アイデンティティ ポリシーの設定

IEEE 802.1x 規格では、クライアントサーバ ベースのアクセス コントロールとしての 802.1x ポートベース認証と、未認可のクライアントがパブリック ポート経由で LAN に接続することを制限する認証プロトコルを規定しています。認証サーバは、インターフェイスに接続された各クライアントを検証してから、ルータまたは LAN により提供されたサービスを使用可能にします。

クライアントが認証されるまでは、802.1x アクセス コントロールにより、クライアントの接続先のインターフェイスを介した Extensible Authentication Protocol over LAN（EAPOL）トラフィックだけが許可されます。認証が成功すると、通常のトラフィックはそのインターフェイスを通過できるようになります。

802.1x 認証は VPN アクセス コントロールを提供します。この場合、未認証のトラフィックはインターネットにはアクセスできますが、VPN トンネルにはアクセスできません。企業の社員が、他の家族会員がインターネットへのアクセスに使用するホーム アクセス ルータを介して企業 VPN にアクセスする場合は、特にこのソリューションが役立ちます。802.1x を使用する場合、仮想インターフェイスを作成して、未認証トラフィックを伝送します。認証済みトラフィックは引き続き物理インターフェイスを通過します。

802.1x では、DHCP を使用して、認証を要求するクライアントに IP アドレスを提供する必要があります。認証済みトラフィック用と未認証トラフィック用に 1 つずつ、2 つの IP アドレス プールを使用することを推奨します。2 つのプールを使用する場合、企業 DHCP プール内の DNS サーバが企業 DNS サーバを指している必要があります。企業以外の DHCP プールの DNS サーバは、パブリック インターフェイス上の ISP により提供された DNS サーバを使用する必要があります。DHCP を設定するには、DHCP ポリシーを選択します。

Cisco IOS ルータでの 802.1x

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

IEEE 802.1x 規格では、クライアントサーバ ベースのアクセス コントロールとしての 802.1x ポートベース認証と、未認可のクライアントがパブリック ポート経由で LAN に接続することを制限する認証プロトコルを規定しています。認証サーバは、インターフェイスに接続された各クライアントを検証してから、ルータまたは LAN により提供されたサービスを使用可能にします。

クライアントが認証されるまでは、802.1x アクセス コントロールにより、クライアントの接続先のインターフェイスを介した Extensible Authentication Protocol over LAN（EAPOL）トラフィックだけが許可されます。認証が成功すると、通常のトラフィックはそのインターフェイスを通過できるようになります。

802.1x 認証は VPN アクセス コントロールを提供します。この場合、未認証のトラフィックはインターネットにはアクセスできますが、VPN トンネルにはアクセスできません。企業の社員が、他の家族会員がインターネットへのアクセスに使用するホーム アクセス ルータを介して企業 VPN にアクセスする場合は、特にこのソリューションが役立ちます。802.1x を使用する場合、仮想インターフェイスを作成して、未認証トラフィックを伝送します。認証済みトラフィックは引き続き物理インターフェイスを通過します。

802.1x では、DHCP を使用して、認証を要求するクライアントに IP アドレスを提供する必要があります。認証済みトラフィック用と未認証トラフィック用に 1 つずつ、2 つの IP アドレス プールを使用することを推奨します。2 つのプールを使用する場合、企業 DHCP プール内の DNS サーバが企業 DNS サーバを指している必要があります。企業以外の DHCP プールの DNS サーバは、パブリック インターフェイス上の ISP により提供された DNS サーバを使用する必要があります。DHCP を設定するには、DHCP ポリシーを選択します。詳細については、Cisco IOS ルータにおける DHCPを参照してください。

（注） 802.1x は、Cisco 800、1700、1800、1900、2600、2800、2900、3600、3700、3800、3900 シリーズ ルータのプラットフォームでサポートされます。

802.1x の詳細については、次の項を参照してください。

- 802.1x デバイス ロールについて （3 ページ）
- 802.1x インターフェイス認可状態 （3 ページ）
- 802.1x でサポートされるトポロジ （4 ページ）
- 802.1x ポリシーの定義 （5 ページ）

802.1x デバイス ロールについて

802.1x ポートベース認証では、次のデバイス ロールが使用されます。

- クライアント：VPN へのアクセスを要求しているワークステーション。このクライアントでは、Microsoft Windows XP オペレーティング システムで提供されるような、802.1x 準拠クライアント ソフトウェアが実行されている必要があります。
- 認証サーバ：クライアントを認証します。認証サーバーは、クライアントのアイデンティティを検証し、クライアントがネットワークへのアクセスを認可されているかどうかをルータに通知します。サポートされている認証サーバは、EAP 拡張機能付きの Remote Authentication Dial-In User Service（RADIUS）セキュリティ システムだけです。Security Manager では、AAA サーバ オブジェクトで定義されているように、AAA（認証、許可、アカウンティング）サーバが 802.1x ポリシー用の認証サーバです。
- ルータ（エッジルータまたはワイヤレスアクセスポイント）：クライアントの認証ステータスに基づいてネットワークへの物理アクセスを制御します。ルータは、クライアントと認証サーバの中間（プロキシ）です。クライアントからのアイデンティティ情報を要求し、認証サーバを使用してその情報を検証し、応答をクライアントにリレーします。Security Manager では、802.1x ポリシーを設定するルータがスイッチとして機能します。

関連項目

- 802.1x インターフェイス認可状態　（3 ページ）
- 802.1x でサポートされるトポロジ　（4 ページ）
- 802.1x ポリシーの定義　（5 ページ）
- Cisco IOS ルータでの 802.1x　（2 ページ）

802.1x インターフェイス認可状態

802.1x を使用する場合、クライアント ネットワーク アクセスが許可されるかどうかは、インターフェイス状態によって決まります。デフォルトでは、インターフェイスは未認可状態で開始されます。インターフェイスがこの状態の間は、EAPOL パケットを除き、両方向のすべてのトラフィックが禁止されます。クライアントが認証されると、インターフェイスは認可済み状態に移行し、すべてのクライアント トラフィックを正常に伝送できるようになります。

802.1x がサポートされていないクライアントが未認可の 802.1x インターフェイスに接続する場合、ルータはクライアントのアイデンティティを要求します。この状況ではクライアントは要求に応答せず、インターフェイスは未認可状態のままであり、クライアントはネットワークへのアクセスを許可されません。これに対し、802.1x 対応のクライアントが、802.1x プロトコルを実行していないインターフェイスに接続される場合、クライアントでは、EAPOL-Start フレームを送信することによって認証プロセスを開始します。応答を受信できない場合、クライアントは要求を一定の回数送信します。応答を受信できないため、クライアントは、インターフェイスが未認可状態のときと同様にフレームの送信を開始します。

次のいずれかのオプションを選択することにより、インターフェイス認可状態を制御できます。

- [Auto]：802.1x 認証をイネーブルにします。この場合、インターフェイスは未認可状態で開始されます。EAPOL フレームだけが、インターフェイスを介して送受信されます。インターフェイスのリンク状態が down から up に移行したとき、または EAPOL-Start フレームが受信されると、認証が開始されます。ルータはクライアントのアイデンティティを要求し、クライアントと認証サーバー間で認証メッセージのリレーを開始します。ルータは、ネットワークにアクセスしようとする各クライアントの MAC アドレスを、一意のクライアント識別子として使用します。
- [Force authorized]：802.1x 認証をディセーブルにします。この場合、インターフェイスはクライアントを認証せずに認可済み状態に移行します。

クライアントの認証が正常に完了すると、インターフェイス状態が認可済みに変わります。これにより、クライアントからのすべてのフレームがネットワークに入ることができます。認証に失敗した場合、インターフェイスは未認可状態のままになりますが、認証は再試行できます。認証サーバに到達できない場合、ルータは要求を再送信できます。定義された回数試行したあとも認証サーバが応答しない場合、認証は失敗し、クライアントに対してネットワークアクセスが拒否されます。

クライアントはログオフするとき、EAPOL-Logoff メッセージを送信します。これにより、インターフェイスは未認可状態に戻ります。

関連項目

- 802.1x デバイス ロールについて （3 ページ）
- 802.1x でサポートされるトポロジ （4 ページ）
- 802.1x ポリシーの定義 （5 ページ）
- Cisco IOS ルータでの 802.1x （2 ページ）

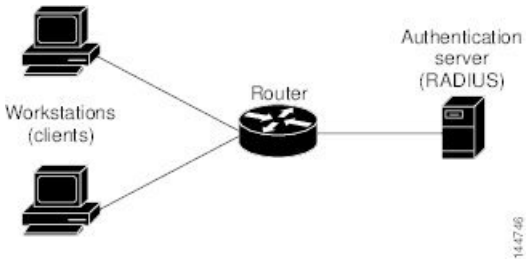
802.1x でサポートされるトポロジ

802.1x ポートベース認証では、次の 2 つのトポロジがサポートされます。

- ポイントツーポイント
- Wireless LAN（ワイヤレス LAN）

ポイントツーポイント設定では、1 つだけのクライアントを 802.1x 対応インターフェイスに接続できます。インターフェイス状態が down から up に変わると、ルータはクライアントを検出します。クライアントがネットワークを出ると、または別のクライアントに置き換えられると、インターフェイス状態が up から down に変わります。これにより、インターフェイスは未認可状態に戻ります。

図 *1 : 802.1x* トポロジ



ワイヤレス LAN 設定においては、802.1x インターフェイスはマルチホスト モードで設定され、1 つのクライアントが認証されるとすぐに認可されます。インターフェイスが認可されると、そのインターフェイスに間接的に接続されている他のすべてのクライアントに対してネットワークへのアクセスが許可されます。（再認証が失敗したか、または EAPOL-Logoff メッセージが受信されたかのいずれかの理由で）ポートが未認可になると、ルータは、接続されているすべてのクライアントに対してネットワークへのアクセスを拒否します。このトポロジでは、ワイヤレス アクセス ポイントがルータへのクライアントとなり、接続されているクライアントを認証します。

関連項目

- 802.1x デバイス ロールについて （3 ページ）
- 802.1x インターフェイス認可状態 （3 ページ）
- 802.1x ポリシーの定義 （5 ページ）
- Cisco IOS ルータでの 802.1x （2 ページ）

802.1x ポリシーの定義

802.1x ポリシーを設定するには、次のものを定義します。

- ネットワークへの接続を試行しているホストを認証する AAA サーバが含まれる AAA サーバ グループ。
- 未認証のトラフィックを伝送する仮想インターフェイスと、認証済みのトラフィックを伝送する物理インターフェイス。
- （任意）物理インターフェイスのプロパティ。コントロール タイプ、自動再認証、および複数のタイムアウト値が含まれます。

802.1x ポリシーを定義するルータが VPN の一部でない場合（たとえば、アクセスを制限する対象の企業ネットワークに直接接続されている場合）、手動でアクセス リストを定義する必要があります。このためには、アクセス ルール ポリシーを定義します（アクセス ルールについてを参照）。

はじめる前に

- 選択したルータを、2 つの IP アドレス プール（認証済みクライアント用と未認証クライアント用に 1 つずつ）を含む DHCP ポリシーとともに設定します。DHCP ポリシーの定義を参照してください。
- ルータが設定済みの AAA（RADIUS）サーバにパケットをルーティングできることを確認します。このことは、ルータからサーバに ping を実行することによって確認できます。

関連項目

- 802.1x デバイス ロールについて （3 ページ）
- 802.1x インターフェイス認可状態 （3 ページ）
- 802.1x でサポートされるトポロジ （4 ページ）
- Cisco IOS ルータでの 802.1x （2 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）> [アイデンティティ（Identity）] > [802.1x] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [アイデンティティ（Identity）] > [802.1x] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[802.1x] ページが表示されます。このページのフィールドの説明については、表 1 : [802.1x] ページ （8 ページ）を参照してください。

ステップ 2 802.1x を使用してクライアントを認証するために使用する AAA サーバーを含む AAA サーバーグループの名前を入力します。または、[選択（Select）] をクリックして、リストからサーバーグループを選択するか、新しいサーバーグループを作成します。選択した AAA サーバは、EAP 拡張機能付きの RADIUS を使用する必要があります。

（注） 選択したグループの各 AAA サーバは、ルータ上に存在するインターフェイスと通信するように設定する必要があります。そうしないと、検証が失敗します。

ステップ 3 [仮想テンプレート（Virtual Template）] フィールドに、未認証トラフィックを伝送するための非信頼仮想インターフェイスとして使用する、インターフェイスまたはインターフェイスロールの名前を入力します。または、[選択（Select）] をクリックして、リストからインターフェイスロールを選択するか、新しいロールを作成します。詳細については、ポリシー定義中のインターフェイスの指定を参照してください。

（注） （Cisco 800、1800、1900、2800、2900、3800、および 3900 シリーズなどの）サービス統合型ルータ（ISR）では、未認証トラフィックを伝送するとき、自動的に VLAN を使用します。ただし、仮想テンプレートを定義した場合は、VLAN の代わりにその仮想テンプレートが使用されます。

（注） ここで定義した仮想テンプレートに PPP が定義されている場合は、展開に失敗することがあります。PPP 接続の定義を参照してください。

ステップ 4 認証済みトラフィックを伝送するための信頼物理インターフェイスとして使用するインターフェイスまたはインターフェイスロールの名前を入力します。または、[選択（Select）] をクリックして、リストからロールを選択します。

選択するインターフェイス ロールは、VPN トポロジの一部として設定された内部の保護対象インターフェイスを表す必要があり、選択したルータ上のそれ以外の物理インターフェイスを表さない必要があります。詳細については、エンドポイントおよび保護対象ネットワークの定義を参照してください。

ステップ 5 （任意）802.1x 認証に使用される物理インターフェイスのデフォルトを変更します。詳細については、表 1 : [802.1x] ページ （8 ページ）を参照してください。

[802.1x] ポリシー ページ

[802.1x] ポリシー ページを使用して、認可済みユーザに対して VPN アクセスを制限するポリシーを作成します。認証済みトラフィックは、ルータ上の指定された物理インターフェイスを通過することを許可されます。未認証トラフィックは、インターネットへの仮想インターフェイスを通過することを許可されますが、VPN へのアクセスは許可されません。

詳細については、802.1x ポリシーの定義 （5 ページ）を参照してください。

（注） 802.1x ポリシーでは、IP アドレスをクライアントに割り当てるために DHCP アドレス プールが必要です。これらのプールを定義するには、同じルータ上で DHCP ポリシーを定義します。[DHCP] ポリシー ページを参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）>[アイデンティティ（Identity）] > [802.1x] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [アイデンティティ（Identity）] > [802.1x] を選択します。[802.1x] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータでの 802.1x （2 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて
- Cisco IOS ルータでの基本的なインターフェイス設定
- インターフェイス ロール オブジェクトについて

フィールド リファレンス

表 *1 : [802.1x]* ページ

要素	説明
AAA サーバー グループ	VPN トンネルにアクセスしようとするユーザのクレデンシャルを認証する RADIUS AAA サーバ グループ。AAA サーバー グループ オブジェクトの名前を入力します。または、[追加（Add）] をクリックして、リストから AAA サーバー グループ オブジェクトを選択するか、新しい AAA サーバー グループ オブジェクトを作成します。 （注） 選択したグループの各 AAA サーバは、ルータ上に存在するインターフェイスと通信するように設定する必要があります。そうしないと、検証が失敗します。
Virtual Template	サービス統合型ルータ（ISR）を除くすべてのルータで必須です。 未認証トラフィックに対してインターネットアクセスを提供する非信頼仮想インターフェイス。インターフェイスの名前またはインターフェイスのロールを入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいグループオブジェクトを作成します。 （注） ISR では自動的に VLAN を使用してアクセスを提供するため、ISR の仮想テンプレートを設定する必要はありません。ただし、仮想テンプレートを定義した場合は、VLAN の代わりにその仮想テンプレートが使用されます。 （注） ここで定義した仮想テンプレートに PPP が定義されている場合は、展開に失敗することがあります。[PPP] ダイアログボックス - [PPP] タブを参照してください。
インターフェイス	認証済みトラフィックに対して VPN アクセスを提供する信頼仮想インターフェイス。インターフェイスの名前またはインターフェイスのロールを入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいグループオブジェクトを作成します。 インターフェイス ロールを使用する場合、インターフェイス ロール内に定義されているパターンは、選択したデバイス上の 1 つだけの物理インターフェイスを表している必要があります。このインターフェイスは、VPN トポロジの一部として設定した内部の保護対象インターフェイスである必要があります。詳細については、エンドポイントおよび保護対象ネットワークの定義を参照してください。

要素	説明
リトライ回数	応答を受信できない場合に物理インターフェイスが認証を再開する前に Extensible Authentication Protocol（EAP）request/identity フレームをクライアントに再送信する回数。 有効な値の範囲は 1 ～ 10 です。デフォルトは 2 です。 （注） リンクが信頼できない場合や、特定のクライアントおよび認証サーバに関連する特定の問題がある場合など、異常な状況を調整する目的以外では、デフォルトを変更しないでください。
Control type	インターフェイスのコントロール状態。ホストがネットワークへのアクセスを許可されるかどうかは、この状態によって決まります。次のオプションがあります。 • [Force Authorize]：802.1x 認証をディセーブルにします。これにより、インターフェイスは認証交換を行わなくても認可済み状態に移行します。つまり、インターフェイスは、ホストの 802.1x ベースの認証なしで通常のトラフィックを送受信します。これがデフォルトです。 • [Auto]：802.1x 認証をイネーブルにします。これにより、インターフェイスは未認可状態で開始されるため、このインターフェイスではEAPOLフレームだけを送受信できるようになります。ホストの認証が正常に完了すると、インターフェイス状態が認可済みに変わります。これにより、このインターフェイスを介するホストからのすべてのフレームがイネーブルになります。
Enable client reauthentication	選択すると、802.1x インターフェイスでのクライアント PC の定期的な再認証がイネーブルになります。再認証は、[Client reauthentication period timeout] フィールドで定義されている時間間隔の経過後に実行されます。デフォルトの期間は 3600 秒（1 時間）です。 選択しない場合、定期的な再認証は実行されません。
Client reauthentication period timeout	[Enable client reauthentication] チェックボックスがオンになっている場合にだけ適用されます。 クライアントの再認証の試行と試行の間の秒数。有効な値の範囲は、1 ～ 65535 秒です。デフォルトは 3600 秒（1 時間）です。
待機時間	クライアントとの認証交換が失敗したあとにルータが待機状態でいる時間。認証交換は、クライアントが無効なパスワードを指定したなどの原因で失敗することがあります。 有効な値の範囲は、1 ～ 65535 秒です。デフォルトは 120 秒です。 （注） デフォルトより小さい値を入力すると、ユーザへの応答時間が速くなります。

要素	説明
Rate Limit period	インターフェイスが、誤作動しているクライアントPCから受信したEAP-Startパケットをスロットルするまでの時間間隔。レート制限と呼ばれるこの設定を使用して、このようなクライアントによってルータ処理能力が浪費されることを回避します。 有効な値の範囲は、1 ～ 65535 秒です。デフォルトでは、レート制限はディセーブルになっています。 （注） 既存のレート制限をディセーブルにするには、このフィールドで定義されている値を削除し、フィールドをブランクにしておきます。
AAA Server timeout	ルータがパケットを AAA サーバに再送信するまでに待機する秒数。ルータが 802.1x パケットを AAA サーバに送信したが、サーバが応答しない場合、ルータはこの時間間隔の経過後に別のパケットを送信します。 有効な値の範囲は、1 ～ 65535 秒です。デフォルトは 30 秒です。
Supplicant period	ルータが EAP-Request/Identity パケットをサプリカント（クライアント PC）に再送信するまでに待機する秒数。ルータがEAP-Request/Identityパケットをクライアント PC（サプリカント）に送信したが、サプリカントが応答しない場合、ルータはこの時間間隔の経過後に再びパケットを送信します。 有効な値の範囲は、1 ～ 65535 秒です。デフォルトは 30 秒です。

Cisco IOS ルータでのネットワーク アドミッション コントロール

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

Network Admission Control（NAC; ネットワーク アドミッション コントロール）は、シスコが後援している業界の先進機能です。NAC では、ネットワーク インフラストラクチャを使用して、ネットワーク コンピューティング リソースへのアクセスを要求するすべてのデバイスにセキュリティ ポリシーを適用することにより、ウイルスやワームによる被害を抑制します。企業はNACを使用することにより、PC、PDA、サーバなど、確立されたセキュリティ ポリシーに完全に適合することが確認されたエンドポイント デバイスにネットワーク アクセスを提供できます。また、適合しないデバイスを識別してこれらのアクセスを拒否したり、これらを隔離エリアに移したり、コンピューティング ソースへのアクセスを制限したりすることもできます。

ネットワーク アクセスの決定は、ポスチャ検証のプロセスを通して行われます。このプロセスでは、エンドポイント デバイスにより提示されたポスチャ クレデンシャルが評価されます。これらのクレデンシャルには、エンドポイントのアンチウイルス状態、オペレーティング システム バージョン、オペレーティング システム パッチ レベル、または Cisco Security Agent のバージョンと設定などの情報が含まれることがあります。

NAC を使用して、ブランチ オフィス、リモート アクセス、ダイヤルイン アクセスなど、多くのタイプの展開でセキュリティ ポリシーを適用できます。

Security Manager で NAC ポリシーを使用すると、Cisco IOS ルータを、ネットワークへのアクセスを要求するデバイスにポリシーを適用するためのネットワーク アクセス デバイス（NAD）として使用できます。ここでは、NAC に関する追加情報を示します。

• NAC コンポーネントについて （12 ページ）
• NAC システム フローについて （12 ページ）

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

• NAC 設定パラメータの定義 （13 ページ）
• NAC インターフェイス パラメータの定義 （15 ページ）
• NAC アイデンティティ パラメータの定義 （16 ページ）

NAC をサポートするルータ プラットフォーム

ルータに NAC ポリシーを設定するには、そのルータが（拡張セキュリティ機能セットを搭載した）Cisco IOS ソフトウェア Release 12.3(8)T イメージ以降を実行している必要があります。ただし、次のルータは NAC をサポートしていません。

- Cisco 7600 シリーズ（7603、7604、7606、7609、7613）
- Cisco 7300 シリーズ（7301、7304）
- Cisco 7100 シリーズ VPN ルータ（7120、7140、7160）
- Cisco 3600 シリーズ マルチサービス プラットフォーム（3620、3631、3661、3662）
- Cisco 1700 シリーズ モジュラ アクセス ルータ（1710、1720、1750）
- Cisco 1600 シリーズ（1601、1602、1603、1604、1605）
- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ（全モデル）
- Cisco 800 シリーズ（801、803、805、811、813、828、851、857、871、876、877、878）
- Cisco SOHO 90 シリーズ セキュア ブロードバンド ルータ（91、96、97）
- Cisco SOHO 77 シリーズ（71、76、77 ADSL、77 H ADSL、78）

NAC コンポーネントについて

NAC には、次のコンポーネントが含まれます。

- Cisco Trust Agent（CTA）：CTA は NAC クライアントとして動作します。CTA は、オペレーティング システムのタイプや、インストールされているアンチウイルス ソフトウェアのバージョンなど、インストールされているエンドポイント デバイスのポスチャ クレデンシャルを提供します。
- ネットワーク アクセス デバイス（NAD）：NAD は、インターセプト ACL がトリガーされると、CTA を使用してポスチャ検証を開始します。NAD は、CTA から受信したポスチャ クレデンシャルを AAA サーバにリレーします。代わりに、NAD は AAA サーバから設定情報を受信します。この設定は、選択したインターフェイスに適用されます。また、NAD は次の処理も行います。
  - 定期的に CTA をポーリングして、CTA がこの IP アドレスで同じクライアントと通信していることを確認します。
  - 現在のセッションをすべて再検証します。
  - CTA（クライアントレス ホスト）の存在しないデバイスから、認証のためにユーザ名およびパスワードの情報を AAA サーバに送信します。
  - デバイス IP アドレスまたは MAC アドレスに基づいて、特定のデバイスに適用される定義済みアクションの例外リストをサポートします。

Security Manager で NAC ポリシーを設定すると、NAD として使用する Cisco IOS ルータの動作が設定されます。

- AAA サーバ：AAA サーバは、CTA から受信したポスチャ クレデンシャルを取得して検証し、NAD に適用するアクセス ポリシーを返します。AAA サーバは、RADIUS プロトコルを実行している Cisco Secure Access Control Server（ACS）である必要があります。クライアントレス ホストへのアクセスを提供するために、既存の ACS 認可サポートを使用できます。ポスチャ検証ルールおよびこれらのルールの結果としてのアクセス ポリシーは、ACS で設定します。

関連項目

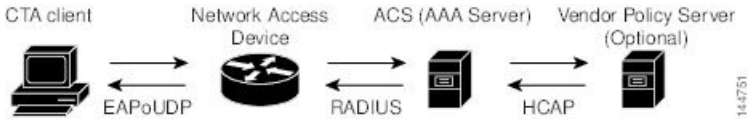
- NAC システム フローについて （12 ページ）
- Cisco IOS ルータでのネットワーク アドミッション コントロール （10 ページ）

NAC システム フローについて

図 2 : NAC システム フロー （13 ページ）に示すように、NAC のシステム フローは次のようになります。

1. 接続デバイスからの IP パケットが、NAD で設定されているインターセプト ACL をトリガーします。
2. NAD は、Extensible Authentication Protocol over User Datagram Protocol（EAP over UDP、または単に EoU とも呼ばれる）を使用して、デバイスで設定されている CTA を使用してポスチャ検証をトリガーします。
3. CTA は、EAP over UDP を使用して、そのポスチャ クレデンシャルを NAD に送信します。
4. NAD は、RADIUS を使用して、これらのポスチャ クレデンシャルを ACS に送信します。
5. ACS はポスチャ検証を実行します。これにより、デバイスがネットワークへのアクセスを許可されるかどうかが決まります（必要に応じて、ACS はサードパーティ製サーバから追加のポスチャ検証を要求します。たとえば、CTA が特定のアンチウイルス アプリケーションに固有のクレデンシャルを転送した場合、ACS は HCAP プロトコルを介して、検証のためにこの情報をベンダーサーバーに転送します）。デバイスがクライアントレスホストの場合、ACS は、受信したユーザ名とパスワードを、ローカルに格納されているリストと照合してチェックします。
6. ACS は、適切なアクセス ポリシーを要求側デバイスに適用するように NAD に指示します。アクセスは許可、拒否、リダイレクト、または制限されます。

図 *2 : NAC* システム フロー



関連項目

- NAC コンポーネントについて （12 ページ）
- Cisco IOS ルータでのネットワーク アドミッション コントロール （10 ページ）

NAC 設定パラメータの定義

NAC 設定パラメータを設定するには、ネットワークに接続しようとするデバイスから受信したポスチャ クレデンシャルを取得して検証する AAA サーバ グループを選択します。Cisco Secure Access Control Server（ACS）に格納されている定義済みのユーザ名とパスワードによって、Cisco Trust Agent（CTA）の存在しないデバイスを認証できるようにするオプションを設定できます。また、EAP over UDP のデフォルト設定も変更できます。これは、ネットワーク アクセス デバイス（NAD）として機能する Cisco IOS ルータと、ネットワークにアクセスしようとするデバイスの間のポスチャ検証通信に使用されるプロトコルです。

関連項目

- NAC インターフェイス パラメータの定義 （15 ページ）
- NAC アイデンティティ パラメータの定義 （16 ページ）

• Cisco IOS ルータでのネットワーク アドミッション コントロール （10 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [アイデンティティ（Identity）] > [ネットワークアドミッションコントロール（Network Admission Control）] を選択し、作業領域で [設定（Setup）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [アイデンティティ（Identity）]>[ネットワークアドミッションコントロール（Network Admission Control）] を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[セットアップ（Setup）] タブをクリックします。

[NAC Setup] タブが表示されます。このタブのフィールドの説明については、表 5 : [Network Admission Control] の [Identities] タブ （24 ページ）を参照してください。

ステップ 2 ポスチャ検証を実行する AAA サーバーを含む AAA サーバーグループの名前を入力します。または、[選択（Select）] をクリックして、リストからサーバーグループを選択するか、新しいサーバーグループを作成します。選択した AAA サーバ グループには、RADIUS を実行している ACS デバイスが含まれる必要があります。

（注） 選択したグループの各 AAA サーバは、ルータ上に存在するインターフェイスと通信するように設定する必要があります。そうしないと、検証が失敗します。

ステップ 3 （任意）メイン サーバ グループのバックアップとして、最大 2 つの AAA サーバ グループを選択します。メイン サーバ グループ内のすべてのサーバが停止した場合、バックアップ サーバ グループ内のサーバが NAC を実行します。

両方のバックアップ サーバ グループは、RADIUS を実行している ACS デバイスで構成されている必要があります。

ステップ 4 （任意）[EAP over UDP] で、次のいずれかまたは両方の [Allow] パラメータを選択します。

a) ACS に送信される RADIUS 要求に IP アドレスを含める場合は、[IPステーションIDを許可（Allow IP Station ID）] チェックボックスをオンにします。

b) CTA がインストールされていないデバイスへのアクセスを提供する場合は、[クライアントレスを許可（Allow Clientless）] チェックボックスをオンにします。このような場合、ACS では、ユーザ名とパスワードを定義済みリストと照合してチェックすることによって、これらのデバイスを認証します。

このチェックボックスをオフにした場合、トラフィックがインターセプト ACL に一致すると、CTA のないデバイスはネットワークへのアクセスを禁止されます。これは、CTA がないと、ポスチャ検証を実行できないためです。

（注） この機能は、Cisco IOS ソフトウェア Release 12.4(6)T 以降を実行しているルータではサポートされません。

ステップ 5 （任意）[Under EAP over UDP] で、必要に応じて、EAP over UDP（EoU）プロトコルに関連するデフォルト設定を変更します。詳細については、表 2 : [Network Admission Control] の [Setup] タブ （19 ページ）を参照してください。

NAC インターフェイス パラメータの定義

NAC インターフェイス パラメータを設定するには、NAC を実行するインターフェイスを選択します。また、インターセプト ACL を定義する必要もあります。これにより、これらのインターフェイス上のどのトラフィックがポスチャ検証を受けるかが決まります。また任意で、EAP over UDP セッションを開始するためのデバイスレベルの設定を上書きし、すべてのセッションを定期的に再検証することもできます（NAC 設定パラメータの定義 （13 ページ）を参照）。

NAC ポリシーが機能するには、少なくとも 1 つのインターフェイス定義が含まれている必要があります。

はじめる前に

- ポスチャ検証を実行する ACS デバイスを含む AAA サーバ グループを選択します。NAC 設定パラメータの定義 （13 ページ）を参照してください。
- NAC ポリシーでポスチャ検証を受けるトラフィックを定義する ACL オブジェクトを定義します。アクセス コントロール リスト オブジェクトの作成を参照してください。
- 選択したインターフェイスのデフォルト アクセスを定義する ACL オブジェクト（デフォルト ACL）を定義します。アクセス コントロール リスト オブジェクトの作成 を参照してください。

関連項目

- NAC 設定パラメータの定義 （13 ページ）
- NAC アイデンティティ パラメータの定義 （16 ページ）
- Cisco IOS ルータでのネットワーク アドミッション コントロール （10 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [アイデンティティ（Identity）] > [ネットワークアドミッションコントロール（Network Admission Control）] を選択し、作業領域で [インターフェイス（Interfaces）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [アイデンティティ（Identity）] > [ネットワークアドミッションコントロール（Network Admission Control）] を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[インターフェイス（Interface）] タブをクリックします。

[NAC Interfaces] タブが表示されます。このタブに含まれるフィールドの説明については、を参照してください。

ステップ 2 NAC の [インターフェイス（Interfaces）] タブで、テーブルからインターフェイス定義を選択し、[編集（Edit）] をクリックするか、[追加（Add）] をクリックして定義を作成します。[NAC Interface Configuration] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、[NAC Identity Action] ダイアログボックス （25 ページ）を参照してください。

ステップ 3 NAC を実行するインターフェイスまたはインターフェイスロールの名前を入力します。または、[選択（Select）] をクリックして、リストからインターフェイスロールを選択するか、新しいインターフェイスロールを作成します。詳細については、ポリシー定義中のインターフェイスの指定を参照してください。

ステップ 4 （任意）インターセプト ACL として機能する ACL オブジェクトの名前を入力します。または、[選択（Select）] をクリックして、リストから ACL オブジェクトを選択するか、新しいオブジェクトを作成します。

選択したインターフェイス上のどのトラフィックが、ネットワークへのアクセスを許可される前にポスチャ検証を受けるかは、インターセプト ACL によって決まります。ACL を選択しない場合、選択したインターフェイス上のすべてのトラフィックがポスチャ検証を受けます。

（注） NAC インターフェイスと同じインターフェイス上に認証プロキシを定義した場合、両方のポリシーで同じインターセプト ACL を使用する必要があります。このようにしない場合、展開が失敗することがあります。認証プロキシの詳細については、IOS デバイスの AAA ルールの設定を参照してください。

ステップ 5 （任意）EAP over UDP セッションを開始するための最大試行回数に定義されているデバイスレベルの値を上書きするには、[EAP over UDP Max Retries] フィールドに新しい値を入力します。

ステップ 6 （任意）NAD ですべての EAP over UDP セッションを定期的に再検証しない場合には、[EOUセッション再検証を有効化（Enable EOU Session Revalidation）] チェックボックスをオフにします。

（注） サブインターフェイスでは、ステップ 5 （16 ページ）およびステップ 6 （16 ページ）で説明されているオプションについてだけ、デフォルト値がサポートされています。

ステップ 7 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。インターフェイス定義は、[NAC Interfaces] タブのテーブルに表示されます。

NAC アイデンティティ パラメータの定義

デフォルトでは、選択したインターフェイスを介するトラフィックのうちインターセプト ACL に一致したトラフィックは、ネットワークに入ることを許可される前に、ポスチャ検証されます。ただし、定義済みアクションの例外リストを作成して、特定のデバイスに適用できます。この例外リストを作成するには、アイデンティティプロファイルを使用します。各プロファイルには次の 2 つの要素が含まれています。

- プロファイル定義。プロファイルが適用されるデバイスを識別します。デバイスは、IP アドレス、MAC アドレス、またはタイプ（Cisco IP Phone の場合）で識別できます。

- アクション。このデバイスがネットワークへのアクセスを試行したときの結果を定義します。各アクションには、ACL、リダイレクト URL、またはその両方を含めることができます。アクションを指定しない場合は、デフォルトの ACL が適用されます。

NAC アイデンティティ パラメータを設定するときは、まず 1 つ以上のアイデンティティ アクションを定義してから、これらのアクションを適用するアイデンティティ プロファイルを作成します。各アクションを複数のプロファイルに適用できます。

関連項目

- NAC 設定パラメータの定義 （13 ページ）
- NAC アイデンティティ パラメータの定義 （16 ページ）
- Cisco IOS ルータでのネットワーク アドミッション コントロール （10 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [アイデンティティ（Identity）] > [ネットワークアドミッションコントロール（Network Admission Control）] を選択し、作業領域で [アイデンティティ（Identities）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [アイデンティティ（Identity）]>[ネットワークアドミッションコントロール（Network Admission Control）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成し、[アイデンティティ（Identities）] タブをクリックします。

[NAC Identities] タブが表示されます。このタブのフィールドの説明については、表 5 : [Network Admission Control] の [Identities] タブ （24 ページ）を参照してください。

ステップ 2 1 つ以上のアイデンティティ アクションを定義します。

a) [NACアイデンティティ（NAC Identities）] タブの下半分のテーブルからアイデンティティアクションを選択し、[追加（Add）] をクリックします。[NAC Identity Action] ダイアログボックスが表示されます。

b) アイデンティティ アクションを定義します。使用可能なフィールドの説明については、表 7 : [NAC Identity Action] ダイアログボックス （26 ページ）を参照してください。

c) [OK] をクリックして定義を保存し、ダイアログボックスを閉じます。[NAC Identities] タブの [Identity Actions] テーブルに、アクションが表示されます。

d) （任意）2.a （17 ページ）～2.c （17 ページ）を繰り返して、必要に応じて追加のアイデンティティアクションを定義します。

ステップ 3 アイデンティティ プロファイルを定義します。

a) [NACアイデンティティ（NAC Identities）] タブの上半分のテーブルからアイデンティティ プロファイルを選択し、[追加（Add）] をクリックします。[NAC Identity Profile] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 6 : [NAC Identity Profile] ダイアログボックス （25 ページ）を参照してください。

b) （ステップ 2 （17 ページ）で定義されているように）アイデンティティアクションの名前を入力するか、[選択（Select）] をクリックしてセレクタを表示します。
c) プロファイルを適用するデバイスを識別するプロファイル定義を選択および定義します。
d) [OK] をクリックして定義を保存し、ダイアログボックスを閉じます。[NAC Identities] タブの [Identity Profiles] テーブルに、プロファイルが表示されます。
e) （任意）3.a （17 ページ）～3.d （18 ページ）を繰り返して、必要に応じて追加のアイデンティティプロファイルを定義します。

[Network Admission Control Policy] ページ

Network Admission Control（NAC; ネットワーク アドミッション コントロール）ポリシーを使用すると、エンドポイントがネットワークに接続しようとするときに、Network Access Devices（NAD; ネットワーク アクセス デバイス）として機能する Cisco IOS ルータにアクセス権限を適用できます。アクセス決定は、エンドポイントデバイスにより提供された情報（現在のアンチウイルス状態など）に基づいて行われるため、セキュアでないノードからネットワークが感染することを回避できます。

[Network Admission Control] ポリシー ページの次のタブから Cisco IOS ルータ上の NAC ポリシーを設定できます。

- [Network Admission Control] ページ - [Setup] タブ （19 ページ）
- [Network Admission Control] ページ - [Interfaces] タブ （21 ページ）
- [Network Admission Control] ページ - [Identities] タブ （23 ページ）

詳細については、Cisco IOS ルータでのネットワーク アドミッション コントロール （10 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [アイデンティティ（Identity）] > [ネットワークアドミッションコントロール（Network Admission Control）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [アイデンティティ（Identity）] > [ネットワークアドミッションコントロール（Network Admission Control）] を選択します。[ネットワークアドミッションコントロール（Network Admission Control）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存ポリシーを選択します。

[Network Admission Control] ページ - [Setup] タブ

[Network Admission Control] の [Setup] タブを使用して、NAC プロセス中に認証に使用される Cisco Secure Access Control Server を選択します。また、NAD と、ネットワークへのアクセスを試行するクライアントとの間の通信に対して EAP over UDP 設定を定義します。

ナビゲーション パス

[Network Admission Control Policy] ページ （18 ページ）に移動し、[セットアップ（Setup）] タブをクリックします。

関連項目

- NAC 設定パラメータの定義 （13 ページ）
- [Network Admission Control] ページ - [Interfaces] タブ （21 ページ）
- [Network Admission Control] ページ - [Identities] タブ （23 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて

フィールド リファレンス

表 2 : [Network Admission Control] の [Setup] タブ

要素	説明
AAA サーバー グループ	NAC 認証に使用される AAA サーバ グループ。RADIUS プロトコルを実行している Cisco Secure Access Control Server（ACS）デバイスを構成するサーバ グループを選択する必要があります。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 （注） 選択したグループの各 AAA サーバは、ルータ上に存在するインターフェイスと通信するように設定する必要があります。そうしないと、検証が失敗します。
Backup AAA Server Group 1	メイン グループの AAA サーバが停止した場合のバックアップ AAA サーバ グループ。
Backup AAA Server Group 2	メイン グループの AAA サーバおよび最初のバックアップ グループが停止した場合のセカンダリ バックアップ AAA サーバ グループ。
EAP over UDP (EoU) settings	

要素	説明
Allow IP Station ID	選択すると、ACS に送信される RADIUS 要求の calling-station-id フィールドに IP アドレスを含めることができます。 選択しない場合、ACS に送信される RADIUS 要求の calling-station-id フィールドに IP アドレスは含められません。
Allow Clientless	選択すると、Cisco Trust Agent（CTA）がインストールされていないデバイスを、ACS で設定されているユーザ名とパスワードを使用して認証できます。 このチェックボックスをオンにした場合は、提供されたフィールドにユーザ名とパスワードを（確認も含めて）入力します。 選択しない場合、NAC では、トラフィックがインターセプト ACL に一致すると、CTA のないデバイスによるネットワークへのアクセスが禁止されます（[NAC Interface Configuration] ダイアログボックス （22 ページ）を参照）。 （注） この機能は、Cisco IOS ソフトウェア Release 12.4(6)T 以降を実行しているルータではサポートされません。
Max Retry	接続デバイスと EAP over UDP セッションを開始するときに、このルータ上のすべての NAC インターフェイスで行う最大試行回数。 有効値の範囲は 1 ～ 3 です。デフォルトは 3 です。 （注） 必要に応じて、特定のインターフェイス上のこのグローバル値を上書きできます。[Network Admission Control] ページ - [Interfaces] タブ （21 ページ）を参照してください。
レート制限	ルータが同時に処理できる EAP over UDP ポスチャ検証の数。1 つ以上のデバイスを削除しないかぎり、追加のデバイスを検証できません。 有効値の範囲は 1 ～ 200 です。デフォルトは 20 です。この値を 0 に設定すると、レート制限がオフになります。
[ポート（Port）]	EAP over UDP セッションで使用する UDP ポート。 有効値の範囲は 1 ～ 65535 です。デフォルトは 21862 です。 （注） NAC が機能するためには、このルータ上のデフォルト ACL が、EAP over UDP トラフィックに対してここで指定したポートを介する UDP トラフィックを許可している必要があります。詳細については、アクセス ルールについてを参照してください。

要素	説明
Enable Logging	選択すると、このルータ上の EAP over UDP イベントがデバイスに記録されます。 選択しない場合、EAP over UDP ロギングがディセーブルになります。これがデフォルトです。

[Network Admission Control] ページ - [Interfaces] タブ

[Network Admission Control] の [Interfaces] タブを使用して、NAC を実行するルータ インターフェイスを選択および設定します。このとき、インターセプト ACL および選択済み EoU インターフェイス パラメータを設定します。NAC ポリシーが機能するためには、少なくとも 1 つのインターフェイス定義が含まれている必要があります。

ナビゲーション パス

[Network Admission Control Policy] ページ （18 ページ）に移動し、[インターフェイス（Interfaces）] タブをクリックします。

関連項目

- NAC インターフェイス パラメータの定義 （15 ページ）
- NAC インターフェイス パラメータの定義 （15 ページ）
- [Network Admission Control] ページ - [Identities] タブ （23 ページ）
- テーブル カラムおよびカラム見出しの機能
- テーブルのフィルタリング

フィールド リファレンス

表 3 : [Network Admission Control] の [Interfaces] タブ

要素	説明
インターフェイス	NAC を実行するインターフェイスの名前。
Intercept ACL	インターセプト ACL の名前。インターフェイスによるポスチャ検証チェックをトリガーする着信トラフィックは、インターセプト ACL によって決まります。
EoU Max Retries	このインターフェイスが接続デバイスとの EoU セッションを開始するときに実行する最大再試行回数。
Revalidate	インターフェイスがその EoU セッションを再検証して、それらがまだアクティブであることを確認するかどうかを示します。

要素	説明
[追加（Add）] ボタン	[NAC Interface Configuration] ダイアログボックス （22 ページ）が開きます。ここから、NAC インターフェイスを定義できます。
[編集（Edit）] ボタン	[NAC Interface Configuration] ダイアログボックス （22 ページ）が開きます。ここから、選択した NAC インターフェイスを編集できます。
[削除（Delete）] ボタン	選択した NAC インターフェイスをテーブルから削除します。

[NAC Interface Configuration] ダイアログボックス

[NAC Interface Configuration] ダイアログボックスを使用して、NAC を実行するルータ インターフェイスを追加または編集します。

ナビゲーション パス

[Network Admission Control] ページ - [Interfaces] タブ （21 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- NAC インターフェイス パラメータの定義 （15 ページ）
- Cisco IOS ルータでの基本的なインターフェイス設定
- インターフェイス ロール オブジェクトの作成
- アクセス コントロール リスト オブジェクトの作成

フィールド リファレンス

表 4 : [NAC Interface Configuration] ダイアログボックス

要素	説明
インターフェイス（Interface）	接続デバイス上で NAC を実行するインターフェイス。インターフェイスの名前またはインターフェイスのロールを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

要素	説明
Intercept ACL	ポスチャ検証を必要とするトラフィックを定義するACL。ACLオブジェクトの名前を入力します。または、[追加（Add）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 （注） 認証プロキシがNACと同じインターフェイスで設定されている場合、両方のポリシーで同じインターセプトACLを使用する必要があります。このようにしないと、展開が失敗する場合があります。認証プロキシの詳細については、IOSデバイスの AAA ルールの設定を参照してください。
EAP over UDP Max Retries	ルータが接続デバイスとのEoUセッションの開始を試行する最大回数。有効値の範囲は 1 ～ 3 です。デフォルトは 3 です。 （注） サブインターフェイスではデフォルト値だけがサポートされます。
Enable EoU Session Revalidation	選択すると、ルータは必要に応じてその EoU セッションを再検証します。これがデフォルトです。 選択しない場合、EoU セッション再検証は実行されません。 （注） サブインターフェイスではデフォルト値だけがサポートされます。

[Network Admission Control] ページ - [Identities] タブ

[Network Admission Control] の [Identities] タブを使用して、NAC アイデンティティ プロファイルとアイデンティティ アクションを表示、作成、編集および削除します。アイデンティティ プロファイルは、選択済みのデバイス（IP アドレス、MAC アドレス、またはデバイス タイプで識別される）から受信されたトラフィックに対して実行する特定のアクションを定義します。このように、アイデンティティ プロファイルを持つデバイスは NAC によって処理されます。ACS と照合してポスチャ検証を実行する必要はありません。

ナビゲーション パス

[Network Admission Control Policy] ページ （18 ページ）に移動し、[インターフェイス（Interfaces）] タブをクリックします。

関連項目

- NAC インターフェイス パラメータの定義 （15 ページ）
- [Network Admission Control] ページ - [Setup] タブ （19 ページ）
- [Network Admission Control] ページ - [Identities] タブ （23 ページ）
- テーブル カラムおよびカラム見出しの機能

- テーブルのフィルタリング

フィールド リファレンス

表 5 : [Network Admission Control] の [Identities] タブ

要素	説明
[Identity Profiles] テーブル	
Profile Definition	アイデンティティ プロファイルのタイプ。デバイス IP アドレス、MAC アドレス、またはデバイス タイプ（IP Phone）です。
アクション名	このNACアイデンティティ プロファイルに割り当てられる（[Identity Actions] テーブルで定義されている）アクションの名前。
[追加（Add）] ボタン	[NAC Identity Profile] ダイアログボックス （24 ページ）を開きます。ここから、アイデンティティ プロファイルを定義できます。
[編集（Edit）] ボタン	[NAC Identity Profile] ダイアログボックス （24 ページ）が開きます。ここから、選択したアイデンティティ プロファイルを編集できます。
[削除（Delete）] ボタン	選択したアイデンティティ プロファイルをテーブルから削除します。
[Identity Actions] テーブル	
アクション名	アイデンティティ アクションの名前。
ACL	このアイデンティティ アクションが割り当てられたプロファイルに適用される ACL。
リダイレクト URL	このアイデンティティ アクションが割り当てられたデバイスからのトラフィックがリダイレクトされる宛先の URL。
[追加（Add）] ボタン	NAC アイデンティティ アクションを定義するための [NAC Identity Action] ダイアログボックス （25 ページ）を開きます。
[編集（Edit）] ボタン	選択した NAC アイデンティティ アクションを編集するための [NAC Identity Action] ダイアログボックス （25 ページ）を開きます。
[削除（Delete）] ボタン	選択したアイデンティティ アクションをテーブルから削除します。

[NAC Identity Profile] ダイアログボックス

[NAC Identity Profile] ダイアログボックスを使用して、特定のアイデンティティに一致するデバイスに割り当てられた NAC プロファイルを追加または編集します。アイデンティティ プロファイルでは、IP アドレス、MAC アドレス、またはデバイス タイプ（IP Phone の場合）に基づいて、特定のデバイスから送信されたすべてのトラフィックに適用される NAC アクションを定義します。

ナビゲーション パス

[Network Admission Control] ページ - [Identities] タブ （23 ページ）に移動してから、[アイデンティティプロファイル（Identity Profiles）] テーブルの下にある [追加（Add）] ボタンまたは [編集（Edit）] ボタンをクリックします。

関連項目

- [NAC Identity Action] ダイアログボックス （25 ページ）
- NAC アイデンティティ パラメータの定義 （16 ページ）

フィールド リファレンス

表 6 : [NAC Identity Profile] ダイアログボックス

要素	説明
アクション名	プロファイルに割り当てるアクションの名前。アクションの名前を入力するか、[選択（Select）] をクリックしてセレクタを表示します。アクションの作成の詳細については、[NAC Identity Action] ダイアログボックス （25 ページ）を参照してください。
Profile Definition	このプロファイルを割り当てるデバイス。 • [IP Address]：このプロファイルを割り当てるデバイスの IP アドレス。複数のプロファイルで同じ IP アドレスを使用することはできません。 • [MAC Address]：このプロファイルを割り当てるデバイスの MAC アドレス。 • [Cisco IP Phone]：Cisco IP Phone に NAC アイデンティティ プロファイルを定義する場合に使用します。

[NAC Identity Action] ダイアログボックス

[NAC Identity Action] ダイアログボックスを使用して、NAC アイデンティティ プロファイルに割り当てるアクションを追加または編集します。

ナビゲーション パス

[Network Admission Control] ページ - [Interfaces] タブ （21 ページ）に移動してから、[アイデンティティアクション（Identity Action）] テーブルの下にある [追加（Add）] ボタンまたは [編集（Edit）] ボタンをクリックします。

関連項目

- [NAC Identity Profile] ダイアログボックス （24 ページ）

- NAC アイデンティティ パラメータの定義 （16 ページ）
- アクセス コントロール リスト オブジェクトの作成

フィールド リファレンス

表 *7: [NAC Identity Action]* ダイアログボックス

要素	説明
名前	アイデンティティ アクションを説明する名前。NAC アイデンティティ プロファイルに割り当てるアクションを選択するときは、この名前を使用します。 [NAC Identity Action] ダイアログボックス （25 ページ）を参照してください。
アクセス コントロール リスト	このアクションを含むプロファイルが割り当てられたデバイスから受信したトラフィックを処理する方法を定義する ACL。ACL オブジェクトの名前を入力します。または、[追加（Add）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 （注） インターセプト ACL に使用されている ACL オブジェクトと同じ ACL オブジェクトは選択できません。 [NAC Interface Configuration] ダイアログボックス （22 ページ）を参照してください。
リダイレクト URL	デバイスからのトラフィックをリダイレクトする宛先の修復サーバのアドレス。通常、リダイレクト URL の形式は、**http://URL** または **https://URL** です。

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