Cisco Unified Communications Operating System アドミニストレーション ガイド for Cisco Unity Connection

Release 7.x
Published August 25, 2008

Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection

Release 7.x
Published August 25, 2008

Text Part Number: OL-17873-01-J

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

**本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。
米国サイト掲載ドキュメントとの差異が生じる場合があるため、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。**

Cisco Unified Communications Operating System アドミニストレーション ガイド for Cisco Unity Connection

CONTENTS

はじめに

この章には、次の項があります。

対象読者と用途

『*Cisco Unified Communications Operating System アドミニストレーション ガイド*』では、Cisco Unified Communications オペレーティング システム の Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）の使用方法について説明します。

このマニュアルは、Cisco Unified Communications オペレーティング システムの管理とサポートを担当するネットワーク管理者を対象としています。ネットワーク技術者、システム管理者、または電気通信技術者は、このマニュアルを参照してオペレーティング システムの機能を理解し、その管理を行います。このマニュアルを使用するには、テレフォニーおよび IP ネットワーキング テクノロジーに関する知識が必要です。

さまざまなシステムおよびネットワークに関連する共通タスクを実行する際に使用する Command Line Interface（CLI; コマンドライン インターフェイス）の詳細については、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』を参照してください。

表記法

このマニュアルでは、次の表記法を使用しています。

表記	説明
太字	コマンドおよびキーワードは、太字で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{ x | y | z }	必ずどれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
ストリング	引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングと見なされます。
`screen` フォント	システムが表示する端末セッションおよび情報は、`screen` フォントで示しています。
太字の **`screen`** フォント	ユーザが入力しなければならない情報は、太字の **`screen`** フォントで示しています。
イタリック体の *`screen`* フォント	ユーザが値を指定する引数は、イタリック体の *`screen`* フォントで示しています。
⟶	例の中で重要なテキストを強調しています。
^	^ 記号は、Ctrl キーを表します。たとえば、画面に表示される ^D というキーの組み合せは、Ctrl キーを押しながら D キーを押すことを意味します。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。

（注）は、次のように表しています。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ワンポイント アドバイスは、次のように表しています。

ワンポイント・アドバイス 時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。

ヒントは、次のように表しています。

ヒント 役立つヒントです。

注意は、次のように表しています。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告は、次のように表しています。

警告 **「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。**

関連資料

Cisco.com にある Cisco Unity Connection のマニュアルの説明および URL については、『*Documentation Guide for Cisco Unity Connection Release 7.x*』を参照してください。マニュアルは、Cisco Unity Connection に同梱されていますが、http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/roadmap/7xcucdg.html から入手することもできます。

関連する Cisco IP テレフォニー アプリケーションおよび製品の詳細については、ご使用のリリースに対応する『*Cisco Unified Communications Manager Documentation Guide*』を参照してください。次の URL から入手できます。
http://cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html

マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン

マニュアルの入手方法、Service Request ツールの使用方法、および追加情報の収集方法については、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。『*What's New in Cisco Product Documentation*』には、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

Really Simple Syndication（RSS）フィードとして『*What's New in Cisco Product Documentation*』に登録し、リーダ 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します。RSS フィードは無料サービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

シスコのテクニカル サポート

次の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。

http://www.cisco.com/en/US/support/index.html

以下を含むさまざまな作業にこの Web サイトが役立ちます。

- テクニカル サポートを受ける
- ソフトウェアをダウンロードする
- セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける
- ツールおよびリソースへアクセスする
  - Product Alert の受信登録
  - Field Notice の受信登録
  - Bug Toolkit を使用した既知の問題の検索
- Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する
- トレーニング リソースへアクセスする
- TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する

Japan テクニカル サポート Web サイトでは、Technical Support Web サイト（http://www.cisco.com/techsupport）の、利用頻度の高い ドキュメントを日本語で提供しています。Japan テクニカル サポート Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

Service Request ツールの使用

Service Request ツールには、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

日本語版の Service Request ツールは次の URL からアクセスできます。

http://www.cisco.com/jp/go/tac/sr/

シスコの世界各国の連絡先一覧は、次の URL で参照できます。

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

その他の情報の入手方法

シスコの製品、サービス、テクノロジー、ネットワーキング ソリューションに関する情報について、さまざまな資料をオンラインで入手できます。

- シスコの E メール ニュースレターなどの配信申し込みについては、Cisco Subscription Center にアクセスしてください。

  http://www.cisco.com/offer/subscribe

- 日本語の月刊 Email ニュースレター「Cisco Customer Bridge」については、下記にアクセスください。

  http://www.cisco.com/web/JP/news/cisco_news_letter/ccb/

- シスコ製品に関する変更やアップデートの情報を受信するには、Product Alert Tool にアクセスし、プロファイルを作成して情報の配信を希望する製品を選択してください。Product Alert Tool には、次の URL からアクセスできます。

  http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

- 『*Cisco Product Quick Reference Guide*』はリファレンス ツールで、パートナーを通じて販売されている多くのシスコ製品に関する製品概要、主な機能、製品番号、および簡単な技術仕様が記載されています。『*Cisco Product Quick Reference Guide*』を発注するには、次の URL にアクセスしてください。

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

- ネットワークの運用面の信頼性を向上させることのできる最新の専門的サービス、高度なサービス、リモート サービスに関する情報については、Cisco Services Web サイトを参照してください。Cisco Services Web サイトには、次の URL からアクセスできます。

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

- Cisco Marketplace では、さまざまなシスコの書籍、参考資料、マニュアル、ロゴ入り商品を提供しています。Cisco Marketplace には、次の URL からアクセスできます。

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

- DVD に収録されたシスコの技術マニュアル（Cisco Product Documentation DVD）は、Product Documentation Store で発注できます。Product Documentation Store には、次の URL からアクセスできます。

  http://www.cisco.com/go/marketplace/docstore

- 日本語マニュアルの DVD は、マニュアルセンターから発注できます。マニュアルセンターには下記よりアクセスください。

  http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/manual_center/index.shtml

- Cisco Press では、ネットワーク、トレーニング、認定関連の出版物を発行しています。Cisco Press には、次の URL からアクセスできます。

  http://www.ciscopress.com

- 日本語のシスコプレスの情報は以下にアクセスください。

  http://www.seshop.com/se/ciscopress/default.asp

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスできます。

  http://www.cisco.com/ipj

- 『*What's New in Cisco Product Documentation*』は、シスコ製品の最新マニュアル リリースに関する情報を提供するオンライン資料です。毎月更新されるこの資料は、製品カテゴリ別にまとめられているため、目的の製品マニュアルを見つけることができます。

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

- シスコの Web サイトの各国語版へは、次の URL からアクセスしてください。

  http://www.cisco.com/public/countries_languages.shtml

（注） このマニュアルには、日本語化されたマニュアル名と英語版 URL が併記された箇所があります。日本語版マニュアルを参照する場合は、次の URL にアクセスしてください。

http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/index_uc_cuc.shtml

CHAPTER 1

概要

Cisco Unified Communications Manager では、Cisco Unified Communications オペレーティング システムを使用して、多くの一般的なシステム管理機能を実行できます。

この章は、次の項で構成されています。

概要

Cisco Unified Communications オペレーティング システムの管理ページを使用して、Cisco Unified Communications オペレーティング システムを設定および管理できます。管理タスクには、次のものがあります。

- ソフトウェアおよびハードウェアのステータスを確認する。
- IP アドレスを確認および更新する。
- 他のネットワーク デバイスに対して PING を実行する。
- NTP サーバを管理する。
- システム ソフトウェアおよびオプションをアップグレードする。
- サーバのセキュリティ（IPSec や証明書など）を管理する。
- リモート サポート アカウントを管理する。
- システムを再起動する。

次の各項では、オペレーティング システムの各機能について詳細に説明します。

ブラウザ要件

次のブラウザを使用して、Cisco Unified Communications オペレーティング システムにアクセスできます。

- Microsoft Internet Explorer バージョン 6.x
- Netscape Navigator バージョン 7.1 以降

（注） その他のブラウザ（Mozilla Firefox など）については、シスコではサポートもテストも実施していません。

製品のすべての機能を正常に動作させるには、ブラウザの「信頼済みサイト ゾーン」または「ローカル イントラネット サイト ゾーン」に Cisco Unified Communications オペレーティング システム サーバの URL（**https://***servername*）が含まれている必要があります。

オペレーティング システムのステータスと設定

［**表示（Show）**］メニューから、次のようなオペレーティング システムの各種コンポーネントのステータスを確認できます。

- クラスタとノード
- ハードウェア
- ネットワーク
- システム
- インストールされているソフトウェアおよびオプション

詳細については、第 3 章「ステータスと設定」を参照してください。

設定

［設定（Settings）］メニューから、次のオペレーティング システム設定を表示および更新できます。

- IP：アプリケーションのインストール時に入力された IP アドレスおよび Dynamic Host Configuration Protocol（DHCP）クライアント設定を更新します。
- NTP サーバの設定：外部 NTP サーバの IP アドレスを設定します。また、NTP サーバを追加または削除します。
- SMTP の設定：オペレーティング システムが電子メール通知の送信に使用する SMTP ホストを設定します。

詳細については、第 4 章「設定」を参照してください。

［設定（Settings）］>［バージョン（Version）］ウィンドウでは、次のオプションの中から選択して、システムを再起動またはシャットダウンできます。

- バージョンの切り替え：アクティブなディスク パーティションと非アクティブなディスク パーティションを切り替え、システムを再起動します。通常は、非アクティブなパーティションが更新された後、新しいソフトウェア バージョンの実行を開始するときに、このオプションを選択します。
- 現在のバージョン：パーティションを切り替えずにシステムを再起動します。
- システムのシャットダウン：実行中のソフトウェアをすべて停止し、サーバをシャットダウンします。

（注） このコマンドを実行しても、サーバの電源は切断されません。サーバの電源を切断するには、電源ボタンを押してください。

詳細については、第 5 章「システムの再起動」を参照してください。

セキュリティ設定

オペレーティング システムのセキュリティ オプションを使用すると、セキュリティ証明書および Secure Internet Protocol（IPSec）を管理できます。［セキュリティ（Security）］メニューから、次のセキュリティ オプションを選択できます。

- 証明書の管理：証明書、Certificate Trust List（CTL; 証明書信頼リスト）、および Certificate Signing Request（CSR; 証明書署名要求）を管理します。証明書を表示、アップロード、ダウンロード、削除、および再生成できます。証明書の管理では、サーバ上の証明書の有効期限を監視することもできます。
- IPSEC の管理：既存の IPSEC ポリシーを表示または更新します。また、新しい IPSEC ポリシーおよびアソシエーションを設定します。

詳細については、第 6 章「セキュリティ」を参照してください。

ソフトウェア アップグレード

ソフトウェア アップグレード オプションでは、オペレーティング システム上で動作しているソフトウェア バージョンをアップグレードしたり、特定のソフトウェア オプション（Cisco Unified Communications オペレーティング システムの Locale Installer、ダイヤル プラン、TFTP サーバ ファイルなど）をインストールしたりすることができます。

［**インストール / アップグレード（Install/Upgrade）**］メニュー オプションでは、ローカル ディスクまたはリモート サーバからシステム ソフトウェアをアップグレードできます。アップグレードしたソフトウェアは、非アクティブなパーティションにインストールされます。その後、システムを再起動してパーティションを切り替え、システムが新しいソフトウェア バージョンで動作を開始するようにすることができます。

（注） Cisco Unified Communications オペレーティング システムの GUI およびコマンドライン インターフェイスに含まれるソフトウェア アップグレード機能を使用して、すべてのソフトウェアのインストールとアップグレードを実行する必要があります。システムでアップグレードおよび処理できるソフトウェアは、シスコシステムズによって認定されたソフトウェアに限られます。Cisco Unified Communications Manager の以前のバージョンで使用していたサードパーティ製もしくは Windows ベースのソフトウェア アプリケーションは、インストールしたり使用したりできません。

詳細については、第 7 章「ソフトウェア アップグレード」を参照してください。

サービス

このアプリケーションには、次に示すオペレーティング システムのユーティリティが用意されています。

- PING：他のネットワーク デバイスとの接続性を確認します。
- リモート サポート：シスコのサポート担当者がシステムにアクセスするときに使用できるアカウントを設定します。このアカウントは、指定した日数を経過すると自動的に期限切れになります。

詳細については、第 8 章「サービス」を参照してください。

コマンドライン インターフェイス

コマンドライン インターフェイスには、コンソールから、またはサーバへのセキュア シェル接続でアクセスできます。詳細については、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』を参照してください。

CHAPTER 2

Cisco Unified Communications オペレーティング システムの管理ページへのログイン

この章では、Cisco Unified Communications オペレーティング システムの管理ページにアクセスする手順、およびパスワードをリセットする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。

Cisco Unified Communications オペレーティング システムの管理ページへのログイン

Cisco Unified Communications オペレーティング システムの管理ページにアクセスしてログインするには、次の手順を実行します。

（注） Cisco Unified Communications オペレーティング システムの管理ページを使用中は、ブラウザ コントロール（たとえば、［戻る］ボタン）を使用しないでください。

手順

ステップ 1　Cisco Unified CM の管理ページにログインします。

ステップ 2　［Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）］ウィンドウの右上隅にある［ナビゲーション（Navigation）］メニューから［**Cisco Unified OS の管理（Cisco Unified OS Administration）**］を選択し、［**移動（Go）**］をクリックします。

Cisco Unified Communications オペレーティング システムの管理ページのログイン ウィンドウが表示されます。

（注） 次の URL を入力して、Cisco Unified Communications オペレーティング システムの管理ページに直接アクセスすることもできます。
http://*server-name*/**cmplatform**

ステップ 3　管理者ユーザ名とパスワードを入力します。

（注） 管理者ユーザ名とパスワードは、インストール中に設定されるか、コマンドライン インターフェイスを使用して作成されます。

ステップ 4　［**送信（Submit）**］をクリックします。

［Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）］ウィンドウが表示されます。

管理者パスワードとセキュリティ パスワードのリセット

管理者パスワードまたはセキュリティ パスワードを紛失した場合は、次の手順を実行してこれらのパスワードをリセットします。

パスワードをリセットするには、システム コンソールを使用してシステムに接続する必要があります。つまり、サーバにキーボードとモニタが接続されている必要があります。システムにセキュア シェル セッションで接続した場合、パスワードをリセットできません。

注意　セキュリティ パスワードは、クラスタ内のすべてのノードで一致している必要があります。セキュリティ パスワードは、すべてのマシン上で変更してください。変更していない場合、クラスタ ノードが通信不能になります。

注意　セキュリティ パスワードを変更した後に、クラスタ内の各サーバをリセットする必要があります。サーバ（ノード）をリブートしない場合、システム サービスで問題が発生するほか、サブスクライバ サーバ上の Cisco Unified CM の管理ページの各ウィンドウで問題が発生します。

（注）　この手順の実行中は、システムへ物理的にアクセスできることを証明するため、有効な CD または DVD をいったんディスク ドライブから取り出し、再び挿入するように求められます。

手順

ステップ 1　次のユーザ名とパスワードを使用して、システムにログインします。

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

［Welcome to platform password reset］ウィンドウが表示されます。

ステップ 2　任意のキーを押して続行します。

ステップ 3　ディスク ドライブに CD または DVD が入っている場合は、ここで取り出します。

ステップ 4　任意のキーを押して続行します。

ディスク ドライブから CD または DVD が取り出されたことを確認するためのテストが実行されます。

ステップ 5　有効な CD または DVD をディスク ドライブに挿入します。

（注）　このテストでは、音楽 CD ではなくデータ CD を使用する必要があります。

ディスクが挿入されたことを確認するためのテストが実行されます。

ステップ 6　システムがディスクの挿入を確認すると、次のいずれかのオプションを入力して処理を続行するよう指示されます。

- 管理者パスワードをリセットする場合は、**a** を入力します。
- セキュリティ パスワードをリセットする場合は、**s** を入力します。
- 処理を終了する場合は、**q** を入力します。

ステップ 7　上で選択したタイプのパスワードについて、新しいパスワードを入力します。

ステップ 8　新しいパスワードを再度入力します。

パスワードには少なくとも 6 文字が必要です。新しいパスワードの強度が確認されます。パスワードが強度チェックの基準を満たしていない場合は、新しいパスワードを入力するよう指示されます。

ステップ 9　新しいパスワードの強度が確認された後、パスワードがリセットされます。次に、任意のキーを押してパスワード リセット ユーティリティを終了するように要求されます。

CHAPTER 3

ステータスと設定

この章では、システムの管理について説明します。次の項について取り上げます。

- クラスタ ノード
- ハードウェア ステータス
- ネットワークの設定
- インストールされているソフトウェア
- システム ステータス
- IP 設定

クラスタ ノード

クラスタ内のノードに関する情報を表示するには、次の手順を実行します。

手順

ステップ 1　［Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）］ウィンドウで、**［表示（Show）］** > **［クラスタ（Cluster）］**に移動します。

［クラスタノード（Cluster Nodes）］ウィンドウが表示されます。

ステップ 2　［クラスタノード（Cluster Nodes）］ウィンドウの各フィールドの説明については、表 3-1 を参照してください。

表 3-1　クラスタ ノードのフィールド説明

フィールド	説明
［ホスト名（Hostname）］	サーバの完全ホスト名を表示します。
［IP アドレス（IP Address）］	サーバの IP アドレスを表示します。
［エイリアス（Alias）］	サーバのエイリアス名を表示します（定義されている場合）。
［ノードのタイプ（Type of Node）］	サーバがパブリッシャ ノードかサブスクライバ ノードかを示します。

ハードウェア ステータス

ハードウェア ステータスを表示するには、次の手順を実行します。

手順

ステップ 1　［Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）］ウィンドウで、**［表示（Show）］** > **［ハードウェア（Hardware）］**に移動します。

［ハードウェアステータス（Hardware Status）］ウィンドウが表示されます。

ステップ 2　［ハードウェアステータス（Hardware Status）］ウィンドウの各フィールドの説明については、表 3-2 を参照します。

表 3-2　ハードウェアのステータスのフィールド説明

フィールド	説明
［プラットフォームタイプ（Platform Type）］	プラットフォーム サーバのモデル ID を表示します。
［プロセッサ速度（Processor Speed）］	プロセッサの速度を表示します。
［CPU タイプ（CPU Type）］	プラットフォーム サーバのプロセッサ タイプを表示します。
［メモリ（Memory）］	メモリの総量を MB 単位で表示します。
［オブジェクト ID（Object ID）］	オブジェクト ID を表示します。
［OS バージョン（OS Version）］	オペレーティング システムのバージョンを表示します。
［RAID の詳細（RAID Details）］	RAID ドライブの詳細を表示します。コントローラ、論理ドライブ、および物理デバイスの情報が含まれています。

ネットワークの設定

表示されるネットワーク ステータス情報は、Network Fault Tolerance（NFT; ネットワーク耐障害性）が有効になっているかどうかによって異なります。ネットワーク耐障害性が有効になっている場合、イーサネット ポート 0 に障害が発生すると、イーサネット ポート 1 が自動的にネットワーク通信を引き継ぎます。ネットワーク耐障害性が有効になっている場合は、イーサネット 0、イーサネット 1、および Bond 0 というネットワーク ポートのネットワーク ステータス情報が表示されます。ネットワーク耐障害性が有効になっていない場合は、イーサネット 0 のステータス情報だけが表示されます。

ネットワーク ステータスを表示するには、次の手順を実行します。

手順

ステップ 1　［Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）］ウィンドウで、**［表示（Show）］** > **［ネットワーク（Network）］**に移動します。

［ネットワークの設定（Network Configuration）］ウィンドウが表示されます。

ステップ 2　［ネットワークの設定（Network Configuration）］ウィンドウの各フィールドの説明については、表 3-3 を参照します。

表 3-3　［ネットワークの設定（Network Configuration）］のフィールド説明

フィールド	説明
［イーサネットの詳細（Ethernet Details）］	
［DHCP］	イーサネット ポート 0 について、DHCP が有効になっているかどうかを示します。
［ステータス（Status）］	イーサネット ポート 0 および 1 について、ポートがアップ状態であるかダウン状態であるかを示します。
［IP アドレス（IP Address）］	イーサネット ポート 0（および、ネットワーク耐障害性（NFT）が有効になっている場合はイーサネット ポート 1）の IP アドレスを表示します。
［IP マスク（IP Mask）］	イーサネット ポート 0（および、NFT が有効になっている場合はイーサネット ポート 1）の IP マスクを表示します。
［リンク検出済（Link Detected）］	アクティブなリンクがあるかどうかを示します。
［キューの長さ（Queue Length）］	キューの長さを表示します。
［MTU］	最大伝送ユニットを表示します。
［MAC アドレス（MAC Address）］	ポートのハードウェア アドレスを表示します。
受信済み統計用フィールド（RX）	受信済みのバイト、パケット、およびエラーについて、廃棄とオーバーランの統計とともに情報を表示します。
送信済み統計用フィールド（TX）	送信済みのバイト、パケット、およびエラーについて、廃棄、キャリア、およびコリジョンの統計とともに情報を表示します。

表 3-3　［ネットワークの設定（Network Configuration）］のフィールド説明（続き）

フィールド	説明
［DNS の詳細（DNS Details）］	
［プライマリ（Primary）］	プライマリ ドメイン ネーム サーバの IP アドレスを表示します。
［セカンダリ（Secondary）］	セカンダリ ドメイン ネーム サーバの IP アドレスを表示します。
［オプション（Options）］	設定されている DNS オプションを表示します。
［ドメイン（Domain）］	サーバのドメインを表示します。
［ゲートウェイ（Gateway）］	イーサネット ポート 0 上のネットワーク ゲートウェイの IP アドレスを表示します。

インストールされているソフトウェア

ソフトウェア バージョンおよびインストールされているソフトウェア オプションを表示するには、次の手順を実行します。

手順

ステップ 1　［Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）］ウィンドウで、**［表示（Show）］** > **［ソフトウェア（Software）］**に移動します。

［ソフトウェアパッケージ（Software Packages）］ウィンドウが表示されます。

ステップ 2　［ソフトウェアパッケージ（Software Packages）］ウィンドウの各フィールドの説明については、表 3-4 を参照してください。

表 3-4　［ソフトウェアパッケージ（Software Packages）］のフィールド説明

フィールド	説明
［パーティションのバージョン（Partition Versions）］	アクティブなパーティションおよび非アクティブなパーティションで動作しているソフトウェア バージョンを表示します。
［インストールされているアクティブなソフトウェアオプションのバージョン（Active Version Installed Software Options）］	アクティブなバージョンにインストールされているソフトウェア オプション（ロケールやダイヤル プランなど）のバージョンを表示します。
［インストールされているアクティブでないソフトウェアオプションのバージョン（Inactive Version Installed Software Options）］	非アクティブなバージョンにインストールされているソフトウェア オプション（ロケールやダイヤル プランなど）のバージョンを表示します。

システム ステータス

システム ステータスを表示するには、次の手順を実行します。

手順

ステップ 1　［Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）］ウィンドウで、**［表示（Show）］** > **［システム（System）］**に移動します。

［システムステータス（System Status）］ウィンドウが表示されます。

ステップ 2　［システムステータス（System Status）］ウィンドウの各フィールドの説明については、表 3-5 を参照します。

表 3-5　［システムステータス（System Status）］のフィールド説明

フィールド	説明
［ホスト名（Host Name）］	Cisco Unified Communications オペレーティング システムがインストールされている Cisco MCS ホストの名前を表示します。
［日付（Date）］	オペレーティング システムのインストール時に指定された大陸と地域に基づいて、日時を表示します。
［タイムゾーン（Time Zone）］	インストール時に選択されたタイム ゾーンを表示します。
［ロケール（Locale）］	オペレーティング システムのインストール時に選択された言語を表示します。
［製品バージョン（Product Version）］	オペレーティング システムのバージョンを表示します。
［プラットフォームバージョン（Platform Version）］	プラットフォームのバージョンを表示します。
［アップタイム（Uptime）］	システムの動作期間に関する情報を表示します。
［CPU］	CPU の処理能力のうち、アイドル状態になっている割合、システム プロセスの実行に使用されている割合、およびユーザ プロセスの実行に使用されている割合を表示します（% 単位）。
［メモリ（Memory）］	メモリの使用状況について情報を表示します。メモリの総量、空き容量、および使用量が KB 単位で示されます。
［ディスク（Disk）］の［active］	アクティブなディスクについて、ディスク スペースの総量、空き容量、および使用量を表示します。
［ディスク（Disk）］の［inactive］	アクティブでないディスクについて、ディスク スペースの総量、空き容量、および使用量を表示します。
［ディスク（Disk）］の［logging］	ディスクのロギングに使用されるディスク スペースについて、総量、空き容量、および使用量を表示します。

IP 設定

［IP 設定（IP Preferences）］ウィンドウを使用すると、システムが使用可能な登録済みポートのリストを表示できます。［IP 設定（IP Preferences）］ウィンドウには、次の情報が含まれています。

- ［アプリケーション（Application）］
- ［プロトコル（Protocol）］
- ［ポート番号（Port Number）］
- ［タイプ（Type）］
- ［変換済みポート（Translated Port）］
- ［ステータス（Status）］
- ［説明（Description）］

［IP 設定（IP Preferences）］ウィンドウにアクセスするには、次の手順を実行します。

手順

ステップ 1　［Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications OS Administration）］ウィンドウで、**［表示（Show）］** > **［IP 設定（IP Preferences）］**を選択します。

［IP 設定（IP Preferences）］ウィンドウが表示されます。このウィンドウには、アクティブな（以前の）クエリーのレコードも表示されることがあります。

ステップ 2　データベース内のレコードをすべて表示するには、ダイアログボックスを空欄のままにして、ステップ 3 に進みます。

レコードをフィルタリングまたは検索するには、次の手順を実行します。

- 最初のドロップダウン リスト ボックスで、検索パラメータを選択します。
- 2 番目のドロップダウン リスト ボックスで、検索パターンを選択します。
- 必要に応じて、適切な検索テキストを指定します。

（注）　検索条件をさらに追加するには、［+］ボタンをクリックします。条件を追加した場合、指定した条件をすべて満たしているレコードが検索されます。条件を削除する場合、最後に追加した条件を削除するには、［–］ボタンをクリックします。追加した検索条件をすべて削除するには、**［フィルタのクリア（Clear Filter）］**ボタンをクリックします。

ステップ 3　**［検索（Find）］**をクリックします。

条件を満たしているレコードがすべて表示されます。1 ページあたりの項目の表示件数を変更するには、［ページあたりの行数（Rows per Page）］ドロップダウン リスト ボックスで別の値を選択します。

［IP 設定（IP Preferences）］の各フィールドの説明については、表 3-6 を参照してください。

表 3-6　IP 設定のフィールド説明

フィールド	説明
［アプリケーション（Application）］	ポートを使用している（リッスンしている）アプリケーションの名前。
［プロトコル（Protocol）］	このポートで使用されているプロトコル（TCP や UDP など）。
［ポート番号（Port Number）］	ポート番号（数値）。
［タイプ（Type）］	このポートで許可されるトラフィックのタイプ。 • ［パブリック（Public）］：すべてのトラフィックが許可される • ［変換済み（Translated）］：すべてのトラフィックが許可されるが、別のポートに転送される • ［プライベート（Private）］：定義済みの一連のリモート サーバ（クラスタ内の他のノードなど）からのトラフィックのみ許可される
［変換済みポート（Translated Port）］	このポートを宛先とするトラフィックは、［ポート番号（Port Number）］列に表示されているポートに転送されます。このフィールドが適用されるのは、［変換済み（Translated）］タイプのポートのみです。
［ステータス（Status）］	ポートの使用状況。 • ［有効（Enabled）］：ファイアウォールで開かれていて、アプリケーションが使用中 • ［無効（Disabled）］：ファイアウォールでブロックされていて、未使用状態
［説明（Description）］	ポートの使用状況に関する簡単な説明。

CHAPTER 4

設定

IP 設定、ホスト設定、および Network Time Protocol（NTP; ネットワーク タイム プロトコル）設定を表示および変更するには、［設定（Settings）］のオプションを使用します。

この章は、次の項で構成されています。

IP 設定

IP 設定のオプションを使用すると、イーサネット接続の IP とポートの設定を表示および変更できます。

イーサネットの設定ウィンドウでは、Dynamic Host Configuration Protocol（DHCP）がアクティブであるかどうかが示されます。また、関連するイーサネット IP アドレス、およびネットワーク ゲートウェイの IP アドレスも表示されます。

イーサネット設定はすべて、Eth0 だけに適用されます。Eth1 の設定値を設定することはできません。デフォルトでは、Eth0 の Maximum Transmission Unit（MTU; 最大伝送ユニット）は 1500 です。

IP 設定を表示または変更するには、次の手順を実行します。

手順

ステップ 1　［Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）］ウィンドウで、**［設定（Settings）］**>**［IP］**>**［イーサネット（Ethernet）］**に移動します。

［イーサネットの設定（Ethernet Configuration）］ウィンドウが表示されます。

ステップ 2　イーサネット設定を修正するには、適切なフィールドに新しい値を入力します。［イーサネットの設定（Ethernet Configuration）］ウィンドウの各フィールドの説明については、表 4-1 を参照してください。

（注）　DHCP を有効にすると、ポートとゲートウェイの設定は無効になり、変更できなくなります。

ステップ 3　変更内容を保存するには、**［保存（Save）］**をクリックします。

注意　サーバの IP アドレスまたはホスト名を変更すると、システムのパフォーマンスに影響する場合があります。

表 4-1　［イーサネットの設定（Ethernet Configuration）］のフィールドと説明

フィールド	説明
［DHCP］	DHCP が有効であるか無効であるかを示します。
［ホスト名（Hostname）］	サーバのホスト名を表示します。
［IP アドレス（IP Address）］	システムの IP アドレスを表示します。
［サブネットマスク（Subnet Mask）］	IP サブネット マスク アドレスを表示します。
［デフォルトゲートウェイ（Default Gateway）］	ネットワーク ゲートウェイの IP アドレスを表示します。

NTP サーバ

外部 NTP サーバがストラタム 9 またはそれより上位（つまり、ストラタム 1 ～ 9）であることを確認してください。外部 NTP サーバを追加、削除、または修正するには、次の手順を実行します。

（注） NTP サーバの設定値は、最初のノードまたはパブリッシャに限り設定できます。

手順

ステップ 1　［Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）］ウィンドウで、**［設定（Settings）］** > **［NTP サーバ（NTP Servers）］** に移動します。

［NTP サーバの設定（NTP Server Settings）］ウィンドウが表示されます。

ステップ 2　NTP サーバを追加、削除、または修正できます。

- NTP サーバを削除するには、適切なサーバの前にあるチェックボックスをオンにして、**［削除（Delete）］** をクリックします。
- NTP サーバを追加するには、**［追加（Add）］** をクリックし、ホスト名または IP アドレスを入力して、**［保存（Save）］** をクリックします。
- NTP サーバを修正するには、IP アドレスをクリックし、ホスト名または IP アドレスを修正して、**［保存（Save）］** をクリックします。

（注） NTP サーバに対する変更が完了するまでに、最大で 5 分かかることがあります。NTP サーバに対して変更を行った場合は、必ずウィンドウをリフレッシュして、正しいステータスを表示する必要があります。

ステップ 3　［NTP サーバの設定（NTP Server Settings）］ウィンドウをリフレッシュして正しいステータスを表示するには、**［設定（Settings）］** > **［NTP サーバ（NTP Servers）］** を選択します。

（注） NTP サーバを削除、変更、または追加したら、クラスタ内の他のすべてのノードを再起動し、変更を有効にする必要があります。

SMTP 設定

［SMTP 設定（SMTP Settings）］ウィンドウでは、SMTP ホスト名を表示または設定でき、SMTP ホストがアクティブであるかどうかが示されます。

ヒント　システムから電子メールが送信されるようにするには、SMTP ホストを設定する必要があります。

SMTP 設定にアクセスするには、次の手順を実行します。

手順

ステップ 1　［Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）］ウィンドウで、**［設定（Settings）］**>**［SMTP］**に移動します。

［SMTP 設定（SMTP Settings）］ウィンドウが表示されます。

ステップ 2　SMTP ホスト名または IP アドレスを入力または修正します。

ステップ 3　**［保存（Save）］**をクリックします。

時刻設定

時刻を手動で設定するには、次の手順を実行します。

（注） サーバの時刻を手動で設定する前に、設定済みの NTP サーバを削除する必要があります。詳細については、「NTP サーバ」を参照してください。

手順

ステップ 1　［Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）］ウィンドウで、**［設定（Settings）］** > **［時間（Time）］**に移動します。

ステップ 2　システムの日時を入力します。

ステップ 3　**［保存（Save）］**をクリックします。

ステップ 4　日付を変更したり、2 分を超えて時刻を変更した場合、CLI コマンド **utils system restart** を使用してサーバを再起動します。

CHAPTER 5

システムの再起動

この章は、次の項で構成されています。

バージョンを切り替えて再起動

新しいソフトウェア バージョンにアップグレードする場合、または以前のソフトウェア バージョンにフォールバックする必要がある場合、このオプションを使用できます。アクティブなディスク パーティションで動作しているシステムをシャットダウンしてから、非アクティブなパーティション上のソフトウェア バージョンを使用してシステムを自動的に再起動するには、次の手順を実行します。

注意 この手順を実行すると、システムが再起動して一時的にアウト オブ サービスになります。

手順

ステップ 1 ［Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）］ウィンドウで、**［設定（Settings）］** > **［バージョン（Version）］**に移動します。

［バージョン設定（Version Settings）］ウィンドウが表示され、アクティブなパーティション上と非アクティブなパーティション上の両方のソフトウェア バージョンが示されます。

ステップ 2 バージョンを切り替えて再起動するには、**［バージョンの切り替え（Switch Versions）］**をクリックします。操作を中止するには、**［キャンセル（Cancel）］**をクリックします。

［バージョンの切り替え（Switch Versions）］をクリックすると、システムが再起動し、現在非アクティブなパーティションがアクティブになります。

現在のバージョンの再起動

バージョンを切り替えずに現在のパーティションでシステムを再起動するには、次の手順を実行します。

注意　この手順を実行すると、システムが再起動して一時的にアウト オブ サービスになります。

手順

ステップ 1　［Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）］ウィンドウで、**［設定（Settings）］** > **［バージョン（Version）］**に移動します。

［バージョン設定（Version Settings）］ウィンドウが表示され、アクティブなパーティション上と非アクティブなパーティション上の両方のソフトウェア バージョンが示されます。

ステップ 2　システムを再起動するには、**［リスタート（Restart）］**をクリックします。操作を中止するには、**［キャンセル（Cancel）］**をクリックします。

［リスタート（Restart）］をクリックすると、バージョンを切り替えずに現在のパーティションでシステムが再起動します。

システムのシャットダウン

注意　サーバの電源ボタンを押すと、システムがただちにシャットダウンします。

システムをシャットダウンするには、次の手順を実行します。

注意　この手順を実行すると、システムがシャットダウンします。

手順

ステップ 1　［Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）］ウィンドウで、**［設定（Settings）］** > **［バージョン（Version）］**に移動します。

［バージョン設定（Version Settings）］ウィンドウが表示され、アクティブなパーティション上と非アクティブなパーティション上の両方のソフトウェア バージョンが示されます。

ステップ 2　システムをシャットダウンするには、**［シャットダウン（Shutdown）］**をクリックします。操作を中止するには、**［キャンセル（Cancel）］**をクリックします。

［シャットダウン（Shutdown）］をクリックすると、システムがすべてのプロセスを停止してシャットダウンします。

（注）　ハードウェアの電源は自動的に切断されません。

CHAPTER 6

セキュリティ

この章は、次の項で構成されています。

Internet Explorer のセキュリティ オプションの設定

サーバから証明書をダウンロードするには、Internet Explorer のセキュリティ設定値が次のように設定されていることを確認します。

手順

ステップ 1 Internet Explorer を起動します。

ステップ 2 ［**ツール**］>［**インターネット オプション**］に移動します。

ステップ 3 ［**詳細設定**］タブをクリックします。

ステップ 4 ［詳細設定］タブで、［セキュリティ］セクションまでスクロールダウンします。

ステップ 5 必要に応じて、［**暗号化されたページをディスクに保存しない**］チェックボックスをオフにします。

ステップ 6 ［**OK**］をクリックします。

証明書と証明書信頼リストの管理

次の各項では、［証明書の管理（Certificate Management）］メニューから実行できる機能を説明します。

- 証明書の表示
- 証明書または CTL のダウンロード
- 証明書の削除と再生成
- 証明書または証明書信頼リストのアップロード
- サードパーティの CA 証明書の使用方法
- 証明書の有効期限の監視

（注） ［セキュリティ（Security）］メニューの項目にアクセスするには、管理者パスワードを使用して Cisco Unified Communications オペレーティング システムの管理ページに再度ログインする必要があります。

証明書の表示

既存の証明書を表示するには、次の手順を実行します。

手順

ステップ 1　**［セキュリティ（Security）］> ［証明書の管理（Certificate Management）］**に移動します。

［証明書の一覧（Certificate List）］ウィンドウが表示されます。

ステップ 2　検索条件フィールドを使用して、証明書リストをフィルタリングできます。

ステップ 3　証明書または信頼ストアの詳細を表示するには、そのファイル名をクリックします。

［証明書の設定（Certificate Configuration）］ウィンドウに、証明書に関する情報が表示されます。

ステップ 4　［証明書の一覧（Certificate List）］ウィンドウに戻るには、［関連リンク（Related Links）］リストで**［検索 / リストに戻る（Back To Find/List）］**を選択し、**［移動（Go）］**をクリックします。

証明書または CTL のダウンロード

Cisco Unified Communications オペレーティング システムから PC に証明書または CTL をダウンロードするには、次の手順を実行します。

手順

ステップ 1　**［セキュリティ（Security）］> ［証明書の管理（Certificate Management）］**に移動します。

［証明書の一覧（Certificate List）］ウィンドウが表示されます。

ステップ 2　検索条件フィールドを使用して、証明書リストをフィルタリングできます。

ステップ 3　証明書または CTL のファイル名をクリックします。

［証明書の設定（Certificate Configuration）］ウィンドウが表示されます。

ステップ 4　**［ダウンロード（Download）］**をクリックします。

ステップ 5　［ファイルのダウンロード］ダイアログボックスで、**［保存］**をクリックします。

証明書の削除と再生成

次の各項では、証明書の削除と再生成について説明します。

- 証明書の削除
- 証明書の再生成

証明書の削除

信頼済み証明書を削除するには、次の手順を実行します。

注意　証明書を削除すると、システムの動作に影響する場合があります。［証明書の一覧（Certificate List）］で選択する証明書については、システムから既存の CSR がすべて削除されます。新しい CSR を生成する必要があります。詳細については、P.6-8 の「証明書署名要求の生成」の手順を参照してください。

手順

ステップ 1　**［セキュリティ（Security）］**>**［証明書の管理（Certificate Management）］**に移動します。

［証明書の一覧（Certificate List）］ウィンドウが表示されます。

ステップ 2　検索条件フィールドを使用して、証明書リストをフィルタリングできます。

ステップ 3　証明書または CTL のファイル名をクリックします。

［証明書の設定（Certificate Configuration）］ウィンドウが表示されます。

ステップ 4　**［削除（Delete）］**をクリックします。

証明書の再生成

証明書を再生成するには、次の手順を実行します。

注意　証明書を再生成すると、システムの動作に影響する場合があります。

手順

ステップ 1　［セキュリティ（Security）］>［証明書の管理（Certificate Management）］に移動します。

［証明書の一覧（Certificate List）］ウィンドウが表示されます。

ステップ 2　［新規作成（Generate New）］をクリックします。

［証明書の作成（Generate Certificate）］ダイアログボックスが開きます。

ステップ 3　［証明書の名前（Certificate Name）］リストから、証明書の名前を選択します。表示される証明書の名前の説明については、表 6-1 を参照してください。

ステップ 4　［新規作成（Generate New）］をクリックします。

表 6-1　証明書の名前と説明

名前	説明
［tomcat］	この自己署名ルート証明書は、HTTPS サーバのインストール中に生成されます。
［ipsec］	この自己署名ルート証明書は、MGCP ゲートウェイおよび H.323 ゲートウェイとの IPSec 接続のインストール中に生成されます。
［CallManager］	この自己署名ルート証明書は、Cisco Unified Communications Manager のインストール中に自動的にインストールされます。この証明書はサーバの名前と Global Unique Identifier（GUID; グローバル一意識別子）を含んでおり、サーバの ID となります。
［CAPF］	このルート証明書は、Cisco CTL クライアントの設定を完了すると、現在のサーバまたはクラスタ内のすべてのサーバにコピーされます。

証明書または証明書信頼リストのアップロード

注意　新しい証明書ファイルまたは Certificate Trust List（CTL; 証明書信頼リスト）ファイルをアップロードすると、システムの動作に影響する場合があります。新しい証明書または証明書信頼リストをアップロードした後は、［**Cisco Unified サービスアビリティ（Cisco Unified Serviceability）**］>［**Tools**］>［**Service Activation**］を選択して、Cisco CallManager サービスを再起動する必要があります。詳細については、『*Cisco Unified Serviceability アドミニストレーション ガイド*』を参照してください。

（注） システムが信頼証明書を他のクラスタ　ノードに自動的に配信することはありません。複数のノードで同じ証明書が必要な場合は、証明書を各ノードに個々にアップロードする必要があります。

次の各項では、CA ルート証明書、アプリケーション証明書、または CTL ファイルをサーバにアップロードする方法について説明します。

- 証明書のアップロード
- 証明書信頼リストのアップロード
- ディレクトリ信頼証明書のアップロード

証明書のアップロード

手順

ステップ 1　［**セキュリティ（Security）**］>［**証明書の管理（Certificate Management）**］に移動します。

［証明書の一覧（Certificate List）］ウィンドウが表示されます。

ステップ 2　［**証明書のアップロード（Upload Certificate）**］をクリックします。

［証明書のアップロード（Upload Certificate）］ダイアログボックスが開きます。

ステップ 3　［**証明書の名前（Certificate Name）**］リストから、証明書の名前を選択します。

ステップ 4　サードパーティの CA から発行されたアプリケーション証明書をアップロードする場合は、［**ルート証明（Root Certificate）**］テキスト ボックスに、CA ルート証明書の名前を入力します。CA ルート証明書をアップロードする場合は、このテキスト ボックスを空白のままにしておきます。

ステップ 5　次のいずれかの手順を実行して、アップロードするファイルを選択します。

- ［**ファイルのアップロード（Upload File）**］テキスト ボックスに、ファイルへのパスを入力します。
- ［**参照**］ボタンをクリックし、アップロードするファイルに移動してから、［**開く**］をクリックします。

ステップ 6　ファイルをサーバにアップロードするには、［**ファイルのアップロード（Upload File）**］ボタンをクリックします。

証明書信頼リストのアップロード

手順

ステップ 1　［セキュリティ（Security）］>［証明書の管理（Certificate Management）］に移動します。

［証明書の一覧（Certificate List）］ウィンドウが表示されます。

ステップ 2　［証明書のアップロード（Upload Certificate）］をクリックします。

［証明書信頼リストのアップロード（Upload Certificate Trust List）］ダイアログボックスが開きます。

ステップ 3　［証明書の名前（Certificate Name）］リストから、証明書の名前を選択します。

ステップ 4　サードパーティの CA から発行されたアプリケーション証明書をアップロードする場合は、［ルート証明（Root Certificate）］テキスト ボックスに、CA ルート証明書の名前を入力します。CA ルート証明書をアップロードする場合は、このテキスト ボックスを空白のままにしておきます。

ステップ 5　次のいずれかの手順を実行して、アップロードするファイルを選択します。

- ［ファイルのアップロード（Upload File）］テキスト ボックスに、ファイルへのパスを入力します。
- ［参照］ボタンをクリックし、アップロードするファイルに移動してから、［開く］をクリックします。

ステップ 6　ファイルをサーバにアップロードするには、［ファイルのアップロード（Upload File）］ボタンをクリックします。

ディレクトリ信頼証明書のアップロード

手順

ステップ 1　［セキュリティ（Security）］>［証明書の管理（Certificate Management）］に移動します。

［証明書の一覧（Certificate List）］ウィンドウが表示されます。

ステップ 2　［証明書のアップロード（Upload Certificate）］をクリックします。

［証明書信頼リストのアップロード（Upload Certificate Trust List）］ダイアログボックスが開きます。

ステップ 3　［証明書の名前（Certificate Name）］リストから、**directory-trust** を選択します。

ステップ 4　［ファイルのアップロード（Upload File）］フィールドに、アップロードするファイルを入力します。

ステップ 5　ファイルをアップロードするには、［ファイルのアップロード（Upload File）］ボタンをクリックします。

ステップ 6　Cisco Unified Serviceability にログインします。

ステップ 7　［**Tools**］>［**Control Center - Feature Services**］に移動します。

ステップ 8　サービス **Cisco Dirsync** を再起動します。

ステップ 9　Cisco Unified Communications オペレーティング システム CLI に管理者としてログインします。

ステップ 10　コマンド **utils service restart Cisco Tomcat** を入力し、Tomcat サービスを再起動します。

ステップ 11　サービスを再起動した後、SSL のためのディレクトリ契約を追加できます。

サードパーティの CA 証明書の使用方法

Cisco Unified Communications オペレーティング システムは、サードパーティの Certificate Authority（CA; 認証局）が PKCS # 10 Certificate Signing Request（CSR; 証明書署名要求）によって発行する証明書をサポートしています。次の表に、このプロセスの概要と参照先のドキュメントを示します。

	タスク	参照先
ステップ 1	サーバ上で CSR を生成する。	P.6-8 の「証明書署名要求の生成」を参照してください。
ステップ 2	CSR を PC にダウンロードする。	P.6-8 の「証明書署名要求のダウンロード」を参照してください。
ステップ 3	CSR を使用して、CA からアプリケーション証明書を取得する。	アプリケーション証明書の取得に関する情報は、CA から入手してください。その他の注意事項については、P.6-9 の「サードパーティの CA 証明書の取得」を参照してください。
ステップ 4	CA ルート証明書を取得する。	ルート証明書の取得に関する情報は、CA から入手してください。その他の注意事項については、P.6-9 の「サードパーティの CA 証明書の取得」を参照してください。
ステップ 5	CA ルート証明書をサーバにアップロードする。	P.6-5 の「証明書のアップロード」を参照してください。
ステップ 6	アプリケーション証明書をサーバにアップロードする。	P.6-5 の「証明書のアップロード」を参照してください。
ステップ 7	CAPF または Cisco Unified Communications Manager の証明書を更新した場合は、新しい CTL ファイルを生成する。	『*Cisco Unified Communications Manager セキュリティ ガイド*』を参照してください。
ステップ 8	新しい証明書によって影響を受けるサービスを再起動する。	すべての証明書タイプで、対応するサービスを再起動します（たとえば、Tomcat 証明書を更新した場合は、Tomcat サービスを再起動します）。さらに、CAPF または Cisco Unified Communications Manager の証明書を更新した場合は、TFTP サービスを再起動します。 サービスの再起動については、『*Cisco Unified Communications Manager Serviceability アドミニストレーション ガイド*』を参照してください。

証明書署名要求の生成

証明書署名要求（CSR）を生成するには、次の手順を実行します。

手順

ステップ 1　［セキュリティ（Security）］>［証明書の管理（Certificate Management）］に移動します。

［証明書の一覧（Certificate List）］ウィンドウが表示されます。

ステップ 2　［CSR の作成（Generate CSR）］をクリックします。

［証明書署名要求の作成（Generate Certificate Signing Request）］ダイアログボックスが開きます。

ステップ 3　［証明書の名前（Certificate Name）］リストから、証明書の名前を選択します。

（注） Cisco Unified オペレーティング システムの現行リリースでは、［証明書の名前（Certificate Name）］リストの［ディレクトリ（Directory）］オプションは使用できなくなりました。ただし、DirSync サービスをセキュア モードで実行する場合に必要となる、以前のリリースのディレクトリの信頼証明書はアップロードできます。

ステップ 4　［CSR の作成（Generate CSR）］をクリックします。

証明書署名要求のダウンロード

証明書署名要求をダウンロードするには、次の手順を実行します。

手順

ステップ 1　［セキュリティ（Security）］>［証明書の管理（Certificate Management）］に移動します。

［証明書の一覧（Certificate List）］ウィンドウが表示されます。

ステップ 2　［CSR のダウンロード（Download CSR）］をクリックします。

［証明書署名要求のダウンロード（Download Certificate Signing Request）］ダイアログボックスが開きます。

ステップ 3　［証明書の名前（Certificate Name）］リストから、証明書の名前を選択します。

ステップ 4　［CSR のダウンロード（Download CSR）］をクリックします。

ステップ 5　［ファイルのダウンロード］ダイアログボックスで、［保存］をクリックします。

サードパーティの CA 証明書の取得

サードパーティの CA が発行するアプリケーション証明書を使用するには、CA から署名付きアプリケーション証明書と CA ルート証明書の両方を取得する必要があります。これらの証明書の取得に関する情報は、CA から入手してください。証明書取得プロセスは、CA によって異なります。

CAPF および Cisco Unified Communications Manager の CSR には、CA へのアプリケーション証明書要求に含める必要のある拡張情報が含まれています。CA が ExtensionRequest メカニズムをサポートしていない場合は、CSR 生成プロセスの最後のページに一覧表示される X.509 拡張を有効にする必要があります。

Cisco Unified Communications オペレーティング システムは、証明書を DER および PEM 符号化フォーマットで生成し、CSR を PEM 符号化フォーマットで生成します。また、DER および PEM 符号化フォーマットの証明書を受け入れます。

証明書の有効期限の監視

証明書が有効期限に近づくと、システムから自動的に電子メールが送信されるようにすることができます。証明書モニタを表示および設定するには、次の手順を実行します。

手順

ステップ 1　証明書モニタの現在の設定を表示するには、**［セキュリティ（Security）］**>**［証明書モニタ（Certificate Monitor）］**に移動します。

［証明書モニタ（Certificate Monitor）］ウィンドウが表示されます。

ステップ 2　必要な設定情報を入力します。［証明書モニタ（Certificate Monitor）］の各フィールドの説明については、表 6-2 を参照してください。

ステップ 3　変更内容を保存するには、**［保存（Save）］**をクリックします。

表 6-2　［証明書モニタ（Certificate Monitor）］のフィールド説明

フィールド	説明
［通知開始時期（Notification Start Time）］	証明書が期限切れになる何日前に通知を受け取るかを入力します。
［通知の頻度（Notification Frequency）］	通知の頻度を時間単位または日単位で入力します。
［メール通知の有効化（Enable E-mail Notification）］	このチェックボックスをオンにすると、電子メール通知が有効になります。
［メール ID（Email IDs）］	通知の送信先となる電子メール アドレスを入力します。 **（注）**　システムが通知を送信するためには、SMTP ホストを設定する必要があります。

IPSEC の管理

次の各項では、IPSec のメニューで実行できる機能を説明します。

- 新しい IPSec ポリシーの設定
- 既存の IPSec ポリシーの管理

（注） IPSec は、インストール時にクラスタ内のノード間で自動的に設定されません。

新しい IPSec ポリシーの設定

新しい IPSec ポリシーおよびアソシエーションを設定するには、次の手順を実行します。

（注） システムのアップグレード中に IPSec ポリシーに対して行った変更は、すべて失われます。そのため、アップグレード中に IPSec ポリシーを修正したり作成したりしないでください。

注意 IPSec は、特に暗号化に関して、システムのパフォーマンスに影響を及ぼします。

手順

ステップ 1　**［セキュリティ（Security）］**>**［IPSEC 設定（IPSEC Configuration）］**に移動します。

［IPSEC ポリシーの一覧（IPSEC Policy List）］ウィンドウが表示されます。

ステップ 2　**［新規追加（Add New）］**をクリックします。

［IPSEC ポリシーの設定（IPSEC Policy Configuration）］ウィンドウが表示されます。

ステップ 3　［IPSEC ポリシーの設定（IPSEC Policy Configuration）］ウィンドウで、適切な情報を入力します。このウィンドウの各フィールドの説明については、表 6-3 を参照してください。

ステップ 4　新しい IPSec ポリシーを設定するには、**［保存（Save）］**をクリックします。

表 6-3　IPSEC ポリシーとアソシエーションのフィールド説明

フィールド	説明
［ポリシーグループ名（Policy Group Name）］	IPSec ポリシー グループの名前を指定します。この名前には、文字、数字、およびハイフンだけを使用できます。
［ポリシー名（Policy Name）］	IPSec ポリシーの名前を指定します。この名前には、文字、数字、およびハイフンだけを使用できます。
［認証方式（Authentication Method）］	認証方式を指定します。
［共有キー（Preshared Key）］	［認証方式（Authentication Method）］フィールドで［事前共有キー（Pre-shared Key）］を選択した場合は、事前共有鍵を指定します。
［ピアタイプ（Peer Type）］	ピアが同じタイプであるか異なるタイプであるかを指定します。
［着信先アドレス（Destination Address）］	宛先の IP アドレスまたは FQDN を指定します。
［着信先ポート（Destination Port）］	宛先のポート番号を指定します。
［ソースアドレス（Source Address）］	送信元の IP アドレスまたは FQDN を指定します。
［ソースポート（Source Port）］	送信元のポート番号を指定します。
［モード（Mode）］	Tunnel モードまたは Transport モードを指定します。
［リモートポート（Remote Port）］	宛先で使用するポート番号を指定します。
［プロトコル（Protocol）］	特定のプロトコルまたは［Any］を指定します。 • ［TCP］ • ［UDP］ • ［Any］
［暗号化アルゴリズム（Encryption Algorithm）］	ドロップダウン リストから、暗号化アルゴリズムを選択します。選択肢は次のとおりです。 • ［DES］ • ［3DES］
［ハッシュアルゴリズム（Hash Algorithm）］	ハッシュ アルゴリズムを指定します。 • ［SHA1］：フェーズ 1 IKE ネゴシエーションで使用されるハッシュ アルゴリズム • ［MD5］：フェーズ 1 IKE ネゴシエーションで使用されるハッシュ アルゴリズム
［ESP アルゴリズム（ESP Algorithm）］	ドロップダウン リストから、ESP アルゴリズムを選択します。選択肢は次のとおりです。 • ［NULL_ENC］ • ［DES］ • ［3DES］ • ［BLOWFISH］ • ［RIJNDAEL］
［フェーズ 1 のライフタイム（Phase One Life Time）］	フェーズ 1 IKE ネゴシエーションのライフタイムを秒単位で指定します。
［フェーズ 1 の DH（Phase One DH）］	ドロップダウン リストから、フェーズ 1 の DH 値を選択します。選択肢は［2］、［1］、［5］、［14］、［16］、［17］、および［18］です。

表 6-3　IPSEC ポリシーとアソシエーションのフィールド説明（続き）

フィールド	説明
［フェーズ 2 のライフタイム（Phase Two Life Time）］	フェーズ 2 IKE ネゴシエーションのライフタイムを秒単位で指定します。
［フェーズ 2 の DH（Phase Two DH）］	ドロップダウン リストから、フェーズ 2 の DH 値を選択します。選択肢は［2］、［1］、［5］、［14］、［16］、［17］、および［18］です。
［ポリシーの有効化（Enable Policy）］	このチェックボックスをオンにすると、ポリシーが有効になります。

既存の IPSec ポリシーの管理

既存の IPSec ポリシーを表示、有効化、無効化、または削除するには、次の手順を実行します。

（注） システムのアップグレード中に IPSec ポリシーに対して行った変更は、すべて失われます。そのため、アップグレード中に IPSec ポリシーを修正したり作成したりしないでください。

注意 IPSec は、特に暗号化に関して、システムのパフォーマンスに影響を及ぼします。

注意 既存の IPSec ポリシーに対する変更は、通常のシステム動作に影響する場合があります。

手順

ステップ 1　**［セキュリティ（Security）］** > **［IPSEC 設定（IPSEC Configuration）］** に移動します。

（注） ［セキュリティ（Security）］メニューの項目にアクセスするには、管理者パスワードを使用して Cisco Unified Communications オペレーティング システムの管理ページに再度ログインする必要があります。

［IPSEC ポリシーの一覧（IPSEC Policy List）］ウィンドウが表示されます。

ステップ 2　ポリシーを表示、有効化、または無効化するには、次の手順を実行します。

a. ポリシー名をクリックします。

［IPSEC ポリシーの設定（IPSEC Policy Configuration）］ウィンドウが表示されます。

b. ポリシーを有効または無効にするには、**［ポリシーの有効化（Enable Policy）］** チェックボックスを使用します。

c. **［保存（Save）］** をクリックします。

ステップ 3　1 つまたは複数のポリシーを削除するには、次の手順を実行します。

a. 削除するポリシーの隣にあるチェックボックスをオンにします。

［**すべてを選択（Select All）**］をクリックしてすべてのポリシーを選択したり、［**すべてをクリア（Clear All）**］をクリックしてすべてのチェックボックスをオフにしたりすることができます。

b. ［**選択項目の削除（Delete Selected）**］をクリックします。

CHAPTER 7

ソフトウェア アップグレード

この章では、Cisco Unity Connection のアップグレード方法および Cisco Unity Connection の言語のインストール方法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。

アップグレード前の作業

アップグレードを開始する前に、次の作業を実行してください。

- 新しいリリースのリリース ノートを読んで、新しい機能について理解し、システムに関係する他の製品（JTAPI、IPMA、RTMT、IPCC、ファイアウォールなど）とアップグレード中に対話する方法を把握します。

  Cisco Unity Connection のリリース ノートは http://cisco.com/en/US/products/ps6509/prod_release_notes_list.html で入手可能です。
- 新しいリリース用の必要なライセンス ファイルがあることを確認します。
- アップグレードを開始する前に、システムをバックアップします。

アップグレード前の作業が完了したら、P.7-2 の「ソフトウェアのアップグレードとインストール」に進みます。

ソフトウェアのアップグレードとインストール

システムの動作中に、サーバにアップグレード ソフトウェアをインストールできます。システムには、2 つのパーティション（アクティブなブート可能パーティションと非アクティブなブート可能パーティション）が存在します。システムは、アクティブなパーティションというマークが付いたパーティションで完全に起動して動作します。

アップグレード ソフトウェアをインストールする場合は、非アクティブなパーティションにインストールします。ソフトウェアのインストール中も、システムは正常に機能し続けます。準備ができた後、非アクティブなパーティションをアクティブにして、新しいアップグレード ソフトウェアでシステムをリブートします。システムが再起動すると、現在アクティブなパーティションが非アクティブなパーティションとして識別されます。次のアップグレードまで、現在のソフトウェアは非アクティブなパーティションに残ります。設定情報は、アクティブなパーティション内のアップグレード済みバージョンに自動的に移行されます。

クラスタ内のすべてのサーバで、同一リリースの Cisco Unity Connection が実行されている必要があります。唯一の例外は、クラスタ ソフトウェア アップグレードの実行中です。この間は、一時的な不一致が発生しても問題となりません。

何らかの理由でアップグレードを取り消す場合は、古いバージョンのソフトウェアを含む非アクティブなパーティションに切り替えてシステムを再起動することができます。ただし、ソフトウェアのアップグレード後に行った設定変更はすべて失われます。

（注） アクティブなパーティション上のデータベースだけに変更を加えることができます。非アクティブなパーティション上のデータベースは更新されません。アップグレード後にデータベースに変更を加えた場合は、パーティションの切り替え後にその変更を繰り返す必要があります。

パッチまたはアップグレード バージョンは、DVD（ローカル ソース）から、または Cisco Unity Connection サーバがアクセスできるネットワーク ロケーション（リモート ソース）からインストールできます。

（注） ソフトウェア アップグレード プロセスを開始する前に、必ずシステム データをバックアップしてください。詳細については、『*Disaster Recovery System アドミニストレーション ガイド*』を参照してください。

この項は、次の内容で構成されています。

クラスタの並行アップグレード

Cisco Unity Connection 7.x（アップグレードがサポートされるバージョン）を実行しているクラスタをアップグレードするには、パブリッシャ ノードを最初にアップグレードします。アップグレード バージョンの情報で install.conf ファイルが更新された後、後続のノードの並行アップグレードを開始できます。パブリッシャ ノードのアップグレード中に、Cisco Unified Communications オペレーティング システムの管理ページの［ソフトウェアのインストール / アップグレード（Software Installation/Upgrade）］ウィンドウまたはコマンドライン インターフェイス（CLI）を使用して、インストール ログを表示してください。

新しいバージョンをアクティブにする準備ができた後、最初のノードで新しいソフトウェアをアクティブにしてから、他のすべてのノードでもアクティブにする必要があります。

アップグレード ファイルの取得

アップグレード プロセスを開始する前に、適切なアップグレード ファイルを Cisco.com から取得する必要があります。詳細については、適切な Cisco Unity Connection リリース ノートの「インストールとアップグレードに関する情報」の項を参照してください。このドキュメントは、http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html にあります。

（注） システムが有効なファイルだと認識できなくなるため、パッチ　ファイルの名前は変更しないでください。

（注） ファイルを unzip または untar しないでください。unzip または untar した場合、アップグレード ファイルをシステムが読み取れないおそれがあります。

インストール プロセス中も、アップグレード ファイルにはローカル DVD かリモートの FTP または SFTP サーバからアクセスできます。アップグレード ファイルにアクセスするときに入力するディレクトリ名とファイル名では、大文字と小文字が区別されることに注意してください。

ローカル ソースからのソフトウェアのアップグレードまたはロケールのインストール

ローカル DVD を使用してソフトウェアをアップグレードするには、次の手順を実行します。

手順

ステップ 1　Cisco Unity Connection アップグレードを実行する場合は、ステップ 2 に進みます。

Cisco Unity Connection ロケールを追加する場合は、Connection Conversation Manager サービスおよび Connection Mixer サービスを停止します。

a. Cisco Unity Connection Serviceability を起動します。

b. ［**Tools**］>［**Control Center - Feature Services**］に移動します。

c. ［Critical Services］の［Connection Conversation Manager］行で、［**Stop**］をクリックします。

d. サービスが停止するまで待ちます。

e. ［Critical Services］の［Connection Mixer］行で、**［Stop］**をクリックします。

f. サービスが停止するまで待ちます。

ステップ 2　アップグレードするローカル サーバのディスク ドライブに新しい DVD を挿入します。

ステップ 3　ブラウザに次の URL を入力して、Cisco Unified Communications オペレーティング システムの管理ページにログインします。

http://*server-name***/cmplatform**

server-name は、サーバの名前または IP アドレスです。

ステップ 4　**［ソフトウェアアップグレード（Software Upgrades）］**>**［インストール / アップグレード（Install/Upgrade）］**に移動します。

［ソフトウェアのインストール / アップグレード（Software Installation/Upgrade）］ウィンドウが表示されます。

ステップ 5　**［ソース（Source）］**リストから、**［DVD/CD］**を選択します。

ステップ 6　［ディレクトリ（Directory）］フィールドに、CD または DVD 上のパッチ ファイルへのパスを入力します。

ファイルがルート ディレクトリにある場合、または ISO イメージの DVD を作成した場合は、［ディレクトリ（Directory）］フィールドにスラッシュ（/）を入力します。

ステップ 7　アップグレード プロセスを続行するには、**［次へ（Next）］**をクリックします。

ステップ 8　インストールするアップグレード バージョンを選択し、**［次へ（Next）］**をクリックします。

ステップ 9　次のウィンドウで、ダウンロードの進捗を監視します。

ステップ 10　Cisco Unity Connection のアップグレードを実行する場合は、ステップ 11 に進みます。

Cisco Unity Connection ロケールをインストールしており、別のロケールをインストールする場合は、**［他のソフトウェアをインストール（Install Another）］**をクリックし、ステップ 4 に戻ります。

別のロケールをインストールしない場合は、Connection Conversation Manager サービスおよび Connection Mixer サービスを再起動します。

a. Cisco Unity Connection Serviceability を起動します。

b. **［Tools］**>**［Control Center - Feature Services］**に移動します。

c. ［Critical Services］の［Connection Conversation Manager］行で、**［Start］**をクリックします。

d. サービスが開始されるまで待ちます。

e. ［Critical Services］の［Connection Mixer］行で、**［Start］**をクリックします。

f. サービスが開始されるまで待ちます。

g. 残りの手順をスキップします。

ステップ 11　アップグレードをインストールし、自動的にアップグレード済みパーティションに切り替えてリブートする場合は、**［アップグレードされたパーティションをリブート（Reboot to upgraded partition）］**を選択します。システムが再起動し、アップグレード済みソフトウェアを実行します。

ステップ 12　アップグレードをインストールした後に手動でアップグレード済みパーティションに切り替えてリブートする場合は、次の手順を実行します。

a. ［**アップグレード後にリブートしない（Do not reboot after upgrade）**］を選択します。

b. ［**次へ（Next）**］をクリックします。

アップグレードのステータスウィンドウにアップグレード ログが表示されます。

c. インストールが完了した後、［**終了（Finish）**］をクリックします。

d. システムを再起動してアップグレードをアクティブにするには、［**設定（Settings）**］>［**バージョン（Version）**］を選択し、［**バージョンの切り替え（Switch Versions）**］をクリックします。

システムが再起動し、アップグレード済みソフトウェアを実行します。

リモート ソースからのソフトウェアのアップグレードまたはロケールのインストール

ネットワーク ロケーションまたはリモート サーバからソフトウェアをアップグレードするには、次の手順を実行します。

（注）　Cisco Unified オペレーティング システムの管理ページにアクセスしている間は、ブラウザの制御機能（表示の更新や再読み込みなど）を使用しないでください。代わりに、インターフェイスに用意されているナビゲーション制御を使用します。

手順

ステップ 1　アップグレードするサーバからアクセスできる FTP サーバまたは SFTP サーバにアップグレード ファイルを置きます。

ステップ 2　Cisco Unity Connection のアップグレードを実行する場合は、ステップ 3 に進みます。

Cisco Unity Connection ロケールを追加する場合は、Connection Conversation Manager サービスおよび Connection Mixer サービスを停止します。

a. Cisco Unity Connection Serviceability を起動します。

b. ［**Tools**］>［**Control Center - Feature Services**］に移動します。

c. ［Critical Services］の［Connection Conversation Manager］行で、［**Stop**］をクリックします。

d. サービスが停止するまで待ちます。

e. ［Critical Services］の［Connection Mixer］行で、［**Stop**］をクリックします。

f. サービスが停止するまで待ちます。

ステップ 3　ブラウザに次の URL を入力して、Cisco Unified Communications オペレーティング システムの管理ページにログインします。

http://*server-name***/cmplatform**

server-name は、サーバの名前または IP アドレスです。

ステップ 4　［**ソフトウェアアップグレード（Software Upgrades）**］>［**インストール / アップグレード（Install/Upgrade）**］に移動します。

［ソフトウェアのインストール / アップグレード（Software Installation/Upgrade）］ウィンドウが表示されます。

ステップ 5　［**ソース（Source）**］リストから、［**リモートファイルシステム（Remote Filesystem）**］を選択します。

ステップ 6　［**ディレクトリ（Directory）**］フィールドに、リモート システム上のパッチ ファイルを含むディレクトリへのパスを入力します。

アップグレード ファイルが Linux サーバまたは Unix サーバ上にある場合は、ディレクトリ パスの先頭にスラッシュを入力する必要があります。たとえば、アップグレード ファイルが patches ディレクトリにある場合は、`/patches` と入力する必要があります。

アップグレード ファイルが Windows サーバ上に配置されている場合は、FTP サーバまたは SFTP サーバに接続することになるため、次のような適切な構文を使用するよう注意してください。

- パスの記述はスラッシュ（/）で開始し、パスの区切り文字には常にスラッシュを使用します。
- パスの先頭部分は、サーバ上の FTP または SFTP ルート ディレクトリにする必要があります。したがって、C: などのドライブ文字で開始される Windows 絶対パスは入力できません。

ステップ 7　［**サーバ（Server）**］フィールドに、サーバ名または IP アドレスを入力します。

ステップ 8　［**ユーザ名（User Name）**］フィールドに、リモート サーバ上のユーザ名を入力します。

ステップ 9　［**ユーザパスワード（User Password）**］フィールドに、リモート サーバ上のパスワードを入力します。

ステップ 10　［**転送プロトコル（Transfer Protocol）**］フィールドから、転送プロトコルを選択します。

ステップ 11　アップグレード プロセスを続行するには、［**次へ（Next）**］をクリックします。

ステップ 12　インストールするアップグレード バージョンを選択し、［**次へ（Next）**］をクリックします。

ステップ 13　次のウィンドウで、ダウンロードの進行状況を監視します。

（注）　アップグレード プロセスの進行中にサーバとの接続を失った場合、またはブラウザを閉じた場合は、［ソフトウェアアップグレード（Software Upgrades）］メニューに再度アクセスしようとすると、次のメッセージが表示されることがあります。

警告：別のセッションでソフトウェアがインストール中です。［制御の取得（Assume Control）］をクリックすると、インストールを引き継ぐことができます。（Warning: Another session is installing software, click Assume Control to take over the installation.）

セッションを最初からやり直す場合は、［**制御の取得（Assume Control）**］をクリックします。

［制御の取得（Assume Control）］が表示されない場合は、リアルタイム監視ツールでアップグレードを監視することもできます。

ステップ 14 アップグレード ソフトウェアをインストールする場合は、ステップ 15 に進みます。

Cisco Unity Connection ロケールをインストールしており、別のロケールをインストールする場合は、**［他のソフトウェアをインストール（Install Another）］**をクリックし、ステップ 4 に戻ります。

別のロケールをインストールしない場合は、Connection Conversation Manager サービスおよび Connection Mixer サービスを再起動します。

a. Cisco Unity Connection Serviceability を起動します。
b. **［Tools］** > **［Control Center - Feature Services］**に移動します。
c. ［Critical Services］の［Connection Conversation Manager］行で、**［Start］**をクリックします。
d. サービスが開始されるまで待ちます。
e. ［Critical Services］の［Connection Mixer］行で、**［Start］**をクリックします。
f. サービスが開始されるまで待ちます。
g. 残りの手順をスキップします。

ステップ 15 アップグレードをインストールし、自動的にアップグレード済みパーティションに切り替えてリブートする場合は、**［アップグレードされたパーティションをリブート（Reboot to upgraded partition）］**を選択します。システムが再起動され、アップグレードされたソフトウェアが実行されます。

ステップ 16 アップグレードをインストールした後に手動でアップグレード済みパーティションに切り替えてリブートする場合は、次の手順を実行します。

a. **［アップグレード後にリブートしない（Do not reboot after upgrade）］**を選択します。
b. **［次へ（Next）］**をクリックします。

   アップグレードのステータスウィンドウにアップグレード ログが表示されます。
c. インストールが完了した後、**［終了（Finish）］**をクリックします。
d. システムを再起動してアップグレードをアクティブにするには、**［設定（Settings）］** > **［バージョン（Version）］**を選択し、**［バージョンの切り替え（Switch Versions）］**をクリックします。

システムが再起動し、アップグレード済みソフトウェアを実行します。

アップグレードの途中停止

アップグレード ソフトウェアのインストール中に、アップグレードが途中停止したように見える場合があります。アップグレード ログは、新しいログ メッセージの表示を中止します。アップグレードが停止した場合は、アップグレードをキャンセルし、I/O スロットリングを無効にして、アップグレード手順をやり直す必要があります。アップグレードが正常に完了したときに、I/O スロットリングを再び有効にする必要はありません。

I/O スロットリングを無効にするには、CLI コマンド **utils iothrottle disable** を入力します。

I/O スロットリングのステータスを表示するには、CLI コマンド **utils iothrottle status** を入力します。

I/O スロットリングを有効にするには、CLI コマンド **utils iothrottle enable** を入力します。デフォルトでは、I/O スロットリングは有効になっています。

システムがキャンセルに応じない場合は、サーバをリブートし、I/O スロットリングを無効にして、アップグレード プロセスの手順をやり直す必要があります。

以前のバージョンに戻す

アップグレード後、システムを再起動して非アクティブなパーティション上のソフトウェア バージョンに切り替えることにより、アップグレード前に実行されていたソフトウェア バージョンに戻すことができます。

注意

Connection 2.x から 7.x にアップグレードした後に Connection 2.x に戻す場合、戻した後に Connection 7.x に再び切り替えることはできません。Connection 7.x へのアップグレードを再度インストールする必要があります。

Connection クラスタが設定されている場合、パブリッシャ サーバを Connection クラスタのないシングル サーバに変換してから 2.x に戻す必要があります。これは、2.x が Connection クラスタをサポートしていないためです。

この項は、次の内容で構成されています。

スタンドアロン サーバまたはクラスタを以前のバージョンに戻す

スタンドアロン サーバまたはクラスタを以前のバージョンに戻すには、次の主要手順を実行します。

	タスク	詳細情報の参照先
ステップ 1	Connection サーバまたはパブリッシャ ノードを戻す（Connection クラスタが設定されている場合）。	Connection サーバまたはパブリッシャ ノードを戻す（Connection クラスタが設定されている場合）（P.7-9）
ステップ 2	サブスクライバ ノードを戻す（Connection クラスタが設定されている場合）。	サブスクライバ ノードを以前のバージョンに戻す（P.7-9）

Connection サーバまたはパブリッシャ ノードを戻す（Connection クラスタが設定されている場合）

手順

ステップ 1　次の URL を入力して、Cisco Unified Communications オペレーティング システムの管理ページを直接開きます。

https://*server-name*/**cmplatform**

ここで、*server-name* は Cisco Unity Connection サーバのホスト名または IP アドレスです。

ステップ 2　管理者ユーザ名とパスワードを入力します。

ステップ 3　［**設定（Settings）**］>［**バージョン（Version）**］を選択します。

［バージョン設定（Version Settings）］ウィンドウが表示されます。

ステップ 4　［**バージョンの切り替え（Switch Versions）**］ボタンをクリックします。

システムの再起動について確認すると、システムが再起動します。処理が完了するまでに、最大で 15 分かかることがあります。

ステップ 5　バージョンの切り替えが正常に完了したことを確認するには、次の手順を実行します。

a. 開かれている Cisco Unified Communications オペレーティング システムの管理ページに再度ログインします。

b. ［**設定（Settings）**］>［**バージョン（Version）**］を選択します。

［バージョン設定（Version Settings）］ウィンドウが表示されます。

c. アクティブなパーティションで、適切な製品バージョンが実行されていることを確認します。

d. アクティブにしたサービスがすべて動作していることを確認します。

e. 次の URL を入力し、ユーザ名とパスワードを入力して Cisco Unified CM の管理ページにログインします。

https://*server-name*/**ccmadmin**

f. ログインできること、および設定データが存在することを確認します。

サブスクライバ ノードを以前のバージョンに戻す

手順

ステップ 1　次の URL を入力して、Cisco Unified Communications オペレーティング システムの管理ページを直接開きます。

https://*server-name*/**cmplatform**

ここで、*server-name* は Cisco Unified Communications Manager サーバのホスト名または IP アドレスです。

ステップ 2　管理者ユーザ名とパスワードを入力します。

ステップ 3　［**設定（Settings）**］>［**バージョン（Version）**］を選択します。

［バージョン設定（Version Settings）］ウィンドウが表示されます。

ステップ 4　［**バージョンの切り替え（Switch Versions）**］ボタンをクリックします。

システムの再起動について確認すると、システムが再起動します。処理が完了するまでに、最大で 15 分かかることがあります。

ステップ 5　バージョンの切り替えが正常に完了したことを確認するには、次の手順を実行します。

a. 開かれている Cisco Unified Communications オペレーティング システムの管理ページに再度ログインします。

b. ［**設定（Settings）**］>［**バージョン（Version）**］を選択します。

［バージョン設定（Version Settings）］ウィンドウが表示されます。

c. アクティブなパーティションで、適切な製品バージョンが実行されていることを確認します。

d. アクティブにしたサービスがすべて動作していることを確認します。

ロケールのインストール

Cisco Unity Connection ロケール（言語）は、国別のシステム プロンプト、グラフィカル ユーザ インターフェイス、およびテキスト / スピーチ機能を提供します。Cisco Unity Connection のロケールのダウンロードについては、http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html にある適切な Cisco Unity Connection リリース ノートの「インストールとアップグレードに関する情報」の項を参照してください。

注意　5 個を超える Cisco Unity Connection ロケールをインストールしないでください。

ロケールのインストール

この章で前述したソフトウェア アップグレードのインストール プロセスと同じプロセスで、ローカル ソースまたはリモート ソースからロケール ファイルをインストールできます。このプロセスの詳細については、P.7-2 の「ソフトウェアのアップグレードとインストール」を参照してください。

（注）　新しくインストールしたロケールをアクティブにするには、サーバを再起動する必要があります。

CHAPTER 8

サービス

この章では、別のシステムに対する PING の実行やリモート サポートの設定など、オペレーティング システムで使用可能なユーティリティ機能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。

PING

PING ユーティリティのウィンドウでは、ネットワーク内の別のサーバに対して PING を実行できます。

別のシステムに対して PING を実行するには、次の手順を実行します。

手順

ステップ 1　［Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）］ウィンドウで、**［サービス（Services）］** > **［Ping］** に移動します。

［Ping の設定（Ping Configuration）］ウィンドウが表示されます。

ステップ 2　PING の対象となるシステムの IP アドレスまたはネットワーク名を入力します。

ステップ 3　PING の間隔を秒単位で入力します。

ステップ 4　パケット サイズを入力します。

ステップ 5　PING 回数（システムに対して PING を実行する回数）を入力します。

（注）　複数の PING を指定した場合は、Ping コマンドで PING の日時がリアルタイムに表示されません。Ping コマンドでは、指定した回数の PING が完了した後、データが表示されることに注意してください。

ステップ 6　IPSec を確認するかどうかを選択します。

ステップ 7　**［Ping］** をクリックします。

［Ping の設定（Ping Configuration）］ウィンドウに PING 統計情報が表示されます。

リモート サポート

［リモートアクセスの設定（Remote Access Configuration）］ウィンドウでは、シスコのサポート担当者が指定された時間にシステムにアクセスできるリモート アカウントを設定できます。

リモート サポート プロセスは、次のように機能します。

1. お客様がリモート サポート アカウントを設定します。このアカウントには、設定可能な有効期限が含まれています。この有効期限によって、シスコ担当者がこのアカウントにアクセスできる期間が決まります。
2. リモート サポート アカウントが設定されると、パス フレーズが生成されます。
3. お客様がシスコ サポートに電話をかけ、リモート サポート アカウント名とパス フレーズを伝えます。
4. シスコ サポートがパス フレーズをデコーダ プログラムに入力すると、パス フレーズからパスワードが生成されます。
5. シスコ サポートが、デコードされたパスワードを使用して、お客様のシステムのリモート サポート アカウントにログインします。
6. アカウントの有効期限が切れると、シスコ サポートはリモート サポート アカウントにアクセスできなくなります。

リモート サポートを設定するには、次の手順を実行します。

手順

ステップ 1　［Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）］ウィンドウで、**［サービス（Services）］** > **［リモートサポート（Remote Support）］**に移動します。

［リモートアクセスの設定（Remote Access Configuration）］ウィンドウが表示されます。

ステップ 2　**［アカウント名（Account Name）］**フィールドに、リモート アカウントのアカウント名を入力します。

アカウント名は、6 文字以上で、すべて英小文字にする必要があります。

ステップ 3　**［アカウントの有効期限（Account Duration）］**フィールドに、アカウントの有効期限を日数で入力します。

デフォルトのアカウント有効期限は 30 日間です。

ステップ 4　**［保存（Save）］**をクリックします。

［リモートアクセスの設定（Remote Access Configuration）］ウィンドウが表示されます。［リモートアクセスの設定（Remote Access Configuration）］ウィンドウの各フィールドの説明については、表 8-1 を参照してください。

ステップ 5　生成されたパス フレーズを使用してシステムにアクセスするには、シスコ担当者に問い合せます。

ステップ 6　リモート アクセス サポート アカウントを削除するには、**［削除（Delete）］**ボタンをクリックします。

表 8-1　［リモートアクセスの設定（Remote Access Configuration）］のフィールドと説明

フィールド	説明
［デコードバージョン（Decode version）］	使用されるデコーダのバージョンを示します。
［アカウント名（Account name）］	リモート サポート アカウントの名前を表示します。
［期限切れ（Expiration）］	リモート アカウントへのアクセスが期限切れになる日時を表示します。
［パスフレーズ（Passphrase）］	生成されたパス フレーズを表示します。

INDEX

さ

し

す

せ

そ

ね

の

は

ひ

ふ

め

り

ろ