



# サイレント モニタリング

- ・サイレント モニタリングの概要 (1 ページ)
- ・サイレント モニタリングの前提条件 (2 ページ)
- ・サイレント モニタリングの設定タスク フロー (2 ページ)
- ・サイレント モニタリングの連携動作 (8 ページ)
- ・サイレント モニタリングの制約事項 (9 ページ)

## サイレント モニタリングの概要

サイレント コール モニタリングを使用すると、スーパーバイザが電話での会話を傍受できます。これが最も一般的に使用されるのは、コール エージェントが顧客と会話するコール センターです。コール センターでは、コール センターのエージェントが提供するカスタマー サービスの品質を保証できるようにする必要があります。サイレント モニタリングにより、スーパーバイザは、両方の通話者の声を聞くことができますが、どちらの通話者にもスーパーバイザの声は聞こえません。

サイレント モニタリングを呼び出すことができるのは、JTAPI または TAPI インターフェイスを介した CTI アプリケーションのみです。Cisco Unified Contact Center Enterprise や Cisco Unified Contact Center Express などのシスコの多数のアプリケーションには、サイレント モニタリングの機能があります。コールをモニタする CTI アプリケーションには、application-user または end-user アカウントについて有効な対応するモニタリング権限が必要です。

サイレント モニタリングはコール ベースです。スーパーバイザがサイレント モニタリング セッションを呼び出すと、以下が発生します。

- ・スーパーバイザは、モニタする特定のコールを選択します。
- ・アプリケーションからの開始モニタリング要求により、スーパーバイザの電話はオフフックとなり、エージェントに対するモニタリング コールが自動的にトリガーされます。
- ・エージェントの電話はモニタリングコールに自動で応答します。モニタリングコールは、エージェントに表示されません。

### セキュアサイレントモニタリング

セキュアサイレントモニタリングを設定することもできます。セキュアサイレントモニタリングにより、暗号化されたメディア（sRTP）コールのモニタリングが可能です。コールのモニタリングは、監視対象のコールのセキュリティステータスに関係なく、エージェントの電話の機能により決定される最高レベルのセキュリティを使用して常に確立されます。セキュリティの最高レベルは顧客、エージェント、およびスーパーバイザ間のいずれかのコールでのセキュアメディアキーの交換により維持されます。保護されたメディアを使用したコールのモニタリングにより、約4000bpsのさらなる帯域幅のオーバーヘッドが伝送されますが、これは標準的なセキュアメディア（sRTP）コールと同様です。

エージェントの電話で暗号化が有効になっている場合、セキュアサイレントモニタリングを可能にするにはスーパーバイザの電話でも暗号化が有効になっている必要があります。エージェントの電話で暗号化が有効になっているが、スーパーバイザの電話では有効になっていない場合、モニタリング要求は失敗します。

### ウィスパーコーチング

Unified Communications Manager 顧客が聞いていなくてもモニタリングセッションが実行されている一方で、スーパーバイザはエージェントと会話できるサイレントモニタリングでのCTI強化であるウィスパーコーチングもサポートしています。ウィスパーコーチングはCTIアプリケーションでのみ開始できます。サイレントモニタリングが既に設定されている場合、ウィスパーコーチングには Unified Communications Manager の追加設定は必要ありません。

## サイレントモニタリングの前提条件

サイレントモニタリングを呼び出すことができるのは、外部CTIアプリケーションのみです。Cisco Unified Contact Center Enterprise や Cisco Unified Contact Center Express などのシスコアプリケーションは、サイレントモニタリングセッションを開始できます。詳細については、次を参照してください。

- Cisco Unified Contact Center Enterprise : Cisco Unified Contact Center Enterprise でサイレントモニタリングをセットアップする方法の詳細については、『[Cisco Remote Silent Monitoring Installation and Administration Guide](#)』を参照してください。
- Cisco Unified Contact Center Express—この章には、Cisco Finesse を介した Unified Contact Center Express のサイレントモニタリングを設定するためのサンプル設定が含まれています。Cisco Unified Contact Center Express に関連するその他のマニュアルは、<https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/tsd-products-support-series-home.html> を参照してください。

## サイレントモニタリングの設定タスクフロー

このタスクフローでは、CTIアプリケーションでのモニタリング機能の使用を許可するために、Unified Communications Manager 内で実行する必要があるタスクについて説明します。

## 始める前に

- 電話機能リストのレポートを実行して、どの電話機でサイレントモニタリングがサポートされているかを判別します。詳細については、[電話機能一覧の生成](#)

## 手順

|        | コマンドまたはアクション   | 目的   |
|--------|--|--|
| ステップ 1 | 次のいずれかの手順を実行します。 <ul style="list-style-type: none"> <li>クラスタ全体の電話での組み込みブリッジの有効化 (3 ページ)</li> <li>電話での組み込みブリッジの有効化 (4 ページ)</li> </ul> | エージェントの電話機で組み込みのブリッジをオンにします。サービスパラメータを使用してクラスタ全体のデフォルトを設定するか、または個々の電話機で組み込みのブリッジを有効化できます。<br><br>(注) 個々の電話機のブリッジ設定は、クラスタ全体のデフォルト設定を上書きします。 |
| ステップ 2 | スーパーバイザのモニタリング権限の有効化 (4 ページ)   | サイレントモニタリングを許可するグループにスーパーバイザを追加します。  |
| ステップ 3 | モニタリング コーリング サーチ スペースの割り当て (5 ページ)   | スーパーバイザの電話機でモニタリング コーリング サーチ スペースを設定します。   |
| ステップ 4 | サイレント モニタリングの通知トーンの設定 (5 ページ)  | コールの参加者に通知トーンを再生するかどうかを設定します。  |
| ステップ 5 | セキュア サイレント モニタリングの設定 (6 ページ)   | <b>オプション。</b> コールを暗号化する場合、セキュア サイレント モニタリングを設定します。   |
| ステップ 6 | Unified Contact Center Express のサイレント モニタリングの設定 (7 ページ)  | Unified Contact Center Express 導入では、Cisco Finesse を使用してサイレントモニタリングを設定します。  |

## クラスタ全体の電話での組み込みブリッジの有効化

組み込みブリッジのクラスタ全体のサービスパラメータを有効に設定すると、クラスタ内のすべての電話で組み込みブリッジのデフォルト設定が有効に変わります。ただし、[電話の設定 (Phone Configuration)] ウィンドウの組み込みブリッジ設定は、クラスタ全体のサービスパラメータを上書きします。

- 
- ステップ 1 [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。[システム (System)] > [サービスパラメータ (Service Parameters)]。
- ステップ 2 [サーバ (Server)] ドロップダウンリストから、CallManager サービスが実行されているサーバを選択します。
- ステップ 3 [サービス (Service)] ドロップダウンリストから、[Cisco CallManager] を選択します。
- ステップ 4 [有効な組み込みブリッジ (Builtin Bridge Enable)] サービスパラメータを [オン (On)] に設定します。

ステップ5 [保存 (Save) ]をクリックします。

---

## 電話での組み込みブリッジの有効化

個々の電話で組み込みブリッジを有効にするには、次の手順を使用します。個々の電話の組み込みブリッジ設定は、クラスタ全体のサービス パラメータを上書きします。

### 始める前に

クラスタ内のすべての電話で組み込みブリッジをデフォルトに設定するには、サービス パラメータを使用します。詳細については、「[クラスタ全体の電話での組み込みブリッジの有効化 \(3 ページ\)](#)」を参照してください。

---

ステップ1 [Cisco Unified CM 管理 (Cisco Unified CM Administration) ]から、以下を選択します。[デバイス (Device) ]> [電話 (Phone) ]。

ステップ2 [検索 (Find) ]をクリックして、エージェントの電話を選択します。

ステップ3 [組み込みブリッジ (Built in Bridge) ]ドロップダウン リストから、次のいずれかのオプションを選択します。

- [オン (On) ]: 組み込みブリッジが有効になります。
- [オフ (Off) ]: 組み込みブリッジが無効になります。
- [デフォルト (Default) ]: [組み込みブリッジの有効化 (Builtin Bridge Enable) ]クラスタ全体サービスパラメータの設定が使用されます。

ステップ4 [保存 (Save) ]をクリックします。

---

## スーパーバイザのモニタリング権限の有効化

スーパーバイザがエージェントのカンパセーションをモニタできるようにするには、スーパーバイザはモニタリングが許可されるグループの一部である必要があります。

### 始める前に

次のいずれかの手順を実行して、エージェントの電話でビルトインブリッジを有効にします。

- [クラスタ全体の電話での組み込みブリッジの有効化 \(3 ページ\)](#)
- [電話での組み込みブリッジの有効化 \(4 ページ\)](#)

---

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 スーパーバイザをユーザの一覧から選択します。

- ステップ3 [権限情報 (Permissions Information)] セクションで、[アクセスコントロールグループに追加 (Add to Access Control Group)] をクリックします。
- ステップ4 [標準 CTI 許可コール モニタリング (Standard CTI Allow Call Monitoring)] および [標準 CTI を有効にする (Standard CTI Enabled)] ユーザ グループを追加します。
- ステップ5 [保存 (Save)] をクリックします。

## モニタリング コーリング サーチ スペースの割り当て

モニタリングを機能させるには、モニタリング コーリング サーチ スペースをスーパーバイザの電話回線に割り当てる必要があります。モニタリング コーリング サーチ スペースには、スーパーバイザの電話回線およびエージェントの電話回線の両方を含める必要があります。

- ステップ1 [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。[デバイス (Device)] > [電話 (Phone)]。
- ステップ2 [検索 (Find)] をクリックしてスーパーバイザの電話機を選択します。  
左側のナビゲーション ウィンドウに、スーパーバイザの電話機で利用可能な電話回線が表示されます。
- ステップ3 モニタリングに使用されるスーパーバイザの電話回線ごとに、次の手順を実行します。
- 電話回線をクリックします。[電話番号の設定 (Directory Number Configuration)] ウィンドウに、電話回線の設定情報が表示されます。
  - [モニタリング コーリング サーチ スペース (Monitoring Calling Search Space)] ドロップダウン リストから、スーパーバイザの電話回線およびエージェントの電話回線の両方を含むコーリング サーチ スペースを選択します。
  - [保存 (Save)] をクリックします。

## サイレントモニタリングの通知トーンの設定

特定の管轄区域では、コールがモニタされていることを示す通知トーンを、エージェント、顧客、あるいはその両方向けに再生する必要があります。デフォルトでは、Unified Communications Manager は、通知音を鳴らしません。通知トーンを有効にするには、サービスパラメータを設定する必要があります。

- ステップ1 [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。[システム (System)] > [サービスパラメータ (Service Parameters)]。
- ステップ2 [サーバ (Server)] ドロップダウンリストから、CallManager サービスが実行されているサーバを選択します。
- ステップ3 [サービス (Service)] ドロップダウンリストから、[Cisco CallManager] を選択します。
- ステップ4 次のサービスパラメータの値を設定します。

- エージェントに対して通知トーンを再生するには、**[観察対象のターゲットにモニタリング通知トーンを再生 (Play Monitoring Notification Tone To Observed Target)]** サービスパラメータの値を **[はい (True)]** に変更します。
- 顧客に対して通知トーンを再生するには、**[観察対象の接続先にモニタリング通知トーンを再生 (Play Monitoring Notification Tone To Observed Connected Parties)]** サービスパラメータの値を **[True]** に変更します。

ステップ5 **[保存 (Save)]** をクリックします。

ステップ6 サービスパラメータの設定を変更した場合は、エージェント電話をリセットします。

## セキュアサイレントモニタリングの設定

sRTPを使用したセキュアサイレントモニタリングを設定するには、暗号化を含む電話機のセキュリティプロファイルを設定し、それをスーパーバイザの電話機と、モニタ対象のすべてのエージェントの電話機に適用します。

### 手順

|       | コマンドまたはアクション                                  | 目的   |
|-------|---|--|
| ステップ1 | <a href="#">暗号化電話セキュリティプロファイルの設定 (6 ページ)</a>  | エージェントの電話機とスーパーバイザの電話機に暗号化を含む電話セキュリティプロファイルを設定します。 |
| ステップ2 | <a href="#">電話へのセキュリティプロファイルの割り当て (7 ページ)</a> | エージェントの電話機とスーパーバイザの電話機に暗号化された電話セキュリティプロファイルを適用します。 |

## 暗号化電話セキュリティプロファイルの設定

セキュアサイレントモニタリングを設定するには、スーパーバイザの電話機とエージェントの電話機の電話セキュリティプロファイルで、**[デバイスセキュリティモード (Device Security Mode)]** に **[暗号化済 (Encrypted)]** を指定するよう設定する必要があります。

ステップ1 **[Cisco Unified CM 管理 (Cisco Unified CM Administration)]** から、以下を選択します。 **[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)]** 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。

- **[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、既存の電話セキュリティプロファイルを選択します。

ステップ3 新しい電話セキュリティプロファイルを作成した場合は、**[電話セキュリティプロファイルタイプ (Phone Security Profile Type)]** ドロップダウンリストから、お使いの電話モデルを選択します。

ステップ4 電話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5** [デバイス セキュリティ モード (Device Security Mode)] ドロップダウン リストから、[暗号化済 (Encrypted)] 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** スーパーバイザの電話機とエージェントの電話機の電話セキュリティプロファイルを設定するまで、上記の手順を繰り返します。

---

## 電話へのセキュリティ プロファイルの割り当て

次の手順を実行して、電話に電話セキュリティ プロファイルを割り当てます。セキュア サイレント モニタリングを機能させるには、電話セキュリティ プロファイルをエージェントの電話とスーパーバイザの電話の両方に割り当てる必要があります。

- ステップ1** [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。1[デバイス (Device)] > [電話 (Phone)]。
- ステップ2** [検索 (Find)] をクリックして、電話セキュリティ プロファイルを設定するエージェント電話を選択します。
- ステップ3** [デバイス セキュリティ プロファイル (Device Security Profile)] ドロップダウン リストから、設定した電話セキュリティ プロファイルを選択します。
- ステップ4** [保存 (Save)] をクリックします。
- ステップ5** スーパーバイザの電話に対しても、前述の手順を繰り返します。

---

## Unified Contact Center Express のサイレント モニタリングの設定

次の手順には、Cisco Finesse を介した Cisco Unified Contact Center Express 設定のサイレント モニタリングの例が含まれています。

### 始める前に

エージェントとスーパーバイザーの両方の電話機が Cisco Finesse に対応していることを確認してください。 <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html> の『Unified CCX ソフトウェア互換性マトリクス』を参照してください。

- ステップ1** テスト エージェントとスーパーバイザーを、Unified Contact Center Express 上に設定します。
- (注) エージェントとスーパーバイザーの IP 連絡先センター (IPCC) の内線番号は、一意である必要があります。これは、[コールルーティング (Call Routing)] > [ルート プラン レポート (Route Plan Report)] の下にある Cisco Unified Communications Manager から確認できます。
- ステップ2** エージェントの電話に組み込み型の Bridge (BIB) があることを確認します。これは、電話またはクラスターレベルで行うことができます (デフォルトの [サービス (Service)] パラメータをオンに設定)。

- ステップ3** エージェントとして Finesse にログインします。
- ステップ4** Finesse にスーパーバイザーとしてログインし、スーパーバイザーが [NOT READY] になっていることを確認します。
- ステップ5** Resource Manager Contact Manager (RMCM) ユーザには、コールモニタリングとコール録音の必須のロールがあることを確認します。標準のコンピュータテレフォニーインテグレーション (CTI) はコールモニタリングと録音を許可します。
- (注) これは、RMCM ユーザの最初のセットアップ時に、Unified Contact Center Express によって自動的に実行されます。Cisco Unified Communications Managerの [アプリケーションユーザ (Application User)] ウィンドウでロールが存在することを確認します。
- ステップ6** エージェントの回線のパーティションを含めるために、モニタリング用 CSS (コーリングサーチスペース) をスーパーバイザーの電話機に割り当てます。
- ステップ7** コールをエージェントログインにルーティングするには、Unified Contact Center Express に電話をかけます。エージェントが TALKING 状態になったら、スーパーバイザーから、サイレントモニタリングを開始します。その後、スーパーバイザーは、エージェントと発信者の間の会話を聞くことができるようになります。

## サイレントモニタリングの連携動作

| 機能               | データのやり取り  |
|------------------|---|
| 通話保持             | モニタ対象のエージェントコールが通話保護モードになると、Unified Communications Manager はモニタリングコールも通話保持モードにします。                          |
| セキュアモニタリングコールの転送 | Unified Communications Manager 接続先のスーパーバイザデバイスが、モニタされているエージェントのセキュリティ機能を超えている限り、セキュアモニタリングセッションの転送をサポートします。 |
| 録音トーン            | 録音およびモニタリングされるコールに関しては、録音トーンがモニタリングトーンよりも優先されます。コールの録音およびモニタが行われると、録音トーンだけ再生されます。                           |

| 機能       | データのやり取り   |
|----------|--|
| セキュア トーン | <p>セキュア トーンが設定されていてコールがセキュアな場合、モニタリング トーンが設定されているかどうかに関係なく、コールの開始時にコール参加者にセキュア トーンが再生されます。</p> <p>セキュア トーンとモニタリング トーンの両方が設定されていると、セキュア トーンが一度再生され、続いてモニタリング トーンが再生されます。</p> <p>セキュア トーン、モニタリング トーン、および録音トーンすべてが設定されていて、コールが録音およびモニタされている場合、セキュア トーンが一度再生され、続いて録音トーンが再生されます。モニタリング トーンは再生されません。</p> |

## サイレントモニタリングの制約事項

| 機能                               | 制約事項  |
|----------------------------------|---|
| 割り込み                             | Unified Communications Manager サイレントモニタリングを使用した割り込みはサポートされません。エージェントコールがモニタされている場合、共有回線からの割り込みコールが失敗します。エージェントコールへの割り込みがすでに行われている場合、モニタリング コールが失敗します。 |
| クラスタ間トランク経由でのセキュアなサイレントモニタリングの転送 | Unified Communications Manager クラスタ間トランク経由でのセキュアなサイレントモニタリングの転送をサポートしません。   |
| サイレントモニタリングの制限事項                 | <p>スーパーバイザが非セキュアモードでログインし、エージェントが MRA モードにログインすると、モニタリングは失敗します。</p> <p>詳細については、「セキュアサイレントモニタリング」の項を参照してください。</p>                                      |

