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を説明します。この章の内容は以下のとおりです。

Cisco Clean Access（NAC アプライアンス）とは

Cisco Network Admission Control（NAC）アプライアンスは Cisco Clean Access とも呼ばれており、使いやすく強力なアドミッション制御 / 適合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、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、完全なネットワーク制御とセキュリティを実現します。Cisco NAC アプライアンスは、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、適合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 Clean Access（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、Clean Access 脆弱性評価、修復（ポスチャ評価とも呼ばれます）などのセキュリティ機能があります。Clean Access は、ウイ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 Clean Access（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、CAS およびオプションの CAA 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 アプライアンスはネットワークの必要性に応じ、最適な設定で使用できます。Clean Access Server 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使用できます。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。

そのほかにも、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。
- Active Directory SSO — Windows サーバの Active Directory と統合して、Clean Access Agent ユーザが Windows システムにシングル サインオンでログインできるようにします。
- Clean Access 適合性ポリシー — Clean Access 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の脆弱性評価および修復の設定が可能です。
- L2 または L3 配置のオプション — CAS は、ユーザの L2 近接内に配置することも、またユーザから複数ホップ離して配置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）導入オプション — Cisco NAC アプライアンスはユーザ トラフィックを処理するように配置することも、アウトオブバンドで配置して、クライアントが脆弱性評価および修復の処理中にのみ Clean Access ネットワークを経由し、認証後（ポスチャ評価）はバイパスできるようにすることができます。
- 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 ポリシーにより、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できます。
- ハイ アベイラビリティ — アクティブ / パッシブなフェールオーバー（2 つのサーバが必要）により、予期せぬシャットダウンが発生してもサービスを続行できます。CAM マシンまたは CAS マシンのペアをハイ アベイラビリ モードで構成できます。

Cisco NAC アプライアンス コンポーネント

Cisco NAC アプライアンスは、Clean Access Manager の Web コンソールから管理し、CAS およびオプションの CAA 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、パッチやアンチウイルス 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）—** Clean Access 用の管理サーバ。CAM の Web コンソールを通じ、1 カ所で最大 20 の CAS を管理できます（SuperCAM をインストールする場合は 40 の CAS）。アウトオブバンド（OOB）配置の場合、Web 管理コンソールで SNMP を使用してスイッチおよびユーザ ポートの VLAN 割り当てを制御できます。

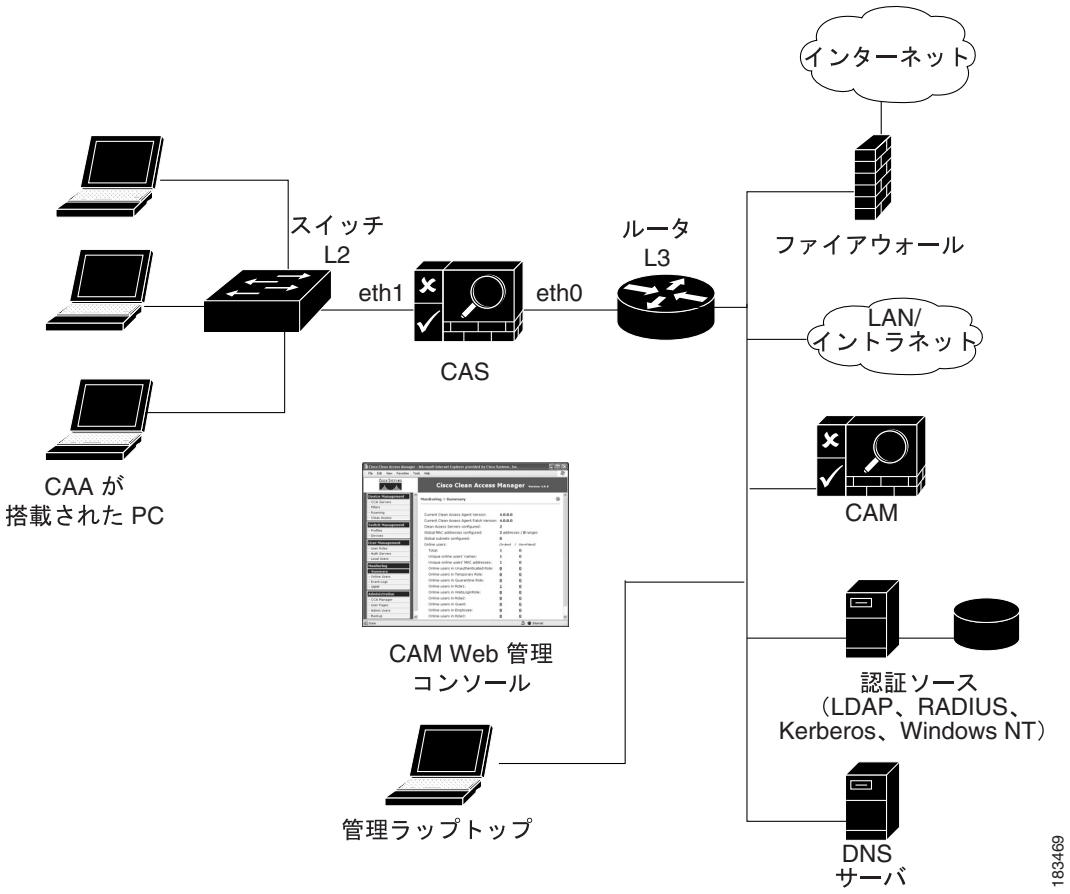
（注）　CAM Web 管理コンソールには、Internet Explorer 6.0 以上、および高度暗号化（64 ビットまたは 128 ビット）を必要とします。高度暗号化はクライアント ブラウザの Web ログインおよび CAA の認証にも必要です。

- **Clean Access Server（CAS）—** 非信頼（管理対象）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、認証条件、帯域幅の制限、Clean Access システムの条件など、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。インバンド（常にユーザ トラフィックを処理する）またはアウトオブバンド（認証 / ポスチャ評価中にのみユーザ トラフィックを処理する）で配置できます。レイヤ 2 モード（ユーザは CAS に L2 隣接）またはレイヤ 3 モード（ユーザは CAS から複数 L3 ホップ離れる）で配置することもできます。
- **Clean Access Agent（CAA）—** Windows クライアントに常駐するオプションの読み取り専用エージェント。CAA 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条件およびソフトウェア条件にクライアントが適合しているかどうか確認します。

（注）　CAA　の脆弱性評価には、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、稼働していても、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。

- **Clean Access Policy Updates —** 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、OS（オペレーティング システム）、AV（アンチウイルス）、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されます。24 の AV ベンダーおよび 17 の 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。

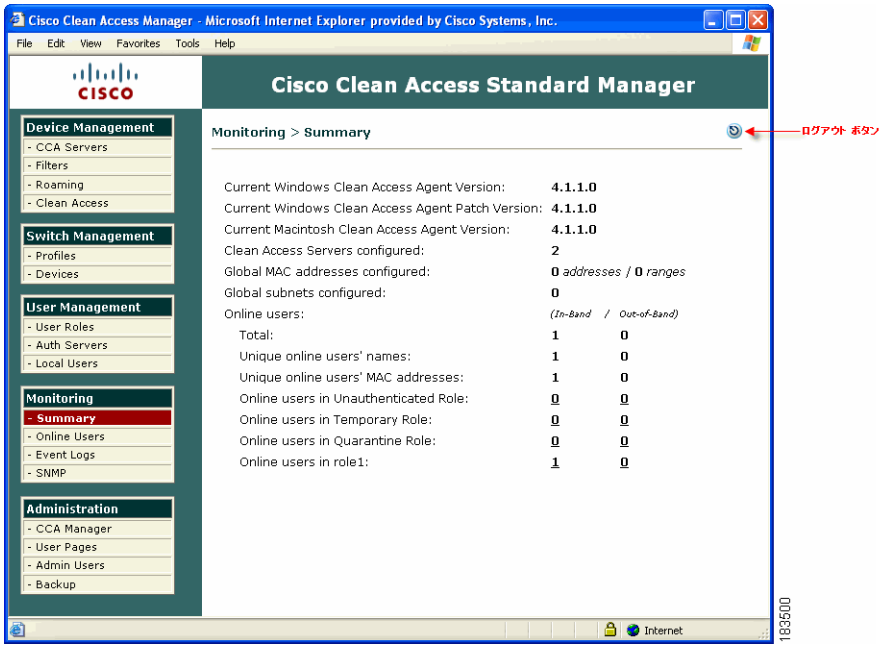
図 1-1　Cisco NAC アプライアンスの配置（L2 インバンド例）



CAM

CAM は、導入された Cisco NAC アプライアンスのすべての CAS、ユーザ、ポリシーの設定およびモニタリングを集中管理するサーバであり、またデータベースでもあります。1 つの CAM で最大 20 の CAS を管理できます。CAM の Web 管理コンソールは、ブラウザベースのセキュアな管理インターフェイスです（図 1-2 を参照）。Web コンソールのモジュールに関する概要は、「管理コンソールの概要」（p.1-12）を参照してください。アウトオブバンド（OOB）配置で利用する場合、Web 管理コンソールは、**スイッチ管理**モジュールとなり、CAM のドメイン内でスイッチの追加や制御およびスイッチ ポートの構成を行います。

図 1-2　CAM Web 管理コンソール



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として機能します。CAS は次のいずれかのインバンド（IB）モードまたはアウトオブバンド（OOB）モードで動作できます。

- IB Virtual Gateway（L2 トランスペアレント ブリッジ モード）
- IB Real-IP Gateway
- IB NAT Gateway（NAT サービス付きの IP ルータ / デフォルト ゲートウェイ）
- OOB Virtual Gateway
- OOB Real-IP Gateway
- OOB NAT Gateway

（注）　NAT Gateway（インバンドもアウトオブバンドも）は、実働環境での利用にはサポートされていません。

このマニュアルでは、CAM Web 管理コンソールを使用した CAS および Cisco NAC アプライアンスのグローバル コンフィギュレーションと管理について説明します。

CAS 動作モードの概要は、「管理ドメインへの CAS の追加」（p.3-2）を参照してください。CAS 構成の詳細は、『*Cisco NAC Appliance - Clean Access Server Installation and Administration Guide*』Release 4.1(1) を参照してください。

OOB の実装および設定の詳細は、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。

DHCP 設定、Cisco VPN コンセントレータの統合、CAS ハイ アベイラビリティの統合またはローカル トラフィック ポリシーの設定など、CAS でローカルに設定されたオプションの詳細は、『*Cisco NAC Appliance - Clean Access Server Installation and Administration Guide*』Release 4.1(1) を参照してください。

Clean Access Agent

Cisco NAC アプライアンスを導入すると、ネットワークにアクセスするコンピュータが指定のシステム条件に適合しているどうかを CAA で確認できます。CAA は、ユーザの Windows マシンにインストールされる軽くて使いやすい読み取り専用プログラムです。CAA は、ユーザがネットワークへのアクセスを試行すると、クライアント システムを検査して、必要なソフトウェアがあるかどうかを確認し、足りないアップデートまたはソフトウェアがあればユーザがそれを取得できるように支援します。

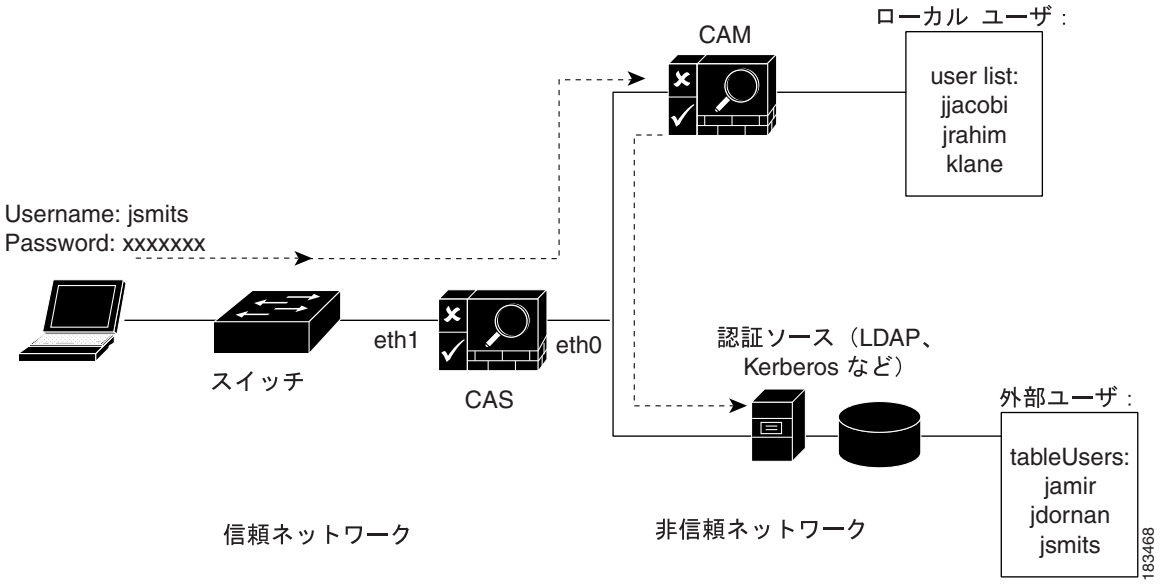
設定されたシステム検査に合格しない Agent ユーザは、CAA Temporary ロールに割り当てられます。このロールのユーザには、限定的なアクセス権が付与され、Clean Access の条件を満たすために必要なリソースだけにネットワーク アクセスが制限されます。クライアント システムが条件を満たせば、「クリーン」であるとみなされ、ネットワーク アクセスが許可されます。

ユーザの管理

CAM を使用すると、既存の認証メカニズムをネットワーク上のユーザに簡単に適用できます（図 1-3 を参照）。ユーザ ロールをカスタマイズしてグループにまとめて、特定のユーザ グループ用のトラフィック ポリシー、帯域幅制限、セッション期間、Clean Access 脆弱性評価など Cisco Clean Access のポリシーを定義できます。その後、ロールマッピングを使用して、外部認証ソースから渡された VLAN ID または属性に基づいてユーザをこれらのポリシーにマップできます。

CAS は、非信頼ネットワークから HTTP 要求を受信すると、その要求が認証済みのユーザからのものかどうかを確認します。認証済みのユーザからの要求でない場合は、そのユーザにカスタマイズ可能な安全な Web ログイン ページが提示されます。Web ログイン ページを介して安全に送信されたユーザの証明書は、CAM 自身（ローカル ユーザの検査の場合）によって、または LDAP、RADIUS、Kerberos、Windows NT など、外部認証サーバで実行できます。Clean Access Agent が配布される場合、ユーザは初期 Web ログイン後に Agent をダウンロードおよびインストールし、その後ログイン / ポスチャ評価に使用します。

図 1-3　認証パス



Web 管理コンソールの Clean Access モジュールを使用して CAA やネットワーク ポート スキャンのスキャンの条件を設定すると、Clean Access の脆弱性評価や修復（ポスチャ評価）を設定して認証済みユーザに適用できます。

IP ベースおよびホストベースのトラフィック ポリシーによって、認証前、ポスチャ評価の実行中、およびユーザ デバイスが「クリーン」と証明されたあとに、ユーザのネットワーク アクセスを制御できます。

IP ベース、ホストベース、および（Virtual Gateway 構成の場合）レイヤ 2 イーサネットのトラフィック ポリシーによって、認証前、ポスチャ評価の実行中、およびユーザ デバイスが「クリーン」と証明されたあとに、ユーザのネットワーク アクセスを制御できます。

（注） レイヤ 2 イーサネットのトラフィック制御は、Virtual Gateway モードの CAS 動作にのみ適用されます。

さらに、Online Users ページ（L2 および L3 配置の場合）や Certified Devices List（L2 配置の場合のみ）を通じて、Web コンソールからユーザの活動を監視できます。

インストール要件

ここでは、次の項目について説明します。

製品ライセンスおよびサービス契約のサポート

（注）　製品ライセンスの入手およびインストール手順、および Cisco NAC アプライアンスのサービス契約へのサポートの詳細は、『*Cisco NAC Appliance Service Contract / Licensing Support*』を参照してください。

初期 CAM ライセンスを追加すると、CAM Web コンソールの上部にインストールされた Clean Access Manager ライセンスのタイプが表示されます。

- **Cisco Clean Access Lite Manager** は 3 つの Clean Access Server をサポートします。
- **Cisco Clean Access Standard Manager** は 20 の Clean Access Server をサポートします。
- **Cisco Clean Access Super Manager** は 40 の Clean Access Server をサポートします（SuperCAM は NAC-3390 プラットフォームでのみ実行されます）。

また、ライセンスの追加後、**Administration > CCA Manager > Licensing** ページに現在存在するライセンス タイプが表示されます。詳細は、「ライセンス」（p.14-21）を参照してください。

ソフトウェアのアップグレード

CAM/CAS を最新のソフトウェア リリースにアップグレードする手順の詳細は、『*Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.1(1)*』の「Upgrading to 4.1(1)」を参照してください。

Cisco NAC アプライアンスのハードウェア プラットフォーム

Cisco NAC アプライアンス 3300 シリーズは、CAM（MANAGER）または CAS（SERVER）アプリケーションとともにプリインストールされる Linux ベースのネットワーク ハードウェア アプライアンス、オペレーティング システム、および関連するすべてのコンポーネントを 1 台の専用サーバ マシンに提供します。オペレーティング システムは、Fedora Core をベースにした Hardened Linux カーネルで構成されています。Cisco NAC アプライアンスは、その他のパッケージまたはアプリケーションの CAM または CAS 専用マシンへのインストールはサポートしていません。

（注）　Cisco NAC アプライアンス 3300 シリーズのハードウェア プラットフォームをリリース 4.1(1) 以降にアップグレードできます。ただし、リリース 4.1(0) は利用できず、NAC 3300 シリーズのプラットフォームにインストールできません。詳細は、該当する『*Release Notes*』を参照してください。

（注）　Cisco NAC アプライアンス 3300 シリーズには、Cisco Clean Access 3140（CCA-3140-H1）NAC アプライアンスが含まれます（近々 EOL になる予定）。CCA-3140-H1 は CAS または CAM ソフトウェアのいずれかの CD インストールが必要です。

Cisco NAC アプライアンス 3300 シリーズ アプライアンスの詳細は、『*Cisco NAC Appliance Hardware Installation Quick Start Guide*』Release 4.1(1) を参照してください。

サポートされているサーバ ハードウェア プラットフォーム

Cisco NAC アプライアンス ソフトウェアをインストールする独自のサーバ ハードウェアを用意する場合、『*Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)*』に説明されているサポート対象プラットフォームにインストール可能なソフトウェアとして CAM を利用できます。

最小システム要件

CAM および CAS ソフトウェアおよび CAA クライアント ソフトウェアの最小システム要件の詳細は、『*Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)*』マニュアルの「System Requirements」を参照してください。

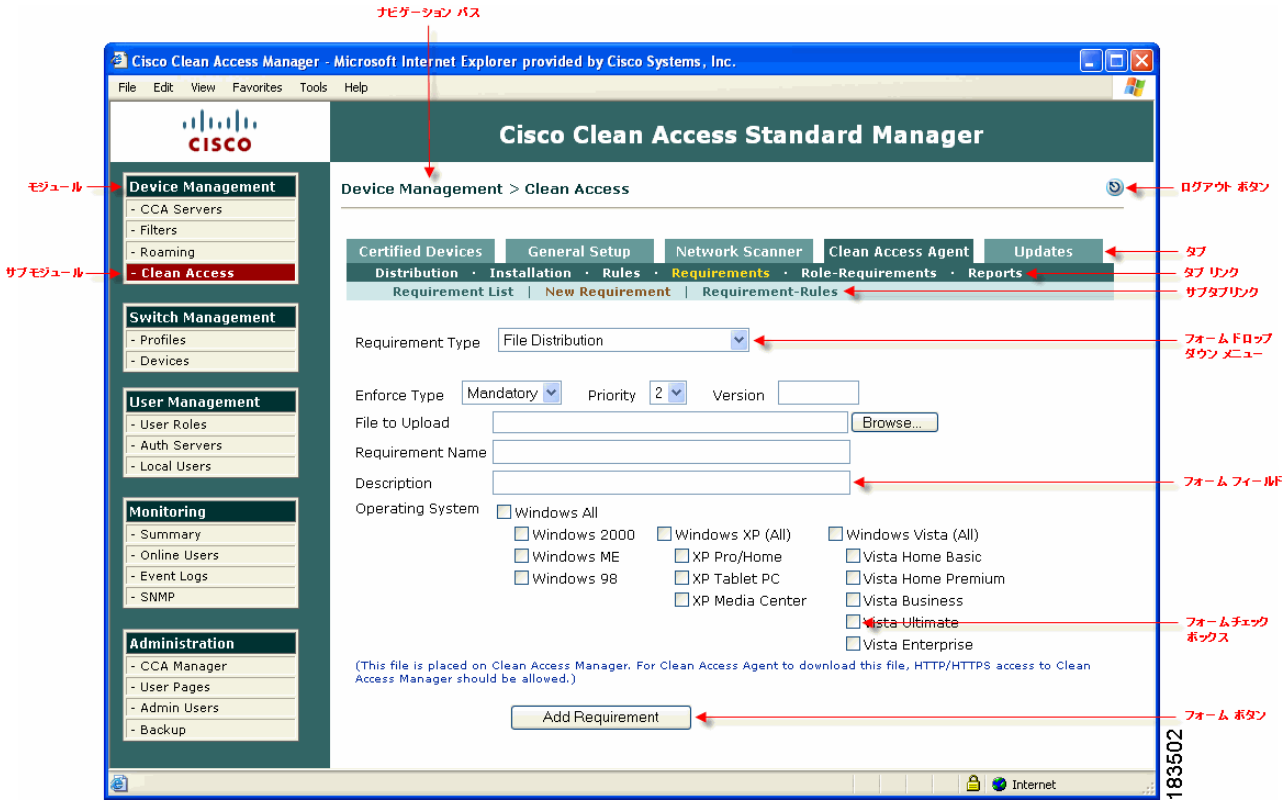
重要なリリース情報

4.1(1) ソフトウェア リリースの追加情報および最新情報は、『*Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.1(1)*』を参照してください。

Web 管理コンソールの要素

ライセンスによって Cisco NAC アプライアンス ソフトウェアが使用可能になると、CAM の Web 管理コンソールを通じて、Cisco NAC アプライアンスを簡単に管理できるようになります。Web コンソールの左側のパネルには、主なモジュールとサブモジュールが表示されます。Web コンソール上部のナビゲーション パスを見れば、今、このインターフェイス内のどのモジュールおよびサブモジュールが表示されているのかがわかります。サブモジュールをクリックすると、そのインターフェイスのタブが開くか、あるいは直接、設定のページまたはフォームが表示されます。設定ページではアクションを実行し、設定フォームではフィールドに情報を入力します。Web 管理コンソールのページは、次の要素で構成されています（図 1-4 を参照）。

図 1-4　Web 管理コンソールのページの要素



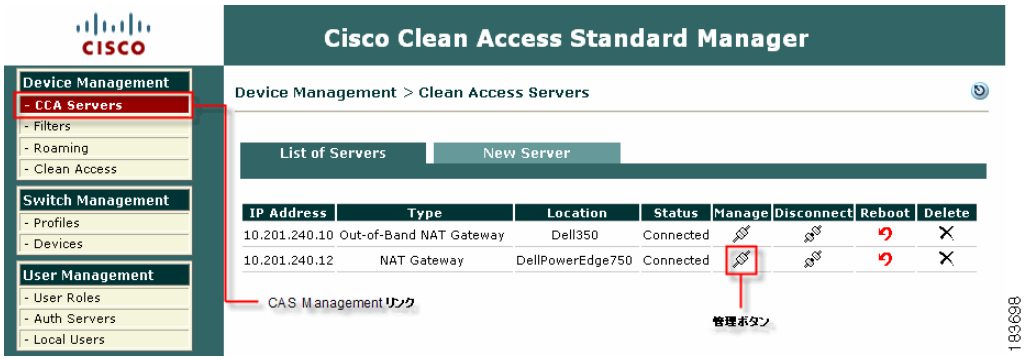
（注）　このマニュアルでは、管理コンソールのナビゲーション リンクに次の表記方法を使用します。**Module > Submodule > Tab > Tab Link > Subtab link**（該当する場合）

CAS 管理ページ

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 Server 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、第 3 章「デバイス管理：CAS の追加、フィルタの追加」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、図 1-6 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 1-5　CAS List of Servers ページ

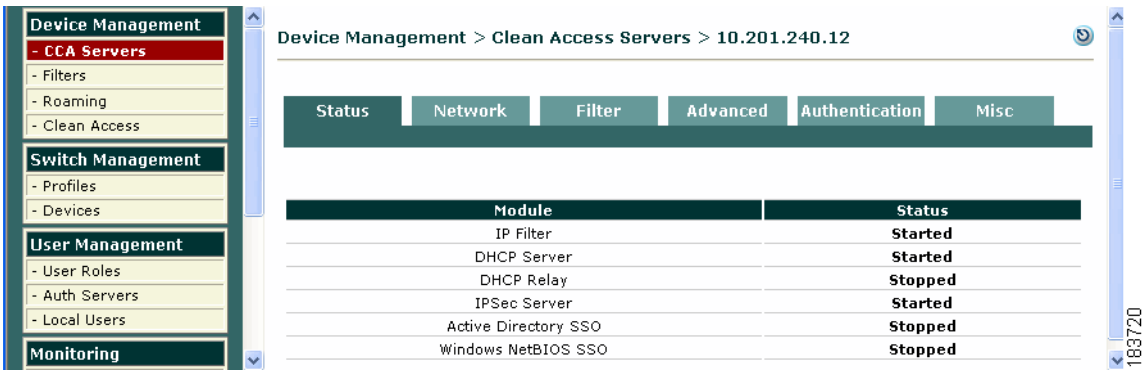


2. アクセスしたい CAS の IP アドレスの **Manage** ボタンをクリックします。

（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 アドレスはカッコ内に表示されます。

3. CAS 用の CAS 管理ページは、図 1-6 のように表示されます。

図 1-6　CAS 管理ページ



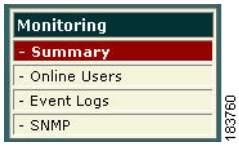
管理コンソールの概要

表 1-1 に、Web 管理コンソールの各モジュールの主な機能をまとめて示します。

表 1-1　Clean Access Manager Web 管理コンソールのモジュールの概要

モジュール	モジュールの説明
	**Device Management** モジュールでは、次のことができます。 • CAS 管理ページ（図 1-6 を参照）での CAS の追加、設定、管理、ソフトウェア アップグレード。第 3 章「デバイス管理：CAS の追加、フィルタの追加」を参照してください。AD SSO、DHCP、Cisco VPN コンセントレータの統合、CAS ハイ アベイラビリティ（フェールオーバー）など、ローカル CAS の設定については、『*Cisco NAC Appliance - Clean Access Server Installation and Administration Guide*』Release 4.1(1) を参照してください。アップグレード情報については、『*Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.1(1)*』の「Upgrading to a New Software Release」セクションを参照してください。 • 非信頼側にあるデバイスが認証とポスチャ評価（このマニュアルでは「Clean Access 証明」と呼んでいます）を回避できるようにデバイスまたはサブネットのフィルタを設定します。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。 • ユーザ ロールおよび OS 単位の Clean Access（Network Scanning/CAA）の脆弱性評価の設定。次の章を参照してください。 — 第 9 章「Clean Access の設定概要」 — 第 12 章「ネットワーク スキャンの設定」 — 第 11 章「CAA 要件の設定」 **（注）** ユーザ セッションは、MAC アドレス（該当する場合）または IP アドレスと、ユーザが指定したユーザ ロールで管理されます。ユーザ ロールは、**User Management** モジュールで設定します。
	Cisco NAC アプライアンスの OOB 配置には、**Switch Management** モジュールを使用します。このモジュールでは次のことができます。 • アウトオブバンドのグループ、スイッチ、ポートのプロファイルの設定および Clean Access Manager の SNMP レシーバーの設定 • サポート対象のアウトオブバンド スイッチの追加、送信する SNMP トラップの設定、**Ports**（**Port Profile**）ページを通じた個々のスイッチ ポートの管理、検出されたクライアントのリストの監視 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。

表 1-1　Clean Access Manager Web 管理コンソールのモジュールの概要（続き）

モジュール	モジュールの説明
	**User Management** モジュールでは、次のことができます。 • 正常ログイン ユーザのロールの設定。ユーザ グループを認証パラメータ、トラフィック制御ポリシー、セッション タイムアウト、帯域幅制限に関連付けることができます。OOB ポート プロファイルにロールベースの設定を使用している場合は、ユーザ ロールを使用してアクセス VLAN を設定できます。 • IP およびホストベースのトラフィック制御ポリシーを追加して、すべてのユーザ ロールのネットワーク アクセスを設定します。CAA Temporary ロールのトラフィック ポリシー / セッション タイムアウトと Quarantine ロールの設定。クライアント デバイスが条件を満たしていない場合またはネットワーク スキャンで脆弱性が発見された場合、そのデバイスのネットワーク アクセスを制限できます。 • CAM への認証サーバの追加（ネットワーク上の外部認証ソースの設定） • CAS に AD SSO または Cisco VPN コンセントレータ統合が設定されている場合、Active Directory SSO や Cisco VPN SSO などの認証ソースを追加して SSO をイネーブルにします。 • 複雑なマッピング ルールの作成。LDAP もしくは RADIUS の属性、または VLSN ID に基づいてユーザをユーザ ロールに対応付けることができます。 • RADIUS アカウンティングの実行 • CAM によって内部認証されたローカル ユーザの作成（試用） 詳細は、次の章を参照してください。 — 第 6 章「ユーザ管理：ユーザ ロールとローカル ユーザの設定」 — 第 7 章「ユーザ管理：認証サーバの設定」 — 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」 Cisco VPN コンセントレータ統合に関する詳細は、『*Cisco NAC Appliance - Clean Access Server Installation and Administration Guide*』Release 4.1(1) を参照してください。
	**Monitoring** モジュールでは、次のことができます。 • ご使用の Cisco Clean Access（NAC アプライアンス）のステータス概要の表示 • インバンドおよびアウトオブバンドのオンライン ユーザの管理 • CAM イベント ログの表示、検索、リダイレクト • CAM 用の基本的な SNMP ポーリングおよび警告の設定 第 13 章「モニタリング」を参照してください。
	**Administration** モジュールでは、次のことができます。 • CAM ネットワークおよびハイアベイラビリティの設定 第 15 章「ハイ アベイラビリティ（HA）の設定」を参照してください。 • CAM SSL 証明書、システム時間、CAM/CAS プロダクト ライセンスの設定、CAM データベース バックアップ スナップショットの作成と復元、テクニカル サポート ログのダウンロード 第 14 章「管理」を参照してください。 • CAM でのソフトウェア アップグレードの実行 『*Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.1(1)*』の「Upgrading to a New Software Release」セクションを参照してください。 • デフォルト ログイン ページ（すべてのユーザ認証に必須）の追加、および Web ログイン ユーザ用の Web ログイン ページのカスタマイズ 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。 • 複数の管理者グループおよびアクセス権限の設定 「管理ユーザ」（p.14-25）を参照してください。