

Cisco IPICS のインストール

この章では、Cisco IPICS オペレーティング システムと Cisco IPICS サーバ ソフトウェアのインストールに必要な手順について説明します。

この章は、次の項で構成されています。

- [開始する前に \(P.2-2\)](#)
- [Cisco IPICS オペレーティング システムのインストール \(P.2-8\)](#)
- [Cisco IPICS サーバ ソフトウェアのインストール \(P.2-19\)](#)
- [サーバの再起動またはシャットダウン \(P.2-30\)](#)
- [Cisco IPICS を使用する準備 \(P.2-33\)](#)

開始する前に

この項では、Cisco IPICS オペレーティング システムおよびサーバのインストールで必要になる準備作業について説明します。次のトピックを扱います。

- [Cisco IPICS システムの IP アドレスの取得 \(P.2-2\)](#)
- [インストール前のチェックリスト \(P.2-3\)](#)

Cisco IPICS システムの IP アドレスの取得

Cisco IPICS システムでは、ユーザ間の通信を容易にするため、ネットワーク ドメイン内のすべてのユーザが到達できる IP アドレスをまとめたプールが必要です。

Cisco IPICS サーバには、ネットワーク上にアドバタイズされるローカルの固定 IP アドレスが必要です。PMC や Cisco Unified IP Phone などの Cisco IPICS エンドポイントが通信を維持するには、これらのエンドポイントが Cisco IPICS サーバの固定アドレスを知っている必要があります。

Cisco IPICS はアナログの Push-to-Talk (PTT) 無線トラフィックを IP トラフィックに変換するため、各無線チャネルは IP マルチキャスト アドレスにマッピングされます。同様に、Hoot & Holler システムの場合は、各トーク グループが IP マルチキャスト アドレスにマッピングされます。IP で接続されたデバイス (PMC など) のユーザは、マルチキャスト IP アドレスを使用して接続するか、Session Initiation Protocol (SIP) を通じてユニキャストのリモート接続を使用することで、これらのチャネルに参加できます。

Cisco IPICS では、次のそれぞれの処理でマルチキャスト アドレスが必要です。

- PTT チャネルの作成
- Hoot & Holler システムでのトーク グループの作成
- 仮想トーク グループ (VTG) のアクティブ化
- チャネルまたは VTG へのダイヤルユーザの接続

IP アドレスの割り当てを容易にするには、同じサブネットに所属するデバイスを設定できる IP アドレスの、サブネットを取得すると便利です。

Cisco IPICS では、router media service (RMS; ルータ メディア サービス) のループバック インターフェイスに使用される IP アドレスも必要です。ループバック インターフェイスは、ループバック ケーブルと呼ばれる短いケーブルで互いに接続された、RMS の 2 つの T1/E1 インターフェイスで構成されます。ループバック インターフェイスは、Cisco IPICS の SIP ベースのすべての接続において、音声のシグナリングとメディアに使用されます。



(注)

RMS への IP パスが複数ある場合は、Loopback0 インターフェイスを明示的に設定することをお勧めします。ただし、基準に合う場合は Loopback0 以外のインターフェイスを設定することもできます。この基準の詳細については、『[Cisco IPICS Server Administration Guide, Release 2.1\(1\)](#)』の付録「Configuring the Cisco IPICS RMS Component」を参照してください。



Cisco IPICS システム、チャンネル、VTG、および RMS の IP アドレスの取得については、ネットワーク管理者に問い合せてください。



Cisco IPICS での IP アドレスの設定と使用、および RMS の詳細については、『[Cisco IPICS Server Administration Guide Release 2.1\(1\)](#)』の付録「Configuring the Cisco IPICS RMS Component」を参照してください。

インストール前のチェックリスト

インストールを開始する前に、次の作業を必ず行ってください。

インストール前の作業	チェック 記入欄
Cisco IPICS インストールパッケージの CD がどちらも揃っていることを確認します。	<input type="checkbox"/>
サーバとモニタの電源コードがしっかりと接続され、電源に接続されていることを確認します。	<input type="checkbox"/>

インストール前の作業（続き）	チェック 記入欄
<p>サーバの Ethernet 0 (eth0) ポートに、イーサネット ネットワーク ケーブルを接続します。</p>	<input type="checkbox"/>
<p> (注) ネットワーク ケーブルは、サーバの eth0 インターフェイスに接続する必要があります。イーサネット インターフェイスのラベルが NIC 1 や NIC 2 となっているサーバの場合、通常は NIC 1 インターフェイスにイーサネット ケーブルを接続します。通常は、このインターフェイスが eth0 インターフェイスです。イーサネット インターフェイスのラベルが 1 や 2 となっているサーバについては、サーバに付属する製品マニュアルを参照して、そのサーバでのインターフェイスの表記を確認してください。いずれの場合も、使用するサーバの eth0 インターフェイスの位置について、作業前に確認しておくことをお勧めします。</p>	
<p>Cisco IPICS サーバのハードディスクに、使用可能な領域が 160 GB 以上あることを確認します。</p>	<input type="checkbox"/>
<p>シスコでは、システムに uninterruptible power supply (UPS; 無停電電源装置) を接続することを強くお勧めします。また、UPS が正常に動作していることを確認してください。</p>	<input type="checkbox"/>
<p>モニター ケーブルのコネクタが、サーバ上のコネクタと適合するものであることを確認します。Video Graphics Array (VGA) アナログと VGA デジタルはコネクタ タイプが共通ですが、適切なアダプタを使用しない限り互換性はありません。</p>	<input type="checkbox"/>
<p>インストールプロセスを開始する前に、モニターの電力設定を調べて、画面表示にタイムアウト値が設定されていないことを確認します。</p>	<input type="checkbox"/>
<p> (注) インストールの実行中に表示タイムアウトが発生し、進捗状況がモニターに表示されなくなった場合は、マウスを動かすと画面表示が回復します。キーボードのキーは、画面表示を回復させる目的では押さないでください。情報を画面に表示できない状態でキーを押すと、不要な処理が実行される場合があります。</p>	

インストール前の作業（続き）	チェック 記入欄
<p>Cisco IPICS サーバの IP アドレス、サブネット マスク、デフォルトゲートウェイ、および DNS サーバ（オプション）の情報をネットワーク管理者から入手しておきます。</p>	<input type="checkbox"/>
<p>Cisco IPICS サーバの eth0 インターフェ이스の Media Access Control (MAC; メディア アクセス制御) アドレスを確認しておきます。Cisco IPICS は、サーバの MAC アドレスを使用して Cisco IPICS ライセンスを検証します。MAC アドレスの確認方法については、P.2-8 の「Cisco IPICS オペレーティング システム ソフトウェアのインストール」の ステップ 30 を参照してください。</p> <p> (注) システムが複数の network interface card (NIC; ネットワーク インターフェイス カード) を備えている場合、eth0 が無効になっていても、Cisco IPICS は常に eth0 の MAC アドレスを使用してライセンスを検証します。</p>	<input type="checkbox"/>
<p>ネットワークで Network Time Protocol (NTP; ネットワーク タイム プロトコル) を使用している場合は、NTP サーバの IP アドレスまたは DNS 名を取得してください。</p> <p> (注) NTP は、Cisco IPICS オペレーティング システム ソフトウェアのインストール時に設定するか、あるいは Cisco IPICS ソフトウェアのインストール後に <code>ntpsetup</code> コマンドを使用して設定します。<code>ntpsetup</code> コマンドについては、『Cisco IPICS Troubleshooting Guide, Release 2.1(1)』の「Using the Cisco IPICS CLI Tools and Service Commands」の章の「Configuring NTP on the Cisco IPICS Server with the ntpsetup Tool」の項を参照してください。</p>	<input type="checkbox"/>
<p>サードパーティ証明書をインストールして、Cisco IPICS の自己署名証明書と置き換えることができます。サードパーティ証明書のインストールの詳細については、P.2-47 の「Cisco IPICS サーバへのサードパーティ証明書のインストール」を参照してください。Cisco IPICS では、サードパーティ証明書の使用は必須ではありません。</p>	<input type="checkbox"/>

Cisco IPICS を確実に動作させるには、Cisco IPICS のインストール前またはインストール後に次の作業も実施する必要があります。

作業	チェック 記入欄
<p>チャンネルおよび VTG に使用されるマルチキャスト IP アドレスを入手します（この情報を入手できない場合は、システム管理者に問い合わせてください）。</p>	<input type="checkbox"/>
<p>RMS の T1/E1 インターフェイスが、ループバック ケーブルで互いに接続されていることを確認します。このケーブルは、ピン割り当てが 1-4、2-5、4-1、5-2 となっている短いクロスケーブルです。ケーブルの一端を、RMS デバイスの T1/E1 インターフェイスにある各 RJ-45 コネクタに接続します。接続されたインターフェイスは、Cisco IPICS の SIP ベースのすべての接続において、音声のシグナリングとメディアに使用されます。クロスケーブルが手元にない場合は、シスコ認定サポート担当者にお問い合わせの上、入手してください。</p>	<input type="checkbox"/>
<p>ループバック ケーブルで接続された RMS インターフェイスのアドレスを入手します（この情報を入手できない場合は、システム管理者に問い合わせてください）。</p>	<input type="checkbox"/>

ダイヤルインとダイヤルアウトの機能を制御する Cisco IPICS ダイヤルエンジンを使用する場合は、ダイヤル エンジンの使用前に、次の作業を必ず実施してください。

作業	チェック 記入欄
<p>SIP プロバイダーの IP アドレス、SIP リスニング ポート、および優先トランスポート タイプを確認します。SIP ベースのダイヤル機能のサポートは、SIP プロバイダーとして Cisco Unified Communications Manager（または、サポートされているバージョンの Cisco IOS、および Cisco Unified Communications Manager Express を実行しているシスコルータ）によって提供されます。ポリシー エンジンでは、お客様のネットワークに SIP プロバイダーが設定されていることが要件になります。</p> <p>SIP プロバイダーの設定については、『Cisco IPICS Server Administration Guide, Release 2.1(1)』を参照してください。</p>	<input type="checkbox"/>
<p>SIP プロバイダーが Cisco Unified Communications Manager である場合は、Cisco IPICS が Cisco Unified Communications Manager へのコールの開始時に使用する認証クレデンシャルを決定します。</p> <p>Cisco Unified Communications Manager Express の場合、認証は必要ありません。</p>	<input type="checkbox"/>
<p>SIP プロバイダーが、サポートされているバージョンの Cisco Unified Communications Manager、Cisco IOS、および Cisco Unified Communications Manager Express を使用していることを確認します。Cisco IPICS での使用がサポートされているハードウェアおよびソフトウェアの最新のリストについては、『Cisco IPICS Compatibility Matrix』を参照してください。</p>	<input type="checkbox"/>
<p>Cisco IPICS システムが、SIP プロバイダーのダイヤルプランにどのように組み込まれているかを確認します。たとえば、SIP プロバイダーから Cisco IPICS システムまでルーティングされる必要のある電話番号 (DN) の範囲を特定します。</p>	<input type="checkbox"/>

Cisco IPICS オペレーティング システムのインストール

この項では、Cisco IPICS オペレーティング システムのインストールに必要な手順について説明します。この項では、次のトピックを扱います。

- [Cisco MCS 7825 サーバへのインストール時の警告事項 \(P.2-8\)](#)
- [Cisco IPICS オペレーティング システム ソフトウェアのインストール\(P.2-8\)](#)

Cisco MCS 7825 サーバへのインストール時の警告事項

Cisco IPICS オペレーティング システムを Cisco MCS 7825 サーバにインストールする場合は、次の点に注意してください。

- Cisco IPICS は、Cisco MCS 7825 サーバ上の Redundant Array of Inexpensive Disks (RAID; 冗長ディスクアレイ) をサポートしていません。Cisco MCS 7825 サーバで RAID が有効になっている場合は、オペレーティング システムをインストールする前に必ず無効にしてください。
- Cisco IPICS オペレーティング システムを Cisco MCS 7825-H1 サーバおよび Cisco MCS 7825-H2 サーバにインストールする場合は、Serial ATA (SATA) コントローラ オプションと Virtual Install Disk オプションを両方とも無効にして、RAID を無効にする必要があります。この作業は、Cisco IPICS オペレーティング システムを Cisco MCS 7845 サーバにインストールする場合は不要です。Cisco IPICS は、これらのサーバについては RAID をサポートしています。

RAID、Serial ATA コントローラ オプション、および Virtual Install Disk オプションを無効にするには、[P.2-8](#) の「[Cisco IPICS オペレーティング システム ソフトウェアのインストール](#)」にある手順の [ステップ 3](#) に従ってください。

Cisco IPICS オペレーティング システム ソフトウェアのインストール

Cisco IPICS オペレーティング システム 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。

手順

ステップ 1 サーバの前面パネルにある電源ボタンを押して、サーバの電源をオンにします。

ステップ 2 Cisco IPICS オペレーティング システムのインストール CD をサーバのディスクドライブに挿入します。

システムがブートを開始します。

Cisco IPICS オペレーティング システムを Cisco MCS 7825-H1 サーバまたは Cisco MCS 7825-H2 サーバにインストールする場合は、組み込みの SATA ソフトウェア RAID および Virtual Install Disk オプションを無効にする必要があります。

これらのモデル サーバでこれらの機能を無効にする手順は、[ステップ 3](#) を参照してください。



(注) 別の Cisco MCS 7825 サーバに Cisco IPICS をインストールする場合は、サーバに付属する製品マニュアルを参照して、RAID が有効になっているかどうかを確認し、RAID を無効にする手順を確認します。

Cisco IPICS オペレーティング システムを Cisco MCS 7845 サーバにインストールする場合は、これらの機能を無効にする必要はありません。[ステップ 5](#) に進むことができます。

ステップ 3 次の手順に従って、System Maintenance メニューに入ります。

- a. サーバのブート中は、サーバから聞こえてくる音を注意して聞き、モニタの表示内容を確認します。
- b. サーバからビープ音が聞こえて、「Press F10 key to enter System Maintenance Menu」というメッセージが表示されたら、**F10** キーを押します。

System Maintenance メニューが表示され、次のオプションが示されます。

- Setup Utility : サーバ コンポーネント (組み込みの SATA ソフトウェア RAID や Virtual Install Disk など) の設定を変更する設定ユーティリティにアクセスできます。
- Inspect Utility : サーバおよびサーバ コンポーネントの統計情報にアクセスできます (PCI Device Info や System Memory Map など)。
- Diagnostic Utility : メモリ テストや CPU テストなどの診断テストをサーバに対して実行するユーティリティが用意されています。

ステップ 4 System Maintenance メニューの **Setup Utility** を選択し、**Enter** キーを押して Setup Utility に入ります。

Setup Utility が表示されます。

- a. Setup Utility メニューで、↓ キーを押して **Advanced Options** を強調表示し、**Enter** キーを押します。

Advanced Options メニューが表示されます。

- b. ↓ キーを押して **Virtual Install Disk** を強調表示します。

Virtual Install Disk を強調表示すると、メニューの下に現在のステータスが表示されます。

- c. Virtual Install Disk のステータスに応じて、次のいずれかの操作を実行します。

— ステータスが **Disabled** と表示されている場合は、ステップ e. に進みます。

— ステータスが **Enabled** と表示されている場合は、Configuration Selection の値を変更します。選択内容を変更するには、**Enter** キーを押してメニューを開き、↓ キーを押して **Disabled** を選択および強調表示します。

- d. 選択内容を確定するには、**Enter** キーを押します。

Virtual Install Disk の設定が **Disabled** と表示されます。

- e. Advanced Options メニューで、↓ キーを押して **Embedded SATA RAID** または **Sata Software Raid** のいずれかを選択および強調表示します (SATA RAID オプションの表記は、サーバハードウェアによって異なります)。

現在のステータスがメニューの下に表示されます。

- f. ステータスが **Disabled** と表示されている場合は、ステップ h. 進みます。

Embedded SATA RAID または Sata Software Raid のステータスが **Enabled** と表示されている場合は、**Enter** キーを押してメニューを開き、↓ キーを押して **Disabled** を選択および強調表示します。

- g. 選択内容を確定するには、**Enter** キーを押します。

- h. **Esc** キーを 2 回押してメニューを閉じ、ユーティリティを終了します。

- i. **F10** キーを押して終了を確定し、変更内容を保存します。



(注) F10 キー以外のキーを押すと、Setup Utility のメイン メニューに戻ります。この場合は、Setup Utility の手順を [ステップ 4](#) から繰り返す必要があります。

CD からのブートが開始されます。ここでは、システムからビープ音が聞こえても CD からのブートを続行します。

Cisco IPICS オペレーティング システムの CD のバージョンと、ハードドライブの内容を上書きするオプションが表示されます。

ステップ 5 ハードドライブの内容を上書きして Cisco IPICS オペレーティング システムの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。

- a. ハードドライブの内容を上書きするように求められたら、**Y** と入力し、**Enter** キーを押します。



(注) インストール中は、SysRq キーを含めてキーを何も押さないでください。SysRq キーを押すと、サーバ上でカーネルパニック状態が発生し、修正するにはハードリブートが必要になります。

Cisco IPICS オペレーティング システムの Installation Progress ウィンドウに、インストールの進捗状況が表示されます。ファイル システムがフォーマットされ、ソフトウェア パッケージがインストールされます。



(注) パッケージのインストールが完了した後に、ウィンドウが無反応になったように見える場合や、画面表示が消える場合があります。システムがバックグラウンドでのセキュリティ プロセスを完了するまで、しばらく待機してください。

インストール CD が取り出され、Installation Complete ウィンドウが表示されます。

- b. CD をドライブから取り出します。



(注) オペレーティング システムの再インストールが必要になった場合に備え、インストール CD は安全な場所に保管しておいてください。

- c. Cisco IPICS オペレーティング システムのこのリリースに関する技術情報を参照する場合は、**Release Notes** をクリックするか、**Alt+R** キーを押します。



(注) カーソルが画面上で不自然に動き始めた場合は、オペレーティング システムに不適切なマウス ドライバがロードされている可能性があります。この状態になってマウス操作に支障が生じている場合は、キーボード ショートカットを使用してステップ c ～ステップ e を実行します。

ステータス ウィンドウではインストールの完了が報告されますが、Cisco IPICS サーバ ソフトウェアをインストールする前に、さらにいくつかの作業を行う必要があります。この手順の残りのステップを必ず実行して、Cisco IPICS オペレーティング システムの設定を完了してください。

- d. **Release Notes** のウィンドウを閉じるには、**X** をクリックするか、**Alt+C** キーを押します。

Release Notes ウィンドウが閉じます。

- e. ウィンドウを閉じてサーバをリブートするには、**Exit** をクリックするか、**Alt+E** キーを押します。

サーバがリブートします。

起動プロセス中に、Cisco IPICS ソフトウェア インストールが強調表示された状態で **GRUB** ウィンドウが表示されます。

- ステップ 6** **GRUB** ウィンドウが表示されたら、**Enter** キーを押して起動プロセスを続行します。または、何も操作しないでウィンドウをタイムアウトにします。

次のいずれかのウィンドウが表示されます。

- **Kudzu** ハードウェア検出ユーティリティのウィンドウが表示されます。このユーティリティでは、Cisco IPICS オペレーティング システムのインストール中に新しいハードウェアを検出し、設定することができます。
- **Welcome** ウィンドウが表示されます。**Welcome** ウィンドウ以降に表示される一連のウィンドウでは、Cisco IPICS のネットワーク設定情報を入力します。

ステップ 7 Kudzu ハードウェア検出ユーティリティのウィンドウが表示されたら、任意のキーを押します。



(注) 3,600 秒 (1 時間) 以内にキーを押す必要があります。押さない場合は Kudzu ウィンドウがタイムアウトします。Kudzu ウィンドウがタイムアウトした場合は、初期インストール プロセスの完了後に Kudzu ハードウェア検出ユーティリティを再度実行する必要があります。Kudzu ハードウェア検出ユーティリティを再実行する方法の詳細については、[P.5-3](#) の「Cisco IPICS がインストール中に NIC を検出できない」を参照してください。

ステップ 8 表示されるウィンドウに応じて、次のいずれかの手順を実行します。



(注) 表示されるウィンドウは、使用するハードウェア プラットフォームによって異なります。eth0 インターフェイスを設定するように初めて求められたときは、Dynamic Host Configuration Protocol (DHCP) を選択する必要があります ([ステップ 10](#) を参照)。この手順は、適切なドライバを確実にインストールするために必要です。次に、eth0 インターフェイスの DHCP 設定を固定 IP アドレスで上書きする必要があります ([ステップ 19](#) を参照)。eth1 インターフェイスを設定するように求められた場合は、必ず **Ignore the device** オプションを選択します。Cisco IPICS では、eth1 インターフェイスの使用をサポートしていません。

- システムに新しいNICが追加されたことを示すウィンドウが表示される場合は、[ステップ 9](#) に進んで eth0 インターフェイスを設定します。



(注) サーバへのネットワーク接続を有効にするには、eth0 インターフェイスを設定する必要があります。

- Intel SATA コントローラまたは Intel IDE コントローラのいずれかが検出されたことを示すウィンドウが表示される場合は、[ステップ 14](#) に進みます。
- Welcome ウィンドウが表示される場合は、[ステップ 15](#) に進みます。

ステップ 9 **Enter** キーを押して、次のオプション リストから **Configure** オプションを選択します。

- **Configure** : eth0 インターフェイスを制御する NIC を設定するには、このオプションを選択します。このオプションがデフォルトです。
- **Ignore the device** : サーバに追加する必要があるハードウェアが何もない場合は、このオプションを選択します。
- **Do nothing** : ハードウェアを設定しない場合は、このオプションを選択します。サーバをリブートすると、ハードウェアは新規にインストールされたものとして検出され、ハードウェアを設定するように求められます。

Cisco IPICS オペレーティング システムの設定プログラムによって、インターフェイス設定ウィンドウが表示されます。

ステップ 10 **Space** キーを押して、**Use dynamic IP/configuration (BOOTP/DHCP)** を選択します。

チェックボックス領域にアスタリスク (*) が表示され、DHCP の使用を選択していることが示されます。



(注)

この手順によって、サーバ上の eth0 インターフェイスを制御する NIC を Cisco IPICS オペレーティング システムで検出し、このインターフェイス用の適切なドライバをインストールできるようになります。Cisco IPICS は DHCP を使用しません。Cisco IPICS サーバのネットワーク接続を設定する場合は、固定 IP アドレスを使用する必要があります。固定 IP アドレスの設定は、[ステップ 19](#) で説明している Network Setup ウィンドウで行います。

ステップ 11 **Tab** キーを押すか、← キーと → キーを使用して **OK** を選択します。

ステップ 12 選択内容を受け入れるには、**Enter** キーを押します。

ステップ 13 別の NIC が検出されたことを示す 2 番目のウィンドウが表示される場合は、次の操作を実行して、eth1 インターフェイスの設定を無視します。

- a. **Tab** キーを押して **Ignore** を選択します。

b. **Enter** キーを押して設定を確認します。



(注) eth1 インターフェイスは設定しないでください。Cisco IPICS では、eth1 インターフェイスの設定をサポートしていません。

Cisco IPICS オペレーティング システムの設定プログラムでは、eth1 インターフェイスを設定しないまま処理が継続され、Intel コントローラを検出したことを示すウィンドウが表示されます。

ステップ 14 Intel SATA コントローラまたは Intel IDE コントローラのいずれかが検出されたことを示すウィンドウが表示される場合は、**Enter** キーを押して **Configure** オプションをそのまま使用し、コントローラを設定します。

コントローラが自動的に設定されます。

Cisco IPICS オペレーティング システムの Welcome ウィンドウが表示されます。

ステップ 15 Welcome ウィンドウで、**Next** をクリックします。

Root Password ウィンドウが表示されます。

ステップ 16 ルート ユーザのパスワードを入力します。

ルート ユーザは、Cisco IPICS サーバのすべてのファイルにアクセスできます。Cisco IPICS では、少なくとも 8 文字で、次の要素を含むセキュリティ性の高いパスワードを使用する必要があります。

- 1 文字以上の英小文字
- 1 文字以上の英大文字
- 1 文字以上の数字
- 1 文字以上の特殊文字（次のいずれか）：
@ [] ^ _ ` ! " # \$ % & ' () * + , - . / : ; { < | = } > ~ ?



(注) ルートのパスワードを後で変更する場合は、Cisco IPICS サーバにルートユーザとしてログインし、**reset_pw** コマンドを使用して変更します。詳細については、『[Cisco IPICS Troubleshooting Guide, Release 2.1\(1\)](#)』の「Using the Cisco IPICS CLI Tools and Service Commands」の章の「Resetting, Changing, or Creating a Password With the reset_pw Tool」の項を参照してください。

ステップ 17 パスワードを再度入力し、**Next** をクリックします。

Network Setup ウィンドウが表示されます。

DNS サーバの情報を入力するように求められます。

ステップ 18 Network Setup ウィンドウの DNS Information 領域で、プライマリ DNS およびセカンダリ DNS（存在する場合）、およびサーバのドメイン名を所定のフィールドに入力します。

ステップ 19 Ethernet Port 1 (device eth0) 領域で、サーバのホスト名、IP アドレス、サブネットマスク、およびデフォルト ゲートウェイを所定のフィールドに入力します。

ステップ 20 **Next** をクリックします。

Timezone ウィンドウが表示されます。

ステップ 21 選択リストの選択肢から、現在の地域の適切な時間帯を選択します。

システム クロックで Universal Coordinated Time (UTC; 世界標準時) を使用している場合は、**System Clock uses UTC** チェックボックスがオンになっていることを確認します。

ステップ 22 **Next** をクリックします。

Date and Time ウィンドウが表示されます。

ステップ 23 次のいずれかのアクションを実行して、システムの日付と時刻を設定できます。

- ネットワークでネットワーク タイム プロトコル (NTP) を使用している場合は、**Enable Network Time Protocol** チェックボックスをオンにして、Server フィールドに NTP サーバの名前または IP アドレスを入力してください。



(注)

サーバで NTP を設定する場合、システム管理者は、PMC クライアントマシンで Windows Time Service も設定して PMC とサーバ ログの間の同期を可能にするように、PMC ユーザに指示する必要があります。Windows Time Service の設定方法については、<http://support.microsoft.com/>にある Microsoft サポート サイトで文書番号 307897 を検索してください。

期間限定ライセンスをシステムにインストールする場合で、NTP を有効にする際は、注意が必要です。システムの日付の調整によって、Cisco IPICS でライセンスが無効にされる場合があります。詳細については、[P.2-44 の「期間限定ライセンスの管理」](#)を参照してください。

- ネットワークで NTP を使用しない場合は、現在の日付と時刻を該当するフィールドに入力してください。

ステップ 24 **Next** をクリックします。

Finish Setup ウィンドウが表示されます。

ステップ 25 **Next** をクリックします。

システムは、起動中に内部チェックリストを処理します。システムが起動すると、次のメッセージが表示されます。

Cisco IPICS

hostname login:

表示の意味は次のとおりです。

hostname は、[ステップ 19](#) で指定したホスト名を表しています。

ステップ 26 *hostname login*: フィールドに **root** と入力し、**Enter** キーを押します。

ルート ユーザのパスワードを入力するように求められます。

ステップ 27 **ステップ 16** で作成したルート ユーザのパスワードを入力し、**Enter** キーを押します。

ステップ 28 ネットワークの接続を確認するには、次のコマンドを入力します。

```
[root]# ping <destination-ip-address>
```

表示の意味は次のとおりです。

<*destination-ip-address*> は、デフォルト ゲートウェイのアドレス、またはネットワーク上にある別のホストの IP アドレスを表しています。

ステップ 29 **Ctrl+C** キーを押して、*ping* の実行を停止します。

ping で正常に応答が返らない場合は、ネットワーク管理者と連携して、ネットワーク接続の問題を解決してください。

ステップ 30 次の手順に従って、*eth0* インターフェイスのハードウェア MAC アドレスを確認します。

a. *eth0* インターフェイスの MAC アドレスを表示するには、次のコマンドを入力します。

```
[root]# ifconfig eth0
```

b. コマンド出力の *HWaddr* フィールドを確認します。

HWaddr フィールドに *eth0* インターフェイスの MAC アドレスが示されています。

c. *eth0* インターフェイスの MAC アドレス情報を書き留めて、Cisco IPICS のライセンスの取得に使用できるようにします。

d. サーバからログアウトするには、次のコマンドを入力します。

```
[root]# exit
```

Cisco IPICS オペレーティング システムのインストールはこれで完了です。Cisco IPICS サーバソフトウェアのインストールを続行できます。Cisco IPICS をすぐにインストールしない場合は、後でインストールを再開できます。

Cisco IPICS サーバソフトウェアをインストールするには、「[Cisco IPICS サーバソフトウェアのインストール](#)」の項を参照してください。

Cisco IPICS サーバソフトウェアのインストール

Cisco IPICS オペレーティング システムが正常にインストールされたら、次の方法のいずれかを使用して、Cisco IPICS サーバソフトウェアをインストールします。

- Cisco IPICS サーバでインストール CD を使用して、直接インストールする
- インストーラ ファイルをサーバにコピーし、リモート コマンドを入力して、リモートでインストールする

Cisco IPICS サーバインストール プログラムは、テキストベースのインターフェイスを使用します。graphical user interface (GUI; グラフィカル ユーザ インターフェイス) はサポートしていません。このインストール手順を使用すると、次のインストール オプションから選択できます。

- Install : Cisco Security Agent (CSA) を含めて Cisco IPICS サーバソフトウェアをインストール。
- Upgrade : サーバを Cisco IPICS の以前のバージョンからアップグレード。Cisco IPICS サーバソフトウェアのアップグレードの実行については、[第3章「Cisco IPICS のアップグレード」](#)を参照してください。



(注)

インストーラが表示するオプションは、システムで実行されている現在のソフトウェアバージョンによって異なります。

この項では、次のトピックを扱います。

- [Cisco IPICS サーバソフトウェアの直接インストールの実行 \(P.2-20\)](#)
- [Cisco IPICS サーバソフトウェアのリモートインストールの実行 \(P.2-25\)](#)

Cisco IPICS サーバソフトウェアの直接インストールの実行

Cisco IPICS サーバに物理的にアクセスできる場合は、サーバソフトウェアをサーバ上で直接インストールできます。直接インストールを実行するには、製品パッケージに同梱されている Cisco IPICS インストール CD が必要です。



(注)

Cisco IPICS のインストールを実行するには、ルート ユーザとしてログインする必要があります。他のユーザ ID を使用してインストールを実行しようとすると、エラーが返されてインストールが終了します。



ヒント

インストールプロセスを途中で終了するには、**Ctrl+C** キーを押します。

Cisco IPICS サーバソフトウェアをサーバ上で直接インストールするには、次の手順を実行します。

手順

ステップ 1 端末のコンソールで、*hostname login:* フィールドに **root** と入力し、**Enter** キーを押します。

ルート ユーザのパスワードを入力するように求められます。

ステップ 2 P.2-8 の「Cisco IPICS オペレーティング システム ソフトウェアのインストール」の **ステップ 16** で作成したルート ユーザのパスワードを入力し、**Enter** キーを押します。

ルート ユーザとして Cisco IPICS オペレーティング システムにログインした状態になります。

ステップ 3 `free` コマンドを入力して、`total` カラムに表示される情報を読み、搭載されているメモリの総容量を確認します。

Cisco IPICS をインストールするには、少なくとも 2 GB のメモリが必要です。

次の例は、サーバに少なくとも 2 GB のメモリがあることを示しています。

```
[root]# free
              total            used             free             shared           buffers           cached
Mem:  2055340            881152          1174188                0             25520            389028
-/+ buffers/cache:           466604           1588736
Swap:           2048248                0           2048248
```

サーバが十分な容量のメモリを搭載していない場合は、シスコの代理店に問い合せて、追加メモリのご購入方法を確認してください。具体的なメモリ要件については、『[Cisco IPICS Compatibility Matrix](#)』を参照してください。

ステップ 4 Cisco IPICS サーバの CD ドライブに、Cisco IPICS のインストール CD を挿入します。

ステップ 5 次のコマンドを入力して、CD の内容をサーバにマウントします。

```
[root]# mount /mnt/cdrom
```

ステップ 6 CD のロケーションに移動するには、次のコマンドを入力します。

```
[root] #cd /mnt/cdrom
```

ステップ 7 インストーラ ファイルを表示するには、次のコマンドを入力します。

```
[root] #ls -l
```

CD のディレクトリが表示されます。

ステップ 8 インストーラ ファイルをディレクトリ リストで確認します。

Cisco IPICS のインストーラ ファイルには `.run` というファイル拡張子が付いています。

ステップ 9 インストールを開始するには、次のコマンドを入力します。

```
[root]# bash <installerfilename>.run
```

表示の意味は次のとおりです。

<installerfilename>.run には、[ステップ 7](#) で確認したインストーラ ファイルの名前を指定します。

インストール プロセスが開始されます。

処理の続行には、エンド ユーザ ライセンス契約 (EULA) を読んで同意する必要があることを通知するメッセージが表示されます。

ステップ 10 **Enter** キーを押して EULA を表示します。

Cisco IPICS インストーラに EULA が表示されます。

ステップ 11 **Space** キーを押して EULA をスクロールし、全文を読みます。EULA に同意する場合は、**y** または **yes** と入力してインストールを続行します。

処理を続行するには、EULA にご同意いただく必要があります。



(注) EULA が表示されている間にインストールを終了するには、**Ctrl+C** キーを押します。インストール プログラムが EULA の全文を表示した後、インストールが終了します。EULA の表示を省略してインストール プロセスを終了するには、**q** キーを押します。

ipics ユーザのパスワードを入力するように求められます。ipics ユーザは、Cisco IPICS Administration Console を使用して、管理に関連するすべての作業を実行できます。

ステップ 12 ipics ユーザのパスワードをパスワード フィールドに入力します。

セキュリティ性の高いパスワードにするには、少なくとも 8 文字にし、次の文字をそれぞれ 1 文字以上含むパスワードを使用します。

- 1 文字の英小文字
- 1 文字の英大文字
- 1 文字の数字
- 次のいずれかの特殊文字：
@ [] ^ _ ` ! " # \$ % & ' () * + , - . / : ; { < | = } > ~ ?

**(注)**

インストール プログラムは、ランダム アルゴリズムを使用することによって、informix linux ユーザ用のパスワードも作成します。informix ユーザには、Informix データベース インスタンスに関するフル管理権限が与えられます。これらのユーザは、ipics および informix linux グループに属します。ipics linux グループには、Cisco IPICS アプリケーション関連のフォルダ、ファイル、およびスクリプトに関する権限が含まれています。informix linux グループには、Cisco IPICS データベース サーバのフォルダ、ファイル、スクリプトに関するフル権限が含まれています。このユーザ ID のパスワードは、無期限に有効になります。

ステップ 13 パスワードを再度入力し、**Enter** キーを押します。

Cisco IPICS の ipicsadmin (管理) ユーザのパスワードを入力するように求められます。ipicsadmin ユーザは ipics linux グループに属します。また、ipicsadmin ユーザは Informix データベースに対するデータの読み取り権限と書き込み権限が与えられます。

ステップ 14 パスワード フィールドにパスワードを入力して、ipicsadmin ユーザのパスワードを作成します。

セキュリティ性の高いパスワードにするには、少なくとも 8 文字にし、次の文字をそれぞれ 1 文字以上含むパスワードを使用します。

- 1 文字の英小文字
- 1 文字の英大文字
- 1 文字の数字
- 次のいずれかの特殊文字：
@ [] ^ _ ` ! " # \$ % & ' () * + , - . / : ; { < | = } > ~ ?



(注) ipicsadmin ユーザのパスワードは、無期限に有効になります。

ステップ 15 インストールプロセスを開始するには、**y** または **yes** を入力します。

インストールプロセスが開始されます。

経過表示バーが表示され、インストールの進捗率が示されます。

ステップ 16 ファイルのインストールが完了すると、ステータスを通知するメッセージが表示されます。

次のテキストは、インストールが正常に完了した場合に表示されるメッセージの例です。

```
"The installation has completed successfully."
```

```
    You can view the installation log file by navigating  
    to the following directory:
```

```
"/var/opt/CSCOipics/run/20061018092707/ipics-install-log.txt"
```

```
    To complete the installation, you must reboot your server.  
Do you want to reboot now? (YES/NO): [YES]
```

ステップ 17 **YES** と入力して、サーバをリブートします。

サーバがリブートし、Cisco IPICS サーバを使用できる状態になります。



(注) **NO** を入力する場合は、Cisco IPICS にログインする前に再起動してください。Tomcat サービスやデータベース サーバなどの Cisco IPICS プロセスは、サーバをリブートするまでは起動しません。

サーバを後でリブートする場合は、[P.2-30](#) の「サーバの再起動またはシャットダウン」の手順に従ってください。

Cisco IPICS サーバソフトウェアのリモートインストールの実行

この項では、ネットワークにリモートで接続されている PC から Cisco IPICS をインストールする場合の手順について説明します。

Cisco IPICS サーバソフトウェアをリモート ロケーションからインストールするには、次の手順を実行します。

手順

ステップ 1 インストーラ ファイルを Cisco IPICS インストール CD から Cisco IPICS サーバに転送します。転送するには、次のいずれかのタスクを実行します。

- CD を Cisco IPICS サーバに挿入し（または、他の人に挿入を依頼し）、インストーラ ファイルをサーバにコピーします。この手順を実行するには、[ステップ 2](#) で説明している手順に従います。
- CD を PC に挿入し、Secure Shell (SSH) Client ソフトウェア（または同等の機能を備えたソフトウェア）などの File Transfer Protocol (FTP; ファイル転送プロトコル) クライアント ソフトウェア プログラムを使用して、インストーラ ファイルを Cisco IPICS サーバに転送します。この手順を実行するには、[ステップ 3](#) で説明している手順に従います。

ステップ 2 インストーラ ファイルを CD からコピーするには、次の手順を実行します。

- a. Cisco IPICS インストール CD をサーバのディスク ドライブに挿入します。
- b. **Start > Programs > SSH Secure Shell > Secure Shell Client** を選択して、Cisco IPICS サーバにリモートで接続します。



(注) SSH のアイドル タイムアウト値は、120 分（2 時間）です。このため、SSH のリモート接続セッションを 2 時間以上放置してセッションをタイムアウトさせないでください。



ヒント

Secure Shell Client が PC にインストールされていない場合は、別のセキュア クライアント プログラムを使用してください。

- c. **Quick Connect** をクリックして、Cisco IPICS サーバに接続します。
Connect to Remote Host ウィンドウが表示されます。
- d. Host フィールドに Cisco IPICS サーバの DNS ホスト名または IP アドレスを入力してから、**Tab** キーを押します。
- e. User Name フィールドに **root** と入力します。
- f. **Connect** をクリックします。
Enter Password ウィンドウが表示されます。
- g. ルート ユーザのパスワードを入力し、**OK** をクリックします。
SSH Secure Shell Client ソフトウェアのウィンドウが表示されます。
- h. 次のコマンドを入力して、CD の内容をサーバにマウントします。

```
[root]# mount /mnt/cdrom
```



(注) インストールプロセス中に CD にアクセスすると、**cdrom_decode_error** などのエラー メッセージが表示される場合があります。これらのメッセージは、Cisco IPICS サーバのインストールおよび動作には影響しませんので、無視してかまいません。

- i. 次のコマンドを入力して、CD の **cdrom** サブフォルダに移動します。

```
[root] #cd /mnt/cdrom
```
- j. インストーラ ファイルを表示するには、次のコマンドを入力します。

```
[root] #ls -l
```


CD のディレクトリが表示されます。
- k. インストーラ ファイルをディレクトリ リストで確認します。
Cisco IPICS のインストーラ ファイルには **.run** というファイル拡張子が付いています。
- l. 次のコマンドを入力して、インストーラ ファイルを /root ディレクトリにコピーします。

```
[root]# cp /mnt/cdrom/<installerfilename>.run /root
```


表示の意味は次のとおりです。
<installerfilename>.run は、ステップ j で表示された .run ファイルの名前を表しています。
インストーラ ファイルが CD から /root ディレクトリにコピーされます。

- m. 次のコマンドを入力して、**/mnt/cdrom** ディレクトリからサーバ上の内部ディレクトリに移動します。
- ```
[root]# cd <serverdirectory>
```
- 表示の意味は次のとおりです。
- <serverdirectory> は、サーバ上の内部ディレクトリまたはサブディレクトリです。
- n. インストール CD をアンマウントし、ディスク ドライブから取り出すには、次のコマンドを入力します。
- ```
[root]# eject
```



(注) **/mnt/cdrom** ディレクトリから移動し、**eject** コマンドを入力して CD の内容をアンマウントし、サーバから CD を取り出す必要があります。イジェクト ボタンを押して CD を取り出そうとしても、CD は取り出せません。

ステップ 3 ファイルをリモート ロケーションからサーバに転送するには、次の手順に従います。

- a. Cisco IPICS インストール CD を PC の CD ドライブに挿入します。
- b. **Start > Programs > SSH Secure Shell > Secure File Transfer Client** を選択して、Secure File Transfer Client を開きます。



(注) PC に Secure File Transfer Client がインストールされていない場合は、PC とサーバの間でセキュアなファイル転送セッションを実行できる、その他のプログラムを使用してください。

SSH Secure Shell の File Transfer Client ウィンドウが表示されます。PC のデスクトップが左側のペインに表示されます。

- c. **Quick Connect** をクリックして、Cisco IPICS サーバに接続します。
Connect to Remote Host ウィンドウが表示されます。
- d. Host フィールドに、Cisco IPICS サーバの DNS ホスト名または IP アドレスを入力します。次に、**Tab** キーを押します。
- e. User Name フィールドに **root** と入力します。

- f. **Connect** をクリックします。
Enter Password ウィンドウが表示されます。
- g. ルート ユーザのパスワードを入力し、**OK** をクリックします。
SSH Secure Shell の File Transfer Client が Cisco IPICS サーバに接続し、/root ディレクトリの内容をウィンドウの右側のペインに表示します。
- h. ウィンドウの左側のペインで、Cisco IPICS インストール CD のロケーションに対応する PC 上のフォルダに移動します (**My Computer\Compact Disk Z:** など)。
- i. **CD** フォルダをダブルクリックして、CD の内容を参照します。
CD の内容が表示されます。
- j. **cdrom** サブフォルダをダブルクリックして、フォルダの内容を参照します。
- k. CD の **cdrom** サブフォルダにあるインストーラ ファイルを確認します。
インストーラ ファイルは、拡張子が **.run** になっています。
- l. ウィンドウの左側のペインから右側のペインに向かってインストーラ ファイルをドラッグし、コピー プロシージャを開始します。
ファイルがサーバの /root ディレクトリにコピーされている間は、進捗ウィンドウが表示されます。コピー プロシージャが完了すると、インストーラ ファイルが右側のペインに表示されます。
- m. SSH Secure Shell の File Transfer Client を閉じます。

ステップ 4 SSH Secure Shell Client ソフトウェアまたは同等の機能を備えたソフトウェアを使用して、Cisco IPICS サーバにアクセスするターミナル ウィンドウを開きます。

ステップ 5 User Name フィールドに **root** と入力します。

ステップ 6 **Connect** をクリックします。

Enter Password ウィンドウが表示されます。

ステップ 7 ルート ユーザのパスワードを入力し、**OK** をクリックします。

SSH Secure Shell Client ソフトウェアのウィンドウが表示されます。

ステップ 8 インストーラ ファイルを表示するには、次のコマンドを入力します。

```
[root] #ls -l
```

/root ディレクトリの内容が表示されます。

ステップ 9 インストーラ ファイルをディレクトリ リストで確認します。

Cisco IPICS のインストーラ ファイルには `.run` というファイル拡張子が付いています。

ステップ 10 次のコマンドを入力して、インストーラ ファイルのアクセス モードを変更します。

```
[root]# chmod 550 <installerfilename>.run
```

表示の意味は次のとおりです。

`<installerfilename>.run` は、インストーラ ファイルの名前を表しています。



(注) このコマンドを入力すると、ルート ユーザ ID でインストーラ ファイルを読み取り、実行できます。

ステップ 11 SSH Secure Shell Client ソフトウェア（または同等の機能を備えたソフトウェア）ウィンドウからインストーラを実行するには、「[Cisco IPICS サーバソフトウェアの直接インストールの実行](#)」の項で説明されている手順を参照し、[P.2-22](#) の [ステップ 9](#) から実行してください。

サーバの再起動またはシャットダウン

サーバを再起動するには、次の手順を実行します。



注意

サーバをシャットダウンまたは再起動するときは、ユーザの通信がすべて終了することに注意してください。また、Administration Console にログインしているユーザもすべてログアウトされます。このため、サーバのシャットダウンまたは再起動は、メンテナンス時間帯、またはシステムが使用されないその他の期間だけにしてください。

手順

ステップ 1 次のいずれかの操作を実行して、Cisco IPICS サーバにルート ユーザ ID でログインします。

- サーバにサーバ コンソールからログインするには、次の手順に従います。
 - a. ユーザ名に **root** と入力して、サーバにログインします。
 - b. パスワードの入力を求められたら、ルート ユーザのパスワードを入力します。
- サーバにリモートでログインするには、次の手順に従います。
 - a. SSH Secure Shell Client ソフトウェアまたは同等の機能を備えたソフトウェアを使用して、ターミナル ウィンドウを開きます。
 - b. サーバの IP アドレスまたはホスト名を入力して、サーバにログインします。
 - c. ユーザ名として **root** と入力し、ルート ユーザ ID でログインします。
 - d. パスワードの入力を求められたら、ルート ユーザのパスワードを入力します。

ターミナル ウィンドウが表示されます。

ステップ 2 サーバをリブートするには、次のコマンドを入力します。

```
[root]# reboot
```

サーバがリブートします。

サーバをシャットダウンするには、次の手順を実行します。



(注)

サーバは、電源ボタンを押してシャットダウンせずに、次の手順を実行して正常にシャットダウンすることをお勧めします。

手順

ステップ 1 ルート ユーザ ID を使用して Cisco IPICS サーバにログインします。

ターミナル ウィンドウが表示されます。

ステップ 2 サーバで実行中のプロセスをシャットダウンするには、次のコマンドを入力します。

```
[root]# shutdown -h <time>
```

表示の意味は次のとおりです。

<time> は、シャットダウン スクリプトの実行を開始するまでの待ち時間（秒単位）です。



ヒント

実行中のプロセスをただちにシャットダウンするには、次のコマンドを入力します。

```
[root]# shutdown -h now
```

実行中のプロセスが終了します。サーバに直接接続されている場合は、各プロセスが終了すると、コンソールにその都度メッセージが表示されます。

ステップ 3 シャットダウン スクリプトが完了するのを待ってから、サーバの前面パネルにある電源ボタンを押して、サーバの電源をオフにします。

サーバをオフにする前に、次のいずれかのアクションを実行して、シャットダウン スクリプトが完了していることを確認してください。

- サーバにコンソール接続で直接接続されている場合は、次のメッセージが表示されるまで待機します。

Power down.

- サーバにリモートで接続している場合は、すべてのプロセスが確実に終了するまで、約 5 分間待機します。



(注) サーバが設置されている場所で、サーバの電源を手動でオフにする必要があります。サーバの電源を CLI コマンドでオフにすることはできません。

サーバがシャットダウンします。

Cisco IPICS を使用する準備

ソフトウェアのインストールを完了したら、Cisco IPICS を使用する前に、次のタスクを完了する必要があります。

- [インストールの確認 \(P.2-33\)](#)
- [ライセンスと証明書の管理 \(P.2-35\)](#)
- [ライセンスの要約情報の表示 \(P.2-41\)](#)
- [Cisco IPICS サーバへのサードパーティ証明書のインストール \(P.2-47\)](#)
- [Cisco IPICS PMC アプリケーションのインストーラの生成 \(P.2-54\)](#)

Cisco IPICS のその他の管理作業および設定作業については、『[Cisco IPICS Server Administration Guide Release 2.1\(1\)](#)』を参照してください。

インストールの確認

Cisco IPICS サーバソフトウェアのインストールを完了した後は、サポートされているブラウザを使用してログインすると、Cisco IPICS Administration Console にアクセスできます。Administration Console には、次の要件を満たす任意のコンピュータからアクセスできます。

- Cisco IPICS サーバに IP で接続できる
- 次のいずれかのオペレーティング システムを実行している
 - Windows 2000 SP4 以降
 - Windows XP SP2 以降
- Internet Explorer Version 6.0.2 を実行している



(注)

Cisco IPICS サーバが再起動してからユーザが Administration Console にアクセスできるようになるまでに、数分間かかることがあります。

Cisco IPICS Administration Console にアクセスしてインストールを確認するには、次の手順を実行します。

手順

- ステップ 1** PC で、サポートされているインターネット ブラウザのウィンドウを開きます。
- ステップ 2** Address フィールドに、[P.2-8](#) の「[Cisco IPICS オペレーティング システムのインストール](#)」で Cisco IPICS サーバに対して設定した固定 IP アドレスまたは DNS 名のいずれかを含む HTTP over Secure Socket Layer (HTTPS) URL を入力します。

URL は、次の形式で入力してください。

https://<ipaddress>|<dnsname>

表示の意味は次のとおりです。

<ipaddress> はサーバの IP アドレス、<dnsname> はサーバに対して設定したホスト名です。

Security Alert ウィンドウが表示されます。



(注) Security Alert ウィンドウが表示されるのは、Cisco IPICS に添付されている自己署名証明書が、Certificate Authority (CA; 認証局) から発行されたものではないためです。この自己署名証明書を CA から発行されたサードパーティ証明書に置き換える場合は、[P.2-47](#) の「[Cisco IPICS サーバへのサードパーティ証明書のインストール](#)」の手順に従います。

- ステップ 3** Yes をクリックしてウィンドウを閉じ、ログイン画面にアクセスします。
- ステップ 4** ipics ユーザの ID とパスワードを使用してログインします。



(注) ipics ユーザ ID はアプリケーション レベルのユーザ ID であり、Administration Console を使用して、管理に関連するすべての作業を実施できます。

Administration > License Management ウィンドウに、システムの使用前にライセンス ファイルをアップロードするよう指示するメッセージが表示されます。

ライセンス ファイルを取得するには、[P.2-36](#) の「ライセンス ファイルの取得」を参照してください。

Cisco IPICS にブラウザからアクセスできない場合は、[P.5-13](#) の「ブラウザを使用してサーバに接続できない」を参照してください。

ライセンスと証明書管理

Cisco IPICS のインストール後は Administration Console にログインできます。ただし、ライセンス ファイルをアップロードするまではどの機能も使用できません。ライセンス ファイルを取得するには、Cisco IPICS の製品パッケージに添付されている Product Authorization Key (PAK) を使用します。

ご購入いただいたライセンスは、ライセンスの対象となる次の機能の総数に基づいています。

- 同時使用の land mobile radio (LMR; 陸上移動無線) ポートの数
- 同時使用マルチキャスト ポートの数
- 同時使用 PMC ユーザの数
- 同時使用 IP Phone ユーザの数
- 同時使用ダイヤル ユーザの数
- ops ビューの総数



(注) ポリシー エンジンを使用可能にするには、専用のライセンスが必要です。

LMR ポート、マルチキャスト ポート、PMC ユーザ、IP Phone ユーザ、ダイヤル ユーザ、および ops ビューの総数は、ご購入いただいたライセンス (複数の場合もあります) で指定された数を超えることはできません。追加のライセンスが必要な場合は、シスコの代理店にお問い合わせください。

この項では、次のトピックを扱います。

- [ライセンス ファイルの取得 \(P.2-36\)](#)
- [Cisco IPICS ライセンス ファイルのアップロード \(P.2-38\)](#)

ライセンス ファイルの取得

Cisco IPICS の製品パッケージには、PAK を含む Software License Claim Certificate が添付されています。この証明書は、ご発注ごとに個別に作成されます。インストールした Cisco IPICS のライセンスを取得するには、このキーを使用します。

初期ライセンスは、インストール プロセスを開始した後にいつでもご注文いただけます。



注意

Cisco IPICS Release 1.0 からアップロードする場合、現在ご使用のライセンスは Cisco IPICS Release 2.1(1) と互換性がありません。シスコの代理店にお問い合わせいただき、Cisco IPICS Release 2.1(1) の新しいライセンスを取得してください。リリース 2.0(2) からアップグレードする場合は、Cisco IPICS リリース 2.1(1) で有効な現在のライセンスを使用できます。

PAK を使用して Cisco IPICS のライセンスを取得するには、次の手順を実行します。

手順

- ステップ 1** Cisco IPICS の製品パッケージに添付されている Software License Claim Certificate を用意します。この証明書の末尾にある PAK を確認します。



(注) Cisco IPICS サーバ ソフトウェアをシスコに直接ご注文いただいた場合、パッケージに添付されている PAK は 1 つだけです。代理店または小売店を通じて Cisco IPICS をご購入いただいた場合は、パッケージごとにそれぞれ固有の PAK があります。この場合は、すべての PAK を個別に処理する必要があります。シスコからは、PAK ごとにライセンス ファイルが送信されます。

ステップ 2 Cisco IPICS オペレーティング システムのインストール中に書き留めた MAC アドレスを確認します。

MAC アドレスを紛失した場合は、P.2-8 の「Cisco IPICS オペレーティング システム ソフトウェアのインストール」のステップ 30 の作業を行って入手します。

ステップ 3 次の URL で Cisco.com にアクセスして、ライセンスを注文します。

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

この URL にアクセスするには、有効な Cisco.com ユーザ ID とパスワードが必要です。

ライセンス注文を処理すると、ライセンス ファイルの添付された電子メールが Cisco.com から送信されます。複数の PAK を Cisco.com で処理した場合は、返信の電子メールが複数送信され、それぞれにライセンス ファイルが添付されます。これらのファイルをアップロードすると、Cisco IPICS はライセンスを各ファイルから抽出して追加し、集約されたライセンス ファイルに基づいてシステムの動作を監視します。

ステップ 4 次の手順を実行して、ライセンス ファイル（複数可）を PC に保存します。

- a. ライセンス ファイルの添付された電子メールを開きます。
- b. 電子メールに添付されているライセンス ファイルを右クリックします。
- c. **Save As** をクリックします。
Save Attachment ウィンドウが表示されます。
- d. ライセンス ファイルのダウンロード先となる PC 上のフォルダを選択します。
- e. Save Attachment ウィンドウのフィールドに、次の値が表示されていることを確認します。
 - File name フィールドに、ライセンスのファイル名がファイル タイプ .lic として表示されている。
 - Save as type フィールドに、**All Files (*.*)** が表示されている。
- f. **Save** をクリックします。
ライセンス ファイルが PC にダウンロードされます。



(注) Cisco IPICS では、ライセンス ファイルの名前やファイル タイプの編集および変更をサポートしていません。ライセンス ファイルの名前を変更した場合や、.lic 以外の拡張子を使用した場合は、ライセンスが無効になり、システムが動作不能になることがあります。

ステップ 5 Cisco IPICS ライセンスをアップロードします。

Cisco IPICS ライセンス ファイルのアップロード手順については、[P.2-38](#) の「[Cisco IPICS ライセンス ファイルのアップロード](#)」を参照してください。

ライセンス ファイルをアップロードすると、ライセンス マネージャが新しいライセンスを処理し、ライセンスの総数を更新します。

ステップ 6 追加のライセンスが必要な場合は、代理店または小売店にお問い合わせの上、ライセンスをご購入ください。

Cisco IPICS ライセンス ファイルのアップロード

ライセンス ファイルを受信した後は、Cisco IPICS Administration Console の **Administration > License Management** ウィンドウにアクセスしてライセンス ファイルをアップロードできます。



(注) ライセンス ファイルをアップロードすると、Cisco IPICS によって次のディレクトリに配置されます。
`/root/tomcat/current/webapps/license`

ライセンス ファイルをアップロードするには、次の手順を実行します。

手順

- ステップ 1** PC で、サポートされているブラウザ ウィンドウを開きます。
- ステップ 2** ブラウザの Address フィールドに、Cisco IPICS サーバの IP アドレスまたは DNS 名を含む HTTPS URL を次の形式で入力します。

`https://<ipaddress>|<dnsname>`

表示の意味は次のとおりです。

<ipaddress> はサーバの IP アドレス、<dnsname> はサーバに対して設定したホスト名です。

Security Alert ウィンドウが表示されます。

- ステップ 3** **Yes** をクリックしてウィンドウを閉じ、ログイン画面にアクセスします。

Cisco IPICS Login ウィンドウが表示されます。

- ステップ 4** ipics ユーザの ID とパスワードを使用して、Cisco IPICS サーバにログインします。

ライセンス ファイルをアップロードするように求められます。



(注) ライセンス ファイルを以前にアップロードした場合は、ライセンス ファイルのアップロードを求められません。ライセンス ファイルをアップロードするように求められなかった場合は、Administration Console の **Server** タブで **Administration > License Management** に移動します。

License Management ウィンドウが表示されます。

- ステップ 5** **Browse** をクリックし、PC にダウンロードしたライセンス ファイルの位置に移動します。

- ステップ 6** ライセンス ファイルを選択し、**Open** をクリックします。

ステップ 7 Upload をクリックして、ライセンス ファイルをサーバにアップロードします。

ライセンス マネージャが新しいライセンスを処理します。

ステップ 8 Apply をクリックします。

Cisco IPICS がライセンス ファイルをサーバに関連付けて、ライセンス マネージャを再起動します。更新されたライセンス情報が、License Management ウィンドウの License Summary ペインに表示されます。



(注) **Apply** をクリックしてから Administration Console にアクセスできるようになるまでに、数分間かかることがあります。

ステップ 9 ライセンス ファイルが複数ある場合は、[ステップ 5](#)～[ステップ 8](#)を繰り返して、すべてのライセンス ファイルをアップロードします。



ヒント アップロード プロセスの進行を追跡しやすくするため、ライセンス ファイルは 1 つずつアップロードし、その都度 **Apply** をクリックすることをお勧めします。



(注) Cisco IPICS は、古いライセンス ファイルを新しいライセンス ファイルで上書きするわけではありません。新しいライセンスを取得することによって、追加機能を購入できます。新しいライセンスをアップロードして適用すると、Cisco IPICS は、新しいライセンス機能を既存のライセンス機能に追加します。

ベストプラクティスとして、(期間限定ライセンスを永久ライセンスに置き換えた場合など) ライセンスを変更したときは必ず、古いライセンス ファイルを削除することをお勧めします。期間限定ライセンスの削除については、[P.2-45](#) の「古い期間限定ライセンスをサーバから削除」を参照してください。

ライセンスの要約情報の表示

Administration Console で **Administration > License Management > Summary** タブから License Summary ペインにアクセスすると、システムのライセンス取得済みの機能を表示できます。このペインには、Cisco IPICS のベース サーバライセンスとポリシー エンジンのベース ライセンスのライセンス情報も表示されます。

Cisco IPICS の機能がライセンスのある使用可能な機能をどのように使用するかについては、[P.2-42](#) の「[ライセンスの使用状況の追跡](#)」を参照してください。



(注)

License ブラウザ ウィンドウに表示されるデータは、ライセンス ウィンドウに最後にアクセスした時点の使用状況を示しています。最新のライセンス情報を表示するには、ブラウザ ウィンドウをリフレッシュします。ブラウザ ウィンドウは、期間を空けずにリフレッシュし、サーバ管理機能の実行前にもリフレッシュして、最新の情報が表示された状態で作業してください。最新のデータが表示されていないウィンドウで管理アップデートを実行しようとする、アップデートは成功せずエラーが表示されます。エラーが表示される場合は、ブラウザ ウィンドウをリフレッシュし、操作を再度実行します。

この項では、次のトピックを扱います。

- [ライセンスの使用状況の追跡 \(P.2-42\)](#)
- [期間限定ライセンスの管理 \(P.2-44\)](#)

ライセンスの使用状況の追跡

ポート、PMC、IP Phone、ポリシー エンジン、および ops ビューの使用によるライセンス使用状況を特定する Cisco IPICS での基準について、表 2-1 で説明します。

表 2-1 Cisco IPICS ライセンスの使用基準


フィールド	説明
Concurrent LMR Ports	<p>有効になっているチャンネルまたは無線は、LMR ポート ライセンスを使用します。管理者がチャンネルまたは無線を無効にすると、LMR ライセンスは解放され、使用可能な状態になります。</p> <p>無線とチャンネル セレクタの組み合わせをチャンネルと関連付けても、ライセンス使用状況には影響しません。</p> <p>Cisco IPICS でチャンネルのライセンスが使用される対象は、マルチキャスト アドレスとロケーションの一意の組み合わせです。チャンネルがマルチキャスト アドレスを 2 つ使用する場合は、単一のチャンネルが 2 つのライセンスを使用します。管理者がマルチキャスト アドレスを 1 つ削除すると、ライセンスが 1 つ解放され、ポートが使用するライセンスは 1 つになります。</p>
Concurrent Multicast Ports	<p>アクティブな VTG は、マルチキャスト ポート ライセンスを使用します。管理者が VTG を非アクティブにすると、マルチキャスト ライセンスは解放され、使用可能な状態になります。</p> <p> (注) アクティブではない VTG は、ポリシーがその VTG を起動した (アクティブになった) 場合、ライセンスを使用することに注意してください。このため、ライセンス数を超過している場合、ポリシーは VTG をアクティブにできません。サーバ上に、ポリシーの設定に対して十分な数の使用可能ライセンスがあることを確認してください。</p>

表 2-1 Cisco IPICS ライセンスの使用基準 (続き)


フィールド	説明
Concurrent PMC Users	<p>PMC ユーザは、PMC セッションにログインすると、その都度ライセンスを使用します。</p> <p>同じ PMC ユーザが複数の PMC クライアント マシンを使用し、複数の PMC セッションにログインした場合、そのユーザはライセンスを複数使用します (PMC セッションごとに1つずつ)。</p> <p> (注) 使用可能な PMC ライセンスがすべて使用されている場合、PMC ユーザはシステムにアクセスできません。PMC ライセンスの現在のステータスに注意して、使用可能な PMC ライセンスがすべて使用されている場合は、追加のライセンスをただちにご購入いただき、インストールしてください。</p>
Concurrent Cisco Unified IP Phone Users	<p>IP Phone ユーザは、Cisco IPICS に IP Phone からログインすると、その都度ライセンスを使用します。すべての IP Phone ライセンスが使用されている場合、以降の IP Phone ユーザは、チャンネルおよび VTG にダイヤルインできません。</p>
Concurrent Dial Users	<p>ポリシー エンジン、ダイヤル エンジンがダイヤルインまたはダイヤルアウト アクションを実行するたびに、ライセンスを使用します。すべてのダイヤル ユーザ ライセンスが使用されている場合、ダイヤル エンジン、ダイヤルインおよびダイヤルアウト アクションをそれ以上実行できません。</p>
Cisco IPICS Ops View	<p>追加の ops ビュー機能を含むライセンスをご購入いただいた場合は、ops ビューを作成すると、その都度ライセンスが1つ使用されます。</p>

表 2-1 Cisco IPICS ライセンスの使用基準 (続き)

フィールド	説明
Cisco IPICS Base Server License	ライセンスの使用状況は、このフィールドには適用されません。このフィールドは、Cisco IPICS のベース ライセンスを保有しているかどうかを示します。
Policy Engine Base License	ライセンスの使用状況は、このフィールドには適用されません。このフィールドは、ポリシー エンジンのベース ライセンスを保有しているかどうかを示します。

期間限定ライセンスの管理

Cisco IPICS では、期間限定ライセンスもサポートしています。評価用ライセンスやデモンストレーション ライセンスなどの期間限定ライセンスは、ライセンスの有効期限があらかじめ設定されているという点で、ご購入いただいた（無期限の）ライセンスとは異なります。

期間限定ライセンスの期限切れが近づくと（期限切れの約 30 日前）、まもなく期限切れになることを示す警告メッセージが表示されます。



(注)

最新の期間限定ライセンスをサーバにインストールしても、期限が切れていない他の期間限定ライセンスがインストールされていて、上記の警告メッセージをまだ処理していない場合は、この警告メッセージが表示されることがあります。この警告メッセージが表示されないようにするには、サーバにインストールされている期限の切れていない古いライセンスを削除します。詳細については、[P.2-45](#) の「古い期間限定ライセンスをサーバから削除」を参照してください。

- ライセンス機能が期限切れになると、そのライセンスに関連する機能は無効になります。
- ライセンスは、期限切れになった後、期限切れの日付から最長で 24 時間は有効なままです（サーバは 24 時間ごとに期限切れライセンスがあるかどうかを確認します）。

- Cisco IPICS サーバ ソフトウェアのインストール後、システム日付をライセンス開始日より前に変更すると、Cisco IPICS では期間限定ライセンスが無効になります。ライセンスが無効になると、Cisco IPICS システムは動作不能になります。



(注) システムの日付の変更を有効にするには、ライセンス マネージャを再起動するか、サーバをリブートする必要があります。

ライセンス マネージャを再起動してライセンスを再度有効にするには、次の手順を実行します。

手順

ステップ 1 ターミナル ウィンドウを開き、ルート ユーザ ID を使用してログインします。

ステップ 2 次のコマンドを入力して、ライセンス マネージャを再起動します。

```
[root]# service ipics_lm restart
```

ステップ 3 ライセンスを再度有効にするには、**Administration > License Management** に移動し、**Apply** をクリックしてライセンス サーバを再起動します。

古い期間限定ライセンスをサーバから削除

ライセンスの期限切れの警告メッセージが表示された場合に、期限が切れていない期間限定ライセンスが複数インストールされているときは、古い期間限定ライセンスを削除して、この警告メッセージが表示されないようにする必要があります。期間限定ライセンスを削除するには、次の手順を実行します。

手順

ステップ 1 ターミナル ウィンドウを開き、ルート ユーザ ID を使用してログインします。

- ステップ 2** 次のコマンドを入力して、Cisco IPICS がライセンス ファイルを格納しているディレクトリに移動します。

```
[root]# cd tomcat/current/webapps/license
```

- ステップ 3** 次のコマンドを入力して、ライセンス ファイルを表示します。

```
[root]# ls -l *.lic
```

ライセンス ファイルが、ライセンスが最後に変更された日付と時刻とともに表示されます。

- ステップ 4** 必要のないライセンスをメモします。

ファイル情報とともに表示される日付と時刻を参考にして、どのファイルを削除する必要があるかを判断します。

- ステップ 5** 次のコマンドを入力して、必要のないライセンス ファイルを削除します。

```
[root]# rm <licensefilename>.lic
```

表示の意味は次のとおりです。

<licensefilename>.lic は、削除するライセンス ファイルの名前です。

**注意**

cisco.opt ファイルは削除しないでください。このファイルは、Cisco IPICS が正しく動作するために必要です。

- ステップ 6** 削除する必要があるライセンス ファイルごとに、[ステップ 5](#) を繰り返します。

- ステップ 7** 次のコマンドを入力して、サーバを再起動します。

- ステップ 8** [root]# service ipics restart

- ステップ 9** ipics ユーザ ID を使用して Administration Console にログインし、**Administration > License Management** ウィンドウに移動します。

- ステップ 10** ライセンスの削除をシステム設定に適用するには、**Apply** をクリックします。
- ステップ 11** ライセンスがまもなく期限切れになることを示すメッセージが表示されたら、**Dismiss Warnings** をクリックします。
-

Cisco IPICS サーバへのサードパーティ証明書のインストール

Cisco IPICS サーバには、自己署名証明書が添付されています。この証明書は、CA が発行したお客様独自のサードパーティ証明書に置き換えることができます。CA は、信頼できる第三者の立場から、ユーザ、組織、サーバ、または証明書内に指定されたその他のエンティティの資格情報を確認して、セキュリティ強化のためのデジタル証明書を発行および管理します。CA の例としては、VeriSign、Thawte、および Entrust があります。

サードパーティ証明書を要求し、Cisco IPICS サーバにインストールする手順については、次のトピックで説明します。

- [サードパーティ証明書の要求 \(P.2-47\)](#)
- [サードパーティ証明書のインストール \(P.2-51\)](#)

サードパーティ証明書の要求

サードパーティ証明書を要求するには、次の手順を実行します。

手順

- ステップ 1** ルート ユーザ ID を使用して Cisco IPICS サーバにログインします。
- ルート ユーザとして Cisco IPICS オペレーティング システムにログインした状態になります。
- ステップ 2** 次のコマンドを入力して、tomcat.keystore ファイルを /root ディレクトリにコピーします。

```
[root]# cp /root/tomcat/current/conf/tomcat.keystore /root
```

tomcat.keystore ファイルは、サーバのすべての証明書を保持しています。

ステップ 3 次のコマンドを入力して、/root/tomcat/current/conf/ ディレクトリに移動します。

```
[root]# cd /root/tomcat/current/conf/
```

ステップ 4 次のコマンドを実行して、既存のエントリを削除します。

```
[root@ipics-server]# keytool -delete -alias tomcat -keystore tomcat.keystore
```

ステップ 5 キーストアのパスワードを入力するように求められたら、デフォルト パスワードの **changeit** を入力します。

ステップ 6 次のコマンドを実行して、Certificate Signing Request (CSR; 証明書署名要求) で使用される新しいキーを生成します。

```
[root@ipics-server]# keytool -genkey -alias tomcat -keyalg RSA -keystore  
tomcat.keystore -validity 360
```

有効期間 (validity) の値は、必要な証明書有効日数に応じて異なります。



(注) 正しい情報を入力したことを確認して、CA がシステムのための有効な証明書を生成できるようにしてください。

ステップ 7 次のシステム プロンプトに対して、応答を入力します。

```
Enter keystore password:  
What is your first and last name?  
What is the name of your organizational unit?  
What is the name of your organization?  
What is the name of your City or Locality?  
What is the name of your State or Province?  
What is the two-letter country code for this unit?
```




(注) 入力する情報は、使用する CA によって異なる場合があります。たとえば、姓と名の応答については、VeriSign の場合、Cisco IPICS サーバの完全修飾ホスト名を `server.domain.com` 形式で入力する必要があります。州または県の名前については、VeriSign の場合、省略形式を使用せずに完全な名前を入力する必要があります。



ヒント キーストアのデフォルト パスワードは、**changeit** です。

表示される情報の例を次に示します。

```
Is CN=username, OU=user company name, O=user company name, L=user
city, ST=user state, C=user country correct? [no]:
```

ステップ 8 情報が正しい場合は、**y** または **yes** と入力します。

ステップ 9 次のメッセージが表示される場合は、**Enter** キーを押してデフォルト パスワードをそのまま使用します。

```
Enter key password for <tomcat>
(RETURN if same as keystore password):
```

`<tomcat>` は、証明書のデフォルト エイリアスです。



(注) キーパスワードとキーストアパスワードには、同じ値を使用する必要があります。それぞれ異なるパスワードを使用すると、Tomcat サーバが正常に再起動できなくなります（これらのパスワードを同じものにした場合、キーパスワードを入力するように再度求められることはありません）。

ステップ 10 次のコマンドを実行して、CSR ファイルを作成します。

```
[root@ipics-server]# keytool -certreq -alias tomcat -keyalg RSA -file certrequest.csr  
-keystore tomcat.keystore
```

ステップ 11 キーストアのパスワードを入力するように求められたら、デフォルト値の **changeit** を入力します。

Enter keystore password:

正しいパスワードを入力すると、CSR が作成されます（入力したパスワードが正しくない場合は、エラーが表示されます）。



(注) 証明書を要求する場合は、この CSR ファイルに保持されているテキストを使用する必要があります [ステップ 12](#) を参照してください。

ステップ 12 **certrequest.csr** ファイルをローカルワークステーションにコピーします。

使用する CA によっては、証明書の要求時に、**certrequest.csr** ファイルの内容をコピーしてブラウザに貼り付けるか、CSR ファイルをアップロードする必要があります。



(注) CA が証明書要求を受け付けない場合は、この手順を [ステップ 3](#) から繰り返し、必要な変更を追加して証明書要求を再度生成します。

ステップ 13 証明書を CA から受け取った後、[P.2-51](#) の「サードパーティ証明書のインストール」の手順に進んでサードパーティ証明書をインストールします。

サードパーティ証明書インストール

サードパーティ証明書をサーバにインストールするには、次の手順を実行します。

手順

ステップ 1 証明書を受け取る形態に応じて、次のいずれかの作業を行います。

- 証明書ファイルを CA から直接受け取る場合は、ファイルの名前を **thirdparty.cer** に変更します。
- 電子メールに添付された証明書を受け取る場合は、**thirdparty.cer** という名前の新しいファイルを作成します（このファイルには、電子メール内の証明書の内容だけを含める必要があります）。

CA は、ルート CA 証明書を送信する場合、その他の方法を使用することがあります。CA によって、提供する証明書の中にルート CA を埋め込む場合も、ルート CA 証明書を単体で提供する場合があります（ルート CA 証明書を使用すると、CA からサーバ上のサードパーティ証明書までの信頼チェーンを確立できます）。

ステップ 2 ルート CA 証明書が提供される形態に応じて、次のいずれかの追加作業を行います。

- ルート CA 証明書ファイルを CA の Web サイトから直接ダウンロードした場合は、ファイルの名前を **thirdpartyca.cer** に変更します。
- CA がルート CA 証明書を Web ページに埋め込んで提供した場合は、**thirdpartyca.cer** という名前の新しいファイルを作成します（このファイルには、Web ページのルート CA 証明書の内容だけを含める必要があります）。

ステップ 3 セキュア FTP を使用して、**thirdparty.cer** ファイル（およびオプションの **thirdpartyca.cer** ファイル）をローカルワークステーションからサーバの `/root/tomcat/current/conf/` ディレクトリにコピーします。

ステップ 4 `/root/tomcat/current/conf/` ディレクトリから移動していないことを確認するには、次のコマンドを入力します。

```
[root]# cd /root/tomcat/current/conf/
```

- ステップ 5** ルート CA 証明書を単体で受け取る場合は、次のコマンドを入力して、最初に証明書をインストールします。

```
[root@ipics-server]# keytool -import -alias thirdpartyca -keystore tomcat.keystore  
-trustcacerts -file thirdpartyca.cer
```

- ステップ 6** キーストアのパスワードを入力するように求められたら、**changeit** と入力します。

- ステップ 7** 次のプロンプトが表示されたら、**yes** と入力して証明書を信頼します。

```
Trust this certificate? [no]:
```

証明書がインストールされ、次のメッセージが表示されます。

```
Certificate was added to keystore
```

- ステップ 8** 証明書をインストールするには、次のコマンドを実行します。

```
[root@ipics-server]# keytool -import -alias tomcat -keystore tomcat.keystore  
-trustcacerts -file thirdparty.cer
```

- ステップ 9** キーストアのパスワードを入力するように求められたら、**changeit** と入力します。

ルート CA 証明書をインストールしていない場合は、次のエラー メッセージが表示されます（この証明書は必須です）。

```
keytool error: java.lang.Exception: Failed to establish chain from  
reply
```

このエラーが発生した場合は、CA に問い合わせるルート CA 証明書を確認し、この手順を [ステップ 5](#) から繰り返します。

- ステップ 10** 次のプロンプトが表示されたら、**yes** と入力して証明書を信頼します。

```
Trust this certificate? [no]:
```

証明書がインストールされ、次のメッセージが表示されます。

```
Certificate reply was installed in keystore
```

ステップ 11 ルート ユーザで次のコマンドを入力して、Tomcat Web サーバを再起動します。

```
[root]# service ipics_tomcat restart
```

ステップ 12 次のコマンドを実行して、証明書がインストールされたことを確認します。

```
[root@ipics-server]# keytool -list -keystore tomcat.keystore
```

ステップ 13 キーストアのパスワードを入力するように求められたら、デフォルト値の **changeit** を入力します。

次の例のような証明書情報が表示されます。

```
Keystore type: jks
Keystore provider: SUN
Your keystore contains 1 entries
Tomcat, May 12, 2006, keyEntry,
Certificate fingerprint (MD5):
88:88:1A:34:38:0A:27:6F:B9:87:CA:8F:36:66:C4:73
```

ルート CA 証明書をインストールした場合、次の例のように、キーストアが2つのエントリを保持していることが示されます。

```
Your keystore contains 2 entries
thirdpartyca, May 20, 2006, trustedCertEntry,
Certificate fingerprint (MD5):
B6:9D:A4:40:52:02:50:0D:D5:9C:E1:B8:4B:66:C4:AC
...
```



(注) フィンガープリントは、システムによって異なります。

Cisco IPICS PMC アプリケーションのインストーラの生成

PMC ユーザは、PMC のインストーラを Cisco IPICS Administration Console からダウンロードします。ユーザが PMC インストーラをサーバからダウンロードできるようにするには、まず管理者が PMC インストーラを生成する必要があります。

PMC インストーラの生成および PMC アップデートの管理の詳細については、『[Cisco IPICS Server Administration Guide Release 2.1\(1\)](#)』の「Performing Cisco IPICS System Administrator Tasks」の章にある「Generating the PMC Installer」と「Managing PMC Versions」の項を参照してください。