CHAPTER 1

はじめに

この章では、Clean Access Server の概要を説明します。この章の内容は、次のとおりです。

NAC アプライアンス（Cisco Clean Access）とは

Cisco Network Admission Control（NAC）アプライアンス（Cisco Clean Access と呼ぶこともあります）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、完全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、Clean Access 脆弱性評価、修復（ポスチャ評価）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 Clean Access 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。
- Clean Access 準拠性ポリシー — Clean Access Agent（CAA）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 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（ポスチャ評価）後 Clean Access ネットワークを迂回し、脆弱性評価と修復時にのみ Clean Access 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 サーバまたはその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。

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、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 Clean Access Agent（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）** — Clean Access 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 Clean Access Server（CAS）を管理できます（Super CAM の場合は最大 40 の CAS）。アウトオブバンドの場合は、Web 管理コンソールでスイッチの制御や SNMP によるユーザ ポートの VLAN 割り当てを実行できます。

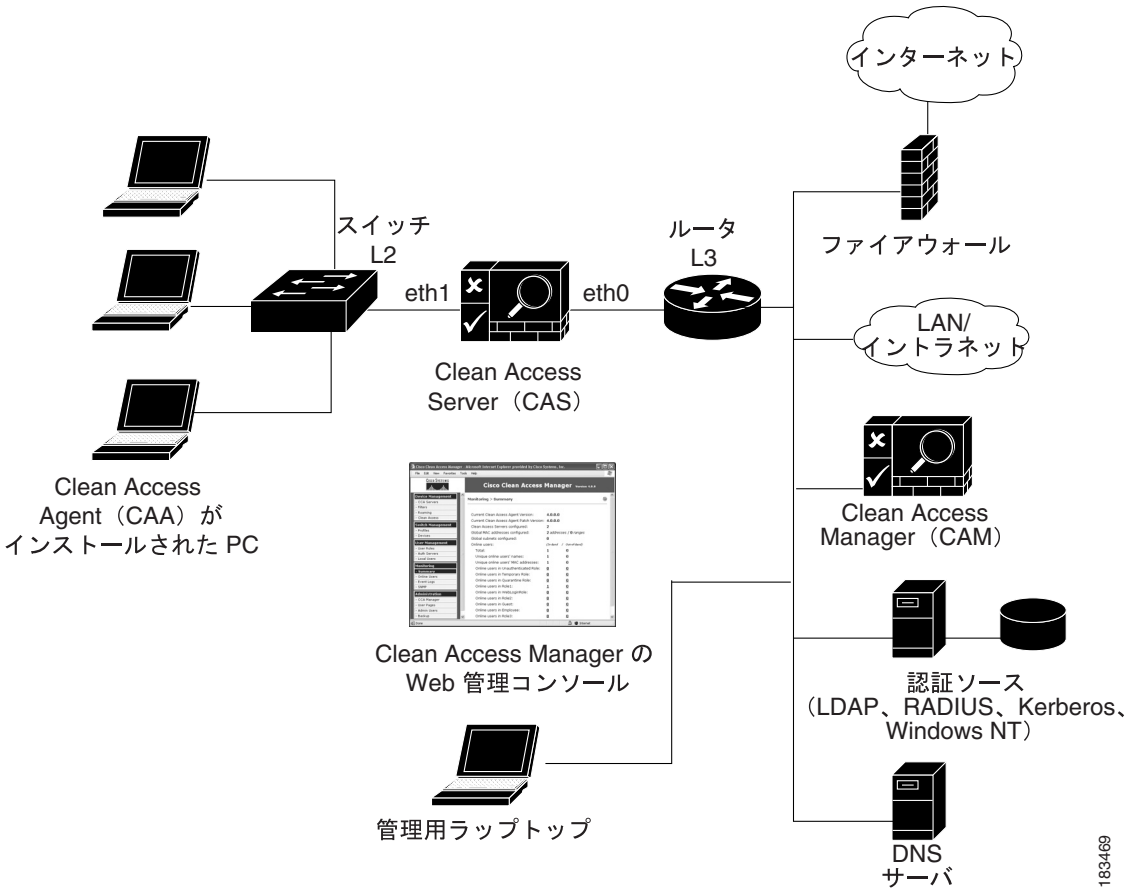
（注） CAM Web 管理コンソールには、Internet Explorer 6.0 以上、および高度暗号化（64 ビットまたは 128 ビット）を必要とします。高度暗号化はクライアント ブラウザの Web ログインおよび CAA の認証にも必要です。

- **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、Clean Access 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、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のみユーザ 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 近接）、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。
- **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 アプライアンスの導入（L2 インバンドの例）



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
- Clean Access 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。

インストール要件

ここでは、次の内容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）　Cisco NAC アプライアンスの製品ライセンスの取得とインストールおよびサービス契約サポートの取得方法についての詳細は、『*Cisco NAC Appliance Service Contract / Licensing Support*』を参照してください。

ソフトウェアのアップグレード

ご使用の CAM または 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方法については、『*Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.1(x)*』の「Upgrading to 4.1(x)」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）のいずれかのアプリケーション、オペレーティング システム、およびすべての関連コンポーネントが専用サーバ マシンにあらかじめインストールされた Linux ベースのネットワーク ハードウェア アプライアンスです。オペレーティング システムには、Fedora Core に基づく強化 Linux カーネルが組み込まれています。Cisco NAC アプライアンスは、CAM または CAS 専用マシンにほかのパッケージやアプリケーションをインストールすることを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 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、4.1(0) リリースは NAC 3300 シリーズ プラットフォームにインストールして使用することはできません。詳細は、該当する リリース ノートを参照してください。

（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（近い将来 EOL になります）が含まれています。CCA-3140-H1 には、Clean Access Server または Clean Access Manager のソフトウェアを CD からインストールする必要があります。

Cisco NAC アプライアンス 3300 シリーズおよび 3100 シリーズ ハードウェア アプライアンスに関する詳細は、『*Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)*』および『*Cisco NAC Appliance Hardware Installation Quick Start Guide, Release 4.1(1)*』を参照してください。

サポート対象のハードウェア プラットフォーム

お手持ちのサーバ ハードウェアに Cisco NAC アプライアンス ソフトウェアをインストールする場合は、Clean Access Manager をサポート対象のプラットフォームにインストールして使用します。サポート対象のプラットフォームについては、『*Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)*』を参照してください。

最小システム要件

Clean Access Manager ソフトウェアと Clean Access Server ソフトウェアおよび Clean Access Agent クライアント ソフトウェアを実行するための最小システム要件に関する詳細は、『*Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)*』の「System Requirements」を参照してください。

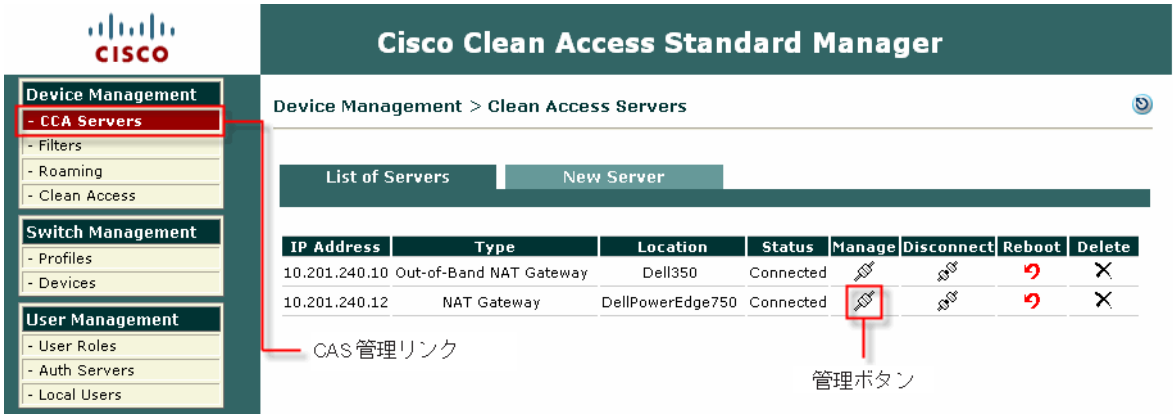
重要なリリース情報

4.1(x) ソフトウェア リリースに関するその他の情報および最新の情報については、『*Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.1(x)*』を参照してください。

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.5-2）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。

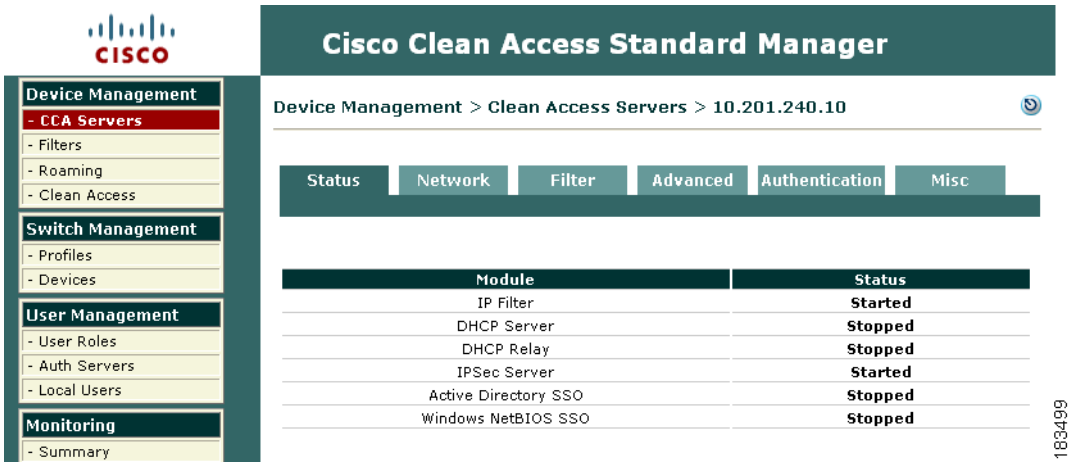


2. アクセスする CAS の **Manage** ボタンをクリックします。

（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 1-2 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 1-2　CAS 管理ページ



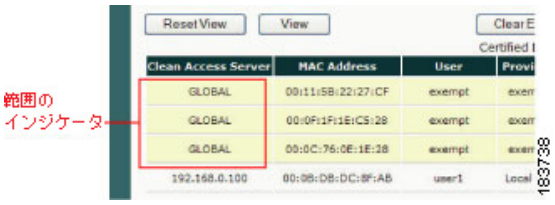
グローバルおよびローカルの管理設定値

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。これらには、認証サーバ情報、グローバル デバイス / サブネット フィルタ ポリシー、ユーザ ロール、Cisco Clean Access コンフィギュレーションなどがあります。
- **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。これらには、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 / 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 1-3 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 1-3　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、設定を作成する場合に使用されるグローバル フォームから追加、編集、および削除されます。ローカル設定は、設定を作成する場合に使用されるローカル フォームから追加、編集、および削除されます。

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、常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。

- デバイス / サブネット フィルタ ポリシー（認証要求の回避）に関しては、ローカル（CAS 固有）設定値がグローバル（CAM）設定値よりも優先されます。
- トラフィック制御ポリシーなど、その他の設定値の場合、グローバルとローカルのどちらのポリシーが強制されるかは、ポリシーのプライオリティ（高または低）によって決まります。
- 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。

- CAA の L3 サポート（マルチホップ L3 構成）
- 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

- Clean Access の要件およびネットワーク スキャン プラグインは、CAM からグローバルとして設定され、すべての CAS に適用されます。