APPENDIX **B**

Unified Communications Manager の設定

（注） Service Monitor でサポートする Cisco Unified Communications Manager のバージョンについては、『*Cisco Unified Service Monitor 8.5 Compatibility Matrix*』を参照してください。

Service Monitor が Unified Communications Manager のデータを収集して分析するには、次の各項の説明に従って、まず Unified Communications Manager システムを設定する必要があります。

サポートされているバージョンの Unified Communications Manager の設定作業

Service Monitor が CVTQ データを Unified Communications Manager から取得するには、まず、次のシステムにログインして設定作業を行う必要があります。

- Unified Communications Manager：Unified Communications Manager Administration および Unified Communications Manager Serviceability にアクセスするため。
- Unified Communications Manager がインストールされているサーバ（Unified Communications Manager 4.x を使用する場合）：Microsoft SQL Server にアクセスするため。

H.323 および SIP ゲートウェイで Voice Activity Detection（VAD; 音声アクティビティ検出）がイネーブルになっている場合は、MOS を適切に計算し、CDR に正しく報告するため、これらのゲートウェイで追加設定を行う必要があります。

ご使用の Unified Communications Manager のバージョンに応じて、この項で記載されている作業の一部を実行する必要があります。Unified Communications Manager のバージョンによって作業が多少異なる場合は、バージョン固有の手順を示してあります。

表 B-1 に、Service Monitor によって CVTQ データを Unified Communications Manager から取得する場合について、Unified Communications Manager のバージョン別に実行する必要のある設定作業を示します。

表 B-1　Unified Communications Manager および Microsoft SQL Server の作業

設定作業	Unified Communications Manager のバージョン別の設定作業の必要性	
	5.x 以降[1]	4.x
「Unified Communications Manager のサービス パラメータの設定」（P.B-2）	X	X
「Unified Communications Manager のエンタープライズ パラメータの設定」（P.B-4）	X	X
「ビリング サーバとしての Service Monitor の Unified Communications Manager 5.x 以降への追加」（P.B-4）	X	—
「Unified Communications Manager 5.x 以降での AXL Web Service のアクティブ化」（P.B-5）	X	—
「Unified Communications Manager 4.x システムのデータベース認証の設定」（P.B-7）	—	X
「音声ゲートウェイの設定」（P.B-12）	X	X

1. Service Monitor でサポートするソフトウェアのバージョンについては、「サポートされているデータ ソース ソフトウェア バージョン」（P.3-7）を参照してください。

注意　データベース認証を説明のとおりに設定できない場合、Unified Communications Manager 4.x システムで CDR の書き込みができない可能性があります。

Unified Communications Manager の設定

ここでは、次の内容について説明します。

- 「Unified Communications Manager のサービス パラメータの設定」（P.B-2）
- 「Unified Communications Manager のエンタープライズ パラメータの設定」（P.B-4）
- 「ビリング サーバとしての Service Monitor の Unified Communications Manager 5.x 以降への追加」（P.B-4）
- 「Unified Communications Manager 5.x 以降での AXL Web Service のアクティブ化」（P.B-5）
- 「Unified Communications Manager 5.x 以降での smuser のパスワード変更」（P.B-6）

Unified Communications Manager 4.x では、必ず 「Unified Communications Manager 4.x システムのデータベース認証の設定」（P.B-7）の作業も実行してください。

Unified Communications Manager のサービス パラメータの設定

（注）　サービス パラメータは、クラスタ内の Unified Communications Manager ごとに設定します。

ステップ 1　Unified Communications Manager Administration にログインします。

ステップ 2　次の手順で、[Service Parameters Configuration] ページに進みます。

- Unified Communications Manager 4.x では、[Service] > [Service Parameters] を選択します。
- Unified Communications Manager 5.x 以降では、[System] > [Service Parameters] を選択します。

（注）　サポートされる Unified Communications Manager ソフトウェアのバージョンについては、「サポートされているデータ ソース ソフトウェア バージョン」（P.3-7）を参照してください。

[Service Parameters Configuration] ページが表示されます。

ステップ 3　次の手順で、サーバとサービスを選択します。

a.　Unified Communications Manager サーバの名前を選択します。これは、Service Monitor によるデータ収集の対象となる Unified Communications Manager です。

b.　Unified Communications Manager サービスを選択します。

ステップ 4　次のパラメータを設定します。

- Unified Communications Manager バージョン 4.x の場合
  - [CDR Enabled Flag] : [System] までスクロール ダウンします。[True] に設定します。
  - [Call Diagnostics Enabled] : [Clusterwide Parameters (Device - General)] までスクロール ダウンします。[True] に設定します。

（注）　パブリッシャと各サブスクライバで [Call Diagnostics Enabled] が true に設定されているかどうか確認することを推奨します。

- Unified Communications Manager 5.x 以降の場合
  - [CDR Enabled Flag] : [System] までスクロール ダウンします。[True] に設定します。
  - [Call Diagnostics Enabled] : [Clusterwide Parameters (Device - General)] までスクロール ダウンします。[Enable Only When CDR Enabled Flag is True] に設定します。

（注）　パブリッシャと各サブスクライバで [Call Diagnostics Enabled] が [Enable Only When CDR Enable Flag is True] に設定されているかどうか確認することを推奨します。

ステップ 5　[Update] をクリックします。

注意　[CDR Log Calls With Zero Duration Flag] サービス パラメータをイネーブルにしないでください。イネーブルにすると、Service Monitor（および CDR の分析と報告）に悪影響が生じる可能性があります。多数の継続時間ゼロのコール レコードの処理にリソースが消費されるため、Service Monitor が処理できる継続時間がゼロでないコールの数が減る可能性があります。

Unified Communications Manager のエンタープライズ パラメータの設定

この手順は、Unified Communications Manager バージョン 4.x 以降で実行します。

ステップ 1　Unified Communications Manager Administration にログインします。

ステップ 2　[System] > [Enterprise Parameters] を選択します。[Enterprise Parameters Configuration] ページが表示されます。

ステップ 3　[CDR Parameters] にスクロール ダウンし、次のパラメータを設定します。

- Unified Communications Manager 4.x の場合
  - [CDR File Time Interval (min)] : **1** を設定します。
  - [CDR Format] : [CDRs will be inserted into database] を選択します。
- Unified Communications Manager 5.x 以降の場合は、[CDR File Time Interval (min)] を **1** に設定します。

ステップ 4　[Cluster ID] までスクロールします。クラスタ ID がすでに存在する Service Monitor である場合は（「データ ソース クレデンシャルの概要と設定」（P.3-2）を参照）、クラスタ ID を変更します。

（注）　Service Monitor に追加する各クラスタには、一意のクラスタ ID が必要です。

ステップ 5　[Update] をクリックします。

ビリング サーバとしての Service Monitor の Unified Communications Manager 5.x 以降への追加

（注）
- この作業を行うのは、Unified Communications Manager バージョン 5.x 以降の場合のみです（詳細については、「サポートされているデータ ソース ソフトウェア バージョン」（P.3-7）を参照してください）。
- この作業は、Service Monitor の稼動中にのみ行ってください。

ステップ 1　Unified Communications Manager Serviceability を起動します。

ステップ 2　[Tools] > [CDR Management] を選択します。

ステップ 3　[Billing Applications Server Parameters] までスクロール ダウンし、[Add New] をクリックします。

ステップ 4　次を入力します。

- [Host Name / IP Address] : Cisco Unified Service Monitor がインストールされているシステムの IP アドレスを入力します。
- [User Name] : smuser を入力します。

（注）　smuser 以外のユーザ名を入力しないでください。

- [Password]：パスワードを入力します。デフォルトのパスワードは smuser です。このパスワードを変更するには、次の手順を実行します。
  - まず Service Monitor でパスワードを変更します（詳細については、「その他の設定項目の設定と表示」（P.3-34）を参照してください）。
  - Service Monitor の他の設定で smuser に対して入力したのと同じパスワードを入力します。

（注）　Service Monitor および Unified Communications Manager でパスワードを変更した場合、その新しいパスワードをすぐに受け付けるわけではないので、しばらく待ってから新しいパスワードを再入力してください。

- [SFTP Protocol] を選択します。
- [Directory Path]：/home/smuser/ を入力します。

（注）　/home/smuser 以外のディレクトリ パスを入力しないでください。

- [Resend on Failure]（Unified Communications Manager 7.0 以降にのみ表示される）：このチェックボックスを選択します。

ステップ 5　[Add] をクリックします。

（注）　場合によっては、新しく追加されたビリング サーバに CDR/CMR ファイルを送信するとき、まず CDR Repository Management Service を再起動しなければならないこともあります。

ステップ 1　Unified Communications Manager Serviceability で [Tools] > [Control Center - Network Services] を選択します。

ステップ 2　Unified Communications サーバの一覧から、パブリッシャを選択します。

ステップ 3　[CDR Services] にスクロール ダウンします。

ステップ 4　[Cisco CDR Repository Manager] オプション ボタンを選択します。

ステップ 5　[Restart] ボタンをクリックします。

Unified Communications Manager 5.x 以降での AXL Web Service のアクティブ化

この手順は、Unified Communications Manager バージョン 5.x 以降で実行します（詳細については、「サポートされているデータ ソース ソフトウェア バージョン」（P.3-7）を参照してください）。

ステップ 1　Unified Communications Manager Serviceability を起動します。

ステップ 2　[Tools] > [Service Activation] を選択します。

ステップ 3　サーバを選択します。

（注）　[Publisher] ノードの [AXL Web Service] をアクティブにします。

ステップ 4　[Database and Admin Services] にスクロール ダウンして、[Cisco AXL Web Service] を選択します。

ステップ 5　[Save] をクリックします。

Unified Communications Manager 5.x 以降での smuser のパスワード変更

（注）　この作業は、Unified Communications Manager バージョン 5.x 以降で必要な場合にのみ行います（詳細については、「サポートされているデータ ソース ソフトウェア バージョン」（P.3-7）を参照してください）。

Service Monitor における smuser の SFTP パスワードと、Unified Communications Manager 5.x 以降における Service Monitor アプリケーション ビリング サーバ smuser のパスワードは、同じである必要があります。どちらか一方を変更したら、もう一方も変更して一致させる必要があります。Service Monitor における smuser の SFTP パスワードを変更するには、「その他の設定項目の設定と表示」（P.3-34）を参照してください。

Unified Communications Manager 5.x における Service Monitor アプリケーション ビリング サーバ smuser のパスワードを変更するには、次の手順を実行します。

ステップ 1　Unified Communications Manager Serviceability を起動します。

ステップ 2　[Tools] > [CDR Manageability] を選択します。

ステップ 3　[Billing Applications Server Parameters] までスクロール ダウンし、Service Monitor のリンクをダブルクリックします。

ステップ 4　新しいパスワードを入力します。

（注）　Service Monitor および Unified Communications Manager でパスワードを変更した場合、その新しいパスワードをすぐに受け付けるわけではないので、しばらく待ってから新しいパスワードを再入力してください。

その他のフィールドの値は変更しないでください。[Host Name / IP Address]、[User Name]、[SFTP Protocol]、および [Directory Path] は元のままにしておく必要があります。

ステップ 5　[Update] をクリックします。

Unified Communications Manager 4.x システムのデータベース認証の設定

Service Monitor で Unified Communications Manager 4.x のクレデンシャルを追加または編集するときは、Service Monitor が使用するデータベース認証のタイプ（SQL 認証か Windows 認証）を選択する必要があります（詳細については、「データ ソース クレデンシャルの概要と設定」（P.3-2）を参照してください）。Unified Communications Manager ですでに使用されているデータベース認証のタイプを選択することを推奨します。

Unified Communications Manager で使用されているデータベース認証のタイプを特定するには、「Unified Communications Manager 4.x システムで使用されている認証モードの特定」（P.B-7）の手順を使用します。次に、Service Monitor でクレデンシャルを設定する前に、使用中のデータベース認証モードに関して次の設定作業を行います。

- SQL 認証：「Unified Communications Manager 4.x システムでの SQL 認証の設定」（P.B-8）
- Windows 認証：「Unified Communications Manager 4.x システムでの Windows 認証の設定」（P.B-10）

Unified Communications Manager 4.x システムで使用されている認証モードの特定

ステップ 1　Unified Communications Manager パブリッシャがインストールされているサーバにログインします。

ステップ 2　[Start] > [Programs] > [Microsoft SQL Server Enterprise Manager] を選択します。

ステップ 3　[Console Root] > [Microsoft SQL Servers] > [SQL Server Group] を選択します。

ステップ 4　右クリックし（**local**）、[Properties] を選択します。ダイアログボックスが表示されます。

ステップ 5　[Security] タブを選択します。

ステップ 6　次のどちらが選択されているかをメモします。

- [SQL Server and Windows]
- [Windows only]

ステップ 7　[Cancel] をクリックします。

ステップ 8　Service Monitor で選択する認証モードについては、表 B-2 を参照してください。

Service Monitor で Unified Communications Manager のクレデンシャルを追加または編集するときは、Unified Communications Manager データベースにアクセスするための対応する認証モードを選択する必要があります（表 B-2 を参照）。

表 B-2　データベース認証の選択

Unified Communications Manager で使用されているデータベース認証モード	Service Monitor の Unified Communications Manager クレデンシャルで選択することが推奨されるモード
[SQL and Windows] （注）　[SQL and Windows] は混合モードとも呼ばれます。	任意で、次のいずれかを選択します。 • [Windows Authentication] • [SQL Authentication]
[Windows only]	[Windows Authentication] を選択する必要があります。

Unified Communications Manager 4.x システムでの SQL 認証の設定

次の各手順は、SQL 認証を使用して Service Monitor から Unified Communications Manager Release 4.x のデータベースにアクセスすることを決定した場合に使用します（「Unified Communications Manager 4.x システムで使用されている認証モードの特定」（P.B-7）と表 B-2 を参照）。

（注）　Unified Communications Manager 4.x のデフォルトの認証は Windows のみの認証です。

SQL 認証を使用するには、次の作業が必要です。

- 混合認証を使用するように Unified Communications Manager パブリッシャ ノードを設定する必要があります。「Unified Communications Manager 4.x における Microsoft SQL Server の混合認証の設定」（P.B-8）を参照してください。
- データベースにアクセスできる Microsoft SQL Server ユーザ アカウントを作成する必要があります。「Unified Communications Manager 4.x における Microsoft SQL Server ユーザ アカウントの追加」（P.B-9）を参照してください。

（注）　Unified Communications Manager 4.x のクレデンシャルを Service Monitor に追加するときは、これらのユーザ アカウントのユーザ名とパスワードを入力する必要があります。

Unified Communications Manager 4.x における Microsoft SQL Server の混合認証の設定

Unified Communications Manager 4.x のデフォルトは Windows のみの認証です。次の手順は、SQL 認証を使用して Service Monitor から Unified Communications Manager のデータベースにアクセスすることを決定した場合にのみ使用します。「Unified Communications Manager 4.x システムで使用されている認証モードの特定」（P.B-7）と表 B-2 を参照してください。

注意　このタスクを説明のとおりに実行できない場合、Unified Communications Manager で CDR の書き込みができない可能性があります。

この作業を行うのは、Unified Communications Manager 4.x の場合のみです。

ステップ 1　Unified Communications Manager がインストールされているサーバにログインします。

ステップ 2　[Start] > [Programs] > [Microsoft SQL Server Enterprise Manager] を選択します。

ステップ 3　[Console Root] > [Microsoft SQL Servers] > [SQL Server Group] を選択します。

ステップ 4　右クリックし（**local**）、[Properties] を選択します。ダイアログボックスが表示されます。

ステップ 5　[Security] タブを選択します。

a. [Authentication] で、[SQL Server and Windows] を選択します。

b. [OK] をクリックします。SQL サーバを再起動するかどうかを尋ねるメッセージが表示されます。[No] をクリックします。

（注） Cisco Security Agent が Unified Communications Manager サーバで稼動している場合、SQL サーバを再起動するかどうかを尋ねるメッセージが表示されない可能性があります。この場合、変更は適用されません。この問題を回避するには、Windows Services ユーザ インターフェイスを開き、Cisco Security Agent を停止します。ステップ 5b および 6 が完了したら、Cisco Security Agent を再起動します。

ステップ 6　次の手順で SQL サーバを再起動します。

a. [Start] > [Settings] > [Control Panel] > [Administrative Tools] > [Services] を選択します。[Services] ウィンドウが表示されます。

b. [MSSQLSERVER] を右クリックし、[Stop] をクリックします。MSSQLSERVER とともに停止されるサービスの一覧が表示されます。停止されるサービスに注意してください。これらは 1 つずつステップ 6c. で再開する必要があります。

c. [MSSQLSERVER] を右クリックし、[Start] をクリックします。前のステップで停止されたその他のサービスに対し、サービスを 1 つずつ右クリックし、[Start] をクリックします。

「Unified Communications Manager 4.x における Microsoft SQL Server ユーザ アカウントの追加」（P.B-9）の指示に従って、ユーザ アカウントも追加する必要があります。

Unified Communications Manager 4.x における Microsoft SQL Server ユーザ アカウントの追加

Unified Communications Manager 4.x のデフォルトは Windows のみの認証です。次の手順は、SQL 認証を使用して Service Monitor から Unified Communications Manager のデータベースにアクセスすることを決定した場合にのみ使用します。「Unified Communications Manager 4.x システムで使用されている認証モードの特定」（P.B-7）と表 B-2 を参照してください。

注意　このタスクを説明のとおりに実行できない場合、Unified Communications Manager で CDR の書き込みができない可能性があります。

SQL 認証を使用する場合は、Service Monitor から Unified Communications Manager 4.x が動作しているシステム上のローカル データベースにアクセスするために、1 つ以上の Microsoft SQL Server ユーザ アカウントが必要です。

Unified Communications Manager にアカウントを追加し、Service Monitor から CDR データベースにアクセスできるようにするには、次の手順を実行します。

ステップ 1　Unified Communications Manager がインストールされているサーバにログインします。

ステップ 2　[Start] > [Programs] > [Microsoft SQL Server Enterprise Manager] > [Security] を選択します。

ステップ 3　[Logins] を右クリックし、[New Login] を選択します。ウィンドウが表示されます。

（注）　ステップ 4 で入力するユーザ名とパスワードを、Service Monitor で Unified Communications Manager のクレデンシャルを入力するユーザに提供できるように準備してください。

ステップ 4　[General] タブで次を実行します。

a.　ユーザ名を入力します。

b.　[SQL Authentication] を選択し、パスワードを入力します。

（注）　[Windows Authentication] *ではなく*、[SQL Authentication] が選択されていることを確認してください。デフォルトで [Windows Authentication] が選択されていることがあります。

ステップ 5　[Server Roles] タブを選択し、[System Administrators] ロールを選択します。

注意　ステップ 5 を完了しないと、Unified Communications Manager からデータベースに CDR を書き込むことができなくなる場合があります。

ステップ 6　[Database Access] タブを選択し、次を実行します。

a.　CDR データベースの [Permit] カラムにチェックマークを付けます。ウィンドウの下に、選択したデータベースのデータベース ロールが表示されます。デフォルトでは [public] にチェックマークが付いています。

b.　[db_owner] ロールにチェックマークを付けます。これにより [public] と [db_owner] にチェックマークが付きます。

注意　ステップ 6b を完了しないと、Unified Communications Manager からデータベースに CDR を書き込むことができなくなる場合があります。

ステップ 7　[OK] をクリックします。確認用のダイアログボックスが表示されます。

ステップ 8　このダイアログボックスに再度パスワード（ステップ 4b で入力したもの）を入力し、パスワードを確定します。

Unified Communications Manager 4.x システムでの Windows 認証の設定

次の手順は、Windows 認証を使用して Service Monitor から Unified Communications Manager のデータベースにアクセスすることを決定した場合に使用します。「Unified Communications Manager 4.x システムで使用されている認証モードの特定」（P.B-7）と表 B-2 を参照してください。

Service Monitor システムをインストールすると、casuser という Windows アカウントが作成されます。Service Monitor が Windows 認証を使用してアクセスする個々の Unified Communications Manager 4.x システムで、casuser Windows アカウントを作成する必要があります。すべての casuser アカウントのパスワードを一致させる必要があります。

ステップ 1　Unified Communications Manager がインストールされているシステムにログインします。

ステップ 2　[Start] > [Settings] > [Control panel] > [Administrative Tools] > [Computer Management] > [Users] > [Local Users and Groups] > [Users] を選択し、右クリックして新しいユーザを追加します。

a. ユーザ名として casuser を入力し、適切なフルネームと説明を入力します。

b. パスワードを入力します。

（注） casuser アカウント用の同じパスワードを、Service Monitor（ステップ 6 を参照）と Windows 認証を設定する他の Unified Communications Manager システムにも入力できるように準備してください。

c. [User must change password at next logon] をオフにします。

d. [Password never expires] を選択します。

e. [Create] をクリックします。

ステップ 3　次の手順で、casuser アカウントに CDR データベースへのアクセス権を割り当てます。

a. [Start] > [Programs] > [Microsoft SQL Server Enterprise Manager] > [Console Root] > [Microsoft SQL Servers] > [SQL Server Group] > [local] > [Security] > [Logins] を選択します。

b. [Logins] を右クリックし、[New Login] を選択します。

c. [General] タブで次を実行します。

- [Name] で、[casuser] を選択します。
- [Windows Authentication] を選択します。
- [Security access] で、[Grant access] を選択します。
- [Defaults] の [Database] で、[master] を選択します。

d. [Database Access] タブで次を実行します。

- [CDR] を選択します。
- [Database roles for 'CDR'] で、[db_owner] を選択し、[public] が選択されていることを確認します（デフォルトでは選択されています）。

e. [OK] をクリックします。Windows のみの認証が使用されていることがすでにわかっている場合（「Unified Communications Manager 4.x システムで使用されている認証モードの特定」（P.B-7）を参照）は、ステップ 4 および 5 を省略できますが、ステップ 6 は必ず実行してください。

ステップ 4　次の手順で、認証を Windows のみに設定します。

a. [Console Root] > [Microsoft SQL Servers] > [SQL Server Group] を選択します。

b. 右クリックし（**local**）、[Properties] を選択します。ダイアログボックスが表示されます。

c. [Security] タブを選択します。

d. [Authentication] で、[Windows only] を選択します（[Windows only] がすでに選択されている場合は、[Cancel] をクリックしてステップ 4e および 5 を省略できますが、ステップ 6 は必ず実行してください）。

e. [OK] をクリックします。SQL サーバを再起動するかどうかを尋ねるメッセージが表示されます。[No] をクリックします。

（注）　Cisco Security Agent が Unified Communications Manager サーバで稼動している場合、SQL サーバを再起動するかどうかを尋ねるメッセージが表示されない可能性があります。この場合、変更は適用されません。この問題を回避するには、Windows Services ユーザ インターフェイスを開き、Cisco Security Agent を停止します。ステップ 5b および 6 が完了したら、Cisco Security Agent を再起動します。

ステップ 5　次の手順で SQL サーバを再起動します。

a. [Start] > [Settings] > [Control Panel] > [Administrative Tools] > [Services] を選択します。[Services] ウィンドウが表示されます。

b. [MSSQLSERVER] を右クリックし、[Stop] をクリックします。MSSQLSERVER とともに停止されるサービスの一覧が表示されます。停止されるサービスに注意してください。これらは 1 つずつステップ 4c. で再開する必要があります。

c. [MSSQLSERVER] を右クリックし、[Start] をクリックします。前のステップで停止されたその他のサービスに対し、サービスを 1 つずつ右クリックし、[Start] をクリックします。

ステップ 6　Service Monitor システムで casuser アカウントのパスワードをリセットし、ステップ 2 で入力したパスワードと一致させます。

a. Service Monitor がインストールされているシステムにログインします。

b. C:\Program Files\CSCOpx\setup\support\ に移動し、resetCasuser.exe ファイルをダブルクリックします。

c. [option 2: Enter causer password] を選択します。

d. パスワードを入力して、確認します。情報ウィンドウが開きます。

e. [OK] をクリックします。

f. 次のコマンドを入力して、デーモン マネージャの停止と起動を行います。

```
net stop crmdmgtd
net start crmdmgtd
```

音声ゲートウェイの設定

次のトピックを参照してください。

- 「VAD がイネーブルの場合の音声ゲートウェイの設定」（P.B-12）
- 「CVTQ をサポートする MGCP 音声ゲートウェイの設定」（P.B-13）

VAD がイネーブルの場合の音声ゲートウェイの設定

（注）　音声アクティビティ検出（VAD）をイネーブルにすると、帯域幅を節約できますが、Service Monitor による CVTQ レポート用の MOS の計算にも影響し、場合によっては単語のクリッピングが顕著な、または許容できないレベルで発生する可能性があります。VAD は、Cisco IOS の音声（ダイヤル ピア設定）ではデフォルトでイネーブルになっており、Unified Communications Manager（[System] > [Service Parameters]）ではデフォルトでディセーブルになっています。

この情報は、Unified Communications Manager versions 4.x 以降に適用されます。クラスタ内の音声ゲートウェイで VAD がイネーブルになっていると、音声ゲートウェイと Cisco Unified IP Phone 間のコールに関して、CVTQ レポートの MOS 値が小さくなることがあります。次の作業が必要です。

- H.323、SCCP、および SIP ゲートウェイで、コンフォート ノイズのペイロード タイプを（デフォルトの 19 から）13 に設定します。これにより、Cisco Unified IP Phone と音声ゲートウェイが MOS の計算を適切に調整できるようになります。

（注）　センサーは、VAD がイネーブルの場合でも音声ゲートウェイの MOS を正しく計算します。

- Cisco Unified IP Phone と MGCP ゲートウェイ間のコールに関しては、CVTQ レポートで報告される MOS が小さいことに注意します（MGCP ゲートウェイではコンフォート ノイズのペイロード タイプを設定できません）。

CVTQ をサポートする MGCP 音声ゲートウェイの設定

MGCP 音声ゲートウェイのサポート要件と構成ガイドについては、『*Cisco Unified Service Monitor 8.5 Compatibility Matrix*』を参照してください。

サポートされる電話機

CVTQ をサポートする Cisco IP Phone については、『*Cisco Unified Service Monitor 8.5 Compatibility Matrix*』を参照してください。

Cisco Unified Communications Manager での TFTP サービスの再起動

この作業は、次の条件がすべて満たされた場合にのみ行う必要があります。

- Cisco 1040 のコンフィギュレーション ファイルおよびバイナリ イメージ ファイルの TFTP サーバとして Unified Communications Manager 5.x 以降を使用している（サポート対象バージョンについては、「サポートされているデータ ソース ソフトウェア バージョン」（P.3-7）を参照してください）。
- 最近、Cisco 1040 のバイナリ イメージ ファイルまたは Cisco 1040 のコンフィギュレーション ファイルを TFTP のルート位置に手動でコピーした。
- Cisco 1040 が最新のファイルをダウンロードできないか、または Service Monitor に登録されていない（Cisco 1040 の設定を表示するには、「Cisco 1040 の Web インターフェイスを使用した設定の表示」（P.4-15）を参照してください）。

（注）　この作業は、営業時間外に行ってください。

ステップ 1　Unified Communications Manager Serviceability にログインします。

ステップ 2　CM サービスの Cisco TFTP を再起動します。詳細については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。