セキュアな電話会議リソースのセットアップ

この章では、安全な電話会議リソースの設定について説明します。

セキュアな会議

セキュアな会議機能は、会議をセキュアにするための認証と暗号化を提供します。すべての参加デバイスでシグナリングとメディアが暗号化されている場合、会議は安全であると見なされます。 セキュアな電話会議機能は、セキュアな TLS または IPSec 接続での SRTP 暗号化をサポートします。

システムは、参加しているデバイスの最も低いセキュリティレベルによって決定される、会議の全体的なセキュリティステータスに対してセキュリティアイコンを提供します。 たとえば、2 つの暗号化された接続と 1 つの認証された接続を含む安全な会議の会議セキュリティ ステータスは認証済みです。

安全なアドホックおよびミートミー会議を設定するには、安全な会議ブリッジを設定します。

- ユーザが認証または暗号化された電話から会議通話を開始すると、 Unified Communications Manager がセキュアな会議ブリッジを割り当てます。
- ユーザが非セキュア電話から発信すると、 Unified Communications Manager は非セキュア電話会議ブリッジを割り当てます。

会議ブリッジ リソースをノンセキュアとして設定すると、電話のセキュリティ設定に関係なく、電話会議はノンセキュアのままになります。

（注） Unified Communications Manager は、電話会議を開始する電話の Media Resource Group List (MRGL) から会議ブリッジを割り当てます。 安全な会議ブリッジが利用できない場合、 Unified Communications Manager はノンセキュアな会議ブリッジを割り当て、会議はノンセキュアです。 安全な会議ブリッジが利用できない場合、 Unified Communications Manager はノンセキュアな会議ブリッジを割り当て、会議はノンセキュアです。 利用できる会議ブリッジがない場合、会議は失敗します。

ミートミーコンファレンスコールの場合、電話会議を開始する電話は、ミートミー番号に設定されている最小のセキュリティ要件も満たす必要があります。 セキュアなコンファレンスブリッジを利用できない場合、または開始者のセキュリティレベルが最低要件を満たさない場合、 Unified Communications Manager は電話会議を拒否します。

割り込みで電話会議をセキュアにするには、暗号化モードを使用するように電話を設定します。 割り込みキーが押され、デバイスが認証または暗号化された後、 Unified Communications Manager が割り込み側とターゲットデバイスの内蔵ブリッジの間の安全な接続を確立します。 システムは、バージコールに接続しているすべての側に対して、電話会議のセキュリティ ステータスを提供します。

（注） リリース 8.3 以降を実行している非セキュアまたは認証済み Cisco Unified IP Phone は、暗号化されたコールを割り込みできます。

会議ブリッジの要件

ハードウェアの Conference ブリッジをネットワークに追加し、Unified Communications Manager の管理でセキュアな会議ブリッジを設定するときに、会議ブリッジをセキュアなメディアリソースとして登録できます。

（注） Unified Communications Manager の処理に対するパフォーマンスの影響により、Cisco はソフトウェア会議ブリッジでのセキュアな電話会議をサポートしていません。

H.323 またはMGCP ゲートウェイ上で電話会議を提供するデジタル シグナル プロセッサ (DSP) ファームは、IP 電話会議のネットワーク リソースとして機能します。 コンファレンスブリッジは、セキュアな SCCP クライアントとしてUnified Communications Managerに登録されます。

- コンファレンスブリッジのルート証明書は、CallManagerの信頼ストアに存在している必要があり、 Cisco CallManager 証明書は、コンファレンスブリッジの信頼ストアに存在している必要があります。
- セキュアな電話会議ブリッジのセキュリティ設定が、登録する Unified Communications Manager のセキュリティ設定と一致している必要があります。

電話会議ルーターの詳細については、ルーターに付属の IOS ルーターのマニュアルを参照してください。

Unified Communications Manager は、動的に電話会議リソースを通話に割り当てます。 利用可能な電話会議リソースと有効なコーデックにより、ルーターごとに同時に開催できるセキュアな電話会議の最大数が決まります。 送信および受信のストリームは、参加しているエンドポイントごとに個別にキーイングされるため (参加者が電話会議を退席したときに、キーの再生成は必要ありません)、DSP モジュールのセキュアな電話会議の総容量は、設定できるノンセキュアな容量の 2 分の 1 になります。

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。

セキュア電話会議アイコン

Cisco IP Phone には、電話会議全体のセキュリティレベルに応じた電話会議セキュリティアイコンが表示されます。 これらのアイコンは、お使いの電話機のユーザ ドキュメントに記載されている安全な 2 者間コールのステータス アイコンと対応しています。

通話の音声とビデオの部分が、電話会議のセキュリティレベルの基礎となります。音声とビデオの両方が安全である場合に限り、通話は安全であると見なされます。

アドホックおよび Meet-Me セキュア会議では、電話会議のセキュリティ アイコンが、電話会議参加者に対して電話ウィンドウの電話会議ソフトキーの隣に表示されます。 表示されるアイコンは、電話会議ブリッジとすべての参加者のセキュリティレベルによって異なります。

- 会議ブリッジがセキュアで、電話会議のすべての参加者が暗号化されている場合は、ロックアイコンが表示されます。
- 会議ブリッジがセキュアで、電話会議のすべての参加者が認証されている場合は、盾アイコンが表示されます。 一部の電話モデルでは盾のアイコンが表示されません。
- 会議ブリッジまたは電話会議の参加者が非セキュアの場合、コール状態アイコン（アクティブ、保留など）が表示されます。一部の古い電話機モデルでは、アイコンは表示されません。

（注） パラメータ値が True で、音声が保護されている場合、「コールセキュリティステータスを指定するときにBFCPアプリケーション暗号化ステータスを上書きする（Override BFCP Application Encryption Status When Designating Call Security Status）] サービスパラメータはロックアイコンを表示します。 この条件は、他のすべてのメディア チャンネルのセキュリティ ステータスを無視します。 既定のパラメータ値は False です。

暗号化された電話がセキュアな会議ブリッジに接続すると、デバイスと会議ブリッジ間のメディアストリーミングが暗号化されます。ただし、会議のアイコンは、他の参加者のセキュリティレベルにより、暗号化される、認証される、または非セキュアになることがあります。非セキュアなステータスは、参加者の一部が安全ではない、または確認できないことを示します。

ユーザーが [バージ（Barge）] を押すと、[バージ（Barge）] ソフトキーの隣に表示されるアイコンが、会議のバージのセキュリティレベルを表示します。割り込みデバイスと割り込みデバイスが暗号化をサポートしている場合、システムは2つのデバイス間のメディアを暗号化しますが、割り込み会議のステータスは、接続者のセキュリティ レベルに応じて、非セキュア、認証済み、または暗号化になります。

セキュア電話会議の状況

参加者が電話会議に出入りするにつれて、電話会議の状況が変化します。認証された参加者または保護されていない参加者がコールに接続すると、暗号化された電話会議は認証されたまたは非セキュアなセキュリティレベルに戻ることができます。同様に、認証済みの参加者または安全ではない参加者が通話を切断した場合、状況は改善できます。セキュアではない参加者が電話会議に接続すると、電話会議が非セキュアになります。

電話会議の状況は、参加者が複数の電話会議を連鎖させるとき、連結された電話会議のセキュリティ状況が変更されるとき、保留中の電話会議が別のデバイスで再開されるとき、電話会議が割り込まれたとき、または転送された電話会議が別のデバイスに完了したときにも変更できます。

（注） Advanced Ad Hoc Conference Enabled サービスパラメータは、複数のアドホック会議を電話会議、参加、直接転送、転送などの機能を使用して相互にリンクできるかどうかを決定します。

Unified Communications Managerには、安全な電話会議を開催するためのオプションが用意されています。

- アドホック会議リスト
- 最低セキュリティ レベルの Meet-Me 電話会議

Ad Hoc 電話会議のリスト

電話会議中にConfListソフトキーを押すと、参加している電話機に電話会議リストが表示されます。各参加者の電話会議の状況およびセキュリティ状況を提供する電話会議リストは、暗号化されていない参加者を識別するために使用されます。

電話会議リストに表示されるセキュリティアイコンは、非セキュア、認証済み、暗号化、保留中です。 電話会議の開始者は電話会議リストを使用して、低セキュリティ ステータスの参加者を退出させることができます。

（注） Advanced Ad Hoc Conference Enabled サービスのパラメータにより、電話会議の開始者以外の参加者が会議参加者を退席させることができるかどうかが決定されます。

参加者が電話会議に参加すると、電話会議リストの一番上に追加されます。 ConfListおよびRmLstCソフトキーを使用して、セキュアな電話会議からセキュアではない参加者を削除するには、電話のユーザ ドキュメントを参照してください。

次のセクションでは、他の機能とのセキュアなアドホック会議の対話について説明します。

セキュアなアドホック会議と会議のチェーン

アドホック電話会議が別のアドホック電話会議に連結されている場合、連結された電話会議は、固有のセキュリティステータスを持つメンバー 「会議」 として表示されます。 Unified Communications Manager は、連結された会議のセキュリティレベルを含めて、電話会議全体のセキュリティ状況を判断します。

セキュアな Ad Hoc 電話会議と cBarge

ユーザがアクティブな電話会議に参加するために cBarge ソフトキーを押すと、 Unified Communications Manager がアドホック会議を作成し、割り込みのセキュリティレベルと MRGL に基づいて会議ブリッジを割り当てます。 cbarge メンバーの名前が電話会議リストに表示されます。

セキュアな Ad Hoc 電話会議と cBarge

セキュアなアドホック電話会議の参加者が割り込みを受けた場合、電話会議リストの割り込みターゲットの隣に、割り込みコールのセキュリティ ステータスが表示されます。割り込みターゲットのセキュリティアイコンは、実際には割り込みターゲットと電話会議ブリッジの間でメディアが暗号化されている場合でも、認証済みと表示される場合があります。これは、割り込み発信者には認証された接続があるためです。

割り込みのターゲットはセキュアですが、それがセキュアではないアドホック会議にある場合、アドホック会議の状況が後でセキュアに変更されると、割り込み発信者アイコンも更新されます。

セキュアな Ad Hoc 電話会議とジョイン

認証または暗号化された電話ユーザは、 Cisco Unified IP Phone (SCCP を実行している電話のみ) でJoin ソフトキーを使用して、セキュアなアドホック電話会議を作成したり、アドホック電話会議に参加したりできます。セキュリティステータスが未知の参加者を既存の電話会議に追加するためにユーザが [参加] を押した場合、 Unified Communications Manager は電話会議のステータスを不明に下げます。 [参加] で新しいメンバーを追加した参加者は電話会議の開始者になり、新しいメンバーや他の参加者を電話会議リストから外すことができます (Advanced Ad Hoc Conference Enabled 設定が True の場合)。

安全な Ad Hoc 電話会議および保留/再開

電話会議の開始者が、参加者を追加するために電話会議を保留にしても、電話会議のステータスは、追加された参加者が通話に応答するまで、不明 (非セキュア) のままになります。 新しい参加者が応答すると、電話会議リストの電話会議のステータスが更新されます。

共有回線上の発信者が別の電話で保留中の電話会議を再開した場合、発信者が [再開] を押すと、電話会議リストが更新されます。

最低セキュリティ レベルの Meet-Me 電話会議

管理者として、ミートミーコンファレンスのパターンまたは番号を非セキュア、認証、または暗号化として設定する場合、電話会議の最低セキュリティレベルを指定することができます。参加者はセキュリティの最低要件を満たさなければなりません。満たしていない場合、システムは参加者をブロックし、通話を切断します。このアクションは、ミートミーコンファレンスコールの転送、再開された共有回線上のミートミーコンファレンスコール、およびチェーンされたミートミーコンファレンスに適用されます。

ミートミーコンファレンスを開始する電話は、最低限のセキュリティレベルを満たす必要があります。満たさない場合、システムは試みを拒否します。最小セキュリティレベルが認証または暗号化を指定しており、セキュアな会議ブリッジが利用できない場合、通話は失敗します。

会議ブリッジングの最小レベルとして非セキュアを指定する場合、会議ブリッジングはすべての通話を受け入れ、会議のセキュリティステータスは非セキュアになります。

以下のセクションでは、他の機能との安全なミートミー電話会議の対話について説明します。

Meet-Me 電話会議および Ad Hoc 電話会議

ミートミー電話会議をアドホック会議に、またはアドホック会議をミートミー電話会議に追加するには、その Ad Hoc 電話会議がミートミー電話会議の最低セキュリティレベルを満たす必要があります。満たさない場合、通話は切断されます。 電話会議が追加されると、電話会議アイコンが変更されます。

Meet-Me 会議とバージ

発信者がミートミー電話会議の参加者にバージするときに、バージ発信者が最小セキュリティ要件を満たさない限り、バージデバイスのセキュリティレベルがダウングレードし、バージ発信者とバージコールの両方がドロップされます。

Meet-Me 電話会議およびホールド/リジューム

共有回線上の電話は、最低セキュリティレベルを満たさない限り、ミートミー電話会議を再開できません。 電話が最低セキュリティ レベルを満たしていない場合、ユーザが [再開] を押すと、共有回線上のすべての電話がブロックされます。

Cisco Unified IP Phone のセキュアな電話会議とアイコンのサポート

これらの Cisco Unified IP Phone はセキュアな会議とセキュアな会議のアイコンに対応しています:

- Cisco Unified IP Phones 7942 および 7962 (SCCP のみ、認証済みのセキュアな会議のみ)
- Cisco Unified IP Phone 6901、6911、6921、6941、6945、6961、7906G、7911G、 7921G、、79411、79411、7941, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 7970G, 7971G, 7971G-GE, 7975G, 8941, および 8945 (SCCP のみ)
- Cisco Unified IP Phone 6901, 6911, 6921, 6941, 6945, 6961, 7906G, 7911G, 7941G, 7941G-GE, 7942G, 7961G, 7961G-GE, 7962G, 7965G, 7970G, 7971G, 7971G-GE, 7975G, 8941, 8945, 8961, 9971, および 9971。

  Cisco IP 電話 7811、7821、7841、7861、 Cisco IP会議電話7832、 Cisco IP 電話 8811, 8841, 8845, 8851, 8851NR, 8861, 8865, 8865NR, Cisco ワイヤレスIP電話 8821, Cisco Unified IP会議電話 8831、 Cisco IP会議電話 8832。

警告 セキュアな電話会議機能を最大限に活用するには、 Cisco Unified IP Phone を 8.3 以降にアップグレードすることをおすすめします。このリリースの暗号化機能はサポートしています。 以前のリリースを実行する暗号化された電話はこれらの新機能を完全にサポートしません。 これらの電話はセキュアな電話会議に認証された参加者またはセキュアではない参加者としてのみ参加できます。

リリース 8.3 以前のリリースを使用している Unified Communications Manager で動作する Cisco Unified IP Phone は、接続のセキュリティステータスを表示し、会議のセキュリティステータスではない。会議リストのようなセキュアな会議機能はサポートしていません。

Unified Communications Manager のセキュアな会議の制限に関連するトピックを参照してください。これらの制限は Cisco Unified IP Phoneにも適用されます。

安全な電話会議およびセキュリティアイコンの詳細については、お使いの電話機の『管理ガイド』および『*Cisco IP* 電話ユーザガイド』を参照してください。

セキュアな会議 CTI サポート

Unified Communications Manager は、ライセンスを受けた CTI 端末でセキュアな会議をサポートします。 このリリースの『*Unified Communications Manager JTAPI* 開発者ガイド』および『*Unified Communications Manager TAPI* 開発者ガイド』を参照してください。

トランクおよびゲートウェイでのセキュアな電話会議

Unified Communications Manager は、クラスタ内トランク (ICT)、H.323 トランク/ゲートウェイ、MGCP ゲートウェイ経由で安全な電話会議をサポートします。ただし、リリース 8.2 またはそれ以前を実行している暗号化された電話は、ICT および H.323 コールに対して RTP に戻り、メディアは暗号化されません。

電話会議に SIP トランクが含まれる場合、セキュアな電話会議の状況は非セキュアになります。 さらに、SIP トランク シグナリングは、クラスタ外の参加者へのセキュアな会議通知をサポートしていません。

CDR データ

CDR データは、電話会議自体のセキュリティ ステータスだけでなく、電話エンドポイントから電話会議ブリッジまでの各コール レッグのセキュリティ ステータスを提供します。 2 つの値は、CDR データベース内の 2 つの異なるフィールドを使用します。

最低セキュリティレベル要件を満たしていない参加の試みがミートミー電話会議で拒否された場合、CDR データは終了原因コード 58 (ベアラー機能は現在利用できません) を提供します。詳細については、『 *CDR* 分析およびレポート管理ガイド 』を参照してください。

連携動作と制限事項

このセクションには次の項目に関する情報が記載されています:

• Cisco Unified Communications Manager とセキュアな電話会議との相互作用 （8 ページ）
• セキュアな電話会議での Cisco Unified Communications Manager の制限 （9 ページ）

Cisco Unified Communications Manager とセキュアな電話会議との相互作用

このセクションでは、 Unified Communications Manager の安全な電話会議機能に関する制限について説明します。

- 電話会議の安全性を維持するために、安全なアドホック電話会議の参加者がコールを保留またはパークした場合、Suppress MOH toConference Bridge サービス パラメータが False に設定されている場合でも、システムはMOHを再生しません。 セキュアな電話会議の状況は変わりません。
- クラスター間環境で、セキュアなアドホック会議でクラスター外の参加者が保留を押すと、デバイスへのメディアストリームが停止し、保留中の音楽が再生され、メディア ステータスが不明に変更されます。 クラスター外の参加者がMOHで保留中の通話を再開すると、電話会議のステータスがアップグレードされる場合があります。
- リモート ユーザがメディア ステータスを不明に変更する電話の機能を起動すると、クラスタ間トランク (ICT) 経由の安全な MeetMe コールが切断されます。
- Unified Communications Manager マルチレベル優先順位と優先権のアナウンス音または通知が、セキュアなアドホック会議中に参加者の端末で再生されると、会議のステータスが非セキュアに変更されます。
- 発信者がセキュアなSCCPコールにバージする場合、システムはターゲットデバイスで内部のトーン再生メカニズムを使用し、ステータスはセキュアなままです。
- 発信者がセキュアなSIP通話に乗り込む場合、システムは保留中の音を提供し、会議の状態は音の間は非セキュアのままとなります。
- 電話会議がセキュアで、RSVP が有効な場合、電話会議はセキュアなままです。
- PSTNが関与する電話会議の場合、セキュリティ電話会議アイコンは通話のIPドメイン部分のみのセキュリティ ステータスを表示します。
- 最大通話継続時間 タイマー サービス パラメータは、電話会議の最大継続時間を制御します。
- 電話会議ブリッジはパケットキャプチャをサポートしています。パケットキャプチャセッション中は、メディアストリームが暗号化されている場合でも、電話会議のノンセキュアステータスが表示されます。
- システムに設定されているメディアセキュリティポリシーにより、安全な電話会議の動作が変わる場合があります。例えば、メディアセキュリティをサポートしていないエンドポイントとの電話会議に参加する場合でも、エンドポイントはシステムのメディアセキュリティポリシーに従ってメディアセキュリティを使用します。

セキュアな電話会議での Cisco Unified Communications Manager の制限

このセクションでは、 Unified Communications Manager の安全な電話会議機能に関する制限について説明します。

- 暗号化された Cisco IP Phone で、リリース 8.2 またはそれ以前を実行しているユーザは、認証された参加者またはセキュアではない参加者としてのみセキュアな電話会議に参加することができます。

- リリース 8.3 以前のリリースを使用している Unified Communications Manager で動作する Cisco Unified IP Phone は、接続のセキュリティステータスを表示し、会議のセキュリティステータスではない。会議リストのようなセキュアな会議機能はサポートしていません。
- Cisco Unified IP Phone 7800 および 7911G はリスト会議をサポートしていません。
- 帯域幅の要件により、 Cisco Unified IP Phone 7942 および 7962 はアクティブな暗号化コールでの暗号化デバイスからの割り込みをサポートしていません。割り込みの試みは失敗します。
- Cisco Unified IP Phone 7931G は会議の連鎖に対応していません。
- SIP トランク経由で発信している電話は、デバイスのセキュリティ ステータスに関係なく、セキュアではない電話として扱われます。
- セキュアな電話が SIP トランク経由でセキュアな Meet-Me 電話会議に参加しようとすると、コールがドロップされます。 SIP トランクは、SIP を実行している電話への 「デバイスは認証されていません」 メッセージの提供をサポートしていないため、電話はこのメッセージで更新されません。 さらに、SIP を実行している 7962 電話は 「端末は認証されていません」 メッセージをサポートしていません。
- クラスター間環境では、電話会議リストにはクラスター外の参加者は表示されません。ただし、クラスタ間の接続でサポートされている限り、接続のセキュリティ ステータスは [電話会議] ソフトキーのとなりに表示されます。 たとえば、H.323 ICT 接続の場合、認証アイコンは表示されませんが、システムは認証された接続をセキュアではないものとして扱います。しかし暗号化された接続の場合は暗号化アイコンが表示されます。

  クラスター外の参加者は、クラスターの境界を越えて別のクラスターに接続する独自の電話会議を作成できます。 システムは、接続済みの電話会議を、2 者間での基本的なコールとして扱います。

電話会議リソースを保護するためのヒント

セキュアな会議ブリッジリソースを構成する前に、以下の情報を考慮してください。

- 電話会議のメッセージでカスタムテキストを表示させる場合は、ローカリゼーションを使用します。 詳細については、 Unified Communications Manager ロケールインストーラのドキュメントを参照してください。
- 電話会議または内蔵ブリッジは、セキュアな電話会議をサポートするために暗号化が必要です。
- 安全な電話会議ブリッジ登録を有効にするには、クラスタセキュリティモードを混合モードに設定します。
- 電話会議を開始する電話が認証済みまたは暗号化されており、セキュアな電話会議ブリッジを得ることを確認してください。

- 共有回線で電話会議の整合性を維持するために、異なるセキュリティモードで回線を共有するデバイスを設定しないでください。たとえば、暗号化された電話を、認証された電話や保護されていない電話と回線を共有するように設定しないでください。
- クラスタ間で電話会議のセキュリティ ステータスを共有する場合は、SIP トランクを ICT として使用しないでください。
- クラスタセキュリティモードを混合モードに設定する場合、DSP ファームに設定されているセキュリティモード (非セキュアまたは暗号化) は、 Unified Communications Manager 管理画面での電話会議ブリッジのセキュリティモードと一致していなければ、電話会議ブリッジは登録できません。両方のセキュリティモードで暗号化が指定されている場合、電話会議ブリッジは暗号化済みとして登録します。両方のセキュリティモードで非セキュアが指定されている場合、会議ブリッジは非セキュアとして登録されます。
- クラスタセキュリティモードを混合モードに設定し、電話会議ブリッジに適用したセキュリティ プロファイルが暗号化されているものの、電話会議ブリッジのセキュリティ レベルがセキュアではない場合、 Unified Communications Manager は、電話会議ブリッジの登録を拒否します。
- クラスタ セキュリティ モードをノンセキュア モードに設定する場合、DSP ファームでセキュリティモードをノンセキュアとして設定し、これにより会議ブリッジが登録できるようになります。 Unified Communications Manager 管理画面 で暗号化が指定されている場合でも、電話会議ブリッジがノンセキュアとして登録されます。
- 登録時に、電話会議ブリッジは認証に合格する必要があります。 認証を通過するためには、DSPファームシステムはUnified Communications Manager CallManager.pem証明書を1つ以上含んでいなければなりませんし、Unified Communications ManagerはDSPファームシステムとDSP接続の証明書をCallManager-trustストアに含んでいなければなりません。 X.509 サブジェクト属性で指定される共通名は、Cisco Unified Communications Manager とDSP ファームシステムで定義された会議ブリッジ名で始まる必要があり、関連する **profile <profile-identifier> を登録する <device-name>?** コマンドを使用します。 サブジェクト代替名属性はサポートされていません。 たとえば、証明書のサブジェクト共通名が ?CN=example.cisco.com? この場合、Unified Communications Manager の電話会議ブリッジ名は「example」でなければなりません。また、DSP ファームシステムコマンドは、**?associate Profile <profile-identifier> register** example でなければなりません。 同じ DSP ファームシステム上に複数のセキュアな電話会議ブリッジがある場合、それぞれが個別の証明書を必要とします。

ヒント　会議ブリッジ名が一意であること、および[デバイス]テーブルの下の他の場所で設定できないことを確認します。 これは、ルートリスト、SIP トランク、IP 電話などに適用されます。

- Cisco Unity 証明書の有効期限が切れたり、何らかの理由で変更されたりした場合は、『Cisco Unified Communications オペレーティング システム アドミニストレーション ガイド』の証明書管理機能を使用して、信頼できるストアの証明書を更新してください。証明書が一致

しない場合、TLS 認証は失敗します。また、電話会議ブリッジは Unified Communications Manager に登録できないため、機能しません。

- セキュアな会議ブリッジは、ポート 2443 の TLS 接続を介して Unified Communications Manager に登録します。セキュアではない会議ブリッジが、ポート 2000 の TCP 接続を介して Unified Communications Manager に登録します。
- コンファレンスブリッジのデバイスセキュリティモードを変更するには、 Unified Communications Manager デバイスをリセットし、Cisco CallManager サービスを再起動する必要があります。

セキュアな電話会議ブリッジのセットアップ

以下の手順は、ネットワークに安全な電話会議を追加するために使用されるタスクを提供します。

ステップ 1 混合モード用の CiscoCTL クライアントがインストールされ、構成されていることを確認します。

ステップ 2 Unified Communications Manager 接続用の DSP ファームのセキュリティ設定を確認します。これには、Unified Communications Manager の証明書をトラストストアに追加することも含まれます。 DSP ファームのセキュリティ レベルを暗号化に設定します。

お使いの電話会議ブリッジのドキュメントを参照してください。

ヒント DSP ファームは、 Unified Communications Manager への TLS ポート接続をポート 2443 で確立します。

ステップ 3 DSP ファーム証明書が CallManager 信頼ストアにあることを確認します。

証明書を追加するには、 Cisco Unified Communications オペレーティングシステム の証明書管理機能を使用して、DSP 証明書を Unified Communications Managerの信頼できるストアにコピーします。

証明書のコピーが完了したら、サーバ上の CiscoCallManager サービスを再起動してください。

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』および『*Cisco Unified Serviceability* アドミニストレーションガイド』を参照してください。

ヒント クラスタの各サーバに証明書をコピーし、クラスタの各サーバで CiscoCallManager サービスを再起動してください。

ステップ 4 Unified Communications Manager の管理で、会議ブリッジタイプとして Cisco IOS Enhanced 会議ブリッジを設定し、デバイスセキュリティモードに暗号化会議ブリッジを選択します。

ヒント このリリースにアップグレードすると、 Unified Communications Manager が自動的に非セキュア会議ブリッジセキュリティプロファイルを Cisco IOS Enhanced 会議ブリッジ構成に割り当てます。

ステップ 5 ミートミー電話会議の最低セキュリティレベルを設定します。

ヒント このリリースにアップグレードする際、Unified Communications Manager は自動的に非セキュアの最小セキュリティレベルをすべての Meet Me パターンに割り当てます。

ステップ 6 セキュアな電話会議ブリッジのパケットキャプチャを設定します。

詳細については、『トラブルシューティングガイド*Cisco Unified Communications Manager* トラブルシューティングガイド』を参照してください。

ヒント パケット キャプチャ モードをバッチ モードに設定し、キャプチャ層を SRTP に設定します。

Cisco Unified Communications Manager Administration でセキュアな電話会議ブリッジをセットアップする

Unified Communications Manager Administration でセキュアな電話会議を設定するには、次の手順を実行します。コンファレンスブリッジの暗号化を設定したら、Unified Communications Manager デバイスをリセットし、CiscoCallManager サービスを再起動する必要があります。

デバイス間の接続をセキュリティ保護するために、Unified Communications Manager と DSP ファームに証明書がインストールされていることを確認してください。

始める前に

事前準備

ステップ 1 **[メディアリソース（Media Resources）]** > **[会議ブリッジ（Conference Bridge）]** を選択します。

ステップ 2 [**会議ブリッジの検索と一覧表示**] ウィンドウで、Cisco IOS Enhanced Conference Bridgeがインストールされていることを確認し、次に移動します セキュアな電話会議ブリッジのセットアップ （12 ページ）。

ステップ 3 端末がデータベースに存在しない場合は、**[新規追加（Add New）]** をクリックし、Cisco Unified Communications Manager Administration でセキュアな電話会議ブリッジをセットアップする （13 ページ）に進みます。

ステップ 4 [電話会議ブリッジの設定] ウィンドウで、[**電話会議ブリッジタイプ**] ドロップダウンリストから **Cisco IOS Enhanced 会議ブリッジ** を選択します。『*Cisco Unified Communications Manager* 管理ガイド』の説明に従って、[電話会議ブリッジの名前]、[説明]、[デバイスプール]、[共通のデバイス構成]、[ロケーション] の設定を行います。

ステップ 5 [端末のセキュリティモード] フィールドで [**暗号化会議ブリッジ**] を選択します。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 [**リセット（Reset）**] をクリックします。

次のタスク

追加の会議ブリッジ設定タスクを実行するには、[ミートミー/番号パターンの設定] ウィンドウまたは [サービスパラメータの設定] ウィンドウに移動できます。これを行うには、[関連リンク] ドロップダウンリストボックスからオプションを選択し、[実行] をクリックします。

ミートミー電話会議の最低セキュリティレベルのセットアップ

ミートミー電話会議の最低セキュリティレベルを設定するには、次の手順を実行します。

ステップ 1 [**通話ルーティング** >] **ミートミー番号/パターンを選択します。**

ステップ 2 [電話会議ブリッジの検索と一覧表示] ウィンドウで、ミートミー番号/パターンが設定されていることを確認し、セキュアな電話会議ブリッジのセットアップ （12 ページ） に移動します。

ステップ 3 ミートミー番号/パターンが設定されていない場合は、 **新規追加** をクリックします。ミートミー電話会議の最低セキュリティレベルのセットアップ （14 ページ） に移動してください。

ステップ 4 [**Meet-Me番号設定**] ウィンドウの [ディレクトリ番号またはパターン] フィールドに、Meet-Me番号または範囲を入力します。 「 *Cisco Unified Communications Manager* 機能設定ガイド」の説明に従って、説明とパーティションを設定します。

ステップ 5 [最小セキュリティレベル（Minimum Security Level）] フィールドで、**[セキュリティ保護なし（Non Secure）]**、**[認証あり（Authenticated）]**、または **[暗号化（Encrypted）]** を選択します。

ステップ 6 **[保存（Save）]** をクリックします。

次のタスク

セキュアな会議ブリッジをまだインストールしていない場合は、セキュアな会議ブリッジをインストールして設定します。

セキュアな電話会議用のパケットキャプチャのセットアップ

セキュアな会議ブリッジのパケットキャプチャを設定するには、[**サービスパラメータ設定**] ウィンドウでパケットキャプチャを有効にします。次に、デバイス構成ウィンドウで、電話、ゲートウェイ、またはトランクに対して、パケット キャプチャ モードをバッチ モードに設定し、キャプチャ層を SRTP に設定します。 詳細については、『 トラブルシューティングガイド*Cisco Unified Communications Manager* トラブルシューティングガイド』を参照してください。

パケット キャプチャ セッション中は、メディア ストリームが暗号化されている場合でも、電話会議のノンセキュア ステータスが表示されます。

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。