



# アナログ電話アダプタの設定

- [アナログ電話アダプタの概要 \(1 ページ\)](#)
- [アナログ電話アダプタの設定 \(2 ページ\)](#)

## アナログ電話アダプタの概要

Cisco アナログ電話アダプタ (ATA) は、通常のアナログ電話と IP ベースのテレフォニー ネットワークとのインターフェイスとなるアナログ電話アダプタとして機能します。Cisco ATA は通常のアナログ電話をインターネット電話に変換します。各アダプタは2個の音声ポートをサポートし、それぞれに固有の電話番号を割り当てることができます。

他の IP デバイスと同様に、Cisco ATA は TFTP サーバからプロファイルと Unified Communications Manager のリストを受信します。TFTP サーバに設定ファイルが存在しない場合、Cisco ATA は、TFTP サーバの名前または IP アドレスとポート番号を、プライマリ Unified Communications Manager の名前または IP アドレスとポート番号として使用します。

Cisco ATA :

- 1 つの 10 BaseT RJ-45 ポート、および 2 つの RJ-11 FXS 標準アナログ電話ポート
- G.711 alaw、G.711 mulaw、G.723 と G.729a 音声コーデックなど、さまざまなコーデックに対応しています
- 音声 を IP データパケットに変換します。
- リダイヤル、スピードダイヤル、自動転送、コール待機、コール保留、転送、会議、ボイスメッセージング、メッセージ受信インジケータ、オフフック呼び出し音、発信者 ID、被発信者 ID、およびコール待機の発信者 ID をサポート

ATA 180 シリーズは SCCP を使用しますが、ATA 190 シリーズは SIP を使用します。詳細については、ATA のドキュメントを参照してください。

- ATA 180 シリーズ : <https://www.cisco.com/c/en/us/support/unified-communications/ata-180-series-analog-telephone-adaptors/tsd-products-support-series-home.html>
- ATA 190 シリーズ : <https://www.cisco.com/c/en/us/support/unified-communications/ata-190-series-analog-telephone-adaptors/tsd-products-support-series-home.html>

# アナログ電話アダプタの設定

## 手順

- ステップ 1** Cisco Unified CM Administration から、[デバイス (Device)] > [電話 (Phone)] を選択します。  
[電話の検索と一覧表示 (Find and List Phones)] ウィンドウが表示されます。
- ステップ 2** [新規追加 (Add New)] をクリックします。
- ステップ 3** [電話のタイプ (Phone Type)] ドロップダウンリストから、使用しているアナログ電話アダプタモデルを選択して、[次へ (Next)] をクリックします。  
[電話の設定 (Phone Configuration)] ウィンドウが表示されます。
- ステップ 4** [電話の設定 (Phone Configuration)] ウィンドウのフィールドを設定します。  
フィールドとその設定オプションの詳細については、「関連項目」の項を参照してください。
- ステップ 5** [保存 (Save)] をクリックします。
- ステップ 6** [設定の適用 (Apply Config)] をクリックして、電話に変更を適用し、同期します。

## アナログ電話アダプタ 186 設定フィールド

表 1: アナログ電話アダプタ 186 設定フィールド

| フィールド                  | 説明   |
|------------------------|--|
| MAC アドレス (MAC Address) | ATA 186 を特定する Media Access Control (MAC) アドレスを入力します。値が 12 桁の 16 進文字列で構成されていることを確認します。<br>次のいずれかの方法で、ATA 186 の MAC アドレスを判別できます。 <ul style="list-style-type: none"> <li>ATA 186 の背面にある MAC ラベルを確認します。</li> <li>ATA 186 の ウェブ ページを表示し、[デバイス情報 (Device Information)] ハイパーリンクをクリックします。</li> </ul> |
| [説明 (Description)]     | ATA 186 の説明テキストを入力します。<br>このフィールドには、128 文字までの値を入力できます。二重引用符 (")、山カッコ (<>)、バックスラッシュ (\)、アンパサンド (&)、パーセント記号 (%) を除くすべての文字を使用できます。  |

| フィールド  | 説明   |
|--|--|
| [デバイスプール (Device Pool) ]                       | ATA 186 を割り当てるデバイス プールを選択します。デバイス プールでは、複数のデバイスに共通の特性 (リージョン、日時グループ、ソフトキー テンプレートなど) のセットを定義します。<br><br>デバイス プール構成の設定を確認するには、[詳細の表示 (View Details) ] リンクをクリックします。 |
| [共通デバイス設定 (Common Device Configuration) ]      | ATA 186 を割り当てる共通デバイス設定を選択します。<br><br>[共通デバイス設定 (Common Device Configuration) ] の設定を表示するには、[詳細の表示 (View Details) ] リンクをクリックします。                                   |
| [電話ボタンテンプレート (Phone Button Template) ]         | 適切な電話ボタンテンプレートを選択します。電話ボタン テンプレートでは、電話機上のボタンを設定し、各ボタンにどの機能 (回線、スピードダイヤルなど) を使用するかを特定します。   |
| [共通の電話プロファイル (Common Phone Profile) ]          | ドロップダウンリストで、使用可能な共通の電話プロファイルのリストから共通の電話プロファイルを選択します。<br><br>[共通の電話プロファイル (Common Phone Profile) ] の設定を表示するには、[詳細の表示 (View Details) ] リンクをクリックします。                |
| [コーリングサーチスペース (Calling Search Space) ]         | ドロップダウンリストを使用から、コーリングサーチスペースを選択するか、コーリングサーチスペースをデフォルトの[なし (None) ] のままにします。  |
| [AARコーリングサーチスペース (AAR Calling Search Space) ]  | ドロップダウンリストから、自動代替ルーティング (AAR) を実行したときに使用するデバイスの適切なコーリングサーチスペースを選択するか、コーリングサーチスペースをデフォルトの[なし (None) ] のままにします。  |
| [メディアリソースグループリスト (Media Resource Group List) ] | 適切なメディアリソースグループリストを選択します。メディアリソースグループリストは、優先順位順に並べられたメディアリソースグループから構成されます。<br><br>[<なし> (<None>)] を選択すると、Cisco Unified CM はデバイスプールで定義されたメディアリソースグループリストを使用します。   |
| [ロケーション (Location) ]                           | ドロップダウンリストから、デバイスプール内の電話およびゲートウェイと関連付けられている場所を選択します。   |
| [AARグループ (AAR Group) ]                         | このデバイスの自動代替ルーティング (AAR) グループを選択します。AAR グループはプレフィックス番号を設定します。この番号は、帯域幅不足のためにブロックされるコールをルーティングする際に使用されます。Cisco Unified CM は、デバイスプールまたは回線と関連付けられている AAR グループを使用します。 |

| フィールド                                  | 説明  |
|--|---|
| [ユーザーロケール (User Locale) ]              | ド롭ダウンリストから、ATA 186 と関連付けられているユーザーロケールを選択します。そのユーザー ロケールは、言語とフォントを含んだ、ユーザーをサポートする一連の詳細情報を識別します。<br><br>ユーザー ロケールが指定されていない場合、Cisco Unified CM はデバイス プールに関連付けられたユーザー ロケールを使用します。   |
| [ネットワークロケール (Network Locale) ]         | ド롭ダウン リストから、ATA 186 と関連付けられているネットワーク ロケールを選択します。ネットワーク ロケールには、特定の地理的領域の電話が使用するトーンとパターンの定義が含まれています。<br><br>ネットワーク ロケールが指定されていない場合、Cisco Unified CM はデバイス プールに関連付けられたネットワーク ロケールを使用します。   |
| [デバイスモビリティモード (Device Mobility Mode) ] | ド롭ダウンリストから、このデバイスのデバイス モビリティ機能をオンまたはオフにします。デフォルトのデバイス モビリティモードを使用する場合は、[デフォルト (Default) ]を選択します。デフォルト設定では、デバイス移行モードのサービスパラメータの値が使用されます。   |
| [オーナー (Owner) ]                        | オーナータイプには、[ユーザー (User) ]または[匿名 (Anonymous) ] (パブリック/共有スペース) を選択します。   |
| [オーナーのユーザーID (Owner User ID) ]         | ド롭ダウンリストから、割り当てられた電話ユーザーのユーザーID を選択します。ユーザー ID は、このデバイスから発信されるすべてのコールの呼詳細レコード (CDR) に記録されます。ユーザー ID をデバイスに割り当てると、そのデバイスが [ライセンスの使用状況レポート (License Usage Report) ]で「」 [未割り当てのデバイス (Unassigned Devices) ]から「」 [ユーザー (Users) ]に移動することにもなります。<br><br>(注) エクステンションモビリティを使用する場合は、このフィールドを設定しないでください。エクステンション モビリティでは、デバイスのオーナーはサポートされていません。 |
| [電話ロード名 (Phone Load Name) ]            | ATA 186のカスタムソフトウェアを入力します。   |

| フィールド   | 説明  |
|---|---|
| [トラステッドリレーポイントを使用 (Use Trusted Relay Point) ] | <p>次の値のいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [オフ (Off) ]: このデバイスで、トラステッドリレーポイント (TRP) の使用を無効にするには、この値を選択します。この設定は、このデバイスに関連付けられている共通デバイス設定の [トラステッドリレーポイントを使用 (Use Trusted Relay Point) ] 設定よりも優先されます。</li> <li>• [オン (On) ]: このデバイスで TRP の使用を有効にする場合は、この値を選択します。この設定は、このデバイスに関連付けられている共通デバイス設定の [トラステッドリレーポイントを使用 (Use Trusted Relay Point) ] 設定よりも優先されます。</li> <li>• [デフォルト (Default) ]: この値を選択した場合、このデバイスが関連付けられている共通デバイス設定の [トラステッドリレーポイントを使用 (Use Trusted Relay Point) ] 設定を使用します。</li> </ul> |
| 常にプライム回線を使用する (Always Use Prime Line)         | <p>ドロップダウンリストから、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [オフ (Off) ]: 電話がアイドル状態になっているときにいずれかの回線でコールを受信すると、電話のユーザは、コールを受信した回線からコールに応答します。</li> <li>• [オン (On) ]: 電話機がアイドル状態 (オフフック) になっているときにいずれかの回線でコールを受信すると、このコールにはプライマリ回線が選択されます。他の回線のコールは鳴り続け、電話機ユーザはそれらの他の回線を選択して、これらのコールに応答する必要があります。</li> <li>• デフォルト: Unified Communications Manager は、[常にプライム回線を使用する (Always Use Prime Line) ] サービスパラメータの設定を使用します。これにより、Cisco CallManager サービスがサポートされます。</li> </ul>                                  |

| フィールド   | 説明  |
|---|---|
| ボイスメッセージには常にプライム回線を使用する (Always Use Prime Line for Voice Message)                       | <p>ドロップダウン リストから、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [オフ (Off)] : 電話がアイドル状態の場合、電話のメッセージ ボタンを押すと、ボイス メッセージが設定されている回線からボイスメッセージシステムに自動的にダイヤルされます。Unified Communications Manager は、常に音声メッセージのある最初の回線を選択します。ボイスメッセージが設定されている回線が存在しない場合に電話のユーザーが [メッセージ (Messages)] ボタンを押すと、プライマリ回線が使用されます。</li> <li>• [オン (On)] : 電話がアイドル状態の場合に電話のメッセージ ボタンを押すと、電話のプライマリ回線がボイス メッセージを受信するアクティブな回線になります。</li> <li>• [デフォルト (Default)] : Unified Communications Manager は、[ボイスメッセージに常にプライム回線を使用する (Always Use Prime Line for Voice Message)] サービス パラメータの設定を使用します。これにより、Cisco CallManager サービスがサポートされます。</li> </ul> |
| [地理位置情報 (GeoLocation) ]   | <p>ドロップダウン リストから地理位置情報を選択します。</p> <p>[未指定の地理位置情報 (Unspecified geolocation) ]を選択すると、このデバイスを地理位置情報に関連付けないように指定できます。</p> <p>さらに、[システム (System) ] &gt; [地理位置情報の設定 (Geolocation Configuration) ] メニュー オプションで設定した地理位置情報も選択できます。</p>   |
| [プレゼンテーションインジケータを無視 (内線コールのみ) (Ignore Presentation Indicators (internal calls only) ) ] | <p>コール単位でコール表示制限を設定する場合に、このチェックボックスをオンにします。このチェックボックスをオンにすると、Unified Communications Manager は内線コールについて受信するすべての表示制限を無視します。</p> <p>この設定と、トランスレーションパターンレベルでの発信者回線IDの表示および接続回線IDの表示の設定を組み合わせで使用します。これらの設定を組み合わせで使用すれば、コールごとに発信側または接続先の回線表示情報を選択的に表示またはブロックするようにコール表示制限を設定できます。</p>  |

| フィールド  | 説明  |
|--|---|
| [CTIからのデバイスの制御を許可 (Allow Control of Device from CTI) ] | CTI に対してこのデバイスの制御と監視を許可する場合は、このチェックボックスをオンにします。<br>関連付けられている電話番号が共有回線を指定している場合、少なくとも1つの関連付けられているデバイスで、CTI がサポートするデバイス タイプとプロトコルの組み合わせが指定されていれば、チェックボックスを有効にする必要があります。   |
| [ハントグループにログイン (Logged into Hunt Group) ]               | CTI ポートをハントリストに追加したら、管理者はこのチェックボックスをオン (またはオフ) にすることによって、ユーザーをログインまたはログアウトさせることができます。<br>ユーザーは電話のソフトキーを使用して、電話をハント リストにログインまたはログアウトします。   |
| [リモートデバイス (Remote Device) ]                            | このチェックボックスをオンにすると、デバイスの登録時にバッファを割り当て、SCCP メッセージを電話機にバンドルします。<br><b>ヒント</b> この機能はリソースを消費するため、シグナリングの遅延が発生している場合にのみ、このチェックボックスをオンにしてください。   |
| [ホットラインデバイス (Hot Line Device) ]                        | このデバイスをホットラインデバイスにするには、このチェックボックスをオンにします。ホットラインデバイスは他のホットラインデバイスにのみ接続できます。これは PLAR の拡張機能です。PLAR では、電話がオフフックになった場合に自動的に1つの電話番号にダイヤルするよう電話を設定します。ホットラインによって、PLAR を使用するデバイスに追加の制限を適用できます。<br>ホットラインを実装するには、補足サービス ソフトキーを含まないソフトキーテンプレートを作成し、それをホットラインデバイスに適用する必要があります。 |

[番号表示トランスフォーメーション (Number Presentation Transformation) ]

表 2:[この電話からのコールの発信者ID (Caller ID For Calls From This Phone) ]

| フィールド  | 説明   |
|--|--|
| [発信側トランスフォーメーションCSS (Calling Party Transformation CSS) ] | この設定により、デバイスの発信者番号をローカライズできます。選択した発信側トランスフォーメーション CSS に、このデバイスに割り当てる発信側トランスフォーメーションパターンが含まれていることを確認してください。 |

| フィールド   | 説明  |
|---|---|
| [デバイスプールの発信側トランスフォーメーションCSSを使用 (Use Device Pool Calling Party Transformation CSS) ] | このデバイスに割り当てられているデバイス プールに設定されている発信側トランスフォーメーションCSSを使用する場合は、このボックスをオンにします。このチェックボックスを選択しない場合、デバイスは [トランク設定 (Trunk Configuration) ] ウィンドウで設定した発信側変換 CSS を使用します。 |

表 3: [リモート番号 (Remote Number) ]

| フィールド   | 説明  |
|---|---|
| [発信側トランスフォーメーションCSS (Calling Party Transformation CSS) ]                            | ドロップダウンリストから、このデバイスに受信したコールのリモート発信者番号に適用する、発信側トランスフォーメーションパターンを含むコーリング サーチ スペース (CSS) を選択します。 |
| [デバイスプールの発信側トランスフォーメーションCSSを使用 (Use Device Pool Calling Party Transformation CSS) ] | リモート通話とリモート接続番号の変換に、このデバイスが属するデバイス プールで設定されている発信側トランスフォーメーションCSS を適用するには、このチェックボックスをオンにします。   |

表 4: [プロトコル固有情報 (Protocol Specific Information) ]

| フィールド  | 説明  |
|--|---|
| [BLFプレゼンスグループ (BLF Presence Group) ]           | ドロップダウンリストから、エンドユーザーの話中ランプフィールド (BLF) プレゼンスグループを選択します。選択したグループは、エンドユーザーがモニター可能な接続先を指定します。<br><br>BLF プレゼンス グループのデフォルト値は [標準のプレゼンスグループ (Standard Presence group) ] であり、インストール時に設定されません。Cisco Unified CM Administration で設定されている BLF プレゼンスグループは、ドロップダウンリストにも表示されます。 |
| [デバイスのセキュリティプロファイル (Device Security Profile) ] | デバイスに適用するセキュリティ プロファイルを選択します。<br><br>Unified Communications Manager Administration で設定するすべてのデバイスに、セキュリティプロファイルを適用する必要があります。   |



| フィールド  | 説明  |
|--|---|
| [SUBSCRIBE コーリングサーチスペース (AAR Calling Search Space) ] | <p>プレゼンス機能によってサポートされる SUBSCRIBE コーリングサーチスペースは、エンドユーザから受け取ったプレゼンス要求を Unified Communications Manager がルーティングする方法を決定します。この設定では、エンドユーザーのプレゼンス (SUBSCRIBE) 要求のコール処理検索スペースと別にコーリングサーチスペースを適用できます。</p> <p>ドロップダウンリストから、エンドユーザーのプレゼンス要求に使用する SUBSCRIBE コーリングサーチスペースを選択します。Cisco Unified Communications Manager Administration で設定するすべてのコーリングサーチスペースが、[SUBSCRIBE コーリングサーチスペース (SUBSCRIBE Calling Search Space) ] ドロップダウンリストに表示されます。</p> <p>ドロップダウンリストから、エンドユーザーに別のコーリングサーチスペースを選択しない場合、SUBSCRIBE コーリングサーチスペースのデフォルトは [なし (None) ] に設定されます。</p> <p>この目的専用の SUBSCRIBE コーリングサーチスペースを設定するには、他のコーリングサーチスペースと同様に新しいコーリングサーチスペースを設定します。</p> |
| [不在ポート (Unattended Port) ]                           | このデバイスの不在ポートを指示する場合に、このチェックボックスをオンにします。   |
| [RFC 2833 Disabled (RFC 2833 の無効化) ]                 | SCCP を実行しているデバイスの場合は、このチェックボックスをオンにして RFC2833 のサポートを無効にします。   |

表 5: 製品固有の設定

| フィールド                     | 説明  |
|---------------------------|---|
| デバイス製造元が定義するモデル固有の設定フィールド | <p>製品固有の設定項目のフィールドの説明とヘルプを表示するには、[製品固有の設定 (Product Specific Configuration) ] エリアで [?] 「」情報アイコンをクリックし、ポップアップダイアログボックスでヘルプを表示します。</p> <p>詳細については、ATA 186 のマニュアルを参照してください。</p> |

## アナログ電話アダプタ 187 設定フィールド

表 6: アナログ電話アダプタ 187 設定フィールド

| フィールド                                    | 説明  |
|--|---|
| MACアドレス (MAC Address)                    | <p>ATA 187 を識別する Media Access Control (MAC) アドレスを入力します。値が 12 桁の 16 進文字列で構成されていることを確認します。</p> <p>次のいずれかの方法で、ATA 187 の MAC アドレスを判別できます。</p> <ul style="list-style-type: none"> <li>• ATA 187 の背面にある MAC ラベルを確認する。</li> <li>• ATA 187 の ウェブ ページを表示し、[デバイス情報 (Device Information)] ハイパーリンクをクリックする。</li> </ul> |
| [説明 (Description)]                       | <p>ATA 187 のテキストの説明を入力します。</p> <p>このフィールドには、128 文字までの値を入力できます。二重引用符 (" )、山カッコ (&lt;&gt;)、バックスラッシュ (\)、アンパサンド (&amp;)、パーセント記号 (%) を除くすべての文字を使用できます。</p>  |
| [デバイスプール (Device Pool)]                  | <p>ATA 187 を割り当てるデバイスプールを選択します。デバイスプールでは、複数のデバイスに共通の特性 (リージョン、日時グループ、ソフトキー テンプレートなど) のセットを定義します。</p> <p>デバイスプール構成の設定を確認するには、[詳細の表示 (View Details)] リンクをクリックします。</p>   |
| [共通デバイス設定 (Common Device Configuration)] | <p>ATA 187 を割り当てる共通デバイス設定を選択します。</p> <p>[共通デバイス設定 (Common Device Configuration)] の設定を表示するには、[詳細の表示 (View Details)] リンクをクリックします。</p>   |
| [電話ボタンテンプレート (Phone Button Template)]    | <p>適切な電話ボタンテンプレートを選択します。電話ボタンテンプレートでは、電話機上のボタンを設定し、各ボタンにどの機能 (回線、スピードダイヤルなど) を使用するかを特定します。</p>  |
| [共通の電話プロファイル (Common Phone Profile)]     | <p>ドロップダウンリストで、使用可能な共通の電話プロファイルのリストから共通の電話プロファイルを選択します。</p> <p>[共通の電話プロファイル (Common Phone Profile)] の設定を表示するには、[詳細の表示 (View Details)] リンクをクリックします。</p>  |
| [コーリングサーチスペース (Calling Search Space)]    | <p>ドロップダウンリストを使用から、コーリングサーチスペースを選択するか、コーリングサーチスペースをデフォルトの[なし (None)]のままにします。</p>  |

| フィールド  | 説明  |
|--|---|
| [AARコーリングサーチスペース (AAR Calling Search Space) ]  | ドロップダウンリストから、自動代替ルーティング (AAR) を実行したときに使用するデバイスの適切なコーリングサーチスペースを選択するか、コーリングサーチスペースをデフォルトの [なし (None) ] のままにします。  |
| [メディアリソースグループリスト (Media Resource Group List) ] | 適切なメディアリソースグループリストを選択します。メディアリソースグループリストは、優先順位順に並べられたメディアリソースグループから構成されます。<br><br>[<なし> (<None>)] を選択すると、Cisco Unified CM はデバイスプールで定義されたメディアリソースグループリストを使用します。                      |
| [ユーザー保留 MOH 音源 (User Hold MOH Audio Source) ]  | ドロップダウンリストから、ユーザーが保留操作を開始する場合に保留音 (MOH) として使用するオーディオソースを選択します。  |
| [ロケーション (Location) ]                           | ドロップダウンリストから、デバイスプール内の電話およびゲートウェイと関連付けられている場所を選択します。  |
| [AARグループ (AAR Group) ]                         | このデバイスの自動代替ルーティング (AAR) グループを選択します。AAR グループはプレフィックス番号を設定します。この番号は、帯域幅不足のためにブロックされるコールをルーティングする際に使用されます。AAR グループが指定されていない場合、Cisco Unified CM はデバイスプールまたは回線に関連付けられている AAA グループを使用します。 |
| [ユーザーロケール (User Locale) ]                      | ドロップダウンリストから、CTI ポートに関連付けられたユーザーロケールを選択します。そのユーザーロケールは、言語とフォントを含んだ、ユーザーをサポートする一連の詳細情報を識別します。<br><br>ユーザーロケールが指定されていない場合、Cisco Unified CM はデバイスプールに関連付けられたユーザーロケールを使用します。            |
| [ネットワークロケール (Network Locale) ]                 | ドロップダウンリストから、CTI ポートに関連付けられたネットワークロケールを選択します。ネットワークロケールには、特定の地理的領域の電話が使用するトーンとパターンの定義が含まれています。<br><br>ネットワークロケールが指定されていない場合、Cisco Unified CM はデバイスプールに関連付けられたネットワークロケールを使用します。      |

| フィールド                                  | 説明  |
|--|---|
| [ビルトインブリッジ (Built In Bridge) ]         | [ビルトインブリッジ (Built In Bridge) ] ドロップダウンリストを使用して割り込み機能用の組み込み型会議ブリッジを有効または無効にします。次のいずれかを実行します。 <ul style="list-style-type: none"> <li>• オン</li> <li>• オフ</li> <li>• デフォルト</li> </ul>   |
| [プライバシー (Privacy) ]                    | プライバシーについて、[プライバシー (Privacy) ] ドロップダウンリストから [オン (On) ] を選択します。  |
| [デバイスモビリティモード (Device Mobility Mode) ] | ドロップダウンリストから、このデバイスのデバイスモビリティ機能をオンまたはオフにします。デフォルトのデバイスモビリティモードを使用する場合は、[デフォルト (Default) ] を選択します。デフォルトの設定では、デバイスの [デバイスモビリティモード (Device Mobility Mode) ] サービス パラメータの値が使用されます。   |
| [オーナー (Owner) ]                        | オーナーのタイプとして、[ユーザー (User) ] または [名前非表示 (パブリック/共有スペース) (Anonymous (Public/Shared Space)) ] を選択します。  |
| [オーナーのユーザー ID (Owner User ID) ]        | ドロップダウンリストから、割り当てられた電話ユーザーのユーザー ID を選択します。ユーザー ID は、このデバイスから発信されるすべてのコールの呼詳細レコード (CDR) に記録されます。デバイスにユーザー ID を割り当てると、[ライセンスの使用状況レポート (License Usage Report) ] でデバイスが [未割り当てデバイス (Unassigned Devices) ] から [ユーザー (Users) ] に移動します。 <p>(注) エクステンションモビリティを使用する場合は、このフィールドを設定しないでください。エクステンションモビリティでは、デバイスのオーナーはサポートされていません。</p> |
| [電話ロード名 (Phone Load Name) ]            | ATA 187 のカスタム ソフトウェアを入力します。   |

| フィールド   | 説明  |
|---|---|
| [トラステッドリレーポイントを使用 (Use Trusted Relay Point) ] | <p>次の値のいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [オフ (Off) ]: このデバイスで、トラステッドリレーポイント (TRP) の使用を無効にするには、この値を選択します。この設定は、このデバイスに関連付けられている共通デバイス設定の[トラステッドリレーポイントを使用 (Use Trusted Relay Point) ]設定よりも優先されます。</li> <li>• [オン (On) ]: このデバイスでの TRP の使用を有効にする場合は、この値を選択します。この設定は、このデバイスに関連付けられている共通デバイス設定の[トラステッドリレーポイントを使用 (Use Trusted Relay Point) ]設定よりも優先されます。</li> <li>• [デフォルト (Default) ]: この値を選択した場合、デバイスはこのデバイスが関連付けられている共通デバイス設定の[トラステッドリレーポイントを使用 (Use Trusted Relay Point) ]設定を使用します。</li> </ul> |
| 常にプライム回線を使用する (Always Use Prime Line)         | <p>ドロップダウンリストから、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [オフ (Off) ]: 電話がアイドル状態になっているときにいずれかの回線でコールを受信すると、電話のユーザは、コールを受信した回線からコールに応答します。</li> <li>• [オン (On) ]: 電話機がアイドル状態 (オフフック) になっているときにいずれかの回線でコールを受信すると、このコールにはプライマリ回線が選択されます。他の回線のコールは鳴り続け、電話機ユーザはそれらの他の回線を選択して、これらのコールに応答する必要があります。</li> <li>• デフォルト: Unified Communications Manager は、[常にプライム回線を使用する (Always Use Prime Line) ]サービスパラメータの設定を使用します。これにより、Cisco CallManager サービスがサポートされます。</li> </ul>                                   |

| フィールド   | 説明   |
|---|--|
| ボイスメッセージには常にプライム回線を使用する (Always Use Prime Line for Voice Message)                       | <p>ドロップダウン リストから、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [オフ (Off) ] : 電話がアイドル状態の場合、電話のメッセージ ボタンを押すと、ボイス メッセージが設定されている回線からボイス メッセージ システムに自動的にダイヤルされます。Unified Communications Manager は、常に音声メッセージのある最初の回線を選択します。ボイスメッセージが設定されている回線が存在しない場合に電話のユーザーが [メッセージ (Messages) ] ボタンを押すと、プライマリ回線が使用されます。</li> <li>• [オン (On) ] : 電話がアイドル状態の場合に電話のメッセージ ボタンを押すと、電話のプライマリ回線がボイス メッセージを受信するアクティブな回線になります。</li> <li>• [デフォルト (Default) ] : Unified Communications Manager は、[ボイスメッセージに常にプライム回線を使用する (Always Use Prime Line for Voice Message) ] サービス パラメータの設定を使用します。これにより、Cisco CallManager サービスがサポートされます。</li> </ul> |
| [地理位置情報 (GeoLocation) ]   | <p>ドロップダウン リストから地理位置情報を選択します。</p> <p>[未指定の地理位置情報 (Unspecified geolocation) ]を選択すると、このデバイスを地理位置情報に関連付けないように指定できます。</p> <p>さらに、[システム (System) ] &gt; [地理位置情報の設定 (Geolocation Configuration) ] メニュー オプションで設定した地理位置情報も選択できます。</p>  |
| [プレゼンテーション インジケータを無視 (内線コールのみ) (Ignore Presentation Indicators (internal calls only)) ] | <p>コール単位でコール表示制限を設定する場合に、このチェックボックスをオンにします。このチェックボックスをオンにすると、Unified Communications Manager は内線コールについて受信するすべての表示制限を無視します。</p> <p>この設定と、トランスレーション パターン レベルでの発信者回線 ID の表示および接続回線 ID の表示の設定を組み合わせ使用します。これらの設定を組み合わせ使用すれば、コールごとに発信側または接続先の回線表示情報を選択的に表示またはブロックするようにコール表示制限を設定できます。</p>   |
| [ハントグループにログイン (Logged into Hunt Group) ]  | <p>ATA 187 をハント リストに追加したら、管理者はこのチェックボックスをオン (またはオフ) にすることによって、ユーザーをログインまたはログアウトさせることができます。</p> <p>ユーザーは電話のソフトキーを使用して、電話をハントリストにログインまたはログアウトします。</p>  |

| フィールド                           | 説明   |
|---------------------------------|--|
| [リモートデバイス (Remote Device) ]     | <p>このチェックボックスをオンにすると、デバイスの登録時にバッファを割り当て、SCCP メッセージを電話機にバンドルします。</p> <p><b>ヒント</b> この機能はリソースを消費するため、シグナリングの遅延が発生している場合にのみ、このチェックボックスをオンにしてください。</p>   |
| [保護されたデバイス (Protected Device) ] | <p>電話機を保護されたデバイスとして指定するには、このチェックボックスをオンにします。この場合、電話機が2秒間トーンを再生してユーザーにコールが暗号化されていることを通知できます。また、発信側と着信側の両方の電話機が保護されたデバイスとして設定できます。このトーンは、コールが応答されたとき、発信側と着信側の両者に対して再生されます。このトーンは、発信側と着信側の両方の電話機が保護されていて、なおかつ暗号化メディア上でコールが行われたときでなければ再生されません。</p> <p>このチェックボックスをオンにすると、再生するセキュア通知トーンの複数の設定要件のうち1つのみが表示されます。セキュア通知トーン機能と設定要件の詳細については、『<i>Cisco Unified Communications Manager 機能設定ガイド</i>』（<a href="http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html">http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html</a>）を参照してください。</p> <p>このチェックボックスがオンで、システムがコールは暗号化されていないと判断すると、電話は非セキュア通知トーンを再生して、コールが保護されていないことをユーザーに通知します。</p> |

### [番号表示トランスフォーメーション (Number Presentation Transformation) ]

表 7:[この電話からのコールの発信者ID (Caller ID For Calls From This Phone) ]

| フィールド   | 説明   |
|---|--|
| [発信側トランスフォーメーションCSS (Calling Party Transformation CSS) ]                            | <p>この設定により、デバイスの発信者番号をローカライズできます。選択した発信側トランスフォーメーションCSS に、このデバイスに割り当てる発信側トランスフォーメーションパターンが含まれていることを確認してください。</p>   |
| [デバイスプールの発信側トランスフォーメーションCSSを使用 (Use Device Pool Calling Party Transformation CSS) ] | <p>このデバイスに割り当てられているデバイスプールに設定されている発信側トランスフォーメーションCSSを使用する場合は、このボックスをオンにします。このチェックボックスを選択しない場合、デバイスは[トランク設定 (Trunk Configuration) ] ウィンドウで設定した発信側変換 CSS を使用します。</p> |

表 8: [リモート番号 (Remote Number) ]

| フィールド   | 説明  |
|---|---|
| [発信側トランスフォーメーションCSS (Calling Party Transformation CSS) ]                            | ドロップダウンリストから、このデバイスに受信したコールのリモート発信者番号に適用する、発信側トランスフォーメーションパターンを含むコーリングサーチスペース (CSS) を選択します。 |
| [デバイスプールの発信側トランスフォーメーションCSSを使用 (Use Device Pool Calling Party Transformation CSS) ] | リモート通話とリモート接続番号の変換に、このデバイスが属するデバイスプールで設定されている発信側トランスフォーメーションCSSを適用するには、このチェックボックスをオンにします。   |

表 9: [プロトコル固有情報 (Protocol Specific Information) ]

| フィールド                                 | 説明  |
|---------------------------------------|---|
| [パケットキャプチャモード (Packet Capture Mode) ] | <p>この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケットキャプチャを実行すると、CPUの使用率が上昇して、コール処理が妨げられる可能性があります。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。</p> <ul style="list-style-type: none"> <li>• [なし (None) ] : このオプションは、パケットキャプチャが発生しないことを示します (デフォルト設定)。この設定は、パケットキャプチャの完了後に行います。</li> <li>• [バッチ処理モード (Batch Processing Mode) ] : Cisco Unified CM が、復号されたメッセージや暗号化されていないメッセージをファイルに書き込み、システムが各ファイルを暗号化します。システムでは、毎日新しいファイルが新しい暗号キーを使用して作成されます。Cisco Unified CM はファイルを7日間保存し、さらにファイルを暗号化するキーを安全な場所に保存します。Cisco Unified CM は、PktCap 仮想ディレクトリにファイルを保存します。1つのファイルの中に、タイムスタンプ、送信元IPアドレス、送信元IPポート、宛先IPアドレス、パケットのプロトコル、メッセージの長さ、およびメッセージが保持されます。TACのデバッグツールでは、HTTPS、管理者のユーザ名とパスワード、および指定された日付を使用して、キャプチャされたパケットを保持している暗号化済みファイルを1つだけ要求します。同様にこのツールでは、暗号化ファイルを復号化するためのキー情報を要求します。</li> </ul> |



| フィールド   | 説明  |
|---|---|
| [パケットキャプチャ時間 (Packet Capture Duration) ]          | <p>この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケットキャプチャを実行すると、CPUの使用率が上昇して、コール処理が妨げられる可能性があります。</p> <p>このフィールドには、1つのパケットキャプチャセッションに割り当てる時間の上限（分単位）を指定します。デフォルト設定は0で、範囲は0～300分です。</p> <p>パケットキャプチャを開始するには、フィールドに0以外の値を入力します。パケットキャプチャが完了すると、値0が表示されます。</p>  |
| [BLFプレゼンスグループ (BLF Presence Group) ]              | <p>ドロップダウンリストから、エンドユーザーの話中ランプフィールド (BLF) プレゼンスグループを選択します。選択したグループは、エンドユーザーがモニター可能な接続先を指定します。</p> <p>BLF プレゼンスグループのデフォルト値は [標準のプレゼンスグループ (Standard Presence group) ] であり、インストール時に設定されます。Cisco Unified CM Administration で設定されている BLF プレゼンスグループは、ドロップダウンリストにも表示されます。</p>  |
| [SIPダイヤルルール (SIP Dial Rules) ]                    | <p>必要に応じて、適切な SIP ダイヤルルールを選択します。SIP ダイヤルルールは、Cisco Unified IP Phone 7940 および 7960 のローカルダイヤルプランを提供するため、ユーザーは、コールが処理される前に、キーを押したり、タイマーを待機したりする必要はありません。</p> <p>SIP を実行している IP 電話にダイヤルルールを適用しない場合は、[SIP ダイヤルルール (SIP Dial Rules) ] フィールドを [なし (&lt;None&gt;)] に設定したままにします。これは、コールが処理される前に、ユーザーがダイヤルソフトキーを使用するか、タイマーが切れるまで待つ必要があることを示します。</p> |
| [MTP優先発信コーデック (MTP Preferred Originating Codec) ] | <p>メディアターミネーションポイントが SIP のコールに必要な場合は、ドロップダウンリストから使用するコーデックを選択します。</p>   |
| [デバイスのセキュリティプロファイル (Device Security Profile) ]    | <p>デバイスに適用するセキュリティプロファイルを選択します。</p> <p>Unified Communications Manager Administration で設定するすべてのデバイスに、セキュリティプロファイルを適用する必要があります。</p>   |

| フィールド  | 説明   |
|--|--|
| [再ルーティング用<br>コーリングサーチス<br>ペース (Rerouting<br>Calling Search<br>Space) ] | <p>ドロップダウンリストから、再ルーティングに使用するコーリングサーチ スペースを選択します。</p> <p>リファラーの再ルーティングコーリングサーチスペースを使用して、参照先へのルートが検索されます。再ルーティングコーリングサーチスペースが原因で参照が失敗すると、Refer Primitive は「405 Method Not Allowed」メッセージによって要求を拒否します。</p> <p>リダイレクト (3xx) プリミティブおよび転送機能も再ルーティングコーリングサーチスペースを使用して、リダイレクト先または転送先を検索します。</p>   |
| [SUBSCRIBEコーリン<br>グサーチスペース<br>(AAR Calling Search<br>Space) ]          | <p>プレゼンス機能によってサポートされる SUBSCRIBE コーリングサーチスペースは、エンドユーザから受け取ったプレゼンス要求を Unified Communications Manager がルーティングする方法を決定します。この設定では、エンドユーザーのプレゼンス (SUBSCRIBE) 要求のコール処理サーチスペースと別にコーリングサーチスペースを適用できます。</p> <p>ドロップダウンリストから、エンドユーザーのプレゼンス要求に使用する SUBSCRIBE コーリングサーチスペースを選択します。Cisco Unified Communications Manager Administration で設定するすべてのコーリングサーチスペースが、[SUBSCRIBE コーリングサーチスペース (SUBSCRIBE Calling Search Space) ] ドロップダウンリストに表示されます。</p> <p>ドロップダウンリストから、エンドユーザーに別のコーリングサーチスペースを選択しない場合、SUBSCRIBE コーリングサーチスペースのデフォルトは [なし (None) ] に設定されます。</p> <p>この目的専用の SUBSCRIBE コーリングサーチスペースを設定するには、他のコーリングサーチスペースと同様に新しいコーリングサーチスペースを設定します。</p> |
| [SIPプロファイル<br>(SIP Profile) ]  | <p>デフォルトの SIP プロファイルまたは作成済みの特定のプロファイルを選択します。SIP プロファイルでは、登録タイマーおよびキープアライブタイマー、メディアポート、Do Not Disturb (サイレント) 制御など、電話機の特定の SIP 情報を提供します。</p>  |
| [ダイジェストユー<br>ザー (Digest User) ]  | <p>ダイジェスト認証 (SIP セキュリティ) で使用するこの設定の電話機に関連付けるエンドユーザーを選択します。</p> <p>選択するユーザーのダイジェストクレデンシャルが [エンドユーザーの設定 (End User Configuration) ] ウィンドウで設定されていることを確認してください。</p> <p>電話設定を保存し、設定の更新内容を電話に適用すると、ユーザーのダイジェストクレデンシャルが電話の設定ファイルに追加されます。</p>   |

| フィールド   | 説明   |
|---|--|
| [メディアターミネーションポイントが必須 (Media Termination Point Required) ] | <p>このフィールドを使用して、ATA 187 がサポートしない機能（保留や転送など）を実装するために、メディアターミネーションポイントを使用するかどうかを指示します。</p> <p>MTP を使用して機能を実装する場合は、[メディアターミネーションポイントが必須 (Media Termination Point Required) ] チェックボックスをオンにします。MTP を使用して機能を実装しない場合は、[メディアターミネーションポイントが必須 (Media Termination Point Required) ] チェックボックスをオフにします。</p> <p>このチェックボックスは、ATA 187 クライアントおよび H.245 Empty Capabilities セットをサポートしない ATA 187 デバイスの場合、または単一のソースを介してメディアストリーミングを終了させる場合のみ使用します。</p> <p>このチェックボックスをオンにして、MTP を必須とし、このデバイスをビデオコールのエンドポイントにすると、コールはオーディオのみになります。</p> |
| [不在ポート (Unattended Port) ]                                | <p>このデバイスの不在ポートを指示する場合に、このチェックボックスをオンにします。</p>   |
| [DTMF受信が必要 (Require DTMF Reception) ]                     | <p>SIP と SCCP を実行しているデバイスの場合に、この電話の DTMF 受信を必須にするには、このチェックボックスをオンにします。</p> <p>(注) Cisco Unified Mobility 機能の設定で、SIP トランク（クラスタ間トランク (ICT) またはゲートウェイ）経由で IP 電話のリモート接続先としてクラスタ間 DN を使用する場合、エンタープライズ機能アクセス ミッドコール機能に不可欠な DTMF 番号をアウト オブ バンドで受信できるように、このチェックボックスをオンにします。</p>  |

表 10: 認証局プロキシ機能 (CAPF) 情報 (Certification Authority Proxy Function (CAPF) Information)

| フィールド                           | 説明  |
|---------------------------------|---|
| [証明書操作 (Certificate Operation)] | <p>ドロップダウン リストから、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [保留中の操作なし (No Pending Operation)] : 証明書の操作が行われない場合に表示されます (デフォルトの設定)。</li> <li>• [インストール/更新 (Install/Upgrade)] : 電話機に新しい証明書をインストールするか、既存のローカルで有効な証明書をアップグレードします。</li> <li>• [削除 (Delete)] : 電話機に存在するローカルで有効な証明書を削除します。</li> <li>• [トラブルシューティング (Troubleshoot)] : ローカルで有効な証明書 (LSC) または製造元でインストールされる証明書 (MIC) を取得し、CAPF トレース ファイルで証明書クレデンシャルを表示できます。電話機に両方の証明書タイプが存在する場合、Cisco Unified CM は、証明書のタイプごとに 1 つずつ、2 つのトレース ファイルを作成します。</li> </ul> <p>[トラブルシューティング (Troubleshooting)] オプションを選択して、電話に LSC または MIC が存在することを確認できます。</p> |

| フィールド                                | 説明 |
|--------------------------------------|----|
| [認証モード<br>(Authentication<br>Mode) ] |    |

| フィールド | 説明  |
|-------|---|
|       | <p>このフィールドでは、電話機が CAPF 証明書の操作時に使用する認証方法を選択できます。</p> <p>ドロップダウン リストから、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [認証文字列 (By Authentication String) ] : ユーザーが電話に CAPF 認証文字列を入力した場合にのみ、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。</li> <li>• [Null スtring (By Null String) ] : ユーザーの介入なしで、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。<br/><br/>このオプションではセキュリティが確保されません。したがって、セキュアな閉じた環境の場合にだけこのオプションを選択することを強く推奨します。</li> <li>• [既存の証明書 (LSCを優先) (By Existing Certificate (Precedence to LSC)) ] : 電話機に製造元でインストールされる証明書 (MIC) またはローカルで有効な証明書 (LSC) が存在する場合に、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に LSC が存在する場合、電話機に MIC が存在するかどうかに関係なく、LSC によって認証が行われます。電話機に MIC と LSC が存在する場合、LSC によって認証が行われます。電話機に LSC が存在しないが、MIC が存在する場合、MIC によって認証が行われます。<br/><br/>このオプションを選択する前に、電話機に証明書が存在することを確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。<br/><br/>MIC と LSC が同時に電話機に存在できる場合でも、電話機が CAPF への認証に使用する証明書は常に 1 つだけです。優先されるプライマリ証明書が何らかの理由で破損した場合、または別の証明書を使用して認証を受ける場合は、認証モードを更新する必要があります。</li> <li>• [既存の証明書 (MICを優先) (By Existing Certificate (Precedence to MIC)) ] : 電話機に LSC または MIC が存在する場合に、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に MIC が存在する場合、電話機に LSC が存在するかどうかに関係なく、MIC によって認証が行われます。電話機に LSC が存在するが、MIC が存在しない場合、LSC によって認証が行われます。<br/><br/>このオプションを選択する前に、電話機に証明書が存在すること</li> </ul> |

| フィールド  | 説明   |
|--|--|
|  | <p>を確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。</p> <p>(注) [電話セキュリティプロファイル (Phone Security Profile) ] ウィンドウで設定される CAPF 設定は、[電話の設定 (Phone Configuration) ]ウィンドウで設定される CAPF パラメータと連携します。</p>   |
| <p>[認証文字列 (Authentication String) ]</p>              | <p>[認証モード (Authentication Mode) ] ドロップダウンリストの [認証文字列 (By Authentication String) ] オプションを選択した場合、このフィールドが適用されます。手動で文字列を入力するか、[文字列の生成 (Generate String) ] ボタンをクリックして、文字列を生成します。4 桁から 10 桁の文字列になるようにしてください。</p> <p>ローカルで有効な証明書をインストール、アップグレード、削除、トラブルシューティングするには、電話機ユーザーまたは管理者が電話機に認証文字列を入力する必要があります。</p>  |
| <p>[キー サイズ (ビット) (Key Size (Bits)) ]</p>             | <p>CAPF で使用されるこの設定では、ドロップダウン リストから証明書のキー サイズを選択します。デフォルト設定は 1024 です。その他のオプションには 512 と 2048 があります。</p> <p>デフォルトの設定より大きいキー サイズを選択すると、電話機でキーの生成に必要なエントロピーを生成するのに時間がかかります。キーの生成を低い優先順位で設定すると、操作の実行中に、電話機が機能します。電話機のモデルによっては、キーの生成が完了するまでに、30 分以上かかることがあります。</p> <p>(注) [電話セキュリティプロファイル (Phone Security Profile) ] ウィンドウで設定される CAPF 設定は、[電話の設定 (Phone Configuration) ]ウィンドウで設定される CAPF パラメータと連携します。</p> |
| <p>[操作の完了期限 (Operation Completes by) ]</p>           | <p>このフィールドは、[インストール/アップグレード (Install/Upgrade) ]、[削除 (Delete) ]、[トラブルシューティング (Troubleshoot) ] の証明書の操作オプションをサポートし、操作の完了期限を指定します。</p> <p>表示される値は、パブリッシャ データベース サーバーに適用されます。</p>   |
| <p>[証明書の操作ステータス (Certificate Operation Status) ]</p> | <p>このフィールドには、証明書の操作の進捗状況が表示されます。たとえば、&lt;操作タイプ&gt;保留中、失敗、成功などです。ここで、操作タイプは [インストール/アップグレード (Install/Upgrade) ]、[削除 (Delete) ]、[トラブルシューティング (Troubleshoot) ] 証明書の操作オプションのいずれかになります。このフィールドに表示される情報は変更できません。</p>   |

表 11: [セキュアシェルユーザー (Secure Shell User) ]

| フィールド                                   | 説明  |
|---|---|
| [セキュアシェルユーザー (Secure Shell User) ]      | <p>セキュア シェルユーザーのユーザー ID を入力します。最大 50 文字の英数字または特殊文字を入力できます。無効な文字は、"、%、&amp;、&lt;、&gt;、\ です。このフィールドは、設定している電話デバイスが SSH アクセスをサポートしている場合に表示されます。</p> <p>Cisco Technical Assistance Center (TAC) では、トラブルシューティングやデバッグを行うときにセキュアシェルを使用します。TAC にお問い合わせください。</p> <p>Cisco Unified CM が SSH クレデンシャルを平文で電話機に送信しないようにするために、暗号化された電話の設定ファイルを設定する方法については、このリリースの『Cisco Unified Communications Manager セキュリティガイド』 (<a href="http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html">http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html</a>) を参照してください。</p> |
| [セキュアシェルパスワード (Secure Shell Password) ] | <p>セキュア シェルユーザーのパスワードを入力します。最大 200 文字の英数字または特殊文字を入力できます。無効な文字は、"、%、&amp;、&lt;、&gt;、\ です。TAC にお問い合わせください。</p> <p>『Cisco Unified Communications Manager セキュリティ ガイド』 (<a href="http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html">http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html</a>) を参照してください。</p>  |

表 12: 製品固有の設定

| フィールド                     | 説明  |
|---------------------------|---|
| デバイス製造元が定義するモデル固有の設定フィールド | <p>製品固有の設定項目のフィールドの説明とヘルプを表示するには、[製品固有の設定 (Product Specific Configuration) ] エリアで [?] 「」 情報アイコンをクリックし、ポップアップダイアログボックスでヘルプを表示します。</p> <p>詳細については、ATA 187 のドキュメントを参照してください。</p> |



## アナログ電話アダプタ 190 設定フィールド

表 13: アナログ電話アダプタ 190 設定フィールド

| フィールド                                    | 説明  |
|--|---|
| MACアドレス (MAC Address)                    | <p>ATA 190 を特定する Media Access Control (MAC) アドレスを入力します。値が 12 桁の 16 進文字列で構成されていることを確認します。</p> <p>次のいずれかの方法で、ATA 190 の MAC アドレスを判別できます。</p> <ul style="list-style-type: none"> <li>• ATA 190 の背面にある MAC ラベルを確認します。</li> <li>• ATA 190 の ウェブ ページを表示し、[デバイス情報 (Device Information)] ハイパーリンクをクリックします。</li> </ul> |
| [説明 (Description)]                       | <p>ATA 190 の説明テキストを入力します。</p> <p>このフィールドには、128 文字までの値を入力できます。二重引用符 (")、山カッコ (&lt;&gt;)、バックスラッシュ (\)、アンパサンド (&amp;)、パーセント記号 (%) を除くすべての文字を使用できます。</p>  |
| [デバイスプール (Device Pool)]                  | <p>ATA 190 を割り当てるデバイスプールを選択します。デバイスプールでは、複数のデバイスに共通の特性 (リージョン、日時グループ、ソフトキーテンプレートなど) のセットを定義します。</p> <p>デバイスプール構成の設定を確認するには、[詳細の表示 (View Details)] リンクをクリックします。</p>  |
| [共通デバイス設定 (Common Device Configuration)] | <p>ATA 190 を割り当てる共通デバイス設定を選択します。</p> <p>[共通デバイス設定 (Common Device Configuration)] の設定を表示するには、[詳細の表示 (View Details)] リンクをクリックします。</p>   |
| [電話ボタンテンプレート (Phone Button Template)]    | <p>適切な電話ボタンテンプレートを選択します。電話ボタンテンプレートでは、電話機上のボタンを設定し、各ボタンにどの機能 (回線、スピードダイヤルなど) を使用するかを特定します。</p>  |
| [共通の電話プロフィール (Common Phone Profile)]     | <p>ドロップダウンリストで、使用可能な共通の電話プロフィールのリストから共通の電話プロフィールを選択します。</p> <p>[共通の電話プロフィール (Common Phone Profile)] の設定を表示するには、[詳細の表示 (View Details)] リンクをクリックします。</p>  |
| [コーリングサーチスペース (Calling Search Space)]    | <p>ドロップダウンリストを使用から、コーリングサーチスペースを選択するか、コーリングサーチスペースをデフォルトの[なし (None)]のままにします。</p>  |

| フィールド  | 説明  |
|--|---|
| [AARコーリングサーチスペース (AAR Calling Search Space) ]  | ドロップダウンリストから、自動代替ルーティング (AAR) を実行したときに使用するデバイスの適切なコーリングサーチスペースを選択するか、コーリングサーチスペースをデフォルトの [なし (None) ] のままにします。  |
| [メディアリソースグループリスト (Media Resource Group List) ] | 適切なメディアリソースグループリストを選択します。メディアリソースグループリストは、優先順位順に並べられたメディアリソースグループから構成されます。<br><br>[<なし> (<None>)] を選択すると、Cisco Unified CM はデバイスプールで定義されたメディアリソースグループリストを使用します。                    |
| [ユーザー保留 MOH 音源 (User Hold MOH Audio Source) ]  | ドロップダウンリストから、ユーザーが保留操作を開始する場合に保留音 (MOH) として使用するオーディオソースを選択します。  |
| [ロケーション (Location) ]                           | ドロップダウンリストから、デバイスプール内の電話およびゲートウェイと関連付けられている場所を選択します。  |
| [AARグループ (AAR Group) ]                         | このデバイスの自動代替ルーティング (AAR) グループを選択します。AARグループはプレフィックス番号を設定します。この番号は、帯域幅不足のためにブロックされるコールをルーティングする際に使用されます。AARグループが指定されていない場合、Cisco Unified CM はデバイスプールまたは回線に関連付けられている AAA グループを使用します。 |
| [ユーザーロケール (User Locale) ]                      | ドロップダウンリストから、CTIポートに関連付けられたユーザーロケールを選択します。そのユーザーロケールは、言語とフォントを含んだ、ユーザーをサポートする一連の詳細情報を識別します。<br><br>ユーザーロケールが指定されていない場合、Cisco Unified CM はデバイスプールに関連付けられたユーザーロケールを使用します。           |
| [ネットワークロケール (Network Locale) ]                 | ドロップダウンリストから、CTIポートに関連付けられたネットワークロケールを選択します。ネットワークロケールには、特定の地理的領域の電話が使用するトーンとパターンの定義が含まれています。<br><br>ネットワークロケールが指定されていない場合、Cisco Unified CM はデバイスプールに関連付けられたネットワークロケールを使用します。     |

| フィールド                                  | 説明  |
|--|---|
| [ビルトインブリッジ (Built In Bridge) ]         | [ビルトインブリッジ (Built In Bridge) ] ドロップダウン リストを使用して割り込み機能用の組み込み型会議ブリッジを有効または無効にします。次のいずれかを実行します。 <ul style="list-style-type: none"> <li>• オン</li> <li>• オフ</li> <li>• デフォルト</li> </ul>  |
| [プライバシー (Privacy) ]                    | プライバシーについて、[プライバシー (Privacy) ] ドロップダウン リストから [オン (On) ] を選択します。   |
| [デバイスモビリティモード (Device Mobility Mode) ] | ドロップダウンリストから、このデバイスのデバイスモビリティ機能をオンまたはオフにします。デフォルトのデバイスモビリティモードを使用する場合は、[デフォルト (Default) ] を選択します。デフォルトの設定では、デバイスの[デバイスモビリティモード (Device Mobility Mode) ] サービス パラメータの値が使用されます。  |
| [オーナー (Owner) ]                        | オーナーのタイプとして、[ユーザー (User) ] または [名前非表示 (パブリック/共有スペース) (Anonymous (Public/Shared Space)) ] を選択します。  |
| [オーナーのユーザー ID (Owner User ID) ]        | ドロップダウンリストから、割り当てられた電話ユーザーのユーザー ID を選択します。ユーザー ID は、このデバイスから発信されるすべてのコールの呼詳細レコード (CDR) に記録されます。デバイスにユーザー ID を割り当てると、[ライセンスの使用状況レポート (License Usage Report) ] でデバイスが [未割り当てデバイス (Unassigned Devices) ] から [ユーザー (Users) ] に移動します。<br><br>(注) エクステンションモビリティを使用する場合は、このフィールドを設定しないでください。エクステンションモビリティでは、デバイスのオーナーはサポートされていません。 |
| [電話ロード名 (Phone Load Name) ]            | ATA 190 のカスタム ソフトウェアを入力します。   |

| フィールド   | 説明   |
|---|--|
| [トラステッドリレーポイントを使用 (Use Trusted Relay Point) ] | <p>次の値のいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [オフ (Off) ]: このデバイスで、トラステッドリレー ポイント (TRP) の使用を無効にするには、この値を選択します。この設定は、このデバイスに関連付けられている共通デバイス設定の[トラステッドリレーポイントを使用 (Use Trusted Relay Point) ]設定よりも優先されます。</li> <li>• [オン (On) ]: このデバイスでの TRP の使用を有効にする場合は、この値を選択します。この設定は、このデバイスに関連付けられている共通デバイス設定の[トラステッドリレーポイントを使用 (Use Trusted Relay Point) ]設定よりも優先されます。</li> <li>• [デフォルト (Default) ]: この値を選択した場合、デバイスはこのデバイスが関連付けられている共通デバイス設定の[トラステッドリレーポイントを使用 (Use Trusted Relay Point) ]設定を使用します。</li> </ul> |
| 常にプライム回線を使用する (Always Use Prime Line)         | <p>ドロップダウン リストから、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [オフ (Off) ]: 電話がアイドル状態になっているときにいずれかの回線でコールを受信すると、電話のユーザは、コールを受信した回線からコールに応答します。</li> <li>• [オン (On) ]: 電話機がアイドル状態 (オフフック) になっているときにいずれかの回線でコールを受信すると、このコールにはプライマリ回線が選択されます。他の回線のコールは鳴り続け、電話機ユーザはそれらの他の回線を選択して、これらのコールに応答する必要があります。</li> <li>• デフォルト: Unified Communications Manager は、[常にプライム回線を使用する (Always Use Prime Line) ]サービスパラメータの設定を使用します。これにより、Cisco CallManager サービスがサポートされます。</li> </ul>                                   |

| フィールド   | 説明   |
|---|--|
| ボイスメッセージには常にプライム回線を使用する (Always Use Prime Line for Voice Message)                     | <p>ドロップダウンリストから、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [オフ (Off)] : 電話がアイドル状態の場合、電話のメッセージボタンを押すと、ボイスメッセージが設定されている回線からボイスメッセージシステムに自動的にダイヤルされます。Unified Communications Manager は、常に音声メッセージのある最初の回線を選択します。ボイスメッセージが設定されている回線が存在しない場合に電話のユーザーが [メッセージ (Messages)] ボタンを押すと、プライマリ回線が使用されます。</li> <li>• [オン (On)] : 電話がアイドル状態の場合に電話のメッセージボタンを押すと、電話のプライマリ回線がボイスメッセージを受信するアクティブな回線になります。</li> <li>• デフォルト : Unified Communications Manager は、[ボイスメッセージには常にプライム回線を使用する (Always Use Prime Line for Voice Message)] サービスパラメータの設定を使用します。これにより、Cisco CallManager サービスがサポートされます。</li> </ul> |
| [地理位置情報 (GeoLocation)]  | <p>ドロップダウンリストから地理位置情報を選択します。</p> <p>[未指定の地理位置情報 (Unspecified geolocation)] を選択すると、このデバイスを地理位置情報に関連付けないように指定できます。</p> <p>さらに、[システム (System)] &gt; [地理位置情報の設定 (Geolocation Configuration)] メニュー オプションで設定した地理位置情報も選択できます。</p>   |
| [プレゼンテーションインジケータを無視 (内線コールのみ) (Ignore Presentation Indicators (internal calls only))] | <p>コール単位でコール表示制限を設定する場合に、このチェックボックスをオンにします。このチェックボックスをオンにすると、Unified Communications Manager は内線コールについて受信するすべての表示制限を無視します。</p> <p>この設定と、トランスレーションパターンレベルでの発信者回線 ID の表示および接続回線 ID の表示の設定を組み合わせ使用します。これらの設定を組み合わせ使用すれば、コールごとに発信側または接続先の回線表示情報を選択的に表示またはブロックするようにコール表示制限を設定できます。</p>   |
| [ハントグループにログイン (Logged into Hunt Group)]   | <p>ATA 190 をハントリストに追加すると、管理者はこのチェックボックスをオン (またはオフ) にして、ユーザーをログインまたはログアウトさせることができます。</p> <p>ユーザーは電話のソフトキーを使用して、電話をハントリストにログインまたはログアウトします。</p>   |

| フィールド                           | 説明   |
|---------------------------------|--|
| [リモートデバイス (Remote Device) ]     | <p>このチェックボックスをオンにすると、デバイスの登録時にバッファを割り当て、SCCP メッセージを電話機にバンドルします。</p> <p>ヒント この機能はリソースを消費するため、シグナリングの遅延が発生している場合にのみ、このチェックボックスをオンにしてください。</p>  |
| [保護されたデバイス (Protected Device) ] | <p>電話機を保護されたデバイスとして指定するには、このチェックボックスをオンにします。この場合、電話機が2秒間トーンを再生してユーザーにコールが暗号化されていることを通知できます。また、発信側と着信側の両方の電話機が保護されたデバイスとして設定できます。このトーンは、コールが応答されたとき、発信側と着信側の両者に対して再生されます。このトーンは、発信側と着信側の両方の電話機が保護されていて、なおかつ暗号化メディア上でコールが行われたときでなければ再生されません。</p> <p>このチェックボックスをオンにすると、再生するセキュア通知トーンの複数の設定要件のうち1つのみが表示されます。セキュア通知トーン機能および設定要件の詳細については、『Cisco Unified Communications Manager セキュリティ ガイド』（<a href="http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html">http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html</a>）を参照してください。</p> <p>このチェックボックスがオンで、システムがコールは暗号化されていないと判断すると、電話は非セキュア通知トーンを再生して、コールが保護されていないことをユーザーに通知します。</p> |

### [番号表示トランスフォーメーション (Number Presentation Transformation) ]

表 14: [この電話からのコールの発信者ID (Caller ID For Calls From This Phone) ]

| フィールド   | 説明  |
|---|---|
| [発信側トランスフォーメーションCSS (Calling Party Transformation CSS) ]                            | <p>この設定により、デバイスの発信者番号をローカライズできます。選択した発信側トランスフォーメーションCSSに、このデバイスに割り当てる発信側トランスフォーメーションパターンが含まれていることを確認してください。</p>   |
| [デバイスプールの発信側トランスフォーメーションCSSを使用 (Use Device Pool Calling Party Transformation CSS) ] | <p>このデバイスに割り当てられているデバイスプールに設定されている発信側トランスフォーメーションCSSを使用する場合は、このボックスをオンにします。このチェックボックスを選択しない場合、デバイスは[トランク設定 (Trunk Configuration) ]ウィンドウで設定した発信側変換CSSを使用します。</p> |

表 15: [リモート番号 (Remote Number) ]

| フィールド   | 説明  |
|---|---|
| [発信側トランスフォーメーションCSS (Calling Party Transformation CSS) ]                            | ドロップダウンリストから、このデバイスに受信したコールのリモート発信者番号に適用する、発信側トランスフォーメーションパターンを含むコーリングサーチスペース (CSS) を選択します。 |
| [デバイスプールの発信側トランスフォーメーションCSSを使用 (Use Device Pool Calling Party Transformation CSS) ] | リモート通話とリモート接続番号の変換に、このデバイスが属するデバイスプールで設定されている発信側トランスフォーメーションCSSを適用するには、このチェックボックスをオンにします。   |

表 16: [プロトコル固有情報 (Protocol Specific Information) ]

| フィールド                                 | 説明  |
|---------------------------------------|---|
| [パケットキャプチャモード (Packet Capture Mode) ] | <p>この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケットキャプチャを実行すると、CPUの使用率が上昇して、コール処理が妨げられる可能性があります。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。</p> <ul style="list-style-type: none"> <li>• [なし (None) ] : このオプションは、パケットキャプチャが発生しないことを示します (デフォルト設定)。この設定は、パケットキャプチャの完了後に行います。</li> <li>• [バッチ処理モード (Batch Processing Mode) ] : Cisco Unified CM が、復号されたメッセージや暗号化されていないメッセージをファイルに書き込み、システムが各ファイルを暗号化します。システムでは、毎日新しいファイルが新しい暗号キーを使用して作成されます。Cisco Unified CM はファイルを7日間保存し、さらにファイルを暗号化するキーを安全な場所に保存します。Cisco Unified CM は、PktCap 仮想ディレクトリにファイルを保存します。1つのファイルの中に、タイムスタンプ、送信元IPアドレス、送信元IPポート、宛先IPアドレス、パケットのプロトコル、メッセージの長さ、およびメッセージが保持されます。TACのデバッグツールでは、HTTPS、管理者のユーザ名とパスワード、および指定された日付を使用して、キャプチャされたパケットを保持している暗号化済みファイルを1つだけ要求します。同様にこのツールでは、暗号化ファイルを復号化するためのキー情報を要求します。</li> </ul> |

| フィールド   | 説明  |
|---|---|
| [パケットキャプチャ時間 (Packet Capture Duration) ]          | <p>この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケットキャプチャを実行すると、CPUの使用率が上昇して、コール処理が妨げられる可能性があります。</p> <p>このフィールドには、1つのパケットキャプチャセッションに割り当てる時間の上限 (分単位) を指定します。デフォルト設定は0で、範囲は0～300分です。</p> <p>パケットキャプチャを開始するには、フィールドに0以外の値を入力します。パケットキャプチャが完了すると、値0が表示されます。</p>  |
| [BLFプレゼンスグループ (BLF Presence Group) ]              | <p>ドロップダウンリストから、エンドユーザーの話中ランプフィールド (BLF) プレゼンスグループを選択します。選択したグループは、エンドユーザーがモニター可能な接続先を指定します。</p> <p>BLF プレゼンスグループのデフォルト値は [標準のプレゼンスグループ (Standard Presence group) ] であり、インストール時に設定されます。Cisco Unified CM Administration で設定されている BLF プレゼンスグループは、ドロップダウンリストにも表示されます。</p>  |
| [SIPダイヤルルール (SIP Dial Rules) ]                    | <p>必要に応じて、適切な SIP ダイヤルルールを選択します。SIP ダイヤルルールは、Cisco Unified IP Phone 7940 および 7960 のローカルダイヤルプランを提供するため、ユーザーは、コールが処理される前に、キーを押したり、タイマーを待機したりする必要はありません。</p> <p>SIP を実行している IP 電話にダイヤルルールを適用しない場合は、[SIP ダイヤルルール (SIP Dial Rules) ] フィールドを [なし (&lt;None&gt;)] に設定したままにします。これは、コールが処理される前に、ユーザーがダイヤルソフトキーを使用するか、タイマーが切れるまで待つ必要があることを示します。</p> |
| [MTP優先発信コーデック (MTP Preferred Originating Codec) ] | <p>メディアターミネーションポイントが SIP のコールに必要な場合は、ドロップダウンリストから使用するコーデックを選択します。</p>   |
| [デバイスのセキュリティプロファイル (Device Security Profile) ]    | <p>デバイスに適用するセキュリティプロファイルを選択します。</p> <p>Unified Communications Manager Administration で設定するすべてのデバイスに、セキュリティプロファイルを適用する必要があります。</p>   |



| フィールド  | 説明   |
|--|--|
| [再ルーティング用<br>コーリングサーチス<br>ペース (Rerouting<br>Calling Search<br>Space) ] | <p>ドロップダウンリストから、再ルーティングに使用するコーリングサーチスペースを選択します。</p> <p>リファラーの再ルーティングコーリングサーチスペースを使用して、参照先へのルートが検索されます。再ルーティングコーリングサーチスペースが原因で参照が失敗すると、Refer Primitive は「405 Method Not Allowed」メッセージによって要求を拒否します。</p> <p>リダイレクト (3xx) プリミティブおよび転送機能も再ルーティングコーリングサーチスペースを使用して、リダイレクト先または転送先を検索します。</p>  |
| [SUBSCRIBEコーリン<br>グサーチスペース<br>(AAR Calling Search<br>Space) ]          | <p>プレゼンス機能によってサポートされる SUBSCRIBE コーリングサーチスペースは、エンドユーザから受け取ったプレゼンス要求を Unified Communications Manager がルーティングする方法を決定します。この設定では、エンドユーザーのプレゼンス (SUBSCRIBE) 要求のコール処理サーチスペースと別にコーリングサーチスペースを適用できます。</p> <p>ドロップダウンリストから、エンドユーザーのプレゼンス要求に使用する SUBSCRIBE コーリングサーチスペースを選択します。Cisco Unified Communications Manager Administration で設定するすべてのコーリングサーチスペースが、[SUBSCRIBE コーリングサーチスペース (SUBSCRIBE Calling Search Space) ] ドロップダウンリストに表示されます。</p> <p>ドロップダウンリストから、エンドユーザーに別のコーリングサーチスペースを選択しない場合、SUBSCRIBE コーリングサーチスペースのデフォルトは [なし (None) ] に設定されます。</p> <p>この目的専用の SUBSCRIBE コーリングサーチスペースを設定するには、他のコーリングサーチスペースと同様に新しいコーリングサーチスペースを設定します。</p> |
| [SIPプロファイル<br>(SIP Profile) ]  | <p>デフォルトの SIP プロファイルまたは作成済みの特定のプロファイルを選択します。SIP プロファイルでは、登録タイマーおよびキープアライブタイマー、メディアポート、Do Not Disturb (サイレント) 制御など、電話機の特定の SIP 情報を提供します。</p>  |

| フィールド   | 説明   |
|---|--|
| [ダイジェストユーザー (Digest User) ]                               | <p>ダイジェスト認証 (SIP セキュリティ) で使用するこの設定の電話機に関連付けるエンドユーザーを選択します。</p> <p>選択するユーザーのダイジェスト クレデンシャルが [エンドユーザーの設定 (End User Configuration) ] ウィンドウで設定されていることを確認してください。</p> <p>電話設定を保存し、設定の更新内容を電話に適用すると、ユーザーのダイジェストクレデンシャルが電話の設定ファイルに追加されます。</p> <p>ダイジェスト認証の詳細については、『Cisco Unified Communications Manager セキュリティ ガイド』 (<a href="http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html">http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html</a>) を参照してください。</p> |
| [メディアターミネーションポイントが必須 (Media Termination Point Required) ] | <p>このフィールドを使用して、ATA 190 でサポートされていない機能 (保留や転送など) を実装するために、メディアターミネーションポイントを使用するかどうかを指示します。</p> <p>MTP を使用して機能を実装する場合は、[メディアターミネーションポイントが必須 (Media Termination Point Required) ] チェックボックスをオンにします。MTP を使用して機能を実装しない場合は、[メディアターミネーションポイントが必須 (Media Termination Point Required) ] チェックボックスをオフにします。</p> <p>このチェックボックスは、ATA 190 クライアントおよび H.245 Empty Capabilities Set をサポートしていない ATA 190 デバイスの場合、または単一ソースを通してメディアストリーミングを終了させる場合にのみ使用します。</p> <p>このチェックボックスをオンにして、MTP を必須とし、このデバイスをビデオコールのエンドポイントにすると、コールはオーディオのみになります。</p>   |
| [不在ポート (Unattended Port) ]                                | <p>このデバイスの不在ポートを指示する場合に、このチェックボックスをオンにします。</p>   |
| [DTMF受信が必要 (Require DTMF Reception) ]                     | <p>SIP と SCCP を実行しているデバイスの場合に、この電話の DTMF 受信を必須にするには、このチェックボックスをオンにします。</p> <p>(注) Cisco Unified Mobility 機能の設定で、SIP トランク (クラスター間トランク (ICT) またはゲートウェイ) 経由で IP 電話のリモート接続先としてクラスター間 DN を使用する場合、エンタープライズ機能アクセス ミッドコール機能に不可欠な DTMF 番号をアウトオブバンドで受信できるように、このチェックボックスをオンにします。</p>  |

表 17: [認証局プロキシ機能 (CAPF) 情報 (Certification Authority Proxy Function (CAPF) Information) ]

| フィールド                             | 説明  |
|-----------------------------------|---|
| [証明書の操作 (Certificate Operation) ] | <p>ドロップダウンリストから、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [保留中の操作なし (No Pending Operation) ] : 証明書の操作が行われない場合に表示されます (デフォルトの設定)。</li> <li>• [インストール/更新 (Install/Upgrade) ] : 電話機に新しい証明書をインストールするか、既存のローカルで有効な証明書をアップグレードします。</li> <li>• [削除 (Delete) ] : 電話機に存在するローカルで有効な証明書を削除します。</li> <li>• [トラブルシューティング (Troubleshoot) ] : ローカルで有効な証明書 (LSC) または製造元でインストールされる証明書 (MIC) を取得し、CAPF トレース ファイルで証明書クレデンシャルを表示できます。電話機に両方の証明書タイプが存在する場合、Cisco Unified CM は、証明書のタイプごとに1つずつ、2つのトレースファイルを作成します。</li> </ul> <p>[トラブルシューティング (Troubleshooting) ] オプションを選択して、電話に LSC または MIC が存在することを確認できます。</p> <p>CAPF 操作の詳細については、『Cisco Unified Communications Manager セキュリティ ガイド』 (<a href="http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html">http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html</a>) を参照してください。</p> |

| フィールド                                | 説明 |
|--------------------------------------|----|
| [認証モード<br>(Authentication<br>Mode) ] |    |

| フィールド | 説明   |
|-------|--|
|       | <p>このフィールドでは、電話機が CAPF 証明書の操作時に使用する認証方法を選択できます。</p> <p>ドロップダウンリストから、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [認証文字列 (By Authentication String) ] : ユーザーが電話に CAPF 認証文字列を入力した場合にのみ、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。</li> <li>• [Null スtring (By Null String) ] : ユーザーの介入なしで、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。<br/><br/>このオプションではセキュリティが確保されません。したがって、セキュアな閉じた環境の場合にだけこのオプションを選択することを強く推奨します。</li> <li>• [既存の証明書 (LSCを優先) (By Existing Certificate (Precedence to LSC)) ] : 電話機に製造元でインストールされる証明書 (MIC) またはローカルで有効な証明書 (LSC) が存在する場合に、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に LSC が存在する場合、電話機に MIC が存在するかどうかに関係なく、LSC によって認証が行われます。電話機に MIC と LSC が存在する場合、LSC によって認証が行われます。電話機に LSC が存在しないが、MIC が存在する場合、MIC によって認証が行われます。<br/><br/>このオプションを選択する前に、電話機に証明書が存在することを確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。<br/><br/>MIC と LSC が同時に電話機に存在できる場合でも、電話機が CAPF への認証に使用する証明書は常に 1 つだけです。優先されるプライマリ証明書が何らかの理由で破損した場合、または別の証明書を使用して認証を受ける場合は、認証モードを更新する必要があります。</li> <li>• [既存の証明書 (MICを優先) (By Existing Certificate (Precedence to MIC)) ] : 電話機に LSC または MIC が存在する場合に、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に MIC が存在する場合、電話機に LSC が存在するかどうかに関係なく、MIC によって認証が行われます。電話機に LSC が存在するが、MIC が存在しない場合、LSC によって認証が行われます。<br/><br/>このオプションを選択する前に、電話機に証明書が存在すること</li> </ul> |

| フィールド   | 説明   |
|---|--|
|   | <p>を確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。</p> <p>(注) [電話セキュリティプロファイル (Phone Security Profile) ] ウィンドウで設定される CAPF 設定は、[電話の設定 (Phone Configuration) ] ウィンドウで設定される CAPF パラメータと連携します。</p>  |
| [認証文字列 (Authentication String) ]              | <p>[認証モード (Authentication Mode) ] ドロップダウンリストの [認証文字列 (By Authentication String) ] オプションを選択した場合、このフィールドが適用されます。手動で文字列を入力するか、[文字列の生成 (Generate String) ] ボタンをクリックして、文字列を生成します。4 桁から 10 桁の文字列になるようにしてください。</p> <p>ローカルで有効な証明書をインストール、アップグレード、削除、トラブルシューティングするには、電話機ユーザーまたは管理者が電話機に認証文字列を入力する必要があります。</p>  |
| [キー サイズ (ビット) (Key Size (Bits) ) ]            | <p>CAPF で使用されるこの設定では、ドロップダウン リストから証明書のキー サイズを選択します。デフォルト設定は 1024 です。その他のオプションには 512 と 2048 があります。</p> <p>デフォルトの設定より大きいキーサイズを選択すると、電話機でキーの生成に必要なエントロピーを生成するのに時間がかかります。キーの生成を低い優先順位で設定すると、操作の実行中に、電話機が機能します。電話機のモデルによっては、キーの生成が完了するまでに、30 分以上かかることがあります。</p> <p>(注) [電話セキュリティプロファイル (Phone Security Profile) ] ウィンドウで設定される CAPF 設定は、[電話の設定 (Phone Configuration) ] ウィンドウで設定される CAPF パラメータと連携します。</p> |
| [操作の完了期限 (Operation Completes by) ]           | <p>このフィールドは、[インストール/アップグレード (Install/Upgrade) ]、[削除 (Delete) ]、[トラブルシューティング (Troubleshoot) ] の証明書の操作オプションをサポートし、操作の完了期限を指定します。</p> <p>表示される値は、パブリッシュ データベース サーバーに適用されます。</p>   |
| [証明書の操作ステータス (Certificate Operation Status) ] | <p>このフィールドには、証明書の操作の進捗状況が表示されます。たとえば、&lt;操作タイプ&gt;保留中、失敗、成功などです。ここで、操作タイプは [インストール/アップグレード (Install/Upgrade) ]、[削除 (Delete) ]、[トラブルシューティング (Troubleshoot) ] 証明書の操作オプションのいずれかになります。このフィールドに表示される情報は変更できません。</p>   |

表 18: [セキュアシェルユーザー (Secure Shell User) ]

| フィールド                                   | 説明   |
|---|--|
| [セキュアシェルユーザー (Secure Shell User) ]      | <p>セキュア シェル ユーザーのユーザー ID を入力します。最大 50 文字の英数字または特殊文字を入力できます。無効な文字は、"、%、&amp;、&lt;、&gt;、\ です。このフィールドは、設定している電話デバイスが SSH アクセスをサポートしている場合に表示されます。</p> <p>Cisco Technical Assistance Center (TAC) では、トラブルシューティングやデバッグを行うときにセキュア シェルを使用します。TAC にお問い合わせください。</p> <p>Cisco Unified CM が SSH クレデンシャルを平文で電話機に送信しないようにするために、暗号化された電話の設定ファイルを設定する方法については、このリリースの『Cisco Unified Communications Manager セキュリティ ガイド』 (<a href="http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html">http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html</a>) を参照してください。</p> |
| [セキュアシェルパスワード (Secure Shell Password) ] | <p>セキュア シェル ユーザーのパスワードを入力します。最大 127 文字の英数字や特殊文字を入力できます。無効な文字は、"、%、&amp;、&lt;、&gt;、\ です。TAC にお問い合わせください。</p> <p>Cisco Unified CM が SSH クレデンシャルを平文で電話機に送信しないようにするために、暗号化された電話の設定ファイルを設定する方法については、このリリースの『Cisco Unified Communications Manager セキュリティ ガイド』 (<a href="http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html">http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html</a>) を参照してください。</p>   |

表 19: 製品固有の設定

| フィールド                     | 説明  |
|---------------------------|---|
| デバイス製造元が定義するモデル固有の設定フィールド | <p>製品固有の設定項目のフィールドの説明とヘルプを表示するには、[製品固有の設定 (Product Specific Configuration) ] エリアで [?] 「」 情報アイコンをクリックし、ポップアップダイアログボックスでヘルプを表示します。</p> <p>詳細については、ATA 190 のドキュメントを参照してください。</p> |

## アナログ電話アダプタ 191 設定フィールド

表 20: アナログ電話アダプタ 191 設定フィールド

| フィールド                                    | 説明  |
|--|---|
| MACアドレス (MAC Address)                    | <p>ATA 191 を識別する Media Access Control (MAC) アドレスを入力します。値が 12 桁の 16 進文字列で構成されていることを確認します。</p> <p>次のいずれかの方法で、ATA 191 の MAC アドレスを判別できます。</p> <ul style="list-style-type: none"> <li>• ATA 191 の背面にある MAC ラベルを確認する。</li> <li>• ATA 191 の ウェブ ページを表示し、[デバイス情報 (Device Information)] ハイパーリンクをクリックする。</li> </ul> |
| [説明 (Description)]                       | <p>ATA 191 のテキストの説明を入力します。</p> <p>このフィールドには、128 文字までの値を入力できます。二重引用符 (")、山カッコ (&lt;&gt;)、バックスラッシュ (\)、アンパサンド (&amp;)、パーセント記号 (%) を除くすべての文字を使用できます。</p>   |
| [デバイスプール (Device Pool)]                  | <p>ATA 191 を割り当てるデバイスプールを選択します。デバイスプールでは、複数のデバイスに共通の特性 (リージョン、日時グループ、ソフトキー テンプレートなど) のセットを定義します。</p> <p>デバイスプール構成の設定を確認するには、[詳細の表示 (View Details)] リンクをクリックします。</p>   |
| [共通デバイス設定 (Common Device Configuration)] | <p>ATA 191 を割り当てる共通デバイス設定を選択します。</p> <p>[共通デバイス設定 (Common Device Configuration)] の設定を表示するには、[詳細の表示 (View Details)] リンクをクリックします。</p>   |
| [電話ボタンテンプレート (Phone Button Template)]    | <p>適切な電話ボタンテンプレートを選択します。電話ボタンテンプレートでは、電話機上のボタンを設定し、各ボタンにどの機能 (回線、スピードダイヤルなど) を使用するかを特定します。</p>  |
| [共通の電話プロファイル (Common Phone Profile)]     | <p>ドロップダウンリストで、使用可能な共通の電話プロファイルのリストから共通の電話プロファイルを選択します。</p> <p>[共通の電話プロファイル (Common Phone Profile)] の設定を表示するには、[詳細の表示 (View Details)] リンクをクリックします。</p>  |
| [コーリングサーチスペース (Calling Search Space)]    | <p>ドロップダウンリストを使用から、コーリングサーチスペースを選択するか、コーリングサーチスペースをデフォルトの[なし (None)]のままにします。</p>  |



| フィールド  | 説明  |
|--|---|
| [AARコーリングサーチスペース (AAR Calling Search Space) ]  | ドロップダウンリストから、自動代替ルーティング (AAR) を実行したときに使用するデバイスの適切なコーリングサーチスペースを選択するか、コーリングサーチスペースをデフォルトの [なし (None) ] のままにします。  |
| [メディアリソースグループリスト (Media Resource Group List) ] | 適切なメディアリソースグループリストを選択します。メディアリソースグループリストは、優先順位順に並べられたメディアリソースグループから構成されます。<br><br>[<なし> (<None>)] を選択すると、Cisco Unified CM はデバイスプールで定義されたメディアリソースグループリストを使用します。                      |
| [ユーザー保留 MOH 音源 (User Hold MOH Audio Source) ]  | ドロップダウンリストから、ユーザーが保留操作を開始する場合に保留音 (MOH) として使用するオーディオソースを選択します。  |
| [ロケーション (Location) ]                           | ドロップダウンリストから、デバイスプール内の電話およびゲートウェイと関連付けられている場所を選択します。  |
| [AARグループ (AAR Group) ]                         | このデバイスの自動代替ルーティング (AAR) グループを選択します。AAR グループはプレフィックス番号を設定します。この番号は、帯域幅不足のためにブロックされるコールをルーティングする際に使用されます。AAR グループが指定されていない場合、Cisco Unified CM はデバイスプールまたは回線に関連付けられている AAA グループを使用します。 |
| [ユーザーロケール (User Locale) ]                      | ドロップダウンリストから、CTI ポートに関連付けられたユーザーロケールを選択します。そのユーザーロケールは、言語とフォントを含んだ、ユーザーをサポートする一連の詳細情報を識別します。<br><br>ユーザーロケールが指定されていない場合、Cisco Unified CM はデバイスプールに関連付けられたユーザーロケールを使用します。            |
| [ネットワークロケール (Network Locale) ]                 | ドロップダウンリストから、CTI ポートに関連付けられたネットワークロケールを選択します。ネットワークロケールには、特定の地理的領域の電話が使用するトーンとパターンの定義が含まれています。<br><br>ネットワークロケールが指定されていない場合、Cisco Unified CM はデバイスプールに関連付けられたネットワークロケールを使用します。      |

| フィールド                                  | 説明  |
|--|---|
| [ビルトインブリッジ (Built In Bridge) ]         | [ビルトインブリッジ (Built In Bridge) ] ドロップダウンリストを使用して割り込み機能用の組み込み型会議ブリッジを有効または無効にします。次のいずれかを実行します。 <ul style="list-style-type: none"> <li>• オン</li> <li>• オフ</li> <li>• デフォルト</li> </ul>   |
| [プライバシー (Privacy) ]                    | プライバシーについて、[プライバシー (Privacy) ] ドロップダウンリストから [オン (On) ] を選択します。  |
| [デバイスモビリティモード (Device Mobility Mode) ] | ドロップダウンリストから、このデバイスのデバイスモビリティ機能をオンまたはオフにします。デフォルトのデバイスモビリティモードを使用する場合は、[デフォルト (Default) ] を選択します。デフォルトの設定では、デバイスの [デバイスモビリティモード (Device Mobility Mode) ] サービス パラメータの値が使用されます。   |
| [オーナー (Owner) ]                        | オーナーのタイプとして、[ユーザー (User) ] または [名前非表示 (パブリック/共有スペース) (Anonymous (Public/Shared Space)) ] を選択します。  |
| [オーナーのユーザー ID (Owner User ID) ]        | ドロップダウンリストから、割り当てられた電話ユーザーのユーザー ID を選択します。ユーザー ID は、このデバイスから発信されるすべてのコールの呼詳細レコード (CDR) に記録されます。デバイスにユーザー ID を割り当てると、[ライセンスの使用状況レポート (License Usage Report) ] でデバイスが [未割り当てデバイス (Unassigned Devices) ] から [ユーザー (Users) ] に移動します。 <p>(注) エクステンションモビリティを使用する場合は、このフィールドを設定しないでください。エクステンションモビリティでは、デバイスのオーナーはサポートされていません。</p> |
| [電話ロード名 (Phone Load Name) ]            | ATA 191 のカスタム ソフトウェアを入力します。   |

| フィールド   | 説明  |
|---|---|
| [トラステッドリレーポイントを使用 (Use Trusted Relay Point) ] | <p>次の値のいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [オフ (Off) ]: このデバイスで、トラステッドリレーポイント (TRP) の使用を無効にするには、この値を選択します。この設定は、このデバイスに関連付けられている共通デバイス設定の[トラステッドリレーポイントを使用 (Use Trusted Relay Point) ]設定よりも優先されます。</li> <li>• [オン (On) ]: このデバイスでの TRP の使用を有効にする場合は、この値を選択します。この設定は、このデバイスに関連付けられている共通デバイス設定の[トラステッドリレーポイントを使用 (Use Trusted Relay Point) ]設定よりも優先されます。</li> <li>• [デフォルト (Default) ]: この値を選択した場合、デバイスはこのデバイスが関連付けられている共通デバイス設定の[トラステッドリレーポイントを使用 (Use Trusted Relay Point) ]設定を使用します。</li> </ul> |
| 常にプライム回線を使用する (Always Use Prime Line)         | <p>ドロップダウンリストから、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [オフ (Off) ]: 電話がアイドル状態になっているときにいずれかの回線でコールを受信すると、電話のユーザは、コールを受信した回線からコールに応答します。</li> <li>• [オン (On) ]: 電話機がアイドル状態 (オフフック) になっているときにいずれかの回線でコールを受信すると、このコールにはプライマリ回線が選択されます。他の回線のコールは鳴り続け、電話機ユーザはそれらの他の回線を選択して、これらのコールに応答する必要があります。</li> <li>• [デフォルト (Default) ]: Cisco Unified Communications Manager は、Cisco CallManager サービスをサポートする [常にプライム回線を使用する (Always Use Prime Line) ] サービスパラメータの設定を使用します。</li> </ul>                       |

| フィールド  | 説明  |
|--|---|
| ボイスメッセージには常にプライム回線を使用する (Always Use Prime Line for Voice Message)                      | <p>ドロップダウン リストから、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [オフ (Off)] : 電話がアイドル状態の場合、電話のメッセージ ボタンを押すと、ボイス メッセージが設定されている回線からボイス メッセージ システムに自動的にダイヤルされます。Cisco Unified Communications Manager は常にボイス メッセージのある最初の回線を選択します。ボイスメッセージが設定されている回線が存在しない場合に電話のユーザーが [メッセージ (Messages)] ボタンを押すと、プライマリ回線が使用されます。</li> <li>• [オン (On)] : 電話がアイドル状態の場合に電話のメッセージ ボタンを押すと、電話のプライマリ回線がボイス メッセージを受信するアクティブな回線になります。</li> <li>• [デフォルト (Default)] : Cisco Unified Communications Manager は、Cisco CallManager サービスをサポートする [ボイスメッセージには常にプライム回線を使用する (Always Use Prime Line for Voice Message)] サービス パラメータの設定を使用します。</li> </ul> |
| [地理位置情報 (GeoLocation)]   | <p>ドロップダウン リストから地理位置情報を選択します。</p> <p>[未指定の地理位置情報 (Unspecified geolocation)] を選択すると、このデバイスを地理位置情報に関連付けないように指定できます。</p> <p>さらに、[システム (System)] &gt; [地理位置情報の設定 (Geolocation Configuration)] メニュー オプションで設定した地理位置情報も選択できます。</p>   |
| [プレゼンテーション インジケータを無視 (内線コールのみ) (Ignore Presentation Indicators (internal calls only))] | <p>コール単位でコール表示制限を設定する場合に、このチェックボックスをオンにします。このチェックボックスをオンにすると、Cisco Unified Communications Manager は内線コールに対して受信したすべての表示制限を無視します。</p> <p>この設定と、トランスレーション パターン レベルでの発信者回線 ID の表示および接続回線 ID の表示の設定を組み合わせ使用します。これらの設定を組み合わせ使用すれば、コールごとに発信側または接続先の回線表示情報を選択的に表示またはブロックするようにコール表示制限を設定できます。</p>  |
| [ハントグループにログイン (Logged into Hunt Group)]  | <p>ATA 191 をハント リストに追加したら、管理者はこのチェックボックスをオン (またはオフ) にすることによって、ユーザをログインまたはログアウトさせることができます。</p> <p>ユーザーは電話のソフトキーを使用して、電話をハントリストにログインまたはログアウトします。</p>  |

| フィールド                           | 説明   |
|---------------------------------|--|
| [リモートデバイス (Remote Device) ]     | <p>このチェックボックスをオンにすると、デバイスの登録時にバッファを割り当て、SCCP メッセージを電話機にバンドルします。</p> <p><b>ヒント</b> この機能はリソースを消費するため、シグナリングの遅延が発生している場合にのみ、このチェックボックスをオンにしてください。</p>   |
| [保護されたデバイス (Protected Device) ] | <p>電話機を保護されたデバイスとして指定するには、このチェックボックスをオンにします。この場合、電話機が2秒間トーンを再生してユーザーにコールが暗号化されていることを通知できます。また、発信側と着信側の両方の電話機が保護されたデバイスとして設定できます。このトーンは、コールが応答されたとき、発信側と着信側の両者に対して再生されます。このトーンは、発信側と着信側の両方の電話機が保護されていて、なおかつ暗号化メディア上でコールが行われたときでなければ再生されません。</p> <p>このチェックボックスをオンにすると、再生するセキュア通知トーンの複数の設定要件のうち1つのみが表示されます。セキュア通知トーン機能および設定要件の詳細については、『Cisco Unified Communications Manager セキュリティ ガイド』（<a href="http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html">http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html</a>）を参照してください。</p> <p>このチェックボックスがオンで、システムがコールは暗号化されていないと判断すると、電話は非セキュア通知トーンを再生して、コールが保護されていないことをユーザーに通知します。</p> |

### [番号表示トランスフォーメーション (Number Presentation Transformation) ]

表 21 : [この電話からのコールの発信者ID (Caller ID For Calls From This Phone) ]

| フィールド   | 説明  |
|---|---|
| [発信側トランスフォーメーションCSS (Calling Party Transformation CSS) ]                            | <p>この設定により、デバイスの発信者番号をローカライズできます。選択した発信側トランスフォーメーションCSSに、このデバイスに割り当てる発信側トランスフォーメーションパターンが含まれていることを確認してください。</p>   |
| [デバイスプールの発信側トランスフォーメーションCSSを使用 (Use Device Pool Calling Party Transformation CSS) ] | <p>このデバイスに割り当てられているデバイスプールに設定されている発信側トランスフォーメーションCSSを使用する場合は、このボックスをオンにします。このチェックボックスを選択しない場合、デバイスは[トランク設定 (Trunk Configuration) ]ウィンドウで設定した発信側変換CSSを使用します。</p> |

表 22: [リモート番号 (Remote Number) ]

| フィールド   | 説明  |
|---|---|
| [発信側トランスフォーメーションCSS (Calling Party Transformation CSS) ]                            | ドロップダウンリストから、このデバイスに受信したコールのリモート発信者番号に適用する、発信側トランスフォーメーションパターンを含むコーリングサーチスペース (CSS) を選択します。 |
| [デバイスプールの発信側トランスフォーメーションCSSを使用 (Use Device Pool Calling Party Transformation CSS) ] | リモート通話とリモート接続番号の変換に、このデバイスが属するデバイスプールで設定されている発信側トランスフォーメーションCSSを適用するには、このチェックボックスをオンにします。   |

表 23: [プロトコル固有情報 (Protocol Specific Information) ]

| フィールド                                 | 説明  |
|---------------------------------------|---|
| [パケットキャプチャモード (Packet Capture Mode) ] | <p>この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケットキャプチャを実行すると、CPUの使用率が上昇して、コール処理が妨げられる可能性があります。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。</p> <ul style="list-style-type: none"> <li>• [なし (None) ] : このオプションは、パケットキャプチャが発生しないことを示します (デフォルト設定)。この設定は、パケットキャプチャの完了後に行います。</li> <li>• [バッチ処理モード (Batch Processing Mode) ] : Cisco Unified CM が、復号されたメッセージや暗号化されていないメッセージをファイルに書き込み、システムが各ファイルを暗号化します。システムでは、毎日新しいファイルが新しい暗号キーを使用して作成されます。Cisco Unified CM はファイルを7日間保存し、さらにファイルを暗号化するキーを安全な場所に保存します。Cisco Unified CM は、PktCap 仮想ディレクトリにファイルを保存します。1つのファイルの中に、タイムスタンプ、送信元IPアドレス、送信元IPポート、宛先IPアドレス、パケットのプロトコル、メッセージの長さ、およびメッセージが保持されます。TACのデバッグツールでは、HTTPS、管理者のユーザ名とパスワード、および指定された日付を使用して、キャプチャされたパケットを保持している暗号化済みファイルを1つだけ要求します。同様にこのツールでは、暗号化ファイルを復号化するためのキー情報を要求します。</li> </ul> |

| フィールド   | 説明  |
|---|---|
| [パケットキャプチャ時間 (Packet Capture Duration) ]          | <p>この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケットキャプチャを実行すると、CPUの使用率が上昇して、コール処理が妨げられる可能性があります。</p> <p>このフィールドには、1つのパケットキャプチャセッションに割り当てる時間の上限（分単位）を指定します。デフォルト設定は0で、範囲は0～300分です。</p> <p>パケットキャプチャを開始するには、フィールドに0以外の値を入力します。パケットキャプチャが完了すると、値0が表示されます。</p>  |
| [BLFプレゼンスグループ (BLF Presence Group) ]              | <p>ドロップダウンリストから、エンドユーザーの話中ランプフィールド (BLF) プレゼンスグループを選択します。選択したグループは、エンドユーザーがモニター可能な接続先を指定します。</p> <p>BLF プレゼンスグループのデフォルト値は [標準のプレゼンスグループ (Standard Presence group) ] であり、インストール時に設定されます。Cisco Unified CM Administration で設定されている BLF プレゼンスグループは、ドロップダウンリストにも表示されます。</p>  |
| [SIPダイヤルルール (SIP Dial Rules) ]                    | <p>必要に応じて、適切な SIP ダイヤルルールを選択します。SIP ダイヤルルールは、Cisco Unified IP Phone 7940 および 7960 のローカルダイヤルプランを提供するため、ユーザーは、コールが処理される前に、キーを押したり、タイマーを待機したりする必要はありません。</p> <p>SIP を実行している IP 電話にダイヤルルールを適用しない場合は、[SIP ダイヤルルール (SIP Dial Rules) ] フィールドを [&lt;なし&gt; (&lt;None&gt;)] に設定したままにします。これは、コールが処理される前に、ユーザーがダイヤルソフトキーを使用するか、タイマーが切れるまで待つ必要があることを示します。</p> |
| [MTP優先発信コーデック (MTP Preferred Originating Codec) ] | <p>メディアターミネーションポイントが SIP のコールに必要な場合は、ドロップダウンリストから使用するコーデックを選択します。</p>   |
| [デバイスのセキュリティプロファイル (Device Security Profile) ]    | <p>デバイスに適用するセキュリティプロファイルを選択します。</p> <p>Unified Communications Manager Administration で設定するすべてのデバイスに、セキュリティプロファイルを適用する必要があります。</p>   |

| フィールド  | 説明  |
|--|---|
| [再ルーティング用<br>コーリングサーチス<br>ペース (Rerouting<br>Calling Search<br>Space) ] | <p>ドロップダウンリストから、再ルーティングに使用するコーリングサーチスペースを選択します。</p> <p>リファラーの再ルーティングコーリングサーチスペースを使用して、参照先へのルートが検索されます。再ルーティングコーリングサーチスペースが原因で参照が失敗すると、Refer Primitive は「405 Method Not Allowed」メッセージによって要求を拒否します。</p> <p>リダイレクト (3xx) プリミティブおよび転送機能も再ルーティングコーリングサーチスペースを使用して、リダイレクト先または転送先を検索します。</p>   |
| [SUBSCRIBEコーリン<br>グサーチスペース<br>(AAR Calling Search<br>Space) ]          | <p>プレゼンス機能によってサポートされる SUBSCRIBE コーリングサーチスペースは、エンドユーザから受け取ったプレゼンス要求を Unified Communications Manager がルーティングする方法を決定します。この設定では、エンドユーザーのプレゼンス (SUBSCRIBE) 要求のコール処理サーチスペースと別にコーリングサーチスペースを適用できません。</p> <p>ドロップダウンリストから、エンドユーザーのプレゼンス要求に使用する SUBSCRIBE コーリングサーチスペースを選択します。Cisco Unified Communications Manager Administration で設定するすべてのコーリングサーチスペースが、[SUBSCRIBE コーリングサーチスペース (SUBSCRIBE Calling Search Space) ] ドロップダウンリストに表示されます。</p> <p>ドロップダウンリストから、エンドユーザーに別のコーリングサーチスペースを選択しない場合、SUBSCRIBE コーリングサーチスペースのデフォルトは [なし (None) ] に設定されます。</p> <p>この目的専用の SUBSCRIBE コーリングサーチスペースを設定するには、他のコーリングサーチスペースと同様に新しいコーリングサーチスペースを設定します。</p> |
| [SIPプロファイル<br>(SIP Profile) ]  | <p>デフォルトの SIP プロファイルまたは作成済みの特定のプロファイルを選択します。SIP プロファイルでは、登録タイマーおよびキープアライブタイマー、メディアポート、Do Not Disturb (サイレント) 制御など、電話機の特定の SIP 情報を提供します。</p>   |



| フィールド   | 説明   |
|---|--|
| [ダイジェストユーザー (Digest User) ]                               | <p>ダイジェスト認証 (SIP セキュリティ) で使用するこの設定の電話機に関連付けるエンドユーザーを選択します。</p> <p>選択するユーザーのダイジェスト クレデンシャルが [エンドユーザーの設定 (End User Configuration) ] ウィンドウで設定されていることを確認してください。</p> <p>電話設定を保存し、設定の更新内容を電話に適用すると、ユーザーのダイジェストクレデンシャルが電話の設定ファイルに追加されます。</p> <p>ダイジェスト認証の詳細については、『Cisco Unified Communications Manager セキュリティ ガイド』 (<a href="http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html">http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html</a>) を参照してください。</p> |
| [メディアターミネーションポイントが必須 (Media Termination Point Required) ] | <p>このフィールドを使用して、ATA 191 がサポートしない機能 (保留や転送など) を実装するために、メディアターミネーションポイントを使用するかどうかを指示します。</p> <p>MTPを使用して機能を実装する場合は、[メディアターミネーションポイントが必須 (Media Termination Point Required) ] チェックボックスをオンにします。MTP を使用して機能を実装しない場合は、[メディアターミネーションポイントが必須 (Media Termination Point Required) ] チェックボックスをオフにします。</p> <p>このチェックボックスは、H.245機能セットをサポートしていない ATA191クライアントとATA191デバイスに対してのみ使用するか、単一のソースからメディアフローを終了する場合に使用します。</p> <p>このチェックボックスをオンにして、MTPを必須とし、このデバイスをビデオコールのエンドポイントにすると、コールはオーディオのみになります。</p>   |
| [不在ポート (Unattended Port) ]                                | <p>このデバイスの不在ポートを指示する場合に、このチェックボックスをオンにします。</p>   |
| [DTMF受信が必要 (Require DTMF Reception) ]                     | <p>SIP と SCCP を実行しているデバイスの場合に、この電話の DTMF 受信を必須にするには、このチェックボックスをオンにします。</p> <p>(注) Cisco Unified Mobility 機能の設定で、SIP トランク (クラスタ間トランク (ICT) またはゲートウェイ) 経由で IP 電話のリモート接続先としてクラスタ間 DN を使用する場合、エンタープライズ機能アクセス ミッドコール機能に不可欠な DTMF 番号をアウト オブ バンドで受信できるように、このチェックボックスをオンにします。</p>  |

表 24: 認証局プロキシ機能 (CAPF) 情報 (Certification Authority Proxy Function (CAPF) Information)

| フィールド                               | 説明   |
|-------------------------------------|--|
| [証明書の変更<br>(Certificate Operation)] | <p>ドロップダウン リストから、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [保留中の操作なし (No Pending Operation)] : 証明書の操作が行われない場合に表示されます (デフォルトの設定)。</li> <li>• [インストール/更新 (Install/Upgrade)] : 電話機に新しい証明書をインストールするか、既存のローカルで有効な証明書をアップグレードします。</li> <li>• [削除 (Delete)] : 電話機に存在するローカルで有効な証明書を削除します。</li> <li>• [トラブルシューティング (Troubleshoot)] : ローカルで有効な証明書 (LSC) または製造元でインストールされる証明書 (MIC) を取得し、CAPF トレース ファイルで証明書クレデンシャルを表示できます。電話機に両方の証明書タイプが存在する場合、Cisco Unified CM は、証明書のタイプごとに1つずつ、2つのトレースファイルを作成します。</li> </ul> <p>[トラブルシューティング (Troubleshooting)] オプションを選択して、電話に LSC または MIC が存在することを確認できます。</p> <p>CAPF 操作の詳細については、『Cisco Unified Communications Manager セキュリティガイド』 (<a href="http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html">http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html</a>) を参照してください。</p> |

| フィールド                                | 説明 |
|--------------------------------------|----|
| [認証モード<br>(Authentication<br>Mode) ] |    |

| フィールド | 説明  |
|-------|---|
|       | <p>このフィールドでは、電話機が CAPF 証明書の操作時に使用する認証方法を選択できます。</p> <p>ドロップダウン リストから、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [認証文字列 (By Authentication String) ] : ユーザーが電話に CAPF 認証文字列を入力した場合にのみ、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。</li> <li>• [Null スtring (By Null String) ] : ユーザーの介入なしで、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。<br/><br/>このオプションではセキュリティが確保されません。したがって、セキュアな閉じた環境の場合にだけこのオプションを選択することを強く推奨します。</li> <li>• [既存の証明書 (LSCを優先) (By Existing Certificate (Precedence to LSC)) ] : 電話機に製造元でインストールされる証明書 (MIC) またはローカルで有効な証明書 (LSC) が存在する場合に、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に LSC が存在する場合、電話機に MIC が存在するかどうかに関係なく、LSC によって認証が行われます。電話機に MIC と LSC が存在する場合、LSC によって認証が行われます。電話機に LSC が存在しないが、MIC が存在する場合、MIC によって認証が行われます。<br/><br/>このオプションを選択する前に、電話機に証明書が存在することを確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。<br/><br/>MIC と LSC が同時に電話機に存在できる場合でも、電話機が CAPF への認証に使用する証明書は常に 1 つだけです。優先されるプライマリ証明書が何らかの理由で破損した場合、または別の証明書を使用して認証を受ける場合は、認証モードを更新する必要があります。</li> <li>• [既存の証明書 (MICを優先) (By Existing Certificate (Precedence to MIC)) ] : 電話機に LSC または MIC が存在する場合に、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に MIC が存在する場合、電話機に LSC が存在するかどうかに関係なく、MIC によって認証が行われます。電話機に LSC が存在するが、MIC が存在しない場合、LSC によって認証が行われます。<br/><br/>このオプションを選択する前に、電話機に証明書が存在すること</li> </ul> |

| フィールド  | 説明   |
|--|--|
|  | <p>を確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。</p> <p>(注) [電話セキュリティプロファイル (Phone Security Profile) ] ウィンドウで設定される CAPF 設定は、[電話の設定 (Phone Configuration) ]ウィンドウで設定される CAPF パラメータと連携します。</p>   |
| <p>[認証文字列 (Authentication String) ]</p>              | <p>[認証モード (Authentication Mode) ] ドロップダウンリストの [認証文字列 (By Authentication String) ] オプションを選択した場合、このフィールドが適用されます。手動で文字列を入力するか、[文字列の生成 (Generate String) ] ボタンをクリックして、文字列を生成します。4 桁から 10 桁の文字列になるようにしてください。</p> <p>ローカルで有効な証明書をインストール、アップグレード、削除、トラブルシューティングするには、電話機ユーザーまたは管理者が電話機に認証文字列を入力する必要があります。</p>  |
| <p>[キー サイズ (ビット) (Key Size (Bits)) ]</p>             | <p>CAPF で使用されるこの設定では、ドロップダウン リストから証明書のキー サイズを選択します。デフォルト設定は 1024 です。その他のオプションには 512 と 2048 があります。</p> <p>デフォルトの設定より大きいキー サイズを選択すると、電話機でキーの生成に必要なエントロピーを生成するのに時間がかかります。キーの生成を低い優先順位で設定すると、操作の実行中に、電話機が機能します。電話機のモデルによっては、キーの生成が完了するまでに、30 分以上かかることがあります。</p> <p>(注) [電話セキュリティプロファイル (Phone Security Profile) ] ウィンドウで設定される CAPF 設定は、[電話の設定 (Phone Configuration) ]ウィンドウで設定される CAPF パラメータと連携します。</p> |
| <p>[操作の完了期限 (Operation Completes by) ]</p>           | <p>このフィールドは、[インストール/アップグレード (Install/Upgrade) ]、[削除 (Delete) ]、[トラブルシューティング (Troubleshoot) ] の証明書の操作オプションをサポートし、操作の完了期限を指定します。</p> <p>表示される値は、パブリッシャ データベース サーバーに適用されます。</p>   |
| <p>[証明書の操作ステータス (Certificate Operation Status) ]</p> | <p>このフィールドには、証明書の操作の進捗状況が表示されます。たとえば、&lt;操作タイプ&gt;保留中、失敗、成功などです。ここで、操作タイプは [インストール/アップグレード (Install/Upgrade) ]、[削除 (Delete) ]、[トラブルシューティング (Troubleshoot) ] 証明書の操作オプションのいずれかになります。このフィールドに表示される情報は変更できません。</p>   |

表 25: [セキュアシェルユーザー (Secure Shell User) ]

| フィールド                                   | 説明  |
|---|---|
| [セキュアシェルユーザー (Secure Shell User) ]      | <p>セキュア シェルユーザーのユーザー ID を入力します。最大 50 文字の英数字または特殊文字を入力できます。無効な文字は、"、%、&amp;、&lt;、&gt;、\ です。このフィールドは、設定している電話デバイスが SSH アクセスをサポートしている場合に表示されます。</p> <p>Cisco Technical Assistance Center (TAC) では、トラブルシューティングやデバッグを行うときにセキュアシェルを使用します。TAC にお問い合わせください。</p> <p>Cisco Unified CM が SSH クレデンシャルを平文で電話機に送信しないようにするために、暗号化された電話の設定ファイルを設定する方法については、このリリースの『Cisco Unified Communications Manager セキュリティガイド』 (<a href="http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html">http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html</a>) を参照してください。</p> |
| [セキュアシェルパスワード (Secure Shell Password) ] | <p>セキュア シェルユーザーのパスワードを入力します。最大 127 文字の英数字や特殊文字を入力できます。無効な文字は、"、%、&amp;、&lt;、&gt;、\ です。TAC にお問い合わせください。</p> <p>Cisco Unified CM が SSH クレデンシャルを平文で電話機に送信しないようにするために、暗号化された電話の設定ファイルを設定する方法については、このリリースの『Cisco Unified Communications Manager セキュリティガイド』 (<a href="http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html">http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html</a>) を参照してください。</p>  |

表 26: 製品固有の設定

| フィールド                     | 説明  |
|---------------------------|---|
| デバイス製造元が定義するモデル固有の設定フィールド | <p>製品固有の設定項目のフィールドの説明とヘルプを表示するには、[製品固有の設定 (Product Specific Configuration) ] エリアで [?] 「」 情報アイコンをクリックし、ポップアップダイアログボックスでヘルプを表示します。</p> <p>詳細については、ATA 191 のドキュメントを参照してください。</p> |

## 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。