CHAPTER 1

はじめに

この章では、Cisco NAC アプライアンス ソリューションの概要について説明します。この章の内容は、次のとおりです。

- 「Cisco NAC アプライアンスとは」（P.1-1）
- 「Cisco NAC アプライアンスのコンポーネント」（P.1-2）
- 「CAS の機能」（P.1-6）
- 「CAS 管理ページの概要」（P.1-7）
- 「グローバルおよび ローカルの管理設定値」（P.1-9）

Cisco NAC アプライアンスとは

Cisco Network Admission Control（NAC）アプライアンス（以前の Cisco Clean Access）は、使いやすく強力なアドミッション コントロールおよび準拠性強制ソリューションです。包括的なセキュリティ機能、インバンドまたはアウトオブバンドの導入オプション、ユーザ認証ツール、帯域およびトラフィックのフィルタリング制御機能を備え、高度なネットワーク制御とセキュリティを実現します。NAC アプライアンス（Cisco Clean Access）は、ネットワークの集中アクセス管理ポイントとして、セキュリティ、アクセス、準拠性のポリシーを一箇所で管理できるので、ネットワークを通じて多くのデバイスにポリシーを伝播する必要はありません。

Cisco NAC アプライアンスには、ユーザ認証、ポリシーベースのトラフィック フィルタリング、クライアント ポスチャ評価と修復などのセキュリティ機能があります。Clean Access は、ウィルスやワームをネットワークのエッジで食い止めます。また、リモート システムやローカル システムの検査によって、指定条件を満たしていないユーザ デバイスは、ネットワークにアクセスできないようにします。

Cisco NAC アプライアンスは、Clean Access Manager（CAM）の Web コンソールから管理し、Clean Access Server（CAS）およびオプションの Agent を通じて実行する統合ネットワーク ソリューションです。NAC アプライアンス ソフトウェアはネットワークの必要性に応じ、最適な設定で導入できます。CAS は、単純なルーティング機能、高度な DHCP サービス、およびその他のサービスを提供するエッジ デバイスの第 1 ホップ ゲートウェイとして導入できます。ネットワーク内の要素がすでにこのサービスを提供している場合は、Bump-In-The-Wire（BITW）方式で導入することにより、既存のネットワークを変更せずに、これらの要素と CAS を共存させることが可能です。

その他にも、Cisco NAC アプライアンスには、次のような機能があります。

- 標準ベースのアーキテクチャ：HTTP、HTTPS、XML、Java Management Extensions（JMX）を使用できます。
- ユーザ認証：Kerberos、LDAP、RADIUS、Windows NT ドメインなど、既存のバックエンド認証サーバと統合できます。

- VPN コンセントレータとの統合：Cisco VPN コンセントレータ（VPN 3000、ASA など）と統合し、Single Sign-On（SSO; シングルサインオン）を実現できます。
- Cisco NAC アプライアンス準拠性ポリシー：Cisco NAC アプライアンス Agent または Nessus ベースのネットワーク ポート スキャンによるクライアント ポスチャ評価および修復の設定が可能です。
- L2 または L3 導入オプション：CAS は、ユーザの L2 近接内、またはユーザから複数ホップ離して導入することもできます。1 つの CAS を L3 と L2 の両方のユーザに使用できます。
- インバンド（IB）またはアウトオブバンド（OOB）の導入オプション：Cisco NAC アプライアンスはユーザ トラフィックが常に通過するように導入することもできますし、またアウトオブバンド構成にして、クライアントは認証後ネットワークを迂回し、ポスチャ評価と修復時にだけネットワークを通過するように導入することもできます。
- トラフィック フィルタリング ポリシー：ロール ベース IP およびホスト ベース ポリシーによって、インバンド ネットワーク トラフィックを細かく柔軟に制御できます。
- 帯域幅管理制御：ダウンロードまたはアップロードの帯域幅を制限します。
- ハイ アベイラビリティ：アクティブまたはパッシブのフェールオーバー（サーバが 2 つ必要）によって不測のシャットダウンが発生しても確実にサービスを継続できます。CAM サーバと CAS サーバの両方またはいずれかのペアをハイ アベイラビリティ モードに設定できます。

（注） Cisco Integrated Services Router（ISR; サービス統合型ルータ）に実装された Cisco NAC ネットワーク モジュールはハイ アベイラビリティをサポートしていません。

Cisco NAC アプライアンスのコンポーネント

Cisco NAC アプライアンスは、CAM の Web コンソールから管理し、CAS およびオプションの Agent を通じて実行する統合ネットワーク ソリューションです。Cisco NAC アプライアンスは、クライアント システムの検査、ネットワーク要求の強制、パッチやアンチウィルス ソフトウェアの配布を実行するとともに、脆弱なクライアントや感染したクライアントをネットワーク アクセス**前に**隔離し、修復します。Cisco NAC アプライアンスは、次のコンポーネントで構成されています（図 1-1 を参照）。

- **Clean Access Manager（CAM）**：Cisco NAC アプライアンス用の管理サーバ。CAM のセキュアな Web コンソールを通じ、一箇所で最大 20 の CAS を管理できます（SuperCAM をインストールする場合は最大 40 の CAS）。アウトオブバンドの場合は、Web 管理コンソールから SNMP を使用してスイッチの制御やユーザ ポートの VLAN 割り当てを実行できます。

（注） CAM Web 管理コンソールには、Internet Explorer 6.0 以上、および高度暗号化（64 ビットまたは 128 ビット）を必要とします。高度暗号化はクライアント ブラウザの Web ログインおよび Agent の認証にも必要です。

- **Clean Access Server（CAS）**：非信頼（管理対象の）ネットワークと信頼ネットワークの間の強制サーバ。CAS は、ネットワーク アクセス権限、認証要件、帯域幅の制限、Cisco NAC アプライアンス システムの要件など、ユーザが CAM Web 管理コンソールで定義したポリシーを強制します。

  CAS はスタンドアロン アプライアンス（Cisco NAC-3300 シリーズなど）に設置するか、Cisco ISR シャーシ内のネットワーク モジュール（Cisco NME-NAC-K9）として設置でき、インバンド（常にユーザ トラフィックが通過）またはアウトオブバンド（認証またはポスチャ評価時だけユーザ トラフィックが通過）で導入できます。また、レイヤ 2 モード（ユーザは CAS と L2 隣接）、またはレイヤ 3 モード（ユーザは CAS から L3 で複数ホップ離れている）で導入することもできます。

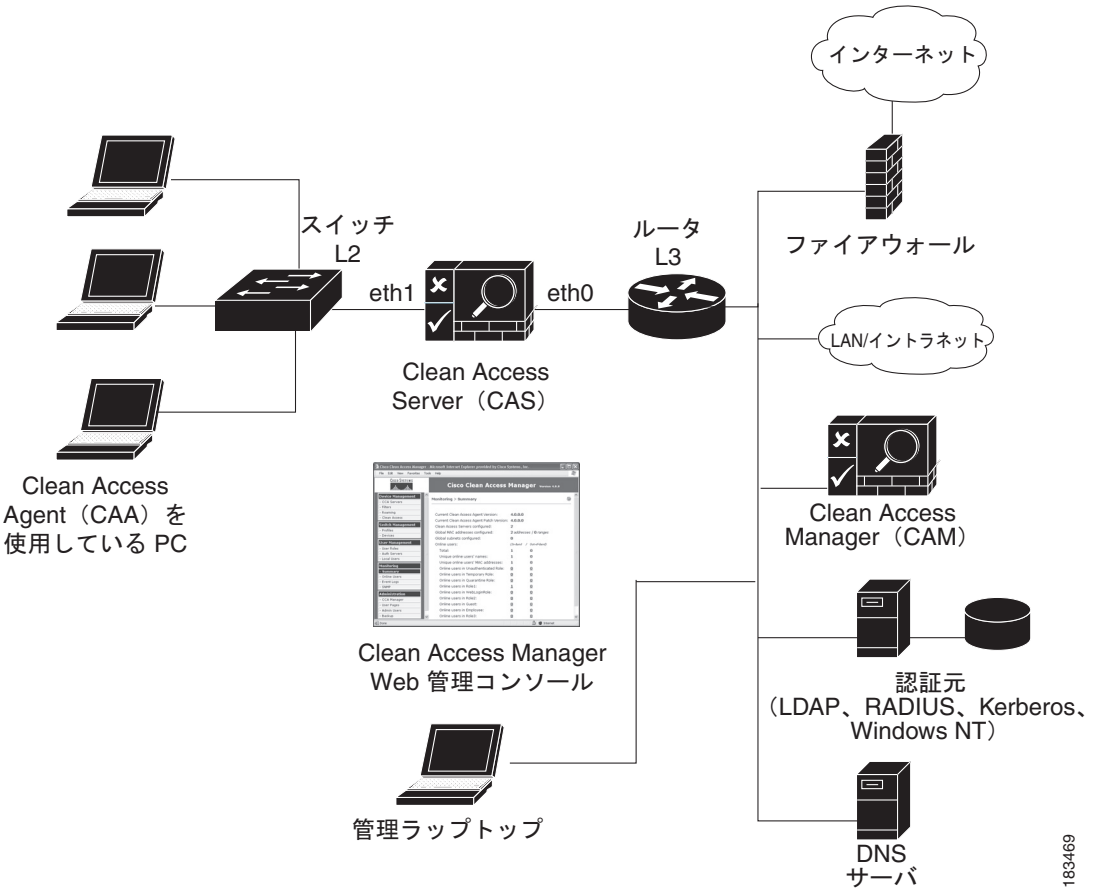
  さまざまなネットワーク セグメントの要件に合わせて、各種のサイズと容量の CAS を複数導入することもできます。Cisco NAC-3300 シリーズ アプライアンスを企業の本社に設置して数千のユーザを処理すると当時に、1 台以上の Cisco NAC ネットワーク モジュールを ISR プラットフォームに設置して、出張所などの少数のユーザ グループを収容するといったことができます。

- **Cisco NAC アプライアンス Agent**：クライアント マシンにあるオプションの読み取り専用の永続的または一時的な Agent。Cisco NAC アプライアンス Agent は、アプリケーション、ファイル、サービス、またはレジストリ キーを検査し、ネットワークへのアクセス権を付与する前に、指定されたネットワーク要件およびソフトウェア要件にクライアント マシンが適合しているかどうか確認します。

  （注）　Agent によるクライアント ポスチャ評価には、クライアント側ファイアウォールによる制約はありません。このエージェントは、パーソナル ファイアウォールがインストールされ、稼動していても、クライアントのレジストリ、サービス、アプリケーションを検査できます。

- **Cisco NAC アプライアンス アップデート**：事前に作成されたひとまとまりのポリシーまたはルールの定期更新ツール。これらのポリシーまたはルールは、オペレーティング システム、antivirus（AV; アンチウィルス）、antispyware（AS; アンチスパイウェア）、およびその他のクライアント ソフトウェアの最新の状態を検査するために使用されます。AV ベンダーおよび AS ベンダーに対するビルトイン サポートを提供しています。

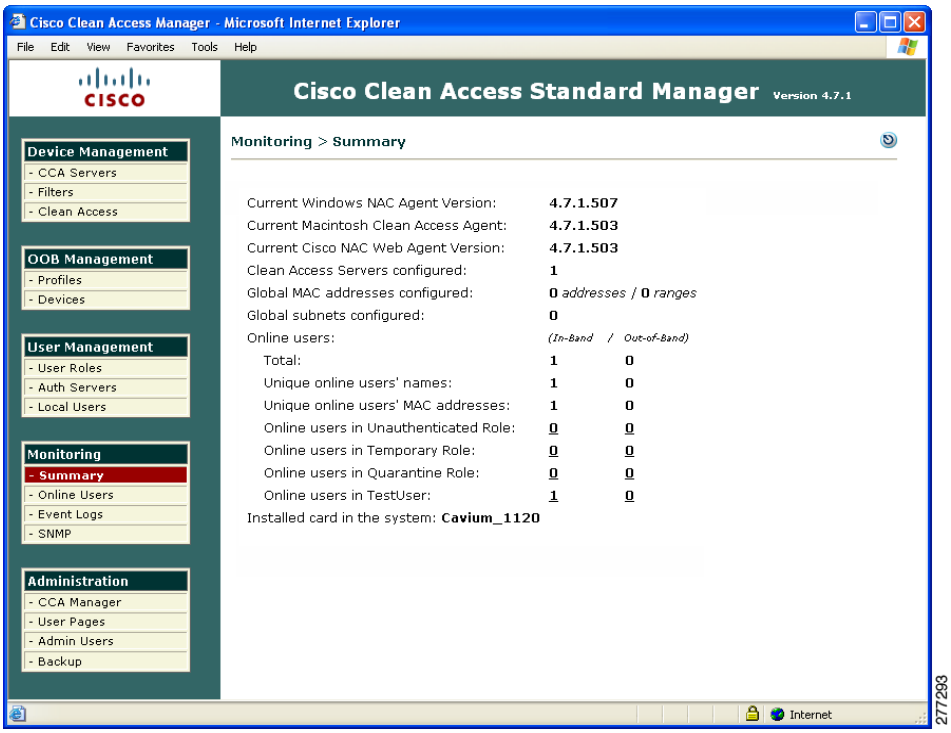
図 1-1　Cisco NAC アプライアンスの導入（L2 インバンドの例）



Clean Access Manager（CAM）

CAM は、Cisco NAC アプライアンスの配置ですべての CAS、ユーザ、およびポリシーの設定と監視を集中管理する管理サーバとデータベースです。CAM を使用して最大 20 の CAS を管理できます。CAM の Web 管理コンソールはセキュアなブラウザベースの管理インターフェイスです（図 1-2）。Web コンソールのモジュールの簡単な説明については、『*Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(1)*』の「Admin Console Summary」を参照してください。アウトオブバンドの場合は、Web 管理コンソールの [OOB Management] モジュールで CAM のドメインのスイッチを追加、制御し、スイッチ ポートを設定できます。

図 1-2　　CAM Web 管理コンソール



Clean Access Server（CAS）

CAS は非信頼ネットワークと信頼ネットワークの間のゲートウェイです。CAS は、次に示すインバンド（IB）モードまたはアウトオブバンド（OOB）モードで動作します。

- IB バーチャル ゲートウェイ（L2 トランスペアレント ブリッジ モード）
- IB Real-IP ゲートウェイ
- OOB バーチャル ゲートウェイ
- OOB Real-IP ゲートウェイ

『*Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(1)*』では、CAM Web 管理コンソールを使用した CAS と Cisco NAC アプライアンスのグローバル設定と管理について説明しています。

Cisco NAC アプライアンス Agent

Agent が Cisco NAC アプライアンスの配置でイネーブルになっている場合、ネットワークにアクセスするコンピュータが、指定したシステム要件を満たしていることを確認できます。Agent は Windows ユーザ マシンに常駐する、使いやすく負荷の小さい読み取り専用のプログラムです。ユーザがネットワークにアクセスしようとすると、Agent では必要とされるソフトウェアについてクライアント システムを確認し、アップデートやソフトウェアが見つからない場合、その入手を支援します。

設定したシステム チェックに失敗した Agent ユーザには Agent Temporary ロールが割り当てられます。このロールでユーザに与えられるネットワーク アクセスは Agent 要件への準拠に必要なリソースへのアクセスに限定されます。クライアント システムは要件を満たすと、「クリーン」と見なされ、ネットワーク アクセスが許可されます。

Cisco NAC アプライアンスで利用できる Cisco NAC アプライアンス Agent には次の種類があります。

- Cisco NAC Agent（Windows クライアント マシン用の永続的な Agent）
- Windows Clean Access Agent（リリース 4.7 が下位互換性のある 4.6(1) よりも前のリリースで利用できる Windows クライアント マシン用の永続的な Agent）
- Mac OS X Clean Access Agent（Macintosh クライアント マシン用の永続的な Agent）
- Cisco NAC Web Agent（Windows クライアント マシン用の一時的な Agent）

Cisco NAC アプライアンスで利用できる Agent の種類の詳細については、『*Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(1)*』の「Cisco NAC Appliance Agents」の章を参照してください。

Cisco NAC アプライアンス アップデート

事前に作成されたひとまとまりのポリシーまたはルールの定期更新ツールは、オペレーティング システム、AV（アンチウィルス）、AS（アンチスパイウェア）、およびその他のクライアント ソフトウェアの最新の状態を検査するために使用できます。Cisco NAC アプライアンスは主な AV ベンダーおよび AS ベンダーに対するビルトイン サポートを提供しています。詳細については、『*Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(1)*』の「Retrieving Cisco NAC Appliance Updates」を参照してください。

CAS の機能

次に、CAS の主な機能および利点を示します。

- インバンドおよびアウトオブバンドでの導入
- レイヤ 2 またはレイヤ 3 の配置
- Cisco VPN コンセントレータとの統合
- セキュアなユーザ認証
- Cisco NAC アプライアンス ネットワークベースおよびエージェントベースのスキャンと修復
- ロールベース アクセス コントロール
- 信頼できない（管理対象）クライアントの DHCP アドレス割り当て、または DHCP リレーまたはパススルー モード
- Network Address Translation（NAT; ネットワーク アドレス変換）サービス、およびダイナミックまたは 1:1 NAT のサポート（非運用環境のみ）

- 帯域幅管理
- イベント ロギングおよびレポート サービス
- VLAN（仮想 LAN）のサポート。CAS を VLAN 終端ポイントに設定したり、VLAN をパススルーさせたり、VLAN ベース アクセス制御を実行することができます。
- ほとんどのネットワーク アーキテクチャに CAS を統合できるようにする柔軟な導入オプション
- ハイ アベイラビリティ：アクティブまたはパッシブのフェールオーバー（サーバが 2 つ必要）によって不測のシャットダウンが発生しても確実にサービスを継続できます。CAM サーバと CAS サーバの両方またはいずれかのペアをハイ アベイラビリティ モードに設定できます。

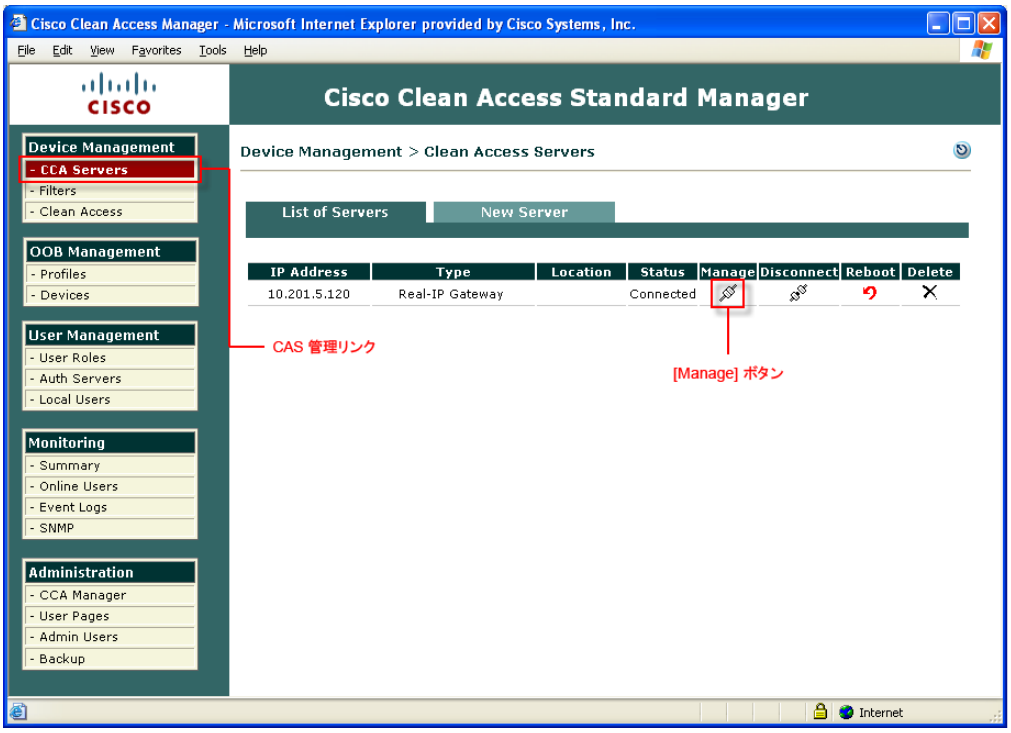
（注）　Cisco Integrated Services Router（ISR; サービス統合型ルータ）に実装された Cisco NAC ネットワーク モジュールはハイ アベイラビリティをサポートしていません。

CAS 管理ページの概要

CAS を Web 管理コンソールから管理できるようにするためには、その CAS を CAM ドメインに追加する必要があります。手順については、「CAM への CAS の追加」（P.4-2）を参照してください。ドメインに追加した CAS に管理コンソールからアクセスするには、次のようにします。このマニュアルで *CAS 管理*ページと記述されている場合、以下に示されている一連のページ、タブ、フォームを表します。

1. [Device Management] モジュールの [CCA Servers] リンクをクリックします。デフォルトでは、[List of Servers] タブが表示されます。

図 1-3　[Device Management] > [CCA Servers] > [List of Servers]

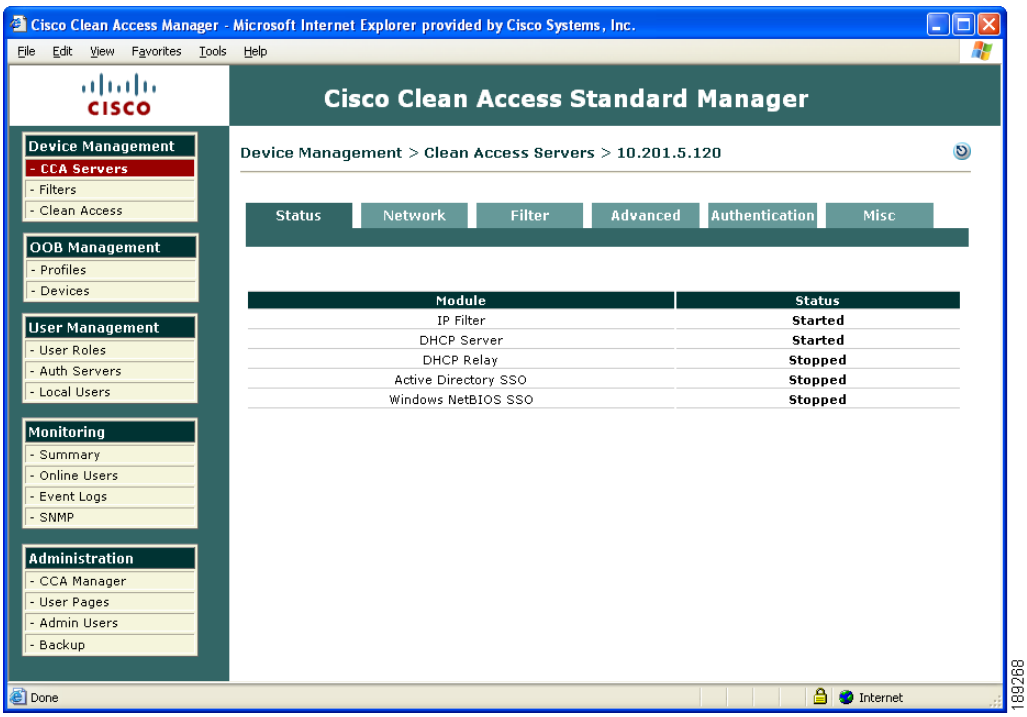


2. アクセスする CAS の [Manage] ボタンをクリックします。

（注）　ハイ アベイラビリティ構成の CAS では、最初にサービス IP が自動的に表示され、現在アクティブな CAS の IP アドレスがカッコ内に表示されます。

3. 図 1-4 に、CAS 管理ページを示します。デフォルトでは、[Status] タブが表示されます。

図 1-4　CAS 管理ページ



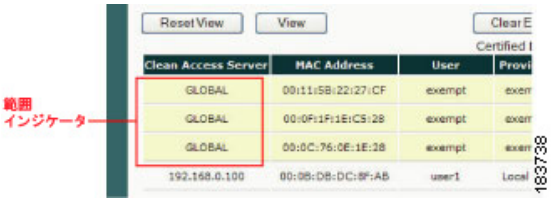
グローバルおよび ローカルの管理設定値

CAM の Web 管理コンソールには、次のような種類の設定値があります。

- **CAM 管理設定値**は、CAM だけに関連する設定値です。これらには、IP アドレスとホスト名、SSL 証明書情報、ハイ アベイラビリティ（フェールオーバー）の設定値などがあります。
- **グローバル管理設定値**は、CAM で設定され、CAM から**すべての** CAS に適用されます。これには、認証サーバ情報、グローバル デバイスおよびサブネット フィルタ ポリシー、ユーザ ロール、Cisco NAC アプライアンスの設定などがあります。
- **ローカル管理設定値**は、該当する管理コンソールの CAS 管理ページで設定され、その CAS だけに適用されます。これには、CAS ネットワークの設定値、SSL 証明書、VPN コンセントレータの統合、DHCP および 1:1 NAT コンフィギュレーション、IPSec キー変更、ローカル トラフィック制御ポリシー、ローカル デバイスおよびサブネット フィルタ ポリシーなどがあります。

設定値のグローバルまたはローカルの範囲は、図 1-5 のように、Web 管理コンソールの [Clean Access Server] カラムに表示されます。

図 1-5　　設定値の範囲



- **GLOBAL**：CAM Web 管理コンソールからグローバル形式で作成されたエントリです。この CAM のドメイン内のすべての CAS に適用されます。
- **<IP アドレス>**：CAS 管理ページからローカル形式で作成されたエントリです。この IP アドレスを持つ CAS だけに適用されます。

ほとんどの場合、グローバル設定は、設定を作成するために使用するグローバル フォームから追加、編集、および削除します。ローカル設定は、設定を作成するために使用するローカル フォームから追加、編集、および削除します。

一部のページには、わかりやすいようにグローバル設定値（GLOBAL で表記）、およびローカル設定値（IP アドレスで表記）も表示されています。通常、これらのローカル設定値はグローバル ページで修正したり削除することができますが、ローカル設定値の**追加**は、特定の CAS 用のローカル CAS 管理ページからしか実行できません。

設定値のプライオリティ

多くの場合、1 つの CAS に、グローバル設定値（すべての CAS 用に CAM で設定された値）とローカル設定値（CAS 固有の値）が両方あります。グローバルとローカルの設定値が競合する場合は、一般にローカル設定値がグローバル設定値よりも優先されます。以下の点に留意してください。

- ある*範囲*の MAC アドレスおよびトラフィック制御ポリシーに影響を与えるデバイス フィルタ ポリシーでは、ポリシーのプライオリティ（[Device Management] > [Filters] > [Devices] > [Order] での高低）により、適用するグローバル ポリシーまたはローカル ポリシーが決まります。個別の MAC アドレスに対するデバイス フィルタ ポリシーは、個別の MAC アドレスを含むある範囲のアドレスに対するフィルタ ポリシー（グローバルまたはローカル）よりも優先されます。
- 1 つのサブネット フィルタがより広いサブネット フィルタ内のアドレス範囲のサブセットを指定しているサブネット フィルタ ポリシーでは、サブネット アドレス範囲の大きさに基づいて CAM がフィルタのプライオリティを決定します。サブネットが小さいほど（サブネット マスク /30 や /28 など）、サブネット フィルタ階層内の優先度が高くなります。
- 一部の機能は、CAM で設定する前に、まず CAS で（CAS 管理ページで）イネーブルにしなければなりません。たとえば、次のような機能が該当します。
  - Agent のレイヤ 3 サポート（マルチホップ L3 配置の場合）
  - 帯域幅管理
  - ユーザ ロール内のユーザと CAS の間での VPN ポリシーの使用
- Cisco NAC アプライアンスの要件およびネットワーク スキャン プラグインは、CAM からグローバルに設定され、すべての CAS に適用されます。