トランクの設定

SIP トランクの概要

コール制御シグナリング用に SIP を展開する場合、SIP ゲートウェイ、SIP プロキシ サーバ、Unified Communications アプリケーション、会議ブリッジ、リモート クラスタ、または Session Management Edition などの外部デバイスに Cisco Unified Communications Manager を接続するための SIP トランクを設定します。

Cisco Unified CM Administration の内部で、[SIP Trunk Configuration] ウィンドウには、Cisco Unified Communications Manager が SIP コールの管理に使用する SIP シグナリング設定が含まれています。

1 つの SIP トランクに、IPv4 または IPv6 のアドレッシング、完全修飾ドメイン名、または単一の DNS SRV レコードを使用して、最大 16 個の異なる宛先アドレスを割り当てることができます。

SIP トランクの前提条件

SIP トランクを設定する前に、次の操作を実行してください。

- トランク接続を理解できるようにネットワークトポロジを計画します。
- トランクを接続するデバイスと、それらのデバイスが SIP を実装する方法を理解していることを確認します。

- トランク用にデバイス プールが設定されていることを確認します。
- トランクに IPv6 を展開する場合は、クラスタ全体のエンタープライズ パラメータを使用するか、トランクに適用できる共通のデバイス設定をしようして、トランクのアドレッシング設定を指定する必要があります。
- トランクを使用するアプリケーションに SIP の相互運用性の問題がある場合は、デフォルトの SIP 正規化または透過性スクリプトの使用が必要になる場合があります。デフォルトのスクリプトのいずれも要件に合わない場合は、独自のスクリプトを作成できます。カスタマイズされた SIP 正規化および透過性スクリプトの作成の詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』を参照してください。

SIP トランクの設定タスク フロー

SIP トランクをセットアップするには、この手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	SIP プロファイルの設定 （2 ページ）	SIP トランクに適用する共通の SIP 設定項目を指定します。
ステップ 2	SIP トランク セキュリティ プロファイルの設定 （3 ページ）	TLS シグナリングまたはダイジェスト認証などのセキュリティ設定を使用して、セキュリティ プロファイルを設定します。
ステップ 3	SIP トランクの設定 （4 ページ）	SIP トランクをセットアップして、そのトランクに SIP プロファイルとセキュリティ プロファイルを適用します。

SIP プロファイルの設定

共通 SIP 設定を使用して SIP プロファイルを設定するには、この手順を使用します。設定した SIP プロファイルは、このプロファイルを使用する SIP デバイスおよびトランクに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、**[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 次のいずれかの手順を実行します。

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

ステップ 3 SIP 電話とトランクで IPv4 と IPv6 のスタックをサポートする場合は、[ANATの有効化（Enable ANAT）]チェックボックスをオンにします。

ステップ 4 SDP の相互運用性を解決するために SDP 透過性プロファイルを割り当てる場合は、[SDP透過性プロファイル（SDP Transparency Profile）]ドロップダウン リストから割り当てます。

ステップ 5 SIP の相互運用性の問題を解決するために正規化スクリプトまたは透過性スクリプトを割り当てる場合は、[正規化スクリプト（Normalization Script）]ドロップダウン リストからスクリプトを選択します。

ステップ 6 （任意） Cisco の**統合された境界要素**を越えてコールをルーティングする必要がある場合は、グローバルダイヤルプランのレプリケーション展開について、[ILS で学習した場合の通知先ルート文字列の送信] チェックボックスをオンにします。

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（Save）]** をクリックします。

SIP トランク セキュリティ プロファイルの設定

セキュリティ設定を使用してSIP中継セキュリティプロファイルを構成し、要約アイデンティティ認証やトップドメイン名システムシグナリング暗号化などを行う。プロファイルをSIPトランクに割り当てると、トランクはセキュリティプロファイルの設定を取得します。

（注） SIP トランクに SIP トランクのセキュリティ プロファイルを割り当てない場合は、Cisco Unified Communications Manager は、デフォルトで、非セキュア プロファイルを割り当てます。

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 TLS を使用した SIP シグナリング暗号化を有効化するには、次の手順を実行します。

a) [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）]を選択します。

b) [着信転送タイプ（Incoming Transport Type）]および [発信転送タイプ（Outgoing Transport Type）]のドロップダウン リストから、[TLS]を選択します。

c) デバイスの認証で、[X.509 のサブジェクト名（X.509 Subject Name）]フィールドで、X.509 証明書のサブジェクト名を入力します。
d) [着信ポート（Incoming Port）]フィールドに、TLS リクエストを受信するポートを入力します。 TLS のデフォルトは 5061 です。

ステップ 4 ダイジェスト認証を有効にするには、次の内容を実行します。

a) [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。
b) システムが新しいナンスを生成するまでの時間（秒数）を[ナンス有効時間（Nonce Validity Time）]に入力します。 デフォルトは 600（10 分）です。
c) アプリケーションのダイジェスト認証を有効にするには、[アプリケーションレベル認証を有効化（Enable Application Level Authorization）]チェックボックスをオンにします。

ステップ 5 **[SIP トランク セキュリティ プロファイルの設定（SIP Trunk Security Profile Configuration）]** ウィンドウで追加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。

ステップ 6 **[保存]** をクリックします。

（注） トランクが設定を使用するためには、**そのプロファイル**をトランク設定ウィンドウでトランクに割り当てる必要があります。

SIP トランクの設定

SIP トランクを設定するには、この手順を使用します。 1 つの SIP トランクには最大 16 個の宛先アドレス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、**[デバイス（Device）]** > **[トランク（Trunk）]** 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 [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 [プロトコルタイプ（Protocol Type）]ドロップダウン リストから、導入環境に適した SIP トランクのタイプを選択し、[次へ（Next）]をクリックします。

- **[なし（None）]（デフォルト）**
- **[Call Control Discovery（コール制御検出）]**
- **[クラスタ間のエクステンションモビリティ（Extension Mobility Cross Cluster）]**
- **[Cisco Intercompany Media Engine]**
- **[IP マルチメディア システム サービス コントロール（IP Multimedia System Service Control）]**

ステップ 5 （オプション）このトランクに**共通デバイス設定**を適用する場合は、ドロップダウン リストから設定を選択します。

ステップ 6 暗号化されたメディアをトランクを介して送信する場合は、[SRTPを許可（SRTP Allowed）] チェックボックスをオンにします。

ステップ 7 すべてのクラスタ ノードに対してトランクを有効化する場合は、[すべてのアクティブなUnified CMノードで実行（Run on All Active Unified CM Nodes）]チェックボックスをオンにします。

ステップ 8 SIP トランクの宛先アドレスを設定します。

a) [宛先アドレス（Destination Address）]テキスト ボックスに、トランクに接続するサーバまたはエンドポイントの IPv4 アドレス、完全修飾ドメイン名、または DNS SRV レコードを入力します。

b) トランクがデュアル スタック トランクの場合は、[宛先アドレス IPv6（Destination Address IPv6）]テキスト ボックスに、トランクに接続するサーバまたはエンドポイントの IPv6 アドレス、完全修飾ドメイン名、または DNS SRV レコードを入力します。

c) 宛先が DNS SRV レコードの場合は、[宛先アドレスは SRV（Destination Address is an SRV）] チェック ボックスをオンにします。

d) 接続先を追加するには、**[+]** をクリックします。

ステップ 9 **[SIP トランク 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 ボックスから、このトランクに SIP トランク セキュリティプロファイルを割り当てます。このオプションを選択しない場合は、非セキュア プロファイルが割り当てられます。

ステップ 10 [SIPプロファイル（SIP Profile）]ドロップダウン リストから、SIP プロファイルを割り当てます。

ステップ 11 （任意） この SIP トランクに正規化スクリプトを割り当てる場合は、[正規化スクリプト（Normalization Script）]ドロップダウン リストから、割り当てるスクリプトを選択します。

ステップ 12 [Trunk Configuration]ウィンドウのその他の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。

ステップ 13 **[保存（Save）]** をクリックします。

SIP トランクの連携動作および制限

機能	説明
複数のセキュア SIP トランクを同じ宛先に接続する	リリース 12.5(1) では、Cisco Unified Communications Manager は、同じ宛先 IP アドレスと宛先ポート番号に対する複数のセキュア SIP トランクの設定をサポートします。 これには、以下の新しい機能や利点があります。 • 帯域幅の最適化：緊急コール用に帯域幅が制限されないルートを提供します。 • 特定のリージョンまたはコーリング サーチ スペースの設定に基づく選択的ルーティング

機能	説明
複数の非セキュア SIP トランクを同じ宛先に接続する	異なるリスニングポートを持つ複数の非セキュア SIP トランクが同じ宛先またはポートを指している場合、通話中の INVITE でそのポートが誤って使用される可能性があります。 したがって、通話は切断されます。
Unified Communications Manager は SIP 180 Ringing の受信時に SIP-UPDATE メッセージを送信する	コールフローで「UPDATE」の値がサポートされている場合、SIP トランクは「183 Session Progress」後に「180 Ringing」を受信すると「UPDATE」SIP メッセージを送信します。
BFCP を使用したプレゼンテーション共有	シスコのエンドポイント向けにプレゼンテーション共有を導入する場合は、すべての中継 SIP トランクの SIP プロファイルで [BFCPを使用したプレゼンテーション共有を許可（Allow Presentation Sharing with BFCP）]チェックボックスがオンになっていることを確認します。 （注） サードパーティ SIP エンドポイントの場合は、**[電話の設定（Phone Configuration）]** ウィンドウでも同じチェックボックスがオンになっていることを確認してください。
IX チャネル	iX メディア チャネルを導入する場合は、すべての中継 SIP トランクでて使用される SIP プロファイルで [iXアプリケーションメディアを許可（Allow iX Application Media）]チェックボックスがオンになっていることを確認します。 （注） 暗号化済の iX チャネルの詳細については、『*Cisco Unified Communications Manager* セキュリティガイド』を参照してください。
90 日間の評価ライセンス	90 日の評価期間を使用して実行している間、セキュア SIP トランクを導入することはできません。 セキュア SIP トランクを導入するには、製品登録トークンで [エクスポート管理された機能を許可（Allow export-controlled functionality）] を選択した Smart Software Manager アカウントにシステムを登録してある必要があり ます。

H.323 トランクの概要

H.323 を導入している場合は、H.323 トランクがリモート クラスタと、ゲートウェイなどのその他の H.323 デバイスに接続を提供します。 H.323 トランクは、Unified Communications Manager がクラスタ内通信でサポートする音声コーデックおよびビデオコーデックのほとんどをサポートします。ただし、広帯域音声および広帯域ビデオについてはサポートしません。H.323 トランクは、コール制御シグナリング用に H.225 プロトコルを使用し、メディア シグナリング用に H.245 プロトコルを使用します。

Cisco Unified CM Administration で、クラスタ間トランク（ゲートキーパー非制御）トランクタイプとプロトコルオプションを使用して H.323 トランクを設定できます。

非ゲートキーパー H.323 導入環境の場合は、Unified Communications Manager が IP WAN 経由でコールできるように、リモート クラスタ内の各デバイス プールに個別のクラスタ間トランクを設定する必要があります。 クラスタ間トランクは、リモート デバイスの IPv4 アドレスまたはホスト名を静的に指定します。

単一のトランクには最大 16 件の宛先アドレスを設定できます。

クラスタ間トランク

2 つのリモート クラスタ間にクラスタ間トランク接続を設定する場合は、一方のトランクが使用する宛先アドレスがリモート クラスタのトランクが使用するコール処理ノードと一致するように、クラスタごとにクラスタ間トランクを設定し、トランク設定を一致させる必要があります。 次に例を示します。

- リモート クラスタ トランクが [すべてのアクティブ ノードで実行（Run on all Active Nodes）] を使用する：リモート クラスタ トランクは、コール処理とロード バランシングにすべてのノードを使用します。 ローカル クラスタ内から始まるローカル クラスタ間トランクでは、リモート クラスタ内の各サーバの IP アドレスまたはホスト名を追加します。
- リモート クラスタで [すべてのアクティブ ノードで実行（Run on all Active Nodes）] を使用しない：リモート クラスタ トランクは、コール処理およびロード バランシング用にトランクのデバイス プールに割り当てられた Unified Communications Manager グループのサーバを使用します。 ローカルのクラスタ間トランク設定では、リモートクラスタトランクのデバイス プールで使用される Unified Communications Manager グループから各ノードの IP アドレスまたはホスト名を追加する必要があります。

セキュアなトランク

H.323 トランクのセキュアなシグナリングを設定するには、トランクに IPSec を設定する必要があります。 詳細については、『*Cisco Unified Communications Manager* セキュリティ ガイド』を参照してください。 メディア暗号化を許可するようにトランクを設定するには、**[トランクの設定（Trunk Configuration）]** ウィンドウで [SRTP を許可する（SRTP allowed）] チェックボックスをオンにします。

（注） ゲートキーパーは今では広く使用されていませんが、ゲートキーパー制御のトランクを使用するように H.323 導入を設定することもできます。 ゲートキーパーが制御するトランクを設定する方法の詳細については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド リリース *10.0(1)*』を参照してください。

H.323 トランクの前提条件

「H-323」導入トポロジーを計画します。 クラスタ間のトランクについては、対応するリモートクラスタがコール処理とロードバランシングに使用されるサーバを認識していることを確認してください。 リモートクラスタ内のトランクによって使用される各コール処理サーバに接続するには、ローカルインタークラスタトランクを設定する必要があります。

トランクでのロードバランシングのためにトランクデバイスプールに割り当てられた Cisco Unified Communications Manager グループを使用している場合は、デバイス プールのコア設定の設定タスク フローの設定を実行します。

H.323 トランクの設定

次の手順を使用して、トランク導入のための設定を構成します。

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 [新規追加] をクリックします。

ステップ 3 **中継タイプドロップダウンリストボックス**から、**クラスタ間中継（非ゲートウェイ保護装置制御）**を選択する。

ステップ 4 **[プロトコル(Protocol)]** ドロップダウン リスト ボックスから、**[SCCP]** を選択します。

ステップ 5 [**デバイス名 (**Device Name)] テキストボックスに、トランクの一意の識別子を入力します。

ステップ 6 [**デバイスプール (**device pool)] ドロップダウンリストボックスで、このトランクに設定したデバイスプールを選択します。

ステップ 7 ローカルクラスタ内のすべてのノードをこのトランクの処理用に使用する場合は、**[すべてのアクティブな統合 CM** ノード上で実行 (Run)] チェックボックスをオンにします。

ステップ 8 トランクでの暗号化メディアを許可する場合は、[**srtp 許可** (srtp)] チェックボックスをオンにします。

ステップ 9 H. 235 パススルーを設定する場合は、**h-235 パススルーを許可**するチェックボックスをオンにします。

ステップ 10 リモート Cisco **Unified Communications Manager の情報**セクションで、このトランクの接続先のリモートサーバごとに 1 つの IP アドレスまたはホスト名を入力します。

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。