クイック スタート ガイド

Cisco Prime Collaboration Manager 1.1（Cisco Prime CM）クイック スタート ガイド

【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。

2 このマニュアルについて
3 製品概要
4 主な機能
5 Cisco Prime CM のライセンスについて
6 Cisco Prime CM のインストール
7 Cisco Prime CM 1.0 から 1.1 への移行
8 ネットワーク上のデバイスのセットアップ
9 はじめに
10 ナビゲーションおよびマニュアルの参照先
11 Cisco Prime CM のアンインストール

改訂日：2012 年 1 月 9 日、OL-25429-01-J

SUPPLEMENTAL LICENSE AGREEMENT FOR CISCO SYSTEMS NETWORK MANAGEMENT SOFTWARE: CISCO PRIME COLLABORATION MANAGER

IMPORTANT-READ CAREFULLY: This Supplemental License Agreement (“SLA”) contains additional limitations on the license to the Software provided to Customer under the End User License Agreement between Customer and Cisco. Capitalized terms used in this SLA and not otherwise defined herein shall have the meanings assigned to them in the End User License Agreement. To the extent that there is a conflict among any of these terms and conditions applicable to the Software, the terms and conditions in this SLA shall take precedence. By installing, downloading, accessing or otherwise using the Software, Customer agrees to be bound by the terms of this SLA. If Customer does not agree to the terms of this SLA, Customer may not install, download or otherwise use the Software.

ADDITIONAL LICENSE RESTRICTIONS:

- Installation and Use. The Software components are provided to Customer solely to install, update, supplement, or replace existing functionality of the applicable Network Management Software product. Customer may install and use the following Software components:
  - Cisco Prime Collaboration Manager: May be installed on a server in Customer's network management environment. For each Software license granted, customers may install and run the Software on a single server to manage the number of endpoints by category as specified in the license file provided with the Software, or as specified in the Software License Claim Certificate. Customers whose requirements exceed the license unit limits must purchase upgrade licenses or additional copies of the Software. The license unit limits are enforced by license registration.
- Reproduction and Distribution. Customers may not reproduce nor distribute the Software.

DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

Please refer to the Cisco Systems, Inc. End User License Agreement.

1 新機能および変更情報

次の表は、『Cisco Prime Collaboration Manager 1.1 クイック スタート ガイド』の初期リリース後に追加または変更された情報を示します。

日付	リビジョン	場所
2012 年 1 月 9 日	• LDAP サーバのグループに作成されたユーザ用の有効なメールボックスを設定するための情報を追加しました。 • Cisco TMS Third Party Booking API ユーザの設定手順を更新しました。	• 「Reporting API for CTS-Manager 1.8 の設定」（P.18） • 「Cisco TMS Third Party Booking API ユーザの設定」（P.18）
2011 年 12 月 16 日	設定手順用に『CPCM 1.1 Deployment Guide』への参照を追加しました。	「ネットワーク上のデバイスのセットアップ」（P.14）
2011 年 12 月 15 日	サポートされる Cisco C および EX シリーズのソフトウェアバージョンとして 5.0 を追加しました。	表 7：「デバイスのクレデンシャルおよびソフトウェア バージョン」

日付	リビジョン	場所
2011 年 11 月 30 日	• ネットワーク上のデバイスのセットアップに関する注意事項を更新しました。 • Cisco Prime CM の起動手順を更新しました。 • SSL 証明書の警告を削除する項を追加しました。	• 「ネットワーク上のデバイスのセットアップ」（P.14） • 「はじめに」（P.20） • 「SSL 証明書の警告の削除」（P.22）
2011 年 10 月 31 日	最初のバージョン	

2 このマニュアルについて

このマニュアルでは、仮想化サーバに Cisco Prime Collaboration Manager Release 1.1 をインストールする方法を説明します。

このマニュアルは、Cisco TelePresence System の設定、監視、およびメンテナンスと、起こり得る問題のトラブルシューティングを担当する管理者を対象としています。これらの管理者は、次のビデオ コラボレーション アプリケーションに精通していなければなりません。

- 管理アプリケーション：Cisco TelePresence Manager アプリケーション（CTS-Manager）および Cisco TelePresence Management System（TMS）。
- コールおよびセッション制御：Cisco Unified Communication Manager（Cisco Unified CM）および Cisco TelePresence Video Communication Server（Cisco VCS）。
- 会議アプリケーション：Cisco Telepresence Multipoint Switch（CTMS）、Cisco TelePresence Server（TS）、および Multipoint Control Units（MCU）、および Cisco Telepresence Media Service Engine（MSE）。

管理者は、仮想化の概念と仮想化環境についても理解しておく必要があります。

Cisco Prime CM の設定と管理の詳細については、『*Cisco Prime Collaboration Manager 1.1 User Guide*』を参照してください。

3 製品概要

Cisco Prime CM は、監視、トラブルシューティング、およびレポートを支援するビデオ サービス保証および管理システムです。このシステムは、サービスおよびネットワーク オペレータに、進行中のすべての Cisco TelePresence セッションを統合したリアルタイムのビューを提供します。

Cisco Prime CM は、各セッションの関連付けられたメディア パスをすぐに表示し、問題の原因を隔離します。Mediatrace 対応デバイスがネットワークに導入されている場合、Cisco Prime CM は、ネットワーク パスを可視化し、ビデオ フロー統計情報の詳細を示します。

Cisco Prime CM：

- タイムリーなエンドツーエンド可視性をサポートし、セッション、エンドポイントおよびネットワークのビデオ関連の問題を隔離します。
- サービスに影響を与える問題をトラブルシューティングし回復するまでの時間を短縮します。
- 重要な傷害およびパフォーマンス統計情報によりメディア パスの詳細な分析を提供します。これにより、サービス低下の原因となるネットワーク デバイスを隔離できます。
- Cisco TelePresence エンドポイントおよびサービスとネットワークのインフラストラクチャ デバイスの包括的なインベントリ、状態、ステータスを介して、大規模な導入を検証します。
- オペレータが使用率および問題履歴を追跡できるレポートを配信します。

4 主な機能

表 1 に、Cisco Prime CM の主な機能の詳細を示します。

表 1　　Cisco Prime CM 主な機能

機能	動作	利点
ビデオ コラボレーション サマリー ダッシュボード	• ビジネスに影響するメトリックの要約（使用率、問題領域）。 • ひと目で確認できる、すべてのビデオ コラボレーション リソースの状態と使用率のステータス。 • 日次、週次、および月次ビュー。 • データを CSV 形式にエクスポートする機能。	• 実行中のセッション、エンドポイント、サービス インフラストラクチャ デバイスに影響を与える問題の詳細を、すぐに簡単に参照できます。 • 空間およびエンドポイント モデルの使用率における傾向を表示することによって、最適なリソースの割り当てを支援します。 • システム コンポーネントの低下を瞬時に可視化することにより、システム稼動時間の向上を支援します。
セッション モニタリング	• 進行中のセッション、最近完了したセッション、およびスケジュールされているセッションのトポロジとステータスを可視化します。 • Cisco TelePresence セッション（スケジュール、アドホック、スタティック）およびエンドポイントの重要な傷害およびパフォーマンス メトリックを提供します。	• セッション モニタリングおよびトラブルシューティングの運用コストを削減します。 • 最も重要なセッションと、最も重要な問題のあるセッションを識別します。 • 問題がエンドポイントにあるか、ネットワークにあるかを判別します。
エンドポイントおよびネットワークの診断	• エンドツーエンド ビューを表示します。これらのビューには、エンドポイント、サービス インフラストラクチャ、およびネットワーク デバイスの詳細が含まれます。これらの診断では、欠陥の可能性があるエンドポイントも強調表示されます。 • ネットワーク パスを可視化します。Medianet 対応デバイスがネットワークに導入されている場合、ビデオ フロー統計情報の詳細を示します。	• トラブルシューティングを簡素化し、ビデオ品質に影響を与える根本的な原因を識別する時間を短縮します。 • ビデオ関連問題の平均修復時間を短縮します。
エンドポイント ダッシュボード	Cisco TelePresence エンドポイントのアラーム、状態の統計情報、およびスケジューリング ステータスのトラッキングを可能にします。 エンドポイントが現在セッションにない場合でも、この機能を使用できます。	• 対処する最も重要な問題があるエンドポイントを評価するのに必要な時間を短縮します。 • エンドポイント スケジューリング ステータスは、サービス オペレータが、解決する問題の優先順位を付けるのに役立ちます。

表 1　　Cisco Prime CM 主な機能（続き）

機能	動作	利点
インベントリ	導入されているすべての Cisco TelePresence エンドポイントを検出し、インベントリを作成するのに役立ちます。 また、関連するサービスおよびネットワーク インフラストラクチャ デバイスを検出してインベントリを作成し、ソフトウェア バージョンおよびすべてのデバイスのステータスを識別するのに役立ちます。	• ソフトウェア アップグレードの検証に必要な運営チーム リソースを軽減します。 • 大規模なビデオ コラボレーション導入で、素早い管理性および包括的なインベントリ詳細を提供します。
レポート	• Cisco TelePresence の導入に関する重要な情報を表示します。 • トラブルシューティング時のエンドポイントおよびネットワーク診断に関するレポートを作成します。	• エンドポイント使用率履歴の詳細なアセスメントに基づく新しいエンドポイントの導入の計画を改善できます。 • 将来の導入について最適な場所とデバイス タイプを判断するのに役立ちます。 • 将来の破壊を防ぐためのデータおよび対応する傾向の分析に役に立ちます。 • 特定の Cisco TelePresence エンドポイントおよびインフラストラクチャ システムの ROI を簡単に計算するのに役立ちます。
障害管理	• エンドポイントおよびネットワーク レベルでセッションに関する重要な障害メトリックを提供します。 • パケット損失、ジッター、遅延、CPU、およびメモリのしきい値をカスタマイズできます。 • イベントおよびイベント重大度のモニタリングをカスタマイズできます。 • サービスに影響する停止の通知を設定できます。	• 問題が発生した場合に、エンドユーザに予防的なサポートとタイムリーなサポートを提供するのに役立ちます。 • 特定のアラーム検出および通知を管理できます。

Cisco Prime CM の機能の詳細については、『*Cisco Prime Collaboration Manager 1.1 User Guide*』を参照してください。

5　Cisco Prime CM のライセンスについて

Cisco Prime CM は、エンドポイント タイプに基づいてライセンスを提供します。エンドポイントのタイプによって、ネットワークを管理するために購入する必要のあるライセンス ユニットの数が決定します。Cisco Prime CM は基本ライセンスと、次に示す 3 つの単一エンドポイント タイプのライセンスを提供します。

- マルチコーデック エンドポイント
- ハイエンド コーデック エンドポイント
- ミッドレンジ コーデック エンドポイント

表 2 に、エンドポイント タイプとライセンス ユニット数のマッピングを示します。

表 2　　エンドポイント タイプとライセンス ユニット

単一エンドポイント タイプのライセンス	エンドポイント タイプ	ライセンス ユニットの数
マルチコーデック エンドポイント	Cisco TelePresence System 3000	300
	Cisco TelePresence System 3010	300
	Cisco TelePresence System 3200	300
	Cisco TelePresence System 3210	300
ハイエンド シングルコーデック エンドポイント	Cisco TelePresence System 500	100
	Cisco TelePresence System 1000	100
	Cisco TelePresence System 1100	100
	Cisco TelePresence System 1300	100
	Cisco TelePresence System 1400	100
	Cisco Profile 52 デュアル	100
	Cisco Profile 52	100
	Cisco Profile 65	100
	Cisco Profile 65 デュアル	100
	Cisco Profile 52-6000MXP	100
	Cisco Codec C90	100
ミッドレンジ シングルコード エンドポイント	Cisco Codec EX60	40
	Cisco Codec EX90	40
	Cisco Codec C60	40
	Cisco Codec C40	40
	Cisco Codec C20	40
	Cisco Profile 42 C20	40
	Cisco Profile 42 C60	40

最初に、Cisco.com の「Network Management Evaluation Products」のリストから、Cisco Prime CM の評価バージョンをダウンロードする必要があります。

Cisco Prime CM は、ライセンス ユニット計算ツールを提供します。このツールを使用して、エンドポイントの管理に必要なライセンス ユニットの数を計算できます。ライセンス ユニット計算ツールの詳細については、『*Cisco Prime Collaboration Manager 1.1 User Guide*』（「Managing Licenses」の項）を参照してください。

評価ライセンスは、5000 ユニットを表します。このライセンスを使用して、最大で次のいずれか 1 つを管理できます。

- 16 個のマルチコーデック エンドポイント
- 50 個のハイエンド シングルコーデック エンドポイント
- 125 個のミッドレンジ シングルコーデック エンドポイント

評価ライセンスは、90 日間使用できます。Cisco Prime CM は、ライセンス ユニット数がサポート限度の 90 % に達すると、通知メッセージを表示します。

次の状況では、評価コピーを基本ライセンスにアップグレードする必要があります。

- 90 日の評価期間が満了する前。
- ライセンス ユニット数が最大限度に達してから 15 日以内。

Cisco Prime CM のライセンスには、ソフトウェアベースの製品登録とライセンス キー アクティベーション技術が組み込まれています。

製品にライセンスを付与するには、次の手順を実行します。

ステップ 1 製品認証キー（PAK）およびライセンス ファイルを取得します。「PAK の入手」と「ライセンス ファイルの入手」を参照してください。

ステップ 2 Cisco Prime CM をインストールした後で、ライセンス ファイルを追加します。ライセンス ファイルの追加については、『*Cisco Prime Collaboration Manager 1.1 User Guide*』を参照してください。

PAK の入手

PAK は、ソフトウェア権利証明書に記載されています。eDelivery システムを介して権利証明書を取得できます。eDelivery については、http://www.cisco.com/web/partners/tools/edelivery.html を参照してください。

ライセンス ファイルの入手

ライセンス ファイルを取得するには、各 Cisco Prime CM サーバで生成される PAK および汎用固有識別子（UUID）を使用して、Cisco.com で Cisco Prime CM 製品を登録する必要があります。UUID は、Cisco Prime CM 評価バージョンをインストールすると、サーバに自動的に生成されます。Cisco Prime CM の [About] ページから、UUID を取得できます。ライセンス ファイルを生成する場合は、この値を指定する必要があります。

ライセンス ファイルは、次の場所に生成できます。

http://www.cisco.com/go/license

ライセンス ファイルを取得した後は、ライセンスを Cisco Prime CM に追加する必要があります。ライセンス ファイルの追加については、『*Cisco Prime Collaboration Manager 1.1 User Guide*』を参照してください。ライセンス ファイルを追加すると、評価ライセンスが自動的に、購入した永続ライセンス タイプに変換されます。

6 Cisco Prime CM のインストール

Cisco Prime CM は、Open Virtual Appliance（OVA）ファイルとして提供されます。OVA を使用することで、事前にパッケージ化された仮想マシン（VM）を容易に導入できます。

はじめる前に

次のことを確認しておく必要があります。

- OVA が、vSphere クライアントのインストール先と同じマシンにダウンロードされ、保存されている。
- VMware ESXi が ESXi ホストにインストールされ、設定されている。ホスト マシンのセットアップと設定については、VMware のマニュアルを参照してください。
- VMware ESXi ホストに、設定されている IP 情報（アドレス、ネットワーク マスク、およびゲートウェイ）を使用して到達できる。
- VMware vSphere Client がインストールされている。ネットワークで仮想ホストが使用可能になった後、その IP アドレスを参照して、VMware vSphere Client をインストールできる Web ベース インターフェイスを表示できます。

（注） VMware vSphere Client は Windows ベースです。したがって、このクライアントは Windows PC からダウンロードし、インストールする必要があります。

VMware vSphere Client をインストールしたら、このクライアントを実行して、仮想ホストのホスト名または IP アドレス、ルート ログイン ID、および設定したパスワードを使用して仮想ホストにログインできます。vCenter を介して管理する場合は、ホストを vCenter に追加できます。詳細は、VMware のマニュアルを参照してください。

- VMware ESXi サーバ ホスト名が、DNS サーバに設定されている。
- VMware ESXi サーバが、NTP サーバと同期している。

ネットワーク内のデバイスのセットアップについては、「ネットワーク上のデバイスのセットアップ」（P.14）を参照してください。

システム要件

Cisco Prime CM 1.1 は、ESXi 4.1 がインストールされた VMware 認定ハードウェアで動作します。Cisco Prime CM は、64 ビット マシンにインストールする必要があります。

（注） VMware 認定の Cisco Unified Computing System（UCS）に Cisco Prime CM をインストールし、実行することを推奨します。

OVA は、CPU、メモリ、ディスク、およびネットワーク リソースを含む仮想マシンの設定を定義します。

仮想マシン要件

表 3 に、Cisco Prime CM で管理されるエンドポイント数に基づいた仮想マシンの要件を示します。

表 3　　仮想マシン要件

Cisco Prime CM で管理されるエンドポイント	CPU	RAM	NIC	ディスク容量
最大 1000 個のエンドポイント	4	8 GB	1 GB	90 GB
1000 個を超えるエンドポイント	4	16 GB	1 GB	90 GB

（注） デフォルトでは、Cisco Prime CM 1.1 の OVA ファイルは、最大 1000 個のエンドポイントをサポートするように設定されます。1000 個を超えるエンドポイントをサポートするように OVA ファイルを編集する方法については、VMware のマニュアルを参照してください。

クライアント マシン要件

一度に最大 10 人の同時ユーザが Cisco Prime CM アプリケーションにログインできます。

表 4 に、Cisco Prime CM 1.1 アプリケーションを効果的に使用するためのクライアント マシン要件を示します。

表 4　　クライアント マシン要件

パラメータ	要件
ディスプレイ解像度	1024 x 768 以上
サポートされるブラウザ	次のブラウザがサポートされます。 • Mozilla Firefox 4.0 および 5.0（Linux、Mac、および Windows） • Windows Internet Explorer 8.0 および 9.0 Cisco Prime CM は、自己署名証明書（HTTPS）を提供します。Cisco Prime CM クライアントのアクセスを可能にするには、Internet Explorer ブラウザでセキュリティが中または低に設定されていることを確認する必要があります。 **（注）** • ブラウザで cookie を有効にしていることを確認します。 • ブラウザで言語として [English (United States) [en-us]] を設定していることを確認します。
Adobe Flash Player	Cisco Prime CM の機能を正しく動作させるには、クライアント マシンに Adobe Floash Player をインストールする必要があります。Adobe Web サイトから Adobe Flash Player バージョン 10.x をダウンロードし、インストールすることを推奨します。

サポートされるポート

表 5 に、Cisco Prime CM で使用されるポートの詳細を示します。

表 5　　使用されるポート

ポート	プロトコル	方向	使用方法
22	TCP	単方向：サーバからエンドポイントへ。	トラブルシューティング プロセス時にエンドポイントへの SSH 接続を開始する。
		単方向：クライアントからサーバへ。	Cisco Prime CM サーバに接続する。
23	TCP	双方向：サーバから Medianet 対応デバイスへ。	トラブルシューティング プロセス時に Medianet 有効デバイスへの Telnet 接続を開始する。
25	TCP	単方向：サーバから SMTP サーバへ。	SMTP
53	TCP	単方向：サーバから DNS サーバへ。	DNS
80	TCP	双方向：クライアントからサーバへ。	ブラウザから Cisco Prime CM へのアクセス（HTTP）。
		双方向：サーバから Medianet 対応デバイスへ。	トラブルシューティング プロセス時に Medianet 有効デバイスへの HTTP 接続を開始する。
161	UDP	単方向：サーバからネットワーク デバイスへ。	SNMP MIB ポーリング
162	UDP	双方向：エンドポイントからサーバへ。	トラップ レシーバ ポート。
		双方向：CM とトラップ レシーバ。	SNMP トラップを送信する。
443	TCP	双方向：クライアントからサーバへ。	セキュア ブラウザから Cisco Prime CM へのアクセス（HTTPS）。
		双方向：サーバからコールおよびセッション制御へ。	RTMT および Cisco Unified CM の登録と Cisco VCS 用の HTTPS 接続。
		双方向：サーバからマルチポイント スイッチおよび管理アプリケーションへ。	CTMS、CTS-Manager、および TMS への HTTPS 接続。
20514	UDP	単方向：エンドポイントからサーバへ。	syslog レシーバ ポート。
8886	TCP	単方向：Cisco VCS から Cisco Prime CM へ。	VCS over HTTP からフィードバック / 通知を受信する。
8888	TCP	単方向：Cisco VCS から Cisco Prime CM へ。	VCS over HTTPS からフィードバック / 通知を受信する。

OVA の導入

すべてのシステム要件を満たしていることを確認します。「はじめる前に」（P.7）および「システム要件」（P.8）の項を参照してください。

OVA を導入するには、次の手順を実行します。

ステップ 1 VMware vSphere Client を起動します。

ステップ 2 [File] > [Deploy OVF Template] を選択します。

[Deploy OVF Template] ウィンドウが表示されます。

ステップ 3 [Deploy from file] オプション ボタンをクリックします。

ステップ 4 [Browse] をクリックして、OVA ファイルを保存した場所にアクセスします。

ステップ 5 [Next] をクリックします。

[OVF Template Details] ウィンドウに、OVF テンプレートの詳細が表示されます。

ステップ 6 製品名、バージョン、およびサイズを含む OVA ファイルの詳細を確認して、[Next] をクリックします。

[Name and Location] ウィンドウが表示されます。

ステップ 7 導入するテンプレートの名前と場所を指定します。名前はインベントリ フォルダ内で固有である必要があり、最大 80 文字で構成できます。

ステップ 8 [Next] をクリックします。

[Disk Format] ウィンドウが表示されます。

ステップ 9 仮想ディスクを保存する形式を指定するには、次のいずれかのオプション ボタンをクリックします。

- **Thin provisioned format**
- **Thick provisioned format**

[Thin provisioned format] オプション ボタンをクリックすることを推奨します。

ステップ 10 [Next] をクリックします。

[Ready to Complete] ウィンドウが表示されます。このウィンドウには、OVA ファイルの詳細、仮想アプライアンスの名前、サイズ、ホスト、ディスク形式、およびストレージの詳細が表示されます。

ステップ 11 オプションを確認したら、[Finish] をクリックして導入を開始します。

このタスクが完了するまで数分かかります。[Deploying Virtual Application] ウィンドウの経過表示バーをチェックして、タスクのステータスをモニタします。

導入タスクが正常に完了すると、確認ウィンドウが表示されます。

ステップ 12 [Close] をクリックします。

導入した仮想アプライアンスが、vSphere クライアントの左側のペインで、ホストの下に表示されます。

仮想アプライアンスの設定

Cisco Prime CM OVA を展開した後、仮想アプライアンスを設定する必要があります。

次の手順に従います。

ステップ 1 仮想マシンの電源をオンにします。これには、仮想アプライアンスを右クリックし、[Power] > [Power On] を選択します。

仮想アプライアンス コンソールが表示されます。

ステップ 2 ローカルホスト ログイン プロンプトで、**`setup`** と入力します。

ステップ 3 コンソール プロンプトで、次のパラメータを入力します。

- [IP Address] : 仮想アプライアンスの IP アドレス。
- [IP default netmask] : IP アドレスのデフォルト サブネット マスク。

- [IP default gateway] : デフォルト ゲートウェイの IP アドレス。
- [Default DNS domain] : デフォルトのドメイン名。
- [Primary nameserver] : プライマリ ネーム サーバ。このネーム サーバは、追加または編集できます。複数のネーム サーバまたは NTP サーバを設定するには、**y** と入力します。
- [Primary NTP server[time.nist.gov]] : プライマリ NTP サーバ。
- [Timezone] : Cisco Prime CM サーバに設定された時間帯。
- [Username] : 最初の管理ユーザの名前。デフォルトの admin を受け入れることができます。

（注） 管理ユーザ名として **cmuser** を使用しないでください。**cmuser** は事前に設定された Cisco Prime CM CLI ユーザなので、この名前を使用すると問題が発生するおそれがあります。

- [Password] : パスワードを入力して、確認します。

（注） 管理パスワードを書き留めておくことを推奨します。このパスワードは、取得またはリセットできません。

[End User License Agreement] が表示されるまでに、数分かかります。

[End User License Agreement] が表示されます。

ステップ 4 ライセンス契約書を確認し、これに同意するには **y** と入力します。

仮想マシンが再起動します。

ステップ 5 Cisco Prime CM アプリケーションにログインして、機能しているかどうかを調べます。「はじめに」（P.20）を参照してください。

Cisco Prime CM のインストールのトラブルシューティング

Cisco Prime CM アプリケーションを起動できない場合は、必要なプロセスが Cisco Prime CM 1.1 サーバで実行されていない可能性があります。

これをチェックするには、次の手順を実行します。

ステップ 1 SSH サービスを使用して、OVA の設定時に作成したユーザで Cisco Prime CM 1.1 サーバにログインします。デフォルトでは、ユーザ名は *admin* です。

ステップ 2 次のコマンドを入力して、実行中のプロセスを表示します。

```
show application status emsam
```

次に、status コマンドの出力例を示します。

```
STAT   PID USER     COMMAND             ELAPSED
================================================
S<l  16583 root     Decap_main       7-22:30:28
Sl   17268 cmuser   emsam_diag       7-22:30:00
Sl   17233 root     emsam_fault      7-22:30:00
Sl   16587 root     emsam_mq         7-22:30:28
Sl   16844 root     emsam_poller     7-22:30:20
Sl    7261 root     emsam_tomcat     7-16:12:11
Ss   16730 oracle   oracle           7-22:30:27
Ssl  16629 oracle   tnslsnr          7-22:30:28
```

[COMMAND] 列のパラメータが、Cisco Prime CM 1.1 サーバで実行中のプロセスです。

これらのプロセスがすべて実行中であることがわからない場合は、次のコマンドを入力して Cisco Prime CM サービスを再起動します。

```
application stop emsam
```

```
application start emsam
```

ステップ 3　ステップ 2 を繰り返して、すべてのプロセスが実行中かどうかをチェックします。

必要なすべてのプロセスがまだ Cisco Prime CM 1.1 サーバで実行されていない場合は、シスコ サポート チームに問い合わせてください。

7 Cisco Prime CM 1.0 から 1.1 への移行

移行プロセスにより、Cisco Prime CM 1.0 設定データが抽出され、Cisco Prime CM 1.1 にインポートされます。

設定されているすべてのデータが、Cisco Prime CM 1.0 から 1.1 に移行されます。デバイス、セッション、およびライセンス ファイルは移行されません。

（注）　Cisco Prime CM 1.0 および Cisco Prime CM 1.1 は、異なる VM サーバに導入する必要があります。移行を行うには、シスコ サポート チームに問い合わせてください。

移行プロセスが完了した後は、必ずデバイスを再検出し、セッションをインポートしてください。

表 6 に、Cisco Prime CM 1.0 から 1.1 に移行される設定データの詳細を示します。

表 6　Cisco Prime CM 1.0 から 1.1 に移行される設定データ

設定データ	Cisco Prime CM 内のナビゲーション	移行後に必要な設定
デバイス アクセス クレデンシャル	[Inventory] > [Device Inventory] > [Manage Credentials]	デバイス タイプをインポートしたクレデンシャル プロファイルに更新し、デバイスを再検出します。
ユーザ アカウント	[Administration] > [User Management]	Cisco Prime CM 1.1 で必要な追加設定はありません。
デバイス モニタリングの設定	[Administration] > [Device Monitoring Configuration]	• 次の新規ビデオ コラボレーション デバイスに対するポーリング間隔： – エンドポイント：C および Ex シリーズ エンドポイント。 – 管理アプリケーション：Cisco TelePresence Multipoint Switch。 – コールおよびセッション制御：Cisco Video Communication Server。 – 会議アプリケーション：Cisco TelePresence Server、Cisco TelePresence Multipoint Control Units（MCU）、および Cisco TelePresence Media Service Engine（MSE）。 • ネットワーク デバイスの CPU 使用率およびメモリ使用率のしきい値。 • Cisco Mediatrace 有効デバイスの [Rx Packet Loss]、[Average Period Jitter]、および [DSCP] のしきい値。

表 6　Cisco Prime CM 1.0 から 1.1 に移行される設定データ（続き）

設定データ	Cisco Prime CM 内のナビゲーション	移行後に必要な設定
システム設定	[Administration] > [System Configuration]	• [Month-to-Month Endpoint Utilization and No Show Reports] チェックボックスをオンにして、集約月次レポートを受信します。 • Cisco Prime NAM を使用してネットワークを管理している場合は、Cisco Prime NAM デバイスを追加するかインポートします。 • Cisco Prime LMS を使用してネットワークを管理している場合は、Cisco Prime LMS サーバの詳細を追加します。 • 外部ツールを使用してトラップを管理している場合は、アラームおよびイベントのトラップ レシーバを設定します。
ユーザ設定	[Administration] > [User Preference Configuration]	Cisco Prime CM 1.1 で必要な追加設定はありません。

8 ネットワーク上のデバイスのセットアップ

Cisco Prime CM でエンドポイント、アプリケーション マネージャ、コール プロセッサ、マルチポイント スイッチ、およびネットワーク デバイスを管理するには、まず、それらのデバイスに次のクレデンシャルを設定する必要があります。

- HTTP：システム ステータスと会議情報をポーリングするために、HTTP を介してデバイスにアクセスします。
- SNMP read コミュニティ ストリングおよび SNMP 認証プロトコル（SNMP V2 または SNMP V3）：デバイスの検出および管理を行います。
- CLI：トラブルシューティング目的でメディア パスを検出するために、CLI を介してデバイスにアクセスします。
- JTAPI：Cisco Unified CM からセッション ステータス情報を取得します。
- CDP：近接デバイスを検出します。

設定手順の詳細については、『*CPCM 1.1 Deployment Guide*』を参照してください。

表 7 に、Cisco Prime CM でデバイスを管理する前に必要とされるデイバスのクレデンシャルとソフトウェア バージョンを示します。

表 7　デバイスのクレデンシャルおよびソフトウェア バージョン

ビデオ コラボレーション アプリケーション	サポートされるソフトウェア バージョン	SNMP	HTTP	CLI	JTAPI	CDP
CTS-Manager	1.7 または 1.8	Yes	Yes	No	No	NA[1]
Cisco Unified CM	8.6	Yes	Yes	No	Yes	NA[1]
Cisco TelePresence Multipoint Switch	1.6.3、1.7、または 1.8	Yes	Yes	No	No	NA[1]

表 7　　デバイスのクレデンシャルおよびソフトウェア バージョン（続き）

ビデオ コラボレーション アプリケーション	サポートされるソフトウェア バージョン	SNMP	HTTP	CLI	JTAPI	CDP
Cisco TelePresence System 500 Cisco TelePresence System 1100 Cisco TelePresence System 1300 Cisco TelePresence System 1400 Cisco TelePresence System 3000 Cisco TelePresence System 3010 Cisco TelePresence System 3200 Cisco TelePresence System 3210	1.6.4、1.7、または 1.8	Yes	No	Yes[2]	No	NA[1]
Cisco TelePresence Management Suite（Cisco TMS）	13.0 または 13.1	Yes	Yes	No	No	—
Cisco TelePresence Video Communication Server（Control と Expressway）	6.0、6.1、または 7.0	Yes	Yes	No	No	—
Cisco TelePresence MCU 4500 シリーズ Cisco MCU MSE 8510	4.1 または 4.2	Yes	Yes[3]	No	No	—
Cisco Telepresence Server 7010 Cisco Telepresence Server MSE 8710	2.1 または 2.2	No	Yes	No	No	—
Cisco Codec EX60 および EX90 Cisco Codec C20、C40、C60、および C90 Cisco Profile 42 C20 および C60 Cisco Profile 52 および Cisco Profile 52 デュアル（C40 と C60） Cisco Profile 65 および Cisco Profile 65 デュアル（C60 と C90）	4.1、4.2、または 5.0	Yes	Yes[3]	Yes[2]	No	—
Cisco MSE 8050（スーパーバイザ）	2.1	Yes	Yes[3]	No	No	—
ネットワーク デバイス（ルータとスイッチ）	—	Yes	No	Yes[4]	No	Yes

1. CDP はデフォルトで有効になっています。
2. このプロトコルの設定には、必須ではありません。
3. Admin 特権が必要です。
4. Medianet 機能を使用する場合は必須です。

ネットワーク上のデバイスのセットアップに関する注意事項

- CTS-Manager、CTMS、Cisco TelePresence System、Cisco Unified CM、Cisco TMS、Cisco TelePresence Server、Cisco VCS（Control と Expressway）、Cisco MCU（アプライアンスと MSE ブレード）、Cisco TelePresence EX シリーズ、Cisco Telepresence System Integrator C シリーズ、Cisco TelePresence System Quick Set C シリーズ、MSE Supervisor、およびネットワーク デバイスには、SNMP 読み取り専用アクセスが必要です。
- Cisco TMS Windows サーバでは、SNMP サービスをイネーブルにする必要があります。
- CTS-Manager および CTMS の場合は、CLI を使用して SNMP をイネーブルにし、設定する必要があります。
- Cisco Unified CM の場合は、Cisco Unified Serviceability ツールを使用して、SNMP をイネーブルにし、設定する必要があります。
- CTS-Manager の Cisco Prime CM アプリケーションには、Live Desk ロールと Reporting API ロールが割り当てられた別個の HTTP ユーザ アカウントを作成する必要があります。admin ユーザ ログイン アカウントは使用しないでください。
- Cisco TMS に作成された HTTP ユーザは、Booking API 自体で生成された Booking API ユーザでなければなりません。このユーザは、Cisco TMS における Admin 特権を持つ必要があります。
- 読み取り専用権限のある List Conferences - All ロールを使用して、Cisco TMS で Cisco Prime CM アプリケーションにユーザ グループを作成する必要があります。
- ソフトウェア バージョン 4.1 で動作する Cisco C シリーズ TelePresence システムの場合、HTTP ユーザ名は小文字にする必要があります。
- HTTP ログイン アクセスには、Cisco TelePresence System の API 特権が必要です。Admin 特権は必要ありません。
- CLI ユーザ アカウントは、Cisco TelePresence System に対する Admin 特権または Helpdesk 特権を持つ必要があります。
- Cisco Unified CM では、HTTP のほかに JTAPI アプリケーション ユーザ アカウントが必要です。このアカウントは、Cisco Unified CM パブリッシャで設定する必要があります。Cisco Unified CM サブスクライバは、Cisco Unified CM パブリッシャと同じ SNMP クレデンシャルを持つ必要があります。
- HTTP ログイン アクセスには、Cisco VCS、Cisco MCU、Cisco TelePresence EX シリーズ、Cisco Telepresence System Integrator C シリーズ、Cisco TelePresence System Quick Set C シリーズ、および Cisco MSE Supervisor に対する Admin 特権が必要です。
- Cisco TelePresence Multipoint Switch には、Diagnostic Technician 特権および Meeting Manager 特権を使用した HTTP ログイン アクセスが必要です。
- Cisco Prime CM は、HTTP プロトコルおよび SNMP プロトコルを使用して非武装地帯（DMZ）にある Cisco VCS Expressway デバイスにアクセスする必要があります。これらのプロトコルがファイアウォールでブロックされている場合、Cisco VCS Expressway デバイスの管理や監視を行うことはできません。
- Cisco TelePresence System で Cisco Prime CM がエンドツーエンドのパス トレース トラブルシューティングを実行する（MTR をトリガーするため）には、CLI ログイン クレデンシャルが必要です。
- Cisco Prime CM は、すべてのデバイスに ping（ICMP）できる必要があります。
- Cisco VCS では、フィードバック イベントに登録できるサーバは 3 台のみです。Cisco VCS フィードバック イベントに登録された Cisco TMS サーバ以外にサーバが存在しないことを確認してください。Cisco Prime CM サーバは、ネットワーク内の Cisco Prime CM サーバによって管理される各 Cisco VCS のフィードバック イベントに対し、サーバの 1 つとして登録されます。

コール プロセッサの設定

すべての CTS エンドポイントが Cisco Unified CM に制御対象デバイスとして追加されている必要があります。それ以外の場合、CTS のコール検出は行われません。

コール プロセッサに HTTP ユーザおよび JTAPI ユーザを設定する必要があります。

HTTP ユーザの作成

次の特権を持つアプリケーション ユーザ（HTTP ユーザ）を作成する必要があります。

- Standard AXL API Access

- Standard CCM Admin Users
- Standard SERVICEABILITY Administration

既存のコール プロセッサ（Cisco Unified CM）スーパー ユーザを使用することもできます。Cisco Unified Operations Manager（CUOM）を使用している場合は、CUOM ユーザを使用できます。

ステップ 1 ユーザ グループ、Standard Cisco Prime CM を作成して、そのグループに次のロールを追加します。

- Standard AXL API Access
- Standard CCM Admin Users
- Standard SERVICEABILITY Administration

ステップ 2 たとえば、**cmuser** ユーザを作成し、このユーザを Standard Cisco Prime CM グループに割り当てます。

ユーザ **cmuser** は、Cisco Prime CM がアプリケーション マネージャから AXL および RIS を使用してエンドポイント情報を取得するために使用されます。

JTAPI ユーザの作成

JTAPI（Java Telephony API）は、デバイスからセッション ステータス情報を取得するのに使用されます。コール プロセッサで、エンドポイントの JTAPI イベントを受信するのに必要な権限を持つ JTAPI ユーザを作成する必要があります。

Cisco Prime CM は、複数のコール プロセッサ クラスタを管理します。セッションの監視は、クラスタ内およびクラスタ間で行われます。クラスタ ID が固有であることを確認する必要があります。クラスタ全体の情報を提供するには、クラスタ パブリッシャにこのユーザを作成する必要があります。

JTAPI はクラスタ全体の情報を提供するので、このアカウントは Cisco Unified CM パブリッシャにのみ設定する必要があります。

ステップ 1 ユーザ名とパスワードを指定したアプリケーション ユーザを作成します。

ステップ 2 すべてのエンドポイント デバイス（Cisco TelePresence コーデックなど）を [Controlled Devices] テーブルに移動します。

ステップ 3 グループに次の権限を割り当てます。

- Standard CTI Allow Call Park Monitoring
- Standard CTI Enabled

ステップ 4 設定を保存します。

次のサービスがアクティブであり、開始されていることを確認します。

- Cisco CTIManager
- Cisco AXL Web Service

アプリケーション ユーザの詳しい設定方法については、*Cisco Unified Communications Manager* のガイドを参照してください。

エンドポイントの設定

CTS の設定時には、仮想 IP アドレスの代わりに、ホットスタンバイ ルータ プロトコル（HSRP）を実行するゲートウェイの実際のインターフェイス IP アドレスを入力することを推奨します。これにより、Cisco Prime CM がトラブルシューティング パスを正確に検出できるようになります。

エンドポイント モニタリングは、SNMP ポーリングに基づきます。必要に応じて、エンドポイントにトラップと syslog を設定できます。トラップと syslog を監視するには、次の作業を行う必要があります。

- コール プロセッサにエンドポイントのトラップおよび syslog レシーバを設定します。

- Cisco Prime CM IP アドレスを入力して、トラップ レシーバを設定します。
- Cisco Prime CM IP アドレスとポート番号 20514 を入力して、syslog レシーバを設定します。syslog は、ソフトウェア バージョン 1.8.0 以上でのみサポートされます。

- エンドポイントがトラップおよび syslog を送信できるようにします。

  トラップの場合：
  - CISCO-TELEPRESENCE-MIB で、[ctpPeripheralErrorNotifyEnable] を true（1）に設定します。
  - CISCO-TELEPRESENCE-CALL-MIB で、[ctpcStatNotifyEnable] を true（1）に設定します。
  - CISCO-TELEPRESENCE-CALL-MIB で、コール統計情報 [ctpcStatMonitoredEntry] のしきい値を設定します。

  syslog の場合：
  - CISCO-SYSLOG-MIB で、[clogNotificationsEnabled] を true（1）に設定します。

Reporting API for CTS-Manager 1.8 の設定

Cisco Prime CM サーバが CTS-Manager 1.8 からデータを取得できるようにするには、CTS-Manager のメトリクス ダッシュボードと Reporting API の有効なライセンスを所有している必要があります。

（注） API のレポート機能の詳細については、http://developer.cisco.com/web/tra/start にある『Getting Started With TelePresence Reporting API』を参照することを推奨します。

Cisco Prime CM サーバが CTS-Manager 1.8 からデータを取得できるようにするには、次の手順を実行します。

ステップ 1 LDAP サーバで、ユーザ グループを作成します。たとえば、`cm_group` という名前のグループを作成します。

ステップ 2 LDAP サーバで作成したグループに、ユーザを作成します。たとえば、`cm_user` という名前のユーザを作成します。

LDAP サーバのグループに作成されたユーザ用に、有効なメールボックスを確実に設定する必要があります。

ステップ 3 CTS-Manager の [Access Management] ページで、LDAP サーバに作成したグループ（ステップ 1 で作成した `cm_group` など）に、Live Desk ロールと Reporting API User ロールを割り当てます。

ステップ 4 LDAP サーバに作成したユーザを使用して、Cisco Prime CM で CTS-Manager を検出します。たとえば、`cm_user` を使用します。

Reporting API の詳細については、『*Cisco TelePresence Manager Reporting API Developer's Guide for Release 1.8*』を参照してください。

LDAP サーバのユーザおよびグループ設定の詳細については、
『*Cisco TelePresence Manager 1.8 Administration and Installation Guide*』を参照してください。

Cisco TMS Third Party Booking API ユーザの設定

Cisco Prime CM サーバで Cisco TMS サーバからデータを取得するには、API を使用するサーバごとにアプリケーション統合ライセンスが 1 つ必要です。

（注） Booking API の詳細については、http://www.tandberg.com/support/tms_documentation.jsp にある Cisco TMS Third Party Booking API のマニュアルを参照することを推奨します。

Cisco Prime CM サーバが Cisco TMS からデータを取得できるようにするには、次の手順を実行します。

ステップ 1 Cisco TMS サーバから、http://localhost/tms/external/booking/remotesetup/remotesetupservice.asmx に移動します。

[RemoteSetupService] ページが表示されます。

（注） 上記の URL にある localhost を Cisco TMS サーバの IP アドレスに置き換えることができます。

ステップ 2 [GenerateConferenceAPIUser] を選択します。

ステップ 3 次のパラメータの値を入力します。

- [userNameBase]：ユーザ名の基本部分。`cm_user` など。
- [encPassword]：新たに作成したユーザに使用する、base64 にエンコードされたパスワード。パスワードを base64 にエンコードするには、http://www.motobit.com/util/base64-decoder-encoder.asp で入手できる Web ユーティリティを使用することを推奨します。
- [emailAddress]：ユーザの電子メール アドレス。このフィールドには、値を入力しないでください。
- [sendNotifications]：ユーザがスケジューリング通知を受信できるようにします。Cisco Prime CM は Cisco TMS からポーリングするので、このフィールドには **`False`** と入力する必要があります。

ステップ 4 [Invoke] をクリックします。

ステップ 5 Cisco TMS アプリケーションで、ステップ 3 で設定したユーザ名が [Users] ページに表示されていることを確認します。

ステップ 6 Cisco TMS アプリケーションで、ユーザ グループを作成します。たとえば、`cm_group` という名前のグループを作成します。

ステップ 7 ステップ 3 で作成したユーザをステップ 6 で作成したグループに追加します。たとえば、`cm_user` を `cm_group` に追加します。

ステップ 8 [Groups] ページで、ステップ 6 で作成したグループに対して、[List Conferences - All]（[Booking] ペイン）の [Read permission] チェックボックスをオンにします。たとえば、`cm_group` が [List Conferences - All] の読み取り権限を持っている必要があります。

ステップ 9 ステップ 3 で作成したユーザを使用して、Cisco Prime CM で、Cisco TMS を検出します。たとえば、`cm_user` を使用します。

Cisco TMS の詳細については、http://www.tandberg.com/support/tms_documentation.jsp にあるマニュアルを参照してください。

グループの作成とグループへの権限の設定の詳細については、『Cisco TelePresence Management Suite Administrator Guide』を参照してください。

ネットワーク デバイスに対する Cisco Mediatrace、Cisco IOS IP SLA、およびパフォーマンス モニタリングの設定

ネットワーク ノードで Cisco Mediatrace をイネーブルにした場合は、Cisco Prime CM は、トラブルシューティング データの一部として Medianet Path View を提供します。ネットワーク ノードで Cisco IOS IP サービス レベル契約（SLA）を有効にしている場合は、事前トラブルシューティング機能を使用してネットワークのパフォーマンスおよび状態を測定できます。

Cisco Mediatrace の場合：

- 発信側ロールまたは応答側ロール、あるいはその両方を有効にします。
- 発信側に特権 15 を持つ Telnet ローカル ログイン ユーザを設定します。
- Web Services Management Agent（WSMA）および IP HTTP サーバを設定します。

Cisco IOS IP サービス レベル契約（SLA）の場合：

- 応答側ロールを有効にします。発信側ロールは必要ありません。

- IP SLA 発信側に特権 15 を持つ Telnet ローカル ログイン ユーザを設定します。

Cisco Prime CM の [Inventory] を使用して、これらのロールがデバイスで有効であるかどうかを確認できます（[Inventory] > [Device Inventory] > [Current Inventory] テーブル）。

パフォーマンス モニタリング（PM）の設定の場合：

関連するインターフェイスにパフォーマンス モニタ ポリシーを設定します。Cisco Prime CM は、MIB を介して PM フロー統計情報を収集します。この機能が設定されている場合、Cisco Prime CM はルータへの CLI アクセスを必要としません。

9 はじめに

クライアント ブラウザを使用して、Cisco Prime CM を起動できます。

Cisco Prime CM にログインするには、次の手順を実行します。

ステップ 1 マシンからブラウザ セッションを開きます。サポートされるブラウザについては、「クライアント マシン要件」を参照してください。

ステップ 2 次のように入力します。

http://*IP Address***/emsam/**
または
https://*IP Address***/emsam/**

（注） Cisco Prime CM サーバの IP アドレスまたはホスト名を使用できます。ホスト名を設定している場合は、ホスト名を使用することを推奨します。

ブラウザに応じて、以下のいずれかのブラウザ ウィンドウが表示されます。

- Windows Internet Explorer の場合は、[Certificate Error: Navigation Blocked] ブラウザ ウィンドウが表示されます。
- Mozilla Firefox の場合は、[Untrusted Connection] ブラウザ ウィンドウが表示されます。

これらのブラウザ ウィンドウが表示されるのは、Cisco Prime CM が自己署名証明書を使用しているためです。

ステップ 3 SSL 証明書の警告を削除します。「SSL 証明書の警告の削除」（P.22）を参照してください。

Cisco Prime CM のログイン ページが表示されます

ステップ 4 ユーザ名とパスワードを入力します。デフォルトでは、*admin* がユーザ名とパスワードになります。

[Change Password] ポップアップ ウィンドウが表示されます。

（注） Cisco Prime CM の使用を続行するには、デフォルト パスワード *admin* を変更する必要があります。[Cancel] をクリックすると、Cisco Prime CM からログアウトします。

ステップ 5 現在のパスワードと新しいパスワードを入力します。

（注） 作成する新しいパスワードは、[Basic Password Validity Rules] ポップアップ ウィンドウに記載されているすべての条件を満たしている必要があります。

ステップ 6 新しいパスワードを確認します。

ステップ 7 [Save] をクリックします。

ここで、Cisco Prime CM からログアウトします。

ステップ 8 新しいパスワードでログインします。

Cisco Prime CM のランディング ページが表示されます。

Cisco Prime CM をインストールした後は、次の表にある作業を実行する必要があります。表には、『*Cisco Prime Collaboration Manager 1.1 User Guide*』の項目も表示されています。これらの項目に、作業の詳細が記載されています。

手順	作業	説明	『Cisco Prime Collaboration Manager User Guide』の項目
ステップ 1	新しいライセンス ファイルを追加します。	製品を評価中の場合、この手順は任意です。 [Administration] > [License Management] を使用して、Cisco Prime CM 基本ライセンス ファイルを追加します。	「Setting Up and Maintaining the Server」の中の「Managing Licenses」
ステップ 2	クレデンシャルを定義します。	[Inventory] > [Device Inventory] > [Manage Credentials] を使用して、Cisco Prime CM でデバイスを管理するために必要なデバイスのクレデンシャルを入力します。詳細については、*「ネットワーク上のデバイスのセットアップ」*を参照してください。	「Managing Devices」の中の「Managing Credentials」
ステップ 3	CTS-Manager を検出します。 および/または Cisco TMS を検出します。	[Inventory] > [Device Inventory] > [Discover Devices] を使用して、CTS-Manager または TMS を検出します。 CTS-Manager と一緒に、Cisco Unified CM、Cisco TelePresence Multipoint Switch、および Cisco TelePresence System、デフォルト ゲートウェイ、およびスイッチが検出されます。 Cisco TMS と一緒に Cisco VCS、Cisco MCU、Cisco Profile および Codec、デフォルト ゲートウェイ、ならびにスイッチが検出されます。	「Managing Devices」の中の「Discovering Devices」
ステップ 4	インベントリを確認します。	[Inventory] > [Device Inventory] を使用して、検出されたすべてのデバイスが管理状態にあるかどうかを確認します。 その他の状態のデバイスが存在する場合は、[Job Management] ページ（[Administration] > [Job Management]）で検出ジョブの詳細を確認してください。	• 「Managing Devices」の中の「Managing Inventory」 • 「Setting Up and Maintaining the Server」の中の「Managing Jobs」

手順	作業	説明	『Cisco Prime Collaboration Manager User Guide』の項目
ステップ 5	セッションのインポート	[Monitoring] > [Session Monitoring] を使用して、セッションを監視するためのビデオ コラボレーション セッションを CTS-Manager、Cisco TMS、および Cisco TelePresence Multipoint Switch からインポートします。 CTS-Manager、Cisco TMS、および Cisco TelePresence Multipoint Switch からセッションを定期的にインポートするには、[Administration] > [Device Monitoring Configuration] を使用し、ビジネス ニーズに基づいたポーリング間隔を定義します。	• 「Monitoring Sessions and Endpoints」の中の「Monitoring Sessions」 • 「Setting Up and Maintaining the Server」の中の「Defining the Polling Intervals」
ステップ 6	セッションを確認します。	[Monitoring] > [Session Monitoring] を使用して、すべてのセッション詳細が CTS-Manager、Cisco TMS、および Cisco TelePresence Multipoint Switch からインポートされているかどうかを確認します。 Cisco Prime CM は 5 日分のスケジュール済みセッションのデータを収集します（前日、当日および今後 3 日）。	• 「Monitoring Sessions and Endpoints」の中の「Monitoring Sessions」

SSL 証明書の警告の削除

この項では、以下の各場合について SSL 証明書の警告を削除する方法を説明します。

- Windows Internet Explorer：Cisco Prime CM 自己署名証明書をインストールすることで、SSL 証明書の警告を永久に削除することができます。
- Mozilla Firefox：例外を追加することで、SSL 証明書の警告を一時的にだけ削除することができます。

Windows Internet Explorer で SSL 証明書の警告を削除するには、次の手順を実行します。

ステップ 1 [Continue to this website (not recommended)] を選択します。

ステップ 2 [Tools] > [Internet Options] を選択します。

[Internet Options] ダイアログボックスが表示されます。

ステップ 3 [Security] タブをクリックし、[Trusted sites] を選択して、[Sites] をクリックします。

ステップ 4 フィールドに表示される URL がアプリケーションの URL と一致することを確認し、[Add] をクリックします。

ステップ 5 すべてのダイアログボックスを閉じ、ブラウザをリフレッシュします。

ステップ 6 アドレス バーの右側にある [Certificate Error] を選択し、[View certificates] をクリックします。

[Certificate] ダイアログボックスが表示されます。

ステップ 7 [Install Certificate] をクリックします。

[Certificate Import Wizard] ダイアログボックスが表示されます。

ステップ 8 [Next] をクリックします。

ステップ 9 [Place all certificates in the following store] オプション ボタンをクリックし、[Browse] をクリックします。

[Select Certificate Store] ダイアログボックスが表示されます。

ステップ 10 [Trusted Root Certification Authorities] を選択し、[OK] をクリックします。

ステップ 11 [Next] > [Finish] の順にクリックします。

[Security Warning] メッセージ ボックスが表示されます。

ステップ 12 [Yes] をクリックします。

[Certificate Import Wizard] メッセージ ボックスが表示されます。

ステップ 13 [OK] をクリックします。

ステップ 14 [Certificate] ダイアログボックスで [OK] をクリックします。

ステップ 15 ステップ 2 とステップ 3 を繰り返します。

ステップ 16 [Websites] セクションで URL を選択し、[Remove] をクリックします。

ステップ 17 すべてのダイアログボックスを閉じ、ブラウザを再起動して、Cisco Prime CM を起動します。Cisco Prime CM の起動方法については、「はじめに」（P.20）を参照してください。

よく知っている URL を適用するには、次の手順を実行します。

a. [Tools] > [Internet Options] を選択します。

[Internet Options] ダイアログボックスが表示されます。

b. [Advanced] タブをクリックします。

c. [Security] セクションで、[Warn about certificate address mismatch] チェックボックスをオフにします。

Mozilla Firefox で SSL 証明書の警告を削除するには、次の手順を実行します。

ステップ 1 [I Understand the Risks] > [Add Exception] の順にクリックします。

[Add Security Exception] ダイアログボックスが表示されます。

ステップ 2 [Confirm Security Exception] をクリックします。

---

10 ナビゲーションおよびマニュアルの参照先

この項では、Cisco Prime CM の機能にアクセスするためのナビゲーション パスの情報と、Cisco Prime CM のマニュアル内でそれらの機能を扱っている項目の詳細を示します。

表 8　　ナビゲーションおよびマニュアルの参照先

作業	Cisco Prime CM 内のナビゲーション	『Cisco Prime Collaboration Manager 1.1 User Guide』の項
セッション詳細、障害、エンドポイント詳細、およびインベントリ詳細など、ビデオ コラボレーション ネットワークのさまざまなセグメントの要約の表示	ホーム	「ビデオ コラボレーション ダッシュボードについて」
ライセンスの管理	[Administration] > [License Management]	「ライセンスの管理」
ユーザおよびロールの定義	[Administration] > [User Management]	「ユーザおよびロールの定義」この項には、作業とロールのマッピングがあります。
ポーリング間隔の定義	[Administration] > [Device Monitoring Configuration]	「ポーリング間隔の定義」
アラームおよびレポート通知に関するシステム設定パラメータの設定	[Administration] > [System Configuration]	「システム コンフィギュレーション パラメータの設定」
イベント重大度のカスタマイズと、すべてのエンドポイントおよびビデオ コラボレーション デバイスのイベント モニタリングの有効化	[Administration] > [Endpoint Event Suppression]	「Customizing Event Parameters」
イベント重大度のカスタマイズと、すべてのエンドポイントおよびビデオ コラボレーション デバイスのモニタリング	[Administration] > [Event Configuration]	「Configuring Event Parameters」
ジョブの管理	[Administration] > [Job Management]	「ジョブの管理」
デバッグするログレベルの設定	[Administration] > [Log Configuration]	「ログ レベルの設定」
タイムゾーンおよび更新間隔の設定	[Administration] > [User Preference Configuration]	「タイムゾーンおよび更新間隔の設定」 Cisco Prime CM サーバの時間帯設定情報も記載されています。
Cisco Prime CM におけるデバイス クレデンシャルの設定	[Inventory] > [Device Inventory] > [Manage Credentials]	「クレデンシャルの管理」
デバイスの検出	[Inventory] > [Device Inventory] > [Discover Devices]	「デバイスの検出」
Cisco Prime CM で管理されるデバイスのインベントリの更新	[Inventory] > [Device Inventory] > [Update Inventory]	「インベントリの更新」

表 8　ナビゲーションおよびマニュアルの参照先（続き）

作業	Cisco Prime CM 内のナビゲーション	『Cisco Prime Collaboration Manager 1.1 User Guide』の項
管理対象エンドポイントおよびインフラストラクチャデバイスに関するインベントリ詳細のエクスポート	[Inventory] > [Device Inventory] > [Export Inventory]	「インベントリのエクスポート」
すべてのエンドポイント、スイッチ、およびデフォルト ゲートウェイが検出されているかどうかの確認	[Inventory] > [Device Inventory (Current Inventory)]	「インベントリの管理」
CTS-Manager および Cisco TMS から Cisco Prime CM へのセッションのインポート	[Monitoring] > [Session Monitoring] > [Import Sessions]	「セッションのモニタリング」
セッションがインポートされているかどうかの確認	[Monitoring] > [Session Monitoring]	「セッションのモニタリング」
エンドポイントが監視されているかどうかの確認	[Monitoring] > [Endpoint Monitoring]	「エンドポイントのモニタリング」
レポートの生成	[Reports] > • All Sessions Summary Report • Endpoint Utilization Report • No Show Endpoints Summary Report	「レポートの生成」
障害の管理	[Monitoring] > [Alarms]、[Monitoring] > [Events]	「障害の管理」
セッションのトラブルシューティング	• 自動トラブルシューティング：[Administration] > [Device Monitoring Configuration] • 手動トラブルシューティング：[Sessions Monitoring] ページおよび [Endpoints Monitoring] ページからのクイック ビュー	「セッションのトラブルシューティング」
ネットワークのパフォーマンスと状態の予防的な測定	[Monitoring] > [Proactive Troubleshooting]	「ネットワークの事前のトラブルシューティング」
バックアップと復元の実行	CLI	「バックアップと復元の実行」

11　Cisco Prime CM のアンインストール

Cisco Prime CM をアン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　Cisco Prime CM 仮想アプライアンスを右クリックします。

ステップ 2　[Remove from Disk] を選択します。

12 関連資料

Cisco Prime Collaboration Manager 1.1 の全マニュアルの一覧は、
『*Cisco Prime Collaboration Manager 1.1 Documentation Overview*』に記載されています。

（注） 元のドキュメントの発行後に、ドキュメントを更新することがあります。マニュアルのアップデートについては、Cisco.com で確認してください。

ここをクリックして、Cisco Prime Collaboration Manager トレーニング VOD にアクセスします。

次の項に、ビデオ コラボレーション アプリケーションのマニュアル リンクを示します。

- Cisco TelePresence 製品（製品を選択し、[Support] ペインで該当するマニュアルをクリック）
- *Cisco TelePresence Manager* のマニュアル
- *Cisco TelePresence* 管理ソフトウェアのダウンロード
- *Cisco Telepresence Multipoint Switch* のマニュアル
- *Cisco Unified Communications Manager（CallManager）*のマニュアル ロードマップ

13 マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。