CHAPTER 14

セキュアな会議リソースの設定

この章は、次の内容で構成されています。

- 「セキュアな会議の概要」（P.14-1）
- 「会議ブリッジの要件」（P.14-2）
- 「セキュアな会議のアイコン」（P.14-3）
- 「セキュアな会議の保守」（P.14-3）
- 「Cisco Unified IP Phone のサポート」（P.14-6）
- 「CTI サポート」（P.14-6）
- 「トランクおよびゲートウェイでのセキュアな会議」（P.14-6）
- 「CDR データ」（P.14-6）
- 「相互作用および制限」（P.14-7）
- 「会議リソースのセキュリティを確保するための設定のヒント」（P.14-8）
- 「セキュアな会議ブリッジの設定用チェックリスト」（P.14-9）
- 「Cisco Unified Communications Manager の管理でのセキュアな会議ブリッジの設定」（P.14-10）
- 「ミートミー会議の最小セキュリティ レベルの設定」（P.14-11）
- 「セキュアな会議ブリッジのパケット キャプチャの設定」（P.14-12）
- 「参考情報」（P.14-12）

セキュアな会議の概要

セキュアな会議機能では、会議の安全を確保するための認証と暗号化を提供します。接続されているすべてのデバイスでシグナリングおよび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ています。

システムには、会議の全体的なセキュリティ ステータスを示すセキュリティ アイコンが用意されています。セキュリティ ステータスは、接続されているデバイスのうち最も低いセキュリティ レベルで決まります。たとえば、2 つの暗号化済み接続と 1 つの認証済み接続を含むセキュアな会議の場合、会議のセキュリティ ステータスは、認証済みになります。

セキュアなアドホック会議とミートミー会議を設定するには、セキュアな会議ブリッジを設定します。

- 認証済みまたは暗号化済みの電話機からユーザが会議コールを開始すると、Cisco Unified Communications Manager はセキュアな会議ブリッジを割り当てます。
- 非セキュアな電話機からユーザがコールを開始すると、Cisco Unified Communications Manager は非セキュアな会議ブリッジを割り当てます。

会議ブリッジ リソースを非セキュアとして設定すると、電話機のセキュリティ設定に関わらず、会議は非セキュアになります。

（注） Cisco Unified Communications Manager は、会議を開始している電話機の Media Resource Group List（MRGL; メディア リソース グループ リスト）から会議ブリッジを割り当てます。セキュアな会議ブリッジが使用不可である場合、Cisco Unified Communications Manager は非セキュアな会議ブリッジを割り当て、会議は非セキュアになります。同様に、非セキュアな会議ブリッジが使用不可である場合、Cisco Unified Communications Manager はセキュアな会議ブリッジを割り当て、会議はセキュアになります。使用可能な会議ブリッジがない場合、コールは失敗します。

ミートミー会議コールの場合、会議を開始する電話機は、ミートミー番号用に設定された最小セキュリティ要件も満たしている必要があります。使用可能なセキュアな会議ブリッジがない場合や開催者のセキュリティ レベルが最小要件を満たしていない場合、Cisco Unified Communications Manager は会議の試行を拒否します。詳細については、「最小セキュリティ レベルでのミートミー会議」（P.14-5）を参照してください。

割り込みを使用する会議の安全を確保するには、暗号化済みモードを使用するよう電話機を設定します。デバイスが認証済みまたは暗号化済みである場合に割り込みキーを押すと、Cisco Unified Communications Manager によって割り込み側と発信先デバイスのビルトイン ブリッジとの間に安全な接続が確立されます。システムは、割り込みコールに接続されているすべての参加者に対して会議のセキュリティ ステータスを示します。

（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の Cisco Unified IP Phone は、暗号化済みコールに割り込むことができるようになりました。

会議ブリッジの要件

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

（注） Cisco Unified Communications Manager の処理のパフォーマンスに影響が及ぶため、ソフトウェア会議ブリッジ上のセキュアな会議はサポートされていません。

H.323 または MGCP ゲートウェイで会議を提供する Digital Signal Processor（DSP; デジタル シグナル プロセッサ）ファームは、IP テレフォニー会議のネットワーク リソースとして機能します。会議ブリッジは、セキュアな SCCP クライアントとして Cisco Unified Communications Manager に登録されます。

- 会議ブリッジのルート証明書が CallManager 信頼ストア内に存在し、Cisco Unified Communications Manager 証明書が会議ブリッジの信頼ストア内に存在している必要があります。
- セキュアな会議ブリッジのセキュリティ設定が、登録する Cisco Unified Communications Manager 内のセキュリティ設定と一致している必要があります。

会議ルータの詳細については、ご使用のルータに添付されている IOS ルータ マニュアルを参照してください。

Cisco Unified Communications Manager は、会議リソースをコールに動的に割り当てます。使用可能な会議リソースと有効なコーデックで、ルータごとに同時に使用可能なセキュアな会議の最大数が提供されます。送信ストリームと受信ストリームで、参加するエンドポイントごとにキーが個別に生成される（したがって、参加者が会議を離れるときにキーを再生成する必要がない）ので、DSP モジュールに対するセキュアな会議全体の容量は、設定可能な非セキュア容量の半分になります。

詳細については、『*Cisco Unified Communications Manager システム ガイド*』の「会議デバイスの概要」を参照してください。

セキュアな会議のアイコン

Cisco Unified IP Phone は、会議全体のセキュリティ レベルを示す会議セキュリティ アイコンを表示します。電話機のユーザ マニュアルで説明されているように、これらのアイコンは、安全な 2 者間のコールのステータス アイコンと同じです。

コールの音声とビデオ部分は、会議のセキュリティ レベルの基盤となります。音声とビデオの両方の部分が安全である場合に限り、コールは安全であると見なされます。

セキュアなアドホック会議およびミートミー会議の場合、会議のセキュリティ アイコンは、会議参加者の電話機のウィンドウで会議ソフトキーの横に表示されます。表示されるアイコンは、会議ブリッジおよび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すべての会議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すべての会議参加者が認証されている場合は、シールド アイコンが表示されます。一部の電話機モデルでは、シールド アイコンが表示されません。
- 会議ブリッジまたはいずれかの会議参加者が非セキュアである場合は、コール状態アイコン（アクティブ、保留中など）が表示されるか、旧式の電話機モデルではアイコンが表示されません。

暗号化された電話機がセキュアな会議ブリッジに接続する場合は、デバイスと会議ブリッジの間のメディア ストリームが暗号化されますが、会議のアイコンは、相手側のセキュリティ レベルに応じて、暗号化済み、認証済み、または非セキュアになります。非セキュア ステータスは、参加者のいずれかが非セキュアであるか、または確認できないことを意味します。

ユーザが [割込み] を押すと、[割込み] ソフトキーの横に表示されるアイコンが、割り込み会議のセキュリティ レベルを示します。割り込むデバイスと割り込まれるデバイスが暗号化をサポートしている場合、システムは両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、接続された参加者のセキュリティ レベルに応じて、非セキュア、認証済み、または暗号化済みになります。

セキュアな会議の保守

会議のステータスは、参加者が加わったときと退席したときに変わります。認証済みまたは非セキュアの参加者がコールに接続すると、暗号化された会議のセキュリティ レベルは認証済みまたは非セキュアに下がる場合があります。同様に、認証済みまたは非セキュアの参加者がコールを切断すると、ステータスは上がる場合があります。非セキュアの参加者が会議コールに接続すると、会議は非セキュアになります。

参加者が会議を結合した場合、結合した会議のセキュリティ ステータスが変わった場合、保留された会議コールが別のデバイスで再開された場合、会議コールに割り込みが入った場合、転送された会議コールが別のデバイスで終了した場合も、会議のステータスが変わる可能性があります。

（注）　Advanced Ad Hoc Conference Enabled サービス パラメータは、会議、参加、直接転送、転送などの機能を使用してアドホック会議を互いにリンクさせることができるかどうかを決定します。

Cisco Unified Communications Manager には、セキュアな会議を保守するため、次のオプションが用意されています。

- 「アドホック会議の会議リスト」（P.14-4）
- 「最小セキュリティ レベルでのミートミー会議」（P.14-5）

アドホック会議の会議リスト

会議リストは、会議コール中に [参加者] ソフトキーが押された場合に、参加者の電話機に表示されます。会議リストは、会議のステータスを示し、また、暗号化されていない参加者を特定するために各参加者のセキュリティ ステータスを示します。

会議リストは、非セキュア、認証済み、暗号化済み、保留中のセキュリティ アイコンを表示します。会議の開始者は、会議リストを使用して、セキュリティ ステータスの低い参加者を退席させることができます。

（注）　Advanced Ad Hoc Conference Enabled サービス パラメータは、会議の開始者以外の参加者が他の参加者を退席させることができるかどうかを決定します。

参加者は、会議に参加すると、会議リストの一番上に追加されます。非セキュアな参加者を [参加者] ソフトキーと [ドロップ] ソフトキーでセキュアな会議から削除する方法は、ご使用の電話機のユーザ マニュアルを参照してください。

次の各項では、セキュアなアドホック会議とその他の機能との相互作用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結合

アドホック会議が別のアドホック会議に結合されると、結合された会議はメンバー「Conference」としてそれ自体のセキュリティ ステータスとともにリストに表示されます。Cisco Unified Communications Manager は、会議全体のセキュリティ ステータスを判別するため、結合された会議のセキュリティ レベルを組み込みます。

セキュアなアドホック会議と C 割り込み

ユーザが [C 割込] ソフトキーを押してアクティブな会議に参加すると、Cisco Unified Communications Manager はアドホック会議を作成し、割り込まれるデバイスのセキュリティ レベルと MRGL に従って会議ブリッジを割り当てます。C 割り込みメンバー名が会議リストに表示されます。

セキュアなアドホック会議と割り込み

セキュアなアドホック会議の参加者に割り込みがあった場合は、会議リストで割り込み元の横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。割り込み元と会議ブリッジの間のメディアが暗号化済みであっても、割り込み発信者の接続が認証済みであるために、割り込み元のセキュリティ アイコンが認証済みとなる場合もあります。

割り込み元がセキュアでアドホック会議が非セキュアである場合に、アドホック会議のステータスが後からセキュアに変更されると、割り込み発信者のアイコンも更新されます。

セキュアなアドホック会議と参加

認証済みまたは暗号化済みの電話機ユーザは、Cisco Unified IP Phone（SCCP を実行する電話機のみ）の [参加] ソフトキーを使用して、セキュアなアドホック会議を作成またはそれに参加することができます。ユーザが [参加] を押してセキュリティ ステータスの不明な参加者を既存の会議に追加すると、Cisco Unified Communications Manager は会議のステータスを「不明」にダウングレードします。[参加] を使用して新規メンバーを追加した参加者は、会議の開始者になり、新規メンバーやその他の参加者を会議リストから退席させることができます（Advanced Ad Hoc Conference Enabled 設定が有効になっている場合）。

セキュアなアドホック会議と保留 / 復帰

会議の開始者が参加者を追加するため会議コールを保留にすると、追加された参加者がコールに応答するまで、会議のステータスは不明（非セキュア）になります。新規参加者が応答すると、会議リストで会議のステータスが更新されます。

シェアドライン上の発信者が保留中の会議コールを別の電話機で復帰する場合は、発信者が [復帰] を押したときに会議リストが更新されます。

最小セキュリティ レベルでのミートミー会議

管理者は、ミートミーのパターンまたは番号を非セキュア、認証済み、または暗号化済みとして設定する際に、会議の最小セキュリティ レベルを指定できます。参加者は、最小セキュリティ要件を満たしている必要があります。これを満たしていないと、システムは参加者をブロックして、コールを切断します。このアクションは、ミートミー会議コール転送、シェアドラインで復帰されたミートミー会議コール、結合したミートミー会議に適用されます。

ミートミー会議を開始する電話機は、最小セキュリティ レベルを満たしている必要があります。これを満たしていないと、システムは試行を拒否します。最小セキュリティ レベルが認証済みまたは暗号化済みを指定していて、セキュアな会議ブリッジが使用不可である場合、コールは失敗します。

会議ブリッジの最小レベルに非セキュアを指定すると、会議ブリッジはすべてのコールを受け入れ、会議のステータスは非セキュアになります。ミートミー会議の安全を確保する方法は、「ミートミー会議の最小セキュリティ レベルの設定」（P.14-11）を参照してください。

次の各項では、セキュアなミートミー会議とその他の機能との相互作用について説明します。

ミートミー会議とアドホック会議

ミートミー会議をアドホック会議に追加したりアドホック会議をミートミー会議に追加したりするには、アドホック会議がミートミー会議の最小セキュリティ レベルを満たしている必要があります。これを満たしていないと、コールは切断されます。会議が追加されると、会議アイコンが変わります。

ミートミー会議と割り込み

ある発信者がミートミー会議の参加者に割り込んだ場合にその割り込み発信者が最小セキュリティ要件を満たしていないと、割り込まれたデバイスのセキュリティ レベルがダウングレードし、割り込み発信者と割り込まれたコールの両方が切断されます。

ミートミー会議と保留 / 復帰

シェアドラインの電話機は、最小セキュリティ レベルを満たしていない限り、ミートミー会議を復帰できません。電話機が最小セキュリティ レベルを満たしていない場合にユーザが [復帰 (Resume)] を押すと、シェアドライン上のすべての電話機がブロックされます。

Cisco Unified IP Phone のサポート

次の Cisco Unified IP Phone は、セキュアな会議とセキュアな会議アイコンをサポートしています。

- Cisco Unified IP Phone 7940G および 7960G（SCCP のみ、認証済みのセキュアな会議のみ）
- Cisco Unified IP Phone 7906G、7911G、および 7931G（SCCP のみ）
- Cisco Unified IP Phone 7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、7962G、7965G、7970G、7971G、7971G-GE、および 7975G

警告　**セキュアな会議機能をフルに活用するため、暗号化機能をサポートするリリース 8.3 に Cisco Unified IP Phone をアップグレードすることをお勧めします。それより前のリリースを実行している暗号化済みの電話機では、これらの新機能が完全にはサポートされません。これらの電話機では、認証済みまたは非セキュアの参加者としてだけセキュアな会議に参加できます。**

Cisco Unified Communications Manager の以前のリリースとともにリリース 8.3 を実行している Cisco Unified IP Phone では、会議コール中に会議のセキュリティ ステータスではなく接続のセキュリティ ステータスが表示されます。また、会議リストなどのセキュアな会議機能はサポートされません。

Cisco Unified IP Phone に当てはまる制限の詳細については、「制限」（P.14-8）を参照してください。

セキュアな会議コールとセキュリティ アイコンの詳細については、ご使用の電話機のユーザ ガイドと、今回の Cisco Unified Communications Manager リリースをサポートする『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』を参照してください。

CTI サポート

Cisco Unified Communications Manager は、ライセンス済み CTI デバイスでのセキュアな会議をサポートしています。詳細については、今回のリリースの『*Cisco Unified Communications Manager JTAPI Developers Guide*』および『*Cisco Unified Communications Manager TAPI Developers Guide*』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会議

Cisco 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、および MGCP ゲートウェイを介したセキュアな会議をサポートしています。ただし、リリース 8.2 以前を実行している暗号化済みの電話機は、ICT および H.323 コールの場合は RTP に戻り、メディアは暗号化されません。

会議に SIP トランクが含まれる場合、セキュアな会議のステータスは非セキュアになります。また、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、会議自体のセキュリティ ステータスに加えて、電話機エンドポイントから会議ブリッジへの各コール レッグのセキュリティ ステータスも示します。CDR データベース内では、2 つの値が 2 つの異なるフィールドを使用します。

最小セキュリティ レベル要件を満たしていない参加試行をミートミー会議が拒否した場合、CDR データは終了原因コード 58（ベアラ機能を現在使用できない）を示します。詳細については、『*CDR Analysis and Reporting Administration Guide*』を参照してください。

相互作用および制限

この項では、次のトピックについて取り上げます。

- 「相互作用」（P.14-7）
- 「制限」（P.14-8）

相互作用

この項では、Cisco Unified Communications Manager とセキュアな会議機能との相互作用について説明します。

- 会議の安全を保つため、Suppress MOH to Conference Bridge サービス パラメータが False に設定されている場合でも、セキュアなアドホック会議の参加者がコールを保留にしたりコールをパークしたとき、システムは MOH を再生しません。セキュアな会議のステータスは変わりません。
- クラスタ間環境では、クラスタ外の会議参加者がセキュアなアドホック会議で保留を押すと、デバイスへのメディア ストリームが停止し、MOH が再生され、メディアのステータスが不明に変わります。クラスタ外の参加者が MOH 付きの保留コールを再開すると、会議のステータスは上がります。
- リモート ユーザが保留/復帰などの電話機能を起動すると、メディアのステータスが不明に変わり、クラスタ間トランク（ICT）でのセキュアなミートミー コールは消去されます。
- Cisco Unified Communications Manager Multilevel Precedence and Preemption 用のアナンシエータのトーンやアナウンスメントがセキュアなアドホック会議中に参加者の電話機で再生されると、会議のステータスは非セキュアに変わります。
- 発信者がセキュアな SCCP 電話機コールに割り込んだ場合、システムは発信先デバイスで内部トーン再生メカニズムを使用し、会議のステータスはセキュアに保たれます。
- 発信者がセキュアな SIP 電話機コールに割り込んだ場合、システムは保留トーンを再生し、その間、会議のステータスは非セキュアになります。
- 会議がセキュアで RSVP が有効である場合、会議はセキュアに保たれます。
- PSTN を含む会議コールでは、コールの IP ドメイン部分のセキュリティ ステータスだけがセキュリティ会議アイコンで示されます。
- Maximum Call Duration Timer サービス パラメータは、最大会議期間も制御します。
- 会議ブリッジは、パケット キャプチャをサポートします。メディア ストリームが暗号化済みであっても、パケット キャプチャ セッション中、電話機は会議について非セキュア ステータスを示します。
- ご使用のシステムに対して設定されているメディア セキュリティ ポリシーがセキュアな会議の動作を変える場合があります。たとえば、エンドポイントは、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会議コールに参加している場合でも、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。

制限

この項では、セキュアな会議機能でのCisco Unified Communications Manager の制限について説明します。

- リリース 8.2 以前を実行している暗号化済みの Cisco Unified IP Phone は、認証済みまたは非セキュアの参加者としてしかセキュアな会議に参加できません。
- Cisco Unified Communications Manager の以前のリリースとともにリリース 8.3 を実行している Cisco Unified IP Phone では、会議コール中に会議のセキュリティ ステータスではなく接続のセキュリティ ステータスが表示されます。また、会議リストなどのセキュアな会議機能はサポートされません。
- Cisco Unified IP Phone 7905G および 7911G は会議リストをサポートしていません。
- 帯域幅要件のため、Cisco Unified IP Phone 7940G および 7960G は、アクティブな暗号化済みコールへの暗号化済みデバイスからの割り込みをサポートしません。割り込みを試みると失敗します。
- Cisco Unified IP Phone 7931G は会議の結合をサポートしていません。
- SIP トランクを介して発信している電話機は、そのデバイスのセキュリティ ステータスにかかわらず、非セキュアの電話機として扱われます。
- セキュアな電話機が SIP トランクを介してセキュアなミートミー会議に参加しようとすると、コールは切断されます。SIP トランクは、SIP を実行する電話機への「認証されていないデバイス」のメッセージの提供をサポートしていないので、電話機はこのメッセージで更新されません。また、SIP を実行する 7960G 電話機も「認証されていないデバイス」のメッセージをサポートしていません。
- クラスタ間では、クラスタ外の参加者に対して会議リストは表示されませんが、クラスタ間の接続でサポートされていれば、接続のセキュリティ ステータスは [会議] ソフトキーの横に表示されます。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（システムは認証済み接続を非セキュアとして扱います）、暗号化済み接続に対する暗号化アイコンは表示されます。

  クラスタ外の参加者は、クラスタ境界を越えて別のクラスタへ接続する独自の会議を作成できます。システムは、接続された会議を基本的な 2 通話者間コールとして扱います。

会議リソースのセキュリティを確保するための設定のヒント

セキュアな会議ブリッジのリソースを設定する前に、次の情報を考慮に入れてください。

- セキュアな会議メッセージ用のカスタム テキストを電話機で表示する場合は、ローカリゼーションを使用します。詳細については、Cisco Unified Communications Manager Locale Installer のマニュアルを参照してください。
- 会議またはビルトイン ブリッジは、会議コールの安全を確保するため、暗号化をサポートしている必要があります。
- セキュアな会議ブリッジ登録を有効にするには、クラスタのセキュリティ モードを混合モードに設定します。
- セキュアな会議ブリッジを確立するため、会議を開始する電話機が認証済みまたは暗号化済みであることを確認してください。
- シェアドラインでの会議の整合性を保つため、回線を共有するデバイスを別々のセキュリティ モードで設定することはしないでください。たとえば、暗号化済みの電話機が認証済みまたは非セキュアな電話機と回線を共有するように設定することはしないでください。
- クラスタ間で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。

- クラスタのセキュリティ モードを混合モードに設定する場合は、DSP ファーム用に設定されたセキュリティ モード（非セキュアまたは暗号化済み）が Cisco Unified Communications Manager の管理の会議ブリッジのセキュリティ モードと一致している必要があります。一致していないと、会議ブリッジは登録されません。両方のセキュリティ モードが暗号化済みと指定されていれば、会議ブリッジは暗号化済みとして登録されます。両方のセキュリティ モードが非セキュアと指定されていれば、会議ブリッジは非セキュアとして登録されます。
- クラスタのセキュリティ モードを混合モードに設定し、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済みで会議ブリッジのセキュリティ レベルが非セキュアである場合、Cisco Unified Communications Manager は会議ブリッジの登録を拒否します。
- クラスタのセキュリティ モードを非セキュア モードに設定する場合は、会議ブリッジが登録されるよう、DSP ファームのセキュリティ モードを非セキュアに設定してください。Cisco Unified Communications Manager の管理での設定が暗号化済みであっても、会議ブリッジは非セキュアとして登録されます。
- 登録時に、会議ブリッジは認証に合格する必要があります。認証に合格するには、DSP ファームに Cisco Unified Communications Manager 証明書が含まれ、Cisco Unified Communications Manager に DSP ファーム システムの証明書と DSP 接続の証明書が含まれている必要があります。会議ブリッジが確実に認証に合格するためには、X.509 証明書名に会議ブリッジ名が含まれている必要があります。
- 会議ブリッジの証明書が失効したか、または何らかの理由で変更された場合は、Cisco Unified Communications オペレーティング システムの管理の証明書管理機能を使用して、信頼ストアの証明書を更新します。証明書が一致しないと TLS 認証は失敗し、会議ブリッジは Cisco 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 で TLS 接続を介して Cisco Unified Communications Manager に登録されます。非セキュアの会議ブリッジは、ポート 2000 で TCP 接続を介して Cisco Unified Communications Manager に登録されます。
- 会議ブリッジのデバイスのセキュリティ モードを変更するには、Cisco Unified Communications Manager デバイスをリセットして Cisco CallManager サービスを再起動する必要があります。

セキュアな会議ブリッジの設定用チェックリスト

ネットワークにセキュアな会議を追加するときには、表 14-1 を参照してください。

表 14-1　セキュアな会議ブリッジの設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	Cisco CTL クライアントを混合モードでインストールして設定したことを確認します。	「Cisco CTL クライアントの設定」（P.4-1）
ステップ 2	信頼ストアへの Cisco Unified Communications Manager 証明書の追加も含め、Cisco Unified Communications Manager 接続用の DSP ファーム セキュリティを設定したことを確認します。DSP ファームのセキュリティ レベルを暗号化済みに設定します。 **ヒント** DSP ファームは、ポート 2443 で Cisco Unified Communications Manager への TLS ポート接続を確立します。	ご使用の会議ブリッジのマニュアルを参照してください。

表 14-1　セキュアな会議ブリッジの設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 3	DSP ファーム証明書が CallManager 信頼ストア内にあることを確認してください。 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 Cisco Unified Communications Manager 内の信頼ストアにコピーします。 証明書のコピーが終わったら、サーバで Cisco CallManager サービスを再起動します。 **ヒント** 証明書はクラスタ内の各サーバにコピーし、クラスタ内の各サーバで Cisco CallManager サービスを再起動してください。	• 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』 • 『*Cisco Unified Serviceability Administration Guide*』
ステップ 4	Cisco Unified Communications Manager の管理で、Cisco IOS Enhanced Conference Bridge を会議ブリッジ タイプとして設定し、暗号化済み会議ブリッジをデバイスのセキュリティ モードとして選択します。 **ヒント** 今回のリリースにアップグレードすると、Cisco Unified Communications Manager は自動的に非セキュアな会議ブリッジ セキュリティ プロファイルを Cisco IOS Enhanced Conference Bridge 設定に割り当てます。	• 「会議リソースのセキュリティを確保するための設定のヒント」（P.14-8） • 「Cisco Unified Communications Manager の管理でのセキュアな会議ブリッジの設定」（P.14-10）
ステップ 5	ミートミー会議の最小セキュリティ レベルを設定します。 **ヒント** 今回のリリースにアップグレードすると、Cisco Unified Communications Manager は自動的に非セキュアな最小セキュリティ レベルをすべてのミートミー パターンに割り当てます。	「ミートミー会議の最小セキュリティ レベルの設定」（P.14-11）
ステップ 6	（オプション）セキュアな会議ブリッジのパケット キャプチャを設定します。 **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。	「セキュアな会議ブリッジのパケット キャプチャの設定」（P.14-12） 『*Troubleshooting Guide for Cisco Unified Communications Manager*』

Cisco Unified Communications Manager の管理でのセキュアな会議ブリッジの設定

Cisco Unified Communications Manager の管理ページでセキュアな会議ブリッジを設定するには、次の手順を実行します。会議ブリッジの暗号化を設定した後、Cisco Unified Communications Manager デバイスをリセットして、Cisco CallManager サービスを再起動する必要があります。

始める前に

デバイス間の接続を安全にするため、Cisco Unified Communications Manager と DSP ファームに証明書をインストールしたことを確認してください。

手順

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(Find and List Conference Bridges)] 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、ステップ 4 に進みます。

データベース内にデバイスが存在しない場合は、[新規追加(Add New)] をクリックし、ステップ 3 に進みます。

ステップ 3　[会議ブリッジの設定(Conference Bridge Configuration)] ウィンドウで、[会議ブリッジタイプ(Conference Bridge Type)] ドロップダウン リスト ボックスから [Cisco IOS Enhanced Conference Bridge] を選択します。『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の説明に従って、会議ブリッジ名、説明、デバイス プール、共通デバイス設定、およびロケーションを設定します。

ステップ 4　[デバイスセキュリティモード(Device Security Mode)] フィールドで、[Encrypted Conference Bridge] を選択します。

ステップ 5　[保存(Save)] をクリックします。

ステップ 6　[リセット(Reset)] をクリックします。

次の作業

その他の会議ブリッジ設定タスクを実行するため、[関連リンク(Related Links)] 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て [移動(Go)] をクリックし、[ミートミー番号の設定(Meet-Me Number Configuration)] ウィンドウまたは [サービスパラメータ設定(Service Parameter Configuration)] ウィンドウに移動します。

追加情報

「関連項目」（P.14-12）を参照してください。

ミートミー会議の最小セキュリティ レベルの設定

ミートミー会議の最小セキュリティ レベルを設定するには、次の手順を実行します。

手順

ステップ 1　[コールルーティング(Call Routing)] > [ミートミー番号/パターン(Meet-Me Number/Pattern)] 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(Find and List Conference Bridges)] 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、ステップ 4 に進みます。

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(Add New)] をクリックし、ステップ 3 に進みます。

ステップ 3　[ミートミー番号の設定(Meet-Me Number Configuration)] ウィンドウで、[電話番号またはパターン(Directory Number or Pattern)] フィールドにミートミー番号または範囲を入力します。『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の説明に従って、説明とパーティションの値を設定します。

ステップ 4　[最小セキュリティレベル(Minimum Security Level)] フィールドで、[非セキュア(Non Secure)]、[認証のみ(Authenticated)] または [暗号化(Encrypted)] を選択します。

ステップ 5　[保存(Save)] をクリックします。

次の作業

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、「Cisco Unified Communications Manager の管理でのセキュアな会議ブリッジの設定」（P.14-10）の説明に従って、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。

追加情報

「関連項目」（P.14-12）を参照してください。

セキュアな会議ブリッジのパケット キャプチャの設定

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 (Service Parameter Configuration)] ウィンドウでパケット キャプチャを有効にしてから、デバイス設定ウィンドウで電話機、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、『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照してください。

メディア ストリームが暗号化済みであっても、パケット キャプチャ セッション中、電話機は会議について非セキュア ステータスを示します。

参考情報

関連項目

- 「システム要件」（P.1-5）
- 「相互作用および制限」（P.1-7）
- 「証明書」（P.1-15）
- 「設定用チェックリストの概要」（P.1-25）
- 「セキュアな会議の概要」（P.14-1）
- 会議ブリッジの要件
- 「セキュアな会議のアイコン」（P.14-3）
- 「セキュアな会議の保守」（P.14-3）
- 「Cisco Unified IP Phone のサポート」（P.14-6）
- 「CTI サポート」（P.14-6）
- 「トランクおよびゲートウェイでのセキュアな会議」（P.14-6）
- 「相互作用および制限」（P.14-7）
- 「会議リソースのセキュリティを確保するための設定のヒント」（P.14-8）
- 「セキュアな会議ブリッジの設定用チェックリスト」（P.14-9）
- 「Cisco Unified Communications Manager の管理でのセキュアな会議ブリッジの設定」（P.14-10）
- 「ミートミー会議の最小セキュリティ レベルの設定」（P.14-11）
- 「セキュアな会議ブリッジのパケット キャプチャの設定」（P.14-12）

シスコの関連マニュアル

- 『*Cisco Unified Communications Manager システム ガイド*』の「会議ブリッジ」
- 『*Cisco Unified Communications Manager システム ガイド*』の「トランスコーディング、会議、および MTP 用の Cisco DSP リソース」
- 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「会議ブリッジの設定」
- 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「ミートミー番号/パターンの設定」
- 『*Cisco Unified Communications Operating System Administration Guide*』
- 『*Troubleshooting Guide for Cisco Unified Communications Manager*』
- 『*CDR Analysis and Reporting Administration Guide*』
- 『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』
- 今回のリリースの Cisco Unified Communications Manager およびご使用の Cisco Unified IP Phone の Cisco IP Phone ユーザ ガイドおよびリリース ノート