CHAPTER 14

ハイ アベイラビリティ（HA）の設定

この章では、HA（ハイ アベイラビリティ）モードの 2 つの Clean Access Server（CAS）を設定する方法について説明します。ハイ アベイラビリティモードで CAS を導入することで、予期せぬシャットダウンが発生した場合も重要なユーザ認証および接続作業を継続できます。この章の内容は、次のとおりです。

概要

次のキーポイントでは、高レベルな HA-CAS 操作の概要を説明します。

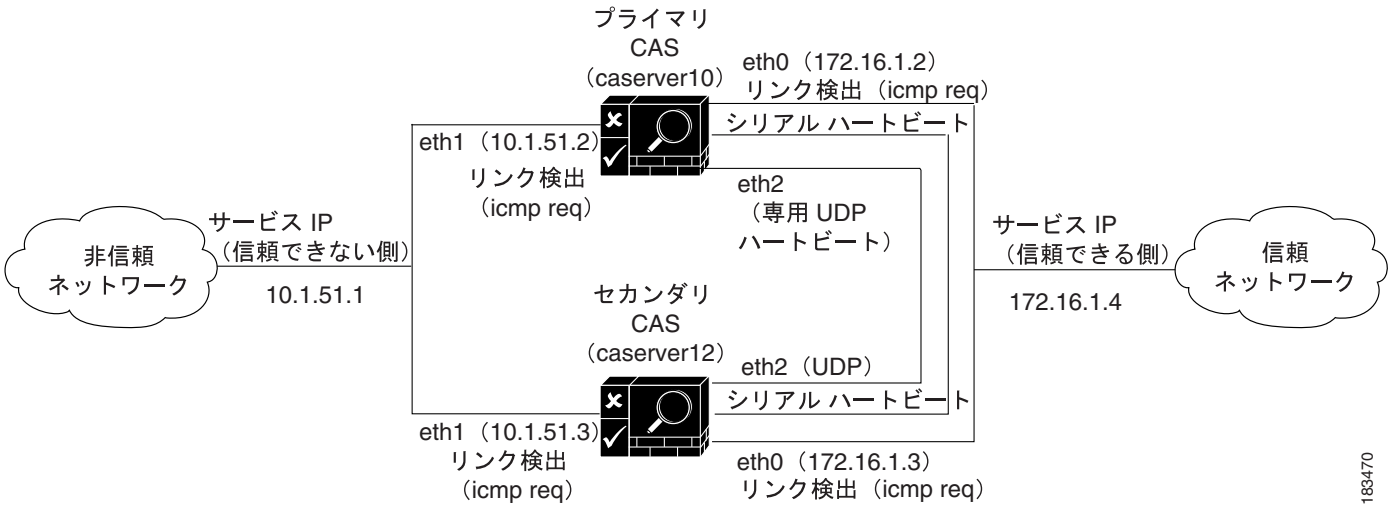
- CAS のハイアベイラビリティ モードは、スタンバイ CAS マシンがアクティブ CAS マシンのバックアップとして機能する、アクティブ / パッシブの 2 つのサーバ構成です。
- アクティブ CAS は、システムのすべての作業を実行します。CAS フェールオーバーが発生すると CAS 設定の大半は CAM に保存されるので、CAM は設定を新しいアクティブ CAS に移動します。
- スタンバイ CAS はインターフェイスの間でパケットを転送しません。
- スタンバイ CAS は、ハートビート インターフェイス（シリアルおよび / または UDP）経由でアクティブ CAS の状態をモニタします。ハートビート パケットはシリアル インターフェイス、専用の eth2 インターフェイス、または eth0 インターフェイス（eth2 インターフェイスが利用できない場合）上で送信できます。
- プライマリおよびセカンダリ CAS マシンは UDP ハートビート パケットを 2 秒ごとに交換します。ハートビート タイマーの期限が切れると、ステートフル フェールオーバーが発生します。
- ハートビートベースのフェールオーバーの他に、CAS は eth0 または eth1 リンク障害に基づいてリンクベースのフェールオーバーも提供します。CAS は、eth0 および / または eth1 インターフェイス経由で ICMP ping パケットを外部 IP アドレスに送信します。1 つの CAS が外部アドレスに ping を実行できる場合のみ、フェールオーバーが発生します。

（注）　これらの ping パケットの状態がハートビート インターフェイス経由で CAS の間で伝達されます。そのため、リンクベースのフェールオーバーを使用する場合はハートビート接続が依然として必要です。

- 両方の CAS は、信頼できるインターフェイス（eth0）および信頼できないインターフェイス（eth1）に対して仮想サービス IP を共有します。サービス IP は SSL 証明書用に使用する必要があります。

図 14-1 に、HA-CAS の構成例における基本的な接続の例を示します。

図 14-1　CAS のハイ アベイラビリティ構成例



（注）「プライマリ / セカンダリ」は HA 用に設定されたときのモードを示します。
「アクティブ / スタンバイ」はサーバの実行時ステータスを示します。

最初に HA ピアを設定する場合、HA プライマリ CAS と HA セカンダリ CAS を指定する必要があります。まず、HA プライマリ CAS がアクティブ CAS になり、HA セカンダリ CAS がスタンバイ（パッシブ）CAS になります。フェールオーバー イベントが発生し、このアクティブ CAS がシャットダウンする、またはピアのハートビート信号への応答を停止した場合、スタンバイ CAS はアクティブ CAS の役割を引き継ぎます。

CAS は再起動時に、ピアがアクティブであるかどうかを調べます。ピアがアクティブである場合、起動中の CAS はスタンバイになります。ピアがアクティブでない場合、起動中の CAS がアクティブの役割を担います。

一般的に、CAS は HA ペアとして同時に設定されます。ただし、新しい CAS を既存のスタンドアロン CAS に追加してハイアベイラビリティ ペアを作成することもできます。このペアを 1 つのエンティティとしてネットワークおよび Clean Access Manager（CAM）に認識させるには、ペアの信頼できるインターフェイス（eth0）に**サービス IP アドレス**と信頼できないインターフェイス（eth1）にサービス IP アドレスを指定する必要があります。

CAS のサービス IP アドレスを使用して CAS を CAM に追加します。図 14-2 では、ハイアベイラビリティ ペアのアクティブ CAS を、CAM Web コンソールの **List of Servers** のペアに対応するサービス IP の横のカッコ内に表示する方法を示します。さらに、信頼できるインターフェイスまたは信頼できないインターフェイスのサービス IP アドレスを使用して、SSL 認証を生成する必要があります。

図 14-2　HA ペアのアクティブ CAS

（注）CAS が事前に設定され、スタンドアロン CAM として CAS に追加された場合、HA 用に設定する前に CAS を削除する必要があります。両方の CAS で HA 構成が完了したら、サービス IP は **New Server** フォームで入力され、HA-CAS ペアを CAM に追加します。

（注）さらに、セキュリティを強化するため、（「ヌル モデム ケーブル」を使用して）各 CAS のシリアル ポートを接続してハートビートを交換することを推奨します。

フェールオーバー イベント

- UDP ハートビートとシリアル ハートビートの両方のインターフェイスを設定する場合、両方に障害が発生しないと、スタンバイ システムは処理を引き継ぎません。詳細については、「物理的な接続」（p.14-5）を参照してください。
- ハートビート経由で CAS が CAM と通信できない場合。
  - すでに接続しているユーザは影響を受けません。
  - 新規のユーザはログインできません。
- リンクベースのフェールオーバーを設定できます。CAS 外部の 2 つの IP アドレスは、リンク検出用に設定されます。1 つは信頼できるネットワーク上で、もう 1 つは信頼できないネットワーク上にあります。
  - アクティブおよびスタンバイ CAS は eth0 経由で ICMP ping パケットを信頼できるネットワーク上の IP アドレスに送信します。
  - アクティブおよびスタンバイ CAS は eth1 経由で ICMP ping パケットを信頼できないネットワーク上の IP アドレスに送信します。

  これらの ping パケットの状態がハートビート信号を介して CAS の間で伝達されます。
  - アクティブおよびスタンバイ CAS が 両方の外部 IP に ping を実行できる場合、フェールオーバーは発生しません。
  - アクティブおよびスタンバイ CAS が 外部 IP のいずれかに ping を実行できない場合、フェールオーバーは発生しません。
  - アクティブ CAS は 外部 IP のいずれかに ping を実行できませんが、スタンバイ CAS が ping を実行できる場合、フェールオーバーが発生します。

リンクベースのフェールオーバー用外部 IP の選択

- CAS がトラフィックを開始したときに、パケットがデフォルト ゲートウェイ宛てでない限り、通常は信頼できない（eth1）インターフェイスからパケットが送信されます。そのため、CAS 用に信頼できるネットワークの外部 IP を選択して eth0 インターフェイス経由で ping を実行する場合、CAS サブネット以外のサブネットに属する IP を選択します。
- CAS 用に信頼できないネットワークの外部 IP を選択して eth1 インターフェイス経由で ping を実行する場合。
  - この IP は CAS 管理サブネット上にある必要があります。
  - CAS のデフォルト ゲートウェイになることはできません。
  - CAS はこれらの ping パケットを eth1 インターフェイスから送信します。
  - eth1 インターフェイスで **Set Management VLAN ID** がイネーブルであるか確認します。このオプションがイネーブルでない場合、CAS は eth1 インターフェイスのタグ付けされていないトラフィックを送信します。スイッチは、これらのパケットをネイティブ VLAN で受信する必要があるかどうか判断します。したがって、信頼できないインターフェイスでは、ネイティブ VLAN が転送されます。
  - 外部 IP アドレスは CAS 管理サブネット内にありますが、信頼できない側にあるので、トラフィックはネイティブ VLAN の CAS から発信します。したがって、ネイティブ VLAN は外部 IP アドレスに向けて転送されます。

設定の詳細については、「c. HA プライマリ モードの設定および更新」（p.14-11）および「c. HA セカンダリ モードの設定および更新」（p.14-16）を参照してください。

CAS ハイ アベイラビリティの要件

ここでは、ハイ アベイラビリティを実行する場合の追加の考慮事項について説明します。

物理的な接続

CAS のハイアベイラビリティ ペアのフェールオーバー ハートビート**専用**の接続を使用することを推奨します。次を使用できます。

- シリアル ヌルモデム ケーブル
- 専用のイーサネット NIC カード（CAS の eth2 インターフェイスとして設定）
- eth0 **および** シリアル ヌルモデム ケーブルでの UDP ハートビート

3 番めの NIC カードを CAS の eth2 インターフェイスとして設定することを推奨します。サーバにネットワークインターフェイスが 2 つのみある場合、この目的で、次のいずれかの NIC カードを購入できます。

- PWLA8492MT = Intel PRO/1000 MT Dual Port Server Adapter（銅線）
- PWLA8492MF = Intel PRO/1000 MF（デュアル SX ファイバ LC コネクタ）

（注） HA（HA-CAM または HA-CAS）のシリアル ケーブル接続の場合、シリアル ケーブルは「ヌル モデム」ケーブルにする必要があります。詳細については、http://www.nullmodem.com/NullModem.htm を参照してください。

3 番めのネットワーク インターフェイス（eth2 など）を使用できる場合は、このインターフェイスを eth0 の代わりに UDP ハートビートに使用できます。この場合は、2 つのマシンの eth2 インターフェイス同士をクロス ケーブルで接続します。別のイーサネット インターフェイスを導入する場合は、インターフェイスの IP アドレスを設定します（「NIC カードの追加設定」[p.4-22] を参照）。

サーバ マシンの専用イーサネット インターフェイス（eth2 など）を使用できない場合は、シリアル ハートビートとともにハートビート UDP インターフェイスとして eth0 がサポートされます。「ハートビート UDP インターフェイスの選択および設定」（p.14-8）を参照してください。

一般に、シリアル ハートビート接続を実行するには、サーバ マシンに少なくとも 2 つのシリアル ポートが必要です。1 つ（ttyS0）はシリアル ハートビート接続用、もう 1 つは設定作業のためのサーバ アクセス用です。詳細については、「シリアル ポートの HA 接続」（p.14-9）を参照してください。

（注） HA（フェールオーバー）設定を開始する前に、シリアル ケーブルを接続しないでください。必ず設定が完了してから、シリアル ケーブルを接続してください。「CAS の接続および設定の完了」（p.14-20）を参照してください。

Switch Interfaces for OOB Deployment

アウトオブバンド配置の場合、CAS および Clean Access Manager（CAM）の接続先となるスイッチ インターフェイスでポート セキュリティがイネーブルでないことを確認します。ポート セキュリティがイネーブルになっていると、CAS HA および DHCP デリバリに問題が生じることがあります。

Service IP Addresses

各 CAS の信頼できるインターフェイスおよび信頼できないインターフェイスの IP アドレスのほかに、CAS ペアの信頼できるインターフェイスおよび信頼できないインターフェイスのサービス IP アドレスを 2 つ指定する必要があります（設定例については、図 14-1 [p.14-2] を参照）。**サービス IP アドレス**は、外部ネットワークがペアのアドレス指定に使用する共通の IP アドレスです。

さらに、信頼できるインターフェイスまたは信頼できないインターフェイスのサービス IP アドレスを使用して、SSL 認証を生成する必要があります。CAS が事前に設定され、スタンドアロン CAM として CAS に追加された場合、HA 用に設定される前に CAS を削除する必要があります。

両方の CAS で HA 構成が完了したら、**New Server** 形式のサービス IP を使用して、HA-CAS ペアを CAM に追加します。HA-CAS ペアは同じサーバ タイプとして自動的に追加されることに注意してください（たとえば、アウトオブバンド バーチャル ゲートウェイ）。

Host Names

ハートビートの場合、CAS ごとに一意なホスト名（またはノード名）が必要です。HA CAS ペアの場合、このホスト名をピアに提供し、DNS を介して解決するか、ピアの /etc/hosts ファイルに追加する必要があります。

DHCP Synchronization

CAS が（DHCP リレー モードまたはパススルー モードではなく）DHCP サーバとして機能する場合は、追加の設定手順を実行して、CAS が DHCP 関連情報を常に同期できるように設定する必要があります。アクティブなリースやリース期間などの DHCP 情報は、「DHCP フェールオーバーの設定」（p.14-22）の説明に従って設定される SSH トンネルを介して交換されます。

SSL Certificates

HA モードの CAS は、スタンドアロン モードの場合と同様に、自己署名付きの一時証明書または CA（認証局）署名付きの証明書のいずれかを使用できます。一時証明書は、テストまたは開発の場合に便利です。運用配置には、CA 署名付き証明書が必要です。いずれの場合も、次の考慮事項があります。

1. 一時証明書および CA 署名付き証明書では、(信頼できるインターフェイスまたは信頼できないインターフェイスの) サービス IP アドレスを使用したり、証明書ドメイン名としてドメイン名を使用することができます。
2. ドメイン名を使用して証明書を作成する場合は、DNS でサービス IP にドメイン名を対応付ける必要があります。証明書でドメイン名を使用しない場合は、DNS マッピングは不要です。
3. 一時証明書の場合は、CAS の 1 つで一時証明書を生成してから、CAS 間で転送します。
4. CA 署名付き証明書の場合は、ペア内の CAS ごとに CA 署名付き証明書をインポートする必要があります。

（注）　CA 署名付き証明書は、サービス IP、または DNS を介してサービス IP に解決可能なホスト名 / ドメイン名のいずれかに基づいている必要があります。

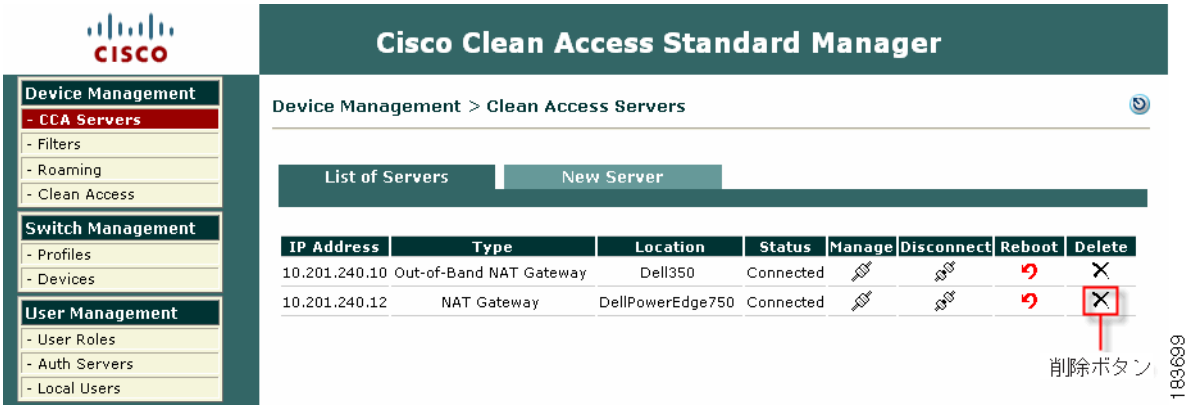
（注）　セッション情報は、フェールオーバー中も CAS によって保持されます。たとえば、ユーザ A がロール B 内のシステムにログインしている場合に、フェールオーバーが発生すると、ユーザ A はログインしたまま、ロール B で指定されたアクセス権が設定されます。CAS が DHCP サーバであり、ユーザに特定の IP アドレスが設定されている場合に、CAS で DHCP フェールオーバーが発生すると、IP アドレスが更新されたときにも、ユーザには同じアドレスが設定されます。「DHCP フェールオーバーの設定」（p.14-22）を参照してください。

（注）　HA CAS ペアの場合、CAS 管理ページまたは CAS ダイレクト アクセス Web コンソールによって HA プライマリ CAS で実行された CAS ネットワークの設定変更もまた、HA セカンダリ CAS ユニットでダイレクト アクセス Web コンソールによって繰り返す必要があります。これらの設定には、SSL 証明書、システム時刻、タイム ゾーン、DNS、またはサービス IP の更新が含まれます。詳細については、「CAS ダイレクト アクセス Web コンソール」（p.13-3）および「ハイ アベイラビリティ設定の変更」（p.14-26）を参照してください。

準備

1. 作業を開始する前に、両方の CAS がインストールされていて、ネットワークを介してアクセスできることを確認します。「初期設定の実行」（p.4-11）を参照してください。
2. CSA が CAM の管理ドメインに追加されている場合は、削除する必要があります。CAS を削除するには、**List of Servers** タブの **Delete** ボタンを使用します。

図 14-3　List of Servers



（注）　Cisco NAC Appliance Web コンソールは、Internet Explorer 6.0 および 7.0 のブラウザをサポートします。

ハートビート UDP インターフェイスの選択および設定

ハートビート UDP インターフェイスが指定されている場合は、ハイ アベイラビリティに関連する UDP ハートビート トラフィックがこのインターフェイスを使用して送信されます。使用されるインターフェイスは、サーバ マシンで使用可能なインターフェイス、および予測される負荷レベルによって決まります。このインターフェイスは専用インターフェイス（eth2）を、専用インターフェイスを使用できない場合は信頼できるインターフェイス（eth0）を使用できます。

一部のサーバでは、追加の NIC カードを搭載して、UDP ハートビート専用のインターフェイス（eth2 など）を提供できます。この場合は、新しいインターフェイスの IP アドレスを設定します（「NIC カードの追加設定」[p.4-22] を参照）。専用インターフェイスを使用する場合は、両方のマシンの専用インターフェイスをクロス ケーブルで接続する必要があります。

一般に、CAS が稼働しているサーバでは、eth0 を信頼ネットワークのインターフェイスとして設定した状態で、使用可能なインターフェイス（eth0 または eth1）を両方とも使用します。一般的な配置では、信頼ネットワークのインターフェイス（eth0）を共有できます。eth0 をハートビート インターフェイスとして使用する場合、シリアル ハートビート接続の設定を追加することを推奨します。

（注）　eth0 を UDP ハートビート インターフェイスとして使用する場合、CAS の管理インターフェイスが他のユーザ トラフィックのある VLAN 上ではなく、自身の VLAN 内にあることを確認します。これは、同じ物理インターフェイス上でフェールオーバー ハートビートを実行するときに、管理トラフィックを分割し保護できる一般的なベスト プラクティスです。

シリアル ポートの HA 接続

CAS ソフトウェアが稼働するマシンごとにシリアル ポートが 2 つある場合は、そのうちの 1 つをシリアル ケーブル接続に使用します。

デフォルトでは、サーバで検出された最初のシリアル接続がコンソール入出力用に設定されます（インストールおよびその他のタイプの管理アクセス用）。

ハイアベイラビリティ モードが選択されている場合、シリアル コンソール ログイン（ttyS0）は自動的にディセーブルになり、HA モードのシリアル ポートが解放されます。ttyS0 をコンソール ログインとして再びイネーブルにするには、**Update** をクリックしてから **Reboot** をクリックし、**Failover > General** タブの **Disable Serial Login** チェックボックスをオフにします。詳細については、「c. HA プライマリ モードの設定および更新」（p.14-11）および「c. HA セカンダリ モードの設定および更新」（p.14-16）を参照してください。

（注）　シリアル コンソール ログインおよび HA シリアル ハートビートを同じシリアル ポートで実現することはできません。

ハイ アベイラビリティの設定

ここでは、ハイ アベイラビリティを設定する 5 つの一般的な手順を示します。

- ステップ 1：プライマリ CAS の設定（p.14-10）
- ステップ 2：HA セカンダリ CAS の設定（p.14-16）
- ステップ 3：CAS の接続および設定の完了（p.14-20）
- ステップ 4：HA CAS ペアのフェールオーバー（p.14-21）
- ステップ 5：DHCP フェールオーバーの設定（p.14-22）

  （DHCP リレー モードやパススルー モードではなく）DHCP サーバとして機能する CAS にハイ アベイラビリティを設定する場合は、CAS 間に SSH トンネルを設定する必要もあります。

（注）「プライマリ / セカンダリ」は HA 用に設定されたときのモードを示します。
「アクティブ / スタンバイ」はサーバの実行時ステータスを示します。

プライマリ CAS の設定

プライマリ CAS を設定する一般的な手順は、次のとおりです。

a. プライマリ CAS のダイレクト アクセス（p.14-10）
b. プライマリのホスト情報の設定（p.14-11）
c. HA プライマリ モードの設定および更新（p.14-11）
d. SSL 証明書の設定（p.14-14）
e. プライマリ サーバのリブート（p.14-15）
f. サービス IP を使用した CAM への CAS の追加（p.14-15）

完了したら、「HA セカンダリ CAS の設定」（p.14-16）に進みます。

a. プライマリ CAS のダイレクト アクセス

CAS にはそれぞれ独自の Web 管理コンソールがあり、CAS の特定の管理設定値を直接設定できます。HA の CAS ペアを設定するには、CAS ダイレクト アクセス Web コンソールを使用する必要があります。

プライマリ CAS のダイレクト アクセス Web 管理コンソールにアクセスする手順は、次のとおりです。

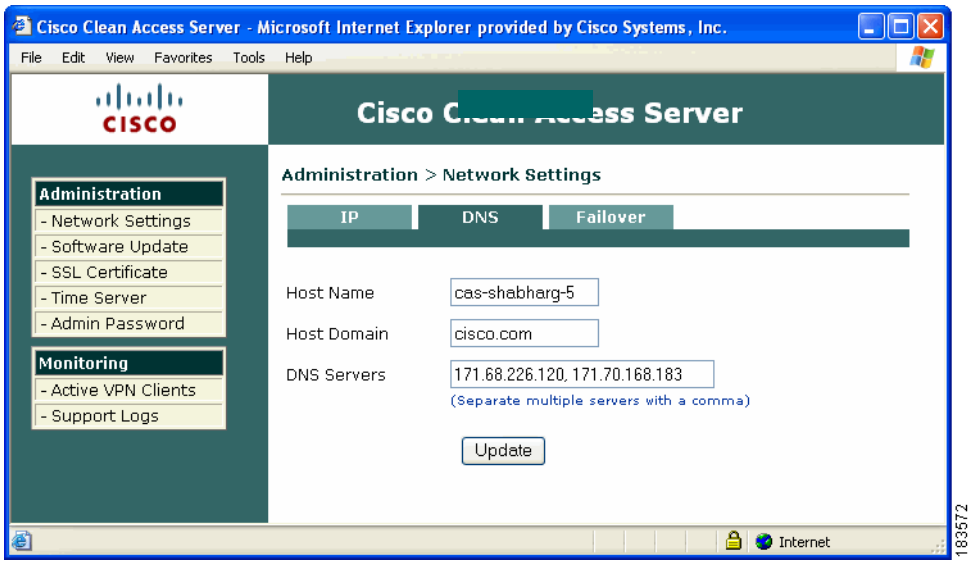
1. Web ブラウザを開き、URL/ アドレス フィールドに CAS の信頼できる（eth0）インターフェイスの IP アドレスを **https://<PrimaryCAS_eth0_IP>/admin** の形式で入力します（例：`https://172.16.1.2/admin`）
2. 一時証明書を受け入れて、ユーザ `admin`（デフォルト パスワードは `cisco123`）としてログインします。

（注）
- 設定フォームに対して値をコピー アンド ペーストするために、各 CAS（プライマリとセカンダリ）の Web コンソールは開いたままにしておくことを推奨します。「a. HA セカンダリ CAS のダイレクト アクセス」（p.14-16）も参照してください。
- セキュリティのために、CAS のデフォルト パスワードを変更することを推奨します。

b. プライマリのホスト情報の設定

3. **Network Settings** リンクをクリックしてから、**DNS** タブをクリックします。
4. **Host Name** フィールドに、プライマリ CAS のホスト名を入力します（caserver10 など）。**Host Domain** フィールドに cisco.com などのドメインが入力されているか確認します。必要に応じて、ドメインを追加し、**Update** をクリックします。

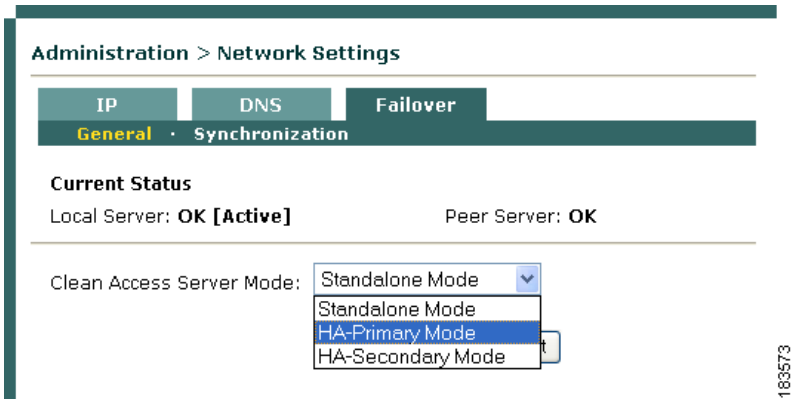
図 14-4　DNS タブ



c. HA プライマリ モードの設定および更新

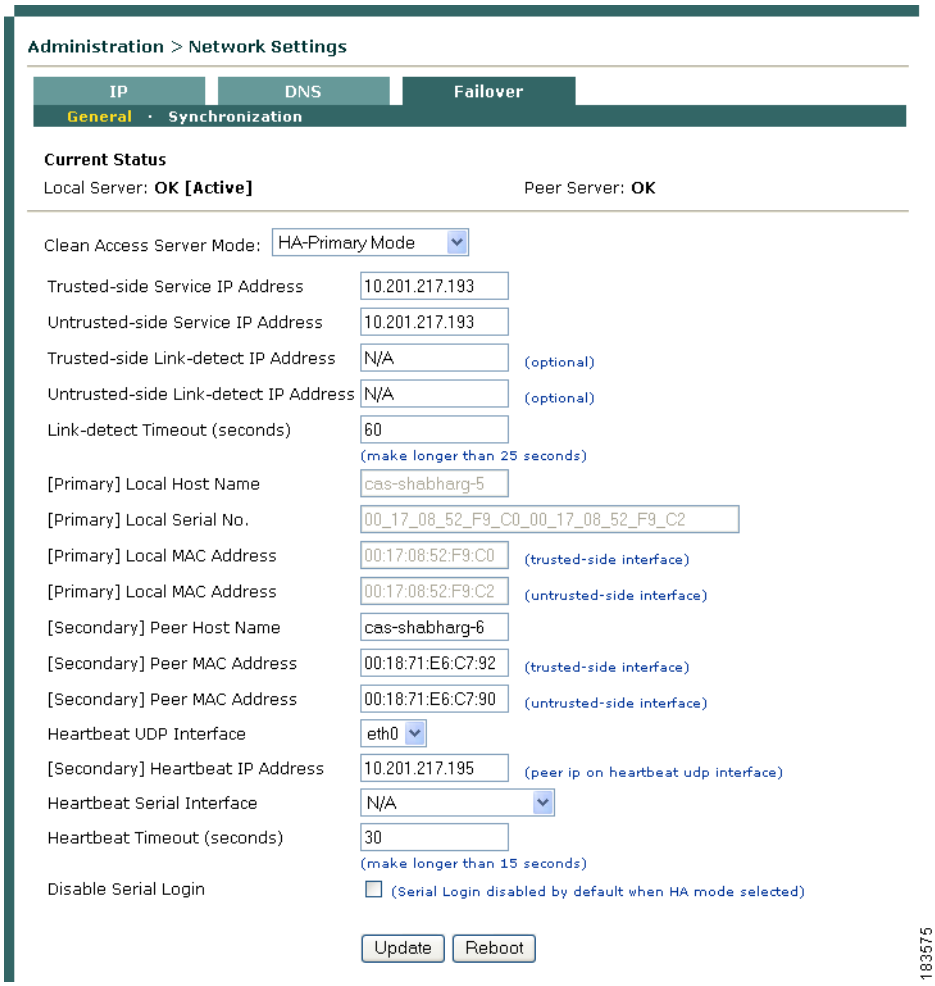
5. **Failover > General** タブをクリックし、**Clean Access Server Mode** ドロップダウン メニューで **HA-Primary Mode** を選択します。

図 14-5　Failover — モード選択



6. 開いている **HA-Primary Mode** フォームの次のフィールドに値を入力します。

図 14-6　Failover — HA-Primary Mode



- **Trusted-side Service IP Address** — 信頼ネットワークからペアをアドレス指定する場合の基準となる共通 IP アドレス（図 14-1 [p.14-2] の例では 172.16.1.4）。
- **Untrusted-side Service IP Address** — 非信頼（管理対象）ネットワークのペアに対する共通アドレス（例では 10.1.51.1）。
- **Trusted-side Link-detect IP Address（任意）** — IP アドレス（アップストリーム ルータなど）をこのフィールドに任意で入力する場合、CAS は信頼できるインターフェイス（eth0）上でこのアドレスに ping を実行しようとします。一般的に、HA プライマリと HA セカンダリ CAS 両方で同じ信頼できる側のリンク検出アドレスを入力しますが、ネットワーク トポロジが異なれば CAS ごとに異なるアドレスを指定できます。
- **Untrusted-side Link-detect IP Address（任意）** — IP アドレス（ダウンストリーム スイッチなど）をこのフィールドに任意で入力する場合、CAS は信頼できないインターフェイス（eth1）上でこのアドレスに ping を実行しようとします。HA プライマリと HA セカンダリ CAS の両方で、同じまたは異なる信頼できない側のリンク検出アドレスを入力できます。
- **Link-detect Timeout (seconds)（任意）** — これは CAS が信頼できる側または信頼できない側のリンク検出 IP アドレスに ping を試行する時間を設定します。26 秒以上の時間を入力します。CAS が指定された時間の間ノードに ping を実行できない場合、ノードは ping で到達できません。

（注）　ハートビート シリアル /UDP 設定のほかに、フェールオーバー イベントとして信頼できる側または信頼できない側のリンク障害に応答するよう CAS を設定することもできます。CAS は、指定された信頼できるまたは信頼できないリンク検出アドレスに ping を試行し、到達したノード数をカウントします。

0- アドレスなし

1- 信頼できる、または信頼できない

2- 信頼できる / 信頼できない両方

スタンバイ CAS がアクティブ CAS よりも多くのノードに到達できた場合、スタンバイ CAS はアクティブ CAS の役割を引き継いでアクティブ CAS になります。両方の CAS が同じ数のアドレス（すべてのアドレスまたはアドレス 1 つのみ）に ping を実行できる場合、どちらの CAS も有利ではないのでフェールオーバーイベントは発生しません。リンク検出をイネーブルにするには、各 CAS で少なくとも 1 つのリンク検出 IP アドレスとリンク検出タイムアウトを入力します。詳細については、「リンクベースのフェールオーバー用外部 IP の選択」（p.14-4）を参照してください。

（注）　CAS は、同じ間隔（約 1 ～ 2 秒ごと）に従ってハートビート接続とリンク検出（任意）を実行します。

- **[Primary] Local Host Name** — HA プライマリ CAS の場合、デフォルトで入力されています。**Administration > Network Settings > DNS | Host Name** の順番で設定されています（例では caserver10）。
- **[Primary] Local Serial No** — HA プライマリ CAS の場合、デフォルトで入力されています。ローカル シリアル番号は、CAM に対してこの CAS を識別します（および eth0/eth1 MAC アドレスで構成されます）。HA-CAS ペアでは、プライマリ CAS のシリアル番号は、CAM データベースのこの CAS 特有の設定情報すべてを関連付けるのに使用するキーです。
- **[Primary] Local MAC Address (trusted-side interface)** — デフォルトで入力されています。HA プライマリ CAS の eth0 インターフェイスの MAC アドレス。
- **[Primary] Local MAC Address (untrusted-side interface)** — デフォルトで入力されています。HA プライマリ CAS の eth1 インターフェイスの MAC アドレス。

（注）

- **[Primary] Local Host Name**、**[Primary] Local Serial No**、および **[Primary] Local MAC Address (trusted/untrusted)** 値は、テキスト ファイルにコピー アンド ペーストできます。これらの値は、あとで HA セカンダリ CAS を設定する場合に必要になります。
- HA セカンダリ CAS 情報を HA プライマリ CAS のフォームに入力するには、HA セカンダリ CAS Web コンソールの対応するフィールドからコピー アンド ペーストします。

- **[Secondary] Peer Host Name** — HA セカンダリ CAS ピアのホスト名（例では caserver12）。ピア マシンの **DNS** タブの **Host Name** 値として、この値を再び指定する必要があります。
- **[Secondary] Peer MAC Address (trusted-side interface)** — これは、HA セカンダリ CAS の信頼できる（eth0）側のピア MAC アドレスです。
- **[Secondary] Peer MAC Address (untrusted-side interface)** — これは、HA セカンダリ CAS の信頼できない（eth1）側のピア MAC アドレスです。

- **Heartbeat UDP Interface** — N/A、eth0、eth2、eth3、eth4 の中から選択できます。専用イーサネット接続を使用できない場合は、CAS を HA モードで設定するときに、シリアル ハートビートとともにハートビート UDP インターフェイスに eth0 を使用することを推奨します。
- **[Secondary] Heartbeat IP Address** — HA セカンダリ CAS の信頼できるインターフェイス（eth0）の IP アドレス（例では、172.16.1.3）。
- **Heartbeat Serial Interface** — シリアル接続の COM ポートを選択します。ハートビート インターフェイスに、シリアル接続と UDP 接続両方を使用することを推奨します。

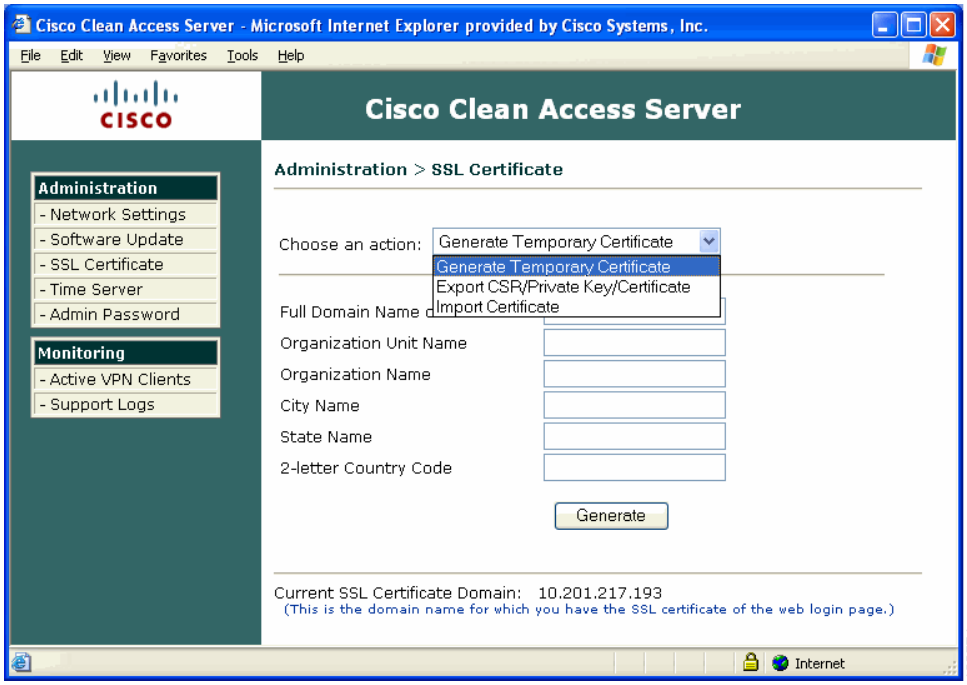
（注）　HA（フェールオーバー）設定を開始する前に、シリアル ケーブルを接続しないでください。必ず設定が完了してから、シリアル ケーブルを接続してください。

- **Heartbeat Timeout (seconds)** — 15 秒よりも大きい値を選択します。
- **Disable Serial Login** — HA モードを選択した場合、デフォルトでシリアル ログインがディセーブルです。シリアル コンソール（ttyS0）を再びイネーブルにするには、この段階で（**Update** をクリックしてから **Reboot** をクリックするまでの間に）**Disable Serial Login** チェックボックスをオフにします。
- **Update** — CAS をリブートしないで HA 設定情報を更新します。
- **Reboot** — HA プライマリ CAS 設定の終了時に CAS をリブートする場合に使用します（この時点では、Reboot をクリック**しないでください**）。

d. SSL 証明書の設定

7. HA プライマリ CAS の SSL 証明書を設定します。**Administration** メニューで、**SSL Certificate** リンクをクリックします。**Generate Temporary Certificate** フォームが表示されます。

図 14-7　Generate Temporary Certificate



8. **SSL Certificate** ページで、使用するのが一時証明書、自己署名付き証明書、または CA 署名付き証明書のいずれであるかに応じて、次の手順の 1 つを実行します。

HA ペアに一時証明書を使用する場合：

a. **Generate Temporary Certificate** フォームに入力し、**Generate** をクリックします。証明書には、HA ペアのサービス IP アドレスを対応付ける必要があります。

b. 一時証明書の生成を終えたら、**Choose an action** ドロップダウン メニューで **Export CSR/Private Key/Certificate** を選択します。

c. **Currently Installed Private Key** の **Export** ボタンをクリックして、SSL 秘密鍵をエクスポートします。この鍵ファイルをディスクに保存します。HA セカンダリ CAS を設定する場合に、あとでこの鍵ファイルをインポートする必要があります。

d. **Currently Installed Certificate** の **Export** ボタンをクリックして、現在の一時証明書をエクスポートします。証明書ファイルをディスクに保存します。あとで、このファイルを HA セカンダリ CAS にインポートする必要があります。

HA ペアに CA 署名付き証明書を使用する場合：

a. **Choose an action** メニューで、**Import Certificate** を選択します。

b. **Certificate File** フィールドの横にある **Browse** ボタンを使用して、証明書ファイルの順番に進みます。

c. **File Type** ドロップダウン メニューで、**CA-signed PEM-encoded X.509 Cert** を選択します。

d. **Upload** をクリックして、証明書をインポートします。あとで、この証明書を HA セカンダリ CAS にインポートする必要があります。

e. **Verify and Install Uploaded Certificates** をクリックします。

f. **Choose an action** リストで **Export CSR/Private Key/Certificate** を選択します。

g. **Export Private Key** ボタンをクリックします。HA セカンダリ CAS を設定する場合に、あとでこの鍵をインポートする必要があります。

詳細については、「CAS SSL 証明書の管理」（p.13-5）を参照してください。

（注）　CA 署名付き証明書は、サービス IP、または DNS を介してサービス IP に解決可能なホスト名 / ドメイン名のいずれかに基づいている必要があります。

e. プライマリ サーバのリブート

9. CAS ダイレクト アクセス インターフェイス（**Network Settings > Failover > General > Reboot** ボタン）または CAM Web コンソール（**Administration > CCA Manager > Network & Failover > Reboot** ボタン）で CAS を**リブート**します。

f. サービス IP を使用した CAM への CAS の追加

10. CAM Web コンソールで、**Device Management > CCA Servers > New Server** に進み、**サーバ IP** アドレスとしてペアのサービス IP（172.16.1.4）を使用して CAS を CAM に追加します。

11. DHCP 設定など、目的のその他の設定値を設定して、CAS の実行時動作を制御します。

12. CAS の信頼できないインターフェイスに接続されたコンピュータから非信頼（管理対象）ネットワークにログインして、設定をテストします。次のステップには、ネットワークへのアクセスに成功した場合のみ進んでください。

HA セカンダリ CAS の設定

HA セカンダリ CAS を設定する一般的な手順は、次のとおりです。

a. HA セカンダリ CAS のダイレクト アクセス
b. HA セカンダリのホスト情報の設定
c. HA セカンダリ モードの設定および更新
d. SSL 証明書の設定
e. HA セカンダリ サーバのリブート

a. HA セカンダリ CAS のダイレクト アクセス

1. Web ブラウザを開き、URL/ アドレス フィールドに HA セカンダリ CAS の信頼できる（eth0）インターフェイスの IP アドレスを **https://<StandbyCAS_eth0_IP>/admin**（例：`https://172.16.1.3/admin`）のように入力して、HA セカンダリ CAS の Web コンソールにアクセスします。
2. ユーザ `admin`（デフォルト パスワードは `cisco123`）としてログインします（ネットワーク環境のセキュリティを高めるために、CAS のデフォルト パスワードを変更することを推奨します）。

（注）
- 設定フォームに対して値をコピー アンド ペーストするために、各 CAS（プライマリとセカンダリ）の Web コンソールは開いたままにしておくことを推奨します。「a. プライマリ CAS のダイレクト アクセス」（p.14-10）も参照してください。
- セキュリティのために、CAS のデフォルト パスワードを変更することを推奨します。

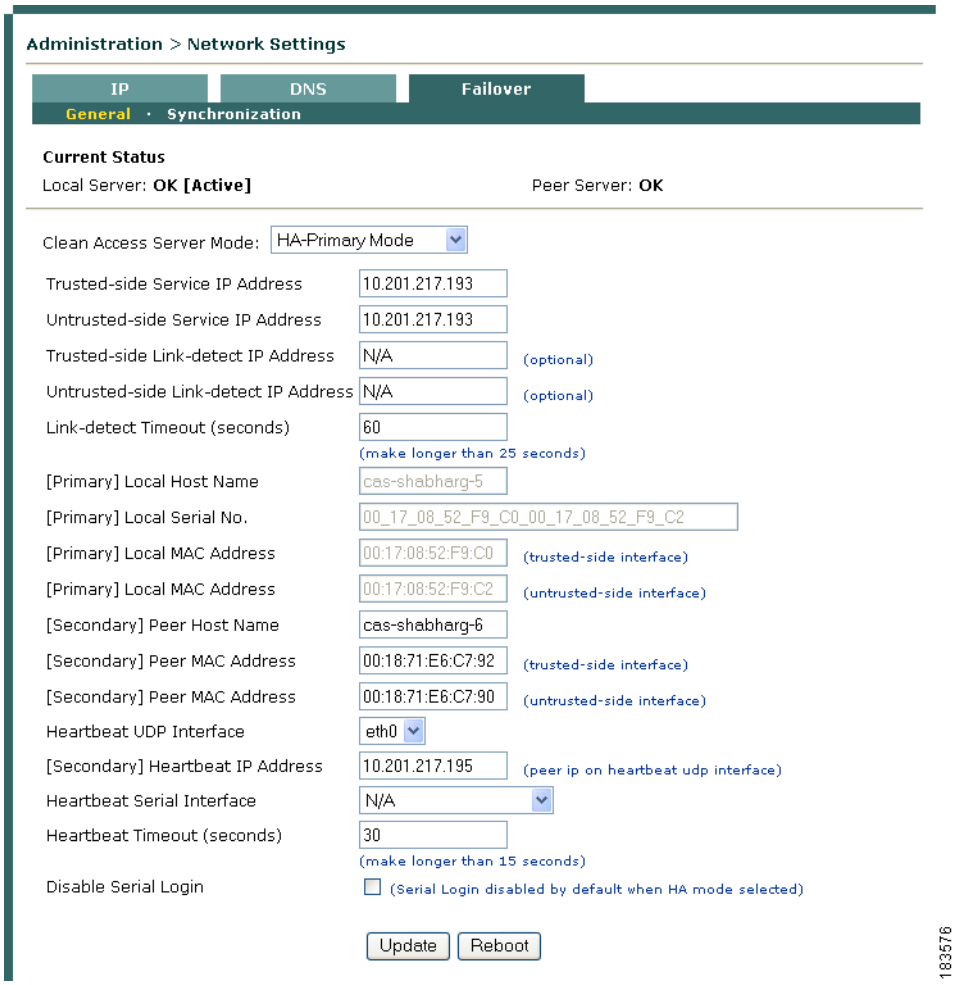
b. HA セカンダリのホスト情報の設定

3. **Network Settings** ページの **DNS** タブを開きます。
4. セカンダリ CAS のホスト名を、`caserver12` のような一意のホスト名に変更します。このタブで指定するドメイン名は、プライマリ CAS に対して指定したドメイン名と同じでなければなりません（「b. プライマリのホスト情報の設定」[p.14-11] を参照）。

c. HA セカンダリ モードの設定および更新

5. **Failover > General** タブをクリックし、**Clean Access Server Mode** ドロップダウン メニューで **HA-Secondary Mode** を選択します。

図 14-8　Failover — HA-Secondary Mode



6. HA-Secondary フォームで、次のフィールドに入力します。
   - **Trusted-side Service IP Address** — *信頼*ネットワークからペアをアドレス指定する場合の基準となる IP アドレス。プライマリ CAS と同じ値を使用します（図 14-1 [p.14-2] の例では 172.16.1.4）。
   - **Untrusted-side Service IP Address** — *非信頼*（管理対象）ネットワークからペアをアドレス指定する場合の基準となる IP アドレス。プライマリ CAS と同じ値を使用します（例では 10.1.51.1）。
   - **Trusted-side Link-detect IP Address（任意）** — IP アドレス（アップストリーム ルータなど）をこのフィールドに任意で入力する場合、CAS はこのアドレスを信頼できるインターフェイス（eth0）に ping を試行します。一般的に、HA プライマリと HA セカンダリ CAS 両方で同じ信頼できる側のリンク検出アドレスを入力しますが、ネットワーク トポロジが異なれば CAS ごとに異なるアドレスを指定できます。
   - **Untrusted-side Link-detect IP Address（任意）** — IP アドレス（ダウンストリーム スイッチなど）をこのフィールドに任意で入力する場合、CAS はこのアドレスを信頼できないインターフェイス（eth1）に ping を試行します。HA プライマリと HA セカンダリ CAS の両方で、同じまたは異なる信頼できない側のリンク検出アドレスを入力できます。
   - **Link-detect Timeout (seconds)（任意）** — これは CAS が信頼できる側または信頼できない側のリンク検出アドレス IP アドレスに ping を試行する時間を設定します。26 秒以上の時間を入力します。CAS が指定された時間の間ノードに ping を実行できない場合、ノードは ping で到達できません。

（注）　詳細については、「リンクベースのフェールオーバー用外部 IP の選択」（p.14-4）を参照してください。

- **[Secondary] Local Host Name** — HA セカンダリ CAS の場合、デフォルトで入力されています（例では、caserver12）。
- **[Secondary] Local Serial No** — HA セカンダリ CAS の場合、デフォルトで入力されています。
- **[Secondary] Local MAC Address (trusted-side interface)** — デフォルトで入力されています。HA セカンダリ CAS の eth0 インターフェイスの MAC アドレス。
- **[Secondary] Local MAC Address (untrusted-side interface)** — デフォルトで入力されています。HA セカンダリ CAS の eth1 インターフェイスの MAC アドレス。

（注）
- **[Secondary] Local Host Name**、**[Secondary] Local Serial No**、および **[Secondary] Local MAC Address (trusted/untrusted)** 値は、テキスト ファイルにコピー アンド ペーストできます。これらの値は、HA プライマリ CAS を設定する場合に必要です。
- HA プライマリ CAS 情報を HA セカンダリ CAS のフォームに入力するには、HA プライマリ CAS Web コンソールの対応するフィールドからコピー アンド ペーストします。

- **[Primary] Peer Host Name** — HA プライマリ CAS のホスト名。プライマリの **DNS** タブの **Host Name** フィールドで指定した値と同じです（例では、caserver10）。
- **[Primary] Peer Serial No** — HA プライマリ CAS のシリアル番号。HA セカンダリ CAS がアクティブになると、CAS 設定情報にアクセスするため、HA プライマリ CAS のシリアル番号を使用して CAM に対して識別する必要があります。
- **[Primary] Peer MAC Address (trusted-side interface)** — HA プライマリ CAS の信頼できる（eth0）側のピア MAC アドレス。
- **[Primary] Peer MAC Address (untrusted-side interface)** — HA プライマリ CAS の信頼できない（eth1）側のピア MAC アドレス。
- **Heartbeat UDP Interface** — N/A、eth0、eth2、eth3、eth4 の中から選択できます。専用イーサネット接続を使用できない場合は、CAS を HA モードで設定するときに、ハートビート UDP インターフェイスに eth0 を使用することを推奨します。
- **[Primary] Heartbeat IP Address** — HA プライマリ CAS の信頼できるインターフェイス（eth0）側の IP アドレス（例では、172.16.1.2）。
- **Heartbeat Serial Interface** — シリアル接続の COM ポートを選択します。ハートビート インターフェイスに、シリアル接続と UDP 接続両方を使用することを推奨します。
- **Heartbeat Timeout (seconds)** — 15 秒よりも大きい値を選択します。
- **Disable Serial Login** — HA モードを選択した場合、デフォルトでシリアル ログインがディセーブルです。シリアル コンソール（ttyS0）を再びイネーブルにするには、この段階で（**Update** をクリックしてから **Reboot** をクリックするまでの間に）**Disable Serial Login** チェックボックスをオフにします。
- **Update** — CAS をリブートしないで HA 設定情報を更新します。

d. SSL 証明書の設定

7. HA セカンダリ CAS の SSL 証明書を設定します。**SSL Certificate** リンクをクリックします。**SSL Certificate** ページで、次のいずれかの手順を実行します。

HA ペアに一時証明書を使用する場合：

a. **Choose an action** メニューで、**Import Certificate** を選択します。

b. **Certificate File** フィールドの横にある **Browse** ボタンを使用して、プライマリ CAS からエクスポートした一時証明書ファイルに対応付けられた秘密鍵を検索します。

c. ファイル タイプとして **Private Key** を選択します。

d. **Upload** をクリックして、秘密鍵をアップロードします。

e. **Choose an action** メニューで、**Import Certificate** を選択し、秘密鍵に対応付けられた一時証明書ファイルを検索します。

f. ファイル タイプとして **CA-signed PEM-encoded X.509 Cert** を選択します。

g. **Upload** をクリックして、一時証明書をアップロードします。

h. **Verify and Install Uploaded Certificates** をクリックします。

HA ペアに CA 署名付き証明書を使用する場合：

a. **Choose an action** メニューで、**Import Certificate** を選択します。

b. **Certificate File** フィールドの横にある **Browse** ボタンを使用して、プライマリ CAS からエクスポートされた秘密鍵ファイルを選択します。

c. ファイル タイプとして **Private Key** を選択します。

d. **Upload** をクリックして、秘密鍵をアップロードします。

e. **Choose an action** メニューで、**Import Certificate** を選択し、プライマリ CAS にインポートした同じ CA 署名付き証明書を検索します。

f. ファイル タイプとして **CA-signed PEM-encoded X.509 Cert** を選択します。

g. **Upload** をクリックして、CA 署名付き証明書をアップロードします。

h. **Verify and Install Uploaded Certificates** をクリックします。

（注）　場合によっては、CA ルート証明書または中間ルート証明書をインポートする必要があります。その場合は、ファイルをインポートするときに **Root/Intermediate Certificate** ファイル タイプを選択します。詳細については、「CAS SSL 証明書の管理」（p.13-5）を参照してください。

e. HA セカンダリ サーバのリブート

8. CAS ダイレクト アクセス インターフェイス（**Network Settings > Failover > General**）で、**Reboot** ボタンをクリックして CAS をリブートします。

CAS の接続および設定の完了

1. HA プライマリ CAS マシンをシャットダウンし、`caserver10` および `caserver12` マシンをシリアル ヌル モデム ケーブルで接続するか（空いているシリアル ポートを接続）、またはクロス ケーブルで接続します（フェールオーバー用の eth2 など、3 番めのイーサネット インターフェイスを使用している場合に、イーサネット ポートを接続）。
2. CAM 管理コンソールを開きます。
3. **Device Management > CCA Servers > List of Servers の順番に進みます。**ハイ アベイラビリティ ペアのアクティブ CAS が、ペアに対応するサービス IP の 横のカッコ内に表示されます（図 14-9 を参照）。HA プライマリ CAS はオフになっているので、**List of Servers** に HA セカンダリ CAS の IP アドレスが表示され、ステータスが Connected になります。

図 14-9　HA ペアのアクティブ CAS

4. ペアの **Manage** ボタンをクリックします。HA セカンダリ CAS（現在はアクティブ CAS）の管理ページが表示されます。
5. HA プライマリ CAS の DHCP 設定と一致するように、DHCP サーバの設定値を設定します。HA CAS ペアが DHCP サーバとして機能している場合は、「DHCP フェールオーバーの設定」（p.14-22）のステップに従って、ピア CAS が DHCP 情報の同期を維持できるようにします。
6. CAS の信頼できないインターフェイスに接続されたクライアント コンピュータから、非信頼（管理対象）ネットワークに許可ユーザとしてログオンして、設定をテストします。ログオンに成功した場合は、ログオンしたまま次のステップに進みます。

HA CAS ペアのフェールオーバー

（注）　DHCP サーバの HA CAS ペアの場合、最初に「DHCP フェールオーバーの設定」（p.14-22）のステップを実行します。

HA システムをテストするには、次のステップに使用します。

1. HA プライマリ CAS マシンをオンにします。CAS が完全に起動し、機能していることを確認してから、先に進みます。
2. クライアント コンピュータからユーザ セッションをログオフし、非信頼（管理対象）ネットワークにユーザとして再度ログオンします。
3. HA セカンダリ CAS マシンはアクティブで、ユーザにサービスを提供します。
4. HA セカンダリ CAS マシンをシャットダウンします。

（注）　フェールオーバーをテストするマシンには、代わりに「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も、**service perfigo stop** と **service perfigo start** の使用を推奨します。Virtual Gateway CAS の場合、代わりに **service perfigo maintenance** を使用して CAS をメンテナンス モードにし、管理 VLAN へのネットワーク接続を可能にします。詳細は、「CLI の使用法」（p.4-20）を参照してください。

5. 約 15 秒後に HA プライマリ CAS がアクティブ サーバになってサービスを提供し、ブラウズを継続できるようになります。
6. HA セカンダリ CAS マシン（スタンバイ サーバ）をオンにします。
7. CAM のイベント ログを調べます。CAS のステータスが正しく記録されている必要があります（例：`[caserver10 is dead. caserver12 is up]`）。
8. これで、ハイ アベイラビリティ設定のテストは完了です。

DHCP フェールオーバーの設定

DHCP サーバ モードで動作するハイアベイラビリティ ピア CAS は、アクティブ リースやリース期間など DHCP アクティビティに関する情報を、セキュアな SSH 接続（トンネル）を介して交換します。（DHCP リレー モードやパススルー モードでなく）DHCP サーバとして機能する CAS にハイアベイラビリティを設定する場合は、DHCP フェールオーバーを設定する必要もあります。HA プライマリと HA セカンダリの両方の CAS に、サーバの鍵、およびサーバにアクセスしているアカウントの鍵が必要です。したがって、合計 4 つの鍵を交換する必要があります。プライマリ CAS とセカンダリ CAS 間で DHCP フェールオーバー情報を転送するために必要なセキュリティ鍵の生成や交換を行うために、以下で説明するインターフェイスが用意されています。

（注）　DHCP サーバおよび CAS フェールオーバーを設定したら、プライマリ CAS とセカンダリ CAS をフェールオーバーして、各サーバに /var/state/dhcp ディレクトリを作成する必要があります。DHCP フェールオーバーを正しく機能させるには、/var/state/dhcp ディレクトリが両方のサーバに存在しなければなりません。「CAS の接続および設定の完了」（p.14-20）および「HA CAS ペアのフェールオーバー」（p.14-21）を参照してください。

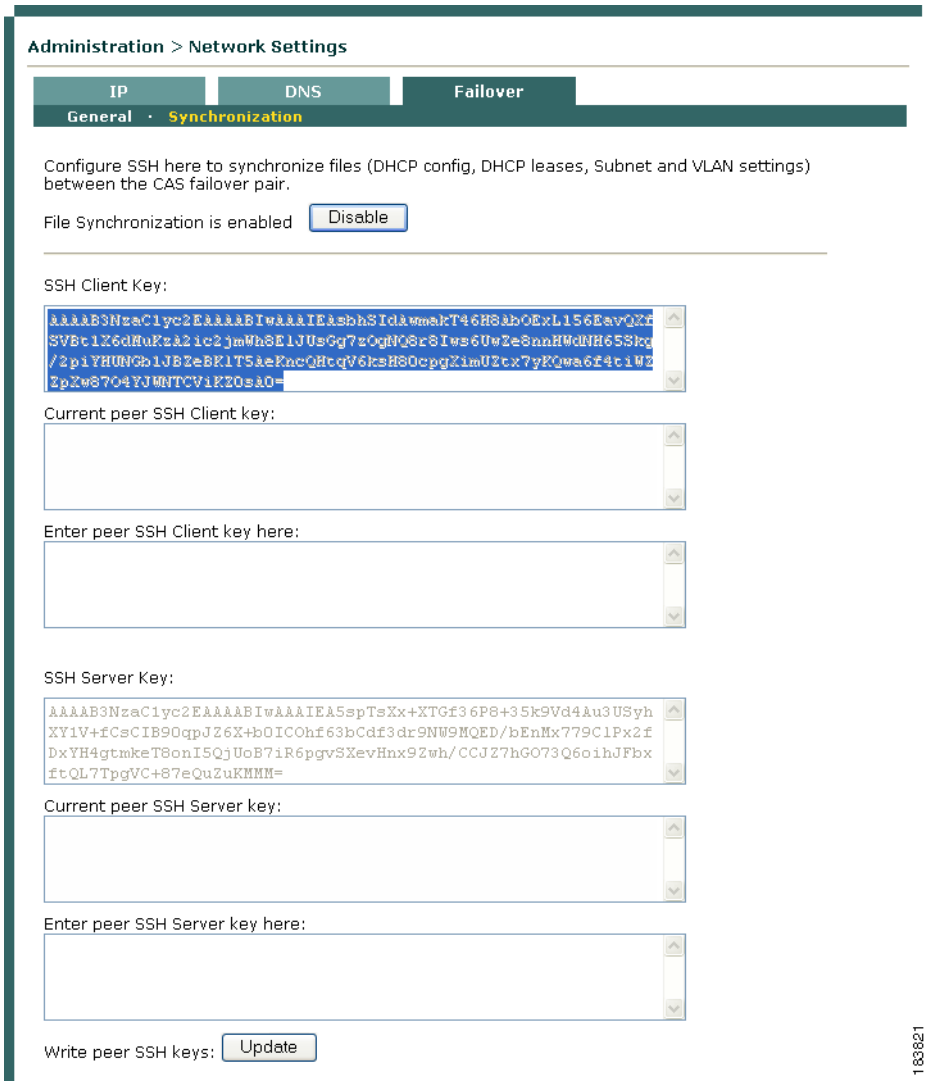
DHCP フェールオーバーの設定手順

手順を開始するには、プライマリ CAS およびセカンダリ CAS の管理コンソールを開きます（`https://<Server IP Address>/admin`）。このプロセス中にブラウザが 2 つ開きます。

ステップ 1　プライマリ CAS の管理コンソールに移動して、**Network Settings > Failover > Synchronization** タブをクリックします。

ステップ 2　**Enable** ボタンをクリックして、プライマリ CAS で DHCP フェールオーバーをイネーブルにします（このボタンが **Disable** に切り替わります）。

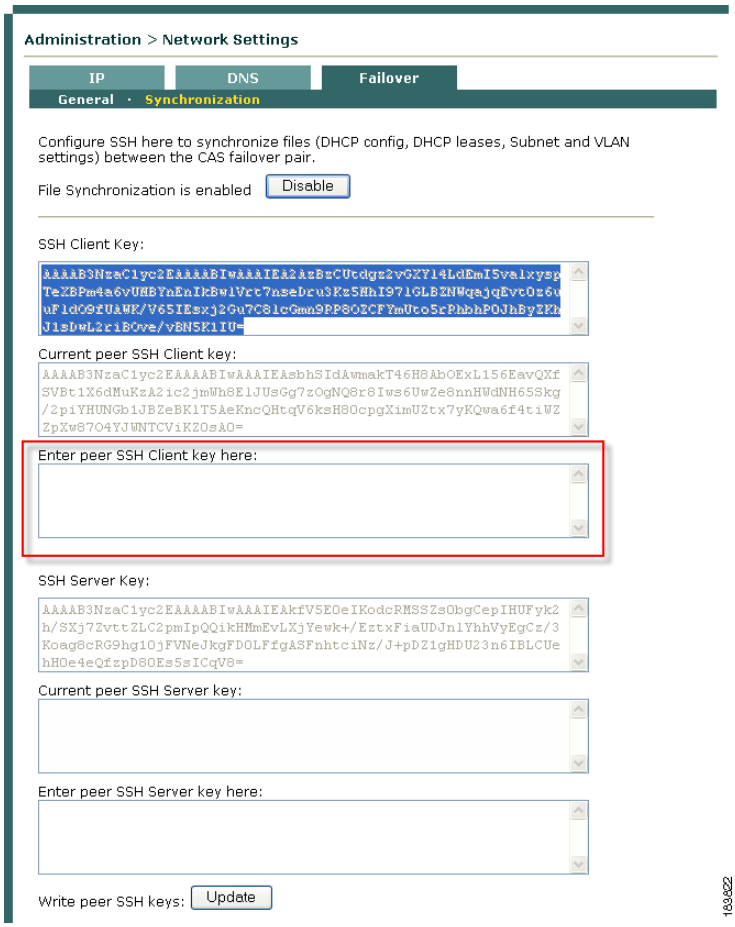
図 14-10　DHCP フェールオーバーのイネーブル化 — プライマリ CAS



ステップ 3　プライマリ CAS の **SSH Client Key** フィールドの値をコピーします。

ステップ 4　セカンダリ CAS の管理コンソールに移動して、**Network Settings > Failover > Synchronization** タブをクリックします（図 14-11 を参照）。

図 14-11　DHCP フェールオーバーのイネーブル化 — セカンダリ CAS



ステップ 5　**Enable** ボタンをクリックして、セカンダリ CAS で DHCP フェールオーバーをイネーブルにします（このボタンが **Disable** に切り替わります）。

ステップ 6　プライマリ CAS でコピーした SSH Client Key を、**Enter peer SSH Client key here** フィールドに貼り付けます。

ステップ 7　セカンダリ CAS の管理コンソールのまま、**SSH Client Key** フィールドの値をコピーします。

ステップ 8　プライマリ CAS の管理コンソールに戻って、セカンダリ CAS の SSH Client Key を **Enter peer SSH Client key here:** フィールドに貼り付けます（図 14-10 を参照）。

ステップ 9　プライマリ CAS の管理コンソールでのまま、**SSH Server Key** フィールドの値をコピーします。

ステップ 10　セカンダリ CAS の管理コンソールに戻って、プライマリ CAS の SSH Server Key を **Enter peer SSH Server key here:** フィールドに貼り付けます。

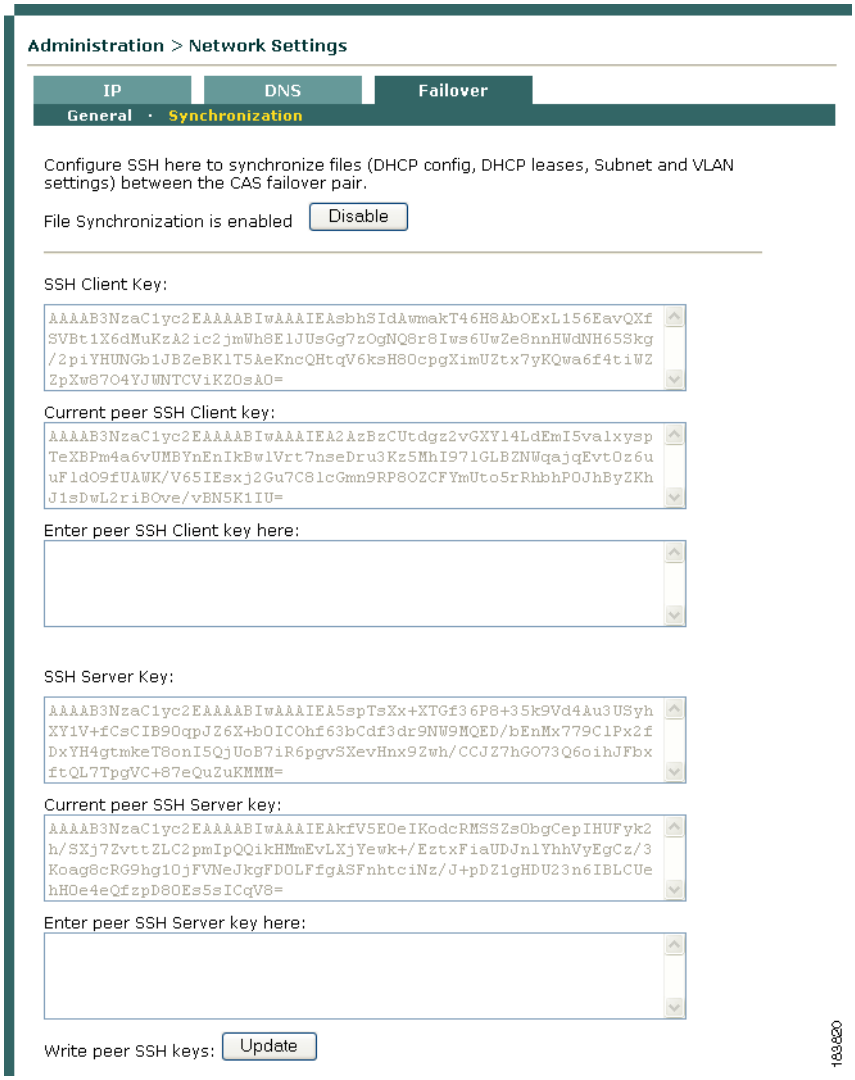
ステップ 11　セカンダリ CAS の管理コンソールのまま、**SSH Server key** フィールドの値をコピーします。

ステップ 12　**Update** ボタンをクリックして、セカンダリ CAS に ピア SSH 鍵を書き込みます。

ステップ 13　プライマリ CAS の管理コンソールに戻って、セカンダリ CAS の SSH Server Key を **Enter peer SSH Server key here:** フィールドに貼り付けます。

ステップ 14　**Update** ボタンをクリックして、プライマリ CAS に ピア SSH 鍵を書き込みます。これで、DHCP フェールオーバー設定は完了です。

図 14-12　DHCP フェールオーバー — 設定の完了



ハイ アベイラビリティ設定の変更

ここでは、既存のハイ アベイラビリティ CAS ペアの設定を変更する手順について説明します。ハイアベイラビリティ ペアのサービス IP、サブネット マスク、またはデフォルト ゲートウェイを変更するには、CAM を更新して、CAS をリブートする必要があります。

また、サービス IP アドレスが変更されていて、CAS の SSL 証明書がこのサービス IP に基づいている場合は、ハイアベイラビリティ ペアの CAS ごとに新しい証明書を生成して、インポートする必要があります。SSL 証明書が CAS のホスト名に基づいている場合は、新しい証明書を生成する必要はありません。ただし、DNS サーバのホスト名の IP アドレスを変更する必要があります。

一般的な手順は次のとおりです。

1. CAM の CAS 設定を最初に更新します（ただしリブートしません）。
2. プライマリ CAS のダイレクト アクセス Web コンソールで HA 設定を更新し、プライマリ CAS をリブートします。
3. プライマリ CAS のリブート中に、CAM の List of Servers でセカンダリ CAS がアクティブになるまで待機します。
4. セカンダリ CAS にステップ 1 ～ 3 を繰り返して、セカンダリ CAS をリブートします。
5. セカンダリ CAS のリブート中に、CAM でプライマリ CAS がアクティブになり、新しい設定が表示されます。

HA-CAS の IP 設定の変更手順

1. CAM Web 管理コンソールで、**Device Management > CCA Servers** の順番に進みます。
2. CAS の **Manage** ボタンをクリックします。
3. **Network** タブをクリックします。
4. 信頼できる / 信頼できないインターフェイスの **IP Address**、**Subnet Mask**、または **Default Gateway** 設定を必要に応じて変更します。
5. **Update** ボタンのみをクリックします。

注意　この段階では、**Reboot** ボタンをクリックしないでください。

6. CAS の SSL 証明書が以前の IP アドレスに基づいている場合は、新規に設定された IP アドレスに基づく新しい SSL 証明書を生成する必要があります。この処理は、**Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs** で行うことができます。詳細は、「CAS SSL 証明書の管理」（p.13-5）を参照してください。
7. SSL 証明書が CAS のホスト名に基づいている場合は、新しい証明書を生成する必要はありません。ただし、DNS サーバのホスト名の IP アドレスを変更する必要があります。
8. 次に、**プライマリ** CAS のダイレクト アクセス Web 管理コンソールを開きます。次のコマンドを実行します。

   ```
   https://<Primary_CAS_eth0_IPaddress>/admin
   ```

9. プライマリ CAS の IP フォームに、**Device Management > CCA Servers > Manage [CAS_IP] > Network > IP** の CAS Web コンソールの変更内容が反映されます。
10. CAS ダイレクト アクセス コンソールで、**Network > Failover> General** タブをクリックします。
11. 必要に応じて、以下を変更します。
    - Trusted-side Service IP Address

- Untrusted-side Service IP Address
- [Secondary] Peer Host Name
- [Secondary] Peer MAC Address (trusted-side interface)
- [Secondary] Peer MAC Address (untrusted-side interface)
- [Secondary] Heartbeat IP Address

12. **Update** ボタンをクリックしてから、**Reboot** ボタンをクリックします。
13. CAM Web 管理コンソールから **Device Management > CCA Servers** の順番に進み、セカンダリ CAS がアクティブになるまで待機します（この処理に数分間かかることがあります）。ハイ アベイラビリティ ペアのアクティブ CAS が、ペアに対応するサービス IP の横のカッコ内に表示されます（図 14-9 [p.14-20] を参照）。**List of Servers** にセカンダリ CAS の IP アドレスが表示され、ステータスが Connected になります。
14. セカンダリ CAS の IP アドレスが **List of Servers** のカッコ内に表示されて、CAS のステータスが Connected になったら、セカンダリ CAS にステップ 1 ～ 11 を繰り返します。
15. 変更して、セカンダリ CAS をリブートすると、List of Servers にプライマリ CAS がアクティブ サーバとして表示され、新しい IP 情報がすべて表示されます。

既存のフェールオーバー ペアのアップグレード

新しい CCA リリースに対応する既存のフェールオーバー ペアの更新手順については、『*Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.1(1)*』の「Upgrading High Availability Pairs」を参照してください。

HA の便利な CLI コマンド

CAS の HA を把握するには、次のディレクトリが役に立ちます。

- /etc/ha.d/perfigo.conf
- /etc/ha.d/ha.cf

HA CAS でのプライマリ / セカンダリ設定ステータスの確認方法

/etc/ha.d/perfigo.conf ファイルでは、including ホスト名（cas1）、ピア ホスト名（cas2）、HA モード（プライマリ）、ハートビート インターフェイス（UDP/ シリアル）、およびリンク検出インターフェイス情報を含めた、HA-CAS に関するさまざまな設定情報を示します。

```
[root@cas1 ha.d]# more perfigo.conf
#linux-ha
#Mon Aug 28 18:50:15 PDT 2006
WIRELESS_SERVICEIP=10.10.20.4
PING_DEAD=25
HOSTNAME=cas1
HA_DEAD=15
PEERGUSSK=
PEERMAC=00\:16\:35\:BF\:FE\:67
PEERHOSTNAME=cas2
TRUSTED_PINGNODE=10.10.40.100
UNTRUSTED_PINGNODE=10.10.20.100
HAMODE=PRIMARY
PEERMAC0=00\:16\:35\:BF\:FE\:66
PEERHOSTIP=10.10.50.2
HA_FAILBACK=off
HA_UDP=eth2
WIRED_SERVICEIP=10.10.20.4
HA_SERIAL=ttyS0
```

/etc/ha.d/ha.cf ファイルでは、ハートビート接続とリンクベースの接続に関する追加情報を示します。

```
[root@cas1 ha.d]# more ha.cf
# Generated by make-hacf-ss.pl
udpport         694
ucast           eth2 10.10.50.2
baud            19200
serial          /dev/ttyS0
keepalive       2
deadtime        15
deadping        25
auto_failback   off
apiauth         default uid=root
respawn         hacluster /usr/lib64/heartbeat/ipfail
ping            10.10.20.100
ping            10.10.40.100

log_badpack     false
warntime        10
debug           0
debugfile       /var/log/ha-debug
logfile         /var/log/ha-log
watchdog        /dev/watchdog
node            cas1
node            cas2
```

HA CAS でのアクティブ / スタンバイの実行時ステータスの確認方法

次に、CLI を使用して、HA ペアの各 CAS の実行時ステータス（アクティブまたはスタンバイ）を判断する例を示します。通常、最後のアップグレードの /store ディレクトリから fostate.sh コマンド（たとえば、**/store/cca_upgrade-4.x.x**）を検索できます。

1. /store/cca_upgrade-4.x.x に Cd を実行し、最初の CAS で fostate.sh スクリプトを実行します。

```
[root@cas1 cca_upgrade-4.x.x]# ./fostate.sh
My node is active, peer node is standby
[root@cas1 cca_upgrade-4.x.x]#
```

この CAS は、HA ペアのアクティブ CAS です。

2. 2 番めの CAS で fostate.sh スクリプトを実行します。

```
[root@cas2 cca_upgrade-4.x.x]# ./fostate.sh
My node is standby, peer node is active
[root@cas2 cca_upgrade-4.x.x]#
```

この CAS は、HA ペアのスタンバイ CAS です。

ネットワークへのハイ アベイラビリティ Cisco NAC アプライアンスの追加

次の図は、HA-CAM および HA-CAS をコア ディストリビューション アクセス ネットワーク（ディストリビューション レイヤとアクセス レイヤに Catalyst 6500 を装備）の例に追加する方法を示します。

図 14-13 に、Cisco NAC アプライアンスを装備していないネットワーク トポロジを示します。コア レイヤおよびディストリビューション レイヤは Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）を実行し、アクセス スイッチはディストリビューション スイッチにデュアル ホームしています。

図 14-13　Cisco NAC アプライアンスを追加する前のコア ディストリビューション アクセス ネットワーク例

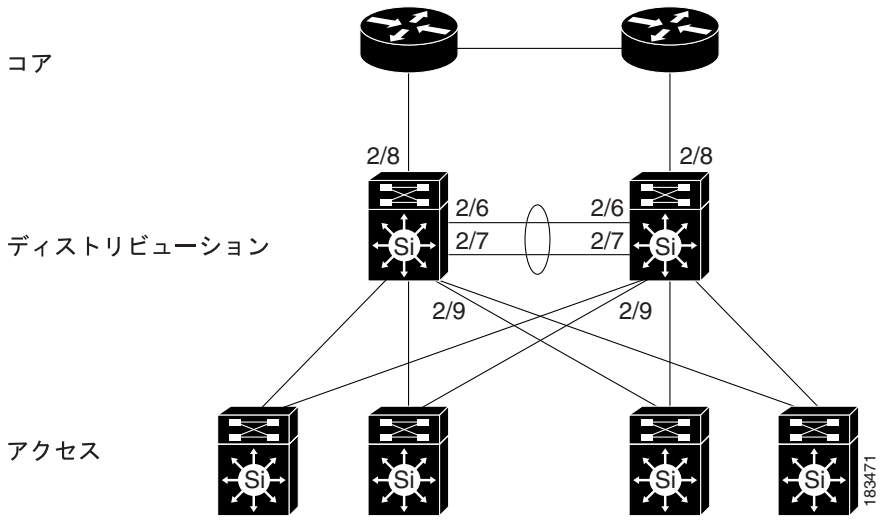


図 14-14 に、HA-CAM をコア ディストリビューション アクセス ネットワークに追加する方法を示します。この例では、HA ハートビート接続は シリアル インターフェイスと eth1 インターフェイス両方で設定されます。

図 14-14　ネットワークへの HA CAM の追加

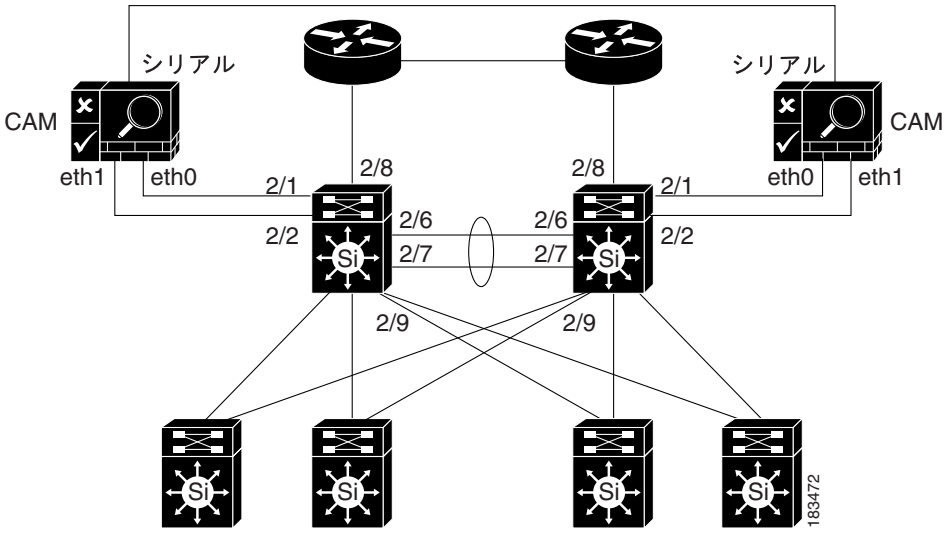


図 14-15 に、HA-CAS をコア ディストリビューション アクセス ネットワークに追加する方法を示します。この例では、CAS は中央配置の L2 OOB バーチャル ゲートウェイとして設定されます。t.HA ハートビート接続は シリアル インターフェイスと専用 eth2 インターフェイス両方で設定されます。リンク障害ベースのフェールオーバー接続もまた、eth0 インターフェイスと eth1 インターフェイスで設定されます。

図 14-15　ネットワークへの HA CAS の追加