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。この章の内容は次のとおりです。

Cisco 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配置オプション、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た Cisco NAC アプライアンスは、ネットワークを制御して保護するための完全な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導入できるため、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、Clean Access ポスチャ評価、修復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ユーザ デバイスは、Clean Access で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）管理サーバの Web コンソールから管理し、Clean Access Server（CAS）および Clean Access Agent/Cisco NAC Web 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。または、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」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、主に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）を使用します。
- 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します。
- 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、シングルサインオン（SSO）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 （Cisco NAC Web Agent では SSO はサポートされません）。
- 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 スキャンを使用することで、クライアントのポスチャ評価および修復の設定が可能です。Cisco NAC Web Agent によって、ポスチャ評価が実行されますが、修復のための手段は提供されません。ユーザは、クライアント マシンを手動で訂正または更新して、Web Agent のポスチャ評価要件を満たすために「再スキャン」する必要があります。
- L2 または L3 配置のオプション：Clean Access Server は、ユーザの L2 近接内に配置することも、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）配置オプション：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インラインで配置することも、アウトオブバンドで配置して、クライアントがポスチャ評価および修復の処理中にだけ Clean Access ネットワークを経由し、認証（ポスチャ評価）後に回避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。Clean Access Manager（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。

（注） Cisco サービス統合型ルータ（ISR）にインストールされている 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 コンポーネント

Cisco NAC アプライアンスは、Clean Access Manager Web コンソールから管理し、Clean Access Server およびオプションの Clean Access Agent または Cisco NAC Web 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 を配置するための管理サーバ。Clean Access Manager のセキュアな Web コンソールを通じ、1 ヶ所で配置内の最大 20 の Clean Access Server 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 管理コンソールでは、Internet Explorer 6.0 以上だけがサポートされ、高度暗号化（64 ビットまたは 128 ビット）が必要です。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 Clean Access Agent/Cisco NAC Web Agent 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。

  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）または Cisco ISR シャーシ内のネットワーク モジュール（Cisco NME-NAC-K9）のいずれかとしてインストールして、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/ポスチャ評価中にだけユーザ トラフィックを処理する）で配置できます。CAS は、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。

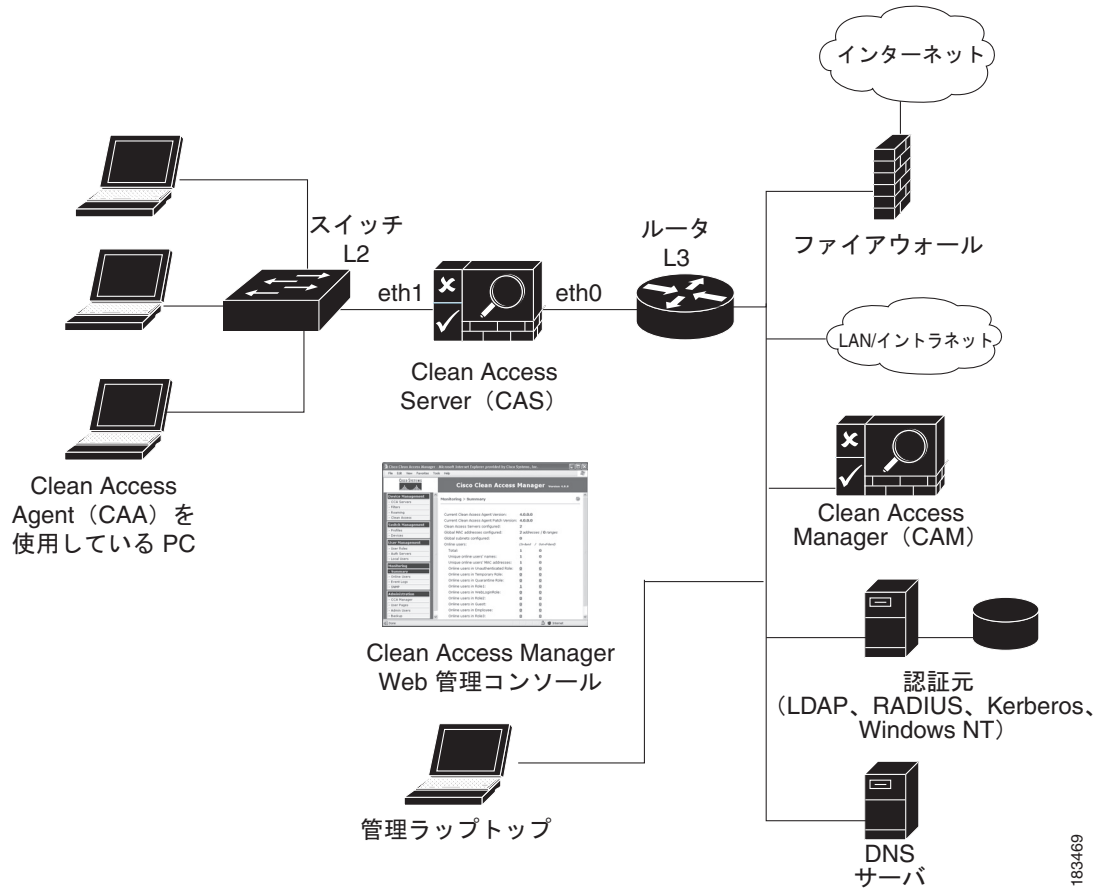
  異なるネットワーク セグメントのニーズを満たすために、さまざまなサイズ/容量の CAS をいくつか配置することもできます。たとえば、数千ものユーザを処理して 1 つ以上の Cisco NAC ネットワーク モジュールを ISR プラットフォームに同時にインストールして、サテライト オフィスにいる小さいユーザ グループに対応するために、Cisco NAC-3300 シリーズ アプライアンスを本社のコアにインストールできます。

- **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。Clean Access 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ことを確認します。

（注） Clean Access Agent のポスチャ評価には、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 Web Agent**：Cisco NAC Web Agent には、クライアント マシン用の時間のポスチャ評価が用意されています。ユーザは、Cisco NAC Web Agent の実行可能ファイルを起動します。このファイルは、ActiveX コントロールまたは Java アプレットを使用してクライアント マシンの一時ディレクトリに Web Agent ファイルをインストールします。ユーザが Web Agent セッションを終了すると、Web Agent はネットワークからユーザをログオフし、ユーザ ID は Online Users リストに表示されなくなります。
- **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、オペレーティング システム、アンチウイルス（AV）、アンチスパイウェア（AS）、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。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。

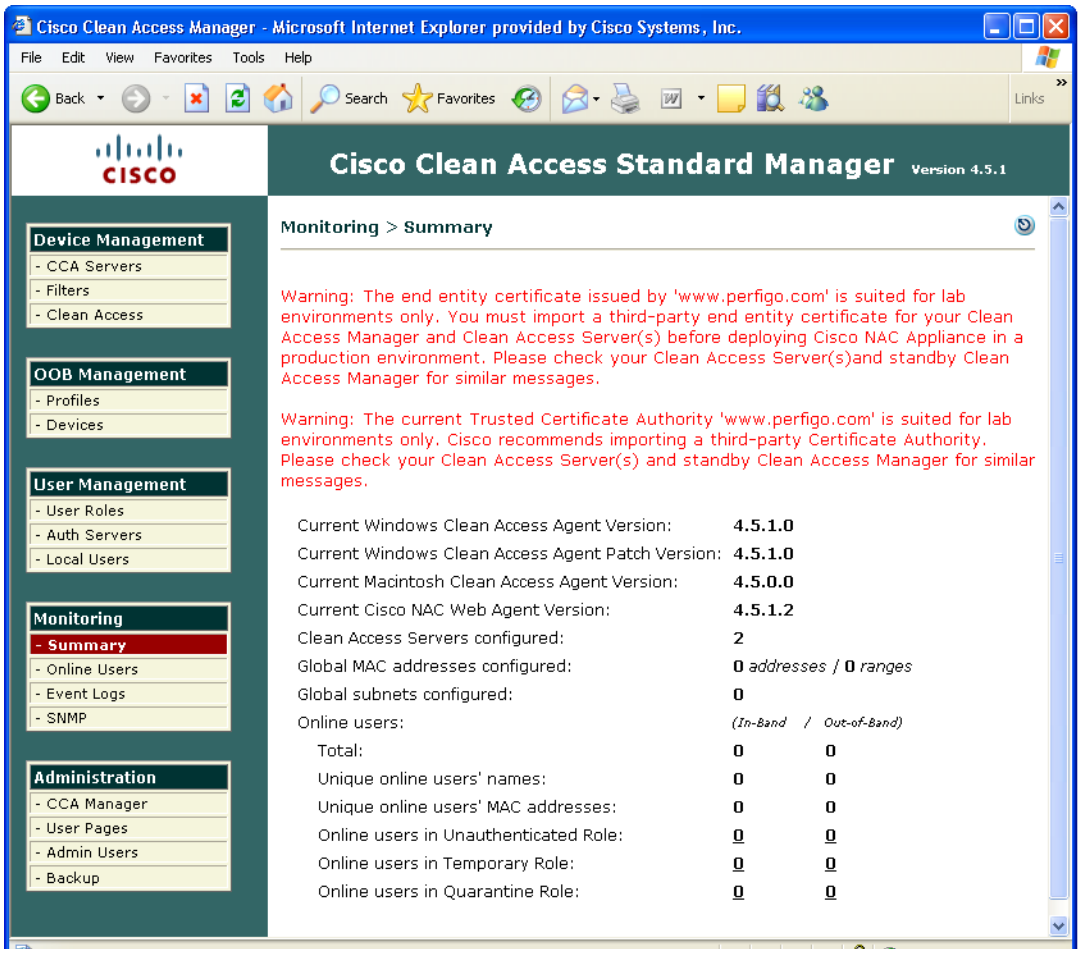
図 1-1　Cisco NAC アプライアンスの配置（L2 インバンド例）



Clean Access Manager（CAM）

Clean Access Manager（CAM）は、導入された Cisco NAC アプライアンスのすべての Clean Access Server、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 Clean Access Server を管理できます。Clean Access Manager 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、「管理コンソールの要約」（P.1-13）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、[OOB Management] モジュールとなり、Clean Access Manager 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



Clean Access Server（CAS）

Clean Access Server（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。Clean Access Server 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（IB と OOB）は、実動環境ではサポートされていません。

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

CAS 動作モードの要約については、「管理ドメインへの Clean Access Server の追加」（P.3-2）を参照してください。CAS 構成の詳細については、『*Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide Release 4.5(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実装、またはローカル トラフィック ポリシーなど、CAS でローカルに設定されたオプションの詳細については、『*Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide Release 4.5(1)*』を参照してください。

Clean Access Agent

Cisco NAC アプライアンスを配置すると、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ことを Clean Access Agent で確認できます。Clean Access Agent 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。Clean Access Agent 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。

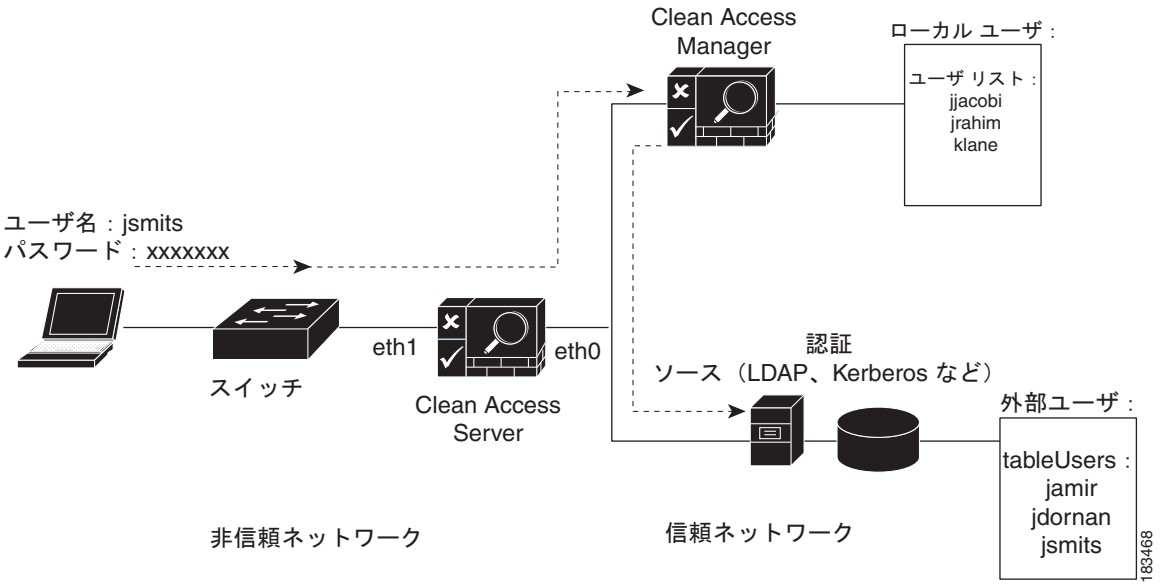
設定されたシステム検査に合格しない Agent ユーザは、Clean Access Agent Temporary ロールに割り当てられます。このロールのユーザには、限定的なアクセス権が付与され、Clean Access の条件を満たすために必要なリソースだけにネットワーク アクセスが制限されます。クライアント システムが要件を満たせば、「クリーン」であると見なされ、ネットワーク アクセスが許可されます。

ユーザの管理

Clean Access Manager 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化して、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 ポスチャ評価、および Cisco Clean Access 内のその他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。

Clean Access Server 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 または Cisco NAC Web Agent を配布する場合、ユーザは最初に Web にログインした後で、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 Agent を使用します。

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 Clean Access Agent やネットワーク ポート スキャンの条件を設定すると、Clean Access のポスチャ評価と修復を設定して、認証済みユーザに適用できます。

（注）　Cisco NAC Web Agent によって、ポスチャ評価が実行されますが、修復のための手段は提供されません。ユーザは、クライアント マシンを手動で訂正または更新して、Web Agent のポスチャ評価要件を満たすために「再スキャン」する必要があります。

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」と証明された後に、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」と証明された後に、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 トラフィック制御は、バーチャル ゲートウェイ モードで動作する Clean Access Server にだけ適用されます。

さらに、Online Users ページ（L2 および L3 配置の場合）や Certified Devices List（L2 配置の場合だけ）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
- ソフトウェアのアップグレード
- Cisco NAC アプライアンスのハードウェア プラットフォーム

- 重要なリリース情報

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サポートの取得手順に関する詳細については、『*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** では、3 つの Clean Access Server がサポートされます。
- **Cisco Clean Access Standard Manager** では、20 の Clean Access Server がサポートされます。
- **Cisco Clean Access Super Manager** では、40 の Clean Access Server がサポートされます（SuperCAM は NAC-3390 プラットフォームでだけ実行されます）。

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。詳細については、「ライセンス」（P.16-26）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については、『*Release Notes for Cisco NAC Appliance Version 4.5(1)*』の「Upgrading to 4.5」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 リリース 4.5 から、Cisco NAC アプライアンス ソフトウェアでは、次の Cisco NAC アプライアンス プラットフォームだけがサポートされ、これらのプラットフォームにだけインストール可能です。

- Cisco CCA-3140
- Cisco NAC-3310
- Cisco NAC-3350
- Cisco NAC-3390
- Cisco NAC ネットワーク モジュール（NME-NAC-K9）

（注）　リリース 4.5 におけるハードウェア互換性の詳細については、『*Release Notes for Cisco NAC Appliance Version 4.5(1)*』を参照してください。

Cisco NAC アプライアンス 3300 シリーズは、CAM（MANAGER）または CAS（SERVER）のいずれかの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。

Cisco NAC ネットワーク モジュールは、Cisco 2800 および 3800 シリーズ ISR シャーシにインストールできる CAS です。Cisco NAC ネットワーク モジュールではハイ アベイラビリティがサポートされないという 1 つの例外を除き、スタンドアロン CAS アプライアンスと同じ機能をすべて備えています。

（注）　Cisco NAC ネットワーク モジュールの詳細については、『*Getting Started with NAC Network Modules in Cisco Access Routers*』と『*Installing Cisco Network Modules in Cisco Access Routers*』を参照してください。

Cisco NAC アプライアンスのオペレーティング 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 3100 シリーズには、Cisco Clean Access 3140（CCA-3140-H1）NAC アプライアンス（EOL）が含まれます。CCA-3140-H1 では Clean Access Server または Clean Access Manager 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については、『*Cisco NAC Appliance Hardware Installation Quick Start Guide Release 4.5*』を参照してください。

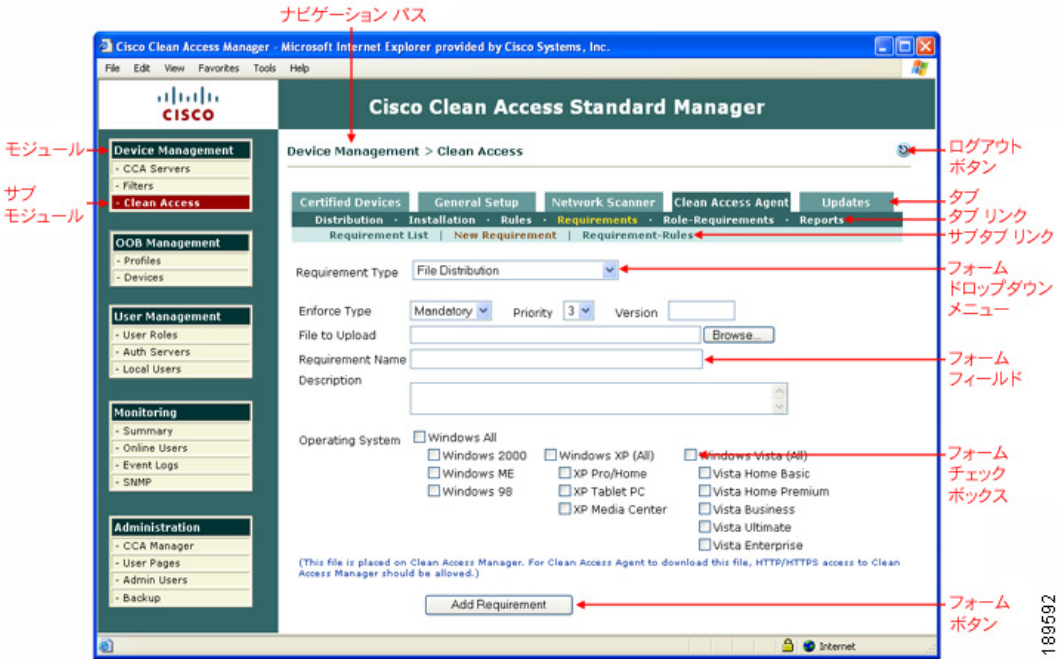
重要なリリース情報

4.5 ソフトウェア リリースの追加情報および最新情報については、『*Release Notes for Cisco NAC Appliance Version 4.5(1)*』を参照してください。

Web 管理コンソールの要素の概要

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 管理コンソールで、Cisco NAC アプライアンスを管理するための簡単に使用できるインターフェイスが提供されます。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でき、設定フォームではフィールドに情報を入力できます。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（P.1-10 の図 1-4 を参照）。

図 1-4　Web 管理コンソールのページの要素



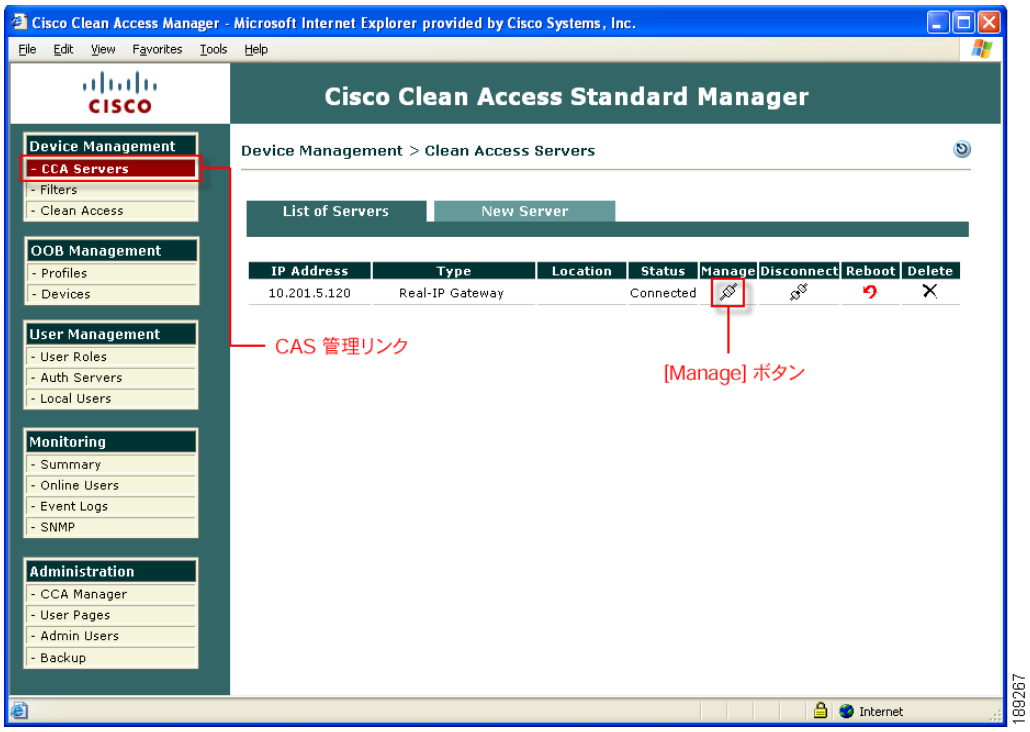
（注）　このマニュアルでは、管理コンソールのナビゲーション リンクに次の表記方法を使用します。[< *モジュール*>] > [< *サブモジュール*>] > [< *タブ*>] > [< *タブ リンク*>] > [< *サブタブ リンク*>]（該当する場合）

Clean Access Server（CAS）管理ページ

Clean Access Server を Web 管理コンソールから管理できるようにするには、その Server を Clean Access Manager ドメインに追加する必要があります。第 3 章「デバイス管理 : Clean Access Server の追加、フィルタの追加」に、手順が説明されています。ドメインに追加した Clean Access Server に管理コンソールからアクセスするには、次の手順を使用します。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

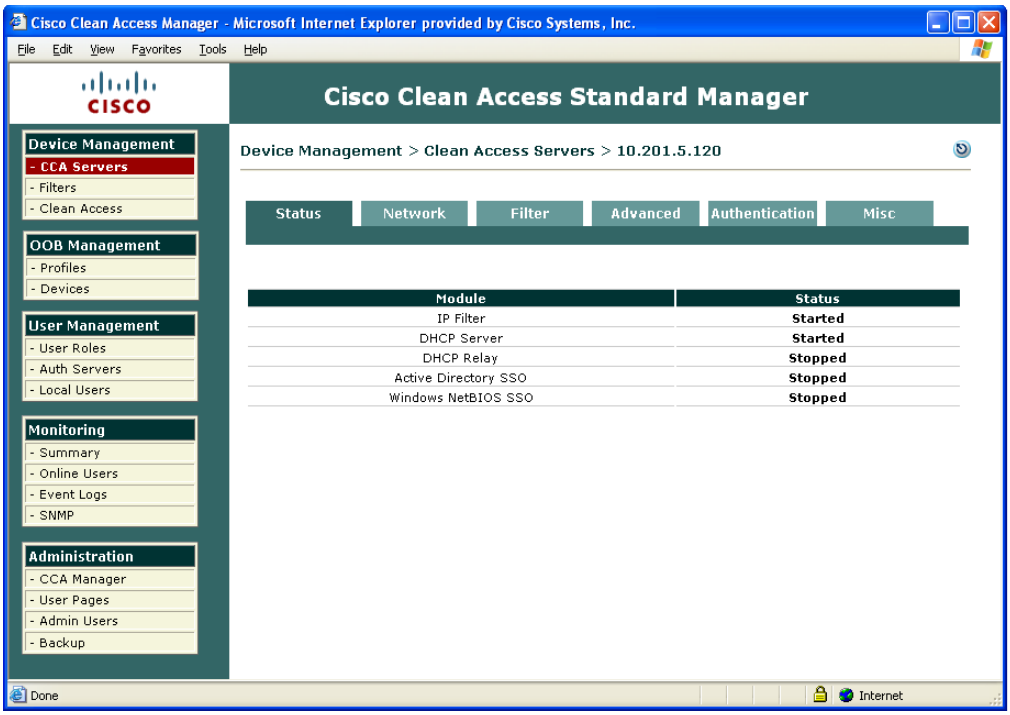


2. アクセスする Clean Access Server の IP アドレスの [Manage] ボタンをクリックします。

（注）　ハイ アベイラビリティ構成の Clean Access Server 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. Clean Access Server 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



管理コンソールの要約

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要約

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）を使用した Clean Access Server でのソフトウェア アップグレードを追加、設定、管理、実行します。 第 3 章「デバイス管理：Clean Access Server 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 Configuration Guide Release 4.5(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 Version 4.5(1)*』の「Upgrading to a New Software Release」の項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。詳細については、「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.3-10）を参照してください。 • ユーザ ロールおよび OS 単位で Clean Access（ネットワーク スキャン/Clean Access Agent/Cisco NAC Web Agent）のポスチャ評価や修復を設定します。次の章を参照してください。 – 第 10 章「Clean Access の設定概要」 – 第 14 章「ネットワーク スキャンの設定」 – 第 12 章「エージェント要件の設定」 **（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 アプライアンスのアウトオブバンド配置には、[OOB 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、WLC、ポートのプロファイル、および Clean Access Manager の SNMP Receiver 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要約 （続き）

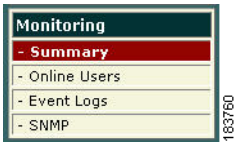
モジュール	モジュールの説明
	[User Management] モジュールでは、次のことができます。 • 正常ログイン ユーザのロールを作成します。ユーザ グループを認証パラメータ、トラフィック制御ポリシー、セッション タイムアウト、帯域幅制限に関連付けることができます。OOB ポート プロファイルにロールベースの設定を使用している場合は、ユーザ ロールを使用してアクセス VLAN を設定できます。 • IP およびホストベースのトラフィック制御ポリシーを追加して、すべてのユーザ ロールのネットワーク アクセスを設定します。Clean Access Agent/Cisco NAC Web Agent Temporary ロールと Quarantine 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 に認証サーバを追加します（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 VLAN 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 アカウンティングを実行します。 • CAM によって内部認証されたローカル ユーザを作成します（試用）。 詳細については、次の項目を参照してください。 – 第 7 章「ユーザ管理：ユーザ ロールとローカル ユーザの設定」 – 第 8 章「ユーザ管理：認証サーバの設定」 – 第 9 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 コンセントレータの統合に関する詳細については、『*Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide Release 4.5(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。 • 配置のステータス要約の表示 • 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 • Clean Access Manager イベント ログの表示、検索、リダイレクト • Clean Access Manager 用の基本的な SNMP ポーリングおよび警告の設定 第 15 章「オンライン ユーザとイベント ログのモニタリング」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要約 （続き）

モジュール	モジュールの説明
	[Administration] モジュールでは、次のことができます。 • Clean Access Manager ネットワークおよびハイアベイラビリティ（フェールオーバー）の設定。 第 17 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 16 章「CAM の管理」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 Version 4.5(1)*』の「Upgrading to a New Software Release」の項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 6 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.16-46）を参照してください。