



クイック スタート ガイド



## Cisco Prime Collaboration Manager 1.2 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/](http://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。

- 1 このマニュアルについて
- 2 製品概要
- 3 Cisco Prime CM のライセンスについて
- 4 Prime CM のインストール
- 5 Prime CM 1.1 から 1.2 へのアップグレード
- 6 ネットワーク上のデバイスのセットアップ
- 7 はじめに
- 8 ナビゲーションおよびマニュアルの参照先
- 9 Prime CM のアンインストール
- 10 関連資料
- 11 マニュアルの入手方法およびテクニカル サポート

# 1 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 1.2 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：Cisco TelePresence Manager (CTS-Manager) および Cisco TelePresence Management System (Cisco TMS)。
- コールおよびセッション制御：Cisco Unified Communications Manager (Cisco Unified CM) および Cisco TelePresence Video Communication Server (Cisco VCS)。
- 会議：Cisco TelePresence Multipoint Switch (CTMS)、Cisco TelePresence Server (TS)、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。

Prime CM の設定と管理の詳細については、『[Cisco Prime Collaboration Manager 1.2 User Guide](#)』を参照してください。

## 新機能および変更情報

次の表では、『Cisco Prime Collaboration Manager 1.2 クイック スタート ガイド』の初期リリース以降に追加または変更された情報について説明します。

日付	リビジョン	場所
2012年7月3日	<ul style="list-style-type: none"><li>• CTS-Manager、Cisco TelePresence Multipoint Switch、および Cisco TelePresence System シリーズでサポートされるソフトウェア バージョンを更新しました。</li><li>• Prime CM 1.2 へのアップグレード後も保持される Prime CM 1.1 の設定データを更新しました。</li><li>• Prime CM 1.0 および 1.1 のユーザ向けのライセンス ファイルの取得方法に関する情報を更新しました。</li></ul>	<ul style="list-style-type: none"><li>• 「ネットワーク上のデバイスのセットアップ」(P.13)</li><li>• 「Prime CM 1.1 から 1.2 へのアップグレード」(P.12)</li><li>• 「Cisco Prime CM のライセンスについて」(P.3)</li></ul>
2012年6月13日	最初のバージョン	

# 2 製品概要

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。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。

Prime CM では、各セッションの関連するメディア パスをただちに表示し、問題の原因の切り分けを行います。Mediatrace 対応デバイスがネットワークに導入されている場合、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。

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の切り分けを行います。

- 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。
- 重要な障害およびパフォーマンスの統計情報とともに、メディアパスの詳細な分析情報を提供します。これにより、サービス低下の原因となっているネットワーク デバイスを特定できます。
- 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、ステータスを利用して、大規模な導入の検証を行います。
- 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。

Prime CM の主な機能の特長については、『[Cisco Prime Collaboration Manager 1.2 User Guide](#)』を参照してください。

## 3 Cisco Prime CM のライセンスについて

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。このリリースでは、次のライセンス カテゴリがサポートされています。

- 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
- マス エンドポイント

表 1 に、ライセンス カテゴリとエンドポイント タイプ間のマッピングを示します。

表 1 ライセンス カテゴリとエンドポイント タイプ

ライセンス カテゴリ	エンドポイント タイプ
マルチコーデック エンドポイント	Cisco TelePresence System 3000
	Cisco TelePresence System 3010
	Cisco TelePresence System 3200
	Cisco TelePresence System 3210
ハイエンド、シングルコーデック エンドポイント	Cisco TelePresence System 1000
	Cisco TelePresence System 1100
	Cisco TelePresence System 1300
	Cisco TelePresence System 1400
	Cisco Profile 42-C20
	Cisco Profile 42-C60
	Cisco Profile 52 デュアル
	Cisco Profile 52
	Cisco Profile 65
	Cisco Profile 65 デュアル
	Cisco Profile 52-6000MXP

表 1 ライセンス カテゴリとエンドポイント タイプ (続き)

ライセンス カテゴリ	エンドポイント タイプ
ミッドレンジ、シングルコーデック エンドポイント	Cisco Codec EX60
	Cisco Codec EX90
	Cisco Codec C90
	Cisco Codec C60
	Cisco Codec C40
	Cisco Codec C20
	Cisco Profile 42 C20
	Cisco Profile 42 C60
	Cisco Profile 150MXP
	Cisco Profile 1000MXP
	Cisco Profile 1700MXP
	Cisco Profile 3000MXP
	Cisco Profile 6000MXP
	Cisco TelePresence MX200
	Cisco TelePresence MX300
	Cisco CTS Manager 500
Cisco TelePresence SX20 クイック セット	
マス エンドポイント	Cisco IP Phone
	Polycom
	Cisco Cius
	Cisco Jabber Video for TelePresence
	Cisco IP Video Phone E20

最初に、Cisco.com の「[Network Management Evaluation Products](#)」のリストから、Prime CM の評価バージョンをダウンロードしてインストールする必要があります。

評価ライセンスの有効期限は 60 日間です。評価ライセンス モードでは、次のタイプのエンドポイントを管理できます。

- 100 個のハイエンド、シングルコーデック エンドポイント
- 100 個のハイエンド、マルチコーデック エンドポイント
- 500 個のミッドレンジ、シングルコーデック エンドポイント
- 2000 個のマス エンドポイント

デフォルトでは、製品をダウンロードしてインストールすると、評価モードで 60 日間有効なライセンスを取得できます。



**(注)** Prime CM1.2 ベース ソフトウェアには、ライセンスは含まれていません。

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](#)」(P.5) と「[ライセンス ファイルの入手](#)」(P.5) を参照してください。
- ステップ 2** 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 1.2 User Guide](#)』を参照してください。

## Prime CM 1.0 および 1.1 ライセンスのサポート

Prime CM 1.2 リリースでは、ライセンス構造が変更されています。

Prime CM 1.0 のユーザであり、Prime CM 1.1 リリースにアップグレードしている場合は、ライセンス ファイルを Prime CM 1.2 用にアップデートする必要があります。Prime CM 1.2 にアップグレードすると、Prime CM 1.0 のライセンス ファイルが認識されなくなります。Prime CM 1.2 用の新しいライセンス ファイルを取得する必要があります。

Prime CM 1.1 を直接インストールして Prime CM 1.2 リリースにアップグレードした場合は、アップグレード後に Prime CM 1.1 のライセンス ファイルが認識されます。ただし、Prime CM 1.1 の基本ライセンスに含まれている Prime CM 1.2 の適切なエンドポイント ライセンスの取得が必要になる場合があります。

\*.lic ファイルを開くと、使用しているライセンス ファイルが Prime CM 1.0 または 1.1 のどちらかを確認できます。ライセンス ファイルで `CM_LARGE_NTWK_DVCS10K` または `CM_CODECS25` という文字列を検索します。いずれかの文字列がライセンス ファイル内に記載されている場合は Prime CM 1.0 のライセンス ファイルを使用しており、記載されていない場合は Prime CM 1.1 ライセンス ファイルを使用しています。

Prime CM 1.2 にアップグレードする前に、シスコのアカウント マネージャに問い合わせ、Prime CM 1.2 Upgrade PID を取得する必要があります。

Prime CM 1.2 のライセンス ファイルを取得するには、Cisco Technical Assistance Center (TAC) チームに連絡する必要があります。TAC チームから、ライセンスの権限付与に関する Prime CM 注文書の明細を求められる場合があります。

## 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 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 Prime CM 製品を登録する必要があります。UUID は、Prime CM の評価バージョンをインストールすると、サーバ上に自動的に生成されます。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 Prime CM に追加する必要があります。詳細については、『Cisco Prime Collaboration Manager 1.2 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。

## 4 Prime CM のインストール

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

次の点を確認します。

- 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 のインストールが可能な 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、そ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 サーバのホスト名が、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。
- Cisco Prime Collaboration Manager の [ソフトウェア ダウンロード](#) サイトから、次のいずれかの Prime CM イメージをダウンロードします。
  - Prime CM 1.2 の新規インストールの場合 : `emsam-va-1.2.0-16941.x86_64.ova`
  - Prime CM 1.1 から Prime CM 1.2 へのアップグレードの場合 : `emsam-appbundle-1.2.0-16941.x86_64.tar.gz`

ファイルをダウンロードするには、Cisco.com の有効なユーザ アカウントが必要です。

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.13) を参照してください。

## システム要件

Prime CM 1.2 は、ESXi 4.1 または 5.0 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。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 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などの仮想マシンの設定を定義します。

### 仮想マシン要件

表 2 に、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 2 仮想マシン要件

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、Prime CM 1.2 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ています。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

同時に最大 10 人のユーザが Prime CM にログインできます。

表 3 に、Prime CM 1.2 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 3 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。 <ul style="list-style-type: none"><li>• Mozilla Firefox 8.0、9.0、および 10.0 (Linux、Mac、および Windows)</li><li>• Windows Internet Explorer 8.0 および 9.0</li></ul> Prime CM は、自己署名証明書 (HTTPS) を提供します。Prime CM クライアントのアクセスを可能にするには、Internet Explorer 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： <ul style="list-style-type: none"><li>• ブラウザで cookie を有効にしていることを確認します。</li><li>• 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。</li></ul>
Adobe Flash Player	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 Flash 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。

## 必須のポート

表 4 に、Prime CM で使用されるポートの詳細を示します。

表 4 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：Prime CM から CTS、C シリーズへ。	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 Prime CM へ。	クライアント マシンから Prime CM サーバに接続する。
23	TCP	双方向：Prime CM 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 対応デバイスへの Telnet 接続を開始する。
25	TCP	単方向：Prime CM から SMTP サーバへ。	SMTP
53	TCP	単方向：Prime CM から DNS サーバへ。	DNS
80	TCP	双方向：クライアントから Prime CM へ。	ブラウザから Prime CM へのアクセス (HTTP)。
		双方向：Prime CM 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 対応デバイスへの HTTP 接続を開始する。
		単方向：Prime CM から Cisco VCS へ。	コール詳細および Cisco VCS のヘルス ステータスをポーリングする (HTTP)。
		単方向：Prime CM から CTMS へ。	コール詳細をポーリングする。
		単方向：Prime CM から MCU へ。	コール詳細および MCU ヘルス ステータスをポーリングする。
		単方向：Prime CM から CTS-Manager へ。	セッションをインポートし、CTS-Manager のヘルス ステータスをポーリングする。
		単方向：Prime CM から TMS へ。	セッションをインポートし、TMS のヘルス ステータスをポーリングする。
		単方向：Prime CM から C シリーズへ。	コール詳細および C シリーズのステータスをポーリングする (HTTP)。
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。
		単方向：Prime CM から Cisco VCS へ。	コール詳細および Cisco VCS のヘルス ステータスをポーリングする (SNMP)。
		単方向：Prime CM から CTMS へ。	CTMS のヘルス ステータスをポーリングする。
		単方向：Prime CM から MCU へ。	MCU のヘルス ステータスをポーリングする。
		単方向：Prime CM から CTS-Manager へ。	CTS-Manager のヘルス ステータスをポーリングする。
		単方向：Prime CM から TMS へ。	TMS のヘルス ステータスをポーリングする。
		単方向：Prime CM から C シリーズへ。	C シリーズのヘルス ステータスをポーリングする。
		単方向：Prime CM から CTS へ。	コール詳細および CTS のヘルス ステータスをポーリングする。



表 4 使用されるポート (続き)

ポート	プロトコル	方向	使用方法
162	UDP	単方向：エンドポイントから Prime CM へ。	トラップ レシーバ ポート。
		単方向：Prime CM からトラップ レシーバへ。	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 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。	Real Time Monitoring Tool (RTMT)、Cisco Unified CM 登録、および 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。
		単方向：Prime CM から VCS へ。	コール詳細および VCS のヘルス ステータスをポーリングする (HTTPS)。
		単方向：Prime CM から CTMS へ。	Prime CM 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。
		単方向：Prime CM から MCU へ。	コール詳細および MCU ヘルス ステータスをポーリングする。
		単方向：Prime CM から CTS-Manager へ。	セッションをインポートし、CTS-Manager のヘルス ステータスをポーリングする。
		単方向：Prime CM から TMS へ。	セッションをインポートし、TMS のヘルス ステータスをポーリングする。
		単方向：Prime CM から C シリーズへ。	Prime CM 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。
514	UDP	単方向：Cisco Unified Communications Manager から Prime CM へ。	syslog レシーバ ポート。
2748	TCP	単方向：Prime CM から Cisco Unified Communications Manager へ。	CTI アプリケーション サーバ。
2749	TCP	単方向：Prime CM から Cisco Unified Communications Manager へ。	CTI アプリケーション (JTAPI/TSP) と CTIManager 間の TLS 接続
2789	TCP	単方向：Cisco Unified Communications Manager から Prime CM へ。	クライアント側の JTAPI アプリケーション サーバ。
8886	TCP	単方向：Cisco VCS から Prime CM へ。	Cisco 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 Prime CM へ。	Cisco 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が満たされていることを確認します。「はじめる前に」(P.5) および「システム要件」(P.7) を確認してください。

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。
- ステップ 3** [Deploy OVF Template] ウィンドウで、[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、emsam-va-1.2.0-16941.x86\_64.ova ファイルを保存した場所に移動します。
- 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。
- ステップ 7** [Name and Location] ウィンドウで、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 フォルダ内で一意である必要があり、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。
- ステップ 9** [Disk Format] ウィンドウで、次のいずれかのオプション ボタンをクリックして、仮想ディスクを保存する形式を指定します。
- **Thin provisioned format**
  - **Thick provisioned format**
- [Thick provisioned format] を推奨します。
- ステップ 10** [Next] をクリックします。
- [Ready to Complete] ウィンドウには、OVA ファイルの詳細、仮想アプライアンスの名前、ディスクのサイズ、ホスト名、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の、ホストの下に表示されます。
- 

## 仮想アプライアンスの設定

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。



- (注)** Prime CM は評価バージョンとしてインストールされており、すべての機能はこのバージョンでサポートされています。評価ライセンスの有効期限は 60 日間です。
- 

仮想アプライアンスを設定するには、次の手順を実行します。

- 
- ステップ 1** 仮想アプライアンスを右クリックし、[Power] > [Power On] を選択して仮想マシンの電源をオンにします。
- 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** 仮想アプライアンス コンソールで、ローカルホスト ログイン プロンプトに対して setup と入力します。
- ステップ 3** コンソール プロンプトで、要求されたパラメータを入力します。各パラメータを入力して Enter を押すと、その次のパラメータが表示されます。



- (注)
- [Time zone] : Prime CM サーバの設定中にシステム時間帯を入力するよう求めるプロンプトが表示された場合は、デフォルトの時間帯である UTC を指定します。時間帯は、Prime CM サーバのインストール後に SSH 経由で変更/設定できます。サポートされている時間帯の一覧については、『Supported Time Zones for Prime Collaboration Manager』を参照してください。Prime CM のインストール後に時間帯を設定する方法の詳細については、『Cisco Prime Collaboration Manager 1.2 User Guide』を参照してください。
  - [Username] : 管理ユーザ名として **cmuser** を使用しないでください。**cmuser** は事前設定された Prime CM の CLI ユーザであるため、使用すると問題が発生する可能性があります。
  - [Password] : 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** Prime CM にログインして、機能しているかどうかを確認します。（「はじめに」(P.16) を参照）。

## Prime CM のインストールに関するトラブルシューティング

Prime CM を起動できない場合は、必要なプロセスが Prime CM 1.2 サーバで実行されていない可能性があります。

インストールのトラブルシューティングを行うには、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 Prime CM 1.2 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	4084	root	Decap_main	1-00:18:32
SNl	5250	root	emsam_fault	1-00:15:55
SNl	4348	root	emsam_inventory	1-00:18:00
SNl	4274	root	emsam_mq	1-00:18:08
SNl	5138	root	emsam_poller	1-00:16:16
SNl	5067	root	emsam_tomcat	1-00:16:19
SNs	4204	oracle	oracle	1-00:18:22
SNsl	4113	oracle	tnslnr	1-00:18:30

[COMMAND] 列のパラメータが、Prime CM 1.2 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 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 Prime CM 1.2 サーバで実行されていない場合は、TAC に問い合わせてください。

## 5 Prime CM 1.1 から 1.2 へのアップグレード

Prime CM 1.1 から 1.2 にアップグレードする場合は、いくつかの設定データが保持されます。表 5 に、保持される設定データの詳細を示します。

現在 Prime CM 1.0 を使用中で、Prime CM 1.2 にアップグレードする場合は、最初に Prime CM 1.1 にアップグレードしてから Prime CM 1.2 にアップグレードする必要があります。Prime CM 1.0 から 1.1 にアップグレードするには、『[Cisco Prime Collaboration Manager Quick Start Guide 1.1](#)』を参照してください。



**(注)** Prime CM 1.1 のインベントリ データは、アップグレード後は保持されません。ただし、デバイスのクレデンシャル データは保持されます。インベントリ データを Prime CM 1.2 のデータベースに追加するには、デバイス ディスカバリ タスク ([Inventory] > [Device Inventory] > [Discover Devices]) を実行します。

アップグレード後は、次の表に示す設定データのみ保持されます。

表 5 Prime CM 1.1 から 1.2 へのアップグレードで保持される設定データ

設定データ	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]	Prime CM 1.2 で必要な追加設定はありません。
ユーザ アカウント	[Administration] > [Management] > [User Management]	Prime CM 1.2 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]	Prime CM 1.2 で必要な追加設定はありません。
イベント設定	[Administration] > [Configuration] > [Event Settings]	Prime CM 1.2 で必要な追加設定はありません。
システム設定	[Administration] > [Configuration] > [System Configuration]	<ul style="list-style-type: none"><li>• [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。</li><li>• 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。</li><li>• 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。</li><li>• 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。</li></ul>

Prime CM 1.1 と Prime CM 1.2 は、同一の仮想マシンにインストールされます。Prime CM 1.1 から Prime CM 1.2 にアップグレードするには、次の手順を実行します。

**ステップ 1** SSH で admin として Prime CM 1.1 サーバにログインします。

**ステップ 2** 次のコマンドを入力して cars リポジトリを作成します。

```
admin# configure terminal
admin(config)# repository cars
admin(config-Repository)# url ftp://111.222.333.444 (for example)
admin(config-Repository)# user admin password plain cisco (for example)
admin(config-Repository)# exit
admin(config)# exit
```

**ステップ 3** 次のコマンドを入力して、Prime CM 1.1 サーバを Prime CM 1.2 にアップグレードします。

```
admin# application upgrade emsam-appbundle-1.2.0-XXXXX.x84_64.tar.gz cars
```

**ステップ 4** SSH 端末から別のセッションを開き、Prime CM admin としてログインし、Prime CM 1.2 サーバのプロセスが実行されていることを確認します。

```
admin# show application status emsam
STAT  PID USER      COMMAND          ELAPSED
=====
S<l  15750 root      Decap_main       15:55:41
S1   17156 root      emsam_fault      15:53:36
S1   16024 root      emsam_inventory  15:55:26
S1   15945 root      emsam_mq         15:55:34
S1   17056 root      emsam_poller     15:53:57
S1   16983 root      emsam_tomcat     15:53:59
Ss   15860 oracle   oracle           15:55:40
Ss1  15781 oracle   tnslnsr         15:55:41
admin# exit
```

Prime CM にログインして、機能しているかどうかを確認します。（「はじめに」(P.16) を参照）。



(注) アップグレードプロセスは完了までに約 20 分かかります。

## 6 ネットワーク上のデバイスのセットアップ

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tring 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。

表 6 に、Prime CM でデバイスを管理する前に必要とされるデバイ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 6 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、1.8	Yes	Yes <sup>1</sup>	No	No	NA
Cisco Unified CM	8.0 ~ 8.6	Yes	Yes	No	Yes	NA
Cisco TelePresence Multipoint Switch	1.7、1.8	Yes	Yes	No	No	NA
Cisco TelePresence System シリーズ	1.7、1.8	Yes	No	Yes	No	NA
Cisco TelePresence Management Suite (Cisco TMS)	13.0、13.1、13.2	Yes	Yes <sup>2</sup>	No	No	—
Cisco TelePresence Video Communication Server (Control と Expressway)	6.0 ~ 7.0	Yes	Yes <sup>3</sup>	No	No	—
Cisco TelePresence MCU シリーズ Cisco MCU MSE 8510	4.1 または 4.2	Yes	Yes <sup>3</sup>	No	No	—

表 6 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
Cisco Telepresence Server 7010	2.1 または 2.2	No	Yes	No	No	—
Cisco Telepresence Server MSE 8710						
Cisco Codec EX シリーズ Cisco Telepresence System Integrator C シリーズ Cisco Telepresence MX シリーズ Cisco Telepresence System Profile シリーズ Cisco Telepresence SX20 クイック セット	4.2 または 5.0	Yes	Yes <sup>3</sup>	Yes	No	—
Cisco TelePresence System MXP シリーズ	9.1	Yes	Yes <sup>3</sup>	Yes	—	—
Polycom VSX シリーズ (8.0、8.5、9.0.5)	9.0	Yes	No	No	—	—
Polycom HDX シリーズ	2.5 ~ 3.0	Yes	No	No	—	—
Cisco Cius	9.2	No	No <sup>4</sup>	No	—	—
Cisco TelePresence Supervisor MSE 8050	2.1	Yes	Yes <sup>3</sup>	No	No	—
Cisco IP Video Phone E20	4.0 または 4.1	Yes	Yes	Yes	—	—
Cisco Jabber Video for Telepresence (Movi)	4.2	No	No	No	—	—
Cisco Telepresence Conductor	1.1	Yes	Yes	No	No	—
Cisco IP Phone (89xx、99xx)	9.2	No	No <sup>4</sup>	No	—	—
ネットワーク デバイス (ルータとスイッチ)	—	Yes	No	Yes	No	Yes

1. Reporting API ライセンスおよび CPCM ユーザの Reporting API ロールが必要です
2. Booking API ライセンスおよび Booking API によって生成された CPCM ユーザが必要です
3. Admin 特権が必要です
4. HTTP アクセス用のクレデンシャルは不要です

#### 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

- Prime CM は IPv4 が設定されたエンドポイントのみをサポートします。IPv6 が設定されたエンドポイントはサポートしません。また、Prime CM はデュアル スタック (IPv4 と IPv6 が設定された) エンドポイントはサポートしません。
- 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 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 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。
- 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 サブスクリバは、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。
- 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 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。
- 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。Prime CM サーバは、ネットワーク内の 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。
- CTS エンドポイントの場合、CPCM 用の CLI ユーザ アカウントに Admin 特権または Helpdesk 特権のいずれかを設定できます。CLI アクセスは、トラブルシューティング機能が必要な場合のみ必要となります。
- C/EX/MX/SX および MXP シリーズのエンドポイントの場合、必要な CLI ユーザ クレデンシャルは HTTP ユーザ クレデンシャルと同一です。そのため、CLI 用に追加のユーザ クレデンシャル設定は必要ありません。
- C/EX/MX/SX および MXP シリーズのエンドポイントの場合、エンドツーエンドのトラブルシューティング パス トレース をモニタリングおよび実行するためには、HTTP 管理者レベルのアクセス権が必要です。
- CPCM からの Cisco Jabber Video for Telepresence (Movi) エンドポイントには、ユーザ アカウントは必要ありません。
- すべてのデバイスは、CPCM から ICMP ping で到達可能になっている必要があります (必要に応じて ICMP ping をディセーブルにできますが、それには CPCM への root アクセスが必要です)。
- Cisco TelePresence Server (TPS) は SNMP をサポートしていません。その場合を除き、CPCM 1.2 には、その他すべてのインフラストラクチャ デバイス タイプへの SNMP 読み取り専用アクセス権が必要です。
- CTSMAN には、Reporting API ライセンスが必要です。HTTP ユーザ アカウントは、メールボックスを持ち、CTSMAN の Reporting API ロールおよび Live Desk ロールを持つユーザ グループの AD ユーザになっている必要があります。
- HTTP 管理者レベル アクセスは、TPS では必要ありません。HTTP API アクセス特権のみが必要です。
- VCS の場合は、CPCM の HTTP ユーザは、読み取りおよび書き込み特権を持っている必要があります。
- ネットワークの問題をトラブルシューティングする CPCM 機能が必要な場合は、ルータおよびスイッチに SNMP v2c または v3 クレデンシャルが必要です。
- また、トラブルシューティング パス トレースが必要な場合は、すべてのネットワーク デバイスで CDP をイネーブルにする必要もあります。
- Medianet ベースのトラブルシューティングが必要な場合は、ルータおよびスイッチに CLI ログイン クレデンシャルが必要です。
- Cisco Unified CM で、Cisco IP Phone (89xx、99xx) および Cisco Cius 用の Web アクセス設定をイネーブルにします。
- Multipoint Switch の Prime CM アプリケーションには、Meeting Scheduler ロールと Diagnostic Technician 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。
- Cisco Unified CM で、次のロールをイネーブルにします。
  - Standard CTI Allow Call Monitoring
  - Standard CTI Enabled
  - Standard CTI Allow Control of Phones supporting Connected Xfer and conf

必要なプロトコル設定については、『[Setting up Devices on the Network for Prime Collaboration Manager](#)』を参照してください。

## 7 はじめに

クライアント ブラウザを使用して、Prime CM を起動できます。

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](#)」(P.7) を参照してください。

**ステップ 2** 次のいずれかを入力します。

- `http://IP Address`
- `https://IP Address`



**(注)** 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。

使用しているブラウザに応じて、次のいずれかのウィンドウが表示されます。

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

これらのウィンドウが表示されるのは、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.18) を参照してください。

Prime CM のログイン ページが表示されます

**ステップ 4** Prime CM のログイン ページで、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。



**(注)** 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] をクリックするとログアウトします。

**ステップ 5** [Change Password] ポップアップ ウィンドウに、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、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。

Prime CM のランディング ページが表示されます。ダッシュボード データは、次の表の作業を実行した後でのみ表示されることに注意してください。

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 1.2 User Guide](#)』内の対応する項も示してあります。これらの項には、作業の詳細が記載されています。



作業	説明	『Cisco Prime Collaboration Manager User Guide』の項
<b>ステップ1</b> 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、Prime CM 基本ライセンス ファイルを追加します。 Prime CM 1.1 から 1.2 にアップグレードする場合、新しいライセンス ファイルを取得する方法の詳細については、「Cisco Prime CM のライセンスについて」(P.3) を参照してください。	「Setting Up and Maintaining the Server」の中の「Managing Licenses」
<b>ステップ2</b> クレデンシャルを定義します。	[Inventory] > [Device Inventory] > [Manage Credentials] を使用して、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」(P.13) を参照してください。 Prime CM 1.1 から Prime CM 1.2 にアップグレードする場合、デバイスのクレデンシャル データが Prime CM 1.2 のデータベースで使用可能です。	「Managing Devices」の中の「Managing Credentials」
<b>ステップ3</b> 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、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。 Cisco Telepresence Conductor は、CTS-Manager/TMS から自動検出されません。Cisco Telepresence Conductor は、個別に検出する必要があります。	「Managing Devices」の中の「Discovering Devices」
<b>ステップ4</b> 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。	<ul style="list-style-type: none"> <li>• 「Managing Devices」の中の「Managing Inventory」</li> <li>• 「Setting Up and Maintaining the Server」の中の「Managing Jobs」</li> </ul>

作業	説明	『Cisco Prime Collaboration Manager User Guide』の項
ステップ5 セッションのインポート	<p>[Monitoring] &gt; [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。</p> <p>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] &gt; [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。</p>	<ul style="list-style-type: none"> <li>「Monitoring Sessions and Endpoints」の中の「Monitoring Sessions」</li> <li>「Setting Up and Maintaining the Server」の中の「Defining the Polling Intervals」</li> </ul>
ステップ6 セッションを確認します。	<p>[Monitoring] &gt; [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。</p> <p>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）。</p>	<ul style="list-style-type: none"> <li>「Monitoring Sessions and Endpoints」の中の「Monitoring Sessions」</li> </ul>

## 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 : Prime CM の自己署名証明書をインストールすることにより、SSL 証明書の警告を完全に削除できます。
- Mozilla Firefox : 例外と追加することによってのみ、SSL 証明書の警告を削除できます。

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。
- ステップ 3 [Internet Options] ダイアログボックスで [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。
- ステップ 7 [Certificate] ダイアログボックスで、[Install Certificate] をクリックします。
- ステップ 8 [Certificate Import Wizard] ダイアログボックスで、[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。
- ステップ 12 [Security Warning] メッセージ ボックスで、[Yes] をクリックします。
- ステップ 13 [Certificate Import Wizard] メッセージ ボックスで、[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、Prime CM を起動します。Prime CM の起動の詳細については、「はじめに」(P.16) を参照してください。

安全な 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。
- b. [Internet Options] ダイアログボックスで、[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。

**ステップ 2** [Add Security Exception] ダイアログボックスで、[Confirm Security Exception] をクリックします。

## 8 ナビゲーションおよびマニュアルの参照先

ここでは、Prime CM の機能にアクセスするためのナビゲーションパスを提供し、それらの機能に関する説明が記載されている Prime CM ドキュメント内の項を示します。

表 7 ナビゲーションおよびマニュアルの参照先

作業	Prime CM 内のナビゲーション	『Cisco Prime Collaboration Manager 1.2 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	「Video Collaboration Dashboard」
ライセンスの管理	[Administration] > [Management] > [License Management]	「Managing Licenses」
ユーザおよびロールの定義	[Administration] > [Management] > [User Management]	「Defining Users and Roles」。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] > [Configuration] > [Device Monitoring Configuration]	「Defining the Polling Intervals」
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] > [Configuration] > [System Configuration]	「Configuring System Configuration 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 デバイスのイベント モニタリングの有効化	[Administration] > [Configuration] > [Event Settings]	「Customizing Event Parameters」

表 7 ナビゲーションおよびマニュアルの参照先 (続き)

作業	Prime CM 内のナビゲーション	『Cisco Prime Collaboration Manager 1.2 User Guide』の項
ジョブの管理	[Administration] > [Management] > [Job Management]	「Managing Jobs」
デバッグするログ レベルの設定	[Administration] > [Configuration] > [Log Configuration]	「Setting the Log Level」
時間帯および更新間隔の設定	[Administration] > [Configuration] > [User Preference Configuration]	「Configuring Timezone and Refresh Interval」。この項には、Prime CM サーバの時間帯設定情報も記載されています。
Prime CM におけるデバイス クレデンシャルの設定	[Inventory] > [Device Management] > [Device Inventory] > [Manage Credentials]	「Managing Credentials」
デバイスの検出	[Inventory] > [Device Management] > [Device Inventory] > [Discover Devices]	「Discovering Devices」
Prime CM で管理されるデバイスのインベントリの更新	[Inventory] > [Device Management] > [Device Inventory] > [Update Inventory]	「Updating Inventory」
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 Management] > [Device Inventory] > [Export Inventory]	「Exporting Inventory」
すべてのエンドポイントとスイッチ、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 Management] > [Device Inventory (Current Inventory)]	「Updating Inventory」
CTS-Manager および Cisco TMS から Prime CM へのセッションのインポート	[Monitoring] > [Sessions & Endpoints] > [Session Monitoring] > [Import Sessions]	「Monitoring Sessions」
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]	「Monitoring Sessions」
エンドポイントがモニタされているかどうかの確認	[Monitoring] > [Endpoint Monitoring]	「Monitoring Endpoints」
レポートの生成	[Reports] > [Interactive] > <ul style="list-style-type: none"> <li>• All Sessions Summary Report</li> <li>• Endpoint Utilization Report</li> <li>• No Show Endpoints Summary Report</li> <li>• Conferencing Device Utilization Report</li> <li>• Session Detail</li> </ul>	「Generating Reports」
障害の管理	[Monitoring] > [Alarms & Events] > [Alarms; Monitoring] > [Events]	「Managing Faults」

表 7 ナビゲーションおよびマニュアルの参照先 (続き)

作業	Prime CM 内のナビゲーション	『Cisco Prime Collaboration Manager 1.2 User Guide』の項
セッションのトラブルシューティング	<ul style="list-style-type: none"> <li>自動トラブルシューティング : [Administration] &gt; [Device Monitoring Configuration]</li> <li>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</li> </ul>	「Troubleshooting Sessions」
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] > [Sessions & Endpoints] > [Proactive Troubleshooting]	「Proactively Troubleshooting the Network」
Cisco Video または TelePresence システムを導入するためのネットワークの準備検査	[Monitoring] > [Sessions & Endpoints] > [Media Path Analysis]	「Analyzing Media Paths」
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」

## 9 Prime CM のアンインストール

Prime CM 仮想アプライアンスを削除するには、次の手順を実行します。

- ステップ 1** vSphere Client にログインして、CM 1.2 を実行している ESX サーバに接続します。
- ステップ 2** Prime CM 仮想アプライアンスを右クリックし、[Power] > [Shut Down Guest] に移動します (または、[Power Off] を選択します)。

## 10 関連資料

Prime CM のマニュアルには、『[Cisco Prime Collaboration Manager 1.2 Documentation Overview](#)』からアクセスできます。



**(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。

## 11 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。

---

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2012 Cisco Systems, Inc.  
All rights reserved.

Copyright © 2012, シスコシステムズ合同会社 .  
All rights reserved.