効な値の範囲は、0 ～ 255 です。

56 ビット アカウンティング セッション ID の RADIUS サポートの設定例

ここでは、次の設定例を示します。

- 「56 ビット アカウンティング セッション ID の RADIUS サポートの設定：例」（P.4）

56 ビット アカウンティング セッション ID の RADIUS サポートの設定：例

次の例では、AAA 認証を設定して、アクセス要求パケット内の RADIUS アトリビュート 44 を有効にし、acct-session-id-count 変数を有効にして、一意識別子変数を 5 に設定します。

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server unique-ident 5
```

その他の参考資料

次の項で、56 ビット アカウンティング セッション ID の RADIUS サポート機能に関する参考資料を紹介します。

関連資料

内容	参照先
RADIUS の設定	「Configuring RADIUS」フィーチャ モジュールを参照してください。
アカウンティングの設定	「Configuring Accounting」フィーチャ モジュールを参照してください。
AAA RADIUS アトリビュート	「RADIUS Attributes Overview and RADIUS IETF Attributes」フィーチャ モジュールを参照してください。
RADIUS コマンド	『*Cisco IOS Security Command Reference*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2139	「RADIUS Accounting」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

56 ビット アカウンティング セッション ID の RADIUS サポートの機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　56 ビット アカウンティング セッション ID の RADIUS サポートの機能情報

機能名	リリース	機能情報
56 ビット アカウンティング セッション ID の RADIUS サポート	12.3(2)T	56 ビット アカウンティング セッション ID の RADIUS サポート機能は、新しい 32 ビット Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）変数の acct-session-id-count を導入しています。 この機能は、Cisco IOS Release 12.3(2)T で導入されました。 **radius-server unique-iden** コマンドが導入または変更されました。

ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス

ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能は、シスコ独自の Vendor Specific Attribute（VSA; ベンダー固有アトリビュート）を使用せずに、業界標準のロード バランシング機能とフェールオーバー機能を Layer 2 Tunnel Protocol Network Server（LNS; レイヤ 2 トンネル プロトコル ネットワーク サーバ）に提供します。この機能は、RFC 2868 で規定されているマルチベンダー ネットワーク環境に使用すべきトンネル アトリビュートに適合しているため、複数のベンダーで製造された Network Access Servers（NAS; ネットワーク アクセス サーバ）間の相互運用性の問題を解決します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンスの機能情報」（P.7）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

前提条件

VPDN と HGW グループの設定はこのマニュアルの範囲を超えています。詳細については、「関連資料」（P.5）を参照してください。

制約事項

次の制約と制限がロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能に適用されます。

- この機能は、VPDN ダイヤルアウト ネットワークをサポートしていません。ダイヤルイン アプリケーション専用に設計されています。
- ネットワーク上で許容される LNS の最大数は、タグ アトリビュート グループ当たり 50 ずつの合計 1550 で、タグは 31 までに制限されています。
- この機能には、RFC 2868 をサポートする RADIUS サーバ実装が必要です。

ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンスに関する情報

ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能は、ロード バランシングおよびフェールオーバー Virtual Private Dialup Network（VPDN; バーチャル プライベート ダイヤルアップ ネットワーク）Home Gateway（HGW; ホーム ゲートウェイ）グループを標準化された方法で提供します。この機能は、新しいソフトウェア機能を導入しています。この機能に関連付けられた新しいコマンドはありません。

独自のアトリビュートではなく、業界標準のアトリビュート

Cisco IOS Release 12.2(4)T までは、LNS のロード バランシングおよびフェールオーバー機能が、シスコ独自の VSA によって提供されていました。マルチベンダー ネットワーク環境で、RADIUS 上の VSA を使用した場合は、複数のベンダーによって製造された NAS 間で相互運用性の問題が発生する可能性があります。特定の RADIUS サーバ実装が要求元の NAS で解読可能な VSA を送信可能な場合でも、ユーザが同じ目的で複数の VSA をシングル サービス プロファイルに保存しておく必要があります。

マルチベンダー ネットワーク環境で使用すべきトンネル アトリビュートに関する合意は RFC 2868 で規定されています。RFC 2868 では、Tunnel-Server-Endpoint と Tunnel-Medium-Type を組み合わせて、NAS が新しいセッションを開始すべきアドレスが指定されます。複数の Tunnel-Server-Endpoint アトリビュートが 1 つのタグ付きアトリビュート グループ内で定義されている場合は、equal-cost load-balancing HGW として解釈されます。

RFC 2868 で規定されている Tunnel-Preference アトリビュートは、ロード バランシングおよびフェールオーバー HGW グループを形成する手段として使用できます。複数のタグ付きアトリビュート グループの Tunnel-Preference 値が同じ場合は、他に指定されていなければ、それらのアトリビュート グループの Tunnel-Server-Endpoint が同じ優先順位に設定されていると見なされます。一部のアトリビュート グループの Tunnel-Preference 値が他のアトリビュート グループよりも高い（プリファレンスが低い）場合は、それらの Tunnel-Server-Endpoint アトリビュートの優先順位が上になります。あるアトリビュート グループの優先順位値が高い場合は、それより優先順位値が低いアトリビュート グループが接続に使用できない場合に、そのアトリビュート グループがフェールオーバーに使用されます。

Cisco IOS Release 12.2(4)T までは、特別に書式設定された文字列がシスコ VSA の「vpdn:ip-addresses」文字列内で NAS に転送され、HGW のロード バランシングおよびフェールオーバーに使用されていました。たとえば、10.0.0.1 10.0.0.2 10.0.0.3/2.0.0.1 2.0.0.2 は、ロード バランシング用の最初のグループに関する IP アドレスの 10.0.0.1、10.0.0.2、および 10.0.0.3 として解釈されます。新しいセッションは、least-load-first アルゴリズムに基づいて、この 3 つのアドレスに送出されます。このアルゴリズムは、ローカルな知識を利用して、新しいセッションを開始する負荷が最低の HGW を選択します。この例では、2 番めのグループ内のアドレスの 2.0.0.1 と 2.0.0.2 が、優先順位が低く、最初のグループ内で指定されたすべての HGW が新しい接続要求に対する応答に失敗した場合にのみ適用可能になります。そのため、2.0.0.1 と 2.0.0.2 がフェールオーバー アドレスになります。RADIUS トンネル プロファイル内でのこのようなフェールオーバー アドレスの設定方法の例については、「ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンスの設定例」（P.5）を参照してください。

マルチベンダー ネットワークにおけるロード バランシングとフェールオーバー

ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能は、図 1 に示す設定のように、ATM やイーサネットなどの WAN リンク上の VPDN レイヤ 2 トンネルを使用する大規模マルチベンダー ネットワーク用に設計されています。

図 1　マルチベンダー ネットワークにおける代表的なロード バランシングとフェールオーバー

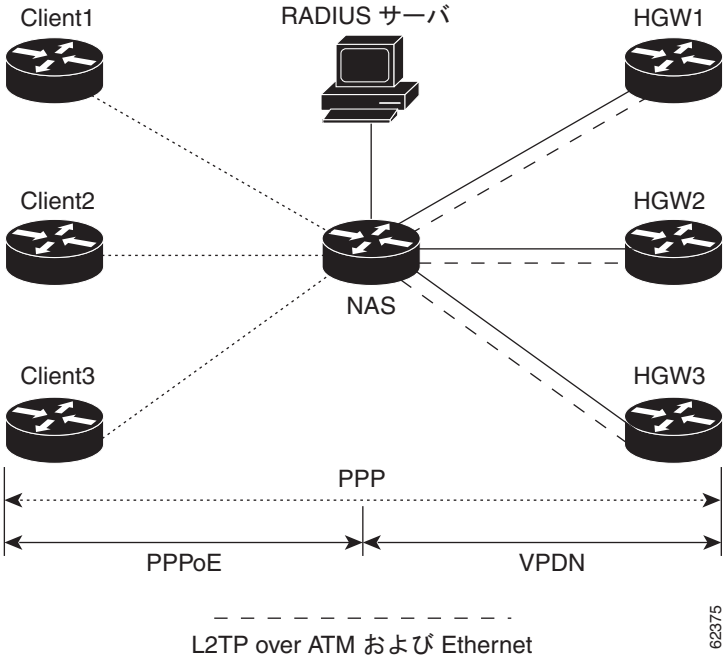


図 1 に示す設定では、NAS が RADIUS サーバからダウンロードされたトンネル プロファイルを使用して、ロード バランシングおよびフェールオーバー用の VPDN レイヤ 2 トンネルを構築します。Point-to-Point over Ethernet（PPPoE）プロトコルが、PPP セッションを生成するクライアントとして使用されます。

関連機能およびテクノロジー

ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能は VPDN で使用されます。加えて、次のテクノロジーとプロトコルに精通していることが求められます。

- ATM
- イーサネット
- L2TP と L2F
- PPP と PPPoE
- RADIUS サーバ

ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンスの設定方法

この機能には新しいコンフィギュレーション コマンドがありません。ただし、ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能の RADIUS トンネル プロファイル内での実装方法については、次の項を参照してください。

ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンスの設定例

次の例は、RADIUS トンネル プロファイルの作成方法を示しています。

```
net3 Password = "cisco" Service-Type = Outbound
        Tunnel-Type = :0:L2TP,
        Tunnel-Medium-Type = :0:IP,
        Tunnel-Server-Endpoint = :0:"1.1.3.1",
        Tunnel-Assignment-Id = :0:"1",
        Tunnel-Preference = :0:1,
        Tunnel-Password = :0:"welcome"

        Tunnel-Type = :1:L2TP,
        Tunnel-Medium-Type = :1:IP,
        Tunnel-Server-Endpoint = :1:"1.1.5.1",
        Tunnel-Assignment-Id = :1:"1",
        Tunnel-Preference = :1:1,
        Tunnel-Password = :1:"welcome"

        Tunnel-Type = :2:L2TP,
        Tunnel-Medium-Type = :2:IP,
        Tunnel-Server-Endpoint = :2:"1.1.4.1",
        Tunnel-Assignment-Id = :2:"1",
        Tunnel-Preference = :2:1,
        Tunnel-Password = :2:"welcome"

        Tunnel-Type = :3:L2TP,
        Tunnel-Medium-Type = :3:IP,
        Tunnel-Server-Endpoint = :3:"1.1.6.1",
        Tunnel-Assignment-Id = :3:"1",
        Tunnel-Preference = :3:1,
        Tunnel-Password = :3:"welcome"
```

これらのプロファイル内でフェールオーバー アドレスがどのように選択されるかの詳細については、「ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンスに関する情報」（P.2）を参照してください。RADIUS トンネル プロファイルの作成に使用するマニュアルについては、「関連資料」（P.5）を参照してください。

その他の参考資料

次の項で、ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能に関する参考資料を紹介します。

関連資料

内容	参照先
RADIUS	「Configuring RADIUS」モジュール
RADIUS アトリビュート	「RADIUS Attributes Overview and RADIUS IETF Attributes」モジュール
バーチャル プライベート ダイヤルアップ ネットワーク（VPDN）のロードマップ	『*Cisco IOS VPDN Configuration Guide*, Release 15.0』

内容	参照先
ダイヤル テクノロジー	『*Cisco IOS Dial Technologies Configuration Guide*, Release 12.4T』
ブロードバンド アクセス：PPP とルーテッド ブリッジ エンカプセレーション	『*Cisco IOS Broadband Access Aggregation and DSL Configuration Guide*, Release 12.4T』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2868	「*RADIUS Attributes for Tunnel Protocol Support*」

ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンスの機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンスの機能情報

機能名	リリース	機能情報
ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス	12.2(4)T	ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能は、シスコ独自の Vendor Specific Attribute（VSA; ベンダー固有アトリビュート）を使用せずに、業界標準のロード バランシング機能とフェールオーバー機能を Layer 2 Tunnel Protocol Network Server（LNS; レイヤ 2 トンネル プロトコル ネットワーク サーバ）に提供します。この機能は、RFC 2868 で規定されているマルチベンダー ネットワーク環境に使用すべきトンネル アトリビュートに適合しているため、複数のベンダーで製造された Network Access Servers（NAS; ネットワーク アクセス サーバ）間の相互運用性の問題を解決します。 この機能は、Cisco IOS Release 12.2(4)T で導入されました。

用語集

HGW：Home GateWay（ホーム ゲートウェイ）。L2TP などのレイヤ 2 トンネリング プロトコルを終端するゲートウェイ。

L2TP：Layer 2 Tunnel Protocol（レイヤ 2 トンネル プロトコル）。PPP のトンネリングを提供する RFC 2661 で規定されたインターネット技術特別調査委員会（IETF）標準トラック プロトコル。L2F と PPTP の最良の機能に基づいて、L2TP が、VPDN を実装するための業界全体で相互運用可能な方式を提供します。

L2TP ネットワーク サーバ：LNS を参照してください。

LNS：L2TP Network Server（L2TP ネットワーク サーバ）。L2TP トンネル エンドポイントの一方の側として機能し、NAS または L2TP アクセス コンセントレータ（LAC）に対するピアであるノード。LNS は、アクセス サーバによってリモート システムからトンネル化されている PPP セッションの論理的終端点です。レイヤ 2 フォワーディング（L2F）HGW に似ています。

NAS：Network Access Server（NAS; ネットワーク アクセス サーバ）パケットの世界（インターネットなど）と回線の世界（公衆電話交換網など）をインターフェイスするシスコ プラットフォームまたはプラットフォームの集合。

Request for Comments：RFC を参照してください。

RFC：Request for Comments。インターネット技術特別調査委員会（IETF）によって収集されたインターネットに関する各種規約。1969 年に発足した IETF は、インターネット アーキテクチャの発展に携わっているネットワーク設計者、運営業者、ベンダー、および研究者の大規模でオープンな国際的コミュニティです。RFC は、ネットワーキング プロトコル、手続き、プログラム、および概念に焦点を当てた、コンピュータ通信のさまざまな側面を規定しています。

VPDN：Virtual Private Dialup Network（バーチャル プライベート ダイヤルアップ ネットワーク）。ネットワーク間のトラフィックをすべて暗号化することにより、パブリック TCP/IP ネットワーク経由でも IP トラフィックをセキュアに転送できます。

ネットワーク アクセス サーバ：NAS を参照してください。

バーチャル プライベート ダイヤルアップ ネットワーク：VPDN を参照してください。

ホーム ゲートウェイ：HGW を参照

レイヤ 2 トンネル プロトコル：L2TP を参照してください。

RADIUS サーバ障害発生時順序変更

RADIUS サーバ障害発生時順序変更機能は、高負荷期間またはサーバで障害が発生した場合に、サーバ グループ内の別のサーバへのフェールオーバーを提供します。障害発生後は、すべての RADIUS トラフィックが新しいサーバに転送されます。新しいサーバからサーバ グループ内の別のサーバにトラフィックが切り替えられるのは、新しいサーバでも障害が発生した場合に限られます。トラフィックが自動的に最初にサーバに戻されることはありません。

RADIUS トランザクションを複数のサーバに分散させることによって、認証要求とアカウンティング要求がより迅速に処理されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「RADIUS サーバ障害発生時順序変更の機能情報」（P.12）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

RADIUS サーバ障害発生時順序変更の前提条件

- 障害発生時に順序変更を実行するように RADIUS サーバを設定する前に、**aaa new-model** コマンドを使用して、Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）を有効にする必要があります。
- 認証、アカウンティング、静的ルート ダウンロードなどの機能用に RADIUS を設定する必要もあります。

RADIUS サーバ障害発生時順序変更の制約事項

- サーバ グループごとに新しい 4 バイトのメモリが消費されます。ただし、ほとんどのサーバは少数のサーバ グループのみに設定されているため、追加の 4 バイトはそれほど性能に影響しない可能性があります。
- Cisco IOS ソフトウェア セット内の RADIUS 機能によっては、この機能を使用できない場合があります。RADIUS 機能で RADIUS サーバ障害発生時順序変更機能を使用できない場合は、順序変更機能が設定されていないかのようにサーバが動作します。

RADIUS サーバ障害発生時順序変更に関する情報

RADIUS サーバ障害発生時順序変更機能を設定するには、次の概念を理解しておく必要があります。

- 「RADIUS サーバの障害」（P.2）
- 「RADIUS サーバ障害発生時順序変更機能の動作方法」（P.3）

RADIUS サーバの障害

RADIUS サーバ障害発生時順序変更機能が設定されていない状態でサーバの障害が発生した場合：

1. 新しい RADIUS トランザクションを実行する必要があります。
2. トランザクション用の RADIUS パケットが、グループ内で停止中としてマークされていない（設定されたデッドタイムに従って）最初のサーバに送信され、設定された再送回数だけ再送されます。
3. 再送のすべてがタイムアウトした（設定されたタイムアウトに従って）場合は、ルータがそのパケットをリストで次の非停止中サーバに設定された再送回数だけ送信します。
4. ステップ 3 は、トランザクションごとに指定された最大送信回数に達するまで繰り返されます。最大送信回数に到達する前にリストの最後に到達した場合は、ルータがリストの先頭に戻ってそこから処理を継続します。

このプロセスのどの時点でも、サーバが停止中サーバ検出基準（設定不可、使用されている Cisco IOS ソフトウェアによって異なる）を満たした場合は、設定されたデッドタイムに合わせてサーバが停止中としてマークされます。

RADIUS サーバ障害発生時順序変更機能の動作方法

RADIUS サーバ障害発生時順序変更機能を設定した場合は、次のように、初期サーバとして使用する RADIUS サーバが決定されます。

- Network Access Server（NAS; ネットワーク アクセス サーバ）が、トランスミッションが送信される最初のサーバである「フラグ設定された」サーバのステータスを保持します。
- フラグ設定されたサーバにトランスミッションが送信された後は、設定された再送回数だけ、フラグ設置されたサーバにトラフィックが再送されます。
- その後は、NAS が、フラグ設定されたサーバの次にリストされたサーバから始めて、設定されたトランザクションの最大再試行回数に到達するか、応答が返されるまで、サーバ グループ内の非停止中サーバのリストの順にトランスミッションを送信します。
- 起動時は、**radius-server host** コマンドを使用して設定されたように、フラグ設定されたサーバがサーバ グループ リストで最初のサーバになります。
- フラグ設定されたサーバが停止中としてマークされている場合は（デッドタイムが 0 の場合でも）、フラグ設定されたサーバの次にリストされた最初の非停止中サーバがフラグ設定されたサーバになります。
- フラグ設定されたサーバが、リスト内の最後のサーバで、停止中としてマークされている場合は、フラグ設定されたサーバがリスト内で停止中としてマークされていない最初のサーバになります。
- すべてのサーバが停止中としてマークされている場合は、トランザクションが失敗して、フラグ設定されたサーバへの変更が実施されません。
- フラグ設定されたサーバが停止中としてマークされており、デッド タイマーが切れた場合は、何も行われません。

（注） トランスミッションのタイプ（Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）、Microsoft CHAP（MS-CHAP）、Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル））によっては、1 つのサーバを何度も往復しなければならない場合があります。このような特殊なトランザクションの場合は、サーバへの往復シーケンス全体が 1 回のトランスミッションのように処理されます。

RADIUS サーバが停止中の場合

次の 1 と 2 の基準が満たされた場合に、サーバを停止中としてマークすることができます。

1. **radius-server transaction max-tries** コマンドで指定された再送回数を超えてサーバが応答しなかった場合。
2. 設定されたタイムアウトまでどの要求にもサーバが応答しなかった場合。両方の基準（これと上の基準）が満たされた場合にのみ、サーバが停止中としてマークされます。デッドタイムが 0 の場合でも、サーバを停止中としてマークすると、RADIUS サーバの再試行方式順序変更システムに重大な影響を及ぼします。

RADIUS サーバ障害発生時順序変更の設定方法

ここでは、次の各手順について説明します。

- 「RADIUS サーバ障害発生時順序変更の設定」（P.4）（必須）
- 「RADIUS サーバ障害発生時順序変更のモニタリング」（P.5）（任意）

RADIUS サーバ障害発生時順序変更の設定

このタスクを実行して、サーバ グループ内のあるサーバを、最初のサーバで障害が発生した場合に別のサーバにトラフィックを転送するように設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server retry method reorder**
5. **radius-server retransmit** {*retries*}
6. **radius-server transaction max-tries** {*number*}
7. **radius-server host** {*hostname* | *ip-address*} [*key string*]
8. **radius-server host** {*hostname* | *ip-address*} [*key string*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Router (config)# aaa new-model`	AAA アクセス コントロール モデルをイネーブルにします。
ステップ 4	**radius-server retry method reorder** 例： `Router (config)# radius-server retry method reorder`	サーバ グループ内の RADIUS トラフィック エントリの順序変更を指定します。
ステップ 5	**radius-server retransmit** {*retries*} 例： `Router (config)# radius-server retransmit 1`	Cisco IOS ソフトウェアが RADIUS サーバ ホストのリストを検索する回数の最大値を指定します。 *retries* 引数は、再送試行の最大回数です。デフォルトは 3 回です。

	コマンドまたはアクション	目的
ステップ 6	**radius-server transaction max-tries** {*number*} 例： `Router (config)# radius-server transaction max-tries 3`	RADIUS サーバ上で試行可能なトランザクション当たりのトランスミッション数の最大値を指定します。 *number* 引数は、トランザクション当たりのトランスミッション数の総数です。このコマンドが設定されなかった場合のデフォルトは 8 トランスミッションです。 （注） このコマンドは、特定のトランザクションに関係するすべての RADIUS サーバに適用されます。
ステップ 7	**radius-server host** {*hostname* | *ip-address*} [**key** *string*] 例： `Router (config)# radius-server host 10.2.3.4 key radi23`	RADIUS サーバ ホストを指定します。 （注） **radius-server key** コマンドを発行することによって、サーバ単位キーが設定されていないすべての RADIUS サーバのグローバル キーを設定することもできます。
ステップ 8	**radius-server host** {*hostname* | *ip-address*} [**key** *string*] 例： `Router (config)# radius-server host 10.5.6.7 key rad234`	RADIUS サーバ ホストを指定します。 （注） 少なくとも 2 つのサーバを設定する必要があります。

RADIUS サーバ障害発生時順序変更のモニタリング

ルータ上でサーバ障害発生時順序変更プロセスをモニタするには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **debug aaa sg-server selection**
3. **debug radius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**debug aaa sg-server selection** 例： `Router# debug aaa sg-server selection`	ルータ内の RADIUS および TACACS+ サーバ グループ システムが特定のサーバを選択している理由に関する情報を表示します。
ステップ 3	**debug radius** 例： `Router# debug radius`	ルータが特定の RADIUS サーバを選択している理由に関する情報を表示します。

例

次の 2 つのデバッグ出力は、RADIUS サーバ障害発生時順序変更機能の動作を示しています。

デバッグ 1

次のサンプル出力では、RADIUS サーバ障害発生時順序変更機能が設定されています。サーバの再送は 0（したがって、次に設定されたサーバへのフェールオーバー前に、各サーバが一度だけ試行される）に設定され、トランザクション当たりのトランスミッション数は 4（3 回めのフェールオーバーでトランスミッション終了）に設定されています。サーバ グループ内で 3 番めのサーバ（10.107.164.118）が、3 回めのトランスミッション（2 回めのフェールオーバー）のトランザクションを受け入れています。

```
00:38:35: %SYS-5-CONFIG-I: Configured from console by console
00:38:53: RADIUS/ENCODE(OOOOOOOF) : ask "Username: "
00:38:53: RADIUS/ENCODE (0000000F) : send packet; GET-USER
00:38:58: RADIUS/ENCODE (0000000F) : ask "Password: "
00:38:58: RADIUS/ENCODE(0000000F) : send packet; GET-PASSWORD
00:38:59: RADIUS: AAA Unsupported [152] 4
00:38:59: RADIUS: 7474 [tt]
00:38:59: RADIUS (0000000F) : Storing nasport 2 in rad-db
00:38:59: RADIUS/ENCODE(0000000F) : dropping service type, "radius-server attribute 6
on-for-login-auth" is off
00:38:59: RADIUS (0000000F) : Config NAS IP: 0.0.0.0
00:38:59: RADIUS/ENCODE (0000000F) : acct-session-id: 15
00:38:59: RADIUS (0000000F) : sending
00:38:59: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 192.1.1.1
00:38:59: RAPIUS(0000000F) : Send Access-Request to 10.10.10.10:1645 id 21645/11, len 78
00:38:59: RADIUS:: authenticator 4481 E6 65 2D 5F 6F OA -lE F5 81 8F 4E 1478 9C
00:38:59: RADIUS: User-Name [1] 7 "username1"
00:38:59: RADIUS: User-Password [2] 18 *
00:38:59: RADIUS: NAS-Port fSl 6 2
00:~8:59: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
00:38:59: RADIUS: Calling-Station-Id [31] 15 "10.19.192.23"
00:39:00: RADIUS: NAS-IP-Address [4] 6 10.0.1.130
00:39:02: RADIUS: Fail-over to (10.2.2.2:1645,1646) for id 21645/11
00:39:02: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 192.2.2.2
00:39:04: RADIUS: Fail-over to (10.107.164.118:1645,1646) for id 21645/11
00:39:04: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server
128.107.164.118
00:39:05: RADIUS: Received from id 21645/11 10.107.164.118:1645, Access-Accept, len 26
00:39:05: RADIUS: authenticator 5609 56 F9 64 4E DF 19- F3 A2 DD 73 EE 3F 9826
00:39:05: RADIUS: Service-Type [6] 6 Login [1]
```

デバッグ 2

次のサンプル出力では、RADIUS サーバ障害発生時順序変更機能が設定されています。サーバの再送は 0 に設定され、トランザクション当たりのトランスミッション数は 8 に設定されています。このトランザクションでは、サーバ 10.10.10.0 へのトランスミッションが 8 回めで失敗します。

```
00:42:30: RADIUS(00000011): Received from id 21645/13
00:43:34: RADIUS/ENCODE(00000012) : ask "Username: "
00:43:34: RADIUS/ENCODE(00000012) : send packet; GET-USER
00:43:39: RADIUS/ENCODE(00000012) : ask "Password: "
00:43:39: RADIUS/ENCODE(00000012) : send packet; GET-PASSWORD
00:43:40: RADIUS: AAA Unsupported [152] 4
00:43:40: RADIUS: 7474 [tt]
00:43:40: RADIUS(00000012) : Storing nasport 2 in rad-db
00:43:40: RADIUS/ENCODE(00000012): dropping service type, "radius-server attribute 6
on-for-login-auth" is off
00:43:40: RADIUS(00000012) : Co~fig NAS IP: 0.0.0.0
00:43:40: RADIUS/ENCODE(00000012) : acct-session-id: 18
```

```
00:43:40: RADIUS(00000012) : sending
00:43:40: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.107.164.118
00:43:40: RADIUS(00000012) : Send Access-Request to 10.107.164.118:1645 id 21645/14, len
78 00:43:40: RADIUS: authenticator B8 OA 51 3A AF A6 0018 -B3 2E 94 5E 07 OB 2A IF
00:43:40: RADIUS: User-Name [1] 7 "username1" 00:43:40: RADIUS: User-Password [2] 18 *
00:43:40: RADIUS: NAS-Port [5] 6 2
00:43:40: RADIUS: NAS-Port-Type [61] 6 Virtual [5] 00:43:40: RADIUS: Calling-Station-]d
[31] 15 "172.19.192.23" 00:43:40: RADIUS: NAS-IP-Address [4] 6 10.0.1.130
00:43:42: RADIUS: Fail-over to (10.10.10.10:1645,1646) for id 21645/14
00:43:42: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.1.1.1
00:43:44: RADius: Fail-over to (10.2.2.2:1645,1646) for id 21645/14
00:43:44: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.2.2.2
00:43:46: RADIUS: Fail-over to (10.107.164.118:1645,1646) for id 21645/14
00:43:46: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.107.164.118
00:43:48: RADIUS: Fail-over to (10.10.10.10:1645,1646) for id 21645/14
00:43:48: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.1.1.1
00:43:50: RADIUS: Fail-over to (10.2.2.2:1645,1646) for id 21645/14
00:43:50: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.2.2.2
00:43:52: RADIUS: Fail-over to (10.107.164.118:1645,1646) for id 21645/14
00:43:52: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.107.164.118
00:43:54: RADIUS: Fail-over to (10.10.10.10:1645,1646) for id 21645/14
00:43:54: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.1.1.1
00:43:56: RADIUS: No response from (10.10.10.10:1645,1646) for id 21645/14 00:43:56:
RADIUS/DECODE: parse response no app start; FAIL 00:43:56: RADIUS/DECODE: parse response;
FAIL
```

RADIUS サーバ障害発生時順序変更の設定例

ここでは、次の設定例について説明します。

- 「RADIUS サーバ障害発生時順序変更の設定例」（P.7）
- 「RADIUS サーバが停止中の送信順序の決定」（P.7）

RADIUS サーバ障害発生時順序変更の設定例

次の設定例は、RADIUS サーバが障害発生時に順序変更されるように設定されます。RADIUS サーバ上で試行可能なトランザクション当たりのトランスミッション数の最大値は 6 です。

```
aaa new-model
radius-server retry method reorder
radius-server retransmit 0
radius-server transaction max-tries 6
radius-server host 10.2.3.4 key rad123
radius-server host 10.5.6.7 key rad123
```

RADIUS サーバが停止中の送信順序の決定

起動時に次のように設定し、

```
aaa new-model
radius-server retry method reorder
radius-server retransmit 0
radius-server transaction max-tries 6
radius-server host 10.2.3.4
radius-server host 10.5.6.7
```

両方のサーバがダウンしているが、まだ、停止中としてマークされていない場合は、最初のトランザクションで、次のようなトランスミッションが見られます。

```
10.2.3.4
10.5.6.7
10.2.3.4
10.5.6.7
10.2.3.4
10.5.6.7
```

順序変更を次のように設定し、

```
aaa new-model
radius-server retry method reorder
radius-server retransmit 1
radius-server transaction max-tries 3
radius-server host 10.2.3.4
radius-server host 10.4.5.6
```

両方の RADIUS サーバが RADIUS パケットに応答していないが、まだ、停止中としてマークされていない（NAS の起動後のため）場合は、最初のトランザクションのトランスミッションが次のようになります。

```
10.2.3.4
10.2.3.4
10.4.5.6
```

以降のトランザクションは、別のパターンに従って転送されます。トランスミッションは、どちらか（または両方）のサーバを停止中としてマークする基準が満たされているかどうかと、前述したサーバのフラグ設定パターンによって異なります。

順序変更を次のように設定し、

```
aaa new-model
radius-server retry method reorder
radius-server retransmit 1
radius-server max-tries-per-transaction 8
radius-server host 10.1.1.1
radius-server host 10.2.2.2
radius-server host 10.3.3.3
radius-server timeout 3
```

RADIUS サーバ 10.1.1.1 が RADIUS パケットに応答していないが、まだ、停止中としてマークされておらず、残りの 2 つの RADIUS サーバが動作中の場合は、次のように表示されます。

最初のトランザクションの場合：

```
10.1.1.1
10.1.1.1
10.2.2.2
```

サーバが停止中としてマークされる前に任意のトランスミッションに対して開始された追加のトランザクションの場合：

```
10.1.1.1
10.1.1.1
10.2.2.2
```

その後開始されたトランザクションの場合：

```
10.2.2.2
```

その後で、サーバの 10.2.2.2 と 10.3.3.3 もダウンした場合は、サーバの 10.2.2.2 と 10.3.3.3 が停止中としてマークされる基準を満たすまで、次のようなトランスミッションが見られます。

```
10.2.2.2
10.2.2.2
10.3.3.3
10.3.3.3
10.1.1.1
10.1.1.1
10.2.2.2
10.2.2.2
```

この後に、トランスミッションが失敗し、方式リスト内で次の方式が使用されます（存在する場合）。

サーバの 10.2.2.2 と 10.3.3.3 がダウンしたが、同時に、サーバ 10.1.1.1 が復旧した場合は、次のようになります。

```
10.2.2.2
10.2.2.2
10.3.3.3
10.3.3.3
10.1.1.1
```

その後で、サーバの 10.2.2.2 と 10.3.3.3 が停止中としてマークされると、次のようになります。

```
10.1.1.1
```

その他の参考資料

次の項で、RADIUS サーバ障害発生時順序変更に関する参考資料を紹介します。

関連資料

内容	参照先
RADIUS	『*Cisco IOS Security Configuration Guide: Securing User Services*』の「Configuring RADIUS」の章
AAA コマンドと RADIUS コマンド	『*Cisco IOS Security Command Reference*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	—

テクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

RADIUS サーバ障害発生時順序変更の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　RADIUS サーバ障害発生時順序変更の機能情報

機能名	リリース	機能情報
RADIUS サーバ障害発生時順序変更	12.3(1) 12.2(28)SB 12.2(33)SRC	RADIUS サーバ障害発生時順序変更機能は、高負荷期間またはサーバで障害が発生した場合に、サーバ グループ内の別のサーバへのフェールオーバーを提供します。 この機能は、12.3(1) で導入されました。 この機能は、Cisco IOS Release 12.2(28)SB に統合されました。 この機能は、Cisco IOS Release 12.2(33)SRC に統合されました。 **debug aaa sg-server selection**、**radius-server retry method reorder**、および **radius-server transaction max-tries** の各コマンドがこの機能で導入または変更されました。

RADIUS サーバ障害発生時順序変更の機能情報

トンネル ターミネータでの RADIUS 経由でのトンネル認証

トンネル ターミネータでの RADIUS 経由のトンネル認証機能で、トンネル ターミネータのローカル設定ではなくリモート RADIUS サーバ経由でトンネル認証および認可を行うことができます。したがって、ユーザが L2TP access concentrator（LAC; L2TP アクセス コンセントレータ）や Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）network server（LNS; L2TP ネットワーク サーバ）データを、LNS または LAC を着信ダイヤルインまたはダイヤルアウト L2TP トンネル終端で設定する際に、Virtual Private Dialup Network（VPDN; バーチャル プライベート ダイヤルアップ ネットワーク）で設定する必要がなくなりました。この設定情報は、リモート RADIUS サーバに追加することができ、トンネル終端での L2TP トンネル認証と認可の、より管理可能でスケーラブルなソリューションを提供します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「トンネル ターミネータでの RADIUS 経由でのトンネル認証の機能情報」（P.10）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

トンネル ターミネータでの RADIUS 経由でのトンネル認証の前提条件

この機能を設定する前に、RADIUS サーバ グループを定義する必要があります。このタスクの実行に関する情報については、『*Cisco IOS Security Configuration Guide: Securing User Services*』の「Configuring RADIUS」を参照してください。

（注） トンネル イニシエータの RADIUS ユーザのプロファイルのサービスタイプは、「Outbound」に設定する必要があります。

トンネル ターミネータでの RADIUS 経由でのトンネル認証の制約事項

トンネル ターミネータの RADIUS を経由したトンネル認証機能は、L2TP でのみ、つまり、Layer 2 Forwarding（L2F; レイヤ 2 転送）や Point-to-Point Tunneling Protocol（PPTP; ポイントツーポイント トンネリング プロトコル）などのプロトコルでのみ適用できます。

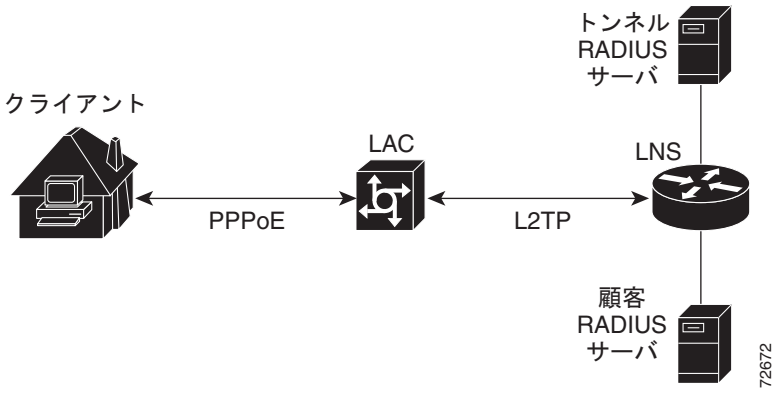
トンネル ターミネータでの RADIUS 経由でのトンネル認証に関する情報

トンネル ターミネータでの RADIUS 経由のトンネル認証機能により、LNS で、着信 LAC ダイヤルイン接続要求での RADIUS を使用したリモート認証および認可を実行できます。また、この機能により、L2TP LAC で、着信 L2TP LNS ダイヤルアウト接続要求での RADIUS を使用したリモート認証および認可を実行できます。

この機能を導入する前は、LNS はローカルでの L2TP トンネル認証および認可のみを実行できます。これらのプロセスでは、多数の LNS 全体を管理するのが難しい場合があります。特に、VPDN グループ数が多い場合などです。これは、LAC 情報を LNS の VDDN グループ設定で設定する必要があるためです。リモート RADIUS 認証および認可で、RADIUS サーバで LAC 設定を保存できます。これにより、この設定情報をローカルで保存しておく必要がなくなります。したがって、新しい LAC 情報を必要に応じて RADIUS サーバに追加でき、LNS グループを、RADIUS の共通ユーザ データベースを使用して認証および認可できます。

図 1 および対応する手順で、この機能の動作について説明します。

図 1　L2TP ダイヤルイン コール トポロジでの LNS リモート RADIUS トンネル認証および認可



- LNS が start-control-connection request（SCCRQ）を受信すると、トンネル認証が開始され、LAC ホスト名とダミー パスワードの「cisco」を添えて RADIUS に要求を送信します（LNS で認証をローカルで行う必要があると判断された場合は、VPDN グループ設定が検索されます）。

（注） ダミー パスワードを変更するには、**vpdn tunnel authorization password** コマンドを使用します。

- LNS から送信されたパスワードと、RADIUS サーバに設定されているパスワードが一致した場合、サーバは LAC 情報が配置された後、アトリビュート 90（Tunnel-Client-Auth-ID）およびアトリビュート 69（Tunnel-Password）を返します。一致しない場合、RADIUS サーバはアクセス拒否を返し、LNS はトンネルをドロップします。
- LNS は次のアトリビュート情報が RADIUS の応答にあるかチェックします。
  - アトリビュート 90（Tunnel-Client-Auth-ID）。LAC ホスト名として使用されます。このアトリビュートが LAC ホスト名と一致しない場合、トンネルはドロップします。
  - アトリビュート 69（Tunnel-Password）。L2TP の見出し様認証共有秘密。このアトリビュートは、SCCRQ で受け取った LAC チャレンジの Attribute-Value Pair（AVP; アトリビュートと値のペア）と比較されます。このアトリビュートが AVP と一致しない場合、トンネルはドロップします。
- 両方のアトリビュートが一致した場合、L2TP トンネルが確立されます。その後、PPP ネゴシエーションとリモート クライアントでの認証を使用して操作を進めることができます。

（注） PPP リモート認証は、お客様が異なる可能性がある RADIUS サーバへ、個々の access-request/access-accept シーケンスにより行われます。トンネル認証は、異なるトンネル RADIUS サーバで行われる可能性があります。

新しい RADIUS アトリビュート

この機能を実装する際に役立つ、シスコ固有の新しい RADIUS アトリビュートが次の 2 つ導入されました。

- Cisco:Cisco-Avpair = "vpdn:dout-dialer = <LAC dialer number>" : どの LAC ダイヤラをダイヤルアウト設定で使用するかを指定します。

- Cisco:Cisco-Avpair = "vpdn:vpdn-vtemplate = <vtemplate number>" : ダイヤルイン設定で LNS のクローニングで使用する仮想テンプレート番号を指定します（このアトリビュートは、vpdn-group 設定の仮想テンプレートの RADIUS の複製です）。

トンネル ターミネータでの RADIUS 経由でのトンネル認証の設定方法

トンネル ターミネータ機能で RADIUS 経由でトンネル認証を設定するタスクについては、次のセクションを参照してください。一覧内の各作業は、必須と任意に分けています。

- 「リモート RADIUS トンネル認証および認可での LNS または LAC の設定」（P.4）（必須）
- 「リモート RADIUS トンネル認証 および認可設定の確認」（P.5）（任意）

リモート RADIUS トンネル認証および認可での LNS または LAC の設定

次のタスクが、着信ダイヤルインまたはダイヤルアウト L2TP トンネル終端での LNS または LAC の設定に使用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authorization network** {**default** | *list-name*} *method1* [*method2...*]
4. **vpdn tunnel authorization network** {*method-list-name* | **default**}
5. **vpdn tunnel authorization virtual-template** *vtemplate-number*
6. **vpdn tunnel authorization password** *password*

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa authorization network** {**default** | *list-name*} *method1* [*method2...*] 例： `Router(config)# aaa authorization network mymethodlist group VPDN-Group`	ネットワーク サービスの AA 認証方式リストを定義します。

	コマンド	目的
ステップ 4	**vpdn tunnel authorization network** {*method-list-name* | **default**} 例： `Router(config)# vpdn tunnel authorization network mymethodlist`	リモート ホスト名ベースの認証で使用する AAA 認証方式リストを指定します。 • *list-name* 引数が **aaa authorization** コマンドで指定された場合、ここでそのリスト名を使用します。 • デフォルトのキーワードが **aaa authorization** コマンドで指定された場合、ここで、**aaa authorization** コマンドを使用してリストされたデフォルトの認証方式を指定するこのキーワードを指定する必要があります。
ステップ 5	**vpdn tunnel authorization virtual-template** *vtemplate-number* 例： `Router(config)# vpdn tunnel authorization virtual-template 10`	（任意）仮想アクセス インターフェイスの複製元のデフォルトの仮想テンプレートを選択します。
ステップ 6	**vpdn tunnel authorization password** *password* 例： `Router(config)# vpdn tunnel authorization password cisco`	（任意）リモート トンネルのホスト名に基づいたトンネル設定を取得するための RADIUS 認証要求の「ダミー」のパスワードを設定します。 **（注）** このコマンドがイネーブルでない場合、このパスワードは「cisco」になります。

リモート RADIUS トンネル認証 および認可設定の確認

L2TP トンネルがアップしているか確認するには、EXEC モードで **show vpdn tunnel** コマンドを使用します。トンネルとセッションが 1 つずつ設定されている必要があります。

```
Router# show vpdn tunnel

L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name   State  Remote Address  Port  Sessions VPDN Group
4571  61568 csidtw13 est    10.0.195.4      1701  1        ?

LocID RemID TunID Intf          Username               State  Last Chg
4     11    4571  Vi4.1         csidtw9@cisco.com       est    00:02:29

%No active L2F tunnels
%No active PPTP tunnels
%No active PPPoE tunnels

To verify that the AAA authorization RADIUS server is configured on the LNS and that the
LNS can receive attributes 90 and 69 from the RADIUS server, perform the following steps:
```

ステップ 1 LNS で **debug radius** コマンドをイネーブルにします。

ステップ 2 LNS で **show logging** コマンドをイネーブルにし、「access-accept」が出力にあり、アトリビュート 90 および 69 が、RADIUS 応答で確認できるようにします。

```
00:32:56: RADIUS: Received from id 21645/5 172.19.192.50:1645, Access-Accept, len 81
00:32:56: RADIUS:  authenticator 73 2B 1B C2 33 71 93 19 - 62 AC 3E BE 0D 13 14 85
00:32:56: RADIUS:  Service-Type        [6]   6   Outbound                  [5]
00:32:56: RADIUS:  Tunnel-Type         [64]  6   00:L2TP                   [3]
00:32:56: RADIUS:  Tunnel-Medium-Type  [65]  6   00:IPv4                   [1]
00:32:56: RADIUS:  Tunnel-Client-Auth-I[90]  6   00:"csidtw13"
00:32:56: RADIUS:  Tunnel-Password     [69]  8   *
00:32:56: RADIUS:  Vendor, Cisco       [26]  29
```

```
00:32:56: RADIUS:   Cisco AVpair       [1]   23  "vpdn:vpdn-vtemplate=1"
```

L2TP トンネルが確立され、LNS がリモート クライアントで PPP ネゴシエーションと認証を実行できるか確認するには、次の手順を実行します。

ステップ 1 LNS で **debug ppp negotiation** および **debug ppp authentication** コマンドをイネーブルにします。

ステップ 2 LNS で **show logging** コマンドをイネーブルにし、LNS が PPP CHAP チャレンジを受信し、PPP CHAP「SUCCESS」をクライアントに送信することを確認します。

```
00:38:50: ppp3 PPP: Received LOGIN Response from AAA = PASS
00:38:50: ppp3 PPP: Phase is FORWARDING, Attempting Forward
00:38:50: Vi4.1  Tnl/Sn4571/4 L2TP: Session state change from wait-for-service-selection
to established
00:38:50: Vi4.1 PPP: Phase is AUTHENTICATING, Authenticated User
00:38:50: Vi4.1 CHAP: O SUCCESS id 1 len 4
```

ステップ 3 PPP 認証が成功したら、デバッグ出力で PPP ネゴシエーションが開始されていることと LNS が LCP（IPCP）パケットを受信していること、およびネゴシエーションが成功していることを確認します。

```
00:38:50: Vi4.1 IPCP: State is Open
00:38:50: Vi4.1 IPCP: Install route to 200.1.1.4
```

トンネル ターミネータでの RADIUS 経由でのトンネル認証の設定例

ここでは、次の設定例について説明します。

- 「L2TP Network Server（LNS; L2TP ネットワーク サーバ）設定の例」（P.6）
- 「リモート RADIUS トンネル認証の RADIUS ユーザ プロファイルの例」（P.6）

L2TP Network Server（LNS; L2TP ネットワーク サーバ）設定の例

次は、LNS でリモート RADIUS トンネル認証および認可をイネーブルに設定する方法の例です。

```
! Define a RADIUS server group
aaa group server radius VPDN-group
 server 64.102.48.91 auth-port 1645 acct-port 1646
!
! RADIUS configurations only
aaa authorization network mymethodlist group VPDN-Group
vpdn tunnel authorization network mymethodlist
vpdn tunnel authorization virtual-template 10
```

リモート RADIUS トンネル認証の RADIUS ユーザ プロファイルの例

次は、LNS で LAC からの L2TP トンネルを終端させる RADIUS ユーザ プロファイルの例です。最初のユーザ プロファイルの最後の行は、**vpdn tunnel authorization virtual-template** コマンドが使用されている場合は任意です。また、最初の RADIUS ユーザ プロファイルが L2TP ダイヤルイン向けで、2 番めの RADIUS ユーザ プロファイルが L2TP ダイヤルアウト向けの場合も任意です。

トンネル イニシエータの RADIUS ユーザのプロファイルのサービスタイプは、「Outbound」に設定する必要があります。

```
csidtw13  Password = "cisco"
        Service-Type = Outbound,
        Tunnel-Type = :0:L2TP,
        Tunnel-Medium-Type = :0:IP,
        Tunnel-Client-Auth-ID = :0:"csidtw13",
        Tunnel-Password = :0:"cisco"
        Cisco:Cisco-Avpair = "vpdn:vpdn-vtemplate=1"

csidtw1 Password = “cisco”
        Service-Type = Outbound,
        Tunnel-Type = :0:L2TP,
        Tunnel-Medium-Type = :0:IP,
        Tunnel-Client-Auth-ID = :0:"csidtw1",
        Tunnel-Password = :0:"cisco"
        Cisco:Cisco-Avpair = "vpdn:dout-dialer=2"
```

その他の参考資料

次のセクションで、トンネル ターミネータ機能での RADIUS 経由のトンネル認証に関連する参考資料を説明しています。

関連資料

内容	参照先
VPN	『*Cisco IOS VPDN Configuration Guide*, Release 12.4T』
RADIUS アトリビュート	『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 15.0』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2868	「*RADIUS Attributes for Tunnel Protocol Support*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

トンネル ターミネータでの RADIUS 経由でのトンネル認証の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　トンネル ターミネータでの RADIUS 経由でのトンネル認証の機能情報

機能名	リリース	機能情報
トンネル ターミネータでの RADIUS 経由でのトンネル認証	12.2(15)B 12.3(4)T	トンネル ターミネータでの RADIUS 経由のトンネル認証機能で、トンネル ターミネータのローカル設定ではなくリモート RADIUS サーバ経由でトンネル認証および認可を行うことができます。 12.2(15)B では、この機能は Cisco 6400 シリーズ、Cisco 7200 シリーズおよび Cisco 7400 シリーズで導入されました。 12.3(4)T では、この機能は Cisco IOS に統合されました。 次のコマンドが導入または修正されました。**vpdn tunnel authorization network**、**vpdn tunnel authorization password**、**vpdn tunnel authorization virtual-template**

用語集

L2TP：Layer 2 Tunnel Protocol（レイヤ 2 トンネル プロトコル）。レイヤ 2 トンネル プロトコルを使用すると、ISP などのアクセス サービスが仮想トンネルを作成し、顧客のリモート サイトやリモート ユーザを企業のホーム ネットワークにリンクさせることができます。具体的には、ISP Point of Presence（POP; アクセス ポイント）にある Network Access Server（NAS; ネットワーク アクセス サーバ）がリモート ユーザと PPP メッセージを交換し、L2F または L2TP の要求や応答を使用して顧客のトンネル サーバと通信し、トンネルのセットアップを行います。

LAC：L2TP Access Concentrator（L2TP アクセス コンセントレータ）。クライアントが直接接続し、PPP フレームが L2TP Network Server（LNS; L2TP ネットワーク サーバ）にトンネリングされる Network Access Server（NAS; ネットワーク アクセス サーバ）です。LAC は、L2TP が 1 つまたは複

数の LNS にトラフィックを渡すために操作するメディアのみを実装します。LAC は PPP 内で伝送されるすべてのプロトコルをトンネルすることができます。また、LAC は着信コールを開始して、発信コールを受け取ります。LAC は L2F ネットワーク アクセス サーバに似ています。

LNS : L2TP Network Server（L2TP ネットワーク サーバ）。L2TP トンネルの終端ポイントと、PPP フレームが処理され、高レイヤ プロトコルに渡されるアクセス ポイント。LNS は PPP を終端させる任意のプラットフォーム上で動作できます。LNS はサーバ側の L2TP プロトコルを処理します。L2TP は、L2TP のトンネルが到達する 1 つのメディアにのみ依存します。LNS は発信コールを開始して、着信コールを受け取ります。LNS は L2F テクノロジーのホーム ゲートウェイに似ています。

TACACS+

TACACS+ の設定

TACACS+ は、認証および認可プロセスについて詳細なアカウンティング情報と柔軟な管理コントロールを提供します。AAA によって TACACS+ は容易になります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「TACACS+ の設定に関する機能情報」（P.15）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

TACACS+ の設定に関する前提条件

ネットワーク アクセス サーバに設定した TACACS+ 機能を使用可能にするには、TACACS+ サーバにアクセスして TACACS+ サーバを設定しておく必要があります。

TACACS+ の設定に関する制約事項

TACACS+ をイネーブルにするには、AAA コマンドを使用する必要があります。

TACACS+ の概要

TACACS+ は、ユーザによるルータまたはネットワーク アクセス サーバへのアクセス試行の集中的な確認を可能にするセキュリティ アプリケーションです。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で動作する TACACS+ デーモンのデータベースで管理されます。

TACACS+ は独立したモジュール型の認証、認可、およびアカウンティング機能を備えています。TACACS+ では、1 つのアクセス制御サーバ（TACACS+ デーモン）が認証、認可、およびアカウンティングの各サービスを個別に提供できます。各サービスをそれぞれ固有のデータベースに結合し、デーモンの機能に応じて、そのサーバまたはネットワーク上で使用できる他のサービスを利用できます。

TACACS+ の目標は、単一の管理サービスから、複数のネットワーク アクセス ポイントを管理する方法論を提供することです。アクセス サーバおよびルーティングのシスコ ファミリおよび（ルータとアクセス サーバ両方の）Cisco IOS ユーザ インターフェイスは、ネットワーク アクセス サーバにすることができます。

ネットワーク アクセス ポイントによって、従来の「低機能な」端末、端末エミュレータ、ワークステーション、パーソナル コンピュータ（PC）、およびルータと、適切なアダプタ（たとえば、モデムまたは ISDN アダプタ）を併用して、Point-to-Point Protocol（PPP）、Serial Line Internet Protocol（SLIP）、Compressed SLIP（CSLIP）、または AppleTalk Remote Access（ARA）プロトコルを使用する通信が可能になります。つまり、ネットワーク アクセス サーバは、単一のユーザ、ネットワークまたはサブネットワーク、および相互接続したネットワークに対して、接続を提供できます。ネットワーク アクセス サーバを介して接続されているエンティティは、*ネットワーク アクセス クライアント*と呼ばれます。たとえば、音声グレードの回路で PPP を実行する PC は、ネットワーク アクセス クライアントです。AAA セキュリティ サービスを介して管理される TACACS+ は、次のサービスを提供できます。

- 認証：ログインとパスワードのダイアログ、チャレンジ/レスポンス、メッセージングのサポートを介して、認証を詳細に制御できます。

  認証機能には、ユーザに任意のダイアログを実行する機能があります（たとえば、ログインとパスワードの指定後に、自宅住所、母親の旧姓、サービス タイプ、社会保険番号などの複数の質問をユーザに試行する機能）。さらに、TACACS+ 認証サービスは、ユーザ画面へのメッセージ送信をサポートします。たとえば、会社のパスワード有効期限ポリシーのために、パスワードを変更する必要があるというメッセージをユーザに通知できます。

- 認可：ユーザ セッションの期間に関するユーザ機能を詳細に制御できます。たとえば、autocommand の設定、アクセス コントロール、セッションの持続時間、プロトコルのサポートなどです。また、TACACS+ 認可機能を使用して、ユーザが実行できるコマンドを制限することもできます。

- アカウンティング：課金、監査、およびレポートに使用される情報を収集し、TACACS+ デーモンに送信します。ネットワーク マネージャは、アカウンティング機能を使用して、セキュリティ監査に関するユーザ アクティビティを追跡することや、ユーザの課金に関する情報を提供することができます。アカウンティング レコードには、ユーザ ID、開始時刻と終了時刻、実行されたコマンド（PPP など）、パケット数、およびバイト数が含まれます。

TACACS+ プロトコルは、ネットワーク アクセス サーバと TACACS+ デーモンの間に認証機能を提供します。また、ネットワーク アクセス サーバと TACACS+ デーモン間のすべてのプロトコル交換は暗号化されるため、機密性を確保できます。

TACACS+ デーモン ソフトウェアを実行するシステムで、ネットワーク アクセス サーバで TACACS+ 機能を使用する必要があります。

独自の TACACS+ ソフトウェアを開発することに関心があるユーザ向けに、シスコでは、TACACS+ プロトコル仕様をドラフトの RFC として使用できるようにしています。

TACACS+ の操作

ユーザが TACACS+ を使用してネットワーク アクセス サーバに対して認証を受けることで、単純な ASCII ログインを試行すると、一般的に、次のプロセスが発生します。

1. 接続が確立すると、ネットワーク アクセス サーバは TACACS+ デーモンに接続してユーザ名のプロンプトをを取得します。また、そのプロンプトはユーザに表示されます。ユーザがユーザ名を入力すると、ネットワーク アクセス サーバは TACACS+ デーモンに接続し、パスワード プロンプトを取得します。ネットワーク アクセス サーバはユーザに対してパスワード プロンプトを表示します。ユーザがパスワードを入力すると、パスワードは TACACS+ デーモンに送信されます。

（注） TACACS+ によって、デーモンとユーザとの間で対話できるようになり、デーモンはユーザの認証に必要な情報を取得できるようになります。通常、この処理は、ユーザ名とパスワードの組み合わせのプロンプトを表示することで完了しますが、TACACS+ デーモンの制御下で、母親の旧姓など、他のアイテムを含めることができます。

2. ネットワーク アクセス サーバは、最終的に TACACS+ デーモンから次のいずれかの応答を得ます。
   a. ACCEPT：ユーザは認証され、サービスを開始できます。認可を必須にするようにネットワーク アクセス サーバが設定されている場合、この時点で認可が開始されます。
   b. REJECT：ユーザは認証に失敗しました。ユーザは以降のアクセスを拒否される可能性があります。または、TACACS+ デーモンに応じてログイン シーケンスを再試行するようにプロンプトが表示されます。
   c. ERROR：認証中のある時点でエラーが発生しました。エラーは、デーモン、またはデーモンとネットワーク アクセス サーバ間のネットワーク接続で発生する可能性があります。ERROR 応答を受信すると、通常、ネットワーク アクセス サーバはユーザを認証する代替方式を使用しようとします。
   d. CONTINUE：追加の認証情報を入力するようにユーザにプロンプトを表示します。
3. PAP ログインは、ASCII ログインに似ていますが、ユーザによる入力ではなく、PAP プロトコルパケットでユーザ名とパスワードがネットワーク アクセス サーバに到達するため、ユーザにはプロンプトが表示されません。PPP CHAP ログインは、原則もにています。

ネットワーク アクセス サーバで認可をイネーブルにしている場合、認証の後に、ユーザは追加の認可段階を実行する必要があります。ユーザは TACACS+ 認証が正常に完了しないうちは、TACACS+ 許可に進めません。

4. TACACS+ の認可が必要な場合も、TACACS+ デーモンに接続します。また、TACACS+ デーモンは、ACCEPT または REJECT 認可応答を返します。ACCEPT 応答が返される場合、この応答には、そのユーザに関する EXEC または NETWORK セッションを指示するために使用されるアトリビュートの形式のデータが含まれます。これによって、ユーザがアクセスできるサービスを判断します。

   次のようなサービスがあります。

   a. Telnet、rlogin、PPP（ポイントツーポイント プロトコル）、Serial Line Internet Protocol（SLIP; シリアル ライン インターネット プロトコル）または、EXEC サービス

   b. ホストまたはクライアントの IP アドレス、アクセス リスト、ユーザ タイムアウトなどの接続パラメータ

TACACS+ の AV ペア

ネットワーク アクセス サーバが TACACS+ 認可機能およびアカウンティング機能を実装するには、各ユーザ セッションで TACACS+ のアトリビュートと値（AV）ペアを送受信します。サポートされる TACACS+ の AV ペアのリストについては、付録の「TACACS+ Attribute-Value Pairs」を参照してください。

TACACS+ を設定する方法

TACACS+ をサポートするようにルータを設定するには、次のタスクを実行する必要があります。

- **aaa new-model** グローバル コンフィギュレーション コマンドを使用して、AAA をイネーブルにします。TACACS+ を使用する予定がある場合、AAA を設定する必要があります。
- **aaa authentication** グローバル コンフィギュレーション コマンドを使用して、認証に TACACS+ を使用する方式リストを定義します。詳細については、「Configuring Authentication」フィーチャ モジュールを参照してください。
- **line** および **interface** コマンドを使用して、定義済みの方式リストを多様なインターフェイスに適用します。詳細については、「Configuring Authentication」フィーチャ モジュールを参照してください。
- 必要に応じて、**aaa authorization** グローバル コマンドを使用して、ネットワーク アクセス サーバの認可を設定します。回線またはインターフェイスごとに設定できる認証とは異なり、認可は、ネットワーク アクセス サーバ全体のグローバル設定です。詳細については、「Configuring Authorization」フィーチャ モジュールを参照してください。
- 必要に応じて、**aaa accounting** コマンドを使用して TACACS+ 接続のアカウンティングをイネーブルにします。詳細については、「Configuring Accounting」フィーチャ モジュールを参照してください。

ここでは、TACACS+ を設定するタスクを実行します。

- 「TACACS+ サーバ ホストの指定」（必須）
- 「TACACS+ 認証キーの設定」（任意）
- 「AAA サーバ グループの設定」（任意）
- 「DNIS に基づく AAA サーバ グループの選択の設定」（任意）
- 「TACACS+ 認証の指定」（必須）
- 「TACACS+ 認可の指定」（任意）

- 「TACACS+ アカウンティングの指定」（任意）

TACACS+ サーバ ホストの指定

tacacs-server host コマンドを使用すると、TACACS+ サーバを保守する 1 つまたは複数の IP ホストの名前を指定できます。TACACS+ ソフトウェアは、指定した順序でホストを検索するため、この機能は、希望のデーモン リストを設定する場合に役立ちます。

TACACS+ ホストを指定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# tacacs-server host hostname [single-connection] [port integer] [timeout integer] [key string]`	TACACS+ ホストを指定します。

tacacs-server host コマンドを使用すると、次のオプションも設定できます。

- **single-connection** キーワードを使用して、単一接続を指定できます（CiscoSecure Release 1.0.1 以降でのみ有効）。通信が必要になるたびに、ルータの接続を開き、TCP 接続を閉じるのではなく、single-connection オプションによって、ルータとデーモン間の単一のオープンな接続を保守します。この方法はデーモンが処理できる TACACS 操作数が多くなるため、効率的です。

  （注） この処理を有効にするには、デーモンが single-connection モードをサポートする必要があります。サポートしていない場合、ネットワーク アクセス サーバとデーモン間の接続が動作しなくなるか、不要なエラーを受信します。

- **port** *integer* 引数を使用して、TACACS+ デーモンに接続するときに使用される TCP ポート番号を指定します。デフォルト ポート番号は 49 です。
- **timeout** *integer* 引数を使用して、ルータがタイムアウトしてエラー宣言するまで、デーモンからの応答を待つ期間（秒）を指定します。

  （注） **tacacs-server host** コマンドによるタイムアウト値の指定は、このサーバに関する **tacacs-server timeout** コマンドで設定されたデフォルトのタイムアウト値よりも優先されます。

- **key** *string* 引数を指定して、ネットワーク アクセス サーバと TACACS+ デーモン間のすべてのトラフィックを暗号化および復号化するための暗号化キーを指定します。

  （注） **tacacs-server host** コマンドによる暗号化キーの指定は、このサーバに関するグローバル コンフィギュレーションの **tacacs-server key** コマンドで設定されたデフォルト キーよりも優先されます。

tacacs-server host コマンドのパラメータの一部は、**tacacs-server timeout** コマンドおよび **tacacs-server key** コマンドによるグローバル設定よりも優先されるため、このコマンドを使用して個別の TACACS+ 接続を一意に設定することで、ネットワークのセキュリティを強化できます。

TACACS+ 認証キーの設定

ネットワーク アクセス サーバと TACACS+ デーモンの間で交換されるすべてのデータを暗号化するために、グローバル TACACS+ 認証キーと暗号化キーを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# tacacs-server key key`	TACACS+ デーモンで使用する、一致する暗号化キーを設定します。

（注） 暗号化に成功するには、TACACS+ デーモンに同じキーを設定する必要があります。

AAA サーバ グループの設定

AAA サーバ グループを使用するようにルータを設定すると、既存のサーバ ホストをグループ化できます。これによって、設定したサーバ ホストのサブセットを選択し、それを特定のサービスに使用できます。サーバ グループは、グローバル サーバ ホスト リストと併せて使用されます。サーバ グループには、選択したサーバ ホストの IP アドレスが一覧表示されます。

サーバ グループには複数のホスト エントリを含めることができます。ただし、各エントリの IP アドレスが一意である必要があります。そのサーバ グループにある異なる 2 つのホスト エントリが 1 つのサービス（アカウンティングなど）に設定されている場合、設定されている 2 番めのホスト エントリは最初のホスト エントリのフェールオーバー バックアップとして動作します。この例の場合、最初のホスト エントリがアカウンティング サービスの提供に失敗すると、2 番めのホスト エントリを使用してアカウンティング サービスを提供するように、ネットワーク アクセス サーバが試行します（試行される TACACS+ ホスト エントリの順番は、設定されている順序に従います）。

サーバ グループ名を使用してサーバ ホストを定義するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。一覧のサーバは、グローバル コンフィギュレーション モードに存在します。

	コマンド	目的
ステップ 1	`Router(config)# tacacs-server host name [single-connection] [port integer] [timeout integer] [key string]`	サーバ ホストの IP アドレスを指定および定義してから、AAA サーバ グループを設定します。**tacacs-server host** コマンドの詳細については、「TACACS+ サーバ ホストの指定」（P.5）を参照してください。

	コマンド	目的
ステップ 2	Router(config-if)# **aaa group server** {**radius** | **tacacs+**} *group-name*	グループ名を指定して AAA サーバ グループを定義します。グループのすべてのメンバは、タイプを同じにする必要があります。つまり、RADIUS または TACACS+ です。このコマンドでは、サーバ グループのサブコンフィギュレーション モードにルータを配置します。
ステップ 3	Router(config-sg)# **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]	特定の TACACS+ サーバを定義済みのサーバ グループと関連付けます。**auth-port** *port-number* オプションを使用して、認証専用の UDP ポートを設定します。**acct-port** *port-number* オプションを使用して、アカウンティング専用の UDP ポートを設定します。 AAA サーバ グループの各 TACACS+ サーバについて、この手順を繰り返します。 **（注）** グループの各サーバは、**tacacs-server host** コマンドを使用して事前に定義する必要があります。

DNIS に基づく AAA サーバ グループの選択の設定

Cisco IOS ソフトウェアを使用すると、セッションの Dialed Number Identification Service（DNIS）番号に基づき、特定の AAA サーバ グループに対してユーザを認証できます。すべての電話回線（通常の自宅電話または商用の T1/PRI 回線）を、複数の電話番号と関連付けることができます。DNIS 番号は、ユーザ宛てに発信された番号を示します。

たとえば、複数の顧客で同じ電話番号を共有する場合に、電話を受ける前に発信元を知りたいことがあります。DNIS を使用すると、応答するときに発信元の顧客がわかるため、電話に応答する方法をカスタマイズできます。

ISDN または内部モデムと接続する Cisco ルータは、DNIS 番号を受信できます。この機能を使用すると、顧客ごとに異なる TACACS+ サーバ グループを割り当て可能です（つまり、DNIS 番号ごとに異なる TACACS+ サーバ）。さらに、サーバ グループを使用して、複数の AAA サービスに同じサーバ グループを指定できます。また、各 AAA サービスに個別のサーバ グループを指定できます。

Cisco IOS ソフトウェアには、認証サービスとアカウンティング サービスを複数の方法で実装できる柔軟性があります。

- グローバル：AAA サービスは、グローバル コンフィギュレーション アクセス リスト コマンドを使用して定義され、特定のネットワーク アクセス サーバ上のすべてのインターフェイスに、全般的に適用されます。
- インターフェイス別：AAA サービスは、インターフェイス コンフィギュレーション コマンドを使用して定義され、特定のネットワーク アクセス サーバに設定されているインターフェイスにだけ適用されます。
- DNIS マッピング：DNIS を使用して、AAA サーバが AAA サービスを提供するように指定します。

複数の AAA コンフィギュレーション方式を同時に設定できるため、シスコでは、AAA サービスを提供するサーバまたはサーバ グループを決定するために、優先順位を設定しました。優先順位は次のとおりです。

- DNIS 別：DNIS を使用し、AAA サービスを提供するサーバ グループを指定するようにネットワーク アクセス サーバを設定している場合、この方式の方がその他の AAA 選択方式よりも優先されます。
- インターフェイス別：サーバから AAA サービスを提供する方法を決定するために、インターフェイス別にネットワーク アクセス サーバを設定してアクセス リストを使用する場合、この方式は、他のグローバル コンフィギュレーション AAA アクセス リストよりも優先されます。
- グローバル：セキュリティ サーバが AAA サービスを提供する方法を決定するために、グローバル AAA アクセス リストを使用してネットワーク アクセス サーバを設定する場合、この方式には最も低い優先度が使用されます。

（注） DNIS に基づいて AAA サーバ グループの選択を設定する前に、各 AAA サーバ グループに関連付けられたリモート セキュリティ サーバを設定する必要があります。詳細については、「TACACS+ サーバ ホストの指定」（P.5）および「AAA サーバ グループの設定」（P.6）を参照してください。

サーバ グループの DNIS に基づいて、特定の AAA サーバ グループを選択するようにルータを設定するには、DNIS マッピングを設定します。DNIS 番号を使用して、サーバ グループをグループ名とマッピングするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# aas dnis map enable`	DNIS マッピングをイネーブルにします。
ステップ 2	`Router(config)# aaa dnis map dnis-number authentication ppp group server-group-name`	DNIS 番号を定義済みの AAA サーバ グループにマッピングします。このサーバ グループのサーバは、認証に使用されます。
ステップ 3	`Router(config)# aaa dnis map dnis-number accounting network [none | start-stop | stop-only] group server-group-name`	DNIS 番号を定義済みの AAA サーバ グループにマッピングします。このサーバ グループのサーバは、アカウンティングに使用されます。

TACACS+ 認証の指定

TACACS+ デーモンを指定し、関連する TACACS+ 暗号化キーを定義したら、TACACS+ 認証の方式リストを定義する必要があります。TACACS+ 認証は AAA を介して実行されるため、認証方式として TACACS+ を指定して、**aaa authentication** コマンドを発行する必要があります。詳細については、「Configuring Authentication」フィーチャ モジュールを参照してください。

TACACS+ 認可の指定

AAA 認可を使用すると、ユーザのアクセスをそのネットワークに制限するパラメータを設定できます。TACACS+ を介する認可は、コマンド、ネットワーク接続、および EXEC セッションに適用できます。AAA によって TACACS+ 認可は容易になるため、認証方式として TACACS+ を指定して、**aaa authorization** コマンドを発行する必要があります。詳細については、「Configuring Authorization」フィーチャ モジュールを参照してください。

TACACS+ アカウンティングの指定

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や、ユーザが消費しているネットワーク リソース量を追跡できます。AAA によって TACACS+ アカウンティングは容易になるため、アカウンティング方式として TACACS+ を指定して、**aaa accounting** コマンドを発行する必要があります。詳細については、「Configuring Accounting」フィーチャ モジュールを参照してください。

TACACS+ の設定例

ここでは、TACACS+ 設定の例を紹介します。

- 「TACACS+ 認証の例」
- 「TACACS+ 認可の例」
- 「TACACS+ アカウンティングの例」
- 「TACACS+ サーバ グループの例」
- 「DNIS に基づく AAA サーバ グループの選択の設定例」
- 「TACACS+ デーモンの設定例」

TACACS+ 認証の例

次に、PPP 認証に使用するセキュリティ プロトコルとして TACACS+ を設定する例を示します。

```
aaa new-model
aaa authentication ppp test group tacacs+ local
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
 ppp authentication chap pap test
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「test」を定義します。キーワード **group tacacs+** は、TACACS+ を介して認証を実行することを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。
- **tacacs-server host** コマンドにより、TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。**tacacs-server key** コマンドにより、共有暗号化キーを「goaway」に定義します。
- **interface** コマンドで回線を選択します。**ppp authentication** コマンドは、テスト方式リストをこの回線に適用します。

次に、PPP 認証のセキュリティ プロトコルとして TACACS+ を設定する例を示します。ただし、「test」方式リストの代わりに、「default」方式リストが使用されます。

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
```

```
 ppp authentication chap default
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「default」を定義します。キーワード **default** は、デフォルトですべてのインターフェイスに PPP 認証が適用されることを示します。**if-needed** キーワードは、ユーザが ASCII ログイン手順を介してすでに認証済みの場合、PPP 認証は不要なので、スキップできることを示します。認証が必要な場合、キーワード **group tacacs+** は、認証が TACACS+ を介して実行されることを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。
- **tacacs-server host** コマンドにより、TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。**tacacs-server key** コマンドにより、共有暗号化キーを「goaway」に定義します。
- **interface** コマンドで回線を選択します。**ppp authentication** コマンドは、デフォルト方式リストをこの回線に適用します。

次に、PAP に同じ認証アルゴリズムを作成し、「default」ではなく「MIS-access」の方式リストを呼び出す例を示します。

```
aaa new-model
aaa authentication pap MIS-access if-needed group tacacs+ local
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
 ppp authentication pap MIS-access
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「MIS-access」を定義します。方式リストの「MIS-access」は、PPP 認証がすべての委付に適用されることを示します。**if-needed** キーワードは、ユーザが ASCII ログイン手順を介してすでに認証済みの場合、PPP 認証は不要なので、スキップできることを示します。認証が必要な場合、キーワード **group tacacs+** は、認証が TACACS+ を介して実行されることを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。
- **tacacs-server host** コマンドにより、TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。**tacacs-server key** コマンドにより、共有暗号化キーを「goaway」に定義します。
- **interface** コマンドで回線を選択します。**ppp authentication** コマンドは、デフォルト方式リストをこの回線に適用します。

次に、IP アドレスが 10.2.3.4 の TACACS+ デーモンと「apple」の暗号化キーの設定を表示する例を示します。

```
aaa new-model
aaa authentication login default group tacacs+ local
tacacs-server host 10.2.3.4
tacacs-server key apple
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。

- **aaa authentication** コマンドで、デフォルトの方式リストを定義します。すべてのインターフェイスでの着信 ASCII ログイン（デフォルト）では、認証に TACACS+ を使用します。応答する TACACS+ サーバがない場合、ネットワーク アクセス サーバは、認証用のローカル ユーザ名データベースに含まれる情報を使用します。
- **tacacs-server host** コマンドにより、TACACS+ デーモンが 10.2.3.4 という IP アドレスを持っていると指定します。**tacacs-server key** コマンドにより、共有暗号化キーを「apple」に定義します。

TACACS+ 認可の例

次に、デフォルトの方式リストを使用して、PPP 認証用のセキュリティ プロトコルとして、TACACS+ を設定する例を示します。また、TACACS+ を介してネットワークの認可を設定する方法も示します。

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
aaa authorization network default group tacacs+
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
 ppp authentication chap default
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「default」を定義します。キーワード **default** は、デフォルトですべてのインターフェイスに PPP 認証が適用されることを示します。**if-needed** キーワードは、ユーザが ASCII ログイン手順を介してすでに認証済みの場合、PPP 認証は不要なので、スキップできることを示します。認証が必要な場合、キーワード **group tacacs+** は、認証が TACACS+ を介して実行されることを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。
- **aaa authorization** コマンドにより、TACACS+ を介するネットワーク認可を設定します。認証リストとは異なり、この認可リストは、ネットワーク アクセス サーバに対するすべての着信ネットワーク接続に常に適用されます。
- **tacacs-server host** コマンドにより、TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。**tacacs-server key** コマンドにより、共有暗号化キーを「goaway」に定義します。
- **interface** コマンドで回線を選択します。**ppp authentication** コマンドは、デフォルト方式リストをこの回線に適用します。

TACACS+ アカウンティングの例

次に、デフォルトの方式リストを使用して、PPP 認証用のセキュリティ プロトコルとして、TACACS+ を設定する例を示します。また、TACACS+ を介してアカウンティングを設定する方法も示します。

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
aaa accounting network default stop-only group tacacs+
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
 ppp authentication chap default
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「default」を定義します。キーワード **default** は、デフォルトですべてのインターフェイスに PPP 認証が適用されることを示します。**if-needed** キーワードは、ユーザが ASCII ログイン手順を介してすでに認証済みの場合、PPP 認証は不要なので、スキップできることを示します。認証が必要な場合、キーワード **group tacacs+** は、認証が TACACS+ を介して実行されることを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。
- **aaa accounting** コマンドにより、TACACS+ を介するネットワーク アカウンティングを設定します。この例では、ネットワーク接続が終了するたびに、終了したセッションについて説明するアカウンティング レコードが、TACACS+ デーモンに送信されます。
- **tacacs-server host** コマンドにより､TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。**tacacs-server key** コマンドにより、共有暗号化キーを「goaway」に定義します。
- **interface** コマンドで回線を選択します。**ppp authentication** コマンドは、デフォルト方式リストをこの回線に適用します。

TACACS+ サーバ グループの例

次に、3 つの異なる TACACS+ サーバ メンバを使用してサーバ グループを作成する例を示します。

```
aaa group server tacacs tacgroup1
    server 172.16.1.1
    server 172.16.1.21
    server 172.16.1.31
```

DNIS に基づく AAA サーバ グループの選択の設定例

次に、特定の AAA サービスを提供するために、DNIS に基づいて TACACS+ サーバ グループを選択する例を示します。

```
! This command enables AAA.
aaa new-model
!
! The following set of commands configures the TACACS+ servers that will be associated
! with one of the defined server groups.
tacacs-server host 172.16.0.1
tacacs-server host 172.17.0.1
tacacs-server host 172.18.0.1
tacacs-server host 172.19.0.1
tacacs-server host 172.20.0.1
tacacs-server key abcdefg

! The following commands define the sg1 TACACS+ server group and associate servers
! with it.
aaa group server tacacs sg1
  server 172.16.0.1
  server 172.17.0.1
! The following commands define the sg2 TACACS+ server group and associate a server
! with it.
aaa group server tacacs sg2
  server 172.18.0.1
```

```
! The following commands define the sg3 TACACS+ server group and associate a server
! with it.
aaa group server tacacs sg3
  server 172.19.0.1
! The following commands define the default-group TACACS+ server group and associate
! a server with it.
aaa group server tacacs default-group
  server 172.20.0.1
!
! The next set of commands configures default-group tacacs server group parameters.
aaa authentication ppp default group default-group
aaa accounting network default start-stop group default-group
!
! The next set of commands enables DNIS mapping and maps DNIS numbers to the defined
! RADIUS server groups. In this configuration, all PPP connection requests using DNIS
! 7777 are sent to the sg1 server group. The accounting records for these connections
! (specifically, start-stop records) are handled by the sg2 server group. Calls with a
! DNIS of 8888 use server group sg3 for authentication and server group default-group
! for accounting. Calls with a DNIS of 9999 use server group default-group for
! authentication and server group sg3 for accounting records (stop records only). All
! other calls with DNIS other than the ones defined use the server group default-group
! for both authentication and stop-start accounting records.
aaa dnis map enable
aaa dnis map 7777 authentication ppp group sg1
aaa dnis map 7777 accounting network start-stop group sg2
aaa dnis map 8888 authentication ppp group sg3
aaa dnis map 9999 accounting network stop-only group sg3
```

TACACS+ デーモンの設定例

次に、TACACS+ デーモンの設定例を示します。実際に TACACS+ デーモンで使用する正確な構文は、この例の構文と異なる可能性があります。

```
user = mci_customer1 {
 chap = cleartext ”some chap password”
 service = ppp protocol = ip {
inacl#1=”permit ip any any precedence immediate”
inacl#2=”deny igrp 0.0.1.2 255.255.0.0 any”
 }
```

その他の参考資料

ここでは、TACACS+ の設定機能に関する関連資料について説明します。

関連資料

内容	参照先
AAA	*『Cisco IOS Security Guide: Securing User Services』*

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によってサポートされる新しい RFC や変更された RFC はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

TACACS+ の設定に関する機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　TACACS+ の設定に関する機能情報

機能名	リリース	機能情報
TACACS+ の設定	10.0	TACACS+ は、認証および認可プロセスについて詳細なアカウンティング情報と柔軟な管理コントロールを提供します。AAA により TACACS+ が容易になります。また、TACACS+ をイネーブルにするには AAA コマンドを実行する必要があります。 この機能は、Cisco IOS Release 10.0 で導入されました。

TACACS+ の設定に関する機能情報

Per VRF for TACACS+ Servers

Per VRF for TACACS+ Servers 機能により、TACACS+ サーバで Per Virtual Route Forwarding（Per VRF; Per Virtual ルーティングおよび転送）の Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）を設定できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「Per VRF for TACACS+ Servers の機能情報」（P.8）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

Per VRF for TACACS+ Servers の前提条件

- TACACS+ サーバ アクセスが必要です。
- TACACS+、AAA および Per VRF AAA、およびグループ サーバ設定の経験が必要です。

Per VRF for TACACS+ Servers の制約事項

- Per VRF for TACACS+ Servers を設定する前に、VRF インスタンスを指定する必要があります。

Per VRF for TACACS+ Servers について

Per VRF for TACACS+ Servers 機能を設定するには、次の概念を理解しておく必要があります。

- 「Per VRF for TACACS+ Servers の概要」（P.2）

Per VRF for TACACS+ Servers の概要

Per VRF for TACACS+ Servers 機能により、TACACS+ サーバで Per VRF AAA を設定できます。Cisco IOS Release 12.3(7)T よりも前のリリースでは、この機能は、RADIUS サーバ上だけで使用可能でした。

Per VRF for TACACS+ Servers の設定方法

ここでは、次の各手順について説明します。

- 「TACACS+ サーバ上の Per VRF の設定」（P.2）（必須）
- 「Per VRF for TACACS+ Servers の確認」（P.4）（任意）

TACACS+ サーバ上の Per VRF の設定

この手順の最初のステップは、AAA およびサーバ グループの設定、VRF ルーティング テーブルの作成、およびインターフェイスの設定に使用されます。ステップ 10 ～ 13 は、TACACS+ サーバ機能上での Per VRF の設定に使用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **exit**
6. **interface** *interface-name*
7. **ip vrf forwarding** *vrf-name*
8. **ip address** *ip-address mask* [**secondary**]
9. **exit**
10. **aaa group server tacacs+** *group-name*
11. **server-private** {*ip-address* | *name*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*]

12. **ip vrf forwarding** *vrf-name*
13. **ip tacacs source-interface** *subinterface-name*
14. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip vrf** *vrf-name* 例： Router (config)# ip vrf cisco	VRF テーブルを設定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher* 例： Router (config-vrf)# rd 100:1	VRF インスタンスに対するルーティングおよびフォワーディング テーブルを作成します。
ステップ 5	**exit** 例： Router (config-vrf)# exit	VRF コンフィギュレーション モードを終了します。
ステップ 6	**interface** *interface-name* 例： Router (config)# interface Loopback0	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip vrf forwarding** *vrf-name* 例： Router (config-if)# ip vrf forwarding cisco	インターフェイスに VRF を設定します。
ステップ 8	**ip address** *ip-address mask* [**secondary**] 例： Router (config-if)# ip address 10.0.0.2 255.0.0.0	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 9	**exit** 例： Router (config-if)# exit	インターフェイス コンフィギュレーション モードを終了します。
ステップ 10	**aaa group server tacacs+** *group-name* 例： Router (config)# aaa group server tacacs+ tacacs1	異なる TACACS+ サーバ ホストを別々のリストと方式にグループ化し、server-group コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 11	**server-private** {*ip-address* | *name*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*] 例： `Router (config-sg-tacacs+)# server-private 10.1.1.1 port 19 key cisco`	グループ サーバに対するプライベート TACACS+ サーバの IP アドレスを設定します。
ステップ 12	**ip vrf forwarding** *vrf-name* 例： `Router (config-sg-tacacs+)# ip vrf forwarding cisco`	AAA TACACS+ サーバ グループの VRF リファレンスを設定します。
ステップ 13	**ip tacacs source-interface** *subinterface-name* 例： `Router (config-sg-tacacs+)# ip tacacs source-interface Loopback0`	すべての発信 TACACS+ パケットに対して、指定されたインターフェイスの IP アドレスを使用します。
ステップ 14	**exit** 例： `Router (config-sg-tacacs)# exit`	server-group コンフィギュレーション モードを終了します。

Per VRF for TACACS+ Servers の確認

Per VRF TACACS+ 設定を確認するには、次の手順を実行します。

（注） **debug** コマンドは、任意の実行順序で使用できます。

手順の概要

1. **enable**
2. **debug tacacs authentication**
3. **debug tacacs authorization**
4. **debug tacacs accounting**
5. **debug tacacs packets**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**debug tacacs authentication** 例： Router# debug tacacs authentication	AAA/TACACS+ 認証に関する情報を表示します。
ステップ 3	**debug tacacs authorization** 例： Router# debug tacacs authorization	AAA/TACACS+ 認可に関する情報を表示します。
ステップ 4	**debug tacacs accounting** 例： Router# debug tacacs accounting	説明可能なイベントが発生したときに、その情報を表示します。
ステップ 5	**debug tacacs packets** 例： Router# debug tacacs packets	TACACS+ パケットに関する情報を表示します。

Per VRF for TACACS+ Server の設定例

ここでは、次の設定例について説明します。

- 「Per VRF for TACACS+ Servers の設定：例」（P.5）

Per VRF for TACACS+ Servers の設定：例

次の出力例では、Per VRF AAA サービスにグループ サーバ **tacacs1** が設定されています。

```
aaa group server tacacs+ tacacs1
    server-private 10.1.1.1 port 19 key cisco
    ip vrf forwarding cisco
    ip tacacs source-interface Loopback0

  ip vrf cisco
   rd 100:1

  interface Loopback0
   ip address 10.0.0.2 255.0.0.0
   ip vrf forwarding cisco
```

その他の参考資料

ここでは、Per VRF for TACACS+ Servers に関する関連資料について説明します。

関連資料

内容	参照先
TACACS+ の設定	「Configuring TACACS+」モジュール
Per VRF AAA	「Per VRF AAA」モジュール
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能がサポートする新規 RFC または改訂 RFC はありません。また、この機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Per VRF for TACACS+ Servers の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　Per VRF for TACACS+ Servers の機能情報

機能名	リリース	機能情報
Per VRF for TACACS+ Servers	12.3(7)T 12.2(33)SRA1 12.2(33)SXI 12.2(33)SXH4 12.2(54)SG	Per VRF for TACACS+ Servers 機能により、TACACS+ サーバで Per Virtual Route Forwarding（Per VRF; Per Virtual ルーティングおよび転送）の Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）を設定できます。 この機能は、Cisco IOS Release 12.3(7)T で導入されました。 この機能は、Cisco IOS Release 12.2(33)SRA1 に統合されました。 この機能は、Cisco IOS Release 12.2(33)SXI に統合されました。 この機能は、Cisco IOS Release 12.2(33)SXH4 に統合されました。 この機能により、次のコマンドが導入または変更されました。**ip tacacs source-interface**、**ip vrf forwarding**（**server-group**）、**server-private**（**TACACS+**）。

Per VRF for TACACS+ Servers の機能情報

RADIUS および TACACS+ アトリビュート

RADIUS アトリビュート

RADIUS アトリビュート概要と RADIUS IETF アトリビュート

Remote Authentication Dial-In User Service（RADIUS; リモート認証ダイヤルイン ユーザ サービス）アトリビュートは、RADIUS デーモンに保存されたユーザ プロファイル内の特定の Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）要素を定義するために使用されます。このモジュールでは、現在サポートされている RADIUS アトリビュートを列挙します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載された機能に関する情報を探したり、各機能がサポートされているリリースのリストを確認したりするには、P. 20 の「RADIUS アトリビュートの概要と RADIUS IETF アトリビュートの機能情報」を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

RADIUS アトリビュートに関する情報

この項では、RADIUS アトリビュートがクライアントとサーバ間で AAA 情報をどのように交換するかを理解するうえで重要な情報について説明します。次の項で構成されています。

- IETF アトリビュートと VSA の比較
- RADIUS パケットのフォーマット
- RADIUS ファイル
- サポートに関するドキュメント

IETF アトリビュートと VSA の比較

RADIUS Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）アトリビュートは、255 個の標準アトリビュートで構成されるオリジナルのセットで、クライアントとサーバ間での AAA 情報の伝達に使用されます。IETF アトリビュートは標準であるため、アトリビュート データは事前定義されてその内容も認識されています。このため、IETF アトリビュートを介して AAA 情報を交換するすべてのクライアントとサーバは、アトリビュートの厳密な意味や各アトリビュート値の一般的な限界など、アトリビュート データに一致させる必要があります。

RADIUS Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）は、1 つの IETF アトリビュート（Vendor-Specific（アトリビュート 26））から派生したものです。アトリビュート 26 を使用すれば、ベンダーは、追加の 255 個のアトリビュートを自由に作成できます。つまり、ベンダーは、どの IETF アトリビュートのデータとも一致しないアトリビュートを作成して、アトリビュート 26 の背後にカプセル化することができます。そのため、新しく作成されたアトリビュートは、アトリビュート 26 を受け入れているユーザに受け入れられます。

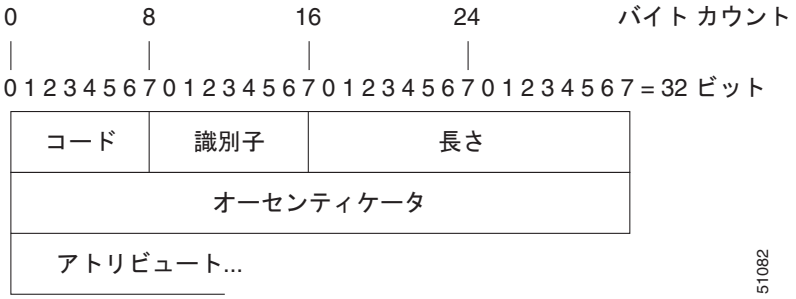
VSA の詳細については、「関連資料」（P.18）を参照してください。

RADIUS パケットのフォーマット

RADIUS サーバと RADIUS クライアント間のデータは、RADIUS パケットで交換されます。データフィールドは左から右に転送されます。

図 1 に、RADIUS パケット内のフィールドを示します。

図 1　RADIUS パケット図



各 RADIUS パケットには、次の情報が含まれています。

- コード：コード フィールドは 1 オクテットです。次の RADIUS パケットのタイプを識別します。
  - Access-Request（1）
  - Access-Accept（2）
  - Access-Reject（3）
  - Accounting-Request（4）

  - Accounting-Response（5）
- 識別子：識別子フィールドは 1 オクテットです。RADIUS サーバの要求と応答の照合を支援し、重複した要求を検出します。
- 長さ：長さフィールドは 2 オクテットです。パケット全体の長さを示します。
- オーセンティケータ：オーセンティケータ フィールドは 16 オクテットです。最上位オクテットが最初に転送されます。RADIUS サーバからの応答の認証に使用されます。次の 2 種類のオーセンティケータがあります。
  - Request-Authentication：Access-Request パケットと Accounting-Request パケットで使用できます。
  - Response-Authenticator：Access-Accept、Access-Reject、Access-Challenge、および Accounting-Response パケットで使用できます。

RADIUS パケット タイプ

次のリストは、アトリビュート情報を含めることが可能なさまざまなタイプの RADIUS パケットをまとめたものです。

Access-Request：クライアントから RADIUS サーバに送信されます。このパケットには、RADIUS サーバで、ユーザにアクセスを許可している特定の Network Access Server（NAS; ネットワーク アクセス サーバ）へのアクセスを許可するかどうかを判断可能な情報が含まれています。認証を実行しているユーザは、Access-Request パケットを提出する*必要があります*。Access-Request パケットを受信した RADIUS サーバは、応答を返す*必要があります*。

Access-Accept：Access-Request パケットを受信した RADIUS サーバは、Access-Request パケット内のすべてのアトリビュート値が受け入れ可能な場合に、Access-Accept パケットを送信する必要があります。Access-Accept パケットには、クライアントからユーザにサービスを提供するために必要な設定情報が含まれています。

Access-Reject：Access-Request パケットを受信した RADIUS サーバは、どのアトリビュート値も受け入れ可能でなかった場合に、Access-Reject パケットを送信する必要があります。

Access-Challenge：Access-Accept パケットを受信した RADIUS サーバは、応答が必要な Access-Challenge パケットをクライアントに送信できます。クライアントで応答の仕方がわからない場合、または、パケットが無効な場合は、RADIUS サーバがそのパケットを破棄します。クライアントがパケットに応答する場合は、オリジナルの Access-Request パケットと一緒に新しい Access-Request パケットを送信する必要があります。

Accounting-Request：クライアントから RADIUS アカウンティング サーバに送信され、アカウンティング情報を提供します。RADIUS サーバが正常に Accounting-Request パケットを記録したら、Accounting-Response パケットを提出する必要があります。

Accounting-Response：RADIUS アカウンティング サーバからクライアントに送信され、Accounting-Request が正常に受信および記録されたことが伝えられます。

RADIUS ファイル

クライアントからサーバに AAA 情報を伝送するためには、RADIUS で使用されるファイルのタイプを理解しておくことが重要です。各ファイルでユーザの認証または認可レベルを定義します。ディレクトリ ファイルでは、ユーザの NAS に実装可能なアトリビュートを定義します。クライアント ファイルでは、RADIUS サーバへの要求が許可されたユーザを定義します。ユーザ ファイルでは、RADIUS サーバでセキュリティ データと設定データに基づいて認証されるユーザ要求を定義します。

- ディレクトリ ファイル

- クライアント ファイル
- ユーザ ファイル

ディレクトリ ファイル

ディレクトリ ファイルには、NAS でサポートされているアトリビュートに依存するアトリビュートのリストが格納されています。ただし、独自のアトリビュートのセットをカスタム ソリューション用のディレクトリに追加できます。このファイルではアトリビュート値が定義されるため、構文解析要求などのアトリビュート出力を解釈できます。ディレクトリ ファイルには次の情報が含まれています。

- 名前：User-Name などのアトリビュートの ASCII 文字列「名」
- ID：アトリビュートの数値「名」。たとえば、User-Name アトリビュートはアトリビュート 1 です。
- 値型：アトリビュートは次の値型のいずれかとして指定できます。
  - abinary：0 ～ 254 オクテット
  - date：ビッグ エンディアン順の 32 ビット値。たとえば、1970 年 1 月 1 日 00:00:00 GMT 以降の秒数。
  - ipaddr：ネットワーク バイト順の 4 オクテット
  - integer：ビッグ エンディアン順の 32 ビット値（上位バイトが先）
  - string：0 ～ 253 オクテット

特定のアトリビュートのデータ型が整数の場合は、オプションで、整数を拡張して何らかの文字列と一致させることができます。次のサンプル辞書には、整数ベースのアトリビュートと対応する値が含まれています。

```
# dictionary sample of integer entry
#
ATTRIBUTE     Service-Type        6                integer
VALUE         Service-Type        Login            1
VALUE         Service-Type        Framed           2
VALUE         Service-Type        Callback-Login   3
VALUE         Service-Type        Callback-Framed  4
VALUE         Service-Type        Outbound         5
VALUE         Service-Type        Administrative   6
VALUE         Service-Type        NAS-Prompt       7
VALUE         Service-Type        Authenticate-Only  8
VALUE         Service-Type        Callback-NAS-Prompt  9
VALUE         Service-Type        Call-Check       10
VALUE         Service-Type        Callback-Administrative  11
```

クライアント ファイル

クライアント ファイルは、RADIUS サーバへの認証要求とアカウンティング要求の送信を許可された RADIUS クライアントのリストが含まれている点で重要です。認証を受けるには、クライアントからサーバに送信された名前と認証キーがクライアント ファイル内のデータと一致する必要があります。

クライアント ファイルの例を次に示します。この例に示すキーは、**radius-server key** *SomeSecret* コマンドと同じにする必要があります。

```
#Client Name        Key
#----------------  ---------------
10.1.2.3:256        test
```

```
nas01               bananas
nas02               MoNkEys
nas07.foo.com       SomeSecret
```

ユーザ ファイル

RADIUS ユーザ ファイルには、RADIUS サーバで認証されたユーザごとのエントリが含まれています。ユーザ プロファイルとも呼ばれるエントリごとに、そのユーザがアクセス可能なアトリビュートが設定されます。

ユーザ プロファイルの最初の行は、常に、「ユーザ アクセス」行です。つまり、サーバはユーザにアクセス許可を出す前に、最初の行のアトリビュートをチェックする必要があります。最初の行にはユーザの名前が含まれています。この名前は、最大 252 文字にすることができ、後ろにユーザのパスワードなどの認証情報が続きます。

ユーザ アクセス行に関連付けられたその他の行は、要求元のクライアントまたはサーバに送信されるアトリビュート応答を表します。応答内で送信されるアトリビュートは、ディレクトリ ファイルで定義する必要があります。

ユーザ ファイルを調べるときは、等号（=）文字の左側のデータがディレクトリ ファイルで定義されたアトリビュートで、等号文字の右側のデータが設定データであることに注意してください。

（注） 空白行はユーザ プロファイルのどの場所にも挿入できません。

RADIUS ユーザ プロファイル（Merit Daemon フォーマット）の例を次に示します。この例では、ユーザ名が cisco.com、パスワードが cisco で、ユーザは 5 つのトンネル アトリビュートにアクセスできます。

```
# This user profile includes RADIUS tunneling attributes
cisco.com  Password="cisco" Service-Type=Outbound
     Tunnel-Type = :1:L2TP
     Tunnel-Medium-Type = :1:IP
     Tunnel-Server-Endpoint = :1:10.0.0.1
     Tunnel-Password = :1:"welcome"
     Tunnel-Assignment-ID = :1:"nas"
```

RADIUS IETF アトリビュート

（注） RADIUS トンネル アトリビュート用の Cisco IOS Release 12.2 では、32 個のタグ付きトンネル セットが L2TP 用にサポートされています。

ここでは、次の各手順について説明します。

- サポートされている RADIUS IETF アトリビュート
- RADIUS アトリビュート解説の包括的リスト

サポートされている RADIUS IETF アトリビュート

表 1 に、シスコがサポートしている IETF RADIUS アトリビュートとそれらが実装されている Cisco IOS リリースを示します。アトリビュートがセキュリティ サーバ固有の形式の場合は、この形式が指定されます。

リスト内のアトリビュートの説明については、表 2 を参照してください。

（注） 特別な（AA）リリースまたは初期開発（T）リリースで実装されたアトリビュートが次のメインライン イメージに追加されています。

表 1　サポートされている RADIUS IETF アトリビュート

番号	IETF アトリビュート	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
1	User-Name	yes	yes	yes	yes	yes	yes	yes	yes
2	User-Password	yes	yes	yes	yes	yes	yes	yes	yes
3	CHAP-Password	yes	yes	yes	yes	yes	yes	yes	yes
4	NAS-IP Address	yes	yes	yes	yes	yes	yes	yes	yes
5	NAS-Port	yes	yes	yes	yes	yes	yes	yes	yes
6	Service-Type	yes	yes	yes	yes	yes	yes	yes	yes
7	Framed-Protocol	yes	yes	yes	yes	yes	yes	yes	yes
8	Framed-IP-Address	yes	yes	yes	yes	yes	yes	yes	yes
9	Framed-IP-Netmask	yes	yes	yes	yes	yes	yes	yes	yes
10	Framed-Routing	yes	yes	yes	yes	yes	yes	yes	yes
11	Filter-Id	yes	yes	yes	yes	yes	yes	yes	yes
12	Framed-MTU	yes	yes	yes	yes	yes	yes	yes	yes
13	Framed-Compression	yes	yes	yes	yes	yes	yes	yes	yes
14	Login-IP-Host	yes	yes	yes	yes	yes	yes	yes	yes
15	Login-Service	yes	yes	yes	yes	yes	yes	yes	yes
16	Login-TCP-Port	yes	yes	yes	yes	yes	yes	yes	yes
18	Reply-Message	yes	yes	yes	yes	yes	yes	yes	yes
19	Callback-Number	no	no	no	no	no	no	yes	yes
20	Callback-ID	no	no	no	no	no	no	no	no
22	Framed-Route	yes	yes	yes	yes	yes	yes	yes	yes
23	Framed-IPX-Network	no	no	no	no	no	no	no	no
24	State	yes	yes	yes	yes	yes	yes	yes	yes
25	Class	yes	yes	yes	yes	yes	yes	yes	yes
26	Vendor-Specific	yes	yes	yes	yes	yes	yes	yes	yes
27	Session-Timeout	yes	yes	yes	yes	yes	yes	yes	yes
28	Idle-Timeout	yes	yes	yes	yes	yes	yes	yes	yes
29	Termination-Action	no	no	no	no	no	no	no	no
30	Called-Station-Id	yes	yes	yes	yes	yes	yes	yes	yes
31	Calling-Station-Id	yes	yes	yes	yes	yes	yes	yes	yes
32	NAS-Identifier	no	no	no	no	no	no	no	yes
33	Proxy-State	no	no	no	no	no	no	no	no
34	Login-LAT-Service	yes	yes	yes	yes	yes	yes	yes	yes
35	Login-LAT-Node	no	no	no	no	no	no	no	yes

表 1　サポートされている RADIUS IETF アトリビュート（続き）

番号	IETF アトリビュート	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
36	Login-LAT-Group	no	no	no	no	no	no	no	no
37	Framed-AppleTalk-Link	no	no	no	no	no	no	no	no
38	Framed-AppleTalk-Network	no	no	no	no	no	no	no	no
39	Framed-AppleTalk-Zone	no	no	no	no	no	no	no	no
40	Acct-Status-Type	yes	yes	yes	yes	yes	yes	yes	yes
41	Acct-Delay-Time	yes	yes	yes	yes	yes	yes	yes	yes
42	Acct-Input-Octets	yes	yes	yes	yes	yes	yes	yes	yes
43	Acct-Output-Octets	yes	yes	yes	yes	yes	yes	yes	yes
44	Acct-Session-Id	yes	yes	yes	yes	yes	yes	yes	yes
45	Acct-Authentic	yes	yes	yes	yes	yes	yes	yes	yes
46	Acct-Session-Time	yes	yes	yes	yes	yes	yes	yes	yes
47	Acct-Input-Packets	yes	yes	yes	yes	yes	yes	yes	yes
48	Acct-Output-Packets	yes	yes	yes	yes	yes	yes	yes	yes
49	Acct-Terminate-Cause	no	no	no	yes	yes	yes	yes	yes
50	Acct-Multi-Session-Id	no	yes	yes	yes	yes	yes	yes	yes
51	Acct-Link-Count	no	yes	yes	yes	yes	yes	yes	yes
52	Acct-Input-Gigawords	no	no	no	no	no	no	no	no
53	Acct-Output-Gigawords	no	no	no	no	no	no	no	no
55	Event-Timestamp	no	no	no	no	no	no	no	yes
60	CHAP-Challenge	yes	yes	yes	yes	yes	yes	yes	yes
61	NAS-Port-Type	yes	yes	yes	yes	yes	yes	yes	yes
62	Port-Limit	yes	yes	yes	yes	yes	yes	yes	yes
63	Login-LAT-Port	no	no	no	no	no	no	no	no
64	Tunnel-Type[1]	no	no	no	no	no	no	yes	yes
65	Tunnel-Medium-Type[1]	no	no	no	no	no	no	yes	yes
66	Tunnel-Client-Endpoint	no	no	no	no	no	no	yes	yes
67	Tunnel-Server-Endpoint[1]	no	no	no	no	no	no	yes	yes
68	Acct-Tunnel-Connection-ID	no	no	no	no	no	no	yes	yes
69	Tunnel-Password[1]	no	no	no	no	no	no	yes	yes
70	ARAP-Password	no	no	no	no	no	no	no	no
71	ARAP-Features	no	no	no	no	no	no	no	no
72	ARAP-Zone-Access	no	no	no	no	no	no	no	no
73	ARAP-Security	no	no	no	no	no	no	no	no
74	ARAP-Security-Data	no	no	no	no	no	no	no	no
75	Password-Retry	no	no	no	no	no	no	no	no
76	Prompt	no	no	no	no	no	no	yes	yes
77	Connect-Info	no	no	no	no	no	no	no	yes

表 1　サポートされている RADIUS IETF アトリビュート（続き）

番号	IETF アトリビュート	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
78	Configuration-Token	no	no	no	no	no	no	no	no
79	EAP-Message	no	no	no	no	no	no	no	no
80	Message-Authenticator	no	no	no	no	no	no	no	no
81	Tunnel-Private-Group-ID	no	no	no	no	no	no	no	no
82	Tunnel-Assignment-ID[1]	no	no	no	no	no	no	yes	yes
83	Tunnel-Preference	no	no	no	no	no	no	no	yes
84	ARAP-Challenge-Response	no	no	no	no	no	no	no	no
85	Acct-Interim-Interval	no	no	no	no	no	no	yes	yes
86	Acct-Tunnel-Packets-Lost	no	no	no	no	no	no	no	no
87	NAS-Port-ID	no	no	no	no	no	no	no	no
88	Framed-Pool	no	no	no	no	no	no	no	no
90	Tunnel-Client-Auth-ID[2]	no	no	no	no	no	no	no	yes
91	Tunnel-Server-Auth-ID	no	no	no	no	no	no	no	yes
200	IETF-Token-Immediate	no	no	no	no	no	no	no	no

1. この RADIUS アトリビュートは、2 つのドラフト IETF 文書、RFC 2868「*RADIUS Attributes for Tunnel Protocol Support*」と RFC 2867「*RADIUS Accounting Modifications for Tunnel Protocol Support*」に基づきます。
2. この RADIUS アトリビュートは RFC 2865 と RFC 2868 に基づきます。

RADIUS アトリビュート解説の包括的リスト

表 2 に、IETF RADIUS アトリビュートとその説明を示します。アトリビュートがセキュリティ サーバ固有の形式の場合は、この形式が指定されます。

表 2　RADIUS IETF アトリビュート

番号	IETF アトリビュート	説明
1	User-Name	RADIUS サーバで認証されるユーザの名前を示します。
2	User-Password	ユーザのパスワードまたは Access-Challenge に続くユーザの入力を示します。16 文字未満のパスワードは、RFC 2865 仕様で暗号化されます。
3	CHAP-Password	Access-Challenge に対する応答で PPP Challenge-Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）ユーザが入力した応答値を示します。
4	NAS-IP Address	認証を要求しているネットワーク アクセス サーバの IP アドレスを示します。デフォルト値は 0.0.0.0/0 です。

表 2　RADIUS IETF アトリビュート（続き）

番号	IETF アトリビュート	説明
5	NAS-Port	ユーザを認証しているネットワーク アクセス サーバの物理ポート番号を示します。NAS-Port 値（32 ビット）は、1 つまたは 2 つの 16 ビット値（**radius-server extended-portnames** コマンドの設定に依存）で構成されます。各 16 ビットの数値は、次のように、解釈用の 5 桁の 10 進整数として表示されるはずです。 非同期端末回線、非同期ネットワーク インターフェイス、および仮想非同期インターフェイスの場合、この値は **00ttt** です。ここで、**ttt** は回線番号または非同期インターフェイス装置番号です。 通常の同期ネットワーク インターフェイスの場合、この値は **10xxx** です。 プライマリ レート ISDN インターフェイス上のチャネルの場合、この値は **2ppcc** です。 基本レート ISDN インターフェイス上のチャネルの場合、この値は **3bb0c** です。 その他のタイプのインターフェイスの場合、この値は **6nnss** です。
6	Service-Type	要求されたサービスのタイプまたは指定されたサービスのタイプを示します。 • 要求内： 既知の PPP または SLIP 接続の場合は Framed。 **enable** コマンドの場合は Administrative-user。 • 応答内： Login：接続を確立します。 Framed：SLIP または PPP を開始します。 Administrative User：EXEC または **enable ok** を開始します。 Exec User：EXEC セッションを開始します。 サービス タイプは、次のような特定の数値で示されます。 • 1：Login • 2：Framed • 3：Callback-Login • 4：Callback-Framed • 5：Outbound • 6：Administrative • 7：NAS-Prompt • 8：Authenticate Only • 9：Callback-NAS-Prompt

表 2　RADIUS IETF アトリビュート（続き）

番号	IETF アトリビュート	説明
7	Framed-Protocol	フレーム化アクセスに使用されるフレーム構成を示します。他のフレーム構成は許可されません。 フレーム構成は次のように数値で指定されます。 • 1 : PPP • 2 : SLIP • 3 : ARA • 4 : Gandalf 独自のシングルリンク / マルチリンク プロトコル • 5 : Xylogics 独自の IPX/SLIP
8	Framed-IP-Address	access-request 内でユーザの IP アドレスを RADIUS サーバに送信することによって、ユーザに対して設定する IP アドレスを示します。このコマンドを有効にするには、グローバル コンフィギュレーション モードで **radius-server attribute 8 include-in-access-req** コマンドを使用します。
9	Framed-IP-Netmask	ユーザがルータまたはネットワークの場合に、ユーザに対して設定する IP ネットマスクを示します。このアトリビュート値によって、指定されたマスクを使用して Framed-IP-Address に静的ルートが追加されることになります。
10	Framed-Routing	ユーザがルータまたはネットワークの場合に、ユーザに対するルーティング方式を示します。このアトリビュートに対しては、「なし」と「送信とリッスン」の値だけがサポートされています。 ルーティング方式は次のように数値で指定されます。 • 0 : なし • 1 : ルーティング パケットの送信 • 2 : ルーティング パケットのリッスン • 3 : ルーティング パケットの送信とリッスン
11	Filter-Id	ユーザのフィルタ リストの名前を示し、%d、%d.in、または %d.out としてフォーマットされます。このアトリビュートは、最近のサービス タイプ コマンドに関連付けられます。ログインと EXEC の場合は、0 ～ 199 の回線アクセス リスト値として %d または %d.out を使用します。フレーム化サービスの場合は、インターフェイス出力アクセス リストとして %d または %d.out を使用し、入力アクセス リストとして %d.in を使用します。この番号は、参照しているプロトコルに対する自己符号化です。
12	Framed-MTU	Maximum Transmission Unit（MTU; 最大伝送ユニット）が PPP またはその他の手段でネゴシエートされない場合に、ユーザに対して設定可能な MTU を示します。
13	Framed-Compression	リンクに使用される圧縮プロトコルを示します。このアトリビュートによって、EXEC 認可中に生成された PPP または SLIP autocommand に「compress」が追加されることになります。非 EXEC 認可には実装されていません。 圧縮プロトコルは次のように数値で指定されます。 • 0 : なし • 1 : VJ-TCP/IP ヘッダー圧縮 • 2 : IPX ヘッダー圧縮
14	Login-IP-Host	Login-Service アトリビュートが含まれている場合に、ユーザが接続するホストを示します（この動作はログイン直後に開始されます）。

表 2　RADIUS IETF アトリビュート（続き）

番号	IETF アトリビュート	説明
15	Login-Service	ユーザをログイン ホストに接続するために使用すべきサービスを示します。 サービスは次のように数値で指定されます。 • 0：Telnet • 1：Rlogin • 2：TCP-Clear • 3：PortMaster • 4：LAT
16	Login-TCP-Port	Login-Service アトリビュートも存在する場合に、ユーザを接続すべき TCP ポートを定義します。
18	Reply-Message	RADIUS サーバ経由でユーザに表示される可能性のあるテキストを示します。このアトリビュートはユーザ ファイルに含めることができますが、プロファイル当たりの Replyp-Message エントリ数を 16 以下にする必要があります。
19	Callback-Number	コールバックに使用するダイヤリング文字列を定義します。
20	Callback-ID	呼び出される場所の名前、つまり、ネットワーク アクセス サーバによって解釈される場所の名前（1 つ以上のオクテットからなる）を定義します。
22	Framed-Route	このネットワーク アクセス サーバ上のユーザに対して設定するルーティング情報を指定します。RADIUS RFC 形式（net/bits [router [metric]]）と従来のドット区切りのマスク（net mask [router [metric]]）がサポートされています。ルータ フィールドを省略するか、0 にした場合は、ピア IP アドレスが使用されます。現在、メトリックは無視されます。このアトリビュートは access-request パケットです。
23	Framed-IPX-Network	ユーザに対して設定される IPX ネットワーク番号を定義します。
24	State	ネットワーク アクセス サーバと RADIUS サーバ間で状態情報の保持を可能にします。このアトリビュートは CHAP チャレンジにしか適用できません。
25	Class	（アカウンティング）RADIUS サーバで入力された場合に、このユーザに関するすべてのアカウンティング パケットにネットワーク アクセス サーバで追加される任意の値。

表 2　RADIUS IETF アトリビュート（続き）

番号	IETF アトリビュート	説明

26	Vendor-Specific	ベンダーに一般使用に適さない独自の拡張アトリビュートの使用を許可します。シスコの RADIUS 実装では、IETF 仕様で推奨される形式を使用したベンダー固有オプションを 1 つサポートしています。シスコのベンダー ID は 9 で、サポートされているオプションは「cisco-avpair」という名前の vendor-type 1 です。この値は次の形式の文字列です。
		`protocol : attribute sep value`
		
		「Protocol」は、特定の認可タイプを表すシスコの「protocol」アトリビュートです。「Attribute」と「value」は、シスコの TACACS+ 仕様で規定されている AV ペアで、「sep」は、必須アトリビュートの場合は「=」で、オプション アトリビュートの場合は「*」です。これにより、TACACS+ 認可で使用できるすべての機能を RADIUS にも使用できるようになります。次に例を示します。
		`cisco-avpair= ”ip:addr-pool=first“`
		`cisco-avpair= ”shell:priv-lvl=15“`
		
		最初の例は、IP 認可中（PPP の IPCP アドレス割り当て中）に、シスコの「複数の名前付き IP アドレス プール」機能をアクティブにします。2 つめの例は、ネットワーク アクセス サーバからのユーザ ログイン直後に EXEC コマンドにアクセスできるようにします。
		表 1 に、サポートされているベンダー固有の RADIUS アトリビュート（IETF アトリビュート 26）を示します。「TACACS+ Attribute-Value Pairs」モジュールに、IETF アトリビュート 26 と一緒に使用可能なサポートされている TACACS+ Attribute-Value（AV）ペアの全リストが記載されています（RFC 2865）。

27	Session-Timeout	セッションを終了する前に、ユーザにサービスを提供する最大秒数を設定します。このアトリビュート値は、ユーザ単位「絶対タイムアウト」になります。
28	Idle-Timeout	セッションが終了する前にユーザに許可されるアイドル接続の最大秒数を設定します。このアトリビュート値は、ユーザ単位「セッション タイムアウト」になります。
29	Termination-Action	終了は次のように数値で指定されます。 • 0：デフォルト • 1：RADIUS 要求
30	Called-Station-Id	（アカウンティング）ネットワーク アクセス サーバから、ユーザが Access-Request パケットの一部として、呼び出した電話番号を送信できるようにします（Dialed Number Identification Service（DNIS; 着信番号識別サービス）または同様のテクノロジー）。このアトリビュートは、ISDN と、PRI と一緒に使用された場合の Cisco AS5200 上のモデム コールに対してのみサポートされます。
31	Calling-Station-Id	（アカウンティング）ネットワーク アクセス サーバから、コールが Access-Request パケットの一部として発信された電話番号を送信できるようにします（自動番号識別または同様のテクノロジー）。このアトリビュートの値は、TACACS+ の「remote-addr」の値と同じです。このアトリビュートは、ISDN と、PRI と一緒に使用された場合の Cisco AS5200 上のモデム コールに対してのみサポートされます。
32	NAS-Identifier	Access-Request を送信したネットワーク アクセス サーバを識別する文字列。 **radius-server attribute 32 include-in-access-req** グローバル コンフィギュレーション コマンドを使用して、Access-Request または Accounting-Request 内で RADIUS アトリビュート 32 を送信します。フォーマットが指定されなかった場合は、デフォルトで、FQDN がアトリビュート内で送信されます。

表 2　RADIUS IETF アトリビュート（続き）

番号	IETF アトリビュート	説明
33	Proxy-State	Access-Request の転送時にプロキシ サーバから別のサーバに送信可能なアトリビュート。このアトリビュートは、Access-Accept、Access-Reject、または Access-Challenge 内でそのまま返され、ネットワーク アクセス サーバに応答が送信される前にプロキシ サーバで削除される必要があります。
34	Login-LAT-Service	ユーザを LAT で接続すべきシステムを示します。このアトリビュートは、EXEC モードでのみ使用できます。
35	Login-LAT-Node	ユーザを自動的に LAT で接続すべきノードを示します。
36	Login-LAT-Group	このユーザの認可に使用される LAT グループ コードを識別します。
37	Framed-AppleTalk-Link	AppleTalk ルータであるユーザへのシリアル リンクに使用すべき別の AppleTalk のネットワーク番号を示します。
38	Framed-AppleTalk-Network	ユーザに AppleTalk ノードを割り当てるためにネットワーク アクセス サーバで使用される AppleTalk ネットワーク番号を示します。
39	Framed-AppleTalk-Zone	このユーザに使用すべき AppleTalk デフォルト ゾーンを示します。
40	Acct-Status-Type	（アカウンティング）この Accounting-Request がユーザ サービスの始まり（開始）または終わり（終了）をマークするかどうかを示します。
41	Acct-Delay-Time	（アカウンティング）クライアントが特定のレコードの送信を試みる秒数を示します。
42	Acct-Input-Octets	（アカウンティング）このサービスの提供中にポートから受信されたオクテット数を示します。
43	Acct-Output-Octets	（アカウンティング）このサービスの配信中にポートに送信されたオクテット数を示します。
44	Acct-Session-Id	（アカウンティング）ログ ファイル内の開始レコードと終了レコードのマッチングを容易にする一意のアカウンティング識別子。Acct-Session ID 番号は、ルータの電源が再投入されるか、ソフトウェアがリロードされるたびに、1 にリセットされます。このアトリビュートを access-request パケット内で送信するには、グローバル コンフィギュレーション モードで **radius-server attribute 44 include-in-access-req** コマンドを使用します。
45	Acct-Authentic	（アカウンティング）ユーザがどのように認証されたか、RADIUS、ネットワーク アクセス サーバ自体、およびその他のリモート認証プロトコルのどれで認証されたかを示します。このアトリビュートは、RADIUS で認証されたユーザの場合は「radius」に、TACACS+ と Kerberos の場合は「remote」に、local、enable、line、および if-needed 方式の場合は「local」に設定されます。その他のすべての方式の場合は、このアトリビュートが省略されます。
46	Acct-Session-Time	（アカウンティング）ユーザがサービスを受信していた時間（秒数）を示します。
47	Acct-Input-Packets	（アカウンティング）このサービスのフレーム化ユーザへの提供中にポートから受信されたパケット数を示します。
48	Acct-Output-Packets	（アカウンティング）このサービスのフレーム化ユーザへの配信中にポートに送信されたパケット数を示します。

表 2　RADIUS IETF アトリビュート（続き）

番号	IETF アトリビュート	説明
49	Acct-Terminate-Cause	（アカウンティング）接続が終了した理由の詳細を報告します。終了の理由は次のように数値で指定されます。 **1.** ユーザ要求 **2.** 搬送波の消失 **3.** サービスの消失 **4.** アイドル タイムアウト **5.** セッション タイムアウト **6.** 管理リセット **7.** 管理リブート **8.** ポート エラー **9.** NAS エラー **10.** NAS 要求 **11.** NAS リブート **12.** ポートの不要化 **13.** ポートの横取り **14.** ポートの保留 **15.** 使用できないサービス **16.** コールバック **17.** ユーザ エラー **18.** ホスト要求 **（注）** アトリビュート 49 に関して、Cisco IOS は 1 ～ 6、9、12、および 15 ～ 18 の値をサポートしています。
50	Acct-Multi-Session-Id	（アカウンティング）ログ ファイル内の複数の関連セッションをリンクするために使用される一意のアカウンティング識別子。 マルチリンク セッション内でリンクされたセッションごとに、一意の Acct-Session-Id 値が割り当てられますが、Acct-Multi-Session-Id は共有されます。
51	Acct-Link-Count	（アカウンティング）アカウンティング レコードが生成された時点で特定のマルチリンク セッション内で認識されていたリンク数を示します。ネットワーク アクセス サーバは、複数のリンクが含まれる任意のアカウンティング要求内にこのアトリビュートを追加できます。
52	Acct-Input-Gigawords	サービスの提供中に Acct-Input-Octets カウンタが一周（2 の 32 乗）した回数を示します。
53	Acct-Output-Gigawords	サービスの配信中に Acct-Output-Octets カウンタが一周（2 の 32 乗）した回数を示します。

表 2　RADIUS IETF アトリビュート（続き）

番号	IETF アトリビュート	説明
55	Event-Timestamp	NAS 上でイベントが発生した時刻を記録します。アトリビュート 55 内で送信されるタイムスタンプは、1970 年 1 月 1 日 00:00 UTC 以降の秒数です。アカウンティングパケット内で RADIUS アトリビュート 55 を送信するには、**radius-server attribute 55 include-in-acct-req** コマンドを使用します。 （注）　アカウンティング パケット内で Event-Timestamp アトリビュートを送信するには、ルータのクロックを設定する*必要があります*（ルータのクロックの設定方法については、『*Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.4T』を参照してください）。 ルータがリロードされるたびにルータのクロックを設定するのを避けるには、**clock calendar-valid** コマンドを有効にします。このコマンドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。
60	CHAP-Challenge	ネットワーク アクセス サーバから PPP CHAP ユーザに送信されたチャレンジ ハンドシェーク認証プロトコル チャレンジが保存されます。
61	NAS-Port-Type	ユーザを認証するためにネットワーク アクセス サーバで使用されている物理ポートのタイプを示します。物理ポートは、次のように数値で示されます。 • 0：非同期 • 1：同期 • 2：ISDN 同期 • 3：ISDN 非同期（V.120） • 4：ISDN 非同期（V.110） • 5：仮想
62	Port-Limit	NAS からユーザに提供される最大ポート数を設定します。
63	Login-LAT-Port	ユーザを LAT で接続すべきポートを定義します。
64	Tunnel-Type[1]	使用されているトンネリング プロトコルを示します。Cisco IOS ソフトウェアは、このアトリビュートに対して L2TP と L2F の 2 つの値をサポートしています。このアトリビュートが設定されていない場合は、L2F がデフォルトとして使用されます。
65	Tunnel-Medium-Type[1]	トンネルの作成に使用される転送メディア タイプを示します。このアトリビュートには、このリリースで使用可能な値（IP）が 1 つしかありません。このアトリビュートに値を設定しなかった場合は、デフォルトとして IP が使用されます。

表 2　RADIUS IETF アトリビュート（続き）

番号	IETF アトリビュート	説明
66	Tunnel-Client-Endpoint	トンネルの開始側端のアドレスが含まれています。Access-Request と Access-Accept の両方のパケットに含めて、新しいトンネルを開始するアドレスを示すこともできます。Tunnel-Client-Endpoint アトリビュートが Access-Request パケットに含まれている場合は、RADIUS サーバがヒントとしてこの値を取得する必要があります。ただし、サーバがこのヒントに従う義務はありません。このアトリビュートは、Accounting-Request パケットに含める*必要があります*。このパケットには、トンネルが開始されたアドレスを示す場合に Start と Stop のどちらかの値を伴う Acct-Status-Type アトリビュートが含まれています。このアトリビュートは、Tunnel-Server-Endpoint アトリビュートや Acct-Tunnel-Connection-ID アトリビュートと一緒に使用して、アカウンティングと監査の目的でトンネルを特定する、グローバルで一意の手段を提供できます。 次のように、このアトリビュートの 127.0.0.X の値を受け入れるためにネットワーク アクセス サーバの機能が拡張されています。 127.0.0.0 は、loopback0 IP アドレスを使用することを示します。 127.0.0.1 は、loopback1 IP アドレスを使用することを示します。 ... 127.0.0.X は、loopbackX IP アドレスを使用することを示します。 実際のトンネル クライアント エンドポイント IP アドレスとして使用されることを示す。この機能拡張によって、複数のネットワーク アクセス サーバ全体のスケーラビリティが向上します。
67	Tunnel-Server-Endpoint[1]	トンネルのサーバ端のアドレスを示します。このアトリビュートのフォーマットは、Tunnel-Medium-Type の値によって異なります。このリリースはトンネル メディア タイプとして IP しかサポートしていないため、このアトリビュートに使用できるのは LNS の IP アドレスまたはホスト名だけです。
68	Acct-Tunnel-Connection-ID	トンネル セッションに割り当てられた識別子を示します。このアトリビュートは、Start、Stop、または上記のいずれかを値として持つ Acct-Status-Type アトリビュートと一緒に Accounting-Request パケットに含める*必要があります*。このアトリビュートは、Tunnel-Client-Endpoint アトリビュートや Tunnel-Server-Endpoint アトリビュートと一緒に使用して、監査の目的でトンネル セッションを一意に特定する手段を提供できます。
69	Tunnel-Password[1]	リモート サーバの認証に使用されるパスワードを定義します。このアトリビュートは、Tunnel-Type の値（AAA_ATTR_l2tp_tunnel_pw (L2TP)、AAA_ATTR_nas_password (L2F)、および AAA_ATTR_gw_password (L2F)）に基づいて、さまざまな AAA アトリビュートに変換されます。 デフォルトで、受信されたすべてのパスワードが暗号化されます。そのため、NAS が暗号化されていないパスワードを復号化しようとすると、認可エラーが発生する可能性があります。アトリビュート 69 で暗号化されていないパスワードの受信を可能にするには、**radius-server attribute 69 clear** グローバル コンフィギュレーション コマンドを使用します。
70	ARAP-Password	ARAP の Framed-Protocol を含む Access-Request パケットを示します。
71	ARAP-Features	NAS から ARAP「feature flags」パケット内のユーザに送信すべきパスワード情報が含まれています。
72	ARAP-Zone-Access	ユーザの ARAP ゾーン リストの使用方法を示します。
73	ARAP-Security	Access-Challenge パケット内で使用すべき ARAP セキュリティ モジュールを示します。

表 2　RADIUS IETF アトリビュート（続き）

番号	IETF アトリビュート	説明
74	ARAP-Security-Data	実際のセキュリティ モジュールのチャレンジまたは応答が含まれています。Access-Challenge パケットと Access-Request パケットの両方に使用できます。
75	Password-Retry	ユーザが切断されるまでに認証を試みることができる回数を示します。
76	Prompt	ユーザの応答をエコーすべきか否かを NAS に指示します（0=エコーなし、1=エコーあり）。
77	Connect-Info	モデム コールに関する追加情報を提供します。このアトリビュートは start と stop のアカウンティング レコード内で生成されます。
78	Configuration-Token	使用すべきユーザ プロファイルのタイプを示します。このアトリビュートは、プロキシに基づく大規模な分散認証ネットワークで使用する必要があります。Access-Accept 内で RADIUS プロキシ サーバから RADIUS プロキシ クライアントに送信されます。NAS には送信しないでください。
79	EAP-Message	Extended Access Protocol（EAP）プロトコルを理解していなくても、NAS で EAP 経由のダイヤルイン ユーザを認証できるように EAP パケットをカプセル化します。
80	Message-Authenticator	CHAP、ARAP、または EAP 認証方式を使用して Access-Requests のスプーフィングを阻止します。
81	Tunnel-Private-Group-ID	特定のトンネル化されたセッションのグループ ID を示します。
82	Tunnel-Assignment-ID[1]	セッションが割り当てられた特定のトンネル イニシエータを示します。
83	Tunnel-Preference	各トンネルに割り当てられた相対プリファレンスを示します。このアトリビュートは、RADIUS サーバからトンネル イニシエータに複数のトンネリング アトリビュートのセットが返される場合に含める必要があります。
84	ARAP-Challenge-Response	ダイヤルイン クライアントのチャレンジに対する応答が含まれています。
85	Acct-Interim-Interval	この特定のセッションの一時更新間隔を秒数で示します。この値は、Access-Accept メッセージにのみ含めることができます。
86	Acct-Tunnel-Packets-Lost	特定のリンク上で失われたパケット数を示します。このアトリビュートは、Tunnel-Link-Stop の値を持つ Acct-Status-Type アトリビュートと一緒に Accounting-Request パケットに含める必要があります。
87	NAS-Port-ID	ユーザを認証している NAS のポートを識別するテキスト文字列が含まれています。
88	Framed-Pool	ユーザにアドレスを割り当てるために使用すべき、割り当て済みのアドレス プールの名前が含まれています。NAS が複数のアドレス プールをサポートしていない場合は、このアトリビュートを無視する必要があります。
90	Tunnel-Client-Auth-ID	トンネル セットアップをトンネル ターミネータで認証するときに、トンネル イニシエータ（NAS とも呼ばれる）で使用される名前を示します。L2F プロトコルと L2TP プロトコルをサポートします。
91	Tunnel-Server-Auth-ID	トンネル セットアップをトンネル イニシエータで認証するときに、トンネル ターミネータ（ホーム ゲートウェイとも呼ばれる）で使用される名前を示します。L2F プロトコルと L2TP プロトコルをサポートします。
200	IETF-Token-Immediate	ファイル エントリがハンドヘルド セキュリティ カード サーバを示しているログイン ユーザから受け取ったパスワードを RADIUS でどのように処理するかを決定します。 このアトリビュートの値は次のように数値で指定されます。 • 0：いいえ、パスワードが無視されることを意味します。 • 1：はい、パスワードが認証に使用されることを意味します。

1. この RADIUS アトリビュートは、2 つのドラフト IETF 文書、RFC 2868「*RADIUS Attributes for Tunnel Protocol Support*」と RFC 2867「*RADIUS Accounting Modifications for Tunnel Protocol Support*」に基づきます。

その他の参考資料

次の項で、RADIUS IETF アトリビュートに関する参考資料を紹介します。

関連資料

内容	参照先
RADIUS	「Configuring RADIUS」モジュール
認証	「Configuring Authentication」モジュール
認可	「Configuring Authorization」モジュール
アカウンティング	「Configuring Accounting」モジュール
RADIUS ベンダー固有アトリビュート	「RADIUS Vendor-Proprietary Attributes」モジュール

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2865	「*Remote Authentication Dial In User Service (RADIUS)*」
RFC 2866	「*RADIUS Accounting*」
RFC 2867	「*RADIUS Accounting Modifications for Tunnel Protocol Support*」
RFC 2868	「*RADIUS Attributes for Tunnel Protocol Support*」
RFC 2869	「*RADIUS Extensions*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

RADIUS アトリビュートの概要と RADIUS IETF アトリビュートの機能情報

表 3 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 3 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 3　RADIUS アトリビュートの概要と RADIUS IETF アトリビュートの機能情報

機能名	リリース	機能情報
RADIUS IETF アトリビュート	Cisco IOS Release 11.1	この機能は、Cisco IOS Release 11.1 で導入されました。

RADIUS ベンダー固有アトリビュート

IETF ドラフト標準には、RADIUS でのネットワーク アクセス サーバと RADIUS サーバ間でベンダー固有情報を通信する方式が規定されています。ただし、ベンダーには固有のアプリケーション向けに拡張した RADIUS アトリビュート セットを持つものがあります。このマニュアルでは、これらベンダー固有 RADIUS アトリビュートの Cisco IOS でのサポート情報について記載します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「RADIUS ベンダー固有アトリビュートの機能情報」（P.13）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

- 「サポートされるベンダー固有 RADIUS アトリビュート」
- 「ベンダー固有 RADIUS アトリビュートの説明に関する包括的なリスト」

サポートされるベンダー固有 RADIUS アトリビュート

表 1 に、シスコがサポートしているベンダー固有 RADIUS アトリビュートおよびこれらを実装している Cisco IOS リリースについて記載しています。アトリビュートがセキュリティ サーバ固有の形式の場合は、この形式が指定されます。説明の一覧については、表 2 を参照してください。

（注） 特別（AA）または初期開発（T）リリースで実装されているアトリビュートは、次の本体イメージに追加されます。

表 1　　サポートされるベンダー固有アトリビュート

番号	ベンダー固有アトリビュート	11.1	11.2	11.3	11.3AA	11.3T	12.0	12.1	12.2	12.3	12.4
17	Change-Password	no	no	yes	yes	yes	yes	yes	yes	no	no
21	Password-Expiration	no	no	yes	yes	yes	yes	yes	yes	no	no
68	Tunnel-ID	no	no	no	no	no	no	no	yes	yes	yes
108	My-Endpoint-Disc-Alias	no	no	no	no	no	no	no	no	no	no
109	My-Name-Alias	no	no	no	no	no	no	no	no	no	no
110	Remote-FW	no	no	no	no	no	no	no	no	no	no
111	Multicast-GLeave-Delay	no	no	no	no	no	no	no	no	no	no
112	CBCP-Enable	no	no	no	no	no	no	no	no	no	no
113	CBCP-Mode	no	no	no	no	no	no	no	no	no	no
114	CBCP-Delay	no	no	no	no	no	no	no	no	no	no
115	CBCP-Trunk-Group	no	no	no	no	no	no	no	no	no	no
116	Appletalk-Route	no	no	no	no	no	no	no	no	no	no
117	Appletalk-Peer-Mode	no	no	no	no	no	no	no	no	no	no
118	Route-Appletalk	no	no	no	no	no	no	no	no	no	no
119	FCP-Parameter	no	no	no	no	no	no	no	no	no	no
120	Modem-PortNo	no	no	no	no	no	no	no	no	no	no
121	Modem-SlotNo	no	no	no	no	no	no	no	no	no	no
122	Modem-ShelfNo	no	no	no	no	no	no	no	no	no	no
123	Call-Attempt-Limit	no	no	no	no	no	no	no	no	no	no
124	Call-Block-Duration	no	no	no	no	no	no	no	no	no	no
125	Maximum-Call-Duration	no	no	no	no	no	no	no	no	no	no
126	Router-Preference	no	no	no	no	no	no	no	no	no	no
127	Tunneling-Protocol	no	no	no	no	no	no	no	no	no	no
128	Shared-Profile-Enable	no	no	no	no	no	no	no	no	yes	yes
129	Primary-Home-Agent	no	no	no	no	no	no	no	no	no	no
130	Secondary-Home-Agent	no	no	no	no	no	no	no	no	no	no
131	Dialout-Allowed	no	no	no	no	no	no	no	no	no	no
133	BACP-Enable	no	no	no	no	no	no	no	no	no	no
134	DHCP-Maximum-Leases	no	no	no	no	no	no	no	no	no	no
135	Primary-DNS-Server	no	no	no	no	yes	yes	yes	yes	yes	yes
136	Secondary-DNS-Server	no	no	no	no	yes	yes	yes	yes	yes	yes
137	Ascend-Client-Assign-DNS	no	no	no	no	no	no	no	no	yes	yes
138	User-Acct-Type	no	no	no	no	no	no	no	no	no	no
139	User-Acct-Host	no	no	no	no	no	no	no	no	no	no
140	User-Acct-Port	no	no	no	no	no	no	no	no	no	no
141	User-Acct-Key	no	no	no	no	no	no	no	no	no	no
142	User-Acct-Base	no	no	no	no	no	no	no	no	no	no
143	User-Acct-Time	no	no	no	no	no	no	no	no	no	no

表 1　サポートされるベンダー固有アトリビュート（続き）

番号	ベンダー固有アトリビュート	11.1	11.2	11.3	11.3AA	11.3T	12.0	12.1	12.2	12.3	12.4
144	Assign-IP-Client	no	no	no	no	no	no	no	no	no	no
145	Assign-IP-Server	no	no	no	no	no	no	no	no	no	no
146	Assign-IP-Global-Pool	no	no	no	no	no	no	no	no	no	no
147	DHCP-Reply	no	no	no	no	no	no	no	no	no	no
148	DHCP-Pool-Number	no	no	no	no	no	no	no	no	no	no
149	Expect-Callback	no	no	no	no	no	no	no	no	no	no
150	Event-Type	no	no	no	no	no	no	no	no	no	no
151	Ascend-Session-Svr-Key	no	no	no	yes	no	no	yes	yes	yes	yes
152	Ascend-Multicast-Rate-Limit	no	no	no	yes	no	no	yes	yes	yes	yes
153	IF-Netmask	no	no	no	no	no	no	no	no	no	no
154	h323-Remote-Address	no	no	no	no	no	no	no	no	yes	yes
155	Ascend-Multicast-Client	no	no	no	yes	no	no	yes	yes	yes	yes
156	FR-Circuit-Name	no	no	no	no	no	no	no	no	no	no
157	FR-LinkUp	no	no	no	no	no	no	no	no	no	no
158	FR-Nailed-Grp	no	no	no	no	no	no	no	no	no	no
159	FR-Type	no	no	no	no	no	no	no	no	no	no
160	FR-Link-Mgt	no	no	no	no	no	no	no	no	no	no
161	FR-N391	no	no	no	no	no	no	no	no	no	no
162	FR-DCE-N392	no	no	no	no	no	no	no	no	no	no
163	FR-DTE-N392	no	no	no	no	no	no	no	no	no	no
164	FR-DCE-N393	no	no	no	no	no	no	no	no	no	no
165	FR-DTE-N393	no	no	no	no	no	no	no	no	no	no
166	FR-T391	no	no	no	no	no	no	no	no	no	no
167	FR-T392	no	no	no	no	no	no	no	no	no	no
168	Bridge-Address	no	no	no	no	no	no	no	no	no	no
169	TS-Idle-Limit	no	no	no	no	no	no	no	no	no	no
170	TS-Idle-Mode	no	no	no	no	no	no	no	no	no	no
171	DBA-Monitor	no	no	no	no	no	no	no	no	no	no
172	Base-Channel-Count	no	no	no	no	no	no	no	no	no	no
173	Minimum-Channels	no	no	no	no	no	no	no	no	no	no
174	IPX-Route	no	no	no	no	no	no	no	no	no	no
175	FT1-Caller	no	no	no	no	no	no	no	no	no	no
176	Ipsec-Backup-Gateway	no	no	no	no	no	no	no	no	yes	yes
177	rm-Call-Type	no	no	no	no	no	no	no	no	yes	yes
178	Group	no	no	no	no	no	no	no	no	no	no
179	FR-DLCI	no	no	no	no	no	no	no	no	no	no
180	FR-Profile-Name	no	no	no	no	no	no	no	no	no	no

表 1　　サポートされるベンダー固有アトリビュート（続き）

番号	ベンダー固有アトリビュート	11.1	11.2	11.3	11.3AA	11.3T	12.0	12.1	12.2	12.3	12.4
181	Ara-PW	no	no	no	no	no	no	no	no	no	no
182	IPX-Node-Addr	no	no	no	no	no	no	no	no	no	no
183	Home-Agent-IP-Addr	no	no	no	no	no	no	no	no	no	no
184	Home-Agent-Password	no	no	no	no	no	no	no	no	no	no
185	Home-Network-Name	no	no	no	no	no	no	no	no	no	no
186	Home-Agent-UDP-Port	no	no	no	no	no	no	no	no	no	no
187	Multilink-ID	no	no	no	yes	yes	yes	yes	yes	yes	yes
188	Ascend-Num-In-Multilink	no	no	no	yes	yes	yes	yes	yes	yes	yes
189	First-Dest	no	no	no	no	no	no	no	no	no	no
190	Pre-Input-Octets	no	no	no	yes	yes	yes	yes	yes	no	no
191	Pre-Output-Octets	no	no	no	yes	yes	yes	yes	yes	no	no
192	Pre-Input-Packets	no	no	no	yes	yes	yes	yes	yes	no	no
193	Pre-Output-Packets	no	no	no	yes	yes	yes	yes	yes	no	no
194	Maximum-Time	no	no	yes	yes	yes	yes	yes	yes	no	no
195	Disconnect-Cause	no	no	yes	yes	yes	yes	yes	yes	yes	yes
196	Connect-Progress	no	no	no	no	no	no	yes	yes	yes	yes
197	Data-Rate	no	no	no	no	yes	yes	yes	yes	yes	yes
198	PreSession-Time	no	no	no	yes	yes	yes	yes	yes	yes	yes
199	Token-Idle	no	no	no	no	no	no	no	no	yes	yes
201	Require-Auth	no	no	no	no	no	no	no	no	yes	yes
202	Number-Sessions	no	no	no	no	no	no	no	no	no	no
203	Authen-Alias	no	no	no	no	no	no	no	no	no	no
204	Token-Expiry	no	no	no	no	no	no	no	no	no	no
205	Menu-Selector	no	no	no	no	no	no	no	no	no	no
206	Menu-Item	no	no	no	no	no	no	no	no	no	no
207	PW-Warntime	no	no	no	no	no	no	no	no	no	no
208	PW-Lifetime	no	no	yes	yes	yes	yes	yes	yes	yes	yes
209	IP-Direct	no	no	no	no	yes	yes	yes	yes	yes	yes
210	PPP-VJ-Slot-Compression	no	no	yes	yes	yes	yes	yes	yes	yes	yes
211	PPP-VJ-1172	no	no	no	no	no	no	no	no	no	no
212	PPP-Async-Map	no	no	no	no	no	no	no	no	no	no
213	Third-Prompt	no	no	no	no	no	no	no	no	no	no
214	Send-Secret	no	no	no	no	no	no	yes	yes	yes	yes
215	Receive-Secret	no	no	no	no	no	no	no	no	no	no
216	IPX-Peer-Mode	no	no	no	no	no	no	no	no	no	no
217	IP-Pool	no	no	yes	yes	yes	yes	yes	yes	yes	yes
218	Static-Addr-Pool	no	no	yes	yes	yes	yes	yes	yes	yes	yes
219	FR-Direct	no	no	no	no	no	no	no	no	no	no

表 1　　サポートされるベンダー固有アトリビュート（続き）

番号	ベンダー固有アトリビュート	11.1	11.2	11.3	11.3AA	11.3T	12.0	12.1	12.2	12.3	12.4
220	FR-Direct-Profile	no	no	no	no	no	no	no	no	no	no
221	FR-Direct-DLCI	no	no	no	no	no	no	no	no	no	no
222	Handle-IPX	no	no	no	no	no	no	no	no	no	no
223	Netware-Timeout	no	no	no	no	no	no	no	no	no	no
224	IPX-Alias	no	no	no	no	no	no	no	no	no	no
225	Metric	no	no	no	no	no	no	no	no	no	no
226	PRI-Number-Type	no	no	no	no	no	no	no	no	no	no
227	Dial-Number	no	no	no	no	no	no	yes	yes	yes	yes
228	Route-IP	no	no	yes	yes	yes	yes	yes	yes	yes	yes
229	Route-IPX	no	no	no	no	no	no	no	no	no	no
230	Bridge	no	no	no	no	no	no	no	no	no	no
231	Send-Auth	no	no	no	no	no	no	yes	yes	yes	yes
232	Send-Passwd	no	no	no	no	no	no	no	no	no	no
233	Link-Compression	no	no	yes	yes	yes	yes	yes	yes	yes	yes
234	Target-Util	no	no	no	yes	no	yes	yes	yes	yes	yes
235	Maximum-Channels	no	no	yes	yes	yes	yes	yes	yes	yes	yes
236	Inc-Channel-Count	no	no	no	no	no	no	no	no	no	no
237	Dec-Channel-Count	no	no	no	no	no	no	no	no	no	no
238	Seconds-of-History	no	no	no	no	no	no	no	no	no	no
239	History-Weigh-Type	no	no	no	no	no	no	no	no	no	no
240	Add-Seconds	no	no	no	no	no	no	no	no	no	no
241	Remove-Seconds	no	no	no	no	no	no	no	no	no	no
242	Data-Filter	no	no	yes	yes	yes	yes	yes	yes	yes	yes
243	Call-Filter	no	no	no	no	no	no	no	no	yes	yes
244	Idle-Limit	no	no	yes	yes	yes	yes	yes	yes	yes	yes
245	Preempt-Limit	no	no	no	no	no	no	no	no	no	no
246	Callback	no	no	no	no	no	no	no	no	yes	yes
247	Data-Service	no	no	no	no	no	no	yes	yes	yes	yes
248	Force-56	no	no	no	no	no	no	yes	yes	yes	yes
249	Billing Number	no	no	no	no	no	no	no	no	no	no
250	Call-By-Call	no	no	no	no	no	no	no	no	no	no
251	Transit-Number	no	no	no	no	no	no	no	no	no	no
252	Host-Info	no	no	no	no	no	no	no	no	no	no
253	PPP-Address	no	no	no	no	no	no	no	no	no	no
254	MPP-Idle-Percent	no	no	no	no	no	no	no	no	no	no
255	Xmit-Rate	no	no	no	yes	yes	yes	yes	yes	yes	yes

ベンダー固有 RADIUS アトリビュートの説明に関する包括的なリスト

表 2 で、次の既存のベンダー固有 RADIUS アトリビュートを一覧で説明しています。

表 2　ベンダー固有 RADIUS アトリビュート

番号	ベンダー固有アトリビュート	説明
17	Change-Password	ユーザのパスワード変更要求を指定します。
21	Password-Expiration	ユーザのファイル エントリのユーザ パスワードの失効日を指定します。
68	Tunnel-ID	（Ascend 5）CLID または DNIS トンネリングを使用する各セッションで、RADIUS により割り当てられるストリングを指定します。アカウンティングが実装されている場合、この値はアカウンティングに使用されます。
108	My-Endpoint-Disc-Alias	（Ascend 5）説明はありません。
109	My-Name-Alias	（Ascend 5）説明はありません。
110	Remote-FW	（Ascend 5）説明はありません。
111	Multicast-GLeave-Delay	（Ascend 5）説明はありません。
112	CBCP-Enable	（Ascend 5）説明はありません。
113	CBCP-Mode	（Ascend 5）説明はありません。
114	CBCP-Delay	（Ascend 5）説明はありません。
115	CBCP-Trunk-Group	（Ascend 5）説明はありません。
116	Appletalk-Route	（Ascend 5）説明はありません。
117	Appletalk-Peer-Mode	（Ascend 5）説明はありません。
118	Route-Appletalk	（Ascend 5）説明はありません。
119	FCP-Parameter	（Ascend 5）説明はありません。
120	Modem-PortNo	（Ascend 5）説明はありません。
121	Modem-SlotNo	（Ascend 5）説明はありません。
122	Modem-ShelfNo	（Ascend 5）説明はありません。
123	Call-Attempt-Limit	（Ascend 5）説明はありません。
124	Call-Block-Duration	（Ascend 5）説明はありません。
125	Maximum-Call-Duration	（Ascend 5）説明はありません。
126	Router-Preference	（Ascend 5）説明はありません。
127	Tunneling-Protocol	（Ascend 5）説明はありません。
128	Shared-Profile-Enable	（Ascend 5）説明はありません。
129	Primary-Home-Agent	（Ascend 5）説明はありません。
130	Secondary-Home-Agent	（Ascend 5）説明はありません。
131	Dialout-Allowed	（Ascend 5）説明はありません。
133	BACP-Enable	（Ascend 5）説明はありません。
134	DHCP-Maximum-Leases	（Ascend 5）説明はありません。

表 2　ベンダー固有 RADIUS アトリビュート（続き）

番号	ベンダー固有アトリビュート	説明
135	Primary-DNS-Server	Microsoft PPP クライアントにより IPCP ネゴシエーション中にネットワーク アクセス サーバから要求される可能性がある、プライマリ DNS サーバを特定します。
136	Secondary-DNS-Server	Microsoft PPP クライアントにより IPCP ネゴシエーション中にネットワーク アクセス サーバから要求される可能性がある、セカンダリ DNS サーバを特定します。
137	Client-Assign-DNS	説明はありません。
138	User-Acct-Type	説明はありません。
139	User-Acct-Host	説明はありません。
140	User-Acct-Port	説明はありません。
141	User-Acct-Key	説明はありません。
142	User-Acct-Base	説明はありません。
143	User-Acct-Time	説明はありません。
144	Assign-IP-Client	説明はありません。
145	Assign-IP-Server	説明はありません。
146	Assign-IP-Global-Pool	説明はありません。
147	DHCP-Reply	説明はありません。
148	DHCP-Pool-Number	説明はありません。
149	Expect-Callback	説明はありません。
150	Event-Type	説明はありません。
151	Session-Svr-Key	説明はありません。
152	Multicast-Rate-Limit	説明はありません。
153	IF-Netmask	説明はありません。
154	Remote-Addr	説明はありません。
155	Multicast-Client	説明はありません。
156	FR-Circuit-Name	説明はありません。
157	FR-LinkUp	説明はありません。
158	FR-Nailed-Grp	説明はありません。
159	FR-Type	説明はありません。
160	FR-Link-Mgt	説明はありません。
161	FR-N391	説明はありません。
162	FR-DCE-N392	説明はありません。
163	FR-DTE-N392	説明はありません。
164	FR-DCE-N393	説明はありません。
165	FR-DTE-N393	説明はありません。
166	FR-T391	説明はありません。
167	FR-T392	説明はありません。
168	Bridge-Address	説明はありません。
169	TS-Idle-Limit	説明はありません。

表 2　ベンダー固有 RADIUS アトリビュート（続き）

番号	ベンダー固有アトリビュート	説明
170	TS-Idle-Mode	説明はありません。
171	DBA-Monitor	説明はありません。
172	Base-Channel-Count	説明はありません。
173	Minimum-Channels	説明はありません。
174	IPX-Route	説明はありません。
175	FT1-Caller	説明はありません。
176	Backup	説明はありません。
177	Call-Type	説明はありません。
178	Group	説明はありません。
179	FR-DLCI	説明はありません。
180	FR-Profile-Name	説明はありません。
181	Ara-PW	説明はありません。
182	IPX-Node-Addr	説明はありません。
183	Home-Agent-IP-Addr	Ascend Tunnel Management Protocol（ATMP）を使用する際に、ホーム エージェントの IP アドレスをドット付き 10 進表記で示します。
184	Home-Agent-Password	ATMP で、外部のエージェントが自身の認証に使用するパスワードを指定します。
185	Home-Network-Name	ATMP で、ホーム エージェントがすべてのパケットを送信する接続プロファイルの名前を示します。
186	Home-Agent-UDP-Port	外部のエージェントが ATMP メッセージをホーム エージェントに送信する際に使用する UDP ポート番号を示します。
187	Multilink-ID	セッションが終了した時のマルチリンク バンドルの ID 番号をレポートします。このアトリビュートは、マルチリンク バンドルの一部のセッションに適用されます。Multilink-ID アトリビュートは、認証応答パケットに送信されます。
188	Num-In-Multilink	アカウンティング終了パケットでレポートされたセッションが終了したときにマルチリンク バンドルに残っているセッション数をレポートします。このアトリビュートは、マルチリンク バンドルの一部のセッションに適用されます。Num-In-Multilink アトリビュートは、認証応答パケットと一部のアカウンティング要求パケットで送信されます。
189	First-Dest	認証後最初に受信したパケットの宛先 IP アドレスを記録します。
190	Pre-Input-Octets	認証前の入力オクテット数を記録します。Pre-Input-Octets アトリビュートは、アカウンティング終了記録で送信されます。
191	Pre-Output-Octets	認証前の出力オクテット数を記録します。Pre-Output-Octets アトリビュートは、アカウンティング終了記録で送信されます。
192	Pre-Input-Packets	認証前の入力パケット数を記録します。Pre-Input-Packets アトリビュートは、アカウンティング終了記録で送信されます。

表 2　ベンダー固有 RADIUS アトリビュート（続き）

番号	ベンダー固有アトリビュート	説明
193	Pre-Output-Packets	認証前の出力パケット数を記録します。Pre-Output-Packets アトリビュートは、アカウンティング終了記録で送信されます。
194	Maximum-Time	任意のセッションで許可される最大時間長を秒で指定します。セッションがこの制限した時間に達すると、接続がドロップします。
195	Disconnect-Cause	接続がオフラインになった理由を特定します。Disconnect-Cause アトリビュートは、アカウンティング終了記録で送信されます。また、このアトリビュートで、認証が実行される前に接続が切断された場合、最初に開始レコードを生成せずに終了レコードが生成されます。詳細については、「Disconnect-Cause アトリビュート値」の表とその意味を参照してください。
196	Connect-Progress	接続が切断される前の接続状態を示します。
197	Data-Rate	接続のライフタイムでの平均ビット/秒値を指定します。Data-Rate アトリビュートは、アカウンティング終了記録で送信されます。
198	PreSession-Time	コールが最初に接続された時から認証が完了した時までの時間長を秒で指定します。PreSession-Time アトリビュートは、アカウンティング終了記録で送信されます。
199	Token-Idle	キャッシュされたトークンが認証間での接続を持続できる最長時間を分で示します。
201	Require-Auth	CLID 認証が行われたクラスで、追加認証が必要かどうかを定義します。
202	Number-Sessions	RADIUS アカウンティング サーバにレポートするクラスごとのアクティブ セッション数を指定します。
203	Authen-Alias	PPP 認証中の RADIUS サーバのログイン名を定義します。
204	Token-Expiry	キャッシュされたトークンのライフタイムを定義します。
205	Menu-Selector	ユーザにデータの入力を指示するために使用するストリングを定義します。
206	Menu-Item	ユーザプロファイルの単一メニュー項目を指定します。プロファイルごとに最大 20 のメニュー項目を割り当てられます。
207	PW-Warntime	（Ascend 5）説明はありません。
208	PW-Lifetime	ユーザ単位ベースで、パスワードの有効日数を指定できます。

表 2　ベンダー固有 RADIUS アトリビュート（続き）

番号	ベンダー固有アトリビュート	説明
209	IP-Direct	このアトリビュートをユーザのファイル エントリに含めると、フレーム ルートがルーティングおよびブリッジング テーブルにインストールされます。 （注）　パケット ルーティングは、この新しくインストールしたエントリだけではなくテーブル全体に依存しています。このアトリビュートを含めても、すべてのパケットが指定の IP アドレスに送信されるとは限りません。したがって、このアトリビュートは、完全にサポートされていません。 このようなアトリビュートの制限は、Cisco ルータが内部ルーティングやブリッジング テーブルを一部しかバイパスできず、指定した IP アドレスにパケットを送信できないために起こります。
210	PPP-VJ-Slot-Comp	VJ 圧縮パケットを PPP リンク経由で送信する際に、Cisco ルータでスロット圧縮しないように指示します。
211	PPP-VJ-1172	PPP で、VJ 圧縮に 0x0037 値を使用するように指示します。
212	PPP-Async-Map	Cisco ルータに、PPP セッション用の非同期制御文字マップを提供します。指定した制御文字は、PPP リンク経由でデータとして渡され、リンク上で起動しているアプリケーションで使用されます。
213	Third-Prompt	ユーザ名とパスワードの次の、ユーザが追加で入力する 3 番めのプロンプトを定義します。
214	Send-Secret	アウトダイヤル パスワードの通常のパスワードの代わりに暗号化パスワードを使用できるようにします。
215	Receive-Secret	暗号化パスワードを RADIUS サーバで検証できるようにします。
216	IPX-Peer-Mode	（Ascend 5）説明はありません。
217	IP-Pool-Definition	アドレスのプールを X a.b.c Z の形式で定義します。ここで、X はプール インデックス番号、a.b.c はプールの開始 IP アドレス、Z はプールの IP アドレス数です。たとえば、3 10.0.0.1 5 は、10.0.0.1 から 10.0.0.5 までをダイナミック割り当てに割り当てます。
218	Assign-IP-Pool	ルータに、ユーザおよび IP アドレスを IP プールから割り当てるよう指示します。
219	FR-Direct	フレーム リレー リダイレクト モードで接続プロファイルを処理するかどうかを定義します。
220	FR-Direct-Profile	この接続をフレーム リレー スイッチまで伝送するフレーム リレー プロファイルの名前を定義します。
221	FR-Direct-DLCI	この接続をフレーム リレー スイッチまで伝送する DLCI を示します。
222	Handle-IPX	NCP のウォッチドッグ要求の処理方法を示します。
223	Netware-Timeout	RADIUS サーバが NCP ウォッチドッグ パケットに応答する時間を分で定義します。

表 2　ベンダー固有 RADIUS アトリビュート（続き）

番号	ベンダー固有アトリビュート	説明
224	IPX-Alias	番号が付いたインターフェイスが必要な IPX ルータでエイリアスを定義できます。
225	Metric	説明はありません。
226	PRI-Number-Type	説明はありません。
227	Dial-Number	ダイヤルする番号を定義します。
228	Route-IP	IP ルーティングがユーザのファイル エントリで許可されているかどうかを示します。
229	Route-IPX	IPX ルーティングをイネーブルにできます。
230	Bridge	説明はありません。
231	Send-Auth	CLID 認証に続く、username-password 認証で使用するプロトコル（PAP または CHAP）を定義します。
232	Send-Passwd	RADIUS サーバで、発信コールの接続のリモート エンドに送信するパスワードを指定できます。
233	Link-Compression	PPP リンクで「stac」圧縮をオンまたはオフのどちらにするか定義します。 リンク圧縮は、次のように、数値で定義します。 • 0：なし • 1：Stac • 2：Stac-Draft-9 • 3：MS-Stac
234	Target-Util	PPP マルチリンクが定義されている場合に、追加チャネルを立ち上げる負荷しきい値を割合で指定します。
235	Maximum-Channels	割り当て済み/割り当て可能な最大チャネル数を指定します。
236	Inc-Channel-Count	説明はありません。
237	Dec-Channel-Count	説明はありません。
238	Seconds-of-History	説明はありません。
239	History-Weigh-Type	説明はありません。
240	Add-Seconds	説明はありません。
241	Remove-Seconds	説明はありません。
242	Data-Filter	ユーザごとの IP データ フィルタを定義します。これらのフィルタは、コールが RADIUS 発信プロファイルを使用して発信された場合か、RADIUS 着信プロファイルを使用して応答した場合にのみ取得されます。最初に一致したフィルタのエントリが適用されます。したがって、フィルタのエントリの入力順が重要です。
243	Call-Filter	ユーザごとの IP データ フィルタを定義します。Cisco ルータでは、このアトリビュートは Data-Filter アトリビュートと同一です。
244	Idle-Limit	セッションがアイドル状態を持続できる最大時間を秒で指定します。セッションがこのアイドル時間に達すると、接続がドロップします。

表 2　ベンダー固有 RADIUS アトリビュート（続き）

番号	ベンダー固有アトリビュート	説明
245	Preempt-Limit	説明はありません。
246	Callback	コールバックをイネーブルまたはディセーブルにできます。
247	Data-Svc	説明はありません。
248	Force-56	チャネルの 64 K すべてが使用可能に見える場合でも、ネットワーク アクセス サーバが 56 K の部分のみを使用するかどうかを指定します。
249	Billing Number	説明はありません。
250	Call-By-Call	説明はありません。
251	Transit-Number	説明はありません。
252	Host-Info	説明はありません。
253	PPP-Address	PPP IPCP ネゴシエーション中に発信ユニットにレポートされた IP アドレスを示します。
254	MPP-Idle-Percent	説明はありません。
255	Xmit-Rate	（Ascend 5）説明はありません。

ベンダー固有 RADIUS アトリビュートの詳細については、「Configuring RADIUS」の章の「Configuring Router for Vendor-Proprietary RADIUS Server Communication」を参照してください。

RADIUS ベンダー固有アトリビュートの機能情報

表 3 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 3 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 3　RADIUS ベンダー固有アトリビュートの機能情報

機能名	リリース	機能情報
RADIUS ベンダー固有アトリビュート	12.2(1)XE	IETF ドラフト標準には、RADIUS でのネットワーク アクセス サーバと RADIUS サーバ間でベンダー固有情報を通信する方式が規定されています。ただし、ベンダーには固有のアプリケーション向けに拡張した RADIUS アトリビュート セットを持つものがあります。このマニュアルでは、これらベンダー固有 RADIUS アトリビュートの Cisco IOS でのサポート情報について記載します。 この機能は、12.2(1) XE で初めて導入されました。

RADIUS ベンダー固有アトリビュートの機能情報

RADIUS ベンダー固有アトリビュート（VSA）および RADIUS Disconnect-Cause アトリビュート値

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）ドラフト標準には、ネットワーク アクセス サーバと RADIUS サーバの間で VSA（Vendor-Specific Attribute; ベンダー固有アトリビュート）（アトリビュート 26）を使用してベンダー固有の情報を伝達する方法が規定されています。アトリビュート 26 はベンダー固有アトリビュートをカプセル化します。このため、ベンダーは一般的な用途に適さない独自の拡張アトリビュートをサポートできます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「RADIUS ベンダー固有アトリビュート（VSA）および RADIUS Disconnect-Cause アトリビュート値の機能情報」（P.14）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

RADIUS ベンダー固有アトリビュート（VSA）および RADIUS Disconnect-Cause アトリビュート値について

シスコの RADIUS 実装では、IETF 仕様で推奨される形式を使用したベンダー固有オプションを 1 つサポートしています。シスコのベンダー ID は 9 で、サポートするオプションはベンダー タイプ 1、名前は「cisco-av-pair」です。値は次の形式のストリングです。

```
protocol : attribute sep value *
```

「Protocol」は、特定の認可タイプを表すシスコの「protocol」アトリビュートです。使用可能なプロトコルには、IP、IPX、VPDN、VOIP、SHELL、RSVP、SIP、AIRNET、OUTBOUND があります。「Attribute」と「value」は、シスコの TACACS+ 仕様に定義されている適切なアトリビュート値（AV）ペアで、「sep」は必須アトリビュートの場合には「=」、オプションのアトリビュートの場合に「*」を使用します。これにより、TACACS+ 認可で使用できるすべての機能を RADIUS にも使用できるようになります。

たとえば、次の AV ペアにより、IP を認可している間（PPP の IPCP アドレス割り当てを行っている間）、シスコの「指定された複数の IP アドレス プール」をアクティブにすることができます。

```
cisco-avpair= ”ip:addr-pool=first”
```

「*」を挿入すると、AV ペア「ip:addr-pool=first」はオプションになります。AV ペアはオプションにできることに注意してください。

```
cisco-avpair= ”ip:addr-pool*first”
```

次に、ネットワーク アクセス サーバからユーザがログインしたときに、すぐに EXEC コマンドを実行する方法の例を示します。

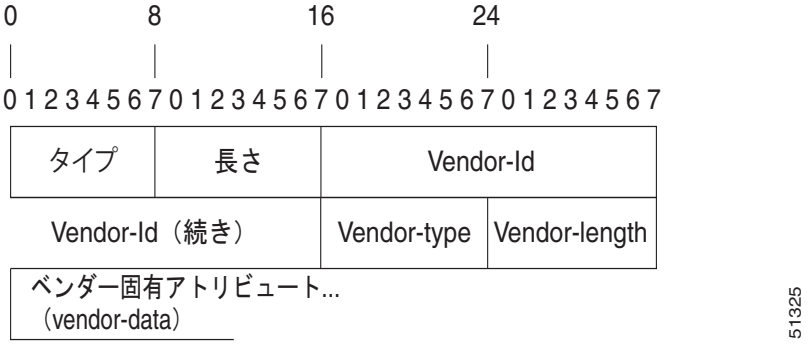
```
cisco-avpair= ”shell:priv-lvl=15”
```

アトリビュート 26 には、次の 3 つの要素が含まれています。

- タイプ
- 長さ
- ストリング（またはデータ）
  - Vendor-Id
  - Vendor-Type
  - Vendor-Length
  - Vendor-Data

図 1 に、アトリビュート 26 の「背後で」カプセル化される VSA のパケット形式を示します。

図 1　アトリビュート 26 の背後でカプセル化される VSA



（注）　VSA の形式はベンダーが指定します。Attribute-Specific フィールド（Vendor-Data とも呼ばれる）は、ベンダーによるそのアトリビュートの定義によって異なります。

表 2 に、サポートされるベンダー固有 RADIUS アトリビュートを示します（IETF アトリビュート 26）。表 1 で、表 2 に示される重要なフィールドについて説明します。

表 1　ベンダー固有アトリビュート テーブル フィールドの説明

フィールド	説明
Number	次の表に示されるすべてのアトリビュートは、IETF アトリビュート 26 の拡張です。
Vendor-Specific Command Codes	特定のベンダーの識別に使用する定義されたコード。コード 9 は Cisco VSA、311 は Microsoft VSA、529 は Ascend VSA を定義します。
Sub-Type Number	アトリビュート ID 番号。この番号は、アトリビュート 26 の背後でカプセル化される「2 番めのレイヤ」の ID 番号である以外は、IETF アトリビュートの ID 番号に似ています。
Attribute	アトリビュートの ASCII ストリング名。
Description	アトリビュートの説明。

表 2　ベンダー固有 RADIUS IETF アトリビュート

番号	ベンダー固有会社コード	Sub-Type 番号	アトリビュート	説明
MS-CHAP アトリビュート				
26	311	1	MSCHAP-Response	PPP MS-CHAP ユーザがチャレンジに対する応答で提供するレスポンス値が含まれます。Access-Request パケットでのみ使用されます。このアトリビュートは、PPP CHAP ID と同じです（RFC 2548）。
26	311	11	MSCHAP-Challenge	ネットワーク アクセス サーバが MS-CHAP ユーザに送信するチャレンジが含まれます。Access-Request パケットと Access-Challenge パケットの両方に使用できます（RFC 2548）。
VPDN アトリビュート				
26	9	1	l2tp-cm-local-window-size	L2TP 制御メッセージの最大受信ウィンドウ サイズを指定します。この値は、トンネルの確立中にピアにアドバタイズされます。

表 2　ベンダー固有 RADIUS IETF アトリビュート（続き）

番号	ベンダー固有会社コード	Sub-Type 番号	アトリビュート	説明
26	9	1	l2tp-drop-out-of-order	正しくない順序で受信したデータ パケットをドロップして、シーケンス番号を順守します。これは受信した場合の処理方法であって、データ パケット上でシーケンス番号が送信されるわけではありません。
26	9	1	l2tp-hello-interval	hello キープアライブ インターバルの秒数を指定します。ここで指定した秒数、トンネルでデータが送信されないと、hello パケットが送信されます。
26	9	1	l2tp-hidden-avp	イネーブルにすると、L2TP 制御メッセージで、大文字小文字を区別する AVP にスクランブルがかけられるか、または非表示になります。
26	9	1	l2tp-nosession-timeout	タイムアウトおよびシャットダウンまでに、セッションなしでトンネルがアクティブのままになる秒数を指定します。
26	9	1	tunnel-tos-reflect	LNS でトンネルに入るパケットに対して、IP ToS フィールドを各ペイロード パケットの IP ヘッダーからトンネル パケットの IP ヘッダーにコピーします。
26	9	1	l2tp-tunnel-authen	このアトリビュートを設定すると、L2TP トンネル認証が実行されます。
26	9	1	l2tp-tunnel-password	L2TP トンネル認証および AVP 隠蔽に使用される共有秘密。
26	9	1	l2tp-udp-checksum	これは認可アトリビュートで、L2TP がデータ パケットに対して UDP チェックサムを実行する必要があるかどうかを定義します。有効な値は「yes」と「no」です。デフォルトは no です。
Store and Forward Fax アトリビュート				
26	9	3	Fax-Account-Id-Origin	アカウント ID の発信元を **mmoip aaa receive-id** コマンドまたは **mmoip aaa send-id** コマンドに対して、システム管理者によって定義されたものとして示します。
26	9	4	Fax-Msg-Id=	Store and Forward Fax 機能によって割り当てられた一意のファクス メッセージ識別番号を示します。
26	9	5	Fax-Pages	このファクス セッション中に送信または受信したページ数を示します。このページ数には、カバー ページも含まれます。
26	9	6	Fax-Coverpage-Flag	カバー ページがこのファクス セッションのオフランプ ゲートウェイで生成されたかどうかを示します。true はカバー ページが生成されたことを示します。false はカバー ページが生成されなかったことを意味します。
26	9	7	Fax-Modem-Time	モデムがファクス データを送信した時間（x）、およびファクス セッションの合計時間（y）を秒単位で示します。これには、fax-mail および PSTN 時間が x/y の形式で含まれます。たとえば、10/15 は送信時間が 10 秒で、合計ファクス セッションが 15 秒であったことを示します。

表 2　ベンダー固有 RADIUS IETF アトリビュート（続き）

番号	ベンダー固有会社コード	Sub-Type 番号	アトリビュート	説明
26	9	8	Fax-Connect-Speed	この fax-mail が最初に送信または受信された時点のモデム速度を示します。有効値は、1200、4800、9600、および 14400 です。
26	9	9	Fax-Recipient-Count	このファクス送信の受信者数を示します。E メール サーバがセッション モードをサポートするまで、この数字は 1 にする必要があります。
26	9	10	Fax-Process-Abort-Flag	ファクス セッションが中断したこと、または正常に終了したことを示します。true はセッションが中断したことを示します。false はセッションが成功したことを示します。
26	9	11	Fax-Dsn-Address	DSN の送信先のアドレスを示します。
26	9	12	Fax-Dsn-Flag	DSN がイネーブルにされているかどうかを示します。true は DSN がイネーブルにされていることを示します。false は DSN がイネーブルにされていないことを示します。
26	9	13	Fax-Mdn-Address	MDN の送信先のアドレスを示します。
26	9	14	Fax-Mdn-Flag	Message Delivery Notification（MDN; メッセージ配信通知）がイネーブルにされているかどうかを示します。true は MDN がイネーブルにされていることを示します。false は MDN がイネーブルにされていないことを示します。
26	9	15	Fax-Auth-Status	このファクス セッションに対する認証が成功したかどうかを示します。このフィールドに対する有効値は、success、failed、bypassed、または unknown です。
26	9	16	Email-Server-Address	オンランプ fax-mail メッセージを処理する E メール サーバの IP アドレスを示します。
26	9	17	Email-Server-Ack-Flag	オンランプ ゲートウェイが fax-mail メッセージを受け入れる E メール サーバから肯定確認応答を受信したことを示します。
26	9	18	Gateway-Id	ファクス セッションを処理したゲートウェイの名前を示します。名前は、hostname.domain-name という形式で表示されます。
26	9	19	Call-Type	ファクスのアクティビティのタイプを、fax receive または fax send のどちらかで記述します。
26	9	20	Port-Used	この fax-mail の送受信いずれかに使用される Cisco AS5300 のスロット/ポート番号を示します。
26	9	21	Abort-Cause	ファクス セッションが中断した場合、中断の信号を送信したシステム コンポーネントを示します。中断する可能性のあるシステム コンポーネントには、FAP（Fax Application Process）、TIFF（TIFF リーダーまたは TIFF ライター）、fax-mail クライアント、fax-mail サーバ、ESMTP クライアント、ESMTP サーバなどがあります。

H323 アトリビュート

表 2　ベンダー固有 RADIUS IETF アトリビュート（続き）

番号	ベンダー固有会社コード	Sub-Type 番号	アトリビュート	説明
26	9	23	Remote-Gateway-ID （h323-remote-address）	リモート ゲートウェイの IP アドレスを示します。
26	9	24	Connection-ID （h323-conf-id）	会議 ID を識別します。
26	9	25	Setup-Time （h323-setup-time）	以前、Greenwich Mean Time（GMT; グリニッジ標準時）およびズール タイムと呼ばれていた Coordinated Universal Time（UTC; 協定世界時）でのこの接続のセットアップ時間を示します。
26	9	26	Call-Origin （h323-call-origin）	ゲートウェイに対するコールの発行元を示します。有効値は、originating および terminating です（回答）。
26	9	27	Call-Type （h323-call-type）	コールのレグ タイプを示します。有効値は、**telephony** および **VoIP** です。
26	9	28	Connect-Time （h323-connect-time）	このコール レグの UTC での接続時間を示します。
26	9	29	Disconnect-Time （h323-disconnect-time）	このコール レグが UTC で接続解除された時間を示します。
26	9	30	Disconnect-Cause （h323-disconnect-cause）	Q.931 仕様によって、接続がオフラインにされた理由を示します。
26	9	31	Voice-Quality （h323-voice-quality）	コールの音声品質に影響する Impairment Factor（ICPIF）を指定します。
26	9	33	Gateway-ID （h323-gw-id）	下位のゲートウェイの名前を示します。
大規模のダイヤルアウト アトリビュート				
26	9	1	callback-dialstring	コールバックに使用するダイヤリング文字列を定義します。
26	9	1	data-service	説明はありません。
26	9	1	dial-number	ダイヤルする番号を定義します。
26	9	1	force-56	チャネルの 64 K すべてが使用可能に見える場合でも、ネットワーク アクセス サーバが 56 K の部分のみを使用するかどうかを指定します。
26	9	1	map-class	ユーザ プロファイルに、ダイヤルアウトするネットワーク アクセス サーバ上で同じ名前のマップ クラスで設定される情報の参照を許可します。
26	9	1	send-auth	CLID 認証に続く、username-password 認証で使用するプロトコル（PAP または CHAP）を定義します。

表 2　ベンダー固有 RADIUS IETF アトリビュート（続き）

番号	ベンダー固有会社コード	Sub-Type 番号	アトリビュート	説明
26	9	1	send-name	PPP 名前認証。PAP に適用する場合は、インターフェイス上で **ppp pap sent-name password** コマンドを設定しないでください。PAP の場合は、アウトバウンド認証の PAP ユーザ名および PAP パスワードとして、「preauth:send-name」および「preauth:send-secret」が使用されます。CHAP の場合、「preauth:send-name」はアウトバウンド認証だけでなく、インバウンド認証にも使用されます。CHAP インバウンドの場合、NAS は発信元のボックスへのチャレンジ パケットで「preauth:send-name」に定義された名前を使用します。 （注）　send-name アトリビュートは時間の経過とともに変わっています。最初は、現在 send-name および remote-name アトリビュートの両方で提供されている機能を実行していました。remote-name アトリビュートが追加されたため、send-name アトリビュートは現在の動作に制限されています。
26	9	1	send-secret	PPP パスワード認証。Vendor-Specific Attributes（VSA; ベンダー固有アトリビュート）の場合は、アウトバウンド認証の PAP ユーザ名および PAP パスワードとして、「preauth:send-name」および「preauth:send-secret」が使用されます。CHAP アウトバウンドの場合、「preauth:send-name」と「preauth:send-secret」の両方が応答パケットに使用されます。
26	9	1	remote-name	大規模のダイヤルアウトで使用するリモート ホストの名前を提供します。ダイヤラは、大規模のダイヤルアウトのリモート名が認証された名前と一致することを確認し、偶発的なユーザ RADIUS 設定ミスから保護します（たとえば、有効な電話番号にダイヤルして、間違ったルータに接続するなど）。
その他のアトリビュート				
26	9	2	Cisco-NAS-Port	NAS-Port アカウンティングに追加的な Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）を指定します。Attribute-Value Pair（AVPair; アトリビュート値ペア）の形式で追加的な NAS-Port 情報を指定するには、**radius-server vsa send** グローバル コンフィギュレーション コマンドを使用します。 （注）　この VSA は、通常アカウンティングで使用されますが認証（Access-Request）パケットで使用される場合もあります。
26	9	1	min-links	MLP に対するリンクの最小数を設定します。

表 2　ベンダー固有 RADIUS IETF アトリビュート（続き）

番号	ベンダー固有会社コード	Sub-Type 番号	アトリビュート	説明
26	9	1	proxyacl#<n>	ダウンロード可能なユーザ プロファイル（ダイナミック ACL）を、認証プロキシを使用して設定でき、これにより設定されたインターフェイスのトラフィックの通過を許可するよう、認証を設定できます。
26	9	1	spi	登録中にホーム エージェントがモバイル ノードの認証で必要とする認証情報を伝送します。この情報は、**ip mobile secure host <addr>** コンフィギュレーション コマンドと同じ構文です。基本的に、この文字列に続く残りのコンフィギュレーション コマンドはそのまま含まれます。これには Security Parameter Index（SPI; セキュリティ パラメータ インデックス）、キー、認証アルゴリズム、認証モード、およびリプレイ保護タイムスタンプ範囲が含まれています。

NAS による VSA の認識と使用の設定の詳細については、「Configuring RADIUS」モジュールの「Configuring Router to Use Vendor-Specific RADIUS Attributes」を参照してください。

RADIUS Disconnect-Cause アトリビュート値

Disconnect-cause アトリビュート値は、接続がオフラインにされた理由を指定します。アトリビュート値は、Accounting 要求パケットで送信されます。セッションの認証が失敗しても、これらの値は、セッションの終了時に送信されます。セッションが認証されないと、アトリビュートが開始レコードを生成せずに終了レコードを発生させる可能性があります。

表 3 に、Disconnect-Cause（195）アトリビュートの原因コード、値、および 説明を示します。

（注）　Disconnect-Cause は、RADIUS AVPairs で使用されるごとに 1000 ずつ増分されます。たとえば、disc-cause 4 は 1004 になります。

表 3　Disconnect-Cause アトリビュート値

原因コード	値	説明
0	No-Reason	接続解除の理由は提供されない。
1	No-Disconnect	イベントは接続解除されていない。
2	Unknown	理由は不明。
3	Call-Disconnect	コールが接続解除された。
4	CLID-Authentication-Failure	calling-party 数の認証の失敗。
9	No-Modem-Available	コールへの接続にモデムが使用できない。
10	No-Carrier	キャリアが検出されない。 （注）　最初のモデム接続中に接続解除があると、コード 10、11、および 12 が送信される場合があります。

表 3　Disconnect-Cause アトリビュート値（続き）

原因コード	値	説明
11	Lost-Carrier	キャリアの喪失。
12	No-Detected-Result-Codes	モデム結果コード検出の失敗。
20	User-Ends-Session	ユーザがセッションを終了した。 （注）　コード 20、22、23、24、25、26、27、および 28 は、EXEC セッションに適用されます。
21	Idle-Timeout	ユーザ入力待機中のタイムアウト。 コード 21、100、101、102、および 120 は、すべてのセッション タイプに適用されます。
22	Exit-Telnet-Session	既存の Telnet セッションによる接続解除。
23	No-Remote-IP-Addr	SLIP/PPP への切り替え不能。リモート エンドに IP アドレスがない。
24	Exit-Raw-TCP	既存の raw TCP による接続解除。
25	Password-Fail	間違ったパスワード。
26	Raw-TCP-Disabled	Raw TCP がディセーブルにされた。
27	Control-C-Detected	Control-C が検出された。
28	EXEC-Process-Destroyed	EXEC プロセスが破棄された。
29	Close-Virtual-Connection	ユーザが仮想接続を終了した。
30	End-Virtual-Connection	仮想接続が終了した。
31	Exit-Rlogin	ユーザが Rlogin を終了した。
32	Invalid-Rlogin-Option	無効な Rlogin オプションが選択された。
33	Insufficient-Resources	不十分なリソース。
40	Timeout-PPP-LCP	PPP LCP ネゴシエーションがタイムアウトした。 （注）　コード 40 ～ 49 が PPP セッションに適用されます。
41	Failed-PPP-LCP-Negotiation	PPP LCP ネゴシエーションが失敗した。
42	Failed-PPP-PAP-Auth-Fail	PPP PAP 認証が失敗した。
43	Failed-PPP-CHAP-Auth	PPP CHAP 認証が失敗した。
44	Failed-PPP-Remote-Auth	PPP リモート認証が失敗した。
45	PPP-Remote-Terminate	PPP がリモート エンドから Terminate Request を受信した。
46	PPP-Closed-Event	上位層がセッションの終了を要求した。
47	NCP-Closed-PPP	開いている NCP がなかったため、PPP セッションが終了した。
48	MP-Error-PPP	MP エラーのため、PPP セッションが終了した。
49	PPP-Maximum-Channels	最大チャネルに達したため、PPP セッションが終了した。
50	Tables-Full	ターミナル サーバ テーブルがいっぱいになったため、接続解除された。
51	Resources-Full	内部リソースがいっぱいになったため、接続解除された。
52	Invalid-IP-Address	Telnet ホストに対する IP アドレスが有効でない。
53	Bad-Hostname	ホスト名が検証されていない。
54	Bad-Port	ポート番号が無効または欠落している。

表 3　Disconnect-Cause アトリビュート値（続き）

原因コード	値	説明
60	Reset-TCP	TCP 接続がリセットされた。 （注）　コード 60 ～ 67 は Telnet または raw TCP セッションに適用されます。
61	TCP-Connection-Refused	TCP 接続がホストによって拒否された。
62	Timeout-TCP	TCP 接続がタイムアウトした。
63	Foreign-Host-Close-TCP	TCP 接続が終了した。
64	TCP-Network-Unreachable	TCP ネットワークに到達できない。
65	TCP-Host-Unreachable	TCP ホストに到達できない。
66	TCP-Network-Admin Unreachable	管理上の理由により、TCP ネットワークに到達できない。
67	TCP-Port-Unreachable	TCP ポートに到達できない。
100	Session-Timeout	セッションがタイムアウトした。
101	Session-Failed-Security	セキュリティ上の理由から、セッションが失敗した。
102	Session-End-Callback	コールバックにより、セッションが終了した。
120	Invalid-Protocol	検出されたプロトコルがディセーブルにされていたため、コールが拒否された。
150	RADIUS-Disconnect	RADIUS 要求による接続解除。
151	Local-Admin-Disconnect	管理上の接続解除。
152	SNMP-Disconnect	SNMP 要求による接続解除。
160	V110-Retries	許可された V.110 リトライを超過した。
170	PPP-Authentication-Timeout	PPP 認証がタイムアウトした。
180	Local-Hangup	ローカルのハングアップによって接続解除された。
185	Remote-Hangup	リモート エンドのハングアップよって接続解除された。
190	T1-Quiesced	T1 回線が休止状態のため接続解除された。
195	Call-Duration	コールの最大継続時間を超過したため、接続解除された。
600	VPN-User-Disconnect	クライアントによってコールが接続解除された（PPP 経由）。 LNS がクライアントから PPP terminate request を受信するとコードが送信されます。
601	VPN-Carrier-Loss	キャリアの喪失。これは回線が物理的に普通になった結果である場合があります。 クライアントがダイヤラを使用してダイヤルアウトできない場合、コードが送信されます。
602	VPN-No-Resources	コールの処理に使用できるリソースがない。 クライアントがメモリを割り当てることができない場合、コードが送信されます（メモリの不足）。

表 3　Disconnect-Cause アトリビュート値（続き）

原因コード	値	説明
603	VPN-Bad-Control-Packet	L2TP または L2F 制御パケットが間違っている。 このコードは、必須の Attribute-Value Pairs（AVP; アトリビュート値ペア）が欠落しているなど、ピアから受信した制御パケットが無効な場合に送信されます。L2TP を使用すると、コードは 6 回の再送信後に送信されます。L2F を使用すると、再送信の回数はユーザ設定が可能です。 **（注）**　トンネルにアクティブなセッションがある場合は、VPN-Tunnel-Shut が送信されます。
604	VPN-Admin-Disconnect	管理上の接続解除。これは、VPN ソフト シャットダウンの結果である場合があります。これは、クライアントが最大セッション制限に達するか、最大ホップカウントを超過した場合に発生します。 トンネルが、**clear vpdn tunnel** コマンドの発行によってダウンした場合に、コードが送信されます。
605	VPN-Tunnel-Shut	トンネルのティアダウン、またはトンネルのセットアップが失敗した。 トンネルにアクティブなセッションがあり、トンネルがダウンした場合にコードが送信されます。 **（注）**　このコードはトンネルの認証が失敗した場合は、送信*されません。*
606	VPN-Local-Disconnect	LNS PPP モジュールによって、コールが接続解除された。 LNS がクライアントに PPP terminate request を送信するとコードが送信されます。これは通常の PPP 接続解除が LNS によって開始されたことを示します。
607	VPN-Session-Limit	VPN ソフト シャットダウンがイネーブルになった。 前述したソフト シャットダウンの制約事項のいずれかによってコールが拒否されると、コードが送信されます。
608	VPN-Call-Redirect	VPN コール リダイレクトがイネーブルになった。

Q.850 原因コードと説明については、『*Cisco IOS Voice Troubleshooting and Monitoring Guide*, Release 12.4T』を参照してください。

その他の参考資料

ここでは、RADIUS Vendor-Specific Attributes（VSA; ベンダー固有アトリビュート）および RADIUS Disconnect-Cause アトリビュート値に関する関連資料について説明します。

関連資料

内容	参照先
セキュリティ機能	『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 15.0』
セキュリティ サーバ プロトコル	
RADIUS の設定	「Configuring RADIUS」モジュール

規格

規格	タイトル
Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）インターネット ドラフト：Network Access Servers Requirements	「*Network Access Servers Requirements: Extended RADIUS Practices*」

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2865	「*Remote Authentication Dial In User Service (RADIUS)*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

RADIUS ベンダー固有アトリビュート（VSA）および RADIUS Disconnect-Cause アトリビュート値の機能情報

表 4 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 4 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 4　RADIUS Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）および RADIUS Disconnect-Cause アトリビュート値の機能情報

機能名	リリース	機能情報
RADIUS Vendor-Specific Attributes（VSA; ベンダー固有アトリビュート）および RADIUS Disconnect-Cause アトリビュート値	12.0(30)S3s 12.3(11)YS1 12.2(33)SRC	このマニュアルは、ネットワーク アクセス サーバと RADIUS サーバの間でベンダー固有アトリビュート（アトリビュート 26）を使用してベンダー固有の情報を伝達する方法を規定する Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）ドラフト標準を扱います。アトリビュート 26 はベンダー固有アトリビュートをカプセル化します。このため、ベンダーは一般的な用途に適さない独自の拡張アトリビュートをサポートできます。 この機能は、Cisco IOS Release 12.0(30)S3s で導入されました。 この機能は、Cisco IOS Release 12.3(11)YS1 に統合されました。 この機能は、Cisco IOS Release 12.2(33)SRC に統合されました。

RADIUS ベンダー固有アトリビュート（VSA）および RADIUS Disconnect-Cause アトリビュート値の機能情報

アクセス要求内の RADIUS アトリビュート 8（Framed-IP-Address）

アクセス要求内の RADIUS アトリビュート 8（Framed-IP-Address）機能は、Network Access Server（NAS; ネットワーク アクセス サーバ）から RADIUS サーバに、ユーザ認証に先立って、ユーザ IP アドレスのヒントを提供できるようにします。RADIUS サーバ上で動作するアプリケーションは、このヒントを使用して、ユーザ名と IP アドレスのテーブル（マップ）を作成できます。RADIUS サーバを使用している場合は、サービス アプリケーションでユーザ ログイン情報を準備して、RADIUS サーバでのユーザ認証に備えることができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「アクセス要求内の RADIUS アトリビュート 8（Framed-IP-Address）の機能情報」（P.7）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

アクセス要求内の RADIUS アトリビュート 8（Framed-IP-Address）の前提条件

RADIUS アクセス要求内で RADIUS アトリビュート 8 を送信する場合は、NAS サーバから IP アドレスを要求するようにログイン ホストを設定しておく必要があります。また、NAS からの IP アドレスを受け入れるようにログイン ホストを設定しておく必要もあります。

NAS は、ログイン ホストをサポートしているインターフェイス上のネットワーク アドレスのプールを使用して設定する必要があります。

アクセス要求内の RADIUS アトリビュート 8（Framed-IP-Address）に関する情報

ネットワーク デバイスが RADIUS 認証用に設定された NAS にダイヤルインすると、NAS がユーザ認証に備えて、RADIUS サーバとの通信プロセスを開始します。通常は、ユーザ認証が成功するまで、ダイヤルイン ホストの IP アドレスが RADIUS サーバに通知されません。RADIUS アクセス要求内でサーバにデバイス IP アドレスを通知すれば、他のアプリケーションがその情報を利用できるようになります。

NAS が RADIUS サーバと通信するようにセットアップされている場合は、NAS が特定のインターフェイス上で設定された IP アドレスのプールからダイヤルイン ホストに IP アドレスを割り当てます。NAS は､ダイヤルイン ホストの IP アドレスをアトリビュート 8 として RADIUS サーバに送信します。そのとき、NAS は、ユーザ名などの他のユーザ情報も RADIUS サーバに送信します。

RADIUS が NAS からユーザ情報を受信した場合は、次の 2 つの選択肢があります。

- RADIUS サーバ上のユーザ プロファイルにすでにアトリビュート 8 が含まれていた場合は、RADIUS が NAS から受け取った IP アドレスをユーザ プロファイル内でアトリビュート 8 として定義された IP アドレスに置き換えます。ユーザ プロファイル内で定義されたアドレスが NAS に返されます。
- ユーザ プロファイルにアトリビュート 8 が含まれていない場合は、RADIUS サーバが、NAS からのアトリビュート 8 を受け入れて、そのアドレスを NAS に返すことができます。

RADIUS サーバから返されたアドレスは、セッションが終わるまで、NAS 上のメモリに保存されます。NAS が RADIUS アカウンティング用に設定されている場合は、RADIUS サーバに送信されるアカウンティング開始パケットにアトリビュート 8 内のものと同じ IP アドレスが含まれています。以降のすべてのアカウンティング パケット、更新（設定されている場合）、および終了パケットにも、アトリビュート 8 で指定されたものと同じ IP アドレスが含まれています。

アクセス要求内の RADIUS アトリビュート 8（Framed-IP-Address）の設定方法

ここでは、次の各手順について説明します。

- 「アクセス要求内の RADIUS アトリビュート 8 の設定」（P.3）（必須）
- 「アクセス要求内の RADIUS アトリビュート 8 の確認」（P.3）

アクセス要求内の RADIUS アトリビュート 8 の設定

アクセス要求内で RADIUS アトリビュート 8 を送信するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server attribute 8 include-in-access-req**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server attribute 8 include-in-access-req** 例： `Router(config)# radius-server attribute 8 include-in-access-req`	access-request パケット内で RADIUS アトリビュート 8 を送信します。

アクセス要求内の RADIUS アトリビュート 8 の確認

RADIUS アトリビュート 8 がアクセス要求内で送信されていることを確認するには、次の手順を実行します。アトリビュート 8 は、すべての PPP アクセス要求内に存在するはずです。

手順の概要

1. **enable**
2. **more system:running-config**
3. **debug radius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**more system:running-config** **例：** `Router# more system:running-config`	現在実行されているコンフィギュレーション ファイルの内容を表示します（**show running-config** コマンドが **more system:running-config** に置き換えられていることに注意してください）。
ステップ 3	**debug radius** **例：** `Router# debug radius`	RADIUS 関連の情報を表示します。このコマンドの出力は、アトリビュート 8 がアクセス要求内で送信されているかどうかを示しています。

アクセス要求内の RADIUS アトリビュート 8（Framed-IP-Address）の設定例

ここでは、次の設定例について説明します。

- 「ダイヤルイン ホストの IP アドレスを RADIUS アクセス要求内で RADIUS サーバに送信する NAS 設定」

ダイヤルイン ホストの IP アドレスを RADIUS アクセス要求内で RADIUS サーバに送信する NAS 設定

次の例は、ダイヤルイン ホストの IP アドレスを RADIUS アクセス要求内で RADIUS サーバに送信する NAS 設定を示しています。NAS は、RADIUS Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）用に設定されています。IP アドレスのプール（async1-pool）が設定され、インターフェイス Async1 に適用されています。

```
aaa new-model
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
!
ip address-pool local
!
interface Async1
 peer default ip address pool async1-pool
!
ip local pool async1-pool 209.165.200.225 209.165.200.229
!
radius-server host 172.31.71.146 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute 8 include-in-access-req
radius-server key radhost<xxx>: Example
```

その他の参考資料

次の項で、アクセス要求内の RADIUS アトリビュート 8（Framed-IP-Address）に関する参考資料を紹介します。

関連資料

内容	参照先
認証の設定と RADIUS の設定	『*Cisco Security Configuration Guide*』の「Configuring Authentication」の章と「Configuring RADIUS」の各章
RFC 2138 (RADIUS)	RFC 2138「*Remote Authentication Dial In User Service (RADIUS)*」

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能がサポートする新規 RFC または改訂 RFC はありません。また、この機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

アクセス要求内の RADIUS アトリビュート 8（Framed-IP-Address）の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　アクセス要求内の RADIUS アトリビュート 8（Framed-IP-Address）の機能情報

機能名	リリース	機能情報
アクセス要求内の RADIUS アトリビュート 8（Framed-IP-Address）	12.2(11)T 12.2(28)SB 12.2(33)SRC	アクセス要求内の RADIUS アトリビュート 8（Framed-IP-Address）機能は、Network Access Server（NAS; ネットワーク アクセス サーバ）から RADIUS サーバに、ユーザ認証に先立って、ユーザ IP アドレスのヒントを提供できるようにします。RADIUS サーバ上で動作するアプリケーションは、このヒントを使用して、ユーザ名と IP アドレスのテーブル（マップ）を作成できます。RADIUS サーバを使用している場合は、サービス アプリケーションでユーザ ログイン情報を準備して、RADIUS サーバでのユーザ認証に備えることができます。 この機能に関する詳細については、次の各項を参照してください。 • 「アクセス要求内の RADIUS アトリビュート 8（Framed-IP-Address）に関する情報」（P.2） • 「アクセス要求内の RADIUS アトリビュート 8（Framed-IP-Address）の設定方法」（P.2） • 「アクセス要求内の RADIUS アトリビュート 8（Framed-IP-Address）の設定例」（P.4） **radius-server attribute 8 include-in-access-req** コマンドが導入または変更されました。

RADIUS トンネル アトリビュート拡張

RADIUS トンネル アトリビュート拡張機能を使用すれば、VPN トンネリングをセットアップするときに、トンネル イニシエータとターミネータの名前（デフォルト以外）を指定して、より高いレベルのセキュリティを設定できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「RADIUS トンネル アトリビュート拡張の機能情報」（P.7）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

RADIUS トンネル アトリビュート拡張の前提条件

RADIUS アトリビュートの 90 と 91 を使用するには、次のタスクを完了する必要があります。

- AAA をサポートするように NAS を設定する。
- RADIUS をサポートするように NAS を設定する。
- VPN をサポートするように NAS を設定する。

RADIUS トンネル アトリビュート拡張の制約事項

RADIUS トンネル アトリビュートの 90 と 91 を使用するには、RADIUS サーバがタグ付きアトリビュートをサポートしている必要があります。

RADIUS トンネル アトリビュート拡張に関する情報

RADIUS トンネル アトリビュート拡張機能は、RADIUS アトリビュート 90（Tunnel-Client-Auth-ID）と RADIUS アトリビュート 91（Tunnel-Server-Auth-ID）を導入しています。この両方のアトリビュートは、ユーザに Network Access Server（NAS; ネットワーク アクセス サーバ）と RADIUS サーバの認証名の指定を許可することによって、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）での強制的トンネリングのプロビジョニングを支援します。

RADIUS トンネル アトリビュート拡張の動作方法

NAS と RADIUS サーバ間の通信がセットアップされたら、トンネリング プロトコルを有効にできます。トンネリング プロトコルのアプリケーションの一部は自発的ですが、その他は強制的トンネリングを伴います。つまり、ユーザが何らかの処置や選択をしなくてもトンネルが作成されます。このような場合は、NAS から RADIUS サーバにトンネリング情報を伝送して認証を確立するための新しい RADIUS アトリビュートが必要です。この新しい RADIUS アトリビュートを表 1 に示します。

（注） 強制的トンネリングでは、配備中のセキュリティ対策がトンネル エンドポイント間のトラフィックにのみ適用されます。トンネル化されたトラフィックの暗号化または完全性保護をエンドツーエンド セキュリティの代替手段と見なさないでください。

表 1　RADIUS トンネル アトリビュート

番号	IETF RADIUS トンネル アトリビュート	同等の TACACS+ アトリビュート	サポートされているプロトコル	説明
90	Tunnel-Client-Auth-ID	tunnel-id	• Layer 2 Forwarding（L2F; レイヤ 2 フォワーディング） • Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）	トンネル ターミネータによるトンネル セットアップの認証時に、トンネル イニシエータ（NAS とも呼ばれる[1]）によって使用される名前を指定します。
91	Tunnel-Server-Auth-ID	gw-name	• Layer 2 Forwarding（L2F; レイヤ 2 フォワーディング） • Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）	トンネル イニシエータによるトンネル セットアップの認証時に、トンネル ターミネータ（ホーム ゲートウェイとも呼ばれる[2]）によって使用される名前を指定します。

1. L2TP が使用されている場合は、NAS が L2TP Access Concentrator（LAC; L2TP アクセス コンセントレータ）として参照されます。
2. L2TP が使用されている場合は、ホーム ゲートウェイが L2TP Network Server（LNS; L2TP ネットワーク サーバ）として参照されます。

RADIUS アトリビュート 90 と RADIUS アトリビュート 91 は次のような状況で追加されます。

- RADIUS サーバが要求を受け入れ、必要な認証名がデフォルトと異なる場合
- アカウンティング要求に値が start と stop のどちらかの Acct-Status-Type アトリビュートが含まれ、トンネル化されたセッションが関係している場合

RADIUS アトリビュート 90 と RADIUS アトリビュート 91 の確認方法

RADIUS アトリビュート 90 と RADIUS アトリビュート 91 がアクセス受け入れとアカウンティング要求内で送信されていることを確認するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# debug radius`	RADIUS 関連の情報を表示します。このコマンドの出力は、アトリビュート 90 と アトリビュート 91 のどちらがアクセス受け入れとアカウンティング要求内で送信されているかを示します。

RADIUS トンネル アトリビュート拡張の設定例

ここでは、次の設定例について説明します。

- 「L2TP Network Server（LNS; L2TP ネットワーク サーバ）設定の例」
- 「RADIUS トンネリング アトリビュートの 90 と 91 を含む RADIUS ユーザ プロファイル：例」

L2TP Network Server（LNS; L2TP ネットワーク サーバ）設定の例

次の例は、RADIUS トンネリング アトリビュートの 90 と 91 を使用した基本的な L2F と L2TP の設定を含む LNS の設定方法を示しています。

```
aaa new-model
aaa authentication login default none
aaa authentication login console none
aaa authentication ppp default local group radius
aaa authorization network default group radius if-authenticated
!
username l2f-cli-auth-id password 0 l2f-cli-pass
username l2f-svr-auth-id password 0 l2f-svr-pass
username l2tp-svr-auth-id password 0 l2tp-tnl-pass
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
accept-dialin
protocol l2f
virtual-template 1
terminate-from hostname l2f-cli-auth-id
local name l2f-svr-auth-id
!
vpdn-group 2
accept-dialin
protocol l2tp
virtual-template 2
terminate-from hostname l2tp-cli-auth-id
local name l2tp-svr-auth-id
!
interface Ethernet1/0
ip address 10.0.0.3 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface Virtual-Template1
ip unnumbered Ethernet1/0
ppp authentication pap
!
interface Virtual-Template2
ip unnumbered Ethernet1/0
ppp authentication pap
!
radius-server host 1.1.1.1 auth-port 1645 acct-port 1646
radius-server key <deleted>
!
```

RADIUS トンネリング アトリビュートの 90 と 91 を含む RADIUS ユーザ プロファイル：例

RADIUS トンネリング アトリビュートの 90 と 91 を含む RADIUS ユーザ プロファイルの例を次に示します。このエントリは 2 つのトンネルをサポートします。1 つは L2F 用、もう 1 つは L2TP 用です。:1 が指定されたタグ エントリは L2F トンネルをサポートし、:2 が指定されたタグ エントリは L2TP トンネルをサポートします。

```
cisco.com Password = "cisco", Service-Type = Outbound
    Service-Type = Outbound,
    Tunnel-Type = :1:L2F,
    Tunnel-Medium-Type = :1:IP,
    Tunnel-Client-Endpoint = :1:"10.0.0.2",
    Tunnel-Server-Endpoint = :1:"10.0.0.3",
    Tunnel-Client-Auth-Id = :1:"l2f-cli-auth-id",
    Tunnel-Server-Auth-Id = :1:"l2f-svr-auth-id",
    Tunnel-Assignment-Id = :1:"l2f-assignment-id",
    Cisco-Avpair = "vpdn:nas-password=l2f-cli-pass",
    Cisco-Avpair = "vpdn:gw-password=l2f-svr-pass",
    Tunnel-Preference = :1:1,
    Tunnel-Type = :2:L2TP,
    Tunnel-Medium-Type = :2:IP,
    Tunnel-Client-Endpoint = :2:"10.0.0.2",
    Tunnel-Server-Endpoint = :2:"10.0.0.3",
    Tunnel-Client-Auth-Id = :2:"l2tp-cli-auth-id",
    Tunnel-Server-Auth-Id = :2:"l2tp-svr-auth-id",
    Tunnel-Assignment-Id = :2:"l2tp-assignment-id",
    Cisco-Avpair = "vpdn:l2tp-tunnel-password=l2tp-tnl-pass",
    Tunnel-Preference = :2:2
```

その他の参考資料

次の項で、RADIUS トンネル アトリビュート拡張に関する参考資料を紹介します。

関連資料

内容	参照先
認証	「Configuring Authentication」モジュール
RADIUS アトリビュート	「RADIUS Attributes Overview and RADIUS IETF Attributes」モジュール
VPDN	『*Cisco IOS VPDN Configuration Guide*, Release 15.0』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2868	「*RADIUS Attributes for Tunnel Protocol Support*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

RADIUS トンネル アトリビュート拡張の機能情報

表 2 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 2 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 2　RADIUS トンネル アトリビュート拡張の機能情報

機能名	リリース	機能情報
RADIUS トンネル アトリビュート拡張の機能情報	12.1(5)T 12.2(4)B3 12.2(13)T	RADIUS トンネル アトリビュート拡張機能を使用すれば、VPN トンネリングをセットアップするときに、トンネル イニシエータとターミネータの名前（デフォルト以外）を指定して、より高いレベルのセキュリティを設定できます。 この機能は、Cisco IOS Release 12.1(5)T で導入されました。 この機能は、Cisco IOS Release 12.2(4)B3 に統合されました。 この機能は、Cisco IOS Release 12.2(13)T に統合されました。

用語集

L2TP アクセス コンセントレータ（LAC）：クライアントが直接接続し、PPP フレームが L2TP Network Server（LNS; L2TP ネットワーク サーバ）にトンネリングされる Network Access Server（NAS; ネットワーク アクセス サーバ）です。LAC は、L2TP が 1 つまたは複数の LNS にトラフィックを渡すために操作するメディアのみを実装します。LAC は PPP 内で伝送されるすべてのプロトコルをトンネルすることができます。また、LAC は着信コールを開始して、発信コールを受け取ります。LAC は L2F ネットワーク アクセス サーバに似ています。

L2TP ネットワーク サーバ（LNS）：L2TP トンネルの終端点で、PPP フレームが処理され、上位レイヤ プロトコルに渡されるアクセス ポイント。LNS は PPP を終端させる任意のプラットフォーム上で動作できます。LNS はサーバ側の L2TP プロトコルを処理します。L2TP は、L2TP のトンネルが到達する 1 つのメディアにのみ依存します。LNS は発信コールを開始して、着信コールを受け取ります。LNS は L2F テクノロジーのホーム ゲートウェイに似ています。

トンネル：L2TP アクセス コンセントレータ（LAC）と L2TP ネットワーク サーバ（LNS）間で複数の PPP セッションを伝送可能な仮想パイプ

ネットワーク アクセス サーバ（NAS）：パケットの世界（インターネットなど）と回線交換の世界（PSTN など）をインターフェイスするシスコ プラットフォームまたは AccessPath システムなどのプラットフォームの集合

バーチャル プライベート ネットワーク（VPN）：リモートでダイヤルイン ネットワークをホーム ネットワークに存在させ、あたかも直接接続されているかのように見せるシステム。VPN は、L2TP と L2F を使用して、L2TP アクセス コンセントレータ（LAC）の代わりに、L2TP ネットワーク サーバ（LNS）でネットワーク接続のレイヤ 2 と上位レイヤを終端させます。

レイヤ 2 トンネル プロトコル（L2TP）：ISP などのアクセス サービスで仮想トンネルを作成し、顧客のリモート サイトやリモート ユーザを会社のホーム ネットワークにリンクさせることが可能なレイヤ 2 トンネリング プロトコル。具体的には、ISP Point of Presence（POP; アクセス ポイント）にある Network Access Server（NAS; ネットワーク アクセス サーバ）がリモート ユーザと PPP メッセージを交換し、L2F または L2TP の要求や応答を使用して顧客のトンネル サーバと通信し、トンネルのセットアップを行います。

レイヤ 2 フォワーディング（L2F）：ISP などのアクセス サービスで仮想トンネルを作成し、顧客のリモート サイトやリモート ユーザを会社のホーム ネットワークにリンクさせることが可能なレイヤ 2 トンネリング プロトコル。具体的には、ISP Point of Presence（POP; アクセス ポイント）にある Network Access Server（NAS; ネットワーク アクセス サーバ）がリモート ユーザと PPP メッセージを交換し、L2F または L2TP の要求や応答を使用して顧客のトンネル サーバと通信し、トンネルのセットアップを行います。

SSH（セキュア シェル）

セキュア シェルの設定

Secure Shell（SSH; セキュア シェル）は、Berkeley の r ツールへのセキュアな置換を提供するアプリケーションおよびプロトコルです。プロトコルは標準の暗号メカニズムを使用してセッションの安全を確保します。アプリケーションは Berkeley の rexec および rsh ツールと同様に使用できます。2 つのバージョンの SSH（SSH バージョン 1 と SSH バージョン 2）を使用できます。ここでは、SSH バージョン 1 について説明します。SSH バージョン 2 については、「Secure Shell Version 2 Support」フィーチャ モジュールを参照してください。

（注） 以降、特に明記していないかぎり、「SSH」という用語は「SSH バージョン 1」だけを示します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「セキュア シェルの設定に関する機能情報」（P.14）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

SSH の設定に関する前提条件

SSH の設定前に、次のタスクを実行します。

- ルータに必要なイメージをダウンロードします SSH サーバには、Cisco IOS Release 12.1(1)T 以降のリリースの IPsec（Data Encryption Standard（DES）または 3DES）暗号化ソフトウェア イメージが必要です。SSH クライアントには、Cisco IOS Release 12.1(3)T 以降のリースの IPsec（DES または 3DES）暗号化ソフトウェア イメージが必要です。ソフトウェア イメージのダウンロードの詳細については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』を参照してください。
- グローバル コンフィギュレーション モードで **hostname** コマンドと **ip domain-name** コマンドを使用して、ルータのホスト名とホスト ドメインを設定します。
- ルータの Rivest, Shamir and Adleman（RSA）キー ペアを生成します。グローバル コンフィギュレーション モードで **crypto key generate rsa** コマンドを入力すると、このキー ペアによって SSH とリモート認証が自動的にイネーブルになります。

（注） RSA キー ペアを削除するには、**crypto key zeroize rsa** グローバル コンフィギュレーション コマンドを使用します。RSA キー ペアを削除すると、SSH サーバは自動的にディセーブルになります。

- ローカルまたはリモート アクセスのためにユーザ認証を設定します。Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）の有無に関係なく、認証を設定できます。詳細については、「Configuring Authentication」、「Configuring Authorization」、および「Configuring Accounting」の各フィーチャ モジュールを参照してください。

SSH の設定に関する制約事項

SSH には、次の制約事項があります。

- SSH サーバと SSH クライアントは、DES（56-bit）および 3DES（168-bit）データ暗号化ソフトウェア イメージでだけサポートされます。DES ソフトウェア イメージの場合、使用できる暗号化アルゴリズムは DES だけです。3DES ソフトウェア イメージの場合、DES と 3DES の両方の暗号化アルゴリズムを使用できます。
- 実行シェルは、唯一サポートされるアプリケーションです。
- ログイン バナーはセキュア シェル バージョン 1 ではサポートされません。セキュア シェル バージョン 2 ではサポートされています。

セキュア シェルの概要

ここでは、SSH の概要について説明します。

- 「SSH サーバ」（P.3）
- 「SSH 統合クライアント」（P.3）
- 「RSA 認証のサポート」（P.3）

（注） 以降、特に明記していないかぎり、「SSH」という用語は「SSH バージョン 1」だけを示します。

SSH サーバ

SSH サーバの機能によって、SSH クライアントは Cisco ルータに対してセキュアで暗号化された接続を実行できます。この接続には、インバウンド Telnet 接続の機能と似ています。SSH 以前は、セキュリティは Telnet のセキュリティに限定されていました。SSH を Cisco IOS ソフトウェア認証と併用することで、強力な暗号化が可能になりました。Cisco IOS ソフトウェアの SSH サーバは、市販の一般的な SSH クライアントと連携できます。

SSH 統合クライアント

SSH 統合クライアント機能は、SSH プロトコル上で動作し、デバイスの認証および暗号化を提供するアプリケーションです。SSH クライアントによって、Cisco ルータは他の Cisco ルータ、または SSH サーバを実行する他のデバイスに対して、セキュアで暗号化された接続を実行できます。この接続には、接続が暗号化されている点を除き、アウトバウンド Telnet 接続と似た機能があります。SSH クライアントは、認証および暗号化により、非セキュアなネットワーク上でセキュアな通信ができます。

Cisco IOS ソフトウェアの SSH クライアントは、市販の一般的な SSH クライアントと相互運用ができます。SSH クライアントは、DES、3DES、およびパスワード認証の暗号をサポートします。ユーザ認証は、ルータに対する Telnet セッションの認証と同様に実行されます。SSH でサポートされるユーザ認証メカニズムには、RADIUS、TACACS+、およびローカルに保存されたユーザ名とパスワードがあります。

（注） SSH クライアント機能を使用できるのは、SSH サーバがイネーブルの場合だけです。

RSA 認証のサポート

SSH クライアントで使用できる RSA 認証は、Cisco IOS ソフトウェアの SSH サーバではデフォルトでサポートされていません。RSA 認証のサポートを設定する手順については、「Secure Shell Version 2 Support」の章の「Configuring a Router for SSH Version 2 Using Private Public Key Pairs」の項を参照してください。

SSH の設定方法

次のタスクを実行して、SSH を設定します。

- 「SSH サーバの設定」（P.4）（必須）
- 「SSH クライアントの呼び出し」（P.5）（任意）

（注） 以降、特に明記していないかぎり、「SSH」という用語は「SSH バージョン 1」だけを示します。

SSH サーバの設定

SSH サーバを設定するには、次の手順を実行します。このタスクによって、Cisco ルータで SSH をイネーブルにできます。

（注） SSH クライアント機能はユーザ EXEC モードで実行され、ルータの設定は特にありません。

（注） SSH コマンドは任意であり、SSH サーバをディセーブルにするとディセーブルになります。SSH パラメータを設定しない場合、デフォルト値が使用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip ssh** {**timeout** *seconds* | **authentication-retries** *integer*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip ssh** {**timeout** *seconds* | **authentication-retries** *integer*} 例： `Router(config) # ip ssh timeout 30`	ルータで SSH コントロール パラメータを設定します。 • SSH コントロール変数の 1 つを選択します。 • *seconds* 引数に、120 秒以下のタイムアウト値を指定します。デフォルトは 120 です。この設定は、SSH のネゴシエーション フェーズに適用されます。EXEC セッションが開始されると、vty に設定された標準のタイムアウトが適用されます。 • デフォルトで、5 個の vty（0 ～ 4）が定義されているため、5 個のターミナル セッションが可能です。SSH がシェルを実行した後、vty タイムアウトが開始されます。vty タイムアウトのデフォルト値は 10 分です。
		• integer 引数で、5 回以下の認証の再試行回数を指定します。デフォルト値は 3 です。 （注） このコマンドは、ユーザに表示するパスワード プロンプトの回数を設定するためにも使用できます。この数値は、次の 2 つの値の低い方です。 – **ssh -o numberofpasswordprompt** コマンドを使用してクライアントから提案された値。 – **ip ssh authentication-retries** *integer* コマンドを使用してルータに設定されている値に 1 を足した値。

SSH クライアントの呼び出し

このタスクを実行して、SSH クライアントを呼び出します。

手順の概要

1. **enable**
2. **ssh -l** *username* **-vrf** *vrf-name ip-address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	（任意）特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**ssh -l** *username* **-vrf** *vrf-name ip-address* **例：** `Router# ssh -l user1 -vrf vrf1 192.0.2.1`	（任意）Cisco IOS SSH クライアントを呼び出し、指定した Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）の IP ホストまたはアドレスに接続します。

トラブルシューティングのヒント

- SSH コンフィギュレーション コマンドが正規のコマンドとして拒否される場合、ルータの RSA キー ペアを適切に生成していません。ホスト名とドメインを指定してください。次に、**crypto key generate rsa** コマンドを使用して RSA キー ペアを生成し、SSH サーバをイネーブルにします。
- RSA キー ペアを設定すると、次のエラー メッセージが表示されることがあります。
  - No hostname specified

    hostname グローバル コンフィギュレーション コマンドを使用して、ルータのホスト名を設定する必要があります。詳細については、「IPsec and Quality of Service」フィーチャ モジュールを参照してください。
  - No domain specified

    ip domain-name グローバル コンフィギュレーション コマンドを使用して、ルータのホストドメインを設定する必要があります。詳細については、「IPsec and Quality of Service」フィーチャ モジュールを参照してください。
- 使用できる SSH 接続数は、ルータに設定されている vty の最大数に制限されます。各 SSH 接続は vty リソースを使用します。
- SSH は、ユーザ認証のためにルータ上で AAA を介して設定されたローカル セキュリティまたはセキュリティ プロトコルを使用します。AAA を設定する場合、ユーザ認証のためにコンソールで AAA をディセーブルにする必要があります。デフォルトでコンソールの AAA 認可はディセーブルです。コンソールで AAA 認可がイネーブルの場合、AAA コンフィギュレーション段階で **no aaa authorization console** コマンドを設定してディセーブルにします。

SSH の設定例

ここでは、Cisco 7200、Cisco 7500、および Cisco 12000 ルータでの **show running-config** EXEC コマンドの出力である次の設定例を紹介します。

- 「Cisco 7200 シリーズ ルータ上の SSH：例」（P.7）
- 「Cisco 7500 シリーズ ルータ上の SSH：例」（P.8）
- 「Cisco 12000 シリーズ ルータ上の SSH：例」（P.10）
- 「SSH の確認：例」（P.11）

（注） 以降、特に明記していないかぎり、「SSH」という用語は「SSH バージョン 1」だけを示します。

（注） **crypto key generate rsa** コマンドは、**show running-config** の出力に表示されません。

Cisco 7200 シリーズ ルータ上の SSH：例

次の例では、60 秒以下のタイムアウト、および 2 回以下の認証再試行回数を指定した SSH が Cisco 7200 に設定されています。SSH サーバ機能をルータに設定する前に、TACACS+ は認証の方式として指定されます。

```
hostname Router72K
aaa new-model
aaa authentication login default tacacs+
aaa authentication login aaa7200kw none
enable password password

username username1 password 0 password1
username username2 password 0 password2
ip subnet-zero
no ip domain-lookup
ip domain-name cisco.com
! Enter the ssh commands.
ip ssh timeout 60
ip ssh authentication-retries 2

controller E1 2/0

controller E1 2/1

interface Ethernet1/0
ip address 192.168.110.2 255.255.255.0 secondary
ip address 192.168.109.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no keepalive
no cdp enable

interface Ethernet1/1
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
no cdp enable

interface Ethernet1/2
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
no cdp enable

no ip classless
ip route 192.168.1.0 255.255.255.0 10.1.10.1
ip route 192.168.9.0 255.255.255.0 10.1.1.1
```

```
ip route 192.168.10.0 255.255.255.0 10.1.1.1

map-list atm
ip 10.1.10.1 atm-vc 7 broadcast
no cdp run

tacacs-server host 192.168.109.216 port 9000
tacacs-server key cisco
radius-server host 192.168.109.216 auth-port 1650 acct-port 1651
radius-server key cisco

line con 0
exec-timeout 0 0
login authentication aaa7200kw
transport input none
line aux 0
line vty 0 4
password password

end
```

Cisco 7500 シリーズ ルータ上の SSH：例

次の例では、60 秒以下のタイムアウト、および 5 回以下の認証再試行回数を指定した SSH が Cisco 7500 に設定されています。SSH サーバ機能をルータに設定する前に、RADIUS は認証の方式として指定されます。

```
hostname Router75K
aaa new-model
aaa authentication login default radius
aaa authentication login aaa7500kw none
enable password password

username username1 password 0 password1
username username2 password 0 password2
ip subnet-zero
no ip cef
no ip domain-lookup
ip domain-name cisco.com
! Enter ssh commands.
ip ssh timeout 60
ip ssh authentication-retries 5

controller E1 3/0
channel-group 0 timeslots 1

controller E1 3/1
channel-group 0 timeslots 1
channel-group 1 timeslots 2

interface Ethernet0/0/0
no ip address
no ip directed-broadcast
no ip route-cache distributed
shutdown

interface Ethernet0/0/1
no ip address
no ip directed-broadcast
no ip route-cache distributed
shutdown
```

```
interface Ethernet0/0/2
no ip address
no ip directed-broadcast
no ip route-cache distributed
shutdown

interface Ethernet0/0/3
no ip address
no ip directed-broadcast
no ip route-cache distributed
shutdown

interface Ethernet1/0
ip address 192.168.110.2 255.255.255.0 secondary
ip address 192.168.109.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache

interface Ethernet1/1
ip address 192.168.109.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown

interface Ethernet1/2
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache

interface Ethernet1/3
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown

interface Ethernet1/4
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
interface Ethernet1/5
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown

interface Serial2/0
ip address 10.1.1.2 255.0.0.0
no ip directed-broadcast
encapsulation ppp
no ip route-cache
no ip mroute-cache

ip classless
ip route 192.168.9.0 255.255.255.0 10.1.1.1
ip route 192.168.10.0 255.255.255.0 10.1.1.1

tacacs-server host 192.168.109.216 port 9000
```

```
tacacs-server key cisco
radius-server host 192.168.109.216 auth-port 1650 acct-port 1651
radius-server key cisco

line con 0
exec-timeout 0 0
login authentication aaa7500kw
transport input none
line aux 0
transport input all
line vty 0 4

end
```

Cisco 12000 シリーズ ルータ上の SSH：例

次の例では、60 秒以下のタイムアウト、および 2 回以下の認証再試行回数を指定した SSH が Cisco 12000 に設定されています。SSH サーバ機能をルータに設定する前に、TACACS+ は認証の方式として指定されます。

```
hostname Router12K
aaa new-model
aaa authentication login default tacacs+ local
aaa authentication login aaa12000kw local
enable password password

username username1 password 0 password1
username username2 password 0 password2
redundancy
main-cpu
    auto-sync startup-config
ip subnet-zero
no ip domain-lookup
ip domain-name cisco.com
! Enter ssh commands.
ip ssh timeout 60
ip ssh authentication-retries 2

interface ATM0/0
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown

interface POS1/0
ip address 10.100.100.2 255.255.255.0
no ip directed-broadcast
encapsulation ppp
no ip route-cache cef
no keepalive
crc 16
no cdp enable

interface POS1/1
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown
crc 32

interface POS1/2
```

```
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown
crc 32

interface POS1/3
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown
crc 32

interface POS2/0
ip address 10.1.1.1 255.255.255.0
no ip directed-broadcast
encapsulation ppp
no ip route-cache cef
crc 16

interface Ethernet0
ip address 172.17.110.91 255.255.255.224
no ip directed-broadcast

router ospf 1
network 0.0.0.0 255.255.255.255 area 0.0.0.0

ip classless
ip route 0.0.0.0 0.0.0.0 172.17.110.65

logging trap debugging
tacacs-server host 172.17.116.138
tacacs-server key cisco

radius-server host 172.17.116.138 auth-port 1650 acct-port 1651
radius-server key cisco

line con 0
exec-timeout 0 0
login authentication aaa12000kw
transport input none
line aux 0
line vty 0 4

no scheduler max-task-time
no exception linecard slot 0 sqe-registers
no exception linecard slot 1 sqe-registers
no exception linecard slot 2 sqe-registers
no exception linecard slot 3 sqe-registers
no exception linecard slot 4 sqe-registers
no exception linecard slot 5 sqe-registers
no exception linecard slot 6 sqe-registers
end
```

SSH の確認：例

SSH サーバがイネーブルであることを確認し、SSH 接続のバージョンおよび設定データを表示するには、**show ip ssh** コマンドを使用します。次に、SSH がイネーブルの例を示します。

```
Router# show ip ssh

SSH Enabled - version 1.5
```

```
Authentication timeout: 120 secs; Authentication retries: 3
```

次に、SSH がディセーブルの例を示します。

```
Router# show ip ssh

%SSH has not been enabled
```

SSH サーバ接続のステータスを確認するには、**show ssh** コマンドを使用します。次に、SSH をイネーブルにしたときのルータ上の SSH サーバ接続の例を示します。

```
Router# show ssh

Connection      Version     EncryptionStateUsername
    0   1.5 3DESSession Startedguest
```

次に、SSH がディセーブルの例を示します。

```
Router# show ssh

%No SSH server connections running.
```

その他の参考資料

ここでは、SSH 機能に関する関連資料について説明します。

関連資料

内容	参照先
Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）	• 「*Configuring Accounting*」フィーチャ モジュール • 「*Configuring Authentication*」フィーチャ モジュール • 「*Configuring Authorization*」フィーチャ モジュール
IPsec	「*IPsec and Quality of Service*」フィーチャ モジュール
SSH バージョン 2	「*Secure Shell Version 2 Support*」フィーチャ モジュール
ソフトウェア イメージのダウンロード	『*Cisco IOS Configuration Fundamentals Configuration Guide*』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によってサポートされる新しい RFC や変更された RFC はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

セキュア シェルの設定に関する機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　セキュア シェルの設定に関する機能情報

機能名	リリース	機能情報
セキュア シェル	12.0(5)S	Secure Shell（SSH; セキュア シェル）は、Berkeley の r ツールへのセキュアな置換を提供するアプリケーションおよびプロトコルです。プロトコルは標準の暗号メカニズムを使用してセッションの安全を確保します。アプリケーションは Berkeley の rexec および rsh ツールと同様に使用できます。2 つのバージョンの SSH（SSH バージョン 1 と SSH バージョン 2）を使用できます。ここでは、SSH バージョン 1 について説明します。

リバース SSH 拡張

Secure Shell（SSH; セキュア シェル）のバージョン 1 と 2 に対してサポートされているリバース SSH 拡張機能は、SSH を有効にしなければならない端末または補助回線ごとに別々の回線を設定する必要がないようにリバース SSH を設定する代替手段を提供します。この機能は、ロータリー グループの制限も排除します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「リバース SSH 拡張の機能情報」（P.10）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

リバース SSH 拡張の前提条件

- SSH を有効にする必要があります。
- SSH クライアントとサーバで同じバージョンの SSH が動作している必要があります。

リバース SSH 拡張の制約事項

- リバース SSH の代替手段をコンソール アクセス用に設定する場合は、**-l** キーワード、*userid* **:**{*number*} {*ip-address*} デリミタ、および引数が必須です。

リバース SSH 拡張に関する情報

リバース SSH 拡張を設定するには、次の概念を理解しておく必要があります。

- 「リバース Telnet」（P.2）
- 「リバース SSH」（P.2）

リバース Telnet

Cisco IOS ソフトウェアには、以前から、リバース telnet と呼ばれる機能が内蔵されているため、特定のポート範囲に telnet して、端末または補助回線に接続できます。リバース telnet は、他の Cisco IOS ルータや他のデバイスのコンソールへの端末回線を複数内蔵した Cisco IOS ルータとの接続によく使用されていました。telnet を使用すれば、特定の回線上のターミナル サーバに telnet することによって、どの場所からでも簡単にルータ コンソールに到達できます。この telnet アプローチは、ルータへのすべてのネットワーク接続が切断されている場合でも、そのルータの設定に使用できます。また、リバース telnet は、Cisco IOS ルータに接続されたモデムをダイヤルアウトに使用することもできます（通常は、ロータリー デバイスと一緒に）。

リバース SSH

リバース telnet は SSH を使用して実現できます。リバース telnet と違って、SSH はセキュアな接続を提供します。リバース SSH 拡張機能は、SSH の設定を容易にします。この機能を使用すれば、SSH を有効にする端末または補助回線ごとに別々の回線を設定する必要がなくなります。以前のリバース SSH 設定方法では、アクセスできるポートの数が 100 に制限されていました。リバース SSH 拡張機能では、ポートの数に制限がありません。リバース SSH 設定の代替手段については、「リバース SSH 拡張の設定方法」（P.2）を参照してください。

リバース SSH 拡張の設定方法

ここでは、次の各手順について説明します。

- 「コンソール アクセス用のリバース SSH の設定」（P.3）
- 「モデム アクセス用のリバース SSH の設定」（P.4）

- 「クライアント上でのリバース SSH のトラブルシューティング」（P.6）
- 「サーバ上でのリバース SSH のトラブルシューティング」（P.6）

コンソール アクセス用のリバース SSH の設定

SSH サーバ上でリバース SSH コンソール アクセスを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **line** *line-number* [*ending-line-number*]
4. **no exec**
5. **login authentication** *listname*
6. **transport input ssh**
7. **exit**
8. **exit**
9. **ssh -l** *userid*:{*number*} {*ip-address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**line** *line-number* [*ending-line-number*] 例： `Router# line 1 3`	設定用の回線を特定して、回線コンフィギュレーション モードに入ります。
ステップ 4	**no exec** 例： `Router (config-line)# no exec`	回線上の EXEC 処理を無効にします。
ステップ 5	**login authentication** *listname* 例： `Router (config-line)# login authentication default`	回線のログイン認証メカニズムを定義します。 （注） 認証方式はユーザ名とパスワードを使用する必要があります。

	コマンドまたはアクション	目的
ステップ 6	**transport input ssh** 例： `Router (config-line)# transport input ssh`	ルータの特定の回線への接続に使用されるプロトコルを定義します。 • リバース SSH 拡張機能の場合は、**ssh** キーワードを使用する必要があります。
ステップ 7	**exit** 例： `Router (config-line)# exit`	ライン コンフィギュレーション モードを終了します。
ステップ 8	**exit** 例： `Router (config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 9	**ssh -l** *userid*:{*number*} {*ip-address*} 例： `Router# ssh -l lab:1 router.example.com`	SSH サーバを実行しているリモート ネットワーキング デバイスにログインするときに使用されるユーザ ID を指定します。 • *userid*：ユーザ *ID* • **:**：ポート番号と端末 **IP** アドレスが *userid* 引数に続くことを示します。 • *number*：端末番号または補助回線番号 • *ip-address*：ターミナル サーバの IP アドレス。 （注） リバース SSH の代替手段をモデム アクセス用に設定する場合は、*userid* 引数、**:rotary**{*number*}{*ip-address*} デリミタ、および引数が必須です。

モデム アクセス用のリバース SSH の設定

リバース SSH をモデム アクセス用に設定するには、後述の「手順の概要」で示す手順を実行します。

この設定では、リバース SSH がダイヤルアウト回線に使用されるモデム上で設定されます。ダイヤルアウト モデムのいずれかに到達するには、下のステップ 10 に示すように、任意の SSH クライアントを使用して SSH セッションを開始し、ロータリー デバイスから次に使用可能なモデムに到達します。

手順の概要

1. **enable**
2. **configure terminal**
3. **line** *line-number* [*ending-line-number*]
4. **no exec**
5. **login authentication** *listname*
6. **rotary** *group*
7. **transport input ssh**
8. **exit**
9. **exit**

10. **ssh -l** *userid*:**rotary**{*number*} {*ip-address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**line** *line-number* [*ending-line-number*] 例： Router# line 1 200	設定用の回線を特定して、回線コンフィギュレーション モードに入ります。
ステップ 4	**no exec** 例： Router (config-line)# no exec	回線上の EXEC 処理を無効にします。
ステップ 5	**login authentication** *listname* 例： Router (config-line)# login authentication default	回線のログイン認証メカニズムを定義します。 **（注）** 認証方式はユーザ名とパスワードを使用する必要があります。
ステップ 6	**rotary** *group* 例： Router (config-line)# rotary 1	1 つ以上の仮想端末回線または 1 つの補助ポート回線からなる回線グループを定義します。
ステップ 7	**transport input ssh** 例： Router (config-line)# transport input ssh	ルータの特定の回線への接続に使用されるプロトコルを定義します。 • リバース SSH 拡張機能の場合は、**ssh** キーワードを使用する必要があります。
ステップ 8	**exit** 例： Router (config-line)# exit	ライン コンフィギュレーション モードを終了します。
ステップ 9	**exit** 例： Router (config)# exit	グローバル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 10	**ssh -l** *userid*:**rotary**{*number*} {*ip-address*} 例： Router# ssh -l lab:rotary1 router.example.com	SSH サーバを実行しているリモート ネットワーキング デバイスにログインするときに使用されるユーザ ID を指定します。 • *userid*：ユーザ *ID* • **:**：ポート番号と端末 IP アドレスが *userid* 引数に続くことを示します。 • *number*：端末番号または補助回線番号 • *ip-address*：ターミナル サーバの IP アドレス。 （注） リバース SSH の代替手段をモデム アクセス用に設定する場合は、*userid* 引数、**:rotary**{*number*}{*ip-address*} デリミタ、および引数が必須です。

クライアント上でのリバース SSH のトラブルシューティング

クライアント（リモート デバイス）上でリバース SSH 設定の問題を解決するには、次の手順を実行します。

手順の概要

1. **enable**
2. **debug ip ssh client**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**debug ip ssh client** 例： Router# debug ip ssh client	SSH クライアントに関するデバッギング メッセージを表示します。

サーバ上でのリバース SSH のトラブルシューティング

ターミナル サーバ上でリバース SSH 設定の問題を解決するには、次の手順を実行します。各ステップは、互いに独立しているため、任意の順序で設定できます。

手順の概要

1. **enable**
2. **debug ip ssh**

3. **show ssh**
4. **show line**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**debug ip ssh** **例：** `Router# debug ip ssh`	SSH サーバに関するデバッギング メッセージを表示します。
ステップ 3	**show ssh** **例：** `Router# show ssh`	SSH サーバ接続のステータスを表示します。
ステップ 4	**show line** **例：** `Router# show line`	端末回線のパラメータを表示します。

リバース SSH 拡張の設定例

ここでは、次の設定例を示します。

- 「リバース SSH コンソール アクセス：例」（P.7）
- 「リバース SSH モデム アクセス：例」（P.8）

リバース SSH コンソール アクセス：例

次の設定例は、リバース SSH が端末回線 1 ～ 3 のコンソール アクセス用に設定されていることを示しています。

ターミナル サーバの設定

```
line 1 3
   no exec
   login authentication default
   transport input ssh
```

クライアントの設定

SSH クライアント上で設定された次のコマンドは、それぞれ、回線 1、2、および 3 とのリバース SSH セッションを形成します。

```
ssh -l lab:1 router.example.com
ssh -l lab:2 router.example.com
ssh -l lab:3 router.example.com
```

リバース SSH モデム アクセス：例

次の設定例は、ダイヤルアウト回線の 1 ～ 200 がモデム アクセス用のロータリー グループ 1 にグループ分けされていることを示しています。

```
line 1 200
   no exec
   login authentication default
   rotary 1
   transport input ssh
   exit
```

次のコマンドは、リバース SSH がロータリー グループの最初の空き回線に接続されることを表示します。

```
ssh -l lab:rotary1 router.example.com
```

その他の参考資料

次の項で、リバース SSH 拡張に関する参考資料を紹介します。

関連資料

内容	参照先
セキュア シェルの設定	次のモジュールを参照 • 「Configuring Secure Shell」 • 「Secure Shell Version 2 Support」 • 「SSH Terminal-Line Access」
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

規格

規格	タイトル
この機能によってサポートされる新しい規格や変更された規格はありません。	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

リバース SSH 拡張の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　リバース SSH 拡張の機能情報

機能名	リリース	機能情報
リバース SSH 拡張	12.3(11)T	Secure Shell（SSH; セキュア シェル）のバージョン 1 と 2 に対してサポートされているリバース SSH 拡張機能は、SSH を有効にしなければならない端末または補助回線ごとに別々の回線を設定する必要がないようにリバース SSH を設定する代替手段を提供します。この機能は、ロータリー グループの制限も排除します。 この機能は、Cisco IOS Release 12.3(11)T で導入されました。 **ssh** コマンドが導入されました。

セキュア コピー

Secure Copy（SCP; セキュア コピー）機能は、ルータ設定またはルータ イメージ ファイルをコピーするセキュアで認証された方法を提供します。SCP は、Secure Shell（SSH; セキュア シェル）、アプリケーション、および Berkeley r ツールのセキュアな代替手段を提供するプロトコルに依存します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「セキュア コピーの機能情報」（P.7）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

セキュア コピーの前提条件

- SCP を有効にする前に、ルータ上で SSH、認証、および認可を正しく設定する必要があります。
- SCP のセキュアな転送は SSH に依存しているため、ルータ上に Rivest, Shamir, and Adelman（RSA）キーのペアを設置する必要があります。

セキュア コピーに関する情報

セキュア コピー機能を設定するには、次の概念を理解しておく必要があります。

- 「セキュア コピーの動作方法」（P.2）

セキュア コピーの動作方法

SCP の動作は、SCP のセキュリティが SSH に依存していることを除いて、Berkeley r ツール スイートからのリモート コピー（rcp）の動作に似ています。加えて、SCP は、ユーザが正しい権限レベルを持っていることをルータ上で判断できるように、authentication, authorization, and accounting（AAA; 認証、認可、およびアカウンティング）許可を設定する必要があります。

SCP を使用すれば、適切な許可を得たユーザは、**copy** コマンドを使用して、Cisco IOS File System（IFS; IOS ファイル システム）内に存在する任意のファイルをルータとやり取りすることができます。許可された管理者はワークステーションからこの操作を実行することもできます。

（注） Cisco IOS ソフトウェアと一緒に pscp.exe を使用している場合は、SCP オプションを有効にします。

セキュア コピーの設定方法

ここでは、次の各手順について説明します。

- 「セキュア コピーの設定」（P.2）
- 「セキュア コピーの設定例」（P.4）

セキュア コピーの設定

Cisco ルータを有効にして、SCP サーバ側機能用に設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
5. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]

6. **username** *name* [**privilege** *level*] {**password** *encryption-type encrypted-password*}
7. **ip scp server enable**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： Router(config)# aaa new-model	ログイン時の AAA 認証を設定します。
ステップ 4	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] 例： Router(config)# aaa authentication login default group tacacs+	AAA アクセス コントロール システムを有効にします。
ステップ 5	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access | configuration**} {**default** | *list-name*} [*method1* [*method2...*]] 例： Router(config)# aaa authorization exec default group tacacs+	ネットワークへのユーザ アクセスを制限するパラメータを設定します。 （注） **exec** キーワードは、認可を実行してユーザが EXEC シェルの実行を許可されているかどうかを判断します。したがって、SCP を設定するときにこのキーワードを使用する必要があります。
ステップ 6	**username** *name* [**privilege** *level*] {**password** *encryption-type encrypted-password*} 例： Router(config)# username superuser privilege 2 password 0 superpassword	ユーザ名をベースとした認証システムを構築します。 （注） TACACS+ や RADIUS などのネットワークベースの認証メカニズムが設定されている場合は、このステップを省略できます。
ステップ 7	**ip scp server enable** 例： Router(config)# ip scp server enable	SCP サーバ側機能を有効にします。
ステップ 8	**show running-config** 例： Router# show running-config	（任意）SCP サーバ側機能を確認します。

	コマンド	目的
ステップ 9	**debug ip scp** **例：** Router# debug ip scp	（任意）SCP 認証問題を解決します。

セキュア コピーの設定例

ここでは、次の設定例について説明します。

- 「ローカル認証を使用した SCP サーバ側設定：例」（P.4）
- 「ネットワークベースの認証を使用した SCP サーバ側設定：例」（P.4）

ローカル認証を使用した SCP サーバ側設定：例

次の例は、SCP のサーバ側機能の設定方法を示しています。この例では、ローカルに定義されたユーザ名とパスワードを使用します。

```
! AAA authentication and authorization must be configured properly for SCP to work.
aaa new-model
aaa authentication login default local
aaa authorization exec default local
username user1 privilege 15 password 0 lab
! SSH must be configured and functioning properly.
ip ssh time-out 120
ip ssh authentication-retries 3
ip scp server enable
```

ネットワークベースの認証を使用した SCP サーバ側設定：例

次の例は、ネットワークベースの認証メカニズムを使用した SCP のサーバ側機能の設定方法を示しています。

```
! AAA authentication and authorization must be configured properly for SCP to work.
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
! SSH must be configured and functioning properly.
ip ssh time-out 120
ip ssh authentication-retries 3
ip scp server enable
```

その他の参考資料

次の項で、セキュア コピーに関する参考資料を紹介します。

関連資料

内容	参照先
セキュア シェル バージョン 1 と 2 のサポート	• 「Configuring Secure Shell」モジュール • 「Secure Shell Version 2 Support」モジュール
認証コマンドと認可コマンド	『*Cisco IOS Security Command Reference*』
認証と認可の設定	『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 15.0』の「Authentication, Authorization, and Accounting (AAA)」

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

セキュア コピーの機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　セキュア コピーの機能情報

機能名	リリース	機能情報
セキュア コピー	12.2(2)T 12.0(21)S 12.2(25)S	Secure Copy（SCP; セキュア コピー）機能は、ルータ設定またはルータ イメージ ファイルをコピーするセキュアで認証された方法を提供します。SCP は、Secure Shell（SSH; セキュア シェル）、アプリケーション、および Berkeley r ツールのセキュアな代替手段を提供するプロトコルに依存します。 この機能は、Cisco IOS Release 12.2(2)T で導入されました。 この機能は、Cisco IOS Release 12.0(21)S に統合されました。 この機能は、Cisco IOS Release 12.2(25)S に統合されました。 **debug ip scp** コマンドと **ip scp server enable** コマンドが導入または変更されました。

用語集

AAA：Authentication, Authorization, and Accounting（認証、認可、およびアカウンティング）。セキュリティ サービスのフレームワークであり、ユーザの身元確認（認証）、リモート アクセス コントロール（認可）、課金、監査、およびレポートに使用するセキュリティ サーバ情報の収集と送信（アカウンティング）の方式を定めています。

rcp：remote copy（リモート コピー）。セキュリティをリモート シェル（Berkeley r ツール スイート）に依存している rcp は、ルータ イメージやスタートアップ設定などのファイルをルータとやり取りします。

SCP：Secure CoPy（セキュア コピー）。セキュリティを SSH に依存している SCP サポートは、Cisco IOS ファイル システム内のあらゆるもののセキュアで認証されたコピーを可能にします。SCP は rcp から派生したものです。

SSH：Secure Shell（セキュア シェル）。Berkeley r ツールのセキュアな代替手段を提供するアプリケーションとプロトコル。プロトコルは標準の暗号メカニズムを使用してセッションの安全を確保します。アプリケーションは Berkeley の rexec および rsh ツールと同様に使用できます。SSH バージョン 1 は Cisco IOS ソフトウェアに実装されています。

セキュア シェル バージョン 2 サポート

セキュア シェル バージョン 2 サポート機能を使用して、Secure Shell（SSH; セキュア シェル）バージョン 2 を設定できます（SSH バージョン 1 のサポートは、以前の Cisco IOS ソフトウェア リリースで実装されていました）。SSH は信頼できる転送レイヤの上位で実行され、強化認証および暗号化機能を実現します。SSH では、信頼できる転送として定義されているのは TCP のみです。SSH で、ネットワーク上の他のコンピュータに安全にアクセスしたり、コマンドを安全に実行できます。SSH とともに提供される Secure Copy Protocol（SCP; セキュア コピー プロトコル）機能で、ファイルを安全に転送できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「セキュア シェル バージョン 2 サポートの機能情報」（P.26）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

セキュア シェル バージョン 2 サポートの前提条件

SSH の設定前に、次のタスクを行ってください。

- 必要なイメージをルータにダウンロードします。SSH サーバでは、Cisco IOS Release 12.3(4)T、12.2(25)S、または 12.3(7)JA から k9（Triple Data Encryption Standard（3DES））ソフトウェア イメージをルータにダウンロードする必要があります。

（注） SSH Version 2 サーバは Cisco IOS Release 12.3(4)T、12.3(2)XE、12.2(25)S、および 12.3(7)JA でサポートされます。SSH Version 2 クライアントは Cisco IOS Release 12.3(7)T からサポートされ、Cisco IOS Release 12.3(7)JA でサポートされています（SSH クライアントは SSH バージョン 1 プロトコルおよびバージョン 2 プロトコルの両方を実行し、Cisco IOS Release 12.3(4)T の k8 および k9 両方のイメージでサポートされます）。

ソフトウェア イメージのダウンロードの詳細については、『*Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.4T』および『*Cisco IOS Network Management Configuration Guide*, Release 15.0』を参照してください。

セキュア シェル バージョン 2 サポートの制約事項

- SSH サーバおよび SSH クライアントは、3DES ソフトウェア イメージでサポートされます。
- サポートされるアプリケーションは、実行シェル、remote コマンドの実行、および SCP のみです。
- Rivest、Shamir、および Adelman（RSA）キー生成は SSH サーバ サイドの要件です。SSH クライアントとして動作するルータは、RSA キーを生成する必要がありません。
- RSA キー ペアのサイズは、768 以上である必要があります。
- 次の機能はサポートされていません。
  - ポート フォワーディング
  - 圧縮

セキュア シェル バージョン 2 サポートに関する情報

- 「セキュア シェル バージョン 2」（P.2）
- 「セキュア シェル バージョン 2 の機能拡張」（P.3）
- 「セキュア シェル バージョン 2 の RSA キーに関する機能拡張」（P.3）
- 「SNMP トラップ生成」（P.4）
- 「SSH キーボード インタラクティブ認証」（P.5）

セキュア シェル バージョン 2

セキュア シェル バージョン 2 サポート機能で、SSH バージョン 2 を設定できます。

SSH バージョン 2 サーバの設定は、SSH バージョン 1 の設定と同様です。**ip ssh version** コマンドは、設定する SSH バージョンを定義できるように導入されました。このコマンドを設定しない場合、デフォルトで SSH は互換モードで実行されます。バージョン 1 とバージョン 2 両方の接続が利用できます。

（注） SSH バージョン 1 は、標準として定義されていないプロトコルです。ルータを定義されていないプロトコル（バージョン 1）に戻したくない場合は、**ip ssh version** コマンドを使用してバージョン 2 を指定してください。

ip ssh rsa keypair-name コマンドも、Cisco IOS Release 12.3(4)T で導入されたため、設定した RSA キーを使用して SSH 接続をイネーブルにできます。すでに、SSH は生成済みの最初の RSA キーにリンクされています（つまり、最初の RSA キー ペアが生成された時点で SSH はイネーブルになっています）。この動作は存在していますが、**ip ssh rsa keypair-name** コマンドを使用してこの動作を行わないようにすることができます。**ip ssh rsa keypair-name** コマンドを、キー ペアの名前を使用して設定する場合、SSH はキー ペアが存在する場合にイネーブルになるか、キー ペアを後で作成する場合は後からイネーブルになります。このコマンドを使用して SSH をイネーブルにする場合、Cisco IOS ソフトウェアの SSH バージョン 1 では必要な、ホスト名とドメイン名を設定を設定する必要はありません。

（注） ログイン バナーは SSH バージョン 2 でサポートされますが、セキュア シェル バージョン 1 ではサポートされません。

セキュア シェル バージョン 2 の機能拡張

SSH バージョン 2 の機能拡張には、VRF aware SSH、SSH デバッグ機能拡張、および Diffie-Hellman（DH）グループ交換のサポートなどの、追加機能がいくつか含まれています。

Cisco IOS SSH 実装では従来、768 ビット絶対値が使用されていましたが、DH グループ 14（2048 ビット）およびグループ 16（4096 ビット）暗号化アプリケーションに対応するため、より大きなキーサイズの必要性が高まり、優先 DH グループを確立するクライアントとサーバ間のメッセージ交換が必要になっています。**ip ssh dh min size** コマンドが Cisco IOS Release 12.4(20)T で導入され、SSH サーバの絶対サイズを設定できるようになりました。これに加え、**ssh** コマンドが拡張され、SSH クライアント サイドのクライアントの VRF インスタンス名を IP アドレスとともに使用して、正しいルーティング テーブルを検索し、接続を確立する機能に、VRF 認識が追加されました。

SSH debug コマンドが修正され、デバッグが拡張されました。**debug ip ssh** コマンドが拡張され、デバッグ処理を簡素化できるようになりました。これまでは、このコマンドで、SSH に関連するデバッグ メッセージが、特に必要なものとそうでないものにかかわらずすべて印刷されていました。この動作は依然として存在しますが、**debug ip ssh** コマンドをキーワードを指定して設定した場合、メッセージが、キーワードで指定した情報に制限されます。

セキュア シェル バージョン 2 の RSA キーに関する機能拡張

Cisco IOS SSH バージョン 2（SSHv2）は、キーボード インタラクティブでパスワード ベースの認証方式をサポートしています。RSA キーの SSHv2 拡張機能は、クライアントとサーバ向けの RSA ベースの公開キー認証もサポートしています。

ユーザ認証：RSA ベースのユーザ認証では、各ユーザに関連付けられている秘密キー / 公開キーのペアを認証に使用します。ユーザは秘密キー / 公開キーのペアをクライアントで生成し、公開キーを Cisco IOS SSH サーバで設定して、認証を完了します。

クレデンシャルの確立を試行する SSH ユーザは、秘密キーを使用して暗号化されたシグニチャを提示します。シグニチャとユーザの公開キーは、認証のために SSH サーバに送信されます。SSH サーバでは、ユーザから提示された公開キーに対してハッシュを計算します。ハッシュは、サーバに一致するエントリがあるかどうかを判断するために使用されます。一致が見つかった場合、RSA ベースのメッセージ検証が公開キーを使用して実行されます。その結果、暗号化されたシグニチャに基づいて、ユーザのアクセスは認証されるか拒否されます。

サーバ認証：SSH セッションの確立中に、Cisco IOS SSH クライアントは、キー交換フェーズ中に使用できるサーバ ホスト キーを使用して、SSH サーバを認証します。SSH サーバ キーは、SSH サーバの識別に使用されます。これらのキーは SSH がイネーブルになるときに作成され、クライアント側で設定する必要があります。

サーバ認証の場合、Cisco IOS SSH クライアントが各サーバにホスト キーを割り当てる必要があります。クライアントがサーバとの間で SSH セッションを確立しようとすると、キー交換メッセージの一部として、サーバのシグニチャを受信します。厳密なホスト キーのチェック フラグがクライアント側でイネーブルの場合、そのサーバに対応するホスト キー エントリがあるかどうかがクライアントで確認されます。一致が見つかると、クライアントはサーバ ホスト キーを使用してシグニチャの検証を試行します。サーバの認証に成功すると、セッションの確立処理は続行します。失敗すると、処理は終了し、「Server Authentication Failed」メッセージが表示されます。

（注） 公開キーをサーバで格納する際、メモリを使用します。したがって、SSH サーバで設定できる公開キーの数は、1 ユーザに最大 2 つの公開キーを作成した場合 10 ユーザ分に限られます。

（注）
- Cisco IOS サーバは RSA ベースのユーザ認証をサポートしていますが、Cisco IOS クライアントは認証方式として公開キーを提案できません。RSA ベースの認証に対するオープンな SSH クライアントからの要求を Cisco IOS サーバが受信した場合、サーバは認証要求を受け入れます。
- サーバ認証の場合、サーバの RSA 公開キーを手動で設定し、Cisco IOS SSH クライアント側で **ip ssh stricthostkeycheck** コマンドを設定します。

SNMP トラップ生成

Cisco IOS Release 12.4(17) では、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップは、トラップがイネーブルで SNMP デバッグがオンになっている場合、SSH セッションが終了した際に自動的に生成されます。SNMP トラップのイネーブル化の詳細については『*Cisco IOS Network Management Configuration Guide*, Release 15.0』の「Configuring SNMP Support」モジュールを参照してください。

（注） **snmp-server host** コマンドを設定する場合、IP アドレスは SSH（Telnet）クライアントがあり、SSH サーバへの IP 接続が可能な PC のアドレスにしてください。SNMP トラップ生成設定の例については、「例：SNMP トラップの設定」（P.20）を参照してください。

また、SNMP デバッグを **debug snmp packet** コマンドを使用してオンにし、トラップを表示する必要があります。トラップ情報には、送信バイト数や SSH セッションで使用されたプロトコルなどの情報が含まれます。SNMP デバッグの例については、「例：SNMP のデバッグ」（P.22）を参照してください。

SSH キーボード インタラクティブ認証

SSH キーボード インタラクティブ認証機能は、SSH での汎用メッセージ認証とも呼ばれ、異なる種類の認証メカニズムを実装するために使用できる方式です。基本的に、現在サポートされている、ユーザの入力のみが必要な認証方式はすべて、この機能で実行することができます。この機能は自動的にイネーブルになります。

次の方式がサポートされています。

- パスワード
- サーバが送信するチャレンジ に応答する番号またはストリングを印刷する SecurID およびハードウェア トークン
- Pluggable Authentication Module（PAM; プラグイン可能な認証モジュール）
- S/KEY（およびその他の使い捨てキー）

自動的にイネーブルにされた SSH キーボード インタラクティブ認証機能のさまざまなシナリオの例については、「例：SSH キーボード インタラクティブ認証」（P.20）を参照してください。

セキュア シェル バージョン 2 サポートの設定方法

ホスト名およびドメイン名を使用した SSH バージョン 2 のルータ設定

このタスクを実行して、SSH バージョン 2 のルータを、ホスト名とドメイン名を使用して設定します。また、SSH バージョン 2 を、RSA キー ペアの設定を使用して設定することもできます（「RSA キー ペアを使用した SSH バージョン 2 のルータ設定」（P.6）を参照）。

手順の概要

1. **enable**
2. **configure terminal**
3. **hostname** *hostname*
4. **ip domain-name** *name*
5. **crypto key generate rsa**
6. **ip ssh** [**time-out** *seconds* | **authentication-retries** *integer*]

7. **ip ssh version** [**1** | **2**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**hostname** *hostname* 例： Router(config)# hostname cisco 7200	ルータのホスト名を設定します。
ステップ 4	**ip domain-name** *name* 例： Router(config)# ip domain-name example.com	ルータのドメイン名を設定します。
ステップ 5	**crypto key generate rsa** 例： Router(config)# crypto key generate rsa	ローカルおよびリモート認証用の SSH サーバをイネーブルにします。
ステップ 6	**ip ssh** [**time-out** *seconds* | **authentication-retries** *integer*] 例： Router(config)# ip ssh time-out 120	（任意）SSH コントロール変数をルータに設定します。
ステップ 7	**ip ssh version** [**1** | **2**] 例： Router(config)# ip ssh version 1	（任意）ルータで実行する SSH のバージョンを指定します。

RSA キー ペアを使用した SSH バージョン 2 のルータ設定

このタスクを実行して、ホスト名またはドメイン名を設定することなく SSH バージョン 2 をイネーブルにします。SSH バージョン 2 は、設定するキー ペアがすでに存在する場合や、後で作成する場合は、後でイネーブルになります。また、SSH バージョン 2 をホスト名とドメイン名を設定して設定することもできます（「ホスト名およびドメイン名を使用した SSH バージョン 2 のルータ設定」（P.5）を参照）。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip ssh rsa keypair-name** *keypair-name*

4. **crypto key generate rsa usage-keys label** *key-label* **modulus** *modulus-size*
5. **ip ssh** [**time-out** *seconds* | **authentication-retries** *integer*]
6. **ip ssh version 2**

手順の詳細

ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip ssh rsa keypair-name** *keypair-name* 例： `Router(config)# ip ssh rsa keypair-name sshkeys`	SSH を使用する際に使用する RSA キー ペアを指定します。 （注） Cisco IOS ルータでは、複数の RSA キー ペアを指定することができます。
ステップ 4	**crypto key generate rsa usage-keys label** *key-label* **modulus** *modulus-size* 例： `Router(config)# crypto key generate rsa usage-keys label sshkeys modulus 768`	ルータでローカルおよびリモート認証を行う SSH サーバをイネーブルにします。 • SSH バージョン 2 では、絶対サイズは 768 ビット以上である必要があります。 （注） RSA キー ペアを削除するには、**crypto key zeroize rsa** コマンドを使用します。RSA キー ペアを削除すると、SSH サーバも自動的にディセーブルになります。
ステップ 5	**ip ssh** [**time-out** *seconds* | **authentication-retries** *integer*] 例： `Router(config)# ip ssh time-out 12`	SSH コントロール変数をルータに設定します。
ステップ 6	**ip ssh version 2** 例： `Router(config)# ip ssh version 2`	ルータで実行する SSH のバージョンを指定します。

RSA ベースのユーザ認証を実行するための Cisco IOS SSH サーバの設定

このタスクを実行して、RSA ベースのユーザ認証を実行するように Cisco IOS SSH サーバを設定します。サーバに保存されている RSA 公開キーが、クライアントに保存されている公開キーと秘密キーのペアを使用して検証されると、ユーザ認証は成功です。

手順の概要

1. **enable**
2. **configure terminal**
3. **hostname** *name*

4. **ip domain-name** *name*
5. **crypto key generate rsa**
6. **ip ssh pubkey-chain**
7. **username** *username*
8. **key-string**
9. **exit**
10. **key-hash** *key-type key-name*
11. **end**

手順の詳細

ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**hostname** *name* 例： `Router(config)# hostname host1`	ホスト名を指定します。
ステップ 4	**ip domain-name** *name* 例： `Router(config)# ip domain-name name1`	Cisco IOS ソフトウェアで使用するデフォルトのドメイン名を定義し、不完全なホスト名のドメインを補完します。
ステップ 5	**crypto key generate rsa** 例： `Router(config)# crypto key generate rsa`	RSA キー ペアを生成します。
ステップ 6	**ip ssh pubkey-chain** 例： `Router(config)# ip ssh pubkey-chain`	SSH サーバ上のユーザおよびサーバ認証用に SSH-RSA キーを設定し、公開キー コンフィギュレーション モードを開始します。
ステップ 7	**username** *username* 例： `Router(conf-ssh-pubkey)# username user1`	SSH ユーザ名を設定し、公開キー ユーザ コンフィギュレーション モードを開始します。
ステップ 8	**key-string** 例： `Router(conf-ssh-pubkey-user)# key-string`	リモート ピアの RSA 公開キーを指定し、公開キー データ コンフィギュレーション モードを開始します。 **（注）** オープン SSH クライアントから（言い換えると .ssh/id_rsa.pub ファイルから）公開キー値を取得できます。
ステップ 9	**exit** 例： `Router(conf-ssh-pubkey-data)# exit`	公開キー ユーザ コンフィギュレーション モードを終了します。

ステップ 10	**key-hash** *key-type key-name* 例： `Router(conf-ssh-pubkey-data)# key-hash ssh-rsa key1`	（任意）SSH キー タイプとバージョンを指定します。 • キー タイプは、秘密公開キー ペアの設定では ssh-rsa である必要があります。 • この手順が任意なのは、**key-string** コマンドが設定されている場合のみです。 • **key-string** コマンドまたは **key-hash** コマンドを設定する必要があります。 （注） 公開キー ストリングのハッシュを計算するには、ハッシュ処理ソフトウェアを使用します。また、別の Cisco IOS ルータからのハッシュ値をコピーすることもできます。初めて公開キー データを入力する場合、**key-string** コマンドを使用して公開キー データを入力することを推奨します。
ステップ 11	**end** 例： `Router(conf-ssh-pubkey-data)# end`	現在のモードを終了し、特権 EXEC モードに戻ります。

RSA ベースのサーバ認証を実行するための Cisco IOS SSH サーバの設定

このタスクを実行して、RSA ベースのサーバ認証を実行するように Cisco IOS SSH クライアントを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **hostname** *name*
4. **ip domain-name** *name*
5. **crypto key generate rsa**
6. **ip ssh pubkey-chain**
7. **server** *server-name*
8. **key-string**
9. **exit**
10. **key-hash** *key-type key-name*
11. **end**
12. **configure terminal**
13. **ip ssh stricthostkeycheck**

手順の詳細

ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**hostname** *name* 例： `Router(config)# hostname host1`	ホスト名を指定します。
ステップ 4	**ip domain-name** *name* 例： `Router(config)# ip domain-name name1`	Cisco IOS ソフトウェアで使用するデフォルトのドメイン名を定義し、不完全なホスト名のドメインを補完します。
ステップ 5	**crypto key generate rsa** 例： `Router(config)# crypto key generate rsa`	RSA キー ペアを生成します。
ステップ 6	**ip ssh pubkey-chain** 例： `Router(config)# ip ssh pubkey-chain`	SSH サーバ上のユーザおよびサーバ認証用に SSH-RSA キーを設定し、公開キー コンフィギュレーション モードを開始します。
ステップ 7	**server** *server-name* 例： `Router(conf-ssh-pubkey)# server server1`	ルータでの公開キー認証について SSH サーバをイネーブルにし、公開キー サーバ コンフィギュレーション モードを開始します。
ステップ 8	**key-string** 例： `Router(conf-ssh-pubkey-server)# key-string`	リモート ピアの RSA 公開キーを指定し、公開キー データ コンフィギュレーション モードを開始します。 **（注）** オープン SSH クライアントから（言い換えると .ssh/id_rsa.pub ファイルから）公開キー値を取得できます。
ステップ 9	**exit** 例： `Router(conf-ssh-pubkey-data)# exit`	公開キー データ コンフィギュレーション モードを終了し、公開キー サーバ コンフィギュレーション モードを開始します。

ステップ 10	**key-hash** *key-type key-name* **例：** `Router(conf-ssh-pubkey-server)# key-hash ssh-rsa key1`	（任意）SSH キー タイプとバージョンを指定します。 • 秘密キー / 公開キー ペアの設定では、キー タイプを ssh-rsa にする必要があります。 • この手順が任意なのは、**key-string** コマンドが設定されている場合のみです。 • **key-string** コマンドまたは **key-hash** コマンドを設定する必要があります。 **（注）** 公開キー ストリングのハッシュを計算するには、ハッシュ処理ソフトウェアを使用します。また、別の Cisco IOS ルータからのハッシュ値をコピーすることもできます。初めて公開キー データを入力する場合、**key-string** コマンドを使用して公開キー データを入力することを推奨します。
ステップ 11	**end** **例：** `Router(conf-ssh-pubkey-server)# end`	公開キー サーバ モードを終了し、特権 EXEC モードに戻ります。
ステップ 12	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 13	**ip ssh stricthostkeycheck** **例：** `Router(config)# ip ssh stricthostkeycheck`	サーバ認証が実行されることを確認します。 • 障害発生時には接続は終了します。

リモート デバイスでの暗号化セッションの開始

リモート ネットワーキング デバイスで暗号化セッションを開始するには、このタスクを実行します（ルータをイネーブルにする必要はありません。SSH はディセーブル モードで実行できます）。

（注） 接続するデバイスは、Cisco IOS ソフトウェアでサポートされる暗号化アルゴリズムを備えた SSH サーバをサポートしている必要があります。

手順の概要

1. **ssh** [**-v** {**1** | **2**}] [**-c** {**3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc**}] [**-m** {**hmac-md5** | **hmac-md5-96** | **hmac-sha1** | **hmac-sha1-96**}] [**l** *userid*] [**-o numberofpasswordprompts** *n*] [**-p** *port-num*] {*ip-addr* | *hostname*} [*command*]

手順の詳細

ステップ 1	**ssh** [**-v** {**1** | **2**}] [**-c** {**3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc**}] [**-m** {**hmac-md5** | **hmac-md5-96** | **hmac-sha1** | **hmac-sha1-96**}] [**l** *userid*] [**-o numberofpasswordprompts** *n*] [**-p** *port-num*] {*ip-addr* | *hostname*} [*command*] **例：** `Router# ssh -v 2 -c aes256-cbc -m hmac-sha1-96 -l user2 10.76.82.24`	リモート ネットワーキング デバイスを使用した暗号化セッションを開始します。

トラブルシューティングのヒント

ip ssh version コマンドは、SSH 設定のトラブルシューティングに使用できます。バージョンを変更すると、どの SSH バージョンが問題かを確認できます。

SSH サーバでのセキュア コピー プロトコルのイネーブル化

このタスクを実行して、SSH サーバ上でセキュア コピー プロトコルをイネーブルにします。このタスクでは SCP に関するサーバサイドの機能を設定します。これは、ルータでリモートのワークステーションからファイルを安全にコピーできる一般的な設定の例です。

前提条件

SCP が正しく機能するかどうかは、AAA 認証と認可に依存しています。したがって、AAA はルータで設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login default local**
5. **aaa authorization exec default local**
6. **username** *name* **privilege** *privilege-level* **password** *password*
7. **ip ssh time-out** *seconds*
8. **ip ssh authentication-retries** *integer*
9. **ip scp server enable**

手順の詳細

ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** **例：** `Router(config)# aaa new-model`	AAA アクセス コントロール モデルをイネーブルにします。
ステップ 4	**aaa authentication login default local** **例：** `Router(config)# aaa authentication login default local`	認証時にローカルのユーザ名データベースを使用するように、ログイン時の AAA 認証を設定します。
ステップ 5	**aaa authorization exec default local** **例：** `Router(config)# aaa authorization exec default local`	ユーザ アクセスを制限するパラメータをネットワークに設定します。認証を実行し、ユーザ ID で EXEC シェルを実行するかどうかを定義します。その後、システムで認証にローカル データベースを使用するかを指定します。
ステップ 6	**username** *name* **privilege** *privilege-level* **password** *password* **例：** `Router(config)# username samplename privilege 15 password password1`	ユーザ名ベースの認証システムを確立し、ユーザ名、権限レベル、非暗号化パスワードを指定します。 **（注）** *privelege-level* 引数の最小値は 15 です。権限レベルが 15 未満の場合、接続が切断されます。
ステップ 7	**ip ssh time-out** *seconds* **例：** `Router(config)# ip ssh time-out 120`	ルータが SSH クライアントの応答を待つ時間間隔を、秒で設定します。
ステップ 8	**ip ssh authentication-retries** *integer* **例：** `Router(config)# ip ssh authentication-retries 3`	インターフェイスのリセット後、認証を試行する回数を設定します。
ステップ 9	**ip scp server enable** **例：** `Router(config)# ip scp server enable`	ルータで、リモート ワークステーションから安全にファイルをコピーできるようにします。

トラブルシューティングのヒント

SCP 認証に関する問題のトラブルシューティングには、**debug ip scp** コマンドを使用します。

show ssh コマンドを使用したセキュア シェル接続のステータスの確認

ルータで SSH 接続のステータスを表示するには、**show ssh** コマンドを使用します。

手順の概要

1. **enable**
2. **show ssh**

手順の詳細

ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show ssh** **例：** `Router# show ssh`	SSH サーバ接続のステータスを表示します。

例

次は、**show ssh** コマンド表示ステータスからの、さまざまな SSH バージョン 1 およびバージョン 2 接続に関する出力例です。

バージョン 1 およびバージョン 2 接続

```
-----------------------------------------------------------------------
Router# show ssh

Connection      Version Encryption      State                   Username
 0              1.5     3DES            Session started         lab
Connection Version Mode Encryption  Hmac                State
Username
1          2.0     IN   aes128-cbc  hmac-md5     Session started       lab
1          2.0     OUT  aes128-cbc  hmac-md5     Session started       lab
-------------------------------------------------------------------------
```

バージョン 1 がないバージョン 2 接続

```
-------------------------------------------------------------------------
Router# show ssh

Connection Version Mode Encryption  Hmac                State
Username
1          2.0     IN   aes128-cbc  hmac-md5     Session started       lab
1          2.0     OUT  aes128-cbc  hmac-md5     Session started       lab
%No SSHv1 server connections running.
-------------------------------------------------------------------------
```

バージョン 2 がないバージョン 1 接続

```
-------------------------------------------------------------------------
Router# show ssh

Connection      Version Encryption      State                   Username
 0              1.5     3DES            Session started         lab
%No SSHv2 server connections running.
-------------------------------------------------------------------------
```

セキュア シェル ステータスの確認

SSH 設定を確認するには、このタスクを実行します。

手順の概要

1. **enable**
2. **show ip ssh**

手順の詳細

ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show ip ssh** 例： Router# show ip ssh	SSH のバージョンおよび設定データを表示します。

例

次は、**show ip ssh** コマンドの、イネーブルになっている SSH のバージョン、認証タイムアウト値、および認証リトライ回数の出力例です。

バージョン 1 およびバージョン 2 接続

```
---------------------------------------------------------------------
Router# show ip ssh

SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
---------------------------------------------------------------------
```

バージョン 1 がないバージョン 2 接続

```
----------------------------------------------------------------------
Router# show ip ssh

SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
----------------------------------------------------------------------
```

バージョン 2 がないバージョン 1 接続

```
----------------------------------------------------------------------
Router# show ip ssh

3d06h: %SYS-5-CONFIG_I: Configured from console by console
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
----------------------------------------------------------------------
```

セキュア シェル バージョン 2 のモニタリングと維持

SSH 接続に関するデバッグ メッセージを表示するには、**debug ip ssh** コマンドと **debug snmp packet** コマンドを使用します。

手順の概要

1. **enable**
2. **debug ip ssh**
3. **debug snmp packet**

手順の詳細

ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**debug ip ssh** 例： Router# debug ip ssh	SSH のデバッグ メッセージを表示します。
ステップ 3	**debug snmp packet** 例： Router# debug snmp packet	ルータで送受信された各 SNMP パケットに関する情報を表示します。

例

次は、ディジット 2 キーワードが割り当てられ、これが SSH バージョン 2 接続であることを示す **debug ip ssh** コマンドの出力例です。

```
Router# debug ip ssh

00:33:55: SSH1: starting SSH control process
00:33:55: SSH1: sent protocol version id SSH-1.99-Cisco-1.25
00:33:55: SSH1: protocol version id is - SSH-2.0-OpenSSH_2.5.2p2
00:33:55: SSH2 1: send: len 280 (includes padlen 4)
00:33:55: SSH2 1: SSH2_MSG_KEXINIT sent
00:33:55: SSH2 1: ssh_receive: 536 bytes received
00:33:55: SSH2 1: input: packet len 632
00:33:55: SSH2 1: partial packet 8, need 624, maclen 0
00:33:55: SSH2 1: ssh_receive: 96 bytes received
00:33:55: SSH2 1: partial packet 8, need 624, maclen 0
00:33:55: SSH2 1: input: padlen 11
00:33:55: SSH2 1: received packet type 20
00:33:55: SSH2 1: SSH2_MSG_KEXINIT received
00:33:55: SSH2: kex: client->server aes128-cbc hmac-md5 none
00:33:55: SSH2: kex: server->client aes128-cbc hmac-md5 none
00:33:55: SSH2 1: expecting SSH2_MSG_KEXDH_INIT
00:33:55: SSH2 1: ssh_receive: 144 bytes received
00:33:55: SSH2 1: input: packet len 144
00:33:55: SSH2 1: partial packet 8, need 136, maclen 0
00:33:55: SSH2 1: input: padlen 5
00:33:55: SSH2 1: received packet type 30
00:33:55: SSH2 1: SSH2_MSG_KEXDH_INIT received
```

```
00:33:55: SSH2 1: signature length 111
00:33:55: SSH2 1: send: len 384 (includes padlen 7)
00:33:55: SSH2: kex_derive_keys complete
00:33:55: SSH2 1: send: len 16 (includes padlen 10)
00:33:55: SSH2 1: newkeys: mode 1
00:33:55: SSH2 1: SSH2_MSG_NEWKEYS sent
00:33:55: SSH2 1: waiting for SSH2_MSG_NEWKEYS
00:33:55: SSH2 1: ssh_receive: 16 bytes received
00:33:55: SSH2 1: input: packet len 16
00:33:55: SSH2 1: partial packet 8, need 8, maclen 0
00:33:55: SSH2 1: input: padlen 10
00:33:55: SSH2 1: newkeys: mode 0
00:33:55: SSH2 1: received packet type 2100:33:55: SSH2 1: SSH2_MSG_NEWKEYS received
00:33:56: SSH2 1: ssh_receive: 48 bytes received
00:33:56: SSH2 1: input: packet len 32
00:33:56: SSH2 1: partial packet 16, need 16, maclen 16
00:33:56: SSH2 1: MAC #3 ok
00:33:56: SSH2 1: input: padlen 10
00:33:56: SSH2 1: received packet type 5
00:33:56: SSH2 1: send: len 32 (includes padlen 10)
00:33:56: SSH2 1: done calc MAC out #3
00:33:56: SSH2 1: ssh_receive: 64 bytes received
00:33:56: SSH2 1: input: packet len 48
00:33:56: SSH2 1: partial packet 16, need 32, maclen 16
00:33:56: SSH2 1: MAC #4 ok
00:33:56: SSH2 1: input: padlen 9
00:33:56: SSH2 1: received packet type 50
00:33:56: SSH2 1: send: len 32 (includes padlen 13)
00:33:56: SSH2 1: done calc MAC out #4
00:34:04: SSH2 1: ssh_receive: 160 bytes received
00:34:04: SSH2 1: input: packet len 64
00:34:04: SSH2 1: partial packet 16, need 48, maclen 16
00:34:04: SSH2 1: MAC #5 ok
00:34:04: SSH2 1: input: padlen 13
00:34:04: SSH2 1: received packet type 50
00:34:04: SSH2 1: send: len 16 (includes padlen 10)
00:34:04: SSH2 1: done calc MAC out #5
00:34:04: SSH2 1: authentication successful for lab
00:34:04: SSH2 1: input: packet len 64
00:34:04: SSH2 1: partial packet 16, need 48, maclen 16
00:34:04: SSH2 1: MAC #6 ok
00:34:04: SSH2 1: input: padlen 6
00:34:04: SSH2 1: received packet type 2
00:34:04: SSH2 1: ssh_receive: 64 bytes received
00:34:04: SSH2 1: input: packet len 48
00:34:04: SSH2 1: partial packet 16, need 32, maclen 16
00:34:04: SSH2 1: MAC #7 ok
00:34:04: SSH2 1: input: padlen 19
00:34:04: SSH2 1: received packet type 90
00:34:04: SSH2 1: channel open request
00:34:04: SSH2 1: send: len 32 (includes padlen 10)
00:34:04: SSH2 1: done calc MAC out #6
00:34:04: SSH2 1: ssh_receive: 192 bytes received
00:34:04: SSH2 1: input: packet len 64
00:34:04: SSH2 1: partial packet 16, need 48, maclen 16
00:34:04: SSH2 1: MAC #8 ok
00:34:04: SSH2 1: input: padlen 13
00:34:04: SSH2 1: received packet type 98
00:34:04: SSH2 1: pty-req request
00:34:04: SSH2 1: setting TTY - requested: height 24, width 80; set: height 24,
width 80
00:34:04: SSH2 1: input: packet len 96
00:34:04: SSH2 1: partial packet 16, need 80, maclen 16
00:34:04: SSH2 1: MAC #9 ok
```

```
00:34:04: SSH2 1: input: padlen 11
00:34:04: SSH2 1: received packet type 98
00:34:04: SSH2 1: x11-req request
00:34:04: SSH2 1: ssh_receive: 48 bytes received
00:34:04: SSH2 1: input: packet len 32
00:34:04: SSH2 1: partial packet 16, need 16, maclen 16
00:34:04: SSH2 1: MAC #10 ok
00:34:04: SSH2 1: input: padlen 12
00:34:04: SSH2 1: received packet type 98
00:34:04: SSH2 1: shell request
00:34:04: SSH2 1: shell message received
00:34:04: SSH2 1: starting shell for vty
00:34:04: SSH2 1: send: len 48 (includes padlen 18)
00:34:04: SSH2 1: done calc MAC out #7
00:34:07: SSH2 1: ssh_receive: 48 bytes received
00:34:07: SSH2 1: input: packet len 32
00:34:07: SSH2 1: partial packet 16, need 16, maclen 16
00:34:07: SSH2 1: MAC #11 ok
00:34:07: SSH2 1: input: padlen 17
00:34:07: SSH2 1: received packet type 94
00:34:07: SSH2 1: send: len 32 (includes padlen 17)
00:34:07: SSH2 1: done calc MAC out #8
00:34:07: SSH2 1: ssh_receive: 48 bytes received
00:34:07: SSH2 1: input: packet len 32
00:34:07: SSH2 1: partial packet 16, need 16, maclen 16
00:34:07: SSH2 1: MAC #12 ok
00:34:07: SSH2 1: input: padlen 17
00:34:07: SSH2 1: received packet type 94
00:34:07: SSH2 1: send: len 32 (includes padlen 17)
00:34:07: SSH2 1: done calc MAC out #9
00:34:07: SSH2 1: ssh_receive: 48 bytes received
00:34:07: SSH2 1: input: packet len 32
00:34:07: SSH2 1: partial packet 16, need 16, maclen 16
00:34:07: SSH2 1: MAC #13 ok
00:34:07: SSH2 1: input: padlen 17
00:34:07: SSH2 1: received packet type 94
00:34:07: SSH2 1: send: len 32 (includes padlen 17)
00:34:07: SSH2 1: done calc MAC out #10
00:34:08: SSH2 1: ssh_receive: 48 bytes received
00:34:08: SSH2 1: input: packet len 32
00:34:08: SSH2 1: partial packet 16, need 16, maclen 16
00:34:08: SSH2 1: MAC #14 ok
00:34:08: SSH2 1: input: padlen 17
00:34:08: SSH2 1: received packet type 94
00:34:08: SSH2 1: send: len 32 (includes padlen 17)
00:34:08: SSH2 1: done calc MAC out #11
00:34:08: SSH2 1: ssh_receive: 48 bytes received
00:34:08: SSH2 1: input: packet len 32
00:34:08: SSH2 1: partial packet 16, need 16, maclen 16
00:34:08: SSH2 1: MAC #15 ok
00:34:08: SSH2 1: input: padlen 17
00:34:08: SSH2 1: received packet type 94
00:34:08: SSH2 1: send: len 32 (includes padlen 16)
00:34:08: SSH2 1: done calc MAC out #12
00:34:08: SSH2 1: send: len 48 (includes padlen 18)
00:34:08: SSH2 1: done calc MAC out #13
00:34:08: SSH2 1: send: len 16 (includes padlen 6)
00:34:08: SSH2 1: done calc MAC out #14
00:34:08: SSH2 1: send: len 16 (includes padlen 6)
00:34:08: SSH2 1: done calc MAC out #15
00:34:08: SSH1: Session terminated normally
```

セキュア シェル バージョン 2 サポートの設定例

例：セキュア シェル バージョン 1 の設定

次に、SSH バージョン 1 を設定する例を示します。

```
Router# configure terminal
Router(config)# ip ssh version 1
Router(config)# end
```

例：セキュア シェル バージョン 2 の設定

次に、SSH バージョン 2 を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip ssh version 2
Router(config)# end
```

例：セキュア シェル バージョン 1 および 2 の設定

次に、SSH バージョン 1 と SSH バージョン 2 の両方を設定する例を示します。

```
Router# configure terminal
Router(config)# no ip ssh version
Router(config)# end
```

例：リモート デバイスでの暗号化セッションの開始

次に、リモート デバイスで暗号化セッションを開始する例を示します。

```
Router# ssh -v 2 -c aes256-cbc -m hmac-sha1-160 -l shaship 10.76.82.24
```

例：サーバサイド SCP の設定

次は、SCP のサーバサイド機能の設定方法の例です。この例では、ルータでの AAA 認証および認可の設定も示しています。この例では、ローカルに定義されたユーザ名とパスワードを使

用します。

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa authentication login default local
Router(config)# aaa authorization exec default local
Router(config)# username samplename privilege 15 password password1
Router(config)# ip ssh time-out 120
Router(config)# ip ssh authentication-retries 3
Router(config)# ip scp server enable
Router(config)# end
```

例：SNMP トラップの設定

次に、設定済みの SNMP トラップの例を示します。トラップ通知は、SSH セッションが終了すると自動的に生成されます。この例の a、b、c、d は SSH クライアントの IP アドレスです。SNMP トラップデバッグ出力の例については、「例：SNMP のデバッグ」（P.22）のセクションを参照してください。

```
snmp-server
snmp-server host a.b.c.d public tty
```

例：SSH キーボード インタラクティブ認証

次は、キーボード インタラクティブ認証機能が自動的に配置されたさまざまなシナリオの例です。

クライアントサイドのデバッグ

次の例では、クライアントサイドのデバッグがオンになっており、プロンプトの最大数が 6（SSH キーボード インタラクティブ認証方式とパスワード方式の認証に 3 ずつ）です。

```
Password:
Password:
Password:
Password:
Password:
Password: cisco123
Last login: Tue Dec 6 13:15:21 2005 from 10.76.248.213
user1@courier:~> exit
logout
[Connection to 10.76.248.200 closed by foreign host]

Router1# debug ip ssh client

SSH Client debugging is on

Router1# ssh -l lab 10.1.1.3
Password:
*Nov 17 12:50:53.199: SSH0: sent protocol version id SSH-1.99-Cisco-1.25
*Nov 17 12:50:53.199: SSH CLIENT0: protocol version id is - SSH-1.99-Cisco-1.25
*Nov 17 12:50:53.199: SSH CLIENT0: sent protocol version id SSH-1.99-Cisco-1.25
*Nov 17 12:50:53.199: SSH CLIENT0: protocol version exchange successful
*Nov 17 12:50:53.203: SSH0: protocol version id is - SSH-1.99-Cisco-1.25
*Nov 17 12:50:53.335: SSH CLIENT0: key exchange successful and encryption on
*Nov 17 12:50:53.335: SSH2 CLIENT 0: using method keyboard-interactive
Password:
Password:
Password:
*Nov 17 12:51:01.887: SSH2 CLIENT 0: using method password authentication
```

```
Password:
Password: lab

Router2>
*Nov 17 12:51:11.407: SSH2 CLIENT 0: SSH2_MSG_USERAUTH_SUCCESS message received
*Nov 17 12:51:11.407: SSH CLIENT0: user authenticated
*Nov 17 12:51:11.407: SSH2 CLIENT 0: pty-req request sent
*Nov 17 12:51:11.411: SSH2 CLIENT 0: shell request sent
*Nov 17 12:51:11.411: SSH CLIENT0: session open
```

TACACS+ ACS がバックエンド AAA サーバ、ChPass がイネーブル、ブランク パスワードの変更あり

次の例では、TACACS+ Access Control Server（ACS; アクセス コントロール サーバ）がバックエンド AAA サーバです。ChPass 機能がイネーブルで、ブランク パスワードの変更が、SSH キーボード インタラクティブ認証方式を使用して行われています。

```
Router1# ssh -l cisco 10.1.1.3
Password:
Old Password: cisco
New Password: cisco123
Re-enter New password: cisco123

Router2> exit
[Connection to 10.1.1.3 closed by foreign host]
```

TACACS+ ACS がバックエンド AAA サーバ、ChPass がイネーブル、パスワードは最初のログインで変更

次の例では、TACACS+ ACS はバックエンド AAA サーバで、ChPass 機能がイネーブルです。パスワードは、SSH キーボード インタラクティブ 認証方式を使用して最初のログインで変更されています。

```
Router1# ssh -l cisco 10.1.1.3
Password: cisco
Your password has expired.
Enter a new one now.
New Password: cisco123
Re-enter New password: cisco123

Router2> exit
[Connection to 10.1.1.3 closed by foreign host]

Router1# ssh -l cisco 10.1.1.3
Password:cisco1
Your password has expired.
Enter a new one now.
New Password: cisco
Re-enter New password: cisco12
The New and Re-entered passwords have to be the same.
Try again.
New Password: cisco
Re-enter New password: cisco

Router2>
```

TACACS+ ACS はバックエンド AAA サーバ、ChPass はイネーブル、パスワードは 3 回のログイン後失効

次の例では、TACACS+ ACS はバックエンド AAA サーバで、ChPass 機能がイネーブルです。パスワードは SSH キーボード インタラクティブ認証方式を使用して、3 回のログイン後期限切れになります。

```
Router# ssh -l cisco. 10.1.1.3
Password: cisco

Router2> exit
[Connection to 10.1.1.3 closed by foreign host]

Router1# ssh -l cisco 10.1.1.3
Password: cisco

Router2> exit

Router1# ssh -l cisco 10.1.1.3
Password: cisco

Router2> exit
[Connection to 10.1.1.3 closed by foreign host]

Router1# ssh -l cisco 10.1.1.3
Password: cisco
Your password has expired.
Enter a new one now.
New Password: cisco123
Re-enter New password: cisco123

Router2>
```

例：SNMP のデバッグ

次は、**debug snmp packet** コマンドの出力例です。出力には、SSH セッションの SNMP トラップ情報が含まれます。

```
Router1# debug snmp packet

SNMP packet debugging is on

Router1# ssh -l lab 10.0.0.2

Password:

Router2# exit

[Connection to 10.0.0.2 closed by foreign host]
Router1#
*Jul 18 10:18:42.619: SNMP: Queuing packet to 10.0.0.2
*Jul 18 10:18:42.619: SNMP: V1 Trap, ent cisco, addr 10.0.0.1, gentrap 6, spectrap 1
local.9.3.1.1.2.1 = 6
tcpConnEntry.1.10.0.0.1.22.10.0.0.2.55246 = 4
ltcpConnEntry.5.10.0.0.1.22.10.0.0.2.55246 = 1015
ltcpConnEntry.1.10.0.0.1.22.10.0.0.2.55246 = 1056
ltcpConnEntry.2.10.0.0.1.22.10.0.0.2.55246 = 1392
local.9.2.1.18.2 = lab
*Jul 18 10:18:42.879: SNMP: Packet sent via UDP to 10.0.0.2
Router1#
```

例：SSH のデバッグの強化

次は、**debug ip ssh detail** コマンドの出力例です。出力には、SSH プロトコルとチャネル要求に関するデバッグ情報が含まれます。

```
Router# debug ip ssh detail

00:04:22: SSH0: starting SSH control process
00:04:22: SSH0: sent protocol version id SSH-1.99-Cisco-1.25
00:04:22: SSH0: protocol version id is - SSH-1.99-Cisco-1.25
00:04:22: SSH2 0: SSH2_MSG_KEXINIT sent
00:04:22: SSH2 0: SSH2_MSG_KEXINIT received
00:04:22: SSH2:kex: client->server enc:aes128-cbc mac:hmac-sha1
00:04:22: SSH2:kex: server->client enc:aes128-cbc mac:hmac-sha1
00:04:22: SSH2 0: expecting SSH2_MSG_KEXDH_INIT
00:04:22: SSH2 0: SSH2_MSG_KEXDH_INIT received
00:04:22: SSH2: kex_derive_keys complete
00:04:22: SSH2 0: SSH2_MSG_NEWKEYS sent
00:04:22: SSH2 0: waiting for SSH2_MSG_NEWKEYS
00:04:22: SSH2 0: SSH2_MSG_NEWKEYS received
00:04:24: SSH2 0: authentication successful for lab
00:04:24: SSH2 0: channel open request
00:04:24: SSH2 0: pty-req request
00:04:24: SSH2 0: setting TTY - requested: height 24, width 80; set: height 24, width 80
00:04:24: SSH2 0: shell request
00:04:24: SSH2 0: shell message received
00:04:24: SSH2 0: starting shell for vty
00:04:38: SSH0: Session terminated normally
```

次は、**debug ip ssh packet** コマンドの出力例です。出力には、SSH パケットに関するデバッグ情報が含まれます。

```
Router# debug ip ssh packet

00:05:43: SSH2 0: send:packet of  length 280 (length also includes padlen of 4)
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: input: total packet length of 280 bytes
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 24 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 272 bytes, maclen 0
00:05:43: SSH2 0: input: padlength 4 bytes
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: input: total packet length of 144 bytes
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 136 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 136 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 16 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 136 bytes, maclen 0
00:05:43: SSH2 0: input: padlength 6 bytes
00:05:43: SSH2 0: signature length 143
00:05:43: SSH2 0: send:packet of  length 448 (length also includes padlen of 7)
00:05:43: SSH2 0: send:packet of  length 16 (length also includes padlen of 10)
00:05:43: SSH2 0: newkeys: mode 1
00:05:43: SSH2 0: ssh_receive: 16 bytes received
00:05:43: SSH2 0: input: total packet length of 16 bytes
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 8 bytes, maclen 0
```

```
00:05:43: SSH2 0: input: padlength 10 bytes
00:05:43: SSH2 0: newkeys: mode 0
00:05:43: SSH2 0: ssh_receive: 52 bytes received
00:05:43: SSH2 0: input: total packet length of 32 bytes
00:05:43: SSH2 0: partial packet length(block size)16 bytes,needed 16 bytes, maclen 20
00:05:43: SSH2 0: MAC compared for #3 :ok
```

関連情報

SSH バージョン 2 をサポートする SSH リモート デバイスを使用する必要があります。また、Cisco IOS ルータに接続する必要があります。

その他の参考資料

関連資料

内容	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
AAA	『*Cisco IOS Security Configuration Guide*』の「*Securing User Services*」の章
• ホスト名およびホスト ドメインの設定 • セキュア シェルの設定	『*Cisco IOS Security Configuration Guide: Securing User Services*』の「Configuring Secure Shell」の章
コマンドのデバッグ	『*Cisco IOS Debug Command Reference*』
シスコ ソフトウェア イメージのダウンロード	『*Cisco IOS Configuration Fundamentals Configuration Guide*』 『*Cisco IOS Network Management Configuration Guide*』
Cisco IOS 設定の基礎	
IPsec	『*Cisco IOS Security Configuration Guide*』の「*Secure Connectivity*」の章
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
SNMP、トラップの設定	『*Cisco IOS Network Management Configuration Guide*』の「Configuring SNMP Support」の章

規格

規格	タイトル
IETF Secure Shell Version 2 Draft 規格	Internet Engineering Task Force の Web サイト

MIB

MIB	MIB リンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

セキュア シェル バージョン 2 サポートの機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　セキュア シェル バージョン 2 サポートの機能情報

機能名	リリース	機能情報
セキュア シェル バージョン 2 サポート	12.2(25)S 12.3(4)T 12.2(11)T	セキュア シェル バージョン 2 サポート機能を使用して、Secure Shell（SSH; セキュア シェル）バージョン 2 を設定できます（SSH バージョン 1 のサポートは、以前の Cisco IOS ソフトウェア リリースで実装されていました）。SSH は信頼できる転送レイヤの上位で実行され、強化認証および暗号化機能を実現します。 12.3(11)T では、Cisco 10000 のサポートが追加されました。 この機能に関する詳細については、次の各項を参照してください。 • 「セキュア シェル バージョン 2 サポートに関する情報」（P.2） • 「セキュア シェル バージョン 2 サポートの設定方法」（P.5） 導入または変更されたコマンド：**debug ip ssh**、**ip ssh min dh size**、**ip ssh rsa keypair-name** 、**ip ssh version**、**ssh**。
セキュア シェル バージョン 2 クライアントおよびサーバ サポート	12.0(32)SY 12.3(7)JA 12.4(17)	Cisco IOS イメージが、SSH セッション終了時に SNMP トラップを自動的に生成するよう更新されました。 この機能に関する詳細については、次の各項を参照してください。 • 「SNMP トラップ生成」（P.4） • 「例：SNMP のデバッグ」（P.22）
SSH キーボード インタラクティブ認証	12.4(18) 12.2(33)SXH3	この機能は、SSH での汎用メッセージ認証とも呼ばれ、異なる種類の認証メカニズムを実装するために使用できる方式です。基本的に、現在サポートされている、ユーザの入力のみが必要な認証方式はすべて、この機能で実行することができます。 この機能に関する詳細については、次の各項を参照してください。 • 「SSH キーボード インタラクティブ認証」（P.5） • 「例：SSH キーボード インタラクティブ認証」（P.20）

表 1　セキュア シェル バージョン 2 サポートの機能情報（続き）

機能名	リリース	機能情報
セキュア シェル バージョン 2 の機能拡張	12.4(20)T	セキュア シェル バージョン 2 の機能拡張には、VRF aware SSH、SSH デバッグ機能拡張、および DH グループ 14 および 16 交換のサポートなどの、追加機能がいくつか含まれています。 この機能に関する詳細については、次の各項を参照してください。 • 「セキュア シェル バージョン 2 の機能拡張」（P.3） • 「例：サーバサイド SCP の設定」（P.19）
セキュア シェル バージョン 2 の RSA キーに関する機能拡張	15.0(1)M 15.1(1)S	RSA キーのセキュア シェル バージョン 2 機能拡張には、SSH 向け RSA キー ベースのユーザ認証や、SSH サーバ ホスト キーの保存や検証のサポートなどの、追加機能がいくつか含まれています。 この機能に関する詳細については、次の各項を参照してください。 • 「セキュア シェル バージョン 2 の RSA キーに関する機能拡張」（P.3） • 「RSA ベースのユーザ認証を実行するための Cisco IOS SSH サーバの設定」（P.7） **ip ssh pubkey-chain** および **ip ssh stricthostkeycheck** の各コマンドが導入または変更されました。

SSH Terminal-Line アクセス

SSH Terminal-Line アクセス機能で、tty（text telephone）回線へのセキュアなアクセスを実現します。tty で、聞き取りおよび発話不良でも、電話を使用してメッセージを入力することで、通信できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「SSH Terminal-Line アクセスの機能情報」（P.9）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

SSH Terminal-Line アクセスの前提条件

必要なイメージをルータにダウンロードします。Cisco IOS Release 12.1(1)T 以降のリリースから、Secure Shell（SSH; セキュア シェル）サーバはルータに IPSec（Data Encryption Standard（DES; データ暗号規格）または 3DES）暗号化ソフトウェア イメージを必要とします。Cisco IOS Release 12.1(3)T 以降のリリースから、SSH クライアントはルータに IPSec（DES または 3DES）暗号化ソフトウェア イメージを必要とします。ソフトウェア イメージのダウンロードの詳細については、『*Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.4T』を参照してください。

SSH サーバは、ローカルのユーザ名およびパスワード、TACACS+ または RADIUS を使用して定義されるユーザ名およびパスワードの使用を必要とします。

（注） SSH Terminal-Line アクセス機能は、SSH が含まれるすべてのイメージで使用できます。

SSH Terminal-Line アクセスの制約事項

コンソール サーバ要件

セキュリティ保護されているサーバ アクセスを設定するには、そのロータリーの各回線を定義し、ユーザがそれらのデバイスにそれぞれアクセスする際にネットワークを介して SSH を使用するよう SSH を設定する必要があります。

メモリおよびパフォーマンスに対する影響

SSH を使用した反転 Telnet を置換すると、vty 処理での暗号化と暗号化プロセスの追加により、使用できる tty 回線のパフォーマンスが低下します（どの暗号化メカニズムも、通常のアクセスよりもメモリを多く使用します）。

SSH Terminal-Line アクセスに関する情報

SSH Terminal-Line アクセス 機能を設定するには、次の概念を理解しておく必要があります。

- 「SSH Terminal-Line アクセスの概要」（P.2）

SSH Terminal-Line アクセスの概要

Cisco IOS は、ユーザがルータ（特定のポート範囲経由）を介して tty（非同期）回線に接続するために Telnet を使用できる反転 Telnet をサポートしています。反転 Telnet で、ユーザは従来 Telnet ではサポートされていない、リモート デバイスのコンソール ポートへの接続を行えます。ただし、この方式は、Telnet トラフィックがすべて、ネットワーク上を暗号化されずに通過するため、ほとんどセキュリティ保護されていません。SSH Terminal-Line アクセス機能で、反転 Telnet を SSH に置き換えます。この機能は、tty 回線のデバイスにアクセスする際に暗号化を使用するよう設定でき、ユーザに強固なプライバシーとセッションの一体性をサポートする接続を提供します。

SSH は rsh、rlogin、rcp などの Berkeley r-tools スイートに安全に置換するアプリケーションおよびプロトコルです（Cisco IOS は rlogin をサポートします）。このプロトコルは標準の暗号メカニズムを使用してセッションの安全を確保します。アプリケーションは Berkeley の rexec および rsh ツールと同様に使用できます。現在、2 つのバージョンの SSH（SSH バージョン 1 と SSH バージョン 2）を使用できます。Cisco IOS ソフトウェアに実装されているのは SSH バージョン 1 のみです。

SSH Terminal-Line アクセス機能で、ユーザがルータを安全にアクセスし、次のタスクを実行するよう設定できます。

- 他のルータ、スイッチ、またはデバイスのコンソールまたはシリアル ポートに接続された複数の端末回線があるルータへの接続。
- 特定の回線上のターミナル サーバに安全に接続することで、任意の場所からのルータへの接続を簡素化。
- ダイヤルアウトを安全に行うために使用されるルータにモデムを取り付け可能。
- ローカルで定義したユーザ名とパスワード、TACACS+、RADIUS を使用して各回線の認証を要求。

（注） モジュールでのセッションを開始するために使用する **session slot** コマンドは、仮想 tty（vty）回線で受け入れられるためには Telnet が必要です。SSH に対してのみ vty 回線を制限する場合、モジュールとの通信にコマンドを使用できません。これは、ユーザがデバイスのモジュールに Telnet できるすべての Cisco IOS デバイスに適用されます。

SSH Terminal-Line アクセスの設定方法

ここでは、次の作業について説明します。

- 「SSH Terminal-Line アクセスの設定」（P.3）

SSH Terminal-Line アクセスの設定

次のタスクを実行して、Cisco ルータで安全なリバース Telnet をサポートするよう設定します。

（注） SSH がすでにルータで設定されている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **line** *line-number* [*ending-line-number*]
4. **no exec**
5. **login** {**local** | **authentication** *listname*}
6. **rotary** *group*
7. **transport input** {**all** | **ssh**}
8. **exit**
9. **ip ssh port** *portnum* **rotary** *group*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**line** *line-number* [*ending-line-number*] **例：** `Router(config)# line 1 200`	設定用の回線を特定して、回線コンフィギュレーション モードに入ります。 **（注）** ルータ コンソール コンフィギュレーションでは、各回線を独自のロータリーで定義し、SSH を各ロータリー上で待ち受けるよう設定する必要があります。 **（注）** ユーザ名とパスワードが必要な認証方式を、各回線で設定する必要があります。これは、ルータに保存されたローカルのユーザ名とパスワードや、TACACS+、RADIUS を使用することで行えます。回線パスワードとイネーブル パスワードは両方とも、SSH で使用するには不十分です。
ステップ 4	**no exec** **例：** `Router(config-line)# no exec`	各回線での exec 処理をディセーブルにします。
ステップ 5	**login** {**local** | **authentication** *listname*} **例：** `Router(config-line)# login authentication default`	回線のログイン認証メカニズムを定義します。 **（注）** 認証方式でユーザ名とパスワードを使用する必要があります。
ステップ 6	**rotary** *group* **例：** `Router(config-line)# rotary 1`	1 つ以上で構成される回線グループを定義します。 **（注）** 使用するロータリーをすべて定義し、定義した各ロータリーは SSH がイネーブルの場合に使用される必要があります。
ステップ 7	**transport input** {**all** | **ssh**} **例：** `Router(config-line)# transport input ssh`	ルータの特定の回線への接続に使用されるプロトコルを定義します。

	コマンドまたはアクション	目的
ステップ 8	**exit** 例： `Router(config-line)# exit`	ライン コンフィギュレーション モードを終了します。
ステップ 9	**ip ssh port** *portnum* **rotary** *group* 例： `Router(config)# ip ssh port 2000 rotary 1`	tty 回線へのセキュア ネットワーク アクセスをイネーブルにします。 • このコマンドを使用して、ロータリー *group* 引数とともに *portnum* 引数に接続します。引数は、回線または回線グループと関連付けられています。 （注） *group* 引数は、ステップ 6 で選択した **rotary** *group* 番号と対応している必要があります。

SSH Terminal-Line アクセスの確認

この機能が動作しているか確認するため、SSH クライアントを使用してルータに接続します。

SSH Terminal-Line アクセスの設定例

ここでは、次の設定例について説明します。

- 「SSH Terminal-Line アクセスの設定例」（P.5）
- 「コンソール（シリアル回線）ポートの SSH Terminal-Line アクセスの設定例」（P.6）

SSH Terminal-Line アクセスの設定例

次は、SSH Terminal-Line アクセス機能を、1 ～ 200 の回線でダイヤルアウトで使用するモデムに設定する方法の例です。任意のダイヤルアウト モデムを取得するには 任意の SSH クライアントを使用し、ルータのポート 2000 で SSH セッションを開始して、次に使用可能なモデムをロータリーから取得します。

```
line 1 200
 no exec
 login authentication default
 rotary 1
 transport input ssh
 exit
ip ssh port 2000 rotary 1
```

コンソール（シリアル回線）ポートの SSH Terminal-Line アクセスの設定例

次は、SSH Terminal-Line アクセス機能を、さまざまなデバイスのコンソールまたはシリアル回線インターフェイスにアクセスするよう設定する例です。このタイプのアクセスでは、各回線は独自のロータリーに設定され、各ロータリーは 1 つのポートで使用されます。この例では、回線 1 ～ 3 が使用されています。設定のポート（回線）マッピングを表 1 に示しています。

表 1　ポート（回線）設定マッピング

回線番号	SSH ポート番号
1	2001
2	2002
3	2003

```
line 1
 no exec
 login authentication default
 rotary 1
 transport input ssh
line 2
 no exec
 login authentication default
 rotary 2
 transport input ssh
line 3
 no exec
 login authentication default
 rotary 3
 transport input ssh

ip ssh port 2001 rotary 1 3
```

その他の参考資料

次の項で、SSH Terminal-Line アクセス機能に関連した関連資料を示します。

関連資料

内容	参照先
SSH	『*Cisco IOS Security Configuration Guide: Securing User Services*』
SSH コマンド	『*Cisco IOS Security Command Reference*』
ダイヤル テクノロジー	『*Cisco IOS Dial Technologies Configuration Guide*』
ダイヤル コマンド	『*Cisco IOS Dial Technologies Command Reference*』
ソフトウェア イメージのダウンロード	『*Cisco IOS Configuration Fundamentals Configuration Guide*』

規格

規格	タイトル
	—

MIB

MIB	MIB リンク
	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

SSH Terminal-Line アクセスの機能情報

表 2 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 2 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 2　SSH Terminal-Line アクセスの機能情報

機能名	リリース	機能情報
SSH Terminal-Line アクセス	12.2(4)JA 12.2(15)T 12.2(6th)S	SSH Terminal-Line アクセス機能で、tty（text telephone）回線へのセキュアなアクセスを実現します。tty で、聞き取りおよび発話不良でも、電話を使用してメッセージを入力することで、通信できます。 この機能は、Cisco IOS Release 12.2(4)JA で導入されました。 この機能は、Cisco IOS Release 12.2(15)T に統合されました。 この機能は、Cisco IOS Release 12.2(6th)S に統合されました。 次のコマンドが、導入または変更されました。**ip ssh port**。

Cisco IOS Login Enhancements（Login Block）

Cisco IOS Login Enhancements（Login Block）機能により、ユーザはサービス拒絶（DoS）攻撃と思われる攻撃が検出された場合、ログイン試行を自動的にブロックするオプションを設定して、ルータのセキュリティを強化できます。

この機能により導入された Login Block オプションおよび Login Delay オプションで、Telnet または SSH 仮想接続を設定できます。この機能をイネーブルにすると、接続試行の失敗が複数回検出された場合に、「待機時間」を強制して「辞書攻撃」をスローダウンし、ルーティング デバイスを DoS 攻撃から保護できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「Cisco IOS Login Enhancements（Login Block）の機能情報」（P.9）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

Cisco IOS Login Enhancements について

サービス拒絶攻撃および辞書ログイン攻撃からの保護

ユーザまたは経営幹部レベルで、デバイスを管理する目的によるルーティング デバイスへの接続は、リモート コンソール（PC など）から Telnet または SSH（セキュア シェル）を使用して最も頻繁に実行されます。ユーザのデバイスと管理デバイスとの間の通信トラフィックが暗号化されるため、SSH では、よりセキュアな接続オプションが提供されます。Login Block 機能をイネーブルにすると、Telnet 接続と SSH 接続の両方に適用されます。12.3(33)SRB2、12.2(33)SXH2、および 12.4(15)T1 以降のリリース バージョンでは、Login Block 機能は HTTP 接続にも適用されます。

この機能によって導入される自動アクティベーション、および Login Block 機能および Quiet Period 機能のロギングは、個人が使用するとネットワーク デバイスを阻害したり、損なう可能性のある 2 つの既知の方法に特に対処したりすることでデバイスのセキュリティをさらに強化するように設計されています。

デバイスの接続アドレスが検出され、到達可能である場合、悪意あるユーザが接続要求のフラッディングによってデバイスの通常の動作を妨げようとする可能性があります。通常のルーティング サービスを適切に処理しようとして、繰り返し行われるログイン接続試行を処理しようとしたり、デバイスがビジーになったり、正規のシステム管理者に通常のログイン サービスを提供できなくなる可能性があるため、この種の攻撃は、サービス拒絶（DoS）攻撃の試行と呼ばれます。

辞書攻撃の主な意図は、一般的な DoS 攻撃とは異なり、デバイスへの管理アクセスを実際に取得することです。辞書攻撃とは、数千、時には数百万ものユーザ名 / パスワードの組み合わせでログインを試行する自動プロセスです（この種の攻撃は、通常、まず、使用可能なパスワードの標準的な辞書のすべての単語を使用するため、「辞書攻撃」と呼ばれます）。このアクセスの試行には、スクリプトまたはプログラムが使用されるため、このような試行のプロファイルは、通常、DoS 攻撃と同じで、短時間に複数のログイン試行が行われます。

検出プロファイルをイネーブルにすることにより、ログイン試行の失敗が反復する場合は、以降の接続要求を拒否して対応するように、ルーティング デバイスを設定できます（ログイン ブロッキング）。このブロックには「待機時間」と呼ばれる、一定の時間を設定できます。システム管理者との関連付けが把握されているアドレスを使用してアクセスリスト（ACL）を設定し、待機時間中でも正規の接続試行を許可できます。

Login Enhancements 機能の概要

連続するログイン試行間の遅延

Cisco IOS デバイスは、仮想接続をできる限り高速で処理して受け入れることができます。ログイン試行間に遅延を導入すると、Cisco IOS ソフトウェアベースのデバイスを辞書攻撃や DoS 攻撃などの悪意あるログイン接続から保護することができます。遅延は次のいずれかの方法でイネーブルにできます。

- **auto secure** コマンド。AutoSecure 機能をイネーブルにすると、デフォルトで 1 秒のログイン遅延時間が自動的に強制されます。
- **login block-for** コマンド。このコマンドは、**login delay** コマンドを発行する前に入力する必要があります。**login block-for** コマンドのみを入力すると、デフォルトで 1 秒のログイン遅延時間が自動的に強制されます。
- ログイン遅延時間の強制を秒単位で指定できる新しいグローバル コンフィギュレーション モード コマンド **login delay**。

DoS 攻撃が疑われる場合のログインのシャットダウン

指定した時間内に設定した回数の接続試行が失敗した場合、Cisco IOS デバイスは「待機時間」に追加の接続を受け入れません（定義済みの Access Control List（ACL; アクセス コントロール リスト）により許可されるホストは待機時間から除外されます）。

待機時間を発生させる接続試行の失敗回数は、新しいグローバル コンフィギュレーション モード コマンド **login block-for** で指定できます。待機時間から除外される定義済みの ACL は、新しいグローバル コンフィギュレーション モード コマンド **login quiet-mode access-class** で指定できます。

この機能は、デフォルトではディセーブルです。AutoSecure がイネーブルの場合はイネーブルになりません。

Cisco IOS Login Enhancement の設定方法

- 「ログイン パラメータの設定」（P.3）（必須）
- 「ログイン パラメータの確認」（P.4）（任意）

ログイン パラメータの設定

Cisco IOS デバイスへの DoS 攻撃と思われる攻撃の検出と辞書攻撃の低減に役立つログイン パラメータを設定するには、次の作業を実行します。

ログイン パラメータのデフォルト

すべてのログイン パラメータは、デフォルトではディセーブルです。他のログイン コマンドを使用する前に、デフォルトのログイン機能をイネーブルにする **login block-for** コマンドを発行する必要があります。**login block-for** コマンドをイネーブルにすると、次のデフォルトが強制されます。

- デフォルトの 1 秒のログイン遅延
- Telnet または SSH を通じて行われるすべてのログイン試行は、待機時間中拒否されます。つまり、**login quiet-mode access-class** コマンドが発行されるまで、ACL はログイン時間から除外されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **login block-for** *seconds* **attempts** *tries* **within** *seconds*
4. **login quiet-mode access-class** {*acl-name* | *acl-number*}

5. **login delay** *seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**login block-for** *seconds* **attempts** *tries* **within** *seconds* 例： Router(config)# login block-for 100 attempts 2 within 100	Cisco IOS デバイスで DoS 検出の提供に役立つログイン パラメータを設定します。 （注） このコマンドは、その他のログイン コマンドを使用する前に発行する必要があります。
ステップ 4	**login quiet-mode access-class** {*acl-name* | *acl-number*} 例： Router(config)# login quiet-mode access-class myacl	（任意）待機モードに切り替わるときに、ルータに適用される ACL を指定します。 このコマンドをイネーブルにしない場合、待機モード中、すべてのログイン要求が拒否されます。
ステップ 5	**login delay** *seconds* 例： Router(config)# login delay 10	（任意）連続するログイン試行間の遅延を設定します。

この次の手順

ルータでログイン パラメータを設定した後、設定を確認する必要がある場合があります。この作業を完了するには、「ログイン パラメータの確認」（P.4）を参照してください。

ログイン パラメータの確認

ルータに適用されたログイン設定と現在のログイン ステータスを確認するには、次の作業を実行します。

手順の概要

1. **enable**
2. **show login** [**failures**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show login** [**failures**] 例： Router# show login	ログイン パラメータを表示します。 • **failures**：失敗したログイン試行に関連する情報のみを表示します。

例

show login コマンドからの次のサンプル出力は、ログイン パラメータが指定されていないことを確認します。

```
Router# show login

No login delay has been applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps

Router NOT enabled to watch for login Attacks
```

show login コマンドからの次のサンプル出力は、**login block-for** コマンドが発行されたことを確認します。この例で、コマンドは 100 秒以内に 16 回以上のログイン要求が失敗した場合、ログイン ホストを 100 秒ブロックするように設定されています。すでに 5 回のログイン要求が失敗しています。

```
Router# show login

A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.

Router enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.

Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds.
Present login failure count 5.
```

show login コマンドからの次のサンプル出力は、ルータが待機モードになっていることを確認します。この例で、**login block-for** コマンドは、100 秒以内に 3 回以上のログイン要求が失敗した場合、ログイン ホストを 100 秒ブロックするように設定されています。

```
Router# show login

A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.

Router enabled to watch for login Attacks.
If more than 2 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.
```

```
Router presently in Quiet-Mode, will remain in Quiet-Mode for 93 seconds.
Denying logins from all sources.
```

show login failures コマンドからの次のサンプル出力は、ルータ上で失敗したすべてのログイン試行を表示します。

```
Router# show login failures

Information about login failure's with the device

Username      Source IPAddr  lPort Count  TimeStamp
try1          10.1.1.1        23    1     21:52:49 UTC Sun Mar 9 2003
try2          10.1.1.2        23    1     21:52:52 UTC Sun Mar 9 2003
```

show login failures コマンドからの次のサンプル出力は、現在記録されている情報がないことを確認します。

```
Router# show login failures

*** No logged failed login attempts with the device.***
```

ログイン パラメータの設定例

- 「ログイン パラメータの設定：例」（P.6）

ログイン パラメータの設定：例

次に、100 秒以内に 15 回ログイン要求が失敗した場合に 100 秒の待機モードに入るようにルータを設定する例を示します。待機時間中、ACL「myacl」からのホスト以外、すべてのログイン要求が拒否されます。

```
Router(config)# login block-for 100 attempts 15 within 100
Router(config)# login quiet-mode access-class myacl
```

その他の参考資料

関連資料

内容	参照先
AutoSecure	「AutoSecure」フィーチャ モジュール
セキュアな管理/管理アクセス	「Role-Based CLI Access」フィーチャ モジュール

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco IOS Login Enhancements（Login Block）の機能情報

表 1 に、この機能のリリース履歴を示します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　Cisco IOS Login Enhancements（Login Block）の機能情報

機能名	リリース	機能情報
Cisco IOS Login Enhancements（Login Block）	12.3(4)T 12.2(25)S 12.2(33)SRA 12.2(33)SRB 12.2(33)SXH 12.4(15)T1	Cisco IOS Login Enhancements（Login Block）により、ユーザは DoS 攻撃と思われる攻撃が検出された場合、ログイン試行を自動的にブロックするオプションを設定して、ルータのセキュリティを強化できます。 この機能は、Cisco IOS Release 12.3(4)T で導入されました。 この機能は、Cisco IOS Release 12.2(25)S に統合されました。 この機能は、Cisco IOS Release 12.2(33)SRA に統合されました。 HTTP ログイン ブロッキングのサポートは、Cisco IOS Release 12.2(33)SRB、12.2(33)SXH、12.4(15)T1 に統合されました。

Cisco IOS Resilient Configuration

Cisco IOS Resilient Configuration 機能で、実行中のイメージおよび設定のワーキング コピーを保護し維持することができます。これにより、イメージや設定ファイルが永続ストレージ（NVRAM やフラッシュ）の内容を消去する不正な攻撃に耐えることができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「Cisco IOS Resilient Configuration の機能情報」（P.8）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

Cisco IOS Resilient Configuration の制約事項

- この機能は、Personal Computer Memory Card International Association（PCMCIA; PC メモリカード国際協会）の Advanced Technology Attachment（ATA）をサポートしているプラットフォームでしか使用できません。少なくとも 1 つの Cisco IOS イメージ（アップグレードの場合は

2 つ）と実行設定のコピーを保存するのに十分なスペースがストレージ デバイス上に存在する必要があります。このソフトウェアには、セキュアなファイル システム用の IOS Files System（IFS; IOS ファイル システム）サポートも必要です。

- 隠しファイルに対するファイル システム サポートが含まれていない古いバージョンの Cisco IOS ソフトウェアを使用している場合は、保護されたファイルが強制的に削除される可能性があります。
- この機能は、ルータへのコンソール接続を通してのみ無効にすることができます。アップグレード シナリオを除いて、機能をアクティブにするためのコンソール アクセスは必要ありません。
- ネットワークからロードしたイメージでブートセットを保護できません。実行イメージは、プライマリとして保護すべき永続ストレージからロードする必要があります。
- 保護されたファイルは、エグゼクティブ シェルから発行された **dir** コマンドの出力に表示されません。これは、IFS がディレクトリ内のセキュアなファイルの一覧表示を阻止するためです。ROM monitor（ROMMON; ROM モニタ）モードには、このような制限がないため、保護されたファイルを一覧表示したり、ブートしたりすることができます。実行イメージと実行設定のアーカイブは Cisco IOS **dir** コマンド出力に表示されません。代わりに、**show secure bootset** コマンドを使用してアーカイブの存在を確認できます。

Cisco IOS Resilient Configuration に関する情報

Cisco IOS Resilient Configuration を使用する前に、次の概念を理解しておく必要があります。

- 「Cisco IOS Resilient Configuration の機能設計」（P.2）

Cisco IOS Resilient Configuration の機能設計

ネットワーク オペレータの大きな課題は、ルータの故障以降の総ダウンタイムと、永続ストレージから消去された運用ソフトウェアと設定データです。オペレータは、設定のアーカイブ コピー（もしあれば）とワーキング イメージを入手して、ルータを復元させる必要があります。その後で、影響を受けたルータごとに回復を実行する必要があるため、総ネットワーク ダウンタイムがさらに増加します。

Cisco IOS Resilient Configuration 機能の目的は、回復プロセスを速めることです。この機能は、常に、ルータ イメージのセキュアなワーキング コピーと起動設定を維持します。これらのセキュアなファイルはユーザが削除できません。このイメージとルータ実行設定のセットは、プライマリ ブートセットと呼ばれています。

Cisco IOS Resilient Configuration の設計では、次の要素が考慮されています。

- プライマリ ブートセット内の設定情報は、この機能が最初に有効にされた時点でルータ内に存在していた実行設定のコピーです。
- この機能は、最小限のファイルのワーキング セットを保護することによって、永続ストレージのスペースを確保します。プライマリ Cisco IOS イメージ ファイルを保護するために余分なスペースは必要ありません。
- この機能は、自動的にイメージまたは設定のバージョン ミスマッチを検出します。
- ファイルを保護し、TFTP サーバ上での複数のイメージと設定の保存からスケーラビリティ メンテナンスの課題を排除するために、ローカル ストレージのみが使用されます。
- この機能は、コンソール セッションを通してのみ無効にすることができます。

Cisco IOS Resilient Configuration の使用方法

ここでは、次の各手順について説明します。

- 「ルータ設定のアーカイブ」（P.3）
- 「アーカイブされたルータ設定の復元」（P.4）

ルータ設定のアーカイブ

このタスクでは、永続ストレージ内のセキュアなアーカイブへのプライマリ ブートセットの保存方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **secure boot-image**
4. **secure boot-config**
5. **end**
6. **show secure bootset**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**secure boot-image** 例： `Router(config)# secure boot-image`	Cisco IOS image resilience を有効にします。
ステップ 4	**secure boot-config** 例： `Router(config)# secure boot-config`	プライマリ ブートセットのセキュアなコピーを永続ストレージに保存します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show secure bootset** 例： `Router# show secure bootset`	（任意）設定回復のステータスとプライマリ ブートセット ファイル名を表示します。

例

この項では、次の出力例について説明します。

- 「show secure bootset コマンドのサンプル出力」（P.4）

show secure bootset コマンドのサンプル出力

次の例は、**show secure bootset** コマンドのサンプル出力を示しています。

```
Router# show secure bootset

IOS resilience router id JMX0704L5GH

IOS image resilience version 12.3 activated at 08:16:51 UTC Sun Jun 16 2002
Secure archive slot0:c3745-js2-mz type is image (elf) []
  file size is 25469248 bytes, run size is 25634900 bytes
  Runnable image, entry point 0x80008000, run from ram

IOS configuration resilience version 12.3 activated at 08:17:02 UTC Sun Jun 16 2002
Secure archive slot0:.runcfg-20020616-081702.ar type is config
configuration archive size 1059 bytes
```

アーカイブされたルータ設定の復元

このタスクでは、ルータが改ざん（NVRAM の消去またはディスクのフォーマットによって）された後に、セキュアなアーカイブからプライマリ ブートセットを復元する方法について説明します。

（注） アーカイブされたプライマリ ブートセットを復元するには、Cisco IOS image resilience を有効にして、永続ストレージ内にアーカイブされていたプライマリ ブートセットを復元する必要があります。

手順の概要

1. **reload**
2. **dir** [*filesystem*:]
3. **boot** [*partition-number*:][*filename*]
4. **no**
5. **enable**
6. **configure terminal**
7. **secure boot-config** [**restore** *filename*]

8. **end**
9. **copy** *filename* **running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**reload** **例：** `Router# reload`	（任意）必要に応じて、ROM モニタ モードに入ります。
ステップ 2	**dir** [*filesystem*:] **例：** `rommon 1 > dir slot0:`	セキュアなブートセット ファイルを含むデバイスの内容を列挙します。 • デバイス名は、**show secure bootset** コマンドの出力内で見つけることができます。
ステップ 3	**boot** [*partition-number*:][*filename*] **例：** `rommon 2 > boot slot0:c3745-js2-mz`	セキュアなブートセット イメージを使用してルータを起動します。

ステップ 4	**no**
	
	例：
	`--- System Configuration Dialog ---`
	`Would you like to enter the initial configuration dialog? [yes/no]: no`
		（任意）セットアップ モードでインタラクティブ設定セッションに入ることを拒否します。
		• NVRAM が消去された場合は、ルータがセットアップ モードに入り、ユーザにインタラクティブ設定セッションを開始するように促します。

ステップ 5	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 6	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 7	**secure boot-config** [**restore** *filename*] **例：** `Router(config)# secure boot-config restore slot0:rescue-cfg`	セキュアな設定を指定されたファイル名に復元します。
ステップ 8	**end** **例：** `Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**copy** *filename* **running-config** **例：** `Router# copy slot0:rescue-cfg running-config`	復元された設定を実行設定にコピーします。

その他の参考資料

次の項で、Cisco IOS Resilient Configuration に関する参考資料を紹介します。

関連資料

内容	参照先
その他のコマンド：完全なコマンド構文、コマンドモード、デフォルト、使用上の注意事項、および例	『*Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.4T*』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能がサポートする新規 RFC または改訂 RFC はありません。また、この機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

Cisco IOS Resilient Configuration の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　Cisco IOS Resilient Configuration の機能情報

機能名	リリース	機能情報
Cisco IOS Resilient Configuration	12.3(8)T	Cisco IOS Resilient Configuration 機能で、実行中のイメージおよび設定のワーキング コピーを保護し維持することができます。これにより、イメージや設定ファイルが永続ストレージ（NVRAM やフラッシュ）の内容を消去する不正な攻撃に耐えることができます。 12.3(8)T で、この機能が導入されました。 **secure boot-config**、**secure boot-image**、および **show secure bootset** コマンドが導入または変更されました。

イメージ検証

イメージ検証機能を使用すると、Cisco IOS イメージの完全性を自動的に検証できます。そのため、ユーザは、イメージが偶発的な破壊から保護されていることを確認できます。破壊は、シスコによってファイルが作成された瞬間からユーザに届くまで、輸送中にいつでも起きる可能性があります。転送エラーやディスク破壊の結果、偶発的にイメージの完全性が破壊された場合に、ルータが自動的に検出できるようになるため、Cisco IOS ルータの効率も上がります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「イメージ検証の機能情報」（P.9）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

イメージ検証の制約事項

Cisco IOS Release 12.2(18)S および 12.0(26)S のみ

イメージ検証は、任意のファイルに適用され実行できますが、ファイルがイメージ ファイルでない場合、イメージ検証は実行されず、「SIGNATURE-NOT-FOUND」というエラーが表示されます。

Cisco IOS Release 12.3(4)T のみ

イメージ検証は、イメージ ファイルだけに適用されます。他のファイルタイプをコピーまたは検証した場合、イメージ検証が実行されたことを示す警告が表示されず、コマンド（コピーまたは検証）はメッセージを表示せずに成功します。

（注） イメージ検証機能は、Cisco IOS デバイスに格納されている Cisco IOS ソフトウェア イメージの完全性を確認するためにだけに使用できます。リモート ファイル システム上のイメージや、メモリ内で実行されているイメージの完全性を確認するためは使用できません。

イメージ検証に関する情報

イメージ検証の動作

実稼動イメージは、一連の転送を経てルータのメモリにコピーされるため、イメージの完全性が転送のたびに偶発的に破壊される危険があります。Cisco.com からイメージをダウンロードするとき、ユーザはダウンロードしたイメージに対して Message Digest 5（MD5; メッセージ ダイジェスト 5）ハッシュを実行し、Cisco.com で公開されている MD5 ダイジェストが、ユーザのサーバで計算した MD5 ダイジェストと同じであることを確認できます。しかし、MD5 ダイジェストが 128 ビット長であり、検証が手動であることから、多くのユーザは MD5 ダイジェストを実行しません。イメージ検証により、ユーザは、ダウンロードしたすべてのイメージの完全性を自動的に検証できるため、ユーザの操作が大幅に削減されます。

イメージ検証の使用方法

ここでは、次の各手順について説明します。

- 「イメージの完全性のグローバルな検証」（P.2）
- 「コピーしようとしているイメージの完全性の検証」（P.3）
- 「リロードしようとしているイメージの完全性の検証」（P.4）

イメージの完全性のグローバルな検証

file verify auto コマンドを使用すると、イメージの検証がグローバルにイネーブルになります。つまり、コピー（**copy** コマンドを使用）またはリロード（**reload** コマンドを使用）されるすべてのイメージが自動的に検証されます。**copy** コマンドと **reload** コマンドには、イメージの検証をイネーブルにする **/verify** キーワードがありますが、イメージをコピーまたはリロードするたびにキーワードを指定する必要があります。**file verify auto** コマンドを使用すると、デフォルトでイメージの検証がイネーブルになるため、イメージ検証を何度も指定する必要がなくなります。

デフォルトでイメージ検証をイネーブルにし、特定のイメージのコピーまたはリロードで検証をディセーブルにする場合は、**/noverify** キーワードを **copy** コマンドまたは **reload** コマンドで指定することで、**file verify auto** コマンドが上書きされます。

自動的なイメージ検証をイネーブルにするには、ここに示す手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **file verify auto**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**file verify auto** 例： `Router(config)# file verify auto`	自動的なイメージ検証をイネーブルにします。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。 イメージをコピーまたはリロードする場合は、グローバル コンフィギュレーション モードを終了する必要があります。

この次の手順

file verify auto コマンドを実行した後は、**/verify** キーワードを **copy** コマンドまたは **reload** コマンドで指定する必要はなくなります。これは、コピーまたはリロードされる各イメージが自動的に検証されるためです。

コピーしようとしているイメージの完全性の検証

copy コマンドを実行するとき、**/verify** キーワードを指定することで、コピーされるファイルの完全性を検証できます。完全性の確認に失敗した場合、コピーされたファイルは削除されます。コピーしようとしているファイルにハッシュが埋め込まれていない場合（古いイメージの場合）、コピー処理を続行するかどうかを質問されます。続行を選択すると、ファイルは正常にコピーされ、続行しないことを選択すると、コピーされたファイルが削除されます。

/verify キーワードを指定しないと、**copy** コマンドにより有効でないファイルがコピーされる可能性があります。そのため、**copy** コマンドを正常に実行した後、いつでも **verify** コマンドを実行して、ルータのストレージに格納されているファイルの完全性を確認できます。

ルータにコピーする前にイメージの完全性を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **copy** [**/erase**] [**/verify** | **/noverify**] *source-url destination-url*
3. **verify** [**/md5** [*md5-value*]] *filesystem*:[*file-url*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**copy** [**/erase**] [**/verify** | **/noverify**] *source-url destination-url* 例： `Router# copy /verify tftp://10.1.1.1/jdoe/c7200-js-mz disk0:`	コピー元からコピー先に任意のファイルをコピーします。 • **/verify**：コピー先のファイルのシグニチャを検証します。検証に失敗すると、ファイルは削除されます。 • **/noverify**：イメージをコピーする前にコピー先ファイルのシグニチャを検証しません。 （注） **/noverify** は、多くの場合、**file verify auto** コマンドがイネーブルになっており、コピーするすべてのイメージのシグニチャが自動的に検証される場合に使用されます。
ステップ 3	**verify** [**/md5** [*md5-value*]] *filesystem:*[*file-url*] 例： `Router# verify bootflash://c7200-kboot-mz.121-8a.E`	（任意）ルータのストレージに格納されているイメージの完全性を検証します。

リロードしようとしているイメージの完全性の検証

reload コマンドを **/verify** キーワード付きで実行することにより、システムにロードしようとしているイメージの完全性が確認されます。**/verify** キーワードを指定した場合、システムがリブートを開始する前にイメージの検証が実行されます。そのため、検証に失敗すると、イメージはロードされません。

（注） プラットフォームが異なれば、ロードするファイルの取得方法も異なるため、BOOTVAR で指定されたファイルが検証されます。ファイルが指定されていない場合、各サブシステム上の最初のファイルが検証されます。

プラットフォームによっては、設定レジスタなどの変数があるため、検証されるファイルがロードされるファイルになるとは限りません。

ルータにリロードする前にイメージの完全性を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **reload** [
   [**warm**] [**/verify** | **/noverify**] *text* |
   [**warm**] [**/verify** | **/noverify**] **in** [*hh*:]*mm* [*text*] | [**warm**] [**/verify** | **/noverify**] **at** *hh*:*mm* [*month day* | *day month*] [*text*] |
   [**warm**] [**/verify** | **/noverify**] **cancel**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**reload** [[**warm**] [**/verify** | **/noverify**] *text* | [**warm**] [**/verify** | **/noverify**] **in** [*hh*:]*mm* [*text*] | [**warm**] [**/verify** | **/noverify**] **at** *hh:mm* [*month day* | *day month*] [*text*] | [**warm**] [**/verify** | **/noverify**] **cancel**] 例： `Router# reload /verify`	オペレーティング システムをリロードします。 • **/verify**：コピー先のファイルのシグニチャを検証します。検証に失敗すると、ファイルは削除されます。 • **/noverify**：イメージをリロードする前にコピー先ファイルのシグニチャを検証しません。 （注） **/noverify** は、多くの場合、**file verify auto** コマンドがイネーブルになっており、コピーするすべてのイメージのシグニチャが自動的に検証される場合に使用されます。

イメージ検証の設定例

グローバル イメージ検証の例

次に、自動的なイメージ検証をイネーブルにする例を示します。このコマンドをイネーブルにした後、コピー（**copy** コマンドを使用）またはリロード（**reload** コマンドを使用）されるすべてのイメージに対し、イメージ検証が自動的に実行されます。

```
Router(config)# file verify auto
```

copy コマンドを使用したイメージ検証の例

次に、イメージをコピーする前にイメージ検証を指定する例を示します。

```
Router# copy /verify tftp://10.1.1.1/jdoe/c7200-js-mz disk0:

Destination filename [c7200-js-mz]?
Accessing tftp://10.1.1.1/jdoe/c7200-js-mz...
Loading jdoe/c7200-js-mz from 10.1.1.1 (via FastEthernet0/0):!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 19879944 bytes]

19879944 bytes copied in 108.632 secs (183003 bytes/sec)
Verifying file integrity of disk0:/c7200-js-mz
.................................................................................
.................................................................................
.................................................................................
.........................Done!
Embedded Hash MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash    MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash            MD5 :44A7B9BDDD9638128C35528466318183

Signature Verified
```

reload コマンドを使用したイメージ検証の例

次に、ルータにイメージをリロードする前にイメージ検証を指定する例を示します。

```
Router# reload /verify

Verifying file integrity of bootflash:c7200-kboot-mz.121-8a.E
%ERROR:Signature not found in file bootflash:c7200-kboot-mz.121-8a.E.
Signature not present. Proceed with verify? [confirm]
Verifying file disk0:c7200-js-mz
.....................................................................
.............................................................Done!
Embedded Hash   MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash   MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash        MD5 :44A7B9BDDD9638128C35528466318183
Signature Verified

Proceed with reload? [confirm]n
```

verify コマンドの出力例

次に、**verify** コマンドでイメージ検証を指定する例を示します。

```
Router# verify disk0:c7200-js-mz

%Filesystem does not support verify operations
Verifying file integrity of disk0:c7200-js-mz.......................................
.................................................................................Done!
Embedded Hash   MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash   MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash        MD5 :44A7B9BDDD9638128C35528466318183
```

Signature Verified

その他の参考資料

関連資料

内容	参照先
システム イメージのロード、メンテナンス、リブートに関する設定作業と情報	『*Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*, Release 12.4T』の「Using the Cisco IOS Integrated File System」フィーチャ モジュール
システム イメージをロード、メンテナンス、リブートするためのその他のコマンド	『*Cisco IOS Configuration Fundamentals Command Reference*, Release 12.4T』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
• なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

イメージ検証の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator により、どの Cisco IOS、Catalyst OS、および Cisco IOS XE ソフトウェア イメージが特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　イメージ検証の機能情報

機能名	リリース	機能情報
イメージ検証	12.2(25)S 12.0(26)S 12.3(4)T Cisco IOS XE Release 2.1	イメージ検証機能を使用すると、Cisco IOS イメージの完全性を自動的に検証できます。 次のコマンドが導入または変更されました。**copy**、**file verify auto**、**reload**、**verify**

IP ソース トラッカー

IP ソース トラッカー機能は、次の方法で情報を追跡します。

- 攻撃対象となっていることが疑われるホストに向けられているトラフィックに関する情報を収集します。
- Denial of Service（DoS; サービス拒否）攻撃のネットワーク入力点を追跡するため、必要なすべての情報を使いやすい形式で生成します。
- 同時に複数の IP を追跡します。
- ネットワーク全体で DoS 攻撃を追跡します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「IP ソース トラッカーの機能情報」（P.11）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

IP ソース トラッカーの制約事項

ルータの場合パケットがドロップされる可能性あり

IP ソース トラッキングは、ホストに対する攻撃を追跡するように設計されています。ラインカードまたはポート アダプタの CPU が過負荷になると、パケットがドロップされる可能性があります。そのため、ルータに対する攻撃を追跡するために IP ソース トラッキングを使用する場合、Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）アップデートなどの制御パケットがドロップされることがあります。

エンジン 0 および 1 のパフォーマンスが Cisco 12000 シリーズで影響を受ける

エンジン 2 およびエンジン 4 のラインカード上の追跡対象でない IP アドレス宛のパケットに対しては、パフォーマンスの影響はありません。これは、IP ソース トラッカーによって影響を受けるのは、追跡対象の宛先だけであるためです。エンジン 0 およびエンジン 1 では、すべてのパケットが CPU でスイッチングされるため、パフォーマンスが影響を受けます。

（注） Cisco 7500 シリーズ ルータでは、追跡対象でない宛先へのパフォーマンスの影響はありません。

IP ソース トラッカーに関する情報

ソース トラッキングを設定するには、次の概念について理解する必要があります。

- 「DoS 攻撃の識別と追跡」（P.2）
- 「IP ソース トラッカーの使用」（P.3）

DoS 攻撃の識別と追跡

今日のカスタマーが直面している多くの課題の 1 つに、サービス拒否（DoS）攻撃の追跡とブロックがあります。DoS 攻撃を抑制するには、侵入検知、ソース トラッキング、ブロッキングを行うことになります。この機能は、ソース トラッキングのニーズに対応します。

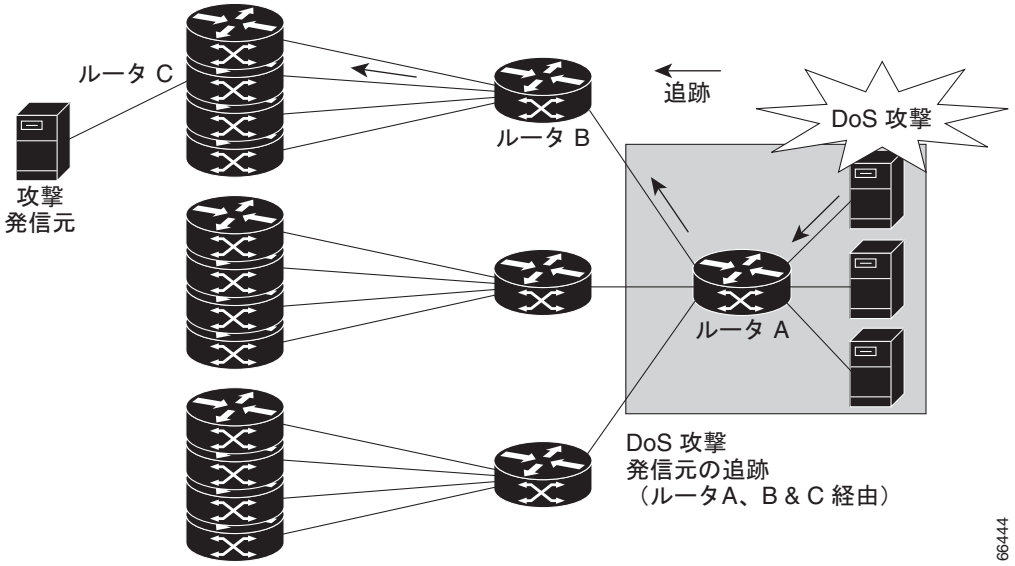
攻撃を追跡するには、NetFlow および Access Control List（ACL; アクセス コントロール リスト）が使用されてきました。攻撃をブロックするには、Committed Access Rate（CAR）と ACL が使用されてきました。Cisco 12000 シリーズ インターネット ルータ でのこれらの機能のサポートは、使用するラインカードの種類に依存してきました。Cisco 7500 シリーズ ルータでのこれらの機能のサポートは、使用するポート アダプタの種類に依存してきました。そのため、攻撃元を追跡し、すべてのラインカードとポート アダプタでサポートされている情報を取得する方法を開発する必要があります。

通常、DoS 攻撃を受けているホストを識別する場合、攻撃を効果的にブロックするためには、ネットワークの入力点を特定する必要があります。この処理は、ホストに最も近いルータで始まります。

たとえば、図 1 で、ルータ A から初めて、調査すべき次の上流のルータを特定します。従来から、ホストに接続されているインターフェイスに出力 ACL を適用し、ACL に一致するパケットをログに記録してきました。ロギング情報は、ルータ コンソールまたはシステム ログにダンプされます。その後、この情報を分析し、複数の ACL を次々と調べて、攻撃の入力インターフェイスを特定します。この例では、情報はルータ B を指しています。

次に、この処理をルータ B に対して繰り返し、ネットワークへの入力点であるルータ C にたどり着きます。この時点で、ACL または CAR を使用して攻撃をブロックできます。この手順では、分析用に大量の出力を生成する複数の ACL を適用することが必要な場合があり、手順が煩雑で、間違いを犯しやすくなります。

図 1　DoS 攻撃におけるソース トラッキング



IP ソース トラッカーの使用

IP ソース トラッカーは、DoS 攻撃を追跡するための、出力 ACL に対する、簡単でスケーラブルな代替手段となります。IP ソース トラッカーは次のように動作します。

- 攻撃対象の宛先を特定した後、**ip source-track** コマンドを入力することで、ルータ全体に対する宛先アドレスの追跡をイネーブルにします。
- 各ライン カードは、追跡対象の宛先アドレスに対し、特別な Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）エントリを作成します。パケット スイッチング用に特別な Application-Specific Integrated Circuit（ASIC; 特定用途向け集積回路）を使用するラインカードまたはポート アダプタの場合、CEF エントリを使用してパケットがラインカードまたはポート アダプタの CPU に送られます。
- 各ラインカードの CPU は、追跡対象の宛先に向かうトラフィックに関する情報を収集します。
- 生成されるデータは、定期的にルータにエクスポートされます。フロー情報の要約を表示するには、**show ip source-track summary** コマンドを入力します。各入力インターフェイスの詳細情報を表示するには、**show ip source-track** コマンドを入力します。
- 統計情報は、追跡対象の各 IP アドレスに対するトラフィックの詳細を示します。この詳細により、次にどの上流のルータを分析すべきかがわかります。現在のルータで IP ソース トラッカーを停止するには、**no ip source-track** コマンドを入力し、上流のルータで再度開始します。
- 攻撃元を特定するまで手順 1 ～ 5 を繰り返します。
- CAR または ACL を適用して攻撃を制限または停止します。

IP ソース トラッカーのハードウェア サポート

IP ソース トラッキングは、Cisco 12000 シリーズ インターネット ルータ のすべてのエンジン 0、1、2、および 4 のラインカードでサポートされています。また、Cisco 7500 シリーズ ルータ上の、CEF スイッチングがイネーブルになっているすべてのポート アダプタと RSP でサポートされています。

IP ソース トラッカーの設定方法

ここでは、次の各手順について説明します。

- 「IP ソース トラッキングの設定」（P.4）（必須）
- 「IP ソース トラッキングの確認」（P.5）（任意）

IP ソース トラッキングの設定

攻撃対象のホストに対して IP ソース トラッキングを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip source-track** *ip-address*
4. **ip source-track address-limit** *number*
5. **ip source-track syslog-interval** *number*
6. **ip source-track export-interval** *number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip source-track** *ip-address* **例：** `Router(config)# ip source-track 100.10.0.1`	指定したホストに対して IP ソース トラッキングをイネーブルにします。
ステップ 4	**ip source-track address-limit** *number* **例：** `Router(config)# ip source-track address-limit 10`	（任意）任意の時点で同時に追跡できるホストの数を制限します。 **（注）** このコマンドがイネーブルでない場合、追跡可能なホストの数に対する制限はありません。

	コマンドまたはアクション	目的
ステップ 5	**ip source-track syslog-interval** *number* 例： `Router(config)# ip source-track syslog-interval 2`	（任意）IP ソース トラッキングがイネーブルになっていることを示す syslog メッセージを生成するために使用する間隔を分単位で設定します。 **（注）** このコマンドがイネーブルでない場合、システム ログ メッセージは生成されません。
ステップ 6	**ip source-track export-interval** *number* 例： `Router(config)# ip source-track export-interval 30`	（任意）IP トラッキング統計情報をエクスポートするために使用する間隔を秒単位で設定します。ラインカードで収集された統計情報は Gigabit Route Processor（GRP）にエクスポートされ、ポート アダプタで収集された統計情報は Route Switch Processor（RSP）にエクスポートされます。 **（注）** このコマンドがイネーブルでない場合、トラフィック フロー情報は、30 秒ごとに GRP および RSP にエクスポートされます。

この次の手順

ネットワーク デバイスでソース トラッキングを設定した後、設定と、トラフィック フローなどのソース トラッキング統計情報を確認することができます。この作業を完了するには、「IP ソース トラッキングの確認」を参照してください。

IP ソース トラッキングの確認

パケット処理やトラフィック フロー情報などのソース トラッキングのステータスを確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show ip source-track** [*ip-address*] [**summary** | **cache**]
3. **show ip source-track export flows**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show ip source-track** [*ip-address*] [**summary** | **cache**] **例：** `Router# show ip source-track summary`	追跡対象 IP ホスト アドレスに対するトラフィック フロー統計情報を表示します。
ステップ 3	**show ip source-track export flows** **例：** `Router# show ip source-track export flows`	ラインカードからルート プロセッサにエクスポートされた最後の 10 個のパケット フローを表示します。 **（注）** このコマンドは、GRP や RSP などの分散プラットフォームだけで実行できます。

例

次に、**show ip source-track summary** コマンドの出力例を示します。この例は、1 台以上のホストに対して IP ソース トラッキングがイネーブルになっていることを確認する方法を示しています。

```
Router# show ip source-track summary

Address          Bytes    Pkts    Bytes/s   Pkts/s
10.0.0.1          119G   1194M    443535      4432
192.168.1.1       119G   1194M    443535      4432
192.168.42.42     119G   1194M    443535      4432
```

次に、**show ip source-track summary** コマンドの出力例を示します。この例は、追跡対象の宛先ホストに対して、まだトラフィックが受信されていないことを確認する方法を示しています。

```
Router# show ip source-track summary

Address        Bytes   Pkts   Bytes/s   Pkts/s
10.0.0.1           0      0         0        0
192.168.1.1        0      0         0        0
192.168.42.42      0      0         0        0
```

次に、**show ip source-track** コマンドの出力例を示します。この例は、IP ソース トラッキングがホストへのパケットを処理しており、ラインカードまたはポート アダプタからの統計情報を GRP および RSP にエクスポートしていることを確認する方法を示しています。

```
Router# show ip source-track

Address          SrcIF    Bytes   Pkts   Bytes/s   Pkts/s
10.0.0.1         PO0/0    119G   1194M    513009     5127
192.168.1.1      PO0/0    119G   1194M    513009     5127
192.168.42.42    PO0/0    119G   1194M    513009     5127
```

IP ソース トラッカーの設定例

ここでは、次の設定例について説明します。

IP ソース トラッキングの設定例

次に、ルータのすべてのラインカードとポート アダプタで IP ソース トラッキングを設定する例を示します。この例で、各ラインカードとポート アダプタは、ホスト アドレス 100.10.0.1 へのトラフィック フロー データを 2 分間収集してから、内部的なシステム ログ エントリを作成します。システム ログに記録されるパケットおよびフロー 情報は、表示用にルート プロセッサまたはスイッチ プロセッサに 60 秒ごとにエクスポートされます。

```
Router# configure interface
Router(config)# ip source-track 100.10.0.1
Router(config)# ip source-track syslog-interval 2
Router(config)# ip source-track export-interval 60
```

追跡対象のすべての IP アドレスに対する送信元インターフェイス統計情報を確認する例

次に、追跡対象ホスト アドレスに対する各送信元インターフェイス上で収集したトラフィック フロー統計情報の要約の例を示します。

```
Router# show ip source-track

Address         SrcIF     Bytes    Pkts     Bytes/s     Pkts/s
10.0.0.1        PO2/0         0       0           0          0
192.168.9.9     PO1/2      131M    511M        1538          6
192.168.9.9     PO2/0      144G   3134M     6619923     143909
```

すべての追跡対象 IP アドレスに対するフロー統計情報の要約の確認例

次に、追跡対象のすべてのホストに対するトラフィック フロー統計情報の例を示します。この例は、まだトラフィックを受信していないことを示しています。

```
Router# show ip source-track summary

Address              Bytes    Pkts     Bytes/s     Pkts/s
10.0.0.1                 0       0           0          0
100.10.1.1            131M    511M        1538          6
192.168.9.9           146G   3178M     6711866     145908
```

ラインカードで収集された詳細なフロー統計情報の確認例

次に、すべての追跡対象ホストに対する、ラインカード 0 上で収集されたトラフィック フロー情報の例を示します。

```
Router# exec slot 0 show ip source-track cache

========= Line Card (Slot 0) =======

IP packet size distribution (7169M total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 0.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  1 active, 4095 inactive, 13291 added
  198735 ager polls, 0 flow alloc failures
  Active flows timeout in 0 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow

SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
PO0/0          101.1.1.0       Null           100.1.1.1       06 00  00      55K
0000 /0  0                     0000 /0  0     0.0.0.0               100    10.1
```

ラインカードとポート アダプタからエクスポートされたフロー統計情報の確認例

次に、ラインカードとポート アダプタから GRP および RSP にエクスポートされたパケット フロー情報を表示する例を示します。

```
Router# show ip source-track export flows

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
PO0/0         101.1.1.0       Null          100.1.1.1       06 0000 0000    88K
PO0/0         101.1.1.0       Null          100.1.1.3       06 0000 0000    88K
PO0/0         101.1.1.0       Null          100.1.1.2       06 0000 0000    88K
```

その他の参考資料

ここでは、IP ソース トラッカーに関する関連資料について説明します。

関連資料

内容	参照先
ACL	『*Cisco IOS Security Configuration Guide: Securing the Data Plane*, Release 12.4T』
ダイナミック ACL	『Configuring Lock-and-Key Security (Dynamic Access Lists)』
DoS 防御	『Configuring TCP Intercept (Preventing Denial-of-Service Attacks)』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

IP ソース トラッカーの機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　IP ソース トラッカーの機能情報

機能名	リリース	機能情報
IP ソース トラッカー	12.0(21)S 12.0(22)S 12.0(26)S 12.3(7)T 12.2(25)S	IP ソース トラッカー機能を使用すると、攻撃対象となっていることが疑われるホストに向けられているトラフィックに関する情報を収集できます。 この機能は、リリース 12.0(21)S で、Cisco 12000 シリーズに導入されました。 この機能は、リリース 12.0(22)S で、Cisco 7500 シリーズに実装されました。 この機能は、リリース 12.0(26)S で、Cisco 12000 シリーズ IP Service Engine（ISE）ラインカードに実装されました。 この機能は、Cisco IOS Release 12.3(7)T に統合されました。 この機能は、Cisco IOS Release 12.2(25)S に統合されました。 次のコマンドが導入または変更されました。**ip source-track**、**ip source-track address-limit**、**ip source-track export-interval**、**ip source-track syslog-interval**、**show ip source-track**、**show ip source-track export flows**

ロールベースの CLI アクセス

ロールベースの CLI アクセス機能を使用すれば、ネットワーク管理者は「ビュー」を定義できます。ビューは、Cisco IOS EXEC コマンドおよびコンフィギュレーション（config）モード コマンドへのアクセスを精選したり部分的に制限する、操作コマンドと設定機能のセットです。ビューは、Cisco IOS Command-Line Interface（CLI; コマンドライン インターフェイス）と設定情報へのユーザ アクセスを制限します。つまり、ビューは、どのコマンドを受け入れて、どの設定情報を表示するかを定義できます。したがって、ネットワーク管理者はシスコ ネットワーキング デバイスへのアクセスを柔軟に管理できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「ロールベースの CLI アクセスの機能情報」（P.14）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

ロールベースの CLI アクセスの前提条件

イメージで CLI ビューをサポートする必要があります。

ロールベースの CLI アクセスの制約事項

合法的傍受イメージの制限

CLI ビューは Cisco IOS パーサーの一部であるため、すべてのプラットフォームと Cisco IOS イメージの一部でもあります。ただし、合法的傍受ビューは、合法的傍受サブシステムが組み込まれたイメージ内でしか使用できません。

許可されたビューの最大数

1 つの合法的傍受ビューを含む CLI ビューとスーパービューの設定可能な最大数は 15 です（これには、ルート ビューは含まれません）。

ロールベースの CLI アクセスに関する情報

CLI ビューを使用するメリット

ビュー：詳細なアクセス コントロール

ユーザは権限レベルとイネーブル モード パスワードの両方を介して CLI アクセスを制御できますが、これらの機能では、ネットワーク管理者に Cisco IOS ルータとスイッチを操作するのに必要な詳細レベルが提供されません。CLI ビューは、より詳細なアクセス コントロール機能をネットワーク管理者に提供するため、Cisco IOS ソフトウェア全体のセキュリティとアカウンタビリティが向上します。

Cisco IOS Release 12.3(11)T 以降では、ネットワーク管理者が、ビューへのインターフェイスまたはインターフェイス グループを指定することもできます。そのため、指定されたインターフェイスに基づくアクセスが可能になります。

ルート ビュー

システムが「ルート ビュー」になっている場合は、レベル 15 権限を持つユーザとして、すべてのアクセス権限が付与されます。管理者がシステムのビュー（CLI ビュー、スーパービュー、合法的傍受ビューなど）を設定する場合は、システムをルート ビューにする必要があります。

レベル 15 権限を持つユーザとルート ビュー ユーザの違いは、ルート ビュー ユーザは、新しいビューを設定したり、ビューに対してコマンドを追加または削除したりできることです。また、CLI ビューでは、ルート ビュー ユーザがそのビューに追加したコマンドにしかアクセスできません。

合法的傍受ビューについて

CLI ビューと同様に、合法的傍受ビューは、特定のコマンドと設定情報へのアクセスを制限します。具体的には、合法的傍受ビューを使用すれば、ユーザは、コールとユーザに関する情報を保存する Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）コマンドの特別なセットである TAP-MIB 内に保持された合法的傍受コマンドへのアクセスを保護できます。

合法的傍受ビュー内で使用可能なコマンドは、次のカテゴリのいずれかに属します。

- 他のビューまたは権限レベルでは使用不可にすべき合法的傍受コマンド
- 合法的傍受ユーザにとっては有効であるが、他のビューまたは権限レベルから除外する必要のない CLI ビュー

スーパービューについて

スーパービューは、1 つ以上の CLI ビューで構成されています。このビューでは、受け入れるコマンドと表示する設定情報を定義できます。スーパービューを使用すれば、ネットワーク管理者は、複数の CLI ビューをユーザ グループに割り当てなくても、設定された CLI ビュー内のすべてのユーザをスーパービューに割り当てることができます。

スーパービューには次の特性があります。

- CLI ビューを複数のスーパービュー間で共有できます。
- スーパービューにはコマンドを設定できません。つまり、CLI ビューにコマンドを追加してから、その CLI ビューをスーパービューに追加する必要があります。
- スーパービューにログインしたユーザは、そのスーパービューに属している CLI ビューに設定されたすべてのコマンドにアクセスできます。
- スーパービューごとにパスワードが設定されます。このパスワードは、スーパービューを切り替えたり、CLI ビューからスーパービューに切り替えたりするために使用されます。
- スーパービューが削除された場合は、そのスーパービューに関連付けられたすべての CLI ビューも削除されます。

ビュー認証と新しい AAA アトリビュート

ビュー認証は、新しいアトリビュートの「cli-view-name」を介して、外部の Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）サーバで実行されます。

AAA 認証は特定のユーザに 1 つのビュー名のみを関連付けます。つまり、認証サーバ内の 1 人のユーザに対して 1 つのビュー名しか設定できません。

ロールベースの CLI アクセスの使用方法

- 「CLI ビューの設定」（P.4）（必須）
- 「合法的傍受ビューの設定」（P.6）（任意）
- 「スーパービューの設定」（P.7）（任意）
- 「ビューとビュー ユーザのモニタリング」（P.9）（任意）

CLI ビューの設定

このタスクを実行して、CLI ビューを作成し、必要に応じて、コマンドまたはインターフェイスをビューに追加します。

前提条件

ビューを作成する前に、次のタスクを実行する必要があります。

- **aaa new-model** コマンド経由で AAA を有効にします。
- システムが権限レベル 15 ではなく、ルート ビューになっていることを確認します。

手順の概要

1. **enable view**
2. **configure terminal**
3. **parser view** *view-name*
4. **secret 5** *encrypted-password*
5. **commands** *parser-mode* {**include** | **include-exclusive** | **exclude**} [**all**] [**interface** *interface-name* | *command*]
6. **exit**
7. **exit**
8. **enable** [*privilege-level*] [**view** *view-name*]
9. **show parser view** [**all**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable view** 例： `Router> enable view`	ルート ビューを有効にします。 • プロンプトが表示されたら、権限レベル 15 パスワード（ルート パスワードなど）を入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parser view** *view-name* 例： `Router(config)# parser view first`	ビューを作成して、ビュー コンフィギュレーション モードに入ります。
ステップ 4	**secret 5** *encrypted-password* 例： `Router(config-view)# secret 5 secret`	CLI ビューまたはスーパービューとパスワードを関連付けます。 （注） このコマンドを発行しなければ、ビューのその他のアトリビュートが設定できません。

	コマンドまたはアクション	目的
ステップ 5	**commands** *parser-mode* {**include** | **include-exclusive** | **exclude**} [**all**] [**interface** *interface-name* | *command*] **例：** `Router(config-view)# commands exec include show version`	ビューにコマンドまたはインターフェイスを追加します。 • *parser-mode*：指定されたコマンドが存在するモード • **include**：ビューにコマンドまたはインターフェイスを追加して、新しいビューに同じコマンドまたはインターフェイスを追加できるようにします。 • **include-exclusive**：ビューにコマンドまたはインターフェイスを追加して、同じコマンドまたはインターフェイスを他のビューに追加できないようにします。 • **exclude**：ビューからコマンドまたはインターフェイスを除外します。つまり、顧客はコマンドまたはインターフェイスにアクセスできません。 • **all**：同じキーワードで始まる特定のコンフィギュレーション モード内のすべてのコマンド、またはビューの一部として指定されたインターフェイスのすべてのサブインターフェイスを許可する「ワイルドカード」 • **interface** *interface-name*：ビューに追加されたインターフェイス • *command*：ビューに追加されたコマンド
ステップ 6	**exit** **例：** `Router(config-view)# exit`	ビュー コンフィギュレーション モードを終了します。
ステップ 7	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 8	**enable** [*privilege-level*] [**view** *view-name*] **例：** `Router# enable view first`	ユーザにパスワードの入力を要求します。このパスワードは、設定された CLI ビューへのアクセスをユーザに許可し、ビュー間の切り替えに使用されます。 正しいパスワードが入力されたら、ユーザはビューにアクセスできます。
ステップ 9	**show parser view** [**all**] **例：** `Router# show parser view`	（任意）ユーザが現在使用しているビューに関する情報を表示します。 • **all**：ルータ上で設定されたすべてのビューに関する情報を表示します。 **（注）** このコマンドはルート ユーザと合法的傍受ユーザの両方が使用できますが、**all** キーワードはルート ユーザしか使用できません。ただし、**all** キーワードは、ルート ビュー内のユーザが、合法的傍受ビューや CLI ビュー内のユーザに使用を許可するように設定できます。

トラブルシューティングのヒント

ビューが正常に作成されたら、次のようなシステム メッセージが表示されます。

```
%PARSER-6-VIEW_CREATED: view 'first' successfully created.
```

ビューが正常に削除されたら、次のようなシステム メッセージが表示されます。

%PARSER-6-VIEW_DELETED: view "first" successfully deleted.

パスワードとビューを関連付ける必要があります。パスワードを関連付けずに、**commands** コマンド経由でビューにコマンドを追加しようとすると、次のようなシステム メッセージが表示されます。

```
%Password not set for view <viewname>.
```

合法的傍受ビューの設定

このタスクを実行して、ビューを初期化し、合法的傍受固有のコマンドと設定情報用に設定します

前提条件

合法的傍受ビューを初期化する前に、**privilege** コマンド経由で権限レベルが 15 に設定されていることを確認します。

制約事項

レベル 15 権限を持っている管理者またはユーザだけが合法的傍受ビューを初期化できます。

手順の概要

1. **enable view**
2. **configure terminal**
3. **li-view** *li-password* **user** *username* **password** *password*
4. **username** [**lawful-intercept**] *name* [**privilege** *privilege-level* | **view** *view-name*] **password** *password*
5. **parser view** *view-name*
6. **secret 5** *encrypted-password*
7. **name** *new-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable view** **例：** `Router> enable view`	ルート ビューを有効にします。 • プロンプトが表示されたら、権限レベル 15 パスワード（ルート パスワードなど）を入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**li-view** *li-password* **user** *username* **password** *password* **例：** `Router(config)# li-view lipass user li_admin password li_adminpass`	合法的傍受ビューを初期化します。 li-view が初期化されたら、**user** *username* **password** *password* options 経由で少なくとも 1 人のユーザを指定する必要があります。
ステップ 4	**username** [**lawful-intercept** [*name*] [**privilege** *privilege-level* | **view** *view-name*] **password** *password* **例：** `Router(config)# username lawful-intercept li-user1 password li-user1pass`	シスコ デバイス上で合法的傍受ユーザを設定します。
ステップ 5	**parser view** *view-name* **例：** `Router(config)# parser view li view name`	（任意）ビュー コンフィギュレーション モードに入ります。このモードでは、合法的傍受ビューのパスワードや名前を変更できます。
ステップ 6	**secret 5** *encrypted-password* **例：** `Router(config-view)# secret 5 secret`	（任意）合法的傍受ビューの既存のパスワードを変更します。
ステップ 7	**name** *new-name* **例：** `Router(config-view)# name second`	（任意）合法的傍受ビューの名前を変更します。 このコマンドが発行されなかった場合、合法的傍受ビューのデフォルト名は「li-view」になります。

トラブルシューティングのヒント

合法的傍受ビューにアクセス可能なすべてのユーザに関する情報を表示するには、**show users lawful-intercept** コマンドを発行します（このコマンドは、認可された合法的傍受ビュー ユーザしか使用できません）。

スーパービューの設定

このタスクを実行して、スーパービューを設定し、スーパービューに少なくとも 1 つの CLI ビューを追加します。

前提条件

CLI ビューをスーパービューに追加する前に、スーパービューに追加する CLI ビューがシステム内で有効なビューであることを確認します。つまり、ビューが、**parser view** コマンド経由で正常に作成されたことを確認します。

制約事項

スーパービューにビューを追加するには、スーパービューに対してパスワードを設定する必要があります（**secret 5** コマンド経由）。その後で、ビュー コンフィギュレーション モードで **view** コマンドを発行して、少なくとも 1 つの CLI ビューをスーパービューに追加します。

手順の概要

1. **enable view**
2. **configure terminal**
3. **parser view** *superview-name* **superview**
4. **secret 5** *encrypted-password*
5. **view** *view-name*
6. **exit**
7. **exit**
8. **show parser view** [**all**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable view** 例： `Router> enable view`	ルート ビューを有効にします。 • プロンプトが表示されたら、権限レベル 15 パスワード（ルート パスワードなど）を入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parser view** *superview-name* **superview** 例： `Router(config)# parser view su_view1 superview`	スーパービューを作成して、ビュー コンフィギュレーション モードに入ります。
ステップ 4	**secret 5** *encrypted-password* 例： `Router(config-view)# secret 5 secret`	CLI ビューまたはスーパービューとパスワードを関連付けます。 （注） このコマンドを発行しなければ、ビューのその他のアトリビュートが設定できません。
ステップ 5	**view** *view-name* 例： `Router(config-view)# view view_three`	正常な CLI ビューをスーパービューに追加します。 特定のスーパービューに追加する各 CLI ビューに対して、このコマンドを発行します。

	コマンドまたはアクション	目的
ステップ 6	**exit** **例：** `Router(config-view)# exit`	ビュー コンフィギュレーション モードを終了します。
ステップ 7	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 8	**show parser view** [**all**] **例：** `Router# show parser view`	（任意）ユーザが現在使用しているビューに関する情報を表示します。 • **all**：ルータ上で設定されたすべてのビューに関する情報を表示します。 **（注）** このコマンドはルート ユーザと合法的傍受ユーザの両方が使用できますが、**all** キーワードはルート ユーザしか使用できません。ただし、**all** キーワードは、ルート ビュー内のユーザが、合法的傍受ビューや CLI ビュー内のユーザに使用を許可するように設定できます。

ビューとビュー ユーザのモニタリング

すべてのビュー（ルート、CLI、合法的傍受、およびスーパー）に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug parser view** コマンドを使用します。

ロールベースの CLI アクセスの設定例

例：CLI ビューの設定

次の例は、"first" と "second" の 2 つの CLI ビューの設定方法を示しています。その後で、実行設定内で CLI ビューを確認できます。

```
Router(config)# parser view first
00:11:40:%PARSER-6-VIEW_CREATED:view 'first' successfully created.
Router(config-view)# secret 5 firstpass
Router(config-view)# command exec include show version
Router(config-view)# command exec include configure terminal
Router(config-view)# command exec include all show ip
Router(config-view)# exit
Router(config)# parser view second
00:13:42:%PARSER-6-VIEW_CREATED:view 'second' successfully created.
Router(config-view)# secret 5 secondpass
Router(config-view)# command exec include-exclusive show ip interface
```

```
Router(config-view)# command exec include logout
Router(config-view)# exit
!
!
Router(config-view)# do show run | beg view
parser view first
 secret 5 $1$MCmh$QuZaU8PIMPlff9sFCZvgW/
 commands exec include configure terminal
 commands exec include configure
 commands exec include all show ip
 commands exec include show version
 commands exec include show
!
parser view second
 secret 5 $1$iP2M$R16BXKecMEiQesxLyqygW.
 commands exec include-exclusive show ip interface
 commands exec include show ip
 commands exec include show
 commands exec include logout
!
```

例：CLI ビューの確認

CLI ビューの "first" と "second" を設定したら、**enable view** コマンドを発行して、各ビュー内で使用可能なコマンドを確認できます。次の例は、ユーザが CLI ビューの "first" にログイン後に、どのコマンドがこのビュー内で使用可能かを示しています（**show ip** コマンドは all オプションと一緒に設定されているため、second ビュー内で include-exclusive キーワードを使用している **show ip interface** コマンドを除く、すべてのサブオプションのセットが表示されます）。

```
Router# enable view first
Password:

00:28:23:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
Router# ?
Exec commands:
  configure  Enter configuration mode
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  show       Show running system information

Router# show ?

  ip       IP information
  parser   Display parser information
  version  System hardware and software status

Router# show ip ?

  access-lists            List IP access lists
  accounting              The active IP accounting database
  aliases                 IP alias table
  arp                     IP ARP table
  as-path-access-list     List AS path access lists
  bgp                     BGP information
  cache                   IP fast-switching route cache
  casa                    display casa information
  cef                     Cisco Express Forwarding
  community-list          List community-list
  dfp                     DFP information
  dhcp                    Show items in the DHCP database
  drp                     Director response protocol
```

```
  dvmrp                   DVMRP information
  eigrp                   IP-EIGRP show commands
  extcommunity-list       List extended-community list
  flow                    NetFlow switching
  helper-address          helper-address table
  http                    HTTP information
  igmp                    IGMP information
  irdp                    ICMP Router Discovery Protocol
.
.
.
```

例：合法的傍受ビューの設定

次の例は、合法的傍受ビューの設定方法、ビューへのユーザの追加方法、および追加されたユーザの確認方法を示しています。

```
!Initialize the LI-View.
Router(config)# li-view lipass user li_admin password li_adminpass
00:19:25:%PARSER-6-LI_VIEW_INIT:LI-View initialized.
Router(config)# end

! Enter the LI-View; that is, check to see what commands are available within the view.
Router# enable view li-view
Password:

Router#
00:22:57:%PARSER-6-VIEW_SWITCH:successfully set to view 'li-view'.
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# parser view li-view
Router(config-view)# ?
View commands:
  commands  Configure commands for a view
  default   Set a command to its defaults
  exit      Exit from view configuration mode
  name      New LI-View name      ===This option only resides in LI View.
  no        Negate a command or set its defaults
  password  Set a password associated with CLI views

Router(config-view)#

! NOTE:LI View configurations are never shown as part of ‘running-configuration’.

! Configure LI Users.
Router(config)# username lawful-intercept li-user1 password li-user1pass
Router(config)# username lawful-intercept li-user2 password li-user2pass

! Displaying LI User information.
Router# show users lawful-intercept

li_admin
li-user1
li-user2
Router#
```

例：スーパービューの設定

次の **show running-config** コマンドのサンプル出力は、"view_one" と "view_two" がスーパービューの "su_view1" に追加され、"view_three" と "view_four" がスーパービューの "su_view2" に追加されていることを示しています。

```
!
parser view su_view1 superview
 secret 5 <encoded password>
 view view_one
 view view_two
!
parser view su_view2 superview
 secret 5 <encoded password>
 view view_three
 view view_four
!
```

その他の参考資料

関連資料

内容	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
SNMP、MIB、CLI 設定	『*Cisco IOS Network Management Configuration Guide*, Release 15.0』
権限レベル	「Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices」モジュール

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ロールベースの CLI アクセスの機能情報

表 1 に、この機能のリリース履歴を示します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　ロールベースの CLI アクセスの機能情報

機能名	リリース	機能情報
ロールベースの CLI アクセス	12.3(7)T 12.3(11)T 12.2(33)SRB 12.2(33)SB 12.2(33)SXI Cisco IOS XE 3.1.0SG	この機能は、ネットワーク管理者が、CLI と設定情報へのユーザ アクセスを制限できるようにします。 12.3(11)T で、インターフェイス単位レベルでユーザ アクセスを制限するように CLI ビュー機能が拡張され、拡張されたビュー機能をサポートするために新しい CLI ビューが導入されました。また、設定された CLI ビューをスーパービューにグループ分けするためのサポートが導入されました。 • **commands (view)**、**enable**、**i-view**、**name (view)**、**parser view**、**parser view superview**、**secret**、**show parser view**、**show users**、**username**、および **view** の各コマンドが導入または変更されました。