CHAPTER 6

ユーザ管理：ユーザ ロールとローカル ユーザの設定

この章の内容は以下のとおりです。

- 概要（p.6-1）
- ユーザ ロールの作成（p.6-2）
- ローカル ユーザ アカウントの作成（p.6-16）

認証サービスの設定に関する詳細は、第 7 章「ユーザ管理：認証サーバの設定」を参照してください。

Web ユーザ ログイン ページの作成および設定に関する詳細は、第 5 章「ユーザ ログイン ページとゲスト アクセスの設定」を参照してください。

ユーザ ロールのトラフィック ポリシーの設定に関する詳細は、第 8 章「ユーザ管理：トラフィック制御、帯域幅、スケジュール」を参照してください。

概要

この章では、Cisco NAC アプライアンスのユーザ ロールについて説明します。具体的な内容は、ユーザ ロールの割り当て方法とそれらの作成および設定方法です。また、CAM によって内部で認証されるローカル ユーザの作成方法（主にテスト用）についても説明します。

ユーザ ロールの作成

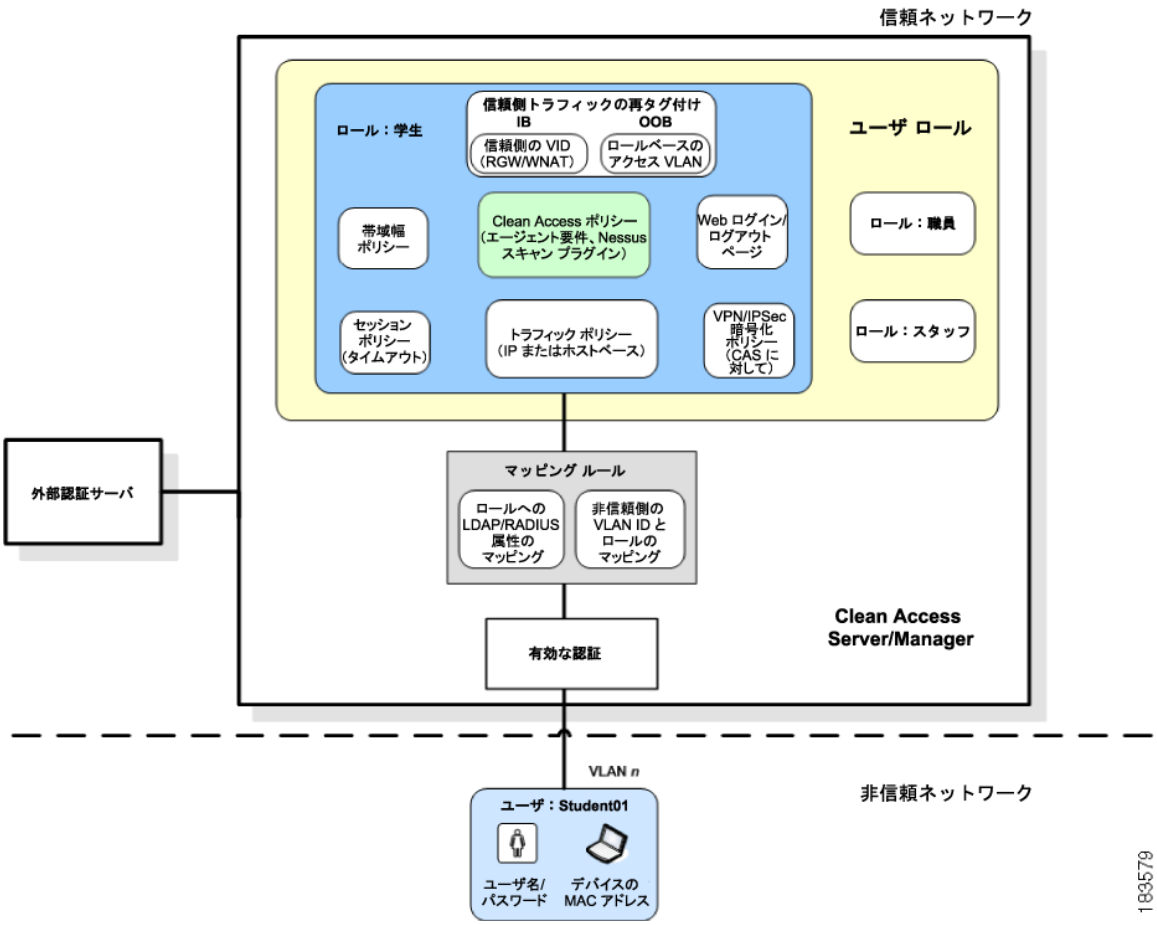
ロールは、Cisco NAC アプライアンスの機能に欠かせない要素であり、次のように考えることができます。

- ユーザ セッション中、持続するユーザの分類スキーム
- 特定グループのユーザの Cisco NAC アプライアンス内でのトラフィック ポリシー、帯域幅制限、セッション期間、Clean Access 脆弱性評価、その他のポリシーを決定するメカニズム

通常、ロールは、ネットワーク内の各ユーザ グループに共通するニーズを反映するような設定にしなければなりません。したがって、ロールを作成する前に、ネットワーク内の権限割当て方法、トラフィック制御ポリシーの適用方法、クライアント デバイスのグループ タイプを検討する必要があります。ロールは、多くの場合、組織内の既存のグループ（学生 / 教員 / スタッフまたは技術 / 販売 / 人事など）に基づいて作成されます。クライアント マシンのグループ（ゲーム ボックスなど）にロールを割り当てることもできます。図 6-1 に示されているように、ロールには、次のようなさまざまなユーザ ポリシーが集約されています。

- トラフィック ポリシー
- 帯域幅ポリシー
- VLAN ID の再タグ付け
- Clean Access ネットワーク ポート スキャン プラグイン
- Clean Access Agent（CAA）クライアント システムの条件

図 6-1　Normal Login ユーザ ロール



ユーザ ロールのタイプ

ユーザのログイン試行時に、システムがそのユーザを 1 つのロールに分類します。システムには、4 つのデフォルト ユーザ ロール（Unauthenticated ロール、Normal Login ロール、Clean Access Agent Temporary ロール、および Clean Access Quarantine ロール）があります。

Unauthenticated ロール

Unauthenticated ロールは 1 つのみで、システム デフォルト ロールです。設定されている Normal Login ロールが削除されると、そのロール内のユーザは Unauthenticated ロールに再割り当てされます（「ロールの削除」[p.6-15] を参照）。Unauthenticated ロールに、トラフィックおよびその他のポリシーを設定することはできますが、このロール自体を編集したりシステムから削除することはできません。

Clean Access Server（CAS）の非信頼（管理対象）側にいるユーザは、最初の Web ログインまたは CAA ログインまで、Unauthenticated ロールになります。Web ログイン / ネットワーク スキャンのみを使用する場合、ユーザはクライアントがスキャンに合格する（Normal Login ロールに移行）、あるいはスキャンに不合格となる（ブロックされるか、Quarantine ロールに移行）までは、Unauthenticated ロールのままになります。

Normal Login ロール

システムには、複数の Normal Login ロールを設定できます。正常にログインしたユーザは、Normal Login ロールになります。Normal Login ロールを設定することにより、ユーザを以下の事項に関連付けることができます。

- ネットワーク アクセス トラフィック制御ポリシー — ロールの間、ネットワークのどの部分およびどのアプリケーション ポートにユーザがアクセスできるか
- VLAN ID：
  - インバンド ユーザの場合、アップストリーム ルータへのプライオリティを区別するために信頼ネットワーク宛のトラフィック（そのロールのユーザとの間の）を再タグ付けします。
  - アウトオブバンド　ユーザの場合、ロールベースの設定を使用している場合は、ロールのユーザのアクセス VLAN ID を設定します。
- Clean Access ネットワーク スキャン プラグイン — 実行する Nessus ポート スキャン（該当する場合）
- CAA の条件 — クライアント システムが満たさなければならないこのソフトウェア パッケージの条件
- Web ログイン成功または失敗後に表示されるエンド ユーザ HTML ページ — さまざまなサブネット /VLAN/ ロールの Web ログインユーザに表示されるページおよび情報詳細は、第 5 章「ユーザ ログイン ページとゲスト アクセスの設定」を参照してください。

通常は、学生、教員、スタッフ（または技術、人事、販売）など、いくつかの Normal Login ロールが使用されます。ユーザへの Normal Login ロールの割り当ては、次の事項に基づいて行うことができます。

- クライアント デバイスの MAC アドレスまたはサブネット **Device Management > Filters** で、デバイスまたはサブネットにロールを指定できます。詳細は、「デバイスおよびサブネットのグローバル フィルタリング」（p.3-8）を参照してください。
- ローカル ユーザの属性。ローカル ユーザは主としてテストに使用され、外部認証サーバではなく、Clean Access Manager（CAM）によって内部で認証されます。**User Roles > Local Users** でローカル ユーザにロールを指定できます。「ローカル ユーザ アカウントの作成」（p.6-16）を参照してください。

- 外部認証サーバの属性。外部認証サーバで検証されたユーザには、以下の事項に基づいてロールを指定できます。
  - そのユーザの非信頼ネットワーク VLAN ID
    非信頼ネットワークの情報を使用してユーザをユーザ ロールにマッピングできます。
  - LDAP および RADIUS 認証サーバからの認証属性
    認証属性に応じて、ユーザを Cisco NAC アプライアンス内で異なるロールにマッピングできます。マッピング ルールが指定されていない場合、ログイン後、認証サーバに対して指定されているデフォルトのロールがユーザに割り当てられます。VLAN マッピングおよび属性マッピングは **User Management > Auth Servers > Mapping Rules** で作成します。

  詳細は、「認証プロバイダーの追加」（p.7-4）および「属性または VLAN ID を使用したユーザとロールのマッピング」（p.7-17）を参照してください。

ロール割り当てのプライオリティ

ロール割り当てのプライオリティ順序は次のとおりです。

1. MAC アドレス
2. サブネット /IP アドレス
3. ログイン情報（ログイン ID、認証サーバから得たユーザの属性、ユーザ マシンの VLAN ID など）

したがって、あるクライアントが MAC アドレスでは「ロール A」に関連付けられているのに、ユーザのログイン ID では「ロール B」に関連付けられている場合は、「ロール A」が使用されます。

「デバイスおよびサブネットのグローバル フィルタリング」（p.3-8）および「アウトオブバンド配置のデバイス フィルタ」（p.3-11）も参照してください。

Clean Access ロール

ネットワーク上で実行できる Clean Access プロセスは、ネットワーク スキャンのみ（図 9-4 を参照）、CAA のみ、または CAA とネットワーク スキャン（図 9-3 を参照）です。Clean Access がイネーブルになっていると、Clean Access 用に次の 2 種類のロールが使用されます。

- **CAA Temporary ロール**

  CAA を使用する場合、認証後のユーザには CAA Temporary ロールが割り当てられます。このロールのユーザには、システムが脆弱にならないように必要なパッケージをダウンロードしインストールするためのネットワーク アクセスのみが許可されます。CAA の条件が満たされるまで、Normal Login ロールのアクセスは許可されません。

  CAA Temporary ロールはシステム内に 1 つだけしかありません。このロールが有効になるのは、ログインに CAA を使用し、Clean Access 条件を満たすことをユーザに要求する場合だけです。

  CAA Temporary ロールは、以下の期間のユーザに割り当てられます。

  a. ログイン試行から正常なネットワーク アクセスまで。クライアント システムは、CAA の条件を満たし、ネットワーク スキャン後に脆弱性は検出されていません。ユーザは、CAA Temporary ロールから、そのユーザの Normal Login ロールに移行します。

  b. ログイン試行から、CAA の条件が満たされるまで。ユーザには、必要なパッケージをダウンロードし、インストールするために、このロールの Session Timer に設定されている時間が与えられます。ユーザが取り消しを実行するか、タイムアウトになると、そのユーザは CAA Temporary ロールから排除され、ログイン プロセスをやり直さなければなりません。与えられた時間内にユーザが必要なものをダウンロードした場合、そのユーザは CAA Temporary ロールのまま、ネットワーク スキャン（イネーブルの場合）に進みます。

  c. ログイン試行から、ネットワーク スキャンでユーザ システムの脆弱性が検出されるまで。クライアント システムが CAA の条件を満たしていても、ネットワーク スキャンで脆弱性が検出されると、ユーザは CAA Temporary ロールから Quarantine ロールに移行します。

- **Quarantine ロール**

  ネットワーク スキャンがイネーブルになっている場合に使用されます。Clean Access Quarantine ロールの目的は、そのユーザに許可するネットワーク アクセスを、ユーザ システムで検出された脆弱性を修正するために必要なリソースへのアクセスだけに制限することです。脆弱性が修正されるまで、Normal Login ロールのネットワーク アクセスは許可されません。

  システムには、1 つ以上の Quarantine ロールを設定できます。ユーザが Quarantine ロールに分類されるのは、以下の場合です。

  — ユーザが Web ログイン ページを使用してログインを試行し、Clean Access のネットワーク スキャンによってユーザ システムで脆弱性が検出された場合

  — ユーザが CAA を使用してログインし、CAA の条件を満たしているが、Clean Access のネットワーク スキャンによって、ユーザ システムで脆弱性が検出された場合

  リソースにアクセスして脆弱性を修正できるように、このロールの Session Timer に設定されている時間がユーザに与えられます。ユーザが取り消しを実行するか、タイムアウトになると、そのユーザは Quarantine ロールからログアウトされ、ログイン プロセスをやり直さなければなりません。次回のログイン試行時には、そのクライアントは再度、Clean Access のプロセスを進みます。

  与えられた時間内にユーザが脆弱性を修正した場合、ログインに CAA を使用しているユーザは、同じセッション中に再度、ネットワーク スキャンへと進むことができます。Web ログインを使用するユーザは、2 度めのネットワーク スキャンを受けるために、ログアウトまたはタイムアウトしてから再度ログインする必要があります。

（注） Web ログインを使用するユーザは、ログアウト ページを閉じないように注意する必要があります（図 5-11 を参照）。ユーザがログアウトできず、セッションがタイムアウトになる前にログインを再試行した場合、そのユーザはまだ元の Quarantine ロールにいるとみなされ、ログイン ページは表示されません。

該当する Normal Login ロールでのネットワーク アクセスが許可されるのは、そのユーザが条件を満たし、脆弱性を修正した場合だけです。すべての Normal Login ロールを 1 つの Quarantine ロールにマッピングすることも、また異なる Quarantine ロールを作成しカスタマイズすることも可能です。たとえば、各 OS（オペレーティング システム）の脆弱性を修正するために異なるリソースが必要な場合は、複数の Quarantine ロールを使用できます。いずれの場合も、1 つの Normal Login ロールとマッピングできる Quarantine ロールは 1 つだけです。ロールの作成後、**Device Management > Clean Access > General Setup** フォームで Normal Login ロールと Quarantine ロールの関連付けを設定します。詳細は、「General Setup の概要」（p.9-18）を参照してください。

セッション タイムアウト

簡単なセッション タイムアウトと、限定されたトラフィック ポリシー権限によって、Clean Access ロールのネットワーク アクセスを制限できます。セッション タイムアウト時間は、Clean Access のチェックを完了し、必要なソフトウェア パッケージを取得するための最低限の時間だけをユーザに与えることを目的としています。Clean Access 関連ロールの最小タイムアウト時間は、次の役割を果たします。

- 脆弱なユーザによるネットワークへの影響を抑制する。
- ユーザが Temporary ロールでネットワークにフルアクセスするのを防ぐ。
  これによって、ユーザが特定の検査に不合格になり、必要なパッケージをインストールして、コンピュータを再起動したが、手動でログアウトしない場合の再検査回避を抑制できます。

ご使用の環境に適したタイムアウト時間を判断するには、ユーザが利用できるネットワーク接続速度や必要となるパッケージのダウンロード サイズを考慮する必要があります。

設定可能な時間（分）後にクライアントに CAS が接続できない場合、全ユーザをログオフするように Hertbeat Timer を設定することも可能です。詳細は、「ユーザ セッション タイムアウトおよびハートビート タイムアウトの設定」（p.8-17）を参照してください。

ユーザ ロールに **Max Sessions per User Account** を設定できます。これによって、管理者は、同じユーザ証明書を同時に使用できるマシンの数を制限できます。この機能を使用すると、各ユーザのログイン セッション数が、設定数に制限されます。あるユーザ名のオンライン ログイン セッションが指定値（1 ～ 255、無制限の場合は 0）を超えると、次回のログイン試行時に、Web ログイン ページまたは CAA を通じて、ユーザがすべてのセッションの終了または最も古いセッションの終了を実行するよう促します。詳細は、「ロール プロパティ」（p.6-8）を参照してください。

デフォルト ログイン ページ

Web ログイン ユーザと CAA ユーザのどちらの認証にも、システム内にデフォルト ログイン ページが追加され、存在している必要があります。

ログイン ページは、Cisco NAC アプライアンスによって生成され、ロール別にエンド ユーザに表示されます。ユーザが初めて Web ブラウザからネットワークへのアクセスを試行すると、HTML ログイン ページが表示され、ユーザ名とパスワードの入力をユーザに求めます。Cisco NAC アプライアンスは、選択された認証プロバイダーにこの証明書を提出し、これを使用してユーザに割り当てるロールを判断します。この Web ログイン ページは、ユーザの VLAN ID、サブネット、OS に基づいて特定のユーザ用にカスタマイズできます。

注意　CAA ユーザの場合は、デフォルト ログイン ページがないと、ログイン試行時にエラー ダイアログが表示されます（[Clean Access Server is not properly configured, please report to your administrator.]）。

（注）　L3 OOB 配置の場合、「ログイン ページの Web クライアントのイネーブル化」（p.5-6）が必要です。

Web ユーザ ログイン ページの作成と設定に関する詳細は、第 5 章「ユーザ ログイン ページとゲスト アクセスの設定」を参照してください。デフォルト ログイン ページの簡単な追加方法については、「デフォルト ログイン ページの追加」（p.5-4）を参照してください。

ロールのトラフィック ポリシー

最初のロール作成時、デフォルト トラフィック フィルタリング ポリシーでは、非信頼側から信頼側に移動するトラフィックは deny all になり、信頼側から非信頼側へのトラフィックは allow all になります。したがって、ロール作成後、適切なトラフィックを許可するポリシーを作成する必要があります。ユーザ ロールへの IP ベースおよびホストベースのトラフィック ポリシーの設定方法については、第 8 章「ユーザ管理：トラフィック制御、帯域幅、スケジュール」を参照してください。

さらに、ネットワークへの全般的なアクセスを防止し、ユーザが条件を満たし脆弱性を修正するために必要な Web リソースまたは修復サイトへのアクセスを許可するには、CAA Temporary ロールおよび Quarantine ロールにもトラフィック ポリシーを設定する必要があります。詳細については、「Agent Temporary および Quarantine ロールのポリシーの設定」（p.8-21）を参照してください。

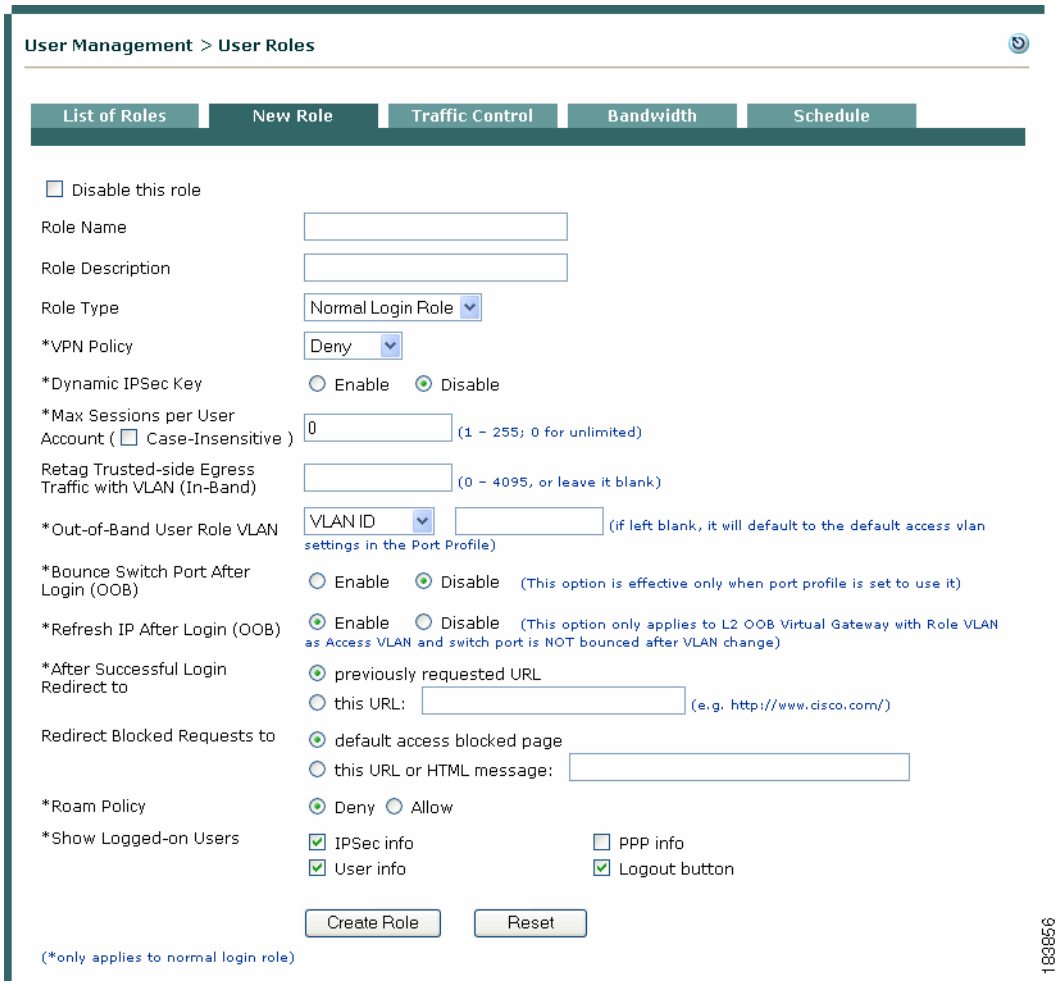
新しいロールの追加

CAA Temporary ロールおよび Quarantine ロールは、あらかじめシステムに作成されているので、必要なのは設定だけですが、Normal Login ロール（追加の Quarantine ロールも）は、最初に追加しなければなりません。新しいロールを作成したら、そのロールをご使用の環境のトラフィック ポリシーや Web コンソールでカスタマイズしたその他のプロパティに関連付けることができます。

（注）　非信頼側から信頼側ネットワークへのトラフィックを許可するためには、新しいロールにトラフィック ポリシーを追加する必要があります。詳細は、第 8 章「ユーザ管理：トラフィック制御、帯域幅、スケジュール」を参照してください。

1. **User Management > User Roles > New Role** の順番に進みます（図 6-2）。

図 6-2　新しいユーザ ロールの追加



2. ロールをすぐにアクティブにする場合は、**Disable this role** を選択しないでおきます。
3. **Role Name** フィールドに、そのロールに固有の名前を入力します。
4. （任意）**Role Description** に、説明を入力します。

5. 以下のいずれかのロール タイプを選択します。
   - **Normal Login Role —** 正常ログイン後のユーザに割り当てられます。認証サーバのマッピング ルールを設定している場合は、認証サーバからの属性を使用してユーザを Normal Login ロールにマッピングします。ネットワーク スキャン プラグインおよび CAA の条件も、Normal Login ロールに関連付けられます。ユーザはログイン時に、プラグインのスキャンを受けるか、または条件が満たされているか、その両方です（Unauthenticated/Temporary ロールの間に）。ユーザが条件を満たしていて、脆弱性がなければ、そのユーザは Normal Login ロールのネットワーク アクセス権を取得します。

（注）　Normal Login ロールだけに適用されるフォーム フィールドには、アスタリスク（*）のマークが付いています。

   - **Quarantine Role —** Clean Access のネットワーク スキャンによってそのユーザのシステムに脆弱性が発見された場合、ユーザを隔離するために割り当てられます。システムには、あらかじめ Quarantine ロールが用意されているので、すぐに設定できます。ただし、必要な場合は、New Role フォームを使用して Quarantine ロールを追加できます。
6. 各ロールの設定値の詳細は、「ロール プロパティ」（p.6-8）を参照してください。

（注）　OOB　配置でロール　ベースのプロファイルを使用する場合は、ユーザ　ロール作成時に、**Out-of-Band User Role VLAN** フィールドにアクセス VLAN を指定する必要があります。詳細は、「Out-of-Band User Role VLAN」（p.6-11）および「ポート プロファイルの追加」（p.4-27）を参照してください。

7. 完了したら、**Create Role** をクリックします。フォームのデフォルト プロパティをリストアするには、**Reset** をクリックします。
8. **List of Roles** タブにこのロールが表示されます。
9. テストを目的としてロールを作成する場合は、次に、このロールに関連付けるローカル ユーザを作成します。「ローカル ユーザ アカウントの作成」（p.6-16）を参照してください。

ロール プロパティ

表 6-1 は、**New Role**（図 6-2）および **Edit Role**（図 6-4）フォームのすべての設定値の説明をまとめたものです。

表 6-1　ロール プロパティ

設定項目	説明
Disable this role	新しいユーザへのこのロールの割り当てを停止します。
Role Name	そのロールに固有の名前
Role Description	ロールの説明（任意）
Role Type	ロールが **Normal Login Role** なのか Clear Access 関連ロール（**Quarantine** ロールまたは **CAA Temporary** ロール）なのか。詳細は「ユーザ ロールのタイプ」（p.6-3）を、その他の情報は第 9 章「Clean Access の設定概要」を参照してください。

表 6-1　ロール プロパティ（続き）

設定項目	説明
VPN Policy	**（注）** IPSec/L2TP/PPTP およびローミングは廃止される可能性があり、今後のリリースで削除される予定です。 このロールのプロバイダー認証ユーザが CAS への接続に IPSec/L2TP/PPTP の暗号化を使用する必要があるかどうか。次のオプションを選択できます。 • **Deny**（デフォルト）— 暗号化は許可されません。ご使用の環境でこのレベルのセキュリティを必要としない場合は、IPSec/L2TP/PPTP 暗号化を拒否して、トラフィックによるネットワーク インフラへの負荷を回避できます。 • **Optional** — クライアントの選択によって暗号化を使用できます。 • **Enforce** — クライアントは IPSec/L2TP/PPTP 暗号化を使用しなければなりません。 **（注）** IPSec/L2TP/PPTP 暗号化ポリシー（Optional または Enforce）は、CAS 上でもイネーブルにしなければなりません（**Device Management > CCA Servers > Manage [CAS_IP] > Network > IPSec**）。CAS のポリシーの設定値がロール ポリシーの設定値よりも優先されます。これによって、ユーザがアクセスした CAS（サブネット）に基づいて暗号化の使用を制御できます。詳細は、『*Cisco NAC Appliance - Clean Access Server Installation and Administration Guide*』Relase 4.1(1) を参照してください。 **（注）** CAS とユーザ ロールの両方で Optional または Enforce の VPN ポリシーがイネーブルになっていると、CAA はログイン成功ダイアログからのリンクとして VPN 情報を表示します（図 11-72 を参照）。Web ログイン ユーザの場合は、VPN 情報フィールドが表示されるようにログアウト ページを設定する必要があります（「Show Logged-on Users」[p.6-13] を参照）。
Dynamic IPSec Key	イネーブルに設定されると、ログイン時に各ユーザに個別のワンタイム事前共有鍵が割り当てられます。ユーザは IPSec 接続を確立するために IPSec クライアントの事前共有鍵として、この鍵を使用しなければなりません。ディセーブルに設定されると、ユーザは IPSec 接続にデフォルトの鍵（すべてのユーザが共有）を使用する必要があります。「Show Logged-on Users」（p.6-13）で **IPSec info** を選択した場合、Web ログイン ユーザには、ログアウト ページで鍵が与えられます。

表 6-1　ロール プロパティ（続き）

設定項目	説明
Max Sessions per User Account (Case-Insensitive)	**Max Sessions per User Account** オプションによって、管理者は、同じユーザ証明書を同時に使用できるマシンの数を制限できます。この機能を使用すると、各ユーザのログイン セッション数が、設定数に制限されます。あるユーザ名のオンライン ログイン セッションが指定値（1 ～ 255、無制限の場合は 0）を超えると、次回のログイン試行時に、Web ログイン ページまたは CAA を通じて、ユーザがすべてのセッションの終了または最も古いセッションの終了を実行するよう促します。 **Case-Insensitive** チェックボックスを使用することにより、管理者は、最大セッション カウントに使用されるユーザ名に関して、大文字と小文字の区別を許可または不許可にすることができます。たとえば、大文字と小文字の区別を許可すると（ボックスは未選択、デフォルト）、`jdoe`、`Jdoe`、`jDoe` はすべて異なるユーザとして処理されます。大文字と小文字の区別をディセーブルにすると（ボックスを選択）、`jdoe`、`Jdoe`、`jDoe` はどれも同じユーザとして処理されます。
Retag Trusted-side Egress Traffic with VLAN (In-Band)	**インバンド構成 — 信頼側トラフィックの VLAN ID の再タグ付け** トラフィックが通過するように CAS 配置されると、CAS の信頼側を出るユーザ トラフィックの再タグ付けに、このフィールドに入力された値が使用されます。たとえば、2 人のユーザが同じ SSID で同じアクセス ポイントに接続した場合、これらのユーザのロールに応じて、ネットワークの信頼側へ CAS 通じてトラフィックが流れるときに、そのトラフィックに異なる VLAN ID をタグ付けできます（図 6-1 を参照）。 そのロールのユーザから外側へのトラフィックに VLAN ID を割り当てるには、このフィールドに値を入力します。VLAN ID 値を使用した内側へのトラフィックは、そのロールで元々使用された値（このような値があれば）が再割り当てされます。インバンド構成では、信頼側 VLAN の再タグ付けが実行されるのは、Real-IP および NAT Gateway モードの場合だけです。インバンドの Virtual Gateways モードでは、ロール割り当てに基づく VLAN の再タグ付けは実行されません。

表 6-1　ロール プロパティ（続き）

設定項目	説明
Out-of-Band User Role VLAN	**OOB（アウトオブバンド）構成 — 信頼側トラフィックへのロール VLAN の再タグ付け** ユーザがポスチャ評価と修復（必要な場合）を完了し、そのクライアント デバイスが証明済みとみなされた場合、そのクライアントが接続されているスイッチ ポートを、**Out-of-Band User Role VLAN** フィールドの指定値に基づき、異なるアクセス VLAN に割り当てることができます。したがって、同じポートに接続しているユーザ（異なる時に）を、そのユーザ ロールの設定値に基づいて異なるアクセス VLAN に指定できます。 OOB 構成では、制御対象ポートに対してロールベースの VLAN 変更が設定されている場合、ユーザ ロール作成時にアクセス LAN ID を指定する必要があります。管理対象スイッチ ポートからアウトオブバンド ユーザがログインすると、CAM は以下のことを実行します。 • そのユーザのログイン証明書に基づいて、そのユーザのロールを判断します。 • ポート プロファイルで、そのポートにロールベースの VLAN 変更が指定されているかどうかを確認します。 • そのクライアントの証明が完了したら、ユーザ ロールの **Out-of-Band User Role VLAN** フィールドに指定されている値に応じて、そのユーザをアクセス VLAN に変更します。 管理者は **New/Edit User Role** フォームに **VLAN Name** または **VLAN ID** を指定することができます。**VLAN Name** では、大文字と小文字が区別されます。VLAN Name にワイルドカードを指定する場合、abc、*abc、abc*、*abc* を使用することができます。スイッチは、ワイルドカード VLAN 名で最初に一致するものを使用します。 **VLAN ID** には番号のみ指定することができます。スイッチで指定された VLAN が検出されない場合（VLAN Name の入力ミスなど）、（イベント ログではなく）perfigo.log にエラーが表示されます。 詳細は、「デバイスおよびサブネットのグローバル フィルタリング」（p.3-8）および第 4 章「スイッチ管理：アウトオブバンド（OOB）配置の設定」を参照してください。
Bounce Switch Port After Login (OOB)	**Switch Management > Profiles > Port > New/Edit** ページで [Bounce the port based on role settings after VLAN is changed] オプションを最初にイネーブルにすると、ログインおよびポスチャ評価後に、エージェントはクライアントマシンの IP アドレスを更新 *しません*。 **（注）** このオプションは、ポート プロファイルがこれを使用するように設定された場合のみ適用されます。

表 6-1　ロール プロパティ（続き）

設定項目	説明
Refresh IP After Login (OOB)	**Switch Management > Profiles > Port > New/Edit** ページで [Bounce the port based on role settings after VLAN is changed] オプションを最初にイネーブルにすると、VLAN が認証 VLAN からアクセス VLAN に変更された場合に、ユーザがネットワークのアクセスに使用しているスイッチポートがバウンスされません。代わりに、この機能をイネーブルにすると、後続のログインおよびポスチャ評価でエージェントがクライアントマシンの IP アドレスを更新します。 **（注）** このオプションは、レイヤ 2 OOB モードが動作する仮想ゲートウェイ CAS にのみ適用されます。
After Successful Login Redirect to	ログインに成功すると、ユーザは、このフィールドに示されている Web ページに転送されます。以下の場所にユーザを転送できます • **previously requested URL —** （デフォルト）ログイン ページにリダイレクトされる前にユーザが要求した URL • **this URL —** 別のページにユーザをリダイレクトするには、テキスト フィールドに、[**http://**] と目的の URL を入力します。URL には、[**http://**] を含める必要があります。 **（注）** 通常、リダイレクト ページが指定されている場合は、新しいブラウザが開きます。ポップアップ ブロッカーがイネーブルになっていると、Cisco NAC アプライアンスは、ログイン ステータス、ログアウト情報、VPN 情報（ある場合）を表示するために、ログアウト ページとしてメイン ブラウザ ページを使用します。 「ログイン サクセス ページのリダイレクト」（p.5-15）も参照してください。
Redirect Blocked Requests to	ユーザがそのロールの [**Block**] IP トラフィック ポリシーによって、あるリソースへのアクセスをブロックされている場合、ユーザがブロックされているページを要求するとリダイレクトされます。以下の場所にユーザを転送できます • **default access blocked page —** ブロックされているアクセス用のデフォルト ページ • **this URL or HTML message —** このテキストフィールドに指定した特定の URL または HTML メッセージ。 「デフォルト ロールのトラフィック ポリシーの追加」（p.8-29）も参照してください。
Roam Policy	**（注）** IPSec/L2TP/PPTP およびローミングは廃止される可能性があり、今後のリリースで削除される予定です。 ローミング サポートがイネーブルになっている場合、このロールのユーザにローミングを許可するかどうかを指定します。詳細は、第 16 章「デバイス管理：ローミング（廃止予定）」を参照してください。

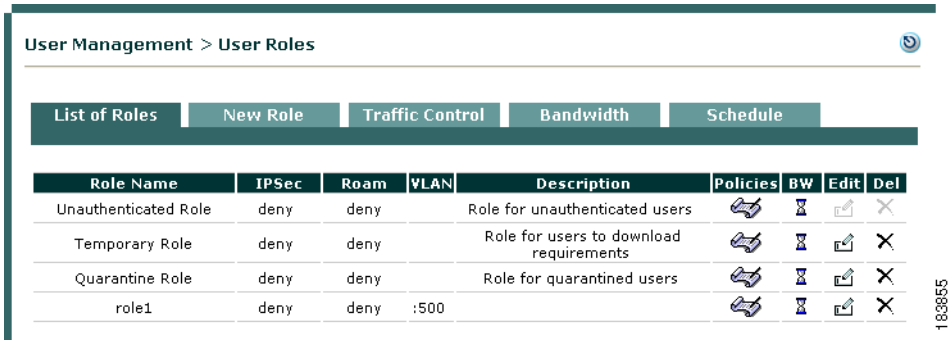
表 6-1　ロール プロパティ（続き）

設定項目	説明
Show Logged-on Users	ログアウト ページで Web ユーザに表示しなければならない情報。Web ユーザがログインに成功すると、ユーザのブラウザにログアウト ページが表示され、選択したオプションの組み合わせに基づいてユーザのステータスが示されます。 • **IPSec info —** そのユーザに割り当てられた IPSec 鍵。ダイナミック IPSec 鍵のオプションがイネーブルになっている場合は、ワンタイムの 128 ビット鍵です。ディセーブルになっている場合は、デフォルトの事前共有鍵です。 • **PPP info —** ネットワーク上の PPP アクセス用のパスワード • **User info —** ユーザ名など、そのユーザについての情報 • **Logout button —** ユーザをネットワークからログオフするボタン（Web ログアウト ページのみ） ログアウト ページの例は、「ログアウト ページの情報の指定」（p.5-16）を参照してください。 （注）　Agent ユーザの場合、CAS とユーザ ロールの両方で Optional または Enforce の VPN ポリシーがイネーブルになっていると、正常ログインおよびタスクバー メニューに、VPN Info ダイアログへのリンクが表示されます。図 11-72 を参照してください。

ロールの変更

List of Roles タブ（図 6-3）から、あらゆるユーザ ロールのトラフィック ポリシーおよび帯域幅ポリシーを設定できます。CAA Temporary ロール、Quarantine ロール、作成した Normal Login ロールを修正することも可能です。

図 6-3　List of Roles



List of Roles タブでは、次の操作を実行できます。

- **Policies** ボタンをクリックすると、**Traffic Control** タブが開き、そのロールのトラフィック フィルタ ポリシーを設定できます。詳細は、第 8 章「ユーザ管理：トラフィック制御、帯域幅、スケジュール」を参照してください。
- **BW** ボタンをクリックすると、**Bandwidth** タブが開き、ロール別のアップストリームとダウンストリームの帯域制限を設定できます。詳細は、「帯域利用の制御」（p.8-15）を参照してください。

- **Edit** ボタンをクリックすると、**Edit Role** タブが開き、ロールのプロパティを変更できます。以下の「ロールの変更」（p.6-14）を参照してください。
- **Delete** ボタンをクリックすると、そのロールと、関連するすべてのポリシーがシステムから削除され、ユーザには Unauthenticated ロールが割り当てられます。「ロールの削除」（p.6-15）を参照してください。
- ロールにネットワーク アクセス スケジュールを指定します。詳細は、「ユーザ セッション タイムアウトおよびハートビート タイムアウトの設定」（p.8-17）を参照してください。

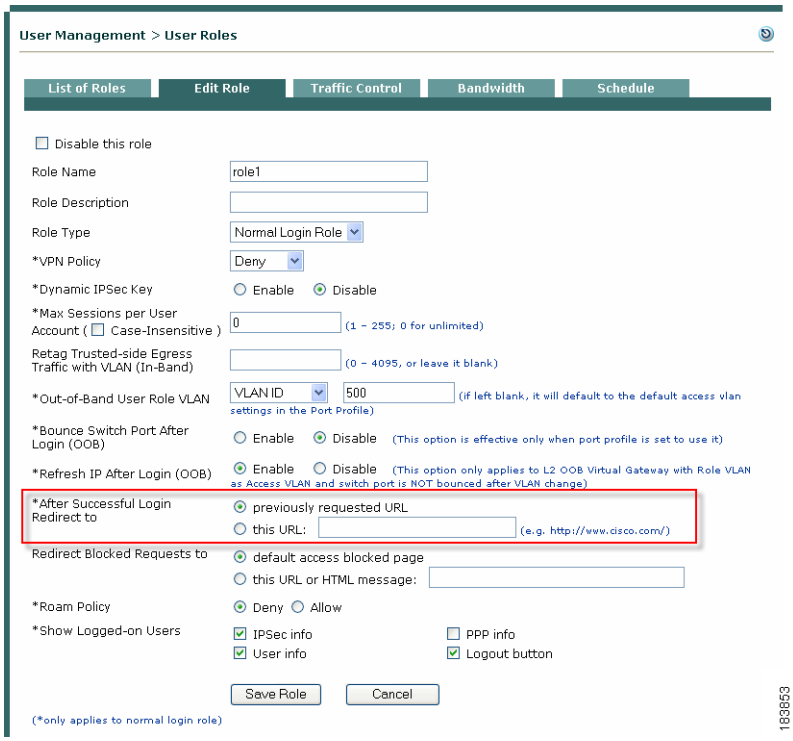
ロールの変更

1. **User Management > User Roles > List of Roles** の順番に進みます。
2. 表示されるロールには、次の種類があります。
   - **CAA Temporary** ロール — ログインおよび Cisco Access 脆弱性評価に CAA が必要とされる場合、CAA のパッケージまたは条件を満たすことを強制するためにユーザに割り当てられます。CAA Temporary ロールはシステム内に 1 つだけしかありません。このロールは修正できますが、追加はできません。
   - **Quarantine Role** — Clean Access のネットワーク スキャンによってそのユーザのシステムに脆弱性が発見された場合、ユーザを隔離するために割り当てられます。システムの Quarantine ロールのみを設定することも、また必要に応じて Quarantine ロールを追加することもできます。
   - **User-defined role** — 作成したユーザ ロール

（注）　**Unauthenticated** ロールにはトラフィック ポリシーと帯域幅ポリシーを設定できますが、その他の点では、このシステム デフォルト ロールは、修正も削除もできません。

3. ロールの横の **Edit** ボタンをクリックすると、**Edit Role** フォームが表示されます。

図 6-4　Edit Role



4. 目的に応じてロールの設定値を変更します。詳細は、「ロール プロパティ」（p.6-8）を参照してください。
5. **Save Role** をクリックします。

ロールの削除

ロールを削除するには、**User Management > User Roles** ページの **List of Roles** タブで、ロールの横に表示されている **Delete** ボタンをクリックします。これによって、そのロールと、関連するすべてのポリシーがシステムから削除され、ユーザには Unauthenticated ロールが割り当てられます。

削除されたロールでネットワークにアクティブに接続されているユーザは、ネットワークを使用できなくなります。ただし、接続はアクティブな状態のままになります。このようなユーザは、**Monitoring > Online Users > View Online Users** ページで、そのユーザの横に表示されている **Kick User** ボタンをクリックし、ネットワークから手動でログオフしなければなりません。このようなユーザは、オンライン ユーザ ページの **Role** カラムに **Invalid** の値が表示されます。

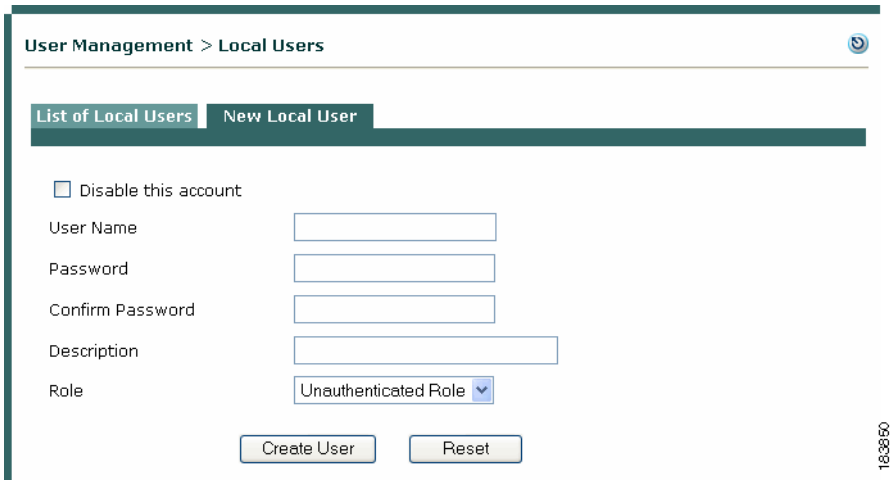
ローカル ユーザ アカウントの作成

ローカル ユーザとは、CAM 自体によって検証され、外部の認証サーバによる検証を受けないユーザです。ローカル ユーザ アカウントは全般的な利用を目的としたものではありません（このユーザは Web 管理コンソール以外でパスワード変更できません）。ローカル ユーザ アカウントは、主として、テストまたはゲスト ユーザ アカウントを目的としています。テストに使用する場合は、ユーザ ロール作成後すぐにユーザを作成しなければなりません。

ローカル ユーザの作成

1. **User Management > Local Users > New Local User** の順番に進みます。

図 6-5　New Local User



2. ユーザ アカウントをすぐにアクティブにする場合は、**Disable this account** チェックボックスを選択しないでおきます。
3. **User Name** に、そのユーザ固有の名前を入力します。これはシステム内でユーザを識別するログイン名です。
4. **Password** フィールドにパスワードを入力し、**Confirm Password** フィールドに再入力します。パスワード値では、大文字と小文字が区別されます。
5. （任意）**Description** にそのユーザの説明を入力します。
6. **Role** リストから、そのユーザのデフォルトのロールを選択します。このリストには、設定されているロールがすべて表示されます。そのユーザに割り当てたいロールがまだない場合は、**User Roles** ページでそのロールを作成し、新しいロールでユーザ プロファイルを変更します。
7. 完了したら、**Create User** をクリックします。

List of Local Users タブにそのユーザが表示されます。ここから、ユーザ情報の表示、名前、パスワード、ロールなどのユーザ設定値の修正、ユーザの削除を実行できます。