AS-SIP エンドポイントの設定

AS-SIP の概要

Assured Services SIP（AS-SIP）エンドポイントは、MLPP、DSCP、TLS/SRTP、および IPv6 に準拠しています。 AS-SIP は、Unified Communications Manager 上で複数のエンドポイント インターフェイスを実現します。

多くの Cisco IP 電話は、AS-SIP をサポートしています。 加えて、サードパーティ製 AS-SIP エンドポイントデバイスタイプを使用すれば、サードパーティ製 AS-SIP 準拠のエンドポイントを設定して Cisco Unified Communications Manager で使用できるようになります。 加えて、サードパーティ製 AS-SIP エンドポイントデバイスタイプを使用すれば、サードパーティ製 AS-SIP 準拠の汎用エンドポイントを設定して Cisco Unified Communications Manager で使用できるようになります。

AS-SIP の機能

AS SIP エンドポイントに対しては、次の機能が実装されているか使用可能になっています。

- MLPP
- TLS
- SRTP
- 優先レベルの DSCP
- エラー応答
- V.150.1 MER
- 会議ファクトリ フローのサポート
- AS-SIP 回線早期オファー

サードパーティ AS-SIP フォン

サードパーティの電話機は、サードパーティー製 AS-SIP エンドポイントデバイスタイプを使用して、Cisoc Unified Communications Manager でプロビジョニングすることができます。

AS-SIP を実行しているサードパーティ製電話機は、Cisco Unified Communications Manager TFTP サーバを使用して設定されません。 お客様が、ネイティブ電話機設定メカニズム（通常は、ウェブ ページまたは tftp ファイル）を使用して、電話機を設定する必要があります。 お客様は、Cisco Unified Communications Manager データベース内のデバイスおよび回線の設定と、ネイティブ電話機設定の同期を保つ必要があります（たとえば、電話機の内線番号 1002 と Cisco Unified Communications Manager の 1002）。 また、回線のディレクトリ番号が変更された場合、Unified CM Administration とネイティブの電話機設定メカニズムの両方で、そのディレクトリ番号が変更されていることを確認する必要があります。

サードパーティの電話機の識別

SIP を実行しているサードパーティ製の電話機は MAC アドレスを送信しないため、ユーザ名を使用して自分自身の身元を証明する必要があります。 REGISTER メッセージには次のヘッダーが含まれています。

```
Authorization: Digest
username="swhite",realm="ccmsipline",nonce="GBauADss2qoWr6k9y3hGGVDAqnLfoLk5",uri
="sip:172.18.197.224",
algorithm=MD5,response="126c0643a4923359ab59d4f53494552e"
```

ユーザ名 **swhite** は、Cisco Unified Communications Manager の **[エンドユーザの設定(End User Configuration)]** ウィンドウで設定されたユーザと一致する必要があります。 管理者は、**[電話の設定(Phone Configuration)]** ウィンドウの **[ダイジェストユーザ(Digest User)]** フィールド内のユーザ（**swhite** など）を使用してサードパーティ製 SIP 電話機を設定します。

（注） 各ユーザ ID は、1 つのサードパーティの電話機にのみ割り当てることができます。 同じユーザ ID がダイジェスト ユーザとして複数の電話機に割り当てられている場合、そのエンドユーザ ID が割り当てられているサードパーティ製電話機は正しく登録されません。

サードパーティ AS-SIP 電話および Cisco IP 電話の設定

下の表は、Cisco Unified IP Phone と AS-SIP を実行しているサードパーティ製電話機の設定上の違いを比較したものです。

表 *1 : Cisco IP* 電話とサードパーティ製電話機の設定の違いの比較

AS-SIP を実行している電話機	中央集中型 TFTP との統合	MAC アドレスの送信	ソフトキー ファイルのダウンロード	ダイヤル プラン ファイルのダウンロード	Unified Communications Manager のフェールオーバーとフォールバックのサポート	リセットと再起動のサポート
Cisco IP 電話	可	可	可	可	可	可
サードパーティ製 AS-SIP デバイス	不可	不可	不可	不可	不可	不可

（注） すべての Cisco IP 電話が AS-SIP をサポートしているわけではありません。 サポート情報については、ご使用の電話機モデルのアドミニストレーション ガイドを参照してください。

[Cisco Unified CM Administration] を使用して、SIP が実行されているサードパーティ製の電話機を設定します（詳細は、『*Cisco Unified Communications Manager* のシステム構成ガイド』の「SIP プロファイルの設定」を参照してください

)。管理者は、SIP を実行するサードパーティの電話機で設定手順を実行する必要があります。次の例を参照してください。

- 電話機のプロキシ アドレスが、Cisco Unified Communications Manager の IP または完全修飾ドメイン名（FQDN）であることを確認します。
- 電話機のディレクトリ番号が、Cisco Unified CM Administration でデバイスに対して設定したディレクトリ番号と一致していることを確認します。
- 電話機のダイジェスト ユーザ ID（承認 ID とも言います）が、Cisco Unified CM Administration で設定したダイジェスト ユーザ ID と一致していることを確認します。

詳細については、サードパーティの電話機に付属するドキュメントを参照してください。

AS-SIP 会議

機能の呼び出し元（保留元、転送元、または会議開催者）でシスコ独自の機能シグナリングがサポートされている場合は、MOH がそのターゲット（保留先、転送直前の転送先、または参加直前の会議出席者）に適用されます。 機能の呼び出し元でシスコ独自の機能シグナリングがサポートされていない場合は、MOH がそのターゲットに適用されません。 また、エンドポイ

ントが会議ミキサーであることを明示的に伝達する場合は、MOH がそのターゲットで再生されません。 AS-SIP 会議には次の 2 つの形態があります。

- ローカル混合
- 会議ファクトリ

ローカル混合

Unified CM からは、会議開催者が他の会議参加者のそれぞれに対してアクティブ コールを同時に確立したようにしか見えません。 会議はイニシエータによってホストされ、そこで音声が混合されます。 会議開催者からのコールにはMOH ソースへの接続を拒否する特殊なシグナリングが含まれています。

会議ファクトリ

会議イニシエータはSIP トランクの外側に設置された会議ファクトリサーバを呼び出します。そして、IVR シグナリングを通して、会議ブリッジを予約するように会議ファクトリに指示します。 会議ファクトリから会議イニシエータに数値アドレス（ルーティング可能な DN）が返され、会議開催者はブリッジとの登録を確立して、参加者を追跡するための会議リスト情報を受け取ります。 会議ファクトリにより、MOH ソースへの接続を拒否する特殊なシグナリングが送信されます。

AS-SIP の前提条件

十分なデバイス ライセンス ユニットが使用可能かどうかを調べます。 詳細については、『*Cisco Unified Communications Manager* のシステム構成』の「スマート ソフトウェア ライセンシング」の章を参照してください。

AS-SIP エンドポイント設定タスク フロー

次のタスクを完了して、AS-SIP エンドポイントを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	ダイジェストユーザの設定 （6 ページ）	SIP リクエストにダイジェスト認証を使用するようにエンドユーザを設定します。
ステップ 2	SIP 電話のセキュア ポートの設定 （6 ページ）	Cisco Unified Communications Manager はこのポートを使用して SIP 回線の登録用の SIP 電話を TLS を介してリッスンします。

	コマンドまたはアクション	目的
ステップ 3	サービスの再起動 （7 ページ）	セキュアポートを設定した後、Cisco CallManager サービスと Cisco CTL Provider サービスを再起動します。
ステップ 4	AS-SIP 用 SIP プロファイルの設定 （7 ページ）	AS-SIP エンドポイントと SIP トランクの SIP 設定を SIP プロファイルで設定します。 （注） 電話機固有のパラメータはサードパーティ製 AS-SIP 電話機にダウンロードされません。 Cisco Unified Communications Manager でのみ使用されます。サードパーティ製電話機では同じ設定値をローカルに設定する必要があります。
ステップ 5	AS-SIP 用電話セキュリティプロファイルの設定 （8 ページ）	電話セキュリティプロファイルを使用して、TLS、SRTP、ダイジェスト認証などのセキュリティ設定を割り当てることができます。
ステップ 6	AS-SIP エンドポイントの設定 （9 ページ）	Cisco IP 電話またはサードパーティエンドポイントを AS-SIP サポートとともに設定します。
ステップ 7	デバイスとエンド ユーザの関連付け （10 ページ）	エンドポイントをユーザに関連付けます。
ステップ 8	AS-SIP 用 SIP トランク セキュリティ プロファイルの設定 （11 ページ）	トランクセキュリティプロファイルを使用して、TLS 認証やダイジェスト認証などのセキュリティ機能を SIP トランクに割り当てることができます。
ステップ 9	AS-SIP 用 SIP トランクの設定 （11 ページ）	SIP トランクを AS-SIP サポートで設定します。
ステップ 10	AS-SIP 機能の設定 （12 ページ）	MLPP、TLS、V.150、IPv6 などの追加の SIP 機能を設定します。

ダイジェストユーザの設定

ダイジェスト認証を使用するダイジェスト ユーザとしてエンド ユーザを設定するには、この手順を使用します。 ユーザに関連付けられているデバイスは、ユーザのダイジェスト クレデンシャルを使用して認証されます。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザの管理（User Management）] > [エンドユーザ（End User）]** を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいユーザを作成するには、[新規追加] をクリックします。
- 既存のユーザを選択するには、[検索（Find）]をクリックします。

ステップ 3 次の必須フィールドが入力されていることを確認してください。

- ユーザー ID（User ID）
- [姓（Last Name）]

ステップ 4 [ダイジェスト認証（Digest Credentials）]フィールドにパスワードを入力します。 エンド ユーザは、エンドポイントを使用する際に、このパスワードを使用して認証する必要があります。

ステップ 5 残りのすべてのフィールドに入力します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 6 **[保存]** をクリックします。

SIP 電話のセキュア ポートの設定

ポートを設定するには、次の手順に従います。 Cisco Unified Communications Manager はこのポートを使用して SIP 回線の登録用の SIP 電話を TLS を介してリッスンします。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [Cisco Unified CM（Cisco Unified CM）]** を選択します。

ステップ 2 [このサーバのCisco Unified Communications Manager TCPポート設定（Cisco Unified Communications Manager TCP Port Settings for this Server）]で、[SIP電話セキュアポート（SIP Phone Secure Port）] フィールドにポート番号を指定するか、またはデフォルト値をそのまま使用します。デフォルト値は5061です。

ステップ 3 **[保存]** をクリックします。

ステップ 4 **[設定の適用（Apply Config）]** をクリックします。

ステップ 5 [OK]をクリックします。

サービスの再起動

Cisco CallManager サービスと Cisco CTL Provider サービスを再起動するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Serviceability インターフェイスで、**[ツール（Tools）]** > **[コントロールセンター - 機能サービス（Control Center - Feature Services）]** を選択します。

ステップ 2 [サーバ（Servers）] ドロップダウンリストから、[Cisco Unified Communications Manager] サーバを選択します。
CM の [サービス（Services）] 領域で、[サービス名（Service Name）]列に Cisco CallManager が表示されます。

ステップ 3 Cisco CallManager サービスに対応するラジオ ボタンをクリックします。

ステップ 4 **再起動（Restart）**をクリックします。
サービスが再起動し、「サービスは正常に再起動しました（Service Successfully Restarted）」というメッセージが表示されます。

ステップ 5 手順 3 と手順 4 を繰り返して、Cisco CTL Provider サービスを再起動します。

AS-SIP 用 SIP プロファイルの設定

AS-SIP エンドポイントと SIP トランクの SIP プロファイルを、SIP 設定を使用して設定するには、次の手順を使用します。

手順

ステップ 1 Cisco Unified CM Administration で、**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[SIP プロファイル（SIP Profile）]** を選択します。

ステップ 2 次のいずれかを実行します。

- 新しい SIP プロファイルを作成するには、[新規追加] をクリックします。
- **[検索（Find）]** をクリックして、既存の SIP プロファイルを選択します。

ステップ 3 SIP プロファイルの [名前（Name）]と [説明（Description）]を入力します。

ステップ 4 [Assured Services SIPとの適合（Assured Services SIP conformance）]チェックボックスをオンにします。

（注） このチェックボックスは、SIP トランクおよびサードパーティ AS-SIP 電話に対してオンにする必要があります。 これは、AS-SIP をサポートしている Cisco IP 電話では必須ではありません。

ステップ 5 [電話で使用されるパラメータ（Parameters used in Phone）]セクションで、作成する予定のコール タイプ向けに DSCP 優先度の値を設定します。

（注） クラスタ全体のサービス パラメータを使用して DSCP 値を設定することもできます。 ただし、SIP プロファイルで設定した DSCP 値は、その SIP プロファイルを使用するすべてのデバイスで、クラスタ全体の設定よりも優先されます。

ステップ 6 [音声コールおよびビデオコールのアーリー オファー サポート（Early Offer support for voice and video calls）]ドロップダウン リストで、次のいずれかのオプションを選択し、このプロファイルを使用する SIP トランク向けのアーリー オファー サポートを設定します。

- 無効
- [ベストエフォート（MTP挿入なし）（Best Effort (no MTP inserted)）]
- [必須（必要に応じてMTPを挿入）（Mandatory (insert MTP if needed)）]

ステップ 7 [SIPプロファイルの設定（SIP Profile Configuration）]ウィンドウで、残りのフィールドを入力します。 フィールドと設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 8 **[保存]** をクリックします。

AS-SIP 用電話セキュリティプロファイルの設定

AS-SIP エンドポイント用の電話セキュリティプロファイルを設定するには、次の手順を使用します。 このセキュリティプロファイルを使用して、TLS や SRTP などのセキュリティ設定を割り当てることができます。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[セキュリティ（Security）]** > **[電話セキュリティプロファイル（Phone Security Profile）]** の順に選択します。

ステップ 2 次のいずれかの手順を実行します。

- [新規追加（Add New）] をクリックして、新しい電話セキュリティ プロファイルを作成します。
- **[検索（Find）]** をクリックし、既存のプロファイルを編集します。

ステップ 3 新しいプロファイルの場合、**[電話機のセキュリティプロファイル]** ドロップダウンからオプションを選択し、**[サードパーティー製 AS-SIP エンドポイント]** を選択して、**[次へ]** をクリックします。

- Cisco IP 電話の場合は、電話機のモデルを選択して、**[次へ (Next)]** をクリックします。
- サードパーティ製 AS-SIP エンドポイント の場合は、**[サードパーティ製 AS-SIP エンドポイント]** を選択し、**[次へ (Next)]** をクリックします。

ステップ 4 プロトコルには、**[SIP]**を選択し、**[次へ (Next)]** をクリックします。

ステップ 5 プロトコルの **[名前（Name）]** と **[説明（Description）]** を入力します。

ステップ 6 次のいずれかの設定に**デバイスセキュリティモード**を割り当てます。

- **[認証（Authenticated）]**：Cisco Unified Communications Manager は TLS シグナリングを使用して、電話機に整合性および認証を提供します。
- **[暗号化]**：Cisco Unified Communications Manager は TLS シグナリングを使用して、電話機に整合性および認証を提供します。 また、SRTP はメディア ストリームも暗号化します。

ステップ 7 [ダイジェスト認証を有効化（Enable Digest Authentication）]チェックボックスをオンにします。

ステップ 8 **[電話のセキュリティプロファイルの設定]** ウィンドウの残りのフィールドを設定します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 9 **[保存]** をクリックします。

AS-SIP エンドポイントの設定

次の手順を使用して、AS-SIP エンドポイントを設定します。 多くの Cisco IP 電話は、AS-SIP をサポートしています。 さらに、サードパーティエンドポイントの AS-SIP を設定することもできます。

手順

ステップ 1 Cisco Unified CM 管理から、**[デバイス]** > **[電話機]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [電話のタイプ（Phone Type）] ドロップダウン リストから、AS-SIP をサポートする Cisco IP Phone を選択します。 それ以外の場合は、[サードパーティ AS-SIP エンドポイント（Third-Party AS-SIP Endpoint）]を選択します。

ステップ 4 [次へ（Next）]をクリックします。

ステップ 5 次の必須フィールドを設定します。フィールドと設定オプションの詳細については、オンライン ヘルプを参照してください。

- [デバイス信頼モード（Device Trust Mode）]：サードパーティ AS-SIP エンドポイントでのみ使用します。 [信頼済み（Trusted）]または [信頼されていない（Not Trusted）]を選択します。
- MAC Address
- [デバイス プール（Device Pool）]
- [電話ボタンテンプレート(Phone Button Template)]
- [オーナーのユーザID(Owner User ID)]

- [デバイスのセキュリティプロファイル（Device Security Profile）]：AS-SIP用にセットアップした電話のセキュリティ プロファイルを選択します。
- [SIPプロファイル（SIP Profile）]：設定した AS-SIP 対応の SIP プロファイルを選択します。
- [ダイジェストユーザ（Digest User）]：ダイジェストユーザとして設定するユーザIDを選択します。 このユーザはダイジェスト認証が有効化されている必要があります。
- [DTMF受信が必要（Require DTMF Reception）]：エンドポイントでDTMF番号を受け付けられるようにするには、このチェックボックスをオンにします。
- 音声とビデオ通話の早期提供サポート: このチェックボックスをオンにすると、早期サービスサポートが有効になります。 このフィールドは、サードパーティの電話機でのみ表示されます。

ステップ 6 [MLPPおよび機密アクセスレベル情報（MLPP and Confidential Access Level Information）]セクションのフィールドを設定します。

ステップ 7 **[保存]** をクリックします。

ステップ 8 ディレクトリ番号を追加します。

a) 左のナビゲーション バーで、[新規DNを追加（Add a New DN）]をクリックします。 [ディレクトリ番号の設定（Directory Number Configuration）]ウィンドウが開きます。

b) **ディレクトリ番号**を追加します。

c) [ディレクトリ番号の設定（Directory Number Configuration）]ウィンドウで、残りのフィールドを入力します。

d) **[保存]** をクリックします。

ステップ 9 [関連リンク（Related Links）]から、[デバイスの設定（Configure Device）]を選択し、[移動（Go）]をクリックします。

ステップ 10 **[設定の適用（Apply Config）]** をクリックします。

デバイスとエンド ユーザの関連付け

エンドユーザを AS-SIP エンドポイントに関連付けるには、次の手順を使用します。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[ユーザ管理（User Management）]** > **[エンド ユーザ（End User）]**。

ステップ 2 [検索（Find）]をクリックして、デバイスに関連付けるユーザを選択します。

ステップ 3 **[デバイス情報（Device Information）]** セクションで、**[デバイスの関連付け（Device Association）]** を選択します。
[ユーザデバイス割り当て（User Device Association）] ウィンドウが表示されます。

ステップ 4 [検索（Find）]をクリックすると、使用可能なデバイスのリストが表示されます。

ステップ 5 関連付けるデバイスを選択して、[選択/変更の保存（Save Selected/Changes）]をクリックします。

ステップ 6 [関連リンク（Related Links）]から、[ユーザの設定に戻る（Back to User）]を選択し、[移動（Go）]をクリックします。
[エンドユーザの設定（End User Configuration）]ウィンドウが表示され、選択し、割り当てたデバイスが、[制御するデバイス（Controlled Devices）]ペインに表示されます。

AS-SIP 用 SIP トランク セキュリティ プロファイルの設定

AS-SIP をサポートする SIP トランク用のセキュリティ プロファイルを設定するには、この手順を使用します。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [セキュリティ（Security）] > [SIP トランクのセキュリティ プロファイル（SIP Trunk Security Profile）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 セキュリティ プロファイルの [名前（Name）]を入力します。

ステップ 4 [デバイスのセキュリティモード（Device Security Mode）] ドロップダウン リストから、[暗号化（Encrypted）] または [認証済み（Authenticated）]を選択します。

ステップ 5 [着信転送タイプ（Incoming Transport Type）]フィールドと [発信転送タイプ（Outgoing Transport Type）]フィールドが、自動的に [TLS]に変更されます。

ステップ 6 [ダイジェスト認証を有効化（Enable Digest Authentication）]チェックボックスをオンにします。

ステップ 7 V.150 を導入する場合は、[SIP V.150アウトバウンドSDPオファーのフィルタリング（SIP V.150 Outbound SDP Offer Filtering）] ドロップダウン リストの値を設定します。

ステップ 8 **[SIP トランクのセキュリティ プロファイルの設定]** ウィンドウで、残りのフィールドを入力します。フィールドと設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 9 **[保存]** をクリックします。

AS-SIP 用 SIP トランクの設定

AS-SIP をサポートする SIP トランクを設定するには、次の手順を使用します。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [トランク（Trunk）]** を選択します。

ステップ 2 次のいずれかを実行します。

- 既存のトランクを選択するには、[検索（Find）]をクリックします。
- **[新規追加（Add New）]** をクリックし、新規トランクを作成します。

ステップ 3 新しいトランクについては、[トランクタイプ（Trunk Type）]ドロップダウン リストから [SIP トランク（SIP Trunk）]を選択します。

ステップ 4 [トランクサービスタイプ（Trunk Service Type）]ドロップダウン リストで、[なし（None）]（デフォルト）を選択し、[次へ（Next）]をクリックします。

ステップ 5 トランクの**デバイス名**を入力します。

ステップ 6 [デバイスプール（Device Pool）]ドロップダウン リストから、デバイス プールを選択します。

ステップ 7 **[宛先アドレス]** フィールドに、トランクを接続するサーバのアドレスを入力します。

ステップ 8 [SIP トランクのセキュリティプロファイル（SIP Trunk Security Profile）]ドロップダウン リストから、AS-SIP 用に作成したプロファイルを選択します。

ステップ 9 **[SIP プロファイル（SIP Profile）]** ドロップダウン リストから、AS-SIP 用に設定した SIP プロファイルを選択します。

ステップ 10 **トランク設定**ウィンドウの残りのフィールドをすべて入力します。 フィールドと設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 11 **[保存]** をクリックします。

AS-SIP 機能の設定

前述のタスク フローの手順では、エンドポイントとトランクの AS-SIP サポートを設定する方法について説明しています。 次の表に、導入可能な AS-SIP の各機能の概要と、それぞれの構成参照を示します。

AS-SIP 機能	設定の説明
早期オファー	SIP 早期提供では、エンドポイントが INVITE 要求および 200OK 応答の間にメディアをネゴシエートできます。 早期提供には次の 2 つのモードがあります。 • ベストエフォート早期提供（MTP 挿入なし） • 必須早期提供 (必要に応じて MTP を挿入) 次の設定ウィンドウのフィールドを使用して、早期サービスサポートを設定します。 詳細なフィールドの説明については、オンライン ヘルプを参照してください。 **SIP プロファイル設定** ウィンドウ • 音声とビデオコールの早期提供サポート:SIP トランクでの早期提供サポートを有効にするため、このフィールドを設定します。 • アーリーオファーおよび再招待の SDP セッション レベル帯域幅修飾子 • [通話中 INVITE での送受信 SDP の送信（Send send-receive SDP in mid-call INVITE）] **[電話の設定]** ウィンドウ (サードパーティ製 AS-SIP エンドポイントデバイスタイプが使用されている場合のみ) • 音声とビデオ通話の早期提供サポート: このチェックボックスをオンにすると、早期サービスサポートが有効になります。
会議ファクトリ	IMS クライアントが会議を設定するために使用する URI を指定します。 1. Cisco Unified CM の管理から、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** の順に選択します。 2. **[サーバ（Server）]** ドロップダウン リストから、Cisco Unified Communications Manager サーバを選択します。 3. [サービス（Service）]から、**Cisco CallManager** を選択します。 4. [クラスタ全体のパラメータ（機能 - 会議）（Clusterwide Paramters (Feature - Conference)）]で、**IMS 会議ファクトリ URI** を割り当てます。 5. **[保存]** をクリックします。

AS-SIP 機能	設定の説明
DSCP マーキング	DSCP 設定を使用すると、ネットワーク内の QoS と帯域幅を管理できます。 DSCP 設定を使用して、優先順位付けされたトラフィッククラスラベルをコールごとのコールに割り当てます。 サービス パラメータを使用して、クラスタ全体の DSCP 設定を指定できます。また、SIP プロファイルを使用して、そのプロファイルを使用するユーザに対してカスタマイズされた QoS ポリシーを割り当てることができます。 たとえば、エグゼクティブ（CEO など）や営業チームのコールに高い優先順位を割り当て、ネットワーク帯域幅の問題が発生した場合にそれらのコールが切断されないようにすることができます。 DSCP の設定については、「DSCP 設定の設定タスク フロー」を参照してください。
IPv6	デフォルトでは、Cisco Unified Communications Manager は IPv4 アドレス指定を使用するように設定されています。 ただし、IPv6 スタックをサポートするようにシステムを構成することで、IPv6 のみのエンドポイントを使用して SIP ネットワークを展開することができます。 IPv6 の設定の詳細については、『*Cisco Unified Communications Manager* システム構成ガイド』の「デュアルスタック Ipv6 構成タスク フロー」の章を参照してください。
Multilevel Precedence and Preemption（MLPP）	Multilevel Precedence and Preemption（MLPP）サービスを使用すると、優先コールをかけることができます。 この機能により、国家の非常事態やネットワークの機能低下など、ネットワークに負荷がかかっている場合に、優先順位の高いユーザが重要な組織や担当者への通信を確実に行うことができます。 MLPP の設定については、「Multilevel Precedence and Preemption のタスク フロー」を参照してください。
Secure Real-Time Transport Protocol（SRTP）	Secure Real-time Transport Protocol (SRTP) を使用すると、コール内のメディアストリームに暗号化と認証を提供できます。 SRTP は、電話機が使用する**電話機のセキュリティプロファイル設定**内の電話機用に設定できます。 **[デバイスセキュリティモード(Device Security Mode)]**フィールドを**[暗号化済]**に設定する必要があります。
トランスポート層のシグナリング (TLS)	Transport Layer Security（TLS）はセキュアポートと証明書交換を使用して、2 つのシステム間またはデバイス間でセキュアで信頼できるシグナリングやデータ転送を実現します。 TLS の設定に関する詳細は、『*Cisco Unified Communications Manager* のセキュリティ ガイド』の「TLS 設定」の章を参照してください。

AS-SIP 機能	設定の説明
V.150	「V. 150 最低必須要件」機能を使用すると、IP ネットワーク経由のモデムで安全なコールを行うことができます。 この機能では、ダイヤルアップモデムを使用して、従来の公衆交換電話網 (PSTN) 上で動作するモデムとテレフォニーデバイスを大規模に設置します。 V.150 を設定するには、『*Cisco Unified Communications Manager* のセキュリティ ガイド』の「Cisco V.150 最低要件（MER）」の章を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。