IX システム用の Cisco Unified Communications Manager の設定

2015 年 4 月

Cisco Systems, Inc.
www.cisco.com

シスコは世界各国 200 箇所にオフィスを開設しています。
所在地、電話番号、FAX 番号 は以下のシスコ Web サイトを
ご覧ください。www.cisco.com/go/offices

Text Part Number:

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

IX システム用の Cisco Unified Communications Manager の設定

このユーザ ガイドの内容

改訂日：2015 年 6 月 17 日

目次

ここでは、次の項について説明します。

このマニュアルの使い方

このガイドには、Cisco Unified Communications Manager（Unified CM）の管理インターフェイスを使用して Cisco TelePresence IX5000 および IX5200 を設定する際に役立つ情報が記載されています。

はじめる前に

このガイドのタスクを開始する前に、以下の項目を確認してください。

Web ブラウザのサポート

Cisco Unified Communications Manager Administration は以下のオペレーティング システムのブラウザをサポートします。

- Microsoft Windows 7：
  - Microsoft Internet Explorer（IE）8、IE 9
  - Mozilla Firefox 4.x、Firefox 10.x
- Apple OS X 以降：
  - Apple Safari 5.x
  - Firefox 4.x、10.x

DHCP と静的 IP 接続

IX システムでは、Dynamic Host Configuration Protocol（DHCP）サーバを使用して接続を確立するか、または静的 IP アドレスを設定できます。DHCP はネットワーク管理者によって設定されます。静的 IP アドレスを設定するには、『*IX5000 and IX5200 First-Time Setup*』マニュアルの「Configuring a IX5000 or IX5200 System With a Static Network Address」の項に記載されている手順に従ってください。

Cisco TelePresence ファイル イメージのダウンロードと設定

cisco.com から IX システム イメージ ファイルをダウンロードし、Unified CM を使用してシステムに適用します。このタスクを完了するための手順については、「COP ファイルの追加と設定」セクション（1 ページ）を参照してください。

システム MAC アドレスの検索

Unified CM でシステムを設定するには、コーデックの MAC アドレスが必要です。コーデックには 2 つの MAC アドレスがあります。アップリンクと EX1 イーサネット接続に最も近いアドレスを使用してください。図 1 に例を示します。

ヒント このアドレスは、システムの起動時に表示されるブルー スクリーンにも表示されます。

図 1　　コーデック上の MAC アドレスの位置

ソフトウェアの互換性

CTS のソフトウェアおよびファームウェアの互換性については、次の URL にある『Cisco TelePresence IX?system Software Compatibility』を参照してください。

http://www.cisco.com/c/en/us/td/docs/telepresence/ix_sw/8_x/compatibility/ix__compat_8_0.html

Cisco TelePresence の帯域幅要件

各種ビデオ レベルの帯域幅要件については、『*Administration Guide for Cisco TelePresence Software Release IX 8*』の「1080p Main Video」の一覧を参照してください。

デバイスとクラスタのセキュリティ モード

[デバイス セキュリティ モード（Device Security Mode）] が [暗号化済（Encrypted）] に設定され、[クラスタ セキュリティ モード（Cluster Security Mode）] が **1**（混合モード）に設定されている場合に限り、コール中、画面に [暗号化済みメディア（Media is Encrypted）]（施錠）アイコンが表示されます。システムを設定する際は、次の設定を確認してください。

- [SIP 電話のセキュリティ プロファイル情報（SIP Phone Security Profile Information）] フィールドで、[デバイス セキュリティ モード（Device Security Mode）] が [暗号化済（Encrypted）] に設定されている。設定情報については、「IX システムの新しい電話セキュリティ プロファイルの追加」セクション（13 ページ）を参照してください。
- [Cisco Unified CM の管理（Cisco Unified CM Administration）] > [システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）] の [CTL クライアントの設定（Configuration Settings for CTL Client）] で、[クラスタ セキュリティ モード（Cluster Security Mode）] フィールドが **1**（混合モード）に設定されている。クラスタ セキュリティ モードのアクティブ化および確認については、『*Securing Cisco TelePresence Products*』ガイドの「Activating the CAPF Server」の項を参照してください。

Unified CM でサポートされる文字と数字

Cisco TelePresence システムの設定や保守で使用する文字と数字の Unified CM でのサポートについては、テーブル 1 の情報を参照してください。Unified CM の一般的なサポート マニュアルについては、使用しているリリースに応じた Unified CM ドキュメント ロードマップを Cisco.com で参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html

（注） Unified CM では、システム パスワードに「$」（通貨記号）を使用できなくなりました。

テーブル 1　　IX システムの設定用に Unified CM でサポートされる文字と数字

文字または数字	説明	使用場所
• **0** ～ **9** の数字 • *（アスタリスク） • **#**（番号記号またはハッシュ） • **+**（プラス記号、エスケープ記号）	ユーザがスピード ダイヤル ボタンを押したときに、システムによりダイヤルされる番号。 **（注）** スピード ダイヤル機能では一時停止や待機を設定できません。	[スピード ダイヤルと短縮ダイヤルの設定（Speed Dial and Abbreviated Dial Configuration）] ウィンドウ、[番号（Number）] フィールド 参照先：第 1 章「IX システム用の Cisco Unified Communications Manager の設定」

ドキュメントの構成

Cisco Unified CM と Cisco TelePresence System アプリケーションの併用については、以下の章に記載されています。

- 第 1 章「IX システム用の Cisco Unified Communications Manager の設定」
- 第 2 章「Cisco TelePresence の機能の設定」
- 第 3 章「IX システムの設定の確認とトラブルシューティング」

IX システム用の Cisco Unified Communications Manager の設定

改訂日：2015 年 6 月 17 日

目次

この章では、Cisco Unified Communications Manager（Unified CM）の Web インターフェイスを使用して、cisco.com の Web サイトから IX ソフトウェアをダウンロードし、新しいデバイスを設定する方法について説明します。この章は以下の項から構成されています。

COP ファイルの追加と設定

IX システムを使用するには、その前に、Cisco Unified Communications Manager（Unified CM）に最新の Cisco Options Package（COP）ファイルをインストールし、IX システムにアップロードする必要があります。

COP ファイルは、IX システムが実行に使用するソフトウェア イメージ ファイルです。COP ファイルには新しいソフトウェア機能がパッケージ化されています。既存のファイルをアップグレードすると、IX システムでそれらの機能が有効になります。

新しい COP ファイルをインストールするには、次の手順を実行します。

IX ソフトウェアのダウンロード

（注）　すでにソフトウェアをダウンロードして Unified CM に追加済みの場合は、この項を省略して「Unified CM への IX システムの追加」セクション（1-16 ページ）に進み、Unified CM に新しいデバイスを追加します。

ステップ 1　www.cisco.com に移動します。

ステップ 2　[ログイン（Log In）] ボタンをクリックし、ユーザ名とパスワードを入力します。

ステップ 3　次の URL に移動します。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/ix5000-series/tsd-products-support-series-home.html

（注）　使用しているソフトウェアが見つからない場合は、次の URL の TX ソフトウェア領域に移動する必要があります。

https://software.cisco.com/download/type.html?mdfid=284307107&flowid=31903

ステップ 4　[TelePresence ソフトウェア（TelePresence Software）] ハイパーリンクをクリックします。

ステップ 5　ダウンロードするソフトウェア イメージ（通常は最新バージョン）の名前をクリックし、[カートに追加（Add to Cart）] をクリックします。

ステップ 6　カートをクリックし、[ダウンロード（Download）] をクリックします。

ステップ 7　[使用許諾契約書に同意（Accept License Agreement）] をクリックし、プロンプトに従ってファイルをダウンロードします。

ステップ 8　Unified CM からアクセス可能なセキュア ファイル転送プロトコル（SFTP）サーバにファイルをコピーします。

Unified CM への IX ソフトウェアの追加

Unified CM に IX ソフトウェアをインストールするには、次の手順を実行します。

ステップ 1　Unified CM でサポートされている Web ブラウザを開きます。

サポートされているブラウザのリストについては、「Web ブラウザのサポート」セクション（vi ページ）を参照してください。

ステップ 2　Web ブラウザのアドレス バーに次の URL を入力します。

https://*UCM-server-name*

引数の説明

UCM-server-name は

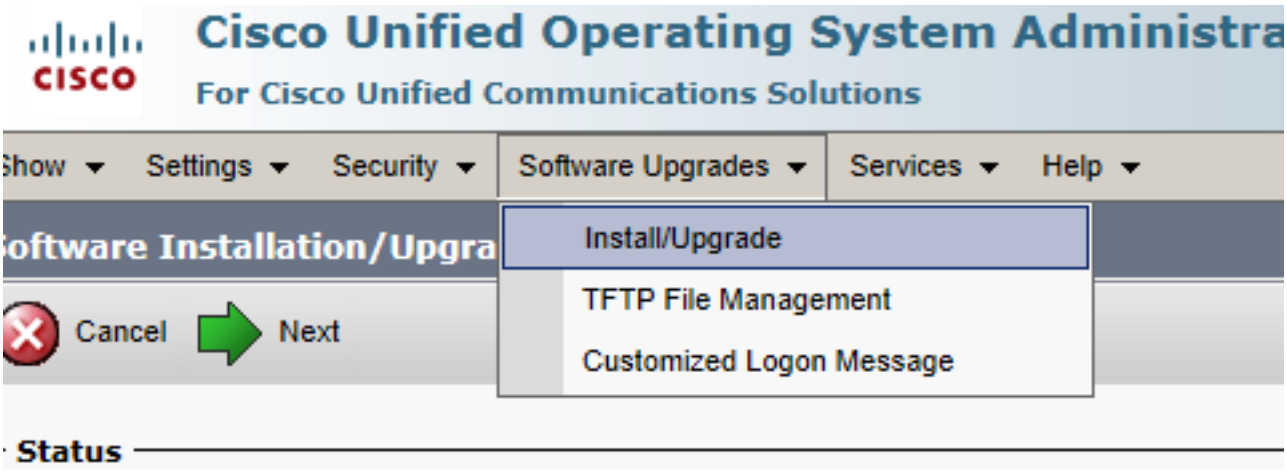
Unified CM の IP アドレスまたは DNS 名です。

ステップ 3　GUI の右上にある [ナビゲーション（Navigation）] ドロップダウン リストから、[Cisco Unified OS の管理（Cisco Unified OS Administration）] を選択します。[移動（Go）] をクリックして [Cisco Unified オペレーティングシステムの管理（Cisco Unified Operating System Administration）] 画面に進みます。

（注）　入力を求められたら、ユーザ名とパスワードを使ってログインします。

ステップ 4　[ソフトウェア アップグレード (Software Upgrades)] > [インストール/アップグレード (Install/Upgrade)] の順に選択します。

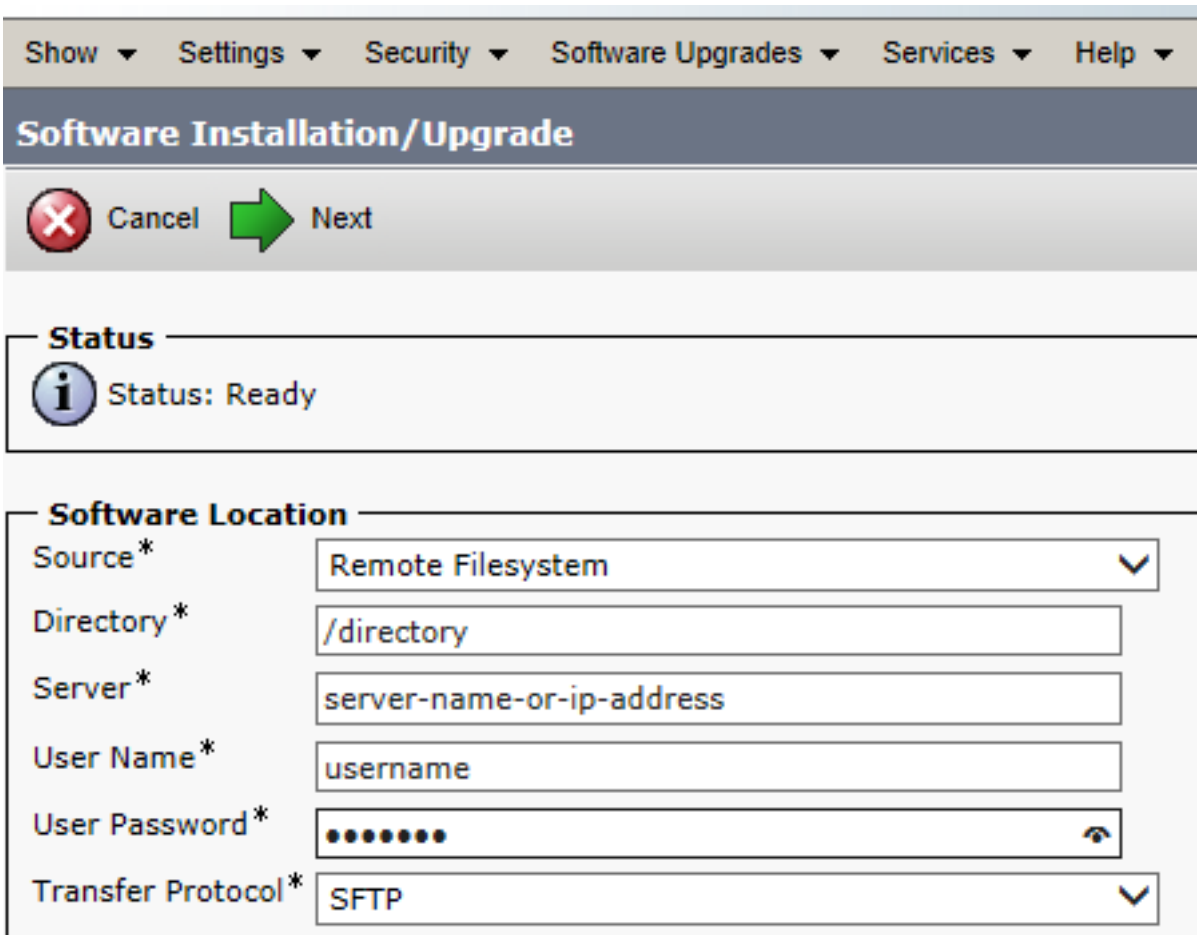
図 1-1　[Cisco Unified オペレーティングシステムの管理（Cisco Unified Operating System Administration）] 画面



ステップ 5　[ソフトウェアの場所（Software Location）] 領域で、各フィールドに次の情報を指定します。

- [ソース（Source）] ドロップダウン リストで、[リモート ファイルシステム（Remote Filesystem）] を選択します。
- [ディレクトリ（Directory）] フィールドに、SFTP サーバ上のファイルの場所を入力します。
- [サーバ（Server）] フィールドにサーバ名または IP アドレスを入力します。
- [ユーザ名（User Name）] フィールドと [ユーザ パスワード（User Password）] フィールドに、SFTP サーバへのアクセスに使用するユーザ名とパスワードを入力します。
- [転送プロトコル（Transfer Protocol）] ドロップダウン リストから [SFTP] を選択します。

図 1-2　　SFTP サーバとファイルの場所の指定

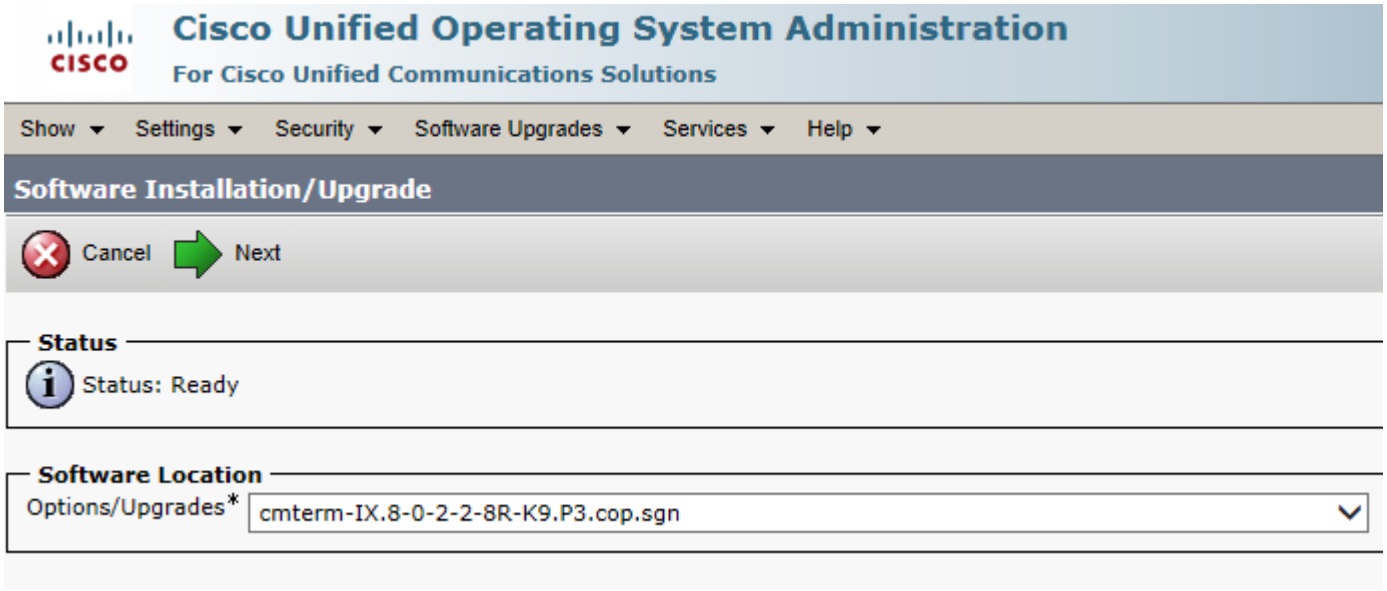


ステップ 6　[次へ（Next）] をクリックします。

Unified CM が SFTP サーバにアクセスします。[ソフトウェアの場所（Software Location）] 領域に、指定したディレクトリで Unified CM が検出したファイルの一覧が示されます。

ステップ 7　[オプション/アップグレード（Options/Upgrades）] ドロップダウン リスト内の使用可能なファイル名から、インストールするファイルを選択します。

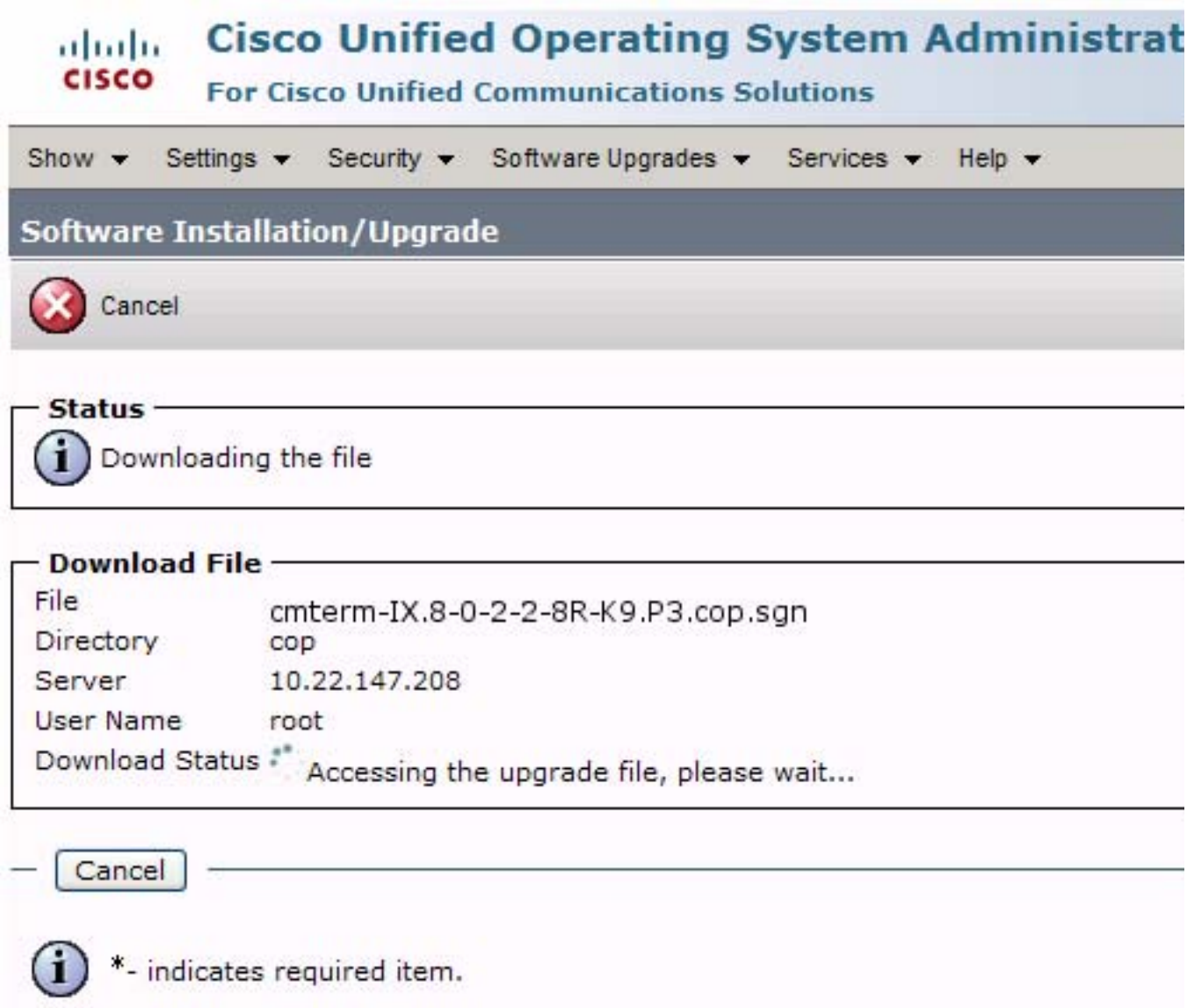
図 1-3　COP ファイルの指定



ステップ 8　[次へ（Next）] をクリックします。

Unified CM GUI に、インストールされているファイルが表示されます。

図 1-4　　COP ファイルのインストール



ステップ 9　インストールが完了したら、次の手順を実行してファイルの有効性を確認します。

a. [ファイルのチェックサムの詳細（File Checksum Details）] 領域の情報をメモしておきます。この値は図 1-5 のとおりです。

b. SFTP サーバにログインし、次のコマンドを入力します。

c. **md5sum** *filename*.cop.sgn

引数の説明

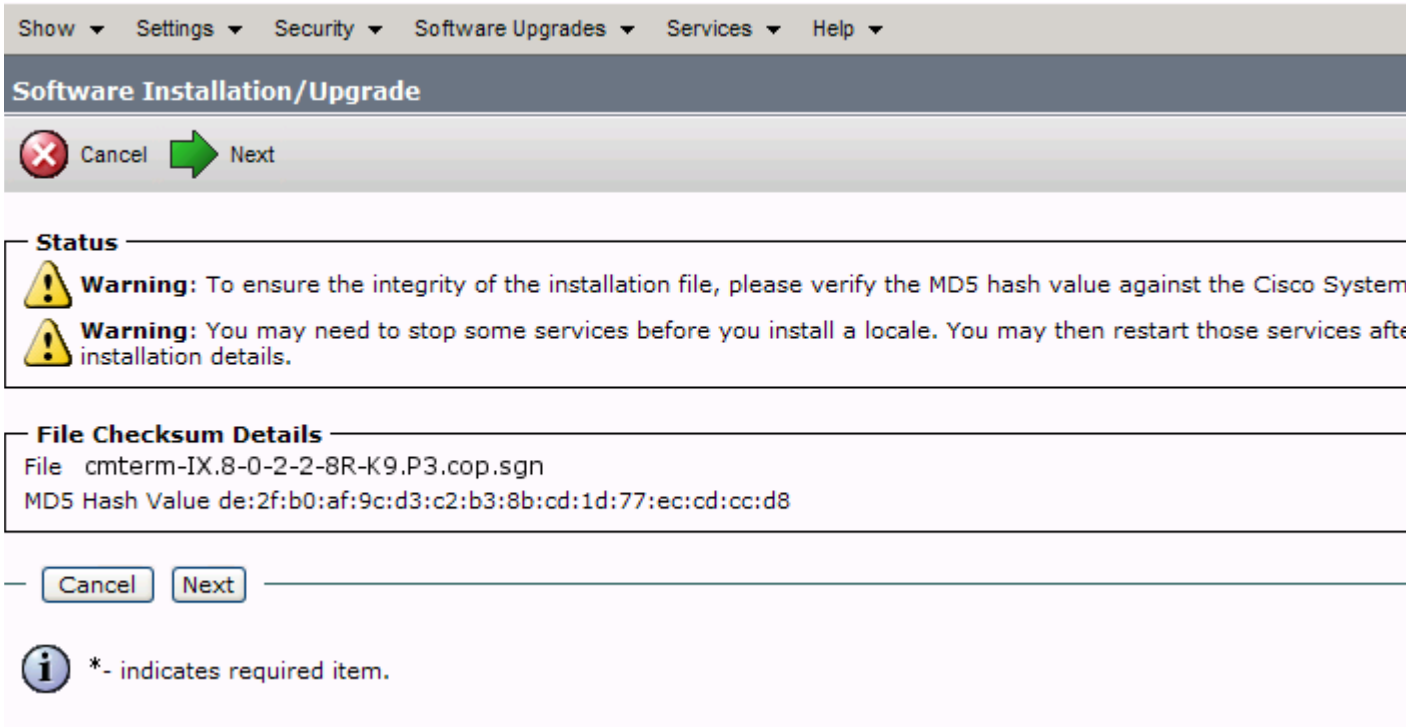
filename は SFTP サーバ上の COP ファイルのファイル名です。

d. md5sum コマンドの結果として表示されるチェックサム値をメモしておきます。

e. この領域に表示される [MD5 ハッシュ値（MD5 Hash Value）] とサーバ上の COP ファイルに記入されている MD5 チェックサム値を比較し、これらが一致しているかチェックして、ファイルが破損していないことを確認します。

f. 値が一致する場合は、次の手順に進みます。値が一致しない場合は、ファイルのインストールを再試行します。

図 1-5　[ファイルのチェックサムの詳細（File Checksum Details）File Checksum Details] 領域

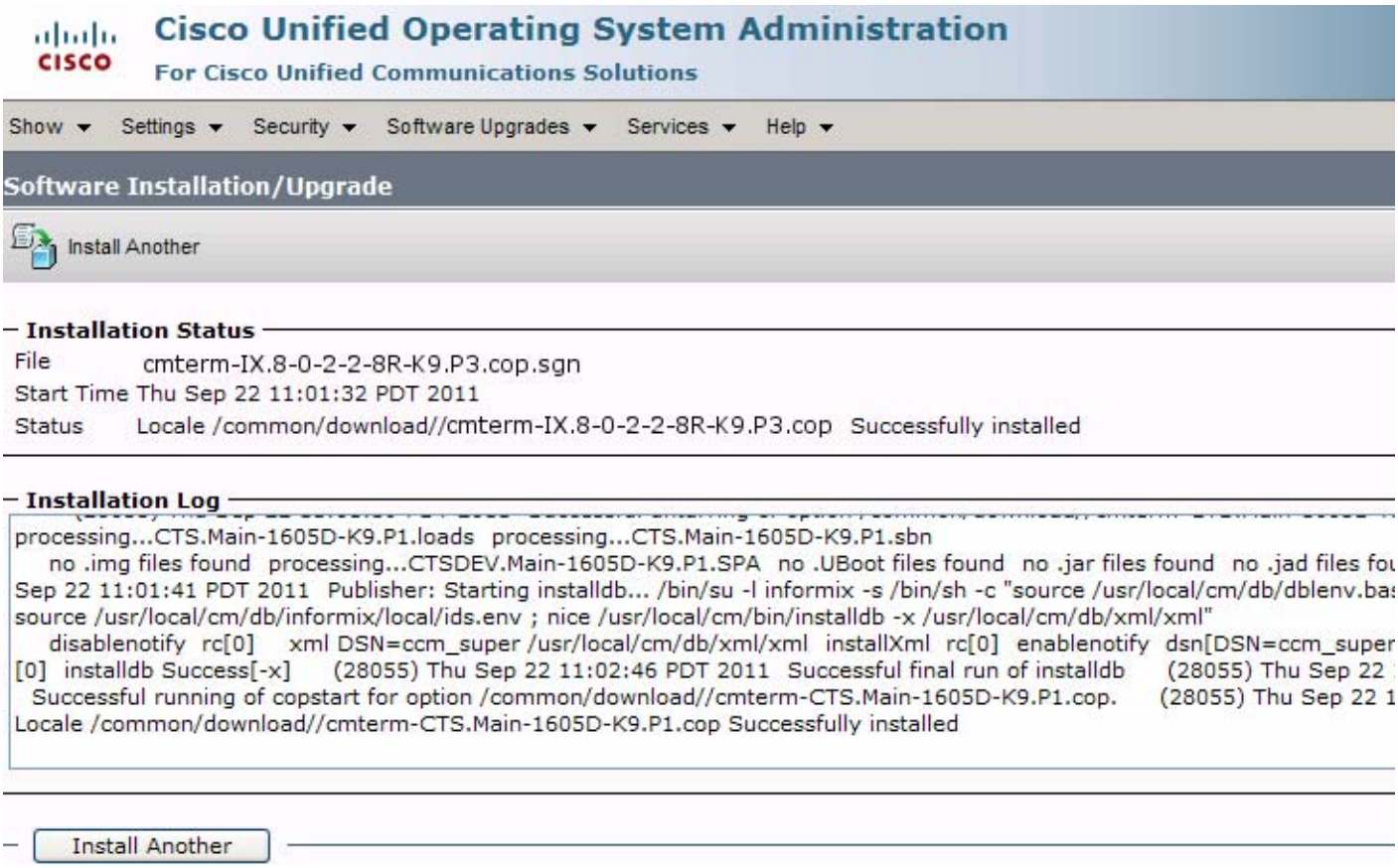


ステップ 10　[次へ（Next）] をクリックしてインストールを開始します。

インストール ログにインストールの進行状況が表示されます。

システム ファイルが抽出されると、インターフェイスの [インストール ステータス（Installation Status）] 領域に [完了（Complete）] ステータスが表示されます。

図 1-6　[インストール ステータス（Installation Status）] 領域



ステップ 11　GUI の右上にある [ナビゲーション（Navigation）] ドロップダウン リストから、[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] を選択し、[移動（Go）] をクリックします。

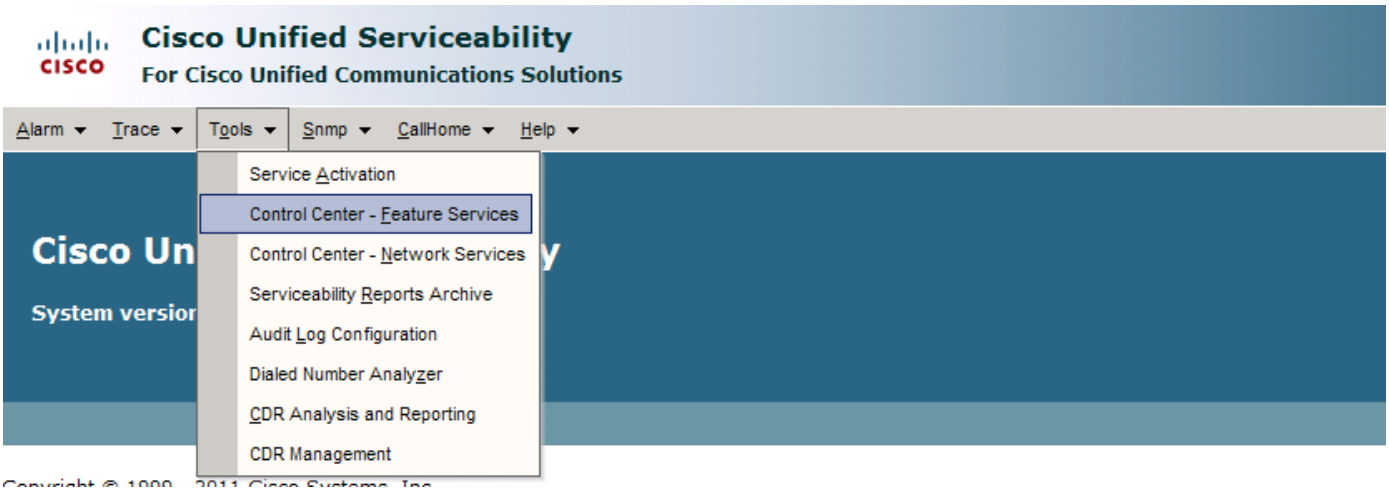
[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] ウィンドウが表示されます。

（注）　入力を求められたら、ユーザ ID とパスワードを入力します。

ステップ 12　次の手順を実行して、TFTP サーバを再起動します。

a.　[Tools（ツール）] > [コントロール センターの機能サービス（Control Center - Feature Services）] の順に選択します。

図 1-7　[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] ウィンドウ

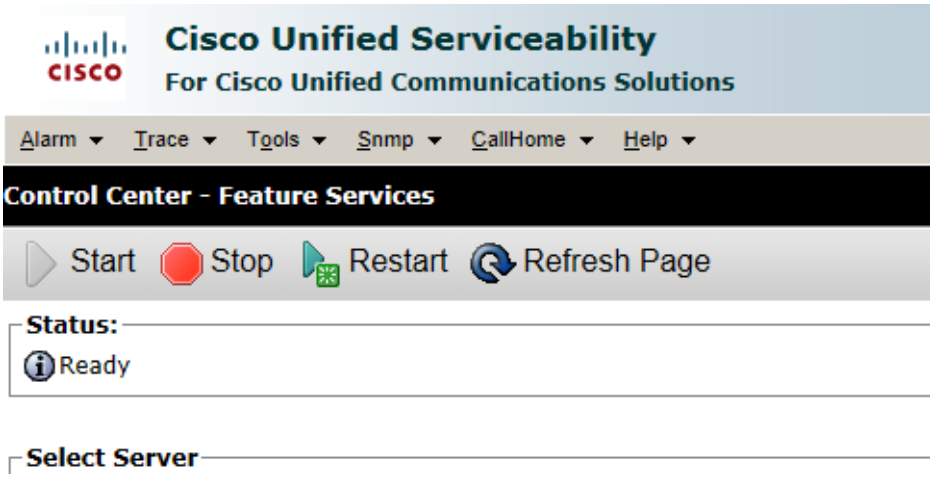


b. 表示されるドロップダウン リストから該当する TFTP サーバを選択し、[移動（Go）] をクリックします。

c. [CM サービス（CM Services）] 領域で、[Cisco Tftp] オプション ボタンをクリックします。

d. [リスタート（Restart）] ボタン（ページの下部にある [リスタート（Restart）] ボタンか、図 1-8 のページ上部のボタン）をクリックします。

図 1-8　[機能サービス（Feature Services）] ページの [リスタート（Restart）] ボタン



ステップ 13　「Unified CM への IX システムの追加」セクション（1-16 ページ）の手順を実行して、Unified CM に IX システムを追加します。

システム用の IX ソフトウェア イメージ ファイルの指定

Unified CM サーバに IX イメージをロードしたら、デフォルト イメージとして使用するファイルを指定します。Unified CM に登録されているすべての IX5000 および IX5200 システムにイメージを指定できます。または、次の手順を実行して、単一のシステムに 1 つのイメージを指定できます。

ステップ 1　GUI の右上にある [ナビゲーション（Navigation）] ドロップダウン リストから、[Cisco Unified CM の管理（Cisco Unified CM Administration）] を選択し、[移動（Go）] をクリックします。

[Cisco Unified CM の管理（Cisco Unified CM Administration）] ウィンドウが表示されます。

ステップ 2　指定したタイプのすべてのデバイスにこのソフトウェアを適用するには、次の手順を実行します。

（注）　このソフトウェアを（デフォルトとして適用するのではなく）デバイスごとにロードするには、ステップ 3 に進みます。

a. [デバイス（Device）] > [デバイスの設定（Device Settings）] > [デバイスのデフォルト（Device Defaults）] の順に選択します。

b. Cisco TelePresence IX5000 の デバイス タイプを探します。

c. 次の手順を実行し、デフォルトのイメージ ファイルとして、IX ソフトウェア イメージ ファイルをすべての IX5000 および IX5200 システムに適用します。

1. [ロード情報（Load Information）] フィールドにファイルの名前を入力します。ファイル名の前の cmterm- と末尾の .cop.sgn ファイルタイプは入力しません。

   たとえば、cmterm-IX.8-0-2-2-8R-K9.P3.cop.sgn という名前のファイルの場合は、**IX.8-0-2-2-8R-K9.P3** と入力します。

2. [Save（保存）] をクリックして変更内容を保存します。

d. [デバイス（Device）] > [電話（Phone）] の順に移動します。

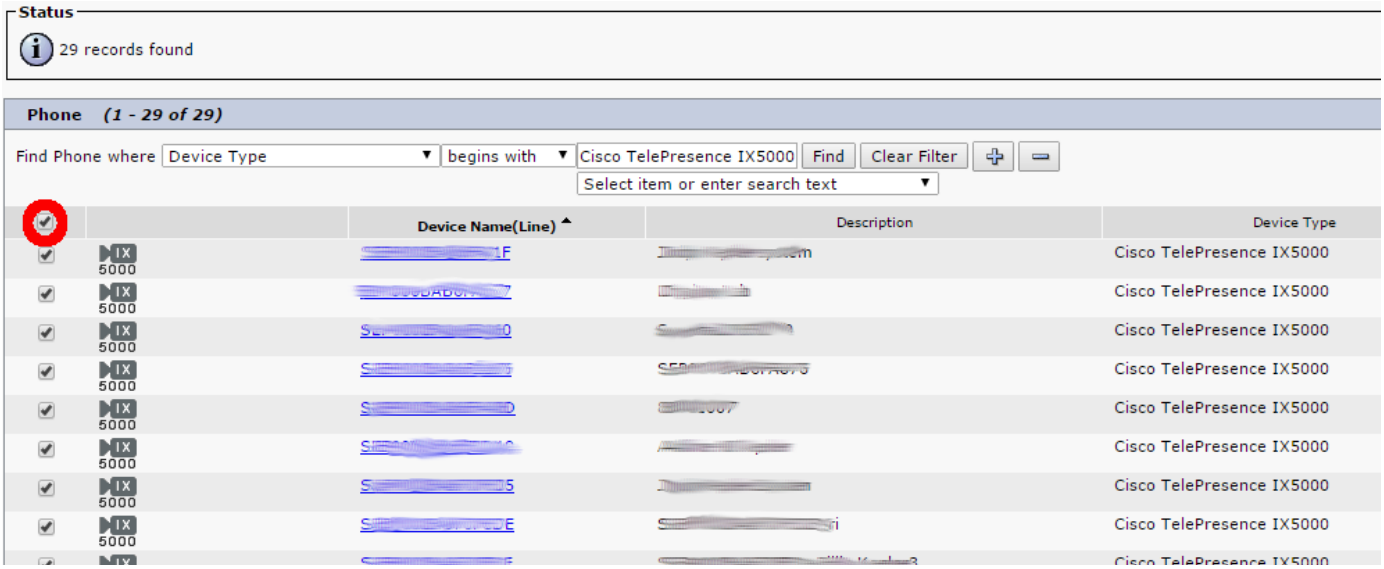
e. 次の手順を実行して、新しいコーデック イメージ ファイルを適用するデバイス タイプを検索してアクセスします。

1. [電話を次の条件で検索（Find Phone Where）] 領域で、ドロップダウン リストから [デバイス タイプ（Device Type）] と [で始まる（begins with）] を選択します。

2. **Cisco TelePresence IX5000** と入力します。

3. [検索（Find）] をクリックします。結果の画面の例は図 1-9 のとおりです。

図 1-9　デバイス タイプの検索後の結果の画面



4. ページの左側にあるチェックボックスを選択して、すべてのデバイスを選択します。

ヒント 図 1-9 では、このチェックボックスが赤い丸で囲まれています。

5. [選択項目への設定の適用（Apply Config to Selected）] をクリックして、選択したすべてのデバイスに設定を適用します。

（注） システムがコール中でない場合は、[選択項目への設定の適用（Apply Config to Selected）] ボタンをクリックするとただちに、すべての IX システムが再起動します。コール中の場合は、コールが終了するとただちに再起動します。

ステップ 3　ソフトウェアを特定のデバイスに対してロードするには、次の手順を実行します。

a. [デバイス（Device）] > [電話（Phone）] の順に移動します。

b. 次の手順を実行し、デバイスを検索してアクセスします。

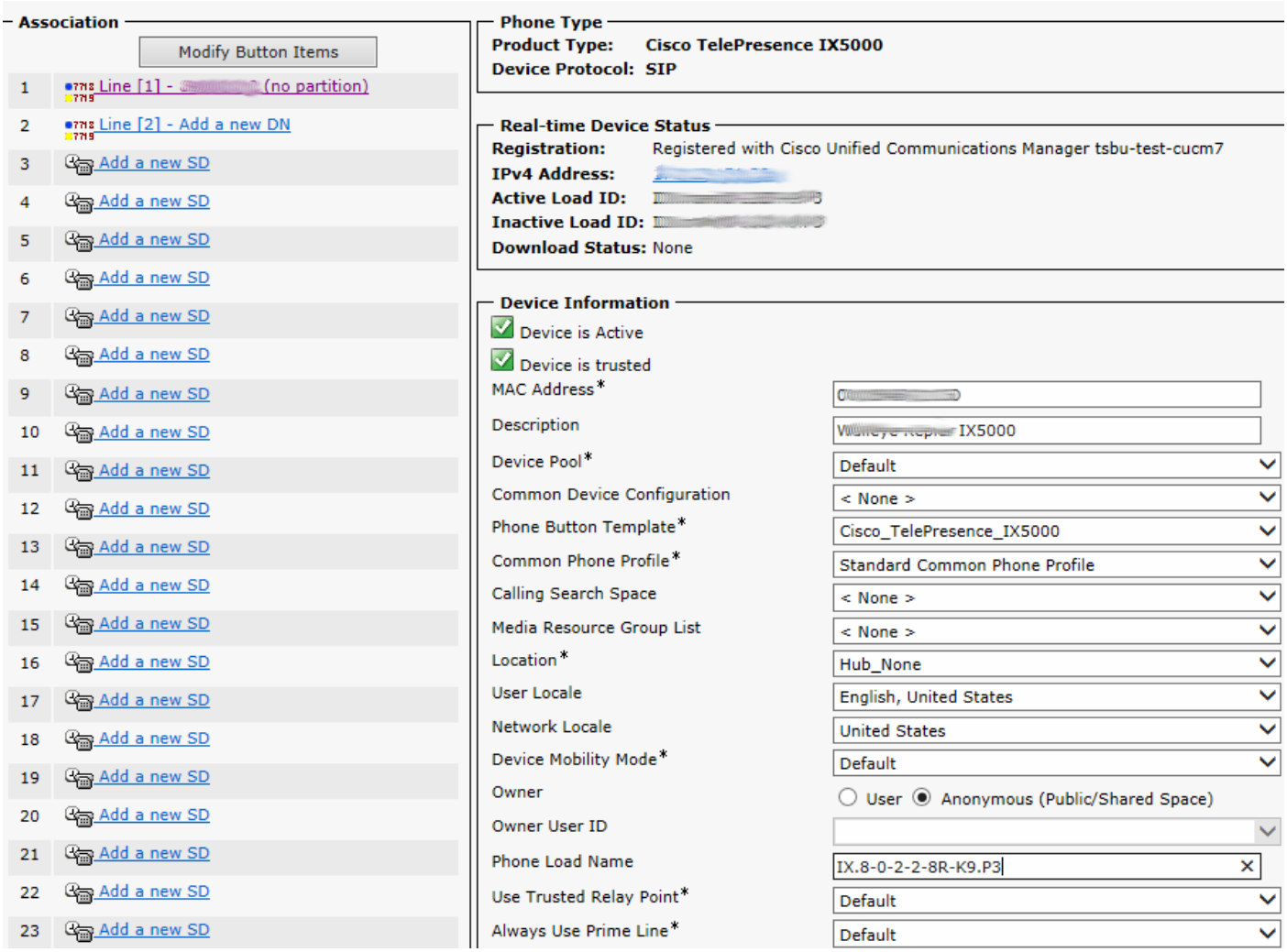
1. ドロップダウンの選択肢を使用して有効な検索条件を指定するか、フィールドを空白のままにしてすべてのデバイスを検索します。
2. [検索（Find）] をクリックします。
3. デバイスに対応する [デバイス名（回線）（Device Name (Line)）] 行内のハイパーテキスト リンクをクリックします。

ステップ 4　次の手順を実行して、コーデック ファイル イメージをシステムに適用します。

a. [電話ロード名（Phone Load Name）] フィールドにファイルの名前を入力します。ファイル名の前の cmterm- は入力しません。

図 1-10 の例では、管理者によって IX.8-0-2-2-8R-K9.P3 というファイル名が指定されています。

図 1-10　[電話ロード名（Phone Load Name）] フィールド



b. [保存（Save）] をクリックします。

c. [設定の適用（Apply Config）] をクリックします。

（注）　システムがコール中でない場合は、[設定の適用（Apply Config）] をクリックするとただちに、すべての IX システムが再起動します。コール中の場合は、コールが終了するとただちに再起動します。

IX システムの新しい電話セキュリティ プロファイルの追加

IX システム の新しい電話セキュリティ プロファイルを追加するには、次の手順に従います。

ステップ 1　[Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスにログインします。

ステップ 2　[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）] の順に移動します。

ステップ 3　ウィンドウの下部にある [新規追加（Add New）] ボタンをクリックします。[電話セキュリティ プロファイルの設定（Phone Security Profile Configuration）] ウィンドウが表示されます。

ステップ 4　[電話セキュリティ プロファイルのタイプ（Phone Security Profile Type）] ドロップダウン メニューから [Cisco TelePresence IX5000] を選択し、[次へ（Next）] をクリックします。

ステップ 5　表 1-1 を参考にして、[電話セキュリティ プロファイル情報（Phone Security Profile Information）] ページに設定情報を入力します。

ステップ 6　[保存（Save）] ボタンをクリックし、設定を保存します。

（注）　管理インターフェイスのアスタリスク（*）が付いているフィールドは必須フィールドです。

表 1-1　[SIP 電話セキュリティ プロファイル情報（SIP Phone Security Profile Information）] フィールド

フィールド	設定
名前 *（Name*）	セキュリティ プロファイルの名前を入力します。 新しいプロファイルを保存すると、電話タイプとプロトコルの [電話の設定（Phone Configuration）] ウィンドウの [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 ボックスにその名前が表示されます。 **ヒント**　セキュリティ プロファイル名にデバイス モデルとプロトコルを含めると、プロファイルの検索または更新時に正しいプロファイルを検索できます。
[説明（Description）]	セキュリティ プロファイルの説明を入力します。
ナンス確認時間 *（Nonce Validity Time*）	ナンス値が有効な分数（秒単位）を入力します。デフォルト値は 600（10 分）です。この期限が切れると、Cisco Unified CM は新しい値を生成します。 **（注）**　ナンス値（ダイジェスト認証をサポートする乱数）を使用して、ダイジェスト認証パスワードの MD5 ハッシュを計算します。

表 1-1　[SIP 電話セキュリティ プロファイル情報（SIP Phone Security Profile Information）] フィールド （続き）

フィールド	設定
デバイス セキュリティ モード *（Device Security Mode*）	ドロップダウン メニューから [暗号化済（Encrypted）] を選択します（推奨）。 暗号化済モードでは、Cisco Unified CM は電話の整合性、認証、および暗号化を提供できます。シグナリングに対して AES128/SHA を使用する TLS 接続が開き、SRTP はすべての SRTP 対応 SIP ホップのすべての通話に対してメディアを伝送します。 **（注）** [デバイス セキュリティ モード（Device Security Mode）] が [暗号化済（Encrypted）] に設定され、[クラスタ セキュリティ モード（Cluster Security Mode）] が 1（混合モード）に設定されている場合に限り、画面に [暗号化済みメディア（Media is Encrypted）]（施錠）アイコンが表示されます。 クラスタ セキュリティ モードを設定するには、使用している Unified CM のリリースに応じた『*Cisco Unified Communications Manager Security Guide*』を参照してください。 [デバイス セキュリティ モード（Device Security Mode）] フィールドのその他の選択肢： • 非セキュア（Non Secure）：イメージ認証を除くセキュリティ機能は電話に適用されていません。TCP 接続が Cisco Unified CM に対して開きます。 • 認証済（Authenticated）：Cisco Unified CM は電話の整合性と認証を提供します。NULL/SHA を使用する TLS 接続が開きます。
転送タイプ *（Transport Type*）	[デバイス セキュリティ モード（Device Security Mode）] が [非セキュア（Non Secure）] の場合は、ドロップダウン リスト ボックスから次のオプションのいずれかを選択します（すべてのオプションが表示されるわけではありません）。 • TCP：伝送制御プロトコルを選択し、パケットが送信したときと同じ順序で受信されるようにします。このプロトコルを使用すると、パケットはドロップされませんが、プロトコルはセキュリティを提供しません。 • UDP：ユーザ データグラム プロトコルを選択し、パケットがすばやく受信されるようにします。このプロトコルはパケットをドロップする可能性があり、パケットは送信された順序で受信されない場合があります。このプロトコルはセキュリティを提供しません。 • TCP + UDP：TCP と UDP を組み合わせて使用する場合は、このオプションを選択します。このオプションはセキュリティを提供しません。 [デバイス セキュリティ モード（Device Security Mode）] が [認証済（Authenticated）] または [暗号化済（Encrypted）] の場合、TLS はデフォルトの [転送タイプ（Transport Type）] になります。TLS は、SIP 電話に対してシグナリングの整合性、デバイス認証、およびシグナリング暗号化（暗号化モードのみ）を提供します。 **（注）** プロファイルで [デバイス セキュリティ モード（Device Security Mode）] を設定できない場合は、転送タイプとして UDP を指定します。
[ダイジェスト認証を有効化（Enable Digest Authentication）]	IX デバイスではサポートされません。このボックスはオフのままにしてください。

表 1-1　[SIP 電話セキュリティ プロファイル情報（SIP Phone Security Profile Information）] フィールド （続き）

フィールド	設定
TFTP 暗号化（TFTP Encrypted Config）	このボックスをオンにすると、Cisco Unified CM は TFTP サーバからの電話のダウンロードを暗号化します。 **ヒント**　このオプションを有効化し、対称キーを設定してダイジェスト信用証明書と管理パスワードを保護することをお勧めします。
設定ファイル内のダイジェスト信用証明書を除外（Exclude Digest Credentials in Configuration File）	このボックスはオフのままにしてください。これは、Cisco Unified IP Phone の一部のモデルでのみサポートされます。

電話セキュリティ プロファイル CAPF 情報

[電話セキュリティ プロファイル CAPF 情報（Phone Security Profile CAPF Information）] のフィールドを設定するには、次の手順を実行します。CAPF セキュリティの詳細については、『*Securing Cisco TelePresence Products*』ガイドの「Activating the CAPF Server」の項を参照してください。

ステップ 1　表 1-2 を参考にして、[電話セキュリティ プロファイル CAPF 情報（Phone Security Profile CAPF Information）] を入力します。

ステップ 2　[保存（Save）] ボタンをクリックし、設定を保存します。

表 1-2　電話セキュリティ プロファイル CAPF 情報

フィールド	設定
認証モード *（Authentication Mode*）	選択肢は次のとおりです。 • Null ストリング • 既存の証明書（LSC の優先） • 既存の証明書（MIC の優先）
キー サイズ（ビット）*（Key Size (Bits)*）	選択肢は次のとおりです。 • 512 • 1024 • 2048

（注）　これらのフィールドは [電話の設定（Phone Configuration）] ページの CAPF 情報の設定に関連するものです。

[電話で使用されるパラメータ（Parameters Used in Phone）] フィールド

[電話で使用されるパラメータ（Parameters Used in Phone）] フィールドを設定するには、次の手順を実行します。

ステップ 1　表 1-3 を参考にして、[SIP 電話ポート（SIP Phone Port）] に情報を入力します。

ステップ 2　[保存（Save）] ボタンをクリックし、設定を保存します。

表 1-3　[電話で使用されるパラメータ（Parameters Used in Phone）] フィールド

フィールド	必須（Required）	設定
SIP 電話ポート（SIP Phone Port）	○	この設定は、UDP 転送を使用している SIP 電話に適用されます。 UDP を使用して Cisco Unified CM からの SIP メッセージを監視している Cisco Unified SIP IP Phone のポート番号を入力します。デフォルト設定は 5060 です。 IX システムで TCP または TLS を使用する場合は、この設定を無視します。

Unified CM への IX システムの追加

（注）　この手順を開始する前に、IX システムの MAC アドレスをメモしてください。MAC アドレスの確認方法については、「はじめる前に」セクション（v ページ）を参照してください。

ここでは、Unified CM に新しい IX システムを追加するための手順および以下の手順について説明します。

Unified CM GUI による IX システムの追加

Unified CM に新しい IX システムを追加するには、次の手順を実行します。

ステップ 1　[Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスにログインします。

ステップ 2　必要に応じて [Cisco Unified CM の管理（Cisco Unified CM Administration）] ドロップダウンから選択し、[移動（Go）] をクリックします。

ステップ 3　[デバイス（Device）] ドロップダウン メニューから [電話（Phone）] を選択します。[電話の検索と一覧表示（Find and List Phones）] ページが表示されます。

ステップ 4　[新規追加（Add New）] ボタンをクリックします。

ステップ 5　[新規電話を追加（Add a New Phone）] ウィンドウで、[電話のタイプ（Phone Type）] ドロップダウン リストから [Cisco TelePresence IX5000] を選択します。

（注）　システムが Cisco TelePresence System IX5200 である場合でも、この電話タイプを指定してください。

ステップ 6　[次へ（Next）] をクリックし、[電話の設定（Phone Configuration）] ウィンドウを表示します。

ステップ 7　[電話の設定（Phone Configuration）] ウィンドウのフィールドに入力します。これらのフィールドについては、表 1-4 から表 1-13 を参照してください。

ステップ 8　変更が完了したら、[保存（Save）] をクリックして設定を保存します。

[デバイス情報（Device Information）] 領域

表 1-4 に、[デバイス情報（Device Information）] 領域のフィールドの説明を示します。

（注）　管理インターフェイスのアスタリスク（*）が付いているフィールドは必須フィールドです。

表 1-4　[デバイス情報（Device Information）] 領域のフィールド

フィールド	設定
MAC アドレス（MAC Address）*	Cisco TelePresence プライマリ コーデックの MAC アドレス。 システムの MAC アドレスを検索するには、「システム MAC アドレスの検索」セクション（vi ページ）を参照してください。
説明	デバイスの簡単な説明。
デバイス プール *（Device Pool*）	デバイス プール。[デフォルト（Default）] を選択するか、ドロップダウン メニューからデバイス プールを選択します。 [詳細の表示（View Details）] をクリックして、[デバイスの詳細（Device Details）] ウィンドウを開きます。このウィンドウには、次のシステム設定情報が含まれています。 • デバイス プール情報（Device Pool Information） • デバイス プール設定（Device Pool Configuration） • [ローミングに合わせて変化する設定（Roaming Sensitive Settings）] • [ローカルルートグループの設定（Local Route Group Settings）] • [デバイスモビリティ関連情報（Device Mobility Related Information）] • 位置情報の設定（Geolocation Configuration） • コール ルーティング情報（Call Routing Information） – [着信の発呼側設定（Incoming Calling Party Settings）] – [着信の着呼側設定（Incoming Called Party Settings）] – [電話の設定（Phone Settings）]

表 1-4　[デバイス情報（Device Information）] 領域のフィールド （続き）

フィールド	設定
共通デバイス設定（Common Device Configuration）	[< なし >（<None>）] を選択します。 [詳細の表示（View Details）] をクリックして、[共通デバイス設定の詳細（Common Device Configuration Detail）] ウィンドウを開きます。このウィンドウには、次のシステム設定情報が含まれています。 • 共通デバイス設定情報 • 電話の IPv6 • MLPP と機密アクセス レベル
電話ボタン テンプレート *（Phone Button Template*）	[Cisco_TelePresence_IX5000] を選択します。
共通の電話プロファイル *（Common Phone Profile*）	[標準の共通の電話プロファイル（Standard Common Phone Profile）] を選択します。
[コーリングサーチスペース（Calling Search Space）]	[< なし >（<None>）] を選択します。 **（注）**　このフィールドには、この Unified CM で作成されたコーリング サーチ スペースが反映されます。
[メディアリソースグループリスト（Media Resource Group List）]	[< なし >（<None>）] を選択します。
[ロケーション（Location）]*	[Hub_None] を選択します。 他の選択肢は、[ファントム（Phantom）] または [シャドウ（Shadow）] です。
ユーザ ロケール（User Locale）	[英語、アメリカ合衆国（English, United States）] を選択します。 **（注）**　現在、他のロケールは使用できません。
ネットワーク ロケール（Network Locale）	[United States（米国）] を選択します。 **（注）**　現在、他のロケールは使用できません。
デバイス モビリティ モード *（Device Mobility Mode*）	[デフォルト（Default）] を選択します。 [現在のデバイス モビリティ設定の表示（View Current Device Mobility Settings）] をクリックし、[デバイス モビリティ詳細（Device Mobility Details）] ウィンドウを開きます。このウィンドウには、現在のデバイス モビリティ設定が表示されます。
[オーナー（Owner）]	[匿名（公共 / 共有スペース）（Anonymous (Public/Shared Space)）] を選択します。
[オーナーのユーザ ID（Owner User ID）]	このフィールドには保存されているユーザ ID が表示されます。[オーナー（Owner）] フィールドで [匿名（Anonymous）] を選択した場合、このフィールドはグレー表示されます。そのままにしてください。

表 1-4　[デバイス情報（Device Information）] 領域のフィールド （続き）

フィールド	設定
電話ロード名（Phone Load Name）	システムのリブート後にロードする Cisco TelePresence ソフトウェアのバージョンを指定します。**IX.8**-*x*-*x*-*x*-*x***R**-**K9**.**P3** の形式でバージョンを指定します。ファイル名の前の cmterm- と拡張子 .cop.sgn は含めません。 たとえば、cmterm-IX.8-0-2-2-8R-K9.P3.cop.sgn という名前のファイルの場合は、**IX.8-0-2-2-8R-K9.P3** と入力します。 **（注）**　また、[デバイス（Device）] > [デバイスの設定（Device Settings）] > [デバイスのデフォルト（Device Defaults）] に移動し、[ロード情報（Load Information）] フィールドでソフトウェア イメージの名前を指定することで、Unified CM に登録されているすべての IX システムに対して 1 つのデフォルト イメージを指定できます。詳細については、「システム用の IX ソフトウェア イメージ ファイルの指定」セクション（1-9 ページ）を参照してください。
信頼されたリレー ポイントを使用 *（Use Trusted Relay Point*）	[デフォルト （Default）] を選択します。
常にプライム回線を使用する *（Always Use Prime Line*）	[デフォルト （Default）] を選択します。
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*）	[デフォルト （Default）] を選択します。
位置情報（GeoLocation）	[< なし >（<None>）] を選択します。
[デバイス情報（Device Information）] 領域のチェックボックス	
ビデオ コールをオーディオとして再試行（Retry Video Call as Audio）	このボックスはオンのままにしてください。
プレゼンテーション インジケータを無視（Ignore Presentation Indicators）	このボックスはオフのままにしてください。
[CTI からのデバイスの制御を許可（Allow Control of Device from CTI）]	このボックスはオンのままにしてください。
ハント グループにログイン（Logged into Hunt Group）	このボックスはオンのままにしてください。
リモート デバイス（Remote Device）	このボックスはオフのままにしてください。
（注）　変更が完了したら、[保存（Save）] をクリックして設定を保存します。	

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

表 1-5 に、[プロトコル固有情報（Protocol-Specific Information）] 領域のフィールドの説明を示します。

（注）　システムを動作させる上で、これらのフィールドを変更する必要はありません。

表 1-5　[番号表示トランスフォーメーション（Number Presentation Transformation）] 領域のフィールド

フィールド	設定
[この電話からのコールの発信者 ID（Caller ID For Calls From This Phone）] 領域	
[発呼側トランスフォーメーション CSS（Calling Party Transformation CSS）]	[< なし >（<None>）] を選択します（選択がグレー表示されます）。
デバイス プールの発呼側トランスフォーメーション CSS を使用（この電話からのコールの発信者 ID）（Device Pool Calling Party Transformation CSS (Caller ID For Calls From This Phone)）	このボックスはオンのままにしてください。
[リモート番号（Remote Number）] 領域	
[発呼側トランスフォーメーション CSS（Calling Party Transformation CSS）]	[< なし >（<None>）] を選択します（選択がグレー表示されます）。
デバイス プールの発呼側トランスフォーメーション CSS を使用（デバイス モビリティ関連情報）（Use Device Pool Calling Party Transformation CSS (Device Mobility Related Information)）	このボックスはオンのままにしてください。
（注）　変更が完了したら、[保存（Save）] をクリックして設定を保存します。	

[プロトコル固有情報（Protocol-Specific Information）] 領域

表 1-6 に、[プロトコル固有情報（Protocol-Specific Information）] 領域のフィールドの説明を示します。

（注）　管理インターフェイスのアスタリスク（*）が付いているフィールドには、基本設定を入力する必要があります。

表 1-6　[プロトコル固有情報（Protocol-Specific Information）] 領域のフィールド

フィールド	設定
パケット キャプチャ モード *（Packet Capture Mode*）	[< なし >（<None>）] を選択します。
パケット キャプチャ時間（Packet Capture Duration）	**0** を選択します。
BLF プレゼンス グループ *（BLF Presence Group*）	[標準のプレゼンス グループ（Standard Presence Group）] を選択します。
SIP ダイヤル規則（SIP Dial Rules）	[< なし >（<None>）] を選択します。
MTP 優先発信コーデック *（MTP Preferred Originating Codec*）	[711ulaw] を選択します（選択がグレー表示されます）。
デバイス セキュリティ プロファイル *（Device Security Profile*）	ここでセキュリティ プロファイルを選択します。 • セキュア プロファイルの場合は、[Cisco TelePresence IX5000— 標準 SIP 非セキュア プロファイル（Cisco TelePresence IX5000—Standard SIP Non-Secure Profile）] を選択します。 • 非セキュア プロファイルの場合は、[Cisco TelePresence IX5000 セキュア プロファイル（Cisco TelePresence IX5000 Secure Profile）] を選択します。 システムのセキュリティを設定するには、電話セキュリティ プロファイルを作成し、このフィールドで IX システムにプロファイルを適用します。詳細については、『*Securing Cisco TelePresence Products*』ガイドの「Configuring Cisco TelePresence Phone Profile Security」の項を参照してください。
再ルーティング用コーリング サーチ スペース（Rerouting Calling Search Space）	[< なし >（<None>）] を選択します。 **（注）**　このフィールドには、この Unified CM で作成されたコーリング サーチ スペースが反映されます。
[SUBSCRIBE コーリングサーチスペース（AAR Calling Search Space）]	[< なし >（<None>）] を選択します。 **（注）**　このフィールドには、この Unified CM で作成されたコーリング サーチ スペースが反映されます。
SIP プロファイル *（SIP Profile*）	[標準 SIP プロファイル（Standard SIP Profile）] を選択します。 Binary Floor Control Protocol（BFCP）を設定する場合でも、このプロファイルを使用します。BFCP の設定方法の詳細については、「BFCP over UDP Collaboration 機能の設定」セクション（2-2 ページ）を参照してください。 このフィールドには、この Unified CM で作成された SIP プロファイルが反映されます。
[ダイジェストユーザ（Digest User）]	[< なし >（<None>）] を選択します。
チェックボックス	
メディア ターミネーション ポイントが必須（Media Termination point Required）	このボックスはオフのままにしてください。
不在ポート（Unattended Port）	このボックスはオフのままにしてください。

表 1-6　[プロトコル固有情報（Protocol-Specific Information）] 領域のフィールド （続き）

フィールド	設定
BFCP を使用するプレゼンテーション共有を許可（Allow Presentation Sharing using BFCP）	プレゼンテーションを共有する場合は、このチェックボックスをオンにして Binary Floor Control Protocol（BFCP）の使用を有効にします。それ以外の場合はオフのままにします。詳細については、「BFCP を使用するための Unified CM の設定」セクション（2-3 ページ）を参照してください。

（注）　変更が完了したら、[保存（Save）] をクリックして設定を保存します。

[CAPF の情報（Certification Authority Proxy Function (CAPF) Information）] 領域

表 1-7 に、[CAPF の情報（Certification Authority Proxy Function (CAPF) Information）] 領域のフィールドの説明を示します。

（注）　管理インターフェイスのアスタリスク（*）が付いているフィールドには、基本設定を入力する必要があります。

（注）　セキュリティ プロファイルには追加の CAPF 設定が含まれています。

CAPF の設定およびアクティブ化の詳細については、『*Securing Cisco TelePresence Products*』ガイドの「Activating the CAPF Server」の項を参照してください。

表 1-7　[CAPF の情報（Certification Authority Proxy Function (CAPF) Information）] 領域のフィールド

フィールド	設定
証明書の操作 *（Certificate Operation*）	[保留中の操作なし（No pending Operation）] を選択します。[CAPF の情報（CAPF Information）] ウィンドウの大部分の設定フィールドは変更できません。 **（注）**　ドロップダウン メニューから [インストール/アップグレード（Install/Upgrade）]、[削除（Delete）]、または [トラブルシューティング（Troubleshoot）] を選択できます。これらのオプションのいずれかを選択すると、[CAPF の情報（CAPF Information）] ウィンドウの他のフィールドを変更できるようになります。
認証モード *（Authentication Mode*）	[証明書の操作（Certificate Operation）] フィールドで [保留中の操作なし（No Pending Operation）] を選択した場合、このフィールドはグレー表示されます。
認証文字列（Authentication String）	[証明書の操作（Certificate Operation）] フィールドで [保留中の操作なし（No Pending Operation）] を選択した場合、このフィールドはグレー表示されます。
キー サイズ（ビット）*（Key Size (Bits)*）	[証明書の操作（Certificate Operation）] フィールドで [保留中の操作なし（No Pending Operation）] を選択した場合、このフィールドはグレー表示されます。
操作の完了期限（Operation Completes By）	[証明書の操作（Certificate Operation）] フィールドで [保留中の操作なし（No Pending Operation）] を選択した場合、このフィールドはグレー表示されます。
証明書の操作ステータス（Certificate Operation Status）	このフィールドのデフォルト値は、[なし（None）] です。他の選択は許可されません。

（注）　変更が完了したら、[保存（Save）] をクリックして設定を保存します。

[外部データ位置情報（External Data Locations Information）] 領域

（注）　システムを動作させる上で、これらのフィールドを変更する必要はありません。

次のフィールドにデフォルト以外の値を入力します。

- 情報（Information）
- ディレクトリ（Directory）
- メッセージ（Messages）
- サービス（Services）
- 認証サーバ（Authentication Server）
- プロキシ サーバ（Proxy Server）
- アイドル（Idle）
- アイドル タイマー（秒）（Idle Timer (seconds)）
- セキュア認証 URL（Secured Authentication URL）
- セキュア ディレクトリ URL（Secured Directory URL）
- セキュア アイドル URL（Secured Idle URL）
- セキュア情報 URL（Secured Information URL）
- セキュア メッセージ URL（Secured Messages URL）
- セキュア サービス URL（Secure Services URL）

[MLPP および機密アクセス レベル情報（MLPP and Confidential Access Level Information）] 領域

表 1-8 に、[MLPP および機密アクセス レベル情報（MLPP and Confidential Access Level Information）] 領域のフィールドを示します。

（注）　システムを動作させる上で、これらのフィールドを変更する必要はありません。

表 1-8　[CAPF の情報（Certification Authority Proxy Function (CAPF) Information）] 領域のフィールド

フィールド	必須かどうか	設定
[MLPP ドメイン（MLPP Domain）]	[いいえ（No）]	[< なし >（<None>）] を選択します。
機密アクセス モード（Confidential Access Mode）	[いいえ（No）]	[< なし >（<None>）] を選択します。 選択肢は、[< なし >（<None>）]、[固定（Fixed）]、[変動（Variable）] です。
機密アクセス レベル（Confidential Access Level）	[いいえ（No）]	[< なし >（<None>）] を選択します。

（注）　変更が完了したら、[保存（Save）] をクリックして設定を保存します。

[プロダクト固有の設定（Product Specific Configuration Layout）] 領域

表 1-9 に、[プロダクト固有の設定（Product Specific Configuration Layout）] 情報フィールドの説明を示します。

（注）　管理インターフェイスのアスタリスク（*）が付いているフィールドには、基本設定を入力する必要があります。

表 1-9　[プロダクト固有の設定（Product Specific Configuration Layout）] 領域のフィールド

フィールド	説明
Cisco TelePresence タイプ *（Cisco TelePresence Type*）	インストールされている Cisco TelePresence System のタイプを示します。選択肢は次のとおりです。 • Cisco TelePresence IX5000（6 シート） • Cisco TelePresence IX5000（18 シート） • Cisco TelePresence IX5000（14 シート）（将来のソフトウェア リリース用に予約）
管理 Web アクセス *（Web Access*）	有効にすると、Cisco TelePresence Web Administration インターフェイスにアクセスできます。 デフォルトは [有効（Enabled）] です。
会議室名（Exchange(R)）（Room Name (from Exchange(R))）	Microsoft Exchange に示されている会議室名。このフィールドには、最大 64 文字までのテキスト文字列を入力できます。 （注）　Cisco TelePresence Manager を使用して会議をスケジュールする場合は、会議室の名前が必要です。この名前は、Microsoft Exchange または Domino データベースに入力したリソース メールボックス（ドメイン名を含む）と正確に一致する必要があります。これは、電話会議をスケジュールするために使用されます。
最大通話時間（分）*（Maximum Call Duration (in minutes)*）	Cisco TelePresence 電話会議に対して許可される最大時間（分単位）。 • 最小値は 0 です。この値は、最大時間が設定されていないことを意味します。 • 最大値は 10080（7 日間）です。 （注）　この機能は、Cisco Unified Communications Manager サービス パラメータの [Maximum Call Duration タイマー（Maximum Call Duration Timer）] に合わせて調整されます。いずれかのフィールドで 0 以外の値が入力されると、小さい方の値が優先されます。
品質（ディスプレイあたり）*（Quality (per Display)*）	システムで使用される帯域幅。 帯域幅の選択の詳細については、『*Administration Guide for Cisco TelePresence Software Release IX 8*』の「1080p 60 Main Video」の項を参照してください。 選択肢は次のとおりです。 • 最高画質、ベスト モーション：1080p（Highest Detail, Best Motion: 1080p）（デフォルト） • 最高画質、ベター モーション：1080p（Highest Detail, Better Motion: 1080p） • 最高画質、グッド モーション：1080p（Highest Detail, Good Motion: 1080p） • 高画質、ベスト モーション：720p（High Detail, Best Motion: 720p） • 高画質、ベター モーション：720p（High Detail, Better Motion: 720p） • 高画質、グッド モーション：720p（High Detail, Good Motion: 720p）

表 1-9　[プロダクト固有の設定（Product Specific Configuration Layout）] 領域のフィールド （続き）

フィールド	説明
帯域幅割り当ての重み付け *（Bandwidth Allocation Weights*）	会議のビデオとプレゼンテーション ビデオ間の帯域幅割り当て比率を設定します。このパラメータのデフォルト値は、合計比率 10 に対して、メイン ビデオの比率が 8、プレゼンテーション ビデオの比率が 2 となります。 選択肢は次のとおりです。 • 9 メイン/1 プレゼンテーション（3 Main/7 Presentation） • 8 メイン/2 プレゼンテーション（8 Main/2 Presentation）（デフォルト） • 6 メイン/4 プレゼンテーション（3 Main/7 Presentation） • 4 メイン/6 プレゼンテーション（3 Main/7 Presentation） • 3 メイン/7 プレゼンテーション（3 Main/7 Presentation） 重み付けの詳細については、『*Administration Guide for Cisco TelePresence Software Release IX 8*』の「Video Bandwidth Allocation Weights」の項を参照してください。
メイン ディスプレイのフレーム数 / 秒 *（Main Display Frames Per Second*）	メイン ディスプレイ画面のフレーム レート（1 秒あたりのフレーム数（fps））を選択します。選択肢は次のとおりです。 • 30 fps メイン（60 fps main） • 60 fps メイン（60 fps main）
ディスプレイ非点灯日（Days Display Not Active）	Touch 10 デバイスをオフにしておく曜日を指定します。選択肢は、[日曜日（Sunday）] から [土曜日（Saturday）] です。デフォルトは [土曜日（Saturday）] と [日曜日（Sunday）] です。 **ヒント**　複数の曜日を選択するには、Ctrl キーを押しながら選択します。 詳細については、「Touch 10 画面のグレー表示」セクション（2-6 ページ）を参照してください。
ディスプレイ点灯時刻（Display On Time）	Touch 10 デバイスが非アクティブな状態からアクティブになる時刻を指定します。24 時間形式で値を入力します。この形式では 00:00 が真夜中の 12:00 を示し、23:59 が午後 11:59 を示します。 デフォルトは 07:30 です。このデフォルト値を使用すると、Touch 10 デバイスは土曜日と日曜日に非アクティブになり、その後、月曜日の午前 7:30 にアクティブになります。 詳細については、「Touch 10 画面のグレー表示」セクション（2-6 ページ）を参照してください。
ディスプレイ点灯継続時間（Display On Duration）	[ディスプレイ オンの時間（Display On Time）] の値が定義されている場合は、Touch 10 デバイスをオンにしておく時間の長さを指定します。24 時間形式で値を入力します。ここで 1:30 は 1 時間 30 分を表します。最大値は 24:00（24 時間）です。 デフォルトは 10:30 です。このデフォルト値を使用すると、Touch 10 デバイスは午後 6 時に非アクティブになります（午前 7:30 にアクティブになってから 10 時間半後）。 **（注）**　デフォルト値をクリアしてフィールドをブランクにすると、ディスプレイは午後 11:59 にオフになります。 詳細については、「Touch 10 画面のグレー表示」セクション（2-6 ページ）を参照してください。

表 1-9　[プロダクト固有の設定（Product Specific Configuration Layout）] 領域のフィールド （続き）

フィールド	説明
CTS 自動応答 *（CTS Auto Answer*）	IX システムが共有回線の Unified CM DN 設定を上書きできるようにします。 選択肢は次のとおりです。 • CUCM DN 設定に従う（Follow CUCM DN Settings）（デフォルト） – 内部のコールは [自動応答（Auto Answer）] または [非自動応答（No Auto Answer）] に設定されます。 – 外部のコールは [非自動応答（No Auto Answer）] に設定されます。 • CTS 優先 - すべてのコールに自動応答（CTS Override - Auto Answer All）：DN 設定に関係なく、内部および外部の両方のコールに自動応答を設定します。 • CTS 優先 - 内部のコールのみに自動応答（CTS Override - Auto Answer Internal Only）：DN 設定に関係なく、内部のコールに自動応答を設定します。 • CTS 優先 - 外部のコールのみに自動応答（CTS Override - Auto Answer External Only）：DN 設定に関係なく、外部のコールに自動応答を設定します。
G.722 コーデックのアドバタイズ *（Advertise G.722 Codec*）	ワイドバンド コーデック。Cisco Telepresence エンドポイントが G.722 オーディオ コーデックを Unified CM にアドバタイズするかどうかを示します。有効な場合、このオーディオ コーデックにプリファレンスが割り当てられます。 選択肢は次のとおりです。 • システム デフォルトの使用（Use System Default）（デフォルト）：この IX システムは、[アドバタイズ G.722 コーデック（Advertise G.722 Codec）] エンタープライズ パラメータで指定された設定に従います。 • 無効（Disabled）：この IX システムは G.722 を Cisco Unified CM にアドバタイズしません。 • 有効（Enabled）：この IX システムは G.722 を Cisco Unified CM にアドバタイズします。
外部 SYSLOG アドレス（External SYSLOG Address）	外部の syslog アドレスを設定します。許容される値：次のいずれかの Syslog アドレス形式が可能です。 • host または • host:port ホストはホスト名または IP アドレス（最大 60 文字）です。ポートは 0 ～ 65535 です。デフォルトは 514 です。
ディレクトリ検索用代替 CUCM（Alternate CUCM for Directory Lookup）	IX システムがディレクトリで照会する代替の Cisco Unified CM IP アドレスを設定します。最大長：64。
セルフ ビュー最大時間（秒）*（Maximum Self View Time (in seconds)*）	IX システムでセルフビューを実行できる最大時間長。デフォルトは 120 秒です。
プレゼンテーションのフレーム数 / 秒 *（Presentation Frames Per Second*）	外部プレゼンテーションの 1 秒あたりのフレーム数（fps）を選択します。デフォルトは 30 fps です。 システムで 15 fps を使用することを選択する場合は、この値が示す最大許容値として [30 fps] を選択します。

表 1-9　[プロダクト固有の設定（Product Specific Configuration Layout）] 領域のフィールド （続き）

フィールド	説明
ライブ サポート番号（Live Support Number）	ユーザが [ライブ サポート（Live Support）] ボタンまたはソフトキーを押したときに、システムがダイヤルする番号を指定します。ライブ サポート機能をアクティブにする場合に使用します。 **（注）**　この機能は最新の IX 8 リリースで使用できます。
コール終了時呼出音を有効にする（Enable Call Termination Ring）	このボックスをオンにすると、コールの終了時の呼出音が有効になります。デフォルトでは、このボックスはオンになります。
シングル マイクロフォン ミュートを有効にする（Enable Single Microphone Mute）	1 つのセグメントのミュート機能を有効にする場合にオンにします。詳細については、「単一セグメントのミュート化」セクション（2-6 ページ）を参照してください。デフォルトでは、ボックスはオフになっています。 **（注）**　この機能は最新の IX 8 リリースで使用できます。

[SSH 情報（SSH Information）] 領域

図 1-11 は、[セキュア シェル（SSH）情報（Secure Shell (SSH) Information）] ウィンドウを示しています。

図 1-11　[SSH 情報（SSH Information）] ウィンドウ

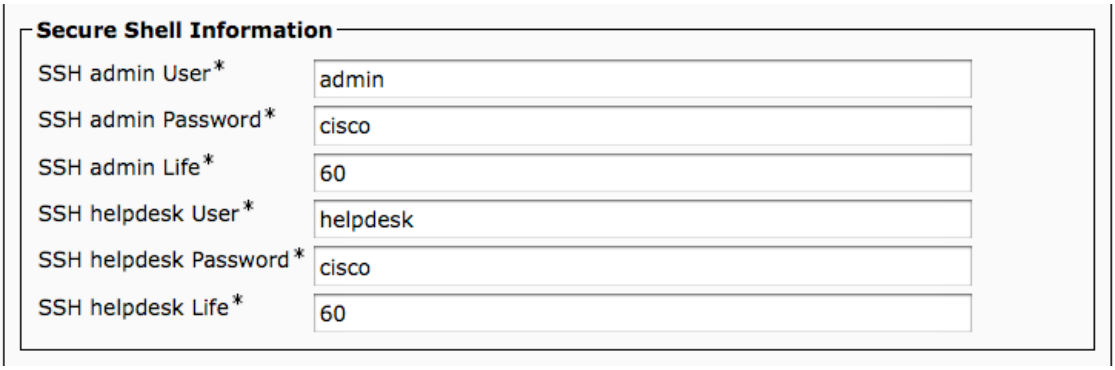


表 1-10 を参考にして、コマンドライン インターフェイス（CLI）や Cisco TelePresence Web 管理インターフェイスへのアクセスに使用する SSH アカウントのユーザ名とパスワードを指定します。

SSH ユーザ名とパスワードを変更すると、Cisco TelePresence 管理インターフェイスのユーザ名とパスワードも変更されます。

[保存（Save）] をクリックして設定を保存します。

表 1-10　Cisco TelePresence セキュア シェルの設定

フィールド	設定
SSH 管理ユーザ *（SSH admin User*）	セキュア シェル アカウントのユーザ名。SSH アクセスおよび Cisco TelePresence 管理インターフェイスへのアクセスに使用されます。Cisco Technical Assistance Center（TAC）では、トラブルシューティングとデバッグにセキュア シェルを使用します。TAC にお問い合わせください。デフォルトのユーザ名は **admin** です。ユーザ名の長さは 6 ～ 64 文字にすることができます。このユーザ名は CLI マルチレベル アクセス（MLA）に対応しています。 次のユーザ名は使用しないでください：**apache**、**daemon**、**help**、**helpdesk**、**nobody**、**operator**、**shutdown**。 ユーザ名とパスワードには、大文字と小文字の英数字およびアンダースコアとダッシュ文字を含めることができます。ユーザ名をハイフン（-）やアンダースコア（_）から始めることはできません。 **SSH 管理および SSH ヘルプデスクのユーザ名に関する注意：**ユーザ名の暫定的な変更を行わずに、SSH 管理ユーザ名と SSH ヘルプデスク ユーザ名を交換することはできません。たとえば、管理ユーザ名が **minad**、ヘルプデスクの名前が **deskhelp** である場合、次の手順を実行して、管理者名を **deskhelp**、ヘルプデスクの名前を **minad** に変更します。 1. 管理ユーザ名を一時パスワード（**admintemp** など）に変更してから、ヘルプデスクの名前を **minad** に変更します。 2. [保存（Save）] をクリックして、[設定を適用（Apply Config）] をクリックします。 3. Touch デバイスに [コール不可（Calls Not Possible）] ポップアップ画面が表示されなくなるまで待ちます。 4. 管理ユーザ名を **deskhelp** に変更します。
SSH 管理パスワード *（SSH admin Password*）	SSH アクセスおよび Cisco TelePresence Web 管理ページへのアクセスに使用される SSH アカウントのパスワード。デフォルトのパスワードは **cisco** です。 • 最大フィールド長は 64 文字です。 • 最小フィールド長は 6 文字です。

表 1-10　Cisco TelePresence セキュア シェルの設定 （続き）

フィールド	設定
SSH 管理期間 *（SSH admin Life*）	コマンドライン インターフェイス（CLI）コマンドを使用する場合に、パスワードの有効期限を設定してシステムが保護されるようにします。このパスワードは定期的に更新する必要があります。パスワードの更新に使用される更新済みの SSH フィールドについては、図 1-11 を参照してください。 パスワードの有効期限として、0 ～ 365 までの値を設定できます。0 を設定すると、パスワード エージングが無効になります。デフォルトは 60 日です。（0 を設定して）設定された有効期間を無効化していない限り、次の場合、パスワードの有効期間は 2 日を残して設定されます。 • 新規インストールおよび初期状態へのリセット。 • ソフトウェアのアップグレード（パスワードの有効期間が設定されている有効期間よりも短い場合） • パスワード回復（**pwrecovery** コマンドを使用） 現在のパスワードの有効期間が残り 14 日になると、画面上の警告メッセージが CLI ユーザに送信されます。メッセージはパスワードの有効期限が切れるまで表示されます。パスワードの失効が有効になっている場合は、[SSH 情報（SSH Information）] 領域ウィンドウに情報を入力して新しいパスワードを作成しない限り、CLI ログインの試みは無視され、ユーザはシステムにアクセスできません。 [リスタート（Restart）] をクリックして変更を保存します。これにより、更新された設定が読み込まれて IX システムに適用され、コール サービスが再起動されます。 または、[リセット（Reset）] をクリックして、IX システムをリブートします。起動時に、IX システムは Cisco Unified CM の設定を読み取り、変更を適用します。 詳細については、『*Cisco TelePresence System Command-Line Interface Reference Guide*』を参照してください。

表 1-10　Cisco TelePresence セキュア シェルの設定 （続き）

フィールド	設定
SSH ヘルプデスクのユーザ *（SSH helpdesk User*）	ヘルプデスク ユーザのセキュア シェル アカウントのユーザ名。SSH アクセスおよび Cisco TelePresence 管理インターフェイスへのアクセスに使用されます。Cisco Technical Assistance Center（TAC）では、トラブルシューティングとデバッグにセキュア シェルを使用します。TAC にお問い合わせください。デフォルトのユーザ名は **helpdesk** です。ユーザ名の長さは 6 ～ 64 文字にすることができます。 ヘルプデスク ユーザは CLI へのアクセスに制限があり、**set** コマンドは使用できません。 次のユーザ名は使用しないでください：**admin**、**apache**、**daemon**、**nobody**、**operator**、**shutdown**。 ユーザ名とパスワードには、大文字と小文字の英数字およびアンダースコアとダッシュ文字を含めることができます。ユーザ名をハイフン（-）やアンダースコア（_）から始めることはできません。 **SSH 管理および SSH ヘルプデスクのユーザ名に関する注意：**ユーザ名の暫定的な変更を行わずに、SSH 管理ユーザ名と SSH ヘルプデスク ユーザ名を交換することはできません。たとえば、管理ユーザ名が **minad**、ヘルプデスクの名前が **deskhelp** である場合、次の手順を実行して、管理者名を **deskhelp**、ヘルプデスクの名前を **minad** に変更します。 1. 管理ユーザ名を一時パスワード（**admintemp** など）に変更してから、ヘルプデスクの名前を **minad** に変更します。 2. [保存（Save）] をクリックして、[設定を適用（Apply Config）] をクリックします。 3. Touch デバイスに [コール不可（Calls Not Possible）] ポップアップ画面が表示されなくなるまで待ちます。 4. 管理ユーザ名を **deskhelp** に変更します。 5. [保存（Save）] をクリックして、[設定を適用（Apply Config）] をクリックします。
SSH ヘルプデスクのパスワード *（SSH helpdesk Password*）	SSH アクセスおよび Cisco TelePresence Web 管理ページへのアクセスに使用される SSH アカウントのパスワード。デフォルトのパスワードは **cisco** です。 • 最大フィールド長は 64 文字です。 • 最小フィールド長は 6 文字です。
SSH ヘルプデスク期間 *（SSH helpdesk Life*）	

[外部 CTS ログ設定（External CTS Log Destination）] 領域

このサブセクションは 6 つのフィールドで構成されています。最初の 4 つのフィールドでは、キャプチャしたログファイルをリモート サーバに「プッシュ」するよう IX システムを設定します。

図 1-12　　[外部 CTS ログ設定（External CTS Log Destination）] 領域

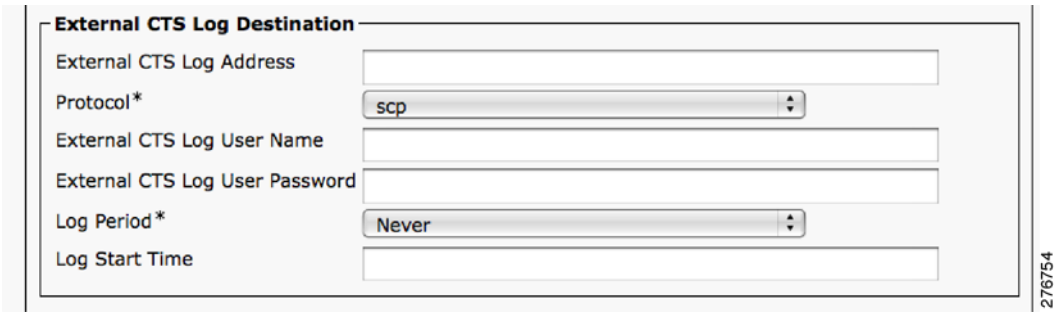


表 1-11 を参考にして、IX システム ログを保存する場所をフィールドに入力します。[保存（Save）] をクリックして設定を保存します。

（注）　管理インターフェイスのアスタリスク（*）が付いているフィールドは必須フィールドです。

表 1-11　　Cisco TelePresence の [外部 CTS ログ設定（External CTS Log Destination）] の設定

フィールド	設定
外部 CTS ログ アドレス（External CTS Log Address）	外部 IX システム ロギング アドレスを設定します。この値を設定すると、IX システム ログの生成時に、選択したプロトコルを使用してログのコピーがこのアドレスに送信されます。リモート マシンのアドレスにログ先のパスを追加できます。 次のいずれかのアドレス形式が可能です。 • host または • host:port ホストはホスト名または IP アドレス（最大 60 文字）です。ポートは 0 ～ 65535 です。デフォルトは 514 です。
プロトコル *	IX システム ログをログ先に転送するために使用するプロトコルを選択します。次のオプションから選択します。 • SCP（デフォルト） • SFTP • FTP
外部 CTS ログ ユーザ 名（External CTS Log User Name）	外部の IX システム ロギング ユーザ名を設定します。 最大長：64
外部 CTS ログ ユーザ パスワード（External CTS Log User Password）	外部の IX システム ロギング ユーザ パスワードを設定します。パスワードは書き込み専用です。 最大長：64

表 1-11　Cisco TelePresence の [外部 CTS ログ設定（External CTS Log Destination）] の設定 （続き）

フィールド	設定
ログ期間 *（Log Period*）	システムで外部 IX システム ログ情報を自動生成する頻度。次のオプションから選択します。 • しない（Never）（デフォルト） • 1 日に 1 回（Once per Day） • 3 日に 1 回（Once per 3 Days） • 1 週間に 1 回（Once per Week）
ログ開始時間（Log Start Time）	IX システムでログを生成する時刻を指定します。この値は 24 時間形式で指定する必要があります。ここで 00:00 は 1 日の始まりを表し、23:59 が 1 日の終わりを表します。このフィールドをブランクにすると、自動ロギング機能はオフになります。 最大長：5

[SNMP 設定パラメータ（SNMP Configuration Parameters）] 領域

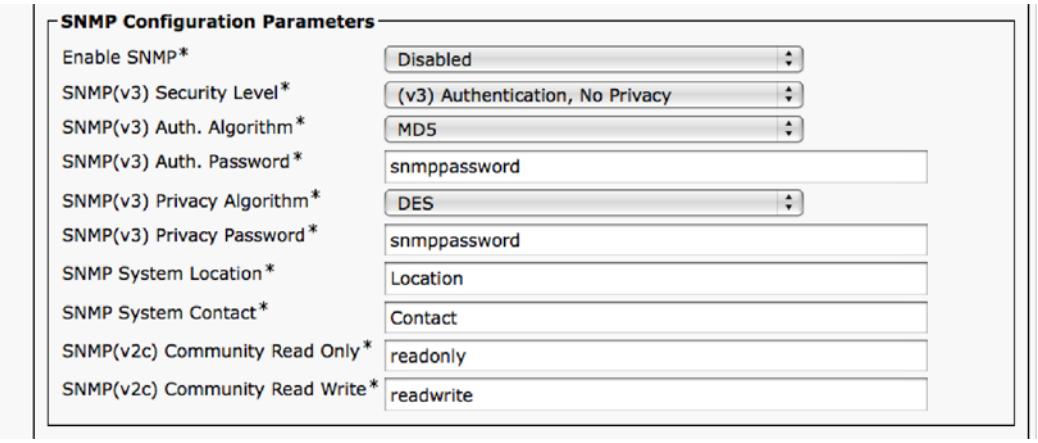
表 1-12 を参考にして、IX システムに関連付けられている SNMP サーバにアクセスするために必要な、簡易ネットワーク管理プロトコル（SNMP）の設定パラメータを指定します。

（注）　SNMP パラメータ フィールドのパスワードは、32 文字以内で指定します。

詳細については、『*Cisco TelePresence System Message Guide*』の「MIBs, RFCs, and SNMP Trap Messages for the Cisco TelePresence System」の章を参照してください。

図 1-13 に、[SNMP 設定パラメータ（SNMP Configuration Parameters）] 画面を示します。

図 1-13　SNMP 設定パラメータ



（注）　すべての SNMP フィールドは、該当する SNMP バージョンを表すようにマークされています。

（注）　管理インターフェイスのアスタリスク（*）が付いているフィールドは必須フィールドです。

表 1-12　Cisco TelePresence の [SNMP 設定パラメータ（SNMP Configuration Parameters）]

フィールド	設定
SNMP を有効にする *（Enable SNMP*）	CTS で SNMP を有効または無効にします。Cisco TelePresence System で SNMP をサポートするためには、SNMP を有効または無効にする必要があります。次のオプションがあります。 • 無効（デフォルト） • 有効（v3）（Enabled (v3)） • 有効（v3/v2）（Enabled (v3/v2)） • 有効（v2c）（Enabled (v2c)） **（注）**　SNMP ユーザ名は、システムによって自動的に「admin」に設定されます。
SNMP（v3）セキュリティ レベル *（SNMP (v3) Security Level*）	SNMP ユーザによってサポートされるセキュリティ レベル。このフィールドは、SNMP v3 だけで使用されます。次のセキュリティ レベルから選択します。 • （v3）認証、プライバシーなし（(v3) Authentication, No Privacy） • （v3）認証、プライバシー（(v3) Authentication, Privacy）
SNMP（v3）認証 アルゴリズム *（Algorithm*）	SNMP ユーザによってサポートされる認証アルゴリズム。このフィールドは、SNMP v3 だけで使用されます。次のアルゴリズムから選択します。 • MD5：メッセージ ダイジェスト アルゴリズム 5 • SHA：セキュア ハッシュ アルゴリズム
SNMP（v3）認証 パスワード *	Cisco TelePresence System に関連付けられた SNMP v3 サーバへのアクセス権を取得するために使用される SNMP 管理ユーザ認証パスワード。デフォルトのパスワードは **snmppassword** です。 • 最大フィールド長は 32 文字です。 • 最小フィールド長は 8 文字です。
SNMP（v3）プライバシー アルゴリズム *（SNMP (v3) Privacy Algorithm*）	SNMP ユーザによってサポートされるプライバシー アルゴリズム。このフィールドは、SNMP v3 だけで使用されます。次のプライバシー アルゴリズムから選択します。 • DES：データ暗号規格 • AES：高度暗号化規格
SNMP（v3）プライバシー パスワード *（SNMP (v3) Privacy Password*）	Cisco TelePresence システムで SNMP v3 を介してアクセスするために使用される SNMP 管理プライバシー パスワード。デフォルトのパスワードは **snmppassword** です。 • 最大フィールド長は 32 文字です。 • 最小フィールド長は 8 文字です。
SNMP システムのロケーション *（SNMP System Location*）	この Cisco TelePresence System に関連付けられた SNMP システムの場所。最大フィールド長は 64 文字です。 デフォルトは Location です。
SNMP システム コンタクト *（SNMP System Contact*）	この Cisco TelePresence System に関連付けられた SNMP システム接点の名前。最大フィールド長は 64 文字です。 デフォルトは Contact です。

表 1-12　Cisco TelePresence の [SNMP 設定パラメータ（SNMP Configuration Parameters）]（続き）

フィールド	設定
SNMP（v2c）コミュニティ（読み取り専用）*（SNMP (v2c) Community Read Only*）	SNMP コミュニティ ストリングは、MIB オブジェクトおよび関数へのアクセスを組み込みのパスワードとして認証します。読み取り専用では、コミュニティ ストリングを除く MIB のすべてのオブジェクトに対する認証済み管理ステーションへの読み取りアクセスが提供されますが、書き込みアクセスは許可されません。このフィールドは、SNMP v2c だけで使用されます。 デフォルトは readonly です。
SNMP（v2c）コミュニティ（読み取り / 書き込み）*（SNMP (v2c) Community Read Write*）	SNMP コミュニティ ストリングは、MIB オブジェクトおよび関数へのアクセスを組み込みのパスワードとして認証します。読み取りと書き込みでは、MIB 内のすべてのオブジェクトに対する認証済み管理ステーションへの読み取りと書き込みのアクセスが提供されますが、コミュニティ ストリングへのアクセスは許可されません。このフィールドは、SNMP v2c だけで使用されます。 デフォルトは readwrite です。

[SNMP トラップ レシーバ パラメータ（SNMP Trap Receive r Parameters）] 領域

表 1-13 に、IX システムに関連付けられている事前設定済みの SNMP トラップ レシーバ パラメータを示します。

（注） 最大 5 つのトラップ宛先を設定できます。

（注） 管理インターフェイスのアスタリスク（*）が付いているフィールドは必須フィールドです。

表 1-13　Cisco TelePresence の [SNMP トラップ レシーバ パラメータ（SNMP Trap Receiver Parameters）]

フィールド	設定
SNMP トラップ レシーバ 1	
1 SNMP（v3）トラップ レシーバ アドレス（1 SNMP (v3) Trap Receiver Address）	SNMP トラップが送信される SNMP トラップ レシーバ（リモートの SNMP システム）の IPV4 IP アドレスまたはホスト名。最大フィールド長は 64 文字です。
SNMP（v3）トラップ ユーザ名（SNMP (v3) Trap Username）	SNMP v3 に限ります。SNMP トラップが受信されるシステムへのアクセスに使用されるユーザ名。最大フィールド長は 32 文字です。ユーザ名は文字から始まる必要があります。 **注：**このフィールドではユーザ名として **admin** を使用しないでください。

表 1-13　Cisco TelePresence の [SNMP トラップ レシーバ パラメータ（SNMP Trap Receiver Parameters）]（続き）

フィールド	設定
SNMP セキュリティ レベル l*（SNMP Security Levell*）	SNMP v3 に限ります。SNMP トラップ レシーバでサポートされるセキュリティ レベル。指定できる値は次のとおりです。 • （v3）認証なし、プライバシーなし（(v3) No Authentication, No Privacy）（デフォルト） • （v3）認証、プライバシーなし（(v3) Authentication, No Privacy） • （v3）認証、プライバシー（(v3) Authentication, Privacy） • （v2c）通知（(v2c) Notification）
SNMP（v3）認証 アルゴリズム *（Algorithm*）	SNMP v3 に限ります。次の認証アルゴリズムから選択します。 • MD5：メッセージ ダイジェスト アルゴリズム 5 • SHA：セキュア ハッシュ アルゴリズム
SNMP（v3）認証 [パスワード（Password）]	SNMP v3 に限ります。Cisco TelePresence System に関連付けられた SNMP サーバへのアクセス権を取得するために使用されるパスワード。デフォルトのパスワードは **snmppassword** です。 • 最大フィールド長は 32 文字です。 • 最小フィールド長は 8 文字です。 **（注）**　各アルゴリズムにプライバシー パスワードと認証パスワードが必要です。
SNMP（v3）プライバシー アルゴリズム *（SNMP (v3) Privacy Algorithm*）	SNMP v3 に限ります。次のプライバシー アルゴリズムから選択します。 • AES：高度暗号化規格 • DES：データ暗号規格
SNMP（v3）プライバシー パスワード（SNMP (v3) Privacy Password）	SNMP v3 に限ります。デフォルトのパスワードは **snmppassword1** です。 • 最大フィールド長は 32 文字です。 • 最小フィールド長は 8 文字です。 **（注）**　各アルゴリズムにプライバシー パスワードと認証パスワードが必要です。
SNMP（v2c）コミュニティ ストリング *（SNMP(v2c) Community String*）	トラップ レシーバでサポートされるコミュニティ ストリング。このフィールドは、SNMP v2c だけで使用されます。 デフォルトは communityString です。最大長：64

（注）　追加の SNMP トラップを指定するには、追加用フィールドを使用します（[2 SNMP（v3）トラップ レシーバ アドレス（2 SNMP (v3) Trap Receiver Address）]、[3 SNMP（v3）トラップ レシーバ アドレス（3 SNMP (v3) Trap Receiver Address）]、[4 SNMP（v3）トラップ レシーバ アドレス（4 SNMP (v3) Trap Receiver Address）]、[5 SNMP（v3）トラップ レシーバ アドレス（5 SNMP (v3) Trap Receiver Address）]）。最大 5 つの SNMP トラップ レシーバーを指定できます。

設定の保存

[電話の設定（Phone Configuration）] ウィンドウでのパラメータの変更が完了したら、[保存（Save）] をクリックし、次に [設定の適用（Apply Config）] をクリックします。[設定情報の適用（Apply Configuration Information）] ウィンドウが開き、選択したデバイス名が表示されます。

（注）　続行する前に設定を保存する必要があります。[設定の適用（Apply Config）] をクリックすると、デバイスが再起動し、すべてのコールがドロップされます。

Cisco TelePresence の機能の設定

改訂日：2015 年 6 月 17 日

目次

ディレクトリ機能の有効化

Cisco TelePresence Touch 10 の [ディレクトリ（Directory）] ボタンを使用すると、同僚の TelePresence 電話番号を調べることができます。

この機能をサポートするには、社内ディレクトリを設定する必要があります。詳細については、使用している Unified CM のリリースに応じた『*Cisco Unified Communications Manager Administration Guide*』で、「LDAP System Setup」、「LDAP Directory Setup」、および「LDAP Authentication Setup」の項を参照してください。

Cisco Unified Communications Manager の管理インターフェイスから、次の手順でユーザのディレクトリを設定します。

ステップ 1 Cisco Unified Communications Manager 管理インターフェイスにログインします。

ステップ 2 [システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）] に移動します。

ステップ 3 [セルフ ケア ポータル（Self Care Portal）] までスクロールします。

ステップ 4 リストで [ディレクトリ検索の許可（Allow Directory Search）] を検索し、ドロップダウン メニューから [True]（デフォルト設定）を選択します。

ステップ 5 [保存（Save）] をクリックして設定を保存します。変更は、次回 Cisco Unified Communications Manager の [ユーザオプション（User Options）] ウィンドウにログインしたときに適用されます。

BFCP over UDP Collaboration 機能の設定

Binary Floor Control Protocol（BFCP）は、会議のメディア リソースへのアクセス制御に使用されます。BFCP を使用すると、IX システムおよびリモート エンドポイントで、プレゼンテーションとメイン ディスプレイのビデオを同時に表示できます。また、一部のサードパーティ製 TelePresence エンドポイントもサポートされます。

IX システムは 3 つのメディア回線を備えています。1 つはオーディオ用、もう 1 つはメイン ビデオ用、残りの 1 つは、セッション記述プロトコル（SDP）を使用するプレゼンテーションまたはコンテンツ用です。また、アプリケーション回線が BFCP コントロール チャネルの SDP で送信されます。

プレゼンテーションのメディア回線の帯域幅は IX システムの機能に対応しています。たとえば、IX システムが 1 秒あたり 30 フレーム（fps）で最大 1080p レートに設定されている場合、プレゼンテーションのメディア回線の帯域幅は 4 Mbps になります。

IX システムは、セキュアと非セキュアの両方の BFCP モードで、ユーザ データグラム プロトコル（UDP）を介して BFCP を使用します。

従来のイマーシブ エンドポイントと BFCP との互換性

BFCP は、CTS Release 1.8 以降のすべての Cisco TelePresence イマーシブ エンドポイントでデフォルトで有効になります。CTS Release 1.8 以前の CTS ソフトウェアを使用しているエンドポイントの場合は、[Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスですべての新規 SIP プロファイルに対して BFCP を無効化するか、すべての CTS エンドポイントを CTS Release 1.8 にアップグレードする必要があります。

次の順序でシステムを設定します。

1. 「BFCP を使用するための VCS の設定」（P.2-2）
2. 「BFCP を使用するための Unified CM の設定」（P.2-3）

BFCP を使用するための VCS の設定

Cisco VCS で BFCP を有効にするには、次の手順を実行します。

- Cisco VCS 管理インターフェイスで [VCS ゾーン（VCS Zone）] のパラメータを変更します。
- Cisco Unified Communications Manager の管理インターフェイスで、Cisco VCS と Unified CM 間のトランクにカスタム BFCP プロファイルを追加します。

次の手順を実行する前に、Video Communication Server（VCS）と Unified CM を動作可能にしておく必要があります。

Cisco VCS 設定のサポートと情報について詳しくは、使用している VCS ソフトウェアのリリースに応じた『*Cisco VCS and CUCM Deployment Guide*』を参照してください。

Cisco VCS のゾーン設定を変更するには、次の手順を実行します。

ステップ 1　管理（admin）ユーザとして VCS にログインします。

ステップ 2　[設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）] に移動します。

ステップ 3　ゾーンのハイパーリンクをクリックして、IX システムを登録する Unified CM サーバのゾーンを選択します。

ステップ 4　[詳細設定（Advanced）] 領域で、ドロップダウン リストから [Cisco Unified Communications Manager（8.6.1 以降）（Cisco Unified Communications Manager (8.6.1 or later)）] を選択します。

ステップ 5　[保存（Save）] をクリックします。

BFCP を使用するための Unified CM の設定

ここでは、Unified CM 向けに BFCP を設定する手順と以下のトピックについて説明します。

新しい BFCP プロファイルの追加

BFCP の新しいプロファイルを追加するには、この項の手順を実行します。

（注）　プレゼンテーションに BFCP を使用するすべてのトランクとデバイスに、このプロファイルを関連付けます。デバイスに対して BFCP を有効にするには、[デバイス（Device）] > [電話（Phone）] に移動してデバイスを選択し、「[プロトコル固有情報（Protocol-Specific Information）] 領域」セクション（1-20 ページ）の [BFCP を使用するプレゼンテーション共有を許可（Allow Presentation Sharing using BFCP）] チェックボックスをオンにします。

ステップ 1　[デバイス（Device）] > [デバイスの設定（Device Settings）] > [SIP プロファイル（SIP Profile）] の順に移動します。

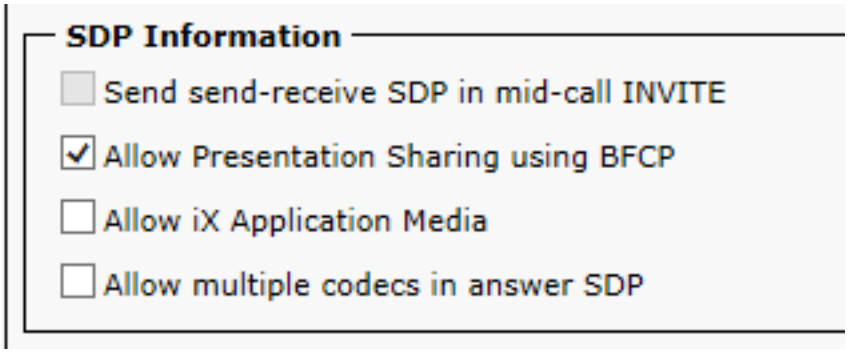
ステップ 2　[新規追加（Add New）] をクリックします。[SIP プロファイルの設定（SIP Profile Configuration）] ウィンドウが表示されます。

ステップ 3　セキュリティ プロファイルの名前を作成します。たとえば、「Standard BFCP SIP Profile」など。

ステップ 4　[SDP 情報（SDP Information）] 領域で、[BFCP を使用するプレゼンテーション共有を許可（Allow Presentation Sharing using BFCP）] チェックボックスをクリックしてオンにします（図 2-1 を参照）。

（注）　2 つの [SDP プロファイル（SDP Profile）] 領域があります。ページの下部にある 2 番目の領域に移動します。

図 2-1　[SDP 情報（SDP Information）] - [BFCP を使用するプレゼンテーション共有を許可（Allow Presentation Sharing using BFCP）]



ステップ 5　残りのフィールドはデフォルトのままにします。

ステップ 6　[保存（Save）] をクリックして、[設定を適用（Apply Config）] をクリックします。

ステップ 7　「Unified CM トランクの設定」セクション（2-4 ページ）のタスクを実行して BFCP トランクを設定します。

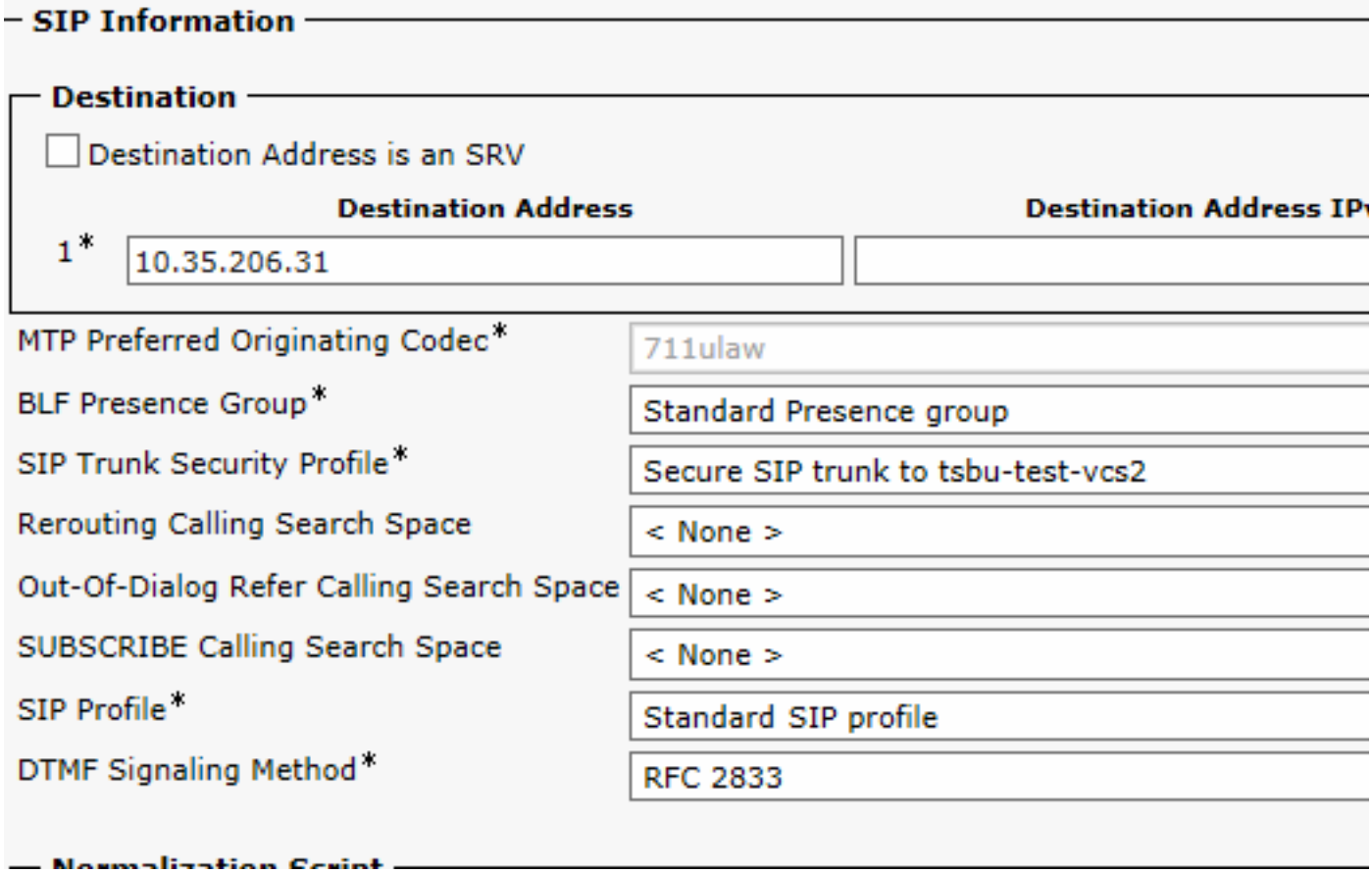
Unified CM トランクの設定

ステップ 1　[デバイス（Device）] > [トランク（Trunk）] に移動します。

ステップ 2　[名前（Name）] 領域でハイパーリンクをクリックして、SIP トランクを選択します。

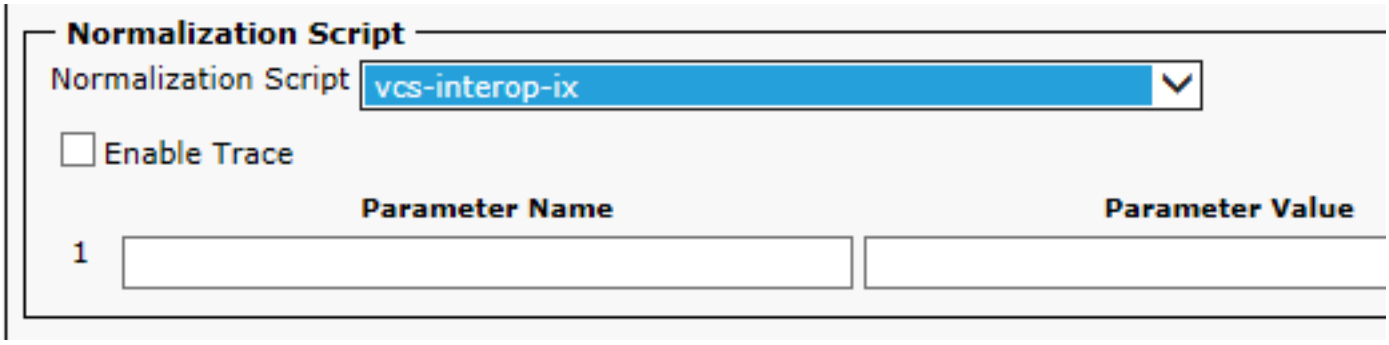
ステップ 3　[SIP 情報（SIP Information）] 領域で、[SDP プロファイル（SDP Profile）] フィールドを変更し、「新しい BFCP プロファイルの追加」セクション（2-3 ページ）で作成したトランクを使用するように設定します。図 2-2 では、[SDP プロファイル（SDP Profile）] フィールドで Standard BFCP SIP Profile が選択されています。

図 2-2　　BFCP プロファイルの選択



ステップ 4　（任意）[正規化スクリプト（Normalization Script）] ウィンドウで [vcs-interop-ix] を選択し、EX および C シリーズのエンドポイント用に、Unified CM と Cisco VCS 間にセキュリティを設定します（図 2-3 を参照）。

図 2-3　　[正規化スクリプト（Normalization Script）] ウィンドウ - VCS の相互運用セキュリティ



ステップ 5　[保存（Save）] をクリックして設定を保存します。

ステップ 6　適切な時間帯に、[リセット（Reset）] をクリックしてトランクをリセットし、新しい BFCP の設定を適用します。

注意　[リセット（Reset）] をクリックすると、このトランクで行われているコールがすべて切断されます。この手順はコール アクティビティが少ない時間帯に実行してください。

単一セグメントのミュート化

（注）　この機能は今後の IX 8 リリースから利用可能になります。

緑色の LED ライトが消えるまで、[ミュート（Mute）] ボタンを 3 秒間押し続けることで、1 つのマイク バーをミュート化できます。マイクがミュート化されます（ミュート化された [マイク（Microphone）] アイコンはメイン画面に表示されません）。ローカルにミュート化されたマイクをミュート解除するには、[ミュート（Mute）] ボタンを 1 回押します。緑色の LED ライトが点灯し、マイクが再びアクティブになります（会議室がすでにミュート化されている場合はミュートになります）。

（注）　任意のテーブル マイクで [ミュート（Mute）] ボタンを 1 回押すことで、引き続き会議室をグローバルにミュート化できます。

単一のマイク バーのミュート化を有効にするには、Cisco Unified Communications Manager の管理インターフェイスにログインし、[プロダクト固有の設定（Product Specific Configuration）] 領域に移動して、[シングル マイクロフォン ミュートを有効にする（Enable Single Microphone Mute）] チェックボックスをオンにします。この機能は、デフォルトではディセーブルになっています。

Touch 10 画面のグレー表示

電力を節約し、Cisco TelePresence Touch 10 デバイスの寿命を延ばすために、Touch 10 は [プロダクト固有の設定（Product Specific Configuration Layout）] で指定された時間数だけグレー表示になります（[ディスプレイ点灯時刻（Display On Time）] と [ディスプレイ点灯継続時間（Display On Duration）] フィールドで指定）。詳細については、「[プロダクト固有の設定（Product Specific Configuration Layout）] 領域」セクション（1-24 ページ）を参照してください。

グレー表示がアクティブな場合は、画面がグレー表示になり、ホーム ボタンが点灯しています。Touch 10 またはそのハード ボタンのいずれかに触れると、デバイスが再びオンになります。デバイスは、システムがアイドル状態になるまで 1 時間オンの状態を維持します。その時間が経過すると、画面は再びグレー表示になります。

システムがコール中、録音中、またはトラブルシューティング中の場合、画面は指定された時間どおりにグレー表示になりません。コールの着信時やポップアップ通知の表示時、またはアップグレードが開始されたとき、画面は自動的に再開されます。

IX システムの設定の確認とトラブルシューティング

改訂日：2015 年 6 月 17 日

目次

ここでは、IX と Unified CM の設定を確認する方法について説明します。

設定のトラブルシューティング

設定をトラブルシューティングするには、表 3-1 の情報を使用します。

はじめる前に

まず、次の条件が満たされていることを確認します。

- Cisco TelePresence System のアセンブリ ガイドに従って、Cisco TelePresence System がインストールされ、設定されていること。
- 本書の説明に従って、Unified CM が IX をサポートするように設定されていること。
- Web UI から IP アドレスを使用してエンドポイントにアクセスできること。

Unified CM サーバの接続のテスト

次の手順を実行して、Unified CM サーバ間の通信が正常かどうかをテストできます。

ステップ 1 セキュア シェル（SSH）を使用して、ユーザ **admin** で CLI セッションを作成します。デフォルトのパスワードは **cisco** です。

ステップ 2 **utils network ping** {*X*} コマンドを入力します。ここで、*X* は Unified CM の IP アドレスまたは DNS 名です。コマンドの結果、パケット損失が 0% である場合、ネットワークは正常に機能しています。パケット損失が発生している場合は、ネットワークに問題がないか確認します。

表 3-1　Cisco TelePresence の設定のトラブルシューティング

問題	考えられる原因	解決策
システムがアップグレードされない。	• システムが Cisco Unified CM TFTP サーバからアップグレード ファイルを検索またはダウンロードできない。 • AutoUpgrade が False に設定されている。	1. Unified CM の [デバイス（Device）] に正しいアップグレード ファイル名が設定されていることを確認します。 2. COP ファイルが TFTP サーバにアップロードされていることを確認します。 3. アップグレード ファイルのアップロード後に TFTP サービスが再起動されていることを確認します。 4. アップグレード ファイルがある TFTP サーバを IX システムが正しく参照していることを確認します。 5. AutoUpgrade を **True** に設定します。現在の設定内容を確認するには、次の CLI コマンドを入力します。 **show upgrade det** AutoUpgrade が False に設定されている場合は、True に再設定します。支援が必要な場合は、TAC に連絡してください。 CLI コマンドの詳細については、『Command Reference for Cisco TelePresence Immersive Systems』も参照してください
IX システムが別の Unified CM に移動されており、登録が拒否される。	**CTL ファイルの問題** システムが別のセキュアな Unified CM に関連付けられていたときの証明書信頼リスト（CTL）ファイルが残っている。	[Cisco Unified CM の管理（Cisco Unified CM Administration）] の管理インターフェイスを使用して古い CTL ファイルを削除します。

表 3-1　Cisco TelePresence の設定のトラブルシューティング （続き）

問題	考えられる原因	解決策
IX システムが Unified CM に登録されない。 • Unified CM のデバイス ページで、システムのステータスが未登録または不明と表示される。 • コーデック Web ユーザ インターフェイス（UI）で、システムのステータスが Unified CM に対して不明またはアクセス不可と表示される。	**IX が認識されない問題** IX システムが不明と表示される場合： • 入力されている MAC アドレスが正しくない。 • Cisco Unified CM がシステムを認識していない。 • システムのケーブルが抜けているために登録されない。 **プロファイルまたはプロビジョニングの問題** • システム プロファイルが Cisco Unified CM で適切にプロビジョニングされていない。 **電話番号の問題** • 電話番号（DN）が設定されていない。	• 次の手順で電話機の登録を確認します。 – [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスにログインします。 – IP アドレスをクリックし、電話機の登録を確認します。 • Unified CM にログインし、システム プロファイルと電話番号（DN）が適切に作成され、設定されていることを確認します。 • システムの MAC アドレスが Unified CM に正しく入力されていることを確認します。 • 証明書信頼リスト（CTL）がシステム上に存在していないことを確認し、存在している場合は削除します。確認するには、初期システム起動後に、IP アドレス（デフォルトのユーザ名とパスワードは、**admin / cisco**）を使用して IX システムの管理 GUI にログインし、[設定（Configuration）] > [コール コントロール マネージャ（Call Control Manager）] に移動して、[証明書信頼リストを削除（Delete Certificate Trust List）] をクリックします。詳細については、『*Administration Guide for Cisco TelePresence Software Release IX 8*』で、「Understanding the Fields In the Interface」の項の「Certificates」を参照してください。 **（注）** ブラウザによっては、[設定（Configuration）] ページに直接移動できません。問題がある場合は、[モニタリング（Monitoring）] をクリックしてから [設定（Configuration）] をクリックしてください。 変更を実行した後、初回セットアップを開始する前に、cisco.com から最新の IX ソフトウェア バージョンをロードして、IX システムにロードする必要があります。 • 関連する DN を含めてシステムを Unified CM から完全に削除してから、システムを再び Unified CM に追加します。 **ヒント** Unified CM のデバイス ページ（[説明（Description）] フィールドなど）で小さな変更を行った場合でも、必ず [保存（Save）] をクリックし、システムを再起動してください。

表 3-1　Cisco TelePresence の設定のトラブルシューティング（続き）

問題	考えられる原因	解決策
IX システムが Unified CM に登録されない（続き）	**TFTP の問題** • Unified CM または TFTP サービスの問題。 • TFTP ポート 6970 がブロックされているため、IX システムが Unified CM TFTP サーバから「デバイス コンフィギュレーション xml」ファイルをダウンロードできない。 **XML の問題** • XML コンフィギュレーション ファイルが Unified CM データベースで破損している可能性がある。	• Unified CM と TFTP サービスが実行していることを確認します。必要に応じて、サービスを再起動します。 • Cisco Unified CM とシステム間に 6970 ポートをブロックしているファイアウォールやデバイスがないことを確認します。
	ホスト名の問題 • Unified CM のホスト名を解決できない。	システムで TFTP サーバとして Unified CM のホスト名を使用している場合は、ホスト名がドメイン ネーム システム（DNS）によって解決できることを確認します。
Touch システムが開始されない。 システムが登録解除されることがある。	**スイッチの問題** • テーブルのスイッチが正しく初期化されていない。	『*IX5000 and IX5200 First-Time Setup*』の「Resetting the Table Switch to Fix Issues with Touch 10 Devices」の項の説明に従って、適切なブートシーケンスを実行する必要があります。
	Touch 10 の問題 • システムを初めて初期化したときに Touch 10 の接続が早すぎた。	『*IX5000 and IX5200 First-Time Setup*』の「Preventing Touch 10 Configuration Issues」の項の説明に従って、Touch 10 接続シーケンスを実行します。
システムが登録解除されることがある。	**SIP の問題** • システムで SIP 登録タイムアウトが発生した。 **ネットワークの問題** • 断続的なネットワークの問題によって、パケットがドロップされた可能性がある。	1. Unified CM が SIP メッセージを受信しているかどうか、およびシステムが応答しているかどうかを確認します。 2. 必要に応じて、パケット キャプチャを収集してシスコの技術担当者に提出し、詳しい検査を依頼します。

表 3-1　Cisco TelePresence の設定のトラブルシューティング（続き）

問題	考えられる原因	解決策
Touch 10 デバイスが認識されないか使用できない。	**COP ファイルの問題** • イメージ ファイルがインストールされていない、または適切にインストールされていない。 **デバイス情報の問題** • Unified CM での電話機ロード名に誤りがある。	• ファイルを再インストールします。手順については「COP ファイルの追加と設定」セクション（ 1-1 ページ）を参照してください。 • Unified CM で正しい電話ロード名を入力します。 – Unified CM にログインし、[デバイス（Device）] > [電話（Phone）] に移動します。 – デバイスの検索条件を入力し、[デバイス名（Device Name）] の下にあるハイパーリンクをクリックして [デバイス情報（Device Information）] ページを表示します。 – 正しい電話ロード名を入力します。 • デバイス パックを再インストールします。
システムまたは Touch 10 で時間が正確に表示されない。	ネットワーク タイム プロトコル（NTP）が正しく設定されていない、またはコーデックが NTP と同期していない。	1. NTP が設定されていない場合は、Cisco Unified CM の日時グループにアクセスし、NTP を正しく設定してシステム デバイス プールに割り当てます。 2. システムが NTP を ping できること、および 123 NTP ポートをブロックしているファイアウォールがないことを確認します。

パスワードの管理

以下の項には、パスワードの管理に役立つ情報が記載されています。

- 「Unified CM セキュア シェル パスワードのリセット」（P.3-5）
- 「IX システムのコーデック パスワードのリセット」（P.3-6）
- 「関連情報」（P.3-9）

Unified CM セキュア シェル パスワードのリセット

セキュア シェル パスワードをリセットするには、次の手順を実行します。

ステップ 1　[Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスにログインします。

ステップ 2　[デバイス（Device）] > [電話（Phone）] の順に移動します。[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 3　特定の電話機を検索するには、検索条件を入力して [検索（Find）] をクリックします。

ステップ 4　[デバイス名（Device Name）] の下にあるハイパーリンクをクリックし、[プロダクト固有の設定（Product Specific Configuration Layout）] 領域 まで下にスクロールします。

ステップ 5　設定の保存 まで下にスクロールします。

ステップ 6　次のガイドラインに従ってパスワードを変更します。

- 最大フィールド長：64 文字
- 最小フィールド長：6 文字

ステップ 7　[SSH 管理期間（SSH admin Life）] で、0 ～ 365 の数値を入力します。この値によってパスワードの時間パラメータを指定します。

- 0 を指定すると、パスワードは無期限になります。
- 365 を指定すると、パスワードは 365 日後に期限切れになります。

ステップ 8　[リスタート（Restart）] をクリックして変更を保存します。これにより、更新された設定が読み込まれてシステムに適用され、コール サービスが再起動されます。または、[リセット（Reset）] をクリックして、システムをリブートします。起動時に、システムは Cisco Unified CM の設定を読み取り、変更を適用します。

パスワード エージングの詳細については、「設定の保存」セクション（ 1-36 ページ）を参照してください。

IX システムのコーデック パスワードのリセット

（注）　メイン ディスプレイに表示される、最近要求されたパスコードを読み込むには、実際に会議室にいる必要があります。

pwrecovery アカウントの入力が必要なあらゆる段階で、プログラムは最大 60 秒間待機します。何も入力しないと、入力に時間がかかりすぎたため終了したことが Cisco TelePresence システムにより通知されます。

問題が発生した場合は、http://tools.cisco.com/ServiceRequestTool/create/ [英語] にアクセスして Technical Assistance Center（TAC）で問題を調べるか、シスコのテクニカル サポートに問い合わせて、担当者に問題について収集した情報を提出してください。

はじめる前に

システムがコール中でないこと、およびパスワードのリセットが試みられた事例が 1 回だけであることを確認します。これを行わないと、システムが中断します。

手順

システムのコーデック パスワードをリセットするには、次の手順を実行します。

ステップ 1　ラップトップからコーデックに SSH 接続します。

ステップ 2　次の資格情報でログインします。

- ユーザ名：**pwrecovery**
- パスワード：**pwreset**

次のメッセージが、SSH クライアント ウィンドウに表示されます。

例 3-1　パスワードのリセットへようこそ

```
dhcp-249:~ $ ssh pwrecovery@10.00.00.100
pwrecovery@10.00.00.100's password:

**********************************************************************
**********************************************************************
**                                                                  **
**      パスワードのリセットへようこそ（Welcome to password reset）       **
**                                                                  **
**********************************************************************
**********************************************************************

続行しますか（Do you want to continue ?）（はい / いいえ）：はい（(y/n):y）
システムを準備しています…（Preparing the system...）
パスコードを入力してください：（Please enter the passcode:）
```

ステップ 3　続行するかどうか確認を求められます。**Y** を入力し、次に Return を押して続行します。

（注）　終了する場合は、他のキーを入力してから、Return を押します。

このシステムでパスワードをリセットする準備が整い、パスコードを求められます。次のように、新しいパスコードがシステムのメイン ディスプレイに表示されます。

パスワードのリセットは実行中です（Password reset is now being run）

パスコード：919175（Passcode: 919175）

（注）　パスコードはランダムに生成される番号で、各ログイン試行ごとに異なります。不正なパスコードを入力すると、次の例に示すように、パスコードが間違っているため終了する旨がシステムにより通知されます。この場合は、上記のステップ 1 とステップ 2 を繰り返します。

例 3-2　無効なパスワード リセット要求

```
続行しますか（Do you want to continue ?）（はい / いいえ）：はい（(y/n):y）
システムを準備しています…（Preparing the system...）
パスコードを入力してください：12345（Please enter the passcode:12345）
それは無効なパスコードです（Sorry that was an invalid passcode...）
ログオフします（Logging off）
10.00.00.100 への接続が閉じられました。（Connection to 10.00.00.100 closed.）
dhcp-249:~ $
```

正しいパスコードを入力すると、システムは管理アカウント名とパスワードをシステム デフォルトにリセットします。次に、正常なパスワード リセット情報の例を示します。

例 3-3　正常なパスワード リセット要求

```
パスコードを入力してください：507530（Please enter the passcode:507530）
管理者名とパスワードをリセットします（resetting admin name and password）
既存の管理セッションを停止します（stopping any existing admin session）
管理者アカウントとパスワードをデフォルトにリセットします（admin account and password reset to default）
セキュリティルールの適用に成功しました（success in applying security rules）
ログオフします（Logging off）
10.00.00.100 への接続が閉じられました。（Connection to 10.00.00.100 closed.）
dhcp-249:~ $
```

（注）　Cisco Unified Communications Manager でシステムを使用している場合は、次回 Unified CM から「更新」または「リセット」を実行したときに、管理アカウント名とパスワードが Unified CM のデバイス ページで指定した値に再設定されます。

IX システムのリセットと同期

次の項には、以下のシステム コンポーネントの管理に関する情報が記載されています。

- 「IX システムのリセット」（P.3-8）
- 「IX システムの同期」（P.3-8）
- 「コーデックとの接続の回復」（P.3-9）

IX システムのリセット

デバイスが Cisco Unified Communications Manager に登録されていない場合は、リセットまたはリスタートできません。デバイスが登録されている場合、シャットダウンせずにデバイスをリスタートするには、[リスタート（Restart）] ボタンをクリックします。デバイスをシャットダウンして起動するには、[リセット（Reset）] ボタンをクリックします。デバイスをリセットまたはリスタートせずに前のウィンドウに戻るには、[閉じる（Close）] をクリックします。

IX システムの同期

電話機を最新の変更と同期させるには、次の手順を実行します。この手順は、最小限の割り込みで未適用の設定を適用します。（たとえば、影響を受けるデバイスでのリセットや再起動が不要です）。

手順

ステップ 1　[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　使用する検索条件を選択し、[検索（Find）] をクリックします。検索条件に一致する電話の一覧がウィンドウに表示されます。

ステップ 3　同期させる電話機の横にあるチェックボックスをオンにします。ウィンドウ内のすべての電話機を選択するには、一致するレコードのタイトル バーのチェックボックスをオンにします。

ステップ 4　[選択項目への設定の適用（Apply Config to Selected）] をクリックします。[設定情報の適用（Apply Configuration Information）] ダイアログが表示されます。

ステップ 5　[OK] をクリックします。

コーデックとの接続の回復

IX システムのコーデックとの接続が失われた場合は、PDU をオフにしてシステムの電源を切り、その後、各スイッチを **On** に切り替えてシステムの電源をオンにします。接続が自動的に回復します。

電源遮断の手順については、『*Field-Replaceable Units and Country- and Region-Specific Power Connectors*』の「Replacing the Camera」の項を参照してください。

インストールに関する完全なマニュアル セットは、次の URL にあります。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/ix5000-series/products-installation-guides-list.html

関連情報

システム パスワードの詳細や、Cisco TelePresence System と Cisco Unified CM の管理インターフェイスおよび関連ハードウェア コンポーネントのトラブルシューティンの詳細については、『Cisco TelePresence System Troubleshooting Guide』を参照してください。

B

C

I

M

S

T

U

V

W

し

せ

そ

た

て

は

ふ

ほ

も

ろ