CHAPTER 2

# Clean Access Manager のインストール

この章では、Clean Access Manager をインストールする方法について説明します。この章の内容は次のとおりです。



## 概要

Cisco NAC アプライアンス 3300 シリーズ ハードウェア プラットフォームは 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。これは専用のサーバ マシンに CAM（マネージャ）または CAS（サーバ）アプリケーションのどちらか、OS、および該当するすべてのコンポーネントとともに事前にインストールされています。OS 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 Clean Access Manager（CAM）または Clean Access Server（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。

新しい Cisco NAC アプライアンスを受け取ったら、アプライアンスに接続し、初期設定を行わなければなりません。

アプライアンスに同梱されているのとは違うバージョンのソフトウェアをインストールする場合は、最初に CD を使用してソフトウェア インストールを行います。Cisco NAC アプライアンス 3300 シリーズ プラットフォームでサポートされているソフトウェアのバージョンについては、『*Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)*』を参照してください。

**ヒント** 『*Cisco NAC Appliance Hardware Installation Quick Start Guide*』に新しい Cisco NAC Appliance アプライアンスの電源をオンにするために必要なすべての指示が記載してあります。

この章では、Clean Access Manager の CD ソフトウェア インストールと初期設定を行う方法について説明します。

CD を使用して Cisco NAC アプライアンス ソフトウェアをインストールするときは、Clean Access Manager または Clean Access Server アプリケーションのどちらをインストールするか選択しなければなりません。専用アプライアンス（アプリケーション、OS、該当するコンポーネント）に CAM または CAS をインストールしてしまうと、他のパッケージまたはアプリケーションの CAM または CAS へのインストールはサポートされません。

**注意**　Cisco NAC アプライアンス リリース 4.5 は、次の Cisco NAC アプライアンス プラットフォームだけをサポートし、次のプラットフォームにだけインストールできます。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）。リリース 4.5 は他のどのプラットフォームにもインストールできません。

**（注）**　固定 IP アドレスを CAM/CAS インターフェイス用に設定しなければなりません。DHCP モードは、これらのインターフェイスの設定用にはサポートされていません。

**（注）**

- NAC-3300 シリーズ アプライアンスのインストールの詳細については、『*Cisco NAC Appliance Hardware Installation Quick Start Guide*』を参照してください。
- Clean Access Server のインストールの詳細については、『*Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.5(1)*』を参照してください。
- Cisco NAC ネットワーク モジュール（ネットワーク モジュール上の CAS）のインストールの詳細については、『*Getting Started with Cisco NAC Network Modules in Cisco Access Routers*』を参照してください。

# 新しいインストールの手順要約

**（注）**　必要な場合は、「Web コンソールからの手動バックアップ」（P.16-58）の説明にしたがって、ローカル コンピュータに現在の Clean Access Manager 設定をバックアップし、スナップショットを保存してください。

**ステップ 1**　ウェルカム レターの指示に従って、ご自分のインストールに有効なライセンス ファイルを取得してください。詳細については、『*Cisco NAC Appliance Service Contract/Licensing Support*』を参照してください（Cisco Clean Access を評価している場合は、http://www.cisco.com/go/license/public を参照して評価ライセンスを入手してください）。

**ステップ 2**　最新バージョンのソフトウェアのブート可能 CD を入手します。Cisco Secure Software にログインし、http://www.cisco.com/pcgi-bin/apps/tblbld/tablebuild.pl?topic=279515766 から最新の 4.5 .ISO image をダウンロードできます。または、こちらの Cisco NAC アプライアンス サポート ページ で「Download Software」リンクをクリックし、それをブート可能ディスクとして CD-R に焼き付けることもできます。

（注）　10x 以下の速度で .ISO イメージを CD-R に焼き付けることを推奨します。もっと高速で焼き付けると、インストール CD が破損またはブート不可能になる可能性があります。

**ステップ 3**　「Clean Access Manager の接続」（P.2-3）の説明にしたがって、CAM をネットワークに接続します。

**ステップ 4**　「Clean Access Manager の接続」（P.2-3）の説明にしたがって、モニタとキーボードを CAM に接続するか、またはシリアル ケーブルを使用してワークステーションを CAM に接続します。

**ステップ 5**　「CD-ROM からの Clean Access Manager ソフトウェアのインストール」（P.2-7）の説明にしたがって、ソフトウェアをインストールします。

（注）　NAC-3310 アプライアンスが CD ROM ドライブのソフトウェアを読み込まず、代わりにハードディスクから起動しようとする場合は、作業を進める前に、「NAC-3310 ベースのアプライアンスでのブート設定」（P.2-6）の説明にしたがって、アプライアンス設定を CD ROM から起動するよう変更する必要があります。

**ステップ 6**　「初期設定の実行」（P.2-9）の説明にしたがって、CAM の初期設定を行ってください。

（注）　High Availability（ハイ アベイラビリティ）モードでは、HA を設定する前に、まず各 CAM をインストールし、初期設定します。詳細については、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 または CAS の HA ペアを設定するために、同一のアプライアンス（たとえば、NAC-3350 と NAC-3350）を使用する必要があります。

**ステップ 7**　「CAM Web コンソールへのアクセス」（P.2-14）の説明にしたがって、CAM Web コンソールにアクセスし、Clean Access Manager 用の有効な FlexLM ライセンス ファイルをインストールします。

**ステップ 8**　「ライセンス」（P.16-26）の説明にしたがって、Web コンソールで [Administration] > [CCA Manager] > [Licensing] に移動し、Clean Access Server 用に追加の FlexLM ライセンス ファイルをインストールします。

**ステップ 9**　「管理ドメインへの Clean Access Server の追加」（P.3-2）の説明にしたがって、Clean Access Server を Clean Access Manager に追加します。

# Clean Access Manager の接続

Clean Access Manager ソフトウェアを CD-ROM からインストールし、初期設定を行うためには、ターゲット マシンを接続し、CAM のコマンドラインにアクセスする必要があります。

**ステップ 1**　Clean Access Manager では、eth0 ネットワーク インターフェイス用に 2 つの 10/100/1000BASE-TX インターフェイス コネクタのうちの 1 つが CAM の背面パネル上に必要です。ターゲット マシンの NIC1 ネットワーク インターフェイスを CAT5 イーサネット ケーブルを使用して LAN（ローカル エリア ネットワーク）に接続します。

必要な場合は、「Cisco NAC Appliance Hardware Summary」（『*Cisco NAC Appliance Hardware Installation Quick Start Guide*』）、または CAM に付属の資料を参照して、シリアル コネクタとイーサネット コネクタを見つけてください。

**ステップ 2**　AC 電源コードの一端をマシンの背面に差し込み、他端を電源コンセントに差し込んでください。

**ステップ 3**　マシンの前面にある電源ボタンを押して、CAM の電源をオンにします。LED 診断テストの実行中、診断 LED が数回点滅します。CAM が起動すると、コンソールにステータス メッセージが表示されます。

**ステップ 4**　CAM のコマンドには次のいずれかの方法でアクセスします。

- 背面パネルのキーボード コネクタとビデオ モニタ / コンソール コネクタを使用して、モニタとキーボードを CAM に直接に接続します。
- 「CAM へのシリアル接続」（P.2-4）の説明にしたがって、シリアル ケーブルで外部ワークステーション（PC またはラップトップ）を CAM に接続し、外部ワークステーションの端末エミュレーション ソフトウェア（HyperTerminal、SecureCRT など）を使用して、シリアル接続を開始します。

**（注）**　CAM の eth1 インターフェイス（NIC2）が必要なのは、HA CAM ペアを接続するときだけです。詳細については、「Configuring Additional NIC Cards」（『*Cisco NAC Appliance Hardware Installation Quick Start Guide*』）を参照してください。

**（注）**　固定 IP アドレスを CAM/CAS インターフェイス用に設定しなければなりません。DHCP モードは、これらのインターフェイスの設定用にはサポートされていません。

# CAM へのシリアル接続

ここでは、シリアル接続を使用して CAM コマンドラインにアクセスする方法について説明します。

**ステップ 1**　シリアル ケーブルを使用して、管理コンピュータのシリアル ポートを CAM の利用できるシリアル ポートに接続します。

**（注）**　CAM が HA（フェールオーバー）用に設定済みの場合、シリアル接続の 1 つはピア ハートビート接続に使用されている可能性があります。このような場合、シリアル接続を通じて CAM を管理するためには、少なくとも 2 つのシリアル ポートが必要です。シリアル ポートが 2 つない場合、ピア接続にイーサネット ポートを使用するという方法もあります。詳細については、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。

**ステップ 2**　ワークステーションを CAM に物理的に接続してから、端末エミュレーション ソフトウェアを使用して、シリアル接続インターフェイスにアクセスします。次の手順では、Microsoft の HyperTerminal を使用して接続を行います。他のソフトウェアを使用する場合は、手順が異なることがあります。

## HyperTerminal 接続の設定

**ステップ 3**　[ スタート ] > [ プログラム ] > [ アクセサリ ] > [ 通信 ] > [ ハイパーターミナル ] の順にクリックして、[ ハイパーターミナル ] ウィンドウを開きます。

**ステップ 4**　セッションの名前を入力し、[OK] をクリックします。


**ステップ 5**　[接続方法] リストで、シリアル ケーブルが接続されているワークステーションの COM ポート（通常は COM1 または COM2）を選択し、[OK] をクリックします。


**ステップ 6**　[ポートの設定] を次のように設定します。

- ビット/秒：9600
- データビット：8
- パリティ：None
- ストップビット：1
- フロー制御：None

**ステップ 7**　[ファイル] > [プロパティ] に進み、セッション用に [プロパティ] ダイアログを開き、[エミュレーション] 設定を [VT100] に変更します。

**ステップ 8**　これで、CAM のコマンド インターフェイスにアクセスできるようになります。次の作業に進んでください。

- 「CD-ROM からの Clean Access Manager ソフトウェアのインストール」（P.2-7）
- 「初期設定の実行」（P.2-9）

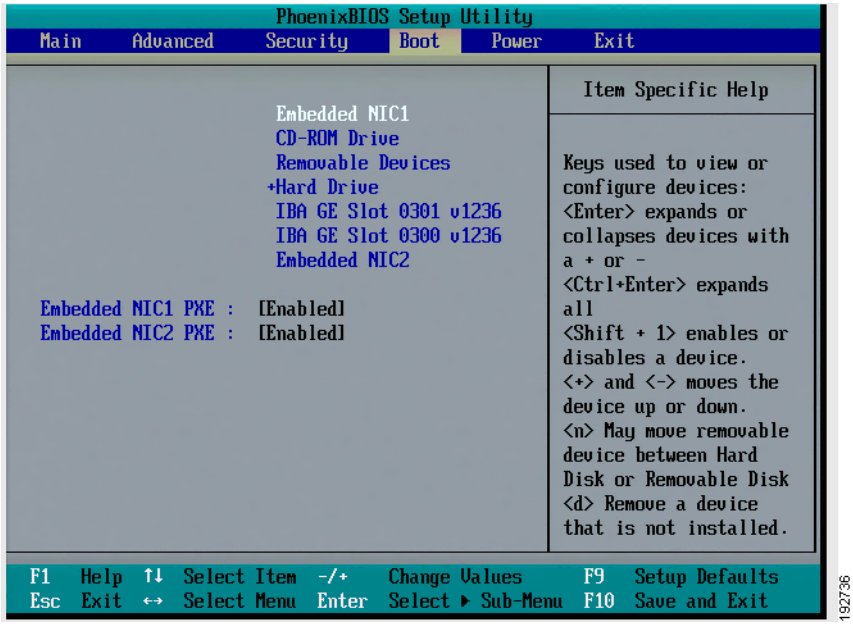
# NAC-3310 ベースのアプライアンスでのブート設定

NAC-3310 アプライアンスが CD ROM ドライブのソフトウェアを読み込まず、代わりにハードディスクから起動しようとする場合は、次の手順を行って、CD からアプライアンスのイメージを再作成したり、アプライアンスをアップグレードしたりしようとする前に、CD ROM から起動するようアプライアンスを設定します。

**ステップ 1**　システムの起動中に F10 キーを押します。

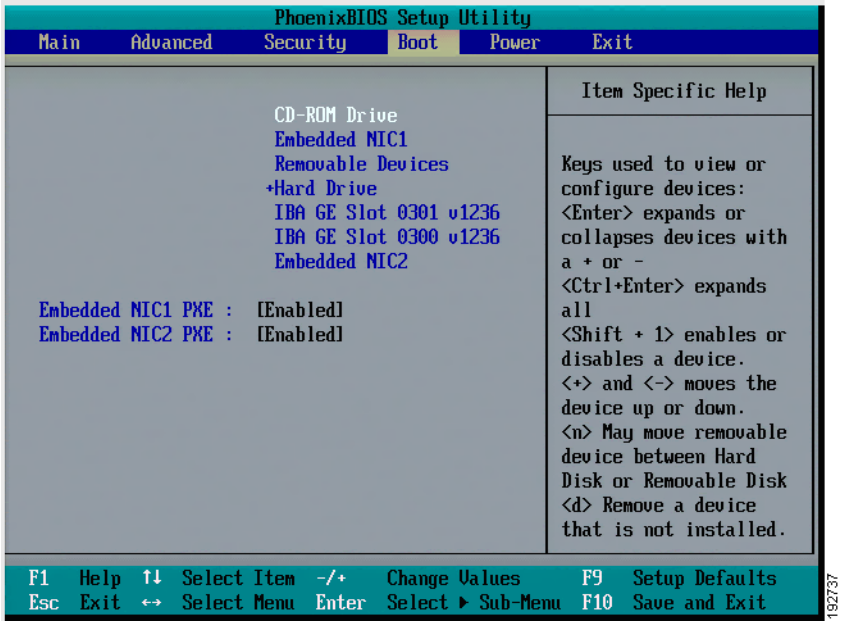
**ステップ 2**　[Boot] メニューに移動します（図 2-1）。

**図 2-1　[Boot] メニュー**




**ステップ 3**　CD ROM から起動するよう設定を変更するには、メニューで [CD-ROM Drive] を選択し、プラス（+）キーを押します（図 2-2）。

図 2-2　CD-ROM ドライブからの起動




**ステップ 4**　F10 キーを押し、Save and Exit します。

# CD-ROM からの Clean Access Manager ソフトウェアのインストール

CAM のコマンドラインに接続し（「Clean Access Manager の接続」（P.2-3）を参照）、次の手順を行って、CD-ROM から Clean Access Manager ソフトウェアをインストールします。

**注意**　Cisco NAC アプライアンス ソフトウェアは、ターゲット マシン上で他のソフトウェアまたはデータと共存することを想定した設計ではありません。インストール プロセスによってターゲット ハード ドライブはフォーマットおよび分割され、ドライブ上のデータまたはソフトウェアはすべて破棄されます。インストールを開始する前に、保持する必要があるデータやアプリケーションがターゲット マシンに格納されていないことを確認してください。

## CD からのインストール手順

「初期設定の実行」（P.2-9）に記載されている設定手順も含めて、インストール プロセス全体には約 15 分の時間がかかります。

**ステップ 1**　Clean Access Manager.ISO ファイルが入っている CD-ROM を、ご使用のターゲット マシン の CD-ROM ドライブに入れます。

**ステップ 2**　マシンを再起動します。マシンの再起動後、次のように、Cisco Clean Access Installer の初期画面が表示されます。

```
Cisco Clean Access 4.5-1 Installer (C) 2009 Cisco Systems, Inc.

                Welcome to the Cisco Clean Access 4.5-1 Installer!

 -  To install a Cisco Clean Access device, press the <ENTER> key.
 -  To install a Cisco Clean Access device over a serial console, enter serial at the boot
prompt and press the <ENTER> key.

boot:
```

**（注）** NAC-3310 アプライアンスが CD ROM ドライブのソフトウェアを読み込まず、代わりにハードディスクから起動しようとする場合は、作業を進める前に、「NAC-3310 ベースのアプライアンスでのブート設定」（P.2-6）の説明にしたがって、アプライアンス設定を CD ROM から起動するよう変更する必要があります。

**ステップ 3**　「boot」と表示されたら、接続の種類に従って、次のオプションの 1 つを入力します。

- モニタとキーボードがアプライアンスに直接接続されている場合は、Enter キーを押します。
- シリアル接続でアプライアンスにアクセスしている場合は、**serial** と入力して、端末エミュレーション コンソールで Enter キーを押します。

**ステップ 4**　Install 選択オプションが表示され、Cisco NAC アプライアンスの真新しいインストールを行うか、またはインストール プロセスを終了またはキャンセルするよう指示されます。次の指示メッセージに、**1** と入力して、新しいバージョンの Cisco NAC アプライアンスをインストールします。

```
Checking for existing installations.
Clean Access Manager 4.1.2.1 installation detected.
Please choose one of the following actions:
1) Install.
2) Exit.
```

**ステップ 5**　次に、Cisco NAC アプライアンス ソフトウェア インストーラは、Clean Access Manager をインストールしているか、Clean Access Server をインストールしているか問い合せます。次の指示メッセージに対し、**1** と入力し、Clean Access Manager のインストールを実行します。

```
Please choose one of the following configurations:
1) CCA Manager.
2) CCA Server.
```

**注意**　Clean Access Manager または Clean Access Server ソフトウェアのインストールには 1 つの CD しか使用されず、インストール スクリプトはターゲット マシン用に CAM または CAS インストールを自動的には検出しません。インストールを行うターゲット マシンについて、適切な種類、CAM または CAS の**どちらか**を選択する必要があります。

**ステップ 6**　Clean Access Manager Package Installation が実行されます。インストールには数分かかります。完了すると、インストール スクリプトが次のメッセージを表示し、Enter を押して CAM を再起動し、Clean Access Manager クイック コンフィギュレーション ユーティリティを開始するよう指示してきます。

```
Installation complete. Press <ENTER> to continue
```

Enter を押すと、Clean Access Manager クイック コンフィギュレーション ユーティリティの初期画面が表示されます。この画面に表示される一連の質問に従って初期設定を行います（「コンフィギュレーション ユーティリティ スクリプト」（P.2-10）を参照）。

（注）　インストールの後、CAM 設定（eth0 IP アドレスなど）をリセットする必要がある場合は、シリアルにまたは SSH を使用して CAM マシンに接続し、**service perfigo config** コマンドを実行します。詳細については、「CAM CLI コマンド」（P.2-19）を参照してください。その他の設定値のほとんども、後で Web 管理コンソールから変更できます。

# 初期設定の実行

CD-ROM から Clean Access Manager をインストールする場合は、ソフトウェア パッケージのインストール後に自動的にコンフィギュレーション ユーティリティ スクリプトが表示され、サーバの初期設定を進めることができます。

（注）　コンフィギュレーション ユーティリティ スクリプトは、必要に応じていつでも手動で起動できます。起動方法は次のとおりです。

1. シリアル接続上で、または CAM で直接操作して、正しいパスワードでユーザ **root** として CAM にログインします。
2. 次のコマンドを入力すると、初期設定のスクリプトが実行します。

   **service perfigo config**

**service perfigo config** コマンドを実行すると、Web 管理コンソールから到達できなくても、サーバの設定を変更できます。CLI コマンドの詳細は、「CAM CLI コマンド」（P.2-19）を参照してください。

# コンフィギュレーション ユーティリティ スクリプト

コンフィギュレーション ユーティリティ スクリプトでは、特定のパラメータのデフォルト値が示されます。設定する際には、次のように、デフォルト値をそのまま使用するか、または新しい値を入力します。

**ステップ 1**　CD からソフトウェアがインストールされ、パッケージのインストールが完了すると、次のように、コンフィギュレーション ユーティリティの初期スクリプトが表示されます。

```
Welcome to the Cisco Clean Access Manager quick configuration utility.

Note that you need to be root to execute this utility.

The utility will now ask you a series of configuration questions.
Please answer them carefully.

Cisco Clean Access Manager, (C) 2009 Cisco Systems, Inc.
```

**ステップ 2**　まず、インターフェイス eth0 の IP アドレスを設定するようプロンプトが表示されます。

```
Configuring the network interface:

Please enter the IP address for the interface eth0 []: 10.201.2.11
You entered 10.201.2.11 Is this correct? (y/n)? [y]
```

プロンプトに **y** と入力してデフォルトのアドレスをそのまま使用するか、または **n** と入力して別の IP アドレスを指定します。別のアドレスを指定する場合は、その信頼ネットワーク インターフェイスに使用するアドレスをドット区切り 10 進表記で入力します。プロンプトに従って値を確認します。

**ステップ 3**　インターフェイスのサブネット マスクを入力するか、または Enter キーを押してデフォルト値を使用します。プロンプトに従って値を確認します。

```
Please enter the netmask for the interface eth0 []: 255.255.255.0
You entered 255.255.255.0, is this correct? (y/n)? [y] y
```

**ステップ 4**　Clean Access Manager のデフォルト ゲートウェイのアドレスを指定し、確認します。これは通常、Clean Access Manager サブネットと Clean Access Server サブネットの間にあるルータの IP アドレスです。

```
Please enter the IP address for the default gateway []: 10.201.240.1
You entered 10.201.2.1 Is this correct? (y/n)? [y] y
```

**ステップ 5**　Clean Access Manager のホスト名を指定します。ホスト名は、Domain Name System（DNS、ドメイン ネーム システム）サーバ内のインターフェイス アドレスと照合され、ブラウザから Clean Access Manager 管理コンソールにアクセスするのに使用できるようになります。デフォルトのホスト名は **nacmanager** です。

```
Please enter the hostname [nacmanager]: cam1
You entered cam1 Is this correct? (y/n)? [y] y
```

**ステップ 6**　ご使用の環境の DNS サーバの IP アドレスを次のように指定します。

```
Please enter the IP addresses for the name servers: []: 172.10.16.16
You entered 172.10.16.16 Is this correct? (y/n)? [y] y
```

**ステップ 7**　1 つの構成内の Clean Access Manager および Clean Access Server は、共有秘密鍵を通じて相互に認証します。共有秘密鍵は、その構成の内部パスワードとして使用されます。デフォルトの共有秘密鍵は、**cisco123** です。プロンプトに共有秘密鍵を入力し、確認します。

```
The shared secret used between Clean Access Manager and Clean Access Server is the default
string: cisco123
```

```
This is highly insecure. It is recommended that you choose a string that is unique to your
installation.

Please remember to configure all Clean Access Devices with the same string.
Only the first 8 characters supplied will be used.
Please enter the shared secret between Clean Access Server and Clean Access Manager:
```

**注意**　同じ構成内の Clean Access Manager とすべての Clean Access Server に、すべて同じ共有秘密鍵を設定しなければなりません。共有秘密鍵が異なっていると、相互に通信できません。

**ステップ 8**　その Clean Access Manager のタイム ゾーンを次のように指定します。

**a.** 大陸と海洋のリストから該当する地域を選択します。リストの該当地域の横に記載されている数字（たとえば、アメリカなら 2）を入力し、Enter キーを押します。GST-10 のように Posix TZ フォーマットでタイム ゾーンを入力する場合は 11 を入力します。

```
The timezone is currently not set on this system.
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
 5) Asia
 6) Atlantic Ocean
 7) Australia
 8) Europe
 9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
```

**b.** 次に、選択した地域の国のリストが表示されます。国のリストから該当する国、米国なら **45** を選択し、Enter キーを押します。

```
Please select a country.
 1) Anguilla              18) Ecuador               35) Paraguay
 2) Antigua & Barbuda     19) El Salvador           36) Peru
 3) Argentina             20) French Guiana         37) Puerto Rico
 4) Aruba                 21) Greenland             38) St Kitts & Nevis
 5) Bahamas               22) Grenada               39) St Lucia
 6) Barbados              23) Guadeloupe            40) St Pierre & Miquelon
 7) Belize                24) Guatemala             41) St Vincent
 8) Bolivia               25) Guyana                42) Suriname
 9) Brazil                26) Haiti                 43) Trinidad & Tobago
10) Canada                27) Honduras              44) Turks & Caicos Is
11) Cayman Islands        28) Jamaica               45) United States
12) Chile                 29) Martinique            46) Uruguay
13) Colombia              30) Mexico                47) Venezuela
14) Costa Rica            31) Montserrat            48) Virgin Islands (UK)
15) Cuba                  32) Netherlands Antilles  49) Virgin Islands (US)
16) Dominica              33) Nicaragua
17) Dominican Republic    34) Panama
```

**c.** その国に複数のタイム ゾーンがある場合は、その国のタイム ゾーンが表示されます。リストから該当するタイム ゾーンを選択し（太平洋標準時なら **19**）、Enter キーを押します。

```
Please select one of the following time zone regions.
 1) Eastern Time
 2) Eastern Time - Michigan - most locations
 3) Eastern Time - Kentucky - Louisville area
 4) Eastern Time - Kentucky - Wayne County
```

```
 5) Eastern Time - Indiana - most locations
 6) Eastern Time - Indiana - Crawford County
 7) Eastern Time - Indiana - Starke County
 8) Eastern Time - Indiana - Switzerland County
 9) Central Time
10) Central Time - Indiana - Daviess, Dubois, Knox, Martin, Perry & Pulaski Counties
11) Central Time - Indiana - Pike County
12) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
13) Central Time - North Dakota - Oliver County
14) Central Time - North Dakota - Morton County (except Mandan area)
15) Mountain Time
16) Mountain Time - south Idaho & east Oregon
17) Mountain Time - Navajo
18) Mountain Standard Time - Arizona
19) Pacific Time
20) Alaska Time
21) Alaska Time - Alaska panhandle
22) Alaska Time - Alaska panhandle neck
23) Alaska Time - west Alaska
24) Aleutian Islands
25) Hawaii
```

**d.** **1** を入力して設定を確認します。設定を取り消してやり直す場合は、**2** を入力します。

```
The following information has been given:

        United States
        Pacific Time

Is the above information OK?
1) Yes
2) No
```

**e.** 次のプロンプトに対し Enter キーを押して現在の日付と時刻を確認するか、または次のフォーマットに正しい日付と時刻を入力します。プロンプトが表示されたら、値を確認します。

```
Current date and time hh:mm:ss mm/dd/yy [11:53:12 08/22/08]: 11:53:12 08/22/08
You entered 11:53:12 08/22/08 Is this correct? (y/n)? [y] y
```

**ステップ 9**　次に、Clean Access Manager と Web ベースの管理コンソールの間の接続のセキュリティを確保するために SSL 認証を設定します。

**a.** 証明書を発行する IP アドレスまたはドメイン名を入力します。

**（注）** これは、Web サーバの応答先の IP アドレスまたはドメイン名でもあります。ドメイン名に DNS が設定されていない場合、CAM Web コンソールはロードされません。サーバに DNS エントリが作成されていることを確認します。作成されていない場合は、CAM の IP アドレスを使用します。

**b.** 組織単位名には、証明書を管理する組織内のグループを入力します（`test` または `engineering` など）。

**c.** 組織名には、証明書を受領する組織名または会社名（`access` など）を入力し、Enter キーを押します。

**d.** その組織の法的所在地となっている市または郡の名前を入力し、Enter キーを押します。

**e.** その組織の所在地を表す 2 文字の州コード（`CA` または `NY` など）を入力し、Enter キーを押します。

**f.** `US` など、2 文字の国コードを入力し、Enter キーを押します。

g. 入力した値の要約が表示されます。表示された値で間違いがなければ、Enter キーを押します。設定し直す場合は、**N** を入力します。

```
You entered the following:
Domain: mydomain.com
Organization unit: test
Organization name: access
City name: My Town
State code: CA
Country code: US
Is this correct? (y/n)? [y]
```

**ステップ 10**　次のようなプロンプトで、プリログイン バナーのサポートを CAM の機能として使用するかどうかを指定します。

```
Enable Prelogin Banner Support? (y/n)? [n]
```

プリログイン バナー機能の詳細と例については、P.2-16 の図 2-4 を参照してください。

**ステップ 11**　インストールした Clean Access Manager の Linux OS 用の root ユーザ パスワードを設定します。root ユーザ アカウントは、シリアル接続または SSH を通じてシステムにアクセスするのに使用します。

Cisco NAC アプライアンスは、ルート ユーザ ログインについて強力なパスワードの使用をサポートします。パスワードの長さは少なくとも 8 文字にし、大文字と小文字の英字、数字、その他の文字の組み合せを使用します。たとえば、パスワード **10-9=One** は、各カテゴリの文字が 2 文字使用されていないため要件を満たしていませんが、**1o-9=OnE** は有効なパスワードです。詳細については、「システム パスワードの管理」（P.16-53）を参照してください。

```
For security reasons, it is highly recommended that you change the password for the root
user.

** Please enter a valid password for root user as per the requirements below! **

Changing password for user root.

You can now choose the new password.

A valid password should be a mix of upper and lower case letters,
digits, and other characters. Minimum of 8 characters and maximum
of 16 characters with characters from all of these classes. Minimum
of 2 characters from each of the four character classes is mandatory.
An upper case letter that begins the password and a digit that ends
it do not count towards the number of character classes used.

Enter new password:
Re-type new password:
passwd: all authentication tokens updated successfully.
```

**ステップ 12**　次に、CAM 直接アクセス Web コンソールの **admin** ユーザのパスワードを入力します。

```
Please enter an appropriately secure password for the web console admin user.

New password for web console admin:
Confirm new password for web console admin:
```

**（注）**　Web 管理コンソール ユーザのパスワード（デフォルト ユーザの **admin** を含む）の設定には、Web 管理コンソールを使用します。詳細については、「システム パスワードの管理」（P.16-53）を参照してください。

**ステップ 13**　CD からインストールした場合、設定完了後に次のようなメッセージが表示されます。

```
Configuration is complete.
```

```
Changes require a REBOOT of Clean Access Manager.
```

設定完了後に、次のコマンドを入力して CAM を再起動します。

```
# reboot
```

再起動後は、Web コンソールを通じて CAM にアクセスできるようになります。アクセス方法については、「CAM Web コンソールへのアクセス」（P.2-14）を参照してください。

- CAM の停止と起動を手動で行うコマンドについては、「CAM CLI コマンド」（P.2-19）を参照してください。
- ネットワーク カードの設定の問題については、「ネットワーク カード ドライバ サポート問題のトラブルシューティング」（P.2-20）を参照してください。

# CAM Web コンソールへのアクセス

Clean Access Manager の Web 管理コンソールは、導入された Cisco Clean Access（NAC アプライアンス）を管理するための Web インターフェイスです。

**警告**　**CAM/CAS および CAM Web コンソールにアクセスするには、製品ライセンスまたは評価ライセンスを取得しておく必要があります。製品ライセンスの入手およびインストール法、および Cisco NAC アプライアンスのサービス契約サポートの入手法の詳細は、『*Cisco NAC Appliance Service Contract / Licensing Suppor*』を参照してください。**

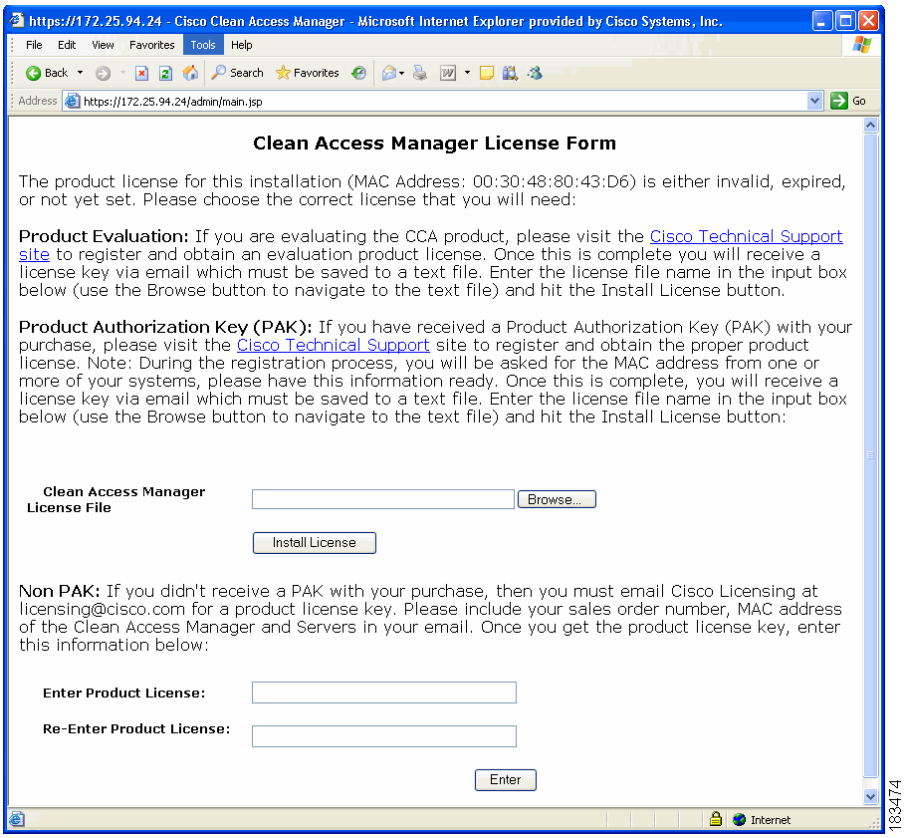
**ステップ 1**　ネットワークを通じて CAM にアクセス可能なコンピュータから Web ブラウザを起動します。この Web コンソールは、Internet Explorer 6.0 または 7.0 をサポートしています。

**ステップ 2**　URL フィールドに、CAM の IP アドレス（必要なエントリを DNS サーバに作成した場合はホスト名）を入力します。

**ステップ 3**　一時 SSL 証明書を使用する場合は、セキュリティの警告プロンプトで [Yes] をクリックし、証明書を受け入れます（署名つきの証明書を使用している場合、このセキュリティ ダイアログは表示されません）。

**ステップ 4**　[Clean Access Manager License Form] が表示され（図 2-3）、CAM FlexLM ライセンス ファイルをインストールするように要求されます。参照のために、フォームの上端に CAM の eth0 MAC アドレスが表示されます。

図 2-3　Clean Access Manager License フォーム




**ステップ 5**　[Clean Access Manager License File] フィールドで、受信したライセンス ファイルを探し、[Install License] ボタンをクリックします。

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

**注意**　大規模かつ継続的なご使用には、永久版ライセンスの取得を推奨します。評価版ライセンスは、試用を目的としたものであり、有効期間は 30 日です。ライセンスの期限が過ぎると、Cisco NAC アプライアンスを起動できなくなります。永久版ライセンスのご購入については、シスコの販売店にお問い合せください。

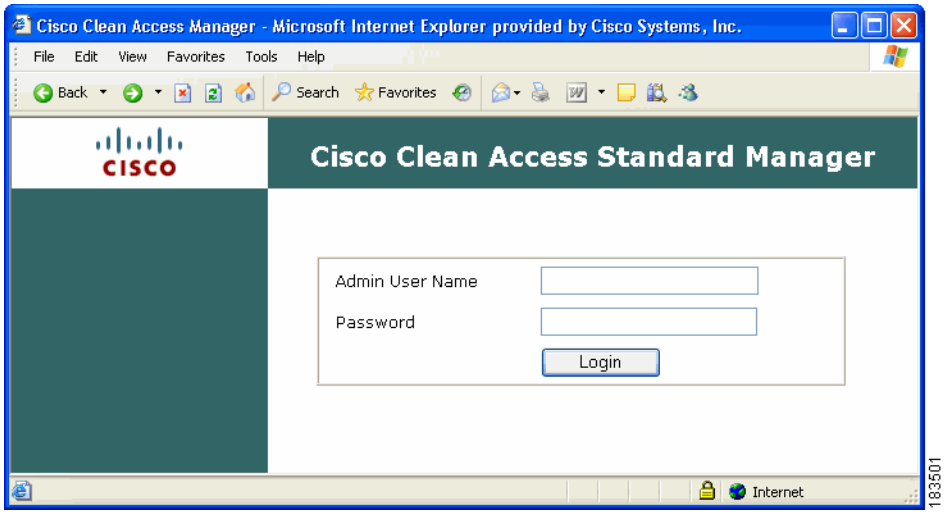
**ステップ 6**　ライセンスが受け入れられると、カスタマイズされた CAM プリログイン バナー（図 2-4）が表示されるか（CAM の初期設定の間にプリログイン バナーをイネーブルにしていた場合）、Web 管理コンソール ログイン ウィンドウが表示されます（図 2-5）。ユーザ名 **admin** と Web 管理ユーザ パスワードを入力し、[Login] をクリックします。

図 2-4　CAM プリログイン バナーの例


プリログイン バナーを使用すると、CAM/CAS で認証証明書を入力する前に、管理ユーザは警告、システム/ネットワーク ステータス、アクセス要件など、広範囲のメッセージを表示できます。管理者がプリログイン バナーのテキストを指定するには、アプライアンスでこの機能をイネーブルにし、コマンドライン コンソールにログインし、**/root/banner.pre** ファイルを編集します。プリログイン バナーのテキストは、管理ユーザが CAM/CAS にログインするときに、Web コンソール インターフェイスとコマンドライン インターフェイスの両方に表示されます。

初期の CAM/CAS 設定 CLI セッションの間、および **service perfigo config** CLI コマンドを使用してベース CAM/CAS を変更するときにいつでも、プリログイン バナーをイネーブルまたはディセーブルにできます。

図 2-5　CAM Web 管理コンソールのログイン ページ




**ステップ 7**　ユーザ名 **admin** と Web 管理ユーザ パスワードを入力し、[Login] をクリックします。

[Monitoring summary] ページが表示され、左側にナビゲーション ペインが表示されます（図 2-6）。Web 管理コンソールのモジュールを通じて、設定ができます。

Web 管理コンソールからログアウトするには、[Logout] ボタンをクリックするか、またはブラウザを閉じます。Web コンソールのさまざまな管理ユーザ レベルの作成については、「管理ユーザ」（P.16-46）を参照してください。

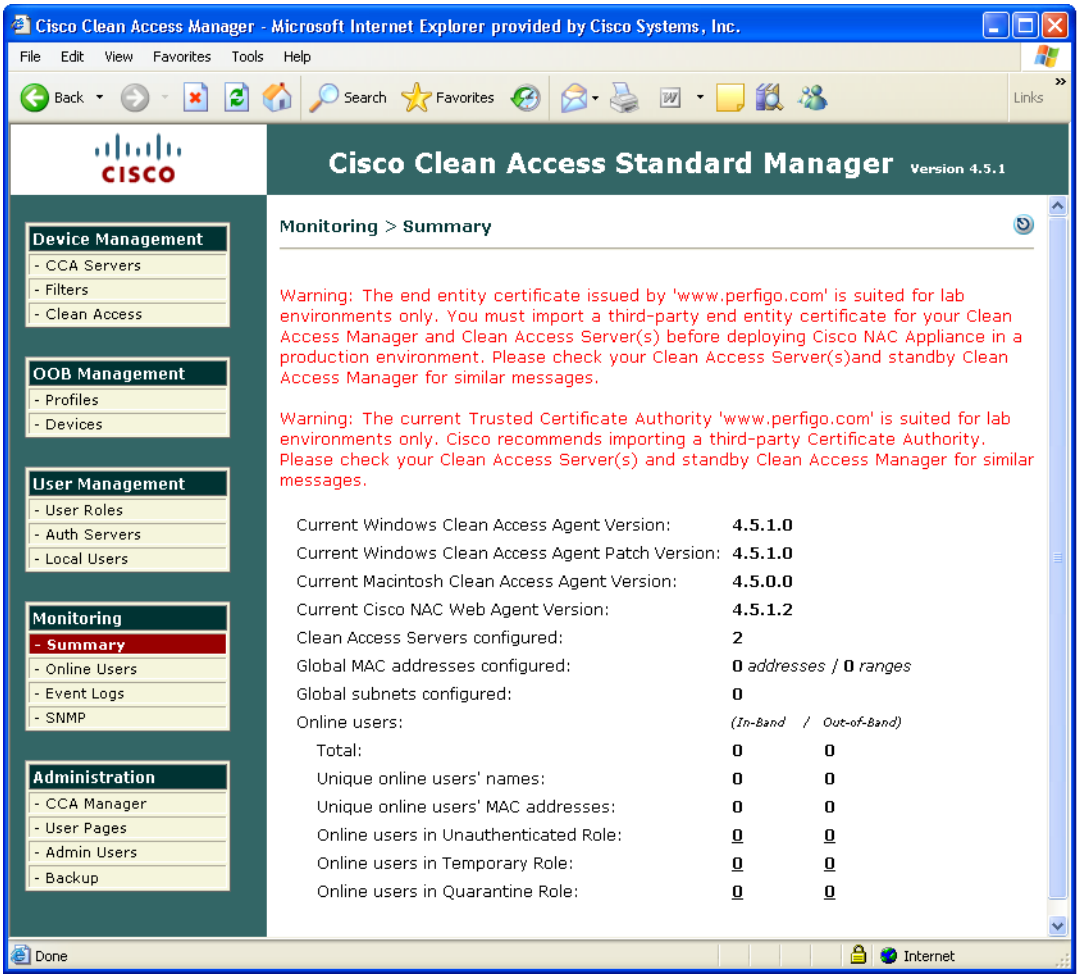
## SSL 証明書に関する重要事項

- 一時 SSL 証明書は、CAM のインストール中に作成しなければなりません。そうしないと、エンドユーザとして CAM にアクセスできなくなります。
- CAM および CAS のインストール後、Certificate Signing Request（CSR）の基礎となる一時証明書を再生成する前に、Web コンソール インターフェイスを通じて、必ず CAM と CAS の時間を同期させてください。CAM についての詳細は、以下を参照してください。
  - 「システム時刻の設定」（P.16-5）
  - 「CAM SSL 証明書の管理」（P.16-6）

  CAS の詳細は、『*Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.5(1)*』を参照してください。
- 実働環境で CAM を使用する前に、サードパーティの認証局から信頼できる証明書を取得し、一時証明書と取り替えることができます（これによって管理ログインの間に、Web ユーザにセキュリティ警告が表示されるのを防げます）。

**（注）** CAS に表示される場合は、CAS Web コンソール（図 2-6）に、「EMAILADDRESS=info@perfigo.com, CN=www.perfigo.com, OU=Product, O="Perfigo, Inc.", L=San Francisco, ST=California, C=US」認証局がご使用の CAS および関連付けられたクライアント マシンをセキュリティ攻撃に対して脆弱にする可能性があるという警告が表示されます。この認証局を見つけ、CAS データベースから削除するには、「信頼できる認証局の管理」（P.16-16）の指示に従います。

図 2-6　信頼できる認証局を取得して、既存の「www.perfigo.com」証明書を削除するよう警告する、管理者の Web コンソール メッセージ



# CAM CLI コマンド

動作の設定など、Clean Access Manager のほとんどの管理作業を Web コンソールで実行でき、CAM の起動や再起動などの操作を実行できます。ただし、ネットワークまたは VLAN の設定に問題があって Web 管理コンソールが使用できない場合など、CAM の設定に直接アクセスしなければならないこともあります。Cisco NAC アプライアンスのコマンドライン インターフェイス（CLI）を使用して、CAM 上で直接、基本的な動作パラメータを設定できます。

CLI コマンドを実行するには、SSH を使用して CAM にアクセスし、ユーザ **root** としてログインし、対応するパスワードを入力します。CAM にシリアルに接続済みの場合は、**root** としてログインした後、端末エミュレーション コンソールから CLI コマンドを実行できます（「Clean Access Manager の接続」（P.2-3）を参照）。コマンドラインからコマンドを入力するには、`service perfigo <command>` というフォーマットを使用します。表 2-1 に、よく使用される Cisco NAC アプライアンス CLI コマンドがリストしてあります。

**表 2-1　　CLI コマンド**

| コマンド | 説明 |
|---|---|
| **service perfigo start** | アプライアンスを起動します。CAM がすでに稼動している場合は、警告メッセージが表示されます。このコマンドを実行するには、CAM を停止しなければなりません。 |
| **service perfigo stop** | Cisco NAC アプライアンスのサービスをシャットダウンします。 |
| **service perfigo restart** | Cisco NAC アプライアンスのサービスをシャットダウンし、再起動します。このコマンドは、稼動中のサービスを再起動する場合に使用します。<br>**（注）**　ハイ アベイラビリティ（フェールオーバー）をテストする際には、**service perfigo restart** は使用しないでください。代わりに、フェールオーバーをテストするマシンでは「シャットダウン」または「再起動」を推奨します。CLI コマンドを使用する場合は、**service perfigo stop** と **service perfigo start** の使用を推奨します。 |
| **service perfigo reboot** | マシンをシャットダウンし、再起動します。Linux の **reboot** コマンドも使用できます。 |
| **service perfigo config** | 設定スクリプトを起動して、CAM 設定を変更できます。**service perfigo config** が完了したら、CAM を再起動する必要があります。 |
| **service perfigo time** | タイム ゾーンの設定を変更するのに使用します。 |

### CAM の電源オフ

CAM の電源をオフにする場合は、SSH 接続中に以下のいずれかを実行します。

- **service perfigo stop** と入力してから、マシンの電源をオフにします。
- **/sbin/halt** と入力してから、マシンの電源をオフにします。

### 初期設定スクリプトの再起動

設定スクリプトを再起動するには、SSH を通じて接続中に、**service perfigo config** と入力します。
例：`[root@camanager root]# service perfigo config`

CAS と CAM のいずれの場合も、このコマンドを実行すると、設定ユーティリティ スクリプトが起動されます。このスクリプトでは、CAM のネットワーク設定を構成できます（手順は「初期設定の実行」（P.2-9）を参照してください）。**service perfigo config** を実行し、完了したら、必ず **service perfigo reboot** または **reboot** を使用して、CAM を変更後の設定値にリセットします。

（注）　コマンドライン ユーティリティを使用して、自動または手動のバックアップ スナップショットからデータベースを復元する手順は、「データベース回復ツール」（P.16-63）を参照してください。

# ネットワーク カード ドライバ サポート問題のトラブルシューティング

詳細については、「Troubleshooting Network Card Driver Support Issues」の項（『*Supported Hardware and System Requirements for Cisco NAC Appliance（Cisco Clean Access）*』）を参照してください。

# WAN（Wide Area Network）での接続

WAN で CAM/CAS を使用するときは、すべての CAM/CAS トラフィックと SNMP トラフィックにプライオリティを付け、HA ペア用のサービス IP アドレスに加えて、CAM と CAS の eth0/eth1 IP アドレスを組み入れる必要があります。

# ファイアウォール経由の Cisco NAC アプライアンス接続

CAM は、CAS との接続の一部に Java Remote Method Invocation（RMI）を使用します。つまり、動的に割り当てられたポートを使用して接続します。CAS と CAM の間にファイアウォールがある場合は、CAS と CAM マシン間の接続を許可するルール、つまり、送信元が CAM で宛先が CAS（その反対も）であるようなトラフィックを許可するルールをファイアウォールに設定する必要があります。

（注）　CAS と CAM の間に NAT ルータがある場合の詳細については、『*Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.5(1)*』のインストールに関する章の「Configuring the CAS Behind a NAT Firewall」の項も参照してください。

表 2-2 に、CAS と CAM 間の通信に必要なポートを示します（Cisco Clean Access のバージョンごと）。

**表 2-2　CAM/CAS のポート接続**

| Cisco NAC アプライアンスのバージョン | 必須のポート |
|---|---|
| **4.5**<br>**4.1(x)**<br>**4.0(x)** | TCP ポート 443、1099、および 8995 ～ 8996 |
| **3.6(x)** | TCP ポート 80、443、1099、および 8995 ～ 8996 |
| **3.5(x)** | TCP ポート 80、443、1099、および 32768 ～ 61000（通常 32768 ～ 32999 で十分です） |

たとえば、SSO 機能では、表 2-3 に示すように、Clean Access Agent と Active Directory サーバ間の接続を可能にするために、別のポートが CAS およびファイアウォール（ある場合）で開かれている必要があります。表 2-3 に、通信デバイス、影響を受けるポート、各ポートの目的の詳細があります。

表 2-3　ポートの使用方法

| デバイス | 通信デバイス | 開くポート | 目的 |
|---|---|---|---|
| ファイアウォール（ある場合） | CAM と CAS | TCP 8995、8996<br>TCP 1099 | 事前接続および接続メッセージなど、CAM と CAS 間の Java Management Extension（JMX）接続。 |
| | | TCP 443 | Agent によるエンド ユーザ マシンの修復など、Agent/CAS/CAM 間の HTTP over SSL 接続。 |
| | | TCP 80（バージョン 3.6.x 以前） | Agent/CAS/CAM 間の HTTP 通信。Agent を CAM からエンド ユーザ マシンにダウンロードします。 |
| | CAS と Agent | UDP 8905、8906 | SWISS、Agent で CAS の UDP 検出に使用される独自の CAS-Agent 接続プロトコル。UDP 8905 はレイヤ 2 検出に使用され、8906 はレイヤ 3 検出に使用されます。<br>詳細については、「Connecting to the CAS Using the SWISS Protocol」の項（『*Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.5(1)*』）を参照してください。 |
| | | TCP 443 | Web ログイン ページへのユーザのリダイレクションなど、Agent/CAS/CAM 間の HTTP over SSL 接続。 |
| | | TCP 80（バージョン 3.6.x 以前） | Agent/CAS/CAM 間の HTTP 通信。Agent を CAM からエンド ユーザ マシンにダウンロードします。 |

表 2-3　ポートの使用方法　（続き）

| デバイス | 通信デバイス | 開くポート | 目的 |
|---|---|---|---|
| CAS とファイアウォール（ある場合） | Agent（Windows OS）と AD（Active Directory）サーバ | TCP 88、135、389、445、1025、1026<br>UDP 88、389 | AD SSO では次のポートが開かれている必要があります。<br>• TCP 88（Kerberos）<br>• TCP 135（RPC）<br>• TCP 389（LDAP）または TCP 636（SSL を使用する LDAP）<br>（注）　LDAP を使用して AD サーバに接続する場合は、デフォルト ポート 389 ではなく、TCP/UDP ポート 3268（デフォルトの Microsoft グローバル カタログ ポート）を使用することを推奨します。こうすると、単一ドメイン環境と複数ドメイン環境の両方ですべてのディレクトリ パーティションの検索を効率的にできます。<br>• TCP 445（Microsoft-SMB; たとえば、DC から PC へのパスワード変更通知に必要）<br>• TCP 1025（RPC）：非標準<br>• TCP 1026（RPC）：非標準<br>AD サーバが Kerberos を使用しているかどうかがわからない場合は、次の UDP ポートを開く必要があります。<br>• UDP 88（Kerberos）<br>• UDP 389（LDAP）または UDP 636（SSL 使用する LDAP）<br>（注）　LDAP を使用して AD サーバに接続する場合は、デフォルト ポート 389 ではなく、TCP/UDP ポート 3268（デフォルトの Microsoft グローバル カタログ ポート）を使用することを推奨します。これによって、単一ドメイン環境と複数ドメイン環境の両方ですべてのディレクトリ パーティションを効率的に検索できます。<br>LDAP サービスが必要な場合は、TCP/UDP 389（プレーン テキスト）の代わりに、TCP/UDP 636（SSL 暗号化を使用した LDAP) を使用してください。<br>AD SSO 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。 |