Cisco Unified Communications オペレーティング システム アドミニストレーション ガイド

Cisco Unified Communications Operating System Administration Guide

リリース 8.0(2)

Text Part Number: OL-21897-01-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。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

CONTENTS

はじめに vii

目的 vii

対象読者 vii

マニュアルの構成 vii

関連資料 viii

表記法 viii

マニュアルの入手方法およびテクニカル サポート ix

シスコ製品のセキュリティ ix

CHAPTER 1 概要 1-1

概要 1-1

ブラウザの要件 1-2

オペレーティング システムのステータスと設定 1-2

設定 1-2

セキュリティ設定 1-3

ソフトウェア アップグレード 1-3

サービス 1-4

コマンドライン インターフェイス 1-4

CHAPTER 2 Cisco Unified Communications オペレーティング システムの管理へのログイン 2-1

Cisco Unified Communications オペレーティング システムの管理へのログイン 2-1

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 2-2

CHAPTER 3 ステータスと設定 3-1

クラスタ ノード 3-1

ハードウェアのステータス 3-2

ネットワーク設定 3-2

インストールされているソフトウェア 3-3

システムのステータス 3-4

IP プリファレンス 3-5

CHAPTER 4 設定 4-1
IP Settings 4-1
イーサネット設定 4-1
イーサネット IPv6 設定 4-2
パブリッシャ設定 4-3
Cisco Unified Communications Manager 後続ノードでの IP アドレスの変更 4-4
NTP サーバ 4-4
SMTP 設定 4-5
時刻設定 4-6

CHAPTER 5 システムの再起動 5-1
バージョンの切り替えと再起動 5-1
現在のバージョンの再起動 5-2
システムのシャットダウン 5-2

CHAPTER 6 セキュリティ 6-1
Internet Explorer のセキュリティ オプションの設定 6-1
証明書と Certificate Trust List の管理 6-1
証明書の表示 6-2
証明書のダウンロード 6-2
証明書の削除と再作成 6-2
証明書の削除 6-3
証明書の再作成 6-3
証明書または Certificate Trust List のアップロード 6-4
証明書のアップロード 6-5
Certificate Trust List のアップロード 6-5
ディレクトリの信頼証明書のアップロード 6-5
サードパーティ製の CA 証明書の使用法 6-6
証明書署名要求の作成 6-7
証明書署名要求のダウンロード 6-7
サードパーティ製の CA 証明書の取得 6-8
証明書の有効期限日の監視 6-9
IPSEC 管理 6-9
新しい IPSec ポリシーの設定 6-9
既存の IPSec ポリシーの管理 6-11
Bulk Certificate Management 6-12
証明書のエクスポート 6-12
証明書のインポート 6-13

CHAPTER 7 ソフトウェア アップグレード 7-1
アップグレード前の作業 7-1
ソフトウェア アップグレードの考慮事項 7-3
ソフトウェア アップグレード手順の概要 7-3
アップグレード時の設定の変更 7-4
管理の変更 7-4
ユーザ プロビジョニング 7-6
クラスタの並行アップグレード 7-6
サポートされるアップグレード 7-7
Cisco Unified Communications Manager Release 6.0(1) よりも前のリリースから Release 6.0(1) 以降へのアップグレード 7-7
Cisco Unified Communications Manager Release 6.0(1) よりも前のリリースから Release 7.0(1) 以降へのアップグレード 7-8
Cisco Unified Communications ManagerRelease 5.1(3e) から 7.1.x Release へのアップグレード 7-8
5.x リリースからのアップグレードにおけるパーティションのサイズ制限 7-9
アップグレード ファイルの取得 7-9
サポートされる SFTP サーバ 7-10
I/O スロットリングの影響 7-11
概要 7-11
サーバ モデル 7-11
書き込みキャッシュ 7-11
ソフトウェア アップグレード手順 7-13
ローカル ソースからのアップグレード 7-13
リモート ソースからのアップグレード 7-14
ブリッジ アップグレード 7-16
アップグレード後の作業 7-17
アップグレードの途中停止 7-18
以前のバージョンへの復帰 7-18
以前のバージョンへのクラスタの復帰 7-18
以前のバージョンへのパブリッシャ ノードの復帰 7-19
以前のバージョンへのサブスクライバ ノードの復帰 7-20
以前の製品リリースに戻す場合のデータベース複製の再設定 7-20
COP ファイル、ダイヤル プラン、およびロケールのインストール 7-20
COP ファイルのインストール 7-21
ダイヤル プランのインストール 7-21
ロケールのインストール 7-21
ロケールのインストール 7-22
Cisco Unified Communications Manager ロケール ファイル 7-22

エラー メッセージ 7-22
サポートされる Cisco Unified Communication 製品 7-23
TFTP サーバ ファイルの管理 7-24
カスタム ログオン メッセージの設定 7-25

CHAPTER 8 サービス 8-1
ping 8-1
リモート サポート 8-2

INDEX

はじめに

目的

このマニュアルでは、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。

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 Unifed Communications Solutions*』を参照してください。

対象読者

このマニュアルは、Cisco Unified Communications オペレーティング システムの管理および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 エンジニア、システム管理者、またはテレコム エンジニアはこのマニュアルを使用して、オペレーティング システムの機能を学習し管理します。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。

マニュアルの構成

次の表は、このマニュアルの構成を示しています。

章	説明
「概要」	この章では、Cisco Unified Communications オペレーティング システムで使用できる機能の概要について説明します。
「Cisco Unified Communications オペレーティング システムの管理へのログイン」	この章では、Cisco Unified Communications オペレーティング システムにログインする手順、および紛失した管理パスワードの回復手順について説明します。
「ステータスと設定」	この章では、オペレーティング システムのステータスおよび設定を表示する手順について説明します。
「設定」	この章では、イーサネット設定、IP 設定、および NTP 設定の表示および変更手順について説明します。

章	説明
「システムの再起動」	この章では、システムの再起動およびシャットダウンの手順について説明します。
「セキュリティ」	この章では、証明書の管理および IPSec の管理の手順について説明します。
「ソフトウェア アップグレード」	この章では、ソフトウェア アップグレードをインストールする手順および TFTP サーバにファイルをアップロードする手順について説明します。
「サービス」	この章では、ping およびリモート サポートを含むオペレーティング システムが提供するユーティリティの使用手順について説明します。

関連資料

関連する Cisco IP テレフォニーのアプリケーションおよび製品の詳細については、次の URL にある該当するリリース番号の『*Cisco Unified Communications Manager Documentation Guide*』を参照してください。

http://cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html

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。

表記法	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。
string	引用符を付けない一組の文字。string 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 string とみなされます。
`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。
	この矢印は、例の中の重要な行やテキストを強調するためのものです。
^	^ 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 情報は、*役立つ「ヒント」の意味です。*

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。機器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、一般的な事故防止対策に留意してください。**

マニュアルの入手方法およびテクニカル サポート

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

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

シスコ製品のセキュリティ

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国での法律を順守するものとします。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

米国の輸出規制の詳細については、次の URL で参照できます。

http://www.access.gpo.gov/bis/ear/ear_data.html

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」
- 「ブラウザの要件」
- 「オペレーティング システムのステータスと設定」
- 「セキュリティ設定」
- 「ソフトウェア アップグレード」
- 「サービス」
- 「コマンドライン インターフェイス」

概要

Cisco Unified Communications オペレーティング システムの管理では、Cisco Unified Communications オペレーティング システムの設定と管理ができます。管理タスクの例として、次のようなものがあげられます。

- ソフトウェアとハードウェアのステータスを確認する。
- IP アドレスの確認と更新を行う。
- 他のネットワーク デバイスに ping を送信する。
- 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。
- サーバをセキュリティ管理する（IPSec や証明書なども含む）。
- 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 システムの各機能の詳細について説明します。

ブラウザの要件

Cisco Unified Communications オペレーティング システムにアクセスするには、次のブラウザが必要です。

Cisco Unified Communications オペレーティング システムへのアクセスに使用するブラウザ	使用するオペレーティング システム
Microsoft Internet Explorer 7	Microsoft XP SP3
Microsoft Internet Explorer 8	• Microsoft XP SP3 • Microsoft Vista SP2
Mozilla Firefox 3.x	• Microsoft XP SP3 • Microsoft Vista SP2 • Apple MAC OS X
Safari 4.x	Apple MAC OS X

製品のすべての機能が正常に動作するには、ブラウザの「信頼済みサイト」や「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

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

- クラスタおよびノード
- 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とオプション

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

[Settings] メニューから、オペレーティング システムに関する次の設定の表示と更新ができます。

- [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）クライアントの設定を更新します。
- [NTP Server] 設定：外部 NTP サーバの IP アドレスの設定、および NTP サーバの追加と削除ができます。
- [SMTP settings]：オペレーティング システムが E 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。

[Settings] > [Version] ウィンドウでは、システムの再起動やシャットダウンに関する次のオプションを選択できます。

- [Switch Version]：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て、システムを再起動します。通常、このオプションを選択するのは、非アクティブなパーティションを更新し、新しいバージョンのソフトウェアを実行する場合です。
- [Current Version]：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。
- [Shutdown System]：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）　このコマンドでは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、電源ボタンを押します。

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と Secure Internet Protocol（IPSec）を管理できます。[Security] メニューでは、次のセキュリティ オプションを選択できます。

- [Certificate Management]：証明書および証明書署名要求（CSR）を管理します。証明書の表示、アップロード、ダウンロード、削除、および再作成ができます。[Certificate Management] を使用すると、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 Management]：既存の IPSEC ポリシーの表示または更新、新規の IPSEC ポリシーとアソシエーション設定を行います。

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 オプションを使用すると、オペレーティング システムで実行され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 ロケール インストーラ、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できます。

[Install/Upgrade] メニュー オプションで、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。アップグレードされ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、その後でシステムの再起動とパーティションの切り替えができます。これにより、システムは新しいソフトウェアのバージョンで再起動します。

（注）　Cisco Unified Communications オペレーティング システム 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。システムでアップロードと処理が可能なソフトウェアは、シスコシステムズが承認したものに限られます。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では、次のオペレーティング システム ユーティリティを使用できます。

- ping：他のネットワーク デバイスとの接続を確認します。
- リモート サポート：シスコのサポート担当者がシステムへのアクセスに使用するアカウントを設定できます。このアカウントは、指定した日数が経過すると自動的に失効します。

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アクセスするには、コンソールを使用するか、サーバにセキュア シェル接続します。詳細については、『*Command Line Interface Reference Guide for Cisco Unifed Communications 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 システムの管理にアクセスする手順および紛失したパスワードを回復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 システムの管理へのログイン」（P.2-1）
- 「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」（P.2-2）

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

Cisco Unified Communications オペレーティング システムの管理にアクセスしてログインするには、次の手順に従います。

（注） Cisco Unified Communications オペレーティング システムの管理を使用する場合、ブラウザのコントロール（[Back] ボタンなど）は使用しないでください。

手順

ステップ 1 Cisco Unified Communications Manager Administration にログインします。

ステップ 2 [Cisco Unified Communications Manager Administration] ウィンドウの右上にある [Navigation] メニューで [Cisco Unified OS Administration] を選択し、[Go] をクリックします。

[Cisco Unified Communications Operating System Administration Logon] ウィンドウが表示されます。

（注） また、「http://*server-name*/cmplatform」という形式の URL を入力して Cisco Unified Communications オペレーティング システムの管理に直接アクセスすることもできます。

ステップ 3 管理者用の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、インストール時に決めるか、コマンドライン インターフェイスを使用して作成します。

ステップ 4　[Submit] をクリックします。

[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

管理者パスワードやセキュリティ パスワードがわからなくなった場合、次の手順に従って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 コンソール経由でシステムに接続している必要があります。つまり、キーボードとモニタをサーバに接続している必要があります。システムにセキュア シェル接続している状態で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 Communications Manager Administration ウィンドウで問題が発生します。

（注）　システムに物理的にアクセスできることを証明するため、この手順の実行中に、ディスク ドライブから有効な CD または DVD を取り出して再挿入する必要があります。

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 や DVD が取り出されていることをシステムが確認します。

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

（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ていることをシステムが確認します。

ステップ 6　ディスクが挿入されていることをシステムが確認した後、次のいずれかのオプションを入力して続行するよう要求されます。

- **a** を入力して、管理者パスワードをリセットする。
- **s** を入力して、セキュリティ パスワードをリセットする。
- **q** を入力して終了する。

ステップ 7　選択したタイプの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入力します。

パスワードには 6 文字以上が必要です。システムが新しいパスワードの有効性を確認します。パスワードが有効性テストに合格しない場合、新しいパスワードを入力するよう要求されます。

ステップ 9　システムが新しいパスワードの有効性を確認すると、パスワードはリセットされ、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。この章は次の内容で構成されています。

- 「クラスタ ノード」
- 「ハードウェアのステータス」
- 「ネットワーク設定」
- 「インストールされているソフトウェア」
- 「システムのステータス」
- 「IP プリファレンス」

クラスタ ノード

クラスタ内の各ノードの情報を表示するには、次の手順に従います。

手順

ステップ 1 [Cisco Unified Communications Operating System Administration] ウィンドウで [Show] > [Cluster] の順に移動します。

[Cluster Nodes] ウィンドウが表示されます。

ステップ 2 [Cluster Nodes] ウィンドウの各フィールドについては、表 3-1 を参照してください。

表 3-1 [Cluster Nodes] のフィールドの説明

フィールド	説明
Hostname	サーバの完全なホスト名が表示されます。
IP Address	サーバの IP アドレスが表示されます。
Alias	サーバのエイリアス名が設定されている場合は、そのエイリアス名が表示されます。
Type of Node	サーバがパブリッシャ ノードであるかサブスクライバ ノードであるかを表します。

ハードウェアのステータス

ハードウェアのステータスを表示するには、次の手順に従います。

手順

ステップ 1　[Cisco Unified Communications Operating System Administration] ウィンドウから [Show] > [Hardware] の順に移動します。

[Hardware Status] ウィンドウが表示されます。

ステップ 2　[Hardware Status] ウィンドウの各フィールドについては、表 3-2 を参照してください。

表 3-2　[Hardware Status] のフィールドの説明

フィールド	説明
Platform Type	プラットフォーム サーバのモデル ID が表示されます。
Processor Speed	プロセッサの速度が表示されます。
CPU Type	プラットフォーム サーバのプロセッサのタイプが表示されます。
Memory	メモリの合計量が MB 単位で表示されます。
Object ID	オブジェクト ID が表示されます。
OS Version	オペレーティング システムのバージョンが表示されます。
RAID Details	RAID ドライブの詳細（コントローラの情報、論理ドライブの情報、物理デバイスの情報など）が表示されます。

ネットワーク設定

表示されるネットワーク ステータス情報は、ネットワークの耐障害性がイネーブルになっているかどうかによって異なります。ネットワークの耐障害性が有効になっていると、イーサネット ポート 0 に障害が発生した場合、イーサネット ポート 1 が自動的にネットワーク通信を継承します。ネットワークの耐障害性がイネーブルになっている場合、ネットワーク ポートのイーサネット 0、イーサネット 1、および Bond 0 のネットワーク ステータス情報が表示されます。ネットワークの耐障害性がイネーブルになっていない場合、イーサネット 0 のステータス情報のみが表示されます。

ネットワークのステータスを表示するには、次の手順に従います。

手順

ステップ 1　[Cisco Unified Communications Operating System Administration] ウィンドウから [Show] > [Network] の順に移動します。

[Network Settings] ウィンドウが表示されます。

ステップ 2　[Network Settings] ウィンドウの各フィールドについては、表 3-3 を参照してください。

表 3-3　[Network Configuration] のフィールドの説明

フィールド	説明
イーサネットの詳細	
DHCP	イーサネット ポート 0 に対して DHCP がイネーブルになっているかどうかを表します。
Status	イーサネット ポート 0 および 1 について、ポートがアップまたはダウンのどちらであるかを表します。
IP Address	イーサネット ポート 0 の IP アドレス（Network Fault Tolerance（NFT; ネットワークの耐障害性）がイネーブルの場合はイーサネット ポート 1 も）が表示されます。
IP Mask	イーサネット ポート 0 の IP マスク（NFT がイネーブルの場合はイーサネット ポート 1 も）が表示されます。
Link Detected	アクティブ リンクが存在するかどうかを表します。
Queue Length	キューの長さが表示されます。
MTU	最大伝送ユニットが表示されます。
MAC Address	ポートのハードウェア アドレスが表示されます。
Receive Statistics (RX)	受信したバイト数、パケット数、エラー数、ドロップやオーバーランの統計情報が表示されます。
Transmit Statistics (TX)	送信したバイト数、パケット数、エラー数、ドロップ、搬送波、衝突の統計情報が表示されます。
DNS の詳細	
Primary	プライマリ ドメイン ネーム サーバの IP アドレスが表示されます。
Secondary	セカンダリ ドメイン ネーム サーバの IP アドレスが表示されます。
Options	設定されている DNS オプションが表示されます。
Domain	サーバのドメインが表示されます。
Gateway	イーサネット ポート 0 のネットワーク ゲートウェイの IP アドレスが表示されます。

インストールされているソフトウェア

ソフトウェア バージョンと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 Operating System Administration] ウィンドウから [Show] > [Software] の順に移動します。

[Software Packages] ウィンドウが表示されます。

ステップ 2　[Software Packages] ウィンドウの各フィールドについては、表 3-4 を参照してください。

表 3-4　[Software Packages] のフィールドの説明

フィールド	説明
Partition Versions	アクティブ パーティションと非アクティブ パーティションで実行中のソフトウェアのバージョンが表示されます。
Active Version Installed Software Options	インストールされているソフトウェア オプションのバージョンを示します。これには、アクティブ バージョンにインストールされているロケールとダイヤル プランも含まれます。
Inactive Version Installed Software Options	インストールされているソフトウェア オプションのバージョンを示します。これには、アクティブでないバージョンにインストールされているロケールとダイヤル プランも含まれます。

システムのステータス

システムのステータスを表示するには、次の手順に従います。

手順

ステップ 1　[Cisco Unified Communications Operating System Administration] ウィンドウから [Show] > [System] の順に移動します。

[System Status] ウィンドウが表示されます。

ステップ 2　[Platform Status] ウィンドウの各フィールドについては、表 3-5 を参照してください。

表 3-5　[Platform Status] のフィールドの説明

フィールド	説明
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 ホストの名前が表示されます。
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た日時が表示されます。
Time Zone	インストール時に選択された時間帯が表示されます。
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が表示されます。
Product Version	オペレーティング システムのバージョンが表示されます。
Platform Version	プラットフォームのバージョンが表示されます。
Uptime	システムのアップタイム情報が表示されます。

表 3-5　[Platform Status] のフィールドの説明 （続き）

フィールド	説明
CPU	CPU のキャパシティのうち、アイドル状態である割合、システム プロセスを実行している割合、ユーザ プロセスを実行している割合がそれぞれパーセント単位で表示されます。
Memory	メモリの使用状況に関する情報（メモリの合計量、メモリの空き容量、メモリの使用量）がそれぞれ KB 単位で表示されます。
Disk/active	アクティブなディスクの容量の合計、空き容量、使用量が表示されます。
Disk/inactive	非アクティブなディスクの容量の合計、空き容量、使用量が表示されます。
Disk/logging	ディスクの容量の合計、空き容量、ディスク ロギングで使用している容量が表示されます。

IP プリファレンス

[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 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
- プロトコル
- ポート番号
- タイプ
- 変換ポート
- ステータス
- 説明

[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 Operating System Administration] ウィンドウで、[Show] > [IP Preferences] を選択します。

[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）照会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、[Clear Filter] ボタンをクリックします。

ステップ 3　[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、[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 Preferences] フィールドの説明については、次を参照してください。

表 3-6　[IP Preferences] フィールドの説明

フィールド	説明
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。
Protocol	このポートで使用されているプロトコル（TCP や UDP など）。
Port Number	ポート番号（数値）。
Type	このポートで許可されるトラフィックのタイプ。 • [Public]：すべてのトラフィックが許可される • [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 • [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
Translated Port	このポートを宛先とするトラフィックは、[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、[Translated] タイプのポートのみです。
Status	ポートの使用状況。 • [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 • [Disabled]：ファイアウォールでブロックされていて、未使用状態
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）設定の表示と変更をするには、設定オプションを使用します。

この章の内容は、次のとおりです。

- 「IP Settings」（P.4-1）
- 「NTP サーバ」（P.4-4）
- 「SMTP 設定」（P.4-5）
- 「時刻設定」（P.4-6）

IP Settings

[IP Settings] 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、後続ノードではパブリッシャの IP アドレスを設定できます。

この項は、次の内容で構成されています。

- 「イーサネット設定」（P.4-1）
- 「パブリッシャ設定」（P.4-3）
- 「Cisco Unified Communications Manager 後続ノードでの IP アドレスの変更」（P.4-4）

イーサネット設定

[IP Settings] ウィンドウには、Dynamic Host Configuration Protocol（DHCP）がアクティブであるかどうかが表示されます。また、関連するイーサネット IP アドレスや、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 にのみ適用されます。Eth1 を対象とした設定はできません。Eth0 の Maximum Transmission Unit（MTU; 最大伝送ユニット）のデフォルトは 1500 です。

IP 設定を表示または変更するには、次の手順に従います。

手順

ステップ 1 [Cisco Unified Communications Operating System Administration] ウィンドウで、[Settings] > [IP] > [Ethernet] の順に移動します。

[Ethernet Settings] 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変更するには、目的のフィールドに新しい値を入力します。[Ethernet Settings] ウィンドウの各フィールドについては、表 4-1 を参照してください。

（注）　DHCP をイネーブルにすると、ポートとゲートウェイの設定がディセーブルになり、変更できなくなります。

ステップ 3　変更を保存するには、[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を変更すると、システムのパフォーマンスに影響が生じる場合があります。詳細については、http://cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html にある『*Changing the IP Address and Host Name for Cisco Unified Communications Manager Release 8.0(2)*』を参照してください。

手順

表 4-1　[Ethernet Configuration] フィールドと説明

フィールド	説明
DHCP	DHCP がイネーブルであるかディセーブルであるかを表します。
Hostname	サーバのホスト名が表示されます。
IP Address	システムの IP アドレスが表示されます。
Subnet Mask	IP サブネット マスク アドレスが表示されます。
Default Gateway	ネットワーク ゲートウェイの IP アドレスが表示されます。

イーサネット IPv6 設定

次の手順に従って、サーバ上の IPv6 をイネーブルおよび設定します。

（注）　イーサネット設定はすべて Eth0 にのみ適用されます。Eth1 を対象とした設定はできません。Eth0 の Maximum Transmission Unit（MTU; 最大伝送ユニット）のデフォルトは 1500 です。

手順

ステップ 1　[Cisco Unified Communications Operating System Administration] ウィンドウで、[Settings] > [IP] > [Ethernet IPv6] の順に移動します。

[Ethernet IPv6 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変更するには、目的のフィールドに新しい値を入力します。[Ethernet IPv6 Configuration] ウィンドウの各フィールドについては、表 4-2 を参照してください。

ステップ 3　変更を保存するには、[Save] をクリックします。

（注）　[Update with Reboot] チェックボックスをオンにすると、[Save] をクリックした後にシステムがリブートされます。IPv6 の設定を有効にするには、システムをリブートする必要があります。

表 4-2　[Ethernet IPv6 Configuration] フィールドと説明

フィールド	説明
Enable IPv6	サーバで IPv6 をイネーブルにするには、このチェックボックスをオンにします。
Address Source	次の IP アドレス ソースから選択します。 • Router Advertisement • DHCP • Manual Entry/Mask 3 つの IP アドレスは相互に独占的です。 （注）　[Manual Entry] を選択した場合を除き、[IP Address] および [Mask] フィールドは変更できません。
IPv6 Address	[Manual Entry] を選択した場合、次の例のようなサーバの IPv6 アドレスを入力します。 fd6:2:6:96:21e:bff:fecc:2e3a
IPv6 Mask	[Manual Entry] を選択した場合、次の例のような IPv6 マスクを入力します。 64
Update with Reboot	[Save] をクリックした直後にシステムをリブートする場合は、このチェックボックスをオンにします。後でリブートする場合は、このチェックボックスをオフにします。 （注）　IPv6 の設定を有効にするには、システムをリブートする必要があります。

パブリッシャ設定

後続ノードまたはサブスクライバ ノードでは、最初のノードまたはノードのパブリッシャの IP アドレスを表示または変更できます。

（注）　クラスタ内のサーバの IP アドレスおよびホスト名を変更する方法の詳細については、http://cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html にある『*Changing the IP Address and Host Name for Cisco Unified Communications Manager Release 8.0(2)*』を参照してください。

パブリッシャの 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 Operating System Administration] ウィンドウで、[Settings] > [IP] > [Publisher] の順に移動します。

[Publisher Settings] ウィンドウが表示されます。

（注）　パブリッシャの IP アドレスは、クラスタの後続ノードでのみ表示および変更が可能で、パブリッシャ自体ではできません。

ステップ 2　新しいパブリッシャ IP アドレスを入力します。

ステップ 3　[Save] をクリックします。

Cisco Unified Communications Manager 後続ノードでの IP アドレスの変更

後続ノードがオフラインのときに、最初の Cisco Unified Communications Manager ノードの IP アドレスを変更すると、後続ノードで Cisco Unified Communications Manager Administration にログインできなくなることがあります。このような状況が発生した場合は、次の手順を実行します。

手順

ステップ 1　次の IP アドレスを使用して、後続ノードからオペレーティング システムの管理に直接ログインします。

http://*server-name*/iptplatform

ここで *server-name* には後続ノードのホスト名または IP アドレスを指定します。

ステップ 2　管理者ユーザ名とパスワードを入力し、[Submit] をクリックします。

ステップ 3　[Settings] > [IP] > [Publisher] の順に移動します。

ステップ 4　パブリッシャの新しい IP アドレスを入力し、[Save] をクリックします。

ステップ 5　後続ノードを再起動します。

NTP サーバ

外部 NTP サーバが Stratum 9 以上（1 ～ 9）であることを確認してください。外部 NTP サーバの追加、削除、または変更を行うには、次の手順に従います。

（注）　最初のノードまたはパブリッシャの NTP サーバ設定のみを設定できます。

手順

ステップ 1　[Cisco Unified Communications Operating System Administration] ウィンドウで、[Settings] > [NTP Servers] の順に移動します。

[NTP Server Settings] ウィンドウが表示されます。

ステップ 2　NTP サーバの追加、削除、または変更ができます。

（注）　互換性、精度、ネットワークのジッタに関する問題が発生しないようにするため、プライマリノードに対して指定する外部 NTP サーバは NTP v4（バージョン 4）である必要があります。IPv6 アドレッシングを使用している場合、外部 NTP サーバは NTP v4 である必要があります。

- NTP サーバを削除するには、当該のサーバの前にあるチェックボックスをオンにしてから [Delete] をクリックします。
- NTP サーバを追加するには、[Add] をクリックし、ホスト名または IP アドレスを入力してから、[Save] をクリックします。
- NTP サーバを変更するには、IP アドレスをクリックし、ホスト名または IP アドレスを変更してから、[Save] をクリックします。

（注）　NTP サーバに対する変更は、完了するまで最大で 5 分かかる場合があります。NTP サーバを変更する場合、ウィンドウを更新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 Server Settings] ウィンドウを更新して正しいステータスを表示するには、[Settings] > [NTP] の順に選択します。

（注）　NTP サーバの削除、変更、または追加が完了した後、変更を反映するには、クラスタ内にある他のすべてのノードを再起動する必要があります。

SMTP 設定

[SMTP Settings] ウィンドウでは、SMTP ホスト名の表示や設定ができ、SMTP ホストがアクティブであるかどうかが表示されます。

ヒント　システムから E メールを送信する場合は、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、次の手順に従います。

手順

ステップ 1　[Cisco Unified Communications Operating System Administration] ウィンドウで、[Settings] > [SMTP] の順に移動します。

[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変更します。

ステップ 3　[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、次の手順に従います。

（注）　サーバ時刻を手動で設定するには、設定済みの NTP サーバをすべて削除する必要があります。詳細については、「NTP サーバ」（P.4-4）を参照してください。

手順

ステップ 1　[Cisco Unified Communications Operating System Administration] ウィンドウで、[Settings] > [Time] の順に移動します。

ステップ 2　システムの日付と時刻を入力します。

ステップ 3　[Save] をクリックします。

ステップ 4　Cisco Unity Connection サーバで、日付を変更した場合、または時刻を 2 分以上変更した場合、CLI コマンド **utils system restart** でサーバを再起動します。

CHAPTER 5

システムの再起動

この項では、次の再起動オプションを使用する手順について説明します。

- 「バージョンの切り替えと再起動」
- 「現在のバージョンの再起動」
- 「システムのシャットダウン」

バージョンの切り替えと再起動

このオプションは、新しいソフトウェアにアップグレードする場合と、以前のソフトウェアのバージョンにフォール バックする場合の両方で使用します。アクティブ ディスク パーティションで実行中のシステムをシャットダウンし、その後非アクティブ パーティションのソフトウェア 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、次の手順に従います。

（注） クラスタをノンセキュアな Cisco Unified Communications Manager の旧リリース（Release 8.0 よりも前）にダウングレードする場合、バージョンを切り替える前にクラスタをロールバックに備えてください。旧リリースにダウングレードする前にクラスタをロールバックに備えないと、システム上の Cisco Unified IP Phone にある ITL ファイルをそれぞれ手動で削除しなければいけません。詳細については、『*Cisco Unified Communications Manager Security Guide*』の「Security by Default」の第 2 章を参照してください。

注意 この手順を実行すると、システムが再起動し、一時的に使用できない状態になります。

手順

ステップ 1 [Cisco Unified Communications Operating System Administration] ウィンドウで、[Settings] > [Version] の順に移動します。

[Version Settings] 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 パーティションと非アクティブ パーティションの両方のソフトウェア バージョンが表示されます。

ステップ 2 バージョンを切り替えて再起動する場合は、[Switch Versions] をクリックします。操作を中止する場合は、[Cancel] をクリックします。

[Switch Version] をクリックするとシステムが再起動し、現在非アクティブである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

現在のパーティションでバージョンを切り替えずにシステムを再起動するには、次の手順に従います。

注意　この手順を実行すると、システムが再起動し、一時的に使用できない状態になります。

手順

ステップ 1　[Cisco Unified Communications Operating System Administration] ウィンドウで、[Settings] > [Version] の順に移動します。

[Version Settings] 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 パーティションと非アクティブ パーティションの両方のソフトウェア バージョンが表示されます。

ステップ 2　システムを再起動する場合は [Restart] をクリックします。操作を中止する場合は [Cancel] をクリックします。

[Restart] をクリックすると、システムはバージョンを切り替えずに現在のパーティションで再起動します。

システムのシャットダウン

注意　サーバをシャットダウンおよびリブートする場合、サーバの電源ボタンを押さないでください。電源ボタンを押すと、誤ってファイル システムを破損し、サーバをリブートできなくなるおそれがあります。

システムをシャットダウンするには、手順 1 または手順 2 に従います。

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 1

ステップ 1　[Cisco Unified Communications Operating System Administration] ウィンドウで、[Settings] > [Version] の順に移動します。

[Version Settings] 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 パーティションと非アクティブ パーティションの両方のソフトウェア バージョンが表示されます。

ステップ 2　システムをシャットダウンする場合は [Shutdown] をクリックします。操作を中止する場合は [Cancel] をクリックします。

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

（注）　ハードウェアが停止するまで数分かかる場合があります。

手順 2（手順 1 の代わり）

ステップ 1　CLI コマンド **utils system shutdown** または **utils system restart** コマンドを実行します。CLI コマンドを実行する手順については、『*Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*』を参照してください。

CHAPTER 6

セキュリティ

この章では証明書の管理と IPSec の管理について説明し、次の作業を実行する手順を説明します。

- 「Internet Explorer のセキュリティ オプションの設定」
- 「証明書と Certificate Trust List の管理」
- 「IPSEC 管理」
- 「Bulk Certificate Management」

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 [Tools] > [Internet Options] を選択します。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 [Advanced] タブの [Security] 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、[Do not save encrypted pages to disk] 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 Certificate Trust List の管理

次の各項では、[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」
- 「証明書のダウンロード」
- 「証明書の削除と再作成」
- 「証明書または Certificate Trust List のアップロード」
- 「サードパーティ製の CA 証明書の使用法」

（注）　[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 システムの管理に再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　[Security] > [Certificate Management] を選択します。

[Certificate List] ウィンドウが表示されます。

ステップ 2　[Find] コントロールを使用すると、証明書の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。

[Certificate Configuration] ウィンドウに該当の証明書の情報が表示されます。

ステップ 4　[Certificate List] ウィンドウに戻るには、[Related Links] リストの [Back To Find/List] を選択し、[Go] をクリックします。

証明書のダウンロード

証明書を Cisco Unified Communications オペレーティング システム から PC に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　[Security] > [Certificate Management] を選択します。

[Certificate List] ウィンドウが表示されます。

ステップ 2　[Find] コントロールを使用すると、証明書のリストをフィルタリングできます。

ステップ 3　証明書のファイル名をクリックします。

[Certificate Configuration] ウィンドウが表示されます。

ステップ 4　[Download] をクリックします。

ステップ 5　[File Download] ダイアログボックスで、[Save] をクリックします。

証明書の削除と再作成

次の各項では、証明書の削除と再作成について説明します。

- 「証明書の削除」
- 「証明書の再作成」

証明書の削除

信頼できる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。[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、「証明書署名要求の作成」（P.6-7）の手順を参照してください。

手順

ステップ 1　[Security] > [Certificate Management] を選択します。

[Certificate List] ウィンドウが表示されます。

ステップ 2　[Find] コントロールを使用すると、証明書の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。

[Certificate Configuration] ウィンドウが表示されます。

ステップ 4　[Delete] をクリックします。

証明書の再作成

証明書を再作成するには、次の手順を実行します。

（注）　証明書の再作成に関する詳細については、『*Cisco Unified Communications Manager Security Guide*』の「Security by Default」の第 3 章を参照してください。

注意　証明書を再作成すると、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　[Security] > [Certificate Management] を選択します。

[Certificate List] ウィンドウが表示されます。

ステップ 2　[Generate New] をクリックします。

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

ステップ 3　[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　[Generate New] をクリックします。

（注）　Cisco Unified Communications オペレーティング システム で証明書を再作成したら、バックアップを実行して、最新のバックアップに再作成した証明書が含まれるようにします。バックアップに再作成した証明書が含まれず、何らかの理由で回復タスクを実行する必要がでた場合は、システム上の電話をそれぞれ手動でロック解除して、Cisco Unified Communications Manager に登録できるようにします。バックアップの実行に関する詳細については、『*Disaster Recovery System Administration Guide*』を参照してください。

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。
TVS	自己署名ルート証明書です。

証明書または Certificate Trust List 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）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 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 Administration Guide*』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」
- 「Certificate Trust List のアップロード」
- 「ディレクトリの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　[Security] > [Certificate Management] を選択します。

[Certificate List] ウィンドウが表示されます。

ステップ 2　[Upload Certificate] をクリックします。

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

ステップ 3　[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 で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、CA ルート証明書の名前を [Root Certificate] テキストボックスに入力します。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ます。

ステップ 5　次のいずれかの手順で、アップロードするファイルを選択します。

- [Upload File] テキストボックスに、ファイルのパスを入力します。
- [Browse] ボタンをクリックしてファイルを選択し、[Open] 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、[Upload File] ボタンをクリックします。

Certificate Trust List のアップロード

手順

ステップ 1　[Security] > [Certificate Management] を選択します。

[Certificate List] ウィンドウが表示されます。

ステップ 2　[Upload Certificate] をクリックします。

[Upload Certificate Trust List] ダイアログボックスが表示されます。

ステップ 3　[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 で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、CA ルート証明書の名前を [Root Certificate] テキストボックスに入力します。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ます。

ステップ 5　次のいずれかの手順で、アップロードするファイルを選択します。

- [Upload File] テキストボックスに、ファイルのパスを入力します。
- [Browse] ボタンをクリックしてファイルを選択し、[Open] 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、[Upload File] ボタンをクリックします。

ディレクトリの信頼証明書のアップロード

手順

ステップ 1　[Security] > [Certificate Management] を選択します。

[Certificate List] ウィンドウが表示されます。

ステップ 2　[Upload Certificate] をクリックします。

[Upload Certificate Trust List] ダイアログボックスが表示されます。

ステップ 3　[Certificate Name] リストから、[directory-trust] を選択します。

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

ステップ 5　ファイルをアップロードするには、[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] を選択します。

ステップ 8　**Cisco Dirsync** サービスを再起動します。

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

ステップ 10　Tomcat サービスを再起動するには、コマンド **utils service restart Cisco Tomcat** と入力します。

ステップ 11　サービスの再起動後、SSL のディレクトリ契約を追加することができます。

サードパーティ製の CA 証明書の使用法

Cisco Unified Communications オペレーティング システム は、サードパーティ製の Certificate Authority（CA; 認証局）が PKCS # 10 Certificate Signing Request（CSR; 証明書署名要求）によって発行した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および参考となる文書を示します。

	作業	参考となる文書
ステップ 1	サーバに CSR を作成する。	「証明書署名要求の作成」（P.6-7）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。	「証明書署名要求のダウンロード」（P.6-7）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、「サードパーティ製の CA 証明書の取得」（P.6-8）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、「サードパーティ製の CA 証明書の取得」（P.6-8）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。	「証明書のアップロード」（P.6-5）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。	「証明書のアップロード」（P.6-5）を参照してください。

	作業	参考となる文書
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 ファイルを作成する。	『*Cisco Unified Communications Manager Security Guide*』を参照してください。
ステップ 8	新しい証明書に影響され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 の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 サービスも再起動します。 **（注）** Tomcat の証明書を更新した場合は、Cisco Unity Connection サービスアビリティで接続 IMAP サーバ サービスも再起動してください。 サービスの再起動の詳細については、『Cisco Unified Communications Manager *Serviceability Administration Guide*』を参照してください。

証明書署名要求の作成

Certificate Signing Request（CSR; 証明書署名要求）を作成するには、次の手順を実行します。

手順

ステップ 1　[Security] > [Certificate Management] を選択します。

[Certificate List] ウィンドウが表示されます。

ステップ 2　[Generate CSR] をクリックします。

[Generate Certificate Signing Request] ダイアログボックスが表示されます。

ステップ 3　[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、[Certificate Name] リストの [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ディレクトリの信頼証明書は、以前のリリースからアップロードできます。

ステップ 4　[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　[Security] > [Certificate Management] を選択します。

[Certificate List] ウィンドウが表示されます。

ステップ 2　[Download CSR] をクリックします。

[Download Certificate Signing Request] ダイアログボックスが表示されます。

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

ステップ 4　[Download CSR] をクリックします。

ステップ 5　[File Download] ダイアログボックスで、[Save] をクリックします。

サードパーティ製の 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、署名付きのアプリケーション証明書と CA ルート証明書の両方を CA から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。入手の手順は、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 が拡張要求メカニズムをサポートしていない場合は、CSR 作成プロセスの最後のページに表示される 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 システムでは、証明書は DER および PEM 符号化フォーマットで、CSR は PEM 符号化フォーマットで作成されます。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。

CAPF 以外の証明書の場合、それぞれのノードについて CA ルート証明書およびアプリケーション証明書を取得およびアップロードしてください。

CAPF の場合、1 つ目のノードについてのみ CA ルート証明書およびアプリケーション証明書を取得およびアップロードしてください。

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 が拡張要求メカニズムをサポートしていない場合は、次の手順に従って X.509 拡張をイネーブルにする必要があります。

- CAPF CSR では、次の拡張情報が使用されます。

```
X509v3 extensions:
X509v3 Key Usage:
Digital Signature, Certificate Sign
X509v3 Extended Key Usage:
TLS Web Server Authentication, IPSec End System
```

- Cisco Unified Communications Manager、Tomcat、および IPSec の CSR では、次の拡張情報を使用します。

```
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System
```

アプリケーション証明書を署名した CA の CA ルート証明書をアップロードします。下位 CA がアプリケーション証明書を署名した場合、ルート CA ではなく、下位 CA の CA ルート証明書をアップロードします。

CA ルート証明書およびアプリケーション証明書をアップロードするには、同じ [Upload Certificate] ダイアログ ボックスを使用します。CA ルート証明書をアップロードする場合、*certificate type*-**trust** 形式の証明書を選択します。アプリケーション証明書をアップロードする場合、証明書タイプのみが含まれる証明書の名前を選択します。たとえば、Tomcat CA ルート証明書をアップロードする場合、[tomcat-trust] を選択し、Tomcat アプリケーション証明書をアップロードする場合、[tomcat] を選択します。

CAPF CA ルート証明書をアップロードすると、CallManager の信頼ストアにコピーされるため、CA ルート証明書を個別に CallManager にアップロードする必要はありません。

証明書の有効期限日の監視

証明書の有効期限日が近づいたときに、システムから自動的に E メールを送信できます。証明書有効期限モニタの表示と設定をするには、次の手順を実行します。

手順

ステップ 1　現在の証明書有効期限モニタの設定を表示するには、[Security] > [Certificate Monitor] を選択します。

[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。[Certificate Monitor Expiration] 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、[Save] をクリックします。

表 6-2　[Certificate Monitor Expiration] フィールドの説明

フィールド	説明
Notification Start Time	証明書が無効になる何日前に通知を送信してもらうかを入力します。
Notification Frequency	通知の頻度を時間または日単位で入力します。
Enable E-mail Notification	E メール通知を有効にするには、このチェックボックスをオンにします。
Email IDs	通知の送信先 E メール アドレスを入力します。 **（注）**　システムから通知を送信するようにするには、SMTP ホストを設定する必要があります。

IPSEC 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 ポリシーと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、IPSec ポリシーに何らかの変更を行ってもその変更は無効になります。アップグレード中は IPSec ポリシーを作成したり変更したりしないでください。

注意　IPSec はシステムのパフォーマンスに影響します（特に暗号化した場合）。

手順

ステップ 1　[Security] > [IPSEC Configuration] を選択します。

[IPSEC Policy List] ウィンドウが表示されます。

ステップ 2　[Add New] をクリックします。

[IPSEC Policy Configuration] ウィンドウが表示されます。

ステップ 3　[IPSEC Policy Configuration] ウィンドウに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、[Save] をクリックします。

表 6-3　[IPSEC Policy and Association] フィールドと説明

フィールド	説明
Policy Group Name	IPSec ポリシー グループの名前を指定します。名前には、文字、数字、ハイフンのみを使用できます。
Policy Name	IPSec ポリシーの名前を指定します。名前には、文字、数字、ハイフンのみを使用できます。
Authentication Method	認証方式を指定します。
Preshared Key	[Authentication Method] フィールドで [Pre-shared Key] を選択した場合は、事前共有キーを指定します。 （注）　事前共有 IPSec キーには、英字およびハイフンのみ使用できます。空白文字またはその他の文字は使用できません。Windows ベース バージョンの Cisco Unified Communications Manager から移行する場合、現行バージョンの Cisco Unified Communications Manager と互換性があるように事前共有 IPSec キーの名前を変更する必要があります。
Peer Type	ピアのタイプが同じか異なるかを指定します。
Certificate Name	[Peer Type] で [Different] を選択した場合、新しい証明書の名前を入力します。
Destination Address	宛先の IP アドレスまたは FQDN を指定します。
Destination Port	宛先のポート番号を指定します。
Source Address	ソースの IP アドレスまたは FQDN を指定します。
Source Port	ソースのポート番号を指定します。
Mode	転送モードを指定します。
Remote Port	宛先で使用されるポート番号を指定します。

表 6-3　[IPSEC Policy and Association] フィールドと説明 （続き）

フィールド	説明
Protocol	次のプロトコルまたは [Any] を指定します。 • TCP • UDP • Any
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
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 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
Phase One Life Time	フェーズ 1 の 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。
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。2、1 および 5 から選択できます。
Phase Two Life Time	フェーズ 2 の 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。
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。2、1 および 5 から選択できます。
Enable Policy	ポリシーを有効にするには、このチェックボックスをオンにします。

既存の IPSec ポリシーの管理

既存の IPSec ポリシーを表示、イネーブル/ディセーブル、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、IPSec ポリシーに何らかの変更を行ってもその変更は無効になります。アップグレード中は IPSec ポリシーを作成したり変更したりしないでください。

注意　IPSec はシステムのパフォーマンスに影響します（特に暗号化した場合）。

注意　既存の IPSec ポリシーを変更すると、システムの正常な動作に影響する場合があります。

手順

ステップ 1　[Security] > [IPSEC Configuration] を選択します。

（注）　[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 システムの管理に再ログインする必要があります。

[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、イネーブル、またはディセーブルにするには、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 Policy Configuration] ウィンドウが表示されます。

b. ポリシーをイネーブルまたはディセーブルにするには、[Enable Policy] チェックボックスを使用します。

c. [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横にあるチェックボックスをオンにします。

[Select All] をクリックするとすべてのポリシーを選択でき、[Clear All] を選択するとすべてのチェックボックスをクリアできます。

b. [Delete Selected] をクリックします。

Bulk Certificate Management

Extension Mobility Cross Cluster（EMCC）機能をサポートするため、クラスタ管理者によって構成された共通 SFTP サーバ間で一括インポートおよびエクスポートを実行できます。

（注）　Cisco Unified IP Phone 8961、9951、または 9971 の ファームウェア リリースが 9.0(2) で、クラスタが混合モードで実行されている場合、EMCC 機能が動作するためには、クラスタすべての CTL が共通した一連のセキュリティ トークンで署名される必要があります。すべてのクラスタで共通のトークンが 1 つ以上必要です。

証明書のエクスポート

[Bulk Certificate Management] を使用して証明書をエクスポートするには、次の手順を実行します。

手順

ステップ 1　[Security] > [Bulk Certificate Management] を選択します。

[Bulk Certificate Management] ウィンドウが表示されます。

ステップ 2　[Bulk Certificate Management] ウィンドウに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 6-4 を参照してください。

ステップ 3　入力した値を保存するには、[Save] をクリックします。

ステップ 4　証明書をエクスポートするには、[Export] をクリックします。

[Bulk Certificate Export] ポップアップ ウィンドウが表示されます。

ステップ 5　ドロップダウン メニューからエクスポートする証明書のタイプを選択します。

- Tomcat
- TFTP
- All

ステップ 6　[Export] をクリックします。

システムによって選択した証明書が中央 SFTP サーバにエクスポートおよび保存されます。

証明書のインポート

[Bulk Certificate Management] ウィンドウを使用して、他のクラスタからエクスポートした証明書をインポートすることもできます。ただし、[Import] ボタンが表示されるには、次の操作を完了する必要があります。

- クラスタ 2 つ以上から SFTP サーバに証明書をエクスポートします。
- エクスポートした証明書を統合します。

表 6-4　[Bulk Certificate Management] フィールドの説明

フィールド	説明
IP Address	証明書のエクスポート先となる共通サーバの IP アドレスを入力します。
Port	ポート番号を入力します。 デフォルト：22
User ID	サーバのログインに使用するユーザ ID を入力します。
Password	適切なパスワードを入力します。
Directory	証明書の保存先となるサーバのディレクトリを入力します。 例： /users/cisco

CHAPTER 7

ソフトウェア アップグレード

[Software Upgrades] オプションを使用すると、次のようなインストールとアップグレードを実行できます。

- [Install/Upgrade]：アプリケーション ソフトウェアのアップグレード、Cisco Unified Communications Manager ロケール インストーラとダイヤル プランのインストール、および、デバイス パック、電話機のファームウェア ロード、およびその他の COP ファイルのアップロードとインストールをする場合に、このオプションを使用します。
- [TFTP File Management]：電話機が使用するさまざまなデバイス ファイルを TFTP サーバにアップロードする場合に、このオプションを使用します。アップロード可能な TFTP サーバ ファイルには、カスタム呼出音、コールバック トーン、および電話機の背景画像などがあります。

この章の内容は、次のとおりです。

- 「アップグレード前の作業」（P.7-1）
- 「ソフトウェア アップグレードの考慮事項」（P.7-3）
- 「ソフトウェア アップグレード手順」（P.7-13）
- 「アップグレード後の作業」（P.7-17）
- 「アップグレードの途中停止」（P.7-18）
- 「以前のバージョンへの復帰」（P.7-18）
- 「COP ファイル、ダイヤル プラン、およびロケールのインストール」（P.7-20）
- 「TFTP サーバ ファイルの管理」（P.7-24）
- 「カスタム ログオン メッセージの設定」（P.7-25）

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 Unified Communications Manager のリリース ノートは、次の URL にあります。

  http://cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html
- 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。

Cisco Unified Communications Manager 5.x からアップグレードする場合は、ソフトウェア機能ライセンスを取得してください。ソフトウェア機能ライセンスによって、指定したライセンス バージョンの機能がシステムでアクティブになります。Cisco Unified Communications Manager 6.(x) 以降で 5.0 デバイス ライセンスを使用するには、必ずシステムで実行されている Cisco Unified Communications Manager バージョンのソフトウェア機能ライセンスを取得してください。

ライセンスの取得およびインストール方法に関する詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「License File Upload」の章を参照してください。

- 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。
- [Cisco Unified Serviceability] > [Tools] > [Service Activation] を選択して、Cisco Extension Mobility サービスをディセーブルにします。詳細については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

（注） Cisco Extension Mobility サービスをディセーブルにした場合、Cisco Extension Mobility のユーザは、Cisco Extension Mobility をサポートする電話機でログインおよびログアウトできなくなることに注意してください。

- 大量のデバイスを含む大規模な Class A または Class B サブネットに Cisco Unified Communications Manager をインストールしないでください。Cisco Unified Communications Manager を大量のデバイスがある大規模なサブネットにインストールすると、Address Resolution Protocol（ARP; アドレス解決プロトコル）テーブルが短期間でいっぱいになる可能性があります（デフォルトでは最大 1024 エントリ）。ARP テーブルがフルになると、Cisco Unified Communications Manager はエンドポイントとの通信が困難になり、電話を追加できなくなります。

注意 Cisco Extension Mobility サービスをディセーブルにしないと、アップグレードに失敗する可能性があります。

- 新しいリリースにアップグレードする前に、現在インストールされている COP ファイルのマニュアルを参照して、Cisco Unified Communications Manager のアップグレードに関連する考慮事項がないかを確認してください。

（注） Nokia s60 COP ファイルがインストールされている場合、このファイルの新しいバージョンをインストールしてから Cisco Unified Communications Manager をアップグレードしてください。

- Cisco Unified Communications Manager Release 8.0(2) で IPv6 を使用する場合は、Release 8.0(2) にアップグレードする前に DNS サーバを IPv6 にプロビジョニングできます。ただし、Release 8.0(2) をアップグレードしてから、IPv6 の Cisco Unified Communications Manager DNS レコードを設定してください。

注意 Release 8.0(2) をアップグレードする前に、IPv6 の Cisco Unified Communications Manager DNS レコードを設定すると、アップグレードに失敗します。

- Cisco Unified Communications Manager をアップグレードする前に、Cisco Unified Mobile Communicator デバイス名が 15 文字以下であることを確認してください。Cisco Unified Mobile Communicator のデバイス名が 15 文字より多い場合、アップグレード時にデバイスが移行されません。
- アップグレード前の作業を実行したら、「ソフトウェア アップグレードの考慮事項」（P.7-3）を参照してください。

ソフトウェア アップグレードの考慮事項

この項は、次の内容で構成されています。

- 「ソフトウェア アップグレード手順の概要」（P.7-3）
- 「アップグレード時の設定の変更」（P.7-4）
- 「クラスタの並行アップグレード」（P.7-6）
- 「サポートされるアップグレード」（P.7-7）
- 「Cisco Unified Communications Manager Release 6.0(1) よりも前のリリースから Release 6.0(1) 以降へのアップグレード」（P.7-7）
- 「Cisco Unified Communications Manager Release 6.0(1) よりも前のリリースから Release 7.0(1) 以降へのアップグレード」（P.7-8）
- 「Cisco Unified Communications ManagerRelease 5.1(3e) から 7.1.x Release へのアップグレード」（P.7-8）
- 「5.x リリースからのアップグレードにおけるパーティションのサイズ制限」（P.7-9）
- 「アップグレード ファイルの取得」（P.7-9）
- 「サポートされる SFTP サーバ」（P.7-10）
- 「I/O スロットリングの影響」（P.7-11）

ソフトウェア アップグレード手順の概要

このバージョンの Cisco Unified Communications Manager では、では、コンピュータの運用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することができます。システムには、2 つのパーティションがあります。1 つはアクティブな、もう 1 つはアクティブでない、ブート可能パーティションです。システムのブートと動作はすべてアクティブ パーティションとしてマークされているパーティションで実行されます。

（注）　Cisco Extension Mobility にログイン中またはログアウト中のユーザがいる場合は、アップグレードに失敗することがあります。アップグレードを開始する前に、Cisco Extension Mobility サービスを無効にする必要があります。詳細については、「アップグレード前の作業」（P.7-1）を参照してください。

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、アクティブでない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通常通り動作します。準備ができたら、非アクティブ パーティションをアクティブにして、アップグレードしたソフトウェアでシステムをリブートします。現在アクティブなパーティションは、システムの再起動後に非アクティブ パーティションとして認識されます。現在のソフトウェアは、次のアップグレードまで非アクティブ パーティションにそのまま残ります。設定情報は自動的にアクティブ パーティションにあるアップグレード バージョンに移行されます。

クラスタをアップグレードする場合、最初のノードからアップグレードを開始します。「クラスタの並行アップグレード」（P.7-6）で説明しているとおり、最初のノードがアップグレードの指定した段階に達すると、後続ノードのアップグレードを並行して開始できます。

クラスタ内のすべてのサーバで、同一リリースの Cisco Unified Communications Manager 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から元の状態に戻す場合、ソフトウェアの以前のバージョンがある非アクティブ パーティションでシステムを再起動できます。しかし、ソフトウェアのアップグレード後に行った設定の変更はすべて失われます。

（注）　データベースへの変更は、アクティブなパーティションに対してのみ実行できます。アクティブでないパーティション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、パーティションを切り替えてから同じ変更を繰り返す必要があります。

アップグレード サイクル中に最初のノードをアップグレードして、新しいバージョンに切り替えた後に後続ノードのアップグレードが失敗した場合、またはクラスタ内のいずれかの後続ノードのアップグレードが失敗した場合、次の手順を実行できます。

- 後続ノードで、アップグレードの失敗の原因になったエラーを修正できます。クラスタ内のノードのネットワーク接続を確認し、後続ノードを再起動してから、後続ノードのサーバ メモリおよび CPU 使用率が高すぎないかを確認してください。後続ノードを再度アップグレードします。
- アクティブなパーティションの最初のノードで、サーバにインストールされた最新バージョンのソフトウェアが実行できることを確認してください。アクティブなパーティションの最初のノードで実行されているのと同じソフトウェア バージョンで後続ノードのフレッシュ インストールを実行します。後続ノードを再インストールする場合は、Cisco Unified CM の管理からサーバを削除して、『Cisco Unified Communications Manager Administration Guide』の手順に従ってサーバを再度追加します。
- 「以前のバージョンへの復帰」（P.7-18）に従い、最初のノードおよび後続ノードすべてを前のバージョンに戻し、後続ノードに前のバージョンをインストールします。次に、最初のノードを新しいバージョンに再度アップグレードして（戻すのではない）、後続ノードを新しいバージョンにアップグレードします。最初のノードを、新しいバージョンに再度アップグレードするのではなく前のバージョンに戻すと、データベースが同期されず、同期を修復できません。

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）または Cisco Unified Communications Manager 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。

Cisco Unified Communications Manager のインストール直後または他の製品バージョンへの切り替え直後の短時間、電話機ユーザによって実行された設定の変更が適用されない場合があります。電話機ユーザ設定の例には、コール転送やメッセージ待機インジケータのライト設定などがあります。これは、インストール後またはアップグレード後に Cisco Unified Communications Manager データベースが同期され、電話機ユーザによる設定の変更が上書きされる場合があるためです。

（注）　ソフトウェアのアップグレード プロセスを開始する前にシステム 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 Administration Guide*』を参照してください。

アップグレード時の設定の変更

ここでは、アップグレード時に適用される設定およびプロビジョニングの変更に関する制限について説明します。

管理の変更

管理者はアップグレード中に Cisco Unified Communications Manager の設定を変更しないでください。設定の変更には、Cisco Unified Communications Manager Administration、Cisco Unified Serviceability、および [User Option] ウィンドウで実行するすべての変更が含まれます。

アップグレード時の設定の変更はアップグレード完了後に失われる可能性があり、一部の設定によりアップグレードが失敗する可能性があります。

Cisco Unified Communications Manager Release 8.0(2) では、この制限はリリース 4.x、5.x、および 6.x に適用されます。

Cisco Unified Communications Manager Release 5.x および 6.x からのアップグレードでは、Cisco Unified Communications オペレーティング システムの管理またはコマンド ライン インターフェイスのいずれかを使用して新しいリリースにアップグレードする前に、すべての設定操作を中断する必要があります。

システムをアップグレードする場合は、この項のアップグレード タスクを実行してから、設定タスクを実行してください。

注意　これらの推奨事項を実行しないと、予期せぬ動作が発生する可能性があります（ポートが予期される通りに初期化されないなど）。

アップグレード作業

アップグレード タスクを正常に完了するには、アップグレード作業を次の順番とおりに実行してから設定を変更してください。

（注）　アップグレードがクラスタ内すべてのサーバで完了し、サーバをアップグレードされたパーティションに切り替えて、データベースの複製が機能していることを確認するまで設定作業を実行しないことを推奨します。

手順

ステップ 1　設定作業をすべて停止します。つまり、さまざまな Cisco Unified Communications Manager 関連 GUI または CLI（Cisco Unified Communications オペレーティング システム GUI でのアップグレードを除く）での設定作業を実行しないでください。

ステップ 2　クラスタ内の最初のノード（パブリッシャ ノード）をアップグレードします。

ステップ 3　クラスタ内の後続ノード（サブスクライバ ノード）をアップグレードます。

ステップ 4　最初のノードをアップグレードされたパーティションに切り替えます。

ステップ 5　後続ノードをアップグレードされたパーティションに切り替えます。

（注）　後続ノードは、サイト要件に応じてアップグレードされたパーティションにすべて同時に切り替えることも、1 つづつ切り替えることもできます。

ステップ 6　最初のノードと後続ノード間でデータベースの複製が機能していることを確認してください。データベースの複製ステータスは次のいずれかの方法で確認できます。

- Cisco Unified Reporting で、Unified CM データベース ステータス レポートにアクセスします。続行する前に、必ずレポートにエラーがなくデータベースの複製ステータスが良好であることを確認します。Cisco Unified Reporting の使用に関する詳細については、『*Cisco Unified Reporting Administration Guide*』を参照してください。
- Cisco Real Time Monitoring Tool で、[CallManager] タブの Database Summary サービスにアクセスして、データベースの複製ステータスを監視します。次に、データベースの複製ステータスに関する進行状況を示します。

- 0：初期化中。
- 1：複製セットアップ スクリプトがこのノードから送信されます。
- 2：複製が良好。
- 3：複製が不調。
- 4：複製の設定に失敗。

続行する前に、必ずデータベースの複製ステータスが良好であることを確認します。Real Time Monitoring Tool の使用に関する詳細については、『*Cisco Unified Real Time Monitoring Tool Administration Guide*』を参照してください。

ステップ 7　その他すべてのアップグレード作業が完了したら、必要に応じて設定作業を実行できます。

ユーザ プロビジョニング

Cisco Unified Communications Manager Release 4.x および 5.x からのアップグレードでは、アップグレード開始後にエンド ユーザがユーザ方向機能に対して行ったプロビジョニングが失われる可能性があります。

Cisco Unified Communications Manager Release 6.x からのアップグレードでは、ユーザ方向機能に対して行った変更はアップグレード完了後に保存されます。

- Call Forward All（CFA; 全コール転送）
- Message Waiting Indication（MWI; メッセージ待機表示）
- プライバシーの有効 / 無効
- Do Not Disturb（DND）の有効 / 無効
- Extension Mobility（EM; エクステンション モビリティ）のログイン
- ハント グループのログアウト
- デバイス モビリティ
- エンド ユーザおよびアプリケーション ユーザの CTI CAPF ステータス
- クレデンシャルのハッキングと認証
- レコーディングの有効化
- シングル ナンバー リーチの有効化

クラスタの並行アップグレード

Cisco Unified Communications Manager 5.x または 6.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 Cisco Unified Communications Manager 8.0(2) にアップグレードするには、最初のノードをアップグレードします。最初のノードがアップグレードの指定した段階に達すると、後続ノードのアップグレードを並行して開始できます。

最初のノードのアップグレード中に、Cisco Unified Communications オペレーティング システムの管理の [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（install_log_<date+time>.log）を表示してください。ログに次の情報が表示されていれば、後続のノードのアップグレードを開始できます。

PRODUCT_TARGET が製品ターゲット ID。

PRODUCT_NAME が製品名。

PRODUCT_VERSION が、アップグレード後の製品バージョン（8.0(2) など）。

また、CLI を使用して次の手順に従うと、インストール ログの関連情報を検索できます。

手順

ステップ 1　インストール ログを一覧表示します。次に例を示します。

```
file list install install_* date

install_log_2008-10-01.09.41.57.log     install_log_2008-10-08.12.59.29.log
install_log_2008-10-14.09.31.06.log
dir count = 0, file count = 3
```

ステップ 2　ストリング PRODUCT_VERSION の最新インストール ログを検索します。次に例を示します。

```
file search install install_log_2008-10-14.09.31.06.log PRODUCT_VERSION

Searching path: /var/log/install/install_log_2008-10-14.09.31.06.log
Searching file: /var/log/install/install_log_2008-10-14.09.31.06.log
08/10/14 09:52:14 upgrade_os.sh|PRODUCT_VERSION is 7.1.0.39000-97|<LVL::Info>

Search completed
```

ステップ 3　**file search** コマンドによってインストール ログで PRODUCT_VERSION ストリングが検索されたら、後続ノードのアップグレードを開始できます。

注意　最初のノードと並行して後続ノードをアップグレードする場合は、最初のノードおよび後続ノードのいずれでも、アップグレード オプションの設定時にアップグレードされたパーティションで [Reboot] を選択しないでください。これを選択すると、後続ノードのアップグレード中に最初のノードのアップグレードが完了して、再起動される可能性があります。この場合、後続ノードのアップグレードに失敗します。

新しいバージョンをアクティブにする準備が整ったら、その他のノードで新しいソフトウェアをアクティブにする前に、最初のノードの新しいソフトウェアをアクティブにしてください。

サポートされるアップグレード

サポートされるアップグレードについては、製品リリースのリリース ノートおよび次の URL にある Cisco Unified Communications Manager の互換性マトリクスを参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html

Cisco Unified Communications Manager Release 6.0(1) よりも前のリリースから Release 6.0(1) 以降へのアップグレード

Cisco Unified Communications Manager Release 6.0(1) 以降、CAPF では証明書とキーの管理に Certificate Manager Infrastructure が使用されています。このため、Release 6.0(1) よりも前のリリースから Release 6.0(1) 以降にアップグレードすると、CAPF のキーと証明書は自動的に再作成されます。

その後 CTL Client アプリケーションを再実行し、CTL ファイルをアップグレードする必要があります。Cisco Unified Communications Manager での CAPF の使用方法については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

Cisco Unified Communications Manager を新しいリリースにアップグレードする前に、まずリリースのライセンスを取得する必要があります。アップグレード後に新しいライセンスをインポートしてからシステムを有効にする必要があります。ライセンスおよびライセンス取得の詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

Cisco Unified Communications Manager Release 6.0(1) よりも前のリリースから Release 7.0(1) 以降へのアップグレード

Cisco Unified Communications Manager を Release 6.0(1) よりも前のリリースから Release 7.0(1) 以降にアップグレードする場合、サーバ上に /spare パーティションが作成されません。Release 6.0(1) 以降から Release 7.0(1) 以降にアップグレードする場合、または Release 7.0(1) 以降のフレッシュ インストールを実行する場合は、/spare パーティションが作成されます。

/spare は、サーバの CTI Monitor トレースの効率を向上させるパーティションです。

Cisco Unified Communications ManagerRelease 5.1(3e) から 7.1.x Release へのアップグレード

この情報は、次のリリースから 7.1.x リリースにアップグレードする場合に適用されます。

- 5.1(3e) (5.1.3.6000-2)
- 次の 5.1(3e) Engineering Special リリース
  - 5.1(3.6103-1)
  - 5.1(3.6102-1)
  - 5.1(3.6101-1)

アップグレードする前に、COP ファイル ciscocm.513e_upgrade.cop.sgn をサーバにインストールしてください。この COP ファイルは次の URL から入手できます。

http://tools.cisco.com/support/downloads/go/ImageList.x?relVer=COP-Files&mdfid=280735907&sftType=Unified+Communications+Manager%2FCallManager+Utilities&optPlat=&nodecount=2&edesignator=null&modelName=Cisco+Unified+Communications+Manager+Version+5.1&treeMdfId=278875240&treeName=Voice+and+Unified+Communications&modifmdfid=&imname=&hybrid=Y&imst=N&lr=Y

この COP ファイルをインストールする手順については、COP ファイルに含まれている手順に従ってください。

（注） 互換性のある Cisco Unified Communications Manager 5.1 バージョン（http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html にある互換性マトリクスを参照）から DVD を使用して以降の Cisco Unified Communications Manager リリースにアップグレードする場合、[Software Installation/Upgrade] ウィンドウで、「To ensure the integrity of the installation file, verify the MD5 hash value against the Cisco Systems website.」というチェックサム手順の指示を無視して [Next] をクリックします。

5.x リリースからのアップグレードにおけるパーティションのサイズ制限

Cisco Unified Communications Manager 5.x リリースでは固定サイズのディスク パーティションが作成されます。固定パーティションの要件以上の空きディスク容量があるサーバに 5.x リリースをインストーすると、固定サイズのパーティションが作成されます。

このようなサーバを 5.x リリースからアップグレードすると、ディスク パーティションのサイズは固定されたままになります。フレッシュ インストールを実行すると、ディスク パーティションはディスク空き容量の比率に基づいて作成されるので、サーバのディスク空き容量がすべて効率的に使用されます。

サポートされるアプライアンス リリースから Cisco Unified Communications Manager にアップグレードする前に、アップグレードを実行するのに十分なディスク空き容量が共通パーティションにあることを確認してください。十分なディスク空き容量を確保するため、DVD または Cisco.com の ISO ファイルのサイズを確認します。ローカル ソース（DVD）からアップグレードする場合は、ISO ファイルと同じディスク空き容量が必要です。ネットワーク ソースからアップグレードする場合は、ISO ファイルを組み合わせたサイズの 2 倍のディスク空き容量が必要です。

共通パーティションのディスク空き容量を確認するには、次のいずれかの手順を実行します。

- **show status** CLI コマンドを使用して、Disk/logging 見出しの下に表示される情報を記録します。
- Cisco Unified Communications オペレーティング システム で [Show] > [System] を選択します。
- Real Time Monitoring Tool で [System] > [Server] > [Disk Usage] を選択します。[Disk Usage] の [Host] ドロップダウン リスト ボックスからサーバを選択して、共通パーティションの [Used Space (MB)] を表示します。

十分なディスク空き容量がない場合は、Real Time Monitoring Tool を使用して、コア ファイルおよびトレース ファイルを収集し、サーバから削除します。ファイルの収集に関する詳細については、『*Cisco Unified Real Time Monitoring Tool Administration Guide*』を参照してください。

また、ログ パーティション モニタリング サービスあるいは Command Line Interface（CLI; コマンド ライン インターフェイス）を使用して、サーバのファイルを削除できます。ただし、システム パフォーマンスに影響を与える可能性があるため、通常の業務時間内にこれらのツールを使用することは推奨しません。ログ パーティション モニタリングの設定に関する詳細については、『*Cisco Unified Real Time Monitoring Tool Administration Guide*』を参照してください。CLI に関する詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。

（注）　今後、大量のトレース ファイルが原因で発生するディスク使用率の問題を防止するには、Cisco Unified Serviceability でトレースの設定を確認してください（[Trace] > [Configuration]）。サービスの最大トレース ファイル数を減らすか、トレース設定をデフォルト値に設定できます。

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。メジャー アップグレード、つまりリリース トレイン間のアップグレード（6.01(1) から 7.0(1) へのアップグレードなど）を実行する場合、Product Upgrade Tool（PUT）を使用して DVD を取得するか、代理店からアップグレードを購入してください。

PUT を使用するには、https://tools.cisco.com/gct/Upgrade/jsp/index.jsp にアクセスします。シスコ契約番号（Smartnet、SASU または ESW）を入力して、DVD/DVD セットを請求してください。Cisco Unified Communications Manager の契約がない場合は、代理店からアップグレードを購入してください。

マイナー アップグレード、つまりリリース トレイン内のアップグレード（7.0(1) から 7.1(2) へのアップグレードなど）を実行する場合、Cisco.com からもアップグレード ファイルを入手できます。

サポートされる Cisco Unified Communications Manager 5.1(x) リリースからのアップグレード

Cisco Unified Communications Manager Release 5.1(3) からのアップグレードの場合、アップグレードには、パッチ セットと呼ばれる一連のファイルが必要です。このファイルはシスコが提供する DVD のディレクトリ cisco-ipt-k9-patchX.X.X.X-X にあります。X.X.X.X-X はリリースおよびビルド番号を示します。

（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、インストールする前にこの中のディレクトリ名またはファイル名は変更しないでください。

Cisco Unified Communications Manager 6.x および 7.x からのアップグレード

Cisco Unified Communications Manager Release 6.x または 7.x からのアップグレードの場合、アップグレード ファイル名は次の形式になります。

```
UCSInstall_UCOS_X.X.X.X.X.sgn.iso
```

X.X.X.X-X は、リリースとビルド番号を表します。

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。

サポートされる SFTP サーバ

シスコでは任意の SFTP サーバ製品を使用できますが、Cisco Technology Developer Partner Program（CTDP）を介してシスコが認定する SFTP 製品を使用することをお勧めします。GlobalSCAPE などの CTDP パートナーは、Cisco Unified Communications Manager の特定のバージョンについて同社の製品を認定しています。お使いの Cisco Unified Communications Manager バージョンを認定したベンダーに関する情報については、次の URL を参照してください。

http://www.cisco.com/pcgi-bin/ctdp/Search.pl

GlobalSCAPE をサポートされる Cisco Unified Communications バージョンで使用する方法については、次の URL を参照してください。

http://www.globalscape.com/gsftps/cisco.aspx

シスコでは社内テストに次のサーバを使用しています。いずれかのサーバを使用できますが、サポートについては各ベンダーにお問い合わせください。

- Open SSH（http://sshwindows.sourceforge.net/ を参照）
- Cygwin（ http://www.cygwin.com/ を参照）
- Titan（http://www.titanftp.com/ を参照）

シスコでは、SFTP 製品、freeFTPD の使用はサポートしません。この SFTP 製品では、ファイル サイズが 1GB に制限されているためです。

（注）　CTDP プロセスによって認定されていないサードパーティ製品に関する問題については、各サードパーティ ベンダーにお問い合わせください。

I/O スロットリングの影響

この項では、スロットリングがアップグレード プロセスに影響を与え、アップグレード速度の低下または停止の考えられる原因の特定とアップグレード速度を向上できる操作について説明します。

ここでは、次の情報について説明します。

- 「概要」（P.7-11）
- 「サーバ モデル」（P.7-11）
- 「書き込みキャッシュ」（P.7-11）

概要

スロットリングにより、コール処理の低下を防止できますが、アップグレードにかかる時間が長くなる可能性があります。スロットリングはデフォルトでイネーブルです。また、通常の業務時間中にアップグレードを実行する場合不可欠です。アップグレード中にシステムのコール処理の負荷が高いほど、アップグレード タスクにかかる時間が長くなるので注意してください。

サーバ モデル

使用するサーバ モデルはアップグレード速度に影響を及ぼします。SATA ハード ドライブを搭載したサーバ（MCS-7816、MCS-7825、MCS-7828）は、SAS/SCSI ハード ドライブを搭載したサーバ（MCS-7835 および MCS-7845）よりアップグレードに時間がかかります。

書き込みキャッシュ

サーバの書き込みキャッシュがディセーブルの場合、アップグレード プロセスの実行速度が遅くなります。旧式サーバのバッテリ切れなど、書き込みキャッシュがディセーブルになる要因はいくつか考えられます。

アップグレードを開始する前に、MCS-7828-H4 および MCS-7835/45 ディスク コントローラの書き込みキャッシュのステータスを確認してください。MCS-7816、MCS-7825、またはその他の MCS-7828 サーバでは書き込みキャッシュのステータスを確認する必要はありません。書き込みキャッシュのステータスを確認するには、Cisco Unified オペレーティング システムの管理にアクセスして [Show] > [Hardware] を選択します。

バッテリ切れにより、書き込みキャッシュがディセーブルになったと判断した場合、ハード ディスク コントローラのキャッシュ バッテリを交換してください。バッテリの交換を実行するには、ローカル サポートの手順に従ってください。

次に示す [Show] > [Hardware] メニューの出力例を参照して、バッテリおよびライトバック キャッシュのステータスを確認する詳細を確認してください。

次の例では書き込みキャッシュがイネーブルであることを示しています。この例では、キャッシュの 50 %が書き込みに予約されており、キャッシュの 50 %が読み取りに予約されています。書き込みキャッシュがディセーブルの場合、キャッシュの 100 %が読み込みに予約されているか、Cache Status が「OK」ではありません。また、バッテリ カウントが「1」になっています。コントローラのバッテリが切れている、またはない場合は「0」と示されます。

例 7-1　　書き込みキャッシュがイネーブルの 7835/45-H1、7835/45-H2、7828-H4 サーバ

```
--------------------------------
RAID Details      :
```

```
Smart Array 6i in Slot 0
   Bus Interface: PCI
   Slot: 0
   Cache Serial Number: P75B20C9SR642P
   RAID 6 (ADG) Status: Disabled
   Controller Status: OK
   Chassis Slot:
   Hardware Revision: Rev B
   Firmware Version: 2.80
   Rebuild Priority: Low
   Expand Priority: Low
   Surface Scan Delay: 15 sec
   Cache Board Present: True
   Cache Status: OK
   Accelerator Ratio: 50% Read / 50% Write
   Total Cache Size: 192 MB
   Battery Pack Count: 1
   Battery Status: OK
   SATA NCQ Supported: False
```

次の例では、バッテリ ステータスがイネーブルで、書き込みキャッシュ モードが（ライトバック）モードでイネーブルになっています。

例 7-2　　書き込みキャッシュがイネーブルの 7835/45-I2 サーバ

```
----------
RAID Details      :
Controllers found: 1

------------------------------------------------------------------------
Controller information
------------------------------------------------------------------------
   Controller Status                    : Okay
   Channel description                  : SAS/SATA
   Controller Model                     : IBM ServeRAID 8k
   Controller Serial Number             : 20ee0001
   Physical Slot                        : 0
   Copyback                             : Disabled
   Data scrubbing                       : Enabled
   Defunct disk drive count             : 0
   Logical drives/Offline/Critical      : 2/0/0
   ---------------------------------------------------
   Controller Version Information
   ---------------------------------------------------
   BIOS                                 : 5.2-0 (15421)
   Firmware                             : 5.2-0 (15421)
   Driver                               : 1.1-5 (2412)
   Boot Flash                           : 5.1-0 (15421)
   ---------------------------------------------------
   Controller Battery Information
   ---------------------------------------------------
   Status                               : Okay
   Over temperature                     : No
   Capacity remaining                   : 100 percent
   Time remaining (at current draw)     : 4 days, 18 hours, 40 minutes
   ---------------------------------------------------
   Controller Vital Product Data
   ---------------------------------------------------
   VPD Assigned#                        : 25R8075
   EC Version#                          : J85096
   Controller FRU#                      : 25R8076
   Battery FRU#                         : 25R8088
```

```
---------------------------------------------------------------------
Logical drive information
---------------------------------------------------------------------
Logical drive number 1
   Logical drive name                  : Logical Drive 1
   RAID level                          : 1
   Status of logical drive             : Okay
   Size                                : 69900 MB
   Read-cache mode                     : Enabled
   Write-cache mode                    : Enabled (write-back)
   Write-cache setting                 : Enabled (write-back) when protected by battery
   Number of chunks                    : 2
   Drive(s) (Channel,Device)           : 0,0 0,1
Logical drive number 2
   Logical drive name                  : Logical Drive 2
   RAID level                          : 1
   Status of logical drive             : Okay
   Size                                : 69900 MB
   Read-cache mode                     : Enabled
   Write-cache mode                    : Enabled (write-back)
   Write-cache setting                 : Enabled (write-back) when protected by battery
   Number of chunks                    : 2
   Drive(s) (Channel,Device)           : 0,2 0,3
```

ソフトウェア アップグレード手順

この項では、ローカルまたはリモート ソースからのアップグレード手順について説明します。この項は、次の内容で構成されています。

- 「ローカル ソースからのアップグレード」（P.7-13）
- 「リモート ソースからのアップグレード」（P.7-14）
- 「ブリッジ アップグレード」（P.7-16）

ローカル ソースからのアップグレード

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　シスコから提供されるアップグレード ディスクが手元にない場合は、ISO イメージ形式でダウンロードしたアップグレード ファイルを DVD に書き込んで、アップグレード ディスクを作成します。

（注）　DVD に .iso ファイルをコピーしただけでは、正しく動作しません。商用ディスク書き込みアプリケーションの多くで、ISO イメージ ディスクを作成できます。

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

ステップ 3　Cisco Unified Communications オペレーティング システム 管理ページにログインします。

ステップ 4　[Software Upgrades] > [Install/Upgrade] に移動します。

[Software Installation/Upgrade] ウィンドウが表示されます。

ステップ 5　[Source] リストから [DVD] を選択します。

ステップ 6　[Directory] フィールドにスラッシュ（/）を入力します。

ステップ 7　[Next] をクリックしてアップグレード プロセスを続行します。

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て、[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行状況を監視します。

ステップ 10　アップグレードをインストールして、アップグレードされたパーティションに自動的に再起動する場合は、[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起動されます。

ステップ 11　アップグレードをインストールして、後でアップグレードされたパーティションに手動で再起動する場合は、次のいずれかの手順を実行します。

a. [Do not reboot after upgrade] を選択します。

b. [Next] をクリックします。

[Upgrade Status] 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ら、[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、[Settings] > [Version] を選択して、[Switch Version] をクリックします。

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起動されます。

リモート ソースからのアップグレード

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がアクセスできる FTP または SFTP サーバにアップグレード ファイルを置きます。

サポートされる Release 5.1(x) からアップグレードする場合は、パッチ セットと呼ばれる一連のファイルが必要です。次のいずれかの方法を使用して、パッチ セットのファイルを FTP サーバまたは SFTP サーバに配置してください。

a. シスコから提供されたアップグレード ディスクが手元にある場合は、ディスクの内容をリモート サーバにコピーします。

b. アップグレード ファイルをダウンロードした場合は、ダウンロードしたファイルをリモート サーバにコピーします。

ステップ 2　Cisco Unified Communications オペレーティング システム 管理ページにログインします。

ステップ 3　[Software Upgrades] > [Install/Upgrade] に移動します。

[Software Installation/Upgrade] ウィンドウが表示されます。

ステップ 4　[Source] リストから [Remote Filesystem] を選択します。

ステップ 5　パッチ ファイルを格納したリモート システム上のディレクトリ パスを、[Directory] フィールドに入力します。

アップグレード ファイルが Linux または Unix サーバ上にある場合は、ディレクトリ パスの先頭にフォワード 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。

- パスの記述はフォワード スラッシュ（/）で開始し、パスの区切り文字には常にフォワード 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 6　[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 7　[User Name] フィールドに、リモート サーバでのユーザ名を入力します。

ステップ 8　[User Password] フィールドに、リモート サーバでのパスワードを入力します。

ステップ 9　[Transfer Protocol] フィールドで、転送プロトコルを選択します。

ステップ 10　[Next] をクリックしてアップグレード プロセスを続行します。

ステップ 11　インストールするアップグレード バージョンを選択して、[Next] をクリックします。

- Cisco Unified Communications Manager Release 5.1(x) からアップグレードする場合は、パッチ セットと呼ばれる一連のファイルが必要です。リストから、インストールするアップグレード バージョンを選択します。アップグレード バージョンの名前はパッチ セットを表しており、ファイル拡張子は含まれていません。
- Cisco Unified Communications Manager Release 6.x または 7.x からのアップグレードの場合は、アップグレード ファイルの拡張子は sgn.iso になります。

ステップ 12　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、[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。

Warning: Another session is installing software, click Assume Control to take over the installation.

セッションを引き継ぐ場合は、[Assume Control] をクリックします。

[Assume Control] が表示されない場合は、Real Time Monitoring Tool でアップグレードを監視することもできます。

ステップ 13　アップグレードをインストールして、アップグレードされたパーティションに自動的に再起動する場合は、[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起動されます。

ステップ 14　アップグレードをインストールして、後でアップグレードされたパーティションに手動で再起動する場合は、次のいずれかの手順を実行します。

a.　[Do not reboot after upgrade] を選択します。

b.　[Next] をクリックします。

[Upgrade Status] 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ら、[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、[Settings] > [Version] を選択して、[Switch Version] をクリックします。

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起動されます。

ブリッジ アップグレード

ブリッジ アップグレードは、製造中止された Cisco Unified Communications Manager サーバから Cisco Unified Communications Manager の最新リリースをサポートするサーバに移行するユーザに移行パスを提供します。

サポートが中止されたサーバは、ブリッジ アップグレード サーバとして機能することが許可され、アップグレードおよび起動できますが、Cisco Unified Communications Manager は正しく機能しません。

Cisco Unified Communications Manager のバージョンを製造中止されたサーバ モデルでアップグレードすると、Cisco Unified Communications Manager によってアップグレード ログにメッセージが挿入されます。このアップグレード ログはアップグレードが Cisco Unified Communications オペレーティング システム 管理ページ ウィンドウで開始されると Web ブラウザに表示されるか、CLI を使用してアップグレードを実行した場合は、CLI を使用して表示できます。このメッセージによって、この新しいバージョンを DRS バックアップの取得にのみ使用できることが通知されます。ログの警告メッセージに続いて、ブリッジ アップグレードを実行しない場合にアップグレードをキャンセルできる遅延があります。

システムが新しい Cisco Unified Communications Manager バージョンを起動するとコンソールに、新しい Cisco Unified Communications Manager バージョンでは DRS バックアップのみが実行できるという警告が表示されます（「This hardware has limited functionality.Backup and Restore is the only supported functionality」）。コンソールの表示に制限があるため、警告は CLI および GUI セッション中に表示されます。

ブリッジ アップグレードを実行するには、次の手順に従います。

手順

ステップ 1　製造中止されたサーバの最初のノード（パブリッシャ）で新しい Cisco Unified Communications Manager バージョンへのアップグレードを実行します。実行できるアップグレードの種類については、この章の前の項を参照してください。コンソールに表示される、新しい Cisco Unified Communications Manager バージョンでは DRS バックアップのみが実行できるという警告を確認します（「This hardware has limited functionality.Backup and Restore is the only supported functionality」）。

ステップ 2　後続ノード（サブスクライバ）サーバで新しい Cisco Unified Communications Manager バージョンへのアップグレードを実行します。実行できるアップグレードの種類については、この章の前の項を参照してください。

ステップ 3　すべてのノード間でデータが同期されていることを確認します。これには、CLI コマンドの utils dbreplication runtimestate および utils dbreplication status を使用できます。詳細については、『*Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*』を参照してください。

ステップ 4　製造中止されたサーバの最初のノードにある新しい Cisco Unified Communications Manager バージョンを使用して、DRS バックアップを実行します。DRS バックアップはインストール時に入力されたクラスタ セキュリティ パスワードを使用して暗号化されます。このパスワードは復元時に「古い」パスワードの入力として求められることがあるため、このセキュリティ パスワードは「古い」パスワードとして記録してください。『*Disaster Recovery System Administration Guide*』を参照してください。

ステップ 5　製造中止されたサーバをネットワークから切断します。

ステップ 6　新しいサポートされるサーバの最初のノードに新しい Cisco Unified Communications Manager バージョンをインストールします。このサーバに新しいライセンスを取得して、インストールする必要があります。ガイドとして『*Installing Cisco Unified Communications Manager*』を参照してください。「新しい」パスワードの入力が求められます。このパスワードはステップ 4 で記録した「古い」パスワードとは異なります。『*Installing Cisco Unified Communications Manager*』では、Cisco Unified Communications Manager が受け入れる「新しい」セキュリティ パスワードの要件が示されています。この「新しい」パスワードは覚えておいてください。

ステップ 7　新しいサポートされたサーバの最初のノードで新しい Cisco Unified Communications Manager バージョンを使用して『*Disaster Recovery System Administration Guide*』の「Restoring the First Node only (Rebuilding the Publisher Alone)」の手順を実行します。まず、復元する最初のノードのみを選択します。最初のノードの復元が完了してから後続ノードを復元に選択できます。ステップ 4 で作成した製造中止されたサーバのバックアップ ファイルを使用します。ステップ 4 で記録した「古い」セキュリティ パスワードが求められます。詳細については、『*Disaster Recovery System Administration Guide*』を参照してください。

ステップ 8　新しい最初のノード サーバで、ブリッジ アップグレード前に製造中止になった最初のノード サーバでアクティブであったサービスをすべてアクティブにします。『*Administration Guide for Cisco Unity Connection Serviceability*』を参照してください。

ステップ 9　すべてのノード間でデータが同期されていることを確認します。これには、CLI コマンドの utils dbreplication runtimestate および utils dbreplication status を使用できます。詳細については、『*Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*』を参照してください。

アップグレード後の作業

アップグレードの完了後に、次の作業を実行してください。

- [Cisco Unified Serviceability] > [Tools] > [Service Activation] を選択して、Cisco Extension Mobility サービスをイネーブルにします。詳細については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

  （注）　Cisco Extension Mobility サービスをディセーブルにしないと、Cisco Extension Mobility のユーザは、Cisco Extension Mobility をサポートする電話機でログインおよびログアウトできなくなることに注意してください。

- 次のタイプのコールを発信して、電話機の機能を確認します。
  - ボイス メール
  - 局間
  - 携帯電話
  - 市内
  - 国内
  - 国際
  - シェアドライン
- 次の電話機能をテストします。

- 会議
- 割り込み
- 転送
- C 割り込み
- シェアドラインへの着信
- Do Not Disturb（サイレント）
- プライバシー
- プレゼンス
- CTI 呼制御
- ビジー ランプ フィールド

- 必要に応じて、Real Time Monitoring Tool を再インストールします。

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 ログには新しいログ メッセージが表示されなくなります。アップグレードが途中停止した場合は、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初めからやり直す必要があります。詳細については、「I/O スロットリングの影響」（P.7-11）を参照してください。

以前のバージョンへの復帰

アップグレード後も、アップグレード前に実行していたソフトウェア バージョンに戻すことができます。これには、[Switch Version] オプションを使用してシステムをアクティブでないパーティションのソフトウェア バージョンに切り替えます。

この項は、次の内容で構成されています。

- 「以前のバージョンへのクラスタの復帰」（P.7-18）
- 「以前のバージョンへのパブリッシャ ノードの復帰」（P.7-19）
- 「以前のバージョンへのサブスクライバ ノードの復帰」（P.7-20）
- 「以前の製品リリースに戻す場合のデータベース複製の再設定」（P.7-20）

以前のバージョンへのクラスタの復帰

（注）　クラスタをノンセキュアな Cisco Unified Communications Manager の旧リリース（Release 8.0 よりも前）にダウングレードする場合、バージョンを切り替える前にクラスタをロールバックに備えてください。旧リリースにダウングレードする前にクラスタをロールバックに備えないと、システム上の Cisco Unified IP Phone にある ITL ファイルをそれぞれ手動で削除しなければいけません。詳細については、『*Cisco Unified Communications Manager Security Guide*』の「Security by Default」の第 2 章を参照してください。

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。

	作業	詳細情報の参照先
ステップ 1	パブリッシャ ノードを以前のバージョンに戻します。	「以前のバージョンへのパブリッシャ ノードの復帰」（P.7-19）
ステップ 2	すべてのバックアップ サブスクライバ ノードを以前のバージョンに戻します。	「以前のバージョンへのサブスクライバ ノードの復帰」（P.7-20）
ステップ 3	すべてのプライマリ サブスクライバ ノードを以前のバージョンに戻します。	「以前のバージョンへのサブスクライバ ノードの復帰」（P.7-20）
ステップ 4	以前の製品リリースに戻す場合は、クラスタ内のデータベース複製を再設定します。	「以前の製品リリースに戻す場合のデータベース複製の再設定」（P.7-20）

以前のバージョンへのパブリッシャ ノードの復帰

手順

ステップ 1　次の URL を入力して、直接 Cisco Unified Communications オペレーティング システムの管理を表示します。

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

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　[Settings] > [Version] の順に選択します。

[Version Settings] ウィンドウが表示されます。

ステップ 4　[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 システムの管理に再度ログインします。

b. [Settings] > [Version] の順に選択します。

[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 Communications Manager Administration の管理にログインします。

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。

以前のバージョンへのサブスクライバ ノードの復帰

手順

ステップ 1　次の URL を入力して、直接 Cisco Unified Communications オペレーティング システムの管理を表示します。

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

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　[Settings] > [Version] の順に選択します。

[Version Settings] ウィンドウが表示されます。

ステップ 4　[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 システムの管理に再度ログインします。

b.　[Settings] > [Version] の順に選択します。

[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。

以前の製品リリースに戻す場合のデータベース複製の再設定

クラスタ内のサーバを元のバージョンに戻し、以前の製品リリースを実行する場合は、クラスタ内のデータベース複製を手動で再設定する必要があります。データベース複製を再設定するには、すべてのクラスタ サーバを以前の製品リリースに戻した後、パブリッシャ サーバ上で CLI コマンド **utils dbreplication reset all** を入力します。

Cisco Unified Communications オペレーティング システムの管理または CLI を使用してバージョンを切り替えようとすると、メッセージが表示され、以前の製品リリースに戻す場合はデータベース複製の再設定が必要になることが通知されます。

COP ファイル、ダイヤル プラン、およびロケールのインストール

この項は、次の内容で構成されています。

- 「COP ファイルのインストール」（P.7-21）
- 「ダイヤル プランのインストール」（P.7-21）
- 「ロケールのインストール」（P.7-21）

COP ファイルのインストール

次のガイドラインは COP ファイルのインストールに適用されます。この全般的なガイドラインが特定の COP ファイルのマニュアルと矛盾する場合は、COP ファイルのマニュアルに従ってください。

- COP ファイルをクラスタ内のすべてのサーバにインストールします。
- COP ファイルをインストールしたら、サーバを再起動します。

（注）　COP ファイルのインストール時に行った設定の変更を確実データベースに上書きするため、Cisco Unified Communications Manager を再起動します。この再起動はオフピーク期間に実行することを推奨します。

ダイヤル プランのインストール

ダイヤル プラン ファイルは、この章の初めの方で説明したソフトウェア アップグレードのインストール方法と同じ手順を使用して、ローカル ソースまたはリモート ソースからインストールできます。この手順の詳細については、「ソフトウェア アップグレード手順」（P.7-13）を参照してください。

ダイヤル プラン ファイルをシステムにインストールした後、Cisco Unified Communications Manager Administration にログインし、[Call Routing] > [Dial Plan Installer] を選択して、ダイヤル プランのインストールを完了します。

ロケールのインストール

シスコは、ロケール固有のバージョンの Cisco Unified Communications Manager ロケール インストーラを www.cisco.com で提供しています。このロケール インストーラはシステム管理者がインストールするもので、これを使用すると、ユーザがサポートされているインターフェイスを使用するときに、選択した翻訳済みテキストまたはトーン（使用可能な場合）を表示/受信できます。

ユーザ ロケール

ユーザ ロケール ファイルは、ユーザが選択したロケールの電話機表示用の翻訳済みテキストとボイス プロンプト（使用可能な場合）、ユーザ アプリケーション、および Web ページを提供します。ユーザ専用のロケール インストーラは Web 上にあります。

ネットワーク ロケール

ネットワーク ロケール ファイルは、国固有の電話機トーンやゲートウェイ トーン（使用可能な場合）を提供します。ネットワーク専用のロケール インストーラは Web 上にあります。

1 つのロケール インストーラに複数のネットワーク ロケールが組み合されている場合があります。

（注）　Cisco Media Convergence Server（MCS）またはシスコ承認の、顧客が提供するサーバは、複数のロケールをサポートできます。複数のロケール インストーラをインストールすることにより、ユーザは複数のロケールから選択できるようになります。

クラスタ内のすべてのサーバをリブートしないと、変更は有効になりません。クラスタ内のすべてのサーバにロケールのインストールが終了するまで、サーバをリブートしないように強くお勧めします。通常の業務時間後にサーバをリブートして、コール処理の中断を最小限にとどめてください。

ロケールのインストール

ロケール ファイルは、この章の初めの方で説明したソフトウェア アップグレードのインストール方法と同じ手順を使用して、ローカル ソースまたはリモート ソースからインストールできます。この手順の詳細については、「ソフトウェア アップグレード手順」（P.7-13）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。

Cisco Unified Communications Manager にインストールする必要のあるロケール ファイルについては、「Cisco Unified Communications Manager ロケール ファイル」（P.7-22）を参照してください。複数のロケールをインストールしてから、サーバを再起動できます。

Cisco Unified Communications Manager ロケール ファイル

Cisco Unified Communications Manager のロケールをインストールする場合、次のファイルをインストールする必要があります。

- ユーザ ロケール ファイル：特定の言語と国に関する言語情報が格納されています。ファイル名の表記は、次のとおりです。

  cm-locale-*language-country-version*.cop

- 複合ネットワーク ロケール ファイル：すべての国に対応した、さまざまなネットワーク項目（電話機のトーン、Annunciator、およびゲートウェイ トーンなど）の国固有のファイルが格納されています。複合ネットワーク ロケール ファイル名の表記は、次のとおりです。

  cm-locale-combinednetworklocale-*version*.cop

エラー メッセージ

ロケール インストーラをアクティブ化するときに発生する可能性のあるメッセージの説明については、表 7-1 を参照してください。エラーが発生した場合は、インストール ログにあるメッセージを表示できます。

表 7-1　ロケール インストーラのエラー メッセージと説明

メッセージ	説明
[LOCALE] File not found: <language>_<country>_user_locale.csv, the user locale has not been added to the database.	データベースに追加するユーザ ロケール情報が格納されている CSV ファイルが見つからない場合にこのエラーが発生します。これはビルド プロセスのエラーを示しています。
[LOCALE] File not found: <country>_network_locale.csv, the network locale has not been added to the database.	データベースに追加するネットワーク ロケール情報が格納されている CSV ファイルが見つからない場合にこのエラーが発生します。これはビルド プロセスのエラーを示しています。

表 7-1　ロケール インストーラのエラー メッセージと説明 （続き）

メッセージ	説明
[LOCALE] Communications Manager CSV file installer installdb is not present or not executable	このエラーが発生するのは、installdb という Cisco Unified Communications Manager アプリケーションが存在する必要があるためです。このアプリケーションは、CSV ファイルに格納されている情報を読み取り、この情報を正しく Cisco Unified Communications Manager データベースに適用します。このアプリケーションが見つからない場合、アプリケーションが Cisco Unified Communications Manager と共にインストールされていない（可能性は非常に低い）、削除された（可能性あり）、またはサーバに Cisco Unified Communications Manager がインストールされていない（可能性が最も高い）ことが考えられます。データベースに適切なレコードが格納されていないとロケールは機能しないため、ロケールのインストールは中止されます。
[LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maDialogs_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maMessages_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maGlobalUI_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt.Checksum.	このエラーは、システムがチェックサム ファイルの作成に失敗した場合に発生します。原因としては、Java 実行ファイの /usr/local/thirdparty/java/j2sdk/jre/bin/java が存在しない、Java アーカイブ ファイルの /usr/local/cm/jar/cmutil.jar が存在しないか損傷している、Java クラスの com.cisco.ccm.util.Zipper が存在しないか損傷していることなどが考えられます。これらのエラーが発生した場合でも、ロケールは正常に機能します。ただし、Cisco Unified Communications Manager Assistant ではローカライズされた Cisco Unified Communications Manager Assistant ファイルの変更は検出されません。
[LOCALE] Could not find /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt in order to update Unified CM Assistant locale information.	このエラーは、適切な場所にファイルが見つからない場合に発生します。原因としては、ビルド プロセスのエラーの可能性があります。
[LOCALE] Addition of <RPM-file-name> to the Cisco Unified Communications Manager database has failed!	このエラーは、ロケールのインストール時に発生した何らかの失敗が累積されたために発生し、終了条件を示しています。

サポートされる Cisco Unified Communication 製品

Cisco Unified Communications Manager ロケール インストーラがサポートしている製品のリストについては、次の URL から『*Cisco IP Telephony Locale Installer for Cisco Unified Communications Manager*』を参照してください。

http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-locale-51

TFTP サーバ ファイルの管理

TFTP サーバに、電話機で使用するファイルをアップロードできます。アップロード可能なファイルには、カスタム呼出音、コールバック トーン、および背景画像などがあります。このオプションは、接続先の特定のサーバにのみファイルをアップロードするもので、クラスタ内の他のノードはアップグレードされません。

デフォルトでは、ファイルは tftp ディレクトリにアップロードされます。tftp ディレクトリのサブディレクトリにもファイルをアップロードできます。

クラスタ内に 2 台の Cisco TFTP サーバが設定されている場合、両方のサーバで次の手順を実行する必要があります。この手順を実行しても、ファイルがすべてのサーバに配信されるわけではなく、クラスタ内の 2 台の Cisco TFTP サーバにも配信されません。

TFTP サーバ ファイルをアップロードまたは削除するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified Communications Operating System Administration] ウィンドウで、[Software Upgrades] > [TFTP File Management] を選択します。

[TFTP File Management] ウィンドウが表示され、現在アップロードされているファイルの一覧が表示されます。[Find] を使用すると、ファイルの一覧をフィルタリングできます。

ステップ 2　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。

a. [Upload File] をクリックします。

[Upload File] ダイアログボックスが表示されます。

b. ファイルをアップロードするには、[Browse] をクリックし、アップロードするファイルを選択します。

c. tftp ディレクトリのサブディレクトリにファイルをアップロードするには、[Directory] フィールドにサブディレクトリを入力します。

d. アップロードを開始するには、[Upload File] をクリックします。

ファイルのアップロードが成功すると、[Status] 領域に表示されます。

e. ファイルをアップロードしたら、Cisco TFTP サービスを再起動します。

（注）　複数のファイルをアップロードする場合は、すべてのファイルをアップロードした後に Cisco TFTP サービスを一度だけ再起動してください。

サービスの再起動の詳細については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

ステップ 3　ファイルを削除するには、次の手順を実行します。

a. 削除するファイルの横にあるチェックボックスをオンにします。

また、[Select All] をクリックするとすべてのファイルを選択でき、[Clear All] をクリックするとすべての選択をクリアできます。

b. [Delete Selected] をクリックします。

（注）　tftp ディレクトリに存在するファイルを修正する場合は、CLI コマンド **file list tftp** を使用して TFTP ディレクトリ内のファイルを表示し、**file get tftp** を使用して TFTP ディレクトリ内のファイルをコピーします。詳細については、『*Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*』を参照してください。

カスタム ログオン メッセージの設定

Cisco Unified Communications オペレーティング システムの管理ページ、Cisco Unified Communications Manager の管理ページ、およびコマンド ライン インターフェイスに表示されるカスタマイズされたログオン メッセージが含まれるテキスト ファイルをアップロードできます。

カスタマイズされたログオン メッセージ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　[Cisco Unified Communications Operating System Administration] ウィンドウで、[Software Upgrades] > [Customized Logon Message] を選択します。

[Customized Logon Message] ウィンドウが表示されます。

ステップ 2　アップロードするテキスト ファイルを選択して、[Browse] をクリックします。

ステップ 3　[Upload File] をクリックします。

（注）　アップロードできるファイルは 10kB 以内です。

システムにカスタマイズされたログオン メッセージが表示されます。

ステップ 4　デフォルトのログオン メッセージに戻すには、[Delete] をクリックします。

カスタマイズされたログオン メッセージが削除され、システムにデフォルトのログオン メッセージが表示されます。

CHAPTER 8

サービス

この章では、他のシステムに対する ping やリモート サポートの設定など、このオペレーティング 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。

この章の内容は、次のとおりです。

- 「ping」（P.8-1）
- 「リモート サポート」（P.8-2）

ping

[Ping Utility] ウィンドウでは、ネットワーク内の別のサーバに ping を送信できます。

別のシステムに ping を送信するには、次の手順に従います。

手順

ステップ 1 [Cisco Unified Communications Operating System Administration] ウィンドウで、[Services] > [Ping] の順に移動します。

[Ping Remote] ウィンドウが表示されます。

ステップ 2 ping の送信先となるシステムの 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 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 ping を送信する回数）を入力します。

（注） 複数回の ping を指定した場合、ping コマンドでは ping の日時を即時表示しません。ping コマンドがデータを表示するのは、指定した回数だけ ping を送信した後です。

ステップ 6 IPSec を検証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 Remote] ウィンドウに ping の統計情報が表示されます。

リモート サポート

[Remote Account Support] ウィンドウで、シスコのサポート担当者が指定日時にシステムにアクセスできるようにするためのリモート アカウントを設定できます。

リモート サポートは次の手順で行われます。

1. ユーザがリモート サポート アカウントを設定します。このアカウントには、シスコの担当者がアクセスできる制限時間があります。この制限時間には、さまざまな値を設定できます。
2. リモート サポート アカウントの設定が完了すると、パス フレーズが生成されます。
3. ユーザはシスコのサポートに電話し、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. シスコのサポート担当者はパス フレーズをデコーダ プログラムに入力し、パス フレーズからパスワードを生成します。
5. シスコのサポート担当者はデコードしたパスワードを使用して、お客様のシステムにリモート サポート アカウントでログインします。
6. アカウントの制限時間が経過すると、シスコのサポート担当者はリモート 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、次の手順に従います。

手順

ステップ 1　[Cisco Unified Communications Operating System Administration] ウィンドウで、[Services] > [Remote Support] の順に移動します。

[Remote Access Configuration] ウィンドウが表示されます。

ステップ 2　[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 文字以上が必要です。使用する文字はすべてアルファベットの小文字です。

ステップ 3　アカウントの保持期間となる日数を [Account Duration] フィールドに入力します。

デフォルトのアカウント保持期間は 30 日です。

ステップ 4　[Save] をクリックします。

[Remote Support Status] ウィンドウが表示されます。[Remote Support Status] ウィンドウの各フィールドについては、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方法については、シスコの担当者にお問い合わせください。

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、[Delete] ボタンをクリックします。

表 8-1　[Remote Support Status] のフィールドと説明

フィールド	説明
Decode version	使用しているデコーダのバージョンを表します。
Account name	リモート サポート アカウント名が表示されます。
Expiration	リモート アカウントが無効になる日時が表示されます。
Pass phrase	生成されたパス フレーズが表示されます。

INDEX

C

Certificate Trust List
　「CTL」を参照
CLI
CTL
　アップロード　6-4
　管理　6-1
　ダウンロード　6-2

I

Internet Explorer
　set セキュリティ オプション　6-1
IPSec
　新しいポリシーの設定　6-9
　管理　6-9
　表示ポリシー　6-11
　ポリシーの変更　6-11
　ポリシー フィールド（テーブル）　6-10

N

NTP サーバ設定　4-4

P

ping　8-1

S

SMTP 設定　4-5

T

TFTP サーバ、インストール ファイル　7-24

い

イーサネット設定　4-1
インストール
　ダイヤル プラン　7-21
　ロケール　7-21, 7-22
メニュー
　インストール / アップグレード　1-3
インストールされている製品　7-23
インストールされているソフトウェア
　手順　3-3
　フィールド（テーブル）　3-4

え

エラー メッセージ
　説明（テーブル）　7-22

お

オペレーティング システム
　概要　1-1
　管理者パスワード　2-2
　構成　1-2, 3-1
　サービス　1-4
　再起動　5-2
　ステータス　1-2, 3-1
　セキュリティ　1-3
　設定　1-2, 4-1

ソフトウェア アップグレード 1-3
ネットワーク ステータス フィールド（テーブル） 3-3
ハードウェア ステータス
手順 3-2
フィールド（テーブル） 3-2
はじめに 1-1
ブラウザ要件 1-2
ログイン 2-1

か

管理者パスワード 2-2

く

クラスタ ノード
手順 3-1
フィールド（テーブル） 3-1

こ

構成
オペレーティング システム 1-2, 3-1
コマンドライン インターフェイス
「CLI」を参照

さ

サービス
ping 1-4, 8-1
概要 8-1
リモート サポート 1-4
概要 8-2
設定 8-2
再起動
現在のバージョン 5-2
システム 5-1

し

時刻設定 4-6
システム
再起動 5-1
シャットダウン 5-2
ステータス
手順 3-4
フィールド（テーブル） 3-4
シャットダウン、オペレーティング システム 5-2
証明書
アップロード 6-4
管理 6-1
再作成 6-2, 6-3
削除 6-2
署名要求のダウンロード 6-7
ダウンロード 6-2
表示 6-2
有効期限日の監視 6-9
有効期限日の監視フィールド（テーブル） 6-9

す

ステータス
オペレーティング システム 1-2, 3-1
システム
手順 3-4
フィールド（テーブル） 3-4
ネットワーク
フィールド（テーブル） 3-3
ハードウェア
手順 3-2
フィールド（テーブル） 3-2

せ

セキュリティ
IE オプションの設定 6-1
概要 6-1

構成 1-3
メニュー 1-3
設定
IP 4-1
NTP サーバ 4-4
SMTP 4-5
イーサネット
手順 4-1
フィールド（テーブル） 4-2
概要 4-1
時刻 4-6
パブリッシャ 4-3
メニュー 1-2

そ

ソフトウェア
アップグレード 1-3
概要 7-1
ブリッジ アップグレード 7-16
リモート ソースから 7-14
ローカル ソースから 7-13
インストールされている
手順 3-3
フィールド（テーブル） 3-4

た

ダイヤル プランのインストール 7-21

ね

ネットワーク ステータス
フィールド（テーブル） 3-3

の

ノード、クラスタ
手順 3-1
フィールド（テーブル） 3-1

は

バージョン、再起動 5-2
ハードウェア、ステータス
手順 3-2
フィールド（テーブル） 3-2
パスワード、回復 2-2
パブリッシャ設定 4-3

ひ

表示、メニュー 1-2

ふ

ブラウザ要件 1-2

め

メッセージ、エラー
メニュー
インストール / アップグレード 1-3
セキュリティ 1-3
設定 1-2
表示 1-2

り

リモート サポート
ステータス フィールド（テーブル） 8-2
設定 8-2

ろ

ログイン

概要 2-1
手順 2-1
ロケール
インストーラ
エラー メッセージ（テーブル） 7-22
インストール 7-21, 7-22
ファイル 7-22