



第 4 章

IX システムの設定

作成日：2014 年 12 月
改訂日：2015 年 4 月 6 日

目次

この章は、次の項で構成されています。

- 「IX System の Cisco Unified Communications Manager の設定」 (P.4-1)
- 「初回セットアップ」 (P.4-2)
- 「ネットワーク設定 (Network Settings)」 (P.4-3)
- 「Call Control Manager の設定」 (P.4-4)
- 「証明書の設定」 (P.4-5)
- 「設定のトラブルシューティング」 (P.4-7)
- 「IX コーデック パスワードのリセット」 (P.4-7)
- 「IX システム コンポーネントのトラブルシューティング」 (P.4-9)

IX System の Cisco Unified Communications Manager の設定

IX システムを使用する前に、Cisco Unified Communications Manager (Unified CM) でシステムを設定する必要があります。

Unified CM で IX システムを設定する前に、システムを設定してこの章の手順をすべて完了できますが、デバイスを登録するまでは次の操作を完了できません。

- Unified CM から Touch デバイス ソフトウェアをダウンロードできず、ログにエラーメッセージが表示されます。
- Touch デバイスは電話をかけた受けたりできません。

Unified CM でデバイスを設定するには、次の手順を実行します。

■ 初回セットアップ

- ステップ 1 Unified CM サーバに Cisco TelePresence Administration Software のイメージをロードします。詳細については、「IX システムの即時ソフトウェア アップグレードの要件」(P.-vii) および「Unified CM デバイスパックの要件」(P.-viii) を参照してください。
- ステップ 2 Unified CM で、システムをデバイスとして登録します。詳細については、『Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System』の「Configuring a Cisco TelePresence Device」の項を参照してください。
- ステップ 3 TelePresence IX5000 管理者インターフェイスを使用して、お使いの Unified CM サーバ用の TFTP サーバをシステムに追加します。詳細については、使用しているソフトウェア リリースに対応する『Cisco TelePresence System Administration Guide』の「Cisco Unified Communications Manager Settings」を参照してください。

Cisco TelePresence デバイスを使用した Unified CM の設定の詳細については、『Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System』を参照してください。

初回セットアップ

管理者ユーザ インターフェイスに初めてログインするときは、すぐに [初回セットアップ (First Time Setup)] 領域に移動して IX システムをセットアップする必要があります。

図 4-1 [初回セットアップ (First Time Setup)] セクション



初回セットアップ手順の完全な説明と設定手順については、次の URL の『IX5000 and IX5200 First-Time Setup』のドキュメントを参照してください。

http://www.cisco.com/c/en/us/td/docs/telepresence/ix5000/first_time_setup/ix5000_first_time_setup.html [英語]

ネットワーク設定 (Network Settings)

[ネットワーク (Network)] 領域には、Cisco TelePresence IX システムのネットワーク アドレッシング情報が表示されます。次のネットワーク設定を表示し、管理できます。

- DHCP : ネットワークで DHCP が使用されている場合は、[フル (Full)] または [混合 (Mixed)] を選択します。
 - フルモードでは、DHCP ですべてのネットワーク値 (IP アドレス、サブネット、ゲートウェイ、DNS サーバ、ドメイン) を割り当てることができます。
 - 混合モードでは、ユーザがシステムに静的 IP を割り当てることができ、DHCP はその他すべてのネットワーク値を割り当てます。
- ネットワークで DHCP を使用していない場合は、すべての IP アドレス値を手動で割り当てるように [スタティック (Static)] を選択します。
- IP アドレス (IP Address)
- サブネット
- ゲートウェイ
- DNS サーバ (1 と 2)

IP 設定を表示および管理するには、次の手順を実行します。

ステップ 1 [設定 (Configuration)] > [ネットワーク (Network)] を選択します。[ネットワーク (Network)] 領域が [図 4-2](#) (DHCP) や [図 4-3](#) (DHCP なし) のように表示されます。

図 4-2 [設定 (Configuration)] > [ネットワーク (Network)] セクション: (DHCP) [フル (Full)]

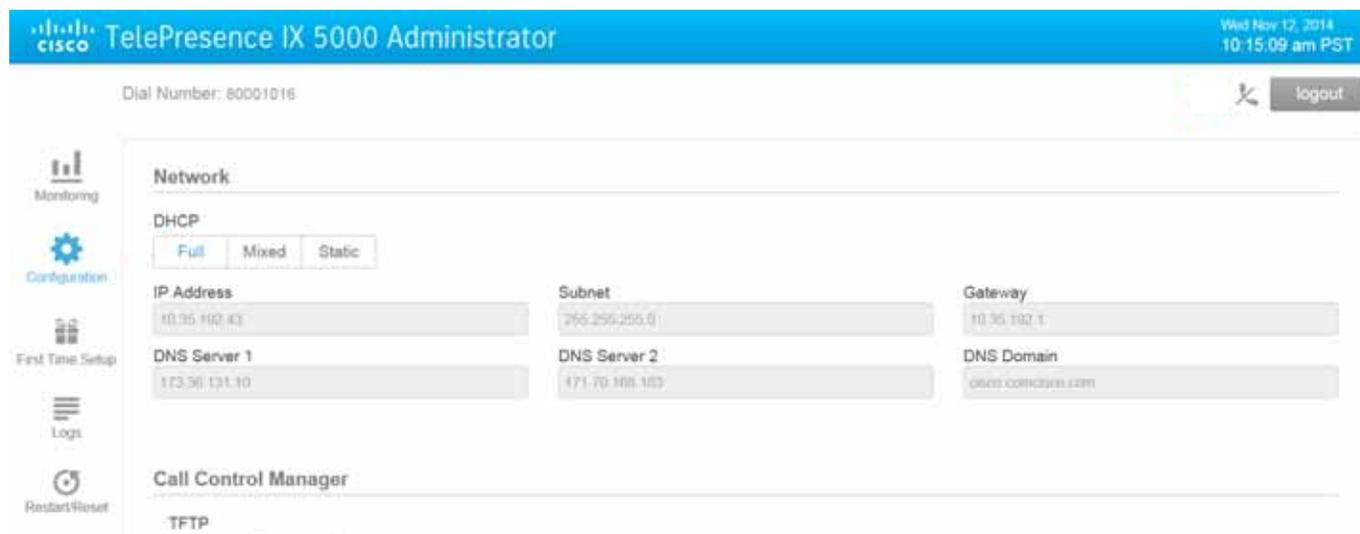


図 4-3 [設定 (Configuration)] > [ネットワーク (Network)] セクション: (DHCP なし) [スタティック (Static)]

ステップ 2 ネットワークに Cisco TelePresence System アップリンクを設定します。Cisco TelePresence System は次の方法で設定できます。

- フル/ピュア ダイナミック：DHCP を使用してすべての設定を決定します。
- スタティック/ピュア スタティック：スタティック設定を使用してすべての設定を決定します。
- 混合/ハイブリッド：IP アドレスにはスタティック設定を使用しますが、残りの設定は DHCP を使用して決定します。



ヒント

[設定 (Configuration)] > [ネットワーク (Network)] フィールドに変更を加えると、ページの下部にある [再起動 (Restart)] および [適用 (Apply)] ボタンがアクティブになります。

ステップ 3 元の設定に戻すには、[再起動 (Restart)] をクリックします。

ステップ 4 新しい設定または変更した設定を登録するには、[適用 (Apply)] をクリックします。



(注)

リセットを完了させるには、システム上のすべてのコーデックが接続されイネーブルになっている必要があります。デバイスを登録するには、『[Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System](#)』の「Optional Hardware」の項を参照してください。

Call Control Manager の設定

TFTP サーバの場所を指定し、Cisco TelePresence IX システムに使用可能な設定のリストを表示するには、次の手順を実行します。

ステップ 1 [設定 (Configuration)] を選択し、図 4-4 に示す [Call Control Manager] セクションまでスクロールします。

図 4-4 [設定 (Configuration)] > [Call Control Manager] セクション

ステップ 2 Unified CM TFTP サーバを設定します。



(注) [TFTPサーバ (TFTP Server)] フィールドのいずれかに新しい値を入力しても変更が持続しない場合は、[証明書信頼リストの削除 (Delete Certificate Trust List)] ボタンをクリックして証明書信頼リスト (CTL) を削除してから TFTP サーバ情報を再度入力します。

[設定 (Configuration)] ページの下部にある [リセット (Reset)] および [適用 (Apply)] ボタンは、[TFTPサーバ (TFTP Server)] フィールドに値が入力されるとアクティブになります。

ステップ 3 新しい設定または変更した設定を登録するには [適用 (Apply)] をクリックし、元の設定に戻すには [リセット (Reset)] をクリックします。



(注) リセットを完了させるには、システム上のすべてのコーデックが接続されイネーブルになっている必要があります。デバイスを登録するには、『[Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System](#)』の「Optional Hardware」と「Troubleshooting the Cisco TelePresence Configuration」の項を参照してください。

証明書の設定

[証明書 (Certificates)] 領域では、IX システムの 802.1X 認証をセットアップします。ここでは、802.1X 認証をセットアップするための次の項目を含む手順について説明します。

- [セキュリティ証明書を使用した IX システムの認証](#)
- [IX システムのセキュリティ証明書の検証](#)



(注) 802.1X 認証を完了するには、802.1X に対しまだ有効になっていないポートを使用する必要があります。

セキュリティ証明書を使用したIXシステムの認証

Cisco TelePresence IX システムはオーセンティケータから認証チャレンジを受信すると、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) を使用して応答します。MIC と LSC の両方がインストールされている場合は、システムは LSC を使用して認証を行います。LSC がインストールされていない場合は、Cisco TelePresence System は MIC を使用します。MIC は製造元でシステムに組み込まれています。認証の詳細については、「[802.1X 認証](#)」(P.3-13) を参照してください。

LSC では、各システムに固有の公開キー インフラストラクチャ (PKI) が作成されるため、LSC のほうがセキュリティにおいて優れています。LSC を使用してコーデックを認証するには、Unified CM の認証局プロキシ機能 (CAPF) を使用して LSC をシステムに手でインストールする必要があります。詳細については、[LSC のインストール](#) を参照してください。

LSC のインストール

LSC をインストールするには、[設定 (Configuration)] > [証明書 (Certificates)] に移動し、[証明書 (Certificate)] フィールドの情報を参照してください。

IXシステムのセキュリティ証明書の検証

証明書が有効で期限切れでなく CAPF によって発行されていることを確認するために、802.1X 認証されたシステムでセキュリティ証明書 (MIC または LSC) を調べることができます。

IX システムのセキュリティ証明書を検証するには、次の 2 つの方法のいずれかを使用して証明書のコピーを自分のシステムにダウンロードします。

- [CLI を使用したセキュリティ証明書のダウンロード](#)
- [管理者インターフェイスを使用したセキュリティ証明書のダウンロード](#)

CLI を使用したセキュリティ証明書のダウンロード

CLI を使用して MIC または LSC をダウンロードするには、次の手順を実行します。

- ステップ 1 CLI にログインします。
- ステップ 2 次のコマンドを入力します。 **file get cert** {cert-type} {SCP-user} {SCP-password} {IP-address-or-hostname} {file-save-location}

構文の説明については、[表 4-1](#) を参照してください。

表 4-1 構文の説明

引数	説明
<i>cert-type</i>	取得する証明書のタイプ (MIC または LSC)
<i>SCP-user</i>	セキュア コピー (SCP) ユーザのユーザ名
<i>SCP-password</i>	SCP ユーザのパスワード
<i>IP-address-or-hostname</i>	ターゲット システムのホスト名または IP アドレス
<i>file-save-location</i>	ターゲット システム上のファイルを保存する場所

コマンドの入力時に取得する証明書のタイプとして MIC を選択した場合は、セキュリティ証明書はターゲットシステムの指定されたファイル保存場所に保存します。

```
file get cert MIC username password 10.1.1.1 /home/user
Uploading MIC to 10.1.1.1...DONE
```

取得する証明書のタイプとして LSC を選択したが、LSC が Cisco TelePresence System にインストールされていない場合は、コマンドラインは次のようになります。

```
admin:file get cert LSC username password 10.1.1.1 /home/user
Uploading LSC to 10.1.1.1...LSC does not exist
Executed command unsuccessfully
```

LSC コマンドが失敗した場合は、コーデックに LSC をインストールする必要があります。[LSC のインストール](#)を参照してください。コマンドが正常に実行されたら、次のステップに進みます。

ステップ 3 指定したファイル保存場所に移動し、証明書を表示するファイルをクリックします。

管理者インターフェイスを使用したセキュリティ証明書のダウンロード

管理者インターフェイスから MIC または LSC をダウンロードするには、次の手順を実行します。

- ステップ 1** 管理者インターフェイスにログインし、[設定 (Configuration)] > [証明書 (Certificates)] に移動します。
- ステップ 2** 証明書の列の右側にある [ダウンロード (Download)] をクリックし、証明書をダウンロードして表示します。[ダウンロード (Download)] ボタンが選択不可の場合は、証明書が付与されていないことを示します。

設定のトラブルシューティング

設定のトラブルシューティングの詳細については、『[Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System](#)』の「[Troubleshooting Your Configuration](#)」の項を参照してください。

IX コーデック パスワードのリセット

この項には、Cisco TelePresence IX システムでのパスワード問題の管理とトラブルシューティングに関する情報が含まれます。



(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ワードを読み込むには、Cisco TelePresence 会議室にいる必要があります。

pwrecovery アカウントが入力を要求するあらゆる段階で、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、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

IX システムがコール中でないことと、誰かがパスワードをリセットしようとした事例が 1 つあることを確認します。次のいずれかの条件がある場合、セッションは中断されます。

コードブックパスワードは通常、Unified CM から設定されます。Unified CM が使用できずパスワードが不明の場合は、次の手順を実行します。

手順

IX システムのコードブ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 セキュア シェル (SSH) または他の安全なホストクライアントを使用して、Cisco TelePresence System GUI にログインします。

ステップ 2 次の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 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 システムによって続行するかどうか尋ねられます。**Y** を入力し、次に **return** を入力して続行します。



(注) 必要に応じて、他のキーを入力し、終了するには **return** を入力します。

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。新しいパスコードは IX システムのメインディスプレイに表示されます (次の例を参照)。

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。不正なパスワードを入力すると、次の例に示すように、パスワ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 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...)
パスワードを入力してください : 12345 (Please enter the passcode:12345)
それは無効なパスワードです (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:~ $
```

正しいパスワードを入力すると、IX 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。



(注) 画面の右上に以前のデフォルト以外のユーザ名がまだ表示されている場合があります。このユーザ名は使用せず、デフォルトのユーザ名とパスワードを引き続き使用してください。

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 正常なパスワードリセット要求

```
パスワ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) Unified CM で IX 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」を実行すると、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 コンポーネントのトラブルシューティング

IX システム コンポーネントのトラブルシューティングに関する詳細については、この管理ガイドの「[初回セットアップ](#)」の項を参照してください。

