CHAPTER 4

Application Networking Manager を使用する前に

この章では、Cisco Application Networking Manager（ANM）を使用するための準備に関する事項を説明します。この章の構成は次のとおりです。

Cisco Application Networking Manager のライセンスの取得およびアップロード

ANM を使用するには、ANM のライセンスが必要です。ANM のライセンスをインストールするには、Cisco.com のユーザとして登録を済ませ、ソフトウェア CD に付属しているサービス ライセンス認証キー（PAK）を準備しておく必要があります。詳細については、*User Guide for the Cisco Application Networking Manager 2.2* の「Administering the Cisco Application Networking Manager」の章の「Understanding ANM License Information」を参照してください。

（注） ライセンスのインストール スクリプトによって ANM が再初期化されます。HA のアップグレードを実施した場合は、どのホストがアクティブ ホストかをシステムが判断するのに少々時間がかかる可能性もあります。インストールまたはアップグレード後に、ANM にログインするには、数分かかる可能性があります。

ステップ 1 Cisco.com で、http://www.cisco.com/go/license にアクセスします。Cisco.com にログインするように求められます。登録ユーザでない場合は、登録なしでログインするオプションなどを含むさまざまなオプションが利用できます。ログインが完了すると、PAK を入力するように求められます。

ステップ 2　シスコ情報パケットに添付されているラベルに表示されているものと厳密に一致するように PAK を入力します。PAK が見つからない場合は、シスコ サポート チームに連絡するか、リンクをクリックしてデモ ライセンスを入手してください。

（注）　デモ ライセンスは、発行後 90 日間有効です。90 日を過ぎると、製品には標準ライセンスが必要になります。

ステップ 3　ライセンス Web サイトでの登録に関する手順に従ってください。登録が終わると、登録を確認するメッセージが表示され、製品の登録時に入力した電子メール アドレス宛てにライセンス / キー ファイルを含む電子メールが送信されます。

ステップ 4　電子メール経由でソフトウェア ライセンス キーを受け取ったら、その電子メールと添付されているライセンス ファイル（.lic）を、安全に保管するためにハード ドライブ上の一時ディレクトリに保存します。

ステップ 5　（オプション）ファイルを一時ディレクトリから ANM サーバにコピーします。

ステップ 6　コマンドラインから **/opt/CSCOanm/bin/anm-license install** */path/ANMxxxxxxxxxxxxxxxx.lic* コマンドを入力してライセンスを ANM サーバにインストールします。

path はライセンス ファイルの場所、*ANMxxxxxxxxxxxxxxxx.lic* はライセンス ファイルの名前を指します。

/opt/CSCOanm/bin/anm-license install *license1* [*license2* **...**] コマンドを使用して複数のライセンス ファイルを一度にインストールできます。

ステップ 7　ANM にログインし、[Administration] タブで [ANM Management] > [License Management] を選択して ANM サーバと ANM-AD のライセンスの両方が表示できるようにします。

両方のライセンスが表示されない場合は、手順が欠落しています。ネットワーク管理者に連絡して、足りないライセンスをインストールしてください。

（注）　ライセンスの詳細については、「ライセンスの種類」（P.4-5）を参照してください。

サーバ認証のためのサイト特有の証明書 / キー ペアのファイルのアップロード

リリース ANM 2.0 以降では、任意の証明書 / キー ペアを使用してサーバを認証できます。

（注）　このオプションの手順は、インストール時だけでなくいつでも実行できます。証明書 / キー ペアは、ANM に自動的にインストールされます。HA モードでは、両方のノードでこの手順を実行する必要があります。

サーバ認証のためのサイト固有の証明書/キー ペアのファイルをアップロードするには、次の手順に従います。

ステップ 1　必要に応じて、ファイル（証明書およびキー）を一時ディレクトリから ANM サーバにコピーします。

ステップ 2　コマンドラインから、**/opt/CSCOanm/bin/anm-certificate install** *certificate key* [*key-password*] コマンドを入力します。ここで、*certificate* はインストールする証明書ファイルの名前で、*key* は証明書キー ファイルの名前、*key-password* はキー パスワード（必要な場合）です。

（注）　キー パスワードが必要なのは、キーが暗号化されている場合だけです。

Cisco Application Networking Manager へのログイン

ANM の機能へは、Web ベースのインターフェイスを使用してアクセスします。ANM ログイン ウィンドウでは、ANM サーバへのログイン、アカウントのパスワードの変更、および **[Help]** をクリックしてオンライン ヘルプを参照できます。

ANM にログインするには、次の手順に従います。

ステップ 1　次のいずれかから選択します。

- 新規インストール後にログインするには、ブラウザのアドレス フィールドに「**https://***host*」と入力します。デフォルトの Web ポートは 443 および 80 です。

  （注）　ポート番号を明示的に入力する必要はありません。

  注意　HTTP を使用してログインする場合は、プロパティ ファイルを変更する必要があります。詳細については、「Cisco Application Networking Manager インストール後の設定値の変更」（P.4-20）を参照してください。HTTP をイネーブルにすると、ANM への接続のセキュリティ状態が低下することに注意してください。

- アップグレード後にログインするには、以前のリリースでどのポートがイネーブルになっていたかに応じて、ブラウザのアドレス フィールドに「**https://***host***:10443**」または「**http://***host***:10080**」と入力します。アップグレードでは、ユーザが指定した Web ポートである 10443 および 10080 を使用します。これらのポート番号は明示的に入力する必要があります。

（注）　すべてのブラウザで、cookie、JavaScript/スクリプト、およびポップアップ ウィンドウをイネーブルにする必要があります。後続の ANM リリースを再インストールする場合は、cookie を削除し、ブラウザのキャッシュをクリアします。

たとえば、「**https://192.168.10.10**」と入力します。ログイン ウィンドウが表示されます。

新しいインストールでは、クレデンシャルが事前に定義されています。ユーザ名とパスワードはどちらも admin です。最初にログインする際には、admin を使用します。

ステップ 2　[User Name] フィールドに「**admin**」と入力します。

admin アカウントは、ANM がインストールされた際に作成されています。ログイン後、追加のユーザ アカウントを作成できます。ユーザ アカウントの設定の詳細については、オンライン ヘルプまたは『*User Guide for the Cisco Application Networking Manager 2.2*』の第 15 章「Administering the Cisco Application Networking Manager」にある「Managing User Accounts」を参照してください。

ステップ 3　[Password] フィールドに ANM のインストールに使用したパスワードを入力します。

ステップ 4　[Login] をクリックします。

注意　ANM のインストールでは、初期化が完了するのに 90 秒程度かかります。ログイン ウィンドウが表示されたら、ログインする前に少なくとも 90 秒待機するようにしてください。最低 90 秒待機しないと、エラーが発生してしまう可能性があります。

ログイン時には、[Config] > [Devices] ウィンドウが表示されます。「Cisco Application Networking Manager へのネットワーク要素の追加」（P.4-9）で説明したいずれかの方法によってネットワーク要素を追加するまで、インターフェイスにはデータが含まれません。ユーザ インターフェイスの詳細については、オンライン ヘルプの概要または『*User Guide for the Cisco Application Networking Manager 2.2*』の第 1 章「Application Networking Manager Overview」を参照してください。

Cisco Application Networking Manager のライセンス管理

ANM が、ご使用のネットワーク要素すべてを管理できるようにするには、ネットワーク要素に対し、適切な数の ANM ライセンスを有する必要があります。ソフトウェアには ANM サーバ ライセンスが付属していますが、インストール後にそれを ANM にアップロードする必要があります。

ANM では、それぞれデフォルトで 5 つの仮想コンテキストのセットを持つ最大 2 つの ACE アプライアンスを管理できます。標準的な設定を超えたネットワーク要素を管理する場合は、追加のライセンスが必要になります。

管理するネットワーク要素の数を拡張するために、新しい ANM のライセンスを追加する詳細については、オンライン ヘルプまたは『*User Guide for the Cisco Application Networking Manager 2.2*』の第 15 章「Administering the Cisco Application Networking Manager」にある「Managing ANM Licenses」を参照してください。

ANM サーバ ライセンスのアップロード方法については、「Cisco Application Networking Manager のライセンスの取得およびアップロード」（P.4-1）を参照してください。

ライセンスの種類およびライセンス管理の詳細については、「ライセンスの種類」（P.4-5）またはオンラインヘルプまたは『*User Guide for the Cisco Application Networking Manager 2.2*』の第 15 章「Administering the Cisco Application Networking Manager」を参照してください。

ここでは、次の内容について説明します。

ライセンスの種類

ライセンスの管理では、ライセンスの状態の表示、ライセンスの追加、および ANM 上のライセンス情報の追跡が可能です。ご使用の ANM のライセンスが適合していない場合、または ANM のライセンスの期限切れが近い場合には、ANM に警告が表示されます。Cisco ANM では、次のような異なる種類のライセンスを購入できます。

- ACE アプライアンスおよびモジュール用のライセンス：ANM-AD-xx は、特定数の ACE アプライアンスまたはモジュールを管理できます。
- CSS または CSM ネットワーク要素 / モジュール用のライセンス：ANM-CD-xx は、特定数の CSS または CSM ネットワーク要素 / モジュールを管理できます。
- ネットワーク要素を仮想エンティティに拡張するための仮想ライセンス：ANM-AV-xx は、サポート対象となる仮想コンテキスト用の ACE のライセンス（ACE-VIRT-xx）を持つ 1 つの ACE アプライアンスまたはモジュールを管理できます。たとえば、ACE-VIRT-050 がインストールされている ACE 4710 アプライアンスを使用している場合は、ソフトウェアに付属していた PAK を参照して入力し、Cisco.com 上でライセンス ファイルを入手します。
- デモ ライセンス：ANM-DEMO は、無料の 30、60、または 90 日間のライセンスで、ANM 2.2 では最大 3 つのデモ ライセンスを使用できます。
- サーバ ライセンス：ANM-SERVER は、ANM サーバを実行できます。

ANM ライセンスのアップロード

ANM サーバがアクセスできるディレクトリにライセンス ファイルをダウンロードした場合は、ANM ライセンスをアップロードできます。詳細については、「Cisco Application Networking Manager のライセンスの取得およびアップロード」（P.4-1）を参照してください。

（注） ご使用のユーザ ロールによってこのオプションが利用できるかどうかが決まります。ロール ベースのアクセスの詳細については、オンライン ヘルプまたは『*User Guide for the Cisco Application Networking Manager 2.2*』の第 15 章「Administering the Cisco Application Networking Manager」にある「Controlling Access to ANM」を参照してください。

ANM の追加ラインセスをアップロードするには、以下の手順に従います。

ステップ 1　[Admin] > [ANM Management] > [License Management] > [Licenses] を選択します。[Licenses] テーブルが表示されます。

ステップ 2　[Licenses] テーブルから、[Add] をクリックします。[New License] ウィンドウが表示されます。

ステップ 3　[New License] ウィンドウから、[Browse] をクリックして新しいライセンスの名前を参照します。ブラウザを使用して、ライセンス ファイルを選択します。

ステップ 4　ブラウザ ウィンドウから、[Upload] をクリックして入力したライセンスを ANM サーバにコピーするか、[Cancel] をクリックして終了します。

ライセンス ファイルが [Licenses] テーブルおよび [License Files] テーブルに表示されます。[Licenses] テーブルからは、フィルタ処理、ライセンスの追加、またはテーブルのビューの変更も可能です。テーブルのボタンの説明については、オンライン ヘルプを参照してください。

[License Files] テーブルには、ライセンス ファイルのインストール状態と、エラーがある場合はそのエラーが表示されます。対処方法については、オンライン ヘルプを参照してください。

HA インストールを実行している場合は、2 番目のホスト マシン用のライセンスも必要です。スタンバイ サーバの ANM にログインし、上記の手順を繰り返します。

ネットワーク要素の追加準備

ANM では、データベースに次のネットワーク要素を個別に追加できます。

- ACE アプライアンス
- ACE モジュール
- Catalyst 6500 シリーズのシャーシ
- Cisco 7600 シリーズのルータ
- Cisco Content Services Switch（CSS ネットワーク要素）
- Cisco Content Switching Module（CSM）
- Cisco Global Site Selector（GSS ネットワーク要素）

（注）　アプライアンス、モジュール、またはその他のネットワーク要素をインポートする前に、ANM サーバはネットワーク要素の IP アドレスに対して ping を実行します。ANM サーバとインポートするネットワーク要素の間でファイアウォールを使用している場合は、ファイアウォールを変更して、ping のトラフィックがネットワーク要素または ACE モジュールに到達できるようにする必要があります。

ヒント　アプライアンス、モジュール、またはネットワーク要素を追加したら、ANM CLI の同期プロセスの詳細について「ACE からの Syslog メッセージのイネーブル化」（P.4-19）を参照してください。サポートされるネットワーク要素の詳細については、『*Supported Devices Table for the Application Networking Manager 2.1 and 2.2*』を参照してください。

ANM は、Secure Shell （SSH; セキュア シェル）およびその他のプロトコルを使用してネットワーク要素と通信します。ANM がネットワーク要素からデータを収集できるようにそれらのネットワーク要素を設定する必要があります。ここでは、次の内容について説明します。

- 「Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータにおける SSH または Telnet によるアクセスのイネーブル化」（P.4-7）
- 「ACE モジュールと ACE アプライアンスでの SSH アクセスと HTTPS インターフェイスのイネーブル化」（P.4-7）
- 「ANM からの SNMP ポーリングのイネーブル化」（P.4-9）

Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータにおける SSH または Telnet によるアクセスのイネーブル化

ANM で Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータをインポートするには、Telnet または SSH を使用できます。Catalyst 6500 シリーズ スイッチでは、Telnet がデフォルトでイネーブルになっています。シャーシで Telnet がディセーブルになっている場合、ACE モジュールの初期設定およびインポートを実行するには Telnet をイネーブルにする必要があります。ACE モジュールを直接 ANM にインポートしたい場合、Catalyst 6500 シリーズ スイッチ上で Telnet は必須ではありません。

シャーシおよびACE モジュール 上で SSH2 をイネーブルにし、ANM がシャーシのネットワーク要素の情報を追加できるようにする必要があります。シャーシ上で SSH サーバをイネーブルにするには、K9 （Triple Data Encryption Standard [3DES]）ソフトウェア イメージが必要です。ANM では、シャーシ上で SSH2 をイネーブルにする必要があります。

次の表には、シャーシ上で SSH2 をイネーブルにするためのコマンドを一覧表示します。

コマンド	目的
`ip ssh version 2`	SSH バージョン 2 をイネーブルにします。
`ip domain-name abc.com`	
`crypto key generate rsa general-keys modulus 1024`	キーを生成します。
`username <username> password <password>`	ユーザ名とパスワードを入力できるようにします。
`line vty 0 4`	
`session-timeout 60`	
`login local`	Cisco IOS 12.2.18SXF(10) には適用されますが、Cisco IOS 12.2.18SXF(8) には適用されません。
`transport input telnet ssh`	シャーシに SSH と Telnet を使用できるようにします。
`transport output telnet ssh`	シャーシが ACE モジュールに SSH と Telnet を使用できるようにします。

ACE モジュールと ACE アプライアンスでの SSH アクセスと HTTPS インターフェイスのイネーブル化

ANM は、HTTPS 経由で SSH と XML を使用して ACE モジュールおよび ACE 4710 アプライアンスと通信します。SSH アクセスと HTTPS の両方をイネーブルにする必要があります。これらの設定は、「Cisco Application Networking Manager へのネットワーク要素の追加」（P.4-9）で説明されているようにネットワーク要素のインポート中または CLI 内でイネーブルにできます。

（注）　ユーザ インターフェイスに適用される管理ポリシーが SSH を許可することを確認します。

次の表は、ANM がアクセスできるようにするために SSH と HTTPS を ACE で設定するコマンドの一覧です。次のコマンドを設定モードで管理コンテキストに入力します。

ヒント　ACE モジュールまたはアプライアンスが新品で、工場出荷時の設定のままの場合は、SSH がベアブレードの設定でイネーブルになっているのでこれらのコマンドを使用する必要はありません。ACE アプライアンスが工場出荷時の設定になっていない場合は、管理コンテキストで次のコマンドを使用します。

コマンド	目的
`ssh key rsa 1024 force`	ACE 上で SSH アクセスを設定します。
`access-list acl line 10 extended permit ip any any`	
`class-map type management match-any ANM_management`	検出を実行します。

`2 match protocol ssh any`
`3 match protocol telnet any`
`4 match protocol https any`
`5 match protocol snmp any`
`6 match protocol icmp any`
`7 match protocol xml-https`
	左側の列のコマンド テキストの前に行番号を指定します。
	• 行 2 は SSH トラフィックを分類します。
	• 行 4 は ACE 上の設定を変更するために ANM で必要になります。
	• 行 5 は統計のために ANM で必要になります。
	• 行 6 は必須ではありませんが、ネットワークとルートの検証に役立ちます。
	• 行 7 は、ACE 4710 アプライアンスでのみ必要です。

`policy-map type management first-match ANM_management`
`  class ANM_management`
`  permit`
	管理クラス マップ内で一致するプロトコルを許可します。

`interface vlan 30`
`  ip address 192.168.65.131 255.255.255.0`
`  access-group input acl`
`  service-policy input ANM_management`
`  no shutdown`
	ACL 付きのユーザ インターフェイスとして機能し、管理サービス ポリシーを定義します。このインターフェイスをクライアントまたはサーバのインターフェイスとして使用することは推奨されません。

`username admin password 5 $1$faXJEFBj$TJR1Nx7sLPTi5BZ97v08c/ role Admin domain default-domain`	管理者を指定します。
`ip route 0.0.0.0 0.0.0.0 192.168.0.1`	ANM が同じサブネット内にない場合にユーザ インターフェイスを使用して ANM にトラフィックが到達するように障害ルート（または適切なルート）を指定します。

ACE モジュール上で SSH アクセスを設定する詳細については、Cisco.com から入手可能な『*Cisco Application Control Engine Module Administration Guide*』を参照してください。

ACE アプライアンス上で SSH アクセスをイネーブルにする方法の詳細については、Cisco.com から入手可能な『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』の第 2 章「Enabling Remote Access to the ACE」を参照してください。

ANM からの SNMP ポーリングのイネーブル化

ANM からのネットワーク イベントの SNMP ポーリングをイネーブルにできます。ACE 1.0 モジュールでは、ポーリングが必要なすべてのコンテキスト上で SNMP トラフィックを許可する適切な管理ポリシーと管理 IP が必要です。ACE 2.0 モジュールでは、SNMP トラフィックを許可する適切な管理ポリシーと管理 IP を使用し、管理コンテキストを設定する必要があります。その他のすべてのコンテキストは、管理コンテキストの管理 IP を使用してポーリングできます。詳細については、*User Guide for the Cisco Application Networking Manager 2.2* の第 3 章「Configuring Virtual Contexts」を参照してください。

（注）　SNMP トラップを ANM に送信するには、ANM サーバに対して SNMP トラップ ホストを設定し、ANM からトラップを受信できるようにします。

Cisco Application Networking Manager へのネットワーク要素の追加

次のモジュール、スイッチ、ルータ、およびネットワーク要素を ANM データベースに個別に追加できます。

- ACE アプライアンス
- ACE モジュール
- Catalyst 6500 シリーズ スイッチ
- Cisco 7600 シリーズのルータ
- Cisco Content Services Switch（CSS ネットワーク要素）
- Cisco Content Switching Module（CSM）
- Cisco Global Site Selector （GSS ネットワーク要素）

（注）　ACE モジュールとアプライアンスを正常にインポートするには、次のことを確認する必要があります。

- ACE モジュールまたは CSM が正常に起動し、OK/Pass の状態になっている（Cisco IOS コマンドの **show module** を使用）。
- ACE 4710 または CSS の状態が稼動中である。これらのネットワーク要素が稼動中かどうかを検証するコマンドはありません。

ここでは、次の内容について説明します。

- 「ANM へのモジュール、スイッチ、ルータ、およびその他のネットワーク要素の追加」（P.4-10）
- 「ANM への ACE モジュールの追加」（P.4-14）
- 「Cisco Content Switching Module のインポート」（P.4-16）
- 「Cisco Global Site Selector のインポート」（P.4-17）

ANM へのモジュール、スイッチ、ルータ、およびその他のネットワーク要素の追加

ANM では、ACE アプライアンス、Catalyst 6500 シリーズ シャーシ、Cisco 7600 シリーズ ルータ、CSS、および GSS ネットワーク要素を、検出を実行して [Discovery Jobs] テーブルからインポートする代わりに、またはその作業に加えて、それぞれデータベースに追加できます。モジュールをインポートする方法については、「ANM への ACE モジュールの追加」（P.4-14）を参照してください。CSM ネットワーク要素をインポートする方法については、「Cisco Content Switching Module のインポート」（P.4-16）を参照してください。

ネットワーク要素をインポートするのにかかる時間は、インポート対象のアプライアンス、シャーシ、モジュール、およびコンテキストの数に依存します。たとえば、50 個の仮想コンテキストを持つ ACE アプライアンスは、25 個のコンテキストを持つ ACE アプライアンスよりも長くかかります。ANM がネットワーク要素をインポートする間、同じセッションでは別の処理を実行できません。ただし、ANM がネットワーク要素をインポートする間、ANM サーバと新しいセッションを確立し、別のアプライアンス、シャーシ、モジュール、または仮想コンテキストに対する処理を実行できます。

ACE アプライアンスとその他のサポートされるネットワーク要素を ANM データベースに個別に追加するには、次の手順に従います。

ステップ 1　[Config] > [Devices] > [All Devices] を選択します。[All Devices] テーブルが表示されます。

ステップ 2　デバイス ツリーまたは [All Devices] デーブルで、[Add] をクリックします。[New Device] ウィンドウが表示されます。

ステップ 3　表 4-1 内の情報を使用してネットワーク要素の情報を入力します。

表 4-1　[New Device] の属性

フィールド	説明
[Name]	ネットワーク要素に一意の名前を入力できるフィールドです。引用符の付いていない、スペースを含まないテキスト文字列が有効なエントリで、最大 26 文字の英数字を使用できます。
[Model]	インポートするアプライアンスまたはサポートされるネットワーク要素の種類です。 • ACE4710：ACE 4710 アプライアンス。 • CSS：Cisco Content Services Switch。 • Cisco IOS Device：サポートされる Catalyst 6500 シリーズ シャーシまたは Cisco 7600 シリーズ ルータ。 • GSS：高性能のネットワーク要素。これはデータ センターごとの SLB の状態と負荷を監視し、その情報とお客様側で制御するルーティング アルゴリズムを使用して、リアルタイムで最適かつ最も負荷の少ないデータ センターを選択します。
[Primary IP]	ネットワーク要素の IP アドレスをドット付き十進法の形式で入力できるフィールドです。
[Access Protocol]	モデルに [GSS] または [IOS Device] を選択すると表示されるフィールドです。ANM がネットワーク要素または Cisco IOS ネットワーク要素にアクセスするのに使用するプロトコルとして、[Secure/SSH2] または [Telnet] を選択します。GSS では、Secure/SSH2 を使用します（これが表示される唯一のオプションです）。
[Username]	ネットワーク要素のアクセス用のアカウント名を入力できるフィールドです。 **（注）**　この手順の前に、シャーシ上でアカウントを設定しなかった場合は、スペースを含まない英数字の文字列を入力し、この手順を完了できます。不正なアクセスを防ぐために、ネットワーク要素上でアカウントを設定することを推奨します。
[Password]	アカウントのパスワードを入力できるフィールドです。

表 4-1　[New Device] の属性（続き）

フィールド	説明
[Enable Password]	Catalyst 6500 シリーズ シャーシ、Cisco 7600 シリーズ ルータ、および GSS ネットワーク要素向けにセキュリティ レベルを強化するために表示されるフィールドです。
[SNMP V2C Enabled]	Catalyst 6500 シリーズ シャーシ、Cisco 7600 シリーズ ルータ、および CSS 向けに表示されるフィールドです。 [SNMP V2C Enabled] チェックボックスをオンにし、SNMP アクセスを設定します。
[Community]	[SNMP V2C] チェックボックスをオンにすると表示されるフィールドです。 ネットワーク要素用のコミュニティ文字列を入力します。 （注）　Catalyst 6500 シリーズ シャーシを追加する場合、Catalyst 6500 シリーズ シャーシ上で既に設定されている SNMP コミュニティ文字列を [Community] フィールドに入力します。ANM は、この文字列を使用して VLAN およびインターフェイスの状態などのネットワーク要素の状態に関する情報を問い合せます。この SNMP コミュニティ文字列は、指定された Catalyst 6500 シリーズ スイッチ内の CSM モジュールでも使用されます。 Catalyst 6500 シリーズ シャーシ、CSS、および CSM ネットワーク要素に関しては、ANM がポーリングするのにネットワーク要素上であらかじめ設定されている SNMP コミュニティ文字列が使用されます。ACE モジュールおよび ACE アプライアンスに関しては、ANM に入力された SNMP コミュニティ文字列が ACE モジュール/アプライアンス上で設定され、ネットワーク要素をポーリングするのに使用されます。
説明	ネットワーク要素の簡潔な説明を入力できるフィールドです。

ステップ 4　次のいずれかを実行します。

- [Next] をクリックしてエントリを保存し、ネットワーク要素情報をインポートします。ネットワーク要素に関連付けられた ACE モジュールがない場合は、経過表示バーに状態が表示され、[All Devices] テーブルが更新された情報でリフレッシュされます。ACE モジュールがネットワーク要素に関連付けられている場合は、経過表示バーに状態が表示され、[Modules] 設定ウィンドウが表示されます。ステップ 5 にスキップします。
- エントリを保存せずに手順を終了し、[All Devices] テーブルに戻るには [Cancel] をクリックします。[Cancel] をクリックすると、ネットワーク要素情報がインポートされず、ACE モジュールの検出が行われません。

ステップ 5　[Modules] ウィンドウでは、現在のモジュールをインポートするか、[Next] をクリックしてこのモジュールをスキップし次のモジュールに進みます。

ステップ 6　モジュールをインポートするには、[Card Slot] フィールドに現在のモジュールが表示されるか確認します。

ステップ 7　[Card Type] フィールドで、正しいネットワーク要素の種類が表示されるのを確認します。

（注）　ネットワーク要素のサポートされるバージョンも表示されますが、表示されるのはメジャー リリース別です。たとえば、8.2x がサポートされる場合でも、8.2 だけが表示されます。

[Module has been imported into ANM] フィールドは、表示されますが変更できません。モジュールがインポート済みであることを示す場合は、チェックボックスがオンであり、まだインポートされていないことを示す場合は、チェックボックスがオフになっていることを確認します。これは読み取り専用のフィールドです。

ステップ 8　[Operation to Perform] フィールドで、次のいずれかを選択します。

- **Import**：ANM が ACE モジュールの設定をインポートできます。ステップ 9 にスキップします。
- **Perform initial setup and import**：ANM が ACE モジュールと通信し、ACE モジュールの設定をインポートするのに必要な初期設定を手動で実行できます。ステップ 10 にスキップします。

（注）　工場出荷時のデフォルトだけで設定されている ACE モジュールに対しては、[Perform initial setup and import] を選択することを推奨します。

ステップ 9　[Import] を選択する場合は、次の情報を入力します。

a.　[Admin Context IP] フィールドに、このモジュールで使用する IP アドレスを入力します。

b.　[Username] フィールドに、このモジュールにアクセスするためのユーザ名を入力します。

c.　[Password] フィールドに、このモジュールにアクセスするためのパスワードを入力します。[Confirm] フィールドにパスワードを再入力します。

d.　ステップ 11 にスキップします。

ステップ 10　[Perform initial setup and import] を選択する場合は、次の情報を入力します。

a.　[Hostname] フィールドに、このモジュール用の一意の名前を入力します。スペースを含まない英数字の文字列が有効なエントリで、最大 32 文字を使用できます。

b.　[Admin Context IP] フィールドに、このモジュール用の IP アドレスを入力します。

c.　[Netmask] フィールドで、プルダウン メニューからこの IP アドレスに適用するサブネット マスクを選択します。

d.　[Gateway] フィールドに、使用するゲートウェイ ルータの IP アドレスを入力します。

e.　[VLAN] フィールドで、このモジュールが属する VLAN を選択します。

ステップ 11　ACE ブレードが工場出荷時のデフォルトの管理クレデンシャル（admin/admin）を使用して設定されるかどうかは、次のように指定します。

- デフォルトの管理クレデンシャルを変更している場合は、[Username] と [Password] のフィールドに新しいネットワーク要素クレデンシャルを入力します。
- デフォルトの管理クレデンシャル（admin/admin）を変更していない場合は、[Username] と [Password] のフィールドに ACE 上の新しいクレデンシャルを入力します。

（注）　セキュリティ上の理由から、ご使用の ACE アプライアンス（およびモジュール）のユーザ名とパスワードは、インポート後に変更することを推奨します。シスコから出荷されたすべての ACE モジュールでユーザ名とパスワードが同じ設定になっているため、それらを変更しないとご使用の ACE モジュールのセキュリティが侵害される可能性があります。詳細については、オンライン ヘルプまたは『*User Guide for the Cisco Application Networking Manager 2.2*』の第 2 章「Adding and Managing Devices」にある「Changing ACE Module Passwords」を参照してください。

ステップ 12　次のいずれかを実行します。

- エントリを保存してネットワーク要素の設定を続行するには、[OK] をクリックします。経過表示バーに状態が表示され、[Device] 設定ウィンドウが表示されます。オンライン ヘルプまたは『*User Guide for the Cisco Application Networking Manager 2.2*』の第 2 章の「Adding and Managing Devices」を参照してください。
- ACE モジュールをインポートせずに [All Devices] テーブルに戻るには、[Cancel] をクリックして手順を終了します。

（注）　このウィンドウで [Cancel] をクリックしてもシャーシのインポート プロセスはキャンセルされません。

ステップ 13　ACE 上の仮想コンテキストが ANM に正常にインポートされたことを確認します。

a.　[Config] > [Devices] を選択します。デバイス ツリーが表示されます。

b.　デバイス ツリーで、今インポートした ACE を選択します。[Virtual Contexts] テーブルが表示され、そのネットワーク要素のコンテキストが一覧表示されます。

c.　コンテキストが正常にインポートされたことを確認します。

- [Config Status] 列に [OK] と表示されたら、コンテキストは正常にインポートされています。
- [Config Status] 列に [Import Failed] と表示されたら、コンテキストは正常にインポートされませんでした。

d.　コンテキストを選択して [Sync] をクリックし、失敗したコンテキスト インポートに関する設定を同期させます。ANM は、ACE アプライアンスからコンテキストをアップロードすることで、コンテキスト同期を行います。

仮想コンテキストの同期の詳細については、オンライン ヘルプまたは『*User Guide for the Cisco Application Networking Manager 2.2*』の第 3 章「Configuring Virtual Contexts」にある「Synchronizing Virtual Context Configurations」を参照してください。

（注）　ACE モジュールおよびアプライアンスをインポートしようとして、認証エラーまたは不正なユーザ名 / パスワードのエラーが表示された場合は、ユーザ名およびパスワードの設定と制限事項に関する ACE ドキュメントを、cisco.com のサイト（http://www.cisco.com/en/US/products/ps7027/tsd_products_support_series_home.html）から入手してください。

ANM への ACE モジュールの追加

シャーシまたはルータのインポート後は、ACE モジュールを ANM データベースにいつでもインポートできます。

ACE モジュールをインポートするのにかかる時間は、インポートするモジュールとコンテキストの数に依存します。たとえば、20 個の仮想コンテキストを持つ ACE モジュールは、5 個のコンテキストを持つ ACE モジュールよりも長くかかります。ANM がモジュールをインポートする間、同じセッションでは別の処理を実行できません。ただし、ANM がネットワーク要素をインポートする間、ANM サーバと新しいセッションを確立し、別のネットワーク要素、モジュール、または仮想コンテキストに対する処理を実行できます。

ACE モジュールおよびアプライアンスをインポートしようとして、認証エラーまたは不正なユーザ名 / パスワードのエラーが表示された場合は、ユーザ名およびパスワードの設定と制限事項に関する ACE ドキュメントを、サイト（http://www.cisco.com/en/US/products/ps7027/tsd_products_support_series_home.html）から入手してください。

シャーシ内の ACE モジュールを物理的に交換する場合は、ANM 内のシャーシを同期させる必要があります。「ACE からの Syslog メッセージのイネーブル化」（P.4-19）で説明しているように、ANM 自動同期プロセスを活用できるように Syslog 設定の調節から始めることをお勧めします。

この手順を開始する前に、ACE モジュールを含むネットワーク要素を少なくとも 1 つ ANM データベースにインポートし、インポートされるモジュールが正常に起動され、*OK/Pass* の状態であることを必ず検証してください。モジュールの状態をチェックするには、Cisco IOS コマンドの **show module** を使用してください。

ステップ 1　[Config] > [Devices] > [All Devices] を選択します。[All Devices] テーブルが表示されます。

ステップ 2　[All Devices] テーブルから、インポートする ACE モジュールを含むネットワーク要素を選択し、[Modules] をクリックします。次の手順で説明するフィールドを含む [Modules] テーブルが表示されます。

ステップ 3　インポートするモジュールを選択し、[Import] をクリックします。[Modules] 設定ウィンドウが表示されます。

ステップ 4　[Card Slot] フィールドで、正しいモジュールが表示されるのを確認します。

ステップ 5　[Card Type] フィールドで、正しいバージョンが表示されるのを確認します。

ステップ 6　[Operation to Perform] フィールドで、次のインポート オプションのいずれかを選択します。

- **Import**：ANMACE モジュール設定をインポートできます。ステップ 7 にスキップします。
- **Perform initial setup and import**：ANM により、ACE モジュールに事前検出設定ファイルを提供し、ACE モジュール設定をインポートできます。このオプションは、ACE モジュールが以前に設定されたことがない場合だけ選択してください。ACE ブレードが工場出荷時のデフォルトの管理クレデンシャル（admin/admin）を使用して設定されているかどうかについては、次のように指定します。
  - デフォルトの管理クレデンシャルを変更している場合は、[Username] と [Password] のフィールドに新しいネットワーク要素クレデンシャルを入力します。
  - デフォルトの管理クレデンシャル（admin/admin）を変更していない場合は、[Username] と [Password] のフィールドに新しいクレデンシャルを入力すると、ANM が ACE 上のクレデンシャルを設定します。

  ステップ 8 にスキップします。

ステップ 7　[Import] を選択する場合は、次の情報を入力します。

a. [Admin Context IP] フィールドに、このモジュールで使用する IP アドレスを入力します。

b. [Username] フィールドに、このモジュールにアクセスするためのユーザ名を入力します。

c. [Password] フィールドに、このモジュールにアクセスするためのパスワードを入力します。

（注） セキュリティ上の理由から、ご使用の ACE アプライアンス（およびモジュール）のユーザ名とパスワードは、インポート後に変更することを推奨します。シスコから出荷されたすべての ACE モジュールでユーザ名とパスワードが同じ設定になっているため、それらを変更しないとご使用の ACE モジュールのセキュリティが侵害される可能性があります。詳細については、オンライン ヘルプまたは『*User Guide for the Cisco Application Networking Manager 2.2*』の第 2 章「Adding and Managing Devices」にある「Changing ACE Module Passwords」を参照してください。

ステップ 8　[Perform Initial Setup And Import] を選択する場合は、次の情報を入力します。

a. [Hostname] フィールドに、モジュール用の一意の名前を入力します。スペースを含まない英数字の文字列が有効なエントリで、最大 32 文字を使用できます。

b. [Admin Context IP] フィールドに、モジュール用の IP アドレスを入力します。

c. [Netmask] フィールドで、プルダウン メニューから IP アドレスに適用するサブネット マスクを選択します。

d. [Gateway] フィールドに、ゲートウェイ ルータの IP アドレスを入力します。

e. [VLAN] フィールドで、モジュールが属する VLAN を選択します。

ステップ 9　次のいずれかを実行します。

- エントリを保存するには、[OK] をクリックします。経過表示バーに状態が表示され、[Modules] テーブルが更新された情報でリフレッシュされます。
- モジュールをインポートせずに [Modules] テーブルに戻るには、[Cancel] をクリックして手順を終了します。

ステップ 10　モジュール上の仮想コンテキストが ANM に正常にインポートされたことを確認します。

a. [Config] > [Devices] を選択します。デバイス ツリーが表示されます。

b. デバイス ツリーから、今インポートしたモジュールを選択します。[Virtual Contexts] テーブルが表示され、そのモジュールのコンテキストが一覧表示されます。

c. コンテキストが正常にインポートされたことを確認します。

- [Config Status] 列に [OK] と表示されたら、コンテキストは正常にインポートされています。
- [Config Status] 列に [Import Failed] と表示されたら、コンテキストは正常にインポートされませんでした。

d. コンテキストを選択して [Sync] をクリックし、失敗したコンテキスト インポートに関する設定を同期させます。ANM は、モジュールからコンテキストをアップロードすることで、コンテキスト同期を行います。

仮想コンテキストの同期の詳細については、オンライン ヘルプまたは『*User Guide for the Cisco Application Networking Manager 2.2*』の第 3 章「Configuring Virtual Contexts」にある「Synchronizing Virtual Context Configurations」を参照してください。

Cisco Content Switching Module のインポート

シャーシまたはルータのインポート後は、CSM ネットワーク要素を ANM データベースにいつでもインポートできます。

（注）　ANM は、ネットワーク要素のタイプ CSM を、CSM と CSM-S ネットワーク要素の両方に割り当てます。この割り当ては、ANM がネットワーク要素から受け取った情報を収集および割り当てる方法に関係するもので、機能には影響を及ぼしません。これらのネットワーク要素を区別する方法については、ユーザ インターフェイス内の説明を参照してください。

CSM をインポートするには、次の手順に従います。

ステップ 1　[Config] > [Devices] > [All Devices] を選択します。[All Devices] テーブルが表示されます。

ステップ 2　[All Devices] テーブルから、インポートする CSM を含むネットワーク要素を選択し、[Modules] をクリックします。[Modules] テーブルが表示されます。

ステップ 3　[Modules] テーブルから、インポートする CSM を選択し、[Import] をクリックします。[Modules] 設定ウィンドウが表示されます。

ステップ 4　次の読み取り専用のフィールドに含まれる情報が正しいか検証します。

- [Card Slot] : モジュールが備わっているシャーシ内のスロットです。
- [Card Type] : ネットワーク要素の種類で、ここでは CSM です。
- [Module has been imported into ANM] : 既にインポートされていることを示す場合はオンで、まだインポートされていないことを示す場合はオフになっているチェックボックスです。

ステップ 5　[Operation to Perform] フィールドで、[Import] を選択します。

ステップ 6　次のいずれかを実行します。

- エントリを保存するには、[OK] をクリックします。経過表示バーに状態が表示され、[Modules] テーブルが更新された情報でリフレッシュされます。
- ネットワーク要素をインポートせずに [Modules] テーブルに戻るには、[Cancel] をクリックして手順を終了します。

Cisco Global Site Selector のインポート

GSS ネットワーク要素を ANM データベースにインポートできます。GSS ネットワーク要素をインポートするには、次の手順を実行します。

ステップ 1　[Config] > [Devices] > [All Devices] を選択します。[All Devices] テーブルが表示されます。

ステップ 2　[All Devices] テーブルから、[Add] ボタンを選択します。[New Device] ページが表示されます。

ステップ 3　[New Device] ページから、表 4-2 内の情報を使用してネットワーク要素を設定します。

表 4-2　GSS 設定オプション

フィールド	説明
[Name]	ネットワーク要素に割り当てられた名前です。
[Model]	GSS を選択できるプルダウン メニューです。
[Primary IP Address]	ネットワーク要素の IP アドレスを含む読み取り専用フィールドです。
[User Name]	ANM データベースにインポートされた他の GSS ネットワーク要素を表示するフィールドです。
[Password]	このユーザ アカウントのパスワードを指定できるフィールドです（設定可能、定義された最小値または最大値に基づく）。
[Enable Password]	Catalyst 6500 シリーズ シャーシ、Cisco 7600 シリーズ ルータ、CSS、および GSS ネットワーク要素向けにセキュリティ レベルを強化するために表示されるフィールドです。
説明	このネットワーク要素の簡潔な説明を入力できるフィールドです。

ステップ 4　次のいずれかを実行します。

- エントリを保存するには、[OK] をクリックします。経過表示バーに状態が表示され、[Modules] テーブルが更新された情報でリフレッシュされます。
- ネットワーク要素をインポートせずに [Modules] テーブルに戻るには、[Cancel] をクリックして手順を終了します。

GSS のファイアウォール環境での配置

ご使用の GSS をファイアウォール越しに配置する場合は、DNS トラフィックをネットワーク要素の中に許可する必要があります。ネットワーク要素間のトラフィックがファイアウォールを通過するように、複数の GSS ネットワーク要素を配置している場合は、GSS 間の通信と GSS 間の状況報告が許可されるようにファイアウォールを設定します。ご使用の GSS 設定によっては、他のトラフィックがファイアウォールを越えられるようにすることもできます。この要件は、ご使用の GSS 設定（たとえば、TCP ベースまたは KAL-AP キープアライブを使用している場合）や、特定の GSS サービス（たとえば、SNMP）にファイアウォールを介してアクセスできるかどうかに依存します。

GSS は、GSS 間で通信を行うために、NAT の後ろ側へネットワーク要素を配置する構成はサポートしません。ネットワーク要素の実際の IP アドレスはパケットのペイロードに組み込まれているので、GSS ネットワーク要素間の通信に NAT の後ろ側にある中間ネットワーク要素を含めることはできません。詳細については、サイト（http://www.cisco.com/en/US/products/hw/contnetw/ps4162/tsd_products_support_series_home.html）から入手可能な GSS ドキュメントを参照してください。

表 4-3 は、ANM が GSS と通信するのに使用される TCP ポートの一覧です。

表 4-3　GSS によって ANM 向けに使用される TCP ポート

ポート	説明
22	SSH
2001	Java RMI
3002	Java RMI
3003	Secure RMI
3004	Secure RMI
3005	Secure RMI
3006	Secure RMI
3007	Secure RMI
3008	Secure RMI

ACE からの Syslog メッセージのイネーブル化

ネットワーク要素が Syslog メッセージを受信すると自動同期が行われるように設定できます。[Setup Syslog for Autosync] をイネーブルにした場合、デフォルトのポーリング期間が過ぎるのを待たずに、Syslog メッセージを受信すると ANM が同期されます。

ANM に仮想コンテキスト用の Syslog メッセージを受信させるには、次の手順に従います。

ステップ 1　[Config] > [Devices] > [Setup Syslog for Autosync] を選択します。[Setup Syslog for Autosync] ウィンドウが表示されます。

ステップ 2　[All VC] または自動同期の Syslog メッセージの対象となる、仮想コンテキストの設定を含む ACE のいずれかを選択します。経過表示バーのウィンドウが表示されます。

チェックを付けた仮想コンテキストと ACE アプライアンスごとに、[Setup Syslog for Autosync?] 列の中にチェックマークの付いたチェックボックスが表示されます。

ステップ 3　[Setup Syslog for Autosync] ウィンドウから、[Setup Syslog] をクリックします。

次の CLI コマンドが、イネーブルされたネットワーク要素に送信されます。

```
logging enable
logging trap 2
logging device-id string <ACE-Ip>/Admin
logging host <ANM-Ip>  udp/514
logging message 111008 level 2
```

ANM に目的のシャーシ、モジュール、およびアプライアンスが入力されたら、次のことを実行できます。

- リソース、ユーザ、およびサービスを管理するために仮想コンテキストを設定する。オンライン ヘルプまたは『*User Guide for the Cisco Application Networking Manager 2.2*』の第 3 章「Configuring Virtual Contexts」にある「Using Virtual Contexts」を参照してください。
- ネットワーク上で実装するための設定テンプレートをセットアップする。オンライン ヘルプまたは『*User Guide for the Cisco Application Networking Manager 2.2*』の第 13 章「Using Configuration Building Blocks」を参照してください。
- リソースを効果的に管理するためのリソース クラスを設定する。オンラインヘルプまたは『*User Guide for the Cisco Application Networking Manager 2.2*』の第 3 章「Configuring Virtual Contexts」にある「Using Resource Classes」を参照してください。
- ユーザを追加する。オンライン ヘルプまたは『*User Guide for the Cisco Application Networking Manager 2.2*』の第 5 章「Administering the Application Networking Manager」を参照してください。
- データをバックアップする。「データのバックアップと復元」（P.5-8）を参照してください。

ANM 機能の概要については、オンライン ヘルプまたは『*User Guide for the Cisco Application Networking Manager 2.2*』の第 1 章「Cisco Application Networking Manager Overview」を参照してください。

Cisco Application Networking Manager インストール後の設定値の変更

ANM をインストールしたら、ANM ポートおよびその他のいくつかの ANM 設定プロパティを再設定できます。

注意　HTTP をイネーブルにすると、ANM への接続のセキュリティ状態が低下します。

ポートまたはその他の ANM 設定プロパティを再設定するには、次の手順に従います。

ステップ 1　「root ユーザになる」（P.1-5）で説明したように、Linux のコマンド ラインから、root ユーザとしてログインします。

ステップ 2　コマンドラインから、次のいずれかを入力します。

- 標準的な設定変更には、**/opt/CSCOanm/bin/anm-tool configure** コマンドを入力します。
- HA から非 HA のシステム設定に切り替えるには、**/opt/CSCOanm/bin/anm-tool --ha=0 configure** コマンドを入力します。
- 非 HA から HA のシステム設定に切り替えるには、**/opt/CSCOanm/bin/anm-tool --ha=1 configure** コマンドを入力します。

「Keep existing ANM configuration? [y/n]（既存の ANM 設定を保持しますか？ [y/n]）」というメッセージが表示されます。

ステップ 3　「**n**」を入力します。

インストール時に表示されたものと同じ設定情報を含むメッセージが表示されます。

ステップ 4　設定プロパティごとに、現在の値が角カッコに囲まれて表示されます。

次のいずれかを実行します。

- 設定プロパティとして値を受け入れる場合は、**Enter** キーを押します。
- 設定プロパティを変更するには、適切な情報を入力します。

設定プロパティの値をすべて承認または変更したら、すべてのプロパティのリストが表示され、「Commit these values? [y/n/q]（これらの値をコミットしますか？ [y/n/q]）」というメッセージが表示されます。

ステップ 5　次のいずれかを実行します。

- 値を承認し、ANM を再起動するには、「**y**」（はい）と入力します。
- 設定プロパティのリストを再確認するには、「**n**」（いいえ）と入力します。
- 元の値を保持して設定セッションを終了するには、「**q**」と入力します。

HA プロパティの設定値を変更しようとした際にエラーが発生した場合、ホスト ID をチェックし、アクティブとスタンバイの値が切り替わっていないことを確認します。

ステップ 6　ANM を再起動し、変更をプロパティ ファイルに適用します。詳細については、「Cisco Application Networking Manager の停止」（P.5-5）および「Cisco Application Networking Manager の起動」（P.5-5）を参照してください。

HA 設定セッションの例

次に、HA システムの設定セッションの例を挙げます。非 HA システムには、いずれの HA プロパティも含まれませんが、限定されたプロパティ値の設定が含まれます。カッコに囲まれた値は、現在設定されている値です。

```
/opt/CSCOanm/bin/anm-tool configure
Configuring ANM

Checking ANM configuration files
Keep existing ANM configuration? [y/n]: n
Creating config file (/opt/CSCOanm/etc/cs-config.properties)

HTTP Port of Web Server [80]:
Enable HTTP for Web Server [false]:
HTTPS Port of Web Server [443]:
Enable HTTPS for Web Server [true]:
Database Password [passme]:
HA Node 1 UName [rh46.cisco.com]:
HA Node 2 UName [rh47.cisco.com]:
HA Node 1 Primary IP [192.168.65.46]:
HA Node 2 Primary IP [192.168.65.47]:
HA Node 1 HeartBeat IP [10.100.1.46]:
HA Node 2 HeartBeat IP [10.100.1.47]:
HA Virtual IP [192.168.65.126]:
HA Node ID [1]:

These are the values:
HTTP Port of Web Server: 80
Enable HTTP for Web Server: false
HTTPS Port of Web Server: 443
Enable HTTPS for Web Server: true
Database Password: passme
HA Node 1 UName: rh46.cisco.com
HA Node 2 UName: rh47.cisco.com
HA Node 1 Primary IP: 192.168.65.46
HA Node 2 Primary IP: 192.168.65.47
HA Node 1 HeartBeat IP: 10.100.1.46
HA Node 2 HeartBeat IP: 10.100.1.47
HA Virtual IP: 192.168.65.126
HA Node ID: 1

Commit these values? [y/n/q]: y
Committing values ... done
Keeping existing configuration: /opt/CSCOanm/lib/java/thirdparty/ctm_config.txt

Stopping services
Stopping monit services (/etc/monit.conf) ...   (0)
Stopping monit ...  Stopped
Stopping heartbeat ...  Stopped

Installing system configuration files

Setting service attributes
Enabling mysql for SELinux
Service monit is started by OS at boot time

Starting mysql ... Started

Configuring mysql
Checking mysql user/password
Setting mysql privileges
```

```
Enabling mysql replication
Setting up database
executing /opt/CSCOanm/lib/install/etc/dcmdb.sql ...  done

Starting services
Starting monit ... Started
```

ANM ポートの参考資料

ANM は目的に合せて特定のポートを使用します。図 4-1 は、ネットワーク内での一般的な ANM サーバの配置を示しています。この図では、通常の配置における異なるネットワーク デバイスによって使用されるプロトコルとポートを示しています。

- 表 4-4 は、ANM クライアント（ブラウザ）または ANM サーバおよび ANM のハイ アベイラビリティの通信で使用されるポートの一覧です。
- 表 4-5 は、ANM と管理対象デバイス間の通信に使用されるポートの一覧です。

図 4-1　ANM サーバの配置

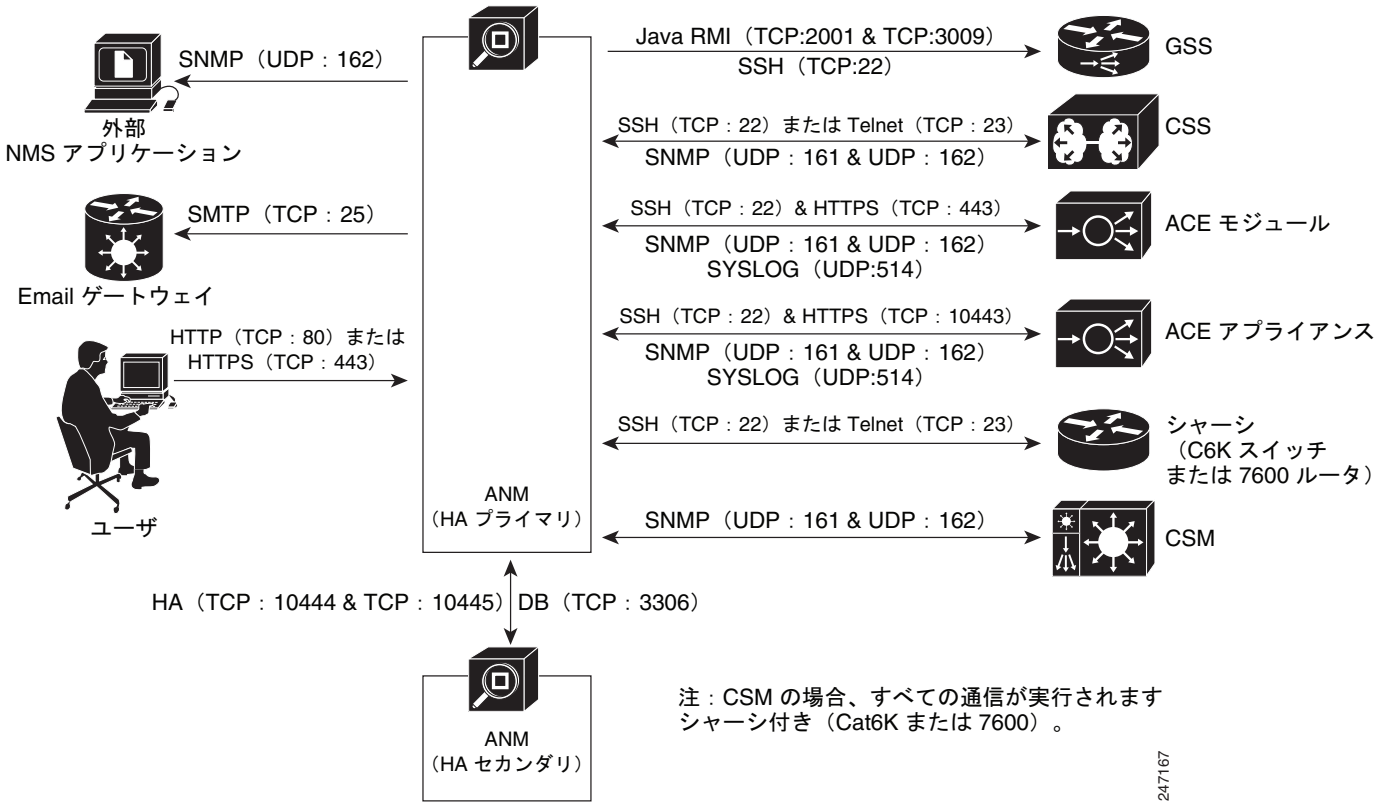

表 4-4　ネットワーク配置の中で ANM によって使用されるポート[1]

ポート	説明
TCP（80）	ANM が HTTP を使用してアクセスするように設定されている場合（AMN インストーラを使用）のデフォルトのポート。
TCP（443）	ANM が HTTPS を使用してアクセスするように設定されている場合（デフォルトのインストール オプションを使用）のデフォルトのポート。
TCP（3306）	MySQL データベース システム（ANM HA インストールでは、ピア ANM と通信するためにこのポートが開かれます)。
TCP（10444） および TCP（10445）	ANM License Manager （ANM HA インストールでは、ピア ANM と通信するためにこれらの 2 つのポートが開かれます)。
TCP（25）	ANM サーバが SMTP 経由で電子メールのゲートウェイと通信するために使用するポート。
UDP（162）	ANM サーバが外部の NMS アプリケーションにトラップ通知を送信するために使用するポート。

1. ANM はスタンドアロン デバイス上で実行することを強く推奨します。ただし、ANM を共有デバイス上で実行する場合、ANM が内部通信用に次のポートをローカルで開いている点に注意してください。

   TCP ポート：10003、10004、10023、40000、40001、40002、40003
   UDP Port：10003

表 4-5　ANM が管理対象デバイスとの通信に使用するポート

デバイスの種類	ポート	説明
シャーシ（Catalyst 6500 スイッチまたは Cisco 7600 ルータ）	SSH（TCP:22）または Telnet（TCP:23）	シャーシの設定を検出します。
ACE（アプライアンスまたはモジュール）	HTTPS（TCP:443）	ACE モジュール用：特定の **show** CLI コマンドを使用して検出、設定、および監視をするのに使用されるデバイス上の XML/HTTPS インターフェイス。
	HTTPS（TCP:10443）	ACE アプライアンス用：特定の **show** CLI コマンドを使用して検出、設定、および監視をするのに使用されるデバイス上の XML/HTTPS インターフェイス。
	SSH（TCP: 22）	ACE ライセンスの検出および設定、証明書/キー（crypto）のライセンス設定、スクリプト、およびチェックポイント。
	SNMP（UDP: 161 & UDP:162）	SNMP リクエスト（UDP: 161）経由で ACE を監視し、トラップ通知（UDP: 162）を受信します。
CSM	SNMP（UDP: 161 & UDP:162）	SNMP リクエスト（UDP: 161）経由で CSM を監視し、トラップ通知（UDP: 162）を受信します。

表 4-5　ANM が管理対象デバイスとの通信に使用するポート（続き）

デバイスの種類	ポート	説明
CSS	SSH（TCP:22）または Telnet（TCP:23）	シャーシの設定を検出します。
	SNMP（UDP: 161 & UDP:162）	SNMP リクエスト（UDP: 161）経由で CSS を監視し、トラップ通知（UDP: 162）を受信します。
GSS	SSH（TCP:22）	シャーシの設定を検出し、DNS 規則と VIP 応答の稼動状況を監視します。
	RMI（TCP:2001 & TCP:3009）	DNS 規則と VIP 応答を起動/一時停止します。