



セキュアなコールのモニタリングおよび録音のセットアップ

この章では、セキュアなコールのモニタリングおよび録音のセットアップについて説明します。

- [セキュア コールのモニタリングと録音のセットアップについて \(1 ページ\)](#)
- [セキュアなコールのモニタリングと録音のセットアップ \(2 ページ\)](#)

セキュアコールのモニタリングと録音のセットアップについて

セキュア コールは、この項で説明するようにモニタリングおよび録音を行えます。

- スーパバイザは、セキュア コールまたは非セキュア コールに対してセキュアなモニタリングセッションを確立できます。
- 元のコールのコールセキュリティが、コールモニタリング要求の結果として、影響を受けたりダウングレードされたりすることは決してありません。
- モニタリング コールは、エージェントのデバイス機能と同じセキュリティレベルで確立および維持できる場合に限り続行できます。
- エージェントとお客様間の元のコールには、モニタリングコールの暗号キーとは異なる暗号キーが必要です。モニタリングセッションでは、システムによってまずエージェントとお客様の混合音声 新しいキーで暗号化され、その後スーパバイザに送信されます。



(注) 認証された電話でのセキュアな録音またはセキュアでない録音はサポートされていません。

Unified Communications Manager は、安全でないレコーダーを使用しているときに、認証された電話の通話の録音をサポートしています。セキュアコールレコーダーを使用したコールの場合、レコーダーが SRTP フォールバックをサポートしている場合に限り録音が許可され、レコーダーに対するメディアストリームが RTP にフォールバックされます。

認証済みの電話機を使用したコールを録音するには:

- 電話を許可するには、Cisco callmanager Service パラメータで**認証済みの電話録音**を設定します。この場合、コールは認証されますが、録音サーバへの接続は非認証であり、暗号化されません。
- クラスタ **SIPOAuth Mode** フィールドが Cisco callmanager enterprise パラメータであることを確認します。[有効 (Enabled)] に設定されていることを確認します。

セキュアなコールのモニタリングと録音のセットアップ

セキュアなコールのモニタリングと録音を設定するには、次の手順を実行します。

手順

ステップ 1 エージェントとスーパーバイザの電話にセキュリティ機能をプロビジョニングします。

ステップ 2 次の設定を使用して、セキュアな SIP トランクを作成します。

- [Device Security Mode] を [Encrypted] に設定します。
- [Transmit Security Status] チェックボックスをオンにします。
- [SRTP Allowed] チェックボックスをオンにします。
- TLS SIP トランクをレコーダに設定します。

ステップ 3 非セキュアな場合と同様にモニタリングと録音を設定します。

- a) エージェントの電話のビルトインブリッジを設定します。
- b) エージェントの電話の DN ページを使用して、[Recording Option] ([Automatic Call Recording Enabled] と [Application Invoked Call Recording Enabled]) を設定します。
- c) レコーダのルート パターンを作成します。
- d) DN に通話録音プロファイルを追加します。
- e) 必要に応じてモニタリング トーンと録音トーンをプロビジョニングします。

手順の詳細については、『*Feature Configuration Guide for Cisco Unified Communications Manager*』の「**Monitoring and Recording**」の章を参照してください。